UNIVERSITAS INDONESIA

MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING*
(Studi Kasus: Penyidikan Tindak Pidana Hacking Website Partai Golkar Oleh Unit V IT & Cybercrime Bareskrim Polri)

Disertasi ini diajukan sebagai salah satu syarat untuk memperoleh gelar

DOKTOR
KAJIAN ILMU KEPOLISIAN

PETRUS REINHARD GOLOSE
NPM: 9103070058

PROGRAM STUDI KAJIAN ILMU KEPOLISIAN
PROGRAM PASCASARJANA
JAKARTA
2008

JUDUL DISERTASI : MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING* (*Studi Kasus: Penyidikan Tindak Pidana Hacking Website Partai Golkar Oleh Unit V IT & Cybercrime Bareskrim Polri*)

Disertasi ini telah diperbaiki dan disahkan oleh Tim Pembimbing Disertasi dalam Ujian terbuka Doktor di Program Studi Kajian Ilmu Kepolisian Program Pascasarjana Universitas Indonesia.

Jakarta, Juni 2008

Mengetahui
Ketua Program Studi
Kajian Ilmu Kepolisian,

Prof. Dr. Sarlito W. Sarwono, Psi
NIP : 130.440.955

Tim Promotor :

1. Prof. Dr. Sarlito W. Sarwono, Psi (Promotor)
2. Prof. Mardjono Reksodiputro, SH.MA (Ko Promotor)
3. Prof. Dr. Tb. Ronny Nitibaskara (Ko Promotor)

JUDUL DISERTASI : MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING* (*Studi Kasus: Penyidikan Tindak Pidana Hacking Website Partai Golkar Oleh Unit V IT & Cybercrime Bareskrim Polri*)

Disertasi ini telah dipertahankan di depan Komisi Penguji Ujian Terbuka Doktor di Program Studi Kajian Ilmu Kepolisian Program Pascasarjana Universitas Indonesia, pada tanggal, 7 Juni 2008 dan dinyatakan **LULUS** dengan predikat **(SANGAT MEMUASKAN/CUM LAUDE)**

Jakarta, Juni 2008

Mengetahui
Ketua Program Studi
Kajian Ilmu Kepolisian,

Prof. Dr. Sarlito W. Sarwono, Psi
NIP. 130.440.955

Tim Penguji :

1. Prof. dr. Purnawan Junadi, MPH (Ketua Sidang) — 1. .....
2. Prof. Dr. Sarlito W. Sarwono, Psi (Promotor/Penguji) — 2. .....
3. Prof. Mardjono Reksodiputro, SH.MA (Ko Promotor/Penguji) — 3 .....
4. Prof. Dr. Tb. Ronny Nitibaskara (Ko Promotor/Penguji) — 4. .....
5. Prof. Dr. Awaloedin Djamin, MPA (Penguji) — 5. .....
6. Prof. Dr. Valerine Kriekhoff, SH.MA (Penguji) — 6. .....
7. Prof. Dr. Barda Nawawi Arief, SH (Penguji) — 7. .....
8. Prof. Drs. Koesparmono Irsan, SH.MM.MBA (Penguji) — 8. .....
9. Prof. Dr. Toemin Masoem (Penguji) — 9. .....

DAFTAR ISI

DAFTAR BAGAN

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR SINGKATAN

AB:	*Algemene Bepalingen*
AI:	*Artificial Intelligence*
ADSL:	*Asymmetric Digital Subscriber Line*
AKBP:	Ajun Komisaris Besar Polisi
AKP:	Ajun Komisaris Polisi
APJII:	Asosiasi Penyelenggara Jasa Internet Indonesia
ARPA:	*Advanced Research Project Agency*
ATM:	*Automatic Teller Machine*
ACPO:	*Association of Chief Police Officers*
Bareskrim:	Badan Reserse Kriminal
BBC:	*British Broadcasting Corporation*
BCA:	Bank Central Asia
BAP:	Berita Acara Pemeriksaan
BPHN:	Badan Pembinaan Hukum Nasional
CD – ROM:	*Compact Disc - Read Only Memory*
CD:	*Compact Disc*
CETS:	*Child Exploitation Tracking System*
CFCE:	*Certified Forensic Computer Examiner*
CJS:	*Criminal Justice System*
CMS:	*Content Management System*
CNN:	*Cable News Network*
CPU:	*Central Processing Unit*
CoE:	Council of Europe
DMCA:	*Digital Millenium Copyright Act*
Depperindag:	Departemen Perindustrian dan Perdagangan
Dirjen:	Direktorat Jenderal
DNS:	*Domain Name Service*
DoS:	*Denial of Service*

DPP:	Dewan Pimpinan Pusat
E-Gov:	*Electronic Government*
Fasilkom UI:	Fakultas Ilmu Komputer Universitas Indonesia
FGD:	*Focus Group Discussion*
FRED:	*Forensic Recovery Evidence Device*
FTP:	*File Transfer Protocol*
Golkar:	Golongan Karya
HKI:	Hak Kekayaan Intelektual
HTCN:	*The High Tech Crime Network*
HTTP:	*Hyper Text Transfer Protocol*
IAC:	*Independent Artists Club*
IC3:	*Internet Crime Complaint Center*
IDT:	Inpres Desa Tertinggal
IMAP:	*Internet Message Access Protocol*
IP:	*Internet Protocol*
IRCP:	*Internet Relay Chat Protocol*
ISP:	*Internet Service Provider*
IT:	*Information and Technology*
IN2015:	*Intelligent Nation by 2015*
Internet:	*Interconnected Network*
Infotek:	Informasi dan Teknologi
Indag:	Industri dan Perdagangan
ITE	Informasi dan Transaksi Elektronik
Juklak:	Petunjuk Pelaksana
Jukmin:	Petunjuk Administrasi
Juknis:	Petunjuk Teknis
Juklap:	Petunjuk Lapangan
Kombes:	Komisaris Besar
Kompol:	Komisaris Polisi
KUHAP:	Kitab Undang-undang Hukum Acara Pidana

KUHP:	Kitab Undang-undang Hukum Pidana
Depkominfo:	Departemen Komunikasi dan Informatika
KPU:	Komisi Pemilihan Umum
Kanit:	Kepala Unit
Kbps:	*Kilobit Per Second*
LAN:	*Local Area Network*
LSM:	Lembaga Swadaya Masyarakat
MA:	Mahkamah Agung
MIT:	*Massachusetts Institute of Technology*
Mbps:	*Megabit Per Second*
Mahmilub:	Mahkamah Militer Luar Biasa
MAKEHJAPOL:	Mahkamah Agung-Kehakiman-Kejaksaan-Polisi
MSNBC:	*Microsoft Network National Broadcasting Company*
NCB:	*National Central Bureau*/Interpol
NGO:	*Non Government Organization*
NCCS:	*National Computer Crime Squad*
NNTP:	*Network News Transfer Protocol*
NHTCU:	*National Hi-Tech Crime Unit*
Pama:	Perwira Pertama
Pamen:	Perwira Menengah
Polri :	Kepolisian Negara Republik Indonesia
PBB:	Perserikatan Bangsa-Bangsa
PC:	*Personal Computer*
PDA	*Personal Digital Assistant*
PIN:	*Personal Identification Number*
PSK:	Pekerja Seks Komersial
POP3:	*Post Office Protocol, Version 3*
PPNS:	Penyidik Pegawai Negeri Sipil
PMPTK:	Peningkatan Mutu Pendidik dan Tenaga Kependidikan
Pusident:	Pusat Identifikasi

Puslabfor:	Pusat Laboratorium dan Forensik
RAM:	*Random Access Memory*
RUU:	Rancangan Undang-Undang
Rutan:	Rumah Tahanan Negara
SCI:	*Scientific Crime Investigation*
SIM:	Surat Ijin Mengemudi
Scele:	*Student Centered E-Learning Environment*
SPK:	Sentra Pelayanan Kepolisian
SPP:	Sistem Peradilan Pidana
SP3:	Surat Perintah Penghentian Penyidikan
SMTP:	*Simple Mail Transfer Protocol*
SOP:	*Standard Operating Procedure*
SPDP:	Surat Pemberitahuan Dimulainya Penyidikan
Sprinsidik:	Surat Perintah Penyidikan
Springas:	Surat Perintah Tugas
SSH:	*Secure Shell*
STOMP:	*Straits Times Online Mobile Print*
SD:	Sekolah Dasar
SMP:	Sekolah Menengah Pertama
SMA:	Sekolah Menengah Atas
TI:	Teknologi Informasi
TPTI:	Tindak Pidana di bidang Teknologi Informasi
TV:	Televisi
TK:	Taman Kanak-Kanak
TR:	Telegram Rahasia
TCD:	*Technology Crime Division*
TCP:	*Transmission Control Protocol*
TKP:	Tempat Kejadian Perkara
Telnet:	*Telecommunication Network*
UCLA:	*University of California Los Angeles*

U K:	*United Kingdom*
UU:	Undang-undang
VER:	*Visum et Repertum*
VPN-IP:	*Virtual Private Network* berbasis *Internet Protocol*
VoIP:	*Voice over Internet Protocol*
Warnet:	Warung Internet
WORM:	*Write - Once - Read – Many*
Wakabareskrim:	Wakil Kepala Badan Reserse Kriminal
WWW:	*World Wide Web*
YLBHI:	Yayasan Lembaga Bantuan Hukum Indonesia

KATA PENGANTAR

Cybercrime merupakan suatu kasus transnasional yang dihadapi oleh dunia pada saat ini. Salah satu bentuk kejahatan *cyber* adalah *hacking*. Sudah terdapat dua kasus *hacking website* yang telah disidangkan di Indonesia, yang pertama adalah kasus *hacking website* KPU yang ditangani oleh Polda Metro Jaya. Sedangkan yang kedua adalah kasus *hacking website* Partai Golkar yang ditangani oleh Unit V *IT & Cybercrime* Direktorat II Eksus Bareskrim Polri.

Dengan menggunakan metode penelitian kualitatif disertasi ini berupaya mengungkapkan Manajemen Penyidikan Tindak Pidana *Hacking* dengan studi kasus Penyidikan *hacking website* Partai Golkar oleh Unit V *IT & Cybercrime* Bareskrim Polri.

Judul ini saya pilih, mengingat ketertarikan saya terhadap *cybercrime* terutama kasus *hacking*, dimana kaedah normatif baik formil maupun materil belum diatur secara khusus pada saat itu , ditambah lagi dengan pengalaman penyidik, penuntut umum dan hakim dalam menangani kasus ini yang masih langka. Sedangkan ke depan, diperkirakan *cybercrime* masih akan semakin marak terjadi di Indonesia dengan beragam cara dan berbagai bentuk seiring dengan perkembangan teknologi yang semakin canggih.

Tujuan yang ingin dicapai dalam penelitian ini adalah untuk mengkaji dan memberikan pemahaman yang komprehensif mengenai *hacking* sebagai bagian dari *cybercrime*, karakteristik tindak pidana *hacking* yang berbeda dengan tindak pidana konvensional, dan manajemen penyidikan *hacking* serta faktor-faktor yang mempengaruhi meliputi faktor kepemimpinan, budaya organisasi dan *stakeholders*.

Untuk mendeskripsikan *hacking* sebagai suatu kejahatan maka diperlukan pengetahuan mengenai konsep dan teori kejahatan tentang *hacking*. Oleh karenanya penelitian ini didasarkan pada pengamatan di lapangan yaitu pengamatan terlibat selama penanganan kasus *hacking website* Partai Golkar, selanjutnya bagaimana pemaknaan atau penafsiran para penyidik Unit V *IT & Cybercrime* terhadap ketentuan yuridis normatif baik materil maupun formil yang berlaku saat itu dihubungkan dengan tindak pidana *hacking*.

Penafsiran terhadap ketentuan hukum dan karakteristik *hacking* yang khas berbeda dengan kejahatan konvensional merupakan permasalahan-permasalahan dan tantangan bagi para penyidik dalam melakukan penyidikan. Penyidik menerapkan prinsip-prinsip dan fungsi manajemen dalam proses penyidikan yang dipengaruhi oleh faktor-faktor kepemimpinan, budaya organisasi dan *stakeholders*.

Puji dan syukur saya ucapkan kepada Tuhan yang telah memberkati saya sehingga saya dapat menyelesaikan tulisan ini. Selama penulisan disertasi ini, telah begitu banyak menyerap energi, pikiran dan waktu saya selama berbulan-bulan. Selama itu pula, orang tua, istri dan anak-anak tercinta, setia memberikan perhatian, menemani dan menyemangati agar saya dapat menyelesaikan tugas ini dengan baik dan tepat waktu. Untuk itu saya ucapkan terima kasih dan rasa cinta yang kian mendalam kepada mereka. Tanpa dorongan mereka, saya telah patah arang di tengah jalan.

Dalam penulisan disertasi ini, saya sadar bahwa tanpa bimbingan, arahan dan bantuan dari berbagai pihak tentunya sulit untuk mewujudkan penulisan ini. Oleh karenanya saya ingin mengucapkan penghargaan yang tulus dan terimakasih yang mendalam kepada Prof. Parsudi Suparlan, Phd. (Alm) pada awalnya sebagai Promotor yang selalu bersedia memberikan waktu dan menyumbangkan pemikiran dalam penulisan disertasi ini. Semoga amal ibadahnya diterima oleh Tuhan Yang Maha Kuasa. Terima kasih yang sedalam-dalamnya juga saya sampaikan kepada Prof. Dr. Victor Purba, SH., LLM (Alm), yang pada awalnya melakukan pengujian untuk usulan penelitian saya, semoga Tuhan Yang Maha Kuasa menerima segala amal ibadahnya.

Selanjutnya saya juga ingin mengucapkan penghargaan dan terimakasih yang sebesar-besarnya kepada Prof. Dr. Sarlito W. Sarwono, Psi selaku Promotor, dan Prof. Mardjono Reksodiputro, S.H., M.A serta Prof. Dr. Tb. Ronny Nitibaskara selaku Ko Promotor. Prof. Dr. Awaloedin Djamin, MPA, Prof. Dr. Valerine Kriekhoff, SH., MA, Prof Dr. Barda Nawawi Arief, SH, Prof. Drs. Koesparmono Irsan, SH., MM, MBA, Prof. Dr. Toemin Masoem, yang senantiasa telah memberikan sumbangan pemikiran dalam penulisan disertasi ini.

Ungkapan yang tulus kepada Kabareskrim Polri Komjen Pol Drs. Bambang Hendarso Danuri, MM, Kalakhar BNN Irjen Pol Drs. Gories Mere, Brigjen Pol Drs. Surya Dharma dan seluruh anggota satuan tugas anti teror/bom atas dukungan moril kepada saya, kemudian terima kasih juga kepada Brigjen Pol. Wenny Warouw mantan Direktur II Tindak Pidana Ekonomi & Khusus Bareskrim Polri. Kombes Pol Drs. Edmon Ilyas, MH selaku Direktur II Tindak Pidana Ekonomi & Khusus Bareskrim Polri. Saya juga mengucapkan terima kasih yang sebesar-besarnya kepada seluruh penyidik Unit V *IT & Cybercrime* yang telah bersedia memberikan waktu untuk menerima permintaan wawancara, bahkan beberapa diantaranya bersedia diwawancara untuk kedua-kalinya demi pemahaman yang komprehensif atas gejala yang ada. Terima kasih juga saya ucapkan kepada rekan-rekan korespondensi di luar negeri yang telah bersedia memberikan jawaban atas rangkaian pertanyaan yang telah saya kirimkan.

Tidak lupa saya ucapkan terima kasih kepada Sdri. Sri Maulani Heuer, S.H., M.H. dan Sdr. Agung Nugroho W., S.H., S.Sos., M.M., serta rekan-rekan sekalian dari BM & Partners Law Office yang kerap memberikan pertimbangan, sumbang saran dan diskusi intensif, berikut pencarian berbagai bahan literatur sehingga disertasi ini dapat terselesaikan dengan baik. Selain itu, saya juga mengucapkan terima kasih kepada semua pihak yang telah membantu saya dalam menulis disertasi ini, yang tidak mungkin saya dapat sebutkan satu persatu.

Demikianlah, kata pengantar ini saya sampaikan, saya menyadari sekali walau saya telah berupaya sebaik mungkin, namun tentu saja tetap ada kelemahan dalam disertasi ini. Untuk itu saya sangat mengharapkan sumbangan saran serta kritik agar pada penulisan yang akan datang, saya dapat menghasilkan suatu karya yang lebih baik lagi. Untuk itu saya sangat menghargai setiap komentar dan saran pembaca sekalian. Pembaca dapat menghubungi saya di petrus@golose.net. Terima kasih untuk partisipasi dan investasi anda membaca disertasi saya.

Jakarta, 7 Juni 2008

Petrus Reinhard Golose

ABSTRAK

A. Nama : Petrus Reinhard Golose
Nomor Pokok Mahasiswa : 9103070058
B. Judul disertasi : Manajemen Penyidikan Tindak Pidana *Hacking* (*Studi Kasus: Penyidikan Hacking Website Partai Golkar oleh Unit V IT & Cybercrime Bareskrim Polri*)
C. Jumlah halaman : 338 halaman, 18 bagan, 20 gambar, 12 tabel, 7 lampiran dan 3 halaman riwayat hidup penulis

D. Isi ringkasan :

Disertasi ini merupakan hasil analisis dari penelitian kualitatif dan literatur secara mendalam yang terfokus pada manajemen penyidikan *hacking* oleh Unit V *IT & Cybercrime* yang diterapkan pada proses penyidikan kasus *hacking website* Partai Golkar. Kasus *hacking website* Partai Golkar merupakan kasus *hacking* pertama yang telah berkekuatan hukum tetap yang ditangani oleh Unit V *IT & Cybercrime*. Dalam pelaksanaan penyidikan *hacking*, Unit V *IT & Cybercrime* menghadapi permasalahan berkaitan dengan belum adanya ketentuan hukum materil yang secara tegas mengatur mengenai tindak pidana *hacking* pada saat itu dan belum adanya ketentuan hukum formil yang mengatur secara khusus mengenai penanganan bukti digital. Permasalahan tersebut berhasil dihadapi penyidik dengan melakukan interpretasi terhadap ketentuan hukum yang ada. Disertasi ini mengajukan suatu pengertian tindak pidana *hacking* sebagai setiap kegiatan yang menggunakan komputer atau sistem elektronik lainnya yang dilakukan dengan cara mengakses suatu sistem jaringan komputer baik yang terhubung dengan internet atau tidak, baik dengan tujuan maupun tidak, untuk memperoleh, mengubah dengan cara menambah atau mengurangi, menghilangkan atau merusak informasi dalam sistem komputer dan atau sistem elektronik lainnya dengan melawan hukum. *Hacking* berbeda dengan kejahatan konvensional. *Hacking* dapat dilakukan dari berbagai tempat yang terpisah atau tidak mengenal batas wilayah (*borderless*) dan transnasional (lintas batas negara). *Hacking* tidak meninggalkan jejak berupa catatan atau dokumen fisik dalam bentuk kertas (*paperless*) akan tetapi semua jejak hanya tersimpan dalam komputer dan jaringan tersebut dalam bentuk data atau informasi digital berupa *log files*. Penyidikan tindak pidana *hacking* juga berbeda dengan penyidikan kejahatan konvensional yaitu sebagian proses penyidikan dilakukan di *cyberspace*, adanya masalah yurisdiksi hukum, eksistensi bukti digital (*digital evidence*) dan penanganan komputer sebagai tempat kejadian perkara (*crime scene*) dimana diperlukan dukungan laboratorium komputer forensik untuk menganalisa bukti digital yang telah didapat. Penyidik menerapkan prinsip-prinsip dan fungsi manajemen dalam proses penyidikan. Proses manajemen tersebut diterapkan sebagai suatu siklus yang terdiri dari perencanaan, pengorganisasian, implementasi, serta pengawasan dan evaluasi. Secara khusus disertasi ini memotret proses manajemen penyidikan *hacking* sehingga menghasilkan proses manajemen yang terdiri dari penerimaan laporan (*accepting input*), penugasan (*assigning*), perencanaan (*planning*), pelaksanaan dan penyesuaian (*executing and adjusting*), pengendalian dan

evaluasi (*controlling and evaluation*), penyerahan hasil (*result delivery*), bantuan di persidangan (*court support*) serta dokumentasi hukum (*legal documentation*). Dengan manajemen penyidikan tindak pidana *hacking* tersebut, proses manajemen penyidikan tidak berhenti pada penyerahan berkas perkara ke penuntut umum saja, tetapi terus berlanjut ke tahap persidangan, dimana penyidik berperan sebagai saksi verbalisan dan membantu penuntut umum dalam menghadirkan saksi dan ahli. Disamping itu terdapat pula dokumentasi hukum, dimana putusan hakim akan didokumentasikan oleh penyidik sehingga dapat digunakan sebagai pertimbangan dalam perencanaan penyidikan pada kasus *hacking* yang terjadi di kemudian hari. Proses manajemen penyidikan tersebut tidak berjalan secara independen melainkan terdapat faktor-faktor yang mempengaruhi proses tersebut seperti: budaya organisasi, kepemimpinan dan peranan *stakeholders*. Berdasarkan hasil diskusi kelompok dan wawancara berpedoman diketahui bahwa Unit V *IT & Cybercrime* mempunyai budaya organisasi yang berbeda. Sub budaya organisasi yang ada saat ini di Unit V *IT & Cybercrime* mendorong anggotanya untuk terus maju (progresif) hal ini didukung dengan penghargaan dari pemimpin dan *peer pressure* dari anggota unit lainnya sebagai motivasi ekstrinsik. Peranan Kepala Unit sebagai pemimpin menjadi motivator Unit V *IT & Cybercrime* tampak dominan terlihat dari ketergantungan Unit V *IT & Cybercrime* terhadap pemimpinnya dalam hubungannya dengan *stakeholders* dan dalam melakukan transformasi budaya.

E. Jumlah halaman : 19 Peraturan Perundang-undangan, 75 buku, 23 jurnal, 16 artikel-artikel internet, 7 bahan tersier dalam kurun waktu tahun 1945-2003.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Disertasi ini merupakan hasil kajian secara mendalam mengenai manajemen penyidikan yang diterapkan di Unit V *IT & Cybercrime* Direktorat II Ekonomi dan Khusus Bareskrim Polri (selanjutnya akan disebut sebagai Unit V *IT & Cybercrime*) dalam proses penyidikan tindak pidana *hacking*. Disertasi ini memberikan penekanan khusus pada pendekatan interpretasi yang dilakukan oleh penyidik dalam mengungkapkan tindak pidana *hacking* berikut faktor-faktor yang mempengaruhi berjalannya sistem manajemen penyidikan tindak pidana *hacking* yang efektif. Disertasi ini telah melalui penelitian yang dilakukan secara terfokus dengan studi kasus penyidikan tindak pidana *hacking website* Partai Golongan Karya (Golkar) yang telah berhasil dilaksanakan oleh Unit V *IT & Cybercrime*. Proses penyidikan tersebut merupakan pelaksanaan tugas dan fungsi para penyidik dalam Unit V *IT & Cybercrime* dan merupakan implementasi dari fungsi dan prinsip manajemen penyidikan.

Tema besar yang diangkat dalam disertasi ini berangkat dari berkembangnya kejahatan di bidang teknologi informasi. Perkembangan teknologi informasi pada saat ini telah memunculkan berbagai fenomena baru di berbagai bidang kehidupan manusia. Kemajuan teknologi informasi terwujud dengan terciptanya komputer, jaringan komputer, internet, dan berbagai bentuk teknologi lainnya. Internet merupakan perpaduan antara teknologi komputer dan teknologi informasi. Internet digunakan sebagai media yang menghubungkan jaringan komputer yang terdapat di berbagai tempat. Perpaduan tersebut telah menciptakan jaringan komputer (*computer network*) yang bersifat mendunia.

Dipandang dari aspek kegunaan, terciptanya jaringan komputer tersebut telah memberikan sumbangan besar berupa kemudahan dalam berbagai kegiatan manusia. Para penggunanya dapat berkomunikasi, menyebarluaskan informasi atau bertukar informasi, bahkan bertransaksi secara cepat tanpa perlu adanya

eksistensi secara fisik pada tempat yang sama, serta tanpa perlu menyediakan dokumen dalam bentuk fisik berupa kertas (*paperless*). Di sisi lain, banyak pula pihak yang secara tidak bertanggung jawab menggunakan kemajuan teknologi tersebut untuk melakukan aksi-aksi kejahatan.

Salah satu kejahatan yang berkaitan dengan penggunaan sistem jaringan komputer dan teknologi informasi adalah *hacking*. Istilah *hacking* dapat diartikan sebagai suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa izin atau secara melawan hukum dari pemilik sah jaringan komputer tersebut (Hamzah dan Marsita, 1990: 38-39). *Hacking* dilakukan dengan memanfaatkan teknologi internet yang menghubungkan komputer satu dengan yang lainnya sehingga membentuk jaringan komputer. Tidak semua orang dapat melakukan tindak pidana *hacking*. Pelaku tindak pidana *hacking* atau *hacker*, biasanya mempunyai pengetahuan dan keahlian khusus di bidang komputer dan internet, seperti penguasaan atas ilmu komputer, *programming*, dan pemanfaatan media internet. Di samping itu, pelaku juga harus mempunyai akses, baik dalam kepemilikan komputer pribadi yang memiliki fasilitas internet maupun melalui penyewaan pada warung internet yang pada saat ini sudah menjamur hampir di seluruh kota di Indonesia.

Dengan menggunakan teknologi komputer dan komunikasi (dalam hal ini jaringan komputer melalui media internet), tindak pidana *hacking* dapat dilakukan dari berbagai tempat yang terpisah dengan korbannya. Bahkan, korban dan *hacker* dapat berasal dari negara yang berbeda. Sehingga tindak pidana *hacking* seringkali bersifat *borderless* (tanpa batas wilayah) bahkan transnasional (lintas batas negara). Di samping itu, tindak pidana *hacking* tidak meninggalkan jejak berupa catatan atau dokumen fisik dalam bentuk kertas (*paperless*), akan tetapi semua jejak hanya tersimpan dalam komputer dan jaringannya tersebut dalam bentuk data atau informasi digital (*log files)*. Karakteristik-karakteristik tersebutlah yang membedakan tindak pidana *hacking* dengan jenis tindak pidana konvensional.

Hacking merupakan salah satu jenis kejahatan yang merupakan dampak dari kemajuan teknologi informasi. Di Indonesia, menurut data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2003 telah terdapat

2.267 kasus *network incident,* sedangkan tahun 2004 terdapat 1.103 kasus serupa.[1] Akan tetapi, ternyata tidak banyak kasus tindak pidana *hacking* yang benar-benar telah ditindak oleh penegak hukum dan yang pelakunya telah dikenai hukuman. Sampai saat ini tercatat hanya dua kasus tindak pidana *hacking* di Indonesia yang berhasil diungkap dan diproses ke pengadilan, yaitu kasus tindak pidana *hacking website* Komisi Pemilihan Umum Nasional pada tahun 2004 dan kasus tindak pidana *hacking website* Partai Golkar pada tahun 2006. Kedua kasus tindak pidana *hacking* yang terjadi di Indonesia tersebut telah menarik perhatian publik karena secara entah kebetulan atau tidak keduanya dilakukan terhadap dua *website* yang bernuansa politik kental dan istilah *hacking* sendiri relatif baru di telinga publik karena terminologinya belum dikenali dan dipahami secara baik oleh masyarakat umum.

Keberhasilan pengungkapan kedua kasus tersebut, merupakan hasil kerja keras penyidik Polri yang bernaung dalam suatu unit yang khusus menangani kasus *cybercrime*. Yang pertama, kasus tindak pidana *hacking website* Komisi Pemilihan Umum dengan tersangka *hacker* bernama Dani Firmansyah berhasil diungkap dan disidik oleh Satuan *Cybercrime* Polda Metro Jaya. Yang kedua, kasus tindak pidana *hacking website* Partai Golkar yang ditangani oleh Unit V *IT & Cybercrime*.

Pengungkapan kasus tindak pidana *hacking* merupakan perwujudan pelaksanaan tugas dan fungsi Polri sebagai aparat penegak hukum, diantaranya dilaksanakan oleh Unit V *IT & Cybercrime* sebagai suatu unit khusus di bawah Direktorat II Ekonomi dan Khusus Bareskrim Polri yang didirikan dengan tugas khusus dalam rangka mengantisipasi adanya dampak dari kemajuan teknologi

---

[1]Adanya aktivitas internet yang merugikan seperti *spam, abuse* dan *fraud* telah diinventarisir oleh APJII. Data-data aktivitas tersebut adalah sebagai berikut: *Spam*: tahun 2003 sebanyak 8.389 kasus, tahun 2004: 3.872 kasus; *Network Incident*: tahun 2003 sebanyak 2.267 kasus, tahun 2004 sebanyak 1.003 kasus; *Open Proxy*: tahun 2003 sebanyak 1.210 kasus, tahun 2004 sebanyak 3.856 kasus; *Fraud*: tahun 2003 sebanyak 210 kasus dan tahun 2004 sebanyak 61 kasus. Yang dimaksud dengan *Network Incident* - kategori baru (berlaku mulai 01 Oktober 2003) - aktivitas yang dilakukan terhadap *network* milik orang lain serta segala aktivitas terkait dengan penyalahgunaan network. Sebelumnya, kategori ini disebut dengan *Abuse Network*. *Open Proxy* yang juga merupakan kategori baru yang berlaku 01 Oktober 2003, adalah aktivitas *spam* yang dilakukan dengan memanfaatkan dari kelemahan sistem. Sedangkan kategori *Fraud* yang dimaksud adalah penyalahgunaan kartu kredit. Data tersebut merupakan data terakhir yang dipublikasikan oleh APJII dan dapat diakses pada *website* APJII pada *www.apjii.or.id*.

informasi.

Langkah penanggulangan tindak pidana *hacking* oleh Unit V *IT & Cybercrime* berkaitan erat dengan fungsi Kepolisian Negara Republik Indonesia (Polri) sebagai induk organisasi yang lebih besar. Polri merupakan salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat (Pasal 2 Undang-undang No.2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, LN No. 2, TLN No. 4168 "**Undang-undang Kepolisian**"). Berkaitan dengan penegakan hukum, maka seorang polisi harus mengetahui hukum sebelum dia dapat menegakkan hukum secara adil dan cerdik (Sullivan, 1992: 113). Saat ini, masalah yang dihadapi oleh polisi Indonesia yang bertugas di lingkungan unit organisasi yang bertanggung jawab dalam penegakan hukum di bidang *IT & Cybercrime* adalah kondisi kejahatan yang harus diberantas berkembang sejalan dengan perkembangan teknologi informasi yang semakin canggih, sementara ketentuan hukum normatif yang harus ditegakkan belum tersedia pada saat itu. Sehingga dalam pelaksanaan tugas dan fungsinya, polisi dihadapkan pada berbagai permasalahan yang harus dicarikan solusinya agar tujuan organisasinya tetap dapat tercapai.

Upaya pemecahan masalah tersebut, dalam disertasi ini dipandang sebagai proses yang dilakukan dalam suatu sistem manajemen penyidikan yang dilaksanakan oleh Unit V *IT & Cybercrime* sejalan dengan upaya pencapaian tujuan organisasinya. Dalam pelaksanaan tugasnya, Unit V *IT & Cybercrime* ini dipimpin oleh seorang komisaris besar (Kombes) polisi dengan didukung oleh 25 personil yang terdiri dari para penyidik maupun staf pendukung. Di samping ketersediaan sumber daya manusia tersebut, sumber daya lain yang tersedia adalah sumber daya *logistic/material* berupa infrastruktur teknologi dan laboratorium forensik komputer serta kerjasama dengan pihak luar.

Berkaitan dengan pelaksanaan tugas dan fungsi penyidikan yang diembannya selaku penegak hukum di bidang teknologi informasi, Unit V *IT & Cybercrime* melaksanakan fungsi penyidikan[2]. Dalam melaksanakan penyidikan

---

[2]Fungsi penyidikan yang dilaksanakan Unit V *IT & Cybercrime* yaitu melaksanakan penyidikan sebagaimana dimaksud dalam Pasal 1 butir 2 Undang-undang No.8 Tahun 1981

tindak pidana *hacking*, para penyidik dalam Unit V *IT & Cybercrime* dihadapkan pada hambatan-hambatan yang berkaitan dengan karakteristik dari tindak pidana *hacking* yang telah diuraikan sebelumnya di atas seperti dalam proses penerapan hukum terhadap tindak pidana *hacking* dan dalam proses penyidikannya.

Masalah penerapan hukum terhadap tindak pidana *hacking* berkaitan dengan penerapan ketentuan yuridis materil. Sampai saat penelitian dilakukan, belum ada ketentuan hukum yang secara khusus mengatur mengenai tindak pidana *hacking*. Dalam prakteknya penyidik dituntut untuk melakukan interpretasi terhadap ketentuan yuridis materil yang tersedia untuk dapat mengatakan bahwa perbuatan *hacking* itu adalah suatu tindak pidana.

Sedangkan dalam proses penyidikannya, penyidik tidak dapat menghindari adanya hambatan-hambatan yang berkaitan dengan pengungkapan dan penyingkapan kasus tindak pidana *hacking* yang melibatkan penggunaan komputer dan internet baik sebagai modus, alat, maupun tujuan tindak pidana itu sendiri. Hal ini karena hukum acara pidana yang ada saat ini belum mengakomodasi pedoman yang dapat digunakan sebagai acuan khususnya berkaitan dengan keberadaan bukti digital, sehingga untuk itu, penyidik pun dituntut untuk melakukan interpretasi terhadap ketentuan yuridis yang tersedia, agar penyidikannya dapat menghasilkan suatu berkas perkara yang dapat diterima oleh penuntut umum.

Menghadapi hambatan-hambatan tersebut, Unit V *IT & Cybercrime* dituntut untuk mampu mendayagunakan seluruh kemampuan sumber daya yang dimilikinya dengan menggerakkan sistem manajemen penyidikannya, agar tujuan organisasi yang telah ditetapkan dapat tercapai. Praktek manajemen yang efektif dalam kepolisian adalah suatu sistem pemecahan masalah. Pemecahan masalah

---

tentang Kitab undang-undang Hukum Acara Pidana, LN No. 75, TLN No. 3209 "KUHAP", yaitu serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Undang-undang Hukum Acara Pidana untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Menurut Djamin (1995 : 123), penyidikan meliputi juga proses penyelidikan yang berarti serangkaian tindakan penyidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang. Sedangkan secara umum, Sullivan (1992 : 178) menyatakan bahwa penyidikan dilakukan oleh bagian reserse dengan melaksanakan penegakan hukum selektif yang merupakan suatu prosedur yang sangat baik dalam pemeriksaan suatu kejahatan dengan tidak merenehkan kejahatan-kejahatan yang dilakukan dengan cara licik, cerdas dan banyak akal.

yang dimaksud merupakan suatu proses kompleks yang dimulai dengan pengujian yang hati-hati atas setiap masalah untuk memperoleh sebanyak mungkin informasi mengenai masalah tersebut sehingga diperlukan suatu sistem manajemen untuk mentransformasikan ide-ide menjadi tindakan (aksi) (Butler, 1992 : 14-17). Sedangkan manajemen kasus adalah cara yang terencana, terkoordinasi, dan teruji untuk memaksimalkan baik efisiensi dan produktivitas dalam melaporkan serta menginvestigasi berbagai kasus. Keberhasilan manajemen kasus secara langsung berhubungan dengan tujuan suatu organisasi baik yang tertulis maupun yang tidak tertulis. Selain itu, tipe dari organisasi juga akan berpengaruh terhadap manajemen penyidikan terutama dalam hal pembagian tugas dan distribusi kewenangan dan pertanggungjawaban penyidik dalam melaksanakan tugasnya (Ward, 2005: 68,70).

Walaupun menghadapi hambatan yang cukup mendasar dalam pelaksanaan tugasnya, Unit V *IT & Cybercrime* sebagai salah satu unit kerja dalam Bareskrim Polri yang telah ditetapkan secara organisasional menjadi unit yang bertugas menegakkan hukum di bidang teknologi informasi dan memberantas kejahatan *IT & Cybercrime* diharapkan mampu mencapai tujuan organisasi yang telah ditetapkan.

Berkaitan dengan hal tersebut di atas, dalam disertasi ini, menarik untuk dibahas mengenai penerapan prinsip dan pendayagunaan fungsi manajemen dalam proses penyidikan oleh Unit V *IT & Cybercrime*. Hal ini berkaitan dengan tuntutan terciptanya teknik penyidikan tindak pidana *hacking* sebagai suatu *cybercrime* yang mempunyai sifat dan karakteristik yang khas, sehingga penanganan dalam penyidikannya pun melahirkan karakteristik yang khas, khususnya karena melibatkan penyidik yang harus mempunyai kemampuan/keahlian teknologi informasi yang baik; memerlukan sumber daya pendukung berupa infrastruktur teknologi informasi yang canggih dan *up-to-date* dalam suatu laboratorium forensik komputer; serta menuntut adanya hubungan yang baik dengan pihak internal dan eksternal kepolisian yang berada di dalam maupun di luar negeri.

Di samping itu, agar pembahasan mengenai manajemen penyidikan dapat dilakukan secara lebih mendalam sebagai hasil dari suatu sistem manajemen yang

menyeluruh, maka menjadi penting pula untuk dikaji faktor-faktor yang memberikan pengaruh bagi berjalannya sistem manajemen penyidikan dalam Unit V *IT & Cybercrime*. Faktor-faktor tersebut diantaranya adalah budaya organisasi, kepemimpinan dan lingkungan organisasi.[3] Oleh karenanya diperlukan kajian lebih lanjut mengenai pengaruh faktor-faktor tersebut dalam penerapan manajemen penyidikan tindak pidana *hacking* dengan meneliti dan mengkaji setiap gejala yang ada dan mengkaji hubungan antar gejala tersebut selama proses penyidikan kasus tindak pidana *hacking* oleh Unit V *IT & Cybercrime*. Dengan begitu, eksplorasi atas gejala dan hubungannya secara sistematis mampu menghasilkan abstraksi-abstraksi sebagai konsep-konsep yang saling mempunyai keterkaitan, untuk menggambarkan bekerjanya sistem manajemen penyidikan dalam Unit V *IT & Cybercrime*.

1.2 Masalah Penelitian

Disertasi ini pada dasarnya mengkaji tema-tema penting mengenai pelaksanaan manajemen penyidikan oleh Unit V *IT & Cybercrime* dalam proses penyidikan tindak pidana *hacking*. Dalam pelaksanaan penyidikan tindak pidana *hacking*, Unit V *IT & Cybercrime* menghadapi permasalahan berkaitan dengan belum adanya ketentuan hukum materil yang secara tegas mengatur mengenai delik tindak pidana *hacking* dan belum adanya ketentuan hukum formil yang mengatur mengenai perlakuan terhadap bukti digital dan proses penyidikannya. Permasalahan tersebut berhasil dihadapi dan dicarikan solusinya dengan mengupayakan proses penyidikan yang mencerminkan penerapan prinsip-prinsip dan pendayagunaan fungsi manajemen dalam proses menyidik dan menindak pelaku tindak pidana *hacking*. Dalam proses manajemen penyidikan tersebut

[3]Yang dimaksud budaya organisasi dalam disertasi ini adalah pola dasar dari asumsi, nilai, dan kepercayaan yang dipertimbangkan bersama sebagai arahan yang benar dari cara berpikir dan bertindak atas permasalahan dan kesempatan yang dihadapi oleh organisasi tersebut (McShane, 2003: 448). Sedangkan kepemimpinan pada umumnya adalah *apa yang harus dipunyai, dijalankan, dan atau dipergunakan oleh setiap orang yang berkedudukan sebagai "Pemimpin"* (Sunindhia dan Widiyanti, 1993: 99). Selanjutnya lingkungan organisasi dimaksudkan sebagai lingkungan eksternal dan lingkungan internal dalam organisasinya sendiri. Berbagai teori dan hasil penelitian mengenai pengaruh budaya organisasi dan gaya kepemimpinan dalam penerapan fungsi dan prinsip manajemen telah dihasilkan; salah satunya adalah Haris dan Bob Gett yang menyatakan bahwa budaya organisasi menentukan performa manajemen (McShane, 2003: 455).

terdapat faktor-faktor yang dianggap memberikan pengaruh terhadap berjalannya sistem manajemen yang efektif yaitu faktor budaya organisasi, kepemimpinan dan lingkungan organisasi (*stakeholders*).

Disertasi ini memfokuskan pada manajemen penyidikan tindak pidana *hacking* oleh Unit V *IT & Cybercrime*. Dalam menghadapi berbagai permasalahan dalam memproses kasus tindak pidana *hacking* sebagaimana diuraikan di atas, para penyidik Unit V *IT & Cybercrime* telah melakukan interpretasi terhadap berbagai ketentuan yuridis yang berlaku saat itu untuk mengatasi kesenjangan baik terhadap ketentuan hukum materil yang dapat diberlakukan terhadap suatu tindak pidana *hacking*, maupun ketentuan hukum formil untuk diterapkan pada proses penyidikan tindak pidana *hacking*. Interpretasi tersebut dilakukan oleh penyidik Unit V *IT & Cybercrime* dipandang sebagai suatu proses manajemen penyidikan yang diterapkan dalam Unit V *IT & Cybercrime* dalam rangka mencapai tujuan organisasi yang telah ditetapkan, dengan menggunakan dan mengupayakan sumber-sumber daya yang tersedia ataupun yang diperlukan dalam proses penyidikan. Proses manajemen tersebut diimplementasikan dalam suatu siklus manajemen yang terdiri dari perencanaan, pengorganisasian, implementasi serta pengawasan dan evaluasi selama proses penyidikan tindak pidana *hacking*. Analisis mengenai siklus manajemen tersebut diharapkan dapat mengidentifikasikan penyidikan tindak pidana *hacking* yang mempunyai karakteristik yang khas; mulai dari penerimaan laporan, pencarian dan pengumpulan bukti, penetapan tersangka, penentuan *locus* dan *tempus delictie*, sampai pembuatan berita acara tentang pelaksanaan tindakan penyidikan, dan penyerahan berkas perkara, tersangka dan barang bukti kepada penuntut umum. Untuk lebih memahami masalah tersebut di atas, dilakukan penelitian dengan studi kasus. Kasus yang diteliti adalah manajemen penyidikan yang diterapkan dalam penanganan kasus tindak pidana *hacking website* Partai Golkar tahun 2006 yang dilaksanakan oleh Unit V *IT & Cybercrime*.

Berkaitan dengan proses implementasi manajemen penyidikan oleh Unit V *IT & Cybercrime* tersebut, telah dikaji juga faktor-faktor yang memberikan pengaruh terhadap tercapainya proses manajemen penyidikan tindak pidana *hacking* yang efektif yaitu faktor budaya organisasi, kepemimpinan dan

stakeholders. Faktor-faktor tersebut dianggap memberikan kontribusi atau pengaruh baik positif maupun negatif dalam proses penyidikan yang dilakukan untuk mencapai target penyidikan yaitu pelimpahan berkas perkara ke penuntut umum.

1.3 Tujuan dan Kegunaan Penelitian

1.3.1 Tujuan Penelitian

Tujuan yang ingin dicapai dalam studi ini adalah untuk mengkaji dan memberikan pemahaman yang komprehensif mengenai:

a. Masalah penentuan delik pidana yang dilakukan oleh penyidik Unit V *IT & Cybercrime* terhadap tindak pidana *hacking* sebagai salah satu jenis *cybercrime* berdasarkan interpretasi penyidik terhadap ketentuan yuridis materil yang berlaku saat itu, sehingga tindak pidana *hacking* dapat diproses secara hukum;
b. Masalah penyidikan kasus tindak pidana *hacking* oleh Unit V *IT & Cybercrime* yang menunjukkan karakteristik yang khas sebagai hasil interpretasi penyidik terhadap ketentuan yuridis formil yang berlaku saat itu, sehingga kasus tindak pidana *hacking* dapat ditangani dengan dilakukan penyidikan yang menghasilkan berkas perkara yang diterima oleh penuntut umum;
c. Masalah penerapan prinsip dan pendayagunaan fungsi manajemen oleh Unit V *IT & Cybercrime* dalam proses penyidikan kasus tindak pidana *hacking* sehingga penyidik Unit V *IT & Cybercrime* mampu mencapai tujuan Unit V *IT & Cybercrime* serta faktor-faktor yang memberikan pengaruh terhadapnya, diantaranya budaya organisasi, kepemimpinan dan *stakeholders*.

1.3.2 Kegunaan Penelitian

Sejalan dengan tujuan penelitian, disertasi ini diharapkan juga dapat menghasilkan kegunaan baik secara teoritis maupun secara teknis. Secara teoritis, kegunaan studi ini adalah agar dapat memberikan kontribusi yang positif terhadap

perkembangan ilmu pengetahuan dengan memberikan alternatif pengertian *hacking* dan manajemen penyidikan serta memberikan masukan mengenai unsure-unsur dari tindak pidana *hacking*. Selain itu, disertasi ini juga diharapkan dapat memberikan gambaran mengenai penerapan fungsi dan prinsip manajemen dalam pelaksanaan penyidikan oleh Unit V *IT & Cybercrime* serta pengaruh kepemimpinan, budaya organisasi dan *stakeholders* pada manajemen organisasi kepolisian.

Selain kegunaan teoritis, disertasi ini juga memberikan kontribusi praktis berupa pengacuan pasal yang dapat diinterpretasikan untuk memenuhi unsur tindak pidana *hacking*, penyusunan prosedur penanganan bukti *digital* dan panduan pelaksanaan manajemen penyidikan kasus tindak pidana *hacking*, serta persyaratan khusus atau kualifikasi penyidik yang menangani kejahatan *hacking* atau kejahatan berbasis teknologi informasi lainnya.

Kontribusi praktis tersebut merupakan wujud dari kontribusi disertasi ini bagi kepolisian selain usulan agar diadakan diskusi lebih lanjut mengenai sistem kaderisasi di Unit V *IT & Cybercrime*.

1.4 Kerangka Konsep dan Teori

Studi ini menggunakan teori-teori dan konsep-konsep yang relevan yang dapat membantu dan memberikan pengertian yang bersifat teoritis maupun praktis selama proses penelitian. Adapun kerangka teori dan konsep tersebut meliputi teori-teori dan konsep-konsep mengenai kejahatan, *hacking* dan *cybercrime*, masyarakat informasi dan komunitas *virtual*, Polri baik dari aspek organisasi Polri maupun manajemen Polri, penyidikan dan manajemen penyidikan, serta sistem manajemen dan faktor-faktor yang memberikan pengaruh terhadap berjalannya sistem manajemen yaitu budaya organisasi, kepemimpinan dan lingkungan organisasi.

1.4.1 Kejahatan *Hacking* dan *Cybercrime*

Untuk dapat menjelaskan dan memberikan pemahaman yang komprehensif mengenai *hacking* sebagai suatu kejahatan, maka terlebih dahulu akan dijelaskan

mengenai konsep kejahatan yang akan dipergunakan dalam disertasi ini.

Dalam kaitannya dengan masalah penanggulangan kejahatan *hacking*, maka konsep kejahatan yang dipergunakan akan merujuk pada beberapa konsep kejahatan yang dikemukakan oleh ahli-ahli kriminologi maupun oleh ahli hukum pidana. Diantaranya Fattah (1997) dalam Nitibaskara (2000: 1) yang mengemukakan dua definisi secara hukum yang populer mengenai kejahatan, yaitu: pertama, merumuskan bahwa kejahatan adalah apa yang disebut oleh hukum sebagai kejahatan; kedua, menyatakan bahwa kejahatan adalah suatu tindakan yang disengaja atau kelalaian yang dapat dikenai sanksi pidana oleh hukum.

Pengertian mengenai kejahatan tersebut secara umum menyebutkan hukum dalam mendeskripsikan kejahatan. Hukum disini berkaitan dengan hukum pidana yang mengatur mengenai perbuatan-perbuatan yang dikategorikan sebagai tindak pidana. Menurut Nitibaskara (2000: 2), dalam hukum pidana terdapat tiga (3) permasalahan yang senantiasa menjadi pembicaraan, yaitu perbuatan yang dilarang, pelaku perbuatan yang dilarang, dan ancaman pidana. Perbuatan yang dilarang adalah perbuatan yang bertentangan dengan hukum; suatu perbuatan melawan hukum atau tidak memenuhi perintah hukum. Perbuatan ini ada yang bersifat nyata-nyata berlawanan dengan bunyi undang-undang dan ada pula yang menentang rasa keadilan masyarakat, tetapi tidak melanggar bunyi ketentuan hukum formal. Yang pertama disebut melawan hukum formal (*formeele wederechtelijkheidsbegrip*), sedangkan yang kedua melawan hukum material (*materiele wederechtelijkheidsbegrip*). Perbuatan yang mengandung sifat melawan hukum formal dapat diproses secara pidana menurut ketentuan pidana yang ada.

Kejahatan-kejahatan yang berkaitan dengan teknologi informasi dan telekomunikasi sebagaimana telah diuraikan di bagian Latar Belakang di atas, telah menjadi perhatian masyarakat luas bahkan masyarakat dunia. Berbagai pihak telah mengemukakan istilah-istilah yang dipergunakan untuk mendeskripsikan kejahatan tersebut. Ada yang menyebutnya sebagai kejahatan komputer, penyalahgunaan komputer atau pun tindak pidana yang berkaitan dengan komputer. Istilah dalam bahasa Inggris pun beragam, beberapa sarjana

menggunakan istilah *computer misuse*, *computer abuse*, *computer fraud*, *computer-related crime*, *computer-assisted crime*, atau *computer crime*. Di Indonesia istilah yang biasa dipergunakan adalah 'penyalahgunaan komputer' atau 'kejahatan komputer' (Reksodiputro, 1997: 10). Menurut U.S. Department of Justice, pengertian penyalahgunaan komputer adalah "*...any illegal act requiring Knowledge of computer technology for its perpretation, investigation, or prosecution*" (Al-Wisnubroto, 1999: 22). Sedangkan menurut Jongerius (1987), sebagaimana dikutip oleh Reksodiputro (1997: 11), penyalahgunaan komputer dapat dibagi dalam kategori sebagai berikut: (a) manipulasi komputer, (b) spionase komputer (c) sabotase komputer, (d) pemakaian secara tidak sah komputer, dan (e) 'memasuki' secara tidak sah sistem komputer.

Menurut Kartasudirja (1999: 1-4), istilah kejahatan komputer lebih sering digunakan di Indonesia karena penyalahgunaan komputer mengandung pengertian bahwa komputer adalah alat untuk melakukan tindak pidana. Masih menurut Kartasudirja (1999: 1), dalam kenyataannya seringkali komputer dan data komputer menjadi obyek tindak pidana. Menurutnya, kejahatan komputer memuat pengertian yang lebih luas yaitu semua tindakan yang menjadikan komputer sebagai sarana untuk melakukan suatu tindak pidana, juga merupakan obyek dari tindak pidana itu sendiri. Dalam Black`s Law Dictionary, kejahatan komputer diartikan sebagai kejahatan yang melibatkan penggunaan sebuah komputer seperti sabotase atau pencurian data yang disimpan secara elektronik (Bryan A. Garner, 2004: 399).

Dalam diskusi selanjutnya, dapat dibedakan kelompok sarjana hukum yang memberikan pengertian terhadap kejahatan komputer dalam pengertian yang sempit dan yang luas. Sarjana yang menganut pandangan yang sempit memberikan pengertian atau definisi kejahatan komputer sebagai 'tindak pidana yang dilaksanakan dengan menggunakan teknologi canggih, tanpa penguasaan ilmu dimana tindak pidana tidak mungkin dapat dilaksanakan' (*...any illegal act for which knowledge of computer technology is essential for its perpetration*) (Kartasudirja, 1999: 2). Sedangkan sarjana yang menganut pandangan kejahatan komputer dalam arti luas, diantaranya Comer, Mandell dan Sieber (Kartasudirja, 1999: 2 - 3). Comer memberikan pengertian kejahatan komputer (*computer fraud*)

sebagai setiap perbuatan yang dilakukan dengan itikad buruk untuk tujuan keuangan yang melibatkan komputer (Kartasudirja, 1999: 2). Mandell membagi kejahatan komputer atas dua kegiatan yaitu: (i) penggunaan komputer untuk tujuan melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan; (ii) ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan (Kartasudirja, 1999: 2). Selanjutnya, Sieber seperti dikutip oleh Kartasudirja (1999: 3) merumuskan kejahatan komputer secara lebih luas lagi, dengan menggolongkan kejahatan komputer sebagai kejahatan yang berhubungan dengan komputer (*computer-related crimes*) yang terdiri dari:

a. penipuan dengan memanipulasi komputer;
b. mata-mata dengan komputer dan pembajakan perangkat lunak;
c. sabotase komputer;
d. pencurian data;
e. memasuki *DP system* tanpa otoritas dan *hacking;*
f. komputer sebagai alat untuk melakukan kejahatan tradisional.

Pengertian-pengertian kejahatan komputer atau penyalahgunaan komputer tersebut di atas, pada prinsipnya memberikan penjelasan tindakan-tindakan kejahatan yang melibatkan komputer. Kartasudirja (1999: 3) menyimpulkan bahwa dalam pengertian yang luas, kejahatan komputer adalah tindak pidana apa saja yang dilakukan dengan memakai komputer ('*hardware*' dan '*software*') sebagai sarana/alat, atau komputer sebagai obyek, baik untuk memperoleh keuntungan maupun tidak, dengan merugikan pihak lain, sedangkan dalam pengertian sempit, diartikan sebagai tindak pidana yang dilakukan dengan menggunakan teknologi komputer yang canggih.

Upaya penanggulangan dan pencegahan kejahatan komputer atau penyalahgunaan komputer di dunia internasional telah dilakukan dengan mengadakan berbagai pertemuan tingkat internasional yang khusus membahas masalah ini, diantaranya Kongres Persatuan Bangsa-Bangsa mengenai *The Prevention of Crime and the Treatment of Offender* ke-8 tahun 1990 di Havana, Kuba dan kongres ke-10 tahun 2000 di Wina (Shinder, 2002: 17). Pada kongres

tersebut secara khusus telah dibahas topik mengenai *crime related to computer network*, dan menghasilkan pengertian mengenai *cybercrime* yang dibagi menjadi 2 (dua) kategori definisi yaitu:

a. *Cybercrime* dalam pengertian sempit (kejahatan komputer), adalah tingkah laku *illegal* apapun yang diarahkan dengan cara pengoperasian elektronik yang mentargetkan keamanan sistem komputer dan data yang diprosesnya.
b. *Cybercrime* dalam pengertian luas (kejahatan berkaitan dengan komputer), adalah tingkah laku *illegal* apapun yang dilakukan dengan cara, atau sehubungan dengan, sistem komputer atau jaringan, termasuk kejahatan seperti kepemilikan secara *illegal* (dan) menawarkan atau mendistribusikan informasi melalui sistem komputer atau jaringan.

Istilah *cybercrime* untuk menjelaskan kejahatan yang berhubungan dengan komputer dan jaringannya juga dipergunakan oleh Shinder (2002: 5) yang menyatakan bahwa dalam *cybercrime* terdapat berbagai hubungan tindak kejahatan dengan komputer atau jaringan komputer diantaranya:

a. Komputer atau jaringan komputer dapat menjadi alat kejahatan dalam arti digunakan untuk melakukan kejahatan.
b. Komputer atau jaringan komputer dapat menjadi sasaran kejahatan atau korban.
c. Komputer atau jaringan komputer dapat digunakan untuk maksud-maksud insidental yang berkaitan dengan kejahatan, umpamanya mencatat semua penjualan obat-obatan secara ilegal.

Disertasi ini akan menggunakan istilah *cybercrime* baik dalam arti luas maupun dalam arti sempit tersebut di atas untuk menggambarkan tindak pidana yang harus ditanggulangi oleh Unit V *IT & Cybercrime*, khususnya terhadap tindak pidana *hacking* yang dianggap sebagai bagian dari *cybercrime*. Istilah *hacking* digunakan untuk menggambarkan usaha (baik yang berhasil maupun tidak) untuk memperoleh akses ilegal ke dalam suatu sistem komputer (Burdett *et al.*, 1995 : 95). Dalam pengertian tersebut, tindak pidana *hacking* dianggap sebagai suatu penetrasi ke sebuah komputer atau sistem komputer secara diam-diam dan tanpa hak. Cara melakukan tindak pidana *hacking* dapat bermacam-macam, baik secara langsung dengan menggunakan komputer di suatu tempat

yang tetap, maupun menggunakan terminal luar (*remote terminal*) di tempat lain.

Suatu perbuatan yang merugikan masyarakat yang belum dirumuskan dalam hukum pidana positif sebagai perbuatan pidana, secara yuridis belum dianggap sepenuhnya sebagai suatu kejahatan (Nitibaskara, 2000: 2). Pendapat tersebut sangat penting untuk pembahasan dalam disertasi ini, berkaitan dengan fakta bahwa tindak pidana *hacking* secara khusus belum ada pengaturannya dalam hukum pidana Indonesia, sementara *hacker* telah dapat diproses secara pidana dan bahkan mendapat sanksi pidana berdasarkan putusan pengadilan negeri yang berwenang. Gejala inilah yang menjadi salah satu bahasan dalam disertasi ini berkaitan dengan pemanfaatan ketentuan hukum pidana yang tersedia oleh penyidik Polri untuk menegakkan hukum di bidang teknologi informasi dan telekomunikasi.

Untuk memahami dan mengkaji gejala tersebut di atas, perlu disampaikan faktor-faktor yang saling temali dalam suatu kejahatan yaitu (i) pelaku kejahatan, (ii) modus kejahatan, (iii) korban kejahatan, (iv) reaksi sosial atas kejahatan, (v) hukum atas kejahatan tersebut (Nitibaskara, 2000: 1). Faktor-faktor tersebut dipergunakan sebagai salah satu ukuran untuk memahami tindak pidana *hacking*. *Hacker* telah menimbulkan reaksi sosial dalam masyarakat, oleh karenanya *hacking* dapatlah dianggap sebagai suatu tindak pidana bagi masyakarat dan karenanya memerlukan tindakan hukum atas perbuatannya tersebut.

Masalahnya, dalam penegakan hukum selalu harus terikat pada ketentuan perundang-undangan. Dalam praktek, adakalanya penegak hukum memerlukan untuk memberikan penafsiran (interpretasi) kepada istilah-istilah tertentu dalam perundang-undangan (Kanter dan Sianturi, 1982: 63). Dalam Kamus Besar Bahasa Indonesia, interpretasi berarti pemberian kesan, pendapat atau pandangan teoritis terhadap sesuatu atau penafsiran (1995: 384). Pendapat ini tidaklah jauh dari kenyataan karena seringkali penyidik Polri selaku penegak hukum melakukan interpretasi terhadap peraturan perundang-undangan yang berlaku untuk memproses dan menindak suatu perbuatan yang oleh masyarakat dianggap merugikan dan melanggar hukum. Begitu pun dalam kasus tindak pidana *hacking*, penyidik Polri telah berhasil menindak dan memproses kasusnya dengan menggunakan peraturan perundang-undangan yang tersedia dalam perumusan

delik pidananya berdasarkan proses interpretasi. Bahkan kasus *hacking* yang berhasil disidik tersebut, telah diadili di hadapan pengadilan negeri yang berwenang dan pelakunya telah menjalani hukuman pidana.[4]

Berkaitan dengan penafsiran peraturan perundang-undangan oleh penegak hukum, maka perlu diperhatikan urutan penafsiran yang disampaikan oleh Kanter dan Sianturi (1982: 65) yaitu: **Pertama** dilakukan penafsiran secara otentik, yaitu mencari pasal-pasal undang-undang; **Kedua** penafsiran menurut penjelasan undang-undang (*Memorie van teolichting*); **Ketiga** penafsiran sesuai dengan yurisprudensi, yaitu terutama mencari dalam Putusan-putusan Kasasi Mahkamah Agung, Putusan-putusan banding atau putusan pengadilan/mahkamah pada tingkat pertama yang telah mempunyai kekuatan hukum tetap dan sudah lazim diikuti oleh peradilan lainnya; **Keempat** penafsiran menurut doktrin hukum pidana.

Dalam proses penyidikan, selain harus memperhatikan ketentuan yuridis materil dalam merumuskan delik yang dipersangkakan, penyidik juga harus selalu memperhatikan ketentuan yuridis formal. Ketentuan yuridis materil meliputi ketentuan tindak pidana yang diatur di dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan yang diatur di luar KUHP untuk tindak pidana khusus. Sampai saat ini belum ada ketentuan tindak pidana *hacking* yang diatur secara eksplisit dalam suatu undang-undang. Dalam perkembangannya, penegakan hukum atas tindak pidana *hacking* dilaksanakan melalui upaya interpretasi dengan mengacu pada beberapa tindak pidana yang unsur-unsurnya dapat diinterpretasikan sebagai tindak pidana *hacking*, yaitu:

Dalam Pasal 22 huruf b jo Pasal 50 Undang-undang Republik Indonesia nomor 36 tahun 1999 tentang Telekomunikasi, LN No. 154, TLN No. 3881 ("Undang-undang Telekomunikasi"):

---

[4]Kasus Tindak Pidana *Hacking Website* Komisi Pemilihan Umum Nasional dengan pelaku Dani Firmansyah telah diadili oleh hakim Pengadilan Negeri Jakarta Pusat dengan register perkara nomor: 1322/PID.B/2004/PN.JKT.PST, dan pelaku dijatuhi hukuman pidana selama 6 bulan 21 hari karena dinyatakan bersalah telah melakukan perbuatan pidana memanipulasi akses kejaringan telekomunikasi khusus. Sedangkan kasus Iqra Syafaat (pelaku tindak pidana *hacking website* Partai Golkar) telah diadili oleh hakim Pengadilan Negeri Jakarta Barat dengan register perkara nomor: 3254/PID.B/2006/PN.JKT.BAR. Dalam putusannya majelis hakim telah memutuskan bahwa Iqra Syafaat telah melakukan tindak pidana tanpa hak, tidak sah memanipulasi akses jaringan telekomunikasi dan dijatuhi hukuman pidana selama 1 tahun 2 bulan.

"Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jasa telekomunikasi" (Pasal 22 huruf b).

"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah)" (Pasal 50).

Pasal 406 ayat (1) KUHP (Moeljatno, 2001: 146)

"Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah."

Pasal 64 ayat (1) KUHP (Moeljatno, 2001: 28)

"Jika antara beberapa perbuatan, meskipun masing-masing merupakan kejahatan atau pelanggaran, ada hubungannya sedemikian rupa sehingga harus dipandang sebagai satu perbuatan berlanjut (*voortgezette handeling*), maka hanya dikenakan satu aturan pidana; jika berbeda-beda, yang dikenakan yang memuat ancaman pidana pokok yang paling berat."

Selain ketentuan yuridis normatif materil untuk pendeskripsian atau perumusan delik/tindak pidana *hacking* tersebut di atas, tersedia pula ketentuan yuridis formal yang harus diterapkan dalam proses penyidikan *hacking*. Ketentuan yang dimaksud adalah ketentuan dalam Kitab Undang-undang Hukum Acara Pidana (KUHAP) maupun ketentuan dalam undang-undang lain yang berkaitan dengan pengakuan bukti elektronik (*digital evidence*) sebagai salah satu alat bukti yang diakui dalam persidangan pemeriksaan perkara pidana di Indonesia.[5]

---

[5]Pasal 184 KUHAP mengandung asas segitiga pembuktian (*evidence triangle*) untuk memenuhi aspek legalitas dan aspek legitimasi dalam pembuktian pada perkara pidana di hadapan pengadilan. Saat ini hanya beberapa perundang-undangan di Indonesia yang mengatur tentang *digital evidence*, antara lain:

a. Undang-undang No. 8 tahun 1997 tentang Dokumen Perusahaan, "Undang-undang

1.4.2 Masyarakat Informasi dan Komunitas Virtual

Masyarakat menurut Suparlan terdiri dari dua bagian besar yaitu masyarakat luas *(society)* dan masyarakat terbatas *(community)* (Suparlan, 2003: 31). Masyarakat *(society)* dilihat sebagai sebuah satuan kehidupan yang menempati sebuah wilayah tertentu dengan batas yang jelas, yang mempunyai sebuah kebudayaan dengan pranata-pranata sebagai pedoman operasional dalam bertindak kehidupan sehari-hari dan dapat hidup bersama di dalam wilayahnya. Walaupun anggota masyarakat dapat tidak saling mengenal satu sama lain, mereka terikat pada sebuah ideologi mengenai kebersamaan dan jati diri mereka. Sedangkan pengertian dari sebuah komuniti *(community)* adalah kesatuan sosial yang terutama terikat oleh rasa kesadaran wilayah.

Berkat kemajuan teknologi informasi dan komunikasi, timbul fenomena baru yaitu beralihnya masyarakat modern dari 'masyarakat industri' menjadi 'masyarakat informasi' (Reksodiputro, 1997: 2). Masyarakat informasi menguasai dan menggunakan informasi yang kebanyakan tersimpan data elektronik atau digital dalam komputer atau jaringan komputer. Para pelaku kejahatan berusaha

---

Dokumen Perusahaan" LN No. 18, TLN No. 3674. Dengan Undang-undang ini, Pemerintah Indonesia berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan), misalnya *Compact Disc - Read Only Memory* (*CD-ROM*), dan *Write-Once-Read-Many* (WORM), sebagai alat bukti yang sah.

b. Undang-Undang No. 25 tahun 2003 tentang Perubahan atas undang-undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang, "Undang-undang Tindak Pidana Pencucian Uang" LN No. 108, TLN No. 4324. Undang undang ini mengatur mengenai alat bukti elektronik atau *digital evidence* (Pasal 38 huruf (b)) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.
c. Undang-Undang No. 15 tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, "Undang-undang Pemberantasan Tindak Pidana Terorisme" LN No. 45, TLN No. 4284. Undang-undang ini yang mengatur mengenai alat bukti elektronik (Pasal 27 huruf (b)) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.
d. Undang-undang Telekomunikasi.
e. Undang-undang No. 32 Tahun 2002 Tentang Penyiaran, "Undang-undang Penyiaran" LN No. 139, TLN No. 4252.
f. Undang-undang No. 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang, "Undang-undang Pemberantasan Tindak Pidana Perdagangan Orang" LN No. 58, TLN No. 4720.

untuk memperoleh atau menyalahgunakan data elektronik atau digital tersebut dengan mencari akses dalam jaringan komputer atau membuat modus baru dengan kecanggihan komputer untuk tujuan keuntungan pribadi yang dapat merugikan orang lain ataupun masyarakat pada umumnya.

Lebih lanjut, dengan terciptanya jaringan komputer melalui media internet tercipta pula komunitas yang dikenal dengan istilah *virtual community*, yaitu suatu komunitas yang beranggotakan para pengguna internet. Komunitas *virtual* didefinisikan sebagai suatu komunitas masyarakat yang saling berbagi minat, gagasan dan perasaan melalui internet atau jaringan kolaboratif lainnya (Miller dan Slater, 2003: 21-22).

1.4.3 Polri

Kepolisian Negara Republik Indonesia merupakan salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat (Pasal 2 Undang-undang Kepolisian). Menurut Awaloedin Djamin (2001: 49), fungsi Polri meliputi fungsi represif, preventif dan pre-emitif. Fungsi represif dilaksanakan melalui upaya penyelidikan dan penyidikan yang dilakukan oleh Polri. Fungsi preventif adalah pelaksanaan pencegahan atas terjadinya suatu tindak pidana dalam masyarakat. Sedangkan fungsi represif adalah fungsi pencegahan tidak langsung terhadap tindak pidana. Pelaksanaan tugas dan fungsi Polri memerlukan bantuan teknis seperti laboratorium indentifikasi forensik, komunikasi elektronik serta bantuan administratif yang tepat misalnya sistem perencanaan, penganggaran, sistem manajemen personel, logistik dan pengawasan.

Sedangkan menurut Suparlan dalam artikelnya yang berjudul Implementasi Polisi Masyarakat pada Fungsi Lalu Lintas (1999: 397), fungsi polisi adalah untuk menegakkan hukum, memelihara keteraturan dan ketertiban dalam masyarakat, mendeteksi dan mencegah terjadinya kejahatan serta memeranginya. Fungsi Polri mencakup tiga hal, antara lain: (1) Polri menegakkan hukum dan bersamaan dengan itu menegakkan keadilan sesuai dengan hukum yang berlaku; (2) memerangi kejahatan yang menggangu dan merugikan masyarakat dan Negara;

(3) mengayomi warga masyarakat dan Negara dari ancaman dan kejahatan yang mengganggu dan merugikan. Fungsi tersebut selanjutnya dijabarkan dalam tugas dan wewenang Polri. Demikian juga menurut Mardjono Reksodiputro (1999: 75) dalam artikelnya Polisi dan Masyarakat Dalam Era Reformasi: Polisi Sebagai Alat Penegak Hukum, fungsi Polri meliputi penegakan hukum pidana dan pemelihara ketertiban keamanan dan ketertiban masyarakat. Fungsi Polri yang diharapkan oleh masyarakat adalah fungsi penegakan hukum pidana (*enforcing the criminal law*).

Pelaksanaan fungsi Polri sebagaimana telah dijelaskan di atas, bertujuan untuk mewujudkan keamanan dalam negeri yang meliputi terpeliharanya keamanan dan keterlibatan masyarakat, tertib dan tegaknya hukum, terselenggaranya perlindungan, pengayoman dan pelayanan masyarakat, serta terbinanya ketentraman masyarakat dengan menjunjung tinggi hak asasi manusia sebagaimana diatur dalam Pasal 4 Undang-undang Kepolisian. Fungsi Polri selanjutnya dijabarkan dalam tugas pokoknya memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, dan memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat (Pasal 13 Undang-undang Kepolisian). Penegakan hukum sebagai tugas pokok Polri dilaksanakan melalui upaya penyidikan.

1.4.3.1 Organisasi Polri

Untuk melakukan tugas dan mencapai tujuannya, Polri mempunyai susunan organisasi dan tata kerja Polri diatur oleh Presiden (Pasal 7 Undang-undang Kepolisian). Polri terbagi atas satuan-satuan fungsional yang terdiri dari: unsur pimpinan, unsur pembantu pimpinan atau staf, unsur pelaksanaan staf, unsur pelaksana pendidikan dan staf khusus, dan unsur pelaksana utama pusat.

Menurut Stoner (1996: 6), organisasi adalah dua orang atau lebih yang bekerja sama dalam cara yang terstruktur untuk mencapai sasaran spesifik atau sejumlah sasaran. Menurutnya, organisasi mempunyai prestasi kerja organisasi, yaitu ukuran seberapa efisien dan efektif sebuah organisasi itu mencapai tujuan yang memadai. Efisiensi adalah kemampuan untuk meminimalkan penggunaan sumber daya dalam mencapai tujuan organisasi. Sedangkan efektivitas merupakan kemampuan untuk menentukan tujuan yang memadai: "melakukan hal dengan

tepat".

Organisasi apapun yang mempunyai orientasi pada sasaran, seperti Polri, perlu pengendalian peraturan. Max Weber (1864-1920) mengembangkan sebuah teori mengenai manajemen birokrasi yang menekankan pada kebutuhan akan hierarki yang ditetapkan dengan ketat untuk mengatur peraturan dan wewenang yang jelas. Birokrasi merupakan organisasi dengan struktur formal dan struktur hierarkis yang disahkan, juga merujuk pada proses struktur formal di dalam sebuah organisasi (Stoner, 1996: 37).

Mengacu pada Keputusan Polri No.Pol.:KEP/54/X/2002 tanggal 17 Oktober 2002, terdapat struktur organisasi Polri dari tingkat Markas Besar sampai dengan Polres. Dalam struktur tersebut terdapat Bareskrim (Badan Reserse Kriminal) sebagai suborganisasi Polri, yang terbagi menjadi beberapa bagian. Unit V *IT & Cybercrime* adalah unsur pelaksana pada Direktorat II Ekonomi dan Khusus Bareskrim Polri yang bertugas melaksanakan penyelidikan dan penyidikan tindak pidana *cyber* (*cybercrime*) terutama kegiatan yang berhubungan dengan teknologi informasi (teknologi komputer, teknologi telekomunikasi, teknologi elektronika dan teknologi penyiaran) dan menyelenggarakan fungsi laboratorium forensik komputer dalam rangka memberikan dukungan teknis proses penyidikan *cybercrime*. Berkaitan dengan penegakkan hukum atas kejahatan *hacking*, Unit V *IT & Cybercrime* merupakan salah satu garda terdepan yang mengemban fungsi Polri sebagai penegak hukum yang berhubungan dengan *information technology & cybercrime*.

Menurut Suparlan (1999: 397), fungsi Polri meliputi: (i) menegakkan hukum dan bersamaan dengan itu menegakkan keadilan sesuai dengan hukum yang berlaku, yaitu menegakkan keadilan dalam konflik kepentingan yang dihasilkan dari hubungan antara individu, masyarakat, dan negara (yang diwakili oleh pemerintah) dan hubungan antar individu serta antar masyarakat; (ii) memerangi kejahatan yang mengganggu dan merugikan masyarakat, warga masyarakat, dan negara; dan (iii) mengayomi warga masyarakat, dan negara dari ancaman dan tindak kejahatan yang mengganggu dan merugikan.

Untuk dapat menjalankan fungsi sebagai penegak hukum, polisi melakukan

penyelidikan dan penyidikan.[6] Yang dimaksud dengan penyelidikan (Pasal 1 Undang-undang Kepolisian) adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang. Penyelidik menurut Pasal 1 Undang-undang Kepolisian adalah pejabat Kepolisian Negara Republik Indonesia yang diberi wewenang oleh undang-undang untuk melakukan penyelidikan. Selanjutnya yang dimaksud dengan penyidikan menurut Pasal 1 Undang-undang Kepolisian adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Sedangkan penyidik adalah pejabat Kepolisian Negara Republik Indonesia yang diberi wewenang oleh undang-undang untuk melakukan penyidikan (Pasal 1 Undang-undang Kepolisian).

Penyelidikan dan penyidikan tersebut termasuk tugas Polri dalam melaksanakan tugas pokok Polri sebagaimana dimaksud dalam Pasal 14 Undang-undang Kepolisian khususnya tugas Polri untuk (i) melakukan penyelidikan dan penyidikan terhadap semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya; tugas ini memberikan peranan utama kepada Polri dalam penyelidikan dan penyidikan sehingga secara umum diberi kewenangan untuk melakukan penyelidikan dan penyidikan terhadap semua tindak pidana, dengan tetap memperhatikan dan tidak mengurangi kewenangan yang dimiliki oleh penyidik lainnya sesuai dengan peraturan perundang-undangan yang menjadi dasar hukumnya masing-masing; (ii) menyelenggarakan identifikasi kepolisian, kedokteran kepolisian, laboratorium forensik dan psikologi kepolisian untuk kepentingan tugas kepolisian; penyelenggaraan identifikasi kepolisian dimaksudkan untuk kepentingan penyidikan tindak pidana dan pelayanan

---

[6]Dalam bahasa Inggris, dikenal dengan kata *investigate* yang berarti; mencari jejak, mencari hingga dapat mempelajari fakta-fakta; yang diperoleh secara sistematis, (Wesbster's New World Dictionary: Third College Edition, 712) Menurut Kamus Besar Bahasa Indonesia (Balai Pustaka: Edisi Kedua, 899) penyelidikan adalah 1) usaha memperoleh informasi melalui pengumpulan data; 2) proses, perbuatan, cara menyelidiki, pengusutan; pelacakan: sedangkan penyidikan adalah: n serangkaian tindakan penyidik yang diatur oleh undang-undang untuk mencari dan mengumpulkan bukti pelaku tindak pidana.

identifikasi non tindak pidana bagi masyarakat dan instansi lain dalam rangka pelaksanaan fungsi kepolisian; (iii) melayani kepentingan warga masyarakat untuk sementara sebelum ditangani oleh instansi dan/atau pihak yang berwenang; hal ini dilakukan oleh anggota Polri sebatas pengetahuan dan kemampuannya untuk kepentingan penegakan hukum, perlindungan, dan pelayanan masyarakat.

Untuk melaksanakan tugas tersebut, Polri mempunyai wewenang (Pasal 15 Undang-undang Kepolisian) di antaranya: menerima laporan dan/atau pengaduan; membantu menyelesaikan perselisihan warga masyarakat yang dapat mengganggu ketertiban umum; melaksanakan pemeriksaan khusus sebagai bagian dari tindakan kepolisian dalam rangka pencegahan yang berupa upaya paksa dan/atau tindakan lain menurut hukum yang bertanggung jawab guna mewujudkan tertib dan tegaknya hukum serta terbinanya ketentraman masyarakat; melakukan tindakan pertama di tempat kejadian; mengambil sidik jari dan identitas lainnya serta memotret seseorang; mencari keterangan dan barang bukti yang berkaitan baik dengan proses pidana maupun dalam rangka tugas kepolisian pada umumnya termasuk melakukan kerja sama dengan kepolisian negara lain dalam menyidik dan memberantas kejahatan internasional; mewakili Pemerintah Republik Indonesia dalam organisasi kepolisian internasional.

Polri sebagai kepolisian nasional diorganisasikan secara vertikal, utuh dan terintegrasi dari tingkat pusat ke seluruh tanah air. Menurut Djamin, sebagai upaya penyempurnaan organisasi, Polri perlu mempertimbangkan prinsip-prinsip organisasi, sebagaimana yang dianut dalam penyempurnaan aparatur pemerintahan, yaitu (1) prinsip pembagian habis tugas, (2) prinsip perumusan tugas pokok dan fungsi sejelas mungkin, (3) prinsip pengorganisasian, (4) prinsip koordinasi, integrasi, dan sinkronisasi, (5) prinsip kontinuitas dan konsistensi, (6) prinsip jalur dan staf, (7) prinsip kesederhanaan, (8) prinsip fleksibilitas, (9) prinsip pendelegasian, wewenang yang jelas, dan (10) prinsip pengelompokkan tugas yang homogen (Djamin, 2001: xviii).

Dalam menghadapi tantangan di berbagai bidang, organisasi Polri sebagai organisasi besar dan kompleks yang mengemban tugas yang sangat luas, memerlukan (1) kemampuan teknis operasional yang harus didukung oleh teknologi kepolisian yang sederhana, madya, maupun yang canggih, (2) manajer-

manajer kepolisian dari tingkat terendah sampai tertinggi dan manajer-manajer fungsional yang lebih berkualitas (Djamin, 2001: xix). Khususnya dalam menghadapi kemajuan di bidang teknologi komputer, informasi dan telekomunikasi seperti yang sudah terjadi saat ini, yang diikuti dengan berbagai bentuk jenis kejahatan dengan modus operandinya yang semakin canggih.

1.4.3.2 Manajemen Polri

Menurut Stephen P. Robbins (1996: 8), manajemen adalah proses pengkoordinasian dan pengintegrasian kegiatan kerja sehingga lebih efisien dan efektif. Proses mewakili fungsi atau kegiatan utama meliputi : perencanaan, pengorganisasian, kepemimpinan dan pengawasan. Proses manajemen adalah proses menetapkan tindakan dan keputusan berkelanjutan yang melibatkan fungsi manajemen. Efisiensi adalah kemampuan untuk meminimalkan penggunaan sumber daya dalam mencapai tujuan organisasi. Sedangkan efektivitas merupakan kemampuan untuk pencapaian tujuan yang sudah ditetapkan.

Dalam pengelolaan organisasi Polri yang modern ditinjau dari fungsi manajemen sebagaimana yang telah dikenal di lingkungan Polri, ada 4 fungsi manajemen yaitu: fungsi perencanaan, pengorganisasian, pelaksanaan dan pengendalian (Biro Ortala, 2007: 2). Sedangkan sistem manajemen yang diterapkan oleh Polri adalah suatu sistem menyeluruh (*total system*) yang bidang serta unsur-unsurnya saling terkait dan saling berhubungan (Djamin, 2001: 123). Pelaksanaan tugas pokok Polri (manajemen operasional) terkait dan tergantung dari manajemen pembinaan dan dukungan teknologi (Djamin, 2001: 123). Manajemen pembinaan berkaitan dengan pengembangan sumber daya manusia, dimana pendidikan dan latihan berkaitan dengan tugas dan wewenangnya menjadi kegiatan penting dalam manajemen pembinaan. Sementara itu, dukungan teknologi menjadi unsur penting dalam manajemen Polri, berkaitan dengan pelaksanaan tugas di lapangan yang memerlukan ketersediaan teknologi baik di tingkat paling sederhana sampai di tingkat yang paling canggih.

1.4.4 Penyidikan dan Manajemen Penyidikan

1.4.4.1 Penyidikan

Dalam melakukan suatu proses penyidikan suatu tindak pidana, diawali dengan proses penyelidikan[7]. Menurut Yahya Harahap (2006: 101), penyelidikan merupakan tindakan tahap pertama permulaan penyidikan akan tetapi penyelidikan bukan tindakan yang berdiri sendiri terpisah dari fungsi penyidikan. Dalam melaksanakan penyelidikan, penyelidik mempunyai wewenang yang meliputi kegiatan menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana; mencari keterangan dan barang bukti; menyuruh berhenti seseorang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri; mengadakan tindakan lain menurut hukum yang bertanggung-jawab; atas perintah penyidik, dapat melakukan tindakan berupa penangkapan, larangan meninggalkan tempat, penggeledahan dan penahanan; pemeriksaan dan penyitaan surat; mengambil sidik jari dan memotret seseorang; serta membawa dan menghadapkan seseorang pada penyidik. Penyelidik membuat dan menyampaikan laporan hasil pelaksanaan tindakan berdasarkan wewenangnya tersebut di atas kepada penyidik (Pasal 5 KUHAP).

Setelah dilakukan penyelidikan, proses dapat diteruskan dengan kegiatan penyidikan. Penyidik mempunyai wewenang seperti: menerima laporan atau pengaduan tentang adanya tindak pidana; melakukan tindakan pertama pada saat di tempat kejadian; menyuruh berhenti seorang tersangka dan memeriksa tanda pengenal diri tersangka; melakukan penangkapan, penahanan, penggeledahan dan penyitaan; melakukan pemeriksaan dan penyitaan surat; mengambil sidik jari dan memotret seseorang; memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi; mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara; mengadakan penghentian penyidikan; mengadakan tindakan lain menurut hukum yang bertanggung jawab.

Di samping tugas dan wewenang dalam lingkup penyidikan tersebut di atas, penyidik juga mempunyai tugas administrasi yang meliputi tugas untuk membuat

---

[7]Penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menemukan dapat atau tidaknya dilakuakn penyidik menurut cara yang diatur dalam aundang-undang (Pasal 1 angka 5 KUHAP).

berita acara tentang pelaksanaan tindakan penyidikan; dan menyerahkan berkas perkara kepada penuntut umum dengan ketentuan jika dianggap sudah selesai. Penyidik juga menyerahkan tanggung jawab atas tersangka dan barang bukti kepada penuntut umum (Pasal 8 KUHAP).

Uraian mengenai penyelidikan dan penyidikan yang tersebut di atas sejalan dengan konsep penyidikan yang disampaikan oleh Djamin (1995), Sullivan (1992), yang pada intinya merupakan suatu proses yang dilaksanakan oleh reserse selaku penyelidik sekaligus penyidik yang memerlukan pengetahuan dan kemampuan yang umumnya dikenal sebagai taktik dan teknik kriminal dan meliputi kegiatan-kegiatan seperti: (i) mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana; (ii) menentukan dapat atau tidaknya dilakukan penyidikan; (iii) mencari serta mengumpulkan bukti; (iv) membuat terang tentang tindak pidana yang terjadi; dan (v) menemukan tersangka pelaku tindak pidana.

Penyelenggaraan penyidikan sebagai suatu penegakan hukum oleh penyidik, menurut Soerjono Soekanto dan Mustafa Abdullah (1987) sebagaimana yang dikutip dalam Nitibaskara (2000: 3) menghendaki empat syarat yaitu:

a. Adanya aturan;
b. Adanya lembaga yang akan menjalankan peraturan itu;
c. Adanya fasilitas untuk mendukung pelaksanaan peraturan itu;
d. Adanya kesadaran hukum dari masyarakat yang terkena peraturan itu.

1.4.4.2 Manajemen Penyidikan

Merujuk pada teori-teori yang dikemukakan oleh Stoner (1996: 6-9), Djamin (2001), Ward (2005), dan Bouza (2005), pelaksanaan fungsi penyidikan haruslah memperhatikan prinsip dan fungsi manajemen, yang pada intinya menghendaki diterapkannya prinsip dan fungsi manajemen dalam suatu proses penyidikan. Penulis akan mengkaji penyidikan *hacking* dengan memandang proses penyidikan *hacking* yang dilakukan oleh Unit V *IT & Cybercrime* - yang merupakan suborganisasi dari organisasi Polri - sebagai suatu bagian dari sistem manajemen Polri yang menyeluruh (*total system*) yang bidang serta unsur-unsurnya saling terkait dan saling berhubungan, khususnya dalam pelaksanaan proses merencanakan, mengorganisasikan, memimpin, dan mengendalikan pekerjaan anggota organisasi dan menggunakan semua sumber daya organisasi

untuk mencapai sasaran organisasi yang sudah ditetapkan. Perspektif tersebut didasarkan pada teori-teori manajemen dengan pendekatan klasik, di mana kajian dilakukan untuk menemukan dan menjelaskan anatomi organisasi yang melahirkan konsekuensi diikutinya prinsip-prinsip manajemen apabila organisasi tersebut akan dijalankan secara efisien (Roberg dan Kuykendall, 1997: 25).

Untuk memperoleh konsep mengenai manajemen penyidikan, penulis telah mengkaji teori-teori manajemen, khususnya teori manajemen klasik yang terdiri dari manajemen ilmiah, manajemen birokratis, dan manajemen administratif yang melahirkan teori manajemen kepolisian klasik (Roberg dan Kuykendall, 1997: 29). Teori manajemen kepolisian yang dipengaruhi oleh aliran manajemen klasik, terlihat dari penekanan mereka pada Teori Manajemen Ilmiah Taylor yang memfokuskan pada efisiensi, Teori Birokrasi Weber yang memberikan penekanan pada kewenangan hierarkis dan kontrol, serta prinsip-prinsip umum yang dikemukakan oleh ahli-ahli manajemen administratif. Dengan pendekatan ini, manajemen kepolisian dipandang sebagai model para-militer yang menekankan fungsi penegakan hukum dan praktek manajerial ditujukan untuk mengontrol tingkah laku polisi dengan tujuan meningkatkan pengendalian kejahatan dan mengurangi praktek korupsi (Roberg dan Kuykendall, 1997: 29).

Selain itu, penulis juga mengkaji konsep manajemen penyidikan sebagaimana yang dikemukakan oleh Butler (1992) dan Ward (2005), yaitu sebagai suatu cara yang terencana, terkoordinasi, dan teruji untuk memaksimalkan baik efisiensi dan produktivitas dalam melaporkan serta menginvestigasi berbagai kasus *hacking* dalam suatu praktek manajemen yang efektif. Praktek manajemen yang efektif dimaksud adalah suatu sistem pemecahan masalah sebagai suatu proses kompleks yang dimulai dengan pengujian yang hati-hati atas setiap masalah untuk memperoleh sebanyak mungkin informasi mengenai masalah tersebut sehingga diperlukan suatu sistem manajemen untuk mentransformasikan ide-ide dengan tindakan-tindakan (aksi).

Sedangkan untuk hal yang berkaitan dengan pemecahan masalah, digunakan pendekatan detektif sebagai ilmuwan sebagaimana yang dikemukakan Irving Copi dalam Pengantar Logika (C.A Qadir, 1995: 51-53) dimana baik sebagai ilmuwan maupun sebagai detektif, walaupun masalah yang dihadapi

tidak persis sama tetapi keduanya menggunakan pendekatan dan teknik menjelaskan metode ilmiah seperti adanya masalah, hipotesis awal, pengumpulan fakta tambahan, merumuskan hipotesis dan menyimpulkan akibat lebih lanjut, menguji akibat dan penerapan. Selanjutnya dijabarkan pula dalam melakukan kegiatannya ilmuwan sedang beraksi dengan menggunakan penyelidikan ilmiah.

Proses adalah cara sistematik yang sudah ditetapkan dalam melakukan kegiatan. Aktivitas manajemen dapat digambarkan melalui proses manajemen yang bersifat interaktif meliputi: merencanakan, mengorganisasikan, memimpin dan mengendalikan (Butler, 1992: 17-21). Merencanakan (*planning*) adalah proses menetapkan sasaran dan tindakan yang perlu untuk mencapai sasaran tadi. Mengorganisasikan (*organizing*) adalah proses mempekerjakan dua orang atau lebih untuk bekerja sama dengan cara terstruktur guna mencapai sasaran spesifik atau beberapa sasaran. Memimpin (*leading*) adalah proses mengarahkan dan mempengaruhi aktivitas yang berkaitan dengan pekerjaan dari anggota kelompok atau seluruh organisasi. Pengendalian *(controlling)* adalah proses untuk memastikan bahwa aktivitas sebenarnya sesuai dengan aktivitas yang direncanakan.

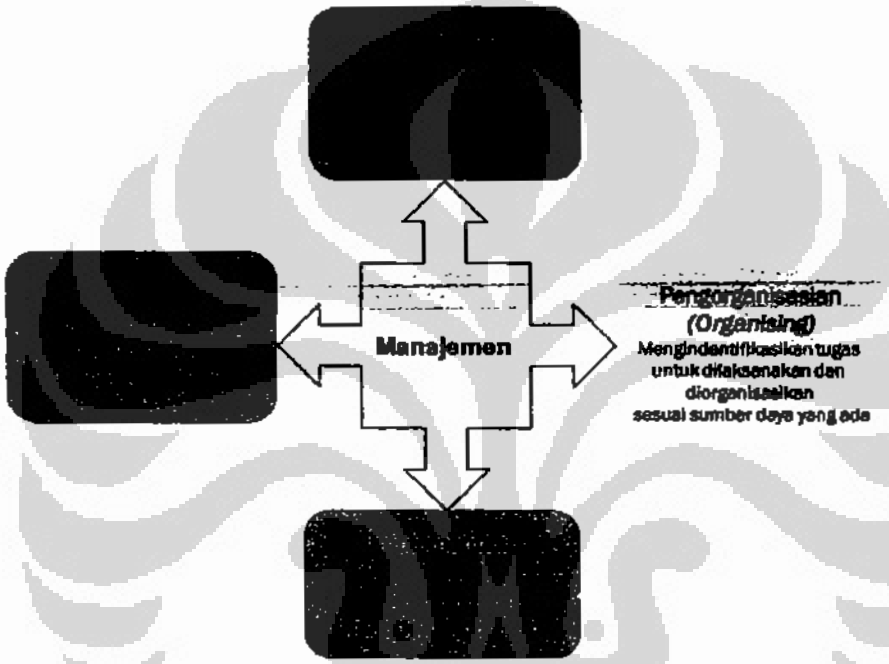
Menurut Butler (1992: 17), proses dari pendefinisian masalah menuju penyelesaian masalah memerlukan suatu sistem manajemen untuk mengubah ide menjadi aksi. Menurutnya terdapat empat tahapan yang berbeda dalam proses tersebut yaitu:

a. Permasalahan diidentifikasi melalui sistem analisis. Ketika permasalahan telah jelas, proses perencanaan berjalan untuk mengeksplorasi alternatif-alternatif metode untuk mencapai tujuan yang diharapkan dan memilih alternatif yang paling layak untuk dilakukan.
b. Sumber daya manusia akan mengorganisasi rencana dasar tersebut.
c. Ketika rencana telah lengkap maka rencana tersebut diimplementasikan.
d. Setelah implementasi, pekerjaan tersebut diawasi dan dikontrol untuk menjamin apakah mereka mengerti peranan mereka dan instruksi yang diberikan. Hasil pekerjaan tersebut diukur dengan parameter yang telah ditentukan pada proses perencanaan.

Dari proses manajemen tersebut diharapkan timbul sinergi. Sinergi adalah

situasi saat keseluruhan lebih besar daripada bagian-bagiannya (Djamin, 1995: 65). Dalam arti organisasi, sinergi berarti bahwa departemen yang berinteraksi secara kooperatif lebih produktif daripada kalau mereka beroperasi sendiri-sendiri.

Bagan 1.1
Siklus Manajemen



(Sumber: Butler, 1992: 18)

Berdasarkan kajian mengenai teori manajemen klasik yang dikemukakan oleh aliran manajemen administratif, siklus manajemen yang dikemukakan Butler tersebut di atas dipahami sebagai pelaksanaan fungsi manajemen dalam proses penyidikan. Sedangkan prinsip-prinsip manajemen yang diterapkan dalam proses penyidikan, yang menggambarkan hubungan manajemen dan organisasi, dikaji berdasarkan konsep prinsip manajeman yang dikemukakan oleh Henri Fayol (1841-1925) sebagaimana dikutip oleh Stoner dan Freeman (1992: 66) yang terdiri dari 14 prinsip manajemen untuk menciptakan manajemen yang efektif yaitu:

a. **Pembagian tugas**. Semakin terspesialisasi semakin efisien.
b. **Wewenang**. Manajer harus memberikan perintah sehingga tugas selesai. Selain wewenang formal terdapat juga wewenang pribadi berdasarkan pengalaman yang relevan.
c. **Disiplin**. Disiplin berasal dari kepemimpinan yang baik pada semua tingkat, persetujuan yang adil, dan penerapan saksi yang bijaksana.
d. **Kesatuan komando**. Setiap karyawan harus menerima instruksi hanya dari satu orang. Bila seorang karyawan menjadi bawahan dari beberapa orang manajer maka akan terjadi konflik dalam instruksi dan kekacauan dalam wewenang.
e. **Kesatuan dalam pengerahan**. Operasi dalam organisasi yang mempunyai obyektif sama harus diarahkan hanya oleh seorang manajer yang menggunakan satu rencana.
f. **Kepentingan individual di bawah kepentingan umum**. Dalam keadaan apapun kepentingan pribadi karyawan tidak boleh didahulukan dari kepentingan organisasi secara keseluruhan.
g. **Imbalan**. Kompensasi untuk pekerjaan yang dilakukan harus adil bagi karyawan dan majikan.
h. **Sentralisasi**. Sentralisasi adalah mengurangi peran bawahan dalam pembuatan keputusan; sedangkan meningkatkan peran bawahan adalah disentralisasi. Fayol percaya bahwa manajer harus mempertahankan tanggung jawab akhir, tetapi pada saat yang sama harus memberikan wewenang yang cukup kepada bawahan untuk mengerjakan tugasnya dengan baik. Masalahnya adalah menemukan seberapa jauh sentralisasi dalam setiap kasus.
i. **Hierarki**. Garis wewenang dalam sebuah organisasi, berjalan menurut peringkat dari manajemen puncak ke tingkat paling bawah.
j. **Susunan**. Material dan orang harus berada di tempat yang tepat pada waktu yang tepat. Orang terutama, harus pada pekerjaan atau posisi yang paling cocok baginya.
k. **Keadilan**. Manajer harus bersahabat dan adil kepada bawahannya.
l. **Stabilitas staf**. Banyaknya karyawan yang keluar mengungkapkan fungsi efisiensi dari sebuah organisasi.

m. **Inisiatif**. Bawahan harus diberikan kebebasan untuk memikirkan dan melaksanakan rencana mereka, walaupun beberapa kesalahan mungkin terjadi.

n. **Semangat korps**. Mempromosikan semangat tim akan memberikan rasa kesatuan pada organisasi. Bagi Fayol, bahkan faktor yang kecil pun harus membantu mengembangkan semangat. Fayol menyarankan, misalnya, penggunaan komunikasi verbal sebagai ganti dari komunikasi format tertulis.

Konsep prinsip manajemen sebagaimana disampaikan Fayol tersebut di atas, tidak akan dipergunakan sebagai dasar untuk mengevaluasi manajemen penyidikan yang diterapkan dalam Unit V *IT & Cybercrime*, akan tetapi lebih dipergunakan sebagai kerangka teori untuk melihat dan memahami proses penyidikan tindak pidana *hacking website* Partai Golkar yang dipandang sebagai suatu proses manajemen penyidikan.

1.4.5 Sistem Manajemen dan Faktor-faktor yang Mempengaruhinya

Sebagaimana telah disampaikan oleh Djamin (2001: 123) bahwa sistem manajemen yang diterapkan oleh Polri adalah suatu sistem menyeluruh (*total system*) yang bidang serta unsur-unsurnya saling terkait dan saling berhubungan, maka dalam meneliti dan mengkaji hasil penelitian dalam disertasi ini, dipergunakan kerangka pemikiran kesisteman untuk memahami organisasi Unit V *IT & Cybercrime* sebagai unit yang merupakan sub organisasi Bareskrim Polri. Dengan berkembangnya kejahatan di bidang *IT & Cybercrime*, maka sesuai dengan tugas pokok, fungsi dan tujuan organisasinya, Unit V *IT & Cybercrime* dituntut untuk menjaga ketentraman masyarakat khususnya para pengguna komputer dan komunitas *virtual*. Berkaitan dengan itu, dalam disertasi ini, perlu ditekankan asumsi dasar pendekatan berikut ini untuk menjelaskan sistem manajemen dalam Unit V *IT & Cybercrime* yang pada gilirannya mempengaruhi proses penyidikan tindak pidana *hacking* yang menjadi tugasnya: (1) realitas sosial dalam suatu sistem, (2) proses suatu sistem hanya dapat dipahami dalam suatu kerangka hubungan timbal balik anter bagian-bagian yang saling terkait dan tergantung satu dengan yang lain, dan (3) suatu sistem terkait pada proses-proses tertentu yang bertujuan untuk mempertahankan integritas.

Di samping asumsi tersebut di atas, dalam penelitian dan pengkajian hasil

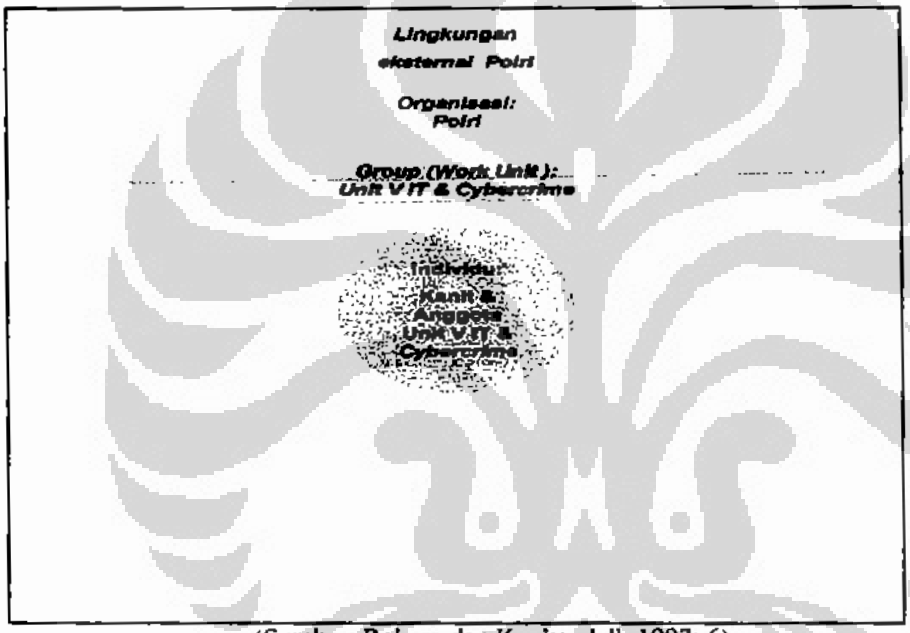
penelitian, dan guna mencari jawaban atas permasalahan penelitian, penulis telah mengkaji teori-teori yang memandang organisasi polisi sebagai suatu organisasi yang kompleks, yang muncul dari pendekatan kontemporer, khususnya teori manajemen kepolisian dengan menggunakan teori sistem dan teori kontinjensi (Roberg dan Kuykendall, 1997: 37–45) untuk mempelajari organisasi kepolisian. Pendekatan tersebut digunakan untuk membentuk perspektif penulis bahwa organisasi kepolisian adalah suatu sistem yang terdiri dari elemen-elemen yang saling berhubungan, dengan penekanan pentingnya hubungan yang saling terkait antara bagian-bagian dalam organisasi dan antara organisasi dengan lingkungannya. Untuk keperluan tersebut, penulis akan menggunakan *four levels of analysis* untuk meningkatkan pemahaman yang lebih baik terhadap tingkah laku organisasi yang kompleks. Analisa Tingkat Organisasi Unit V *IT & Cybercrime* ini terlihat dalam Bagan 1.2.

Tingkat analisis suatu organisasi terdiri dari empat level yaitu: level individu, level group *(work unit)*, level organisasi dan level lingkungan eksternal. Keempat level tersebut penting untuk ditelaah agar dapat memahami perilaku suatu organisasi yang kompleks. Level pertama adalah analisis dasar dari suatu organisasi itu sendiri yaitu individu. Individu dalam Unit V *IT & Cybercrime* disini terdiri dari pemimpin atau Kepala Unit (Kanit) dan anggota Unit V *IT & Cybercrime*. Hal yang dianalisis pada level pertama adalah motivasi, gaya kepemimpinan dan pengaruh gaya kepemimpinan terhadap motivasi anggota. Level kedua adalah kelompok kerja seperti unit, team, *shift*, atau program.

Kelompok kerja terdiri dari individu yang bekerja bersama untuk mencapai beragam tugas dan tujuan tertentu. Dalam disertasi ini, yang dimaksud dalam kelompok kerja adalah Unit V *IT & Cybercrime*. Unit analisis dalam level kedua ini adalah budaya organisasi dan pengaruh kepemimpinan dalam merubah budaya organisasi tersebut sehingga terjadi transformasi manajemen dalam Unit V *IT & Cybercrime*. Level ketiga adalah organisasi yang terdiri dari beberapa *group* yang berusaha mencapai tujuan organisasi. Organisasi yang dimaksud dalam disertasi ini adalah Polri sebagai organisasi besar dan kompleks yang terdiri dari sub-sub organisasi seperti Bareskrim dan Direktorat II. Analisis pada level ketiga menjabarkan hubungan antara Unit V *IT & Cybercrime* dengan suborganisasi

yang secara hierarki berada di atas Unit V *IT & Cybercrime* atau disebut juga *internal stakeholders*. Level terakhir adalah lingkungan di luar organisasi tempat organisasi menjalin interaksi, sebagian ahli menamakannya sebagai *external stakeholders* (Roberg dan Kuykendall, 1997: 6). Dari analisis terhadap keempat level tersebut dapat dikaji hubungan dan pengaruh antara kepemimpinan, budaya organisasi dan *external stakeholders* yang berlaku pada Unit V *IT & Cybercrime*.

Bagan 1.2
Analisis Tingkat Organisasi Unit V *IT & Cybercrime*
Berdasarkan Analisis Tingkat Organisasi



(Sumber: Roberg dan Kuykendall, 1997: 6)

1.4.5.1 Budaya Organisasi

Iklim kerja organisasi berkaitan erat dengan budaya organisasi. Budaya organisasi menurut McShane (2003: 448) adalah pola dasar dari asumsi, nilai, dan kepercayaan yang dipertimbangkan bersama sebagai arahan yang benar dari cara berpikir dan bertindak atas permasalahan dan kesempatan yang dihadapi oleh organisasi tersebut. Budaya organisasi menentukan apa yang penting dan tidak penting bagi organisasi. Budaya organisasi bekerja seperti DNA, tidak kelihatan tetapi sangat kuat mencetak apa yang terjadi di tempat kerja. Budaya organisasi mempunyai artefak yang dapat dilihat secara nyata seperti struktur fisik, bahasa,

ritual dan seremoni, serta cerita dan legenda-legenda yang berkembang dalam organisasi tersebut.

Budaya atau kebudayaan berasal dari bahasa Sansekerta, yaitu *buddhayah*, yang merupakan bentuk jamak dari buddhi (budi atau akal) diartikan sebagai hal-hal yang berkaitan dengan budi dan akal manusia (Koentjaraningrat, 2002: 181). Hal ini berarti kebudayaan dapat diartikan sebagai hal-hal yang bersangkutan dengan akal. Zoetmulder (Koentjaraningrat, 2002: 181) membedakan pengertian budaya dari kebudayaan, budaya diartikan sebagai "daya dari budi" yang berupa cipta, karsa dan rasa sedangkan kebudayaan adalah hasil dari cipta, karsa dan rasa itu. Koentjaraningrat mengatakan bahwa dalam istilah "antropologi budaya" perbedaan antara budaya dengan kebudayaan itu ditiadakan, kata budaya digunakan sebagai suatu singkatan dari "kebudayaan" dengan arti yang sama.

Kebudayaan sebagai panduan untuk berperilaku dilandasi oleh pemaknaan terhadap lingkungan dan segala sesuatu yang melingkupinya. Setiap gejala dan bentuk fisik kemudian dianggap sebagai simbol yang mempunyai makna dan saling berhubungan sebagai suatu sistem. Sistem makna ini kemudian dihayati sebagai kepercayaan untuk menempatkan diri dan berperilaku. Kepercayaan berasal dari kata percaya, artinya mengakui atau menyakini akan kebenaran. Kepercayaan adalah hal-hal yang berhubungan dengan pengakuan atau keyakinan akan kebenaran (Prasetya, 1998: 232).

Menurut Carol dan Melvin (1980) sebagaimana dikutip oleh T.O. Ihromi (1984: 28), pada umumnya kebudayaan dapat dikatakan bersifat adaptif karena kebudayaan itu melengkapi manusia dengan cara-cara penyesuaian diri pada kebutuhan-kebutuhan fisiologis dari badan mereka sendiri, dan penyesuaian pada lingkungan yang bersifat fisik-geografis, maupun pada lingkungan sosialnya. Sebagaimana kebudayaan merupakan suatu penyesuaian pada lingkungan fisik dan kebutuhan-kebutuhan biologis, kebudayaan juga merupakan suatu penyesuaian pada lingkungan sosial.

Cordner (2005: 13) menyebutkan bahwa tiap organisasi mengembangkan budaya berdasarkan norma dan nilai-nilai yang memandu karyawan dalam berpikir dan bertindak. Norma dan nilai-nilai yang konsisten dengan tujuan departemen dan prinsip demokratis harus didukung dengan segala cara yang

memungkinkan. Budaya organisasi di lingkungan Polri adalah kebiasaan-kebiasaan yang sedemikian rupa telah melekat pada tubuh Polri dan berlaku dari waktu ke waktu secara berkesinambungan dan meskipun kadarnya berfluktuasi dengan ketergantungan pada watak dan karakter pimpinan puncak Polri dan bentuk serta sifat organisasi dan perkembangan lingkungan di luar organisasi Polri.

Bob Gett berpendapat bahwa budaya organisasi dapat mempengaruhi performa perusahaan (McShane, 2003: 455). Dengan budaya organisasi yang kuat dan sesuai dengan lingkungan organisasi maka akan membentuk kesuksesan organisasi. Budaya organisasi diyakini mempunyai tiga fungsi yaitu: (i) budaya organisasi tertanam sebagai kontrol sosial yang mempengaruhi anggota dalam mengambil keputusan dan berperilaku; (ii) budaya organisasi berperan sebagai perekat sosial yang menyatukan mereka dan menyadarkan mereka sebagai bagian dari organisasi; (iii) budaya organisasi membantu anggota dalam menjalankan pekerjaan karena mereka telah mengetahui apa yang diharapkan dari anggota dan telah mempunyai persepsi yang sama.

Manning (2005: 564) menyebutkan bahwa budaya kerja bangkit dari sebuah set tugas yang diulang dan rutin dalam tingkat yang bermacam-macam, dan sebuah teknologi yang bervariasi dan dampaknya secara tak langsung (diperantarai oleh struktur organisasi), menghasilkan suatu sikap dan struktur yang menjelaskan keyakinan (ideologi). Budaya kerja akan membuat tampilan yang mempertunjukkan, menciptakan, dan memelihara otoritas.

Budaya organisasi dapat mempengaruhi kinerja organisasi apabila: (i) isi dari budaya tersebut sesuai dengan lingkungan organisasi; (ii) terdapat budaya organisasi yang cukup kuat yang memiliki nilai-nilai dominan yang dianut anggotanya; (iii) terdapat budaya adaptif. Budaya adaptif merupakan budaya organisasi dengan karakteristik anggotanya yang terfokus pada perubahan kebutuhan pelanggan dan pihak kepentingan lainnya *(stakeholders)* serta mendukung adanya inisiatif untuk mengikuti perubahan tersebut (McShane, 2003: 455-459).

1.4.5.2 Kepemimpinan

Agar tidak salah menerapkan manajemen penyidikan *hacking*, perlu juga diperhatikan pendapat Dantzker, yang membedakan antara manajemen dan kepemimpinan. Manajemen didefinisikan sebagai elemen yang memimpin, mengarahkan atau mengatur organisasi untuk mencapai tujuannya. Sedangkan kepemimpinan didefinisikan termasuk proses bagaimana anggota organisasi dipengaruhi untuk memfasilitasi pencapaian tujuan dan obyektif dari organisasi (Dantzker, 1999: 78). Kepemimpinan adalah proses mempengaruhi anggota organisasi agar ingin dan secara tepat menggunakan energi mereka untuk memfasilitasi pencapaian tujuan departemen kepolisian (Swanson, Territo, dan Taylor, 2008: 270).

Kepemimpinan dapat diartikan sebagai orang atau kelompok orang yang memimpin. Hal ini berarti kepemimpinan tidak lain daripada nama kolektif untuk para pemimpin. Kata kepemimpinan yang merupakan terjemahan dari kata "*leadership*" dalam bahasa Inggris dapat diberi pengertian dengan menggunakan pengertian yang diberikan untuk *leadership* itu. Ordway Tead merumuskan pengertian *leadership* sebagai suatu kegiatan mempengaruhi orang-orang untuk bekerja sama mencapai tujuan yang sama yang mereka inginkan bersama (Sunindhia dan Widiyanti, 1993: 4). Bagi Tead, *leadership* hanya merupakan kegiatan mempengaruhi orang.

Kamus Istilah Antropologi (Koentjaraningrat, *et. al.*, 2003: 168, 189) mendefinisikan pemimpin (*leader*) berbeda dengan pimpinan (*leadership*). Pemimpin (*leader*) adalah seorang atau sejumlah orang yang mampu memerintah, menyuruh, membina dan melindungi warga masyarakat karena kewibawaan, kekuasaan, dan wewenang yang dimilikinya berdasarkan adat-istiadat dan hukum yang berlaku dalam masyarakat yang bersangkutan. Sedangkan pimpinan (*leadership*) adalah sistem memerintah, menyuruh, membina, dan melindungi warga masyarakat karena kewibawaan, kekuasaan, dan wewenang berdasarkan adat istiadat dan hukum yang berlaku dalam masyarakat yang bersangkutan. Hal ini berarti pengertian dari pimpinan (*leadership*) lebih diarahkan kepada sistemnya sedangkan pengertian dari pemimpin (*leader*) lebih diarahkan kepada individu atau kelompoknya.

Menurut Sunindhia dan Widiyanti (1993: 99), kepemimpinan (*leadership*) pada umumnya adalah apa yang harus dipunyai, dijalankan, dan atau dipergunakan oleh setiap orang yang berkedudukan sebagai "Pemimpin". Kepemimpinan sebagai sesuatu yang harus dipunyai dapat diartikan sebagai kemampuan, bakat, sifat-sifat, atau kecakapan. Kepemimpinan sebagai sesuatu yang harus dijalankan adalah kepemimpinan sebagai kewajiban, fungsi, kegiatan-kegiatan, dan tanggung jawab. Sedangkan kepemimpinan sebagai sesuatu yang harus dipergunakan adalah kepemimpinan sebagai teknik atau sarana.

Menurut Lewin, Lippet, and White (1939) sebagaimana dikutip oleh Swanson, Territo, dan Taylor (2008: 278-279), gaya kepemimpinan terbagi menjadi tiga , yaitu:

a. **Kepemimpinan otoriter;** pemimpin membuat semua keputusan tanpa melibatkan lainnya. Karakteristik dari kepempimpinan otoriter adalah semua kebijaksanaan dibuat oleh pemimpin, teknik dan langkah-langkah kegiatan diarahkan oleh pemimpin, biasanya satu langkah pada satu waktu, untuk menciptakan ketidakjelasan di masa depan. Pemimpin biasanya mendiktekan tugas tertentu dan mendampingi pekerjaan setiap anggota organisasi. Pujian dan kritik atas pekerjaan anggota menjadi sangat personal.
b. **Kepemimpinan demokratis;** diterapkan dengan cara mengajak anggota organisasi untuk terlibat dalam perencanaan dan pelaksanaan tugas dengan karakteristik sebagai berikut: membuat semua kebijakan sebagai hasil dari diskusi kelompok dan keputusan bersama; menggunakan informasi dari diskusi untuk menciptakan pilihan; memberikan kebebasan kepada anggota organisasi untuk bekerja dengan siapa mereka suka dan memberikan kebebasan kepada kelompok mengenai pembagian kerja; memuji atau mengkritik anggota secara obyektif dan berdasarkan fakta.
c. **Kepemimpinan *Laissez Faire;*** memberikan kebebasan sepenuhnya kepada kelompok untuk menentukan dengan sedikit partisipasi atau tidak ada partisipasi sama sekali dari pemimpin, menyediakan materi dan informasi bila diminta tapi tidak berpartisipasi dalam diskusi, jarang memberikan pujian atau kritik kecuali diminta.

Menurut Gunawan (2006: 122) terdapat korelasi antara kompetensi, gaya kepemimpinan dan iklim kerja yang digambarkan dalam Bagan 1.3

Bagan 1.3
Korelasi Kompetensi, Gaya Kepemimpinan, & Iklim Kerja (Gunawan, 2006: 122)

(Sumber: Gunawan, 2006: 122)

Bagan 1.3 menggambarkan gaya kepemimpinan suatu organisasi dipengaruhi oleh persyaratan kompetisi jabatan dan kompetisi yang dimiliki oleh setiap individual. Gaya kepemimpinan tersebut kemudian mempengaruhi iklim kerja organisasi yang pada akhirnya mempengaruhi kinerja organisasi.

1.4.5.3 Stakeholders

Pihak yang berkepentingan *(stakeholders)* adalah kelompok yang secara langsung atau tidak langsung terpengaruh oleh cara organisasi berusaha mencapai sasarannya. Pihak yang berkepentingan tersebut terbagi menjadi pihak berkepentingan eksternal *(external stakeholders)* yaitu kelompok atau individu dalam lingkungan eksternal sebuah organisasi yang mempengaruhi aktivitas organisasi tersebut. Pihak berkepentingan internal *(internal stakeholders)* adalah kelompok atau individu seperti karyawan yang tidak benar-benar merupakan bagian dari lingkungan organisasi tetapi seorang manajer tetap bertanggung jawab atas orang atau kelompok tersebut.

1.5 Metodologi

Studi ini menggunakan metode penelitian kualitatif. Metode penelitian kualitatif digunakan untuk memperoleh data primer yang menjadi sumber analisis bagi pemahaman yang komprehensif terhadap konteks permasalahan yang kompleks untuk ditelaah dan dianalisis berdasarkan suatu kerangka teori sebagai hasil dari kajian pustaka. Kajian pustaka sendiri digunakan untuk mengumpulkan dan menganalisis data sekunder yang diambil dari berbagai bahan bacaan baik *text book* dari dalam dan luar negeri, jurnal ilmiah, hasil-hasil penelitian dan seminar atau diskusi dari para ahli atau peneliti terdahulu, berikut berita atau opini di media massa baik cetak maupun elektronik termasuk situs-situs di internet. Di samping itu, dipergunakan juga bahan hukum primer dan bahan hukum sekunder dalam penelitian yang dilakukan berkaitan dengan kajian yang berhubungan dengan hukum.

Selanjutnya studi ini juga menggunakan pendekatan *grounded theory* yang merupakan teori yang dihasilkan secara induktif dari kerja lapangan yaitu teori yang muncul dari pengamatan penulis dan hasil wawancara dalam dunia nyata bukan yang dihasilkan dari *laboratory* atau *academy* (Patton, 2002: 11). Dengan pendekatan tersebut, kajian dalam studi ini akan melakukan eksplorasi gejala-gejala yang terdapat dalam lingkungan Unit V *IT & Cybercrime* selama menjalankan manajemen penyidikan *hacking*. Eksplorasi tersebut dimaksudkan agar dapat menjelaskan hubungan-hubungan antar gejala-gejala tersebut secara sistematis. Selanjutnya eksplorasi gejala-gejala tersebut menghasilkan abstraksi-abstraksi sebagai konsep-konsep yang saling mempunyai keterkaitan. Penggunaan pendekatan tersebut mempunyai tujuan yang bersifat umum untuk menggunakan metode penelitian kualitatif agar mampu mendeskripsikan dan menjelaskan setepat dan selengkap mungkin sehingga pendeskripsian dan penjelasannya berhubungan sedekat mungkin dengan kenyataan yang sebenarnya terjadi (Patton, 2002: 546).

1.6 Metode Penelitian

Penelitian kualitatif dalam disertasi ini dilakukan dengan cara pangamatan terlibat, wawancara berpedoman, diskusi kelompok terfokus dan *virtual ethnography*. Pengamatan terlibat dilakukan selama penanganan kasus *hacking website* Partai Golkar; penulis berperan sebagai Kepala Unit V *IT & Cybercrime*. Dalam periode itu telah dilakukan wawancara spontan dengan para informan. Di luar periode tersebut, terhadap para informan juga telah dilakukan wawancara berpedoman[8]. Penulis menetapkan dua kriteria untuk informan dari anggota reserse tersebut yaitu (i) sedang dan telah menjalankan tugas sebagai penyelidik atau penyidik dalam kasus *hacking;* dan (ii) bersedia diwawancarai. Selaku pimpinan, penulis terlibat dan melibatkan diri dalam organisasi Polri untuk dapat memahami prinsip-prinsip dan fungsi manajemen dalam proses penyidikan *hacking* secara langsung. Sedangkan selaku penyidik, penulis merasakan dan mengalami interaksi dalam proses penyidikan *hacking*, baik dengan para anggota Unit V *IT & Cybercrime*, dengan tersangka, saksi, ahli, korban serta pihak lainnya yang terlibat.

Untuk memahami penyidikan kasus *hacking website* Partai Golkar, penulis telah mengamati dan/atau terlibat dalam proses penerimaan laporan pada tanggal 17 Juli 2006, penahanan pada tanggal 23 Agustus 2006 sampai pada tanggal 1 Oktober 2006. Penelitian di Jakarta terfokus pada organisasi Unit V *IT & Cybercrime* dan para anggotanya dalam mengungkap kasus *hacking* tersebut yang dilaksanakan selama lima (5) bulan terhitung sejak bulan Juli 2006 sampai dengan Desember 2006.

Wawancara berpedoman juga dilakukan terhadap korban dan advokat. Kepada mereka telah ditanyakan perilaku penyidik dalam melaksanakan penyidikan dan harapan mereka terhadap penyidik dalam mengungkapkan kasus *hacking* tersebut.

---

[8]Wawancara berpedoman dilaksanakan untuk mengumpulkan informasi sebagaimana dimaksud oleh Suparlan (1994) yaitu sebagai teknik untuk mengumpulkan informasi dari para anggota masyarakat yang diteliti mengenai suatu masalah khusus dengan teknik bertanya yang bebas tetapi berdasarkan atas suatu pedoman yang tujuannya adalah untuk memperoleh informasi khusus dan bukannya untuk memperoleh respon atau pendapat mengenai suatu masalah.

Diskusi kelompok terfokus dilakukan kepada semua anggota Unit V *IT & Cybercrime* untuk mengetahui persepsi mereka terhadap budaya organisasi dan kepemimpinan yang terjadi di Unit V *IT & Cybercrime* serta harapan mereka terhadap kondisi yang ideal bagi pencapaian tujuan organisasi.

Yang dimaksud dengan diskusi kelompok terfokus adalah suatu kelompok yang tujuan, ukuran, komposisi dan prosedurnya telah ditentukan terlebih dahulu secara khusus. Tujuan diskusi kelompok tersebut untuk mendengarkan dan mengumpulkan informasi. Diskusi kelompok merupakan suatu cara untuk memahami lebih baik bagaimana persaan orang, apa pikiran mereka terhadap suatu topik, produk atau jasa. Para peserta dipilih karena mereka mempunyai karakteristik yang sama yang berkaitan dengan topik yagn dibicarakan dalam kelompok. (Krueger dan Casey, 2000: *4-5*)

Diskusi kelompok terfokus adalah salah satu teknik yang digunakan peneliti untuk menggali data dan informasi mengenai permasalahan yang diteliti. Data yang dihasilkan akurat dan mempunyai validitas tinggi, sebab semua informasi tersebut merupakan hasil kesepakatan seluruh peserta diskusi kelompok, setelah mempertimbangkan berbagai perbedaan yang ada meninjaunya secara mendalam dalam diskusi. Apabila ada keraguan mengenai informasi yang diberikan oleh salah satu peserta, maka peserta lain akan memberikan koreksi, sehingga terjadi tukar pikiran di masing-masing anggota diskusi. Dengan demikian informasi terakhir yang ada, telah melalui proses validasi oleh seluruh anggota diskusi. Biasanya kegiatan ini dipandu oleh seorang moderator/fasilitator dan seorang notulen. (Patilima: 2005, 76)

Selain pengamatan terlibat dalam dunia nyata tersebut di atas, penulis juga melakukan pengamatan terlibat dalam dunia *cyber* (*cyberspace*[9]). Penulis

---

[9]Istilah *cyberspace* pertama kali diperkenalkan oleh *William Gibson*, pada tahun 1984, dalam novel fiksi ilmiahnya yang berjudul "*Neuromancer*". Novel tersebut menggambarkan tentang perusahaan-perusahaan raksasa (*large corporations*) yang mengendalikan pemerintahan di berbagai negara, bahkan menggantikan pemerintah yang ada, serta para *hacker* yang melakukan perang terhadap data (*secure data*) yang tersimpan di dalam komputer atau sistem komputer. Setting kisah novel tersebut ternyata telah sangat mempengaruhi komunitas komputer pada saat itu, karena situasi dan cara-cara serta kejadian-kejadian yang digambarkan didalam novel tersebut, diwujudkan tanpa eksistensi fisik. Situasi dan cara-cara mewujudkan kejadian tersebut (tanpa ekstensi fisik) itulah yang oleh *William Gibson* disebut sebagai *cyberspace*, yang didefinisikan sebagai "*a futuristic computer network that people use by plugging their minds into it*" atau diartikan sebagai suatu jaringan komputer masa depan yang digunakan manusia dengan

melakukan observasi dan wawancara dengan metode *virtual ethnography*. Penulis turut serta sebagai pengguna teknologi informasi dan menjadi bagian dari sejumlah komunitas *virtual* di dunia *cyber* dan berinteraksi dengan pengguna internet sebagai sesama anggota komunitas *virtual* (Miller dan Slater, 2003: 21-22).

1.7 Pengorganisasian Penelitian

Penelitian dalam studi ini secara formal dilaksanakan selama 6 (enam) bulan setelah proposal disetujui yaitu dimulai pada bulan Agustus 2007 sampai dengan awal Januari 2008, dengan tahapan sebagai berikut:

Tahap Pertama: pembuatan proposal yang terdiri dari penentuan topik, pengumpulan bahan literatur, penentuan metodologi dan penyusunan rencana penelitian serta presentasi proposal penelitian dihadapan tim penguji. Tahap pertama telah dilakukan secara informal sebelum dilakukan pengujian yang dilakukan pada bulan Juli 2007.

Tahap Kedua: pengumpulan data komprehensif yang meliputi studi literatur lebih mendalam, analisis kualitatif dengan cara pengamatan terlibat, diskusi kelompok terfokus dan wawancara berpedoman. Kegiatan yang telah dilakukan dalam tahap kedua ini yaitu penelitian lapangan dan penelitian literatur. Kedua metode pengumpulan data ini akan dijelaskan dalam sub bab tersendiri.

Tahap Ketiga: pengolahan data dan penulisan laporan yang terdiri dari pengelompokan data, analisis data sesuai dengan sistematika yang telah ditentukan dan penulisan laporan hasil penelitian sesuai kaedah yang berlaku di lingkungan akademis.

Tahap Keempat: Pengujian dan presentasi dari hasil penelitian tersebut hingga dapat dipertanggungjawabkan secara akademis.

---

menghubungkan pikirannya ke dalam jaringan tersebut.

1.7.1 Penelitian Lapangan

1.7.1.1 Wawancara Berpedoman

Wawancara berpedoman dilakukan kepada responden di dalam dan di luar lingkungan Unit V *IT & Cybercrime*. Wawancara tersebut dilakukan berdasarkan daftar pertanyaan yang telah ditentukan sebelumnya dengan pengembangan pertanyaan yang relevan selama proses wawancara disesuaikan dengan jawaban informan.

Wawancara berpedoman telah dilakukan kepada informan yang merupakan para penyidik Unit V *IT & Cybercrime* Bareskrim Polri yaitu:

a. Eddy Hartono, S.Ik, Ajun Komisaris Besar Polisi
b. Setiady, S.H., Ajun Komisaris Besar Polisi
c. Drs. Idam Wasiadi, S.H., S.Kom, MT, Ajun Komisaris Besar Polisi
d. Parmin, S.H., Komisaris Polisi
e. Zamri, S.Kom, Komisaris Polisi
f. Dicky Patrianegara, S.H., S.Ik, M.Si, Komisaris Polisi
g. Surawan, S.Ik, Komisaris Polisi
h. Lyndriyani, S.H., Ajun Komisaris Polisi
i. Arif Mahfudiarto, S.Ik, Ajun Komisaris Polisi
j. I K Budi Hendrawan, S.H., S.Ik, Ajun Komisaris Polisi
k. Alexander Sabar, S.Ik., Ajun Komisaris Polisi
l. Poibe Intan Nosa Lince, Inspektur Polisi I
m. H. Budhi Sutrisno, S.H., M.H. Inspektur Polisi
n. Dra.S Laksmi D, Ajun Komisaris Besar Polisi
o. Gagas Nugraha, Ajun Komisaris Besar Polisi

Selain itu, dilakukan juga wawancara mendalam dengan Dra. S. Laksmi D., Ajun Komisaris Besar Polisi yang mendalami *Child Exploitation Tracking System* (*CETS*), dan anggota Unit V *IT & Cybercrime* yang bertanggung jawab atas laboratorium forensik komputer. Wawancara tersebut menitikberatkan pada program kerja Unit V *IT & Cybercrime* yang telah mereka lakukan serta proses kerja yang biasa diterapkan oleh mereka dalam pekerjaan sehari-hari. Selanjutnya telah dilakukan juga wawancara lanjutan dengan Gagas Nugraha, Ajun Komisaris

Besar Polisi. Pertanyaan dalam wawancara terhadapnya terfokus pada organisasi Unit V *IT & Cybercrime*, seperti: struktur organisasi, visi dan misi, tanggung jawab dan wewenang, manajemen organisasi Unit *V IT & Cybercrime* yang meliputi: perencanaan program kerja, pelaksanaan program kerja termasuk di dalamnya pengelolaan sumber daya manusia, peningkatan infrastruktur, perluasan *networking*, penegakan hukum, dan evaluasi program kerja. Selain itu, ditanyakan juga mengenai aspek organisasi dan sistem komando yang menyangkut hubungan antar anggota, hubungan anggota dengan pimpinan dan hubungan dengan pihak eksternal.

Wawancara berpedoman yang dilakukan terhadap informan dari luar Unit V *IT & Cybercrime,* yang menyangkut korban kejahatan *hacking* dalam hal ini Partai Golkar diwakili oleh Ir. Fayakhun Andriadi selaku pimpinan yang membawahi bidang *Information Technology* Partai Golkar, sedangkan dari pihak penasehat hukum pelaku kejahatan diwakili oleh Agung Nugroho W., S.H., S.Sos, M.M.

Data dari para narasumber tersebut merupakan data pelengkap, bukan data utama yang menjadi prioritas yang dikaji dalam studi ini karena fokus penelitian lebih mengarah pada Unit V *IT & Cybercrime*.

1.7.1.2 Penyebaran Pertanyaan Terbuka Melalui *E-mail*

Penelitian juga dilakukan dengan menyebarkan pertanyaan terbuka melalui *email* yang ditujukan kepada aparat penegak hukum di bidang komputer dari berbagai negara. Hasil pertanyaan terbuka tersebut diperoleh dari perwakilan negara Inggris, Amerika Serikat, Hong Kong, serta dari perwakilan Dewan Eropa (Council of Europe). Informasi yang diperoleh dari jawaban pertanyaan terbuka tersebut merupakan masukan yang berharga sebagai perbandingan manajemen penyidikan *hacking* di Indonesia dengan negara lain yang relatif lebih maju di bidang teknologi, sumber daya manusia dan kaya akan pengalaman menangani kasus *cybercrime*.

1.7.1.3 Diskusi Kelompok Terfokus (*Focus Group Discussion*)

Diskusi kelompok terfokus dilakukan berdasarkan panduan diskusi kelompok terfokus yang dibuat oleh penulis. Diskusi kelompok terfokus telah

dilakukan terhadap dua kelompok yang pemilihan partisipannya berdasarkan kepangkatan mereka yaitu:

a. Kelompok I adalah para penyidik Unit V *IT & Cybercrime*, Perwira Menengah (Pamen) sebanyak 10 partisipan yang disebut kelompok Robocop 01.
b. Kelompok II adalah para penyidik dari Unit V *IT & Cybercrime*, Perwira Pertama (Pama) sebanyak 11 orang yang disebut kelompok Robocop 02.

Diskusi kelompok terfokus dipandu oleh moderator independen yaitu Rulas Sihombing, dan dilaksanakan di kantor peneliti independen Prompt (PT Riset Prima Indonesia) yang beralamat di Century Tower lantai 5, suite 501, Jalan HR Rasuna Said, Kav. X-2 No.4 Jakarta 12950. Selama proses diskusi kelompok terfokus dilaksanakan, penulis melakukan observasi terhadap jalannya diskusi kelompok yang dilakukan di ruang observasi kantor tersebut dan melakukan analisis hasil diskusi, serta memberikan pertanyaan pengembangan sesuai dengan respon partisipan yang terungkap dalam diskusi tersebut yang diberikan secara tidak langsung melalui moderator independen yang memimpin diskusi yang bersangkutan.

Tujuan dari diskusi kelompok terfokus ini adalah untuk menganalisis hubungan antara penerapan manajemen penyidikan *hacking* dengan pencapaian tujuan organisasi Unit V *IT & Cybercrime*, yang dipengaruhi oleh budaya organisasi dan gaya kepemimpinan organisasi serta lingkungan organisasi. Dalam diskusi kelompok tersebut digali mengenai: bagaimana manajemen diterapkan pada Unit V *IT & Cybercrime*; pihak-pihak yang berkepentingan dengan Unit V *IT & Cybercrime (Stakeholder Mapping)*; bagaimana budaya organisasi Unit V *IT & Cybercrime* dijalankan; bagaimana kepemimpinan pada Unit V *IT & Cybercrime*; budaya organisasi dan kepemimpinan yang mempengaruhi kinerja organisasi dalam menerapkan prinsip dan memberdayakan fungsi manajemen pada saat melakukan penyelidikan dan penyidikan yang diterapkan dalam Unit V *IT & Cybercrime*; serta hal-hal yang perlu diubah, dipelihara untuk mencapai peningkatan performa organisasi. Pertanyaan-pertanyaan yang tidak sempat diajukan atau jawaban yang dianggap penulis kurang memadai, telah ditanyakan kembali kepada individu yang bersangkutan melalui wawancara berpedoman

lanjutan.

1.7.2 Penelitian Literatur

Penelitian lapangan dilakukan secara bersamaan dengan penelitian literatur. Sesuai dengan masukan dari tim penguji proposal, penulis lebih terfokus pada jurnal ilmiah yang berkaitan dengan ilmu antropologi, sosiologi, dan psikologi yang berhubungan dengan organisasi, manajemen, penyidikan dan kejahatan komputer. Pencarian jurnal ilmiah dilakukan baik secara konvensional maupun *online*. Liputan media massa mengenai topik terkait juga dimasukkan dalam penulisan penelitian agar ulasan menjadi lebih terkini.

1.8 Sistematika Penulisan

Disertasi ini disusun dengan sistematika penulisan yang terdiri dari lima (5) bab sebagai berikut:

Bab I Pendahuluan

Bab ini menjelaskan latar belakang pentingnya penelitian ini, masalah penelitian yang dikaji, tujuan dan kegunaan penelitian, kerangka teori, metodologi penelitian, metode penelitian, dan pengorganisasian penelitian yang diterapkan berikut sitematika penulisan disertasi.

Bab II *Hacking* sebagai Tindak Pidana

Bab ini menjelaskan mengenai perbuatan *hacking* sebagai suatu tindak pidana yang dimulai dengan penjelasan tentang perkembangan komputer dan internet serta penggunaannya dalam kehidupan manusia yang juga menimbulkan dampak negatif berupa berkembangnya kejahatan berkaitan dengan komputer dan internet. Sehubungan dengan itu, akan dijabarkan mengenai konsep *cybercrime* yang meliputi pengertian, karakteristik dan kategorisasi *cybercrime,* dan pembahasan mengenai pengaturannya yang telah disampaikan oleh beberapa ahli hukum serta diskusi mengenai kemungkinan pengaturan *cybercrime* secara khusus di Indonesia. Selanjutnya secara khusus akan dibahas mengenai *hacking* sebagai suatu tindak pidana yang meliputi pengertian dan jenis perbuatan *hacking,* karakteristik *hacker* sebagai pelaku *hacking*, serta berbagai ketentuan hukum yang

berlaku baik dalam KUHP maupun undang-undang khusus lainnya yang dapat diterapkan untuk tindak pidana *hacking*, serta pengaturannya dalam RUU KUHP dan RUU TPTI.

Bab III Manajemen Penyidikan Tindak Pidana *Hacking*

Bab ini menjelaskan mengenai penyidikan tindak pidana, berikut dengan teknik dan prosedurnya yang terdiri dari penjelasan mengenai penyidikan tindak pidana yang meliputi rangkaian kegiatan penyidikan tindak pidana yaitu penyelidikan, penindakan, pemeriksaan tindak pidana serta penyelesaian dan penyerahan berkas perkara, berbagai dukungan teknis penyidikan tindak pidana, administrasi penyidikan tindak pidana serta pengawasan dan pengendalian penyidikan tindak pidana. Bab ini juga membahas mengenai penyidikan tindak pidana *hacking*, yang terdiri dari rangkaian kegiatan penyidikan tindak pidana *hacking*, prosedur penyelidikan dan penindakan tindak pidana *hacking*, proses pemeriksaan tindak pidana *hacking* serta tahap penyelesaian dan penyerahan berkas perkara tindak pidana *hacking*, mengenai dukungan teknis penyidikan *hacking* serta administrasi penyidikan *hacking*, yang secara umum menunjukkan karakteristik penyidikannya yang khas berkaitan dengan proses interpretasi penyidik atas ketentuan hukum formil dalam pelaksanaan penyidikannya. Selanjutnya dibahas pula mengenai penyidikan tindak pidana *hacking* di negara lain, serta mengenai manajemen penyidikan tindak pidana yang meliputi setiap proses perencanaan, pengorganisasian, dan pelaksanaan/implementasi serta pengawasan dan pengendalian.

Bab IV Penerapan Manajemen Penyidikan oleh Unit V *IT & Cybercrime*

Bab ini membahas mengenai manajemen penyidikan pada Unit V *IT & Cybercrime* dengan studi kasus manajemen penyidikan dalam penanganan kasus *hacking website* Partai Golkar. Pertama-tama akan dijelaskan mengenai organisasi Unit V *IT & Cybercrime* sebagai pelaksana penyidikan kasus *hacking*, kemudian dijelaskan mengenai posisi kasus *hacking website* Partai Golkar dan prosedur penanganan yang diterapkan oleh para penyidik dalam Unit V *IT & Cybercrime*. Selanjutnya dibahas mengenai berbagai permasalahan yang dihadapinya dan bagaimana mereka berhasil memecahkan masalah dengan mencarikan solusinya yang tepat. Berdasarkan analisis atas kasus tersebut, penulis akan membahas

mengenai manajemen penyidikan *hacking* yang diterapkan oleh Unit V *IT & Cybercrime* dan faktor-faktor yang memberikan pengaruh terhadap berjalannya sistem manajemen dalam Unit V *IT & Cybercrime* yaitu faktor kepemimpinan, budaya organisasi dan *stakeholders*.

Bab V Penutup

Bab ini menyajikan kesimpulan disertasi dan beberapa hal yang dapat disampaikan sebagai kontribusi bagi ilmu pengetahuan dan kontribusi dalam praktek, diskusi lebih lanjut serta keterbatasan dari disertasi ini.

BAB II

HACKING SEBAGAI TINDAK PIDANA

2.1 Teknologi Internet

Saat ini dunia berada dalam era informasi (*information age*) yang merupakan tahapan lebih lanjut setelah era prasejarah, era agraris dan era industri sebagaimana disampaikan oleh Anne W. Branscomb dalam bukunya *Toward a Law of Global Communication Network* (1986: 1). Dalam era agraris, kehidupan manusia sangat tergantung pada daerah yang subur atau sumber daya alam untuk mendapatkan makanan. Manusia mengembangkan sistem agraria berupa penguasaan tanah untuk kepentingan masyarakat. Lebih lanjut ternyata manusia terus berkembang dan sadar bahwa hidupnya tidak tergantung pada alam saja tetapi juga hubungan antar masyarakat untuk saling bertukar. Disinilah manusia memasuki era industri dimana manusia saling bertukar barang kebutuhan dengan masyarakat lain sehingga berkembanglah dunia perdagangan dan industri. Berkat kemajuan teknologi, hubungan manusia semakin intens dengan adanya keberagaman alat komunikasi sehingga manusia memasuki era informasi. Dalam era informasi, keberadaan informasi berperan penting dalam semua aspek kehidupan serta merupakan kebutuhan hidup baik bagi individu maupun organisasi (Makarim, 2005: 27-28).

Tabel 2.1
Perkembangan Peradaban Manusia

Perkembangan Peradaban Manusia dan Kebudayaannya	Gelombang Pertama	Gelombang Kedua	Gelombang Ketiga	Gelombang Keempat	Gelombang Kelima
	Masyarakat Pra Sejarah	Masyarakat Agraris	Masyarakat Industri	Masyarakat Informasi	Masyarakat Pengetahuan
Energi	otot	air, angin, api, tanah	batu bara, gas alam, mesin, elektronik	listrik, laser, energi matahari	barang dan jasa dari ilmu pengetahuan dan teknologi
Kekuasaan	kekuatan fisik	tanah dan makanan	keterampilan usaha	uang, informasi	pengetahuan

Perkembangan Peradaban Manusia dan Kebudayaannya	Gelombang Pertama	Gelombang Kedua	Gelombang Ketiga	Gelombang Keempat	Gelombang Kelima
Hukum	hukum rimba	hukum agraris, adat	*civil code* Perancis, kebebasan berkontrak, *common law*	hukum publik, hukum administrasi dan konstitusi	kembali ke kehidupan beragama, hukum sebagai panduan terhadap toleransi kebebasan individu, globalisasi dan hukum international

(Sumber: Makarim, 2005: 28)

Berkembangnya teknologi informasi memberikan kesempatan untuk hidup dan bekerja dalam suatu komunikasi yang global. Komunikasi bahkan transaksi uang dalam jumlah besar dapat dilakukan dari berbagai tempat yang berjauhan dengan waktu yang cepat dan biaya yang lebih murah. Perkembangan teknologi komputer, akses internet yang luas, dan pesatnya pasar alat komunikasi yang semakin canggih telah mengubah cara hidup manusia dalam berbagai kegiatannya seperti bisnis, pendidikan dan lain-lain. Sebaliknya, bentuk kejahatan pun berubah seiring dengan perkembangan teknologi. Misalnya, akses internet yang semakin luas telah membuka kesempatan bagi pelaku kejahatan untuk mencapai tujuannya dengan memanfaatkan akses tersebut secara melawan hukum. Akibatnya terjadi kerugian terhadap masyarakat seperti kehilangan uang melalui transaksi elektronik (*online*), bahkan dapat menimbulkan akibat fisik seperti kegiatan terorisme yang mengancam kehidupan masyarakat. Sayangnya, dalam beberapa kasus, hukum tertinggal di belakang perkembangan kejahatan, dan untuk menghadapi ancaman baru yang semakin berkembang (yang disebut *cybercrime*) seringkali kekurangan teknologi dan sumber daya manusia yang terlatih (Shinder, 2002: 2).

2.1.1 Pengertian Internet

Internet adalah rangkaian jaringan komputer yang saling terhubung, bersifat luas dan dapat diakses oleh masyarakat umum yang melakukan pengiriman data

melalui pertukaran paket menggunakan *Internet Protocol* (*IP*) *standard* (http://en.wikipedia.org/wiki/Internet, 28 Februari 2008). Internet merupakan 'jaringan dari seluruh jaringan' yang terdiri dari jutaan jaringan yang lebih kecil milik domestik, akademi, bisnis dan pemerintahan, yang secara bersama-sama membawa berbagai informasi dan pelayanan, seperti surat elektronik (*email*), *online chat*, pengiriman *file*, dan halaman-halaman *web* yang saling terhubung serta sumber lain dari *World Wide Web* (*WWW*). Internet juga dapat diartikan sebagai hasil dari interkoneksi ribuan jaringan, yang sekarang bahkan menghubungkan ratusan juta komputer di seluruh dunia (Furnell, 2002: 4-5).

2.1.2 Perkembangan Internet

Pada awalnya internet adalah jaringan komputer untuk sistem pertahanan yang dikembangkan oleh Departemen Pertahanan Amerika Serikat. Proyek jaringan ini bernama *Advanced Research Projects Agency* (ARPA). Jaringan komputernya sendiri diberi nama ARPANET. Pada tahun 1969, para ilmuwan memikirkan untuk membuat suatu jaringan komputer yang dapat menghubungkan mereka agar dapat berkomunikasi satu dengan lainnya. Departemen Pertahanan Amerika Serikat kemudian menjadi sponsor untuk mewujudkan ide ini melalui ARPANET. Demonstrasi pertama dari ARPANET dilakukan pada tahun 1969 yaitu dengan menghubungkan jaringan komputer ke empat universitas yaitu *University of California Los Angeles* (UCLA), *Stanford Research Institute*, *University of California Santa Barbara* dan *University of Utah*. Seiring berjalannya waktu, muncul jaringan lain seperti *United Kingdom Joint Academic Network* (JANET) yang ditujukan untuk pendidikan, jaringan militer Amerika Serikat (U.S. MILNET) yang merupakan hasil dari pemisahan sistem pertahanan dari ARPANET pada tahun 1983, dan *U.S. National Science Foundation* (NSFNET). Semua jaringan ini mampu berkomunikasi satu sama lain karena mempunyai protokol yang sama dan menggunakan infrastruktur yang sama yaitu internet. ARPANET secara resmi dinonaktifkan pada tahun 1990.

Pada saat ini, infrastruktur internet semakin meluas dan semakin banyak jaringan tergabung dalam internet. Tidak sampai tahun 1990, dunia sadar akan pentingnya internet dan penggunaannya makin meningkat pesat (Furnell, 2002: 3-

5). Perkembangan internet selanjutnya terkait dengan tersedianya dua fasilitas yaitu *email*[10] dan banyaknya *server www*.[11]

2.1.3 Kegunaan Internet

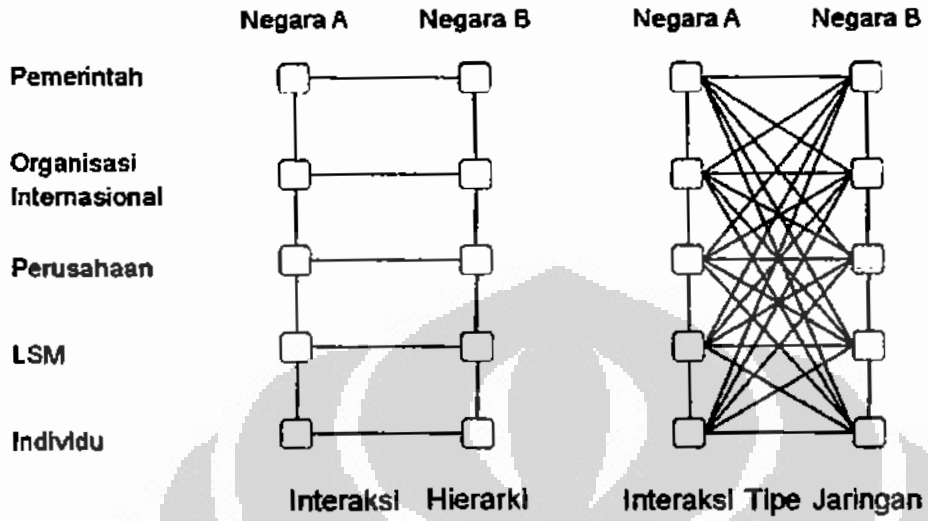
Ryuhei Hosaya dalam makalahnya "*Cyberspace and Virtual Diplomacy: The end of nation-state?*" (1997: 10) membuat suatu analisis mengenai implikasi perkembangan internet sebagai alat komunikasi terhadap hubungan diplomasi suatu negara dengan negara lain. Menurut Ryuhei, telah terjadi perubahan pola interaksi antara elemen-elemen di dua negara yang tadinya hierarki atau berjenjang menjadi interaksi jaringan. Setiap elemen masyarakat di suatu negara dapat melakukan hubungan langsung dengan elemen masyarakat di negara lain dengan mudah. Pemerintah, organisasi internasional, perusahaan, Lembaga Swadaya Masyarakat (LSM); dan setiap individu sebagai warga suatu negara tertentu dapat berinteraksi langsung dengan pihak lain baik di dalam negara tersebut ataupun negara lain. Jaringan komunikasi interaktif dan multimedia yang menyebar luas melalui internet digunakan oleh banyak pihak untuk menyalurkan kepentingan masing-masing yang berbeda-beda. Penggunaan internet pada masing-masing pihak tersebut dapat terlihat pada Gambar 2.1.

---

[10]Internet semakin berkembang dengan maraknya penggunaan *email*. *Email* sendiri dapat berkembang karena adanya layanan *online*, misalnya *America Online*, *Compu Serve*, dan sebagainya, yang menciptakan jaringan internet melalui *email*. Internet berfungsi sebagai pusat penghubung untuk *email* di luar komunitas internet. Seorang pelanggan *online service* dapat mengirim surat kepada pelanggan lain menggunakan internet sebagai saluran penghubung. Internet menjadi perekat dunia dalam surat menyurat elektronik (Ariyus, 2005: 160-161).

[11]Internet juga semakin berkembang dengan banyaknya *server www* yang menjadi penggabung dokumen dari seluruh dunia. *www* menyediakan pertukaran informasi tak terbatas yang berkembang pesat. Dengan adanya penjelajah *web* yang berbasis grafis seperti *Mosaic* dan *Netscape Navigator*, dan kemudian disusul oleh *Microsoft Internet Explorer*, seluruh khasanah informasi ini menjadi mudah diakses oleh seluruh pengguna komputer. *web* juga berkembang menjadi tempat penyimpanan *driver*, *updates*, dan demo yang dapat di-*download* melalui *browser* (Ariyus, 2005: 160-161).

Gambar 2.1
Hierarki dengan Tipe Interaksi Jaringan



(Sumber: Ryuhei Hosaya, 1997 : 10)

2.1.3.1 Penggunaan Internet pada Pemerintahan

Era informasi akan berpotensi menjadi masa paling demokratis sepanjang sejarah, karena setiap individu dapat saling berhubungan baik diantara individu tersebut maupun dengan pemerintahnya. Pada era informasi, semua warga negara mempunyai akses terhadap berbagai informasi dan kesempatan yang sama untuk saling berbagi pendapat dan pandangan. Menurut laporan Bangemann[12] (*Bangemann Report*), penerapan pelayanan publik yang semakin efisien, transparan dan responsif akan mendekatkan pemerintah dengan warga negaranya dengan biaya yang minim (Munir, 1999: 9).

Electronic Government (*e-Gov*) juga telah dicanangkan oleh Pemerintah Indonesia terutama untuk meningkatkan daya saing Indonesia terhadap negara lain dan untuk meningkatkan pelayanan publik. Sebagai contoh, *e-Gov* yang diterapkan oleh Departemen Perindustrian dan Perdagangan Republik Indonesia (Depperindag). Dalam seminar bertema "Penanganan Masalah *Cybercrime* di

[12] *Bangemann Report* adalah laporan yang dihasilkan oleh komisi yang dipimpin oleh Martin Bangermann yang bertugas untuk memberikan rekomendasi kepada Council of Europe yang dapat digunakan untuk membuat revolusi komunikasi di Eropa yang pada akhirnya akan memperkuat daya saing negara-negara Eropa dalam persaingan global dan dalam sistem ekonomi yang saling tergantung antara negara yang satu dengan negara yang lain (Munir, 1999: 16).

Indonesia dan Pengembangan Kebijaksanaan Nasional yang Menyeluruh dan Terpadu" yang diselenggarakan secara bersama oleh Departemen Luar Negeri, Bank Indonesia dan Departemen Komunikasi dan Informatika (Depkominfo), perwakilan Direktorat Jenderal (Dirjen) Perdagangan Luar Negeri Deperindag menyatakan bahwa Dirjen Depdagri akan menerapkan Surat Keterangan Asal (*Certificate of Origin*) secara otomatis di 23 Instansi Penerbit Surat Keterangan Asal, dan menyediakan fasilitas pertukaran data elektronik di antara empat Direktur Jenderal yaitu: Dirjen Perdagangan Luar Negeri, Dirjen Perdagangan Dalam Negeri, Dirjen Bea dan Cukai serta Dirjen Pajak, menyangkut Kebijakan dan Perizinan Ekspor dan Impor serta Laporan Keuangan Perusahaan (Depperindag, 9 Agustus 2006: 3).

2.1.3.2 Penggunaan Internet pada Dunia Usaha

a. ***E-media***

Saat ini media massa konvensional, baik media cetak maupun media elektronik banyak menyajikan informasi, hiburan dan edukasi melalui halaman elektronik (*web pages)*. Sebagai contoh, televisi (TV) terutama yang menyajikan berita (*hardnews*), selain tampil di layar kaca juga tampil dalam tayangan *website* atau lebih dikenal dengan istilah *TV Online* seperti: *http://www.cnn.com/; http://www.bbc.co.uk/*. Hal ini tercermin dari survei yang dilakukan lembaga Deloitte & Touche terhadap warga Amerika Serikat pada bulan Oktober 2007, yang menyatakan bahwa sekitar 38 persen konsumen lebih memilih menonton televisi secara *online* melalui internet (Kompas, 2008: 14).

Media cetak pun hadir dalam bentuk *online* seperti koran: *http://www.kompas.com/* dan *http://www.thejakartapost.com/*, *http://kontan-harian.com*; majalah: *http://www.time.com/time/*, termasuk majalah kontroversial *http://www.playboy.com/magazine/*. Ada pula media massa yang murni memilih bentuk *online* di internet tanpa ada edisi konvensionalnya seperti portal berita *http://detik.com/*.

Teknologi internet juga dapat digunakan sebagai media promosi terutama bagi para pelaku usaha untuk mempromosikan produknya baik berupa barang maupun jasa kepada masyarakat luas. Sebagai contoh, perusahaan telepon seluler

NOKIA meluncurkan program terbaru yaitu *Independent Artists Club* (*IAC*) yang dapat diakses melalui alamat *website www.nokia.co.id/iac* (Kompas, 21 Desember 2007: 16).

Selain itu, warga biasa juga dapat membuat media massa *online* sendiri seperti layaknya reporter profesional yang memberikan laporan baik berita, foto maupun video atau lebih dikenal dengan istilah *citizen reporter* (*netizen*). Sebagai contoh, media *online* asal Singapura *Straits Times Online Mobile Print* (*STOMP*) yang diwadahi oleh koran berpengaruh Singapura *The Strait Times*. Media ini memberikan kebebasan kepada para *netizen* untuk aktif berinteraksi secara *online* seperti layaknya wartawan profesional. Dengan tiga *platform* yang digunakan yakni cetak, *mobile*, dan *online*, *STOMP* dapat berinteraksi dengan warga Singapura dengan cara baru yang lebih menarik dan tidak pasif. Selain *STOMP*, ada beberapa media massa *online* untuk *netizen* seperti "*i-Report*" oleh *Cable News Network* (*CNN*), "*People of the Web*" dan "*Eyewitness News*" yang dikeluarkan Yahoo!. *British Broadcasting Corporation* (*BBC*) membuat "*Eyewitness Tale*" untuk foto dan "*Survivor Amateur Videos*" untuk video. *Microsoft Network National Broadcasting Company* (*MSNBC*) menciptakan "*Citizen Journalists Report*". Selain itu, ada juga "*Reuters online*", "*OhmyNews*" (Korea Selatan), dan di Indonesia ada "*Wikimu*" dan "*Panyingkul*" (Kompas, 30 November 2007: 45).

b. *E-Commerce* (perdagangan elektronik)

Dimungkinkannya transaksi melalui internet telah mendorong adanya perdagangan internet dalam suatu bisnis *virtual*, seperti *virtual store* dan *virtual company*. Dengan adanya komunikasi antar komputer melalui pertukaran data elektronik (*Electronic Data Interchange),* pelaku bisnis tidak lagi mengandalkan basis perusahaan yang konvensional atau nyata. Contohnya adalah *http://hub.ebay.com/buy* untuk jual beli beragam barang baru dan bekas yang menawarkan lebih dari 30 kategori barang dari mulai barang antik sampai *video games*. Ada juga *http://www.amazon.com/* yang menjual beragam buku, majalah, koran dan *textbooks* serta 10 kategori lainnya mulai dari film sampai dengan peralatan. Di Indonesia juga terdapat *http://www.glodokshop.com/* yaitu penjual barang elektronik *online* dengan jaminan 6 jam barang terkirim.

Pemesanan baik barang maupun jasa melalui internet memangkas biaya operasional pelaku usaha dan memudahkan konsumen karena tidak perlu datang ke suatu *counter*, dan mengantri membeli barang atau jasa. Sebagai contoh pemesanan tiket pesawat terbang lengkap dengan pilihan keberangkatan, kota tujuan, dan jam penerbangan; pembayaran dilakukan dengan kartu kredit seperti yang ditawarkan Air Asia (*http://www.airasia.com/*). Untuk jasa perhotelan, kamar dapat dipesan secara *online* ke berbagai hotel dengan cara pembayaran secara *online* pula, contohnya pemesanan kamar pada Ibis Hotel pada alamat *http://www.ibishotel.com*. Tiket nonton konser pun dapat dipesan melalui internet pada *http://www.cheaptickets.com*.

Jasa perbankan pun juga memanfaatkan fasilitas internet dalam pelayanannya dengan bentuk *e-banking*. *E-banking* adalah saluran distribusi bank yang memberi kemudahan bagi nasabah untuk mengakses rekening yang dimilikinya melalui internet ataupun telepon genggam. Layanan yang tersedia dalam *internet banking* contohnya seperti layanan pada *internet banking* Bank Mandiri (*http://www.bankmandiri.co.id/*) meliputi transfer antar rekening Bank Mandiri, pembayaran tagihan, informasi saldo, aktivitas transaksi *internet banking*, permintaan buku cek/BG, *update* profil, personalisasi dan pendaftaran layanan notifikasi *SMS Banking Mandiri*.

c. *E-Learning, Distance Learning*

Pendidikan berperan dalam mempersiapkan sumber daya manusia. Melalui pendidikan, diperoleh pengetahuan dan keterampilan di berbagai bidang, sehingga mampu mendapatkan, mengartikan dan memodifikasi informasi yang tersedia untuk perkembangan ilmu pengetahuan. Dunia pendidikan juga tidak ketinggalan dalam memanfaatkan internet. Penerapan teknologi informasi dan komunikasi seperti internet dalam dunia pendidikan tentu bertujuan bukan untuk mempersulit pembelajaran tetapi untuk memudahkan dan membuat proses pembelajaran yang menyenangkan bagi anak didik. Hal ini akan mengubah proses belajar-mengajar di sekolah ke arah pendidikan yang mendorong inovasi dan eksperimen. Di Korea, Telekom telah mendonasikan lebih dari seratus ribu *Personal Computer* (*PC*) ke enam ribu tiga ratus sekolah di seluruh negeri (Munir, 1999: 11).

Pada bulan Agustus 2007 di Singapura tercatat lima ribu enam ratus *hotspot*

tersedia untuk melayani lima ratus dua puluh ribu pelanggan internet. Hal ini dilakukan Pemerintah Singapura untuk mendukung penggunaan teknologi informasi dan komunikasi secara nasional terutama untuk dunia pendidikan dalam rangka mewujudkan bangsa yang cerdas yang disebut *Intelligent Nation by* 2015 (IN2015). Sama seperti Singapura, Indonesia sendiri ternyata juga mampu memberikan kontribusi dalam pemanfaatan internet untuk dunia pendidikan yaitu dengan adanya *software* pendidikan fisika (*Amazing Physics*) dan pendidikan matematika (*Amazing Mathematics*) berbentuk animasi yang dikeluarkan oleh PT Pesona Edukasi. *Software* ini bahkan sudah dipakai di 22 negara dan seribu lima ratus sekolah di Indonesia (Kompas, 26 November 2007: 14).

Dengan persaingan yang ketat di dunia pendidikan baik di dalam mapun di luar negeri, mendorong terciptanya beragam fasilitas yang disediakan institusi pendidikan untuk memenuhi kebutuhan masyarakat di bidang pendidikan. Misalnya, tersedia sistem pengajaran jarak jauh (*distance learning*) yang materi pengajarannya diberikan dalam bentuk modul dan tatap muka antara murid/mahasiswa dan guru/dosen diminimalisir dengan korespondensi baik konvensional maupun elektronik. Pembelajaran secara elektronik semakin diperlukan. Oleh karena itu, para guru/dosen diharapkan menyediakan materi yang dapat di-*upload* di internet untuk kemudian diakses oleh anak didiknya. Di Universitas Indonesia, *E-learning* telah diterapkan, yaitu dengan program *Student Centered E-Learning Environment* atau *Scele*. *Scele* adalah sebuah upaya yang dilakukan oleh Fakultas Ilmu Komputer Universitas Indonesia (Fasilkom UI) untuk meningkatkan akses bagi pendidikan dengan menggunakan media internet sebagai solusinya. Untuk tujuan ini, Fasilkom UI mengembangkan sebuah sistem untuk menangani pembelajaran jarak jauh yang dimodifikasi dari Moodle (*http://www.moodle.org*), sebuah *Open Source Content Management System* (CMS)[13] (*http://scele.cs.ui.ac.id/*, 1 Maret 2008). Selain Universitas Indonesia, institusi pendidikan yang menerapkan program *e-learning* adalah Universitas Terbuka (*http://student.ut.ac.id/*).

---

[13] *Content Management System* (CMS) adalah sistem yang digunakan untuk mengatur isi dari suatu *website*. Isi yang diatur termasuk *file* komputer, media gambar, *file* audio, dokumen elektronik dan isi dari *web* (*http://en.wikipedia.org/wiki/Content_management_system*, 1 Maret 2008).

Di samping program-program *E-Learning* tersebut di atas, program lain yang cukup populer dan telah giat diupayakan oleh universitas-universitas lainnya adalah upaya menyediakan berbagai satuan acara perkuliahan atau materi kuliah dalam bentuk elektronik yang dapat diakses melalui internet, dengan tujuan agar anak didik lebih siap menghadapi tatap muka di kelas atau sebagai pengganti pertemuan kelas yang tertunda. Untuk pembelajaran jarak jauh diperlukan perpustakaan elektronik yang menyediakan berbagai buku, jurnal dan makalah elektronik. Perpustakaan elektronik yang saat ini telah tersedia diantaranya *http://pustaka.ut.ac.id/* atau *https://nestor.rug.nl/webapps/* dimana setiap mahasiswa mempunyai *user id* dan *password* tersendiri untuk dapat mengakses perpustakaan tersebut.

Berdasarkan data dari Direktorat Jenderal Peningkatan Mutu Pendidik dan Tenaga Kependidikan (PMPTK) tahun 2005-2006, tingkat guru yang berpendidikan sarjana masih rendah misalnya untuk Taman Kanak-Kanak (TK) baru 10,69 persen, Sekolah Dasar (SD) 16,57 persen, Sekolah Menengah Pertama (SMP) 61,31 persen, dan Sekolah Menengah Atas (SMA) 83,43 persen. Untuk mendukung program pembelajaran jarak jauh (*e-learning*), pada tahun 2008 pemerintah menyediakan anggaran sejumlah 1 triliun rupiah untuk membangun sumber atau *resources centre* di sekolah-sekolah dalam rangka mempercepat penggunaan teknologi informasi dan komunikasi seperti penyediaan komputer dan perangkat multimedia lain. Tentu hal ini harus diimbangi dengan kesiapan guru-guru yang berkualifikasi dalam artian mampu memanfaatkan fasilitas ini dengan baik (Kompas, 3 Desember 2007: 14).

d. Perawatan kesehatan/*Telemedicine*

Perkembangan teknologi telekomunikasi kini memungkinkan dilakukannya diagnosa penyakit dalam jarak hingga ribuan kilometer antara dokter dengan para pasiennya. Dokter-dokter yang berada di Bandung, misalnya, dapat melakukan penelusuran sebab-sebab penyakit para pasien yang tinggal di Banda Aceh atau tempat-tempat lain melalui terminal *video conference* yang terhubung ke jaringan *Virtual Private Network* berbasis *Internet Protocol* atau biasa disingkat *VPN-IP* Telkom. Aplikasi layanan *telemedicine* merupakan kombinasi antara percakapan video jarak jauh (*video conference*), pertukaran dan

analisis data medis, serta pelatihan jarak jauh (*teletutorial*) bagi tenaga medis di Aceh. Menteri Kesehatan Siti Fadilah Sapari, telah meresmikan pengoperasian layanan pengobatan jarak jauh (*telemedicine*) melalui *VPN-IP* Telkom yang dilakukan oleh Rumah Sakit (RS) Hasan Sadikin dan RS Mata Cicendo Bandung (*www.pikiran-rakyat.com*, 28 April 2005).

2.1.3.3 Penggunaan Internet pada Organisasi Internasional, LSM, Organisasi Kemasyarakatan dan Partai Politik

Kegunaan eksternal internet pada organisasi adalah untuk mendapatkan simpati dan pemahaman dari masyarakat (*public*) sebagai *stakeholder* suatu organisasi seperti organisasi internasional, LSM, organisasi kemasyarakatan dan partai politik. Organisasi-organisasi ini perlu memberikan informasi mengenai visi dan misi, program kerja, para pengurus organisasi tersebut. Selain untuk menyebarkan informasi, internet dapat juga digunakan untuk menampung aspirasi masyarakat misalnya melalui *email* sebagai kritik dan saran serta mengundang peran serta masyarakat untuk turut melakukan hal seperti rekruitmen pegawai atau anggota, atau turut menandatangani petisi atau mengikuti acara organisasi bahkan turut serta pada suatu kampanye baik politik maupun non politik.

Berdasarkan informasi yang ditelusuri dari *website* Komisi Pemilihan Umum (KPU) yaitu *www.kpu.go.id*, tercatat ada 16 partai politik yang memiliki *website* diantaranya adalah:

Tabel 2.2
Partai politik dan *website*-nya

No.	Nama Partai Politik	Alamat *Website*
1.	Partai Demokrasi Indonesia Perjuangan	*www.pdi-perjuangan.or.id*
2.	Partai Demokrat	*www.demokrat.or.id*
3.	Partai Persatuan Pembangunan	*www.ppp.or.id*
4.	Partai Keadilan Sejahtera	*www.pk-sejahtera.org*
5.	Partai Damai Sejahtera	*www.partaidamaisejahtera.com*
6.	PNI Marhaenisme	*dpp-pni.tripod.com*
7.	Partai Buruh Sosial Demokrat (PBSD)	*www.pb-sd.org*
8.	Partai Merdeka	*www.partaimerdeka.or.id*
9.	Partai Indonesia Baru (PIB)	*www.partai-pib.or.id*
10.	Partai Nasional Banteng Kemerdekaan (PNBK)	*www.pnbk.i-p.com*
11.	Partai Kebangkitan Bangsa (PKB)	*www.kebangkitanbangsa.org*
12.	Partai Golkar	*www.partai-golkar.or.id/ www.golkar.or.id*
13.	Partai Patriot Pancasila	*www.patriotpancasila.org*

No.	Nama Partai Politik	Alamat *Website*
14.	Partai Bulan Bintang (PBB)	*www.pbb-online.org*
15.	Partai Pelopor	*www.partaipelopor.or.id*
16.	Partai Serikat Indonesia	*www.psi.online.or.id*

(Sumber: *www.kpu.org.id*)

Adapun beberapa LSM atau *Non Government Organization* (*NGO*) yang sudah memiliki *website* sendiri, diantaranya: (Djakarta The Magazine, 21 November 2007)

Tabel 2.3
LSM dan *website*-nya

No.	Nama LSM	Alamat *Website*
1.	*Wahana Lingkungan Hidup Indonesia*/WALHI (LSM pelestarian lingkungan hidup yang sehat, lestari dan hijau)	*www.walhi.or.id*
2.	GREENPEACE (LSM internasional untuk penyelamatan lingkungan)	*www.greenpeace.or.id*
3.	Panda (LSM dibawah *World Wide Fun* (*WWF*) untuk penyelamatan hewan langka)	*www.panda.or.id*
4.	Ikatan Profesional Lingkungan Hidup Indonesia/IPLHI (LSM untuk penyelamatan lingkungan).	*www.IPLHI.org*

(Sumber: Djakarta The Magazine, 21 November 2007: 5)

2.1.3.4 Penggunaan Internet pada Individu

Internet, selain digunakan untuk fasilitas *email* dan *browsing*, dapat dijadikan sebagai media ajang ekspresi diri baik dengan identitas asli maupun palsu. Kebebasan berpendapat dan berekspresi semacam ini diterapkan dalam pembuatan *blog*. Dalam membuat *blog* pengguna dapat melakukan kegiatan seperti membuat tulisan dalam *blog*, meng-*upload* foto atau lagu, sekaligus membuka peluang bagi orang lain untuk mengetahui informasi yang dibuat pemilik *blog* (*blogger*) pada *blog*-nya. Bahkan, *blog* juga dapat dimanfaatkan sebagai peluang bisnis *online* misalnya pemasang iklan pada suatu *blog* akan membayar sejumlah uang kepada pemilik *blog* sebagai biaya pemasangan iklan. Tentunya *blog* yang banyak diakses oleh pengguna internetlah yang berpotensi besar mendapatkan keuntungan ini. Selain itu, ada *blogger* yang dibayar atau disebut juga *blogger* berbayar. Seorang *blogger* dengan keahliannya dapat diminta sebuah media *online* untuk menulis kolom tetap. *Technorati,* situs

pencatat *web*, mencatat bahwa sampai September 2007 sudah terdapat 106 juta *blog* di seluruh dunia (Kompas, 2007: 16). Berdasarkan penelitian yang dilakukan oleh majalah *Business Week*, kota Jakarta termasuk salah satu dari empat kota besar di Asia yang memiliki jumlah *blogger* terbesar di dunia, kurang lebih berjumlah 130.000 *blogger* yang tersebar di seluruh Indonesia (Kompas, 5 November 2007: 34).

Dunia internet dapat digunakan sebagai media penyimpanan data atau kerap disebut *online storage* seperti *BoxNet* yang tersedia dalam dua layanan yaitu gratis dan berbayar. Setiap pengguna dapat menyimpan data dalam layanan ini seperti lagu, video dan lain-lain. Biasanya layanan ini digunakan oleh mereka yang memiliki mobilitas tinggi tapi ingin datanya dapat diakses dengan mudah tanpa harus membawa media penyimpanan seperti *flash disk* dan *Compact Disc* (*CD*). Tentu dengan syarat pengguna memiliki akun yang tetap dan terhubung dengan internet dan juga adanya aplikasi *web browser* untuk mengakses setiap layanan. Selain itu ada layanan *office online* yang didalamnya antara lain berisi aplikasi *word processor*, *spreadsheet*, dan presentasi berbasis *web* sehingga dapat diolah langsung di internet seperti *Google Document* yang dapat memudahkan seseorang untuk bekerja di mana pun dan kapan pun tanpa harus memusingkan apakah perangkat *PC* atau *notebook*-nya memiliki aplikasi *office* atau tidak (Kompas, 26 Desember 2007: 61).

2.1.4 Cara Kerja Internet

Pada umumnya masyarakat menikmati jasa internet melalui berbagai cara di antaranya melalui fasilitas institusi di mana mereka berada atau bekerja seperti kantor, kampus, atau sekolah. Selain itu, dapat berlangganan secara pribadi menggunakan kabel (*broadband*) seperti pada "Kabel Vision" atau *dial-up* baik yang tagihannya bersamaan dengan tagihan telepon seperti pada "Telkomnet *Instant*" atau terpisah seperti pada "*Speedy*" atau *provider* internet lainnya. Selain dihubungkan dengan kabel, koneksi internet dapat diperoleh melalui *wifi*. Pengguna internet menggunakan *laptop* di tempat-tempat tertentu seperti kafe, bandara, apartemen untuk dapat menikmati internet nirkabel di area yang terdapat fasilitas *wifi*. *Laptop* dapat juga dihubungkan dengan *compact modem* untuk

mengakses internet dari *provider* tertentu. Alternatif lainnya adalah warung internet (warnet) yang menyewakan koneksi internet dengan hitungan waktu tertentu (menit atau jam), atau yang lebih canggih lagi yaitu melalui *handphone*.

Menurut Reed (2004: 8-9), fungsi pengiriman informasi melalui internet dilakukan dengan cara meng-*copy* informasi digital dari komputer yang satu komputer yang lain sampai *copy* tersebut diterima oleh komputer penerima. Informasi itu bukan dikirim melalui jalur yang berkelanjutan. Melainkan komputer pengirim pesan memecah informasi tersebut dalam beberapa paket terpisah atau *datagrams* ke setiap alamat komputer penerima. Kemudian komputer penerima menyusun kembali paket informasi tersebut saat menerimanya. Sedangkan ada yang namanya komputer perantara (*intermediaries*) yang bekerja secara sederhana dengan hanya mengirim kembali paket informasi ke komputer lain sampai diterima oleh komputer yang dituju. Jadi ada 2 pihak yang terlibat dalam pertukaran informasi melalui internet yaitu pihak yang saling bertukar paket informasi dan komputer perantara yang menerima dan meneruskan paket informasi tersebut. Para pihak yang terlibat terbagi menjadi dua kelompok yaitu kelompok saling bertukar dan kelompok perantara. Kelompok saling bertukar adalah kelompok yang bertukar informasi seperti komputer pengirim dan penerima pesan yang merupakan akhir dari pengiriman pesan tersebut. Kelompok perantara adalah semua komputer yang menerima dan menyampaikan paket informasi tersebut. Menurut Hartono (2000: 342-343), secara garis besar, ada tiga teknik penggunaan internet yaitu melalui penyedia jasa internet (*Internet Service Provider/ISP*)[14], penyedia jasa informasi[15] dan koneksi internet secara langsung[16].

---

[14]Hubungan internet melalui penyedia jasa internet dilakukan dengan menjadi anggota penyedia jasa internet, misainya di Indonesia: Wasantara, Idola, *CBN*, *Speedy* dan lain sebagainya. Dengan membayar biaya bulanan, pemakai akan diberi nomor telepon yang dapat dihubungi untuk menghubungkan komputer miliknya ke jaringan yang ada pada penyedia jasa. Penyedia jasa internet akan memberikan identitas pemakai (*user-id* atau *account*) dan *password* (kata sandi). *Password* tersebut dapat disesuaikan dengan pilihan pelanggan. Selain itu, untuk dihubungkan ke penyedia jasa, komputer masih memerlukan perangkat lunak komunikasi yang menggunakan protokol internet yang disebut *Transmission Control Protocol* (TCP) atau *Internet Protocol (IP)*. Dengan perangkat lunak ini, pemakai dapat melakukan koneksi melalui saluran telepon (*dial-up connection*) dengan menggunakan modem. Jika sudah terhubung atau terkoneksi, maka pemakai sudah masuk ke dalam jaringan internet (Hartono, 2000: 342).

[15]Hubungan internet melalui penyedia jasa informasi. Penyedia jasa informasi yang terkenal di Amerika Serikat adalah *American Online* dan *Prodigy*. Penyedia jasa informasi ini menyediakan bermacam-macam informasi yang terbaru seperti olahraga, berita, belanja,

Bagian penting dalam penggunaan internet adalah *Internet Port Number* yang merupakan nomor tempat, saluran dan tujuan yang digunakan di dalam internet. *Service* pada internet diakses melalui *port-port* tertentu. Setiap *IP Address* dapat diaktifkan *port* dengan nomor 0 sampai 65535 yang didapat dari 2 pangkat 16 yang jumlahnya adalah 65536. *Port* ini bersifat logis, bukan fisik seperti halnya *serial port* atau *parallel port* pada komputer. Namun seperti juga *port* fisik, *port* ini digunakan untuk mengakses layanan tertentu pada internet. *Port* yang biasa digunakan tercantum dalam tabel 2.4 berikut ini.

Tabel 2.4
Nama *Port*

No.	Nama *Port*	Penjelasan
1.	*Port* 21 *FTP*	*File Transfer Protocol*
2.	*Port* 22 *SSH*	*Secure Shell*
3.	*Port* 23 *Telnet*	*Telecommunication Network*
4.	*Port* 25 *SMTP*	*Simple Mail Transfer Protocol*
5.	*Port* 80 *HTTP*	*Hypertext Transfer Protocol*
6.	*Port* 110 *POP3*	*Post Office Protocol, Version 3*
7.	*Port* 119 *NNTP*	*Network News Transfer Protocol*
8.	*Port* 139 *NBSS*	*NetBIOS session service*
9.	*Port* 143 *IMAP*	*Internet Message Access Protocol*
10.	*Port* 194 *IRC*	*Internet Relay Chat Protocol*

(Sumber: Ariyus, 2005: 160-162)

Untuk mengakses suatu layanan di internet, *port-port* di atas akan digunakan sesuai jenis layanan yang dipilih. Bila pengguna internet ingin *browsing* di internet, maka yang akan dipakai untuk mengaksesnya merupakan *port* 80 pada situs yang akan diakses. Bila pengguna internet akan mengambil *email*, maka digunakan *port* 110. Mengirim *email* menggunakan port 25. *Web email* menggunakan *port* 143. Membaca *newsgroup* lewat *ISP* akan menggunakan

---

permainan dan lain-lain yang dikemas dalam bentuk menu yang mudah dipilih. Kepopuleran internet juga membuat para penyedia jasa informasi ini menyediakan beragam alternatif dalam menghubungkan ke jaringan internet (Hartono, 2000: 342).

[16]Hubungan secara langsung ke internet dapat dilakukan dengan membuat jaringan *Local Area Network* (*LAN*) yang dihubungkan ke *internet host*. Selanjutnya komputer-komputer pemakai internet dihubungkan dengan *LAN* tersebut. Hubungan langsung ini biasanya dilakukan oleh perusahaan atau perguruan tinggi yang mempunyai banyak terminal untuk dapat mengakses ke jaringan internet. Untuk hubungan langsung, diperlukan alamat *IP* (*IPN address*) yang dapat diperoleh dan didaftarkan ke *Internet Network Information Center* (Hartono, 2000: 342).

port 119. *Chatting* menggunakan *port* 194, dan lain sebagainya. Pada umumnya hanya *port* 25, 110, dan 139 yang terbuka dengan asumsi pengguna komputer dengan Windows 9x/ME akan membuka *port* 139. Karena itulah *port* ini perlu mendapat perhatian khusus sebab dapat menjadi celah masuknya penyerang ke komputer Windows 9x/ME. Untuk menjaga agar komputer yang digunakan tidak terlalu resiko diserang oleh *hacker* dan *cracker* maka disarankan untuk tidak membuka *port-port* yang tidak diperlukan (Ariyus, 2005: 160-162).

2.2 *Cybercrime*

Cybercrime dapat diartikan sebagai kegiatan ilegal dengan perantara komputer dan dapat dilakukan melalui jaringan elektronik global. Perbedaannya dengan kejahatan pada umumnya dapat dilihat dari kemampuan serbaguna yang ditampilkan akibat perkembangan informasi dan teknologi komunikasi yang semakin canggih. Sebagai contoh, komunikasi melalui internet membuat pelaku kejahatan lebih mudah untuk beraksi melewati batas wilayah negara untuk melakukan kejahatannya tersebut (transnasional). Internet juga membuat kejahatan semakin terorganisir dengan menggunakan teknik yang semakin canggih untuk mendukung dan mengembangkan jaringan untuk perdagangan obat, pencucian uang, perdagangan senjata ilegal, penyeludupan dan lain-lain (Thomas dan Loader, 2000:3).

Menurut Mardjono Reksodiputro (1997: 10), kejahatan komputer bukan merupakan suatu hal yang baru di Indonesia. Sehubungan dengan kejahatan komputer, di Indonesia kasus yang berkaitan dengan kejahatan komputer adalah kasus penipuan melalui komputer di Bank Negara Indonesia (BNI) cabang New York pada tahun 1987 yang berjumlah 9,1 juta dollar Amerika. Kejahatan ini dilakukan oleh mantan pegawai BNI yang masih memiliki *user ID* dan *password*. *User ID* dan *password* itu digunakan untuk melakukan manipulasi terhadap komputer Bank. Kejahatan ini dilakukan dengan menggunakan komputer di suatu hotel di New York yang terkoneksi dengan komputer Bank yang juga berada di New York. Kemudian mentransfer dana tersebut ke beberapa rekening di Panama dan Swiss. Pelaku dihukum karena melakukan pencurian sebagaimana diatur

dalam pasal 363 KUHP. Kasus ini dilakukan dengan mempergunakan bantuan kecanggihan peralatan komputer. Sehingga berawal dari kasus ini mulai timbullah istilah kejahatan komputer atau dalam disertasi ini digunakan istilah *cybercrime*.

Pada bagian ini akan ditelaah lebih lanjut mengenai pengertian *cybercrime*, karakteristik *cybercrime* dan kategorisasinya.

2.2.1 Pengertian *Cybercrime*

Kongres Perkumpulan Bangsa-Bangsa (PBB) ke-10 mengenai Pencegahan Kejahatan dan Penanganan Pelaku Tindak Pidana, yang membahas isu mengenai kejahatan yang berhubungan dengan jaringan komputer, membagi *cybercrime* menjadi dua kategori yaitu *cybercrime* dalam arti sempit dan *cybercrime* dalam arti luas. *Cybercrime* dalam arti sempit (kejahatan komputer: *computer crime*) adalah setiap perilaku ilegal yang ditujukan dengan sengaja pada operasi elektronik yang menargetkan sistem keamanan komputer dan data yang diproses oleh sistem komputer tersebut. *Cybercrime* dalam arti luas (kejahatan yang berkaitan dengan komputer: *computer related crime*) adalah setiap perilaku ilegal yang dilakukan dengan maksud atau berhubungan dengan sistem komputer atau jaringan, termasuk kejahatan pemilikan, penawaran, atau distribusi dari komputer sistem atau jaringan. Tentu saja definisi ini sangat kompleks. Perbuatan yang dianggap illegal di suatu negara belum tentu dianggap ilegal di negara lain (Shinder, 2002: 17).

Sebagaimana telah disebutkan sebelumnya istilah *cybercrime* berbeda-beda ada yang menggunakan istilah kejahatan komputer, kejahatan mayantara dan lain-lain. Sedikitnya terdapat dua kelompok para ahli yang memberikan pendapat mengenai istilah ataupun definisi mengenai kejahatan komputer; kejahatan yang berkaitan erat dengan komputer; atau penyalahgunaan komputer. Ada yang memandang kejahatan komputer dalam arti sempit, yakni kejahatan yang perlu menggunakan keahlian khusus pada komputer atau jaringan. Ada pula yang mengartikan dalam arti luas yaitu semua kejahatan yang berhubungan dengan komputer.

2.2.1.1 Pengertian *Cybercrime* dalam Arti Luas

Ada beberapa pengertian kejahatan komputer oleh berbagai ahli sebagaimana dikutip dalam (Kartasudirja, 1999: 2-3). Menurut Comer, *cybercrime* adalah setiap perbuatan yang dilakukan dengan itikad buruk untuk tujuan keuangan yang melibatkan komputer. Menurut Mandel mendefinisikan pengertian *cybercrime* meliputi: penggunaan komputer untuk tujuan melaksanakan perbuatan penipuan, pencurian atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan; ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase dan pemerasan. Kemudian menurut Kaspersen, *cybercrime* adalah setiap perbuatan melawan hukum yang secara langsung mengganggu proses program komputer yang telah dirancang. Sedangkan Ulrich Sieber mendefinisikan kejahatan komputer menjadi: penipuan dengan memanipulasi komputer; mata-mata dengan komputer dan pembajakan perangkat lunak; sabotase komputer; pencurian data; memasuki *DP system*[17] tanpa otoritas dan *hacking*; dan komputer sebagai alat untuk melakukan kejahatan tradisional.

Menurut Kartasudirja (1999: 3), dalam pengertian luas, *cybercrime* adalah tindak pidana apa saja yang dapat dilakukan dengan memakai komputer (*hardware* dan *software*) sebagai sarana atau alat, komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

2.2.1.2 Pengertian *Cybercrime* dalam Arti Sempit

Para ahli yang menganut pandangan yang sempit memberikan pengertian atau definisi kejahatan komputer sebagai 'tindak pidana yang dilaksanakan dengan menggunakan teknologi canggih, tanpa penguasaan ilmu mana tindak pidana tidak mungkin dapat dilaksanakan' (*...any illegal act for which knowledge of computer technology is essential for its perpetration*) (Kartasudirja, 1999: 2). Pakar hukum komputer, Don Parker dan Nycum, memberikan pengertian kejahatan komputer dalam arti sempit yaitu setiap perbuatan hukum yang

---

[17] *Dual Processor System* (*DP System*) adalah sistem komputer yang memiliki 2 *chip* prosesor yang masing-masing berdiri sendiri, berbeda dengan *dual core system* yang memiliki 2 prosesor dalam satu *chip* (*http://www.pcmag.com/encyclopedia_term/0,2542,t=dual+ processor&i=55471,00.asp*, 12 Februari 2008).

menjadikan pengetahuan khusus mengenai teknologi komputer sangat penting untuk pelaksanaan, penyidikan dan penuntutan sebagaimana dikutip oleh Kartasudirja (1999: 3).

Menurut Kartasudirja, dalam pengertian sempit, *cybercrime* adalah tindak pidana yang dilakukan dengan menggunakan teknologi komputer yang canggih.

2.2.2 Karakteristik *Cybercrime*

Ada beberapa karakteristik yang membedakan *cybercrime* dengan tindak pidana konvensional. Karakteristik *cybercrime* dibandingkan tindak pidana lain menurut Nitibaskara (2000: 1) ada empat yaitu: Penggunaan Teknologi Informasi (TI) dalam modus operandi; Korban *cybercrime* dapat menimpa siapa saja mulai dari perseorangan sampai negara; *Cybercrime* bersifat *non violence* (tanpa kekerasan); Karena tidak kasat mata maka *fear of crime* (ketakutan atas kejahatan) tidak mudah timbul.

Cybercrime berbeda dengan kejahatan komputer lainnya. Hal ini dipengaruhi dengan adanya kecepatan *cyberspace* sehingga terjadi perubahan mendasar mengenai kejahatan ini. **Pertama,** karena kecanggihan *cyberspace,* kejahatan dapat dilakukan dengan cepat bahkan dalam hitungan detik. **Kedua,** karena *cyberspace* yang tidak terlihat secara fisik maka interaksi baik individu maupun kelompok terjadi sehingga pemikiran yang dianggap ilegal diluar dunia *cyber* dapat disebarkan ke masyarakat melalui dunia *cyber*. **Ketiga,** karena dunia *cyber* yang universal memberikan kebebasan bagi seseorang mempublikasikan idenya termasuk yang ilegal seperti muncul bentuk kejahatan baru seperti *cyberterrorism*. **Keempat,** karena *cyberspace* tidak dalam bentuk fisik maka konsep hukum yang digunakan menjadi kabur. Misalnya konsep batas wilayah negara dalam sistem penegakan hukum suatu negara menjadi berkurang karena keberadaan dunia *cyber* dimana setiap orang dapat berinteraksi dari berbagai tempat di dunia (Clifford, 2006: 7-8).

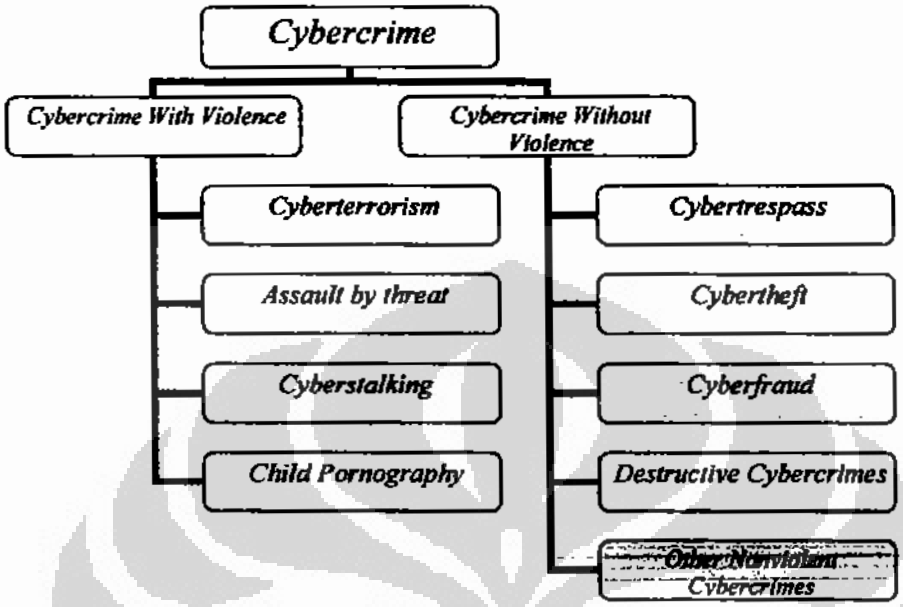
Keberadaan dunia *cyber*, sekarang ini menjadi urusan dunia internasional bukan urusan domestik suatu negara lagi. Karena pengaruh yang ditimbulkan dapat menimpa siapa saja, dimana saja dan kapan saja. Sebagai contoh yang dikemukakan Schmidt (2006: 123-124) adalah penyebaran virus "*I Love You*"

pada tahun 2000 yang meluas di luar perkiraan sebelumnya. Virus ini adalah salah satu virus pertama yang menjangkiti kurang lebih 45 juta sistem jaringan di dunia dan membuat kerugian sekitar 10 milyar dollar US. Setelah diselidiki, pelakunya adalah seorang mahasiswa suatu universitas komputer di Filipina yaitu Onel de Guzman yang beralasan itu semua dilakukan dalam rangka proyek penelitian kampus. Karena pada tahun tersebut Filipina belum ada aturan yang mengatur tentang *hacking* maka aparat penegak hukum membatalkan semua tuduhan terhadapnya (Schmidt, 2006; 123-124). Hal ini menandakan bahwa *cybercrime* bersifat global dalam artian akibat yang ditimbulkan tidak terbatas dalam satu wilayah suatu negara saja.

2.2.3 Kategorisasi *Cybercrime*

Untuk lebih mempermudah pembahasan mengenai *cybercrime*, kita mengikuti kategorisasi menurut Shinder (2002: 19) yang membagi *cybercrime* menjadi dua kategori. Kategori pertama adalah kejahatan dengan kekerasan atau secara potensial mengandung kekerasan seperti: *cyberterrorism*, *assault by threat*, *cyberstalking*, dan *child pornography*. Sedangkan kategori kedua adalah kejahatan komputer tanpa kekerasan yang meliputi *cybertrespass*, *joycomputing*, *cyber infringements of privacy*, *cybertheft*, *cyberfraud*, *destructive cybercrimes*, dan *other nonviolent cybercrimes*

Bagan 2.1
Kategorisasi *Cybercrime*



(Sumber: Shinder. 2002: 19)

2.2.3.1 Kategori *Cybercrime* yang Mengandung Kekerasan (*Cybercrime With Violence*)

Kategori ini membawa kejahatan komputer sebagai sesuatu yang dapat menciptakan korban kekerasan baik itu masyarakat, kelompok masyarakat, keluarga, individu maupun anak-anak. Shinder (2002: 19-21) mengelompokkan dalam 4 kategori yaitu *cyberterrorism, assault by threat, cyberstalking,* dan *child pornography.*

a. Terorisme internet (*Cyberterrorism*)

Pemerintah Amerika Serikat mendefinisikan terorisme sebagai perancang kekerasan berlandasan politik yang melakukan kejahatan dengan target orang tak bersenjata yang dilakukan oleh agen tersembunyi dan kelompok subnasional. *Cyberterrorism* mengacu pada teror yang dilakukan, direncanakan dan dikoordinasikan melalui *cyberspace* yaitu melalui jaringan komputer.

Kelompok teroris juga menikmati kemajuan teknologi untuk agenda

politiknya dengan cara menggunakan *email* atau *website,* serta jaringan komputer sampai pada titik ekstrim seperti sabotase sistem komputer untuk kontrol lalu-lintas udara yang dapat mengakibatkan pesawat udara bertabrakan; penyusupan dalam sistem komputer penanganan air dan meracuni persediaan air; *hacking* ke dalam *database* komputer rumah sakit dan mengubah atau menghapus informasi yang dapat mengakibatkan perawatan yang salah dan berbahaya bagi pasien; menganggu pasokan listrik yang penting bagi alat pemanas di musim dingin atau alat pendingin di musim panas sehingga dapat mengakibatkan kematian karena suhu udara.

Teroris dapat juga disebut sebagai sekelompok orang atau individu yang bertindak atas dasar sentimen pada suatu kelompok atau pihak tertentu, dan melakukan berbagai aktivitas yang bertujuan untuk menunjukkan eksistensi mereka pada lingkungan dunia. Tingkatan kemampuan yang dimiliki kelompok ini adalah yang tertinggi karena menggabungkan berbagai sumber daya yang ada, level kemampuan, bahkan menggunakan sarana prasarana bantuan dari pihak sponsor yang membantu seperti satelit komunikasi.

Satu contoh pemanfaatan internet oleh teroris adalah kasus penyerangan teroris terhadap tentara Inggris. Penyerangan ini menyebabkan sejumlah tentara Inggris tewas pada awal tahun 2007. Fakta yang mengejutkan dalam kasus ini adalah bukti yang diperoleh intelijen Inggris bahwa teroris menggunakan layanan *Google Earth* untuk mengetahui lokasi dan target penyerangan berupa foto yang dicetak dari *Google Earth*. Adanya layanan ini dalam dunia internet memudahkan pengguna internet untuk melihat lokasi suatu wilayah di permukaan bumi secara lebih detil. Teroris disinyalir telah menggunakan situs khusus dalam perjuangannya dengan memberikan informasi seperti bagaimana melakukan teror, melakukan rekruitmen anggota militan untuk menjadi pelaku bom bunuh diri, bagaimana cara merakit bom berdaya ledak tinggi. Penyebaran informasi untuk kalangan terbatas/*non-public* atau lebih dikenal dengan istilah *narrowcasting* melalui situs internet dilakukan oleh para teroris sebagai salah satu cara penyebaran ideologi (Kompas, 23 November 2007: 45).

Di Indonesia sendiri, salah satu kasus *cyberterrorism* yang mencuat adalah kasus situs *www.anshar.net.* Situs *www.anshar.net* adalah situs yang digunakan

oleh kelompok teroris Noordin M. Top untuk menyebarluaskan paham terorisme. Di dalamnya berisi cara-cara melakukan teror seperti cara melakukan pengeboman, menentukan lokasi teror, jenis-jenis bahan-bahan peledak dan senjata. Selain itu situs ini juga menyebarkan orasi Noordin M. Top serta adegan pelaku bom bunuh diri. Tersangka pelaku pembuat situs ini adalah mahasiswa Fakultas Teknik Universitas Semarang Agung Prabowo (24) yang memakai nama *cyber* Max Fiderman dan Agung Setyadi (30), dosen Fakultas Teknik Informasi Stikubank Semarang. Kasus ini ditangani oleh Unit V *IT & Cybercrime* Direktorat II Bareskrim Polri.

Gambar 2.2
Kasus *cyberterrorism* situs www.anshar.net

(Sumber: Unit V *IT & Cybercrime* Direktorat II Bareskrim Polri)

Gambar 2.3
Pihak-pihak yang terlibat dalam pembuatan *website*

(Sumber: Unit V *IT & Cybercrime* Direktorat II Bareskrim Polri)

b. Serangan dengan ancaman (*assault by threat*)

Assault by threat dilakukan dengan *email*, dimana pelaku membuat orang takut dengan cara mengancam target atau orang yang dicintai target. Hal ini juga termasuk ancaman bom yang di *email* kepada perusahaan atau institusi pemerintah. Contoh kasus ini adalah kasus ancaman terhadap Sekolah *Falls Church* di Amerika Serikat oleh seorang warga Indonesia bernama Emelia Karolina (EK). *Email* itu ditujukan kepada Kathryn Hopkins yang bekerja di sekolah tersebut. Wanita berkewarganegaraan Amerika Serikat itu adalah calon istri mantan kekasih EK, Dewa Putu Dirga. "Apabila anda tidak mengirim tunangan anda kembali ke Indonesia sebelum tanggal 31 Januari 2005 saya akan meletakkan beberapa bom dan bahan peledak lainnya di *Falls Church City Public School* terutama di George Mason High School." Begitulah bunyi salah satu *email* yang dikirimkan oleh tersangka EK melalui *faksimile* dan *email* dengan *user name* Sri Kusumaningsih (*srikusumaningsih@hotmail.com*) dan Abdul Azis (*ulomemeilovemeyoukillme@yahoo.com*) pada tanggal 16 Desember 2004. Hal ini dilakukan karena kecemburuan EK terhadap Kathryn yang menjadi kekasih Dewa. Emosi yang tak terbendung membuat EK menebar teror kepada mantan kekasihnya. Dewa Putu Dirga dan Kathryn Hopkins, dimulai pada bulan

Desember 2004 hingga Januari 2005. Kasus ini ditangani oleh dua lembaga kepolisian yang saling bekerja sama yaitu Polda Metro Jaya yang dipimpin AKBP Petrus Reinhard Golose, Kepolisian Falls Church dan *Secret Service* (*http://www.fallschurchva.gov*, 5 Maret 2005).

c. Penguntitan di internet (*Cyberstalking*)

Dari pelecehan seksual melalui internet yang menciptakan ketidaknyamanan dapat berkembang menjadi ancaman fisik dan menciptakan trauma mendalam pada diri korban. Ancaman tersebut dapat meningkat menjadi penguntitan di dunia nyata dan perilaku kekerasan. Dalam suatu kasus *cyberstalking* di Amerika yang dipublikasikan surat kabar Los Angeles Times 22-23 Januari 1999, yaitu korban seorang gadis yang "tersiksa" sehingga mengalami trauma berkepanjangan. Selain kondisi kesehatannya yang menurun drastis, dia kehilangan pekerjaan dan takut untuk keluar dari rumah. Hal ini bermula dari pertemuan korban dengan pelaku *cyberstalking* yaitu seorang satpam berusia kurang lebih 50 tahun di suatu gereja. Dalam pertemuan itu diketahui bahwa pelaku ternyata menyukai korban dan berusaha melakukan pendekatan namun korban menolak cinta pelaku. Pelaku marah dan tersinggung kemudian untuk mengobati rasa sakit hatinya, dia mem-*posting* identitas pribadi korban seperti penampilan fisik, alamat dan nomor telepon ke internet bahkan dia memberitahu bagaimana cara untuk menerobos sistem keamanan *web* milik korban. Bahkan dia menambahkan informasi bahwa korban adalah "perempuan mesum" dan mem-*posting*nya ke dalam suatu media *online*. Alhasil, kurang lebih 500 *user* mengakses *web* korban dan meninggalkan pesan yang menjijikkan bahkan setiap malam korban mendapat telepon dari berbagai lelaki yang tidak dikenal dan hal ini sangat menyiksa korban (Barua, Yogesh dan Denzyl P. Dayal., 2001: 153).

d. Pornografi anak (*child pornography*)

Pornografi anak pada umumnya dikelompokkan sebagai kejahatan dengan kekerasan, walaupun beberapa pihak yang terlibat tidak melakukan kontak fisik dengan anak-anak yang menjadi objek kejahatan ini. Ini adalah suatu kejahatan karena kekerasan seksual secara fisik terhadap anak-anak dilakukan untuk menghasilkan materi pornografi dan karena orang-orang yang tertarik melihat

materi-materi ini seringkali tidak cukup membatasi ketertarikan mereka pada gambar-gambar dan khayalan saja akan tetapi juga melakukannya secara nyata seperti pedofilia (Shinder, 2002: 21).

2.2.3.2 Kategori *Cybercrime* yang Tidak Mengandung Kekerasan (*Cybercrime Without Violence*)

Kejahatan komputer dalam kategori ini terfokus pada kegiatan yang tidak menimbulkan kekerasan fisik. Beberapa di antaranya berakibat di *cyberspace* dan lainnya juga berakibat langsung di dunia nyata.

a. Cybertrespass

Pelaku kejahatan memasuki jaringan komputer tanpa adanya otorisasi atau wewenang tetapi tidak menyalahgunakan atau merusak data di jaringan komputer tersebut. Pelaku *cybertrespass* (*cybertrespasser*) senang mengintip dan membaca *email* pribadi dan dokumen orang lain. Pelaku gemar mengamati program yang ada di sistem komputer orang lain dan *website* yang dikunjungi orang lain. Walaupun tidak dapat dibuktikan adanya kerusakan atau kerugian, pelaku *cybertrespass* dapat dikenakan tindak pidana karena telah memasuki suatu sistem komputer tanpa izin pemilik.

Joycomputing adalah seseorang yang menggunakan komputer secara tidak sah/tanpa izin, dan mempergunakannya melampaui wewenang yang diberikan. Istilah *joycomputing* ini merupakan pendapat dari N.Keyzer dalam ceramahnya tentang Hukum Pidana Belanda dan Penyalahgunaan Komputer, di BPHN Jakarta. Maksud *joycomputing* adalah seseorang yang menggunakan komputer secara tidak sah/tanpa izin dan melampaui wewenang yang diberikan. Istilah *joycomputing* mengingatkan orang kepada istilah *joyriding* yaitu memakai mobil orang lain tanpa izin untuk bersenang-senang setelah itu mobil tersebut dikembalikan lagi. Jadi yang dimaksud dengan *joycomputing* disini adalah perbuatan seseorang memanfaatkan waktu penggunaan komputer (mencuri waktu penggunaan atau pelayanan komputer) secara tidak sah untuk kepentingan pribadi atau kelompoknya pada saat dinas. Misalnya, seorang pegawai suatu perusahaan tanpa izin dari atasannya telah mempergunakan komputer (yang menjadi salah satu tugasnya) dengan tujuan memprogram permasalahan untuk kepentingan

pribadi diluar tugas-tugas yang telah ditetapkan oleh atasannya (Wisnubroto, 1999: 33-34).

Cyber Infringements of Privacy. Selain memasuki tanpa izin, kejahatan komputer biasa ditujukan terhadap informasi pribadi seseorang yang tersimpan pada formulir data pribadi secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor *Personal Identification Number* (PIN) *Automatic Teller Machine* (ATM), cacat atau penyakit tersembunyi dan sebagainya (Golose, 2006: 10). Kejahatan semacam ini dalam dunia perbankan dikenal dengan istilah "*typo site*"[18]. Dimana pelaku kejahatan membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika ada seorang korban salah mengetikkan alamat dan tersesat di situs palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi *user ID* dan *password* korbannya, dan dapat dimanfaatkan untuk merugikan korban (Ginting, 10 Agustus 2006: 2).

Ada beberapa istilah yang termasuk *Cyber Infringements of Privacy* dalam buku "Hukum Internet: Pengenalan Mengenai Masalah Hukum di *Cyberspace*[19]", (Sitompul: 2001, 25-26) yaitu *Junk Mail*[20] dan *Cookies*[21].

---

[18]Salah satu contoh kasus *typo site*. Dunia perbankan melalui internet (*e-banking*) Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto (dikutip dari *CyberTECH*, 6 November 2002 dengan judul "Steven Haryanto"), seorang *hacker* dan jurnalis pada majalah Master *Web*. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan internet banking Bank Central Asia (BCA). Steven membeli *domain-domain* dengan nama mirip *www.klikbca.com* (situs asli internet banking BCA), yaitu *www.klikbca.com, kilkbca.com, clikbca.com, klickca.com. dan klikbac.com.* Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya *security* untuk bertransaksi dan adanya formulir akses (*login form*) palsu. Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (*user id*) dan nomor identitas pribadi (*PIN*) dapat di ketahuinya. Diperkirakan, 130 nasabah BCA tercuri data-datanya. Menurut pengakuan Steven pada situs bagi para *webmaster* di Indonesia, *www.webmaster.or.id*, tujuan membuat situs plesetan adalah agar publik menjadi lebih berhati-hati dan tidak ceroboh saat melakukan pengetikan alamat situs (*typo site*), bukan untuk mengeruk keuntungan (Golose, 10 Agustus 2006: 3-4).

[19]*Cyberspace* adalah lokasi yang berbentuk struktur data yang diciptakan oleh teknologi komputer yang canggih, yang mencakup antara lain grafik, suara dan lain-lain (Thro, 1991: 72).

[20]*Junk Mail* salah satu kejahatan komputer adalah masalah privasi di internet terutama apabila seseorang melakukan transaksi lewat internet, baik itu membeli, mendaftar di suatu organisasi, menjadi anggota suatu *mailinglist* atau *newsgroup*, maka pengguna internet tersebut diharuskan mengirim data pribadi secara singkat. Yang menjadi masalah adalah, tidak lama setelah ia melakukan transaksi tersebut, maka ia akan segera menerima berbagai *"junk-mail"*, yang

b. *Cybertheft*

Menurut Shinder (2002: 24), *cybertheft* adalah pencurian yang dilakukan dengan komputer atau jaringan untuk mencuri informasi, uang, dan barang berharga lainnya karena hal tersebut adalah motivasi terbesar seseorang melakukan kejahatan. Selain itu, keahlian dalam melakukan pencurian jarak jauh akan mengurangi resiko seorang pencuri terlacak atau tertangkap. Ada beberapa kegiatan yang dikategorikan sebagai *cybertheft*, antara lain: *embezzlement*[22], *unlawful appropriation*[23], *corporate/industrial espionage*[24], *plagiarism*[25],

---

bermacam-masam isinya, mulai dari undian sampai kepada penawaran berbagai barang kebutuhan sehari-hari. Hal tersebut menyangkut privasi dari pengguna internet karena bagaimanapun juga masuknya *email* dalam jumlah yang besar akan mengganggu pengguna internet, karena *email* tersebut akan bercampur dengan *email* yang penting bagi pemilik *email* (Sitompul, 2001: 25).

[21] *Cookies* juga merupakan masalah privasi lainnya. Pengguna internet mengeluh dengan adanya program *"cookies"* yang masuk ke komputer begitu pengguna internet menggunakan salah satu program internet, dimana *cookies* ini akan dapat menelusuri kegiatan pengguna internet seperti situs-situs yang dikunjunginya, berapa lama ia mengakses situs tersebut, dan berbagai data kegiatan lainnya. Di Indonesia memang masalah privasi belum merupakan masalah yang sangat berarti bagi sebagian besar masyarakat, namun bukan berarti tidak penting dan dapat diabaikan. Masalah privasi merupakan hak bagi setiap orang, dalam arti seseorang tidak boleh dengan leluasa masuk ke dalam wilayah privasi orang lain. Masuknya program *cookies* ke dalam komputer pengguna internet menurut sebagian pengguna internet di Amerika Serikat merupakan pelanggaran hak privasi mereka, namun belum sampai ke tingkat penuntutan ke pengadilan. Meskipun demikian, sudah banyak pengguna internet yang mengajukan protes mengenai hal tersebut lewat organisasi-organisasi pendukung privasi (Sitompul, 2001: 25).

[22] *Embezzlement* adalah pengelapan uang atau properti yang dipercayakan orang lain kepada pelaku. Melalui komputer, karyawan dapat memanipulasi data mengenai penjualan, persediaan, atau kualitas dari barang atau aset milik perusahaan tersebut. Perusahaan dapat memperkirakan barang-barang yang datanya telah dimanipulasi telah terjual atau tidak layak pakai sehingga perlu dimusnahkan/dibuang. Pelaku mendapat keuntungan dari mengambil barang tersebut dan mengalihkannya atau menjualnya ke tempat atau pihak lain (Shinder, 2002: 24).

[23] *Unlawful Appropriation.* Berbeda dengan penggelapan, pada kejadian ini, pelaku tidak mendapat kepercayaan terhadap barang berharga tersebut. Pelaku memperoleh akses dari luar organisasi dan mentransfer dana, serta merubah dokumen sehingga pelaku berhak atas properti yang sebenarnya tidak ia miiiki (Shinder, 2002: 24).

[24] *Corporate/Industrial Esplonage*. Hal ini dilakukan baik orang luar maupun orang dalam perusahaan yang menggunakan jaringan komputer untuk mencuri atau mensabotase rahasia dagang seperti resep minuman, data keuangan, daftar rahasia klien, strategi pemasaran atau informasi lain dari pelaku usaha saingannya yang digunakan untuk meroperoleh keuntungan (Shinder, 2002: 24).

[25] *Plagiarism* (plagiat) dilakukan dalam bentuk pencurian hasil kerja orang lain dan mengakuinya sebagai jerih payahnya sendiri (Shinder, 2002: 24).

piracy[26], *identity theft*[27], *sniffing*[28], *Domain Name Service* (*DNS*) *cache poisoning*[29] (Shinder, 2002: 24). Sedangkan kegiatan yang termasuk *cybertheft* menurut Puslitbang Hukum dan Pengadilan Mahkamah Agung RI (2004: 21-31) adalah *data diddling*[30], *electronic piggybacking*[31], teknik salami[32],

---

[26]*Piracy* (pembajakan) meliputi kegiatan meng-*copy* secara tidak sah dari perangkat lunak, film, musik, seni, buku dan sebagainya yang dilindungi dengan hak cipta, sehingga menghasilkan kerugian pendapatan dari pemegang hak cipta tersebut. Tindak pidana terhadap hak atas kekayaan intelektual (*offense againts intelectual property*) ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Contoh tindak pidana ini antara lain: peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya (Shinder, 2002: 24).

[27]*Identity Theft* adalah tindakan pelaku menggunakan komputer untuk mendapatkan data pribadi korban seperti nomor jaminan sosial, nomor Surat Izin Mengemudi (SIM) untuk dapat melakukan kejahatan dengan identitas tersebut atau mengambil uang atau properti atau menggunakan kartu kredit atau kartu debet atau rekening bank milik korban (Shinder, 2002: 24).

[28]*Sniffing* adalah upaya untuk mendapatkan *user ID* dan *password* dengan jalan mengamati paket data yang melalui suatu jaringan komputer (Ginting, 10 Agustus 2006: 2).

[29]*DNS cache poisoning* dilakukan dengan cara pelaku melakukan pencegatan secara ilegal untuk menyusup memasuki isi dari *DNS cache* komputer untuk mengubah arah transmisi jaringan ke *server* pelaku. Yang diambil di sini tidak harus uang tapi bisa juga berupa informasi perusahaan (Shinder, 2002: 24).

[30]*Data diddling* menurut Parker (1986: 71) adalah perubahan data sebelum, pada saat pemasukan data atau informasi (*input*), atau pada saat pengeluaran (*output*) dalam pengoperasian komputer. Istilah inipun merupakan pendapat dari Jusuf Rendy dalam bukunya *Proteksi terhadap Kriminalitas Dalam Bidang Komputer*. *Data diddling* adalah suatu perbuatan yang mengubah data yang sah dengan cara yang tidak sah, yaitu dengan mengubah *input* atau *output* data. Yang dimaksud dengan mengubah data disini adalah perbuatan sedemikian rupa yang mengakibatkan isinya menjadi berubah dari isi yang asli, atau sehingga data tersebut menjadi berbeda dari yang asli. Data itu tidak senantiasa diganti dengan yang lain, dapat pula perubahan dilakukan dengan cara mengurangkan, menambah, atau mengubah sesuatu dari data tersebut. Misal: seorang pegawai *computer operation* pada suatu universitas membantu seorang mahasiswa di universitas tempat ia bekerja agar mahasiswa tersebut mencapai prestasi tertentu dimana mahasiswa itu adalah saudaranya. Caranya adalah dengan merubah prestasi akademis yang ada dalam komputer universitas tersebut kemudian menaikkan nilai-nilai mahasiswa tersebut atau menambah kredit (SKS) dari yang sebenarnya atau mengubah pernyataan "tidak lulus" menjadi pernyataan sebaliknya (Wisnubroto, 1999: 37).

[31]*Electronic piggybacking* dilakukan dengan menyembunyikan terminal atau alat penghubung ke dalam sistem komputer secara diam-diam. Melalui terminal tersebut, data komputer dapat dipelajari dan ditransfer untuk kemudian dicuri apabila komputer sedang tidak digunakan. Semakin banyak komputer dihubungkan kepada *central terminal*, semakin besar kemungkinan seseorang untuk dapat menyadap komputer tanpa diketahui orang lain (Puslitbang Hukum dan Pengadilan MA RI, 2004: 23).

[32]Teknik Salami (*Salami Techique*) merupakan penggelapan yang dilakukan dengan mengambil uang dalam jumlah yang tidak terlalu banyak seperti mengambil uang nasabah berbentuk pecahan yang disimpan pada suatu bank. Nasabah dengan jumlah simpanan besar biasanya tidak menyadari uangnya berkurang. Uang yang telah dikumpulkan tersebut dimasukkan ke dalam pembukuan fiktif yang dapat diambil sewaktu-waktu. Tindak kejahatan tersebut lebih

penyalahgunaan kartu debet[33] dan kartu kredit[34], dan *data leakage*[35].

c. Penipuan di internet (*Cyberfraud*)

Shinder (2002: 25), menyatakan bahwa penipuan melibatkan pemberian infomasi yang tidak benar untuk mendapatkan sesuatu yang berharga atau menguntungkan. Korban mengetahui dan secara sukarela memberikan uang atau barang berharga ke pelaku tetapi berdasarkan informasi yang salah atau tidak benar. *E-commerce* tidak sedikit membuka peluang bagi terjadinya tindak pidana penipuan. Contoh kasus *cyberfraud* sebagaimana dikemukakan oleh Golose (2006: 3) yaitu kasus penipuan yang dilakukan oleh sekelompok pemuda di Medan yang memasang iklan di salah satu *website* terkenal "Yahoo!". Iklan itu seolah-olah menjual mobil mewah *Ferrari* dan *Lamborghini* dengan harga murah sehingga menarik minat seorang pembeli dari Kuwait. Perbuatan tersebut dapat dilakukan tanpa adanya hubungan terlebih dahulu antara penjual dan pembeli, padahal biasanya untuk kasus penipuan terdapat hubungan antara korban atau tersangka.

d. *Destructive Cybercrimes*

Termasuk dalam kegiatan ini adalah semua kegiatan yang mengganggu jaringan pelayanan. Data dirusak atau dihancurkan bukan dicuri atau

---

cepat dilakukan melalui sistem komputer yang tidak memiliki sistem keamanan yang ketat dibandingkan dengan sistem manual (Puslitbang Hukum dan Pengadilan MA RI, 2004: 21).

[33]Penyalahgunaan kartu debet (*cash card*) dilakukan dengan mengambil uang dari mesin pembayar otomatis seperti *cash dispenser* atau *ATM* melebihi dana yang ada atau dananya sudah tidak ada; dengan menggunakan kata sandi (*Password*/PIN) yang sah (Puslitbang Hukum dan Pengadilan MA RI, 2004: 26).

[34]Penyalahgunaan kartu kredit (*credit card*), berdasarkan Pasal 301.1 Hukum Pidana Kanada, meliputi mencuri atau memalsukan kartu kredit; memiliki, menggunakan atau melakukan transaksi apapun dengan menggunakan kartu kredit yang diperoleh secara melawan hukum atau; menggunakan sebuah kartu kredit yang telah dicabut atau dibatalkan (Puslitbang Hukum dan Pengadilan MA RI, 2004: 31).

[35]*Data leakage* atau kebocoran data adalah suatu pembocoran data rahasia yang dilakukan dengan cara menulis data rahasia tersebut ke dalam kode–kode tertentu sehingga data dapat dibawa ke luar tanpa diketahui oleh pihak yang berwenang. Pembocoran dapat terjadi dalam bentuk kebocoran data rahasia negara, kebocoran rahasia perusahaan, dan lain sebagainya. Masalah kebocoran data ini dapat pula menyangkut pihak– pihak (orang pribadi) yang telah dipercaya penuh atau telah diberi kepercayaan penuh oleh pihak pemakai jasa orang tersebut untuk menyimpan data atau keterangan yang bersifat rahasia serta diwajibkan untuk mengamankan dari pihak–pihak yang tidak bertanggung jawab (Wisnubroto, 1999: 35).

disalahgunakan. Beberapa bentuk kejahatan ini antara lain: *hacking* ke dalam jaringan dan menghapus data atau *program files*, *hacking* ke dalam suatu *web server* dan melakukan perusakan pada *web page* (Shinder, 2002: 26). Dalam dunia perbankan, tindakan ini dinamakan *Denial of Service (DoS). Denial of Service* dilakukan dengan mengirimkan data dalam jumlah sangat besar dengan maksud untuk melumpuhkan atau merusak sistem sasaran (Ginting, 10 Agustus 2006: 3). Setelah memasuki suatu sistem, *hacker* dapat melakukan hal apa saja yang diinginkan misalnya menyebarkan *virus*[36], *worm*[37] dan *trojan horse*[38].

Contoh kasus d*estructive cybercrimes* adalah kasus *hacking website* partai Golkar (*www.golkar.or.id*) yang dilakukan oleh Iqra Syafaat pada awal Juli 2006. Hal yang dilakukan adalah mengganti foto tokoh Golkar di *website* tersebut yaitu foto Yusuf Kalla dengan gambar gorila serta semboyan partai Golkar "Bersatu untuk Maju" diganti dengan kata "Bersatu untuk Malu".

---

[36]Virus yaitu program yang dapat menyebabkan hal-hal yang tidak inginkan atau bahkan merusak ketika dijalankan tanpa sepengetahuan pemilik komputer. Virus dapat menggandakan dirinya dan menyebar ke sistem lain dengan masuk ke dalam disket yang digunakan ke dalam suatu komputer atau melalui jaringan. Virus seringkali berpindah melalui *email* atau dalam dokumen pengolahan kata. Beberapa jenis virus aktif secara otomatis atau ketika terjadinya instalasi suatu program dan ada jenis virus lain yang menunggu untuk aktif sampai tanggal atau waktu tertentu atau harus dipicu oleh suatu sistem tertentu dalam komputer tersebut (Shinder, 2002: 337).

[37]*Worm* yaitu program yang dapat berpindah melalui jaringan dari komputer yang satu ke komputer yang lain. *Worm* dapat menggandakan dirinya dan meyebar melalui suatu jaringan. Perbedaan antara virus dan *worm* masih belum jelas. Pada dasarnya istilah *worm* digunakan untuk menggambarkan kode yang menyerang sistem jaringan sedangkan virus menggambarkan progam yang menggandakan dirinya dalam suatu komputer. Tujuan utama *worm* adalah menggandakan diri. Pada mulanya digunakan untuk mengerjakan tujuan tertentu dalam manajemen jaringan namun kemampuan mereka menggandakan diri disalahgunakan oleh *hacker* yang menciptakan *worm* berbahaya yang dapat menyebar luas dan juga dapat mengeksploitasi kelemahan sistem operasi dan melakukan perusakan (Shinder, 2002: 338).

[38]Bisa juga perusakan dilakukan dengan memasukkan program yang tidak berbahaya dan sah tetapi di dalamnya terdapat kode jahat (*maliclous code)* tersembunyi yang disebut *trojan horse. Trojan horse* merupakan pintu masuk dari virus dan *worm* ke komputer atau jaringan komputer. *Trojan horse* dapat menambah, mengurangi, atau mengubah data atau instruksi pada sebuah program sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melaksanakan tugas lain yang tidak sah. *Trojan hourse* juga dapat membuat data atau instruksi pada sebuah program menjadi tidak terjangkau sehingga data atau instruksi pada itu dapat hilang untuk memenuhi kepentingan pribadi/kelompok. Sebagai contoh: *programmer* suatu bank telah mengubah program sehingga perhitungan bunga nasabah bank tersebut akan dikurangi beberapa sen untuk dimasukkan ke dalam rekening bank milik programmer tersebut. Para korban biasanya tidak menyadari kecurangan yang dilakukan *programmer* tersebut. Biasanya para nasabah selalu kesulitan dalam menghitung bunga uangnya, apalagi hasil perhitungannya selisih beberapa sen saja, mereka biasanya tidak perduli (Hamzah dan Marsita, 1990: 40).

e. Kejahatan komputer non-kekerasan lainnya (*Other Nonviolent Cybercrimes*)

Ada beberapa kejahatan komputer non-kekerasan lain yang menggunakan komputer untuk melakukan aksinya walaupun tindakan kejahatan tersebut telah ada sejak lama. Yang termasuk dalam kejahatan komputer non-kekerasan lainnya adalah iklan internet prostitusi (*Cyber Prostitute Ads*)[39], Perjudian di internet (*Cybergambling*)[40], Penjualan obat dan narkotika di internet (*cyber drugs sales*)[41],

---

[39]Iklan internet prostitusi (*Cyber Prostitute Ads*). Internet kini dipergunakan sebagai media untuk menawarkan atau mengiklankan jasa Pekerja Seks Komersial (PSK). Modus baru kejahatan internet ini terbongkar ketika satuan reserse *cybercrime* Polda Metro Jaya menangkap Ramdoni alias Rino dan Yanti Sari alias Bela di sebuah hotel di bilangan Jakarta Selatan, Mei lalu. Dalam menjalankan kejahatannya, para PSK dengan berbagai kelengkapan data diri termasuk tarif, ukuran vital dan nomor telepon yang dapat dihubungi, ditawarkan melalui situs *poskota.net*. Sepintas, situs ini hanya berisi jual beli barang, konsultasi paranormal, serta panti pijat. Namun, pada direktori tersembunyi, seperti diiklankan lewat media cetak, dapat ditemui sekitar 30-an foto perempuan. Jika ada yang berminat dan cocok dengan harga penawaran yang berkisar antara 1-4 juta per tiga jam, telepon pemesanan pun sudah tercantum dalam situs ini. Transaksi dilakukan ketika lelaki hidung belang bertemu dengan PSK di tempat yang telah ditentukan (*http://www.sinarharapan.co.id/berita/0306/14/opi01.html*, 14 Juni 2003).

[40]Perjudian di internet (*Cybergambling*). Ada beberapa kegiatan yang dilarang oleh hukum untuk dilakukan di suatu wilayah tertentu menjadi dapat dilakukan dengan mudah di dunia *cyber*. Salah satu kegiatan tersebut adalah judi melalui internet (*internet gambling*) seperti yang dapat ditemui pada *http://www.gambling-forum.com/* atau *http://www.gonegambling.com/*. Fasilitas yang diberikan dapat beragam seperti taruhan pada acara olahraga atau juga judi layaknya dalam kasino seperti: *blackjack, video poker, virtual three reel slot machines, craps, roulette, baccarat, kenc, pai gow poker*, dan *caribbean stud*. Di internet juga terdapat lotere dan *bingo*, atau *off track betting* seperti taruhan pada pacuan kuda atau anjing. Pembayaran dapat dilakukan dengan kartu kredit, pulsa telepon atau pengiriman deposit uang terlebih dahulu (*http://www.gamblingandthelaw.com*). Pengungkapan kejahatan ini masih sangat kecil sekali karena banyak kendala dan hambatan yang dihadapi dalam upaya pengungkapannya. Saat ini, bagi mereka yang senang akan perjudian dapat juga melakukan judi dari rumah atau kantor hanya dengan mengakses situs *www.indobetonline.com* atau *www.tebaknomor.com* dan banyak lagi situs sejenis yang menyediakan fasilitas tersebut. Mereka dapat memanfaatkan fasilitas *internet banking* untuk pembayarannya.

[41]Penjualan obat dan narkotika di internet (*cyber drugs sales*). Internet kini menggantikan pojok-pojok jalan untuk mengedarkan narkotika dengan adanya *cyber drugs sales* (penjualan obat dan narkotika di internet). Toko obat berbasis internet sedang menjadi jalur baru transaksi ilegal perdagangan obat. Munculnya toko obat berbasis internet telah memudahkan dan memperluas sistem pelayanan medis dan obat-obatan, namun bersamaan dengan itu juga memberikan kemudahan bagi peredaran jenis obat yang dikontrol dan obat ilegal. Karena penjualan obat melalui toko obat berbasis internet, membuat kita tidak perlu menunjukkan resep obat yang berlaku untuk mendapatkan obat yang kita perlukan. Perdagangan internasional obat-obat terlarang melalui internet meningkat tajam menurut Badan Pengawasan Narkotika PBB (*INCB*). Lembaga tersebut menyatakan bahwa obat-obat berbahaya dijual tanpa resep dokter di internet, sehingga sulit diawasi. Dalam laporan tahunannya, lembaga itu menyatakan bahwa 90% penjualan obat-obatan yang mengandung narkotika seperti morfin untuk meredakan sakit seseorang di internet berlangsung tanpa adanya resep dokter. Laporan itu juga menyatakan bahwa para pemasok legal ikut memarakkan perdagangan ini dengan menyediakan obat-obatan kepada toko

pencucian uang di internet (*Cyber Laundering*)[42], *cybercontraband*[43].

2.2.4 Pengaturan *Cybercrime*

Para ahli masih berbeda pendapat mengenai pengaturan tindak pidana di bidang komputer terlebih lagi mengenai *hacking* sebagai bagian dari kejahatan komputer. Pada kenyataannya bila menerapkan tindak pidana konvensional pada kasus *hacking* maka diperlukan interpretasi terhadap ketentuan tindak pidana untuk tindakan tersebut. Selama ini ketentuan tindak pidana yang diterapkan dapat diambil dari Kitab Undang-undang Hukum Pidana (**KUHP**), dan di luar KUHP yaitu Undang-undang (**UU**). Ada pula Rancangan Undang-undang (**RUU**) yang sedang dalam pembahasan di negara kita atau aturan hukum di negara lain mengenai *hacking* yang layak dijadikan telaah perbandingan.

---

obat internet tanpa ijin. *INCB* memperingatkan, situs internet semakin menjadi sumber obat-obat terlarang bagi anak-anak dengan menawarkan akses yang tidak terbatas oleh usia."Penjualan gelap di internet sudah dipastikan sebagai salah satu sumber utama bagi obat-obat resep yang disalahgunakan oleh anak-anak dan orang dewasa di sejumlah negara tertentu, seperti Amerika Serikat," kata badan tersebut (*http://www.bbc.co.uk/indonesian/news/story/2005/03/050302_internetdrugsau.shtml*, 2 Maret 2005).

[42]*Cyberlaundering* melibatkan penggunaan internet untuk menyembunyikan uang yang diperoleh dari suatu perbuatan ilegal. Pencucian uang merupakan kejahatan yang cukup lama dilakukan namun dengan keberadaan internet membuat hal ini menjadi mudah bagi pelaku tindak pidana untuk mengubah uang kotor menjadi aset yang sah atau menjadi investasi (Shinder, 2002: 32).

Istilah *money laundering* digunakan untuk menggambarkan kejahatan yang memproses "uang haram" melalui berbagai transaksi untuk menyamarkan darimana sebenarnya uang itu berasal dan membuatnya seolah-olah berasal dari sumber yang legal/sah. Menurut Robinson (1994), proses pencucian uang meliputi 3 tahap. Pertama, penempatan (*placement*) adalah proses awal menempatkan uang hasil kejahatan ke sumber yang legal misalnya rekening bank. Kedua, *layering* adalah proses memindahkan aset ke dalam berbagai transaksi untuk menyamarkan siapa pemilik dan darimana sumber "uang haram" tersebut. Ketiga, *integration* adalah untuk memasukkan uang tersebut ke dalam berbagai kegiatan ekonomi untuk menghilangkan keaslian sumber "uang haram" tersebut (Grabosky dan Smith, 1998: 175).

[43]*Cybercontraband* adalah kejahatan *cyber* yang berkaitan dengan data yang dilarang untuk dimiliki atau dikirimkan kepada masyarakat luas. Sebagai contoh *software* yang dirancang untuk memecahkan kode pengamanan suatu *software* yang diproteksi sesuai dengan hak kekayaan intelektual yang dimiliki oleh pemilik atau perusahaan pembuat *software* tersebut. *Software* semacam ini dilarang karena melanggar hak dari pembuat atau pemilik *software* tersebut. Sebagai contoh dalam ketentuan *Digital Millenium Copyright Act* (*DMCA*), *software* yang dapat memecah kode pengamanan suatu materi yang dilindungi oleh hak kekayaan intelektual dilarang untuk dimiliki secara umum (Shinder, 2002: 32).

2.2.4.1 Pendapat para Ahli Mengenai Pengaturan Kejahatan Komputer

Menurut Prof. Romli Atmasasmita dalam artikelnya "Model Kerjasama Dalam Pemberantasan *Cybercrime*" (12 Juli 2004: 2), ada tiga alasan pentingnya peranan hukum dalam mengatur dampak negatif perkembangan teknologi. **Pertama,** pertukaran informasi dan komunikasi antara warga di dunia memerlukan ketentuan hukum yang menjamin kepastian hukum. **Kedua,** kemajuan sarana teknologi informasi dan komunikasi sering digunakan perorangan atau kelompok terorganisir untuk memperoleh keuntungan finansial atau material dan merugikan lebih dari satu negara yang dilakukan bertentangan dengan hukum. **Ketiga,** perbedaan sistem hukum antarnegara berdampak serius dalam pelaksanaan kerjasama hukum antarnegara.

Sebagaimana dijelaskan sebelumnya bahwa *cybercrime* tidak lepas dari penggunaan komputer dalam melakukannya. Menurut Widyopramono (1994: 41-46), terdapat dua perbedaan pendapat di antara para ahli mengenai perlu tidaknya dibuatkan suatu ketentuan baru mengenai kejahatan komputer. Ada yang setuju dan ada pula yang tidak setuju dengan dibuatnya ketentuan baru mengenai kejahatan komputer.

Para ahli yang menyatakan bahwa **tidak perlu dibuatkan ketentuan baru yang mengatur tindak pidana di bidang komputer** di antaranya adalah:

Guru Besar Fakultas Hukum Universitas Diponegoro Prof. Dr. Muladi, S.H., yang menyatakan bahwa jika diciptakan undang-undang secara khusus tentang tindak pidana komputer, maka dalam waktu singkat undang-undang itu akan ketinggalan zaman. Tindak pidana komputer belum merupakan tindak pidana yang sudah meluas sehingga perlu ditangkal dengan undang–undang khusus. Tindak pidana komputer baru bersifat sporadis. Padahal, ciri sebuah undang–undang baru diberlakukan bila persoalan itu sudah menjadi masalah masyarakat. Diperlukan keberanian hakim untuk mengadili perkara tindak pidana di bidang komputer dengan undang-undang yang sudah ada dengan cara memperluas penafsiran, hingga pencurian data komputer misalnya dapat dianggap sebagai pencurian dengan menafsirkan barang di pasal pencurian, termasuk juga data komputer atau barang digital (Widyopramono, 1994: 41-42).

Himawan, S.H., Mantan Jaksa Agung Muda Bidang Tindak Pidana Khusus Kejaksaan Agung RI, dalam majalah Tempo Edisi 24 Oktober 1987 menyatakan bahwa yang penting bukan dengan apa kejahatan itu dilakukan tetapi yang penting adalah perbuatannya. Apa pun bentuk kejahatan yang dilakukan dengan komputer di masa depan, dapat diantisipasi dengan undang–undang yang ada. Sehingga dalam kasus tindak pidana komputer, kejaksaan harus siap menggunakan pasal penggelapan dalam KUHP atau menggunakan Undang-undang Tindak Pidana Korupsi karena undang–undang antikorupsi dapat menjerat siapa saja yang melakukan tindak pidana yang merugikan keuangan negara (Widyopramono, 1994: 42).

Para ahli yang menyatakan **perlu dibuat ketentuan khusus dalam KUHP atau undang–undang khusus** yang mengatur tindak pidana di bidang komputer adalah sebagai berikut:

Teuku M. Radhie, S.H., mantan Kepala Badan Pembinaan Hukum Nasional mengatakan bahwa lembaganya sudah mengkaji undang–undang khusus untuk tindak pidana komputer sejak tiga tahun lalu. Hanya saja, sampai saat ini belum ada ahli yang khusus mempersiapkan tindak pidana komputer itu dalam tata hukum pidana baru nanti. Beliau memperkirakan bahwa tindak pidana komputer itu akan masuk pasal–pasal penggelapan dan bukan pasal korupsi (Widyopranomo, 1994: 44).

Sementara itu Prof. Dr. CFG. Sunaryati Hartono, S.H., dalam Seminar Nasional Iptek dan Teknologi tanggal 4-5 Nopember 1992 di Fakultas Universitas Muhammadiyah Jakarta menyatakan bahwa akibat pengaruh teknologi, kini sudah berkembang bidang–bidang hukum yang baru yang bersifat interdisipliner, seperti hukum komputer dan informatika. Bagaimanapun setiap bidang hukum yang baru itu akan bersumber pada Pancasila dan Undang–Undang Dasar 1945, berlandaskan pada undang–undang lain dan peraturan perundang-undangan; mengembangkan yurisprudensi dan hukum kebiasaan di bidang yang bersangkutan. Juga diperlukan adanya keterpaduan dan kesearahan antara pembentuk hukum, pengadilan, aparat penegak hukum, aparat pelayanan hukum, profesi hukum dan masyarakat. Dengan demikian, semuanya akan menjadi satu kesatuan terpadu (Widyopranomo, 1994: 44).

Prof. Dr. J.E Sahetapy, Guru Besar Hukum Pidana Universitas Airlangga Surabaya, menyatakan bahwa hukum pidana yang ada tidak siap untuk menghadapi kejahatan komputer. Karena tidak mudah menganggap kejahatan komputer berupa pencurian data sebagai pencurian. Di samping itu, ada kemungkinan kesulitan pembuktian dan kerugian, maka sangat diperlukan produk hukum baru yang dapat menangkal dampak kemajuan teknologi, agar dakwaan terhadap terdakwa dalam kasus tindak pidana komputer tidak meleset. Contoh tentang sulitnya pembuktian dari kasus ini adalah data digital dapat di-*copy* secara melawan hukum ataupun diambil. Bedanya adalah dalam hal di-*copy* secara ilegal, pemilik masih dapat menguasai data tersebut. Juga meng-*copy* data secara ilegal dapat dilakukan secara cepat dan sulit terlihat malahan terkadang pemilik pun tidak mengetahui bahwa data-datanya telah di-*copy* (Widyopranomo, 1994: 44-45).

Todung Mulya Lubis, Mantan Ketua Yayasan Lembaga Bantuan Hukum Indonesia (YLBHI) berpendapat bahwa sudah saatnya dilahirkan undang–undang khusus tentang tindak pidana komputer di Indonesia. Todung Lubis beralasan bahwa tindak pidana ini termasuk *white collar crime*, tindak pidana yang dilakukan oleh kalangan "orang kantoran" dan menggunakan teknik yang canggih dan rumit; untuk dapat dibuktikan tidak cukup menggunakan pasal–pasal tindak pidana konvensional. Selain itu ancaman dari pasal–pasal pidana itu tidaklah memadai dibandingkan dengan akibat tindak pidana yang terjadi (Widyopranomo, 1994: 45).

J. Sudama Sastroandjojo, S.H. menghendaki perlu adanya ketentuan baru yang mengatur mengenai permasalahan tindak pidana komputer. Beliau mengusulkan bahwa tindak pidana yang menyangkut komputer harus ditangani secara khusus; cara-cara, lingkungan, waktu dan letaknya dalam melakukan tindak pidana komputer adalah berbeda dengan tindak pidana lain (Widyopranomo, 1994: 46).

Dari berbagai pendapat yang telah dijelaskan sebelumnya baik yang setuju maupun tidak setuju terhadap pengaturan kejahatan komputer dalam undang-undang tersendiri, Prof. Mardjono Reksodiputro, S.H., MA. dari Universitas Indonesia dalam bukunya "Kemajuan Pembangunan Ekonomi dan Kejahatan"

menyatakan bahwa masih perlu dibentuk panitia yang mengkaji permasalahan aturan hukum pidana yang dapat menanggulangi penyalahgunaan komputer (*computer abuse*) atau kejahatan komputer (*computer crime; computer criminaliteit*). Beliau merujuk pada pendapat Piragoff (1986) yang juga telah dilakukan oleh Komisi Franken di Belanda bahwa hal pertama yang harus dilakukan adalah memeriksa apakah undang-undang hukum pidana yang berlaku masih dapat digunakan dalam lingkungan komputer (*computer environment*). Mardjono berpendapat bahwa kejahatan komputer sebenarnya bukan kejahatan baru dan masih terjangkau oleh KUHP yang berlaku di Indonesia. Oleh karena itu, pengaturan untuk menanggulangi kejahatan ini sebaiknya diintegrasikan dalam KUHP dan tidak dalam bentuk undang–undang tersendiri. Misalnya dengan memperluas pengertian surat yang dapat mencakup data elektronik atau barang yang dapat mencakup informasi. Namun beliau berpendapat bahwa perhatian khusus harus diberikan pada kejahatan "manipulasi komputer" karena perbuatan ini merupakan kejahatan "*computer fraud*" sebagai bagian dari "*computer related economic crimes*" yang dapat menimbulkan kerugian besar sehingga perlu dipikirkan pengaturannya dalam undang-undang tindak pidana ekonomi (Reksodiputro, 1997: 20).

Dalam membuat ketentuan baru mengenai suatu kejahatan dalam hal ini kejahatan komputer, perlu dipertimbangkan beberapa alasan yaitu: berapa luasnya kerugian potensial yang mungkin terjadi bilamana ada pelanggaran; adakah padanan dalam aturan lama yang berlaku; tidakkah aturan baru ini akan mengganggu kelancaran informasi dan harmonisasi dengan peraturan perundang-undangan negara lain. Hal ini dilakukan agar tidak terjadi konsep hukum yang tidak jelas (*unwarranted legal*) atau efek sosial ekonomi (*socio-economic effects*) dan pengaturan tindak pidana yang berlebihan (*over-criminalization*) dalam hal akan dilakukannya penambahan atau perubahan undang-undang hukum pidana yang berlaku (Reksodiputro, 1997: 20).

2.2.4.2 Pengaturan *Cybercrime* di Indonesia

Menurut Guru Besar Kriminologi Universitas Indonesia Prof. Nitibaskara dalam artikelnya "Problema Yuridis *Cybercrime*", sulitnya menciptakan peraturan-peraturan di *cyberspace*, khususnya membuat *Cybercrime Law*, adalah

disebabkan perubahan-perubahan radikal yang dibawa oleh revolusi teknologi informasi yang membalikkan paradigma-paradigma. Untuk membuat ketentuan hukum yang memadai di dunia *cyber*, tampaknya para pembuat hukum terpaksa harus rela menunggu revolusi mulai reda. Reaksi sosial yang semakin keras terhadap *cybercrime* akan mendorong lahirnya pengaturan-pengaturan yang lebih ketat di *cyberspace*, termasuk *cybercrime law*. Seberapa keras reaksi sosial, sangat tergantung dari seberapa besar *fear of crime* masyarakat dan kepedulian negara terhadap *cybercrime*. Sekiranya ketentuan-ketentuan hukum yang sekarang ada dapat dipergunakan, maka pelaksanaannya akan berbeda dengan penegakan hukum di dunia biasa, khususnya yang harus dilakukan oleh aparat kepolisian. Dalam dunia *cyber*, polisi sebagai *crime hunter* mempunyai senjata utama berupa keterampilan teknis di bidang teknologi informasi. Tetapi, tanpa pegangan hukum yang kokoh tidak terlalu banyak yang mampu dilakukan aparat penegak hukum (Nitibaskara, 31 Juli 2000: 1-3).

Secara eksplisit sampai saat ini tidak ada peraturan perundang-undangan yang menyebutkan kata *hacking*. Namun unsur-unsur tindak pidana yang menyerupai atau dapat dikategorikan atau digunakan untuk tindak pidana *hacking* tersebar baik di dalam KUHP, di luar KUHP, dan dalam rancangan undang-undang yang sedang disusun.

Menurut Prof. Barda Nawawi Arief (2006: 91-92), perumusan tindak pidana yang ada dalam KUHP masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cybercrime*. Sebagai contoh dalam menghadapi masalah pemalsuan kartu kredit dan transfer data elektronik saja, KUHP mengalami kesulitan karena tidak ada ketentuan khusus mengenai pembuatan kartu kredit palsu yang ada hanya pasal mengenai sumpah/keterangan palsu, pemalsuan mata uang dan kertas, pemalsuan meterai dan merek, pemalsuan surat. Oleh karena itu, kemungkinan dalam praktek digunakan pasal-pasal lain yang berkaitan dengan **penggunaan** kartu kredit palsunya (untuk melakukan kejahatan), bukan dalam hal **pembuatan** kartu kredit palsu tersebut.

2.3 Tindak Pidana *Hacking*

Untuk memahami *hacking* sebagai suatu kejahatan, secara umum dapat diperhatikan pendapat Nitibaskara (2000: 1) yang mengulas mengenai kejahatan (*crime*) yang tidak dapat dilepaskan dari lima faktor yang saling tali temali, yaitu pelaku kejahatan, modus kejahatan, korban kejahatan, reaksi sosial atas kejahatan, dan hukum. Menurut Fattah (1997) dalam Nitibaskara (2000: 1), ada dua definisi secara hukum yang popular mengenai kejahatan. Definisi pertama merumuskan bahwa kejahatan adalah apa yang disebut oleh hukum sebagai kejahatan (*crime is what the law say it is*). Kemudian definisi kedua menyatakan bahwa kejahatan adalah suatu tindakan yang disengaja atau kelalaian yang dapat dikenai sanksi pidana oleh hukum (*crime as an act or omission punishable by law*).

Selanjutnya masih menurut Nitibaskara (2000: 2) dalam hukum pidana ada tiga permasalahan yang senantiasa menjadi pembicaraan, yaitu perbuatan yang dilarang, pelaku perbuatan yang dilarang, dan ancaman pidana. Perbuatan yang dilarang adalah perbuatan yang bertentangan dengan hukum, suatu perbuatan melawan hukum atau tidak memenuhi perintah hukum. Perbuatan ini ada yang bersifat nyata-nyata berlawanan dengan bunyi undang-undang dan ada pula yang menentang rasa keadilan masyarakat, tetapi tidak melanggar bunyi ketentuan hukum formal. Yang pertama disebut melawan hukum formal (*formeele wederechtelijkheidsbegrip*), sedangkan yang kedua melawan hukum materiil (*materiele wederechtelijkheidsbegrip*). Perbuatan yang mengandung sifat melawan hukum formal yang dapat diproses secara pidana menurut ketentuan pidana yang ada. Suatu perbuatan yang merugikan masyarakat yang belum dirumuskan dalam hukum pidana positif sebagai perbuatan pidana, secara yuridis belum dianggap sepenuhnya sebagai suatu kejahatan.

Dalam mengungkap kasus *cybercrime* khususnya *hacking* bukan hal yang mudah. Di Indonesia, belum ada ketentuan khusus yang mengatur tentang *cybercrime*. Bila dikaitkan dengan pasal 1 ayat 1 KUHP bahwa tidak ada suatu perbuatan dapat dipidana jika belum ada ketentuan yang mengaturnya, tentu hal ini akan memberikan kesulitan bagi aparat penegak hukum dalam memproses kasus-kasus yang berkaitan dengan *cybercrime*. Oleh karena itu perlu dilakukan

terobosan dalam bidang hukum yakni dengan melakukan interpretasi terhadap ketentuan yang ada seperti ketentuan dalam KUHP. Suatu kejahatan tentu memberikan kerugian terhadap korban, oleh karena itu hukum perlu ditegakkan untuk melindungi hak-hak korban demi terwujudnya keadilan dan kepastian hukum.

2.3.1 Pengertian *Hacking*

Hacking adalah istilah yang digunakan untuk menggambarkan usaha (baik berhasil maupun tidak) untuk memperoleh akses yang ilegal ke dalam suatu sistem komputer. Hal ini berkaitan dengan penggunaan komputer yang tidak sah atau akses ilegal ke data atau program tertentu yang tersimpan di komputer tersebut, sebagai contoh, terhadap orang-orang yang mengakses suatu komputer melebihi izin sah yang mereka miliki (Burdett *et al*., 1995: 95).

Istilah *hacking* merupakan pendapat N. Keyzer dalam ceramahnya tentang Hukum Pidana Belanda dan Penyalahgunaan Komputer di Badan Pembinaan Hukum Nasional (BPHN) tanggal 28 Juli 1986. Maksud *hacking* adalah suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa izin (dengan melawan hukum) dari pemilik sah jaringan komputer tersebut (Hamzah dan Marsita, 1990: 38).

Dalam *Black's Law Dictionary*, penjabaran *hack* terdapat pada kata *Crack* (Garner, 2004: 395). *Crack* adalah membuka atau membongkar sandi (informasi keamanan), guna menemukan kode atau membongkar sandi yang diperlukan untuk masuk ke dalam komputer, jaringan dan *server* atau *database*. *To hack* adalah untuk melalui sistem keamanan yang didesain untuk mencegah adanya akses tanpa wewenang. *To hack* dapat dilakukan pada suatu komputer, jaringan, server atau database dengan maksud menyebabkan kerusakan atau gangguan.

Dari berbagai definisi *hacking* di atas dapat diketahui bahwa *hacking* merupakan suatu kegiatan yang dilakukan dengan memasuki ke dalam sistem komputer atau sistem jaringan tanpa hak. Namun definisi-definisi tersebut belum menjelaskan mengenai koneksi dengan internet. Karena *hacking* tidak hanya dapat dilakukan terhadap suatu komputer saja secara langsung (tanpa koneksi internet) tetapi dapat juga dilakukan melalui internet seperti *hacking* ke dalam *website*.

2.3.2 Pelaku *Hacking* (*Hacker*)

Dalam buku "*Hackers: Heroes of the Computer Revolution*", yang ditulis oleh Steven Levy tahun 1984, diceritakan bahwa istilah *hacker* pada awalnya yaitu tahun 1950 dan 1960, ditujukan sebagai penghargaan terhadap kemampuan yang dimiliki oleh *hacker*. Pada tahun 1960, para *hacker* adalah ahli dalam *hardware* dan *software* dan istilah *hacker* ditujukan kepada seseorang yang mampu mengimplementasikan solusi teknik yang lebih maju tentang sistem teknologi canggih. Namun pada era milenium, istilah *hacker* menjadi berbeda karena ditujukan kepada orang yang dapat memiliki akses secara tidak sah atas suatu sistem dan data. Secara ekstrim perbuatannya merusak suatu sistem yang mereka masuki seperti menghapus *file*, mengubah data dan mencuri informasi atau dikenal dengan istilah *cracker* (Furnell, 2002: 41-42).

Pengertian *hacker* secara umum adalah orang yang melakukan kejahatan *hacking*. Menurut Doswell dan Simons (1986: 47-48) *hacking* menggambarkan suatu kegiatan kriminal, keahlian dalam menggunakan komputer untuk melakukan kegiatan ilegal.

Perbedaan yang jelas tentang *hacker* dapat dilakukan berdasarkan motif dari *hacker* tersebut, yaitu *black hat* (topi hitam), *grey hat* (topi abu-abu) dan *white hat* (topi putih). *Black Hat* ditujukan kepada sebagaian besar para *hacker* misal *hacker* yang memasuki sistem tanpa izin, dan seringkali merusak (disebut juga *darkside hacker*). *White Hat* adalah kebalikannya, adalah *hacker* yang beretika, bekerja untuk kepentingan suatu sistem keamanan jaringan komputer. Sedangkan *Grey Hat* adalah seseorang yang dapat dikategorikan ke dalam dua istilah *hacker* diatas, dimana motifnya belum jelas atau cenderung dapat berubah-ubah (Furnell, 2002: 43-44).

Untuk mengilustrasikan tentang perbedaan hitam dan putih atau baik dan buruknya *hacker*, ada beberapa istilah *hacker* yang digunakan dalam komunitas *hacker*. *Cyberterrorist* adalah teroris yang memiliki keahlian *hacker* untuk mengancam atau melakukan penyerangan terhadap suatu sistem, jaringan dan atau data. *Cyberwarriors* adalah seseorang yang memiliki keahlian *hacking* dengan tujuan menyerang sistem komputer yang mendukung infrastruktur yang vital seperti pelayanan darurat, transaksi finansial, transportasi dan komunikasi. Hal ini

berhubungan dengan *hacking* dalam konteks militer atau perang. *Hacktivist* adalah *hacker* yang menyusup ke suatu sistem komputer untuk mempromosikan dirinya atau tujuan tertentu seperti *deface* suatu *website*. *Malware writters* adalah seseorang yang bertanggung jawab dalam menciptakan program yang merusak seperti virus, *worm* dan *trojan horse*. *Phreakers* adalah seseorang yang memfokuskan dirinya meng-*hacking* jaringan telepon dan teknologi yang berkaitan, dimana tujuannya dapat berupa hanya untuk melihat-lihat saja sampai mengubah hal-hal yang ada di dalamnya misalnya membuat penggunaan telepon menjadi gratis atau tidak membayar sama sekali. *Samurai* adalah seseorang yang disewa untuk melakukan pekerjaan *cracking* yang legal, masuk ke dalam sistem komputer suatu perusahaan untuk alasan yang lebih sah, disebut juga *sneakers*. *Script kiddies* adalah seseorang tidak terlalu ahli dalam *hacking* karena tergantung pada program yang dibuat oleh orang lain atau *hacker* yang lebih ahli. *Warez dudez* adalah seseorang yang bertujuan untuk memperoleh dan mendistribusikan *copy* ilegal suatu *software* yang resmi disebut juga *Software Pirates* (Furnell, 2002: 44-45).

Dalam komunitas *hacker* ternyata ada etika dan aturan main yang membedakan antara *hacker* dan *cracker*, maupun *hacker* kelas rendahan. Salah satu etika yang berhasil diformulasikan dengan baik ada pada buku "*Hackers: Heroes of the Computer Revolution*", yang ditulis oleh Steven Levy tahun 1984, ada enam etika yang perlu diresapi seorang *hacker*, yaitu; akses ke komputer dan apapun yang akan mengajarkan kepada anda bagaimana dunia ini berjalan atau bekerja harus dilakukan tanpa batas dan total; selalu mengutamakan pengalaman lapangan; semua informasi harus bebas, tidak disembunyikan; tidak pernah percaya otoritas, percaya pada desentralisasi; seorang *hacker* hanya dinilai dari kemampuan *hacking*-nya, bukan kriteria buatan seperti gelar, umur, posisi atau suku bangsa; seorang *hacker* membuat seni dan keindahan di komputer; komputer dapat mengubah hidup seseorang menuju yang lebih baik (Furnell, 2002: 64).

2.3.3 Modus Operandi *Hacking*

Bila *hacker* telah berhasil masuk dalam suatu sistem komputer dan berhasil menimbulkan kerusakan seperti yang direncanakannya maka terjadilah kerusakan

sistem. Komputer dan sistem yang ada tidak dapat berfungsi sebagaimana seharusnya. Kejadian seperti itu disebut *cracking*. Menurut Prana (1994: 45) sebagaimana dikutip Makarim (2005: 434-435) proses penyusupan yang dilakukan *hacker* dapat dibagi menjadi beberapa tahapan yaitu mencari sasaran sistem komputer yang hendak dimasuki, menyusup dan menyadap *password*, dan menjelajahi sistem komputer.

Mencari sasaran sistem komputer yang hendak dimasuki. Dengan perkembangan internet, *hacker* lebih mudah menyusup. *Hacker* tidak perlu lagi menghubungi nomor telepon yang memiliki akses ke jaringan modem sampai ditemukan suatu *signal carrier*. Dahulu, *signal carrier* tersebut merupakan celah untuk memasuki sistem komputer dari saluran telepon. Saat ini *hacker* hanya perlu mencari *host* yang dijadikan sasaran dengan cara mencari *port* tempat data keluar masuk dari satu komputer ke komputer lainnya. *Hacker* menggunakan program-program seperti *port scanner* untuk mencari *port* komputer tersebut. Salah satu program *port scanner* adalah *finger* yang mempunyai fasilitas mencari informasi pemakai jaringan atau pemakai sistem, waktu *login* terakhir, dan *login name* (Makarim, 2005: 434-435).

Menyusup dan menyadap *password*. *Hacker* menebak *user name* dan *password* dalam sistem yang dijadikan sasaran serangan *hacking*. Cara ini semakin sulit dilakukan karena telah tersedia perlindungan terhadap data atau informasi dengan adanya *enkripsi* (penyandai) terhadap suatu pesan. Dalam menebak *password*, *hacker* dapat menyusun nama-nama yang mungkin dipakai oleh orang atau menggunakan metode lain yaitu *brute forcing* yang mampu mengkombinasikan karakter baik huruf, angka atau karakter lain (Makarim, 2005: 435).

Menjelajahi sistem komputer. *Hacker* kemudian melakukan *sniffing* yaitu kegiatan menyadap dan memeriksa data-data yang melintas dalam jaringan. *Hacker* berupaya mencari kelemahan dalam sistem tersebut. Banyak alternatif tindakan yang dapat dilakukan oleh *hacker* untuk memperoleh akses seperti *Cache Poison* yang digunakan sebagai kombinasi atau untuk meracuni tabel daftar alamat dalam suatu *router* atau perangkat sejenisnya. *Key Logger* adalah program yang digunakan oleh *hacker* untuk mendeteksi setiap tombol yang ditekan oleh

pemakai komputer dalam menulis *login* atau *password*. Untuk menghilangkan jejak setelah *hacker* melakukan aksinya, dia menggunakan *Trojan Horse*. Kemudian *Decoy* merupakan program yang mirip dengan program *login*, tapi sebenarnya berdiri sendiri sehingga sangat mungkin pemakai tertipu dengan tampilan di layar. Setelah pemakai memasukkan *password*nya, program *decoy* akan menyimpan kombinasi tersebut ke dalam sebuah *file* (Makarim, 2005: 435).

2.3.4 Pengaturan Tindak Pidana *Hacking*

Dalam melakukan penyidikan suatu tindak pidana terutama penuntutan tentu dilakukan berdasarkan ketentuan hukum yang berlaku. Dalam hal kejahatan *cyber*, yang merupakan tindak pidana yang belum diatur secara khusus dalam ketentuan hukum yang berlaku di Indonesia, maka penafsiran (interpretasi) terhadap ketentuan yang ada sangat diperlukan. Karena tidak mungkin pengadilan dalam hal ini hakim menolak untuk memproses suatu perkara yang belum ada ketentuannya. Tentu digunakan ketentuan yang sudah ada dengan melakukan penafsiran. Menurut Kanter dan Sianturi (1982: 64-69), penafsiran yang digunakan menurut doktrin dan analogi adalah:

a. Penafsiran secara otentik yaitu mencari pengertian yang diinginkan pada pasal undang-undang.
b. Penafsiran menurut penjelasan undang-undang (*memorie van toelichting*).
c. Penafsiran sesuai dengan yurisprudensi yaitu mencari dalam Putusan-putusan Kasasi Mahakamah agung (MA), Fatwa MA, Surat Edaran MA, Putusan-putusan Banding atau Putusan-putusan pengadilan pada tingkat pertama yang telah mempunyai kekuatan yang tetap dan sudah lazim diikuti oleh peradilan lainnya.
d. Penafsiran menurut doktrin atau ilmu pengetahuan ada sembilan cara penafsiran yaitu:
    a) Penafsiran menurut tata bahasa (*gramnaticale interpretatie*) adalah penafsiran yang memberikan arti kepada suatu istilah atau perkataan sesuai dengan tata bahasa. Misalnya jika perumusan berbunyi "pegawai menerima suap" maka subjek disini adalah pegawai negeri bukan profesi pekerjaan lain.

b) Penafsiran secara sistematis adalah apabila suatu istilah atau perkataan dicantumkan dua kali dalam suatu pasal, atau undang-undang maka pengertiannya harus sama pula. Misalnya istilah pencurian yang tercantum pada Pasal 363 KUHP harus sama dengan pengertian istilah yang sama tercantum dalam Pasal 362 KUHP,

c) Penafsiran mempertentangkan (*redeneering a contrario*) adalah penafsiran yang menemukan kebalikan dari pengertian suatu istilah yang sedang dihadapi. Misalnya apabila ada ketentuan dilarang melakukan suatu tindakan tertentu, kebalikannya adalah jika seseorang melakukan sesuatu tindakan yang tidak dilarang maka orang itu tidak tunduk pada ketentuan larangan tersebut.

d) Penafsiran memperluas (*extensieve interpretatie*) adalah penafsiran yang memperluas pengertian dari suatu istilah berbeda dengan pengertiannya yang digunakan sehari-hari. Penafsiran ini sering menjadi perdebatan karena sukar menentukan batas bagi perluasan tersebut. Hal ini menjadi perhatian karena analogi juga dikatakan sebagai perluasan pengertian atau perluasan cakupan ketentuan suatu peraturan, padahal pada umumnya analogi tidak boleh dipergunakan dalam hukum pidana. Contohnya adalah kasus *hacking* yang dilakukan Iqra Syafaat dalam kasus *hacking website* Partai Golkar dan Dani Firmansyah dalam kasus *hacking website* Komisi Pemilihan Umum[44].

e) Penafsiran mempersempit (*restrictieve interpretatie*) adalah penafsiran yang mempersempit pengertian suatu istilah misalnya UU. Undang-undang dalam pengertian luas mencakup semua produk perundang-

---

[44]Menurut penyidik, pengubahan isi dalam *website* Partai Golkar dan *website* KPU disamakan dengan rusaknya suatu barang yang dapat diancam pidana sebagaimana diatur dalam Pasal 406 KUHP. Jika dilihat dari pengertian barang atau benda dalam tinjauan hukum pidana, pengertian barang atau benda dalam penjelasan Pasal 362 KUHP, yaitu segala sesuatu yang berwujud atau tidak berwujud (misal listrik, gas) dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang. Bila dilakukan interpretasi ekstensif, maka hal ini berarti *website* tersebut dianggap sebagai barang atau benda tak berwujud. Tindak pidana *hacking* belum secara tegas dan khusus diatur dalam suatu ketentuan hukum atau undang-undang tersendiri, sehingga interpretasi diperlukan dalam penanganan kasus ini. Oleh karena itu kasus-kasus ini dapat menjadi yurisprudensi atau sebagai dasar hukum untuk digunakan dalam penanganan kasus *cybercrime* lainnya khususnya tindak pidana *hacking*.

undangan baik yang dibuat Pemerintah, DPR, Gubernur dan lain sebagainya. Sedangkan UU bila dipersempit artinya hanya mencakup UU yang dibuat oleh Pemerintah bersama DPR saja.

f) Penafsiran secara historis adalah penafsiran yang mempelajari sejarah hukum yang berkaitan atau mempelajari pembuatan undang-undang yang bersangkutan sehingga akan ditemukan pengertian dari istilah tersebut. Misalnya dari risalah-risalah pembahasan RUU.

g) Penafsiran teleologis adalah penafsiran yang mencari tujuan atau maksud dari suatu ketentuan undang-undang. Misalnya tujuan pembentukan Mahkamah Militer Luar Biasa (Mahmilub), Undang-undang No. 16 Tahun 1963 adalah untuk mempercepat penyelesaian suatu perkara khusus, sehingga banding dan kasasi ditiadakan namun masih ada upaya hukum lain yaitu memohon grasi kepada Presiden.

h) Penafsiran logis adalah penafsiran yang mencari pengertian dari suatu istilah atau ketentuan berdasarkan hal-hal yang masuk akal. Cara ini tidak banyak dipergunakan.

i) Penafsiran analogi adalah penafsiran yang memperluas cakupan atau pengertian dari ketentuan undang-undang.

2.3.4.1 Pengaturan Tindak Pidana *Hacking* di dalam KUHP

Dalam KUHP terdapat beberapa tindak pidana yang dapat dikaitkan dengan *hacking* begitu pula konsep-konsep dalam KUHP yang berhubungan erat dengan kejahatan komputer seperti:

a. Ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain tanpa hak

Dalam KUHP telah diatur tentang perbuatan memasuki atau melintasi wilayah tanpa hak. Hal ini dapat dilihat dalam ketentuan Pasal 167 KUHP[45] yaitu

---

[45]Pasal 167 KUHP berbunyi: Moeljatno (2001: 63-64)

"(1) Barangsiapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum, atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama sembilan bulan atau denda paling banyak tiga ratus rupiah.

(2) Barangsiapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu atau pakaian jabatan palsu atau barangsiapa tidak setahu yang berhak lebih

tanpa hak memasuki rumah, ruangan atau pekarangan tertutup yang ditempati orang lain. Berdasarkan pasal tersebut, wilayah yang dimaksud adalah bersifat fisik, dan sifat fisik inilah yang membatasi aturan pidana untuk diterapkan dalam kasus *cybercrime*. Oleh karena itu perlu adanya pendekatan baru dalam artian tindakan memasuki disini tidak lagi langsung pada objek yang bersifat fisik. Tindakan yang dimaksud di sini berupa suatu jejak elektronik (*electronic path*), yang berisikan angka atau data matematis yang mengindikasikan telah berlangsung aktivitas elektronis (Makarim, 2005: 440).

Interpretasi yang digunakan dalam pengunaan pasal ini adalah interpretasi ekstensif yang memperluas pengertian wilayah. Kasus *hacking* suatu *website* dapat menggunakan ketentuan pasal ini dimana *website* dianggap sebagai wilayah milik orang lain. Ketika seseorang memasuki suatu *website*, dan melakukan kegiatan yang dapat mengubah isi dari *website* tersebut tanpa izin yang sah dari pemilik *website*, maka hal ini dapat dikategorikan sebagai tindakan *hacking*.

Ketentuan Pasal 167 KUHP berkaitan dengan *right of privacy*[46]. *Right of privacy* adalah hak yang berhubungan dengan kebebasan pribadi atau hak seseorang dan segala yang dimilikinya untuk hidup bebas dari publikasi secara umum (Garner, 2004: 1350). *Right of Privacy* ini juga berkaitan dengan hak mendapatkan informasi. Tentunya hak ini tidak bersifat mutlak dalam artian tidak dapat diganggu gugat oleh pihak lain. Hal ini dapat dilihat dalam ketentuan yang diatur dalam Undang Undang Dasar 1945 misalnya pasal 28 F UUD 1945 dan pasal 14 UU No. 39 tahun 1999 tentang Hak Asasi Manusia, LN No. 165, TLN

---

dahulu serta bukan karena kekhilafan masuk dan kedapatan di situ pada waktu malam, dianggap memaksa masuk.

(3) Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, pidana menjadi paling lama satu tahun empat bulan.

(4) Pidana tersebut dalam ayat 1 dan 3 dapat ditambah sepertiga, jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu."

[46]Berdasarkan Penjelasan Pasal 26 ayat 1 UU ITE, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

No. 3886, yang memberikan hak bagi seseorang untuk memperoleh informasi dengan menggunakan jenis saluran yang tersedia. Bila dihubungkan dengan penggunaan teknologi termasuk internet, berarti ketentuan ini memberikan kebebasan bagi seseorang untuk dapat memperoleh informasi yang ia inginkan. Namun bukan berarti dia bebas melakukan hal itu, misalnya pelaku *cybertrespass* yang tanpa izin memasuki *website* pihak lain bahkan dapat disertai dengan pengubahan isi *website* dan pencurian informasi bersifat rahasia dari *website* tersebut. Pembatasan atas kebebasan ini diatur dalam pasal 28 J UUD 1945, bahwa dalam menjalankan hak dan kebebasan tersebut, setiap orang wajib tunduk kepada pembatasan yang ditentukan oleh undang-undang. Hal ini dilakukan untuk menjamin pengakuan dan penghormatan atas hak dan kebebasan yang juga dimiliki oleh orang lain.

Perkembangan teknologi komputer sekarang ini berkembang pesat yang dapat digunakan pada setiap aspek kehidupan masyarakat yang membawa pengaruh terhadap pembangunan *Central Processing Unit* (*CPU*) yang melayani komputer tertentu baik dalam rumah tangga maupun instansi tertentu melalui terminal sistem. Istilah *hacking* sebagaimana dijelaskan oleh N. Keyzer adalah suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa izin (dengan melawan hukum) dari pemilik sah jaringan komputer tersebut. Apabila dikaitkan dengan delik-delik yang tercantum dalam pasal-pasal KUHP, maka perbuatan *hacking* dapat dikategorikan sebagai perbuatan tanpa wewenangnya masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan atau tanpa haknya berjalan di atas tanah milik orang lain, sehingga pelaku dapat diancam ketentuan dalam Pasal 167 KUHP (Hamzah dan Marsita, 1990 :38-39).

b. Ketentuan yang berkaitan dengan perbuatan penghancuran atau perusakan barang

Ketentuan mengenai penghancuran atau perusakan barang diatur dalam Pasal 406 KUHP[47]. Menurut Andi Hamzah dan Budi Marsita (1990: 33-34) ada 4

---

[47]Pasal 406 KUHP berbunyi: Moeljatno (2001: 146)

"(1) Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah

pengertian tentang "*menghancurkan, merusak, membuat tidak dapat dipakai lagi dan menghilangkan*"[48]. Dalam kejahatan *cyber* perbuatan ini dikenal dengan istilah "penyia-nyiaan data komputer" yaitu suatu perbuatan dengan sengaja merusak atau menghancurkan media disket dan sejenisnya yang berisikan data atau program kerja menjadi tidak berfungsi dan pekerjaan-pekerjaan yang melalui proses komputer tidak dapat dilaksanakan. Sebagaimana telah dijelaskan sebelumnya bahwa data/program komputer dapat disamakan dengan pengertian barang. Oleh karena itu, pelaku perbuatan penyia-nyiaan data komputer yang pada hakekatnya adalah perbuatan penghancuran atau perusakan data atau program komputer, dapat dikenakan ketentuan Pasal 406 ayat (1) KUHP dan seterusnya (Wisnubroto, 1999: 90-91).

Interpretasi yang digunakan dalam pasal ini yang berhubungan dengan tindak pidana *hacking* adalah penafsiran *ekstensif* yang memperluas pengertian barang. Sebagai contoh adalah kasus *hacking website* partai Golkar yang dilakukan Iqra Syafaat. Dimana penyidik menginterpretasikan bahwa *website* Partai Golkar adalah barang sebagaimana disebutkan dalam Pasal 406 ayat 1 KUHP. Iqra Syafaat diduga telah sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu

---

kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah.

(2) Dijatuhkan pidana yang sama terhadap orang yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin tak dapat digunakan atau menghilangkan hewan, yang seluruhnya atau sebagian adalah kepunyaan orang lain."

[48]Yang dimaksud dengan tindakan "**menghancurkan**" pada kasus penyalahgunaan komputer adalah suatu perbuatan menghancurkan disket dan sejenisnya yang berisi data atau program komputer sehingga mengakibatkan disket, data atau program didalamnya menjadi hancur dan tidak dapat dimanfaatkan lagi. Yang dimaksud dengan tindakan "**merusak**" pada kasus penyalahgunaan komputer adalah suatu perbuatan merusak isi disket dan media penyimpan lainnya seperti menghapus data atau program, membuat cacat data atau program (membuat cacat isi disket dan sejenisnya), menambahkan data baru kedalam disket dan sejenisnya secara acak dengan kata lain mengacaukan isi disket dan media penyimpan lainnya. Yang dimaksud dengan "**menghilangkan**" pada kasus kejahatan komputer adalah perbuatan menghilangkan atau menghapus data atau program yang tersimpan didalam disket dan media penyimpan lain sehingga mengakibatkan semua data atau program tersebut hilang sama sekali. Yang dimaksud dengan "**membuat tidak dapat dipakai lagi**" (membuat tidak berguna) pada kasus penyalahgunaan komputer adalah suatu perbuatan yang dilakukan sedemikian rupa sehingga data atau program komputer yang seharusnya dapat dimanfaatkan sesuai dengan isinya. Hal ini disebabkan karena data atau program tersebut telah diubah seluruhnya atau pada beberapa bagiannya, atau dirusak seluruhnya atau beberapa bagiannya, atau dihapus seluruhnya atau beberapa bagiannya, maka maksud penggunaan data atau program komputer tersebut terhalangi (tidak dapat dipakai lagi sesuai dengan fungsinya), dan tidak dapat diperbaiki lagi (Hamzah dan Marsita, 1990: 33-34).

yang seluruhnya atau sebagian milik orang lain dalam hal ini *website* milik Partai Golkar.

2.3.4.2 Pengaturan Tindak Pidana *Hacking* di luar KUHP

Sebagaimana telah dijelaskan sebelumnya, bahwa belum ada ketentuan khusus yang mengatur tentang *cybercrime* termasuk *hacking*. Oleh karena itu dalam memproses kejahatan *cyber* termasuk *hacking*, dilakukan interpretasi terhadap ketentuan yang sudah ada dalam hal ini adalah ketentuan dalam KUHP. Selain menggunakan ketentuan KUHP, ada ketentuan dalam UU lain yang dapat digunakan untuk memproses suatu kejahatan *cyber* termasuk *hacking* yaitu Undang-undang Telekomunikasi. Undang-undang Telekomunikasi mengancam pidana terhadap perbuatan: manipulasi akses ke jaringan telekomunikasi atau *ilegal access* (Pasal 50[49] jo. Pasal 22[50]); menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi atau *data interference* (Pasal 55[51] jo. Pasal 38[52]); menyadap informasi melalui jaringan telekomunikasi atau *illegal interception in the computer, systems and computer networks* (Pasal 56[53] jo. Pasal 40[54]). Pasal-pasal dalam Undang-undang Telekomunikasi yang

---

[49]Pasal 50 Undang-undang Telekomunikasi berbunyi:
"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)."

[50]Pasal 22 Undang-undang Telekomunikasi berbunyi:
"Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:
a. akses ke jaringan telekomunikasi; dan atau
b. akses ke jasa telekomunikasi; dan atau
c. akses ke jaringan telekomunikasi khusus."

[51]Pasal 55 Undang-undang Telekomunikasi berbunyi:
"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 38, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)."

[52]Pasal 38 Undang-undang Telekomunikasi berbunyi:
"Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi."

[53]Pasal 56 Undang-undang Telekomunikasi berbunyi:
"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun."

[54]Pasal 40 Undang-undang Telekomunikasi berbunyi:
"Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui

berkaitan dengan kejahatan teknologi canggih adalah sebagai berikut:

Pasal ini diterapkan dalam kasus *hacking* yang dilakukan oleh Iqra Syafaat (*hacking website* Partai Golkar) yang diadili di Pengadilan Negeri Jakarta Barat dengan putusan No. 3254/PID.B/2006/PN.JKT.BAR yang dinyatakan bersalah telah melakukan perbuatan pidana memanipulasi akses kejaringan telekomunikasi khusus (Pasal 22 huruf c Undang-undang Telekomunikasi) dan dijatuhi hukuman pidana selama satu tahun dua bulan. Sedangkan kasus Dani Firmansyah (*hacking website* KPU) yang diadili di Pengadilan Negeri Jakarta Pusat dengan putusan No: 1322/PID.B/2004/PN.JKT.PST dinyatakan bersalah telah melakukan tindak pidana tanpa hak, tidak sah memanipulasi akses jaringan telekomunikasi (Pasal 22 Undang-undang Telekomunikasi) dan dijatuhi hukuman pidana selama enam bulan dua puluh satu hari. Kedua kasus ini dinyatakan bersalah karena melanggar ketentuan dalam Undang-undang Telekomunikasi.

Indonesia tentu tidak dapat melepaskan diri dari perkembangan teknologi yang ada. Kenyataan ini menyebabkan pentingnya sebuah negara memiliki hukum yang mengatur tentang teknologi informasi atau yang dikenal dengan nama *Cyberlaw*. *Cyberlaw* yang dimaksud adalah regulasi yang mengatur hal-hal yang tidak hanya terbatas pada kegiatan *internet*, tetapi juga semua kegiatan yang memanfaatkan perangkat komputer dan instrumen elektronik lainnya. Kehadiran UU Informasi dan Transaksi Elektronik (UU ITE) diformulasikan untuk menjadi solusi untuk hal-hal semacam ini, karena UU ini secara komperehensif mengakui alat bukti elektronik sebagai perluasan alat bukti yang ada dalam hukum acara baik pidana maupun perdata, dan sebagai perluasan alat bukti dalam hukum acara yang ada pada saat ini.[55] *Cybercrime* diatur dalam Pasal 26-34 UU ITE, pasal-pasal yang mencakup kegiatan *hacking* juga termasuk di dalamnya yaitu Pasal 30 UU ITE[56]. Pelanggaran terhadap Pasal 30 UU ITE diatur dalam Pasal 46[57].

---

jaringan telekomunikasi dalam bentuk apapun."

[55]Sampai saat ini, penulis aktif terlibat dalam panitia kerja dan panitia khusus, sebagai wakil dari pemerintah Republik Indonesia untuk turut merumuskan undang-undang informasi dan transaksi elektronik (UU ITE) yang sudah disahkan DPR melalui rapat paripurna 25 Maret 2008.

[56]Pasal 30 UU ITE berbunyi:

"(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

2.3.4.3 Pengaturan Tindak Pidana *Hacking* dalam RUU

Dalam mengantisipasi penanggulangan *cybercrime* dengan hukum pidana, saat ini telah dipersiapkan berbagai RUU yang berkaitan dengan masalah *cybercrime* termasuk RUU KUHP. Berdasarkan konsep RUU KUHP tahun 2000 yang mengalami perubahan sampai dengan tahun 2004 dalam Buku I tentang Ketentuan Umum, dimasukkan beberapa perluasan pengertian dalam KUHP terutama yang dapat digunakan untuk kejahatan *hacking*. Pengertian **barang**[58] yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon/telekomunikasi/jasa komputer. Pengertian **anak kunci**[59], yang didalamnya termasuk kode rahasia, kunci masuk komputer, kartu magnetik, signal yang telah diprogram untuk membuka sesuatu. Pengertian **surat**[60] termasuk data tertulis/tersimpan dalam disket, pita magnetik, media penyimpan komputer,

---

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

[57]Pasal 46 UU ITE berbunyi:
(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

[58]Pasal 165 RUU KUHP berbunyi:
"Barang adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk aliran listrik, gas, data dan program komputer, jasa termasuk jasa telepon, jasa telekomunikasi, atau jasa komputer."

[59]Pasal 158 RUU KUHP berbunyi:
"Anak kunci adalah alat yang digunakan untuk membuka kunci, termasuk kode rahasia, kunci masuk komputer, kartu magnetik, atau signal yang telah diprogram yang dapat digunakan untuk membuka sesuatu oleh orang yang diberi hak untuk itu."

[60]Pasal 207 RUU KUHP berbunyi:
"Surat adalah surat yang tertulis di atas kertas, termasuk juga surat atau data yang tertulis atau tersimpan dalam disket, pita magnetik, atau media penyimpan komputer atau media penyimpan data elektronik lain."

atau penyimpan data elektronik lainnya. Pengertian **ruang**[61] termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu. Pengertian **masuk**[62], termasuk mengakses komputer atau masuk ke dalam sistem komputer. Pengertian **jaringan telepon**[63], termasuk jaringan komputer atau sistem komunikasi komputer. Sedangkan dalam Buku II tentang Tindak pidana, dilakukan perubahan perumusan delik atau menambah delik baru yang berkaitan dengan kemajuan teknologi dengan harapan agar ketentuan ini dapat menjaring kasus-kasus yang berkaitan dengan *cybercrime* yang terjadi. Untuk sementara dimasukkan dalam Bab VIII tentang Tindak Pidana yang Membahayakan Keamanan Umum bagi Orang, Barang, dan Lingkungan Hidup antara lain mengakses komputer tanpa hak misalnya Pasal 373 RUU KUHP[64] dimana denda yang dapat dikenakan berdasarkan Pasal 80[65] RUU KUHP paling banyak Rp

---

[61]Pasal 204 RUU KUHP berbunyi:
"Ruang adalah termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu."

[62]Pasal 186 RUU KUHP berbunyi:
"Masuk adalah termasuk mengakses komputer atau masuk ke dalam sistem komputer."

[63]Pasal 174 RUU KUHP berbunyi:
"Jaringan telepon adalah termasuk jaringan komputer atau sistem komunikasi komputer."

[64]Pasal 373 RUU KUHP berbunyi:
"Dipidana dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak Kategori IV, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik."

[65]Pasal 80 RUU KUHP berbunyi:
"(1) Pidana denda merupakan pidana berupa sejumlah uang yang wajib dibayar oleh terpidana berdasarkan putusan pengadilan.
(2) Jika tidak ditentukan minimum khusus maka pidana denda paling sedikit Rp 15.000,00 (lima belas ribu rupiah).
(3) Pidana denda paling banyak ditetapkan berdasarkan kategori, yaitu :
a. kategori I Rp 1.500.000,00 (satu juta lima ratus ribu rupiah);
b. kategori II Rp 7.500.000,00 (tujuh juta lima ratus ribu rupiah);
c. kategori III Rp 30.000.000,00 (tiga puluh juta rupiah);
d. kategori IV Rp 75.000.000,00 (tujuh puluh lima juta rupiah);
e. kategori V Rp 300.000.000,00 (tiga ratus juta rupiah); dan
f. kategori VI Rp 3.000.000.000,00 (tiga miliar rupiah).
(4) Pidana denda paling banyak untuk korporasi adalah kategori lebih tinggi berikutnya.
(5) Pidana denda paling banyak untuk korporasi yang melakukan tindak pidana yang diancam dengan :
a. pidana penjara paling lama 7 (tujuh) tahun sampai dengan 15 (lima belas) tahun adalah pidana denda Kategori V;
b. pidana mati, pidana penjara seumur hidup, atau pidana penjara paling lama 20 (dua puluh) tahun adalah pidana denda Kategori VI.

75.000.000,00 (tujuh puluh lima juta rupiah) (Arief, 2006: 95-96).

Dalam RUU Tindak Pidana di bidang Teknologi Informasi (RUU TPTI) merumuskan berapa tindak pidana dalam hal pemanfaatan teknologi informasi yaitu dari Pasal 11-12[66] dan 19, 21 dan 22[67] RUU TPTI. Dalam RUU ini, yurisdiksi hukum sebagaimana dijelaskan dalam Pasal 33 dan 34 berlaku di

---

(6) Pidana denda paling sedikit untuk korporasi sebagaimana dimaksud pada ayat (5) adalah pidana denda Kategori IV.
(7) Dalam hal terjadi perubahan nilai uang, ketentuan besarnya pidana denda ditetapkan dengan Peraturan Pemerintah."

[66]Pasal 11 RUU TPTI berbunyi:
Mengakses Tanpa Hak
"Barangsiapa dengan sengaja dan melawan hukum memasuki lingkungan dan atau sarana fisik Sistem Informasi tanpa hak atau secara tidak sah menggunakan sandi akses palsu, melakukan pembongkaran tanpa seijin pemiliknya yang sah atau perusakan dengan atau tanpa maksud merugikan pemilik sah, dipidana penjara paling singkat 2 (dua) tahun dan paling lama 4 (empat) tahun atau denda sedikit – dikitnya Rp. 200.000.000,- (dua ratus juta rupiah) dan sebanyak-banyaknya Rp. 800.000.000,- (delapan ratus juta rupiah)."
Pasal 12 RUU TPTI berbunyi:
Mengakses Tanpa Hak Terhadap Sistem Informasi Strategis
"1. Barangsiapa dengan sengaja dan melawan hukum memasuki lingkungan dan atau sarana fisik Sistem Informasi milik instansi pemerintah, militer, perbankan, atau instansi strategis lainnya tanpa hak atau secara tidak sah dengan menggunakan sandi akses palsu, melakukan pembongkaran atau perusakan dengan atau tanpa maksud merugikan instansi yang dituju, dipidana penjara paling singkat 7 (tujuh) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit-dikitnya Rp. 700.000.000,- (tujuh ratus juta rupiah) dan sebanyak-banyaknya Rp. 1.500.000.000,- (satu milyar lima ratus juta rupiah).
2. Apabila pelaku kejahatan dimaksud ayat (1) terbukti telah menyebarkan dan atau mengumumkan informasi yang harus dilindungi kepada pihak yang tidak berwenang, dipidana penjara sesuai Ayat (1), ditambah 2 (dua) tahun."

[67]Pasal 19 RUU TPTI berbunyi:
Mengakses Tanpa Hak Terhadap Komputer Yang Dilindungi
"Barangsiapa dengan sengaja dan secara melawan hukum melakukan akses melalui komputer tertentu yang statusnya dilindungi oleh pihak yang berwenang atau melanggar hak akses yang diberikan atau tidak diberikan kepadanya, dengan maksud untuk mencuri atau memperoleh sesuatu yang bukan merupakan haknya, dipidana penjara paling singkat 5 (lima) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit – dikitnya Rp. 1.000.000.000,- (satu milyar rupiah) dan sebanyak-banyaknya Rp. 2.500.000.000,-(dua milyar lima ratus juta rupiah)."
Pasal 21 RUU TPTI berbunyi:
Intersepsi
"Barangsiapa dengan sengaja dan melawan hukum melakukan intersepsi tanpa hak, secara tidak sah, atau ilegal, dipidana penjara paling singkat 2 (dua) tahun dan paling lama 5 (lima) tahun."
Pasal 22 RUU TPTI berbunyi:
Merusak Situs Internet
"1. Barangsiapa dengan sengaja terbukti merusak situs Internet milik orang atau badan hukum lain, yang menimbulkan kerugian material bagi orang atau badan hukum lain tersebut dipidana penjara paling singkat 1 (satu) tahun dan paling lama 5 (lima) tahun.
2. Apabila situs Internet yang dirusak dimaksud ayat (1) pasal ini, milik pemerintah, militer atau situs Internet lain yang termasuk dilindungi oleh pihak yang berwenang, dipidana penjara peling singkat 5 (lima) tahun dan paling lama 7 (tujuh) tahun."

seluruh wilayah Negara Kesatuan Republik Indonesia dan untuk setiap orang di luar Indonesia yang melakukan tindak pidana di bidang teknologi informasi yang akibatnya dirasakan di Indonesia.

2.3.5 Pengaturan Tindak Pidana *Hacking* di Luar Negeri

Perkembangan teknologi yang semakin pesat mengakibatkan perlu adanya pengaturan terhadapnya, terutama dalam hal terjadi penyalahgunaan teknologi. Perubahan tata hidup suatu bangsa yang ideal selalu diimbangi dengan perkembangan atau penyempurnaan peraturan perundang-undangan (hukum yang tertulis). Demikian juga halnya dengan perkembangan kejahatan di bidang komputer yang semakin merajalela, membuat aparat penegak hukum untuk berpikir mengimbanginya dengan peraturan perundang-undangan seiring dengan kuantitas kejahatan (Hamzah dan Marsita, 1990: 51).

Perbedaan tradisi hukum yang dianut oleh berbagai negara tersebut tentu saja sangat berpengaruh terhadap keragaman kebijakan pengaturan penyalahgunaan komputer, belum lagi jika dikaitkan dengan perbedaan sistem hukum pada masing-masing negara. Menurut Roeslan Saleh sebagaimana dikutip Wisnubroto (1999: 206), secara umum terdapat tiga cara penyelesaian penyalahgunaan komputer dapat dinilai dengan menggunakan tiga pendekatan yaitu *property approach*[68], *forgery approach*[69] dan *information approach*[70].

---

[68] *Property approach* adalah bentuk penilaian dengan melihat penyalahgunaan komputer sebagai suatu bagian dari delik terhadap harta kekayaan (*property*). Dengan demikian, isi inti dari catatan-catatan komputer tersebut diterjemahkan menurut nilai finansialnya. Kepentingan-kepentingan yang dikaitkan dengan penggunaan sistem komputer dimasukkan ke dalam pengertian *property*. Perlu diketahui bahwa pendekatan ini merupakan yang tertua dan paling banyak dilakukan (Wisnubroto, 1999: 206).

[69] *Forgery approach* melihat penyalahgunaan komputer terutama sebagai bagian dari delik-delik pemalsuan, di mana integritas dari keterangan-keterangan catatan komputer merupakan hal yang paling utama yang harus diperhatikan dalam suatu penyelesaian (Wisnubroto, 1999: 206).

[70] *Information approch* merupakan penyelesaian yang terutama diarahkan pada sifat dipercayainya isi dan arti dari catatan-catatan tersebut. Perbedaan latar belakang tradisi hukum dan cara pendekatan dalam penyelesaian penyalahgunaan komputer di berbagai negara secara umum dapat digambarkan dalam tiga hal, yaitu; diatur dalam sistem kodifikasi yakni dengan cara memperbaharui KUHP (*Code Penal*); memperbaharui beberapa ketentuan dalam undang-undang hukum pidana yang terkait dengan sarana amandemen; menciptakan undang-undang hukum pidana yang secara khusus mengatur masalah penyalahgunaan komputer (Wisnubroto, 1999: 206).

Untuk mencegah dan memberantas *cybercrime maka* berdasarkan Resolusi Kongress PBB ke-10 Tahun 2000, PBB menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan bahaya *cybercrime* dengan melakukan modernisasi hukum pidana materiil dan hukum pidana formil. Resolusi ini dibuat agar terjadi koordinasi antar negara di dunia untuk saling memfasilitasi, meningkatkan dan memperbaharui metode-metode khusus dalam memerangi *cybercrime* (*http://www.unejin.org/Documents/congr10/10e.pdf, 2008*).

2.3.5.1 Pengaturan Tindak Pidana *Hacking* di Inggris

Undang-undang Penyalahgunaan Komputer (*Computer Misuse Act*) yang dibuat oleh Parlemen Inggris mengatur secara spesifik tentang *hacker*. Undang-undang ini mendefinisikan penyalahgunaan komputer sebagai penggunaan yang tidak sah atas sistem komputer dan terkait juga dengan perangkat keras (penggunaan komputer tertentu tanpa izin) dan perangkat lunak (mengakses sistem komputer tanpa izin). Ada tiga tindak pidana baru terkait, yaitu: akses terhadap sistem komputer tanpa izin, modifikasi, dan penghapusan data. Penyalahgunaan komputer tidak didefinisikan secara jelas, pada umumya dijelaskan sebagai penggunaan yang keliru atas suatu sistem dan *software* komputer untuk tujuan ilegal seperti penipuan, pembuatan virus, terorisme, dan pornografi (Burdett *et al*., 1995: 91).

Inggris menganut *common law system*. Walaupun demikian, sebenarnya sistem hukum di Inggris telah berkembang sedemikian rupa hingga terlihat adanya pengaruh-pengaruh dari sistem hukum Eropa Kontinental. Pemerintah Inggris akhirnya menyadari bahwa perkembangan penyalahgunaan komputer mengikuti pesatnya perkembangan teknologi komputer sehingga merasa perlu membuat undang-undang khusus yang mengatur mengenai penyalahgunaan komputer. Salah satu persoalan rumit yang sulit dipecahkan dengan undang-undang yang ada di Inggris adalah perbuatan *hacking*. Oleh karena itu, pada bulan Oktober 1989, komisi hukum telah merekomendasikan pembuatan tiga ketentuan pidana baru. Ketentuan-ketentuan itu menyangkut persoalan tindakan-tindakan secara tidak sah dalam hubungan dengan sistem-sistem komputer, termasuk *hacking*. Rekomendasi tersebut telah dijadikan landasan dalam sebagian besar

materi Rancangan Undang-Undang Penyalahgunaan Komputer (*Computer Misuse Bill*) yang disampaikan oleh Michael Calvin MP dan memperoleh dukungan pemerintah, selanjutnya telah disahkan menjadi Undang-Undang Penyalahgunaan Komputer (*Computer Misuse Act 1990*) pada tanggal 29 Juni 1990. Tindak pidana baru yang diatur dalam undang-undang tersebut adalah *unauthorized to computer material*[71], *unauthorized access with intent to commit facilitate commission of further offences*[72], *unauthorized modification of computer material*[73] (Wisnubroto, 1999: 214-215).

2.3.5.2 Pengaturan Tindak Pidana *Hacking* di Amerika Serikat

Di Amerika Serikat, banyak negara bagian telah memiliki pengaturan mengenai kejahatan komputer yang secara umum ditegakkan oleh polisi lokal dan negara bagian. Contohnya: *Texas Panel Code Computer Crimes Section* 33.02, yang hanya mengatur satu pelanggaran yaitu *Breach of Computer Security*. Pelanggaran terhadap keamanan komputer didefinisikan sebagai secara sengaja mengakses komputer, jaringan komputer, atau sistem komputer tanpa izin dari pemilik. Hukumannya meningkat tergantung pada kerugian finansial dari pemilik sistem dan dari keuntungan penyerang. Hal serupa terdapat dalam *California Penal Code* (*Section* 502) yang mendefinisikan delapan kegiatan yang termasuk dalam kejahatan komputer. Termasuk didalamnya yaitu: *altering* (pengalihan), *damaging, deleting* (penghapusan); atau menggunakan data komputer untuk menjalankan skema penipuan, pemalsuan, pemerasan, atau secara salah

---

[71]Akses tidak sah atas suatu materi komputer *(unauthorized to computer material)* adalah perbuatan yang dapat dijatuhi hukuman penjara paling lama tiga bulan atau denda paling banyak £ 1.000, ini juga meliputi *hacking* komputer. Syarat agar seseorang dapat dipersalahkan melakukan tindak pidana ini adalah orang tersebut secara sadar mengetahui bahwa akses yang dilakukannya pada suatu sistem komputer adalah melawan hukum (Wisnubroto, 1999: 214-215).

[72]Akses tidak sah atas suatu komputer dengan tujuan melakukan atau memudahkan peleksanaan suatu tindak pidana yang lebih lanjut *(unauthorized access with intent to commit facilitate commission of further offences)*. Tindak pidana ini juga mencakup perbuatan di mana seorang *hacker* mengakses sistem komputer dengan maksud menghapus/merusak data atau bermaksud mencuri uang (Wisnubroto, 1999: 214-215).

[73]Modifikasi ilegal terhadap materi komputer *(unauthorized modification of computer material)* merupakan tindak pidana yang diancam dengan hukuman penjara paling lama lima tahun. Kententuan terhadap tindak pidana ini dibuat untuk memperkokoh dan mengkonsolidasi hukum tentang perusakan, karena berlaku terhadap program dan data komputer. Bedanya dengan kejahatan perusakan barang (sebagaimana diatur dalam *Criminal Damage Act 1971)* adalah bahwa tindak pidana ini tidak dapat disangkal dengan alasan kelalaian (Wisnubroto, 1999: 214-215).

melanggar atau menyimpan uang, properti atau data; menggunakan pelayanan komputer tanpa izin, menganggu pelayanan komputer, membantu orang lain secara melawan hukum mengakses komputer atau menyebarkan virus pada sistem atau jaringan (Shinder, 2002: 16).

KUHP negara bagian California di Amerika Serikat, sudah mencantumkan pasal-pasal baru khusus mengatur tentang kejahatan di bidang komputer. Perumusan delik komputer tercantum juga di dalam paragraf 1030 KUHP Amerika Serikat *(fraud and related activity in connection with computers)*[74]

---

[74]Paragraf 1030 KUHP Amerika Serikat adalah:

a. Barangsiapa
   (a). Dengan mengetahui mengadakan pendekatan dengan suatu komputer tanpa ijin, atau telah mengadakan pendekatan dengan sesuatu komputer dengan ijin, memakai kesempatan pendekatan itu guna tujuan-tujuan yang tidak termasuk ijin itu, dan dengan jalan perbuatan demikian mendapatkan keterangan yang telah ditentukan oleh Pemerintah Amerika Serikat sesuai dengan perintah Eksekutif atau Undang-Undang untuk dilindungi terhadap pembocoran yang tidak diijinkan untuk tujuan pertahanan nasional atau hubungan internasional atau data yang dibatasi sebagai ditentukan di dalam paragraf Pasal 11 dari Undang-Undang Tenaga Atom 1954, dengan maksud ateu alasan untuk mempercayai bahwa keterangan yang diperoleh demikian akan dipergunakan untuk merugikan Amerika Serikat atau untuk keuntungan bagi negara asing.
   (b). Dengan mengetahui mengadakan pendekatan dengan suatu komputer tanpa ijin atau telah mengadakan pendekatan dengan suatu komputer dengan ijin, memakai kesempatan pendekatan itu dipergunakan untuk tujuan-tujuan yang tidak termasuk ijin itu dan dengan itu memperoleh keterangan yang termuat didalam suatu catatan keuangan, yang keterangan-keterangan itu dirumuskan di dalam *Right to Financial Privacy Act of 1987* atau termuat di dalam berkas dari Perwakilan laporan konsumen yang hal itu ditentukan di dalam *Fair Credit Reporting Act*.
   (c). Dengan mengetahui mengadakan pendekatan dengan suatu komputer tanpa ijin, atau telah mengadakan dengan suatu komputer dengan ijin, komputer itu, jika komputer itu dioperasikan untuk atau atas nama Pemerintah Amerika Serikat dan perbuatan itu memberi efek operasi tersebut; diancam pidana sesuai ketentuan ayat (c) dari pasal ini. Tidak merupakan delik menurut paragraf (2) atau (3) dari ayat ini dalam hal seseorang telah mengadakan pendekatan dengan suatu komputer dengan ijin dan mempergunakan kesempatan pendekatan itu untuk tujuan yang tidak termasuk pendekatan itu, jika pemakaian kesempatan itu terdiri hanya dengan penggunaan komputer itu.

b.
   (a). Barangsiapa mencoba melakukan suatu delik menurut ayat (a) pasal ini diancam pidana seperti ditentukan didalam ayat (c) pasal ini.
   (b). Barangsiapa menjadi anggota komplotan yang terdiri dari dua orang atau lebih untuk melakukan suatu delik menurut ayat (a) dari pasal ini, jika seseorang dari peserta terlibat di dalam suatu perbuatan dalam melanjutkan delik tersebut, diancam pidana denda menurut jumlah tidak lebih daripada yang ditentukan sebagai maksimum denda untuk delik tersebut menurut ayat dari pasal ini atau penjara tidak lebih dari setengah jangka waktu yang ditentukan sebagai maksimum penjara untuk delik tersebut menurut ayat (c) pasal ini kedua-duanya.

c. Pidana untuk suatu delik menurut ayat (a) atau (b) (1) dari pasal ini, ialah: (1) (A) denda yang tidak lebih daripada $ 10.000.- atau dua kali jumlah yang diperoleh dengan delik itu atau

(Hamzah dan Marsita, 1990: 51).

Berdasarkan terjemahan Pasal 1030 KUHP Amerika Serikat tersebut, ada beberapa modus operandi kejahatan yang memakai komputer sebagai sarana, yaitu: memperoleh keterangan yang telah diklasifikasi oleh komputer; memperoleh keterangan keuangan atau kredit dari komputer; dan mengganggu pengoperasian suatu komputer pemerintah.

2.3.5.3 Pengaturan Tindak Pidana *Hacking* di Hong Kong

Berdasarkan wawancara terhadap informan dari Hong Kong, yang berwenang memproses kasus *cybercrime* termasuk *hacking* adalah suatu unit khusus dalam Kepolisian Hong Kong yang bernama *Technology Crime Division* (*TCD*). *Hacking* didefinisikan sebagai "*unauthorized access to computer by telecommunications*" atau "*access to computer with criminal or dishonest intent*". *Hacking* dianggap perbuatan yang dilarang ketika *hacker* memperoleh akses ke suatu komputer tanpa adanya kewenangan berdasarkan hukum atau alasan yang kuat. Cara inilah yang digunakan oleh pelaku tindak pidana untuk memperoleh infromasi dari korban untuk memperoleh uang atau tujuan lain untuk digunakan

---

penjara tidak lebih dari sepuluh tahun, atau keduanya, dalam hal suatu delik menurut ayat (a) (1) dari pasal ini yang tidak terjadi sesudah pemidanaan untuk delik lain menurut pasal ini, atau suatu percobaan untuk melakukan suatu delik yang dapat dipidana menurut ayat ini; dan (b) denda yang tidak lebih dari $ 100.000 atau dua keli jumlah nilai yang diperoleh dengan delik itu atau penjara yang tidak lebih dari dua puluh tahun, atau keduanya dalam hal delik menurut ayat (a) (1) pasal ini yang terjadi sesudah pemidanaan untuk delik lain menurut ayat tersebut, atau suatu percobaan untuk melakukan suatu delik yang dapat dipidana menurut ayat ini; dan (2) (A) denda yang tidak lebih dari $5.000.- atau dua kali nilai yang diperoleh atau kerugian yang ditimbulkan oleh delik tersebut atau penjara yang tidak lebih dari sepuluh tahun, atau kedua-duanya, dalam hal delik menurut ayat (a) (2) atau (a) (3) dari ayat ini yang tidak terjadi sesudah suatu pemidanaan untuk delik lain menurut ayat tersebut, atau suatu percobaan untuk melakukan suatu delik yang dapat dipidana menurut butir ini; dan (B) denda tidak lebih dari $10.000.- atau dua kali nilai yang diperoleh atau kerugian yang ditimbulkan oleh delik tersebut atau penjara yang tidak lebih dari sepuluh tahun, atau kedua-duanya, dalam hal suatu delik menurut ayat (a) (2) atau (a) (3) dari pasal ini yang terjadi sesudah suatu pemidanaan untuk delik lain menurut ayat tersebut atau suatu percobaan untuk melakukan suatu delik yang dapat dipidana menurut butir ini.

d. *Secret Service* Amerika Serikat akan mempunyai wewenang untuk menyidik delik-delik menurut pasal ini, sebagai tambahan pada suatu badan lain yang mempunyai wewenang demikian. Wewenang demikian dari *Secret Service* Amerika Serikat, akan dilaksanakan sesuai dengan suatu persetujuan yang akan diadakan oleh Menteri Keuangan dan Jaksa Agung.

e. Sebagaimana yang dipergunakan menurut pasal ini istilah "komputer" berarti *processing* data yang sangat cepat yang elektronik, magnetik, optikal, elektro kimia, atau *processing* data yang sangat cepat yang lain, yang dimaksudkan untuk fungsi penciptaan logik, arismatik atau penyimpanan dan meliputi fasilitas penyimpanan data atau fasilitas komunikasi yang langsung berkaitan untuk pengoperasian bagi tujuan tersebut. Tetapi istilah tersebut tidak meliputi mesin tik otomatis atau mesin *setter*, kelkulator *portable*, atau tujuan-tujuan yang sama.

dalam kegiatan ilegal lainnya. Oleh karena itu sangat penting tindak pidana *hacking* diatur dalam suatu peraturan. Tindak pidana yang diatur dalam hukum di Hong Kong adalah:

a. Bagian 27A, *Telecommunications Ordinance*, bab 106 berupa akses tidak sah terhadap komputer melalui telekomunikasi (*Unauthorized access to computer by telecommunications)*, denda 20.000 dollar Hong Kong.
b. Bagian 59-60, *Crimes Ordinance*, bab 200 yaitu menghancurkan atau merusak barang – perluasan arti "barang" termasuk "penyalahgunaan komputer" seperti mengubah, menghapus dan menambah program atau data ke dalam suatu komputer atau media penyimpanan komputer serta menyebabkan suatu komputer tidak berfungsi sebagaimana mestinya, ancaman pidana 10 tahun penjara.
c. Bagian 85, *Crimes Ordinance*, bab 200, perluasan arti membuat akses palsu untuk memalsukan buku rekening yang disimpan di bank manapun dalam bentuk elektronik dan lain-lain, ancaman pidana penjara seumur hidup.

2.3.5.4 Pengaturan Tindak Pidana *Hacking* di Council of Europe

Negara-negara yang tergabung dalam Dewan Eropa (Council of Europe)[75] pada tanggal 23 November 2001 di kota Budapest, Hongaria telah membuat dan menyepakati *Convention on Cybercrime*[76] yang kemudian dimasukkan dalam *European Treaty Series* dengan nomor 185. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal (*criminal policy*) yang bertujuan untuk melindungi masyarakat dari *cybercrime,* baik melalui undang-

---

[75]Council of Europe (CoE) adalah organisasi internasional yang berdiri sejak 1949, dan berkedudukan di Strasbourg. Tujuannya adalah menegakkan supremasi hukum, demokrasi dan untuk berjuang demi kepentingan negara-negara Eropa. CoE berbeda dengan European Union. Dalam hal keanggotaan, CoE memiliki 47 negara anggota dan 5 negara pengawas (Kanada, Kosta Rika, Jepang, Meksiko, Afrika Selatan dan Amerika Serikat). Sedangkan EU memiliki 25 negara anggota. Dalam hal perjanjian juga berbeda dimana perjanjian yang dihasilkan dalam CoE tidak otomatis mengikat negara anggota tetapi tergantung apakah mereka meratifikasinya atau tidak sedangkan EU sebaliknya. Pada tahun 1980, dua organisasi ini saling berbagi bendera dan lagu kebangsaan yang sama. Hal ini tidak terlepas dari sejarah perjuangan masing-masing organisasi untuk integrasi Eropa (*http://en.wikipedia.org/wiki/Council_of_europe*, 2008).

[76]Sampai saat ini, konvensi ini telah diratifikasi oleh 22 negara yaitu Albania, Armenia, Bosnia Herzegovina, Bulgaria, Kroasia, Siprus, Denmark, Estonia, Finlandia, Prancis, Hungaria Islandia, Latvia, Lithuania, Belanda, Norwegia, Rumania, Slowakia, Slovenia, Republik Macedonia, Ukraina dan Amerika Serikat (*http://conventions.coe.int/Treaty/Commun/ ChercheSig.asp?NT=185&CM=&DF=&CL=ENG*, 2008).

undang maupun kerjasama internasional. Hal ini dilakukan dengan penuh kesadaran sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi, yang menurut pengalaman *Prinsip-Prinsip Cyber Law dan Kendala Hukum Positif dalam Menanggulangi Cybercrime* dapat juga digunakan untuk melakukan tindak pidana (Ahmad M. Ramli, 2005: 8-9).

Konvensi ini telah disepakati oleh negara anggota Council of Europe sebagai konvensi yang terbuka untuk diakses oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrumen Hukum Internasional dalam mengatasi kejahatan *cyber*, tanpa mengurangi kesempatan setiap individu untuk tetap mengembangkan kreativitasnya dalam mengembangkan teknologi informasi. Dalam *Convention on Cybercrime* yang dibuat oleh Council of Europe, terdapat pengaturan mengenai *cybercrime* yaitu:

a. Tindak pidana yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer (*offences against the confidentiality, integrity and availability of computer data and systems*)
   (a). Pasal 2 – melakukan akses tidak sah (*illegal access*)
   (b). Pasal 3 – intersepsi secara ilegal (*illegal interception*)
   (c). Pasal 4 – mengganggu data (*data interference*)
   (d). Pasal 5 – mengganggu sistem (*system interference*)
   (e). Pasal 6 – penyalahgunaan alat (*misuse of devices*)
b. Tindak pidana yang berkaitan dengan komputer (*computer-related offences*)
   (a). Pasal 7 - pemalsuan melalui komputer *(computer-related forgery*)
   (b). Pasal 8 - penipuan melalui komputer *(computer-related fraud*)
c. Tindak pidana yang berhubungan dengan isi atau muatan data atau sistem komputer (*content-related offences)*, yaitu diatur dalam Pasal 9 tindak pidana yang berkaitan dengan pornografi anak (*offences related to child pornography*).
d. Tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait (*offences related to infringements of copyright and related rights*).

BAB III

MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING*

3.1 Penyidikan Tindak Pidana

Sebagai salah satu unsur dalam *Criminal Justice System* (CJS)[77], Polri sebagai alat negara penegak hukum, pelindung dan pengayom masyarakat berkewajiban untuk memelihara tegaknya hukum, keadilan dan perlindungan terhadap harkat dan martabat manusia, serta ketertiban dan kepastian hukum. Berkaitan dengan fungsinya sebagai penegak hukum, Polri melakukan tugas penyidikan tindak pidana. Tugas-tugas penyidikan tindak pidana dalam rangka penegakan hukum tersebut dijalankan oleh penyidik atau penyidik pembantu baik oleh fungsi reserse maupun fungsi operasional Polri lainnya dan Penyidik Pegawai Negeri Sipil (PPNS) yang diberi wewenang untuk melakukan penyidikan. Penyidikan tindak pidana pada hakekatnya merupakan wujud penegakan hukum yang diatur dalam perundang-undangan mengingat tugas-tugas penyidikan tindak pidana banyak berkaitan dengan hal-hal yang menyangkut hak-hak azasi manusia.

Berdasarkan Juklak Tentang Proses Penyidikan Tindak Pidana Mabes Polri, kegiatan-kegiatan pokok dalam rangka penyidikan tindak pidana dapat terdiri dari: **penyidikan tindak pidana**[78] yang meliputi kegiatan penyelidikan, penindakan (pemanggilan, penangkapan, penahanan, penggeledahan, dan penyitaan), pemeriksaan (saksi, ahli dan tersangka), penyelesaian dan penyerahan

---

[77]Menurut Muladi (1995), sebagaimana dikutip oleh Irsan (April-September 2000: 6), Sistem Peradilan Pidana (SPP) atau *CJS* adalah suatu pendekatan sistem dalam prosedur penanganan perkara pidana yang diwujudkan dalam bentuk *input-through output* atau keluaran untuk memelihara dan meningkatkan efisiensi prosedur antara lembaga-lembaga *CJS*.

[78]Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tindak pidana yang terjadi dan guna menemukan tersangkanya (Pasal 1 angka 1 KUHAP).

berkas perkara (pembuatan resume, penyusunan berkas perkara dan penyerahan berkas perkara); **dukungan teknis penyidikan**; **administrasi penyidikan**; serta **pengawasan dan pengendalian penyidikan.**

Dalam pelaksanaannya, penyidikan tindak pidana yang menjadi tugas Polri banyak menghadapi tantangan yang bersifat krusial selama proses penyidikan diantaranya adalah masalah perbedaan penafsiran tentang kewenangan penyidikan/yurisdiksi; masalah perbedaan penafsiran penerapan undang-undang serta kasus-kasus tertentu yang memerlukan perhatian; masalah-masalah lain yang menyangkut teknis pelaksanaan penyidikan seperti kurang memadainya dukungan personil, logistik maupun anggaran serta hal-hal yang menyangkut faktor-faktor yang berpengaruh dalam proses penyidikan, diantaranya pengaruh intervensi baik secara formal struktural maupun secara informal dari luar struktur Polri terhadap konsistensi dan indepensi dari para penyidik yang bertugas.

Bagan 3.1
Kegiatan-Kegiatan Pokok Dalam Rangka Penyidikan Tindak Pidana

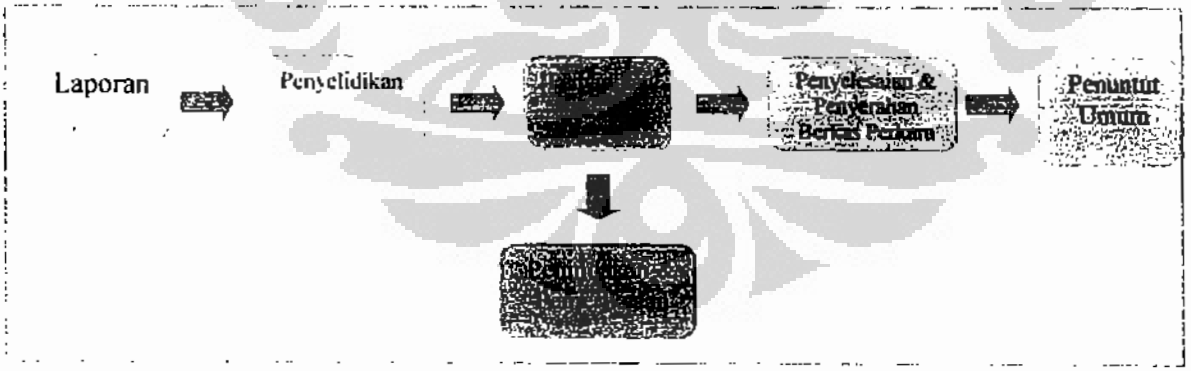
(Sumber: Penulis)

3.1.1 Rangkaian Kegiatan Penyidikan Tindak Pidana

Berdasarkan Petunjuk Pelaksanaan (Juklak) Tentang Proses Penyidikan Tindak Pidana" (Mabes Polri, 2001: 10-28), rangkaian proses penyidikan tindak

pidana[79] terdiri dari proses penyelidikan tindak pidana, penindakan tindak pidana, dan pemeriksaan tindak pidana serta penyelesaian dan penyerahan berkas perkara. Penyidikan tindak pidana dilaksanakan setelah diketahui bahwa suatu peristiwa yang terjadi merupakan tindak pidana. Suatu tindak pidana dapat diketahui melalui adanya laporan, pengaduan, dan keadaan tertangkap tangan. Dalam hal petugas polisi yang berwenang telah menerima penyerahan tersangka beserta atau tanpa barang bukti baik dari anggota polisi maupun dari masyarakat, maka yang bersangkutan wajib membuat laporan polisi, mendatangi Tempat Kejadian Perkara (TKP) dan melakukan tindakan yang diperlukan serta membuat Berita Acara atas setiap tindakan yang dilakukan. Dalam hal suatu tindak pidana diketahui langsung oleh petugas polisi maka petugas polisi tersebut wajib melakukan tindakan-tindakan sesuai kewenangan masing-masing, kemudian membuat LP dan atau Berita Acara tentang tindakan-tindakan yang dilakukannya, guna penyelesaian selanjutnya. Setelah diketahui bahwa suatu peristiwa yang terjadi diduga atau merupakan tindak pidana, maka pejabat polisi yang berwenang wajib segera melakukan penyidikan melalui kegiatan-kegiatan penyelidikan, penindakan, pemeriksaan serta penyelesaian dan penyerahan berkas perkara (Mabes Polri, 2001: 10-11).

Bagan 3.2
Proses Penyidikan Tindak Pidana



(Sumber: Penulis)

[79]Penyidikan tindak pidana adalah proses untuk menemukan, mengumpulkan, mengidentifikasi, menyiapkan, menganalisa dan mempresentasikan bukti, baik langsung maupun tidak langsung dengan suatu kejadian tindak pidana, untuk membuktikan suatu kebenaran atau kesalahan secara hukum (Axelrod dan Antinozzi, 2003: 8).

Sumber hukum pelaksanaan penyidikan tindak pidana adalah KUHAP. Dalam pelaksanaannya, Polri menerbitkan himpunan Petunjuk Pelaksanaan (Juklak) dan Petunjuk Teknis (Juknis) mengenai proses penyidikan tindak pidana, yang ditetapkan dalam Surat Keputusan Kapolri. Selanjutnya diterbitkan pula Buku Petunjuk Lapangan (Juklap) dan Buku Petunjuk Administrasi (Juknis) berdasarkan Surat Keputusan Kapolri, yang berisi petunjuk pelaksanaan lapangan meliputi penjabaran tentang proses penyidikan tindak pidana dan administrasi penyidikan tindak pidana, yang merupakan pedoman dan petunjuk bagi para penyidik/penyidik pembantu dalam rangka pelaksanaan penyidikan tindak pidana. Berikut akan diuraikan mengenai proses dan prosedur penyidikan tindak pidana yang dilakukan oleh polisi dengan berdasarkan pada KUHAP maupun Bujuklak, Bujuknis, dan Bujuklap yang berlaku saat ini dalam lingkungan Polri.

3.1.1.1 Penyelidikan Tindak Pidana

Menurut Yahya Harahap (2006: 101-102), penyelidikan[80] merupakan tindakan tahap pertama permulaan penyidikan namun bukan tindakan sendiri yang terpisah dari fungsi penyidikan. Penyelidikan bertujuan untuk mengumpulkan bukti permulaan atau bukti yang cukup agar dapat dilakukan tindak lanjut penyidikan.

Penyelidik[81] dalam hal ini kepolisian, memegang peranan penting dalam usaha menemukan suatu peristiwa yang diduga merupakan tindak pidana, dimana hasil dari penemuannya akan sangat menentukan sikapnya apakah peristiwa yang ditemukan tersebut dapat dilakukan penyidikan atau tidak. Pelaksanaan kegiatan penyelidikan dapat dilaksanakan secara optimal apabila petugas penyelidik senantiasa memperhatikan syarat dan teknik maupun sasaran penyelidikan secara benar sebagaimana diatur dalam KUHAP dan Juklap tentang Penyelidikan yang

---

[80]Menurut Pasal 1 angka 5 KUHAP, yang dimaksud dengan penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang.

[81]Penyelidik menurut Pasal 1 angka 4 KUHAP adalah pejabat Polisi Negara Republik Indonesia yang diberi wewenang oleh undang-undang untuk melakukan penyelidikan.

berlaku dalam lingkungan Polri berdasarkan Surat Keputusan Kapolri.

Kewenangan yang dimiliki oleh penyelidik menurut Pasal 5 KUHAP bersumber baik dari jabatannya[82] maupun dari perintah penyidik[83]. Selain itu dalam Pasal 5 huruf b angka 4 KUHAP, bahwa kewenangan penyelidik berdasarkan jabatannya yang lain adalah kewenangan untuk mengadakan **tindakan lain** menurut hukum yang bertanggung jawab. Yang dimaksud dengan "tindakan lain" dari kalimat tersebut menurut penjelasan Pasal 5 angka 4 KUHAP adalah tindakan dari penyelidik untuk kepentingan penyelidikan, dengan syarat tindakan tersebut tidak bertentangan dengan suatu aturan hukum; tindakan tersebut harus selaras dengan kewajiban hukum yang mengharuskan dilakukannya suatu tindakan jabatan; tindakan tersebut harus patut dan masuk akal dan termasuk dalam lingkungan jabatannya; dan atas pertimbangan yang layak berdasarkan keadaan memaksa; serta tetap menghormati hak asasi manusia. Kewenangan penyelidik yang bersumber dari perintah penyidik berdasarkan Pasal 5 KUHAP, terbatas pada apa yang dituangkan dalam perintah penyidik sehingga penyelidik dalam melaksanakan kewenangannya ini merupakan perpanjangan kewenangan dari penyidik.

Proses penyelidikan dilaksanakan oleh polisi baik berdasarkan laporan atau pengaduan yang diterima maupun diketahui langsung oleh penyelidik/penyidik; LP; Berita Acara Pemeriksaan di TKP; atau Berita Acara Pemeriksaan tersangka dan/atau saksi (Mabes Polri, 2001: 11). Dalam prakteknya pelaksanaan penyelidikan bukanlah suatu hal yang mudah, karena untuk dapat mencapai tujuan dan sasaran penyelidikan yang telah ditargetkan, diperlukan penyelidik yang memiliki kemampuan yang telah terlatih secara baik, dan menguasai teknik-teknik penyidikan secara baik. Untuk itu, pembinaan dan pelatihan terhadap para penyelidik juga memegang peranan penting terhadap kesuksesan suatu proses

---

[82]Kewenangan yang berdasarkan pada jabatannya menurut Pasal 5 huruf a KUHAP, meliputi wewenang untuk menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana; mencari keterangan dan barang bukti; menyuruh berhenti seseorang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri; dan mengadakan tindakan lain menurut hukum yang bertanggung jawab.

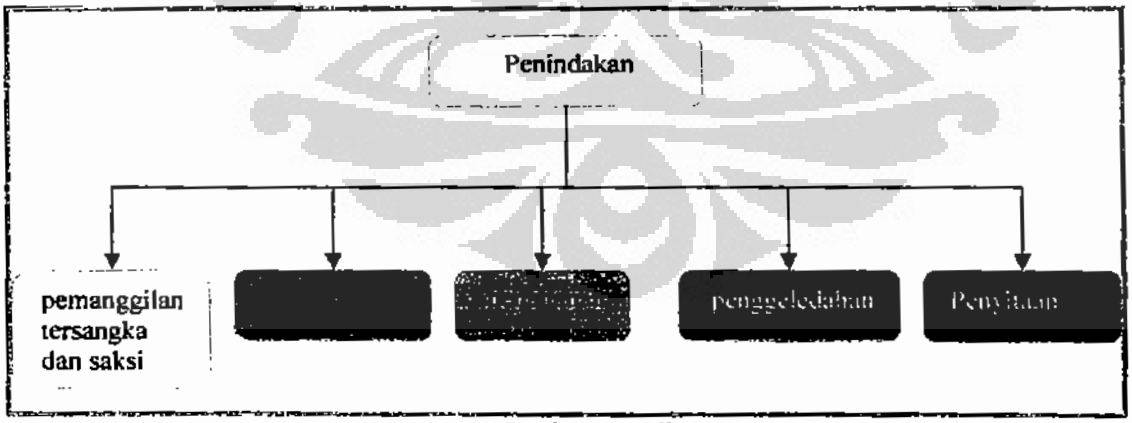
[83]Kewenangan yang diberikan oleh penyidik berdasarkan suatu perintah penyidik menurut Pasal 5 huruf b KUHAP, berupa penangkapan, larangan meninggalkan tempat, penggeledahan dan penyitaan; pemeriksaan dan penyitaan surat; pengambilan sidik jari dan pemotretan seseorang; ataupun membawa dan menghadapkan seseorang kepada penyidik.

penyelidikan. Mengingat penyelidikan biasanya dilakukan terhadap kasus-kasus yang membahayakan atau terhadap kasus yang melibatkan kejahatan terorganisasi, yang seringkali sudah mengantisipasi kegiatannya agar tidak tercium oleh penegak hukum atau polisi, maka penyelidikan terhadapnya pun memerlukan kemampuan dan keterampilan yang handal dan telah dipersiapkan, direncanakan, ditargetkan serta dilaksanakan dan dikoordinasikan secara cermat.

3.1.1.2 Penindakan Tindak Pidana

Penindakan[84] adalah setiap tindakan hukum yang dilakukan oleh penyidik/penyidik pembantu terhadap orang maupun benda/barang yang ada hubungannya dengan tindak pidana yang terjadi (Mabes Polri, 2001: 13). Pada prinsipnya, penindakan merupakan upaya paksa dalam kegiatan penyidikan tindak pidana, meliputi kegiatan untuk melakukan pemanggilan, penangkapan, penahanan, penggeledahan dan penyitaan. Kegiatan-kegiatan dalam penindakan pada dasarnya membatasi kebebasan atau hak-hak seseorang dan perannya dalam pelaksanaannya harus memperhatikan norma-norma hukum dan ketentuan-ketentuan yang mengatur atas tindakan tersebut. Pada dasarnya sumber hukum pelaksanaan penindakan adalah KUHAP dan Undang Undang Kepolisian yang berlaku.

Bagan 3.3
Kegiatan dalam Proses Penindakan Tindak Pidana



(Sumber: Penulis)

[84]Menurut buku "Petunjuk Lapangan tentang Penindakan" (Mabes Polri, 2001: 178), penindakan dalam rangka penyidikan tindak pidana dapat digolongkan menjadi pemanggilan tersangka dan saksi, penangkapan, penahanan, penggeledahan dan penyitaan. Tindakan-tindakan hukum tersebut hanya dapat dilakukan oleh pihak yang berwenang, dalam hal ini adalah kepala kesatuan atau pejabat yang ditunjuk selaku penyidik/penyidik pembantu.

a. Pemanggilan Tersangka dan Saksi

Yang dimaksud dengan pemanggilan adalah tindakan penyidik untuk menghadirkan saksi[85] atau tersangka[86] guna didengar keterangannya sehubungan dengan tindak pidana yang terjadi (Mabes Polri, 2001: 176). Pemanggilan tersangka dan atau saksi untuk didengar keterangannya dilakukan dengan mempertimbangkan hal-hal sebagai berikut yaitu: **Pertama**, bahwa seseorang mempunyai peranan sebagai tersangka atau saksi dalam suatu tindak pidana yang telah terjadi dimana peranannya itu dapat diketahui dari laporan polisi, pengembangan hasil pemeriksaan yang dituangkan dalam Berita Acara Pemeriksaan; dan Laporan Hasil Penyelidikan. **Kedua**, untuk melengkapi keterangan-keterangan, petunjuk-petunjuk dan bukti-bukti yang sudah didapatkan tetapi dalam hal tertentu masih terdapat beberapa kekurangan. **Ketiga**, adanya permintaan bantuan dari penyidik/penyidik pembantu ke kesatuan lain/di luar daerah hukum agar seseorang diperiksa sebagai tersangka dan/atau saksi atau permintaan bantuan untuk kepentingan pemeriksaan melalui Interpol (Mabes Polri, 2001: 178-179).

b. Penangkapan

Pengertian penangkapan menurut pasal 1 angka 20 KUHAP adalah suatu tindakan penyidik berupa pengekangan sementara waktu kebebasan tersangka atau terdakwa apabila terdapat cukup bukti guna kepentingan penyidikan atau penuntutan dan/atau peradilan dalam hal serta menurut cara yang diatur dalam undang-undang. Berdasarkan ketentuan tersebut, penyidik memiliki wewenang untuk mengurangi kebebasan dan hak asasi seseorang akan tetapi hal itu harus dilakukan berdasarkan landasan hukum dan untuk kepentingan pemeriksaan dan sangat diperlukan (Yahya Harahap, 2006: 157). Berdasarkan Pasal 17 KUHAP, perintah penangkapan hanya dapat dilakukan terhadap seseorang yang diduga keras telah melakukan tindak pidana berdasarkan bukti permulaan[87] yang cukup.

---

[85]Saksi menurut Pasal 1 angka 26 KUHAP adalah orang yang dapat memberikan keterangan guna kepentingan penyidikan, penuntutan dan peradilan tentang suatu perkara pidana yang didengar, dilihat, dan dialami sendiri.

[86]Tersangka menurut Pasal 1 angka 14 KUHAP, adalah seorang yang karena perbuatannya atau keadaannya berdasarkan bukti permulaan patut diduga sebagai pelaku tindak pidana.

[87]Mengenai bukti permulaan yang cukup sebagai alasan untuk melakukan penangkapan

Menurut Dan Montgomery dalam artikelnya "*Excessive Force 101*" (FBI *Law Enforcement Bulletin*, Agustus 2005: 9), dalam melakukan penangkapan ketika aparat penegak hukum melihat kemungkinan untuk melakukan upaya paksa, mereka dapat melakukan program "*use-of-force spectrum*". Mencakup lima tingkat alternatif penggunaan upaya paksa agar tersangka bersedia memenuhi perintah aparat ketika terjadi penangkapan. Pertama adalah membujuk seseorang untuk melakukan sesuatu misal menyuruh seseorang untuk tetap di dalam kendaraannya. Kedua, mendapatkan pemenuhan perintah atas tersangka dan adanya kontak fisik misalnya menyuruh seseorang untuk membawa barang dari titik A ke titik B dimana perintah itu dia lakukan. Ketiga, memperoleh pemenuhan dan kendali dengan menggunakan teknik atau alat pengontrol seperti borgol. Keempat, membela diri baik sendiri maupun dengan bantuan petugas lain dan penggunaan senjata misal fisik (tangan, kaki) dan pistol berpeluru karet.

---

masih terdapat perbedaan pendapat di antara para penegak hukum. Oleh karena itu, di bawah ini akan dikemukakan beberapa pendapat mengenai "bukti permulaan" itu (Prinst, 1998: 50-52).

Menurut Kapolri, dalam Surat Keputusan No. Pol. SKEEP/04/I/1982, tanggal 18 Februari 1982 menentukan bahwa bukti permulaan yang cukup itu adalah bukti yang merupakan keterangan dan data yang terkandung di dalam dua diantara berikut ini: Laporan Polisi; Berita Acara Pemeriksaan di TKP; Laporan Hasil Penyelidikan; Keterangan Saksi/Ahli; dan Barang Bukti (Prinst, 1998: 50-51).

Menurut Drs. P. A. F. Lamintang, SH dalam bukunya Kitab Undang-undang Hukum Acara Pidana mengatakan bahwa bukti yang cukup dalam rumusan Pasal 17 KUHAP itu harus diartikan sebagai "bukti-bukti minimal", berupa alat-alat bukti seperti yang dimaksud dalam Pasal 184 ayat 1 KUHAP, yang dapat menjamin bahwa penyidik tidak akan menjadi terpaksa untuk menghentikan penyidikannya terhadap seseorang yang disangka melakukan tindak pidana setelah terhadap orang tersebut dilakukan penangkapan (Prinst, 1989: 52).

Menurut Rapat Kerja Mahkamah Agung-Kehakiman-Kejaksaan-Polisi (MAKEHJAPOL) tanggal 21 Maret 1984 menyimpulkan bahwa bukti permulaan yang cukup setidaknya minimal LP ditambah salah satu alat bukti lainnya Prinst (1989: 52).

Menurut Pengadilan Negeri Sidikalang, melalui penetapannya No. 4/Pred-Sdk/1982, tanggal 14 Desember menyatakan bahwa penyidik berwenang untuk melakukan penangkapan dan penahanan sejauh tindakan itu dilakukan dalam batas-batas ketentuan Pasal 17 dan 21 ayat (1) KUHAP, yaitu penangkapan berdasarkan bukti permulaan yang cukup dan penahanan berdasarkan bukti yang cukup dan tentu saja bukti permulaan yang cukup dan bukti yang cukup tersebut ada terlebih dahulu sebelum diadakannya penangkapan dan penahanan. Bahwa bukti permulaan yang cukup dan bukti yang cukup dikemukakan di atas kiranya tidak merupakan dan tidak termasuk salah satu alat bukti yang disebutkan dalam Pasal 184 KUHAP, dan menurut pengadilan negeri hal tersebut sebagai bukti lebih merupakan informasi untuk mengusut sebagai alat bukti yang memberikan dugaan keras bahwa pemohon telah melakukan tindak pidana pemerkosaan dan pembunuhan. Penangkapan dan penahanan atas diri pemohon adalah tanpa alasan yang berdasarkan undang-undang. Dari penetapan pengadilan negeri Sidikalang ini dapat disimpulkan bahwa "bukti permulaan yang cukup" itu haruslah mengenai alat-alat bukti yang diatur dalam Pasal 184 ayat (1) KUHAP bukan yang lain-lainnya, seperti laporan polisi dan lain-lain (Prinst, 1989: 52).

c. Penahanan

Berdasarkan Juklap Tentang Penindakan, penahanan[88] terhadap tersangka dapat dilakukan dengan pertimbangan bahwa berdasarkan hasil pemeriksaan, tersangka diduga keras telah melakukan/percobaan melakukan/membantu melakukan tindak pidana dengan bukti yang cukup dan atau adanya keadaan yang menimbulkan kekhawatiran bahwa tersangka akan melarikan diri, merusak atau menghilangkan barang bukti dan atau akan mengulangi tindak pidana (Mabes Polri, 2001: 193-194).

Jenis-jenis penahanan menurut Pasal 22 ayat 1 KUHAP adalah penahanan di Rumah Tahanan Negara (Rutan), penahanan rumah, dan penahanan kota. Menurut Juklap Tentang Penindakan (Mabes Polri, 2001: 199), jenis penahanan dapat dialihkan, dengan pertimbangan bahwa dalam hal pemeriksaan terhadap tersangka telah selesai dan tidak dikhawatirkan tersangka akan melarikan diri serta tidak menyulitkan dalam pengawasannya, keadaan/kondisi kesehatan tersangka yang memerlukan perawatan dokter (rawat jalan), dan/atau kehadiran tersangka sangat diperlukan oleh masyarakat karena profesi atau keahliannya.

d. Penggeledahan

Menurut Juklap Tentang Penindakan (Mabes Polri, 2001: 206-215), tindakan penggeledahan dilakukan baik terhadap badan, rumah, atau tempat-tempat tertutup yang bertujuan untuk mendapatkan bukti-bukti dan atau barang bukti, serta untuk melakukan tindakan-tindakan penangkapan terhadap tersangka. Penggeledahan rumah berdasarkan pasal 1 angka 17 KUHAP adalah suatu tindakan dari penyidik untuk memasuki rumah tempat tinggal dan tempat tertutup lainnya untuk melakukan pemeriksaan dan/atau penyitaan dan/atau penangkapan, sesuai dengan undang-undang. Sedangkan penggeledahan badan berdasarkan pasal 1 angka 18 KUHAP adalah suatu tindakan dari penyidik untuk mengadakan pemeriksaan badan atau pakaian tersangka untuk mencari benda yang diduga keras ada pada badannya atau dibawanya serta untuk disita. Untuk melakukan penggeledahan rumah atau tempat tertutup atau penggeledahan badan, maka penyidik sesuai ketentuan pasal 33 KUHAP harus dengan izin Ketua Pengadilan

---

[88]Menurut Pasal 1 angka 21 KUHAP, penahanan adalah penempatan tersangka atau terdakwa di tempat tertentu oleh penyidik atau penuntut umum atau hakim dengan penetapannya, dalam hal serta menurut cara yang diatur dalam undang-undang.

Negeri. Namun dalam **keadaan yang sangat perlu atau mendesak**[89], penyidik dapat melakukan penggeledahan tanpa mendapat surat izin terlebih dahulu dari Ketua Pengadilan Negeri. Penggeledahan yang dilakukan dapat meliputi penggeledahan halaman dan rumah, tempat lain dimana tersangka tinggal atau berdiam, tempat tindak pidana dilakukan/ada berkasnya dan tempat penginapan/tempat lainnya.

e. Penyitaan

Menurut Juklap tentang Penindakan (Mabes Polri, 2001: 216-224), penyitaan[90] dilakukan dengan pertimbangan bahwa diperlukan barang bukti yang ada kaitannya dengan kasus/tindak pidana yang terjadi untuk pembuktian kasus, dan diperlukan persyaratan kelengkapan berkas perkara guna pembuktian dalam proses penyidikan, penuntutan dan peradilan.

Tujuan dilakukannya penyitaan[91] lebih untuk kepentingan pembuktian. Tanpa barang bukti, penyidik akan kesulitan untuk membangun kasus yang sedang disidiknya. Penyitaan terhadap barang bukti dilakukan agar dapat dipergunakan sebagai bukti dalam penyidikan, penuntutan maupun pengadilan. Permasalahan yang sering kali muncul dalam proses penyitaan bukti adalah dalam hal bukti yang akan disita bukan milik si tersangka, misalnya mobil curian, dimana si tersangka menguasai mobil tersebut yang merupakan hasil kejahatan pencurian yang dilakukan. Penyitaan terhadap mobil tersebut akan sangat mengganggu hak si pemilik mobil yang sah. Dalam kehidupan sehari-hari,

---

[89]Menurut Prinst (1989: 68), yang dimaksud dengan keadaan sangat perlu atau mendesak adalah bilamana di tempat yang akan digeledah diduga keras terdapat tersangka atau terdakwa, yang dikhawatirkan segera melarikan diri atau mengulangi tindak pidana, atau benda yang dapat disita dikhawatirkan segera dimusnahkan atau dipindahkan, sedangkan surat izin dari Ketua Pengadilan Negeri tidak mungkin diperoleh dengan cara yang layak dan dalam waktu yang singkat.

[90]Menurut pasal 1 angka 16 KUHAP, penyitaan adalah serangkaian tindakan penyidik untuk mengambil alih dan atau menyimpan di bawah penguasaannya benda bergerak atau tidak bergerak, berwujud atau tidak berwujud untuk kepentingan pembuktian dalam penyidikan, penuntutan dan peradilan.

[91]Menurut M. Yahya Harahap (2006: 265), penyitaan dalam pengertian hukum acara pidana yang digariskan KUHAP adalah "upaya paksa" yang dilakukan penyidik untuk mengambil atau katakan saja "merampas" sesuatu barang tertentu dari seorang tersangka, pemegang atau penyimpan. Tetapi perampasan yang dilakukan dibenarkan oleh hukum dan dilaksanakan menurut aturan Undang-undang, bukan perampasan liar dengan cara yang melawan hukum (*wederechtelyk*). Setelah barangnya diambil atau dirampas oleh penyidik, ditaruh atau disimpan di bawah kekuasaannya.

masalah ini seringkali meresahkan masyarakat yang merupakan korban kejahatan, karena barang yang seharusnya dapat dinikmati harus disita untuk kepentingan penyidikan, penuntutan ataupun proses pembuktian di pengadilan.

3.1.1.3 Pemeriksaan Tindak Pidana

Pemeriksaan merupakan salah satu kegiatan penyidik untuk mendapatkan keterangan, kejelasan dan keidentikan baik tersangka, saksi-saksi/ahli, maupun tentang tindak pidana yang terjadi serta pemenuhan unsur-unsurnya sehingga wajib dilaksanakan dengan menjunjung tinggi hukum yang berlaku serta senantiasa memperhatikan hak-hak azasi manusia. Kemudian hasilnya dituangkan dalam Berita Acara Pemeriksaan ("BAP"), yang berpedoman pada syarat-syarat pemeriksaan dan sesuai dengan perundang-undangan/hukum yang berlaku Menurut Juklap Tentang Pemeriksaan, pemeriksaan adalah kegiatan untuk mendapatkan keterangan, kejelasan, dan keidentikan tersangka, ahli dan atau barang bukti maupun tentang unsur-unsur tindak pidana yang telah terjadi sehingga kedudukan atau peranan seseorang maupun barang bukti di dalam tindak pidana tersebut menjadi jelas dan dituangkan dalam berita acara pemeriksaan (Mabes Polri, 2001: 229-230).

Selama proses pemeriksaan, perlu dipenuhi syarat-syarat pemeriksaan seperti kewenangan pejabat yang melakukan pemeriksaan, kemampuan membuat BAP. Persiapan lain yang menjadi syarat pemeriksaan adalah mengenai tempat dan waktu pemeriksaan, sarana pemeriksaan dan kondisi dari pihak yang diperiksa harus dalam keadaan sehat jasmani dan rohani. Kemudian pemeriksa menyusun dan merumuskan daftar pertanyaan pemeriksaan untuk mendapatkan jawaban atas pertanyaan "7 **KAH**" (siapakah, apakah, dimanakah, dengan apakah, bagaimanakah, bilamanakah, mengapakah) (Mabes Polri, 2001: 229-230).

Menurut Simons dan Boetig (Juni 2007: 9-20), ada 8 tahap dalam *investigative interview*. **Tahap persiapan** meliputi strategi, taktik, pelaksanaan dan pertimbangan hukum contoh adanya tujuan dilakukan wawancara. **Tahap pengenalan**, petugas mengidentifikasikan dirinya dan kesatuannya, meyakinkan diri mereka apakah mereka memiliki kewenangan baik secara hukum maupun administratif atas suatu kasus. **Tahap hubungan**, apabila ada hubungan kuat maka orang yang diwawancarai akan merasa bahwa penyidik mengerti,

menghargai atau saling berbagi pengalaman dan pendapat. **Tahap menanyakan,** daftar pertanyaan yang tersusun, terstruktur dan berurutan akan menghasilkan informasi yang akurat dan lengkap dari yang diwawancarai dibandingkan yang belum tersusun. Ada dua tipe pertanyaan yaitu *open ended question* yang akan menghasilkan tanggapan berbentuk narasi dan *close ended question* yang akan menghasilkan jawaban yang lebih pendek dan rinci. **Tahap penyeleksian,** bertujuan untuk meyakinkan keakuratan pernyataan yang diwawancarai dan untuk mengingatkan. Misalnya dengan mengulang pernyataan yang telah diucapkan oleh orang yang diwawancarai untuk mencegah ketidakakuratan dalam ingatan penyidik yang dapat muncul karena salah pengertian, penyimpangan, penyelaan, kemampuan mendengarkan yang kurang baik atau bahasa yang tidak jelas artinya. Orang yang diwawancarai dapat melakukan koreksi apabila ada kesalahan. **Tahap pemeriksaan umum,** memberikan kesempatan kepada penyidik untuk mendapatkan informasi tambahan yang mungkin penyidik cari selama ini misalnya dengan menanyakan kepada orang yang diwawancarai apakah ada lagi yang akan dikatakan. **Tahap pemberangkatan**, setelah selesai melakukan tahap-tahap diatas, misal dengan memberikan kartu nama penyidik apabila ada yang ingin dibicarakan secara pribadi. **Tahap kritik,** akan meningkatkan kualitas wawancara ke depan, misal apakah sebelumnya penyidik telah memperkenalkan diri atau belum. Wawancara dalam proses penyidikan adalah bagian yang penting dalam setiap penegakan hukum. Proses pemeriksaan dalam rangka penyidikan tindak pidana diselesaikan dengan cara mengevaluasi hasil pemeriksaan. Agar memperoleh keterangan, petunjuk-petunjuk, bukti-bukti, data yang cukup dan benar, maka hasil-hasil pemeriksaan Tersangka/Saksi/Ahli yang dituangkan dalam Berita Acara Pemeriksaan baik secara sendiri-sendiri maupun secara keseluruhan dievaluasi guna mengembangkan dan mengarahkan pemeriksaan berikutnya ataupun untuk membuat suatu kesimpulan dari pemeriksaan sebagai salah satu kegiatan penyidikan yang telah dilakukan

3.1.1.4 Penyelesaian dan Penyerahan Berkas Perkara

Kegiatan penyelesaian dan penyerahan berkas perkara merupakan kegiatan akhir dari proses penyidikan tindak pidana yang dilakukan oleh penyidik/penyidik pembantu. Menurut Jukmin Tentang Penyelesaian dan Penyerahan Berkas Perkara

(Mabes Polri, 2001: 277-294), penyelesaian dan penyerahan berkas perkara meliputi pembuatan resume, penyusunan isi berkas perkara dan penyerahan berkas perkara serta penyerahan tanggung jawab atas tersangka dan barang bukti. Berkas perkara adalah kumpulan dari seluruh kegiatan dan atau keterangan yang berkaitan dengan tindakan penyidikan tindak pidana dalam bentuk produk tertulis yang dilakukan oleh penyidik/penyidik pembantu. Pelaksanaan penyelesaian berkas perkara haruslah dilakukan secara cermat dan teliti agar semua isi berkas perkara menjadi benar dan lengkap dan tersusun secara sistematis sebagai dokumen yang dipergunakan untuk proses hukum sampai pada sidang pengadilan.

Berkas perkara kemudian diserahkan oleh pihak kepolisian kepada penuntut umum yang bertugas untuk melakukan proses penuntutan[92] di pengadilan. Menurut Yahya Harahap (2006: 385), penuntut umum adalah instansi yang diberi wewenang oleh undang-undang untuk melakukan penuntutan dan melaksanakan putusan dan penetapan pengadilan. Sebelum masuk ke proses penuntutan, penuntut umum dapat melakukan proses pra penuntutan untuk memeriksa kelengkapan dan kecukupan dari berkas perkara yang diberikan oleh pihak kepolisian. Apabila penuntut umum menganggap bahwa berkas perkara itu belum cukup maka dapat dikembalikan ke penyidik untuk diperbaiki (P-19) sebagaimana diatur dalam Pasal 138 KUHAP. Apabila penuntut umum menganggap bahwa berkas perkara sudah lengkap dan cukup (P-21) maka dapat dilanjutkan dengan proses penuntutan di pengadilan. Kemudian penuntut umum berwenang untuk menghentikan penyidikan berdasarkan hal-hal sebagaimana diatur dalam Pasal 140 ayat 2 KUHAP yaitu: tidak cukup bukti, peristiwa itu bukan tindak pidana atau perkara ditutup demi hukum. Hal ini ditandai dengan dikeluarkannya Surat Perintah Penghentian Penyidikan (SP3).

3.1.2 Dukungan Teknis Penyidikan Tindak Pidana

Dalam melaksanakan tugas penyidikan tindak pidana diperlukan dukungan teknis dari ahli tertentu untuk kepentingan pembuktian dalam rangka pelaksanaan

---

[92]Pasal 1 angka 7 KUHAP berbunyi:
"Penuntutan adalah tindakan penuntut umum untuk melimpahkan perkara pidana ke Pengadilan negeri yang berwenang dalam hal dan menurut cara yang diatur dalam undang-undang ini dengan permintaan supaya diperiksa dan diputus oleh hakim di sidang pengadilan."

penyidikan secara ilmiah. Menurut Juklak Tentang Proses Penyidikan Tindak Pidana (Mabes Polri, 2001: 30-31), dukungan teknis tersebut antara lain:

Proses identifikasi yang dilakukan untuk mengenali seseorang melalui sidik jari (*dactiloscopy*), untuk mengenali orang atau benda melalui potret dan/atau pemotretan, untuk pengenalan seseorang melalui *signyalemen potrait parly*, dan untuk pengenalan seseorang melalui identifikasi gigi. Dalam pelaksanaannya, perolehan dukungan teknis berupa proses identifikasi dikoordinasikan dengan Pusat Identifikasi (Pusident) setempat (Mabes Polri, 2001: 30).

Peranan **laboratorium forensik** diperlukan dalam usaha pengungkapan tindak pidana yang menggunakan aspek teknologi. Laboratorium forensik melaksanakan pemeriksaan benda bukti mati (*physical evidence*) dengan menggunakan *Scientific Crime Investigation* (*SCI*) yang meliputi kimia forensik, biologi forensik, fisika forensik, balistik forensik, metalurgi forensik, dokumen forensik, uang palsu forensik dan fotografi forensik. Dukungan pemeriksaan laboratorium forensik dalam pelaksanaannya dikoordinasikan dengan Pusat Laboratorium dan Forensik (PusLabfor) Polri atau Labfor cabang setempat (Mabes Polri, 2001: 30-31).

Untuk mengungkap tindak pidana yang berhubungan dengan pemeriksaan tubuh/badan akibat luka, dan pemeriksaan mayat diperlukan peranan **Kedokteran Kepolisian (Forensik)** untuk menentukan sebab-sebab luka, sebab kematian, saat kematian dan lain-lain yang dituangkan dalam bentuk *Visum et Repertum* (*VER*) (Mabes Polri, 2001: 31).

Peranan **Dinas Psikologi** dalam penyidikan tindak pidana adalah untuk melakukan pemeriksaan psikologi terhadap saksi/tersangka tentang keadaan jiwanya apakah keterangannya dapat dipertanggungjawabkan secara hukum atau tidak. Hasilnya dapat digunakan sebagai bahan pertimbangan dalam penyidikan, penuntutan dan pemeriksaan di pengadilan. Selain sebagai pertimbangan dalam penuntutan dan pengadilan, hasil pemeriksaan psikologi juga dapat dipergunakan untuk menentukan metode dan cara penyidik/penyidik pembantu dalam melakukan pemeriksaan tersangka ataupun saksi (Mabes Polri, 2001: 31).

3.1.3 Administrasi Penyidikan Tindak Pidana

Menurut Soeherto (2002: 13-37), yang dimaksud dengan administrasi dalam arti luas adalah suatu proses dari suatu badan yang terdiri dari kumpulan manusia dan alat peralatan yang disusun dalam hubungan kerjasama sedemikian rupa dan dengan menggunakan suatu tata kerja sehingga dapat melaksanakan tugas pokoknya dengan cara tertentu untuk mencapai tujuan yang telah ditetapkan secara berdaya guna dan berhasil guna. Sedangkan administrasi secara sempit diartikan sebagai kegiatan penatausahaan yang diperlukan untuk kepentingan suatu organisasi/kegiatan yang meliputi kegiatan pencatatan, pelaporan, surat-menyurat dan pendataan. Menurut Soeherto (2002: 13-37), pelaksanaan penyelenggaraan administrasi penyidikan dilakukan dengan selalu memperhatikan lima asas penyelenggaraan administrasi penyidikan yaitu asas tanggung jawab[93], kecepatan[94], kepastian[95], keamanan[96], dan kesinambungan[97].

---

[93]Asas tanggung jawab, asas ini berkaitan dengan sifat dari kegiatan penyidikan tindak pidana yang didalamnya meliputi kewenangan-kewenangan yang dapat menyebabkan seseorang yang semula bebas menjadi terkekang kemerdekaannya, bahkan kemudian dapat dijatuhi hukuman, sehingga dalam pelaksanaannya setiap langkah penyidikan harus dapat dipertanggungjawabkan, baik proses pelaksanaannya maupun penerapan pasal-pasalnya. Dalam hal ini penyelenggaraan administrasi penyidikan merupakan salah satu wujud pertanggungjawaban penyidik dalam melaksanakan kegiatan penyidikan, dan sebaliknya penyelenggaraannya harus dapat dipertanggungjawabkan sesuai dengan peraturan perundang-undangan yang berlaku, yang meliputi: kewenangan dan kewajiban pembuatan, penandatanganan, penyimpanan, pengiriman/penyerahan dan pencatatan surat-surat Berita Acara dalam penyelenggaraan administrasi penyidikan (termasuk surat panggilan, surat perintah, berita acara/berita acara pemeriksaan, penetapan) (Soeherto, 2002: 13-17).

[94]Asas kecepatan, seluruh kegiatan dalam proses penyidikan tindak pidana dibatasi oleh waktu yang sangat ketat, baik berdasarkan ketentuan-ketentuan yang diatur dalam KUHAP maupun faktor-faktor lain yang mempengaruhi dalam pelaksanaan penyidikan. Oleh karenanya dalam penyelenggaraan administrasi penyidikan perlu memperhatikan kecepatan, baik dalam proses pembuatan/penyelenggaraan administrasi penyidikan maupun dalam hal pendistribusiannya (Soeherto, 2002: 27-32).

[95]Asas kepastian, penyelenggaraan administrasi penyidikan yang merupakan persyaratan mutlak dalam mendukung pelaksanaan penyidikan tindak pidana baik sebelum, selama maupun sesudahnya, harus dibuat secara pasti baik mengenai dasar hukumnya, waktu, tempat, pasal yang dipersangkakan, tindak pidana yang terjadi, barang bukti yang disita maupun identitas tersangkanya/saksinya, sesuai dengan yang dikehendaki KUHAP (Soeherto, 2002: 19-20).

[96]Asas keamanan, administrasi penyidikan merupakan tulisan/catatan yang bersifat otentik dan mempunyai nilai pembuktian yang tinggi, karena merupakan salah satu alat bukti yang sah (alat bukti berupa surat) yang dijadikan dasar pemeriksaan di hadapan sidang pengadilan. Oleh karena itu pengamanan semua bentuk administrasi penyidikan multak diperlukan dari kemungkinan adanya gangguan dari pihak yang tidak bertanggung jawab. Apabila penyelenggaraan administrasi penyidikan karena sesuatu hal hasilnya menjadi tidak benar atau

Sehubungan dengan penyidikan tindak pidana, yang dimaksud dengan administrasi penyidikan menurut Juklap tentang Proses Penyidikan Tindak Pidana (Mabes Polri, 2001: 31-32) adalah penatausahaan segala kelengkapan administrasi yang diperlukan untuk mempertanggungjawabkan seluruh kegiatan penyidikan meliputi pencatatan, pelaporan, surat-menyurat dan pendataan, untuk menjamin ketertiban, kelancaran, keamanan dan keseragaman pelaksanaan administrasi baik untuk kepentingan peradilan, operasional maupun untuk kepentingan pengawasan. Administrasi penyidikan meliputi penatausahaan tentang kelengkapan administrasi penyidikan yang merupakan isi berkas perkara dan penatausahaan tentang kelengkapan administrasi penyidikan yang tidak merupakan isi berkas perkara.

3.1.4 Pengawasan dan Pengendalian Penyidikan Tindak Pidana

Sebagai pengemban tugas penyidikan, Polri dituntut dapat meningkatkan kemampuan secara profesional serta dapat melakukan pengawasan dan pengendalian terhadap setiap proses penyidikan, mulai dari penyelidikan, penindakan, proses penyidikan, mulai dari penyelidikan, penindakan, pemeriksaan serta penyelesaian dan penyerahan Berkas Perkara. Menurut buku Jukmin Tentang Pengawasan Dan Pengendalian Kegiatan dalam Proses Penyidikan (Mabes Polri, 2001: 318-319), pengawasan dan pengendalian kegiatan dalam proses penyidikan terdiri dari pengawasan dan pengendalian penerimaan laporan dan penanganan laporan polisi, pengawasan dan pengendalian kegiatan penyelidikan tindak pidana, pengawasan dan pengendalian kegiatan penindakan tindak pidana, pengawasan dan pengendalian kegiatan penyelesaian dan

---

tidak sesuai dengan ketentuan undang-undang, hal itu akan dapat menimbulkan kesulitan bagi penyidik bahkan mungkin dapat berakibat tuntutan hukum bagi penyidik/Polri (Soeherto, 2002: 33-35).

[97]Asas kesinambungan, seluruh kegiatan penyelenggaraan administrasi penyidikan pada dasarnya merupakan suatu proses yang berkesinambungan dan saling berhubungan satu dengan yang lainnya, baik yang berupa Laporan/Laporan Polisi, Surat/Surat Perintah, Berita Acara/Berita Acara Pemeriksaan, Buku Register, Buku Ekspedisi, dan jenis-jenis administrasi penyidikan lainnya. Tiap-tiap kegiatan penyidikan dan administrasi penyidikannya masing-masing harus saling terkait satu sama lain, serta bersambung, apabila penyelenggaraan salah satu bagian dari administrasi penyidikan yang diperlukan ternyata salah satu tidak dilaksanakan, maka akan sangat mempengaruhi kegiatan pelaksanaan penyidikan selanjutnya (Soeherto, 2002: 35-37).

penyerahan perkara, pengawasan dan pengendalian perkara pada tahap penuntutan, pengawasan dan pengendalian perkara pada tahap peradilan, serta pengawasan dan pengendalian terhadap tahanan.

3.2 Penyidikan Tindak Pidana *Hacking*

Melakukan kejahatan komputer atau kejahatan yang berhubungan dengan komputer seperti *hacking* dapat sangat sederhana, sebaliknya penyidikan atas kejahatan tersebut seringkali sangat sulit dan membuat frustrasi (Axelrod dan Antinozzi, 2003: 14). Menurut Kim Rossmo dalam artikelnya "*Criminal Investigative Failures*", proses penyidikan suatu tindak pidana memainkan peran yang penting dan khusus di setiap negara yang menganut prinsip *rule of law*. Kegunaannya adalah untuk mencari kebenaran "tanpa ketakutan dan tanpa kepentingan". Tugas itu harus dilakukan dengan tanpa keberpihakan dan profesional demi terwujudnya keadilan dan ketertiban umum. Bila hal ini tidak dilakukan maka hasilnya adalah kejahatan yang tidak terungkap (*FBI Law Enforcement Bulletin*, 2006: 18).

Sebagaimana telah diuraikan sebelumnya pada Bab II, tindak pidana *hacking* sebagai salah satu jenis *cybercrime* merupakan tindak pidana yang melibatkan komputer dan jaringan komputer. Karena karakternya yang lintas batas negara dan tidak meninggalkan bekas/jejak secara fisik melainkan dalam bentuk data elektronik, maka penegak hukum yang bertugas memberantas jenis kejahatan ini menghadapi berbagai tantangan. Tantangan yang paling signifikan dalam kegiatan penyidikan tindak pidana *hacking* atau pada umumnya *cybercrime* adalah masalah bukti (Shinder, 2002: 547). Faktor-faktor yang menyebabkan adanya tantangan tersebut diantaranya adalah sifat jaringan komputer yang tersebar menyebabkan juga penyebaran TKP dan menimbulkan masalah praktis dan yurisdiksi; sifat data digital yang mudah dihapus ataupun dirubah, mengharuskan pengumpulan dan pengamanannya secepat mungkin; jika kejahatan melibatkan jaringan komputer, maka diperlukan ahli teknis yang beragam; dan penyidikan tindak pidana yang berhubungan dengan sistem komputer melibatkan jumlah data yang besar (Casey dan Seglem, 2002: 5).

Selain permasalahan mengenai pembuktian, masalah lain yang juga tidak kalah penting untuk diantisipasi adalah kesulitan dalam menentukan definisi kasus *hacking* itu sendiri, masalah yurisdiksi yang seringkali timbul ketika tersangka dan korban berada dalam lokasi geografi yang berbeda, serta perbedaan-perbedaan tingkah laku dan gaya hidup yang menciptakan kesulitan bagi polisi dan profesional IT untuk bekerja sama (Shinder, 2002: 37). Tanpa memperhatikan pembahasan mengenai hambatan-hambatan dalam melaksanakan penuntutan kasus *cybercrime*, maka mustahil untuk dapat membawa kasus *cybercrime* ke pengadilan. Oleh karena itu dalam praktek, hambatan-hambatan tersebut menyebabkan pelaksanaan tugas penyidikan *cybercrime* menjadi relatif lebih sulit dibandingkan ketika harus melakukan penyidikan terhadap tindak pidana konvensional yang tidak melibatkan komputer atau jaringan komputer sebagai media ataupun korbannya. Begitupun dengan pelaksanaan penyidikan tindak pidana *hacking* yang jelas merupakan salah satu jenis dari *cybercrime*. Tiga dari empat tantangan atau hambatan signifikan yang disampaikan oleh Shinder tersebut di atas, juga ditegaskan oleh Schmidt (2006: 88-91) yang berpendapat bahwa berkaitan dengan keberadaan *cyberspace* perlu dipertimbangkan kejelasan atas tiga konsep yang menjadi tantangan dalam *cyberspace* yaitu masalah definisi *hacking*[98], masalah bukti[99] dan masalah yurisdiksi[100].

---

[98]Pertama, masalah sulitnya membuat definisi atas masalah dan kejadian yang perlu ditindak secara hukum berkaitan dengan tidak adanya preseden atau analogi yang dapat diterapkan. Beberapa konsep hukum yang telah didefinisikan secara jelas dan diatur oleh hukum dalam dunia nyata harus dipertimbangkan untuk diterapkan dalam *cyberspace*. Contohnya, perbuatan menerobos dan pencurian. Analogi seringkali digunakan dalam pembelaan terhadap serangan *hacker* bahwa jika sistem dibiarkan terbuka sehingga orang bisa masuk dan melihat-lihat atau meng-*copy* sesuatu, ini merupakan masalah pemilik sistem. Hal ini menjadi perdebatan hukum utama selama bertahun-tahun. Analogi lain yang menggambarkan dilema ini adalah jika seseorang pergi keluar kota dan meninggalkan pintu depan rumahnya tak terkunci tetapi tidak terbuka juga dan seseorang masuk dan melihat-lihat, tidak memegang apapun, apakah itu perbuatan melawan hukum atau bukan? Jika seseorang masuk ke suatu rumah dengan mendobrak pintunya tetapi tidak mencuri sesuatu, hal itu merupakan penerobosan. Akan tetapi jika kemudian dia mencuri sesuatu dari rumah itu, maka hal itu termasuk perampokan. Ketentuan hukum tersebut tidak berlaku dalam *cyberspace*. Tidak ada ketentuan yang melarang kegiatan-kegiatan tersebut dalam *cyberspace* karena tidak adanya undang-undang yang mengaturnya dan berlaku dalam *cyberspace*. *Hacker* tidak secara fisik berada dalam sistem yang dijelajahinya, akan tetapi semua tindakan yang dilakukannya dalam *cybercrime* mempunyai implikasi dalam dunia nyata (fisik) (Schmidt, 2006: 88-89).

Hal yang sama juga berlaku terhadap definisi tindakan pencurian. Pencurian baik dari definisi sejarah maupun secara hukum bukan berarti pengambilan suatu barang, tetapi lebih pada perampasan penggunaan barang tersebut dari pemiliknya. Ketika seorang *hacker* masuk dalam suatu sistem dan meng-*copy* suatu *file*, dia tidak merampas kegunaan *file* tersebut dari pemiliknya.

Masalah-masalah yang menjadi hambatan penegakan hukum di atas, menjelaskan bahwa bukan hanya ketiadaan hukum yang baik yang mempersulit pemberantasan perbuatan melawan hukum atau kejahatan dalam *cyberspace*, akan tetapi kurangnya proses yang baik dan sumber-sumber yang cukup menyebabkan sulitnya upaya pemberantasan kejahatan yang terjadi di *cyberspace*. Berkaitan dengan hambatan tersebut, Shinder (2002: 553) menekankan bahwa para penegak hukum harus bekerja sama untuk memperoleh penegasan mengenai definisi-definisi dan meyakinkan bahwa mereka mengerti elemen-elemen yang harus

---

Dia hanya mendapatkan keuntungan dari penggunaan *file* tersebut untuknya sendiri. Dalam hal ini apakah pencurian terjadi?, implikasinya disini jelas sangat besar. Dengan demikian, dapatlah dipahami bahwa penentuan mengenai apakah suatu tindakan atau kejadian dalam *cyberspace* itu merupakan tindak pidana atau bukan, sangatlah tergantung pada keberadaan undang-undang yang mengaturnya (Schmidt, 2006: 89). Hal tersebut juga berlaku di Indonesia. Dengan merujuk pada azas hukum pidana yang berlaku menurut KUHP yaitu *"tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada, sebelum perbuatan dilakukan"* (Pasal 1 ayat (1) KUHP), maka masalah belum diaturnya tindakan/perbuatan melawan hukum atau kejahatan dalam suatu peraturan perundang-undangan menjadi suatu tantangan utama dalam upaya memberantas kejahatan yang terjadi di *cyberspace*, yang di antaranya tindak pidana *hacking*.

[99]Kedua, yang merupakan tantangan atau hambatan dalam memberantas kejahatan yang terjadi di *cyberspace* menurut Schmidt (2006: 90) adalah masalah bukti. Mengingat penyidikan pidana didasarkan pada bukti, maka apakah yang disebut sebagai "original" atau "asli" dan karenanya menjadi bukti terbaik? Dari kaca mata hukum, bukti terbaik adalah salinan asli. Asumsinya segala dokumen yang merupakan salinan dari dokumen asli dapat dirusak. Sedangkan untuk *digital file*, dapat di-*copy* beberapa kali dan masih tetap merupakan salinan asli. Itulah konsep yang dipergunakan sekarang, walaupun bertahun-tahun lalu bukti digital ini bersifat unik dan menimbulkan situasi yang membingungkan.

[100]Ketiga, menurut (Schmidt, 2006: 90) yang juga penting untuk diantisipasi adalah konsep yurisdiksi mengenai dimana sebenarnya hukum dilanggar. Contohnya mengenai pornografi dewasa di Amerika Serikat, yang dilindungi oleh *First Amendment*, akan tetapi diserahkan kepada etika dan budaya komunitas pribadi untuk pelarangan atau pembatasan di tingkat lokal. Dalam hal seseorang yang tinggal di daerah yang konservatif diperbolehkan untuk melakukan koneksi pada sistem komputer dan selanjutnya melakukan *download* pornografi, dimana tempat kejadian kejahatan tersebut tentu menjadi masalah. Kemungkinan di kota dengan tingkat moral yang tinggi hal tersebut merupakan pelanggaran hukum. Dalam hal ini hukum tidak cukup memberikan dasar untuk mengidentifikasi dimana kegiatan tersebut sebenarnya terjadi dan karenanya apakah hal tersebut melanggar hukum. Sehingga adanya perbedaan keberlakukan suatu peraturan di suatu daerah dengan daerah lainnya, yang dalam *cyberspace* menjadi tanpa batas, seringkali menimbulkan masalah yurisdiksi mengenai perdebatan dimana sebenarnya kejahatan telah terjadi dan melawan hukum yang mana. Masalah yurisdiksi tersebut akan semakin kompleks jika berkaitan dengan yurisdiksi internasional. Contohnya kasus sistem pelayanan kesehatan di Kanada yang diberikan oleh Schmidt. Dinas kesehatan setempat telah meminta bantuan *outsourcing IT* dari suatu perusahaan yang berbasis di Amerika. Ketika terjadi kerusakan dengan sistem *IT* tersebut, Departemen Hukum Kanada menghubungi Departemen Hukum Amerika Serikat dan meminta bantuan untuk memperoleh ijin untuk menyidik perusahaan Amerika tersebut. Masalah yang muncul adalah mengenai apakah kejahatannya terjadi di Kanada atau di Amerika Serikat. Perbedaan hukum pembuktian di antara kedua negara tersebut dapat menimbulkan masalah yurisdiksi yang sulit.

dibuktikan dalam menangkap dan menuntut suatu kasus *cybercrime*. Shinder menambahkan juga bahwa mengenai masalah yurisdiksi, para penyidik harus disiapkan untuk masalah-masalah hukum ketika *cybercrime* melewati batas negara, dan mereka pun harus menyadari bahwa walaupun mereka secara hukum memiliki yurisdiksi, banyak faktor praktis dapat menghambat keberhasilan penuntutan dari kasus-kasus *cybercrime* yang bersifat multiyurisdiksional.

3.2.1 Karakteristik Penyidikan Tindak Pidana *Hacking*

Sebagaimana telah dijelaskan sebelumnya di bab 2 bahwa karakteristik *cybercrime* berbeda dengan tindak pidana pada umumnya. Masalah definisi perbuatan *hacking*, bukti digital, melibatkan keahlian di bidang *IT* dan yurisdiksi membuat penyidikannya pun berbeda dengan penyidikan tindak pidana biasa. Berikut ini akan dijelaskan lebih lanjut mengenai karakteristik penyidikan tindak pidana *hacking*.

3.2.1.1 Sebagian Proses Penyidikan Dilakukan dalam *Cyberspace*

Dalam proses penyidikan tindak pidana *hacking*, penyidik dihadapkan pada masalah dari mana dan dimana harus memulai penyidikan. Akibat perbuatan *hacking* baik yang diketahui pertama kali oleh penyidik yang sedang melakukan *cyber-patrolling* maupun berdasarkan laporan dari korban *hacking*, pertama kali diketahui melalui layar monitor suatu komputer yang terhubung dengan jaringannya melalui koneksi internet. Oleh karenanya proses awal penyelidikan mau tidak mau harus melibatkan komputer dan jaringannya yang terkoneksi melalui internet. Bukti-bukti dapat tersimpan di dalam sistem komputer, karenanya inti dari suatu proses penyelidikan adalah bagaimana menemukan dan selanjutnya menyita komputer milik tersangka. Dari komputer tersebutlah penyidik dapat menentukan jika ada bukti-bukti kejahatan.

Untuk kasus *hacking*, biasanya korban *hacking* sendiri dapat memeriksa dan memastikan ada tidaknya serangan atau gangguan dari *hacker* dengan memeriksa sistem yang dirusak atau di-*hacked* oleh seorang atau lebih *hacker*. Oleh karenanya komputer dan sistemnya merupakan benda-benda yang dapat menjadi bukti. Pada *server* komputer terdapat apa yang dikenal dengan *log files* yaitu suatu

file yang menyimpan pesan-pesan yang dihasilkan oleh suatu aplikasi, *service* atau sistem operasi. Pesan-pesan tersebut digunakan untuk melacak operasi yang telah dijalankan. Contohnya, *web servers* memelihara *log files* mengenai daftar permintaan atau perintah yang dibuat kepada *server*. *Log files* biasanya berupa *plain text*[101] *files* dan seringkali memiliki suatu *log extension*. Dalam proses *backup*[102], suatu *file* yang berisi suatu catatan tanggal pembuatan rekaman dan nama *files* dan direktori yang di-*back up* dan disimpan. Kegiatan jasa *logs* dan *alerts*[103] juga menciptakan *log files*.

Dalam penyidikan *hacking*, *log files* memegang peranan penting dalam tahap awal proses penyidikan. Untuk mengetahui kapan, berapa kali dan sifat serta jenis serangan-serangan atau penyusupan *hacker*, *log files* dapat memberikan informasi berupa catatan atas perintah-perintah atau pesan-pesan kepada *server* korban yang dilancarkan atau dilakukan oleh *hacker*. Pada *log files* terdapat pula informasi mengenai dari mana dan oleh siapa serangan-serangan atau penyusupan dilakukan. Dalam bahasa *software*, identitas seseorang berupa *IP Address*[104]. Sehingga yang dapat diketahui dari *log files* hanyalah *IP Address hacker*. Dengan

---

[101]Yang dimaksud *plaintext* adalah pesan asli atau yang pesan yang dihasilkan sebelum proses *encryption* dan setelah proses *decryption*. Secara umum juga dikenal sebagai *cleartext* (Slade, 2006: 143).

[102]*Backup* berarti suatu salinan duplikat data yang dibuat untuk melindungi dari kerusakan atau kehilangan. Sedangkan jika dipergunakan sebagai kata kerja, *backup* berarti suatu proses menciptakan data duplikat/salinan (Slade, 2006: 20).

[103]*Alert* berarti pengumuman bahwa suatu kejadian atau insiden telah terjadi (Slade, 2006: 8).

[104]Contoh lain mengenai kasus yang kurang lebih menggambarkan situasi yang sama adalah sebagaimana disampaikan Schmidt (2006: 92) bahwa jika seseorang yang dicurigai sebagai tersangka yang melakukan tindak pidana *hacking* tinggal dalam sebuah rumah bersama teman-temannya, dimana mereka masing-masing mempunyai *account* pada satu komputer yang sama, yang menyimpan *files/folders* untuk penggunaan setiap orang dan setiap pengguna mempunyai *folder* pribadi yang dapat diakses dengan *password* pribadi. Dokumen, *IP Address* dan teknik tindak pidana *hacking* biasanya ditemukan dalam *folder* bersama. Walaupun komputer milik tersangka, akan tetapi karena dipergunakan secara bersama-sama, tersangka dapat berkata dengan akurat bahwa walaupun komputer tersebut miliknya tetapi *file* yang ditemukan dapat diakses oleh setiap orang yang menggunakan sistem tersebut, sehingga penentuan tersangka menjadi tidak mudah. Khususnya apabila terdapat dua orang atau lebih dalam TKP. Dengan demikian penentuan tersangka *hacker* juga tidak semudah hanya mencari pemilik *IP Address* yang dapat diperiksa dalam daftar pengguna internet pada *ISP*. Dalam hal ini, penyidik harus menggunakan teknik pencarian tersangka dengan mencari informasi mengenai siapa-siapa saja yang kiranya menggunakan *IP Address* tersebut dan yang diperkirakan atau dicurigai mempunyai kepentingan atau suatu motif tertentu untuk melakukan tindak pidana *hacking*.

mengetahui *IP Address hacker*, penyidikan dapat dilanjutkan untuk menentukan siapa pemilik atau pengguna *IP Address* tersebut yang dipergunakan untuk melakukan tindak pidana *hacking*. Masalahnya pemilik *IP Address* atau pihak yang namanya terdaftar sebagai pemilik *IP Address* pada perusahaan *ISP* belum tentu sebagai pelaku, apalagi jika *IP Address* merupakan milik warnet yang dipergunakan oleh banyak orang.

Sebagaimana telah diuraikan sebelumnya, *hacker* umumnya ahli komputer yang biasanya memiliki suatu komunitas sendiri dalam *cyberspace*. Untuk dapat mencari informasi mengenai identitas *hacker* yang dicurigai, penyidik dapat melakukan penyidikan di *cyberspace* dengan melaksanakan *virtual-undercover* melalui *chatting* pada *chatroom* yang dicurigai atau *chatroom* milik komunitas *hacker* tertentu, ataupun melakukan *net-observation* terhadap anggota-anggota komunitas tertentu dalam kehidupan atau pergaulan di *cyberspace* yang dicurigai. Melalui teknik tersebut diharapkan penyidik memperoleh informasi mengenai siapa-siapa saja yang dicurigai telah melakukan tindak pidana *hacking*. Mengingat umumnya tindak pidana *hacking* dilakukan dengan tujuan agar eksistensinya dalam *cyberspace* diakui atau karena faktor keingintahuan ataupun perasaan penasaran semata, maka seringkali *hacker* di dalam *cyberspace* saling mengenal satu sama lain dan saling mengetahui kemampuan masing-masing. Berkaitan dengan itu, penyidik tindak pidana *hacking* setidaknya harus mengetahui dan *familiar* dengan kehidupan dalam *cyberspace* dan dapat bergaul serta melakukan kontak dan berkomunikasi dengan anggota lainnya dalam komunitas *virtual* dalam *cyberspace*.

Penyidik yang berwenang menangani tindak pidana *hacking* atau kasus *cybercrime* lainnya atau yang mempunyai spesialisasi menyidik kasus *cybercrime* yang melibatkan eksistensi komputer tidak harus menghabiskan seluruh waktunya di depan komputer. Komputer hanyalah sarana yang dipergunakan untuk melakukan *cybercrime* tetapi pelaku kejahatan tetaplah manusia, dan rekayasa manusia (menjebak pelaku tindak pidana) seringkali memegang peranan besar dalam proses pengejaran dan penangkapan serta proses memahami tindakan tersangka (Axelrod dan Antinozzi, 2003: 183). Begitupun dengan para *hacker*, penyidik dapat melakukan penyamaran di *cyberspace* dengan teknik *cyber-*

undercover sebagai salah seorang anggota komunitas *virtual* dengan berpura-pura mempunyai minat yang sama dengan para *hacker* dalam komunitasnya sehingga memperoleh kepercayaan dari mereka untuk diterima sebagai salah satu anggota komunitasnya, dan mempunyai kesempatan untuk menggali informasi sebanyak mungkin agar diperoleh keterangan lengkap mengenai tersangka yang dicurigai.

Apabila telah ditentukan satu atau beberapa tersangka yang dicurigai menggunakan *IP Address* untuk melakukan serangan atau tindak pidana *hacking*, penyidik kemudian dapat menggunakan teknik *surveillance* dimana biasanya jumlahnya sudah semakin kecil dan tersangkanya semakin spesifik. Dalam tahap ini, proses penyelidikan dilakukan secara fisik dengan berdasarkan pada ketentuan KUHAP dan peraturan perundangan yang berlaku lainnya sebagaimana pelaksanaan proses penyelidikan tindak pidana pada umumnya. Penyidik melakukan pembuntutan terhadap tersangka yang dicurigai dan mencari saksi-saksi atau informasi lainnya mengenai kegiatan-kegiatan tersangka dan mencari apakah ada hubungannya antara catatan dalam *log files* seperti waktu-waktu dan tempat-tempat penyerangan dengan keterangan-keterangan mengenai kegiatan-kegiatan tersangka di luar *cyberspace*.

Selanjutnya penyidik dapat meningkatkan proses penyidikan dengan melakukan upaya penindakan baik penangkapan tersangka, penahanan, penggeledahan, maupun penyitaan barang bukti. Proses penangkapan, penahanan dan penggeledahan terhadap tersangka *hacker* secara umum tidak berbeda dengan proses penangkapan, penahanan dan penggeledahan tersangka pelaku tindak pidana konvensional lainnya. Sedangkan proses penyitaan barang bukti dalam kasus tindak pidana *hacking* memerlukan metode, keahlian dan pengetahuan yang spesifik, berkaitan dengan adanya *digital evidence*.

3.2.1.2 Eksistensi Bukti Digital (*Digital Evidence*) dalam Proses Penyidikan Tindak Pidana *Hacking*

Sebagaimana telah diuraikan di atas, proses penyelidikan dan penindakan tindak pidana *hacking* sebagai salah satu jenis *cybercrime* tidak dapat dilepaskan dari tantangan untuk menemukan, mengumpulkan, menyimpan dan menyajikan

bukti digital[105] yang merupakan barang bukti yang dapat memberi petunjuk atau mendukung alat bukti yang digunakan sebagai dasar penuntutan tindak pidana *hacking* atau *cybercrime* lainnya di hadapan pengadilan.

Di Indonesia sampai saat ini belum ada ketentuan khusus tentang alat bukti yang mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah disertai ketentuan-ketentuan tentang prasyarat dan kriteria yang harus dipenuhi tentang akurasi dan kebenaran alat bukti dimaksud. Mengenai masalah dokumen elektronik (termasuk *e-contract* dan *digital signature*) sebagai alat bukti di pengadilan, pada dasarnya hakim berdasarkan Pasal 22 Algemene Bepalingen (AB) dilarang menolak untuk mengadili suatu perkara yang belum ada pengaturan hukumnya. Selain itu hakim juga dituntut untuk melakukan *rechtsvinding* (penemuan hukum) dengan mengkaji norma-norma yang tumbuh dalam masyarakat dalam menyelesaikan kasus dimaksud. Dengan demikian, esensinya para hakim dalam proses pembuktian adalah mencari segala macam informasi untuk mendapatkan keyakinan tentang adanya peristiwa hukum dan/atau suatu hubungan hukum dengan menggunakan berbagai media/alat bukti, sejauh hal itu relevan dan valid (Ramli, Gunung dan Apriadi, 2007: 41-42). Selanjutnya dengan merujuk pada ketentuan pasal 183 KUHAP, hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar

---

[105]Menurut Shinder (2002: 550-551), bukti digital dapat diklasifikasikan sebagai bukti digital asli (*original digital evidence*) yang berarti barang secara fisik dan obyek data yang berkaitan dengan barang-barang tersebut pada saat bukti disita; bukti digital duplikat (*duplicate digital evidence*) yang merujuk pada reproduksi digital yang akurat dari seluruh obyek data yang tersimpan di dalam benda mati yang asli. Sedangkan mengenai bukti "tertulis" dikenal istilah bukti yang bersifat demonstratif dan bukti yang bersifat dokumenter. Bukti demonstratif adalah bukti yang membangun kembali tempat kejadian atau peristiwa dalam pertanyaan dan membolehkan ahli hukum melihatnya melalui bantuan visual seperti grafik, *charts*, gambar dan model. Sedangkan bukti dokumenter biasanya merujuk pada dokumen tertulis yang merupakan bukti. Contolnya suatu surat atau foto biasanya dianggap sebagai bukti dokumenter. Ketika dokumen diajukan sebagai bukti, seluruh dokumen harus diakui walaupun hanya sebagian kecil saja yang dibaca di pengadilan. Dalam beberapa kasus bukti digital, seringkali terjadi perdebatan diantara para ahli mengenai apakah akan mengklasifikesikan bukti digital sebagai bukti demonstratif atau dokumenter. Bukti komputer tidak seperti bukti dokumenter yang biasanya berbentuk kertas karena suatu *copy* dari *digital file* biasanya identik dengan aslinya, dan suatu dokumen dapat di-*copy* tanpa secara fisik memindahkan dari lokasinya atau meninggalkan indikasi bahwa dokumen tersebut telah di-*copy*. Banyak sarjana menyatakan bahwa bukti digital sebagai bukti yang bersifat demonstratif karena bidang forensik komputer pada dasarnya berkaitan dengan rekonstruksi TKP. Akan tetapi pendapat tersebut sangat tergantung dari jenis bukti digital yang berhubungan dengan kejahatan.

terjadi dan bahwa terdakwalah yang bersalah melakukannya.

Sesuai dengan penjelasan di atas, polisi melaksanakan tugas penyidikan tindak pidana *hacking* dengan menggunakan parameter alat bukti yang sah sebagaimana dimaksud dalam Pasal 184 KUHAP, yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Dalam proses penyidikan tindak pidana *hacking*, bukti digital saat ini belum masuk dalam salah satu jenis alat bukti tersebut.

Di Amerika, berdasarkan *Federal Rule of Evidence*, ditentukan bahwa bukti komputer berbeda dari bukti tertulis. *Rule* 1001-3 menyatakan *"If data are stored by computer or similar device, any print out or other output readable by sight, shown to reflect data accurately is an original"*. Masalah yang muncul ada pada pihak yang harus menunjukkan bahwa bukti benar-benar merefleksikan data secara akurat. Harus dibuktikan bahwa bukti adalah apa yang diklaim dan belum dirubah sejak disimpan pada tempat penyimpanan (*custody*). Jika tidak, maka bukti akan dianggap tidak dapat diterima (Shinder, 2002: 551).

Masalah di Indonesia adalah apabila belum ada pengaturan mengenai bukti digital, apakah berarti kasus tindak pidana *hacking* yang notabene barang buktinya berbentuk bukti digital tidak dapat dilanjutkan penyidikannya karena bukti digital belum diakui sebagai alat bukti. Hal itu ternyata tidak terjadi di Indonesia. Walaupun KUHAP belum mengakomodasi pengaturan mengenai bukti digital akan tetapi para penegak hukum mulai dari polisi, jaksa dan hakim ternyata menggunakan ketentuan peraturan perundang-undangan yang tersedia dengan memberikan interpretasi yang diyakini kebenarannya telah memenuhi syarat sebagai barang bukti berdasarkan hukum acara yang berlaku. Barang bukti dimaksud merupakan barang-barang baik yang berwujud, bergerak atau tidak bergerak yang dapat dijadikan sebagai alat bukti dan fungsinya untuk diperlihatkan kepada terdakwa ataupun saksi dalam persidangan guna memperoleh keyakinan hakim dalam menentukan kesalahan terdakwa.

Penyidik Polri memulai penyidikan tindak pidana menggunakan parameter alat bukti yang sah sesuai dengan pasal 184 KUHAP yang dikaitkan dengan segitiga pembuktian (*evidence triangle*) untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi, namun hanya

beberapa perundang-undangan di Indonesia yang mengatur tentang *digital evidence*.

Dengan dikeluarkannya Undang-undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya *CD-ROM* dan WORM, yang diatur dalam Pasal 12 undang-undang tersebut sebagai alat bukti yang sah.

Undang-undang No. 25 Tahun 2003 Tentang Perubahan Undang-undang No. 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang. Undang-undang ini juga mengatur mengenai alat bukti elektronik atau *digital evidence* sesuai dengan pasal 38 huruf (b) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

Undang Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-undang Pemberantasan Tindak Pidana Terorisme. Undang-undang ini mengatur mengenai alat bukti elektronik sesuai dengan pasal 27 huruf (b) yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Alat bukti elektronik sangatlah berperan dalam penyidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan/aktor intelektualnya dilakukan dengan memanfaatkan fasilitas internet untuk menerima perintah atau menyampaikan kondisi dilapangan. Para pelaku menyadari bahwa pelacakan melalui internet lebih sulit. Fasilitas yang sering digunakan dalam terorisme adalah *email* dan *chat room* selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list*.

Dalam Pasal 26 A UU No 20 Tahun 2001 Tentang Perubahan atas Undang-Undang Nomor 31 Tahun 1999 Tentang pemberantasan Tindak Pidana Korupsi, bukti elektronik juga menjadi salah satu alat bukti selain yang diatur dalam

hukum acara pidana. Pasal ini menjadi acauan dalam RUU KUHAP tentang ketentuan alat bukti.

Dalam Pasal 44 ayat 2 Pasal 44 ayat 2 UU No 30 Tahun 2002 Tentang Komisi Pemberantasan Tindak Pidana Korupsi dinyatakan bahwa bukti permulaan yang cukup dianggap telah ada apabila telah ditemukan sekurang-kurangnya 2 (dua) alat bukti, termasuk dan tidak terbatas pada informasi atau data yang diucapkan, dikirim, diterima, atau disimpan baik secara biasa maupun elektronik atau optik.

Menurut Pasal 29 UU No. 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang, mengatur tentang *digital evidence* sebagai salah satu alat bukti dalam proses pembuktian tindak pidana perdagangan orang, dimana alat bukti selain sebagaimana ditentukan dalam undang-undang hukum acara pidana, dapat pula berupa: informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apa pun selain kertas, atau yang terekam secara elektronik, termasuk tidak terbatas pada tulisan, suara, atau gambar, peta, rancangan, foto, atau sejenisnya; atau huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Dalam UU ITE, secara komperehensif mengakui alat bukti elektronik sebagai perluasan alat bukti yang ada dalam hukum acara baik pidana maupun perdata, dan sebagai perluasan alat bukti dalam hukum acara yang ada pada saat ini. Untuk dapat dipercaya sebagai alat bukti dapat dilakukan dengan cara: mengggunakan peralatan komputer untuk menyimpan dan memproduksi *print-out*; proses data seperti pada umumnya dengan memasukkan inisial dalam sistem pengelolaan arsip yang dikomputerisasikan dan menguji data dalam waktu yang tepat setelah data dituliskan oleh seseorang yang mengetahui peristiwa hukumnya (Ramli, Gunung dan Apriadi, 2007: 41-43).

Dalam Pasal 179 RUU KUHAP, alat bukti yang sah adalah surat; keterangan ahli; keterangan saksi; pengamatan hakim selama sidang; dan

keterangan terdakwa. Alat bukti elektronik telah diakomodir kedalam salah satu alat bukti yaitu pengamatan hakim. Dimana berdasarkan Pasal 183 RUU KUHAP pengamatan hakim dilakukan dengan mempertimbangkan keterangan saksi; surat; dan/atau keterangan terdakwa. Pengertian surat disini mencakup alat bukti elektronik.

Dalam RUU TPTI, ketentuan alat bukti yang sah mencakup bukti elektronik sebagaimana diatur dalam Pasal 33 RUU ini. Bukti elektronik ini dalam bentuk catatan elektronik yang tersimpan dalam sistem komputer. Selain catatan elektronik, maka berdasarkan Pasal 33 ayat 3 dapat digunakan sebagai alat bukti meliputi : **Pertama**, informasi yang diucapkan, dikirimkan, diterima atau disimpan secara elektronik atau yang serupa dengan itu. **Kedua**, data, rekaman atau informasi yang dapat dilihat, dibaca dan atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada : 1). Tulisan, suara atau gambar; 2). Peta, rancangan, foto atau sejenisnya; 3). Huruf, tanda, angka, simbol atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya. **Ketiga**, alat bukti elektronik, khususnya yang berwujud perangkat lunak diperoleh dengan cara penggandaan dari lokasi asalnya dengan cara tertentu tanpa merusak struktur logika program.

3.2.1.3 Penanganan Komputer sebagai TKP (*Crime Scene*)

TKP atau *crime scene* adalah tempat dimana suatu tindak pidana dilakukan/terjadi dan tempat-tempat lain dimana tersangka dan/atau korban dan/atau barang-barang bukti yang berhubungan dengan tindak pidana tersebut dapat ditemukan. Untuk kasus tindak pidana *hacking*, yang menjadi TKP selain tempat-tempat dimana *hacker* melakukan tindak pidana *hacking* juga tempat-tempat dimana korban menderita kerugian akibat tindak pidana *hacking*. Hal ini dapat terjadi mengingat tindak pidana *hacking* yang dapat dilakukan dari tempat yang terpisah dengan korbannya. Sehingga tempat si korban seringkali berbeda dengan tempat si pelaku tindak pidana *hacking*.

Selain tempat-tempat yang telah disebutkan di atas, yang terpenting dan menjadi TKP utama yang harus diuji tindak pidana *hacking* adalah komputer dan

jaringannya, sebagai tempat dimana sistem komputer terletak. Berkaitan dengan TKP tersebut, penyidikan forensik komputer menjadi hal yang penting dalam proses penyidikan tindak pidana *hacking*. *Computer hacking forensic investigation* adalah proses pendeteksian serangan *hacking* dan pengambilan bukti secara baik untuk melaporkan tindak pidana dan melaksanakan audit untuk mencegah serangan di masa yang akan datang.

Sedangkan forensik komputer adalah aplikasi sederhana penyidikan komputer dan teknis analisis sehubungan dengan penentuan alat bukti sah yang potensial (*http://www.globalnettraining.com/certified-ethical-hacking-chfi-boot camp.asp*, 10 Februari 2008).

Penentuan alat bukti ini sesuai dengan substansi pasal 184 ayat 1 KUHAP yang secara definitif menyatakan bahwa alat-alat bukti yang sah adalah keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Di Indonesia, standar pelaksanaan penyidikan forensik komputer belum diatur secara khusus dalam suatu peraturan perundang-undangan. Walaupun demikian, Polri telah mempunyai sarana untuk melakukan penyidikan forensik komputer yang berupa laboratorium forensik komputer yang saat ini berada di bawah kewenangan Unit V *IT & Cybercrime* Bareskrim Polri. Pembahasan mengenai laboratorium forensik komputer akan diuraikan lebih jelas dalam Bab IV.

Menurut Lee (1994) sebagaimana dikutip Casey (2000: 47-63), ada beberapa aspek dalam memproses dan menganalisa bukti yaitu pengakuan (*recogniton*)[106]; pemeliharaan, pengumpulan dan pendokumentasian

[106]Pengakuan atas *digital evidence* melalui dua proses. Pertama, penyidik harus mengakui *hardware* (seperti komputer, disket, kabel jaringan) yang mengandung informasi digital. Kedua, penyidik harus dapat membedakan antara informasi yang tidak relevan dan data digital yang dapat digunakan memperkuat bahwa suatu kejahatan telah dilakukan atau dapat menyediakan *link* atau menghubungkan antara kejahatan dan korbannya atau antara kejahatan dan pelakunya. Setelah dikenali maka *digital evidence* harus dijaga bentuk aslinya. Hal itu dikarenakan hukum mempersyaratkan agar bukti harus otentik dan tidak berubah. Aspek utama dalam mengumpulkan *digital evidence* adalah mengumpulkannya dengan tidak merusaknya. Alat dan teknik khusus sangat berguna dalam menjaga dan mengumpulkan *digital evidence* dengan baik sehingga bukti itu dapat diterima di pengadilan. Ada dua faktor yang perlu dipertimbangkan dalam mengumpulkan *digital evidence*. Disatu sisi, untuk menghindari barang bukti tertinggal, bila dianggap perlu penyidik dapat mengambil setiap benda yang ditemukan. Di lain sisi, penyidik mungkin hanya mengambil yang penting untuk menghemat waktu, usaha dan sumber daya serta untuk mengurangi resiko dituntut karena merusak atau mengganggu hidup atau bisnis seseorang lebih dari yang seharusnya dilakukan. Misal peranan komputer sangat penting untuk operasional suatu institusi seperti rumah sakit dan apabila komputer tersebut diambil dapat beresiko membahayakan nyawa (Casey, 2000:47-48).

(*preservation, collection and documentation*)[107]; pengklasifikasian, perbandingan dan pemisahan (*classification, comparison and individualization*)[108]; dan rekonstruksi (*reconstruction*)[109].

Walaupun telah banyak pedoman diterbitkan untuk memberikan panduan pelaksanaan penyidikan berkaitan dengan bukti *digital*, tapi masing-masing pedoman atau prosedur juga memiliki kekurangan, diantaranya kurangnya pedoman untuk melakukan analisis forensik atau tidak dapat mengantisipasi munculnya teknologi lainnya yang lebih baru dan canggih. Hal ini memang wajar karena sifat dari setiap penyidikan memang berbeda, sehingga mengakibatkan sulitnya menciptakan suatu *Standard Operating Procedure* (*SOP*) yang mencakup

---

[107]Dalam proses pemeliharaan, pengumpulan dan pendokumentasian, apabila *hardware* rusak ketika sedang diambil sebagai barang bukti, atau komputer tidak menyala karena alasan yang tidak jelas, bukti dapat saja hilang. Dalam beberapa kasus sangat masuk akal apabila komputer dibiarkan menyala, simpan *file* yang diperlukan dan tinggalkan. Dengan cara ini, ada penurunan resiko merusak komputer, menghancurkan barang bukti, mengganggu bisnis seseorang dan komputer tersebut tidak dapat dipakai lagi. Apabila memang ada *hardware* yang harus dikumpulkan maka tidak perlu untuk mengumpulkan semua yang terlihat dalam komputer tersebut, cara yang paling baik adalah dengan mengumpulkan *hardware* yang berdiri sendiri (*independent component hardware doctrine*) yaitu penyidik hanya mengumpulkan *hardware* yang diartikan sebagai dasar pencarian dan penyitaan contoh komponen itu adalah bukti. Selain itu, penyidik juga harus mengumpulkan *hardware* yang berfungsi sebagai dasar *input* dan *output* komputer contoh *hard drive*. Apabila penyidik akan mengumpulkan seluruh perangkat komputer, maka *hardware* lain seperti printer dapat disita dengan kemungkinan ada bukti berupa gambar. Hal ini untuk memperkuat bukti bahwa pelaku lah yang menciptakan barang bukti tidak hanya men*download*nya dari internet. Hasil *print-out* dan kertas yang terkait dengan komputer, harus dikumpulkan karena mungkin saja mengandung informasi yang dibutuhkan. Setiap *hardware* yang dikumpulkan harus dijaga dengan hati-hati dan bersih dari debu, panas yang berlebihan, daya magnet dan lain-lain. Selain itu penyidik harus membuat dua *copy* dari *digital evidence* dan pastikan setidaknya salah satu dapat berfungsi (Casey, 2000: 48-49).

[108]Pengklasifikasian *digital evidence* adalah proses untuk menemukan ciri-ciri yang dapat digunakan untuk menggambarkan secara umum dan membedakannya dari yang lain misalnya dari bentuk. *Digital evidence* dapat dikelompokkan, dibandingkan dan dipisahkan ke dalam tiga cara yaitu *content, function dan characteristics*. *Content* misal isi *email* yang digunakan penyidik untuk melacak dari komputer mana *email* itu berasal. *Function* misal penyidik memeriksa bagaimana suatu program bekerja dan mengklasifikasikan serta memisahkan *digital evidence*. *Characteristics* misal nama *file*, pesan, dan tanggal yang dapat membantu dalam mengklasifikasikan dan memisahkan sebagai *digital evidence* (Casey, 2000:60-62).

[109]Dalam merekonstruksi ada dua aspek yang perlu diperhatikan yaitu *digital evidence* yang rusak dapat direkonstruksi melalui berbagai proses dan *digital evidence* dapat juga digunakan untuk merekonstruksi kejadian seputar kejahatan tersebut. Dalam melakukan rekonstruksi, hal-hal yang harus diperhatikan adalah tipe komputer yang digunakan, sistem operasi dan perpaduan antar *hardware* dan *sofware* yang digunakan. Konsep yang digunakan cukup mudah. Semua barang bukti yang tersedia dapat digunakan untuk mendapat pemahaman tentang apa, siapa, bagaimana, dimana dan mengapa kejahatan itu terjadi. Namun tidak boleh juga tergantung kepada *digital evidence*, diusahakan mencari bukti fisik lain yang dapat mendukung (Casey, 2000:62-63).

semua aspek analisis forensik bukti *digital* secara mendalam. Oleh karenanya memiliki suatu pendekatan metodologis untuk mengorganisasikan dan menganalisis tipikal data komputer dalam jumlah besar dan *network* menjadi hal yang penting. Oleh karena itu, ilmu forensik secara umum dan rekonstruksi tindak pidana[110] secara khusus menyediakan metodologi tersebut (Casey dan Seglem, 2002: 8).

Menurut Thornton (1997) sebagaimana dikutip oleh Casey dan Seglem (2002: 8), ilmu forensik adalah ilmu yang dilaksanakan berdasarkan hukum dalam penyelesaian konflik. Sedangkan forensik komputer adalah seni dan ilmu menerapkan ilmu komputer untuk membantu proses hukum (Brown, 2006: 18). Menurut Brown, penyidik forensik komputer melaksanakan komponen *scientific crime scene investigation* sebagaimana didefinisikan oleh Dr. Henry C. Lee yaitu memformulasikan proses bagaimana penyidik forensik dalam mendokumentasikan dan mengumpulkan bukti mati (*physical digital*), menggunakan pengetahuan ilmiah dan teknik forensik untuk mengidentifikasi bukti dan menghasilkan panduan untuk membantu pemecahan suatu kejahatan. Masih menurut Brown, *scientific crime scene investigation* atau yang diterjemahkan sebagai penanganan TKP secara ilmiah, didasarkan pada prinsip pertukaran *Locard*, yang menyatakan bahwa ketika dua obyek saling berhubungan, selalu ada pengalihan material dari satu obyek kepada obyek yang lain. *Operating system log* mencatat tindakan *hacking* dan data yang tertinggal pada *hard disk* di bagian yang tidak teralokasi adalah contoh penggunaan prinsip *Locard*.

Menurut Casey (2000: 115-118), ilmu forensik dapat diterapkan dalam *digital evidence* di internet. Namun *digital evidence* tidak sama dengan *digital evidence* yang tersimpan dalam suatu komputer. *Digital evidence* di internet tersimpan dalam komputer yang terletak jauh seperti *web puges* atau tidak tersimpan dimanapun kecuali ada usaha untuk mencarinya. Urutan proses pemeriksaan *digital evidence*nya sama dengan proses dalam ilmu forensik. Dalam pengakuan *digital evidence*, pencarian dalam internet melalui *search engine* dapat

[110]Rekonstruksi tindak pidana (*Crime Reconstruction*) adalah proses untuk memperoleh pemahaman yang mendalam tentang suatu kejahatan dengan menggunakan bukti yang ada (Casey dan Seglem, 2002: 8).

memakan waktu lama karena masing-masing mengandung informasi yang berbeda dan caranya pun berbeda. Setiap komputer yang mengakses internet, memiliki sedikit *digital evidence*. *Web browser* menyimpan catatan situs yang dikunjungi, *email* memiliki *copy* pesan yang telah dikirimkan dan lain-lain. Dalam *preservation, collection and documentation* dari *digital evidence,* usaha keras untuk mendapatkan bukti yang tersimpan dalam komputer sangat dibutuhkan. Dan jangan mengubah *digital evidence* seperti nama *file*, dan jangan merubah isi *file* tersebut. Dalam *reconstruction,* akan lebih mudah untuk merekonstruksi beberapa aspek tertentu dari suatu kejahatan sebelum menggabungkannya menjadi utuh misal *web pages* mungkin harus diperbaiki dulu sebelum gambarnya muncul. Merekonstruksi *web pages* tentu membutuhkan keahlian yang khusus.

Menurut Brown (2006: 6-9), forensik komputer dapat dibagi menjadi 4 (empat) tahap, yaitu pengumpulan[111], pengamanan[112], penyeleksian[113] dan penyajian[114] perangkat sistem komputer yang dapat berpotensi memiliki nilai

---

[111]Tahap pengumpulan, forensik komputer tahap pengumpulan adalah ketika perangkat komputer dianggap bernilai sebagai pembuktian, diidentifikasi dan dikumpulkan. Biasanya meliputi perangkat komputer data digital dalam bentuk *disk drives, flash memory drives,* atau bentuk digital dan data lainnya, akan tetapi dapat pula meliputi perangkat komputer pendukung seperti kebijakan keamanan perusahaan dan prosedur *backup* (Brown, 2006: 6).

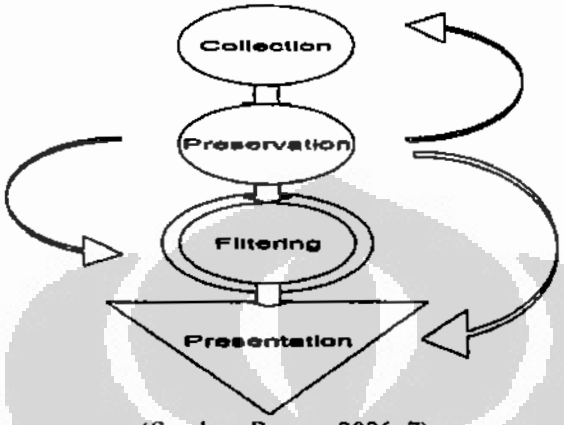
[112]Tahap pengamanan, forensik komputer tahap pengamanan terfokus pada perlindungan perangkat komputer asli dengan yang dapat dipercaya, lengkap, akurat dan dapat diverifikasi. *Cryptographic hashing, checksums,* dan pendokumentasian adalah komponen kunci dalam tahap pengamanan. Pentingnya istilah *reliable,* lengkap, akurat dan *verifiable* pada saat menyinggung bukti potensial jelas merupakan tahap yang dapat diidentifikasi, hal ini dapat dilakukan berulang-ulang melalui proses forensik komputer (Brown, 2006: 7).

[113]Tahap penyeleksian, merujuk pada tahap analisis forensik komputer. Pada tahap ini penyidik akan berusaha untuk mengeluarkan data yang tidak berisi perangkat komputer bernilai pembuktian dan menyaring perangkat komputer yang berpotensi memiliki nilai pembuktian. Berbagai alat dan teknik digunakan dalam tahap penyaringan ini, diantaranya termasuk membandingkan nilai bagian-bagian yang berisi sandi/petunjuk mengenai barang atau tersangka dari data yang telah diketahui. *Operating system* dan alat aplikasi khusus yang lainnya digunakan untuk menempatkan dan mengeluarkan data sangatlah penting untuk tahap penyeleksian. Salah satu jenis alat adalah *Internet history specific tools* yang akan menempatkan dan mengeluarkan data yang ada yang ditinggalkan oleh kegiatan *Web browser* (Brown, 2006: 7-8).

[114]Tahap penyajian adalah tahap akhir dari forensik komputer adalah ketika perangkat komputer potensial yang bernilai pembuktian disajikan atau dipresentasikan dalam berbagai bentuk. Presentasi biasanya dimulai dengan kegiatan penyidik mengeluarkan media asli dan kemudian membuat langkah-langkah dan mengorganisasikannya dalam *CD-ROM* atau *DVD-ROM*. Laporan penyidik, dokumen pendukung, pernyataan-pernyataan, disposisi-disposisi, dan kesaksian di hadapan pengadilan dapat dianggap sebagai tahap presentasi forensik komputer

pembuktian (lihat: Bagan 3.4).

Bagan 3.4
Tahap Presentasi Forensik Komputer



(Sumber: Brown. 2006: 7)

Dalam pelaksanaan tahapan forensik komputer sebagaimana diungkapkan Brown tersebut di atas, di Indonesia tidak semudah itu dapat dilaksanakan. Hal ini terkait dengan peraturan perundang-undangan berkaitan dengan pengaturan alat bukti dan barang bukti digital. Untuk tahap pengumpulan bukti digital, pengamanan dan penyaringan atau penyeleksiannya, sudah dapat dilakukan dengan cukup memadai oleh Bareskrim Polri, dengan bantuan teknis dari laboratorium forensik komputer yang terdapat pada Unit V *IT & Cybercrime* Bareskrim Polri. Akan tetapi, begitu memasuki tahap presentasi, dari beberapa kasus yang melibatkan bukti digital ternyata menghadapi hambatan yang cukup serius, terutama dalam hal menyamakan persepsi dengan penegak hukum yang lain yaitu penuntut umum dan para hakim. Seringkali dijumpai penuntut umum atau bahkan hakim yang belum dapat menerima bahwa bukti digital dapat diakui sebagai salah satu barang bukti yang dapat mendukung alat bukti yang diajukan, karena masih terpaku pada persyaratan alat bukti sebagaimana diatur dalam KUHAP.

3.2.1.4 Masalah Yurisdiksi Hukum

Berkaitan dengan masalah yurisdiksi hukum, telah diakui beberapa prinsip

---

(Brown. 2006: 9).

yurisdiksi antara lain prinsip teritorialitas sebagai prinsip dasar dalam penerapan yurisdiksi hukum suatu negara. Selain itu dikenal juga prinsip nasionalitas pelaku maupun korban, dan prinsip universalitas. Namun demikian jika terjadi konflik yurisdiksi hukum pidana dalam kaitan kejahatan yang menggunakan teknologi informasi, sampai saat ini belum ada satu lembaga internasional yang memiliki wewenang untuk memutuskan yurisdiksi negara yang berwenang menuntut dan mengadili kasus dimaksud. Sekalipun demikian prinsip umum hukum internasional sudah mengakui bahwa pilihan yurisdiksi hukum pidana terhadap *cybercrime* yang bersifat transnasional merupakan wewenang negara "*locus delicti*" dilihat dari sisi nasionalitas pelaku atau korban atau tempat dimana sarana teknologi komputer itu digunakan. Selain dari negara *locus delicti*, juga telah diterima prinsip yurisdiksi yang bersifat opsional bahwa negara lain yang telah dirugikan karena kejahatan transnasional tersebut dapat mengajukan klaim yurisdiksi yang sama.

Sedangkan menurut Darrel Mentine (2000) sebagaimana dikutip oleh Ramli (2004: 7), dalam hukum internasional dikenal tiga jenis yurisdiksi, yakni yurisdiksi untuk menetapkan undang-undang (*the jurisdiction to prescribe*), yurisdiksi untuk penegakan hukum (*the jurisdiction to enforce*) dan yurisdiksi untuk menuntut (*the jurisdiction to adjudicate*). Selanjutnya Ramli menyatakan juga bahwa berdasarkan karakteristik khusus yang terdapat didalam *cyber space* dapat dikemukakan beberapa teori yurisdiksi seperti *theory of the uploader and the downloader, theory the law of the server, the theory of international spaces.*

The theory of the uploader and the downloader. Berdasarkan teori ini, suatu negara dapat melarang dalam wilayahnya, kegiatan *uploading* dan *downloading* yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk *uploading* kegiatan perjudian atau kegiatan perusakan lainnya dalam wilayah negara, dan melarang setiap orang dalam wilayahnya untuk *downloading* kegiatan perjudian tersebut. Kota Minnesota di Amerika Serikat adalah salah satu negara bagian pertama yang menggunakan yurisdiksi ini.

Theory the law of the server. Pendekatan ini memperlakukan *server* dimana *webpages* secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data

elektronik. Menurut teori ini sebuah *webpages* yang berlokasi di *server* pada Stanford University tunduk pada hukum California. Namun teori ini akan sulit digunakan apabila *uploader* berada dalam yurisdiksi asing.

The theory of international spaces. Ruang *cyber* dianggap sebagai *the fourth space*. Yang menjadi analogi adalah tidak terletak pada kesamaan fisik, melainkan pada sifat internasional, yakni *sovereignless quality*. Secara yuridis untuk ruang *cyber* sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi hukum konvensional untuk dapat dijadikan obyek dan perbuatan.

Masih menurut Ramli, dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu: *subjective territoriality*, yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain. *Objective territoriality*, yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan. *Nationality*, yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku. *Passive nationality*, yang menekankan yurisdiksi berdasarkan kewarganegaraan korban. *Protective principle*, yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah. *Universality*, asas ini juga disebut sebagai "*universal interest jurisdiction*". Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (*crimes against humanity*), misalnya penyiksaan, genosida, pembajakan udara, dan lain-lain. Meskipun dimasa mendatang asas yurisdiksi universal ini mungkin dikembangkan untuk internet *piracy, cracking, carding, hacking* dan *viruses*.

Menurut Darius Valatkevièius, dengan berbagai yurisdiksi dalam *Convention on Cybercrime* yang dapat digunakan, tentunya memberikan dampak akan timbulnya konflik yurisdiksi mengenai negara mana yang dapat memproses

suatu kasus *cybercrime*. Oleh karena itu, keberagaman yurisdiksi tersebut harus diatasi tentunya berdasarkan alasan-alasan yang logis. Hal-hal yang harus dievaluasi oleh semua pihak adalah mengenai negara mana yang memiliki kedekatan kuat dan memiliki prioritas sebagai negara yang berhak memproses kasus *cybercrime*. Terlepas dari hak negara-negara untuk mengklaim bahwa negaranya lah yang berhak menangani kasus *cybercrime*, masalah yurisdiksi mungkin akan tetap muncul, yaitu ketika tidak ada negara yang mengakui yurisdiksinya atas suatu kasus *cybercrime*. Prinsip larangan terhadap aparat penegak hukum suatu negara untuk bertindak di dalam wilayah negara lain tanpa persetujuan yang tegas juga berlaku dalam hal mengakses data komputer seperti mencari, menampilkan atau meng*copy* informasi dari server atau komputer yang terletak di negara lain dalam hal ini di dalam internet (*http://www.leidykla.eu /en/journals/law/law-2007-vol-62/d-valatkevicius-the-problems-of-jurisdiction-in-computer-crime-investigation/*, 10 Februari 2008).

Dalam kaitan masalah yurisdiksi hukum pidana ini, sistem hukum pidana yang berlaku di Indonesia belum cukup memadai untuk menjangkau kasus kejahatan transnasional yang menggunakan komputer sebagai sarana untuk mencapai tujuannya. Peraturan perundangan di Indonesia yang bersifat khusus dan komprehensif mengenai *cybercrime* belum ada, walaupun telah disusun suatu RUU tentang Teknologi Informasi yang di dalamnya dimuat ketentuan pidana. Namun di dalam UU tersebut belum secara eksplisit mengatur masalah yurisdiksi hukum pidana atas kasus-kasus kejahatan yang dilakukan melalui teknologi informasi yang bersifat ekstrateritorial. Dalam UU ITE tersebut, yurisdiksi yang diterapkan berlaku untuk setiap orang baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

3.2.2 Rangkaian Kegiatan Penyidikan Tindak Pidana *Hacking*

Dalam memulai penyidikan tindak pidana, penyidik menggunakan parameter alat bukti yang sah sesuai dengan ketentuan Pasal 184 KUHAP yang dikaitkan dengan segitiga pembuktian (*evidence triangle*) untuk memenuhi aspek

legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi. Adapun rangkaian kegiatan penyidik dalam melakukan penyidikan tindak pidana *hacking* adalah penyelidikan, penindakan, pemeriksaan dan penyelesaian berkas perkara. Pelaksanaan tiap kegiatan penyidikan tersebut sampai dengan saat ini tetap didasarkan pada ketentuan KUHAP dan merujuk pada proses penyidikan yang dimaksud dalam Undang-undang Kepolisian serta ketentuan pelaksanaan yang termasuk dalam Buku Juklak, Buku Jukmin dan Buku Juklap yang berlaku dalam lingkungan Polri berdasarkan Surat Keputusan Kapolri. Dalam hal ini, rangkaian kegiatan penyidikan tindak pidana *hacking* pada prinsipnya bersumber pada ketentuan yang sama, sehingga prinsip-prinsip dasar pelaksanaan kegiatan tidak berbeda dengan proses penyidikan tindak pidana konvensional lainnya.

Berkaitan dengan hal tersebut, dalam praktek, pelaksanaan rangkaian kegiatan penyidikan tindak pidana *hacking* menghadapi berbagai macam karakteristik yang khas, sekaligus sebagai suatu tantangan, yang dimiliki oleh tindak pidana tersebut sebagai salah satu *cybercrime*. Sebagaimana telah dibahas sebelumnya, tantangan atau kesulitan yang paling signifikan dalam proses penyidikan tindak pidana *hacking* sebagai salah satu jenis *cybercrime* adalah proses penyidikan yang berkaitan dengan masalah pembuktian, baik karena sifat dari bukti digital yang khas, maupun karena peraturan perundang-undangan dalam sistem hukum pidana di Indonesia yang belum secara tegas dan terpadu mengatur secara khusus hal tersebut.

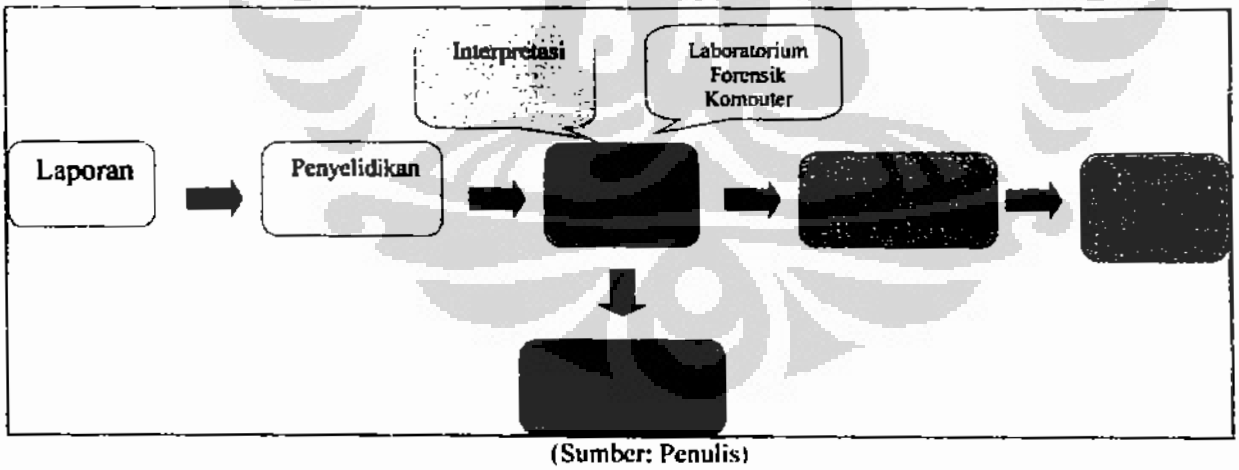
Selain karakteristik yang berkaitan dengan aspek pembuktian, aspek lain yang dalam prakteknya juga merupakan dalam proses penyidikan tindak pidana *hacking* adalah aspek yurisdiksi hukum berkaitan dengan karakteristik tindak pidana *hacking* yang khas yaitu seringkali bersifat lintas batas negara, sehingga penentuan yurisdiksi hukum mengenai siapa yang berwenang melakukan penyidikan dan penuntutan serta hukum negara mana yang harus diterapkan juga menjadi masalah yang harus diantisipasi.

Dalam hal ini bagaimana polisi bekerja secara maksimal untuk mencapai tujuan penyidikan walaupun berbagai tantangan dan kesulitan menghadang, menjadi isu yang penting, karena tidak ada alasan yang dapat diterima jika polisi tidak mampu menyelesaikan penyidikan tindak pidana *hacking* dengan alasan

adanya kesulitan dan tantangan-tantangan tersebut. Isu tersebut, membuat Polri sebagai penyidik tindak pidana *hacking* sampai saat ini tetap bekerja keras secara profesional dan menggunakan serta mendayagunakan kemungkinan dan kesempatan yang tersedia, agar terus mampu mengantisipasi perkembangan kejahatan yang dewasa ini semakin canggih. Sehingga polisi mampu menempatkan dan mendayagunakan perkembangan teknologi yang ada lebih sebagai sarana atau alat yang mendukung penyidikan yang menjadi tugasnya, dan bukan sebagai suatu kesulitan dan hambatan yang tidak mampu diatasi.

Pada dasarnya proses penyidikan tindak pidana *hacking* sama dengan proses penyidikan tindak pidana konvensional yaitu setelah laporan diterima dilakukan proses penyelidikan, penindakan, pemeriksaan dan penyelesaian berkas perkara yang kemudian hasilnya diserahkan ke kejaksaan. Namun yang membedakan proses penyidikan tindak pidana *hacking* dengan tindak pidana konvensional adalah peranan laboratorium forensik komputer. Laboratorium forensik komputer disini bertugas untuk memproses dan menemukan bukti digital yang berguna untuk membuktikan di pengadilan bahwa telah terjadi suatu tindak pidana *hacking*.

Bagan 3.5
Proses Penyidikan Tindak Pidana *Hacking*



(Sumber: Penulis)

3.2.2.1 Penyelidikan Tindak Pidana *Hacking*

Tahap penyelidikan merupakan tahap pertama yang dilakukan oleh penyidik dalam melakukan penyidikan tindak pidana serta merupakan tahap tersulit dalam proses penyidik. Dalam tahap ini penyidik harus dapat membuktikan tindak

pidana yang terjadi, bagaimana terjadinya dan apa sebab-sebab tindak pidana tersebut untuk dapat menentukan bentuk laporan polisi yang akan dibuat. Informasi biasanya diperoleh dari *National Central Bureau* (*NCB*) atau Interpol yang menerima pemberitahuan atau laporan dari negara lain yang kemudian diteruskan ke unit *cybercrime* atau satuan lain yang ditunjuk. Selain itu, laporan dari masyarakat atau pihak yang merasa telah dirugikan juga menjadi salah satu sumber informasi untuk dapat memulai suatu proses penyelidikan terhadap suatu kasus tindak pidana *hacking* dan/atau jenis *cybercrime* lainnya, selain informasi yang diperoleh dan ditemukannya sendiri oleh penyidik.

Dalam penyelidikan kasus-kasus *cybercrime* yang modusnya seperti kasus *carding* metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkotika terutama menggunakan metode *undercover* dan *control delivery*. Petugas setelah menerima informasi atau laporan dari Interpol atau *merchant* yang dirugikan melakukan koordinasi dengan pihak *shipping* untuk melakukan pengiriman barang. Permasalahan yang ada dalam kasus seperti ini adalah laporan yang masuk terjadi setelah pembayaran barang yang ternyata ditolak oleh bank dan barang sudah diterima oleh pelaku, disamping adanya kerja sama *carder* dengan karyawan *shipping* sehingga apabila polisi melakukan koordinasi informasi tersebut akan bocor dan pelaku tidak dapat ditangkap sebab identitas yang biasanya dicantumkan adalah palsu.

3.2.2.2 Penindakan Tindak Pidana *Hacking*

Penindakan dalam pelaksanaannya ditandai dengan upaya paksa seperti pemanggilan, penangkapan, penahanan, penggeledahan, dan penyitaan. Dalam penyidikan tindak pidana *hacking*, upaya paksa yang dilakukan pada prinsipnya sama sesuai dengan ketentuan baik dalam KUHAP maupun petunjuk teknis dalam lingkungan Polri. Namun perbedaannya adalah dalam hal penyitaan barang bukti dalam hal ini adalah bukti digital yang dilakukan dengan bantuan laboratorium forensik komputer.

Menurut Axelrod dan Antinozzi (2003: 182-183), kegiatan yang dilakukan laboratorium forensik komputer meliputi: menguji *file* komputer untuk *file* data dan dokumen yang relevan, membandingkan *file* data yang dipertanyakan terhadap *file* dokumen dan data, menguji transaksi komputer untuk menentukan

waktu dan urutan dimana *file* data diciptakan, pengambilan *file* data dari media penyimpanan, meliputi pemulihan data-data yang dihapuskan, melaksanakan pencarian data menggunakan kata untuk yang relevan terhadap kejahatan dalam proses investigasi, dan *decrypting*[115] dan pemulihan kata sandi, serta menganalisa kode sumber komputer untuk menentukan bagaimana program tertentu bekerja dan apa tujuan kegiatannya.

Menurut Shinder (2002: 552), dalam suatu proses pengumpulan bukti digital sedikitnya terlibat 3 pihak yaitu: *the first responders*[116] (karyawan atau petugas keamanan kantor yang datang pertama kali ke TKP), penyidik atau tim penyidik dan teknisi TKP atau ahli yang dipanggil untuk memproses bukti.

Pihak lain yang berperan penting dalam pencarian bukti *digital* adalah penyidik itu sendiri. Penyidik atau tim penyidik pada umumnya bertanggung jawab untuk mengkoordinasikan kegiatan semua pihak yang hadir di TKP dan akan bertanggung jawab untuk; menciptakan rantai komando[117], melaksanakan

---

[115]Istilah *decrypting* adalah kegiatan untuk menyadap informasi yang telah disembunyikan oleh enkripsi (Ariyus, 2005: 95).

[116]Peranan *the first responders* sangat penting karena mereka tidak boleh melakukan tindakan apapun yang dapat membahayakan hilangnya bukti di komputer dan mereka juga tidak boleh menyentuh apapun apalagi mematikan komputer. Seringkali pelaku *hacker* menyimpan *Trojan Horse* pada sistem komputer yang diserang, dimana jika komputer dimatikan atau diputus koneksi internetnya, maka secara otomatis akan memerintahkan sistem komputer untuk menghilangkan jejak, menghapus semua data yang berguna untuk penyidikan. Oleh karenanya *the first responders* harus memahami tugasnya untuk mengidentifikasi TKP dan mengamankan lokasi yang menurutnya berkaitan dengan tindak pidana yang terjadi. Dalam suatu *cybercrime* dimana bukti *digital* harus diperoleh, semua komputer termasuk apapun yang terlihat tidak berfungsi harus dianggap sebagai bagian dari TKP meliputi laptop, *notebook*, dan *portable computer* lainnya maupun *Personal Digital Assistant* (*PDA*). Selain itu *first responders* harus menunggu sampai penyidik datang yang kemudian menentukan mana yang akan disita dan mana tidak. Selain itu, *first responders* juga harus mengamankan bukti yang bersifat sementara dan rapuh. Apabila ada kondisi bukti dapat hilang sebelum penyidik datang (seperti informasi pada layar monitor yang berubah-ubah), maka sebaiknya dilakukan langkah-langkah untuk mengamankan atau merekam hal tersebut. Misalnya membuat foto layar monitor dengan kamera yang berarti juga mengamankan bukti (Shinder, 2002: 552).

[117]Menciptakan rantai komando. Penyidik yang berwenang harus yakin bahwa semua pihak yang ada di TKP menyadari adanya rantai komando dan seluruh keputusan penting harus ditentukan oleh penyidik tersebut. Komputer dan peralatan lainnya yang terkait tidak boleh digunakan, atau dipindahkan tanpa instruksi jelas dari penyidik. Penyidiklah yang menentukan bentuk dan mengendalikan penyidikan. Jika penyidik yang bertugas harus meninggalkan TKP maka harus didelegasikan penyidik lain untuk tinggal di TKP yang akan bertanggung jawab atas TKP dan harus tetap berhubungan dengan semua pihak sampai seluruh bukti dikumpulkan dan dipindahkan ke tempat penyimpanan yang aman (Shinder, 2002: 554).

pencarian TKP[118] dan memelihara integritas bukti (Shinder, 2002: 554-555).[119]

Pemegang peran penting lainnya dalam pencarian bukti *digital* adalah ahli/teknisi TKP yang apabila mungkin telah dididik dan dilatih secara khusus dalam bidang forensik komputer. Menurut Clifford (2006: 155-166), dalam melakukan pengumpulan *digital evidence* di TKP sedapat mungkin dilakukan oleh orang yang ahli komputer untuk menjaga keotentikan bukti. Tentu harus ada kejelasan mengenai wewenang dan payung hukum bagi orang tersebut agar dapat memeriksa komputer atau barang bukti tersebut tentunya pekerjaan itu dilakukan dibawah pengawasan penyidik.

Ahli forensik komputer harus memiliki latar belakang yang kuat mengenai teknologi komputer dan pengetahuan yang luas mengenai bagaimana *disk* dibuat/dibentuk, bagaimana sistem *files* bekerja, serta bagaimana dan dimana data direkam/disimpan. Secara umum ahli TKP *hacking* bertanggung jawab atas tugas-tugas meliputi:[120] pengamanan bukti yang mudah menguap/rusak, mematikan

---

[118]Melaksanakan pencarian TKP. Penyidik harus mengatur pencarian TKP, yang mungkin akan dilakukan oleh penyidik atau pun petugas lainnya. Jika ijin telah diperoleh, penyidik/petugas harus mencari seluruh *hardware*, *software*, catatan tertulis dan lain-lain yang berkaitan dengan operasi komputer. Hal ini termasuk pada printer, *scanner*, dan semua media penyimpanan: disket, disket optik (*CD, DVD*, dll), rekaman, Zip atau Jaz dan *removable disk* lainnya, ataupun *hard disk* "extra" yang mungkin ada di tempat tersebut (Shinder, 2002: 554).

[119]Memelihare integritas bukti. Penyidikan harus berlanjut pada pemeliharaan bukti yaitu dengan melakukan persiapan untuk mengamankan *volatile evidence* (bukti yang mudah rusak), membuat duplikat disket, dan secara aman mematikan sistem komputer. Penyidik harus mengawasi kegiatan teknisi TKP dan menyampaikan pertimbangan khusus yang harus dilakukan berdasarkan kasusnya dan pengetahuan mengenai tersangka (Shinder, 2002: 555).

[120]Tugas-tugas ahli TKP meliputi : **Pengamanan bukti** yang mudah menguap/rusak (*volatile evidence*) dan membuat duplikat disket. Data yang mudah menguap/rusak terdapat di dalam *memory* komputer dan terdiri dari proses yang bekerja. Disket harus dibuat duplikatnya sebelum komputer dimatikan ("*shut down*"). **Mematikan sistem** sebelum dibawa ke tempat penyimpanan bukti. Proses mematikan komputer harus dilakukan secara benar, dengan menggunakan metode standar untuk menghindari hilangnya *files* dalam sistem. **Pelabelan dan penyimpanan bukti.** Seluruh bukti harus diberi tanda dengan singkatan nama dari penyidik atau teknisi, waktu dan tanggal dikumpulkan, nomor kasus, dan informasi yang teridentifikasi. **Pengemasan bukti.** Bukti komputer, khususnya setiap *circuits boards* yang terlihat (seperti *hard disk*), harus ditempatkan pada kantong yang aman. Dokumentasi berupa kertas harus ditempatkan pada kantong plastik atau harus dilindungi dari setiap kerusakan. **Membawa bukti** dengan ketentuan seluruh bukti yang diperoleh harus segera dibawa ke tempat penyimpanan yang aman. Selama dalam proses penyidikan, bukti tidak boleh terhubung dengan segala peralatan yang dapat menghasilkan medan magnet (termasuk radio polisi dan perlengkapan elektronik lainnya) atau dibiarkan di bawah matahari ataupun diletakkan di tempat yang suhunya dapat meningkat. **Memproses bukti**, dimana ketika disket duplikat dibawa ke laboratorium, *image* dari disket dapat direkonstruksi dan data yang diperoleh dianalisa dengan menggunakan *forensic software tools* yang bersifat khusus (Shinder, 2002: 555-556).

sistem sebelum dibawa ke tempat penyimpanan bukti, pelabelan dan penyimpanan bukti, pengemasan bukti, membawa bukti, memproses bukti (Shinder, 2002: 555-556).

Dalam memproses bukti, kegiatan yang dilakukan adalah menganalisis bukti. Dalam tahap ini, analisis forensik atas suatu bukti seringkali sangat krusial. Pada tahap ini pula dilakukan tindakan yang seringkali dikenal dengan istilah *computer hacking forensic investigation* yang berarti suatu proses untuk mendeteksi serangan-serangan dan secara wajar mencari bukti untuk melaporkan kejahatan ataupun pelaksanaan audit untuk mencegah serangan di kemudian hari. Forensik komputer adalah aplikasi investigasi komputer dan analisis teknik untuk kepentingan penentuan bukti hukum yang potensial. Bukti dapat dicari pada berbagai kejahatan *hacking* atau jenis *cybercrime* lainnya. Untuk itu, perlu suatu metode atau prosedur yang tepat yang dapat dipergunakan untuk menemukan data yang tersimpan dalam sistem komputer atau mengembalikan informasi *file* yang rusak, dihapus atau *encrypted* (*http://www.globalnettraining.com/certified-ethical-hacking-chfi-boot camp.asp*, 10 Februari 2008).

Seperti penyidikan tindak pidana lainnya, pelaksanaan penyidikan tindak pidana *hacking* juga mensyaratkan dipenuhinya ketentuan hukum yang berkaitan dengan prosedur penyidikan dan perlindungan hak asasi manusia. Penyidikan tindak pidana *hacking* juga dilakukan sesuai ketentuan hukum. Prosesnya meliputi analisis forensik dan penyajian laporan kepada penuntut umum untuk tindak lanjut upaya hukum selanjutnya. Penangkapan, penahanan dan pengadilan jika diperlukan dapat dilakukan.

Berbagai teknik dan prosedur penyidikan tindak pidana *hacking* dan/atau *cybercrime* telah dibahas dan didiskusikan oleh berbagai ahli di bidang keamanan teknologi informasi maupun para penegak hukum di bidang *cybercrime*. Persamaan yang signifikan dari pendapat para ahli tersebut adalah perlunya penyidik yang *familiar* dengan proses pengumpulan data, materi-materi, dan informasi yang mungkin berkaitan dengan penuntutan suatu kejahatan, diantaranya yang disampaikan Shinder (2002: 637) bahwa *criminal investigation* memerlukan informasi yang dikenal oleh penyidik untuk dipergunakan dalam proses membuktikan kesalahan terdakwa di hadapan pengadilan. Menurutnya,

proses penyidikan tindak pidana tersebut harus diformulasikan untuk menyediakan struktur standar yang sesuai dengan ketentuan hukum yang mengatur mengenai pengumpulan bukti-bukti. Selain itu, seorang penyidik yang menjalankan tugas penyidikan *cybercrime*[121] juga dapat menggunakan alat-alat investigasi standar (*standard investigative tools*), yang terdiri dari informasi; wawancara dan interogasi; instrumen[122].

---

[121]Adapun langkah-langkah yang diperlukan dalam penyidikan *cybercrimes* menurut Shinder (2002: 646-650) terdiri dari: **Analisa Laporan;** meliputi evaluasi kemungkinan pernyataan bahwa pelanggaran hukum telah terjadi, mempertimbangkan jenis dan keseriusan kejahatannya, dan mempertimbangkan faktor-faktor lain yang mungkin membuat kompleks penuntutan kejahatan. **Mengumpulkan bukti-bukti fisik;** walaupun bukti-bukti mungkin dalam bentuk digital atau elektronik, akan tetapi disk dimana bukti tersimpan adalah suatu benda berwujud yang dapat dikumpulkan, diberi tanda, dan disimpan dalam tempat yang aman untuk proses pengadilan. Bukti-bukti fisik selain informasi digital, meliputi sidik jari, dokumen dan lain-lain, yang harus dilaksanakan sesuai dengan praktek standar. **Mencari pendapat ahli;** jika diperlukan; dalam hal kejahatan melibatkan rincian teknis di luar pengetahuan penyidik dan/atau penuntut, seringkali hal ini menjadi bagian investigasi. Pendapat ahli tersebut diperoleh dari pendapat dari ahli-ahli sesuai bidangnya, termasuk mencari penterjemah dalam hal saksi-saksi menggunakan bahasa asing. Dalam kasus *cybercrimes*, biasanya dipergunakan pendapat ahli dari para akademisi, ahli komputer, atau instruktur keamanan komputer. **Interview saksi-saksi dan interogasi tersangka;** langkah ini dapat menjadi proses yang terus berlanjut selama proses investigasi. **Menyusun laporan kasus;** setelah semua bukti fisik telah dikumpulkan dan didokumentasikan serta interogasi telah dilaksanakan, maka langkah selanjutnya adalah memulai penyusunan laporan kasus. Hal ini adalah elemen penting dalam tahap persiapan kasus. Dokumen kasus memuat seluruh dokumentasi kasus termasuk tetapi tidak terbatas pada laporan permulaan dari penyidik yang menindaklanjuti laporan pidana; menindaklanjuti laporan-laporan; dokumentasi bukti-bukti; laporan laboratorium dari ahli forensik; pernyataan-pernyataan tertulis dari saksi-saksi, tersangka, dan ahli; laporan TKP, foto-foto dan rekaman *video*; *print out* dari bukti-bukti *digital* yang berkaitan. **Analisa kasus;** ketika dokumen kasus telah dibuat dan seluruh dokumentasi telah dimasukkan, maka langkah selanjutnya adalah menganalisis informasi hukum dan bukti-bukti yang ada. Langkah ini biasanya dilakukan melalui kerjasama dengan penuntut, yang mungkin dapat memberikan arahan kepada penyidik atas kelemahan-kelemahan kasus dan tambahan informasi atau bukti yang perlu untuk diperoleh dalam rangka memperkuat tuntutan. **Menindaklanjuti kasus;** setelah melakukan analisis, penyidik perlu memperoleh bukti tambahan atau klarifikasi fakta-fakta dan informasi. *Interview* ulang dengan saksi-saksi dapat dilakukan pula dalam tahap ini, untuk memperoleh informasi tambahan khusus dan menyegarkan ingatan tentang kasusnya, dan menyiapkan saksi-saksi untuk proses persidangan jika kasusnya bergulir ke pengadilan. **Membuat keputusan untuk menuntut;** setelah informasi tambahan diperoleh, berkas perkara dinyatakan lengkap, penuntut umum akan membuat keputusan untuk melakukan penuntutan hukum kepada tersangka dalam suatu persidangan (tergantung dari yurisdiksi dan prosedurnya). Dalam tahap ini, pilihan jenis tuntutan juga ditetapkan berdasarkan kemampuan pembuktian elemen-elemen dan kesulitan memperoleh pengakuan serta hukuman.

[122]**Informasi;** sebagai dasar bagi suatu kasus, informasi dapat diperoleh dengan berbagai jalan, mulai dari observasi, pengujian dokumen atau data elektronik, dan pengujian bukti-bukti fisik. Dalam kasus *cybercrime*, kebanyakan bukti-bukti tersimpan dalam *hard disk* atau bahkan masih dalam *memory*. Walaupun demikian, yang terpenting bagi penyidik adalah memperoleh informasi melalui *crime scene search*, yang bertumpu pada komputer. *Wawancara* dan **interogasi;** alat ini dipergunakan untuk memperoleh informasi dari pihak-pihak yang terlibat dalam *cybercrime*. *Interview* meliputi perolehan informasi dengan memberikan pertanyaan kepada saksi-saksi, korban, dan pihak lain yang mungkin memiliki informasi yang relevan pemecahan

3.2.2.3 Pemeriksaan Tindak Pidana *Hacking*

Penerapan pasal-pasal yang dikenakan terhadap suatu kasus tindak pidana *hacking* merupakan suatu permasalahan tersendiri. Dalam hal terdapat *hacker* yang melakukan pencurian data, apakah dia dapat dikenakan pasal 362 KUHP. Pasal tersebut mengharuskan ada sebagian atau seluruhnya milik orang lain yang hilang, sedangkan data yang dicuri oleh *hacker* tersebut sama sekali tidak berubah. Pemeriksaan terhadap saksi dan korban dalam kasus tindak pidana *hacking* juga banyak mengalami hambatan. Mereka hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan tersebut seperti tampilan yang berubah maupun tidak berfungsinya program yang ada.

Peranan ahli memegang peranan cukup penting dalam memberikan keterangan pada kasus tindak pidana *hacking*. Hal tersebut berkaitan dengan keperluan untuk memperoleh keterangan yang valid yang hanya dapat diperoleh dari ahli yang mengerti mengenai apa yang terjadi dalam dunia *cyber*. Ahli tersebut harus mempunyai keterampilan dan keahlian yang spesifik mengenai bidang yang akan dijelaskannya. Dalam proses penyidikan tindak pidana *hacking*, seringkali melibatkan lebih dari satu ahli sesuai dengan permasalahan yang dihadapi. Khusus untuk kasus *deface*, disamping diperlukan ahli yang menguasai desain grafis juga dibutuhkan ahli yang memahami masalah jaringan serta program-program yang terkait dengan tindak pidana *hacking*.

Untuk kasus *cybercrime* lainnya, misalnya *carding*, masalah yang seringkali muncul adalah kesulitan melakukan pemeriksaan terhadap saksi korban, yang kebanyakan berada di luar negeri sehingga menyulitkan dalam melakukan

---

kasus. Sedangkan interogasi meliputi perolehan informasi dengan memberikan pertanyaan kepada pihak-pihak (para tersangka) yang dicurigai melakukan *cybercrimes*. Adapun tekniknya dilakukan dengan pendekatan simpatik yang meliputi: pendekatan logis; menggunakan alasan-alasan untuk meyakinkan tersangka untuk mengakui perbuatannya; *indifference;* dengan berpura-pura tidak memerlukan pengakuan karena penyidik telah memiliki cukup bukti walaupun tanpa pengakuan. Hal tersebut efektif untuk kasus dengan banyak tersangka, dimana keterangan yang bersangkutan saling dikonfrontir; *Facing-saving approach*; dengan membiarkan tersangka memberikan alasan-alasan atas tindakannya dan menunjukkan pengertian mengapa yang bersangkutan melakukan tindakan tersebut. **Instrumen;** kegunaan teknologi dalam memperoleh bukti-bukti. Dalam kasus-kasus *cybercrimes*, penggunaan data teknik *recovery* untuk menemukan informasi yang telah "*deleted*" dan "*erased*" dalam suatu disket adalah tipe instrumennya. Selain itu, contoh-contoh tradisional lainnya meliputi teknik forensik untuk mengumpulkan dan menganalisa bukti-bukti, analisa *Deoxyribonucleic Acid* (*DNA*) dan yang sejenisnya (Shinder, 2002: 640-644).

pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban. Apakah mungkin nantinya hasil BAP dari luar negeri yang dibuat oleh kepolisian setempat dapat dijadikan kelengkapan isi berkas perkara ?. Mungkin nanti apabila tanda tangan digital (*digital signature*) sudah disahkan maka pemeriksaan dapat dilakukan dari jarak jauh dengan melalui *email* atau *messenger*.

Contoh lain diantaranya kasus yang menggunakan internet sebagai sarana untuk melakukan penghinaan dan pelecehan. Penggunaan internet dalam hal itu sangatlah efektif untuk "pembunuhan karakter". Penyebaran gambar porno atau *email* yang mendiskreditkan seseorang sangat sering terjadi. Permasalahan yang ada berkaitan dengan adanya keengganan dari pihak yang menjadi korban untuk melaporkan tindak pidana tersebut ke polisi ataupun menjadi saksi karena berbagai alasan. Apabila hanya berupa tulisan atau foto-foto yang tidak terlalu *vulgar*, penyidik tidak dapat bersikap aktif dengan langsung menangani kasus tersebut melainkan harus menunggu laporan dari mereka yang merasa dirugikan karena kasus tersebut merupakan delik aduan (pencemaran nama baik dan perbuatan tidak menyenangkan).

3.2.2.4 Penyelesaian dan Penyerahan Berkas Perkara Tindak Pidana *Hacking*

Tahap penyelesaian dan penyerahan berkas perkara adalah tahap akhir dalam rangkaian kegiatan tindak pidana *hacking* atau pada umumnya *cybercrime*. Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang sering timbul adalah masalah barang bukti. Sebagaimana telah dijelaskan sebelumnya, barang bukti yang ditemukan dalam kasus tindak pidana *hacking* seringkali merupakan bukti digital. Dalam hukum yang berlaku di Indonesia, bukti digital belum memiliki rumusan yang jelas dalam penentuannya sebab bukti digital tidak selalu tersedia dalam bentuk fisik yang nyata. Mengenai masalah barang bukti ini, seringkali menimbulkan masalah karena tidak ada kesamaan persepsi diantara para aparat penegak hukum, sehingga seringkali proses penyerahan berkas perkara untuk proses selanjutnya yaitu penuntutan oleh penuntut umum ke hadapan pengadilan menjadi terhambat.

Selama ini dalam praktek, beberapa penegak hukum masih mempunyai

persepsi lain terkait dengan istilah hukum tentang barang bukti dan alat bukti, sebagaimana yang diatur dalam pasal 184 ayat (1) KUHAP. Dalam hal pengertian barang bukti, khususnya mengenai *digital evidence*, dimungkinkan adanya 3 (tiga) alat bukti dalam 1 (satu) barang bukti, contohnya dalam hal *recovery hard disk*, akan didapatkan alat bukti berupa surat, petunjuk dan keterangan ahli sebagaimana pasal 184 ayat (1) KUHAP.

3.2.3 Dukungan Teknis Penyidikan

Dalam proses penyidikan tidak dapat dipungkiri perlunya dukungan teknis untuk menunjang kelancaran dan kemudahan penyidikan. Dukungan teknis ini meliputi ketersediaan personal atau sumber daya manusia yang handal, sarana prasana yang bersifat *up to date* terhadap perkembangan teknologi serta akses kerja sama dengan pihak eksternal baik dari dalam negeri maupun luar negeri.

a. Laboratorium Forensik Komputer

Salah satu pendukung teknis yang memegang peranan penting adalah tersedianya sarana prasarana teknologi informasi yang *up to date*. Tanpa adanya dukungan teknis ini hampir pasti penyidikan tindak pidana *hacking* tidak dapat dilaksanakan. Sebagaimana sifat kejahatannya yang melibatkan komputer dan jaringannya, maka pengungkapannya pun akan selalu melibatkan dan menggunakan komputer dan jaringannya sebagai alat pendukung teknis. Dalam praktek, sarana prasarana tersebut diwujudkan dalam suatu laboratorium yang dikenal dengan sebutan laboratorium forensik komputer. Laboratorium inilah yang digunakan oleh penyidik untuk melakukan *computer forensic investigation*. Disinilah pengelolaan TKP dilakukan baik oleh teknisi komputer maupun penyidik yang mempunyai pengetahuan dan kemampuan forensik komputer.

Pengetahuan dan kemampuan forensik komputer dasar merupakan syarat mutlak yang harus dimiliki oleh ahli teknisi komputer atau bahkan penyidik yang melakukan tugas penyidikan forensik komputer. Pengetahuan dan keahlian yang diperlukan tersebut dapat berbeda-beda dari kasus ke kasus, oleh karenanya penyidik perlu untuk mengerti bagaimana komponen komputer bekerja dan bagaimana komponen-komponen tersebut berinteraksi satu dengan lainnya. Komponen penting tersebut meliputi *central processor, Physical RAM (Random*

Access Memory), Alat-alat independen pada *output* dan *input* komputer, dan *physical storage*.

Penyidik harus memahami bagaimana *central processor* dengan *physical RAM* bekerja dalam suatu komputer, bagaimana *physical RAM* bekerja dengan *operating system* yang berbeda sehingga menghasilkan *memory* pada *hard disk*. Penyidik harus menguasai dan memahami bagaimana alat-alat tersebut berinteraksi satu dengan lainnya. Seluruh *items* yang berfungsi untuk menyimpan dan memanggil data dari dalam *physical storage* seperti *hard disk*. Penyidik harus benar-benar memahami dan menguasai proses fungsi *items* tersebut dan proses untuk menghasilkan data yang diperlukan.

Pengetahuan dan kemampuan ahli teknisi komputer atau penyidik, dapat diperoleh dengan mengikuti program-program pendidikan dan pelatihan yang tersedia melalui perusahaan-perusahaan yang membuat *software* dan peralatan forensik, seperti NTI (*www.forensics-intl.com/training.html*) dan DIBS (*www.dibsusa.com/training/training.html*), melalui komunitas perguruan tinggi dan universitas, melalui beberapa lembaga penegakan hukum yang memberikan pelayanan pendidikan ataupun melalui asosiasi dan organisasi forensik/kejahatan komputer. Selain itu, penyidik juga perlu untuk mengambil ujian sertifikasi seperti sertifikat COMTIA A+, yang dirancang untuk mengakui pengetahuan *PC* tingkat dasar yang disyaratkan untuk ahli/teknisi *PC*. Penyidik juga harus ingat bahwa walaupun sertifikasi untuk tingkat dasar itu juga penting, namun pendidikan lanjutan dan pengalaman juga tidak kalah pentingnya.

Dewasa ini, program akreditasi dan sertifikasi Laboratorium Forensik yang paling diterima dan diutamakan adalah *ISO* 17025. Selain itu dikenal juga program sertifikasi untuk forensik komputer yang dikenal dengan *Certified Forensic Computer Examiner* (*CFCE*) *Certification* yang diterbitkan oleh *IACIS* serta *Certified Computer Forensic Technition Crime Investigator* dan *Certified Computer Crime Investigator Certifications* dari *The High Tech Crime Network* (*HTCN*).

Sertifikasi yang diterbitkan oleh *IACIS* ditujukan untuk individu baik dari kalangan penegak hukum maupun dari kalangan lainnya. *IACIS* mengajukan suatu

aplikasi yang mendemonstrasikan pengetahuan yang luas, pelatihan dan atau pengalaman dalam bidang forensik komputer bersama dengan pengertian pengertian atas prosedur, standar, etika dan masalah hukum serta masalah *privacy*. Calon peserta harus memiliki pengetahuan dan keahlian teknis dan mempunyai peralatan yang diperlukan untuk melaksanakan pengujian forensik. Untuk memperoleh sertifikasi, calon peserta juga lulus dalam proses ujian dimana mereka harus melengkapi sejumlah latihan penyelesaian masalah, menyiapkan laporan dan mempresentasikan bukti yang diperoleh, kemudian lulus ujian tertulis. Informasi mengenai sertifikasi *CFCE* dapat diperoleh lebih lanjut pada *web-site www.cops.org/External%20Certification.html.*

Berbeda dengan program sertifikasi yang ditawarkan *CFCE*, *HTCN* menawarkan sertifikasi baik dasar maupun lanjutan untuk teknisi komputer dan penyidik kasus *cybercrime*. Untuk memperoleh sertifikasi dari *HTCN* tersebut, peserta harus mampu memperlihatkan sedikitnya kombinasi pendidikan dan pengalaman dalam bidang penegakan hukum atau lingkungan kerja, dan menyampaikan dokumentasi berasal dari sepuluh kasus. Informasi mengenai *HTCN* dapat diperoleh lebih lanjut pada *web-site www.htcn.org/certification.htm.*

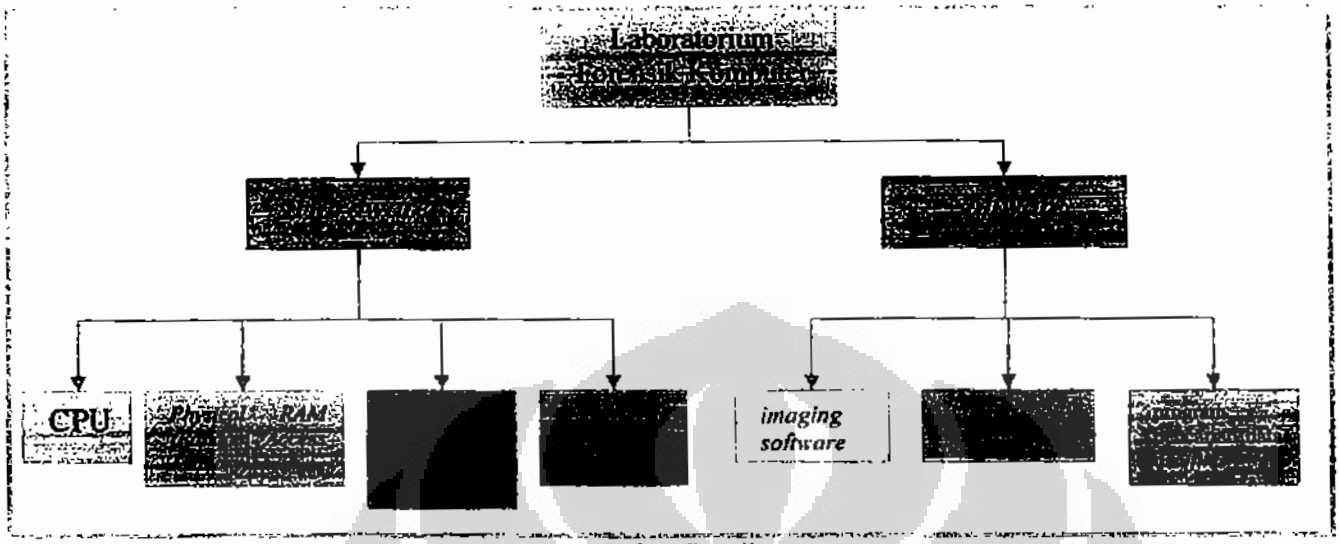
Selain penyidik atau ahli/teknisi komputer pelaksana tugas penyidikan forensik komputer harus mempunyai kemampuan dan pengetahuan forensik komputer yang baik, sarana perlengkapan pendukung yang juga harus tersedia dalam proses penyidikan melalui kegiatan forensik komputer adalah perlengkapan dan *software* forensik komputer. Adapun jenis perlengkapan yang dapat digunakan untuk pelaksanaan penyidikan forensik komputer.

Alat *imaging*. Alat ini dipergunakan untuk membuat salinan *bitstream* dari suatu *hard disk* ke dalam suatu *hard disk* lainnya, atau alat penyimpan data lainnya seperti *optical cartridge* atau *tape*. Selain itu dapat dipergunakan pula untuk melakukan *write-protection features* untuk meyakinkan bahwa data tidak dapat dirusak setelah dilakukannya proses *copy* tersebut. Alatnya dapat berupa unit *portable* yang mudah dibawa dalam tas kerja sehingga dibawa-bawa secara mudah ke lokasi TKP untuk melakukan proses *copy* di tempat kejadian sebelum komputer dimatikan (*shut down*).

Forensic Workstation yang lengkap dibuat untuk memudahkan proses rekonstruksi dan analisis dari *drives* yang di-*copy*, biasanya dengan *drive racks* yang dapat dipindah-pindah, yang memungkinkan proses menyalakan "*working copies*" dari disket tersangka. Analisis *software* di-*install* untuk membantu mencari jenis data khusus dengan menggunakan teknik *Artificial Intelligence* (*AI*) atau *fuzzy logic*. *Data recovery software* di-*install* untuk menyimpan data dari *files* yang diharus atau dirusak. *Workstation* yang dapat berpindah-pindah dipasang dalam suatu komputer *portable*. Contohnya *DIBS forensic workstation* dan *Forensic Recovery of Evidence Device* (*FRED*) yang dibuat oleh *Digital Intelligence* (*www.digitalintel.com/fred.htm*).

Paket-paket *software* forensik yang disediakan oleh perusahaan-perusahaan seperti *NTI* dan *DIES*, diantaranya *imaging software*, *"undeleted" programs*, serta program pencarian data dan *files*. Program-program tersebut diantara digunakan untuk melakukan proses verifikasi akurasi *bitstream copies*, untuk memudahkan proses analisis data secara lebih mudah, untuk membuat direktori data dan *files* secara lebih mudah, untuk mencari dan menemukan data yang terletak pada ruang yang tidak teralokasi, dan lain-lain. *Website* yang menunjukkan beberapa program *software* forensik yang terbaik diantaranya *website* milik *Timberline Technologies* pada *www.timberlinestechnologies.com /products/forensics.html*. Beberapa alat forensik juga dapat diperoleh secara gratis dari perusahaan *NTI* pada alamat *www.forensic-intl.com/download.html*.

Bagan 3.6
Perangkat di Laboratorium Forensik Komputer



(Sumber: Penulis)

Tabel 3.1
Daftar *Hardware* dan *Software* di Laboratorium Forensik Komputer
Unit V *IT & Cybercrime*

NO	DESKRIPSI	JUMLAH	JENIS	KEGUNAAN
1	*Forensic Computer's Original Forensic Tower II*	4	*Hardware*	Komputer yang digunakan untuk menganalisa barang bukti digital (*Hard drive, CD, Removable Disk*)
2	*FRED Computer Analysis*	1	*Hardware*	Komputer yang digunakan untuk menganalisa barang bukti digital (*Hard drive, CD, Removable Disk*)
3	*Dell Inspiron 9400*	3	*Hardware*	Laptop untuk menganalisa barang bukti digital
4	*Airlite Mobile Forensic Machines*	2	*Hardware*	Laptop mobile + Write Blocker Kit yang digunakan untuk menganalisa barang bukti digital (*Hard drive, CD, Removable Disk*)
5	*Image MASSter Solo-3*	1	*Hardware*	Alat *clonning harddsik*
6	*Logicube talon kit*	2	*Hardware*	Alat *clonning* dan *imaging hard disk*
7	*Maxtor 300GB External hard disk*	2	*Hardware*	*Backup* data
8	*3Com Baseline Dual Speed Hub*	1	*Hardware*	Alat yang berfungsi sebagai terminal jaringan
9	*HP Deskjet 5650 Printer*	1	*Hardware*	Alat cetak
10	*100 piece Toolkit*	3	*Hardware*	Alat perlengkapan
11	*Stego (Stego Search Software) Suite*	2	*Software*	*Software* untuk memeriksa *file* steganografi

NO	DESKRIPSI	JUMLAH	JENIS	KEGUNAAN
12	*Gargoyle Investigator (Malicious Programs Search Software)*	2	*Software*	*Software* untuk analisa program *malicious, payware*
13	*APC International Back UPS 350 USB*	7	*Hardware*	*Battery Backup PC*
14	*Easy Media Creator Suite 9*	4	*Software*	*Software* untuk membuat data digital, video dan foto
15	*Dymo Letra Tag*	1	*Hardware*	Alat untuk membuat label
16	*Cushioned Shield Bag*	3-100 *PCs*	*Hardware*	Plastik elastis untuk melindungi *harddsik* dan media digital lainnnya.
17	*Prtition Magic 8.0*	4	*Software*	*Software* untuk mempartisi *hard disk*
18	*Kanguru 60Gb Media X change 2.0*	1	*Hardware*	Alat untuk mem*backup* data dari *memory card* tanpa menggunakan komputer
19	*4 port USB Hub*	2	*Hardware*	Terminal USB 4 port
20	*Canon Scan LiDE 60*	1	*Hardware*	Alat *scanning*
21	*SATA Write Protect Adapter*	2	*Hardware*	Alat untuk proteksi *hard disk*
22	*Encase V.4 Forensic Software*	3	*Software*	*Software* untuk menganalisa barang bukti digital (*recovery data*)
23	*Encase V. 5 Forensic Software*	5	*Software*	*Software* untuk menganalisa barang bukti digital (*recovery data*)
24	*Encase V. 6 Forensic Software*	1	*Software*	*Software* untuk menganalisa barang bukti digital (*recovery data*)
25	*Acces Data Ultimate Forensic Toolkit*	5	*Software*	*Software* untuk menganalisa barang bukti digitel (*recovery data*)
26	*WipeDrive & Media Wiper*	7	*Software*	*Software* untuk membersihkan *hard drive* atau *CD-R* sebelum *hard drive* tersebut dipakai untuk mem*backup* barang bukti
27	*Paraben's Device Seizure Kit*	3	*Hardware + Software*	Alat untuk menganalisa *handphone*
28	*Belkin RJ45 CAT5e Patch Cable*	1	*Hardware*	Alat detektor kabel jaringan LAN
29	*Toolkit forensic komputer*	4	*Hardware*	Peralatan forensik komputer secara *mobile*
30	*USB 2.0 to SATA/IDE*	4	*Hardware*	Alat yang digunakan untuk menghubungkan *hard drive* SATA/ IDE ke forensik komputer
31	*Fastblock*	3	*Hardware*	Alat yang menghubungkan antara forensik komputer dengan barang bukti digital untuk dianalisa (*Write Protect*)
32	*Cyber Shot Digital Camera*	5	*Hardware*	Kamera yang digunakan untuk dokumentasi barang bukti
33	*Wireles Broadband Router (WAP)*	1	*Hardware*	*Wireless* untuk koneksi internet

NO	DESKRIPSI	JUMLAH	JENIS	KEGUNAAN
34	*Maxtor External Hard drive 300 GB*	2	*Hardware*	*Hard drive* untuk mem*backup* hasil analisa barang bukti sementara
35	*Ultrakit*	2	*Hardware*	Peralatan forensik komputer secara *mobile*
36	*Net Analysis*	1	*Software*	*Software* untuk pemeriksaan internet *history*
37	*Encase Fim*	1	*Software*	*Software* untuk menganalisa barang bukti digital (*recovery data*) melalui jaringan
38	*I2 Analyst Notebook*	1	*Software*	*Software* untuk menganalisa/ pelacak no *handphone*
39	*ACOS5 Card Reader*	1	*Hardware*	Alat untuk membaca berbagai jenis kartu *memory* (MMC)
40	*Cyptomate Client Kit Software*	1	*Hardware + Software*	Alat untuk mengkompres *file*
41	*ACR-100 Software*	1	*Software*	*Software driver* ACR-120 Smart Card Reader
42	*ACR-120 Smart Card Reader*	1	*Hardware + Software*	Alat untuk membaca kartu *contactless smart card*
43	*ACS-SIMmate2*	2	*Software*	Alat untuk membaca SIM *Card*
44	*DEMI-UAS*	1	*Hardware*	Alat *clonning hard disk*
45	*Magnetic card Reader*	1	*Hardware*	Alat untuk membaca *magnetic card*

(Sumber: Penulis)

b. Kerjasama dengan *Internet Service Provider* (*ISP*)

Dukungan teknis penyidikan diperlukan oleh penyidik dari pihak eksternal kepolisian. Dalam hal ini polisi seringkali sulit untuk dapat melengkapi seluruh tahap penyidikan tindak pidana *hacking*, tanpa memiliki hubungan kerja sama dengan berbagai pihak, khususnya pihak eksternal kepolisian baik dari perusahaan *ISP*, maupun dari para ahli teknisi komputer. Contohnya dalam penyidikan tindak pidana *hacking*, polisi memperoleh data *log files* dari server yang terdapat pada perusahaan *ISP* dimana si tersangka memperoleh *IP Address* atau *IP Address* yang dipergunakan si tersangka untuk melakukan serangan terdaftar. Hubungan kerja sama yang baik dan adanya dukungan teknis dari *ISP* akan sangat membantu memudahkan tugas penyidik dalam melaksanakan penyidikan tindak pidana *hacking*.

Hal yang sama diungkapkan oleh informan penelitian berasal dari *United Kingdom* (UK) yang memberikan penjelasan melalui *email* mengenai pentingnya

pihak eksternal dalam proses penyidikan, secara tegas yang bersangkutan menyatakan bahwa polisi hampir tidak pernah memiliki keahlian teknis untuk dapat melengkapi seluruh proses penyidikan. Berdasarkan pengalamannya baik sebagai penyidik maupun karyawan dari dunia industri, dia berkesimpulan bahwa untuk melakukan analisis *malware* atau *log files* dalam proses pengujian komputer, bantuan dunia industri sangat penting hampir terhadap semua kasus. Keengganan untuk memanfaatkan dunia industri seringkali berlandaskan alasan biaya dan juga isu kepercayaan.

Begitupun di Indonesia, dalam proses penyidikan tindak pidana *hacking* juga bergantung pada kerja sama dengan perusahaan *ISP* ataupun asosiasi penyelenggara jaringan internet lainnya. Tanpa ada kerja sama dengan pihak-pihak dari perusahaan *ISP* tersebut, penyidik dihadapkan pada masalah kesulitan memperoleh data guna menelusuri keberadaan si tersangka *hacker*.

3.2.4 Administrasi Penyidikan

Pada prinsipnya administrasi yang diterapkan dalam proses penyidikan tindak pidana *hacking* atau *cybercrime* bersumber dari ketentuan umum maupun ketentuan pelaksanaan dan petunjuk-petunjuk mengenai pelaksanaan administrasi penyidikan tindak pidana yang berlaku dan ditetapkan dalam lingkungan Polri. Walaupun secara spesifik proses penyidikan tindak pidana *hacking* dan *cybercrime* berbeda dan mempunyai karakteristik yang khas yang membedakannya dengan tindak pidana konvensional pada umumnya, namum berkaitan dengan administrasi penyidikan belumlah perlu untuk dilakukan pembedaan, sehingga prosedur dan tata cara administrasi penyidikan yang diterapkan secara umum masih dapat diberlakukan dalam proses administrasi penyidikan tindak pidana *hacking* dan *cybercrime*.

Hal yang paling signifikan berkenaan dengan proses administrasi penyidikan tindak pidana *hacking* berkaitan dengan proses administrasi dalam pelaksanaan TKP maupun pada saat akan menyajikan barang bukti kepada penuntut umum. Sebagaimana dibahas sebelumnya, masalah penyajian bukti digital kepada penuntut umum atau di hadapan pengadilan di Indonesia saat ini belum secara serempak disepakati konsepnya. Sebagian telah mengadopsi

berbagai ketentuan mengenai pengakuan bukti *digital* sebagai bukti yang dapat diakui keberadaannya, sebagian lainnya belum mengakui karena masih terpaku pada ketentuan alat bukti berdasarkan KUHAP. Dengan demikian proses administrasi penyidikan terhadap kelengkapan administrasi bukti digital saat ini pun masih belum seragam diantara para penegak hukum.

Hal lain yang cukup signifikan membedakan administrasi penyidikan tindak pidana *hacking* dan *cybercrime*, diantaranya seringkali adanya hubungan dengan pihak asing, baik perusahaan asing maupun aparat kepolisian dari negara lain, sehingga dalam proses administrasi seringkali mempergunakan bahasa Inggris khususnya dalam melakukan komunikasi dengan pihak-pihak tersebut. Hal ini dapat dipahami sejalan dengan sifat dari kejahatan itu sendiri yang bersifat mendunia sehingga istilah asing dan penggunaan bahasa asing menjadi suatu keharusan yang tidak dapat dihindari.

Dalam praktek, masalah pengetahuan tentang teknologi komputer seringkali menjadi kendala bagi penyidik Polri terutama dalam melakukan penyidikan terhadap kejahatan *cyber*. Kejahatan *cyber* yang tidak mengenal ruang dan waktu menuntut aparat penegak hukum untuk meningkatkan keahliannya. Perkembangan teknologi yang semakin meningkat berpotensi meningkatkan kejahatan *cyber*.

3.3 Penyidikan Tindak Pidana *Hacking* di Luar Negeri

Penyidikan tindak pidana *hacking*, sama halnya dengan penyidikan *cybercrime* di negara-negara lain yang pada prinsipnya menghadapi kendala yang hampir kurang lebih sama. Di Inggris, Amerika, bahkan Hong Kong, permasalahan yang dihadapi dalam proses penyidikan tindak pidana *hacking* sebagai salah satu jenis *cybercrime* yang utama adalah bukti *digital*, masalah yurisdiksi dan masalah rumusan tindak pidana itu sendiri. Sedangkan pengaturan Council of Europe, konvensi *cybercrime* hanya merupakan panduan saja, hal yang bersifat teknis di lapangan tetap menjadi kewenangan negara-negara pihak.

3.3.1 Penyidikan Tindak Pidana *Hacking* di Inggris

Proses penyidikan kejahatan *cyber* di Inggris dilakukan dengan

menggunakan *Good Practice Guide for Computer Based Electronic Evidence*[123] yang dihasilkan oleh *The Association of Chief Police Officers* (*ACPO*). Ada 4 pihak yang terlibat dalam proses penyidikan ini. **Pertama**, petugas yang datang ke TKP bertugas untuk mengamankan, mengumpulkan dan membawa peralatan dari lokasi pencarian untuk memperoleh bukti digital dan identifikasi informasi yang dibutuhkan untuk melakukan penyidikan kejahatan berteknologi tinggi. **Kedua**, penyidik yang merencanakan dan mengatur identifikasi, presentasi, dan penyimpanan data digital. **Ketiga**, staf yang bertugas memperoleh data digital yang dilatih untuk mengembalikan fungsi bukti digital tersebut dan memperoleh pelatihan yang berkaitan dalam rangka memberikan bukti untuk pengadilan. **Keempat**, saksi ahli yang dibutuhkan untuk membantu proses penyidikan seperti proses identifikasi dan interpretasi bukti digital (*http://www.7safe.com /electronic_evidence/ACPO_guidelines_computer_evidence.pdf*, 2008).

Panduan ini memberikan berbagai pengalaman berdasarkan kasus yang dialami oleh aparat penegak hukum, akademisi dan sektor swasta. Ada beberapa tahap yang dilakukan dalam proses penyidikan *cybercrime* yaitu pengakuan (*recognition*), pengumpulan (*collection*) dan pemeliharaan (*preservation*) bukti digital. Kita tidak dapat melihat apa yang terkandung didalam bukti digital tersebut. Peralatan dan *software* sangat dibutuhkan untuk memperoleh bukti digital. Sedangkan kesaksian diperlukan untuk menjelaskan proses pemeriksaan bukti digital dan proses penyidikan lainnya. Panduan ini dibuat berdasarkan prinsip-prinsip yang dibangun sebagai hasil kolaborasi dengan *International*

---

[123]Prinsip yang digunakan dalam *Good Practice Guide for Computer Based Electronic Evidence* yaitu: (Casey dan Seglem, 2002: 7-8).

Prinsip 1 : tidak boleh ada tindakan yang dilakukan baik yang dilakukan oleh polisi maupun agennya yang dapat merubah data yang terdapat dalam suatu komputer atau media lain yang mungkin diandalkan di hadapan pengadilan.

Prinsip 2 : pada keadaan luar biasa dimana seseorang merasa perlu untuk mengakses data asli yang terdapat dalam komputer sasaran, orang tersebut harus berkompeten untuk melakukannya dan untuk memberikan bukti yang menerangkan relevansi dan implikasi dari tindakan-tindakannya.

Prinsip 3 :suatu audit investigasi atau catatan lain dari seluruh proses yang dilakukan terhadap bukti komputer harus kreatif dan bersifat melindungi. Pihak ketiga yang independent harus dapat menguji proses tersebut dan menghasilkan hal yang sama.

Prinsip 4 : petugas yang berwenang atas suatu kasus bertanggungjawab untuk meyakinkan bahwa hukum dan prinsip-prinsip ini terakomodasi. Hal ini berlaku pada posisi dan akses informasi yang terdapat dalam suatu komputer. Mereka harus diyakinkan bahwa seseorang yang mengakses komputer atau setiap penggunaan dari alat pembuat salinan/duplikat telah sesuai dengan hukum dan prinsip-prinsip ini.

Organization of Computer Evidence (*SWGDE* 1999) (Casey, 2002: 7-8).

Panduan dalam *The Good Practices Guide for Computer Based Evidence* tersebut di atas tidak mengasumsikan bahwa penyidikan akan murni bersifat *digital*, tetapi juga terdapat peringatan kepada penyidik untuk tidak menyentuh *keyboard* atau *mouse*. Hal ini menunjukkan bahwa teknik penyidikan tindak pidana konvensional juga tetap berlaku dalam penentuan tersangka, diantaranya untuk mengantisipasi kemungkinan adanya sidik jari yang tertinggal pada komputer yang menjadi bukti. Panduan *ACPO* tersebut juga terdiri dari panduan, *flowchart* dan *template forms* untuk pengujian awal komputer dan mendiskusikan proses pembuatan salinan yang sama persis dari suatu disket. Panduan lain yang juga telah diterbitkan diantaranya *IACIS* 2000 dan US *DOJ* 2001 juga berisi aspek penting penanganan bukti *digital*. Akan tetapi karena panduan *ACPO* menyediakan *form* yang dipergunakan selama proses, maka panduan ini memberikan alat yang lebih praktis bagi penyidik untuk menghasilkan standarisasi tahap dalam setiap prosesnya (Casey dan Seglem, 2002: 7-8).

Di Inggris, pada awalnya unit khusus yang menangani *cybercrime* adalah *National Hi-Tech Crime Unit* (*NHTCU*). Namun pada 1 April 2006, unit ini dilebur ke dalam organisasi baru yang bernama *Serious Organised Crime Agency* (*SOCA*). *SOCA* merupakan peleburan dari organisasi-organisasi kepolisian yang ada di wilayah *United Kingdom*. *NHCTU* kemudian menjadi unit *e-crime* dalam *SOCA* yang khusus menangani *cybercrime* (*http://en.wikipedia.org/wiki/Serious_Organised_Crime_Agency*, 2008).

3.3.2 Penyidikan Tindak Pidana *Hacking* di Amerika Serikat

Tantangan utama untuk menyelesaikan penyidikan tindak pidana *hacking* di Amerika Serikat adalah tidak adanya yurisdiksi untuk menahan tersangka yang berada di luar negeri. Jika tersangka bertempat tinggal di negara yang mempunyai perjanjian ekstradisi maka dapat diminta bantuan kepada penegak hukum setempat untuk menangkapnya, jika tidak maka penyidik tidak mempunyai pilihan lain untuk menindaklanjuti kasusnya. Di Amerika, sebagian besar tersangka berada di Eropa Timur dan saat ini tidak dapat diekstradisi ke Amerika Serikat. Menurut salah satu informan dalam penelitian yang berasal dari Amerika

Serikat, kasus-kasus tindak pidana *hacking* atau *cybercrime* lainnya menghadapi kesulitan karena alasan-alasan: tersangka dan bukti sebagian besar berada di luar negeri; bukti elektronik mudah dirusak atau dapat dihilangkan jejaknya; teknologi selalu berubah dan berkembang. Sehingga alasan-alasan ini memerlukan perkembangan teknik dan alat penyidikan yang baru dan canggih pula; penyebaran perlengkapan penegakan hukum seperti *anonymizers* yaitu alat untuk menghilangkan jejak ketika sedang *browsing* di internet sehingga tidak terlacak seperti identitas komputer yang digunakan.

Informan penelitian lainnya menyatakan bahwa tantangan terberat dalam proses penyidikan tindak pidana *hacking* dan jenis *cybercrime* lainnya adalah masalah yurisdiksi, karena harus menyelesaikan kasus yang berkaitan dengan keterlibatan pihak-pihak dari berbagai negara yang berbeda. Di samping itu, kurangnya sumber daya yang diperlukan untuk melakukan tugas dengan baik, termasuk kurangnya pendidikan dan latihan para penyidik serta kurangnya perlengkapan karena faktor biaya dan bahasa serta peraturan-perundangan juga menjadi masalah yang harus dihadapi dalam penyelenggaraan penyidikan tindak pidana *hacking* dan jenis *cybercrime* lainnya.

Di Amerika Serikat, prosedur penyidikan tindak pidana *hacking* sama dengan dengan prosedur untuk penyidikan jenis *cybercrime* lainnya bahkan sama juga dengan penyidikan tindak pidana lainnya dan juga diatur dalam ketentuan hukum yang sama. Salah satu informan penelitian yang berasal dari Amerika Serikat mengatakan bahwa perbedaan utama prosedur penyidikan tindak pidana *hacking* adalah karena sifat dari bukti digital, begitu *FBI* mengetahui adanya kasus, maka langkah pengamanan bukti digital dilakukan dengan surat permohonan pengamanan bukti dan perintah pengadilan. Di Amerika Serikat, *FBI* telah membentuk *Internet Crime Complaint Center* (*IC3*), suatu pusat kliring internasional untuk komplain kejahatan internet. *IC3* menerima keluhan atau laporan dari seluruh dunia, dan selanjutnya menyampaikannya kepada agen penyidik yang berwenang.

The US Federal Guidelines for Searching And Seizing Computers (*DOJ* 1994) merupakan panduan dan penggolongan *cybercrime* yang sangat bagus.

Penggolongan ini membuat perbedaan yang sangat penting antara *hardware*[124] dan informasi[125]. *Hardware* disini mencakup semua komponen fisik di dalam komputer sedangkan informasi mencakup data dan program yang tersimpan dan dikirimkan menggunakan komputer.

3.3.3 Penyidikan Tindak Pidana *Hacking* di Hong Kong

Di Hong Kong, polisi Hong Kong adalah pihak yang berwenang sebagai penegak hukum yang melakukan penyidikan tindak pidana *hacking* ataupun jenis *cybercrime* lainnya. Dengan beragamnya kompleksitas teknis dalam proses penyidikan *cybercrime,* tanggung jawab untuk penyidikan kasus-kasus demikian terdapat pada berbagai divisi, distrik, wilayah dan markas besar Kepolisian Hong Kong. Untuk efektifitas penanganan *cybercrime,* Hong Kong telah membuat sejumlah pedoman umum penyidikan sejumlah *cybercrime,* diantaranya untuk kejahatan *online game fraud.* Akan tetapi dengan kemajuan dan perkembangan di dunia *Information and Tecimology* (*IT*), tidak terdapat peraturan tetap dan pasti untuk proses penyidikan dan pedoman yang diusulkan perlu untuk ditinjau dalam beberapa periode tertentu.

Untuk mengatur jumlah kasus yang banyak, termasuk kejahatan *IT* yang dilaporkan kepada polisi Hong Kong, polisi Hong Kong telah membentuk suatu *Communal Information System* untuk menangani informasi yang diperlukan untuk

---

[124] *Hardware* dikategorikan ke dalam 3 kelompok yaitu sebagai hasil kejahatan (*fruits of crime*), alat (*instrumentality*) dan bukti (*evidence*). *Hardware* sebagai benda ilegal dalam artian tidak boleh dimiliki oleh warga sipil atau disebut sebagai *contraband* contohnya *hardware* yang dapat menyadap komunikasi elektronik dan benda yang diperoleh hasil kejahatan (*fruits of crime*) contohnya komputer hasil pencurian. *Hardware* sebagai alat untuk melakukan kejahatan (*instrumentality*) contoh komputer yang dirancang khusus untuk melakukan kejahatan *cyber* seperti masuk ke jaringan komputer seseorang secara ilegal. *Hardware* sebagai barang bukti (*evidence*) yang tidak termasuk *contraband* atau *instrumentality* contoh *scanner* yang digunakan untuk *scanning* gambar pornografi anak memiliki karakter unik yang dapat terhubung dengan *hardware* dan gambar tersebut dapat disita sebagai bukti (Casey, 2000: 20).

[125] *Informasi* juga dikategorikan ke dalam 3 kelompok yaitu sebagai hasil kejahatan (*fruits of crime*), alat (*instrumentality*) dan bukti (*evidence*). Informasi sebagai *fruits of crime* adalah informasi yang tidak boleh dimiliki oleh warga sipil contoh *software enkripsi* yang dapat digunakan untuk melindungi data pelaku *cybercrime* bila tertangkap. Informasi sebagai alat melakukan kejahatan *cyber* contoh program yang dipakai oleh *craker* untuk menerobos ke dalam sistem komputer secara ilegal. Informasi sebagai bukti adalah yang terluas pengertiannya misalnya ketika seseorang sedang *browsing* di internet maka informasi seperti *IP Address* orang tersebut akan terlihat di *log ISP* tempat kita berlangganan. Data itulah yang kemudian menjadi bukti (Casey, 2000: 20-21).

kegiatan sehari-hari kepolisian Hong Kong. Mengenai bukti digital, Hong Kong mempunyai undang-undang mengenai bukti yang mengatur mengenai penggunaan bukti digital dan penyajiannya di depan pengadilan. Ketentuan undang-undang tentang bukti tersebut berperan dalam penuntutan semua tindak pidana berkaitan dengan penyalahgunaan teknologi informasi dan komputer. Di samping itu, Hong Kong juga mempunyai laboratorium forensik komputer di Kepolisian Hong Kong yang digunakan untuk penyimpanan dan pengamanan bukti digital secara terpusat serta proses analisa komputer, jaringan komputer maupun media penyimpanan digital lainnya yang dapat digunakan oleh seluruh penyidik di Hong Kong. Selain itu, terpisah dari laboratorium forensik komputer yang dimiliki oleh kepolisian Hong Kong, terdapat pula laboratorium forensik komputer yang dimiliki oleh badan lainnya seperti Departemen Imigrasi dan Departemen Komisi Independen Pemberantasan Korupsi.

3.3.4 Penyidikan Tindak Pidana *Hacking* di Council of Europe

Berdasarkan hasil penelitian dari informan, Council of Europe adalah organisasi internasional yang tidak terlibat secara teknis dalam proses penyidikan *cybercrime* namun membantu negara-negara di dunia dalam hal pembentukan kerangka ketentuan hukum yang menyeluruh dan untuk memfasilitasi proses penyidikan *cybercrime* yang lebih efisien serta mewujudkan kerjasama internasional. Manajemen penyidikan *cybercrime* di Council of Europe dapat dilihat dalam ketentuan *Convention on Cybercrime*. Ketentuan dalam konvensi ini memberikan kebebasan bagi negara pihak (negara yang meratifikasinya) untuk saling bekerjasama, membuat peraturan dan hal-hal lain yang diperlukan dalam melakukan penyidikan atas suatu kasus *cybercrime*. Dalam konvensi ini diatur tentang standar prosedur penyidikan suatu tindak pidana. Dalam hal penyidikan seperti yang telah dijelaskan bahwa Council of Europe tidak terlibat dalam teknis penyidikan sehingga Council of Europe tidak memiliki laboratorium forensik khusus untuk melakukan pemeriksaan atas bukti digital.

Pasal 16 konvensi ini mengatur tentang pemeliharan data yang tersimpan dalam suatu komputer. Pasal 17 mengenai pemeliharaan dan keterbukaan lalu lintas data. Kemudian dalam Pasal 18 mengatur bahwa setiap pihak

(pemerintahnya) memiliki kewenangan untuk meminta baik individu maupun penyedia layanan internet untuk memberikan segala informasi seperti data komputer yang dimiliki. Informasi ini diperlukan dalam rangka penyidikan suatu tindak pidana *cybercrime*.

Dalam Pasal 19 diatur tentang pencarian dan pengambilan data yang tersimpan dalam komputer. Yang menjadi sasaran dalam kegiatan ini adalah sistem komputer atau bagiannya dan media penyimpanan data komputer. Tiap negara pihak dapat memberikan kewenangan kepada pihak yang ditunjuk untuk bertanggung jawab dalam hal melakukan kegiatan seperti mengumpulkan dan mengamankan suatu sistem komputer, bagiannya serta media penyimpanan data komputer; membuat dan menjaga *copy* data komputer tersebut; memelihara integritas dari data komputer yang disimpan; memberi jalan masuk ke dalam sistem komputer atau memindahkan data dari sistem komputer tersebut.

3.4 Manajemen Penyidikan Tindak Pidana

Istilah manajemen mempunyai rumusan atau definisi yang beraneka ragam. Pendekatan klasik yang disebut pendekatan fungsional merumuskan manajemen sebagai proses perencanaan, pengorganisasian, penyusunan staf, koordinasi, pemimpin (*leading*), dan pengendalian serta proses penggunaan semua sumber daya untuk tercapainya tujuan organisasi. Manajemen dapat diartikan pula sebagai suatu proses merencanakan, mengorganisasikan, memimpin dan mengendalikan pekerjaan anggota organisasi dan menggunakan semua sumber daya organisasi untuk mencapai sasaran organisasi yang sudah ditetapkan (Stoner, 1996: 10). Menurut Bouza sebagaimana dikutip dalam Ensiklopedia Kepolisian (2005: 456) bahwa manajemen menyiratkan penggunaan maksimum dari sumber daya yang tersedia untuk mencapai tujuan organisasi.

Menurut Thibault, Lynch dan McBride (2007: 106) dalam bukunya "*Proactive Police Management*" menjelaskan manajemen menurut teori klasik yaitu *POSDCORB* (Gullick dan Urwick, 1937: 1-45). Teori ini menjelaskan bagaimana fungsi utama dari manajemen suatu organisasi dan bagaimana manajemen ini dijalankan. *POSDCORB* adalah kepanjangan dari *Planning,*

Organizing, Staffing, Directing, Coordinating, Reporting dan Budgeting. *POSDCORB* melihat bahwa fungsi manajemen mencakup perencanaan, pengorganisasian, perekrutan staf, pengarahan, pengkoordinasian, pelaporan dan anggaran. Teori ini hampir sama dengan Stoner (1996: 10), dimana ada unsur perencanaan dan pengorganisasian. Namun ada perbedaan dibandingkan Stoner. Stoner memasukkan perekrutan staf (*staffing*) dalam fungsi pengorganisasian sedangkan *POSDCORB* membedakannya menjadi fungsi tersendiri. *POSDCORB* dalam teorinya tidak menggunakan istilah *leading* dan *controlling*, tetapi menggunakan istilah *directing, coordinating, reporting* dan *budgeting.*

Untuk menciptakan manajemen yang baik, Henri Fayol (1841-1925) menetapkan 14 prinsip manajemen. **Pembagian tugas,** dengan pembagian tugas dapat meningkatkan efisiensi sesuai dengan besar usaha yang telah dilakukan. Akan tetapi, ada pengecualian terhadap pekerjaan-pekerjaan apa saja yang dapat dispesialisasikan. **Wewenang dan tanggung jawab,** pihak yang memiliki hak untuk memerintah dan dipatuhi, tidak dapat memiliki wewenang tanpa disertai tanggung jawab. **Disiplin,** bermanfaat untuk suatu organisasi agar berjalan efektif, akan tetapi proses pendisiplinan tergantung dari pemimpinnya. **Kesatuan komando,** setiap bawahan harus menerima perintah hanya dari satu orang saja. Bila ada kondisi dimana ada seorang bawahan dibawah perintah beberapa orang pemimpin maka akan terjadi konflik dalam hal instruksi dan kekacauan dalam wewenang. **Kesatuan dalam pengerahan,** harus ada satu pemimpin dan satu rencana dalam suatu organisasi yang memiliki tujuan yang sama. **Kepentingan individual di bawah kepentingan umum,** dalam keadaan apapun kepentingan pribadi tidak boleh didahulukan dari kepentingan organisasi secara keseluruhan. **Imbalan terhadap karyawan,** kompensasi untuk pekerjaan yang dilakukan harus adil bagi karyawan dan pimpinan. **Sentralisasi,** banyaknya penyatuan dan pendelegasian tergantung dari keadaan. Sentralisasi adalah mengurangi peranan bawahan dalam pembuatan keputusan; sedangkan pendelegasian adalah meningkatkan peranan bawahan adalah desentralisasi. Fayol percaya bahwa manajer harus mempertahankan tanggung jawab akhir, tetapi pada saat yang sama harus memberikan wewenang yang cukup kepada bawahan untuk melakukan tugasnya dengan baik. Masalahnya adalah menemukan seberapa jauh sentralisasi

dalam setiap kasus. **Hierarki** adalah urutan peringkat dari yang tertinggi sampai yang terendah dalam suatu organisasi, hierarki menggambarkan jalur komunikasi vertikal. Selain komunikasi vertikal, komunikasi horisontal juga harus ditingkatkan, selama si pemimpin dalam hierarki tersebut tetap diinformasikan. **Susunan,** sumber daya yang ada termasuk sumber daya manusia harus berada di tempat yang tepat dan pada waktu yang tepat. Terutama individu harus berada pada pekerjaan atau posisi yang paling sesuai dengannya. **Keadilan,** bawahan harus diperlakukan dengan baik dan adil. **Stabilitas staf,** seorang karyawan membutuhkan waktu untuk menyesuaikan dengan pekerjaan baru dan mencapai titik kepuasan atas penampilannya; banyaknya karyawan yang keluar mengungkapkan fungsi efisiensi dari sebuah organisasi dan hal ini harus dihindari. **Inisiatif,** kemampuan untuk mengerti dan melaksanakan tugas (melalui pemikiran dan kebebasan) harus ditingkatkan dan dikembangkan di berbagai level organisasi. **Semangat korps,** contoh kesatuan yang kuat, keharmonisan dan kerjasama merupakan hal yang penting untuk organisasi yang efektif (Roberg dan Kuykendal, 1997: 28).

Dalam literatur kepolisian, dewasa ini sering dikemukakan istilah manajemen penyidikan atau dalam istilah asing dikenal pula sebagai *investigation management*. Manajemen penyidikan dimaksudkan sebagai suatu proses menemukan, mengumpulkan, mengidentifikasikan, mempersiapkan, menganalisa dan mempresentasikan bukti baik secara langsung dari TKP atau tempat yang berkaitan dengan tindak pidana tersebut, untuk membuktikan apakah terjadi suatu tindak pidana atau tidak (Axelrod dan Antinozzi, 2003: 13). Di samping itu dikenal juga istilah *case management* atau manajemen kasus yang berarti cara yang terencana, terkoordinasi, dan teruji untuk memaksimalkan baik efisiensi maupun produktivitas dalam melaporkan serta menginvestigasi berbagai kasus (Ward, 2005: 68).

Praktek manajemen dalam kepolisian adalah suatu sistem pemecahan masalah, dimana pemecahan masalah adalah suatu proses kompleks yang dimulai dengan pengujian yang hati-hati atas setiap masalah untuk memperoleh sebanyak mungkin informasi mengenai masalah tersebut sehingga diperlukan suatu sistem manajemen untuk mentransformasikan ide-ide menjadi tindakan atau aksi (Butler,

1992: 14, 17).

Menurut salah satu informan penelitian yang berasal dari Amerika Serikat, manajemen penyidikan adalah proses dengan mana kasus-kasus diprioritaskan dan dilihat untuk meyakinkan penyidikan yang sukses dan penuntutan seseorang. Kunci manajemen penyidikan adalah menciptakan suatu proses seragam untuk melaksanakan penyidikan sehingga bukti ditangani secara baik dan seluruh kegiatan penyidikan didokumentasikan secara benar. Protokol manajemen harus diterapkan secara seragam terhadap seluruh kasus sejak awal untuk melakukan bahwa semuanya ditangani dengan standar tinggi. Manajemen yang benar memberikan perbedaan yang signifikan dalam proses dan dapat menciptakan perbedaan antara penuntutan yang sukses terhadap seseorang dan hanya membiarkannya pergi dengan bebas.

Informan penelitian lainnya bahkan menekankan bahwa manajemen penyidikan memerlukan pengalaman. Hal ini berkaitan dengan tingginya jumlah kasus dan fakta bahwa tidak semua kasus dapat dipecahkan karena terlalu bersifat teknis dan memerlukan waktu lama. Seorang manajer yang berpengalaman secara umum dapat menentukan mana kasus yang membuang waktu untuk dilihat secara mendalam dan mana kasus yang berkerja keras. Pengalamanlah yang sulit untuk diajarkan kepada penyidik. Informan ini juga menyampaikan bahwa gaya manajemen juga memegang peranan penting. Dia mencontohkan gaya manajemennya dimana dia mendesain rencana penyidikan awal yang baik dan kemudian memastikan bahwa dia menjaga, mengawal, mengawasi penyidikan secara teratur (setidaknya seminggu sekali) untuk memastikan bahwa rencana berjalan efisien dan semua berjalan lancar. Beberapa penyidik bersifat naïf dan memerlukan pedoman tetap agar mereka fokus dan tidak bekerja melewati batas kewenangan hukum yang mereka miliki pada saat menyidik suatu kasus. Mereka juga tidak menyadari kapan kasusnya "mati" dan kapan mereka harus memulai kasus yang lainnya. Manajemen kasus yang baik memerlukan pengalaman dan kemampuan yang cepat untuk mengerti kasus-kasus teknis dimana terdapat jurang pemisah, bahwa petunjuk hampir kelihatannya ditemukan dan untuk mengerjakan hal ini dengan kasus yang berulang setiap hari dengan penyidik yang memiliki tingkat kemampuan teknis yang berbeda.

Dalam lingkungan Polri, manajemen penyidikan diperkenalkan di lingkungan Bareskrim Polri dalam suatu draft naskah Manajemen Penyidikan Tindak Pidana pada bulan Juni 2007 yang hingga saat ini belum disahkan oleh Kepala Bareskrim Polri. Naskah tersebut dimaksudkan untuk dapat dijadikan pedoman bagi para penyidik dan atasan penyidik dalam rangka melakukan penyidikan terhadap tindak pidana yang dilaporkan atau diterima oleh Kepolisian Republik Indonesia. Tujuan dari naskah tersebut adalah untuk mewujudkan kesamaan pola pikir dan pola tindak dalam pelaksanaan tugas penyidikan tindak pidana sehingga mampu menciptakan situasi Kamtibmas yang kondusif dan terciptanya kepastian hukum bagi masyarakat. Sedangkan ruang lingkupnya meliputi penyelenggaraan manajemen penyidikan tindak pidana, peran para pejabat Polri sebagai atas penyidik serta para penyidik Polri. Kerangka manajemen penyidikan yang diusung dalam naskah tersebut dimaksudkan sebagai suatu pola yang merupakan suatu wujud nyata dari kultur dan organisasi profesional di bidang fungsi penyidikan secara utuh dan terukur.

Aktualisasi manajemen penyidikan adalah seluruh sumber daya yang tersedia (personil, materil dan data), dimobilisir secara terencana, terorganisir, dan terkendali untuk kepentingan pelaksanaan proses penyidikan yang maksimal, efektif dan efisien. Dalam tatanan manajemen penyidikan suatu tindakan pidana, adalah tahap pengorganisasian penyidik sebagai *teamwork* yang solid merupakan tahap awal. Pada tahapan pengorganisasian ini dilakukan persiapan pelaksanaan penyidikan dengan memilih, menunjuk penyidik yang tepat (memiliki otoritas, kompetensi dan integritas).

Setelah organisasi penyidikan terbentuk, sesuai disposisi, petunjuk, arahan atasan penyidik, para penyidik mempelajari tindak pidana yang menjadi obyek penyidikan dan kemudian menyusun dan mengajukan rencana penyidikan, guna memperoleh pengesahan atau persetujuan dari atasan penyidik. Setelah diperoleh persetujuan dari atasan penyidik, maka dilakukan penyiapan atau persiapan peralatan, perlengkapan dan dana yang dibutuhkan sesuai Rencana Penyidikan. Persiapan tersebut dibutuhkan untuk memasuki tahap terpenting dalam proses penyidikan, yakni tahap pelaksanaan penyidikan itu sendiri. Sangat mungkin dalam tahap pelaksanaan proses penyidikan, penyidik akan menghadapi berbagai

permasalahan baik yang bersumber dari dinamika tindak pidana yang ditangani maupun kendala internal dan eksternal organisasi penyidikan. Dalam hal ini, peran fungsional atasan penyidik maupun peran manajerial atasan penyidik yang lebih tinggi (Kabareskrim/Kapolda, Kapolwil, Kapolres dan Kapolsek) sangat diperlukan dalam mengambil langkah-langkah yang penting dan strategis, sehingga penyidikan dapat berjalan lancar sesuai rencana penyidikan.

Proses penyidikan yang sedang berjalan, dapat dihentikan penyidikannya apabila penyidik tidak menemukan cukup bukti, atau peristiwa yang sebelumnya diduga tindak pidana ternyata bukan merupakan tindak pidana. Atau demi hukum, penyidik harus menghentikan proses penyidikan misalnya karena tersangka meninggal dunia.

Akhir dari proses penyidikan adalah kegiatan penyelesaian penyidikan dan penyerahan hasil penyidikan (berkas perkara, tersangka dan barang bukti) kepada penuntut umum. Tahap penyelesaian penyidikan dan penyerahan tanggung jawab hasil penyidikan kepada penuntut umum, merupakan bagian yang cukup penting, karena pada tahap inilah akan dapat diketahui kualitas dari seluruh proses penyidikan yang dilakukan dari aspek formal maupun materiil.

Terhadap seluruh rangkaian kegiatan proses penyidikan tersebut di atas, dilakukan pengawasan dan penyidikan oleh atasan penyidik maupun atasan yang lebih tinggi agar pelaksanaan tugas berjalan sebagaimana mestinya. Bentuk penyidikan tersebut dapat dilakukan secara **Teknis Administratif**, dengan mempelajari laporan kemajuan perkembangan penyidikan maupun gelar perkara, disamping pengawasan terhadap penyelenggaraan administrasi penyidikan dan **Teknis Operasional**, dengan pengecekan secara langsung pelaksanaan kegiatan yang dilakukan antara lain melihat ada tidaknya tersangka di ruang tahanan dan lain-lain.

Berdasarkan uraian mengenai berbagai pendapat tentang manajemen penyidikan tindak pidana tersebut di atas, peneliti mengkaitkannya dengan inti permasalahan dalam suatu penyidikan, yaitu adanya masalah berupa kasus pidana. Bagaimana masalah tersebut dapat dipecahkan, dengan merujuk pada konsep yang dikemukakan oleh Butler (1992: 17-22), maka diperlukan suatu sistem manajemen yang mampu merubah ide-ide yang dimiliki atau tersedia menjadi

serangkaian aksi atau tindakan. Hal senada juga disampaikan oleh berbagai ahli manajemen, yang menjelaskan bahwa untuk pencapaian tujuan, diperlukan suatu proses manajemen yang terdiri dari fungsi-fungsi manajemen dimulai dengan tindakan merencanakan, mengorganisasikan, memimpin dan mengendalikan.

Apabila dikaitkan dengan proses penyidikan maka tahapan dalam proses manajemen dengan merujuk pada konsep siklus manajemen yang kemukakan oleh Butler (1992: 17) adalah sebagai berikut:

Kasus yang terjadi atau dilaporkan harus diidentifikasi melalui sistem analisis. Apabila posisi kasus sudah jelas, maka proses perencanaan dapat dijalankan untuk mengeksplorasi alternatif-alternatif metode yang dapat digunakan untuk mencapai tujuan penyidikan, yaitu ditetapkannya tersangka dan dikumpulkannya bukti-bukti yang membuktikan adanya tindak pidana yang dilakukan oleh tersangka yang bersangkutan, kemudian penyidik harus memilih alternatif yang paling layak untuk dipergunakan dalam proses penyidikan yang bersangkutan.

Sumber daya manusia yang akan mengorganisasi rencana dasar penyidikan yang telah ditentukan harus mempunyai kewenangan dan kemampuan serta keahlian yang memadai. Kemudian dia harus mampu melakukan pengorganisasian untuk menentukan pembagian tugas di antara penyidik yang ditunjuk dan menentukan alokasi sarana pendukung serta bertindak sebagai seorang manajer yang handal yang akan mengawasi dan mengkoordinasi proses penyidikan yang telah direncanakan dan diorganisir sesuai kebutuhan. Ketika rencana telah lengkap dan pengorganisasian telah dilaksanakan maka rencana tersebut diimplementasikan. Implementasi ini berkaitan dengan tugas dan beban kerja masing-masing yang telah ditentukan dalam tahap perencanaan dan pengorganisasian. Dalam tahap ini, semua penyidik bekerja dengan memperhatikan tugas dan kewenangannya masing-masing dengan memanfaatkan seluruh sarana pendukung teknis agar tujuan yang telah ditetapkan dalam tahap perencanaan dapat segera tercapai. Setelah implementasi, proses penyidikan tindak pidana tersebut harus diawasi dan dikontrol untuk menjamin apakah setiap penyidik mengerti peranan mereka dan instruksi yang diberikan. Hasil penyidikan selanjutnya harus diukur dengan parameter yang telah ditentukan dalam proses

perencanaan.

Uraian proses manajemen dalam rangka tugas penyidikan, pada prinsipnya melibatkan penyidik yang bertugas melakukan penyidikan baik yang terdiri dari atasan penyidik maupun penyidik dan penyidik pembantu. Koordinasi antara atasan penyidik dengan penyidik dan penyidik pembantu, serta alokasi dan pemanfaatan sarana pendukung teknis menjadi faktor-faktor yang menurut manajemen klasik dikelompokkan sebagai unsur manajemen yang terdiri dari sumber daya manusia, sumber daya lainnya berupa sarana dan prasarana serta peraturan perundang-undangan yang membentuk suatu sistem manajemen yang menyeluruh. Dalam sistem tersebut dituntut adanya sinergi yang menunjukkan bahwa seluruh unsur saling terkait dan saling berhubungan dalam pelaksanaan proses merencanakan, mengorganisasikan, memimpin dan mengendalikan proses penyidikan dan dengan menggunakan semua sumber daya yang tersedia untuk mencapai sasaran penyidikan yang sudah ditetapkan. Dengan demikian manajemen penyidikan dapat berjalan sesuai yang diharapkan.

Berkaitan dengan manajemen penyidikan tindak pidana *hacking* yang merupakan salah satu jenis *cybercrime*, beberapa informan penelitian baik yang berasal dari Amerika Serikat maupun Hong Kong, mempunyai persamaan persepsi mengenai perlunya menerapkan suatu manajemen yang baik dan sesuai dalam menangani penyidikan *cybercrime*. Manajemen penyidikan kasus harus meliputi fungsi pemeliharaan dan penginterogasian data operasional yang berkaitan dengan proses kasus, uang jaminan, administrasi *property* dan penyesuaian, menahan orang dan pergerakannya serta asetnya, persiapan untuk menyita surat-surat, keperluan rutin dan statistik, pembuatan laporan dan pencapaian tujuan. Itulah informasi umum yang diperlukan untuk setiap kasus, kemudian secara sistematik memproses informasi itu untuk meningkatkan efektifitas dan efisiensi organisasi yang menangani *cybercrime*.

Berikut mengenai penerapan masing-masing fungsi manajemen yang termasuk dalam siklus manajemen, yaitu perencanaan, pengorganisasian, dan pelaksanaan, serta pengawasan dan pengendalian dalam proses penyidikan tindak pidana.

3.4.1 Perencanaan

Perencanaan[126] mempunyai definisi yang berbeda-beda. Berbagai ahli manajemen dari berbagai negara telah memberikan definisi terhadap perencanaan sebagaimana dikutip oleh Datzker (1999: 101). Menurut *POSDSCORB*, perencanaan adalah kegiatan yang dilakukan dengan mempersiapkan segala hal yang akan dilaksanakan dan metode-metode untuk melaksanakannya dalam rangka mencapai tujuan yang telah ditetapkan (Swanson, Territo dan Taylor, 2008: 172).

Berbagai definisi tersebut pada prinsipnya menggambarkan bahwa perencanaan merupakan suatu konsep, metode atau tindakan. Terdapat aspek-aspek yang sama yang dipergunakan dalam memberikan pengertian tentang perencanaan. Analisis terhadap berbagai definisi mengenai perencanaan yang paling tepat untuk dipergunakan sebagai definisi perencanaan dalam bidang kepolisian adalah kegiatan atau proses. Dengan memandang bahwa perencanaan merupakan suatu proses, maka analisa mengenai perencanaan dapat dimulai dengan mengetahui serangkaian proses yang terjadi dalam tahap perencanaan.

Menurut Wallace, Roberson, dan Steckler (1995), suatu proses perencanaan harus secara mudah dapat beradaptasi kepada seluruh organisasi dan dapat

---

[126]Beberapa definisi perencanaan yang telah cukup dikenal sebagaimana dikutip oleh Dantzker (1999: 101) diantaranya:

Perencanaan adalah proses dinamis yang melibatkan sejumlah kegiatan dan metode untuk menciptakan rencana-rencana yang mampu memberikan kepada suatu organisasi pembaharuan dan perubahan yang mendasar untuk pencapaian tujuan yang lebih efektif (Whisenand dan Ferguson, 1978: 125);

Perencanaan dapat dipahami sebagai apa yang dilakukan sebelum membuat suatu keputusan atau melaksanakan tindakan. Perencanaan merupakan suatu proses persiapan: pengumpulan informasi, pertimbangan atas berbagai alternatif serta perkiraan atas akibat-akibat dari berbagai alternatif. Dalam proses perencanaan, masa depan dipertimbangkan secara eksplisit dan komprehensif, atau setidaknya diciptakan koordinasi antara keputusan dan tindakan yang dilakukan. Tanpa persiapan yang dilakukan dalam suatu perencanaan, keputusan dan tindakan dilakukan tanpa memperhatikan akibat jangka panjang yang berkaitan dengan keputusan atau tindakan-tindakan (Hudzik dan Cordner, 1983: 34);

Secara lebih sederhana, perencanaan adalah suatu proses sebelum pembuatan keputusan yang memberikan pertimbangan jelas mengenai masa depan, dan menciptakan koordinasi mengenai hubungan timbal balik antara keputusan dan tindakan. Perencanaan secara ideal memberikan pencapaian tujuan dan pembuatan pilihan rasional diantara berbagai program alternatif yang tersedia (Klofas, Stojkovic, dan Kalinich, 1990: 281);

Perencanaan adalah suatu pelatihan dengan mana informasi, sumber-sumber daya, cita-cita dan tujuan (sebagai *input*) mungkin dapat diproses dalam suatu upaya untuk membangun tujuan rencana dan program (sebagai *output*) (Sheenan dan Cordner, 1995: 171).

dipahami oleh seluruh anggotanya. Proses perencanaan meliputi tahap identifikasi masalah, penentuan tujuan, pengumpulan data, merancang solusi, partisipasi dan pengukuran[127] (Dantzker, 1995: 102).

Proses perencanaan dalam pelaksanaan penyidikan tindak pidana juga memegang peranan penting. Perencanaan sebagai bagian dari proses manajemen penyidikan melibatkan sumber daya yang tersedia. Sumber daya tersebut setidaknya terdiri dari sumber daya manusia yaitu para penyidik yang mempunyai kemampuan dan keahlian serta kewenangan melakukan kegiatan penyidikan; dan sumber daya lainnya berupa sarana dan prasana pendukung pelaksanaan tugas penyidikan. Di samping itu, perangkat hukum berupa ketentuan perundang-undangan, norma serta nilai yang berlaku dalam lingkungan juga menjadi faktor penting yang perlu dipertimbangkan dalam suatu proses perencanaan penyidikan.

Butler (1992: 19) juga menekankan bahwa aspek penting dalam perencanaan adalah bagaimana menetapkan tujuan, memperoleh informasi sebanyak mungkin berkaitan dengan tujuan, mengeksplorasi dan memilih

---

[127]Menurut Dantzker (1999: 102-105), tahap pertama proses perencanaan adalah mengidentifikasi masalah-masalah yang potensial yang mungkin dihadapi baik dalam jangka pendek maupun jangka panjang. Penentuan tujuan adalah tahap penting kedua dalam proses perencanaan. Setelah masalah diketahui atau diidentifikasi, selanjutnya bagaimana menyelesaikannya. Bagaimana masalah yang ada diselesaikan, dan apa hasil akhir yang ingin dicapai serta alat apa yang dapat digunakan untuk mencapai tujuan tersebut. Kegagalan untuk menentukan tujuan, akan merusak rencana itu sendiri bahkan sebelum rencana tersebut dapat dilaksanakan. Suatu rencana tanpa tujuan yang ditentukan secara khusus tidak akan lebih dari hanya suatu daftar harapan saja. Pengumpulan data atau informasi yang relevan dan penting merupakan bagian dari proses perencanaan. Hilangnya data atau informasi yang penting dan berkaitan dengan proses perencanaan dapat menyebabkan rencana yang dibangun menjadi tidak tepat. Suatu perencanaan yang baik akan selalu menggabungkan seluruh data atau informasi yang dapat dikumpulkan atau diperoleh. Tahap selanjutnya adalah solusi. Kunci dalam proses perencanaan adalah mengetahui apa yang dapat dilakukan untuk menyelesaikan masalah yang telah teridentifikasi. Pengidentifikasian masaleh tidak akan berguna apabila tidak dicari cara-cara penyelesaiannya. Oleh karena itu apapun masalahnya, perencanaan memerlukan solusi yang cukup dapat diandalkan dalam menyelesaikan masalah yang teridentifikasi. Partisipasi dari berbagai pihak yang berkaitan merupakan hal penting dalam tahap kelima yaitu proses perencanaan. Dalam perencanaan, selain pimpinan, diperlukan partisipasi dari anggota-anggota organisasi lainnya. Bahkan jika diperlukan, partisipasi dari pihak eksternal dapat memberikan nilai tambah dalam proses perencanaan. Perencanaan yang dilakukan dengan hanya melibatkan partisipasi pimpinan akan membuat perencanaan kurang *applicable* dalam pelaksanaannya oleh seluruh anggota organisasi yang bertugas. Hampir sebagian besar penulis setuju bahwa satu tahap dalam proses perencanaan adalah pengukuran atau evaluasi (Hudzik dan Coedner: 1983, Souryal: 1985, Stone dan DeLuca: 1985, Holden: 1994, Seehan dan Cordner: 1995, Dantzker: 1999). Evaluasi terhadap setiap rencana dapat memberikan informasi yang berharga mengenai sejauh apa kesuksesan rencana dan menghasilkan data untuk proses perencanaannya selanjutnya. Alat yang digunakan untuk mengevaluasi rencana harus diidentifikasi dan menjadi bagian rencana final sebelum rencana tersebut mulai dilaksanakan.

alternatif yang terbaik, menuangkan pilihan alternatif penyelesaian dalam suatu strategi khusus dengan mengidentifikasi elemen utama masalah, konsekwensi pilihan maupun biaya, sumber daya manusia dan sumber daya lainnya. Selanjutnya menetapkan alat atau sarana yang dipergunakan serta menentukan mekanisme pengawasan terhadap pilihan yang akan dilakukan.

Dalam tahap perencanaan ini, penyidik yang berwenang melakukan penyelenggaraan manajemen penyidikan, harus mampu mengidentifikasi baik masalah dan alternatif tindakan yang akan dipergunakan untuk menyelesaikan masalah, maupun mengidentifikasi dan menentukan sumber daya apa saja yang diperlukan untuk pelaksanaan rencana yang sedang disusun. Sumber daya manusia dan sarana pendukung merupakan faktor yang penting untuk dipertimbangkan sebagai pelaksana dan sarana untuk melaksanakan rencana yang disusun. Selain itu, metode-metode, cara-cara ataupun mekanisme perlu ditetapkan pula agar dapat dipergunakan sebagai pedoman pelaksanaan rencana yang disusun.

Perencanaan penyidikan sebagai salah satu fungsi manajemen yang perlu diterapkan dalam manajemen penyidikan tindak pidana memegang peranan penting dalam keseluruhan siklus manajemen penyidikan tindak pidana. Perencanaan merupakan tahap awal siklus manajemen penyidikan. Dalam draft naskah Manajemen Penyidikan Bareskrim Polri (2007: 34), ditegaskan bahwa perencanaan penyidikan harus memperhatikan beban tugas yang diemban, norma dan nilai yang berlaku serta sumber daya yang ada (sumber daya manusia dan sarana prasarana), demikian pula peluang dan kendala yang dihadapi (baik internal/organisasi penyidikan maupun eksternal/lingkungan strategis). Dalam naskah tersebut, perencanaan penyidikan dibagi menjadi 2 perencanaan pokok, yaitu Rencana Penyelidikan[128] dan Rencana Penyidikan[129].

---

[128]Rencana Penyelidikan dapat dibedakan dalam dua kategori/bentuk. Bentuk yang pertama adalah rencana penyelidikan dalam rangka tindakan penyelidikan yang dilakukan sebelum tindakan penyidikan. Tujuan akhirnya adalah untuk menentukan apakah suatu peristiwa yang terjadi/dilaporkan/diadukan merupakan perbuatan pidana atau bukan. Hasil penyelidikan tersebut, menentukan dapat atau tidaknya dilakukan tindakan penyidikan sesuai aturan hukum acara pidana. Bentuk yang kedua adalah rencana penyelidikan dalam rangka penyidikan atau penindakan (pemanggilan, penangkapan, penahanan, penggeledahan, penyitaan dan pemeriksaan) untuk memudahkan, memperlancar tindakan-tindakan penyidikan. Misalnya dalam rangka tindakan penangkapan, maka penyelidikan dilakukan untuk mengetahui, memastikan keberadaan atau

Rencana Penyelidikan dan Rencana Penyidikan dibuat oleh penyelidik/penyidik dan harus mendapat persetujuan dari atasan penyidik yang diberi kewenangan untuk meneliti, menyetujui, menolak atau merevisi/mengarahkan rencana tersebut. Perlu disadari, bahwa apabila atasan penyidik bertanggung jawab terhadap kemampuan yang dimiliki oleh Penyelidik/Penyidik, untuk melaksanakan kegiatan penyelidikan/tindakan penyidikan. Demikian juga tentang pemenuhan terhadap peralatan perlengkapan dan dana pelaksanaannya.

Perencanaan dalam proses manajemen penyidikan tindak pidana yang dirumuskan dalam naskah Manajemen Penyidikan Tindak Pidana sebagaimana diuraikan di atas, pada prinsipnya mengandung aspek-aspek proses perencanaan yang diperlukan dalam suatu penyusunan rencana penyelidikan dan penyidikan tindak pidana. Secara umum, rumusan mengenai penjelasan proses perencanaan penyelidikan dan penyidikan tersebut di atas merupakan panduan yang dapat dipergunakan oleh penyidik dalam menjalankan tugasnya dengan menerapkan salah satu fungsi manajemen penyidikan yaitu perencanaan. Rumusan tersebut lebih bersifat panduan umum dan proses administrasi pembuatan suatu rencana,

---

identitas orang yang akan ditangkap, serta menganalisis dan memastikan kendala dan peluang yang mungkin dihadapi penyidik dalam tindakan penangkapan. Ada beberapa hal yang harus dimuat di dalam Rencana Penyelidikan yaitu identitas penyelidik; obyek penyelidik; sasaran dan target hasil penyelidikan yang diharapkan; rincian kegiatan yang dilakukan; peralatan, perlengkapan dan dana yang diperlukan dalam pelaksanaan kegiatan penyelidikan, waktu yang diperlukan untuk melaksanakan penyelidikan, koordinasi antara fungsi kepolisian dan lintas sektoral (Bareskrim Polri (2007: 34).

[129]Rencana Penyidikan dibuat dengan tujuan akhir adalah untuk membuktikan dugaan tindak pidana yang terjadi dan menentukan tersangkanya, sehingga hasil kegiatan penyidikan tersebut dapat diserahkan kepada Penuntut Umum dan selanjutnya diajukan ke sidang pengadilan. Rencana Penyidikan harus memuat/mencakup beberapa hal penting, yaitu menyusun dan menyiapkan administrasi penyidikan sesuai dengan Juklak/Juknis dan Jukmin proses penyidikan tindak pidana; menyiapkan penyidik yang akan melaksanakan penyidikan, lengkap dengan identitasnya. Penentuan para penyidik untuk masing-masing kegiatan penyidikan harus memperhatikan otoritas, kompetensi dan integritas yang dimiliki sehingga pelaksanaan tugas dapat berjalan baik dan meminimalisir/mencegah distorsi yang tidak perlu; membuat anatomi kasus yang akan disidik; menyusun daftar pertanyaan untuk saksi dan tersangka dalam rangka pemeriksaan; menentukan waktu/jadwal rencana pemeriksaan terhadap saksi/ahli, dan tersangka; menentukan jadwal/waktu rencana pra-rekonstruksi/rekonstruksi (bila diperlukan); menyiapkan sarana dan prasarana serta merencanakan kebutuhan anggaran yang diperlukan; menyiapkan/menunjuk penasehat hukum dalam hal tersangka melakukan tindak pidana dengan ancaman pidana mati atau pidana 15 tahun atau lebih bagi tersangka yang tidak mempunyai penasehat hukum sendiri (pasal 56 KUHAP); mengajukan rencana penyidikan kepada atasan penyidik secara berjenjang (Bareskrim Polri (2007: 34).

yang dapat dipergunakan sebagai pedoman bagi penyidik dalam membuat suatu rencana penyelidikan tindak pidana.

3.4.2 Pengorganisasian

Untuk melihat bagaimana fungsi dari pengorganisasian dalam manajemen penyidikan, penting untuk diketahui pengertian pengorganisasian itu sendiri. Ada beberapa pengertian pengorganisasian sebagaimana dikutip oleh Dantzker (1999: 115-116). yang menyatakan bahwa fungsi pengorganisasian sangat penting dalam organisasi polisi. Hal ini berkaitan dengan struktur kewenangan agar tugas dan kegiatan yang diperlukan digunakan untuk mencapai tujuan yang telah ditentukan, dengan cara mengatur, mendefinisikan dan menggkoordinasikan tugas-tugas dan kewenangan yang tersedia. Dalam pemolisian modern, pengorganisasian dipandang sebagai pendelegasian kewenangan, kesatuan komando dan penerapan manajemen.

Menurut *POSDCORB*, pengorganisasian adalah pembentukan struktur formal suatu organisasi seperti pembagian organisasi ke dalam beberapa bagian dimana seluruh bagian itu akan dikoordinir untuk mencapai tujuan organisasi tersebut (Swanson, Territo dan Taylor, 2008: 172).

Menurut Gulick (1978) sebagaimana dikutip oleh Dantzker (1999: 115), pengorganisasian adalah pembentukan kewenangan struktur formal yang dipergunakan untuk mengatur, mendefisinikan dan mengkoordinasikan bagian-bagian pekerjaan untuk mencapai suatu tujuan yang ditentukan. Menurut Stieglitz (1971: 20), pengorganisasian juga mempunyai arti sebagai suatu proses mengelompokkan kegiatan secara logis, pembagian kewenangan dan tanggung jawab, serta merancang hubungan kerja antara organisasi dengan anggotanya agar menyadari tujuan bersama yang ingin dicapai. Pengorganisasian menurut Sheehan dan Cordner (1995: 176), didefinisikan pula sebagai suatu proses untuk menempatkan secara bersama-sama seluruh subsistem dari suatu organisasi untuk mencapai efisiensi, efektivitas dan produktivitas secara maksimum dalam pencapaian cita-cita dan tujuan organisasi. Dalam literatur kepolisian, pengorganisasian dikaitkan dengan penciptaan struktur formal organisasi polisi, pekerjaan suatu perusahaan, tujuannya untuk mengkoordinasikan seluruh unit

organisasi untuk mencapai tujuan organisasi dengan cara yang paling efisien (Thibault, Lynch dan McBride, 1995: 67).

Dengan berdasar pada definisi-definisi tersebut di atas, peneliti dapat menguraikan suatu konsep bahwa pengorganisasian dalam manajemen penyidikan melibatkan seluruh sumber daya yang dimiliki untuk dialokasikan dan diberdayakan peran dan fungsinya sesuai dengan rencana penyidikan yang telah ditentukan dalam rangka mencapai tujuan penyidikan itu sendiri. Sejalan dengan konsep yang disampaikan oleh Butler (1992: 18) tentang pengorganisasian sebagai bagian dari siklus manajemen, peneliti memandang bahwa pengorganisasian merupakan kegiatan yang dilakukan untuk memastikan bahwa penyidik selaku sumber daya manusia telah ditempatkan sesuai dengan peran, tanggung jawab, kemampuan dan kewenangannya, dan sumber daya pendukung lainnya telah dialokasikan sesuai kebutuhan guna mewujudkan apa yang telah ditentukan dalam tahap perencanaan penyidikan sehingga menjadi suatu kegiatan penyidikan yang terorganisir dengan baik.

Dalam suatu proses penyidikan baik pada tahap pelaksanaan penyelidikan maupun tindakan penyidikan, selalu diperlukan tersedianya unsur-unsur petugas: penyidik, peralatan perlengkapan, dana dan metode penyidikan. Unsur-unsur tersebut tersebut diorganisir di dalam hubungan-hubungan organisasional, baik di lingkungan Polri maupun di luar Polri.

Berdasarkan naskah Manajemen Penyidikan Tindak Pidana Bareskrim Polri (2007: 37), pembentukan organisasi penyidikan dapat dilakukan melalui 2 (dua) cara yaitu menggunakan unit penyidikan yang secara struktural telah ada pada organisasi Polri[130] dan menggunakan penyidik yang diperluas (diluar

---

[130]Pertama, menggunakan unit penyidikan yang secara struktural telah ada pada organisasi Polri. Jumlah penyidik yang dilibatkan dalam pelaksanaan penyidikan sifatnya bervariasi, tergantung pada kebutuhan pelaksanaan proses penyidikan. Dalam menentukan penyidik yang akan ditunjuk melakukan penyidikan suatu perkara tindak pidana, perlu dipertimbangkan aspek-aspek sebagai berikut: memiliki moral dan integritas yang tinggi; memiliki etika dan profesionalisme; kemampuan yang dimiliki penyidik, dihubungkan dengan jenis tindak pidana, bobot problematik atau tingkat kesulitan yang akan dihadapi, skala maupun dampak yang ditimbulkan tindak pidana tersebut; jumlah penyidik yang dibutuhkan untuk melakukan penyidikan; hubungan (subyektivitas) yang mungkin ada atau dapat timbul antara penyidik dengan tersangka maupun peristiwa tindak pidana yang menjadi obyek penyidikan; kerjasama *(team work)* antara penyidik dalam rangka pelaksanaan penyidikan (Bareskrim Polri, 2007: 37).

struktur)[131]. Sebagaimana disampaikan dalam draft naskah Manajemen Penyidikan Tindak Pidana Bareskrim Polri, apabila organisasi penyidikan menjadi lebih besar dengan mengikut sertakan penyidik dengan berbagai kemampuan/keahlian, maka peralatan dan dana akan mengalami penambahan sesuai kebutuhan. Ada beberapa aspek yang perlu dipertimbangkan untuk melaksanakan penyidikan di luar struktural (diperluas).

Memilih, menentukan dan mempersiapkan penyidik-penyidik yang handal dan berkualitas dan diberi mandat untuk melakukan tindakan penyidikan. Menyusun pembagian hubungan tata kerja, sehingga setiap penyidik yang berada dalam organisasi penyidikan yang diperluas, mengetahui hubungan kerjanya, apa yang harus dilakukan, bekerjasama dengan siapa dan bertanggung jawab kepada siapa. Menyiapkan sarana dan prasarana serta dana yang dibutuhkan selama penyidikan. Penyiapan administrasi yang diperlukan baik administrasi umum maupun administrasi penyidikan.

Penyidik yang terorganisir di dalam organisasi penyidikan yang diperluas mempunyai tanggung jawab baik secara struktural maupun fungsional tanggung jawab penyidik secara struktural dapat dilihat dari tingkat keberhasilan yang dicapai dalam pelaksanaan penyidikan. Penilaian keberhasilan penyidik dilakukan secara rutin dan berkala oleh atasan penyidik, sesuai Pedoman Penilaian Kinerja Penyidik Polri. Tanggung jawab fungsional sebagai seorang penyidik merupakan tanggung jawab secara hukum, dimana yang dilihat dari benar atau salahnya penyidik dalam melakukan penyidikan.

Penyidik dalam menjalankan tugas penyidikan yang telah diberikan kepadanya berdasarkan pengorganisasian yang dilakukan, harus sesuai dengan ketentuan hukum acara yang berlaku. Apabila penyidik dalam melakukan atau tidak melakukan suatu tindakan penyidikan, menyimpang atau tidak sesuai dengan ketentuan hukum acara yang berlaku, maka yang bersangkutan dapat dikatakan telah salah dalam menjalankan tugas. Untuk itu, penyidik harus memiliki komitmen dan visi dalam pelaksanaan tugas di lapangan sesuai dengan

---

[131]Kedua, menggunakan penyidik yang diperluas (diluar struktur). Pengorganisasian penyidikan dengan menggunakan unit penyidikan yang diperluas, dilakukan untuk penyidikan tindak pidana yang berskala luas karena unit penyidikan yang terstruktur/rutin, dinilai kurang memadai untuk menangani sendiri penyidikan tersebut (Bareskrim Polri, 2007: 37).

tugas yang diberikan kepadanya.

3.4.3 Pelaksanaan

Pelaksanaan merupakan realisasi dari perencanaan, yaitu perwujudan dalam bentuk tindakan nyata di lapangan dari apa yang telah disiapkan/direncanakan sebelumnya. Menurut Butler (1992: 20), pelaksanaan atau tahap implementasi dapat dipandang dari dua sudut pandang yang berbeda, pertama sebagai tahap penyelesaian rencana yang melibatkan seluruh personel yang akan bertanggung jawab atas pelaksanaan strategi yang dipilih, dan kedua, implementasi dipandang sebagai pelaksanaan aktual dari metode yang dipilih dalam tahap perencanaan disertai dengan pengawasan dan pengkoordinasian tugas yang dijalankan.

Pada tahap inilah efektivitas manajemen penyidikan yang diterapkan akan diuji tentang kelengkapan alat bukti, ketepatan dan akuntabilitas, serta kecepatan seluruh tindakan penyidik. Oleh karena itu perencanaan yang baik merupakan perencanaan yang disusun secara logis dan memuat secara detail tindakan yang akan dilakukan sehingga merupakan pedoman yang memudahkan pelaksanaannya. Sebaliknya, rencana yang dilakukan secara asal-asalan, sama saja dengan merencanakan kegagalan. Tidak tertutup kemungkinan dalam tahap pelaksanaan penyidikan, terdapat dinamika yang membutuhkan tindakan yang sebelumnya belum diatur dalam perencanaan, misalnya diperlukan tambahan penyidik atau perlengkapan tertentu untuk menyelesaikan penyidikan. Dalam hal ini, diperlukan langkah-langkah solutif baik berupa revisi terhadap perencanaan maupun tindakan-tindakan darurat lainnya yang harus diambil segera dengan tetap memperhatikan ketentuan hukum yang berlaku. Langkah-langkah darurat tersebut dapat terkait dengan berbagai hal, misalnya memperbesar mandat, konflik kewenangan, kemampuan, pembantuan, sumber daya, dan lain sebagainya. Semua langkah-langkah tersebut harus teregistrasi baik dalam administrasi umum maupun administrasi penyidikan.

Dalam pelaksanaan teknis penyidikan ada kemungkinan timbul permasalahan yang tidak diduga sebelumnya atau tidak termuat dalam perencanaan, sehingga perlu segera dilakukan upaya pemecahan masalah, misalnya dengan mengadakan gelar perkara, koordinasi dan lain-lain. Tindakan-

tindakan tersebut harus dilakukan dengan menjunjung tinggi norma hukum dan hak asasi manusia, masih tetap berada dalam koridor teknis penyidikan serta berorientasi pada tujuan yang ingin dicapai. Untuk menyelesaikan berbagai permasalahan dan kendala yang dihadapi dalam proses penyidikan, dimungkinkan bagi penyidik dan atasan penyidik untuk meminta bantuan taktis dan teknis secara berjenjang sebagai bentuk *backup* satuan lebih tinggi terhadap satuan di bawahnya.

3.4.4 Pengendalian dan Pengawasan

Pengendalian dan pengawasan penyidikan sebagai salah satu fungsi manajemen tidaklah berdiri sendiri, tetapi berada atau melekat pada semua fungsi manajemen, baik pada tahap perencanaan, pengorganisasian dan pelaksanaan. Fungsi pengawasan memegang peranan penting dalam menentukan dan mengevaluasi perencanaan, pengorganisasian serta penyidikan pelaksanaan.

Menurut Butler (1992: 178), pengendalian dan pengawasan adalah tahap akhir dalam siklus manajemen dalam hal ini manajemen penyidikan dan merupakan sumber yang penting dalam menentukan perencanaan untuk masa depan. Pengawasan penyidikan pada tahap perencanaan pada dasarnya merupakan kegiatan evaluasi terhadap tingkat visibilitas (realistis/tidaknya) rencana yang sedang disusun dengan memperhatikan hal-hal berikut ini: apakah kegiatan-kegiatan yang akan dilakukan telah mengarah kepada tujuan-tujuan khusus yang ditetapkan maupun tujuan akhir yang diharapkan; Apakah penentuan tujuan-tujuan tersebut (khusus maupun umum) telah mempertimbangkan berbagai aspek yang mempengaruhi, baik kendala maupun peluang yang mungkin dihadapi dilingkungan internal maupun eksternal; Apakah sumber daya manusia yang tersedia sudah memadai melaksanakan tugas yang akan dilaksanakan; Apakah penentuan waktu sudah memadai jika dilihat dari beban tugas, serta tantangan dan kendala yang akan dihadapi; Apakah sarana dan prasarana yang disiapkan sudah mencukupi untuk pelaksanaan tugas yang berdaya guna dan berhasil guna; Apakah biaya sudah memadai untuk memenuhi kebutuhan pelaksanaan tugas secara maksimal.

Pengendalian dan pengawasan penyidikan tahap pengorganisasian pada dasarnya merupakan kegiatan evaluasi terhadap suatu tim penyidik yang diorganisir, dengan memperhatikan: jumlah penyidik yang diperlukan untuk melakukan penyidikan; kompetensi profesional penyidik yang dipilih untuk melakukan penyidikan; sistem hubungan antara personil yang berada dalam satu tim untuk menjamin kekompakan dan kerjasama sebagai *team work*; pembagian pekerjaan yang tepat dan jelas untuk masing-masing personil yang berada dalam tim, sehingga distribusi pekerjaan terbagi secara tepat dan proporsional; apakah setiap orang yang berada dalam tim memiliki komitmen dan visi yang sama.

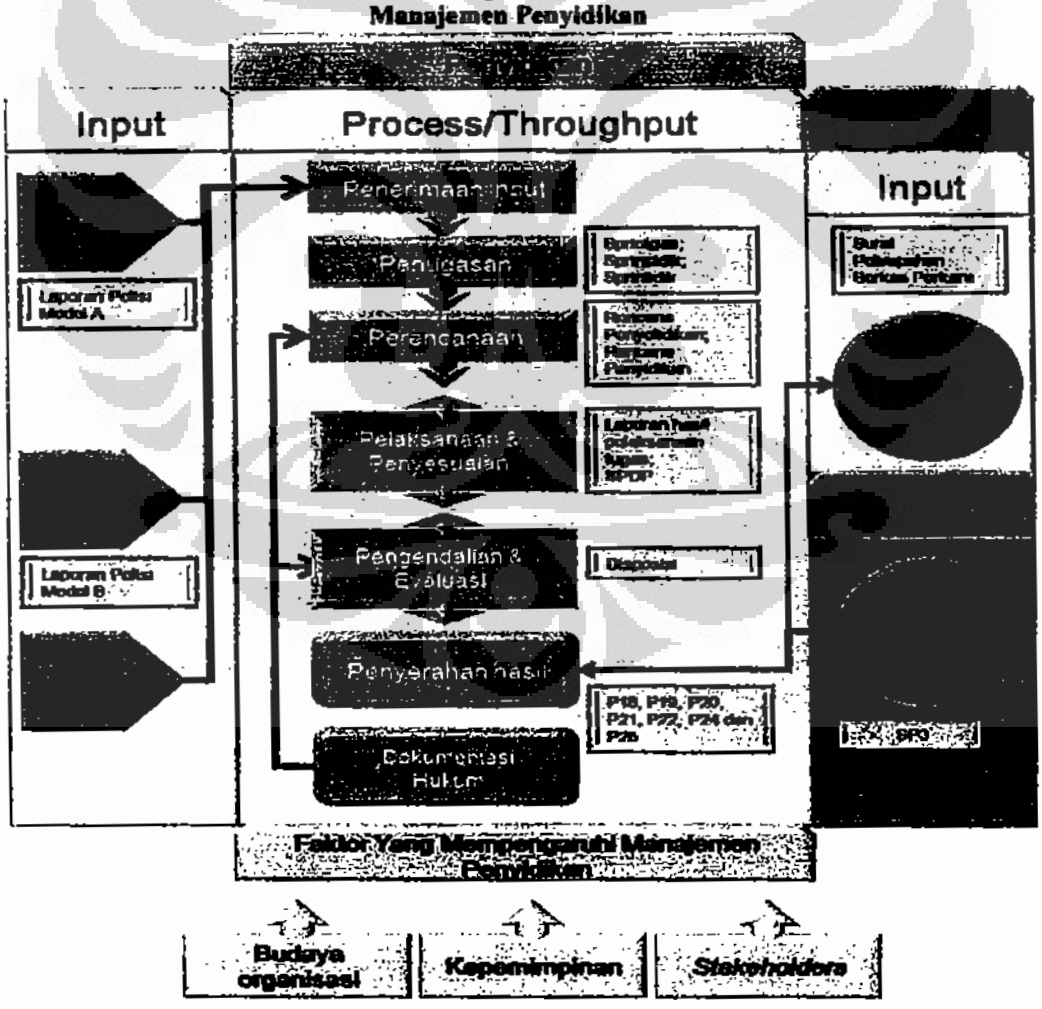
Pengendalian dan pengawasan penyidikan pada tahap pelaksanaan pada dasarnya merupakan kegiatan mengendalikan pelaksanaan agar tidak menyimpang dari apa yang telah direncanakan. Dalam pelaksanaan tugas penggeledahan, ketua tim lapangan sebagai perwira pengawas melakukan pemeriksaan kepada anggota yang melaksanakan tugas penggeledahan baik rumah, barang maupun orang. Pimpinan sebagai pengawas bertanggung jawab atas jalannya penyidikan, dan melakukan kontrol berlapis kepada anggota. Dalam tahap pelaksanaan, maka pengawasan penyidikan dilaksanakan melalui dua cara yaitu secara administrasif, antara lain melalui administrasi penyidikan, register perkara, laporan kemajuan dan laporan perkembangan penyidikan Secara fisik, antara lain: pengarahan, supervisi, bimbingan teknis penyidikan, penyidikan dan gelar perkara. Setelah pelaksanaan selesai, perlu dievaluasi baik terhadap keberhasilan maupun kegagalan dalam pelaksanaan.

3.4.5 Telaah Terhadap Teori Manajemen Penyidikan

Penyidikan berdasarkan ketentuan formil (KUHAP) dan ketentuan internal (petunjuk pelaksanaan), dipandang sebagai proses penegakan hukum dimana suatu tindak pidana dibuat menjadi terang dan jelas, diurai dan memenuhi unsur-unsurnya dan akan menghasilkan pelimpahan berkas perkara ke penuntut umum atau apabila tidak dapat diurai maka akan ditetapkan penghentian penyidikan. Dalam ketentuan penyidikan tersebut terdapat berbagai kegiatan-kegiatan prosedural yang diatur oleh hukum berikut pembagian fungsi yang tegas antara penyidik dengan penuntut umum.

Disini penulis melihat perlunya paradigma yang bebeda, yang lebih komprehensif dalam penanganan suatu perkara oleh penyidik sehingga penyidik perlu melakukan manajemen penyidikan. Manajemen Penyidikan (*investigation management*) merupakan suatu proses penanganan perkara yang menerapkan prinsip dan fungsi-fungsi manajemen sehingga menjadi suatu kegiatan penegakan hukum yang sistematis terdiri dari penerimaan input (*accepting input*), penugasan (*assigning*), perencanaan (*planning*), pelaksanaan (*executing*) dan penyesuaian (*adjusting*), pengendalian (*controlling*) dan evaluasi (*evaluation*), serta penyerahan hasil (*result delivery*). Manajemen penyidikan tersebut dapat digambarkan dengan bagan berikut ini:

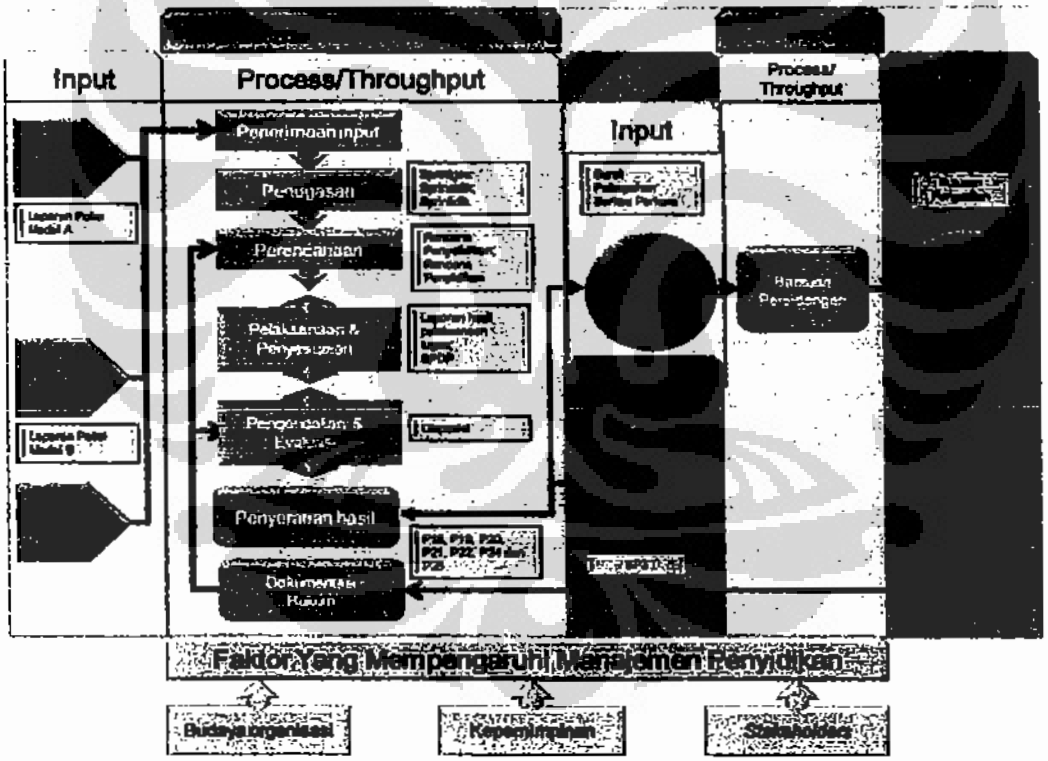
Bagan 3.7
Manajemen Penyidikan



(Sumber: Penulis)

Pada kenyataannya, peranan penyidik tidak hanya sampai pada penyerahan berkas perkara ke penuntut umum, tetapi juga mendukung proses pengadilan dengan menjadi saksi verbalisan, turut menyiapkan saksi dan ahli. Disamping itu, setelah hakim membuat keputusan, penyidik juga perlu mengetahui keputusan dan analisa hukum terhadap kasus yang telah ditanganinya sebagai proses pembelajaran dalam menangani kasus serupa di masa yang akan datang. Fenomena tersebut membutuhkan suatu manajemen penyidikan terpadu yang tidak berhenti pada saat penyerahan berkas perkara tapi membentuk suatu siklus manajemen dan proses pembelajaran yang tiada terputus dengan menambahkan adanya langkah berupa bantuan persidangan (*court support*) dan dokumentasi (*documentation*).

Bagan 3.8
Manajemen Penyidikan Terpadu



(Sumber: Penulis)

Penjabaran manajemen penyidikan terpadu meliputi kegiatan sebagai berikut:

Penerimaan Input (*input accepting*). Manajemen penyidikan dimulai dari adanya masukan berupa dugaan telah dilakukan tindak pidana. Dugaan tersebut

dapat berupa laporan dari masyarakat, atau aduan tergantung pada tindak pidana yang diduga telah terjadi, berupa delik aduan atau delik laporan. Polisi secara proaktif juga dapat melakukan input apabila tertangkap tangan atau mengetahui adanya dugaan tindak pidana berdasarkan penyelidikan yang dilakukan terlebih dahulu. Penerimaan input tersebut diwujudkan dalam dokumentasi berupa laporan polisi. Dokumentasi yang dihasilkan adalah laporan polisi model A untuk tindak pidana yang dilaporkan oleh polisi sendiri dan laporan polisi model B untuk tindak pidana yang dilaporkan oleh masyarakat.

Penugasan (*assigning*), setelah menerima laporan polisi, kepala unit yang terkait memberikan tugas kepada penyidik tertentu untuk menangani kasus tersebut. Penugasan ini merupakan fungsi pendelegasian dari kepala unit kepada penyidik. Dokumentasi yang dihasilkan berupa Surat Perintah Tugas (Springas) yang kemudian setelah bukti awal didapat dapat dikeluarkan Surat Perintah Penyidikan (Sprinsidik).

Perencanaan (*planning*), setelah mendapatkan surat tugas sebagai mandat untuk dilakukannya penyidikan maka disusunlah strategi dan rencana secara lebih mendetail mengenai siapa melakukan apa, kapan, dimana, bagaimana caranya, apa saja yang diperlukan, berapa biaya yang diperlukan, berapa lama waktu yang diperlukan serta target yang ingin dicapai dari masing-masing kegiatan tersebut. Dokumentasi yang dihasilkan adalah rencana penyelidikan atau rencana penyidikan.

Pelaksanaan dan penyesuaian penyidikan (*executing and adjusting investigation*), setelah proses perencanaan, pelaksanaan penyidikan dimulai dengan dikeluarkannya Surat Pemberitahuan Dimulainya Penyidikan (SPDP). Rencana yang telah disusun hanya berupa panduan karena pada kenyataanya diperlukan penyesuaian akibat adanya informasi baru yang menentukan strategi dan pelaksanaan penyidikan. Dokumentasi yang dihasilkan dari proses pelaksanaan tersebut berikut penyesuaiannya berupa laporan hasil pelaksanaan tugas.

Pengendalian dan evaluasi penyidikan (*controlling and evaluation investigation*) merupakan kegiatan simultan yang dilakukan pada pelaksanaan penyidikan. Setiap kegiatan perlu dikontrol agar tidak bertentangan dengan

ketentuan hukum formil dan menyimpang terlalu jauh dengan rencana atau strategi yang telah ditetapkan atau disesuaikan. Evaluasi secara mendalam dapat terbagi menjadi tiga yaitu:

Evaluasi pertama : Apakah penyelidikan perlu dilanjutkan dengan penyidikan?

Evaluasi kedua : Apakah penyidikan yang telah dilakukan berakhir dengan pelimpahan berkas perkara ke penuntut umum atau penetapan penghentian penyidikan?

Dokumen yang dihasilkan pada evaluasi kedua ini adalah Surat Pelimpahan Berkas Perkara ke penuntut umum atau Surat Penghentian Penyidikan Perkara .

Dalam tahap evaluasi ini, penyidik kerap membuka diri terhadap pihak lain yang berkepentingan seperti penuntut umum, korban ataupun pengacara dengan mengadakan gelar perkara.

Evaluasi ketiga : Dilakukan setelah adanya keputusan pengadilan mengenai atau terkait dengan kasus tersebut. Evaluasi tahap akhir yang meliputi pembelajaran yurisprudensi terhadap kasus yang ditangani atau kasus serupa digunakan untuk pada perencanaan dan penyusunan strategi penanganan kasus berikutnya.

Penyerahan hasil (*result delivery*), merupakan keputusan dari hasil evaluasi kedua. Dari evaluasi kedua tersebut dapat diambil dua langkah alternatif yaitu langkah penghentian penyidikan dan pelimpahan berkas perkara ke Penuntut Umum. Penghentian penyidikan dapat dilakukan dengan alasan bahwa peristiwa tersebut bukan termasuk sebagai tindak pidana dan pelaku tidak pidana tersebut telah meninggal dunia atau tindak pidananya telah kadaluwarsa. Apabila ketiga alasan tersebut tidak terpenuhi dan unsur-unsur tindak pidana tersebut dapat diurai maka diadakan pelimpahan berkas perkara ke penuntut umum.

Bantuan pengadilan (*court support*): Peranan penyidik pada prakteknya tidak terbatas hanya pada proses penyidikan saja tetapi juga dalam proses persidangan Disini, penyidik berkerja sama dengan penuntut umum dalam penyediaan saksi dan ahli, menjadi ahli, bahkan berperan sebagai saksi verbalisan.

Dokumentasi hukum (*legal documentation*), adalah proses pembuatan dokumentasi yang diperlukan untuk setiap tahapan. Dokumentasi disini masih perlu ditambahkan lagi dengan yurisprudensi kasus yang terkait untuk membantu penyidik melakukan interpretasi dari ketentuan hukum pidana yang ada.

BAB IV

PENERAPAN MANAJEMEN PENYIDIKAN TINDAK PIDANA *HACKING WEBSITE* PARTAI GOLKAR OLEH UNIT V *IT & CYBERCRIME*

4.1 Unit V *IT & Cybercrime*

Dalam era informasi, keberadaan informasi berperan penting dalam semua aspek kehidupan serta merupakan kebutuhan hidup baik bagi individu maupun organisasi. Perkembangan teknologi komputer, akses internet yang luas, dan pesatnya pasar untuk alat komunikasi yang semakin canggih merupakan sarana yang dibutuhkan manusia dalam memperoleh informasi dan bertukar informasi. Kecanggihan teknologi informasi telah memberikan kemudahan bagi manusia dalam melakukan aktivitasnya sehari-hari. Apalagi sekarang ini manusia hidup dan bekerja dengan media komputer dan komunikasi yang global.

Internet adalah bagian dari perkembangan teknologi informasi yang pada saat ini berperan penting dalam kehidupan manusia dalam bertukar informasi. Fasilitas internet digunakan oleh individu, instansi pemerintahan, dunia usaha, organisasi internasional, lembaga swadaya masyarakat, partai politik, sekolah maupun lembaga penelitian. Dengan kehadiran internet, manusia dapat memperoleh hiburan melalui *TV-Online*, melakukan transaksi jual beli dalam nilai yang besar dengan berbagai orang di belahan dunia lain dengan cepat dan biaya lebih murah melalui media internet (*E-Commerce*). Melalui fasilitas internet, manusia juga dapat melakukan pembelajaran (*E-Learning*), diagnosa penyakit dalam jarak jauh (*Telemedicine*) dan komunikasi interaktif melalui internet (*Teleconference*).

Seiring dengan perkembangan teknologi informasi (internet) dan semakin banyaknya penggunaan fasilitas internet dalam aktivitas manusia, bentuk kejahatan yang menggunakan komputer dengan fasilitas internet juga berkembang dan telah memunculkan berbagai fenomena baru di berbagai bidang kehidupan

manusia. Kejahatan maupun penyalahgunaan fasilitas internet (kejahatan *cyber*) atau yang sering disebut dengan *cybercrime* telah mengakibatkan kerugian dan keresahan masyarakat, seperti kehilangan uang melalui transaksi elektronik (*online*), perusakan, penyebaran virus, *hacking*, pencemaran nama baik dan bahkan dapat menimbulkan akibat fisik seperti kegiatan terorisme. Penyalahgunaan internet telah mengancam keamanan dan ketertiban masyarakat terutama para pengguna fasilitas internet (Shinder, 2002: 2).

Keamanan dan ketertiban dalam negeri merupakan syarat utama mendukung terwujudnya masyarakat madani yang adil, makmur dan beradab berdasarkan Pancasila dan Undang-undang Dasar Negara Republik Indonesia Tahun 1945. Teciptanya keamanan dalam negeri merupakan tujuan Polri yang dinyatakan secara tersirat dalam Undang-undang Kepolisian. Pemeliharaan keamanan dalam negeri dilakukan melalui upaya penyelenggaraan fungsi pokok Polri sebagai satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman dan pelayanan kepada masyarakat sebagaimana disebutkan dalam Pasal 2 dan Pasal 4 Undang-undang Kepolisian.

Menurut Awaloedin Djamin (1995: 135), fungsi utama Polri yaitu bimbingan kepada masyarakat, prevensi dan represif. Fungsi bimbingan kepada masyarakat merupakan upaya untuk menggugah perhatian (*attention*) dan menanamkan pengertian (*understanding*) pada masyarakat untuk melahirkan sikap penerimaan (*acceptance*) sehingga secara sadar mau berperan serta (*participation*) dalam upaya pembinaan kamtibmas pada umumnya dan ketaatan pada hukum (*law abiding citizen*) khususnya. Fungsi pencegahan (prevensi) merupakan upaya pemeliharaan keselamatan jiwa raga, harta benda dan lingkungan intern dari gangguan ketertiban atau bencana termasuk pemberian perlindungan dan pertolongan. Fungsi represif merupakan upaya penindakan dalam bentuk penyelidikan dan penyidikan gangguan kamtibmas dan kriminalitas.

Fungsi Polri sebagaimana telah dijelaskan diatas selanjutnya dijabarkan dalam tugas pokok dan wewenang Polri. Tugas Polri menurut Undang-undang Kepolisian adalah memelihara keamanan dan ketertiban masyarakat, menegakkan hukum dan memberikan pelindungan, pengayoman, dan pelayanan kepada

masyarakat. Tindakan penyelidikan dan penyidikan atas semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya merupakan salah satu pelaksanaan tugas pokok Polri. Untuk melaksanakan tugas, peranan dan fungsinya, maka kepada Polri harus diberi wewenang. Wewenang yang merupakan pengejawantahan wewenang negara yaitu kekuasaan yang memaksa, yang berdasarkan kehendak dari rakyat (undang-undang) dan merupakan pelaksanaan yang bersifat legal (Awaloedin Djamin, 1995: 135). Dalam Pasal 15 dan 16 Undang-undang Kepolisian, Polri berwenang menerima laporan dan atau pengaduan, melakukan penangkapan, penahanan, penggeledahan, penyitaan, menyerahkan berkas perkara kepada penuntut umum dan melakukan tindakan lain menurut hukum yang berlaku.

Penegakan hukum terhadap *cybercrime* yang telah mengganggu rasa aman pengguna fasilitas internet merupakan pelaksanaan salah satu tugas pokok Polri. Penegakan hukum atas *cybercrime* dilaksanakan melalui penyelenggaraan penyelidikan dan penyidikan terhadap *cybercrime* sesuai dengan ketentuan peraturan perundang-undangan yang memuat tugas pokok Polri dalam kaitannya dengan peradilan pidana (KUHP, KUHAP) dan berbagai undang-undang tertentu lainnya. Akan tetapi, kenyataannya dalam beberapa kasus *cybercrime*, penyelenggaraan penegakan hukum (penyelidikan dan penyidikan) terhadap *cybercrime*, hukum masih tertinggal di belakang kejahatan yang sudah terjadi lebih dahulu, seperti dalam kasus tindak pidana *hacking*.

Tindak pidana *hacking* telah menjadi ancaman bagi keamanan dan ketertiban masyarakat khususnya pengguna fasilitas internet, sedangkan Polri dituntut untuk melakukan penegakan hukum atas tindak pidana *hacking* yang terjadi berdasarkan hukum yang berlaku. Tetapi dalam kenyataannya hukum yang mengatur masih tertinggal dari perkembangan tindak pidana *hacking* yang terjadi. Polri dituntut dapat melaksanakan fungsinya sehingga masyarakat pengguna media internet merasa aman dalam menggunakan internet sebagai media komunikasi maupun transaksi dalam kehidupan sehari-hari.

Polri sebagai aparat penegak hukum dalam memelihara keamanan dan ketertiban masyarakat telah mengantisipasi adanya perkembangan kejahatan *cyber* terutama dalam bidang informasi dengan mendirikan satu unit khusus di bawah

Direktorat II Ekonomi dan Khusus Bareskrim Polri yaitu Unit V *IT & Cybercrime*. Unit V *IT & Cybercrime* dibentuk berdasarkan Keputusan Kepala Kepolisian Republik Indonesia No.Pol.: Kep/9/V/2001 tanggal 25 Mei 2001 tentang Organisasi dan Tata Kerja Korserse Polri. Sedangkan tugas pokok Unit V *IT & Cybercrime* diatur dalam Pasal 180[132] dan Pasal 181[133].

Selanjutnya, berdasarkan validasi Polri pada tanggal 17 Oktober 2002 dengan berubahnya Korps Reserse menjadi Bareskrim Polri Dengan Skep No. Pol.: Kep/53/X/2002, Unit V *IT & Cybercrime* menjadi salah satu unit khusus dalam Direktorat II Ekonomi dan Khusus yang merupakan unit kerja dari Bareskrim Polri.

Unit V *IT & Cybercrime* dipimpin oleh seorang Komisaris Besar Polisi yang saat ini dijabat oleh Kombes Pol. Petrus R. Golose, dengan didukung oleh lebih dari 25 personil yang terdiri dari penyidik dan staf pendukung. Unit V *IT & Cybercrime* bertugas melaksanakan penyelidikan dan penyidikan tindak pidana *cyber* terutama kegiatan yang berhubungan dengan teknologi informasi (teknologi komputer, teknologi telekomunikasi, teknologi elektronika dan teknologi penyiaran) dan menyelenggarakan fungsi laboratorium forensik komputer dalam rangka memberikan dukungan teknis proses penyidikan *cybercrime*.

---

[132]Pasal 180 berbunyi:
"Membantu menyelenggarakan pembinaan fungsi teknis di lingkungan Pidana Tertentu dan menyelenggarakan penyidikan terhadap tindak pidana perbuatan pelanggaran hukum/kejahatan infotek sebagai kejahatan berintensitas tinggi yang mempunyai ruang lingkup internasional dan berdampak terhadap proses globalisasi."

[133]Pasal 181 berbunyi:
"Dalam melaksanakan tugasnya :
1) Menyelenggarakan dan melaksanakan kegiatan represif Kepolisian melalui upaya penyidikan kasus-kasus kejahatan yang bersifat multi dimensi dan mempunyai intensitas tinggi dengan dampak nasional maupun internasional khususnya kejahatan dibidang elektronika termasuk didalamnya kejahatan *E-commerce, Internet Banking* dan Pornografi;
2) Membantu dalam Penyelenggaraan pembinaan fungsi teknis pidana tertentu dalam rangka pembinaan fungsi Reserse secara menyeluruh;
3) Memberikan bantuan operasional kepada Satuan Kewilayahan dan instansi di luar Polri sesuai lingkup tugasnya."

Gambar 4.1
Ruangan Unit V *IT & Cybercrime*

(Sumber: Unit V *IT & Cybercrime*)

Dalam melaksanakan tugas yang diemban, Unit V *IT & Cybercrime*, memerlukan petunjuk dan arah dalam mencapai tujuan organisasi. Unit V *IT & Cybercrime* dibentuk untuk dapat melakukan fungsi Polri dalam bidang penegakan hukum, perlindungan, pengayoman dan pelayanan kepada masyarakat dalam bidang informasi dan teknologi.

Unit V *IT & Cybercrime* merupakan organisasi formal dan modern. Unit V *IT & Cybercrime* merupakan suatu bentuk kerja sama antara sekelompok orang yang tergabung dalam suatu wadah tertentu guna mencapai tujuan bersama seperti yang telah ditetapkan bersama. Secara sederhana, Unit V *IT & Cybercrime* mempunyai tiga unsur, yaitu anggota organisasi, kerjasama antar anggota dan tujuan organisasi. Unit V *IT & Cybercrime* terdiri dari orang-orang yang terdiri dari penyidik dan petugas laboratorium forensik komputer. Dalam melakukan penyidikan, ada kerjasama antara anggota dalam melaksanakan tugas. Kemudian terdapat juga tujuan bersama yang saling terkait atau saling berhubungan sehingga merupakan suatu kesatuan yang utuh.

Unsur tujuan merupakan unsur yang paling utama dalam Unit V *IT & Cybercrime*. Tujuan tersebut menggambarkan apa yang akan dicapai dan apa yang

diharapkan oleh Unit V *IT & Cybercrime* melalui program kerja, kerjasama, kebijakan, strategi, anggaran dan pedoman teknis yang telah ditetapkan. Tujuan juga berfungsi sebagai acuan kinerja Unit V *IT & Cybercrime*. Tujuan Unit V *IT & Cybercrime* diterjemahkan dalam beberapa bentuk tugas-tugas pokok yang dituangkan dalam visi dan misi Unit V *IT & Cybercrime*. Perumusan visi dan misi Unit V *IT & Cybercrime* harus tetap mengacu pada visi dan misi Bareskrim Polri dan Polri sebagai organisasi induk, karena dalam pelaksanaan tugas dan fungsi V *IT & Cybercrime* juga merupakan pelaksanaan tugas dan fungsi Bareskrim Polri dan Polri sebagai organisasi induk.

Visi Unit V *IT & Cybercrime* adalah menjadi penyidik Polri (*Cyber Cop*) yang profesional dalam penegakan hukum di *cyber space* dan kejahatan yang berhubungan dengan teknologi informasi serta meningkatkan kemampuan forensik komputer. Sedangkan misi Unit V *IT & Cybercrime* adalah meningkatkan pengetahuan dan ketrampilan penyidik sebagai penyidik *cyber* dan pelayan masyarakat; menjalin kerja sama dengan sesama aparat penegak hukum, profesional, instansi terkait, universitas dan masyarakat dalam rangka penegakan hukum di bidang teknologi informasi; meningkatkan koordinasi dan kerja sama dalam pengungkapan dan penanggulangan kejahatan transnasional khususnya kejahatan *cyber* dengan aparat penegak hukum negara lain/internasional dan menjadi pusat informasi, pengendalian dan penindakan kejahatan *cyber* dengan mengedepankan laboratorium forensik komputer. Visi dan misi tersebut pada akhirnya dijabarkan melalui pembentukan program kerja Unit V *IT & Cybercrime*, sebagaimana diungkapkan oleh seorang Pamen Unit V *IT & Cybercrime* dalam wawancara berpedoman berikut ini:

> *"Visi dan misi tersebut dijabarkan dalam program kerja yang dibuat skala signifikan untuk dilakukan secara bersama-sama secara konsisten oleh Kanit dan para anggota"* (WBIS 08B)

Untuk melaksanakan fungsi dan tugas Unit V *IT & Cybercrime* dalam mencapai tujuan organisasi, Unit V *IT & Cybercrime* juga telah membentuk struktur Unit V *IT & Cybercrime*, sehingga dalam pelaksanaan tugas sudah terdapat susunan komponen-komponen (unit-unit kerja) dalam organisasi,

hierarki, distribusi kewenangan, deskripsi tugas, kebijakan, prosedur, dan peraturan. Selain itu juga, dengan adanya struktur Unit V *IT & Cybercrime* akan memudahkan dalam penunjukan spesialisasi-spesialisasi pekerjaan, saluran perintah dan penyampaian laporan (Cordner, 2005: 13).

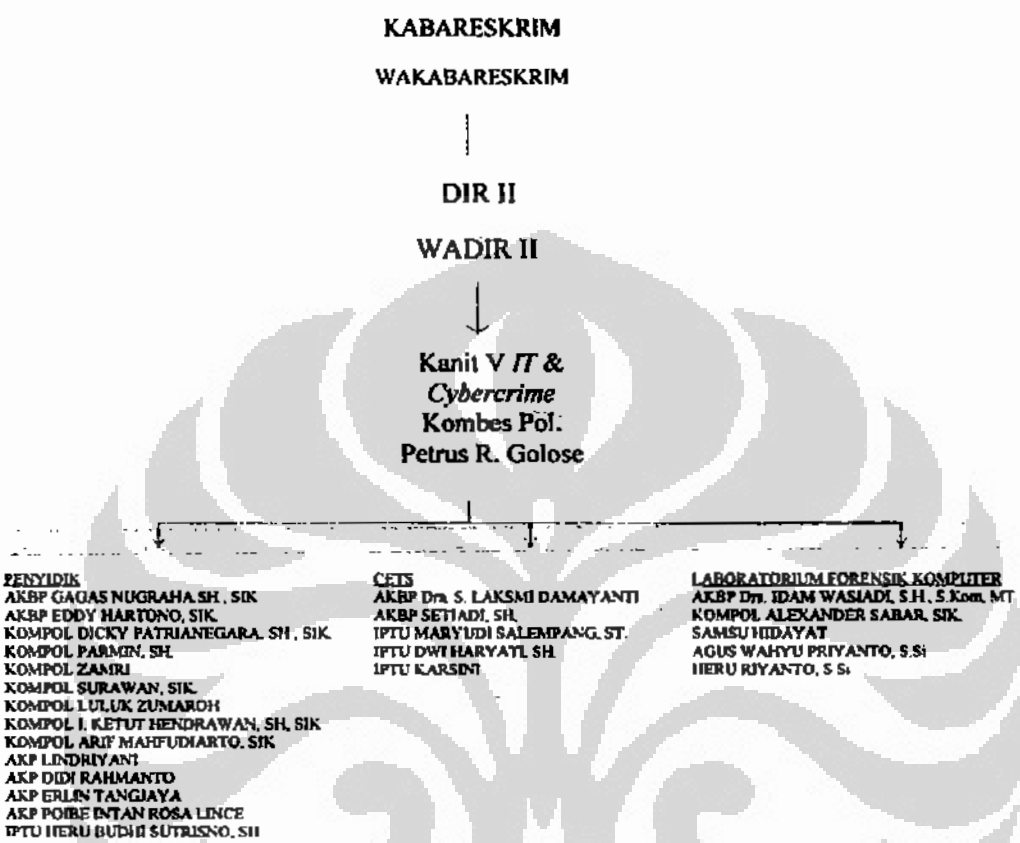
Struktur Unit V *IT & Cybercrime* mengacu pada struktur organisasi Bareskrim Polri sebagai organisasi yang secara hierarki lebih tinggi. Struktur Unit V *IT & Cybercrime* terbagi atas bagian penyidikan dan laboratorium forensik komputer. Struktur organisasi pada Unit V *IT & Cybercrime* menganut struktur organisasi yang berbentuk datar *(flat)* yang terdiri dari Kanit *IT & Cybercrime* dan para anggota. Struktur *flat* ini digunakan agar semua anggota Unit V *IT & Cybercrime* mampu melakukan penyidikan dan bertanggung jawab langsung kepada Kanit sebagai pimpinan organisasi, sebagaimana diungkapkan oleh Pamen dalam wawancara berpedoman.

> *"Struktur organisasi saat ini berbentuk unit dan penyidik secara flat karena masing-masing orang mendapat, kanit dapat mendapat pekerjaan yang sama dalam, ibaratnya sama dan sederajat jadi sama-sama tidak ada batasan sehingga flat kecuali yang kebagian laboratorium forensic karena memerlukan keahlian khusus."* (WBIS 07B)

Dengan struktur organisasi yang *flat*, setiap anggota Unit V *IT & Cybercrime* mempunyai tugas dan tanggung jawab yang sama dalam hal penyidikan kasus *cybercrime*. Namun demikian, *controlling* untuk pelaksanaan tugas sehari-hari adalah dari Kanit V *IT & Cybercrime* dan jika Kanit berhalangan datap didelegasikan kepada Pamen.

> *"Penyidik atau anggota Unit V IT & Cybercrime dan bagian Laboratorium Forensic bertanggung jawab langsung kepada Kepala Unit IT & Cybercrime tetapi dapat juga bertanggung jawab kepada Pamen yang dituakan pada saat Kepala Unit IT & Cybercrime tidak ditempat."* (WBIS 13)

Bagan 4.1
Struktur Organisasi Unit V *IT & Cybercrime*



(Sumber: Unit V *IT & Cybercrime*)

Menurut anggota perwira menengah Unit V *IT & Cybercrime* dalam wawancara berpedoman menyebutkan bahwa Unit V *IT & Cybercrime* berada di bawah struktur organisasi Bareskrim, sehingga bagaimanapun juga kebijaksanaan yang dilakukan oleh Unit V *IT & Cybercrime* merupakan kebijaksanaan dari Bareskrim. Selama unit tersebut masih menyatu apalagi dengan situasi sekarang, Unit V *IT & Cybercrime* bukanlah suatu satuan kerja, tetapi bagian dari pada unit kerja yang mana unit kerjanya adalah Direktorat II Eksus, sehingga bagaimanapun juga kebijakan dari Bareskrim sangat berpengaruh pada kebijaksanaan visi dan misi yang harus dilakukan oleh Unit V *IT & Cybercrime* (WBIS 08B).

Wewenang dan pekerjaan laboratorium forensik komputer adalah spesialisasi di bidang laboratorium forensik komputer yang melaksanakan

kegiatan pemeriksaan *digital evidence* yang diberikan penyidik. Wewenang dan pekerjaan penyidik Unit V *IT & Cybercrime* adalah melaksanakan kegiatan penyelidikan dan penyidikan dengan kewenangan penyidik yang diatur dalam KUHAP dan Undang-undang.

Dengan visi dan misi serta bentuk struktur organisasi yang *flat*, Unit V *IT & Cybercrime* melaksanakan tugas dan kegiatan penyidikan kasus-kasus yang berhubungan dengan informasi dan transfer digital/elektronik seperti *carding, cyberlaundering, cybergambling, cyberpornography, cyberfraud, cyber threatening, cyberterrorism,* pencurian data, pencemaran nama baik, penggelapan data dan sebagainya. Melakukan penyidikan terhadap kasus-kasus yang berhubungan dengan teknologi telekomunikasi yang meliputi penyadapan telepon, penggunaan *Voice on Internet Protocol* (*VoIP*), penipuan melalui telepon genggam dan lainnya.

Unit V *IT & Cybercrime* juga melakukan penyidikan terhadap kejahatan komputer seperti pencurian data, penggelapan data, Ddos *attacks, hacking,* Botnet, pembuatan dan penyebaran virus komputer seperti: *Malicous Code, Spyware, Worm, Trojan horse,* dan lainnya; Penyidikan terhadap kejahatan yang berhubungan dengan Hak Kekayaan Intelektual (HKI) seperti pembajakan *software,* rekaman suara multi media dan sebagainya; Melakukan pembinaan sistem, metode dan personil melalui pelatihan-pelatihan, sosialisasi pembentukan *team building,* menjalin komunikasi dan melakukan pembinaan personil melalui *reward and punishment.*

Dalam prakteknya pelaksanaan penyidikan bukanlah suatu hal yang mudah, karena untuk dapat mencapai tujuan dan sasaran penyidikan yang telah ditargetkan, diperlukan penyidik yang memiliki kemampuan yang telah terlatih secara baik, dan menguasai taktik dan teknik penyidikan. Untuk itu, pembinaan dan pelatihan terhadap para penyidik juga memegang peranan penting terhadap kesuksesan suatu proses penyidikan. Dari data Unit V *IT & Cybercrime,* sejak tahun 2006 sampai dengan 2007 para anggota telah ikut serta dalam beberapa pelatihan dan seminar yang diadakan baik di dalam maupun di luar negeri.

Tabel 4.1
Pelatihan dan Seminar Internasional

No	Tahun	Pelatihan/Seminar	Negara
1	2006	*8th Annual International Fugitive Investigators Conference*	Kanada
2	2006	*Training Computer Facilitated Crimes Against Children*	Thailand
3	2006	*Training Cyber Crime and Computer Facilitated Crimes Againts Children. (Microsoft)*	Indonesia
4	2006	*Law Enforcement and Prosecutor Advanced Cybercrime Training.*	Bangkok
5	2006	*Workshop Hands-on Cybercrime Law Enforcement Technology Microsoft's Corporate Campus.*	USA
6	2006	*Investigation Management Workshop*	Philipina
7	2006	*Task Force FBI Innocent Images National Initiative HQ*	USA
8	2006	*Cyber Terrorism*	Philipina
9	2006	*Training Cybercrime Investigation*	Korea
10	2006	*Financial Crime Forum Asia Pasific*	Hong Kong
11	2006	*Workshop Cybercrime Investigation*	Singapura
12	2006	*Workhop Regional on Terrorism Financing*	Malaysia
13	2007	*Seminar Fighting Cybercrime Intelligence, Enforcement and Exchanges of Best Practices Police*	Singapura
14	2007	*The Asian Pasific Risk Management Conference (VISA)*	Singapura
15	2007	*ID SIRTII (Cybercrime)*	Philipina
16	2007	*4th Asean Regional Forum (ARF) Seminar on Cyber Terrorism.*	Korea
17	2007	*CETS International Meeting*	Italy
18	2007	*8th CITINS Annual Conference and The 5th ICPO Crime Investigation*	Jepang

No	Tahun	Pelatihan/Seminar	Negara
19	2007	*5th International Botnet Task Force Conference*	USA
20	2007	*6th International Botnet Task Force Conference*	Australia
21	2008	*Training for Trainers on Computer Forensics*	New Zealand

(Sumber: Unit V *IT & Cybercrime*)

Gambar 4.2
Pelatihan Anggota Unit V *IT & Cybercrime* di Luar Negeri

Law Enforcement and Prosecutor Advanced Cybercrime Training di Bangkok Thailand 20 Juni 2006

(Sumber: Unit V *IT & Cybercrime*)

Dalam rangka pembenahan fasilitas yang mendukung terhadap pelaksanaan tugas Unit V *IT & Cybercrime*. Unit V *IT & Cybercrime* juga melakukan pembinaan materiil, fasilitas dan jasa melalui inventarisasi alat utama (alut) dan alat khusus (alsus), menata dan merenovasi fasilitas: Melakukan *back up* teknis dan supervisi ke wilayah dalam rangka penanganan kasus *cybercrime* yang terjadi; Pengadaan fasilitas-fasilitas pendukung yang belum tersedia untuk menambah efektivitas dan efisiensi operasional Unit V *IT & Cybercrime*.

Gambar 4.3
Fasilitas Unit V *IT & Cybercrime*

Forensic Recovery of Evidence Device (FRED)

(Sumber: Unit V *IT & Cybercrime)*

Gambar 4.4
Fasilitas Unit V *IT & Cybercrime*

Talon Logicube* yang digunakan untuk *Imaging* dan *Cloning

(Sumber: Unit V *IT & Cybercrime*)

Dalam penanganan kasus *cybercrime*, penyidik Unit V *IT & Cybercrime* bekerja sama dengan laboratorium forensik komputer. Apabila penyidik menemukan alat bukti digital dalam penanganan kasus *cybercrime*, penyidik memberikan secara perlahan kepada petugas laboratorium forensik komputer. Penyidik membuat surat atau permohonan secara formal bahwa kasus tersebut perlu dilakukan proses forensik sehingga dituangkan juga mengenai isi-isinya. Setelah itu, pihak laboratorium forensik komputer menindak lanjuti dan hasil dari proses tersebut akan dibuatkan berita acara sebagai masukan bagi penyidik untuk pemberkasan, sebagaimana diungkapkan oleh perwira menengah Unit V *IT & Cybercrime* dalam wawancara berpedoman berikut ini:

> *"Saya melihat secara fungsional disitu adanya unit Cybercrime memiliki Laboratorium Komputer Forensic secara fungsi dan sesuai dengan job description. Disamping sebagai penyidik dalam hal penyelidikan unit Cybercrime juga melakukan kegiatan Laboratorium Forensic, sehingga mendukung kegiatan operasional pada fungsi-fungsi lain. Saya melihat sejauh ini kinerja yang dilakukan pun sangat baik sekali sejauh ini." (WBIS 07B)*

Gambar 4.5
Laboratorium Forensik Komputer

(Sumber: Unit V *IT & Cybercrime*)

Selain menjalin hubungan kerja sama dengan laboratorium forensik komputer, Unit V *IT & Cybercrime* juga menjalin hubungan dan koordinasi dengan instansi terkait dalam rangka terjalinnya kerja sama nasional dan internasional yang efektif untuk dapat memberikan dukungan dan solusi penanganan tindak pidana *cybercrime* di Indonesia. Unit V *IT & Cybercrime* telah melakukan perluasan *networking* di dalam tubuh Polri seperti dengan unit lain, direktorat/DENSUS 88, Bareskrim dan Polda. Perluasan *networking* di luar tubuh Polri, misalnya dilakukan dengan Asosiasi Pengusaha Jasa Internet Indonesia (APJII), Microsoft, Depkominfo. Kanit V *IT & Cybercrime* juga berusaha untuk membangun perluasan *networking* dengan membuat rencana perluasan tersebut ke dalam program kerja sehingga seluruh para anggota juga turut berperan aktif.

Berkaitan dengan penegakan hukum atas *cybercrime*, Unit V *IT & Cybercrime* merupakan salah satu unit terdepan yang mengemban fungsi Polri sebagai penegak hukum yang berhubungan dengan kejahatan dalam bidang teknologi informasi dan *cybercrime*. Penyidikan merupakan upaya dalam rangka penegakan hukum yaitu untuk menjamin adanya kepastian hukum yang didambakan oleh pencari keadilan. Penyidikan atas kejahatan dalam bidang teknologi informasi dan *cybercrime* merupakan upaya Unit V *IT & Cybercrime* dalam mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana *cyber* dalam bidang teknologi informasi, menentukan apakah peristiwa tersebut dapat dilanjutkan ke tahap penyidikan, mencari serta mengumpulkan barang bukti, membuat terang kejahatan dalam bidang teknologi informasi dan *cybercrime* dan menemukan tersangka sebagaimana diatur dalam Pasal 1 angka 2 KUHAP.

Unit V *IT & Cybercrime* dalam melaksanakan tugasnya dalam hal penyidikan tentu sangat berbeda dengan tugas unit lainnya, karena *cybercrime* bukanlah tindak pidana konvensional sehingga dalam penanganannya diperlukan keahlian teknologi dan informasi serta tak kalah pentingnya keahlian dalam bidang hukum. Sebagaimana diungkapkan dalam *Focus Group Discussion* (*FGD*) dengan Pama berikut ini:

"yang istimewa mungkin mas karena dia penyidik nya kan ...kalau apa ...di Cybercrime itu kan nggak bisa nyata ...kejahatan nya yang maya lantas bisa terungkap ...beda dengan reserse – reserse yang lain" (*FGD* Pama)

Dari data hasil penanganan kasus Unit V *IT & Cybercrime* tahun 2005 sampai dengan tahun 2007, jumlah laporan yang diterima sebanyak 35 kasus. Dari jumlah laporan tersebut, laporan yang berhasil diselesaikan adalah sebanyak 17 laporan dari jumlah laporan yang diterima. Sedangkan 17 laporan lain masih dalam proses dan 1 laporan dilimpahkan ke Polda Metro Jaya. Data dari jumlah laporan polisi yang ditangani Unit V *IT & Cybercrime* tahun 2005 sampai dengan tahun 2007 dapat diperoleh gambaran kinerja Unit V *IT & Cybercrime* dalam pelaksanaan tugasnya.

Pada tahun 2005 terdapat 4 (empat) laporan, dari jumlah laporan yang diterima tersebut, jumlah laporan yang telah ditangani sebanyak 2 (dua) laporan dari jumlah laporan yang diterima sampai pada proses penyerahan berkas perkara kepada penuntut umum (P.21). Sedangkan dua laporan lainnya masih dalam proses penyidikan Unit *V IT & Cybercrime* sehingga persentasi penyelesaian kasus untuk tahun 2005 sebesar 50 persen dari jumlah kasus yang diterima Unit V *IT & Cybercrime.*

Sedangkan pada tahun 2006, jumlah laporan polisi yang diterima adalah sebanyak 23 (dua puluh tiga) laporan. Dari jumlah laporan tersebut, 14 (empat belas) laporan telah selesai ditangani, sedangkan 9 (sembilan) kasus lainnya masih dalam proses penanganan, meliputi 1 (satu) laporan masih dalam proses penyelidikan, 6 (enam) laporan masih dalam tahap penyidikan sedangkan 2 (dua) laporan lainnya masih dalam tahap pengembalian berkas perkara untuk dilengkapi (P.19). Dari jumlah penanganan atas laporan yang diterima pada tahun 2006, Unit V *IT & Cybercrime* telah menyelesaikan 61 persen dari jumlah laporan yang diterima.

Pada tahun 2007, jumlah laporan yang diterima oleh Unit V *IT & Cybercrime* adalah sebanyak 8 (delapan) laporan. Dari jumlah laporan tersebut, 2 (dua) laporan telah selesai ditangani. Sedangkan 6 (enam) laporan lainnya masih dalam proses penyidikan. Dari jumlah laporan yang diselesaikan, Unit V *IT & Cybercrime* hanya menyelesaikan penanganan kasus 25 persen dari jumlah kasus

yang diterima. Jumlah kasus tersebut belum termasuk pengaduan dari luar negeri mengenai *cybercrime* yang dilakukan dari Indonesia. Dari data kasus penipuan via internet pelaku berbasis *web house* di Indonesia periode Januari-Desember 2007 sebagai contoh pada tahun 2007 terdapat pengaduan dari Australia, Polandia, Perancis, Swiss dan USA sebanyak 7 pengaduan. Pengaduan tersebut meliputi penipuan melalui internet, percobaan penipuan menggunakan kartu kredit dan penipuan belanja *online*.

Jumlah penyelesaian penanganan kasus pada tahun 2007 mengalami penurunan dibandingkan jumlah penyelesaian penanganan kasus pada tahun 2006 dan tahun 2005 sebagaimana terlihat dalam tabel di bawah ini, hal tersebut dikarenakan pada bulan Maret 2006 sampai bulan Desember 2007, Kepala Unit V *IT & Cybercrime* tidak secara rutin berada di kantor.

Tabel 4.2
Penanganan Kasus Unit V *IT & Cybercrime* Tahun 2005 s/d 2007

Tahun	Jumlah Laporan	Selesai ditangani	Proses Penanganan	Persentase
2005	4	2	2	50 persen
2006	23	14	9	61 persen
2007*	8	2	6	25 persen
Jumlah	35	18	17	51 persen

(Sumber: Unit V *IT & Cybercrime*)

*)Catatan: Dari bulan Maret sampai dengan Desember 2007, Kanit V *IT & Cybercrime* tidak secara rutin berada di kantor.

Dari data jumlah penanganan kasus yang telah berhasil ditangani oleh Unit V *IT & Cybercrime* sejak tahun 2005 sampai dengan tahun 2007 merupakan wujud pelaksanaan tugas Unit V *IT & Cybercrime* sebagai fungsi penegakan hukum atas *cybercrime* khususnya dalam bidang teknologi informasi yang terjadi. Salah satu diantaranya adalah pelaksanaan penyidikan atas tindak pidana *hacking website* Partai Golkar yang terjadi pada tanggal 8 Juli 2006.

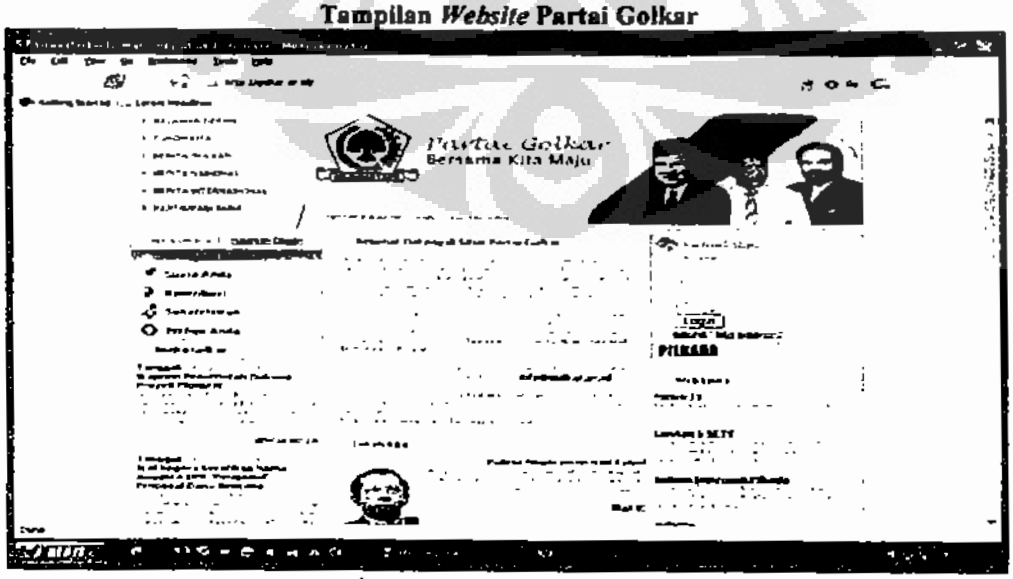
4.2 Penyidikan Tindak Pidana *Hacking Website* Partai Golkar

4.2.1 Website Partai Golkar

Website atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara, dan atau gabungan dari semuanya itu baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman. *Website* dapat dimiliki oleh orang, perusahaan maupun partai yang digunakan sebagai salah satu media informasi. Salah satu partai yang memiliki alamat *website* adalah Partai Golkar.

Partai Golkar memiliki *website* resmi yang beralamatkan *www.golkar.or.id* (**"*Website* Partai Golkar"**). *Website* ini digunakan oleh Partai Golkar sebagai media komunikasi antar anggota Partai maupun media komunikasi dengan masyarakat umum yang ingin mengetahui atau mendapatkan informasi mengenai Partai Golkar, baik berita-berita aktual, tokoh-tokoh partai, visi dan misi Partai Golkar, dan sebagainya. *Website* resmi Partai Golkar ini dapat diakses oleh semua pengguna internet sehingga setiap orang dapat mencari informasi-informasi aktual yang berkaitan dengan Partai Golkar.

Gambar 4.6
Tampilan *Website* Partai Golkar



(Sumber: *www.golkar.go.id)*

4.2.2 Pelaporan

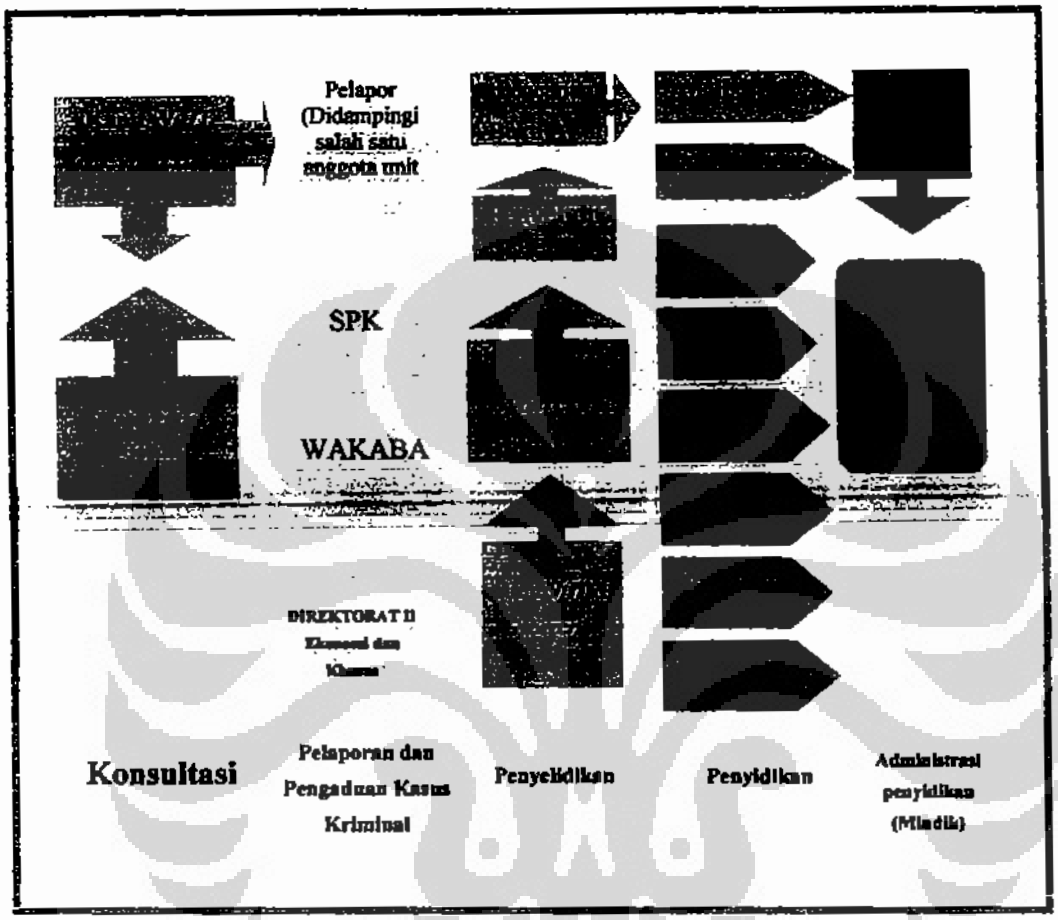
Dalam melakukan rangkaian proses hukum terhadap kasus pidana, penyidik terlebih dahulu menerima laporan dan atau pengaduan dari masyarakat atau korban di Sentra Pelayanan Kepolisian (SPK) sebagaimana diatur dalam Pasal 5 dan 7 KUHAP. Selanjutnya petugas piket di SPK akan membuatkan laporan polisi dalam rangkap enam yang isinya berkaitan dengan keterangan tentang identitas pelapor, uraian singkat kejadian atau perkara yang dilaporkan atau diadukan, korban dan kerugian yang diderita, tindak pidana yang dilanggar beserta pasal-pasal yang dikenakan serta penerima laporan dan kepala SPK.

Selanjutnya Kepala SPK melanjutkan laporan atau pengaduan kepada Wakil Kepala Bareskrim Polri (Wakabareskrim), kemudian didistribusikan kepada direktur sesuai dengan bidang tugasnya masing-masing. Selanjutnya oleh direktur didistribusikan kepada kepala unit (Kanit) berdasarkan disposisi siapa yang menangani laporan polisi atau pengaduan. Kemudian oleh Kanit di disposisi atau diterbitkan surat perintah tugas kepada penyidik dibawahnya untuk menangani laporan polisi tersebut.

Setelah diterbitkan surat perintah tugas kepada penyidik, penyidik mulai bekerja melakukan penyidikan atas kasus yang dilaporkan atau diadukan tersebut. Dalam melakukan penyidikan, para penyidik dapat melakukan pemanggilan, penahanan, penyitaan, pemeriksaan, penangkapan dan penggeledahan.

Penanganan kasus kasus tindak pidana *hacking website* Partai Golkar, terlebih dahulu dilakukan konsultasi antara pelapor dari perwakilan korban dengan Kanit V *IT & Cybercrime* selanjutnya membuat laporan polisi, peyelidikan dan penyidikan selanjutnya dilakukan pemberkasan berkasa untuk diserahkan ke penuntut umum, sebagaimana dijelaskan dalam bagan 4.2 berikut ini.

Bagan 4.2
Skema Penanganan Kasus *Hacking Website* Partai Golkar



(Sumber: Penulis)

Dalam kasus tindak pidana *hacking website* Partai Golkar, laporan oleh perwakilan Partai Golkar dilakukan setelah bertemu dan berdiskusi terlebih dahulu dengan Unit V Diskusi tersebut dilakukan pada tanggal 17 Juli 2006, yang pada intinya membahas mengenai jenis tindak pidana yang akan dikenakan terhadap *hacker website* Partai Golkar.

Diskusi seperti itu, bukan merupakan prosedur formal dalam proses pelaporan, akan tetapi dalam hal ini pelaporan dilakukan oleh Ir. Fayakhun dan Zulhendri Hasan, S.H., M.H., selaku perwakilan Partai Golkar untuk membahas rencana pelaporan yang akan dilakukan oleh Partai Golkar, mengingat jenis tindak pidana *hacking* belum secara tegas diatur dalam ketentuan yuridis yang

tersedia. Hal lain yang melatarbelakangi kedatangan pelapor kepada Unit V *IT & Cybercrime*, sebagaimana terungkap dalam wawancara berpedoman dengan pelapor:

> *"...sudah mendengar bahwa kepolisian Republik Indonesia sudah mempunyai unit cybercrime dibawah Bareskrim..."(*WBOS 02).

> *"Baik yang pertama serius menanggapi dengan serius... yang kedua sistematis...jadi kita kan Golkar gak tangan kosong ketika kita datang diinternet itu tidak ada yang tidak ada jejaknya pak kejahatan bisa dilakukan tapi jejaknya ada itu yang kita tau...*(WBOS 02).

Pelapor sadar bahwa tindak pidana yang akan dilaporkan merupakan bagian dari ruang lingkup tugas Unit V *IT & Cybercrime*, disamping kepercayaan mereka bahwa Unit V *IT & Cybercrime* dianggap mampu menyelesaikan penyidikan tindak pidana *hacking*, sehingga mereka tidak akan pulang dengan tangan kosong setelah melaporkan kasusnya kepada Unit V *IT & Cybercrime*.

Dalam pertemuan tersebut, dibahas mengenai tindak pidana *hacking* terhadap *Website* Partai Golkar yang terjadi beberapa kali dan belum diketahui siapa pelakunya. Partai Golkar merasa telah dirugikan karena kerusakan akibat tindak pidana *hacking* dinilai sangat mengganggu kepentingan Partai Golkar dan bahkan merusak kredibilitasnya. Partai Golkar mempunyai kepentingan yang besar untuk segera mengetahui siapa pelakunya dan menuntut proses hukum terhadap pelaku.

Dalam pertemuan tersebut disepakati bahwa tindakan *hacking Website* Partai Golkar dapat dikategorikan sebagai suatu tindak pidana, dan proses penyidikan terhadapnya seyogyanya tetap harus dilakukan menurut ketentuan hukum yang berlaku. Partai Golkar selanjutnya membuat suatu laporan tindak pidana resmi menurut prosedur yang berlaku di lingkungan Bareskrim Polri yaitu melalui unit SPK.

Oleh karena pembuatan laporan pidana tersebut telah dibicarakan sebelumnya, maka proses pembuatan laporannya menjadi lebih cepat, dan melewati beberapa tahap birokrasi sebelum diperoleh disposisi, sehingga mempercepat proses dimulainya tindak lanjut laporan oleh Unit V *IT &*

Cybercrime. Proses demikian bukanlah proses yang berlaku secara normatif di lingkungan Bareskrim Polri. Hal ini terungkap dalam pernyataan seorang Pama dalam Wawancara Berpedoman (WBIS 01 A) sebagai berikut:

> *"...biasanya laporan polisi yang diterima dipiket siaga itu tidak akan langsung ke unit yang bersangkutan tapi sampai dulu ke Wakabareskrim atau Kabareskrim baru kemudian ke direktur dari direktur baru kemudian ke unit ..."*

Dari uraian di atas terungkap bahwa penyidik Unit V *IT & Cybercrime* langsung menerima laporan dari pihak korban yang kemudian membantu proses pembuatan laporan polisi, kemudian penyidik mendampingi korban dalam proses pembuatan laporan polisi yang telah dibuat. Hal ini menunjukkan bahwa penanganan kasus oleh Unit V *IT & Cybercrime* dilakukan secara lebih responsif dan dengan melewati beberapa tahap birokrasi untuk menghasilkan proses yang lebih cepat. Alasan yang melatarbelakangi hal tersebut adalah karena sebelumnya pihak korban telah mengetahui keberadaan Unit V *IT & Cybercrime*, mengenal dengan baik Kanit V *IT & Cybercrime* serta adanya kekhawatiran bahwa petugas piket yang berjaga di SPK kurang dapat memahami tindak pidana yang dilaporkan dan menentukan tindak pidana yang disangkakan kepada terlapor atau tersangka.

Sejalan dengan pembuatan laporan polisi tersebut di atas, Kepala Unit V *IT & Cybercrime* segera menindaklanjutinya dengan menerbitkan Surat Perintah Tugas No.Pol.SP.Gas/145/VII/2006/Dit II Eksus tertanggal 17 Juli 2006, yang memerintahkan kepada 16 (enam belas) anggota Unit V *IT & Cybercrime* untuk melakukan **penyelidikan dan penyidikan** terhadap tindak pidana di bidang telekomunikasi dan perusakan terhadap tampilan *website* Partai Golkar.

4.2.3 Proses Penyidikan Tindak Pidana *Hacking Website* Partai Golkar

Proses penyidikan kasus tindak pidana *hacking website* Partai Golkar dilaksanakan oleh Unit V *IT & Cybercrime*. Pelaksanaan penyelidikan dan penyidikan kasus tindak pidana *hacking website* Partai Golkar tersebut pada prinsipnya harus tetap berpedoman pada ketentuan hukum acara yang berlaku dan merujuk pada aturan atau sistem operasional yang berlaku di Polri seperti

pedoman penyidikan tindak pidana dan pedoman penyelenggaraan administrasi penyidikan.

Dalam pembahasan mengenai proses penyidikan kasus tindak pidana *hacking website* Partai Golkar ini dilaksanakan dalam tiga tahap, yaitu: penyelidikan; penindakan dan pemeriksaan; dan penyelesaian dan penyerahan berkas perkara.

4.2.3.1 Tahap Pertama: Penyelidikan

Sebagaimana telah dibahas dalam Bab III, penyelidikan merupakan tindakan tahap pertama permulaan penyidikan, namun bukan tindakan sendiri yang terpisah dari fungsi penyidikan (Harahap, 2006: 101-102). Penyelidikan dilakukan untuk mengumpulkan bukti permulaan atau bukti yang cukup agar dapat dilakukan tindak lanjut penyidikan. Dalam tahap ini, penyelidik dituntut untuk menemukan suatu peristiwa yang diduga merupakan tindak pidana, dimana hasil dari penemuannya akan sangat menentukan sikapnya untuk melanjutkan dilakukannya penyidikan atau tidak.

Proses penyelidikan kasus tindak pidana *hacking website* Partai Golkar dimulai dengan proses pelaporan yang dibuat oleh Partai Golkar. Dalam laporan tersebut, pelapor yang mewakili Partai Golkar telah memberikan keterangan mengenai uraian singkat kejadian serangan perusakan *website* Partai Golkar. Sebagai respon atas laporan polisi tersebut, Kanit V *IT & Cybercrime* segera menindaklanjutinya dengan menerbitkan Surat Perintah Tugas No. Pol.SP.Gas/145/VII/2006/Dit II Eksus tertanggal 17 Juli 2006, yang memerintahkan kepada 16 (enam belas) anggota Unit V *IT & Cybercrime* untuk melakukan penyelidikan dan penyidikan perusakan tampilan *website* www.golkar.or.id. Para anggota tersebut adalah: (1) Eddy Hartono, S.Ik., Ajun Komisaris Besar Polisi (AKBP); (2) Dra. S Laksmi D., AKBP; (3) Setiady, S.H., AKBP; (4) Drs. Idam Wasidi, SKom., MT, AKBP; (5) Parmin, Komisaris Polisi (Kompol); (6) Zamri, SKom., Kompol; (7) Dicky Patrianegara, S.H., S.Ik., M.Si., Kompol; (8) Surawan, S.Ik., Kompol; (9) Lindriayani, S.H., Ajun Komisaris Polisi (AKP); (10) Arif Makhfudiarto, S.Ik., AKP; (11) I K Budi Hendrawan, S.H., S.Ik., AKP; (12) Alexander Sabar, S.Ik., AKP; (13) Didi Novi Rahmanto,

AKP; (14) Poibe Inten Nosa Lince, Inspektur Polisi I; (15) H. Budhi Sutrisno, S.H., M.H., Inspektur Polisi I; (16) Maryudi Salempang, S.T., Inspektur Polisi II.

Berdasarkan Surat Perintah Tugas tersebut, tim penyelidik yang ditunjuk segera melaksanakan pemeriksaan terhadap 2 (dua) orang saksi yaitu Zulhendri Hasan dan Daulat Firman Abraham. Terhadap kedua saksi tersebut telah diperiksa dengan menggunakan teknik penyelidikan yang berupa wawancara (*interview*). Wawancara terhadap Zulhendri Hasan selaku saksi pelapor dilakukan oleh Eddy Hartono, S.iK, bersama-sama dengan Alexander Sabar, S.iK. Hasil wawancara tersebut kemudian dituangkan dalam Berita Acara Pemeriksaan (Saksi) tertanggal 17 Juli 2006 dan ditandatangani oleh kedua penyidik dan saksi yang bersangkutan.

Berdasarkan Berita Acara Pemeriksaan (Saksi) atas nama Zulhendri Hasan tersebut, tim penyelidik memperoleh informasi yang pada intinya menjelaskan bahwa saksi pelapor mengetahui peristiwa penggantian halaman depan *website* Partai Golkar dari bagian *IT* yang bernama Ir. Fayakhun Andriadi. Selanjutnya menurut keterangannya, dia mengetahui berdasarkan laporan pihak *IT* bahwa serangan terhadap *website* Partai Golkar tersebut dilakukan sebanyak lima kali. Serangan pertama dilakukan pada tanggal 8 Juli 2006 sekitar pukul 21.00 WIB dimana halaman depan diganti dengan foto seronok artis Hollywood dan tulisan "Bersama kita malu". Serangan kedua pada tanggal 9 Juli 2006 sekitar pukul 17.00 WIB, tampilan diganti dengan tulisan "Hidup Indonesia Merdeka, Oleh Batam Hackerindo". Serangan ketiga pada tanggal 10 Juli 2006 sekitar pukul 09.00 WIB, halaman depan diganti dengan foto gorila putih dan tulisan "Bersama Kita Malu", dan aplikasi sistem manajemen konten juga dirusak. Pada tanggal 11 Juli 2006 terjadi lagi serangan sehingga *Web Administrator* mematikan sama sekali Partai Golkar tanpa mengambil sistem-sistem *back end* yang ada. Pada tanggal 13 Juli 2006, kembali halaman depan diganti dengan foto gorila putih sehingga *Web Administrator* mengangkat seluruh perangkat lunak yang ada.

Menurut keterangan saksi pelapor bahwa dalam setiap serangan tersebut, *Web Administrator* selalu mengembalikan situs ke kondisi normal kecuali pada tanggal 11 dan 13 Juli 2006. Karena serangan tersebut, saksi pelapor menerangkan bahwa Golkar adalah pihak yang dirugikan baik dari sisi politik

maupun dari sisi penegakan hukum. Di samping itu, serangan tersebut telah menimbulkan kerusakan pada sistem komputer situs Partai Golkar, sehingga Golkar telah mengalami kerugian secara material sebesar Rp.150.000.000,00 (seratus lima puluh juta Rupiah). Bagi Partai Golkar *website* tersebut merupakan alat komunikasi politik Partai yang digunakan sebagai sarana pendidikan politik bagi kader Partai Golkar.

Sedangkan pemeriksaan (saksi) terhadap Daulat Firman Ibrahim dilakukan dengan teknik wawancara (*interview*) oleh Dicky Patrianegara, S.H., SiK., Msi., selaku penyidik yang dituangkan dalam Berita Acara Pemeriksaan (Saksi) tertanggal 17 Juli 2006. Dari keterangan Daulat Abraham Firman, diperoleh keterangan bahwa saksi merupakan tenaga profesional pada Dewan Pimpinan Pusat (DPP) Partai Golkar, yang menjabat sebagai pengelola *website* Partai Golkar sejak bulan Juni 2005, dan mempunyai tugas dan tanggung jawab untuk mengembangkan situs atau *website* Partai Golkar, dan *maintainance* atau mengelola *website* Partai Golkar. Lebih lanjut Daulat Firman Abraham menerangkan juga bahwa ia mengetahui telah terjadi 5 (lima) kali serangan terhadap *website* milik partai Golkar *www.golkar.or.id* berbentuk perusakan tampilan dan sistem manajemen konten. Serangan pertama dilakukan pada hari Sabtu tanggal 8 Juli 2006 pukul 21.00 WIB dengan mengubah tampilan *website* berupa foto setengah badan menggunakan bikini Anna Nicole Smith (artis *Hollywood*) dengan tulisan di atas foto tersebut "Bersama Kita Malu". Serangan kedua pada hari Minggu tanggal 9 Juli 2006 lebih kurang pukul 17.00 WIB *website* Partai Golkar terjadi serangan dengan penggantian halaman muka sehingga terdapat tulisan "Hidup Indonesia Merdeka" oleh "Batam Hackerindo". Serangan ketiga pada hari Senin tanggal 10 Juli 2006 lebih kurang pukul 09.00 WIB dimana situs *website* Partai Golkar mempunyai tampilan yang tidak semestinya, yaitu "foto gorila putih" dan tulisan "Bersatu kita malu" dan serangan kali ini telah merusak *script* dan aplikasi manajemen konten situs *website* Partai Golkar.

Masih menurut Daulat Firman Abraham, serangan keempat pada tanggal 11 Juli 2006 sekitar pukul 11.00 WIB ditemukan ketika *chatting* dengan *pt_mvn_supp@yahoo.com* tehnikal *support* dari PT Master Web Network untuk

menanyakan mengenai *back up website* Partai Golkar. Serangan tersebut menyebabkan tampilan *website* tersebut telah berganti kembali dengan foto gorila putih dengan tulisan di atasnya "Bersatu Untuk Malu" dan manajemen konten tetap tidak dapat diakses. Serangan terakhir pada tanggal 14 Juli 2006 pukul 01.00 WIB menyebabkan halaman depan *website* Partai Golkar berganti kembali dengan foto gorila putih dengan tulisan diatasnya "Bersatu Untuk Malu".

Sebagai tenaga *IT* yang bertanggung jawab terhadap *website* Partai Golkar mengetahui tindakan serangan tersebut, Daulat Firman Abraham menyatakan telah mengambil tindakan mengganti halaman yang di-*deface* tersebut seperti semula. Saksi Daulat Firman Abraham melakukan tindakan mengganti halaman yang di-*deface* tersebut dengan cara masuk ke *server master web net* menggunakan *software* FTP yang terdapat di laptop, selanjutnya memasukkan *host address www.golkar.or.id, user name* **t66679,** password **Golkar)^,** dan mengklik *connect*. Cara tersebut akan menyebabkan layar komputer akan menampilkan *directory* dari golkar.or.id. Kemudian masuk ke *folder sites* dan halaman yang rusak, yaitu indeks.php dihapus kemudian *up load* indeks.php yang semestinya.

Selanjutnya Daulat Firman Abraham menerangkan bahwa dia juga melakukan cara lain, dengan menghubungi *host master* dari pada *website* Partai Golkar, yaitu PT Master Web Network melalui *Yahoo Messanger pt_mvn_supp@yahoo.com* dan *email* ke *support@masterwebnet.com* untuk menginformasikan bahwa telah terjadi serangan berupa *deface* ke *website* Partai Golkar. Akibat yang ditimbulkan adalah adanya tanggapan dari PT Master Web Network yang akan mengecek *log files* dari *server* mereka.

Untuk mengetahui apa yang terjadi dengan *website* Partai Golkar, Daulat Firman Abraham men-*download log files* dari tanggal 8 – 14 Juli 2006, yang dilakukan dengan cara masuk ke *server master web net* menggunakan *software* FTP yang terdapat di laptop. Selanjutnya memasukkan *host address www.golkar.or.id, user name* **t66679,** password **Golkar)^,** dan meng-klik *connect*, akibatnya di layar akan ditampilkan *directory* dari Golkar.or.id. Kemudian ia masuk ke *folder Log* dan mengklik *download* untuk meng-*copy* semua data antara tanggal 8 – 14 Juli 2006.

Di samping itu, Daulat Firman Abraham, menerangkan juga bahwa *website* Golkar dibuat berdasarkan putusan rapat pimpinan nasional Partai Golkar pada bulan Desember 2005. Ia menyatakan bahwa ia beserta tim yang terdiri dari Agung Farhadi, Lenny dan Nano Surbakti adalah pihak yang melaksanakan tugas pembuatan *website* Partai Golkar. Menurutnya, setiap orang bisa mengakses *website* Partai Golkar tersebut namun setiap orang tidak dapat mengubah dan menambah tampilan yang ada kecuali orang-orang yang memiliki akses admin, yaitu Daulat Firman Abraham selaku *web master*, Agung, Viktus Murin, Hayadi, Ratno dan Uus selaku redaksi pelaksana serta Fayakhun Andriadi.

Sehubungan dengan pemeriksanaan saksi-saksi tersebut di atas, penyidik telah melakukan penyitaan barang bukti satu keping *CD* yang berisikan *log files* www.golkar.or.id tanggal 8 Juli 2006 sampai dengan 14 Juli 2006 dan *hard copy* akses *log* dari tanggal 8 Juli 2006 sampai dengan 14 Juli 2006 sebanyak tujuh bundel. Atas barang bukti yang diserahkan oleh pelapor telah dibuatkan Surat Tanda Penerimaan Barang Bukti No. Pol.: STP/07/VII/2006/Dit Eksus serta Berita Acara Penyitaan dengan dasar Surat Perintah Penyitaan No. Pol.: SP. Sita/ 76/ VII/ 2006/ Dit Eksus.

Dari hasil pemeriksaan tersebut, penyidik memberikan laporannya kepada Kanit V *IT & Cybercrime* Bareskrim Polri. Selanjutnya tim penyidik bersama dengan Kanit *IT & Cybercrime* mempelajari dan menganalisis keterangan-keterangan yang telah diperoleh dari 2 (dua) orang saksi beserta barang bukti yang disita berupa satu keping *CD* yang berisikan *log files www.golkar.or.id* tanggal 8 Juli 2006 sampai dengan 14 Juli 2006 dan *hard copy* akses *log* dari tanggal 8 Juli 2006 sampai dengan 14 Juli 2006 sebanyak tujuh bundel. Berdasarkan hasil analisis atas keterangan dan informasi yang terdapat dalam satu keping *CD* yang telah disita, tim penyidik setelah berdiskusi dengan Kanit V *IT & Cybercrime* selanjutnya telah menyatakan bahwa hasil penyelidikan yang dilaksanakan dengan menggunakan teknik wawancara (*interview*) terhadap dua orang saksi sebagaimana dijelaskan di atas, dianggap telah memenuhi bukti permulaan atau bukti yang cukup agar dapat dilakukan tindak lanjut penyidikan.

Berdasarkan uraian di atas, diketahui bahwa penyidik Unit V *IT & Cybercrime* telah melaksanakan bagian dari proses penyelidikan yaitu melakukan

pemeriksaan saksi yang mengetahui mengenai kejadian serangan-serangan berupa *deface* tampilan *website* Partai Golkar, dan mengenai pihak-pihak yang dianggap terlibat atau mengetahui mengenai serangan-serangan tersebut. Disamping itu, dilakukan pula tindakan penyitaan terhadap barang bukti yang diserahkan oleh saksi pelapor, diantaranya berupa *log files* yang sangat diperlukan dalam proses penyidikan selanjutnya, yaitu pengungkapan dan pencarian tersangka yang melakukan tindak pidana *hacking* tersebut. Oleh karenanya, berdasarkan laporan hasil penyelidikan dan evaluasi yang dilakukan serta informasi dari barang bukti yang diperoleh, penyidik berkesimpulan bahwa peristiwa hukum penyerangan *website* Partai Golkar adalah tindak pidana.

Untuk dapat menetapkan suatu tindakan yang dilaporkan sebagai tindak pidana, maka harus memenuhi bukti permulaan yang cukup agar dapat dilakukan tindak lanjut penyidikan (Yahya Harahap, 2006: 101). Dalam hal ini, bukti permulaan yang dianggap cukup oleh penyidik Unit V *IT & Cybercime* adalah Laporan Polisi dan keterangan-keterangan saksi yang diperiksa dalam tahap penyelidikan dimana penyidik juga memperoleh barang bukti berupa satu keeping *CD* yang berisikan *log files www.golkar.or.id* tanggal 8 Juli 2006 hingga 14 Juli 2006 dan *hard copy* akses *log* dari tanggal 8 Juli 2006 hingga 14 Juli 2006 sebanyak tujuh bundel.

Karena tindak pidana yang diselidiki adalah tindak pidana yang dilakukan dengan dan melibatkan komputer dan jaringan komunikasi, maka upaya pencarian tersangka bukan hal yang mudah. Masalah inilah yang menjadi beban berat bagi penyidik yang bertugas untuk mengusut kasus ini, dalam menentukan siapa pelaku yang merubah tampilan *website* Partai Golkar dan bahkan mencari serta menemukannya agar dapat mempertanggungjawabkan perbuatannya dimana hal ini memerlukan suatu teknik penyidikan khusus yang berbeda dari teknik penyidikan tindak pidana konvensional lainnya.

Dalam tahap proses penyelidikan yang dilakukan penyidik Unit V *IT & Cybercrime* dalam kasus ini, teknik penyelidikan yang dipergunakan belum terlalu kelihatan perbedaannya, karena perbedaan tersebut baru benar-benar muncul pada tahap penyidikan selanjutnya, dimana penyidik ditugaskan untuk melakukan penyidikan tindak pidana dengan target mencari dan menemukan

tersangka selanjutnya menindaknya sesuai dengan ketentuan yang berlaku.

4.2.3.2 Tahap Kedua: Penindakan dan Pemeriksaan

Dalam tahap kedua penyidikan, penyidik Unit V *IT & Cybercrime* meningkatkan atau melanjutkan upaya penyelidikan ke upaya penindakan dan pemeriksaan. Dalam hukum acara pidana, proses ini merupakan suatu tindakan penyidikan karena di dalam tahap ini penyidik dengan kewenangan yang dimiliki berdasarkan Pasal 7 KUHAP dapat melakukan beberapa upaya paksa meliputi: pemanggilan dan pemeriksaan saksi, penyitaan, penangkapan, penahanan, penggeledahan dan pemeriksaan surat.

Hal yang pertama dilaksanakan setelah peningkatan status dari penyelidikan ke tahap penindakan dan pemeriksaan adalah diterbitkannya Surat Perintah Penyidikan No. Pol.: SP.Sidik/ 80/ VII/ 2006/ Dit II Eksus pada tanggal 17 Juli 2006 oleh Kanit V *IT & Cybercrime* Bareskrim Polri Komisaris Besar Polisi (Kombes Pol) Petrus Reinhard Golose atas nama Direktur II Ekonomi dan Khusus, yang memerintahkan kepada (1) Gagas Nugraha, S.H., S.Ik., Ajun Komisaris Besar Polisi (AKBP; (2) Eddy Hartono, S.Ik., (AKBP; (3)Parmin, Komisaris Polisi (Kompol; (4) Zamri, S, Kom, (Kompol; (5) Dicky Patrianegara, S.H., S.Ik, M.Si, (Kompol; (6) Surawan, S.Ik, (Kompol) ; (7) Lindriayani, S.H. Ajun Komisaris Polisi (AKP); (8) Arif Makhfudiarto, S.Ik., (AKP); (9) I K Budi Hendrawan, S.H., S.Ik, (AKP); (10) Alexander Sabar, S.Ik (AKP); (11) Didi Novi Rahmanto, (AKP); (12) Poibe Inten Nosa Lince, Inspektur Polisi I; (13) H. Budhi Sutrisno, S.H., M.H., Inspektur Polisi I; (14) Maryudi Salempang, S.T., Inspektur Polisi II untuk melakukan penyelidikan dan penyidikan terhadap tindak pidana di bidang telekomunikasi dan/atau perusakan terhadap tampilan *website* Partai Golkar (*deface*) atau turut serta atau memberikan kesempatan ataupun membantu sebagaimana dimaksud dalam Pasal 22 dan Pasal 50 Undang-Undang Telekomunikasi, Pasal 406 KUHP jo Pasal 55 jo Pasal 56 KUHP dan membuat rencana penyidikan serta melaporkan setiap perkembangan pelaksanaan penyidikan tindak pidana pada kesempatan pertama kepada pimpinan. Surat Perintah tersebut berlaku sejak tanggal diterbitkan.

Surat Perintah Penyidikan tersebut juga mengandung informasi penting yaitu target penyidikan ditetapkan untuk membuktikan suatu tindak pidana yang

tersangkanya masih belum dapat ditentukan. Hal ini menunjukkan adanya masalah yang tidak mudah yang harus dipecahkan oleh penyidik, dimana penyidik harus mencari dan menemukan tersangkanya yang masih belum diketahui pada saat dilaporkan oleh Partai Golkar.

Upaya yang dilakukan oleh penyidik berikutnya adalah melakukan pemeriksaan terhadap saksi-saksi seiring dengan pemeriksaan terhadap *hard disk server* Partai Golkar yang ada pada PT Web Master Network di PT Telkom Kandatel Jakarta Barat dan *hosting*nya dilaksanakan di Gedung *Cyber* dengan dibantu oleh fungsi laboratorium forensik komputer Unit V *IT & Cybercrime*. Pemeriksaan tersebut dilaksanakan pada tanggal 18 Juli 2006 dimana dalam *hard disk* terdapat *log files*.[134] *Log files* tersebut dapat digunakan untuk menentukan kapan seseorang mengakses (*log in*) dan darimana dia mengakses (*log in*). *Server log* telah merekam *IP Addresses* yang digunakan dengan waktu yang spesifik, sebagai contoh ketika seseorang mengirim sebuah *email*, tindakan ini terekam dalam *server file email* yang digunakannya. Kemudian pada saat seseorang mengakses *web pages*, *IP Addresses* dari komputer yang digunakan juga tercatat dalam *web server access log*.

Hal tersebut merupakan sesuatu yang tidak penting dimana sebagian besar *log files* berisikan informasi mengenai lalu-lintas yang masuk dan bukan mengenai lalu lintas yang keluar. Hal ini menyebabkan relatif mudah untuk menentukan apa yang telah dilakukan seseorang terhadap komputer, tetapi membuat itu menjadi sulit untuk menentukan spesifik komputer yang digunakan pelaku. Dalam perkembangannya, beberapa sistem administrators telah meng-*isnstall* perangkat lunak IP dalam komputernya untuk menciptakan *logs* dari semua TCP/IP baik yang masuk maupun keluar Eoghan Casey (2000: 133).

Dari uraian di atas dapat kita lihat betapa pentingnya *log files* dalam pengungkapan tindak pidana *hacking website* Partai Golkar karena *log files* menyimpan informasi yang berisi mengenai siapa yang mengakses (*log in*), dari mana serta *IP Address* yang digunakan dan kapan *log in* dilakukan. Informasi dan data-data digital tersebut dapat dijadikan barang bukti materiil dalam mengungkap

---

[134] *Log files* merupakan wadah sejumlah informasi yang besar mengenai seorang pengguna komputer dan dapat dijadikan alat bukti digital.

suatu tindak pidana.

Tindakan pertama yang dilakukan oleh penyidik adalah melakukan tindakan *imaging hard disc server website* Partai Golkar sebagai bagian dalam forensik atas bukti digital dalam suatu kejahatan komputer dengan dibantu oleh tim laboratorium forensik komputer berdasarkan permintaan yang disampaikan oleh penyidik. Teknik ini diketahui berdasarkan pengalaman dan pengetahuan penyidik atas penanganan barang bukti yang berkaitan dengan kejahatan komputer, untuk menghindari kerusakan atas bukti digital dan agar penyidik dapat memeriksa lebih lanjut bukti tersebut.

Setelah proses *imaging* tersebut dilakukan, penyidik pada tanggal 19 Juli 2006 mengadakan pemeriksaan terhadap saksi Riyanto Jatmiko dari PT Master Web Network sebagai pihak penyedia jasa *hosting website* Partai Golkar. Saksi Riyanto Jatmiko adalah Manajer Operasional Umum PT Master Web Network yang mempunyai tugas memonitor pekerjaan dari bagian-bagian lain, yaitu bagian *Billing*, bagian *Technical Support*, bagian *Marketing*, bagian *Research and Development* dan bagian *Web Development*. Selain memonitor, saksi juga membantu mencarikan solusi apabila ada permasalahan di lingkup operasional, misalnya mengatur jadwal *shift*, *hosting*, dan berhubungan dengan klien.

Saksi mengetahui bahwa *website* Partai Golkar adalah salah satu klien atau pelanggan dari layanan *hosting* PT Master Web Network, Partai Golkar mendaftarkan secara *online* melalui *website www.masterwebnet.com* atas nama Daulat Firman Abraham sejak tanggal 8 September 2005, pada saat itu nama *domain* yang digunakan atas *account* tersebut adalah *www.partai-golkar.or.id*.

Nama *domain* tersebut kemudian diubah oleh Daulat Firman Abraham pada tanggal 23 November 2005 dengan mengirimkan permohonan penggantian nama *domain* melalui *email* yang ditujukan pada *billing@masterwebnet.com* dari *email jakarta512@gmail.com* dan di tembuskan kepada *firman@intermatik.co.id* tentang penggantian nama *domain* dari *partai-golkar.or.id* menjadi *golkar.or.id*. *Website www.golkar.or.id* hanya menjadi pelanggan atau *client* PT Master Web Network untuk fasilitas layanan *hosting* atau *hostmaster* saja, sehingga tanggung jawab berdasarkan peraturan dan persetujuan PT Master Web Network yang sudah disetujui oleh klien pada saat pendaftaran pertama adalah menyediakan

layanan fasilitas *website* dan *email* agar berfungsi dan dapat diakses. PT Master Web Network bukan pembuat maupun pengembang *website* tersebut serta tidak bertanggung jawab terhadap isi *website* dan gangguan yang terjadi karena *hacker* atau *cracker* seperti terhapusnya data, *cracking, deface* atau hal-hal lain yang timbul akibat kelalaian klien sesuai dengan isi kontrak. Lebih lanjut saksi Riyanto menyampaikan bahwa ia mengetahui adanya serangan perusakan tampilan (*deface*) dan sistem manajemen konten berdasarkan laporan melalui layanan *chating* Yahoo Messenger *pt mwn supp@yahoo.com* dari *yahoo.id*: *fusionz512@yahoo.com* atas nama Firman yang diterima oleh Jimmy Zakaria *technical support* pada tanggal 9 Juli 2006 sekitar pukul 15.00 WIB dan melaporkan adanya *deface* terhadap *website* Partai Golkar.

Atas serangan yang terjadi tersebut, PT Master Web Network sebagai *hostmaster* mengusulkan kepada klien untuk me-*restore* (dikembalikan) ke bentuk semula dari *back up server* dan setelah disetujui maka akan melakukan *restore* serta menyarankan untuk melakukan *up date* pada aplikasi yang digunakan untuk membuat *website*, karena aplikasi *website* tersebut menggunakan *software mambo open source versi 4.5.2* sedangkan *up date* terbaru dari versi aplikasi tersebut adalah *mambo versi 4.6*. Untuk dapat membuktikan bahwa telah terjadi serangan terhadap *website* tersebut dapat dilihat dari *log files* yang ada dalam aplikasi *website*, sedangkan server dan *log files* dari *website* Partai Golkar merupakan milik PT Web Master Network yang diletakkan di pusat data Telkom Slipi.

Dari pemeriksaan terhadap Riyanto Jatmiko, penyidik menyita barang bukti berupa 1 (satu) buah *Hard Disc* merk "SEAGATE", tipe Barakuda 7200.9, kapasitas 200 GB, serial number : 4ND32XQV, ST3250824A, P/N: 98D33-303. Atas penyitaan tersebut diterbitkan Surat Tanda Penerimaan Barang Bukti No.Pol.: STP/07/ VII/ 2006/ Dit II Eksus serta dibuatkan Berita Acara Penyitaan tertanggal 18 Juli 2006. Selanjutnya dilakukan pemeriksaan oleh tim laboratorium forensik komputer atas *log files* yang ada dalam *hard disc server website* Partai Golkar tersebut. Dari hasil pemeriksaan penyidik menemukan petunjuk kapan dan darimana penyerangan terhadap *website* Partai Golkar. Dari petunjuk yang diperoleh, penyidik mengetahui bahwa penyerangan diduga dari beberapa kota di Indonesia seperti Bandung, Jakarta, Medan, Bekasi dan Batam, bahkan

penyerangan juga diduga dari beberapa negara seperti Malaysia, Turki, Amerika Serikat, Brazil, dan Rumania. Tetapi berdasarkan hasil yang ditemukan, penyidik mencurigai tiga tempat penyerangan, yaitu di Jakarta, Bandung dan Batam. Dari tiga kota tersebut telah terjadi akses ataupun penyerangan terhadap *website* Partai Golkar lebih banyak dibandingkan dengan kota lain.

Penyidikan dimulai dari Bandung dan Jakarta dengan dibantu oleh pihak *ISP* tetapi tidak menemukan pelaku dengan *IP Address* yang dicurigai digunakan *hacker website* Partai Golkar sehingga alternatif terakhir adalah Batam. Pada tanggal 2 Agustus 2006 tim penyidik melakukan rangkaian pemeriksaan dan pengumpulan barang bukti di Batam dimulai dari pemeriksaan terhadap saksi-saksi dari *ISP*. Pemilik *IP Address* yang dicurigai adalah PT Inforsys Indonesia yang mempunyai anak perusahaan PT Primera Telekomunikasi dengan bidang usaha internet dan memiliki *IP Address* yang sama dengan yang ditemukan dalam *history log files* dalam *hard disk server website* Partai Golkar yaitu *IP Address* 222.124.136.81.

Saksi yang diperiksa dari pihak *ISP* PT Inforsys Indonesia adalah Gani selaku Direktur Utama dan Irwan, S.Kom yang menjabat sebagai *Technical Support*. Sebagai Direktur Utama, Gani mempunyai tugas dan tanggung jawab menjalankan perusahaan dan menentukan arah masa depan perusahaan yang bergerak di bidang bisnis *software* seperti *accounting, payroll, manufacturing system*. Sedangkan Irwan bertugas membantu pemasangan jaringan internet dari pelanggan yang mendaftar. Selain itu, Irwan juga bertugas untuk memperbaiki kerusakan secara teknik, bertanggung jawab terhadap kelancaran jaringan internet dan bertanggung jawab langsung terhadap direktur. Sebagai sarana promosi, perusahaan memiliki *website* yaitu *www.inforsys.co.id*.

Para saksi mengetahui pemilik *IP Address* yang ditunjukkan oleh penyidik, yaitu PT Inforsys Indonesia. *IP Address* tersebut merupakan sebagian dari *IP Address* yang dimiliki dan didapatkan perusahaan dari PT Telkom Indonesia (Riau Kepulauan), sebagai mitra bisnis penyelenggaraan *ADSL* (*Asymmetric Digital Subscriber Line*)[135]. *Range IP Address* yang dimiliki adalah 128 *IP*

[135]Suatu teknologi yang mampu memberdayakan saluran telepon menjadi saluran digital *high speed* yang dapat melewatkan sinyal suara dan data secara simultan tanpa saling

Address, yaitu 222.124.136.0 – 222.124.136.127. *IP Address* tersebut dimiliki sejak November 2005 dengan jenis *IP Address Static Public*, artinya *IP Address* tersebut tetap dan tidak berubah serta dikenal di jaringan internet Global. Sejak tanggal 3 Agustus 2003 sampai dengan tanggal 1 Maret 2006, *IP Address* 222.124.136.81 digunakan oleh PT Giken Precision yang beralamat di Kawasan Industri Sekupang. Namun setelah itu, *IP Address* 222.124.136.81 secara resmi tidak digunakan oleh siapapun karena pelanggan tersebut tidak memakai jasa internet dari PT INFORSYS INDONESIA sejak tanggal 1 Maret 2006. Akan tetapi *IP Address* 222.124.136.81 sifatnya tidak ditutup secara resmi sehingga sangat mungkin dapat digunakan oleh pihak lain untuk mengakses dengan menggunakan *IP Address* tersebut.

Dari hasil pemeriksaan dan bantuan pihak *ISP*, diketahui bahwa *IP Address* disewakan oleh *ISP* ke Warnet Barelang yang terletak di Jalan Raden Patah No. 81 Batam, dimana *IP Address* tersebut sebenarnya tidak aktif namun dapat digunakan pihak lain karena sifatnya tidak ditutup secara resmi, pihak lain tersebut biasanya adalah pelanggan *ISP* PT Inforsys.

Di samping pencarian terhadap pengguna *IP Address* yang dicurigai, di Batam penyidik juga melakukan *virtual undercover* atas *nickname* yang ditemukan dari data *log files*. Penyidik dengan dibantu oleh komunitas *hacker* yang ada di Batam melakukan penyamaran dan berupaya melalui *chatting email* dengan *nick name* yang diketahui *IP Address*-nya. Melalui *chatting*, terdapat seorang *hacker* yang mengakui dialah yang meng-*hacking website* Partai Golkar. Dari penyidikan diketahui pelakunya adalah Iqra Syafaat alias Nogra alias *singapore_bm@yahoo.com*.

Dengan hasil yang didapat dari pemeriksaan saksi-saksi dari *ISP* dan pemetaan pengguna *IP Address* 222.124.136.81 serta informasi dari komunitas *hacker* tersebut, penyidik menuju ke Warnet Barelang dan penyidik kemudian mendapati tersangka Iqra Syafaat berada di sana dan segera melakukan penangkapan dengan Surat Perintah Penangkapan No. Pol: Sprin-Kap/ 100/ VIII/ 2006/ Dit Eksus tertanggal 2 Agustus 2006 yang ditandatangani penyidik atas

---

mengganggu.

nama Direktur II Ekonomi dan Khusus Kanit V *IT & Cybercrime*. Atas penangkapan tersebut dibuatkan Berita Acara Penangkapan tanggal 2 Agustus 2006 pada pukul 21.00 WIB dimana tersangka ditangkap berdasarkan bukti permulaan yang cukup, dengan tuduhan tindak pidana perusakan dan penyalahgunaan jaringan informasi sebagaimana dimaksud dalam perkara pidana Pasal 50 Undang-Undang Telekomunikasi subsider Pasal 406 KUHP.

Penangkapan terhadap tersangka diiringi dengan penggeledahan rumah tinggal Daniel H yang merupakan orang tua tersangka, beralamat di Batu Merah RT.15 RW.04 Batu Ampar Batam-Riau. Penggeledahan tersebut dilakukan pada tanggal 3 Agustus 2006 terhadap tempat yang diduga merupakan tempat kejadian perkara atau tempat persembunyian tersangka atau tempat disembunyikan barang – barang bukti, baik yang ada kaitannya langsung maupun yang tidak langsung dengan perkara pidana sebagaimana disangkakan kepada tersangka. Dalam melakukan proses penggeledahan, penyidik terlebih dahulu menunjukkan Surat Perintah Penggeledahan Rumah No.Pol.: SP.DAH/ 50/ VIII/ 2006/ Dit II Eksus tertanggal 2 Agustus 2006.

Penggeledahan tersebut juga diiringi dengan penyitaan barang-barang bukti berupa 1 (satu) unit laptop warna biru merek "*Twinhead*", *serial number*: SY1030001656 dengan model No: A5010 dan 1 (satu) *CPU* rakitan warna silver. Atas penyitaan tersebut, diterbitkan Surat Tanda Penerimaan Barang Bukti No. Pol.: STP/ 03/ VII/ 2006/ Dit II Eksus dan Berita Acara Penyitaan tertanggal 3 Agustus 2006.

Setelah penangkapan tersangka Iqra Syafaat dan penggeledahan kediaman rumah tinggal Daniel H yang diikuti dengan penyitaan, penyidik melakukan pemeriksaan terhadap tersangka pada tanggal 3 Agustus 2006. Hal ini untuk menentukan apakah tersangka dapat dikenakan tindakan atau upaya paksa selanjutnya, yaitu penahanan. Dari pemeriksaan tersangka, tersangka mengakui telah melakukan *deface* atau perusakan tampilan *website* partai Golkar. Tindakan tersebut dilakukan hanya untuk menguji sistem keamanan *website* Partai Golkar. Tersangka pada awalnya hanya menggunakan *website* sebagai *proxy* tetapi tidak berhasil. *Deface* tersebut dilakukan pada tanggal 9 Juli 2006 pukul 01.00 WIB dengan menggunakan *IP Address* 222.124.136.81 dan pada tanggal 10 Juli 2006

pukul 13.00 WIB dengan *IP Address* 222.124.136.101 dari Warnet Barelang di Jalan Raden Fatah No. 81, Batam dengan menggunakan komputer milik warnet tersebut.

Tersangka melakukan *deface* dengan cara memanfaatkan *bugs mambo* yang di dapat dari milworm.com dan mencari target di *google.co.id* dan kebetulan tersangka mendapatkan *www.golkar.or.id*. Kemudian tersangka masuk ke *server*nya dan meng-*upload file backdoor mod_access.php* ke *folder http://www.golkar.or.id/modules/mod_access.php*. Setelah berhasil masuk, tersangka melakukan *deface* mengganti halaman muka dengan foto wanita seksi yang sedang memegang buah dada. Foto tersebut didapatkan dari *search engine google*. Menurut pengakuan tersangka, foto wanita tersebut cantik dan seksi, di atas foto tersebut terdapat tulisan "Bersatu Untuk Malu" yang diplesetkan dari kata "Bersatu Untuk Maju" sebagai semboyan dari Partai Golkar, seperti tampilan di bawah ini:

Gambar 4.7
***Website* Partai Golkar Diubah Foto Wanita Seksi**

Tampilan *website* Partai Golkar setelah diubah tampilannya dengan foto wanita seksi
(Sumber: Berita Acara Pemeriksaan)

Setelah itu, *website* Partai Golkar berganti tampilan muka dengan tulisan *maintenance* lalu mengganti kembali *file index.php* dengan gambar gorila dengan tulisan "Bersatu Untuk Malu". Foto gorila di-*link* dari situs yg dicari dari *www.google.com*. Penggantian halaman depan *website* Partai Golkar dengan gambar gorila putih karena tersangka menganggap lucu, gorila tersebut sedang

nyengir, seperti tampilan di bawah ini.

Gambar 4.8
***Website* Partai Golkar Diubah Foto Gorila**

Website Partai Golkar setelah diubah tampilannya dengan foto gorila

(Sumber: Berita Acara Pemeriksaan)

Selain terhadap tersangka, pemeriksaan di Batam juga dilaksanakan terhadap saksi Muhammad Rafi, seorang teknisi Warnet. Muhammad Rafi menerangkan bahwa ia bekerja sebagai teknisi di Warnet Barelang sejak tahun 2004 dan bertanggung jawab terhadap kerusakan yang terjadi di warnet seperti lambatnya akses internet maupun perawatan terhadap perangkat komputer di Warnet. Ia bertanggung jawab kepada Linus Gusdar selaku pemilik Warnet.

Warnet Barelang menggunakan 2 (dua) *IP Address* yaitu 222.124.136.87 dan 222.124.136.81. *IP Address* diperoleh dari PT Pimera Telekomunikasi anak perusahaan PT Inforsys Indonesia dengan tujuan agar apabila salah satu dari *IP Address* tersebut mengalami gangguan atau tidak dapat koneksi internet, maka berpindah kepada *IP Address* yang kedua. *IP Address* yang kedua adalah 222.124.136.81 dan diperoleh tanpa seizin dari Primera. Saksi menjelaskan juga bahwa dari daftar laporan harian yang ditunjukkan oleh penyidik dan didapat dari Warnet Barelang, saksi mengetahui bahwa yang menggunakan *PC* 10 & 11 pada tanggal 7 Juli 2006 hingga tanggal 14 Juli 2006 adalah tersangka Iqra Syafaat. Iqra Syafaat merupakan salah satu langganan tetap di Warnet Barelang. Data

laporan harian tersebut sebagai berikut:

Tabel 4.3
Daftar Laporan Harian langganan tetap di Warnet Balerang

No.	Tanggal	Pukul	Durasi	*PC* No.	Pengguna
a.	7 Juli 2006	13: 27: 20	04: 51: 02	*PC* 11	Iqra Syafaat
b.	7 Juli 2006	21: 56: 18	03: 40: 24	*PC* 11	Iqra Syafaat
c.	8 Juli 2006	11: 36: 50	03: 59: 02	*PC* 10	Iqra Syafaat
d.	8 Juli 2006	19: 54: 18	06: 10: 25	*PC* 11	Iqra Syafaat
e.	9 Juli 2006	21: 29: 35	02: 17: 15	*PC* 11	Iqra Syafaat
f.	10 Juli 2006	12: 22: 05	00: 56: 25	*PC* 11	Iqra Syafaat
g.	11 Juli 2006	20: 15: 17	05: 43: 50	*PC* 11	Iqra Syafaat
h.	12 Juli 2006	13: 32: 44	03: 34: 13	*PC* 10	Iqra Syafaat
i.	12 Juli 2006	21: 39: 16	03: 17: 17	*PC* 10	Iqra Syafaat
j.	13 Juli 2006	13: 33: 32	06: 11: 39	*PC* 11	Iqra Syafaat
k.	14 Juli 2006	08: 27: 24	02: 18: 20	*PC* 10	Iqra Syafaat
l.	14 Juli 2006	16: 43: 40	01: 35: 29	*PC* 11	Iqra Syafaat

(Sumber: Berita Acara Pemeriksaan)

Dari tabel di atas, menjelaskan bahwa Iqra Syafaat adalah salah satu pelanggan tetap warnet Balerang dan pada tanggal 7 Juli 2006 hingga tanggal 14 Juli 2006 Iqra Syafaat telah menggunakan fasilitas internet di warnet balerang dengan lama tiap pemakaian antara dua sampai 6 jam.

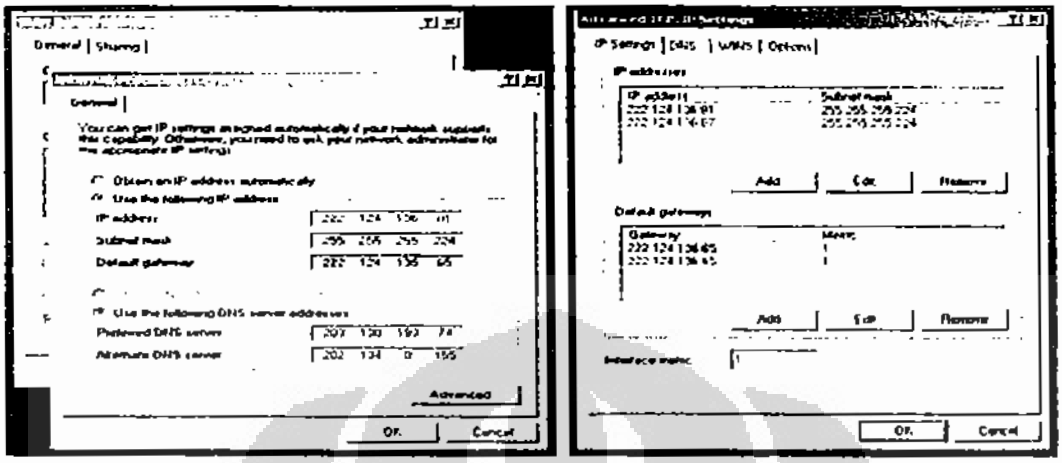
Saksi juga menjelaskan tampilan *setting IP Address* pada komputer operator (*server*) dimana saksi menunjukkan kepada penyidik mengenai *IP Address* untuk koneksi ke internet dengan menggunakan *IP Address* 222.124.136.87 dan 222.124.136.81. dengan menggunakan tampilan berikut ini.

Gambar 4.9
IP* Komputer Operator/*Server

Tampilan *setting IP Address* pada komputer operator (*server*)

(Sumber: Berita Acara Pemeriksaan)

Gambar 4.10
Setting IP* Komputer Operator/*Server

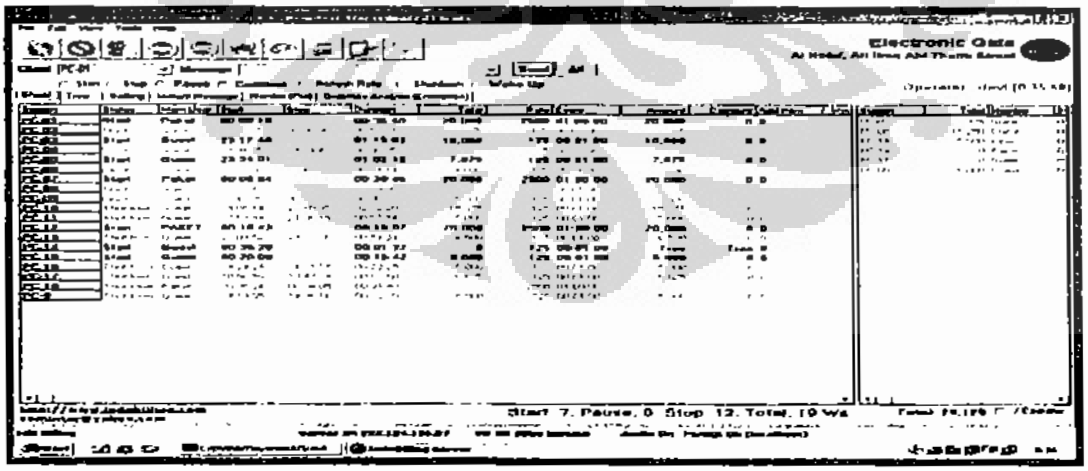


Tampilan *setting IP* Komputer Operator (*server*)

(Sumber: Berita Acara Pemeriksaan)

Selain tampilan tersebut, saksi menjelaskan tampilan daftar pemakai (*user*) di Warnet Barelang pada tanggal 3 Agustus 2006 pukul 00:35:50 WIB dan tampilan *IP Address* pada *PC* 11 untuk koneksi ke internet di Warnet Barelang Raden Patah yang ditunjukkan oleh penyidik, adapun tampilan-tampilan tersebut sebagai berikut:

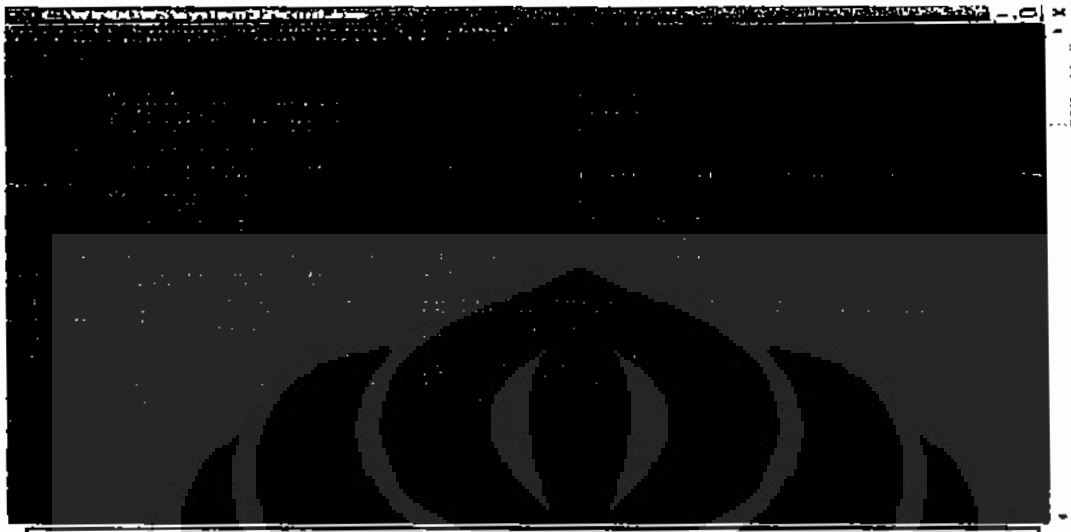
Gambar 4.11
Tampilan *Billing* tanggal 3 Agustus 2006



Tampilan daftar pemakai (*user*) di Warnet Barelang pada tanggal 3 Agustus 2006 pukul 00:35:50 WIB

(Sumber: Berita Acara Pemeriksaan)

Gambar 4.12
Tampilan *setting IP Address* pada *PC* 11



Tampilan *IP Address* pada *PC* 11 untuk koneksi ke internet di Warnet Barelang Raden Patah

(Sumber: Berita Acara Pemeriksaan)

Bahwa untuk kepentingan penyidikan dan berdasarkan hasil pemeriksaan yang telah dilakukan sehingga diperoleh bukti yang cukup, tersangka dapat dikenakan salah satu upaya paksa, yaitu penahanan[136].

Tujuan penahanan sebagaimana disebutkan dalam Pasal 20 KUHAP, terdapat tiga alasan yaitu untuk kepentingan penyidikan, penuntut umum dan kepentingan peradilan. Untuk kepentingan penyidikan, penyidik atau penyidik pembantu atas perintah pihak yang berwenang melakukan penahanan. Mengenai ukuran kepentingan penyidikan pada dasarnya ditentukan oleh kenyataan keperluan pemeriksaan penyidikan itu sendiri secara obyektif yaitu tergantung pada kebutuhan tingkat upaya penyidik untuk menyelesaikan fungsi pemeriksaan penyidikan yang tuntas dan sempurna sehingga penyidikan benar-benar mencapai hasil pemeriksaan yang akan diteruskan kepada penuntut umum, untuk

---

[136] Pengertian penahanan dalam KUHAP Pasal 1 butir 2 KUHAP adalah: penempatan tersangka atau terdakwa di tempat tertentu oleh penyidik atau penuntut umum atau hakim dengan penetapannya, dalam hal serta menurut cara yang diatur dalam undang-undang ini. Untuk melakukan penahanan terhadap tersangka, penyidik harus mempunyai landasan dasar yang kuat untuk melakukan penahanan terhadap tersangka.

dipergunakan sebagai dasar pemeriksaan di depan sidang pengadilan. Berarti jika pemeriksaan penyidikan sudah cukup, penahanan tidak diperlukan lagi, kecuali ada alasan lain untuk tetap menahan tersangka (Pasal 20 ayat (1)).

Sedangkan penahanan yang dilakukan oleh penuntut umum, bertujuan untuk kepentingan dalam tahap penuntutan (Pasal 20 ayat (2)) dan penahanan yang dilakukan oleh peradilan, dimaksud untuk kepentingan pemeriksaan di pengadilan. Hakim berwenang melakukan penahanan dengan penetapan yang didasarkan kepada perlu tidaknya penahanan dilakukan sesuai dengan kepentingan pemeriksaan di sidang pengadilan (Pasal 20 ayat (3)).

Lebih lanjut Yahya Harahap (2006:165) menjelaskan landasan penahanan meliputi dasar hukum, keadaan, serta syarat-syarat yang memberi kemungkinan melakukan tindakan penahanan. Kesemua unsur tersebut saling berkaitan dan mendukung satu sama lain. Hal ini menyebabkan jika salah satu unsur tidak ada, tindakan penahanan kurang memenuhi asas legalitas meskipun tidak sampai dikualifikasi sebagai tindakan yang tidak sah (*illegal*). Misalnya yang terpenuhi hanya unsur obyektif, tetapi tidak didukung unsur keperluan atau yang disebut unsur subyektif serta tidak dikuatkan syarat-syarat yang ditentukan undang-undang, penahanan yang seperti itu lebih bernuansa "kezaliman", dan kurang berdimensi relevansi dan urgensi. Adapun unsur yang menjadi landasan dasar penahanan, Yahya Harahap (2006:166) membagi dalam 3 landasan dasar, yaitu: landasan dasar atau unsur yuridis sebagaimana telah disebutkan dalam Pasal 21 ayat (4) KUHAP[137], landasan unsur keadaan kekhawatiran[138] dan dipenuhinya

---

[137] Penahanan tersebut hanya dapat dikenakan terhadap tersangka atau terdakwa yang melakukan tindak pidana dan/atau percobaan maupun pemberian bantuan dalam tindak pidana sebagai berikut:

a. "Yang diancam dengan pidana penjara "lima tahun atau lebih" dan;
b. Penahanan juga dapat dikenakan terhadap pelaku tindak pidana yang disebut pada pasal KUHP dan Undang-undang Pidana khusus di bawah ini, sekalipun ancaman hukumannya kurang dari lima tahun. Yang termasuk dalam hal ini adalah:
   (a). Yang terdapat dalam pasal-pasal KUHP: Pasal 282 ayat (30, Pasal 296, Pasal 335 ayat (1), Pasal 353 ayat (1), Pasal 372, Pasal 378, Pasal 379 a, Pasal 453, Pasal 454, Pasal 455, Pasal 459, Pasal 480, dan Pasal 506;
   (b). Kelompok kedua ialah pasal-pasal yang berasal dari tindak Undang-Undang Tindak Pidana Khusus:
      - Pasal 25 dan 26 *Rechten Ordonantie* (pelanggaran terhadap ordonansi Bea dan Cukai, terakhir diubah dengan St. Tahun 1931 Nomor 471);
      - Pasal 1, Pasal 2, dan Pasal 4 Undang-Undang Tindak Pidana Imigrasi (Undang-undang Darurat Nomor 8 Tahun 1855);

syarat Pasal 21 ayat (1) KUHAP[139].

Apabila dikaitkan dengan kasus tindak pidana *hacking website* Partai Golkar, penyidik telah melakukan penahanan terhadap tersangka. Tersangka ditempatkan di Rumah Tahanan Negara di Badan Reserse Kriminal Polri Jl. Trunojoyo No. 3, Kebayoran Baru, Jakarta Selatan selama 20 hari terhitung mulai tanggal 3 Agustus 2006 sampai dengan 22 Agustus 2006. Tindakan penahanan tersebut dapat dikaitkan dengan syarat-syarat penahanan sehingga dapat diketahui apakah penahanan tersebut telah memenuhi tujuan maupun landasan dasar penahanan sebagaimana penjelasan diatas. Hal ini dapat dianalisa dimulai dari tindakan penyidikan yang telah dilakukan serta dari pertimbangan dan dasar dikeluarkannya Surat Perintah Penahanan No. Pol.: SP. Han/49/VII/2006/Dit II tertanggal 3 Agustus 2006.

Dalam diktum pertimbangannya, surat penahanan tersebut dikeluarkan untuk kepentingan penyidikan dan berdasarkan hasil pemeriksaan diperoleh bukti yang cukup, tersangka diduga keras melakukan tindak pidana yang dapat dikenakan penahanan, tersangka dikhawatirkan akan melarikan diri, merusak atau menghilangkan barang bukti dan atau mengulangi tindak pidana. Berdasarkan alasan tersebut maka polisi merasa perlu mengeluarkan Surat Perintah Penahanan. Dasar dari pertimbangan tersebut terdiri dari tiga dasar yaitu dasar pertama: Pasal 17 ayat (1) huruf 4, Pasal 11, Pasal 20, Pasal 1, Pasal 22, Pasal 24 ayat (1) KUHAP; dasar kedua: Undang-Undang Kepolisian dan dasar Ketiga: Surat Perintah Penangkapan No. Pol. : SP.Kap/100/VIII/2006/Dit II Eksus tanggal 2 Agustus 2006.

Berdasarkan isi dari surat penahanan tersebut, orang yang akan ditahan adalah Iqra Syafaat, jenis kelamin laki-laki, tempat/tanggal lahir: Batam, 21 Juli

---

- Pasal 36 ayat (7), Pasal 41, Pasal 42, Pasal 43, Pasal 47, dan Pasal 48 Undang-undang Nomor 9 Tahun 1976 Tentang Narkotika (LN Tahun 1976 Nomor 37 TLN Nomor 3086)."

[138] Landasan Unsur Keadaan Kekhawatiran menitikberatkan kepada keadaan atau keperluan penahanan ditinjau dari segi subyektivitas si tersangka atau terdakwa, yang dinilai secara subjektif oleh penegak hukum yang bersangkutan.

[139]Keadaan yang menimbulkan kekhawatirkan, yaitu: tersangka atau terdakwa akan melarikan diri; merusak atau menghilangkan barang bukti; atau dikhawatirkan akan mengulangi tindak pidana.

1979, agama Islam, pekerjaan pegawai swasta, kewarganegaraan Indonesia, alamat, Batu Merah RT 15 RW 04 Batu Merah Batu Ampar dan Bukit Timur RT. 04/06 No. 4 Tanjung Uma, Batam. Dasar alasan penahanan tersebut adalah karena diduga telah melakukan tindak pidana penyalahgunaan jaringan informasi dan perusakan sebagaimana dimaksud dalam Pasal 50 Undang-Undang Telekomunikasi dan Pasal 406 KUHP.

Dari pertimbangan dan dasar dikeluarkannya Surat Perintah Penahanan dapat dilihat bahwa penyidik mendasarkan penahanan terhadap tersangka dengan landasan dasar secara yuiridis (obyektif) maupun secara subyektif. Landasan Dasar secara obyektif adalah terlihat pada salah satu pasal yang disangkakan oleh penyidik pada tersangka dimana yang disangkakan adalah Pasal 22 huruf b[140] jo Pasal 50 Undang-Undang Telekomunikasi[141].

Dari Pasal tersebut nampak bahwa landasan dasar penyidik secara obyektif adalah ancaman hukuman selama 6 tahun. Hal ini berarti penahanan yang dilakukan penyidik terhadap tersangka telah memenuhi syarat-syarat obyektif karena ancaman pidana pada pasal yang dituduhkan kepada tersangka berupa hukuman selama 6 tahun.

Disamping landasan dasar secara obyektif penyidik juga mendasarkan pada alasan atau dasar secara subyektif. Hal ini dapat dilihat dari kehawatiran penyidik akan diri tersangka sebagaimana dilihat dari pertimbangan Surat Perintah Penahanan dimana tersangka dikhawatirkan akan melarikan diri, merusak atau menghilangkan barang bukti dan/atau mengulangi tindak pidana.

Landasan terakhir sebagaimana yang disampaikan Yahya Harahap (2000) adalah terpenuhinya unsur dalam Pasal 21 ayat (1) KUHAP, yaitu tersangka diduga keras sebagai pelaku dan dugaan keras itu didasarkan pada bukti yang cukup. Apabila dikaitkan dengan kasus tindak pidana *hacking website* Partai Golkar, unsur-unsur pada Pasal 21 ayat (1) KUHAP tersebut sudah terpenuhi sebagaimana dapat dilihat dari proses penyidikan yang telah dilakukan. Hal ini disebabkan alat-alat bukti yang berupa keterangan saksi mengarah kepada

---

[140]"Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jasa telekomunikasi." Pasal 22 huruf b Undang-Undang Telekomunikasi.

[141]"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah)

tersangka terutama adanya alat bukti yang dapat digunakan di persidangan, yaitu keterangan tersangka yang mengakui perbuatannya dan keterangan saksi lainnya. Berdasarkan hal tersebut, tersangka dilakukan penahanan terhitung mulai tanggal 3 Agustus 2006 sampai dengan 22 Agustus 2006. Atas penahanan tersangka telah dibuatkan Berita Acara Penahanan pada tanggal yang sama.

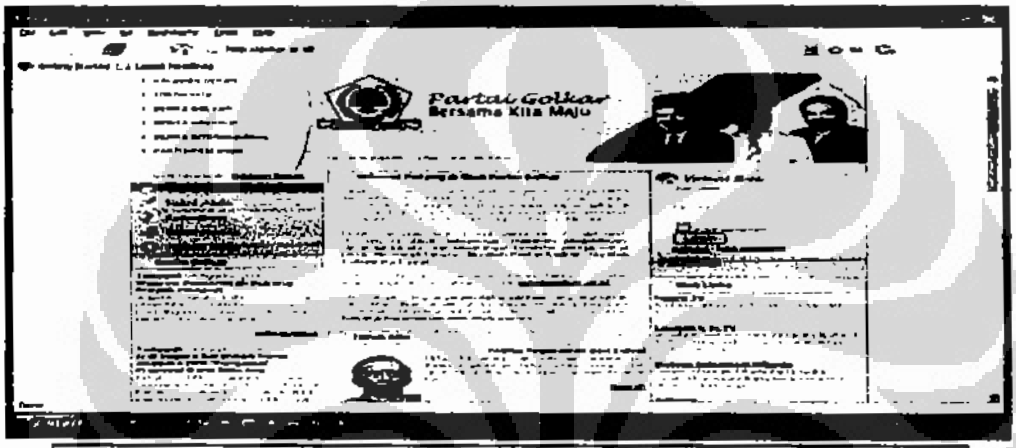
Setelah dilakukan pemeriksaan saksi dan diikuti dengan penyitaan barang bukti yang terkait dengan tindak pidana yang dilakukan oleh tersangka, Kanit V *IT & Cybercrime* pada tanggal 7 Agustus 2006 menerbitkan Surat Perintah Pemeriksaan Barang Bukti Digital No. Pol: SP.BBD/08/VIII/2006/ Dit II Eksus kepada AKBP Drs. Idam Wasiadi, S.H., S.Kom, MT selaku Pemeriksa Laboratorium Forensik Komputer atau Penyidik Madya untuk melaksanakan pemeriksaan terhadap barang bukti digital berkaitan dengan tindak pidana yang dilakukan oleh tersangka.

Pada tanggal 9 Agustus 2006 dilaksanakan Pemeriksaan Tambahan terhadap tersangka, yang menambahkan keterangan terdahulu dengan lebih rinci tentang kapan dan bagaimana tersangka memasuki sistem *website* Partai Golkar serta kapan dan bagaimana tersangka melakukan *deface* halaman muka (*home page*) *website* Partai Golkar.

Dari pemeriksaan tersebut, tersangka menjelaskan bahwa tersangka pertama kali memasuki *website* tersebut pada tanggal 8 Juli 2006, adapun cara yang dilakukan untuk memasuki sistem *website* adalah: (1). Mencari *bug* (kelemahan) baru di *website www.milworm.com* dan menemukan *bug* baru untuk melakukan *PHP Injection* pada aplikasi "MAMBO" yang biasa digunakan untuk membuat *website*; (2). Setelah menemukan *bug* tersebut tersangka melakukan *searching* dengan menggunakan *search engine* "Google" dengan kata kunci **allinurl:com_simpleboard** untuk menemukan *website* yang menggunakan modul *simpleboard* pada MAMBO. (3). Hasil dari *searching* tersebut ditemukan *website* Golkar yang menggunakan modul tersebut, kemudian tersangka mengklik *link* yang terdapat di *google* dan sebelum semua tampilan terbuka, pelaku menghentikan proses *loading* dengan mengklik *icon stop* pada *toolbar* kemudian mengganti *url* menjadi *www.golkar.or.id/components/com_simpleboard/file_upload.php?sbp=http://iahc*

.net/log/c; (4). Setelah dilakukan penggantian *url* tersebut, maka *server website* Golkar akan memproses *file http://iahc.net/log/c*, kemudian tersangka meng-*up load file back door* **mod_access.php** ke *folder www.golkar.or.id/modules/* sehingga tersangka dapat masuk ke *server* Partai Golkar kapanpun selama *file* akses tersebut masih ada; (5). Kemudian tersangka menutup jalan masuk dengan cara men-*deface file_upload.php* dengan gambar animasi dan tulisan "*hacked by Garong-Online*" sehingga orang lain tidak dapat masuk melalui *file_upload.php*.

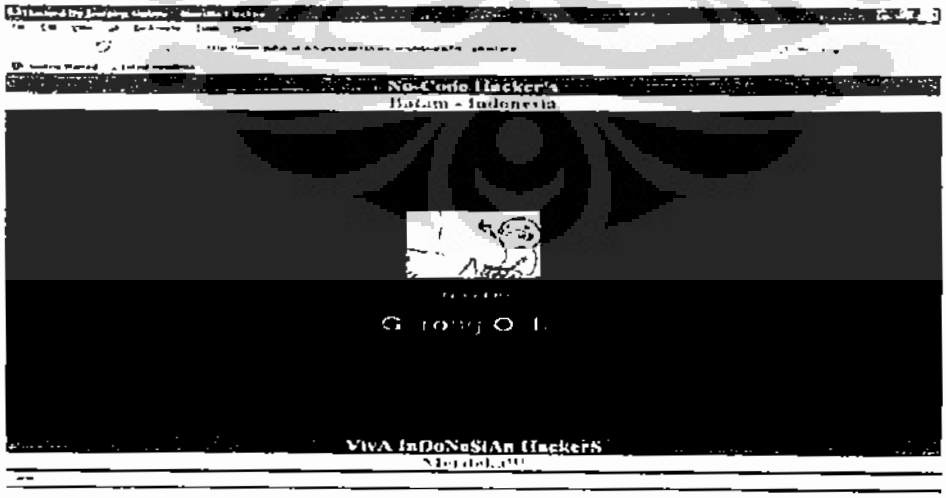
Gambar 4.13
Tampilan *website* Partai Golkar sebelum *deface*



Tampilan *website* Partai Golkar sebelum di-*deface* ke-1

(Sumber: Berita Acara Pemeriksaan)

Gambar 4.14
Tampilan *website* Partai Golkar setelah penutupan akses



Tampilan *website* Partai Golkar setelah tersangka menutup jalan masuk

(Sumber: Berita Acara Pemeriksaan)

Kemudian tersangka melakukan *deface website* Partai Golkar beberapa kali. Pada tanggal 9 Juli 2006, pukul 01.00 WIB untuk pertama kali pelaku mengganti tampilan muka *website* Partai Golkar, yaitu hanya pada wajah tokoh–tokoh partai Golkar dengan gambar gorila putih sedang tersenyum yang didapat dari www.google.com dan di-*link* ke situs di internet, *deface* tersebut dilakukan dari Warnet Barelang Jalan Raden Patah No. 81 Batam dengan menggunakan *IP Address* 222.124.136.81.

Gambar 4.15
Tampilan *website* Partai Golkar setelah *deface* pertama

Tampilan *website* Partai Golkar setelah di-*deface* pertama

(Sumber: Berita Acara Pemeriksaan)

Pada tanggal 10 Juli 2006, untuk kedua kalinya dari Warnet Barelang dengan menggunakan *IP Address* 222.124.136.101, pelaku kembali mengganti tampilan muka *website* Golkar dengan gambar wanita cantik seksi sedang memegang buah dada yang didapat dari www.google.com dan di-*link* ke suatu situs di internet dengan tulisan bersatu untuk malu.

Gambar 4.16
Tampilan *website* Partai Golkar setelah *deface* ke dua

Tampilan *website* Partai Golkar setelah di-*deface* ke dua

(Sumber: Berita Acara Pemeriksaan)

keterangan ahli menyangkut tindak pidana yang disangkakan kepada tersangka dengan dilampiri Surat Panggilan Pemeriksaan No. Pol.: SP/ 674/ IX/ 2006/ Dit II Eksus untuk ahli menghadap guna didengar keterangannya pada tanggal 11 September 2007.

Atas panggilan terhadap ahli tersebut, pada tanggal 11 September 2006 dilaksanakan pemeriksaan terhadap ahli yang menerangkan saat diperiksa dalam keadaan sehat jasmani dan rohani serta bersedia untuk diperiksa. Ahli menjelaskan bahwa proses *deface* dapat dilakukan dengan berbagai cara dengan teknis yang bermacam-macam.

Penyidik menunjukkan dan menyampaikan tindakan yang dilakukan tersangka kepada ahli dan diminta menjelaskan secara teknis tentang proses kegiatan yang dilakukan oleh tersangka atas hal tersebut. Ahli menjelaskan bahwa untuk melakukan *deface* seseorang harus mengetahui alamat situs (*website*) yang akan di-*deface*, selanjutnya orang tersebut harus mengetahui sistem operasi yang digunakan oleh situs tersebut serta mencari kelemahan dalam sitem operasi yang digunakan atau mencari *bug* dalam program aplikasi tersebut.

Kemudian untuk melakukan perubahan tampilan di *website* seseorang harus memiliki otoritas atau kewenangan, seperti sistem administrator atau orang lain yang diberikan kewenangan untuk itu. Dalam melakukan perubahan *website* biasanya diperlukan otorisasi seperti dibutuhkan *password* atau *passkey*, apabila seseorang yang tidak memiliki *password* atau bukan orang yang berwenang melakukan perubahan tampilan *website* tersebut, maka orang tersebut harus berupaya memanipulasi informasi bahwa dia seolah-olah berwenang melakukan perubahan tampilan di *website* tersebut.

Atas apa yang dilakukan oleh tersangka Iqra Syafaat terhadap *website* Partai Golkar, ahli menjelaskan bahwa tersangka tidak mempunyai hak untuk mengubah tampilan *website* Partai Golkar. Hal ini disebabkan yang berhak melakukan pengubahan tampilan *website* adalah orang yang memiliki *website*, atau orang yang diberikan wewenang untuk mengelola *website* tersebut. Perbuatan yang dilakukan oleh tersangka telah melanggar Pasal 50 jo Pasal 22 huruf b Undang-

Undang Telekomunikasi jo Pasal 406 KUHP[142].

Lebih lanjut saksi menjelaskan tentang apa yang dimaksud dengan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jasa telekomunikasi adalah perbuatan seseorang yang tanpa kewenangannya melakukan suatu tindakan atau biasanya disebut akses di dalam telekomunikasi tanpa adanya izin atau otoritas dari orang yang memiliki kewenangan atau institusi yang memiliki jasa telekomunikasi tersebut sehingga perbuatan yang dilakukannya merupakan perbuatan yang ilegal. Seseorang dilarang melakukan perbuatan manipulasi akses ke jasa telekomunikasi dimana tindakan tersebut adalah tindakan yang seolah-olah bahwa orang tersebut memiliki wewenang atau otoritas untuk melakukan atau mengakses ke jasa telekomunikasi atau mengakses ke jasa telekomunikasi.

Jasa telekomunikasi berdasarkan Pasal 14 ayat (1) huruf c Peraturan Pemerintah No. 52 Tahun 2000 Tentang Penyelenggaran Telekomunikasi adalah jasa telekomunikasi multimedia. Jasa telekomunikasi multimedia penyelenggaraannya meliputi pelayanan berbasis teknologi informasi termasuk di dalamnya antara lain penyelenggaraan jasa *VoIP*, internet dan intranet.

4.2.3.3 Tahap Ketiga: Penyelesaian dan Penyerahan Berkas Perkara

Setelah melaksanakan seluruh proses penyelidikan dan pemeriksaan serta penindakan yang diperlukan oleh tim penyidik dalam menangani kasus ini, pada tanggal 11 September 2006 penyidik mulai melakukan tahapan terakhir dari penyidikan, yaitu penyelesaian dan penyerahan berkas perkara yang dalam kasus tindak pidana *hacking website* Partai Golkar yang meliputi: pembuatan Berita Acara Pendapat/resume; penyusunan isi berkas perkara; pemberkasan; dan penyerahan berkas perkara.

Sebagaimana hal tersebut, penyidik telah menyusun berkas Berita Acara Pendapat (*resume*) atas hasil pemeriksaan saksi-saksi, keterangan-keterangan dan pengumpulan barang bukti selama proses penyelidikan dan penyidikan, dengan isi dan susunan berupa dasar penyelidikan dan penyidikan perkara dan fakta-fakta

---

[142]"Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah" (Moeljatno, 2001: 146)

yang diperoleh meliputi: TKP, acara pemanggilan, penangkapan, penggeledahan, penyitaan penahanan, keterangan saksi-saksi, keterangan ahli, keterangan tersangka dan barang bukti.

Tempat Kejadian Perkara berada di Kantor Sekretariat Partai Golkar Jln. Anggrek Nelli Murni Slipi Jakarta Barat 11480 tidak dilakukan penanganan olah TKP. Pemanggilan terhadap saksi Zulhendri Hasan, S.H., M.H, Daulat Firman Abraham, Riyanto Jatmiko, Fayakhun Andriadi, Gani, Irwan S.Kom, Agus Haryanto alias Hantu, Muhammad Rafi dan ahli Freddy Harris, SH, LLM, ACCS untuk dimintai keterangannya. Selanjutnya atas tindakan tersebut telah dibuatkan Berita Acara Pemeriksaan Saksi dan atau laporan polisi.

Upaya paksa berupa penangkapan, penahanan terhadap tersangka yang bernama Iqra Syafaat, penggeledahan rumah tersangka dan penyitaan terhadap barang-barang yang berkaitan dengan peristiwa pidana telah dilakukan oleh penyidik. Selanjutnya atas tindakan tersebut di atas telah dibuatkan berita acara penangkapan, penahanan, penggeledahan tersangka dan penyitaan terhadap barang-barang yang berkaitan dengan peristiwa pidana.

Selanjutnya berita acara pendapat tersebut kemudian disusun dalam berkas perkara disertai dengan isi berkas-berkas lainnya yang susunan seluruhnya meliputi Sampul Berkas Perkara No. Pol.: BP/53/IX/2006/Dit II Eksus, atas Perkara "Tindak Pidana Perbuatan Tanpa Hak, Tidak Sah atau Memanipulasi Akses ke Jasa Telekomunikasi Subsider Perusakan Terhadap *website* Golkar (*www.golkar.or.id*) sebagaimana dimaksud dalam Pasal 22 huruf b jo Pasal 50 Undang-Undang Telekomunikasi *subsider* Pasal 406 KUHP jo Pasal 64 ayat (1); Daftar Isi Berkas Perkara yang terdiri dari: Sampul berkas perkara, Daftar Isi Berkas Perkara resume, Laporan Polisi No. Pol.: LP/232/VII/2006/Siaga-II tanggal 17 Juli 2006, Surat Perintah Tugas No. Pol.: SP. Gas/145/VII/2006/Dit II Eksus, tanggal 17 Juli 2006, Surat Perintah Penyidikan No. Pol.: SP. Sidik/80/VII/2006/Dit II Eksus, tanggal 17 Juli 2006, Surat Pemberitahuan Dimulainya Penyidikan No. Pol.: B/48 /VII/2006/Dit II Eksus, tanggal 17 Juli 2006, Berita Acara Pemeriksaan Saksi Zulhendri Hasan, SH, MH, Berita Acara Pemeriksaan Saksi Fayakhun Andriadi, Berita Acara Pemeriksaan saksi-saksi, Berita Acara Pengambilan Sumpah Ahli, Berita Acara Pemeriksaan Ahli Freddy

Haris, SH, LLM, ACCS, Surat Perintah Pemeriksaan Barang Bukti Digital No.Pol.: SP.BBD/12/VIII/2006/Dit II Eksus tanggal 7 Agustus 2006, Berita Acara Pemeriksaan Laboratorium Forensik Komputer No. Lab.: 12/VIII/2006/ LABKOMFOR tanggal 22 Agustus 2006, Berita Acara Pemeriksaan Tersangka Iqra Syafaat, Surat Perintah Penangkapan Tersangka Iqra Syafaat No. Pol. : Sprin. Kap/100/VIII/2006/Dit II Eksus, tgl 2 Agustus 2006, Berita Acara Penangkapan Tersangka Iqra Syafaat, Surat Perintah Penahanan Tersangka Iqra Syafaat No. Pol. : SP.HAN/49/VIII/2006/Dit II Eksus, tanggal 3 Agustus 2006, Berita Acara Penahanan Tersangka Iqra Syafaat, Surat Permintaan Perpanjangan Penahanan No. Pol.: B/49a/VIII/2006. tanggal 14 Agustus 2006, Surat Perpanjangan Penahanan dari Kejaksaan Tinggi DKI Jakarta Nomor B: 4434/0.14/epp.1/08/2006 tanggal 22 Agustus 2006, Berita Acara Pelaksanaan Perpanjangan Penahanan tanggal 22 Agustus 2006, Surat Perintah Penggeledahan No. Pol.: SP. Dah/50/VIII/2006, tanggal 2 Agustus 2006, Berita Acara Penggeledahan tanggal 3 Agustus 2006, Surat Permohonan memperoleh persetujuan Penetapan atas Penggeledahan No. Pol.: B/ 282/VIII/2006/Dit II Eksus tanggal 9 Agustus 2006, Surat Persetujuan Penggeledahan dari Ketua Pengadilan Negeri Batam No187/Pen.Pidana/2006/PN Batam tanggal 15 Agustus 2006, Surat Perintah Penyitaan No. Pol.: STP. Sita/76/VII/2006/Dit II Eksus, tanggal 17 Juli 2006, Surat Tanda Penerimaan No. Pol.: STP. Sita/07/VII/2006/Dit II Eksus tanggal 17 Juli 2006 dari Zulhendri Hasan, SH, MH, Berita Acara Penyitaan dari Zulhendri Hasan, SH, MH tanggal 17 Juli 2006, Surat Permohonan Penetapan Penyitaan dari Ketua Pengadilan Negeri Jakarta Selatan Nomor 698/VIII/2006/Dit II Eksus tanggal 24 Agustus 2006, Surat Persetujuan Penetapan Penyitaan dari Ketua Pengadilan Negeri Jakarta Selatan Nomor 2255/Pen.per.sit/2006/PN Jaksel tanggal 31 Agustus 2006, Surat Tanda Penerimaan No. Pol.: STP. Sita/06/VII/2006/Dit II Eksus tanggal 18 Juli 2006 dari Riyanto Jatmiko, Berita Acara Penyitaan dari Riyanto Jatmiko tanggal 18 Juli 2006, Surat Permohonan Persetujuan Penetapan atas Penyitaan Barang Bukti Riyanto Jatmiko pada Ketua Pengadilan Negeri Jakarta Selatan Nomor B/699/VIII/2006/Dit II Eksus tanggal 24 Agustus 2006, Surat Permohonan Persetujuan Penetapan atas Penyitaan Barang Bukti RIYANTO JATMIKO pada

Ketua Pengadilan Negeri Jakarta Selatan Nomor B/699/VIII/2006/Dit II Eksus tanggal 24 Agustus 2006, Surat Tanda Penerimaan No. Pol: STP. Sita/02/VIII/2006/Dit II Eksus tanggal 2 Agustus 2006 dari Muhammad Rafi, Berita Acara Penyitaan dari Saksi Muhammad Rafi tanggal 2 Agustus 2006, Surat Permohonan Penetapan Penyitaan dari Ketua Pengadilan Negeri Batam Nomor 718/IX/2006/Dit II Eksus, Surat Persetujuan Penetapan Penyitaan dari Ketua Pengadilan Negeri Batam Nomor 799/PEN/PID/2006/PN.BATAM tanggal 6 September 2006, Surat Tanda Penerimaan No. Pol.: STP. Sita/03/03/VIII/2006/Dit II Eksus, tanggal 3 Agustus 2006 dari Tsk Iqra Syafaat Berita Acara Penyitaan dari Tsk Iqra Syafaat, Surat Permohonan Persetujuan Penetapan atas Penyitaan No. Pol.: B/283 /VIII/2006/Dit II Eksus, tanggal 9 Agustus 2006, Surat Penetapan Persetujuan Penyitaan dari Ketua Pengadilan Negeri Batam Nomor 744/pen.pid/2006/PN.BTM. tanggal 15 Agustus 2006. Berita Acara Pemeriksaan Laboratorium Forensik Komputer, daftar tersangka, daftar saksi, daftar barang bukti dan lampiran.

Setelah semua berkas disusun rapi, selanjutnya penyidik melakukan pemberkasan dengan menyusun hasil penyidikan dalam bentuk tulisan dengan susunan dan syarat-syarat pengikatan, penjilidan serta penyegelan. Ketika semua proses sudah dilakukan, penyidik menyerahkan berkas perkara kepada penuntut umum berikut penyerahan tanggung jawab tersangka dan barang buktinya yang dilaksanakan dalam dua tahap, yaitu tahap pertama penyidik hanya menyerahkan Berkas Perkara dan tahap kedua atau setelah berkas perkara dinyatakan lengkap, penyidik menyerahkan tanggung jawab tersangka Iqra Syafaat dan barang buktinya kepada penuntut umum.

4.2.4 Masalah yang Dihadapi Unit V *IT & Cybercrime*

Tindak pidana *hacking* dengan sifat dan karakteristik yang khas dan berbeda dengan tindak pidana konvensional atau tindak pidana pada umumnya menimbulkan kesulitan tersendiri dalam penyingkapan dan pengungkapannya. Hambatan tersebut pada umumnya disebabkan karena tindak pidana *hacking* yang tidak mengenal batas wilayah (*borderless*), dapat dilakukan lintas negara *(transnational)*, adanya penggunaan teknologi komputer dan komunikasi (dalam

hal ini jaringan komputer melalui internet) dan kemampuan dan *skill* khusus dari si pelaku *(hacker)* untuk dapat melakukan tindak pidana *hacking*.

Kekhasan yang dimiliki tindak pidana *hacking* tersebut dalam penanganan *hacking website* Partai Golkar menyebabkan penyidik dihadapkan pada hambatan cukup pelik yang ditemukan di lapangan dalam pelaksaanaan penyidikan. Hambatan tersebut disebabkan belum diakomodirnya implikasi kemajuan teknologi informasi yang melibatkan penggunaan komputer dan internet baik sebagai modus, alat maupun tujuan tindak pidana itu sendiri ke dalam peraturan-peraturan yuridis materiil maupun formil yang berlaku saat itu di Indonesia. Sebagai contoh dalam pelaksanaan penyidikan tindak pidana *hacking*, penyidik kerap menemukan hambatan seperti dalam hal pengumpulan barang bukti; penentuan *locus delictie* dan yurisdiksi hukum serta presentasi barang bukti.

Adanya hambatan tersebut oleh penyidik dipecahkan dengan melakukan interpretasi, mengandalkan pengalaman dan pengetahuan dari masing-masing penyidik maupun melakukan upaya lain dikaitkan dengan peraturan yang berlaku di Indonesia seperti menyajikan bukti digital ke dalam bentuk hasil *print out*, dan penguatan hasil penyidikan dengan keterangan ahli. Hasil pemecahan masalah yang dibuat oleh penyidik Unit V *IT & Cybercrime* menunjukkan karakter khusus penanganan kasus tindak pidana *hacking* dalam teknik dan prosedur penyidikan, yang membedakannya dengan penanganan tindak pidana konvensional.

Berikut ini, dibahas mengenai permasalahan yang muncul selama proses penyidikan kasus tindak pidana *hacking website* Partai Golkar yang juga merefleksikan karakteristik dari penyidikan kasus tindak pidana *hacking*.

4.2.4.1 Penentuan Jenis Tindak Pidana

Permasalahan pertama yang dihadapi oleh penyidik adalah penentuan jenis tindak pidana. Dalam kasus tindak pidana *hacking website* Partai Golkar, masalah penentuan jenis tindak pidana yang akan dilaporkan oleh Golkar telah dikonsultasikan dan didiskusikan terlebih dahulu antara perwakilan Golkar dan Kanit V *IT & Cybercrime* beserta beberapa penyidik di kantor Unit V *IT & Cybercrime*.

Sehingga sejak bertemu perwakilan Golkar, issu mengenai penentuan tindak pidana yang akan dilaporkan sudah menjadi pembahasan antara calon pelapor dan

penyidik Unit V *IT & Cybercrime* yang merupakan unit yang mempunyai tugas dan fungsi melakukan penyidikan tindak pidana *IT & Cybercrime* sesuai dengan visi dan misi organisasinya. Sebagaimana terungkap dalam pembahasan mengenai pelaporan pada sub bab 4.2.2 di atas, datangnya perwakilan Golkar ke kantor Unit V *IT & Cybercrime* dengan alasan mereka telah mengetahui tentang adanya unit khusus yang menangani tindak pidana *IT & Cybercrime.*

Dalam pertemuan tersebut, penyidik dengan pengalaman dan pengetahuannya menjelaskan tentang tindak kejahatan apa yang dilakukan oleh tersangka yang saat itu belum diketahui, dan membantu merumuskan uraian singkat kejadian dan barang bukti yang dapat diserahkan untuk persiapan pembuatan laporan polisi sesuai dengan kejadian yang dialami. Kemudian penyidik Unit V *IT & Cybercrime* membantu membuatkan *draft* laporan polisi bersama dengan perwakilan Partai Golkar. Selanjutnya *draft* tersebut diserahkan kepada SPK dengan didampingin oleh penyidik Unit V *IT & Cybercrime* sebagai pelaksanaan prosedur pembuatan laporan.

Berdasarkan laporan polisi tersebut, selanjutnya Kanit V *IT & Cybercrime* segera menentukan jenis tindak pidana yang harus diselidiki sebagai arahan bagi para penyidik yang ditunjukkan untuk melakukan tahap penyelidikan sebagaimana dituangkan dalam Surat Perintah Tugas No. Pol.SP.Gas/145/VII/2006/Dit II Eksus tertanggal 17 Juli 2006.

Dalam Surat Perintah disebutkan bahwa tindak pidana yang harus diselidiki dan disidik adalah tindak pidana di bidang telekomunikasi dan perusakan terhadap tampilan *website www.golkar.or.id* atau turut serta atau memberikan kesempatan ataupun membantu sebagaimana dimaksud dalam Pasal 22, 50 Undang-Undang Telekomunikasi dan Pasal 406 KUHP atau Pasal 55, 56 KUHP Jo. Pasal 406 KUHP.

Dari uraian di atas, terungkap bahwa sebenarnya analisa mengenai tindak pidana yang akan ditentukan sudah mulai dibahas dan diarahkan sejak pertemuan pertama kali dengan perwakilan Golkar. Penentuan tindak pidana di bidang telekomunikasi dan perusakan tampilan *website* Partai Golkar, selanjutnya dikaitkan dengan ketentuan Pasal 22, Pasal 50 Undang-Undang Telekomunikasi

dan Pasal 406 KUHP atau Pasal 55, Pasal 56 KUHP Jo Pasal 406 KUHP.

Penentuan ketentuan pidana terhadap perusakan tampilan *website* Partai Golkar dimaksudkan sebagai arahan bagi penyidik dalam melakukan proses penyidikan tindak pidana yang dilaporkan, agar ada panduan yang dapat dijadikan target penyidikan. Arahan dari Kanit tersebut merefleksikan bahwa Kanit telah melakukan analisa atas kejahatan yang terjadi terhadap *deface* Partai Golkar, dengan mempelajari keterangan awal atau uraian singkat kejadian yang disampaikan dalam laporan polisi, sehingga dihasilkan hubungan antara tindak pidana yang dilaporkan dengan ketentuan normatif yang ada pada saat itu.

Hal tersebut di atas, menjelaskan bahwa dalam hal ini penyidik telah melakukan interpretasi karena uraian kejadian tidak secara tegas dan jelas merujuk pada unsur-unsur dalam pasal-pasal yang akan diterapkan tersebut. Disini terlihat bahwa penyidik sejak awal telah menentukan perbuatan yang dilakukan dapat disangkakan atau dikategorikan sebagai suatu tindak pidana konvensional yang dapat dijerat dengan pasal-pasal dalam KUHP, yaitu Pasal 406 KUHP maupun sebagai tindak pidana khusus yang diatur dalam Pasal 22 jo Pasal 50 Undang-Undang Telekomunikasi. Hal yang sama, juga tercermin dalam Surat Perintah Penyidikan No. Pol.: SP.Sidik/80/VII/2006/Dit II Eksus yang diterbitkan oleh Kanit V *IT & Cybercrime* tertanggal 17 Juli 2006.

Dalam pelaksanaan proses penyidikan kasus tindak pidana *hacking website* Partai Golkar sebagaimana diungkapkan dalam pembahasan pada Sub Bab 4.2.3 di atas, penyidik berkewajiban untuk mencari dan menemukan fakta-fakta kejadian untuk memenuhi unsur-unsur tindak pidana sebagaimana ditentukan dalam Surat Perintah Tugas dan Surat Perintah Penyidikan, dimana mengandung arahan dari pimpinan bahwa tindak pidana yang disidik adalah sebagaimana dimaksud dalam ketentuan Pasal 22, 50 Undang-Undang Telekomunikasi dan Pasal 406 KUHP atau Pasal 55, 56 KUHP Jo. Pasal 406 KUHP. Hal ini merupakan permasalahan tersendiri yang muncul berkaitan dengan penerapan pasal yang disangkakan menjadi satu tantangan bagi penyidik sebagaimana disampaikan oleh seorang Pamen dalam Wawancara Berpedoman berikut ini:

> *"...kesulitan dalam penyidikan tentu saja banyak kami temukan, diantaranya adalah menerapkan unsur pasal dengan fakta-fakta yuridis*

yang ada. Untuk pidana umum sendiri sebagai suatu pasal untuk kasus perusakan situs partai golkar, jelas sangat sulit karena salah satu unsur yang disyarati adalah rusaknya barang sehingga tidak dapat dipergunakan lagi. Kejahatan tersebut sama sekali tidak ada barang yang rusak...". (WBIS 04)

Penggunaan ketentuan pasal-pasal KUHP dan Undang-undang Telekomunikasi tersebut dalam proses penyidikan tindak pidana *hacking* seringkali juga masih diperdebatkan dalam diskusi, apabila dikaitkan dengan kekuatan pemenuhan unsur-unsur dalam pasal-pasal tersebut untuk membuktikan tindak pidana yang disangkakan. Hal tersebut diantaranya disampaikan oleh seorang Pamen dalam Wawancara Berpedoman sebagai berikut:

"....Untuk pemilihan atau untuk penetapan pasal yang kita gunakan dalam kasus cybercrime, kita masih menggunakan KUHP. Seandainya itu pun di juncto kan, kita akan juncto kan dengan undang – undang telekomunikasi 36 tahun 99 pasal 22 a, b, c. Tetapi menurut kami sebenarnya undang – undang 36 tahun 99 itu sendiri pun, sebenarnya kalau ada pengacara yang cukup jeli, dia akan menanyakan system jaringan informasi khusus itu apa termasuk internet, dan itu tidak dijelaskan didalam undang – undang 36 tahun 99..". (WBIS 07)

Dengan demikian, masalah penggunaan Pasal 20 dan Pasal 50 Undang-undang Telekomunikasi maupun Pasal 406 KUHP atau Pasal 55, Pasal 56 KUHP Jo. Pasal 406 KUHP, terdapat keraguan dari penyidik untuk menggunakan pasal tersebut dalam proses penyidikan tindak pidana *hacking*. Seorang Pamen dalam wawancara berpedoman secara tegas menjelaskan bahwa apa yang dilakukannya untuk menyelesaikan tugas penyidikan kasus tindak pidana *hacking* adalah melakukan interpretasi atas ketentuan normatif yang ada, sebagai berikut:

"....yang bedanya adalah pada saat kita dalam pasal, pasal disini kan kita hanya menggunakan pasal KUHP dan undang-undang spesialis yaitu undang-undang telekomunikasi No. 36 tahun 99 tentang telekomunikasi dimana disitu dikatakan bahwa mengakses tanpa hak jaringan telekomunikasi dan pasal 22 huruf b sama c, kalau yang c itu kan jaringan telekomunikasi khusus itu pengertian nya jaringan telekomunikasi khusus itu adalah HT cuma kita interpretasikan bahwa ini merupakan jaringan internet sehingga pada saat itulah Jaksa akhirnya kita limpahkan kepada jaringan telekomunikasi kita komunikasikan dengan saksi ahli pidana

kemudian dengan Jaksa kita terapkan pasal 22 huruf b undang-undang 36 dan pasal 406 KUHP yaitu perusakan." (WBIS 09)

Hal itu mengungkapkan bahwa penyidikan kasus tindak pidana *hacking* dilakukan oleh penyidik dengan melakukan interpretasi untuk memecahkan masalah tidak tersedianya hukum yang secara khusus mengatur tindak pidana *hacking*. Hal tersebut secara tegas juga diungkapkan pula oleh seorang Pamen dalam wawancara berpedoman sebagai berikut:

*"...itu semua adalah **interpretasi** daripada penyidik dalam memahami suatu perkara yang ada dikaitkan dengan tindak pidana umum karena menggunakan KUHP, seperti deface ya kita gunakan perusakan 406, ataupun misalnya penipuan melalui internet kita gunakan Pasal 372, 378 KUHP..."* (WBIS 07)

Masalah yang muncul berkaitan dengan pada saat itu, belum tersedia aturan hukum yang secara khusus mengatur tindak pidana *hacking*, padahal tindakan *hacking* saat ini sudah banyak terjadi. Dalam kondisi demikian, penyidik dituntut untuk mencari solusi pemecahan dengan melakukan interpretasi terhadap hukum normatif yang tersedia. Masalahnya, interpretasi itu tergantung dari persepsi penyidik yang bersangkutan, sehingga hasil interpretasi akan berbeda-beda setiap penyidik sebagaimana yang terungkap dalam wawancara berpedoman berikut ini:

"...Karena interpretasi itu tergantung daripada persepsi ataupun pandangan dari orang yang melihat kasus itu sendiri." (WBIS 07)

Untuk mencapai interpretasi yang paling mendekati, tentunya dituntut pengetahuan, pemahaman dan kemampuan yang tinggi dari penyidik dalam melaksanakan tugas penyidikan tindak pidana *hacking* mengenai tindak pidana tersebut. Dalam Unit V *IT & Cybercrime*, hal yang mendukung mereka untuk mampu melakukan interpretasi terhadap ketentuan undang-undang, adalah pengetahuan dan pemahaman mereka yang cukup baik mengenai *cybercrime*, sebagaimana diungkapkan oleh seorang Pamen dalam wawancara berpedoman sebagai berikut:

> *"...Dengan adanya pelatihan tersebut paling tidak kita punya gambaran ataupun wawasan mengenai apa sih yang dimaksud dengan cybercrime dan bagaimana kejahatan itu berlangsung dan bagaimana pula seorang penyidik mesti membuktikan sesuatu yang tidak nampak secara nyata untuk dibawa ke suatu pembuktian yang secara nyata sehingga diperlukan suatu interpretasi dan kalau tidak didukung oleh gambar atau wawasan sebelumnya sangat sulit untuk membuat sesuatu itu menjadi gampang dimengerti oleh orang yang tidak mengerti, orang awam lainnya."* (WBIS 08)

Para penyidik Unit V *IT & Cybercrime* sebagian besar telah mengikuti kursus-kursus, pelatihan-pelatihan, seminar-seminar maupun acara-acara lain mengenai kejahatan komputer, yang salah satunya mengenai tindak pidana *hacking*. Para penyidik juga telah mendapatkan pengetahuan mengenai *cybercrime* dengan belajar secara otodidak.

Selain itu, aspek pengalaman juga menjadi faktor penting bagi penyidik dalam menyelesaikan tugasnya dalam melakukan penyidikan kasus tindak pidana *hacking*. Contohnya, penyidik yang pernah menangani kasus yang kurang lebih serupa, yaitu tindak pidana *hacking website* KPU, sehingga lebih mudah ketika melaksanakan penyelesaian penyidikan tindak pidana *hacking website* Partai Golkar.

Sebagian penyidik telah mempunyai pemahaman mengenai tindak pidana *hacking* sebagaimana dalam hasil wawancara berpedoman berikut ini:

> *"Hacking dari pengetahuan saya membaca dan mendengar dari yang lain hacking itu perbuatan seseorang masuk kekomputer orang lain atau ke jaringan komputer tanpa sepengetahuan pemilik jadi bagaimana orang itu masuk kejaringan komputer orang lain atau ke komputer orang lain tanpa ijin dari pemiliknya..."* Pama (WBIS 01 A)

> *"Pengetahuan kami mengenai hacking itu adalah seseorang yang memasuki akses internet ataupun jaringan tanpa hak atau pun tanpa ijin melakukan mungkin perubahan-perubahan maupun untuk mencari informasi tentang website tentang informasi yang ada diinternet..."* Pamen (WBIS 09 A)

Dari pemahaman penyidik atas pengertian tindak pidana *hacking* sebagaimana dijelaskan diatas, pada umumnya penyidik memahami tindak pidana *hacking* sebagai suatu tindakan memasuki jaringan komputer milik orang lain

tanpa izin atau hak dari pemiliknya dengan maksud tertentu seperti untuk mengetahui kelemahan sistem komputer, merusak atau mengubah sistem komputer dan mengambil keuntungan atas perbuatan yang dilakukannya. Selain berdasarkan interpretasi dan pengetahuan serta pengalaman, penyidik juga meminta keterangan dari ahli.

Berdasarkan uraian di atas dapat diketahui bahwa penentuan pasal-pasal yang dikenakan oleh penyidik merupakan hasil interpretasi berdasarkan pemahaman dan pengetahuan penyidik mengenai tindak pidana *hacking* beserta pendapat ahli. Hal tersebut dihubungkan dengan penyerangan yang dilakukan melalui media internet dengan memasuki jaringan komputer milik orang lain (Partai Golkar) tanpa izin atau hak sehingga menyebabkan kerusakan pada *website* Partai Golkar. Ditambah dengan yurisprudensi atas putusan kasus tindak pidana *hacking website* KPU yang ternyata dapat dijerat dengan Undang-Undang Telekomunikasi, menambah keyakinan penyidik bahwa kasus tindak pidana *hacking website* Partai Golkar dapat disidik dan dapat dilimpahkan ke penuntut umum.

Dengan demikian, dalam kasus tindak pidana *hacking website* Partai Golkar, penyidik dapat menggunakan Undang-undang Telekomunikasi, dimana penyidik menyimpulkan bahwa tindakan yang dilakukan oleh tersangka akhirnya dianggap sebagai pelanggaran terhadao Pasal 22 UU yang menyebutkan bahwa setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses jaringan telekomunikasi; jasa telekomunikasi dan jaringan telekomunikasi khusus. Selain itu, penyidik memasukkan Pasal 406 untuk menghubungkannya dengan perusakan barang sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana.

Atas penentuan pasal-pasal tersebut, serangan atas *website* Partai Golkar dapat digolongkan sebagai tindak pidana *hacking* yang menimbulkan kerusakan *website* Partai Golkar. Jika dilihat dari pengertian *hacking* komputer (*unauthorized access*) atau *computer trespass* bahwa akses terhadap sistem komputer yang dilakukan dengan menggunakan atau memanfaatkan *password*, untuk melakukan suatu perbuatan kriminal, atau memanfaatkan komputer dengan

cara yang salah merupakan perbuatan (tindakan) *illegal* yang sedikit banyak akan mempengaruhi kinerja suatu jaringan informasi (Makarim, 2005: 432).

Hal ini berarti tindak pidana *hacking website* Partai Golkar diinterpretasikan oleh penyidik sebagai pelanggaran Pasal 22 Undang-undang Telekomunikasi, karena penyerang (tersangka) telah melakukan perbuatan ilegal atau tanpa hak atau tanpa izin dengan memasuki jaringan komputer Partai Golkar dan dapat diancam pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp. 600.000.000,- (enam ratus juta rupiah) sebagaimana diatur dalam Pasal 50 Undang-undang Telekomunikasi.

Sedangkan tindak pidana *hacking website* Partai Golkar yang mengakibatkan rusaknya *website* Partai Golkar disamakan dengan rusaknya suatu barang yang dapat diancam pidana sebagaimana diatur dalam Pasal 406 KUHP. Jika dilihat dari pengertian barang atau benda dalam tinjauan hukum pidana, pengertian barang atau benda dalam penjelasan Pasal 362 KUHP, yaitu segala sesuatu yang berwujud atau tidak berwujud (misal listrik, gas) dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang. Hal ini berarti *website* itu dapat digolongkan sebagai barang atau benda tak berwujud sebagaimana diungkapkan oleh keterangan ahli dalam pemeriksaan yang dilakukan pada tanggal 1 September 2006.

Berdasarkan uraian-uraian yang telah dibahas di atas, penentuan jenis tindak pidana dalam kasus ini didasarkan pada pengetahuan, pemahaman dan pengalaman yang dimiliki oleh penyidik serta pendapat ahli, yang menghasilkan persepsi yang sama dalam melihat kasus tindak pidana *hacking* sehingga mampu membuat interpretasi terhadap ketentuan normatif yang tersedia, walaupun faktanya tindak pidana *hacking* belum secara tegas dan khusus diatur dalam suatu ketentuan hukum atau undang-undang tersendiri pada saat itu.

Dalam jangka panjang, penyidikan tindak pidana dengan menggunakan interpretasi undang-undang sebaiknya segera diakhiri dengan dibuatnya suatu undang-undang yang mengatur secara tegas hal tersebut. Hal ini disampaikan oleh seorang Pamen dalam wawancara berpedoman berikut ini:

> *"Dalam tindak pidana hacking memang sudah seharusnya kita sudah mempunyai suatu undang – undang atau peraturan sendiri yang spesifik*

mengatur mengenai masalah hacking itu sendiri, tidak lagi berinterpretasi. Karena interpretasi itu tergantung daripada persepsi ataupun pandangan dari orang yang melihat kasus itu sendiri. Yang paling, sebenarnya untuk kasus cybercrime ini, kalau mau dikatakan dibantah paling mudah, itu sebenarnya paling mudah. Seperti kasus penyebaran pornografi melalui internet. Satu aja Jaksa yang mengatakan mana saksi yang melihat". (WBIS 07)

Hal tersebut dipahami dari sudut pandang penyidik yang bertugas melakukan penyidik kasus tindak pidana *hacking* merupakan suatu kebutuhan penting yang dapat memudahkan kerja penyidikannya, sehingga dalam melakukan penyidikan tindak pidana *hacking*, yang bersangkutan tidak harus melakukan interpretasi tapi uraian kejahatan sudah jelas diatur dalam suatu undang-undang yang spesifik untuk itu. Sementara pendapat lain terungkap dalam wawancara berpedoman sebagai berikut:

"Kalau menurut saya tindak pidana hacking itu setidaknya harus diatur didalam undang-undang tersendiri karena sampai sekarang ini Indonesia belum memiliki undang-undang yang berkaitan dengan kejahatan cybercrime atau kejahatan komputer secara umum kalau bisa harus ada undang-undang payung dulu baru undang-undang dibawahnya yang merupakan breakdown dari undang-undang payungnya sebagai contoh misalnya undang-undang tentang lingkungan hidup merupakan undang-undang payung untuk undang-undang kehutanan, undang-undang perairan, undang-undang pencemaran lingkungan itu harus ada undang-undang lingkungan hidupnya dulu yang sekarang ini kalau dalam tindak pidana hacking itu merupakan diatur dalam undang-undang tersendiri kemudian undang-undang itu mengacu pada undang-undang tindak pidana komputer secara umum atau luas." (WBOS 01A)

Dengan demikian, pengaturan mengenai tindak pidana *hacking* dalam suatu undang-undang yang spesifik juga dinilai akan dapat memberikan kejelasan mengenai tindak pidana *hacking* sebagai suatu perbuatan yang dilarang dan bagi yang melakukan akan dikenakan sanksi pidana tertentu.

4.2.4.2 Penemuan dan Pengumpulan Barang Bukti

Hambatan lain yang harus dihadapi oleh penyidik kasus tindak pidana *hacking website* Partai Golkar adalah masalah penemuan dan pengumpulan bukti yang sebagian besar berupa bukti digital. Hal ini menjadi salah satu perhatian

penting karena penyidik seringkali berbenturan dengan ketentuan hukum acara pidana dan ketentuan normatif lainnya dalam proses penyidikan, dimana ketentuan hukum dimaksud belum mengakomodir perihal bukti digital sebagai salah satu alat bukti, sementara dalam proses penyidikan tindak pidana *hacking*, bukti digital seringkali merupakan bukti yang paling representatif untuk menjelaskan mengenai tindak pidana *hacking*. Hal senada disampaikan oleh seorang Pamen dalam wawancara berpedoman sebagai berikut:

> *"...disamping pasal yang diterapkan kemudian juga tentang barang bukti digital, barang bukti digital ini memang hal yang sangat belum familiar dalam sistem hukum kita sehingga Jaksa sendiri itu masih bingung...".* (WBIS 09)

Dari ungkapan di atas, dapat dijelaskan bahwa barang bukti digital dirasa sebagai sesuatu yang belum diatur secara khusus dalam sistem hukum Indonesia, sehingga tentang barang bukti digital dianggap sebagai suatu hambatan dalam melakukan penyidikan dan harus dicarikan solusinya dalam upaya pencarian dan penemuan bukti untuk kasus tindak pidana *hacking*. Bahkan salah seorang Pamen dalam Wawancara Berpedoman menegaskan bahwa barang bukti digital merupakan suatu kesulitan yang mendasar, berikut kutipannya:

> *"...Sebagai contoh kesulitan lain yang mendasar adalah ketika barang bukti digital, ketika kejahatan itu dapat diurai dari barang bukti digital tentang pemberlakuannya sendiri sampai saat ini belum ada aturan baku yang mengatur,... "* . (WBIS 04)

Barang bukti sendiri dalam KUHAP maupun perundang-undangan pidana lainnya tidak dijelaskan mengenai definisi atau pengertiannya namun pengertian barang bukti dapat dipahami dari beberapa doktrin hukum. Wirjono Projodikoro (1985: 58-59) memberikan pengertian barang bukti sebagai: 1) Obyek yang menjadi sasaran perbuatan melanggar hukum pidana, seperti: barang-barang yang dicuri atau digelapkan, atau yang didapatkan secara penipuan; 2) Barang-barang yang tercipta sebagai buah dari perbuatan yang melanggar hukum pidana, seperti: uang logam atau uang kertas yang dibuat oleh terdakwa dengan maksud mengedarkannya sebagai uang asli, termasuk didalamnya tulisan palsu; 3)

Barang-barang yang dipakai sebagai suatu alat untuk melakukan perbuatan yang melanggar hukum pidana, seperti: suatu pisau atau senjata api atau tongkat yang dipakai untuk membunuh atau menganiaya orang, perkakas-perkakas yang dipakai untuk membuat uang paisu; 4) Barang-barang yang pada umumnya dapat menjadi barang bukti yang memberatkan atau meringankan kesalahan terdakwa. Sedangkan Andi Hamzah (1986: 100) memberikan pengertian barang bukti sebagai barang mengenai mana delik dilakukan (obyek delik) dan barang dengan mana delik dilakukan, yaitu alat yang dipakai melakukan delik, misalnya pisau yang dipakai untuk menikam orang. Termasuk juga adalah barang bukti ialah hasil dari delik, seperti uang negara yang dipakai (korupsi) untuk membeli rumah pribadi, maka rumah pribadi itu merupakan barang bukti, atau hasil dari delik.

Dalam pelaksanaan penyidikan tindak pidana *hacking website* Partai Golkar, penyidik menghadapi masalah dalam mengumpulkan barang bukti digital, disebabkan oleh adanya perbedaan antara penanganan tindak pidana *hacking* dengan penanganan tindak pidana konvensional dimana barang bukti yang terkait dengan tindak pidana pada umumnya berupa barang bukti kasat mata (terlihat) dan dapat dikumpulkan langsung dari tempat kejadian perkara berdasarkan hasil pengolahan Tempat Kejadian Perkara (TKP). Sedangkan barang bukti pada tindak pidana *hacking website* Partai Golkar lebih banyak berupa bukti-bukti digital (elektronik) yang terdapat dalam barang yang kasat mata, misalnya *laptop*, *CPU*, dan komputer. Pada hakekatnya bukan barang tersebut yang menjadi barang bukti utama namun data-data digital yang tersimpan di dalamnya yang menjadi barang bukti. Barang bukti tersebut masih dicari dan dikumpulkan dari beberapa lokasi baik dari TKP maupun dari tempat lain yang berkaitan dengan terjadinya tindak pidana. Hal ini berarti penyidik harus mengumpulkan serta merunut satu per satu dari bukti yang diperoleh.

Permasalahan pengumpulan bukti-bukti tersebut diawali dari penyerahan barang bukti berupa *CD* yang berisikan *log files www.golkar.or.id* dan dan *hard copy* akses *log* dari tanggal 8 Juli 2006 hingga 14 Juli 2006 sebanyak tujuh bundel oleh Zulhendri Hasan, SH., MH dan Daulat Firman Abraham pada tanggal 8 Juli 2006 hingga 14 Juli 2006. Kemudian dari pemeriksaan saksi terlapor tersebut diperoleh informasi penting mengenai pengumpulan barang bukti digital, info

tersebut mengenai lokasi dimana *hard disc server website* Partai Golkar itu ditempatkan (*posting*), yaitu di Gedung *Cyber*. Kemudian penyidik melakukan pemeriksaan di tempat *hard disc server website* Partai Golkar itu berada, yaitu di PT Master Web Network pada PT Telkom Kandatel Jakarta Barat yang *posting*nya di Gedung *Cyber*. Atas *hard disk* tersebut, penyidik melakukan *recovery* atau biasa dikenal dalam Unit V *IT & Cybercrime* sebagai *imaging* kemudian *hard disc* yang telah di-*imaging* tersebut diperiksa oleh tim laboratorium forensik komputer Unit V *IT & Cybercrime*. Proses *imaging* merupakan tahap awal memproses bukti digital dimana hasilnya selanjutnya harus dianalisis secara forensik dengan menggunakan *forensic software tools* yang bersifat khusus.

Penyidik kemudian melakukan pemeriksaan terhadap saksi Riyanto Jatmiko dari PT Master Web Network Penyidik pada tanggal 19 Juli 2006 disertai penyitaan barang bukti berupa 1 (satu) buah *hard disc* merk "Seagate", tipe Barracuda 7200.9, kapasitas 250 GB, S/N:4ND3250824A, P/N:98D33-303, yang merupakan hasil *image* dalam proses pengumpulan barang bukti.

Tahap pengumpulan barang-barang bukti tersebut, dilakukan dengan prosedur penyitaan yang berlaku umum dalam penyidikan tindak pidana konvensional, yaitu penyitaan berupa satu keping *CD* dan *hard copy* akses *log* dari tanggal 8 Juli 2006 hingga 14 Juli 2006, serta 1 (satu) buah *hard disc* merk "Seagate", tipe Barracuda 7200.9, kapasitas 250 GB, S/N:4ND3250824A, P/N:98D33-303.

Dengan barang-barang bukti tersebut di atas, penyidik kemudian melakukan analisis terhadap *content* yang terkandung di dalamnya dengan menggunakan fasilitas pada laboratorium forensik komputer dimana di dalamnya terdapat *forensic software tools* yang bersifat khusus. Pemeriksaan forensik tersebut dimaksudkan untuk menganalisa *history log files* yang ada di *hard disk* untuk mengetahui informasi-informasi siapa saja pihak yang mengakses atau melakukan perintah terhadap *website* Partai Golkar. Dari hasil pemeriksaan laboratorium forensik komputer diperoleh bukti-bukti *script* program yang digunakan untuk menyerang *website* Partai Golkar serta bukti-bukti kapan penyerangan terhadap *website* Partai Golkar tersebut dilakukan, darimana dan kemana *IP Address* serta

siapa *ISP*-nya, sehingga dapat diperoleh keterangan mengenai pihak-pihak yang berkaitan dengan pelaku, tanggal-tanggal dilakukannya serangan, tempat-tempat dilakukannya penyerangan dan tempat-tempat yang diserang.

Berdasarkan hasil laboratorium forensik komputer terhadap serangan *website* Partai Golkar, penyidik memperoleh informasi bahwa penyerangan diduga dari beberapa kota di Indonesia seperti Bandung, Jakarta, Medan, Bekasi dan Batam, bahkan penyerangan juga diduga dari beberapa negara seperti Malaysia, Turki, USA, Brazil dan Rumania.

Dari beberapa tempat yang didapatkan, penyidik mencurigai tiga tempat penyerangan, yaitu di Jakarta, Bandung dan yang terakhir dan paling dicurigai adalah Batam karena dari kota tersebut diketahui telah terjadi akses terhadap *website* Partai Golkar yang lebih banyak dibandingkan dengan kota lain. Dari hal tersebut kemudian penyidik memetakan serangan dan dapat menentukan proses penyidikan selanjutnya.

Penyidik kemudian melakukan pemeriksaan terhadap *ISP* yang dicurigai, yaitu yang berada di Jakarta dan Bandung, tetapi ternyata tidak menunjukkan titik terang penyidikan. Dengan dibantu oleh pihak *ISP*, penyidik terus mencoba menemukan pelaku maupun *IP Address* yang dicurigai digunakan *hacker website* Partai Golkar yang berada di wilayah Batam. Pada tanggal 2 Agustus 2006, tim penyidik melakukan rangkaian pemeriksaan dan pengumpulan barang bukti di Batam dimulai dari pemeriksaan terhadap saksi-saksi dari *ISP* yang dicurigai, yaitu PT Inforsys Indonesia yang mempunyai anak perusahaan PT Primera Telekomunikasi dengan bidang usaha internet, dan memiliki *IP Address* yang sama dengan yang ditemukan dalam *history log files* dalam *server website* Partai Golkar, yaitu *IP Address* 222.124.136.81.

Saksi yang diperiksa dari pihak *ISP*, PT Inforsys Indonesia adalah Gani, Direktur Utama dan Irwan, S.Kom. yang menjabat sebagai *Technical Support*. Dari pemeriksaan terhadap saksi-saksi tersebut penyidik mengetahui pemilik *IP Address* yang diduga digunakan oleh pelaku, yaitu *IP Address* 222.124.136.81, 222.124.136.52 dan 222.124.136.101 yang merupakan *IP Address* milik PT Inforsys Indonesia. *IP Address* tersebut merupakan sebagian dari *IP Address* yang

dimiliki dan didapatkan dari PT Telkom Indonesia (Kepulauan Riau) dengan range *IP Address* yang dimiliki adalah 128 *IP Address*, yaitu 222.124.136.0 – 222.124.136.127 sejak November 2005.

Dari hasil pemeriksaan dan bantuan pihak *ISP* tersebut, lebih lanjut diketahui bahwa *IP Address* tersebut di-*share* atau disewakan oleh *ISP* ke Warnet Barelang yang terletak di Jalan Raden Patah No.81 Batam, dimana *IP Address* tersebut sebenarnya tidak aktif namun dapat digunakan pihak lain karena sifatnya tidak ditutup secara resmi, pihak lain tersebut biasanya adalah pelanggan *ISP* PT Inforsys Indonesia.

Disamping pencarian terhadap pengguna *IP Address* yang dicurigai, di Batam penyidik juga melakukan *virtual undercover* atas *nickname* yang ditemukan dari data *log files* dengan dibantu oleh komunitas *hacker* yang ada di Batam. Penyidik melakukan hal ini melalui penyamaran *chatting email* terhadap *nick name* yang diketahui *IP Address* atau *email*nya melalui informasi dari komunitas *hacker*. Tersangka mengakui di dalam *chatting* dan *email* bahwa tersangka telah menyerang *website* Partai Golkar dan selanjutnya dari penyidikan tersebut diketahui bahwa tersangka tersebut adalah Iqra Syafaat.

Berdasarkan hasil yang diperoleh dalam pemeriksaan saksi-saksi dari pihak *ISP* dan pemetaan pengguna *IP Address* 222.124.136.81 serta informasi dari komunitas *hacker* tersebut, penyidik menuju ke Warnet Barelang. Di Warnet Barelang, penyidik mendapati tersangka Iqra Syafaat berada disana dan segera melakukan penangkapan diikuti dengan pemeriksaan tersangka. Kemudian penyidik melakukan penggeledahan tempat tinggal tersangka dan penyitaan barang bukti berupa 1 (satu) unit laptop warna biru merk "Twinhead" *serial number*: SY1030001656 model No: A5010 dan 1 (satu) *CPU* rakitan warna silver. Setelah itu, terhadap tersangka juga dilakukan penahanan.

Dari Warnet Barelang, penyidik melakukan pemeriksaan terhadap saksi Muhammad Rafi serta melakukan pengumpulan dan penyitaan barang bukti berupa *daily report* dari *print out billing* Warnet Barelang yang menunjukkan bahwa tersangka melakukan akses internet dari *PC* Nomor 10 dan 11 Warnet Barelang mulai tanggal 7 Juli 2006 sampai dengan 14 Juli 2006. Pada tanggal-tanggal tersebut terjadi serangan terhadap *website* Partai Golkar.

Dari uraian tersebut di atas, barang bukti yang telah ditemukan dan dikumpulkan oleh penyidik selama proses penyidikan berupa: 1 (satu) keping *CD* yang berisikan *log files www.golkar.or.id* tanggal 8 Juli 2006 sampai dengan 14 Juli 2006, R1.0; 7 (tujuh) *bundle hard copy* akses log dari tanggal 8 Juli 2006 sampai dengan 14 Juli 2006; 1 (satu) buah *hard disc* merk "Seagate", tipe Barracuda 7200.9, kapasitas 250 GB, S/N: 4 ND3250824A, P/N: 98D33-303 (hasil *image*); 1 (satu) eksemplar hasil *print out* dari *billing* Warnet Barelang, dari tanggal 7 Juli 2006 sampai dengan tanggal 14 Juli 2006; 1 (satu) unit Laptop warna biru merk "Twinhead", S/N: SY1030001656, Model No.:A5010 dam 1 (satu) unit *CPU* rakitan warna *silver*.

Atas barang bukti yang telah ditemukan, dikumpulkan dan disita tersebut, Kanit V *IT & Cybercrime* memerintahkan pemeriksaan lebih lanjut kepada penyidik terutama terhadap barang bukti yang mengandung bukti *digital* yang mampu menjelaskan tindak pidana yang dilakukan tersangka Iqra Syafaat melalui Surat Perintah Pemeriksaan Barang Bukti Digital No. Pol.: SP.BBD/08/VIII/2006/Dit II Eksus tertanggal 7 Agustus 2006. Selain itu, Kanit V *IT & Cybercrime* memerintahkan untuk membuat Berita Acara Pemeriksaan Laboratorium Kriminalistik terhadap analisis bukti digital.

Pada tanggal 22 Agustus 2006, hasil pemeriksaan terhadap barang bukti yang disampaikan telah selesai dilaksanakan dan dilaporkan dengan Berita Acara Pemeriksaan Laboratorium Kriminalistik No. Lab.: 12/VIII/2006/ LABKOMFOR dengan barang bukti yang diperiksa berupa 1 (satu) buah *hard disc* merk "Seagate", tipe Barracuda 7200.9, kapasitas 250 GB, S/N: 4 ND3250824A, P/N: 98D33-303 (hasil *image*); 1 (satu) unit laptop warna biru merk "Twinhead", S/N: SY1030001656, Model No.:A5010; 1 (satu) unit *CPU* rakitan warna *silver*.

Dengan hasil pemeriksaan atas bukti tersebut, diperoleh bukti-bukti kode/*script* program yang digunakan oleh penyerang untuk menyerang *website* Partai Golkar dan *log http access* (bukti kunjungan) *website* Partai Golkar. Pada barang bukti 1 (satu) unit *CPU* rakitan warna *silver* didapatkan bukti-bukti bahwa barang bukti tersebut pernah digunakan untuk melakukan serangan terhadap *website* Partai Golkar. Hal ini dapat dilihat dari bukti *internet history* dan *html carver* yang hasil pemeriksaannya dilampirkan dalam bentuk *print out*.

Dari uraian tersebut di atas, terungkap bahwa dalam pelaksanaan penyidikan tindak pidana *hacking website* Partai Golkar, penyidik menghadapi masalah dalam mengumpulkan barang bukti digital. Masalah tersebut timbul karena adanya perbedaan antara penanganan tindak pidana *hacking website* Partai Golkar dengan penanganan tindak pidana konvensional.

4.2.4.3 Penentuan *Locus Delictie* dan Kompetensi Relatif Pengadilan

Penentuan *locus delectie* (tempat kejadian perkara) dan yurisdiksi hukum sangat sulit ditentukan karena tindak pidana *hacking* bersifat *borderless* dimana setiap orang dapat melakukan tindak pidana *hacking* dimana saja dan akibat yang ditimbulkan bisa saja terjadi di tempat atau wilayah lain yang berbeda dengan tempat atau wilayah tindak pidana *hacking* dilaksanakan.

Dalam tindak pidana *hacking website* Partai Golkar dari pemeriksaan diketahui bahwa tindak pidana tersebut dilakukan di Batam namun akibatnya dapat terlihat dimana saja ketika setiap orang mengakses *website* Partai Golkar. Namun serangan terhadap *website* dapat dilihat dari *history* di tempat *server website* Partai Golkar yang berada di PT Master Web Network pada PT Telkom Kandatel Jakarta Barat Jl. S. Parman Kav. 8 Jakarta Barat dan *hosting*nya berada di Gedung *Cyber*. Hal ini menimbulkan permasalahan mengenai apakah kasus tersebut *locus delictie-nya* berada di Jakarta atau Batam. Penentuan *locus delictie* ini berkaitan dengan apakah hasil penyidikan akan dilimpahkan ke Kejaksaan di Jakarta atau Kejaksaan Batam.

Ketika permasalahan ini didiskusikan dengan Kejaksaan Jakarta, antara pihak penyidik dengan Kejaksaan timbul perbedaan pendapat mengenai *locus delectie* kasus tindak pidana *hacking website* Partai Golkar. Hal ini dapat dilihat dari pendapat Kejaksaan Jakarta yang menyarankan agar kasus tersebut nantinya dilimpahkan ke Batam. Dengan pertimbangan kejadian *locus delictie*-nya berada di tempat dimana tindak pidana itu dilakukan. Sedangkan penyidik berpendapat bahwa kasus tindak pidana *hacking website* Partai Golkar tersebut dapat dilimpahkan ke Kejaksaan Tinggi Jakarta dan disidangkan di Jakarta karena korban dan para saksi banyak yang berada di Jakarta. Selain itu, akibat yang ditimbulkan berupa rusaknya *hard disk server website* Partai Golkar yang ditempatkan di PT Master Web Network terletak pada PT Telkom Kandatel

Jakarta Barat.

Menurut *Black's Law Dictionary* (2004), *locus delictie* diartikan sebagai tempat dimana suatu tindak pidana terjadi; tempat dimana kejadian (tindak pidana) dapat menyebabkan pelaku harus bertanggung jawab. Sedangkan menurut Utrecht (1997: 234-238), untuk menyelesaikan persoalan tentang *locus delictie,* ilmu hukum pidana bersama-sama dengan yurisprudensi hukum pidana telah membuat tiga macam teori, yaitu teori perbuatan materiil, teori alat yang dipergunakan dan teori akibat. Dalam teori perbuatan materiil, penentuan *locus delictie*nya adalah tempat dimana pembuat melakukan segala perbuatan yang dapat mengakibatkan delik yang bersangkutan. *Locus delictie* adalah tempat dimana perbuatan yang perlu ada supaya delik dapat terjadi. Berbeda dengan teori alat yang dipergunakan, menurut teori ini, delik dilakukan di tempat dimana alat yang dipergunakan itu menyelesaikannya. Sedangkan menurut teori akibat, yang menjadi *locus delictie* adalah tempat akibat terjadi.

Menurut E. Y. Kanter dan S. R. Sianturi (1982: 113-115), teori *locus delictie* terdiri dari empat teori dengan adanya satu penambahan teori, yaitu: teori tindakan badaniah, teori tempat bekerjanya alat, teori akibat dari tindakan dan teori berbagai tempat tindak pidana untuk menentukan *locus delictienya* adalah gabungan dari ketiga-tiganya atau dua diantara ajaran-ajaran tersebut di atas. Dengan demikian dapat dilihat bahwa penyidik telah mendasarkan pendapatnya mengenai *locus delictie* dilihat dari akibat tindak pidana yang dilakukan, yaitu mengakibatkan rusaknya *hard disk server website* Partai Golkar yang *hosting*-nya pada PT Telkom Kandatel Jakarta Barat. Lebih lanjut pendapat penyidik tersebut dilatarbelakangi juga dari hasil diskusi dengan ahli hukum pidana dan hasil pemeriksaan ahli dimana dalam pemeriksaan, saksi ahli menyampaikan bahwa untuk menentukan *locus delictie* dalam kasus tindak pidana *hacking website* Partai Golkar dapat dilihat 3 (tiga) tolok ukur yang perlu dilihat, yaitu: komputer sebagai alat (*computer as a tool*); komputer sebagai tempat penyimpanan (*computer as a storage*); dan komputer sebagai target (*computer as a target*).

Terhadap peristiwa tindak pidana *hacking website* Partai Golkar, perbuatan yang dilakukan oleh tersangka termasuk dalam kriteria komputer sebagai target. Hal ini berarti lokasi terjadinya tindak pidana adalah lokasi *server* tersebut

ditempatkan. Namun karena sifat *cybercrime* sering lintas batas (*borderless*) maka beberapa negara menggunakan prinsip perlindungan korban (*victim protection*). Begitu pula prinsip *Victim Protection* di mana domisili pihak yang dirugikan merupakan yurisdiksi yang diutamakan dalam pelaksanaan proses hukumnya. Sejalan dengan peristiwa *website* Partai Golkar, yurisdiksi hukumnya adalah di mana pihak yang dirugikan berdomisili. Dalam kasus ini adalah di mana lokasi *server* ditempatkan (*computer as a target*). Hal ini berarti yurisdiksi hukum yang digunakan berada di PT Master Web Network pada PT Telkom Kandatel Jakarta Barat yang beralamat di Jl. S. Parman Kav. 8, Jakarta Barat. Selain itu, dalam kasus ini juga digunakan sistem *Victim Protection* dimana domisili pihak yang dirugikan merupakan yurisdiksi yang diutamakan. Berdasarkan uraian tersebut di atas, penyidik menentukan bahwa *locus delictie hacking website* Partai Golkar adalah di PT Telkom Kandatel Jakarta Barat yang beralamat Jl. S. Parman Kav. 8, Jakarta Barat.

Hal lain yang terkait dengan penentuan *locus delectie* adalah masalah kompetensi relatif (kewenangan mengadili) kasus tersebut. Sebagaimana masalah *locus delictie* yang timbul, permasalahan mengenai kompentensi relatif ini juga menimbulkan perbedaan dimana kejaksaan meminta supaya persidangan kasus tindak pidana *hacking website* Partai Golkar di Batam, sedangkan penyidik beranggapan bahwa kompetensi relatif kasus tersebut berada di Jakarta karena di Jakarta terdapat banyak saksi dan *locus delictie*nya juga berada di Jakarta.

Darwan Prinst (1998: 128) Teori Kompetensi Pengadilan (kewenangan mengadili) terdiri dari kompetensi absolut dan kompetensi relatif. kompetensi absolut menyangkut kewenangan dari jenis pengadilan yang berwenang untuk mengadili perkara itu. Misalnya apakah menjadi wewenang Pengadilan Negeri, Pengadilan Agama, Pengadilan Tata Usaha Negara atau Pengadilan Militer. Sedangkan kompetensi relatif menyangkut wewenang pengadilan mana (sejenis) untuk memeriksa perkara itu. Misalnya apakah menjadi wewenang Pengadilan Negeri Medan atau Pengadilan Negeri Kabanjahe untuk memeriksa perkara itu.

Dari ketentuan Pasal 84 ayat (1) dan (2) KUHAP[143], berarti bahwa

---

[143]Pasal 84 ayat (1) dan (2) KUHP

1) "Pengadilan Negeri berwenang mengadili segala perkara mengenai tindak pidana yang

kewenangan mengadili suatu Pengadilan Negeri adalah didasarkan pada tempat perkaranya (*locus delictie*) dalam daerah hukum atau Pengadilan Negeri dimana terdakwa bertempat tinggal, berdiam terakhir, di tempat ia ditemukan. Namun sebagian besar saksi yang dipanggil lebih dekat pada tempat Pengadilan Negeri dimana perkara terjadi.

Dengan demikian, dapat dilihat bahwa pendapat penyidik mengenai Kompetensi Relatif atau Pengadilan Negeri mana yang berwenang telah menginterpretasikan Pasal 84 ayat (1) dan (2) KUHAP yang mengatur mengenai kompetensi relatif atau pengadilan negeri mana yang berwenang, dengan menempatkan Pengadilan Negeri Jakarta Barat sebagai kompetensi relatifnya.

4.2.4.4 Presentasi Barang Bukti

Barang bukti yang dikumpulkan dari penyidikan adalah barang bukti yang didalamnya terdapat data-data digital (elektronik), yang dalam sistem hukum Indonesia tidak dikenal atau diakui sebagai barang bukti sehingga hal ini membuat kesulitan tersendiri. Hal ini sesuai juga dengan apa yang disampaikan oleh Edmon Makarim (2005: 455) dimana kesulitan mendasar penggunaan bukti elektronik dalam proses pembuktian perkara pidana, khususnya mengenai tindak pidana dengan menggunakan komputer, yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik ini di dalam perundang-undangan. Padahal dalam kejahatan komputer bukti yang akan mengarahkan suatu peristiwa pidana adalah berupa data-data elektronik baik yang berada di dalam komputer itu sendiri (*hard disc/compact disc/flash disc/floppy disc*) atau yang merupakan hasil *print out*, atau dalam bentuk lain berupa jejak dari suatu aktivitas penggunaan komputer.

Andi Hamzah (1996: 257) mengatakan bahwa pembuktian tentang benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam acara pidana. Dalam hal ini, hak asasi manusia dipertaruhkan. Bagaimana akibatnya jika seseorang yang didakwa dinyatakan

---

dilakukan dalam daerah hukumnya;

2) Pengadilan Negeri yang di dalam daerah hukumnya terdakwa bertempat tinggal, berdiam terakhir, di tempat ia diketemukan atau ditahan, hanya berwenang mengadili perkara terdakwa tersebut, apabila tempat kediaman sebagian besar saksi yang dipanggil lebih dekat pada tempat pengadilan negeri itu daripada tempat kedudukan pengadilan negeri yang di dalam daerahnya tindak pidana itu dilakukan."

terbukti melakukan perbuatan yang didakwakan berdasarkan alat bukti yang ada disertai keyakinan hakim, padahal tidak benar. Dari uraian tersebut dapat disimpulkan bahwa betapa pentingnya barang bukti digital dalam pembuktian perkara pidana yang menggunakan komputer atau jaringan komputer yang nantinya sangat bermanfaat dalam proses pembuktian di persidangan terutama berkaitan dengan alat bukti yang lain. Darwan Prinst (1998: 134) menyebutkan mengenai empat teori tentang pembuktian, yaitu: teori pembuktian positif, teori pembuktian negatif, teori pembuktian bebas dan teori pembuktian berdasarkan keyakinan.

Menurut teori pembuktian positif, bahwa bersalah atau tidaknya terdakwa tergantung sepenuhnya kepada sejumlah alat bukti yang telah ditetapkan terlebih dahulu. Keyakinan hakim menurut teori ini harus dikesampingkan. Teori ini berkembang pada abad pertengahan, dan kini jarang diterapkan dalam praktik di pengadilan. Teori pembuktian negatif, hakim hanya boleh menjatuhkan pidana apabila sedikit-dikitnya 2 (dua) alat bukti yang telah ditentukan dalam undang-undang ada, ditambah keyakinan hakim yang diperoleh dari adanya alat-alat bukti itu. Bahwa terdakwa dapat dipersalahkan melakukan tindak pidana yang didakwakan kepadanya, apabila alat-alat bukti itu ada ditambah keyakinan hakim sendiri.

Penggunaan teori pembuktian negatif dalam KUHAP tersebut, terlihat jelas dari Pasal 183 KUHAP yang mengatur bahwa untuk menentukan pidana kepada terdakwa harus kesalahannya terbukti dengan sekurang-kurangnya dua alat bukti yang sah dan atas keterbuktian dengan sekurang-kurang dua alat bukti yang sah sebagaimana diatur dalam Pasal 184 KUHAP[144], hakim "memperoleh keyakinan" bahwa tindak pidana benar terjadi dan terdakwalah yang bersalah melakukannya.

Keberadaan barang bukti sangat penting dalam mencari dan menemukan kebenaraan materiil serta menjadi bagian yang saling terkait dengan alat bukti. Hal ini termasuk bukti *digital* yang berperan penting dalam kejahatan komputer.

Dalam mengungkap kasus tindak pidana *hacking website* Partai Golkar,

---

[144]Pasal 184 KUHAP disebutkan bahwa alat bukti yang sah dalam sistem hukum Indonesia adalah: keterangan saksi; keterangan ahli; surat; petunjuk dan keterangan terdakwa. Hal ini berarti terhadap keberadaan bukti digital tidak dikenal sebagai alat bukti dalam sistem hukum di Indonesia.

penyidik berupaya mencari jalan keluar bagaimana cara mempresentasikan bukti *digital* yang didapat agar dapat diterima dalam hukum acara pidana yang berlaku di Indonesia meskipun belum ada peraturan yang mengakomodir data-data digital sebagai barang bukti. Permasalahan penerimaan bukti digital sebagai barang bukti tidak hanya terbatas supaya diterima dalam proses pembuktian baik pada tahap penyidikan maupun persidangan namun yang tidak kalah pentingnya adalah bagaimana bukti-bukti berupa data-data digital yang ada dapat diterima dan dimengerti oleh penuntut umum serta hakim.

Dalam pelaksanaannya penanganan kasus tindak pidana *hacking website* Partai Golkar, masalah mempresentasikan barang bukti digital, tidak terlepas dari keragu-raguan atas bukti digital oleh penuntut umum. Penuntut umum mempermasalahkan dan meragukan kebenarannya atas barang bukti digital karena belum diakomodir dalam sistem hukum di Indonesia. Oleh karena itu penyidik terus melakukan diskusi untuk menyusun strategi mengenai bukti yang dapat digunakan dalam tindak pidana *hacking*. Antara penyidik dan penuntut umum terdapat perbedaan interpretasi mengenai barang bukti *digital*. Hal ini dapat dilihat dari pernyataan Pamen dalam wawancara berpedoman berikut ini:

> *"Sementara kami masih mencari format lain bahwa kejahatan yang dilakukan tersangka adalah memasuki jaringan milik orang lain secara melawan hukum. Hal ini pun menjadi kesulitan karena ketika dijelaskan memasuki jaringan milik orang lain ini akan bisa tergambarkan pada hasil pemeriksaan digital evidence yang ada oleh laboratorium komputer forensic. Ketika dua pidana ini disandingkan ini adalah barang baru untuk bisa diterima oleh pihak kejaksaan. Karena dalam hal ini dari pihak kejaksaan pun masih bersikeras untuk tidak bisa menerima berkas ini dengan sempurna. Hanya dua pasal, dua perundangan yang bersanding yang sama-sama tidak menyentuh kedua-duanya. Kalaupun itu dapat diterima itu harus dengan kemampuan penyidik untuk meyakinkan rekan jaksa untuk melihat bentuk kejahatan ini adalah sempurna pernah dilakukan atau dalam hal ini kerusakan yang terjadi tidak melulu pada barang, bentuk-bentuk seperti ini berakhir pada pada jika saja alat bukti yang ada tidak bisa diangkat untuk meyakinkan peran tersangka bahwa benar-benar dirinya telah melakukan kejahatan tersebut, tentu hal ketika penerimaan berkas itu menjadi tidak bisa diterima. Sedangkan yurisprudensi yang ada yang bisa diangkat untuk kejahatan cybercrime belum banyak. Pada akhirnya adalah kami melihat bentuk-bentuk kejahatan komputer cybercrime banyak banyak hal yang ditemui penyidik terutama dalam mengangkat fakta-fakta hukum yang ada dalam bentuk*

berkas perkara sehingga dapat diterima". (WBIS04)

Hal tersebut dilakukan agar barang bukti digital dapat diterima oleh penuntut umum dan dapat digunakan dalam mendukung keyakinan seorang hakim dalam memutuskan perkara. Penyidik menyelesaikannya dengan mengubah data-data yang tadinya masih berupa data-data digital menjadi semacam bukti surat atau ditampilkan dalam bentuk *hard copy* berupa hasil *print out* sehingga dapat diterima oleh penuntut umum maupun hakim. Upaya penyidik agar barang bukti digital dapat diterima, penyidik juga meminta keterangan ahli dan keterangan saksi-saksi lain yang dapat mendukung pembuktian tersebut.

4.2.5 Pihak-pihak Luar yang Terlibat dalam Proses Penyidikan

Pihak yang berkepentingan (*stakeholders*) adalah kelompok atau individu yang secara langsung atau tidak langsung mempengaruhi cara organisasi berusaha mencapai sasarannya. Pihak yang berkepentingan tersebut terbagi menjadi pihak berkepentingan eksternal (*external stakeholders*), yaitu kelompok atau individu dalam lingkungan eksternal sebuah organisasi yang mempengaruhi aktivitas organisasi tersebut. Pihak berkepentingan internal (*internal stakeholders*) adalah kelompok atau individu yang merupakan bagian dari lingkungan organisasi dimana seorang pemimpin tetap bertanggung jawab atas orang atau kelompok tersebut.

Menurut Rhenald Kasali (1994: 75-76), *external stakeholders* adalah unsur-unsur yang berada di luar kendali organisasi (*uncontrollable*). Dalam organisasi, setiap pemimpin organisasi selalu dibekali dengan teknik untuk mendesain organisasinya sesuai dengan keadaan lingkungan eksternalnya. Unsur dalam lingkungan luar dapat dilihat dalam dua hal, yaitu: kompleksitas lingkungan dan stabilitas lingkungan.

Unsur kompleksitas lingkungan dapat diukur dari banyaknya pihak di luar organisasi yang perlu mendapat perhatian organisasi karena pengaruhnya. Semakin banyak aktor yang perlu diperhatikan, berarti kompleks. Semakin sedikit, berarti sederhana. Sedangkan unsur stabilitas lingkungan diukur dari

perubahan yang telah ditimbulkan. Bila terlalu sering terjadi perubahan peraturan, perubahan peran aktor dalam lingkungan lainnya, maka lingkungan dikatakan tidak stabil (labil). Keadaan sebaliknya disebut stabil.

Dalam lingkungan yang stabil, organisasi cenderung didesain mekanistis, artinya cenderung mengandalkan peraturan, prosedur, dan lebih birokratis. Hampir setiap anggota mempunyai deskripsi pekerjaan dan tanggung jawab yang didefinisikan dengan jelas. Sedangkan dalam keadaan labil, tidak ada standar pekerjaan, setiap orang diharapkan dapat mengerjakan pekerjaan lainnya secara serabutan.

Dalam melaksanakan proses penyidikan, keberhasilan penyidik Unit V *IT & Cybercrime* dalam mengungkap kasus tindak pidana *hacking website* Partai Golkar tidak hanya berdasarkan kemampuan dan kinerja penyidik namun juga didukung oleh pihak-pihak luar yang memberikan pengaruh langsung maupun tidak langsung yang cukup signifikan dalam proses penyidikan serta keberhasilan pengungkapan kasus tersebut. Pihak-pihak luar tersebut adalah: Partai Golkar, *Internet Service Provider* dan informan.

Pengaruh yang diberikan oleh pihak-pihak di luar penyidik dapat terlihat dari adanya informasi maupun bukti-bukti yang diperoleh dan dikumpulkan oleh penyidik dari pihak-pihak di luar penyidik tersebut. Dengan diperolehnya informasi maupun bukti dari pihak luar tersebut, penyidik dapat mengambil perencanaan maupun pelaksanaan atas rencana yang telah disusun oleh penyidik dalam proses penyidikan, seperti langkah awal dimulainya penyidikan, tempat-tempat yang dicurigai, tempat dilakukannya penyerangan sampai dengan diketahuinya identitas tersangka dan dilakukannya upaya-upaya penindakan.

4.2.5.1 Partai Golkar

Partai Golkar sebagai pemilik *website* Partai Golkar merupakan korban tindak pidana *hacking* yang dilakukan oleh tersangka Iqra Syafaat. Partai Golkar adalah pihak luar pertama yang memberikan pengaruh dalam proses penyidikan karena berawal dari hal yang disampaikan oleh Partai Golkar, penyidik dapat merencanakan proses penyidikan dan bukti apa yang mesti disertakan oleh Partai Golkar dalam pelaksanaan pelaporan guna kepentingan penyidikan. Dalam diskusi maupun pembuatan laporan polisi, Partai Golkar sangat membantu dengan

menyampaikan uraian kejadian dan memberikan barang bukti.

4.2.5.2 *Internet Service Provider* (*ISP*)

Internet Service Provider adalah badan usaha yang menyediakan layanan koneksi internet. *Internet Service Provider* untuk di Indonesia, ditangani oleh APJII. Perusahaannya biasa disebut dengan *ISP*. Hal-hal yang biasa dilakukan oleh *ISP* tersebut ialah pemberian *IP Address* publik kepada para pelanggannya beserta perihal pengaturan *bandwidth*[145]. Isi dari *ISP* adalah orang dan peralatan-peralatan yang diperlukan untuk memberikan pelayanan koneksi internet kepada pelanggan-pelanggannya. Peralatan-peralatan tersebut biasanya berupa *server*, *router*, peralatan-peralatan untuk koneksi ke pelanggan-pelanggannya dan peralatan-peralatan interkoneksi mereka ke *upstream*. Biasanya *ISP* bekerja sama dengan operator jaringan dalam menjalankan usahanya. Hal ini disebabkan terdapat *ISP* yang tidak memiliki peralatan jaringan.

Dalam kasus tindak pidana *hacking website* Partai Golkar ini, *ISP* selaku pihak di luar ikut membantu dalam keberhasilan penyidikan dalam mengungkap pelaku tindak pidana *hacking* sebagaimana terungkap dalam proses penyidikan bahwa melalui kerjasama dengan *ISP* diketahui *IP Address* penyerang.

4.2.5.3. Informan

Informan selaku pihak yang berada di luar penyidik ikut berperan juga dalam proses penyidikan tindak pidana *hacking website* Partai Golkar. Informan berperan dalam memberikan informasi kepada penyidik mengenai pelaku dari tindak pidana tersebut.

Dalam melakukan upaya penyidikan kasus tindak pidana *hacking website* Partai Golkar, penyidik melakukan melakukan *virtual undercover* atas *nickname* yang ditemukan dari data *log files* dengan dibantu oleh komunitas *hacker* yang ada di Batam dengan penyamaran melalui *chatting* terhadap *nick name* pelaku. Melalui *chatting* penyidik mengetahui *email* pelaku dan tersangka mengakui bahwa dirinya adalah *hacker website* Partai Golkar. Dari penyidikan lebih lanjut

---

[145] *Bandwidth* dapat diartikan sebagai jalan raya. Semakin besar jalannya, aktivitas internet akan semakin lancar dan *bandwith* ini ditentukan dengan ukuran *kbps* (*kilobit per second*). *Kbps* merupakan ukuran kecepatan transfer data, bahkan sekarang sudah dalam hitungan *mbps* (*mega bit per second*) atau bahkan Giga.

diketahui bahwa identitas pelaku adalah Iqra Syafaat alias Nogra alias *singapore_bm@yahoo.com*.

Hal ini berarti komunitas *hacker* tersebut ikut berperan dalam proses pengungkapan pelaku tindak pidana *hacking website* Partai Golkar. Dalam hal ini, komunitas *hacker* dapat dikategorikan sebagai informan. Informasi yang diperoleh dari komunitas *hacker* sangat berguna bagi pihak penyidik.

4.3 Manajemen Penyidikan Tindak Pidana *Hacking Website* Partai Golkar

Dalam pembahasan Bab III sebelumnya telah dijelaskan mengenai manajemen penyidikan tindak pidana *hacking*. Dalam sub bab ini akan dibahas mengenai bagaimana manajemen penyidikan tersebut diterapkan dalam penyidikan kasus tindak pidana *hacking website* Partai Golkar.

Penyidikan kasus tindak pidana *hacking website* Partai Golkar merupakan serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti, yang dengan bukti itu membuat atau menjadi terang tindak pidana yang terjadi serta sekaligus menemukan tersangkanya atau pelaku kasus tindak pidana *hacking website* Partai Golkar sehingga dapat menghasilkan pelimpahan berkas perkara ke penuntut umum atau apabila tidak dapat memenuhi unsur tindak pidana maka akan ditetapkan penghentian penyidikan.

Pelaksanaan kegiatan penyidikan dapat dilaksanakan secara optimal apabila penyidik senantiasa memperhatikan syarat-syarat, teknik maupun sasaran penyidikan secara benar sebagaimana diatur dalam KUHAP dan Juklap Tentang Penyidikan yang berlaku dalam lingkungan Polri berdasarkan Surat Keputusan Kapolri. Pelaksanaan penyidikan kasus tindak pidana *hacking website* Partai Golkar tersebut pada prinsipnya harus tetap berpedoman pada ketentuan hukum acara yang berlaku dan merujuk pada sistem operasional yang berlaku di Polri seperti pedoman penyidikan tindak pidana, pedoman penyelenggaraan administrasi penyidikan dan lain-lain.

Sebagaimana telah dijelaskan di sub bab 4.2 bahwa dalam proses

penyidikan kasus tindak pidana *hacking website* Partai Golkar yang terdiri dari proses penyelidikan, penindakan, dan pemeriksaan kasus tindak pidana *hacking website* Partai Golkar serta penyelesaian dan penyerahan berkas perkara ke penuntut umum yang menjadi tujuan penyidikan. Selain tujuan pemberkasan perkara, dalam penyidikan kasus tindak pidana *hacking website* Partai Golkar, penyidik juga dituntut agar dapat mendukung proses persidangan. Pada tahap penuntutan, penyidik diharapkan dapat memberikan pemahaman kepada penuntut umum melalui koordinasi antara penyidik dengan penuntut umum mengenai penentuan *locus delictie* dan penggunaan bukti digital. Pada proses persidangan, penyidik diharapkan dapat menjadi saksi verbalisan serta turut menyiapkan saksi dan ahli.

Manajemen penyidikan tindak pidana *hacking* sangat diperlukan untuk dapat mencapai tujuan penyidikan. Akan tetapi dalam upaya pencapaian tujuan penyidikan kasus tindak pidana *hacking website* Partai Golkar mengalami kesulitan-kesuitan mengenai ketentuan hukum baik ketentuan hukum formil maupun materiil serta kegiatan teknis dalam pelaksanaan penyidikan sebagaimana telah dijelaskan sebelumnya. Pelaksanaan penyidikan terhadap kasus tindak pidana *hacking website* Partai Golkar merupakan kerja tim penyidik dengan dukungan tim laboratorium forensik komputer. Proses penyidikan terhadap kasus tindak pidana *hacking website* Partai Golkar berhubungan erat dengan pihak-pihak lainnya seperti pihak Golkar sebagai korban, pelaku, saksi, penasehat hukum dan penuntut umum sebagaimana telah dijelaskan sebelumnya. Oleh karena itu, dalam pelaksanaan penyidikan tindak pidana *hacking website* Partai Golkar diperlukan suatu sistem manajemen yang mampu merubah ide-ide yang dimiliki atau tersedia menjadi serangkaian aksi atau tindakan dalam melakukan penyidikan.

Suatu proses manajemen terdiri dari fungsi-fungsi manajemen dimulai dengan tindakan merencanakan, mengorganisasikan, memimpin dan mengendalikan. Apabila dikaitkan dengan proses penyidikan maka tahapan dalam proses manajemen dengan merujuk pada konsep siklus manajemen yang kemukakan oleh Butler dimaksudkan sebagai suatu cara yang terencana, terkoordinasi, dan teruji untuk memaksimalkan baik efisiensi dan produktivitas

dalam melaporkan serta menginvestigasi berbagai tindak pidana dalam suatu praktek manajemen yang efektif.

Aktualisasi manajemen penyidikan dalam kasus tindak pidana *hacking website* Partai Golkar dilaksanakan melalui mobilisasi seluruh sumber daya yang tersedia baik personil penyidik, infrastruktur, finansial secara terencana, terorganisir, dan terkendali untuk kepentingan pelaksanaan proses penyidikan yang maksimal dalam mencapai tujuan penyidikan. Dipandang dari perspektif fungsi manajemen penulis melihat bahwa dalam proses penyidikan kasus tindak pidana *hacking website* Partai Golkar terdapat penerapan prinsip-prinsip dan pendayagunaan fungsi manajemen dalam proses penyidikan yang meliputi: proses penerimaan laporan (*input*), penugasan, perencanaan, pelaksanaan dan penyesuaian, pengendalian dan evaluasi dalam proses penyidikan kasus tindak pidana *hacking website* Partai Golkar.

Proses penyidikan kasus tindak pidana *hacking website* Partai Golkar dimulai dengan proses pelaporan yang dibuat oleh Partai Golkar sehingga proses manajemen dapat dimulai dari proses penerimaan laporan sampai dengan pengendalian dan evaluasi. Sebagaimana diungkapkan oleh Pama dalam wawancara berpedoman berikut ini:

> *"Menurut pendapat saya manajemen adalah keseluruhan tindakan yang dilakukan oleh seseorang dalam inilah pemimpin untuk menggerakkan anak buahnya mengorganisasikan kelompoknya untuk mencapai suatu tujuan yang diharapkan dan diterapkan oleh kelompok nya itu secara bersama-sama....Kegiatan yang dilakukan bisa melalui dengan cara perencanaan, kemudian pengorganisasian, kemudian pelaksanaan dan pengendalian sebagai evaluasi ini."* (WBIS 01A)

> *"Manajemen penyidikan utamanya saya ngalamin juga pada saat kita melakukan penyidikan deface partai Golkar ini yang jelas harus ada pengorganisasian jadi pada saat penyidikan telah terbentuk tim siapa yang harus melakukan penyidikan ini jadi ada pengorganisasian ada pengaturan yang disampaikan pada penyidik namun begitu terutama adalah perencanaan orang mengatakan perencanaan adalah sukses awal dari suatu organsiasi. Sebelum kita melakukan penyelidikan telah disampaikan sebelumnya jauh sebelum melakukan penyelidikan telah ada penyampaian dari pimpinan pada saat itu bahwa pihak Golkar akan datang untuk membuat laporan polisi berkaitan dengan deface website partai Golkar sehingga telah dilakukan perencanaan awal walaupun pihak Golkar nya*

sendiri belum datang penyidik telah berkumpul merencanakan apa yang akan dilakukan sebelum pihak partai Golkar datang kekantor membuat laporan sehingga apa yang akan dilakukan selanjutnya sudah tergambar karena sudah ada perencanaan sebelumnya selain itu fungsi-fungsi manajeman yang lain ada kontroling yang dilakukan oleh Kanit pada saat itu melakukan pengecekan selalu sampai sejauh mana penyidikan yang telah dilakukan termasuk mengecek administrasi penyidikan yang telah dibuat oleh penyidik jadi penyidik dalam melakukan tugas-tugasnya tidak pernah dalam artian melakukan sendiri jadi dia melakukan sendiri dan tidak tau harus melapor kepada siapa tapi karena pada saat itu sudah berencana dengan benar penyidik ini orang-orang ini melakukan ini dan melapornya kepada siapa jadi sudah ada pembagian tugas atau boleh dikatakan bentuk dari staffing jadi penyidik sendiri telah dibagi siapa melakukan apa dan tanggung jawab kepada siapa."

Demikian juga diungkapkan dalam wawancara berpedoman dengan Pamen, berikut ini:

"Menurut saya sudah suatu keharusan dan yang mau tidak mau dan tidak bisa ditawar-tawar lagi dalam melakukan penyelidikan atau penyidikan kasus hacking harus ada manajemen yang jelas runtut dan Focus jadi dan juga dengan persyaratan-persyaratan tertentu ya." (WBIS 10A)

"Yang saya tahu dari kegiatan penyidikan perusakan situs partai Golkar tersebut, manajemen manajemen sudah betul-betul diterapkan oleh kepala unit waktu itu adalah setelah mendapatkan informasi dari korbannya, dalam hal ini partai Golkar sendiri, kemudian." (WBIS 03A)

4.3.1 Penerimaan Laporan (*Input*)

Penyidikan tindak pidana kasus tindak pidana *hacking website* Partai Golkar dilaksanakan setelah diketahui bahwa suatu peristiwa yang terjadi merupakan tindak pidana. Suatu tindak pidana dapat diketahui melalui adanya laporan, pengaduan dan inisiatif polisi sendiri. Dalam melakukan rangkaian proses hukum terhadap kasus pidana, penyidik terlebih dahulu menerima laporan dan atau pengaduan dari masyarakat atau korban di SPK sebagaimana telah diuraikan dalam bab III sebelumnya.

Dalam kasus tindak pidana *hacking website* Partai Golkar, penyidik terlebih dahulu menerima laporan dari perwakilan Partai Golkar oleh Ir. Fayakhun dan Zulhendri Hasan, S.H., M.H yang dilakukan setelah bertemu dan

berdiskusi terlebih dahulu dengan Unit V *IT & Cybercrime*. Diskusi tersebut membahas rencana pelaporan yang akan dilakukan oleh Partai Golkar, mengingat jenis kejahatan *hacking* belum secara tegas diatur dalam ketentuan yuridis. Diskusi tersebut tidak diatur dalam ketentuan yuridis tetapi hanya merupakan kebijakan dan inisiatif pelapor dan Kanit V *IT & Cybercrime*. Dalam diskusi tersebut disepakati bahwa tindakan *hacking Website* Partai Golkar dapat dikategorikan sebagai suatu tindakan pidana, dan proses penyidikan terhadapnya seyogyanya tetap harus dilakukan menurut ketentuan hukum yang berlaku sehingga proses penyidikan dapat dilanjutkan. Hasil diskusi tersebut menjadikan proses pembuatan laporannya menjadi lebih cepat sehingga terhadap tindak pidana tersebut segera dapat dilakukan proses penyidikan. Hal ini menunjukkan bahwa penanganan kasus oleh Unit V *IT & Cybercrime* dilakukan secara lebih responsif.

4.3.2 Penugasan

Berdasarkan laporan polisi tersebut di atas, Kanit *V IT & Cybercrime* segera menindaklanjutinya dengan menerbitkan Surat Perintah Tugas No.Pol.SP.Gas/145/VII/2006/Dit II Eksus tertanggal 17 Juli 2006, yang memerintahkan kepada 16 (enam belas) anggota Unit V *IT & Cybercrime* untuk melakukan **penyelidikan dan penyidikan** terhadap tindak pidana di bidang telekomunikasi dan perusakan terhadap tampilan *website* Partai Golkar. Penugasan tim penyidik dengan menerbitkan surat perintah tugas yang disusul dengan surat perintah penyidikan merupakan proses lanjutan dari laporan yang telah diterima dan segera untuk ditindak lanjuti.

4.3.3 Perencanaan Penyidikan

Perencanaan dapat dipahami sebagai apa yang dilakukan sebelum membuat suatu keputusan atau melaksanakan tindakan. Perencanaan merupakan suatu proses persiapan: pengumpulan informasi, pertimbangan atas berbagai alternatif serta perkiraan atas akibat-akibat dari berbagai alternatif. Dikaitkan dengan penyidikan, kegiatan perencanaan merupakan kegiatan awal untuk menentukan

langkah-langkah apa yang akan dilakukan dan menjadi sukses awal dari proses penyidikan. Perencanaan penyelidikan merupakan tahap menentukan target penyidikan dan persiapan yang diperlukan dalam penyidikan. Dalam proses penyidikan kasus tindak pidana *hacking website* Partai Golkar, proses perencanaan dapat terlihat dalam Surat Perintah Penyidikan No. Pol.: SP.Sidik/80/VII/2006/Dit II Eksus pada tanggal 17 Juli 2006 oleh Kanit V *IT & Cybercrime*. Salah satu isi dari Surat Perintah Penyidikan tersebut adalah memerintahkan kepada penyidik untuk membuat rencana penyidikan atas kasus tindak pidana *hacking website* Partai Golkar serta melaporkan setiap perkembangan pelaksanaan penyidikan tindak pidana pada kesempatan pertama kepada pimpinan.

Pembuatan perencanaan penyidikan disusun setelah diperoleh informasi maupun bukti dari pihak luar karena dalam perencanaan akan menjabarkan apa yang harus dilakukan dalam penyidikan dan kapan akan dilaksanakan. Perencanaan tersebut meliputi langkah awal dimulainya penyidikan, tempat-tempat yang dicurigai, tempat dilakukannya penyerangan sampai dengan diketahuinya identitas tersangka dan dilakukannya upaya-upaya penindakan. Dari hasil wawancara berpedoman dengan Pama (WBIS 01A) mengutarakan bahwa perencanaan penyidikan pun sudah dilakukan sebelum pelaporan diterima dari pelapor, karena sebelum Partai Golkar melapor, sudah terlebih dahulu melakukan konsultasi dengan unit V *IT & Cybercrime*. Dari hasil konsultasi tersebut, penyidik telah dapat mempersiapkan perencanaan penyidikan atas kasus tindak pidana *hacking website* Partai Golkar, seperti dalam kutipan wawancara berikut ini:

> *"Sebelum kita melakukan penyelidikan telah disampaikan sebelumnya jauh sebelum melakukan penyelidikan telah ada penyampaian dari pimpinan pada saat itu bahwa pihak Golkar akan datang untuk membuat laporan polisi berkaitan dengan deface website partai Golkar sehingga telah dilakukan perencanaan awal walaupun pihak Golkar nya sendiri belum datang penyidik telah berkumpul merencanakan apa yang akan dilakukan sebelum pihak partai Golkar datang kekantor membuat laporan sehingga apa yang akan dilakukan selanjutnya sudah tergambar karena sudah ada perencanaan."* (WBIS 01A)

Dalam penanganan kasus tindak pidana *hacking website* Partai Golkar menurut informan dari unit V *IT & Cybercrime*, fungsi manajemen dalam hal perencanaan penyidikan tersebut sudah diterapkan walaupun belum diterapkan secara maksimal. Hal ini terjadi karena pada saat perencanaan tidak semua penyidik mengetahui kasus tersebut. Dalam perencanaan penyidikan dibagi tugas, tanggung jawab dan pertanggungjawaban sehingga setiap penyidik yang terlibat mengerti dan memahami akan tugas dan tanggung jawabnya dalam proses penyidikan sebagaimana diungkapkan oleh seorang Pama dalam wawancara berpedoman berikut ini:

> *"Yang perlu dibenahi dalam manajemen didalam hacking saya pikir yang paling mendasar sekali ada di bidang perencanaan kalau kita harus bicara dibidang manajer pak, yang paling mendasar adalah perencanaan karena itu memang bentuk alasnya dasarnya dia berdiri, nah selama ini yang kita rasakan karena tim kita juga banyak atau ataupun masih kesulitan tentang kasus hacking jadi yang dalam hal perencanaan pembagian tugasnya juga mungkin masih secara umum tidak sangat spesifik."* (WBIS 02A)

Tujuan diberikannya Surat Perintah Tugas tersebut sejalan dengan tujuan dari organisasi Unit V *IT & Cybercrime*, yaitu melaksanakan fungsi penyidikan tindak pidana *hacking* yang dianggap sebagai salah satu jenis tindak pidana *IT & Cybercrime*. Berdasarkan Surat Perintah Tugas tersebut, anggota yang diperintahkan untuk melakukan upaya penyelidikan dan penyidikan atas tindak pidana yang dilaporkan oleh Partai Golkar tersebut, memperoleh wewenang untuk segera melakukan rangkaian kegiatan guna mencari keterangan dan mengumpulkan barang bukti sehingga tim penyelidik tersebut mampu mempersiapkan semaksimal mungkin fakta-fakta, keterangan, dan bahan bukti sebagai landasan hukum untuk memulai penyidikan.

Surat Perintah Tugas No.Pol.SP.Gas/145/VII/2006/Dit II Eksus tertanggal 17 Juli 2006 dan Surat Perintah Penyidikan No. Pol.: SP.Sidik/80/VII/2006/Dit II Eksus pada tanggal 17 Juli 2006 merupakan perwujudan dari pelaksanaan administrasi penyidikan yang berlaku secara normatif. Penunjukan surat-surat tersebut dimaksudkan sebagai referensi yang secara nyata menjelaskan target penyidikan yang telah ditetapkan oleh Unit V *IT & Cybercrime* dalam

menindaklanjuti laporan polisi yang dibuat oleh Partai Golkar. Hal mana menunjukkan pula bahwa penetapan target penyidikan merupakan tahap penting yang harus dilakukan dalam proses penyidikan. Penetapan target penyidikan menunjukkan pula bahwa proses penyidikan kasus tindak pidana *hacking* tersebut telah merefleksikan proses manajemen, yaitu perumusan masalah yang merupakan tahap identifikasi sebelum proses manajemen berikutnya dapat dilaksanakan.

4.3.4 Pelaksanaan dan Penyesuaian Penyidikan

Pelaksanaan atau tahap implementasi penyidikan kasus tindak pidana *hacking website* Partai Golkar merupakan tahap eksekusi dari perencanaan yang telah dibuat sebelumnya. Pelaksanaan penyidikan dilaksanakan setelah Kanit V *IT & Cybercrime* mengeluarkan Surat Perintah Penyidikan yang ditindaklanjuti dengan pemanggilan dan pemeriksaan para saksi, pengolahan bukti digital, penindakan dan pembuatan berita acara.

Jika dalam kenyataannya ternyata kondisi lapangan berbeda dengan apa yang telah direncanakan maka akan segera dilakukan penyesuaian terhadap kondisi lapangan yang dihadapi. Hal ini dilakukan agar tujuan penyidikan dapat tercapai meskipun bergeser dari perencanaan yang sudah ditentukan lebih dahulu mengikuti kondisi lapangan. Perubahan atas perencanaan yang telah dibuat dapat dilaksanakan sepanjang masih tetap pada arah tujuan penyidikan yang akan dicapai.

Dalam pelaksanaan penyidikan kasus tindak pidana *hacking website* Partai Golkar harus didukung oleh manajemen proses penyidikan di lapangan dimana setiap personel paham dan menguasai fungsi dan tugas dari masing-masing personil dalam pelaksanaan proses penyidikan. Dalam pelaksanaan penyidikan harus dilaksanakan pengorganisasian setiap sumber daya yang dimiliki. Selain itu untuk mendukung pelaksanaan penyidikan yang efektif, harus didukung dengan biaya yang memadai.

Pengorganisasian dalam manajemen penyidikan kasus tindak pidana *hacking website* Partai Golkar telah melibatkan dan memberdayakan peran dan fungsi seluruh sumber daya yang dimiliki Unit V *IT & Cybercrime* dalam rangka

mencapai tujuan penyidikan yaitu penyerahan berkas perkara ke penuntut umum. Proses pengorganisasian tersebut mengacu pada perencanaan yang telah dibuat. Dengan instruksi dari Kanit V *IT & Cybercrime* menunjuk diantara para anggotanya siapa saja yang terlibat dalam kasus tindak pidana *hacking* Golkar tersebut. Instruksi tersebut dapat berupa instruksi tertulis (surat perintah) maupun instruksi lisan yang dilakukan melalui tatap muka antara anggota dengan Kanit dan melalui komunikasi *email* dan telepon. Dalam instruksi lisan yang dilakukan melalui tatap muka dilakukan dengan cara diskusi dan maupun langsung. Proses pengorganisasian dalam pelaksanaan penyidikan kasus tindak pidana *hacking website* Partai Golkar telah dilaksanakan dengan membagi tugas setiap anggota yang akan melakukan penyidikan, sebagaimana terlihat dalam pernyataan seorang Pama dalam wawancara berpedoman berikut ini:

> "*Manajemen penyidikan utamanya saya ngalamin juga pada saat kita melakukan penyidikan deface partai Golkar ini yang jelas harus ada pengorganisasian jadi pada saat penyidikan telah terbentuk tim siapa yang harus melakukan penyidikan ini jadi ada pengorganisasian ada pengaturan yang disampaikan pada penyidik namun begitu terutama adalah perencanaan orang mengatakan perencanaan adalah sukses awal dari suatu organsiasi. Sebelum kita melakukan penyelidikan telah disampaikan sebelumnya jauh sebelum melakukan penyelidikan telah ada penyampaian dari pimpinan pada saat itu bahwa pihak Golkar akan datang untuk membuat laporan polisi berkaitan dengan deface website partai Golkar sehingga telah dilakukan perencanaan awal walaupun pihak Golkar nya sendiri belum datang penyidik telah berkumpul merencanakan apa yang akan dilakukan sebelum pihak partai Golkar datang kekantor membuat laporan sehingga apa yang akan dilakukan selanjutnya sudah tergambar karena sudah ada perencanaan sebelumnya selain itu fungsi-fungsi manajeman yang lain ada kontroling yang dilakukan oleh Kanit pada saat itu melakukan pengecekan selalu sampai sejauh mana penyidikan yang telah dilakukan termasuk mengecek administrasi penyidikan yang telah dibuat oleh penyidik jadi penyidik dalam melakukan tugas-tugasnya tidak pernah dalam artian melakukan sendiri jadi dia melakukan sendiri dan tidak tau harus melapor kepada siapa tapi karena pada saat itu sudah berencana dengan benar penyidik ini orang-orang ini melakukan ini dan melaporrnya kepada siapa jadi sudah ada pembagian tugas atau boleh dikatakan bentuk dari staffing jadi penyidik sendiri telah dibagi siapa melakukan apa dan tanggung jawab kepada siapa....*" (WBIS 01 A)

> "*Khusus mengenai penyidikan deface defacing website partai Golkar*

seperti saya sampaikan tadi sebelum pihak Golkar datang Kanit telah membagi siapa yang akan menerima laporan yang kebetulan pada saat itu saya ditunjuk oleh Kanit bersama dengan kompol Dicky untuk menerima laporan sehingga pada saat penyidik datang kita sudah siap perintahnya pada saat itu disampaikan oleh Kanit segera membuat laporan polisi yang pada saat itu langsung kita tangani langsung dan ditanda tangani siaga jadi yang membuat kita...." (WBIS 01 A)

Dalam penanganan kasus tindak pidana *hacking website* Partai Golkar dilakukan secara paralel antara tim penyidik dan tim forensik. Penanganan kasus secara paralel terlihat dari mekanisme penyelesaian yang dilakukan oleh tim penyidik dan tim forensik. Ketika laporan kasus tindak pidana *hacking website* Partai Golkar ke Unit V *IT & Cybercrime*, penyidik akan segera melakukan proses penyidikan dan setiap barang-barang bukti yang perlu dianalisa akan segera dilimpahkan ke tim forensik komputer. Penanganan secara paralel terlihat ketika penyidik melakukan penyidikan terhadap kasus dimana terdapat barang bukti yang masih harus dianalisa oleh tim forensik, penyidik tidak menunggu hasil dari tim forensik dalam melakukan kelanjutan penyidikan. Tim penyidik langsung melakukan proses penyidikan lanjutan meskipun hasil analisa dari tim forensik belum diterima.

Selain pengorganisasian anggota dalam proses penyidikan kasus tindak pidana *hacking website* Partai Golkar, pengorganisasian juga dilakukan terhadap pihak luar yang memberikan kontribusi dalam proses penyidikan, antara lain: pihak Golkar sebagai pelapor, Warnet Barelang dan *virtual undercover* terhadap komunitas *hacker*. Pengorganisasian tersebut dilaksanakan supaya tujuan dari penyidikan tersebut dapat tercapai.

4.3.5 Pengendalian dan Evaluasi Penyidikan

Pengendalian penyidikan sebagai salah satu fungsi manajemen penyidikan tidaklah berdiri sendiri, tetapi berada atau melekat pada semua fungsi manajemen, baik pada tahap perencanaan, pengorganisasian dan pelaksanaan. Pengendalian memegang peranan penting dalam menentukan dan mengevaluasi perencanaan, pengorganisasian serta pelaksanaan penyidikan setelah penyerahan berkas perkara kepada penuntut umum.

Terhadap fungsi pengendalian dan evaluasi terhadap proses penyidikan di Unit V *IT & Cybercrime* dilaksanakan secara berjenjang dimana Kanit mengendalikan setiap anggota melalui disposisi, direktur mengawasi Kanit, Kaba mengawasi direktur sebagaimana diungkapkan oleh Pama dan Pamen dalam wawancara berpedoman berikut ini.

"*Pengawasan dilakukan oleh Kanit...*" Pama (WBIS 08 B)

"Maksudnya apa pak...Sesuai dengan kan tadi dalam unit cybercrime secara struktural kami dipimpin oleh Kanit IT dan cybercrime dimana langsung Kanit langsung penyidik sehingga sistem mekanisme pengendalian untuk Kanit kami penyidik membuat rencana tadi...." Pamen (WBIS 09A)

Dalam Unit V *IT & Cybercrime* adalah pengendalian dan koordinasi yang berjenjang yang telah diatur dalam Tugas Pokok Polri 2007.

Pelaksanaan penyidikan akan berlangsung simultan dengan pengendalian dan evaluasi. Setiap kegiatan perlu dikontrol agar tidak bertentangan dengan ketentuan hukum formil dan menyimpang terlalu jauh dengan rencana atau strategi yang telah ditetapkan atau disesuaikan.

Pengendalian dalam proses penyidikan kasus tindak pidana *hacking website* Partai Golkar terdapat prioritas-prioritas yang harus diperhatikan. Pengendalian diutamakan pada prosedur hukum dalam penyidikan yang meliputi perlindungan hak-hak tersangka, saksi dan korban maupun syarat-syarat administratif **(administrasi penyidikan).** Prioritas kedua di tekankan pada pengendalian terhadap waktu penyidikan dan biaya yang harus dikeluarkan. Terakhir, pengendalian difokuskan pada perencanaan dan pelaksanaan. Jika dalam pelaksanaan terdapat perubahan terhadap kegiatan yang sudah direncanakan, maka Kanit akan melakukan perubahan tersebut. Jika perubahan pelaksanaan tersebut tidak sesuai dengan rencana prioritas atau tidak mendekati rencana prioritas, maka Kanit akan mengendalikan penyidikan ke arah perencanaan yang sudah diprioritaskan.

Pelaksanaan fungsi manajemen penyidikan dalam pelaksanaan penyidikan kasus tindak pidana *hacking website* Partai Golkar telah dilaksanakan meskipun

tidak secara menyeluruh. Penilaian ini dapat diiihat dari proses evaluasi atas tindakan tim penyidik dalam melakukan penyidikan terutama dalam menerapkan fungsi dan prinsip manajemen. Dari hasil evaluasi terhadap pelaksanaan fungsi manajemen dalam pelaksanaan penyidikan kasus tindak pidana *hacking website* Partai Golkar perlu dilakukan perbaikan dalam penerapan fungsi manajemen. Penyidikan kasus tindak pidana *hacking website* Partai Golkar terdapat masalah pembagian tugas pada saat pelaksanaan (*execution)* penyidikan. Sehingga dengan adanya evaluasi tidak terjadi lagi saling melempar tanggungjawab antara personel dalam penangnan kasus tindak pidana *hacking* dikemudian hari. Selanjutnya yang menjadi masalah dalam proses penyidikan kasus tindak pidana *hacking website* Partai Golkar adalah masalah penganggaran, dimana anggaran terlambat diturunkan sehingga kecepatan dalam menangani kasus menjadi terlambat. Sebagaimana diungkapkan dalam wawancara berpedoman dengan seorang Pamen Unit V *IT & Cybercrime* berikut ini:

> *"Yang saya tahu dari kegiatan penyidikan perusakan situs partai Golkar tersebut, manajemen sudah betul-betul diterapkan oleh kepala unit waktu itu adalah setelah mendapatkan informasi dari korbannya, dalam hal ini partai Golkar sendiri, kemudian..."*(WBIS 03)

Dalam pelaksanakan penyidikan atas kasus tindak pidana *hacking website* Partai Golkar belum ada aturan-aturan yang jelas yang mengatur tentang *hacking* sehingga diharapkan dalam Rancangan Undang-Undang tentang informasi dan transaksi elektronik harus ada aturan-aturan tersendiri yang berkaitan dengan tindak pidana *cybercrime*. Selain itu, hal-hal yang perlu diperbaiki dalam penanganan kasus *hacking website* Partai Golkar adalah apabila kejahatannya diancam dengan hukuman di atas lima tahun lebih baik didampingi oleh kuasa hukum sejak dari awal pemeriksaan perkara.

Evaluasi terhadap tindakan penyidikan atas kasus *hacking website* Partai Golkar dapat memberikan kontribusi terhadap cara kerja penyidik Unit V *IT & Cybercrime* dalam menangani kasus yang terjadi di kemudian hari maupun penilaian terhadap kinerja penyidik secara keseluruhan maupun per individu sehingga dapat memberikan masukan bagi pengembangan sumber daya manusia penyidik Unit V *IT & Cybercrime* maupun dalam pembuatan perencanaan pada

penanganan kasus pada penanganan kasus dikemudian hari. Hasil evaluasi ini merupakan kontribusi jangka pendek bagi Unit V *IT & Cybercrime.*

Sedangkan evaluasi yang dapat menjadi kontribusi jangka panjang bagi Unit V *IT & Cybercrime* adalah yurisprudensi atas kasus tindak pidana *hacking website* Partai Golkar. Kontribusi ini dapat diperoleh melalui evaluasi terhadap putusan hakim atas kasus tindak pidana *hacking website* Partai Golkar yang dapat dijadikan arahan atau dasar, seperti dalam hal penentuan pasal, barang bukti, alat bukti digital sebagai alat bukti pada kasus yang akan terjadi di kemudian hari. Yurisprudensi ini penting dan sangat mendesak mengingat ketentuan yang mengatur tindak pidana *hacking* saat itu belum diatur secara khusus.

4.4 Faktor-faktor yang Mempengaruhi Manajemen Penyidikan

Seperti yang telah dikemukakan dalam kerangka konsep, suatu organisasi dapat dianalisis dalam empat level yaitu level individu, level group (*work unit*), level organisasi (*internal stakeholders*) dan level lingkungan eksternal (*external stakeholders*). Dari analisa ke empat level tersebut, penulis mengetahui faktor-faktor yang mempengaruhi manajemen penyidikan yaitu kepemimpinan, budaya organisasi dan *stakeholders*.

4.4.1 Analisis Pengaruh Kepemimpinan dalam Manajemen Penyidikan

Menurut Sunindhia dan Widiyanti (1993: 99), kepemimpinan (*leadership*) pada umumnya adalah apa yang harus dipunyai, dijalankan, dan atau dipergunakan oleh setiap orang yang berkedudukan sebagai pemimpin. Kepemimpinan sebagai sesuatu **yang harus dipunyai** dapat diartikan sebagai kemampuan, bakat, sifat-sifat, atau kecakapan. Kepemimpinan sebagai sesuatu **yang harus dijalankan** adalah kepemimpinan sebagai kewajiban, fungsi, kegiatan-kegiatan dan tanggung jawab. Kemudian kepemimpinan sebagai sesuatu **yang harus dipergunakan** adalah kepemimpinan sebagai teknik atau sarana. Kepemimpinan dalam Unit V *IT & Cybercrime* dapat digambarkan sesuai dengan

definisi tersebut melalui tabel di bawah ini:

Tabel 4.4
Kepemimpinan Pada Unit V *IT & Cybercrime*

Yang harus dipunyai	Yang harus dijalankan	Yang harus dipergunakan
Pintar (*Smart)*	• Membuka ruang diskusi, membina dan memberikan arahan anak buah berdasarkan pengetahuan, keterampilan, dan pengalaman dalam menangani kasus *cybercrime.* • Menerapkan manajemen: mendelegasikan tugas, pengendalian dan pengawasan.	Gaya kepemimpinan tergantung situasi dan kepentingan:
Networking	• Mensejahterakan anggota, mencari dana untuk biaya operasional, mencari dana dan kesempatan untuk pelatihan. • Memperbaiki atau meng-*upgrade* infrastruktur. • Membangun jaringan di luar tubuh Polri: lembaga internasional, lembaga negara asing, lembaga swadaya masyarakat, asosiasi perusahaan, perusahaan, pengusaha.	• Militeristis • Paterialistik • Demokratis • Bebas
Pandai berbahasa Inggris, *parlente*	• Mewakili Indonesia di pertemuan internasional, regional atau bilateral membuka kesempatan untuk memperkenalkan perkembangan Unit V *IT & Cybercrime.*	
Mengerti anak buah	• Mendalami perbedaan kemampuan, potensi dan karakter anggota agar tercipta sinergi serta mempergunakan sumber daya manusia dan teknologi yang ada di Unit V *IT & Cybercrime.*	
Tanggap	• Responsif terhadap perubahan dan memiliki kemampuan mengantisipasi perubahan.	
Bertanggung jawab	• Menanggung beban perbuatan anggota. • Menjamin kesejahteraan anggota.	

(Sumber: Diskusi Kelompok Terfokus)

Anggota Unit V *IT & Cybercrime* mempunyai kriteria khusus yang harus dipunyai oleh seorang pemimpin/Kepala Unit (Kanit). Kriteria tersebut sebagai gambaran sosok ideal Kanit yang diinginkan oleh anggota Unit V *IT & Cybercrime*. Mereka menginginkan figur Kanit yang mempunyai kemampuan intelektualitas tinggi, bijaksana, mampu berbahasa inggris dan berpenampilan fisik yang baik. Intelektualitas tinggi diartikan sebagai kemampuan memahami dan mengerti mengenai permasalahan yang berkaitan dengan *cybercrime* sebagaimana diungkapkan dalam *FGD* Pama berikut ini:

"Pintar... kaya... smart ya... (tulis di depan)... ya... jago English... jago Inggris... bijak... cakep.... ganteng... parlente... parlente.... ya.... yang bergaya gitu... ya itu komandan saya... hahaha... mbak Indri... mbak Indri... ada lagi... udah semua... Pak Petrus... smart ya... masa... semua itu terpenuhi... apalagi... nggak... yang jelas punya kemampuan inilah... masalah internet ya... ya pinter udah termasuk... bijaksana... termasuk arif... hahahaha... kan judulnya arief... hahaha.... ini pintar... apa istimewanya pintar... ya... pintar... menguasai... berarti dia harus pintar... pinter mengembangkan juga disitu... pintar untuk... yang dimaksud dengan pintar apa sih... ini cerdas mungkin... nggak... pintar itu biasa." (*FGD* Pama)

Apabila pemimpin tidak dapat memenuhi kriteria tersebut, performa Unit V *IT & Cybercrime* turut terpengaruh dan menjadi tidak berkembang baik itu karena "jalan di tempat" (*stagnant)* atau mengalami kemunduran sebagaimana diungkapkan dalam *FGD* Pama berikut ini:

"Kalau semuanya nggak dipenuhi nggak masalah... tetep jalan tapi jalan di tempat... makanya tadi kalau ditanyakan lagi... kalau misalnya nggak bisa bahasa Inggris nggak masalah... tetep bisa jalan... tapi jalan di tempat ..." (*FGD* Pama)

Seorang Kanit diharapkan oleh anggotanya melakukan beberapa hal yang harus dijalankan sebagai pelaksanaan dari tugas dan tanggung jawab pemimpin diantaranya memenuhi kesejahteraan para anggotanya. Unit V *IT & Cybercrime* membutuhkan Kanit yang kaya. Kanit tersebut harus dapat mengatasi kekurangan anggaran operasional karena anggaran yang didapat dari Polri tidak mencukupi kebutuhan Unit V *IT & Cybercrime.* Selain itu, apabila Kanit bukanlah orang yang kaya, ada kekhawatiran dari anggota, Kanit akan sibuk memperkaya diri sendiri sebagaiman diungkapkan dalam *FGD* Pama sebagai berikut:

"Oke... kenapa harus kaya... karena tugas cyber butuh dana besar... kalau yang jabatnya nggak kaya... nyari kekayaan dulu... hahahaha... nggak... ahaha.. itu apa pengaruhnya... atau ke manajemen pendidikan... e... manajemen penyidikan... dan... e... kalau dia mencari kekayaan buat dirinya sendiri... dia nggak akan bertanggung jawab mas... lagi rasanya udah males..." (*FGD* Pama)

Seorang Kanit juga harus memberikan pengarahan dan masukan terhadap

pekerjaan anggotanya. Kanit harus menyakinkan bahwa apa yang dikerjakan para anggota tersebut sudah benar apalagi pekerjaan Unit V *IT & Cybercrime* berkaitan dengan penegakan hukum yang membutuhkan banyak penerapan kaedah-kaedah hukum dalam proses penanganan perkara. Bila kaedah tersebut tidak dilaksanakan, penyidik dapat dikenakan sanksi. Hal ini merupakan beban yang berat bagi penyidik. Maka, penyidik memerlukan Kanit yang mempunyai pengetahuan hukum dan dapat memberikan pengarahan sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Sekarang gini mas kalau nggak cerdas... e... penyidik itu e... kan akan mendapat tekanan pekerjaan... pekerjaan itu beban berat e... kalau kita sudah dibebani tugas yang berat tapi leader-nya itu nggak smart... tidak berani mengutarakan pendapat... ini... ni... tidak mudah mengutarakan pendapat... kepada pimpinan kalau hal itu... bertentangan dengan hukum yang ada di Indonesia itu tentunya kita akan tertekan terus... tidak akan maju... nah smart ini adalah berani mengutarakan bahwa yang dia kerjakan adalah benar gitu aja... ."* (*FGD* Pama)

Seorang Kanit juga harus mensinergikan berbagai karakter dan potensi dari anggota yang berbeda-beda sehingga menjadi suatu kekuatan dan pengolahan sumber daya anggota yang optimal dalam memimpin organisasi. Untuk menciptakan sinergi di antara anggota Unit V *IT & Cybercrime*, Kanit harus memilih dan mempergunakan gaya kepemimpinan yang sesuai dengan tugas dan fungsi Unit V *IT & Cybercrime* serta mempertimbangkan perbedaan karakter, potensi, dan kemampuan para anggota.

Gaya kepemimpinan sebagai teknik yang harus dipergunakan pemimpin menurut Riberu (1987: 7-9), Sunindhia dan Widiyanti (1993: 29-41) dan Furnham (1997: 576-577) dapat terdiri dari beberapa golongan antara lain: otokratis, militeristis, paternalistis, kharismatis, demokratis, dan bebas atau *laissez faire*. Seorang pemimpin yang meminta dan menerima masukan dari anggotanya merupakan pemimpin yang diperlukan dalam Unit V *IT & Cybercrime* karena pemimpin tersebut akan menjadi pengambil keputusan (*decision maker*) sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Dalam decision maker itu pengaruh juga secara pimpinan, dia minta*

masukan dari anggotanya sehingga itu akan jadi bahan pertimbangan, untuk membuat keputusan itu tadi itu sangat mempengaruhi keputusan itu tadi, sebelum dia memutuskan dia bertanya apa sih" (*FGD* Pama)

Melihat tendensi tersebut, tampak bahwa gaya kepemimpinan yang dianut dalam Unit V *IT & Cybercrime* cenderung gaya demokrasi. Hal ini diperkuat lagi dengan adanya budaya *sharing* yang dilakukan oleh anggota sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

*"... yang pasti tujuan pimpinan itu pasti biar kita mudah mengeluarkan pendapat kita kan... kita nggak ngeliat kalau di mana ya... polisi dulunya militer ya... dianggap sebagai bagian militer... di dalam... *...* ... militer... ya tau lah... ada level gitu berhubung ngomong dia mau ijin dia... ini begini... begini... tapi putusan akhir selalu pada senior gitu kan... nah disini kita diubah gimana caranya posisi kita sama... kita bebas mengeluarkan pendapat... didiskusikan bersama..."* (*FGD* Pama)

Sejak bulan Maret 2007 hingga akhir Desember 2007, Kanit *V IT & Cybercrime* begitu terfokus dengan tanggung jawabnya dalam memberantas teroris sehingga tidak secara teratur hadir atau datang ke Unit V *IT & Cybercrime*. Pada saat tersebut, terjadi keadaan dimana anggota dapat bertindak bebas tanpa pengawasan. Dengan kondisi seperti itu, para anggota menikmati gaya kepemimpinan yang bebas.

Tetapi ada pula keadaan tertentu, saat Kanit V *IT & Cybercrime* langsung memberikan instruksi kepada para anggotanya dan instruksi tersebut harus langsung dilaksanakan dengan tepat dan cepat tanpa adanya bantahan atau pertanyaan dari para anggota. Mengingat cara pencapaian perintah yang langsung dan berdasarkan rantai komando tersebut, budaya militeristik tampaknya masih tertanam secara laten dalam Unit V *IT & Cybercrime* terutama untuk melaksanakan tugas yang dirasakan penting dan mendesak.

Menurut Sir Robert Peel (Cordner, 2005: 11) yang dikutip oleh Suparlan dalam buku Kebudayaan Polri: Struktur dan Anti Strukur, prinsip dasar budaya polisi adalah polisi harus berada di bawah satu kendali perintah, tugas utamanya adalah mencegah terjadinya kejahatan dan kekacauan serta keberhasilan polisi tergantung pada persetujuan publik atau umum. Prinsip berikutnya adalah organisasi polisi harus disusun berdasarkan organisasi militer. Calon anggota

kepolisian harus dipilih secara tepat dengan pendidikan dan latihan yang sesuai tugas-tugas pemolisian, sebelum disahkan sebagai petugas kepolisian. Calon petugas kepolisian harus menjalani masa kerja magang. Kekuatan polisi harus menyebar menurut waktu dan wilayah, dan polisi hanya diizinkan untuk menggunakan tindakan kekerasan bila dipandang perlu. Suparlan menganggap yang paling menonjol dari prinsip tersebut di Polri adalah jenjang kepangkatan dan kewenangan kekuasaan yang ketat batas-batasnya. Pola perintah atasan secara lisan tidak dapat dibantah oleh bawahannya.

Melihat gejala yang terjadi di Unit V *IT & Cybercrime*, cara atau gaya kepemimpinan dapat berubah tergantung kondisi dari organisasi itu sendiri dan kepentingan Kanit. Berdasarkan observasi dan hasil *FGD* maka terdapat setidaknya empat gaya kepemimpinan yang diterapkan dalam Unit V *IT & Cybercrime* yaitu: militeristis, patrialistis, demokratis dan bebas, sebagaimana bagan di bawah ini:

Bagan 4.3
Gaya Kepemimpinan yang Diterapkan dalam Unit V *IT & Cybercrime*

(Sumber: Penulis)

Bila dilihat dari tingkat partisipasi anggota, gaya kepemimpinan dapat diurutkan dari tingkatan partisipasi anggota paling rendah ke tingkat partisipasi anggota paling tinggi dengan urutan sebagai berikut: otokratif (tingkat partisipasi anggota paling rendah), militeristis, patrialistis, demokratis, dan bebas (tingkat partisipasi anggota paling tinggi). Semakin tinggi tingkat partisipasi anggota, semakin rendah dominasi pemimpin. Begitu pula sebaliknya, semakin rendah tingkat partisipasi anggota, semakin tinggi dominiasi pemimpin. Untuk tugas-

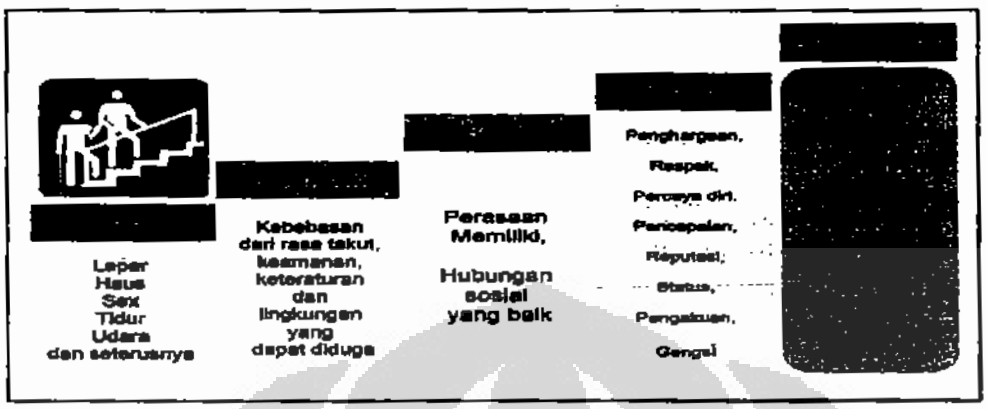
tugas yang penting dan mendesak dan diperlukan waktu pengerjaan yang cepat, maka diperlukan pemimpin yang mendominasi. Untuk tugas-tugas yang kurang penting atau tidak mendesak serta waktu pengerjaan yang relatif tidak cepat, maka partisipasi anggota dapat dipergunakan untuk memperoleh kontribusi dan komitmen dari para anggota dalam pelaksanaan tugas tersebut.

Kanit juga menentukan arahan untuk mencapai tujuan organisasi. Kanit memberikan petunjuk ataupun instruksi mengenai apa yang harus dikerjakan atau bagaimana cara mengerjakannya. Arahan tersebut memberikan rasa nyaman dan aman bagi para anggota sehingga dapat memberikan hasil kerja yang optimum sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Mungkin suasana kerja ya, suasana kerja di mana seorang pimpinan mau memberikan arahan, apa-apa yang mau kita pikirkan... berbuat dia sudah terlebih dahulu menangkap, misalnya mau kemana kita, mau gimana kita, sebenernya mau tau hasil akhir yang maksimum, itu yang membuat saya merasa nyaman."* (*FGD* Pama)

Dalam buku *Motivation in Organization,* (Smith, 1991: 81), disampaikan kembali teori motivasi klasik dari Maslow (1943). Maslow membagi kebutuhan manusia menjadi lima kelompok besar yaitu: 1) Kebutuhan fisik; 2) Keamanan; 3) Sosial; 4) Kebanggaan; dan 5) Aktualisasi diri. Kebutuhan tersebut berhubungan dengan pola berjenjang atau hierarki, di mana kebutuhan pertama terpenuhi, baru beranjak ke kebutuhan kedua, ketiga dan seterusnya. Dalam hierarki itu, kebutuhan fisik merupakan kebutuhan yang dasar yang berada di bawah, sedangkan kebutuhan akan aktualisasi diri berada di puncak. Bila kebutuhan dasar telah terpenuhi, manusia akan berupaya memenuhi kebutuhan di jenjang yang lebih tinggi dan begitu seterusnya.

Bagan 4.4
Teori Hierarki Kebutuhan Maslow



(Sumber: Adair (1995: 12) dan (Smith, 1991: 81))

Kebutuhan anggota Unit V *IT & Cybercrime* dapat dijabarkan melalui hierarki kebutuhan Maslow di atas. Kebutuhan fisiologis dari anggota berikut keluarganya merupakan kebutuhan yang utama. Untuk memenuhi kebutuhan tersebut, gaji dan tunjangan yang diterima dari Polri tidaklah mencukupi. Polisi pada umumnya mengharapkan tambahan penghasilan dari kasus yang mereka tangani. Namun, pada Unit V *IT & Cybercrime,* kasus yang mereka tangani biasanya tidak menghasilkan penghasilan tambahan. Harapan anggota tertumpu kepada Kanit V *IT & Cybercrime* untuk dapat memenuhi kesejahteraan para anggota.

Kebutuhan akan rasa aman dari setiap anggota relatif lebih mudah dipenuhi di Unit V *IT & Cybercrime* dibandingkan dengan apabila anggota bernaung pada bagian lain seperti antiteror ataupun reserse. Banyak pekerjaan di Unit V *IT & Cybercrime* berkaitan dengan komputer dan dilakukan di dalam kantor (belakang meja) dibandingkan kegiatan di lapangan. Dengan cara kerja seperti itu, resiko yang berhubungan dengan keselamatan jiwa menjadi lebih kecil dibandingkan dengan bekerja pada bagian lainnya. Resiko yang berhubungan dengan pekerjaan pada Unit V *IT & Cybercrime* adalah masalah ketidakjelasan ketentuan hukum materil dan formil yang menuntut penyelidik untuk melakukan terobosan dan interpretasi terhadap ketentuan yang ada. Penyelidik harus berpikir lebih keras dalam menangani kasus tindak pidana *hacking* atau *cybercrime* dibandingkan dengan penanganan kasus tindak pidana konvensional. Resiko yang ada dapat

berupa praperadilan karena diperlukannya penafsiran dari tindak pidana yang diajukan ataupun ditolaknya berkas perkara oleh penuntut umum.

Sebagian dari anggota Unit V *IT & Cybercrime* merasa dirinya dibuang dari unit terdahulu dengan alasan dianggap membangkang atau sebagai akibat politik kantor *"like and dislike"*. Ada juga yang merasa disia-siakan oleh pemimpinnya terdahulu, tidak diperhatikan, atau tidak diperlukan lagi. Para anggota tersebut kemudian berkumpul dalam Unit V *IT & Cybercrime*. Mereka menemukan Unit yang dapat menerima mereka. Dengan penerimaan tersebut dan perasaan senasib sepenanggungan, **kebutuhan sosial** para anggota menjadi terpenuhi.

Kebutuhan akan harga diri juga dapat mereka peroleh dari Unit V *IT & Cybercrime*. Para anggota merasa bangga menjadi bagian dari Unit V *IT & Cybercrime*. Mereka merasa lebih hebat dibandingkan dengan penyidik tindak pidana konvensional. Kebanggaan tersebut muncul karena adanya anggapan bahwa mereka lebih mengetahui mengenai teknologi komunikasi dan *cybercrime*. Apalagi hal ini didukung pula dengan pelatihan, seminar di berbagai negara serta adanya tamu atau kunjungan penegak hukum dari luar negeri ke Unit V *IT & Cybercrime*. Tidak semua anggota Polri dapat memiliki kesempatan seperti mereka.

Pemenuhan kebutuhan akan aktualisasi diri juga dapat ditemui di Unit V *IT & Cybercrime*.. Dengan perkembangan teknologi yang semakin pesat, penanganan *cybercrime* menjadi semakin penting. Oleh karena itu, diperlukan orang yang mau belajar secara berkelanjutan untuk memahaminya. Di samping itu, aturan hukum yang tidak memadai menantang penyidik untuk dapat melakukan terobosan hukum, berpikir kreatif, dan bertindak inovatif dalam melakukan interpretasi dan mempersiapkan berkas perkara.

Motivasi tidak saja dapat dilihat dari tingkatannya tapi juga dapat dilihat dari sumbernya. Berdasarkan sumbernya, motivasi terbagi menjadi dua yaitu motivasi intrinsik dan motivasi ekstrinsik. Motivasi intrinsik artinya adalah suatu motivasi yang timbul dari diri sendiri yaitu saat seseorang melakukan sesuatu karena ia ingin melakukannya. Motivasi esktrinsik berasal dari luar diri orang tersebut. Seseorang melakukan sesuatu untuk memenangkan suatu hadiah yang khusus ditawarkan untuk perilaku tersebut. (Leavitt, 1992: 22). Motivasi setiap

manusia dapat berbeda-beda dipengaruhi oleh berbagai faktor. Berdasarkan sumbernya dan faktor-faktor yang mempengaruhinya, anggota Unit V *IT & Cybercrime* memiliki bentuk motivasi tersendiri. Gambaran umum motivasi tersebut dapat dilihat pada bagan 4.5 berikut ini.

Anggota Unit V *IT & Cybercrime* mempunyai berbagai alasan mengapa mereka masuk dalam Unit V IT *& Cybercrime* selain memang ditugaskan. Ada yang berupaya beradaptasi dengan mempelajari *cybercrime* sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"...Saya ditugaskan ke Bareskrim... jadi saya bergabung dengan bapak–bapak... dan ibu–ibu ini...kurang lebih baru 3 bulan... jadi secara resmi ...secara pengetahuan saya masih nol... untuk reserse–resersean khususnya di cybercrime jadi kalau ilmu ke-reserse-an... saya masi... tapi saya berusaha... ingin tau dan ingin belajar sama bapak–bapak dan ibu–ibu ini... mudah – mudahan saya juga bisa..."* (*FGD* Pama)

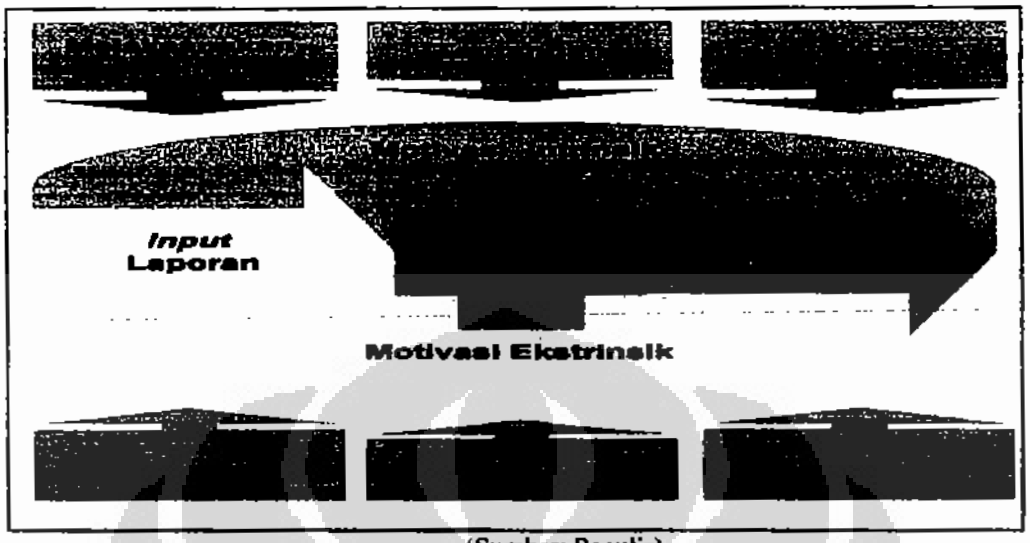
Ada juga anggota, yang masuk karena memandang Unit V *IT & Cybercrime* lebih tidak menyita waktu dan kurang beresiko dibandingkan bagian lain atau sesuai dengan minat sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Kalau anti terror jarang berkumpul dengan keluarga... pokoknya jarang pulang lah... resikonya besar... saya berpikir nya pertama kapan berkumpul dengan keluarga nya...ya kan... terus resikonya... jelas kita berhitung resiko kan... begitu ditempatkan di cyber...wah.. ini kan jadi ada perubahan besar kan... kebetulan saya hobby di komputer Lucky kan jadi nya... dari terror ... ditempatkan di posisi yang menurut saya pas dengan ini saya...au saya sebenernya Lucky ... tertunjuk."* (*FGD* Pama)

Selain itu, ada anggota yang memang memilih penempatan di posisi yang paling anggota anggap kuasai sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Saya pikiran pertama begitu saya masuk Cybercrime... saya langsung tau disitu ada laboratorium... ada yang dalam laboratorium forensic komputernya dan ada yang untuk penyidikan... saya langsung nyadarin.. saya lemah dalam peyidikan...karena dasar saya intelejen... jadi saya ingat betul waktu ditawarin sampe masuk laboratoriumkan..."* (*FGD* Pama)

Bagan 4.5
Pengaruh Motivasi Pada Manajemen Penyidikan



(Sumber: Penulis)

Motivasi tidak saja datang dari dalam diri pribadi anggota tetapi juga dari orang lain seperti rekan kerja yang humoris dan pintar, teman yang datang menawarkan posisi di Unit V *IT & Cybercrime*, pertimbangan keluarga atau faktor suami yang telah bekerja di reserse sebagai alasan untuk bergabung dengan Unit V *IT & Cybercrime* sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> "*Berhubung suami saya udah di Reserse... dari awal nya udah di Reserse nggak mungkin saya ... dua–duanya di Reserse... kita bagi... walaupun kita satu karakter... satu profesi... hm... saya juga punya anak kan gitu... kalau nanti dua– duanya masuk Reserse... bagaimana perkembangan anak – anak ... e.. waktu itu saya udah komitmen juga sama suami... oke.. saya nggak akan ke Reserse... cukup saya diturunin kan... jadi kalau personel itukan jelas...pulang dan berangkat nya itu jelas... jadi kita bisa ngurusin anak juga... kemudian ada temen saya ini ...nawarin waktu itu...*" (*FGD* Pama)

Pemimpin berperan memotivasi anggotanya untuk bekerja lebih giat dengan berbagai cara. Salah satu caranya adalah dengan memberikan jaminan biaya operasional dan kesejahteraan anggota. Penghargaan berupa uang merupakan motivasi utama yang dirasakan oleh anggota sebagaimana diungkapkan dalam *FGD* Pamen sebagai berikut:

> "*Saya punya kepuasan lebih karena saya katakan tadi, habis gelap terbitlah terang, dulu mikir pekerjaan tidak terpikirkan cybercrime itu banyak biaya tanpa adanya benefit, tapi begitu beliau masuk kita nggak usah mikir kesejahteraan, yang penting kesejahteraan tercukupi, itu membuat semua suasana menjadi nyaman, dalam bekerja pun menjadi enak, seseorang bekerja kan membutuhkan suatu motivasi, kenapa orang membawa suatu pekerjaan, seperti Pak Bagas bilang, mau pergi bensinnya aja nggak ada, uang bensin nggak ada, ngapain kalau saya, cuma dikasih uang perintah doang suruh jalan, makasih aja gitu loh, kasarnya seperti itu, suatu yang bulshit kalau kita bicara perjuangan*" (*FGD* Pamen)

Selain uang, penghargaan juga dapat berupa kesempatan mengikuti pelatihan di luar negeri, sekolah di dalam negeri, pujian, pengakuan atas hasil kerjanya serta peningkatan jenjang karir.

Menurut Kotter (1997: 35) syarat-syarat pribadi yang diperlukan untuk memberikan kepemimpinan yang efektif berupa motivasi, nilai-nilai pribadi, kemampuan dan keahlian, reputasi dan catatan rekor, relasi dalam perusahaan dan industri serta pengetahuan mengenai industri dan organisasi. Hal tersebut selaras dengan kepemimpinan pada Unit V *IT & Cybercrime* dimana Kanit memberikan motivasi ekstrinsik berupa penghargaan bagi para anggota.

4.4.2 Analisis Pengaruh Budaya Organisasi dalam Manajemen Penyidikan

Dalam konteks organisasi, budaya perusahaan (organisasi) adalah kesatuan nilai dan asumsi yang dipegang oleh kesatuan sumber daya manusia. Budaya organisasi juga merupakan sebuah sistem progresif yang terus berkembang. Berbeda dengan peraturan perusahaan yang lebih kognitif, budaya organisasi lebih mengakar dan lebih berpengaruh pada tingkah laku karyawan (Matindas, 1997: 95).

Dalam organisasi yang besar terdapat budaya dominan yang mengungkapkan nilai inti yang dimiliki bersama oleh sebagian besar anggota organisasi. Pada organisasi besar, timbul beberapa sub-budaya yang mencerminkan masalah bersama, situasi, atau pengalaman yang dihadapi para anggotanya. Sub-budaya tersebut dapat bersifat vertikal dan horisontal. Sebagian besar sub-budaya tersebut muncul karena adanya pembagian berdasarkan

departemen atau pemisahan secara geografis. (Robbins, 1995: 482).

Selaras dengan pandangan Koentjaraningrat, J.J. Honigmann dalam bukunya *The World of Man* (1959: 11-12) membedakan tiga gejala kebudayaan yaitu ide, aktivitas, dan artefak. Ketiga gejala tersebut kemudian dijabarkan oleh Koentjaraningrat sebagai unsur-unsur atau wujud dari kebudayaan, yaitu: wujud kebudayaan sebagai suatu kompleks dari ide-ide, gagasan, nilai-nilai, norma-norma dan peraturan dan sebagainya; wujud kebudayaan sebagai suatu kompleks aktivitas serta tindakan berpola dari manusia dalam masyarakat; wujud kebudayaan sebagai benda-benda hasil karya manusia (Koentjaraningrat, 2002: 186-188; Prasetya, 1998: 32-33).

Unit V *IT & Cybercrime* sebagai bagian dari Polri juga terikat dan menganut kebudayaan Polri dalam eksistensinya. Namun sebagai sub-organisasi dari Polri, Unit V *IT & Cybercrime* dalam pengamatan peneliti mempunyai beberapa kekhasan yang sekaligus menunjukkan bahwa Unit V *IT & Cybercrime* memiliki sub-budaya organisasi tersendiri. Misalnya, polisi yang bernaung pada Bareskrim Polri mempunyai aturan tata tertib yang sama, tetapi kebiasaan dan perilaku masing-masing unit dalam Bareskrim Polri dapat saja berbeda.

Bila kita telaah, di Unit V *IT & Cybercrime* terdapat budaya organisasi yang khas yang merupakan sub-budaya dari organisasi Polri atau Bareskrim atau Direktorat II. Sub-budaya Unit V *IT & Cybercrime* tersebut berlaku di antara sesama anggota Unit V *IT & Cybercrime.* Sub-budaya tersebut, bila dilihat dari kaca mata organisasi, yang memandang satu unit adalah suatu organisasi dengan satu pimpinan dan sekelompok orang menjadi anggota, akan menjadi suatu budaya organisasi tersendiri. Budaya organisasi tersebut menjadi pembeda dengan unit-unit lain yang sejajar (horisontal) dan dengan organisasi hirarki di atasnya seperti Direktorat dan Bareskrim (vertikal).

Selain sebagai pembeda atau pemberi ciri khas, budaya organisasi dapat berperan sebagai unsur pelekat atau pemersatu anggota di dalam satu unit. Wujud budaya organisasi di Unit V *IT & Cybercrime* secara teoritis dapat dibedakan secara sederhana menjadi tiga wujud yaitu: nilai, kegiatan, dan artefak. Artefak juga dapat diartikan sebagai alat atau benda kebudayaan hasil karya manusia (Koentjaraningrat *et. al.*, 2003: 15). Artefak yang dimiliki Unit V *IT &*

Cybercrime berupa foto-foto di luar negeri yang mereka pajang di laptop, plakat kerja sama dengan institusi asing, dokumen baik berupa *hardcopy* maupun *softcopy*, perangkat keras komputer (*hardware*) dan perangkat lunak (*software*), serta dokumen berkas acara pemeriksaan termasuk bukti digital yang di-*printout*.

Tabel 4.5
Wujud Budaya Organisasi Unit V *IT & Cybercrime*

Ide dan Nilai	Kegiatan	Artefak
a. Loyalitas, respek, hirarki: suatu doktrin militer yang ditanamkan pada institusi pendidikan polisi	▪ Mengikuti penempatan ▪ Administrasi tanda tangan senior ▪ Jenjang perintah/instruksi	▪ Surat perintah ▪ Dokumentasi internal lainnya ▪ Pembedaan gaji, fasiltas, tunjangan
b. Kerja rumit duit sedikit: Bukan posisi yang basah, tidak berharap mendapat penghasilan dari kasus yang ditangani	▪ Menerima kasus *cybercrime* tanpa mempertimbangkan pendapatan dari kasus tersebut ▪ Menanti atau mengharapkan Kanit memberikan kesejahteraan kepada anggota	▪ Berkas perkara tindak pidana yang berhubungan dengan kejahatan komputer ▪ Penghargaan baik dalam bentuk uang maupun barang
c. *Teamwork:* Bekerja sama saling membantu menyelesaikan tugas	▪ *Sharing*, diskusi bersama untuk mencari solusi dari permasalahan yang sedang dihadapi ▪ Bekerja sebagai satu tim: ada penyidik dan ada forensik	▪ Dokumen hasil laporan forensik ▪ Berita acara pemeriksaan ▪ Dokumen hasil diskusi
d. Bangga: Menjadi anggota unit yang dianggap mempunyai kemampuan lebih dibandingkan dengan unit lain	▪ Menganggap dirinya lebih karena mengetahui perihal *cybercrime*	▪ Menggunakan atribut *cybercrime*: pada *wall paper* di laptop, *T-shirt* ▪ Memajang foto-foto di luar negeri di kala pelatihan ▪ Memajang plakat-plakat kerja sama dengan institusi asing ▪ Memiliki laboratorium forensik komputer tersendiri
e. *Work smarter not harder* Bekerja lebih pintar bukan lebih keras	▪ Melakukan penyidikan melalui komputer bukan ke lapangan ▪ Melakukan patroli di internet bukan di lapangan	▪ Penggunaan berbagai *software* dan *hardware*, termasuk internet ▪ Memiliki laboratorium forensik komputer tersendiri
f. Progressif: Teknologi informasi terus berkembang diperlukan usaha untuk mengikuti perkembangan tersebut	▪ Mengikuti pelatihan di dalam dan di luar negeri ▪ Belajar mandiri untuk menambah pengetahuan ▪ Membiasakan diri menggunakan teknologi informasi: *chatting, internet* ▪ Menggunakan berbagai peralatan teknologi terkini	▪ Buku sebagai bahan bacaan ▪ Program komputer ▪ *Hardware: CPU, Laptop* ▪ *Software* ▪ Sertifikat pelatihan ▪ Catatan pelatihan ▪ Bahan presentasi
g. Adaptif: Anggota melakukan terobosan, hal-hal inovatif	▪ Melakukan interpretasi terhadap aturan undang-undang ▪ Mengundang saksi yang	▪ Membuat bukti digital menjadi kertas hasil cetak (*print out*)

Ide dan Nilai	Kegiatan	Artefak
untuk mendapatkan tujuan organisasi sesuai dengan keadaan yang ada saat ini	mempunyai pengetahuan di bidang *cybercrime* atau teknologi komunikasi	▪ Berita acara pemeriksaan kasus *cybercrime*

(Sumber: Penulis)

Wujud kebudayaan berupa nilai-nilai atau ide berikut wujud kebudayaan berupa kegiatan atau aktivitas dari Unit V *IT & Cybercrime* adalah sebagai berikut:

4.4.2.1 Loyalitas, Respek, Hierarki

Di kalangan anggota Unit V *IT & Cybercrime* yang mengikuti pendidikan polisi tertanam sebuah doktrin loyalitas, respek, hierarki sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Di pendidikan saya di Akademi... Jadi saya diajarkan 3... Yang pertama adalah loyalitas... Respek dan Hierarki ..atau dibalik-balik... tiga – tiga itu melekat ..saya inget karena sering di beginikan... itu yang paling *... * di wilayah nanti kita di daerah ... kita bekerja ...loyalitas ...respek ..hierarki ..." (FGD Pama)*

Loyalitas, respek dan hierarki tersebut tertanam mendalam sebagai sesuatu yang dipercayai tanpa adanya upaya untuk mengkritisi. Jelas dalam doktrin ini terlihat sifat meliterisme yang masih mengental dalam pendidikan Polri dan terbawa dalam lingkungan kerja. Nilai tersebut diterapkan dalam kehidupan sehari-hari sebagai bagian dari nilai yang dianggap penting dan diagungkan oleh anggota Polri. Kesetiaan pada organisasi diterapkan dengan mengikuti perintah atau instruksi dari atasan. Begitu pula rasa hormat atau respek dilihat dari perilaku seorang anggota terhadap atasannya atau terhadap rekan dengan memperhatikan hirarki yang ada. Penempatan pada Unit V *IT & Cybercrime*, bagi sebagian anggota merupakan pelaksanaan perintah semata. Para anggota mendapat telegram rahasia (TR) berisi penempatan dan berusaha mengikuti proses penempatan tersebut walaupun mungkin minat dan kemampuan mereka tidak selaras dengan penempatan yang diperintahkan. Hal tersebut mencerminkan loyalitas dan respek terhadap keputusan yang telah dibuat terhadap para anggota.

4.4.2.2 Kerja Rumit Duit Sedikit

Mendapatkan penempatan pada Unit V *IT & Cybercrime* dianggap sebagai posisi yang tidak basah, padahal perkerjaannya memeras otak sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"... anggota polisi banyakan berpikirnya gitu.. praktis aja lah... jarang yang berpikir ribet-ribet, praktisnya itu bagaimana caranya duitnya banyak, tapi saya ga pusing dengan yang rumit-rumit itu."* (*FGD* Pama)

Pemahaman tersebut yang menyebabkan beberapa personil polisi enggan untuk ditempatkan di Unit V *IT & Cybercrime*. Mereka berpikir apabila mereka tergabung dalam Unit V *IT & Cybercrime* maka penghasilan mereka tidak akan banyak sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Sekarang orang berfikir... infotek... infotek.. kan kegiatan mana yang ditangkep... apa yang mau dijadikan... sedangkan orang lain yang di Mabes nggak tau... nggak dapet jatah uang... dengan perbankan aja banyak bank-bank gelap... e... pemikirannya mungkin bisa untuk tambahan... tambahan penghasilan...terus yang lain kan bagus-bagus ya... makanya infotek jaman itu... apalagi sedikit... orang nggak mau karena baru denger Infotek aja ...apa yang mau di..."* (*FGD* Pama)

Unit V *IT & Cybercrime* dianggap sebagai IDT (Inpres Desa Tertinggal). Kering akan lahan garapan sebagai penghasilan tambahan. Perlunya penempatan pada lahan yang basah merupakan nilai yang dianut umum oleh anggota Polri. Sedangkan di Unit V *IT & Cybercrime,* mereka ditempatkan dalam posisi 'pekerjaan rumit, duit sedikit'. Sebagai kompensasi terhadap pekerjaan yang tidak menghasilkan tersebut, anggota Unit V *IT & Cybercrime* banyak bergantung kepada pemimpin untuk mensejahterakan anggotanya. Sub-budaya organisasi inilah yang berbeda bahkan bertentangan dengan budaya Polri sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> "...tapi maunya mereka menyelidiki kasus-kasus yang memang menghasilkan duit... tapi saya tidak mau pusing dengan IT... IT ini... karena banyak juga diantara temen-temen... mau pindah ke unit *Cyber*... nggak ah.. susah...kenapa susah..." (*FGD* Pama)

4.4.2.3 Kerjasama Tim *(Teamwork)*

Kerja sama tim merupakan hal yang penting di dalam Unit V *IT & Cybercrime*. Para penyidik harus bekerja sama satu dengan lainnya untuk memecahkan masalah yang dihadapi. Keterbatasan kaedah normatif yang ada menuntut kemampuan penyidik untuk bertukar pikiran dan berdiskusi melakukan interpretasi terhadap aturan materil maupun formil. Kesuksesan penyidikan dan pemberkasan perkara tidak saja ditunjang oleh kinerja penyidik tetapi juga kerja sama dengan anggota laboratorium forensik komputer. Kerja sama di antara penyidik dengan anggota laboratorium forensik komputer menciptakan sinergi bagi kelancaran penyidikan.

Nilai kerja sama tim tersebut semakin tampak jelas dengan adanya kegiatan ***sharing***. Diskusi tersebut memungkinkan adanya pernyataan, perdebatan, atau bahkan sangggahan dari setiap peserta terhadap peserta yang lain. Diskusi ini melibatkan semua penyidik yang bertugas di Unit V *IT & Cybercrime* yang terdiri dari anggota dengan jenjang kepangkatan yang berbeda-beda sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Tetapi kalau selama ini yang saya masuk di Unit Cybercrime Mabes Polri itu kita mempunyai permasalahan... permasalahan itu kita pecahkan bersama... punya permasalahan... umpamanya saya menangani kasus e... cybercrime ... itu kita... kita diskusikan... kita rapatkan... kita diskusi kan dan disanggah oleh rekan-rekan... sehingga itu merupakan pembelajaran yang... yang sangat tepat... yang bisa kita terima... sehingga antara yang belum bisa... dan yang pinter.... itu akan bisa ngikut... yang... yang nggak bisa itu cepet ngikut... itu yang perlu"* (*FGD* Pama)

Setiap anggota bebas mengeluarkan pendapatnya, sehingga suasana diskusi menjadi lebih hidup karena setiap anggota ikut berpartisipasi dalam diskusi penanganan kasus *cybercrime*. Mereka menganggap pelaksanaan diskusi tersebut berbeda dengan keadaan ketika mereka belum ditugaskan pada Unit V *IT & Cybercrime* sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"Kalau saya... kalau saya mengalami... lebih hebat yang sekarang... sekarang ini... lebih apa... lebih terbuka... terus lebih terbuka... lebih... lebih... lebih jelas terbukanya... lebih jelas terbukanya... maksudnya... ini lho... ini kan acara tentang... tentang kita bebas berbicara kan... hmm... bebas berbicara... bebas mengeluarkan pendapat... sekarang ini yang baru saya temukan... dulunya nggak pernah..." (*FGD* Pama)

Perbedaan jenjang kepangkatan dari peserta yang terlibat dalam diskusi ini bukan hanya sejauh satu atau dua tingkat namun juga melibatkan perbedaan tingkatan atau kategori kepangkatan yaitu dari perwira pertama sampai perwira menengah. Dengan demikian, kegiatan ini mempertemukan penyidik berpangkat Ipda sampai AKBP. Ditinjau dari sudut pandang senioritas, tentunya akan ada kesenjangan yang cukup jauh. Jika ditinjau dari masa tugas, kegiatan ini mempertemukan penyidik yang lulus dari jenjang pendidikan yang sama dari angkatan yang berbeda lebih dari 20 tahun. Hal yang menarik dari kegiatan diskusi tersebut adalah masing-masing anggota unit memiliki posisi yang setara sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"Kita dari bawahan sama atasan tetep hormat masih ada... hanya saja kita kapasitasnya kalau di.... di kantor... itu jadi masih ada juga.... jadi kita diskusi bersama antara senior dengan junior... itu seolah-olah tidak ada jenjang ... tidak ada keterkaitan..." (*FGD* Pama).

Setiap peserta diskusi akan mempunyai dan mengutarakan pendapat yang berbeda atau berlawanan. Dapat juga mereka saling meluncurkan bantahan atau berdebat dengan anggota yang lebih senior atau berpangkat. Bukan berarti mereka tidak menghormati atau bahkan menghina anggota tersebut. Dari perdebatan yang ada justru timbul pandangan yang berbeda yang menambah pengetahuan anggota yang terlibat atau hadir dalam proses diskusi tersebut. Setiap anggota Unit V *IT & Cybercrime*, dalam berdiskusi tidak lagi melihat dari jenjang kepangkatan tetapi dari kemampuan intelektualitas setiap anggota. Apabila terdapat seorang anggota yang memiliki tingkat kepandaian lebih tinggi meskipun anggota tersebut hanya berpangkat rendah, ia dapat saja memberikan masukan atau saran bagi pemecahan permasalahan kasus-kasus *cybercrime* sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"Mungkin gini... dalam... dalam bersikap... e... antar perorangan itu kita tau... jelas kalau memandang masalah hierarki... tetapi ketika kita memecahkan satu pekerjaan... atau satu permasalahan... kita tidak liat itu... karena apa... kita menyadari bahwa belum tentu yang sekolahnya lebih pinter dia lebih tau... atau dia... dia pangkat nya lebih tinggi... dia lebih tau....itu kita kesampingkan ....*... "* (*FGD* Pama)

Hal ini tentunya menjadi anomali dalam keberadaaan mereka sebagai bagian dari institusi Polri yang terikat dengan struktur dan jenjang kepangkatan yang mendapatkan konsekuensi berupa hubungan yang hirarkis di antara jenjang kepangkatan tersebut. Dalam kegiatan *sharing*, sangat mungkin pendapat dari seorang penyidik berpangkat perwira menengah disanggah oleh penyidik lain yang berpangkat perwira pertama. Hal yang lebih menandakan lagi ke-khas-an ini adalah hal tersebut dapat diterima oleh seluruh anggota, baik yang berpangkat perwira pertama maupun perwira menengah. Namun meskipun dalam diskusi itu tidak ada kesenjangan yang jauh, tetapi dalam Unit V *IT & Cybercrime* juga tetap mempunyai senioritas, terutama untuk hal-hal yang menyangkut pelaporan dan adminitrasi. Budaya pemecahan masalah secara bersama-sama ini telah mengakar pada setiap anggota dari Unit V *IT & Cybercrime*. Budaya ini juga ditularkan dari anggota yang lama kepada anggota yang baru masuk ke dalam Unit V *IT & Cybercrime* sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"Kan kalau dibilang tadi kenapa membiarkan semuanya berjalan seperti apa namanya... seperti mengalir tanpa harus ada hirarkis... bukan... bukan membiarkan secara tidak ada hierarki nggak... kita walaupun sama rata... kesenioritasan tetep ada." (*FGD* Pama)

Dalam menangani kasus-kasus *cybercrime*, setiap anggota Unit V *IT & Cybercrime* memerlukan kerja sama dimana setiap anggota mempunyai peran masing-masing dan peran itu saling mendukung satu sama lain sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"Kalau saya melihatnya peran kita masing-masing itu saya melihatnya sebagai tubuh manusia, ada sebagai tangan, sebagai kaki, mata dan sebagainya... jadi 99% ini bisa beranggapan sebagai tangan, oh kawan kita yang satu lagi sebagai kakinya, oh ya, supaya manusia ini utuh sebagai manusia dia bisa beraktifitas itu yang pertama, yang kedua

sebelum kita melihat yang itu kita melhatnya memandang dari masalah fungsional dan struktural, kalau struktural kita sama, apa namanya penyidik, formalitas ya, tapi sebagai fungsional kita semua adalah penyidik kecuali mas Idang ini ada kelebihan, karena saking ini punya kelebihan di bidang forensik, itu dua, lalu yang terakhir kalau kita lihat dari peranan masing-masing sama seperti tadi di sampaikan kita semua memeriksa oh bagian kasus ini banyak rekan tim ini masuknya kelompok itu, ini kelompok ini, tapi semua itu harus sinergi, nggak bisa ibaratnya menangani satu kasus kelompok itu, setidaknya ada input atau saran rekan-rekan yang lain, karena kalau seperti ini istilahnya udah mumet" (*FGD* Pama)

Pembagian peran tersebut mengungkapkan penerapan manajemen dalam penanganan penyidikan yang dilakukan Unit V *IT & Cybercrime* sebagaimana diungkapkan dalam *FGD* Pamen sebagai berikut:

*"Soalnya organisasi... yang pernah kita alami sendiri... kita mesti melakukan perencanaan... namun perencanaan itu e... tentunya... kalau buta perencanaan di penyidikan.. sebetulnya kan perencanaan itu harus ada e.... kita harus... umpamanya kita ditunjuk oleh kanit... untuk melakukan peyidikan satu perkara ..ditunjuk ada yang senior... jadi nanti senior melakukan seperti mas lakukan... itu merencanakan... jadi memilah – milah kekuatan yang ada, memecahkan persoalan itu... terus kita membagi ....dibagi siapa bertanggung jawab melakukan apa ..ada ...ada perwira pam.. perwira pertama yang ditunjuk untuk ...sebagai supervisor lah ....hierarkis tetap ...dalam pelaksanaan tugas hirarki tetep mas... berkaitan dengan tandatangan administrasi... saya punya pendapat gini ...ini kan POAC inikan harus teori... teori itu diciptakan... memang berdasarkan proses–proses yang ilmu pengetahuan... tetapi menurut saya di cyber itu sebener nya perencanaan dan organisasi itu dalam satu badan... bener–bener berarti dia yang merencanakan juga ada juga yang mengorganisasi juga... berkaitan dengan pengawasan... jadi nggak... ngak bisa ngak bisa berdiri sendiri ya ...nggak bisa berdiri sendiri secara utuh ...jadi memang perencanaan di kepolisian nggak mesti ngikutin teori – teori yang ada dibuku itu ...karena dalam prateknya dengan perencanaan itu udah satu jalan ...kecuali perencanaan dan pelaksanaan ada perbedaan ...kalau pelaksanaan itu udah mau kerjanya ...tapi kalau perencanaan itu *... * itu aja."* (*FGD* Pamen)

Dalam hal pembagian tugas, peranan Kanit sangat penting sebagaimana diungkapkan dalam *FGD* Pamen sebagai berikut:

"Tapi dalam organisasi sekecil apapun itu harus ada yang namanya leader, kalau tidak ada, Kita tidak akan bisa melaksanakan tugas-tugas itu, itu emang dalam satu organisasi kenapa di Polri ada pangkat dan sebagainya, emang itu adalah salah satu itu sudah terbentuk yang demikian, kalau semuanya sudah punya kemampuan, semuanya bisa dan tanggung jawab mereka semuanya penyidik, kalau toh itu ada cas kecil itu akan di bentuk satu tembok untuk memecahkan itu, kalau semuanya tidak merasa ada leader atau siapa yang minta di sebutkan sebagai anatomi, ini tidak akan menjadi tujuan apa yang kita harapkan, nah itu jelas, saya rasa leader itu perlu di situ, tapi didalam unit, emang leadernya adalah satu unit di bawahnya staf, kalau semua itu udah ada pembagian tugas, tugasnya apa bertanggung jawab kepada siapa, harusnya itu jelas, tidak bisa bahwasannya, nanti ikut ini, saya nanti ikut ini, walaupun itu tembok, yang relatif sangat kecil di bentuk, ada 3 orang atau 4 orang, siapa yang di-leader-kan di situ dengan maksud apa, untuk mengkoordinasi bukan berarti leader-nya paling hebat, tidak, hanya untuk mengkordinasikan, apa yang telah dicapai oleh tim ini." (*FGD* Pamen)

Kanit mengetahui keahlian masing-masing anggota yang beragam dan berupaya saling melengkapi untuk menciptakan sinergi sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"Kalau itu semua nya rata masing-masing, ini tidak akan tercapai, tentunya ada ka unit, jenjang ini lah yang membuat suatu sistim ini bisa berjalan, ada leader-nya, tadi yang di sebut oleh Pak Dicky walaupun itu suatu cara peraturannya memang ada keuntungan dan kerugian, keuntungan di mana, kerugian di mana, yang kita harapkan semuanya bisa menguasai dan bisa tapi ada case-case tertentu yang tidak bisa ditangani seorang butuh pengaturan beberapa orang, terus ada membutuhkan dari keahlian yang lain sebagai contoh dari apa unit lodrom yang ada di dalam sini, saling mendukung dalam tim ini" (*FGD* Pama)

4.4.2.4 Kebanggaan Karena Memerlukan Pengetahuan Khusus

Tingkat kesulitan pekerjaan bagi anggota Unit V *IT & Cybercrime* adalah hal paling signifikan yang membedakan mereka dengan polisi yang lain. Bidang yang ditangani Unit V *IT & Cybercrime* terkait dengan teknologi maju dan alat-alat canggih. Mereka dihadapkan pada kesenjangan pengetahuan dan keterampilan Polisi yang diberikan institusi Polri dengan kegiatan penyidikan yang mereka emban sebagai tugas. Kesenjangan inilah yang membuat mereka percaya bahwa pekerjaan yang mereka lakukan lebih sulit dari pekerjaan Polisi

pada umumnya sebagaimana diungkapkan dalam *FGD* Pama.

> *"Saya kira wajar... karena dari bahasanya aja... bahasa asing... IT... Cybercrime... kita juga harus menyadari bahwa dengan nama itu kita jadi terbebani untuk lebih mendalam berkaitan dengan komputer... komputer itu sesuatu yang rumit... nggak sembarang orang bisa kan... nggak sembarang orang bisa menguasai komputer... kalau orang bekerja di cybercrime berarti....hebat dong...ha..ha..ha..."* (*FGD* Pama)

Perbedaan tersebut memberikan kebanggaan tersendiri. Keberadaan para anggota di Unit V *IT & Cybercrime* memberikan para anggota pengetahuan dan kesempatan yang tidak didapatkan penyidik tindak pidana konvensional sebagaimana diungkapkan dalam *FGD* Pama.

> *"...pada dasarnya kita sama-sama mendapatkan pendidikan, namun kita diberi kemampuan lebih tentang kasus-kasus, sehingga anggapan dari temen-temen yang konvensional itu kan sudah ada frame-nya, kita didik itu bisa, namun bagi para penyidik ini, ini butuh keterampilan khusus, yang dilatarbelakangi dengan kemampuan dan keterampilan sehingga anggapan mereka ini adalah memang orang-orang yang terampil atau expert dalam bidangnya selain dia punya kemampuan penyidikan dia juga punya kemampuan IT."* (*FGD* Pama)

Dengan mengetahui teknologi komputer sebagai alat komunikasi, anggota Unit V *IT & Cybercrime* dianggap lebih atau hebat oleh polisi lainnya yang biasanya menangani tindak pidana konvensional sebagaimana diungkapkan dalam *FGD* Pama.

> *"...kau masuk aja ke unit Cybercrime ..saya pikir koq saya ke Cybercrime...koq susah banget... tapi begitu saya di Cybercrime banyak sekali yang saya dapet... saya bisa keluar negri.. saya ngerti internet... saya mengerti komputer...temen saya nggak tau... saya tau... puluhan e-mail saya tau... apa itu browsing... apa itu chatting... temen saya nggak ada yang tau sampe hari ini... mereka nggak punya e-mail... saya punya e-mail... saya bicara sama di angkatan saya... dan saya dianggap mereka tu hebat ...hebat sekali..."* (*FGD* Pama)

> *"Orang kan berpikir kan komputer gitu kan ...wah hebat nih... komputer..."* (*FGD* Pama)

Selain itu, anggota Unit V *IT & Cybercrime* mempuyai kesempatan yang lebih besar untuk dikirim ke luar negeri dalam menjalin kerja sama dengan negara lain atau untuk kepentingan pelatihan sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Tapi saya bangga di unit saya... pas dibuka... wah di mana nih... di Singapura ...Singapura sekolah ... ya... padahal jalan – jalan... "* (*FGD* Pama)

> *"Ya ...kebetulan saya masuk ke cybercrime masih blank ...tapi setelah saya jalani ...ternyata saya sangat beruntung ...beruntung ...ya banyak ilmu dan... yang saya dapatkan ....kalau untuk *..... * saya udah sempet keluar negeri walaupun itu ke Singapura .."* (*FGD* Pama)

> *"Pada saat kita menangani satu kasus yang sifatnya lebih bergengsi seperti cybercrime, narkotik, terorisme, itu orang melihat kita ini orang punya kemampuan lebih sehingga kita tempatkan disana."* (*FGD* Pama).

4.4.2.5 Bekerja Lebih Pintar Bukan Lebih Keras (*Work Smarter Not Harder)*

Sebagai unit yang menangani kejahatan komputer, para penyidik di Unit V *IT & Cybercrime* mempunyai cara kerja yang berbeda dengan penyidik lainnya yang menangani tindak pidana konvensional. Mereka bekerja lebih didominasi dengan otak bukan otot dalam melakukan penyidikan. Mereka percaya untuk berpikir lebih cerdas bukan bekerja lebih keras. Kemampuan anggota dalam penyidikan dibarengi dengan kemampuan memahami penggunaan teknologi komputer dalam melakukan tindak pidana sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Ya... kan... karena disini kita bekerja berdasarkan logika... logic gitu... ya... satu lagi mungkin gini... Indonesia ini kan menerima komputer... internet itu blek... langsung jadi gitu lho...o... kita kan tau nya o... komputer itu seperti ini... internet itu seperti ini... prosesnya kan kita nggak pernah tau kan.... ya... di Cybercrime kita tuh mempelajari itu ...suatu...misalnya terjadi pengiriman e-mail...isinya apa-apa gitu kan ...orang kita awam taunya breg ..itu e-mail kita terima...nah di Cyber kita*

mempelajari... menelusuri ...ke belakang...ini prosesnya gimana...sih ...sampe e-mail itu ada disitu ...yang jadi spesifik di situ...orang jadinya o...hebat dong ...Cybercrime..." (*FGD* Pama)

Sebagian penyidikan dilakukan juga di *cyberspace* sehingga penyidik memerlukan keterampilan berinteraksi melalui komputer, tidak seperti reserse lainnya yang melakukan penyidikan pada umumnya.

"Yang istimewa mungkin mas karena dia penyidik nya kan... kalau apa...di Cybercrime itu kan nggak bisa nyata... kejahatan nya yang maya lantas bisa terungkap ... beda dengan reserse – reserse" (*FGD* Pama)

"Penjahat ditangkep... lewat komputer... bukan ditangkep lewat komputer maksudnya... dicari penyadap gitu... ini bisa dinyatakan tersangka atau ini terdeteksi... karena ini berbuat tindak pidana... lewat komputer itu... nah dia baru berpikir... koq bisa... lewat komputer koq bisa...gitu" (*FGD* Pama)

"...Jadi dalam hal penyidikan... kalau di kejahatan nyata yang nggak tau kaya kriminal secara umum... itu kalau untuk penyidikan... kan itu betul-betul orang yang peka... orang yang menyelidiki... diambil di lokasi... tapi kalau kejahatan di internet penyidikannya itu adalah berupa seperti imajinasi begitu... kita masuk ke suatu...e...room nya orang... jadi kita pura-pura... jadi penyidikannya bukan dengan manusia yang hadir... tapi bahasa-bahasa... bahasa-bahasa komputer lah istilahnya... peralatan komputer ....nah itu yang bikin sulit ...dan berbeda dengan kejahatan secara... penyidikan makanya pengungkapan kejahatan dari cyber relatif sangat sulit... daripada penyidikan kejahatan nyata... karena kalau kejahatan nyata dia bisa bertanya kepada orang lain... ya... itulah penyidik, dia juga bertanya kepada orang lain... kalau kita penyidik dalam komputer... orang ini kan benda mati... kita bertanya ini susah... ya itu dia yang susah ya itu dia yang susah dipahami... dalam hal itu...dalam hal penyidikan... saya rasa versi – versi yang lain juga ada tu..." (*FGD* Pama)

Penyidik Unit V *IT & Cybercrime* perlu memiliki kemampuan penyidikan tindak pidana konvensional ditambah dengan kemampuan penyidikan melalui internet dan *laboratorium* forensik komputer sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"...proses penyidikan konvensional tetap jalan... yang unik disitu... berkaitan dengan alat bukti yang harus dikumpulkan... bukti-bukti yang harus dikumpulkan karena ada...ada berkaitan dengan komputer... jaringan komputer... dan sistemnya segala macem... kaitannya dengan bukti elektronik... itu yang spesifik... dengan fungsi lain... makanya dikita pun ada laboratorium... ada laboratorium forensiknya..." (*FGD* Pama)
"Sebetulnya dalam penyidikan memang a....lebih sulit ya ...tapi dalam pembuktian menurut saya ....sangat lebih mudah ...karena bukti yang kita temukan adalah ...bukti obyektif.... apa yang direkam ...di komputer itu kan pasti ...gitu..." (*FGD* Pama)

"Contohnya gini Pak misalnya ...sama sih cuma saya lebih mudah lagi ...kalau katakanlah orang mencuri ...ditemukan ada bukti – bukti..mencongkel ya ...merobek... itu barang buktinya ...alatnya ada pisau.. obeng apa... ha .pisau ...apa semua itu ..polisi mengumpulkannya mudah kalau ada disitu ...kalau di kita kan barang buktinya ..file ..log file ...ya nggak .. data-data digital ...dividen-nya apalagi nih misalnya e..cakram nya ..ininya ...ininya ...itu agak sulit ..." (*FGD* Pama)

4.4.2.6 Budaya Progresif

Perkembangan teknologi semakin cepat, begitu pula perkembangan *cybercrime*. Untuk mengikuti perkembangan tersebut anggota Unit V *IT & Cybercrime* memacu diri meningkatkan kemampuannya untuk mempelajari hal-hal yang baru secara pribadi, melalui ajang diskusi non-formal atau pelatihan. Kegiatan belajar secara mandiri untuk mengejar ketinggalan dalam pengetahuan komputer dilakukan oleh beberapa anggota sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"...tadi Pak Arief bilang banyak polisi itu gaptek... ya termasuk saya... juga gaptek... begitu saya masuk unit Cyber... kita belajarnya juga seperti kura-kura... terseok-seok... begitu nggak tau... ya itu tadi Pak... seperti yang saya bilang... polisi itu umumnya gaptek..." (*FGD* Pama)

"Pengalaman saya.... saya chatting pertama kali diajarin sama Bapak Setiadi ...baru pertama kali saya ...kemudian saya suruh milih itu nama ...saya pilih nama Bagas Nugraha ..." (*FGD* Pama)

*"Terus .... kalau *...* keluar itu begitu ngomong dines di mana .. cybercrime ...orang-orang udah ..wah ...hah.a.a.a.padahal ...haha.dulu sebelum masuk cybercrime ...saya nggak bisa main chatting ..main*

internet ...itu nggak ....nggak ..tapi setelah lama di situ insya allah ..." (*FGD* Pama)

Tidak hanya peningkatan sumber daya manusia, Unit V *IT & Cybercrime* juga melakukan peningkatan infrastruktur untuk menunjang pelaksanaan tugas Unit V *IT & Cybercrime*. Budaya untuk terus berpacu merupakan perwujudan dari budaya progesif. Tanpa adanya budaya progressif, penyidikan *cybercrime* akan tertinggal dengan kejahatan yang semakin canggih sebagaimana diungkapkan dalam *FGD* Pamen sebagai berikut:

"Seperti yang di sampaikan pak edi tadi, di samping positifnya teknologi ini ada dampak negatifnya, penipuan, terorisme, yang kedua terjadinya pergeseran kejahatan konvesional yang berbentuk kekerasan, pake linggis dan senjata tajam lainnya, kalau teknologi itu menjadi pergeseran dengan komputer kita bisa melakukan segalanya segalanya, apakah itu mencuri data, menipu, sehingga dengan adanya kejahatan ini yang biasanya kita menangani kejahatan konvesional kita jadi gaptek bagaimana kalau terjadi cara menggunakan kejahatan-kejahatan dengan teknologi, maka dengan kejahatan ini diperlukan orang yang khusus dan peralatan yang khusus gitu loh, nah peralatan ini sangat mahal, kita nggak bisa jadi di cybercrime, seperti kita mau melakukan pemecahan satu kasus, butuh apa namanya advis, nah advis itu mahal dan itu perlu orang khusus untuk menangani hal ini". (*FGD* Pamen)

4.4.2.7 Budaya Adaptif

Perkembangan teknologi mempunyai dampak negatif dengan adanya kecenderungan berkembangnya bentuk kejahatan yang berbasis teknologi. Bentuk kejahatan ini semakin berkembang dan marak dengan antisipasi yang tidak memadai dari perangkat hukum. Para penyidik Unit V *IT & Cybercrime* memahami keberadaannya sebagai bentuk antisipasi dari institusi Polri. Para penyidik harus lebih giat melakukan terobosan dalam penyidikan *cybercrime* sebagaimana diungkapkan dalam *FGD* Pamen sebagai berikut:

"...sedangkan sekarang sudah berkembang kejahatan cyber di Indonesia, karena hanya Indonesia dan Laos di Asia yang belum punya peraturan undang-undang, dan mungkin 2007 akan di-launching-kan undang-undang ini, itu kalau untuk Indonesia, mungkin boleh dikatakan selama

Indonesia masih primitif perundang-undangannya, umbrella-nya tidak ada, mudah-mudahan dengan ini bisa dikatakan Polri sudah jauh melangkah dengan negara yang lain, selangkah atau dua langkah lebih maju..." (*FGD* Pamen)

Kaedah hukum normatif yang ada di Indonesia belum mencakup penggunaan internet, data eletronik dan jaringan sehingga diperlukan kemampuan interpretasi dari para penyidik sebagaimana terungkap oleh beberapa partisipan dalam diskusi kelompok terfokus dan informan wawancara berpedoman sebagaimana diungkapkan dalam *FGD* Pamen, *FGD* Pama, WBIS 01 A, WBIS 02 A sebagai berikut:

"Mungkin tingkat kesulitannya contohnya tadi sudah dicontohkan oleh Pak Alex ...penggunaan melalui internet ...itu kan dalam KUHP dikatakan barang siapa....mungkin agak mudah barang siapa melakukan ..e..kemudian nanti dikatakan di muka umum ..nah apakah internet itu udah media umum ...di muka umum ...dalam penyidikan kita perlu apa ...masih menganalogi ..masih menganalogi kembali apakah ...dengan menista seseorang melalui (internet) ..internet itu sudah dikatakan di muka umum ...gitu ....sedangkan kesulitan dalam memenuhi unsur." (*FGD* Pamen)

"Kita menganalogikan ...artinya ...jadi ...misalnya kita berpikir nya kan seperti ini ...dulu aliran listrik, aliran listrik dulunya kan ditetapkan dengan ...sebab pencurian aliran listrik dulunya... dulunya udah ada ....* dikatakan sebagai benda ...termasuk benda kan dia barang ...nah kenapa kita berpikir nya bahwa data elektronik yang ada di e..jaringan komputer atau di media-media komunikasi lainnya ..itu sebagai ...sebagai barang atau benda ...apa bedanya dia dengan aliran listrik ...kan kita menganalogi nya seperti itu ...misalnya orang kasus yang ...sebenernya yang banyak a...deface itu sebenernya hacking ya ...perbuatan hacking ...dia kan masuk kejaringan orang merusak gitu kan ..ha..kita...kita bisa menganalogikan ...dia melakukan perbuatan merusak ...dia kita analogikan masuk ke pekarangan orang tanpa ijin dan pengrusakan gitu ..."* (*FGD* Pama)

"Menurut saya dari memahami pengalaman negara lain yang saya temui di beberapa conference maupun seminar kita bisa membuat aturan sendiri berkaitan dengan kejahatan komputer atau cybercrime yang dalam hal ini menyangkut hacking sehingga ada payung hukum bagi penyidik untuk melakukan penindakan untuk penyidikan disitu juga diperlukan aturan-aturan tersendiri yang berkaitan dengan tindak pidana cybercrime ini

utamanya dikaitkan dengan data digital dan berapa lama pihak-pihak untuk menyimpan data-data yang berkaitan dengan data digital ini seperti misalnya USB berapa lama dia harus menyimpan data yang ada padanya sehingga pada saat penyidik membutuhkan data itu dia bisa memberikan data tersebut sehingga dibutuhkan undang-undang atau aturan tersendiri yang keluar dari yang berada di luar KUHP." (WBIS 01 A)

"Dari segi pemenuhan acara ada kesulitan terutama yang tadi saya sebutkan kasus-kasus yang ditangani oleh cyber misalnya adalah tentang pencurian data, pencurian data informasi melalui komputer misalnya itu kita harus bisa membuktikan apakah yang dicuri data itu sudah termasuk pengrusakan karena istilah pengrusakan di KUHP sesuatu barang yang sudah tidak bisa digunakan kembali, sedangkan data itu bisa diambil dengan menggunakan alat yang ada di forensik dan data itu yang bisa timbul kembali itu yang menjadi permasalahan, kok data ini sudah hilang tapi bisa timbul kembali apakah data itu yang disebut rusak itu yang masih menjadi kontra" (WBIS 02A)

"Pada waktu itu kami memiliki payung hukum Undang-undang 22 tahun Undang-undang 36 tahun 99 tentang pertelekomunikasi kita menggunakan pasal 22 ayat b tentang penyalahgunaan memasuki akses jaringan orang secara tidak sah kemudian kita menggunakan pasal 406 tentang pengrusakan nah ini yang jadi masalah adalah pada saat kita mempermasalahkan pasal 406 dari Jaksa pun ragu-ragu karena yang disebut dengan merusak itu bagaimana ini kan bukan barang itu yang jadi permasalahan." (WBIS 02A).

Tidak hanya dalam normatif materil, pada normatif formil pun terdapat permasalahan kelemahan hukum terutama menyangkut barang bukti sebagaimana diungkapkan dalam *FGD* Pama dan WBIS 01 A sebagai berikut:

"Masalahnya KUHAP kita ..e.. Hukum Acara Pidana kita tidak ... tidak ...tidak mengaku bukti itu ...di situ masalahnya.. jadi yang dilakukan oleh penyidik ...rekan-rekan temen-temen penyidik ini ...gimana data-data yang ada itu ...seperti yang didapat dari komputer ..dan media penyimpanan lain itu bisa menjadi alat bukti seperti yang diharapkan oleh Hukum Acara Pidana" (*FGD* Pama)

"Dalam kasus partai Golkar mungkin kesulitan yang dihadapi penyidik adalah bagaimana mengangkat data-data yang ada atau data digital yang ada dari server itu menjadi alat bukti yang akan digunakan diperadilan yang mana KUHAP kita sendiri belum mengakomodir mengenai alat bukti digital sehingga langkah yang dilakukan adalah mengubah dari bukti

digital itu menjadi memenuhi unsur pasal 184 untuk alat bukti yang diakomodir oleh KUHAP." (WBIS 01 A)

Anggota Unit V *IT & Cybercrime* pun merasa telah melakukan terobosan hukum dalam menangani kasus *cybercrime* sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

*"Sebetulnya ...menurut saya pribadi ya ...sebetulnya mulai tahun ini ...saya rasakan kita *...* seperti mendobrak beberapa bukti yang belum ada ...kita berusaha menemukan ...seperti nya berusaha mendobrak ....makanya sekarang *.....* yang terbaru ini mulai cepat-cepat dibutuhkan karena*.....* itu kalau mau dibilang ..ya ...ini yang ..yang ...ada lagi kalau bukti yang agak susah ya ...mungkin orang nggak lazim ya ...misalnya kita melakukan kejahatan dengan komputer itu contohnya ... yang dulu kasus *.....* kemudian kita hapus ya ...file-nya kita hapus ...orang kan ...kalau orang yang nggak ngerti ...dan saya juga saat itu juga nggak tau ...nggak semua orang bisa buka ...dicari file-nya kan sudah kosong ...di line *..* juga sudah dihapus ...terus cari datanya di mana..."* (*FGD* Pama)

Dalam perspektif ilmu manajemen, budaya adaptif (*adapative culture*) adalah budaya dari organisasi yang memiliki anggota yang terfokus pada perubahan kebutuhan pelanggan dan *stakeholders* lainnya serta mendukung inisiatif-inisiatif untuk mengejar perubahan tersebut. Elemen dari budaya adaptif terdiri dari: fokus pada eksternal; anggota memberikan perhatian pada proses sebanyak perhatian pada hasil dengan cara para anggota berupaya memperbaiki proses internal yang ada dalam organisasi untuk melayani *external stakeholders*; anggota mempunyai rasa memiliki yang kuat dan mereka percaya bahwa peningkatan *performance* organisasi merupakan tanggung jawab bersama bukan tanggung jawab perorangan (McShane & Glinow, 2003: 457). Dalam Unit V *IT & Cybercrime* tersebut telah terdapat benih-benih budaya adaptif sebagaimana yang dicirikan oleh McShane. Benih-benih ini contohnya adalah Unit V *IT & Cybercrime* telah terfokus pada *external stakeholders*, dalam hal ini pelapor sebagai bagian dari masyarakat, walaupun perangkat undang-undang baik formil dan materil belum memadai. Selain itu, mereka juga memiliki kebanggaan atas unitnya dan menyadari pentingnya kerja sama antar anggota unit untuk

menciptakan sinergi.

Menurut Kasali (1994: 285), budaya organisasi menghasilkan identitas perusahaan baik *visible* maupun *invisible*. Budaya organisasi tersebut berasal dari kompleksitas lingkungan. Kompleksitas lingkungan itu berasal dari nilai-nilai karyawan dan yang terpenting lagi nilai-nilai para pendiri dan pemimpin puncak. Seorang pemimpin dengan gaya kepemimpinannya berdampak langsung pada pembentukan suatu budaya organisasi. Pemimpin tersebut memberikan teladan nilai-nilai yang dianggap baik, dari kegiatan yang dianggap positif sampai dengan diproduksinya benda-benda sesuai standar pemimpin. Seorang pemimpin yang demokratis misalnya, akan menimbulkan suatu budaya organisasi yang terbuka akan saran para anggota.

Kanit V *IT & Cybercrime* mempunyai pengaruh bagi setiap anggotanya. Apabila pemimpin tersebut tidak peduli terhadap tugasnya, maka setiap anggotanya juga akan berperilaku yang sama, yaitu tidak peduli atau masa bodoh terhadap apa yang telah menjadi tugas dan tanggung jawabnya sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Kalau memang leader-nya itu juga masa bodo saya rasa anak buahnya juga ikut masa bodo... tergantung... jadi berpengaruh... kalau pemimpin kita baik... ya akan baik... istilah nya mengerti... bidang tugasnya... saya rasa anak buahnya ikut melaksanakan tugasnya dengan baik..."* (*FGD* Pama)

Kepemimpinan di Unit V *IT & Cybercrime* juga berhasil menciptakan suasana yang kondusif bagi para anggota untuk bekerja sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Tentu yang bikin nyaman lingkungan, rekan kerja di sini ya itu atasannya, istilahnya komunikasi ini, saling bekerja sama-lah, tidak mengucilkan, membedakan dan sebagainya, kita akan nyaman, dan yang kedua nasib juga, apa ya, masalah lalu di wilayah, jauh kesibukan, sedangkan di wilayah itu jauh, sehingga apalagi mengingat usia saya masanya pensiun tentu kalau di tempat lain yang butuh kesibukan, jadi saya cenderung masih di cyber di samping itu pun kita ke wilayah yang kita dapatkan, di cyber itu istilahnya kok nggak monoton, di situ informasi kita bisa masuk"* (*FGD* Pama)

Suasana atau lingkungan kerja yang nyaman tergantung dari seorang pemimpinnya. Seorang pemimpin diharapkan dapat menciptakan suasana kerja yang kondusif sehingga kinerja organisasi dapat berjalan dengan lancar. Berdasarkan hasil wawancara berpedoman dengan anggota Unit V *IT & Cybercrime*, terdapat perbedaan manajemen antara kepemimpinan terdahulu dengan sekarang. Penjabarannya terdapat dalam Tabel 4.6 berikut:

Tabel 4.6
Perbandingan Unit V *IT & Cybercrime* dulu VS sekarang

Kriteria	Sebelum 23 Januari 2006	Setelah 23 Januari 2006
Pemahaman	berkaitan dengan umur, pemahaman Kanit mengenai *cybercrime* tidak ada	memiliki pengetahuan mengenai *cybercrime* sehingga penyidikan semakin berkembang
Penegakan hukum	basif, menunggu laporan, tidak ada kegiatan	aktif, melakukan pelatihan, pemberdayaan sumber daya manusia, meningkatkan jaringan kerja sama, *cyber patrol*, melakukan berbagai program kerja lainnya.
Kinerja	seperti *Time Zone*, datang main *game*, selesai pulang.	ada tugas baik penyidikan maupun non-penyidikan yang harus dilakukan.
Pelatihan	hanya orang tertentu	pelatihan merata hampir ke seluruh anggota baik dalam dan luar negeri
Anggaran	jarang disetujui	sering disetujui atau Kanit menyediakan dananya.
Proses Kerja	sangat jauh berbeda dengan sekarang, tidak terstruktur	setiap anggota sudah cukup baik dan mampu bekerja, terdapat proses kerja yang lebih matang
Kasus yang ditangani	bukan kasus *cybercrime*	kasus *cybercrime* dan kejahatan komputer
Fasilitas	sangat tidak manusiawi, hanya tiga komputer dan satu pesawat telepon	masing-masing anggota mempunyai komputer, terdapat *printer*, fax, telepon, laptop dan *laboratorium* forensik komputer.

(Sumber: *FGD* Pama dan Pamen)

Perubahan pada Unit V *IT & Cybercrime* terdeteksi oleh para anggota dan mereka lebih menyukai perubahan yang terjadi. Mereka menganggap perubahan

tersebut membawa kemajuan dan berdampak baik pada kinerja Unit V *IT & Cybercrime* sebagaimana diungkapkan dalam *FGD* Pamen dan *FGD* Pama sebagai berikut:

> *"Ya sebenernya itu awal-awal itu karena ....nggak sebanyak ...kasusnya nggak sebanyak ini ..ya ...dulu waktu pembentukan tiga orang itu ya ...kita masih terima surat-surat....semacam kaya surat pengaduan ...jadi kita nggak sesibuk kaya sekarang ...kasus tu banyak ..dulu kita hanya sekedar back up ...cuma bales surat aja ...kalau ada diskusi-diskusi ...jadi karena kita terbatas tiga orang itu aja ..ya ...jadi kita sekedar .. hah.a.a.ya. ...bales surat biasa aja ...jadi sekarang kaya banyak kasus jadi kita kerjakan rame-rame ...kita sharing ...kalau dulu ya ...cuma bales-bales surat aja ....gitu aja"* (*FGD* Pamen)

> *"Terus saya sescapa di hukum 6 bulan... abis di hukum 6 bulan saya Indag satu tahun tiga bulan ...kemudian saya ditarik ke Cybercrime ...Cybercrime itu ... bapak–bapak ini belum ada. ..yang ada saya sama bapak itu ....berdua .... Bapak Budi... sepi.... kaya hutan ...begitu ....begitu ... tapi saya seneng banget ...karena pas dia masuk ....rombak"* (*FGD* Pama)

Budaya yang ada di Unit V *IT & Cybercrime* merupakan budaya yang baru dan merupakan transformasi dari budaya yang lama sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Bebas berbicara ....bebas mengeluarkan pendapat ....sekarang ini yang baru saya temukan ...dulunya nggak pernah ..."*(*FGD* Pama)

> *"Dari pimpinan saya yang baru ini ...mulai dari Pak Petrus ...jadi kita diberi kebebasan ....walaupun disaat beliau nggak ada ...cuma kumpul-kumpul gini ya ...yang hierarki itu tetep ada ....kita lapor ke beliau ...tapi kita tetep jalan ...kalau dulu sih saya nggak menemukan seperti ini ...mas ...diem ...nunggu perintah baru jalan ..."* (*FGD* Pama)

> *"Kalau kita sudah kumpul...kita mengeluarkan pendapat ...pun itu takut sekali dan sampe sekarang masih ada pimpinan itu yang masih .. ... itu tergantung leader nya ..."* (*FGD* Pama)

> *"Jadi mungkin kepemimpinan dulu itu beda. ...mungkin masa bodo bisa*

jadi ... kalau memang leader nya itu juga masa bodo saya rasa anak buah nya juga ikut masa bodo...tergantung ..jadi berpengaruh ...kalau pemimpin kita baik ...ya akan baik ...istilahnya mengerti ...bidang tugasnya ...saya rasa anak buahnya ikut melaksanakan tugas nya dengan baik. ... " (*FGD* Pama)

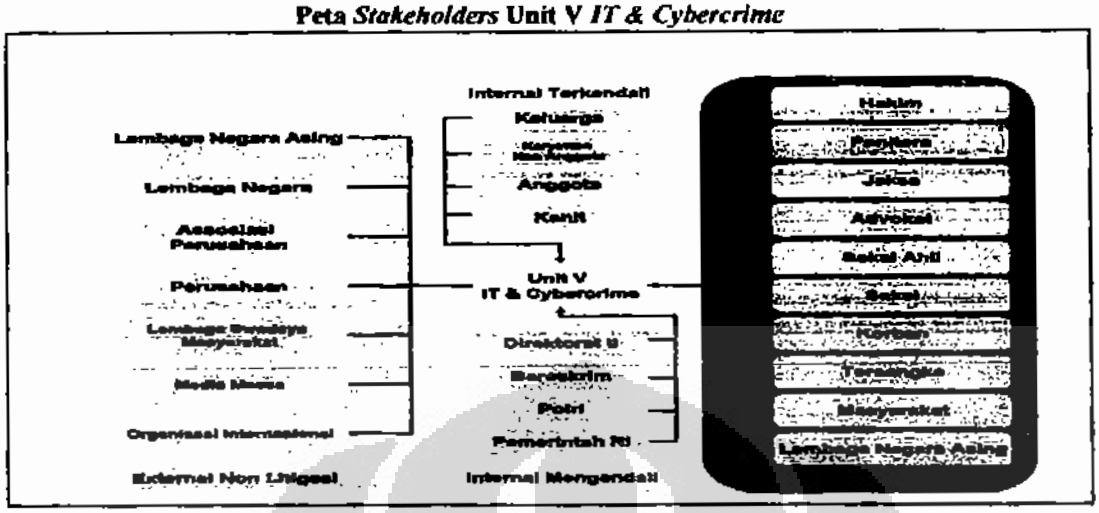
Budaya yang baru tertanam belum tentu sesuai atau bahkan bertentangan dengan budaya Polri pada umumnya sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

"Saya pernah ngalamin... ... ...saya pernah ngalamin ...kita lagi nanganin satu permasalahan ya ...saya dari Cyber waktu itu bersama salah satu seorang senior ...diminta bantuan mem-back up ...pekerjaan unit lain ...direktorat lain ....sampe di tempat kita berkumpul ...pimpinan yang ada di situ pada saat itu mengajak ...oke ..kita sharing ..katanya kan ...sharing ...saya berpikir sharing seperti di Cyber ...ngomong bebas apa adanya ..karena saya berpikir seperti itu ...ya ...saya ngomong seperti di Cyber ...di tegur ...kamu itu ...wah ...saya jadinya ...wah ini salah bukan sharing jadinya ... " (*FGD* Pama)

4.4.3 Analisis Pengaruh *Stakeholders* dalam Manajemen Penyidikan

Dalam implementasinya, manajemen penyidikan tindak pidana *hacking* tidak dapat terlepas dari berbagai faktor yang dapat mempengaruhi tercapainya tujuan penyidikan. Faktor yang mempengaruhi tersebut terdiri dari pihak yang berkepentingan (*stakeholders*) baik eksternal dan internal. Menurut Kasali (1994: 63) dan Stoner (1996: 64) pihak yang berkepentingan atau *stakeholders* adalah kelompok atau individu yang secara langsung atau tidak langsung mempengaruhi cara organisasi berusaha mencapai sasarannya. Pihak berkepentingan (*internal stakeholders*) adalah kelompok atau individu yang merupakan bagian dari lingkungan organisasi yang memiliki seorang pemimpin yang tetap bertanggung jawab atas orang atau kelompok tersebut. Sedang *external stakeholders* merupakan pihak yang berkepentingan namun di luar organisasi.

Bagan 4.6
Peta *Stakeholders* Unit V *IT & Cybercrime*



(Sumber: Hasil Observasi, *FGD*, wawancara berpedoman yang diolah Penulis)

*Stakeholder*s yang jumlah dan kepentingannya banyak dan beragam tersebut dapat dipetakan berdasarkan pengaruhnya pada tujuan Unit V *IT & Cybercrime*, serta ditentukan tingkat prioritas hubungannya seperti Tabel 4.7 di bawah ini:

Tabel 4.7
***Stakeholders* Unit V *IT & Cybercrime* dan kepentingannya**

***Internal Stakeholders* Pengendali**	**Kepentingan**
Polri, Bareskrim, Direktorat II, Kanit	Terlaksananya: visi, misi, instruksi, kebijakan
***Internal Stakeholders* Terkendali**	**Kepentingan**
Anggota	Kepuasan kerja, pendapatan, jenjang karir
Karyawan non Anggota	Kepuasan kerja, pendapatan,
Keluarga	Waktu bersama keluarga, pendapatan, keselamatan
***External Stakeholders* Litigasi**	**Kepentingan**
Jaksa	Berkas perkara yang lengkap, penyidikan sesuai prosedur, ketersedian barang bukti dan ahli serta saksi pendukung lainnya, imbalan.
Hakim	Berkas perkara yang lengkap, ketersediaan saksi, ahli, barang bukti, proses pengadilan yang lancar, prosedur penyidikan yang sesuai dengan aturan, imbalan.
Tersangka	Penerapan hukum, penegakan hak tersangka, terbebas/lepas dari dakwaan, hukuman yang ringan, proses yang manusiawi, proses cepat biaya murah.
Advokat	Penerapan hukum termasuk hak tersangka, kemudahan dan keringanan bagi kliennya, aparat yang kooperatif, imbalan.
Korban	Hukuman yang setimpal, proses yang cepat dan murah.
Saksi	Proses yang cepat.
Ahli	Proses yang cepat, kasus yang menantang, imbalan.
Panitera	Dokumentasi yang lengkap, proses yang cepat, para pihak yang koperatif, imbalan.
Masyarakat	Terciptanya rasa keadilan.

Lembaga negara asing	Kerja sama antara lembaga atau aparat penegak hukum, *transfer* atau *sharing* pengalaman dan pengetahuan, tegaknya hukum
External Stakeholders **Nonlitigasi**	**Kepentingannya**
DPR, Bank Indonesia	Masukan bagi kebijaksanaan, pembuatan undang-undang
Media massa	Berita terhangat
Perusahaan, asosiasi perusahaan	Bantuan atau kerja sama peningkatan di bidang infrastruktur, sumber daya manusia, alih teknologi, keamanan
Lembaga Swadaya Masyarakat	Bantuan atau kerja sama peningkatan di bidang infrastruktur, sumber daya manusia, alih teknologi
Pengusaha	Jaringan, kesepahaman, rasa aman
Organisasi internasional/regional	Terbentuknya kerja sama di tingkat internasional/regional, bantuan atau kerja sama peningkatan di bidang infrastruktur, sumber daya manusia, alih teknologi, keamanan
Lembaga negara asing	Terbentuknya bantuan atau kerja sama antar negara peningkatan di bidang infrastruktur, sumber daya manusia, alih teknologi, keamanan

(Sumber: Observasi, *FGD*, Wawancara berpedoman)

4.4.3.1 Analisis Pengaruh *Internal Stakeholders*

Dalam tubuh Polri, Unit V *IT & Cybercrime* bekerja sama dengan unit atau satgas Polri lainnya untuk menegakan hukum. Pengetahuan khusus mengenai forensik komputer diperlukan untuk mengerjakan kasus yang menjadi bagian dari satgas atau unit lain. Dalam pelaksanaan tugas tersebut terjalin kerja sama dan koordinasi lintas unit sebagaimana diungkapkan dalam WBIS 01 A sebagai berikut:

> *"Pengalaman saya kemarin saya pernah menangani membantu satgas yang bekerja di illegal mining yang membutuhkan penanganan server satu server terdapat 7 minimal 7 hard disk yang harus kita backup sehingga untuk tugas berkaitan dengan data digital saja pengambilan data digital saja sudah membutuhkan anggaran yang tidak kecil itu belum dikaitkan dengan mobilitas penyidik sendiri mobilitas komunikasi dan sebagainya yang memang butuh dana yang tidak kecil."* (WBIS 01 A)

Sedangkan di Bareskrim, bila ada laporan yang berkenaan *cybercrime*, pelapor dapat langsung membuat laporan dengan kebijaksanaan satu pintu di Bareskrim untuk kemudian laporan tersebut diserahkan kepada unit yang paling berkaitan. Kebijaksanaan tersebut tidak berlaku secara kaku sebagaimana yang terjadi dalam kasus *deface website* Partai Golkar. Partai ini berkonsultasi dahulu pada Kanit V *IT & Cybercrime* baru kemudian membuat laporan sebagaimana diungkapkan dalam WBIS 01 A sebagai berikut:

"Pertimbangan kanit pada saat itu bahwa yang mengerti teknis cybercrime ini adalah kita unit cybercrime sehingga akan lebih memudahkan memberikan pelayanan kepada pihak yang akan melapor sehingga tidak mengambil waktu yang lama tidak bolak balik laporan polisi karena biasanya laporan polisi yang diterima dipiket siaga itu tidak akan langsung ke unit yang bersangkutan tapi sampai dulu ke wakabareskrim atau kabareskrim baru kemudian ke direktur dari direktur baru kemudian ke unit sehingga yang diinginkan kanit pada saat itu adalah terima laporan lakukan pemeriksaan terhadap saksi atau korban pada saat itu juga sehingga itu juga merupakan wujud pemberian pelayanan kepada pelapor sehingga yang diberikan tugas pada saat itu adalah saya dan Kompol Dicky untuk membuat laporan polisi dan begitu korban datang kami langsung membuat laporan polisi dan saat itu juga kami melakukan pemeriksaan terhadap korban yang diwakili oleh divisi hukum Partai Golkar yang terlibat lainnya adalah AKBP Edi yang ditunjuk langsung oleh kanit untuk mengkoordinir penyidikan, AKBP Edy bertugas memberikan semacam supervisi bagi penyidik apa yang harus dilakukan langkah-langkah selanjutnya sudah sejauh mana penyidikan apa yang harus dilakukan berikutnya kemudian AKBP Idam dilibatkan khususnya berkaitan dengan data digital yang harus kita ambil dari server dari website Partai Golkar dan semuanya penyidik melakukan tindakan itu bertanggung jawab ke kanit walaupun secara berjenjang dilakukan misalnya laporan dilakukan kepada AKBP Edy nanti dari AKBP Edy melaporkan ke kanit." (WBIS 01 A).

Pengaruh Direktorat II tampak pada pembagian anggaran. Anggaran yang diberikan sangatlah terbatas sehingga seorang Kanit V *IT & Cybercrime* harus mempunyai kebijakan dalam mengatur permasalahan kesejahteraan anggotanya dan biaya operasional sebagaimana diungkapkan dalam *FGD* Pamen sebagai berikut:

"Kalau bicara kemampuan saya setuju kalau bicara struktur itu harus dibedakan, kenapa saya bilang beda, wajar kalau kita mengajukan anggaran itu sulit, karena kita tau itu sebagai subunit kerja, sulit, kita mengajukan ke direktorat, nah disana tergantung dari kebijakan kepala unit kerja ini, ya mungkin dipotong berapa persen dibayarkannya, mau sampe mana gitu kan, tapi kalau kita status cukup besar dengan satuan ini, kita dapat anggaran langsung, anggaran langsung ini bisa kita lihat sesuai dengan kebutuhan kita, kita bisa mempunyai dipa sendiri tapi tergantung dari dipa unit kerja yang juga bergantung dari unit satuan kerja....mungkin kalau dia Densus punya satuan unit kerja sendiri walaupun dia unit satuan kerja dari Bareskrim mungkin itu lebih baik karena harus mengajukan anggaran atau dana tersendiri." (*FGD* Pamen)

4.4.3.2 Analisis Pengaruh *External Stakeholders*

Selain *internal stakeholders* terdapat pula *external stakeholders* yaitu kelompok atau individu dalam lingkungan eksternal sebuah organisasi yang mempengaruhi aktivitas organisasi tersebut (Kasali, 1994: 63 dan Stoner, 1996: 64). Ada juga ahli yang membagi dalam lingkungan umum dan lingkungan khusus. Lingkungan umum mencakup kondisi yang mungkin mempunyai dampak terhadap organisasi namun relevansinya tidak begitu jelas. Sedangkan lingkungan khusus adalah bagian dari lingkungan yang secara langsung relevan bagi organisasi dalam mencapai tujuannya. Kapan pun, lingkungan khusus adalah bagian dari lingkungan yang menjadi perhatian manajemen karena terdiri dari konstituensi kritis yang secara positif atau negatif mempengaruhi keefektifan organisasi dan berubah sesuai dengan kondisinya (Robbins, 1996: 227). Bila dilihat dari kedua konsep tersebut terdapat kesamaan pengertian antara lingkungan khusus dengan *stakeholders*. Melihat *stakeholders mapping* dari Unit V *IT & Cybercrime, external stakeholders* terbagi menjadi dua yaitu litigasi dan nonlitigasi sebagaimana diungkapkan dalam *FGD* Pama sebagai berikut:

> *"Yang terkait APJII Asosiasi Pengelola Jasa Internet Indonesia, AKKI Asosiasi Kartu Kredit Indonesia, provider, bank, ahli IT, Microsoft, ICTAP, hacker" (FGD* Pama*)*

Pada *external stakeholders* litigasi, kerja sama antara jaksa, hakim, dan Unit V *IT & Cybercrime* sangat diperlukan untuk kelanjutan kasus ke proses persidangan. Jaksa dan hakim yang tidak mengerti akan teknologi informasi tentunya akan tergantung pada penyidik dan menjadi beban penyidik untuk membantu upaya jaksa dan hakim memahami kasus *cybercrime* sebagaimana diungkapkan dalam WBIS 02 A sebagai berikut:

> *"Seharusnya memang yang pertama kira harus kinerja sistem harus bersama polisi, jaksa baik maupun hakim harus sama-sama mereka harus satu rel satu kesepahaman tentang kasus ini karena ini memang cybercrime jarang sekali terjadi dan mereka belum pernah menangani masalah ini, itu yang pertama, yang kedua sudah tentu jaksa dan hakim pun akan meminta ini dasarnya bagaimana jadi kalau minta dasarnya harus dibuatkan payung hukum lagi tentang khusus masalah ini kejahatan*

yang berkaitan dengan cybercrime yang saya ketahui sedang diatur di DPR." (WBIS 02A)

Korban dari *cybercrime* beraneka ragam dapat berupa individu, perusahaan hingga partai politik sebagaimana diungkapkan dalam WBIS 01 A sebagai berikut:

"Kejahatan komputer kalau yang berkaitan langsung dengan komputer ya deface partai Golkar kasus defacing kemudian penipuan fraud melalui e-mail yang terjadi yang pada saat itu pelakunya ada di Jawa Timur melakukan menggunakan e-mail account seseorang dan dia menyebarkan kata-kata yang seolah-olah berasal dari pemilik account yang sebenarnya tapi digunakan juga untuk menelpon seseorang seolah-olah menjual anjing jadi semacam penipuan fraud kemudian kasus yang lain adalah pengancaman melalui e-mail yang dilakukan oleh seseorang dari suatu perusahaan pada saat itu kasusnya berkaitan dengan perusahaan dari Singapura yang ada di Indonesia berkaitan dengan pengancaman melalui e-mail." (WBIS 01 A)

Untuk melakukan penyidikan, Unit V *IT & Cybercrime* perlu bekerja sama dengan korban dan saksi untuk dapat menemukan tersangka sebagaimana diungkapkan dalam WBIS 02A sebagai berikut:

"Peranan saya pada waktu itu sebatas melakukan pemeriksaan kepada saksi...Ya....Jadi kami ada dua di cybercrime itu ada tim penyidik dan tim laboratorium nah kami bekerja sesuai data yang dimiliki oleh laboratorium kami tidak tahu laboratorium bekerja bagaimana tapi menyerahkan ke kita ini datanya yang untuk dibuktikan kemudian tidak berangkat ke Batam di sana kita menemui PT Inforsis kemudian melakukan pemeriksaan memeriksakan data yang kami miliki log file nya segala macam kemudian orang itu kami periksa kami tanyakan IP yang ada berdasarkan yang kami punya data ini dimiliki oleh siapa itu sebatas kami periksa di situ kemudian dia menunjukkan ini adalah milik suatu warnet dan IP ini sebetulnya sudah tidak digunakan kemudian kami melakukan penyidikan disitu." (WBIS 02A)

Korban dari *cybercrime* beraneka ragam dapat berupa individu, perusahaan hingga partai politik sebagaimana diungkapkan dalam WBIS 01 A sebagai berikut:

"Kejahatan komputer kalau yang berkaitan langsung dengan komputer ya deface partai Golkar kasus defacing kemudian penipuan fraud melalui e-mail yang terjadi yang pada saat itu pelakunya ada di Jawa Timur melakukan menggunakan e-mail account seseorang dan dia menyebarkan kata-kata yang seolah-olah berasal dari pemilik account yang sebenarnya tapi digunakan juga untuk menelpon seseorang seolah-olah menjual anjing jadi semacam penipuan fraud kemudian kasus yang lain adalah pengancaman melalui e-mail yang dilakukan oleh seseorang dari suatu perusahaan pada saat itu kasusnya berkaitan dengan perusahaan dari Singapura yang ada di Indonesia berkaitan dengan pengancaman melalui e-mail." (WBIS 01 A)

Untuk melakukan penyidikan, Unit V *IT & Cybercrime* perlu bekerja sama dengan korban dan saksi untuk dapat menemukan tersangka. *External stakeholder* yang tidak berhubungan langsung dengan proses penegakan hukum dapat termasuk DPR, APJII, Perusahaan telekomunikasi, Bank Indonesia, media massa, sampai dengan organisasi internasional ataupun lembaga pemerintahan asing seperti: FBI, AFP dan Council of Europe. Untuk meningkatkan kinerja dan mencapai sasaran Unit V *IT & Cybercrime*, diperlukan adanya pembinaan sumber daya manusia di dalam dan di luar negeri, peningkatan peralatan teknologi, serta pendanaan untuk menutupi biaya operasional maupun terpenuhinya kesejahteraan para anggota.

BAB V
PENUTUP

5.1 Kesimpulan

Disertasi ini menghasilkan definisi ***hacking*** yaitu setiap kegiatan menggunakan komputer atau sistem elektronik lainnya yang dilakukan dengan cara mengakses suatu sistem jaringan komputer baik yang terhubung dengan internet atau tidak, baik dengan tujuan maupun tidak, untuk memperoleh, mengubah dengan cara menambah atau mengurangi, menghilangkan atau merusak informasi dalam sistem komputer dan atau sistem elektronik lainnya dengan melawan hukum. Dari pengertian *hacking* di atas, ***hacking*** dikategorikan sebagai kejahatan komputer tanpa kekerasan (*cybercrime without violence*) dan termasuk dari kejahatan komputer yang merusak (*destructive cybercrime).* Tindakan yang digolongkan sebagai *hacking* seperti kegiatan yang mengganggu jaringan pelayanan, dimana data-data tersebut diganti, dirubah, dan dirusak. Kegiatan yang tergolong *hacking* lainnya adalah mengakses secara ilegal ke dalam jaringan komputer kemudian menghapus data atau program *file*, mengakses secara illegal ke dalam suatu *website* dan melakukan perusakan atau perubahan wajah pada halaman *website (deface*).

Disertasi ini juga berhasil mengidentifikasikan ***karakteristik tindak pidana hacking*** dibandingkan dengan tindak pidana konvensional. Tindak pidana *hacking* dilakukan dengan menggunakan teknologi informasi, dapat dilakukan dari berbagai tempat yang terpisah dan tidak mengenal batas wilayah (*borderless*) dan lintas batas negara (transnasional). Tindak pidana *hacking* tidak meninggalkan jejak berupa catatan atau dokumen fisik dalam bentuk kertas (*paperless*) akan tetapi semua jejak hanya tersimpan dalam komputer dan jaringannya tersebut dalam bentuk data atau informasi digital (*log files*). Korban tindak pidana dapat menimpa siapa saja mulai dari perseorangan, perusahaan, organisasi non pemerintahan sampai negara. Karena *hacking* bersifat tanpa kekerasan (*non violence*) dan karena *cybercrime* tidak kasat mata maka *fear of*

crime (ketakutan terhadap kejahatan) tidak mudah timbul walaupun akibat yang muncul melebihi tindak pidana konvensional.

Disertasi ini juga menemukan adanya **pengaturan yang berbeda dari tindak pidana *hacking* dan tersebar di dalam dan di luar KUHP serta perlunya interpretasi penyidik secara ektensif** untuk dapat memenuhi ketentuan materil dan formil yang relevan dengan tindak pidana *hacking*. Dengan adanya UU ITE, undang-undang tersebut dapat dijadikan dasar hukum bagi aparat penegak hukum dalam penanganan kasus tindak pidana *hacking* yang akan datang. Pengaturan tindak pidana *hacking* juga terdapat dalam RUU, yaitu RUU KUHP dan RUU TPTI. Unsur-unsur dan sanksi pidana untuk tindak pidana *hacking* diatur berbeda dalam ketentuan yang tersebar tersebut sehingga tidak terdapat konsistensi.

Dari disertasi ini, terdapat karakteristik penyidikan *hacking* yang berbeda dengan penyidikan tindak pidana konvensional. Perbedaan tersebut dipicu oleh karakteristik tindak pidana *hacking* itu sendiri yang khas, sehingga penyidikannya harus dilakukan berbeda dengan penyidikan tindak pidana konvensional. Pertama, sebagian proses penyidikan dilakukan di *cyberspace*, dimana untuk menemukan pelaku *hacking* (*hacker*) tidak cukup dengan melakukan penyidikan seperti biasa, dalam artian fisik dalam dunia nyata. Penyidik dalam melakukan penyidikan perlu menjelajah dunia *cyber* bahkan melakukan penyamaran di internet (*virtual undercover)* untuk menemukan *hacker* yang pada umumnya aktif menggunakan internet (*netter*) dan merupakan bagian dari komunitas virtual (*virtual community*). Kedua, adanya eksistensi bukti digital (*digital evidence*) dalam proses penyidikan tindak pidana *hacking*, yaitu *log files* yang dapat memberikan informasi berupa catatan atas perintah-perintah atau pesan-pesan kepada *server* korban yang dilancarkan atau dilakukan oleh *hacker*. Pada *log files* terdapat pula informasi mengenai dari mana dan oleh siapa serangan-serangan atau penyusupan dilakukan yaitu identitas yang ditinggalkan seseorang berupa *IP Address*. Ketiga, penanganan komputer sebagai TKP (*crime scene*) dimana dalam proses penyidikan menggunakan alat-alat (*tools*) untuk menangani bukti digital baik di lapangan maupun analisa di laboratorium forensik komputer. Peranan laboratorium forensik komputer sangat penting dalam

keberhasilan penyidikan. Dengan perangkat keras dan lunak yang ada, bukti-bukti digital tersebut dapat diurai sehingga dapat membantu penyidik mencari bukti-bukti untuk memenuhi unsur-unsur dari tindak pidana *hacking*. Hasil analisis komputer forensik tertuang dalam berita acara pemeriksaan laboratorium forensik komputer. Keempat, masalah yurisdiksi hukum dimana ada permasalahan mengenai negara yang berhak mengadili pelaku tindak pidana *hacking* apabila *hacker* melakukan serangan di negara lain.

Sebagai hasil perbandingan dengan Hong Kong, Amerika Serikat maupun Council of Europe, dalam disertasi ini dinyatakan, **diperlukannya aturan khusus** mengenai *hacking/cybercrime*, **berikut unit/direktorat** yang khusus didedikasikan untuk melakukan penyidikan dimana unit/direktorat tersebut dilengkapi dengan **laboratorium forensik komputer.**

Disertasi ini menghasilkan teori manajemen penyidikan tindak pidana *hacking* yang merupakan serangkaian tindakan penyidik dalam melaksanakan penyidikan tindak pidana *hacking* dengan menerapkan prinsip-prinsip dan fungsi manajemen yang terdiri dari penerimaan input (*input accepting*), penugasan (*assigning*), perencanaan penyidikan (*planning*), pelaksanaan dan penyesuaian penyidikan (*executing and adjusting investigation*), serta pengendalian dan evaluasi penyidikan *(controlling and evaluation of investigation)*, penyerahan hasil penyidikan (*result delivery*), bantuan di pengadilan (*court support*) dan dokumentasi hukum *(legal documentation)*. Kegiatan penyidik pada manajemen penyidikan tindak pidana *hacking* ini tidak berhenti pada penyerahan berkas perkara ke jaksa penuntut umum tetapi berlanjut membantu jaksa penuntut umum dalam proses persidangan dan menganalisis hasil keputusan hakim sebagai bahan telaah hukum untuk penyidikan yang lain. Manajemen penyidikan tindak pidana *hacking* dapat diterapkan pada proses penyidikan *cybercrime* lainnya dengan penggunaan bukti digital dan peranan laboratorium forensik komputer.

Disertasi ini telah berhasil mengidentifikasikan **faktor-faktor yang mempengaruhi penerapan dari manajemen penyidikan** serta hubungan antara faktor-faktor tersebut yaitu budaya organisasi, kepemimpinan dan *stakeholders*. **Kepemimpinan** memegang peranan yang sangat dominan sebagai motor penggerak atau generator yang dapat mempengaruhi kedua faktor lainnya yaitu

budaya organisasi dan *stakeholders*. Dengan gaya kepemimpinan yang dipilih, seorang pemimpin dapat membentuk budaya organisasi yang sesuai dengan nilai-nilai yang dianut dan dianggap berpengaruh positif bagi kinerja unitnya. Selain itu tekanan teman sejawat *(peer group pressure)* turut berperan dalam mendorong anggota berperilaku yang selaras dengan budaya organisasi. Untuk memotivasi anggota, pemimpin perlu memberikan contoh serta penghargaan kepada anggota. Penghargaan tersebut dapat berupa insentif, kesempatan mengembangkan pengetahuan dan pengalaman, didengar pendapatnya serta diberikan tanggung jawab yang lebih tinggi. Semua hal tersebut merupakan motivasi ekstrinsik bagi para anggota untuk bekerja lebih baik lagi.

Salah satu bentuk dari sub budaya organisasi yang berbeda dengan budaya semi militer adalah kegiatan *sharing*. Dalam kegiatan *sharing* tersebut terjadi diskusi pro dan kontra mengenai suatu issu dimana anggota yunior bisa saja berbeda atau bahkan berlawanan pendapat dengan anggota senior. Disini benar atau salah, ditentukan oleh kemampuan berargumentasi dan penggunaan nalar bukan atas dasar hirarki atau senioritas. Tidak sepaham dengan argumen senior bukan berarti tidak patuh. Hal seperti ini berlawanan dengan dogma polisi: loyalitas, respek, dan hirarki. Sehingga yang terjadi dalam proses *sharing* adalah anti-struktur dimana struktur dan jenjang kepangkatan selama kegiatan *sharing* menjadi tidak berlaku secara mutlak.

Pemimpin sangat berperan aktif dalam menjalin hubungan dengan *stakeholders*. Dengan memperluas dan mengintensifkan jaringan dengan *stakeholders*, pemimpin dapat mengajak *stakeholders* untuk turut membangun infrastruktur dan pemberdayaan manusia. Pembangunan infrastruktur dan adanya peluang pemberdayaan manusia pada akhirnya menumbuhkan motivasi intrinsik para anggota untuk mempunyai kinerja yang lebih baik.

5.2. Kontribusi

Sejalan dengan tujuan penelitian, disertasi ini diharapkan juga dapat menghasilkan kegunaan baik secara teoritis maupun praktek.

5.2.1 Kontribusi Disertasi dalam Pengembangan Ilmu Pengetahuan

Untuk pengembangan ilmu pengetahuan disertasi ini telah memberikan pengertian *hacking*, berikut karakteristik *hacking* sebagai suatu tindak pidana yang berbeda dengan tindak pidana konvensional. Lebih jauh lagi, disertasi ini telah memberikan teori manajemen penyidikan terpadu yang dapat digunakan dalam penyidikan kasus tindak pidana *hacking* serta mengidentifikasikan karakteristik dari penyidikan tindak pidana *hacking* yang berbeda dengan penyidikan tindak pidana konvensional. Disertasi ini telah menemukan faktor-faktor yang mempengaruhi pelaksanaan manajemen penyidikan berikut hubungan diantara faktor-faktor tersebut.

5.2.2 Kontribusi Disertasi dalam Praktek

Selain kegunaan teoritis, disertasi ini juga memberikan kontribusi dalam praktek berupa pasal-pasal yang dapat digunakan untuk tindak pidana *hacking* dan pengacuan pasal yang dapat diinterpretasikan untuk memenuhi unsur tindak pidana *hacking* baik dalam KUHP, UU Telekomunikasi, UU ITE, RUU TPTI dan RUU KUHP. Dengan diberlakukannya UU ITE baru-baru ini, tindak pidana tindak pidana *hacking* dapat dikenakan ketentuan yang lebih khusus lagi (*lex specialist derogate lex generalis*) yaitu Pasal 30 UU ITE. Pengaturan bukti digital dalam penyidikan telah dipaparkan dalam disertasi ini, baik pengaturan dalam UU seperti UU Pencucian Uang dan lain-lain, serta dalam bentuk RUU seperti RUU TPTI dan RUU KUHAP. Dengan pembahasan yang mendalam mengenai aturan hukum baik materil maupun formil yang berkaitan dengan tindak pidana *hacking* dan bukti digital, disertasi ini memberikan informasi yang komprehensif kepada para pihak yang berkaitan dengan proses penegakan hukum kasus tindak pidana *hacking* seperti: polisi, jaksa penuntut umum, pembela dan hakim bahkan ahli, korban dan pelaku.

Disertasi ini telah menyediakan petunjuk penanganan bukti *digital* serta persyaratan khusus atau kualifikasi penyidik yang menangani tindak pidana *hacking* atau kejahatan berbasis teknologi informasi lainnya. Bukti digital tersebut akan diserahkan ke laboratorium forensik komputer untuk dianalisis

dengan *software* dan *hardware* tertentu. Dengan adanya panduan tersebut, penyidik yang tidak mempunyai latar belakang *IT* dapat mengamankan dan menangani bukti digital untuk diproses lebih lanjut di laboratorium forensik komputer sehingga tidak perlu menunggu penyidik berpengalaman dari Bareskrim Polri harus datang ke tempat ditemukannya bukti digital tersebut.

Disertasi ini juga telah memberikan penjabaran mengenai manajemen penyidikan terpadu sehingga penyidik lebih memahami proses penyidikan dan dapat melakukan penyidikan secara lebih sistematis dan profesional dengan penerapan prinsip-prinsip dan fungsi manajemen. Manajemen penyidikan terpadu tersebut apabila diterapkan akan melibatkan jaksa penuntut umum dan hakim sebagai bagian dari *criminal justice system*. Karena manajemen penyidikan terpadu tidak berhenti pada penyerahan berkas perkara ke jaksa penuntut umum tetapi juga berlanjut dengan pengawasan dan evaluasi pada proses persidangan sampai adanya keputusan. Jaksa penuntut umum akan dibantu oleh penyidik dalam proses persidangan. Sedangkan keputusan hakim mengenai kasus tersebut akan ditelaah dan didokumentasikan oleh penyidik sebagai referensi hukum bagi penanganan kasus yang akan datang. Hal ini sejalan dengan *criminal justice system* yang menciptakan sinergi dengan aparat penegak hukum lainnya. Dengan penerapan manajemen penyidikan terpadu ini berdampak pada peningkatan kemampuan penyidik yang menjadi terasah dalam menangani suatu kasus.

Dilihat dari metode penelitian yang dilakukan, disertasi ini telah menguak metode penelitian kualitatif dalam bentuk diskusi kelompok terfokus (*focus group discussion*) sebagai acuan pengumpulan data primer bagi penelitian ilmu kepolisian. Diskusi kelompok terfokus ini dapat menggambarkan dengan rinci persepsi dan ungkapan pendapat para anggota mengenai unitnya, sehingga sangat tepat digunakan sebagai wadah intropeksi diri atau evaluasi organisasi dan cara mendapatkan data yang komprehensif untuk mengetahui faktor-faktor yang mempengaruhi penerapan manajemen penyidikan atau pun kinerja organisasi. Kontribusi praktis tersebut di atas merupakan sumbangsih disertasi ini bagi kepolisian.

5.3 Diskusi Lebih Lanjut

5.3.1 Konsistensi Pengaturan *Hacking* dan Bukti Digital di Indonesia

Dalam melakukan penegakan hukum terhadap kasus tindak pidana *hacking*, perlu diteliti lebih lanjut akibat dari ketidak-konsistenan dari unsur-unsur tindak pidana *hacking* itu sendiri. Dengan berbagai peraturan baik yang sudah berlaku maupun yang masih dalam tahap pembahasan, telah diatur berbagai perbuatan pidana yang dapat dikategorikan dengan tindak pidana *hacking* beserta variasinya. Tentu diperlukan kesamaan pandangan dalam hal mengkategorikan suatu perbuatan sebagai tindak pidana *hacking* agar aturan pidana tentang tindak pidana *hacking* tidak saling tumpang tindih atau bertentangan. Apabila hal tersebut terjadi, akan menyulitkan penyidik dalam menangani kasus tindak pidana *hacking* dan menciptakan ketidakpastian hukum. Bukannya tidak mungkin karena kelemahan tersebut, *hacker* dapat lolos dari jeratan hukum. Untuk itu sangat diperlukan kesamaan pandangan dari para pembuat undang-undang guna memberikan konsep yang jelas dan menyeluruh tentang unsur-unsur perbuatan apa saja yang disebut dengan tindak pidana *hacking*.

Selain itu, dalam hal sanksi pidana yang dapat dikenakan terhadap *hacker* juga perlu penelitian lebih lanjut. Pasal 50 UU Telekomunikasi menyatakan bahwa "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak enam ratus juta rupiah". Kemudian dalam RUU KUHP, tindak pidana *hacking* diatur dalam Pasal 373 RUU KUHP dengan pidana penjara paling lama 4 (empat) tahun atau berdasarkan Pasal 80 RUU KUHP pidana denda paling banyak kategori IV yaitu tujuh puluh lima juta rupiah. Sedangkan dalam Pasal 11 RUU TPTI dipidana penjara paling singkat 2 (dua) tahun dan paling lama 4 (empat) tahun atau denda sedikit-dikitnya dua ratus juta rupiah dan sebanyak-banyaknya delapan ratus juta rupiah. Perbedaan juga terjadi pada UU ITE Pasal 46 (3), pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak delapan ratus juta rupiah. Masing-masing aturan ini berbeda dari segi lamanya sanksi penjara dan besarnya denda sehingga dapat merobek rasa keadilan, dimana perbuatan hukum yang sama dapat dikenakan pasal dan ganjaran

yang berbeda-beda.

Oleh karena itu, pembuat undang-undang sebaiknya membuat ketentuan yang jelas dalam hal menentukan besar kecilnya pidana, baik penjara maupun denda, yang akan dijatuhkan kepada *hacker*. Misalnya dengan mempertimbangkan kerugian-kerugian yang dapat ditimbulkan oleh tindak pidana *hacking* itu sendiri. Jangan sampai di kemudian hari ketentuan yang mengatur perbuatan tindak pidana *hacking* saling bertentangan satu sama lain padahal yang diharapkan adalah masing-masing aturan saling melengkapi satu sama lain sehingga penegakan hukum dapat berjalan sesuai dengan harapan. Sebagai solusinya adalah lebih baik lagi apabila peraturan yang serba *lex specialist* tersebut dikodifikasikan ke dalam suatu KUHP mengingat sampai sekarang masih dalam bentuk RUU KUHP.

Pengaturan bukti digital selama ini hanya terdapat pada UU ITE, UU Pencucian Uang, UU Pemberantasan Tindak Pidana Terorisme, UU Pemberantasan Tindak Pidana Korupsi dan UU Pemberantasan Tindak Pidana Perdagangan Orang. Sedangkan dalam bentuk rancangan undang-undang, bukti digital hanya terdapat pada RUU KUHAP. Sebagaimana ketentuan materil mengenai tindak pidana *hacking*, ketentuan formil mengenai bukti digital juga tersebar dalam berbagai undang-undang dan RUU. Untuk mencegah pengaturan yang tumpang tindih bahkan saling bertentangan, di masa yang akan datang diperlukan suatu pengabungan aturan formil dalam bentuk KUHAP mengingat sampai sekarang, masih dalam bentuk RUU KUHAP.

5.3.2 Kaderisasi Kepemimpinan dan Restrukturisasi Unit V *IT & Cybercrime*

Bila ditelaah dari analisis disertasi ini, dinyatakan bahwa pemimpin mempunyai peranan yang sangat besar sebagai motor penggerak unit. Hal ini dapat berimplikasi buruk dengan adanya ketergantungan suatu unit dengan figur pemimpin. Apabila terjadi pergantian pemimpin dan figur pemimpin yang menggantikan tidak sesuai dengan harapan para anggota, maka dapat mengakibatkan penurunan kinerja unit tersebut. Apalagi bila para anggota unit telah menetapkan standar yang tinggi terhadap kriteria pemimpin.

Permasalahan ini membuka penelitian lebih lanjut mengenai persiapan sumber daya manusia dan kaderisasi pada tingkatan unit: bagaimana caranya agar pengelolaan sumber daya manusia dapat memenuhi kebutuhan tenaga kerja sebagai pemimpin yang memiliki pengetahuan, pengalaman dan kemampuan yang spesifik tersebut. Salah satu usaha yang dapat ditempuh adalah kaderisasi pemimpin. Bagian sumber daya manusia harus menciptakan suatu mekanisme transfer ilmu dan pengetahuan antara pemimpin yang saat ini menjabat dengan beberapa kandidat pemimpin. Salah satu caranya adalah menggunakan sistem *mentoring* ataupun *coaching*. Pemimpin memberikan pengarahan langsung serta meluangkan waktu dan tenaga untuk pemberdayaan para kandidat. Dengan adanya *mentoring/coaching* tersebut, konsentrasi pemimpin dalam mempersiapkan dan mentransfer ilmu pengetahuan dan pengalaman diharapkan dapat berjalan dengan lancar.

Restrukturisasi unit yang menangani kejahatan *IT & Cybercrime* juga dapat menjadi bahan penelitian lebih lanjut mengingat ke depan, peranan *IT* semakin penting dan potensi bahaya *cybercrime* semakin nyata. Lagipula untuk menegakan hukum dan memberantas *cybercrime*, diperlukan jaringan internasional yang kuat mengingat *cybercrime* dapat terjadi lintas negara. Adanya restrukturisasi tersebut dapat berupa penambahan personil dan kewenangan yang menyangkut pendanaan dan kerja sama internasional sehingga unit tersebut lebih gesit dalam mencari peluang guna meningkatkan infrastruktur dan sumber daya manusia baik sebagai penyidik *cybercrime* dan ahli forensik komputer. Hal ini sejalan dengan hasil perbandingan penanganan *cybercrime* di luar negeri seperti Hong Kong, Amerika Serikat maupun Council of Europe, dimana terdapat departemen/direktorat yang khusus didedikasikan untuk melakukan penyidikan dalam tubuh organisasi polisi. Bentuk sub organisasi tersebut lebih besar dibandingkan bentuk unit seperti di Bareskrim Polri untuk menjembatani beban tanggung jawab yang semakin berat dalam melakukan penegakan hukum, apa lagi bagian tersebut juga bertanggung jawab memanajemen laboratorium forensik komputer.

5.4. Keterbatasan Teori dan Studi

Penulis menyadari bahwa disertasi ini memiliki kelemahan dan tidak terlepas dari keterbatasan walaupun penelitian sudah dilakukan sesuai standar dan prosedur penelitian kualitatif yang baku. Keterbatasan tersebut terjadi karena pembentukan teori yang ada hanya diambil dari satu studi kasus yang terjadi di satu unit saja, yaitu: Unit V *IT & Cybercrime*. Hal ini memungkinkan adanya perbedaan penerapan apabila manajemen penyidikan diterapkan pada penyidikan kasus lainnya di luar *hacking/cybercrime*. Sebagai suatu unit, Unit V *IT & Cybercrime* tersebut juga relatif baru dibentuk sehingga memudahkan tranformasi nilai diantara anggota Unit V *IT & Cybercrime* karena nilai-nilai yang ada pada saat transformasi belum mengakar. Selain itu secara infrastruktur, Unit V *IT & Cybercrime* masih membutuhkan dukungan teknologi yang lebih lengkap dan canggih dibandingkan unit lainnya yang menangani tindak pidana konvensional berikut dukungan peningkatan sumber daya manusia. Hal ini membuka kemungkinan adanya perbedaan faktor-faktor yang mempengaruhi manajemen penyidikan apabila diterapkan pada unit lainnya. Pada saat penyidikan dan penelitian dilakukan terhadap kasus tersebut, UU ITE baru berupa rancangan undang-undang, sedangkan pada saat disertasi ini selesai RUU ITE telah dicanangkan menjadi undang-undang. Namum di balik keterbatasan teori dalam disertasi ini, penulis telah berupaya mengembangkan keberadaan kajian ilmu kepolisian sebagai suatu interdisiplin ilmu.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Indonesia. *Undang-undang Dasar 1945*.

_____. *Undang-undang Tentang Hukum Acara Pidana*. UU No. 8 Tahun 1981, LN No. 75, TLN No. 3209.

_____. *Undang-undang Tentang Dokumen Perusahaan*. UU No. 8 Tahun 1997, LN No. 18, TLN No. 3674.

_____. *Undang-undang Tentang Telekomunikasi*. UU No. 36 Tahun 1999, LN No. 154, TLN No. 3881.

_____. *Undang-undang Tentang Hak Asasi Manusia*. UU No. 39 Tahun 1999, LN No. 165, TLN No. 3886.

_____. *Undang-undang Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi*. UU No. 20 Tahun 2001, LN No. 134, TLN No. 4150.

_____. *Undang-undang Tentang Kepolisian Negara Republik Indonesia*. UU No. 2 Tahun 2002, LN No. 2, TLN No. 4168.

_____.*Undang-undang Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme*, UU No. 15 Tahun 2003, LN No. 45, TLN No. 4284.

_____.*Undang-undang Tentang Perubahan atas Undang-undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang*. UU No. 25 Tahun 2003, LN No. 108, TLN No. 4324.

_____.*Undang-undang Tentang Komisi Pemberantasan Tindak Pidana Korupsi*. UU No. 30 Tahun 2002, LN No. 137, TLN No. 4250.

_____.*Undang-undang Tentang Pemberantasan Tindak Pidana Perdagangan Orang*, UU No. 21 Tahun 2007, LN No. 58, TLN No. 4720.

_____.*Undang-undang Tentang Informasi dan Transaksi Elektronik*, UU No. 11 Tahun 2008, LN No. 58, TLN No. 4843.

_____. *Keputusan Presiden Republik Indonesia Tentang Organisasi dan Tata Kerja Kepolisian Negara Republik Indonesia,* Kepres No. 70 Tahun 2002.

_____. *Keputusan Kepala Kepolisian Negara Republik Indonesia No. Pol.:Kep/54/X2002, tanggal 17 Oktober 2002 Tentang Organisasi dan Tata Kerja Satuan-Satuan Organisasi Pada Tingkat Kepolisian Negara Republik Indonesia.*

_____. *Rancangan Undang-undang Republik Indonesia Nomor [...] Tahun [...] Tentang Kitab Undang-undang Hukum Pidana.*

_____. *Rancangan Undang-undang Republik Indonesia Nomor [...] Tahun [...] Tentang Kitab Undang-undang Hukum Acara Pidana.*

_____. *Rancangan Undang-undang Republik Indonesia Nomor [...] Tahun [...] Tentang Tindak Pidana Di Bidang Teknologi Informasi.*

Kitab Undang-undang Hukum Pidana (Wetboek van Strafrecht). (2001). Diterjemahkan oleh Moeljatno. Cet. 21. Jakarta: Bumi Aksara.

Himpunan Bujuklak, Bujuklap dan Bujukmin Proses Penyidikan Tindak Pidana. (2001). Jakarta: Markas Besar Kepolisian Negara Republik Indonesia.

Buku

Adair, John. (1995). *Bukan Bos Tetapi Pemimpin.* Jakarta: Gramedia Pustaka Utama.

Arief, Barda Nawawi. (2006). *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia.* Jakarta: PT Grafindo Persada.

Ariyus, Dony. (2005). *Kamus Hacker.* Yogyakarta: Andi Publisher.

Axelrod, Alan dan Guy Antinozzi. (2001). *Criminal Investigation.* United States of America: Pearson Education Company.

Badan Reserse Kriminal (Bareskrim). (2007) *Draft Manajemen Penyidikan Tindak Pidana.* Jakarta: Markas Besar Kepolisian Negara Republik Indonesia.

Barua, Yogesh dan Denzyl P. Dayal., (2001). *Cyber Crimes Notoriious Aspects of The Humans and The Net.* New Delhi: Dominant Publishers and

Distributors.

Bouza, Anthony V. (2005). *Inspection* (*Inspeksi*), Ensiklopedia Ilmu Kepolisian, editor William G. Bailey. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

Brown, Christopher L.T. (2006). *Computer Evidence Collection & Preservation.* Massachusetts: Charles River Media Inc.

Burdett, *et al*. (1995). *A Glossary of Computing Terms*. Eight Edition, Singapore: Longman.

Butler, A. J. P. (1992). *Police Management*. United States of America: Dartmouth Publishing Company Limited.

Casey, Eoghan. (2000). *Digital Evidence Forensic Computer and The Internet Computer Crime*. London: Academic Press.

Casey, Eoghan dan Seglem (2002). *Handbook of Computer Crime Investigation (Forensic Tools and Technology)*. United States of America: Academic Press.

Clifford, Ralph D. (2006). *The Investigation, Prosecution and Defense of A Computer–related Crime*. Cet.II. Durham, North Carolina: Carolina Academic Press.

Cordner, Gary W. (2005). *Administration (Administrasi)*. Ensiklopedia Ilmu Kepolisian, editor William G. Bailey. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

Dantzker, M. L. (1999). *Police Organization and Management*. United States of America: Butterworth Heinemann.

Djamin, Awaloedin. (1995). *Administrasi Kepolisian*. Jakarta: CV Mandira Buana.

_____, Awaloedin. (2001). *Agenda Reformasi Polri*. Jakarta: PTIK Press.

Doswell, R. dan G. L. Simons. (1986). *Fraud and Abuse of IT System*. England: The National Computing Center Limited.

Ember, Carol R. dan Ember, Melvin. (1984). *Konsep kebudayaan*. Editor. T. Ihromi. . Jakarta: PT Gramedia.

Furnell, Steven. (2002). *Cybercrime Vandalizing The Information Society*. United States of America: Pearson Education Limited.

Furnham, A. (1997). *Psychology of Behaviour at Work*. United Kigdoms: Biddles Ltd and King's Lynn.

Grabosky, P. N., dan Russel G. Smith. (1998). *Crime In The Digital Age: Controling Telecomunications Illegalities*. Australia: The Federation Press.

Gunawan, Budi. (2006). *Membangun Kompetensi Polri*. Cet.I. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

Hamzah, Andi. (1986). Kamus Hukum. Jakarat: Ghalia Jakarta.

_____. (1996). *Hukum Pidana Ekonomi*. Cet.VI. Jakarta: Erlangga.

Hamzah, Andi., dan Marsita Boedi D. (1990). *Aspek-aspek Pidana di Bidang Komputer*. Cet.II. Jakarta: Sinar Grafika.

Harahap, M. Yahya. (2006). *Pembahasan Permasalahan dan Penerapan KUHAP (Penyidikan dan Penuntutan)*. Cet.VIII. Jakarta: Sinar Grafika.

Hartono, Jogiyanto. (2000). *Pengenalan Komputer Dasar Ilmu Komputer, Pemrograman, Sistem Informasi dan Intelegensi Buatan*. Edisi ketiga, Cet.III. Yogyakarta: Andi.

Hosaya, Ryuhei. (1997). *Cyberspace and Virtual Diplomacy: The End of The Nation-State?*. IIPS Policy Paper 1880J/E.

Kanter, E.Y dan S.R. Sianturi. (1982) *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*. Jakarta: Alumni AHM-PTHM.

Kartasudirja, Eddy Djunaedi. (1999). *Bahaya Kejahatan Komputer* Jakarta: Tanjung Agung.

Kasali, Rhenald. (1994). *Manajemen Public Relations*. Jakarta: Temprint.

Kepolisian Negara Republik Indonesia. (2002). *Kebijakan dan Strategi Kapolri Tahun 2002-2004*. Jakarta: Polri.

Kepolisian Negara Republik Indonesia. (2005). *Revisi Rencana Kerja Bareskrim Polri (Renja Bareskrim Polri)*. Jakarta: Polri.

Kepolisian Negara Republik Indonesia. (2006). *Rencana Kerja Bareskrim Polri (Renja Bareskrim Polri*. Jakarta: Polri.

Kepolisian R.I. Staff Deputi perencanaan Umum dan Pengembangan. (2007). Perkembangan Organisasi Polri (Perubahan Organisasi Polri ke Arah Organisasi Berbasis Kinerja). Jakarta: Biro Ortala.

Koentjaraningrat. (2002). *Pengantar Ilmu Antropologi*, Cet. 8. Jakarta: PT Rineka Cipta.

Kotter, John. P. (1997). *The Leadership*. Terj. Hari Suminto. Jakarta: Prenhallindo.

Krueger, Richard A. & Mary Anne Casey. (2000), *Focus Group 3rd Edition,* KOTA: *Sage publications.*

Leavitt, Harold. J. (1992). *Managerial Psychology*. Terj. Muslichah Zarkasi. Jakarta: Erlangga.F

Makarim, Edmon. (2005). *Pengantar Hukum Telematika Suatu Kajian Kompilasi.* Jakarta: PT. Raja Grafindo Persada.

Matindas, R. (1997). *Manajemen SDM Lewat Konsep A.K.U.* Jakarta: PT. Pustaka Utama Grafiti.

Manning, Peter K. (2005). *Budaya Pekerjaan (Occupational Culture).* Ensiklopedia Ilmu Kepolisian, editor William G. Bailey. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

McShane, Steven L., dan Mary Ann Von Glinow. (2003). *Organizational Behavior*. United States of America: International Edition.

Miller, Daniel dan Don Slater. (2003). *The Internet*. United States of America: :. Berg.

Munir, Abu Bakar. (1999). *Cyber Law Policies and Challenges*. Kuala Lumpur: Butterworths Asia.

Patilima, Hamid. (2005) *Metode Penelitian Kualitatif,* Cet.I Bandung: Alfabeta.

Patton, Michael Quinn. (2002). *Qualitative Research & Evaluation Methods*. Third Edition. Sage Publications, Inc.

Prasetya, Joko Tri. (1998). *Ilmu Budaya Dasar*. Jakarta: Rineka Cipta.

Prinst, Darwan. (1998). *Hukum Acara Pidana dalam Praktik.* Cet.II. Jakarta: Djambatan.

Projodikoro, Wirjono. (1985). *Hukum Acara Pidana Indonesia.* Bandung: Sumur.

Qadir, C.A. (1995). *Ilmu Pengetahuan dan Metodenya*. Jakarta: Yayasan Obor Indonesia.

Ramli, Ahmad M., Pager Gunung dan Indra Apriadi. (2007). *Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik.* Jakarta:

Departemen Komunikasi dan Informatika Republik Indonesia.

Reed, Chris. (2004). *Internet Law*. United Kingdom: Cambridge University Press.

Reksodiputro, Mardjono. (1997). *Kemajuan Pembangunan Ekonomi dan Kejahatan*. Jakarta: Pusat Pelayanan dan Pengabdian Hukum Universitas Indonesia.

Riberu, J. (1987). *Dasar-dasar Kepemimpinan*. Jakarta: CV Pedoman Ilmu Jaya.

Robbins, Stephen P., dan Mary Coultar. (1996). *Management*. Cet.VI. United States of America: Prentice Hall, Inc.

_____, Stephen P. (1996). *Managing Today*. San Diego State University: Prentice Hall Inc.

Roberg, Roy R., dan Jack Kuykendal. (1997). *Police Management*. Los Angeles: Roxbury Publishing Company.

Schmidt, Howard A. (2006). *Patrolling Cyberspace: Lessons Learned From A Lifetime In Data Security*. United States of America: Larstan Publishing, Inc.

Shinder, Debra Littlejohn. (2002). *Scence of the Cybercrime*. United States of America: Syngress Publishing.

Sitompul, Asril. (2001). *Hukum Internet Pengenalan Mengenai Masalah Hukum di Cyberspace*. Cet.I. Bandung: PT. Citra Aditya Bakti.

Smith. (1991). *Motivation in Organization*. United States of America: Prentice Hall Inc.

Stoner, James A. F., R., Edward Freeman, Daniel R. Gilbert JR. (1992). *Manajemen*. Jilid 1. Jakarta: PT. Prentice-Hall Inc.

Stoner, James A. F., R., Edward Freeman, Daniel R. Gilbert JR. (1996). *Manajemen Jilid 1*. Jakarta: PT. Prentice-Hall Inc.

Sullivan, John L. (1992). *Pengantar Ilmu Kepolisian*. Jakarta: Pusat Pengembangan Ilmu dan Teknologi Kepolisian Perguruan Tinggi Ilmu Kepolisian.

Sunindhia, Y. W., dan Ninik Widiyanti. (1993). *Kepemimpinan dalam Masyarakat Modern*. Jakarta: Rineka Cipta.

Swanson, Charles R., Leonard Territo, dan Robert W. Taylor. (2008) *Police Administration Structures, Processes, and Behavior*, Seventh Edition,

(New Jersey: Pearson Education, Inc.

Thibault, Edward A., Lawrence M. Lynch dan R. Bruce McBride. (2007). *Proactive Police Management*. New Jersey: Pearson Education Inc.

Thomas. dan Brian D Loader. (2000). *Cybercrime Law Enforcement: Security and Surveillance in The Information Age*. London: Routledge.

Utrecht, E. (1997). *Rangkaian Sari Kuliah Hukum Pidana II*. Surabaya: Pustaka Tinta Mas.

W.A., Soeherto. (2002). *Administrasi Penyidikan*. Megamendung. Bogor: Pusat Pendidikan Reserse dan Intel.

Ward, Richard H. (2005). *Case Management* (*Manajemen Kasus*), Ensiklopedia Ilmu Kepolisian, editor William G. Bailey. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

Widyopramono. (1994). *Kejahatan di Bidang Komputer*. Cet.I. Jakarta: Pustaka Sinar Harapan.

Wisnubroto, Al. (1999). *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*. Yogyakarta: Universitas Atma Jaya.

Laporan, Jurnal, Makalah, Kertas Kerja, Disertasi, Tesis dan Skripsi

Atmasasmita, Romli. Model Kerjasama Dalam Pemberantasan *Cybercrime* (Makalah disampaikan dalam Seminar Nasional tentang *Cybercrime*. Jakarta. (7 Desember 2004).

Blogger. (2007 November 5). *Kompas*, 34.

_____. Awaloedin. *Penyempurnaan Organisasi dan tata kerja kepolisian Negara Republik Indonesia 2002*. Jurnal Polisi Indonesia 2002 IV, 5.

Deperindag. *Paper Based Culture Versus Electronic Based Culture*. 9 Agustus 2006.

Ginting, Ramlan. *Kejahatan Dunia Maya (Cybercrime) di Sektor Perbankan*. (Makalah disampaikan dalam Seminar Penanganan Masalah Cybercrime di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh dan Terpadu, Jakarta, 10 Agustus 2006).

Golose, Petrus Reinhard. *Perkembangan Cybercrime dan Upaya Penanganannya*

di Indonesia oleh Polri. (Makalah disampaikan dalam Seminar Penanganan Masalah Cybercrime di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh dan Terpadu, Jakarta, 10 Agustus 2006).

Internet di SD Memang Sudah Zamannya. (2007 Desember 3). *Kompas*, 14.

Irsan, Koesparmono. *Polri mandiri dan kebudayaannya.* Jurnal Polisi Indonesia 2000 II, 6.

LSM dan *website*nya. (2007 November 21) *Djakarta The Magazine*, 12.

Montgomery, Dan. Agustus 2005. FBI Law Enforcement Bulletin: Excessive Force 101, Washington. Federal Bureau Investigation.

Nitibaskara, TB Ronny R : Problema Yuridis "*Cyber Crime*". (2000, 31 Juli). *Kompas*, 1-3.

"Netizen". (2007 November 30). *Kompas*, 45.

"Nokia, Independent Artists Club". (2007 Desember 21). *Kompas*, 16.

Online Storage. (2007 Desember 26). *Kompas*, 61.

Puslitbang Hukum dan Peradilan Mahkamah Agung Republik Indonesia. (2004). *Kejahatan Internet (Cybercrimes).* Jakarta: Mahkamah Agung Republik Indonesia

Ramli. M. Ahmad. (4 September 2004). *Prinsip-Prinsip Cyber Law dan Kendala Hukum Positif dalam Menanggulangi Cyber Crime.*

Reksodiputro, Mardjono. (1999). *Polisi Dan Masyarakat Dalam Era Reformasi: Polisi Sebagai Alat Penegak Hukum (Suatu Pemikiran Tentang Polisi Indonesia).* Jurnal Polisi Indonesia I, 75.

Rossmo, Kim. (2006). FBI Law Enforcement Bulletin: *Criminal Investigative Failures, Avoiding the Pitfalls (Part Two).* 18.

"Sofware Pendidikan". (2007 November 26). Kompas, 14.

Suparlan, Parsudi. (2003). *Pembangunan Komuniti, konflik, dan Pemolisian Komuniti.* Jurnal Polisi Indonesia IV, 31.

Suparlan, Parsudi. (1999). *Implementasi Polmas pada fungsi lalu lintas. Ilmu Kepolisian. Editor.* Chrysnanda DL, 397

Suparlan, Parsudi. (1994). *Metode Penelitian Kualitatif.* Program Kajian Wilayah Amerika. Program Pascasarjana Universitas Indonesia. 9

TV "Online" Makin Digemari Warga Amerika. (2008 Januari 3). *Kompas*, 14.

Artikel-artikel internet dari hasil penelusuran dalam situs berikut:

"Arrest Made in Falls Churh City Schools Bomb Threat Case." *http://www.fallschurchva.gov/Government/officeOfCommunications/documents/SuspectBombThreatArrested050305.pdf* (3 Mei 2005)

"Computer Hacking Forensic Investigator (CHFI)." *http://www.globalnettraining.com/certified-ethical-hacking-chfi-boot camp.asp* (10 Februari 2008)

"Convention on Cybercrime." *http://conventions.coe.int/Treaty/Commun/ ChercheSig.asp?NT=185&CM=&DF=&CL=ENG* (12 Februari 2008)

"Council of Europe." *http://en.wikipedia.org/wiki/Council_of_europe* (20 Maret 2008)

"Dual Processor System (DP System)." *http://www.pcmag.com/encyclopedia_term/0,2542,t=dual+ processor&i=55471,00.asp* (12 Februari 2008)

"Good Practice Guide for Computer-Based Electronic Evidence." *http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf* (10 Februari 2008)

"Internet" *http://en.wikipedia.org/wiki/Internet* (28 Februari 2008)

"Internet Kini Jadi Pelarian". *http://64.203.71.11/portal/infotekno/view.cfm?p=2007.11.23150427.* (2007 November 23)

"Marak, penjualan narkotika lewat internet." *http://www.bbc.co.uk /indonesian /news/story/2005/03/050302/internetdrugsau.shtml* (2 Maret 2005)

"Partai politik dan website-nya." *www.kpu.go.id* (12 Februari 2007)

"Serious Organised Crime Agency." *http://en.wikipedia.org/wiki/Serious_Organised_Crime_Agency* (10 Februari 2008)

"Student Centered E-Learning Environment (Scele)." *http://scele.cs.ui.ac.id/* (1 Maret 2008)

"Transaksi Seks, Modus Baru Kejahatan Internet." *http://www.sinarharapan.co.id /berita/0306/14/opi01.html* (14 Juni 2003)

"Telemedicine: Manfaatkan VPN-IP Telkom." *http://www.pikiran-rakyat.com /cetak/2005/0405/28/0605.htm* (28 April 2005)

"Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna, 10-17 April 2000." *http://www.uncjin.org /Documents /congr10/10e.pdf* (12 Februari 2007)

Valatkevièius, Darius. "The Problems Of Jurisdiction In Computer Crime Investigation." *http://www.leidykla.eu/en/journals/law/law-2007-vol-62/d-valatkevicius-the-problems-of-jurisdiction-in-computer-crime-investigation/* (10 Februari 2008)

Bahan Tersier

Departemen Pendidikan dan Kebudayaan. (1995). *Kamus Besar Bahasa Indonesia* edisi ke-2. Jakarta: Balai Pustaka.

Garner, Bryan A. (2004). *Black Law Dictionary*. United States of America: A Thomson Business.

Koentjaraningrat, Budhisantoso, Danandjaya, Suparlan, Masinambow, Sofian, (2003). *Kamus Istilah Antropologi*. Jakarta: Progres.

Pusat Pembinaan dan Pengembangan dan Bahasa Departemen Pendidikan dan Kebudayaan. (1993). *Pedoman Umum Ejaan Bahasa Indonesia yang Disempurnakan*. Cet.XVII. Jakarta: Balai Pustaka.

Slade, Robert. (2006). *Dictionary of Information Security*. Kanada: Syngress.

Thro, Ellen. (1991). *The Artificial Intelligence Dictionary*. San Marcos: Microtrend

Yayasan Pengembangan Kajian Ilmu Kepolisian. (2005). *Ensiklopedia Ilmu Kepolisian Edisi Bahasa Indonesia*. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

Riwayat Hidup Penulis

Nama : Petrus Reinhard Golose

Pangkat : Komisaris Besar Polisi

Tempat/Tgl Lahir : Manado, 27 November 1965

Pendidikan :

- Akademi Kepolisian (AKPOL) lulus tahun 1988
- Perguruan Tinggi Ilmu Kepolisian (S1) lulus tahun 1998
- Sekolah Staf dan Pimpinan (Sespim) selesai tahun 2002
- Pendidikan Magister Manajemen (S2) lulus tahun 2002

Riwayat Penugasan:

- Kepala Kepolisian Sektor (Kapolsek) Lodoyo, Blitar (1988-1991);
- Komandan Peleton Taruna (Dantontar), AKPOL (1991-1992);
- Kepala Sub Unit Pembunuhan dan Penculikan, Polda Metro Jaya (1993);
- Kepala Sub Unit Pencurian, Polda Metro Jaya (1994);
- Kepala Sub Unit Kejahatan dengan Kekerasan, Polda Metro Jaya (1995-1996);
- Kepala Unit Reserse Mobil, Korserse Polri (1998-2001);
- Kepala Kelompok Penyidikan Narkoba Bareskrim Polri (2001-2002);
- Penyidik Madya Unit Antiteror Direktorat I Bareskrim Polri (2002-2003);
- Kepala Satuan *Cybercrime* Polda Metro Jaya (2003-2006);
- Wakil Kepala Detasemen 88 Antiteror Polda Metro Jaya (2005-2006);
- Kepala Unit V *IT & Cybercrime* Bareskrim Polri (2006 sampai sekarang).

Kursus di luar negeri yang telah diikuti:

- *Counter Disaster Course* at the *Royal Military College of Science*, Swindon-England, 1995;
- FBI *National Academy,* Quantico ,VA,USA, 1999;
- FBI *National Academy Retraining*, Gold Coast, Australia, 2003;
- *Advance Computer Crime Course*, ILEA, Bangkok, Thailand, 2003;
- *Networks and Networking for Agent/System Security and Exploitation Course*, Hawaii, USA, 2004;
- *International Narcotics Enforcement Management Seminar* (INEMS), Maryland, USA, 2004;
- *Comprehensive Security Response to Terrorism, Asia Pacific Centre for Security Studies* (APCSS), Hawaii, USA, 2005;
- *Cybercrime Training Advance*, ILEA, Bangkok, Thailand, 2006;

- *International Program for Counter Terrorism* (DST), Paris, 2007.

Konferensi atau seminar yang telah diikuti meliputi:

- *Asian Drug Enforcement Conference* (ADEC), Tokyo, Japan, 2005;
- *Cybercrime, High Tech Crime, Conference*, Canberra, Australia, 2005;
- *International Drug Enforcement Conference*, (IDEC), Santiago, Chile, 2005;
- *The Fourth Botnet Task Force, Conference Center, Interpol Headquarters, Lyon, France*, 24 - 28 April 2006;
- *Head Country Risk Management, Conference Fighting Fraud Enchancing Trust in Visa Payments Singapura*, 28 - 30 Juni 2006;
- *Conference on Information Technology Solutions to the Identification of on-line Victims of Child Abuse , Santa Julian , Malta*, 11 – 13 September 2006;
- *The 7th CTINS Annual Conference and Interpol Asia-South Pacific Working Party on Information Technology Crime 4th Information Technology Crime Investigation and Training Seminar;*
- *6th International BotNet Task Force Conference*, Sidney, Australia, 2007;
- *Octopus Interface Conference Cooperation Against Cybercrime, Council of Europe, Strasbourg, France (2008).*

Penyidikan internasional yang pernah dijalani:

- *Investigation into the murder of NIO BENG SENG and tracking of the suspect* HONG LIE *and others* in Singapore, Malaysia, 1994;
- *Investigation into the triple murders committed by* OKI HARNOKO DEWANTONO in Los Angeles CA, USA, 1995;
- *Investigation into SHIROSAKI in the terrorist case involving Japanese Red Army*, 1997;
- *Investigation in* East Timor *and* New Zealand *into the murder of private MANNING, UN Peace Keeper from New Zealand Military*, 1999;
- *Coordinating and exchange information about drugs trafficking with US DEA , Singapore*, 2001;
- *Investigation into and coordinating with CNB and US DEA in the frame work of the tracking of HANS PHLIP in Singapore*, 2002;
- *Control Delivery, Surveillance Curaccau* (Netherlands Antilles), South America, 2002;
- *Coordinating with Thai Police (Special Branch)*, Cambodia *Police of the tracking of* HAMBALI *in* Bangkok *and* Phnom Penh, 2003;
- *Investigation into* Dulmatin *and* Umar Patek *in the* Bali *Bombing case*, Manila, 2004.

Kegiatan selaku pembicara (*speaker*):

- *Presentation about Bali Bombing Case in* Philadelphia, USA, 2003;
- *Speaker for Asian Drug Enforcement Conference* (ADEC), Tokyo, Japan, 2005;

- *Speaker* for The Anti Money Laundering Network Counter Terrorism Task Force, Hongkong, 2006;
- Speaker for *Cybercrime* Advance Course, Bangkok Thailand, 12 - 16 Juni 2006;
- *Speaker* for The 6th CTINS Annual Conference, Tokyo, Japan, 2006 ;
- *Speaker for Regional Seminar "Fighting Cybercrime: Intelligence, Enforcement and Exchanges Best Practices"*, Singapore, 2007;
- *Speaker for ICPO-CBI India 7th Conference on Cybercrime*, New Delhi, India, 2007.

Peace Keeping Force (UN CIVPOL):

- Cambodia-UNTAC (1993)
- Bosnia-Herzegovina-UNMIBH (2000-2001)

Penulis juga telah menyelesaikan beberapa tulisan dan telah dipublikasikan, baik dalam bentuk buku dan artikel diantaranya:

- Buku Satuan *Cybercrime*, Jakarta Metropolitan Police 2006;
- *Guide For Electronic Evidence Seizure and Handeling* (Pedoman Penyitaan dan Penanganan Bukti Elektronik, 2007;
- Artikel Perkembangan *Cybercrime* dan Upaya Penanganannya di Indonesia Oleh Polri, 2006.
- Artikel *Cybercrime* Permasalahan dan Tantangan ke Depan, 2007

Penulis aktif terlibat dalam Panitia Kerja dan Panitia Khusus, sebagai wakil dari Pemerintah Republik Indonesia untuk turut merumuskan Rancangan Undang-undang Informasi dan Transaksi Elektronik (RUU ITE) yang sudah disahkan DPR RI dalam Rapat Paripurna tanggal 25 Maret 2008 dan sudah menjadi Undang-undang No. 11 Tahun 2008. Penulis juga bersama-sama dengan rekan-rekan dari Departemen Komunikasi dan Informatika sedang menyiapkan Peraturan Pemerintah untuk Undang-undang ITE.

LAMPIRAN-LAMPIRAN

PETRUS REINHARD GOLOSE

9103070058

DAFTAR LAMPIRAN

Pelaksanaan Penelitian Lapangan

I. Wawancara Berpedoman

TIPE	NAMA	JABATAN	WAWANCARA PERTAMA (A)					
			TGL	JAM AWAL	JAM AKHIR	LAMA	TEMPAT	PEWAWANCARA/ MODERATOR
WBOS								
01	Agung Nugroho Wahyujatmiko	Pengacara	03 Agt 2007	12.05	13.00	95 Menit	Kompleks Polri Pejaten	Petrus R Golose
02	Ir Fayakhun Andriadi, M Kom	Sekretaris umum Badan Informasi Komunikasi PP Partai Golkar	15 Agustus 2007	17.20	17.40	20 Menit	Hotel Nikko	Petrus R Golose
WBIS								
01	AKP Alexander Sabar, S. IK	Penyidik Muda	02 Agt 2007	8.20	09.02	82 Menit	Kompleks Polri Pejaten	Petrus R Golose
02	AKBP Eddy Hartono, S. IK	Penyidik Madya	02 Agt 2007	22.40	23.25	85 Menit	Kompleks Polri Pejaten	Petrus R Golose

TIPE	NAMA	JABATAN	WAWANCARA PERTAMA (A)					
			TGL	JAM AWAL	JAM AKHIR	LAMA	TEMPAT	PEWAWANCARA/ MODERATOR
03	AKP I Ketut Budi Hendrawan, S.H., S. IK	Penyidik Muda	02 Agt 2007	23.35	00.10	75 Menit	Kompleks Polri Pejaten	Petrus R Golose
04	Kompol Zamri S, Kom	Penyidik Muda	03 Agt 2007	13.40	14.40	100 Menit	Kompleks Polri Pejaten	Petrus R Golose
05	Kompol Parmin, S.H	Penyidik Muda	03 Agustus 2007	22.10	22.45	35 Menit	Kompleks Polri Pejaten	Petrus R Golose
06	AKBP Drs Idam Wasiadi, S.H, S. Kom, MT	Penyidik Madya	03 Agustus 2007	22.50	23.20	70 Menit	Kompleks Polri Pejaten	Petrus R Golose
07	Kompol Dicky Patrianegara S. IK., S.H., Msi	Penyidik Madya	05 Agustus 2007	20.15	21.20	105 Menit	Kompleks Polri Pejaten	Petrus R Golose
08	Kompol Surawan S. IK	Penyidik Muda	05 Agustus 2007	21.25	21.35	10 Menit	Kompleks Polri Pejaten	Petrus R Golose
09	AKP Poibe Intan Noda Lince	Penyidik Pratama	06 Agustus 2007	22.15	22.35	20 Menit	Kompleks Polri Pejaten	Petrus R Golose

TIPE	NAMA	JABATAN	WAWANCARA PERTAMA (A)					
			TGL	JAM AWAL	JAM AKHIR	LAMA	TEMPAT	PEWAWANCARA/ MODERATOR
10	AKP Arif Mahfudiarto S. IK	Penyidik Muda	06 Agustus 2007	23.30	23.50	20 Menit	Kompleks Polri Pejaten	Petrus R Golose
11	AKBP Setiadi, S.H	Penyidik Madya	07 Agustus 2007	16.15	16.50	35 Menit	Hotel Nikko	Petrus R Golose
12	AKP Lindriani AMD	Penyidik Pratama	07 Agustus 2007	17.00	17.20	20 Menit	Hotel Nikko	Petrus R Golose
13	AKBP. Dra.S Laksmi D	Penyidik Madya	05 Oktober 2007	11.00	12.50	110 Menit	Kompleks Polri Pejaten	Petrus R Golose
14	AKBP Gagas Nugraha	Penyidik Madya	13 Januari 2008	21.24	22.17	53 Menit	Kompleks Polri Pejaten	Petrus R Golsoe

TIPE	NAMA	JABATAN	WAWANCARA KEDUA (B)					
			TGL	JAM AWAL	JAM AKHIR	LAMA	TEMPAT	PEWAWANCARA/ MODERATOR
WBIS								
09 (B)	AKP Poibe Intan Noda Lince	Penyidik Pratama	12 Januari 2008	14.07	14.23	30 Menit	Kompleks Polri Pejaten	Petrus R Golose
12 (B)	AKP Lindriani AMD	Penyidik Pratama	12 Januari 2008	15.11	15.28	39 Menit	Kompleks Polri Pejaten	Petrus R Golose
07 (B)	Kompol Dicky Patrianegara S. IK., S.H., Msi	Penyidik Madya	12 Januari 2008	15.29	16.49	80 Menit	Kompleks Polri Pejaten	Petrus R Golose
02 (B)	AKBP Eddy Hartono, S. IK	Penyidik Madya	13 Januari 2008	22.32	22.57	25 Menit	Kompleks Polri Pejaten	Petrus R Golose

II. Focus Group Discussion

FGD								
Robocop 01	Alexander Sabar, I Ketut Budi Hendrawan, Arif Mahfudiarto, Poibe Intan Noda Lince, Lindriani, H.	PAMA	02 Agustus 2007	10.00	14.10	410 Menit	Prompt Office	Rulas

	Budi Sutrisno, Maryudi Salempang, Eddy Tanjaya, Karsini, Nia Daniati							
Robocop 02	Zamri, Surawan, Idang Maryadi, Dicky Patrianegara, Eddy Hartono, Setiadi, Gagas Nugraha, Suminta, Hendra, Damayanti, Jumaroh	PAMEN	07 Agustus 2007	10.00	13.45	385 Menit	Prompt office	Rulas

III. Pengiriman Kuisioner Melalui Email

No	Nama Responden	Negara	Tgl Kirim	Feed Back
1	Mr. Gerhard Rosskopf	Austria	01 Nov 07	
2	Mr Alberto GARCIA MORALES	Spain	10 Nov `07	13 Nov `07
3	Mr Chris SIOURIS	USA	10 Nov `07	16 Nov `07
4	Mr Alexander SEGER	Council of Europe	10 Nov `07	21 Nov `07
5	Mr. Steve Santorelli	USA	10 Nov 07	
6	Mr. Michael C Dehneke			
7	Mr. Chi Hung Man	Hongkong	11 Nov 07	

Daftar Personel Unit V *IT & Cybercrime*

1. KOMBES. POL. Drs. PETRUS REINHARD GOLOSE, MM. (KANIT)
2. AKBP GAGAS NUGRAHA. SH.,SIK.
3. AKBP EDDY HARTONO, SIK.
4. AKBP Dra.S.LAKSMI DAMANYANTI
5. AKBP SETIADI, SH.
6. AKBP ARIS BUDIMAN, Msi
7. AKBP Drs. IDAM WASIADI, SH., S.Kom.
8. KOMPOL DICKY PATRIANEGARA, SH., SIK.
9. KOMPOL PARMIN, SH.
10. KOMPOL ZAMRI
11. KOMPOL SURAWAN, SIK.
12. KOMPOL LULUK ZUMAROH
13. KOMPOL I. KETUT HENDRAWAN, SH, SIK.
14. KOMPOL ARIF MAHFUDIARTO, SIK.
15. KOMPOL ALEXANDER SABAR, SIK.
16. AKP LINDRIYANI
17. AKP DIDI RAHMANTO
18. AKP ERLIN TANGJAYA
19. AKP POIBE INTAN NOSA LINCE
20. IPTU HERU BUDHI SUTRISNO, SH.
21. IPTU MARYUDI SALEMPANG, ST.
22. IPTU DWI HARYATI, SH.
23. IPTU KARSINI

Pedoman Wawancara

Penasihat Hukum Iqra Syafaat

Nama : **Agung Nugroho Wahyujatmiko**
Jabatan : **Pengacara**

Tempat :
Hari/Tgl : Jumat / 30-7-07
Pewawancara: Petrus R Golose

No.	Daftar Pertanyaan	Status
1.	Sudah berapa lama anda bekerja sebagai Advokat?	
2.	Tindak pidana apa saja yang pernah ditanggani oleh anda?	
3.	Apakah anda pernah menangani kejahatan komputer? Kejahatan komputer yang seperti apa? Tolong jabarkan!	
4.	Apakah anda pernah menangani kasus *hacking*?	
5.	Apakah anda pernah mengikuti pelatihan atau pembekalan mengenai kejahatan komputer? Mengenai *hacking*?	
6.	Bagaimana anda mencari tahu mengenai kejahatan komputer? Mengenai *hacking*?	
7.	Apakah anda pernah mengadakan penelitian mengenai kejahatan komputer? *Hacking*? Mengapa? Mengapa tidak? Apa yang anda lakukan?	
8.	Menurut pendapat anda, apakah *hacking* itu? Hubungannya dengan *cybercrime*?	
9.	Bagaimana anda manangani kasus *hacking* tersebut? Tolong ceritakan proses penanganan perkara tersebut!	
10.	Dalam menangani tindak pidana *hacking* (dalam hal ini kasus hacking Website Golkar), apakah anda mengalami	

No.	Daftar Pertanyaan	Status
	kesulitan dari segi pemilihan dan pemenuhan unsur-unsur tindak pidana sebagai hukum materil? Menurut anda, bagaimana seharusnya tindak pidana *hacking* diatur?	
11.	Dalam menangani tindak pidana *hacking* (dalam hal ini kasus hacking Website Golkar), apakah anda mengalami kesulitan dari segi hukum acara sebagai hukum formil? Menurut anda, bagaimana seharusnya hukum formil mengakomodasi kejahatan komputer atau *hacking*?	
12.	Bagaimana peranan penyidik dalam mengungkapkan tindak pidana pada umumnya? Berdasarkan pengalaman dan pendapat anda (dalam kasus hacking website Partai Golkar), apa yang perlu dibenahi?	
13.	Bagaimana peranan penyidik dari Unit IT & *Cybercrime* Bareskrim Polri dalam mengungkapkan tindak pidana *hacking*? Berdasarkan pengalaman dan pendapat anda, apa yang perlu dibenahi?	
14.	Sebagai informasi tambahan: selama ini, fasilitas komputer atau internet apa yang digunakan oleh anda? Apa kegunaannya?	
15.	Menurut pendapat anda, bagaimana Unit V IT & *Cybercrime* menangani perkara *hacking*? Apakah anda mengetahui siapa saja yang melakukan penyidikan kasus tersebut ? Apakah anda tahu pangkatnya apa? Siapa komandannya? Siapa yang paling berperan dalam penyidikan kasus tersebut hingga berkas perkara anda terima?	
16.	Menurut anda, apakah penyidik yang menangani kasus hacking website Partai Golkar menguasai apa itu yang namanya *hacking*? Pasal apakah yang digunakan penyidik untuk menjerat pelaku? Apakah penggunaan pasal tersebut sudah tepat? Jika belum, pasal apa yang menurut anda lebih tepat? jelaskan	
17.	Dalam kasus hacking website partai Golkar, bukti-bukti apa saja yang dilimpahkan oleh penyidik kepada kejaksaan? Apakah bukti-bukti tersebut cukup dapat diterima atau diperlakukan sebagai bukti yang	

No.	Daftar Pertanyaan	Status
	membuktikan tindak pidana hacking oleh Iqra Syafaat? Masalah apa saja yang menurut anda muncul sehubungan dengan bukti-bukti untuk kasus hacking?	
18.	Harap jelaskan proses pelimpahan berkas perkara hacking website Partai Golkar oleh Unit V IT & *Cybercrime* ? Apakah anda terlibat? Bagaimana menurut anda prosesnya, sudah baik, cukup baik, atau masih kurang baik? jelaskan	
19.	Menurut pendapat anda, apakah berkas perkara yang disiapkan dan dilimpahkan oleh Unit V IT & *Cybercrime* atas perkara hacking website Partai Golkar sudah cukup baik, baik atau baik sekali ataukah masih kurang baik?	
20.	Menurut anda, apa yang perlu diperbaiki dari penanganan kasus *hacking* baik dilihat dari segi penyidik, pembela, jaksa penuntut umum dan hakim yang memutus perkara anda.	

Note:
- Direkam menggunakan tape recorder dan video cam
- Dilaksanakan mulai pukul 12.05 sampai dengan _____

Pedoman Wawancara

Korban : **Partai Golkar**
Nama : Ir Fayakun Andriyadi, M Kom
Jabatan : Sekretaris Umum Badan Komunikasi PP Partai Golkar
Tempat : Hotel Nikko
Hari/Tgl : Rabu, 15-08-07
Pewawancara: Petrus R Golose

No.	Daftar Pertanyaan	Status
1.	Sudah berapa lama anda bekerja atau menggeluti bidang IT?	
2.	Selama ini, fasilitas komputer atau internet apa yang digunakan oleh anda? Apa kegunaannya?	
3.	Darimana anda mengetahui tentang kejahatan computer? Bagaimana dengan hacking?	
4.	Apakah yang anda ketahui tentang hacking? Apa itu hacking menurut anda? Apakah termasuk kejahatan?	
5.	Apa yang anda lakukan untuk mengatasi kejahatan komputer tersebut?	
6.	Apa yang anda lakukan untuk mengantisipasi kejahatan komputer tersebut?	
7.	Anda pernah mengikuti pelatihan atau pembekalan mengenai kejahatan komputer? Mengenai *hacking*?	
8.	Apakah anda pernah menjadi korban kejahatan komputer atau *hacking*? Tolong jabarkan! (hacking terhadap apa dan apa akibat hacking tersebut)	
9.	Hal-hal apa saja yang anda lakukan setelah anda menjadi korban hacking? (apa tindakan anda, apakah melaporkan, dan kemana melaporkan, apa alasan melaporkan ke instansi tersebut?)	
10.	Menurut pendapat anda, bagaimana Unit V IT & *Cybercrime* menangani perkara hacking? Siapa saja yang melakukan penyidikan kasus anda? Apakah anda tahu	

No.	Daftar Pertanyaan	Status
	pangkatnya apa? Siapa komandannya? Siapa yang paling berperan dalam penyidikan kasus anda?	
11.	Tindakan apa saja yang telah dilakukan oleh penyidik terhadap kasus hacking yang anda laporkan? (apakah penangkapan, penahanan, penyitaan barang bukti (apa saja khususnya dari pihak korban))?	
12.	Apakah penyidik yang melakukan penyidikan kasus hacking yang anda laporkan, menurut anda, menguasai apa itu yang namanya *hacking*? Apakah anda tahu, penyidik menggunakan pasal apa untuk menjerat pelaku?	
13.	Apakah anda mengetahui bagaimana penyidik Mabes Polri dapat menungkap kasus hacking yang anda laporkan? (bagaimana pelaku sampai tertangkap? Apakah anda memberikan bantuan? Jika ya, bantuan apa?)	
14.	Menurut anda, apakah fasilitas IT dan laboratorium Komputer Forensik yang dimiliki Mabes Polri sudah baik atau canggih? jelaskan	
15.	Harap jelaskan proses pelimpahan berkas perkara hacking yang anda laporkan dilakukan oleh penyidik ke pihak kejaksaan? Apakah anda dilibatkan? Bagaimana menurut anda prosesnya, sudah baik, cukup baik, atau masih kurang baik? jelaskan	
16.	Menurut pendapat anda, bagaimana Unit V IT & *Cybercrime* menanggapi laporan anda?	
17.	Menurut anda, apa yang perlu diperbaiki dari penanganan kasus *hacking* baik dilihat dari segi penyidik, pembela, jaksa penuntut umum dan hakim yang menutus perkara anda.	

Note:

- Direkam menggunakan tape recorder dan video cam
- Dilaksanakan mulai pukul 17.20 sampai dengan 17.40

edoman Wawancara

enyidik Unit V IT & Cyber Crime

ama : Alexander Sabar, SIK
abatan : Penyidik muda

empat : Kompleks Polri Legaten
ari/Tgl : Kamis / 2-7-2007
ewawancara : Petrus & Gibik

No.	Daftar Pertanyaan	Status
	[Pengenalan, maksud penelitian, gunanya alat perekam, penyajian data akan anonim, diulah secara umum]	
.	Pengalaman ▪ Sudah berapa lama anda bekerja sebagai penyidik? Sebelum menjadi penyidik? ▪ Tindak pidana apa saja yang pernah ditangani oleh anda? ▪ Apakah anda pernah menangani kejahatan komputer? ▪ Kejahatan komputer seperti apa yang pernah anda tangani? Tolong jabarkan!	
.	Pelatihan ▪ Pelatihan atau pendidikan apa yang telah anda jalani selama anda menjadi polisi atau penyidik? Seminar? Di dalam negeri? Luar negeri? ▪ Apakah anda pernah mengikuti pelatihan atau pembekalan mengenai kejahatan komputer? Mengenai *hacking*? Kapan? Dimana? Berapa lama? Hal baru apa yang anda pelajari? Bergunakah pelatihan tersebut di pekerjaan anda sehari-hari?	
.	Belajar sendiri ▪ Apakah anda pernah mecari tahu sendiri mengenai kejahatan komputer? Mengenai *hacking*? ▪ Bagaimana anda mencari tahu mengenai kejahatan komputer? Mengenai *hacking*? ▪ Apakah anda pernah mengadakan penelitian mengenai kejahatan komputer? Mengenai *hacking*? Mengapa? Mengapa tidak? Apa yang anda lakukan dalam penelitian tersebut?	

Pedoman Wawancara

Nama : Pol BE Intan / AKP
Jabatan : Penyidik
Tempat : Kejaksaan
Hari/Tgl. : Sabtu / 12-01-08
Pewawancara : Petrus R Golose

Prolog

Ucapan selamat datang, pengenalan, paparkan:

- Maksud penelitian
- Penggunaan alat perekam
- Penyajian data akan anonim
- Data akan diolah secara umum

Sesi Pertama:

1. **Perbandingan**

Sebagai suatu organisasi, Unit V IT & *Cybercrime* mengalami berbagai perubahan:

Dapatkah anda menceritakan cikal bakal atau awal dari pendirian Unit V IT & *Cybercrime*?
Bagaimana anda mengetahuinya?
Dapatkah anda memberikan gambaran terperinci mengenai perbandingan keadaan Unit V IT & Cybercrime antara Kanit terdahulu dengan Kanit yang sekarang:
Kapan perubahan itu terjadi?
Bagaimana prosesnya?
Apa saja yang berubah?
Gali hingga dapat mejelaskan perubahan yang terjadi di Unit V IT & *Cybercrime*:

- Pengelolaan sumber daya manusia: training, pelatihan, sekolah
- Keuangan/anggaran
- Suasana kerja
- Manajemen, proses kerja
- Infrastruktur: komputer, laboratorium komputer forensik, line telpon
- Jejaringan, networking, kerja sama dengan pihak lain di luar Unit V IT & *Cybercrime*:
  - Masih dalam tubuh POLRI
  - Di luar organisasi POLRI

Dengan Kanit terdahulu:
Apa yang anda sukai dari keadaan Unit V IT & *Cybercrime*? Apalagi? Apalagi?
Apa yang anda tidak sukai dari keadaan Unit V IT & *Cybercrime*? Apalagi? Apalagi?

Dengan Kanit saat ini:
Apa yang anda sukai dari keadaan Unit V IT & *Cybercrime*? Apalagi? Apalagi?
Apa yang anda tidak sukai dari keadaan Unit V IT & *Cybercrime*? Apalagi? Apalagi?

2. **Pengaruh Lingkungan Eksternal**

Sebagai suatu organisasi, Unit V IT & *Cybercrime* berhubungan atau berinteraksi dengan pihak/organisasi lain dalam lingkup Bareskrim Polri, Organisasi Polri, atau bahkan pihak di luar organisasi Polri.

Bareskrim Polri

- Bagaimana anda menggambarkan, hubungan fungsional yang terjadi antara Unit V IT & *Cybercrime* dengan Unit lain dalam Bareskrim Polri?
- Bagaimana Unit V IT & *Cybercrime* memandang Bareskrim Polri?
- Menurut pendapat anda, bagaimana Bareskrim Polri mempengaruhi kinerja Unit V IT & *Cybercrime* dalam melakukan penyidikan:
  - Bareskrim Polri berpengaruh positif terhadap manajemen penyidikan.

    - Contohnya:
  - Bareskrim Polri berpengaruh negatif terhadap manajemen penyidikan.
    - Contohnya:
  - Bareskrim Polri tidak mempunyai pengaruh terhadap manajemen penyidikan.
    - Contohnya:

Polri

- Bagaimana anda menggambarkan, hubungan fungsional yang terjadi antara Unit V IT & Cybercrime dengan Polri?
- Bagaimana Unit V IT & *Cybercrime* memandang Polri?
- Menurut pendapat anda, bagaimana Polri mempengaruhi kinerja Unit V IT & *Cybercrime* dalam melakukan penyidikan:
  - Bareskrim Polri berpengaruh positif terhadap manajemen penyidikan.
    - Contohnya:
  - Bareskrim Polri berpengaruh negatif terhadap manajemen penyidikan.
    - Contohnya:
  - Bareskrim Polri tidak mempunyai pengaruh terhadap manajemen penyidikan.
    - Contohnya:

Lingkungan di luar Polri

- Selain dengan Polri, Unit V IT & *Cybercrime* juga berhubungan dengan pihak lainnya.
- Dapatkah anda menyebutkan dan mengelompokan pihak lain yang berhubungan dengan Unit V IT & *Cybercrime* tersebut!
- Contoh: (jangan dibacakan, apabila responden sudah memiliki pengelompokan sendiri)
  - Media massa
    - Dalam negeri
    - Luar negeri
  - Penegak hukum
    - Dalam negeri: kejaksaan, hakim, pengacara
    - Luar negeri: FBI, AFP, Singapore
  - Badan internasional: Interpol, UN,
  - Industri
    - Umum: perbankan
    - Berhubungan langsung dengan komputer: Microsoft, Asosiasi Industri Penyedia Jasa Internet.
  - Lembaga Swadaya Masyarakat
    - Dalam negeri
    - Luar negeri
  - Akademisi
    - Dalam negeri
    - Luar negeri
  - Pemerintahan
    - Dalam negeri: Bank Indonesia, DPR
    - Luar negeri: Masing-masing negara
  - Masyarakat;
    - Korban kejahatan
    - Pelaku kejahatan
- Siapa yang biasanya menjalin hubungan dengan para pihak tersebut?
- Bagaimana caranya?
- Menurut pendapat anda, dari semua pihak yang berada di luar Unit V IT & *Cybercrime*, mana yang paling penting (skala prioritas) untuk dibina hubungannya? Mengapa? Mengapa tidak?
- Menurut pendapat anda, bagaimana lingkungan luar mempengaruhi kinerja Unit V IT & *Cybercrime* dalam melakukan penyidikan:
  - Lingkungan luar berpengaruh positif terhadap manajemen penyidikan.
    - Contohnya:
  - Lingkungan luar berpengaruh negatif terhadap manajemen penyidikan.
    - Contohnya:
  - Lingkungan luar tidak mempunyai pengaruh terhadap manajemen penyidikan.

- Contohnya:

Tambahan hanya untuk Perwira

1. Struktur organisasi Unit V IT & *Cybercrime*

   - Dapatkah anda menceritakan bagaimana struktur organisasi Unit V IT & *Cybercrime* yang ada saat ini?
   - Apa wewenang dan pekerjaan masing-masing bagian dari struktur organisasi tersebut?
   - Dari struktur organisasi tersebut, bagaimana rantai komando diterapkan?
   - Siapa bertanggung jawab pada siapa?
   - Siapa yang merencanakan? Melaksanakan? Mengawasi atau memonitor? Mengevaluasi pekerjaan yang ada di Unit V IT & *Cybercrime*?
   - Apakah struktur organisasinya saat ini sudah cukup baik? Atau apakah menurut anda perlu perubahan? Mengapa? Mengapa tidak? Apa kelebihan dan kekurangan dari struktur organiasi yang flat (mendatar) tersebut?

2. Visi dan Misi Unit V IT & *Cybercrime*

   - Apakah visi dan misi Unit V IT & *Cybercrime*?
   - Siapa yang membuat visi dan misi tersebut?
   - Bagaimana visi dan misi tersebut dijabarkan dalam program kerja Unit V IT & *Cybercrime*?
   - Apakah anda dilibatkan dalam proses pembuatan visi dan misi tersebut? Mengapa? Mengapa tidak?
   - Apakah visi dan misi Unit V IT & *Cybercrime* sudah cukup baik? Atau apakah menurut anda perlu perubahan? Mengapa? Mengapa tidak?

3. Manajemen Organisasi Unit V IT & *Cybercrime*

   - Menurut pendapat anda, apa yang dimaksud dengan manajemen organisasi?
   - Bagaimana anda menggambarkan manajemen organisasi Unit V IT & *Cybercrime*?
   - Apakah peranan anda dalam _____ di Unit V IT & *Cybercrime*?
     - Perencanaan
     - Pelaksanaan/program kerja
     - Evaluasi
   - Bagaimana Unit V IT & *Cybercrime* sebagai suatu organisasi melakukan perencanaan?
     - Siapa yang membuat perencanaan tersebut?
     - Apakah anda dilibatkan dalam proses perencanaan tersebut? Mengapa? Mengapa tidak?
     - Kapan biasanya dilakukan perencanaan?
   - Bagaimana perencanaan dan pelaksanaan Unit V IT & *Cybercrime* mengenai:
     - Pengelolaan sumber daya manusia:
       - Seleksi
       - Perekutan
       - Pengenalan
       - Peningkatan sumber daya manusia
       - Jenjang karir
     - Peningkatan infrastruktur termasuk di dalamnya laboraterium forensik:
       - Pengadaan alat
       - Pelatihan
     - Penegakan Hukum
       - Peningkatan kesadaran masyarakat
       - Pelaksanaan penyidikan
       - Lainnya
     - Penggalangan dana
       - Sumber dana dari anggaran Polri
       - Sumber dana lainnya
     - Hal-hal lain

- Dalam pelaksanaan siapa yang berperan:
  - mengawasi pelaksanaan
  - mengkoordinasikan pelaksanaan
  - menawarkan pilihan-pilihan penyelesaian masalah
  - mengambil keputusan termasuk merubah rencana
- Bagaimana Evaluasi dari Program Kerja Unit V IT & *Cybercrime* dilakukan?
  - Siapa yang membuat evaluasi tersebut?
  - Apakah anda dilibatkan dalam proses evaluasi kerja tersebut? Mengapa? Mengapa tidak?
  - Kapan evaluasi kerja tersebut dilakukan?
  - Apa kreteria/parameter sukses atau gagal suatu program kerja?
  - Apa tindakan yang diberikan terhadap anggota yang telah sukses melakukan suatu program kerja?
  - Apa tindakan yang diberikan terhadap anggota yang telah gagal melakukan suatu program kerja?
  - Apakah hasil evaluasi tersebut mempengaruhi rencana organisasi atau pelaksanaan program kerja ke depan? Mengapa? Mengapa tidak?
- Apa program kerja Unit V IT & *Cybercrime:*
  - Tahun ini
  - Tahun lalu
  - Tahun depan

4. Manajemen Penyidikan
   - Bagaimana anda menceritakan alur masuknya perkara di Unit V IT dan *Cybercrime* sampai dengan pelimpahan berkas perkara ke Kejaksaan atau penghentian perkara?
   - Dalam alur tersebut terdapat proses penyidikan, bagaimana penyidikan dilakukan di Unit V IT dan *Cybercrime* bila ditelaah dari:
     - Perencanaan
     - Pelaksanaan
     - Evaluasi
   - Siapa yang bertanggung jawab atas pelaksanaan penyidikan kasus dalam Unit V IT dan *Cybercrime*? Jelaskan bagaimana pertanggungjawabannya? Pembagaian kerjanya? Mengapa?
   - Bagaimana peran laboratorium forensik komputer dalam proses penyidikan di Unit V IT dan *Cybercrime*? Siapa yang menyelenggarakan laboratorium tersebut?
   - Siapa yang berperan dalam masalah pendanaan dalam proses penyidikan di Unit V IT dan *Cybercrime*? Bagaimana pengaturannya? Mengapa? Mengapa tidak?
   - Bagaimana fungsi pengawasan terhadap proses penyidikan di Unit V IT dan *Cybercrime*? Siapa yang menjalankan fungsi tersebut? Bagaimana pelaksanaannya?
   - Bagaimana dalam hal suatu Unit V tidak mampu mengungkap suatu kasus IT & *Cybercrime*? Apa yang dilakukan? Mengapa? Mengapa tidak?
   - Hal-hal apa sajakah yang dapat menjadi halangan, hambatan atau kesulitan-kesulitan dalam manajemen penyidikan di Unit V IT dan *Cybercrime*? Jelaskan!
   - Adakah pihak luar yang terlibat dalam penyidikan di Unit V IT dan *Cybercrime:*
     - *Di luar negeri.*
       - Contohnya:
     - *Di dalam negeri.*
       - Contohnya:
   - Dalam penyelidikan kasus hacking website Partai Golkar, adakah pihak luar yang terlibat dalam penyidikan di Unit V IT dan *Cybercrime:*
     - *Di luar negeri.*
       - Contohnya:
     - *Di dalam negeri.*
       - Contohnya:

5. Budaya organisasi

Dari pengalaman anda selama di Unit V IT dan *Cybercrime*

- Menurut pendapat anda, hal-hal apa atau tindakan atau kebiasaan apa yang dianggap penting (dominan) oleh sesama anggota tim, misalnya (tidak harus dibacakan semua, hanya sebagai contoh).
  - Tepat waktu:
    - "Datang tidak harus tepat waktu tapi pekerjaan selesai." atau;

- "Datang tepat waktu walau tidak tahu harus mengerjakan apa".
- Tanggung jawab kesalahan:
  - "Kalau ada kesalahan saling melindungi, tidak peduli siapa yang salah." atau;
  - "Kalau ada kesalahan harus dicari siapa yang salah, agar dia yang bertanggung jawab dan tak terulang lagi".
- Pengerjaan tugas:
  - "Pekerjaan diselesaikan bersama-sama, hasil yang dicapai juga atas nama bersama" atau;
  - "Pekerjaan diselesaikan sendiri, tanggung jawab masing-masing dan hasil yang dicapai juga atas nama individu."
- Kerja sama:
  - "Kalau ada yang tidak bisa menjalankan tugas, yang lain membantu" atau
  - "Kalau ada yang tidak bisa menjalankan tugas, dipermalukan, diganti dengan orang yang bisa."
- Pendanaan:
  - "Kalau ada pekerjaan harus ada uang ekstra, tidak ada uang tidak jalan" atau
  - "Ada atau tidak ada uang ekstra, pekerjaan harus dijalankan."
- Kepuasan
  - "Untuk apa repot banting tulang, toh gaji tetap sama" atau ;
  - "Bekerja sebaik mungkin, untuk kepuasan diri pribadi'.
- Penghargaan
  - "Jika sukses melakukan suatu pekerjaan mengharapkan penghargaan (pujian, uang)" atau;
  - "Jika sukses melakukan suatu pekerjaan itu adalah kewajiban. Hal biasa."
- Hal-hal lainnya yang dianggap penting...

- Menurut pendapat anda, hal-hal apa atau tindakan atau kebiasaan apa yang dianggap penting (dominan) oleh pimpinan, misalnya:
  - Penampilan:
    - "Penampilan harus menyakinkan. pakaian rapih dan bersih, mentereng, rambut terawat, ngomong menyakinkan" atau;
    - "Penampilan tidak penting yang penting kualitas atau hasil, pekerjaan beres tempat waktu, penampilan boleh sekenanya",
  - Inisiatif anggota:
    - "Proaktif, anggota diharapkan melakukan inisiatif sendiri, mengusulkan suatu solusi, dan bertanggung jawab atas pilihannya" atau
    - "Pasif, anggota diharapkan menunggu perintah, melaksanakan sesuai dengan perintah. Tanpa perintah tidak ada yang jalan. Tidak ada yang berani bertanggung jawab."
  - Pengambilan keputusan:
    - "Demokratis, memberikan kesempatan anggota mengeluarkan pendapatnya, dan mengambil keputusan dari pendapat terbanyak" atau
    - "Partisipatif, memberikan kesempatan anggota mengeluarkan pendapatnya dan mengambil keputusan dengan mempertimbangkan pendapat anggota" atau
    - "Otoriter, tidak memberikan peluang untuk mengeluarkan pendapat, semuanya terserah pimpinan."
  - Pemberdayaan manusia
    - "Kemampuan harus terus diasah, bahasa Inggris, komputer, bila perlu ikut seminar di dalam dan luar negeri. siap jadi pembicara" atau;
    - "Kemampuan diasah sendiri, baca buku sendiri, tidak perlu ada investasi untuk menambah kemampuan."
  - Penghargaan
    - "Penghargaan diberikan secara subyektif, tidak ada kreteria yang jelas, begitu pula cara dan bentuk dari penghargaan tersebut, semuanya tergantung pemimpin".
    - "Penghargaan diberikan secara seobyektif mungkin, dengan kreteria yang jelas, dengan mempertimbangkan pendapat teman sejawat".
  - Laporan
    - "Pimpinan tidak ingin mendengar adanya permasalahan. Semuanya harus baik dan siap. Laporan dibuat asal bapak senang sehingga tidak sesuai dengan kenyataan".
    - "Pimpinan ingin melihat fakta kalau ada permasalahan dicari alternatif permasalahan sendiri dan selesaikan sendiri."
    - "Pimpinan ingin melihat fakta, kalau ada permasalahan dicari alternatif permasalahan bersama dan selesaikan bersama."

- Menurut pendapat anda, bagaimana kebiasaan-kebiasaan yang dominan mempengaruhi kinerja Unit V IT & *Cybercrime* dalam melakukan penyidikan:
  - Kebiasaan di Unit V IT & *Cybercrime* yang **berpengaruh positif** terhadap manajemen penyidikan.
    - Contohnya:
  - Kebiasaan di Unit V IT & *Cybercrime* yang **berpengaruh negatif** terhadap manajemen penyidikan.
    - Contohnya:
  - Kebiasaan di Unit V IT & *Cybercrime* **tidak mempunyai pengaruh** terhadap manajemen penyidikan.
    - Contohnya:

6. Kepemimpinan

Sekarang kita berbicara mengenai kepemimpinan.

- Menurut pendapat anda, apa yang dimaksud dengan kepemimpinan?
- Bagaimana anda menggambarkan kepemimpinan di Unit V IT & *Cybercrime*?
- Menurut pendapat anda, bagaimana kepemimpinan mempengaruhi kinerja Unit V IT & *Cybercrime* dalam melakukan penyidikan:
  - Kepemimpinan di Unit V IT & *Cybercrime* yang **berpengaruh positif** terhadap manajemen penyidikan.
    - Contohnya:
  - Kempemimpinan di Unit V IT & *Cybercrime* yang **berpengaruh negatif** terhadap manajemen penyidikan.
    - Contohnya:
  - Kepemimpinan di Unit V IT & *Cybercrime* **tidak mempunyai pengaruh** terhadap manajemen penyidikan.
    - Contohnya:
- Menurut pendapat anda, tanpa kehadiran seorang pemimpin, dapatkah Unit V IT & *Cybercrime* tetap eksis dan menjalankan tugasnya? Mengapa? Mengapa tidak?
- Bagaimana anda menggambarkan kepemimpinan yang ideal untuk Unit V IT & *Cybercrime* di masa yang akan datang? Apa lagi? Apa lagi?

7. Kerangka Peningkatan [*Improvement Grid*]

- Apabila anda diberi wewenang untuk memimpin Unit V IT & *Cybercrime*, hal-hal apa saja yang akan anda lakukan:
  - Hal-hal apa saja yang menurut anda baik tapi perlu dilakukan lebih sering lagi [*Do more*].
    - Contohnya:
  - Hal-hal apa saja yang menurut anda baik tapi perlu dilakukan secara berbeda [*Do differently*].
    - Contohnya:
  - Hal-hal apa saja yang menurut anda buruk dan harus segera dihentikan [*Stop doing*]
    - Contohnya:
  - Hal-hal apa saja yang menurut anda belum dilakukan dan harus mulai dilakukan [*Start doing*].
    - Contohnya:

Penutup

Terima kasih atas masukan dan waktu anda. Penjelasan anda sangat penting bagi penelitian yang saya lakukan.

Identitas

Nama	: Bpk. ANW
Pangkat	:
Bagian	:
Umur	:
Status	:
Pendidikan	:

Narasi

Responden adalah lawyer dari Terdakwa dalam kasus hacking website Partai golkar. Responden memulai karirnya sejak tahun 1998 yaitu bekerja di Citibank sebagai legal documentation dengan tugas mengecek loan agreement apakah sudah sesuai dengan jaminannya atau tidak, meriview para pihaknya, dan sebenarnya sudah ada standard tersendiri kemudian pada tahun 2000 Responden pindah ke kantor hukum William Effendi sebagai legal associate yang bertugas melakukan legal audit untuk Bonds dengan kepailitan, selain bekerja di William &Efffendi Responden juga mengajar di Universitas Indonusa Esa Unggul. Kemudian pada tahun 2002 Responden mengikuti pendidikan lagi, dan pada tahun 2006 Responden bergabung dengan BM & Partners sebuah kantor hukum.

Responden masuk Universitas Indonesia pada tahun 1993 dan lulus pada tahun 2000, kemudian pada tahun 1994 Responden masuk Komunikasi FISIP UI dan lulus pada tahun 1999, selanjutnya mengikuti pendidikan di Prasetya Mulya dari tahun 2000-2005.

Selama menjadi lawyer Responden sudah menangani beberapa perkara, namun perkara yang ditangani ada yang hanya sampai pada tingkat kepolisian dan ada juga yang sudah sampai di tingkat Pengadilan. Untuk kasus yang sudah sampai di Pengadilan yang pernah ditangani oleh Responden adalah kasus yang berhubungan dengan penipuan kemudian kekerasan dalam rumah tangga, serta hacking website partai golkar. Sedangkan yang masih dalam proses kepolisian masih diusahakan untuk melakukan perdamaian diantaranya kasus penipuan, penggelapan dalam jabatan.

Responden pernah mendampingi untuk kasus penipuan, dimana ada penipuan pembayaran hotel dia sudah menginap dihotel tapi tidak membayar kemudian ada juga perjanjian tinggal diapartemen ternyata tidak mau melakukan pembayaran. Pada kasus tersebut Responden mendampingi mulai dari tingkat Kepolisian, Kejaksaan sampai ke Pengadilan dan sampai pada Putusan. Selanjutnya kasus rumah tangga dimana pihak istrinya menganggap suaminya melakukan kekerasan pemukulan sehingga ada bekas lukanya 2 x 3 cm warna biru kemudian dilakukan pemberkasan

dipolisi, dipolisi Responden tidak mendampingi tetapi Responden berperan di Pengadilannya, kemudian Responden juga beberapa kali melakukan pendampingan yang tidak sampai kepengadilan karena mungkin dia sebagai saksi, atau belum sampai ke tersangka dan atau sampai sekarang berkasnya masih berlanjut yaitu kasus dispute pemegang saham di Manado kemudian ada dispute pemegang saham juga antar pemegang saham atau ahli warisnya di Jakarta. Penanganan-penanganan kasus tersebut terjadi dari tahun 2006-2007.

Sebagaimana telah disebutkan diatas, Responden pernah menangani kasus hacking, yaitu hacking pada website partai golkar, dimana Responden adalah Lawyer dari Iqra Syafaat yang melakukan perubahan penampilan dari website partai Golkar secara melawan hukum dimana dia tidak mempunyai otoritas untuk melakukan itu, dan dia melakukan penjebolan sekuriti dari websitenya partai Golkar kemudian dia melakukan perubahan-perubahan.

Mengenai pendidikan terhadap kejahatan komputer Responden pernah mengikuti seminar 1 (satu) kali di Bank Indonesia, dimana para pesertanya para konsultan hukum bankers, dalam seminar tersebut Pembicaranya hanya membicarakan secara umum saja tidak khusus mengenai hacking, jadi dalam seminar tersebut bertujuan meningkatkan wearnest bahwa sudah ada kasus mengenai kejahatan komputer dan dibutuhkan aturan hukum yang mengaturnya.

Menurut Responden pelaku hacking disebut dengan hacker, dimana hacker ini masuk kedalam suatu sistem komputer yang bukan miliknya, dimana tidak mempunyai otoritas jadi dia berusaha masuk kedalam sistem komputer bisa internal komputer dalam suatu perusahaan bisa juga melalui internet kemudian dia melakukan kegiatan-kegiatan yang tidak berdasarkan otoritasnya dan bisa mengambil dokumen, bisa acak-acak dokumen tersebut bisa juga merubah penampakan dokumen tersebut atau juga bisa memasukkan dokumen serta menyebarkan virus dijaringan tersebut jadi intinya masuk kedalam suatu sistem tanpa ijin.

Menurut Responden sebelumnya Responden tidak terlalu memahami mengenai hacking namun setelah menangani kasus hacking Responden menjadi cukup mengerti karena pada saat mendampingi Tersangka, Tersangka sendiri menceritakan kenapa bisa menjadi hacker, kenapa dia tertarik, kemudian apa yang dilakukan untuk bisa merubah website partai golkar dan kegiatan apa yang dilakukan sebelumnya untuk bisa memasuki website partai golkar. Berdasarkan keterangan yang disampaikan oleh Tersangka kepada Responden pengrusakan terhadap tampilan website partai Golkar bukanlah yang pertama kali dilakukan oleh tersangka tapi Tersangka sudah beberapa kali melakukannya namun tidak ada tindak pidana yang lebih lanjut. Untuk menambah pengetahuannya mengenai hacking Responden mencari tau lebih dalam mengenai hacking, dimana Responden mencari taunya melalui internet kemudian dari seminar, dan juga melalui buku.

Menurut Responden kasus hacking website partai golkar sangat menantang baginya, oleh karenanya Responden secara intends melakukan penelitian. Penelitian yang dilakukan oleh Responden adalah penelitian base research dari bahan literature, mengenai aturan undang-undangnya kemudian proses penyidikannya juga ada kaidah-kaidahnya, kemudian kaidah-kaidah itu diperiksa apakah benar hak-hak dari terdakwa dijaga oleh para Penyidik jangan sampai para Penyidik melanggar hak-haknya Tersangka. Kemudian diadakan studi perbandingan dengan kasus hacking yang terdahulu yaitu mengenai kasus hacking Danny Firmansah. Karena kasus hacking Iqra Syafaat mirip dengan kasus Hacking Danny Firmansah.

Responden melihat hubungan komputer dan tekhnologi informasi berkaitan erat dengan berbagai macam kehidupan. Sebagai contoh apabila mau transfer uang dulunya kita datang ke bank memakai ATM dari ATM bisa bergeser bisa lewat handphone bisa lewat internet, dari situ banyak terjadi aktivitas dari banyaknya aktivitas tersebut akhirnya orang mempunyai opportunity untuk melakukan kejahatan, dimana ada yang melakukan penipuan, penipuan dimulai dari membuat homepage, dimana homepagenya mirip seperti homepagenya salah satu bank, sehingga orang akan memberikan passwordnya, kemudian pemesanan dikomputer dengan nama palsu, penyebaran virus jadi banyak kejahatan-kejahatan yang akhirnya berkecimpung didunia maya karena aktivitas orang juga akhirnya lebih banyak disana lebih intens dari situ.

Dengan demikian menurut Responden hubungan hacking dengan cyber crime yaitu satu modus kejahatan yang ada didunia maya atau berhubungan dengan komputer dengan ciri khasnya sendiri adalah masuknya seseorang hacker ke suatu sistem tanpa mempunyai otoritas secara illegal yang membedakan dengan kejahatan yang lain.

Responden menjelaskan bahwa pendampingan yang dilakukannya terhadap Tersangka adalah setelah pemeriksaan berjalan. Proses penanganan yang dilakukan oleh Responden yang pertama adalah pengenalan kemudian mencari tau latar belakangnya, keluarganya, pendidikannya dan segala macam untuk bahan pembelaannya. Pertemuan pertama Responden dengan Tersangka yaitu pada saat pemeriksaan di Mabes Polri kemudian Responden mengunjunginya lagi di Rutan Salemba karena ada beberapa data yang kurang jelas dan langkah lanjut yang akan diambil untuk penanganan selanjutnya. Kemudian Responden berusaha menyakinkan Tersangka bahwa Responden mampu untuk menjadi pendampingnya. Selanjutnya Responden mencoba menggali informasi yang lebih dalam dari Tersangka, mengenai kronologis kejadiannya, apa saja yang sudah disampaikan oleh Tersangka kepada Penyidik, dsb.

Dari hasil investigasi tersebut Responden menemukan bahwa Tersangka adalah orang yang lugu bukan orang yang mempunyai motivasi tertentu untuk mengambil keuntungan dari deface website partai Golkar, dia tidak mempunyai motivasi politik ataupun motivasi financial, namun hanya iseng saja, sehingga Responden merasa kasihan terhadapnya. Berdasarkan keterangan Tersangka kepada Responden,

Tersangka mengetahui bahwa perbuatannya merupakan suatu kesalahan namun dia tidak menyadari bahwa konsekuensinya bisa sampai dipenjara, selain itu menurut Tersangka banyak juga hacker-hacker lain yang melakukannya.

Menurut Responden selama penanganan kasus tersebut Penyidik sudah melakukan semua prosedur sebagaimana mestinya, dan terhadap hak-hak Tersangka juga sudah terpenuhi.

Terhadap pemilihan dan pemenuhan unsur-unsur tindak pidana, menurut Responden pada saat itu Penyidik banyak memberikan pilihan mulai dari pasal yang ada di KUHP sampai yang undang-undang telekomunikasi kemudian dari pilihan tersebut menurut Responden tidak tahu mana yang akhirnya ditembak oleh Penyidik. Dalam surat dakwaannya sendiri pasal yang digunakan adalah KUHP dan juga telekomunikasi tapi kalau dilihat dari perkembangannya dari kasus Dani Firmansyah, sepertinya Penyidik juga mengarahkan Tersangka dengan undang-undang telekomunikasi dan menurut Responden hal itu lebih berbahaya karena ganjarannya ada uang dan penjara lebih lama jika dibandingkan dengan pengaturan yang ada di KUHP.

Menurut Responden pembuktian dalam kasus tersebut terlalu abstrak bagi para Jaksa dan hakim karena menurut Responden mereka tidak mengetahu tentang email atau chatting kemudian mereka harus menjelaskan mengenai adanya suatu jaringan dan ada orang masuk kedalam jaringan secara illegal, sehingga menurut Responden hal tersebut menjadi susah dalam pembuktiannya karena ada kesenjangan pengetahuan.

Menurut Responden ada hal yang unik dalam kasus hacking website partai golkar karena kejadiannya di Batam sementara penahanannya di Jakarta kemudian berkaitan dengan bukti-bukti yang ada karena tidak ada saksi matanya. Kemudian yang menjadi pertanyaan adalah sepertinya kasusnya sangat kuat sementara tidak ada saksi yang melihat dan tidak ada bukti-bukti yang secara konkrit. Namun demikian Majelis hakim dalam kasus hacking website partai gokar mengacu pada kasus Danny Firmansyah dimana dalam kasus tersebut Majelis hakim mempertimbangkan bukti-bukti digitalnya, sehingga bukti digitalnya di printout dijadikan bukti surat, begitu pula halnya yang terjadi dalam kasus Iqra Syafaat, dengan demikian ada interpretasi dan yurisprudensi dari kasus-kasus terdahulu, jadi semua bukti-bukti digital berupa cd saka, berupa program di print out dan dikedepankan di depan Jaksa dan Hakim sebagai bukti tertulis.

Menurut Responden pengaturan tindak pidana hacking sudah terakomodasi dalam undang-undang telekomunikasi namun apabila ingin lebih dipertegas lagi seperti negara lain Responden tidak keberatan, menurut Responden yang diperlukan tidak hanya pengaturan mengenai alat bukti digital akan tetapi pengetahuan Jaksa dan Hakimnya karena menurut Responden Jaksa dan Hakim hanya mengajukan dokumen-dokumen yang di copy paste dari apa yang diberikan oleh Penyidik jadi disini Penyidik adalah kunci penegakkannya, karena menurut Responden dia pernah

berdiskusi dengan Jaksa dimana dia memberikan argument namun Jaksa tidak tau dasar-dasarnya, mereka hanya mengambil apa yang dikatakan oleh penyidik, jadi sumber-sumbernya benar-benar penyidik.

Didalam proses pembuktian sendiri tidak tergambarkan secara jelas pembuktiannya, Responden mencontohkan kalau dilihat di film-film Amerika kesan yang didapat terhadap bukti, bukti benar-benar ditunjukkan prosesnya dimana ada presentasi bagaimana proses kejadiannya. Namun dalam kasus ini hal tersebut tidak dilakukan, pembuktiannya adalah barang-barang bukti berupa kertas yang tidak menggambarkan kejadian sebenarnya. Menurut Responden hal tersebut akan berbeda apabila buktinya diceritakan tuntutannya, ini ada program kemudian dimasuki oleh hacker, jadi ada simulasi, menurut Responden hal tersebut lebih menyakinkan kepada hakim kepada jaksa yang tidak mengerti atau yang belum memahami mengenai hacking, dan menurut Responden sebaiknya presentasi tersebut dilakukan oleh penyidik maupun saksi ahli sehingga ada preseden yang bagus dimasyarakat.

Dalam kasus ini sendiri menurut Responden terdapat tekanan-tekanan dari factor eksternal, dimana akhirnya yang dirugikan adalah Klien Responden karena factor eksternalnya adalah partai golkar yang masih dominan didalam pemerintahan dan Yusuf Kalla, karena tampilan depan dari website partai golkar adalah gambar Yusuf Kalla, dimana satu blok halaman tersebut dirubah Tersangka menjadi gorilla dan bisa diinterprestasikan gambar Yusuf Kalla yang dirubahnya menjadi gorilla padahal Tersangka tidak tau disitu ada yusuf kalla bahkan Tersangka sendiri tidak tau kalau Yusuf Kalla itu siapa. Dengan demikian menurut Responden ada tekanan-tekanan social terlebih lagi tekanan-tekanan politik yang lebih mempengaruhi keputusan Jaksa dan Hakim dalam melakukan proses pengadilan dibandingkan factor-faktor teknis legal itu sendiri.

Terhadap segi hukum acaranya sendiri, Responden cukup mengalami kesulitan daiam hukum formilnya karena prosesnya abstrak dan tidak bisa direkayasa ulang dengan mudah dimana seharusnya proses tersebut sangat penting bagi pembuktian unsur-unsur ada tidaknya tindak pidana. Selanjutnya mengenai prosedur hukum pembuktiannya, karena saksi ahli, penyidik serta pihak-pihak yang terkait memberikan pemahaman yang sangat abstrak, sehingga bagi orang yang tidak mengetahui tekhnologi tidak akan memahaminya sedangkan pemahaman terhadap hal tersebut sangat penting untuk membuat suatu Putusan.

Kemudian menurut Reponden Jaksa dan Hakim tidak dapat diberi pertimbangan untuk mengarahkan bahwa sebelumnya telah ada kasus yang hampir sama, dengan harapan apabila Hakim mau mempertimbangkannya maka hukuman terhadap Terdakwa akan lebih ringan, namun saat itu hakim menyatakan mempunyai otoritas diluar keputusan tersebut sehingga putusannya berbeda tajam dengan kasus Danny Firmansayah, dan hal tersebut menjadi kekhawatiran tersendiri bagi Responden karena masyarakat akan mempertanyakan dimana letak keadilan.

Menurut Responden peranan penyidik di unit cyber crime lebih baik knowledge dibanding dengan penyidik yang lain, karena Responden pernah berhubungan di Polsek dan dia menanyakan apa itu litigasi, dimana tentu saja sumber daya tersebut sangat mencemaskan untuk level seorang penyidik yang sudah lima tahun bekerja. Peranan penyidik sendiri dalam kasus ini adalah penyidik harus membuktikan unsur-unsur dari tindak pidana tersebut kepengadilan dimana yang dia lakukan pertama adalah menggunakan saksi ahli kedua merubah bukti-bukti yang digital itu menjadi bukti-bukti tertulis maka dilakukanlah proses penjelasan secara verbal. Menurut Responden untuk hal yang sangat high-tech ini penjelasan secara verbal tidak cukup, diperlukan bantuan visual, apa lagi mengingat Jaksa dan Hakim atau pun pengacaranya belum tentu memahami apa yang dia katakan karena terlalu banyak bahasa-bahasa yang berbau teknologi yang familiar bagi penyidik tapi tidak bagi hakim atau jaksanya. Dengan demikian penyidik perlu secara proaktif melakukan training kepada jaksa dan hakim sehingga mereka lebih memahaminya karena apabila hakim atau jaksa bertanya email itu apa didepan khalayak ramai, maka hal tersebut akan menjadi lucu, karena hal tersebut sudah familiar didalam dunia pengacara tapi masih jarang bagi mereka.

Menurut Responden Internet sangat berguna baginya karena memudahkan dalam melakukan pekerjaannya karena bisa tanya jawab langsung dengan kliennya seperti sms, kemudian bisa browsing beberapa peraturan yang tersedia untuk public secara online diantaranya ada homepagenya PSHK, legalitas dimana dalam situs tersebut bisa dilakukan browsing untuk mencari peraturan serta update berita-berita tertentu.

Menurut Responden penanganan kasus hacking yang dilakukan oleh unit cyber crime tidak terdapat suatu kesalahan karena pertanyaan yang diajukan oleh penyidik kepada Tersangka cukup jelas kemudian dalam memberikan kesaksian di Pengadilan juga Responden tidak menemukan sesuatu yang kesalahan yang fatal yang bisa menimbulkan argument dari pengacara. Sepengetahuan Responden para penyidik yang menangani kasus tersebut adalah Edy Hartono, Zamri, Dicky kemudian Ketut terus ada beberapa orang dari lab forensic dan dipimpin oleh Bapak Petrus Golose.

Terhadap kemampuan penyidik dalam penanganan kasus hacking tersebut menurut Responden sudah cukup baik karena kalau dilihat dari cara dia bertanya kemudian memberikan kesaksian dia menguasai bahkan dia bisa menceritakan kronologisnya dengan cukup baik dimulai dari sebelum dilakukan perubahannya website partai golkar yaitu adanya upaya-upaya attack yaitu upaya hacker untuk memasuki suatu system dipartai golkar tersebut dan itu berkali-kali dimana tidak hanya Tersangka yang melakukannya namun ada beberapa orang yang melakukan pengrusakan dan itu bisa dijelaskan oleh penyidik. Namun menurut Responden kelemahan dari penyidik adalah tidak konsisten dalam berkas acaranya untuk mencatat berapa hari Tersangka melakukan perbuatannya, yaitu apakah 4 hari atau 5 hari sedangkan dalam kejahatan konvensional hari-hari dimana pelaku melakukan tersebut sangat penting.

Responden tidak keberatan dengan pasal yang didakwakan kepada Tersangka yaitu pasal 22 huruf b dan c undang-undang telekomunikasi karena didalam kasus hacking website tersebut, partai golkar memiliki cukup bukti mulai dari hard disknya partai golkar kemudian ada log file yang membuktikan masuknya Tersangka ke sistemnya partai golkar kemudian ada juga bukti berupa laptop milik Tersangka sendiri. Namun dalam kasus tersebut terdapat kelemahan mengenai buktinya sebagai contoh mengenai kerusakan program website partai golkar menurut Responden ada hal yang aneh karena sebenarnya hard disk program yang didalam itu tidak rusak karena providernya sendiri mengaku dia mempunyai backup, backup yang bisa memperbaiki websitenya sebelum terjadi larangan tapi itu tetap di ajukan sebagai bukti adanya kerusakan website golkar dan bukan programnya yang ditunjukkan tapi hard disk-hard diskmnya dimana kesannya harddiksnya yang rusak padahal hard disknya tidak rusak tapi programnya. Sehingga memaksakan sesuatu yang seharusnya digital dijadikan kejahatan yang konvensional karena hakim dan jaksanya tidak mengerti dan pada saat dijelaskan oleh Responden seakan-akan itu suatu hal yang menyulitkan bagi mereka jadi mereka berusaha lebih memilih untuk menerima sesuatu yang ingible suatu yang berbentuk benda dibanding sesuatu yang berbentuk program sehingga mereka berfikir harddisk program itu berupa kotak hitam yang besi itu. Dengan demikian terdapat miss sliding, miss sliding yang dilakukan penyidik yang dimakan sama Jaksa dan Hakimnya.

Terhadap berkas perkara yang diajukan oleh unit V IT & cyber crime, menurut Responden perlu ada perbaikan-perbaikan dimana seperti yang disebutkan oleh Responden sebelumnya adalah kekonsistenan dalam membuat berkas acara perkara, namun secara keseluruhan menurut Responden kemampuan dari penyidik sudah cukup bagus diatas rata-rata. Namun menurut Responden penyidik terbentur kendala aturan mengenai digital evidence jadi performance mereka akhirnya memaksakan hal-hal yang tidak seharusnya berupa digital dipaksakan sebagai bukti kejahatan konvensional biasa. Namun bagaimanapun juga seharusnya hal tersebut tidak dapat dilakukan.

Menurut Responden hal-hal yang perlu diperbaiki dalam penanganan kasus hacking adalah apabila kejahatannya diancam dengan hukuman diatas lima tahun lebih baik didampingi oleh Pengacara sejak awal.

Identitas

Nama	: Bpk. F.I
Pangkat	:
Bagian	:
Umur	:
Status	:
Pendidikan	:

Narasi

Responden tertarik dengan IT sejak komputer disketnya masih bolak balik yaitu tahun 1991. Menurut Responden pada tahun 1991 Responden orang pertama yang merubah sistim pendapatan asli daerah Propinsi Irian Jaya dari sistimnya AS 400 IBM ke PC Program netwell. Sampai saat ini Responden tetap konsisten dibidang IT. Responden merupakan salah satu anggota dari partai golkar dengan jabatan Sekretaris Badan Informasi Komunikasi Pengurus Pusat Partai Golkar. Responden aktif di partai sejak tahun 1995. sedangkan mulai bergabung di PPBIK sejak tahun 2004 dimana ketua umumnya Yusuf Kalla. Fasilitas komputer yang selama ini sering digunakan Responden adalah laptop, sedangkan ditempat tinggalnya sendiri Responden mnegunakan jaringan WIFI memakai Speedy, begitu juga dikantornya memakai jaringan speedy, sedangkan apabila sedang berjalan Responden menggunakan jaringan Fren dimana kegunaannya untuk bekerja, untuk studi, untuk keperluan partai, dan hampir untuk semua aspek kehidupan, bahkan membuat janjipun dengan menggunakan internet.

Responden menjelaskan mengetahui kejahatan komputer karena merupakan salah satu pelaku dari komputer, dimana Responden mengetahui bahwa dalam computer dapat melakukan suatu kejahatan. Menurut Responden apabila ingin mencari tau lebih banyak mengenai kejahatan komputer adalah melalui internet karena didalam internet itu sendiri para pelaku kejahatan komputer punya milis-milis baik dari yang masih dipakai pemula sampai yang sudah advance. Menurut Responden hacking sering kali dilakukan tanpa kesadaran pelakunya bahwa perbuatannya tersebut merupakan tindak pidana, mungkin awalnya hanya duduk-duduk didepan komputer, kemudian mencoba-coba membobol situs dan ternyata bisa, selanjutnya membobol situs pribadi, karena orang yang di bobol tersebut tidak bisa marah lama-lama selanjutnya Pelaku menipu di kartu fraud seperti yang dilakukan mahasiswa-mahasiswa.

Responden menganalogikan Hacking sebagai perompak. Perompak adalah seseorang yang merebut kapal yaitu orang yang mengambil bukan haknya, menyusup yang bukan haknya, merusak yang bukan haknya. Menurut Responden pelaku hacking

awalnya seperti latihan, namun tujuannya tetap uang yaitu bagaimana mendapatkan keuntungan financial.
Menurut Responden kejahatan komputer mempunyai dua faktor yaitu adanya keinginan dan yang kedua ada kesempatan. Apabila pelaku sudah berniat untuk melakukan kejahatannya maka hal itu sudah 50% tercipta dan kemudian si Pelaku melihat kesempatan maka sudah tercipta suatu kejahatan. Dengan demikian menurut Responden yang bisa dilakukan saat ini adalah pihak-pihak yang berkecimpung di dunia komputer memanfaatkan fungsi komputer karena sudah sepantasnya mengetahui bagaimana cara melindungi komputer tersebut dari kejahatan orang lain karena rang-orang seringkali lalai untuk melindungi komputernya dia hanya bisa pakai tapi tidak memikirkan kalau datanya bisa dicuri dan dirusak oleh orang lain.

Responden tidak pernah mengikuti pelatihan atau pembekalan mengenai kejahatan komputer. Sedangkan mengenai hacking sendiri Responden sering berdiskusi secara informal tetapi bukan dalam suatu forum yang formal karena menurut Responden tidak tertarik untuk menghacking.

Responden memiliki situs pribadi dan juga situs organisasi. Situs organisasi yang saat ini diikuti oleh Responden pernah menjadi korban dari kejahatan hacking. Responden dipercaya untuk membuat pengamanan-pengamanan terhadap website tersebut, namun ternyata pengamanan tersebut tidak cukup yang akhirnya situs partai golkar tersebut dapat dibobol oleh Pelaku. Tindakan yang dilakukan oleh Responden terhadap kejadian tersebut adalah menganalisis kelemahan untuk segera dicarikan penangkalnya karena teamnya tidak mau masuk kelobang yang sama dua kali, cukup satu kali saja sehingga sistim pengamanannya diperkuat lagi. Oleh karena yang dirusak adalah situs sebuah partai yang besar maka menurut Responden dan teamnya hal tersebut perlu ditindaklanjuti dengan melaporkannya kepada pihak yang berwajib selain itu Responden mendengar bahwa Kepolisian Republik Indonesia sudah memiliki unit cyber crime. Sehingga Responden melaporkan ke Kepolisian Republik Indonesia unit cyber crime dibawah bareskrim. Menurut Responden Pemimpin Unit cyber crime memiliki reputasi yang baik sekali, sehingga Responden merasa yakin untuk melaporkannya ke unit cyber crime. Responden mengumpamakan apabila dalam sebuah restoran diketahui bahwa kokinya enak maka kita akan masuk ke restoran tersebut.

Menurut Responden selaku korban dari kejahatan hacking, penanganan kasus hacking oleh unit cyber crime adalah serius menanggapi, serta sistematis. Sistematis dalam hal ini adalah unit cyber crime melacaknya secara sistematis dengan menggolongkan asal dari serangan misalnya serangan dari Batam, serangan dari Bandung. Serangan–serangan tersebut dianalisa sehingga hal tersebut cukup efisien terutama stafnya yang outsourcing yang chiness itu. Walaupun tidak banyak bicara tapi dia sistematis memilahnya. Sehingga pihak Golkar tidak sia-sia melaporkannya kepada unit cyber crime. Terhadap proses penanganannya sendiri menurut Responden keberadaan Pelaku masih dapat diketahui karena diinternet itu sendiri dapat diketahui jejaknya,

yaitu rekaman selama pelaku merusak masih tersimpan datanya dikomputer. Oleh karenanya internet website partai golkar sangat membantu kinerja unit cyber crime.

Tindakan-tindakan yang dilakukan oleh Penyidik dalam menangani kasus hacking tersebut adalah Penyidik meminta data-data yang berkaitan dengan pengrusakan tersebut, dan oleh karena situs partai golkar tersebut diletakkan di Web Master maka Penyidik melakukan penyitaan terhadap perangkat kerasnya supaya tidak dilakukan lagi pengrusakan atau dengan kata lain barang tersebut diamankan oleh Penyidik. Responden sangat puas dengan penanganan kasus hacking yang dilakukan oleh unit cyber crime menurut Responden hal tersebut merupakan bentuk penegakan hukum yang nyata karena semua berjalan sempurna, Pelaku dapat ditangkap selanjutnya diadakan pemberkasan, kemudian masuk ke Kejaksaan dan akhirnya diputus oleh Pengadilan.

Menurut Responden Penyidik yang melakukan penyidikan terhadap kasus hacking website partai golkar cukup menguasai bidangnya dengan perbandingan 50-60% namun ada kemauan dari penyidik untuk meningkatkan kemampuannya. Pasal yang digunakan oleh penyidik dalam kasus tersebut adalah menggunakan Undang-undang telekomunikasi dan juga KUHP. Menurut Responden bantuan yang diberikan oleh pihak golkar untuk mengungkap kasus tersebut adalah memberikan bantuan diawal berupa rekaman selama masa-masa yang dicuri yaitu Log filenya selanjutnya sepenuhnya unit cyber crime yang menganalisa.

Menurut Responden fasilitas IT dan laboratorium computer forensic yang dimiliki oleh Mabes Polri saat ini masih kurang, karena Menurut Responden Mabes Polri belum memiliki IP Monitoring yang ditempatkan di simpul-simpul intercens, dimana setiap waktu bisa didownload dari kantor, oleh karenanya Responden menyarankan agar Mabes Polri juga memilikinya karena sangat berguna untuk mengontrol seratus persen terhadap lalu lintas IP yang ada di Indonesia sehingga diperoleh rekaman apapun yang lewat dan apapun yang keluar. Namun demikian hal tersebut sebenarnya tidak dapat dilakukan karena hal tersebut merupakan suatu agains law enforcement.

Menurut Responden setiap kali berurusan dengan Polisi hasilnya selalu memuaskan dan efisien karena tidak ada yang malas-malasan, Responden menyarankan agar hal tersebut tetap dipertahankan.

Mengenai proses pelaporan, Responden menjelaskan bahwa pada saat melaporkan ke polisi tentang adanya pengrusakan terhadap website partai golkar, pelaporannya langsung ditujukan kepada penyidik yang berasal dari cyber crime bukan melalui depan, hal tersebut dilakukan karena mempunyai relasi yang baik dengan unit cyber crime selain itu desk yang jaga di depan belum tentu memahami hal tersebut dan malah menimbulkan masalah karena dia tidak tau laporan apa yang diterima, jadi sebelum berangkat ke kantor Polisi Responden bersama teamnya sudah membahas dimana jangan sampai desknya tidak memahami kasusnya. Menurut Responden tidak

semua orang memahami kasus hacking, bahkan Penasehat hukum golkar sendiripun masih kurang bisa memahaminya. Oleh karenanya partai gokar mengadakan seminar untuk menambah pengetahuan mengenai hacking dan saat ini sudah dibuatkan bukunya dan buku tersebut dijadikan acuan di komisi satu DPR

Menurut Responden yang perlu diperbaiki lagi dalam penangan kasus hacking baik dilihat dari segi Penyidik, Pembela, Jaksa Penuntut Umum maupun Hakim adalah dari segi Penyidiknya sendiri sudah baik, kwalitas dari Jaksanya sendiri sudah cukup memahami walaupun belum memahami seratus persen tapi sudah mengarah, dari segi hakimnya sendiri tidak menganggap hal tersebut sebagai makhluk aneh dimana hakim juga bisa memahaminya. Menurut Responden saat ini yang perlu ditingkatkan adalah kwantitasnya, karena apabila dalam waktu bersamaan terdapat kasus yang sama maka akan kewalahan untuk menanganinya.

Identitas

Nama	: Bpk. EH
Pangkat	: AKBP
Bagian	: Unit V IT & Cybercrime
Umur	: 41
Status	: Menikah
Pendidikan	: SD 1977
	SMP 1983
	SMA 1986
	Akabri 1987

Narasi

Responden sudah hampir 14 tahun menjadi Polisi tapi sebagai Penyidik sendiri baru sekitar lima tahunan. Sebelum menjadi Penyidik Responden bertugas sebagai Kapolsek dan Wakapolres. Kasus-kasus yang ditangani oleh Penyidik selama ini kebanyakan tindak pidana umum seperti perampokan, pencurian, penipuan, penggelapan yang sifatnya masuk kategori Rerserse umum.

Responden mengikuti pendidikan Akademi kepolisian, kemudian Pendidikan Tinggi Ilmu Kepolisian Sespim, selanjutnya mengikuti spesialis kejuruan yaitu kejuruan perwira struktur Reserse di Mega Mendung selanjutnya mengikuti seminar-seminar yang dilaksanakan pada saat tugas dicyber crime yaitu seminar tentang cyber crime baik di Indonesia maupun diluar negeri sekitar tahun 2006.

Responden pernah mengikuti Pelatihan yang diadakan oleh Microsoft di Redmount tentang botnet pada awal tahun 2007 selama dua minggu, kemudian di Bangkok pada bulan Maret dan Agustus tahun 2006 tentang kejahatan cyber crime. Terhadap Hacking sendiri secara spesifik Responden belum pernah mengikutinya tapi secara umum cyber crime sudah pernah diikuti.

Menurut Responden, kejahatan cyber crime ini merupakan hal yang baru bagi Responden karena selama ini Responden hanya menangani kasus yang sifatnya konvensional dan hal ini merupakan pengalaman yang sangat berharga bagi Responden karena sejak lulus dari Espim kemudian masuk ke Bareskrim dan ditempatkan diunit cyber crime, maka sejak itulah Responden merasakan mendapatkan hal baru tentang modus kejahatan khususnya kejahatan didunia cyber.

Menurut Responden pelatihan-pelatihan yang diadakan oleh unit cyber crime tersebut sangat berguna dan sangat membantu dalam pengembangan diri Responden maupun dalam melakukan penyelidikan dan penyidikan kasus cyber crime. Sebagai contoh, Responden menjadi mengerti bagaimana cara melakukan penyelidikan dengan menggunakan tool-tool ataupun alat-alat yang banyak tersedia didalam internet itu sendiri maupun tool yang ada dikantor cyber crime yaitu laboratorium komputer forensik.

Sebagai penyidik di unit cyber crime, Responden merasa sangat tertantang untuk mengetahui bagaimana kejahatan komputer, karena kedepan menurut Responden cyber crime berpotensi cukup tinggi di Indonesia, hal itu dirasakan oleh Responden setelah tim unit cyber crime berhasil mengungkap kasus cyber hacking di Batam, semenjak kejadian tersebut Responden sangat tertantang ingin mendalami bagaimana hacker melakukan modus kejahatannya, dengan cara online di internet, membaca buku-buku, serta browsing di internet. Terhadap kejahatan hacking sendiri Responden mengetahuinya berdasarkan informasi yang diterima selama bertugas di unit cyber crime.

Responden mencari tahu sendiri mengenai kejahatan komputer dengan mengikuti seminar maupun training yang di adakan di Bangkok maupun di Amerika, dimana hal itu djadikan oleh Responden sebagai landasan untuk sumber informasi dalam mencari informasi berkaitan dengan kejahatan komputer. Mengenai hacking sendiri Responden mencari tahu dengan cara membaca-baca literatur dari internet maupun dari buku-buku, selanjutnya menanyakan langsung kepada pelaku-pelaku yang sudah tertangkap, dimana Responden mencoba sharing dengan pelaku untuk bahan informasi bagi responden untuk pengembangan diri dibidang penyidikan.

Responden belum pernah melakukan penelitian mengenai kejahatan komputer maupun mengenai hacking, karena menurut Responden tidak mempunyai cukup waktu untuk melakukannya, dan selama ini banyak bertugas di luar Jawa, yaitu di Gorontalo kemudian Sulawesi.

Kasus-kasus yang pernah ditangani oleh Responden yang bersifat spesialis sejak bergabung dengan cyber crime adalah kejahatan penipuan lewat komputer dalam hal ini jaringan dalam internet, perjudian, kemudian hacking dan juga masalah cyber terorism.

Defenisi mengenai cyber crime diatur dalam berbagai sumber. Responden sendiri sependapat dengan defenisi cyber crime yang diatur dalam *convention on cyber crime* di Budapest 2001 bahwa yang termasuk penyidikan cyber crime yaitu computer crime dan computer cyber crime baik kejahatan komputer dan kejahatan yang berhubungan dengan komputer, selain itu Responden juga sependapat dengan yang dianalogikan oleh Kanit cyber crime bahwa cyber crime adalah kejahatan yang melawan hukum yang menggunakan komputer maupun internet sehingga komputer dijadikan subjek maupun objek tindak pidana. Sedangkan hacking sendiri menurut Responden adalah seseorang yang memasuki akses internet ataupun jaringan tanpa hak atau pun tanpa ijin melakukan perubahan-perubahan maupun untuk mencari informasi tentang website yang ada diinternet.

Responden adalah salah satu Penyidik yang ikut terlibat dalam penyidikan kasus defacing website partai golkar. Dalam menangani kasus defacing website partai golkar tersebut Responden menjelaskan bahwa setelah menerima laporan dari Pelapor

tahapan diawali dengan pengambilan data dari server yang ada di Telkom yaitu postingnya di gedung cyber kemudian hard disk yang ada dicyber itu dianalisa. Dari hasil analisa log file yang ada di hard disk tersebut ditentukan pola serangan yang ada di log file tersebut, kemudian direcovery di laboratorium forensik, selanjutnya dipetakan karena terdapat beberapa serangan terhadap website partai golkar tersebut, selanjutnya setelah dipetakan barulah diurut melalui inspidati, karena didalam log file tersebut dapat tergambar dengan jelas real timenya kapan, hacknya kapan diserangnya, melalui mana, ke ISP mana.
Terhadap mekanisme pelaporan sendiri Responden menjelaskan bahwa Pelapor melaporkan kronologis kejadiannya kepada unit cyber crime, yang diterima di Siaga kemudian pihak Penyidik membantu dalam hal menguraikan kejadian ataupun modusnya, setelah itu disusun rencana penyidikan, kemudian dibuat surat panggilan kepada pelapor untuk dibuat berita acara sebagai dasar untuk pengembangan kasusnya, dan berdasarkan keterangan dari pelapor tersebut penyidik meminta bukti-bukti awal kejahatannya, dalam kasus ini bukti awalnya adalah data yang ada di log file website partai golkar tersebut. dan menurut Responden pada prinsipnya berdasarkan berita acara tersebutlah ditentukan mulai dari mana harus melakukan penyidikan.

Dalam hal penyitaan sendiri menurut Responden terdapat dua pandangan, yaitu menurut Penyidik sendiri apabila berkaitan dengan kepentingan umum atau public maka harus dilakukan penyitaan, dimana memerlukan posisi magine, namun karena urutan-urutannya belum ada ataupun belum ada ketentuan yang pasti, Penyidik melakukan inovasi ataupun mengendap berdasarkan beberapa pelajaran yang diterima oleh para Penyidik pada saat pelatihan cyber crime, maka Penyidik melakukan imagine terhadap hard disk tersebut melalui tools-tools yang ada di laboratorium forensik untuk dianalisa. Selanjutnya diajukan penetapan ke pengadilan untuk dijadikan sebagai barang bukti dengan dilampiri berita acara pemeriksaan dilaboratorium forensik.

Penangkapan dilakukan setelah menganalisa log file, dimana berdasarkan log file tersebut diketahui serangan yang paling banyak adalah berasal dari Batam sehingga diputuskan untuk berangkat ke Batam. Setelah tiba di Batam dilakukan pemeriksaan terhadap ISP untuk mengecek IP address yang ada di log file dan juga untuk mengetahui log filenya milik siapa, karena dari sari log file tersebut dapat diketahui IP yang di share kepada warnet mana misalnya ISP tersebut disewakan.

Menurut Responden pada saat itu teamnya mengalami kesulitan, karena hacker menggunakan nick name didalam log file tersebut. Nick name adalah nama samaran yang ada didata itu untuk menyerang website partai golkar, karena log file melalui email, maka tim memandu secara konvensional melalui komunitas hacker yang ada di Batam dan dari situ tim berkolaborasi dengan komunitas hacker yang ada di Batam untuk dapat menangkap pelakunya, dimana ada cover divirtual atau penyamaran melalui penyamaran chatting email terhadap nick name tadi. Setelah diketahui IP-nya atau emailnya melalui informasi dari komunitas hacker tersebut maka di pancing-

pancing melalui email, penyidik berkomunikasi lewat email dan kebetulan dia mengakui didalam chating email tersebut, bahwa betul dia yang pernah menghacking website partai golkar.

Menurut Responden secara umum dalam setiap penyidikan terdapat beberapa kesulitan dalam hal pemberkasan, dalam kasus hacking website golkar sendiri Responden mengalami kesulitan dalam hal Pasal, karena Pasal di undang-undang hanya menggunakan pasal KUHP dan undang-undang spesialis yaitu undang-undang No 36 tahun 1999 tentang Telekomunikasi sebagaimana diatur pada Pasal 22 huruf b dan c dimana dalam undang-undang tersebut dikatakan bahwa mengakses tanpa hak jaringan telekomunikasi....., dimana defenisi jaringan telekomunikasi adalah jaringan telekomunikasi khusus yaitu HT, namun berdasarkan hasil diskusi dengan Jaksa dan Saksi Ahli, akhirnya diinterpretasikan bahwa jaringan yang dimaksud adalah termasuk jaringan internet sebagaimana diatur dalam Pasal 22 huruf b Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi dan Pasal 406 KUHP tentang Pengrusakan. Selain masalah penerapan pasal, terdapat masalah lain yaitu mengenai barang bukti digital, karena dalam sistem hukum Indonesia sendiri belum familiar dengan barang bukti digital sehingga Jaksa sendiri masih bingung, ini bentuknya seperti, apa ini, apakah ini benar hasil dari pada server atau log file yang di hard disknya server partai golkar.

Menurut Responden terdapat masalah dalam hal segi pemenuhan hukum acara, namun dengan adanya diskusi dengan Jaksa dan Saksi Ahli sehingga tidak ditemukan kesulitan dalam hal penetapan pasalnya.

Menurut Responden seharusnya pengaturan alat bukti sebagaimana diatur dalam Pasal 184 KUHAP dapat mengakomodasi mengenai barang bukti digital.

Menurut Responden manajemen penyidikan adalah sesuai dengan teorinya yaitu mengenai Perencanaan, Pengorganisasian, Pelaksanaan dan Pengendalian. Menurut Responden Manajemen penyidikan sangat penting dan harus diterapkan karena jika tidak diterapkan maka tahapan-tahapan dalam penyidikan tidak akan fokus sehingga progresnnya tidak akan terlihat. Dalam kasus hacking website golkar sendiri Manajemen Penyidikan tersebut telah diterapkan. Sebagai contoh pada saat menerima laporan, Penyidik harus membuat rencana penyidikan, dimana rencana penyidikan tersebut dilaporkan kepada pimpinan unit cyber crime yaitu Kanit. Dalam perencanaan tersebut ditentukan apa berbuat apa, bertanggung kepada siapa, kemudian tahapan kegiatannya apa yang pertama dilakukan, sehingga kanit secara berkala dapat memberikan arahan dan petunjuk supaya progress ini bisa dipercepat sehingga mencapai hasil untuk pegangan kasus.

Terhadap masalah sumber pembiayaan, Responden menyatakan terdapat permasalahan klasik yaitu money matrial, manusia, peralatan. Walaupun dikatakan sekarang sudah diberikan anggaran, namun tidak memadai apalagi untuk menangani kasus seperti hacking website partai golkar, dimana dalam setiap langkah penyidikan

sangat-sangat membutuhkan biaya, sebagai contoh pada saat berangkat keluar daerah untuk mengecek IP, hal tersebut menggunakan internet dan kesemuanya itu adalah membutuhkan biaya.

Dalam Bareskrim sendiri pengaturan mengenai anggaran telah diatur dalam TCK yaitu Hubungan antara kerja antara unit dengan struktural yang ada di Bareskrim sehingga penyidik kalau sebelum menjalankan tugas membuat ren sidik ajukan anggaran, namun yang dialami Responden apabila permohonan diajukan, mungkin turun tapi telah beberapa bulan baru turun itu pun tidak maksimal, dengan alasan bahwa tidak ada anggaran atau tidak tidak ada pos untuk kasus ini, jadi dianggap global seperti kasus-kasus biasa. Anggaran satu kasus tergantung dari klasifikasinya yaitu kasus ringan sedang dan berat, kalau berat satu kasus adalah lima juta, namun Responden tidak mengetahui secara persisnya, menurut Responden pihak yang lebih tahu adalah bagian keuangan.

Menurut Responden pembiayaan terhadap hacking sangat mahal karena setiap langkah pasti membutuhkan biaya, selain itu kasus hacking tidak sama seperti kasus konvensional karena hard disk sendiri sangat mahal.

Menurut Responden hal-hal yang perlu diperbaiki lagi dalam kasus hacking yang pertama adalah manusia dalam hal ini adalah penyidik polri khususnya cyber crime, Penyidik harus memiliki kemampuan, dan harus diadakan pendidikan ataupun pelatihan secara rutin karena walaupun sudah pernah dilatih hal tersebut tidak dapat menjamin bahwa dia telah mampu. Selanjutnya mengenai money, dulu memang dikatakan hal ini merupakan hal yang tabu untuk dibicarakan namun diera sekarang ini harus sangat dan sangat perlu secara proporsional diatur sehingga terjadi percepatan dalam pekembangan kasus sehingga Kanit tidak perlu lagi memikirkan bagaimana sumber biayanya dan idealnya tinggal menggunakan dana lalu berangkat.

Identitas

Nama	: Bpk. IKB
Pangkat	: AKP
Bagian	: Unit Cyber Crime Bareskrim
Umur	: 33 Tahun
Status	: Menikah
Pendidikan	:

- SD 1981-1987 Cimahi
- SMP 1987-1990 Cimahi
- SMA 1990-1993 Magelang
- AKPOL 1996 Semarang
- Univ 17 Agustus 2002 Cirebon
- PTIK 2005 Jakarta

Narasi

Responden sudah hampir 1 tahun 3 atau empat bulan menjadi Penyidik, sebelumnya Responden telah dua kali menjadi Kapolsek

Responden lulus Akademi Kepolisian tahun 1996, tugas pertama ditempatkan di Banten menjabat sebagai Pamapta Res Lebak Banten selama dua atau tiga bulan pada tahun 1998, kemudian karena Responden tidak mengurusnya serta pada saat itu Responden masih mencari bentuk kemudian Responden dipindah ke Cirebon menjabat sebagai KBD Lantas Res Cirebon pada tahun 2001, kemudian dipindah lagi ke Purwakarta menjabat sebagai Kasatlantas, selanjutnya Responden pindah ke Bandung Tengah menjadi Kapolsek Cibeunying Kidul Resta Bandung Tengah pada tahun 2002, kemudian pada tahun 2003 Responden menjabat sebagai Kapolsekta di daerah Lengkong Bandung Tengah, selanjutnya pada tahun 2004 Responden pindah ke Polda Jawa Barat di bagian Tindak pidana korupsi (Tipikor).

Selanjutnya pada tahun 2004 Responden masuk pendidikan PTIK kemudian Responden berkompetisi untuk mencari jurusan di Reserse, yang akhirnya Responden masuk kejurusan Gakum. Responden sangat bangga dengan jurusannya dan mendapat nilai yang cukup bagus, namun ada sedikit kekecewaan yang dirasakan oleh Responden karena Responden telah belajar dengan sepenuh hati dan bekerja keras akan tetapi di tempatkan di Papua yaitu pada bagian Kasubag Ren Ops di Polda papua. Kemudian pada saat bertugas di Papua ada kesempatan untuk mendaftar yang akhirnya Responden diterima di Bareskrim kebetulan Responden masuk di unit cyber crime sehingga menjadi Penyidik yang spesialis dirasakan oleh Responden adalah setelah masuk di Mabes Polri dan bergabung dengan unit cyber crime.

Tindak Pidana yang pernah ditangani oleh Responden adalah Tindak Pidana Umum dan Tindak Pidana tertentu, selain itu Responden juga sudah pernah menangani kasus

cyber crime yaitu pada saat menjabat sebagai Kapolsek namun saat itu menurut Responden levelnya masih rendah yaitu kardig, dimana korbannya waktu itu berasal dari Belanda dan Finlandia, saat itu Responden mendapatkan barang buktinya berupa tenda alat tato, mainan-mainan dan lain-lain. Saat itu Responden dibantu dan dibackup oleh Kanit cyber dari Mabes yaitu Pak Brata Mandala dan kasus itu vonis sampai P 21.

Kasus lain yang pernah ditangani oleh Responden adalah tentang penyalahgunaan kartu kredit, dimana Responden sudah tiga kali mengungkapnya, menurut Responden kejahatan kartu kredit bukanlah kejahatan cyber crime karena berdasarkan pengamatan Responden cara pembuatannya dengan computer adalah berbeda dimana kartu kredit dijual dan diisi oleh mesin yang harganya menjadi dua kali lipat dengan menggunakan computer.

Pelatihan-pelatihan mengenai kejahatan computer yang pernah diikuti oleh Responden adalah pelatihan berupa seminar pada tahun 2003, pelatihan dengan FBI di Hilton tentang *weapon mess destruction* kemudian pelatihan di Mabes terutama cyber crime, selanjutnya di Singapura work shop selama tiga hari- dua hari, kemudian pelatihan di BNN tentang *Iarsi insdent respond* kurs, pelatihan di Manila tentang *computer fasilitate crime* dan juga pernah mengikuti pelatihan di Bali yaitu yang berkaitan dengan kejahatan anak-anak atau CADS yaitu kejahatan crime terhadap anak-anak.

Responden sudah pernah mengikuti Pembekalan tentang kejahatan computer, namun tidak secara spesifik, karena hanya dijelaskan secara umum saja, misalnya teknik-teknik bagaimana cara mengungkapnya, apa yang harus kita lakukan dalam melakukan pengungkapan perkaranya atau searching-searchingnya.

Mengenai hacking sendiri Responden belum pernah mengikuti pelatihan secara khusus akan tetapi diberikan dasar-dasarnya yaitu di Bali dimana yang melatih waktu itu TJ Campano dari Microsoft. Selain itu Responden juga sudah pernah mengikuti Pelatihan di Amerika tentang botnet, dimana dalam pelatihan tersebut dijelaskan bagaimana metodenya. Akan tetapi menurut Responden pada saat itu tidak dapat menyerap semuanya karena waktunya yang terlalu singkat.

Responden sangat suka mencari tau tentang kejahatan komputer. Adapun cara yang digunakan Responden untuk mengetahuiya adalah dengan dua cara yaitu membaca buku-buku tentang hacker salah satunya karangan dari Seto tentang hacker dimana buku tersebut adalah buku milik temannya, akan tetapi Responden kurang tertarik dengan buku tersebut karena Responden belum menguasai kejahatan komputer, akhirnya Responden hanya secara sepintas membacanya kemudian dengan cara yang kedua yaitu mencari informasi diinternet terutama di websitenya jasa comp.

Terhadap hacking sendiri Responden belum pernah mempelajarinya, akan tetapi Responden sudah pernah mencari tahu pada saat itu di Bandung tahun 2003, dimana

waktu itu ada buku muapan kemudian Kapolresnya mendorong Responden menemukan hacker untuk berbicara tentang segala macam tentang hacker akan tetapi pada saat itu Responden belum spesifik mempelajarinya, hanya untuk mencari tau saja.

Responden mencari tau tentang hacking melalui media internet, sebenarnya di unit cyber crime tidak ada yang mengajari tetapi menurut Responden apabila membuka situs-situs jasa comp sudah banyak informasi yang didapat. Responden tidak hanya membaca yang berkaitan dengan kebaikan akan tetapi juga yang kejahatan karena dalam situs tersebut terdapat juga bagaimana mencari kartu kredit orang, bagaimana cara mencari password snip snup dan lain sebagainya, tapi Responden sendiri tidak tertarik dengan hal-hal tersebut tapi hanya ingin tau aja.

Terhadap pencarian Responden mengenai hacking masih terbatas melalui internet dan belum langsung keorangnya. Responden belum pernah melakukan penelitian baik mengenai kejahatan komputer maupun mengenai hacking, dengan alasan setelah Responden memiliki dasar-dasar yang kuat, maka Responden akan melakukan penelitian.

Pengaturan mengenai cyber crime banyak terdapat dalam berbagai teori-teori ataupun kongres PBB, namun menurut Responden cyber crime adalah suatu kejahatan yang didalam dunia ataupun dunia maya yang tidak terlihat jadi kejahatan itu dengan menggunakan media computer dengan aksesnya dijaringan internet itu. Sedangkan hacking menurut Responden banyak orang yang mendefinisikannya sebagai hacker, ada cracker, ada playker, dimana keseluruhannya itu menurut Responden adalah termasuk kegiatan hacking dimana Pelaku mencari tau kelemahan orang, mencari tau kelemahan system keamanannya, kemudian dia juga berusaha untuk mencuri passwordnya.

Responden sudah pernah menangani kasus hacking yaitu defacing website partai golkar di Batam, dimana peranan Responden pada saat itu melakukan pemeriksaan kepada saksi-saksi. Responden menjelaskan pada saat menangani kasus tersebut terdiri dari dua tim yaitu tim penyidik dan tim laboratorium. Pada saat itu menurut Responden mereka bekerja sesuai data yang dimiliki oleh laboratorium, Responden tidak tahu cara kerja laboratorium akan tetapi tim laboratorium menyerahkan ke tim Penyidik datanya untuk dibuktikan. Selanjutnya berangkat ke Batam menemui PT Inforsys kemudian melakukan pemeriksaan terhadap data yang ada di log file, kemudian orang itu diperiksa dan ditanyakan IP tersebut milik siapa kemudian dia menunjukkan ini adalah milik suatu warnet dan IP ini sebetulnya sudah tidak digunakan kemudian penyidik melakukan penyidikan disitu.

Menurut Responden pada saat menangani kasus hacking website partai golkar terdapat kesulitan dalam pemenuhan unsur-unsur tindak pidana, dimana ada sedikit hambatan dengan Jaksa, dimana Jaksa yang menangani kasus tersebut menyampaikan bahwa baru pertama kali ini menangani kasus cyber crime dan sebelumnya dia belum

pernah menanganinya kemudian tentang masalah pembuktian di lokasi atau dilocusnya di (Tempat kejadian Perkara) TKP-nya karena dalam kasus golkar, lokasi korbannya banyak di Jakarta tapi dari Jaksanya menyarankan supaya persidangan di Batam itu yang jadi masalah karena dia mempermasalahkan ini TKP-nya dimana, tolong dicari dasar hukumnya justru itu juga yang membalikkan penyidik dimana dalam hal ini penyidik meminta bantuan Jaksa untuk mencari dasar hukumnya, TKP-nya dimana supaya bisa disidangkan kemudian yang berikutnya di Kejaksaan pun dipermasalahkan tentang barang buktinya ini barang bukti begini apa yang bisa dibuktikan saya gak berani, yang lain juga tidak berani jadi seperti seolah-olah dilemparkan keinstansi lain.

Menurut Responden terhadap pengaturan tindak pidana hacking yang pertama harus diperhatikan adalah system kinerja dimana seharusnya Polisi, Jaksa maupun Hakim harus bersama-sama satu rel, satu kesepahaman tentang kasus ini karena ini memang cyber crime jarang sekali terjadi dan mereka belum pernah menangani masalah ini, dimana menurut Responden apabila terdapat kasus cyber crime maka Jaksa maupun Hakim akan meminta dasar hukumnya, yang kedua adalah tentang payung hukum terhadap kasus cyber crime, dimana menurut Responden saat ini sedang dalam tahap pembahasan di Dewan Perwakilan Rakyat (DPR).

Terhadap pemenuhan hukum acara sendiri menurut Responden terdapat kesulitan misalnya pencurian data informasi melalui komputer dimana penyidik harus bisa membuktikan apakah yang dicuri data itu sudah termasuk pengrusakan karena istilah pengrusakan di KUHP sesuatu barang yang sudah tidak bisa digunakan kembali, sedangkan data itu bisa diambil dengan menggunakan alat yang ada diforensik dan data itu bisa timbul kembali, kok data ini sudah hilang tapi bisa timbul kembali apakah data itu yang disebut rusak itu yang masih menjadi kontra.

Dengan demikian Responden menyarankan agar KUHP tidak perlu dirubah akan tetapi dibuat undang-undang yang lebih spesialis karena negara kita menganut azas lex spesialis derogate lex generalis, jadi kita perlu bikin undang-undang yang khusus tentang cyber crime supaya penanganan-penanganan perkaranya lebih terakomodir.

Menurut Responden Manajemen adalah keseluruhan tindakan yang dilakukan oleh seseorang, dimana dalam hal ini pemimpin berperan untuk menggerakkan anak buahnya, mengorganisasikan kelompoknya untuk mencapai suatu tujuan yang diharapkan dan diterapkan oleh kelompok nya itu secara bersama-sama. Kegiatan-kegiatan yang termasuk dalam manajemen adalah perencanaan, pengorganisasian, pelaksanaan dan pengendalian sebagai evaluasi.

Menurut Responden Manajemen tersebut dapat diterapkan dalam kasus hacking, yaitu terdapat dalam point pertama mengenai perencanaan dimana sebelum melakukan kegiatan harus direncanakan dulu siapa yang menyidik, siapa yang menyelidiki kemudian nanti siapa yang akan bergerak sebagai informan dan lain-lain

kemudian didalam pengorganisasian juga harus dibentuk tim yang menanganinya berikut juga dengan pada saat pelaksanaannya dan pengendaliannya.

Dalam penanganan kasus defacing website partai golkar sendiri menurut Responden Manajemen tersebut sudah diterapkan walaupun belum 100% dilaksanakan dengan baik mengapa demikian? karena pada saat perencanaan tidak semua penyidik mengetahui kasus tersebut, Responden sendiri hanya mengetahui setengah-setengah, dimana seharusnya pada saat itu, seluruh penyidik dikumpulkan dan dijelaskan bagaimana kasusnya jadi dalam perencanaan semua harus disampaikan kemudian pada saat pelaksanaan dalam hacking website golkar seharusnya yang bergerak adalah tim yang benar-benar solid yang sudah mengetahui secara pasti, menurut Responden masih terdapat kekurangan pada saat menangkap pelakunya karena penyidik masih menggunakan hacker atau pun orang lain padahal seharusnya penyidik sendiri yang melakukan informan.

Terhadap pembiayaan kasus hacking menurut Responden adalah relative, belum tentu cukup besar ataupun kecil tapi relative, apabila pelaku masih di Jakarta maka masih dapat terjangkau, tapi apabila Pelaku berada di luar kota maka memerlukan anggaran khusus untuk menanganinya ataupun di luar negeri maka membutuhkan biaya yang cukup besar, yaitu untuk biaya tiket, untuk hotel akomodasi dan lain-lain tapi kalau untuk didalam negeri menurut Responden masih cukup. Terhadap masalah anggaran sendiri menurut Responden masih kurang.

Menurut Responden hal-hal mendasar yang perlu diperbaiki dalam penerapan manajemen adalah di bidang perencanaan, dimana apabila membicarakan tentang manajer, yang paling mendasar adalah perencanaan karena itu memang bentuk alas dasarnya dia berdiri, selama ini menurut Responden manajemennya masih kurang karena timnya banyak ataupun masih kurangnya pengetahuan penyidik tentang kasus hacking, oleh karenanya dalam hal perencanaan pembagian tugasnya juga masih secara umum saja belum spesifik tapi kalau sudah sangat spesifik misalnya si A harus berbuat apa mencari kemana hubungi siapa bagaimana cara mengambilnya, bagaimana cara membuktikannya maka akan lebih baik sehingga menurut Responden yang paling lemah selama ini adalah dalam hal perencanaan sedangkan dalam pelaksanaan sudah baik.

Selain itu menurut Responden terdapat kelemahan dalam hal berkomunikasi, karena tidak terdapat komunikasi yang intensif dengan orang-orang yang memiliki kemampuan di bidang hacking, apabila dianalogikan Responden menggambarkannya bahwa setiap kepolisian di dunia dalam mengungkap perkara dia menggunakan agen, agen itu mungkin secara umum bisa dibahasakan informan, selama ini para penyidik bekerja dikantor dan tidak mungkin ataupun tidak ada kesempatan ataupun tidak ada tidak ada channel untuk bisa bersentuhan langsung dengan orang yang memiliki kemampuan dibidang hacking, karena pada dasarnya hacker itu tidak selalu jahat tapi juga ada yang baik dia hanya ingin tahu sistemnya bagaimana dan tidak merusak.

Maka menurut Responden apabila penyidik memiliki kemampuan tersebut maka akan menjadi kekuatan yang luar biasa.

Selanjutnya menurut Responden yang perlu dibenahi lagi adalah dari penyidiknya sendiri karena kemampuannya masih terbatas, dimana dibidang hubungan keluar penyidik masih berputar di dalam maka untuk hubungan keluar harus ada orang yang mengajak untuk keluar, dikenalkan dengan orang yang memiliki kemampuan dan dia memiliki akses. Selain itu juga pada saat memimpin sebaiknya ada regenerasi misalnya seandainya Kanit pindah maka anggotanya tidak stak, Responden merasa khawatir, apabila ada seorang miliki kemampuan leadership sangat bagus misalnya kanit komandannya bagus begitu ada perubahan karena tidak selamanya menjabat pindah itu akan terjadi stak karena anggota penyidik-penyidik lain belum bisa menjembataninya tapi kalau diajak dan dikenalkan dengan pihak-pihak luar maka anggotanya akan bisa melanjutkannya.

Selain itu menurut Responden dalam bidang Penyidikan diperlukan pelatihan-pelatihan secara khusus untuk masalah hacking, karena menurut Responden selama ini pengetahuan Penyidik hanya terbatas pada hal-hal yang umum saja bahkan terkadang menangani kasus di luar cyber crime. Menurut Responden sebaiknya ada tim khusus yang menangani masalah hacking karena hacking harus dipelajari secara mendasar dan membutuhkan orang yang ahli dibidangnya kalau hanya belajar diinternet tidak akan cukup.

Selanjutnya dalam bidang manajemen, karena manajemen tidak hanya didalam tapi juga keluar, maka harus difasilitasi koordinasi dengan instansi diluar kepolisian, misalnya kejaksaan ataupun hakim ataupun organisasi lain misalnya APJI kemudian provider-provider, kemudian pihak-pihak lain yang pada pokoknya orang-orang yang memiliki akses dibidang telekomunikasi karena memang kebanyakan pelaku kejahatan menggunakan jasa telekomunikasi.

Identitas

Nama	: Bpk. Z
Pangkat	: Kompol
Bagian	: Unit V IT & Cyber Crime Dit II Eksus
Umur	: 37 Tahun
Status	: Menikah
Pendidikan	:

- SD 1982 Jakarta
- SMPN 32 1985 Jakarta
- SMAN 17 1988 Jakarta
- D III PAT Informatika 1992 Jakarta
- S-1 ST Inf & Komputer 1996 Jakarta
- S-2 Hukum Bisnis 2003 Jakarta namun tidak lulus

Narasi

Responden bekerja sebagai penyidik sejak tahun 1997. Sebelum menjadi penyidik Responden beberapa kali diikutkan pada kegiatan-kegiatan penyidikan di Direktorat Reserse Umum diantaranya, sejak tahun 1993-1997 menjabat sebagai Palir Top DSP Dit Personel dimana Responden ikut bekerja membangun system pencarian data kendaraan hilang di satuan reserse umum Polda metro Jaya. Kemudian pada tahun 1997 Responden bertugas sebagai Panit III Perbankan Polda Metro Jaya, selanjutnya pada tahun 1998 Responden bertugas sebagai Kasubnit III Perbankan Polda Metro Jaya, kemudian karir Responden tidak berhenti hanya sampai disitu dimana pada tahun 2000 Responden menjabat sebagai Kasubnit V Perbankan, kemudian pada tahun 2002 bertugas sebagai Penyidik unit III Fismonden Polda Metro Jaya, selanjutnya pada tahun 2004 Responden menjabat sebagai Kasubden Bantuan Datasemen 88 Polda Metro Jaya, selain itu Respoden juga pernah bekerja sebagai Staff pribadi pimpinan dan pernah diikutkan oleh Bapak Petrus Golose dan juga Bapak Goris mengikuti kegiatan penyidikan pembunuhan dinas hutan rimba. Selanjutnya pada dari tahun 2005 sampai dengan saat ini Responden bertugas sebagai Penyidik Muda Dit II Eksus Bareskrim Polri.

Tindak pidana yang pernah ditangani oleh Responden adalah tindak pidana di bidang Perbankan, selain itu Responden juga pernah menangani perkara yang berskala besar yaitu mengenai penyidikan tindak pidana terorisme, selain itu menangani kasus yang berkaitan dengan penyidikan tentang keamanan negara, menangani kasus yang berkaitan dengan penyidikan tentang penggelapan dana negara yang melibatkan KH Abdur Rahman Wahid Presiden Republik Indonesia.

Menurut Responden hampir seluruh kegiatan-kegiatan penyidikan untuk tindak pidana diperbankan terkolerasi dengan komputer namun dalam pelaksanaannya mempergunakan aturan hukum yang ada dipidana umum, namun demikian dalam proses

penyidikannya sesungguhnya banyak kegiatan-kegiatan penyidikan yang terkait dengan kejahatan komputer namun pada saat itu tidak dipergunakan karena mungkin kemampuan penyidik pada saat itu belum semuanya dapat menerimanya sebagai alat bukti jadi penyidik hanya mempergunakannya sebagai petunjuk-petunjuk, namun setelah bergabung dicyber crime ada satu kasus yang pernah ditangani yaitu pengrusakan situs golkar pada saat itu ditemukan pelakunya dan dicoba diterapkan dengan aturan yang baru yaitu pidana khusus disamping dengan pendampingan kejahatan tentang pidana umum tentang pengrusakan jadi menurut Responden penanganan kasus yang pernah ditanganinya yang terkait dengan cyber crime adalah pengrusakan situs website situs atau website partai golkar.

Selanjutnya Responden juga pernah melakukan penyidikan terhadap tindak pidana teroris yang terkait dengan situs www.arshad.net yaitu berkaitan dengan dua tokoh pelaku pemboman di Indonesia yaitu Dr. Azhari dan Nurdin dimana waktu itu pelakunya ditemukan di Semarang dan sudah vonis saat ini. Selain itu tindak pidana yang pernah ditangani oleh Responden adalah tindak pidana tentang pembajakan software milik Microsoft yang melibatkan perusahaan asing yang sudah go public dan cukup besar di Indonesia.

Pelatihan atau pendidikan yang pernah diiukuti oleh Responden selama menjadi Polisi adalah mengikuti pendidikan dasar perwira Reserse Tahun 2001, selanjutnya mengikuti seminar-seminar, diantaranya seminar di luar negeri tentang kartu kredit Visa tahun 2006. Selain itu Responden juga penah mengikuti pelatihan financial terrorism yang ada beberapa keterkaitan dengan kejahatan komputer. Menurut Responden pelatihan-pelatihan tersebut sangat penting dan sangat berguna terutama untuk menambah wawasan, karena wawasan sangat penting dalam melakukan penyidikan agar terstruktur. Selain itu menurut Responden dengan adanya pelatihan Responden menjadi tau betapa pentingnya pengetahuan yang didapatkan atas pelatihan tersebut dan dapat bertemu dengan pihak-pihak dari instansi lain terutama yang terkait dengan criminal justice system.

Responden suka mencari tau sendiri mengenai kejahatan komputer karena latar belakang pendidikan Responden adalah komputer oleh karenanya pada saat kuliah Responden sering berdiskusi dengan teman-temannya membahas tentang kejahatan komputer. Sedangkan mengenai hacking sendiri Responden belum pernah mencari taunya. Responden belum pernah mengadakan penelitian tentang kejahatan komputer karena tidak ada waktu yang cukup untuk melakukannya sehingga tidak ada kesempatan untuk mencari tau. Namun menurut Responden apabila dia akan melakukan penelitian maka dia tidak mau melakukannya setengah-setengah tapi harus total dan dia harus bekerja ditempat yang baru agar mempunyai waktu yang cukup.

Menurut Responden cyber crime adalah segala bentuk kejahatan yang terkait dengan penggunaan alat komputer khususnya komputer yang dipergunakan sebagai media untuk komunikasi. Sedangkan hacking adalah suatu bentuk kejahatan melakukan pembajakan atas sistem yang telah dibuat oleh seseorang atau perusahaan sehingga sistem tersebut

tidak dapat dipergunakan atau terganggu atau si pelakunya mendapatkan keuntungan atau sipelakunya mendapatkan keuntungan atas kegiatan yang dilakukan, sebagai contoh pengrusakan website partai golkar dimana seseorang memasuki satu system jaringan milik orang lain kemudian dengan kemampuan yang dimiliki nya dia melakukan aktivitas yang kemudian membuat jaringan itu tidak dapat dipergunakan atau terganggu.

Menurut Responden proses penanganan dalam kasus hacking website partai golkar bermula dari keterangan yang diperoleh dari korban kemudian dikembangkan oleh sebagian anggota sehingga dilakukan penangkapan terhadap pelaku, kemudian dilakukan penyidikan untuk mendapatkan barang bukti, melakukan pemeriksaan terhadap saksi-saksi untuk dilakukan pemberkasan. Pada saat penyidikan situs partai golkar penyidik bekerjasama dengan tim yang lain dimana sudah dilakukan pembagian tugas saat itu.

Menurut Responden tindakan yang dilakukan setelah proses penangkapan dilakukan adalah melakukan penggeledahan disalah satu warnet yang dipergunakan oleh pelaku dan kemudian dari penggeledahan tersebut dilakukan pengambilan data untuk barang bukti yang kemudian dilakukan pemeriksaan secara laboratories setelah itu dilakukan pemeriksaan terhadap saksi-saksi, selain itu diminta keterangan dari ahli ditambah dengan keterangan tersangka yang menjelaskan bahwa kegiatan hacking yang dia lakukan adalah semata-mata hanya untuk menguji kehandalan system pengamanan situs partai golkar sendiri tidak ada unsur kesengajaan lain.

Selanjutnya dilakukan pemberkasan perkara dimana dalam kasus tersebut dipersangkakan atas dua tindak pidana yaitu melakukan pengrusakan sebagaimana dimaksud pasal 406 KUHP dan undang-undang telekomunikasi yaitu memasuki jaringan komunikasi milik orang lain secara tanpa hak. Atas kasus tersebut telah divonis oleh Majelis Hakim dimana yang diterima hanya pengrusakannya saja.

Menurut Responden dalam penanganan kasus hacking terdapat kesulitan dalam penerapan pasal diantaranya adalah dalam menerapkan pasal dengan fakta-fakta yuridis yang ada. Untuk kasus pengrusakan situs partai golkar, jelas sangat sulit karena salah satu unsure yang disyarati adalah rusaknya barang sehingga tidak dapat dipergunakan. Dalam kejahatan tersebut sama sekali tidak ada barang yang rusak. Selain dengan pasal pengrusakan barang dalam pasal 406 KUHP tersebut penyidik juga mencari format lain bahwa kejahatan yang dilakukan tersangka adalah memasuki jaringan milik orang lain secara melawan hukum. Hal ini pun menjadi kesulitan karena ketika dijelaskan memasuki jaringan milik orang lain ini akan bisa tergambarkan pada hasil pemeriksaan digital evident yang ada oleh laboratorium forensic. Ketika dua pidana ini disandingkan, maka hal tersebut akan menjadi barang baru yang bisa diterima oleh pihak kejaksaan.

Oleh karena dalam hal ini pihak kejaksaan masih bersikeras untuk tidak bisa menerima berkas ini dengan sempurna. Dimana terdapat dua pasal, dalam dua perundang-undangan yang bersanding sama-sama tapi tidak menyentuh kedua-duanya. Kalaupun itu dapat diterima itu harus dengan kemampuan penyidik untuk meyakinkan Jaksa untuk melihat bentuk kejahatan ini adalah sempurna pernah dilakukan atau dalam hal ini kerusakan yang terjadi tidak melulu pada barang, maka penanganan kasus hacking akan

berakhir apabila Jaksa tidak mau menerima pemberkasannya sedangkan yurisprudensi yang ada yang bisa diangkat untuk kejahatan cyber crime belum banyak. Pada akhirnya Responden bersama teamnya menemukan banyak hal terhadap bentuk-bentuk kejahatan cyber crime dalam mengangkat fakta-fakta hukum yang ada dalam bentuk berkas perkara sehingga dapat diterima.

Kesulitan lain yang ditemui oleh Responden dalam penanganan kasus tersebut adalah mengenai barang bukti digital karena pemberlakuan barang bukti digital sendiri sampai saat ini belum ada aturan baku yang mengatur, sebagai contoh ketika barang tersebut diambil dengan cara di image atau di kloning dari sebuah server adalah dalam bentuk hard disc kemudian formatnya dibuatkan hal yang serupa. Saat diangkat, ditetapkan menjadi alat bukti maka perlu ditetapkan apakah dipersamakan dengan barang bukti atau tidak. Apabila dipersamakan maka harus ada ketentuan untuk mendapatkan penetapan, namun demikian data yang diperoleh dari hasil pengangkatan dalam bentuk imaging atau kloning itu bukan merupakan barang bukti yang disyaratkan oleh Hukum Acara Pidana, bukan merupakan alat yang dipergunakan, bukan merupakan alat yang dihasilkan atau alat yang ada hubungannya dengan kejahatan.

Dengan demikian menurut Responden kesulitan mendasar adalah tentang pemberlakuan barang bukti digital. Hal ini sangat mendasar karena seseorang dapat dipersangkakan melakukan tindak pidana apabila jelas-jelas ada alat bukti yang mendukung, diantaranya adalah apa alat bukti yang dipergunakan dan keterangan ahli yang akan terbit dari hasil pemeriksaan.

Responden memandang kondisi saat ini sudah sangat mendesak untuk membuat suatu aturan yang jelas mengenai pengaturan hacking, karena perkembangan peradaban masyarakat komunikasi sudah merupakan sebuah kebutuhan sementara dari komunikasi kata atau komunikasi informasi, dll, itu cenderung akan menjadi suatu penyalahgunaan yang berakhir pada kejahatan. Ketentuan-ketentuan yang ada dalam undang-undang sekarang ini sangat jauh untuk bisa mengatur bentuk-bentuk kejahatan baru dalam format kerangka hukum yang ada. Oleh karenanya Responden menyarankan harus ada ketentuan yang mengatur tentang bagaimana teknis penyidikan yang terkait dengan sesuatu yang berbasis teknologi informasi atau komputer. Selanjutnya apabila sudah ada aturan yang baku, maka yang paling penting adalah orang-orang yang akan mengawakinya. Aturan hukum yang belum ada yang mengatur lebih spesifik sementara orang-orang yang berhadapan dengan hukum itu tersebut sudah harus memiliki kemampuan, terutama kemampuan dibidang teknologi informasi, dia juga harus mempunyai kemampuan dalam bidang penyidikan.

Dari segi pemenuhan hukum acara sendiri menurut Responden tidak ditemui kesulitan secara umum, namun apabila lebih spesifik maka akan ditemui kesulitan terhadap Jaksa Penuntut Umum, terutama memberikan pemahaman karena penyidik tidak mempunyai pemahaman yang sama dengan Jaksa Penuntut Umum.

Menurut Responden apabila aturan mengenai hacking sudah diatur maka format hukum acaranyapun harus disesuaikan dengan jelas agar kejahatan hacking dapat diterima. Saat

ini sudah ada perundang-undangan yang mengatur tentang penanganan digital atau kejahatan yang terkait dengan penggunaan komputer sebagai alat, namun tidak menjelaskan bagaimana teknis acaranya.

Berdasarkan pengalaman Responden, pada saat menjelaskan kepada Jaksa Penuntut Umum mengenai bagaimana menerapkan hukum acara pidana terhadap kasus kejahatan komputer maka penyidik tidak semata-mata lagi murni pada penyidikan tindak pidana yang terkait dengan tindak pidana cyber crime atau masalah hacking tadi. Sebagai contoh pada saat menangani kasus cyber crime horizon, penyidik menjelaskan bagaimana seseorang melakukan aksi terror dengan menerbitkan penayangan sebuah situs yang dianggap berbahaya bagi orang yang dapat mengaksesnya dan situs tersebut dijadikan mediasi untuk menyampaikan kegiatan yang telah dilakukan. Pada saat itu yang digunakan adalah undang-undang terorisme, dimana di dalam undang-undang terorisme pun dijelaskan tentang alat bukti ditambahkan di pasal 27 bahwa alat bukti yang ditambahkan oleh 184 jelas diantaranya data informasi yang disimpan dalam media cakram atau tempat penyimpanan-penyimpanan media elektronik, ketika itu diangkat dari barang bukti digital yang ada kita coba minta untuk ditambahkan sebagai barang bukti selanjutnya memberikan pemahaman kepada Jaksa bahwa barang bukti digital ini adalah barang bukti yang dipergunakan oleh pelaku.

Sampai pada akhirnya jika pemahamannya tidak sama, kegiatan penyidikan berkembang ke upaya penyidik untuk meyakinkan hakim. Jadi dalam hal ini sudah melompat, peran penyidikan yang dilakukan tidak lagi meyakinkan berkas ini dapat diterima oleh Jaksa tapi kami berupaya bahwa hakim pun harus dapat menerima. Kegiatan yang dilakukan sudah melampaui dari normalnya kegiatan penyidikan yang ada. Ini sangat mendasar, dimana dijelaskan bahwa barang bukti digital adalah demikian sesuai dengan ketentuan pasal 27 tetapi ketentuan yang mengatur di dalamnya bagaimana perolehannya, bagaimana pemrosesannya, bagaimana hasilnya itu tidak dijelaskan dengan lengkap. Tidak terasa bahwa ketika undang-undangnya tidak sempurna mengatur secara detail tahapan-tahapannya, maka yang dilakukan untuk dapat diterima adalah kemampuan si penyidik, disamping meyakinkan Jaksa untuk bisa sampai dengan harus meyakinkan kepada Hakim yang akan menanganinya. Sebuah tingkat kesulitan yang sangat besar.

Menurut Responden Manajemen adalah sebuah kegiatan yang dilakukan oleh seseorang untuk dapat melakukan sebuah kegiatan yang terstruktur untuk mendapatkan suatu hasil yang maksimal. Menurut Responden untuk sebuah kegiatan manajemen sudah pasti didahului dengan perencanaan. Untuk dikaitkan dengan penyidikan, kegiatan perencanaan sebagai kegiatan awal untuk menentukan langkah-langkah apa yang akan dilakukan. Setelah itu dilakukan pengorganisasian, disini akan terlihat satu tuntutan kegiatan harus menjelaskan siapa yang akan berbuat apa. Setelah kegiatan tersebut dilakukan maka tugas selanjutnya bagaimana kita mengaktualisasikan apa-apa yang sudah direncanakan tadi dan orang-orang yang menanganinya. Untuk sebuah manajemen penyidikan, sangat dominand ditentukan hasilnya dari pengawasan yang ada. Menurut Responden tingkat pengawasan yang tinggi sangat berpengaruh pada hasil yang diharapkan.

Menurut Responden Manajemen sangat penting diterapkan dalam kegiatan penyidikan kasus hacking, karena banyak hal yang harus diangkat sebagai contoh untuk menentukan bagaimana kejahatannya dilakukan oleh pelaku, dimana dilakukan, bersama siapa, atau akan dilakukan, dimana diperlukan sebuah kegiatan penyelidikan. Penyelidikan sudah barang tentu memerlukan jumlah orang, kemampuan orang, waktu dan biaya, kemampuan dari penyidiknya sendiri, alat dan dukungan seperti biaya, dll.

Dalam kasus hacking website partai golkar sendiri, menurut Responden Manajemen tersebut telah betul-betul diterapkan oleh kepala unit. Dimana setelah mendapatkan informasi dari korbannya, dalam hal ini partai golkar sendiri, sudah dibentuk beberapa orang untuk melakukan investigasi awal penyelidikan. Dari orang-orang yang dituntut untuk melakukan penyelidikan, didapatkan bahwa pelaku berada di satu lokasi di Sumatera, di Batam. Jadi ada beberapa titik-titik yang diduga ditentukan pelakunya karena pelaku mempunyai kemampuan untuk melakukan memindahkan situs keberadaan dirinya di beberapa negara, di beberapa daerah dan bahkan di beberapa negara di seluruh dunia.

Saat itu penyidik harus punya satu ketetapan menentukan dimana pelaku dengan berdasarkan karakteristik penyerangan dilakukan. Dimana pada saat itu terdapat 12.000 (dua belas ribu) kali penyerangan dari beberapa negara dan juga di Indonesia, maka ditentukanlah bahwa berdasarkan karakteristik yang sering itu di Batam. Dapat dibayangkan apabila kepada seluruh negara tersebut dilakukan penyidikan atau didatangi lokasinya atau beberapa wilayah Indonesia didatangi sungguh sebuah pekerjaan yang mahal dan memerlukan tenaga, waktu dll yang sangat besar. Disini dijelaskan dengan jelas bahwa peran penyidik terutama hal ini dipimpin oleh kepala unit selaku manajer itu sangat dominan menentukan langkah-langkah yang menekan biaya, mendapatkan hasil yang maksimal. Setelah didapatkan pasti bahwa pelaku ada di Batam, kemudian dikirimlah beberapa orang untuk melakukan penangkapan, tentu di dahului dengan kegiatan observasi awal. Setelah dipastikan bahwa pelaku adalah seseorang yang berada di satu lokasi yang tidak berpindah-pindah, dilakukan penangkapan.

Responden menjelaskan pada saat penangkapan di Batam, Responden tinggal di sebuah Hotel di Batam. Menurut Responden untuk kegiatan pendanaan peran leader waktu itu sangat menentukan karena waktu itu untuk mendapatkan dana penyidikan dari birokrasi cukup panjang, mengajukan dulu baru kemudian untuk mendapatkannya membutuhkan proses yang panjang sementara kegiatan penyidikan yang dilakukan adalah seketika dan saat itu harus terlaksana. Penyidik yang terlibat pada saat itu adalah AKBP Edi Hartono, Akpol Dicki, AKP Ketut Budi, ada seorang ahli yang direkrut yaitu Erik, dan dipimpin oleh KANIT ketika itu. Responden memandang bahwa proses penyidikan memerlukan biaya yang tidak dapat diukur dari semula, dari awal, mengapa demikian? karena untuk menentukan seseorang jadi pelaku, kita pastikan bahwa alat-alat yang dipergunakannya ada di satu titik atau tidak tersebar, dimana waktunya tidak bisa diprediksi, dan ketika waktu tidak bisa diprediksi maka anggaran lain menjadi mahal seperti biaya akomodasi, makan, dll. Hal inilah yang tidak bisa di cover dan pemimpin ketika itu sangat berperan untuk menjadikan sebuah penyidikan ini berhasil atau tidak.

Menurut Responden ada beberapa hal yang perlu diperbaiki dalam manajemen kegiatan penyidikan kasus hacking. Yang pertama, kemampuan penyidik dan kemampuan penguasaan teknologi informasi di samping kemampuan penguasaan ilmu penyidikannya yang perlu diperbaiki. Responden melihat hal tersebut sangat penting karena untuk kejahatan-kejahatan yang terkait dengan cyber crime, dua hal itu harus dimiliki oleh seorang penyidik. Disamping pengetahuannya tentang penyidikan juga tentang tekhnologi komputer atau tekhnologi informasi.

Hal lain yang perlu diperbaiki menurut Responden adalah bagaimana penyidikan itu bisa berhasil dan tepat apabila tidak didukung oleh sebuah dukungan dana yang cukup, sehubungan dengan proses penyidikan yang tidak terukur jangka waktunya. Selanjutnya yang perlu diperbaiki dan mungkin mendasar adalah ketentuan regulasi yang ada. Karena regulasi yang ada sangat tidak menjamin bahwa penyidikan yang telah dilakukan oleh penyidik dengan susah payah akan memberikan efek jera dengan hasil yang maksimal. Dengan demikian menurut Responden apabila dilakukan penyidikan yang terkait dengan kejahatan komputer atau cyber crime atau seperti kejahatan hacking tersebut, perlu sekali dibentuk sebuah format atau suatu pelatihan bersama-sama dengan pihak-pihak yang terkait.

Identitas

Nama	: Bpk. P
Pangkat	: Kompol
Bagian	: Unit V IT & Cyber Crime DIT II Eksus
Umur	: 47 Tahun
Status	: Menikah
Pendidikan	:

- SDN 1972 Sragen
- STN 1975 Sragen
- STM 1979 Sragen
- STHI/S1 2007 Jakarta

Narasi

Responden tamat Bintara Reserse Lido 2 Tahun 1981. Pada saat pendidikan Responden dididik menjadi Dinas Reserse karena latar belakang pendidikannya kejuruan Sebaserse jadi dididik Bintara khusus untuk jadi Reserse. Tugas pertama kali, Responden ditempatkan sebagai reserse di bagian Narkotik dimana namanya dulu Diskrim Teksila PMJ di Polda Metro Jaya dari tahun 1981-1986. Kemudian pada tahun 1986 sampai dengan tahun 1991 Responden menjabat sebagai anggota curanmor PMJ di Polda Metro Jaya. Selanjutnya dari tahun 1991 sampai tahun 1997 Responden menjabat sebagai Pauralins/Opsjan Pusdik Resintel MM di Mega Mendung Bogor. Kemudian dari tahun 1997 sampai tahun 2002 Responden menjabat sebagai Kasubnit II Prodag PMJ di Polda Metro Jaya. Selanjutnya dari tahun dari 2002 sampai 2003 Responden menjabat Kasubnit II Tipikor PMJ di Polda Metro Jaya selama 1 (satu). Kemudian dari tahun 2003-2006 Responden menjabat sebagai Kanit III Cyber Crime PMJ Polda Metro Jaya. Selanjutnya setelah Responden bertugas di Polda Metro Jaya, pada tahun 2006 sampai dengan sekarang Responden bertugas di Mabes Polri menjabat sebagai Penyidik Muda di Cyber Crime.

Tindak pidana yang pernah ditangani oleh Responden adalah tindak pidana secara umum yaitu kasus-kasus narkotik, yaitu ganja, pilkita atau ekstasi, morfin, kasus Judi, kemudian sejak tahun 1987-1989 Responden menangani kasus curanmor yaitu khusus dalam mendalami pencurian motor, selanjutnya Responden juga pernah menangani kasus pembajakan hak cipta, paten dan merk, pembongkaran-pembongkaran kaset VCD, DVD di Jakarta dan rata-rata sudah sidang dan sudah diserahkan ke Pengadilan. Kasus yang paling banyak dilakukan operasi adalah masalah pemalsuan merk, bentuknya seperti tas, dompet, ikat pinggang, pulpen, contoh merk terkenal yang dipalsukan seperti aigner, fandy dan merk-merk lainnya yang terkenal di dunia. Menurut Responden dalam setiap operasi tidak pernah ditemukan pabriknya akan tetapi hanya beroperasi di penjual, misalnya di Mangga Dua dan operasi terakhir yang dilakukan Responden adalah operasi handphone Nokia di ITC mangga dua.

Pada saat bertugas di Polda Metro Jaya, Responden cukup banyak menangani kasus kejahatan komputer diantaranya penyerangan terhadap website KPU pada saat pemilihan presiden tahun 2004, dimana website KPU tersebut diserang oleh seorang hacker yang bernama Daniel Firmansyah. Selain itu masalah VCD porno melalui website komputer, yang terakhir tertangkap adalah di Malang dan sudah disidang dan terkena 6 bulan penjara, nama Tersangkanya Gorgina. Selanjutnya masalah pencemaran nama baik melalui email dan sempat P21. Kemudian program-program komputer secara konvensional yaitu penjualan komputer yang ada di toko-toko tempat jual alat-alat komputer.

Pelatihan atau pendidikan yang pernah diikuti oleh Responden adalah pada tahun 1985 Responden ke Jerman untuk mengikuti pelatihan dan penugasan masalah observasi karena di Jerman masalah observasi ditangani khusus oleh polisi khusus yang memang tugasnya hanya mencari informasi dan melakukan penyelidikan, dari hasil itu seorang penyelidik disana tidak ikut menangkap tetapi hanya memberikan data kepada polisi-polisi yang tugasnya melakukan eksekusi. Kemudian tahun 1997 Responden dikirim lagi ke Jerman dengan tugas di bidang pantobil yaitu berhubungan dengan komputer terhadap pelaku-pelaku kejahatan yang umum diketahui seperti sket wajah, dan sebagainya dimana dimasukkan ke dalam komputer kemudian di edit dan seandainya ada saksi yang melihat kita bisa gambarkan. Selain itu Responden juga belajar tentang photografi tetapi di khususkan pada photografi masalah sidik jari. Kemudian pada tahun 2003 Responden ke Malaysia mengikuti pelatihan tentang pengamanan jaringan internet dari serangan-serangan virus, termasuk hacker.

Selanjutnya pada tahun 2004 Responden ditugaskan ke Australia sehubungan dengan pemeriksaan digital yang berhubungan dengan hardisk-hardisk milik Tersangka Daniel Firmansyah dan juga dari warnet-warnet di Jogja serta hardisk yang diserang oleh hacker dan hardisk kasi yang ada di Jalan Diponegoro. Hardisk-hardisk tersebut dibawa ke Australia kurang lebih selama 2 minggu dalam rangka pemeriksaan digital karena Indonesia belum mempunyai laporan tersebut. Kemudian Responden pernah ke Malaysia tahun 2003, dan kesemua pelatihan tersebut menurut Responden sangat berguna bagi dirinya.

Responden belum pernah mencari tau mengenai kejahatan komputer karena menurut Responden kasus yang terjadi di Indonesia baru 2 kali, yang pertama tentang penyerangan KPU tahun 2004, dan yang kedua pada tahun 2006 penyerangan terhadap website golkar yang diungkap oleh Mabes Polri, dimana pelakunya dan juga TKPnya di Batam sehingga Responden belum bisa mencari sendiri karena hacker bersifat tertutup dan Responden sendiri belum bisa masuk ke jaringannya. Namun kalau chating dengan para hacker Responden pernah melakukannya tetapi mereka tidak pernah mau terbuka karena khusus hanya untuk hacker.

Sedangkan terhadap kejahatan hacking Responden cukup memahaminya, karena Responden bertugas dibagian investigasi hacker. Dalam kasus Daniel Firmansyah

Responden mengetahui bagaimana cara penyerangannya, dimana mereka mencoba masuk dan meminta izin kepada jaringan internet dengan menggunakan teknik-teknik menyerang untuk membongkar jaringan yang sudah dilengkapi dengan pengaman, namun Responden tidak mengetahui secara pasti bagaimana Daniel Firmansyah bisa masuk ke website yang menggunakan user ID dengan password tanpa meminta kepada user, dengan tidak open account dsb.

Responden belum pernah melakukan penelitian terhadap kejahatan komputer karena belum sempat melakukannya dan selama ini Responden banyak melakukan penyelidikan khusus kasus-kasus yang berhubungan dengan kejahatan komputer.

Menurut Responden cyber crime mempunyai 2 (dua) pengertian yaitu kejahatan komputer yang ada hubungannya dengan masalah hacking, yang kedua cyber crime adalah kejahatan komputer seperti cyber gambling, cyber pornografi. Sedangkan hacking adalah masuk ke jaringan internet tanpa seizin pemilik website dengan maksud untuk mengetahui content atau isi-isi di website tersebut atau hanya ingin tahu, tetapi ada juga yang dengan sengaja masuk mungkin untuk merusak data atau mengubah data sekaligus mungkin menghapus data.

Kasus hacking yang pernah ditangani oleh Responden adalah kasus hacking pada website KPU yang terjadi pada tahun 2004. Tindakan yang dilakukan oleh Polda Metro Jaya pada saat itu mencari data dari log filenya yaitu penyerangnya kira-kira datang dari mana, dimana dari log file tersebut dapat dibaca dan telusuri yang akhirnya mengarah pada Daniel Firmansyah.

Selain menangani kasus hacking website KPU (Komisi Pemilihan Umum) Responden juga terlibat dalam penanganan kasus hacking website partai golkar dimana Responden berperan dalam meminta penetapan, penggeledahan dan penyitaan dari Pengadilan Batam. Proses penanganannya sendiri menurut Responden sama seperti pada saat menangani kasus KPU di Polda Metro Jaya yaitu website yang di hack itu, hardisknya di kloning dan diambil untuk disidik dan diperiksa secara laboratorium. Hasil dari laboratorium pasti mendapatkan log file dari hasil penyerangan terhadap website golkar dan dari situlah baru ketahuan log-file-log file yang penyerangnya dari mana, dan diketahui ternyata penyerangnya kebanyakan dari Batam.

Sampai saat ini undang-undang yang digunakan dalam penanganan masalah hacker adalah Undang-Undang Telekomunikasi dan Rancangan undang-undang tentang teknologi dan informasi belum disahkan oleh DPR. Menurut Responden tindak pidana hacker sebenarnya sama saja dengan kejahatan-kejahatan yang lain dimana kejahatan hacking juga meresahkan masyarakat khususnya masalah teknologi dan informasi, oleh karenanya menurut Responden semestinya hacker diatur dalam undang-undang tersendiri dengan hukuman seberat-beratnya.

Menurut Responden tidak ada kesulitan dari segi hukum acara terhadap penanganan kasus hacking karena selama ini undang-undang yang digunakan adalah Undang-Undang Telekomunikasi seperti pada kasus Daniel Firmansyah dimana kasusnya sudah divonis. Dengan demikian proses penyelidikan sampai proses penegakan hukum di pengadilan tidak ada masalah. Dalam pandangan Responden masalah kejahatan komputer semestinya harus dilaksanakan seperti yang tertuang dalam Rancangan undang-undang Tekhnologi dan Informasi agar aplikasi di lapangan lebih baik ke depannya. Oleh karenanya sebaiknya Undang-undang Teknologi dan Informasi segera disahkan.

Menurut Responden dalam Manajemen harus ada 4 (empat) dimana dalam manajemen itu harus ada namanya planning, kemudian harus ada organizing atau organisasi, kemudian yang ketiga harus ada pelaksanaan dan yang paling penting harus ada controling. Jadi yang ada di dalam manajemen tersebut satu sama lain harus saling berkaitan, kalau tidak manajemen tidak akan berjalan. Mengenai penerapan manajemen, menurut Responden tidak hanya dalam kasus hacking namun dalam setiap kasus baik dalam tindak pidana umum maupun tindak pidana khusus.

Menurut Responden dalam kasus hacking website partai golkar manajemen penyidikan tersebut sudah diterapkan, dimana prosesnya dimulai dari planning. Dalam tindak pidana hacking apabila sudah terjadi berarti sudah ada TKP (Tempat Kejadian Perkara), oleh karena itu harus dibuat planning atau rencana bagaimana dalam pembuatan TKP harus jelas dan dibagi tugas siapa saja yang berangkat dalam perencanaan itu kemudian siapa dan tugasnya apa, semuanya harus jelas sebelum berangkat. Kemudian organizing harus jelas berapa orang dalam organisasi tersebut, organisasi itu penting karena tanpa organisasi pekerjaan tidak akan berjalan dengan baik. Masalah pelaksanaan tentunya sudah dalam pelaksanaan eksekusi.

Menurut Responden menangkap hacking tidak sesulit menangkap teroris atau pelaku kejahatan keras yang lain termasuk perampokan dsb, karena mereka adalah pakar-pakar IT dan orangnya biasa, jadi dalam menangkap hacker tidak perlu dengan kekerasan akan tetapi dengan perencanaan, organisasi yang baik, dan pelaksanaannya. Pembiayaan terhadap penyelidikan dan penyidikan dalam kasus hacking disediakan oleh Negara hal tersebut tidak hanya berlaku di Indonesia namun diseluruh dunia akan tetapi menurut Responden yang terjadi selama ini adalah biaya penyelidikannya agak sulit, dimana biayanya menurut Responden sebenarnya tidak terlalu besar seperti pada saat Responden berangkat ke Australia.

Menurut Responden hal-hal yang perlu diperbaiki lagi dalam penerapan manajemen penyidikan kasus hacking adalah harus ada planning, organizing, pelaksanaan, controlling dimana kesemuanya harus saling berkaitan yaitu apabila planningnya tidak bagus maka pelaksanaan sampai controlingnya tidak bagus, tetapi kalau pelaksanaannya bagus dan tidak keluar dari tata cara perundang-undangan dan diatur dalam hukum acara akan menghasilkan hasil yang baik. Selanjutnya menurut Responden yang perlu diperbaiki lagi adalah mengenai sumber pembiayaannya.

Identitas

Nama : Bpk. I W
Pangkat : AKBP
Bagian : Unit V IT & Cyber Crime
Umur : 42 Tahun
Status : Menikah
Pendidikan :

- SD 1977 Blora
- SMP 1981 Blora
- SMA 1984 Blora
- S-1 Biologi 1991 UGM Yogyakarta
- S-1 Teknik dan Informatika Komputer 1999 Unika Surabaya
- S-1 Ilmu Hukum 2002 Unkar Surabaya
- S-2 Teknik Lingkungan 2002 ITS Surabaya

Narasi

Responden mengawali karirnya dengan menjabat sebagai PA beasiswa dari tahun 1989 sampai dengan tahun 1991, kemudian pada tahun 1991 Responden menjabat sebagai Pama Polwil di Yogyakarta dan sebagai Pama Labfor cabang Surabaya. Kemudian dari tahun 1991-1995 Responden menjabat sebagai Panit Kimia Forensik Labfor di Surabaya, kemudian dari tahun 1995-2003 Responden menjabat sebagai Kanit Biologi Forensik Labfor cabang Surabaya. Selanjutnya dari tahun 2003-2006 Responden bertugas di Bareskrim Polri dengan menjabat sebagai Laboran Madya Unit Upal Puslabfor. Selanjutnya dari tahun 2006 sampai dengan sekarang Responden menjabat sebagai Penyidik Madya Dit II Eksus di Bareskrim Polri.

Responden masuk Polisi melalui program Ikatan Dinas Mabes ABRI, akan tetapi pada semester 7 Responden tidak melanjutkan pendidikannya, kemudian Responden ikut testing, dan masuk Mantra Polisi kebetulan waktu itu basic Responden adalah S1 di UGM yaitu Biologi kemudian setelah lulus Responden ditempatkan di laboratorium Forensik cabang Surabaya di bidang Biologi Forensik. Kemudian tahun 1996, Responden ditugaskan di Inggris selama 2 bulan untuk mempelajari atau belajar tentang DNA Finger Print atau Sidik Jari DNA. Kemudian setelah berdinas selama bekerja di Surabaya, Responden menyelesaikan S1 dan S2-nya dalam bidang ilmu yang lain yang pertama adalah bidang Komputer Koordinator Teknik Informatika, yang kedua adalah Sarjana Hukum.

Mengenai penanganan kasus sendiri, Responden pernah terlibat dalam penanganan kasus kejahatan komputer yaitu berperan dalam memeriksa barang bukti digital evidence, yaitu memback-up penyidik dalam arti menghitung muatan.

Menurut Responden kejahatan komputer bisa diketahui berdasarkan 2 (dua) sumber; Pertama, jika terjadi kejahatan komputer dilaporkan langsung oleh korban atau victim. Yang kedua penyidik sendiri bersifat proaktif dalam arti mencari tahu secara baru misalnya melalui cyber crime atau cyber under cover dan sebagainya. Dengan teknik–teknik under cover tapi melalui sarana investigasi secara online. Apabila ingin mencari tau langsung dapat meminta bantuan dari rekan kerja bagaimana melakukan cyber under cover, mencari data–data atau pelaku–pelakunya yang memang secara online dia aktif untuk melakukan kejahatan melalui sarana internet.

Pelatihan atau pendidikan yang pernah diikuti oleh Responden selama menjadi polisi adalah mengikuti pendidikan di luar negeri yaitu tahun 2003 belajar tentang komputer forensik di Singapura, kemudian tahun 2006 atau 2007 belajar tentang investigasi cyber crime di Korea, kemudian belajar tentang Child Sex is Potent Facilitated by Computer di Filipina. Selanjutnya untuk kursus atau satuan di dalam negeri yaitu belajar tentang CTRC yang difasilitasi oleh FBI.

Namun pelatihan yang secara spesifik mengenai kejahatan komputer yang pernah diikuti oleh Responden adalah di Korea tentang penyidikan atau investigasi tentang cyber crime. Sedangkan mengenai hacking tidak dipelajari oleh Responden. Menurut Responden untuk pengetahuan tentang hacking Responden balajar secara otodidak atau belajar sendiri karena Responden sudah lama menjadi pengamat atau pemerhati bidang IT yaitu sejak tahun 1995 sejak Responden kuliah S1 Informatika.

Hal baru yang dipelajari oleh Responden mengenai masalah-masalah komputer adalah tentang teknik–teknik yang digunakan oleh para pelaku, dimana seiring dengan berjalannya waktu, selalu mengalami perkembangan dari waktu ke waktu, biasanya teknik–tekniknya akan berkembang dan akan lebih maju daripada teknik–teknik sebelumnya yang memang kalau zaman dulu kejahatan komputer masih sederhana. Kemudian dengan berkembangnya teknologi internet ini, teknik atau metode kejahatan komputer ini makin berkembang karena makin mudahnya para hacker ini melakukan tukar menukar informasi diantara komunite hackingnya. Dengan adanya pelatihan-pelatihan tersebut menurut Responden sangat berguna untuk menambah wawasan dan perkembangan teknik-teknik kejhatan IT atau kejahatan komputer.

Responden sering mencari tau sendiri mengenai kejahatan komputer yaitu dengan cara belajar langsung dari situs–situs tertentu yang memang banyak bertebaran, bisa ratusan atau ribuan situs yang membahas atau mengupas tentang kejahatan tersebut. Misalnya apabila ingin mencari tau informasi tinggal pakai google, search engine google, selanjutnya ketik topik apa yang diinginkan dan kita akan mendapatkan apa saja yang kita mau. Begitu juga mencari tau tentang hacking, menurut Responden mudah sekali untuk mencari informasinya, bahkan teknik yang mereka pakai bisa dipelajari dengan cepat melalui sarana search engine. Selain itu untuk mencari tau mengenai hacking juga dapat dilihat melalui internet karena semua informasi yang paling terkini atau terbaru selalu ada situsnya di internet terutama dalam komunite–

komunite hacker. Ada beberapa komunite hacker yang selalu diikuti oleh Responden yaitu Yogya Hacker dimana disana juga banyak kajian tentang ilmu komputer, jasa komp juga ada, situs diluar Indonesia juga banyak sekali, cukup pakai search engine dan akan ketahuan dan sangat mudah.

Responden belum pernah mengadakan penelitian mengenai kejahatan komputer karena menurut Responden Satgasnya tidak mendukung untuk melakukan research terhadap bidang ilmu tersebut.

Menurut Responden defenisi tentang cyber crime banyak diatur dalam berbagai sumber dan mempunyai defenisi yang berbeda-beda, misalkan defenisi yang diatur dalam United Nation akan berbeda dengan masyarakat di Eropa kemudian akan berbeda juga dengan yang diatur dalam komite IT di Amerika, kemudian juga menurut beberapa kamus tertentu seperti kamus dalam Wikipedia juga punya definisi sendiri. Sedangkan Responden sendiri lebih cocok atau cenderung sependapat dengan definisi yang disebutkan dalam Deklarasi atau menurut United Nations atau PBB yaitu bahwa kejahatan komputer itu sebenarnya adalah perkembangan lebih lanjut dari kejahatan komputer. Jadi, sebelum teknologi internet ditemukan, kita hanya mengetahui bahwa kejahatan IT hanya kejahatan komputer yang menggunakan sarana IT sebagai alat bantu untuk melakukan kejahatan atau tindak pidana. Kemudian makna kejahatan komputer ini sendiri kemudian berkembang yaitu setelah adanya teknologi internet sehingga orang bisa berkomunikasi dalam satu wilayah ke wilayah lain tanpa adanya batas wilayah atau batas negara. Orang bisa melakukan akses, melakukan tindak pidana kejahatan komputer ke komputer yang lain dalam jarak atau ruang waktu yang tidak dibatasi oleh suatu batas wilayah atau batas negara. Ini adalah makna dari kejahatan komputer yang kemudian berkembang lagi menjadi kejahatan cyber ini.

Terhadap defenisi hacking sendiri banyak sekali maknanya karena berbagai pakar mempunyai pandangan yang berbeda-beda mengenai defenisi hacking, namun menurut Responden hacking adalah memasuki suatu komputer atau jaringan komputer orang lain secara tidak sah atau tidak hak tetapi si hacker ini atau orang yang melakukan kegiatan hacking ini tidak mempunyai tujuan apa–apa, maksudnya tidak akan merusak datanya, tidak mengambil data, tidak menyebar suatu program tertentu yang bisa merugikan dan hacking ini atau hacker ini mempunyai tujuan positif, kadangkala dia karena keahliannya seringkali dimintai bantuan oleh orang lain tertentu, misalnya, temannya mungkin komunitenya untuk mengetahui kelemahan suatu system.

Dalam penanganan kasus hacking website partai golkar, proses penyidikan dimulai dengan melakukan koordinasi dengan pemilik situs tersebut, kemudian setelah dilakukan negosiasi dengan Pemerintah tim forensic laboratorium datang ketempat situs Golkar yaitu PT. Master Web dan setelah itu berangkat menuju ke server dimana situs tersebut ditempatkan yaitu kebetulan situs tersebut tersimpan di Telkom Jakarta Barat. Kemudian dilakukan proses cloning, kemudian hasil kloningnya

dianalisis di laboratorium. Selanjutnya dicari tahu di log file tersebut, karena log file akan memberikan informasi–informasi terhadap siapa saja atau pihak mana saja yang melakukan, mengakses atau melakukan instruksi terhadap situs tersebut, dan akan tercatat di dalam suatu log file atau MPV File.

Menurut Responden seorang pemeriksa akan selalu memiliki feeling awal, dimana pada saat menangani kasus hacking website partai gokar Responden mempunyai feeling bahwa penyerangnya berasal dari Batam dan ternyata setelah diperiksa lagi dari beberapa analisis data long file tersebut memang menuju ke arah itu. Pada saat itu ada yang mengakses dari Bandung, dari Palembang, dan dari Batam. Responden sendiri pada saat itu lebih cenderung merasa penyerangnya dari Batam.

Menurut Responden Manajemen adalah ilmu dimana sesuatu hal yang akan mengatur, ilmu yang akan mengatur bagaimana sesuatu tujuan itu bisa tercapai dengan maksimal dan efisien. Tujuannya akan bisa tercapai dengan efisien dan maksimal. Ilmu manajemen dibagi menjadi beberapa teori, salah satunya yaitu manajemen mengenai money planning atau perencanaan, kemudian pengorganisasian kemudian action atau pelaksanaan dan yang terakhir tentunya adalah system controlling yang akan mengontrol semua kegiatan sehingga akan bisa berjalan efektif dan efisien.

Menurut Responden semua kejadian atau kegiatan harus diatur melalui proses manajemen termasuk juga didalam penanganan kasus hacking. Semua harus memakai manajeman. Dalam penyidikan kasus hacking website partai golkar sendiri manajemen penyidikan tersebut telah diterapkan dimana sudah ada pembagian kerja yang bagus, si A melakukan apa, si B melakukan apa, si C melakukan apa, siapa yang melakukan controlling, siapa yang membiayai, menurut Responden pada saat menangani kasus hacking website partai golkar sayap pengamanannya sangat bagus sehingga bisa berhasil dan efektif bisa menangkap si pelaku.

Menurut Responden hal-hal yang perlu diperbaiki lagi dalam penerapan manajemen penyidikan kasus hacking adalah meningkatkan pengetahuan dari sumber daya manusianya atau para penyidik, yaitu mengenai apa sebenarnya hacking itu dalam arti bukan hanya mengerti tentang definisinya saja tetapi bagaimana teknik yang mereka lakukan itu, sehingga pada waktu sesuatu terjadi, si penyidik itu bisa langsung mengetahui kira–kira apa, kemudian bagaimana suatu kasus hacking terjadi. Kemudian setelah penyidik memahaminya maka tentunya mereka akan bisa melakukan penyelidikan dengan baik, akan tetapi harus juga dimanage dengan baik pula. Kemudian harus ada dukungan biaya yang bagus, entah itu darimana, mungkin bisa dari dinas atau mungkin dari pembiayaan dari rekanan, atau dari pembiayaan sendiri, kemudian support dari pimpinan karena hal tersebut sangat penting sekali, selanjutnya dukungan terhadap laboratorium forensic.

Identitas

Nama : Bpk. D.P
Pangkat : Kompol
Bagian : Cyber Crime
Umur : 36 Tahun
Status : Menikah
Pendidikan :

- SD 1984 Jakarta
- SMP 1987 Banda Aceh
- SMA 1990 Semarang
- AKPOL 1993 Semarang
- S-1 Hukum 1999 Surakarta
- PTIK 2002 Jakarta
- S-2 Kajian Ilmu Kepolisian 2005 Jakarta
- Sespim 2007 Bandung

Narasi

Responden lulus Akademi kepolisian pada tahun 1993, kemudian sejak tahun 1994-1995 Responden bertugas sebagai Pabapta Polresta Surakarta Polda Jawa Tengah . Kemudian dari tahun 1995 sampai dengan 1997 menjabat sebagai Kapolsek di Kertasuro Polda Jawa Tengah. Kemudian dari tahun 1997-1999 Responden menjabat sebagai Kasatserse di Polresta Surakarta Polda Jawa tengah, selanjutnya dari tahun 1999-2000 menjadi Kasubag KM Serse Umum Polda Jateng. Selanjutnya Responden mengikuti pendidikan di PTIK dan lulus pada tahun 2002 kemudian Responden ditempatkan di Bareskrim Polri selama 6 (enam) sebagai Penyidik muda pada unit II cyber crime, selanjutnya dari tahun 2006 Responden menjabat sebagai Penyidik Madya Unit II IT cyber crime.

Tindak pidana yang pernah ditangani oleh Responden adalah tindak pidana konvensional pada umumnya, seperti pencurian, penipuan lalu penggelapan, pemalsuan baik itu uang maupun dokumen, kemudian narkotika dan kejahatan konvensional lainnya. Sedangkan selama di cyber crime Responden pernah menangani kasus penipuan melalui internet. Tapi sejauh ini belum pernah ada yang berhasil diselesaikan, kemudian kasus pencemaran nama baik melalui e-mail dan penyebaran foto porno serta kasus hacking.

Kejahatan komputer yang pernah ditangani oleh Responden adalah kasus hacking yaitu penyerangan web site Golkar yang merubah tampilan web site tersebut dari gambar petinggi Golkar menjadi gambar wanita cantik dan gambar gorilla. Selanjutnya kasus pengancaman melalui e-mail yang dilakukan oleh salah seorang karyawan terhadap pimpinan perusahaan tersebut kemudian penyebaran gambar porno di internet yang dilakukan oleh pacarnya karena kecewa terhadap kekasihnya.

Pendidikan yang pernah diikuti oleh Responden selama menjadi Polisi adalah mulai dari AKPOL tahun 1993, kemudian untuk Dikjur–Dikjur, Responden memiliki Dikjur uang palsu tahun 1996, kemudian Dikjur Korupsi tahun 1999, kemudian PTIK tahun 2000 dan lulus pada tahun 2002, kemudian Sesimpol tahun 2007. Sedangkan untuk pendidikan umumnya, Responden S1 Hukum di Universitas Paratriadi tahun 1999, kemudian kajian ilmu kepolisian S2 UI tahun 2005.

Setelah bergabung di Mabes Polri pada unit cyber crime Responden telah mengikuti kursus mengenai cyber crime di luar negeri, seperti di Hongkong mengenai "Child Exploitation", kemudian di Bangkok, di Vietnam, konferensi mengenai hack-hack Crime, lalu di Malaysia untuk Computer Emergency Responding dan seminar – seminar lokal di Indonesia mengenai cyber crime.

Terhadap pembekalan atau pelatihan mengenai kejahatan komputer sendiri Responden juga sudah pernah mengikutinya lebih kurang 3 kali yaitu di Bangkok 2 kali mengenai investigator dan di Vietnam sekali mengenai hack hack crime. Sedangkan mengenai hacking sendiri Responden belum pernah mengikuti pendidikannya secara khsusus.

Menurut Responden pelatihan-pelatihan yang diikutinya tersebut sangat berguna dimana dengan adanya pelatihan tersebut memberikan gambaran ataupun wawasan mengenai apa yang dimaksud dengan cyber crime dan bagaimana kejahatan itu berlangsung dan bagaimana pula seorang penyidik mesti membuktikan sesuatu yang tidak nampak secara nyata untuk dibawa ke suatu pembuktian yang secara nyata sehingga diperlukan suatu interpretasi dan kalau tidak didukung oleh gambaran atau wawasan sebelumnya sangat sulit untuk membuat sesuatu itu menjadi gampang dimengerti oleh orang yang tidak mengerti, atau orang awam lainnya.

Responden pernah mencari tau sendiri mengenai kejahatan komputer yaitu dengan cara searching di Internet, searching artikel-artikel mengenai cyber crime, dan juga perkembangan kasus yang terjadi dibidang cyber crime. Di internet sendiri Responden mengunjungi www. fbi.com selanjutnya mengunjungi website yahoo ataupun google dengan kata kunci computer crime atau cyber crime sehingga banyak artikel – artikel lepas yang bisa dibaca dan dipelajari mengenai perkembangan cyber crime itu sendiri. Sedangkan untuk mencari tau mengenai hacking sendiri Responden banyak menjalin network, menjalin hubungan dengan orang–orang yang memiliki kemampuan–kemampuan hacking ataupun memahami mengenai teknologi computer yaitu dengan cara berkenalan ataupun mencari tahu siapa kira – kira yang mengerti suatu permasalahan mengenai hacking ini. Misalnya jika punya teman si A, maka langsung ditanyakan kepadanya, permasalahan begini, kira – kira punya teman nggak yang mengerti. Biasanya Responden diperkenalkan oleh temannya kepada orang yang lebih mengetahui permasalahan tersebut. Namun dalam pergaulan tersebut Responden tidak pernah membawa dirinya sebagai seorang polisi tapi bergaul sebagaimana layaknya bahwa Responden sama seperti mereka dan Responden hanya ingin mengetahui saja apa yang mereka kerjakan.

Responden belum penah melakukan penelitian mengenai kejahatan komputer, akan tetapi Tesis Responden dan task up nya mengenai kejahatan komputer dilihat dari sudut organisasinya. Misalnya bagaimana sebenarnya Polri yang baik untuk menghadapi kejahatan cyber crime karena saat ini unit cyber crime tidak dapat mengcover kejadian yang ada, sehingga unit tersebut perlu diperbesar. Kalau bicara dari supremasinya Unit yang ada sekarang ini sifatnya adalah satuan daripada unit unit kerja, jadi kalau satuan kerjanya adalah bareskrim, unit kerjanya adalah direktorat maka satuan kerja itu adalah unit–unit yang ada di bareskrim tersebut. Sehingga untuk berkoordinasi maupun membuat suatu keputusan seorang Kanit tentunya sangat sulit karena melalui berbagai macam birokrasi. Tetapi seandainya itu diperbesar menjadi sebuah Direktorat bagaimanapun ini menjadi sebuah satuan kerja, unit kerja.

Dalam tesis tersebut Responden menjelaskan diperlukan suatu keputusan atau spesifikasi lebih lagi, seperti halnya unit kerja yang satuan kerja bareskrim seperti Labfor terus indem ataupun densus 88 yang mereka dapat mengadakan peralatannya sendiri dapat mendapatkan anggaran sendiri untuk unit kerja mereka melalui satuan kerja bareskrim.

Sedangkan pada saat di Sespim Responden pernah membuat naskah dengan judul "Kemampuan peningkatan Kemampuan Penyidik", dalam tulisan tersebut digambarkan mengenai kemampuan secara umum saja. Apabila seandainya seorang penyidik ingin menangani kasus cyber crime apa saja yang harus dia kuasai dan apa saja yang harus dimiliki oleh satuan tersebut. Responden menjelaskan penelitiannya di Polda Metro Jaya dengan berdasarkan dokumen – dokumen saja ataupun persepsi Responden terhadap satuan tersebut berdasarkan buku tahunan, laporan satuan (Lap Sat), yang dimiliki oleh satuan cyber crime pada Polda Metro Jaya.

Terhadap hacking sendiri Responden belum pernah mengadakan penelitian karena menurut Responden hacking itu banyak terjadi tetapi banyak juga yang tidak dilaporkan. Selain itu Responden tidak terlalu menguasai mengenai cara melakukan hacking, karena kemampuan berfikirnya sudah tidak sanggup lagi untuk mengikuti cara berpikir seseorang yang melakukan hacking. Oleh karenanya Responden tidak mengadakan penelitian mengenai hacking namun memfokuskan bagaimana caranya mengaplikasikan, cara melakukan penyidikan untuk mengetahui bagaimana kejahatan itu dapat terjadi.

Menurut Responden cyber crime adalah salah satu kejahatan yang berkaitan dengan network, jaringan dan computer di segala kegiatan yang berkaitan network jaringan komputer. Sedangkan hacking adalah suatu perbuatan memasuki suatu system jaringan computer milik orang lain, tanpa seizin daripada si pemilik jaringan itu sendiri, entah hanya melihat – lihat, merusak ataupun memperbaiki system yang ada disana.

Responden pernah menangani kasus hacking yaitu kasus hacking website partai golkar. Dalam penanganan kasus tersebut yang pertama dilakukan adalah melakukan pemeriksaan yaitu pemeriksaan terhadap admin website itu sendiri. Pada saat awal melakukan pemeriksaan terhadap admin tersebut terdapat kesulitan karena admin merasa bahwa menjaga security daripada website tersebut adalah tanggung jawab daripada tempat dimana website tersebut didaftarkan yaitu web master tempat dimana website tersebut diletakkan diserver milik perusahaan provider tersebut. Namun ternyata setelah dilakukan penyidikan dan pemeriksaan terhadap provider tersebut, mereka katakan mereka hanya tempat menyewa servernya saja, jadi ibaratnya apabila kita mengontrak rumah, mereka hanya menyediakan rumahnya saja, sedangkan sekuriti dari rumah tersebut adalah tanggung jawab daripada sipemilik.

Menurut Responden si admin tidak terlalu memahami mengenai teknologi itu sendiri. Jadi ibaratnya dia hanya sekedar membuat website, selesai dengan suatu harga, didaftarkan, dilaunching, dan dia sendiri tidak menguasai bagaimana caranya menjaga sekuriti daripada website tersebut, sehingga terjadilah website tersebut dijebol orang.

Kemudian Responden bersama teamnya menggunakan salah satu tenaga ahli yang berada di unit cyber tersebut untuk membantu membaca log server yang ada di server tempat website tersebut berada. Dari hasil pemeriksaan log server tersebut, dianalisa bahwa serangan itu terjadi hingga ratusan kali, bahkan kurang lebih seribu dua ratus sekian. Kemudian dipilah – pilahkan lagi berapa banyak serangan yang terjadi sesuai dengan hari–harinya karena ada jangka waktu lima hari terjadinya serangan, dari awal hingga akhir baru dilaporkan oleh korban.

Dari analisa serangan tersebut Responden bersama teamnya berangkat ke Bandung, karena banyak serangan dari Bandung, dan ternyata setelah diperiksa tidak ditemukan adanya bukti petunjuk bahwa serangan tersebut terjadi dari Bandung. Kemudian dipelajari lagi, dimana terdapat tiga kemungkinan yaitu Jakarta, Palembang dengan Batam sehingga setelah koordinasi dengan penyidik lainnya diputuskan untuk berangkat ke Batam.

Responden bersama Teamnya berangkat ke Batam memeriksa ISP PT Inforsys yang mana IT nya digunakan untuk melakukan serangan terhadap website Golkar tersebut. Dari pemeriksaan di PT Inforsys tersebut diketahui bahwa IT yang digunakan untuk menyerang website Golkar adalal IT yang sudah tidak ada lagi pemiliknya, dalam arti kata IT nya disewakan tetapi kontrak kepemilikan IT tersebut sudah tidak ada lagi. Sehingga IT ini IT bebas tetapi mereka tidak pernah melakukan cek ataupun pemeriksaan terhadap IT tersebut.

Dengan bantuan dari pihak inforsys untuk memetakan IT – IT tersebut terlihatlah ada satu kesamaan IT tersebut dengan letak sebuah warnet dan IT lain yang masih aktif. Pada saat itu juga, tenaga ahli menemukan suatu tutorial cara melakukan hacking. Dalam tutorial tersebut nampak bahwa tindakan hacking tersebut dilakukan oleh si

pembuat website, persis sama. Sehingga dicari informasi siapa pembuat website ini. Pembuat website ini dari Batam juga sehingga akhirnya dapat ditemukan pelakunya, yaitu si pembuat tutorial itu sendiri. Tetapi ternyata setelah di cek, IT tempat dia melakukan online ataupun hubungan dengan internet bukan IT yang menyerang daripada website Golkar tersebut. Sehingga dimulai lagi pencarian terhadap IT yang dikatakan sudah tidak digunakan lagi. Ternyata setelah di cek, IT tersebut digunakan oleh seseorang di warnet warnet yang mungkin dilakukan oleh si pelakunya. Hal itu dapat diketahui dari system pemantauan IT yang dimiliki oleh ISP PT Inforsys itu sendiri. Jadi dia bilang ini sebenarnya sudah dipakai tapi pada hari itu IT tersebut digunakan. Seharusnya IT tersebut sudah tidak digunakan lagi.

Penyidik berkoordinasi untuk mencari tahu siapa kira – kira yang menggunakan IT tersebut. Dari hasil pengumpulan informasi yang ada didapatlah sebuah nama yang disinyalir sering melakukan deface ataupun sekedar usil – usilan saja. Tetapi pelaku ini lebih condong kepada fising melakukan penipuan terhadap orang lain, mencuri kartu kredit milik orang lain atau fising. Selanjutnya dilakukanlah chatting dengan yang diduga tersangka. Pada saat chatting, diminta bantuan dari informan, dalam chatting tersebut si tersangka mengakui bahwa dia melakukan hal tersebut sehingga langsung menuju ke warnet. Pada saat menuju ke warnet, belum diketahui siapa sebenarnya nama si pelaku ini, yang diketahui adalah nick namenya ini, dia menggunakan IT ini, sehingga pada saat ke warnet, dilakukan pengecekan terhadap admin warnet tersebut, bahwa IT tersebut di meja nomor berapa sehingga ketahuanlah IT tersebut di meja yang digunakan oleh pelaku. Jadi pada saat itu harusnya computer. komputer yang ada 10 komputer menggunakan IT local, IT warnet 1 sampai 10, tapi untuk computer yang nomor 1 ini aktif tapi tidak menggunakan IT local sehingga disinyalir, computer ini menggunakan IT yang diduga digunakan untuk melakukan serangan. Sehingga para penyidik masuk kesana, dilakukan pengecekan melalui file sending nya untuk IT conflict yang pada computer tersebut. Pada IT conflict tersebut tercetaklah IT daripada IT yang sudah digunakan itu lagi. Sampai sekarang juga menurut pangakuan daripada tersangka setelah tertangkap dia lakukan searching di IT milik PT Inforsys tersebut. Karena dia bilang jaringan tersebut tidak terlalu skill bisa dimasuki untuk mencari IT yang kira – kira kabur bisa digunakan. Karena dengan IT yang ada tersebut dia bisa koneksi sendiri. Kecepatan download maupun upload menjadi lebih cepat dibandingkan dengan IT local daripada warnet itu sendiri.

Berkaitan dengan pembuatan laporan polisi menurut Responden pada saat itu Polisi membuat laporan setelah adanya laporan dari admin website golkar dimana Pelapor datang ke unit cyber crime tapi tidak langsung ke bawah ke tempat pelaporan seperti biasa dengan alasan kecepatan untuk penanganan.pada saat itu. Karena seandainya langsung lapor ke bawah akan ditemui beberapa kendala-kendala yang pertama mungkin di bawah itu juga akan kesulitan untuk memahami kasus yang terjadi, yang kedua tentunya dibawah itu akan menanyakan barang bukti yang ada itu apa. Barang bukti yang ada itu hanya berupa kertas – kertas dan foto dan mungkin untuk kasus konvensional itu tidak cukup sebagai barang bukti dan juga tidak ada bukti secara

fisik dimana telah terjadi suatu tindak pidana. Yang ketiga, setelah dari bawah tersebut, agar laporan tersebut naik ke unit yang menangani itu memakan waktu cukup lama, bisa tiga atau empat hari. Sedangkan kalau itu dilakukan tentunya penanganan pun akan semakin lama. Sehingga itu adalah suatu kendala sendiri, itu suatu birokrasi. Tapi itu adalah birokrasi yang standard dari kasus lainnya dan hal ini tidak bisa dilakukan seperti itu untuk kasus cyber crime karena membutuhkan kecepatan dalam suatu penanganannya.

Menurut Responden terhadap pemilihan pasal dan pemenuhan unsure-unsur tindak pidana sendiri terdapat kendala-kendala. Dalam kasus tersebut Pasal yang digunakan adalah masih menggunakan KUHP seandainya itu pun di juncto kan, maka akan juncto kan dengan undang – undang telekomunikasi No. 36 tahun 1999 Pasal 22 a, b, c. Tetapi menurut Responden sebenarnya undang – undang No. 36 tahun 1999 itu sendiri pun, sebenarnya kalau ada pengacara yang cukup jeli, dia akan menanyakan system jaringan informasi khusus itu apa termasuk internet, dan itu tidak dijelaskan didalam undang – undang No. 36 tahun 1999. Itu semua adalah interpretasi daripada penyidik dalam memahami suatu perkara yang ada dikaitkan dengan tindak pidana umum karena menggunakan KUHP, seperti deface pasal yang digunakan adalah pengrusakan pasal 406 KUHP, ataupun misalnya penipuan melalui internet pasal yang digunakan Pasal 372 dan Pasal 378 hanya kasus-kasus konvensional saja sehingga memang dibutuhkan suatu keterampilan sendiri. Oleh karenanya penyidik melakukan interpretasi ataupun melakukan pemeriksaan terhadap saksi ahli untuk menyatakan bahwa barang bukti tersebut merupakan sah sebagai alat bukti karena kalau menurut alat bukti yang sah, tidak ada yang mengatakan suatu digital evidence sebagai bukti.

Walaupun dalam beberapa undang – undang lainnya itu sudah mengatur mengenai digital evidence. Namun dalam undang-undang tersebut belum mengatur digital evidence sebagai alat bukti, dan belum ada yurisprudensi dalam kasus yang mengatakan bahwa digital evidence sebagai alat bukti. Oleh karenanya Responden menyarankan sebaiknya tindak pidana hacking diatur dalam suatu undang – undang atau peraturan sendiri yang spesifik mengatur mengenai masalah hacking itu sendiri, tidak lagi berinterpretasi. Karena interpretasi tergantung daripada persepsi ataupun pandangan dari orang yang melihat kasus itu sendiri.

Identitas

Nama	: Bapak S
Pangkat	: Kompol
Bagian	: Unit V IT & Cyber Crime DIT II Eksus
Umur	:
Status	: Menikah
Pendidikan	:

- SD 1986 Tuban
- SMP 1989 Tuban
- SMA 1992 Tuban
- Akpol 1995 Semarang
- PTIK 2005 Jakarta

Narasi

Responden bertugas pertama kali pada tahun 1996 sampai dengan 1997 di Jawa Barat sebagai Pamapta Bandung Tengah, selanjutnya Responden masih bertugas di daerah Jawa Barat pada tahun 1997 sampai dengan tahun 1998 pada saat itu Responden menjabat sebagai Waka Polsek Cibeunying Kidul, kemudian tahun 2001 Responden menjabat sebagai Kasat Intel Polresta Bogor Jawa Barat, tahun 2001 sampai dengan tahun 2002 Responden menjabat sebagai Kanit Intel DIT Polda Jabar, setelah menjabat sebagai Kanit Intel DIT Polda Jabar Responden pernah juga menjabat sebagai Kapolsek Lembang di Jawa Barat pada tahun 2002 sampai dengan tahun 2004, kemudian Responden mendapat tugas di Daerah Sulawesi Utara atau Gorontalo pada tahun 2005 Responden menjabat sebagai Kabag OPS Polres Limboto Gorontalo, dan pada tahun 2005 sampai dengan sekarang Responden mendapat kan tugas di Bareskrim Polri menjabat sebagai Penyidik di Unit V IT & Cyber Crime.

Tindak pidana yang pernah ditangani oleh Responden selama menjadi Kapolsek adalah menangani kasus penipuan kemudian penganiayaan, tawuran antar kampung kemudian untuk kasus perampokan. Setelah menjabat sebagai intel Responden sudah tidak pernah menangani perkara karena sebagai penyidik saja.

Responden pernah menangani kasus kejahatan computer selama bertugas di unit cyber crime, yaitu kasus – kasus cyber crime, kemudian software, kemudian kasus hacker partai golkar namun Responden tidak terlibat secara langsung.

Pelatihan-pelatihan yang pernah diikuti oleh Responden selama bertugas sebagai Polisi adalah yaitu pelatihan CETS di Bali yaitu Child and Exploitation Computer Facilities, kemudian pelatihan di Bangkok untuk basic investigation computer, selanjutnya konferensi di Vietnam.

Responden belum pernah mengikuti pelatihan ataupun pembekalan mengenai kejahatan computer ataupun mengenai hacking. Namun demikian Responden pernah mencoba belajar masalah hacking yaitu cara melakukan hacking, bagaimana cara cracking password kemudian masalah injection, Namun tepatnya Responden sendiri belum pernah tembus, cara belajar yang digunakan oleh Responden adalah melalui media baca, kemudian mempelajari dari kasus-kasus yang pernah, selanjutnya konsultasi dari teman yang mungkin pernah kenal masalah hacking. Responden belum pernah melakukan penelitian secara khusus mengenai kejahatan computer maupun mengenai hacking dengan alasan Responden belum mempunyai tujuan untuk melakukan penelitian.

Menurut Responden cyber crime adalah yang pertama, kejahatan yang berhubungan dengan computer, kemudian kejahatan computer itu sendiri. Contoh kejahatan yang berhubungan dengan computer yaitu penggunaan computer dalam kejahatan criminal, contohnya mungkin digunakan untuk penipuan atau pencurian data. Kemudian kejahatan computer sendiri misalnya hacking computer sebagai sasaran kejahatan. Sedangkan hacking secara umum menurut Responden adalah memasuki jaringan orang lain, memasuki jaringan computer orang, bisa menyusup atau dia hanya sekedar menyusup kemudian mengambil data dari situ atau merubah yang ada di dalam jaringan computer orang lain.

Responden belum pernah menangani kasus hacking secara langsung namun hanya membantu rekannya yang kebetulan menangani penyidikan masalah hacking, membantu dengan memberi masukan, kemudian kalau ada kesulitan dibicarakan bersama dalam rapat di kantor

Menurut Responden Manajemen bisa berupa pola yang didalamnya terdapat perencanaan, semua gagasan, pelaksanaan dan pengendalian. Manajemen adalah suatu langkah untuk mencapai tujuan. Terhadap penerapannya menurut Responden Manajemen penyidikan bisa diterapkan dalam menangani kejahatan karena dalam suatu proses pekerjaan menuju suatu tujuan diperlukan suatu manajemen di dalamnya, baik itu perencanaan, kemudian pengorganisasian terutama perencanaan dari anggaran, kemudian langkah apa yang akan digunakan, personil siapa yang harus melaksanakan, kemudian pengendalian sendiri dari pimpinan di kantor.

Dalam kasus hacking website partai golkar sendiri menurut Responden manajemen penyidikan tersebut telah diterapkan dimana pada saat ada kejadian hacking, yang pertama dilaksanakan adalah pembentukan tim untuk penanganan kasus sendiri. Ada beberapa orang yang diunjuk sebagai pelaksana dalam penanganan kasus tersebut. Kemudian ada juga yang melaksanakan tugas. Kemudian setelah pembentukan tim yang akan melaksanakan tugas, baru dilaksanakan penyidikan. Selanjutnya penyidikan dilakukan di Tempat Kejadian Perkara (TKP) maupun penyidikan ke tempat – tempat yang dimungkinkan hacking melaksanakan pekerjaan itu sendiri dan juga perencanaan anggaran daripada pelaksanaan tugasnya, yang terakhir masalah penyidikan setelah kasus tersebut terungkap.

Menurut Responden hal-hal yang perlu diperbaiki lagi mengenai manajemen penyidikan hacking adalah masalah pembagian tugas daripada pelaksana itu sendiri, yaitu siapa berbuat apa, karena berdasarkan pengamatan Responden ada beberapa kendala dalam pelaksanaan tugasnya dalam organisasi itu sendiri, karena mungkin ada beberapa personil yang merasa bukan tanggung jawabnya sehingga saling melempar tanggung jawab ke rekan – rekannya. Kemudian masalah penganggaran, karena selama ini yang menjadi kesulitan Responden di dalam kantor sendiri adalah masalah anggaran, dimana anggarannya memang ada, akan tetapi turunnya sendiri terlambat sehingga kecepatan dalam menangani kasus agak sering terlambat.

Identitas

Nama	: Ibu. P.I.N.L
Pangkat	: AKP
Bagian	: Unit V IT & Cyber Crime DIT II Eksus
Umur	: 41 Tahun
Status	: Menikah
Pendidikan	:

SD Sutomo 1979 Medan
SMPN 10 Medan 1982 Medan
SMA 1985 Medan
SEBA Polwan 1987 Jakarta
SECAPA 2001 Jakarta/Sukabumi

Narasi

Responden menjadi Polisi sejak tahun 1987 dan tugas pertama kali ditempatkan pada bagian Subdit uang palsu (Subdit udpal) Bareskrim Polri bagian analisa dan evaluasi. Pada saat Responden di bagian subdit uang palsu Responden belum ditugasi untuk memegang Mindik. Setelah beberapa tahun Responden dipindah ke unit uang palsu dan waktu itu Responden bertugas di bagian Mindik namun belum disuruh memeriksa, belum disuruh apa-apa selanjutnya setelah beberapa tahun bertugas baru diperbolehkan memeriksa saksi tapi tidak boleh memeriksa Tersangka, yaitu kira-kira dari tahun 1987-1998.

Selanjutnya Responden dipindah lagi ke (PIK) Pusat Informasi Kriminal. Responden bertugas disana kurang lebih 2 (dua) setengan tahun yaitu dari tahun 1998-2000. Pada bagian unit informasi tersebut Responden hanya memegang data-data, selanjutnya pada tahun 2001 Responden masuk CAPA, setelah selesai CAPA Responden ditempatkan di Binfung selama 6 (enam) bulan kemudian ditempatkan di Ekonomi Direktorat 2 Eksus pada Unit Indag selama 3 bulan yaitu pada tahun 2002-2003, dan semenjak itulah Responden menjadi Penyidik. Selanjutnya Responden dipindah ke unit cyber crime Bareskrim Polri pada bagian Mindik yaitu dari tahun 2003 sampai sekarang.

Tindak pidana yang pernah ditangani oleh Responden adalah, tindak pidana uang palsu, merk. Responden pernah ikut terlibat dalam menangani kasus kejahatan komputer, walaupun tidak secara langsung karena hanya bekerja pada bagian Mindiknya saja. Kejahatan komputer yang pernah ditangani oleh Responden adalah kejahatan hacking terhadap website partai golkar dengan Tersangka Iqra dimana Tersangka merubah tampilan website partai golkar menjadi tampilan seekor binatang.

Selama menjadi Penyidik Responden juga pernah mengikuti pelatihan-pelatihan baik dalam negeri maupun diluar negeri seperti seminar-seminar. Dalam unit cyber crime sendiri sering mengadakan pelatihan terhadap para penyidiknya diantaranya yang

pernah diikuti oleh Responden adalah pelatihan tentang n case, pelatihan tentang kejahatan computer di Hongkong dan Singapura, selanjutnya pelatihan tentang kejahatan komputer untuk *geats general explore action trading system* yang diadakan di Bali. Selain itu Responden juga pernah mengikuti seminar tentang Money Laundry di Hongkong, dimana Pembicaranya adalah Bpk. Petrus Golose. Namun pelatihan terhadap hacking sendiri Responden belum pernah mengikutinya.

Menurut Responden dengan adanya pelatihan-pelatihan tersebut sangat berguna bagi Penyidik, dimana Penyidik menjadi tau bagaimana pelaku melakukan kejahatannya seperti bagaimana cara melakukan deface. Untuk menambah pengetahuannya mengenai kejahatan komputer Responden juga mencari tau sendiri melalui internet atau melalui buku. Buku yang pernah dibaca oleh Responden adalah tentang penipuan melalui internet dengan modus Pelaku menggunakan kredit orang lain untuk membeli suatu barang. Namun terhadap hacking sendiri Responden belum pernah belajar

Responden belum pernah mengadakan penelitian mengenai kejahatan komputer karena menurut Responden hal tersebut sangat rumit.

Menurut Responden cyber crime adalah kejahatan didunia maya. Sedangkan hacking sendiri adalah orang-orang yang berkutat didepan komputer mengerjakan segala sesuatu yang berhubungan dengan komputer mungkin karena dia ahli untuk di software.

Responden sudah pernah ikut terlibat dalam menangani kasus hacking yaitu menangani kasus hacking website partai golkar dimana Responden bertugas pada bagian Mindik yaitu membuat surat-surat Sprint Penangkapan, Sprint Penahanan. Sepengetahuan Responden kejahatan yang dilakukan oleh Pelaku dalam kasus tersebut adalah merubah tampilan yang seharusnya tidak boleh ditampilkan. Terhadap pengaturan hacking sendiri menurut Responden sebaiknya tindak pidana hacking diatur dalam undang-undang khusus yang mengatur tentang hacking.

Menurut Responden penanganan terhadap kasus hacking website golkar tidak mengalami kesulitan karena kasusnya sendiri sampai P21. Pada saat ditanyakan mengenai bagaimana seharusnya hukum acara mengakomodasi kejahatan komputer atau hacking Responden menjawab tidak mengetahuinya.

Menurut Responden Manajemen adalah metode yang mengatur segala sesuatu baik organisasi di rumah tangga bahkan juga mengatur diri sendiri. Manajemen tersebut menurut Responden sangat dapat dan harus diterapkan dalam penyidikan karena kalau dilihat dari kasusnya sendiri sudah susah, maka membutuhkan perencanaan yang baik, pengorganisasian, dan pelaksanaan serta evaluasi.

Menurut Responden dalam penyidikan kasus hacking website partai golkar sendiri manajemen penyidikan tersebut sudah diterapkan karena semenjak Laporan Polisi

diterima sudah dimulai dengan proses-proses perencanaan, pengorganisasian, pelaksanaan dan evaluasi. Peranan Responden sendiri dalam kasus tersebut adalah melakukan administrasi penyidikan yaitu membuat Sprintnya, Sprinitif, Sprincitas, dan Sprintganda.

Menurut Responden hal-hal yang perlu diperbaiki lagi mengenai Manajemen Penyidikan adalah mengenai sumber daya manusianya dimana harus dilakukan training, dan juga mengikuti pendidikan.

Identitas

Nama : Bpk. A M
Pangkat : AKP
Bagian : Unit V IT & Cyber Crime Dit II Eksus
Umur : 33 Tahun
Status : Menikah
Pendidikan :

- SD 1987
- SMP 1990
- SMA 1993
- AKPOL 1996 Semarang
- PTIK 2005 Jakarta

Narasi

Responden adalah salah satu Penyidik muda unit cyber crime. Responden lulus pendidikan Akademi Kepolisian tahun 1996. Kemudian Responden mengikuti pendidikan Tinggi Ilmu Kepolisian dan lulus pada tahun 2005. Responden memulai karirnya dengan menjabat sebagai Pamapta C Polres Magetan, kemudian pada tahun 1998 Responden menjabat sebagai Kasat Sabhara Polres Magetan Selanjutnya dari tahun 1999-2000 Responden menjabat sebagai Kapolsek Kawedanan Res Magetan. Menurut Responden pada saat menjabat sebagai Kapolsek sebenarnya sudah mendapat Skep Penyidik, namun tidak menangani secara langsung karena hanya menandatangani berkas perkara. Kemudian pada tahun 2002 Responden menjabat sebagai Kasat Intelkam Res Ngawi, selanjutnya pada tahun 2003 Responden menjabat sebagai Kasat Intelkam Resta Kediri. Menurut Responden pada saat menjabat sebagai Kasat Intel sebenarnya mendapat Skep Penyidik juga namun tidak pernah menyidik karena tugas intel sebenarnya bukan menyidik. Selanjutnya pada tahun 2005 Responden menjabat sebagai Pama Polda Nanggroe Aceh Darussalam dan pada tahun yang sama Responden menjabat sebagai Kassubag Min Ops Biro Ops Polda Nanggroe Aceh Darussalam. Selanjutnya sejak April 2006 sampai sekarang Responden ditempatkan di Bareskrim Polri sebagai Penyidik Muda Dit II unit cyber crime .

Tindak pidana yang pernah ditangani oleh Responden selama menjabat sebagai Kapolsek adalah tindak pidana pencurian biasa sebagaimana terdapat dalam pasal 362 KUHP, tindak pidana pencurian dengan pemberatan sebagaimana terdapat dalam pasal 363 KUHP, tindak pidana penganiayaan dan pengroyokan sebagaimana terdapat dalam Pasal 170 dan 351 KUHP, sedangkan tindak pidana yang pernah ditangani oleh Responden selama bertugas diunit cyber crime adalah tindak pidana penipuan dengan modus menggunakan internet, dan pengrusakan internet.

Responden pernah menangani tindak pidana kejahatan komputer yaitu pengrusakan dengan merubah tampilan website partai golkar menjadi artis Hollywood dan gorilla.

Selama menjadi Polisi Responden pernah mengikuti pelatihan-pelatihan atau pendidikan melalui seminar-seminar baik didalam negeri maupun di luar negeri seperti pelatihan n case di Mega mendung, kemudian pelatihan ceats yaitu *child exploitation agent system* di Bali, selanjutnya mengikuti seminar di Singapura tentang visa dan mengikuti seminar di Malaysia tentang terrorism, serta mengikuti pelatihan di Amerika tentang Botnet yaitu kejahatan yang dilakukan oleh seseorang dengan melakukan penjarahan terhadap server perusahaan atau seseorang dengan menggunakan komputer lain sebagai Zombie atau untuk melakukan penyerangan jadi marimut. Jadi pelaku tidak melakukan kejahatan secara langsung namun dilakukan secara bot hacker untuk mengendalikan komputer dan melakukan penyerangan terhadap sasaran.

Menurut Responden dengan adanya pelatihan-pelatihan tersebut sangat berguna sekali dalam melakukan pekerjaan sehari-hari. Sedangkan pelatihan mengenai hacking sendiri Responden belum pernah mengikutinya.

Oleh karena masih kurangnya pengetahuan Responden mengenai kejahatan komputer, Responden mencari taunya sendiri melalui browsing di Internet dan juga membaca buku-buku tentang pengertian cyber teorism. Selain itu Responden juga suka mencari tau sendiri mengenai hacking melalui buku, berdiskusi dan berteman dengan orang yang lebih ahli mengenai hacking, dimana pada saat mereka menjelaskan bagaimana mengungkap kasus hacking, Responden mendegarkan secara baik-baik, dengan demikian Responden telah mendapat gambaran tentang bagaimana mengungkap kasus hacking. Responden belum pernah melakukan penelitian tentang kejahatan komputer karena menurut Rresponden belum mampu untuk melakukannya.

Menurut Responden cyber crime adalah seseorang yang melakukan tindak kejahatan dengan menggunakan komputer atau jaringan untuk memasuki komputer atau jaringan orang atau pun dengan menggunakan sarana komputer atau jaringan internet untuk melakukan kejahatan. Sedangkan hacking adalah perbuatan atau memasuki jaringan internet komputer orang.

Responden menjelaskan kronologis penanganan hacking website partai golkar adalah pertama-tama Responden bersama teamnya mendatangi Tempat Kejadian Perkara (TKP) website server tempat dimana website golkar ditempatkan, kegiatan tersebut dilakukan untuk mencari tau dimana penyerangnya atau darimana penyerang itu melakukannya, dengan melacaknya dari address-addressnya.

Dalam hal pemanggilan, setelah mendapat laporan adanya hacking terhadap website partai golkar, maka pertama-tama dilakukan pemanggilan terhadap Pelapor yaitu korban sendiri yang dalam hal ini adalah pihak partai golkar, yaitu admin-admin website partai golkar dan orang –orang yang mengetahui kejadian tersebut. Setelah dilakukan pemanggilan, kegiatan selanjutnya adalah melakukan pencarian terhadap Tersangka, dan kemudian pemanggilan terhadap ahli.

Menurut Responden pada saat menangani hacking website partai golkar terdapat kesulitan karena Hukum Acara Pidana tidak mengatur secara.....Menurut Responden seharusnya ada undang-undang tertentu yang mengatur tentang tindak pidana hacking.

Identitas

Nama	: Bpk. S
Pangkat	: AKBP
Bagian	: Penyidik Cyber Crime
Umur	: 43 Tahun
Status	: Menikah
Pendidikan	:

- SD Negeri Siliwangi 1971-1976 Semarang Jawa Tengah
- SMP Negeri 1 1977-1980 Semarang Jawa Tengah
- SMA Negeri 3 1980-1983 Semarang Jawa Tengah
- S-1 FH Universitas Diponegoro 1983-1988 Semarang Jawa Tengah
- S-2 F H Universitas Indonesia 2004-2006 Jakarta

Narasi

Responden lulus pada tanggal 3 Mei 1989. Karir awal Responden adalah Perwira Hukum Polda Nusra dan penempatannya di Bali kemudian tahun 1990-1991 di Pasie Hukum Polwil Tim-Tim Dilli Timor-Timur dibagian Operasi Seroja dan Tim Yustisi, pada tahun 1992 sampai 1994 Responden ditugaskan di Denpasar Bali menjabat sebagai Kaur Bin Diskum Polda Nusra, dan menjabat sebagai Penyidik Pratama Ditserse Polda Denpasar Bali tahun 1995, masih dalam tahun yang sama sampai dengan pertengahan tahun 1998 Responden menjabat sebagai Kasubbag Ops Diserse Polda Denpasar Bali, pada tahun akhir tahun 1998 Responden menjabat sebagai Dan Unit I Korwas PPNS Reserse dan ditempatkan di Koreserse Jakarta sampai tahun 1999, dan tahun 1999 Responden juga menjabat sebagai Penyidik Muda DIT V/Tipiter Bareskrim Jakarta sampai dengan tahun 2003, selanjutnya dari tahun 2004 sampai dengan sekarang Responden menjabat sebagai Penyidik Madya DIT II/Eksus di Bareskrim Polri.

Pada saat bertugas di Bali Responden menangani beberapa tindak pidana diantaranya menangani kasus tanah, kasus penganiayaan, kasus narkoba, kasus orang asing yang melakukan penipuan di Bali dengan menggunakan kartu card berharga, kasus pencemaran lingkungan dan kasus mengenai penanaman modal asing di hotel-hotel. Sedangkan pada saat bertugas di Bareskin Responden menangani kasus yang cukup beragam mulai dari kerusuhan massal di Kalimantan, Sambas, kemudian di Sampit, kasus separatisme di Aceh, kayu Illegal Logging, Illegal meaning masalah batubara, Kalimantan Tengah dan Batam, lalu kasus tentang lingkungan hidup baik pencemaran maupun pengrusakan pinggir pantai alang-alang, kasus-kasus yang melibatkan KSDL konvortasi sumber daya alam baik perikanan kemudian hasil hutan lain, kasus-kasus mengenai hak atas kekayaan intelektual, hak cipta, hak paten bersama dengan unit-

unit dan gabungan dari indag dengan unit-unit tipiter dulu, kemudian kasus-kasus tanah, kasus pencemaran nama baik melalui jaringan atau fasilitas internet, dimana kasus tersebut sudah P 21, kasus software dan kasus tersebut juga sudah P 21, lalu kasus penggelapan di Bank Muamalat dan kasus tersebut juga sudah P 21.

Selain menangani kasus-kasus tersebut diatas Responden juga sudah pernah menangani kasus kejahatan komputer dimana tersangka mengirim email kepada korban kemudian ditembuskan ke beberapa orang yaitu kepada keluarga korban, serta komunitas korban dimana isinya menjelek-jelekkan nama dan kehormatan dari si korban, selanjutnya kasus kejahatan komputer yang lain adalah pelaku menggunakan email address yaitu email address untuk berlangganan di cbn.net.id

Selama menjadi Polisi Responden pernah mengikuti seminar maupun training diantaranya mengikuti pelatihan di Mega Mendung, pelatihan dari FBI maupun dari USSS mengenai crab crime processing training di Mega Mendung termasuk mengikuti pendidikan tentang witness protection, program marketing di Miami Florida selama beberapa bulan, kemudian mengikuti kursus yang diadakan oleh BSDOJ bekerjasama dengan Microsoft di Des Praha Seattle, kemudian kursus di Perbanas pada bagian ITnya dan beberapa seminar-seminar dan workshop yang diselenggarakan di Jepang, Korea dan Filipina.

Terhadap pelatihan mengenai kejahatan komputer sendiri Responden juga sudah pernah mengikutinya yaitu pada tahun 2004 di Korea yang diselenggarakan oleh KOIKA penyelenggara-penyelenggara APEC yaitu tentang internet dan komputer training, pelatihan di KJK bersama dengan kepolisian Jepang yang tergabung dalam CBNS, mengikuti kursus di Perbanas tentang komputer, mengikuti pelatihan n case versi 4 dari Aden Sofware, pelatihan tentang kejahatan internet dan terorism di visilight yaitu bagaimana para pelaku menggunakan sarana IT dan komputer dalam melakukan kejahatannya, pelatihan Botnet pertama di Seattle, Botnet kedua di Praha, dan Botnet ketiga di Seattle.

Menurut Responden hal baru yang dipelajarinya adalah ternyata di balik penggunaan komputer melalui jaringan internet, terdapat celah-celah atau sarana-sarana tertentu dalam hal jaringan internet dan komputer tersebut untuk melakukan berbagai kejahatan, dimana hal tersebut tidak pernah tergambarkan sama sekali oleh Responden. Sebagai contoh Pelaku menggunakan nama palsu untuk seolah-olah menyatakan diri sebagai orang lain kemudian mengambil data milik orang lain tanpa ijin dimana kesemua kejahatan tersebut dilakukan melalui komputer.

Menurut Responden pelatihan-pelatihan tersebut sangat berguna dan membuat kita lebih hati-hati dan lebih teliti khususnya untuk memproteksi bagaimana untuk mengamankan data pribadi, data milik organisasi atau milik kesatuan, data milik instansi dimana kita bekerja misalnya data yang seharusnya tidak boleh keluar dari sarana komputer tersebut harus diamankan baik dengan password maupun dengan

kode-kode akses tertentu atau diberikan personal identification number atau pin yang setidaknya bagi orang lain tidak dapat membuka atau mendapatkannya.

Untuk menambah pengetahuannya mengenai kejahatan komputer Responden suka mencari tau sendiri diantaranya melalui buku. Buku yang pernah di baca oleh Responden adalah buku karangan Wisma Dismantoro tentang kejahatan komputer. Selain itu Responden selalu menyempatkan waktu untuk mencari informasi tentang kejahatan komputer baik di toko perpustakaan maupun di internet. Sehingga Responden tidak perlu menunggu menghadiri seminar atau workshop.

Sedangkan mengenai hacking sendiri Responden mengetahuinya sejak tahun 2004 ketika Responden mengikuti seminar tentang keamanan sistem informasi dan teknologi dalam pemilu 2004 di gedung KPU sekitar bulan februari atau maret tahun 2004 dan pada waktu itu memang tidak ada gambaran mengenai apa itu hacking. Namun setelah terselenggaranya pemilu 2004 sekitar bulan-bulan Mei, Juni terdengar adanya informasi bahwa terjadi perubahan nama-nama para peserta partai politik yang mengikuti pemilu tahun 2004 dan saat itu dari berbagai masukan atau informasi dari Polri maupun diluar Polri ada istilah hacking dan craking, dan terdorong oleh rasa ingin tahu apa itu arti hacking dan cracking, akhirnya Responden mencari informasi sendiri tentang istilah-istilah tersebut melalui media cetak, media elektronik maupun media internet melalui mesin pencari di google maupun yahoo, kemudian mencari informasi dari relasi atau teman kuliah yang menginformasikan ada pengambilan data, pengrusakan data yang ada di komputer oleh orang lain dan meminta konsultasi dari mereka.

Responden belum pernah melakukan penelitian mengenai kejahatan komputer, dengan alasan Responden hanya menulis makalah tentang kejahatan komputer.

Defenisi mengenai cyber crime banyak terdapat dalam berbagai sumber, diantaranya Menurut Prof Muladi di salah satu buku yang dikarang oleh Wisma Dismantoro, menurut beliau cyber crime adalah kejahatan-kejahatan yang tidak atau belum diatur dalam kitab undang-undang hukum pidana dan kejahatan-kejahatan yang konvensional yang didalam melakukan kegiatannya menggunakan sarana telekomunikasi dan informasi, sedangkan hacking adalah mengganti atau merubah atau merusak sesuatu yang sebelumnya sudah pernah ada yang sebagian atau seluruhnya bukan milik dari yang melakukan pengrusakan itu atau yang merubah itu menjadi suatu tampilan yang justru tampilan yang telah dirubah itu tidak dikehendaki oleh sipemilik tampilan ataupun barang ataupun gambaran yang pencipta semula. Sebagai contoh merubah lukisan monalisa menjadi gambar yang lain dengan menggunakan sarana informasi dan teknologi

Responden belum pernah menangani kasus hacking, namun pernah mengikuti paparan mengenai hasil penanganan kasus hacking baik yang ditangani oleh Polda Metro maupun yang ditangani oleh Bareskrim unit cyber crime tahun 2006 yaitu perubahan tampilan yang terjadi di website golkar.org.id. Menurut Responden

seharusnya tindak pidana hacking diatur didalam undang-undang tersendiri karena sampai sekarang ini Indonesia belum memiliki undang-undang yang berkaitan dengan kejahatan cyber crime atau kejahatan komputer secara umum. Menurut Responden harus ada undang-undang dulu sebagai payung hukumnya, baru ada undang-undang dibawahnya yang merupakan breakdown dari undang-undang payungnya. Sebagai contoh undang-undang tentang lingkungan hidup merupakan undang-undang payung untuk undang-undang kehutanan, undang-undang perairan, undang-undang pencemaran lingkungan itu harus ada undang-undang lingkungan hidupnya dulu yang sekarang ini kalau dalam tindak pidana hacking itu merupakan diatur dalam undang-undang tersendiri kemudian undang-undang itu mengacu pada undang-undang tindak pidana komputer secara umum atau luas.

Responden menyarankan sebaiknya hukum acara tentang hacking juga diatur dalam undang-undang tersendiri, karena undang-undang No.8 Tahun 1981 tentang KUHAP belum mengatur secara jelas dan rinci bagaimana menangani kasus tindak pidana komputer termasuk hacking. Jadi didalam undang-undang yang akan mengatur kejahatan hacking ini harus diatur hukum acaranya tersendiri sebagai contoh misalnya bagaimana seorang penyidik itu untuk mendapatkan suatu barang bukti berupa data berupa informasi berupa angka ataupun tulisan dan gambar yang dirubah dari komputer atau pun jaringan yang itu harus dilakukan secara transparan dan diketahui oleh semua pihak jadi harus ada aturan-aturan yang jelas dalam hukum acaranya

Menurut Responden Manajemen adalah suatu metode atau suatu sistem dimana kita akan mendapatkan sesuatu atau untuk mendapat tujuan tertentu kita harus melalui berbagai proses tahapan dan persyaratan-persyaratan tertentu yang semuanya itu diatur secara rinci dan jelas dalam suatu rangkaian kata-kata atau kalimat dan dituangkan dalam bentuk tulisan yang secara integral yang nantinya berguna didalam menuntun suatu proses atau kegiatan kita, mendapatkan atau melakukan perbuatan tertentu. Jadi manajemen adalah suatu cara untuk mengatur dan mengarahkan suatu pekerjaan atau suatu kegiatan dalam mendapatkan dalam melakukan kegiatan atau pekerjaan.

Menurut Responden Manajemen merupakan suatu keharusan yang wajib dilaksanakan dalam melakukan penyidikan atau penyelidikan kasus hacking, dimana harus ada manajemen yang jelas runtut dan focus dengan persyaratan-persyaratan tertentu yang sesuai dengan prosedur yang sudah disepakati bersama karena apabila tidak diatur secara manajerial atau terarah penyelidikan dan penyidikannya tidak akan runtut jadi justru akan loncat-loncat mana yang didahulukan dan mana yang dipertengahan dan mana yang pada saat kesimpulan jadi sudah kebutuhan pokok.

Menurut Responden dalam penanganan kasus hacking website golkar sendiri manajemen penyidikan tersebut telah diterapkan walaupun masih terdapat kekurangan oleh karena kasus hacking merupakan hal yang baru di unit cyber crime, maka penyidik tidak siap sama sekali sehingga ada sedikit tempo yang seharusnya

bisa dilakukan banyak hal namun tidak bisa dilakukan, misalnya mengenai pengamanan barang bukti. Barang bukti tersebut tidak dapat langsung diamankan karena berdasarkan informasi pertelepon harus menunggu, selanjutnya satu atau dua orang anggota penyidik itu datang ketempat TKP yaitu dimana kantor golkar berada kemudian di ISP yang disewa oleh golkar untuk ditempatkan diserver atau database nya dan juga termasuk dikantor penyidik hal tersebut dilakukan untuk membuka kemudian mengamankan tampilannya apakah benar telah terjadi hacking terhadap website golkar tersebut.

Kekurangan selanjutnya adalah oleh karena sifatnya menunggu, maka akan kehilangan berbagai hal yang penting. Dengan demikian dibutuhkan kecepatan dan ketepatan didalam melakukan pengamanan terhadap barang bukti. Selain itu menurut Responden masih terdapat kekurangan yang lain yaitu mengenai dukungan sarana khususnya alat untuk menganalisa database ataupun barang bukti. Kurangnya dukungan anggaran yang cukup memadai dalam kasus tersebut menurut Responden mengakibatkan kurang maksimalnya hasil kerja penyidik karena seharusnya dalam waktu bersamaan penyidik dapat melakukan pengecekan terhadap dua tiga tempat pemilik IP yang dilakukan secara simultan.

Menurut Responden hal-hal yang perlu diperbaiki dalam penerapan penyidikan kasus hacking adalah penyusunan suatu metode atau sistem yang dikelompokkan dalam standard operating dan prosedur khusus dalam penanganan kasus hacking karena penanganan kasus hacking berbeda dengan kasus-kasus yang lain yang menggunakan sarana komputer dimana dalam kasus hacking apabila kita lengah selama lima menit sampai satu jam maka akan kehilangan database karena sengaja dibuang atau di musnahkan atau dihilangkan dari tampilannya oleh Pelaku.

Selain itu menurut Responden sebaiknya diusulkan adanya semacam tim terpadu atau team refleks out seminggu atau tiga minggu sekali, sebagai antisipasi apabila ada ancaman kejadian hacking karena hacking tidak bisa diprediksikan bisa dalam 1 menit 2 menit, bisa satu jam bahkan setiap saat terjadi. Jadi satu tim standby secara fisik dikantor maupun secara komunikasi mobile dimasing-masing tempat. Selanjutnya melakukan pelatihan secara terorganisir dan berkala, misalnya satu atau tiga bulan sekali bersama-sama penyidik diwilayah dan juga mendapatkan informasi-informasi dari yang lain.

Selanjutnya dukungan sarana dan prasarana yang memadai khususnya alat-alat sarana yang cukup signifikan baik teknologi maupun kehandalannya dan juga anggaran yang sangat memadai dan yang paling penting adalah dukungan saksi ahli yang berkompeten dibidang kejahatan komputer. Selanjutnya pembentukan tim-tim hacking diwilayah karena wilayah Indonesia sangat luas jadi kejadian hacking tidak harus terjadi di Jakarta atau pelakunya di Jakarta saja tapi dikota-kota besar di Indonesia dan juga bisa juga pelakunya terjadi atau melakukannya di kota-kota kecil yang telah memiliki sarana informasi dan teknologi. Selanjutnya kerja sama dengan pihak internasional atau negara-negara lain yang telah memiliki pengalaman budaya,

memiliki ilmu pengetahuan dan sarana prasarana yang sangat memadai didalam mengungkap kasus hacking.

Identitas

Nama	: Ibu. L
Pangkat	: AKP
Bagian	: Unit V IT & Cyber Crime Dit II Eksus
Umur	: 36 Tahun
Status	: Menikah
Pendidikan	:

- SDN 01 1983 Jakarta
- SMPN 143 1986 Jakarta
- SMAN 73 1989 Jakarta
- D III (Diploma 3) Keuangan dan Perbankan 1993

Narasi

Latar belakang pendidikan Responden adalah D3 Perbankan. Responden lulus Susapeka pada tahun 1996. Pertama kali bertugas Responden ditempatkan di Mabes Polri yaitu pada Korp Reserse unit Perbankan dari tahun 1997 sampai tahun 2000. Pada saat bertugas di Mabes Polri, Responden berada dibawah PIN-nya Bapak Basuki dimana pada saat itu Responden belum pernah menangani kasus secara langsung akan tetapi hanya membantu Timnya Bapak Basuki membongkar kasus-kasus lama yang belum sempat diselesaikan. Selanjutnya Responden dipindah ke unit import export (Impeks), yang dipimpin oleh Bapak Edy Wardoyo. Pada saat bertugas di Impeks, Responden mempunyai tugas membantu memeriksa saksi-saksi kasus selundupan baju-baju bekas, dimana dulu Tersangka utamanya adalah Pak Abi, namun kasusnya sampai sekarang belum selesai. Saat ini Responden bertugas sebagai Penyidik Unit V IT & cyber crime Mabes Polri.

Selain bertugas di unit Impex Responden juga ditempatkan pada unit Infotech yaitu pada bagian Surat Perintah (Sprint), yang dipimpin oleh Pak Brata Mandala, selain Responden, Pak Edy Purnama juga bergabung di bagian Sprint tersebut.

Menurut Responden orang-orang tidak ada yang mau di unit infotech, karena belum ada ruangan khusus untuk unit infotech dan ruangannya masih bergabung dengan ruangan Indag, sampai-sampai Kanitnya marah. Sebenarnya Kanitnya pun merasa kurang nyaman bergabung dengan ruangan unit Indag, karena tidak mungkin dalam satu ruangan terdapat dua dokumen yang ditangani. Sehingga Kanitnya turun duluan kebawah bergabung dengan ruangan Pak Ud.

Menurut Responden, pada saat bertugas di infotech sempat menjadi bingung mau menjalankan perintah yang mana karena pada saat itu Responden belum ada tugas dari direktur untuk kasus-kasus infotech, namun hanya membalas surat-surat dari MCB mengenai komplain-komplain penipuan melalui internet. Sedangkan yang

berhubungan langsung secara komunikasi adalah Pak Brata sendiri dimana pada saat itu terdapat kasus Rotok Sembiring yaitu penipuan melalui pemesanan barang alat-alat musik yang terjadi pada tahun 2003 dan sampai saat ini kasusnya kurang jelas penanganannya.

Awalnya Responden tidak mengetahui mengenai kejahatan komputer karena pada saat di unit Perbankan Responden hanya mengetik surat dan membuat BAP.

Tindak pidana yang secara spesifik pernah ditangani oleh Responden adalah tindak pidana perbankan, tindak pidana penipuan, penggelapan dan penyelundupan.

Responden sudah pernah menangani kasus kejahatan komputer namun tidak terlibat secara langsung, karena hanya bertugas pada bagian administrasinya saja. Perkara yang pernah ditangani oleh Responden secara langsung yaitu kasus Penipuan SMS melalui handphone Nokia.

Mengenai pelatihan sendiri Responden pernah mengikuti pelatihan di Thailand tentang hack crime pada tahun 1998, selanjutnya di Singapura. Selain itu Responden pernah belajar ilmu komputer di Perbanas, kemudian pelatihan n case empat (4) mengenai kejahatan komputer, namun untuk yang n case 6 (enam) Responden belum pernah mengikutinya. Sedangkan mengenai hacking sendiri Responden belum pernah mengikutinya.

Walaupun Responden tidak terlalu memahami mengenai komputer ataupun kejahatan komputer, namun Responden suka membaca-baca buku tentang kejahatan komputer, dan juga mencari tau melalui internet sedangkan mengenai hacking sendiri Responden belum pernah membacanya.

Responden belum pernah mengadakan penelitian mengenai kejahatan komputer, karena menurut Responden ilmu yang didapatnya selama ini belum sampai kesana, ilmu yang gampang saja Responden belum terlalu memahami apalagi yang susah, tapi pada prinsipnya Responden berusaha untuk belajar memahaminya.

Menurut Responden cyber crime adalah kejahatan didunia maya yang menggunakan sarana komputer atau alat tekhnologi yang lain. Sedangkan Hacking adalah merubah tampilan, jadi yang dirubah hanya tampilannya saja.

Responden belum pernah menangani kasus hacking, kecuali administrasi misalnya membuat surat untuk pemanggilan saksi, membuat surat penetapan, penggeledahan, penyitaan. Dalam hal pemberkasan perkara Responden hanya membuat daftar berkas perkara.

Tindak pidana yang dikenakan pada kasus hacking website golkar adalah tentang pencemaran nama baik. Responden menyarankan sebaiknya tindak pidana hacking diatur dalam undang-undang khusus yang mengatur kejahatan komputer.

Menurut Responden Manajemen adalah suatu sistim yang mengatur suatu kegiatan untuk mendapatkan suatu hasil yang diinginkan. Misalnya Perencanaan, pengorganisasian, analisa dan pengendalian. Menurut Responden Manajemen Penyidikan sudah diterapkan dalam penyidikan kasus hacking dan Manajemen Penyidikan tersebut perlu diterapkan untuk tercapainya apa yang kita inginkan.

Menurut Responden dalam penyidikan hacking website partai golkar sendiri Manajemen Penyidikan sudah diterapkan karena sudah ada perencanaan dan analisa.

Menurut Responden hal-hal yang perlu diperbaiki lagi dalam Manajemen Penyidikan adalah sebaiknya segala sesuatunya harus di rencanakan secara betul-betul, apa yang harus diperbuat, kemudian bagaimana penanganan barang bukti karena harus hati-hati sebab berkaitan dengan bukti digital yang mungkin semua orang belum pernah tahu. Selanjutnya koordinasi atau kerjasama dengan ahli yaitu meminta pendapat ahli dalam artian supaya tindakan yang dilakukan tidak salah, karena masih kurangnya pengetahuan penyidik mengenai kejahatan komputer.

Identitas

Nama	: Ibu Lks
Pangkat	: AKBP
Bagian	: Unit V IT & Cyber Crime Dit II Eksus
Umur	: 49 Tahun
Status	: Menikah
Pendidikan	:

- SD Santa Angela tahun 1970
- SMPN XII tahun 1976
- SMAN XI Bulungan 1979
- IKIP Jakarta 1983
- SEPAMILSUKWAN Polri tahun 1984
- DIKJUR PASERSE 1985.

Narasi

Responden sudah hampir 23-24 tahun bekerja di Kepolisian. Jenjang pendidikan Responden dimulai dengan mengikuti Sepa Milsukwan tahun 1984 di Sukabumi kemudian Dikjur PA Serse tahun 1985 di Megamendung. Sedangkan pelatihan dan training yang pernah diikuti oleh Responden selama menjadi Polisi adalah Training Pollution Respect No Boundaries US EPA Region 10 Seattle Washington USA tahun 1996, Training Narcotic Law Enforcement US-DEA di Jakarta tahun 1997, Training On Control Drug Offences III di NPA And JICA di Tokyo Japan tahun 2001, Training Drug Unit Commanders dari US-DEA di Jakarta tahun 2005, Training Incident Response Cyber (IRC) dari USA-ATA di Megamendung tahun 2006, Training Cets di TNCC Jakarta Indonesia tahun 2006, Penempatan di Innocent Images International Task Force pada FBI-IINI HQ di Calverton Maryland Amerika tahun 2006, Cets International Meeting di Roma pada Italian National Polce HQ.

Tugas pertama kali Responden ditempatkan di Parespem Unit Jitkaor Sattama Serse Krim Koserse Polri pada 08 November 1984, kemudian pada tanggal 01 Maret 1985 Responden ditugaskan di Panit SAT IDIK Harda Subdit Serse UM Dit Serse Polri, selanjutnya pada tanggal 01 November 1997 bertugas sebagai DANUNIT I SAT Idik Tropika Dit Serse Narkoba Korserse Polri, dan menjabat sebagai Kabag Anev Ditserse Narkoba Korserse Polri pada tanggal 01 Maret 2000, kemudian pada tanggal 11 Desember 2001 Responden menjabat sebagai Kasubbag Binops DIT Serse PID Narkoba Korserse Polri, selanjutnya pada tanggal 08 September 2003 Responden bertugas di Bareskrim Polri menjabat sebagai Penyidik Madya Unit I DIT IV/TP Narkoba dan OC Bareskrim Polri, pada tanggal 25 April 2005 sampai dengan sekarang menjabat sebagai Penyidik Madya Unit V Dit II/Ekonomi dan Khusus Bareskrim Polri karena mutasi penempatan.

Sebagai petugas polisi Responden mempunyai beberapa pekerjaan diantaranya melakukan penyelidikan terhadap website PUBER 18 pada tahun 2005, website

porno pada tahun 2006 dan penyidikan cyber crime, selain itu Responden juga pernah terlibat dalam penyidikan kasus Cyber Pornography, Pencemaran nama baik di Internet, dan Pencabulan Anak.

Menurut Responden Struktur Organisasi Unit V IT & cyber Crime adalah mengacu pada struktur organisasi Bareskrim dimana terbagi atas bagian penyidikan dan Lab Forensic, untuk bagian penyidikan dibuat dengan sistem flat dengan maksud semua anggota polri di unit V IT & Cybercrime mampu melakukan penyidikan. Namun demikian controlling untuk pelaksanaan tugas sehari-hari adalah dari Kanit dan didelegasikan kepada Pamen yang dituakan. Mengenai rantai komando yang diterapkan dalam unit V IT & cyber crime adalah Penyidik/anggota Unit V IT dan bagian lab forensic bertanggung jawab langsung kepada Kanit tetapi dapat juga bertanggung jawab kepada pamen yang dituakan pada saat Kanit tidak ditempat.

Wewenang dan pekerjaan lab adalah specialisasi di bidag lab digital forensic yaitu melaksanakan kegiatan pemeriksaan digital evidence yang diberikan penyidik. Wewenang dan pekerjaan penyidik unit V IT & Cyber crime adalah melaksanakan kegiatan penyelidikan dan penyidikan dengan kewenangan penyidik yang diatur dalam KUHAP dan UU. Menurut Responden struktur organisasi Unit V It & cyber crime saat ini sudah cukup baik, dan untuk sementara tidak perlu dirubah tetapi untuk kedepannya mungkin perlu dirubah sesuai kebutuhan.

Dengan mengacu pada visi dan misi Bareskrim Polri menurut Responden Visi dan Misi Unit V IT & Cybercrime adalah menjadi penyidik Polri (Cyber Cop) yang professional dalam penegakan hukum di cyber space dan kejahatan yang berhubungan dengan tekhnologi informasi serta meningkatkan kemampuan komputer. Sedangkan misinya adalah meningkatkan pengetahuan dan keterampilan penyidik sebagai penyidik cyber dan pelayan masyarakat; Menjalin kerjasama dengan sesama aparat penegak hukum (CJS), professional, instansi terkait, universitas dan masyarakat dalam rangka penegakan hukum di bidang tekhnologi informasi; Meningkatkan koordinasi dan kerjasama dalam pengungkapan dan penanggulangan kejahatan transnasional khususnya kejahatan cyber dengan aparat penegak hukum negara lain/Internasional; Menjadi pusat informasi, pengawasan dan penindakan kejahatan cyber dengan mengedepankan laboratorium komputer forensic.

Visi dan misi tersebut dijabarkan dalam program kerja Unit V IT & Cybercrime yaitu dengan mengikutsertakan anggota cyber crime untuk training/pelatihan di Luar Negeri dan Dalam Negeri, mengadakan pertemuan atau rapat koordinasi dengan CJS, bekerjasama baik dalam bidang penyidikan maupun pelatihan dengan pihak Luar Negeri. Menurut Responden pembuatan visi dan misi melibatkan seluruh anggota unit V IT & Cyber Crime.

Responden menggambarkan manajamen organisasi Unit V IT & Cybercrime yaitu berdasarkan keputusan Kapolri No.Pol.:Kep/54/X/2002 tanggal 17 Oktober 2002 adalah unsur pelaksana pada Direktorat II Ekonomi dan Khusus Bareskrim Polri yang

bertugas melaksanakan Penyelidikan dan Penyidikan tindak pidana dunia maya (*Cyber Crime)* terutama kegiatan yang berhubungan dengan teknologi informasi (teknologi komputer, teknologi telekomunikasi, teknologi elektronika dan teknologi penyiaran) dan menyelenggarakan fungsi laboratorium Komputer Forensik dalam rangka memberikan dukungan teknis proses penyidikan Cyber Crime.

Perencanaan dalam program kerja Unit V IT & Cybercrime adalah menyesuaikan perencanaan organisasi pada Bareskrim, dan Pelaksanaan program kerja dijabarkan pada regiant unit V IT & Cyber Crime, Evaluasi perencanaan dalam organisasi unit V IT & Cyber Crime meliputi perencanaan penyidikan, operasional, dan perencanaan capacity building, training berkaitan dengan anggaran kemudian Evaluasi secara umum berjalan baik. Menurut Responden Perencanaan dibuat oleh seluruh anggota cyber dalam rapat anggota pimpinan Kanit dan dilaksanakan pada mingguan, bulanan, harian dan sebagainya.

Menurut Responden terhadap perencanaan dan pelaksanaan Unit V IT & Cybercrime mengenai Pengelolaan sumber daya manusia dalam Seleksi Perekutan, Pengenalan, Peningkatan sumber daya manusia, Jenjang karir adalah tidak dilakukan Seleksi, dan perekrutan dilakukan melalui personil Bareskrim; Pengenalan dilakukan training dan diikut sertakan dalam penyidikan; Peningkatan SDM melalui training baik dalam dan luar negeri; Jenjang karir dengan sendirinya, pengajuan Kanit Cq Dir Ke Pers.

Mengenai peningkatan infrastruktur terhadap laboratorium forensic yaitu mengenai pengadaan alat pelatihan menurut Responden Pengadaan alat selalu dilakukan baik bantuan maupun dari dinas dan pelatihan.

Unit V IT & Cybercrime melakukan perluasan Net working baik terhadap instansi yang terdapat dalam tubuh Polri maupun di luar Bareskrim Polri. Untuk instansi yang terdapat dalam tubuh Bareskrim Polri, Unit V IT & Cybercrime selalu menjalin hubungan dengan unit lain dan direktorat lain seperti Densus 88, sedangkan kerjasama dengan pihak diluar tubuh Bareskrim misalnya Brimob, APJI, Microsoft, Kominfo, ICYTAP. Selain itu menurut Responden Unit V IT & Cybercrime melakukan juga perluasan net working dengan penegakan hukum yaitu sosialisasi, dimana Kanit sebagai pembicara, pelaksanaan penyidikan. Terhadap penggalangan dana Sumber dana Polri, menurut Responden kadang ada kadang tidak, sedangkan sumber dana lainnya berasal dari Pelapor atau dana pribadi Kanit.

Menurut Responden yang paling berperan dalan pelaksanaan adalah adanya pengawasan langsung dari Kanit, yaitu mengkoordinasikan pelaksanaan, menawarkan pilihan-pilihan penyelesaian masalah, dan terhadap pengambilan keputusan sepenuhnya ditangan Kanit.

Menurut Responden alur masuknya perkara di Unit V IT & Cybercrime sampai dengan pelimpahan berkas perkara ke Kejaksaan atau penghentian perkara adalah

dengan one gate system yaitu dapat berdasarkan info setelah dilakukan penyelidikan dan ditemukan bukti yang cukup kemudian dituangkan laporan polisi A 1 yaitu penyidik sebagai pelapor, dapat berdasarkan laporan yang dibuat oleh pelapor setelah pelapor berkonsultasi dulu di Unit V IT & Cybercrime berdasarkan hasil penelitian sementara ada BB printout dari Internet dsb. Dapat juga berupa informasi dan terus akan menjadi informasi sebelum ditemukan bukti-bukti yang cukup setelah dilakukan penyidikan untuk diangkat menjadi laporan polisi. Di Laporan Polisi dilakukan pengumpulan barang bukti terkait browsing di internet.

Dalam alur tersebut terdapat proses penyidikan, maka apabila ditelaah dari segi Perencanaan, pelaksanaan dan evaluasi, menurut Responden Perencanaan dilakukan oleh penyidik yang bersangkutan dan dilemparkan ke anggota unit V IT Cybercrime dalam diskusi untuk mendapat masukan dan pelaksanaan oleh penyidik dan team sedangkan evaluasi perkara tuntas dapat P.21 serah terima tanggung jawab tersangka dan Barang Bukti, diberikan tidak cukup bukti, di 87 ke kewilayahan dan yang paling bertanggung jawab atas pelaksanaan penyidikan kasus dalam Unit V IT dan Cybercrime adalah Kanit dimana secara berjenjang telah diatur dalam Tupok Polri 2007

Terhadap fungsi pengawasan terhadap proses penyidikan di Unit V IT & Cybercrime, menurut Responden fungsi pelaksanaan secara berjenjang dimana Kanit mengawasi anggota, Direktur mengawasi Kanit, Kaba mengawasi Direktur, dalam unit V IT Cyber crime diantara pamen saling mengawasi terhadap anggota pama.

Dalam setiap kasus yang ditangani tentu saja tidak semuanya dapat terungkap, oleh karenanya menurut Responden apabila terdapat kasus yang tidak terungkap maka tindakan yang dilakukan adalah menghentikannya dengan dasar tidak cukup bukti dengan diawali dengan gelar perkara oleh penyidik ditingkat unit. Bila diperlukan diangkat ditingkat Ro Analis untuk mendapat masukan dan menjadi keputusan Penyidik dan diketahui oleh Pimpinan dan anggota/pejabat-pejabat terkait.

Identitas

Nama	: Bapak G N
Pangkat	: AKBP
Bagian	: Unit V IT & Cyber Crime DIT II Eksus
Umur	: [*] Tahun
Status	: Menikah
Pendidikan	:

Narasi

Responden menjelaskan struktur organisasi unit V IT & Cyber Crime yang ada pada saat ini merupakan bentukan Kep 54 tahun 2002 dimana terdapat beberapa unit direktorat kemudian turun menjadi unit kanit. Kemudian posisi Cyber crime sendiri berada dibawah direktorat II yang seyogyanya mungkin saat ini bentukan yang terjadi tidak Kanit tetapi adalah sub unit. Wewenang dan pekerjaan dari struktur organisasi tersebut adalah sampai detik ini yang ada hanya kanit kemudian turun ke penyidik, penyidik madya, penyidik muda, sedangkan pembagian yang lain belum bisa terstruktur sebagaimana yang telah diatur dalam kep yang ada, dan terhadap rantai komando yang ada Responden menjelaskan bahwa pembagian tugas hanya pada pertanggungjawaban dalam proses penyidikan dimana seharusnya ada beberapa sub unit namun hal ini belum dicanangkan menjadi sub unit yang diakui terstruktur, sehingga unit cybercrime hanyalah penyidik, tidak ada laboratorium cybercrime, CETS dan sebagainya. Terhadap pertanggungjawaban pekerjaan baik penyidik madya maupun penyidik muda bertanggungjawab kepada kanit secara struktur dan secara fungsional mereka bertanggung jawab secara pribadi.

Menurut Responden yang melakukan perencanaan berkaitan dengan struktur organisasi berpedoman pada program kerja, yaitu progiat (program kegiatan) yang dilakukan di direktorat sehingga nanti turun menjadi kegiatan yang dilakukan oleh unit. Program penyusunan perencanaan berada dibawah kendali kanit dengan mendiskusikan kepada seluruh anggota, dalam pelaksanaannya tentunya yang melaksanakan adalah anggota, sedangkan pengawasan dilakukan adalah kanit.

Responden menjelaskan bahwa struktur organisasi yang ada saat ini diperlukan pengembangan mengingat tantangan yang dihadapi kedepan sehingga kedepannya unit cybercrime menjadi sebuah direktorat karena berdasarkan kasus-kasus yang ada saat ini sudah dapat mengakomodir daripada beberapa direktorat yang ada di bareskrim. Namun kekurangan dari struktur organisasi yang flat seperti sekarang tidak adanya suatu rantai kemampuan yang berlapis-lapis dimana menurut Responden apabila terdapat SDM-SDM yang memiliki kemampuan maka akan lebih terkendali dan meminimalisasi serangan dari luar.

Sebuah visi dalam suatu organisasi tidak terlepas dari visi Negara, kemudian visi Negara turun ke visi daripada Polri itu sendiri, selanjutnya dijabarkan pada visi

Bareskrim sampai menembus pada visi Direktorat, sedangkan visi daripada unit sendiri adalah untuk meminimalisasi iklim daripada terjadinya suatu kejahatan yang berinvestasi khususnya terhadap informasi dan tekhnologi yang ada di Indonesia, dimana yang membuat visi dan misi tersebut adalah kanit bersama anggotanya.

Responden menjelaskan visi dan misi yang mendasari program kerja terhadap pekerjaan yang ada sehingga menjadi program kegiatan dan menjadi sasaran prioritas yang akan diutamakan dan semua anggota Unit V IT & Cybercrime terlibat dalam pembuatan visi dan misi tersebut. Menurut Responden visi yang ada sekarang ini sudah cukup baik, namun terhadap misi yang ada sekarang ini perlu dievaluasi lagi, misalnya misi dalam peningkatan sumber daya manusianya dan penyediaan sarana dan prasarana dan anggaran dari unit.

Menurut Responden manajemen adalah suatu proses kegiatan, yang secara sistematis mulai dari remorlatda dengan memanfaatkan sumber daya yang ada, main materiil untuk mencapai tujuan. Manajemen organisasi sendiri yang ada di Unit V IT & Cybercrime sudah berjalan sebagaimana yang sudah ada, namun terhadap waskaya perlu diitngkatkan lagi, selanjutnya dari sisi sumber daya yang ada terkait dengan masalah kegiatan yang sudah ada, karena secara implementasinya sumber dayanya masih terbatas, kemudian anggaran juga selama ini tidak terakomodir oleh dinas karena masih ada kesenjangan kemudian terhadap metodenya juga perlu diitngkatkan yaitu soal materiil, walaupun saat ini sudah memiliki alat-alat yang canggih namun ada hal-hal baru yang perlu ditingkatkan lagi.

Tahapan-tahapan proses manajemen penyidikan terdiri dari perencanaan, dimana dalam proses perencanaan terdapat Wasdaya, gelar perkara, dalam unit V IT & Cybercrime sendiri perencanaan secara umum tergambarkan dalam rencana kegiatan yang sudah ada, namun dalam hal penanganan kasus masing masing anggota diberi tanggung jawab terhadap apa yang harus dilakukan dalam proses awal sampai dengan selesai selanjutnya dilakukan proses evaluasi terhadap pekerjaan yang dilakukan. Evaluasi dilakukan oleh tim dan kemudian dilakukan petunjuk oleh Kanit untuk menangani setiap permasalahan yang muncul di Unit V IT & Cybercrime. Responden menjelaskan secara umum perencanaan dibuatkan secara bersama sama yang dipimpin oleh Kanit, untuk memecahkan terhadap apa yang akan direncanakan dengan mengevaluasi permasalahan yang sebelumnya dengan berpijak, berawal, bertolak dari kasus kasus yang sebelumnya secara bersama-sama yang melibatkan seluruh anggota termasuk Responden sendiri. Namun terhadap pelaksanaan dari perencanaan tersebut pada faktanya apa yang dikerjakan terlalu lama prosesnya, tidak seketika bisa dipenuhi dan alat-alat yang ada secara umum semuanya merupakan suatu bantuan dari luar. Adanya suatu keterlambatan dalam hal proses pengadaan, juga akan mempengaruhi dalam proses kinerja dari unit sendiri.

Perencanaan biasanya dilakukan pada awal tahun anggaran dengan mengevaluasi daripada kasus kasus yang ada dengan melihat presentasi daripada pekerjaan yang sudah dilakukan kemudian ditindaklanjuti dengan program-program yang akan

dilakukan kedepan dengan alokasi waktu yang sudah ditentukan selama kurun waktu triwulan, bisa pertengan tahun, sampai setahun.

Terhadap proses seleksi yang dilakukan tidak bersikap open manajemen tapi close manajemen, dimana kita menerima langsung dari atas. Dalam unit V IT & Cybercrime sendiri sering diusulkan untuk pengembangan diri tapi selalu berbenturan dengan quota dan sebagainya. Selanjutnya terhadap peningkatan kemampuan anggota sendiri sudah berjalan dan tersusun dengan baik dimana sudah dilakukan suatu kegiatan tambahan pengenalan suatu materi atau informasi baru yang dilakukan secara internal polri maupun diluar internal polri atau eksternal, dalam arti kata dilakukan dengan kerjasama dengan beberapa institusi diluar untuk bisa memberikan kemampuan pada para anggota.

Kaitan antara perencanaan dalam hal peningkatan kesadaran masyarakat terhadap penegakan hukum menurut Responden Perencanaan dilakukan secara selektif prioritas dalam arti kata setiap penanganan dilakukan secara kritis mana yang akan didahulukan, dan khusus dalam penegakan hukum, maka pelaksanaannya dilakukan secara lebih transparansi dalam proses penyidikannya kemudian sistem pelaporan dan percepatan dalam penanganan kasus itu sendiri. Jika dikaitkan perencanaan dengan sumber pendanaan menurut Responden pengajuan dana selama ini berkesinambungan antara dana yang diajukan dengan dana yang diperoleh, didalam tubuh polri itu sendiri tidak mengalokasikan. Dalam penanganan kasus cybercrime sendiri tidak dapat diprediksikan apakah case ini akan membutuhkan anggaran besar sehingga harus ada dana taktis sendiri yang harus diberikan sebagai posting negara. Dalam pelaksanaannya mereka akan diminta suatu pertanggungjawaban berbasis kinerja yang dibuktikan dengan bukti-bukti administrasi pendukung untuk mendapatkan keakuratan dari pertanggungjawaban. Menurut Responden selama ini untuk mendukung sumber dana yang ada selalu diupayakan dan diusahakan oleh Kanit sendiri, namun Responden merasa pesimis apakah hal tersebut akan tetap berlanjut apabila terjadi pergantian kepemimpinan, karena untuk pemimpin yang sekarang selau memperhatikan dan mengupayakan sumber dana sedangkan Pemimpin yang akan menggantikannya belum tentu berbuat hal yang sama.

Terhadap pengawasan dalam Unit V IT & Cybercrime dilakukan oleh Kanit, dimana Kanit memberikan peluang kepada masing-masing anggota untuk berkreativitas untuk melakukan dan berupaya seoptimal mungkin dalam menyelesaikan tugas-tugasnya. Proses waskanya dilakukan dengan sistem pelaporan yang disampaikan kepada kanit yang dilakukan secara langsung maupun secara tidak langsung, dan seyogianya yang mengkoordinasikan pelaksanaan adalah ketua tim yang dibentuk tapi dalam hal *sign person* maka *person* itu yang akan mempertanggungjawabkan apa yang dilaksanakannya kepada kanit.

Dalam hal penawaran penyelesaian menurut Responden penawaran penyelesaian terhadap kasus-kasus yang ada selama ini dilakukan dengan mengadakan suatu pembagian, dimana ada kasus yang langsung dari Kanit karena keterbatasan personel

yaitu dengan membentuk tim untuk mempercepat proses efektifitas dan efisiensi kasus, dan selanjutnya tim akan menyelesaikan kasus-kasus tersebut dengan memberikan suatu pertanggungjawaban secara fungsional dan struktural kepada Kanit dan yang mengambil keputusan dan merubah rencana adalah Kanit juga. Selain itu terhadap evaluasi kerja juga dilakukan oleh Kanit dengan penjelasan daripada masing masing yang mempunyai beban tugas pelaksanaan, termasuk Responden sendiri juga dilibatkan dalam pelaksanaan evaluasi hasil kerja, dan evaluasi dilakukan pada tahap awal penentuan kasus atau masalah, pada pertengahan dan pada tahap akhir.

Adapun parameter sukses terhadap kasus yang ditangani adalah apabila kasus dapat diselesaikan tepat waktu atau lebih awal dari waktu yang telah ditentukan dan semuanya bisa dipertanggungjawabkan secara administrsi. Sedangkan penanganan suatu kasus dikatakan gagal apabila program yang ada tidak dilaksanakan sebagaimana mestinya.

Responden menjelaskan pemimpin unit V IT & Cybercrime sangat menghargai angggotanya dimana apabila ada anggota yang sukses melakukan suatu program kerja maka Kanit akan reward berupa ucapan maupun insentif untuk memacu kinerja mereka, sama halnya apabila ada anggota yang gagal dalam melaksanakan tugas maka Kanit akan memberikan suatu teguran untuk pembenahan, sehingga yang bersangkutan berubah untuk melaksanakan tugas lebih baik. Dengan adanya evaluasi tersebut tentunya akan berpengaruh terhadap rencana kedepan, karena dari proses evaluasi itu sendiri berpijak pada hasil presentase daripada yang dicapai, sehingga kasus perencanaan nantinya akan mengkompulir permasalahan-permasalahan yang ada kemudian melihat target yang akan dicapai semua akan dirangkum dalam pembicaraan ini untuk masa kedepan dengan schedule waktu, alokasi waktu, dengan kekuatan yang ada untuk dilakukan dalam proses kegiatan pelaksanaan. Sedangkan evaluasi terakhir ada termin waktu yang panjang berbulan-bulan, triwulan pertengah tahun atau tahunan adalah bentuk evaluasi secara reguler.

Menurut Responden program kerja Unit V IT & Cybercrime sendiri untuk tahun lalu masih membias, karena Responden sendiri tidak tahu program itu sudah dibuat atau belum, tapi setelah setahun berjalan maka dibuat suatu visi dan misi, kemudian dibuat sasaran sebagai prioritas yang akan dilakukan sehingga akan lebih tertata, selanjutnya dengan rencana strategi polisi akan di *breakdown* ke bawah sampai nanti kepada program daripada unit itu sendiri dalam melaksanakan tugasnya.

Terhadap alur masuknya perkara di Unit V IT & Cybercrime sampai dengan pelimpahan perkara kekejaksaan dan penghentian perkara, sampai dengan saat ini menurut Responden alur yang ada adalah menerima Laporan dari Induk dari pos-pos pertama yang ada kemudian masuk ke bareskrim secara umum. Dari filterisasi bareskrim kemudian di distribusikan ke direktorat, direktorat melihat daripada kacamata apakah kasus-kasus terkait dengan cyber, kemudian dari direktorat kemudian didelegasikan ke unit V IT & Cybercrime. Proses penyidikan sendiri

dilakukan dengan melakukan penilaian terhadap LP yang ada, kemudian pengamatan oleh Kanit lalu didelegasikan kepada anggota untuk melakukan proses penyelidikan dan berlanjut sampai tindak penyidikan, kemudian proses penyelidikan diperkuat administrasi-administrasi sampai dengan proses pengumpulan berkas perkara ke tingkat penuntut umum. Secara umum yang bertanggung jawab kepada proses penyidikan secara fungsional adalah seluruh anggota yaitu penyidik sendiri, namun pertanggungjawaban secara struktural adalah kepada Kanit.

Menurut Responden sampai dengan saat ini tidak semua masyarakat mengetahui bahwa Unit V IT & Cybercrime memiliki suatu unit Laboratorium, sehingga perlu peranan dari Laboratorium Forensic komputer untuk melakukan sounding kepada semua pihak dan dikuatkan dengan regitimasi struktural sehingga kedepan laboratorium ini diakui keberadaannya.

Dalam hal pendanaan kasus penyidikan kasus cybercrime menurut Responden Kanit sangat berperan aktif dimana Kanit mendelegasikan kepada penyidik langsung, yaitu kepada pihak yang dituakan didalam organisasi tersebut untuk mengajukan anggaran baik kasus yang berat, ringan maupun kasus yang sedang, namun demikian pada faktanya selama ini kasus yang ada di Unit V IT & Cybercrime adalah rata-rata kasus berat, sedangkan alokasi dana yang diterima adalah nilai nominal yang telah ditetapkan dan dari pihak Unit sendiri tidak bisa menetapkan nominalnya sehingga penanganan kasus tidak akan bisa dilakukan secara maksimal, karena untuk tingkat penyidikan saja dananya sudah tidak cukup. Menurut Responden untuk menanggulangi hal-hal tersebut Kanit sangat berperan aktif untuk menyelesaikan masalah pendanaan karena apabila dikembalikan kepada dinas, dinas sendiri tidak akan dapat mengkovernya.

Mengenai pengawasan sendiri secara struktural dilakukan oleh Kanit, namun diberikan kepada para penyidik yang senior untuk melakukan proses pengawasan dan dipertanggunjawabkan kepada kanit. Menurut Responden tindakan yang dilakukan apabila suatu kasus tidak dapat diungkap adalah melakukan gelar perkara dan ditelaah faktor-faktor yang mempengaruhi proses penyelidikan dan penyidikan, kemudian dalam proses gelar perkara tersebut akan ditinjau apakah kasus tersebut merupakan suatu tindak pidana atau tidak dan meningkat pada gelar perkara-gelar perkara berikutnya dan dilakukan secara menyeluruh, dimana anggota dilibatkan dalam proses ini untuk mengetahui saran dan masukan dari anggota, dan Kanit memberikan peluang kepada semuanya untuk memberikan saran dan masukan sehingga menjadi keputusan yang bulat dalam menentukan proses selanjutnya.

Menurut Responden faktor-faktor yang menjadi hambatan-hambatan dan kesulitan-kesulitan dalam manajemen penyidikan adalah kemampuan sumber daya yang berbeda, kemudian latar belakang pengalaman yang berbeda, kemudian kemampuan penyidikan yang masing-masing orang berbeda, selanjutnya dukungan secara material. Sedangkan untuk metodenya sendiri sudah berjalan, yaitu dengan adanya

sistem pembuatan KK dan sebagainya dimana hal tersebut merupakan suatu proses kontrol dalam penanganan.

Pihak luar yang tergabung dalam proses penanganan penyidikan kasus cybercrime, untuk di dalam negeri bisa JJS, dan pemanfaatan beberapa lembaga-lembaga sosial yang memberikan kontribusi seperti AKKI (Assosiasi Kartu Kredit Indonesia), APJI (Assosiasi Pengguna Jasa Internet), AWARI (Assosiasi Warung Internet Indonesia), Lembaga dibawah naungan pemerintah yang bertugas mengawasi penggunaan traffic internet Indonesia, IDISETI adalah Lembaga dibawah naungan pemerintah yang bertugas mengawasi penggunaan traffic internet Indonesia, sedangkan pihak dari luar negeri adalah AFP (Australian Federation Police), FBI (Federation Investigation of America) JK Bank, kemudian dari SIDIN. Dalam penyidikan kasus hacking website golkar sendiri pihak dari luar negeri dilibatkan dalam kasus tersebut yaitu berkaitan pengecekan IP di Indonesia, karena ada beberapa IP dari Luar Negeri sehingga memanfaatkan fasilitas yang ada di Luar Negeri contohnya seperti Yahoo dan sebagainya.

Menurut Responden budaya organisasi yang terbaik di unit V IT & cybercrime adalah anggota datang tepat waktu dan mereka berpotensi menyelesaikan suatu kasus dengan profesionalisme, dimana mereka harus kreatif di lapangan dan menghasilkan produk-produk yang benar-benar bisa dipertanggunjawabkan. Terhadap proses pertanggungjawaban sendiri dalam unit V IT & Cybercrime pemimpim memperhatikan penyelesaian permasalahan dan mempertanggungjawabkan permasalahan. Terhadap pelaksanaan tugas, pekerjaan dilakukan secara teamwork, dimana pekerjaan dilakukan secara bersama-sama dan hasilnya juga merupakan hasil tim. Dalam ada anggota yang tidak mampu menjalankan tugasnya maka akan dilaksanakan secara bersama-sama oleh tim. Kaitannya dengan sumber pendanaan menurut Responden dalam bekerja harus commit walaupun ada tidaknya dana ekstra karena mereka sudah mempunyai gaji sendiri. Adanya anggapan untuk apa bekerja banting tulang tapi mempuyai gaji yang sama, menurut Responden tergantung dari style manusia masing-masing. Hal-hal tersebut bisa terjadi dengan dilatarbelakangi oleh perbedaan pangkat, sudut pandang masing-masing. Namun yang terjadi dalam unit V IT & Cybercrime adalah mereka melaksanakan tugas dengan sungguh-sungguh dan di latarbelakangi karena tuntutan tugas dan mereka harus mengambil pengalaman dari tugas yang di lakukan. Budaya yang terjadi di unit cybercrime menurut Responden pimpinan melihat hasil pekerjaan dari kualitas pekerjaan, namun secara keseluruhan tampilan mewujudkan keseriusan dalam melakukan tugas.

Terhadap inisiatif anggota dalam unit V IT & Cybercrime diharapkan anggota bisa aktif, yaitu aktif melakukan aktifitas atau kegiatan dan mereka ditunut sebagaimana pertanggungjawaban masing-masing anggota dalam pelaksanaannya. Gaya kepemimpinan sendiri yang terdapat dalam unit cybercrime menurut Responden adalah gaya kepemimpinan partisipatif dan demokratis karena pimpinan selalu meminta pendapat anggotanya dan mengambil keputusan terbanyak. Terhadap peningkatan kualitas sumber daya manusia di unit cybercrime menurut Responden

sudah terlaksana dengan baik karena ada penambahan-penambahan kemampuan yang dilakukan baik di dalam negeri maupun luar negeri.

Pemimpin unit cybercrime sangat menghargai anggotanya dengan demikian menurut Responden selama ini pemimpin selalu memberikan penghargaan secara obyektif, yaitu dengan mempertimbangkan pendapat teman sejawat secara keseluruhan. Pandangan pimpinan terhadap masalah laporan menurut Responden Pemimpin ingin melihat fakta-fakta yang ada untuk dibahas secara bersama-sama. Kebiasaan-kebiasaan yang dominan yang mempengaruhi kinerja unit V IT dan cybercrime dalam melakukan penyidikan adalah adanya pendelegasian, pembentukan tim, discussing sebelum melakukan proses penyelidikan maupun penyidikan. Sedangkan kebiasaan-kebiasaan yang negatif adalah pembiaran terhadap anggota yang tidak melakukan kegiatan antar satu dan yang lain tanpa memberikan dukungan atau tanpa ada proses pengajakan.

Menurut Responden kepemimpinan seseorang bisa dilatar belakangi oleh style dan gaya kepemimpinan baik itu bawaan ataupun proses pembelajaran untuk menggerakkan atau memanage daripada orang untuk melakukan suatu kerja untuk mencapai tujuan yang diharapkan. Untuk pemimpin yang sekarang menurut Responden gaya kepemimpinan yang ada adalah bersifat demokratis yaitu dengan memberikan kesempatan kepada anggota untuk menyampaikan pendapatnya secara berpartisipasi aktif untuk memberikan suatu masukan kepada pimpinan dan keputusan itu dilakukan sebagai keputusan secara bersama.

Pengaruh kepemimpinan yang bersifat positif dalam unit cybercrime menurut Responden adalah kewenangan secara mutlak, penuh, pendelegasian secara penuh, kewenangan yang sudah digariskan dalam struktur yang mengandung konsekuensi tugas dan konsekuensi jabatan, kemudian hal yang perlu ditambahkan adalah gaya yang harus dimiliki oleh pemimpin yang sifatnya memotivasi. Pengaruh positif pemimpin unit V IT & Cybercrime yang ada saat ini terhadap manajemen penyidikan adalah adanya proses pengawasan, reward, dan punishment yang diberikan, serta pendewasaan terhadap anggota. Sedangkan pengaruh pemimpin unit cybercrime yang bersifat negatif adalah pembiaran terhadap anggota yang melakukan tindak kesalahan, kemudian adanya intervensi-intervensi yang berasal dari tingkat atas yang mempengaruhi proses penyidikan. Menurut Responden kehadiran seorang pimpinan dalam unit cybercrime sangat penting terhadap manajemen penyidikan karena harus ada pengawasan dari pimpinan sebab tanpa adanya kontrol dan pengawasan dari pimpinan maka tidak akan bisa berjalan dengan baik.

Menurut Responden kepemimpinan yang ideal saat ini pada Unit V IT & Cybercrime adalah pemimpin harus mempunyai wawasan terhadap ruang lingkup tugasnya, untuk mengetahui kekuatan daripada sumber daya yang ada di institusi itu sendiri kemudian untuk mengembangkan bagaimana proses itu bisa berkembang, dan tidak monoton selanjutnya adanya suatu kreativitas dari pimpinan terhadap pengembangan diri yaitu dengan melakukan penambahan sumber daya, peningkatan kemampuan sumber daya

termasuk anggaran material. Sejauh ini menurut Responden hal-hal yang harus dilakukan terhadap perbaikan dalam unit V IT & Cybercrime adalah pembenahan anggota, pembagian anggota, pembagian tugas dan pembagian kewenangan kepada anggota berdasarkan organisasi yang ada di unit itu sendiri, kemudian yang membedakan adalah proses peningkatan daripada sumberdaya tentunya untuk penggalian lebih jauh lagi dan adanya keterlibatan dari beberapa unsur disitu sehingga akan diperoleh personil yang *capable* dan mampu melaksanakan tugasnya, sedangkan hal-hal buruk menurut Responden yang harus dihentikan adalah masalah mekanisme penerimaan anggaran karena pertanggungjawaban penggunaan anggaran yang selama ini diperoleh dari sumber daya tidak secara keseluruhan bisa diperoleh dan hal tersebut harus segera diantisipasi, revisi, dan diperbaiki.

Identitas

Nama	: Ibu. P.I.N.L
Pangkat	: AKP
Bagian	: Unit V IT & Cyber Crime DIT II Eksus
Umur	: 41 Tahun
Status	: Menikah
Pendidikan	:

SD Sutomo 1979 Medan
SMPN 10 Medan 1982 Medan
SMA 1985 Medan
SEBA Polwan 1987 Jakarta
SECAPA 2001 Jakarta/Sukabumi

Narasi

Responden menjelaskan bahwa awal pendirian cybercrime sudah ada dalam validasi tapi pada saat itu belum ada unitnya, selanjutnya ada beberapa pihak yang diminta untuk bergabung dengan unit cybercrime dan diberikan pengetahuan dibidang cybercrime yaitu pada sekitar tahun 2003. Pada saat itu unit cybercrime belum ada ruangannya, dan belum ada anggotanya, selanjutnya pada saat itu Responden diminta untuk bergabung dengan unit cybercrime dan kemudian diberikan pemahaman dan ditempatkan pada unit cybercrime, dan pada saat itu belum ada Kanitnya.

Menurut Responden perbandingan keadaan kepemimpinan yang terdahulu dengan kepemimpinan unit V IT & Cybercrime yang sekarang sangat jauh sekali perbedaannya dimulai dari ruangan, pada pemimpin yang terdahulu ruangan terbagi atas dua dan fasilitasnya juga tidak memadai dan ruangan tersebut tidak menggambarkan unit cybercrime, kemudian anggotanya juga sedikit. Perubahan terjadi pada saat unit mendapat bantuan dari Isitab untuk melakukan kerjasama. Adapun prosesnya adalah Isitab datang berkali-kali ke unit cybercrime selanjutnya setelah terjadi kesepakatan akhirnya dilanjutkan dengan pembangunan gedung cybercrime serta bantuan alat-alat, sehingga terdapat perubahan secara total mulai dari gedung, komputer, lab, ruang meeting, serta pantry.

Selanjutnya perbandingan terhadap pengelolaan sumber daya manusia khususnya training maupun pelatihan sangat dirasakan perbedaannya oleh Responden karena pada saat kepemimpinan yang sebelumnya Responden sama sekali tidak mengetahui apa-apa mengenai cybercrime, namun setelah pergantian pemimpin Unit V IT & Cybercrime yang sekarang akhirnya Responden memahami mengenai kejahatan cybercrime, dan mengikuti training-training dibidang cybercrime sehingga Responden dapat mengembangkan diri dalam bidang cybercrime.

Terhadap masalah anggaran jika dibandingkan dengan pemimpin yang sebelumnya, menurut Responden pemimpin yang sekarang lebih baik karena pimpinan yang sebelumnya tidak ada dana sama sekali, sehingga unit cybercrime menangani kasus-

kasus diluar unitnya, hal tersebut dilakukan untuk bisa membeli alat-alat keperluan kantor. Sama halnya dengan suasana kerja Responden menggambarkan suasana kerja yang ada pada saat itu adalah seperti hutan. Kemudian terhadap manajemen penyidikan sendiri belum terlihat ada manajemen penyidikan. Menurut Responden sebenarnya infrastruktur sudah terpenuhi seperti line telepon, laboratorium komputer forensik juga sudah tersedia namun tidak terdapat sumber daya manusia yang dapat menjalankannya.

Kemudian untuk masalah interaksi dengan pihak luar dilain unit V IT & Cybercrime sangat jauh berkembang dibanding dengan pemimpin yang sebelumnya karena pada saat pemimpin yang terdahulu tidak terdapat hubungan kerjasama dengan pihak lain, namun saat ini Unit V sudah banyak membina hubungan dengan pihak diluar Unit Cybercrime seperti APJI, Depkominfo dan lain sebagainya.

Hal-hal yang disukai oleh Responden dari Pemimpin yang sebelumnya adalah karena yang bersangkuktan sudah tua sehingga dia diangkat menjadi Kanit menurut Responden sebenarnya pemimpin yang terdahulu juga berusaha untuk memajukan Unit Cybercrime namun tidak sesuai dengan yang diharapkan oleh anggotanya. Hal-hal yang tidak disukai oleh Responden dari pemimpin yang sebelumnya adalah karena suasana kerja seperti hutan, masuk apel pagi dan pulang gak ada siapa-siapa.

Sedangkan terhadap pemimpin yang sekarang, hal-hal yang disukai oleh Responden adalah Responden sangat menyukai suasana kerja yang ada di Unit V IT & Cybercrime dimana dengan adanya penyidik-penyidik yang baru diharapkan bisa memajukan unit cybercrime terlebih untuk penanganan kasusnya, dan tidak ada hal yang tidak disukai oleh Responden dari pemimpin yang sekarang karena semua anggotanya kompak-kompak dan selalu bersama-sama.

Menurut Responden hubungan fungsional yang terjadi antara Unit V IT & Cybercrime dengan unit lain di Bareskrim polri sangat membantu, hal tersebut terbukti dengan adanya unit-unit lain yang meminta bantuan dari unit cybercrime untuk membantu mereka menemukan barang bukti di laboratorium forensik. Menurut Responden sebagai Unit cybercrime seharusnya unit cybercrime mengikuti apapun yang diinginkan oleh Bareskrim Polri, dan sejauh ini menurut Responden Bareskrim Polri sangat mendukung kasus-kasus yang ditangani oleh cybercrime seperti cyber terrorism, cyber gambling. Sedangkan pengaruh negatif Bareskrim Polri terhadap manajemen penyidikan adalah sering dipersulit terhadap administrasi penyidikan, dimana untuk meminta tanda tangan saja harus menunggu-nunggu pimpinan, dan menurut Responden sejauh ini Bareskrim Polri mempunyai pengaruh terhadap kinerja Unit cybercrime. Menurut Responden untuk mengembangkan hubungan yang ada antara Unit cybercrime dengan Bareskrim Polri seharusnya Unit cybercrime dijadikan sebagai sebuah direktorat.

Responden menjelaskan bahwa Polri sebagai organisasi yang besar mempunyai pengaruh terhadap kinerja unit cybercrime, salah satunya adalah pengaruh yang

positif. Sejauh ini pihak-pihak yang terlibat dengan unit cybercrime adalah hubungan kerjasama dengan Apji, Depkominfo, selanjutnya dengan warnet, sedangkan dari luar negeri adalah hubungan kerjasama dengan Microsoft, Interpol, kemudian hightech, FBI, dan AFP. Menurut Responden sejauh ini yang membina hubungan-hubungan tersebut adalah Kanit sendiri. Dari beberapa hubungan interaksi dengan pihak luar tersebut menurut Responden prioritas hubungan yang harus tetap dibina adalah dengan Isitab karena berkaitan dengan alat-alat, selanjutnya dengan Microsoft untuk pelatihan atau seminar dan workshop.

Pengaruh lingkungan luar terhadap kinerja Unit V IT & Cybercrime dalam melakukan penyidikan menurut Responden masyarakat sangat senang dengan adanya unit cybercrime, sebagai contoh menurut Responden saat ini sudah banyak pihak yang mengakui kemampuan dari unit cybercrime. Sedangkan terhadap pengaruh negatif sejauh ini menurut Responden tidak ada. Dengan demikian menurut Responden apabila dikaitkan dengan hubungan unit cybercrime baik dari luar maupun dari dalam unit cybercrime seharusnya unit cybercrime dapat berdiri sendiri menjadi sebuah direktorat yang dipimpin oleh seorang direktur dengan membawahi beberapa unit.

Identitas

Nama	: Ibu. L
Pangkat	: AKP
Bagian	: Unit V IT & Cyber Crime Dit II Eksus
Umur	: 36 Tahun
Status	: Menikah
Pendidikan	:

- SDN 01 1983 Jakarta
- SMPN 143 1986 Jakarta
- SMAN 73 1989 Jakarta
- D III (Diploma 3) Keuangan dan Perbankan 1993

Narasi

Responden menjelaskan bahwa pada saat Responden ditugaskan dalam Unit Cybercrime, Unit V masih belum terbentuk menjadi sebuah unit sendiri namun masih dibawah indag dengan nama Infotech, dimana pada saat itu anggotanya berjumlah kurang lebih 4 (empat) orang. Selanjutnya dibentuklah unit baru dengan diberikan ruangan disebelah Kaud. Dalam unit Infotech menurut Responden tugas yang dilakukan adalah melakukan PLP yang masuk dari NC, namun tidak dilanjutkan karena pelakunya berada di Luar Negeri namun sebelum Responden masuk pemimpinnya sudah membuat ADLP, yaitu laporan yang sampai sekarang belum ada penyelesaian terhadap kasus Robot Sembiring. Selanjutnya beberapa bulan kemudian ada penambahan penyidik utama dan saat itu berjumlah sekitar 9 (sembilan) orang dan pada saat itu juga belum ada kasus laporan polisi yang mendekati cybercrime, sehingga pada saat pergantian pemimpin terdapat perubahan-perubahan yaitu dengan adanya penanganan kasus dan adanya kursus-kursus yang diberikan.

Perbandingan antara Peminpin yang sebelumnya dengan pemimpin yang sekarang menurut Responden sangat jauh sekali perbedaannya dimana pada saat pemimpin yang terdahulu belum ada kemajuan dalam arti kata belum ada sumber daya manusia yang bisa menangani kasus IT sekalipun sudah mengikuti beberapa kursus selain itu tidak semua angggota dilibatkan dalam mengikuti kursus tersebut, namun hanya orang-orang tertentu saja, dan tugas yang dilakukan pada saat itu adalah hanya menerima laporan pengaduan NCB dengan membalas suratnya saja yaitu surat koordinir dan segala macam, sedangkan dengan pemimpin yang sekarang Unit V telah menangani beberapa kasus yang berkaitan IT, dan semua anggota juga diikutkan dalam kursus-kursus mengenai cybercrime sehingga seluruh anggota dapat memahaminya dan dapat dipraktekkan dalam Laporan Polisi, perubahan tersebut terjadi sekitar tahun 2005 -2006, dimana prosesnya sangat signifikan.

Terhadap pengelolaan sumber daya manusia, training dan pelatihan atau sekolah pada pemimpin yang sebelumnya menurut Responden dispesialilasikan hanya 1 orang saja

yang ditugaskan, sebagai contoh 1 orang dispesialisasikan untuk analisa hukum, sehingga hanya satu orang yang dapat menguasainya sedangkan pemimpin yang sekarang menerapkan pengelolaan sumber daya manusia, training dan pelatihan secara merata dimana semua anggota dapat mengikuti pelatihan-pelatihan maupun training.

Terhadap pengajuan anggaran, dana diajukan secara dinas. Terhadap perbandingan suasana kerja pemimpin yang sebelumnya dengan yang sekarang menurut Responden suasana kerja pemimpin yang sekarang lebih bagus dibanding yang sebelumnya walaupun Responden tidak dilibatkan secara langsung dalam penyidikan karena Responden bertugas pada bagian Mindik, namun Responden dapat memahami hal tersebut. Mengenai Infrastruktur sendiri menurut Responden untuk saat ini sudah terpenuhi dibandingkan dengan yang sebelumnya, dan saat ini menurut Responden Unit V sudah memiliki jaringan-jaringan dengan pihak luar seperti Microsoft.

Responden menjelaskan hal-hal yang tidak disukai dari Pemimpin yang sebelumnya adalah pemimpin kurang menguasai pemahaman tentang IT, dan hanya ada satu orang yang mengerti tentang kejahatan cybercrime sehingga anggota menjadi bingung untuk mencari solusi kemana sedangkan pihak yang menguasai permasalahannya tersebut terlalu sibuk dan tidak bisa menjelaskan kepada sesama anggota. Selain itu pada saat itu belum ada internet langsung, belum ada kerjasama dibidang pelatihan.

Hal-hal yang disukai oleh Responden dari pemimpin yang sekarang adalah keahlian dan kepintaran dibidang cybercrime, sehingga angggotanya dapat menyerap ilmu yang ada selain itu Pemimpin juga memberikan kursus-kursus seperti seminar-seminar ataupun pelatihan-pelatihan di luar negeri, sehingga menurut Responden semuanya sudah terpenuhi dengan baik. Sedangkan hal-hal yang tidak disukai oleh Responden dari Pemimpin yang sekarang adalah kurangnya komunikasi antara Pemimpin dengan anggotanya, karena jarang bertemu sehingga angggota tidak dapat menyampaikan masalahnya kepada pimpinan.

Hubungan fungsional yang terjadi antara unit V IT & Cybercrime dengan Bareskrim adalah saling membantu dalam pemeriksaan barang bukti pada unit laboratorium forensic. Menurut Responden apabila Unit V IT & Cybercrime diberi kesempatan yang lebih banyak maka akan berkembang menjadi lebih besar, dan saat ini scoopnya unit V sudah internasional oleh karenanya menurut Responden sebaiknya struktur organisasi dijadikan menjadi sebuah Direktorat. Pengaruh Bareskrim terhadap kinerja Unit V IT & Cybercrime dalam melakukan penyidikan selama ini kurang mendukung, dalam artian mereka menganggap unit cybercrime belum ada apa-apanya, hal tersebut terjadi karena mereka tidak memahami unit cybercrime, mereka masih menganggap unit cybercrime seperti yang unit yang sebelumnya yaitu unit Infotech. Pengaruh negatif Mabes Polri terhadap manajemen penyidikan adalah terdapat kesulitan dalam hal prosedur barang bukti di forensic, selanjutnya mengenai pengajuan anggaran, walaupun sudah diberikan penjelasan terhadap kebutuhan dana

namun mereka tidak memahaminya dan masih menanyakan apakah hal tersebut dibutuhkan atau tidak.

Pengaruh organisasi Polri terhadap Unit V IT & Cybercrime adalah kerjasama dengan Interpol. Menurut Responden saat ini Polri belum memberikan fasilitas semacam software, pelatihan dan segala macam dari luar negeri seperti telematika dan materi-materi pelatihan. Pengaruh Polri terhadap kinerja Unit V IT & Cybercrime adalah melakukan kerjasama. Sedangkan pengaruh negatifnya adanya kesulitan dalam prosedur penyidikan.

Pihak-pihak yang berhubungan dengan Unit V IT & Cybercrime diluar Polri adalah Asosiasi Jasa Internet yang selalu mendukung dan memudahkan dalam melakukan pekerjaan, selain itu Asosiasi Kartu Kredit, Microsoft untuk software-softwarenya. Dari pihak pemerintah sendiri adalah dengan Depkominfo, selanjutnya dari pihak Universitas sendiri adalah universitas-universitas yang ada kaitannya dengan IT yaitu ITB sedangkan dengan masyarakat sendiri Unit V IT & Cybercrime bekerjasama dengan warnet-warnet yang ada. Menurut Responden pihak yang banyak membina hubungan dengan pihak luar adalah penyidiknya, karena penyidik biasanya membutuhkan saksi ahli terhadap kasus yang ditanganinya, maka akan dibuat surat permintaan kepada saksi ahli tersebut atau kepada instansi yang bersangkutan untuk dijadikan sebagai ahli terhadap kasus yang ditangani.

Menurut Responden pihak lain di luar Unit V IT & Cybercrime yang harus diprioritaskan untuk menjalin hubungan dengan Unit V adalah Kominfo yaitu dari pihak pemerintah. Pengaruh lingkungan luar terhadap kinerja Unit V IT & Cybercrime adalah sangat penting sebagai contoh dalam hal kehadiran seorang saksi ahli untuk membuat terang terhadap suatu perkara, sedangkan pengaruh negatifnya adalah apabila Saksi Ahli memberikan jawaban tidak sesuai dengan apa yang kita harapkan. Sedangkan pihak yang tidak mempunyai pengaruh terhadap kinerja Unit V IT & Cybercrimen adalah masyarakat awam yang tidak mengerti dengan IT.

Identitas

Nama : Bpk. D.P
Pangkat : Kompol
Bagian : Cyber Crime
Umur : 36 Tahun
Status : Menikah
Pendidikan :

- SD 1984 Jakarta
- SMP 1987 Banda Aceh
- SMA 1990 Semarang
- AKPOL 1993 Semarang
- S-1 Hukum 1999 Surakarta
- PTIK 2002 Jakarta
- S-2 Kajian Ilmu Kepolisian 2005 Jakarta
- Sespim 2007 Bandung

Narasi

Berdasarkan hasil wawancara Responden dengan Bapak Edi Wardoyo Kanit Indag pada saat itu dan Bapak Suyitno Landung selaku Kabareskrim yang saat pembentukan unit tersebut masih menjadi direktur pidana khusus, cikal bakal berdirinya Unit V IT dan cybercrime awalnya berada di bawah unit indag yaitu Industri dan perdagangan, dimana tujuan awal pembentukan unit tersebut adalah mengantisipasi penipuan melalui internet, yang lebih fokusnya berada pada carding pada saat itu, sehingga laporan yang masuk tidak ada yang mewadahinya. Menurut Responden pada saat itu direktur tindak pidana tertentu di indag membuat kebijaksanaan bahwa unit ataupun satuan cybercrime ada dibawah unit industri dan perdagangan dan validasi dilakukan pada tahun 2002, kemudian unit indag tersebut ditingkatkan menjadi unit, sehingga terciptalah unit cybercrime pada saat ini.

Menurut Responden perbandingan keadaan unit V IT & Cybercrime antara Kanit yang terdahulu dengan Kanit yang sekarang sangat signifikan sekali, yaitu dapat dilihat dari kinerja. Menurut Responden Kanit yang terdahulu dibentuk, ditunjuk berdasarkan perintah, dan pemahaman mengenai cybercrime sendiri tidak ada. Sedangkan untuk Kanit yang sekarang memiliki pengetahuan mengenai cybercrime sehingga penyelidikan maupun penyidikan yang dilakukan semakin berkembang.

Menurut Responden perubahan itu terjadi ketika serah terima jabatan dari Kanit yang terdahulu yaitu sekitar tahun 2006, dimana proses perubahan itu sendiri menurut Responden pada saat Kanit terdahulu Responden bersikap pasif saja, menunggu laporan yang masuk dan itupun jarang sekali didapati, fasilitas yang adapun ketika itu kurang mendukung, sehingga cybercrime mabes tak ubahnya seperti Time zone, datang main game selesai, pulang dan tidak ada kegiatan investigasi yang dilakukan,

dan pada saat itu pimpinananya belum memahami penanganan suatu kasus cybercrime.

Untuk pelaksanaan training menurut Responden pada saat Kanit yang sebelumnya hanya untuk orang-orang tertentu saja, tetapi saat ini semua anggota sudah pernah melakukan training di luar negeri secara merata dan kesempatan sekolah pun semua anggota sudah pernah mengikutinya sehingga tidak ada yang didahulukan dan tidak ada yang dibelakangi.

Terhadap keuangan anggaran saat ini sudah lebih baik karena pada saat akan melakukan suatu investigasi penyelidikan dan penyidikan, dapat mengajukan anggaran dan sering disetujui, walaupun tidak semua disetujui namun sering disetuji dibanding saat terdahulu yang sama sekali bisa dikatakan jarang untuk disetujui.

Menurut Responden untuk suasana kerja saat ini cukup baik, yaitu adanya kesinambungan dalam melakukan pekerjaan, dan terhadap proses kerja yang ada saat ini sudah cukup baik karena setiap anggota sudah mampu dan dapat melakukan pekerjaan, dimana hal tersebut sangat jauh sekali ketika dibanding pada masa terdahulu karena masa terdahulu kasus yang ditangani kebanyakan bukan kasus cyber crime.

Untuk sarana prasarana menurut Responden sejauh ini sangat jauh lebih baik karena Kanit yang terdahulu sudah mulai melakukan pembangunan infrastruktur tetapi belum dimanfaatkan secara optimal, karena pada saat itu harus ada unit yang dibentuk sehingga fasilitasnya sangat seadanya dan sangat-sangat tidak manusiawi tetapi yang penting harus ada unit.

Terhadap networking atau jaringan, kerjasama dengan pihak lain diluar unit V IT & Cybercrime menurut Responden sejauh ini sudah cukup baik dan lebih meningkat dibanding yang terdahulu, walaupun sebenarnya untuk Kanit yang terdahulu pun sudah terdapat networking dengan pihak lain.

Pada saat ditanyakan mengenai hal-hal yang disukai oleh Responden dengan kepemimpinan yang sebelumnya Responden menyatakan tidak ada yang disukainya karena selama kepemimpinan yang terdahulu Responden merasa patah arang karena selalu dipindah-pindah dan tidak ada sesuatu yang bisa diharapkan. Sedangkan hal-hal yang disukai oleh Responden dengan kepemimpinan yang sekarang adalah pemimpin sangat mendukung keinginan anggotanya dan diberikan kesempatan untuk mengembangkan diri sehingga anggota dapat mengembangkan keinginannya sesuai dengan tugas dan kewajiban sebagai penyidik.

Hal-hal yang tidak disukai oleh Responden dengan kepemimpinan yang sekarang adalah sistem yang ada belum terbentuk secara utuh karena saat ini menurut Responden pekerjaan dilakukan berdasarkan figur, dimana apa yang di kerjakan oleh anggota berdasarkan perintah Kanit sehingga menurut Responden apabila Kanitnya

diganti belum tentu berhasil seperti situasi yang sekarang. Namun demikian secara garis besar menurut Responden semua berjalan dengan lancar.

Menurut Responden hubungan fungsional antara Unit V IT & Cybercrime dengan unit lain dalam Bareskrim Polri yaitu adanya laboratorium komputer forensic dimana berfungsi sesuai dengan *job description*. Penyidik dalam hal penyelidikan unit Cybercrime juga melakukan kegiatan Laboratorium Forensic, sehingga mendukung kegiatan operasional pada fungsi-fungsi lain. Responden melihat sejauh ini kinerja yang dilakukan pun sangat baik sekali.

Pandangan Responden terhadap Bareskrim Polri ditinjau dari kacamata unit IT Bareskrim Polri adalah pemahaman terhadap level tersebut sudah cukup baik dibanding dengan masa terdahulu, karena pada masa terdahulu unit hanya sekedar ada, karena merupakan salah satu pra operasional crime yang dicanangkan oleh *Soft* PC maupun pertemuan-pertemuan lain karena Cybercrime termasuk kejahatan trans nasional, sehingga harus ada yang mewadahinya.

Menurut Responden secara umum Bareskrim sudah lebih maju terutama masalah pengaturan dukungan operasional untuk melakukan suatu kegiatan operasional dibanding dengan unit V IT & Cybercrime karena apabila diajukan permohonan anggaran untuk penyidikan maupun penyelidikan kasus Cybercrime tidak harus ada pelakunya pada saat orang itu melaporkan. Sedangkan paradigma Polri masih menginginkan kejelasan dari suatu kasus dan terkadang kasus sudah selesai baru diberikan uangnya, apabila hal tersebut yang terjadi menurut Responden tidak akan pernah merasakan hasilnya, namun demikian saat ini dukungan seperti itu mungkin dengan pemahaman yang lebih baik saat ini sudah mencukupi.

Responden menilai tidak terdapat pengaruh negatif secara langsung dari Bareskrim Polri terhadap manajemen penyidikan, tapi mungkin saja hal tersebut terjadi karena adanya keterbatasan pengetahuan dan pemahaman. Menurut Responden kadang-kadang Bareskrim menganggap sesuatu yang berkaitan dengan IT itu urusannya langsung ke Unit Cybercrime, padahal mungkin saja pada saat itu kasus tersebutpun tidak nyambung dengan unit Cybercrime hanya sifatnya secara umum, contohnya ada orang yang kenalan melalui internet lalu ketemu nyata terjadi suatu kejadian kejahatan, orang berpikir ini akibat internet, namun hal tersebut tidak bisa dilihat sebagai akibat internet, tapi harus dilihat bahwa kasus ini murni pidana tanpa hubungan dengan internet.

Menurut Responden pengaruh Bareskrim Polri terhadap manajemen penyidikan adalah bahwa selama ini Unit IT & Cybercrime masih dibawah struktur cybercrime namun bagaimanapun juga kebijaksanaan yang dilakukan oleh unit merupakan kebijaksanaan dari Bareskrim. Jadi selama unit tersebut menyatu apalagi dengan situasi sekarang unit tersebut bukan suatu satuan kerja, tapi bagian daripada unit kerja yang mana unit kerjanya adalah Direktorat, sehingga bagaimanapun juga

kebijakan dari Bareskrim berpengaruh pada kebijaksanaan visi dan misi yang harus dilakukan oleh unit Cybercrime.

Responden menggambarkan hubungan fungsional yang terjadi antara Unit V IT & Cybercrime dengan Polri, untuk rencana kerja tahun 2005, program 5 tahun Polri cybercrime akan dikembangkan hingga ke satuan Polda ataupun ke tiap-tiap Polda, Responden melihat bahwa Polri sendiri menilai bahwa perkembangan teknologi pasti akan menimbulkan kejahatan yang tidak mengenal batas wilayah sehingga Polri mengantisipasi dengan menyiapkan unit-unit ataupun satuan-satuan hingga ke tingkat atau level Polda dan menurut Responden hal tersebut merupakan suatu hal yang positif sekali.

Responden menilai kebijakan-kebijakan yang dikeluarkan oleh Polri selama ini baru sekedar wacana saja belum pada taraf pelaksanaan. Perencanaan yang ada hanya sekedar perencanaan menyesuaikan dengan keinginan daripada zaman atau keinginan secara umum, namun belum keinginan yang secara nyata ada. Dalam artian kalau memang mau dikembangkan seharusnya itu terkoneksi dengan penyiapan personil, sarana prasarana dan anggaran yang ada. Sedangkan kalau masalah personel tentang masalah training, penyelidikan dsb mereka yang dikirimkan adalah bagian yang bukan dari bagian cybercrime dan terhadap masalah anggaran belum ada anggaran tersendiri yang menyesuaikan dengan kebutuhan yang ada. Sebagai contoh seseorang punya 100 dari yang 100 ini mau apa. Menurut Responden apabila diberikan perhatian yang lebih banyak atau persiapan yang lebih maximal untuk mengembangkannya maka akan disiapkan anggarannya sesuai dengan kemampuan yang ada.

Dalam hal pengaruh positif Polri terhadap kinerja Unit V IT & Cybercrime dalam melakukan penyidikan adalah adanya penerimaan secara langsung dari luar dan diberi ijin secara tidak langsung, sebagai contoh dalam hal pengadaan barang kebanyakan bukan diadakan oleh Polri tetapi oleh bantuan dari negara lain seperti network. Namun sampai sejauh ini belum terdapat pengaruh yang negatif.

Pengaruh organisasi Polri baik secara langsung maupun tidak langsung adalah berkaitan dengan unit tersebut dimana anggota unit tersebut merupakan anggota Polri yang tentunya ada pengaruh langsung pada pengadaan seperti personilnya, staff nya maupun anggaran dan sebagainya.

Berdasarkan pengetahuan Responden sejauh ini hubungan Unit V IT & Cybercrime dengan pihak lain yaitu adanya kerjasama cybercrime dengan pemerintah (DEPKOMINFO) dimana kerjasama tersebut sudah cukup baik, saling mengisi dalam melakukan sosialisasi IT. Sedangkan dengan pihak swasta ada Microsoft yang selalu memberikan kesempatan pada Unit V IT & Cybercrime untuk mengikuti pelatihan atau studi banding ke luar negeri dan ada juga dari NGO. Selain itu terdapat juga kerjasama dengan instansi lain atau negara lain seperti Amerika dengan ICTAB dan Australia dengan AFP. Dalam hal ini ICTAB berkaitan dengan pengembangan unit

secara struktural dan infrastruktur yang ada, sarana dan prasarana, AFP dengan pengembangan penyidikan yang dilakukan. Hubungan Unit V IT & Cybercrime dengan akademisi lebih condong pada personil dalam kaitannya dengan saksi ahli, tapi secara institusi masih jarang. Selain itu terdapat juga kerjasama dengan pihak KIK dimana secara keseluruhan kerjasama tersebut sudah berjalan dengan baik karena KIK sering mengundang unit V IT & Cybercrime sebagai pembicara untuk menjelaskan apa yang dilakukan cybercrime dan sejauh mana pemahaman Polri terhadap cybercrime tersebut.

Hubungan Unit IV IT & Cybercrime dengan badan-badan internasional hubungannya cukup baik walaupun belum terasa secara langsung, sebagai contoh adanya konferensi interpol mengenai IT crime, dimana Unit V IT & Cybercrime dilibatkan sebagai panitianya atau dengan United Nation yang mengadakan suatu seminar dan Unit V diundang untuk mengikutinya walaupun sponsornya berasal dari Microsoft untuk Indonesia. Akan tetapi Responden melihat belum ada bantuan yang signifikan yang diberikan oleh badan-badan internasional tersebut terhadap perkembangan unit V IT & Cybercrime dalam arti kata signifikan adalah memberikan beasiswa untuk mengikuti suatu pendidikan yang sifatnya teknis ataupun memberikan bantuan sarana prasarana.

Hubungan Unit V IT & Cybercrime dengan masyarakat sebagai korban kejahatan atau pelaku kejahatan sudah cukup baik, dimana masyarakat sudah mampu menilai bahwa saat ini Unit V IT & Cybercrime sudah mampu menangani kasus cybercrime. Jadi saat ini malah masyarakat sudah mulai mengakui bahwa kepolisian sudah mampu menangani kasus cybercrime.

Dalam kaitan hubungan Unit V IT & Cybercrime dengan pihak lain menurut Responden hubungan tersebut terjalin tergantung pada masing-masing person, dalam hal ini Kanit secara struktur mau tidak mau harus menjalin *network* dengan semua bidang atau golongan dimana hal tersebut memang ada kaitannya dengan tugasnya. Sedangkan untuk anggota hanya mengikuti perintah yang diberikan misalnya ditugaskan untuk mengikuti pertemuan dengan pihak lain, maka anggota hanya menjalaninya dan tetap menjalin hubungan dengan saling tukar informasi maupun diskusi untuk membahas suatu masalah yaitu melalui hubungan email, melalui telepon dan alat-alat komunikasi lainnya ataupun kadang-kadang sekedar informal dengan kumpul bersama ataupun makan siang bersama yang sifatnya menumbuhkan rasa kebersamaan sehingga pada saat butuh bantuan ataupun saran, maka akan cepat menerimanya dibanding dengan berlaku secara formal.

Menurut Responden hubungan yang harus diprioritaskan untuk dijalin oleh Unit V IT & Cybercrime dengan pihak lain adalah dengan Interpol, karena kadang-kadang laporan yang masuk dari luar adalah melalui interpol dan jika ingin melakukan penyidikan keluar maka harus menunggu prosedur melalui interpol. Sedangkan untuk instansi pemerintah di luar Polri yang harus dijalin oleh Unit V adalah dengan DEPKOMINFO karena bagaimana pun juga regulasi dan pengaturan daripada IT di

indonesia banyak berada disana. Sedangkan untuk badan-badan lainnya menurut Responden Unit V harus melakukan hubungan dengan semua pihak seperti AFP, FBI, ICTAP karena terdapat profesionalisme dari mereka yang dibutuhkan untuk meberikan saran kepada Unit V. Selain itu hubungan yang harus dibina oleh Unit V adalah dengan pihak Microsoft karena terdapat hubungan simbiosis mutualisme dimana pihak Microsoft memberikan pendidikan cybercrime dan unit cybercrime memiliki pemahaman terhadap cybercrime sehingga penegakan hukum terhadap kasus-kasus cybercrime lebih signifikan.

Untuk saat ini dukungan pihak luar terhadap unit cybercrime dalam melakukan penyidikan mengenai kasus cybercrime adalah berhubungan dengan ISP (internet Service Provider) atau saksi ahli. Menurut Responden pihak luar seperti media massa, penegak hukum dan lembaga masyarakat menyambut positif terhadap tindakan-tindakan yang dilakukan oleh unit cybercrime dan mereka sangat menghargainya karena merasa unit cybercrime ditangani secara profesional.

Pengaruh negatif pihak luar terhadap Unit V IT & cybercrime adalah adanya beberapa praktisi yang menggampangkan saja suatu investigasi cybercrime yang dilakukan tetapi dia sendiri tidak memahami bagaimana investigasi tersebut dilakukan sehingga masalah pembuktian, seperti masalah pemeriksaan terhadap barang bukti mereka tidak mempunyai pemahaman terhadap itu, tapi mereka menganggap itu sebagai hal yang mudah.

Lingkungan luar yang tidak mempunyai pengaruh terhadap manajemen penyidikan adalah mereka yang menganggap bahwa cybercrime hanya kejahatan-kejahatan lucu saja dan bukan merupakan suatu tindak pidana, jadi tidak perlu ditindak secara hukum, pandangan tersebut berasal dari para pelajar, mahasiswa maupun masyarakat secara umum.

Responden menjelaskan struktur organisasi di unit cybercrima saat ini berbentuk falat dimana Kanit dan penyidik berada pada posisi sejajar dan mendapat pekerjaan secara sama dan sederajat jadi sama-sama tidak ada batasan sehingga bersifat flat, kecuali yang kebagian laboratorium forensic karena memerlukan keahlian khusus. Wewenang dan pekerjaan dari masing-masing struktur organisasi tersebut secara umum adalah melakukan penyidikan.

Rantai komando yang diterapkan adalah perintah langsung dari Kanit terhadap penyidik, dan para Penyidik bertanggung jawab kepada Kanit. Sedangkan yang merencanakan dan melaksanakan, mengawasi dan memonitor dan yang mengevaluasi pekerjaan yang ada di unit V IT & Cybercrime adalah Kanit juga.

Menurut Responden sistem organisasi flat sudah cukup baik, karena masing-masing bertanggung jawab, namun system seperti ini juga mempunyai kekurangan karena bergerak berdasar figur bukan berdasar dari pada system yang terbentuk.

Menurut Responden seharusnya dibawah Kanit, Kanit bukan membentuk unit tapi tim yang berisi satu tim yang terdiri dari empat atau lima orang oleh penyidik yang senior, dimana dalam suatu penanganan kasus tim selalu bersama-sama dalam arti kata ada LPA tim ini yang mengerjakan, LPB tim B, LPC tim C, ada LPD tim A lagi yang mengerjakan tetapi saat ini karena sifatnya yang langsung dari kanit begitu ada LP tim A yang mengerjakan, ada LPB sebagian tim A yang mengerjakan, ada LPC mungkin sebagian tim A lagi yang mengerjakan. Sehingga pada saat ditampilkan kasus ini dinilai kurang cukup menarik oleh para anggota yang masih junior, ataupun yang jadi anggota saja pada saat itu bukan yang bertanggung jawab pada LP tersebut, dia akan melihat bagaimana yang penting lebih menguntungkan atau membuat nyaman yang bersangkutan. Tidak berdasar tanggung jawab yang diminta sehingga menurut Responden dapat dicek mungkin cara mengeceknya misalnya hari ini dapat dicek si A mengerjakan apa misalnya saya mengerjakan penyidikan terhadap cyber cop dan bukan tidak mungkin pada dua hari kemudian dia ditanya dia akan menyatakan hal yang sama karena mungkin itu yang paling mudah bagi dia tapi pada saat mungkin dicek secara langsung dia akan bingung karena ternyata hari ini saya tidak mengerjakan apa-apa, beda ketika kanit datang kekantor semua mengerjakan perintah sesuai keinginan kanit dan itu berjalan. Tapi kalau kanit tidak ada saya menilai itu hanya semu saja.

Kelebihan dari struktur organiasai yang flat atau mendatar seperti sekarang adalah masing-masing orang dapat memiliki inovasi ataupun cara untuk bertindak ataupun merencanakan apa yang ingin diperbuat. Mengenai kekurangannya dia menjadi bergantung dalam arti kata ketika orang meminta, atau Kanit tidak ada dia menjadi stag disitu saja. Padahal yang diinginkan dari adanya system flat ini adalah suatu inovasi. Tapi Responden belum lihat adanya suatu inovasi tanpa adanya perintah. Menurut Responden sistem flat belum cukup tepat karena para anggota masih berparadigma bahwa tetap harus ada siapa bertanggungjawab pada siapa dan siapa berbuat apa, itu masih ada.

Visi dan misi Unit V IT & Cybercrime dibuat oleh Kanit dan para anggota, dimana visi dan misi tersebut dijabarkan dalam program kerja yang dibuat secara signifikan untuk dilakukan secara bersama-sama secara konsisten oleh Kanit dan para anggota dan Responden sendiri dilibatkan dalam proses pembuatan visi dan misi tersebut.

Responden menilai visi dan misi yang ada sekarang ini sudah cukup baik dan tidak perlu dilakukan perubahan namun terhadap program kerja akan dibicarakan secara bersama dan dilaksanakan bersama.

Menurut Responden Manajemen Organisasi adalah bagaimana seorang manager mengatur organisasi yang berada dibawah pimpinannya atau dibawah tanggungjawabnya untuk mencapai suatu tujuan.

Responden menggambarkan management organisasi unit V IT & Cybercrime sudah sesuai dengan management organisasi tersebut, karena Kanit sebagai manager dimana

untuk mencapai masalah kepuasan atau tidaknya tergantung Kanit, dan menurut Responden apa yang diperintahkan oleh Kanit sebagai manager telah berjalan seperti yang diharapkan.

Peranan Responden sendiri dalam perencanaan dalam unit V IT & Cybercrime adalah memberikan masukan, sedangkan dalam hal pelaksanaan Responden berperan menjadi pelaksana dalam beberapa program kerja tersebut, dan terhadap evaluasi program kerja Responden menjelaskan selalu diadakan pertemuan rutin untuk membahas apa yang telah dikerjakan dan apa yang akan dikerjakan, dimana dalam pertemuan tersebut masing-masing pihak saling mengevaluasi satu dengan yang lain.

Dalam Unit V IT & Cybercrime perencanaan dilakukan paling tidak seminggu sekali yaitu pada hari senen. Menurut Responden berkaitan dengan perencanaan dan pelaksanaan Unit V IT & Cybercrime mengenai pengelolaan sumber daya manusia, seleksi, perekrutan, pengenalan, peningkatan sumber daya manusia, jenjang karir dan sebagainya, unit V IT & Cybercrime adalah bagian dari bareskrim sebagai satuan kerja, ataupun polri sebagai suatu organisasi, Responden melihat unit V IT & cybercrime secara umum yang sifatnya berkaitan dengan organisasi itu belum terlalu nampak, karena memang organisasi sendiri sudah mempunyai fungsi dan tugas masing masing. Mungkin untuk pengembangan karir, untuk promosi, untuk jabatan itu tergantung daripada personel, tapi untuk pengembangan unit sendiri dalam arti kata pengembangan anggota secara internal Responden melihat sudah cukup baik sekali karena seluruh anggota sudah pernah melakukan pendidikan ataupun pelatihan di luar negeri.

Terhadap peningkatan infrastruktur termasuk didalamnya laboratorium komputer forensik, pengadaan alat dan pelatihan saat ini Responden menilai sudah cukup baik karena adanya hubungan yang baik dengan pihak ketiga seperti Banpolwil, karena dari polwil sendiri Responden melihat adanya bantuan ataupun peran secara nyata atau kelihatan langsung. Sama halnya dengan pelatihan, karena pelatihan bukan berasal dari Polri tetapi dari pihak luar yaitu pihak ketiga.

Responden menilai saat ini masyarakat mulai melihat bahwa tidak dapat melakukan suatu tindakan atau perbuatan sesuka hati di internet ataupun dunia maya, karena tentunya ada dampaknya dan itu bukan tidak mungkin dapat ditindak secara teropong. Saat ini kemauan masyarakat agar negara mengurus cybercrime menurut Responden jauh lebih baik dibanding masa sebelum mungkin adanya tindakan yang diberikan. Terhadap sumber dana sendiri untuk saat ini sudah cukup baik, namun oleh karena saat ini sistem kepemimpinan yang ada bersifat figur maka kebijaksanaan ataupun saat ini untuk memenuhi kebutuhan daripada unit tersebut tergantung dari Kanitnya, kalau dari polri sendiri Responden melihat masih kurang.

Dalam hal pelaksanaan, yang berperan mengawasi pelaksanaan, kemudian mengkoordinasikan pelaksanaan, menawarkan pilihan-pilihan penyelesaian masalah, mengambil keputusan termasuk merubah rencana dalam managemen organisasi

adalah Kanit, namun demikian karena sistemnya flat masing masing anggota berpendapat untuk menawarkan solusi dari penyelesaian suatu permasalahan tetapi tetap diputuskan oleh Kanit berdasarkan pertimbangan anggota yang ada. Sedangkan perubahan kegiatan tersebut dilakukan bersama dengan anggota dalam forum pertemuan. Terhadap evaluasi program kerja Unit V IT & Cybercrime dilakukan oleh Kanit yang biasanya dilakukan sebulan sekali secara bersama sama. Suatu program kerja dikatakan sukses apabila berhasil dilaksanakan dengan baik ataupun berhasil dilaksanakan walaupun terdapat kendala-kendala dan dengan adanya kendala tersebut maka ditelaah lagi kenapa terdapat kendala. Sedangkan program kerja dikatakan gagal, apabila program tersebut sama sekali tidak dilaksanakan.

Responden menjelaskan bahwa kepemimpinan yang sekarang sangat menghargai anggotanya dimana apabila ada anggota yang telah sukses melaksanakan suatu pekerjaaan maka biasanya Kanit memberikan suatu Reward ataupun hadiah. Sedangkan terhadap anggota yang gagal dalam melaksanakan tugasnya adalah dengan memberikan masukan dan evaluasi mengenai kegagalan tersebut dan didukung oleh rencana organisasi atau pelaksanaan program kerja kedepan. Hal tersebut dilakukan karena pada saat dilakukan evaluasi, maka akan terlihat program kerja yang sudah dilaksanakan dan yang belum dilaksanakan. Apabila tidak sesuai dengan jadwal yang telah direncanakan mungkin program tersebut tidak dilaksanakan, namun bila dipaksa untuk tetap dilaksanakan kemungkinan besar gagal, sehingga pada saat evaluasi program kerja harus dilihat apakah sudah dijalankan ataukah ada program lain yang bisa dijalankan. Dengan adanya evaluasi tersebut diharapkan dikemudian hari tidak terjadi kegagalan yang sama.

Program kerja Unit V IT & Cybercrime untuk tahun pertama adalah pengembangan dari unit itu sendiri, kemudian melakukan sosialisasi terhadap cybercrime dan tahun berikutnya melakukan penyidikan cybercrime secara profesional.

Responden menjelaskan alur masuknya perkara di Unit V IT & Cybercrime sampai dengan pelimpahan berkas perkara ke pengadilan adalah apabila yang lapor polisi model B, maka unit cybercrime sudah melakukan penyelidikan dan penyidikan terhadap kasus tersebut. Setelah dilakukan penyelidikan diperoleh bukti IT berupa digital evidence atau didukung oleh pemeriksaan laboratorium forensik komputer selanjutnya dilakukan penetapan ataupun penyitaan sesuai dengan prosedur pada pengadilan, kemudian SPDP di kirimkan kepada kejaksaan, dimana pada saat itu sudah mulai melakukan penyidikan. Kemudian apabila sudah cukup bukti ditingkatkan prosesnya menjadi penyidikan. Responden menjelaskan laporan polisi biasanya tidak langsung dibuat, tetapi dilakukan penyelidikan terlebih dahulu untuk melihat unsur pidana atau dapat tidaknya kasus tersebut ditangani.

Setelah semua proses tersebut dijalani, maka akan dilakukan pemberkasan yang sebelumnya telah terlebih dahulu dikoordinasikan secara informal dengan jaksa, dalam arti kata diberikan pemahaman kepada mereka tentang kasus Cybercrime, karena kasus cybercrime agak berbeda dengan tindak pidana hukum yang lainnya,

karena kadang kadang barang bukti yang diberikan adalah digital evidence yang dalam kasus pidana umum belum diatur secara spesifik, sehingga harus diberikan pemahaman kepada jaksa atau mungkin bahkan para hakim untuk meyakinkan mereka bahwa memang benar telah terjadi suatu tindak pidana. Sejauh ini alur penyidikan tersebut jika ditelaah dari perencanaan, pelaksanaan dan evaluasi menurut Responden sudah sesuai dengan apa yang telah direncanakan sebelumnya sesuai dengan prosedur.

Terhadap pertanggungjawaban atas pelaksanaan penyidikan suatu kasus saat ini pembagian kasus tidak dibagi dalam tim-tim tetapi dibagi per LP, setiap LP baru dibentuk suatu tim berdasarkan tim tersebut. Yang bertanggungjawab disini adalah mereka yang paling senior didalam laporan polisi tersebut, dan pembagian kerjanya masing-masing orang mengerjakan bersama sama kasus tersebut. Tapi kadang kadang begitu ada LP ke dua, ke tiga mungkin yang yunior yunior ini bisa terlibat juga di LP ke dua, ke tiga sehingga mereka akan melihat mana yang paling menguntungkan atau mungkin yang paling nyaman untuk mereka kerjakan atau kemungkinan keberhasilannya tinggi, sehingga senior senior inilah bertanggungjawab terhadap LP tanpa adanya tanggungjawab secara moril dari mereka yang menjadi anggotanya.

Peranan laboratorium komputer forensik sangat vital sekali dalam cybercrime, karena bagaimanapun juga barang bukti yang ada yaitu digital evidence yang harus diambil dengan tehnik tersendiri menggunakan peralatan yang ada sehingga adanya laboratorium forensik sangat mendukung sekali jalannya penyidikan yang dilakukan. Responden menjelaskan Komputer forensik dibawah Unit V IT & cybercrime juga, tetapi anggota daripada laboratorium komputer forensik tidak melakukan penyidikan terhadap kasus itu.

Menurut Responden apabila Unit V tidak mampu mengugkap suatu kasus maka tindakan yang dilakukan adalah melakukan gelar perkara terhadap kasus tersebut dan dibuatkan nota dinas atau meminta saran atau pendapat kepada pimpinan apakah ini akan di SP3kan ataukah untuk didiamkan saja, tetapi lebih sering di SP3kan karena memang susah diungkap lebih lanjut karena mungkin kurang saksi, kurang bukti. Hal-hal yang menjadi halangan dalam manajemen penyidikan dilingkungan unit Cybercrime untuk saat ini belum ada yang terlalu fatal namun di masa yang akan datang ada baiknya untuk diadakan pembagian tim secara jelas.

Responden menjelaskan pihak luar yang terlibat dalam penyidikan kasus cybercrime adalah AFP namun tidak terlibat secara langsung akan tetapi memberikan bantuan teknis, sedangkan pihak lain yang terlibat adalah dari pihak saksi akademisi dalam hal ini adalah saksi ahli hukum pidana yang mengerti mengenai tindak pidana cybercrime

Dalam melakukan penyelidikan kasus hacking website Partai Golkar, menurut Responden ada juga pihak-pihak yang ikut terlibat dalam penyidikan kasus tersebut namun tidak terlibat secara langsung oleh karenanya penyidik memanfaatkan network yang sudah ada dari kalangan akademisi, kalangan IT, bahkan dari kalangan hacker

itu sendiri untuk memperoleh informasi ataupun data yang diinginkan untuk menyelesaikan kasus ini.

Berkaitan dengan budaya organisasi, berdasarkan pengalaman Responden sebagai penyidik unit V IT & cybercrime, tindakan atau kebiasaan yang dilakukan tim minimal sesama anggota tim adalah datang tepat waktu tapi tidak melakukan apa-apa.

Untuk masalah tanggungjawab terhadap kesalahan, budaya yang ada dalam Unit V IT & cybercrime adalah masing-masing pihak saling melepas tanggung jawab dan melimpahkan tanggung jawab pada orang lain dan melepaskan kesalahan pada orang lain. Sebagai contoh menurut Responden apabila dia melakukan kesalahan dia tidak mau dikatakan salah, dia tetap mencari pembenaran sehingga secara langsung bisa dilimpahkan kepada orang lain. Sedangkan terhadap pelaksanaan tugas dikerjakan bersama namun terhadap hasil pekerjaan tersebut diakui oleh atas nama sendiri. Namun apabila ada yang tidak bisa menjalankan tugas, maka dia akan jujur mengakuinya dan menyatakan mengalami kesulitan sehingga pihak yang lain akan membantu secara bersama-sama.

Dalam hal pendanaan, paradigma yang ada sekarang ini menurut Responden adalah apabila ada pekerjaan maka harus ada uang ekstra kalau tidak ada maka tidak akan jalan.

Terhadap kepuasan menurut Responden adalah mengerjakan sesuatu dan mendapat kepuasan pribadi ketika dapat melakukan sesuatu yaitu berkaitan yang Di Atas. Menurut Responden hal yang diharapkan apabila sukses dalam melakukan sesuatu pekerjaan adalah mendapatkan pujian berupa uang. Terhadap inisiatif anggota dalam budaya unit cybercrime adalah anggota bersifat pasif, dimana anggota menunggu perintah melaksanakan susunan perintah, tanpa ada yang berani menentangnya.

Dalam budaya organisasi Unit V IT & Cybercrime pengambilan keputusan dilakukan secara partisipasif yaitu memberikan kesempatan anggota mengeluarkan pendapat dan mengambil keputusan dengan mempertimbangkan pendapat anggota. Terhadap pemberdayaan sumber daya manusia dalam Unit V IT & Cybercrime harus diasah, bahasa inggris, komputer bila perlu, mengikuti seminar dalam dan luar negeri, siap jadi pembicara. Terhadap penghargaan menurut Responden sebaiknya diberikan secara subyektif, mungkin dengan kriteria yang jelas dengan meminta pendapat teman sejawat.

Untuk masalah laporan menurut Responden Pimpinan ingin melihat fakta terhadap permasalahan yaitu dengan mencari alternatif bersama dan diselesaikan bersama. Menurut Responden pengaruh positif anggota dalam melakukan penyidikan adalah mereka akan melakukan penyidikan seoptimal mungkin apabila diawasi oleh Kanit. Dengan demikian terdapat respon yang negatif terhadap penyidikan dimana apabila Kanit tidak ada, maka anggota datang tepat waktu dan tidak tau harus berbuat apa.

Menurut Responden Penimpin mempunyai berpengaruh dalam melakukan penyidikan.

Menurut Responden Kepemimpinan adalah cara dari seorang pemimpin untuk mengatur atau memimpin suatu organisasi, kaitannya dengan gaya kepemimpinan Unit V IT & Cybercrime yang sekarang Responden menggambarkan kepemimpinan yang ada adalah Kepemimpinan yang memberikan contoh atau keteladanan dalam arti kata apa yang diperintahkan oleh Kanit sebagai pimpinan bisa dikerjakan oleh Kanit sendiri sehingga tidak ada alasan bagi anggota untuk tidak bisa mengerjakannya selain itu juga bersifat demokrasi dimana apabila ada keberatan atau permasalahan anggota dapat memberikan suatu pandangan atau gambaran terhadap keberatan atau permasalahan yang dihadapi.

Menurut Responden dalam kepemimpinan terdapat pengaruh yang positif dan negatif dimana untuk hal yang positif kepemimpinan Unit V IT & Cybercrime dalam melakukan manajemen penyidikan untuk saat ini sudah bagus dimana hal tersebut dapat terlihat dalam penanganan kasus hacking website partai golkar, dimana Kanit memberikan beban tanggung jawab kepada anggotanya untuk mengungkap kasus ini karena memang Kanit pernah mengungkap kasus yang serupa, sehingga hal tersebut merupakan suatu hal yang positif dalam membangun motivasi bagi anggota untuk mengungkap kasus tersebut. Sedangkan hal yang negatif dari kepemimpinan unit yang sekarang adalah tergantung kepada figur sehingga pada saat Kanit tidak ada maka tidak ada progres yang bagus, dan menurut Responden tanpa kehadiran seorang pimpinan untuk saat ini maka Unit V IT & Cybercrime tidak akan bisa eksis dalam menjalankan tugasnya karena saat ini kepemimpinan tergantung pada figur atau komandannya dan belum ada suatu pola atau sistem yang berjalan diatas, unit ini dalam arti kata pembagian tugasnya yang berkaitan dengan tanggung jawab yang secara utuh tidak setengah-setengah ataupun sistem pendanaan atau anggaran. Sehingga pada saat Kanit tidak ada semua tidak berjalan..

Menurut Responden kepemimpinan yang ideal untuk unit V IT & Cybercrime adalah Kanit membuat suatu sistem yang baku mulai dari penerimaan laporan, pelaksanaan penyidikan hingga dukungan anggaran, sehingga apabila Kanit tidak ada maka pekerjaan tetap dapat dilaksanakan dengan tanggung jawab yang paling senior dan didukung oleh anggota tim tersebut, sedangkan untuk cara kepemimpinan yang ada saat ini sangat berbeda.

Dalam hal pergantian kepemimpinan menurut Responden Kanit tidak terlibat dalam menentukan pergantian pemimpin karena Kanit merupakan bagian dari organisasi Polri sehingga yang menentukan Kanit adalah Polri, sehingga seseorang menjadi Kanit bukan didasarkan pada kemampuan akan tetapi didasarkan pada jabatan dan struktur.

Identitas

Nama	: Bpk. EH
Pangkat	: AKBP
Bagian	: Unit V IT & Cybercrime
Umur	: 41
Status	: Menikah
Pendidikan	: SD 1977
	SMP 1983
	SMA 1986
	Akabri 1987

Narasi

Cikal bakal awal pendirian Unit V IT & Cybercrime dilatarbelakangi oleh perkembangan kejahatan pada tahun 2000 sampai tahun 2001 dimana banyak terjadi kasus-kasus cybercrime sehingga berdasarkan Kep Kapolri Kep dimana pada saat itu masih menjadi korp serse Kep No.9 tahun 2001 dibentuklah Unit Cybercrime kemudian pada proses perjalanannya di validasi menjadi Kep 54 sehingga terbentuklah Unit IT & Cybercrime dibawah direktorat dua ekonomi khusus bareskrim, hal tersebut diketahui oleh Responden setelah bertugas di Cybercrime dengan melihat *job description* yang ada.

Responden menjelaskan pada masa awal bergabung dengan cybercrime, Responden masih merasa bingung karena tidak ada yang mengarahkan, dan memberikan penjelasan mengenai cybercrime itu sendiri sehingga Responden harus mencari tau sendiri. Namun apabila dibandingkan dengan Pemimpin Unit V yang sebelumnya dengan Pemimpin yang sekarang menurut Responden jauh lebih baik karena terdapat perubahan-perubahan misalnya Pemimpin yang sekarang memberikan pemahaman kepada anggota tentang cybercrime sehingga secara bertahap anggota dapat pembelajaran dari waktu ke waktu untuk memahami cybercrime. Terhadap masalah keuangan sendiri pada saat ini lebih baik dibanding dengan pimpinan yang sebelumnya karena pada pimpinan yang sebelumnya anggaran tentang cyber crime belum terlalu teralokasikan dengan baik dalam arti keseriusan dan Kapolri pun pada saat itu belum mengalokasikan anggaran khusus cyber crime. Namun untuk saat ini terhadap masalah anggaran sudah tersedia sebagaimana terdapat dalam Proja dengan mekanisme pengajuan dana kepada dinas.

Terhadap perbandingan suasana kerja sendiri menurut Responden suasana kerja yang sekarang lebih dinamis, hal tersebut dirasakan oleh Responden semenjak bergabung dengan unit Cybercrime dimana sampai saat ini Responden telah dua tahun bergabung dengan unit cybercrime, Responden merasa memiliki banyak kemajuan dalam pengembangan kemampuannya dalam memahami cybercrime. Untuk proses manajemen kerja menurut Responden bersifat opportunity dimana setiap anggota diberi kesempatan untuk berkembang, dengan cara Kanit memberikan pendelegasian setiap penyidikan kepada anggota dan diberikan kebebasan untuk berdiskusi sehingga

kontrol tetap dipegang oleh Kanit namun anggota bebas menyumbang saran dan masukan kepada Kanit sehingga dinamika penyidikan dapat terlihat.

Untuk masalah infrastruktur dalam mendukung kinerja para angggota, pemimpin sangat memperhatikannya dimana semua fasilitas pendukung baik laboratorium komputer forensic maupun alat untuk masing-masing penyidik disediadakan oleh Pemimpin termasuk line telpon juga disediakan oleh Pemimpin untuk memudahkan controling dari kanit kepada masing-masing penyidik sehingga kanit dalam arti menanyakan cukup dengan menelpon.

Salah satu misi cybercrime adalah meningkatkan kerjasama penyidikan, dan meningkatkan kemampuan dari sumber daya manusianya sehingga kanit sudah membuat terobosan-terobosan, baik didalam negeri seperti menjalin kerjasama dengan instansi formal pemerintahan yaitu Kominfo selanjutnya menjalin kerjasama dengan pihak-pihak luar yang mendukung cyber crime seperti APJI, AKI, AWARI sedangkan dari luar negeri adanya peningkatan alat tool-tool kemudian kemampuan penyidik maupun penyidik dalam lab forensik dengan polisi luar negeri seperti Australia ataupun FBI dimana kanit memanggil ahli forensik luar negeri untuk memberikan pembelajaran mengenai training pelatihan bagaimana lingkup tugas dari pada komputer forensik yang ada di unit cybercrime.

Hal-hal yang disukai oleh Responden dari Pemimpin yang sebelumnya adalah karena cybercrime merupakan satu hal yang baru bagi Responden, sedangkan hal-hal yang tidak disukai oleh Responden dari pemimpin yang sebelumnya adalah terdapat ketidakpedulian antara sesama anggota maupun dengan partner.

Hal-hal yang disukai oleh Responden dari pemimpin yang sekarang adalah terciptanya suasana kerja yang bersifat kekeluargaan sehingga secara struktural walaupun kanit membawahi 20 orang penyidik, namun secara dinamika kedinasan tanpa disadari tercipta suasana saling memiliki dimana apabila ada salah satu anggota yang susah dalam hal pribadi maka semua anggota turut merasakan hal yang sama, kemudian saling membantu sesuai kemampuan masing-masing. Sedangkan terhadap kekurangan pemimpin yang sekarang menurut Responden seorang manusia mempunyai kelemahan dan kekurangan namun bagi Responden hal tersebut merupakan tantangan untuk bisa dipecahkan secara bersama-sama. Kekurangan tersebut adalah dalam hal kurang maksimalnya terhadap pengontrolan anggota, sebagai contoh dalam Unit V IT & Cybercrime penyidik madya muda belum merasa belum siap untuk menangani kasus cybercrime, dan mereka merasa tidak pernah difungsikan karena hanya orang-orang tertentu saja yang selalu ditugaskan namun masalah tersebut dapat diselesaikan dengan cara mengkomunikasikannya kepada mereka.

Sebagai suatu organisasi Unit V IT & Cybercrime selalu berinteraksi dengan pihak luar dimana hubungan tersebut terjadi karena masing-masing unit mempunyai tugas job descriptionnya masing-masing, namun menurut penilaian Responden pihak luar

tidak pernah secara terbuka meminta bantuan kepada Unit V, hal tersebut bisa disebabkan oleh ketidaktauan ataupun karena merasa malu untuk meminta bantuan kepada Unit V, sehingga yang terjadi apabila pihak luar membutuhkan bantuan dilakukan secara informal atau melalui individu.

Pandangan Unit V IT & Cybercrime menurut Responden terhadap kebijakan-kebijakan yang dikeluarkan oleh Polri dipengaruhi oleh organisasi, dimana seharusnya dalam budaya organisasi dipengaruhi oleh budaya-budaya jawa maksudnya *ewuh pakewuh,* dalam artian apabila ada hal-hal yang ingin diungkapkan walaupun hal tersebut merupakan hal yang tabu bagi orang lain maka hal tersebut harus diungkapkan, karena penyelesaian yang dibutuhkan pada saat ini adalah hal-hal yang baik harus disampaikan dan hal-hal yang buruk juga harus disampaikan tanpa ada interest pribadi untuk perbaikan kedepannya.

Responden menjelaskan secara formal manajemen ataupun mekanisme penyidikan sudah diatur dalam buku penyidikan reserse yang di revisi setiap tahunnya, namun dalam perkembangannya banyak dipengaruhi oleh budaya organisasi yang mana lebih dominan kepada unsur subyektifitas, hal tersebut dapat terjadi karena perkembangan lingkup politik negara sehingga polisi menurut Responden tidak bisa membedakan mana tugas polri dan mana tugas politik.

Menurut Responden bareskrim mempunyai pengaruh terhadap manajemen penyidikan, salah satu pengaruh negatif bareskrim terhadap manajemen penyidikan adalah kurangnya evaluasi secara berkala dari level atas sampai kebawah.

Responden menggambarkan hubungan fungsional yang terjadi antara Unit V IT & Cybercrime dengan polri secara hak terdapat hubungan tata cara kerja di lingkup bareskrim polri sehingga setiap langkah dan kegiatan didasarkan pada tugas pokok dan program kerja sehingga diharapkan unit cybercrime dapat melaksanakan apa yang menjadi tugas pokok polri dalam arti kepolisian negara Republik Indonesia untuk melakukan pelayanan kepada masyarakat.

Pandangan Unit V IT & Cybercrime terhadap Polri menurut Responden selaku anggota organisasai Polri secara struktural maka unit cybercrime harus menjadi anggota polri sesuai dalam tugas pokoknya seperti yang diatur dalam Undang-Undang Kepolisian Republik Indonesia. Adapun pengaruh Polri terhadap kinerja Unit Cybercrime menurut Responden Polri sangat berpengaruh, dimana hal tersebut dirasakan oleh Responden karena Polri banyak memberikan kemampuan baik secara pripadi maupun yang dikembangkan sendiri oleh Responden khususnya di unit cybercrime.

Adapun pengaruh negatif Polri terhadap manajemen penyidikan menurut Responden menjadi seorang penyidik memiliki banyak tantangan, karena Polri dipengaruhi oleh budaya kekerasan, pungli dan segala macamnya sehingga pada saat melaksanakan tugas otomatis masing-masing penyidik Polri berusaha bagaimana untuk memenuhi

kebutuhannya walaupun itu bertentangan dengan benturan yang ada. Padahal menurut Responden pada saat dilantik, penyidik telah disumpah untuk tidak berbuat hal yang tidak baik, namun pada kenyataannya Polri memberikan dampak yang sebenarnya negatif, yaitu dengan adanya kewenangan yang sangat besar sebagaimana diatur dalam KUHAP sehingga mempunyai peluang ataupun kesempatan yang besar untuk melakukan suatu tindakan diluar kerwenangannya.

Kaitannya dengan pihak-pihak yang berhubungan dengan Unit V IT & Cybercrime menurut Responden secara internal unit cybercrime berinteraksi dengan unit-unit yang ada pada Direktorat dua, kemudian secara umum lagi kepada direktorat yang lain dimana tim 1, 2, 3 dan 4 apabila secara teknis memerlukan bantuan sesuai kebutuhan pokok cybercrime dalam hal laboratorium computer forensic sudah terdapat mekanisme tersendiri. Selanjutnya dari pihak eksternal terbagi menjadi dua yaitu pihak dari dalam negeri dan luar negeri, untuk pihak yang dalam negeri disamping tenaga birokrasi, juga terdapat kerjasama dengan Kominfo kemudian departemen luar negeri, departemen HAM Hukum dan Ham, kemudian departemen pertahanan, kemudian di luar negeri unit cybercrime bekerjasama dengan interpol kemudian lembaga-lembaga seperti Icitab kemudian dari AFP, selanjutnya FBI kemudian lembaga-lembaga lain yang berhubungan dengan cybercrime.

Dalam hal pembinaan hubungan tersebut menurut Responden yang paling berperan untuk membina hubungan tersebut adalah Kanit karena menurut Responden anggota tidak mempunyai akses-akses untuk membina hubungan dengan pihak luar. Sejauh ini menurut Responden hubungan prioritas yang harus dibina oleh unit cybercrime adalah dengan lembaga yang pernah memberikan bantuan kepada unit cybercrime seperti Icitab, kemudian AFP dan FBI karena hal tersebut bertujuan untuk peningkatan kemampuan dalam arti melengkapi peralatan karena teknologi di update terus, apabila dalam dua tahun, tiga tahun tanpa di update maka akan ketinggalan. Namun selama ini menurut Responden pihak yang memberikan pengaruh positif terhadap manajemen penyidikan adalah Criminal Justice System (CJS) selain itu kantor Advokat, LSM dan lembaga-lembaga seperti APJI, AKI dan AWARI.

Menurut Responden lingkungan luar memiliki pengaruh terhadap menajemen penyidikan, salah satu pengaruh negatifnya adalah dalam penanganan suatu kasus apabila seorang penyidik tidak memiliki prinsip atau pegangan maka akan susah membedakan fungsi kejaksaan maupun fungsi pengacara, karena seorang penyidik rentan terhadap penyalahgunaan kewenangan.

Brief Penelitian
Proyek Robot Cop

Tanggal: 31 Juli 2007
Klien: Petrus Reinhard Golose GOLOSE

Gambaran Proyek:
Diskusi Kelompok Terfokus (FGD) pada penyidik dan non penyidik dari Unit V IT dan Cybercrime Bareskrim Polri mengani manajemen penyidikan *hacking* kasus website partai Golkar.

Latar Belakang
- Teknologi komputer berkembang pesat dan mempengaruhi semua lini kehidupan.
- Hal tersebut mengundang sebagian orang untuk melakukan kejahatan komputer dengan berbagai motivasi dan modus operasi.
- Salah satu bentuk kejahatan komputer adalah *hacking*.
- Untuk memberantas hacking dan kejahatan komputer lainnya didirikanlah Unit V IT & Cybercrime Bareskrim Polri
- Polisi selaku penegak hukum melakukan fungsi polisi selaku penegak hukum dengan melaksanakan kegiatan penyidikan.

Tujuan Penelitian
Untuk menganalisis hubungan antara penerapan manajemen penyidikan *hacking* dengan pencapaian tujuan organisasi Unit V IT & *Cybercrime*, yang dipengaruhi oleh budaya organisasi dan gaya kepemimpinan organisasi serta lingkungan eksternal organisasi.

Untuk itu peneliti perlu menggali:
- Bagaimana manajemen diterapkan pada Unit V IT & Cybercrime?
- Pihak-pihak apa saja yang berkepentingan dengan Unit V IT & Cybercrime *(Stakeholder Mapping)*
- Bagaimana budaya organisasi Unit V IT & Cybercrime?
- Bagaimana kepemimpinan pada Unit V IT & Cybercrime?
- Bagaimana pihak yang berkepentingan, budaya organisasi dan kepemimpinan mempengaruhi kinerja organisasi dalam menerapkan fungsi dan prinsip manajemen pada saat melakukan penyelidikan diterapkan dalam *Unit V IT & Cybercrime*?
- Hal-hal apa saja yang perlu diubah, dipelihara untuk mencapai peningkatan performa organisasi.

Metodelogi
- Diskusi kelompok terfokus dari para anggota Unit V IT & Cybercrime

Pembagian Kelompok
- FGD: Kelompok I adalah para penyidik Unit V IT & Cybercrime, Perwira Menengah (Pamen)

- FGD: Kelompok II adalah para penyidik dari Unit V, Perwira Pertama (Pama)

Langkah Aksi
- Hasil penelitian ini akan dilampirkan dan dimasukan ke dalam analisis manajemen pada disertasi

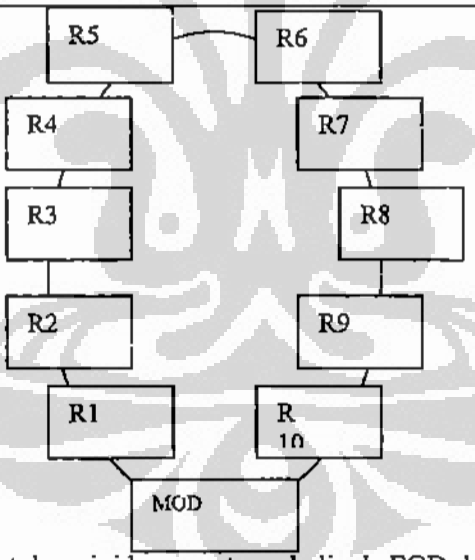
Laporan berupa:
- Formal presentation + power points soft copy
- Transcript (soft copy)
- DVD/VCD recording

Waktu:
- Group Pertama:
  pertengahan Agustus 2007, dengan observer Petrus
- Group Kedua:
  Pertengahan September 2007, dengan observer Petrus
- Tidak dapat pada tanggal 8-13, 16-19, 26-27 Agustus 2007

Anggaran:
- Agency tidak perlu mengeluarkan biaya rekruitmen. Rekruitmen akan dilakukan oleh klien
- Profile responden akan diberikan oleh klien ke agency.
- Biaya yang diperlukan berupa venue, konsumsi, analisis

Project name	: Robocop
Transcriber Name	: Idawati
Group	: 1
Tanggal pelaksanaan	: 02 Agustus 2007
Hari / jam pelaksanaan	: Kamis / 10.00 wib
Moderator	: Rulas
Kriteria group :	
Usia	: --
Jenis Kelamin	: Pria/ Wanita
SES	: --
Usership	: --

R1 : I ketut Budi (ketut)
R2 : Arief Sugiarto (Arief)
R3 : Alexander A (Alex)
R4 : Eddy Tanjaya (Eddy)
R5 : Prayudhi Salembang (Yudhi)
R6 : Intan
R7 : Karsini
R8 : Nia Daniati
R9 : Indri
R10 : Budi



M : saya juga sebetulnya ini baru pertama kali ada FGD dengan Responden dengan mengundang dari Kepolisian gitu …karena yang dateng polisi pasti suasana nya agak beda …karena …kalau biasanya e…kalau kita ….apa namanya .. mengundang responden …kita udah langsung ….ngomong nya udah langsung lu…gua…bebas gitu ngomong nya …saya nih nggak tau ..kalau misalnya buat temen – temen ini ..nggak apa – apa …
R : nggak apa – apa …(bareng)
M : oke …kalau buat temen – temen disini seperti apa …
R : gue – gue nggak apa – apa …
M : lu ..gue ..nggak apa – apa …oke…kayanya lebih enak kaya gitu

…e…gue sebenernya …gue kerja disini …gue sebagai peneliti..nah kita ini ..tadi sebener nya udah cerita – cerita banyak bersama temen yang udah pulang …kita ini di hire ..sama perusahaan …yang kita lakukan ..kita ngobrol – ngobrol santai ..tapi kita ingin tau apa yang menjadi pendapat – pendapat pribadi .. bahkan sampe perasaan – perasaan …kepengen nya sampe kesana ..untuk biasa nya kita analisis pengembangan produk …atau pengembangan strategi …untuk program – program …ini memang jadi mengulang lagi sedikit nih …acara ini acara santai ..bebas …kalau mau …jadi bukan kaya acara anggota DPR gitu …jadi harus angkat tangan ,….harus apa namanya …harus angkat tangan kalau mau ngomong …bebas aja ..kaya ngobrol – ngobrol biasa. ..e…ada rekaman video gunanya untuk dokumentasi ..jadi nggak akan muncul di Patroli ..

R : ha.h.ah.a.a.h.a (bareng)

M : ketawa juga ya ….soalnya biasanya kalau saya perhatiin ya .. jadi ini hanya dokumentasi ..kalau muncul di Tabloit ..pasti semua ketawa deh …

R : Tabloit cek dan ricek …

M : di Katakan Cinta gitu ya …nah …karena nanti …e..saya sama team itu harus membuat semacam laporan …jadi kan kalau udah ada transkrip nya …ada tulisan nya …itu semua nanti kita buat …di belakang ini ..ini…mungkin tadi bingung …mungkin tadi udah ada yang sempet masuk situ ..disini ada team …nah ..kalau tadi sempet …ada yang cerita- cerita mungkin tentang Pak Petrus …ini juga masuk sebagian yang …sebagai team juga ..karena seperti di cerita kan tadi …sebagian dari apa yang kita bicarakan …nanti akan digunakan untuk desertasi doctor beliau…jadi e….oke ..perkenalan selanjut nya ..nama saya Rulas …lengkapnya Rulas Lombardo Sihombing …e…usia …32 lah…jalan 32…

R : sama …sama …saya 31…

M : sama ya …status masih single ..sampe sekarang …

R : ya …sama …

M : pacar itu ya…satu lah ya …

R : satu di Jogya …satu ..di ..Surabaya ..hah.a.ha.h.a

R6 : tadi mau bilang gitu tapi nggak sanggup ….ha.h.a..ha.

R : takut ketauan ,….

M : prestasi yang diraih belum banyak dosa …

R : ha.ha.h.a.(bareng)…

R6 : sama …

M : sama ya …sama ya ….hahah.a..

R : beda tipis …

M : apalagi …hobby ….hobby sebenernya …e…

R : liat – liat …

M : liat – liat boleh …tapi sebener nya hobby olahraga …walaupun badan kaya gini …orang pasti ragu …kalau dibilang olahraga …

R : bukan main catur ya …

M : ya …olahraganya harus yang kegiatan otaknya . …catur ..billiard ..ping pong ..

R : bridge ..

M : bridge …kalau dirumah dulu ada istilah namanya …manjat … kalau …orang batak suka bilang …maklum lah …pendidikan …

R : untuknya orang batak cuma dua disini…kalau empat sudah ..

haha.ha.h.a.

all ngobrol bareng

M : terus ya …tadi status sudah ya …apalagi …

R : pendidikan …

M : ya…pendidikan …a…S1…e…apa namanya …lulus itu lama sekali…dari UI …Fisipol UI …memang lulus nya lama …sempet 7 tahun ,..

R5 : MAPALA….

R4 : MAPALA…..Mahasiswa paling lama …

R6 : berapa tahun …

M : tujuh tahun …

R : banyakan dia dong …

M : berapa tahun .

R6 : 12 tahun …

R : hah.a.ha.h.a.kebanyakan libur tapi …

M : nah masalah nya itu …dibilang demo juga nggak ..dibilang kegiatan mahasiswa juga nggak…emang lama aja …hah.ahah.a

R6 : suka – suka aja ya …

R : suka – suka aja …

M : oke…itu…ini enaknya sambil perkenalan itu …kita keliling – keliling aja ya …maksudnya

R : ya …boleh ….

M : bisa cerita dari ….

R1 : siapa …saya …

M : ya …

R : Nama saya …I ketut Budi …saya orang Bali …

R : kira Sunda …ha.ha.h.a.a.

M : kira ini namanya agak – agak Menado …gitu …

R : ada tampang sedikit lah..a..ha.ha..

R1 : kalau kata orang katanya saya mirip orang Philipina

All ketawa semua ….

R1 : soalnya waktu saya ke Philipina ..Are yoe Philippines …ya ..aja .. begitu udah ngomong Tagalok saya udah bingung …saya lahir di Bandung …kemudian ..saya ..Arief sama Alex ni …satu lighting …artinya satu level…satu angkatan ..kemudian pendidikan saya lulus dari PTIK…sudah S1..terus masalah ..ya ..e..pernah kuliah di Universitas 17 Agustus..terus di PTIK kan setingkat dengan S1..tapi gelar nya S IK..Sarjana Ilmu Kepolisian .. tapi kalau itu bilangnya SIKSAK …Sarjana Kepolisian …

R2 : asal jangan Sarjana Keperawatan …ha.h.a.h.a sama kan …

R1 : Keperawanan harusnya ha.ha.a.ha.ada juga S krim …Sarjana Kriminologi …

M : Skrim …

R1 : saya sudah mendengar banyak tentang Focus Discussion Group FGD waktu saya kuliah ..kuliah di PTIK terutama …diajarkan tentang FGD tetapi mengalami tidak …semua dosen …dosen Metologi .ini kalau Facultative gini …gini …modelnya bisa dengan discussion .diskusi gitu ...FGD saya udah pernah dengar …tapi kita melaksanakan nya nggak pernah …baru sekarang …jadi ini buat saya pengetahuan …sebenernya FGD bagus ..saya kira itu cukup ..

M : status nya …
R1 : oh ya ..status ..sudah berkeluarga anak baru 2 …
M : istri…
R : istri 1…
R : mau cari lagi …
R1 : nggak lah…satu aja susah …nggak habis – habis ….ha.ha.h.
M : oke …ini santai aja …ni ada kopi ..jadi kita kalau ngobrol …
R : bisa dipanasin …
M : ini panas ….
M : nah kita sambil merokok ya …bebas aja …mau sambil ambil … ngobrol …
R : nggak ada yang ngerokok disini ..nggak ada …
Responden buat kopi sambil ngobrol ….
M : oke …lanjut dulu dong …
R : oke….saya kira udah cukup ….Arief …
R2 : oke …nama saya Arief …lengkapnya Arief Sugiarto ..aslinya Jawa tapi muka Batak …
R : nggak ah ….
R2 : darimana…dari batak…ha...ha.karena wajahnya agak gemurusuh ….hah.a.a.ha..
R6 : asli Jawa muka Batak ….
R2 : saya dinas di Jakarta baru …udah jalan 2 tahun ini …terus selama – lamanya…sebelum nya dinesnya di ..kampung ..
M : di kampung …
R : di Jawa …tapi di kampung …kalau ke Jawa …kalau ke gedung tadi ya …sempet bingung juga…seperti orang kampung…bingung ..hah.a.a.h.a terus saya …sebener nya udah pernah denger FGD .,..apa ….
R all : ha.h.a.ha.h.a..
R2 : tapi yang paling itu…FGD itu…ha.ha…terus ….terus status saya udah berkeluarga …anak 2 laki semua …
Responden ngobrol bareng …
R2 : makanya saya trauma kalau ngeliat begini ni ….ha.ha.a..aha..
R : kaya aquarium soalnya….hah.a.a..a
R2 : saya kira cukup…tentang saya …
M : oke….
R3 : Saya Alex….Alexander Afar …asli nya sih orang Toraja …saya lahir dan besar di Makasar …lahir besar di Makasar …sekolah dari SD sampe SMA di Makasar ..nggak pernah jauh dari keluarga …tapi begitu jauh …jauh beneran …karena begitu selesai Akademi ..96 saya satu angkatan dengan Arief dan Ketut …langsung keluar negeri …
R : wuih….hah.a.ha..timor timur. ..haha.ha…
R3 : sekarang nggak boleh free kan…
R6 : ya …harus pake passport ….
R2 : itu kalau jejak pendapat sekarang nggak akan balik ha.hh.a.a..a
R3 : ya .,…kalau Habibie nggak jejak pendapat nggak balik – balik …
M : ya …berapa lama disana …
R3 : dua tahunan ….
R2 : ya …karena ada jejak pendapat itu …kalau nggak …ya ..nggak balik….hhah.a.ha..

R3 : 2 tahun di Timor Timur….terus e….selesai jejak pendapat di kasih pilihan …mau kemana …

M : dikasih pilihan …

R3 : ya ,…dikasih pilihan …mau kemana…

R6 : tetep di Timor Timur atau ke ..tenggara lah …

R3 : saya ngisi angket…Jakarta …dipenuhi…cuma kadung saya ke Makasar …ditahan sama ini kan …udah lah disini aja …ngapain ke Jakarta …udah dines di Makasar …2 tahun di Makasar …dua ribu…..

M : dines nya di Makasar …di …

R3 : di Poltabes …di Intelejen…sih…saya dari awal di Intelejen … sebener nya sama aja …jadi intel …

R2 : intel Jawa Timur…

R3 : 2002 …2002 ada kesempatan saya masuk PTIK …di Jakarta dua tahun …2004 saya ikut ke Sumatra Selatan …Sumatra Selatan …tetep Intel juga …terus awal 2006 Januari …ada panggilan untuk SATGAS …ke BARESKRIM dengan kasus Perbankan …dua ribu ….bulan apa ya kita disana …

R : Februari ….

R3 : Februari …Februari kita di Cyber Crime …berarti sekarang udah setahunan lah …satu setengah tahun di Cyber Crime …

M : status gemana nih …

R3 : Status saya punya tiga anak …

All ngobrol bareng

R3 : dua di Makasar …satu di Palembang …wong Palembang …

R : ya …wong Plembang …

R : *…….*

R3 : nggak tau ya .,..orang Sumatra ngomong nya gitu ya …kalau tentara itu kentro …ya ..kan …

R6 : bapak itu bilang …tentara itu..TANTARA …

M : TANTARA…

R6 : ya …

R4 : sama orang Makasar tu bu …

R6 : kalau bilang Mabes itu …MABES...

M : MABES…

R6 : bilang Reserse itu …bukan Reserse ….RESERSE …

R3 : kalau Brebes …BREBES…hah.a.a.h.

M : kalau mereka bilang orang Jakarta nggak konsisten …kubilang menteng …e…TEBET …dia bilang tebet …waktu kubilang waktu kubilang menteng …haha.a..a.a..h.

R : kaya Opung aja …

R1 : tapi memang jadi berbahaya ….saya inget temen saya …Daya Victor …dia orang Alor pada saat saya bilang …

R : silahkan …itu kursinya Pak ….(R10 baru dateng) …

R1 : dia ngomong sikap mental …karena logat nya …jadi sikap mental ….kan udah beda artinya …sikap mental …mental itu kan cleng …artinya …terbang … sikap mental …

R : mental….mental ….

R2 : nyasar ya Pak ….

R10 : nggak nyasar….

R : lupa tadi sama OB bersangkutan di lift…hahah.a.ha.a.h
M : ini sudah jalan …kita lanjut aja lagi ….
R10 : ya ….
M : hobby Pak …
R3 : hobby ….renang …baca …
M : renang …baca…baca apa …
R3 : baca buku….baca majalah …
M : majalah apa …
R : yang porno…h.ah.ah.a.h.ah.a.
M : oke …lanjut dulu nih …
R4 : nama saya mas …Eddy Tanjaya …besarnya di Makasar … sekolah ..lahir di Makasar …terus masuk Akademi tahun 97 …
M : selama ini tugas di …
R4 : pertama tugas dulu di Sulawesi Tenggara …Kendari …terus ada 3 kabupaten ..Bau – Bau terus Polres *…*
M : sebentar …Bau – Bau….itu bau …
R4 : ya …bang …
M : seneng bau …hah.a.a.h.a
R4 : Bau – Bau ….
M : emang daerah Sulawesi Tenggara itu ..kayanya di ulang – ulang ya …
R4 : jalan – jalan nya begitu jugakan …
R6 : toli – toli …pare – pare ….haha.ha.
R4 : 2005 …2006 saya mutasi ke Mabes …cuma baru aktif …baru beberapa bulan ini …karena saya sakit sudah menjalani operasi enam kali ..
M : wuih …sakit apa …
R : pendarahan …infeksi pencernaan …
R4 : baru aktif beberapa bulan ini …
M : o…
R4 : kurang lebih 5 bulan …
M : tapi sekarang udah ..udah …..normal …
R4 : sudah lumayan ….
M : status …
R4 : status masih bujangan …

Responden ngobrol bareng ….

R3 : elo lahir tahun berapa sih …
R4 : 78 ya ….
R : Cuma buat kencing aja ya….haha.ha..
M : ya ..itu yang harus kita dwi fungsi …
R : nah itu …
R4 : terus selama bertugas ….selama bertugas *…..* terus Danreskim …2 tahun …kemudian Kalpolsek …terus Kasat Intel …
M : di…
R : Sulawesi Tenggara juga ….kebetulan dosen saya nih ada disini ..(R 10)…selama bertugas di Laskrim tapi nggak pernah sekolah Reserse …begitu di sekolahkan di Intel juga. ..sama dengan Arief…Jama di Intel juga. ..
R3 : panggil Tuan atau panggil Pak …ya ..kan …hah.a.ha.h.
R2 : beda satu …tu ya …

R4 : ya …ekstrim banget sih lo …
M : oke ..hobby apa nih ….
R4 : kalau hobby sampe sekarang saya main basket …
M : sampe sekarang masih main basket …ya..kalau saya liat polisi – polisi masih segar bugar lah badan nya kan …
R2 : kalau saya sih senang nya yang bukan – bukan …haha.ha..
R6 : dulu lebih bugar ….
R2 : kalau saya cari yang bugar….
R4 : kebetulan dosen saya waktu di Pusdik Intel….Pak Budi ….tapi ngajar nya ngajarin Reserse ….jadi kan bingung …di Pusdik Intel ngajar nya Reserse ….
M : hm…oke …
R : strategi lapangan…h.ah.a..
All ngobrol bareng ….
M : oke …lanjut ….
R : oke …terima kasih selamat siang …
R : cie …..(bareng)…ha.ha.h.a..
All ngobrol bareng …..
R5 : nama saya ini …panggilan saya ni Yudhi ….
R : panggilan malam nya apa ….
R5 : tapi nama ini saya …panjang saya….nama kebesaran lah … menurut Pak Kanit ….Prayudhi Salembang .S.T. ha.h.a.a..a…sesuai dengan pendidikan saya …saya Sarjana Tehnik …
R : Jurusan apa …
R5 : *……* salam hal apapun saya harus kuat …
R all : ha.h.a.h.a.ha..a
R5 : saya dari Toraja…sama dengan Bang Alex…..saya lahir dan besar di negeri orang …di Sulawesi tenggara …orang tua merantau disana …jadi saya lahir dan besar disana …nanti saya pas lulus SMA …saya ..e..pindah ke Makasar …saya pindah sendiri kesana …saya kuliah …sekitar 8 tahun …
R : kuliah di Makasar …dan *…* di Makasar …
R5 : saya kuliah delapan tahun…dan nganggur sekitar 2 tahun ha..ha …dan daftar polisi …dan masuk …pendidikan selama 11 bulan ..setelah itu …penempatan pertama saya langsung masuk Bareskrim saya sampe sekarang dari tahun 2004 ..kalau masalah status saya sampe sekarang kurang jelas juga…haha.h.a..
All ngobrol bareng sambil hah.ha.a.h.a.
R : nggak jelas..
R : completecated ….ha.h.a.ha.h.ah
M : kalau kata orang jaman sekarang curhat colongan nih …ha.ha…
R5 : kalau hobby saya …buat saya sih hobby segala – galanya asyik – asyik aja ..
R All : cie …h.a.h.a…
R : hah.ha….gitu aja koq repot ….
R5 : yang penting yang menyegarkan gitu aja ….
R : dan yang penting puas ….ha.ha…
R : hobby nya membuat dosa….hah.a.h.a.h.a
M : oke …lanjut dulu nih ….

R6 : selamat siang dulu ya sekali lagi .,.....nama saya Intan …saya biasa dipanggil Boys ..karena saya seangkatan dengan bapak ini…bapak ini ..bapak ini….bapak ini …dan ibu ini…tapi saya paling tua …usia 41 …

M : wah…nggak keliatan …

R6 : saya paling tua ….diantara ini semuanya …sama bapak ini dan ibu ini …

R : Bapak itu berapa bu …

R6 : saya sudah menikah …anak dua laki – laki …suami saya kerja nya di swasta ….

M : di…mana mbak …

R : di ….*…* Engineer ..di group Bakrie …di Baja…di Cilegon ..

R6 : hobby saya menyanyi…menari..dan baca Nova…mungkin saya nyasar kali ya ….masuk polisi….

M : ya ….

R : tapi saya di pohon situ nggak bisa menari nggak bisa nyanyi .,.. ha.ha.ha..

R all : ha.ha.h.a.ha..

R6 : saya asalnya dari Melayu …karena saya lahir di Medan …nari Bali saya nggak bisa…karena dasarnya saya tari Melayu …

R : nari …kosentrasi …

R6 : saya dinas di Baleskrim itu sudah 20 tahun…di sub bid Pupar paling lama ..terus saya pindah ke PIG karena saya hamil … terus saya masuk Sescapa ...abis masuk Sescapa 6 bulan saya di …terus saya di informasi Kriminal …

R2 : itu pindah karena hamil atau …

R6 : karena saya hamil …karena sering cepat pulang …

R3 : jadi karena hamil bisa membuat orang pindah ya ….

R6 : bisa…capek …

R2 : capek….

R6 : terus saya Sescapa di hukum 6 bulan …abis di hukum 6 bulan saya Indag satu tahun tiga bulan …kemudian saya ditarik ke Cyber Crime …Cyber crime itu …bapak – bapak ini belum ada. ..yang ada saya sama bapak itu ….berdua ….Bapak Budi…sepi…kaya hutan …begitu ….begitu …

M : begitu ada mereka ….jadi rame kaya hutan juga….

R all : ha….ha.h.a.h.a.

R6 : begitu bapak – bapak ini masuk ….

M : kenapa tu …

R6 : rrammme sekali ……

M : kaya hutan juga ….hah.h.a.

R6 : kaya hutan sekali ….jadi ditambah dengan hutan rimba … masalah nya Pak Petrus masuk lebih rame lagi …

M : hah.ah.a.h.a

R6 : tapi saya seneng banget …karena pas dia masuk …..rombak semua ….anak nya nggak nakal – nakal ….masih it's okay lah …abis mereka hanya nakal diluar lah …didalam nggak …ya begitulah saya seneng sekali bergabung sama Bapak – bapak ini ….mereka pinter – pinter …lucu – lucu …

M : terima kasih ….

R all : ha.h.a.ha..a..h.a.
R7 : koq …mas yang terima kasih …harusnya bapak – bapak ini….
R6 : saya rasa …saya rasa kalau ini dibuat team udah bagus banget
R2 : team volley …
R6 : bola kaki…futsal cukup …masih bisa…itu aja …ya …

M : lanjut ….
R7 : oke …selamet siang …nama saya Karsini ….saya asli dari Jawa Tengah …tepat nya di Solo …Sukoharjo…
R : wong solo…
R : orang Solo …
R7 : tapi saya masuk pendidikan tahun 88 disekolah …lulus tahun 89 ..pertama kali saya dines itu saya ditempat kan di Polres Jakarta Selatan ..dibagian Personel….
M : o…o…
R7 : sampe saya tahun 2003 …jadi di Personel itu dari …masuk … e..keluar Polisi pertama kali …sampe saya keluar daftar CAPA itu ..di Personel terus …kemudian pendidikan tahun 2002 sampe 2003 di SESCAPA Sukabumi …kemudian di tempatkan di POLDA METRO Jaya…SK saya memang waktu itu ditempatkan di *…* Polda Metro Jaya ..namun saya di beritahukan di Personel nya di birokrat juga…kemudian sampe tahun dua ribu…..2007 kemarin…bulan April …saya ditugaskan ke Bareskrim …jadi saya bergabung dengan Bapak – bapak…dan ibu – ibu ini …kurang lebih baru 3 bulan ..jadi secara resmi …secara pengetahuan saya masin nol…untuk reserse – reserse an khususnya di Cyber Crime
M : baru kali ini juga ikutan ini ya …
R7 : ha….
R7 : kemudian status saya sudah married ….anak saya 2 laki – laki … semuanya …yang satu udah kelas 1 SMA …yang satunya kelas VI…saya juga seumuran dengan senior saya…walaupun beda dua tahun …dua tahun sekarang ….beliau ini angkatan 10 saya angkatan 12 …
M : pertama tugas…
R : pertama tugas saya di Polres Jakarta Selatan ….bagian Personel ..kemudian sampe sekarang ..bergabung nya …baru tiga bulan
M : ya …ya…
R : jadi kalau ilmu ke reserse an…saya masih ..tapi saya berusaha .. ingin tau dan ingin belajar sama bapak – bapak dan ibu – ibu ini….mudah – mudahan saya juga bisa…
R6 : pake dukun…ha.ha..ha.
M : hobby …hobby apa ….
R7 : hobby …kalau saya …ya…seneng jalan – jalan aja …
R4 : sekarang lagi hobby chatting …hah.ah.a.h.
R7 : betul….betul…chatting …
M : jadi masuk Cyber crime …hobby nya jadi chatting ….
R7 : selain itu internet …
M : internet bagus…
Responden ngobrol bareng …
R7 : pengalaman saya ….saya chatting pertama kali diajarin sama

Bapak Setiadi …baru pertama kali saya …kemudian saya suruh milih itu nama …saya pilih nama Bagas Nugraha …

R all : ha…ha.h.a.ha..ha.

M : ini menarik nih….kita akan ngomongin ….

R7 : katanya suruh milih …yang milih itu kan kita orang nya nggak tau …ya …saya pilih nama Bagas Nugraha itu perasaan saya o… namanya bagus ..kan gitu …begitu nama Bagas Nugraha …mau chatting …chatting ..misalnya mau ketemu dimana …ketemu dimana …oke lah kita janjian ...

R all : ha.ha..a.a..a.a.a.masuk …

R7 : begitu masuk…mbak Indri nya masuk …chatting an sama siapa .. ya ini mbak…Bagas …lho ini Bagas …iho ini kan punya Pak Gagas katanya ..lho jangan – jangan bener Pak Gagas …nggak tau nya Ya….

R6 : soalnya dia pake Laptop …

R7 : AKBP Gagas Nugraha ada …akhir nya saya di panggil …kamu chattingan sama siapa ….

All : hah.ah.a.h.a.h.a.

R7 : saya sempet down…karena apa ..katanya chatting an itu orang nya kita nggak kenal …walaupun kita belum ketemu …walaupun hanya sekedar janjian …saya merasa nggak tau …masa sama Bapak …itukan saya ID saya …katanya gitu ..waduh ..saya sempet mau nangis di depan Pak Gagas …saya pikir masa sih saya cengeng banget …

R6 : ketawa kenapa sih…koq ceritanya serius sekali …

R7 : selama ketemu sama Bambang …ya itu Pak Gagas …

R all : ha.ha.h.ah.a..a.

R7 : semenjak itu saya mau main chatting takut …

R all : ha.h.ah.a..jadi trauma …

R7 : jadi sampe sekarang chatting an sama mbak Indri aja …

M : jadi ini curhat ….

R1 : tapi isi chatting nya …udah …udah …

Responden ngobrol bareng

M : ini sebener nya udah masuk ke obrolan kita ya ..tapi masih ada dua orang lagi …

R1 : itu…itu cyber ya …

R7 : saya udah dikerjain sama mbak Indri ini…saya jadinya saya takut …udah …down …

R all : hha.h.a.ha..

R7 : bener nggak sih…Gagas …antara ya dan tidak …kayanya saya udah malu banget … pengen nangis juga. ..malu ..gitu ..kitakan udah …

R all : hhah..h.a.ha..a

R7 : saya disitu umurnya 21

R all : ha.ha..a.ha..ah.a.

R7 : masih sekolah …

R1 : tapi Pak Gagas ketawa – ketawa aja kan …

R6 : Pak Gagas nggak ngerti ya …ketawa – ketawa aja …

R2 : koq ..jadi merah gitu sih…haha..a.

R7 : saya udah ketakutan…sampe sekarang saya nggak mau chatting lagi …

R1 : Puas tapi ….

R6 : haha..a..ha.h.a..a.
R7 : karena saya takut nyasar ya ….terutama yang saya takutin.. nanti sama Pak Idham lagi jangan – jangan …
R : kebo ireng …haha.h.a.h.a
M : oke …ini lanjut dulu deh ….nanti kita ngomongin itu lagi …
R8 : oke …nama *…….*
M : ha ..siapa tadi …
R8 : asal Jakarta …
M : siapa …
R9 : Nia Daniati ….
M : o……
R all : o..Nia Daniati …
M : o..Nia Daniati …
R8 : penempatan pertama di Mabes Polri ..begitu Sescapa langsung penempatan di *…….* status saya udah punya anak dua ….hobby ….jalan – jalan ngabisin duit …haha.ha..
R2 : ini kalau hobby terus ketawa – ketawa ….
Responden ngobrol bareng sambil haha.a..a.ha.
M : hobby apa dong …
R8 : jalan – jalan ….
M : oke …lanjut …..
R9 : langsung aja nih ….tadi kan udah tau …udah disebutin …Nama Indriani …dari lahir sampe sekarang di Jakarta terus … penempatan pertama langsung …pertama e….
R : langsung ….
R9 : jangan di potong dong ….
R all : hah.ah.a.h.a.h.
R9 : penempatan pertama tahun 97 langsung di tempatkan di Mabes di Bareskrim ..e….mungkin karena latar belakang saya D3 Perbankan …jadi langsung saya ditempatkan di unit Perbankan …dan dari mulai pertama …dari 97 saya nggak pernah dines keluar ….saya sampe sekarang masih dines di Mabes …sekarang ini di unit Cyber ini …status saya menikah punya anak 2 ..kalau hobby jalan – jalan …
M : suami ….
R : suami satu ….
R2 : suami Polisi…
M : o…polisi juga…
R9 : suami Polisi juga….udah….
M : hobby tadi jalan – jalan …
R9 : e…hm….
M : shopping …
R9 : e.he….apalagi kalau duit banyak ….
Responden ngobrol bareng ….
M : oke lanjut ….
R : pakaian nya udah nggak rapih ….
R10 : ini tadi dari kelapa dua …ngurusin barang bukti …Nama saya Budi Sutrisno …terus …e….lulus dari Akademi Polisi tahun 90 – 91 penempatan pertama di Polda Bogor …di Reserse kemudian lulus Perwira sama dengan dua orang ini kebetulan satu lifting …2002 – 2003 dinas

pertama di Pusdik Bintal …disana ambil ilmu Hukum dan yang ber bau – bau *……*

R : baunya apa …

R10 : seperti ini ….h.a.ha..a.a.

R all : hahah.a.h.a..

R10 : di Pusdik Bintal sekitar 2 tahun …setelah …setengah tahun di Satgas …akhir nya masuk ke Cyber Crime …saya lahir di Jakarta …orang tua Madura …tapi saya lahir di Jakarta …sampe besar…

M : status ….

R10 : status e…married. …

M : anak …

R10 : anak satu ….

R6 : kalau dikumpulin anak nya udah banyak ….

R : ha.ha.h.a..ada yang udah jadi …

R10 : anak nya cowok…

R9 : jadi nya nemenin ya ….

R10 : ya …jadi kalau pergi kemana disangka temen saya …hah.ah.a.

M : oke…

M : oke …ini kayanya kita …kalau misalnya perlu kopi atau teh…ini ada disini…santai aja. ..sebenernya kalau kita mulai ….walaupun tadi udah diceritain sama temen – temen disini …sejarahnya Cyber Crime saya pengen tau …kalau …katakanlah saya ini mau cerita sama orang …saya abis ngobrol …*….* Cyber Crime …gitu kan …saya nggak ngerti ..*…….* kalau saya mau jelasin kepada mereka …apa yang harus saya jelasin …apa yang harus dijelasin

R : coba ulangin Pak ….gemana ….

M : ya …jadi gini…kalau saya mau cerita sama temen – temen saya ..tentang IT dan Cyber Crime ini …apa sih yang harus saya ceritain kepada mereka …

R6 : tentang unit 5 ya …

M : ya ….soalnya mungkin orang …maksud saya pasti masih banyak yang belum tau …gitu ya ..temen – temen saya sendiri sih …saya juga males …tadi udah ditanya – tanya …siapa sih tu ….polisi …o…kaya gitu ..

R2 : kaya gitu tu … tu gemana maksudnya … kaya gitu nggak di jelas-in terus ketawa ….ha.ha.ha..

R all : hah.a.a.ha.h.a..

M : jadi penampilan nya beda ….lebih rapih …atau yang ..apa nama nya ….alah ….gitu …hah.a.ha..

R7 : nggak nyangka kalau polisi ….karena dari pakaian nya diliat kaya bos semua …

R2 : udah bos semua lah ya ….

M : tadi saya juga udah bilang ….saya udah bilang …sama mereka …itu polisi …polisi apaan …itu unit 5…Cyber Crime …apaan tu Cyber Crime …a….langsung bingung …darimana ya ceritain nya

R2 : itu yang bertanya cewek …cowok …

R all : ah…hha.ha.ha..

All ngobrol bareng sambil ..haha.h.a.

M : oke …

R1 : memang sih banyak kalau ada orang telphone …dia tanya …saya

dikantor Cyber…orang itu tunjuk gedung Cyber yang dimana …di jalan apa tu ..

R3 : kuningan itu …

R1 : ya …jadi banyak orang nggak tau kalau Cyber Crime itu polisi … jadi ..kantor apa sih …saya bilang gedung Cyber …keren ….o..dia pikir gedung Cyber yang tinggi itu …

M : nah kalau temen – temen disini harus cerita …apa sih Unit 5 Cyber Crime itu …

R6 : kalau saya ….

M : enak nya darimana kalau jelasin tu …

R6 : kalau saya jelasin nya …kita nggak jelasin ke umum ya ….karena kan kita lebih banyak ke kantor …kalau ke umum pun…kaya saudara – saudara saya tanya ..e..Intan dimana …kalau saya ..mami saya kebetulan datang dari Kupang …kebetulan kan dia juga Sarjana Bahasa Inggris …dia dijelaskan dia lebih tau karena Cyber Crime dia tau artinya …tapi kalau saya jelasin mami …saya berperan itu …menangani…seperti yang saya dapetin dari Komandan saya ..gitu …saya berperan itu menangani kasus – kasus ….yang berhubungan dengan satu ada komputer …dan satu lagi lebih kepada internet …kejahatan itu bisa dilakukan di internet …saya nggak ngambil contoh yang jauh – jauh …misalnya saya transaksi sama mami …kita buat kesepakatan melalui internet …jadi nggak usah pake surat …ditulis disini …tapi kita bertransaksi di internet …itu kalau sudah mami melakukan kesalahan …bagi saya itu sudah suatu kejahatan ..itu yang saya tangani …jadi saya nggak bisa nerangin macem – macem pake bahasa Inggris …seperti bapak – bapak ini bisa jelasin …tapi yang salah satu contoh yang bisa mami saya ngerti …o..ya …Intan itu di unit yang agak rumit …yang agak susah …nah dia agak mengerti kalau saya jelasin itu …

M : jadi yang agak rumit …agak susah …ya …

R : e..he…

R3 : sebenernya mau jelasin kemana pun ….

R6 : ya ….

M : nah justru itu misalnya itu …kalau ada orang tanya …inikan orang nggak tau …darimana caranya …menjelaskan ..

R3 : susah juga lho kita mengatakan di Cyber Crime …apalagi dengan IT….IT itu aja apa …artinya satu – satu nya unit yang menggunakan istilah dalam bahasa Inggris di Bareskrim itu unit kita …IT….IT sendiri udah istilah tehnis bahasa Inggris …disingkat lagi kan …information Tehologi kan …itukan udah ..udah ..terlalu …udah terlalu gemana …kalau dijelas kan di depan umum bingung …orang – orang …

M : kalau misalnya orang – orang nya itu saya dan temen – temen saya …disini …saya nanya …kalau temen – temen disuruh menjelaskan ..

R3 : apa itu Cyber Crime …

M : ya …apa itu unit 5 karena kan kita udah ngomongin …apa satuan kerja lah …

R : ya …

M : gemana …gemana cara menjelaskan nya …dan dari mana mulai nya untuk menjelaskan sama mereka …

R3 : e…yang jelas pertama kita ngomongin …

M : apa yang perlu dijelaskan deh …

R3 : unit Cyber Crime itu adalah bagian dari Bareskrim mungkin … ..
kalau Bareskrim mungkin orang udah tau …orang udah tau Bareskrim …a…kemudian kita jelasin lagi di Bareskrim itu ada beberapa bagian nya lagi …bawahnya lagi …ada direktorat – direktorat nya …mungkin agak..agak kritik juga kalau jelasin direktorat …juga..yang mengetahui istilah nya …..

R : ya bagiannya aja…

R3 : a…ha…bagiannya aja gitu …bagian dimana unit 5 nya ini ada dibagian Ekonomi …dan khusus …kejahatan – kejahatan yang berkaitan dengan ekonomi …dan kejahatan – kejahatan specific …khusus…

M : ya…ya …

R3 : nah di unit 5 ini …menangani kejahatan – kejahatan yang berka-itan dengan penggunakan komputer dan jaringannya …atau pun kejahatan – kejahatan yang menjadikan komputer dan jaringannya itu sebagai sasaran …jelas nggak kalau dihubungin kaya gitu …

R1 : mungkin gini …pendapat saya …

M : karena gini…maksudnya pertanyaan …tapi mungkin kalau tadikan mbak siapa tadi …

R : mbak Intan ….

M : mbak Intan …tadi bilang ..kalau kita jelaskan sama orang …saya pengennya jadinya satu – satu …

R : ya …

M : tadi mbak Intan cara menjelaskan nya seperti itu …lain lagi dengan cara mas siapa …

R : mas Alex…

M : mas Alex….nah kalau yang lain seperti apa …kalau mas Ketut gemana cara menjelaskan nya …

R1 : jadi gini….e…

M : dari mana mulai menjelaskannya ….

R1 : tergantung ….pertama tergantung dulu siapa yang bertanya …
kebanyakan orang – orang yang nggak bukannya nggak berpendidikan …tapi mungkin yang hanya SMA …misalkan ..atau supir …atau apa …dia nanya ke saya …saya nggak akan bilang saya di Cyber Crime …saya bilang di Mabes …atau di Bareskrim ….Bareskrim itu orang nggak banyak tau …jadi saya bilang Mabes …pasti orang tau …nah begitu si penanya levelnya udah agak tinggi …dia tanya saya dimana …saya bilang …saya di Mabes …Mabesnya dimana …dia nanya ….saya bilang di Bareskrim …di Cyber Crime …abis itu dia mulai diem lagi kan …dia nggak tau …di ..diumum banyak yang nggak tau …tapi kalau orang bilang Bareskrim ..pasti tau …itu untuk kita bertanya …tapi kalau untuk orang – orang dalam dia polisi tapi dia bukan di Mabes ..banyak juga yang tau unit Cyber …Cyber Crime …tapi kalau orang sipil dia taunya Bareskrim …tapi kalau Cyber nya sendiri ….banyak yang nggak tau …karena mungkin…memang inikan masih baru …2003 atau 2004

R : 2002

R1 : 2002 ..mungkin …ya banyak…yang …yang nggak ini lah ..yang nggak tau …tapi ada juga yang tau …tapi belum banyak yang tau kalau di Bareskrim …

M : seberapa sering sih kejadian kaya gitu …orang – orang nggak tau

satuan unit 5…

R6 : banyak….

R all : banyak ….

R3 : kadang kalau kita telp keluar …misalnya nanya keluar…ini dari mana …kita mau bilang dari Cyber Crime …nggak ngerti …kalau kita ngomong dari Bareskrim Polri …baru mereka nyambung …

R10 : tapi nggak juga ..saya kalau keluar …banyak yang …dines dimana …di Cyber Crime …wah ..kalau udah denger kata – kata Cyber Crime …wah..dikiranya kita orang yang ……paling …

R : dia bisa gitu karena kita polisi. …

R10 : rata – rata ..sekarang dines dimana …di Cyber Crime Mabes Polri …kalau yang polisi udah berpikiran wah….*…….* ya dianggep udah paling jago …dalam hati sih ….

R3 : cemen…

R10 : ya ..gitu aja …hah.aha.h.ah.a

R2 : tapi lain lagi di kampung saya …saya kalau pulang kampung saya menjelaskan nya …dia tau nya itu cuma Intel …dan Reserse …

R all : ya ….

R2 : dimana …saya kan juga biasa tugas di Pindad …katanya kamu masih dines di Pindad…nggak ..saya dinas di bagian Reserse …bagian apa ..bagian Komputer…karena berhubungan dengan komputer kan ..karena dia kenalnya kan…kalau saya jelaskan …keliatan nya nggak nyambung …dan dia tanya bedanya Reserse sama Intel apa sih …

M : lebih banyak yang tau ya …selama ini …kalau kita ngomong sama orang …lebih banyak yang tau atau lebih banyak yang nggak tau ..

R : fifty – fifty lah …

R6 : karena masih baru …

R2 : kalau di Jakarta orang udah banyak tau …tapi kalau yang saya temuin sih banyak yang atau …

R7 : semuanya sih rata – rata tau …

M : kalau orang luar …

R6 : yang tau yang Sarjana IT…

M : Sarjana IT…

All ngobrol bareng ….

R3 : nggak …nggak umum ….

R10 : rata – rata pengalaman orang itu …Cyber Crime cuma menangani kasus …yang menggunakan alat komputer…

M : itu pada saat apa sih …

R10 : contohnya kaya SMS…itu Cyber Crime …

M : tapi pada saat …kan ada orang nggak tau …biasanya reaksi mereka seperti apa sih …

……..

R6 : karena dipikiran mereka …itu kejahatan komputer. …

R2 : dan bisa betulin komputer.haha.h.a.ha

R3 : itu yang paling sering …hhah.a..a.paling sering kalau diling-kungan polisi …kita bahkan bisa betulin komputer …

R2 : kena virus…kena virus…telp Cyber Crime …haha.ha.h.a.

R1 : jadi gini …ada pengalaman pribadi …saya naik ke ruangan ..ada

tu di ruangan Cyber ..diatas nya ada ruangan Perbankan ..terus ada ruangan Indag …saya ke ruangan Perbankan …ketemu rekan saya Hadi …disitu ada senior juga ..ada Bang Rizal …pas saya masuk ke atas …saya ngerokok keatas …ketemu sama saya …nah ini orang Cyber Crime ..coba tolong dibenerin komputer nya …padahal komputer saya juga kena virus …

R all : ha.ha.h.a.a.

R3 : emang kebanyakan gitu …

R1 : jadi yang mereka tau Cyber itu jago segala – galanya …

R3 : padahal cemen…

R all : cemen….hah.a.ha.a.jagonya cuma chatting …

R9 : orang Cyber itu bisa berbahasa Inggris …

R3 : orang Cyber itu udah keluar negeri semua …

R6 : padahal kita ngomong nya juga masih …ngak…ngok…tapi Dimata temen – temen saya hebat sekali …..

M : oke …

R10 : apalagi …apalagi di laptop itu foto nya yang diluar negeri semua …hah.ah.a.h.a

M : padahal itu …

R6 : tapi saya bangga di unit saya …

R10 : pas dibuka …wah dimana nih …di Singapura …Singapura sekolah …ya …padahal jalan – jalan ….

M : oke ….

M : nah ini yang saya tertarik ….kan tadi dibilang kalau pas ada reaksi orang dan cara menjelaskan …adalah menjelaskan dengan sesuatu yang kayanya supaya lebih dikenal sama orang gitu kan …soalnya ada dua …tadi ada yang bilang …sampe ada yang bilang …ngomong apa ..menjelaskan Reserse …dengan Intel….saya masih belum lancar …istilah – istilah polisi …bug dog….apa gitu …kan suka ada …kalau menjelaskan kepada mereka …itu lebih…lebih mudah …menjelaskan dengan sesuatu yang lebih dikenal …

R2 : karena kita menjelaskan ke orang itu …biar orang itu …orang yang kita ajak …kita ajak bicara itu …bisa mengerti dengan mudah …tapi dia harus gemana …gitu …apa sih namanya Bareskrim itu ….karena apa …Bareskrim itu adalah singkatan – singkatan ..boleh dikatakan polisi itu sering menggunakan istilah – istilah yang tidak lazim …digunakan oleh orang …kadang Bareskrim …kadang apa …pengumpulan dan pengolahan data nanti sehingga singkatan – singkatan itu …e…di *…* oleh orang umum…sehingga kita menjelaskan ke orang ….orang itu bisa berpikir dua kali …untuk mengerti ..

R6 : kalau masyarakat itu …tugas polisi itu yang diliat …Polantas … menangkap …kalau udah dibilang menangkap pasti Reserse ..

R3 : kalau di Makasar orang bilang …bagian ..Sekrea….

M : apa itu ..

R3 : Reserse itu …

R6 : kalau dibilang menangkap …pasti dia …o ..menangkap ..pasti reserse …

R3 : jadi yang kaya tadi Pak Arief ngomong …tergantung orang nya .. kita kan orang ini ..latar belakang nya apa dulu …dia nanya …dia nanya gitu …kita liat dulu orang ini kelemahan nya sampe sejauh mana …kalau kira –

kira dia bisa dan paham dengan penyampaian seperti yang kita sampaikan …ini Reserse ..ini Intelejen …ini Bareskrim …ya ngertilah …bisa …bisa kuasain …kaya ini ya …Cyber Crime itu ini …ini ….

M : apalagi jaman saya kecil dulu namanya Tekab …

R6 : Tekab …ya ..kakak saya Tekab…

R3 : tapi ngomong ke orang yang nggak tau …taunya polisi itu yang ngatur lalulintas …yang nangkap – nangkap …yang patroli – patroli yang seperti itu …dulu ya …Reserse …ya Intel …

R4 : temen saya ada dulu ….dia tanya saya tugas dimana …saya bilang saya di Cyber Crime …dia bilang bahaya tu…karena dia pelaku kejahatan ….hahah.a.

R all : hhaah..h.a.a.

R4 : ya …memang dia kegiatan gitu…selama kuliah ..

R2 : Hacker…

R4 : Hacker…

R2 : berarti dia tau …

R4 : langsung tau dia ….

M : ini memang satu hal yang menarik ya …tadi dibilang reaksi orang biasanya wah …ini hebat …

R : ya …

M : kalau menurut pendapat temen – temen sendiri gemana … melihat reaksi mereka ….bukan ini ya …bukan tentang apa ya …sorry ..maksud saya terhadap reaksi mereka nya …

R2 : saya kira wajar …karena dari bahasanya aja …bahasa asing ..IT Cyber Crime …kita juga harus menyadari bahwa e…dengan nama itu kita jadi terbebani untuk lebih ….lebih untuk mendalam

R5 : mereka mengatakan kita hebat …yang gemana – gemana karena ..apa namanya …latar belakang …dari ketidak mengertian mereka …

R3 : karena pandangan orang yang awam …dia berpikir nya …ini berkaitan dengan komputer …komputer itu sesuatu yang rumit …apa ..terlalu…apa …nggak sembarang orang bisa kan …nggak sembarang orang bisa menguasai komputer. ..kalau orang bekerja di Cyber Crime berarti ….hebat dong …hahaha..yang berpikiran seperti itu …berpikiran ya …wajar dong…

M : nah sekalian nanya …sekalian nanya …kalau ada polisi terus kerjanya ngomongin Cyber Crime …apa sih sebenernya kerjanya

R3 : ya sebenernya sama dengan penyidik …

M : penyidik …

R7 : penyidik juga…tapi patroli Cyber …nggak gini bang…kalau orang umum …itu setau saya …saya juga sering ditanya ya …apa sih Cyber Crime itu …

M : Cyber….

R7 : Cyber Crime …Siber krime gitu lah …hah.a..itu kita menjelaskan memang agak susah ya …setau …sepengetahuan saya …kejahatan lewat internet ….dia balik bertanya ….kenapa sih koq kejahatan bisa di diteksi dengan internet …dengan komputer …sedang kan orang – orang polisi biasanya itu kejahatan itu …tau orang umum itu …nangkep ini lho penjahat nya …ditangkep nih ..jadi nyata …nyata gitu …kan ketangkep dibawa ke

polisi proses ..ini jelas – jelas diliat mata …sedangkan ini kejahatan di internet itu kan komputer ..kenapa bisa …itulah…orang – orang itulah …lho koq bisa …orang umum mengatakan koq bisa sih …

M : makanya dibilang hebat ….

R7 : penjahat ditangkep ….lewat komputer …bukan ditangkep lewat komputer maksudnya …dicari penyadap gitu …ini bisa dinyatakan tersangka atau ini terdeteksi …karena ini berbuat tindak pidana …lewat komputer itu …nah dia baru berpikir …koq bisa …lewat komputer koq bisa …gitu …

M : makanya dibilang hebat …gitu …dari hal itu yang bisa menyidik

R7 : ya …kan nggak semua orang bisa …

R3 : orang kan berpikir kan komputer gitu kan …wah hebat nih … komputer ...

R : nah itu …

Responden ngobrol bareng ….

M : apa bedanya ….*…* tentu saja polisi dengan penyidik itu lain … apa yang istimewa ….

R4 : yang istimewa mungkin mas karena dia penyidik nya kan …kalau apa …..di Cyber Crime itu kan nggak bisa nyata …kejahatan nya yang maya lantas bisa terungkap …beda dengan reserse – reserse yang …

R7 : tekab ….

R4 : yang menggunakan …*…* kan jelas …

R7 : jelas pelaku nya ini …

R10 : salah satu contoh begini ……yang waktu pak Arief …Pak Alex yang waktu kita kerjakan dimana …di Probolinggo …orang bingung koq bisa sampe kesana …padahal …

R3 : bisa tau koq pelakunya disana …

R10 : pelakunya ada di Probolinggo koq bisa ditangkep …jangankan masyarakat umum …polisi mana …polisi Probolinggo tadi juga bingung …koq…Cyber Crime

R3 : gemana ya …

R2 : gaptek …

R3 : gaptek ….nggak ngikutin …nggak ngikutin

R7 : kemajuan jaman …

R3 : a….ya …dan banyak an itu ,…anggota polisi …berpikir nya itu praktis nya ajalah …jarang yan berpikir yang ribet – ribet…

R6 : praktisnya itu bagaimana caranya duitnya banyak …tapi saya nggak pusing dengan yang yang rumit gitu …

R2 : nggak mau repot …

R1 : nah ini mas …jadi ada satu spesifikasi yang sangat berbeda pekerjaan antara nyata dan tidak nyata …

M : saya sambil nyatet ya ….

R1 : jadi dalam hal mungkin orang udah tau semua bahasanya …jadi dalam hal penyidikan …kalau di kejahatan nyata yang nggak tau kaya kriminal secara umum …itu kalau untuk penyidikan …kan itu betul – betul orang yang peka …orang yang menyelidiki …diambil di lokasi …tapi kalau kejahatan di internet penyidikan nya itu adalah berupa seperti imajinasi begitu ..kita masuk ke suatu …e…room nya orang …jadi kita pura – pura …jadi penyidikannya bukan dengan manusia yang hadir …tapi bahasa –

bahasa …bahasa – bahasa komputer lah istilahnya …peralatan komputer ….nah itu yang bikin sulit …dan berbeda dengan kejahatan o..secara *…..*…penyidikan makanya pengungkapan kejahatan dari Cyber relatif sangat sulit …daripada penyidikan kejahatan nyata ..karena kalau kejahatan nyata dia bisa bertanya kepada orang lain …ya …itulah penyidik ,….dia juga bertanya kepada orang lain ..kalau kita penyidik dalam komputer ..orang ini kan benda mati …kita bertanya ini susah …ya itu dia yang susah ya itu dia yang susah dipahami …dalam hal itu…dalam hal penyidikan ..saya rasa versi – versi yang lain juga ada tu …

M : ini saya sambil mencatat ya …supaya nggak lupa …kan kita nggak liat diskusi ini …..

R : sebetulnya dalam penyidikan memang a….lebih sulit ya …tapi dalam pembuktian menurut saya ….sangat lebih mudah …karena bukti yang kita temukan adalah …bukti obyektif….

R1 : ya …

R3 : dan bukti – bukti nya pasti …

R10 : ya …buktinya obyekyif bukan bukti subyektif….

R3 : apa yang direkam …di komputer itu kan pasti …gitu …

M : oke ….

M : ini saya kalau tadi nggak salah tangkep …dibilang kenapa sih ….

R : kalau salah tangkep …bisa ….hah.a.ha.h.a

R6 : bukan intel …

M : salah mengerti ya …kalau saya tidak salah mengerti tadi dibilang kenapa orang – orang disini hebat …kayanya ada kesan e…koq bisa melakukan sesuatu yang tidak mungkin bisa dilakukan oleh orang lain …bahkan nggak keliatan ya …

R : ya …

M : itukan kalau saya pikir ya …ada bedanya nggak sih dengan dukun …

R : itu beda ….

M : apa bedanya dengan dukun…..nggak bedanya …kan gini ..koq bisa pake dukun …sebagai perbandingan gemana ….karena ini yang saya liat ada …ada. ..kaya esensi lah ya …kayanya erat …kenapa …koq tau ada sesuatu disana …

R : o…paranormal gitu maksudnya …

M : kesannya kenapa itu jadi hebat …orang – orang kan beitu hebat …tapi ada yang nggak bis di mengerti satu sama lain …

R : itu logika ….

R3 : ya …benar …koncinya disitu …dukun itu tidak logic …

R1 : ya …

R3 : ya …kan …karena disini kita bekerja berdasarkan logika …logic gitu …ya…satu lagi mungkin gini …Indonesia ini kan menerima komputer …internet itu blek…langsung jadi gitu lho …o..kita kan tau nya o..komputer itu seperti ini …internet itu seperti ini …proses nya kan kita nggak pernah tau kan ..ya …di Cyber Crime kita tu mempelajari itu …suatu …misalnya terjadi pengiriman email …isinya apa – apa gitu kan …orang kita awam taunya breg ..itu email kita terima …nah di Cyber kita mempelajari …menelusuri …kebelakang …ini prosesnya gemana ..sih …sampe email itu

ada disitu …yang jadi spesific disitu …orang jadinya o…hebat dong …Cyber Crime …

R1 : itu namanya …istilah dengan *…* Tehnologi …

R3 : terus kalau dibilang sama … apa bedanya dengan proses nya .. metodeloginya …yang nggak ada …di dukun nggak ada …

M : oke ..prosesnya berbeda tapi kayanya akibat atau kesaktian nya jadi ….*….*

R all : ha..ha.h.a..

R10 : dukun saktinya mungkin lupa …

All ngobrol bareng

R3 : semboyan reserse aja Sidik Sakti kan …ha.ha.ha.

R6 : rajawali …tangkap …

R : jeli bak Rajawali …hah.h.a.aha

M : oke …ya …ya ….nah satu lagi …saya tadi mau tanya soal ini… e..kebanyakan kalau polisi ..pengen …elo udah dapet duit …tapi nggak ribet …brag….

R3 : itu…itu banyak …

M : jadi dapet nya gemana …

R6 : itu nggak polisi aja ….

M : ya betul …sebetulnya terjadi dimana – mana ya …mungkin kalau dia jadi ….

R1 : kalau misalnya mudah kenapa di persulit …

M : oke …

R6 : mungkin gini …karena Cyber IT …tadi Pak Arief bilang banyak polisi itu gaptek …ya termasuk saya ..juga gaptek ..begitu saya masuk unit Cyber …kita belajar nya juga seperti kura – kura …terseok – seok ….begitu nggak tau teriak sana …teriak sini …padahal begitu dijelasin…oh ya ..begini …oh ya …begini …ya mungkin polisi lain juga begitu ..nggak mau ribut …dengan …

R3 : nggak mau melalui proses…

R6 : nggak mau *….* …tapi maunya mereka menyelidiki kasus – kasus yang memang menghasilkan duit …tapi saya tidak mau pusing dengan IT ..IT ini …karena banyak juga diantara temen – temen …mau pindah ke unit Cyber …nggak ah ..susah …kenapa susah …padahal paling enak …

R3 : awalnya saya ditanyain gitu …begitu ditanya ..kamu dimana Lex …..diunit Cyber Crime ..IT…ngapain gabung disitu …di gituin saya ..

M : oke …ini menarik …ni…semua temen – temen disini memang memilih ..atau ditugaskan ..atau gemana …

R3 : posted kan itu …

M : tertunjuk …

R6 : kalau saya terbuang malah ….

M : terbuang …

R6 : karena di Indap nggak butuh itu …waktu itu

R3 : kalau saya sebenernya Lucky …

M : lucky….gemana sih …

R : tertunjuk….

R3 : a….awalnya …saya udah di Satgas waktu itu …saya dulu Satgas sama sama Pak Budi …saya …saya …rencana penempatan saya itu …di ..direktorat lain …di direktorat lain di ditasemen khusus anti terror …pro*..*

tapi ada senior yang mengubah …fronting penempatan saya masuk Cyber …saya jadi dressing miss dress .

M : apa artinya tu …

R3 : ya ..tadi saya berpikiran nya gini saya mendengar kabar dari temen – temen orang yang berdinas di terorisme ….anti terror jarang berkumpul dengan keluarga …pokoknya jarang pulang lah ..resikonya besar ..

M : anti terror …

R : duit nya nggak jelas…

R3 : duitnya nggak jelas ..kita ngomong nya gitu ya …saya nggak berpikir begitu ya …saya berpikir nya pertama kapan berkumpul dengan keluarga nya …ya kan…terus resikonya ..jelas kita berhitung resiko kan .. begitu ditempatkan di Cyber …wah..ini kan jadi ada perubahan besar kan …kebetulan saya hobby

M : emang hobby disitu …

R3 : hobby ….di komputer …

M : tadi dibilang Lucky …

R3 : Lucky kan jadi nya …dari terror …ditempatkan di posisi yang menurut saya pas dengan ini saya …

R1 : o..diliat dari latar belakang …lebih cocok …

M : orang bisa jadi punya pengalaman …atau apa namanya …sikap yang beda – beda juga …kalau yang lain gemana …apakah … juga merasa Lucky …atau memang …

R6 : saya nggak merasa Lucky saya…

R1 : saya merasa dibuang …

R6 : saya dulu waktu validasi …saya *…….* dari situ ..itu ..waktu itu Kanit nya nggak dibutuhkan …kau masuk aja ke unit Cyber Crime ..saya pikir koq saya ke Cyber Crime …koq susah banget …tapi begitu saya di Cyber Crime banyak sekali yang saya dapet….saya bisa keluar negri ..saya ngerti internet …saya mengerti komputer …temen saya nggak tau…saya tau …puluhan email saya tau …apa itu browshing …apa itu chatting ..temen saya nggak ada yang tau sampe hari ini ….mereka nggak punya email…saya punya email …..saya bicara sama di angkatan saya …dan saya dianggap mereka tu hebat …hebat sekali …

R10 : kalau saya kecewa awalnya …haha.ha..

M : itu menarik tu….gemana …

R6 : jadi saya Lucky…pak Alex Lucky…

M : ada ilmu perbankan disini ..h..h.a.ha.h.

R10 : pada awalnya kan …bisa di *…* Pak Alex..Pak ketut dulu sama – sama dari Satgas ya…pokoknya dari Satgas dulu *……..* pada saat itu …nah cuma bagi orang – orang yang …yang ini …pendapat pribadi saya …bagi orang – orang yang e…menentang dengan kebijakan ……

R3 : pimpinan…

R10 : pak Agung ya …saya gara – gara ….disuruh *…* saya nggak mau waktu itu …dapet ….*…..* akhirnya pada saat floting pertama …nama saya nggak ada …nama saya nggak ada waktu itu …terus e….ada floting berikut nya ….Cyber Crime …saya sempet kecewa …kecewa nya apa …karena saya menggunakan komputer cuma bisa untuk …ngetik aja paling

...sementara kejahatan – kejahatan di Cyber Crime itu saya masih bingung ...apa yang mesti saya kerjakan ...apalagi Cyber Crime di Mabes Polri ..takut nya begitu balik ke ..pulang ke Bogor atau kemana ...apa Cyber Crime itu saya nggak bisa jawab ...saya khawatirnya ...gitu ...

R1 : ada rahasianya ...ada yang lebih phobia daripada saya ...

R3 : ya itu tadi Pak.,..seperti yang saya bilang ...polisi itu umumnya gaptek ...mau menggunakan komputer itu hanya untuk ....

R6 : ngetik BAP dan surat ...

R1 : Pak Budi itu memang ditugaskan di Perbankan ...kemudian saya main keatas ke Hadi ...disitu ketemu dengan Pak Rizal ...saya ngeliat ada ketikan agar TR ya ..*.....* ...Budi ke Perbankan ...terus di Cyber TR udah keluar ...Pak Budi masuk ke Cyber Crime ...itu saya nggak tau ...apa itu Cyber ...saya bilang ke Pak Rizal ...Pak ini udah ada TR nya ..masuk ke Cyber ..terus ditarik lagi ke Perbankan ...akhirnya itu nama langsung di coret kan ..karena udah ada TR masuk ke Cyber ...tadi nya mau ditarik lagi ke Perbankan ....

R10 : TR yang keluar itu nama saya nggak ada ...jadi yang settle nama – nama orang yang bertentangan dengan Pak Agung saat itu ...

R3 : ya ...kita langsung di buang ...mas nggak tau TR itu apa ... Telegram ...Telegram Rahasia ...TR ...

R6 : tapikan setelah itu berbahagia kan di unit Cyber...

R10 : saya sangat bersyukur....

R6 : nah....itu. ...

M : saya kira merasa dibuang ...

R10 : saya nggak merasa kebuang ...saya ditempat kan di tempat yang tidak sesuai dengan keinginan saya ..kalau keinginan justru saya kalau bisa saya itu pengen ke ...*...* bukan ..bukan karena itu ...memang dulu juga pada saat saya masih di Polresta Bogor...banyak kasus gugatan yang saya alami

R3 : soalnya kita udah punya pengetahuan disitu kan ..

R10 : ya ...kebetulan saya masuk ke Cyber Crime masih blank ...tapi setelah saya jalani ...ternyata saya sangat beruntung ...beruntung ...ya banyak ilmu dan...yang saya dapatkan ....kalau untuk *.....*saya udah sempet keluar negri ..walaupun itu ke Singapura ..

R6 : nanti ke Tim Tim ....

R10 : terus ....kalau *...* keluar itu begitu ngomong dines dimana .. Cyber Crime ...orang – orang udah ..wah ...hah.a.a.a.padahal ...haha.dulu sebelum masuk Cyber Crime ...saya nggak bisa main Chatting ..main interenet ...itu nggak ....nggak ..tapi setelah lama disitu insya allah ...

M : ada yang lain nggak...justru begitu masuk di Cyber Crime ini kaya nya ada sesuatu yang jadi beban ...atau malah ...

R7 : saya ...

M : oke ...

R7 : saya begini ...e....sebetulnya saya itu dari dulu dines ...karena mungkin udah kelamaan di Personel ya ..jadi seolah – olah saya mau terjun ke Reserse itu udah malas ...pertama kalau saya mau jujur ...di Polda Metro pu saya udah ditawarin untuk ke Reserse ...berhubung suami saya udah di Reserse ...dari awal nya udah di Reserse nggak mungkin saya ...dua – duanya di Reserse ....kita bagi....walaupun kita satu karakter...satu profesi

…hm..saya juga punya anak kan gitu …kalau nanti dua – duanya masuk Reserse ..bagaimana perkembangan anak – anak …e..waktu itu saya udah komitmen juga sama suami …oke ..saya nggak akan ke Reserse …cukup saya diturunin kan …jadi kalau personel itukan jelas…pulang dan berangkat nya itu jelas ..jadi ktia bisa ngurusin anak juga …kemudian ada temen saya ini …nawarin waktu itu ….

R3 : siapa itu …

R7 : ni ibu Dwi ini

M : jelasin dong

R7 : e…kronologis nya …mau nggak kamu masuk ke Bareskrim … Bareskrim itu gemana …gitu ..menurut saya sih waktu itu ya …nggak ah …saya nggak punya background Reserse ….nggak lah disana santai …pokoknya nggak …nggak rumit banget lah gitu ..belajar nanti juga disana juga bisa …kata temen saya gitu …karena udah termakan ini akhirnya saya oke lah …ikut ..daftar lah …begitu daftar sempet ditentang juga saya komandan saya..waktu di birokrasi …begitu saya kasih berkas …berkas sampai dibuang segala …sampe nggak mau tanda tangan ….kalau nggak mau tanda tangan ya udah …akhirnya saya ke Personel kan …gitu…komandan saya nggak setuju …maksud saya komandan langsung saya itu tidak setuju kalau saya mau pindah …

R1 : o ..pengen tetep disitu aja …

R7 : komandan saya mengharapkan saya harus disitu …nggak usah pindah …

R1 : kan TR nya ada ….

R7 : sebelum ada TR pak …ini sebelum ada TR …

R1 : o..belum gerilya …

R7 : hah..ha.ha..waktu itu ya ini ada desakan dari temen ini …udah Bareskrim aja ….

R1 : lagi pula udah bosen juga …

R7 : sebetulnya memang udah bosen …hanya saja pimpinan saya itu nggak memperhatikan saya …harus bagaimana gitu …

M : apa yang bikin ..sampe ngotot …walaupun atasan langsung tidak setuju tapi tetep …coba mengajukan …

R7 : e…pikir saya …karena saya udah pernah juga…ya …waktu birokrasi …jabatan saya itu tidak sesuai dengan apa yang saya kerjakan ..sebetulnya saya menjabat di A ….tapi saya di *…….* kerjaan di B…sedangkan jabatan B ini seharusnya lebih tinggi …tapi selama disitu selama tiga tahun ya …saya itu tidak dikukuhkan disitu …nggak ada istilah nya

M : ditingkatkan …

R : definitive gitu nggak ada …jadi jabatan saya tetep di A walaupun volume kerjaan itu di B .,..otomatis kan bertentangan dengan bathin hati nurani saya …akhirnya saya ngajuin secara tertulis …nah ngajuin secara tertulis …komandan saya merasa tersinggung …padahal itu ada surat resminya …ya …penawaran gitu …akhir nya berkas dibanting sama komandan saya itu …nggak ditanda tangani …ya udah …nggak ditanda tangani akhirnya saya melambung ke bagian personel nya …

R3 : harus nya udah syukur ya …nggak …

R7 : bagian personelnya itu ya ..istilah nya melambung lah gitu ..

melambung …mungkin dari personel itu dikirim ke Mabes …itu sempet yang Pak…yang personel itu …telphone ke komandan saya itu …

R3 : personel Mabes …

R7 : Personel Polda Pak

R3 : o……

R7 : personel Polda dulu ….sempet berdebat juga ..katanya ini anak nggak keluar …tetep ini saya pertahankan …akhirnya …pokoknya intinya nggak boleh pindah …akhir nya ya sudah gemana …karena saya udah mau pindah tapi juga bapak…komandan saya tidak memperhatikan nasib saya ..saya disitu udah bergabung tiga tahun hanya melaksanakan tugas tanpa ada pengukuhan …akhirnya saya melambung lagi ..kan gitu …to…

R1 : bu…tadi komandan nya udah pernah disampaikan kenapa saya sudah tiga tahun begini – begini aja …

R7 : sudah …sudah pernah disampaikan juga ..

M : ya …tadi sudah ngomong …

R7 : saya sudah ngomong Pak …secara lisan saya minta pindah ke jabatan saya …aja nggak dikasih ..terus …nggak mungkin dong saya minta Pak…saya dikukuhkan disitu kan nggak mungkin …itu nggak .haha..nanti menjilat diri saya …harusnya dengan saya ngomong begitu ….kan harusnya komandan harus bisa berpikir …gitu …akhirnya melambung lagi …masuk ke Cyber Crime ini …begitu masuk ke Cyber Crime saya jadi bingung …mikir …apa yang saya akan lakukan …saya bengong …jelongot ..kaya sapi ompong …bener terus terang bilang sama mbak Indri …mbak saya kayanya saya salah masuk sini …saya bilang …kenapa mbak…rasanya saya pusing mbak ..saya punya istilah jiwa ke reserse an itu nggak ada …

R : ser…ser…an nggak ada ….

R7 : kemudian …ya udah lah …

R4 : apalagi salah chatting ya bu ya .,…

R7 : sama :…hah.ah.a. Dwi yang buka – buka komputer …sampe sekarang ilmu yang saya serap ya …masih nol aja …gitu …tapi saya alhamdulillah saya bersyukur walaupun masih delongot – delongot …saya udah pernah ke Singapura …haha.ha.itu bangga bagi saya …dan keluarga saya ….o..ya ..orang kampung …sampe ke negara tetangga Singapura …kan jarang …

R4 : ceritanya kan rame udah nyampe sana …

R7 : ya udah rame Pak …ini orang baru masuk Reserse …disangka nya kerjanya udah bagus lah ..udah dikirim ke Singapura …padahal disana delongot – delongot …haha.ha..itu aja tapi saya bersyukur dan saya sebetulnya e….hati saya karena udah terlanjur masuk …udah terlanjur nyebur …saya berusaha bisa …karena apa …hah.a.karena pekerjaan ini bisa diliat mata….kecuali mata saya buta …saya akan nyerah …a…sebetulnya bisa …dan saya intinya jadi orang pekerja …nggak mau saya itu orang males …istilahnya saya agak….tapi tetep …kalau saya memang udah dinilai pimpinan saya…dari dulu buang sana …buang sini …nyatanya saya sampe

All ngobrol bareng …..

M : yang lain gemana …..pengalaman waktu masuk ke Cyber Crime ..kan ada juga tadi …begitu masuk ya sebetulnya …

R6 : awalnya itu namanya bukan Cyber Crime …awalnya dulu waktu saya tahun berapa ya …waktu validasi …tahun 2003

R9 : bukan validasi mak ....dulu waktu saya masih di IMPEK...mama masih di PIG saya tuh masih di unit IMPEK ya ...Import dan Eksport ...dulu tu pecah ...bukan pecah ...ada unit baru namanya IMPOTEK ...dulu masih Pak Brata ...jadi ini belum berbentuk unit ya ...masih gabung sama ini ...

M : masih embryo ...

R9 : waktu di IMPOTEK itu sudah mau diajak pak Brata itu karena ada kasus nya si Rodo Sembiring ...

M : ya ...

R6 : maksudnya ...awalnya itu ...waktu validasi itu Ciber Crime itu sudah masuk ...tapi belum berdiri sendiri dia masih masuk ke unit INDAG .,..namanya bukan Cyber Crime ...tapi INFOTEK...Informasi dan Tehnologi ..

M : ini menarik juga ya ...

R9 : dulu nggak ada yang mau masuk ...ke Infotek ...asal ada TR yang masuk ke Infotek...pasti nolak ...apa itu Infotek ....

R6 : dulu dibilang IDT ...

M : apa tu ...

R6 : yang ketinggalan jaman ...IDT ...kan ada daerah IDT ...

M : o...desa tertinggal ...

R6 : jadi ini UDT ...unit daerah tertinggal ...nggak ada yang mau masuk ...nggak ada ...

R1 : gini mas ....sebener nya kan permasalahan nya itu ...saat itu jaman dulu...kita ngomong past tense adalah uang ...

M : penghasilan ...

R1 : saat itu memang waktu jaman kegelapan ...

R : jaman batu gitu ....

R1 : saya juga ngalamin kalau nangkep orang sih ...waktu saya jadi Kapolsek ...saya juga pernah melakukan ...melakukan juga memerlukan uang ...jaman saya pernah ...latar belakang – latar belakang itu jaman itukan biasa – biasa aja ....nggak jadi masalah...sekarang orang berfikir ...Infotek ...infotek ..kan kegiatan mana yang ditangkep ..apa yang mau dijadikan ...sedangkan orang lain yang di Mabes nggak tau ..nggak dapet jatah uang ....dengan perbankan aja banyak bank – bank gelap ..e..pemikirannya mungkin bisa untuk tambahan – tambahan penghasilan ...terus yang lain kan bagus – bagus ya ...makanya infotek jaman itu ,...apalagi sedikit ...orang nggak mau karena baru denger Infotek aja ...apa yang mau di ...

R : yang mau dikerjain ...

R1 ; apa yang mau dikerjain terus ...saya disitu dapet apa ...jadi kalau sekarang saya baru tau memang kalau kita berpikir ...uang ya susah....kita berfikir kemampuan aja .. menambah kemampuan aja ...nanti baru dipake ditempat lain ..baru nanti kita serap ...

R3 : kalau saya sih ...pertama masuk ...yang saya pikir bukan itu ... saya sadar dasar saya kan intelejen Pak ..saya bukan orang Reserse ..pemikiran saya yang pertama waktu saya masuk ...

M : apa bedanya sin Reserse sama Intelejen ...

R2 : jadi kalau Reserse titik berat nya ...dia penyidikan ...

R7 : undercover ....

R3 : *....* segala macem ...Reserse juga sama membuat laporan ...

awamnya ya …yang memeriksa laporan …Interlejen itu dia apa …membuat penyelidikan dan membuat laporan gitu aja …

R7 : tapi nggak bisa menyidik …

R3 : nggak bisa meriksa orang …

R4 : bisa memeriksa

R3 : bisa memeriksa tapi kapasitas nya bukan untuk menegakkan hukum ….

M : oke,….oke….

R3 : saya pikiran pertama begitu saya masuk Cyber Crime …saya langsung tau disitu ada laboratorium …ada yang dalam laboratorium forensic komputer nya dan ada yang untuk penyidikan …saya langsung nyadarin ..saya lemah dalam peyidikan …karena dasar saya intelejen …jadi saya ingat betul waktu ditawarin sampe masuk laboratorium kan …begitu Pak Hadi…siapa yang masuk laboratorium ..saya langsung sadar …saya lemah di peyidikan ..

R : tiba – tiba dia pingsan ….

M : saya mau tanya dulu nih …yang dimaksud dengan penyidikan itu itu apa …bisa cerita nggak ….

R3 : penyidikan kan ….

R : serangkaian tindakan …

R3 : itu terlalu bahasa hukum ….

M : oke ….maksudnya ..saya …biar ngerti pake bahasa hukum nggak apa – apa ….

R3 : apa yang dibuat sama polisi ..membuat …apa …nyari bukti – bukti…meriksa orang ..biar orang itu …pelaku kejahatan itu bisa diproses di peradilan ..itu penyidikan …

R2 : jadi penyidikan itu mengumpulkan bukti – bukti ….

R7 : ha….buka kamus dulu..ha.ha.h.a.

R : jadi kalau nggak ada bukti – bukti itu ….

R3 : begitu saya dibilang mau laboratorium nggak …laboratorium .. pertama itu sejalan dengan hati saya …

R2 : ada yang bilang pebedaan intel sama reserse …kalau intel dari luar ke dalam …tapi kalau reserse dari dalam keluar ….

R3 : maksud nya luar kedalam itu apa …

R2 : contohnya saya …ada suatu kejadian …

R3 : jadi sentrifugal dan sentriala…

R10 : kejadian di tempat ..kejadian perkara …tapi kalau intel dia dari luar kedalam

M : oke….

R3 : jadi ada kejadian …orang reserse kan berpikir nya dari kejadian itu baru keluar ..dia baru mencari keluar kan ..kira – kira apa yang membuat jelas …kejadian ini …kalau orang reserse dia dari luar

R : intel…

R3 : intel itu dari luar masuk ke dalam …

M : nah kalau misalnya penyidikan ini siapa yang *……..* tapi kalau penyidikan yang dilakukan oleh unit 5 IT Cyber Crime ini seperti apa sih …

R3 : sama …konvensional penyidikannnya …maksudnya gini…artinya dia begini penyidikan *…* dan konvensional tidak pernah ditinggalkan …proses penyidikan konvensional tetap jalan ….a…yang unik disitu

..berkaitan dengan alat bukti yang harus dikumpulkan …bukti – bukti yang harus dikumpulkan karena ada ….ada berkaitan dengan komputer …jaringan komputer …dan sistemnya segala macem …kaitannya dengan bukti elektronik …itu yang spesifik …dengan fungsi lain …makanya dikita pun ada laboratorium ..ada laboratorium forensic nya …

R1 : jadi gini …

M : kayanya masih bingung ….

R1 : contohnya gini Pak misalnya …sama sih cuma saya lebih mudah lagi …kalau katakanlah orang mencuri …ditemukan ada bukti – bukti..mencongkel ya …merobek …tiu barang buktinya …

R3 : alatnya ada pisau..obeng apa…

R1 : ha….pisau …apa semua itu ..polisi mengumpulkan nya mudah kalau ada disitu …kalau di kita kan barang buktinya ..file ..log file …ya nggak ..

R3 : data – data digital …

R1 : data – data digital …dividen nya apalagi nih misalnya e..cakram nya ..ininya …ininya …itu agak sulit …

M : oke….

R3 : sama ….sama dengan yang umum …

M : apa itu berarti kalau tadi diomongin agak sulit …sama nggak sih kalau ngomongin tingkat kesulitan lah ..penyidikan yang dilakukan didalam *……..*

R3 : sebenernya nggak bisa dikatakan sama ya …yang saya bilang tadi susahnya itu ya di digital nya itu …

M : oke …

R3 : masalahnya KUHAP kita ..e..Hukum Acara Pidana kita tidak … tidak …tidak mengaku bukti itu ..disitu masalah nya ..jadi yang dilakukan oleh penyidik …rekan – rekan temen – temen penyidik ini …gemana data – data yang ada itu …seperti yang didapat dari komputer ..dan media penyimpanan lain itu bisa menjadi alat bukti seperti yang diharapkan oleh Hukum Acara Pidana ..

M : hm….

R3 : tapi itu e….ada beberapa kejadian …kejahatan yang khusus memang udah mengaku model itu ya …ada bukti lain termasuk data elektronik ..cuma kalau kejahatannya e…misalnya penghinaan …tapi dia menggunakan media internet …kesulitannya kan disitu …bagaimana data yang ada dikomputer itu bisa kita gunakan memenuhi alat bukti yang di..hukum acara Pidana …yang tidak di akomodir ..data digital itu tidak di akomodir ..sama hukum acara pidana kita…

M : jadi gemana kiat – kiat nya …

R10 : mungkin tingkat kesulitan nya contohnya tadi sudah dicontohkan oleh Pak Alex …penggunaan melalui internet …itu kan dalam KUHP dikatakan barang siapa….mungkin agak mudah barang siapa melakukan ..e..kemudian nanti dikatakan dimuka umum ..

R3 : nah apakah internet itu udah media umum …dimuka umum …

R10 : dalam penyidikan kita perlu apa …masih menganalogi ..masih

menganalogi kembali apakah …dengan menista seseorang melalui (internet) ..internet itu sudah dikatakan dimuka umum …gitu ….sedangkan kesulitan dalam memenuhi unsur

R3 : tadi mas nya nanya …langkah keluarnya apa …jalan keluarnya apa ..

M : ya …kiat – kiat nya apa….

R3 : kita menganalogikan …artinya …

M : oke ..maksudnya menganalogi kan .. ..

R3 : jadi…misalnya kita berpikir nya kan seperti ini …dulu aliran listrik aliran listrik dulunya kan ditetapkan dengan …sebab pencurian aliran listrik dulunya …dulunya udah ada …*…..* dikatakan sebagai benda …termasuk benda kan dia barang …nah kenapa kita berpikir nya bahwa data elektronik yang ada di e..jaringan komputer atau di media – media komunikasi lainnya ..itu sebagai …sebagai barang atau benda …apa bedanya dia dengan aliran listrik …kan kita menganalogi nya seperti itu ..misalnya orang kasus yang …sebenernya yang banyak a…deface itu sebenernya hacking ya …perbuatan hacking …dia kan masuk kejaringan orang merusak gitu kan ..ha..kita…kita bisa menganalogikan …dia melakukan perbuatan merusak …dia kita analogikan masuk ke pekarangan orang tanpa ijin dan pengrusakan gitu …

R1 : nah maka itu lah mas …saya nyambung ke Alex. ..benda lain juga ditingkat peradilan …maksudnya kejaksaan …hakim …kita dengan Pak Budi pernah ya …

R10 : ya …

R1 : kita sama – sama ketemu jaksa …terus dia bilang kesaya …email ..email bagaimana …dia email nggak ngerti …gemana kita mau ngejelasin berkas yang banyak itu …yang kita bawa itu …ini melalui email…email itu apa …ya pak..gemana email…saya gemana ngejelasin nya …kalau di kejaksaan tinggi nya itu nggak ngerti ….itu dikejaksaan tinggi …terus yang kedua pernah juga ada kasus yang dikembalikan lagi …karena pertanyaan nya ..tolong jelaskan bedanya laptop dengan notebook. ….itu juga begitu …kita lagi berbenah ya …tapi dia di kejaksaan ataupun dia hakim juga harus sama – sama …

R3 : sebenernya bukan Jaksa sama Hakim aja …tapi secara umum …

R10 : tapi jujur aja banyak salut nya juga …artinya yang di Cyber Crime ini banyak menemukan bahan – bahan …*….*

R1 : sebetulnya …menurut saya pribadi ya …sebetulnya mulai tahun ini …saya rasakan kita *…* seperti mendobrak beberapa bukti yang belum ada …ktia berusaha menemukan …seperti nya berusaha mendobrak ….makanya sekarang *……* yang terbaru ini mulai cepat – cepat dibutuhkan karena*……* itu kalau mau dibilang ..ya …ini yang ..yang …ada lagi kalau bukti yang agak susah ya …mungkin orang nggak lazim ya …misalnya kita melakukan kejahatan dengan komputer itu contohnya … yang dulu kasus *…..* kemudian kita hapus ya …file nya kita hapus …orang kan …kalau orang yang nggak ngerti …dan saya juga saat itu juga nggak tau …nggak semua orang bisa buka …dicari file nya kan sudah kosong …di line *..* juga sudah di hapus …terus cari data nya dimana….

R10 : nggak usah jauh – jauh waktu kita nanganin

R1 : datanya masih ada mas di hard disk nya …kalau dibuka …cuma

nggak bisa buka …karena orang itu pinter …dia bisa buka …data yang sudah dihapus …itu jadi bareng bukti …saya nggak bisa ..karena saya penyidiknya .

R6 : nggak bisa…

R10 : nggak usah jauh – jauh waktu kita nangani Cyber terrorism pada saat Max Spiderman melakukan e…logging ….logging ya …e..jaksanya nanya siapa saksinya …hah.a.a.a.

M : terus gemana ….

R10 : *…….* yang gue nggak ngerti a…sangat kecil kemungkinan ada orang yang menyaksikan …karena dia akan berhadapan dengan internet …

R3 : pelaku – pelaku kejahatan dalam komputer gemana ya …mas ya …dia dalam ruangan sendiri yang dihadapin cuma komputer…sehingga siapa yang mau saksikan …nggak ada kan …yang saksinya ya komputer dia

R10 : siapa yang menyaksikan ..

R3 : ya …umumnya memang masyarakat Indonesia

M : bagaimana kalau temen – temen disini sendiri melihat masalah itu

R3 : e….maksudnya …

M : jadi masalah nggak …

R3 : ya jadi masalah …

M : kenapa itu jadi masalah …

R3 : ya …karena kita kayanya gemana ya ….arti kata kita bertepuk sebelah tangan …ya ..kita ngerti orang lain nggak nyambung …

R10 : dan penyidikan kita dianggap tidak lengkap …karena ….e… perbuatan e…max spiderman tadi …itu dikatakan tidak cukup …emang ada azas .*……*saksi ….ya …tetapi kan bisa dikaitkan tidak harus seseorang a….melakukan perbuatan itu harus minimal dua orang …tetapi dengan saksi – saksi …yang terpisah …tersendiri tetapi berkaitan itu …bisa dikatakan …*…*

M : ini menarik sekali …banyak hal yang beda dalam penyidikan *……* cyber crime ini …kalau …kita kan sering juga dengar kata Manajemen…itu semua ada dimana – dimana …apalagi di dunia organisasi …dunia perusahaan segala macem …nah sekarang kalau kita ngomongin hal ini sekarang di *……* mungkin di unit apa …Cyber crime itu juga manajemen seperti apa sih …bisa diceritain nggak …apa sih sebenernya yang dimaksud dengan Manajemen …kalau saya dengar misalnya …waktu itu saya pernah denger juga …di ini kita punya manajemen yang bagus …apa artinya …

R2 : sebenernya kan Manajemen adalah ilmu untuk mengatur orang …atau menyuruh orang …dan selalu sama – sama kan …

R : di satu tujuan …

R3 : emang kita kerjanya bersama – sama team work ..yang jelas pertamakan setiap kita lakukan kegiatan yang jelas kan pertama setiap kita lakukan kegiatan ya …selalu ada

R1 : oke …oke..saya paham maksud nya …karena saya mikir lama karena gini kalau…yang dibutuhkan ada lah manajemen praktis ya …ya Practis Cyber ya …oke …kalau kita kembali ke teorinya …JohnTerry bilang kan tahun 1996 itu TOA training Organisasi itu lah segala macem …nah tapi kalau secara praktis di Cyber…yang kaya …menurut saya ya …yang

manajemen Cyber itu begini ...kalau ada kasus ada case ada perkara ...ditangani oleh penyidik ...barang bukti diserahkan ke Lab ...nanti dari Lab itu ...sudah dapet analisanya baru diserahkan ke kami ...

R3 : itu kan memang peng organisasi an kita ...

R1 : ya ...itu bagian dari Manajemen ...

R3 : bagian dari itu ...setiap ada kasus ...ada kasus kita menerima laporan ...begitu laporan kita terima ...yang ada pertama kumpul ...di penyidik e..jadi kita di Cyber itu ..pimpinan memperlakukan kita sama ...sama – sama penyidik ...jadi setiap ada pertemuan begini ...kita berada dalam posisi yang sama ...sama sama penyidik ...*.....*

R3 : .....yang pasti tujuan pimpinan itu pasti biar kita mudah mengeluarkan pendapat kita kan ...kita nggak ngeliat kalau dimana ya ...polisi dulunya militer ya ...dianggap sebagai bagian militer ...didalam ..*...* militer ...ya tau lah ...ada level gitu berhubung ngomong dia mau ijin dia ...ini begini ..begini ...tapi putusan akhir selalu pada senior gitu kan ...nah disini kita diubah gemana caranya posisi kita sama ...kita bebas mengeluarkan pendapat ...didiskusikan bersama

R10 : sejauh....

R3 : sejauh itu bisa di pertanggung jawab kan ...berdasarkan aturan atau hukum yang ada dan kita sepakati bersama dan itu dilaksanakan ...

R10 : tidak melihat siapa yang bicara ...

R3 : tidak melihat siapa yang bicara ...ya ....

M : menurut pendapat temen – temen kita sendiri ....

R2 : saya sependapat dengan pendapat rekan – rekan juga...yang perlu saya ....e...yang perlu saya tambahkan tu ...sebetulnya saya berangkat dari intelejen ..dari unit intel....satuan intel yang sebenernya tugas dan perannya itu sangat jauh dengan serse ...e...saya ilmu dalam penyidikan juga jauh sekali ...menurut saya mengerti aja ...kalau baca itu ...baca sendiri susah saya ...tetapi kalau selama ini yang saya masuk di unit Cyber crime Mabes Polri itu kita mempunyai permasalahan ...permasalahan itu kita pecahkan bersama ...punya permasalahan...umpamanya saya menangani kasus e...cyber crime ...itu kita ...kita diskusikan ,...kita rapatkan...kita diskusi kan dan disanggah oleh rekan – rekan ...sehingga itu merupakan pembelajaran yang ...yang sangat tepat ...yang bisa kita terima ...sehingga anatara yang belum bisa ...dan yang pinter ....itu akan bisa ngikut ...yang ..yang nggak bisa itu cepet ngikut ...itu yang perlu ....e....

M : oke...seperti itu ...

R3 : jadi kaya ...ini kaya jadi meja sharing ...orang bilang kan berpikir bersama lebih baik daripada kita berpikir sendiri kan ...dengan bersama – sama gitu kan kita secara tidak langsung itukan pembelajaran ...kita nyerap pengetahuan dari orang ....menjadi...e...apa ...kita bertambah jadi nya ...

M : oke ...ini sangat menarik buat saya ...karena kenapa ...karena kalau kita ngomongin di organisasi polisi menurut saya ...apa ...selain militer tapi tetep punya unsur militer...iitu jenjang karena hirarkis ...gemana pendapat anda ...apa yang hirarkis itu

R3 : e...hirarkis dalam hal ini tetep ada ...jenjang hirarki tetep ada ... dalam artian pangkat ada ...ya kan ...pangkat ..senioritas ada ... itu pasti ..jabatan pasti ...

R1 : coba kasih kesempatan dulu …mbak Indri …forward ..gantian coba …kan ini diskusi ..gantian ….kayanya saya terus nih …

M : yang lain bisa nanggepin juga ya …

R9 : bisa ….

M : oke …

M : oke …karena ini topik nya menarik lho …kalau menurut saya …betul ada hal itu …kenapa sampe …*…* seperti berpakaian sipil …terus memposisikan kalau dalam penyidikan ..semua di posisikan sama …kenapa itu jadinya satu yang istimewa …satu yang jadi penting atau …jadi ada yang positif …kalau tadi dibilang karena lebih cepet belajar …apa dengan cara – cara misalnya senior mengajarkan ke junior…itu bukannya cara yang cepet juga…apa bedanya ..

R7 : maksudnya gemana …

M : kan kalau dibilang tadi kenapa membiarkan semuanya berjalan seperti apa namanya …seperti mengalir tanpa harus ada hirarkis

R7 : bukan ..bukan membiarkan secara tidak ada hirarki nggak …kita walaupun sama rata …kesenioritasan tetep ada …

M : oke …

R7 : kita dari bawahan sama atasan tetep hormat masih ada …hanya saja kita kapasitas nya kalau di..dikantor …itu jadi masih ada juga….jadi kita diskusi bersama antara senior denga junior …itu seolah – olah tidak ada jenjang ..tidak ada keterkaitan …

M : koq bisa ngomong kaya gini …seolah – olah tidah ada jenjang .,.. darimana ….

R7 : karena semua …

R1 : karena ada AKBP, ada Kapten, ada Letnan 1…

R3 : sebetul nya kita memang ada hirarki …

R1 : kalau kita pake baju dines …itu pangkat nya beda – beda …

R7 : beda – beda …..

M : itu kenapa seolah – olah …

R : seolah – olah kaya sama aja …kan begini kalau diskusi …jadi sama – sama …saya panggil Pak Alex ya biasa aja gitu …

R4 : rileks mas

R7 : e..he…rileks …nggak terikat banget gitu …

R4 : keinginan kasus untuk bersama – sama …

M : artinya kalau kita baju seragam kita nggak akan bisa diskusi seperti ini ….

R7 : ya bisa juga sih …

R6 : bisa…bisa …

R10 : mungkin gini…dalam …dalam bersikap …e..antar perorangan itu kita tau ..jelas kalau memandang masalah hirarki …tetapi ketika kita memecahkan satu pekerjaan …atau satu permasalahan …kita tidak liat itu ..karena apa …kita menyadari bahwa belum tentu yang sekolahnya lebih pinter dia lebih tau …atau dia …dia pangkat nya lebih tinggi …dia lebih tau….itu kita kesampingkan ..*…..*

M : oke …

R3 : *……* ilmu social mas …jadi nggak bisa kita mengatakan yang senior pasti lebih tau …

R7 : nggak …

R3 : dan dia ilmu social lho ..
R2 : kalau diajarin senior secara langsung …itu saya kira .e…
R1 : lu tu ye. ..hha.ha.a.
R2 : kita nerimanya …
R3 : kita di doktrin kalau ngomong …
All ngobrol bareng
R1 : pokoknya gue nggak mau tau …haha.h.h.a.
M : saya …saya …darimana nih …bisa tau dan berpikir kaya gini .. karena ….
R3 : ya ..kita jalani …
M : oke ..bagaimana itu bisa berjalan ..karena yang saya tau … banyak yang pasti dari sekolah …sekolah ..pasti biasanya juga bukan seperti ini …
R6 : sebelum ini …ini kita bicara reserse ya …
M : ya …
R6 : sebelum reserse itu memakai uniform seperti ini …kita make nya itu PDH …
M : baju dinas …baju dinas harian …
R : kalau kita sudah kumpul…kita mengeluarkan pendapat …pun itu takut sekali
M : hm….
R6 : dan sampe sekarang masih ada pimpinan itu yang masih .. …
R2 : itu tergantung leader nya …
R3 : leadernya …
R6 : leader nya bagaimana …cukup …
R3 : leadernya memberikan itu …nggak …
R6 : betul saya setuju dengan mas Alex ….
M : oke…
R6 : sekarang masih juga ditemukan kita mau mengeluarkan pendapat …nggak boleh …ini saya yang punya …
R3 : saya pernah ngalamin……saya pernah ngalamin …kita lagi nanganin satu permasalahan ya …saya dari Cyber waktu itu bersama salah satu seorang senior …diminta bantuan mem back up …pekerjaan unit lain …direktorat lain ….sampe ditempat kita berkumpul …pimpinan yang ada disitu pada saat itu mengajak …oke ..kita sharing ..katanya kan …sharing …saya berpikir sharing seperti di Cyber …ngomong bebas apa adanya ..karena saya berpikir seperti itu …ya …saya ngomong seperti di Cyber …di tegur …kamu itu …wah …saya jadinya …wah ini salah bukan sharing jadinya …
R1 : kau ..ngapain ngomong kaya gitu …ha.ha.h.a.
R all : hahah..ha.h.a
R3 : jadi ya udah …saya berpikir …udah lah kalau gitu ..katanya tadi sharing …tapi kan tergantung siapa yang mimpin disitu …
R6 : jadi paradigma – paradigma lama itu memang nggak bisa ditang-galkan ….
M : dari kapan sih kaya gitu …kalau sekarang saya mau bilang gini … artinya sebelum dia tau *….*…nggak salah melepaskan hirarkis beberapa saat …sedang kan itu kalau dimiliter atau yang seperti militer …itu hal yang

lebih dihalalkan …tidak pernah ada terjadi gitu kan …jadi kita kan nggak tau acara seperti ini …

R10 : kalau saya merasa dulu …

M : dari kapan tu ..

R10 : kalau saya berasa waktu di Pusdik …mulai dari di Pusdik …
terakhir Satgas…Cyber …tapi waktu belum di Pusdik …waktu masih saya tugas di Polresta …itu masih jaman militer…ada beberapa perkara …ada tersangka ..*…..*

R3 : PTIK itu kebetulan diangkatan saya itu ada tujuh angkatan ya
..tujuh angkatan .,..boleh dibilang dari angkatan 91 sampai 97 angkatan 91 sampe 97 setiap kita ada diskusi …a.,..yang dibawa oleh pemimpin diskusi ..oleh moderator …segala macem …mengatakan ini media akan miss..silahkan bebas berpendapat …menyampaikan pendapat masing – masing …nah disitu saya mulai awal …o..ya …dalam meja ..dalam hal tertentu itu diperlukan ..kita tidak melihat jenjang kepangkatan …kita tidak melihat posisi kita…siapa kita. .perlu untuk memecahkan satu permasalahan ..PTIK selama dua tahun saya ngalamin itu…karena menganggap itu media …

M : itu dari PTIK ya …yang lain …dari mana …

R2 : sebenernya kalau masalah itu kan kita melihat dari ….dari..kalau
saya sendiri …melihat kebetulan setiap saya dinas pasti mendapat pimpinan yang demokratis …yang bisa e…apa …

M : saling sharing gitu …

R2 : namun lebih menonjol lagi pada saat sekarang saya ada di Cyber
crime …lebih menonjol….diskusi itu kita lebih cepet untuk menerima dibanding system perintah …kalau yang dulu waktu saya dikampung itu masih yang up down …

R6 : apa kata babe …

R2 : ya …kita diskusi tetapi …perintah tetep jalan …

R1 : kalau saya nggak ada pendapat ….saya point nya aja …pertama
di pendidikan saya di Akademi …jadi saya diajarkan 3…yang pertama adalah loyalitas …respek dan hirarki ..atau dibalik – balik …tiga – tiga itu melekat ..saya inget karena sering di beginikan …itu yang paling *…* diwilayah nanti kita didaerah …kita bekerja …loyalitas …respek ..hirarki …nah hirarki adalah yang tadi …yang tadi kita ngomong masalah hirarki ..yang berupa perintah …yang kedua hirarki itu tidak berarti jelek ya …kalau memang digunakan dengan tepat ,….tapi kalau digukan tidak tepat itu akan berbenturan ….karena kaitannya dengan birokrasi ….makanya kita sering menyampaikan masalah birokrasi …semakin tinggi birokrasi semakin jelek …ini nya …profesionalisme nya …itu kaitannya dengan ..dengan kemampuan …dengan profesionalisme kaitannya dengan hirarki …kalau terlalu gencar …jadi kalau hirarki terlalu gencar ..terlalu ketat akhirnya timbul birokrasi …contoh…saya mau memperkenalkan Kapolda …harus ini dulu …harus ini dulu …harus ini dulu …repot kan…kalau saya ada berita penting …ini saya alami waktu saya dines di Cirebon …ini nyata ….Kapolda Helmi Ismail …bintang 2….waktu saya lagi rapat di POLDA ….uh..waktu itu saya rapat di gedung hotel Avitamrin …seluruh perwira di Jawa Barat karena Wakapolda nya mau ngasih pengarahan …di wilayah …di Cirebon itu lagi ada kasus tawuran …sudah ada mobil Kodim yang dibakar …motor

polisi dan motor – motor yang ada di Kodim dibakar …sehingga anggora Polsek itu menyiram monil Kodim itu menggunakan helm …karena mobil nya dua yang kebakar …dan mobil – mobil disana banyak yang dibakar …

M : menyiram pake apa …

R : pake air …

R1 : air selokan …air selokan …

R2 : memadamkan ….

R1 : ya …memadamkan …

R7 ; memadamkan api ….

R1 : ini Perwira Siaga…Perwira Siaga ya …itu mau melapor ke Kapolda ..mau melaporkan ke Kapolres …karena Kapolres nya ikut …mau melapor juga ke Kapolwil …karena Kapolwil itu juga ada disitu ..diruangan rapat ..tapi nggak bisa karena ditahan di depan …ada apa …saya mau menyampaikan gini …gini ….nanti tunggu Pak Kapolres selesai….tapi ini mendesak …nggak bisa …akhir nya tunggu …dia sudah SMS …Handphone sudah ada …dia udah SMS ke Kapolres …Kapolres nya juga bingung …dia mau menyampaikan langsung nggak bisa …karena ini ..tadi itu…hirarki itu ..yang terjadi begitu selesai ….pengarahan …begitu langsung lapor …Kapolres …ke Kapolwil …berjenjang terus …berjenjang gitu ..kan nunggu …nunggu …sampai lah ke Kapolda …ijin Pak…gini..gini …gini ….bubar itu …suasana diruang itu bubar …kalang kabut ….saya juga ikut kelokasi tawuran itu ..udah hancur …saya kena tembak juga…

All ngobrol bareng

R1 : itu yang saya bilang kalau hirarki yang digunakan tidak pada tempat nya tapi bukan berarti hirarki nggak bagus juga. ..

R3 : ditempatkan pada posisi yang benar ….

M : oke …masih inget nggak gimana rasanya …

R1 : oh ya ..masih ada satu lagi saya tambahin…maaf ya ….e..kebetulan saya ada kesempatan ke Philippines disana saya ada pengalaman yang bagus sekali …kaitannya dengan tadi ..Hirarki tadi …waktu ada kepolisian Seibu ya …itu diminta untuk memaparkan kegiatan mereka kaitannya dengan kejahatan Pornografi …karena pimpinan nya setingkat dengan kapolres tidak bisa hadir …akhir nya yang ditunjuk Bintara …padahal disitu ada perwira ..karena yang mampu bintara …ct..c.t…ct …ya nggak ada malu – malunya …kalau dikita kan nggak bisa ..kapan kita ngungkapin nggak bisa …harus perwira …nah sekarang pertanyaannya ..perwiranya nggak mampu apakah dia layak …untuk tampil …menyampaikan sesuatu misalnya …atau memberikan sesuatu ilmu lah …atau dia mungkin mewakili dalam hal tertentu…kalau misalnya dia nggak mampu …itu yang jadi masalah …

M : sampe sini ….maksud nya apa tu …

R1 : nah sedang kan yang saya alami …saya ke Manila …(ha..ha. ha..) ya …saya sharing aja …yang saya alami ke Manila ..ya itu ..dia pintar ..Bintara …Bintara nya ngomong di depan …yang dia nggak pangkat …

M : saya kagum banget …karena ada sesuatu yang mungkin nggak pernah kebayang buat saya ya …ada di organisasi kaya Polisi …dengan apa namanya …melupakan ..walaupun itu cuma seadanya ..tapi ….*…..* oke ..nggak apa …nggak apa – apa …gelasnya nanti diambil …pasti ada yang narok disitu …nggak apa nanti akan dateng sendiri …nih kita lebih hebat dari pada Cyber ,….kita ngomong ini ..kita belum jelas …oke …oke…sampe

dimana tadi …ada jenjang hirarki yang dilupakan untuk sementara waktu …padahal mulai dari masuk polisi itu semuanya perintahnya itu hirarki ..

R : ya …(bareng) ….

M : kita bicara soal masalah perintah …system perintah …terus apa artinya lagi system perintah kalau memang tadi yang dibilang disini adalah

R1 : justru menghambat …

R3 : bukan …bukan ….menghambat …

R6 : kadang – kadang ….

M : ya ….

R : maksudnya ….

R6 : nggak selalu ya …kadang – kadang …tapi perintah itu juga penting …karena anak buah itu kalau nggak diperintah itu lelet …

R1 : hah…ha.ha.ya …

R3 : Cuma kita nggak boleh main perintah ….mohon petunjuk ..apa .. segala macam …

R6 : ya ..jadi harus bisa dipilah – pilah …

R3 : ya …harus bisa ditempatkan …

M : untuk yang…saya pertanyaan nya untuk yang lama disini ada dua orang …dari dulu memang seperti ini …apa namanya … mulai dari calon..di unit Cyber ini ….apakah seperti itu terjadi …

R6 : lambat …

R2 : bukan system manajemen nya …

M : system manajemen yang kayanya ….

R6 : dan memang perlu …dan dari awal …jadi memang perlu di unit Cyber itu dari leader nya sampe ke anak buahnya …ya harus se ide …sejalan …sepinter …ya itu …supaya unit Cyber ini maju …kalau leader nya nggak bisa apa – apa …sementara cuma anggotanya doang …itu juga nggak cukup …

R3 : nggak maksudnya gini …e…waktu dulu itu …

R : kepemimpinan dulu …

R6 : e…mati semua …

R9 : dulu kan nggak serame ini mas ….

R6 : dulu kan kaya hutan …

R9 : awalnya tiga orang …

Responden ngobrol bareng

R6 : sudah berbeda …sudah tidak …*..* kita bukan …kitakan juga bisa melihat seperti yang tadi diomongin …Cyber ini kan luas …yang ditangani kan juga spesific. ..jadi itu memerlukan seorang Leader yang mengetahui kasus yang seperti itu …tapi ..kalau saya mas ditanya …dulu tu seperti apa …seperti hutan tidak seperti ini …

R : kuburan….sepi banget …

R6 : kuburan …sepi yang ada dagang ini yuk …dagang ini yuk ….Pak Kanit datang ….

M : tapi dari dulu ada hirarkis nggak disana …maksudnya ...

R6 : oh….ada ….ada ….(bareng) ….

M : sama nggak hirarkis …atau kan kalau diliat sekarang ini kayanya

lebih pada saat pendidikan terus *....* itu terjadi dari dulu atau baru sekarang – sekarang ini ...ini sudah berapa lama ...ini dari awal gitu ...gemana ceritanya ...

R6 : kalau saya kalau saya mengalami ....lebih hebat yang sekarang – sekarang ini ...lebih apa ...lebih terbuka ....terus lebih terbuka ... lebih....lebih ...

R7 : lebih jelas terbukanya ...

M : lebih jelas terbukanya ...maksudnya ...

R6 : ini lho... ini kan acara tentang ...tentang kita bebas berbicara kan

M : hm...

R : bebas berbicara ....bebas mengeluarkan pendapat ....sekarang ini yang baru saya temukan ...dulunya nggak pernah ...

M : maksudnya sekarang itu dari kapan sampe kapan ...hari ini ... atau berapa bulan ,....

R6 : dari pimpinan saya yang baru ini ...mulai dari Pak Petrus ...jadi kita diberi kebebasan ....walaupun disaat beliau nggak ada ...cuma kumpul – kumpul gini ya ...yang hirarki itu tetep ada ....kita lapor ke beliau ...tapi kita tetep jalan ...kalau dulu sih saya nggak menemukan seperti ini ...mas ...diem ...nunggu perintah baru jalan .....

R7 : jadi mungkin kepemimpinan dulu itu beda. ...mungkin masa bodo bisa jadi ...

M : *.....*

R6 : ya ....

R7 : kalau memang leader nya itu juga masa bodo saya rasa anak buah nya juga ikut masa bodo...tergantung ..jadi berpengaruh ...kalau pemimpin kita baik ...ya akan baik ...istilah nya mengerti ...bidang tugasnya ...saya rasa anak buahnya ikut melaksanakan tugas nya dengan baik . ...

M : *.....*

R all : hah.a.a.h.a.

R6 : ya... akal adalah sebagian dari ini lah ...

M : sebagian dari kemudahan ...haha.h. kalau elo gemana ...

R9 : ya sebener nya itu awal – awal itu karena ....nggak sebanyak ... kasusnya nggak sebanyak ini ..ya ...dulu waktu pembentukan tiga orang itu ya ...kita masih terima surat – surat ....semacam kaya surat pengaduan ...jadi kita nggak sesibuk kaya sekarang ...kasus tu banyak ..dulu kita hanya sekedar back up ...cuma bales surat aja ...kalau ada diskusi – diskusi ...jadi karena kita terbatas tiga orang itu aja ..ya ...jadi kita sekedar ..

M : kaya kantor pos dong ....hah.a.aa

R9 : hah.a.a.ya. ...bales surat biasa aja ...jadi sekarang kaya banyak kasus jadi kita kerjakan rame – rame ...kita sharing ...kalau dulu ya ...cuma bales – bales surat aja ....gitu aja ...

R10 : sebetulnya kasus crime itu sangat luas sekali ...dari penipuan dan penggelapan ...sampe penganiayaan pun ...nah kalau dibuat pake komputer ...

R all : hah.a.ha.h.a

M : nah saya juga tertarik sama ini...ini kayanya ....ceritanya ini yang paling senior ..

R : bukan saya kalau senior ...mbak ini....(Intan)...

M : oke ...

R9 : boys ….
M : oke …boys ….
R6 : kalau untuk tugas dilapangan dia paling senior …
M : oke ..
R : tapi untuk di Bareskrim paling senior
R : paling tua …
R6 : ya…saya …
M : oke …nah saya tertarik pengalaman nya tadi…tadikan waktu perkenalannya e…sorry ….
R4 : mbak Intan
M : nah katanya Pak Budi ini gurunya dulu …
R6 : gurunya dia …
M : nah ini gemana …begitu masuk udah langsung ….
R4 : S.H.

Responden ngobrol bareng sambil haah.ah.a..

R10 : kebetulan ….kebetulan aja …lulus sekolah Perwira …saya ditempat kan di Pusdik Intel …padahal background saya reserse …nah karena di Pusdik Intel itu …orang reserse nya nggak ada …jadi ketika pelajaran ..e…Typologi kejahatan KUHAP..KUHP….terus proses pelajaran Pidana …itu diserahkan ke saya …
M : oke …
R10 : sebener nya bukan…karena e..apa ..senior itu nggak …bukan … cuma ….
R3 : berdasarkan berlatar belakang pendidikan …
R10 : latar belakang saya reserse pada waktu itu …
R3 : dan latar belakang pendidikan ..hukum ..
R10 : di Pusdik Intel ….
R4 : jadi..yang menjadi apa …dasar – dasar reserse .,…kebetulan yang diajar orang itu …*….*
M : topik yang mau saya ….ini…untuk yang …katakanlah …punya senior apa …lebih senior …gemana rasanya begitu ada dalam lingkup yang seperti ini ….ada junior ..atau ada apa namanya …katakanlah yang mungkin lebih baru …itu dia bisa bebas …berbicara …..
R10 : paling …ini..senior saya …beliau ini lebih senior daripada saya
R2 : senior pangkat …
R10 : dan siswa pada saat di Pusdik Intel itu senior semua …
R4 : sampe Kompol ..ada ya pangkat nya Mayor …
R3 : ya…kalau dibilang senior pangkat …ini kami bertiga paling senior sama mbak Fitri….ini 01 Januari mudah – mudahan kita Kompol…
M : pertanyaannya tadi …sebelumnya pernah terjadi nggak di unit kerja yang lain …atau masa dinas yang lain …
R3 : kalau saya sih …nggak …
M : belum pernah …
R3 : nggak …siapa pun yang bicara …saya tidak melihat pangkat nya sih …saya sudah berpikiran ya apa salahnya …orang yang lebih junior dari kita ..tapi dia punya kemampuan ….kenapa nggak …
R10 : mungkin Pak Alex melihat begini …Pak Alex tidak melihat siapa

yang berbicara …tapi apa yang dibicarakan …kalau siapa yang berbicara ..tukang becak …kalau tukang becak …artinya apa yang dibicarakan ..nah kalau yang dibicarakan tukang becak itu baik …

M : oke kalau yang junior ….ngomong kaya gitu …yang senior ngomong kaya gitu …tapikan tadi dibilang juga …nah pernah juga kadang – kadang …kalau senior …tetep harus hirarkis …maksudnya

R3 : ya ada beberapa senior …yang tetap pengen dianggap senior … itu ada …

R6 : itu watak kali ….

R3 : itu ada ….tapi …*…..* kalau kita tau orang nya seperti apa …ya menempatkan dirilah ..seperti yang dia inginkan …

M : oke …sekarang gini kalau …sekarang kita mau nyoba demokratis

R3 : tapi kan kita diteken dari atas harus kaya gitu …

M : rasanya …

R10 : ya …rasa – rasa nya ya dongkol ….walaupun kadang tugas yang diberikan kita kerjakan …

R3 : ya ….

R9 : nggak ngerti dongkol …

M : oke ….kira – kira orang nya seperti apa ..orang – orang kaya gini

R : hha.ah…h.a.a.

R8 : kebetulan disini nggak ada …

R1 : makanya sampe sekarang masih saya pikirin…haha.h..

R9 : disini nggak ada ….nggak ada …nggak ada …

M : oke ..ijin dulu sebentar mau keluar….

M keluar …all responden ngobrol bareng ….

R : disini nggak ada …

R10 : nggak nanti dikhawatirkan …kalau nanti masih begitu ..padahal yang lain juga begitu ..dan nanti *……..* maksudnya …akhirnya nanti jangan sampe ada junior sampe mengadakan 170 ha.ha.a.

R6 : orang *……*

R10 : nggak …masalahnya ..kita kadang …*….* kita harus ada yang open ,….yang open itu maksudnya …yang mengingat kan …tapi mengingat kan itu harus ada *…..*

R9 : supaya ada keseimbangan

R5 : kadang situasi – situasi begini bang …yang membuat kita agak segan mengungkapkan suatu masalah …untuk satu saran .,..ya .. dalam situasi – situasi begitu kan ,…

R : ah…susah kali kau….h.h..a.a.h..

M masuk kembali ….melanjutkan diskusi ….

M : oke …lanjut sebentar lagi ….ini saya tertarik tentang .,..masih …banyak sebenernya topiknya …tentang manajemen penyidikan …kalau ..kalau…sekarang gini kalau di unit – unit lain .boleh dibilang …dan unit lain juga punya penyidikan dan unit lain juga punya manajemen seperti apa sih yang dilakukan dan bagaimana caranya melakukan …di unit Cyber crime …misalnya kita udah punya perbandingan …apa sih yang menggerakan mungkin dari …dari Cyber sendiri aja …karena saya belum dapet gambaran ..tadikan sempet dijelaskan …tapi masih bingung ….dicoba dicatet …apa sih yang menggerakkan …maksudnya dari …menggerakan penyidikan si Cyber ini …

R3 : menggerakan penyidikan ….
R9 : laporan polisi …
M : laporan …oke…
R3 : kalau kita ini kan law in forceman ….menegakkan hukum ya .,..
kita nggak bergerak kalau tidak ada hukum yang dilanggar …
R2 : mungkin….mungkin maksudnya bisa di perjelas …
M : sebenernya proses ..proses penyidikan yang terjadi .dan bagai-
mana pengaturan ….
R : siklus …
M : o…siklus …ya …siklus nya …
R6 : ini mulai dari awal laporan polisi …
M : ya …
R6 : berarti itukan tehnik penyidikan …
……..
R3 : kalau untuk proses penyidikan sama aja Pak…
M : semua gambarnya sama …gambarnya tentang …
R : dari Laporan …(bareng) …
R2 : pengendalian …
R3 : di Bareskrim itu …di Bareskrim ada…ada. …ada. ..ada piket yang
menerima laporan …
R6 : satu pintu …
R3 : satu pintu …satu gate …
R6 : laporan polisi itu tidak langsung di jawab dulu …bisa laporan
polisi itu dibuat di unit – unit …tapi begitu pergantian pimpinan …
tidak boleh …
R3 : untuk pengawasan …
R6 : untuk pengawasan dan tidak ada orang yang meng …meng apa
ya …membisniskan laparan polisi …dibuatlah satu pintu …diterima di piket
siaga …nanti dilihat itu laporan polisi itu masalah yang dilaporkan itu …mau
dilempar ke direktorat mana …itu tergantung orang yang siaga …kalau dia
berbau IT …berarti ke Cyber Crime …kalau ke tipu gelap …ke Pidum
…kalau perbankan atau keuangan ke Perbankan …kalau korupsi ya ke
korupsi ..jadi kita yang di unit Cyber itu …
M : terima dari piket sebetulnya …
R6 : kecuali ada pelapor yang dateng ke kita…ini lho Pak …saya
dicemarkan nama baik saya …lewat email…by phone …lewat ini…oke kita
yang tangani…
M : siapa yang terima …disini di Cyber ,….
R6 : e..bukan,…boleh siapa aja ..boleh …
R4 : maksudnya begini mas …
R6 : harus ke piket siaga dulu untuk dibuat laporan …
M : kalau dari piket siaga ..itu akan turun kemana…di Cyber ini …
kesiapa …
R : ada staf nya …
R6 : itukan dari piket siaga ..dikirim ke Biro Analis …setelah itu…kalau
misalnya itu untuk unit Cyber itu nanti ke Wakaba …abis dari Wakaba
disposisi…disposisi lagi ke Bareskrim …dari Bareskrim disposisi ke
Direktur …Direktur disposisi unit mana yang pas menangani …sesuai pasal
yang dilaporkan ….

M : oke …pada saat begitu sampe ke unit …apasih yang dilakukan di unit …ini …

R : proses penyidikan …

R6 : proses polisinya …

M : bukan …

R6 : di…di…dilapor ke Kanit …

R2 : oke siapa yang menunjuk ….menunjuk …

R6 : ya…didalam disposisi pasti tertulis …AKBP ini…ni…ni….yang kanan ini …

M : yang menunjuk itu Kanit sendiri…..

R : ya ….

R6 : kan Ka unit …

M : ya ,…

R10 : jadi untuk pertanggung jawaban …untuk menyelesaikan kasus itu ..lapor ditengah jalan.,…e.pada saat menyelesaikan pekerjaan itu kita diskusi --

M : bagaimana jalannya

R1 : maksudnya kan yang disposisi kan kanit ..tapi kalau Kanit lagi diluar kota …atau keluar negri itu mendesak itu …bisa diwakilkan sama senior juga…

R6 : tapi laporan tetep ke Kanit …

R1 : tetep ….tetep lapor …nggak stak untuk jalan …

M : terus bagaimana dengan manajemen penyidikannya …

R3 : misalnya ada laporan masuk …e…biasanya kami akan menunjuk siapa – siapa yang barus menangani …jadi ditentukan penyidik nya …

M : oke…terus …

R3 : nah ditentukan penyidiknya …terus a…apa …penyidik ini tentu nya membuat rencana yang harus dilakukan …rencana – rencana yang akan …kapan dia harus dia harus memeriksa saksi …kapan kita harus meriksa orang yang melapor ….

M : oke……..

R1 : mas sebentar pinjem spidolnya saya gambarin aja …gambar nya mungkin begini pak …

R3 : tapikan ditentukan siapa – siapa yang nangani kan …

R1 : kita mulai dari dipangkas aja …dari LP sudah masuk ke Kanit..e …ke unit …ni unit …dari unit sudah masuk LP..apa tu Laporan Polisi …pengaduan masyarakat yang ke kita..dari sini ini di Unit ya …ini kan udah ada disposisi selain direktur …terus ditangani oleh Kanit …kan harus keluar disposisi …ditujukan kepada siapa …gitu …kepada Penyidik …disini siapa …siapa aja …siapa yang ditunjuk sesuai dengan e….kalau .tapi ini banyak pak ..bisa Alex..bisa saya …bisa semua …semua bergantian disana cukup satu orang …saya kepengen nya gini …kemudian dia membuat kelengkapan administrasi penyidikan …

R6 : meeting awal

R1 : ini namanya aktivis penyidikan …isinya mulai dari surat perintah .. nah pokoknya sedapat nya kelengkapan …surat – surat tugas ….e..ini penyidik …kita semua kan penyidik ..kita penyidik …karena saking banyaknya …e…jadi masing – masing bisa membuat …tapi semua surat – surat ini …itu tetap ditandatangan

M : siapa yang tanda tangan …
R : yang tanda tangan ya Kanit ..
M : harus Kanit ya…
R : ya …
R6 : sekarang direktur …
M : o…sekarang direktur
R3 : oh..ya …kecuali penangkapan …
R6 : surat panggilan …
R1 : surat panggilan ya …
R3 : surat panggilan …
R1 : nah baru selesai surat – surat lapangan sudah lengkap barulah mulai dengan proses….
M : prosesnya …
R1 : prosesnya itu dari di panggil ….udah mulai dengan pemeriksaan – pemeriksaan ….dan lain – lain …udah itu aja ….
M : dalam proses penyidikan tadi kan ada seperti tadi diceritain …ada perencanaan e…apa lagi sih …apa sih bagian – bagian …
R3 : dibagi lah …ini akan meriksa siapa itu udah jelas .….dari laporan polisi akan ketahuan …awal nya saksi yang bisa kita periksa ..periksa awal siapa aja …kan abis itu diuraikan siapa aja saksi nya kan …setelah itu langsung akan …ada pembagian tugas dong …misalnya pak Budi meriksa ini ..
M : maksud nya mungkin ada beberapa proses ..beberapa proses ,.. dalam manajemen terus ada pelaksanaan …ada pengawasan … terus apalagi …
R1 : ada penggalian …
M : ada penggalian …
R3 : pengendalian ….
M : sorry pengendalian ….
R : pengawasan lah …
M : perencanaan ….pengorganisasian …
R : pelaksanaan …
M : pelaksanaan …dan …pengawasan …
R1 : pelaksanaan dan pengendalian itu menurut John Terry …tahun 1990 kalau nggak salah …
R : halaman berapa ….
R1 : halaman 36 buku merah …
M : apa itu…
R1 : pengendalian mas …
M : o..itu bukan setara ..tapi beda …beda ….
R3 : sebener nya pengendalian bersama – sama kan …dalam tahap perencanaan ..pengawasan ..pengendalian itu sudah berjalan …
M : oke ..
R3 : stuffing ada juga sebenernya ..
M : berarti dalam manajemen penyidikan ini berlaku nggak sih ya …
R : ya .,.
M : ini berlaku disemua manajemen penyidikan atau …
R6 : seharusnya semua …
M : seharus nya semua …

R6 : seharusnya …
M : berarti ada yang berbeda …ada yang nggak seharus nya …
selama ini menurut pendapat temen – temen disini …ada beda nggak…yang terjadi dalam hal ini …
R6 : bisa saja ada …wong kita nggak tau koq…ini kerjanya bagaimana
M : oke….bekerja di minta…
R : lho tadikan saya cerita….saya dari sersan 2 itu …12 tahun kalau nggak salah di unit Pupar …itu amburadul dulu …disitu amburadul nggak ada begini ….sesuka hati …di Indap udah mulai agak baikan …bukan mulai agak baikan …tapi sudah baik kalau saya bilang …
M : tapi dari dulu tau ..
R6 : tau …kitakan diajarin …
M : oke yang lain gcmana ….ada nggak hal yang berbeda dalam ..
dalam manajemen …Perencanaan…Pengorganisasian …dan pelaksanaan …apa yang terjdai di unit Cyber …dan diunit yang lain …
R3 : kalau pengalaman di Intelejen malah ribet lagi ..dengan oprasional yang bekerja …
M : apa yang berbeda ..
R : lebih ribet lagi …
R10 : kalau di Intelejen itu e..kita tugasnya sebenernya mudah …tapi dalam rangka pelaksanaan …apa itu pertanggung jawaban dinasnya itu sulit …semua dibikin secara tertulis …siapa pun harus dilaporkan secara tertulis …
R3 : mulai dari tahap perencanaan itu sudah harus
R10 : meskipun tidak ada akibat hukum nya …tapi di reserse ini kan nanti harus ada manajemen yang bagus…karena nanti ada akibat hukumnya ..
M : oke …
R3 : akibat hukum itu karena kita menahan orang …kalau kita menangkap orang kita nggak ada upaya hukum nya …
M : dalam melakukan perencanaan nya …yang selama ini dialami … dilakukan …apa – apa aja yang menurut temen – temen disini … beda ..ada nggak …ada unit lain atau yang umum …yang biasa kerja ..
R3 : kalau perencanaan semua melakukan …
R2 : soalnya organisasi …yang pernah kitaalami sendiri …kita mesti melakukan perencanaan …namun perencanaan itu e…tentunya …kalau buta perencanaan di penyidikan …sebetulnya kan perencanaan itu harus ada .e….kita harus …umpamanya kita ditunjuk oleh Kanit ..untuk melakukan peyidikn satu perkara ..ditunjuk ada yang senior …jadi nanti senior melakukan seperti mas lakukan ..itu merencanakan …jadi memilah – milah kekuatan yang ada .,….memecahkan persoalan itu … terus kita membagi ..dibagi…siapa bertanggung jawab …melakukan apa …
M : oke …berarti dalam pelaksanaan yang ditonjolin adalah …e..yang menonjol itu adalah ..yang paling senior…….
R3 : ada …ada perwira Pam …Perwira pertama yang ditunjuk untuk …sebagai supervisor lah …
M : tapi tetep ada hirarkis nya …
R3 : Hirarkis tetap …dalam pelaksanaan tugas hirarki tetep mas…ber-

kaitan dengan tandatangan administrasi …

R1 : saya punya pendapat gini ..ini kan POAC inikan harus teori … teori itu diciptakan …memang berdasarkan proses – proses yang ilmu pegentahuan…tetapi menurut saya di Cyber itu sebener nya perencanaan dan organisasi itu dalam satu badan …bener – bener berarti dia yang merencanakan juga da juga yang mengorganisasi juga…

R3 : berkaitan dengan pengawasan ..

R1 : jadi nggak …ngak .bisa

R3 : ngak bisa berdiri sendiri

R1 : ya …nggak bisa berdiri sendiri secara utuh …jadi memang perencanaan di Kepolisian nggak mesti ngikutin teori – teori yang ada dibuku itu ..karena dalam prateknya dengan perencanaan itu udah satu jalan …kecuali perencanaan dan pelaksanaan ada perbedaan …kalau pelaksanaan itu udah mau kerjanya …tapi kalau perencanaan itu *…* itu aja

R2 : susah – susah dipilah ,…

M : susah dipilah ini terjadi diunit kerja temen – temen sekarang atau memang *…….*

R1 : susah karena ini memang satu konsep …kalau menurut saya perencanaan dan pelaksanaan satu konsep …prinsip nya hampir sama yang dikerjakan itu …azas perencanaan dak pelaksanaan itu ..

M : oke …tadi saya minta makananya dibawa kedalam aja …

R : boleh …boleh ….(bareng)

M : oke kalau buat temen – temen ya …selama ini ada nggak hal – hal diluar menurut temen – temen diluar apa yang kita bicarakan disini yang mempengaruhi sukses atau nggak sukses diri kira…

R3 : anggaran mas …

M : apapun yang bisa jadi kendala….

R : anggaran (bareng) .,…

R3 : cyber itu menggunakan peralatan yang tidak ada ditempat lain …

R6 : dan biaya nya juga jauh lebih besar

R3 : harus unlimited

R2 : untuk sementara ini sih kita masih fight ….

R 6 : ha.ha.h.a..masih fight…

M : apa itu artinya sekarang itu dana dan fasilitas itu sangat kurang .. untuk menunjang pekerjaan …

R3 : ya …gemana ya …selama ini ditanggung di unit …secara organisasi kepolisian belum …

M : gemana kiat – kiat temen – temen biar nggak ngeluh aja ….

R2 : gini mas …kita di kepolisian itu masih menganggap anggaran di teckel dulu …dilaksanakan dulu …baru anggaran …

R9 : karena kita nggak punya duit …

R3 : ya …karena kita nggak punya duit …

R6 : darimana ….*…* banyak orang yang malas …mau cari jalan pintas

R1 : hambatan – hambatan yang ada …ini tadi anggaran ..saya tambahin….jadikan saya kebetulan yang lain juga mungkin sama e…kita mencari kasus – kasus yang bisa diungkap …misalnya ada penipuan

hambatan yang saya alami ya ..pada saat saya udah masuk …terus saya minta informasi ke Bank…KTP nya palsu …

R3 : nggak kalau kita kaitin dengan ini ya ….dengan manajemen ya ..Men ..Money ..Material …Method ..ya …jelas pertama sumber daya manusia yang jelas …karena yang saya bilang tadi spesific…butuh …butuh ..jadi kita butuh pengetahuan hukum nya …butuh tehnis nya …tehnis komputernya ..

M : apa masalah nya …yang dihadapi dengan sumber daya manusia

R3 : kita orang baru …kita orang baru …ya kan..masuk ke Cyber Crime ini binatang baru nih …ini apa ni …

R6 :

R3 : ya…dengan latar belakang yang beda …

R2 : ada yang lalulintas …

R3 : ada yang laiulintas…ada yang personil …ada yang

R9 : dari empat mata….

R1 : intinya kan beda …ya kan sumber daya manusia pasti …

M : apa pengaruh nya ke penyidikan …

R3 : terhambat …nggak nyambung …

R7 : nggak nyambung …

M : *……..* kita punya ……

R1 : saya nggak sanggah….dan saya nggak *…* diri …latar belakang pendidikan …cuma saya ngasih gambaran gini ….tahun 2003 saya menjabat Kapolsek di Bandung ..buah batu …Kapolsek di Legok ya …saya menjabat Kapolsek saya nangani kasus Cyber crime …*…* saya sampaikan kasusnya ke pusat …kasusnya polis representative …selesai…itu saya buktikan saya mampu ..dengan latar belakang lalulintas ..memang saya pernah berapa kali menjabat reserse tapi nggak ada ini nya mbak …saya dulu pernah menjabat reserse tapi nggak ada ini nya …nggak ada sket nya …nggak diurus…terus saya pernah menjabat Kasat Intel …dua bulan …tapi juga nggak saya urus …akhir nya …pernah juga saya di titipin di POLDA …

R3 : ya …karena kita punya anggota ….

R : ya …

R3 : masalah nya disitu …

R7 : yang nyelesai in anggota kan …

R3 : ya ….lagian gini bos …secara umum sebener nya polisi itu sudah menerima seluruh pelatihan reserse..lalulintas dan fungsi – fungsi lain diterima pada saat pendidikan …tetapi pada saat di berdinas …pasti ada satu focus dia ..ada satu focus dia …kaya Arief temen saya focus nya Intelejen …sekarang memang dia intelejen aja …Ketut oke dia lalulintas dasar nya …tapi dia kan pernah melaksanakan fungsi reserse ….apa lagi pada saat di Kapolsek …dia melaksanakan seluruh fungsi …otomatis dia harus belajar disitu …

R9 : nggak jadi ….

R3 : nggak …Kapolsek …

R1 : Kapolsek….

R3 : Kapolsek berarti kapolri diwilayah polsek …..

R6 : ya ….number one …

R3 : manager dia disitu kan …

R4 : makanya kadang – kadang dia disuruh kumpul …

R : briefing ....
R all : hhah.a.ha.h.a.becanda ....
M : kita sambil makan ya ....
R : boleh....
M : kita ambil dulu deh makanan nya ....
R2 : intinya kita dulu ...intinya kita dulu jadi anggota ...kita dulu bodoh ..kita dulu bodoh – bodoh ....
R3 : cemen
R all : h.ha.ha.h..ha..
Responden mulai makan .....
M : sambil ini aja ...nanti kalau ditanya sambil makan nggak apa – apa kan ....
R : nggak ...
R1 : jadi gini mas ....saya punya cerita yang paling beragam dalam hidup saya ...dan saya udah sampaikan ke mertua dan istri saya
R all : ha..ha.h.a.ha..a.
R1 : dua hari yang lalu saya baru cerita sama istri saya ...masalah ini ...ya istri saya bilang o..gitu ceritanya ...
R3 : maksudnya ceritanya cerita apa ....
R1 : pada saat saya lulus ...lulus ya ...ada penjurusan mau milih lalulintas ..Reserse ...Intel ...Brimob atau ...Sabara ya ....
R3 : nggak ada cuma tiga fungsi tambah satu brimob ...
R1 : Brimob ya ...hadapi pilihan itu ...terus waktu itu saya pacaran sama istri ....mertua saya bilang gini ..Bud kamu masuk lalu lintas ya ...soalnya lalulintas itu jam kerjanya jelas
R2 : jadi yang arahkan lalulintas itu mertua ...
R1 : ya...ya...bu ya ...
R2 : o..mertua perempuan
R all : ha..ha.h..a.h..
R1 : mungkin juga sih ...tapi bapak nya serse koq...bapak nya intel ... terus saya pilih lalulintas. ..setelah saya pilih lalulintas ...
R3 : Bud..mertua polisi Bud...
R1 : setelah saya masuk lalulintas kejuruan ...koq...bisa – bisanya saya polantas nangkep perampok ...waktu itu saya nangkep perampok ...yang nggak kapok ....saya nangkep ini perampokan ...cat ...container besar itu ...ketangkep situ ..sampe senjata juga jatuh ...akhir nya kebongkar ...terus saya pindah lagi jadi Kasat lantas ...Purwakarta ,....di Purwakarta. ..
R2 : berarti reward nya itu ...nangkep penjahat.,..
R1 : ya ..itu lah diantara ....pindah kesitu saya juga nangkep perampok bank ...dulu ada perampokan ...
M : nggak sengaja juga ...
R1 : ya ...good luck nya pas aja ...lucky ...terus ada pencurian mobil juga dapet ...hockey terus ...terus saya mikir – mikir nih ...dan saya Kasat lantas Purwakarta ...justru banyak complain ...pimpinan banyak complain karena kan masalah nya duit ...pimpinan kan taunya duit ...duit ...duit....karena saya nggak bisa mengakomodir ...akhirnya saya ke polsek minta ...minta berhenti ...karena pimpinan taunya duit ...mintanya duit ...lama – lama kan kita jadi kaya pelayan ..setor ...salah sebetulnya ..akhir

nya konflik …saya ke polda …pas pindah itu …terus saya memulai hidup baru ..baru ..jadi Kapolsek deh ceritanya …

R2 : Kapolsek …Kapolsek Legong lagi …

R3 : nggak hidup baru jadi Kapolsek …

R1 : ya …saya hidup baru jadi Kapolsek …

R2 : Kapolsek itu enaknya sedikit …tapi *…* enak sekali karena punya apa …pertama punya wilayah …yang kedua dia punya … pekarangan itu yang paling enak

…

R : enaknya apa …

R2 : ya ..kalau ..bisa tahan dulu…bisa dijual tanahnya …hah..a. ah.tahan dulu biar jelas …hah.a.ha..

M : oke …

R2 : saya dulu masuk intel juga nggak mau …

R1 : belum selesai ya ceritanya ….intinya kalau saya udah pulang ke markas saya ke markas itu supaya aman …supaya nggak bentrok dengan penjahat …hidup tenang …duit ada ..cukup …tau – taunya ketembak di leher ..23 jaitan …Provost saya di Bandung …saya telp ke Jordan ..gue ketembak elo dateng kerumah sakit …dia yang tanda tangan mewakili orang tua ..ya resiko nya diri saya …dia satu angkatan …justru saya disitu ada hikmah nya buat saya …temyata walaupun kita lalulintas kalau kita emang ini …justru temen saya Erwin Kurniawan …dia Kasat Intel ..yang dilapangan yang memang nembak – nembak juga dia malah nggak kena tembak …justru saya yang kena …dan memang semua pekerjaan ada resiko nya …

M : yang lain …

R2 : pokoknya …berhasil tidak dipuji ….salah dicaci maki …hilang nggak dicari…mati tidak diakui …

R4 : siapa tu ..hah.ah.ah.a.

R2 : tinggal tambah satu lagi…rejeki tidak dibagi – bagi..h.a.ha.h.a.

M : selama ini pernah nggak sih ada kasus ….oh ya …aku kayanya lebih enak begini …nanti juga pasti makan …kalau kaya gini kan enak bisa sambil nanya – nanya ….pernah nggak sih ada paling mengesankan ..buat temen – temen … setiap orang mungkin punya pengalaman dan penugasan yang beda – beda ..

R : di daerah apa di Cyber …

M : di Cyber …

R : o..di Cyber ….

R10 : pertama ya nangkep orang di Probolinggo itu …aku udah berangkat di caci maki …hah.a.a..

R1 : udah ada pesanan nih…sempet gue nggak dapet ..ketawa aja …

R6 : kasus *…* apa kasus Cyber …

R : cyber …(bareng)

R6 : o…ya..ya…..

R10 : pengalaman pertama kita itu …pas pulang nggak ada hasilnya gue pulang ketawa aja …

R3 : itu tantangan sih itu …kita berangkat itu mas …kita berangkat itu mas …kita berapa orang ya …

R10 : Pak Alex ..saya ..

R3 : berempat ya ….berempat adalah senior yang ngomong …belum

jelas juga udah mau berangkat …terus ngomong nya …sempet nggak ke tangkep …gue ketawa aja …waduh ini koq kaya gini …bukannya ngasih motivasi …ya tapi ya ..kita berangkat aja …

M : memang kalau misalnya dalam penugasan …penting ya motivasi dari senior…

R : ya ..perlu (bareng) ….

M : apa yang biasanya dilakukan oleh senior …

R10 : kalau perlu dukungan dan logistik nya …dan pemikiran itu yang lebih penting…jangan sampe Junior mau berangkat ke Jepara dua orang ongkosnya seratus ribu …

M : berarti ada hal kaya gitu …

R : tetep ada ….

R6 : tetapi kalau *…* nggak ada yang loyalitas gitu kan jalan – jalan aja dia …

R1 : dari kantor sebenernya anggaran ada untuk itu kan ..cuma *….* nanti kalau ada kesulitan telp ya …tapi ada …sebetulnya nggak terlalu ini juga …cuma kadang – kadang yang diluar ..diluar …apa …situasi kan nggak mungkin mulus …kalau situasi nya nggak pas …

M : biasanya apasih yang terjadi misalnya kalau tadikan udah dikata-kan kasus ya …senior nya itu bukan memberi motivasi …e…

R : kadang menghambat….

M : kadang menghambat …sebetul nya itu menghambat atau nggak .

R3 : ya menghambat…

R10 : kalau kita waktu itu nggak memaksakan diri …

R2 : kita nih karena …artinya bukan…bukan motivasi yang kita dapet *……*

R3 : awal kita belum jelas….*……..* dia udah ngerti *……..* diakui belum jelas *…..* kan nggak dapet…..*..* membuat kita bisa

R2 : kan penyelidikan kita ini …penyelidikan di by tehnologi dulu :..tapi kita matang kan di lapangan by konvensional …harus kita dateng kesana …kita tidak bisa menangkap orang dan memastikan alamat itu kalau kita tidak dateng ke situ …jadi kita dateng kesitu untuk mengatakan bahwa informasi yang kita dapet dari tehnologi itu …nyata gitu …dilapangan ….itu yang kita nyatakan ..dan ada ..kemudian kita tangkep …

M : jadi tadi kan sempet ngomong nih …memaksakan diri …maksud nya memaksakan diri itu apa …artinya si atasan itu nggak ngasih restu tapi tetep jalan …

R2 : sebenernya bukan atasan ya …tapi senior …kalau atasan kan… kalau kita ..kalau atasan itu tidak memberikan surat jalan ..kita nggak bisa jalan …kita nggak diperintahkan tugas …kita nggak tugas ….tapi itukan bukan….bukan …bukan …bukan Manager …sehingga kita berani melawan …

M : soalnya kaya gini ni …senior bisa bilang …koq belum jelas udah jalan …artinya sebetulnya kita juga nggak ada perintah sampe kita harus jalan …ceritanya itu ….itu wajib jalan atau ….

R3 : gini mas….artinya administrasi pendidikan reserse itu ada …*….* orang – orang itu ditunjuk …penyidik – penyidik …penyidik inilah yang menentukan apa yang harus dilakukan …pangkat *…* apa …setelah ini saya harus melakukan apa …tapi tidak terlepas kita melapor…kita laporan ke

pimpinan …sebagai bentuk pertanggung jawaban dan kegiatan yang kita laksanakan dan sekaligus …menyampaikan sejauh mana yang kita laksanakan …dan rencana kita selanjut nya apa …kan gitu kan …nah kalau dibilang …e…perintah pergi atau nggak itu tergantung penyidik nya dong ..penyidiknya kalau berkesimpulan …oke ..kita udah bisa sentuh sasaran …atau kita udah bisa tangkep …ya kita nangkap …tapi bersarakan pertimbangan – pertimbangan itu ..dan berdasarkan diskusi – diskusi ….ya kan …ya tapikan …namanya kita baru ya …kita baru …dan kita menganggap senior ini lebih tau dari kita ….kita tidak …tahun 2006

M : tahun 2006

R2 : itu pengalaman kita …pengalaman – pengalaman kita …..
pengalaman baru dalam rangka pengungkapan kasus di Cyber Crime …itu yang …sehingga kita tidak bisa lepas dari ingatan ….

M : oke …itu kasus apa …

R : tau nya kerugian kecil sekali …14 juta …14 juta kecil sekali bagi Mabes Polri …dulu sempet diejek juga sama Jaksa Tinggi ya …Jaksa Tinggi ya …karena kasus begini di tangani Mabes Polri …tapi dia tidak melihat bahwa kasus ini …sama pelapor ini sudah dilaporkan ke Polwiltabes Bandung …Polwiltabes Bandung tidak menanggapi kan ..dilaporkan ke Polda Jabar…sama juga karena nggak bisa menangani …terus lapor ke Mabes Polri ..apa kita tolak …kan nggak …kita juga tidak melihat kerugian nya kan …kita itu bahwa itu …

R3 : itu merupakan pelanggaran kan …

R1 : orang Jawa bilang gini …Koramil nya bilang gini …hanya orang Mabes aja yang bisa nangani ini …karena kalau Mabes nggak bisa siapa lagi …

R3 : ya …dia mulai dari bawah ya …dia melapor di Poliwiltabes …
Polda Jabar …Polda Metro pun lapor dia ..sepanjang itu nggak jalan dia lapor ke Mabes …dimana – mana Polda nggak bisa …ya ..lapor ke Mabes …nggak mungkin Mabes diem aja …

R1 : kalau Mabes nggak bisa …ya lapor keluar aja …

M : dimana kasusnya …

R : e….masyarakat itu ..

R2 : kan kita kasus harus dilaporkan dulu ..ada kasus …harus ada korban …nah korban ini melapor ke

M : koq kesannya *…….*

R2 : ya ..karena pelakunya ada *….* ..nah korban nya ada di Bandung …dan di Jakarta ..masing – masing korban itu sudah melapor ke organisasi polisi yang kecil …tapi nggak ditanggapi …karena ya mungkin kerugiannya dan caranya juga masih aneh bagi mereka…sehingga lapor ke kita …dengan tanggapan kita yang baru …pengetahuan kita yang baru menjadi tantangan kita …untuk mengungkap …akhir nya menjadi tantangan kita kan …namun ditengah jalannya …ada sedikit hambatan ya itu tadi ….

M : sebener nya kalau kejahatan yang ditangani e…Cyber ini ada berapa jenis sih …kalau kita ngomongin pengelompokkan …

R3 : kalau teorinya Cyber Crime …ada …ada …ada Computer Crime ..ada komputer yang *…* crime ..Computer Crime nya itu …yang memang memanfaatkan kelemahan system atau program atau …komputer itu sendiri …memanfaatkan …Hacking …ya kan …Tracking …itu kejahatan

komputer…tapi ada juga kejahatan yang berkaitan dengan komputer …menggunakan komputer …menggunakan fasilitas komputer …misalnya dia menyebarkan fitnah …melalui komputer …itu sebenernya kejahatan biasa tapi berkaitan dengan komputer …ya kan …jadi sebener nya luas ….di Cyber itu ..

M : Hacking itu berarti masuk ke bagian …
R : yang computer Crime
R4 : ya lebih luasnya seperti tadi …
R : masih lama toh …
M : nggak kira – kira 20 menit lagi ….
M : kalau misalnya tadi….kalau menangani Hacking …yang itu bisa dibilang …
R6 : dia penipuan …
R3 : penipuan …
R6 : penipuan dengan penawaran barang ya …
R3 : penawaran barang melalui komputer ….
R6 : penawaran barang tapi melalui internet ….ditawarkan di internet .. barang itu ditawarkan tapi dia menipu ..

M : kalau hacking …pernah nggak nangani …
R3 : Hacking ya deface …
R5 : pengrusakan …
M : oke ..untuk menangani kasus yang seperti itu …ada hal yang berbeda nggak sih …dari …kita ngomongin masalah manajemen ..masalah e…ada yang berbeda nggak disini …
R3 : sebenernya dari penanganan awal …menerima itu udah berbeda karena kan memang laporan itu harus lewat siaga …tapi pada saat itu kita langsung tangani karena pemikiran waktu itu pak Kanit menyampaikan yang tau tehnis nya …unit kita…jadi kita aja yang langsung buat laporan polisinya ..berpikir kalau yang siaga ..dia bingung mau diarahkan kemana …akhirnya kita langsung …
M : hm….langsung tau ..tau hal itu darimana …
R : ada korban melapor …
R3 ; lapor …
R6 : ini boleh Pak…jadi pelapor itu tidak usah ke siaga ..ke unit juga boleh ..asal kasus yang dia laporkan itu ada kaitannya dengan unit . …itu boleh kita tampung …kita buat LP nya sendiri …nanti kita …
R3 : kita bawa ke siaga …
R6 : ini lho …tapi begitu misalnya pas yang dilaporkan yang nanti kita kerjakan …semuanya oke …nggak akan dikasih ke Pidum. ..nggak akan dikasih ke …karena yang ada itu hanya unit Cyber Crime yang bisa nangani itu …
R1 : ya sampai situ nggak ada masalah …
R5 : tidak tergantung masalah ini …semua kasus bisa kita hadapi…
R6 : nggak bisa bang….
R5 : yang ada ..dia punya via ini …atas namanya …
R6 : tipu gelap nggak boleh kekita …nggak akan masuk kekita… kecuali kita yang kasak kusuk unit Cyber …nanti tu dicegat di analis ..dicegat di …di Satgas yang diatas …atau dicegat di ….

R5 : penipuan – penipuan ….
R4 : penipuan bisa masuk ….
R6 : itu dengan sarana internet boleh ….
R : karena masih bisa ke …
R6 : karena itu masuk nya ke Pidum …nggak akan jatuh ke kita …
R5 : walaupun dia punya kemampuan menggunakan ….
R6 : nggak usah jauh – jauh timpidum itu diprotes abis – abisan …
R4 : kalau Timpidum emang nggak ada hubungannya
R6 : ya itu …tapi kenapa bisa masuk …itu makanya rame…itu kan dia marah – marah di kita …
M : berarti sebetulnya ini sangat mungkin terjadi …apa namanya … dua lisme penyidikan …kalau dibilang tadi …kan ada ..tadi masalah kejahatan yang dengan media komputer…artinya kejahatan itu sama juga ditindak pidana in …
R3 : kejahatan terhadap computer letter crime …crime ..tindak pidana umum …cuma ada..ada peralatan komputer nya …
R10 : sejauh kejahatan itu e..melibatkan
R6 : IT ya …
R10 : IT dan
R1 : sebetulnya gini kita penyidik ya …kita bekerja e..sudah ada pos …kan sudah ada *….* nya… diluar daripada itu kan pimpinan yang ngasih perintah…contoh …kasus masalah optik …optik kan lebih cenderung nya mungkin Cyber atau industri dalam perdagangan …unit khusus yang menangani masalah optik ..VCD …tapi kalau dengan berita itu tidak ada masalah semua itu dialihkan ditangani direktorat 5
M : 5 itu apa …
R1 : *……..* maksudnya yang langsung bagian saya menangani kasus itu ..tapi karena pimpinan ..dipindahkan oleh polisi pimpinan..bisa berubah ke unit lain yang nanganin …direktorat lain yang nanganin ….
R6 : itu yang tadi itu pokoke…itu …pokoke saya yang kasih perintah .. yang punya kuasa …Pieter yang tanganin…ya Pieter yang akan nyambut
R1 : yang jadi masalah kan gini …yang jadi masalah dulu Pieter nggak mau …pada saat *…….* kan anggotanya nggak punya kemampuan …nggak punya pengetahuan yang banyak kan itu …akhirnya kan jadi stak nya disitu ..contohnya gini …yang kita sekarang *…..* judi internet kan yang menangani kan memang Cyber Crime tapi juga ada dari analis Cyber Crime ..unit Cyber crime bukan …
R3 : analis …
R1 ; yang kemarin nongkrong – nongkrong itu …
R3 : Direktorat 1 nangkap judi – judi internet ….tapi cuma semalam dilepas …karena dia bingung …dia nggak tau bukti dari mana …
R1 : pembuktian nya mana …tapi dia membuktikan nya susah …rugi dong …
R6 : rugi dia ….
M : kalau misalnya ….saya perlu mencatat sedikit….dalam proses penyidikan atau pekerjaan terkait dengan apa aja sih sebener nya baik orang maupun badan …dengan siapa aja …
R6 : unit 2
M : internal atau external …

R6 : unit 5 maksudnya …
M : ya…unit 5
R1 : o..unit 5
R3 : kaitannya dengan apa aja gitu …
M : ya ….teribat kerja gitu …
R : ACI
M : apa
R : Assosiasi ….
R : APJI…
M : APJI…apa tu …
R : Assosiasi Pengelola Jasa Internet ….
M : (menulis) …oke …seratus ….terus …
R : AKKI…
M : AKKI…
R : Asosiasi Kartu Kredit Indonesia …
R : doble K
M : ini terus apalagi ….
R : Provider …
M : Provider …
R : tiga ratus …ha.ha.h.a.
R : Bank juga …
R : ya …Bank …
R : ahli IT ….
R : kementrian …departemen
R : ya ..komiko…
M : ahli IT …ahli Hukum …
R : Hacker …
M : terus apalagi…
R : kepolisian – kepolisian asing …Interpol ..FBI…
R : Interpol…Microsoft …
M : apalagi…
R : ICTAP

Responden ngobrol bareng

YANG TERKAIT

- A P J I Asosiasi Pengelola Jasa Internet
- AKKI Asosiasi Kartu kredit Indonesia
- Provider
- Bank
- Komiko ?
- Ahli IT
- Ahli Hukum
- Microsoft
- ICTAP
- Hacker

M : oke …kalau ini kan semua yang terlibat …apa namanya ..mereka nih bisa nggak sih kita kelompok – kelompok kan …
R : maksudnya ….
M : berdasarkan pentingnya buat kita…atau hubungannya dengan

kita…dengan unit 5

R : Jaksa ..Hakim kan berhubungan dengan kita. ..JJS disitu …kalau sampe terlibat jauh …

M : kalau kita…kalau kita …kelompokkan mereka berdasarkan penting nya hubungan dengan kita gemana

R : boleh di kelompokan …

R6 : maksud nya ahli IT ahli Hukum jadi satu …

R3 : profesi nya …

M : kalau kita mengelompokkan mereka berdasarkan penting nya buat kita …bisa nggak …

R3 : penting semua …walaupun dalam satu kasus penyidikan tidak semua kita libatkan …tergantung kasusnya …tergantung kasusnya ..

R6 : yang kita tangani selama ini semua nya udah kita …

R3 : nggak maksudnya tidak semua nya bersamaan dalam satu kasus ..yang jelas kaya misalnya Interpol …

R2 : Interpol itu kan bisa di bagi …

M : ada nggak yang membedakan mereka ….

R4 : ya mungkin ada bedanya kan …seperti mas tadi ngomong – ngomong dengan saya masalah rokok …kita rokok – rokok kan …ini rokok Samsu …ya ..rokok ini cocoknya siapa yang isap….perempuan apa laki – laki …yang suka Samsu …

R2 : yang suka menthol gemana….

M : ya ..ya… …

R : yang pasti perempuan …

M : yang pasti bisa membedakan …

R4 : bisa …

M : oke …seperti apa kelompok nya …

R4 : kalau yang Hacker ini nggak boleh dikelompokkan maksudnya kelompok yang apa …*…:…..* tugas di Cyber Crime karena dia juga kadang – kadang lapor kejahatan ..ini ..

M : yang ini ya …

R3 : itu kan resourching jatuhnya …

M : ada lagi….jadi selain ini …semuanya masih bisa dikatakan satu kelompok lah …

R3 : Interpol sebenernya nggak ini juga. ..nggak terlalu intens sih …

……

R4 : soalnya saya dulu pernah ini mas …waktu di Curug …pernah nangkep di Cyber Crime …karena temen juga …hacker juga. .itu pelakunya ..saya ngambilnya langsung di kantor Pos …terus nyerahin di…saya punya senior di Polda Jawa…bahwa ini pelaku kejahatan internet…dan betul memang barang bukti nya sudah diambil dari kantor Pos …

R2 : tapi bukan ikan …

R4 : udah satu mobil barang bukti nya …udah satu mobil …yang dikeluarkan dari kantor pos …bukan …dia ngeluarin Laptop ..terus *…* itu nangkap …bukan karena saya telusuri dari komputer …kebetulan temen aja yang jadi pelaku ….

R : temennya ….temen

R4 : karena bersaing …saingan ….

R : makanya jangan di kelompokin …diadu domba …aja …

M : oke …ini yang terakhir ….
R : yang terakhir …
R : tadi yang terakhir ….hah.a.h.a
R1 : nggak ..tadi saya tu …saya kurang pas …pertanyaan nya mungkin gampang …bukan dikelompok kan …tapi orang – orang ini …point – point ini …korelasi nya apa …korelasi ke kita sebagai apa ….kalau dibalikin lagi …itunya ..berbeda bukan dikelompokkan …tapi mereka ini relevansi nya dengan kita dibidang apa nya …boleh…(menulis didepan)…..
R1 : kalau ini kan …ini AKKI….Asosiasi Kartu Kredit Indonesia …kalau sesuatu yang berhubungan dengan kartu kredit …kita korelasi dengan dia …nggak bisa kita korelasi dengan ICTAP…ini nggak bisa ..kan bidang nya lain …nggak ada hubungan ….kalau kita berhubungan dengan email …makanya tadi ……
R5 : mungkin apa sih namanya …kita berhubungan sama mereka tergantung dari permasalahannya …
R3 : kasus ya.,..tergantung kasus ….
R5 : kalau kita langsung pencarian nya di ….permasalahan penipuan – penipuan …yang berhubungan dengan nomer rekening ya …jelas kita berhubungan dengan Bank …ngapain kita pergi …dengan orang dipelosok …hah.a.a.ha..ha
M : ini berpengaruh nggak sih ….apa nama nya …mereka ini terhadap manajemen penyidikan …
R : ya ,…dia sumber informasi ….
R2 : perencanaan juga kan …kita membutuhkan …
R7 : kita saling membutuhkan …
R3 : pada saat perencanaan kita sudah ….*…*
M : tadi ada …soalnya tadi ada selentingan ada yang membutuhkan informasi atau dari segi *….* nggak ada …misalnya Interpol itu … tadi sebetulnya masalah dana
R2 : nggak ..masalah nya nggak intens …nggak intens ,….kalau Interpol dalam rangka kita menangkap kasus yang ditangani kebetulan tersangkanya ada di Indonesia ….ngapain kita butuh Interpol …
R1 : jadi mungkin gini pertanyaan nya kapan kita membutuhkan jasa Interpol ….kalau ada pelaku kejahatan yang diluar negeri …kita korelasi sama interpol …tapi melalui surat menyurat …
M : ya ..ya ….fungsinya itu terkait dengan apa yang ada di .,..apa … kasus yang dunia Cyber ….
R : ya….
M : oke ….
M : yang terakhir …ini ….kalau misalnya saya punya kuasa …. katakanlah pemimpin …atau bukan …bukan pemimpin …tapi bukan seorang pemimpin …yang akan mengembangkan unit 5 ini menjadi lebih baik ….lebih baiknya itu menurut temen – temen …orang yang seperti apa sih yang harus saya ambil…
R6 : pintar …kaya …
R : ha.h.h.h.a.h.
M : oke ..pintar …kaya …

R6 : pintar …kaya …karena kembali tadi ke dana kan…karena dari badan reserse sendiri itu nggak turun …jadi pimpinan saya yang
R3 : tadi pinter dalam rangka …
R4 : cerdas…cerdas …
R6 : smart ….
R3 : bukan ….mengetahui bidang tugas nya ….
R6 : ya …bidang tugasnya …
Responden ngobrol bareng
M : pintar …kaya …smart ya …(tulis di depan)
R : ya ..
R1 : jago English …
M : jago inggris …
R1 : bijak …
R : cakep….ganteng
R6 : parlente ..
M : parlente
R : ya ..yang bergaya gitu …ya itu komandan saya …ha..ha.ha..
R1 : mbak Indri …mbak Indri …
M : ada lagi …
R : udah semua …
R : Pak Petrus ….smart ya …
M : masa….
R : semua itu terpenuhi …
M : apalagi …
R1 : nggak…yang jelas punya kemampuan inilah …masalah internet
R3 : ya …
R6 : ya pinter udah termasuk …
R : bijaksana …
R : termasuk Arif ….ha.ah.a.ha..a
R2 : kan judul nya Arief …haha..ha
M : ini pintar …apa istimewanya pintar ….
R : ya ..pintar .,.menguasai …
R6 : berarti dia harus pintar
R10 : pinter mengembangkan juga disitu ….
R6 : pintar untuk ….
M : yang dimaksud dengan pintar apa sih …
R4 : ini cerdas mungkin …
R2 : nggak…pintar itu bisa ..
M : ya ..ya ..orang bisa macam – macam …
R6 : pintar itu ada ..pintar matematika …pintar Bahasa Indonesia ..pintar menyanyi ….belum tentu dia pintar menyanyi …kalau dia pimpinan Cyber Crime berarti dia harus …pintar …pintar menguasai unit Cyber ini …
M : jadi maksudnya pintar disini menguasai bidang Cyber ini
R6 : ya dong …itu kalau menurut saya ….
……..
R2 : menjadi apa yang dipimpin nya itu bisa maju ….kalau dia harus mengetahui permasalahan itu …*……..*
all ngobrol bareng
M : nggak …saya lupa konfirmasi dengan yang lain ….seperti tadi ….

kalau saya pengen mengangkat seorang KANIT lah disini …. selain sifat – sifat ini masih ada lagi nggak ..yang harus ada …

R2 : mengerti anak buahnya …

R3 : jadi ada yang spesific di Cyber mas….orang – orang di Cyber ni …orang – orang yang gemana ya …aneh – aneh ….hah.ah.a

M : maksudnya ..

R3 : maksudnya orang – orangnya suka nentang …ada yang .. pokoknya aneh – aneh lah …nggak ini …

R6 : saya rasa …

R3 : pimpinan nya harus bisa itu …bisa..

R1 : membuktikan keanehannya ..h.ah.ah.a..a.

R3 : menggabungkan itu …

R : sumber daya .,..

R3 : nah ya itu …

R6 : itu menjadi kekuatan …

R1 : pengetahuan sifat …karena perbedaannya suku

R2 : mengetahui kelemahan dari watak…

R : karakter masing – masing ….

R6 : kan kita punya bagian …..ada yang diem kaya kue lindri …

R3 : kan beda – beda

R6 : ada yang cerewet ..kaya saya …

R3 : pimpinannya harus bisa memanfaat kan

M : ada lagi selain yang telah kita sebutkan disini ….

R7 : yang ngerti anak buah dong …

R6 : ya. .mengerti anak buah itu kan udah luas artinya …ih…

R2 : maksudnya kepribadian anak buah itu gemana ….

R9 : bukannya terbalik …pengertian anak buah gitu ….

Responden ngobrol bareng

R7 : menerima usul dan saran anak buah …itu namanya apa gitu ..

R1 : kepemimpinan …jadi mengerti anak buah …terus ..ini …

R : semuanya ….

R ; ya itu lah …kebijaksanaan ….

R10 : tanggap tangkas ….mengerti

M : tanggap…apa sih ….

R : tanggap …kalau anak buah susah…ngerti ….

R : ada anak buah macem – macem tau ….hah.ah.a.ha.

M : ini mengerti dan tanggap terhadap anak buah ya …

R : ya …(bareng)

R10 : bukan tanggap aja ….tanggap luas …tanggap pekerjaan …

R8 : tanggap kelakuan …

R1 : ada lagi mas …Responsible …Responsibelity ….pertanggung jawaban ….ada juga pimpinan yang nggak mau tanggung jawab

Responden ngobrol bareng

R6 : karena kalau ada bapak buah itu ada yang agak *..*…kalau begitu bapak buahnya campak in …..

R3 : yang bertanggung jawablah …

M : oke …oke. ..ini semua sifat – sifat udah kita ..kita dapatkan …ada pintar …kaya ….smart ….jago inggris …parlente ….mengerti anak buah …

R : kira – kira siapa lah …

R6 : parlente itu artinya ini ya …*…..* pake ini baju bagus ….jadi saya seneng gitu lho. …

R2 : kalau kaya gini rasa nya nyaman …ha.aha.ha..

M : ini semua sifat – sifat nya …dari semua sifat – sifat ini ….yang mana yang paling penting …dan paling banget harus ada ….yang khusus untuk Cyber crime …

R : bertanggung jawab (bareng)….

R6 : saya setuju …

M : bertanggung jawab …maksudnya bertanggung jawab ..itu …

R : cakep …dan dapat dipercaya perkataan dan perbuatanya …ha. hah.a

R : tanggap ya …

M : bertanggung jawab disini …apa yang spesific ….dari Cyber yang *….* bertanggung jawab …

R1 : tanggung jawab terhadap pekerjaan ….terhadap tugas

R6 : terhadap kesejahteraan …

M : nah itu saya nggak enak hha.ha.h.a.h

R : kalau disini yang ada Arief nya pak ..bijaksana nya nggak ada …

All ngobrol bareng

M : kesejahteraan …apa lagi …

……..

M : artinya kalau pun ..kasarnya ni nggak ada orang yang cocok … paling nggak kalaupun dia nggak pintar …nggak kaya ….nggak smart ..nggak jago inggris nggak parlente

R2 : jangan jadi KANIT unit 5 …

R all : hahaha.h..a.ha.h..ha.

M : tapi gue responsible dengan ini ..pekerjaan

R3 : kalau responsible menuntut itu …responsible …bagaimana orang akan bertanggung jawab terhadap tugas kalu dia nggak pintar … susah mas …

R6 : banyak anggota di Bareskrim ..bapak – bapak nya bertanggung jawab …banyak ya …

R3 : nggak maksudnya …bagaimana dia mempertanggung jawabkan tugasnya kalau dia tidak mengerti tugas nya …ya kan …jadi intinya disitu ….

M : jadi sebetulnya ini sesuatu yang luas …ada didalam keseluruhan itu …

R10 : oke …kenapa harus kaya …

R3 : karena tugas Cyber butuh dana besar …

R10 : kalau yang jabat nya nggak kaya …nyari kekayaan dulu …h.aha.. ha nggak ….

R all : hah.a.ha.h.a.

M : itu apa pengaruhnya …..atau ke manajemen pendidikan ..e manajemen penyidikan ….dan…e…

R3 : kalau dia mencari kekayaan buat dirinya sendiri ..dia nggak akan bertanggung jawab mas …

R10 : lagi rasanya udah males …

R1 : jadi gini…kalau saya punya pendapat gini …suatu hari ini dari

pengalaman ….suatu hari saya jadi kapten di Lebak …Kapolres rapat di Polda Bandung …wakapolres juga sama …jadi bener – bener itu saya sendiri …pekerjaan tetep jalan…jadi keseluruhan ini …itu kan cuma kemampuan – kemampuan secara …yang idealnya ya …kalau pun ini semua nggak ada tapi tetep harus berjalan ….cuma prestasi nggak akan tercapai …e..target nggak akan tercapai….prestasi nya nggak akan ada ….jadi misalnya gini …orang nya nggak pinter …orang nya nggak kaya …nggak jago inggris …dulu mungkin pernah ada …tetep berjalan …tapi tidak akan tercapai target dan prestasi … kalau pengen tercapai ….target dan prestasi ….bisa memiliki *…* yang bagus

Responden ngobrol bareng

M : tadikan udah jelas … kayanya ini butuh dana besar …sehingga nggak mungkin ….*……*

R10 : nggak bukan itu aja …*…..* pokoknya ada kepentingan dinas yang di *……..* masa saya masih naik motor aja …

M : kalau smart ….kalau smart …kenapa harus smart ….apa yang istimewa dari smart ….

R2 : smart itu cerdas….bijak …kalau beliau nggak cerdas nggak usah jadi KANIT….haha.ha..

M : maksudnya seperti itu …kenapa seperti itu …apa sih istimewanya …orang smart ini …sehingga dia bisa lebih ….

R2 : sekarang gini mas kalau nggak cerdas ..e..penyidik itu e…kan akan mendapat tekanan pekerjaan …pekerjaan itu beban berat e…kalau kita sudah dibebani tugas yang berat tapi leadernya itu nggak smart …tidak berani mengutarakan pendapat …ini ..ni tidak mudah mengutarakan pendapat …kepada pimpinan kalau hal itu …bertentangan dengan hukum yang ada di Indonesia itu tentunya kita akan tertekan terus ..tidak akan maju …nah smart ini adalah berani mengutarakan bahwa yang dia kerjakan adalah benar

R3 : gitu aja….kalau nggak ..kita yang melaksanakan yang ditekan …

M : hm..oke…jadi yang dia bisa lakukan adalah dia menghilangkan tekanan pada anak buah …orang yang smart ini …

R : e.he…

M : oke …jago inggris …

R6 : itu pasti …

M : kenapa …

R3 : cyber crime itu lintas negara

R1 : nggak Cyber crime itu udah bahasa Inggris …

R6 : cyber crime itu sudah berbahasa inggris ..

M : oke ..inikan jago inggris…kalau misalnya inggris nya biasa – biasa aja …emang kenapa …

R6 : nggak apa – apa …tapi paling nggak dia bisa berbahasa inggris ..

R1 : tadikan saya udah kasih pembukaan ….kalau semuanya nggak dipenuhi nggak masalah ..tetep jalan tapi jalan ditempat …makanya tadi kalau ditanyakan lagi …kalau misalnya nggak bisa bahasa inggris nggak masalah …tetep bisa jalan …tapi jalan di tempat …

M : kalau boleh saya tau kenapa dari detail – detail ini ..saya liat parlente …

R3 : a..itu factor penting …
R6 : penting dong …kharisma …
R3 : ya ..ya. ..kharisma
R7 : ya…jangan parlente lah …kharisma …
R6 : kharisma ya ….dari penampilan nya baik …
M : apa istimewanya …
R6 : karena ada hubungannya kan dengan luar negri …
R3 : kan kaitannya dengan ..hubungan nya dengan lalulintas ..expansi
R6 : terus kita juga berhubungan dengan instansi lain …
R2 : kalau orang nya sudah kecil…hitam…jelek …ya kantor yang bagus…megah itu …ya ..nggak keliatan
R6 : terus wangi…kan sedep ….
M : oke …rasanya seperti apa …kalau orang kita bisa mengambil orang ini sebagai pemimpin kita ..organisasi atau badan yang lain
R6 : seneng dan bangga….
R2 : kalau kita mempunyai seorang pemimpin semacam itu sudah terpenuhi …kita sebagai anak buah ini mau berjalan kemana mana tu tegak …mau melakukan tugas itu senang hati …..dibanding dengan unit – unit yang lain yang nggak sebut namanya …berjalan dengan pimpinan begitu pun e..kita tidak mau …
R1 : ditambahin boleh nggak ….jadi gini…teorinya …seseorang itu akan timbul kepercayaan ..kemampuan dan dia bisa berprestasi itu kalau dia sudah bisa membentuk image building ….cie…jadi harus dibangun dulu citranya ….kalau citranya bagus …saya dulu pernah dapat teori gini bangun citra …citra harus bagus segala macem itu kan kita jadi bangga nah kalau udah bangga
M : oke …apa yang istimewa dan apa yang bisa dilakukan oleh pemimpin yang tanggap ini …
R : si unit 5 ini bisa menjadi lebih baik …
R3 : cyber crime itu kan tehnologi …tehnologi itu nggak stak …
R6 : maju terus
R3 : berkembang …lah kalau orang yang berada disitu nggak tanggap ..ya…nggak bisa ngikutin jangan ditempat kan …
R2 : nggak usah jadi Kanit …hah..a.h.
R3 : tehnologi lho mas …dia ..dia harus bisa ngikutin perkembangan
M : nah selama ini temen – temen tau …selama ini yang temen – temen tau ntah itu senior …ntah itu apa …lebih banyak yang memiliki sifat ini …atau lebih sedikit …
R : lebih sedikit ..
R9 : sedikit banget …..
R2 : satu dibanding ….
R7 : adanya Pak Arief dan bijaksana
M : kira – kira kalau misalnya orang nya nggak ada diganti dengan orang yang tidak punya sifat seperti ini …
R7 : ya tetep ada ..
R2 : ya tetep ada …unit 5…
R6 : unit 5 tetep ada tapi dua kemungkinan kembali lagi ke jaman hutan kaya kemarin lagi …
R3 : atau kaya cyber crime …cyber crime metro…bubar …

R7 : jalan ditempat malah mundur….
M : apa yang terjadi sama temen – temen seandainya …
R6 : pasti hengkang satu – satu
M : kalau misalnya diganti …kitakan nggak tau ini mau mundur atau nggak ..saya juga nggak tau …kalau misalnya ada pergantian Kanit ..dia nggak bisa memenuhi …anda sendiri gemana
R3 : kita tetep disitu
R7 : yang bener masa tetep disitu ….
R2 : mungkin tetep disitu dalam jangka pendek …tetapi kita tidak termotivasi kerja yang bagus
R6 : kasak kusuk cari mutasi
R4 : pindah ke SDM
M : oke ..mungkin dari *…* sudah kasak kusuk cari mutasi ….
R : ya …..maksud nya cari yang lain itu gemana mas …
R2 : sudah tidak mencari pasangan hha.ha..
R10 : tidak berpikir lagi untuk bekerja tapi berpikir untuk bagaimana caranya …
R3 : bagaimana survive …
M : apa artinya saat – saat ini …saat ini temen – temen disini ada yang berpikir untuk cari iniian lain atau
R6 : gemana – gemana maksudnya ….
M : seandainya KANIT nya nggak memenuhi itu …itu akan ..ya nggak terlalu maksimal kerjanya atau bahkan cari ….apa namanya …unit kerja yang lain ….
R2 : paling tidak motivasi kerja kita ..tidak akan sama dengan yang .. yang sekarang ini …
R3 : *……* akan stak …
M : selama ini kalau dengan KANIT yang sekarang
R10 : kalau saya tidak berpikir …kalau saya dipindahkan ke tempat yang lebih enak ..ya ….
R all : hhah.a.h.a.h.a.
R2 : keinginan yang paling dalam dari kita ..ilmu Cyber crime ini kan baru saya terima sebener nya saya pengen mengembangkan lebih besar ya ..karena apa …kalau *…..* polisi kan harus tepat dan maju terus kan …paling tidak kan saya harus punya kemampuan lebih …lebih lagi …tetapi kalau punya pimpinan yang begitu itu …e..yang tidak memenuhi kriteria ini paling tidak saya …apa itu ..mau mengembangkan diri saya ini akan terhambat ….
M : kalau saya punya kekuasaan sampe ya seperti Kapolri ..dan saya nawarin sama anda – anda semua disini …kalau mau pindah itu pindah kemana …oke ..kalau satu – satu ….
R10 : satu – satu atau
M : satu – satu aja ….kalau saya Kapolri saya tawarin …kalau mau pindah …pindah kemana…maksudnya satuannya …
R10 : serse di Polda
M : kenapa ke Polda Metro
R10 : karena kalau saya pindahnya ke Papua ….
M : tapi kenapa tetep di serse
R10 : karena rasanya …enak lagi …ha.ha.a.ha.karena selama ini saya

banyak bisa berbuat di serse jadi kalau saya di mutasi

M : jadi kalau saya menawarkan …

R9 : serse juga

M : serse di Jakarta

R9 : ya …

M : kalau mbak

R8 : sama serse juga ..

M : sama

M : yang lain dari sini…

R2 : saya kira tempat di polisi itu enak semua tapi yang penting masih terlihat monas….h.h.a.a.ha..h

R : orang kampung nih mas …

M : kalau ditawarkan boleh pilih

R2 : saya kira saya dinas dimana aja terserah ya ….meskipun saya dinas di *……* yang penting ada *…..* meskipun ditempat yang enak ..pimpinan nya nggak enak ….sama aja …yang penting ada ketenangan …

M : saya …misalnya saya Kapolri …

R3 : saya situ aja ….

R7 : selama Pak Petrus masih ada nggak mau pindah …hah.a.

R1 : pindah ..kita pindah nya kemana…

M : saya tawarkan kalau mau ditempat kan

R3 : saya situ aja …saya kan dari Cyber kan nah saya mau pindah ke Laboratorium Forensik aja …

R7 : sama aja ….

R3 : oke …tapi kalau alternatif mau pindah saya ke Lab *…* aja …

M : oke …kalau harus pindah …

R1 : saya ngajar …kalau saya cenderung ya..saya cenderung a….lebih senang ya …cenderung lebih senang dinas yang dinas ditempat yang tidak terhenti …yang intensitas nya tinggi ….

R3 : ke Polda Metro…

R1 : ya…bisa ….di Metro …

Responden ngobrol bareng

R1 : yang kedua saya senang kalau ada anak buah yang bisa mengaplikasikan ..tapi tinggal saya pilih aja ..

M : kalau mbak …

R6 : saya tetep di Bareskrim ….

M : tetep jadi serse

R6 : tetep di Bareskrim …serse itu kan banyak bisa di Polda ..bisa di Bareskrim

R : kalau narkoba gemana …

R3 : kan tetep di serse …

R6 : ya pokoknya tetep di Bareskrim …

R3 : kalau pengen jadi polisi jadilah reserse ..polisi yang sesungguh nya kan di reserse

R2 : *…….*kalau saya tidak kuat …*….*

R6 : tapi kalau saya liat memang mas Arief nggak kuat …

Responden ngobrol bareng

R5 : kalau saya dimana aja …di ujung berung pun …yang penting di reserse …

M : sekarang kan penempatan di Cyber …saya tawarkan pilih penempatan dimana …

R5 : bebas…

M : boleh bebas dimana aja …mau tetep disini juga nggak apa …

R : kemarin dia mau pindah ke lalulintas ….hah.ah.a.

R5 : saya dimana aja …

M : nggak harus milih tapi mau ditempat kan dimana aja …

R5 : Polda Metro aja …

Responden ngobrol bareng

R5 : tergantung dari kebijakan pimpinan ya kan ….

R4 : kalau saya sih sekarang yang perlu sekolah …saya mau sekolah dulu …

M : kalau penempatan …penempatan …

R4 : di Mabes .

M : oke …ini mungkin udah lebih dari dua puluh menit …tapi jangan langsung pulang dulu …saya mau konfirmasi dulu …

KANIT

- PINTAR
- KAYA
- SMART
- JAGO INGGRIS
- PARLENTE (KHARISMA)
- MENGERTI ANAK BUAH
- TANGGAP
- BERTANGGUNG JAWAB
    - KESEJAHTERAAN

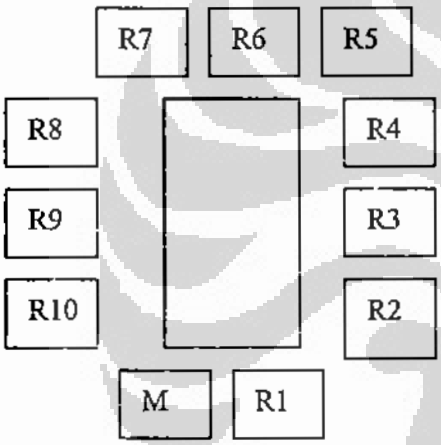
M : mau ngucapin terima kasih

R6 : tadi koq nggak ada pertanyaan kaya gini ..unit Cyber itukan IT ya

: …IT itu kan mengikuti perkembangan jaman maunya kita itu ..unit Cyber itu kedepannya itu bagaimana ..artinya unit Cyber itu direktorat bukan unit …dipimpin oleh seorang jendral …didalamnya itu unit ..unit…unit….jadi dibawah nya jenderal ini ada unit ..unit …jadi berdiri sendiri itu Cyber Crime …

M : yang pasti saya tutup aja ..terima kasih banyak udah mau datang kesini ….

Project name	: Robocop
Transcriber Name	: Eiy
Group	: 2
Tanggal pelaksanaan	: 7 Agustus 2007
Hari / jam pelaksanaan	: Selasa / 10.00 wib
Moderator	: Rulas
Kriteria group :	
Usia	: --
Jenis Kelamin	: Pria/ Wanita
SES	: --
Usership	: --



M **moderator**
R1 **idang**
R2 **surawan**
R3 **hendra**
R4 **edi hartono**
R5 **bagas**
R6 **damayanti**
R7 **zamri**
R8 **surawan**
R9 **dicky**
R10 **Jumaro**

KASET 1 SIDE A

M mungkin sebagai pembuka kita kenalan dulu kali ya, tempat kita ini sebenernya perusahaan riset saya bekerja di perusahaan ini sebagai seorang peneiliti, pekerjaan kita macam-macam ya, saya nggak tau, saya sempet belajar juga dari serse, saya ini seperti intel, ada apa dimana, saya datang kesana juga, kalau ada mitra kita kesulitan nih di daerah ini, kita datang kesana, biasanya kita di pake oleh perusahaan-perusahaan yang

punya program marketing, kadang-kadang mengevaluasi apa yang mereka lakukan, mereka bikin strategi apa yang harus mereka lakukan, pada intinya marketing pemasaran, saat ini saya dan temen saya sedang membuat penelitian tentang bareskrim polri, kita ingin tau informasi lebih banyak bagaimana, apa dan perkembangannya seperti apa, yang di harapkan kedepan, apa yang bisa di lakukan, nah tujuannya selain memberikan masukan pada polri juga adn yang terkait sebagian nanti akan di gunakan oleh seseorang yang ada di ultima, pak petrus juga sedang berada dalam perjalanan menuju kesini, ini acaranya santai-santai aja, ngobrol-ngobrol, mungkin nggak harus kayak di dpr, ada interupsi segala macam, ini hanya ngobrol biasa, ini emang di rekam pake video gunanya untuk dokumentasi, di belakang sini ada temen saya, yang akan mencatat semua yang kita bicarakan disini secara detail, nggak ada yang hilang, jadi kita tau siapa yang ngomong apa, degan apa jadi bisa nyambung gitu loh, di belakang saya ada one mirror, dia bisa liat kita, mereka tim saya yang mencatat dan mungkin juga nanti kasih masukan, tolong dong tanyain soal ini, jadi mereka semua ada disana, jadi nanti akan datang beberapa, teknisi saya juga, jadi jangan kaget, kalau ada apa-apa kita perlu apa tiba-tiba udah ada

R4 kalau one mirror udah biasa ya he he he, sebelum mulai saya mau tanya mas siapa

M rulas

R4 ini kan mau ngobrol-ngobrol, ini kan mas sebagai moderator atau art nya lah, ini kan membahas masalah cyber crime, seperti mas sampaikan tadi bahwa mas mengadakan penelitian berdasarkan pesanan, intinya mas sudah punya bahan dasar mengenai cyber crime ini, entah unitnya itu bagaimana cara kerjanya itu bagaimana, sekarang mas menggali lebih dalam lagi, jadi obrolan kita jadi lancar, berdasarkan yang mas tau dari awal, mungkin awalnya mas tau ini A, saya rasa nggak ada masalah, tapi kok menurut mas ini kok, ternyata kok B

M betul, justru ini pendapat-pendapat secara pribadi, nggak semua sama, karena tiap orang punya pengalaman yang beda, punya pandangan yang berbeda seperti itu, jadi bukan bicara salah benar, mungkin saya akan banyak nanya hal-hal yang, mungkin pertanyaan saya akan terlalu mendasar

R4 nggak masalah

M karena belum paham betul

R4 diskusi ini sifatnya satu arah atau 2 arah atau gimana

M oke, nanti saya akan lempar pertanyaan, yang lain juga boleh menanggapi juga pertanyaannya

R7 secara experience lah ya

M iya secara pengalaman, nanti saya jelasin apa yang akan kita lakukan, nama saya Rulas, lengkapnya rula rebaldo sihombing, usia saya mungkin paling muda disini, status masih lajang, dalam proses persiapan

R8 perlu di teliti juga mas

M mobilitas terlalu tinggi

R8 di telitinya lebih jauh

All he he he he

R7 kalau itu terakhir aja
M oke, kita mulai kenalan dulu siapa, walaupun udah ada nama tapi lebih enak kalau itu di bahas
R3 bapak bisa tunjuk
M mungkin dari sebelah kanan aja silahkan
R1 nama saya idang maryadi
M usia berapa
R1 usia saya 42 tahun
M berapa lama sudah tugas di unit ini
R1 2 tahun
M oke, lanjut
R2 setiadi usia 43 tahun lebih 3 bulan , masuk unit cyber crime 1 januari 2004, lalu terhitung juli 2006 saya masuk crime track system, intinya menangani masalah-masalah yang berkaitan kejahatan exploitasi anak-anak masih masuk dalam cyber crime
M oh exploitasi anak-anak yang di foto-foto itu ya
R2 bukan Cuma di foto-foto aja mas, foto-foto itu nggak ada artinya, kalau hanya melihat foto kan percuma toh
M oh oke
R2 ada tindak lanjutnya yang lain beberapa langkah
M oke
R2 itu yang lebih berbahaya
M oke, terima kasih
R3 nama saya suminta nama samaran ricky
All he he he he
R3 jabatan parmin S D T A
R3 biar panjang ya he he he
All he he he he
R3 kalau itu asli bukan rekayasa, umur sekarang 18 jalan maksudnya jalan-jalan, umur 47 tahun, terus satu istri 2 anak yang resmi ya pak
All he he he
M di unit ini udah berapa lama pak
R3 2 tahun, tapi sebelumnya polda metro udah 3 tahun lama, baru setelah ketemu pak dicky itu, apalagi ya, itu aja
M terima kasih pas, silahkan pak edi
R4 saya edi hartono, saya masuk 2005, oktober sekarang udah 2 tahun, umur 40 tahun
R5 nama saya hendra, usia 40 tahun, dinas di cyber baru 1 tahun 9 bulan, mungkin baru waktu singkat ya ada cyber, itukan berhubungan dengan teknologi, ini kan suatu senjata dari polri untuk mengatasi kejahatan cyber dimasa yang akan datang
M sebelumnya tugas dimana pak?
R5 saya sebelumnya banyak sekali, terakhir saya anggota polres di kaltim
M oek, silahkan
R6 nama saya damayanti, umur saya 49 tahun, mungkin saya paling tua disini, saya di cyber crime sudah 2 tahun
M sebelumnya di?
R6 sebelumnya saya di direktorat narkoba

M oke
R7 saya Zamri, dinas sudah 1,5 tahun, masih muda, umur baru 39 tahun
M sebelumnya dinas di?
R7 polda metro di densus 88
M silahkan
R8 nama saya surawan, umur 33 tahun, saya berdinas di cyber crime baru 1,5 tahun, sebelumnya saya bertugas di ujung sulawesi gorontalo
R4 masih indonesia
M oke
R9 nama saya dicky kertanegara, usia saya hampir 36 tahun, tugas di cyber crime mungkin paling lama dari tahun 2003
M tahn 2003
R9 iya, sudah hampir 5 tahun
M sebelumnya
R9 sebelumnya saya di jawa tengah, sebagai kasaserse
M kasaserse
R9 iya
M oke, silahkan
R10 nama saya ibu jumaroh, usia 48 tahun, saya di cyber baru 1 tahun 6 bulan
M sebelumnya di
R10 polres jakarta selatan
M di
R3 personil
M oke, ini saya ingin minta masukan tentang keberadaaan cyber crime ini, saya masih orang awam, mungkin banyak sekali orang-orang seperti saya, kalau di bilang ada satu unit di polri yang menangani it dan cyber crime, untuk apa di perlukan ini gitu, mungkin bisa di ceritain nggak, sebenernya unit ini perlu nggak sih? Kalau perlu kenapa ya, nanti di tanggapi ya
R4 saya mencoba menggambarkan secara singkat jadi emang awalnya ini di betuk tahun 2001 sebenernya dulu masih jadi porserse, itu mungkin masih sifatnya masih embrio, yang penting terbentuk dulu, untuk antisipasi karena kejahatan cyber khususnya kejahatan komputer, kemudian di kembangkan lagi di direktorat 2, itu di bentuk cyber crime, itu tugasnya itu adalah melakukan penyidikan-penyidikan kasus cyber crime dan melakukan menyelanggarakan crime forensik, hanya ada di satu kesatuan
M itu emang belum ada di polda ya
R4 mabes, itu tahun 2002 sampe sekarang, dulu porserse sekarang bareskrim, kemudian berkembang jadi unit it dan cyber crime

M oke
R5 itu kan tantangan ya, tugas polri yang bergeser dari kejahatan konvesional ke kejahatan cyber crime, terbentuknya di kalangan pusdenkasus dan kapolri tahun 2001, polri sudah lebih dini mengantisipasi, akan terjadinya kasus-kasus yang berlatar belakang IT, kemudian berkembang-berkembang sampe saat ini yang mana posisi dan keberadaannya berada di direktorat 2, tindak kejahatan khusus, artinya kejahatan teknologi ini di anggap kejahatan khusus spesialis, mungkin itu suatu aturan perlu tindakan khusus dalam penanganannya, mungkin itu awalnya masuk,

kejahatan yanga berbau cyber ini mungkin yang berbau awam, kejahatan cyber ini yang bernuansa teknologi, di mabes sendiri memiliki 1 unit pada saat proses penyidikan kasus-kasus cyber, satu lagi adalah pemeriksaan secara forensik, kemudian berkembang-berkembang sampe beberapa kepemimpinan, ada beberapa kemungkinan jadi muncul unit it dan cyber yang di pimpin pak petrus pada saat itu, sehingga di perjelas lah, kemudian di bentuk lagi, di perjelas lagi, dengan mengadopsi beberapa sumber sources yang ada untuk mempertegas apa sih unit cyber itu menurut polrinya sendiri, sebetulnya di lingkungan polri sendiri, sebenernya timbul pendapat yang berbeda

M ini menarik nih

R5 sehingga butuh pemahaman dan pendalaman oleh seluruh anggota, mereka sendiri mungkin unit it mereka belum paham, ada yang menganggap itu sebagai workshop, secara teknis adalah latar belakang suatu penyidik, menyidik kasus-kasus yang berlatar belakang it, yang lebih dominannya ada beberapa perbedaan pendapat, sehingga kedepannya di harapkan mengerti di lingkungan polri sendiri, sedangkan sekarang sudah berkembang kejahatan cyber di indonesia, karena hanya indonesia dan laos di asia yang belum punya peraturan undang-undang, dan mungkin 2007 akan di launchingkan undang-undang ini, itu kalau untuk indonesia, mungkin boleh dikatakan selama indonesia masih primitif perundang-undangannya, umbrelanya tidak ada, mudah-mudahan dengan ini bisa di katakan polri sudah jauh melangkah dengan negara yang lain, selangkah atau 2 langkah lebih maju dari mereka

M saya sambil nulis ya

R2 barangkali saya melihatnya pak edi membahas skop lebih dalam lagi, saya sebelum membahas lebih fokus lagi, mungkin kita bisa melihat tinjauan bahwa kejahatan itu ada beberapa hal yang perlu kita bagi, kejahatan yang konvesional, dari zaman dulu sampe sekarang masih ada, kemudian kejahatan-kejahatan terhadap kekayaan negara, korupsi, malak-malak kayu, tambang dan sebagainya, kemudian kejahatan trans nasional, antar negara, yang terkahir itu kejahatan-kejahatan krusial, yang apa namanya urgensi, misalnya penadah, kemudian ada kejahatan subversif, teroris, mau tidak mau, suka tidak suka pasti menggunakan teknologi, misalnya mas ini mau mengancam kan, sekarang ini kana da teknologi SMS, kalau dulu, kita ada teknologi pager, kan nggak mungkin kitamau ngancem orang, itupun bisa" operator saya mau ngancam ini ini, bisa juga, tapi kalau ancaman operator nggak akan menyampaikan kan

M iya

R2 sekarang ini kan bisa sms sendiri, telpon sendiri, kejahatan korupsi sekarang sama menggunakan teknologi, jadi karena semuanya itu menggunakan teknologi, kita mau nggak mau polisi harus lebih mengerti dan menguasai teknologi dan segala pemanfaatanya baik yang efektif maupun positif mas, nah tadi pak edi sudah

M artinya ada peningkatan sarana dan prasarana

R2 betul, karena sarana dan teknologi itukan ada posiif dan negatifnya, itu masukan dari saya

M oke, ini menarik nih, pertanyaan saya tadi apa urgensinya sebetulnya kan, kalau bapak bilang karena ada perkembangan teknologi yang sangat besar sehingga bisa di manfaatkan ke hal-hal yang justru negatif, selain itu apalagi urgensinya yang perlu saya tau, apakah sebegitu urgent nya sehingga harus di buat menjadi 1 unit

R8 kalau kita bicara soal urgensi, awalnya di buat karena unsur kepentingan, tahun 2001, kebetulan saya tau asal usul cyber crime, awalnya itu hanya sebuah divisi tahun 2001, itu ada official meeting internasional crime, cyber crime itu masuk salah salah satu crime yang ada di divisi tersebut, nah di indonesia belum ada unit yang menangani secara khusus, sedangkan banyak kejahatan pada saat itu penipuan melalui internet, waktu itu sebatas hanya masalah carding, jadi pemesanan barang ke luar pake kartu kredit orang lain, tapi semua barang di kirim di indonesia, tahun 99-2001, itu sangat banyak sekali di Indonesia pada saat itu, banyaknya carding-carding sehingga di bentuklah unit cyber crime ya di bentukan tim untuk mengatasi masalah ini, terus tim ini kalau nggak salah itu kabsunit itu di bawah unit pindad, di bawah derektorat ekonomi pada saat itu, setelah ada cap 54 tahun 2002, di bentuklah yang tadinya di bawah pindad tersebut unit sendiri yang di sebut unit cyber crime, sejak berdirinya cyber crime itu awalnnya memang kita khusus mengatasi masalah carding tadi, tapi seiring dengan perkembangan zaman dan dengan bertambahnya, pengetahuan baik dari sisi polrinya, penegakan hukumnya, baik dari segi pelakunya saat ini kasus rintangan itu tidak sekedar penipuan melalui internet dan itu membutuhkan kemampuan sendiri, sampe kita punya lab makanya tadi kata pak bagas mungkin bukan work shop ya, tapi kita sebagai saksi ahli saja, atau kendaraan yang di gunakan untuk membantu penyidikan tindak pidana lain, yang menggunakan komputer, memang komputer bisa sebagai sasaran, bisa sebagai alat untuk melakukan kejahatan, bisa juga sebagai alat penyimpanan kejahatan itu sendiri, sehingga persepsi tersebut membuat unit ini bagi sebagian orang mungkin yang di maksudkan menjadi sudah tidak terlalu besar, tapi kita melihat hal tersebut salah, di luar negri mungkin ada yang bicara masalah teknis computer dan sebagainya itu di bawah labfor, tapi yang berkaitan dengan cyber crime langsung itu unit cyber crime punya, punya lab sendiri itu di bagi beberapa sub kerja, ada bagian lab nya, ada bagian ada bagian pendidikannya, ada bagian analisisnya, kalau kita liat menurut saya ini masih terlalu kecil kenapa saya bilang kecil karena kita ini sebuah unit, ini bukan unit satuan kerja, karena unit satuan kerja disini adalah bareskim, unit kerjanya nya adalah direktorat sedangkan unitnya yang ada di bawah puslabfor ada lah unit kerja, sedangkan dia untuk maju kedepannya nantinya dan dengan intesitas kejahatan yang ada sekarang, memang kita tidak bisa mengatakan kejahatan ini sudah banyak sekali, kenapa, kelemahan kita adalah kita tidak punya data, yang secara kongkrit yang menyatakan bahwa memang kejahatan ini segera di tangani, karena misalnya kita berpatokan data ada 1200 kejadian baru 100 yang di tangani ini kan membahayakan

M iya

R8 tapi baik yang dari infomiko, Abzis yang punya kepentingan dengan isp, itu mereka tidak melakukan kompulasi data, sehingga data yang adapun kalau menurut kami yang paling lengkap ya di unit kami, karena itu ada kejahatan langsung, dalam arti kata yang merasakan korban secara langsung tapi yang sifatnya mungkin bersifat memasuki sistim jaringan itu dan segala macam itu sangat jarang sekali menelan korban, mereka hanya melaporkan biasanya ke Isp, dan isp pun jarang mengkompulasi laporan tersebut sehingga itu salah mungkin kelemahan kita, ini sangat urgent, tapi kita tidak mengatakan kenapa ini urgent, mana buktinya, mana faktanya, sehingga undang-undang cyber law itu sendiri pun masih menggantung, makanya saya katakan unit ini perlu dan sangat penting dan malah sebaiknya di besarkan karena cyber crime itu sendiri mungkin rekan-rekan yang pernah ke luar negeri, begitu nanya"anda di divisi mana" cyber crime itu kelasnya beda dengan penyidik atau investigator konvensional

M maksudnya kelasnya beda

R9 pada saat kita menangani satu kasus yang sifatnya lebih bergengsi seperti cyber crime, narkotik, terorism, itu orang melihat kita ini orang punya kemampuan lebihan lebih sehingga kita tempatkan disana

M oke ada pendapat seperti itu, ada kecenderungan seperti itu,

R5 kalau saya menangkan memang darai kisan-kiasan yang tersirat dari mereka, pada dasarnya kita sama-sama mendapatkan pendidikan, namun kita di beri kemampuan lebih tentang kasus-kasus, sehingga anggapan dari temen-temen yang konvesenional itukan sudah ada framenya, kita didik itu bisa, namun bagi para penyidik ini, ini butuh ketrampilan khusus, yang di latar belakangi dengan kemampuan dan ketrampilan sehingga anggapan mereka ini adalah memang orang-orang yang trampil atau expert dalam bidangnya selain dia punya kemampuan penyidikan dia juga punya kemampuan it

R7 saya tambahkan sedikit tadi ada pertanyaan seberapa penting sih perlu ini, seperti yang sudah di jelaskan tadi sangat perlu dan mesti di kembangkan, ini terbukti dengan pelatihan yang di laksanakan dimana beberapa polda itu sudah di bentuk satuan sub unit cyber crime, bareskrim dalam hal ini sebagai pembina fungsi itu turut serta mengirimkan personilnya itu dari pihak luar, itu membuat kita mau tidak mau, suka tidak suka, tidak bisa di pungkiri lagi, meskipun RUU yang sedang di godok dan mau keluar ini, sudah mencakup semua undang-undang dan relugasi sudah ada yang mengatur, Cuma saja mungkin seperti yang pak bagas bilang untuk duduk di cyber crime itu paling tidak harus punya 2 ketrampilan, ketrampilan sebagai penyidik dan ketrampilan dalam hal teknologi informasi, sekarang masalahnya adalah seberapa banyak orang yang bisa menguasai 2 secara bersamaan, kalaupun ada mungkin dia penyidik di tempa pendidikan, untuk belajar teknologi ataupun sebaliknya, orang teknologi yang di rekrut belum bisa dia di penyidikan, ini sebuah persoalan, kemudian bagaimana dengan bareskrim sendiri dalam hal ini di unit 5 atau 2, ini secara berkala mengikut sertakan personilnya yang sudah memiliki sebuah kemampuan penyidikan untuk berlatih di luar negri, training, di satu sisi untuk rekan-rekan yang baru bergabung dari fungsi-fungsi yang lain, di polri itu ada

beberapa fungsi ya, di polri itu ada beberapa fungsi ya, seperti polisi lalu lintas itu segera bergabung untuk mekanisme sebuah penyidikan, jadi intinya dua, dia harus punya ketrampilan penyidikan dan ketrampilan teknologi informasi

R4 sesuai dengan yang tadi saya katakan, unit cyber crime dan unit forensik, jadi 2 ini harus di miliki oleh penyidik yang ada di unit cyber crime, idealnya

M yang menarik buat saya adalah pertanyaan tadi kenapa unit ini perlu, kebanyakan dari temen-temen tadi disini bicara soal kronologis dan soal penetapan siapa yang punya kepentingan, tapi kalau misalnya saya Tanya pendapat pribadi temen-temen sendiri, emang sebegitu urngetnya

R4 iya

M perlu untuk memiliki satu unit

R2 harus ada nggak hanya unit tapi division

M kenapa

R5 kita pernah, bahwasannya semua tindak pidana yang saat ini ada beberapa direktorat, direktorat 1, itu untuk tentang keamanan negara, direktorat 2, itu tentang eksus kita, direktorat 3, tipikor, direktorat 4 tentang narkotik, 5 divider, yang nota bene semua tindak kejahatan yang ada dunia, dengan kemajuan teknologi tidak ada yang tidak menggunakan teknologi, baik teknologi sebagai subyek maupun sebagai obyek sehingga di butuhkan juga untuk seorang anggota polri, untuk bisa lebih baik, kalau ini hanya di bentuk di mabes, kalau itu skupnya hanya kecil bagaimana kalau terjadi mis di lapangan, dengan keefektifan dan kecepatan dalam proses penyidikan

M sorry saya potong, saya tertarik pendapatnya, kenapa ini perlu sebagai unit, kalau perlu jadi divisi, kenapa ini tidak bisa di lakukan misalnya di setiap saya jupitel, atau kasub itu masing-masing punya satu bagian yang menangani atau apa namanya yang bekerja untuk penyidikan dengan kemampuan tadi, it dan cyber crime, karena pada prinsipnya kan di bilang, dari semua itu kan unit-unit satuan kerja itu ada penyidik, kan bedanya it dan cyber crime, yang lainnya sama, kenapa nggak di buat di setiap unit misalnya golkaso atau apa, yang emang berhubungan dengan teknologi

R5 tidak semudah itu di dalam tubuh polri untuk membentuk satu kesatuan restrukturisasi organisasi dan sebagainya, semunya membutuhkan suatu proses yang panjang

M oke

R5 jadi tidak semerta-merta, hari ini di bicarakan besok terjadi, tergantung juga dari kebijakan daripada pimpinan kalau menurut saya untuk antisipasi polri sebagai public pelayanan masyarakat, ini segera di bentuk dalam bentuk yang besar ada reformasi organisasi mungkin nanti unit cyber crime yang mas rulas bilang tadi ini semuanya sudah memiliki, kalau direktorat sendiri, setiap kejahatan ada berbau teknologi, otomatis nanti semua tidak ada yang tidak bisa di tangani oleh cyber, orang cyber bisa menangani itu, itukan penyidik mungkin dia punya kemampuan itu, daripada harus 2 kali ya efektifitas kerja, nggak tau orang manggil orang cyber, lebih baik dia sudah punya kemampuan itu

R4 saya tambahankan gini, kita punya data skem justru data skem itu penjelasannya harus di revisi sebenernya iya, kan, secara apa namanya itu belum di jelaskan apa sih maksudnya cyber crime, itu yang di revisikan sebenernya oke, oleh itu sudah di fungsikan

M oke, saya minta tolong

R4 takutnya diskusi kita belum selesai pak petrusnya sudah datang

R7 tapi itukan topiknya beda ya, cyber crime ini menurut secara pribadi kan

R3 saya ingin menggaris bawahi apa yang tadi dikatakan, mas rulas mengatakan bahwa apakah ini perlu, kalau aku bilang, itu sangat urgent sekali, ya, karena ada beberapa hasil penelitian, Indonesia pernah indonesia pernah ikutan di vina tapi soal penyalahgunakan teknologi gitukan, tapi justru penggunaan internet itu paling bawah kita, tapi penyalahgunaannya tinggi, justru ini lah faktor-faktor yang menyebabkan ini sangat perlu, karena akan berdampak pada ekonomi, pada negara, besar, makanya harus ada ti walaupun belum semuanya, kalau misalnya cyber crime ini seperti majalah tempo, tempo kan slogannya"enak di baca dan perlu", tapi cyber unit itu bukan hanya enak di baca tapi sangat di perlukan dan apa memiliki produk yang bagus, saya bangga dong, di cyber crime karena baru setahun he he he

M oke, iya

R1 saya ingin menggarisbawahi apa yang di katakan, mungkin ya, kalau kita katakan ya, tanpa di dukung datapun saya katakan bahwa pembentukan unit cyber crime itu sangat perlu sekali, itu kan di bentuknya tahun 2002 ya, itupun kalau di bandingkan negara lain, negara kita sangat terlambat, singapure tahun 93 udah punya cyber com, india kalau tahun 90 dia udah punya cyber cop

M kalau negara lain sudah lebih dulu, itu nggak menjelaskan kenapa kita perlu sekarang

R1 entar dulu saya bicara belum selesai

M iya iya

R4 he he he he

R1 kalau di katakan teknologinya relatif sama, singapure penduduknya itu berapa 3 juta, kalau dia semua rakyatnya pake internet, kalau kita berapa 10% nya aja udah 23 juta yang pake internet, belum lagi yang salah penggunaan, itu dari segi penggunan internet, jadi termasuk tahun 2001 itu sangat terlambat dari segi pembentukan ya, force invorsmentnya, di bandingkan dengan regulasinya, kita juga sangat terlambat sekali, kenapa tahun 2007 tak satu pun yang spesifik mengatur kejahatan cyber,

M belum ada ya

R belum ada, sekarang singapure udah ada 7, yang mengatur undang kegiatan cyber, termasuk india banyak sekali, justru india yang akan membantu negara-negara rekanyang belum ada

M india emang maju juga ya

R1 itu dari pembanding, kalau dari data konkrit itu segi kelemahan birokrasi kita, itu kelemahan entah di polisi itu sama, sampe di hankam pun ambaradul semua

M jadi cyber crime nggak ada birokasi

R1 maksudnya di birokrasi lembaga-lembaga yang lain jadi yang kita rasakan termasuk pak adi kita rasakan bahwa penyalahgunakan it itu kita rasakan, itu tenang kejahatan siapa aja, kita banyak laporan kan, mana teratasi dengan baik nggak, kemuduan yang lain banyak juga, dari internet dari segi kualitatif apa yang di rasakan masyarakan apa yang kita rasakan, itu kelemahan kita, datanya amburadul semua, itu sudah sangat sangats\sangat kejahatan it nya ya itu dari HP, dan itu digital kamera atau internet sarana teknologi informasi yang lain itu sudah menjadi catatan sendiri mas

M itu sudah ada ancaman dari situ ya

R1 iya

R7 pak idang mohon maaf pak idang, kalaupun data itu lengkap, katakanya jumlahnya datanya jutaan, tapi bagi masyarakat itu belum satu hal menekutkan

R1 jangan di rasakan, kayak kegiatan penipuan aja, ini kok polisi nggak pernah melayani, paling 1 2 dari ratusan ribu masyarakat komplain, ini misalnya

R7 masalah penyelidikan seberapa banyak masyarakat butuh

R1 jangan tanya masyarakat dulu, yang masyarakat teknologi informasi, entah hp, itu banyak di protes loh jangan kira

R7 tapi mereka nggak ada yang takut

M jadi yang saya pengen tau juga pertanyaan saya, saya minta di yakinin, saya masyarakat awam nih, saya nggak tau tuh, saya nggak tau prosedur, bahwa ada skem apa segala macam dan kenapa itu perlu jadi unit perlu ada, kenapa itu jadi unit, apa perlunya

R6 saya setuju semua pendapat, saya bilang perlu seperti pengalaman saya pribadi dia seperti kasus poli ex kebeulan saya menangani itu berantai, berantai dari email list nah itu hanya obat, itu gimana dengan info yagn apa ya, misalnya bisa ada bom atau apa yang nggak bener itu suatu apa ya

R5 keresahan

R6 iya

R7 masyarakat jadi takut

R6 jadi was was, ini bener nggak nih, itu satu kasus pentingnya ada satu unit cyber dan lebih bagus di perbesar lagi jadi direktorat atau divisi

R2 aktualnya mas kalau kita baca di korand an internet, itu pemerintah dan unilever, kominfo, yayasan lembaga konsumen mengeluarkan 1 juta exemplar untuk hati-hati penipuan lewat sms, internet, maupun di koran, karena kan mereka menggunakan atlease teknologi, "selamat anda menang sekian transfer sekian, berartikan mengunakan teknologi juga" itu memberikan gambaran pemerintah sedemikian pedulinya kepada masyarakat yang pulsanya suka di habisin kayak gitu lah, itu salah satu cyber crime loh

M oke, dari tadi yang saya tangkap adalah, kita perlu banyak alasan untuk itu, yang belum saya yakin kenapa ini perlu jadi unit bahkan kenapa perlu di kembangkan

R4 maaf mas saya potong, perkembangan teknologi pesat juga, teknologi itukan itu memudahkan kita, untuk berbuat iya kan di samping positif banyak juga negatifnya, nah negatifnya ini makanya di bentuk cyber

crime, pengancaman lewat sms, internet segala macam, karena persentase keadaannya sangat mengkuatirkan

R6 semuanya bisa masuk tindak pidana cyber crime itu

M ini terjadi perdebatan sebetulnya apakah ini hanya jadi workshop, nah ini gimana .

KASET 1 SIDE B

R3 seperti yang di sampaikan pak edi tadi, di samping positifnya teknologi ini ada dampak negatifnya, penipuan, terorisme, yang kedua terjadinya pergeseran kejahatan konvesional yang berbentuk kekerasan, pake linggis dan senjata tajam lainnya, kalau teknologi itu menjadi pergeseran dengan komputer kita bisa melakukan segalanya segalanya, apakah itu mencuri data, menipu, sehingga dengan adanya kejahatan ini yang biasanya kita menangani kejahatan konvesional kita jadi gaptek bagaimana kalau terjadi cara menggunakan kejahatan-kejahatan dengan teknologi, maka dengan kejahatan ini di perlukan orang yang khusus dn peralatan yang khusus gitu loh, nah peralatan ini sangat mahal, kita nggak bisa jadi di cyber crime, seperti kita mau melakukan pemecahan satu kasus, butuh apa namanya advis, nah advis itu mahal dan itu perlu orang khusus untuk menangani hal ini

M oke

R9 sedikit tambahan sedikit menurut saya kenapa cyber crime tidak setiap unit itu ada mungkin menurut saya kenapa penting adalah agar penangananya lebih fokus, sebab kalau itu di setiap unit ada, dia menangani dengan konvensional, atau perkara lain ditanganinya, sedangkan untuk menangani ini tidak bisa di sambi, itu perlu kefokusan sehingga di butuhkan unit sendiri

M ini kalau saya nggak salah tangkap ya, kenapa ini harus jadi unit intinya adalah efisiensi, ada birokrasi seperti pak bagas bilang terus ada juga kondisi-kondisi yang terjadi mulai dari proses, cara-cara skill segala macam, yang berbeda dengan unit lain, ini akan menghambat efektifitas bila terjadi kasus seperti ini, dengan tipe seperti ini

R7 mungkin salah tangkap, yang lebih dominan adalah bergesernya modus dari yang kovensional, ini di tangani segera, kalau birokrrasi yang di kedepankan, jadi dimana upaya manfaat itu dimana kan nggak keliatan

M iya

R7 jadi itukan sebuah keputusan yang nggak bisa di tolerir

R4 ini kembali ke tugas pokoknya, tugas pokoknya seperti kita, saat melakukan penyidikan tugas puslabforensik

R7 yang pertama kenapa itu di bentuk

M yang saya dapatkan dari temen-temen, satu bagian kerja keberadaan satu organissi yang menangani adalah perkembangan teknologi yang memang ini bisa di gunakan untuk kejahatan tapi semua alasan itu, di bagian awal belum menjelaskan kenapa ini jadi suatu unit gitukan yang terkahir pembicaraan kita kenapa harus mejadi satu unit karena kita perlu efisiensi dari birokrasi dan efisiensi sumber daya, sumber daya artinya karena unit yang lain bicara penyidikan kita perlu mengadakan alat-alat yang mendukung terus dia akan di unit-unit yanglain menangnai cyber crime perlu ada bagian cyber crime itu akan lebih bagus

R4 nggak pak, tadikan bapak mengatakan kenapa tidak di setiap unit, itu dari awal yang namanya manjemen dari awal itu pembagian tugas jelas makanya ada unit yang namanya cyber crime, kalau yang lain sduah di tangani, karena hal ini baru itu karena belum ada sampe adanya perkembangan kejahatan itu tadi, apa perlu unit cyber crime, nggak perlu lagi, karena sudah ada bagian-bagiannya

M oke, ada tambahan komentarnya

R5 saya menyimak secara general tantangan itu udah jelas, masalah perkembagan teknologi itu sudah jelas yang harus bisa di tangani polri, lemudian dalam sisi organisasi unit ini perlu, kenapa, tadi disebutkan bahwasannya kalau tok emang efektifitas cybe crie jadi unit, memang kita udah punya struktur organisasi, nah struktur organisasi ini dalam kaitanya manajemen adalah untuk membagi, pembagian tugas harus ada pembagian tugas, kemudian struktur organisasi untuk supaya tidak terjadi mis, ini harus di satukan dalam satu unit, yang memang punya kemampuan spesifikasi, memang dalam tubuh saya kira setiap organiasi punya birokrasi, birokrasi ini di buat untuk mempermudah untuk bekerja dari satu kegiatan termasuk dalam proses masalah matrialnya, dan sebagainya, seperti yang pake edi, pak surawan katakan untuk meminimize sumber daya matrialnya karena ini mungkin perlu force yang paling besar, pak dikcy menyebutkan perlu adanya lebih terfokus tidak semuanya, sehingga tidak bisa di switch antara satu dengan yang lain, karena masalah ini, emang unit spesial, special force

R4 specialforce saya bangga jadi itu pak

All he he he he

R3 kembali ke laptop, saya sudah dengar dari para panelise diskusi dari A – Z, dari yang mempunyai master teknik sampe MSI, saya sarjan hukum sebentar lagi, kembali ke pokok permasalahan, yang di tanyakan moderator, unit cyber apakah penting, sangat penting khususnya di indonesia, jawaban saya dari diskusi tadi sangat-sangat penting, kenapa karena kejahatan konvesional sudah sangat berubah, kenapa karena di undonesia sudah banyak kejahatan yang menggunakan teknologi infromasi, dengan banyaknya kejahatan yang berbasic informasi perlu di bentuk suatu unit cyber crime, itu kalau di mabes unit tapi kalau di polda itu bentuknya udah kesatuan, kesatuan cyber ya, kenapa sangat petning karena yang pertama, menurut saya unit cyber itu tidak perlu berkembang jadi divisi, dan sebagainya karena banyaknya personil, banyaknya anggota, banyaknya segala macam kalau tidak di dukung dengan kemampuan, skill, sarana, prasana, itu non sense itu nggak akan ini, nggak akan jalan, kemudian, orang harus bekerja di cyber crime harus punya keinginan

M keinginan

R3 iya, harus punya keyakinan, perlu, kita mau di unit itu, karena dinas di cyber itu bukan seperti itu, dinas perbankan, pajak, ini dinas khusus semua teknologi, pekerjaan sehari-hari itu teknologi, susahnya di cyber itu bukan karena ide, suatu pekerjaan, suatu pekerjaan polisi lah, kita berhasil kalau mereka punya kemampuan, skill untuk melakukan penyidikan yang baik, pada dasarnya cyber semua nya sama, mau di jerman, Mau di seluruh dunia pengumululan data yang akurat dalam rangka melakukan

penyidikan, yaitu penangkapan, penyidikan makanya intinya kita harus bisa melakukan penyidikan dengan baik, itu baik konvesional maupun kejahatan yang berbau teknologi kalau tinggal nangkap itu ibaratnya kayak nunggu orang mau melahirkan, cyber itu perlunya biaya yang tinggi, perlu sarana dan prasarana, alat media yang kita punya perlu alat bantu, alat bantu juga penting pak, nggak akan berjasil tanpa di alat bantu, supaya bisa berhasil karena sarananya tok nggak ada, keudian yang kedua, unit cyber perlu, nggak perlu kayak singapore yang personilnya ratusan lebih pak, seperti dulu, kejahatan konvesional itu kita bentuk file, kita perlu bentuk divisi lengkap, ada bagian penyidik, ada bagian nangkep, bagian prasarana lengkap, tidak terlalu banyak orang tapi efisien

M menarik nih, bagaiman pendapat yang lain

R7 yang penting kemampuan

R3 pertama efisiensi, iya toh, ratusan orang, kata orang jawa itu, the man behind the gun, kalau dia nggak make sama aja, mau nembak belakang yang kena depan pak, jadi itu warning aja

M ini menarik nih, ada pendapat yang beda nih

R3 nggak perlu banyak orang, banyak orang nggak efisien

R7 tapi kalau mampu

R1 banyak orang tapi harus bagus

R2 banyak orang perlu

R4 jadi gini sebenernya unit crime itu udah bagus, kalau perlu besar atau tidaknya, sebenernya kemampuan yang harus di besarkan

R7 kualitasnya

R4 jadi cyber crime ini bisa mengcover seluruh indonesia jadi dana untuk efisiensi, di dukung aja nih yang cyber crimenya, di urus anggarannya, personilnya perlu di matengin, ibaratnya teorinya, dalam kopasus itu dalam 1 orang punya kemampuan 9 orang, setiap orang nah ini gimana percetakan ini, sumber daya itukan individu, ya kemampuanna, skilnya kedua satu kebanggan itu udah ada organisasi, job descriptionnya harius jelas, nah yang ketiga ini yang harus ada sehingga sudah tercover semua seluruhin donesia

R3 kenapa setiap unit sebagai satuan cyber crime karena gini pak, menajemen di kepolisian ini secara tidak langsung membawahi reserse reserse yang ada seluruh indoensia ini dan ini sudah berlangsung, sudah berjalan itukan ada kejahatan perbankan mungkin masalah transfer yang berkaitan dengan teknologi, itu biasanya dari situ minta tolong sama kita cyber kita punya operator magic komputer, kalau mereka mau ambil data, dalam masalah perpajakan ambil data dari komputer nggak masalah, jadi memang jadi nggak perlu masing2, cukuplah unit cyber sudah cukup lah, untuk mabes terus kapolda satu sat8

R2 mungkin gini mas kalau waktunya berbeda itu no problem, tapi kalau beberapa tempat saling minta bantuan kita, itu pasti satu saat pasti akan terjadi terjadi, kalau saya cenderung ke pake edi kalau kita memiliki personil yang memadai katakan 40 orang punya kemampuan untuk 120 orang itu lebih bagus lagi, kalau sekarang 20 orang kita mau kesini nggak bisa kesini nggak, terbatas, kemudian kedua nah kasus yang didepan mata, tapi anggaran dari kantor lebih minim, nggak ada, nah ini jadi pekerjaan

apa ini kita kerja atau kerja bakti, kita koreksi juga pda pimpinan, bukan hanya memerintah tapi juga kebijakan angggaran yang memadai

M ini menarik

R4 idealnyamemang seperti itu

R9 kalau bicara kemampuan saya setuju kalau bicara struktur iyu haus di bedarkan, kenapa saya bilang beda, wajar kalau kita mengajukan anggaran itu sulit, karena kita tau itu sebagai sub unit kerja, sulit, kita mengajukan ke direktorat, nah disana tergantung dari kebiajkan kepala unti kerja ini, ya mungkin di potong berapa persen di bayarkannya, mau sampe mana gitu kan, tapi kalau kita status cukup besar dengan satuan ini, kita dapat anggaran langsung, anggaran langsung ini bisa kita lihat sesuai dengan kebutuhan kita, kita bisa mempunyai dipa sendiri tapi tergantung dari dipa unit kerja yang juga bergantung dari unit satuan kerja mungkin kalau dia densus punya satuan unit kerja sendiri walaupun dia unit satuan kerja dari bareskrim mungkin itu lebih baik karena harus mengajukan anggaran atau dana tersendiri dan yang kedua bicara kemampuan, saat ini saya setuju dengan pendapat pak parmin, kalau bicara kemampuan mungkin mencari orang yang mampu tidak terlalu sulit bagi saya di banding orang yang mau, mungkin seperti pengalaman bapak juga di polda metro jaya begitu kesatuan cyber crima di polda metro jaya di bentuk, kenapa saa di tempatkan disini, pertanyaan nya seperti itu

M oke, mungkin itu topik selanjutnya, ini menarik mungki9n ada tanggapan

R5 kita semua ini punya pendapat ada yang minta di kecilkan, di besarkan, nah menurut mas sama nggak, namanya organisasi itu pasti harus ada sumbernya, kalau kita bicara organisasi yang besar pasti ada sumber daya manusianya iya kan, termasuk anggarannya, alat-alatnya, matrialnya, kemudian yang berhubungan dengan system, itu semuanya harus jelas di besarkan, bagaimana ini tidak terlepas dari satu kebijakan, kita membutuhkan profesionalisme seseorang dari sumber dayanya, emang seseorang itu sangat trampil mempunyai kemampuan dan mempunyai knowledge iya kan, ini memang orang profesional, tapi kalau kita mendefinisikan lebih banyak orang profesional akan lebih rusak atau lebih banyak orang profesional akan lebih baik, kita harus pertimbangkan, kalau lebih banyak, harus di pertimbangkan masalah cost nah kalau Cuma sedikit, ini sangat berkaitan dengan masalah, saya sebut aja, ini dalam tubuh organisasi kita sebetulnya, memang anggaran berbasis kerja dan saat ini juga boleh di katakan tindakan-tindakan yang dengan berdiri sendiri, kemudian kejahatan cyber itu memiliki suatu anggaran yang berda, ada anggaran-anggaran terentu yang beda, karena tingkatannya jadi kalau menurut saya kedepannya kalau memang berqualified besar, besar dan bagus, itu lebih baik di bandingkan dengan sedikit, yang sedikit nanti akan timbul pendiskriminasian dan lain sebagainya, ada berbagai kepentingan tapi kalau banyak, oh kita bisa lolos kita ganti yang lain, dalam satu organisasi itu harus kesana

R2 perlu di garisbawahi mas, pembesar ini jangan sampe instant, beda dengan kalau kita ke mak erot, tapi natural. Karena tuntutan dari pekerjaan, tuntutan dari ancaman memang saatnya harus di usahakan

R5 ya tadi di sebutkan tenaganya 20 orang, untuk 1 unit itu paling tidak 30 orang terus yang timbul kalau semuanya meminta kita minta bantuan extra tenaga khusus, ini salah satu cara untuk mengantisipasi, dan sampai detik inipun tidak perlu di besarkan kenapa harus di anggarkan untuk membentuk satu penyidikan tujuannya demikian, mungkin reformasinya kita mulai level middle ya, di mabes, yang nantinya bisa memberikan di bidang teknis, operasional yang punya kemampuan lebih di bandingkan dengan yang ada di wilayah

R7 ini baru kok, belum

M saya dari tadi liat bu jumaro mencatat terus, ibu gimana bu

R10 di samping saya baru disini, namun pengalaman saya, dari bentuknya menurut pendapat saya cenderung untuk di besarkan sebagai contoh emang terus terang saya awam dengan teknologi, berjalanya waktu, tentu dengan bantuan rekan-rekan yang lebih senior, sedikit demi sedikit kami, kami tau internet sebagian kecil saya pikir selangkah bisa yang tadinya, kasarnya belum bisa apa itu tau internet, saya berfikir, betapa banyaknya istilahnya hal-hal yang tadi sudah di katakan kemajuan teknologi, ada sisi positif tentu sisi lain ada sisi negatifnya, kalau kita liat itu banyak gantinya itu, namun, kita ini kok kayaknya kecil sekali, contohkan saja, pak petrus "coba ini patroli cyber", setelah mendalami kok banyak sekali hal-hal yang didapat mengarah kepada kejahatan teknologoi, nah disitu dengan orang sedikit ini apa mungkin mengcover yang segitu luas apalagi dengan dunia maya ini sangat luas, dengan orang yang sedikit, menurut pendapat saya justru setuju sekali kalau unit cyber crime ini di perbesar

R1 saya tambahkan karena unttuk menetapkan traget operasi, yang paling banyai cyber data ini paling banyak bertebaran, jadi kejahatan demikian bisa di dapatkan oleh polri, itu yang sudah terjadi dan korban sudah ada, yang kedua adalah inisiatif polri, banyak bertebaran penjahat ini di dunia maya, penjahat ini bsia mencari korban, jadi sebelum terjadi korban kita ini, seolah kita ini yang jadi korban

R4 berarti mencari jadi ada 2 hal, kenapa perlunya di perbesar ini mas. tidak akan tertangani mas

M satu hal yang menarik sebelum diskusi ini saya dapat sedikit bahan untuk diskusi ini, dari yang saya lihat ini, yang berada di unit kan kan tidak Cuma bapak-bapak yang berada disini, mungkin ada yang membedakan entah posisi, entah pangkat, entah bagian, entah pengalaman, kalau menuurt saudara-saudara yang ada disini, sepenting apa peran-pernah anda dalam organisasi kita, peran yang di ambil dan bagaimana peran anda dalam organisasi ini

R4 peran kita udah jelas, kita kembali gengan tugas itu, tugas kita apa sih, dengan tugas itu, kan kanit langsung wakil kanit ya, kalau menurut kami ya, kalau masalah pangkat itu sama dengan mahkota, tujuanya satu kanit, semuanya sama, mau pangkatnya kpp, poco, sama kecuali kalau ada pengecualian dari kanit itu sebagai mandat baru di tunjuk kanit, sebenernya tugas ini sudah paham semua ya, tergantung kasus yang di tangani, nantikan ada pembagian tugas, sehingga semua yang di cyber crime ini tidak akan nganggur, nanti ada masing-masing ada, ada kanitnya,

ada masalah pendidikannya, ada yang ngurus masalah unitnya itu adalah, jadi kanit itu membagi tugas

M itu sebagai segi formal ya

R4 ya

M tapi bagaimana anda sendiri memandang posisi anda dalam unit ini nih

R8 saya rasa kita ini tembok lah kita ini kan bagian dari sebuah unit kerja kalau yang bisa merasakan kepentingan kan bukan kita sendiri oficcial atau rekan-rekan kita

M nah ini menarik jadi yang menilai peran-peran anda ya mungkin

R3 kalau saya melihatnya peran kita masing-masing itu saya melihatnya sebagai tubuh manusia , ada sebagai tangan, sebagai kaki, mata dan sebagainya, jadi 99% ini bisa beranggapan sebagai tangan, oh kawan kita yang satu lagi sebagai kakinya, oh ya, supaya manusia ini utuh sebagai manusia dia bisa beraktifitas itu yang pertama, yang kedua sebelum kita melihat yang itu kita melhatnya memandang dari masalah fungsional dan struktural, kalau struktural kita sama, apa namanya penyidik, formalitas ya, tapi sebagai fungsional kita semua adalah penyidik kecuali mas idang ini ada kelebihan, karena saking ini punya kelebihan di bidang forensik, itu 2, lalu yang terakhir kalau kita lihat dari peranan masing-masing sama seperti tadi di sampaikan kita semua memeriksa oh bagian kasus ini banyak rekan tim ini masuknya kelompok itu , ini kelompok ini, tapi semua itu harus sinergy, nggak bisa ibaratnya menangani satu kasus kelompok itu, setidaknya ada input atau saran rekan-rekan yang lain, karena kalau seperti ini istilahnya udah mumet

R7 pertanyaannya sebenernya sederhana dari anda semua apa perannya, kalau saya tidak sependapat ya, bagaimana kita meberikan kontribusi gitu kan

M oke, kalau kita berandai-andai ini satu organisasi tapi dalam satu organisasi tentunya ada pendapat pribadi ya, dalam satu organiasi kan banyak orang yang terlibat, dan mungkin punya pengalaman, bahkan jenjang, predikan apapun ya, yang berbeda, terus bagaimana yang terlibat dalam organisasi ini mengambil peran

R4 berarti mas tanya dinamikanya kan

M iya

R6 penyidik sama kanit itu harus bisa kemampuan penyidik semuanya

M pertanyaan saya sebenernya gini nah sekarang yang tadi di jelaskannoleh pake edi adalah struktur yang sudah ada yang saya tanyakan adalah pendapat temen-temen disini tentang struktur itu

R8 saya ingin memberikan pendapat saya, seperti yang dikatakan tadi semua anggota punya kedudukan yang sama karena semuanya friend sejauh ini menurut riset kita, apabila di berikan tugas dari kanit, semuanya berjalan, menurut saya walaupun itu semua berjalan fair perlu adanya pembagian kerja seperti yang tadi pakbagas bilang teamwork dan harus konsisten, harus ada pertanggung jawabannya , misalnya gini, saya bisa minta nulis nggak, mungkin tidak secara struktur di buat, ada tugas yang nangani LBD 2, biasanya yang di tunjuk sebagai yang tertua, itu yang tertua, anggaplah x disini, y disini, a b c, tapi a b c tidak jarang terlibat di lbd juga, nah yang terlibat dibawahnya ini, biasanya kan disini, yang terua pak bagas dan pak edi gitukan, yang dibawahnya ini disiplinya pak edi ada,

pak bagas ada, biasanya kita melihat mana yang menguntungkan, karena kadang bapak bagas lebih mudah, semuanya kari kesini, kanit menanyakan gimana perkembangan kasusnya, "wah saya masih bantuin pak bagas" menurut saya, yang di hasilkan lba dia tidak sebanding lagi dengan lbd, walaupun lbc di masukan ke dalam yang menangani lpa, jadi kita ada pertanggung jawaban dari pelaksana kepada kordinator pelaksana, semua sama, jadi sifatnya sebagai teamwork itu menurut saya, harusnya seperti itu, jadi tidak ada lagi tim c, adalagi nama z, nah kalau disini a b c, kalau udah menangani judi, wah lebih enak, lebih enak korbannya

All he he he he

R8 nah yang disini bingung, lo saya kok nggak di ajak

R5 tapi dalam organisasi sekecil apapun itu harus ada yang namanya leader, kalau tidak ada, Kita tidak akan bisa melaksanakan tugas-tugas itu, itu emang dalam satu organisasi kenapa di polri ada pangkat dan sebagainya, emang itu adalah salah satu itu sudah terbentuk yang demikian, kalau semuanya sudah punya kemampuan, semuanya bisa dan tanggung jawab mereka semuanya penyidik, kalau toh itu ada cas kecil itu akan di bentuk satu tembok untuk memecahkan itu, kalau semuanya tidak merasa ada leader atau siapa yang minta di sebutkan sebagai anatomi, ini tidak akan menjadi tujuan apa yang kita harapkan, nah itu jelas, saya rasa leader itu perlu disitu, tapi didalam unit, emang leadernya adalah satu unit di bawahnya staf, kalau semua itu udah ada pembagian tugas, tugasnya apa bertanggung jawab kepada siapa, harusnya itu jelas, tidak bisa bahwasannya, nanti ikut ini, saya nanti ikut ini, walaupun itu tembok, yang relatif sangat kecil di bentuk, ada 3 orang atau 4 orang, siapa yang di eladerkan di situ dengan maksud apa, untuk mengkordinasi bukan berarti leadernya paling hebat, tidak, hanya untuk mengkordinasikan, apa yang telah di capai oleh team ini

M iya iya

R5 kalau itu semua nya rata masing-masing, ini tidak akan tercapai, tentunya ada ka unit, jenjang ini lah yang membuat suatu sistim ini bisa berjalan, ada leadernya, tadi yang di sebut oleh pak dicky walaupun itu suatu cara peraturannya memang aa keuntungan dan kerugian, keuntungan dimana, kerugian dimana, yang kita harapkan semuanya bisa menguasai dan bisa tapi ada case case tertentu yang tidak bisa di tangani seorang butuh pengaturan beberapa orang, terus ada membutuhkan dari ke ahlian yang lain sebagai contoh dari apa unit lodrom yang ada di dalam sini, saling mendukung dalam tim ini

R9 ada teori begini, ada yang memberikan proses ada yang mebmerikan hasil ada yang bilang prosesnya nggak perlu yang penting hasilnya, ada yang bilang hasil nggak perlu yang penting prosesnya

All he he he he

M tapi ada satu hal yang menarik buat saya, di dalam lingkungan ini adalah ada pamen pamen perwira menengah, disini juga ada pa bagaimana anda melhat fungsinya si pama ini, dan bagaimana anda melihat peran anda di dalam organisasi ini, apa istimewanya kalau ada pam, pamen dalam organisasi seperti ini, masih berlalu nggak, kalau ngak berlaku kenapa,

kalau masih berlaku kenapa apa yanga terjadi itusih sebenernya pertanyaan saya

R5 ada bebrapa yang berlaku sesuai tingkat kemampuan, dan tingkat kepangkatan yang di miliki, memang ada yang memiliki kemampuan di atas tapi ada beberapa hal yang tidak bisa di lakukankan, jadi kalau pamen memerintah itu tidak berjalan karena yang ada kultur budaya itu sendiri demikian

M oke

R7 saya melihat begini bahwa seorang menjadi pamen dia tetep pamen, pamen itu adalah menunjukan kemampuan yang di tunjuk, jangan mentang-mentang jaid pamen, lalu yang pama, masalahnya adalah kualitas tetep dijaga nah bicara kualitas waktu dia pama bagaimana dia jadi pama, nah yang terjadi di polri adalah seeorang pemimpin yang tidak kredibel bagimana dia bisa mengintruksikan perintah, karena dia sendiri tidak mengerti, ini terjadi, karenamerintah yang salah, sementara di level bawah pamenya sudah berfikir jauh

M iya

R7 tapi sebuah organisasi yang bagus cyber crime bagaiman jadinya kalau di pimpin oleh orang yang sumir, susah, saya melihat begini pangkat di tetep di perlukan tapi harus di berangi dengan kemampuan

M ini menarik nih

R4 in out nya he he he

M ini masalah mungkin bukan Cuma di polri aja mungkin di tempat lain juga banyak, mungkin di tempat saya juga bisa ya

R5 emang idealnya demikian proses pelevelan dari bintara, tantama, pame pamen dan jendral semuanya melewati proses ini dan mereka harus melewati jenjang ini, kalau kita meberikan contoh, for example kalau di institusi lain, kepentingan politik di taro orang nya nah ini akan menungganng sebuah organisasi, tapi kalau organisasi yang bener-bener ideal, orang meniti karir dari bawah, jadi pada saat dia dia tas top manejer, dia punya kemampuan yang di milki, namun hars di berangein denga style , itu mereka udah bisa menggerakan namun kemampuan ini style orang berbeda, gaya kepemimpinan akan berbeda, ada yang pemimpin pasif ada yang aktif, itu akan berpengaruh kebawah

M oke

R2 saya melihatnya, dari tadi informasi kita ini sangat menarik untuk mas, menarik semua, kalau saya melihatnya ada fungsi dari pimpinan, bahwa itu di besakan antara lain di lapis-lapis kemampuan, di tingkat bareskrim, tingkap polda nah kalau berkaitan dengan pangkat saya rasa itu udah ada semacam ketentuan, mungkin orang awam tidak tau, kita udah ada semacam rule of the game, lapis-lapis kemampuan, pangkat ini demikian, pangkat ini demikian, dan kemampuan seseorang ini bukan aksi ke pangkat dan itu memang berindikasi dengan responbility atau tanggung jawab yang bersangkutan dan kemampuan sesorang itu bukan hanya perpatokan ke pangkat tapi kepada dirinya sendiri sama dengan pak edi tadi kalau misalnya pamaya maih kompol tapi kemampuannya luar biasa berarti selevel dangan akbp, tapi beda sedikit lah dengan pemikiran, tapi karena di batasi dengan pangkatnya yang kompol itu

M oke, yang lain pendapatnya sama nggak, apakah jejakl lapis kemampuan yang berkaitan dengan jenjang kepangkatan artinya bisa saja kan yang
R2 itu bisa terjadi dimana-mana mas tidak hanya di polri
M ini saya tertarik, ini emang di polri sedangkan yang saya tau, yang namanya entah polisi, saya nggak terlalu jauh dengan militer ada jenjang pangkat yang menunjukan perbedaan posisi, pertanyaan saya apa sih yang membedakan pama dengan pame, ini secara pribadi ya, emang punya tanggung jawab yang lebih
R7 iya
M kenapa?
R7 ini pertanyaannya secara umum atau
M saya bertanya itu untuk semuanya
R4 bedanya dikit, seharusnya seorang pamen itu mempunyai tanggung jawab yanga lebih tinggi daripada pama, idealnya seperti itu
R7 sesuai gaji pokok he he he
R4 responsibilitynya emang harus beda, yang pertama kanit seorang pamem ini dalam struktur tugas penyidik gitukan, beda jabatan sehingga tujuan yang akan di capai ini berhasil, pamen itu harus bagaimana, seperti tadi umpamanya kemampuan yang di miliki itu harus di gunakan, supaya berjalan dengan baik, tadikana da sekolah tuh, ada SP, SH, SIK, SMI, itukan masing-masing develope

KASET 2 SIDE A

R3 nah itu namanya satu tim saja, pendidik ini, pendidik tua, pendidik muda, itu semua adalah pendidik, kenapa dalam satu tim, ada pamen, ada sersan, ada kopral, kenapa itu harus ada, supaya adanya senergi dalam satu tim ada yang di perintah ada yang memerintah, apa pun semua siap, itu namamnya pamen, tapi sekarang ini adalah era globalisasi, antara pama, pane , kopral sersan, atau disini tidak ada yang top, dia punya kesempatan kah
R4 he he he he
R3 itu mau dokter, atau SMP itu beda tipis saja kalau kita nggak liat dari kepangkatan, itu di biarkan saja, di sini nggak ada yang paling pinter, masalahnya dia punya kesempatan
all ha ha ha
R3 sekarang kembali pada itu saja, kenapa harus ada pemimpin supaya ada sinergi supaya program itu berjalan dengan baik, kalau semuanya memerintah nggak akan berjalan, kalau pamen perintahnya nggak jelas pam juga akan bingung, memang jadi pamen itu berat, karena orang menilai, orang yang sudah pamen, itu melalui secapa, selapa, semua itu di anggap nggak mampu, harus punya kemampuan yang lebih, tapi praktek di lapangan, orang yang sudah supati aja, di lemhanas masih banyak yang komplain pak, karena itu punya kemampuan, kesempatannya kurang, di tempatkan tidak sesuai
R7 keinginan
R3 sesuai dengan skillnya makanya kalau bapak pernah ke negara luar luar lah, contohnya eropa, jerman, saya pernah di sana 2 tahun, bukan polisi aja, orang yang mempunyai pekerjaan yang profesional, orang yang pinter,

kerjananya berhasil harus profesional dulu, menguasai, kalau udah profesional itu jangan di pindah-pindah, contohnya itu, di jerman itu orang yang dari awal jadi guru itu sampe pensiun kalau mau profesional, orang harus dididik dan di kerjakan, kalau dia ahli sidik, sidik aja, oke, kalau dalam skop yang lebih luas, emang walaupun belum punya jabatan yang strategis di sini ada masih ada nama yang lain, kayak polisi nilang 10 ribu ketauan, langsung di pindah pak, di brimob kan nggak nyambung, jadi kalau mau profesional, orang di didikdi kerjakan dalam bidang itu, contohnya pak idang di forensik nanti sampe pensiun tetep forensik jangan di pindah-pindah tapi jenjangnya jelas, dari akbp, kombes sampe bintang 1

R7 tapi disini nggak bisa

R3 disini masih ada like and dislike

R7 itu bedanya

R3 intinya pamen pama secara ini nggak ada beda, tetapi secara struktural management harus beda, supaya ada yang di perintah dan memerintah

R4 ada yang bertangung jawab

R3 jadi yang utama itu perbedaannya jelas beda

R3 udah tanggung jawab salah wah, jadi jelas kalau pamen itu lebih banyak ada

All he he he he

M kalau kita memang dalam posisi yang beda ada pama dan pamen seharusnya apa yang di dapat beda

R1 sesuai tangung jawabnya

M sesuai tanggung jawabnya oke, pamen harus lebih besar dari pama tanggung jawabnya

R4 rejekinya juga

M rejekinya juga harus gitu, yang terjadi dalam unit ini, yang saya sempet denger adalah, ada saat-saat dimana, katanya yang saya tahu pankat itu di lupakan

R5 sama-sama penyidik, nah itu di harapkan kita semua bisa bekn semuanya untuk bekerja, sesuai kapasitas tim

R8 kenyataannya seperti ini mas saya bukannya merendahkan ya, pertama kali saya masuk ke cyer crime, itu nggak jelas pekerjaannya

M ini menarik, sebelumnya, nanti saya akan tanyakan itu, sebelumnya sebenernya apa sih yang penting dalam hubungan atasan dan bawahan

R3 maksudnya dalam suatu proses kerja

M iya

R7 yang penting adalah satu, kesamaan persepsi untuk tugas itu menjadi berhasil, dalam konteks tertentu terjadi pembedeaan, di mana yang di bawah di bungkam tidak boleh berpendapat, yang pokoknya begitu gitu loh, di mana seorang pamen di perlakukan pimpinan seperti itu jangan harap tugasnya berhasil di yang paling penting adalah kesamaan persepsinya agar tugasnya berhasil

M yang lain ?

R3 mungkin persamaan kesempatan, persamaan persepsi tapi tidak mempengaruhi kesempatan yang ada, ya sami mawon

M kenapa

R7 menurut saya penting, bicara kesempatan membutuhkan kesempatan yang sama, Cuma bagaimana mengimpelementasikan kesempatan yang ada, kalau kesempatan itu tidak di gunakan semaksimal mungkin jangan harap kesempatan itu datang dua kali biasanya di cut

M oke, tapi persamaan persepsi kenapa itu penting

R5 seorang pimpinan seorang manager dalam menggerakkan beberapa orang persamaan persepsi untuk mencari suatu tujuan, tentunya yang pertama adalah kesempatan, penyamaan persepesi untuk mencapai tujuan, apa tujuannya, nah baru mebedakan tugas seusai dengan profile masing-masing dari yang ada, kalau semuanya mampu saya kira suatu kemimpinan, leader tidak akan sulit, tapi tetep harus ada pembagian tugas, karena tidak ada pekerjaan yang tidak di bagi-bagi, mesti ada pembagian, supaya semuanya ada suatu pemerataan semua merasakan pekerjaan, tujuan yang sama goalnya, tujuannya ini lih, goalnya ini loh

M bukannya si atasan itu juga berasal darai bawah dia sudah mempunyai pengalaman yang banyak sudah tertempa berbagai ini

R8 sebenernya gini, kita mau liat tugasnya seperti apa, kita ngomongnya a, ternyata b, kita butuh kalau yang a yang a, itu sesuai dengan omongannya, selama ini di cyber crime saya lupa loh, tapi sejak pak petrus saya di pacu, kamu harus bisa harus bisa, di pacu di pacu, nanti semua di samakan dulu, jadi di samping persamaan persepsi juga, ada persamaan rasa juga, akhirnya ada temen yang ketinggalan jangan di diemin aja, nah ini tugasnya pamen

R3 kalau ada kesempatan, anggaran juga ada, itu salah satu ya, misalnya seperti yang kita alami, katakan lah ada patroli cyber ada temuan ini, temuan itu, birokrasi muter-muter akhirnya nggak jalan, akhirnya kita cari jalan lagi, memang harus ada semacam produksi yang tepat dan benar supaya kita punya kesamaan persepsi untuk pekerjaan kita, tugas kita ke depan adalah begini kemudian ada kesempatan yang sama, tim ini menangani ini, tim yang lain menanggani yang lain, tapi di dukung juga sarana yang memadai, termasuk anggaran

M oke, nanti saya akan bertanya anggaran kalau misalkan saya ambil posisi sebagai orang yang sangat mengamini yang namanya hirakiis, tolong kalau pada beberapa saat, sinergi kan harus menghimpun dalam satu kesatuan ya, kenapa saya perlu menyatukan persepsi saya, kenapa saya tidak bisa bilang pokoknya begini karena saya sudah punya banyak orang, saya sudah banyak tempat, saya sudah punya tempat lapis yang lebih tinggi, kenapa harus sinergi

R4 ya memang, gimana supaya kebijakan ini bisa di sinergi, berarti harus ada perubahan juga, saya maunya begini, tapi harus menggali juga juga begini

M oke

R6 nanti dia jadi kerdil, semuanya nggak ada pengembangan apa-apa, kalau pemimpinnya otoriter, pokoke pokoke bawahannya itu kan, itu gak bisa kan

M didalam unit nggak bisa seperti itu

R3 bisa terjadi

R7 kejadiannya seperti itu mas tadi pak edi bilang kemampuan rata-rata kalau di bilang orang yang mandiri, mengawasi, dengan kemampuan orang rata-

rata yang sama, terlepas dari kejengjang pangkatnya, kita kan sekrang seperti sub versi apa, sub versi apagitu kan, jadi saya mau seperti ini saya kerjakan itu, nggak cuma seperti itu karena seperti ini tidak bisa di tetapkan seperti itu,karena pekerjaan ini dinamis, nah di sini perlunya amademen, "menurut kamu bagaimana", "menurut kamu bagaiman", "oke kita bandingan", ini sudah terjadi di sebagian besar memang ada yang ketinggalan, kembali lagi sejauh mana dia mau

M kenapa hal itu penting dalam unit ini saling dengar

R5 ya maksudnya untuk, saling mendengar, ini hubungan antara bawahan dengan atasannya, secara kemapuan yang atas sampai yang bawah, nah ini kan oragnanisasi ya, untuk mencapai suatu tujuan dalam menggerakan beberapa orang yang notabene orang ini mempunya kemampuan Style yang berbeda, iya kan, personalnya juga berbeda, nah mungkin ini akan di satukan dalam suatu tujuan, nah seorang leader disini sudah punya kemampuan gimana membagi-bagiakan tugas, sehingga apa yang di kehendaki seorang leader akan tecapai tujuan itu akan tercapai, porsi-porsi ini yang bisa melakukan adalah pimpinan yang ada disini, kalau tadi orangnya nggak punya kapabel, nggak punya kemampuan nanti pembagiannya akan salah dan tidak aken sampai pada tujuan yang di harapkan, kalau hubungan erat sama pimpinan memang bagus, kemudian mengetahui bagaimana sikonnya, kemudian yang kedua dia mengetahui kemampuan dari pada itu, kemudian mereka juga dalam menjalankan mendengar apa yang akan di sampaikan, jadi semuanya harus terakumulasi, supaya akan berjalan organisasi ini dalam sub unit kecil ya, itu akan terealisasi juga itu akan tercapai apa yang di kehendaki

M kenapa saya mepertanyakan ini, sebetulnya ini berjalan sistem yang di namis, dari bawah laporan dari atas perintah, selama ini jalannya lancar-lancar aja, apa lagi polri sekarang semakin besar setelah pisah dengan tni, semakin besar pengaruhnya. Semakin signifikasi semakin besar buat masyarakat , jadi berjalan dengan di namis tadi, katakanlah sangat minim sekarang ini di butuhkan sinergi atasan dengan bawahan, tapi yang saya tahu nggak seperti itu seluruhnya, semua sejsjar bisa saling diskusi jadi kenapa pertanyaan saya seperti itu

R2 karena sebenernya yang terbaik itu kita bisa menyatukan top ground sama low bup nya satu, kalau hanya dengan top ground itu kita seakan mematikan inspirasi, aspirasi maupun wacana dari bawah, up down, pokoke, pokoke, kalau top ground, tapi kalau buter up , intinya info dari bawah itu, conformise itu tujuan utama kita, karena masing-masing satu yang harus kita yakinin masing-masing mempunyai kekurangan dan kelemahan, justru dengan kelamahan ini kita mampu memajukan untuk menjadi yang tekuat

M saya usul Sambil makan aja ya gimana

R3 usul mas nasi padang

All he he he

M kira-kira di ambil dulu aja

R4 makan nggak apa-apa

M nggak apa-apa

R7 satu hal ya, pembicaraan kita menjadi tidak terarah satu belum tejawab, kayak jaka sembung bawa golok, kita kebanyakan muter-muter tujuan akhir belum tercapai, kalau berdebat terus menerus
M oke
R3 berhenti dulu supaya fresh
All he he he
(break makan siang)
R7 sudah tuntutan zaman kejahatan tidak bisa di atasi
R3 kita kerja untuk cari gaji ya
R3 di brimob oke lah, gaji 3 juga oke, sduah di hiting, transport sekian, ini sekian
R3 kalau di luar itu sejahtera, kalau disini kesejahteraan tergantung pada jabatan
R6 ada yang basah ada yang kering ya
R7 jadi polisi aja udah sejahtera kita
R8 emang pak zamri mau makan seperti itu aja, nggak kan
R7 dari tadi bapak tidak banyak omong ya, takut kepancing
R5 orang profesional itu cocok di terapkan di negara orang aja, di indonesia nggak
R7 mungkin nggak orang tidak memberi tapi bisa menerima
R8 berarti kalau ini bicara polisi profesional berarti kita bodoh ya mau terima, oke, saya sidik, berapa lo berani gitu kan
R7 itu yang terjaid pak
R6 berarti litbang bikin buku tentang profesional salah dong
R7 saya dulu protes ada pelajaran profesional ya, gimana kalau jadi profesional, setia sama negara dan piinpinan, kalau pimpinannya salah gimana, aku di musuhin sekelas" huuuuuu' kalau pimpinan salah masa harus setia
R8 profesional itu kalau ada job duluan di bayar
R3 di luar itu gajinya itu 40 juta pak, itu nggak cukup
R8 kalau di indonesia yang gaji itu 3 juga tapi pengeluarannya 4 juta
R6 he he he
R5 gaji 3 juta tapi punya villa
R3 karena kita profesional kita banyak bantu orang jadi kita di bayar
R2 di belakang sini ada yang nunguin kita ya
R7 kita udah selesai kok, dulu waktu bapak ikut pendidikan di sumpah nggak
R8 semuanya dari sumpah
R9 ya ikutin kata hati aja
R3 saya ingin memanasi suasana di sini, kalau pemimpin tertinggal, gimana mau bener
R2 termasuk pemberian gaji, profesional juga anggarannya
R5 berbicara profesional, itulah yang amatir, itulah bodoh-bodohnya pejabat kita, dia ngomong setelah proporsional-proporsional, goblok kalau dia bilang begitu, kenapa, kalau namanya proporsional itu namanya bayaran, dia bisa aja atas kemampuan dia

KASET 2 SIDE B

M oke, saya teruskan

R7 mas sorry, teknis mas berpatokan pada waktu atau pertanyaan yang di ajukan
M saya berpatokan dengan pertanyaan yang di ajukan
R7 nah kalau mas liat pembicaraan sudah tidak sesuai dengan konteksnya mas cut, jadi nggak ada istilah, "jangan motong dulu", nggak ada harus sesuai dengan konteks loh
R3 ini berapa lama lagi
M 2 ,5 jam tapi tadi ada yang cukup menarik
R3 nggak apa-apa saya suka
R4 he he he he
R7 kalau boleh begini mas, mas seperti najwa sihab
M oke, tadi saya agak ragu aja mau motong-motong
R6 deg degan gitu ya
R7 nggak masalah mas
All he he he he
R6 yang nggak suka di potong pak idang, dia marah
M sekarang sambil makan aja ya
R7 nggak masalah
M oke, nah yang bertugas di sini kan macam-macam ya masa tugasnya, bisa tau nggak, tau kapan ada unit ini
R7 ya dari pertama kali tau, di kasih tau ke suluruh khalayak polisi bahwa ada satuan unit cyber crime
R8 buat kita atau buat polri yang lainnya
M buat temen-temen yang ada di sini
R7 oh nggak tau
M siapa tau pas masuk ke sini sudah tau
R8 pada saat saya masuk ke siru baru saya tau
R7 saya kan ikut ke polda, terus ke staf yang lain, terus tiba-tiba di likuidasi ya, membutuhkan unit satuan kerja, saat itu ya sata tau, jadi sebelumnya tau, dan saya rasa seluruh anggota sama rata kalau unit itu didirikan
M waktu tau ada unit ini, seperti apa sih sistemnya
R8 saya ya, kalau saya orang-orang yang terbuang, yang nggak qualified nggak punya kemampuan masuk situ, dulu ya waktu di polda kecuali kayak om dicky, berdasarkan kemampuan yang di milki
M yang lain gimana pendapatnya sama
R3 saya kan yang awal-awal, karena masih baru
R7 pak surawan mungkin punya pengalaman bagus karena dia merasa kebuang
M oke, perasaannya gimana
R8 kalau saya pertama masuk situ, saya mikir mau ngapain tuh, lulus pptik, lulus abis ikut pendidikan, di bareskirim saya masuk ke cyber crime anggotanya Cuma 5, komputer aja pentium dua waktu itu, apa lagi internet ngak ada, pake telpon gantian, saya kasus pidana kenapa di kasih di situ
M nah ini menarik
R8 kalau sekarang saya merasa, karena pada saat itu saya melihat saya ada disini saya tidak ngerti apa pun juga, saya tidak dapat apa-apa karena kesejahteraan polisi tergantung pada jabatan, jabatan bagus pokoknya sejahtera aja, meskipun waktu itu makan siang aja susah, tapi masa sih

nggak ada yag saya dapetdari situ, saya mulai belajar, belajar mencoba mencari tau, apa sih cyber crime apa aja sih yang di tangani, saya belajar, saya bukan belajar dari polisi karena polisi nggak ada yang ngerti, saya belajar dari dari teman-teman saya yang mengerti komputer dan lain sebagainya, semakin lama saya di nikmati, ketika di tanya sama mau milih mana saya pilih cyber crime, di situlah saya mengerti, kalau di tanya mau pindah ke mana, saya mau pindah ke wilayah, saya akan dari awal, karena saya sudah punya kemampuan yang lebih , kalau saya di tanya"kau mau pindah kemana, ya pindah ke wilayah karena saya sudah 5 tahun lebih di cyber crime ini

R7 bapak tadikan kecewa

M sebentar ibu dulu

R6 pertama saya di tempatin di cyber crime, saya mikir email, apa ya itu, begitu saya masuk kok seperti mainan time zone, saya nggak ngerti, setiap datang pagi saya buka game, akhirnya saya beli buku, saya coba belajar sendiri tapi nggak ada yang arahkan, bertanya susah tidak ada jawaban, nah itu begitu saya masuk pimpinan baru, bukan saya cari muka, kita di paksa untuk, apa sih cyber, di trainingin, awalnya saya pikir seperti tempat bermain

M waktu pertama kali di pindah kesitu perasananya gimana

R6 karena kebetulan saya sudah 8 tahun saya ingin punya ilmu yang lain

M minta di tempatkan

R6 kita di isi angket, mau pindah kemana, permintaan pertama saya mau pindah ke penilihan pertama infomikom, tapi ternyata saya di tempatkan di cyber crime

R7 pak surawan punya pengalaman bagus pak

R4 nanti jatahnya di bagi 2 sama pak zamri, karena dia jadi moderator juga

All he he he he

M oke, gimana mas, ibu jumaro

R10 memang awalnya kita di wilayah karena kekurangan yang promosi jabatan sangat penuh, terus memang di tawarkan siapa yang mau pindah keluar dari sini, termasuk salah satunya ada di mabes, berdasarkan itu saya juga mendaftarkan diri untuk pindah ke mabes ternyata di sana dari mabes memang ada bedanya, sehinga saya masuk ke mabes, awal masuk saya memang kaget sekali, dalam artian apa yang harus saya kerjakan, sementara begitu di diwilyah sangat sekali kita kekurangan waktu, kok disini saya plonga plongo lah istilahnya, kalau ada patroli cyber saya juga buka internet terus terang aja

M perasaannya waktu kesempatan itu gimana, itu kemajuan karir atau penghambatan karir

R sola kemajuan karir atau penghambat karir kita nggak berpikir ke sana, kalau di mabes itu peluang karir ada untuk belajar nggak ada, dari saya piket dari pagi sampai sore sangat jenuh sekali menunggu waktu, sampai saya pikir kesan di wilayah itu, sangat sibuk kok disini terus terang bingung apa yang harus saya lakukan, lalu saya mencoba menyesuaikan diri

M ada nggak keraguan-keraguan, itu posisi yang sekarang nggak enak, katakanlah buat kesejahteraannya jelas, dulu saya pernah ngbrol sama

saya, posisi yang sekarang ngak enak, dulu dia di bagian logistik, katakan buat kesehateran jelas, nggak penting pangkat, yang penting bagian saya tetep disini, itukan bukan Cuma polri, yang penting saya juga di bagian ini, di perusahaan saya yakin, nah iut gimana

R9 kalau secara formal, memang cyber crime pada umumnya itu sama struktural sama fungsional, misalnya atpol atau apa ada jenjang pendidikan yang harus di tempuh, misalnya kalau untuk penerimaan polsek dia haruis lulusan apa, pselapa, secapa, gradenya kalau mau jaid wakapolres, harus ke ptika itu yang struktural ya, tapi kalau dalam fungsional itu harus berdasarkan daripada pengalaman, kemampuan dan jam terbangnya dia, itu fugsional kemudian ada juga hal yang sifatnya tergantung pendidikannya

M nah itu kalau kita bicara soal struktur ya, tapi ini bicara soal perasaan

R9 nah itu kan yang berlaku, ada yang kembali kepada kita sendiri, motivasi kita pada saat masuk polisi, terus terang aja umumnya dari dulu kurang profesional karena polisi hanya sebatas cari pekerjaan, kalau dulu zaman di bawahnya abri kalau dulu ada tes mental psikologi, lo kerja cair j\gaji ya, nggak, tapi itukan tidak di ungkapkan dalam tesnya kan gitu, tapi itu nggak di lupakan, yang penting gtw masuk dulu nih, pas masuk kok gini , itulah timbul kekecewaan-kekecewaan ini makanya itulah butuhnya seorang pemimpin untuk menampung rasa tadi

R7 kembali ke cyber crime berdiri pertamanya gimana

R9 pertama gini

All hc he he

R9 pertama saya nggak ngurus, saya nggak gnerti cber crime itu apa, saya tugasnya apa ya

R7 mas lulus tahun berapa

R9 2005

R7 harusnya udah denger

R7 denger tapi nggak tau tugasnya apa ya, saya masuk situ, kok begini, tiap pagi datang sore pulang, karena nggak jelas karena manegementnya nggak ada, udah kamu disini aja, santai disini aja,

M bagaimana hal yang terkait dengan masalah kesejahteraan, kalau saya kan pegawai swasta, saya gampang aja begitu di sini nggak sejahtera, kalau ada tawaran ya saya pindah, ada berapa kali tawaran belum naik, saya menolak, nggak mau

R9 nilai-nilai yang terkandung dalam budaya, ada sebuah perjuangan

R7 ini cerita idealnya atau faktanya nih

R9 kalau idealnya kayak gitu

R7 kalau saya tambahkan kalau saya merasa nyaman di sini saya punya uang sedikit, saya nggak pindah ke yang lain, idealnya, katakan pimpinannya bukan pak petrus ya, saya nggak akan berlama-lama, saya pake uang saya, saya akan pindah, cari yang basah lagi

M itukan bisa di lakukan

R7 idealnya

M kita nggak bicara yang ideal, kita bicara pribadi

R4 jangan terjebak kayak gini maksudnya kita kan dapet gaji tapi nggak cukup, Cuma hal ini jangan di jadikan suatu alasan yang mutlak, kita kan

indonesia, terus terang aja ya mas, banyak pemuda-pemuda gitu yang jadi polisi

R7 jangan munafik

R4 oh saya nggak munafik

M mas udah menikah

R4 udah

R7 pertanyaannya di rubah pak kalau nggak merasa nyaman disini apa yang bapak lakukan

M oke, kalau saya di kapolri saya kasih kebebasan kepada semua yang ada di sini, mau penempatan di mana, satu-satu aja

R7 pilih cyber nggak gitu

M terserah mau pilih cyber atau yang lain

R1 di laboratorium, emang dari dulu hobi saya, jadi tidak terpengaruh situasi yang anda

M kalau bapak

R2 kalau saya pilih cyber karena maunya yang mengembangkan karir untuk saya, kalau misalkan ada kesemoatan pengembangan saya mengikuti itu, kalau pimpinanan mempercayakan ke tempat yang lain kita ya loyalitas

M kalau saya kasih kebebasan untuk milih

R2 ini kan terkait dengan karir, tentu seuai dengan keinginan kita

R7 mau pindah kemana

R4 ada densus 88, pindad

R2 saya di eksus, pindad misalnya

R6 logistik gitu kan

M kalau bapak

R3 kalau saya, selama 27 tahun jadi polisi saya sudah dinas di narkoba, susila, curanmor, produksi dan perdagangan, kemudian di pendidikan 8 tahun, masuk lagi cyber, kalau menurut saya jadi kalau menurut saya di mana pun saya suka, dimana saya berdiri itulah bumi saya saya pasti berhasil, kita duduk, makan apa yang ada disitu, pasti berhasil

M semua suka di antara yang suka mana yang paling

R3 cyber, ya memang kalau menurut pendapat saya,saya sudah mulai tua he he he

All he he he

R3 di cyber kita nggak perlu tenaga, jadi ada pepatah yang mengatakan apa tuh saya lupa

All he he he

M sambil di inget pepatahnya ya pak, kalau pake edi

R4 sebelum saya mecoba berartikan saya butuh proses, dulu saya bertanya, apa cyber, kok begini, tapi sejak saya di warnai selama ini saya merasakan manfaatnya, sudah mulai menikmati seperti ini, karena saya masih enjoy, saya sudah merasakan manfaatnya ini saya tenang kalau dulu saya di tanya maunya provost sekarang nggak perlu

All he he he

R3 jadi cyber itu dengan semboyan itu smarter no harder

M oke, bapak

R5 kalau saya sih kita kembalikan pada semuanya, rasa itu tergantung pada manusianya masing-masing, tadi pak edi megatakan demikian, pak

surawan megatakn demikian, nah semua pembinaan itu tidak bisa menilai, ditanya atau tidak itu juga seharusnya bukan suatu pertanyaan, itu privasi, pada seseorang, dari sudut pandang mana kita mau, dari sutu pengetahuan oke kita mau, tapi dulu masuk situ kita bukan orang it kita bertanya-tanya apa yang membuat kita masuk situ, makanya tergantung leadernya, kalau leadernya tidak punya knowledge kita akan masuk jurang tapi kalau di bawa kita menuju untuk maju kita seneng, dengan adanya kita untuk maju, hal yang lain di perhatrikan itu manusiawi, siapa pun manusia, nah dengan dunia yang sekarang dengan adanya perhatian dari anggota, kemudian kebebasan untuk memperoleh pendidikan, dan sebagainya, orang masing-masing berbeda, tapi kalau misalnya pimpinan tidak meperhatikan sama sekali, loe jalan sendiri, o mau ini, ya mohon maaf, saya dari sana nggak dapat ongkos sama sekali, kalau di hitung matermatika gaji nggak akan cukup, kalau gaji 10 juta untuk 5 orang anak itu nggak akan cukup, dengan pola hidup yang berbeda memang kedudukan seseorang akan mengikuti, kalau sekarang enak, kalau dulu tidak jelas mau kemana, tidak bisa menetukan itu tegantung pada pimpinan, saya tidak bisa, oh saya harus begini

M pak bagas, yang saya tanyakan yang penting-penting saja, apa alasannya prosesnya kan

R5 saya tau jadi saya mengarahkan ke situ

M kalau ibu

R6 jadi saya di un 12 thn, saya sudah mendapat banyak dan saya sudah berbuat banyak, di seksi un, saya pikir sudah seimbang, saya di narkoba, saya mendapat ilmu baru tentang narkoba, 8 thn saya di sana, saya sduah berbuat, saya sudah dapat, saya selalu ingin hal-hal yang baru yang belum saya tahu kan, ternyata saya dapat di cyber crime , ya baru dan saya pikir masih baru sekali, saya sudah mendapat banyak tapi saya belum berbuat untuk cyber , saya pikir saya masih di cyber aja

R5 tapi kalau nanti pimpinanya lain gimana

All he he he he

R7 kalau saya nggak munafik ya, kalau saya bekerja menurut kata hati saya yang saya dapatkan, sepanjang saya dapat pimpinan yang nyaman, pimpinan mengakomodasi aspirasi saya, di sisi lain dapet tambahan lah ya, terus yang kedua saya melihat satu sisi ini dunia baru, meskipun bagi saya dunia baru ini sebagai pekerja organisasai yang dulu, terus terang kalau tidak dengan ke pemimpinan saat ini saya akan pindah, kenapa, saya liat pendidikan dari situ,cikal bakalnya disitu, maju nggak nya, sukses nggaknya sebuah organisasi itu kuncinya adalah pendidikan, jadi dengan kemampuan saya yang sempit ini, saya lebih menorehkan perbaikan meskipun kecil, karena saya merasa nyaman di salurkan di cyber crime saya tetep di cyber crime

M apa yang mebuat anda nyaman

R7 mungkin suasana kerja ya, suasana kerja di mana seorang pimpinan mau memberikan arahan, apa-apa yang mau kita pikirkan berbuat dia sudah terlebih dahulu menangkap, misalnya mau kemana kita, mau gimana kita, sebenernya mau tau hasil akhir yang maksimum, itu yang mebuat saya merasa nyaman

M apa artinya yang bisa nyaman itu pimpinanan

R7 kalau saya dominanan dia, karena apa saya suka mengekspresikan kemampuan kita

M masih ada dua lagi ya

R8 kalau menurut saya lebih nyaman di sekretari, masih banyak lagi hal-hal yang du laukan, karena masih banyak kasus baru

R9 kalau saya di tanya jujur saya mau pindah , karena saya dari pertama saya masuk, bukannya saya tidak berusaha untuk pindah, tetapi karena tidak di indahi he he he, kemudian masuklah kadit baru, ibarat kata kartini habis gelap terbitlah terang, di situ artinya apa yang saya sudah pupuslah untuk mendapatkan lebih, untuk berprestasi saja saya tidak bisa, kita di pacu, kamu mau buat apa saya siapkan, saya sudah merasa lengkap untuk probadi saya aja ya, walalupun du liat sebelah pihak, say juga termasuk tim tersebut, yang kedua yang saya katakna kenapa say mau pindah tentunya saya sudah 5 thn lebih, saya mau suasana baru selama sebagai kandit bukan permasalahan terlalu besar, tapi kalau di katakan keinginan saya ingin pindah, saya mau variasi dan nuansa lain

M apa istimewanya suasana baru sama variasi

R9 bagi saya hal tersebut berkaitan dengan pengalaman aja, seperti pendidikan yang kemarin, ketika orang membicarakn masalah hal polisi secara umum

KASET 3 SIDE A

R9 saya tidak begitu memahami karena saya membaca saja, tapi begitu mengaplikasikannya saya mencoba lebih memahami walaupun belum paham benar

M apa sih istimewanya kita bisa lebih paham tentang sesuatu yang baru yang lebih banyak pengalaman apa istimewanya

R9 ya seperti yang dikatakan tadi di polisi ini tidak seperti di tentara, kalau di tentara begitu dia masuk infantri begitu pensiun dia tetap jadi infantri, kalau dia masuk dari pelaut kalau udah pensiun dia tetap jadi pelaut tidak mungkin dia jadi mariner, begitu juga tapi beda dengan polisi sekarang saya masuk lalu lintas besok saya jadi serse seperti yang dikatakan juga waktu saya ngobrol dengan pak kanit, saatnya kita untuk mengembangkan diri, seperti yang saya katakan tadi tentunya kita mau masuk ke swasta yang lain dengan jabatan yang lain tentunya kita ada kesempatan walaupun itu belum pasti untuk mengembangkan diri, bahwa untuk revorwages semua itu sistemnya sama jadi untuk mengembangkan diri yang sifatnya manajerial dengan level pangkatan dengan hiraki tadi itu mungkin agak sulit, tapi aku bilang ya kesempatan diri untuk manajerial itu lebih terbuka

M kalau ibu

R1 itu kalau menurut saya, kata hati saya seperti kata pak zamri istilahnya ada kenyamanan disitukah saya akan betah disana, kalau disitu tidak nyaman bagaimana kita bekerja

M apa yang bikin ibu nyaman

R10 tentu yang bikin nyaman lingkungan, rekan kerja disini ya itu atasanya, istilahnya komunikasi ini, saling bekerja sama lah, tidak mengucilkan, membedakan dan sebagainya, kita akan nyaman, dan yang kedua nasib

juga, apa ya, masalah lalu di wiliyah, jauh kesibukan, sedangkan di wilayah itu jauh, sehingga apalagi mengingat usia saya masanya pensiun tentu kalau di tempat lain yang butuh kesibukan, jadi saya cenderung masih di cyber di samping itupun kita ke wilayah yang kita dapatkan, di cyber itu istilahnya kok nggak monoton , disitu informasi kita bisa masuk

M nah saya tertarik sama pendapatnya nih, kenyamanan, itu penting yang di tentukan, kalau misalnya berbeda dengan yang sekarang?

R9 sekaranng gini kehidupan resiko itu selalu ada, untuk pekerjaan saya saat ini nyaman kenapa, kesehateraan saya cukup, emang, untuk tindakan saya sekolah tercukup tapi saya harus berfikir, saya ingin seperti pak petrus yang bia memimpin angotanya membuat kenyaman,nah waktu saya bicara dengan beliau saatnya adalah untuk pengembangan diri karir kedepan, mengaplikasikan apa yang saya liat, ibaratnya oh kemimpinannya bagus lalu saya bagaimana mau mengaplikasikannya, saya tidak berkembang misalnnya saya pindah salah satu wilayah saya jadi kasad di polda tentunya saya punya anggota yang saya rasakan nyaman, saya mencoba mengambil kepimpinan tersebut dalam diri saya sebagai teladan dalam diri saya

M artinya, anda termotivasi justru karena pak petrus

R9 pasti itu salah satu motivasi saya, pasti saya ingin panutan bukan figur saya seperti beliau itu adalah hal yang manusiawi tidak puas dengan satu hal saja

M seberapa menentukan gaya kemimpian itu tadikan hanya sekedar stay

R9 saya punya kepuasan lebih karena saya katakan tadi, habis gelap terbitlah terang, dulu mikir pekerjaan tidak terpikirkan cyber crime itu banyak biaya tanpa adanya benefit, tapi begitu beliau masuk kita nggak usah mikir kesejahteraan, yang penting kesejahteraan tercukupi, itu membuat semua suasana menjadi nyaman, dalam bekerja pun menjadi enak, seseorang bekerja kan membutuhkan suatu motivasi, kenapa orang membawa suatu pekerjaan, seperti pak bagas bilang, mau pergi bensinnya aja nggak ada , uang bensin nggak ada, ngapain kalau saya Cuma dikasih uang perintah doang suruh jalan, makasih aja gitu loh, kasarnya seperti itu, suatu yang bulshit kalau kita bicara perjuangan

M oke, pak bagas ada komentar

R5 saya rasa sama

R7 saya nggak sepakat

R7 itu sutau feel dari masing orang-orang, itu masing-masing yang merasakan ada yang oh ini saya dengan cyber ini sayasudah nyaman, tapi sudut pandang mereka beda-beda, jadi rasa kenyamana itu ebrbeda masing-masing orang, pada intinya meman orang ingin dfapat gaji dapat honor harus bekerja ada biaya. tapi tidak mencukupi apakah dia harus menutupi gajinya untuk menutupi biaya itu kan nggak dengan adanya cyber crime ini di berikan, saya katakan kalau misalnya nanti ganti kepemimpinan dengan style yang berbeda, jadi style itu emang yang utama, style itu bisa mengakomodir tugas, bisa mencapai tujuan dengan pola yang yang semuanya bisa merasakan

M oke adalagi

R7 saya sependapat, di cyber crime itu nyaman bukan semata-mata hanya sepert itu, ini perlu terjadi pergeseran, kemaren jadi polisi untuk apa ini di sarankan untuk bekerja, itu penting gitukan, salah satunya dapat dari pimpinan kita bisa punya temen, dan saat itu kita harus menggunakan semua kekuatan yang ada maksud saya tetep di butuhkan target harus bisa, jaid saya kurang pendapat kalau tidak ada dukungan sesuatu terus pekerjaan tidak bekerja, tidak boleh, tanpa di dukungan pun kita harus tetep bekerja

R5 itu saya lakukan

M bapak dari tadi belum komentar pak

All he he he he

M oke saya coba kondisikan dengan kantor saya sekarang, disini ada 4 divisi, saya ada satu divisinya, mungkin saya juga merasakan seperti bapak, membuat saya nyaman, cukup memberikan saya jejak ruang, buat saya untuk bekerja, terus saya tidak perlu banyak memikirikan problem-problem saya apa itu di luar pekerjaan,oke, tapi, kdang-kadang kita sebagai manusia, manusia itukan nggak ada yang sempurna, saya yakin maish banyak orang lain kalau mau bicara gaya kepimpinan mungkin ada yang lebih baik dari dia, pertanyaan saya adalah, seperti apa sih yang lebih baik sehingga saya mau pindah ke divisi yang lain, atau perusahaan lain, kalau perusahaan seperti ini kan sama, saya tinggal bilang ke direktur saja, gimana

R4 standarisasinya

M iya standarisasi atau bagaimana, ini pertanyaannya lebih terbuka, kalau saya mau jadi pemimpin yang adil, supaya saya yakin bahwa dia akan memberikan kenyaman yang lebih apa yang mesti saya lakukan

R5 sekarang gini, dalam teori itu house before maintence, kita harus tau kondisi kerja dulu, kalau udah kerja tau itu, kita akan bikin langkah-langkah apa sih yang harus di dahulukan, nah dari semua ini itu rasa dulu, sebelum tugas ya, apa sih yang ada di cyber crime ini, sebab bagaimana mau kerja dia, suasana nggak enak, ruangannya nggak ac pusing di rumah segala macam

M atau saya rubah pertanyaannya, kalau anda jadi kanit disini

R5 teori kita harus mempelajari organisasi kita mempelajari oraganisasi tersebut bagaimana dulu dan sekarang itu bisa kita compare yang baik yang mana, sebagai contoh tadi, ada beberpa hal yang mempengaruhi itu harus kita ketahui, untuk memilih organisasi kita harus melihat, kesehatan dalam organisasi itu bagaimana, faktor-faktor yang mempengaruhi norganisasi itu apa, ini kalau kita sudha mengetahui dua-duanya ini punya style yang demikian, oh mungkin nggak bisa, harus kita lakukan perubahan dalam style kita, nah kita harus berfikiran maju, dan tidak standarisasi dari yang dulu, oh itu bagus, kita minimal harus meningkatkan, mempelajari apa yang bagus

M dari yang sudah ada ini apa yang perlu di kembangkan supaya lebih baik

R5 satu sisi emang kita harus bersatu, operasionalnya organisasi

M maksudnaya operasional organisasi

R2 ya kemampuan anggota kita tingkatkan dengan sumber daya manusia, dengan anggarannya, metodenya, matrialnya, itu sangat urgent dalam organisasi yang sedang berjalan

M oke

R5 kalau itu tidak ada salah satunya tidak akan berjalan, kalau anggarannya ngak ada ya nggak bisa berjalan, matrialnya nggak ada ya nggak akan berjalan, sumber daya itu harus bisa berjalan dalam organiasi

M oke, kalau saya tanya kebelakang mungkin nggak itu butter upnya

R5 boleh karena kita harus menggunakan sistim open manajemen, buter up dari bawah apa yang teraspirasi dari bawah, yang saat itu tidak bisa di laksanakan sehingga yang jadi kendala itu, ini akan jadi peluang

M oke

R4 dalam desicion maker itu pengaruh juga secara pimpinan, dia minta masukan dari angotanya sehingga itu akan jadi bahan pertimbangan, untuk membuat keputusan itu tadi itu sangat mempengaruhi keputusan itu tadi, sebelum dia memutuskan dia bertanya apa sih

R5 jadi ini suatu pelajaran untuk kita, walaupun kita sebagai orang pemimpin, kita di beri pelajaran baru, kita bikin open manejemen, emang kepemimpinan punya kekuasaan untuk memutuskan pendapat yang banyak lebih bagus daripada satu orang, jadi itu pelajaranb

M oke, apa yang kurang apa yang hilang kalau hal ini tidak di lakukan

R4 hasilnya tidak akan maksimal mungkin pendidikan doang, tidak berbaur

R5 satu sisi itu kebersamaan semuanya bisa merasakan, kalau hambatannya seperti ini, jadi keputusannya itu tidak merupakan satu hal mutlak jadi satu kepemimpinan disitu bisa di pelajari dengan satu proses

M oke, komentar atau pendapat yang lain kalau jadi

R7 menyikapi prinsipanya pak idang bekerja cerdas bukan berkerja keras, saya mengambil bisa mengambil keputusan jadi satu, pemimpin itu bekerja cerdas yaitu mampu mengakomodasi semuanya, dan kita mengambil keputusan, kalau saya jadi kanit, saya bikin performa sebelum saya buat pengelompokan,(ganti kaset video) dalam arti gini yang saya lakukan misalnya pendapat dari yang low itu, itu yang akan saya lakukan

M kalau saya milanya ambil satu contoh, kalau bicara soal perusahaan, saya akan inta pindah ke tim lain, saya yakin tim saya kurang bagus, bisnis di perusahaan ini, ada 2 tim kualitatif, 2 tim kuantitatif, saya termasuk yang di kualititaif, kalau direktur kuantitaif itu saya gantikan, saya tidak yakin, pekerjaan saya lebih baik dari yang saya lakukan, kalau untuk anda sendiri kalau anda di gantikan orang lain, saya gini saya kurang bisa memberikan contoh, karena saya tidak kenal figur yang menurut anda baik, atau yang anda angap tidak baik kalau saya pemimpin yang top down, bagaimana kinerjanya, atau ada yang bisa kasih contoh nggak, yang menurut anda mempengaruhi bekerjanyajaid tidak maksimal

R4 gini mas, saya kan tugas sudah 16 tahun ya, sebelum di cyber crime saya sudah bekerja jadi kabag, kapolres, nah dengan pekerjaan saya itu saya bisa merasakan itu, yang saya rasakan justru yang dibawah, tapi kalau yang di atas dia sekedar aja, hasilnya nggak maksimal hanya melaksanakan itu aja hasilnya pasti beda

M oke, hasilnya pasti beda ya

R4 pasti beda
M oke, ini sesi terakhir saya ingin mengajak kesebuah permainan, saya ingin mengajak temen-temen disini kalau kita bisa mengibaratkan sesuatu jadi orang misalnya kalau BMW jadi orang, saya akan terbayang jadi orang apa, dia jadi laki-laki, kokoh, gaya terus
R4 power full
M oke, saya bingung nih kalau ada banyak organisasi mana yang lebih gampang di ubah jadi orang golkar dengan apa
R5 pks lah
M oke, kalau misalnya kita ubah jadi orang, saya harus ambil karakter yang mana, laki atau perempuan
R4 laki-laki
M umurnya
R5 50
R3 60
M kenapa nggak 70
R2 ketuaan
R5 masa produktif manusia segitulah
M terus pekerjaannya
R2 birokrat
R4 politikus
M bagaimana sifatnya, stylenya
R7 diktator
R2 berwibawa
M apa yang terpenting dalam hidupnya dia
R1 matre
R8 kekuaasaan
R10 prestise
R4 gengsi
M nah sekarang pks jadi orang
R10 laki-laki
R1 brewok
M golkar nggak brewok ya
R1 nggak, parlente kalau ini brewok
M umur berapa
R2 35 tahun
M malah justru lebih muda
R1 muda itu
M apa pekerjaannya
R4 ustadz
R10 dakwah
M sifatnya
R2 agamis,
R1 santun, nuansa islam lah
M gayanya apa
R8 bebas dia
R4 munafik
M muna

R3 iya, nolak volvo di rumah punya mercy
R1 poligami
M oke, setiap manusia punya kelebihan dan kekurangan dari golkar
R5 percaya diri
R6 dermawan kali ya
R3 intelektual
M oke, apa kekurangan dia, yang bikin kita nggak suka
R4 arogan
R3 individualis
R1 sok kuasa
M oke, pks apa hal positif dari dia
R1 menyejukan
R3 yang penting kekuasaan
R6 religius
M apa positifnya dari sifat religiusnya dia
R6 jadi yang haram nggak di halalkan
R5 konsisten
M kalau yang negatifnya
R6 tukang kawin
R4 munafik itu udah semuanya pak
R5 terlalu aku, gue banget he he he
M ini berfikir kekuasaan, tapi beda dengan yang disini ya
R2 beda

KASET 3 SIDE B

R3 contohnya itu tidak mau pake mobil mewah cari popularitas aja supaya kesannya bersih
M iya, iya, bah itu kalau organisasi pks sebagai organiasi, kalau misalnya polri jadi orang wujudnya akan seperti apa
R1 macho
R7 orang tua
M orang tua umur berapa
R3 umur 50 sampe 55 tuh awam
M oke gayanya gimana
R7 mapan
R4 menolong
R8 jiwa sosial
R5 sejahteralah
R2 hidup dengan banyak problem
R4 iya dinamikanya sangat tinggi kadng turun kadang naik
M oke, kalau saya mau bikin film tentang seseorang yang punya karakter orang ini dari sifat-sofatnya dia ada nggak
R2 wibawa jelas
R7 suka gratisan
R4 itu pak dicky
R robert
R6 problem pekerjaan
M berseamngat
R5 tidak sombong, rajin pangkal kaya suka menabung

R2 jangan, ini figur, menganyomi
R2 menolong
M menganyomi maksudnya
R7 berjiawa sosial
M kalau kita kasih nama nya siapa nih?
R8 robocop
R4 tukul
M atau saya yaga kaish nama deh wawan
R1 nggak cocok
R6 robert chip
M oke, kita kasih nama robert ya, kalau kita ubah robert ini umurnya 50-60, dia ini berkecukupan, dia mapan tapi hidupnya penuh dengan problem, ini seperti apa nih, tadikan di sebutkan hidupnya banyak problem
R3 terlalu banyak tanggungan
R6 terlalu banyak pekerjaan
R3 maksudnya punya problem solving dia ya
M oke kita butuh rokok
R3 boleh
R5 minum aja belum kok
R7 minum aja dulu
M bagaimana dia menghadapi problem apa yang bisa alat atau senjatanya dia
R1 sabar
R7 kita berpatokan apa seseorang ya kalau kita menghayal lagi susah
M emang ada kesan nggak jelas gitu ya
R2 emang sengaja di anu mas
R7 udah lanjut aja mas
R5 ini Cuma skenario
R1 udah sabar
R7 bijaksana
M ini kayaknya semua hal-hal yang ideal tapikan hiduonya penuh dengan prblem
R1 diakan problem solving
M yang paling penting buat dia dalam hidupnya
R9 pengakuan
R6 kemapanan dia banyak masalah
R1 eksistensi diri, misalkan ada masalah , selama ini udah
M kurang begitu , punya kelebuihan kekurangan, kalau golkkar tadi parlente kalau apa kelebihan di robert
R3 familiar
R5 low profile
R7 pertanyaanya dulu apa, kok low profile
M d tadi golkar punya sgaya parlente kalau polri
R1 necis
R2 bersahaja
R4 tidak sombong
M yang paling penting dalam hidupnya
R1 pengakuan
R5 lebih baik pengakuan

R6 eksistensi
M pengakuan apa sih
R6 aktualisasi diri
M pengakuan sebagai apa sih
R6 eksistensi dia
R3 di akui lingkungannya dia, misalnya kalau tetangga ada masalah minta tolongnya sama dia
R7 contohnya gini loh mas, apa yang di lakuin sama dia dapat di terima
R5 dimana pun berada dapat di terima
M apakah artinya selama ini si robert itu kurang begitu di terima kurag begitu d hargai
R1 nggak begitu mas, tetep semua manusia begitu
M oke, seperti tadi ya setiap manusia punya kelebihan punya kekurangan , apa kelebihanya si robert
R4 mapan
R6 wibawa
R3 suka menolong
M oke, mapan wibawa
R12 familiar
M apalagi kalau kekurangan nya
R1 sok kuasa
R3 gampang terpengaruh
R6 nyelekit lagi kalau ngomong
M apalagi hal yang bikin kita nggak suka sama si robert
R4 kurang peduli sama lingkungan
R2 tadi suka menolong kok
R7 moderatornya pada satu orang
M ini untuk semua
R3 mudah di hasut
M apalagi
R2 pelit
R7 saya kurang setuju si ricky baik mas
M kita ngomongin si robert, ini kekurangannya
R5 tidak cooperative
M maksudnya tidak cooperartive
R5 masa bodoh
M oke, adalagi, kalau sifat positif yang bikin kita suka sama dia apa?
R6 ya itu tadi familiar
R7 mapan
R2 tidak sombong rajin menabung
M sorry yang penting dalam hidupnya apa tadi
Ali pengakuan
R2 aktualisasi diri
M dengan cara apa dia dapat itu
R1 berbuat baik
M apa yang bisa di andalkan dari dia untuk bisa berbuat baik itu
R5 dia harus bisa intropeksi diri, menggali kekurangan untuk jadi kelebihan

M itu saya masih menangkap kesan ideal, kalau dari karakter robert apa yang selama ini dia andalkan untuk tujuannya dia
R5 kan dia mapan
M Kan kita bilang tadi ingin mendapatkan pengakuan artinya pengakuan itu bisa di terima dengan orang lain ya
R8 posisisnya dia sudah mapan
M yang bisa di andalkan oleh dia untuk menunjukan rasa baiknya dia
R4 predikat nya ya
R5 pososinya dia lah
M posisinya dia, oke, posisinya dia bisa melakukan apa aja
R2 dengan kewenangannya dia ya
M tadi kita bicara soal si polri kalau unit ini gimana sama seperti tadi, kita buat nama deh
R5 untung pak namanya
M untungnya ya
R1 sama awalnya U kan
M oke
R1 smart
R7 ahli teknologi
M oke, ini menarik, begitu tadi saya tanya yang keluar umur, tapi kalau ini langsung keluar smart, kenapa yang spontan itu keluar smart kenapa
R3 hitech
R7 kareba berhubungan dengan teknologi
M usia
R5 30
R6 40-50
R2 40-50
M apalagi?
R4 work aholic, pekerja keras
M maksudnya pekerja keras disini
R5 tidak mengenal waktu kalau kerja belum selesai
M oke, selain itu apalagi
R6 telaten
R8 ulet
R1 prestise
R1 kebanggaan prestasi
R4 keren
M ini kita bicara soal si untung, kira-kira apa yang bisa di katakan positf atau yang kta suka sama dia
All semuanya
M yang paling kita suka
All smart
R1 smart dan prestise
R5 bijaksana
R7 yang paling penting itu punya harapan
M apalagi yang membuat kita suka
R2 dermawan
R4 nggak, untung orangnya jelas

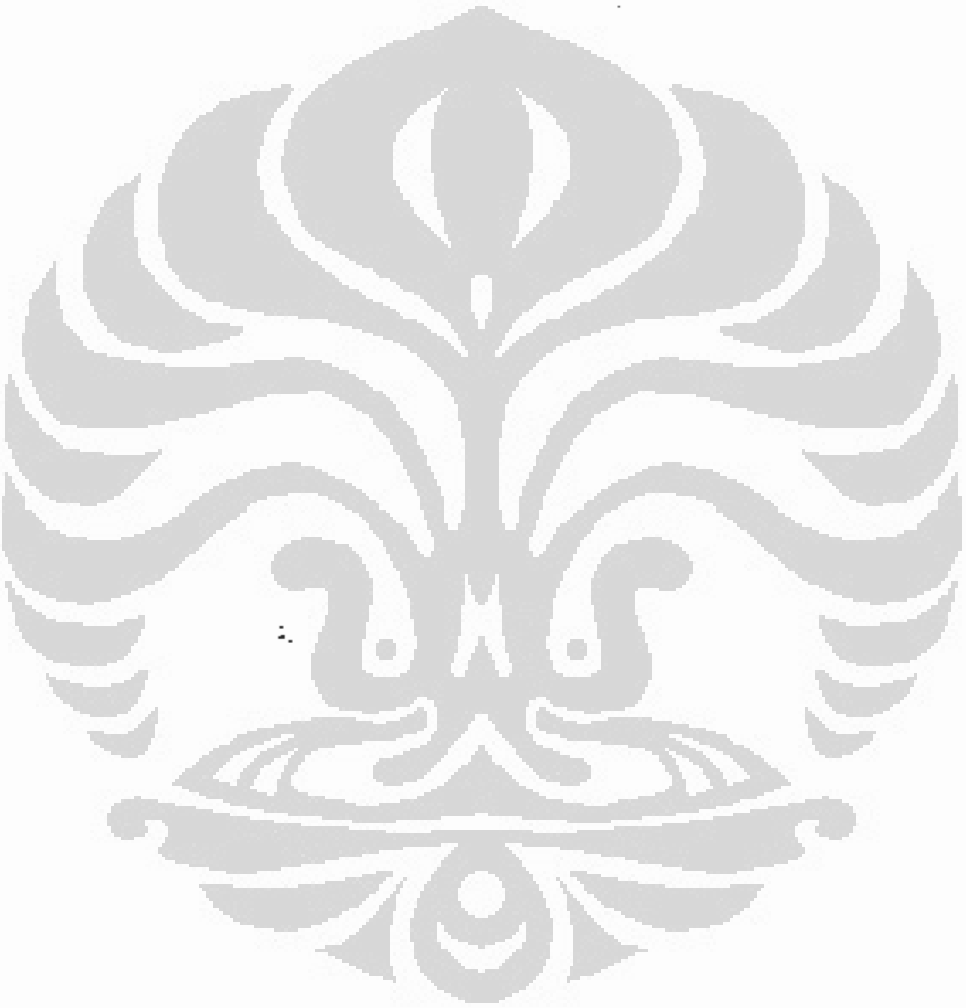
M apa yang jelas dari untung
R8 dermawan
R6 nggak pelit
M maksudnya jelas
R9 maksudnya apa yang di omongin jelas, jadi konsekwen lah, konsisten
M mungkin konsisten tadi kita ngomongin polri seperti apa? Si robert seperti apa si untung seperti apa, seperti ada bedanya
R5 bapak nggak lagi mejebak kan
M nggak
R7 biarina ja
M kalau saya bicara supir apa yang kebayang
R5 anduk kecil
M tapikan supir itu macam-macam ada supir taxi, secara umum, ini bisa jadi sisi yang lain atau kekurangannya nggak beda, apa yang bikin kita suka sama dia, adalagi nggak
R6 baik hati
R1 sama dermawan sama aja
M oke, seperti tadi, untung ini tetep manusia
R5 transpasrasi
R3 keterbukaan
M oke, sebagai manusia apa kekurangan si untung ini
R4 keras
M maksudnya keras ini apa?
R4 sifat aja, sifatnya keras
M apa yang kita sukai dari sifat keras
R4 perempuan suka semua loh he he he
M apa yang tidak kita sukai dari si untung, pasti dia punya kelebihan dan kekurangan
R5 sifat manusia itu pasti ada sifat marah gitu
R7 maksudnya, pak dicky suka marah gitu
All he he he he
R1 manusia loh
M oke, suka marah, apalagi yang kita tidak sukai dari si untung ini
All ha ha ha ha
M ini bebas aja ya, kalau kita gambarin manusia
R8 memang bebas tapi konsekwensinya he he he
All he he he he
M ini jujur aja, untuk pengembangan ke depan, apa yang bisa jadi masukan sesuatu yang lebih baik
R7 Royal
M royal ini maksudnya apa
R7 boros
R6 boros
M oke, apalagi yang kita nggak sukai dari dia
R5 bapak galinya menjebak, baoak tanya satu-satu
All he he he he
M kenapa kita buatnya seperti ini
R5 manusia itu punya sifat lupa, mungkin si untung punya sifat lupa

All he he he he
M apalagi?
R6 udah kayaknya
R1 kalau nggak di gali nggak keluar
R6 pak idang nggak bisa ngomong
M sebentar waktu kita menggambarkan golkar kita tidak mengacu pada seseorang, pada organisasi, pks juga seperti itu, bahkan waktu polri tidak mengacu ke seseorang tapi pada saat unit ini saya mendapat kesan kalau kita ihni membicarakan seseorang
R8 gini mas, mas itu ke seseorang, jadi kita susah ininya, kejelekan organisasi dengan kejelekan sama perorangan itub beda loh, karena kalau organisasi itu include kan
R5 di anggap satu orang, sekarang bebas aja
R1 ini bukan perorangan pak, ini di jadikan manusia
R8 susah, nggak bisa dong
R5 tanya satu-satu pake edi gimana, pak idang gimana, nanti baru saya bisa ketemu
M saya mau konfirmasi yang saya tulis-tlis disini, saya konformasi sebagai sesuatu yang sangat persepsi yang sama, apakah semua disini berpendapat si untung ini smart
All iya
R5 oke
M semua kayak gitu
All oke
R7 pak idang aja tanyain
R1 kita perlu responsif dulu, kalau smart itu usia produkti, 30-50 lah
R3 karena kita dia atas 30 semua
All he he he
M apa yang negatif, yang membuat kita tidak suka atau orang lain tidak suka
All nggak ada
R8 kalau untung ini sebagai orang smart, dengan smart ini dia banyak berbuat, dia tidak iri gitu loha
R7 untung siapa

M oke, apa yang penting dalam hidupnya
R8 prestasi kerja yang terbaik
M kenapa
R3 demi kaiir, demi keluarga
M sebenernya ini sesi terakhir, saya tinggal sebentar mungkin ada tambahan pertanyaan dari temen saya
R7 sampe malam juga nggak apa-apa mas
R3 pak dicky takud sama pak ricky
R7 ini nanti ada lagi ya
R1 ngusir
All he he he he
R7 apa komentar mereka pak
M sebenernya ini sungguh menarik sekali mungkin nanti kita ada obrolan lanjutan

R7 waktunya kapan

=== Thanks & Close ==



LAMPIRAN FOTO

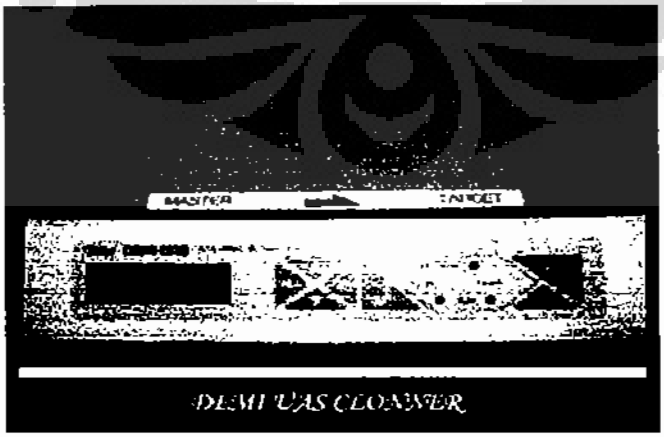
Kegiatan di ruang kerja CETS

Kegiatan di ruang kerja Unit CyberCrime

Tallon Logicube Imaging

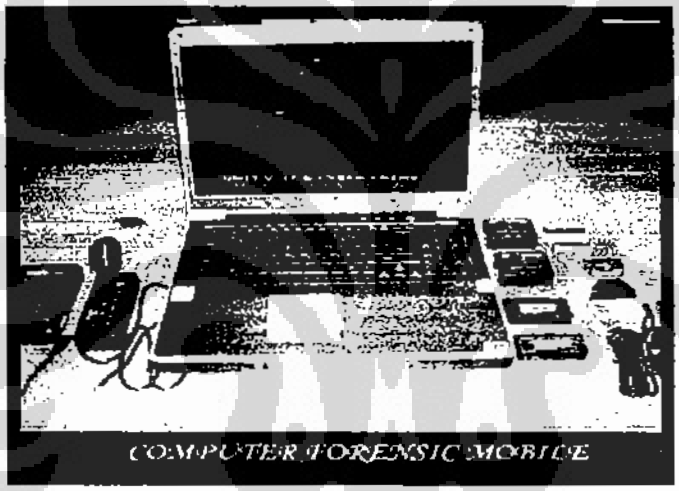
Komputer Forensik

Paraben Device Seizure

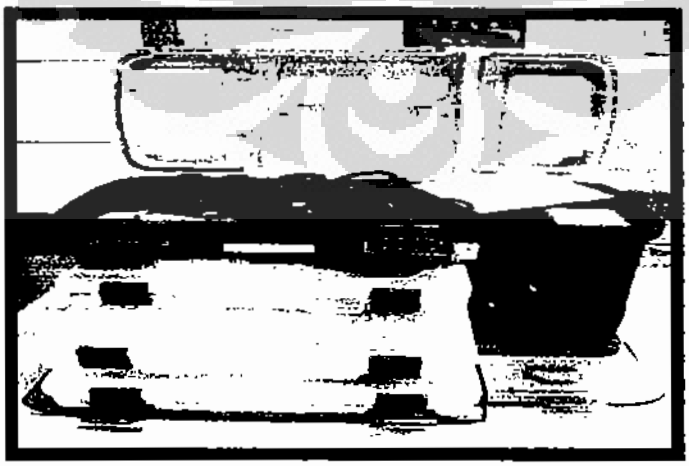


DEMI UAS CLONNER

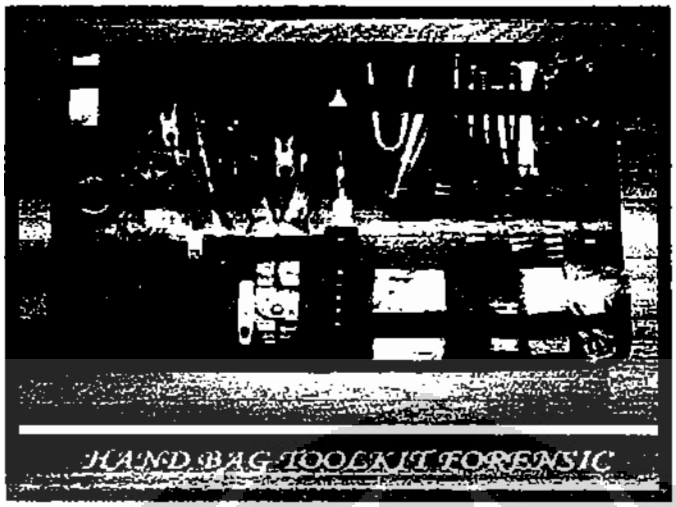
Toolkit Forensic



Computer Forensic Mobile



Toolkit Forensic



Hand Bag Toolkit Forensic

FRED (Forensic Recovery Evidence

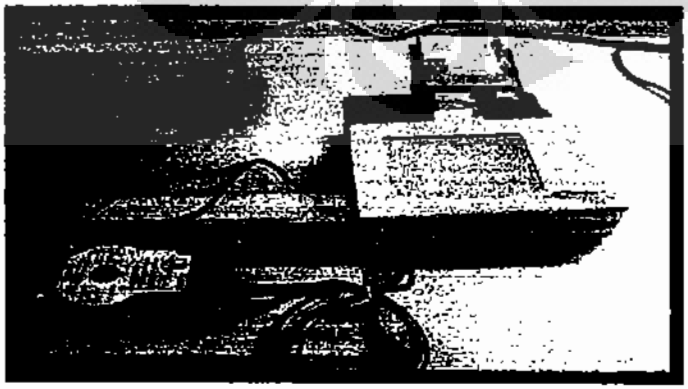


Image Masster Solo 3

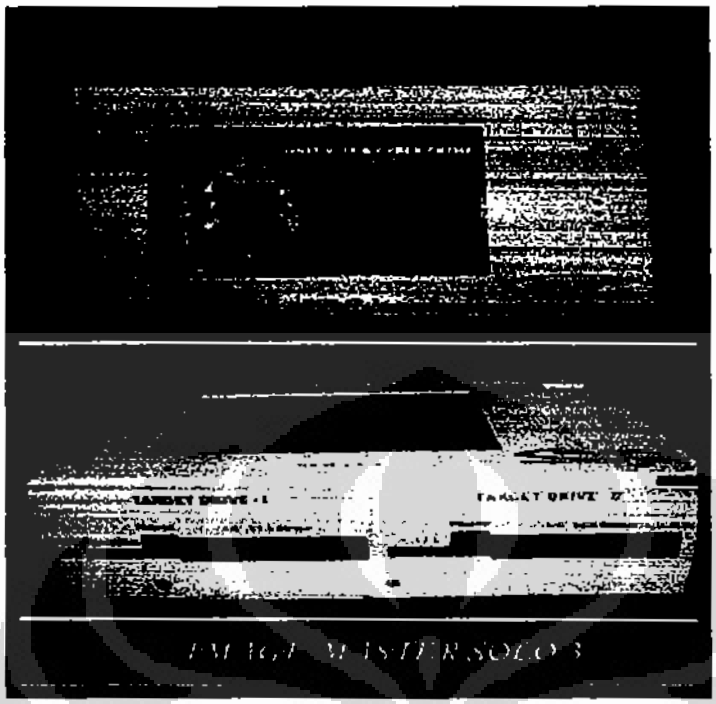
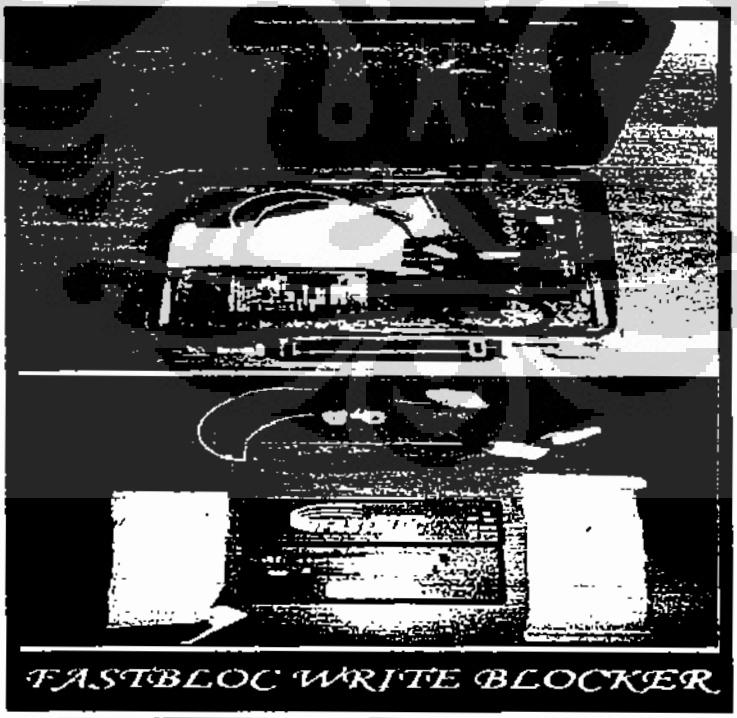


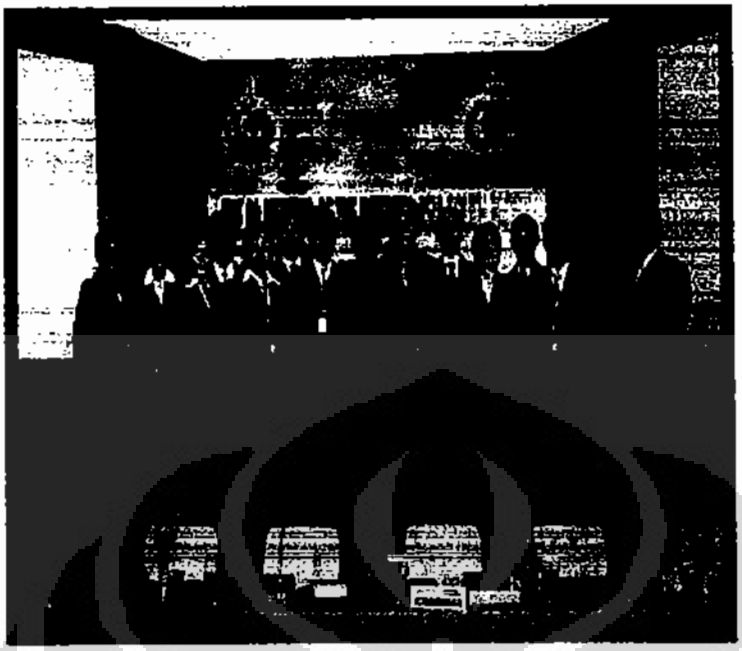
Image Master Solo 3



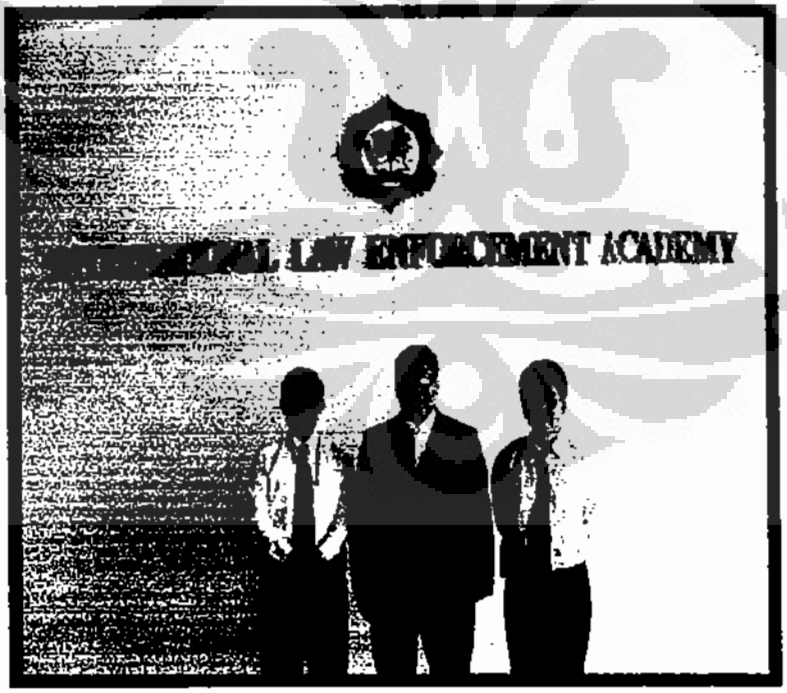
Fast Block Write Blocker

Pelatihan EnCase di Unit Cyber Crime
Bareskrim Polri tahun 2008

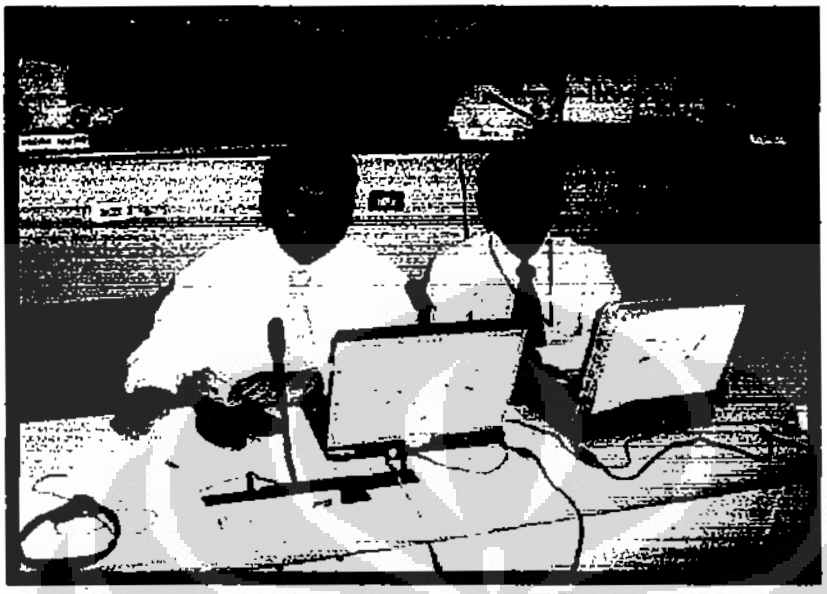
Ruangan Laboratorium Forensik Komputer



Interpol Meeting mengenai Cyber Crime di Bali tahun 2007



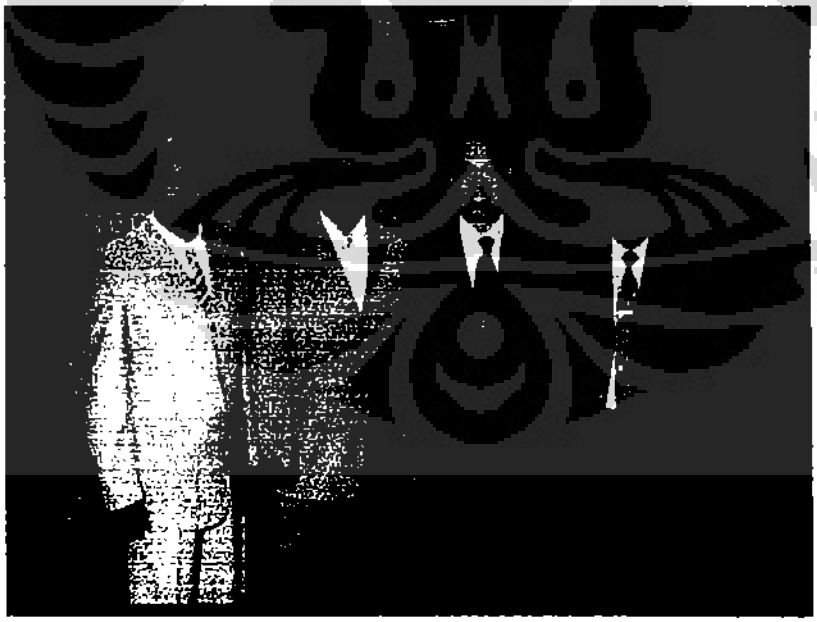
Hongkong



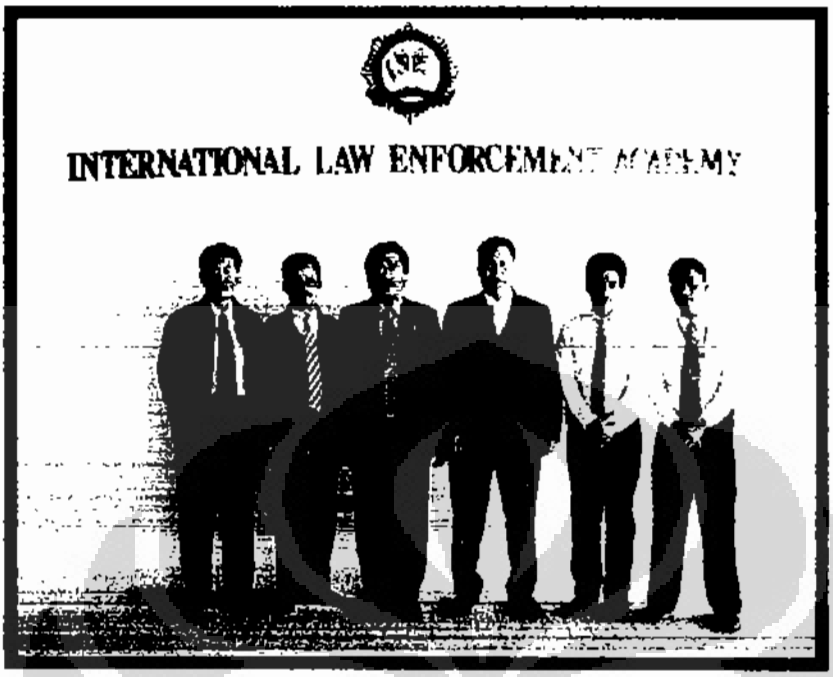
Law Enforcement and Prosecutor Advanced Cybercrime Training
di Bangkok Thailand 20 Juni 2006

Sosialisasi RUU ITE di Manado tahun 2007

Seminar Fighting Fraud di Singapura tahun 2006



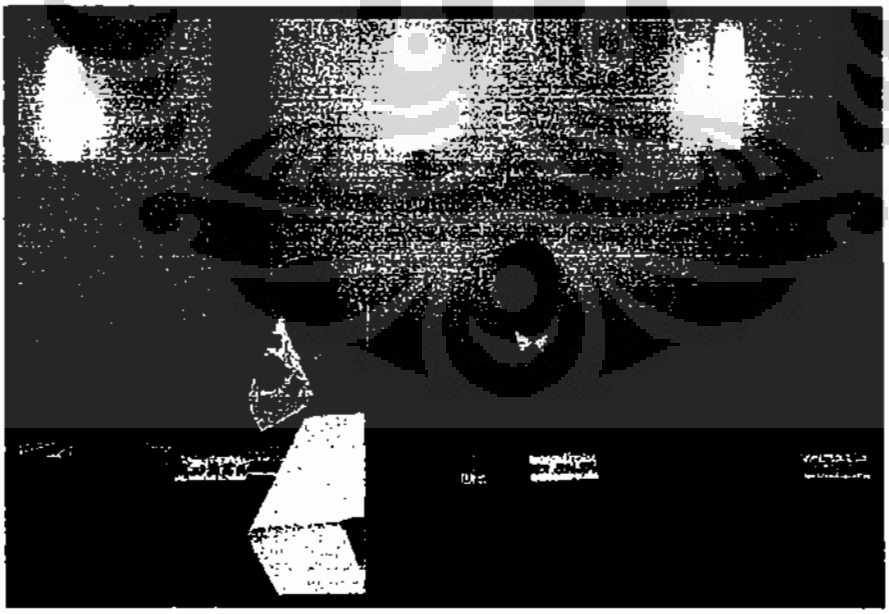
Seminar Cyber Crime di Singapura tahun 2007



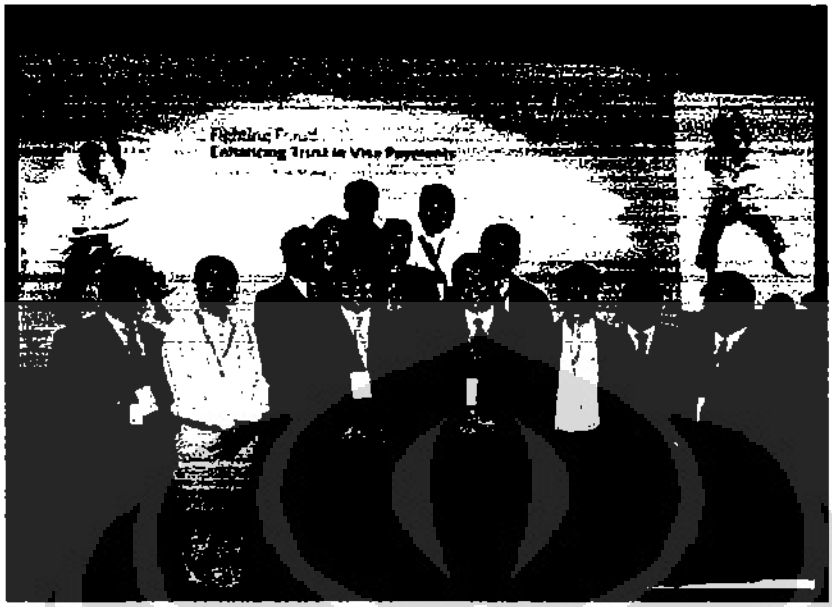
Hongkong

Seminar Cyber Crime di Singapura tahun 2007

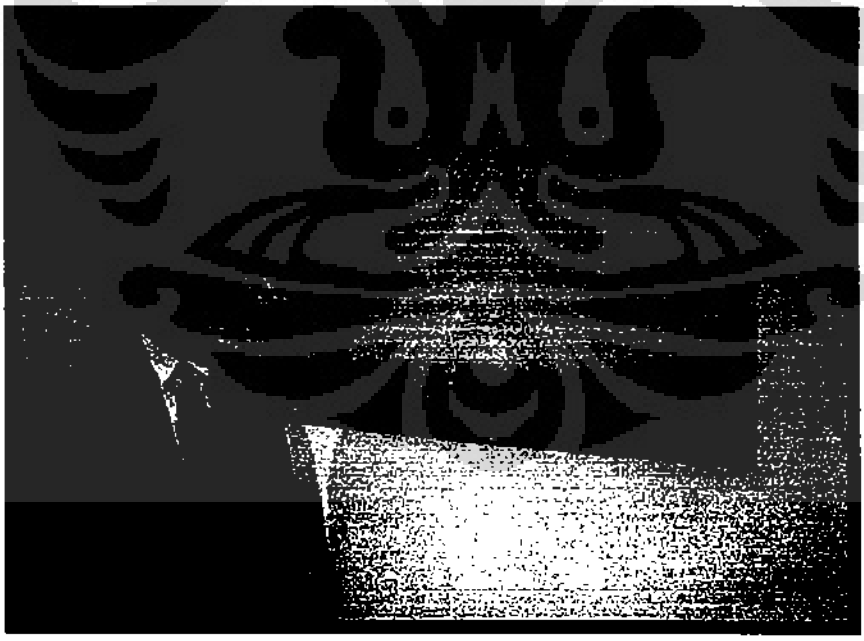
Konferensi Interpol mengenai Cyber Crime di India tahun 2007



Seminar Cyber Crime di Singapura tahun 2007



Seminar Fighting Fraud di Singapura tahun 2006



Seminar Cyber Crime di Singapura tahun 2007

Konferensi Interpol mengenai Cyber Crime di India tahun 2007

Seminar Cyber Crime di Singapura tahun 2007

Questionnaire

Subject	:	Investigation Management for Hacking or IT & Cyber Crime Case
Researcher	:	Petrus Reinhard Golose
Name Respondent	:	Gerhard Rosskopf
Institution	:	
Position of Respondent	:	
Time	:	
Place	:	

Please fill your answers in third columns:

No. (1)	Questions (2)	Answer (3)
1.	• In your country, do you have a special or dedicated unit to counter IT misconduct and/or cyber crime? • If, your answer is yes, please explain how the organization works and what is its aim and programs (both short term and long terms?)	Yes One unit is established on a national level and nine smaller units are established in federal states. Aims: Assistance in computer crime cases for other police forces and handle computer crime cases (e.g. hacking cases) report with injured person till report to the curt
2.	• How long have you been involved in the organization and what is your position? • Have you investigated cyber crime cases? • Please mention the case and if possible can I get the brief of such cases?	7 years. Head of department 5..2.1 Yes Different cases. Most Seizure of E-Evidences and Data damage, …….
3.	• How do you or your organization handle the cyber crime cases? • How do you or your organization investigate such cases?	Considering national and international guidelines

	• Do you have any standard procedure to deal with the investigation on cyber crime? • Would you please explain how the investigation process carried out by your organization? • Do you have any certain system specially established relating to such investigation? Please explain the details.	
4.	• Do you apply certain management system when you or your organization handling the IT & Cyber crime cases? • Do you think it is necessary or even obligatory to apply a good and proper management in dealing with the investigation of IT & Cyber Crime cases? • What is your opinion about investigation management? What is it? And how does it work? Please feel free to give your own opinion	We are using special Software to handle cyber crime cases. Top priority – don't change the original data's. Obey legal power and guidelines Yes
5.	• During the investigation on cyber crime, do you have any problem which makes you or your organization cannot accomplish your work or your investigation? • Please explain, and share examples	Encryption. We would need more training possibilities. Data retension New hard- and software → training is necessary
6.	• Do you have any computer forensic laboratory to support your investigation on the cyber crime?	We are the computer forensic unit.

	• Is it in your internal organization or is it an independent laboratory that also prepared for investigating any crime including conventional crime as well as cyber crime? Why? And what is your opinion about that?	Within the organization
7.	• Do you have any special regulation against IT & Cyber Crime? • Please explain. And what is your opinion about that?	We have special legislation about computer crime Very important
8.	• Do you have regulation supporting digital evidence? • How does it work? • What is your opinion about it?	Yes OK
9.	• During the last 5 years, how many IT & Cyber Crime cases have been reported, investigated and brought to court? • If any, do you think that number represented all the cases of IT & Cyber crimes happen in your country? Please explain	There is no reliable statistic within this period No
10.	• Do you know "hacking"? • Is it one of the cyber crimes in your country? • Has it been regulated in a certain regulation? • What is your own opinion about it? • Do you think hacking is	Yes Yes Yes Necessary Yes

	dangerous? • Do you think hacking also has to be combat? • Do you think hacking also has to be regulated in a certain law? • Please share your opinion	Yes Yes
11.	• Do you think it is necessary or even obligatory to establish a certain investigation management while you or your organization conduct an investigation on hacking cases? • Why and how does it supposed to be applied? • Do you think the good and proper investigation management would make any difference in your investigation process? • If yes, please explain why.	Yes Because of authenticity at court. Based on national and international guidelines Yes Because of authenticity at court.
12.	• What do you think about external involvements in the investigation process of hacking cases? The external investigation would be other organization, other unit in your organization, or even other foreign organization. • What are they? • Do you think that the external aspects give contribution to the success of the investigation? • Please share your opinion,	In dependence of the case it could be necessary to get assistance from other national an international established police forces or from the private sector.

	with example will be more appreciated.	
13.	• Do you think the cooperation with other similar organization from other countries is required to combat the hacking cases or other IT & Cyber Crime? • Why and how does it (the cooperation with other country) suppose to be developed? • Has your organization developed the cooperation with similar organization from other country? Please mention names if possible. • What kind of cooperation does your organization develop with other country? Please explain.	Yes Based on international treaties. Austria is a member of different international working groups within Interpol, Europol and other organizations (e.g. Interpol working party, botnet taskforce, agis program,……) Austria is a member of different international working groups within Interpol, Europol and other organizations (e.g. Interpol working party, botnet taskforce, agis program,……)

Thank you for your participation. This questionnaire is very meaningful for my findings.

Sincerely yours,
Petrus Reinhard Golose

Questionnaire

Subject	:	Investigation Management for Hacking or IT & Cyber Crime Case
Researcher	:	Petrus Reinhard Golose
Name Respondent	:	Alberto GarcíaMorales.
Institution	:	Spanish Civil Guard.
Position of Respondent	:	Lieutenant.
Time	:	
Place	:	Madrid, Spain.

Please fill your answers in third columns:

No. (1)	Questions (2)	Answer (3)
1.	• In your country, do you have a special or dedicated unit to counter IT misconduct and/or cyber crime? • If, your answer is yes, please explain how the organization works and what is its aim and programs (both short term and long terms?)	Yes. There are teams dedicated to research, high tech and databases.
2.	• How long have you been involved in the organization and what is your position? • Have you investigated cyber crime cases? • Please mention the case and if possible can I get the brief of such cases?	Four years ago. Actually I am a lieutenant of High tech team. Yes. For example: • Operation "Navy": One hacker attacks the systems of submarine dry dock. • Operation "Jineta": Several people apologized "yihad" though internet. • So on...
3.	• How do you or your organization handle the cyber crime cases? • How do you or your organization investigate such cases?	Network investigations and forensic analisis.

	• Do you have any standard procedure to deal with the investigation on cyber crime? • Would you please explain how the investigation process carried out by your organization? • Do you have any certain system specially established relating to such investigation? Please explain the details.	Yes. Essentially the method have tree steps. First previous reconaissance, analysis and finally forensic analisis. No, such investigation needs a different hack techniques.
4.	• Do you apply certain management system when you or your organization handling the IT & Cyber crime cases? • Do you think it is necessary or even obligatory to apply a good and proper management in dealing with the investigation of IT & Cyber Crime cases? • What is your opinion about investigation management? What is it? And how does it work? Please feel free to give your own opinion	Yes. Yes, this is absolutely necessary. It is necessary to implement a method, also new methods of ciber crime are changing and very specialized.
5.	• During the investigation on cyber crime, do you have any problem which makes you or your organization cannot accomplish your work or your investigation? • Please explain, and share examples	No.
6.	• Do you have any computer forensic laboratory to support your investigation on the cyber crime? • Is it in your internal organization or is it an independent laboratory that also prepared for investigating any crime	Yes. The forensic laboratory support our investigations and it makes support to judicial forces.

	including conventional crime as well as cyber crime? Why? And what is your opinion about that?	
7.	• Do you have any special regulation against IT & Cyber Crime? • Please explain. And what is your opinion about that?	No.
8.	• Do you have regulation supporting digital evidence? • How does it work? • What is your opinion about it?	Yes. For specialists. It is necessary.
9.	• During the last 5 years, how many IT & Cyber Crime cases have been reported, investigated and brought to court? • If any, do you think that number represented all the cases of IT & Cyber crimes happen in your country? Please explain	120 cases approximately. 25 for cyber crime case and 95 for IT.
10.	• Do you know "hacking"? • Is it one of the cyber crimes in your country? • Has it been regulated in a certain regulation? • What is your own opinion about it? • Do you think hacking is dangerous? • Do you think hacking also has to be combat? • Do you think hacking also has to be regulated in a certain law? • Please share your opinion	Yes. Yes. Yes, criminally as long as it breaks systems. The purposes are good if only is knowledge reason. Yes. Yes but only for if it's necessary. Yes, of course. We need hacking because about it our systems are strengthened.

11.	• Do you think it is necessary or even obligatory to establish a certain investigation management while you or your organization conduct an investigation on hacking cases? • Why and how does it supposed to be applied? • Do you think the good and proper investigation management would make any difference in your investigation process? • If yes, please explain why.	Yes, of course. In the same way. No
12.	• What do you think about external involvements in the investigation process of hacking cases? The external investigation would be other organization, other unit in your organization, or even other foreign organization. • What are they? • Do you think that the external aspects give contribution to the success of the investigation? • Please share your opinion, with example will be more appreciated.	It is necessary. Different companies as Microsoft, Guidance, Dell, S21sec and others. Yes, of course. Collaborate with different companies is essential everyday, for example our groups works with Microsoft and other ones training.
13.	• Do you think the cooperation with other similar organization from other countries is required to combat the hacking cases or other IT & Cyber Crime? • Why and how does it (the cooperation with other country) suppose to be developed? • Has your organization developed the cooperation with similar organization from other country? Please mention names if possible.	Yes, of course. Training with different work groups and sharing the knowledge. Yes, Europol and Interpol.

	• What kind of cooperation does your organization develop with other country? Please explain.	Actually only training for trainers.

Thank you for your participation. This questionnaire is very meaningful for my findings.

Sincerely yours,
Petrus Reinhard Golose

Questionnaire

Subject	:	Investigation Management for Hacking or IT & Cyber Crime Case
Researcher	:	Petrus Reinhard Golose
Name Respondent	:	Chris A. Siouris
Institution	:	Postal Inspector, U.S. Postal Inspection Service
Position of Respondent	:	
Time	:	
Place	:	

Please fill your answers in third columns:

No. (1)	Questions (2)	Answer (3)
1.	• In your country, do you have a special or dedicated unit to counter IT misconduct and/or cyber crime? • If, your answer is yes, please explain how the organization works and what is its aim and programs (both short term and long terms?)	Yes, the U.S. Postal Inspection Service now has an active cyber-crime unit which solely investigations crimes with computer nexus. The aim is to stop hackers from defrauding American consumers through the illicit use of the U.S. Mail system.
2.	• How long have you been involved in the organization and what is your position? • Have you investigated cyber crime cases? • Please mention the case and if possible can I get the brief of such cases?	I have been employed as a Postal Inspector since August 2001. I have investigated cyber-crime cases, with the most notable being United States vs. Roman Vega, a Ukrainian national who was arrested with a laptop containing over one million stolen (hacked) credit card numbers.
3.	• How do you or your organization handle the cyber crime cases? • How do you or your organization investigate such cases? • Do you have any standard procedure to deal with the	We have dedicated analysts who comb computer data and cull it all into comprehensive analyses and reports. We also work closely with foreign law

	investigation on cyber crime? • Would you please explain how the investigation process carried out by your organization? • Do you have any certain system specially established relating to such investigation? Please explain the details.	enforcement and American internet companies, i.e. Google, Yahoo, etc. The investigation consists of police work, proper reporting and presentation to prosecutors, Grand Jury indictment, and then arrest and prosecution.
4.	• Do you apply certain management system when you or your organization handling the IT & Cyber crime cases? • Do you think it is necessary or even obligatory to apply a good and proper management in dealing with the investigation of IT & Cyber Crime cases? • What is your opinion about investigation management? What is it? And how does it work? Please feel free to give your own opinion	Nothing out of the ordinary. We treat cyber-crime cases with the same protocol as regular, non-cyber cases. Proper management is of course paramount. Admittedly, I am not totally familiar with the term "investigation management".
5.	• During the investigation on cyber crime, do you have any problem which makes you or your organization cannot accomplish your work or your investigation? • Please explain, and share examples	The only problem which we face is overseas jurisdictional issues, i.e. we cannot arrest or extradite some suspects in certain countries.
6.	• Do you have any computer forensic laboratory to support your investigation on the cyber crime? • Is it in your internal organization or is it an independent laboratory that also prepared for investigating any crime including conventional crime as well as cyber crime? Why? And what is your opinion about that?	The Postal Inspection Service employs various computer forensic examiners scattered throughout the country. Our lab work is conducted internally, by specially-trained Postal Inspectors.

7.	• Do you have any special regulation against IT & Cyber Crime? • Please explain. And what is your opinion about that?	There are currently no special enhancements for computer crime in the United States. I assume that there will be in the future, however.
8.	• Do you have regulation supporting digital evidence? • How does it work? • What is your opinion about it?	Digital evidence must be handled like any other evidence: with extreme care.
9.	• During the last 5 years, how many IT & Cyber Crime cases have been reported, investigated and brought to court? • If any, do you think that number represented all the cases of IT & Cyber crimes happen in your country? Please explain	I do not know; I do not have access to those statistics.
10.	• Do you know "hacking"? • Is it one of the cyber crimes in your country? • Has it been regulated in a certain regulation? • What is your own opinion about it? • Do you think hacking is dangerous? • Do you think hacking also has to be combat? • Do you think hacking also has to be regulated in a certain law? • Please share your opinion	I am familiar with hacking and it is regarded as a cyber-crime in the United States. Legislation has not yet caught up with the frequency with which it is carried out in my country. I hope that stiffer penalties are imposed in the future. Hacking is, of course, dangerous and should be combated no matter what. I agree that hacking should be regulated in a certain law(s).
11.	• Do you think it is necessary or even obligatory to establish a certain investigation management while you or your organization conduct an	

	investigation on hacking cases? • Why and how does it supposed to be applied? • Do you think the good and proper investigation management would make any difference in your investigation process? • If yes, please explain why.	
12.	• What do you think about external involvements in the investigation process of hacking cases? The external investigation would be other organization, other unit in your organization, or even other foreign organization. • What are they? • Do you think that the external aspects give contribution to the success of the investigation? • Please share your opinion, with example will be more appreciated.	I am not opposed to certain external forces being involved in my investigation(s), so long as it is a constructive relationship. I more readily welcome foreign law enforcement liaison before fellow U.S. agency assistance. The external aspects definitely contribute to the success of said investigation.
13.	• Do you think the cooperation with other similar organization from other countries is required to combat the hacking cases or other IT & Cyber Crime? • Why and how does it (the cooperation with other country) suppose to be developed? • Has your organization developed the cooperation with similar organization from other country? Please mention names if possible. • What kind of cooperation does your organization develop with other country? Please explain.	Absolutely. Hacking is now truly a global problem which can only be combated by international efforts. Cooperation may be fostered through networking and meeting contacts at conferences. The Postal Inspection Service works for foreign law enforcement agencies in the former USSR, as well as Europol and Interpol entities.

Thank you for your participation. This questionnaire is very meaningful for my findings.

Sincerely yours,
Petrus Reinhard Golose

Questionnaire

Subject	:	Investigation Management for Hacking or IT & Cyber Crime Case
Researcher	:	Petrus Reinhard Golose
Name Respondent	:	Alexander Seger
Institution	:	Council of Europe
Position of Respondent	:	Head of Economic Crime Division
Time	:	21 November 2007
Place	:	Strasbourg

Please fill your answers in third columns:

No. (1)	Questions (2)	Answer (3)
1.	• In your country, do you have a special or dedicated unit to counter IT misconduct and/or cyber crime? • If, your answer is yes, please explain how the organization works and what is its aim and programs (both short term and long terms?)	The Council of Europe is an international organization. We are not involved in investigating cybercrime but in helping countries around the world implement the Convention on Cybercrime. This includes in particular development a comprehensive legal framework to criminalise conduct (substantive law), to facilitate more efficient investigations (procedural law) and international cooperation.
2.	• How long have you been involved in the organization and what is your position? • Have you investigated cyber crime cases? • Please mention the case and if possible can I get the brief of such cases?	With the Council of Europe since 1999. Currently head of the Economic Crime D ivision. As mentioned above, we are not operational in the sense of investigations.
3.	• How do you or your organization handle the cyber crime cases? • How do you or your organization investigate such cases?	See above. However, the Convention on Cybercrime foresees procedural measures which will facilitate a minimum of

	• Do you have any standard procedure to deal with the investigation on cyber crime? • Would you please explain how the investigation process carried out by your organization? • Do you have any certain system specially established relating to such investigation? Please explain the details.	harmonization of investigative measures and procedures: *Title 2 – Expedited preservation of stored computer data* **Article 16 – Expedited preservation of stored computer data** 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is

		to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Article 17 – Expedited preservation and partial disclosure of traffic data** 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. *Title 3 – Production order*

			Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and

other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is

		lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot

		adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Article 21 – Interception of content data** 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of

		technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
4.	• Do you apply certain management system when you or your organization handling the IT & Cyber crime cases?	See above.

	• Do you think it is necessary or even obligatory to apply a good and proper management in dealing with the investigation of IT & Cyber Crime cases? • What is your opinion about investigation management? What is it? And how does it work? Please feel free to give your own opinion	
5.	• During the investigation on cyber crime, do you have any problem which makes you or your organization cannot accomplish your work or your investigation? • Please explain, and share examples	Experience from countries that we are cooperating with suggests that among the main problem are: • Lack of legislation allowing for efficient investigations, in particular regarding the expedited preservation of data, search and seizure of computer data, production order • Inefficient international cooperation • Difficult cooperation between law enforcement and service providers (we are currently elaborating guidelines as to how such cooperation can be made more effective)
6.	• Do you have any computer forensic	No.

	laboratory to support your investigation on the cyber crime? • Is it in your internal organization or is it an independent laboratory that also prepared for investigating any crime including conventional crime as well as cyber crime? Why? And what is your opinion about that?	
7.	• Do you have any special regulation against IT & Cyber Crime? • Please explain. And what is your opinion about that?	Yes. Convention on Cybercrime (see www.coe.int/cybercrime)
8.	• Do you have regulation supporting digital evidence? • How does it work? • What is your opinion about it?	See the procedural measure of the Convention on Cybercrime.
9.	• During the last 5 years, how many IT & Cyber Crime cases have been reported, investigated and brought to court? • If any, do you think that number represented all the cases of IT & Cyber crimes happen in your country? Please explain	Experience in Europe clearly shows that only a very small percentage of cybercrimes are reported and investigated.
10.	• Do you know "hacking"? • Is it one of the cyber crimes in your country?	Yes. See Article 2 of the Convention. See also the country profiles on cybercrime

	• Has it been regulated in a certain regulation? • What is your own opinion about it? • Do you think hacking is dangerous? • Do you think hacking also has to be combat? • Do you think hacking also has to be regulated in a certain law? • Please share your opinion	legislation at www.coe.int/cybercrime
11.	• Do you think it is necessary or even obligatory to establish a certain investigation management while you or your organization conduct an investigation on hacking cases? • Why and how does it supposed to be applied? • Do you think the good and proper investigation management would make any difference in your investigation process? • If yes, please explain why.	
12.	• What do you think about external involvements in the investigation process of hacking cases? The external investigation would be other organization, other unit in	Cooperation with service providers is often essential. Since most cybercrime is transnational, cooperation with foreign

	your organization, or even other foreign organization. • What are they? • Do you think that the external aspects give contribution to the success of the investigation? • Please share your opinion, with example will be more appreciated.	authorities is very important.
13.	• Do you think the cooperation with other similar organization from other countries is required to combat the hacking cases or other IT & Cyber Crime? • Why and how does it (the cooperation with other country) suppose to be developed? • Has your organization developed the cooperation with similar organization from other country? Please mention names if possible. • What kind of cooperation does your organization develop with other country? Please explain.	Yes. The Council of Europe is cooperating with a large number of countries and organizations (including Interpol, Eurpol, United Nations, Organisation of American States, International Telecommunication Union and many others).

Thank you for your participation. This questionnaire is very meaningful for my findings.

Sincerely yours,
Petrus Reinhard Golose

Questionnaire

Subject	:	Investigation Management for Hacking or IT & Cyber Crime Case
Researcher	:	Petrus Reinhard Golose
Name Respondent	:	Steve Santorelli
Institution	:	Team Cymru
Position of Respondent	:	Manager of Investigations
Time	:	16:40 PST 5th October 2007
Place	:	Redmond, WA, USA

Please fill your answers in third columns:

No. (1)	Questions (2)	Answer (3)
1.	• In your country, do you have a special or dedicated unit to counter IT misconduct and/or cyber crime? • If, your answer is yes, please explain how the organization works and what is its aim and programs (both short term and long terms?)	Yes, in the USA responsibility for the investigation of breaches of computer crime legislation that falls under Federal remit is investigated by the FBI and the US Secret Service. Both agencies have specially trained agents in their field offices as well as clusters of specialist agents, analysts and support technicians at headquarters in Washington DC. Both agencies have significant other roles with a higher priority than cyber-crime but generally the majority of cases are devolved to the field offices where they are worked by agents with some specialist training. Major cases are supervised and co-ordinated from HQ but still generally worked by the field agents. The strength of these US Federal agencies is that they have Legal Attaché offices in US Embassies worldwide so they have the ability to action requests outside of the continental United States. [In the UK there is no longer any specialist squad with national responsibility. The NHTCU has been effectively disbanded and SOCA does not have a similar remit. Scotland Yard's Computer Crime Unit only has technical responsibility for London].
2.	• How long have you been involved in the	I was a police officer from 1994 until 2004,

	organization and what is your position? • Have you investigated cyber crime cases? • Please mention the case and if possible can I get the brief of such cases?	working at Scotland Yards Comouter Crime Unit from 2000 to 2004. I was a Detective Sergeant there supervising the unit when I left. I then left to work at Microsoft's Internet Crime Investigations Team from 2004 until 2007 and I now work as Manager of Investigations for the non-profit research group called Team Cymru. I have worked hundreds of cyber-crime cases over the years including successful investigations of viruses (for example, Gokar, Redessi, Leaves), hacking teams (for example, Fluffy Bunny) and Botnets (for example, Zotob). Some analysis on some of these cases is available on request.All involved extensive liaison with international law enforcement.
3.	• How do you or your organization handle the cyber crime cases? • How do you or your organization investigate such cases? • Do you have any standard procedure to deal with the investigation on cyber crime?	We proactively look through our data and refer cases to law enforcement. These reports detail who the criminal is and what they have done and these reports are sent directly to the law enforcement agency that has jurisdiction where the suspect resides. We also reactively investigate cases at the request of law

	• Would you please explain how the investigation process carried out by your organization? • Do you have any certain system specially established relating to such investigation? Please explain the details.	enforcement at no charge – we are funded by the commercial wing of the company. Each case, especially with the highly technical nature of the cases we deal with (often cases where specialist law enforcement have been unable to solve the case themselves) requires a customized approach so there is no standardized approach. Essentially the request come to me and I design an investigation plan which is provided to the allocated investigator. The investigator works through that plan and reports back to me with a brief summary of their findings. If appropriate, then that investigator will write up the investigation in a detailed reports with all the intelligence and I will review it and send it to the correct law enforcement agency. All our work is intelligence only – we will not support any of our work in court. Proactive cases are generally similar. We have dedicated intelligence databases to capture our proactive work online and we are currently designing a case management system.
4.	• Do you apply certain management system	Investigation management requires experience.

	when you or your organization handling the IT & Cyber crime cases? • Do you think it is necessary or even obligatory to apply a good and proper management in dealing with the investigation of IT & Cyber Crime cases? • What is your opinion about investigation management? What is it? And how does it work? Please feel free to give your own opinion	This is due to the high volume of cases and the fact that you can't possibly hope to solve all of them – these cases are too technical and take too long to work through. An experienced manager can generally tell which cases are a waste of time to lock into in much depth and which cases are worth working hard at. It is this experience that is hard to teach a non-police officer. My management style is to design a good initial investigative plan and then to make sure that I oversee the investigation at regular intervals (at least once a week) to make sure that the plan is still efficient and to keep things moving. Some investigators are naïve and need constant guidance to make sure they stay focused and do not over step the legal boundaries in the work they do on a case. They might also not realize when a case is dead and when they should move onto a new investigation. Good investigation management requires this experience and the ability to rapidly understand technical cases – where the gaps in a case are, where the clues are most likely to be found and

		to do this with multiple cases a day with investigators of different levels of technical proficiency.
5.	• During the investigation on cyber crime, do you have any problem which makes you or your organization cannot accomplish your work or your investigation? • Please explain, and share examples	When I was in law enforcement the biggest problems I had were jurisdictional – getting things done in different countries, as well as a lack of willingness by my management to give us the resources we needed to do the job right. We also lacked the training and equipment as well as facing issues with travel budgets and language as well as inadequate legislation and a general feeling that our senior management didn't really care about cyber crime.
6.	• Do you have any computer forensic laboratory to support your investigation on the cyber crime? • Is it in your internal organization or is it an independent laboratory that also prepared for investigating any crime including conventional crime as well as cyber crime? Why? And what is your opinion about that?	At Scotland Yard we used to rely on the central forensics lab which just did keyword searches, then we took on our own forensic training and we did our own forensics for our own highly technical hacking /malware cases. This was much better as we had pride and did a much more thorough job than a technician at the lab. A central general lab can't possibly have the time and high tech experience of investigation needed for forensics on computer crime cases. They can search for child porn pics and

		keywords but that is as far as they can do. You need an experienced police officer, preferably the office in the case (who arrested and interviewed the suspect and searched his house) to do this examination.
7.	• Do you have any special regulation against IT & Cyber Crime? • Please explain. And what is your opinion about that?	UK legislation is the Computer Misuse Act 1994 which is old now – it needs updating. US legislation is complex and appears also to be out of date. The law needs to be updated every few years to keep pace with technology advances but it is difficult to get time with the legislative bodies to fit this in – they are not used to changes in the law of this frequency.
8.	• Do you have regulation supporting digital evidence? • How does it work? • What is your opinion about it?	In the UK there are established principles regarding the fairness of evidence and these are based, for computer crime, on the Association of Chief Police Officers Evidential Guidelines for Computer Based Evidence. This is a document ratified by the senior officers from expert guidance. It also needs updating but in court the final arbiter of what is permissible is the judge and he bases his decision on expert witness testimony from independent experts hired by the prosecution and the defense – not

		the police.
9.	• During the last 5 years, how many IT & Cyber Crime cases have been reported, investigated and brought to court? • If any, do you think that number represented all the cases of IT & Cyber crimes happen in your country? Please explain	In the UK, not counting child porn cases, probably less than 20. That is probably less than 0.01% due to a host of reasons including crimes never being noticed, never being reported to the police, never being recorded by the police, never being investigated by the police, never making it to court and also being dropped at court.
10.	• Do you know "hacking"? • Is it one of the cyber crimes in your country? • Has it been regulated in a certain regulation? • What is your own opinion about it? • Do you think hacking is dangerous? • Do you think hacking also has to be combat? • Do you think hacking also has to be regulated in a certain law? • Please share your opinion	Yes, it's a clear breach of the Computer Misuse Act in the UK. See http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm and http://en.wikipedia.org/wiki/Computer_Misuse_Act: 1(1) A person is guilty of an offence if: a) He causes a computer to perform any function with intent to secure access to any program or data held in a computer; b) the access he intends to secure is unauthorized; and c) he knows at the time when he causes the computer to perform the function that this is

		the case. 'Hacking', when it is done with malicious intent, should be a crime everywhere in the world. It costs millions and can cause lives to be endangered..
11.	• Do you think it is necessary or even obligatory to establish a certain investigation management while you or your organization conduct an investigation on hacking cases? • Why and how does it supposed to be applied? • Do you think the good and proper investigation management would make any difference in your investigation process? • If yes, please explain why.	I am not sure I understand this question. Hacking cases need to be approached in exactly the same way as traditional investigations as I have outlined in my answer to question 4 above.
12.	• What do you think about external involvements in the investigation process of hacking cases? The external investigation would be other organization, other unit in your organization, or even other foreign organization. • What are they?	Police almost never have the technical expertise to successfully complete every stage of an investigation. From analysis of malware or log files to forensic examination of computers – I have seen both sides to this as a police officer and now as an industry

	• Do you think that the external aspects give contribution to the success of the investigation? • Please share your opinion, with example will be more appreciated.	person…industry help is essential to most cases. Some officers are reticent to use industry as there is often a cost implication as well as a trust issue – but trusted contacts are possible given time. I have plenty of examples, let me know if you want me to outline some of them later.
13.	• Do you think the cooperation with other similar organization from other countries is required to combat the hacking cases or other IT & Cyber Crime? • Why and how does it (the cooperation with other country) suppose to be developed? • Has your organization developed the cooperation with similar organization from other country? Please mention names if possible. • What kind of cooperation does your organization develop with other country? Please explain.	I have never had a major computer crime case that did not require the involvement and assistance of either foreign police or foreign industry experts. If you do a case that doesn't need foreign contacts then you are either very lucky or you are missing a lot of clues. It is best to develop links before you need them, by being represented at conferences, at HTCIA and SANS events. Networking on forensic forums and getting training slots on the courses of foreign police agencies on exchange programs. There are often lot s of people willing to work with you, all you have to do is ask – because they all know that one day they will need to pick up the phone and have a contact in your country to ask YOU for

		help. This is a small world of contacts as it is so highly specialized – it tends to be the same people involved in each major case – probably less than 50 police and industry specialists worldwide who are full time involved in international cyber crime investigations and have been for several years.

Thank you for your participation. This questionnaire is very meaningful for my findings.

Sincerely yours,
Petrus Reinhard Golose

FEEDBACK FORM

Subject : Investigation Management for Hacking or IT & Cyber Crime Case

Researcher : Petrus Reinhard Golose

Respondent : Michael C. Dehncke

Position of Respondent : Special Agent, FBI

No.	Questions	Explanation
1.	In your country, do you have a special or dedicated unit to counter IT misconduct and/or cyber crime? If, yes please explain how the organization works and what is its aim and programs (both short term and long terms?)	There are dedicated cyber crime units within several agencies in the United States. First, the FBI has a Cyber Division with 527 agents dedicated to cyber crime (out of 12,000 total agents). Every field office has agents assigned to cyber investigations. The US Secret Service also has a cyber branch with investigative responsibilities which overlap the FBI's in several areas including hacking and trafficking in access devices. Several of the large US Government

No.	Questions	Explanation
		Agencies have an Office of the Inspector General which has responsibility for investigating crimes committed within or against that agency. These OIG offices have investigators assigned to cyber investigations which effect their agencies. Many local law enforcement agencies also have detectives assigned to work cyber crime cases under state law. Within the FBI, cyber crime is the third highest investigative priority following counter-terrorism and counter-intelligence investigations. Within the cyber crime division, priority is assigned to investigations as follows: 1) computer intrusions; 2) crimes against children (child pornography and pedophiles

No.	Questions	Explanation
		who attempt to meet children over the internet) 3) Intellectual property right violations 4) Fraud (email scams, auction fraud, remailer schemes)
2.	How long have you been involved in the organization and what is your position? Have you investigated cyber crime cases? Please mention the case and if possible can I get the brief of such cases?	11 years. Special Agent assigned to Extra-territorial investigations. None that are specifically cyber crime, but several cases which involved elements of cyber crime. None of these cases have been made public, so I cannot discuss the specifics of them.
3.	How do you or your organization handle the cyber crime cases?	Our investigative procedures are the same for cyber crime cases as with any other type of investigation and

No.	Questions	Explanation
	How do you or your organization investigate such cases? Do you have any standard procedure to deal with the investigation on cyber crime? Would you please explain how the investigation process carried out by your organization? Do you have any certain system specially established relating to such investigation? Please explain the details.	are governed by the same internal regulations. The chief difference would be that because of the fleeting nature of digital evidence, as soon as the FBI becomes aware of an incident we take steps to preserve that evidence through preservation requests and court orders. The FBI has established the Internet Crime Complaint Center (IC3), an international clearing house for internet crime complaints. The IC3 receives complaints from all over the world, attempts to link them to other crimes, and refers the leads to the appropriate investigative agency.
4.	Do you apply certain management	The FBI applies the same

No.	Questions	Explanation
	system when you or your organization handling the IT & Cyber crime cases?	management system for cyber cases as for all investigations.
	Do you think it is necessary or even obligatory to apply a good and proper management in dealing with the investigation of IT & Cyber Crime cases?	Good and proper management is essential to ensure the protection of evidence and the successful prosecution of cyber cases.
	What is your opinion about investigation management? What is it? And how does it work? Please feel free to give your own opinion	Investigation management is the process by which cases are prioritized and overseen to ensure successful investigation and prosecution of subjects. The key to investigation management is to create a uniform process for conducting investigations so that evidence is properly handled and all investigative activity is properly documented.
5.	During the investigation on cyber crime, do you have any problem	Cyber crime cases are made more difficult due to the following:

No.	Questions	Explanation
	which makes you or your organization cannot accomplish your work or your investigation? Please explain, and share examples	1) subjects and evidence are often overseas; 2) electronic evidence is easily destroyed or tainted; 3) the technology is constantly changing, which requires the development of new investigative techniques and tools; 4) the proliferation of counter-enforcement tools such as anonymizers; 5) the massive volume of cyber crime being committed and the use of tools to target extraordinary numbers of victims.
6.	Do you have any computer forensic laboratory to support your investigation on the cyber crime? Is it in your internal organization or is it an independent laboratory that also	Each FBI field office has a Computer Analysis Response Team (CART) which has its own laboratory. In addition, the FBI Laboratory and the FBI Electronic Research Facility assist the field offices in their

No.	Questions	Explanation
	prepared for investigating any crime including conventional crime as well as cyber crime? Why? And what is your opinion about that?	analysis. The FBI also has special units dedicated to data wiretaps, pen registers, and email wiretaps. In certain situations, the FBI will contract with private companies to conduct forensic examinations of damaged or otherwise unique digital evidence.
7.	Do you have any special regulation against IT & Cyber Crime? Please explain. And what is your opinion about that?	Cyber crime is primarily prosecuted in the United States under the following statutes: 18 USC (United States Code) 1341: Mail fraud; 18 USC 1343: Wire fraud; 18 USC 1030: computer intrusion; 18 USC 1029: trafficking in access devices; 18 USC 1028: identity theft.

No.	Questions	Explanation
8.	Do you have regulation supporting digital evidence? How does it work? What is your opinion about it?	The introduction of evidence in criminal cases in the United States is governed by the Federal Rules of Evidence. Digital evidence is treated the same way as documentary evidence under these rules, which are subject to interpretation by the courts which has led to a series of rules spelled out in case law.
9.	During the last 5 years, how many IT & Cyber Crime cases have been reported, investigated and brought to court? If any, do you think that number represented all the cases of IT & Cyber crimes happen in your country? Please explain	The best I can come up with is from the FBI website. This represents a very small percentage of all of the cyber crime which are committed: From January 1, 2006 – December 31, 2006, the IC3 website received 207,492 complaint submissions. This is a 10.4% decrease when compared to 2005 when 231,493 complaints were received. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet. In 2006, IC3 processed more than 200,481 complaints that support Internet crime investigations by law enforcement and regulatory agencies nationwide. These complaints were composed of many different fraud types such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child

No.	Questions	Explanation
		pornography. All of these complaints are accessible to federal, state, and local law enforcement to support active investigations, trend analysis, and public outreach and awareness efforts. From the submissions, IC3 referred 86,279 complaints of crime to federal, state, and local law enforcement agencies around the country for further consideration. The vast majority of cases were fraudulent in nature and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was $198.44 million with a median dollar loss of $724.00 per complaint. This is up from $183.12 million in total reported losses in 2005. Other significant findings related to an analysis of referrals include: • Internet auction fraud was by far the most reported offense, comprising 44.9% of referred complaints. Non-delivered merchandise and/or payment accounted for 19.0% of complaints. Check fraud made up 4.9% of complaints. Credit/debit card fraud, computer fraud, confidence fraud, and financial institutions fraud round out the top seven categories of complaints referred to law enforcement during the year. • Of those individuals who reported a dollar loss, the highest median losses were found among Nigerian letter fraud ($5,100), check fraud ($3,744), and other investment fraud ($2,695)

No.	Questions	Explanation
		complainants. • Among perpetrators, 75.2% were male and half resided in one of the following states: California, New York, Florida, Texas, Illinois, Pennsylvania and Tennessee. The majority of reported perpetrators were from the United States. However, a significant number of perpetrators where also located in United Kingdom, Nigeria, Canada, Romania, and Italy. • Among complainants, 61.2% were male, nearly half were between the ages of 30 and 50 and one-third resided in one of the four most populated states: California, Texas, Florida, and New York. While most were from the United States, IC3 received a number of complaints from Canada, Great Britain, Australia, India, and Germany. • Males lost more money than females (ratio of $1.69 dollars lost per male to every $1.00 dollar lost per female). This may be a function of both online purchasing differences by gender and the type of fraudulent schemes by which the individuals were victimized. • Electronic mail (e-mail) (73.9%) and webpages (36.0%) were the two primary mechanisms by which the fraudulent contact took place. • Recent high activity scams seen by IC3 include hit man scams, phishing attempts associated with spoofed sites, and counterfeit checking scams.

No.	Questions	Explanation
10.	Do you know "hacking"?	Yes
	Is it one of the cyber crimes in your country?	Yes
	Has it been regulated in a certain regulation?	18 USC 1030: computer intrusion
	What is your own opinion about it?	hacking is a serious problem in that it causes many millions of dollars in damages each year, and the waste of significant resources in preventing hacking attacks.
	Do you think hacking is dangerous?	Hacking is typically not dangerous except in a financial sense. Most hacking can be prevented through the use of prevention tools and proper security procedures. Hacking has changed in recent years in that in the
	Do you think hacking also has to be combat?	
	Do you think hacking also has to be regulated in a certain law?	
	Please share your opinion	

No.	Questions	Explanation
		past it was typically done for bragging rights whereas now it is committed for financial gain. Stronger penalties for hacking crimes would reduce the number of incidents.
11.	Do you think it is necessary or even obligatory to establish a certain investigation management while you or your organization conduct an investigation on hacking cases? Why and how does it supposed to be applied? Do you think the good and proper investigation management would make any difference in your investigation process?	Hacking cases are managed in the same manner as all other FBI investigations. Management protocols must be uniformly applied to all cases from their inception in order to ensure that all are held to a high standard. Proper management makes a significant difference in the process, and can make the difference between successfully prosecuting a subject and seeing him go free.

No.	Questions	Explanation
	If yes, please explain why.	
12.	What do you think about external involvements in the investigation process of hacking cases? The external investigation would be other organization, other unit in your organization, or even other foreign organization. What are they? Do you think that the external aspects give contribution to the success of the investigation? Please share your opinion, with example will be more appreciated.	The FBI typically has external involvement in two situations: 1) a computer crime which is transnational in character and requires the cooperation of foreign law enforcement agencies to obtain evidence or access to subjects. These cases cannot be investigated without the assistance of the foreign police agency and any success is a joint effort. 2) In cases where a computer network is attacked, the FBI relies heavily on the company or agency computer security and network specialists to provide a starting point and the initial evidence related to the intrusion. Particularly in the instance of complex networks, this assistance is

No.	Questions	Explanation
		crucial to investigators.
13.	Do you think the cooperation with other similar organization from other countries is required to combat the hacking cases or other IT & Cyber Crime? Why and how does it (the cooperation with other country) suppose to be developed? Has your organization developed the cooperation with similar organization from other country? Please mention names if possible. What kind of cooperation does your organization develop with other country? Please explain.	Cooperation between national police agencies is absolutely essential due to the transnational nature of cyber crime. The cooperation is necessary in almost any crime which is transnational in character and requires the cooperation of foreign law enforcement agencies to obtain evidence or access to subjects. These cases cannot be investigated without the assistance of the foreign police agency and any success is a joint effort. The FBI has active relationships with virtually every developed country in the world through IC3 as well as through individual joint investigations

No.	Questions	Explanation
		and MLATs. Cooperation varies from simply referring leads on cyber crime to other countries through the IC3, to full partnerships on cases of mutual interest in which investigators from both countries will work together for extended periods of time.

Please give note about when and where you are completing the above feedback form.

Time : 1530 15 September 2007

Place : Los Angeles, California, USA

FEEDBACK FORM

Subject : Investigation Management for Hacking or IT & Cyber Crime Case

Researcher : Petrus Reinhard Golose

Respondent : MAN Chi-hung, Alan

Position of Respondent :Senior Superintendent, Head of Technology Crime Division, Commercial Crime Bureau, HongKong Police Force

No.	Questions	Explanation
1.	In your country, do you have a special or dedicated unit to counter IT misconduct and/or cyber crime? If, yes please explain how the organization works and what is its aim and programs (both short term and long terms?)	Yes. Hong Kong Police Force has a dedicated unit called "Technology Crime Division (TCD)" to counter IT crimes and cyber attack. TCD comes under the Commercial Crime Bureau and is headed by a Senior Superintendent and a Superintendent of Police. Basically, TCD comprises with two sections: 1) Operations and 2) Computer Forensics. The Operations Section responsible to investigate complex and sophisticated technology crimes in Hong Kong. It also has a crime prevention role to educate the public from falling prey to the ever-increasing computer crimes. The Computer Forensics Section provides centralized digital evidence preservation and analysis service of standalone computers, computer

No.	Questions	Explanation
		networks and other digital storage media. Besides, a dedicated training team regularly prepares training to the whole Division and other members of LEAs to broaden the investigation capability in IT crimes. To effectively carry out the enforcement actions, TCD based on the following eight strategies for their shot term and long term planning:- • Maintaining a professional investigation capability; • Broadening the investigation capability within the Force; • Developing accredited computer forensics; • Proposing changes in laws and policies; • Prevention and education; • Enhanced liaison with private sectors; • Liaison with local and overseas LEAs; • Continuing to develop best practices to keep up with advances in technology.
2.	How long have you been involved in the organization and what is your position? Have you investigated cyber crime cases?	I have been attached to the organization since April 2005 and my position is the Head of Technology Crime under the Commercial Crime Bureau. We do investigate various kinds of cyber crime, which included hacking, online fraud, BotNets, email scams, phishing...etc. However, we have to obey the Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong

No.	Questions	Explanation
	Please mention the case and if possible can I get the brief of such cases?	Kong, to maintain data privacy and confidentiality of the cases. As a result, we can't provide you the brief of the cases.
3.	How do you or your organization handle the cyber crime cases? How do you or your organization investigate such cases? Do you have any standard procedure to deal with the investigation on cyber crime? Would you please explain how the investigation process carried out by your organization? Do you have any certain system specially established relating to such	Hong Kong Police Force is the main law enforcement agency in Hong Kong to investigate cyber crimes. Given the wide variation of technical complexity in cyber crime investigations, the responsibility for the investigation of cases laid between various police division, district, region and the police headquarters. To effectively del with cyber crime, we have developed a number of general guidelines governing the investigation of a number of cyber crime cases, e.g. online game fraud. However, with the advance and frequent changing in IT, there is no hard and fast rule for the investigation process and the proposed guidelines need to be reviewed within a certain period of time.

No.	Questions	Explanation
	investigation? Please explain the details.	
4.	Do you apply certain management system when you or your organization handling the IT & Cyber crime cases? Do you think it is necessary or even obligatory to apply a good and proper management in dealing with the investigation of IT & Cyber Crime cases? What is your opinion about investigation management? What is it? And how does it work? Please feel free to give your own opinion	To manage the large number of cases, including IT crimes, being reported to the police, Hong Kong Police Force has developed a Communal Information System to handle information required for the daily operations in the Force. I think there is a necessity to apply a good and proper management in dealing with the investigation of IT crimes. The case investigation management should include the functions of maintaining and interrogating operational data that encompass case processing, bail processing, property administration and matching, detained persons and their movements and property, preparation of charge sheets, routine enquiries as well as statistics and reports generations and archiving. Those are the information normally required for every crime cases, we should systemically process those information to enhance the effectiveness and efficiency of the organization in handling IT crimes.
5.	During the investigation on cyber crime, do you have any problem which makes you or your organization	IT crime is borderless and the cross jurisdiction issues sometimes cause problems in the context of investigation. For example, hacking is not an offence in Mexico but a Mexican hacker illegally intruded and

No.	Questions	Explanation
	cannot accomplish your work or your investigation? Please explain, and share examples	damaged a computer in Hong Kong through the Internet, should the hacker be dealt with by the laws of Hong Kong or the laws in Mexico? Can the LEA in Mexico helps us to collect the evidences against the hacker? I believed that the most effective way to tackle the global nature of the problems is to through international support and cooperation from law enforcement agencies around the world. Furthermore, we need to take active steps in developing our own professional investigative capability, as well as an accredited computer forensics capability for addressing the changing scene of technology crime.
6.	Do you have any computer forensic laboratory to support your investigation on the cyber crime? Is it in your internal organization or is it an independent laboratory that also prepared for investigating any crime including conventional crime as well as cyber crime? Why? And what is your opinion about that?	Yes. A computer forensic laboratory is established within the Hong Kong Police Force to provide centralized digital evidence preservation and analysis service of standalone computers, computer networks and other digital storage media to our Force members. In Hong Kong, apart from the Hong Kong Police Force, other LEAs such as the Customs & Excise Department, the Immigration Department and the Independent Commission Against Corruption Department also have their own computer forensics laboratory. In my opinion, the trend tends to establish a centralized forensics laboratory for well use of resources and efficiency saving.

No.	Questions	Explanation
7.	Do you have any special regulation against IT & Cyber Crime? Please explain. And what is your opinion about that?	The main piece of legislation against IT crime is the Computer Crimes Ordinance. Enacted in 1993, it has, through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210), broadened the coverage of existing offences to cover computer elements. A complete list of the offences can be found in attached table and the current legislations could cover nearly all the aspect of IT crime. However, due to the ever changing IT environment, the legislations also need to review to combat the changes.
8.	Do you have regulation supporting digital evidence? How does it work? What is your opinion about it?	In Hong Kong, we have an evidence ordinance, Cap 8, laws of Hong Kong governing the usage of digital evidence. The principles for the provisions accepted by court are laid out in detail in documentary evidence in Criminal Proceeds from Computer Records at sec 22A of that Ordinance. The ordinance covers the essential element in the presentation of evidence to the court of laws and be applicable to various kinds of IT crime prosecution.
9.	During the last 5 years, how many IT & Cyber Crime cases have been reported, investigated and brought to court?	The total number of technology crime reports for 2005, 2006 and the first six months of 2007 are at the attached. However, we do not keep figures for the cases that had brought to court. Similar to traditional crimes, there exist un-reported cases and therefore the figures could not represent all the cases of IT crimes in our jurisdiction.

No.	Questions	Explanation
	If any, do you think that number represented all the cases of IT & Cyber crimes happen in your country? Please explain	
10.	Do you know "hacking"? Is it one of the cyber crimes in your country? Has it been regulated in a certain regulation? What is your own opinion about it? Do you think hacking is dangerous? Do you think hacking also has to be combat? Do you think hacking also has to be	Yes. In Hong Kong, we defined "hacking" as "Unauthorized access to computer by telecommunications" or "Access to computer with criminal or dishonest intent". As refer to the legislations listed in part 8, we have laws to regulate this kind of offence. Hacking is illegal when the hacker gains entry to a computer without lawful authority or reasonable excuse. This is one of the major methods used by criminals to obtain information from victims for monetary gain or further use in other illegal activities. As a result, it is necessary to regulate the offence by legislations.

No.	Questions	Explanation
	regulated in a certain law? Please share your opinion	
11.	Do you think it is necessary or even obligatory to establish a certain investigation management while you or your organization conduct an investigation on hacking cases? Why and how does it supposed to be applied? Do you think the good and proper investigation management would make any difference in your investigation process? If yes, please explain why.	Due to the complexity and diversification of IT crimes, cyber crime investigators need to be equipped with fundamental knowledge of IT before they could conduct investigation against the crime. As a result, a cyber crime investigator should be capable to investigate various kinds of IT crimes, including hacking. Though it may be good if someone specialized in the investigation of specific type of crime, it is not a good decision from the management point of view to train an investigator who could only capable in hacking investigation.
12.	What do you think about external	Hacking normal required the usage of Internet to gain access into the

No.	Questions	Explanation
	involvements in the investigation process of hacking cases? The external investigation would be other organization, other unit in your organization, or even other foreign organization. What are they? Do you think that the external aspects give contribution to the success of the investigation? Please share your opinion, with example will be more appreciated.	victim's computer. The traces left behind by a hacker at the victims include IP address, the files illegally created at the computer and relevant logs recording the intrusion. In order to trace the hacker, we require the cooperation of Internet Service Providers to provide us the subscribers of the IP address. If the service provider is outside our jurisdiction, request to overseas law enforcement to obtain from their Internet Service providers are required. If we cannot obtain this information, it will cause a great implication to our investigation. Sometime we have no choice but to curtail our investigation.
13.	Do you think the cooperation with other similar organization from other countries is required to combat the hacking cases or other IT & Cyber Crime?	Definitely, IT crime is borderless and requires international support and cooperation from law enforcement agencies around the world. This kind of cooperation is established on the partnership amongst law enforcement agencies in their mutual and increasingly connected fight against IT crime.

No.	Questions	Explanation
	Why and how does it (the cooperation with other country) suppose to be developed? Has your organization developed the cooperation with similar organization from other country? Please mention names if possible. What kind of cooperation does your organization develop with other country? Please explain.	Besides the Interpol network, Hong Kong has been actively participated in the "24-Hour Contacts for International High-Tech Crime" under the G8 Subgroup on High-tech Crime. In addition, the Hong Kong Police is also a dedicated member of the Japan cybercrime Technology Information Network System (CTINS) and participated into various kinds of conferences to build up relationship with other cyber crime investigation units. We will provide relevant assistance to overseas counterparts upon the receipt of their requests through official channel, the Interpol or the Mutual Legal Assistance Treaty.

Please give note about when and where you are completing the above feedback form.

Time : On 2007-09-24

Place : Hong Kong

Computer Related Crimes in Hong Kong

Section, Chapter	*Provisions*	*Maximum Penalty*
s.27A, Telecommunications Ordinance, Cap. 106	Unauthorized access to computer by telecommunications	Fine of HK$20,000
ss.59-60, Crimes Ordinance, Cap. 200	Destroying or damaging property – extending the meaning of "property" to include "misuse of a computer" such as altering, erasing and adding program or data into a computer or computer storage medium and causing a computer to function differently	10 years' imprisonment
s.85, Crimes Ordinance, Cap. 200	Making false entry in bank book, etc. – extending the meaning of making false entry to falsification of the books of account kept at any bank in electronic means	Life imprisonment
s.161, Crimes Ordinance, Cap. 200	Access to computer with criminal or dishonest intent	5 years' imprisonment
s.11, Theft Ordinance, Cap. 210	Burglary – extending the meaning of "unlawful damage" to include altering, erasing and adding program or data into a computer or computer storage medium	14 years' imprisonment
s.19, Theft Ordinance, Cap. 210	False accounting – extending the meaning of "record" to include that kept by means of a computer	10 years' imprisonment
s.4, Copyright Ordinance, Cap. 528	Including computer programs within the meaning of literary works, which are in turn copyright protected works	Not applicable
s.26, Copyright Ordinance, Cap. 528	Including the making available of copies of copyright works via the Internet as acts restricted by copyright	Not applicable
ss.118-9, Copyright Ordinance, Cap. 528	Copy without the licence of the copyright owner, an infringing copy of a copyright work	4 years' imprisonment
s.21, Control of Obscene and Indecent Articles Ordinance, Cap. 390	Prohibition on publishing obscene articles – also applies to the display of obscene articles on the Internet	3 years' imprisonment and fine of HK$ 1 million
Electronic Transactions Ordinance, Cap. 553	Giving electronic records and digital signatures the same legal status as that of their paper based counterparts	Not applicable
Gambling Ordinance, Cap.	Considerable amendments are made in	7 years' imprisonment and

Section, Chapter	*Provisions*	*Maximum Penalty*
148	2002 to criminalize:- ● Overseas bookmaking activities targeting Hong Kong; ● HK people betting with overseas bookmakers; ● Promoting or facilitating of overseas bookmaking activities;	fine of HK$ 5 million
Prevention of Child Pornography Ordinance, Cap. 579	● "Child pornography" includes computer-generated image, data stored in a form capable of conversion into a child pornography article; ● "Distribute" includes any means of electronic transmission; ● printing, making, producing reproducing, copying, importing, exporting, publishing and possessing child pornography are criminalized	8 years' imprisonment and fine of HK$ 2 million
Unsolicited Electronic Messages Ordinance Cap. 593	● Initiating transmission of multiple commercial electronic messages with intent to deceive or mislead recipients as to source of messages	8 years' imprisonment

Technology Crime – Statistics

Title of Offence	2005	2006	2007 (Jan - Jun)
Unauthorized Access to Computer by Telecommunication	8	6	2
Access Computer with Criminal or Dishonest Intent	441	471	173
Criminal Damage	6	5	2
Obtaining Property by Deception	145	193	105
Obtaining Services by Deception	9	12	6
Thefts (E-banking Related)	3	0	1
Thefts (Others)	20	24	9
Child Pornography	6	6	5
Criminal Intimidation	6	6	1
Others	9	18	14
Total	653	741	318
Detection Rate (TCD only)	76.9%	63.6%	84.6%
Detection Rate (Overall)	9.5%	9.98%	13.2%

PANDUAN PENANGANAN BUKTI DIGITAL

(Petrus Reinhard Golose)

Berbagai sumber bukti digital dapat ditemukan dalam suatu Tempat Kejadian Perkara (TKP). Sangat penting bahwa sumber-sumber tersebut diidentifikasi dan ditangani secara benar. Sebagian besar sumber barang bukti biasanya berupa komputer akan tetapi bisa juga berupa sumber lain.

Untuk langkah awal, hal-hal yang dapat dilakukan oleh penyidik adalah:

- Mengamankan TKP;
- Apabila ada proses pencetakan, biarkan mesin printer tersebut menyelesaikan proses pencetakannya;
- Hanya petugas yang berkepentingan diperbolehkan masuk ke TKP;
- Jangan menerima saran dari pemakai (tersangka) atau pemilik komputer tersebut;
- Apabila komputer tidak aktif, jangan mengaktifkan/menyalakan;
- Bila dimungkinkan hubungilah ahli forensik komputer misalnya melalui sambungan telepon.

Dalam melakukan penyitaan ada 2 kondisi yang mungkin terjadi yaitu komputer dalam kondisi menyala (aktif) dan komputer dalam kondisi tidak menyala (tidak aktif). Terhadap kondisi-kondisi tersebut ada beberapa tindakan yang dapat dilakukan.

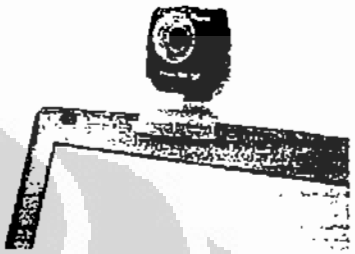
Pertama, apabila komputer dalam kondisi tidak aktif, hal yang dapat dilakukan yaitu:

- Harus dipastikan komputer tersebut tidak aktif, bila tidak tahu anggaplah komputer itu sudah diaktifkan (kadangkala laptop menyala bila tutupannya dibuka);
- Ambil gambar semua bagian komputer termasuk rangkaian sistem dan semua kabel yang terhubung ke alat lain;
- Ambil gambar layar komputer dan/atau catat semua program yang sedang beroperasi;
- Kalau laptop, lepaskan baterainya;

- Berikan label pada semua kabel dan soketnya agar bisa digabungkan kembali pada saat rekonstruksi.

Kedua, apabila komputer dalam kondisi aktif, hal yang dapat dilakukan yaitu:

- Matikan sambungan komputer dari akses remote (apabila memungkinkan) sebagai contoh: telpon dan modem;
- Pisahkan komputer dari kamera *Movie Digital*;

- Apabila diduga bahwa di dalam komputer terdapat jaringan, mintalah bantuan dari ahli forensik komputer sebelum menyentuh apapun;
- Apabila program perusak sedang aktif dan akan menyebabkan hilangnya bukti (contoh: program format, hapus, merusakkan bukti, dll), segeralah tarik kabel listrik dari komputer tersebut;
- Mencatat atau mengambil foto yang ditunjukkan di layar komputer;
- Bila anda bisa melihat *screensaver* atau layar komputernya kosong (hitam), tekan tombol apapun atau gerakkan *mouse*-nya dan layar akan menyala kembali bila tidak dikunci dengan *password*;
- Catat tanggal dan waktu saat menggerakkan/menyentuh *mouse* atau *keyboard*.

Untuk komputer dalam jaringan (2 komputer atau lebih yang digabungkan), hal-hal yang dapat dilakukan yaitu:

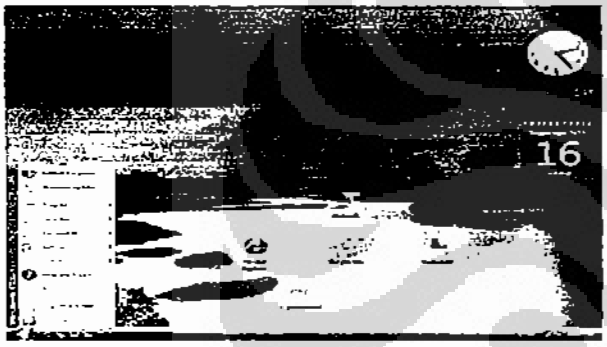
- Jangan disentuh - minta bantuan dari ahli forensik komputer.
- Apabila anda menarik kabel listrik atau mengganggu secara tidak teratur dapat: Mengganggu bisnis yang sah; Menciptakan keadaan dimana Anda bisa dituntut; dan Mengganggu sistem komputer.
- Mengamankan TKP sampai ahli forensik dapat menyarankan cara menangani secara sah/benar.

Untuk sistem Laptop, hal-hal yang dapat dilakukan yaitu andaikata tidak dapat menemukan atau mencabut baterai di dalam laptop, tekanlah tombol "*power*" selama 30 detik (sampai layar menjadi hitam) yang disebut "*hard power down*" (mematikan komputer secara cepat).

Untuk komputer (PC) yang berdiri sendiri, hal-hal yang dapat dilakukan yaitu:

- Sebelum mencabut kabel listrik dari sistem komputer penting sekali untuk mengetahui sistem operasi apa yang digunakan komputer tersebut karena tiap sistem memakai cara berbeda untuk menanganinya. Setelah sistem operasi diidentifikasikan, baru bisa dilaksanakan langkah penanganan. Beberapa contoh *Screenshots* berikut dengan teknik-teknik untuk mengidentifikasikannya:

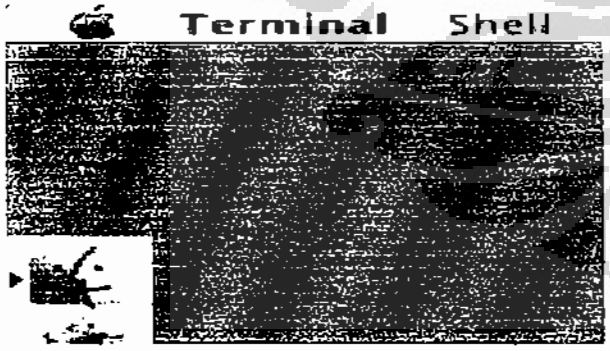
Windows Vista



Perhatikan beberapa indikasi sistem Windows:

- *Recycle Bin*
- *My Computer*
- Tombol *Start*

Apple



Bila terdapat lambang berikut berarti memakai sistem Apple Macintosh:

- Simbol ini terdapat pada komputer yang gunakan system Apple

Linux GUI

Terdapat banyak Linux GUI dan kebanyakan mirip sistem Windows, bahkan ada yang persis sama dengan sistem Windows. Biasanya Linux atau Unix GUI tidak

punya tombol 'Start', lambang "My computer" atau "Recycle bin". – Tetapi tidak selalu begitu – bila tidak yakin – minta bantuan dari ahli forensik komputer.

DOS Command Line

Yang berikut berarti sistem DOS

- Menunjukkan drive yang berjalan (C:\>)

Linux / Unix Command Line

Yang berikut berarti command line Linux / Unix

- Tidak ada huruf "drive"
- Simbol seperti #, @ or# ataupun !

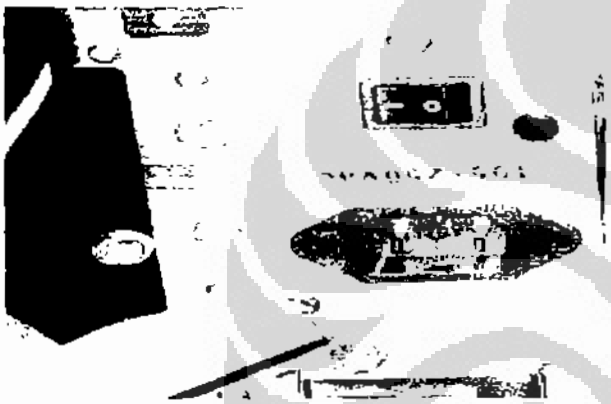
Cara mematikannya (*Shut Down*), setelah sistem operasi telah diidentifikasikan, mematikan komputernya dengan cara berikut:

Sistem Operasi	**Cara Mematikan**
DOS	Copot kabel
Windows 3.1	Copot kabel
Windows 98	Copot kabel
Windows NT	Copot kabel
Windows NT Server	*Shut down*
Windows 2000	Copot kabel
Windows 2000 Server	*Shut down*
Windows XP	Copot kabel
Linux	*Shut down*

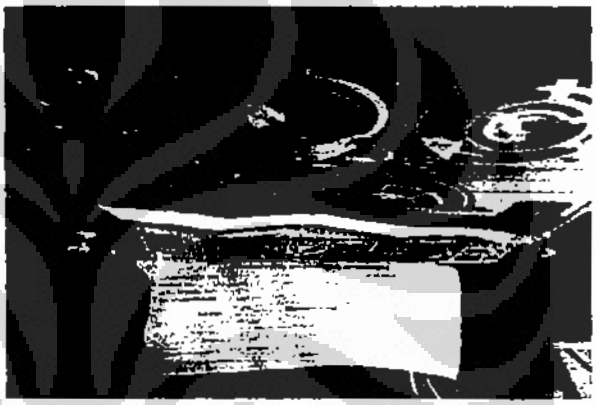
Unix	*Shut down*
Macintosh	Copot kabel

'Mencopot kabel' berarti tarik kabel listrik dari belakang PC - bukan dari dinding.

- '*Shut down*' berarti memakai sistem operasi untuk mematikannya secara biasa. Andaikata Anda tidak tahu cara mematikan ('*shut down*') dan tidak ada ahli forensik komputer yang ikut serta, Anda harus 'tarik kabel' dan mencatat jam dan tanggal tindakan tersebut serta alasan dilakukan. Ahli forensik komputer mungkin juga menyarankan untuk 'copot kabel' daripada *shut down*.



Tarik kabel listrik



Menutup colokan listrik untuk mencegah kecelakaan

- Setelah sistem dimatikan/*shut down* Anda harus mencatat secara resmi (dengan foto, video atau sketsa atau juga dengan menggabungkan ketiga cara tersebut).
- Dengan teliti membongkar alat dan melabel masing-masing komponen barang bukti (yaitu suatu komputer akan mempunyai nomor exhibit, akan tetapi *keyboard*, monitor dan *mouse* akan mempunyai nomor exhibit yang sama dengan nomor bagian yang berbeda);
- Memastikan bahwa semua alat yang sedang disita sudah diisi dan dilengkapi label exhibit. Apabila prosedur ini tidak dilakukan bisa menyebabkan masalah berkelanjutan di kemudian hari (di pengadilan);

Catatan penting:

- Cari tempat penyimpanan kertas kerja, buku harian, dll. untuk *password* atau untuk barang-barang lain yang menarik.
- Tanyakan kepada pemakai jika ada *ID* dan *Password* - jika diberi catat informasinya di buku catatan Anda.
- Buat catatan rinci untuk semua tindakan yang dilaksanakan.
- Pastikan semua bagian komputer ditemukan, khususnya bagian sumber daya untuk laptop.
- Identifikasi pada sketsa semua komputer atau perlengkapan yang disita.
- Foto TKP-nya dan layar komputer yang relevan (jika memungkinkan).
- Catat jam dan tanggal saat mematikan alat komputer
- Tutup colokan listrik dengan memakai selotip.
- Bungkus dengan memakai kantong barang bukti yang sudah disiapkan untuk ditransportasikan bila isi kantong tersebut adalah barang pecah belah.

PDA dan alat yang mirip

PDA menyimpan data di dalam memori dan jika sumber daya hilang ada kemungkinan besar data tersebut bisa hilang. Hal yang dapat dilakukan yaitu:

- Jika PDA mati/tidak dinyalakan – JANGAN DINYALAKAN
- Masukkan PDA ke dalam amplop tertutup sebelum dimasukkan ke dalam kantong barang bukti yang sah supaya tidak nyala secara tidak sengaja.
- Jika memungkinkan, pasang kabel listrik utama ke PDA atau juga PDA dimasukkan ke cradle-nya dan kabel listriknya dibiarkan keluar dari kantong barang bukti supaya PDA bisa tetap di-*charge*. Sebaiknya ini dilakukan secepat mungkin setelah tiba di kantor/ laboratorium forensik;
- Bila alat dalam keadaan AKTIF/NYALA
- Pertimbangkan juga alat dimatikan dengan memakai tombol ON/OFF dan dibungkus/ dikantongkan seperti dijelaskan di atas;

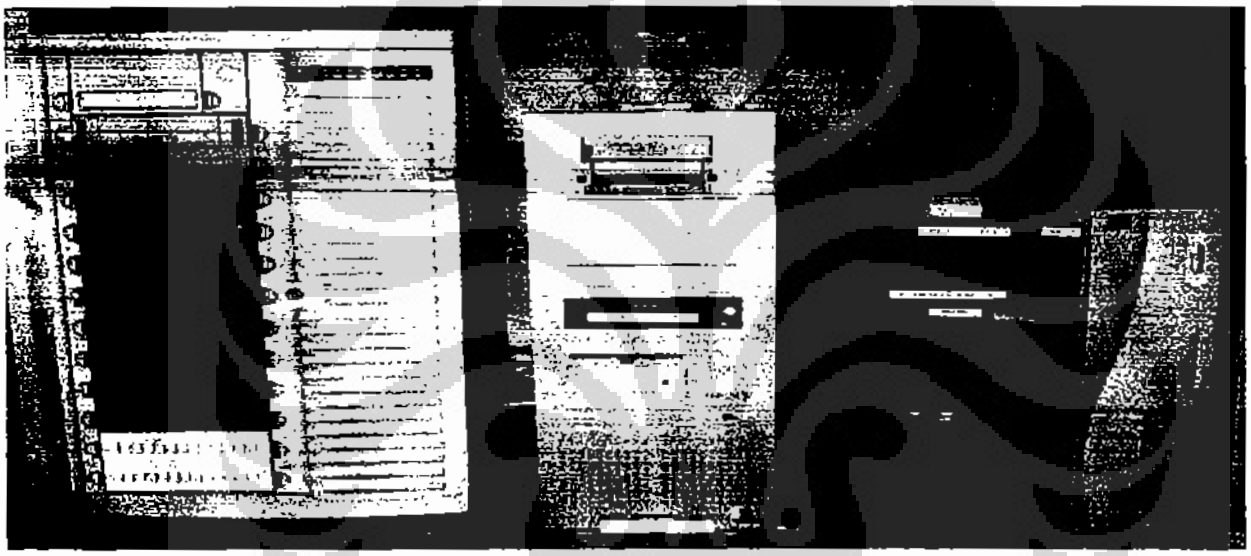
Andaikata Anda tidak pasti dengan apa yang harus dilakukan – minta bantuan forensik profesional.

- Membawa PDA ke ahli foresik komputer secepat mungkin dengan semua cadangan yang terkait (power, cradle, buku pedoman, spare memory dll);
- Baterai PDA harus diperiksa dan diganti secara rutin atau di-*recharged* supaya barang bukti tidak hilang/lenyap.

Apa yang harus disita

Berikut ini adalah beberapa contoh komponen yang harus dicari pada waktu pertama masuk lokasi TKP.

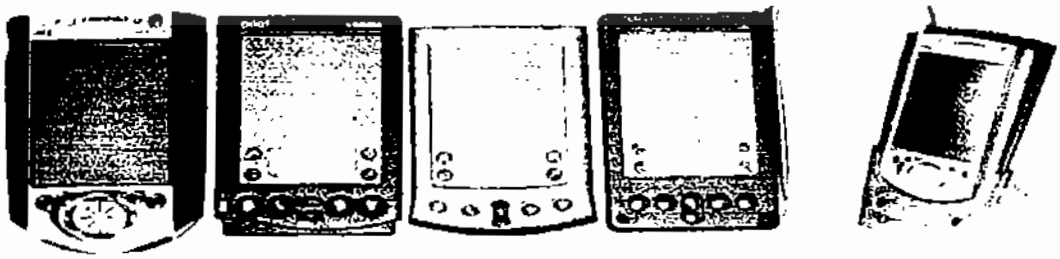
Komputer



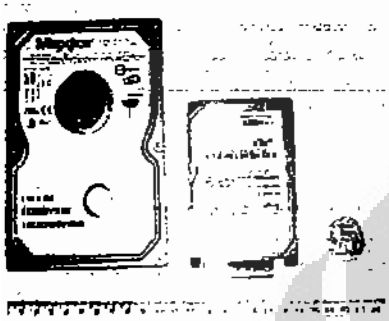
Server **Tower** **Mini Tower** **Desktop (berdiri)**

PDA

Beberapa contoh PDA, Cradle dan Charger.

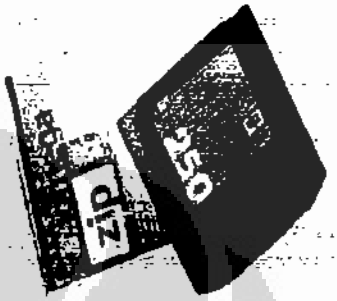


Diskette



Hard Disk (PC dan Laptop)

Floppy Disk



Zip Disk

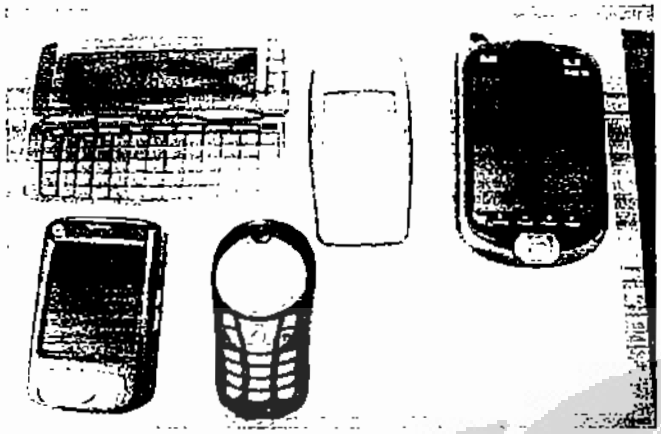
Pita *Backup – Back-up Tape* (berbagai macam pita rekaman)

DLT Travan AIT DDS 3/4

Alat Penyimpanan Data Lain (berbagai alat USB drive memori atau kartu memori)

Mobile Phone

Beberapa contoh *Mobile Phone*.



Berbagai Alat lain

USB (1 Gb) memori di dalam jam tangan

Kamera di dalam jam tangan

Alat lain yang harus disita misalnya alat yang diluar komputer (contoh: hard disk); CD dan DVD (ada kemungkinan CD atau DVD ini tersembunyi diantara CD musik atau DVD film); Kunci komputer; Buku Pedoman; Modem; Catatan kertas atau dari areal sekitarnya; *Power Supply*; Alat untuk jaringan *Wireless*.

Selain itu juga perlu dipertimbangkan oleh penyidik untuk melakukan penyitaan terhadap apakah alat-alat berikut seperti mesin penjawab telepon (*answering machines*), telepon, mesin dikte, sistem *e-mail* yang digabung langsung ke telepon, mesin Fax, Pager dan alat lain yang dapat menyimpan data secara elektronik.

Ada beberapa informasi yang perlu diketahui oleh penyidik misalnya adakah kunci untuk tas komputer apabila memakai kunci gembok; nama *password* untuk pengoperasian komputer; *Email address* yang sedang dipakai beserta *password*.

Peralatan yang harus disiapkan dalam melakukan forensik komputer yaitu *anti static band*; Kamera (plus cadangan film); Kantong barang bukti; Label barang bukti; Sarung tangan; Pena yang tintanya tidak dapat dihapus; *Labeller* (plus kaset cadangan); dan buku nota dan pena.