# BAB 4

# ANALISIS DAN PENGUJIAN SISTEM

## 4.1. Hasil Pengujian dan Analisis Sistem

### 4.1.1. Pengujian dan Analisis Pemindaian Frekuensi

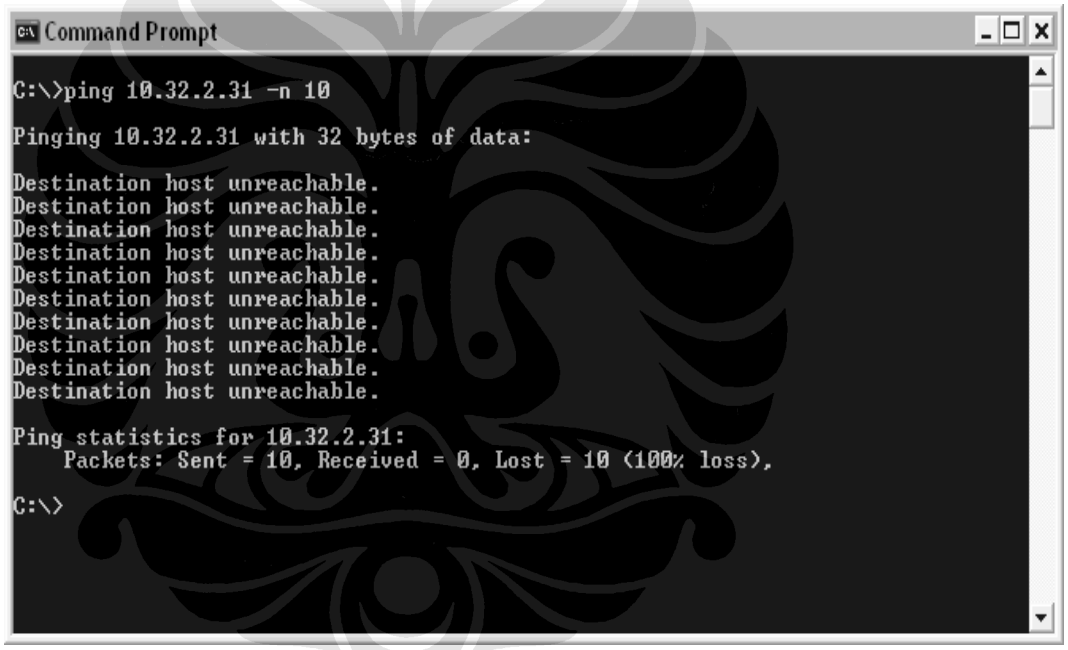
Pengujian pertama yang dilakukan adalah pengujian pemindaian akses poin WiMax. Sebelum melakukan koneksi tiap SS melakukan pemindaian frekuensi-frekuensi sesuai dengan yang yang telah dikonfigurasi pada terminal CPE yang digunakan. Apabila terdapat akses poin WiMax terletak dalam jangkauannya,maka terminal pengguna tersebut otomatis akan mengenalinya. Pada pengujian kali ini perangkat CPE dan akses poin WiMax menggunakan frekuensi 2,5 GHz.


Gambar 4.1 Pemindaian Akses Poin WiMax yang Tersedia

Dari Gambar 4.1 dapat dilihat bahwa stasiun pengguna mendeteksi hanya ada satu akses poin WiMax yang tersedia pada jangkauannya. Pada mode seperti

ini stasiun pengguna tersebut sbenarnya secara fisik sudah mendapatkan sinyal dari akses poin WiMax tersebut, namun koneksinya belum terbentuk dan tidak dapat melakukan transfer data. Hal ini bisa dilihat dari nilai RSSI-nya yang sebesar -25 dBm dan CINR-nya sebesar 28 dB.

Untuk membentuk koneksi, stasiun pengguna tersebut harus melakukan inisiasi dimana ia mengirimkan permintaan koneksi dengan menyertakan data identitas terminal dan kredensial yang disertakannya untuk di autentikasi oleh stasiun utama. Karena belum terkoneksi, maka stasiun pengguna tersebut belum dapat melakukan transfer data apapun. Hal ini bisa dilihat dari hasil tes ping ke server EMS yang berada pada stasiun utama.

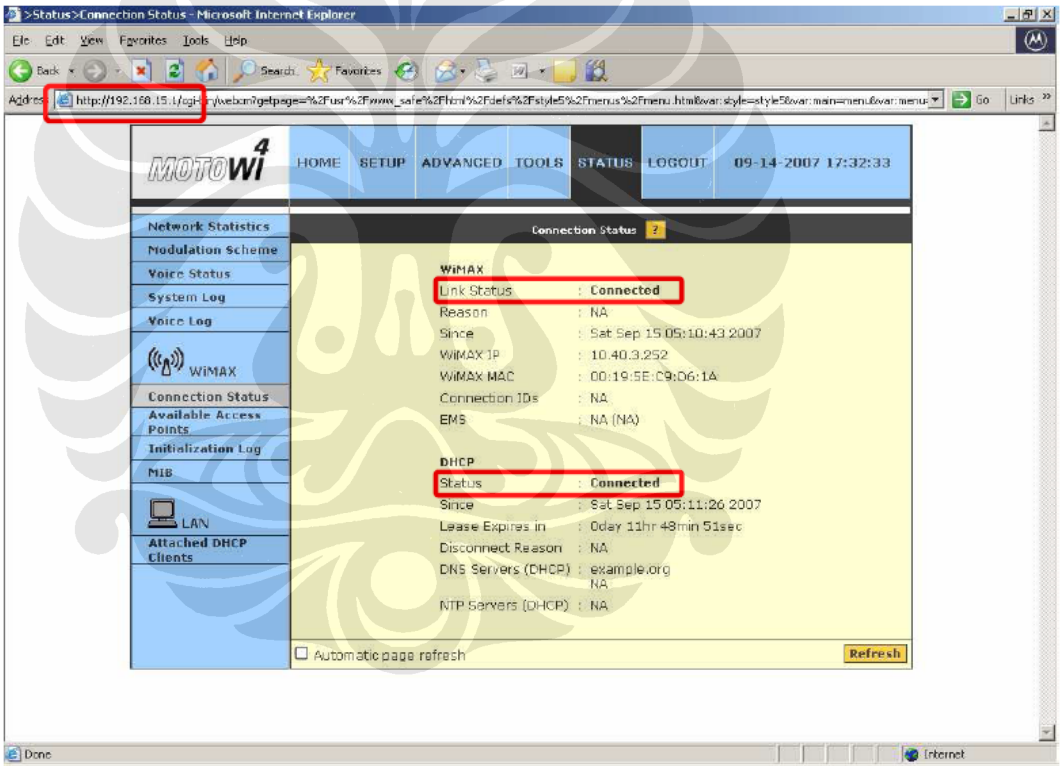



Gambar 4.2 Hasil Tes Ping dari CPE ke EMS Pada Saat CPE Belum Melakukan Inisiasi

### 4.1.2. Pengujian dan Analisis Autorisasi

Apabila Stasiun pengguna berada dalam jangkauan akses poin WiMax dan akses poin tersebut pada status tersedia oleh stasiun pengguna, maka stasiun pengguna tersebut bisa melakukan inisiasi untuk memulai koneksi dengan stasiun utama. Pada saat melakukan inisiasi, stasiun pengguna mengirimkan sinyal permintaan dan menyertakan data-data identitas terminal pengguna untuk di autentikasi oleh stasiun utama.

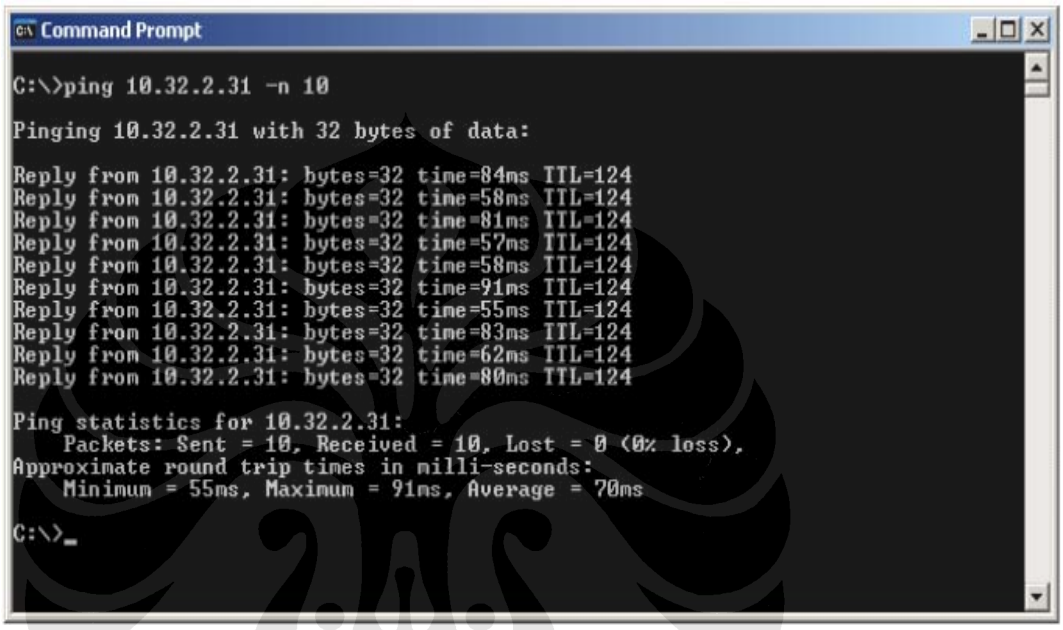
Sertifikat digital yang dikirimkan tersebut akan diteruskan ke server autentikasi. Apabila sertifikat digital itu dikenali sebagai pengguna yang berhak mendapatkan koneksi dari stasiun utama, maka server autentikasi akan memberikan informasi ke stasiun utama untuk memberikan balasan denga mengautorisasi dan mengirimkan CID untuk membentuk sesi-sesi koneksi berikutnya. Bila server autentikasi menolak proses autentikasi karena sertifikasi kredensial yang dikirimkan menunjukkan bahwa stasiun pengguna tidak berhak mendapatkan koneksi dari stasiun utama, maka stasiun utama kan menginformasikan pada CAPC agar stasiun pengguna tersebut diberikan null point oleh *adaptive beamforming antenna*.




Gambar 4.3 Hasil Pengujian Status Autentikasi Terminal Pengguna WiMax

Setelah terminal pengguna membentuk sesi dengan stasiun utama, berikutnya stasiun utama akan memberikan alamat IP pada terminal pengguna melalui server DHCP. Dalam sistem ini alamat IP salalu diberikan oleh stasiun utama secara dinamis.

Hal ini ditunjukkan Gambar 4.3 yang menunjukkan status link dan DHCP yang telah tersambung dengan menampilkan status "*link connected*" dan "*DHCP connetced*". Pada Gambar 4.3 itu juga ditunjukkan alamat IP yang ditentukan oleh server DHCP stasiun utama adalah 10.40.3.252. Selain itu alamat mac dari terminal tersebut juga dikenali, yaitu 00:19:5E:C9:D6:1A.



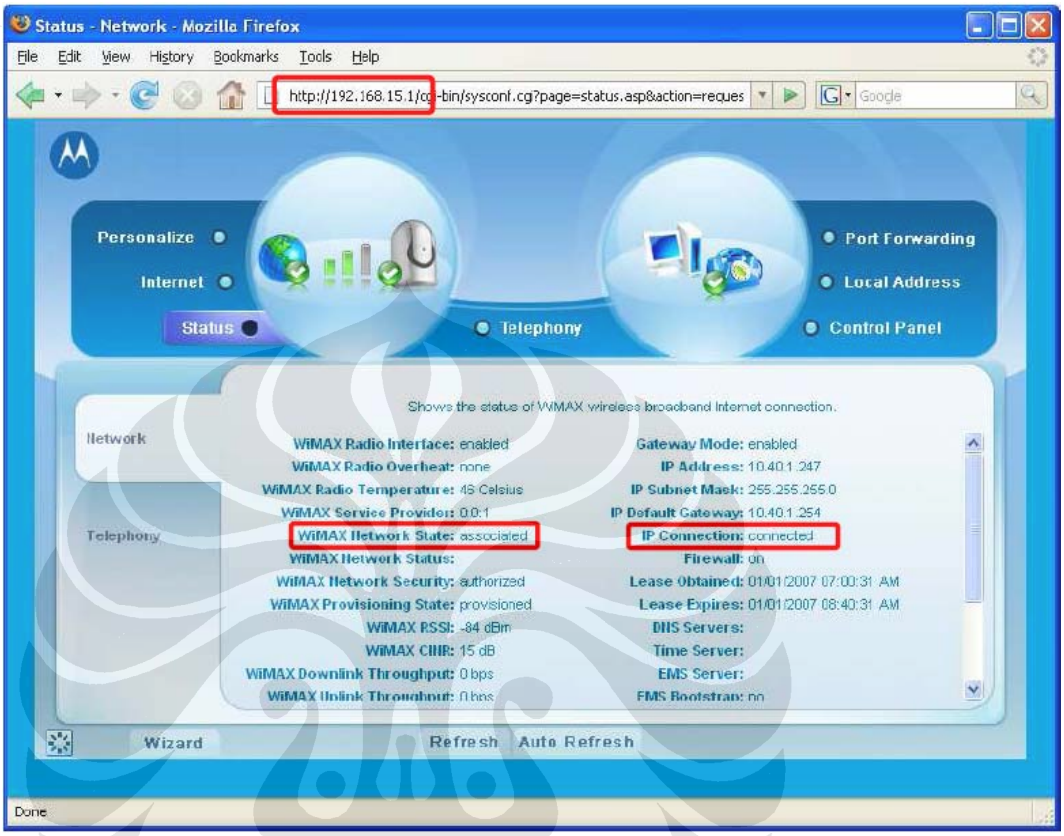

Gambar 4.4 Hasil Tes Ping Dari CPE ke Server EMS Pada Saat Status Tersambung

Sesi yang dibentuk antara stasiun utama dengan stasiun pengguna terus diperbarui dengan terus mengirimkan CID tiap mengirimkan data dan memperbarui kunci yang digunakan sebagai proses proteksi dengan enkripsi. Ketersambungan terminal pengguna ini bisa dibuktikan dengan hasil tes ping dari arah CPE dengan alamat IP 10.40.3.252 menuju server EMS dengan alamat IP 10.32.2.31. Dari semua paket ICMP yang dikirimkan lewat tes ping tersebut, 100% sukses dengan latensi maksimum 91 ms.

### 4.1.3. Pengujian dan Analisis Transfer Data FTP

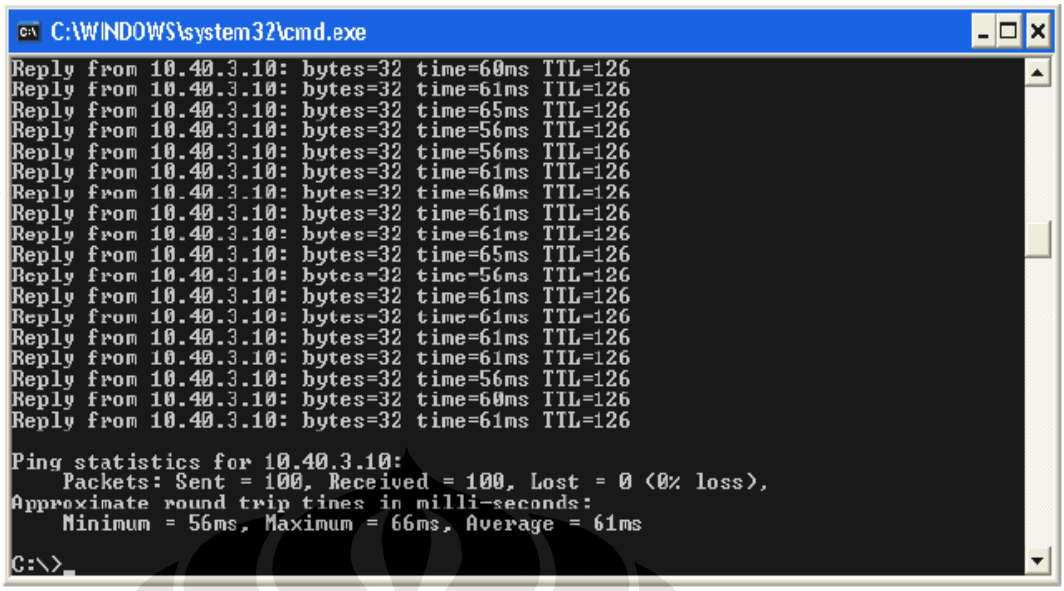
Pengujian beerikutnya adalah dengan melakukan transfer data melalui jaringan WiMax yang telah tersambung. Transfer data tersebut akan dilakukan

antara CPE dengan server FTP yang memiliki IP 10.40.3.10. Pengujian FTP ini dilakukan secara dua arah, yaitu FTP unduh dan FTP unggah.




Gambar 4.5 Status Koneksi Sebelum Melakukan FTP

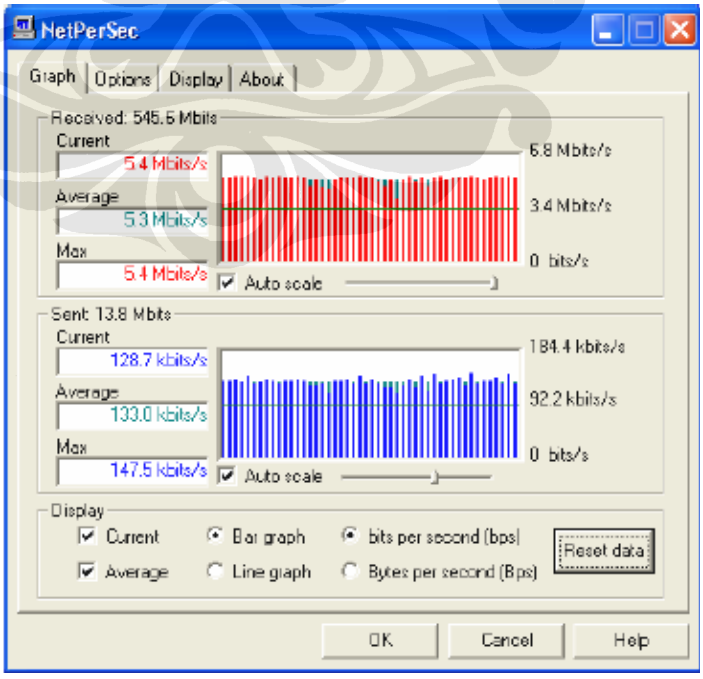
Sebelum melakukan pengujian transfer data melalui FTP, terlebih dulu perlu dilakukan pengujian koneksi dari CPE tersebut ke server FTP. Yaitu dengan melakukan tes ping dari CPE ke server FTP.




Gambar 4.6 Hasil Tes Ping Dari CPE ke Server FTP

### 4.1.3.1. Pengujian Transfer Data FTP Downlink

Pengujian transfer data FTP downlink dilakukan dengan mengambil file dari server FTP oleh terminal pengguna. Dengan mengambil file yang cukup besar maka akan terjadi transfer data secara terus menerus dan membutuhkan sesi koneksi yang berkesinambungan.




Gambar 4.7 Trafik Saat Pengujian FTP Downlink

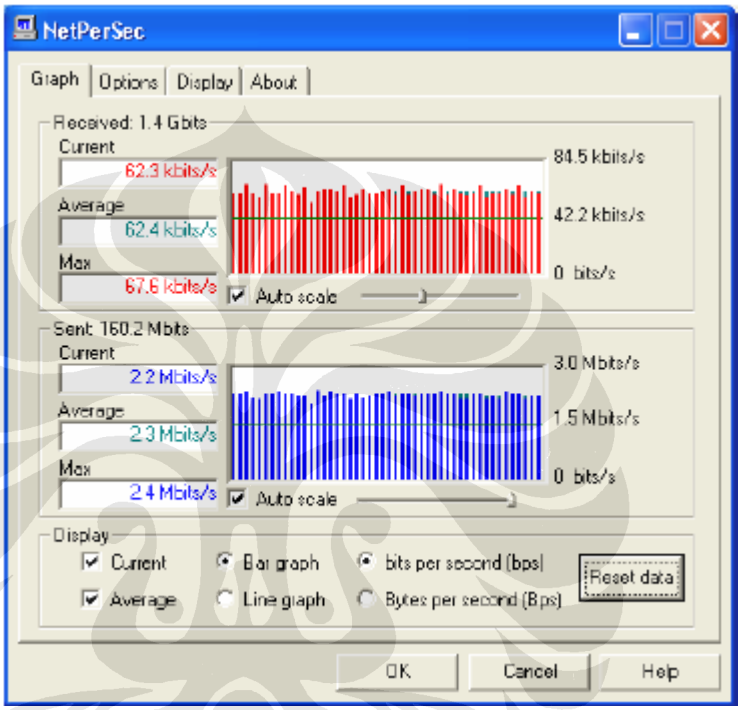
Pada saat melakukan transfer data melalui FTP dapat diamati pada status MAC yang ada pada terminal CPE. Dari Gambar 4.8 dapat dilihat bahwa pada saat itu jumlah paket yang masuk (DL) ke CPE adalah 2738 sedangkan yang keluar (UL) adalah 15. Hal ini karena proses yang sedang terjadi adalah proses unduh, sehingga trafik lebih banyak ke arah CPE. Sedangkan untuk trafik keluar (UL), meskipun tidak ada aktivitas unggah masih terdapat trafik keluar (UL). Hal ini karena meskipun tidak dilakukan aktivitas unggah, CPE akan terus mengirimkan data-data yang besarnya kecil yang berupa kredensial dan CID untuk tetap membentuk sesi antara CPE dengan stasiun utama. Selain itu juga terdapat trafik SNMP antara CPE dengan server manajemen EMS.


Gambar 4.8 Status MAC Pada CPE Saat Melakukan FTP

Selain itu pada Gambar 4.8 juga ditunjukkan status dari berbagai parameter PKM. Di Gambar 4.8 tersebut juga ditunjukkan bahwa "*AK Life Time*" adalah 17277849. Angka ini menunjukkan waktu sisa ata panjang usia dari kunci publik yang digunakan bersama antara stasiun utama dengan terminal pengguna. Kunci tersebut akan terus diperbarui untuk tetap membentuk koneksi.

### 4.1.3.2. Pengujian Transfer Data FTP Uplink

Selain pengujian transfer data downlink juga dilakukan pengujian transfer data uplink. Hal ini sama saja dengan proses FTP downlink hanya saja trafiknya terbalik. Pada proses ini trafik Keluar (UL) CPE lebih tinggi dibandingkan trafik masuk (DL) ke CPE.



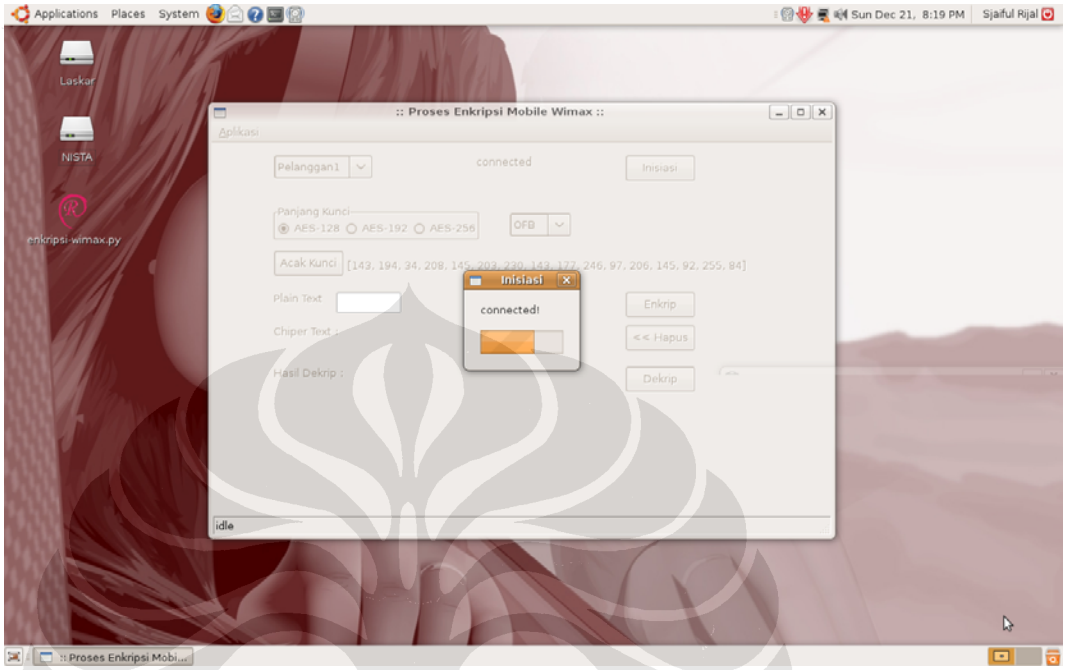

Gambar 4.9 Trafik Saat Transfer Data FTP Uplink

Pada proses transfer data FTP Uplink ini trafik yang keluar (UL) tidak sebesar trafik masuk (DL) pada saat transfer data FTP downlink. Hal ini terjadi karena layanan yang diberikan memang asimetris. Yaitu kapasitas downstream lebih tinggi daripada upstream.

## 4.2. Hasil Pengujian dan Analisis Simulasi

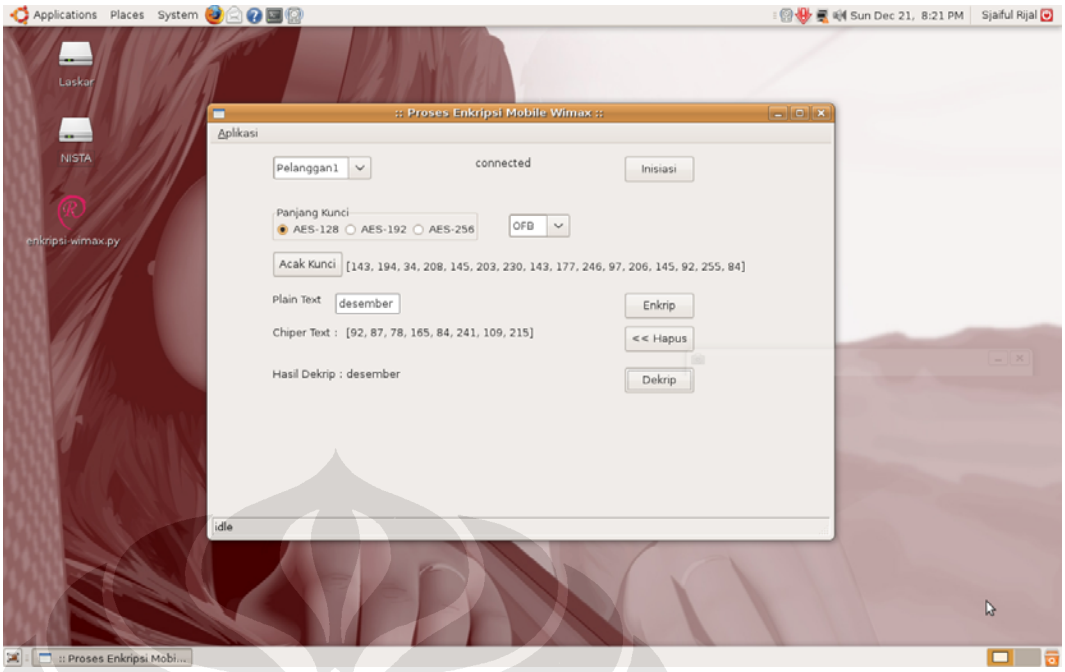
Untuk mengetahui proses pengamanan data pada sistem Mobile WiMax, digunakan perangkat lunak untuk mensimulasikannya. Pada program simulasi ini dilakukan proses pengamanan data dengan cara enkripsi dan dekripsi. Data dienkripsi dengan menggunakan metode *Advance Encryption System* (AES) 128

bit. Dari Gambar 4.10 dapat dilihat hasil eksekusi program shell linux melalui program python2.5.




Gambar 4.10 Tampilan Program Simulasi Proses Inisiasi

Pada simulasi tersebut ditunjukkan proses inisiasi SS terhadap BS. Dalam program tersebut diasumsikan terdapat 4 SS pelanggan, dimana masing-masing memiliki kredensialnya sendiri. Dari tampilan program pada Gambar 4.10 tampak SS Pelanggan1 melakukan permintaan sambungan pada BS. Pada proses ini, SS mengirimkan data kredensialnya berupa MAC dan sertifikasi digital berbasis X.509 yang dimiliki. Kamudian BS memeriksanya, untuk menyamakan dengan data yang dimiliki oleh BS. Bila cocok, maka seperti pada tampilan program yang ada di Gambar 4.10, maka BS akan memberikan koneksi pada SS Pelanggan1 tersebut.




Gambar 4.11 Tampilan Program Simulasi Proses Enkripsi

Setelah proses inisiasi, program simulasi ini dapat menjalankan simulasi proses enkripsi, dimana terdapat tiga pilihan panjang kunci yang akan digunakan pada metode enkripsi AES. Mode-mode enkripsi berdasarkan panjang kuci tersebut, antara lain : AES-128, AES-192 dan AES-256. Karena pada sistem Mobile WiMax yang sedang diuji coba menggunakan metode enkripsi AES dengan panjang kunci 128 bit, maka digunakan AES-128.

Pada Gambar 4.11, ditampilkan kunci-kunci yang digunakan pada proses enkripsi-dekripsi ini. Kunci-kunci tersebut dibangkitkan secara acak yang kemudian akan didistribusikan ke SS. Pada program simulasi ini diasumsikan pengiriman *plaintext* dengan informasi berisi “desember”. Dengan 128 bit kunci AES yang dibangkitkan secara acak (143,194, 34, 208, 145, 203, 143, 177, 246, 97, 206, 145, 92, 255, 84) dihasilkan kode *chipertext* (92,87,78,165, 84, 241, 109, 215).

Angka-angka tersebut merupakan bentuk integer dari tiap blok 8 bit dari masing-masing kode.Enkripsi ini dilakukan dalam bentuk bit namun dilakukan per blok.

Dalam bentuk chipertext tersebutlah dilakukan pengiriman data, sehingga data informasi dapat terjamin kerahasiaannya. Karena hanya dengan kunci yang sama, informasi tersebut dapat terbaca seperti semula.