Analisis artifak pada virtual machine menggunakan pendekatan berbasis digital forensic = Analyzing artifact in virtual machine with digital forensic approach

Arief Admaja, author

Abstrak

Teknologi komputer yang belakangan berkembang dengan pesat adalah hadirnya virtualisasi komputer yang mampu menciptakan banyak virtual machine dalam satu komputer, sehingga membuat kinerja komputer semakin efisien karena pemakaian sumber daya dapat dimaksimalkan. Potensi tindak kejahatan yang dapat terjadi adalah dilakukannya tindakan penetrasi dan intrusi sistem dari dalam virtual machine.
Tulisan ini akan menganalisis dampak dari cara shutdown yang menjadi prosedur dasar digital forensic pada keberadaan artifak digital dalam komputer yang memiliki virtual machine. Adapun jenis virtual machine yang dibandingkan adalah Oracle VM VirtualBox dan VMware Player.
Dari hasil percobaan didapati bahwa forced shutdown pada virtual machine mengakibatkan lebih banyak kerusakan data (9%-25%) dibandingkan dengan normal shutdown. Apabila dilihat dari tampilan visual isi file pada saat virtual machine mendapat forced shutdown, VirtualBox kehilangan kualitas tampilan sebesar 17%, sedangkan VMware mencapai 25%. Adapun bila dilihat dari kesamaan hash dengan file asli pada saat virtual machine mendapat forced shutdown, 50% file uji pada VirtualBox tidak identik sedangkan pada VMware kualitasnya lebih baik dengan hanya 25% file uji yang tidak identik.
<hr>The latest trends in computer technology is the prevalence of computer virtualization that is capable of creating many virtual machine in one computer, thus making the performance of the computer more efficient due to the use of resources can be maximized. Potential crimes that can happen is the act of penetration and intrusion systems from within the virtual machine.
This paper will analyze the impact of shutdown process which is a basic digital forensic procedures on the presence of digital artifacts in a computer that has the virtual machine. As for the type of virtual machine that used is Oracle VM VirtualBox and VMware Player.
The results of the experiment is forced shutdown procedure on virtual machine resulting in more damage data (9%-25%) compared to normal shutdown. When viewed from the visual appearance of the contents of file in virtual machine which gets a forced shutdown, VirtualBox have quality loss by 17%, while VMware reaches 25%. When seen from the hash similarity factor with the original file when virtual machine gets a forced shutdown, 50% test file on VirtualBox not identical while the quality is better on VMware with only 25% of the test files are not identical.