

ANALISIS VIRTUAL MACHINE UNTUK KEPERLUAN KOMPUTER FORENSIK

Danar Iwan Mustofa
Jurusan Teknik Informatika
Fakultas Teknologi Industri
Universitas Islam Indonesia
Yogyakarta

Abstrak---- Dengan semakin meningkatnya kebutuhan akan virtualisasi, baik bagi perusahaan maupun perorangan, maka secara tidak langsung teknologi ini dapat disalahgunakan oleh orang-orang yang tidak bertanggungjawab, untuk merugikan orang lain. Maka perlu dilakukan analisis mengenai peran virtual machine dalam komputer forensik. Namun penelitian pada *virtual machine* untuk keperluan komputer forensik belum dilakukan secara lebih mendalam.

Dalam paper ini, penulis mengusulkan sebuah metodologi baru dalam proses penanganan *virtual machine* sebagai barang bukti digital.

Kata Kunci : Digital Forensik, virtual machine, virtual disk, Live View

I. PENDAHULUAN

Perkembangan dunia teknologi informasi memang sangat pesat. Terhitung pada tahun 2011, jumlah total pengguna internet di dunia adalah sebanyak 2.267.233.742. Angka ini tentunya sangat besar, dibandingkan dengan tahun 2000, dimana pengguna internet hanya 360.985.492. Hal ini menunjukkan bahwa dalam kurun waktu 2000-2011, pertumbuhan pengguna internet di dunia adalah 528,1%. Pengguna internet di Indonesia adalah sebesar 22,4% atau sekitar 55.000.000 dari total populasi 245.613.043 [1].

Menurut FBI dalam laporan tahunannya, pada tahun 2011 terdapat 300.000 keluhan yang dilaporkan kepada Internet Crime Complaint Center (IC3). Angka ini menunjukkan peningkatan sebesar 3,4 persen dari tahun sebelumnya. Diperkirakan, kerugian berdasarkan keluhan yang ada, adalah sekitar \$485.300.000 atau setara dengan Rp4.755.940.000.000 (kurs Rp 9700). Kebanyakan dari korban yang melaporkan adalah korban penipuan, dan pencurian identitas. IC3 sendiri menerima dan memproses 26.000 keluhan tiap bulannya [2].

II. VIRTUAL MACHINE DAN KOMPUTER FORENSIK

Virtual machine, adalah aplikasi yang memungkinkan pengguna-nya untuk dapat meng-*install* lebih dari satu sistem operasi, di dalam satu komputer yang sama. Atau dengan kata lain, meng-*install* sistem operasi lain di dalam sistem operasi. Sehingga pengguna dapat menjalankan beberapa sistem operasi sekaligus dalam waktu yang sama. Sistem operasi yang sebenarnya disebut sistem operasi "*host*". Dan sistem operasi

virtual yang ter-*install* di dalam sistem operasi *host*, disebut sistem operasi "*guest*"[7]. VMWare adalah salah satu perusahaan yang mengelola *cloud computing*. Para analis memperkirakan, sebanyak 80% virtualisasi berjalan pada teknologi dari VMWare [9].

Dalam arsitektur ini, sistem operasi dasar (*host*) diinstall di dalam komputer terlebih dahulu. Kemudian sebuah software yang disebut hypervisor atau *virtual machine monitor* (VMM), dipasang di dalam sistem operasi *host*, dan memungkinkan pengguna untuk menjalankan berbagai sistem operasi *guest* dalam jendela aplikasi mereka sendiri. Produk yang terkenal menggunakan arsitektur ini adalah VMWare Workstation.

Menurut US-CERT [4], komputer forensik adalah *the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law*. Sedangkan Digital Forensic Research Workshop [6], mendefinisikan komputer forensik sebagai *the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*.

Dari penjelasan diatas, dapat disimpulkan bahwa komputer forensik adalah suatu ilmu dan metode, untuk mengumpulkan, memelihara, mengidentifikasi, menganalisis barang bukti digital, untuk kemudian didokumentasikan dan dipresentasikan untuk membuktikan apakah seseorang terbukti melakukan tindak pidana, atau tidak.

Tahapan-tahapan komputer forensik dapat dirangkum kedalam empat tahapan umum berikut ini:

1. Access

Adalah mengumpulkan barang bukti elektronik yang ada di TKP. Lalu kemudian membawa barang bukti elektronik tersebut ke laboratorium untuk diserahkan kepada *forensic examiner*.

2. Acquire

Adalah tahapan untuk mendapatkan data digital, dari barang bukti elektronik. Ada beberapa langkah yang harus dilakukan untuk mendapatkan data-data digital yang dimaksud.

Diantaranya adalah melakukan *write protect*, mem-back up data, dan membuat file *image* dari perangkat digital tersebut.

3. Analyze

Merupakan tahapan inti dari proses digital forensik. Setelah data-data digital terkumpul, maka dilakukan analisis data-data tersebut. Hal ini dilakukan untuk mencari bukti-bukti yang nantinya dapat menguatkan, atau melemahkan tuntutan kepada tersangka di pengadilan.

4. Report

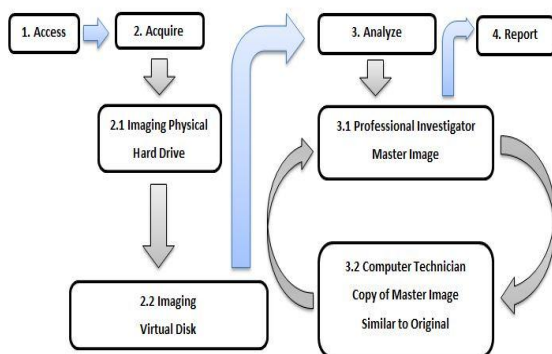
Dokumentasi dan laporan adalah tahap terakhir dalam proses komputer forensik. Pada tahap ini, seorang *forensic examiner* mendokumentasikan hasil analisis-nya, membuat laporan tentang hasil temuan yang didapatkan, lalu kemudian mempresentasikan hasil tersebut.

III. METODOLOGI

Metodologi usulan yang digunakan oleh peneliti mencakup segala aspek dalam tahapan komputer forensik secara umum. Namun dalam penelitian ini, digunakan metode penelitian yang berbeda dari metode penelitian komputer forensik pada umumnya. Perbedaan tersebut terletak pada proses *acquire* (akuisisi) dan pada proses analisis.

Setelah kita mendapatkan barang bukti elektronik dari tempat kejadian perkara, yang harus dilakukan kemudian adalah membuat back up serta file image dari barang bukti tersebut, sehingga didapatkan barang bukti elektronik. Namun file image dari harddisk fisik yang diperoleh belum dapat digunakan untuk melihat dan menganalisis data-data pada *virtual machine disk*. Oleh karena itu dalam proses akuisisi, setelah memback-up semua data dalam harddisk fisik, langkah selanjutnya adalah melakukan *file imaging* dari *virtual disk*. Sehingga *examiner* dapat melihat isi dan struktur file yang ada pada virtual disk.

Ketika masuk ke tahap analisis, barang bukti digital berupa file image dibuat dalam dua file yang berbeda. Yang pertama diserahkan kepada *forensic examiner*, dan yang kedua diserahkan kepada teknisi komputer. Kemudian teknisi komputer mencoba untuk membooting file image tersebut, dan mencari data-data yang ada di dalamnya dengan menggunakan *virtual machine* VMWare Workstation dan Live View.

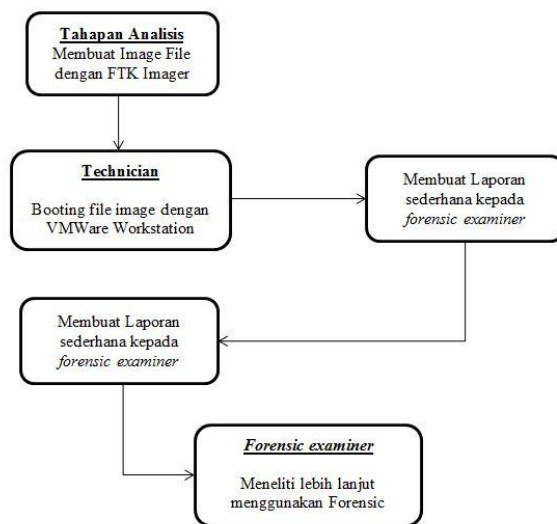


Gambar 1 Metodologi Usulan

Peran teknisi komputer (bukan *forensic examiner*) adalah untuk melakukan booting file image dari *virtual machine* kedalam lingkungan virtual. Hal ini dilakukan untuk dapat memberi gambaran tentang kondisi pada *virtual machine* yang ter-install. Sehingga diharapkan dapat menemukan file-file yang dicurigai sebagai barang bukti kejahatan.

IV. PROSEDUR ANALISIS SERTA AKUISIS PADA VIRTUAL DISK

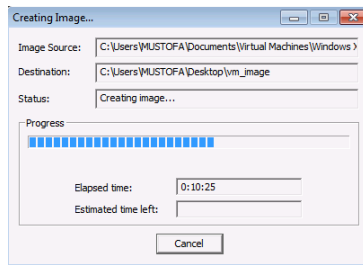
Tujuan utama dari akuisisi dan imaging adalah untuk meminimalisir terjadinya kontaminasi dan memastikan barang bukti dapat diterima menurut hukum. Pada gambar 2 berikut ini, digambarkan alur bagaimana tahapan analisis berlangsung.



Gambar 2 Tahapan Analisis Forensik

Dalam melakukan disk imaging, dibutuhkan software bernama FTK Imager. Selain digunakan sebagai alat akuisisi, FTK Imager juga dapat digunakan untuk melihat sekilas barang bukti yang telah diakuisisi. Dan apabila bukti digital yang ada memerlukan investigasi lebih lanjut, maka perlu dibuat image dari bukti digital tersebut. Untuk menghindari perubahan atau perbedaan data, FTK Imager membuat duplikat sebuah file secara bit-per-bit. Sehingga *forensic image* akan sama dengan bukti aseli. Dalam membuat file image, ada beberapa format image yang dapat dipakai. Salah satunya adalah format DD image.

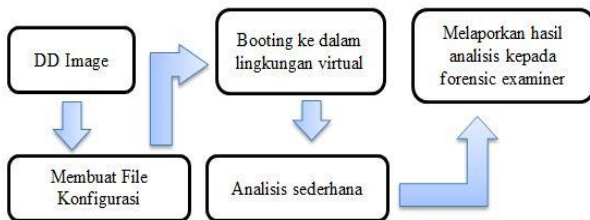
Seperti disebutkan Carvey dalam “Windows Forensic Analysis” [27] DD nama yang diberikan kepada aplikasi yang efektif dari dunia UNIX yang memiliki berbagai macam kegunaan, baik untuk menyalin file maupun harddisk secara keseluruhan. Format DD dipilih, karena telah lama dianggap sebagai standar untuk pembuatan image forensik. Dan banyak dari *tools* forensik yang mendukung format DD. Oleh karena itu, dalam penelitian ini, penulis mencoba membuat file image dengan format DD. Berikut ini adalah informasi dari file image virtual disk yang telah dibuat.



Gambar 3 Proses Imaging pada Virtual Disk

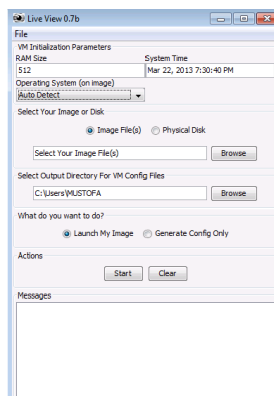
4.1 Hasil Analisis oleh Teknisi

Pada tahap ini, seorang *forensic examiner* menyerahkan sebuah copy dari DD image barang bukti yang sama dengan aslinya kepada teknisi komputer yang belum berpengalaman dalam bidang komputer forensik. Hal ini ditujukan agar seorang teknisi dapat melakukan booting, dan analisis sederhana pada file image tersebut. Kemudian dari hasil analisis sederhana tersebut, teknisi memberikan laporan sederhana kepada *forensic examiner*. Berikut adalah alur tahapan yang harus dilakukan oleh teknisi.



Gambar 4 Tahapan yang dilakukan Teknisi Komputer

Pada tahap ini, sebuah image file dari *virtual machine* Windows XP, akan di-booting dalam lingkungan virtual. Dengan teknik seperti ini, akan dapat memberi gambaran pada *forensic examiner* tentang lingkungan sistem operasi yang dipakai oleh pelaku tindak kriminal. Sebelum dapat membooting file image kedalam lingkungan virtual, maka perlu dilakukan persiapan dengan meng-install VMWare Workstation dan Live View.



Gambar 5 Live View

Dengan melakukan booting pada image virtual machine, maka seorang teknisi dapat melakukan explorasi pada sebuah sistem. Sehingga diharapkan hal ini dapat membantu menemukan data-data yang dimaksud. Pada gambar 6 berikut ini adalah tampilan dari desktop *virtual machine*.



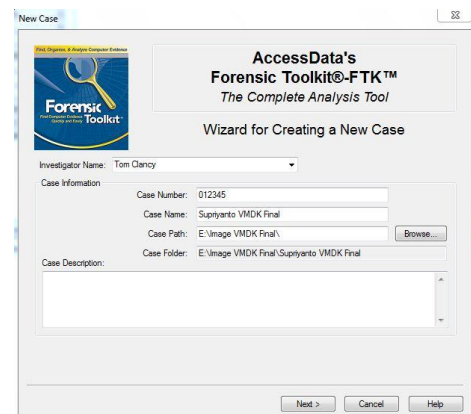
Gambar 6 Tampilan Desktop Virtual Machine

4.2 Hasil Analisis oleh Examiner

Analisis pada tahap ini dilakukan oleh forensic examiner yang sudah ahli di bidangnya. Forensic examiner umumnya menggunakan tools forensik dalam melakukan tugasnya. Tool forensik yang digunakan dalam penelitian ini adalah Forensic Toolkit.

Dari hasil analisis sederhana yang dilakukan oleh teknisi komputer, diharapkan dapat memberikan gambaran mengenai kondisi *virtual machine* tersebut. Sehingga *forensic examiner* dapat dengan cepat menentukan langkah yang harus diambil selanjutnya. Dapat langsung menuju ke inti dari penelitian tersebut. Dengan metode ini juga diharapkan dapat menghemat waktu yang diperlukan oleh *forensic examiner* dalam menganalisis *virtual machine*.

Namun, sebelum dapat melakukan analisis menyeluruh terhadap barang bukti digital, forensic examiner terlebih dahulu harus mengisi data-data tentang barang bukti agar lebih mudah mengidentifikasi, dan tidak tercampur dengan barang bukti yang lain.



Gambar 7 Forensic Toolkit

4.3 Rangkuman Hasil Analisis

Setelah dilakukan penyelidikan terhadap *virtual machine* secara menyeluruh, baik dengan cara mem-booting *virtual machine* maupun dengan menggunakan *software* FTK, maka dapat disimpulkan beberapa temuan diantara keduanya. Ada beberapa file *log* maupun file *history* yang tidak tersimpan di dalam harddisk komputer, melainkan tersimpan di dalam server internet. Seperti contohnya file *log* dalam Yahoo Messenger. Oleh karena itu, melakukan booting pada *virtual machine* sangat diperlukan guna mencari data-data yang diinginkan.

Dari pembahasan pada sub-bab sebelumnya, penulis juga menemukan adanya perbedaan pada tools yang digunakan. Sebagai contoh, analisis menggunakan FTK dan FTK Imager akan menghasilkan hasil yang berbeda. Kedua *software* tersebut memiliki kekurangan dan kelebihan masing-masing. Namun keduanya juga memiliki kelemahan yang sama, yaitu tidak maksimal pada tugas *me-recovery data*. Hal tersebut dapat dilihat pada temuan, yang telah dirangkum dalam tabel 4.1 dibawah ini.

Tabel 4. 1 Perbandingan FTK dan FTK Imager

Features	FTK Imager	Forensic Toolkit
File (Data) Discovery	●	○
File (Data) Recovery	○	○
Reveal File Contents	●	○
File (Data) Access & Analysis	○	●
Imaging	●	○
MD5	●	●
SHA1	●	●

Keterangan : ● Efektif ○ Kurang Efektif

Dari skenario yang disajikan dalam penelitian diatas, dapat diperoleh hasil bahwa formulir barang bukti dapat bermanfaat sebagai petunjuk dalam memprioritaskan suatu kasus. Sehingga *examiner* tahu kasus mana yang harus dikerjakan lebih dulu. Sehingga, diharapkan kasus yang sedang ditangani dapat selesai tepat waktu sebelum persidangan dilakukan.

Kemudian kerjasama antara dua personel yang dilengkapi dengan peralatan dan keahlian yang berbeda, dapat menghasilkan hasil yang lebih cepat. Serta dapat mengurangi beban kerja dari *forensic examiner* profesional. Meskipun tanpa bantuan teknisi dan tanpa menggunakan lingkungan virtual, seorang *forensic examiner* profesional tetap dapat menemukan hasil yang sama. Namun, dengan menggunakan metode konvensional dan virtual tersebut, *forensic examiner* dapat menghemat waktu dan kesempatan menemukan bukti-bukti penting menjadi lebih besar.

Selain itu, dengan menggunakan metode tersebut juga dapat bermanfaat untuk melatih teknisi yang belum berpengalaman agar dapat menjadi lebih mengerti akan bidang komputer forensik, sehingga diharapkan teknisi dapat mengerti konsep dan prosedur dalam komputer forensik sebelum terjun langsung menjadi profesional *forensic examiner*.

Membooting *virtual machine* juga dapat bermanfaat untuk keperluan presentasi di pengadilan. Sehingga orang awam yang tidak mengerti tentang komputer, dapat melihat bagaimana *virtual machine* bekerja, dan dapat melihat rekonstruksi kejadian bagaimana seorang pelaku kriminal melakukan tindak kejahatan.

V KESIMPULAN

Meskipun *virtual machine* sangat identik dengan sistem komputer yang sebenarnya, namun tetap ada beberapa perbedaan struktur file yang harus diwaspadai oleh *forensic examiner*. Salah satunya adalah karakteristik pada *virtual disk* dan cara kerjanya. *Virtual Disk* tidak dapat dianalisis dari file image harddisk fisik. Perlu melakukan export pada *virtual disk*, selanjutnya membuat file image dari *virtual disk* tersebut.

Sebelum dilakukan analisis menyeluruh, pihak berwajib dapat memanfaatkan teknisi komputer untuk menjalankan *virtual machine*. Ditujukan untuk mencari data-data yang berpotensi dimanfaatkan sebagai alat kejahatan, sehingga dapat meningkatkan efektifitas, dan menghemat waktu yang diperlukan dalam proses analisis oleh *forensic examiner*.

Virtual machine dapat di-booting sebagai analisis awal dan dapat dimanfaatkan untuk memperlihatkan bukti-bukti digital yang ada dihadapan pengadilan, dengan tujuan untuk memberikan keterangan serta untuk mempresentasikan bukti-bukti yg ada di dalam *virtual machine* tersebut.

Tidak semua file tersimpan di dalam media penyimpanan komputer, namun dapat juga tersimpan dalam server penyedia layanan. Seperti file *log* pada Yahoo Messenger. Sehingga data-data yang ada tidak dapat dianalisis menggunakan Forensic Toolkit. Oleh karena itu, penyidik kasus dan *forensic examiner* perlu melakukan kerja sama dengan penyedia layanan. Sehingga analisis barang bukti digital tetap dapat dilakukan secara konvensional, karena itu merupakan standar baku dalam penanganan barang bukti digital.

DAFTAR PUSTAKA

- [1] Internet World Stats. (2011). *Usage and Population Statistic*. Retrived October 15, 2012, from <http://www.internetworldstats.com/stats.htm>
- [2] IC3. (2011). Internet Crime Complaint Center. Retrived October 23, 2012, from http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf
- [3] Nardoni, D. (2005). David Nardoni. *Introduction to Computer Forensic*. Retrived November 10, 2012, from <http://www-scf.usc.edu/~itp499cf/Lectures/USC.Computer.Forensics-Computers.and.Networks.pdf>
- [4] US-CERT. (2008). *Computer Forensics*. Retrived November 19, 2012, from <http://www.us-cert.gov/sites/default/files/publications/forensics.pdf>
- [5] Huth, A ., Cebula, J. (2011). *The Basic of Cloud Computing*. United States Computer Emergency Readiness Team
- [6] DFRWS. (2001). *A Road Map for Digital Forensics Research Workshop*. Retrived November 23, 2012, from <http://www.dfrws.org/2001/dfrws-rm-final.pdf>
- [7] Shavers, B. (2008). *Virtual Forensics, A discussion of Virtual Machines Related to Forensics Analysis*. From <http://www.forensicrofocus.com/downloads/virtual-machines-forensics-analysis.pdf>
- [8] Conroy, Sean P. (2010). *History of Virtualization*. Retrived October 3, 2012, from <http://www.everythingvm.com/content/history-virtualization>
- [9] VMWare. (2012). *Accelerate IT Innovate With Your Cloud*. Palo Alto, USA : VMWare, Inc
- [10] Messmer, E., “Gartner predicts nearly half of server workloads will be virtualized”, Network World. Retrieved from <http://www.networkworld.com/news/2009/102009-gartner-server-virtualization.html>, 2010.
- [11] Bem, D., Huebner, E. (2007). Computer Forensik Analysis in a Virtual Environment. *International Journal of Digital Evidence*, 6(2).
- [12] Praveen. (2011). Analysis of Performance in the Virtual Machines Environment. *International Journal of Advanced Science and Technology*, 32.
- [13] National Instruments. (2009). *Virtualization Technology Under the Hood*. Retrived October, 2012, from <http://www.ni.com/white-paper/8709/en>
- [14] Mell, P., Grance T. (2011). *The Definition of Cloud Computing*. National Institute of Standards and Technology.
- [15] Barrett, D., Kipper,G. (2010). *Virtualization and Forensic, A Digital Forensic Investigator's Guide to Virtual Environments*, Burlington : Elsevier.
- [16] Carvey, H. (2009). *Windows Forensic Analysis, DVD Toolkit 2E*, Burlington : Elsevier
- [17] US Departement of Justice . (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* . Washington: National Institute of Justice
- [18] Craiger, J. Philip. (2005). *Computer Forensics Procedures and Methods*. University of Central Florida.
- [19] Horvat, M. (2005). *Disk Cloning*. Sentinel Data Security. From <http://sentinelsecurity.net>
- [20] Hirwani, M., Pan, Y., Stackpole, B., & Johnson, D. *Forensic Acquisition and Analysis of VMWare Virtual Hard Disk*. Rochester Institute of Technology