TEKNIK AKUISISI VIRTUALISASI *SERVER* MENGGUNAKAN METODE *LIVE FORENSIC*

Soni, Yudi Prayudi, Bambang Sugiantoro

Magister Teknik Informatika
Fakultas Teknologi Industri
Universitas Islam Indonesia

sony_bkn@yahoo.com

Abstrak

Virtualisasi server adalah teknologi yang dapat menjalankan beberapa system operasi secara bersamaan dalam satu computer. Munculnya virtualisasi server ini pada praktiknya mengundang celah kejahatan baru dan memunculkan tantangan tersendiri untuk menemukan petunjuk dan bukti digital dalam mengungkap kasus kejahatan yang terjadi. Hal ini tentnnya akan menyulitkan para penyidik untuk melakukan akuisisi terhadap salah satu system operasi dalam ada dalam server tersebut tanpa mengganggu dan tanpa mematikan komputer mengingat betapa pentingnya server tersebut. Selama ini teknik akuisisi umumnya digunakan secara tunggal dimana hanya memuat satu sistem operasi. Oleh karena itu diperlukan teknik untuk mengakuisisi virtualisasi server dengan menggunakan metode live forensic tanpa mengganggu atau mematikan sistem operasi yang sedang berjalan lainnya.Teknik Akuisisi yang dilakukan dengan mengakuisisi salah satu sistem operasi melalui server proxmox.

Kata Kunci: *Live Forensic*, Akuisisi, Virtualisasi Server, Proxmox

1. Pendahuluan

Virtualisasi *server* merupakan teknologi yang saat ini sedang berkembang pesat. Hal ini dibuktikan berdasarkan laporan *survey* yang diterbitkan oleh spiceworks.com, mengatakan bahwa 76 % atau lebih dari tiga perempat responden menggunakan virtualisasi *server* pada data *center* nya. Dari statistik ini terlihat bahwa virtualisasi paling banyak digunakan dan beberapa persen dari *respon* juga telah merencanakan menggunakan virtualisasi (Spiceworks.com, 2016). Teknik virtualisasi yang berkembangpun semakin banyak. Mulai dari yang berbayar dan harganya mencapai puluhan juta sampai yang gratisan dan memiliki kelebihan serta kekurangan masing-masing. Teknik virtualisasi yang paling se*Ring* digunakan seperti *Vmware* Esxi, *Microsoft Hyper-V, Open-VZ*, dan *Proxmox*.

Perkembangan virtualisasi yang demikian pesat tersebut tentunya mengundang sebuah celah kejahatan baru. Kejahatan yang terjadi dengan melibatkan virtualisasi *server* berdampak pada tantangan baru untuk menemukan petunjuk dan mengungkap kasus kejahatan yang ada pada

virtualisasi tersebut. Apabila salah satu mesin *virtual* tersebut digunakan untuk melakukan kejahatan tentu saja akan menyulitkan para investigator untuk mengakuisisi serta menganalisis salah satu mesin *virtual* tersebut. Karena tidak mungkin melakukan akuisisi terhadap keseluruhan *server* itu sendiri mengingat betapa besarnya kapasitas dari keseluruhan *server* tersebut. Dalam melakukan akuisisi juga diperlukan teknik akuisisi yang tepat sehingga mendapatkan kualitas hasil akuisisi yang dapat dibaca oleh *software* forensik untuk dilakukan eksaminasi dan analisis. Karena kualitas dari hasil analisis yang dihasilkan juga tergantung dari proses akuisisi yang digunakan.

Akuisisi komputer umumnya dilakukan secara tunggal dimana satu komputer hanya memuat satu sistem operasi. Tapi saat ini satu komputer dapat memuat lebih dari satu sistem operasi sehingga diperlukan teknik akuisisi yang tepat untuk mengambil data yang diperlukaan saja tanpa mengambil keseluruhan data dalam komputer *server* tersebut. Sayangnya belum ada teknik standar untuk mengakuisisi virtualisasi *server* karena ada beberapa hal yang yang karakteristiknya berbeda apabila satu komputer tersebut memiliki banyak sistem operasi. Sehingga perlu dilakukan penelitian lebih lanjut tentang bagaimana teknik akuisisi dalam virtualisasi *server*. Hal ini diperlukan mengingat proses akuisisi yang akan dilakukan terhadap virtualisasi *server* dengan kondisi *server* fisiknya masih berjalan, maka akuisisi yang dilakukan akan menggunakan metode *live forensic*. Sebagaimana yang disebutkan oleh (Rafique & Khan, 2013) bahwa *live forensic*s yaitu metode forensik dengan mengumpulkan informasi, menganalisis, dan mempresentasikannya menggunakan berbagai macam *tools* forensik pada saat sistem masih berjalan.

2. Landasan Teori

2.1 Forensika Digital

Forensik digital (*digital forensics*) adalah penggunaan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital yang terkait dengan kasus yang terjadi untuk kepentingan rekontruksi kejadian serta keabsahan proses peradilan (Agarwal et.al, 2011). Sedangkan Menurut Al-Azhar (2012) Forensika Digital merupakan aplikasi ilmu pengetahuan dan teknologi komputer untuk melakukan pemeriksaan dan analisis terhadap barang bukti elektronik dan barang bukti digital dalam melihat keterkaitannya dengan kejahatan. Menurut

Zimmerman et al. (2011), proses forensika digital dapat dibagi menjadi empat fase yang berbeda :

1. Koleksi artefak (baik bukti digital dan bahan pembantu) yang dianggap memiliki nilai potensial untuk dikumpulkan
2. Pelestarian artefak asli dengan cara yang handal, lengkap, akurat, dan dapat diverifikasi
3. Analisis penyaringan artefak untuk menghilangkan atau masuknya barang-barang yang dianggap berharga.
4. Presentasi di mana bukti disajikan untuk mendukung penyelidikan.

2.2 Akuisisi

Menurut dokumen SNI 27037:2014, akuisisi merupakan proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktifitas yang dilakukan. Petugas yang melakukan akuisisi harus memilih metode yang paling sesuai berdasarkan situasi, biaya dan waktu, dan mendokumentasikan keputusan yang dipilih untuk menggunakan metode tertentu dan tool yang sesuai. Metode yang dipilih juga harus dapat dipraktekkan, dapat diulang kembali prosesnya dengan hasil yang sama, dan dapat diverifikasi bahwa hasil salinan sama persis dengan barang bukti yang asli. Dalam keadaan dimana proses verifikasi tidak dapat dilakukan, sebagai contoh ketika proses akuisisi yang sedang berjalan, tiba-tiba salinan asli yang sedang dibuat mengalami *error sectors*, maka dalam kasus seperti ini petugas investigasi yang melakukan akuisisi harus memilih metode yang paling memungkinkan untuk melakukan proses akuisisi ulang dan mendokumentasikannya, lalu dapat menjelaskan kenapa dilakukan akuisisi ulang dan dapat mempertahankan argumennya. (Badan Standarisasi Nasional, 2014)

2.3 Live Forensic

Live forensics dilakukan dengan cara mengumpulkan data ketika sistem yang terkena serangan masih berjalan (*running/alive*). Data forensik yang dikumpulkan melalui sistem yang live tersebut dapat memberikan bukti yang tidak dapat diperoleh dari static *disk image*. Data yang dikumpulkan tersebut merupakan representasi dari sistem yang dinamis dan tidak mungkin untuk diproduksi ulang pada waktu berikutnya (Adelstein, 2006).

2.4 Virtualisasi Server

Menurut Kumar & Charu (2015) Virtualisasi server adalah sebuah metode yang memungkinkan sistem operasi yang berbeda untuk berbagi perangkat keras yang sama serta membuatnya mudah untuk bergerak antara sistem operasi dengan virtualisasi hardware. Server yang berbeda adalah partisi dari sebuah server fisik ke server virtual yang lebih kecil untuk membantu memaksimalkan sumber daya virtualisasi server (yang berisi identitas dan jumlah server fisik individu, sistem operasi dan prosesor). Server memiliki sejumlah besar manfaat seperti Peningkatan Pemanfaatan Hardware, Keamanan serta Pengembangan.

3. Metodologi Penelitian

Tahapan penelitian yang dilakukan adalah meggunakan pendekatan dari metodologi teknik live forensik yang akan digambarkan pada gambar 1 dibawah ini :

Gambar 1: Metodologi Penelitian

Metodologi ini dibuat dan digunakan untuk menjelaskan bagaimana tahapan penelitian dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan.

4. Hasil dan Pembahasan

Bab ini akan menjelaskan uraian tentang hasil dan pembahasan yang bertujuan untuk mendapatkan jawaban yang berkaitan dengan permasalahan dari topik penelitian yang diangkat yaitu menerapkan teknik *live forensic* untuk mengakuisisi virtualisasi server.

4.1 Persiapan Sistem

Langkah pertama yang harus dilakukan dalam penelitian ini adalah mempersiapakan perangkat hardware dan software, merancang, membangun serta mengimplementasikan virtualisasi *server* dengan sistem operasi *server proxmox,* Dan juga mengimplemenetasikan dua buah sistem operasi linux ubuntu

dan windows 10, kedua sistem operasi tersebut akan berjalan didalam virtualisasi *server proxmox*.

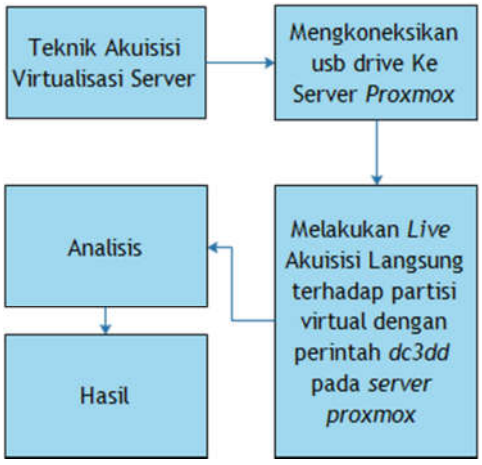
4.2 Skenario Kasus

Merupakan tahapan membuat simulasi kasus pada virtualisasi server dengan memasang web server dan juga menghapus enam file yang selanjutnya akan diakuisisi dan dieksaminasi dan menganalisis apakah web server dan keenam file tersebut dapat ditemukan.

4.2.1 Tahapan Akuisisi

Menurut (Cheng, 2014), *Logical Volume Manager* (LVM) merupakan sebuah penyimpanan hardisk *virtual* yang digunakan untuk mempermudah proses manajemen *disk* dari *hard disk* yang besar. Selain itu, user juga dapat menambahkan / menghapus / mengubah ukuran volume LVM yang telah dibuat. Dalam virtualisasi *server*, hasil dari instalasi dan seluruh partisi serta data yang tersimpan pada mesin *virtual* akan disimpan dalam penyimpanan lvm (*Logical Virtual Manager*). Dengan adanya lvm hardisk akan dibagi menjadi tiga bagian yaitu :

a. *Physical Volume* (PV) adalah media penyimpanan secara fisik yang dapat berupa partisi dalam sistem operasi. Misalnya dapat dikenali dengan /dev/sda/, /dev/sdb/, /dev/sdc/, dan lain sebagainya.
b. *Volume Group* (VG) adalah gabungan dari beberapa physical volume sehingga terbentuklah volume group dalam media penyimpanan.
c. *Logical Volume* (LV) adalah partisi secara logical yang akan digunakan untuk penyimpanan *file* system oleh virtualisasi *server*.



Gambar 2: Tahapan Teknik Akuisisi Virtualisasi Server

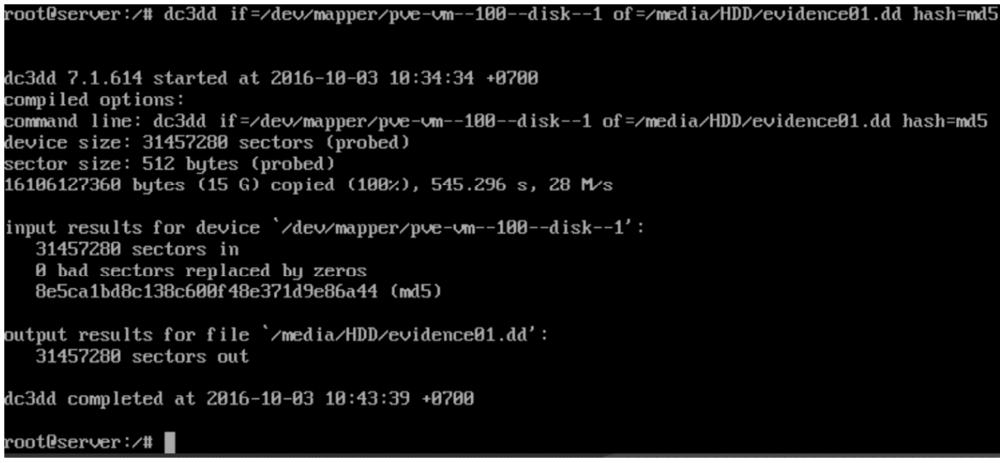
Gambar 2 menjelaskan tahapan teknik akuisisi yang digunakan yang memalui beberapa tahapan utama yaitu : Pertama, mengkoneksikan *usb drive* ke *server proxmox* secara langsung yang nantinya akan digunakan untuk menyimpan hasil akuisisi. Kedua, melakukan proses mounting usb drive. Proses ini perlu dilakukan terlebih dahulu karena *proxmox* tidak bisa secara langsung mendeteksi *usb drive*. Setelah *usb drive* berhasil terkoneksi dengan *proxmox* maka tahapan selanjutnya adalah melakukan akuisisi secara langsung pada salah satu mesin *virtual* yang partisinya tersimpan dalam penyimpanan *logical virtual manager* (lvm) dan terakhir menghasilkan file.dd. Setalah fiile berhasil dilakukan proses selanjutnya adalah menganalisis hasil akuisisi untuk membuktikan apakah teknik live forensik yang digunakan dapat menghasilkan kualitas akuisisi yang baik sehingga hasil akuisisi dapat dibaca oleh tools forensic dan menemukan beberapa file yang telah dihapus.

Teknik akuisisi ini dapat dikatakan sebagai partial akuisisi karena data yang diakuisisi hanya sebagian datanya saja buka keseluruhan isi hardisknya. Dan teknik akuisisi ini telah memenuhi persayaratan untuk dilakukannya partial akuisisi. Hal ini berdasarkan persyaratan yang terangkum dalam (Badan Standarisasi Nasional, 2014) . Adapun persyaratan dilakukannya partial akuisisi adalah sebagai berikut :

a. Kapasitas penyimpanan terlalu besar untuk dilakukan akuisisi
b. Pentingnya sistem sehingga tidak memungkinkan untuk mematikan sistem
c. Ketika data yang diakuisisi hanya sebagian data atau data yang diperlukan saja
d. Ketika dibatasi oleh penegak hukum seperti surat perintah pencarian yang membatasi ruang lingkup akuisisi

4.2.2 Hasil Akuisisi

Teknik akuisisi ini merupakan teknik akuisisi yang dilakukan dengan mengakuisisi secara langsung pada server proxmox terhadap salah satu satu server virtual yang ada didalamnya menggunakan perintah dc3dd. Dalam proxmox partisi sistem operasi virtualnya tersimpan dalam local-lvm pada /dev/mapper/. Dalam /dev/mapper terdapat 2 OS yaitu pve-vm-100- -disk- -1 dan pve-vm-102- -disk- -1. Karena yang akan diakuisisi hanya OS ubuntu yang terletak pada vm - -100 maka yang akan dilakukan akuisisi hanya file mapper pada pve-vm-100- -disk- -1 .

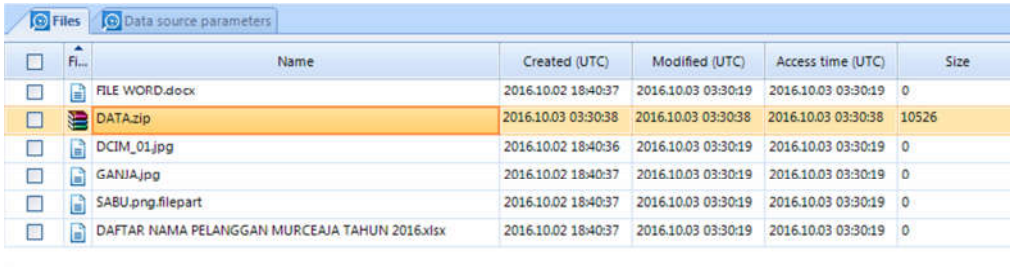


Gambar 3: Hasil Imaging Teknik Akuisisi Virtualisasi Server

Gambar 3 menggambarkan proses dan hasil dari teknik akuisisi. Dimana partisi virtual yang diakuisisi terletak dalam /dev/mapper/pve-vm—100—1. Dan berhasil menghasilkan file akuisisi evidence01.dd dengan nilai hash md5 8E5CA1BD8C138C600F48E371D9E86A44.

4.3 Eksaminasi dan Analisis

Setelah dikakukan berhasil melakukan akuisisi tahapan selanjutnya adalah melakukan ekstraksi dan menganalisis data pada hasil akuisisi menggunakan belkasoft evidence center. Dari hasil eksaminasi yang dilakukan ternyata hasil akuisisi dapat membaca keseluruhan isi file dalam partisi dalam VM OS ubuntu. Dan juga bisa menemukan kembali beberapa file yang telah dihapus berdasarkan skenario kasus yang telah direncanakan. Adapun file yang telah dihapus dapat dilihat pada gambar 4 berikut :

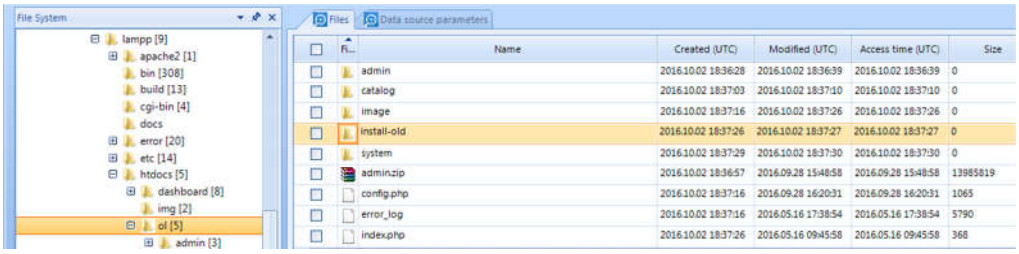


Gambar 4:1 Tampilan *file* yang telah dihapus

Gambar 4 menampilkan beberapa file yang telah dihapus dan berhasil ditemukan oleh tool forensik belkasoft evidence center. File tersebut adalah file yang berekstensi .docx, .zip, .jpg, .png, dan .xlsx.

Dari hasil ekstraksi data menggunakan *belkasoft* juga ditemukan dimana lokasi penyimpanan dari *web server* dan *file* web *server* tersebut dapat dibaca

dengan tool belkasoft *evidence center*. *File* lokasi penyimpanan dari web *server* dapat pada gambar 5 berikut :



Gambar 5: Lokasi penyimpanan *web server*

Gambar 5 menggambarkan lokasi dari penyimpanan file web server. File web server tersebut tersimpan dalam directory /opt/lampp/htdocs/ol/.

5. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan, maka didapatkan kesimpulan yaitu teknik akuisisi yang dilakukan untuk mengakuisisi salah satu virtual mesin yang dalam server proxmox dinyatakan berhasil karena salah partisi vm dalam *server proxmox* berhasil diakuisisi tanpa mengganggu sistem operasi yang lainnya dan semua *file* yang ada dalam partisi tersebut dapat dibaca oleh *software* forensik yaitu *belkasoft* dan *autopsy*. Dan juga beberapa *file* yang telah dihapus dapat ditemukan kembali.

Daftar Pustaka

Adelstein, F. (2006). Diagnosing your system without killing it first. *Communications of the ACM*, *49*(2), 63–66. https://doi.org/10.1145/1113034.1113070

Agarwal, A., Gupta, M., & Gupta, S. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118–134.

Al-Azhar, M. N. (2012). *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba, Infotek.

Badan Standarisasi Nasional. (2014). *SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Jakarta.

Kumar, R., & Charu, S. (2015). An Importance of Using Virtualization Technology in Cloud Computing. *Global Journal of Computers & Technology*, *1*(2), 56–60.

Purbo, O. W. (2012). *Membuat Sendiri Cloud Computing Server Menggunakan Open Source*. Yogyakarta: Andi Publisher.

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056. Retrieved from http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf

Spiceworks.com. (2016). State of it report. Retrieved June 19, 2016, from http://www.spiceworks.com/marketing/state-of-it/report/

Zimmerman, S., Glavach, D., Programs, S., Design, A., Intelligence, U., Cases, U., … Studies, I. C. (2011). Cyber Forensics in the Cloud. *IAnewsletter*, *14*(1), 4–7.