ANALISIS FORENSIK BUKTI DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Imam Riadi [1)] , Rusydi Umar [2)], Imam Mahfudl Nasrulloh [3)]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan Yogyakarta,
[2]Program Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta,
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta
Jalan Prof. Dr. Soepomo, S.H., Umbulharjo, Yogyakarta 55164
[1]imam.riadi@is.uad.ac.id, [2]rusydi_umar@rocketmail.com, [3]mahfudz.mail@gmail.com

ABSTRAK

Bukti digital menjadi hal terpenting dalam pembuktian dan penyidikan kasus kejahatan komputer. Aktivitas kejahatan yang melibatkan perangkat komputer besar kemungkinan terekam oleh sistem komputer pada media penyimpanan. Perkembangan teknologi perangkat keras komputer semakin berkembang pesat, pada teknologi Non Volatile Memory saat ini berkembang teknologi Solid State Disk (SSD). SSD merupakan salah satu media penyimpanan utama selain Harddisk. Bukti digital yang tersimpan pada media penyimpanan utama dapat berupa file yang berisi data, history, atau log pada sistem komputer yang berjalan. Penggunaan software pembeku drive pada komputer sering dilakukan oleh teknisi atau pranata komputer, software tersebut digunakan untuk melindungi komputer dari perubahan yang tidak dikehendaki. Sistem komputer yang ter-install software pembeku drive menjadikan perubahan yang terjadi pada sistem komputer tidak disimpan secara fisik pada media penyimpanan utama, jika komputer di-restart maka keadaan sistem komputer akan kembali seperti semula. Contoh dari software pembeku drive diantaranya Deep Freeze dan Shadow Defender. Ketika kasus ini terjadi apa yang harus dilakukan oleh investigator forensik? Untuk itu pada makalah ini dipaparkan bagaimana menganalisa forensik bukti digital pada media penyimpanan utama yaitu SSD dengan kondisi sistem komputer yang terinstal software pembeku drive. Analisa forensik bukti digital dilakukan dengan metode pengambilan data secara statis dan tahapan analisa forensik dengan metode National Institute of Standars and Technology (NIST) untuk mendapatkan bukti digital.

Kata Kunci : Forensik, Bukti, Digital, SSD, NIST

ABSTRACT

Digital evidence becomes important in the proof and investigation of computer crime cases. Crime activities involving computer equipment may be captured by computer systems on storage media. The development of computer hardware technology is growing rapidly, in Non Volatile Memory technology is currently developing Solid State Disk technology. SSD is one of the main storage media besides Hard disk. The digital evidence stored on the primary storage medium can be a file containing data, history, or logs on a running computer system. The use of drive freezing software on computers is often done by computer technician, the software is used to protect the computer from changes. The computer system that installed the freeze drive software makes the changes that occur in the computer system is not stored physically on the main storage media, if the computer is restarted then the computer system will return to original. Examples of freeze drive software include Deep Freeze and Shadow Defender. When this case happens what is done by forensic investigators? This paper describes how to analyze forensic digital evidence on the main storage media SSD with the condition of the computer system that installed the freeze drive software. Forensic analysis of digital evidence is performed by statistical data retrieval methods and forensic analysis stages by the National Institute of Standards and Technology (NIST) method to obtain digital evidence.

Keywords: *Forensic, Digital, Evidence, SSD, NIST*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang demikian pesat telah membawa perubahan luar biasa bagi kemajuan peradaban dan kebudayaan umat manusia. Teknologi informasi dan komunikasi telah membuka cakrawala baru bagi masyarakat untuk memperoleh informasi secara cepat dan bebas. Teknologi informasi dan komunikasi memiliki andil yang sangat besar dalam perkembangan perangkat keras pemrosesan data yaitu perangkat komputer. Kegiatan pengolahan informasi yang pada mulanya menuntut peralatan-peralatan pemrosesan data yang sangat besar dan rumit, kini digantikan oleh perangkat-perangkat otomatisasi digital dan portable. Pada saat ini sebagian besar aktifitas manusia yang berhubungan dengan data, informasi, dan komunikasi secara langsung maupun tidak langsung akan berhubungan perangkat komputer. Penggunaan dan penerapan teknologi komputer bagi kelangsungan dan kenyamanan hidup manusia juga memiliki dampak positif maupun dampak negatif. Secara positif dampak dari teknologi komputer yang ditimbulkan sangat bermanfaat, sehingga dapat membantu proses dari pekerjaan yang sulit menjadi mudah dan membantu aktivitas manusia menjadi lebih cepat. Dampak teknologi komputer secara negatif ditimbulkan dari penyalahgunaan terhadap teknologi komputer yang digunakan untuk tindak kejahatan sehingga dapat merugikan perseorangan, golongan, instansi atau lembaga, atau bahkan negara.

Kejahatan komputer atau disebut computer crime merupakan kejahatan yang melibatkan teknologi [1]. Kejahatan komputer memiliki bukti digital dari tindak kejahatan berupa jejak aktivitas kejahatan yang dilakukan dan perlu dilakukan analisa terhadap bukti digital yang didapatkan dengan ilmu dan metode forensik. Pada bidang teknologi, analisa forensik terhadap barang bukti digital atau elektronik disebut dengan sebutan komputer forensik atau digital forensic [2]. Komputer forensik atau digital forensic merupakan tindakan memperoleh, mengambil, melestarikan, dan menyajikan data sesuai dengan metode dan tool forensik [1]. Pada kasus-kasus kejahatan komputer yang terjadi pada umumnya akan meninggalkan barang bukti, barang bukti tersebut dapat berupa elektronik maupun barang bukti digital. Barang bukti elektronik dapat berupa bentuk fisik dari perangkat tersebut atau dapat berupa media penyimpanan data (storage device), sedangkan barang bukti digital dapat berupa file data, history, atau log. Bukti digital menjadi hal terpenting dalam suatu kasus kejahatan komputer, karena aktivitas kejahatan yang dilakukan kemungkinan besar terekam oleh sistem komputer pada media penyimpanan utama komputer. Bukti digital dapat diketahui dan dilihat pada saat kejahatan dilakukan atau setelah terjadi tindak kejahatan. Analisa bukti digital perlu dilakukan sesuai prosedur penanganan khusus dengan metode analisa forensik yang tepat dan dengan mengkomparasikan berbagai tool forensik untuk mendapatkan bukti digital yang baik, sehingga dari bukti digital tersebut diperoleh informasi untuk mendukung putusan suatu perkara tindak kejahatan komputer.

Komputer memiliki dua jenis media penyimpanan berjenis Non Volatile Memory dan Volatile Memory. Non Volatile Memory memungkinkan data yang tersimpan tidak akan hilang meskipun aliran listrik terputus, seperti Hard Drive, Harddisk, Solid State Drive, USB flashdisk, dan Nand Flash. Sedangkan media penyimpanan Violatile Memory akan kehilangan data ketika aliran listrik terputus, seperti pada RAM (Random Access Memory) [3]. Perkembangan teknologi perangkat keras komputer semakin berkembang pesat. Pada teknologi Non Volatile Memory saat ini berkembang teknologi Solid State Disk (SSD). SSD merupakan salah satu media penyimpanan utama selain Harddisk. Teknologi SSD menggunakan solid state memory untuk penyimpanan datanya, SSD menggunakan teknologi yang hampir mirip seperti RAM (Random Access Memory). SSD menggunakan semikonduktor, sedangkan pada Harddisk menggunakan platter magnetis yang berputar. Meskipun secara teknis bukan sebuah disk tetapi bentuk atau dimensi SSD sama dengan harddisk, sehingga dapat diletakkan pada komputer dan notebook.

SSD juga menggunakan interface yang sama pada Harddisk yaitu Serial Advanced Technology Attachment (SATA) atau Integrated Drive Electronics (IDE). Saat ini SSD berangsur-angsur menggantikan posisi Harddisk pada media penyimpanan utama komputer [3].

Pada kasus kejahatan komputer pribadi dengan sistem operasi Windows menjadi permasalahan bagi penyidik untuk menemukan file dokumen, history, serta perubahan yang dilakukan oleh pelaku saat Harddisk dibekukan dan di Indonesia sebagian besar pelaku kejahatan komputer atau cybercrime lebih cenderung mengakses Internet di tempat umum seperti warnet, karena jejak browser akan terhapus dari memori secara otomatis setelah komputer itu direstart [4]. Dikatakan oleh perusahaan pengembang software Deep Freeze pada websitenya deepfreeze.com.au, software untuk membekukan drive seperti Deep Freeze dapat mengurangi biaya pemeliharaan komputer sebesar 63%, sehingga mayoritas

perkantoran, instansi, dan warnet di Indonesia mengadopsi perangkat lunak ini. Penggunaan software pembeku drive pada komputer sering dilakukan oleh teknisi atau pranata komputer, software tersebut digunakan untuk melindungi komputer dari perubahan yang tidak dikehendaki. Sistem komputer yang ter- install software pembeku drive menjadikan perubahan yang terjadi pada sistem komputer tidak disimpan secara fisik pada media penyimpanan utama, jika komputer di-restart maka keadaan sistem komputer akan kembali seperti semula. Contoh dari software pembeku drive diantaranya DeepFreeze, Shadow Defender, Windows Steady State, dan Toolwiz Time Freeze. Pada software-software tersebut memiliki fitur pembeku drive media penyimpanan utama seperti Harddisk dan SSD, apabila diaktifkan fiturnya maka perubahan yang terjadi pada sistem komputer tersebut tidak akan disimpan secara fisik pada sistem komputer. Jika komputer tersebut dimatikan dan dihidupkan kembali maka keadaan sistem komputer seperti semula sebelum dilakukan perubahan. Begitu juga jika melakukan proses penyimpanan file pada drive yang dibekukan, maka ketika komputer dimatikan dan dihidupkan kembali drive akan kembali seperti sebelum dilakukan penyimpanan file. Hal ini menjadi tantangan investigator forensik untuk melakukan analisa bukti digital dengan kondisi tersebut diatas.

Literatur Review

Pengumpulan bukti digital pada Non Volatile Memory atau Non Volatile Evidence Collection melibatkan pengumpulan bukti dari media penyimpan, seperti MMC Card, Compact Flash, Flashdisk, SD Card, Flash Memory, dan yang sejenis [1]. Alat forensik yang sesuai harus digunakan untuk mengumpulkan bukti untuk memastikan diterimanya bukti digital tersebut. Integritas dan keaslian dari bukti yang dikumpulkan harus dipastikan melalui mekanisme seperti hashing, dan write protection. Penelitian forensik digital pada SSD menunjukkan hasil perolehan data pada memori SSD tidak dapat diprediksi dan bervariasi [5]. Pada penelitian terhadap Harddisk dan SSD dengan file bukti yang sama, dilakukan penghapusan file dan format dengan interval yang sama, dan dengan Image drive dibuat dengan menggunakan software FTK Imager dan dianalisis secara hati-hati menggunakan FTK Toolkit. Menurut hasil penelitian tersebut terlihat bahwa setelah dilakukan tindakan yang sama pada kedua drive tersebut hasil yang diperoleh tidak sama, sehingga dapat menimbulkan masalah bagi penyidik forensik [6].

Hasil penelitian diatas terjawab pada penelitian ini [7] dikatakan fitur TRIM yang ada pada SSD terbukti berpengaruh terhadap praktek examinasi dan analisis forensika digital. Pada SSD dalam posisi fitur TRIM dalam keadaan non-aktif (disable), sebagian besar data yang terhapus data di-recovery kembali seperti halnya melakukan recovery data pada Harddisk konvensional. Namun, berbeda dengan SSD dalam posisi fitur TRIM dalam keadaan aktif (enable), sebagian besar data yang terhapus tidak dapat di-recovery kembali. TRIM merupakan sebuah perintah yang langsung ditujukan kepada kepada firmware dari SSD [7]. Perbedaan penggunaan tool forensik juga akan mempengaruhi bukti digital yang didapat, pada penelitian yang dilakukan [8]

menggunakan tool forensik yaitu X-Ways Forensics dan WinHex dari kedua tool tersebut dapat digunakan untuk mekanisme pengembalian data atau file secara otomatis maupun pengembalian secara manual, dan dapat digunakan pada media penyimpanan termasuk SSD. Hasil penelitian [8] WinHex memberikan kepuasan dalam pencarian fungsi yang sangat cepat secara simultan pada seluruh data, termasuk untuk data yang telah dihapus, dan data yang disembunyikan. Selain obyek forensik, tool forensik, dan yang tidak kalah penting pada forensik digital adalah metode analisa forensik itu sendiri. Dalam pemilihan model, metode, atau sistematika investigasi digital diantaranya harus memenuhi individualitas (individuality), keterulangan (repeatability), kehandalan (reliability), kinerja (performance), kemampuan uji (testability), skalabilitas (scalability), dan standar kualitas (quality standards) [1]. Pada analisa forensik dapat menggunakan metode dari The U.S. National Institute of Justice (NIJ), dengan alur identification, collection, examination, analysis, dan reporting [9], atau dapat menggunakan metode dari National Institute of Standards and Technology (NIST) dengan rangkaian forensik collection, examination, analysis, dan reporting [10].

METODE PENELITIAN

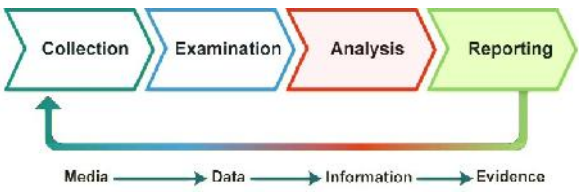
Metode Pengambilan Salinan Bukti Digital

Pengambilan bukti digital mengacu pada metode static forensic atau disebut juga metode akuisisi secara tradisional, hal ini berfokus pada memeriksa salinan duplikat [11]. Salinan duplikat atau image dimbil dari salinan media simpan SSD, seperti file yang dihapus, riwayat penjelajahan web, file yang dibuka, riwayat login pengguna, dan sebagainya. Pengambilan salinan bukti digital harus tetap dipastikan konsisten dengan aslinya sehingga hasil yang akan didapat juga baik, pada umumnya ketika menjalankan

tool forensik baik dalam analisis static dan live untuk memperoleh data dapat menimpa struktur data dari proses data yang sebelumnya berjalan yang dapat menyebabkan inkonsistensi dalam bukti yang akan diperoleh untuk analisis forensik digital [12]. Penggunaan perangkat lunak seperti Fundl, dan RegCon digunakan untuk membuat salinan dan pemilahan data bukti digital untuk dianalisis dan tujuan presentasi [12]. Oleh karena itu, perlunya menggunakan metode yang tepat dan dengan tool forensik yang tepat sehingga dapat dideteksi dan perubahan isi dari media penyimpanan dapat diminimalisir. Bukti digital dapat diperoleh dengan menggunakan berbagai jenis perangkat eksternal seperti USB flashdisk, Harddisk eksternal, CD atau DVD, dan kemudian file salinan dibawa ke laboratorium forensik agar para penyelidik melakukan berbagai jenis langkah untuk menganalisis bukti digital.

Metode Analisa Forensik Bukti Digital

Metode dari National Institute of Standards Technology (NIST) [1] digunakan untuk melakukan tahapan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital. Pada tahap awal data yang didapat dikumpulkan dan diperiksa, kemudian tahap ekstraksi atau pembuatan image data dari SSD dan diubah menjadi format yang dapat diproses oleh tool forensik. Selanjutnya data diterjemahkan menjadi informasi melalui analisis, hasil pada tahap ini menjadi bukti analogi dari pengetahuan ke dalam tindakan menggunakan informasi yang didapatkan dari analisis dalam pelaporan. Menurut penelitian [13] disebutkan, melakukan teknik forensik dan analisa forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir 100% dalam mengumpulkan data-data forensik. Oleh karena itu pada penelitian ini mengacu pada metode yang sudah ada yaitu dengan metode NIST dengan pengembangan sesuai dengan obyek penelitian dan bukti digital yang akan diambil. Jika digambarkan metode NIST mempunyai beberapa tahap yaitu seperti pada Gambar 2.1 [1].



Gambar 2.1. Tahapan Metode National Institute of Standars and Technology (NIST)

Tahapan dari National Institute of Standars and Technology (NIST) ini terbagi menjadi empat tahapan yakni Collecting, Examination, Analysis, dan Reporting [1]. Secara lengkap dipaparkan sebagai berikut:

Tahap Collection (Pengumpulan) merupakan serangkaian kegiatan untuk mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman, dan pengambilan data dari sumber data yang relevan, serta menjaga integritas data.

Tahap Examination (Pemeriksaan) merupakan tahap pemeriksaan data yang dikumpulkan secara forensik dengan scenario otomatis atau manual, serta memastikan bahwa data tersebut memang unik dan asli sesuai dengan yang terdapat pada tempat kejadian perkara. Untuk data digital, misalnya melakukan identifikasi dengan teknik hashing.

Tahap Analysis (Meneliti) dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya disebut sebagai barang bukti digital yang harus dapat dipertanggungjawabkan secara keilmiahan dan hukum.

Tahap Reporting (Pelaporan) dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dana analisis di atas yang sesuai dengan ivestigasi. Selanjutnya melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan (misalnya, pemeriksaan forensik dari sumber data tambahan, mengamankan celah yang teridentifikasi, atau meningkatkan kontrol keamanan yang ada), dan memberikan rekomendasi untuk perbaikan kebijakan, metode, tool, atau aspek lainnya pendukung pada proses tindakan digital forensik.

HASIL PEMBAHASAN

Solid State Drive (SSD)

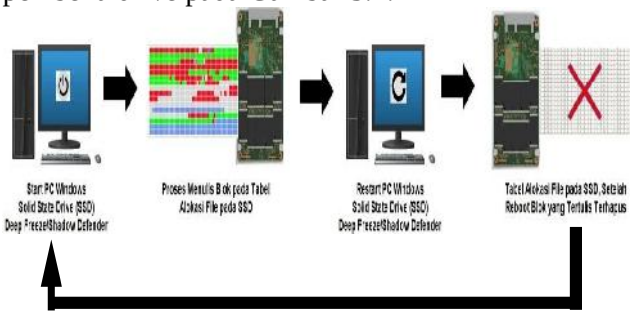
Media penyimpanan terdiri dari duajenis Non Volatile Memory dan Volatile Memory [3]. Non Volatile Memory memungkinkan data yang tersimpan tidak akan hilang meskipun aliran listrik terputus seperti Hard Drive, Harddisk, Solid State Drive (SSD), USB flashdisk, dan Nand Flash, sedangkan media penyimpanan Violatile Memory akan kehilangan data ketika aliran listrik terputus, seperti pada RAM (Random Access Memory) [3]. Solid State Drive atau Solid State Disk disingkat SSD adalah perangkat penyimpan data yang menggunakan serangkaian IC sebagai memori yang digunakan untuk menyimpan data atau informasi [5]. SSD merupakan salah satu media penyimpanan utama selain Harddisk. Teknologi SSD menggunakan solid state memory untuk penyimpanan datanya, SSD menggunakan teknologi yang hampir mirip seperti RAM (Random Access Memory) [3]. SSD menggunakan semikonduktor, sedangkan pada Harddisk menggunakan platter magnetis yang berputar. Meskipun secara teknis bukan sebuah disk tetapi bentuk atau dimensi SSD sama dengan harddisk, sehingga dapat diletakkan pada komputer dan notebook. SSD juga menggunakan interface yang sama pada Harddisk yaitu Serial Advanced Technology Attachment (SATA) atau Integrated Drive Electronics (IDE). Saat ini SSD berangsur-angsur menggantikan posisi Harddisk pada media penyimpanan utama komputer [3].

Frozen Solid State Drive (SSD)

Frozen Solid State Drive yang dimaksudkan disini adalah SSD tersebut dilakukan pembekuan drive, dimana sistem komputer tersebut terinstal software keamanan yang digunakan untuk melindungi komputer dari perubahan yang tidak dikehendaki. Software yang digunakan pada penelitian ini adalah Deep Freeze dan Shadow Defender. Pada software tersebut memiliki fitur pembeku suatu drive, apabila diaktifkan fiturnya maka perubahan yang terjadi pada sistem komputer tersebut tidak akan disimpan secara fisik pada drive penyimpanan utama komputer. Jika komputer tersebut dimatikan dan dihidupkan kembali maka keadaan sistem komputer akan kembali seperti semula

sebelum dilakukan perubahan. Begitu juga jika melakukan proses penyimpanan file atau data pada drive yang dibekukan, maka ketika komputer dimatikan dan dihidupkan kembali drive akan kembali pada saat dibekukan. Pada sistem komputer seperti inilah yang dilakukan analisa bukti digital.

Pada website pengembang software Deep Freeze [14] dikatakan, Deep Freeze menggunakan teknologi untuk mengalihkan informasi yang ditulis ke hard drive ke tabel alokasi, sehingga data asli tetap utuh. Informasi yang dialihkan pada tabel alokasi tidak lagi direferensikan begitu komputer di-restart, sehingga mengembalikan komputer ke keadaan semula, sampai ke byte terakhir. Pengembang software Shadow Defender pada [15] aplikasi Shadow Defender akan mengambil snapshot dari disk dan menjalankan setiap file dalam mode virtual. Setelah pengguna keluar dari "dimensi paralel" setiap perubahan pada sistem dan file pada disk akan dihapus. Kesimpulan adalah bahwa komputer tidak akan terpengaruh oleh perubahan apapun dan tidak ada file berbahaya yang akan ditulis ke komputer. Begitu juga pengembang software Toolwiz Time Freeze pada [16], jika tidak ingin membuat perubahan yang tidak diinginkan pada sistem, perubahan apa yang dibuat, tidak peduli apa yang terjadi, jika dilakukan restart maka akan mengembalikan keadaan semula. Begitu juga file yang didownload dari web akan dihapus, dan perubahan yang tidak diinginkan lainnya semuanya akan dibatalkan saat dilakukan restart pada PC. Diilustrasikan software pembeku drive pada Gambar 3.1.



Gambar 3.1 Cara Kerja Software

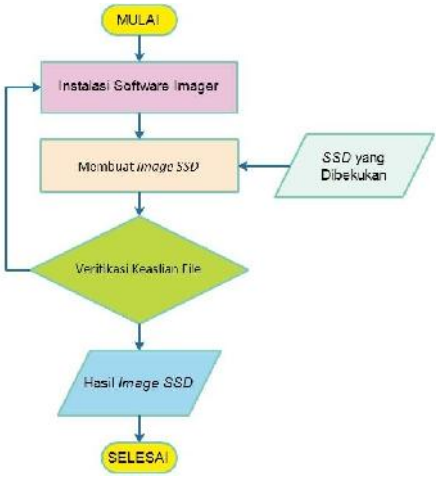
Pembeku Drive

Gambar 3.1 merupakan cara kerja dari software pembeku drive. Pada komputer yang terinstal software pembeku drive seperti Deep Freeze atau Shadow Defender ketika komputer dinyalakan dan digunakan

maka blok pada tabel alokasi file akan terisi, namun ketika komputer di-restart atau dimatikan dan dihidupkan kembali maka blok pada tabel alokasi file akan terhapus kembali.

Tahapan Pengambilan Salinan Bukti Digital pada Frozen Solid State Drive (SSD)

Tahapan pengambilan salinan bukti digital pada SSD yang dibekukan (frozen solid state drive) mengacu pada metode statis forensik, dalam penelitian ini seperti disajikan pada Gambar 3.2 dan pada penelitian ini menggunakan komputer uji coba untuk melakukan poreses pengambilan salinan bukti digital.



Gambar 3.2 Tahapan Pengambilan Salinan Bukti Digital pada Frozen Solid State Drive (SSD)

Tahapan diatas merupakan alur dalam pengambilan pengambilan salinan bukti digital. Pada tahap pengambilan salinan bukti digital ini yang terpenting adalah keaslian file dan hasil salinan baik dengan kata lain image salinan dapat dibuka kembali.

Tahapan Analisa Forensik Bukti Digital pada Frozen Solid State Drive (SSD)

Gambar 3.3 Tahapan Analisa Forensik Bukti Digital pada Frozen Solid State Drive (SSD)

Pada tahapan analisa forensik bukti digital pada SSD yang dibekukan (frozen solid state

drive) secara garis besar mengimplementasikan dan mengadaptasi metode forensik dari National Institute of Standards and Technology (NIST), hasil salinan atau image dilakukan duplikasi dan dianalisa untuk menemukan bukti digital. Bukti digital yang diharapkan ditemukan adalah file dokumen (.doc, .xls, .pdf), file gambar (.jpg, .png), catatan log internet, dan catatan login terbaru, tahapan analisis forensik digambarkan pada gambar 3.3.

Tahapan Implementasi dan Pengujian

Tahap implementasi dan pengujian forensik bukti digital pada SSD yang dibekukan (frozen solid state drive) ditunjukkan pada Gambar 3.4. Implementasi dan pengujian dilakukan dengan tahapan yang telah ditentukan dalam desain skenario, dengan tujuan untuk mendapatkan bukti digital seperti pada skenario perencanaan awal.

Gambar 3.4 Tahapan Implementasi dan Pengujian

Tahapan diatas merupakan implementasi dan pengujian forensik bukti digital pada SSD yang dibekukan (frozen solid state drive). Pada tahap implementasi dan pengujian ini dilakukan sekenario pengujian, dimana komputer diperlakukan dan dikondisikan dengan ter-install software pembeku drive dan digunakan seperti pada umumnya komputer.

PENUTUP

Pembahasan yang sudah dipaparkan pada makalah ini, bukti digital menjadi hal terpenting dalam suatu kasus kejahatan komputer. Analisis bukti digital perlu dilakukan dengan prosedur penanganan khusus dengan metode digital forensik yang tepat, dari pengambilan salinan bukti digital sampai pada tahapan analisa forensik dan juga mengkomparasikan dengan berbagai tool forensik untuk mendapatkan bukti digital yang diharapkan oleh investigator forensik. Dalam melakukan tindakan forensik baik berupa langkah atau tahapan yang jelas dapat menggunakan salah satu metode dari National Institute of Standards and Technology (NIST) dengan rangkaian forensik collection, examination, analysis, dan reporting. Analisa bukti digital juga harus memenuhi beberapa kriteria diantaranya individualitas, keterulangan, kehandalan, kinerja, kemampuan uji, skalabilitas, dan standar kualitas. Penelitian ini diharapkan dapat bermanfaat untuk analisa komputer forensik dan investigasi forensik pada bukti digital. Tidak hanya sebatas itu, kemungkinan pola-pola kejahatan komputer akan mengikuti perkembangan teknologi, sehingga perlu dilakukan penelitian dan pengembangan lanjutan dengan menyesuaikan teknologi yang berkembang di masyarakat, tool forensik yang berkembang, dan metode forensik yang berkembang.

DAFTAR PUSTAKA

Agarwal, Ankit. Gupta, Megha. Gupta, Saurabh. 2011. Systematic Digital Forensic Investigation Model. International Journal of Computer Science and Security (IJCSS), Volume 5. Nomor 1. Halaman 118–131.

Ridho, Faizin. Yudhana, Anton. Riadi, Imam. 2016. Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time. Volume 2. Nomor 1. Halaman 111–116.

Silberschatz, Abraham. Galvin, Peter Baer. Gagne, Greg. 2013. Operating Systeme Concepts: Ninth Edition.

Willey. United States of America. Halaman 469.

Albanna, Faiz. Riadi, Imam. 2017. Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. International Journal of Computer Science and Information Security (IJCSIS)., Volume 15. Nomor 1. Halaman 173–178.

Geier, Florian. 2015. The Differences Between SSD And HDD Technology Regarding Forensic Investigations. Computer Science. Degree of Computer Science. Linnaeus University. Swedia.

Marupudi, Shiva Sai Ram. 2017. Solid State Drive: New Challenge for Forensic Investigation. Information Assurance. Degree of Master of Science. Cloud State University. Minnesota.

Ramadhan, Rizdqi Akbar. Prayudi, Yudi. Sugiantoro, Bambang. 2017. Implementasi Dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive. TEKNOMATIKA. Volume 9. Nomor 2. Halaman 1–13.

Rosalina, Vidila. Suhendarsah, Andri. Natsir, M. 2016. Analisis Data Recovery Menggunakan Software Forensic: Winhex And X-Ways Forensic. PROSISKO. Volume 3. Nomor 1. Halaman 51-55.

Nur Faiz, Muhammad. Umar, Rusydi. Yudhana, Anton. 2017. Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. JISKa. Volume 1. Nomor 3. Halaman 108–114.

Riadi, Imam. Umar, Rusydi. Firdonsyah, Arizona. 2017. Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. International Journal of Computer Science and Information Security (IJCSIS). Volume 15. Nomor 5. Halaman 155-160.

Riadi, Imam. Umar, Rusydi. Sukarno, Wasito. 2015. Analisis Forensik Serangan SQL Injection Menggunakan Metode Statis Forensik. Prosiding Interdisciplinary Postgraduate Student Conference 1st. Yogyakarta. Program Pascasarjana Universitas Muhammadiyah Yogyakarta (PPs UMY). Halaman 102–103.

Rafique, Mamoona, & Khan, M.N.A. 2013. Exploring Static and Live Digital Forensics: Methods, Practices and Tools. International Journal of Scientific & Engineering Research. Volume 4. Nomor 10. Halaman 1048–1056.

Anggara Putra, Roni. Fadlil, Abdul. Riadi, Imam. 2017. Forensik Mobile Pada Smartwatch Berbasis Android. JURTI. Volume 1. Nomor 1. Halaman 41-47.

Deepfreeze. How Deep Freeze Works. Online .ditemukenali 23 November 2017. dari http://deepfreeze.com.au/.

Shadowdefender. What is Shadow Defender?. Online. ditemukenali 25 November 2017. dari http://www.shadowdefender.com/.

Toolwiz. Toolwiz Time Freeze is an easy and effective Instant system restore software. Online. ditemukenali 25 November 2017. dari http://www.toolwiz.com/lead/toolwiz_time_freeze.php.