Digital Forensic
Rabu, 21 Desember 2016 | 11:58:19 WIB **| Endang Kurniawan**

Digital Forensik atau Forensik Digital dikenal sebagai ilmu yang mempelajari Ilmu Komputer dan Ilmu Hukum. Mengapa..?, dalam ilmu komputer banyak dipelajari tentang penggunaan komputer dan teknik-teknik bagaimana intruksi yang diberikan dapat dijalankan oleh mensin dengan menggunakan kode-kode biner. Hal ini dimaksudkan agar mesin dapat mengerjakan sesuai dengan perintah yang diberikan. Sementara Ilmu Hukum, menerjemahkan perilaku dan perbuatan sesuai dengan kaidah ataupun aturan yang digunakan sebagai dasar untuk suatu tindakan ataupun perbuatan.

Secara umum, segala aktifitas dikehidupan saat ini menuntut peranan teknologi sebagai perangkat kerja untuk menghemat waktu dan mempermudah pekerjaan. Penggunaan teknologi ini memberikan dampak yang positif dan negative bagi pihak yang menggunakan. Dari sisi positif, penggunaan teknologi dapat memberikan kemudahaan-kemudahaan dalam menyelesaikan suatu pekerjaan. Sedangkan dari sisi negatifnya, seiring perkembangan teknologi yang memuat banyak informasi-informasi yang diberikan, maka dapat menimbulkan pengaruh negatif bagi yang tidak dapat menyaring informasi tersebut.

Berdasarkan dari uraian di atas, ada beberapa definisi yang dapat digunakan sebagai referensi untuk mengenal lebih jauh tentang forensik digital, diantaranya :

Menurut Marcella : forensik digital adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam kejahatan komputer. Istilah ini relatif baru dalam bidang komputer dan teknologi, tapi telah muncul diluar *term* teknologi (berhubungan dengan investigasi bukti-bukti intelijen dalam penegakan hukum dan militer) sejak pertengahan tahun 1980-an.

Menurut Budhisantoso, forensik digital adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum.

Menurut Ruby Alamsyah, forensik digital adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan.

Menurut Muhammad Nuh Al-Azhar, MSc., adalah aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (Pro Justice), yang dalam hal ini adalah untuk membuktikan kejahahatan berteknologi tinggi atau *computer crime* secara ilmiah (*scientific*) hingga bisa mendapatkan bukti - bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut.

Menurut Noblett, forensik digital adalah ilmu yang berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer.

Berdasarkan keterangan dari beberapa ahli di atas, penulis menyimpulkan bahwa forensik digital adalah ***"perpaduan antara ilmu komputer dan ilmu hukum dalam mengolah data secara ilmiah sehingga dapat dipertanggungjawabkan untuk dijadikan barang bukti dipengadilan".***

TUJUAN
adalah untuk mengamankan dan menganalisa bukti digital. Selain itu juga bertujuan untuk mendapatkan fakta-fakta objektif dari sebuah insiden / pelanggaran keamanan sistem informasi.

Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.

Misalnya, melalui Internet Forensik, kita bisa melacak siapa yang mengirim email kepada kita, kapan dikirim dan sang pengirim berada dimana, ataupun misalnya, dapat melacak siapa saja pengunjung suatu website lengkap dengan informasi IP Address, komputer yang dipakai serta berada di daerah/negara mana dan apa saja aktifitas yang dilakukan pada website tersebut.

KOMPONEN

Komponen pada forensik digital pada umumnya hampir sama dengan bidang yang lain. Komponen ini mencakup manusia (people), perangkat/peralatan(equipment) dan aturan (protocol) yang dirangkai, dikelola dan diberdayakan sedemikian rupa dalam upaya mencapai tujuan akhir dengan segala kelayakan dan kualitas sebagaimana dapat dilihat pada gambar berikut :

Manusia yang diperlukan dalam komputer forensik merupakan pelaku yang tentunya mempunyai kualifikasi tertentu untuk mencapai kualitas yang diinginkan.

Belajar forensik tidak sama dengan menjadi ahli dalam bidang forensik. Dibutuhkan lebih dari sekedar pengetahuan umum tentang komputer, tetapi juga pengalaman (experience) disamping berbagai pelatihan (training) pada materi-materi digital forensik yang telah ditempuh dan dibuktikan dengan sertifikat – sertifikat pendukung.

Ada tiga kelompok sebagai pelaku digital forensik :

1. ***Collection Specialist***, yang bertugas mengumpulkan barang bukti berupa digital evidence.
2. ***Examiner***, tingkatan ini hanya memiliki kemampuan sebagai penguji terhadap media dan mengekstrak data.
3. ***Investigator***, tingkatan ini sudah masuk kedalam tingkatan ahli atau sebagai penyidik

Menurut Budhisantoso, secara garis besar perangkat untuk kepentingan digital forensik dapat dibedakan kepada dua kategori yaitu hardware dan software.

Ada banyak jenis perangkat hardware yang digunakan pada implementasi digital forensik dengan fungsi dan kemampuan yang beragam. Mulai dari yang sederhana dengan komponen single – purpose seperti write blocker (fungsinya hampir sama dengan “write-protect” pada disket, pada optical media dan hardisk fungsi seperti ini tidak ada) yang memastikan bahwa data tidak akan berubah manakala diakses, sampai pada sistem komputer lengkap dengan kemampuan server seperti F.R.E.D (*Forensic Recovery of Evidence Device*).

Sedangkan perangkat software dikelompokkan kedalam dua kelompok yaitu aplikasi berbasis command line dan aplikasi berbasis GUI (*Graphical User Interface*)

Aturan merupakan komponen yang paling penting dalam pemodelan digital forensik, didalamnya mencakup prosedur dalam mendapatkan, menggali, menganalisa barang bukti dan akhirnya bagaimana menyajikan hasil penyelidikan dalam laporan.

TAHAPAN

Ada berbagai tahapan pada proses implementasi digital forensik. Namun menurut Kemmish, secara garis besar dapat diklasifikasikan kepada empat tahapan, yaitu :

1. Identifikasi bukti digital
2. Penyimpanan bukti digital
3. Analisa bukti digital

4. Presentasi

Keempat tahapan ini secara terurut dan berkesinambungan digambarkan pada gambar berikut:

1. Identifikasi Bukti Digital
Pada tahap ini segala bukti-bukti yang mendukung penyelidikan dikumpulkan. Penyelidikan dimulai dari identifikasi dimana bukti itu berada, dimana disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan.

Media digital yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, pen drive, harddisk, atau CD-ROM), PDA, handphone, smart card, sms, e-mail, cookies, source code, windows registry, web browser bookmark, chat log, dokumen, log file, atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Tahapan ini merupakan tahapan yang sangat menentukan karena bukti – bukti yang didapatkan akan sangat mendukung penyelidikan untuk mengajukan seseorang ke pengadilan dan diproses sesuai hukum hingga akhirnya dijebloskan ke tahanan.

Penelusuran bisa dilakukan untuk sekedar mencari "ada informasi apa disini?" sampai serinci pada "apa urutan peristiwa yang menyebabkan terjadinya situasi terkini?".

Berdasarkan klasifikasinya file yang menjadi objek penelusuran terbagi kepada tiga kategori, yaitu : file arsip (archieved files), file aktif (active files) dan file sisa (residual data). File Arsip adalah file yang tergolong arsip karena kebutuhan file tersebut dalam fungsi pengarsipan. Mencakup penanganan dokumen untuk disimpan dalam format yang ditentukan, proses mendapatkannya kembali dan pendistribusian untuk kebutuhan yang lainnya, misalnya beberapa dokumen yang didigitalisasi untuk disimpan dalam format TIFF untuk menjaga kualitas dokumen.

File aktif adalah file yang memang digunakan untuk berbagai kepentingan yang berkaitan erat dengan kegiatan yang sedang dilakukan, misalnya file-file gambar, dokumen teks, dan lain - lain.

Sedangkan file yang tergolong residual mencakup file-file yang diproduksi seiring proses komputer dan aktivitas pengguna, misalkan catatan penggunan dalam menggunakan internet, database log, berbagai temporary file, dan lain sebagainya.

Beberapa software atau tools yang bisa digunakan dalam mendukung tahapan ini antara lain :

- Forensic Acquisition Utilities (http://users.erols.com/gmgarner/forensics/)
- FTimes (http://ftimes.sourceforge.net/FTimes/index.shtml)
- Liveview (http://liveview.sourceforge.net/)
- Netcat (http://www.atstake.com/research/tools/network_utilities/pdd)
- ProDiscover DFT (www.techpathways.com)
- Psloggedon (http://www.sysinternals.com/ntw2k/freeware/psloggedon.shtml)
- TULP2G (http://sourceforge.net/projects/tulp2g/)
- UnxUtils (http://unxutils.sourceforge.net)
- Webjob (http://webjob.sourceforge.net/WebJob/index.shtml)
- dan lain sebagainya

Forensik pada dasarnya adalah pekerjaan identifikasi sampai dengan muncul hipotesa yang teratur menurut urutan waktu. Sangat tidak mungkin forensik dimulai dengan munculnya hipotesa tanpa ada penelitian yang mendalam berdasarkan bukti - bukti yang ada. Dalam kaitan ini pada digital forensik dikenal istilah *chain of custody* dan rules of *evidence*.

Chain of custody artinya pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi.

Tujuan dari chain of custody adalah:

- Menjamin bahwa bukti itu benar-benar masih asli (authentic).
- Pada saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan karena biasanya jarak antara penyidikan dan persidangan relatif lama.

Beberapa hal yang menjadi pertimbangan sesuai dengan aturan chain of custody ini adalah :

- Siapa yang mengumpulkan bukti?
- Bagaimana dan dimana?
- Siapa yang memiliki bukti tersebut?
- Bagaimana penyimpanan dan pemeliharaan bukti itu?

Lalu sebagai alternatif penyelesaian ada beberapa cara yang bisa dilakukan, yaitu :

- Gunakan catatan yang lengkap mengenai keluar-masuk bukti dari penyimpanan.
- Simpan di tempat yang dianggap aman.
- Akses yang terbatas dalam tempat penyimpanan.
- Catat siapa saja yang dapat mengakses bukti tersebut.

Rules of evidenceartinya pengaturan barang bukti dimana barang bukti harus memiliki keterkaitan dengan kasus yang diinvestigasi dan memiliki kriteria sebagai berikut:

a. Layak dan dapat diterima (Admissible).
Artinya barang bukti yang diajukan harus dapat diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai ke pengadilan.

b. Asli (Authentic).
Barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan bukan rekayasa.

c. Akurat (Accurate).
Barang bukti harus akurat dan dapat dipercaya.

d. Lengkap (Complete).
Bukti dapat dikatakan lengkap jika didalamnya terdapat petunjuk-petunjuk yang lengkap dan terperinci dalam membantu proses investigasi.

2. Penyimpanan Bukti Digital
Tahapan ini mencakup penyimpanan dan penyiapan bukti-bukti yang ada, termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik untuk diteliti. Karena bukti digital bersifat sementara (volatile), mudah rusak, berubah dan hilang, maka pengetahuan yang mendalam dari seorang ahli digital forensik mutlak diperlukan.

Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bahkan menghidupkan dan mematikan komputer dengan tidak hati - hati bisa saja merusak/merubah barang

bukti tersebut. Sebagaimana diungkapkan Peter Plummer, *"When you boot up a computer, several hundred files get changed, the data of access, and so on. Can you say that computer is still exactly as it was when the bad guy had it last?"*

Sebuah pernyataan yang patut dipikirkan bahwa bagaimana kita bisa menjamin kondisi komputer tetap seperti keadaan terakhir ketika ditinggalkan oleh pelaku kriminal manakala komputer tersebut kita matikan atau hidupkan kembali. Karena ketika komputer kita hidupkan terjadi beberapa perubahan pada temporary file, waktu akses, dan seterusnya.

Sekali file-file ini telah berubah ketika komputer dihidupkan tidak ada lagi cara untuk mengembalikan (recover) file-file tersebut kepada keadaan semula. Komputer dalam kondisi hidup juga tidak bisa sembarangan dimatikan. Sebab ketika komputer dimatikan bisa saja ada program penghapus/perusak yang dapat menghapus dan menghilangkan bukti - bukti yang ada. Ada langkah – langkah tertentu yang harus dikuasai oleh seorang ahli digital forensik dalam mematikan / menghidupkan komputer tanpa ikut merusak / menghilangkan barang bukti yang ada didalamnya.

Aturan utama pada tahap ini adalah penyelidikan tidak boleh dilakukan langsung pada bukti asli karena dikhawatirkan akan dapat merubah isi dan struktur yang ada didalamnya.

Mengantisipasi hal ini maka dilakukan copy data secara *Bitstream Image* dari bukti asli ke media penyimpanan lainnya. *Bitstream image* adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk file yang tersembunyi (hidden files), file temporer (temporary file), file yang terdefrag (defragmented file), dan file yang belum teroverwrite.

Dengan kata lain, setiap biner digit demi digit di-copy secara utuh dalam media baru. Teknik ini umumnya diistilahkan dengan *cloning* atau *imaging*. Data hasil cloning inilah yang selanjutnya menjadi objek penelitian dan penyelidikan.

3. Analisa Bukti Digital

Tahapan ini dilaksanakan dengan melakukan analisa secara mendalam terhadap bukti - bukti yang ada. Bukti yang telah didapatkan perlu di – explore kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan, seperti :

- Siapa yang telah melakukan ?
- Apa yang telah dilakukan ?
- Apa saja software yang digunakan ?
- Hasil proses apa yang dihasilkan ?
- Waktu melakukan ?

Penelusuran bisa dilakukan pada data-data sebagai berikut:

- alamat URLyang telah dikunjungi,
- pesan e-mail atau kumpulan alamat e-mail yang terdaftar,
- program word processing atau format ekstensi yang dipakai,
- dokumen spreedsheat yang dipakai,
- format gambar yang dipakai apabila ditemukan,
- file-file yang dihapus maupun diformat,
- password,
- registry windows,
- hidden files,

- log event viewers, dan log application.

Termasuk juga pengecekan pada metadata. Kebanyakan file mempunyai metadata yang berisi informasi yang ditambahkan mengenai file tersebut seperti computer name, total edit time, jumlah editing session, dimana dicetak, berapa kali terjadi penyimpanan (saving), tanggal dan waktu modifikasi.

Selanjutnya melakukan recovery dengan mengembalikan file dan folder yang terhapus, unformat drive, membuat ulang partisi, mengembalikan password, merekonstruksi ulang halaman web yang pernah dikunjungi, mengembalikan email - email yang terhapus dan seterusnya.

Tahapan analisis terbagi dua, yaitu :

a. analisis media (media analysis)

- TestDisk (http://www.cgsecurity.org/testdisk.html)
- Explore2fs (http://uranus.it.swin.edu.au/~jn/linux/explore2fs.htm)
- ProDiscover DFT (http://www.techpathways.com)

b. analisis aplikasi (application analysis)

- Libpff (http://libpff.sourceforge.net)
- Md5deep (http://md5deep.sourceforge.net/)
- MD5summer (http://www.md5summer.org/)
- Outport (http://outport.sourceforge.net/)
- Pasco (http://www.foundstone.com/resources/proddesc/pasco.htm)
- RegRipper (http://windowsir.blogspot.com/2008/04/updated-regripper.html)
- Rifiuti (http://www.foundstone.com/resources/proddesc/rifiuti.htm)
- Event Log Parser (http://www.whitehats.ca/main/members/Malik/malik_eventlogs/malik_eventlogs.html)
- Galleta (http://www.foundstone.com/resources/proddesc/galleta.htm)

4. Presentasi

Presentasi dilakukan dengan menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara hukum di pengadilan. Laporan yang disajikan harus dicross-check langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langsung.

Hasil laporan akan sangat menentukan dalam menetapkan seseorang bersalah atau tidak sehingga harus dipastikan bahwa laporan yang disajikan benar-benar akurat, teruji, dan terbukti.

Beberapa hal penting yang perlu dicantumkan pada saat presentasi / panyajian laporan ini, antara lain :

- Tanggal dan waktu terjadinya pelanggaran
- Tanggal dan waktu pada saat investigasi
- Permasalahan yang terjadi
- Masa berlaku analisa laporan
- Penemuan bukti yang berharga (pada laporan akhir penemuan ini sangat ditekankan sebagai bukti penting proses penyidikan)
- Tehnik khusus yang digunakan, contoh: password cracker
- Bantuan pihak lain (pihak ketiga)

STANDARISASI

Standarisasi harus dapat mengisi seluruh- aktivitas dalam komputer forensik. Hal ini mencakup Pendefinisian, Prinsip, Proses, Hasil, dan “Bahasa”. Sejumlah organisasi yang berhubungan langsung dengan bidang komputer forensik bertujuan untuk- memberikan parameter yang berkualitas. Beberapa organisasi tersebut antara lain IOCE (The International Orga-nization on Computer Evidence), IACIS (The International Association of Computer Investigative Specialist), dan masih banyak lainnya.

sumber :

- Carvey, C. A. H. (n.d.). Digital Forensics with Open Source Tools.
- John R. Vacca. (2005). Computer Forensics: Computer Crime Scene Investigation Second Edition.
- Larry E. Daniel, L. E. (n.d.). Daniel Digital Forensics for Legal Professionals.
- Li, C. (n.d.). Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions.
- Sammes, T., & Jenkinson, B. (2007). Forensic Coputing A Practionier’s Guide.
