IT : DIGITAL FORENSIC

Pratomo Djati Nugroho, S.Pi., M.Kom., CHFI
Dosen STMIK Insan Pembangunan, Bitung. Tangerang.
Data Members Registration of Indonesia Forensic Digital Association (AFDI)

Komisaris Besar Polisi Muhammad Nuh Al-Azhar, M.Sc., CHFI., CEI., ECIH
Chairman of Indonesia Forensic Digital Association (AFDI)
Digital Forensic Analysis Team (DFAT) PUSLABFOR MABES POLRI

ABSTRAK

The increasing of information technology in fact followed by issues around cybercrime and computer security. Nowadays, many cases of law has opened our mind and shows us the critical of digital forensic as the method in proofing crimes beside the law and role of regulation that happening. As more criminals utilize technology to achieve their goals and avoid apprehension, there is a developing need for individuals who can analyze and utilize evidence stored on and transmitted using computers. By applying science methods in investigating digital evidence, made digital forensic as the answer of law standing effort in digital era.

Kata kunci : *Digital Forensic, Evidence, Cybercrime.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah dimanfaatkan secara luas dan mendalam. Banyak institusi ataupun perusahaan yang menggantungkan proses bisnisnya pada bidang teknologi informasi dan komunikasi. Bagi mereka, pemanfaatan teknologi informasi dan komunikasi menjadi hal yang penting dan harus ada dalam proses pengembangan institusi / perusahaan. Sehingga dengan ketergantungan ini tanpa disadari akan meningkatkan resiko institusi / perusahaan tersebut akan kejahatan ataupun penyelewengan di dunia teknologi informasi.

Seiring berjalannya waktu, lahirlah UU ITE pada tanggal 21 April 2008 yang bertujuan untuk mengatur transfer informasi elektronik agar berjalan sesuai dengan etika bertransaksi informasi elektronik. Sehingga dengan adanya UU ITE ini diharapkan tidak ada orang perorang ataupun pihak lain yang merasa dirugikan karena transaksi informasi elektronik tersebut.

Hadirnya UU ITE ternyata dirasa kurang memberikan kontribusi yang besar dalam proses penegakan kasus hukum di Indonesia karena UU ini terkesan hanya mengatur perpindahan informasi elektronik secara umum. Padahal terdapat juga hal-hal yang bersifat detail dalam persoalan kasus hukum dan penegakannya di Indonesia yang belum diatur dalam UU. Hal-hal yang bersifat mendetil inilah yang kemudian dijadikan acuan dalam keamanan teknologi informasi dan lebih jauh lagi dalam hal Forensik IT. Hingga pada akhirnya terbentuklah sistem hukum yang kuat, kompeten, transparan dan memberikan keadilan bagi masyarakat.

2. LANDASAN TEORI

2.1 Sejarah Komputer Forensic

Barang bukti yang berasal dari komputer telah muncul dalam persidangan hampir 30 tahun. Awalnya, hakim menerima bukti tersebut tanpa melakukan pembedaan dengan bentuk bukti lainnya. Seiring dengan kemajuan teknologi komputer, perlakuan serupa dengan bukti tradisional akhirnya menjadi bermasalah. Bukti-bukti komputer mulai masuk kedalam dokumen resmi hukum lewat *US Federal Rules of Evidence* pada tahun 1976. Selanjutnya dengan berbagai perkembangan yang terjadi muncul beberapa dokumen hukum lainnya, antara lain adalah:

- *The Electronic Communications Privacy Act* 1986, berkaitan dengan penyadapan peralatan elektronik.
- *The Computer Security Act* 1987 (*Public Law* 100-235), berkaitan dengan keamanan system komputer pemerintahan.
- *Economic Espionage Act* 1996, berhubungan dengan pencurian rahasia dagang.

Pembuktian dalam dunia maya memiliki karakteristik tersendiri. Hal ini dikarenakan sifat alami dari teknologi komputer memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya. Karena itulah salah satu upaya untuk mengungkap kejahatan komputer adalah lewat pengujian sistem dengan peran sebagai seorang detektif dan bukannya sebagai seorang user. Kejahatan komputer *(cybercrime*) tidak mengenal batas geografis, aktivitas ini bisa dilakukan dari jarak dekat, ataupun dari jarak ribuan kilometer dengan hasil yang serupa. Penjahat biasanya selangkah lebih maju dari penegak hukum, dalam melindungi diri dan menghancurkan barang bukti. Untuk itu tugas ahli digital forensik untuk menegakkan hukum

dengan mengamankan barang bukti, rekonstruksi kejahatan, dan menjamin jika bukti yang dikumpulkan itu akan berguna di persidangan.

Bagaimanapun, digital forensik banyak dibutuhkan dalam berbagai keperluan, bukan hanya pada kasus-kasus kriminal yang melibatkan hukum. Secara umum kebutuhan digital forensik dapat diklasifikasikan sebagai berikut:

1. Keperluan investigasi tindak kriminal dan perkara pelanggaran hukum.
2. Rekonstruksi duduk perkara insiden keamanan komputer.
3. Upaya-upaya pemulihan kerusakan sistem.
4. *Troubleshooting* yang melibatkan hardware maupun software.
5. Keperluan untuk memahami sistem ataupun berbagai perangkat digital dengan lebih baik.

2.2 Definisi, Tujuan dan Manfaat IT Forensic

Komputer forensik adalah suatu disiplin ilmu turunan keamanan komputer yang membahas tentang temuan bukti digital setelah suatu peristiwa terjadi. Kegiatan forensik komputer sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa, dan mempergunakan bukti digital menurut hukum yang berlaku.

Sedangkan definisi IT Forensic menurut para ahli diantaranya:

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

Menurut Judd Robin, yaitu penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin.

Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Tujuan utama dari kegiatan IT Forensic adalah untuk mengamankan dan menganalisa bukti digital dengan cara menjabarkan keadaan terkini dari suatu artefak digital. Istilah artefak digital dapat mencakup sebuah sistem komputer, media penyimpanan (harddisk, flashdisk, CD-ROM), sebuah dokumen elektronik (misalnya sebuah email atau gambar), atau bahkan sederetan paket yang berpindah melalui jaringan komputer.

Manfaat dari kegiatan IT Forensic adalah :

1. Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan.
2. Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir.
3. Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.
4. Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik computer.

2.3 Definisi Digital Forensic

Ada beberapa definisi yang bisa dijadikan acuan tentang apa sebenarnya Digital Forensik. Menurut Marcella : digital forensik 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.

Sedangkan menurut Budhisantoso, digital forensik 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.***

Definisi lain sebagaimana yang terdapat pada situs Wikipedia yaitu: ***Komputer forensik yang juga dikenal dengan nama digital forensik, adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan digital***.

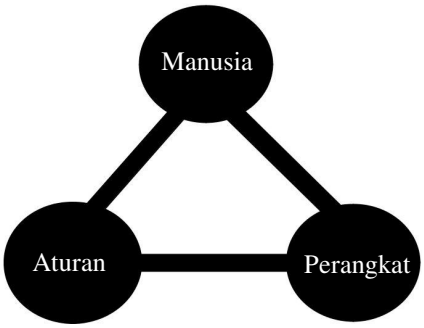
Dari definisi diatas dapat disimpulkan bahwa digital forensic adalah ***penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti / informasi yang secara magnetis tersimpan / disandikan pada komputer atau***

media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum.

Karena luasnya lingkup yang menjadi objek penelitian dan pembahasan digital forensik maka ilmu digital forensik dibagi kedalam beberapa bagian yaitu: ***firewall forensics, network forensics, database forensics*** dan ***mobile device forensics*****.**

2.4 Komponen Digital Forensic

Komponen pada digital forensik 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 bisa dilihat pada gambar berikut :



Gambar 1. Komponen Digital Forensic

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 forensic :

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.

2.5 Undang – Undang IT Forensic

Secara umum, materi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dibagi menjadi dua bagian besar, yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang. Pengaturan mengenai informasi dan transaksi elektronik mengacu pada beberapa instrumen internasional, seperti *UNCITRAL Model Law on eCommerce* dan *UNCITRAL Model Law on eSignature*. Bagian ini dimaksudkan untuk mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat umumnya guna mendapatkan kepastian hukum dalam melakukan transaksi elektronik. Beberapa materi yang diatur, antara lain:

1. Pengakuan informasi / dokumen elektronik sebagai alat bukti hukum yang sah (Pasal 5 & Pasal 6 UU ITE);
2. Tanda tangan elektronik (Pasal 11 & Pasal 12 UU ITE);
3. Penyelenggaraan sertifikasi elektronik (*certification authority*, Pasal 13 & Pasal 14 UU ITE);
4. Penyelenggaraan sistem elektronik (Pasal 15 & Pasal 16 UU ITE);

Beberapa materi perbuatan yang dilarang (*cybercrimes*) yang diatur dalam UU ITE, antara lain:

1. Konten ilegal, yang terdiri dari, antara lain: kesusilaan, perjudian, penghinaan / pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, Pasal 28, dan Pasal 29 UU ITE);

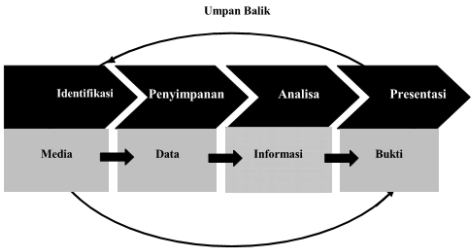
2. Akses ilegal (Pasal 30);
3. Intersepsi ilegal (Pasal 31);
4. Gangguan terhadap data (data interference, Pasal 32 UU ITE);
5. Gangguan terhadap sistem (system interference, Pasal 33 UU ITE);
6. Penyalahgunaan alat dan perangkat (misuse of device, Pasal 34 UU ITE);

3. TAHAPAN PADA DIGITAL FORENSIC

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:



Gambar 2. Tahapan Digital Forensic

4. PEMBAHASAN

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, hard disk, 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
- FTimes
- Liveview
- Netcat
- ProDiscover DFT
- Psloggedon
- TULP2G
- UnxUtils
- Webjob

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:

1. Menjamin bahwa bukti itu benar-benar masih asli *(authentic).*
2. Pada saat persidangan, bukti masih bisa dikatan 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:

1. Siapa yang mengumpulkan bukti?
2. Bagaimana dan dimana?
3. Siapa yang memiliki bukti tersebut?
4. Bagaimana penyimpanan dan pemeliharaan bukti itu?

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

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

Sedangkan *rules of evidence* artinya pengaturan barang bukti dimana barang bukti harus memiliki keterkaitan dengan kasus yang diinvestigasi dan memiliki kriteria sebagai berikut:

1. Layak dan dapat diterima *(Admissible).*
   Artinya barang bukti yang diajukan harus dapat diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai ke pengadilan.
2. Asli *(Authentic).*
   Barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan bukan rekayasa.
3. Akurat *(Accurate).*
   Barang bukti harus akurat dan dapat dipercaya.
4. 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, makapengetahuan 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 ter*overwrite*. 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:

1. Siapa yang telah melakukan
2. Apa yang telah dilakukan
3. Apa saja software yang digunakan
4. Hasil proses apa yang dihasilkan
5. Waktu melakukan.

Penelusuran bisa dilakukan pada data-data sebagai berikut: alamat URL yang 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: analisis media *(media analysis)* dan analisis aplikasi *(application analysis)* pada barang bukti yang ada. Beberapa tools analisis media yang bisa digunakan antara lain:

- TestDisk
- Explore2fs
- ProDiscover DFT

Sedangkan untuk analisis aplikasi, beberapa tools yang bisa digunakan seperti: Event Log Parser, Galleta, Libpff, Md5deep, MD5summer, Outport, Pasco, RegRipper dan Rifiuti

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 di *cross-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)

5. KESIMPULAN

Dengan adanya Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik segala aktivitas digital yang menyangkut informasi dan transaksi elektronik mempunyai payung hukum dan dapat dijadikan sebagai alat bukti yang sah di pengadilan. Berkaitan dengan hal ini perlu suatu mekanisme pembuktian yang legal dan dapat dipertanggungjawabkan secara hukum dalam penelusuran bukti-bukti kejahatan khususnya kejahatan komputer *(cybercrime)*.

Dalam menelusuri bukti digital sampai pada proses pengungkapan di pengadilan, digital forensik menerapkan empat tahapan yaitu: Pengumpulan *(Acquisition)*, Pemeliharaan *(Preservation)*, Analisa *(Analysis)* dan Presentasi *(Presentation)*. Seiring dengan menjadi lebih luas lagi, dan keahlian dalam depan objek penelitian dan cakupan digital forensik akan digital forensik tentu akan lebih dibutuhkan.perkembangan teknologi, dimasa depan objek penelitian dan cakupan digital forensik akan menjadi lebih luas lagi dan keahlian dalam digital forensik tentu akan lebih dibutuhkan.

DAFTAR PUSTAKA

Al-Azhar, Muhammad Nuh, 2012, Digital Forensik Panduan Praktis Investigasi Komputer, Salemba Infotek.

Budhisantoso, Nugroho, Personal Site, (http:// www.forensik-komputer.info, diakses 24 Desember 2010).

http://budi.insan.co.id/courses/el7010/2003/rahmadi-report.pdf, diakses pada: 12 Januari 2011.

Kemmish, R. M. ***What is Forensic Computer***. Australian institute of Criminology, Canberra. (http:// www.aic.gov.au/publications/tandi/ti118.pdf, diakses 15 Desember 2010).

Kirschenbaum, M. G, dkk. 2010. ***Digital Forensic and Born-Digital Content in Cultural Heritage Collection***. Washington: Council on Library and Information Resources.

Marcella, A. J. & Greenfiled, R. S. 2002. ***"Cyber Forensics a field manual for collecting, examining, and preserving evidence of computer crimes"***. Florida:CRC Press LLC.

Prayudi, Y & Afrianto, D. S. 2007. ***Antisipasi Cyber Crime menggunakan Teknik Komputer Forensik***. *Makalah* disajikan pada Seminar Nasional Aplikasi Teknologi Informasi 2007, diselenggarakan Universitas Islam Indonesia, Yogyakarta, 16 Juni 2007.

Simarmata, J. 2006. ***Pengamanan Sistem Komputer***. Yogyakarta : Andi Offset. Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Bab III Informasi Dokumen dan Tanda Tangan Elektronik pasal 5 ayat 1. 2009. Yogyakarta: Pustaka Yustisia.

Wahid, A. & Labib, M. 2005. ***Kejahatan Mayantara (Cyber Crime)***. Bandung: PT. Refika Aditama.

Wikipedia, Komputer Forensik. http://id.wikipedia.org/wiki/Komputer_forensik, diakses 25 Desember 2010.