Digital Forensik

Apa dan Bagaimana

Asrizal

Abstract. The increasing of information technology in fact followed by issues around cyber crime 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 apllying science methods in investigating digital evidence, made digital forensic as the answer of law standing effort in digital era.

Kata kunci: *digital forensik, kejahatan, bukti digital*

Pendahuluan

Kemajuan teknologi dan industri yang merupakan hasil dari budaya manusia disamping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan dan peradaban manusia itu sendiri. Dampak negatif yang dimaksud adalah berkaitan dengan dunia kejahatan. J.E. Saheteapy menyatakan dalam tulisannya, bahwa kejahatan erat kaitannya dengan perkembangan masyarakat. Semakin maju kehidupan masyarakat, maka kejahatan juga ikut semakin maju. Kejahatan juga menjadi sebagian dari hasil budaya itu sendiri. Hal ini berarti bahwa semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya.[1]

Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi dapat dibagi menjadi dua bagian besar. Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Dan kedua, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Namun begitu, mengingat teknologi informasi merupakan konvergensi telekomunikasi, komputer dan media, kejahatan ini berkembang menjadi lebih luas lagi.

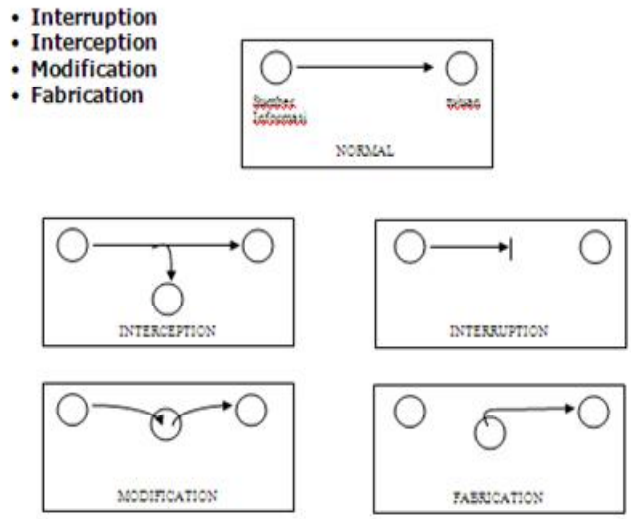
[1] Wahid, A. & Labib, M. 2005, ***Kejahatan Mayantara (Cyber Crime)***, Bandung: PT. Refika Aditama. hal 21.

Dalam catatan beberapa literatur dan situs-situs yang mengetengahkan *cybercrime,* terdapat berpuluh jenis kejahatan yang berkaitan dengan dunia *cyber.* Yang masuk dalam kategori kejahatan umum yang difasilitasi teknologi informasi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedang kejahatan yang menjadikan sistem dan fasilitas TI (teknologi informasi) sebagai sasaran diantaranya adalah *denial of service attack (DOS), defacing, cracking* ataupun *phreaking.*[2]

Berdasarkan fungsi sistem komputer sebagai penyedia informasi, ancaman terhadap sistem komputer dikategorikan menjadi empat yaitu:

1. *Interruption*, merupakan suatu ancaman terhadap *avaibility*, informasi atau data dalam komputer dirusak, dihapus, sehingga jika dibutuhkan sudah tidak ada lagi.
2. *Interception,* merupakan ancaman terhadap kerahasiaan *(secrecy),* informasi yang ada didalam sistem disadap oleh orang yang tidak berhak.
3. *Modification*, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim lalu mengubahnya sesuai keinginannya.
4. *Fabrication,* merupakan ancaman ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan suatu informasi sehingga orang yang menerima informasi menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.[3]

Keempat ancaman terhadap system komputer tersebut digambarkan sebagai berikut:



Gambar 1. **Ancaman terhadap Sistem Komputer**

[2] Ibid, hal 27.
[3] Simarmata, J. 2006, ***Pengamanan Sistem Komputer***, Yogyakarta : Andi Offset, hal 30-31

Dengan meningkatnya kejahatan berbasis teknologi dalam berbagai modus sebagaimana disebutkan diatas, maka diperlukan suatu mekanisme ilmiah untuk menganalisa dan menelusuri bukti-bukti digital yang ada baik yang disimpan maupun yang ditransmisikan melalui komputer atau perangkat digital lainnya.

Sesuai dengan Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah,[4] maka peran digital forensik sebagai metode pembuktian suatu kasus kejahatan secara digital menjadi sangat penting. Sebagaimana tertuang dalam Penjelasan atas Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik: "…… *pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit."*[5]

Lebih lanjut informasi elektronik adalah *satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.*[6]

Berbagai kasus yang mencuat akhir-akhir ini sangat bergantung penelusurannya kepada bukti-bukti digital yang ada. Maka mulailah kita melihat bukti-bukti digital ini diungkap di persidangan dan bahkan diekspose oleh berbagai media dalam pemberitaan mulai dari foto digital, rekaman pembicaraan, rekaman video, sms, email, dan lain sebagainya seperti pada kasus pembobolan ATM, kasus Bank Century, kasus Artalyta Suryani, kasus pembunuhan Nasruddin Zulkarnain yang melibatkan mantan ketua KPK, kasus Prita Mulyasari, kasus video mesra yang melibatkan artis papan atas, dan yang paling menghebohkan adalah kasus mafia pajak Gayus Tambunan.

---

[4] 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. hal 14

[5] Ibid, hal 53.

[6] Ibid, hal 51

Sejarah Komputer Forensik

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 computer *(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.[7]

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:

- Keperluan investigasi tindak kriminal dan perkara pelanggaran hukum.
- Rekonstruksi duduk perkara insiden keamanan komputer.
- Upaya-upaya pemulihan kerusakan sistem.
- *Troubleshooting* yang melibatkan hardware maupun software.

[7] 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.

- Keperluan untuk memahami sistem ataupun berbagai perangkat digital dengan lebih baik.

Definisi Digital Forensik

Ada beberapa definisi yang bisa dijadikan acuan tentang apa sebenarnya Digital Forensik. Menurut Marcella[8]: digital forensik adalah ***aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam kejahatan computer.*** 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[9], 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[10] 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 forensik *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***.

---

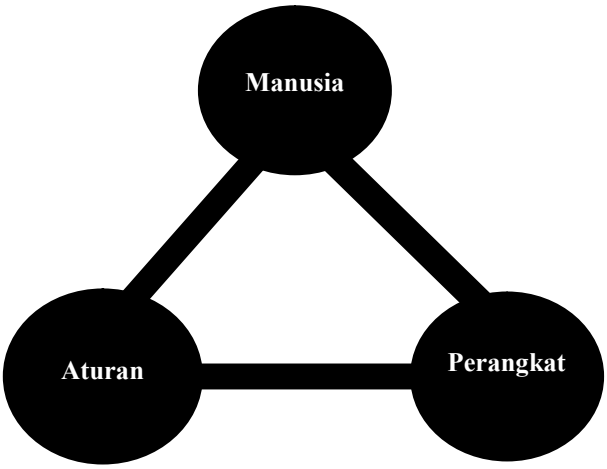
[8] Marcella, A. J. & Greenfiled, R. S. 2002. ***"Cyber Forensics a field manual for collecting, examining, and preserving evidence of computer crimes"***, Florida: CRC Press LLC.

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

[10] Wikipedia, (http://id.wikipedia.org/wiki/Komputer_forensik, diakses 25 Desember 2010)

Komponen Digital Forensik

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 2. **Komponen Digital Forensik**

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,[11] 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,[12] 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.

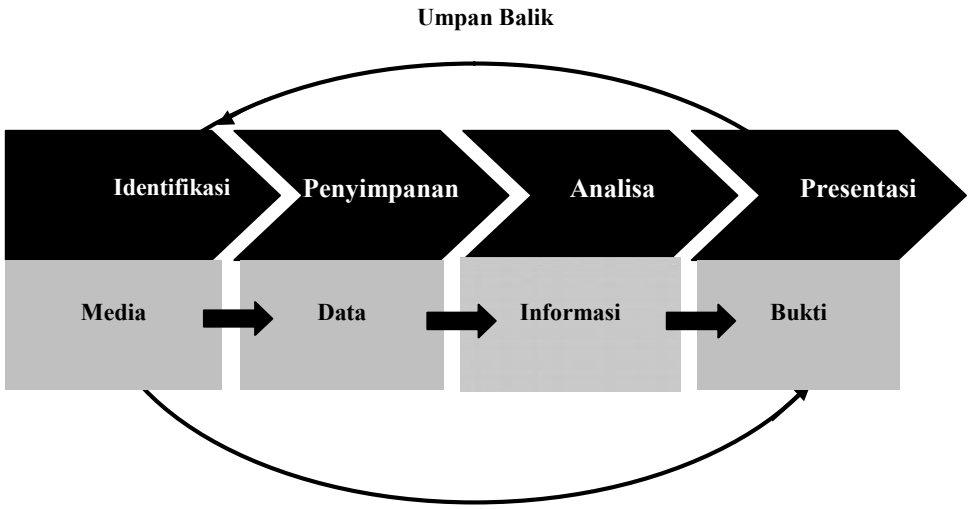
Tahapan pada Digital Forensik

Ada berbagai tahapan pada proses implementasi digital forensik. Namun menurut Kemmish,[13] 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:

[11] Budhisantoso, Nugroho, Personal Site, (http:// www.forensik-komputer.info, diakses 24 Desember 2010).
[12] Kirschenbaum, M. G, dkk. 2010. ***Digital Forensic and Born-Digital Content in Cultural Heritage Collection***. Washington: Council on Library and Information Resources.
[13] 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).



Gambar 3. **Tahapan Digital Forensik**

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 *(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.* [14]

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 dikatan seperti pada saat ditemukan karena biasanya jarak antara penyidikan dan persidangan relatif lama.

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

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:

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, 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[15]:

> *"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.

[15] Seorang pengacara pada Divisi High-Tech Crime di Kepolisian Michigan, Amerika Serikat

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

Sedangkan untuk analisis aplikasi, beberapa tools yang bisa digunakan seperti:

- Event Log Parser *(http://www.whitehats.ca/main/members/Malik/malik_eventlogs/malik_eventlogs.html)*
- Galleta *(http://www.foundstone.com/resources/proddesc/galleta.htm)*

- 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)*

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)

Training dan Sertifikasi

Untuk menjadi seorang ahli dibidang Digital Forensik, seseorang harus mempunyai pengetahuan yang mendalam tentang teknologi informasi baik hardware maupun software. Seperti: sistem operasi, bahasa pemrograman, media penyimpanan komputer, networking, routing, protokol komunikasi dan sekuriti, kriptologi, teknik

pemrograman terbalik, teknik investigasi, perangkat komputer forensik, bentuk/format file, dan segala perangkat digital forensik baik hardware maupun software.

Kemudian harus mendapatkan pelatihan atau training khusus Digital Forensik dari berbagai lembaga yang dibuktikan dengan sertifikat keahlian yang tidak sedikit, antara lain *Certified Information System Security Professional* (CISSP), lalu *Certified Forensics Analyst* (CFA), *Experienced Computer Forensic Examiner* (ECFE), *Certified Computer Examiner* (CCE), *Computer Hacking Forensic Investigator* (CHFI) dan *Advanced Information Security* (AIS).

Seorang ahli Digital Forensik juga ditentukan kapasitasnya dari sudah berapa lama dia bergerak dibidang ini, kasus-kasus apa saja yang sudah ditangani, dan pernah diminta kesaksiannya sebagai saksi ahli dalam kasus-kasus tertentu. Penting untuk diingat bahwa seorang ahli Digital Forensik juga terikat dengan aturan atau kode etik seperti mengutamakan kejujuran, kebenaran, ketelitian, ketepatan tindakan, tidak merusak barang bukti dan independen.

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 perkembangan teknologi, dimasa depan objek penelitian dan cakupan digital forensik akan menjadi lebih luas lagi, dan keahlian dalam digital forensik tentu akan lebih dibutuhkan.

Penulis adalah staf Subbag Akademik dan Kemahasiswaan Fakultas Tarbiyah dan mahasiswa Program Studi Magister Teknik Informatika Universitas Sumatera Utara.

DAFTAR PUSTAKA

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, (http://id.wikipedia.org/wiki/Komputer_forensik, diakses 25 Desember 2010.)