DIGITAL FORENSIK INVESTIGASI

I. PENDAHULUAN

Pemeriksaan suatu perkara pidana di dalam suatu proses peradilan pada hakekatnya adalah bertujuan untuk mencari kebenaran materiil (materiile waarheid) terhadap perkara tersebut. Hal ini dapat dilihat dari adanya berbagai usaha yang dilakukan oleh aparat penegak hukum dalam memperoleh bukti-bukti yang dibutuhkan untuk mengungkap suatu perkara baik pada tahap pemeriksaan pendahuluan seperti penyidikan dan penuntutan maupun pada tahap persidangan perkara tersebut. Sejalan dengan perkembangan yang pesat dunia teknologi telekomunikasi dan teknologi komputer menghasilkan internet yang multiguna. Perkembangan ini membawa kita ke revolusi dalam sejarah pemikiran manusia bila ditinjau dari konstruksi pengetahuam umat manusia yang dicirikan dengan cara berfikir yang tanpa batas dengan Percepatan teknologi semakin lama semakin canggih yang menjadi sebab perubahan yang terus menerus dalam semua interaksi dan aktivitas masyarakat informasi. Internet merupakan bukti masyarakat global. Era informasi ditandai dengan aksesibilitas informasi yang amat tinggi. Dalam era ini, informasi merupakan komoditi utama yang diperjualbelikan sehingga akan muncul berbagai network & information company yang akan memperjualbelikan berbagai fasilitas bermacam jaringan dan berbagai basis data informasi tentang berbagai hal yang dapat diakses olehuser dan pelanggan. Perkembangan Internet dan umumnya dunia cyber tidak selamanya menghasilkan hal-hal yang postif. Salah satu hal negatif yang merupakan efek sampingannya antara lain adalah kejahatan di dunia maya.

Kini, sudah dikenal forensik asuransi, forensik akuntansi, forensik computer, toksikologi forensik dalam kasus kejahatan lingkungan, dan forensik balistik. Meski berbeda sebutan, tujuannya tetap sama. Forensik itu mengungkap kejahatan Saat ini.

Teknologi komputer dapat digunakan sebagai alat bagi para pelaku kejahatan komputer seperti dengan berbagai istilah sehingga munculah istilah carding,hacking, cracking.Barang bukti yang berasal dari komputer telah muncul dalam persidangan30 tahun. awal nya hakim menerima bukti tersebut tanpa membedakan dengan bentuk bukti lainnya namun seiring dengan kemajuan teknologi komputer, perlakuan tersebut menjadi membingungkan karena bukti elektronik sangat sulit dibedakannya antara yang asli dan yang palsu berdasarkan sifat alaminya,data yang ada dalam komputer sangat mudah dimodifikasi.

Oleh karena itu, penulis ingin memberikan pandangan terhadap aksi-aksi cyber crime khususnya yang ada di Indonesia karena selama ini, pemberitaan tentang aksi- aksi kejahatan di internet sangat banyak dan pembuktiannya pun sulit. Dalam

melihat kasus ini adalah mencari akar masalah bukti elektronik atau di kaji dalam computer forensic merupakan alat bukti hukum yang sah.

II. ISI

Menurut Ruby Alamsyah, 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. Jumlah kejahatan komputer (computer crime),terutama yang berhubungan dengan sistem informasi, akan terus meningkat karena kejahatan di internet terbagi dalam berbagai versi. Salah satu versi menyebutkan bahwa kejahatan ini terbagi dalam dua jenis, yaitu kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasan pribadi. Jenis kedua adalah kejahatan dengan motif politik, ekonomi, atau kriminal yang potensial yang dapat menimbulkan kerugian bahkan perang informasi. komputer forensik dapat diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan. Komputer forensik banyak ditempatkan dalam berbagai keperluan, bukan hanya untuk menangani beberapa kasus kriminal yang melibatkan hukum, seperti rekonstruksi perkara insiden keamanan komputer, upaya pemulihan kerusakan sistem, pemecahan masalah yang melibatkan hardware ataupun software, dan dalam memahami sistem atau pun berbagai perangkat digital agar mudah dimengerti. Komputer forensik merupakan ilmu baru yang akan terus berkembang. Ilmu ini didasari oleh beberapa bidang keilmuan lainnya yang sudah ada. Bahkan, komputer forensik pun dapat dispesifikasi lagi menjadi beberapa bagian, seperti Disk Forensik, System Forensik, Network Forensik, dan Internet Forensik. Pengetahuan Disk Forensik sudah terdokumentasi dengan baik dibandingkan dengan bidang forensik lainnya. Beberapa kasus yang dapat dilakukan dengan bantuan ilmu Disk Forensik antara lain mengembalikan file yang terhapus, mendapatkan password, menganalisis File Akses dan System atau Aplikasi Logs, dan sebagainya.

Permodelan Forensik

Model forensik melibatkan tiga komponen terangkai yang dikelola sedemikian rupa sehingga menjadi sebuah tujuan akhir dengan segala kelayakan serta hasil yang berkualitas. Ketiga komponen tersebut adalah:

• Manusia (People), diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.

• Peralatan (Equipment), diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti (evidence) yang dapat dipercaya dan bukan sekadar bukti palsu.

• Aturan (Protocol), diperlukan dalam menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan akan teknologi informasi dan ilmu hukum tentunya.

Ilmu forensik telah didefinisikan sebagai ilmu apapun yang digunakan untuk tujuan hukum (menyediakan) tidak memihak bukti ilmiah untuk digunakan dalam kepentingan peradilan, dan dalam penyelidikan. Menurut Marcus Ranum Jaringan forensik adalah menangkap, merekam, dan analisis peristiwa jaringan untuk menemukan sumber serangan keamanan atau lainnya masalah insiden.

Sedangkan menurut Joel Weise and Brad Powell Komputer forensik adalah Penerapan, pengolahan, pemeliharaan, dan analisis informasi yang diperoleh dari sistem, jaringan, aplikasi, atau sumber daya komputasi lain, untuk menentukan sumber serangan terhadap sumber-sumber itu. Kegiatan-kegiatan ini dilakukan dalam perjalanan sebuah investigasi forensik komputer sebenarnya yang dirasakan atau serangan terhadap sumber daya komputer.

Kecanggihan TIK

Dampak positifnya adalah aktivitas manusia jadi lebih mudah , cepat , murah. Dan dampak negatifnya seperti adanya kejahatan baru di dunia maya (cyber crime), pencurian data pada sebuah site, pencurian informasi, penipuan keuangan dengan internet, carding, hacking, cracking, phising, viruses, cybersquating. Dsb.

Kategori Tindak Pidana Cyber Crime

Kejahatan yang menggunakan TIK untuk melakukan perbuatan tindak pidana seperti:

cyber gambling (perjudian)

cyber terrorism (terorisme)

cyber fraud (penipuan kartu kredit)

cyber sex (pornografi)

cyber smuggling (penyelundupan)

cyber narcotism (narkotika)

cyber attack on critical infrastructure (penyerangan terhadap infrastruktur penting)

cyber blackmail (pemerasan)

cyber threathening (pengancaman)

cyber aspersion (pencemaran nama baik melalui internet)

phising dll

Kejahatan yang dilakukan dengan tujuan dan sasaran TIK seperti :

hacking

cracking

phreaking

DoS attack

Penyebaran kode jahat (malicious code, virus, spyware, Trojan horse, adware. dll)

Botnet (robot internet) dsb.

Menurut sumber yang dikutip dari Internet Crime Complain Center (IC3) yang merupakan lembaga yang berdiri dibawah naungan FBI (Federal Bureau of Investigation) dan National White Collar Crime Center, setiap tahun terjadi peningkatan kasus cyber crime yang mengakibatkan jumlah kerugian yang besar seperti dinyatakan dalam tabel dibawah ini.

Kategori kasus	Tahun 2007	Tahun 2008	Tahun 2009
Jumlah komplain yang diterima IC3 via website	206.884	275.264	334.655
Jumlah kerugian (dalam juta U$ dollar)	239.1	264.6	559.7
Jumlah kasus yang ditangani	90.008	72.940	146.663

Jumlah kasus computer crime dan computer related crime ditangani pusat laboratorium forensik mabes POLRI mencapai sekitar 50 kasus, dengan total jumlah barang bukti elektronik sekitar 150 unit.

Tahun	Jumlah
2006	3 Kasus
2007	3 kasus
2008	7 Kasus
2009	15 Kasus
Mei 2010	27 Kasus

Guna menangani cyber crime dan kejahatan konvensional yang didukung TIK, peran forensic digital sangat penting.

Mengapa forensic digital diperlukan dalam penyelidikan berbagai kasus? Menurut Brian carrier :

1. Teknik forensic computer digunakan untuk menganalisis system digital milik terdakwa terkait kasus pidana dan perdata.

2. Memulihkan data apabila terjadi kegagalan pembacaan atau penyimpanan data pada perangkat keras atau pada perangkat lunak.

3. Menganalisis system computer apabila telah terjadi penyerangan kedalam system computer.

4. Mendapatkan informasi tentang bagaimana system computer bekerja untuk tujuan debugging, kinerja optimasi atau reverse engineering. (Brian carrier, 2005).

Sejarah Forensik

· Francis Galton (1822-1911) : sidik jari;

· Leone Lattes (1887-1954) : Golongan darah (A,B,AB & O)

· Calvin Goddard (1891-1955) : senjata dan peluru (Balistik)

· Albert Osborn (1858-1946) : Document examination

· Hans Gross (1847-1915) : menerapkan ilmiah dalam investigasi criminal

· FBI (1932) : Lab.forensik.

Definisi forensic

Jika dilihat dari kata berarti membawa ke pengadilan. Forensic adalah proses mengumpulkan, menganalisis, dan mempresentasikan secara ilmiah barang bukti di pengadilan (US computer emergency response team, US-CERT, 2008).

Sejarah perkembangan, forensik mengalami pergeseran menyangkut subyek forensic, proses, metodologi, hingga meluas kebidang lain. Salah satunya, muncul istilah forensic computer/forensic digital seiring makin beragamnya perangkat teknologi.

Forensik computer bisa dikatakan metodologi ilmiah dan system untuk mengidentifikasi, mencari, mendapatkan kembali, dan menganalisis barang bukti dari computer, media penyimpanan computer dan perangkat elektronik lainnya serta mempresentasikan hasil penemuan tersebut sesuai dengan standar yang telah ditetapkan oleh pengadilan (chan, Hilton, 2003). Jika menurut FBI ini berarti ilmu mengenalisis dan mempresentasikan data yang sudah diproses secara elektronik dan disimpa dalam media computer. Penggunaan metode ilmiah terhadap penjagaan, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital guna memfasilitasi atau melanjutkan rekontruksi terhadap kejadian tindak pidana (scientific working group on digital evidence, 2007).

Tujuan Digital Forensik

Tujuaan dari digital forensik adalah untuk menjelaskan seputar digital artefak yakni sistem komputer, media penyimpanan (harddisk atau CD-ROM), dokumen elektronik (E-mail atau gambar JPEG) atau paket – paket data yang bergerak melalui jaringan komputer.

Barang Bukti Digital Sebagai Alat Bukti Sah

Menurut Pasal 5 UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyebutkan bahwa “informasi elektronik dan atau dokumen elektronik dan atau hasil cetaknya merupakan alat bukti hukum yang sah”

Bukti Digital / Elektronik

Menurut Eoghan Casey :

“Semua barang bukti informasi atau data baik yang tersimpan maupun yang melintas pada sistem jaringan digital, yang dapat dipertanggungjawabkan di depan pengadilan”

Menurut Scientific Working Group on Digital Evidence :

“Informasi yang disimpan atau dikirimkan dalam bentuk digital”

Contoh barang bukti digital : alamat E-Mail, wordprocessor/spreadsheet files, source code dari perangkat lunak, files bentuk images (JPEG, PNG, dll), web browser bookmarks, cookies serta kalender dan to do list

Penanganan Barang Bukti Digital

Penanganan barang bukti digital perlu dilakukan secara khusus mengingat barang bukti digital tergolong rapuh sehingga sangat besat kemungkinan terjadinya pencemaran barang bukti digital baik disengaja maupun tidak disengaja. Kesalahan kecil pada penanganan barang bukti dapat membuat barang bukti digital tidak dapat diajukan dipengadilan sebagai alat bukti yang sah dan akurat.

Prinsip Kerja Forensik Digital

Menurut Pavel Gladyshev prinsip kerja dari forensik digital adalah :

Pemeliharaan (“Freezing the Crime Scene”) Mengamankan lokasi dengan cara menghentikan atau mencegah setiap aktivitas yang dapat merusak atau menghilangkan barang bukti.

Pengumpulan. Menemukan dan mengumpulkan semua barang bukti digital atau hal – hal yang dapat menjadi barang bukti atau informasi apa saja yang masih bersangkutan dengan kasus yang sedang diselidiki.

Pemeriksaan. Menganilisis barang bukti yang ada dan mencari data sebanyak – banyaknya yang berhubungan dengan kasus. Tahap ini adalah penentuan apakah pelaku kejahatan bisa tertangkap atau lolos dari jeratan hukum

Analisis. Menyimpulkan bukti – bukti yang dikumpulkan selama proses penyelidikan.

Perangkat Forensik Digital

Perangkat yang biasa digunakan oleh para penyidik untuk mengumpulkan bukti – bukti tindak pidana kejahatan adalah :

· Encase Forensic

· Encase Pro Suite

· Encase Deluxe Version

· FTK (Forensic Tool Kit)

· Pro Discover

· SleuthKit-Autopsy

· Helix/Helix Pro

· Paraben Device Seizure

· Forensic Duplicator

· Mobile Forensic

· Write Blocker

Investigasi dan penuntutan kejahatan komputer memiliki beberapa isu unik, seperti:

1. Penyelidik dan pelaku memiliki kerangka waktu padat untuk investigasi.

2. Informasinya tidak dapat diukur.

3. Investigasi harus turut mencampuri tingkah laku normal bisnis organisasi.

4. Pasti ada kesulitan dalam memperoleh bukti.

5. Data yang berkaitan dengan investigasi kriminal harus berlokasi di komputer yang sama sebagaimana kebutuhan data bagi kelakuan normal bisnis (percampuran data).

6. Dalam banyak hal, seorang ahli atau spesialis dibutuhkan.

7. Lokasi yang melibatkan kriminal pasti terpisah secara geografis dari jarak yang cukup jauh dalam yurisdiksi yang berbeda.

8. Banyak yurisdiksi telah memperluas definisi properti untuk memasukkan informasi elektronik.

Aturan Bagi Investigator

pemeriksaan yang dilakukan oleh petudas yang tidak berpengalaman dan tidak mengerti forensic digital (rosedur forensic digital), hampir dapat dipastikan akan menghasilkan bukti yang tidak hampir pasti menghasilkan bukti yang tidak dapat diterima di pengadilan hukum.

Tantangan Forensik Digital

Dalam mengumpulkan bukti forensik digital, banyak tantangan – tantangan yang harus dihadapi oleh para penyidik seperti :

- Bagaimana menangani kasus yang melibatkan media perangkat digital

- Bagaimana menemukan bukti dari web browser secara forensik suara
- Bagaimana menganalisis bukti dalam segala kondisi berbeda baik secara perangkat maupun sistem
- Bagaimana melacak dan mendapatkan pelaku (tak menutup kemungkinan si pelaku adalah orang dalam)
- Bagaimana mengidentifikasi dan menyelidiki kasus – kasus seperti spionase korporasi
- Bagaimana melakukan investigasi network logs guna melacak dan mengadili penjahat cyber

III. PENUTUP

Dalam UU ITE diatur bahwa informasi elektronik/dokumen elektronik dan/atau hasil cetaknya(buktidigital)merupakan alat bukti hukum yang sah, dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Tapi, tidak sembarang informasi elektronik/dokumen elektronik dapat dijadikan alat bukti yang sah. Menurut UU ITE, suatu informasi elektronik/ dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalam UU ITE, yaitu sistem elektronik yang andal dan aman, serta memenuhi persyaratan minimum sebagai berikut: dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang- undangan, dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut; dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan systemelektronik, dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraansistemelektronik. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

KESIMPULAN

Dalam menganalisa barang bukti digital harus dilakukan melalui proses forensik digital sehingga barang bukti dapat diterima sebagai alat bukti yang sah

Perlu dukungan SDM yang memiliki pengetahuan dan skill terkait proses forensik digital (bisa melalui pelatihan (training) dan proses sertifikasi)

Forensik digital tak hanya dibutuhkan untuk tindakan kejahatan cyber, tetapi juga kejahatan konvensional yang didukung perangkat digital

Perlunya panduan proses forensik digital dan aturan hukum / regulasi secara detail.

DAFTAR PUSTAKA

http://www.wahyudi.or.id/2010/01/19/seminar-mencari-bukti-valid-melalui-forensik-digital/

http://www.scribd.com/doc/27116840/Pengantar-Menuju-Ilmu-Forensik

http://www.kusandriadi.com/sertifikat-digital-forensik-di-indonesia/

http://yanto-ssi.blogspot.com/2010/05/komputer-forensik.html

http://id.wikipedia.org/wiki/Komputer_forensik

digial forensic, second kaskuser IT lounge & information technology seminar. By Ruby Z. Alamsyah