Forensik Komputer

Prof. Richardus Eko Indrajit

Email: indrajit@post.harvard.edu Website: http://www.EkoIndrajit.com

Latar Belakang

Bayangkanlah sejumlah contoh kasus yang dapat saja terjadi seperti dipaparkan berikut ini:

- Seorang Direktur perusahaan multi-nasional dituduh melakukan pelecehan seksual terhadap sekretarisnya melalui kata-kata yang disampaikannya melalui e-mail. Jika memang terbukti demikian, maka terdapat ancaman pidana dan perdata yang membayanginya.
- Sebuah kementrian di pemerintahan menuntut satu Lembaga Swadaya Masyarakat yang ditengarai melakukan penetrasi ke dalam sistem komputernya tanpa ijin. Berdasarkan undang-undang yang berlaku, terhadap LSM yang bersangkutan dapat dikenakan sanksi hukum yang sangat berat jika terbukti melakukan aktivits yang dituduhkan.
- Sekelompok artis pemain band terkemuka merasa berang karena pada suatu masa situsnya diporakporandakan oleh perentas (baca: hacker) sehingga terganggu citranya. Disinyalir pihak yang melakukan kegiatan negatif tersebut adalah pesaing atau kompetitornya.
- Sejumlah situs e-commerce mendadak tidak dapat melakukan transaksi pembayaran karena adanya pihak yang melakukan gangguan dengan cara mengirimkan virus tertentu sehingga pemilik perdagangan di internet tersebut rugi milyaran rupiah karena tidak terjadinya transaksi selama kurang lebih seminggu. Yang bersangkutan siap untuk menyelidiki dan menuntut mereka yang sengaja melakukan kegiatan ini.

Mereka yang merasa dirugikan seperti yang dicontohkan pada keempat kasus di atas, paling tidak harus melakukan 3 (tiga) hal utama:

1. Mencari bukti-bukti yang cukup agar dapat ditangani oleh pihak berwenang untuk memulai proses penyelidikan dan penyidikan, misalnya polisi di unit cyber crime;
2. Memastikan bahwa bukti-bukti tersebut benar-benar berkualitas untuk dapat dijadikan alat bukti di pengadilan yang sah sesuai dengan hukum dan perundang-undangan yang berlaku; dan
3. Mempresentasikan dan/atau memperlihatkan keabsahan alat bukti terkait dengan terjadinya kasus di atas di muka hakim, pengacara, dan tim pembela tersangka.

Oleh karena itulah maka dalam ilmu kriminal dikenal istilah forensik, untuk membantu pengungkapan suatu kejahatan melalui pengungkapan bukti-bukti yang sah menurut undang-undang dan peraturan yang berlaku. Sesuai dengan kemajuan jaman, berbagai tindakan kejahatan dan kriminal moderen dewasa ini melibatkan secara langsung maupun

tidak langsung teknologi informasi dan komunikasi. Pemanfaatan komputer, telepon genggam, email, internet, website, dan lain-lain secara luas dan masif telah mengundang berbagai pihak jahat untuk melakukan kejahatan berbasis teknologi elektronik dan digital. Oleh karena itulah maka belakangan ini dikenal adanya ilmu "computer forensics" atau forensik komputer, yang kerap dibutuhkan dan digunakan para penegak hukum dalam usahanya untuk mengungkapkan peristiwa kejahatan melalui pengungkapan bukti-bukti berbasis entitas atau piranti digital dan elektronik.

Definisi Forensik Komputer

Menurut Dr. HB Wolfre, definisi dari forensik komputer adalah sebagai berikut:

"A methodological series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format."

Sementara senada dengannya, beberapa definisi dikembangkan pula oleh berbagai lembaga dunia seperti:

- The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found; atau
- The science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law.

Dimana pada intinya forensik komputer adalah "suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun piranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan."

Tujuan dan Fokus Forensik Komputer

Selaras dengan definisinya, secara prinsip ada tujuan utama dari aktivitas forensik komputer, yaitu:

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat buti yang sah di pengadilan; dan
2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi.

Sementara itu fokus data yang dikumpulkan dapat dikategorikan menjadi 3 (tiga) domain utama, yaitu: (i) Active Data – yaitu informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi; (ii) Archival Data – yaitu informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpan seperti hardisk eksternal, CD ROM, backup tape, DVD, dan lain-lain; dan (iii) Latent Data – yaitu informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya.

Manfaat dan Tantangan Forensik Komputer

Memiliki kemampuan dalam melakukan forensik komputer akan mendatangkan sejumlah manfaat, antara lain:

- Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan;
- Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir;

- Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer; dan
- Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Terlepas dari manfaat tersebut, teramat banyak tantangan dalam dunia forensik komputer, terutama terkait dengan sejumlah aspek sebagai berikut:

- Forensik komputer merupakan ilmu yang relatif baru, sehingga "Body of Knowledge"-nya masih sedemikian terbatas (dalam proses pencarian dengan metode "learning by doing");
- Walaupun berada dalam rumpun ilmu forensik, namun secara prinsip memiliki sejumlah karakteristik yang sangat berbeda dengan bidang ilmu forensik lainnya – sehingga sumber ilmu dari individu maupun pusat studi sangatlah sedikit;
- Perkembangan teknologi yang sedemikian cepat, yang ditandai dengan diperkenalkannya produk-produk baru dimana secara langsung berdampak pada berkembangnya ilmu forensik komputer tesebut secara pesat, yang membutuhkan kompetensi pengetahuan dan keterampilan sejalan dengannya;
- Semakin pintar dan trampilnya para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang;
- Cukup mahalnya harga peralatan canggih dan termutakhir untuk membantu proses forensik komputer beserta laboratorium dan SDM pendukungnya;
- Secara empiris, masih banyak bersifat studi kasus (happening arts) dibandingkan dengan metodologi pengetahuan yang telah dibakukan dimana masih sedikit pelatihan dan sertifikasi yang tersedia dan ditawarkan di masyarakat;
- Sangat terbatasnya SDM pendukung yang memiliki kompetensi dan keahlian khusus di bidang forensik komputer; dan
- Pada kenyataannya, pekerjaan forensik komputer masih lebih banyak unsur seninya dibandingkan pengetahuannya (more "Art" than "Science").

Kejahatan Komputer

Berbeda dengan di dunia nyata, kejahatan di dunia komputer dan internet variasinya begitu banyak, dan cenderung dipandang dari segi jenis dan kompleksitasnya,

meningkat secara eksponensial. Secara prinsip, kejahatan di dunia komputer dibagi menjadi tiga, yaitu: (i) aktivitas dimana komputer atau piranti digital dipergunakan sebagai alat bantu untuk melakukan tindakan kriminal; (ii) aktivitas dimana komputer atau piranti digital dijadikan target dari kejahatan itu sendiri; dan (iii) aktivitas dimana pada saat yang bersamaan komputer atau piranti digital dijadikan alat untuk melakukan kejahatan terhadap target yang merupakan komputer atau piranti digital juga.

Agar tidak salah pengertian, perlu diperhatikan bahwa istilah "komputer" yang dipergunakan dalam konteks forensik komputer mengandung makna yang luas, yaitu piranti digital yang dapat dipergunakan untuk mengolah data dan melakukan perhitungan secara elektronik, yang merupakan suatu sistem yang terdiri dari piranti keras (hardware), piranti lunak (software), piranti data/informasi (infoware), dan piranti sumber daya manusia (brainware).

Contoh kejahatan yang dimaksud dan erat kaitannya dengan kegiatan forensi komputer misalnya:

- Pencurian kata kunci atau "password" untuk mendapatkan hak akses;
- Pengambilan data elektronik secara diam-diam tanpa sepengetahuan sang empunya;
- Pemblokiran hak akses ke sumber daya teknologi tertentu sehingga yang berhak tidak dapat menggunakannya;
- Pengubahan data atau informasi penting sehingga menimbulkan dampak terjadinya mis-komunikasi dan/atau dis-komunikasi;
- Penyadapan jalur komunikasi digital yang berisi percakapan antara dua atau beberapa pihak terkait;
- Penipuan dengan berbagai motivasi dan modus agar si korban memberikan aset berharganya ke pihak tertentu;
- Peredaran foto-foto atau konten multimedia berbau pornografi dan pornoaksi ke target individu di bawah umur;
- Penyelenggaraan transaksi pornografi anak maupun hal-hal terlarang lainnya seperti perjudian, pemerasan, penyalahgunaan wewenang, pengancaman, dan lain sebagainya;
- Penyelundupan file-file berisi virus ke dalam sistem korban dengan beraneka macam tujuan;
- Penyebaran fitnah atau berita bohong yang merugikan seseorang, sekelompok individu, atau entitas organisasi; dan lain sebagainya.

Obyek Forensik

Apa saja yang bisa dipergunakan sebgai obyek forensik, terutama dalam kaitannya dengan jenis kejahatan yang telah dikemukakan tersebut? Dalam dunia kriminal dikenal istilah "tidak ada kejahatan yang tidak meninggalkan jejak". Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Contohnya adalah sebagai berikut:

- Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem;
- File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu;
- Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System);
- Hard disk yang berisi data/informasi backup dari sistem utama;
- Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya;
- Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain);
- Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya);
- Absensi akses server atau komputer yang dikelola oleh sistem untuk merekam setiap adanya pengguna yang login ke piranti terkait; dan lain sebagainya.

Beraneka ragam jenis obyek ini selain dapat memberikan petunjuk atau jejak, dapat pula dipergunakan sebagai alat bukti awal atau informasi awal yang dapat dipergunakan oleh penyelidik maupun penyidik dalam melakukan kegiatan penelusuran terjadinya suatu peristiwa kriminal, karena hasil forensik dapat berupa petunjuk semacam:

- Lokasi fisik seorang individu ketika kejahatan sedang berlangsung (alibi);
- Alat atau piranti kejahatan yang dipergunakan;
- Sasaran atau target perilaku jahat yang direncanakan;
- Pihak mana saja yang secara langsung maupun tidak langsung terlibat dalam tindakan kriminal;
- Waktu dan durasi aktivitas kejahatan terjadi;
- Motivasi maupun perkiraan kerugian yang ditimbulkan;
- Hal-hal apa saja yang dilanggar dalam tindakan kejahatan tersebut;
- Modus operandi pelaksanaan aktivitas kejahatan; dan lain sebagainya.

Tahapan Aktivitas Forensik

Secara metodologis, terdapat paling tidak 14 (empat belas) tahapan yang perlu dilakukan dalam aktivitas forensik, sebagai berikut:

1. Pernyataan Terjadinya Kejahatan Komputer – merupakan tahap dimana secara formal pihak yang berkepentingan melaporkan telah terjadinya suatu aktivitas kejahatan berbasis komputer;

2. Pengumpulan Petunjuk atau Bukti Awal – merupakan tahap dimana ahli forensik mengumpulkan semua petunjuk atau bukti awal yang dapat dipergunakan sebagai bahan kajian forensik, baik yang bersifat tangible maupun intangible;

3. Penerbitan Surat Pengadilan – merupakan tahap dimana sesuai dengan peraturan dan perundang-undangan yang berlaku, pihak pengadilan memberikan ijin resmi kepada penyelidik maupun penyidik untuk melakukan aktiivitas terkait dengan pengolahan tempat kejadian perkara, baik yang bersifat fisik maupun maya;

4. Pelaksanaan Prosedur Tanggapan Dini – merupakan tahap dimana ahli forensik melakukan serangkaian prosedur pengamanan tempat kejadian perkara, baik fisik maupun maya, agar steril dan tidak tercemar/terkontaminasi, sehingga dapat dianggap sah dalam pencarian barang-barang bukti;

5. Pembekuan Barang Bukti pada Lokasi Kejahatan – merupakan tahap dimana seluruh barang bukti yang ada diambil, disita, dan/atau dibekukan melalui teknik formal tertentu;

6. Pemindahan Bukti ke Laboratorium Forensik – merupakan tahap dimana dilakukan transfer barang bukti dari tempat kejadian perkara ke laboratorium tempat dilakukannya analisa forensik;

7. Pembuatan Salinan "2 Bit Stream" terhadap Barang Bukti – merupakan tahap dimana dilakukan proses duplikasi barang bukti ke dalam bentuk salinan yang identik;

8. Pengembangan "MD5 Checksum" Barang Bukti – merupakan tahap untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada;

9. Penyiapan Rantai Posesi Barang Bukti – merupakan tahap menentukan pengalihan tanggung jawab dan kepemilikan barang bukti asli maupun duplikasi dari satu wilayah otoritas ke yang lainnya;

10. Penyimpanan Barang Bukti Asli di Tempat Aman – merupakan tahap penyimpanan barang bukti asli (original) di tempat yang aman dan sesuai dengan persyratan teknis tertentu untuk menjaga keasliannya;

11. Analisa Barang Bukti Salinan – merupakan tahap dimana ahli forensik melakuka analisa secara detail terhadap salinan barang-brang bukti yang dikumpulkan untuk mendapatkan kesimpulan terkait dengan seluk beluk terjadinya kejahatan;

12. Pembuatan Laporan Forensik – merupakan tahap dimana ahli forensik menyimpulkan secara detail hal-hal yang terjadi seputar aktivititas kejahatan yang dianalisa berdasarkan fakta forensik yang ada;

13. Penyerahan Hasil Laporan Analisa – merupakan tahap dimana secara resmi dokumen rahasia hasil forensik komputer diserahkan kepada pihak yang berwajib; dan

14. Penyertaan dalam Proses Pengadilan – merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi.

Kebutuhan Sumber Daya

Untuk melakukan aktivitas forensik, dibutuhkan sejumlah piranti bantu, baik yang berbentuk software maupun hardware. Piranti lunak atau software biasanya dipergunakan oleh praktisi untuk membantu mereka dalam melakukan hal-hal sebagai berikut:

- Mencari dan mengembalikan file yang telah terhapus sebelumnya;
- Membantu merekonstruksi pecahan-pecahan file yang ada (corrupted file);
- Mengidentifikasi anomali program melalui analisa serangkaian data beserta struktur algoritma yang terdapat pada sebuah file atau sistem basis data;
- Menemukan jejak-jejak yang tertinggal dalam sebuah peristiwa kriminal tertentu yang telah dilakukan sebelumnya;
- Mendapatkan data berbasis pola-pola tertentu sesuai dengan permintaan penegak hukum dalam proses penyelidikan maupun penyidikan peristiwa kejahatan internet;
- Memfilter dan memilah-milah antara data yang berguna/relevan untuk kebutuhan forensik dengan yang tidak, agar mekanisme analisa dapat dilakukan secara fokus dan detail;
- Menganalisa kejanggalan-kejanggalan yang terdapat pada suatu program atau sub-program tertentu;
- Mempercepat proses pencarian penggalan instruksi atau data tertentu yang dibutuhkan oleh seorang ahli forensik terhadap sebuah media repositori bermemori besar;
- Menguji dan mengambil kesimpulan terhadap sejumlah kondisi tertentu terkait dengan aktivias dan konsep forensik; dan lain sebagainya.

Dewasa ini piranti lunak tersebut cukup banyak tersedia di pasar, mulai dari yang bersifat gratis (open source) hingga yang komersial (berharga milyaran rupiah).

Disamping aplikasi pendukung aktivitas forensik, diperlukan pula seperangkat piranti keras atau peralatan elektronik/digital agar proses forensik dapat dilakukan secara efektif dan sesuai dengan prosedur baku standar yang berlaku. Piranti keras ini biasanya dibutuhkan untuk melakukan hal-hal sebagai berikut”

- Membuat replikasi atau copy atau cloning dari sistem basis data (atau media basis data) yang akan diteliti dengan cara yang sangat cepat dan menghasilkan kualitas yang identik dengan aslinya;
- Mengambil atau memindahkan atau mengekstrak data dari tempat-tempat atau media penyimpan yang khusus seperti: telepon genggam, server besar (superkomputer), PDA (Personal Digital Assistance), komputer tablet, dan lain-lain;
- Menggenerasi nilai numerik secara urut maupun random secara ultra cepat untuk membongkar kata kunci (password) atau hal sejenis lainnya, sebagai bagian dari proses deskripsi (tilik sandi);
- Membongkar berbagai proteksi secara piranti keras atau lunak yang menjadi proteksi dari sebagian besar perangkat teknologi informasi dan komunikasi;
- Menghapus dan memformat hard disk secara cepat dan efektif dengan melakukan demagnetisasi agar data benar-benar terhapus sebagai bagian dari penyiapan media replikasi; dan lain sebagainya.

Seperti halnya dalam dunia nyata, diperlukan pula ahli Forensik Komputer dalam melaksanakan pekerjaan terkait. Jika dilihat dari kompetensi dan keahliannya, seorang ahli forensik komputer yang baik dan lengkap harus memiliki tiga domain atau basis pengetahuan maupun keterampilannya, yaitu dari segi akademis, vokasi, dan profesi. Dari sisi akademis, paling tidak yang bersangkutan memiliki latar belakang pengetahuan kognitif mengenai cara kerja komputer dalam lingkungan jejaring teknologi informasi dan komputasi, terutama berkaitan dengan hal-hal yang bersifat fundamental dalam pengembangan sistem berbasis digital. Sementara dari sisi vokasi, dibutuhkan kemampuan "untuk melakukan" atau kerap disebut sebagai psiko-motorik, karena dalam prakteknya seorang ahli forensik akan melakukan kajian, analisa, dan penelitian secara mandiri dengan menggunakan seperangkat peralatan teknis yang spesifik. Dan yang terakhir dari perspektif profesi, seorang ahli yang baik akan berpegang pada kode etik (afektif) seorang ahli forensik. Disamping itu dibutuhkan pula pengalaman yang cukup untuk dapat berkreasi dan berinovasi dalam setiap tantangan kasus forensik. Berdasarkan pengalaman, memang yang paling sulit adalah menyiapkan SDM yang handal di bidang forensik komputer, karena hingga sekarang jumlahnya sangatlah sedikit – tidak sepadan dengan besarnya kebutuhan di masyarakat.