SEKILAS MENGENAI FORENSIK DIGITAL

Budi Raharjo
Email: br@paume.itb.ac.id

ABSTRAK

Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital. Sebagai ilmu yang masih baru, masih dibutuhkan pemahaman dan kemampuan untuk menguasai ilmu ini. Penguasaan ilmu ini tidak hanya ditujukan pada kemampuan teknis semata tetapi juga terkait dengan bidang lain, seperti bidang hukum. Makalah ini menguraikan secara singkat mengenai forensik digital.

Kata kunci: forensik, keamanan, teknologi informasi

ABSTRACT

Digital forensic is considered a new field of study. It is a branch of forensic science encompassing the recovery and investigation of data found in digital devices. Digital forensic is needed to solve cyber crimes and related security problems. As a new field, awareness and skills are needed to master this field. Digital forensic is not only related to technical but also legal aspects. This paper describes digital forensic in a nut shell.

***Keywords**: forensic, information technology, security*

* Dosen Sekolah Teknik Elektro dan Informatika,
Institut Teknologi Bandung

PENDAHULUAN

Pemanfaatan teknologi informasi sudah masuk ke dalam kehidupan sehari-hari manusia Indonesia. Menurut statistik dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2013), jumlah pengguna internet Indonesia saat ini sudah mencapai 63 juta orang. Statistik yang dikeluarkan secara berkala oleh Social Bakers (Social Bakers, 2013) menunjukkan pengguna layanan *facebook* dari Indonesia juga cukup dominan, lebih dari 40 juta pengguna. Statistik dari Media Bistro menunjukkan pengguna *twitter* dari Indonesia hampir mendekati 30 juta orang (Media Bistro, 2013). Statistik lain dari pemodal ventura besar di Amerika juga menunjukkan besarnya pasar Indonesia (Meeker, 2013).

Banyaknya pengguna teknologi informasi ini tentunya akan menimbulkan masalah, mulai perbuatan yang tidak menyenangkan sampai pada terjadinya kejahatan (*fraud*). Statistik yang dikeluarkan oleh ID-CERT menunjukkan masalah keamanan (*security*) berupa serangan melalui jaringan (*network attack*) termasuk perusakan situs web (*deface*) dan penerobosan hak akses, virus atau *malware*, *phishing*, dan *fraud* (ID-CERT, 2012). Selain kasus di atas, masih ada kasus lain yang terkait dengan terorisme, seperti kasus *laptop* Imam Samudra. Kemudian masih ada juga kasus terkait dengan korupsi.

FORENSIK DIGITAL

Penanganan kasus yang terkait dengan penggunaan teknologi informasi sering membutuhkan forensik. Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (komputer, *handphone*, tablet, PDA, *net-working devices*, *storage*, dan sejenisnya)

Forensik digital dapat dibagi lebih jauh menjadi forensik yang terkait dengan komputer (*host*, *server*), jaringan (*network*), aplikasi (termasuk database), dan perangkat (*digital devices*). Masing-masing memiliki pendalaman tersendiri.

Pada **forensik komputer**, fokus penyidikan terkait dengan data yang berada atau terkait dengan komputer itu sendiri. Layanan yang disediakan oleh komputer atau *server* biasanya tercatat dalam berbagai berkas log. Sebagai contoh, pengguna yang gagal masuk karena salah memasukkan *password* akan tercatat. Hal ini merupakan bagian dari upaya untuk melakukan penerobosan akses dengan cara *brute force password cracking*. Di sisi desktop, pengguna memasukkan *flash disk* ke port USB juga tercatat.

Forensik komputer ini bergantung pada sistem operasi yang digunakan. Sebagai contoh, kebanyakan pengguna komputer *desktop* menggunakan sistem operasi *Microsoft Windows*. Oleh karena itu, diperlukan kemampuan untuk melakukan forensik pada komputer yang menggunakan sistem operasi *Microsoft Windows* (Carvey, 2005). Sistem operasi yang lain meletakkan data pada berkas yang berbeda dengan format yang berbeda. Sebagai contoh pada sistem UNIX catatan tersedia pada layanan *syslog*, sementara itu pada sistem *Microsoft Windows* catatan dapat dilihat dengan *Event Viewer*. Berbagai *tools* forensik tersedia untuk membantu penyidik dalam mengumpulkan data yang terkait dengan sistem operasi yang digunakan.

Forensik jaringan memfokuskan pada data yang diperoleh berdasarkan pengamatan pada jaringan. Sebagai contoh, kita dapat mengamati *traffic* pada server-server yang diakses oleh seorang pengguna, yang diduga melakukan penerobosan pada sever. Bisa jadi server-server tersebut merupakan target penyerangan dari pengguna. Berbagai perangkat untuk melakukan penyadapan

jaringan dapat digunakan untuk memantau kejadian ini.

Forensik aplikasi terkait dengan penggunaan aplikasi tertentu. Aplikasi memiliki fitur untuk meninggalkan jejak sebagai bagian dari fungsi audit. Ada kewajiban bagi aplikasi untuk mencatat berbagai akses sebagai bagian dari fungsi audit ini. Sebagai contoh, penggunaan *email* dapat ditelusuri dengan adanya catatan jejak di *header* dari *email*. Kejadian yang terkait dengan *email* palsu atau "email kaleng" dapat ditelusuri sumbernya dengan menelusuri *header* dari *email*.

Sering kegiatan forensik dilakukan terhadap komputer atau laptop yang digunakan oleh pengguna. Berbagai dokumen dan aplikasi pada komputer tersebut dapat memberi informasi yang bermanfaat untuk forensik. Sebagai contoh, sejarah *browsing* dari pengguna dapat ditampilkan dan dikorelasikan dengan kejadian yang terkait dengan *server* atau transaksi palsu. Hal ini juga terkait dengan forensik komputer.

Terkait dengan aplikasi adalah penggunaan *database*. Sebagian besar aplikasi saat ini terhubung dengan *database*. Akses terhadap *database* ini juga tercatat sehingga jika terjadi masalah – seperti *fraud* – jejak-jejak yang tertinggal di catatan (*log*) *data-base* dapat digunakan untuk forensik.

Perangkat nonkomputer sekarang lebih banyak digunakan untuk mengakses data (misalnya mengakses internet) dan berkomunikasi (*chat*). *Handphone* dan tablet saat ini bahkan lebih populer daripada komputer dan *laptop*.

Forensik terhadap **perangkat** dilakukan untuk mengumpulkan data dan bukti atas kegiatan tertentu. Karena banyaknya jenis perangkat digital, forensik terhadap perangkat cukup sulit dilakukan.

KEMUDAHAN DAN TANTANGAN FORENSIK DIGITAL

Salah satu kehebatan data digital adalah mudahnya data digandakan (diduplikasi). Hasil penggandaan data digital dapat sama persis dengan aslinya, sehingga perlu didefinisikan apa yang disebut asli atau original. Sebagai contoh, jika saya menggandakan (*copy*) sebuah berkas dari *disk* saya ke *flash disk* Anda dan kemudian Anda membuka berkas itu pada komputer serta mencetaknya, mana yang disebut asli? Jawabannya adalah semuanya. Asli dalam data digital dapat lebih dari satu. Ini sebuah konsep yang agak membingungkan.

Kemudahan menggandakan data digital ini dapat memudahkan kegiatan forensik. Sebagai contoh, jika penyidik mendapatkan sebuah komputer pengguna, penyidik dapat menggandakan *disk* dari komputer pengguna ke *disk* baru. Proses penyidikan kemudian dapat dilakukan pada data di *disk* baru tanpa khawatir akan mencemari data aslinya. Jika terjadi kesalahan dalam pemrosesan data, dapat dilakukan penggandaan ulang dan pemrosesan ulang. Hal ini tidak dapat dilakukan dalam forensik nondigital. Penyidik hanya dapat melakukan pemrosesan sekali saja.

Di sisi lain, data digital dapat mudah berubah atau bahkan dihilangkan. Sebagai contoh, jika kita mengakses sebuah berkas (misalnya membukanya dalam editor berkas), *access time* dari berkas tersebut berubah. Berkas dapat hilang atau tertimpa dengan berkas yang lebih baru. Misalnya ketika kita mengakses sebuah aplikasi pada sebuah computer, berkas *log* dari aplikasi tersebut akan tertimpa dengan data baru. Pencemaran data digital ini dapat terjadi jika kita tidak berhati-hati dalam memprosesnya.

Data digital juga dapat dibuat dengan mudah. Salah satu hal yang ditakutkan adalah adanya penambahan data oleh penyidik (misalnya ada pendambahan data untuk menyudutkan pemilik perangkat digital). Untuk itu, diperlukan adanya mekanisme yang memastikan bahwa penyidik tidak dapat (atau sulit) untuk melakukan rekayasa terhadap data. Ada beberapa mekanisme yang dapat dilakukan, seperti penggunaan *message digest* terhadap berkas yang akan dievaluasi dan penggunaan *tools* yang sudah disertifikasi.

Secara teknis data digital dapat dikumpulkan dan dapat dibuktikan keabsahannya. Apakah data ini dapat diakui sebagai bukti di pengadilan? Ada beberapa konsep yang berbeda antara dunia nyata dan dunia maya (digital). Hukum banyak mengandalkan pada konsep ruang dan waktu. Sementara itu, penerapan teknologi informasi – seperti internet – justru menghancurkan konsep ruang dan waktu. Sebagai contoh, apabila terjadi penerobosan akses (*hacking*) yang dilakukan oleh orang Indonesia terhadap *server* di Amerika yang dimiliki oleh perusahaan Jepang, hukum mana yang akan digunakan? Di mana sebetulnya kejahatan terjadi? Untuk itu, para penegak hukum harus dibekali pengetahuan yang baru. Hukum pun mungkin perlu diperbaharui dengan keberadaan hal ini.

SIMPULAN

Forensik digital merupakan bidang yang baru berkembang tetapi berkembang dengan pesat sejalan dengan pesatnya pemanfaatan teknologi informasi. Berbagai ilmu dan perangkat telah dikembangkan untuk memudahkan penyidik dalam mengumpulkan data serta merangkainya untuk membuktikan kejahatan yang telah terjadi. Sebagai ilmu yang masih baru tentunya masih dibutuhkan waktu untuk mencapai kematangan.

Salah satu masalah yang dihadapi oleh forensik digital adalah cepatnya perkembangan ilmu dan teknologi digital. Pada tahun 2009, Indonesia belum masuk ke dalam statistik penggunaan *twitter*. Empat tahun kemudian, Indonesia sudah menempati peringkat nomor lima di dunia dari jumlah pengguna *twiter* dengan 30 juta pengguna. Perangkat *handphone* dan tablet juga semakin banyak penggunanya dengan sistem operasi yang bervariasi.

Penguasaan teknologi yang berkembang dengan cepat ini merupakan tantangan bagi penyidik digital dan penegak hukum. Upaya-upaya untuk peningkatan pemahaman dan kemampuan harus terus ditingkatkan.

DAFTAR PUSTAKA

APJII, 2012. *Profil Internet Indonesia*, http://www.apjii.or.id/v2/index.php/read/content/laporan-publik/177/profil-internet-indonesia-2012.html, 2012.

Carvey, Harlan. 2005. "*Windows Forensics and Incident Recovery*," Addison Wesley.

ID-CERT, 2012. *Incident Handling Report*. online, http://www.cert.or.id/incident_handling/penelitian/3/, 2012.

Media Bistro. 2013. *Top 20 countries in term of Twitter accounts*, online, http://www.mediabistro.com/alltwitter/twitter-top-countries_b26726.

Meeker, Mary. 2013. *Internet Trends @Standfor Bases*, Kleiner Perkins Caufield Byers (KPCB), online, http://www.slideshare.net/kleinerperkins/2012-kpcb-internet-trends-yearend-update.

Social Bakers. 2013. *Facebook Users (March 2013)*, online, http://www.socialbakers.com/facebook-statistics/.