ANTISIPASI CYBERCRIME MENGGUNAKAN TEKNIK KOMPUTER FORENSIK

Yudi Prayudi, Dedy Setyo Afrianto
Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Jl. Kaliurang Km. 14 Yogyakarta 55501
Telp. (0274) 895287 ext. 122, Faks. (0274) 895007 ext. 148
e-mail: prayudi@fti.uii.ac.id

ABSTRAKSI

Perkembangan pesat dari teknologi informasi ternyata juga diikuti oleh berkembangnya isu seputar keamanan dan kejahatan komputer. Berbagai modus kejahatan baru berbantuan komputer mulai banyak dirasakan oleh masyarakat. Selain perangkat hukum dalam bentuk aturan dan undang-undang, maka dari aspek ilmiah dan teknis juga diperlukan mekanisme pembuktian kejahatan tersebut. Dalam hal ini komputer forensik adalah satu bidang yang akan sangat mendukung upaya-upaya penegakan hukum terhadap tindak kejahatan berbantuan komputer. Makalah ini memberikan gambaran singkat terkait pengertian, metode dan implementasi proses forensik menggunakan sejumlah aplikasi yang tersedia.

Kata kunci: cybercrime, forensik, investigasi, bukti digital.

1. PENDAHULUAN

Perkembangan Teknologi Informasi dan Komputer (TIK) telah mengalami kemajuan yang sangat pesat, terutama sekali setelah diketemukannya teknologi yang menghubungkan antar komputer (*Networking*) dan Internet. Namun demikian, berbagai kemajuan tersebut ternyata diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada penggunaan komputer sebagai alat untuk melakukan berbagai modus kejahatan. Istilah ini kemudian dikenal dengan *cybercrime*.

Permasalahan yang diakibatkan oleh penggunaan komputer untuk kepentingan diatas telah mulai menimbulkan berbagai dampak negatif. Baik secara mikro yang dampaknya hanya pada tingkatan personal/perseorangan, maupun secara makro yang berdampak pada wilayah komunal, publik, serta memiliki efek domino yang luas. Untuk menangani permasalahan ini, maka di beberapa negara telah dibentuk unit khusus kepolisian yang berfungsi sebagai penindak kejahatan yang spesifik terkait dengan permasalahan *cybercrime*.

1.1 Kasus Cybercrime

Berbagai permasalahan yang muncul terkait dengan *cybercrime* telah menyedot perhatian berbagai kalangan yang berhubungan dengan bidang TIK. Hal ini dipicu oleh semakin luasnya dimensi kejahatan di bidang cybercrime ini. Contoh kasusnya antara lain adalah*:*

a. Menurut *Internet Fraud Complaint Center* (IFCC), mitra dari *Federal Beureau and Investigation* (FBI) dan *National White Collar Crime Center*, antara Mei 2000 dan Mei 2001, dalam operasi tahun pertama, website IFFC menerima 30.503 keluhan penipuan internet. Laporan lengkap dapat download pada alamat: *www1.ifccfbi.gov/strategy/IFCC_Annual_Report.pdf.*

b. Menurut Survey Institute Keamanan Komputer pada 2001, bersama dengan Squad Gangguan Komputer dari FBI,186 responden dari agen perusahaan dan pemerintah melaporkan total kehilangan keuangan diatas US$3.5 juta, sebagian besar terjadi karena pencurian informasi kepemilikan dan penipuan keuangan *(*lihat *www.gocsi.com/press/20020407.html).*

c. Menurut *Cybersnitch Voluntary Online Crime* melaporkan sistem kejahatan relasi-internet telah mencakup berbagai aspek mulai dari pemalsuan desktop hingga ke pornografi anak dan juga meliputi kejahatan seperti pencurian elektronik hingga ancaman teroris. (daftar dilaporkan cybercrimes tersedia pada alamat: (*www.cybersnitch.net/csinfo/csdatabase.asp.* .)

1.2 Alasan kemunculan Cybercrime

Pada tahun 2002 diperkirakan terdapat sekitar 544 juta orang terkoneksi secara online. Meningkatnya populasi orang yang terkoneksi dengan internet akan menjadi peluang bagi munculnya kejahatan komputer dengan beragam variasi kejahatannya. Dalam hal ini terdapat sejumlah tendensi dari munculnya berbagai gejala kejahatan komputer, antara lain:

a. Permasalahan finansial. C*ybercrime* adalah alternatif baru untuk mendapatkan uang. Perilaku semacam *carding* (pengambil alihan hak atas kartu kredit tanpa seijin pihak yang sebenarnya mempunyai otoritas*)*, pengalihan rekening telepon dan fasilitas lainnya, ataupun perusahaan dalam bidang tertentu yang mempunyai kepentingan untuk menjatuhkan *kompetitor*nya dalam perebutan *market*, adalah sebagian bentuk cybercrime dengan tendensi finansial.

b. Adanya permasalahan terkait dengan persoalan politik, militer dan sentimen *Nasionalisme*. Salah satu contoh adalah adanya serangan hacker pada awal tahun 1990, terhadap pesawat pengebom paling rahasia Amerika yaitu *Stealth Bomber*. Teknologi tingkat tinggi yang terpasang pada pesawat tersebut telah menjadi lahan yang menarik untuk dijadikan ajang kompetisi antar negara dalam mengembangkan peralatan tempurnya.
c. Faktor kepuasan pelaku, dalam hal ini terdapat permasalahan psikologis dari pelakunya. Terdapat kecenderungan bahwasanya seseorang dengan kemampuan yang tinggi dalam bidang penyusupan keamanan akan selalu tertantang untuk menerobos berbagai sistem keamanan yang ketat. Kepuasan batin lebih menjadi orientasi utama dibandingkan dengan tujuan finansial ataupun sifat sentimen.

Elemen penting dalam penyelesaian masalah keamanan dan kejahatan dunia komputer adalah penggunaan sains dan teknologi itu sendiri. Dalam hal ini sains dan teknologi dapat digunakan oleh fihak berwenang seperti: penyelidik, kepolisian, dan kejaksaan untuk mengidentifikasi tersangka pelaku tindak kriminal.

2. KOMPUTER FORENSIK

Forensik adalah proses penggunaan pengetahuan ilmiah dalam mengumpulkan, menganalisa, dan mempresentasikan barang bukti ke pengadilan. Forensik secara inti berhubungan dengan penyelamatan dan analisis barang bukti laten. Barang bukti laten dapat berbentuk dalam banyak format, mulai dari sidik jari di jendela, DNA yang diperoleh dari noda darah sampai file-file di dalam hard disk komputer.

2.1 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. Sesuai 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:

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

Pembuktian dalam dunia maya memiliki karakteristik tersendiri. Dalam hal ini sifat alami dari teknologi komputer memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya. Karena itulah salah satu upaya untuk mengungkap kejahatan komputer adalah lewat pengujian sistem yang berperan 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 komputer forensik untuk menegakkan hukum dengan mengamankan barang bukti, rekonstruksi kejahatan, dan menjamin jika bukti yang dikumpulkan itu akan berguna di persidangan.

2.2 Definisi Komputer Forensik

Menurut Marcella [4] , secara terminologi, Komputer Forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, [pengambilan/penyaringan, dan dokumentasi bukti komputer dalam kejahatan komputer. Istilah ini relatif baru dalam bidang komputer dan teknologi, tapi telah muncul diluar *term* teknologi (berhubungan dengan investigasi dan investigasi bukti-bukti intelejen dalam penegakan hukum dan militer) sejak pertengahan tahun 1980-an.

Menurut Budhisantoso[1], komputer forensik belum dikenali sebagai suatu disiplin pengetahun yang formal. Dalam hal ini definisi komputer forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sedemikian sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum

Seperti umumnya ilmu forensik lain, komputer forensik juga melibatkan penggunaan teknologi yang rumit, perkakas dan prosedur yang harus diikuti untuk menjamin ketelitian dari pemeliharaan bukti dan ketelitian hasil. Prinsip kerja komputer forensik pada dasarnya mirip dengan proses yang terjadi pada kepolisian ketika hendak mengusut bukti tindak kejahatan dengan menelusuri fakta-fakta yang ada. Hanya saja pada komputer forensik proses dan kejadiannya terdapat pada dunia maya. Selain untuk kepentingan pembuktian, penggunaan forensik komputer secara tepat juga dapat membersihkan seseorang yang tidak bersalah dari dakwaan atau sebaliknya membawa seseorang yang terbukti bersalah kehadapan hukum

3. METODOLOGI FORENSIK

Menurut Wright[7] penyelidikan sebaiknya dimulai bila sebuah rencana telah terumuskan dengan baik. Maka landasan metodologi akan memetakan kontruksi ilmiah dalam menyelesaikan

sebuah pekerjaan. Demikian juga dalam komputer forensik, metodologi diharapkan akan membantu tercapainya hasil yang dituju. Walaupun tidak ada standard baku, namun terdapat sejumlah tahapan yang sebaiknya dilakukan dalam proses komputer forensik, yaitu: menentukan tujuan, memproses fakta, mengungkapkan bukti digital.

Tujuan diperlukan sebagai pengarah akhir dari sebuah investigasi. Dalam hal ini sebuah tujuan sebaiknya juga dideskripsikan dalam bentuk parameter-parameter kesuksesan dalam meng-*investigasi* kejadian. Dengan adanya parameter tersebut maka akan diketahui kapan hasil dari inverstigasi telah berakhir.

3.1 Pengungkapan Bukti Digital

Bukti digital (*Digital Evidence*) merupakan salahsatu perangkat vital dalam mengungkap tindak *cybercrime*. Dengan mendapatkan bukti-bukti yang memadai dalam sebuah tindak kejahatan, sebenarnya telah terungkap separuh kebenaran. Langkah berikutnya adalah menindak-lanjuti bukti-bukti yang ada sesuai dengan tujuan yang ingin dicapai. Bukti Digital yang dimaksud dapat berupa adalah : E-mail, file-file wordprocessors, spreadsheet, sourcecode dari perangkat lunak, Image, web browser, bookmark, cookies, Kalender.

Menurut Kemmish[3], terdapat empat elemen forensic yang menjadi kunci pengungkapan bukti digital. Elemen forensic tersebut adalah: identifikasi bukti digital, penyimpanan bukti digital, analisa bukti digital, presentasi bukti digital.

3.2 Identifikasi Bukti Digital

Elemen ini merupakan tahapan paling awal dalam komputer forensik. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan. *Network Administrator* merupakan sosok pertama yang umumnya mengetahui keberadaan *cybercrime* sebelum sebuah kasus *cybercrime* diusut oleh fihak yang berwenang. Ketika fihak yang berwenang telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemen-elemen vital lainnya, antara lain:

a. Petugas Keamanan (Officer/*as a First Responder*), Memiliki kewenangan tugas antara lain : mengidentifikasi peristiwa,mengamankan bukti, pemeliharaan bukti yang temporer dan rawan kerusakan.
b. Penelaah Bukti (Investigator), adalah sosok yang paling berwenang dan memiliki kewenangan tugas antara lain: menetapkan instruksi-instruksi, melakukan pengusutan peristiwa kejahatan, pemeliharaan integritas bukti.
c. Tekhnisi Khusus, memiliki kewenangan tugas antara lain : memeliharaan bukti yang rentan kerusakan dan menyalin *storage* bukti, mematikan(*shuting down*) sistem yang sedang berjalan, membungkus/memproteksi bukti-bukti, mengangkut bukti dan memproses bukti.

Ketiga elemen vital diatas itulah yang umumnya memiliki *otoritas* penuh dalam penuntasan kasus cybercrime yang terjadi.

3.3 Penyimpanan Bukti Digital

Barang bukti digital merupakan barang bukti yang rapuh. Tercemarnya barang bukti digital sangatlah mudah terjadi, baik secara tidak sengaja maupun disengaja. Kesalahan kecil pada penanganan barang bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan.

Bentuk, isi, makna dari bukti digital hendaknya disimpan dalam tempat yang *steril*. Hal ini dilakukan untuk benar-benar memastikan tidak ada perubahan-perubahan. Sedikit terjadi perubahan dalam bukti digital, akan merubah hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, mengalami kecelakaan. Langkah pertama untuk menghindarkan dari kondisi-kondisi demikian salah satunya adalah dengan melakukan copy data secara *Bitstream Image* pada tempat yang sudah pasti aman.

Bitstream image adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk File yang tersembunyi (*hidden files*), File temporer (temp file), File yang terdefragmen (*fragmen file*), dan file yang belum ter-*overwrite*. Dengan kata lain, setiap biner digit demi digit di-copy secara utuh dalam media baru. Teknik pengkopian ini menggunakan teknik komputasi CRC**.** Teknik ini umumnya diistilahkan dengan *Cloning Disk* atau *Ghosting*.

3.4 Analisa Bukti Digital

Barang bukti setelah disimpan, perlu diproses ulang sebelum diserahkan pada pihak yang membutuhkan. Pada proses inilah skema yang diperlukan akan fleksibel sesuai dengan kasus-kasus yang dihadapi. Barang bukti yang telah didapatkan perlu di-*explore* kembali kedalam sejumlah scenario yang berhubungan dengan tindak pengusutan, antara lain: siapa yang telah melakukan, apa yang telah dilakukan (Contoh : penggunaan software apa saja), hasil proses apa yang dihasilkan, waktu melakukan).

Secara umum, tiap-tiap data yang ditemukan dalam sebuah sistem komputer sebenarnya adalah potensi informasi yang belum diolah, sehingga keberadaannya memiliki sifat yang cukup penting. Data yang dimaksud antara lain : 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, ,Registry

Windows, Log Event viewers dan Log Applications, File print spool.

3.5 Presentasi Bukti Digital

Kesimpulan akan didapatkan ketika semua tahapan telah dilalui, terlepas dari ukuran *obyektifitas* yang didapatkan, atau standar kebenaran yang diperoleh, minimal bahan-bahan inilah nanti yang akan dijadikan "modal" untuk bukti di pengadilan. Selanjutnya bukti-bukti digital inilah yang akan dipersidangkan, diuji otentifikasi dan dikorelasikan dengan kasus yang ada. Pada tahapan ini semua proses-proses yang telah dilakukan sebelumnya akan diurai kebenarannya serta dibuktikan kepada hakim untuk mengungkap data dan informasi kejadian.

4. IMPLEMENTASI PROSES KOMPUTER FORENSIK

Untuk melakukan proses forensic pada sistem komputer maka dapat digunakan sejumlah tools yang akan membantu investigator dalam melakukan pekerjaan forensiknya.

Menurut Budhisantoso[1] secara garis besar tools untuk kepentingan komputer forensik dapat dibedakan secara hardware dan software. Hardware tools forensik memiliki kemampuan yang beragam mulai dari yang sederhana dengan komponen *single-purpose* seperti *write blocker* sampai sistem komputer lengkap dengan kemampuan server seperti F.R.E.D (*Forensic Recovery of Evidence Device).* Sementara Tools software forensik dapat dikelompokkan kedalam dua kelompok yaitu aplikasi berbasis *command line* dan aplikasi berbasis GUI.

Baik dari sisi hardware maupun software, tools untuk komputer forensik diharapkan dapat memenuhi 5 fungsi, yaitu untuk kepentingan akuisisi (*acquisition),* validasi dan diskriminasi (*validation and discrimination),* ekstraksi (*extraction),* rekonstruksi (*reconstruction)* dan pelaporan (*reporting).*

Salah satu software yang dapat digunakan untuk kepentingan identifikasi perolehan bukti digital adalah Spy Anytime PC Spy dari Waresight.Inc (www.waresight.com). Kemampuan dari aplikasi ini antara lain adalah untuk monitoring berbagai aktivitas komputer, seperti: *website logs, keystroke logs, application logs, screenshot logs, file/folder logs.*

Untuk kepentingan penyimpanan bukti digital, salah satu teknik yang digunakan adalah Cloning Disk atau Ghosting. Teknik ini adalah teknik copy data secara bitstream image..Salah satu aplikasi yang dapat digunakan untuk kepentingan ini adalah NortonGhost 2003 dari Symantec Inc. (www.symantec.com).

Untuk kepentingan analisa bukti digital, salah satu aplikasi yang dapat digunakan adalah Forensic Tools Kit (FTK) dari Access Data Corp (www.accesdata.com). FTK sebenarnya adalah aplikasi yang sangat memadai untuk kepentingan implementasi Komputer Forensik. Tidak hanya untuk kepentingan analisa bukti digital saja, juga untuk kepentingan pemrosesan bukti digital serta pembuatan laporan akhir untuk kepentingan presentasi bukti digital.

5. PENUTUP

Mengingat semakin banyak kasus-kasus yang terindikasi sebagai cybercrime, maka selain aspek hukum maka secara teknis juga perlu disiapkan berbagai upaya preventif terhadap penangulangan kasus cybercrime. Komputer forensik, sebagai sebuah bidang ilmu baru kiranya dapat dijadikan sebagai dukungan dari aspek ilmiah dan teknis dalam penanganan kasus-kasus cybercrime.

Kedepan profesi sebagai investigator komputer forensik adalah sebuah profesi baru yang sangat dibutuhkan untuk mendukung implementasi hukum pada penanganan cybercrime. Berbagai produk hukum yang disiapkan untuk mengantisipasi aktivitas kejahatan berbantuan komputer tidak akan dapat berjalan kecuali didukung pula dengan komponen hukum yang lain. Dalam hal ini komputer forensik memiliki peran yang sangat penting sebagai bagian dari upaya penyiapan bukti-bukti digital di persidangan.

PUSTAKA

[1]. Budhisantoso, Nugroho, Personal Site, alamat: www.forensik-komputer.info

[2]. Budiman, Rahmadi, 2003, *Makalah Tugas Keamanan Sistem Lanjut, Komputer Forensik Apa Dan Bagaimana***,** Magister Teknik Elektro Option Teknologi Informasi, Institut Teknologi Bandung.2003

[3]. Kemmish, Rodney Mc., *What is forensic computer*, Australian institute of Criminology, Canberra. Alamat situs: www.aic.gov.au/publications/tandi/ti118.pdf

[4]. Marcella, Albert J., and Robert S. Greenfiled, "*Cyber Forensics a field manual for collecting, examining, and preserving evidence of computer crimes*", by CRC Press LLC, United States of America. Alamat Situs: www.forensics-intl.com/def4.html.

[5]. Shinder, Debra Littlejhon, 2002, *Scene Of Cybercrime, computer forensic hand book.* by Syngress Publishing,Inc.

[6]. Utdirartatmo, Firar, 2001, *Makalah tugas Tinjauan Analisis Forensik Dan Kontribusinya Pada Keamanan Sistem Komputer*, Magister Teknik Elektro Option Teknologi Informasi, Institut Teknologi Bandung.

[7]. Wright, Mal, 2001, "*Investigating an Internal Case of Internet Abus*e", SANS Institute.