KEAMANAN JARINGAN DENGAN KOMPUTER FORENSIK

Helmi Kurniawan

Dosen Jurusan Teknik Informatika STMIK Potensi Utama
STMIK Potensi Utama, Jl. K.L Yos Sudarso Km. 6,5 No.3-A Tj.Mulia Medan
Email : helmikk12@gmail.com

ABSTRACT

In the last decade, the number of crimes involving computers has increased rapidly, resulting in growing companies and products that seek to assist law enforcement in using computer-based evidence to determine who, what, where, when, and how in a crime. Consequently, computer forensics has evolved to ensure proper presentation of the data of computer crime in court. Forensic techniques and tools are often imagined in connection with criminal investigations and the handling of computer security incidents, is used to respond to an incident to investigate a suspect system, collect and preserve evidence, reconstruct events, and predict the status of an event. However, forensic tools and techniques can also be used for other tasks, such as Operational Troubleshooting. Log Monitoring, Data Recovery, Data Acquisition and Due Diligence / Regulatory Compliance.

Keywords: Computer Forensics, Computer Crime and Computer Security

ABSTRAK

Dalam satu dekade terakhir, jumlah kejahatan yang melibatkan komputer telah meningkat pesat, mengakibatkan bertambahnya perusahaan dan produk yang berusaha membantu penegak hukum dalam menggunakan bukti berbasis komputer untuk menentukan siapa, apa, dimana, kapan, dan bagaimana dalam sebuah kejahatan. Akibatnya, komputer forensik telah berkembang untuk memastikan presentasi yang tepat bagi data kejahatan komputer di pengadilan. Teknik dan tool forensik seringkali dibayangkan dalam kaitannya dengan penyelidikan kriminal dan penanganan insiden keamanan komputer, digunakan untuk menanggapi sebuah kejadian dengan menyelidiki sistem tersangka, mengumpulkan dan memelihara bukti, merekonstruksi kejadian, dan memprakirakan status sebuah kejadian. Namun demikian, tool dan teknik forensik juga dapat digunakan untuk tugas-tugas lainnya, seperti Operational Troubleshooting. Log Monitoring, Data Recovery, Data Acquisition dan Due Diligence/Regulatory Compliance.

Kata Kunci : Komputer Forensik, Kejahatan Komputer dan Keamanan Komputer

PENDAHULUAN

Tidak dapat dipungkiri lagi bahwa penggunaan teknologi internet telah banyak membantu dalam kegiatan kita sehari-hari. Banyak hal yang dapat kita lakukan dengan menggunakan internet, misalnya e-banking, e-education, e-commerce, e-goverment dan hal-hal lainnya yang dapat kita lakukan secara virtual dimana kita seolah-olah ada di tempat tersebut dan melakukan hal-hal yang dilakukan secara nyata.

Perkembangan internet yang semakin hari semakin pesat baik itu dari sisi teknologi mau-pun sisi penggunanya membawa dampak negatif dan positif. Dampak negatif yang kita peroleh sudah selayaknya kita syukuri, karena begitu banyak manfaat yang bisa kita peroleh dari teknologi ini, misalnya kita dapat mencari referensi ilmu pengetahuan dengan begitu mudahnya.

Di samping itu kita juga patut mewaspadai kemungkinan terjadinya tindakan kriminal dengan memanfaatkan teknologi internet atau yang lebih dikenal dengan istilah cybercrime. Karena sudah menjadi sifat dasar manusia untuk mencoba segala sesuatu yang baru. Berawal dari rasa ingin tau, banyak orang mulai mencoba-coba atau bahkan menjadi provesinya untuk memperoleh keuntungan secara ilegal.

Perkembangan kejahatan dengan menggunakan teknologi internet pun semakin beragam seiring dengan perkembangan teknologi yang ada. Mulai dari internet abuse, hacking, carding, dan sebagainya. Sehingga muncul pertanyaan apakah jaringan komputer itu cukup aman? Apkah aman bila melakukan proses transaksi perbankan melalui jaringan komputer tanpa khawatir seseorang mensabotase transaksi itu sendiri? Apakah mungkin seseorang mengetahui password orang lain dan menggunakannya tanpa sepengetahuan orang yang lebih berhak? Dapatkah kita mempunyai sebuah jalur komunikasi yang aman di internet? Untuk menjawab semua pertanyaan yang ada di atas tentunya sangat tergantung dengan kondisi dan tingkatan permaslahannya sendiri, serta sangat tergantung kepada setiap kasus yang terjadi.

Umumnya kita sebagai manusia menginginkan privasi, keamanan, dan perasaan aman dalam hidup, termasuk juga dalam hal penggunaan internet. Tentunya kita sangat mengharapkan apa yang kita kerjakan dengan menggunakan teknologi internet bisa aman dan jauh dari kemungkinan untuk di rusak, di curi, atau disalahgunakan oleh pihak-pihak yang sebetulnya tidak mempunyai hak.

Menginggat buruknya dampak yang di timbulkan akibat adanya kejahatan internet. Maka penulis ingin membuka mata pengguna internet untuk mengetahui bahayanya cybercrime dan upaya apa saja yang dapat dilakukan dalam komputer forensik untuk mengatasi masalah yang timbul akibat cybercrime.

Tujuan penelitian

Di masa informasi bebas seperti sekarang ini, terjadi kecenderungan peningkatan kerugian finansial dari pihak pemilik komputer karena kejahatan komputer. Kejahatan komputer dibagi menjadi dua, yaitu computer fraud dan computer crime. Computer fraud meliputi kejahatan atau pelanggaran dari segi sistem organisasi komputer. Sedang computer crime merupakan kegiatan berbahaya di mana menggunakan media komputer dalam melakukan pelanggaran hukum. Untuk menginvestigasi dan menganalisa kedua kejahatan di atas, maka digunakan sistem forensik dalam teknologi informasi.

Metode Penelitian

Metodologi penelitian yang digunakan penulis dalam pengumpulan data ialah dengan menggunakan tehnik literatur, yaitu penelitian kepustakaan dengan menggunakan bahan-bahan pustaka yang mendukung, baik dari buku maupun dari internet.

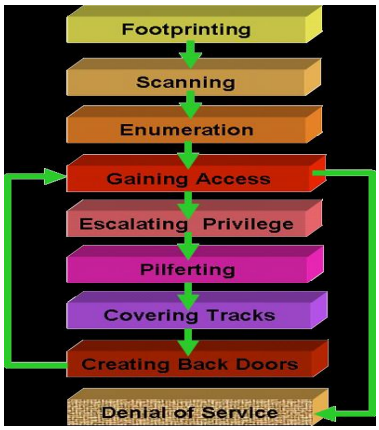
LANDASAN TEORI

Cyber crime adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terkoneksi ke internet, dan mengeksploitasi komputer lain yang juga terhubung ke internet. Banyak istilah yang digunakan dalam kejahatan internet seperti hacker, cracker, script kiddies, serta fase-fase yang dilakukan dalam melakukan penyerangannya.

Hacker secara umum diartikan sebagai orang-orang yang mempunyai kemampuan yang lebih. Istilah hacker sendiri digolongkan atas 3 bagian, yaitu white-hat, blcak-hat, dan gray-hat.
a.) White-hat ditujukan bagi mereka yang membantu menemukan vulnerability di sistem komputer dan terkadang juga memberikan solusi bagaimana cara untuk mengatasinya. b) Sedangkan blcak-hat mengacu kepada orang-orang yang melakukan eksploitasi kelemahan sistem dengan tujuan untuk mendapatkan informasi atau data secara ilegal, atau bahkan merusak seperti melakukan deface situs, pencurian data, penghapusan data, shutdown server korban, install backdoor, dan berbagai bentuk serangan lainnya seperti DoS (Denial of Service) yang membuat sistem tidak berfungsi. c) Gray hat atau hacker abu-abu adalah kombinasi dari kedua di atas, di mana kadang kala tindakan mereka dapat merusak, namun di lain pihak juga membantu dunia komputing security.

Craker ialah sebuat sebutan untuk orang-orang yang menggunakan keahlian hackingnya dengan tujuan merusak atau sering juga disebut black hat.

Script Kiddies ialah mereka- mereka yang tidak mempunyai keahlian khusus di bidang hacking. Mereka hanya meng-download hacking tools dari internet dan kemudian mencoba melakukan hacking dengan tools tersebut.



Gambar 1. Metodelogi Hacking

Fase-Fase Hacking :

a. FootPrintiing

Pada fase ini hacker berusaha untuk memperoleh informasi sebanyak-banyaknya mengenai target atau calon korban seperti nama domain, alamat IP, teknologi yang ada, teknikal kontak dan sebagainya.

b. Scanning

Pada fase ini hacker mulai melakukan probing atau penyelidikan terhadap korban untuk mencari lubang security yang bisa di eksploitasi atau sebagai pintu masuk ke sistem yang ingin diserang.

c. Enumuration

Merupakan telaah intensif terhadap sistem, mencari user account yang absah, resource dan aplikasi yang sedang berjalan pada sistem.

d. Gaining Access (Mendapatan akses)

Apabila ditemukannnya lubang security, maka yang dilakukan selanjutnya adalah men-coba memasuki sistem tersebut atau mendapatkan akses.

e. Escalating Privilege

Bila telah mendapatkan user password di tahap sebelumnya, di tahap ini di usahakan mendapat privilese admin jaringan dengan password cracking atau melakukan eksplotasai.

f. Pilfering

Proses pengumpulan informasi di mulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry, config file, dan user data.

g. Covering Tracks

Ffase ini merupakan fase yang cukup sulit untuk dilakukan dan merupakan fase yang banyak dilupakan oleh para hacker. Umumnya mereka meninggalkan jejak di log file (firewall, IDS, sistem operasi, aplikasi dan lainnya) file-file log ini bisa dianalisa dengan teknik-teknik forensik oleh para penyelidik atau tim forensik. Dan bahkan file log tersebut sudah di hapus oleh hacker, file yang sudah di hapus tersebut juga bisa dikembalikan (retrieve) sehingga bisa menjadi bukti di pengadilan. Itulah kenapa hacker berhasil ditangkap dan berakhir di penjara.

h. Creating Backdoors

Untuk memudahkan masuk kembali ke dalam sistem tanpa harus memulai semua proses dari awal, maka dibuatlah pintu belakang dengan cara membentuk user account palsu, menjadwal-kan catch job, mengubah startup file, menanamkan servis kendali jarak jauh serta monitoring sistem.

i. Denial of service

Serangan ini memaksa target ke dalam suatu kondisi yang kacau sehingga menghentikan layanannya kepada yang lain. Terdapat beberapa cara yang dapat memicu kondisi kacau ini, seperti membanjiri target dengan usaha-usaha koneksi meliputi SYSN flood, teknik-teknik ICMP dan lain-lain. Metode ini merupakan usaha terakhir jika usaha-usaha yang dilakukan di atas mengalami kegagalan.

Dengan menggunakan metode- metode di atas hacker melakukan penyerangan dengan berbagai teknik seperti eksploitasi langsung ke sistem, spoofing (penyamaran), sniffing (capture data) dan social engineering (rekayasa sosial). Lalu apa yang dilakukan Negara untuk mengatasi munclnya cyber crime?

Kepolisnan Negara Republik Indonesia telah membentuk suatu badan yang bernama Cyber Task Force, yang bertugas mengatur segala aspek hukum yang terkait dengan kejahatan-kejahatan yang dilakukan di internet.Yang mana apabila seseorang pelaku kejahatan internet tertangkap, maka selanjutnya akan dilakukan tindakan komputer forensik.

Forensik komputer dapat didefinisikan sebagai ilmu forensik untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer (Noblett).

Definisi dari McKemmish menyebutkan bahwa forensik komputer adalah proses untuk mengidentifikasi, menjaga, menganalisa, dan menyajikan digital evidence (bukti digital) dalam tata cara yang diterima secara hukum. Kedua definisi yang telah disebutkan, berprioritas pada *recovery* dan analisa data.

Bukti Digital (Digital Evidence)

Pada definisi dari McKemmish diperkenalkan istilah *digital evidence* (bukti digital). Bukti digital sangat berkaitan dengan forensik komputer. Istilah bukti digital digunakan untuk menghindari keterbatasan yang ada pada istilah bukti elektronik. Termasuk di dalam bukti digital adalah bukti komputer, *audio digital*, *video digital*, telpon selular, mesin fax dan lain-lain.

Forensik komputer diterapkan pada penanganan kejahatan yang berkaitan dengan teknologi informasi. Forensik komputer dapat dipergunakan untuk menganalisa dan mengamankan bukti digital dan merupakan tata cara yang benar untuk menangani bukti digital. Kesulitan dalam forensik komputer adalah dalam menghadirkan bukti digital yang dapat digunakan dalam persidangan dan besarnya dokumentasi yang diperlukan. Sumber- sumber bukti digital:
1). Komputer desktop, dapat menyimpan data catatan kegiatan pengguna, email, dll, dalam jumlah besar. 2) Server sistem, menyimpan data seperti komputer desktop tetapi untuk semua pengguna, dan file log lainnya. 3) Peralatan komunikasi, router atau modem, yang dapat mengandung IP Address, nomor telpon dan lain-lain. 4) Traffic komunikasi, email, session dalam penjelajahan situs, session dalam transfer file dan lain-lain. 5) *Embedded devices*, sistem komputer kecil yang menjadi bagian dari system yang lebih besar. 6) Telpon bergerak, yang dapat menyimpan data seperti nomor telpon, SMS, call history, gambar, dan video.

Kesulitan- kesulitan yang dihadapi berkaitan dengan bukti digital:
1) Permasalahan kompleksitas, data yang didapatkan biasanya dalam bentuk paling dasar, dan terkadang susah untuk dipahami manusia. 2) Masalah *Quantity*, jumlah data yang harus dianalisa mungkin saja besar. Sangat tidak efisien jika harus menganalisa setiap data. Teknik pengurangan data digunakan untuk memecahkan masalah ini. 3) Bukti digital dapat berubah secara mudah, data komputer dapat berubah setiap saat di dalam computer dan sepanjang jalur transmisi. Data computer dapat diubah dengan mudah tanpa meninggalkan jejak nyata. 4) Permasalahan keberagaman dalam teknologi informasi dan komunikasi, teknologi informasi muncul dalam variasi yang banyak dan terdiri dari bukan hanya peralatan yang dapat dikenali secara mudah seperti computer, tetapi juga peralatan lainnya seperti telpon selular, pager, *organizer*, fax atau mesin penjawab telpon. Begitu juga dengan media penyimpanan yang tidak hanya berupa disket atau CD, tetapi juga flash disk atau SIM card.

Kasus kejahatan komputer sekarang banyak disidangkan. Permasalahan bukti digital bisa jadi sangat kompleks bagi para juri, dan merupakan tugas seorang spesialis forensik komputer untuk membuatnya menjadi lebih sederhana tanpa mengurangi fakta. Biasanya juri yang dihadirkan

mewakili berbagai lapisan masyarakat, sangat kecil kemungkinannya juri terdiri dari para ahli komputer. Maka kompleksitas permasalahan komputer dalam persidangan perlu dijelaskan dalam istilah yang mudah dan dipahami dan jelas. Seringkali kesaksian diberikan dalam beberapa bulan bahkan tahun setelah bukti digital diproses. Dokumentasi yang baik, dan tersusun dalam metode pemrosesan yang diterapkan secara konsisten, bertindak sebagai pengingat bagi spesialis komputer dan dapat menjadi kunci penting dalam kesuksesan atau kegagalan suatu persidangan kejahatan komputer. Hal-hal yang penting untuk didokumentasi:
1) Pengaturan tanggal dan waktu computer, 2) Partisi harddisk, 3) Versi dan Sistem operasi, 4) Integritas sistem operasi dan data, 5) Evaluasi virus computer, 6) Katalog file, 7) Software licensing, 8) Pengambilan software, file input dan file output.

Dokumentasi dari hasil analisis forensik harus lengkap, akurat, dan komprehensif. Untuk siapa dokumentasi atau laporan dibuat juga harus diperhatikan. Dokumentasi dibuat sedetail mungkin untuk menyajikan duplikasi aksi yang lengkap. Tanpa kemampuan untuk rekonstruksi secara akurat terhadap apa yang telah terjadi, bukti penting dapat dipertanyakan. Langkah-langkah analisis dalam dokumentasi harus sesuai dengan pedoman-pedoman yang dipergunakan secara nasional maupun internasional. Sistem dokumentasi dibuat dengan arsitektur yang fleksibel dan mudah dikembangkan.

Empat elemen kunci forensic dalam Teknologi Informasi

1. Identifikasi dari bukti gigital
   Tahap ini merupaka tahap awal forensik dalam teknologi informasi. Dalam tahap ini dilakukan identifikasi di mana bukti itu berada, di simpan, dan bagaimana penyimpanannya. Hal ini dilakukan untuk mempermudah proses atau tahapan berikunya.
2. Penyimpanan bukti digital
   Pada tahapan ini menekankan bahwa bukti digital pada saat ditemukan akan tetap sama baik bentuk, isi, makna, dan hal lainnya dalam jangka waktu yang lama.
3. Analisa bukti digital
   Bukti digital yang di ambil dari tempat asalnya diproses sebelum di limpahkan kepada pihak yang membutuhkan. Skema pemrosesan di sini tergantung pada masing-masing kasus yang di hadapi.
4. Presentasi bukti digital
   Ialah proses persidangan di mana bukti digital akan di uji keasliannya dan hubungannya dengan kasus yang di hadapi. Makna presentasi di sini nerupa penunjukkan bukti digital yang berhubungan dengan kasus yang disidangkan.

Manajemen bukti

Ada dua istilah dalam manajemen barang bukti yang bisa membantu investigator dalam memecahkan suatu kasus, yaitu the chain of custody dan rules of evidence.

a. The Chain of custody

Ialah pemeliharan dengan meminimalisir kerusakkan yang diakibtakan oleh investigasi. Tujuan dari the chain of custody adalah :

1. Menjaga ke aslian bukti
2. Bukti pada saat diserahkan ke persidangan harus sama keadaannya dengan pada saat pertama kali ditemukan.

b. Rules of Evidence

Istilah ini maksudnya ialah bukti harus memiliki korelsi yang nyata dengan kasus yang ada. Dalam Rules of evidence terdapat empat persyaratan yang harus dipenuhi, antara lain :

1. Dapat diterima
   Harus mampu diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai dengan kepentingan pengadilan.
2. Asli
   Bukti yang di dapatkan harus Asli, maksudnya ialah kadar, isi, format bukti pada saat ditemukan sama dengan pada saat diserahkan ke pengadilan. Selain itu bukti juga berkorelasi langusng terhadap kasus yang dihadapi dan bukan hasil rekayasa.

3. Lengkap

   Bukti yang baik adalah bukti yang memiliki petunjuk yang lengkap yang dapat digunakan untuk mempermudah proses penyelidikan.

4. Dapat dipercaya

   Bukti yang ada harus dapat dipercaya agar poin pertama dapat terpenuhi. Sehingga apabila bukti yang ada bisa menggambarkan kejadian yang terjadi dibelakangnya, maka akan sangat membantu dalam proses investigasi.

Metodologi Forensik Teknolgi Informasi

1. **Search & seizure**

   Penyidik dituntut mampu mengidentifikasi, menganalisa, serta memproses bukti yang berupa fisik. Penyidik dalam mengidentifikasi, serta memproses bukti yang berupa fisik diharuskan terjun langsung ke dalam kasus yang di hadapi. Apabila diperlukan penyidik juga berwenang untuk melakukan penyitaan terhadap barang bukti yang dapat membantu proses penyidikan. Penyitaan harus dilakukan sesuai prosedur hukum yang berlaku.

2. **Pencarian Informasi**

   Tahapan pencarian informasi dalam teknologi informasi :

   a. Melakukan penyitaan terhadap hal-hal yang bisa membantu proses penyelidikan, misalnya media penyimpanan (data storage).
   b. Menemukan lokasi tempat kejadian perkara.
   c. Penyidik harus dapat mengolah inforamsi yang terdapat dalam log komputer untuk mengumpulakan bukti-bukti yang akurat.

PEMBAHASAN

Data Recovery

Kapasitas penyimpanan data semakin besar sesuai dengan begitu cepatnya kemajuan teknologi, sehingga memungkinkan oarang menggunakan seluruh ruang hard disk yang ada tanpa melakukan penimpaan data. Jika pun terjadi penimpaan data, biasanya hanya terjadi pada saat melakukan proses format.

Jika sebuah file di hapus, potongan-potongan file tersebut masih tersimpan. Namun potongan-potongan file ini tidak akan bisa ditemukan jika kita mencarinya hanya dengan menggunaka fasilitas searching yang ada pada sistem operasi. Sesungguhnya proses delete data yang sering kita lakukan sebenarnya tidak secara permanent di hapus dari media penyimpanan, tetapi memberitahukan kepada komputer bahwa ruang yang tadinya ditempati data tesebut telah kosong atau siap ditimpa dengan data yang baru. Sehingga file yang kita delete bisa dengan mudah kita kembalikan ke dalam bentuk semula, bila belum ditimpah dengan file yang lainnya dengan menggunakan aplikasi recovery data, misalnya Power Data Recovery.

Dengan semakin berkembangnya sistem enkripsi, seorang penyusup selalu berusaha untuk mendapatkan berbagai informasi, dimanapun dan bagaimanapun bentuk informasi tersebut, bahkan walaupun informasi tersebut sudah dihilangkan. Dengan menggunakan peralatan canggih seperti magnetic force microscopy (MFM) informasi yang berbentuk file yang disimpan pada media magnetic dan telah dihapus serta ditimpa berulang kali dapat diperoleh kembali.

Agar dapat menghapus file dan tidak dapat dikembalikan lagi terutama penghapusan yang aman pada media magnetik, dikenal meetoda lama yang dikenal dengan metoda standar DoD (Department of Defense). Metoda DoD ini adalah dengan menimpa data dengan sebuah pola kemudian ditimpa lagi dengan komplemen pola pertama dan ketiga ditimpa lagi dengan pola lain. Misalnya sebuah data ditimpa oleh pola 1 (satu) semua, kemudian ditimpa oleh komplemennya yaitu 0 (nol) semua dan terakhir dengan pola 10 (satu nol). Tetapi Bruce Schneier menyarankan menghapus file sebanyak tujuh kali. Pertama dengan pola 1 (satu) kemudian dengan pola 0 (nol) sebanyak lima kali dan terakhir dengan pola pseudo-random yang aman secara kriptografi. Tetapi cara ini pun tidak aman setelah dikembangkannya electron-tunneling microscopes.

Cara penghapusan yang aman pada media magnetik adalah seperti yang dikembangkan oleh Peter Gutmann dari Universitas Auckland. Pada metoda ini Peter Gutmann mengembangkan pola tertentu yang disesuaikan dengan cara pengkodean pada harddisk seperti RLL, MFM, dan PRLM.

Konsep dengan cara overwrite ini adalah dengan membalik bidang magnetic pada disk bolak-balik sebanyak mungkin tanpa menulis pola yang sama berturut-turut.

Kaitan dalam komputer forensik

Data recovery merupakan bagian dari analisa forensik di mana hal ini merupakan komponen penting di dalam mengetahui apa yang telah terjadi, rekaman data, korespondensi, dan petunjuk lannya. Banyak orang tidak menggunakan informasi yang berasal dari data recovery karena dianggap tidak murni/asli/orisinil.

Setiap sistem operasi bekerja dalam arah yang unik, berbeda satu sama lain (walaupun berplatform sistem operasi yang sama). Untuk melihat seberapa jauh data sudah dihapus atau belum, perlu memperhatikan segala sesuatu yang ada dalam raw disk. Jika data yang digunakan untuk kejahatan ternyata masih ada, maka cara yang termudah adalah menguji data dengan pemanfaatan tool yang ada pada standar UNIX, seperti strings, grep, text pagers, dan sebagainya. Sayangnya, tools yang ada tidak menunjukkan data tersebut dialokasikan di mana.

Contohnya, intruder menghapus seluruh system log files (dimulai dari bulan, hari, dan waktu) dari minggu pertama Januari, seharusnya ditulis untuk melihat syslog tersebut: Melalui investigasi dari sistem yang dirusak oleh intruder, sistem files UNIX yang modern tidak menyebar contents dari suatu file secara acak dalam disk. Sebagai gantinya, sistem files dapat mencegah fragmentasi file, meskipun setelah digunakan beberapa tahun.

File content dengan sedikit fragmentasi akan lebih mudah untuk proses recover dari pada file content yang menyebar dalam disk (media penyimpanan). Tetapi sistem file yang baik memiliki beberapa keuntungan lain, salah satunya mampu untuk menghapus informasi untuk bertahan lebih lama dari yang diharapkan.

Dalam kasus Linux, sistem file extension tidak akan menghapus lokasi dari urutan pertama 12 blok data yang tersimpan dalam inode jika file sudah dipindah/dihapus. Hal ini berarti menghapus data dapat dikembalikan langsung dengan menggunakan icat dalam inode yang terwakilkan. Seperti metode data recovery lainnya, tidak akan menjamin jika data tetap ada di tempat semula. Jika file dihapus dalam sistem operasi Linux, inode's time akan terupdate. Dengan menggunakan informasi tersebut, data dapat dikembalikan dari 20 inode pada sistem file yang dihapus.

Winhex : Forensic Software

WinHex pada intinya adalah editor hexadecimal universal, yang paling utama adalah sangat membantu dalam bidang computer forensics, data recovery, proses data dalam tingkat yang rendah, dan keamanan IT. Sebuah peralatan yang semakin maju setiap harinya dan penggunaan dalam keadaan darurat : memeriksa dan mengedit semua jenis file mengembalikan data yang telah dihapus atau data yang telah hilang dari hard drives system file yang *corrupt*, atau dari kartu memory digital camera.

Berikut adalah beberapa kelebihan dan cara kerja dari WinHex, antara lain :

1) Disk editor untuk hard disk, floppy disk, CD-ROM & DVD, ZIP, Smart Media, Compact Flash. 2) Dukungan untuk FAT, NTFS, Ext2/3, ReiserFS, Reiser4, UFS, CDFS, UDF, 3) Memiliki interpretasi untuk sistem RAID dan dynamic disks, 4) Berbagai macam teknik pemulihan data, 5)RAM editor, menyediakan akses kepada physical RAM, dan proses–proses yang dimiliki virtual memory, 6) Penerjemah data, mengetauhi 20 jenis type data, 7) Mengedit struktur data menggunakan templates (contoh : untuk memperbaiki tabel partisi / boot sector), 8) Menyatukan dan memisahkan file, menyatukan dan membagi kejanggalan dalam bytes/words, 9) Menganalisa dan membandingkan file – file, 10) Pencarian yang paling flexibel dan mengganti fungsi – fungsi, 11) Disk cloning (undr DOS dengan X-Ways Replica), 12) Mengatur gambar dan mengamankannya (menurut pilihan dikecilkan ukuran filenya atau dipisahkan menjadi dokumen – dokumen sebesar 650 MB), 13) Memprogram interface (API) dan menulis program, 14) Enkripsi AES 256-bit, pengecekan total, CRC32, hashes (MD5, SHA-1), 15) Menghapus file rahasia dengan aman, membesihkan hard drive demi menjaga privacy, 16) Mengimpor semua format clipboard, termasuk ASCII hex, 17) Mengkonversi diantara biner, hex ASCII, Intel hex, dan Motorola S, 18)Setelan karakter : ANSI ASCII, IBM ASCII, EBCDIC, (Unicode). 19) Pergantian jendela yang

cepat. Mencetak. Pembangkit nomor acak, 20) Mendukung file dengan ukuran yang lebih dari 4 GB. Sangat cepat. Mudah digunakan. Pertolongan yang selalu ada setiap saat

X-Ways forensik, edisi forensik dari WinHex, adalah lingkungan computer forensik yang kuat dan mampu dengan sejumlah fitur forensik, menerjemahkannya menjadi perangkat analisis yang kuat : menangkap ruang yang bebas, ruang yang lemah, ruang dalam partisi, dan teks, membuat table yang berisi petunjuk dengan detail yang lengkap dengan segala file yang termasuk dan file yang telah dihapus dan direktori dan bahkan alur data alternative (NTFS), file dengan penomoran yang tertahan, dan banyak lagi. Juga menyediakan sebagai penggambar disk dalam tingkatan rendah dan peralatan cloning yang menciptakan cermin sesungguhnya (termasuk ruang yang lemah) dan membaca sebagian besar format drive dan type media, pendukung – pendukung drive dan file dari ukuran yang pada dasarnya tidak terbatas (bahkan terabytes dari NTFS volumes).

X-Ways forensics dan WinHex pada dasarnya mengartikan dan menunjukan struktur direktori pada FAT, NTFS, Ext2/3, Reiser, CDFS, dan media UDF dan file gambar. Itu menunjukan pemulihan yang aman pada hard disk, memory card, flash disks, floppy disks, ZIP, JAZ, CDs, DVDs, dan banyak lagi. X-Ways forensics dan WinHex menyatukan beberapa mekanisme penyembuhan file yang otomatis dan mengizinkan pemuliha data secara manual. WinHex memberikan kepuasan, pencarian fungsi yang sangat cepat secara simultan yang mungkin anda butuhkan untuk mencari di seluruh media (atau data gambar), termasuk kelemahan, untuk data yang telah dihapus, data yang disembunyikan dan banyak lagi. Melalui akses fisik, hal ini dapat dilakukan meskipun isinya tidak terdeteksi oleh operating system, contohnya yang disebabkan oleh sistem file yang corrupt dan tidak diketahui. Selain fitur-fitu diatas, Winhex juga dapat digunakan untuk:

1. **Drive cloning, drive imaging**
   Membuat suatu duplikasi yang bisa menghemat waktu dalam menginstall suatu dan software lainnya untuk beberapa komputer yang sejenis atau agar memungkinkan kita untuk memperbaiki suatu installasi yang sedang dilakukan apabila ada data yang rusak.
2. **RAM editor**
   Untuk menjalankan/memanipulasi program yang sedang berjalan dan dalam permainan komputer khusus.
3. **Analyzing files**
   Untuk menentukan jenis recoveri data sebagai bagian rantai yang hilang oleh ScanDisk atau ChkDisk
4. **Wiping confidential files or disks**
   Dengan menghapus file rahasia dengan winhex maka tidak satupun dari komputer yang ada bahkan spesialis komputer forensik sekalipun tidak akan bisa mendapatkan file itu lagi.
5. **Wiping unused space and slack space**
   Dengan menghapus ruang kosong yang tidak terpakai maka akan meminimalkan ukuran backup datanya. Pada drive berjenis NTFS, winhex dapat membersihkan semua file $Mft (Master File Table) yang tidak terpakai.
6. **ASCII - EBCDIC conversion**
   Memungkinkan kita untuk bisa merubah kode ASCII ke EBCDIC
7. **Binary, Hex ASCII, Intel Hex, and Motorola S conversion**
   Digunakan oleh programmer yang menggunakan (E)PROM
8. **Unifying and dividing odd and even bytes/words**
   Digunakan oleh programmer yang menggunakan (E)PROM
9. **Conveniently editing data structure**
   Kita bisa merubah struktur data yang ada dengan baik sesuai dengan apa yang kita inginkan.
10. **Splitting files that do not fit on a disk**
    Kita bisa menggabungkan atau membagi file yang tidak muat di disk kita
11. **WinHex as a reconnaissance and learning tool**
    Kita bisa menemukan program-program lain yang disimpan pada suatu file. Kita juga bisa mempelajari file-file yang formatnya tidak kita ketahui dan bagaimana file tersebut bekerja.
12. **Finding interesting values (e.g. the number of lives, ammunition, etc.) in saved game files**
    Menggunakan penggabungan antara pencarian atau menggunakan perbandingan file

13. **Manipulating saved game files**
    Untuk permainan di komputer, kita bisa mengikuti cheat-nya yang ada di internet atau kita bisa membuat cheat sendiri.
14. **Upgrading MP3 jukeboxes and Microsoft Xbox with larger hard drive**
    Untuk meng-upgrade, hard disk baru memerlukan persiapan dan disinilah winhex dipergunakan
15. **Manipulating text**
    Untuk mengubah text di sebuah file berupa binary yang di aplikasi tersebut tidak diizinkan untuk bisa merubahnya.
16. **Viewing and manipulating files that usually cannot be edited**
    Untuk mengubah file yang tidak bisa diubah karena dilindungi oleh windows
17. **Viewing, editing, and repairing sistem areas**
    Seperti master boot record dengan table pembagiannya dan boot sector.
18. **Hiding data or discovering hidden data**
    Winhex secara khusus memungkinkan kita menggunakan bagian yang kelebihan dan tidak digunakan oleh sistem operasi
19. **Copy & Paste**
    Kita dimungkinkan untuk secara bebas untuk mengkopi dari disk dan menuliskannya ke dalam clipboard di disk tanpa perlu melihat batasan bagian/sektor nya
20. **Unlimited Undo**
    Kita bisa mengulang apa yang telah kita ubah atau kerjakan dengan bebas tanpa batasan.
21. **Jump back and forward**
    Winhex menyimpan sejarah/history apa yang telah kita kerjakan sehingga kita bisa kembali ke sebelum atau ke tahap apa yang kita telah kerjakan dengan mudah seperti pada web browser.
22. **Scripting**
    Pengubahan file otomatis menggunakan script. Script bisa dijalankan dari start center atau awal perintahnya. Ketika script dijalankan kita bisa membatalkannya dengan menekan esc.
23. **API (Application Programming Interface)**
    Pengguna yang professional (programer) akan memanfaatkan kemampuan winhex dalam program buatan mereka.
24. **Data recovery**
    Bisa digunakan pada semua file sistem dan bisa memperbaiki beberapa jenis file pada satu waktu seperti file jpg, png, gif, tif, bmp, dwg, psd, rtf, xml, html, eml, dbx, xls/doc, mdb, wpd, eps/ps, pdf, qdf, pwl, zip, rar, wav, avi, ram, rm, mpg, mpg, mov, asf, mid.
25. **Komputer examination / forensiks**
    Winhex adalah sebuah alat atau software yang sangat berharga bagi seorang spesialis investigasi komputer di sebuah perusahaan pribadi dan untuk penegakkan hukum.
26. **Trusted download**
    Dengan winhex apa yang kita download akan lebih aman dan dapat dipercaya kebersihannya dari hal-hal yang dapat mengganggu komputer kita
27. **128-bit encryption**
    Dengan winhex kita bisa membuat file kita tidak bisa dibaca oleh orang lain.
28. **Checksum/digest calculation**
    Untuk memastikan file yang ada tidak ada yang rusak dan tidak terubah, atau untuk mengenali file-file yang dikenal.
29. **Generating pseudo-random data**
    Digunakan untuk beberapa tujuan seperti simulasi ilmiah.

SIMPULAN

Jaringan dan internet di Indonesia masih membutuhkan perhatian yang lebih, karena beberapa kasus masih merajarela hingga saat ini. Integritas kaum hacker, cracker, dan script kiddies masih terjalin dan akan terus hidup di bawah tanah, sejauh kita tidak bisa memantau dan mencegahnya, kejahatan terhadap internet dan jaringan di Indonesia masih akan berlanjut.

Akankah kita membiarkan bangsa kita tetap menjadi momok yang menakutkan bagi bangsa lain, sehingga mereka menutup akses terhadap internet kita? Tentunya hal ini sangat jauh dari yang kita harapkan. Memajukan bangsa ini merupakan tugas dan kewajiban yang harus dibayar sebagai pemuda bangsa.

Dengan demikian sangat jelas bahwa negeri ini sangat membutuhkan keamanan terhadap jaringan dan internet, apalagi dengan berkembangnya internet hingga mencapai instansi pemerintahan dan perbankan, bahkan telah mencapai tingkat pendidikan. Maka sangat diharapkan adanya partisipasi dari pihak muda-mudi serta para masyarakat IT untuk ikut mengamankan dan menjaga otoritas jaringan dan internet di Indonesia, serta menghidupkan kembali citra Indonesia.

Dalam forensik komputer, Metode yang banyak digunakan adalah search, seizure dan pencarian informasi. Search dan seizure merupakan metode yang paling banyak digunakan, sedangkan pencarian informasi (information search) sebagai pelengkap data bukti tersebut.

Jika dilihat dari sisi software maupun hardware dalam forensik ini lebih mencerminkan bahwa kedua komponen komputer itu memang tidak dapat dipisahkan, karena adanya saling ketergantungan satu sama lain. Dalam menginvestigasi suatu kasus, digunakan tools untuk menganalisa computer baik secara software maupun hardware.

Forensik komputer adalah bidang baru di Indonesia, di mana keberadaan forensik ini sangat dibutuhkan untuk memecahkan kasus tertentu. Jika lebih dikembangkan, maka forensik akan menjadi cabang keamanan dari komputer/jaringan dan bagian yang tidak terpisahkan dalam Lab kriminalitas Mabes Polri.

DAFTAR RUJUKAN

Ruslim, Harianto, *Hack Attack*, Jasakom, 2007

Thomas, Tom, *Network Security First step*. Penerbit Andi, Yogyakarta, 2005

Thomas, Tom, *Computer Networking First-step, Computer Networking First-step*. Penerbit Andi, Yogyakarta. 2005

http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/129/129P-09-inal1.0-laws_investigation_ethic.pdf

http://azamul.files.wordpress.com/2009/06/thesis-cybercrime-di-indonesia.pdf

http://budi.insan.co.id/courses/el7010/2003/rahmadi-report.pdf

http://azamul.files.wordpress.com/2007/06/thesis-cybercrime-di-indonesia.pdf

]http://www.badilag.net/data/ARTIKEL/PENANGGULANGANKEJAHATAN HACKING.pdf