ENSIKLOPEDIA

KANDUNGAN NUTRISI BAHAN MAKANAN

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika

Oleh

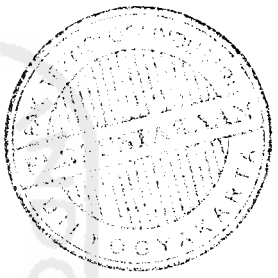
Nama : Tangguh Widiasto
No. Mahasiswa : 03 523 116

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2007

Komputasi Forensik Sebagai Metode Investigasi Cybercrime

TUGAS AKHIR

Diajukan sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika



oleh :

Nama : Dedy Setyo Afrianto
No. Mahasiswa : 02 523 229

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2007

LEMBAR PENGESAHAN PEMBIMBING

ENSIKLOPEDIA

KANDUNGAN NUTRISI BAHAN MAKANAN

TUGAS AKHIR

Oleh :

Nama : Tangguh Widiasto
No. Mahasiswa : 03 523 116

Yogyakarta, 7 Desember 2007

Pembimbing

Sri Kusumadewi S.SI, MT.

LEMBAR PENGESAHAN PEMBIMBING

Komputasi Forensik Sebagai Metode Investigasi Cybercrime

TUGAS AKHIR

oleh :

Nama : Dedy Setyo Afrianto
No. Mahasiswa : 02 523 229

Yogyakarta, 30 Januari 2007

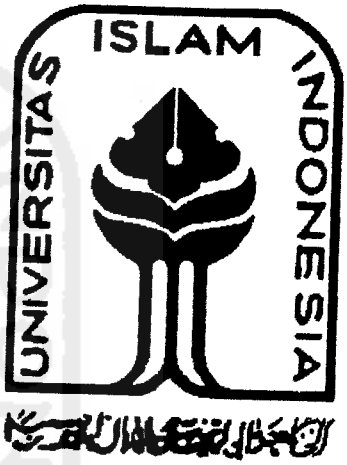
Pembimbing ,

Yudi Prayudi, S.Si, M.Kom

LAPORAN PROJECT PERTAMA

TUGAS AKHIR NON SKRIPSI

Komputer Forensik dan Sistem Keamanan Komputer



DISUSUN OLEH :

Dedy Setyo Afrianto.
02.523.229

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

November 2006

Rangkaian kata inspirasi

"yaa Robbi, jadikanlah hamba paham dan ridho terhadap apa-apa yang tlah Engkau tetapkan dan jadikan barokah apa-apa yang telah Engkau takdirkan, sehingga tidak ingin hamba menyegerakan apa-apa yang engkau tunda dan menunda apa-apa yang Engkau segerakan, Amiin;"

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji Syukur kita panjatkan kehadirat Allah SWT, yang telah memberikan hidayah dan karunia-Nya sehingga dalam kelanjutan nafas ini, kami dapat mengakhiri penyusunan Tugas Akhir selama kurang lebih tiga bulan ini, tak lupa shalawat serta salam kita haturkan kepada junjungan kita Nabi besar Muhammad SAW serta keluarga, sahabat dan pengikutnya sampai akhir zaman.

Tujuan penulisan laporan Tugas Akhir ini pertama adalah sebagai salah satu prasyarat untuk memperoleh Gelar Sarjana di Jurusan Teknik Informatika UII, kedua, sebagai media dokumentasi keilmuan sehingga dapat menjadi salahsatu referensi untuk pembuatan hal yang sama bahkan pengembangan studi ilmu terkait dalam masa-masa mendatang.

Dalam penyusunan ini kami mendapatkan banyak bantuan dari berbagai pihak, baik berupa materi maupun non materi, sehingga dapat terselesaikan dengan baik dan tanpa kendala berarti. Oleh karena itu pada kesempatan ini saya ingin menyampaikan terima kasih dan penghargaan yang setinggi-tingginya kepada :

1. Bapak Fathul Wahid, S.T, M.Sc selaku Dekan Fakultas Teknologi Industri.
2. Bapak Yudi Prayudi S.Si, M.Kom selaku Dosen Pembimbing Tugas Akhir dan Ketua Jurusan Teknik Informatika UII.
3. Ustadz Thulus Mustofa Lc, MA selaku pengasuh Pesantren Mahasiswa Daaru Hiraa' yang selama ini mengayomi dan membimbing.
4. Keluarga tercinta, atas bimbingan dan bekal yang diberikan dalam melangkah.
5. Sahabat – sahabatku di manapun berada, Keluarga Besar Pesantren Mahasiswa Daaru Hiraa' (khususon akhi al-matpy yang minjemin laptopnya dan temen

Komputer Forensik dan Sistem Keamanan Komputer

Project Pertama Tugas Akhir Non Skripsi
Oleh : Dedy Setyo Afrianto (02 523 229)
Jurusan Teknik Informatika, Fakultas Teknologi Industri
Universitas Islam Indonesia
E-mail : dedysetyoa@students.fti.uii.ac.id

Abstraksi

Perkembangan teknologi berangsur-angsur juga telah menambah fenomena-fenomena baru dalam dunia Teknologi Informasi. Beberapa dekade terakhir menunjukan permasalahan Security(Keamanan) mendapatkan perhatian besar baik oleh pengamat maupun praktisi Teknologi Informasi. Semakin besar motif yang digunakan dalam melakukan tindak kejahatan komputer, maka semakin canggih pula perangkat maupun teknik yang digunakan oleh "si penjahat teknologi". Hal inilah yang melatarbelakangi timbulnya disiplin keilmuan baru dalam bidang komputerisasi, khususnya dalam bidang security, yakni ***Komputer Forensik****. Paper ini akan berusaha menunjukan kenapa cabang ini menjadi begitu vital dalam peranannya mengusut tindak kejahatan Komputer.*

Kata kunci : Keamanan komputer, security, forensik, cyber crime

1. Pendahuluan

Fenomena tentang sistem sekuriti komputer merupakan hal yang menarik untuk disimak, perkembangan dunia IT 'melompat' lebih jauh setelah diketemukannya teknologi yang menghubungkan antar komputer (Networking) sampai pada yang paling *revolusioner* dengan dikenalkannya teknologi *Internet* yang seakan-akan membuat dunia tanpa sekat, baik itu waktu maupun tempat pada sekitar dekade 1970-an. Namun, semakin maju perkembangan pada dimensi teknologi ini, semakin maju pula tindak kejahatan yang dengan modus baru dengan memainkan peranan komputer. Istilah ini populer disebut dengan *cybercrime*.

Banyak permasalahan pelik yang kemudian diakibatkan oleh adanya kecenderungan negatif pada sisi ini. Mulai dari imbas yang masih dikategorikan *mikro* karena hanya berefek pada tingkatan personal/perseorangan, sampai kepada persoalan *makro* yang memang sudah pada wilayah komunal, publik, serta memiliki *efek domino* kemana-mana. Untuk negara yang sudah maju dalam IT-nya, pemerintahan setempat atau Profesional swasta bahkan telah membentuk polisi khusus penindak kejahatan yang spesifik menangani permasalahan-permasalahan ini. Polisi cybercrime inilah yang diberikan tugas untuk menindak pelaku-pelaku kriminalitas di dunia cyber, yang tentu saja agak sedikit berbeda dengan polisi 'konvensional', para petugas ini memiliki kemampuan dan perangkat khusus dalam bidang komputerisasi.

1.1 Kasus Cyber crime

Cybercrime, menjadi istilah yang begitu menarik untuk disimak. Kondisi ini nyata adanya. Professional IT, praktisi, pegawai kantoran, administrator jaringan dan siapapun sebagainya yang terlibat *intensif* dengan dunia IT menjadi *"phobia"*

2. Tentang Komputer Forensik

Seperti umumnya ilmu pengetahuan forensik lain, komputer forensik juga melibatkan penggunaan teknologi yang rumit, perkakas dan memeriksa prosedur harus diikuti untuk menjamin ketelitian dari pemeliharaan bukti dan ketelitian hasil mengenai bukti komputer memproses. Pada dasarnya mirip dengan proses yang terjadi pada polisi yang hendak mengusut bukti tindak kejahatan dengan menelusuri fakta-fakta yang ada, namun disini terjadi pada dunia maya. Tapi, secara definitif, apa sebenarnya yang dimaksud dengan Komputer Forensik ?. Pada bab ini akan dibahas lebih lanjut tentang pertanyaan ini.

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 menjadi ambigu. *US Federal Rules of Evidence* 1976 menyatakan permasalahan tersebut sebagai masalah yang rumit. Hukum lainnya yang berkaitan dengan kejahatan komputer:

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

Pada akhirnya, jika ingin menyelesaikan suatu "misteri komputer" secara efektif, diperlukan pengujian sistem sebagai seorang detektif, bukan sebagai user. Sifat alami dari teknologi Internet memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya. Kejahatan komputer tidak memiliki batas geografis. Kejahatan bisa dilakukan dari jarak dekat, atau berjarak ribuan kilometer jauhnya dengan hasil yang serupa. Bagaimanapun pada saat yang sama, teknologi memungkinkan menyingkap siapa dan bagaimana itu dilakukan. Dalam komputer forensik, sesuatu tidak selalu seperti kelihatannya. Penjahat biasanya selangkah lebih maju dari penegak hukum, dalam melindungi diri dan menghancurkan barang bukti. Merupakan tugas ahli komputer forensik untuk menegakkan hukum dengan mengamankan barang bukti, rekonstruksi kejahatan, dan menjamin jika bukti yang dikumpulkan itu berguna di persidangan.

2.2 Landasan Teori

Secara *Terminologi*, Komputer Forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, [pengambilan/penyaringan], dan dokumentasi bukti komputer dalam kejahatan komputer[3]. Istilah ini relatif baru dalam sektor privat beberapa dekade ini, tapi telah muncul diluar *term* teknologi (berhubungan dengan investigasi dan investigasi bukti-bukti intelejen dalam penegakan hukum dan militer) sejak pertengahan tahun 1980-an.

[3] Marcella, A J dan Greenfield, R S(Editors), "*CYBER FORENSICS a field manual for collecting, examining, and preserving evidence of computer crimes*". USA: CRC Press LLC, 2002

2.3 **Standar Metodologi**

Seorang Pakar teknologi *David Morrow* mengungkapkan bahwasanya rencana adalah faktor yang mutlak untuk diperhatikan, sehingga ketika rencana ini belum terumuskan dengan baik, sebaiknya penyelidikan jangan dimulai[4]. Seperti ungkapan ini, sebenarnya landasan metodologi berfungsi memetakan konstruksi ilmiah dalam menyelesaikan pekerjaan. Walaupun sebenarnya tidak ada patron baku dalam hal ini, tapi harapannya sebuah pekerjaan akan terarah dan memperoleh hasil yang dituju. Dengan demikian, langkah-langkah seperti apakah yang sebaiknya digunakan untuk menentukan metodologi.

2.3.1 Menentukan tujuan (Goal) dalam pengungkapan.

Tujuan diperlukan sebagai pengarah dimana nanti investigasi akan berakhir, selain itu didalam *goal* akan terdapat parameter-parameter kesuksesan dalam meng-*investigasi* kejadian. Sehingga *ending* dapat ditentukan kapan dan hasil apa yang diperoleh.

2.3.2 Memproses fakta (Data dan informasi) yang ada

Bukti digital (Digital Evidence) merupakan salahsatu perangkat vital dalam mengungkap tindak cybercrime. Dengan mendapatkan bukti-bukti yang memadai dalam sebuah tindak kejahatan, seseorang sebenarnya telah mengungkap separuh kebenaran. Tinggal bagaimana kemudian *memfollow-upi* bukti-bukti tadi dengan langkah yang tepat.

Bukti Digital yang dimaksud adalah :

- E-mail / alamat e-mail
- Wordprocessors, spreadsheet files
- Sourcecode dari perangkat lunak
- Image
- Web browser, bookmark, cookies
- Kalender

Bukti-bukti diatas masih dimungkinkan belum mencakup keseluruhan dari bukti-bukti empirik yang sering digunakan[5].

2.3.3 **Elemen Kunci Forensik**

Empat **Elemen Kunci Forensik**[6] yang juga harus diperhatikan berkenaan dengan bukti digital dalam Teknologi Informasi, adalah sebagai berikut:

2.3.3.1 **Identifikasi dalam bukti digital *(Identification/Collecting Digital Evidence)***

---

[4] Utdirartatmo, Firrar, "*Tinjauan Analisis Forensik dan Kontribusinya pada Keamanan Sistem Komputer*", Bandung : INSTITUT TEKNOLOGI BANDUNG, 2001.

[5] *Scientific working Group on Digital Evidence, 1999*

[6] Littlejohn Shinder, Debra, dan Ed Tittel (Editor), "*SCENE of CYBERCRIME computer forensic hand book*". Unknown City: Syngress Publishing,Inc, 2002

Analisis kemungkinan juga dapat diperoleh dari motif/latar belakang yang ada sebelum didapatkan kesimpulan. Seperti dijelaskan pada bab-bab sebelumnya (Bab 1.1 **Kasus Cybercrime**), bahwasanya motif yang beragam inilah seringkali memaparkan fakta-fakta yang berkorelasi dengan kenyataan peristiwa, bahwa setiap **sebab** akan menghasilkan **akibat** yang relatif seragam.

2.3.3.4 **Presentasi bukti digital *(Presentation of Digital Evidence)***

Kesimpulan akan didapatkan ketika semua tahapan tadi telah dilalui, terlepas dari ukuran *obyektifitas* yang didapatkan, atau standar kebenaran yang diperoleh, minimal bahan-bahan inilah nanti yang akan dijadikan "modal" untuk ke pengadilan.

Proses digital dimana bukti digital akan dipersidangkan, diuji otentifikasi dan dikorelasikan dengan kasus yang ada. Pada tahapan ini menjadi penting, karena disinilah proses-proses yang telah dilakukan sebelumnya akan diurai kebenarannya serta dibuktikan kepada hakim untuk mengungkap data dan informasi kejadian.

Pada tahapan *final* ini ada beberapa hal yang mutlak diperhatikan, karena memang pada level ini ukuran kebenaran akan ditetapkan oleh pengadilan sebagai pemilik otoritas. Hal-hal yang dimaksud adalah :
- Cara Presentasi
- Keahlian Presentasi
- Kualifikasi Presenter
- Kredibilitas setiap tahapan pengusutan

3. Kejahatan Komputer

Tidak seperti kejahatan konvensional pada umumnya, kejahatan komputer memiliki beragam variasi sesuai dengan keahlian dan motif "si penjahat komputer", semakin besar motif yang melatarbelakangi maka akan semakin canggih pula modus operandi yang digunakan. Seiring dengan perkembangan kecanggihan sistem keamanan komputer biasanya selalu didahului oleh varian kejahatan komputer yang selangkah lebih maju, atau dengan bahasa yang sederhana, sebenarnya upaya keamanan komputer secanggih apapun, akan selalu ada *hole* (lubang/celah) yang dapat dimanfaatkan oleh penjahat ini.

3.1 **Mengidentifikasi dan Mengkategorikan Tipe Serangan**

Pada dasarnya untuk melakukan hal ini, lebih melihat kepada bagaimana cara "penyerang" untuk masuk kepada celah komputer kita. Serta yang lebih penting lagi, upaya ini adalah penting untuk mengatasi serangan-serangan sehingga diharapkan dapat lebih efektif dan effisiennya cara yang digunakan. Pengidentifikasian dan pengkategorian yang dimaksud adalah[9] :

- ✓ Aktivitas pra-serangan
- ✓ Metode cracking Password
- ✓ Teknik Exploit (Mengambil Keuntungan dari karakteristik Sistem Operasi atau protokol)
- ✓ Serangan Virus, Trojan, Worms

Selanjutnya akan dipaparkan secara umum masing-masing dari karakteristik diatas

3.1.1 **Aktivitas pra-serangan**

Pada step ini, biasanya lebih dimanfaatkan untuk mencari informasi terkait dengan target. Hacker yang berpengalaman akan "menginstruksikan" newbie tentang sesuatu dengan berbagai dalih dengan harapan akan memperoleh informasi terkait dengan targetan-targetan hacker. Langkah yang umum dilakukan adalah

1. Pre-attack (Pendahuluan/prolog)
2. Initial access (Inisialisasi akses)
3. Full system access (Akses sistem secara penuh)
4. Planting "back doors" for future access (Mempersiapkan "pintu belakang" untuk kabur)
5. Covering tracks (Menutup jalur)

3.1.2 **Metode cracking password**

Pada tahapan ini, password menjadi hal yang paling vital untuk aktivitas apapun. Dengan mengetahui password target, maka sebenarnya klimaks dalam pencarian pintu masuk telah dilalui. Beberapa manfaat dari penggunaan password adalah :

- Masuk dalam komputer lokal atau jaringan
- Mengakses proteksi website atau FTP.
- Mengakses e-mail.
- Mengakses dokument.

[9] Littlejohn Shinder, Debra, dan Ed Tittel (Editor), "*SCENE of CYBERCRIME computer forensic hand book*". Unknown City: Syngress Publishing,Inc, 2002

5. Glossary

- Cybercrime : Perkara kriminalitas dalam dunia cyber (komputerisasi)
- Revolusioner : Perubahan secara menyeluruh dengan waktu yang singkat
- makro : Cakupan yang luas
- Domino : Berantai, berimbas ke yang lain (kiasan)
- Konvensional : Pola lama
- Phobia : Ketakutan (berlebih)
- Kompetitor : Pesaing
- Market : Pasaran (bisnis)
- Nasionalisme : Sikap/paham mencintai bangsa dan negara sendiri
- Stealth Bomber ; Pesawat pengebom canggih dari AS yang telah berteknologi mutakhir
- Terminologi : Pengertian secara luas
- Otoritas : Hak/wewenang
- Preview : Tampilan singkat
- Searching : Pencarian
- analyzing : Penganalisaan
- space storage : Sisa Ruang (untuk penyimpan digital, seperti Hardisk, CD dll)
- Obyektifitas : Sudut pandang pendapat dengan melihat secara nyata, dari luar, sesuai adanya
- Kredibilitas : Kepemilikan kewibawaan
- FTP : fasilitas untuk meng-upload (mentransfer ke-) secara digital
- BIOS : Fitur dari Motherboard untuk menyimpan informasi dari pabrik
- Oase : mata air di gurun pasir (kiasan)
- Preventif : Pencegahan
- Controller : Pengontrolan/pengendalian

6. Daftar Pustaka

[LIT02] Littlejohn Shinder, Debra, dan Ed Tittel (Editor), *"SCENE of CYBERCRIME computer forensic hand book"*. Unknown City: *Syngress Publishing,Inc,* 2002

[MCK99] Mc Kemmish, Rodney, *"What is forensic computer"*. Australia: Australian institute of Criminology, 1999. http://www.aic.gov.au/publications/tandi/ti118.pdf

[HAC04] Film dokumenter *"Hackers: Outlaws and Angels"*, Discovery Chanel, Februari 2004.

[MAR02] Marcella, A J dan Greenfield, R S(Editors), *"CYBER FORENSICS a field manual for collecting, examining, and preserving evidence of computer crimes"*. USA: CRC Press LLC, 2002

[WRI01] Wright, Mal, *"Investigating an Internal Case of Internet Abuse"*. USA: SANS Institute, 2001.

[UTD01] Utdirartatmo, Firrar, *"Tinjauan Analisis Forensik dan Kontribusinya pada Keamanan Sistem Komputer"*, Bandung : INSTITUT TEKNOLOGI BANDUNG, 2001.

[BUD03] Budiman, Rahmadi, *"Tugas Keamanan Sistem Lanjut, Komputer Forensik Apa dan Bagaimana?"*, Bandung : MAGISTER TEKNIK ELEKTRO OPTION TEKNOLOGI INFORMASI, INSTITUT TEKNOLOGI BANDUNG, 2003

[TEC05] situs www.techpathways.com, diakses pada november 2005

[FOR06] situs www.forensics-intl.com/def2.html, diakses pada november 2005

LAPORAN PROJECT KEDUA

TUGAS AKHIR NON SKRIPSI

Review dan Implementasi Software Forensic

DISUSUN OLEH :

Dedy Setyo Afrianto.
02.523.229

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

Desember 2006

Mengkhususkan peranan softwarenya pada pemantauan aktivitas yang terjadi seperti layaknya kamera yang mengintai di depan monitor. Aktivitas pengintaian yang terjadi pun terus menerus berjalan selama komputer hidup dan bekerja pada *background.*

- STANDAR HARDWARE PC :

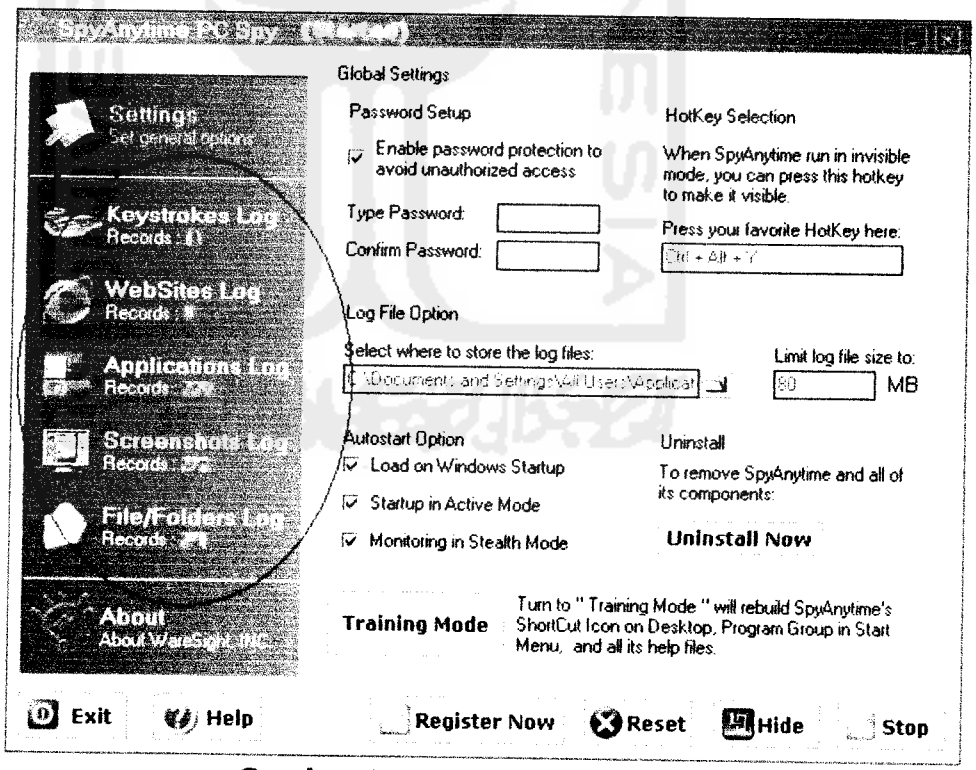
CPU: Pentium Class PC (133 MHz atau lebih tinggi0)
RAM: 32 MB
Disk Space: 3 MB harddisk kosong, 20 MB untuk log files
Video: 800x600, 256 colors
OS: Windows 95/98/ME/NT/2000/XP

- FITUR :

Secara garis besar terbagi atas dua bagian

1. Memantau aktivitas Monitor, meliputi
   a. Keystrokes Monitoring (Melihat tombol keyboard yang ditekan)
   b. WebSites Monitoring (Melihat Halaman URL yang diakses)
   c. Applications Monitoring (Melihat aplikasi yang dijalankan)
   d. Screen Shot Logging (Menangkap gambar)
   e. File/Folders Monitoring (Melihat File/folder yang dijalankan)

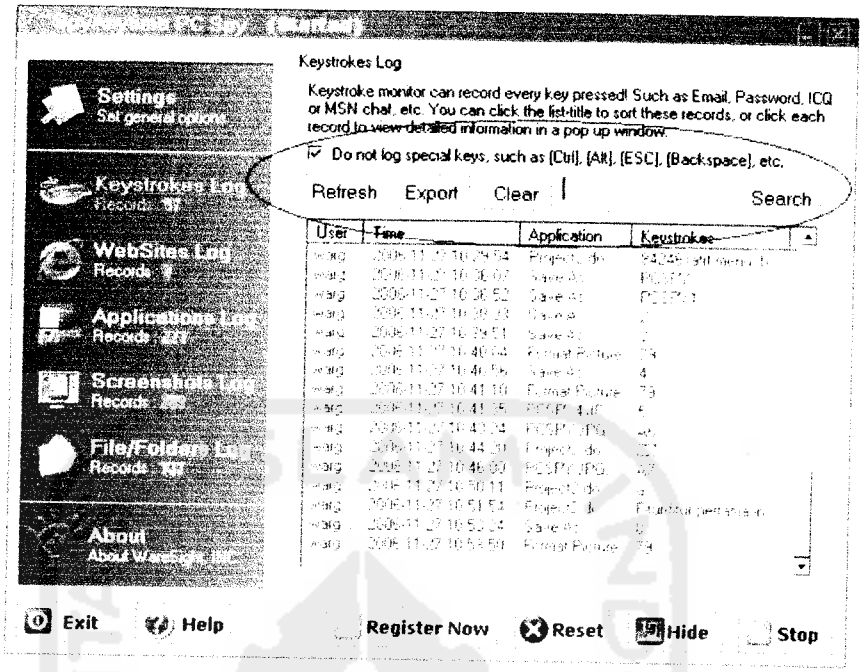
Fitur-fitur pertama ini secara keseluruhan terlketak pada lajur kiri tampilan, dengan posisi seperti dibawah ini.



Gambar 1 Fitur Pertama PC SPY

2. Memantau Logs, meliputi
   a. Refresh Log (memperbaharui Log yang terekam)
   b. Export Log (Mengubah format ekstensi Log)

c. Clear Log (Membersihkan Log)
d. Search Log (Mencari Log)
e. View Screenshot picture (Melihat screenshot gambar aktivitas)



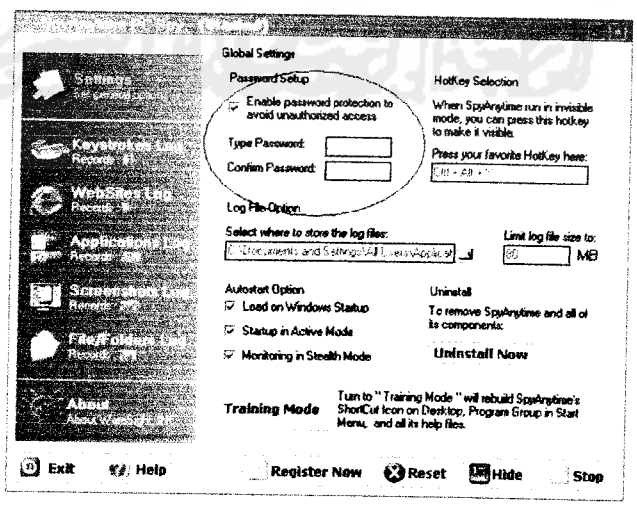
Gambar 2 Memantau Logs

- Setting tambahan

Ada beberapa fitur tambahan yang disediakan dalam mengakses software ini. *Control Panel* merupakan button untuk mengkonfigurasi untuk kemudahan user dalam penggunaan.

- Password Setup

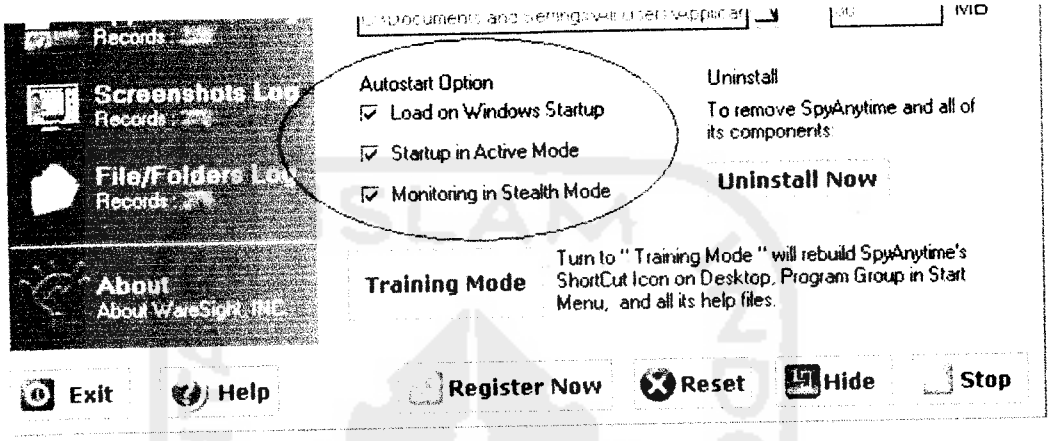
Digunakan untuk mengeset password yang dipakai sebagai piranti security untuk user yang mencegah user yang tidak memiliki hak pakai software.



Gambar 3 Setting Password

- Autostart option

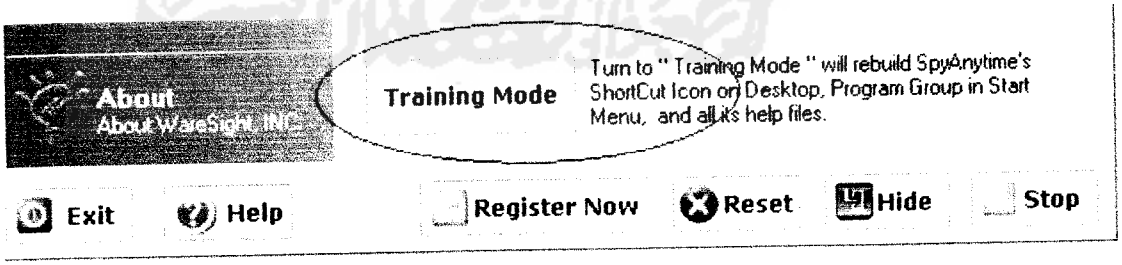
Spyanytime dapat dikonfigurasi dalam tiga varian. *Pertama*, Load on Windows Startup, Spyanytime akan otomatis berjalan ketika komputer hidup. *Kedua*, Startup in Active Mode, Spyanytime akan diberjalan ketika tombol eksekusi ditekan. Ketiga, Monitoring in Stealth Mode, pada varian ini program akan sepenuhnya *invisible* (tidak nampak) ketika berjalan, tidak nampak dalam windows taskbar atau dalam Apllication List Windows. Untuk menampakkan dapat menggunakan Hotkey selection (***default***:Ctrl+Alt+Y).



Gambar 6 Autostart Option

- Skilled Mode and Training Mode

Terdapat dua mode dalam penggunaan. *Pertama*, Skilled Mode, pada option ini, Spyanytime dapat diseting dengan menghilangkan icon pada desktop, start menu, bahakan akan menghilangkan help file. Untuk memanggil program dapat mengetikkan "sa2" pada menu **Run** (START → RUN → *ketikkan* sa2 → Enter) atau dengan menggunakan Hotkey. *Kedua*, Training Mode, pada option ini akan mengembalikan seperti semula setingan yang sebelumnya hilang



Gambar 7 Training Mode

- **Tampilan Output**

Dibawah ini akan dipaparkan tampilan output dari bukti-bukti yang berhasil ditangkap oleh PC spy. Masing-masing akan ditampilkan *data-data bukti* dari fitur software.

dengan aktivitas negatif ini. Kasus yang terjadipun menunjukan bahwa perkara ini tidak main-main, berbagai laporan menunjukan bahwa kejahatan komputer telah menyedot perhatian banyak pihak yang terkait dengan masalah ini, contoh laporan yang ada diantaranya

- 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 penuh dapat download di PDF format pada *(www1.ifccfbi.gov/strategy/IFCC_Annual_Report.pdf.)*
- Menurut Survey Institute Keamanan Komputer Computer pada 2001, bersama dengan Squad Penggangguan 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).*
- Menurut Cybersnitch Voluntary Online Crime melaporkan Sistem Kejahatan Relasi-Internet mencakup dari pemalsuan desktop ke pornografi anak dan meliputi kejahatan yang kejam seperti pencurian elektronik dan teroris threats.(daftar dilaporkan cybercrimes tersedia pada *www.cybersnitch.net/csinfo/csdatabase.asp.*)

Dan masih banyak laporan-laporan tragis yang menunjukan betapa bahayanya aktivitas kriminal ini. Untuk beberapa tahun kedepan, ketika aktivitas IT masyarakat meningkat, akan lebih menambah potensi yang terjadi dalam dunia kriminalitas ini[1].

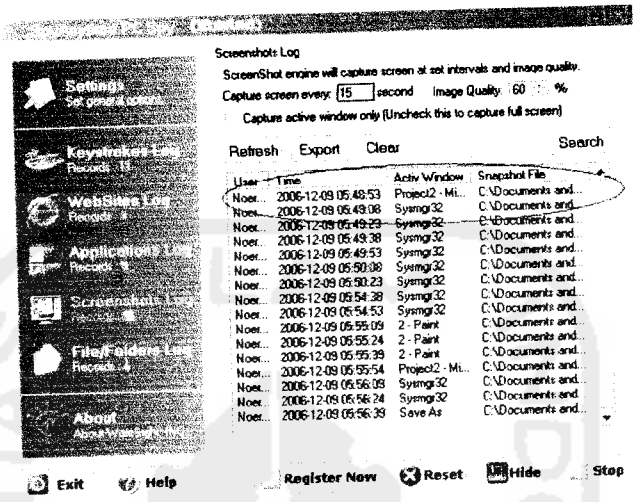
Telah banyak penelitian yang menyebutkan bahwasanya berbagai gejala fenomena kriminalitas dunia maya dilakukan oleh subyek yang tentusaja sarat *tendensi* (kepentingan), berbagai kecenderungan kepentingan yang ada antara lain; 1.)Permasalahan finansial yang dianggap bahwasanya *cybercrime* adalah alternatif baru untuk mendapatkan kucuran uang. Kecenderungan ini benar adanya, 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*, serta masih banyak contoh problem ekonomi yang melatar belakangi perilaku ini. 2.)Adanya permasalahan dalam tingkatan kenegaraan yang menyangkut persoalan politik, militer dan sentimen *Nasionalisme*. Sebuah kasus nyata pernah terjadi pada awal tahun 1990, yakni Pesawat pengebom paling Rahasia Amerika, *Stealth Bomber* dijadikan objek serangan oleh hacker-hacker, diindikasikan memang sangat *secret*-nya spesifikasi khusus pesawat ini. Lagipula memang permasalahan peralatan militer yang berteknologi tinggi menjadikan sebuah kajian menarik dalam kompetisi antar negara dalam mengembangkan peralatan tempurnya. 3.)Faktor kepuasan pelaku, dalam hal ini tentusaja permasalahan psikologis menjadi sebuah pertanyaan besar. Banyak kecenderungan menyebutkan bahwasanya seseorang dengan skill tinggi dalam bidang penyusupan keamanan akan selalu tertantang dengan "rute-rute" baru yang sedikit berliku. Bahkan kepuasan batin lebih menjadi orientasi utama untuk hacker yang lebih memiliki skill tinggi daripada segepok uang, menurut paparan salah seorang Hacker senior di negeri Paman Sam[2].

[1] Littlejohn Shinder, Debra, dan Ed Tittel (Editor), "*SCENE of CYBERCRIME computer forensic hand book*". Unknown City: Syngress Publishing,Inc, 2002

[2] Film dokumenter *"Hackers: Outlaws and Angels"*, Discovery Chanel, Februari 2004.

Pada applications log, hal-hal yang ditangkap lebih bersifat kompleks lagi. Karena aktivitas yang berhubungan dengan munculnya halaman baru akan langsung terekam secara otomatis. Bahkan untuk aktivitas membuka, menutup, running (action) akan langsung tertangkap. Hal-hal lain yang berhasil tertangkap User (nama), Time(waktu akses), Application Name (Nama aplikasi).

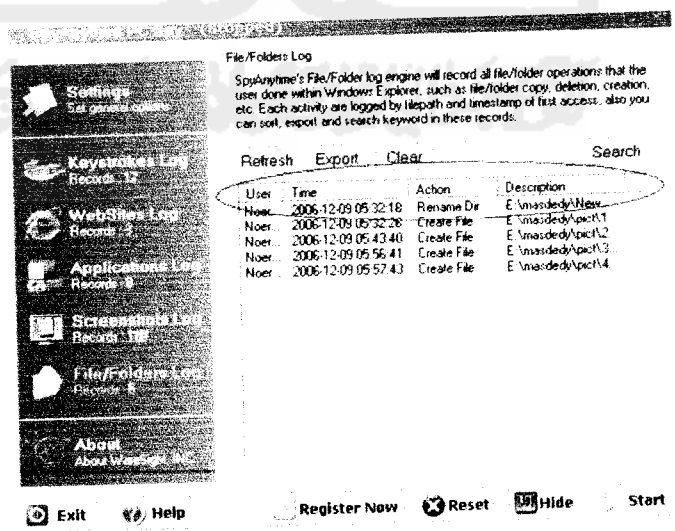
- Screenshots Log (Menangkap gambar)



Gambar 11 Screenshots Log

Karena berhubungan dengan menangkap gambar dengan selang interval waktu tertentu. Aktivitas peng-*capture*-an akan terus berjalan sesuai dengan setingan waktu. Misal dengan setingan 15 s, program akan merekam aktivitas gambar setiap 15 detik. Hal-hal lain yang berhasil ditangkap adalah User (nama), Time(waktu akses), Active Windows(aplikasi yang aktif), Snaphshot File (path gambar yang terekam).

- File/Folders Log (File/folder yang dibuka)



Gambar 12 File/Folders Log

America Online 4 dengan Internet Explorer 4.5

- FITUR :

Secara garis besar program ini terbagi atas tiga item pokok yang masing-masing item memiliki fungsi tersendiri, yakni :

I. Ghost Basic
   - Backup
   - Restore
   - View Log

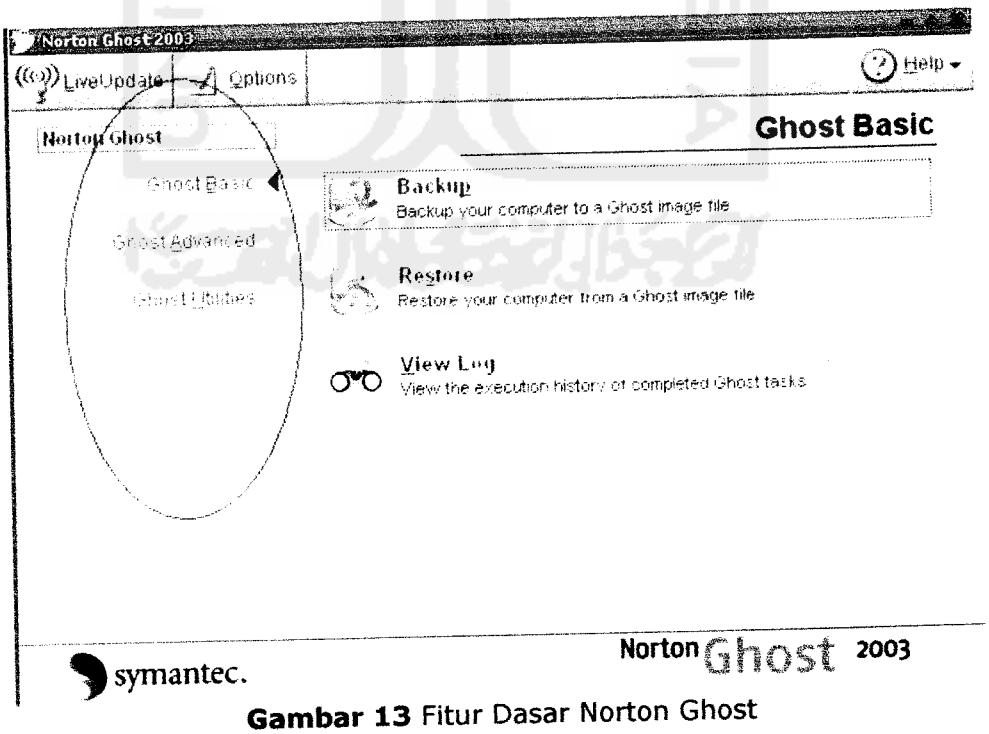
II. Ghost Advance
   - Clone
   - Run Ghost Interactively
   - Peer-to-peer
   - Create virtual Partition
   - Image Integrity check

III. Ghost Utilities
   - Norton Ghost Boot Wizard
   - Norton Ghost Explorer
   - Norton Ghost's User Guide

Kemudian akan diuraikan secara lebih dalam satu persatu dibawa ini (eksplorasi akan difokuskan pada Ghost Basic dan Ghost Advance-Clone, dikarenakan pada poin-poin itulah tujuan untuk Penyimpanan bukti digital sebenarnya telah tercapai) :

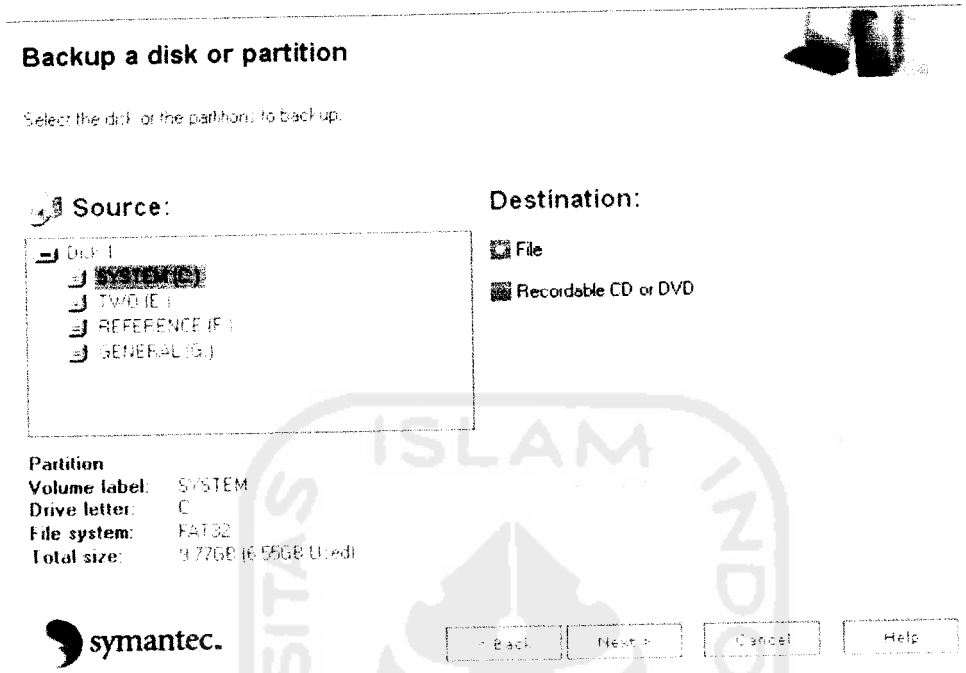
I. Ghost Basic

Memuat fitur-fitur yang merupakan basic (dasar) dari Norton Ghost 2003 ini.



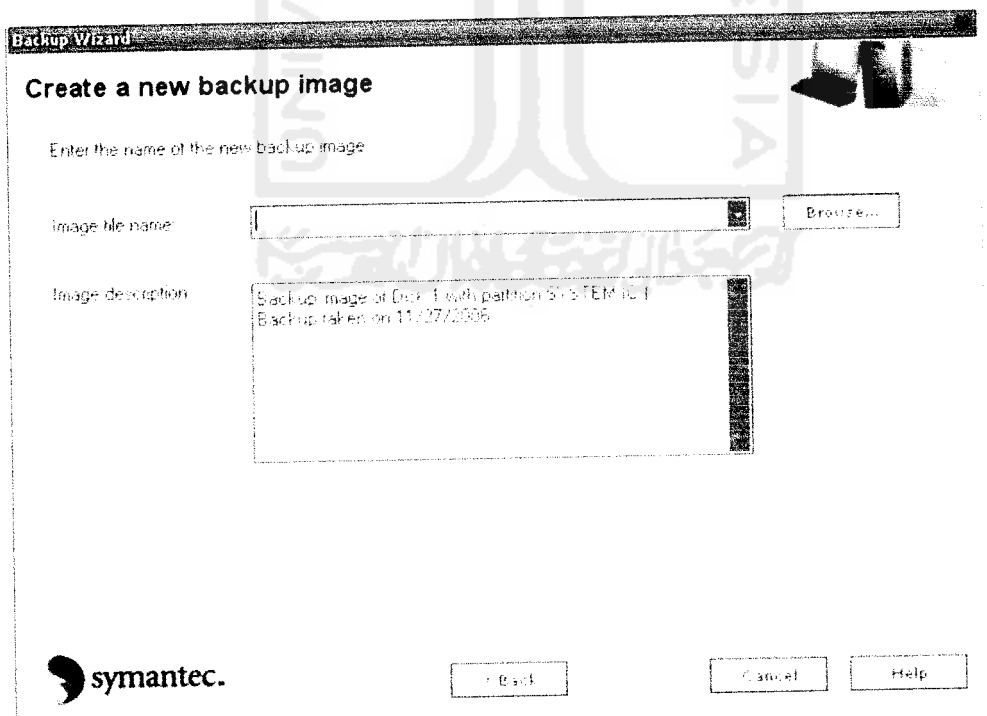
Gambar 13 Fitur Dasar Norton Ghost

- Backup
  Akan membuat image dari Source partisi yang akan diback-up untuk dikopikan diantara dua media(File atau CD/RW/DVD). Pada contoh ini, akan dipilih file (secara default).



Gambar 14 Back up

Kemudian, pilih lokasi penyimpanan di harddisk



Gambar 15 Lokasi Penyimpanan

Analisis kemungkinan juga dapat diperoleh dari motif/latar belakang yang ada sebelum didapatkan kesimpulan. Seperti dijelaskan pada bab-bab sebelumnya (Bab 1.1 **Kasus Cybercrime**), bahwasanya motif yang beragam inilah seringkali memaparkan fakta-fakta yang berkorelasi dengan kenyataan peristiwa, bahwa setiap **sebab** akan menghasilkan **akibat** yang relatif seragam.

2.3.3.4 **Presentasi bukti digital *(Presentation of Digital Evidence)***

Kesimpulan akan didapatkan ketika semua tahapan tadi telah dilalui, terlepas dari ukuran *obyektifitas* yang didapatkan, atau standar kebenaran yang diperoleh, minimal bahan-bahan inilah nanti yang akan dijadikan "modal" untuk ke pengadilan.

Proses digital dimana bukti digital akan dipersidangkan, diuji otentifikasi dan dikorelasikan dengan kasus yang ada. Pada tahapan ini menjadi penting, karena disinilah proses-proses yang telah dilakukan sebelumnya akan diurai kebenarannya serta dibuktikan kepada hakim untuk mengungkap data dan informasi kejadian.

Pada tahapan *final* ini ada beberapa hal yang mutlak diperhatikan, karena memang pada level ini ukuran kebenaran akan ditetapkan oleh pengadilan sebagai pemilik otoritas. Hal-hal yang dimaksud adalah :
- Cara Presentasi
- Keahlian Presentasi
- Kualifikasi Presenter
- Kredibilitas setiap tahapan pengusutan

3. Kejahatan Komputer

Tidak seperti kejahatan konvensional pada umumnya, kejahatan komputer memiliki beragam variasi sesuai dengan keahlian dan motif "si penjahat komputer", semakin besar motif yang melatarbelakangi maka akan semakin canggih pula modus operandi yang digunakan. Seiring dengan perkembangan kecanggihan sistem keamanan komputer biasanya selalu didahului oleh varian kejahatan komputer yang selangkah lebih maju, atau dengan bahasa yang sederhana, sebenarnya upaya keamanan komputer secanggih apapun, akan selalu ada *hole* (lubang/celah) yang dapat dimanfaatkan oleh penjahat ini.

3.1 **Mengidentifikasi dan Mengkategorikan Tipe Serangan**

Pada dasarnya untuk melakukan hal ini, lebih melihat kepada bagaimana cara "penyerang" untuk masuk kepada celah komputer kita. Serta yang lebih penting lagi, upaya ini adalah penting untuk mengatasi serangan-serangan sehingga diharapkan dapat lebih efektif dan effisiennya cara yang digunakan. Pengidentifikasian dan pengkategorian yang dimaksud adalah[9] :

- ✓ Aktivitas pra-serangan
- ✓ Metode cracking Password
- ✓ Teknik Exploit (Mengambil Keuntungan dari karakteristik Sistem Operasi atau protokol)
- ✓ Serangan Virus, Trojan, Worms

Selanjutnya akan dipaparkan secara umum masing-masing dari karakteristik diatas

3.1.1 **Aktivitas pra-serangan**

Pada step ini, biasanya lebih dimanfaatkan untuk mencari informasi terkait dengan target. Hacker yang berpengalaman akan "menginstruksikan" newbie tentang sesuatu dengan berbagai dalih dengan harapan akan memperoleh informasi terkait dengan targetan-targetan hacker. Langkah yang umum dilakukan adalah

1. Pre-attack (Pendahuluan/prolog)
2. Initial access (Inisialisasi akses)
3. Full system access (Akses sistem secara penuh)
4. Planting "back doors" for future access (Mempersiapkan "pintu belakang" untuk kabur)
5. Covering tracks (Menutup jalur)

3.1.2 **Metode cracking password**

Pada tahapan ini, password menjadi hal yang paling vital untuk aktivitas apapun. Dengan mengetahui password target, maka sebenarnya klimaks dalam pencarian pintu masuk telah dilalui. Beberapa manfaat dari penggunaan password adalah :

- Masuk dalam komputer lokal atau jaringan
- Mengakses proteksi website atau FTP.
- Mengakses e-mail.
- Mengakses dokument.

[9] Littlejohn Shinder, Debra, dan Ed Tittel (Editor), "*SCENE of CYBERCRIME computer forensic hand book*". Unknown City: Syngress Publishing,Inc, 2002

- Mengakses BIOS.

Kebanyakan user memakai penggunaan password untuk macam-macam penggunaan dengan memakai pasword yang sama. Jadi, dengan mengetahui satu saja password dari user, sesungguhnya Hacker dengan mudah saja untuk membuka proteksi-proteksi lainnya.

3.1.3 Teknik Exploit (Mengambil Keuntungan dari karakteristik Sistem Operasi atau protokol)

Teknik ini hampir sama dengan analogi seorang pencuri yang tidak dapat memasuki rumah target melalui pintu depan rumah, maka pada malam berikutnya pencuri ini datang lagi dengan memakai pintu belakang. Pemakaian sistem operasi tertentu selalu saja meninggalkan lubang keamanan, yang pada lubang ini akan dimanfaatkan hacker. Atau dengan menggunakan protokol sebagai sarana penghubung dalam jaringan yang tentu saja dengan lubang-lubang pada alamat protokol TCP tertentu. Pada pola ini seirng digunakan seranagan seperti Denial of Service (DoS), SYN/LAND Attacks, The Ping of Death dll.

3.1.4 Serangan Virus, Trojan, Worms

Penyerang yang telah dapat memasuki tanpa akses ini bisa saja telah mempersiapkan program perusak untuk mengganggu internal sistem. Pada akhirnya virus inilah yang akan "memakan" Produktifitas, Waktu, Biaya, Data, dokumen dan banyak hal yang merugikan lainnya.

Dengan Pengklasifikasian dan pengkategorian diatas, diharapkan antisipasi yang direncanakan akan lembih matang dalam mengantisipasi tindakan "penjahat komputer".

4. Penutup

Analogi "pisau yang memiliki dua mata" mungkin tepat untuk menggambarkan perkembangan teknologi saat ini. Disatu sisi ketika keterbutuhan akan teknologi informasi mutlak adanya, dimana disisi manapun kehidupan tidak akan terlepaskan dari perkara ini, namun disisi lain diikuti dengan hal-hal negatif dimana privasi individu, persaingan bisnis, pertahanan negara, kemerosotan moral dipertaruhkan.

Disiplin keilmuan dalam dunia komputerisasi yang relatif baru ini diharapkan mampu menjadi "oase" dalam kegersangan akan penindakan kejahatan computer yang bertajuk cybercrime. Bagaimanapun perkembangan disiplin ini akan terus menerus diperlukan sebagai *controller* kejahatan yang tentusaja akan juga terus menerus berkembang.

Selanjutnya kemudian, upaya *preventif*lah yang hendaknya dilakukan oleh pengguna komputer untuk mencegah setiap kejahatan dengan berbagai modusnya ini. Karena seperti kata pepatah, *'mencegah adalah lebih baik daripada mengobati'* bukan?. *Allahu A'lam.*

5. Glossary

- Cybercrime : Perkara kriminalitas dalam dunia cyber (komputerisasi)
- Revolusioner : Perubahan secara menyeluruh dengan waktu yang singkat
- makro : Cakupan yang luas
- Domino : Berantai, berimbas ke yang lain (kiasan)
- Konvensional : Pola lama
- Phobia : Ketakutan (berlebih)
- Kompetitor : Pesaing
- Market : Pasaran (bisnis)
- Nasionalisme : Sikap/paham mencintai bangsa dan negara sendiri
- Stealth Bomber ; Pesawat pengebom canggih dari AS yang telah berteknologi mutakhir
- Terminologi : Pengertian secara luas
- Otoritas : Hak/wewenang
- Preview : Tampilan singkat
- Searching : Pencarian
- analyzing : Penganalisaan
- space storage : Sisa Ruang (untuk penyimpan digital, seperti Hardisk, CD dll)
- Obyektifitas : Sudut pandang pendapat dengan melihat secara nyata, dari luar, sesuai adanya
- Kredibilitas : Kepemilikan kewibawaan
- FTP : fasilitas untuk meng-upload (mentransfer ke-) secara digital
- BIOS : Fitur dari Motherboard untuk menyimpan informasi dari pabrik
- Oase : mata air di gurun pasir (kiasan)
- Preventif : Pencegahan
- Controller : Pengontrolan/pengendalian

6. Daftar Pustaka

[LIT02] Littlejohn Shinder, Debra, dan Ed Tittel (Editor), *"SCENE of CYBERCRIME computer forensic hand book"*. Unknown City: *Syngress Publishing,Inc,* 2002

[MCK99] Mc Kemmish, Rodney, *"What is forensic computer"*. Australia: Australian institute of Criminology, 1999. http://www.aic.gov.au/publications/tandi/ti118.pdf

[HAC04] Film dokumenter *"Hackers: Outlaws and Angels"*, Discovery Chanel, Februari 2004.

[MAR02] Marcella, A J dan Greenfield, R S(Editors), *"CYBER FORENSICS a field manual for collecting, examining, and preserving evidence of computer crimes"*. USA: CRC Press LLC, 2002

[WRI01] Wright, Mal, *"Investigating an Internal Case of Internet Abuse"*. USA: SANS Institute, 2001.

[UTD01] Utdirartatmo, Firrar, *"Tinjauan Analisis Forensik dan Kontribusinya pada Keamanan Sistem Komputer"*, Bandung : INSTITUT TEKNOLOGI BANDUNG, 2001.

[BUD03] Budiman, Rahmadi, *"Tugas Keamanan Sistem Lanjut, Komputer Forensik Apa dan Bagaimana?"*, Bandung : MAGISTER TEKNIK ELEKTRO OPTION TEKNOLOGI INFORMASI, INSTITUT TEKNOLOGI BANDUNG, 2003

[TEC05] situs www.terbpathways.com, diakses pada november 2005

[FOR06] situs www.forensics.mtl.com/def2.html, diakses pada november 2005

LAPORAN PROJECT KEDUA

TUGAS AKHIR NON SKRIPSI

Review dan Implementasi Software Forensic

DISUSUN OLEH :

Dedy Setyo Afrianto.
02.523.229

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

Desember 2006

Review dan Implementasi Software Forensik

Project ke-2 Tugas Akhir Non Skripsi
Oleh : Dedy Setyo Afrianto (02 523 229)
Jurusan Teknik Informatika, Fakultas Teknologi Industri
Universitas Islam Indonesia
E-mail : dedysetyoa@students.fti.uii.ac.id

Abstraksi

Kinerja investigator dalam mengungkap kasus cybercrime memiliki peran yang besar, sebagai lini terdepan dalam "membedah" kebenaran, kejelian untuk melihat indikasi, bukti atau motif sekecil apapun dari sebuah kasus menjadi wajib adanya. Hal lain yang tak kalah penting adalah adanya "senjata" pembantu yang nantinya akan berkutat pada bukti-bukti kejahatan. Karena tentu saja peranan dari sebuah bukti memiliki peran yang vital, penggunaan alat bantu yang reliable-pun menjadi kebutuhan.

Tulisan ini akan meng-explore sebagian dari berbagai macam software yang bersinggungan langsung dengan digital evidence(bukti digital). Harapannya untuk mengenalkan kelebihan dan kekurangan (review) pada setiap software, sehingga dalam pemilahan penggunaan software akan menemukan tools yang efektif, serta memiliki peran yang signifikan.

Kata kunci : Keamanan komputer, security, software forensik, cybercrime

1. Pengantar

Pada bagian pertama telah dipaparkan bahwasanya aktivitas investigasi Forensik melibatkan peranan penting dari bukti digital. Ketika bukti digital ini diperoleh dan telah diproses dengan baik, maka sebenarnya telah mengungkap separuh dari kebenaran, namun sebaliknya ketika perolehan bukti serta pemrosesan lebih lanjut tidak optimal, maka tugas Investigator akan jauh lebih berat. Dengan *term* seperti ini, maka tugas pertama yang harus diprioritaskan untuk dilakukan adalah upaya mendeteksi bukti-bukti digital. Namun, pada *step* ini diperlukan perangkat pendukung yang berfungsi untuk mempermudah kerja investigator, selain itu juga dengan harapan kinerja akan lebih *efektif* dan *efisien* dengan hasil yang optimal.

2. Aplikasi Elemen Kunci Forensik

Dengan Landasan Empat Elemen Kunci Forensik yang telah dipaparkan pada bab sebelumnya, bab ini akan lebih memaparkan secara terperinci masing-masing tahapan disertai dengan tools program pendukung.

2.1 Identifikasi/Memperoleh dalam bukti digital *(Identification/Collecting Digital Evidence)*

- **Spy Anytime PC SPY**
  - Pengantar :

Program yang berasal dari **WareSight, Inc** dengan alamat situsnya http://www.WareSight.com ini membangun programnya pada Th.2000.

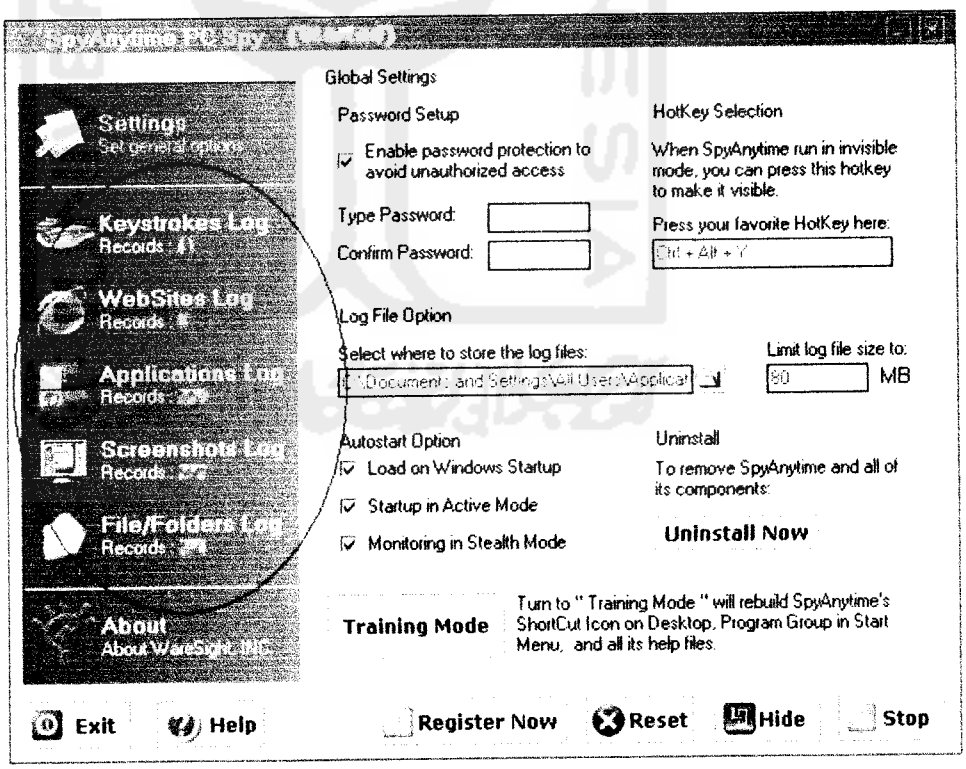
Mengkhususkan peranan softwarenya pada pemantauan aktivitas yang terjadi seperti layaknya kamera yang mengintai di depan monitor. Aktivitas pengintaian yang terjadi pun terus menerus berjalan selama komputer hidup dan bekerja pada *background*.

- STANDAR HARDWARE PC :

CPU: Pentium Class PC (133 MHz atau lebih tinggi0)
RAM: 32 MB
Disk Space: 3 MB harddisk kosong, 20 MB untuk log files
Video: 800x600, 256 colors
OS: Windows 95/98/ME/NT/2000/XP

- FITUR :
  Secara garis besar terbagi atas dua bagian
  1. Memantau aktivitas Monitor, meliputi
     a. Keystrokes Monitoring (Melihat tombol keyboard yang ditekan)
     b. WebSites Monitoring (Melihat Halaman URL yang diakses)
     c. Applications Monitoring (Melihat aplikasi yang dijalankan)
     d. Screen Shot Logging (Menangkap gambar)
     e. File/Folders Monitoring (Melihat File/folder yang dijalankan)

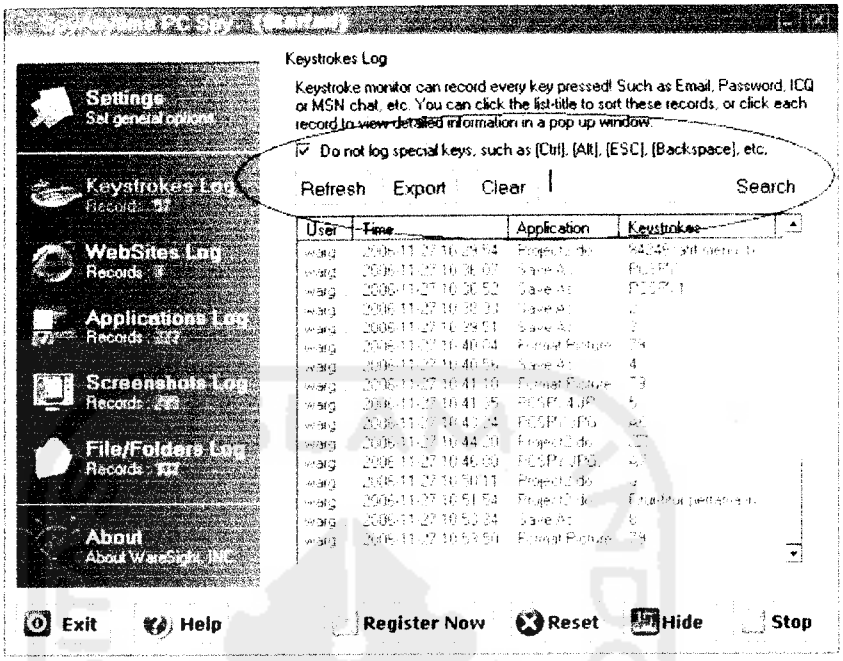
     Fitur-fitur pertama ini secara keseluruhan terlketak pada lajur kiri tampilan, dengan posisi seperti dibawah ini.



Gambar 1 Fitur Pertama PC SPY

  2. Memantau Logs, meliputi
     a. Refresh Log (memperbaharui Log yang terekam)
     b. Export Log (Mengubah format ekstensi Log)

c. Clear Log (Membersihkan Log)
d. Search Log (Mencari Log)
e. View Screenshot picture (Melihat screenshot gambar aktivitas)



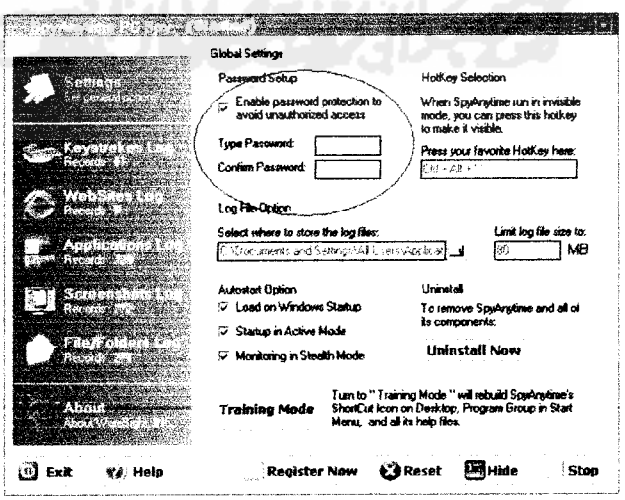
Gambar 2 Memantau Logs

- Setting tambahan

Ada beberapa fitur tambahan yang disediakan dalam mengakses software ini. *Control Panel* merupakan button untuk mengkonfigurasi untuk kemudahan user dalam penggunaan.

- Password Setup

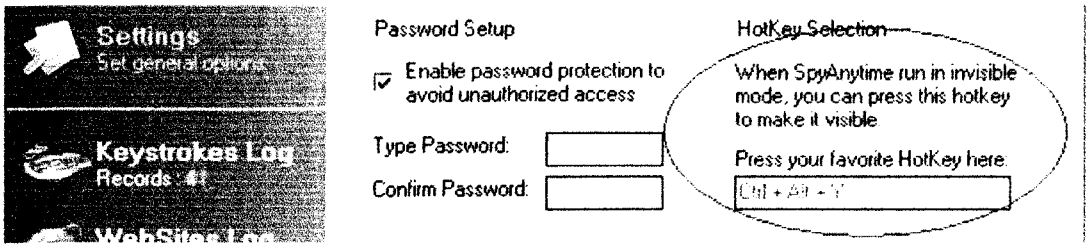
Digunakan untuk mengeset password yang dipakai sebagai piranti security untuk user yang mencegah user yang tidak memiliki hak pakai software.



Gambar 3 Setting Password

- Hotkey Selection

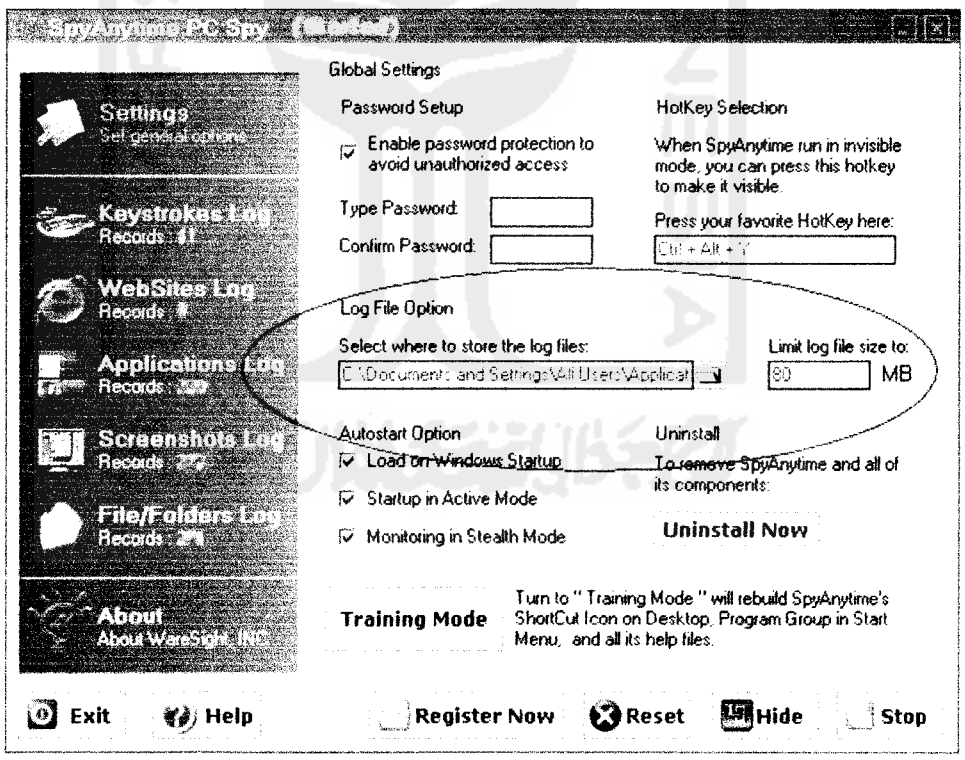
Berguna untuk memanggil program dengan variasi tombol sebagai shortcut yang memberikan kemudahan bagi user (***default***:Ctrl+Alt+Y)



Gambar 4 Hotkey Selection

- Logfile Option

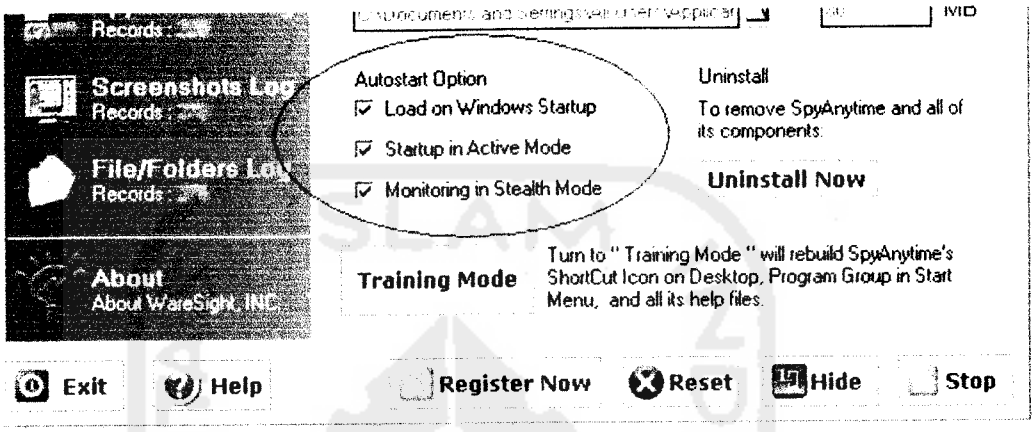
Terdapat dua item, dimana item sebelah kiri menunjukan tempat tujuan Log-log file akan disimpan. Item sebelah kanan menunjukan ukuran maksimal penyimpanan Log File (***default***:80 MB). Semakin besar setingan kapasitas, maka akan semakin banyak pula rekaman log yang tersimpan dalam waktu yang lebih lampau.



Gambar 5 Lokasi Log File

- Autostart option

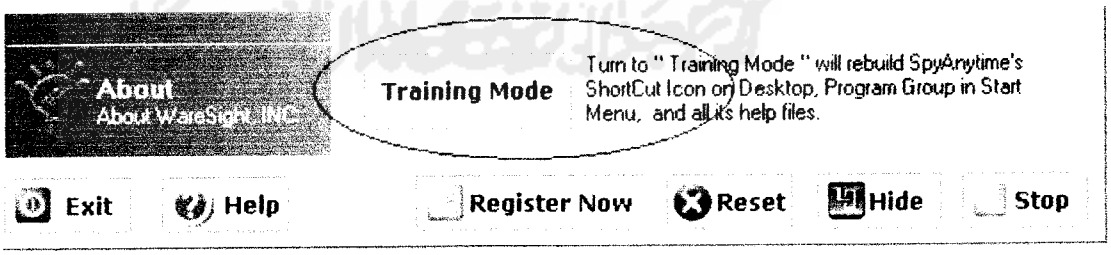
Spyanytime dapat dikonfigurasi dalam tiga varian. *Pertama*, Load on Windows Startup, Spyanytime akan otomatis berjalan ketika komputer hidup. *Kedua*, Startup in Active Mode, Spyanytime akan diberjalan ketika tombol eksekusi ditekan. Ketiga, Monitoring in Stealth Mode, pada varian ini program akan sepenuhnya *invisible* (tidak nampak) ketika berjalan, tidak nampak dalam windows taskbar atau dalam Apllication List Windows. Untuk menampakkan dapat menggunakan Hotkey selection (***default***:Ctrl+Alt+Y).



Gambar 6 Autostart Option

- Skilled Mode and Training Mode

Terdapat dua mode dalam penggunaan. *Pertama*, Skilled Mode, pada option ini, Spyanytime dapat diseting dengan menghilangkan icon pada desktop, start menu, bahakan akan menghilangkan help file. Untuk memanggil program dapat mengetikkan "sa2" pada menu **Run** (START → RUN → *ketikkan* sa2 → Enter) atau dengan menggunakan Hotkey. *Kedua,* Training Mode, pada option ini akan mengembalikan seperti semula setingan yang sebelumnya hilang

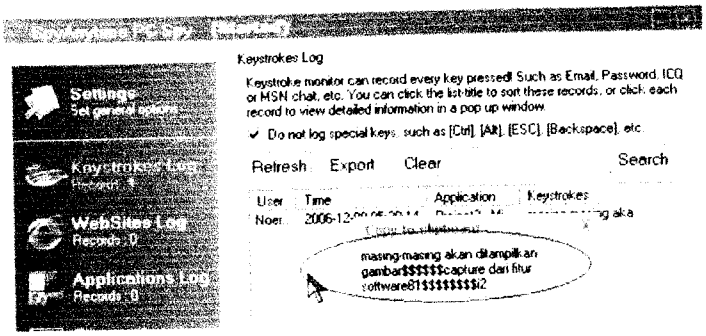


Gambar 7 Training Mode

- **Tampilan Output**

Dibawah ini akan dipaparkan tampilan output dari bukti-bukti yang berhasil ditangkap oleh PC spy. Masing-masing akan ditampilkan *data-data bukti* dari fitur software.

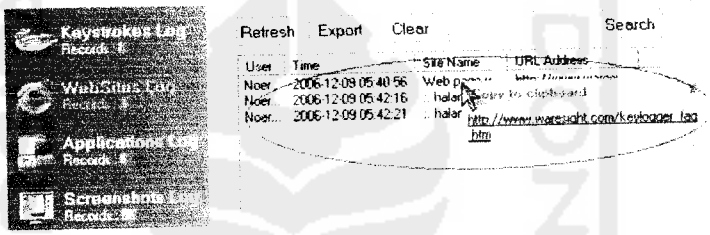
- Keystrokes Log (aktivitas keyboard)



Gambar 8 Keystrokes Log

Gambar diatas ini menangkap aktivitas keyboard yang dilakukan user, juga lengkap beserta keterangan User (nama), Time(waktu), Application (aplikasi yang dijalankan), keystroke (tombol yang ditekan).

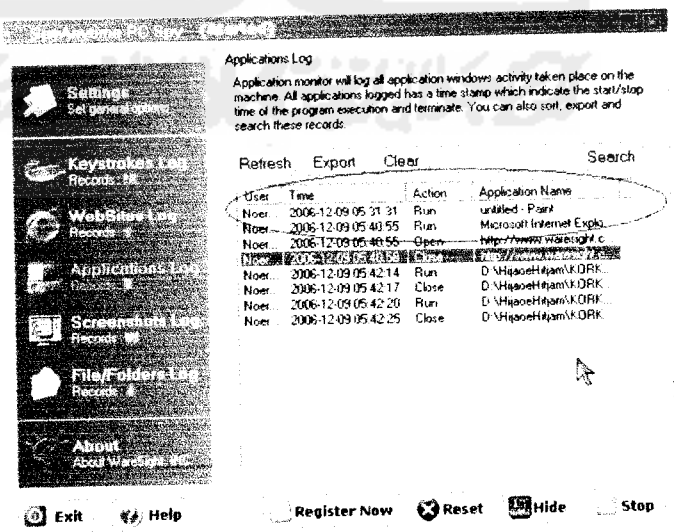
- Website Log (Url yang diakses)



Gambar 9 Website Log

Halaman url (URL Address) yang berhasil tertangkap langsung terekam beserta data-data lain seperti User (nama), Time(waktu akses), Site Name (Nama situs).

- Applications Log (Aplikasi yang dieksekusi)



Gambar 10 Application Log

dengan aktivitas negatif ini. Kasus yang terjadipun menunjukan bahwa perkara ini tidak main-main, berbagai laporan menunjukan bahwa kejahatan komputer telah menyedot perhatian banyak pihak yang terkait dengan masalah ini, contoh laporan yang ada diantaranya

- 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 penuh dapat download di PDF format pada *(www1.ifccfbi.gov/strategy/IFCC_Annual_Report.pdf.)*
- Menurut Survey Institute Keamanan Komputer Computer pada 2001, bersama dengan Squad Penggangguan 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).*
- Menurut Cybersnitch Voluntary Online Crime melaporkan Sistem Kejahatan Relasi-Internet mencakup dari pemalsuan desktop ke pornografi anak dan meliputi kejahatan yang kejam seperti pencurian elektronik dan teroris threats.(daftar dilaporkan cybercrimes tersedia pada *www.cybersnitch.net/csinfo/csdatabase.asp*.)

Dan masih banyak laporan-laporan tragis yang menunjukan betapa bahayanya aktivitas kriminal ini. Untuk beberapa tahun kedepan, ketika aktivitas IT masyarakat meningkat, akan lebih menambah potensi yang terjadi dalam dunia kriminalitas ini[1].

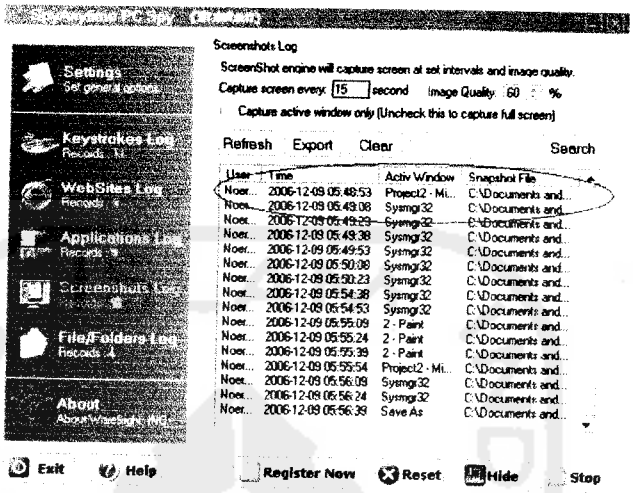
Telah banyak penelitian yang menyebutkan bahwasanya berbagai gejala fenomena kriminalitas dunia maya dilakukan oleh subyek yang tentusaja sarat *tendensi* (kepentingan), berbagai kecenderungan kepentingan yang ada antara lain; 1.)Permasalahan finansial yang dianggap bahwasanya *cybercrime* adalah alternatif baru untuk mendapatkan kucuran uang. Kecenderungan ini benar adanya, 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*, serta masih banyak contoh problem ekonomi yang melatar belakangi perilaku ini. 2.)Adanya permasalahan dalam tingkatan kenegaraan yang menyangkut persoalan politik, militer dan sentimen *Nasionalisme*. Sebuah kasus nyata pernah terjadi pada awal tahun 1990, yakni Pesawat pengebom paling Rahasia Amerika, *Stealth Bomber* dijadikan objek serangan oleh hacker-hacker, diindikasikan memang sangat *secret*-nya spesifikasi khusus pesawat ini. Lagipula memang permasalahan peralatan militer yang berteknologi tinggi menjadikan sebuah kajian menarik dalam kompetisi antar negara dalam mengembangkan peralatan tempurnya. 3.)Faktor kepuasan pelaku, dalam hal ini tentusaja permasalahan psikologis menjadi sebuah pertanyaan besar. Banyak kecenderungan menyebutkan bahwasanya seseorang dengan skill tinggi dalam bidang penyusupan keamanan akan selalu tertantang dengan "rute-rute" baru yang sedikit berliku. Bahkan kepuasan batin lebih menjadi orientasi utama untuk hacker yang lebih memiliki skill tinggi daripada segepok uang, menurut paparan salah seorang Hacker senior di negeri Paman Sam[2].

[1] Littlejohn Shinder, Debra, dan Ed Tittel (Editor), "*SCENE of CYBERCRIME computer forensic hand book*". Unknown City: Syngress Publishing,Inc, 2002

[2] Film dokumenter "*Hackers: Outlaws and Angels*", Discovery Chanel, Februari 2004.

Pada applications log, hal-hal yang ditangkap lebih bersifat kompleks lagi. Karena aktivitas yang berhubungan dengan munculnya halaman baru akan langsung terekam secara otomatis. Bahkan untuk aktivitas membuka, menutup, running (action) akan langsung tertangkap. Hal-hal lain yang berhasil tertangkap User (nama), Time(waktu akses), Application Name (Nama aplikasi).

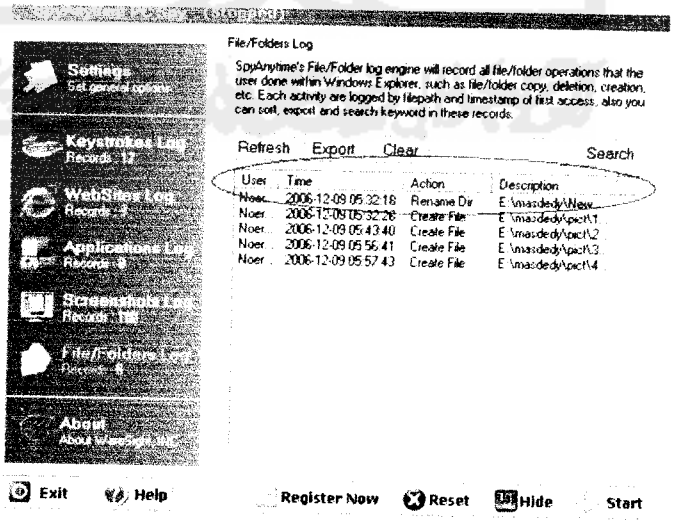
- Screenshots Log (Menangkap gambar)



Gambar 11 Screenshots Log

Karena berhubungan dengan menangkap gambar dengan selang interval waktu tertentu. Aktivitas peng-*capture*-an akan terus berjalan sesuai dengan setingan waktu. Misal dengan setingan 15 s, program akan merekam aktivitas gambar setiap 15 detik. Hal-hal lain yang berhasil ditangkap adalah User (nama), Time(waktu akses), Active Windows(aplikasi yang aktif), Snaphshot File (path gambar yang terekam).

- File/Folders Log (File/folder yang dibuka)



Gambar 12 File/Folders Log

Kalau pada aplikasi ini, berhubungan dengan file atau folder yang dieksekusi, rename atau create. User (nama), Time(waktu akses), Action (perlakuan user pada file/folder yang bersangkutan), Description (path lokasi)

2.2 Penyimpanan bukti digital *(Preserving Digital Evidence)*

Penyimpanan bukti digital adalah salahsatu step vital dalam pemrosesan kebenaran. Step ini mutlak dilakukan seorang investigator karena bukti merupakan alat vital dalam pengungkapan kebenaran.
Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, mengalami kecelakaan. Step pertama untuk menghindarkan dari kondisi-kondisi demikian adalah salahsatunya dengan mengcopy data secara *Bitstream Image* pada tempat yang sudah pasti aman.
Bitstream image adalah methode 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*), file yang belum ter-*ovverwrite*. Dengan kata lain, setiap biner digit demi digit terkopi secara utuh dalam media baru. Tekhnik pengkopian ini menggunakan teknik ***Komputasi CRC***[1]. Teknik ini umumnya diistilahkan dengan *Cloning Disk* atau *Ghosting*.

Pada step kedua ini, salahsatu software yang dapat dipergunakan adalah **Norton Ghost 2003.**

- **Norton Ghost 2003**
  - Pengantar :

Software ini dibangun **Symantec Corporation** (www.symantec.com) sejak 1995 sampai dengan 2002 dan terus berbenah dengan perbaikan-perbaikan fitur sampai sekarang. Orientasi kerja pada pembuatan image yang akan mengkopi bit demi bit sumber data.

- STANDAR HARDWARE PC :

Windows

Windows 95, 98, NT 4.0, 2000, XP atau lebih baru, Pentium 166 mHz atau lebih cepat dengan processor 32 MB RAM
256-color monitor dengan resolusi 800 x 600
Internet Explorer 4 atau lebih baru
Netscape 4 atau lebih baru
America Online 4 (dengan JavaScript di-enabled dan cookies dinyalakan)

Macintosh

Macintosh PowerPC dengan System 8.1 atau lebih baru, 120mhz atau lebih cepat dengan processor 32 MB RAM
256-color monitor dengan resolusi 800 x 600
Internet Explorer 4.5 atau lebih baru
Netscape 4 atau lebih baru

[1] Lihat CRC dalam www.forensics-intl.com/def2.html.

America Online 4 dengan Internet Explorer 4.5

- FITUR :

Secara garis besar program ini terbagi atas tiga item pokok yang masing-masing item memiliki fungsi tersendiri, yakni :

I. Ghost Basic
   - Backup
   - Restore
   - View Log

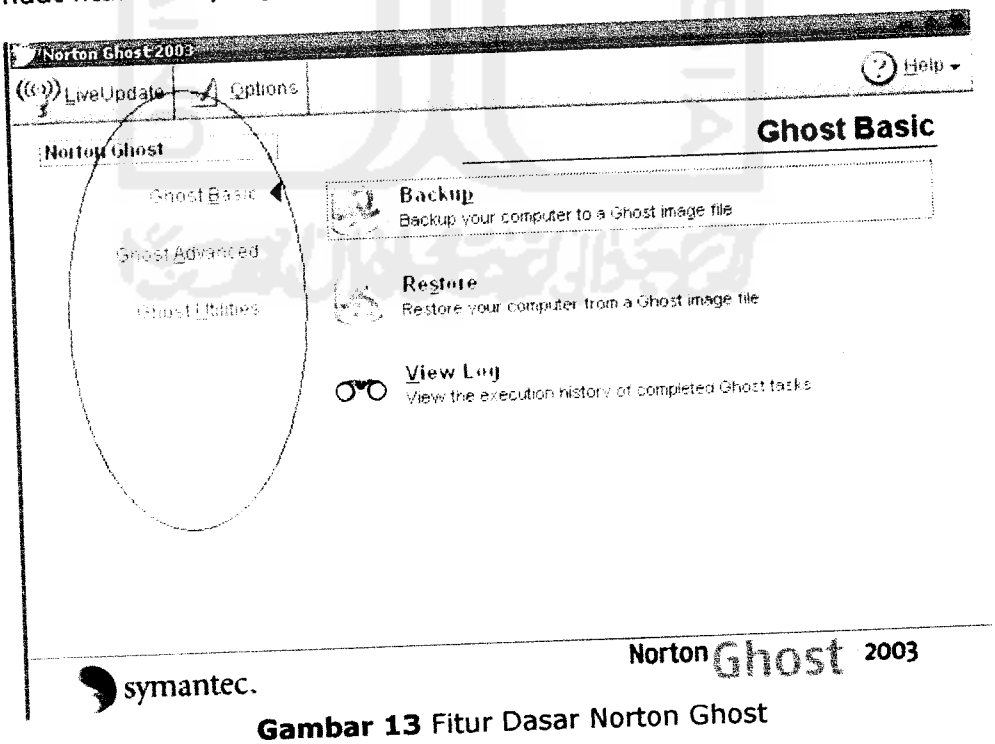
II. Ghost Advance
   - Clone
   - Run Ghost Interactively
   - Peer-to-peer
   - Create virtual Partition
   - Image Integrity check

III. Ghost Utilities
   - Norton Ghost Boot Wizard
   - Norton Ghost Explorer
   - Norton Ghost's User Guide

Kemudian akan diuraikan secara lebih dalam satu persatu dibawa ini (eksplorasi akan difokuskan pada Ghost Basic dan Ghost Advance-Clone, dikarenakan pada poin-poin itulah tujuan untuk Penyimpanan bukti digital sebenarnya telah tercapai) :

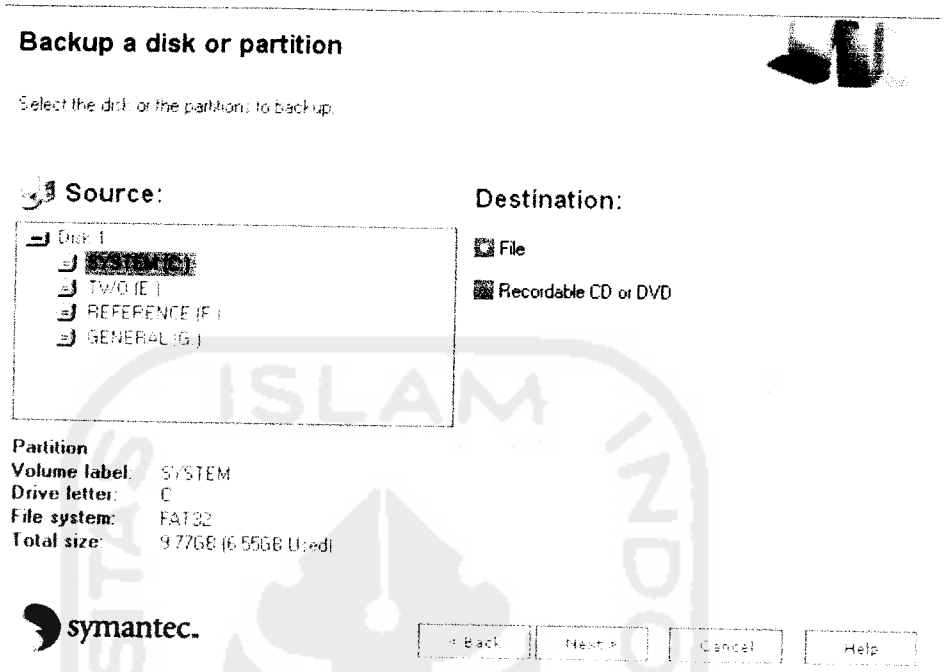
I. Ghost Basic

Memuat fitur-fitur yang merupakan basic (dasar) dari Norton Ghost 2003 ini.



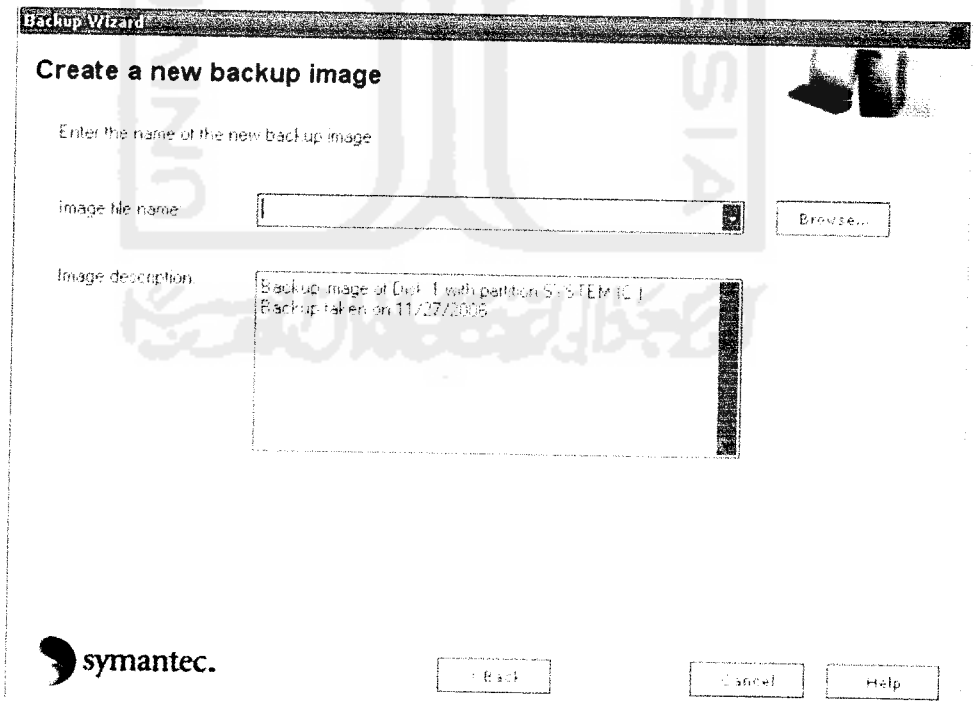
Gambar 13 Fitur Dasar Norton Ghost

- Backup
  Akan membuat image dari Source partisi yang akan diback-up untuk dikopikan diantara dua media(File atau CD/RW/DVD). Pada contoh ini, akan dipilih file (secara default).



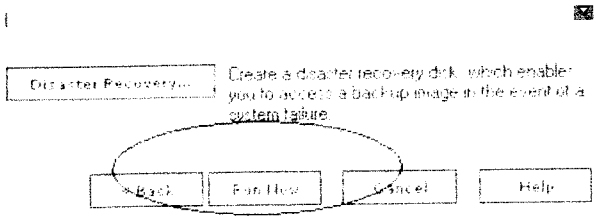
Gambar 14 Back up

Kemudian, pilih lokasi penyimpanan di harddisk



Gambar 15 Lokasi Penyimpanan

Selanjutnya, next → next dan ikuti perintah berikutnya. Sampai ada perintah **Run Now,** seperti dibawah ini



Gambar 16 Keterangan Lanjut

Setelah diklik **Run Now,** akan menuju ke tampilan **DOS** dan menjalankan semua prosedur yang ada.

- **Restore**

Pada prinsipnya adalah ketika back-up tadi menympan kopian dalam bentuk image, pada sesi inilah adalah mengekstrak image menjadi kumpulan file pada tempat tujuan. Langkah-langkah secara sederhana hampir sama dengan sebelumnya (back-up), sampai pada instruksi **Run Now** dan restart komputer ke tampilan DOS.

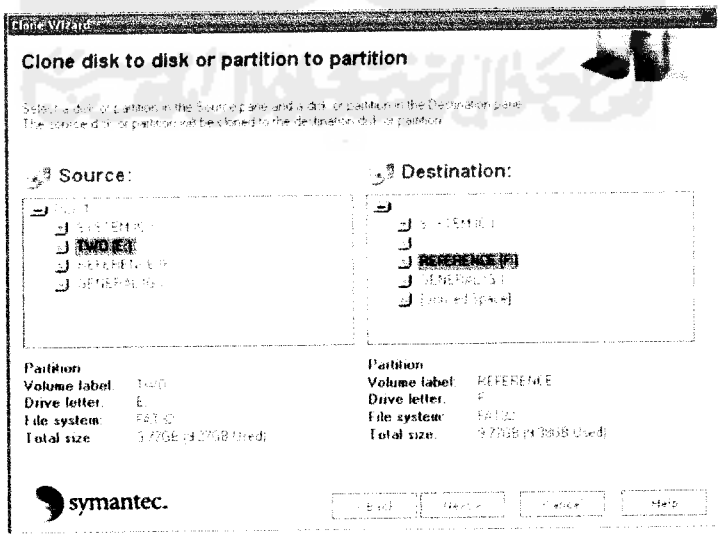
- **View Log**

Pada bagian ini, Log-log pengaksesan akan direkam secara otomatis oleh Noron Ghost 2003, seingga pemrosesan-pemrosesan yang telah dilakukan akan ditampilkan secara detail.

ii. Ghost Advanced

- **Clone**

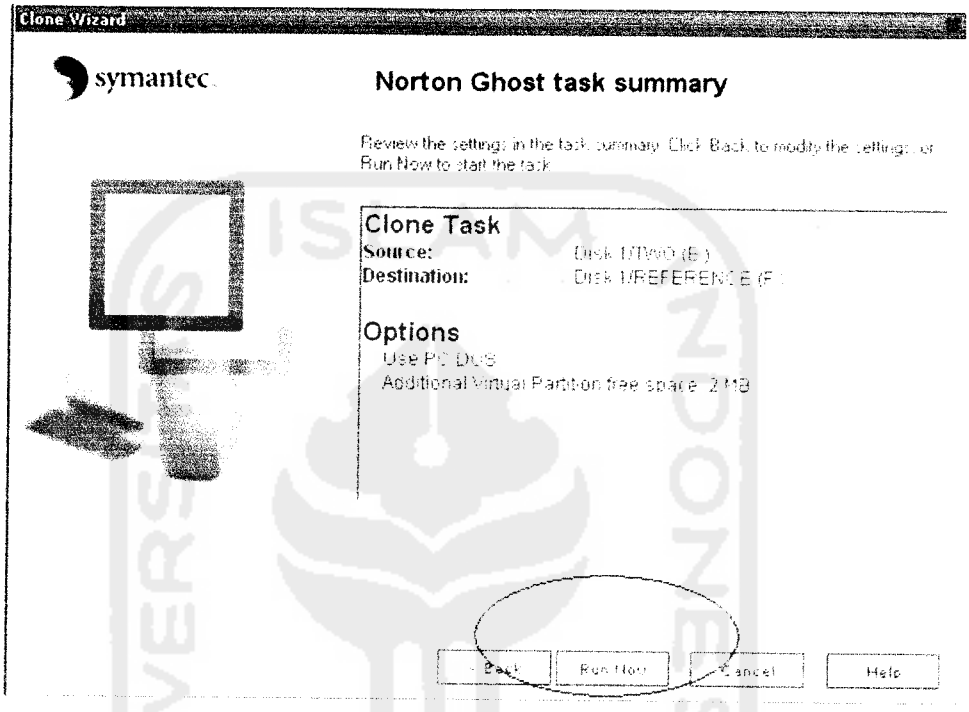
Pada bagian ini, bertujuan untuk menciptakan kloning dari sumber(Source) yang akan sama dan identik. Pada prinsipnya akan menciptakan langsung kloning-an kepada space tujuan(Destination) tanpa menciptakan image terlebih dahulu.



Gambar 17 Clone Disk

Pada tahap inilah diharapkan kehati-hatian dari investigator, lebih-lebih pada alokasi space dari tujuan. Sebisa mungkin space dari tujuan memiliki ruang yang lebih besar dari pada space sumber. Untuk menghindari kecacatan bukti digital karena harus mengulang-ulang proses yang tidak effisien.

Instruksi yang diterapkan tidak terlalu rumit, next → next sampai kepada **Norton Ghost task Summary,** kemudian klik Run Now, seperti pada gambar dibawah ini.



Gambar 18 Task Summary

Komputer akan berjalan dan memproses prosedur-prosedur kemudian masuk ke halaman DOS. Ikuti proses yang berjalan sampai selesai.

Fitur yang tersedia pada Norton Ghost 2003 memiliki varian yang banyak, namun pada intinya proses pemeliharaan bukti digital sudah berakhir disini, tinggal kemudian tugas seorang investigator untuk menguasai lebih banyak dalam berbagai fitur untuk kemudian dapat mengatasi bermacam-macam modus kejahatan yang ada.

2.3 Analisa bukti digital *(Analizing Digital Evidence)*

► Forensic ToolKit (FTK)

- **Pengantar :**

Software ini dibangun oleh AccesData Corp. (www.accessdata.com) pada 2003-2004 dengan terus mengembangkan produk mereka sampai sekarang. Penggunaan lisensi Trademark dilakukan perkomponen fasilitas yang terdapat didalamnya, antara lain

- AccessData terregistrasi trademark oleh AccessData Corp.
- Distributed Network Attack terregistrasi trademark oleh AccessData Corp.
- DNA terregistrasi trademark oleh AccessData Corp.
- Forensic Toolkit terregistrasi trademark oleh AccessData Corp.
- FTK terregistrasi trademark oleh AccessData Corp.
- FTK Imager terregistrasi trademark oleh AccessData Corp.
- Known File Filter terregistrasi trademark oleh AccessData Corp.
- KFF terregistrasi trademark oleh AccessData Corp.
- LicenseManager terregistrasi trademark oleh AccessData Corp.
- Password Recovery Toolkit terregistrasi trademark oleh AccessData Corp.
- PRTK terregistrasi trademark oleh AccessData Corp.
- Registry Viewer terregistrasi trademark oleh AccessData Corp.
- Ultimate Toolkit terregistrasi trademark oleh AccessData Corp

- **Standar Hardware PC :**

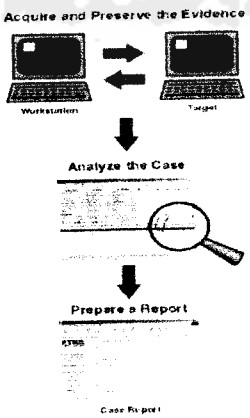
Hardware or Software	Minimum Requirement	Recommended Requirement
Operating System	Windows NT 4.0, 98, 2000, ME, or XP	Windows 2000 or XP
Processor	Intel Pentium II, Celeron, or compatible	1 GHz or faster Intel Pentium III, AMD Athlon, or compatible
RAM	128 MB	512 MB - 1 GB
CD-ROM Drive	4x speed	

Hardware or Software	Minimum Requirement	Recommended Requirement
Hard disk space	• 20 MB for program files • Additional hard disk space for index storage For additional information about the space required for indexes, see "Conducting an Indexed Search" on page 115.	
Monitor	SVGA (800 x 600)	XGA (1024 x 768) or higher resolution
USB or Parallel Port	Dongle shipped with FTK	

- **File sistem yang disupport dan format image**

File Systems	FAT 12, FAT 16, FAT 32
	NTFS
	Ext2, Ext3
Hard Disk Image Formats	Encase
	SnapBack
	Safeback 2.0 and under
	Expert Witness
	Linux DD
	ICS
	Ghost (forensic images only)
	SMART
CD and DVD Image Formats	Alcohol (*.mds)
	CloneCD (*.ccd)
	ISO
	IsoBuster CUE
	Nero (*.nrg)
	Pinnacle (*.pdi)
	PlexTools (*.pxi)
	Roxio (*.cif)
	Virtual CD (*.vcd)

- **FITUR :**



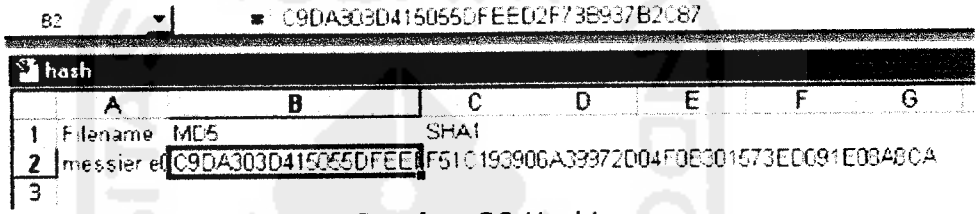
Gambar 19 Fitur FTK

Secara garis besar tool ini memiliki fitur yang sebenarnya sudah lengkap dan layak untuk digunakan sebagai alat bantu investigator karena memang sudah terdapat fitur yang memadai meliputi langkah-langkah penyelidikan (Pemeliharaan bukti, analisis bukti, Laporan Kasus). Namun pada bab ini, hanya akan dipaparkan lebih rinci tentang fitur analyzing-nya(Menganalisis) saja.

Pada tahapan analyzing, mencakup beberapa komponen, antara lain :

- Hashing
  Adalah aktifitas untuk men-generate index secara uniq file-file bukti yang ada, hal ini diperlukan untuk mengecek integritas file atau melacak keotentikan file, aktifitas ini dilakukan melalui file contents-nya.
  Dua fungsi Hash tersedia dalam FTK dan FTK Imager. Message Digest 5 (MD5) dan Secure Hash Algorithm (SHA-1), secara default akan dipilih MD5.

  Gambar dibawah ini akan menunjukan salahsatu contoh file yang diindex oleh FTK.



Gambar 20 Hashing

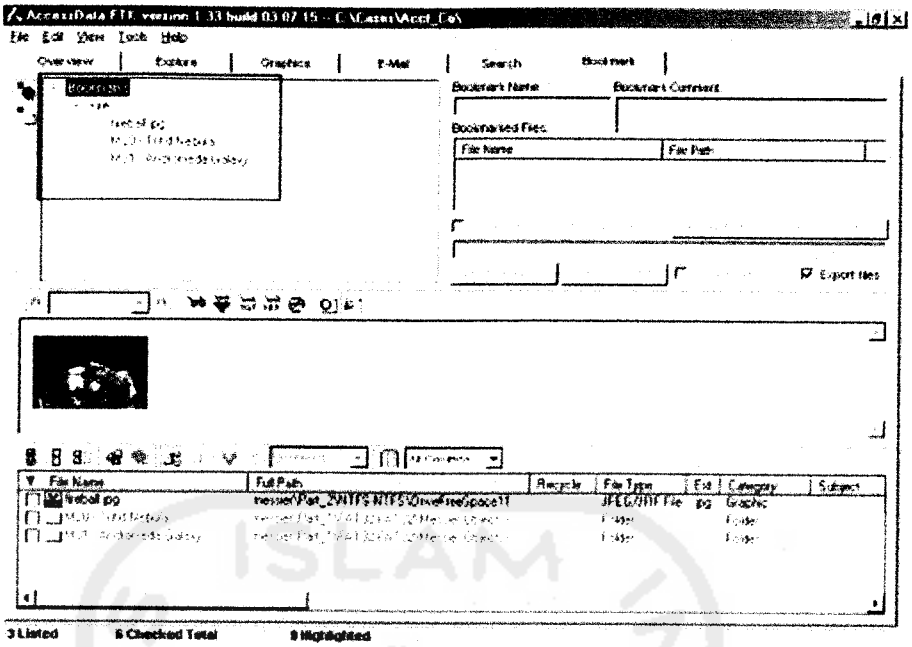
- Known File Filter (KFF)
  Adalah salahsatu fitur dari FTK dengan membandingkan database bukti yang dimiliki dengan file-file yang didapatkan. KFF bertujuan untuk mengiliminir serta mengabaikan (seperti sistem atau program file), memberitahukan kepada investigator tentang adanya file-file yang diduga 'gelap' atau berbahaya dan senantiasa mengecek untuk menduplikasi file.

- Seaching
  Dengan menggunakan FTK, investigator dapat mencari file-file sesuai yang dikehendaki. Dengan menggunakan dua methode, methode live dan methode peng-indexkan. Methode live searching memungkinkan investigator melakukan pencarian dengan mengkomparasikan item demi item dengan term yang dicari. Penggunaan live searching, memungkinkan pencarian dengan karaktek non alphanumerik dan menggunakan ekspresi regular. Sedangkan pencarian dengan methode pengindex-kan merupakan metode pencarian dengan menggunakan index sebagai media bantu file yang dikehendaki.

Pemrosesan Barang bukti

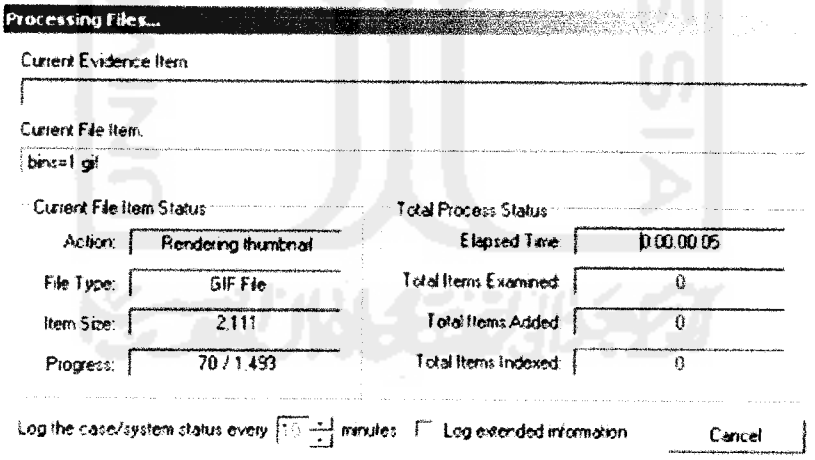
Setelah semua barang bukti dapat list dalam kasus, tahapan urgen dalam penganalisaan dalam penggunaan FTK dapat dipaparkan sebagai berikut;

1. *Penggunaan Bookmarks*
   Bookmarks terdiri dari group yang dapat dijadikan referensi dalam penyelesaian kasus. Penyusunan dapat terdiri daari barang-barang bukti yang memiliki identifikasi kesamaan-kesamaan.



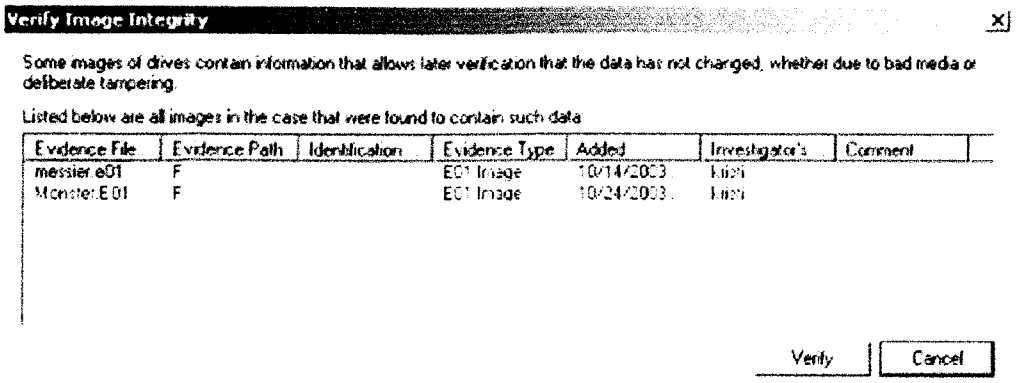
Gambar 21 Bookmarks

2. *Pembuatan Thumbnails*
Pembuatan Thumbnails berguna untuk mengelola graphics agar lebh memudahkan investigator dalam melakukan visualisasi graphics. Untuk graphic-graphic tertentu hal-hal seperti ukuran gambar, tipe prosesor, ukuran RAM benar-benar mempengaruhi pembuatan Thumbnails.



Gambar 22 Thumbnails

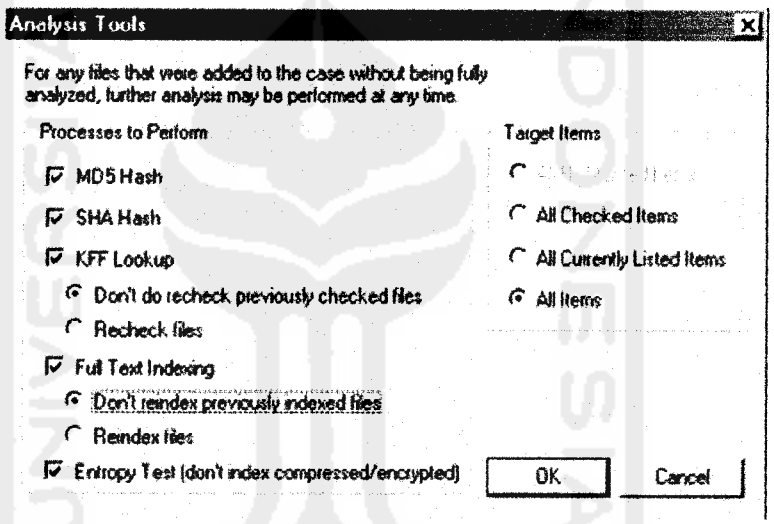
3. *Memverifikasi integritas Image*
Image yang ditemukan bisa saja memiliki media yang buruk atau memang sengaja dirusakkan. Untuk memvalidasi integritas kasus yang sedang ditangani, FTK dapat menghandel barang-barang bukti yang telah berubah dari bentuk orisinilnya. Fitur ini hanya dapat bekerja dengan image yang memang terolah dari dirinya sendiri seperti EnCase, SMART image.
Untuk memverifikasi integritas Image, FTK mengkomparasikan file yang didapatkan dengan sumber orisinilnya.



Gambar 23 Memverifikasi Integritas Image

4. *Menggunakan Tools Analisis*

Ketika pada tahapan setiap bukti telah teridentifikasi dalam kasus, tahapan berikutnya adalah penggunaan Tool Analisis untuk memeriksa Hash, mengenerate hash, membandingkan database hash dengan KFF database, atau mengindex file :



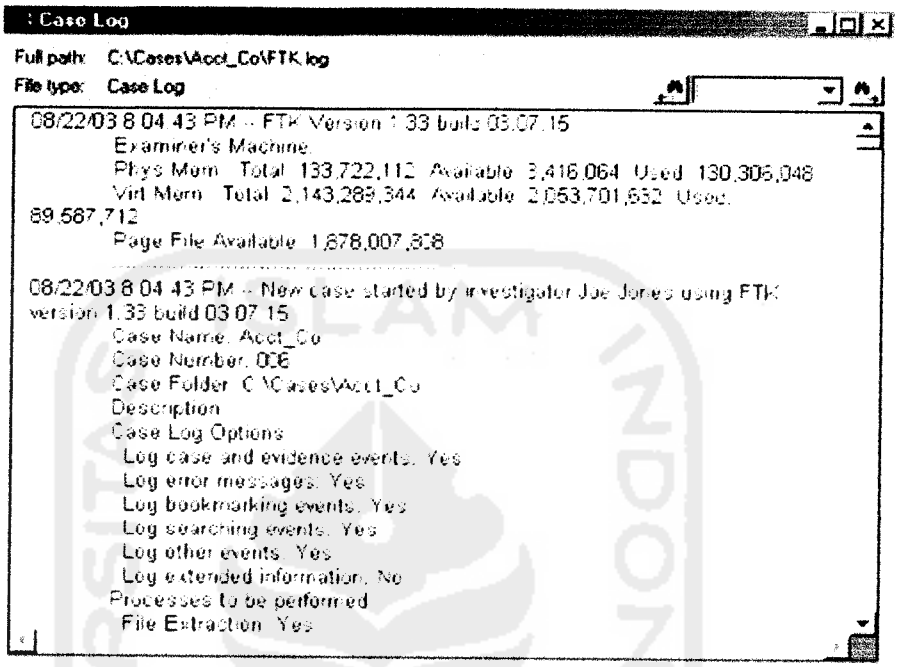
Gambar 24 Tools Analisis

Item-item yang menjadi penting dalam tools analisis adalah :

- MD5 Hash : akan menciptakan digital Fingerprint (Penanda Keotentikan) yang akan digunakan untuk memeriksa integritas file atau membedakan dengan file yang menjadi duplikasi.
- SHA Hash : akan menciptakan digital Fingerprint (Penanda Keotentikan) yang akan digunakan untuk memeriksa integritas file atau membedakan dengan file yang menjadi duplikasi. Secara default, fitur ini tidak dicheck, sehingga untuk menggunakannya harus di check terlebih dahulu.
- KFF Look up : akan menggunakan database KFF, dimana berperan dalam mengeliminasi file-file yang terabaikan, akan memberitahukan file-file yang rusak, atau dalam keadaan tidak pantas pakai.
- Full Text Indexing : Akan meng-index aktivitas keybord dalam kaitannya dengan kasus bukti.

- Entropy Test : Akan menidentifikasi file yang ter-enkripsi atau terkompress.

5. *Menggunakan Log Kasus(Case Log)*
Merupakan alat pendokumentasian untuk setiap aktivitas penelitian atau penyelidikan yang akan merekam secara otomatis.



Gambar 25 Penggunaan Log Kasus

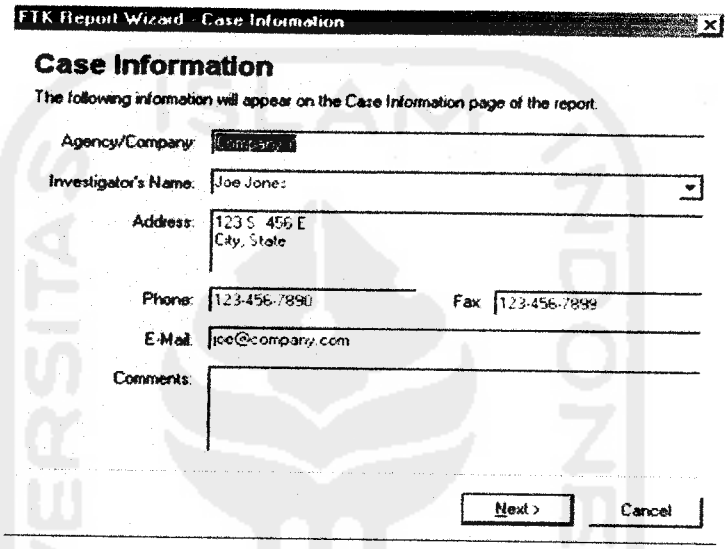
- Case and Evidence Events : Setiap even yang terkait dengan pemrosesan barang bukti atau ketika menggunakan tools analisis dalam setiap waktunya.
- Error Messages : Terkait dengan pesan eror yang diterima ketika pemeriksaan bukti.
- Bookmarks Events : Terkait dengan modifikasi bookmark atau penambahan-penambahan pada bookmarks.
- Searching Events ; Terkait dengan aktivitas pencarian dan hasil yang telah ditemukan.

2.4 Presentasi bukti digital *(Presentation of Digital Evidence)*

Pada tahapan terakhir ini akan digunakan Fitur bawaan dari software anaysis sebelumnya (***Forensics ToolKit***), dimana akan melaporkan secara terperinci hal-hal yang telah dilakukan berkenaan dengan proes investigasi. Laporan akan disampaikan dalam format HTML dengan web browser standar.
Dikatakan tahapan terakhir, karena pada tahapan inilah yang akan menjadi bahan investigator dalam merumuskan perihal kebenaran yang kemudian akan diajukan dalam proses pengadilan.

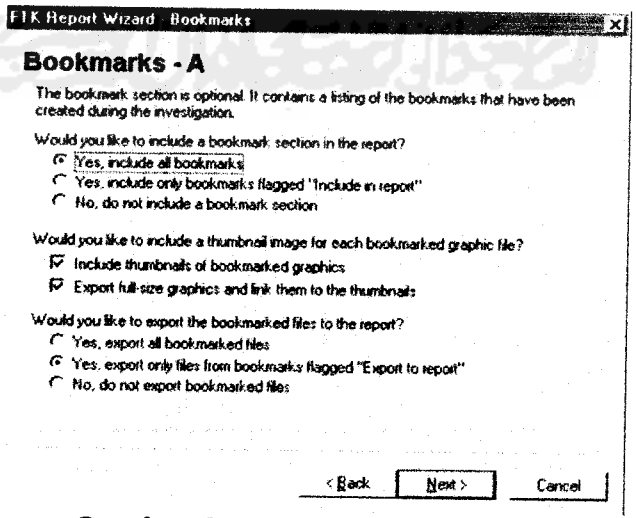
Step pertama.

Pada step ini, investigator akan mengisi informasi dasar yang diperlukan sebagai informasi pokok. Seperti dinyatakan dalam gambar dibawah ini.



Gambar 26 Presentasi Step Pertama

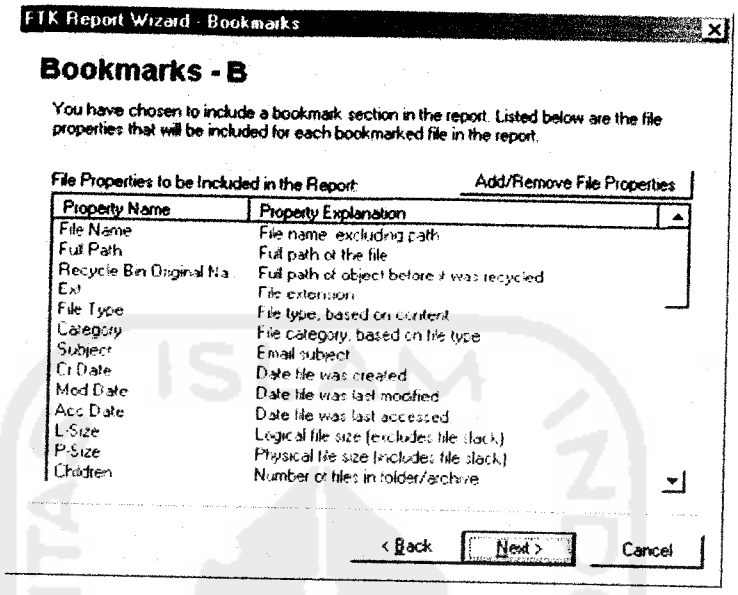
Step kedua
Pada step berikutnya, Pengelolaan terhadap bookmark, memungkinkan akan adanya laporan bookmark yang telah dibuat, modifikasi yang menjadi bahan tambahan (*bersifat opsional*)



Gambar 27 Presentasi Step Kedua

Step ketiga

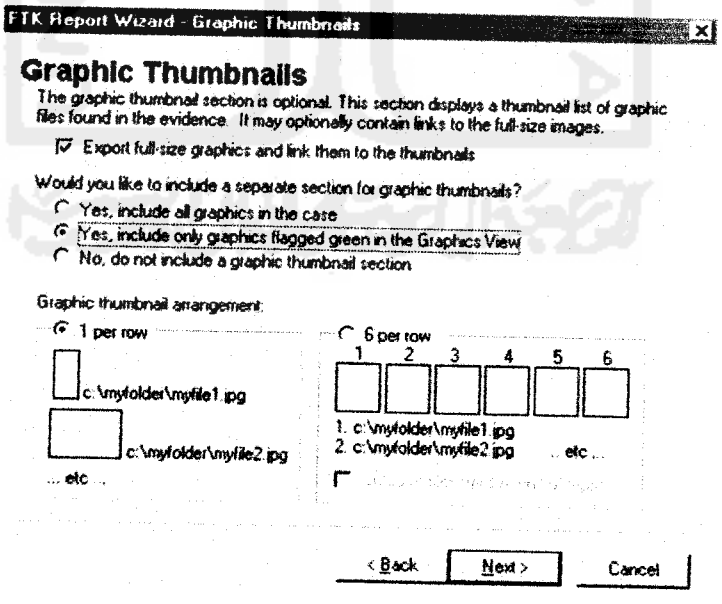
Step berikutnya inilah yang akan mengeksplore terhadap properti-properti apa sajakah yang akan ditampilkan dalam Bookmark sebelumnya. Ketika pada step kedua tadi bookmark tidak dipilih, maka step ke tiga ini tidak muncul.



Gambar 28 Presentasi Step Ketiga

Step Keempat

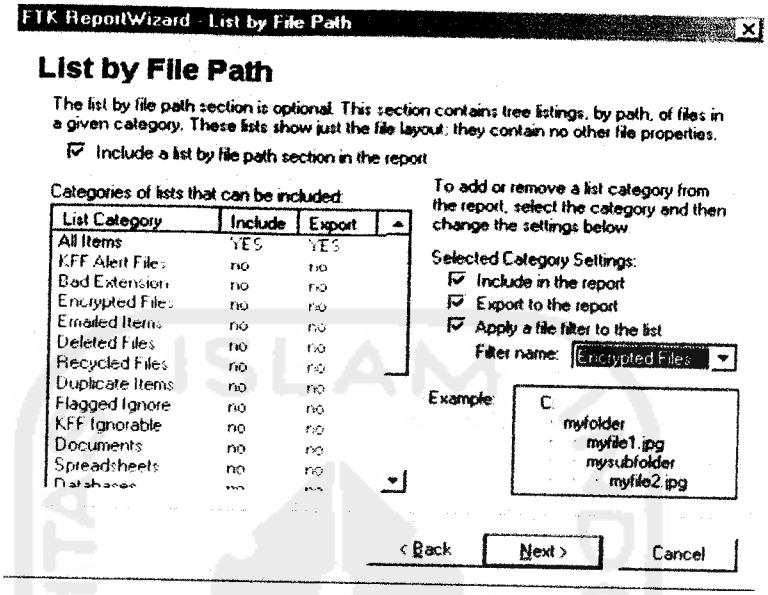
Pada step berikut, adalah untuk memudahkan investigator untuk membuat tampilan thumbnails dalam setiap gambar(graphic) yang diperoleh. Settingan nampak seperti gambar dibawah ini.



Gambar 29 Presentasi step Keempat

Step Kelima

List File by Path memungkinkan untuk membuat list laporan menurut kategori-kategori. Pada step ini laporan dapat disusun dengan settingan yang lebih sederhana secara tampilan. Dengan mencantumkan file beserta sumber-sumbernya*(bersifat opsional).*

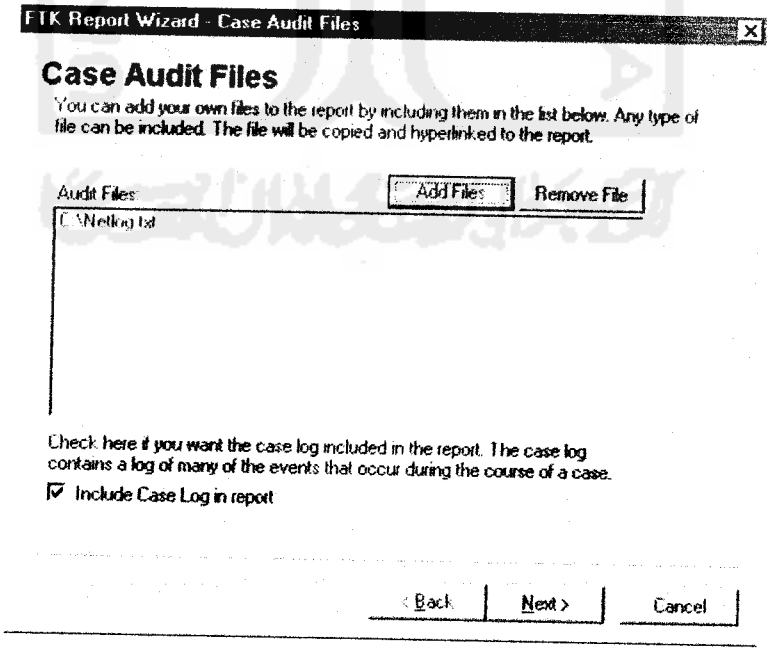


Gambar 30 Presentasi Step Kelima

Step keenam

Menambah File Audit dan Case Log

Pada step ini memungkinkan untuk menambah file-file yang diperlukan untuk audit dan Case Log seperti list Hash atau hasil pencarian untuk menjadi komponen laporan. Aktivitas Case Log juga dapat ditambah sebagai pelengkap rekaman tentang aktivitas penginvestigasian.

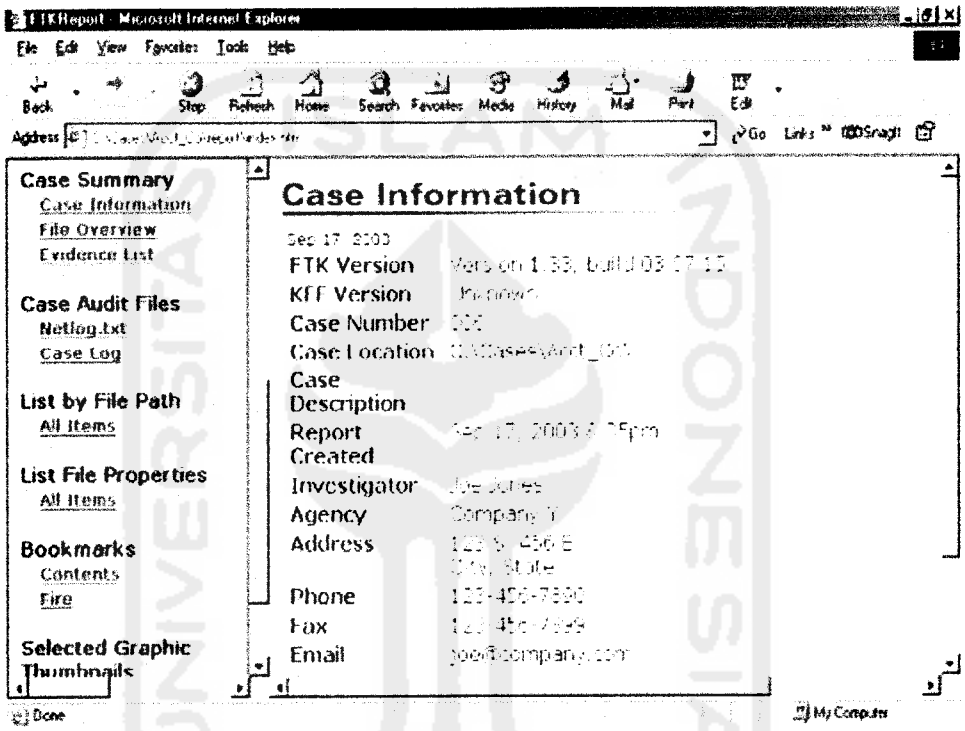


Gambar 31 Presentasi Step Keenam

Step tambahan (Finishing)
Pada step ini dapat ditambahkan seperti logo perusahaan atau gambar-gambar pelengkap sebagai tambahan untuk laporan yang memadai.

Hasil Laporan

Ketika setiap step telah dilalui, laporan yang disusun telah dapat dilihat. Seperti diungkapkan diawal bahwasanya laporan berekstensi .HTML dan dapat diakses melalui web browser standar yang umum digunakan, tanpa ada ketentuan versi tertentu (IE, Mozila, Opera, Fireworks dll.)



Gambar 32 Halaman Laporan

Pada gambar diatas memaparkan bagaimana sebuah laporan berhasil tersusun. Item-item yang diperlukan berada pada lajur sebelah kiri.
Item per item telah dieksplorasi pada setiap langkah sebelumnya. Tersedia juga pembuatan database secara otomatis *(DBMS: Microsoft Acces/.mdb)* yang untuk membukanya dapat langsung di*Open* atau di*save* terlebih dahulu pada harddisk lokal.

3. Penutup

Pemakaian software Activity Monitoring (semacam PCSPY) hendaknya juga memperhatikan kemampuan software terkait, maksudnya ada beberapa fitur software yang bisa dijalankan pasca peristiwa ataupun pra-peristiwa. Sehingga pemakaian fitur tersebut tepat dengan sasaran yang dituju.

Penting kiranya untuk diketahui setiap investigator yang bertindak di lapangan dalam mengetahui peranan, kelebihan, kekurangan Software forensik. Karena setiap investigasi digital, apalagi dengan makin kompleksnya modus cybercrime, menjadikan peranan software ini tidak lagi sebagai pelengkap semata bahkan menjaadikan sebuah kebutuhan yang harus dipergunakan.

Pada paparan diatas hanya menggambarkan sebagian saja tentang software forensik yang umumnya dipakai dalam proses penyelidikan. Penyusunan *review* hanya memaparkan perihal penting berkaitan dengan proses investigasi. Banyak fitur yang tidak disinggung dikarenakan keterbatasan topik bahasan, tempat, waktu dan lain-lain. Akhirnya, seorang investigatorlah yang memiliki faktor vital dalam setiap pengungkapan kebenaran.

4. Glossary

- Background : Bekerja beriringan dengan yang lain
- Capture : Menangkap aktivitas
- Clone : Mencetak tiruan ulang
- Opsional ; Bersifat Pilihan (bisa digunakan atau tidak)
- Review : Menampilkan ulang
- Vital : Bersifat Penting

5. Daftar Pustaka

[WAR06] Anonim, Aplikasi PCSPY http://www.WareSight.com, diakses pada Desember 2006

[SYM06] Anonim, Situs resmi NORTON, **Symantec Corporation** (www.symantec.com), diakses pada Desember 2006

[ACC06] Anonim, Manual Book Forensics Tool Kit dari **AccesData Corp** (www.accessdata.com), diakses pada Desember 2006

[FOR06] situs www.forensics-intl.com/def2.html, diakses pada november 2005

LAPORAN PROJECT KETIGA

TUGAS AKHIR NON SKRIPSI

Studi Kasus Cybercrime dan Metode Penanganannya

DISUSUN OLEH :

Dedy Setyo Afrianto.
02.523.229

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

Desember 2006

Studi Kasus Cybercrime dan Metode Penanganannya

Project ke-3 Tugas Akhir Non Skripsi
Oleh : Dedy Setyo Afrianto (02 523 229)
Jurusan Teknik Informatika, Fakultas Teknologi Industri
Universitas Islam Indonesia
e-mail : dedysetyoa@students.fti.uii.ac.id

Studi Kasus Pertama; Aktivitas Carding dalam dunia Bisnis

Abstraksi

Landasan teoritis untuk mengungkap kasus cybercrime sangat menarik untuk difollowupi lebih lanjut. Perlunya arahan teoritis kadangkala akan menjadi tidak singkron ketika tidak disertai dengan petunjuk teknis dalam mengimplementasikan keilmuan. Artinya, setiap kasus yang terjadi akan menjadi lebih sederhana untuk diungkap kebenarannya ketika dalam landasan ilmiah itu disertai dengan studi real tindakan cybercrime.

Carding merupakan salahsatu varian modus operandi penjahat cyber dalam menjalankan aksinya. Carding atau disebut juga fauder adalah kegiatan penyalahgunaan kartu kredit(uang/rekening) yang bukan hak miliknya. Dalam menjalankan aksinya, pemanfaatan kartu kredit ini sering dipergunakan melalui aktivitas transaksi jalur online yang tentu saja tidak memerlukan tatap muka antara si peminta dan si penawar, seperti e-commerce, e-buy, pentransferan rekening dll.

Tulisan dalam project ke tiga ini akan memaparkan studi kasus tentang kejahatan Carding beserta langkah-langkah penyikapannya.

1. Pendahuluan

Pada project ketiga ini akan memaparkan studi kasus carding fiktif berikut cara pengungkapan kebenaran dari investigator. Skenario ditujukan untuk mengetahui secara lebih rinci aktivitas carding. Beserta teknik metodologis penyelesain masalah.

Masing-masing subbab menjelaskan perihal

- Skenario Kasus : Kejadian naratif kejahatan berikut data-data yang disediakan.
- Follow-up kasus : Tindak lanjut kasus untuk memperoses lebih mendalam dari tindak kejahatan yang dilakukan
- Pemetaan kasus : Memaparkan poin-poin penting yang hendaknya diperhatikan karena bersifat vital
- Penindakan : Menentukan secara bertahap langkah-langkah yang ideal untuk dilakukan sampai kepada hasil.
- Modus Operandi Carding : Menyebutkan salahsatu teknik dan trik untuk melakukan operandi kejahatan carding.

2. Skenario Kasus :

Seorang nasabah bank ABC yang memiliki kartu kredit (bernama fulan), pada suatu ketika mendapati bahwa rekening dalam kartu kreditnya berkurang tujuh juta rupiah. Padahal dalam kurun waktu seminggu terakhir dia tak pernah menggunakan kartu kreditnya untuk aktivitas apapun. Fulan ini yakin benar bahwa rekening dalam kartu kreditnya semula sejumlah Rp.12 juta, keyakinan ini

juga dibuktikan dengan adanya bukti saldo terakhir yang didapatkan dari bank tepat seminggu sebelum kejadian. Berarti, sekarang rekening dalam kartu kreditnya hanya berisi lima juta rupiah. Tanpa pikir panjang komplain dia ajukan kepada pihak bank ABC untuk mengetahui kenapa terjadi demikian, serta untuk menjaga dari hal-hal yang tak diinginkan, Fulan menutup sementara rekening kartu kreditnya di bank ABC untuk batas waktu yang tak ditentukan.

3. Follow-up kasus :

Setelah proses komplain diajukan, pihak bank ABC mengeluarkan skrip detail transaksi yang telah terjadi selama seminggu terakhir. Akhirnya, didapati transaksi yang menyebutkan bahwasanya telah terjadi pembelian di toko online "e-lectronic" dan juga pembayaran jasa layanan Delivery komersiil yang jika ditotal akan bernilai tujuh juta rupiah.
Dengan didampingi oleh pihak ABC dan kepolisian, Fulan mengkonfirmasi keberadaan transaksi "tak terduga" ini. Bukan seperti dugaan Fulan yang mengira telah terjadi kekeliruan administratif belaka, e-lectronic pun memiliki bukti transaksi valid yang menyebutkan bahwasanya pembelian Laptop telah dilakukan atas nomor rekening dan nama lengkap Fulan pada waktu tertentu.
Karena e-lectronic memiliki mitra bisnis dengan perusahaan Delivery swasta, permasalahan tidak berhenti disini, karena untuk permasalahan ini, pihak Delivery pun terlibat karena bertanggungjawab mengantarkan paket barang pesanan sampai kepada tujuan.

Secara sederhana, gambaran kasus seperti ilustrasi di bawah ini

Gambar 1 Ilutrasi kasus

-------→	: Alur Barang didapatkan
1	: Transfer Rekening
2	: Mengirimkan Barang Sampai pada alamat tujuan

4. Pemetaan kasus :

1. Uang rekening berkurang Rp.5 juta secara tak terduga dan dibuktikan secara valid.
2. Terjadi pemesanan via website kepada pihak e-lectronic oleh ip address yang berhasil terekam.
3. Terdapat elemen-elemen yang terlibat dalam kasus, yakni, Bank ABC, toko online e-lectronic, Delivery Service.
4. Bukti yang didapatkan, Laptop senilai Rp.6.750.000, 00, skrip transaksi pihak bank dan e-lectronic, rekening uang dan ip address pemesan.

5. Penindakan :

Poin-poin yang harus diperhatikan :

- Barang bukti berupa Laptop dapat didapatkan kembali dari alamat tujuan yang telah tercatat dalam data Delivery service. Tentu saja dalam tahapan penyelidikan ini tetap memegang asas "praduga tak bersalah" dengan bermitra kepada pihak yang berwenang.
- Informasi ip address yang didapatkan dari pihak e-lectronic memegang kunci penting dalam mengungkap siapa pelaku kejahatan.

- Pembagian peran (seperti diterangkan pada project 1) harus jelas, artinya dalam setiap penindakan modus kejahatan ada peranan yang berfungsi sebagai Officer, Investigator atau Teknisi khusus. Pada paparan dibawah ini lebih detail diexplorasi pada fungsi investigator dalam perannya berkenaan dengan bukti-bukti (evidences), *dimulai Langkah 4*.

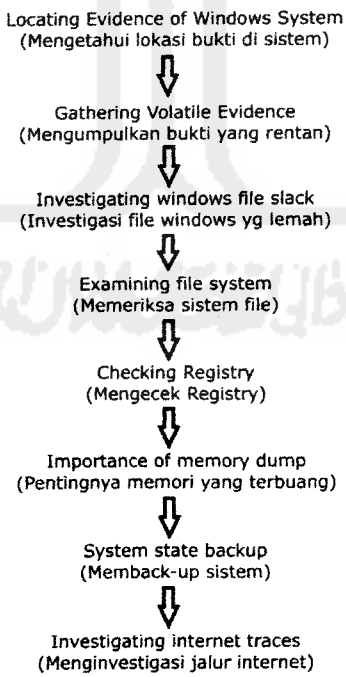
🗁Langkah 1
Penyusuran dapat dimulai dari informasi ip address yang telah didapatkan dari pihak e-lectronic(untuk toko on-line yang memiliki skala besar, umumnya memiliki fasilitas yang dapat melacak alamat ip pembeli)

🗁Langkah 2
Setelah ip address terlacak, dapat dideteksi di wilayah mana ip komputer ini berasal. Lokasi ip sama halnya seperti penomoran pada plat kendaraan atau nomor telepon yang telah memiliki kode area khusus yang telah ditentukan. Atau dapat menghubungi APJII (Asosiasi Penyedia Jasa Internet Indonesia) untuk informasi ip secara lebih mendetail.

🗁Langkah 3
Setelah berhasil disusuri serta lokasi berhasil didapatkan, dapat dimulai dengan memeriksa komputer yang memiliki indikasi telah dipakai bertransaksi. Pada kasus ini ternyata berhasil didapatkan bahwa ip pembeli didapatkan di salah satu warnet di Yogyakarta. Setelah berkomunikasi dengan operator warnet, Komputer untuk bertransaksi juga telah didapatkan.

🗁Langkah 4
Pada langkah inilah, tugas/peranan investigator dalam melacak tindak kejahatan lebih spesifik pada pengungkapan bukti dari fakta-fakta yang ada.

Tahapan yang umum (tidak secara baku) dilakukan dalam pengusutan tindak kejahatan oleh investigator adalah :



Gambar 2 Tahapan Umum Investigasi

ſ Locating Evidence of Windows System

Penting sekiranya untuk diketahui, bahwasanya keberadaan orang pertama (As a first Responder) yang tahu tentang gejala yang terjadi pada sistem. Sehingga ketika terjadi 'hal janggal', mampu mendeteksi kesalahan sejak dini sehingga harapannya tidak terjadi masalah yang lebih akut. Pada kasus tersebut, posisi ini terletak pada Fulan.

ʃ Gathering Volatile Evidence

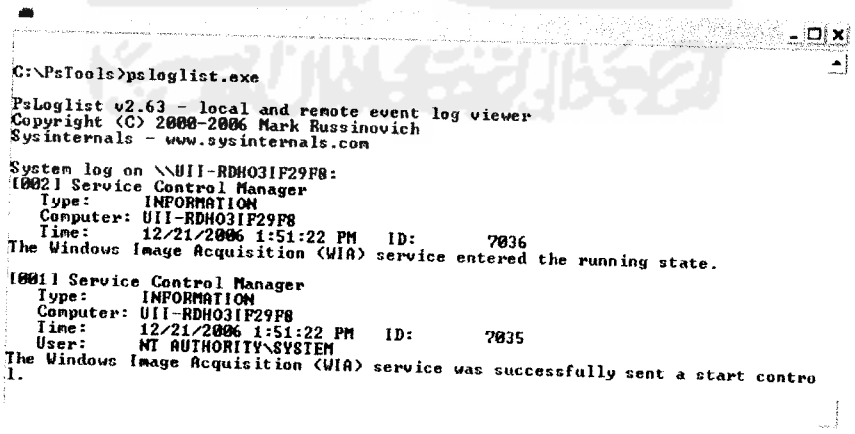
Pada sesi ini, mengumpulkan bukti-bukti vital dapat dilakukan dengan mengkloning terlebih dahulu Harddisk yang didapatkan sebagai bukti (*pada project 2 dengan menggunakan Norton Ghost 2003 dari symantec, dapat menjadi sebuah pilihan*)atau perangkat hardware lain manakala diperlukan. Pengkloningan menjadi penting untuk dilakukan, karena selain untuk menjaga validitas bukti yang tercopy, juga untuk menjaga bukti otentik dari kerusakan-kerusakan yang ditimbulkan akibat pemeriksaan.

ʃ Investigating Windows file Slack + Examining file system

Pada data hasil pengkloningan kemudian dapat diteliti, file-file mana saja yang dapat ditangkap untuk kemudian dapat dijadikan bukti. Penggunaan software seperti PCSPY (dipaparkan pada project 2) dapat dijadikan alternatif. Artinya, dengan merujuk pada data waktu yang diberikan oleh e-lectronic ketika transaksi online berlangsung. Penggunaan software ini dapat langsung secara spesifik melacak aktifitas apa yang sedang terjadi pada komputer yang bersangkutan pada tanggal dan hari tersebut secara lebih detail.

Namun, kesulitan yang terjadi adalah manakala pihak warnet (pada studi kasus ini) tidak menginstalasikan software ini atau software pemantau (monitoring) lainnya. Karena penggunaan PCSPY bertindak sebagai 'kamera pengintai' (Pra/preventif) yang akan berjalan manakala telah terpasang pada sistem, berbeda ketika software ini belum terinstal, software tidak akan berfungsi optimal bahkan tidak sama sekali.

Alternatif perangkat pembantu yang dapat digunakan adalah penggunaan Pstools. Software ini bersifat gratis (freeware) karena dibuat oleh microsoft khusus untuk mengatasi hal-hal demikian. Software ini akan dapat langsung berfungsi walaupun juga telah terjadi rangkaian kasus(Paska). Fitur yang dapat dipakai salahsatunya adalah PsLogList. Perintah yang diinstruksikan dengan tampilan MSDOS yang dapat dieksekusi melalui command prompt. Informasi lebih lanjut dapat melalui alamat http://download.sysinternals.com/Files/PsTools.zip. Berikut contoh tampilan aplikasi yang berhasil tereksekusi



Gambar 3 Aplikasi PsTools

Pada gambar diatas, system akan secara otomatis merekam aktivitas baik yang sedang maupun telah terjadi, walaupun program ini diinstalasikan pada akhir peristiwa.
Secara visual juga ada informasi yang ditampilkan dan memegang peranan penting sebagai informasi, diantaranya Type(log), Computer(nama user), Time(waktu kejadian).

ƒ Checking Registry
Registry merupakan tempat penyimpanan database tentang konfigurasi setting komputer. Bersifat built-in dalam Windows OS, sehingga tanpa harus menginstal lagi. Memiliki sifat yang dapat menangkap apapun aktifitas user dalam penggunaan komputer. Dengan sifat inilah, yang dapat menyebabkan kenapa registry merupakan salah satu tools penting untuk mengungkap kejahatan komputer. Namun, penggunaan yang secara visual toos ini akan terasa rumit untuk orang awam, walaupun juga tidak bisa dibilang mudah unutk proses investigasi bagi seorang investigator karena memang terkait dengan kompleksitas informasi yang tersedia, peletakan yang beralur panjang, kebiasaan dll. Dengan adanya landasan demikian, penggunan tools pembantu untuk pemanfaatan registry dengan segenap kelebihannya menjadi penting untuk dipakai. Salah satu tools yang dapat dipakai adalah RegSeeker dari hoverdesk. Informasi lebih lanjut dapat dicari di alamat (http://www.hoverdesk.net/freeware.htm). Salahsatu tampilan program yang berhasil dieksekusi seperti di bawah ini.

Gambar 4 Aplikasi RegSeeker

ƒ Importance of Memory Dump
Membantu mengecek penggunaan Memory yang terpakai ketika kegagalan mengeksekusi program, selain itu digunakan juga untuk mendiagnosa bugs yang terdapat dalam sistem. Memory dump file merekam setiap penghentian program komputer secara tidak normal. Windows akan senantiasa menyimpan setiap memory dump pada %SystemRoot%/Minidump folder. Sehingga penggunaan memory dump akan melacak penggunaan program yang mengindikasikan terjadinya kejahatan komputer.

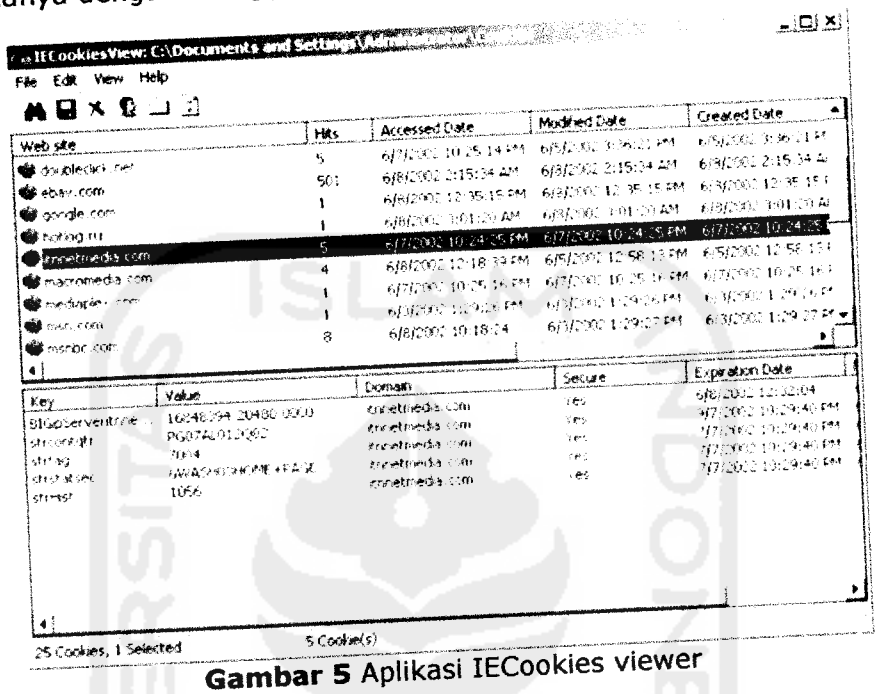
ƒ System state back-up
Pada level ini sebenarnya sudah terpenuhi pada sesi ke dua yang lalu (Gathering volatile Evidence), karena idealnya untuk mengolah bukti otentik adaalah sangat riskan, sehingga back-up bukti-bukti otentik akan lebih baik digunakan pada awal pengumpulan. Namun pada kasus kejahatan yang lain pemback-up an bukti sebenarnya berperan juga sebagai bukti kedua (cadangan) sehingga resiko kerusakan bukti otentik dapat teratasi dengan menggunakan model ini.

ʃ Investigating Internet Traces

Pelacakan jalur internet yang terpakai dapat menggunakan fasilitas pada web browser dengan melihat pada

- Cookies

Akan lebih detail dan maksimal ketika menggunakan tools pembantu, salahsatunya dengan menggunakan IECookiesView.

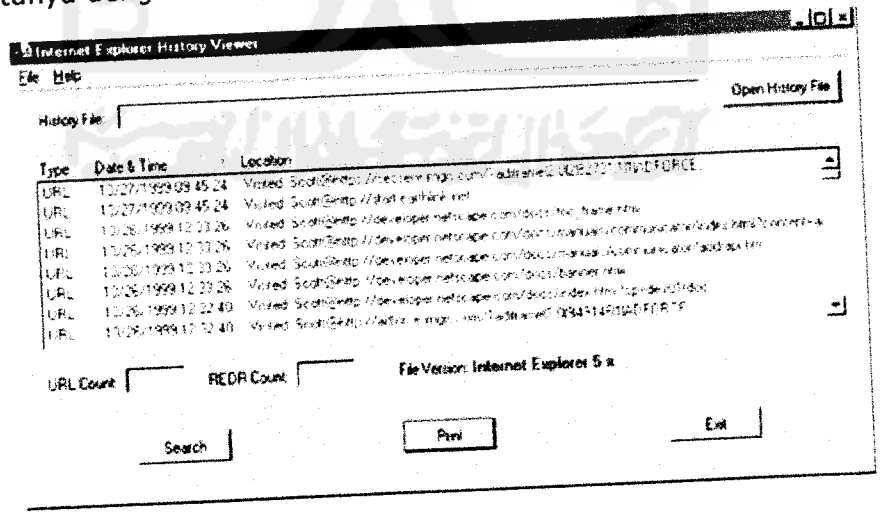


Gambar 5 Aplikasi IECookies viewer

- History

Merupakan rekaman secara otomatis yang akan memantau halaman-halaman mana saja yang telah diakses oleh user.

Akan lebih detail dan maksimal ketika menggunakan tools pembantu, salahsatunya dengan menggunakan Internet Explorer History Viewer.



Gambar 6 Aplikasi IE History Viewer

6. Modus Operandi Carding

Dibawah ini akan ditunjukan salahsatu teknik kejahatan carding yang varian dari penggunaannya tentu saja akan beragam.

Untuk memulai carding, biasanya para carder menggunakan langkah-langkah berikut ini:

(I) menyiapkan credit card valid (biasa disebut cc), untuk mendapatkan cc ada beberapa cara :

I.1. memanfaatkan bugs (lubang, celah keamanan) pada shopping cart, seperti comersus,vp-asp,cart32, Eshop, Sales Cart,dll.
Contoh: bugs comersus shopping cart adalah http://target.com/comersus/database/comersus.mdb
1.cari target situs dengan comersus shopping cart. Caranya buka google ketik allinurl:comersus ("inurl:" ialah sintaks perintah untuk membatasi pencarian yang hanya menghasilkan semua URL yang hanya berisi kata kunci informasi yang dimaksudkan)
2.contoh kita dapat situs dengan comersus shopping cart http://contohnya.com/comersus/store/XXXXX.asp
3. lalu rubah url situs tersebut menjadi http://contohnya.com/comersus/database/comersus.mdb
4. maka secara otomatis kita akan mendownload seluruh database (database adalah tempat berisinya semua informasi termasuk cc) milik target kita(http://contohnya.com). kamu bisa membukanya dengan Ms Access. (.mdb adalah file yang berextensi database).
Untuk contoh target bug shopping comersus bisa didownload disini: http://rapidshare.com/files/3187738/contoh_target_bug_comersus.txt.html

Untuk bugs2 shopping cart bisa dilihat disini: http://jafarhabsyi.blogspot.com/2006/03/cara-dapet-cc-credit-card.html
(untuk mendapat update bug shopping cart terbaru bisa kunjungi http://www.securityfocus.com atau http://www.securitytracker.com ketik pada seacrh "bugs shopping cart")

I.2. menggunakan teknik sql injection, teknik dimana kita bisa langsung masuk kedatabase target.(untuk mengetahui apa dan bagaimana sql injection, cari di google ketik sql injection). Atau download ebook sql injection : http://rapidshare.com/files/3180020/sql_ijection_carding.rar.html

I.3. membuat scam page (halaman konfirmasi palsu), scam page adalah suatu teknik atau cara mendapatkan data cc dengan melakukan konfirmasi bohongan, sehingga yang diberi konfirmasi (pengguna account) akan melakukan verifikasi dengan memasukan data yang diminta halaman scam tersebut. Ketika target memberikan data2nya (entah itu cc, paypal,ebay dll) pada scampage maka secara otomatis data2 tersebut akan dikirim pada sang pembuat scampage. Cara ini memang agak rumit, karena tentunya kita harus dibekali oleh pengetahuan tentang pemrograman website, seperti PHP misalnya. Namun scampage sangat istimewa karena secara tidak langsung akan mampu miminta semua data yang dibutuhkan. Scampage sangat efektif untuk mendapatkan data paypal, ebay, yahoo, dan berbagai data account lainnya.

I.4. memanfaatkan google, dengan menggunakan sintaks2 seperti **inurl** (("inurl:"

ialah sintaks perintah untuk membatasi pencarian yang hanya menghasilkan semua URL yang hanya berisi kata kunci informasi yang dimaksudkan), index of ("Index of " digunakan untuk mendapatkan situs yang menampilkan indeks browsing direktori.) dll.
Contoh:
* pencarian dalam pencarian,"inurl : database mdb". Pencarian akan menghasilkan semua URL yang hanya mengandung informasi tentang "database mdb".
*pencarian dalam allintitle: "index of /admin" (tanpa tanda kutip) akan menampilkan link pada site yang memiliki indeks browsing yang dapat diakses untuk direktori terlarang seperti direktori "admin".

I.5. menggunakan cc generator (software generator yang dapat meyediakan cc dengan mendekripsi nomor kredit) satu hal yang pasti software ini tidak menjamin menghasilkan 100% cc yang valid.

I.6. join (mirc) di channel #cc,#ccs,#cchome,#cvv2 di server2 seperti DALnet,UNDERnet,Efnet. Untuk indonesia #indocarder, #yogyacarding,#gresikcarding. Ketik !cc atau !cvv2.

I.7. membeli cc (biasanya para carding pemula lebih menyukai ini), untuk beli cc bisa di www.malaikat.info atau http://www.geocities.com/malaikatcarding/

(II) menyiapkan proxy, Proxy atau IP address adalah salah satu bagian terpenting dalam proses ini. Menurut mereka IP address akan mewakili keberadaan posisi saat melakukan aktivitas, artinya bila seorang carder memakai proxy amerika maka ia tentu saja akan terlihat sedang berada di amerika, begitu pula bila carder memakai proxy jepang misalnya maka tentu saja seakan-akan ia sedang berada dijepang. Dan berikut iniadalah proses dan teknik ketika mengganti proxy. Untuk proxy lebih lanjut bisa download "ebook carding porxy" . http://rapidshare.com/files/3177338/ebook_carding_proxy.rar.html

(III) modus pengiriman, untuk modus pengiriman ada beberapa macam:

A. Modus langsung :

para carder mengirimkan barang hasil carding mereka langsung ke suatu alamat di Indonesia. Biasanya menggunakan po.box atau mail box, tapi para carder lebih menyukai menggunakan mail box dari pada po.box karna biasanya merchant menolak mengirimkan barang yang beralamatkan po.box contoh : alamat mail box multiplus, Jl. Kyai Caringin No. 28 C Suite # 99 (seperti alamat rumah kan) sedangkan PO BOX 3176 Jakarta 10031

B. modus salah kirim:

para carder tidak lagi secara langsung menuliskan "Indonesia" pada alamat pengiriman, tetapi menuliskan nama negara lain. Kantor pos negara lain tersebut akan meneruskan kiriman yang "salah tujuan" tersebut ke Indonesia. Hal ini dilakukan oleh para carder karena semakin banyak merchant atau e-commere di Internet yang menolak mengirim produknya ke Indonesia. dengan mencantumkan nama negara lain, selain Indonesia, pada data alamat pengiriman. Pihak merchant tentu tidak akan curiga. Asalkan alamat jelas, ada nama kota dan kode pos Indonesia, maka meskipun nama negara yang ditulis adalah bukan Indonesia, perusahaan courier service akan berbaik hati dengan tetap mengantarkannya ke Indonesia. Salah satu nama negara yang menjadi

favorit para carder adalah Singapore.

C. Modus rekanan luar negeri:

para carder mengirimkan paket pesanan mereka ke rekan mereka yang berada di luar negeri. Kemudian rekan mereka tersebut akan mengirimkan kembali paket pesanan tersebut ke Indonesia secara normal dan legal. Hal ini dilakukan oleh carder selain karena modus operandi mereka mulai tercium oleh aparat penegak hukum, juga disebabkan semakin sulit mencari merchant yang bisa mengirim produknya ke Indonesia

D. Modus uang tunai:

sekarang, para carder lebih mengutamakan mendapatkan uang tunai. Caranya adalah dengan mentransfer sejumlah dana dari kartu kredit bajakan ke sebuah rekening di PayPal.com. Kemudian dari PayPal, dana yang telah terkumpul tersebut mereka kirimkan ke rekening bank yang mereka tunjuk. Cara lainnya adalah dengan melakukan penipuan, seolah-olah mereka menjual barang hasil carding, dan menjebak korban dengan meminta mengirimkan uang muka dalam jumlah tertentu kepada mereka

Studi Kasus Kedua; Investigasi *Wireless Network Attacking* (Serangan Jaringan Wireless)

Abstraksi

Dengan semakin pesatnya perkembangan teknologi wireless(tanpa kabel, maka) ancaman keamanan dalam dunia jaringan komputer tanpa kabel(Wireless LAN) merupakan hal yang niscaya adanya. Salahsatu modus yang sering dipakai adalah pencurian akses ke dalam jaringan. Karena, pencurian akses ini merupakan step dasar untuk modus kejahatan yang lain, keberadaannya seakan-akan menjadi 'pintu pertama' untuk level kriminal yang lebih lanjut.

Pada kasus kedua ini akan ditelaah lebih lanjut mengenai Serangan Jaringan Wireless(nirkabel-khususnya Wireless LAN) yang lebih berkonsentrasi pada aktivitas Pencurian Identitas. Sesi ini akan dijabarkan secara umum tentang aktivitas MAC Spoofing dan Filtering, kemudian akan dipaparkan secara terperinci pada setiap sub-bab nya yang meliputi antara lain :

- *Pendahuluan : Mengenalkan tentang konsep jaringan secara umum*
- *Pengenalan Modus Pencurian identitas : memaparkan konsep cybercrime yang hendak ditangani.*
- *Skenario Kasus : narasi kasus beserta keterangan yang dibutuhkan untuk proses pengolahan.*
- *Pemetaan Kasus : poin-poin penting yang menjadi perhatian.*
- *Anatomi Serangan : memaparkan pola serangan (dari subbab 2)*
- *Investigasi Forensik : mengolah kasus untuk mendapatkan barang bukti*

1. Pendahuluan

Saat ini, perkembangan dalam bidang teknologi informasi telah mengarah pada penggunaan teknologi tanpa kabel atau dikenal dengan istilah *wireless.* Dimulai dengan teknologi pager, kemudian telepon tanpa kabel (*cellular phone*), dan berkembang hingga teknologi *bluetooth*. Begitu juga dengan dunia Networking (Jaringan), LAN(Local Area Networking), dari yang semula menggunakan kabel dalam penggunaan infrastrukturnya, lambat laun "pengkabelan" ini menjadi suatu hal yang kurang reliable lagi untuk standar mobilitas, jarak, pengecekan problem, bahkan sampai kepada biaya infrastruktur serta efektifitas dan produktifitas kerja. Sehingga pengalihan metode menjadi hal yang tak terelakkan lagi dalam dunia networking (Wireless Networking), menjadi Wireless LAN (selanjutnya disebut W-LAN).

Namun, walaupun sebagai terobosan teknologi mutakhir, lagi-lagi masalah keamanan masih dianggap sebagai salah satu kelemahan dalam penerapan W-LAN. Hal ini terjadi karena perkembangan masalah keamanan pada W-LAN tidak sepesat penerapan dan perkembangan teknologi W-LAN itu sendiri.

Secara umum masalah keamanan pada Wireless LAN timbul karena[1] :

1. Tipikal Konektivitas Wireless LAN itu sendiri.
Seperti yang kita ketahui, komunikasi pada wireless LAN terjadi dengan memanfaatkan gelombang radio. Jadi di sekitar jaringan akan terdapat sinyal gelombang radio yang dipancarkan. Sinyal Wireless LAN secara normal dapat mencapai radius 200 meter. Oleh karena jauhnya radius sinyal ini, kemungkinan masih bisa tertangkap ketika seseorang memiliki perangkat yang sesuai memiliki potensi yang besar. Dari sinilah kemudian akses keamanan menjadi bahasan tersendiri.

[1] Jhonsen, Jhon Edison, "*Membangun Wireless LAN*", Jakarta : Penerbit PT Elex Media Komputindo Kelompok Gramedia Jakarta, Januari 2006

Hal ini berbeda dengan jaringan konvensional yang menggunakan media kabel untuk berkomunikasi. Untuk dapat mengakses sebuah jaringan, seseorang harus terhubung dengan kabel jaringan yang ada.

2. Kelalaian Manusia (Human Error), khususnya Administrator

Selain masalah diatas, lemahnya keamanan pada W-LAN juga sering diakibatkan karena lalainya administrator jaringan yang membiarkan perangkat W-LAN terpasang pada konfigurasi default. Konfigurasi default yang dimaksudkan adalah konfigurasi yang tidak mengaktifkan fungsi-fungsi dasar perlindungan terhadap W-LAN, seperti enkripsi, membiarkan Acces point menggunakan nama SSID defaultnya, dan lainnya.

2. Pengenalan Modus Pencurian Identitas

Serangan ini memanfaatkan kelengahan pengguna W-LAN sehingga mereka terjebak dengan memberikan data login mereka kepada attacker. Dengan memanfaatkan ESSID yang serupa dengan access point yang sebenarnya dan alamat MAC yang sudah dipalsukan, mereka membuat aplikasi palsu yang menyerupai aslinya, sehingga orang yang memiliki login secara tidak sadar akan memasukkan nama pengguna dan kata kunci yang biasa dipakainya untuk masuk ke dalam jaringan W-LAN. Setelah mendapatkan data login tersebut, attacker akan dengan leluasa masuk ke dalam jaringan W-LAN seakan-akan sebagai pengguna yang sah. Selanjutnya ia akan menikmati akses internet gratis, melihat-lihat file di dalam jaringan, bahkan kejahatan-kejahatan dapat dirancang dengan relatif mudah sesudahnya.

Cara yang paling banyak digunakan adalah dengan melakukan *MAC Spoofing*[2]. Cara ini digunakan untuk mematahkan metode keamanan W-LAN dengan menyimpan daftar wireless client yang diperbolehkan mengakses. Access Point menyimpan daftar alamat MAC dari perangkat wireless client agar dapat melakukan koneksi. Metode ini dikenal sebagai MAC Address filtering. Dengan melakukan pengubahan alamat MAC dari perangkat wireless client, seorang penyusup berpura-pura menjadi komputer yang telah diotentifikasi.

- *Mengganti MAC Address*

Kalimat "MAC ADDRESS SPOOFING" dalam konteks ini berhubungan dengan penyerang yang mengganti mac address kepada nilai yang lain. Konsep ini berbeda dengan IP ADDRESS SPOOFING tradisional yang lain dimana penyerang mengirimkan data dari sumber alamat yang sewenang-wenang dan tidak mengharapkan untuk melihat respon dari sumber IP ADDRESS yang aktual. MAC ADDRESS SPOOFING mungkin lebih akurat menggambarkan sebagai "penyamaran" atau "pemeranan" MAC ADDRESS sejak penyerang menyiasati data dengan sumber yang berbeda daripada alamat transmiting mereka. Ketika penyerang mengganti MAC ADDRESSnya, mereka melanjutkan untuk memanfaatkan kartu wireless yang diharapkan untuk tujuan transport layer 2, transmiting dan menerima dari sumber MAC yang sama.

Kebanyakan semua kartu 802.11 memiliki akses untuk penggantian MAC ADDRESS, seringkali dengan support penuh dan driver dari pabrik. Penggunaan driver opensource LINUX, seorang user dapat mengganti MAC ADDRESS dengan tool ifconfig, atau dengan sebuah program C pendek yang disebut ***fungsi ioctl()*** dengan bendera **SIOCSIFHWADDR**.

[2] PC PLUS (PC+), "*Membangun Wireless LAN mudah dan murah*", Jakarta : PT Prima Infosarana Media, Desember 2006

mengganti MAC ADDRESS mereka dengan memilih properti driver network card mereka dalam applet control panel jaringan.

Seorang penyerang mungkin dapat memilih untuk mengganti MAC ADDRESS untuk beberapa alasan, diantaranya *menyamarkan kehadiran jaringan*, untuk *membypass akses list control*, atau *berkedok user yang terotentifikasi*. Masing-masing akan dieksplorasi seperti dibawah ini

Menyamarkan kehadiran jaringan: Seorang penyerang mungkin akan memilih untuk mengganti MAC ADDRESS mereka dalam percobaan untuk menghindarkan sistem Pendeteksi Gangguan jaringan (Network Intrusion Detection System-NIDS). Kebanyakan contoh dari penyerang mengeksekusi skrip serangan **brute force** dengan sebuah MAC ADDRESS untuk masing-masing percobaan koneksi yang sukses. Seperti sebuah serangan yang akan men-*un*deteksi oleh aplikasi analisis aktivitas jaringan semacam **NetFlow** yang melaporkan aktivitas layer lebih tinggi jaringan atau kuantitas lebar dalam lalu lintas dari sebuah sumber alamat.

Membypass Daftar Kontrol Akses: Menggunakan form dasar kontrol akses W-LAN, administrator biasanya memiliki pilihan untuk mengkonfigurasikan AP atau router yang berdekatan untuk mengijinkan hanya MAC ADDRESS yang terregistrasi saja dalam berkomunikasi di jaringan. Seorang penyerang mungkin akan mengelakkan form akses control dengan *passive monitoring* di jaringan dan menghasilkan daftar MAC ADDRESS yang mengotorisasi untuk berkomunikasi. Dengan daftar MAC ADDRESS yang terdaftar ditangan, seorang penyerang bebas untuk mengeset MAC ADDRESS mereka ke alamat yang syah, membypass mekanisme keamanan yang diharapkan.

Penyamaran user yang terotentifikasi : kemanan hardware WLAN tertentu device otentik mempercayakan pertemuan otentifikasi user dengan sumber MAC ADDRESS klien. Setelah user sukses mengotentifikasi, keamanan gateway mengijinkan lalulintas berdasarkan daftar dinamis dari MAC ADDRESS yang berhak. Seorang penyerang berharap untuk mengelakkan keamanan alat hanya membutuhkan untuk memantau aktivitas jaringan untuk MAC ADDRESS klien yang terotentifikasi dan kemudian mengganti MAC ADDRESS mereka untuk menyamakan dengan MAC ADDRESS yang telah terotentiifikasi sebelum mengkoneksikan dengan jaringan.

- *Pendeteksian MAC yang terindikasi ganjil*

Suatu perangkat keras pabrikan yang mengharapkan untuk menghasilkan kartu jaringan harus memperoleh suatu **three-byte** unik yang mengidentifikasi secara organisasi dari Institut Insinyur Elektrik dan Elektronika (IEEE) untuk digunakan sebagai awalan untuk MAC ADDRESS dari produk mereka. Hal ini mengijinkan suatu pabrikan untuk memelihara prosedur alokasi mereka sendiri untuk MAC, memastikan nomor mereka serentak unik. Pada waktu ini, IEEE telah mengalokasikan 6.278 awalan nomor unik kepada berbagai organisasi (IEEE, 2002).

IEEE membuat daftar alokasi awalan dan informasi perusahaan yang ditugaskan tersedia untuk publik, yang sebagian besar untuk para pemakai untuk suatu potongan peralatan dengan suatu MAC menunjukkan *mark* pabrikan nya. Kita dapat menggunakan daftar ini untuk mengevaluasi semua sumber MAC menunjuk pada jaringan untuk menentukan jika awalan adalah yang dialokasikan oleh IEEE.

MAC menunjuk itu nampak pada jaringan yang menggunakan suatu awalan yang tidak teralokasi maka menunjukan MAC ADDRESS yang ganjil[3].

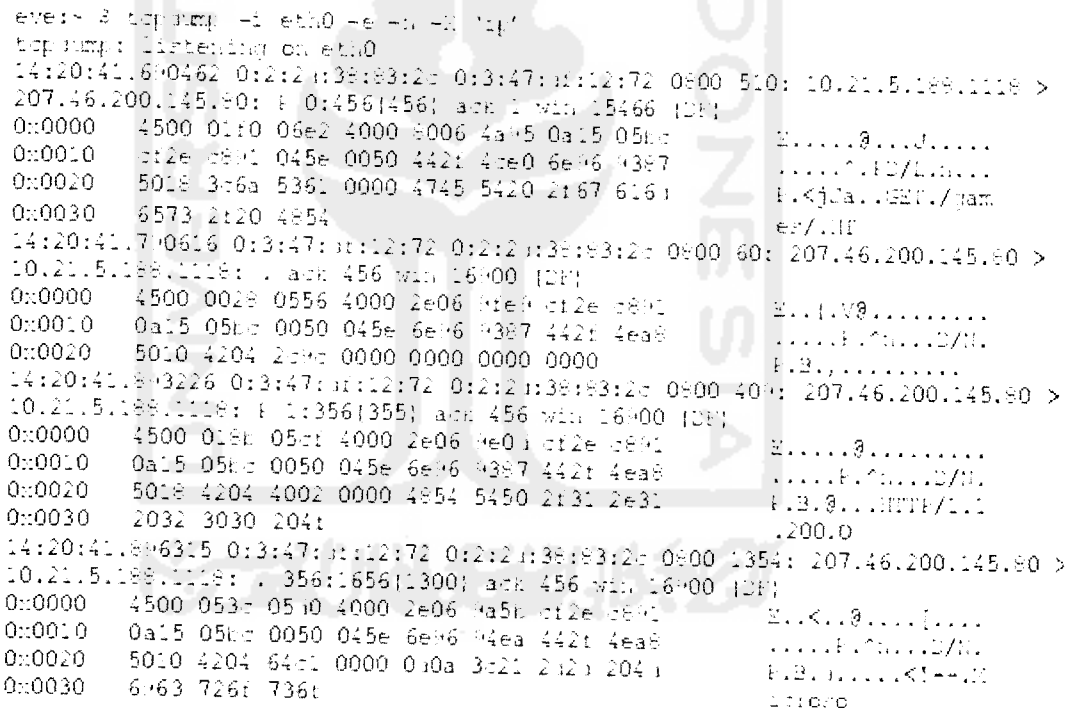
3. Skenario Kasus

Dibawah ini akan dipaparkan studi kasus dengan membypass Mekanisme kontrol Akses Jaringan

Dalam sebuah jaringan terdapat dua klien yakni masing-asing

- Vic (Windows XP, terotentifikasi secara valid, wireless card Lucent 802.11b, MAC ADDRESS : 00:02:2d:38:83:2c dan IP : 10.21.5.188),
- Eve --*Attacker/penyerang*--(Slackware Linux, tidak terotentifikasi, wireless card Lucent 802.11b, MAC ADDRESS : 00:02:2d:09:a1:dd dan IP : 10.21.5.209).

1. Eve menemukan akses point yang terbuka ketika menggunakan Kismet, dan ingin mengakses situs google.com. setelah mengasosiasikan dengan jaringan dan menerima IP Adress dari DHCP SERVER, Eve juga menemukan W-LAN yang terproteksi, setelah membuka web browser dan diredirect untuk halaman permintaan otentifikasi user.
2. Dengan mengetahui kondisi jaringan tersebut, Eve memulai meng-capture lalu lintas jaringan dengan **tcpdump**

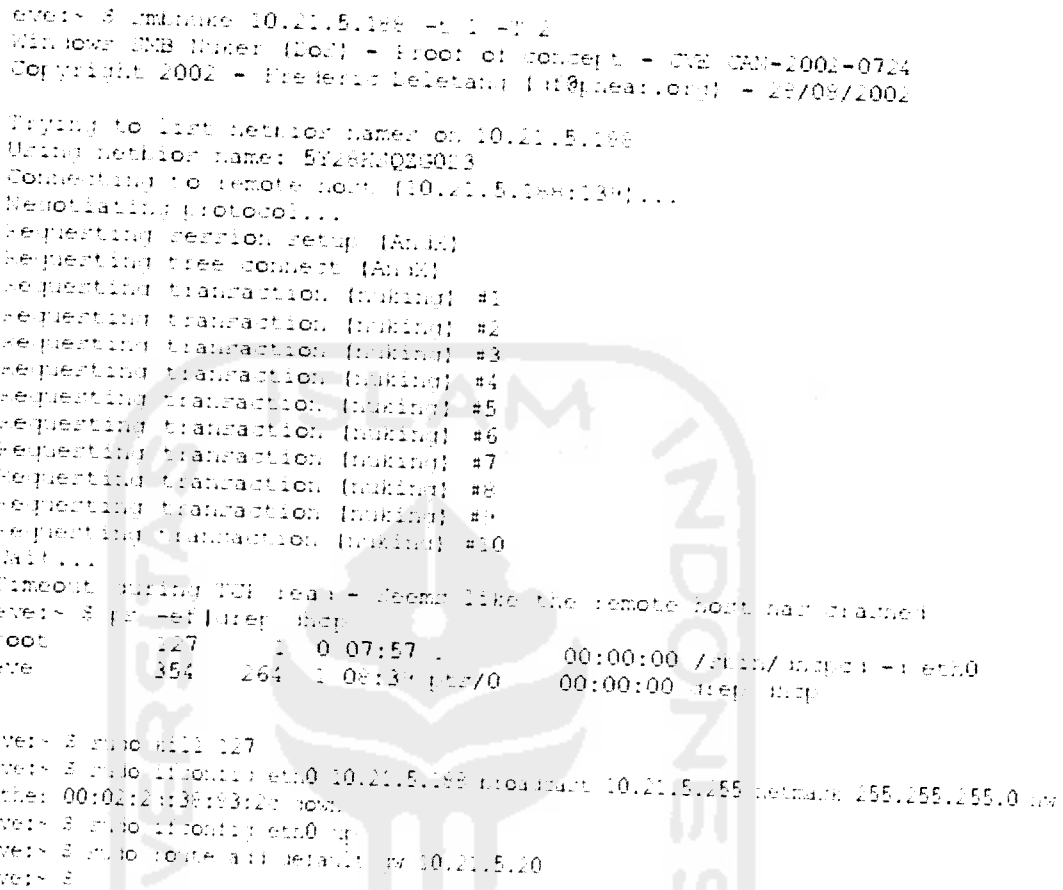


Gambar 7 Capture Tcpdump

Dengan informasi tersebut, Eve mengetahui bahwa vic aktif dalam jaringan dan menyimpan IP Address, MAC ADDRESS, serta informasi gateway. Dari informasi passive-fingerprint dan informasi User-Agent yang tersedia dari aktivitas web browser, juga diketahui kalau vic menggunakan Windows Xp workstation.

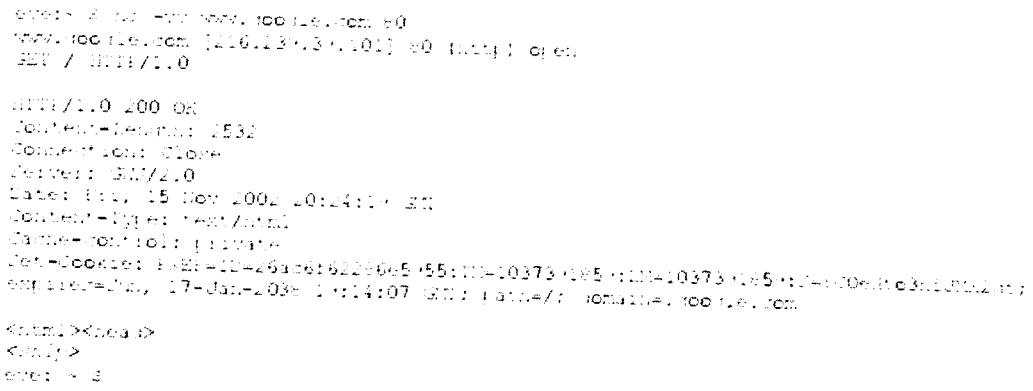
[3] Wright, Joshua, "*Detecting Wireless LAN MAC ADDRESS Address Spoofing*", CCNA, Januari 2003

3. Eve melakukan serangan DoS kepada vic, sehingga menyebabkan kerusakan terminal dengan efek **blue screen of death**. Eve dengan cepat mengganti MAC ADDRESS nya, IP address dan default gateway yang digunakan oleh vic.



Gambar 8 Denial of Service

4. Ketika komputer vic restart, eve memiliki kesempatan untuk mengakses sumber jaringan, dengan membypass sekuriti W-LAN. Eve juga dapat menggunakan kesempatan untuk mengakses sumber internal atau eksternal jaringan, tapi hanya dalam waktu yang singkat (sampai komputer vic pulih kembali). Durasi antara serangan DoS dan vic kembali lagi adalah lebih dari cukup untuk mengoperasikan scan serta mengeksekusi serangan bufferflow jika otomatis menggunakan bahasa script. Dalam kasus ini, eve dengan mudah untuk mengkoneksikan ke google.com dan request HTTP GET.

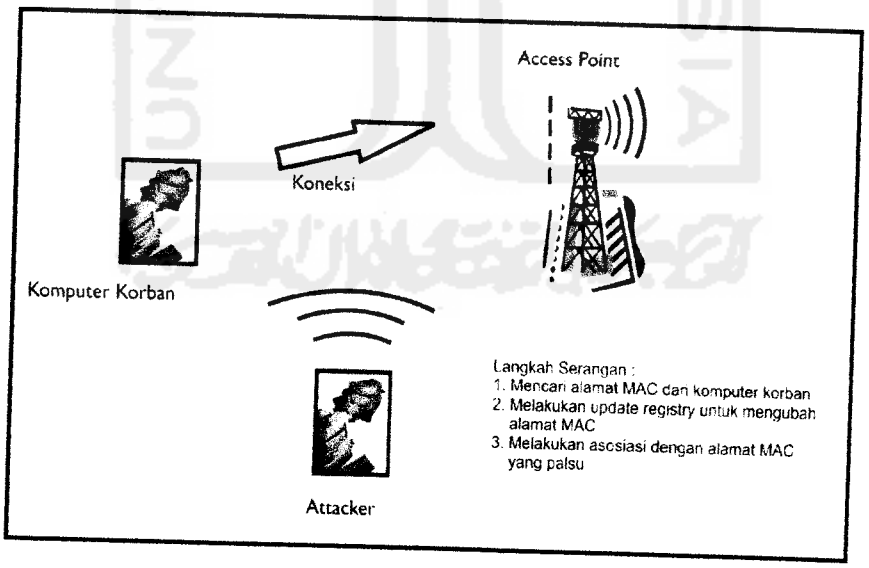


Gambar 9 Pencurian Koneksi

4. Pemetaan Kasus

1. Telah terjadi tindak kriminalitas cyber pada hotspot area tertentu dengan adanya log list pada AP yakni
   - Waktu akses,
   - MAC Address Card,
   - chanel akses,
   - SSID,
   - Nama,
   - Speed,
   - Vendor,
   - Tipe,
   - Enkripsi,
   - Sinyal,
   - Noise,
   - dll

2. Vic memiliki alibi kuat untuk menyatakan dirinya tidak bersalah.



Gambar 10. Gambaran Umum Serangan

5. Anatomi Serangan (Follow up).

Seorang penyusup bisa menyusup ke dalam sistem menggunakan beberapa program gratisan bisa dengan mudahnya diperoleh di internet. Ia bahkan bisa menaklukkan sebuah jaringan nirkabel hanya dalam beberapa urutan langkah.
Berikut adalah beberapa hal yang biasa dilakukan oleh Attacker untuk menaklukkan sebuah jaringan tanpa kabel[4] :

1. Melacak sinyal dari jarak jauh menggunakan kartu jaringan wireless menggunakan antenna tambahan di luar ruangan.

2. Menjadi anonymous tak dikenal menggunakan firewall bawaan dari produk Microsoft atau peranti lain seperti ***ZoneAlarm*** dari Zone Lab untuk melindungi komputernya dari alat pemindai balik IDS (Intrusion Detection System).

3. Mendapatkan IP Address, target access point, dan menggunakan aplikasi seperti ***NetStumbler*** atau program wireless client lainnya.

4. Mengeksploitasi kelemahan – kelamahan jaringan wireless dengan cara yang tidak jauh beda dengan yang dilakukan oleh penyusup jaringan pada umumnya. Biasanya Attacker mengincar dengan kesalahan-kesalahan umum, misalnya : default IP, default password, dll

5. Dengan bantuan alat protocol analyzer, penyusup melakukan sniff gelombang udara, mengambil contoh data yang ada di dalamnya, dan mencari MAC Address dan IP Address yang valid yang bisa dihubungi.

6. Mencuri data penting dari lalu lintas broadcast untuk memetakan jaringan target.

7. Menggunakan peranti seperti Ethereal untuk membuka data yang didapat dari protokol-protokol transparan seperti Telnet, POP (Post Office Protocol), atau HTTP (HyperText Transfer Protocol) untuk mencari data otentikasi seperti username dan password.

8. Menggunakan program lain, seperti SMAC, untuk melakukan spoofing MAC Address dan menangkap lebih banyak paket data dalam jaringan.

9. Melakukan koneksi ke WLAN target.

10. Memeriksa apakah ia telah mendapatkan IP Address atau tidak. Hal ini dilakukan penyusup secara pasif sehingga sangat sulit dideteksi.

11. Menggunakan alat pemindai kelemahan system dan jaringan untuk menemukan kelemahan pada komputer-komputer pengguna, access point, atau perangkat lainnya.

12. Melakukan eksplorasi jaringan untuk memetakan dan memperpanjang akes ke jaringan Wireless berikutnya.

[4] Anonim, Situs Komputer, http://www.xxxxxxxxx.net, diakses pada Januari 05

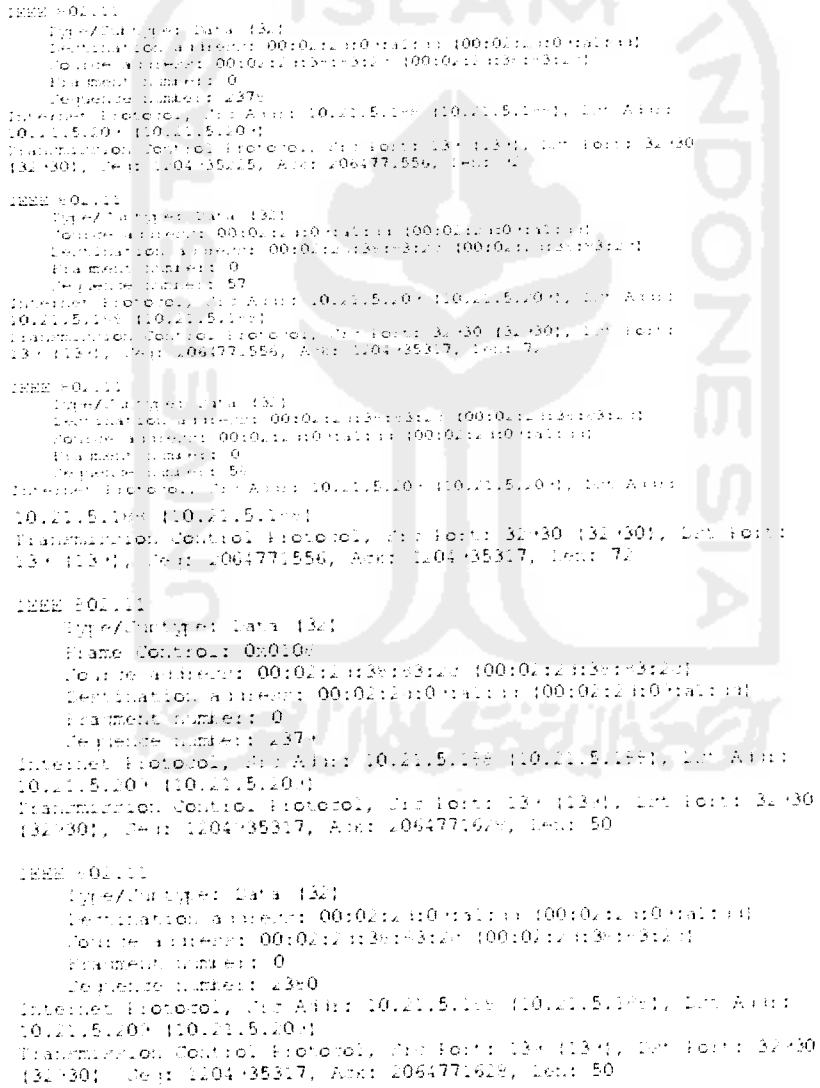
Tools Pelengkap

Kismet : Sebagai pelacak / sniffing network wireless detector
AirSnort : Sebagai Sniffer dan pemecah kunci enskripsi WEP berbasis GUI
AiroDump : Untuk menangkap paket data yang melintas didalam WLAN
Aireplay : Mengirimkan paket data terinjeksi ke Acces Point (AP)
AirCrack : Untuk memecahkan kunci enkripsi WEP

Kismet : http://www.renderlab.net.nyud.net:8090/projects/wrt54g/kiswin.html
AirSnort : http://www.grape-info.com/doc/win2000srv/security/airsnort.html
AiroDump + AirCrack : http://aircrack-ng.org/doku.php#q070
Aireplay : http://forum.tjc.edu.sg/topic.asp?TOPIC_ID=8157

6. Investigasi Forensik

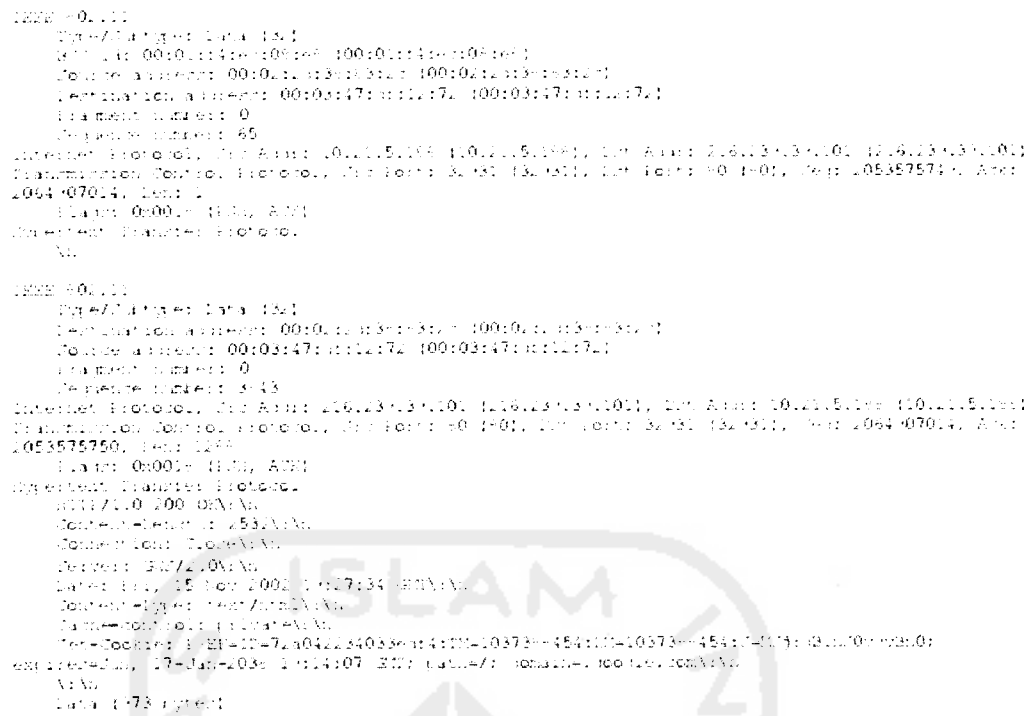
Melalui analisis pengurutan nomor, kita dapat menetapkan sebuah pola aktivitas Eve dan vic, dan dipaparkan dalam eksplorasi dibawah ini :



Gambar 11 Pertukaran data TCP

Dalam data diatas kita dapat melihat pertukaran data TCP diantara eve dan vic, dengan informasi ini kita dapat memulai bahwa 802.11 digunakan oleh masing-masing klien, mengidentifikasi vic menggunakan perurutan dalam range 2378-2380 dimana eve menggunakan nomorm perurutan dalam range 57-58.
Dalam trace dibawah ini kita mengetahui bahwa membuat koneksi ke google.com dengan pertukaran NetBios.

```
IEEE 802.11
    Type/Subtype: Data (32)
    Control Field: 0x4102
    Duration: 44 microseconds
    Destination address: 00:03:47:12:34:56 (00:03:47:12:34:56)
    Transmitter address: 00:0c:41:82:b2:01 (00:0c:41:82:b2:01)
    Source address: 00:03:47:12:34:56 (00:03:47:12:34:56)
    Fragment number: 0
    Sequence number: 2378
Internet Protocol, Src Addr: 10.21.5.100 (10.21.5.100), Dst Addr: 216.239.37.100 (216.239.37.100)
Transmission Control Protocol, Src Port: 3552 (3552), Dst Port: 80 (80), Seq: 2053575733, Ack: 0, Len: 0
    Flags: 0x0002 (SYN)

IEEE 802.11
    Type/Subtype: Data (32)
    Destination address: 00:0c:41:82:b2:01 (00:0c:41:82:b2:01)
    Source address: 00:03:47:12:34:56 (00:03:47:12:34:56)
    Fragment number: 0
    Sequence number: 2379
Internet Protocol, Src Addr: 216.239.37.100 (216.239.37.100), Dst Addr: 10.21.5.100 (10.21.5.100)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 3552 (3552), Seq: 2064070013, Ack: 2053575734, Len: 0
    Flags: 0x0012 (SYN, ACK)

IEEE 802.11
    Type/Subtype: Data (32)
    Destination address: 00:0c:41:82:b2:01 (00:0c:41:82:b2:01)
    Source address: 00:03:47:12:34:56 (00:03:47:12:34:56)
    Fragment number: 0
    Sequence number: 62
Internet Protocol, Src Addr: 10.21.5.100 (10.21.5.100), Dst Addr: 216.239.37.100 (216.239.37.100)
Transmission Control Protocol, Src Port: 3552 (3552), Dst Port: 80 (80), Ack: 2053575734, Ack: 2064070014, Len: 0


    Flags: 0x0010 (ACK)

IEEE 802.11
    Type/Subtype: Data (32)
    Destination address: 00:0c:41:82:b2:01 (00:0c:41:82:b2:01)
    Source address: 00:03:47:12:34:56 (00:03:47:12:34:56)
    Fragment number: 0
    Sequence number: 64
Internet Protocol, Src Addr: 10.21.5.100 (10.21.5.100), Dst Addr: 216.239.37.100 (216.239.37.100)
Transmission Control Protocol, Src Port: 3552 (3552), Dst Port: 80 (80), Seq: 2053575734, Ack: 2064070014, Len: 15
    Flags: 0x0018 (PSH, ACK)
Hypertext Transfer Protocol
    GET / HTTP/1.0\r\n

IEEE 802.11
    Type/Subtype: Data (32)
    Destination address: 00:0c:41:82:b2:01 (00:0c:41:82:b2:01)
    Source address: 00:03:47:12:34:56 (00:03:47:12:34:56)
    Fragment number: 0
    Sequence number: 3842
Internet Protocol, Src Addr: 216.239.37.100 (216.239.37.100), Dst Addr: 10.21.5.100 (10.21.5.100)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 3552 (3552), Seq: 2064070014, Ack: 2053575749, Len: 0
    Flags: 0x0010 (ACK)
```



Gambar 12 Trace Koneksi

Setelah menganalisa dengan lebih dekat, kita melihat bahwa MAC ADDRESS vic (00:02:2d:38:83:2c) adalah bukan dengan memakai perurutan previously established baseline. Agaknya, pengurutan nomor ideal yang lebih dekat merefleksikan eve dalam range 62-65, dengan informasi seperti ini dapat pula kita simpulkan **bahwa MAC ADDRESS 00:02:2d:38:83:2c telah diperdayai dengan Mac spoofing oleh 00:02:2d:09:a1:dd (Eve).**

7. Penutup

Teknik kejahatan carding adalah salah satu dari sekian banyak varian kejahatan komputer, efek yang ditimbulkan biasanya lebih bersifat ke ekonomi. Tindakan yang dilakukan secara preventif kepada keamanan sistem komputer adalah lebih baik untuk dilakukan, selain itu juga konsumen kartu kredit hendaknya selalu waspada terhadap informasi-informasi yang tidak jelas sumbernya, yang biasanya sering digunakan carder untuk mengecoh korbannya.

Handalnya sistem keamanan jaringan tanpa kabel bukan berarti membuat 100% jaringan akan bebas dari masalah keamanan, perlu intensifitas, kejelian untuk membuat sistem jaringan aman, minimalnya memperkecil potensi rusaknya keamanan. Kewaspadaan seorang admin jaringan memang sangat perlukan, selain itu hendaknya selalu menambah dengan wawasan-wawasan baru mengenai topik sekuritas, karena akan selalu berkembang dari waktu ke waktu. Penyebaran tool-tool keamanan yang tersedia gratis di internet akan tergantung proposi penggunaannya oleh si pemakai, untuk tujuan positif ataupun negatif[5].

Dalam informasi tersebut, pentingnya keamanan jaringan komputer tanpa kabel seakan-akan menjadi kebutuhan vital yang level kepentingan nya sama dengan tujuan penggunaannya. Disatu sisi semakin tingginya kebutuhan manusia akan teknologi seakan-akan membuat kebutuhan akan teknologi menjadi kebutuhan primer yang akan dengan mudahnya menghalalkan segala cara.

Kami berharap laporan ini nantinya akan menjadi referensi yang berharga untuk peminat investigasi forensik cybercrime khususnya, serta pecinta Teknologi Informasi pada umumnya. *Wallahu A'lam*.

[5] Anonim, "*Computer Hacking Forensics Investigator*", *Module 7 WINDOWS FORENSICS* EC-Council, 2006

Glossary

- Registry : Keterangan dasar berkaitan dengan mesin komputer (hardware dan software)
- Inurl : perintah untuk melakukan pencarian carding di search engine
- Proxy : fasilitas untuk menghubungkan diri ke internet secara bersama-sama/sharing
- Ip address : pengalamatan komputer yang terseting dalam internet
- Courier service : jasa pengantar barang
- MAC address :Nomor unik hardware oleh pabrik
- MAC Spoofing dan filtering :Aktivitas Pencurian MAC ADDRESS dan pemakaian
- Investigator :Pengusut kasus
- IEEE : Asosiasi internasional yang membuat standar pengalamatan ip
- APJII :Asosiasi penyedia Nomor Publik untuk internet di indonesia
- Bluetooth :Teknologi tanpa kabel standar 802.15.1
- Local Area Networking:Jaringan Komputer dalam ruangan yang sama
- Acces Point (AP) :perangkat hardware untuk koneksi jaringan wireless
- SSID :nama workgroup dalam jaringan wireless
- fungsi ioctl() : Program berbahasa C untuk mengganti MAC ADDRESS
- Brute force :Serangan terus menerus dengan mencoba list phrase satu persatu
- NetFlow :aplikasi untuk men-undeteksi komputer di jaringan
- passive monitoring :Pemantauan traffic secara pasif
- Three-byte :tiga digit pertama MAC ADDRESS
- Tcpdump :aplikasi untuk mengcapture kondisi jaringan
- Denial of Service (DoS) :Serangan bertubi-tubi pada komputer(service) untuk meminta service/respon
- blue screen of death :tampilan biru pada monitor yang menandakan komputer hang
- Enkripsi :metode pengamanan dengan teknik agar tidak terbaca oleh yang tak berhak
- Default gateway :perantara dalam jaringan yang berperan sebagai penghubung yang terseting secara default (natural)
- Network Intrusion Detection System-NIDS :sistem pendeteksi bilamana terjadi indikasi gangguan pada jaringan

Daftar Pustaka

[JHO06] Jhonsen, Jhon Edison, "*Membangun Wireless LAN*", Jakarta : Penerbit PT Elex Media Komputindo Kelompok Gramedia Jakarta, Januari 2006

[PCP06] PC PLUS (PC+), "*Membangun Wireless LAN mudah dan murah*", Jakarta : PT Prima Infosarana Media, Desember 2006

[WRI03] Wright, Joshua, "*Detecting Wireless LAN MAC ADDRESS Address Spoofing*", CCNA, Januari 2003

[ANO06] Anonim, "*Computer Hacking Forensics Investigator*", *Module 7 WINDOWS FORENSICS* EC-Council, 2006.

[YOG05] Anonim, Situs Komputer, http://www.yogyafree.net/, diakses pada Januari 05