
ELEX MEDIA KOMPUTINDO
TEKNIK FORENSIK
Cara Jitu Mengatasi Problematika Komputer
Feri Sulianta

Teknik Forensik

Cara Jitu Mengatasi Problematika Komputer

Sanksi Pelanggaran Pasal 72
Undang-Undang Nomor 19 Tahun 2002
Tentang HAK CIPTA

1. Barangsiapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 Ayat (1) atau Pasal 49 Ayat (1) dan Ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp1.000.000 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp5.000.000.000 (lima miliar rupiah).

2. Barangsiapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran hak cipta atau hak terkait sebagai dimaksud pada Ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000 (lima ratus juta rupiah).

001/I/2014

Teknik Forensik

Cara Jitu Mengatasi Problematika Komputer

Feri Sulianta

PENERBIT PT ELEX MEDIA KOMPUTINDO

KOMPAS GRAMEDIA

001/I/2014

Teknik Forensik **Cara Jitu Mengatasi Problematika Komputer**

Feri Sulianta

Diterbitkan pertama kali oleh
Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Anggota IKAPI, Jakarta 2014

nkfadli@elexmedia.co.id

121142623
ISBN: 978-602-02-5496-8

Dicetak oleh Percetakan PT Gramedia, Jakarta
Isi di luar tanggung jawab percetakan

001/I/2014

Kata Pengantar

Teknik Forensik bukan hanya milik para penyidik, banyak yang tidak mengetahui bahwasannya segudang fakta teknologi informasi dapat diungkapkan secara gamblang dengan teknik forensik. Bahkan dengan teknik komputer forensik, Anda dapat mengelola dan mendapatkan solusi untuk setiap problematika komputer dengan efektif.

Buku ini akan menarik karena berisi ilmu kombinasi baru, metoda, penggagas, penalaran, dan penyampaian deskriptif yang akan berguna pula bagi masyarakat umumnya dalam memanfaatkan dan menangani IT/komputer dengan pemahaman yang lebih baik.

Bacalah sebanyak-banyaknya buku yang menarik untuk Anda baca, dengan demikian akan ada banyak pengetahuan serta pedoman guna mewujudkan yang Anda inginkan. Karena jika Anda mengetahui dengan pasti apa yang diinginkan, maka Anda tidak akan pernah mengalami penyesalan dalam hidup!

Bandung, Juni 2014

Feri Sulianta

Daftar Isi

BAB 1
DASAR KOMPUTER FORENSIK

1.1 Pengertian Forensik

Forensik memiliki arti kata 'menyajikan ke pengadilan', istilah forensik memaksudkan suatu proses ilmiah (didasari oleh ilmu pengetahuan) dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan dikarenakan suatu kasus hukum.

Kekuatan dari forensik memungkinkan proses analisa dan mendapatkan kembali 'fakta' dari kejadian dan lingkungan. Tidak mudah mendapatkan atau lebih tepatnya menemukan fakta, karena fakta sifatnya tersembunyi.

Berbagai fakta dan bukti tersembunyi untuk ditemukan misalnya: darah, struktur gigi, riwayat kesehatan, sidik jari, dan lainnya. Dianalisa sedemikian rupa, sehingga didapat fakta yang layak untuk diajukan sebagai pembuktian. Serangkaian proses ini dikenal dengan istilah forensik.

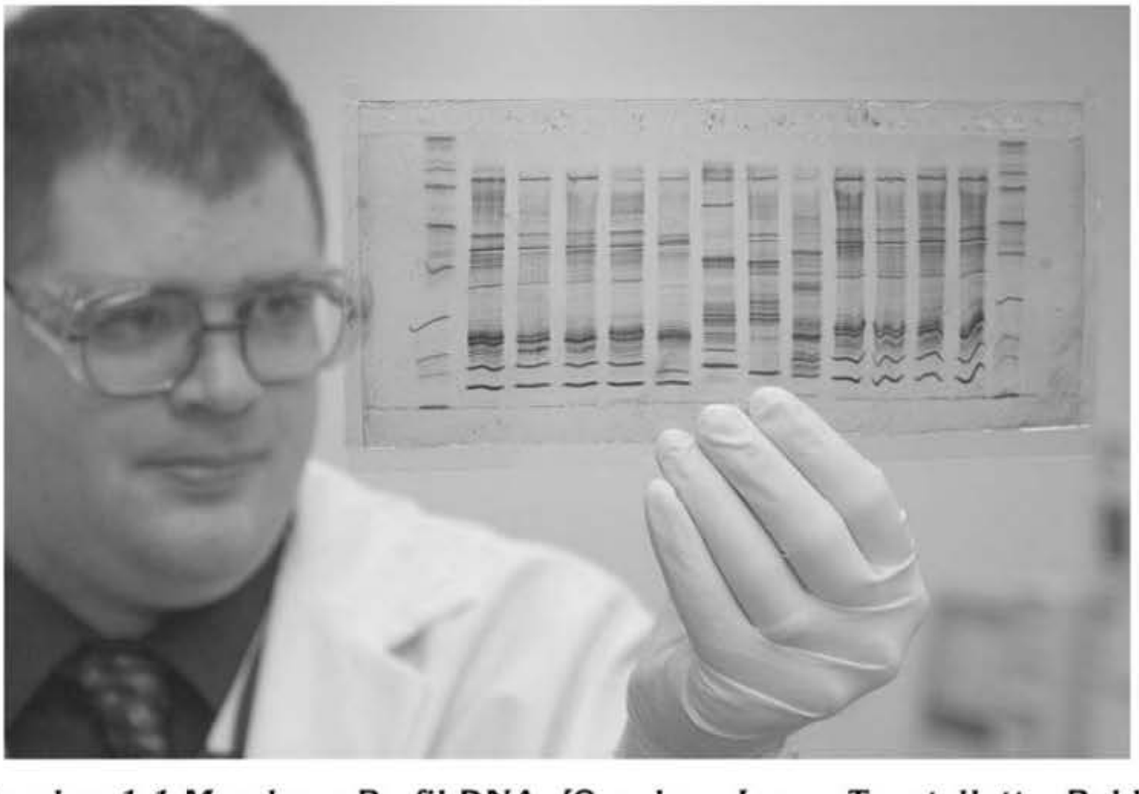
Hanya saja, metodologi dalam Forensik pasti berubah, mengingat peralatan yang digunakan berbeda, bahkan lebih mutakhir, bukti atau evidence pun hadir dengan wajah baru, ilmu pengetahuan yang mendasarinya pun berubah. Apa pun itu perubahannya pasti, membawa pada pembaharuan dan metoda yang lebih baik karena dimunculkannya bidang keilmuan baru dan pengetahuan baru.

Bidang Forensik sudah berkembang lama, diawali oleh seorang tabib yang bernama *Hsi Duan Yu* yang mengkategorikan bagaimana seseorang yang didapati meninggal, misalnya dikarenakan:

- Faktor alami (usia tua).
- Tenggelam.
- Akibat benturan.
- Mati dicekik.

Metode Forensik pun berkembang sampai pada akhirnya digunakan DNA sebagai bukti yang layak untuk dijadikan fakta. Meskipun DNA menjadi suatu pembuktian yang sangat kuat dewasa ini dalam forensik, tidak demikian dahulu halnya.

DNA menjadi bagian dari pembuktian dalam forensik sudah dipahami lama, dan setelah hampir 20 tahun kemudian baru diterima dalam pengadilan di Amerika Serikat setelah menjalani proses yang panjang.



Gambar 1.1 Membaca Profil DNA. [Sumber: James Tourtellotte. Public domain, Wikimedia Commons]

Bukan hanya subjek yang berubah dan meluas, prosesnya pun banyak mengalami perubahan. Ini pun meluas ke bidang-bidang berteknologi baru. Bahkan didapati istilah 'Komputer Forensik' yang mulai mencuat akhir-akhir ini.

Anda tentu setuju bahwa metoda, peralatan, dan ilmu pengetahuan yang melengkapi komputer forensik cenderung belum matang, sangat tidak berimbang dengan perkembangan teknologi informasi itu sendiri.

1.2 Komputer Forensik?

Berbeda dari forensik pada umumnya, komputer forensik memaksudkan pengumpulan dan analisa data dari berbagai sumberdaya komputer yang dikatakan layak untuk diajukan dalam sidang pengadilan, ini mencakup sumberdaya:

- Sistem komputer.
- Jaringan komputer.
- Media komunikasi (mencakup secara fisik menggunakan media kabel dan wireless/nirkabel).
- Berbagai media penyimpanan

Komputer Forensik menjadi bidang ilmu baru yang mengawinkan dua bidang keilmuan, yakni ilmu hukum dan komputer.

Gambar 1.2 Laboratorium Forensik-ICE's Homeland Security Investigation yang dialokasikan di Boston

Gambar 1.3 Seorang Examiner Komputer Forensik sedang bertugas pada Regional Computer Forensics Laboratories (RCFL) yang di sponsori oleh FBI

Berbagai perilaku digital dan digitalisasi yang sudah merambah dalam setiap aktifitas manusia menjadi perilaku yang harus dialamati dengan baik dengan adanya perkembangan tadi.

Komputer forensik atau digital forensik banyak ditempatkan dalam berbagai keperluan, bukan hanya melulu kasus-kasus kriminal yang melibatkan hukum, bahkan berguna untuk kebutuhan khusus lain sehubungan pekerjaan yang melibatkan teknologi informasi.

Secara umum kebutuhan komputer forensik dapat digolongkan sebagai berikut:

- Keperluan investigasi tindak kriminal dan perkara pelanggaran hukum.
- Rekonstruksi duduk perkara insiden keamanan komputer.

- Upaya-upaya pemulihan akibat kerusakan sistem.
- Troubleshooting yang melibatkan hardware ataupun software.
- Keperluan memahami sistem ataupun berbagai perangkat digital dengan lebih baik.

Pentingnya teknik forensik bagi profesional IT: Sadar atau tidak, seorang IT Profesional akan mengasah kemampuan mereka berkomputer, bukan hanya pada level-level pengoperasian umum sistem komputer, tetapi meluas dan kemudian terspesifikasi sesuai kebutuhan, misalnya perihal bagaimana internal sistem operasi bekerja. Sebenarnya, prosesi komputer forensik pada dasarnya bukanlah sesuatu yang baru bagi profesional IT. Berikut beberapa pekerjaan yang dilakukan oleh Profesional IT:

- Seorang profesional IT berperan dalam pengembangan sistem pada level-level strategis, bahkan sistem informasi kritikal dan konfidensial milik perusahaan.
- Bukan hanya mengerti sistem secara umum, tetapi memahami sistem keseluruhan yang melibatkan perangkat keras dan perangkat lunak atau bahkan basis data.
- Memiliki keahlian untuk mempertimbangkan dan membuat pilihan yang terasah dari pengalaman dengan problematika yang pernah dihadapi. Problematika ini mencakup problematika yang diakibatkan oleh pengguna/user, kerusakan perangkat keras, ataupun masalah yang ditimbulkan sehubungan perangkat lunak.
- Profesional IT dengan spesifikasi tertentu pasti memahami cara kerja perangkat keras dan perangkat lunak secara detail dan tahu bagaimana sistem operasi bertingkah laku. Misalnya: sebagian data historikal aplikasi tersimpan pula pada registry Windows.
- Membuat penjadwalan dan kegiatan administrasi yang rapih.

- Tanggung jawab dalam memelihara sistem dan terlibat dalam setiap keputusan yang mempengaruhi sistem.
- Penanganan backup menjadi faktor yang sangat penting dan bagaimana mendapatkan kembali informasi sewaktu terjadi kegagalan sistem yang mempengaruhi data berharga, terlebih bagi komputer forensik yang harus mengambil dan menambang informasi yang minim.

1.3 Bidang Keilmuan Forensik

Ada banyak bidang yang dicakup dan dikombinasikan dalam Forensik, sehingga memunculkan cabang ilmu hibrida, berikut ini contohnya:

Bidang Keilmuan Fisiologi:

- Forensik pathology (forensik tentang penyakit).
- Forensik dentistry (forensik kedokteran gigi).
- Forensik anthropology.
- Forensik entomology (forensik perihal serangga).

Bidang Ilmu Sosial:

- Psikologi forensik.
- Forensik kejiwaan.

Lain-lain keilmuan:

- Fingerprint analysis (analisa sidik jari).
- Forensik akuntansi.
- Ilmu balistik.
- Analisis pola noda darah.

Analisa DNA:

- Forensik toksikologi.
- Forensik pada alas kaki (footwear evidence).
- Pertanyaan bagi dokumen uji.
- Analisa ledakan.

Forensik yang melibatkan Teknologi Cyber:

- Forensik Teknologi Informasi.
- Komputer Forensik.

Dari sekian banyak obyek yang dapat dijadikan barang bukti, misalnya analisa terhadap pola darah yang tertinggal dalam suatu kejadian, berbagai sifat dari darah, bagaiman darah itu mengisi tubuh manusia, kondisi kesehatan/fisik seseorang, dan lain sebagainya menjadi paramater yang bisa dilekatkan dalam analisa.

Misalnya saja seseorang yang terjatuh, tentu kejadiannya dapat dianalisa dari darah yang ditinggalkan/tercecer, dan ini akan menjelaskan apakah seseorang memang terjatuh dari gedung yang cukup tinggi atau tidak, lalu bagaimana posisi dia sebelum terjatuh, lalu apakah aksi bunuh diri atau bahkan pembunuhan, jejak dari cipratan darah mampu menceritakan kronologisnya (istilah dalam Bahasa Inggris: *Bloodstain pattern analysis*)

Dari beberapa contoh tadi, dapat dikatakan bahwa Forensik merupakan ilmu baru dan akan terus meluas dan berkembang dan didasari oleh bidang keilmuan lain yang sudah mapan.

Bahkan komputer forensik pun dapat dispesifikasi lagi menjadi beberapa bagian sebagai berikut:

- Forensik Disk (Forensik terhadap media penyimpanan dan file yang disimpan dalam media penyimpanan).

- Forensik System (Forensik terhadap Sistem Komputer).
- Forensik Jaringan Komputer.
- Forensik Internet.

Dari beberapa bagian ini, beberapa mungkin sudah demikian berkembang, misalnya Disk Forensik yang melibatkan berbagai media penyimpanan yang bertujuan untuk:

- Mendapatkan file-file yang sudah dihapus.
- Mengubah partisi hard dsik.
- Mencari jejak bad sector.

Sistem Forensik dengan ranah bahasan sistem operasi sangat tidaklah mudah untuk ditelaah, karena setiap sistem operasi memiliki karakterisktik dan perilaku yang berbeda, misalnya saja perbedaan file sistem, manajemen memori, penyimpanan komponen sistem operasi di media penyimpanan, dan sebagainya.

Terlebih lagi jika sistem operasi ditujukan sebagai bagian dari jaringan komputer, tentu sistem operasi server akan ditangani secara berbeda dengan sistem operasi client pada workstation, termasuk pula caranya mengumpulkan fakta dan jenis bukti apa yang mungkin didapatkan.

Jika Anda berbicara berkenaan Network Forensik, pasti ini melibatkan OSI (Open System Inter-Connection) layer yang menjelaskan bagaimana komputer berkomunikasi pada jaringan komputer.

Internet Forensik lebih rumit lagi, ada banyak komponen lain yang terlibat, setiap komputer dengan mudahnya terintegrasi dan terdiskoneksi. Meskipun demikian, dikarenakan cakupannya yang demikian luas, ternyata Internet Forensik menjadikan suatu ilmu yang sangat menjanjikan dalam mengungkapkan fakta-fakta dan mengumpulkan bukti dari setiap aktivitas.

Keilmuan Disk Forensik sudah terdokumentasi dengan baik dibandingkan forensik sistem, forensik jaringan komputer atau forensik internet yang masih terus berkembang, bahkan profesional IT pun bisa menangani masalah Disk Forensik ini.

Disk Foresik mencakup kemampuan dalam:

- Mendapatkan 'bit-stream' Image. Hal ini mencakup mendapatkan: slack, unallocated space, dan *file fragment* (potongan-potongan file yang tidak lengkap) yang dihapus.
- Penyidik harus mampu mendemonstrasikan pelaksanaan investigasi dengan aturan dan bukti yang layak.
- Integritas informasi harus disajikan, sehingga terbukti keabsahannya, sama halnya seperti memandang kelayakan informasi perihal sidik jari digital.

Beberapa yang dimampukan dengan adanya Disk Forensik misalnya:

- Me-recover file-file yang terhapus, mendapatkan password, dan kunci kriptografi (penyandian).
- Menganalisa apakah ada: akses file, modifikasi suatu file, dan bagimana, kapan, dan bilamana file dibuat.
- Menganalisa dan memanfaatkan System Logs dan Log Software Aplikasi (misalnya saja: monitoring akses file dijaringan atau penggunaan software aplikasi dan utilitas), dengan demikian aktivitas pengguna dapat dilacak.

  Catatan: Log adalah catatan yang dibuat secara otomatis oleh sistem operasi atau program aplikasi yang berisi riwayat aktivitas sistem dan aplikasi.

Untuk mendapatkan informasi demikian, kita dapat menggunakan software-software siap pakai, ada banyak software komersial yang menyediakan fasilitas demikian, misalnya saja:

- EnCase, yang dikembangkan oleh Guidance Software.
- Pasadena atau SafeBack, yang dikembangkan oleh New Technologies, Inc. (NTI).

Ada banyak perangkat lainnya lagi yang dapat digunakan, misalnya:

- Linux DD, pernah digunakan oleh FBI (Federal Bureau Investigation) dalam kasus Zacarias Moussaoui.
- Coroners Tool Kit (CTK), diimplementasikan pada Sistem Unix.

1.4 Hanya Melulu Komputer?

Komputer Forensik mencakup banyak hal yang harus dipertimbangkan, dikarenakan ilmu baru yang muncul sebagai kombinasi berbagai bidang keilmuan seiring bertumbuhnya kompleksitas dan kebutuhan forensik.

Ada tiga hal utama yang perlu diperhatikan dalam menerapkan Forensik secara umum, antara lain: Prinsip, Policy/Kebijakan, dan Prosedur. Tiga hal ini dipertimbangkan terlepas dari apakah komputer forensik diterapkan karena semata-mata kebutuhan forensik dalam arti hukum, ataupun kebutuhan lain pengelolaan sumberdaya Teknologi Informasi yang melibatkan komputer Forensik. Ketiga komponen ini, yakni:

- Prinsip (Principle): Pada praktiknya ini melibatkan peralatan (*Special tools dan Equipment)* untuk *mengumpulkan electronic evidence* (bukti elektronik). Pada dasarnya, tool bukanlah yang terutama, melainkan keahlian pakar yang sudah teruji lewat pengalaman, bahkan peralatan akan disesuaikan berdasarkan cara kerja seorang ahli forensik.

- Kebijakan (Policy): Pertimbangkan kebijakan dalam memakai peralatan, mencakup perihal mendiskoneksikan media penyimpanan yang berisi *evidence* untuk keperluan investigasi, mengirimkan serta mengemas digital evidence, mengakses suatu dokumen, dan lain sebagainya.
- Prosedur dan Metoda (Procedure): Harus dirancang sedemikian rupa terhadap peralatan dan dalam mendapatkan/mengumpulkan bukti digital (electronic evidence).

Kebutuhan akan peralatan dan perangkat dialamati oleh aspek dari proses yang mencakup: dokumentasi, pengumpulan (collection), pengemasan (packaging), dan pengiriman (transportation).

Ketiga hal utama tadi dilaksanakan dengan berbagai peralatan yang tidak hanya selalu melibatkan perangkat komputer, perangkat forensik pada umumnya (*general crime scene processing tools*) mungkin digunakan dalam komputer forensik, sebagai cara pemberlakukan suatu bukti, misalnya seperti digunakannya:

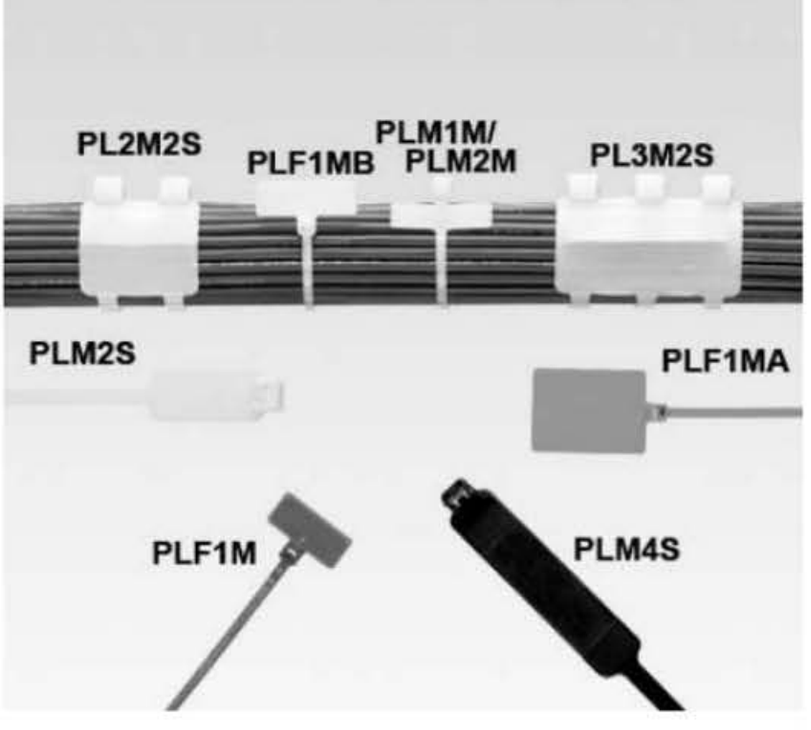
- Notepad (buku catatan).
- Kamera.
- Sketsa (sketchpad).
- Formulir (evidence form).
- Crime scene tape (marka pita tempat kejadian perkara).
- Spidol (marker).

Gambar 1.4 Crime scene tape (marka pita tempat kejadian perkara)

Berbagai peralatan dan perlengkapan yang mungkin digunakan dalam ruang lingkup *electronic crime scene*, dapat dibagi ke dalam beberapa bagian sebagai berikut:

Peralatan Dokumentasi (Documentation Tool):

- Cable tag (pelabel kabel).
- Indelible felt tip marker (spidol tahan air untuk menandai dan memberikan keterangan atau label).
- Stick-on label (stiker khusus kabel).



Gambar 1.5 Cable tag dan marker- Marker Tie, Wrap, 7.4", Standard cross section (sumber: panduit.com/)

Perkakas/ Toolkit (Disassembly and Removal Tool):

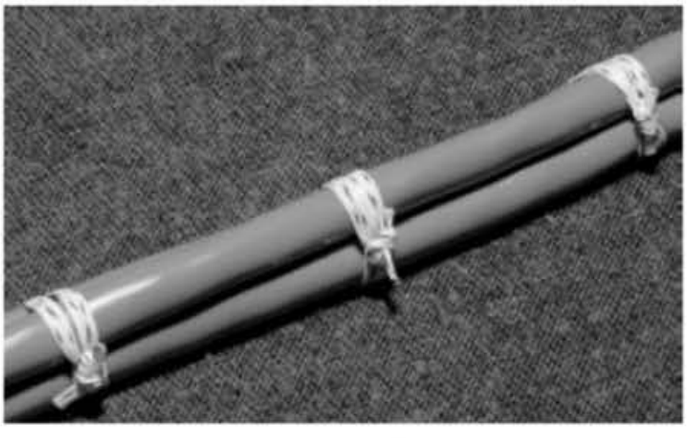
- Pisau (Flat-blade).
- Jenis-jenis Obeng (Philips-type screwdriver, Star-type nut driver, Hex-nut driver).
- Tang (Needle-nose plier).
- Secure-bit driver.
- Pinset (Small tweezer).
- Obeng spesifik (Specialized screwdriver) yang dibuat secara spesifik oleh misalnya: Compaq, Macintosh).
- Tang standar (standard plier).
- Pemotong kabel.

Gambar 1.6 Ragam screwdriver

Pengepakan (Package and Transport Supplies):

- Plastik anti listrik statis (antistatic bag).
- Plastik anti listrik statis yang berisi gelembung-gelembung udara (antistatic bubble wrap).
- Pengikat kabel (cable ties).

- Kantong untuk barang bukti (evidence bag).
- Isolasi untuk barang bukti (evidence tape).
- Packing material (untuk menghindarkan dari material yang dapat menghasilkan listrik statis, seperti misalnya styrofoam).
- Packing tape.
- Sturdy boxes (boks atau kardus) dengan berbagai ukuran.



Gambar 1.7 Pengikat kabel (Gambar: Assortment of cable ties Sumber: Wikipedia – GNU)

Perlengkapan lain yang digunakan:

- Daftar kontak telepon para asisten/staf.
- Floppy disk kosong/belum digunakan (31/2 and 51/4 inch).
- Troli atau alat pengangkut serbaguna (hand truck).
- Kaca pembesar (magnifying glass).
- Karet Gelang (large rubber bands).
- Kertas printer (printer paper).
- Sarung Tangan.
- Floppy disk untuk keperluan booting (seizure disk).
- Small flashlight (lampu senter).

1.5 Autopsi–Digital Forensik

Apa sih yang terbayang dengan aktivitas dalam komputer forensik? Apakah semudah pekerjaan para spesialis komputer pada umumnya?

Jawabannya adalah tidak, justru Komputer Forensik berada di level lebih mendasar dari pada sekedar spesialis informasi. Memang, keilmuan teknologi informasi dan komputer menjadi keharusan, tetapi pada praktiknya apa yang dilakukan dalam komputer forensik lebih dari pada itu, karena mereka mungkin melakukan bukan hanya data recovery biasa, bahkan luar biasa, melebihi batas-batas normal data recovery (pemulihan data), dan banyak lagi hal lain sejenisnya.

Sangat disayangkan pula tidak ada prosedur yang tersertifikasi untuk mengumpulkan evidence dengan 'jaminan aman', bahkan keahlian 'si examiner' harus memampukannya untuk menggunakan metodologi dalam menghasilkan evidence yang nantinya layak untuk diajukan ke pengadilan, yang akan melalui serangkaian tes terlebih dahulu.

Seni dalam menyampaikan hasil forensik pun tidaklah mudah, komputer dan teknologi informasi memiliki sifat yang sangat 'lentur' (kelenturan logika) dan faktor tidak kasat mata pun menimbulkan kesulitan tersendiri yang menghalangi seseorang untuk memahami komputer dengan mudah.

Untuk mendapatkan evidence demikian, mereka harus bekerja pada sistem yang terbukti keabsahannya, yakni:

- Sistem yang terpercaya dan hanya 'examiner' saja yang dapat mengaksesnya,
- Bekerja dalam laboratorium dengan tingkat keamanan tinggi, misalnya: bebas virus komputer..
- Kondisi lingkungan yang terisolasi.

Dokumentasi-Si Examiner harus melalui serangkaian metode, seperti memotret perangkat yang dimaksud sebelum nantinya dipindahkan atau diambil untuk keperluan forensik, ini mencakup dokumentasi pengkabelan, peripheral atau device yang diintegrasikan, sehingga nantinya dapat di re-assembling di laboratorium forensik.

Caranya menangani evidence-Belum cukup sampai situ saja, bagaimana mereka memindahkan perangkat tersebut pun harus diperhatikan, jangan sampai pengaruh panas, benda-benda magnetis ataupun faktor fisik merusaknya.

Examiner tidak akan menyentuh/memperlakukan hard disk, floppy disk dengan ceroboh, karena perubahan sekecil apa pun akan mengubah laporan akhir. Maka dari itu, menduplikasilah data tersebut ke media yang tidak dapat dimodifikasi kemudian, seperti misalnya pada media CD.

Lain-lain yang di luar batas normal penanganan perangkat teknologi informasi, misalnya saja si pelaku menggunting floppy disk, menjadi tugas examiner untuk me-reasembling agar informasi yang ada pada floppy disk bisa didapatkan kembali.

Log Komputer-Bagaimana dengan log file yang ada di komputer? Tidak serta merta harus dipercaya keberadaan informasinya begitu saja. Sangat mudah bagi pelaku untuk melakukan perubahan jam sistem yang akan menyimpangkan informasi yang sebenarnya.

Sudah menjadi manajerial pribadi si examiner untuk selalu mempertimbangkan kejadian atau hasil akhir terburuk.

Faktor-faktor seperti kerapuhan data, mudahnya informasi hilang, dan lain sebagaimnya menjadi faktor-faktor terburuk yang sudah jauh sebelumnya dipertimbangkan.

Dalam praktiknya, si Examiner mungkin melakukan pencarian dan pemeriksaan mendalam terhadap e-mail, file temporer yang diciptakan sistem atau aplikasi, melibatkan pula basis data, *logical file structure*, free space hard disk, setingan perangkat keras dan perangkat lunak, cache file pada web browser, bookmark, dan lainnya.

Lalu bagaimana jika melibatkan jaringan komputer, tentu akan meningkatkan kompleksitas dalam forensik. Ada banyak hal lain yang rumit, menarik, dan upaya di luar batas normal harus dilakukan.

Lebih jauh lagi, Anda akan melihat ruang lingkup dari kasus forensik yang beragam. Karakteristik dari kategorisasi tindak kriminal melibatkan bukti-bukti spesifik yang terelasi kuat dengan aksi kriminal.

Gambar 1.8 Ponsel pada kantong evidence

Secara umum, hal-hal yang dapat digunakan sebagai bukti yang layak dipertimbangkan berkenaan perangkat komputer dalam ruang lingkup komputer forensik antara lain:

- Audio Recorder.
- Caller ID.
- CD-ROM.
- Chip komputer (jumlah yang banyak berkenaan dengan Chip menjadi bukti terhadap tindak pencurian).
- Databank/digital organizer.
- Drive duplicator.
- Flash memory card.
- Floppy disk.
- Hard disk eksternal.
- Hardware Protection Device (kunci proteksi perangkat keras).
- Kabel.
- Kamera digital.
- Mesin fax.
- Mesin fotokopi.
- Mesin penjawab.
- Pager.
- Palm pilots/electronic organizer.
- PCMCIA card (kartu PCMCIA).
- Perangkat GPS.

- Perangkat kecil yang diintegrasikan ke komputer, misalnya modem, USB flash disk, dan sebagainya (atau disebut sebagai: dongle).
- Printer (dalam keadaan aktif).
- Removable media.
- Scanner (film scanner, flatbed scanner, dan lainnya).
- Smart cards/secure ID token.
- Telepon (mencakup pula speed dialers, dan lainnya).
- Telepon selular.
- VCR.
- Wireless access point.

Gambar 1.9 Berbagai media penyimpanan untuk keperluan autopsi [Sumber: Arnold Reinhold. GNU Free Documentation License]

Dari kesemuanya, ternyata berbagai perangkat yang ada hanya sebagian kecil dari beragam komponen yang akan ditambahkan kemudian seiring bentuk tindak kejahatan, misal seandainya kejadian melibatkan internet dan jaringan komputer, ruang lingkup akan meluas, bahkan harus melibatkan rangkaian kegiatan yang membutuhkan kepakaran. Berikut ini daftar yang akan membantu petugas investigasi dalam identifikasi berbagai bukti dan atribut yang dibagi dalam konteks kejahatan yang terjadi:

Penipuan Lelang (Auction Fraud):

- Account data (pada situs lelang online).
- Accounting/bookkeeping software.
- Basis data.
- Buku alamat.
- Catatan pengunaan telepon.
- Chat log (riwayat percakapan).
- Customer information/credit card data.
- Digital camera software.
- E-mail/surat/catatan.
- File image/grafis.
- Financial/asset records.
- Internet browser history/cache files.
- Kalendar.
- Log aktivitas.
- Online financial institution access software.
- Records/documents of testimonial.

Eksploitasi dan pelecehan anak-anak:

- Chat log.
- Digital camera software.
- E-mail/surat/catatan.
- File video.
- Games.
- Graphic editing dan viewing software.
- Image.
- Log aktivitas berinternet.
- Tanggal dan waktu.
- User-created directory (file yang dibuat user) dan nama file yang mengklasifikasi image.

Kejahatan komputer:

- Buku alamat.
- E-mail/surat/catatan.
- File-file teks (username dan password).
- Internet protocol address dan username.
- Internet relay chat (IRC) logs.
- Konfigurasi file.
- Log aktivitas berinternet.
- Program executable.
- Source code.

Investigasi penyebab kematian:

- Buku alamat.
- Buku harian (diary).
- E-mail/surat/catatan.
- Catatan keuangan dan perbendaharaan.
- Gambar/foto.
- Log aktivitas berinternet.
- Dokumen-dokumen berharga (legal documents and wills).
- Riwayat kesehatan dan pengobatan.
- Catatan pengunaan telepon.

Kekerasan rumah tangga:

- Buku alamat.
- Buku harian (diary).
- E-mail/surat/catatan.
- Catatan keuangan dan perbendaharaan.
- Riwayat kesehatan dan pengobatan.
- Catatan pengunaan telepon.

Penipuan keuangan (melibatkan penipuan online dan pemalsuan):

- Buku alamat.
- Kalender.
- Cek, mata uang dan money order image.
- E-mail/surat/catatan.

- False financial transaction form.
- False identification.
- Catatan keuangan dan perbendaharaan.
- Log aktivitas berinternet.
- Online financial institution access software.
- Credit card skimmer.
- Informasi konsumen.
- Data kartu kredit.
- Basis data.

Ancaman via e-mail, pelanggaran privasi atau penguntitan:

- Buku alamat.
- Buku Harian (Diary).
- E-mail/surat/catatan.
- Catatan keuangan dan perbendaharaan.
- Image.
- Log aktivitas berinternet.
- Dokumen/berkas-berkas hukum.
- Catatan pengunaan Telepon.
- Catatan latar belakang korban.

Pemerasan:

- Tanggal dan jam kejadian.
- E-mail/surat/catatan.
- Log historis.
- Log aktivitas berinternet.
- Temporary internet file.
- Nama user.

Perjudian:

- Buku alamat.
- Kalender.
- Database konsumen dan catatan para pemain.
- Informasi konsumen.
- Data kartu kredit.
- Electronic money.
- E-mail/surat/catatan.
- Catatan keuangan dan perbendaharaan.
- Gambar/wajah para pemain.
- Log aktivitas berinternet.
- Online financial institution access software.
- Informasi statistik dari judi yang melibatkan olahraga (Sports betting statistics).

Pencurian Identitas:

- Hardware dan software.
    - Credit card generator.
    - Credit card reader/writer.
    - Kamera digital.
    - Scanner.
    - Perangkat lainnya yang digunakan.
- Atribut identitas (identification templates).
    - Surat kelahiran.
    - Check cashing card.
    - Digital photo images untuk keperluan identifikasi.
    - SIM.
    - KTP.
    - Tanda tangan elektronik (electronic signatures).
    - Registrasi palsu kendaraan (fictitious vehicle registrations).
    - Dokumen asuransi kendaraan (proof of auto insurance document).
    - Scanned signature (pemindaian tanda tangan).
- Aktivitas berinternet yang berhubungan dengan percurian identitas (Internet activity related to ID theft).
    - E-mail dan newsgroup posting.
    - Dokumen terhapus.

- Online order.
- Online trading information.
- System files dan file slack.
- Aktivitas internet pada forgery sites.

Narkotika:

- Buku alamat.
- Kalender.
- Basis data.
- Resep obat-obatan.
- E-mail/surat/catatan.
- False identification (kartu indentitas yang tidak benar).
- Catatan keuangan dan perbendaharaan.
- Log aktivitas berinternet.

Prostitusi:

- Biografi.
- Buku alamat.
- Catatan keuangan dan perbendaharaan.
- Database dan catatan konsumen.
- E-mail/surat/catatan.
- Iklan pada halaman website.
- Informasi yang dipalsukan (False identification).
- Kalender.

- Log aktivitas berinternet.
- Riwayat kesehatan dan pengobatan.

Pembajakan perangkat lunak (software piracy):

- Riwayat percakapan (chat logs).
- E-mail/catatan/surat.
- Image files of software certificates.
- Log aktivitas berinternet.
- Serial number.
- Software cracking information dan software utility.
- User-created directory dan nama file yang diklasifikasikan dalam software ber-copyright.

Penipuan yang melibatkan media telekomunikasi (telecommunications fraud):

- Cloning software.
- Database dan catatan konsumen.
- Electronic Serial Number (ESN)/Mobile Identification Number (MIN) pair record.
- E-mail/surat/catatan.
- Catatan keuangan dan perbendaharaan.
- Buku manual mengenai cara phreaking.
- Aktivitas berinternet.
- Catatan penggunaan telepon.

Informasi demikian penting untuk didokumentasikan dan beberapa temuan lainnya akan juga ditambahkan dalam membantu uji komputer forensik, misalnya:

- Ringkasan kasus.
- Internet protocol (IP)address.
- Daftar kata-kata kunci.
- Nickname (alias).
- Password.
- Informasi kontak.
- Dokumen pendukung lainnya.
- Jenis kejahatan.

BAB 2
PERANGKAT KOMPUTER FORENSIK

2.1 Komponen Komputer dan Informasi

Forensik komputer diimplementasikan pada komputer dan berbagai sumber daya informasi yang mencakup teknologi komunikasi dan informasi. Komponen yang dimaksud antara lain:

- Hardware (perangkat keras)
- Software (perangkat lunak)
- Database (basis data)
- Data/informasi
- Brainware (user, profesional IT)

Setiap komponen terintegrasi untuk membangun 'sistem yang bekerja' dan untuk kebutuhan forensik, komponen dan subkomponennya akan dipindai, diambil, dianalisa untuk mendapati kelengkapan fakta atau bukti forensik, maka penting untuk mengetahui komponen dan fungsi setiap komponennya.

Hardware atau perangkat keras mencakup:

- Perangkat masukan
- Perangkat keluaran
- Media penyimpanan (storage device)
- Komponen pengolahan (kerap dikenal sebagai CPU)

Perangkat masukan memaksudkan perangkat yang diintegrasikan dalam sistem komputer yang akan memberikan instruksi pada komputer.

Beberapa yang dapat dikategorikan ke dalam alat input:

- Keyboard
- Mouse
- Trackball
- Trackpoint
- Trackpad/Touchpad
- Touch Screen
- Joystick
- Source Data Automation (misalnya: Optical Character Recognition (OCR), Bar Code Reader, Handwritten Recognition)
- Scanner (misalnya: Flatbed Scanner, Handy Scanner, Medium Size Scanner)
- WebCam
- Kartu (misalnya: Magnetic Card, Smart Card)
- Biometric Peripheral

Perangkat keluaran/output device digunakan untuk melihat hasil dari eksekusi, instruksi yang diberikan pada komputer akan diproses dan ditampilkan melalui perangkat keluaran.

Beberapa yang dikategorikan ke dalam alat Output:

- Monitor. Cathode Ray Tube (CRT) yang paling umum dipakai untuk komputer desktop. Sedangkan Liquid Crystal Display (LCD), umumnya digunakan pada laptop dan PDA.
- Printer
    - Impact Printer: dikatakan impact karena bekerja dengan sistem 'ketukan' yang memberi tekanan pada media kertas untuk membentuk image, contoh: printer dot matrix, daisywheel.
    - Non Impact Printer: printer dengan tinta (inkjet), atau dengan serbuk/toner (laser printer), atau dengan sistem pemanasan (thermal printer).
- Plotter, digunakan untuk mencetak gambar berukuran besar (misalnya untuk keperluan desain arsitektur, peta, dan lainnya).
- Speaker (internal, external).
- Video output (multimedia proyektor).
- Micro film.

Storage Device atau media penyimpanan.

Istilah ini mengacu pada media penyimpanan sekunder (Secondary Storage Divice), ada banyak istiah yang mengacu pada media penyimpanan sekunder, antara lain:

- Mass Storage (media penyimpanan berkapasitas besar).

- Simpanan luar.
- Auxiliary storage.
- Permanen storage.
- Backing storage.
- Computer data bank.

Secondary storage umumnya digolongkan ke dalam dua bagian:

- **Sequential Access Storage Device (SASD).** Proses baca tulis perangkat ini relatif lambat karena dilakukan dengan modus akses terurut (sequence). Contoh: Magnetic tape. Sudah jarang dipakai, umumnya hanya untuk backup, karena murah jika dibandingkan dengan kapasitasnya yang besar.

Gambar 2.1 Magnetik Tape atau Pita Magentik sebagai media simpan sequential [Sumber: Wikipedia GNU Free Documentation License]

- **Direct Access Storage Device (DASD)**. Prosesnya lebih cepat dibanding SASD karena untuk mengambil data tertentu tidak perlu dicari dari awal berurutan, yakni:
    - Magnetic Disk, menggunakan medan magnet, contoh: floppy disk (disket) dan hard disk.
    - Optical Disk, menggunakan sinar laser, contoh: CD-ROM.

Media penyimpanan yang cukup populer lainnya: CD-ROM, DVD (Digital Versatile Disc), FMD (Fluorescent Multilayer Disc), MO-Disc (magneto-optical disc).

Perangkat penyimpanan yang terdahulu akan ditinggalkan dan digantikan dengan teknologi yang lebih baik dan berdayaguna. Coba perhatikan variasi dari teknologi penyimpanan atau disk storage berikut:

- CD (CD-ROM) Drive - Read Only Memory.
- CD - R Drive (R memaksudkan Readable).
- CD - RW Drive (RW memaksudkan ReWriteable).
- DVD (DVD-ROM) Drive.
- Combo Drive (kombinasi CD-RW dan DVD drive dalam satu Drive) DVD-R, DVD-RW, dan DVD+RW.

Kapasitas penyimpanan ragam storage device diperlihatkan berikut ini:

- CD-ROM (650 - 700 MB). Kapasitas 60 menit dan kemampuan penyimpanan 553 MB, dan yang kapasitas 79 menit dengan kemampuan penyimpanan 681 MB.
- DVD-5 (single sided 4.7 GB).
- DVD-9 (single sided, dual layer 8.5 GB).

- DVD-10 (double sided, single layer 9.4 GB).
- DVD-18 (double sided, dual layer 17 GB).

Perhatikan kapastias penyimpanan antara CD jika dibandingkan dengan kapasitas DVD yang mencapai 26 kali kapasitas CD.

Kecepatan CD-ROM untuk melakukan transfer data sebagai berikut:

- 1X 150 KB/sec 200 - 530.
- 2X 300 KB/sec 400-1060.
- 4X 600 KB/sec 800 - 2,120.
- 8X 1.2 MB/sec 1,600 - 4,240.
- 40X CAV 2.6 - 6 MB/sec 8,900 (constant).

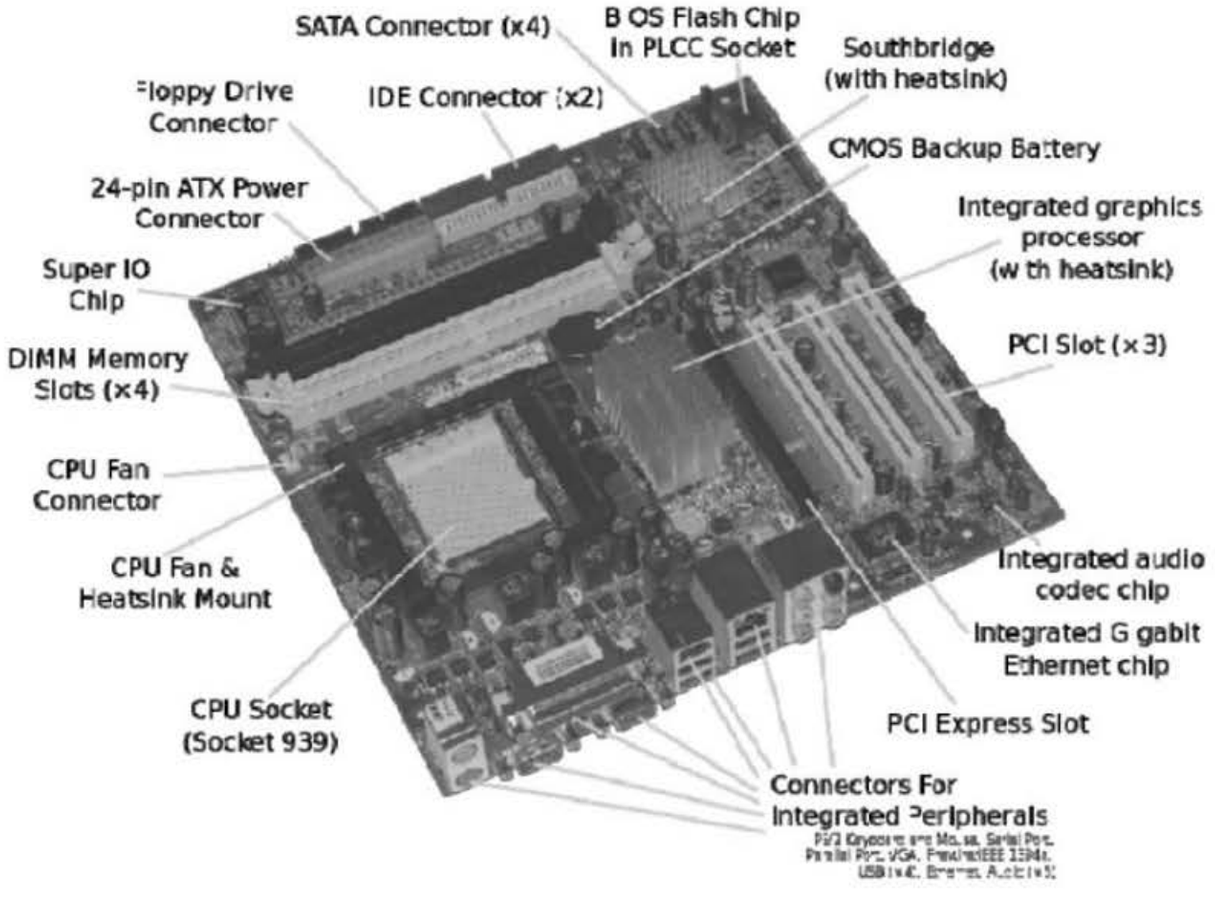
Daftar empat teratas menggunakan metoda CLV (Constant Linear Velocity) yang diterapkan pada CDROM terdahulu, sehingga semakin dekat head pada pusat piringan, maka semakin cepat putaran untuk menghantar data.

Sedangkan metoda CAV memungkinkan CDROM berputar pada putaran yang konstan permenitnya, sehingga pembacaan data yang ada di piringan terluar akan dibaca sedemikian cepat dan melambat dipusat.

Perubahan teknologi memang tidak selalu berpengaruh terhadap Forensik. Mengapa? Karena dalam forensik kita menguak fakta, bukan teknologi. Meskipun demikian, dalam kasus yang lebih detail, pengetahuan seksama akan teknologi amat berguna dalam menggali lebih banyak fakta. Misalnya: waktu yang dibutuhkan dalam menulis data ke CD.

Yang lain lagi dari komponen inti pembangun sistem komputer adalah: CPU (Central Processing Unit). Komponen fundamental sebagai otak komputer ini sering disalahartikan sebagai keseluruhan komponen yang ada pada kotak CPU, padahal CPU hanyalah bagian dari mikromputer,

Processor yang dimaksud dalam CPU untuk PC Desktop sering disebut sebagai MicroProcessor, karena minimnya processor yang menyusun sebuah komputer mikro (PC Desktop), berbeda dengan mainframe yang terdiri dari banyak processor.



Gambar 2.2 Penampang Motherboard - Acer E360 Socket 939 motherboard by Foxconn [Sumber: Wikipedia CC License. GNU Free Documentation License]

CPU dapat digolongkan ke dalam beberapa bagian:

- Control unit: pengatur lalu lintas data di dalam CPU.
- Arithmetic logic unit: pemroses perhitungan (*,:,+,-,^) dan perbandingan (<, >, =, <=,>=).
- Register: pencatat/penyimpan data yang akan diproses (Dapat dianalogikan sebagai memori kecil yang membantu CPU).

Bagaimana komponen ini bekerja, dapat dijelaskan sebagai berikut:

1. Control unit mengambil instruksi dari RAM.
2. Control unit kemudian menerjemahkan instruksi tersebut, dan memerintahkan data yang diperlukan untuk dipindahkan dari RAM ke ALU.
3. ALU melakukan perhitungan dan perbandingan, kemudian ALU menyimpan hasilnya di RAM/Register.

Beberapa faktor yang sangat memengaruhi kinerja CPU antara lain:

- Register, umumnya dapat menyimpan 2 bytes informasi, masing-masing dapat terdiri dari 16, 32, atau 64 bit. Ukuran penyimpanan informasi dalam register disebut wordsize. Semakin besar wordsize semakin tinggi kecepatan processornya.
- Memori, yang dapat digolongkan ke dalam dua bagian:
    - ROM (Read Only Memory). Berisi perintah yang diisi oleh pembuat chip. Isinya tidak dapat diubah/dihapus oleh user.
    - RAM (Random Access Memory). Berisi informasi-informasi selama CPU dijalankan. Bersifat volatile (informasi hilang jika listrik mati).
- Komputer Bus.
    - Data bus: untuk mengalirkan data.
    - Address bus: untuk mengalirkan alamat tujuan data.
    - Control bus: untuk mengalirkan informasi status peralatan.
    - Ukuran bus: 16 bit, 32 bit. Semakin besar ukuran bus, semakin cepat informasi mengalir, proses semakin cepat.

Perkembangan bus: ISA, EISA, MCA, PCI, jenis-jenis sistem BUS yang dimaksud akan dijabarkan sebagai berikut:

- ISA (Industrial Standar Architecture) dengan kecepatan transfer data: 5 MB/s dan memiliki lebar data 8/16 Bit.
- PCI (Peripheral Component Interconnect) dengan kecepatan transfer data 132 MB/s dan lebar data 64 Bit. Digunakan untuk card kecepatan tinggi (misalnya pada: LAN card, Sound Card).
- AGP (Accelerate Graphic Port), sistem bus untuk video display. AGP 1X: 266 MB/s, AGP 2X: 532 MB/s, AGP 4X: 1064 MB/s.
- USB (Universal Serial Bus).
- Cache Memory, berikut pernyataan berkenaan karakteristik yang dimaksud:
    - Komponen yang mirip dengan RAM, tetapi prosesnya jauh lebih cepat.
    - Umumnya digunakan untuk menyimpan instruksi yang sering digunakan oleh CPU, sehingga jika dibutuhkan CPU tidak perlu mencari informasi dari RAM
    - Semakin besar cache memory, semakin cepat proses CPU.

Fungsi dari Cache Memory adalah menyangga data untuk keperluan pemrosesan, dan jika dilihat lebih jauh, ternyata konsep sangga menyangga data ini melibatkan komponen di luar dari CPU, yakni:

Level 1 Cache (L1 Cache) menyangga L2 Cache, RAM, Hard Disk, CD-ROM. L2 Cache menyangga RAM, Hard Disk, CD-ROM. L3 Cache menyangga RAM, Hard Disk, CD-ROM, RAM. Sedangkan Hard Disk menyangga CD-ROM, perhatikan rantai sangga menyangga yang difungsikan untuk mendongkrak kinerja sistem komputer.

- Faktor lain yang memengaruhi kinerja motherboard:
    - Expansion slot (slot untuk komponen/card tambahan).
    - Port (hubungan antara motherboard dengan alat input-output, misalnya: keyboard, mouse, dan lainnya).
    - CPU Fan (berfungsi sebagai pendingin).
    - Casing (kotak CPU).

Penting Anda memahami dengan baik komponen-komponen berikut dengan berbagai penamaan/istilah. Komputer forensik membutuhkan pengetahuan mendalam perihal teknologi dan perangkat komputer lebih dari hanya sekedar mengerti komputer.

Profesional komputer forensik harus memiliki ketertarikan luar biasa dalam bidang komputer, faktor-faktor yang membuatnya menarik untuk ditelusuri akan memicunya untuk menggali dan menganalisa lebih dalam.

Salah pemahaman dalam merujuk pada komponen tertentu akan menimbulkan persepsi yang sama sekali berbeda. Maka dari itu, upayakan untuk memperkaya perbendaharaan kata Anda. (Lebih jauh Anda dapat melihat kamus forensik).

Software

Software atau perangkat lunak digunakan sebagai antarmuka pengguna dan pemberi instruksi terhadap hardware, sehingga bisa dikatakan sebagai satu kesatuan sistem komputer yang bekerja. Perangkat lunak umumnya digolongkan ke dalam dua bagian:

- **Perangkat Lunak Sistem.**

  Dikatakan perangkat lunak sistem karena fungsinya mengelola perangkat keras yang umumnya tidak dapat bekerja tanpa adanya software sistem untuk menjadi sistem komputer yang bekerja.

- **Perangkat Lunak Aplikasi.**

  Perangkat lunak aplikasi dipakai user untuk mengakses sumber daya komputer. Perkembangannya terjadi karena meningkatnya kebutuhan user terhadap aplikasi untuk membantu aktivitas.

  Sedemikian beragamnya perangkat lunak, dapat menimbulkan kesulitan dalam pengklasifikasiannya, tidak ada pembagian baku berkenaan perangkat lunak. Bahkan forensik toolkit kadang melibatkan pula penggunaan perangkat lunak aplikasi dan perangkat lunak utility.

Berikut contoh pembagian perangkat lunak berdasarkan situs anova.org:

- Word Processing.
- Text Editing.
- Outlining, Pim, Calendar.
- Office Tools.
- Spreadsheet, Math, Db.
- System Tools.
- Printing, Fonts, Pdf.
- Image Viewers/Editors.
- Graphics, Image Tools.
- Multimedia, Video.
- Hotkeys, Scripting.
- Online-Only Apps.
- Web-Dev: Css, Rss, Ftp.
- Usenet, P2p/File Sharing Tools.

- File Managers.
- File Utilities; Renamers; Duplicate Finders.
- Archive, Synching, Download Tools.

Sangat sulit mengkategorikan seluruh perangkat lunak aplikasi yang ada karena perkembangan dan kebutuhan yang terus berubah.

Pengkategorian pun sangat bervariasi bergantung cara pandang terhadap aplikasi, misalnya pengkategorian berdasarkan fungsi, dukungan terhadap pekerjaan, pengguna, dan lainnya. Misal, http://www.software-list.com/ yang membagi software dalam kategori sebagai berikut:

- Audio & Multimedia.
- Bisnis.
- Desktop.
- Development
- Edukasi.
- Games & Entertainment.
- Grafika.
- Home & Hobby.
- Komunikasi.
- Network & Internet.
- Security.
- Server.
- System Utility.
- Web Development.

Brainware

Brainware terlatih akan sangat mudah mencerna ilmu komputer forensik. Bahkan dalam suatu kegiatan, mungkin konsep komputer forensik bisa digunakan. Misalnya untuk mengembalikan data yang hilang karena terhapus tidak sengaja. Dibutuhkan tidak hanya sekedar pengetahuan, tetapi pengalaman dalam menggunakan komputer untuk membuatnya terampil mengatasi berbagai aktivitas berkomputer. Umumnya, Brainware dalam konteks ini dapat digolongkan ke dalam tiga bagian, yaitu:

- Profesional IT.
- Insiden Handlers (penanganan kerusakan/kegagalan).
- Investigator.

Profesional IT

Memaksudkan profesional IT pada umumnya, mencakup bermacam deretan istilah seperti: Technical Support, Network Administrator, Database Administrator, Analis Sistem, Programmer, dan lain sebagainya.

Mereka ini pasti mengetahui dasar-dasar penanganan komputer forensik yang berbeda. Brainware kategori ini sangat sedikit menerapkan konsep-konsep komputer forensik dalam kerjanya, meskipun demikian sedikit banyak mereka menerapkan komputer forensik secara tidak langsung sewaktu didapati masalah/problem.

Incident Handler

Memiliki kedekatan dengan keilmuan forensik, meskipun karakteritik pekerjaannya tidak melulu mencakup tindak kriminial dan pelanggaran. Mereka banyak menanganai masalah keamanan, misalnya DoS Attack (Denial of services Attack), perangkat lunak yang berbahaya (Malicious), Bahkan akan banyak mengunakan perangkat lunak komputer forensik dalam pekerjaannya.

Investigator

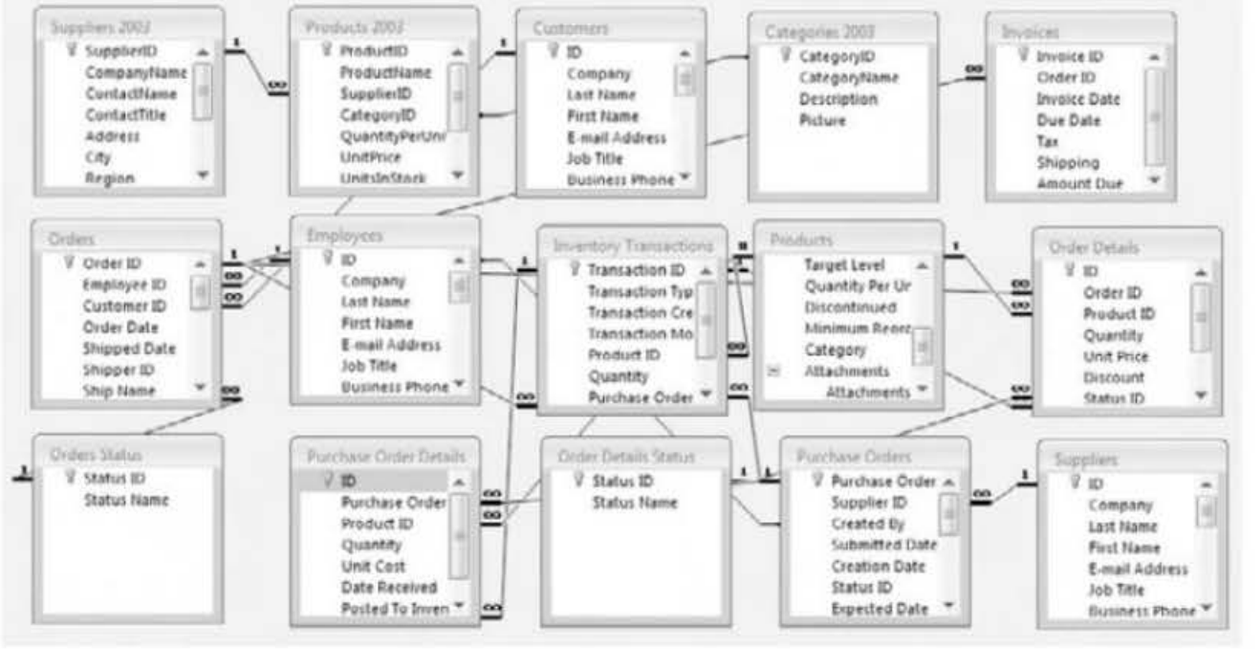
Umumnya, investigator difungsikan dalam menangani kejadian sehubungan tindak kriminal. Investigator berperan dalam menerapkan ilmu komputer forensik.

Database

Umumnya database dikelompokkan pada software aplikasi, meskipun demikian database sudah memiliki ranah keilmuan tersendiri karena fungsinya dalam manajerial data yang tergolong penting.

Database umumnya dikelompokan ke dalam dua bagian digolongkan berdasarkan ketahannya dalam mengorganisasi data, ada Database skala desktop dengan akses multi user dan database skala server karena difungsikan khusus sebagai Database server dengan metode Akses Client Server.

Database adalah sumber penting dalam mengalokasikan data dan menganalisa data. Bahkan konsep data mining yang dibangun karena kemampuan basis data atau database yang menjadi sumber yang bernilai dalam komputer forensik untuk menguak fakta.



Gambar 2.3 Database pada database designer

Data dan Informasi

Data mengacu pada kepingan informasi digital dengan ragam file format. Data umumnya melekat pada berbagai media penyimpanan, menjadi satu paket yang tidak terpisahkan.

Anda dapat menemukan data pada berbagai macam perangkat, misalnya saja:

- Data yang ada pada perangkat jaringan komputer.
- Data aktif, memaksudkan data yang ada dalam sistem komputer yang sedang berjalan, misalnya saja dalam memori komputer (RAM).
- Berbagai komputer portable dengan media penyimpan ada didalamnya.
- Peripheral semisal printer pun dapat menyimpan data, misalnya saja printer laser dengan memory 8 MB, yang dimaksudkan untuk menampung data keperluan cetak.
- Berbagai media penyimpanan, misalnya: USB flash disk, multi media card, portable hard disk, dan lainnya.

2.2 Digital Evidence

Evidence yang dimaksud dalam kasus forensik pada umumnya tidak lain adalah informasi dan data. Cara pandangnya sama, tetapi dalam kasus komputer forensik, kita kenal subyek tersebut sebagai digital evidence.

Kerumitan 'digital evidence' terbentuk karena berbagai media penyimpanan yang digunakan dalam menyimpan data atau informasi, hal ini mencakup pula ragam pilihan format file yang digunakan.

Digital evidence pada ruang lingkup komputer forensik digolongkan dalam tiga kategori sebagai berikut:

- Arsip (Archieval Files).
- File Aktif (Active Files).
- Residual Data (Disebut pula sebagai data sisa, data sampingan atau data temporer).

File yang tergolong arsip dimaksudkan karena fungsinya untuk pengarsipan, mencakup penanganan dokumen untuk disimpan dan format yang ditentukan, proses mendapatkannya kembali dan pendistribusian untuk lain kebutuhan, misalnya beberapa dokumen yang didigitalisasi akan disimpan dalam format TIFF untuk menjaga kualitas dokumen.

File Aktif, memaksudkan File yang digunakan untuk berbagai kepentingan yang berkaitan erat dengan kegiatan yang sedang dilakukan, misalnya saja file-file gambar, dokumen, teks, dan lainnya.

Sedangkan **File yang tergolong Residual** mencakup file-file yang diproduksi seiring proses komputer dan user beraktifitas, misalnya catatan user dalam menggunakan internet, database log, berbagai file temporer.

Digital evidence tersebar dalam berbagai media dan konteksnya, untuk itu diperlukan kejelian yang lebih dari sekadar klasifikasi data untuk tujuan forensik. Perhatikan sumber-sumber potensial evidence dalam ranah komputer forensik sebagai berikut:

Sistem Komputer

Sistem komputer merupakan kombinasi dan integrasi komponen-komponen komputer untuk menjadikannya sebagai sistem yang bekerja.

Komponen inti penyusun sistem komputer dapat dijabarkan sebagai berikut: Central Processing Unit (CPU), data storage atau dikenal dengan

istilah media penyimpanan, dan kemudian ditambahkan berbagai perangkat yang mencakup device dan peripheral untuk memperluas kemampuan komputer, seperti misalnya: monitor, keyboard, and mouse.

Ada banyak bentuk-bentuk sistem komputer dengan ragam spesifikasi, mulai dari mainframe/super komputer, mini komputer, mikro komputer semisal: laptop, desktop komputer, PDA, dan berbagai ubiquitous computer (gadget).

Perlu diingat pula, semakin banyak peripheral atau device yang diintegrasikan ke dalam sistem komputer akan semakin kompleks dan melibatkan banyak pertimbangan untuk mengalamati digital evidence.

Apa pun jenis komputernya, tantangan utama adalah keberhasilan dalam mendapatkan informasi yang ada pada sistem komputer sehubungan digital evidence. Banyak file dapat dijadikan acuan untuk memulai penyaringan evidence, file yang diciptakan user secara langsung menjadi salah satu yang akan memunculkan evidence. Dalam hal ini, file tersebut kita berikan istilah sebagai *user created files*.

User-Created Files

User-created files merupakan salah satu evidence yang sangat penting, di mana seiring dengan aktivitasnya dalam menggunakan komputer, akan ada data yang ditambahkan dan diciptakan, misalnya user mengorganisasi aktivitasnya dalam e-calender, file-file grafik yang disimpan, dan lainnya.

Pelacakan dengan penanganan tertentu mampu menegaskan dan meng-uak karakter yang tersembunyi, misalnya address book yang dikaitkan dengan aktivitas tindak kejahatan, berbagai gambar bergerak dan tidak bergerak yang mungkin menjurus pada pelecehan seksual melibatkan anak-anak, komunikasi yang menjurus pada kriminalitas dengan e-mail, atau mungkin transaksi obat-obat terlarang pada spreadsheet file.

Berikut beberapa yang dikategorikan dalam user-created files:

- Address books.
- Audio/video files.
- E-Calendars.
- Database files.
- Dokumen dan file teks.
- File e-mail.
- Image/grafik files.
- Internet bookmarks/favorites.
- File spreadsheet.
- User-protected files.

'Pelaku tindak kejahatan' pasti akan menjaga kerahasiaan file-file tersebut agar tidak sembarangan di 'expose'. Misalnya saja, sang pelaku menghapus riwayat berselancar di internet atau menyembunyikan file yang tersimpan di komputer.

Berbagai metode penyembunyian dilakukan seperti misalnya enkripsi file dan berbagai metode dengan akses penggunaan password. Bukan hanya sampai di situ saja, penyembunyian dilakukan pada sistem komputer yang dipisahkan atau pemisahan secara fisik pada media penyimpanan, misalnya dengan menggunakan USB flash disk yang dapat dengan mudah diintegrasikan dan didiskonekasikan dari komputer.

Berikut berbagai cara yang dilakukan untuk menjaga pengaksesan file yang dapat menghambat penggalian dan menemukan evidence:

- File terkompresi.
- Salah menamakan file secara disengaja atau tidak.
- Salah dalam memberikan file format, secara disengaja atau tidak.
- File yang diproteksi dengan password.
- Hidden files.
- File Terenkripsi.
- Steganography.

Evidence tidak hanya ditemukan pada user created file semata, seperti dikatakan sebelumnya bahwa ada banyak yang tersembunyi dalam sistem komputer, berbagai aktivitas dan proses sistem komputer yang 'tersembunyi' dari user dapat dijadikan pula sebagai evidence.

Ini mencakup pada berbagai catatan dan laporan dari aktifitas sistem komputer, tentunya berperan dalam memuncukan evidence jenis ini. Misalnya saja:

- Passwords.
- Aktivitas berinternet.
- Temporary backup files.
- Temporary installation files.

Informasi tersebut dapat di-recovery dan dianalisa pada proses forensik.

Kita katakan evidence jenis ini ke dalam *Computer-Created Files*, dikarenakan file-file tersebut secara otomatis diciptakan oleh sistem operasi atau sistem utility seraya komputer menjalankan prosesnya atau seraya user menggunakan sistem komputer, mencakup aktifitas semisal:

waktu dan jam menyangkut file tertentu, modifikasi yang mungkin dilakukan terhadap suatu file, penghapusan waktu pengaksesan, pemiliki dari file tersebut dan berbagai atribut file.

Berikut ini sumber-sumber dari terbentuknya Computer Created-Files:

Computer-Created Files:

- File backup.
- Registry (Windows Registry).
- File log.
- File konfiguration.
- Printer spool files.
- Cookies.
- Swap files.
- Hidden files.
- File system.
- History files
- File temporer.
- Temp files lainnya (Anda temukan file dengan format .TMP).
- Berbagai data areas.
- Bad clusters.
- Computer date, time, and password.
- Deleted files.
- Free space.
- Partisi yang tersembunyi.

- Lost clusters.
- Metadata.
- Partisi-partisi lainnya.
- Reserved areas.
- Slack space.
- Software registration information.
- Area sistem.
- Unallocated space.

Akan dicontohkan sebagian dari penggalian terhadap computer created file dalam kasus Windows Registry untuk keperluan forensik pada bab-bab selanjutnya.

Kemampuan seperti ini tidak harus Anda dapatkan dalam komputer forensik, bahkan pengguna yang terampil pun dapat mempelajarinya dengan mudah.

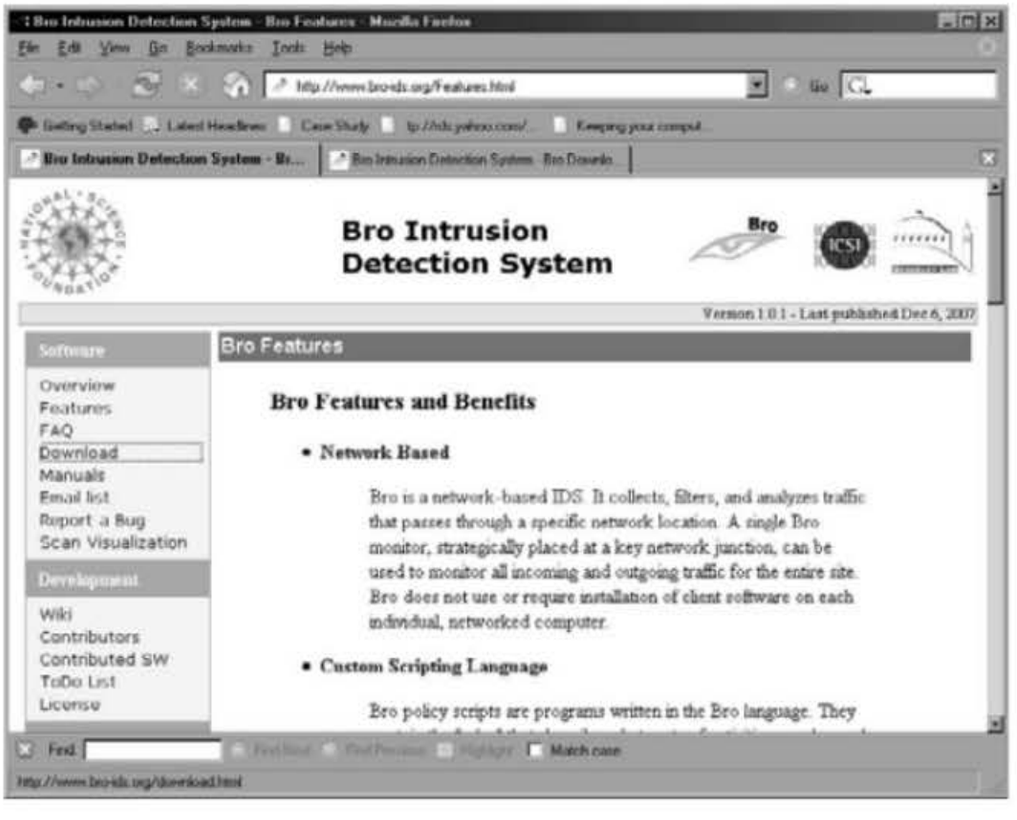
2.3 Peralatan Komputer Forensik

Berbagai software forensik dibuat untuk menangani spesifikasi kebutuhan komputer forensik, meskipun pada praktiknya Anda dapat saja menggunakan berbagai utility yang banyak digunakan untuk keperluan performasi komputer, kemaman, dan berbagai utility non spesifik forensik.

Berikut disajikan berbagai software yang digunakan mencakup website untuk mengakses informasi perihal software yang dimaksud.

2.3.1 Intrusion Detection and Prevention System

Gambar 2.4 Honeypots.net
(link:http://www.honeypots.net/ids/products)



Gambar 2.5 Bro Intrusion Detection System
(Link:http://www.bro-ids.org/Features.html)

Gambar 2.6 ISS Proventia Enterprise Protection by Internet Security Systems (ISS) (Link:http://www.iss.net/products/index.html)

Gambar 2.7 Network packet sniffers and protocol analyzers Packet Storm. (Link:http://packetstormsecurity.org/defense/sniff/)

2.3.2 Network Protocol Analyzers Softpedia

Anda dapat menemukan berbagai aplikasi gratis (freeware) dan GLP sebagai berikut:

- WinPcap 4.1 Beta 2.
- WinPcap memungkinkan Anda untuk meng-capture dan men-transmisikan network packet dengan mem-bypass stack protocol, aplikasi ini dijalankan pada sistem operasi Windows, ukuran file download terbilang kecil, hanya sebesar 535 KB.
- IP Sniffer 1.95.0.2. Freeware yang mampu menganalisa protocol yang menggunakan sistem operasi XP/2K Raw Socket, ukuran file download: 5.97 MB, dan dapat dijalankan pada berbagai versi Windows.
- SniffPass 1.03. Mampu meng-capture password yang melewati network adapter komputer, file download berukuran: 41 KB dan dijalankan dalam lingkungan Windows.
- SmartSniff 1.35. SmartSniff akan meng-capture paket-paket TCP/IP dan mem-view data tersebut, ukuran file sebesar 57 KB, dan dijalankan pada lingkungan Windows.
- Wireshark (formerly Ethereal) 0.99.7. Wireshark, protocol analyzer gratis untuk sistem Unix dan Windows.
- Free HTTP Sniffer 1.0. Software ini mampu melakukan tracking dalam menemukan informasi URLs yang lalu lalang pada LAN. Berukuran 1.39 MB dan dapat dijalankan dalam lingkungan Windows.

Gambar 2.8 Link:http://www.softpedia.com/get/Network-Tools/Protocol-Analyzers-Sniffers/

2.3.3 Beragam Utilitas dan Network Tool

Forensic and Incident Response Environment (F.I.R.E.)

Pada website tersebut dapat Anda temukan berbagai software forensik dengan lisensi GPL (GNU General Public License).

Gambar 2.9 Forensic and Incident Response Environment (F.I.R.E.) (Link:http://fire.dmzs.com/?section=tools)

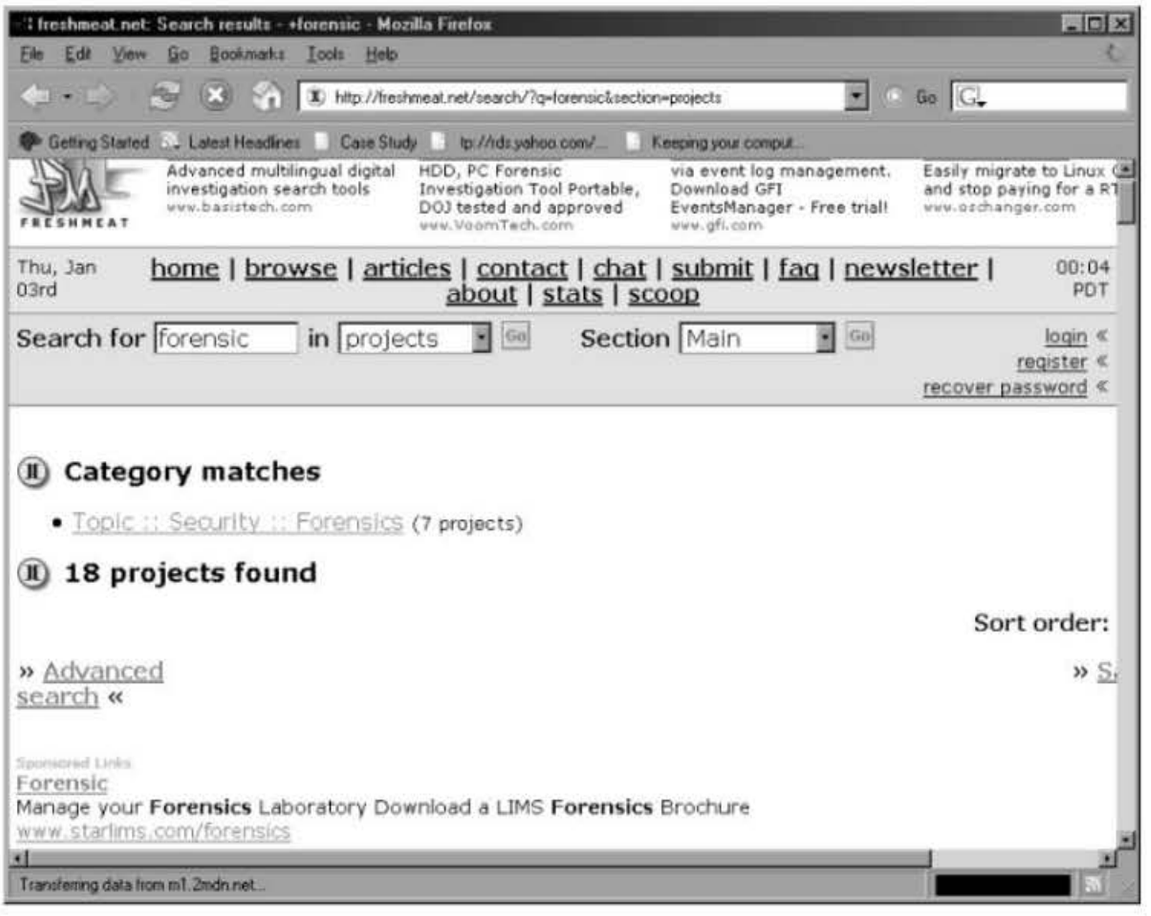
Foundstone

Pada website ini dapat ditemukan perangkat lunak forensik gratis, misalnya The Forensic ToolkitTM v2.0 untuk melakukan pengetesan/ pengujian pada NTFS, masih banyak software yang ditawarkan semisal:

- DumpAutoComplete v0.7.
- Pasco v1.0.
- Galleta v1.0.
- Rifiuti v1.0.
- NTLastô v3.0.
- ShoWinô v2.0.
- PatchItô v2.0.
- Visionô v1.0.
- BinText.

Gambar 2.10 Website Founstone (Link:http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm)

Freshmeat

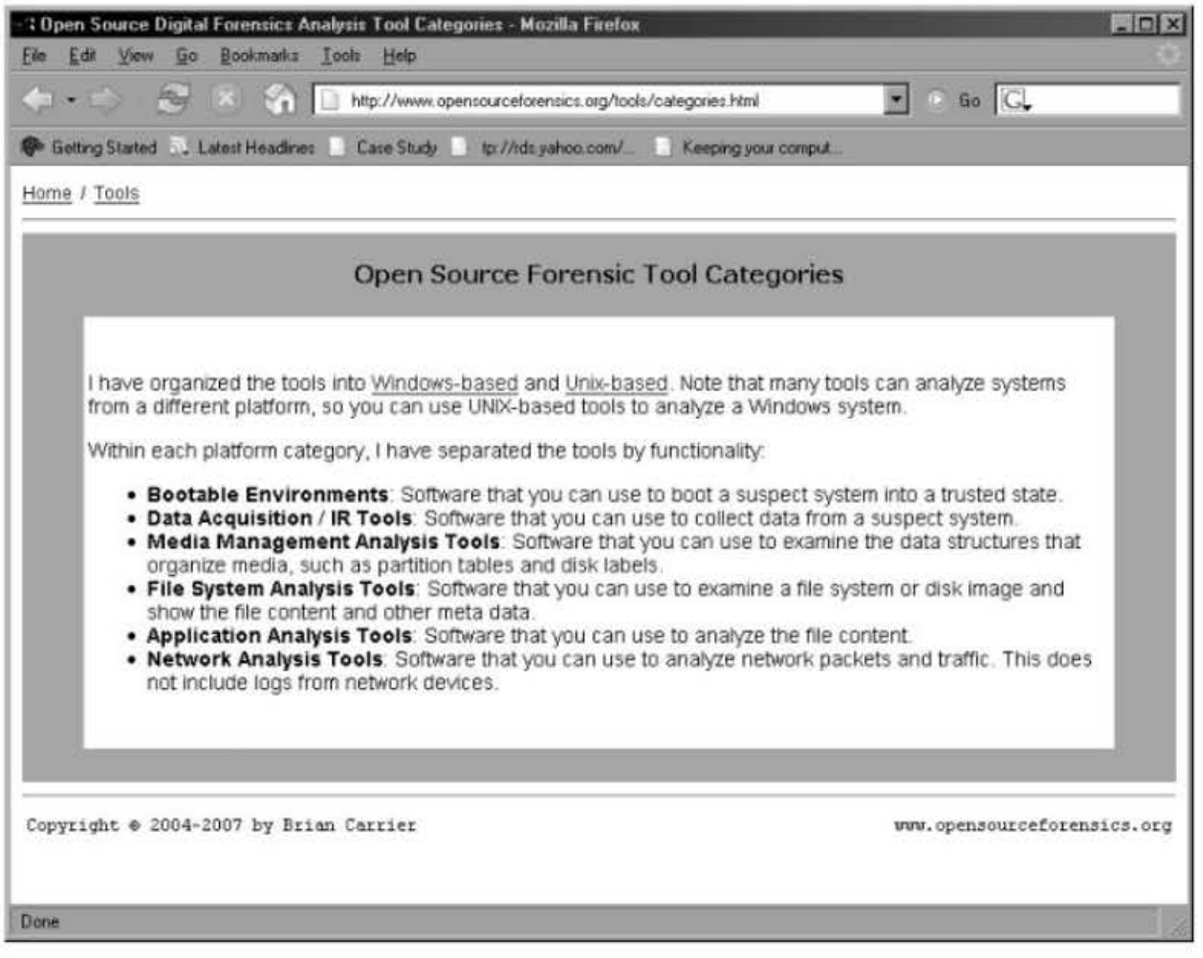


Gambar 2.11 Website Freshmeat (Link:http://freshmeat.net/search/?q=forensic&section=projects)

Open Source Digital Forensics Analysis Tool Categories Sofware yang diorganisasi ke dalam beberapa spesifikasi sebagai berikut:

- Bootable Environments: Anda dapat mem boot sistem suspect pada dalam tingkat kelayakan yang terpercaya.
- Data Acquisition/IR Tools: Software ini memungkinkan Anda untuk mengumpulakan berbagai data pada sistem yang dicurigai (suspect).
- Media Management Analysis Tools: Software ini memungkinkan Anda untuk melakukan pemeriksaan terhadap struktur data dan media, semisal tabel partisi.

- File System Analysis Tools: Pemeriksaan file sistem dan disk image, menampilkan konten file dan meta data dimungkinkan oleh software ini.
- Application Analysis Tools: Anda dapat menganalisa konten file menggunakan software ini.
- Network Analysis Tools: Software ini dapat Anda gunakan dalam menganalisa paket-paket network dan lalulintas jaringan.



Gambar 2.12
Link:http://www.opensourceforensics.org/tools/categories.html

Penguin Sleuth Kit

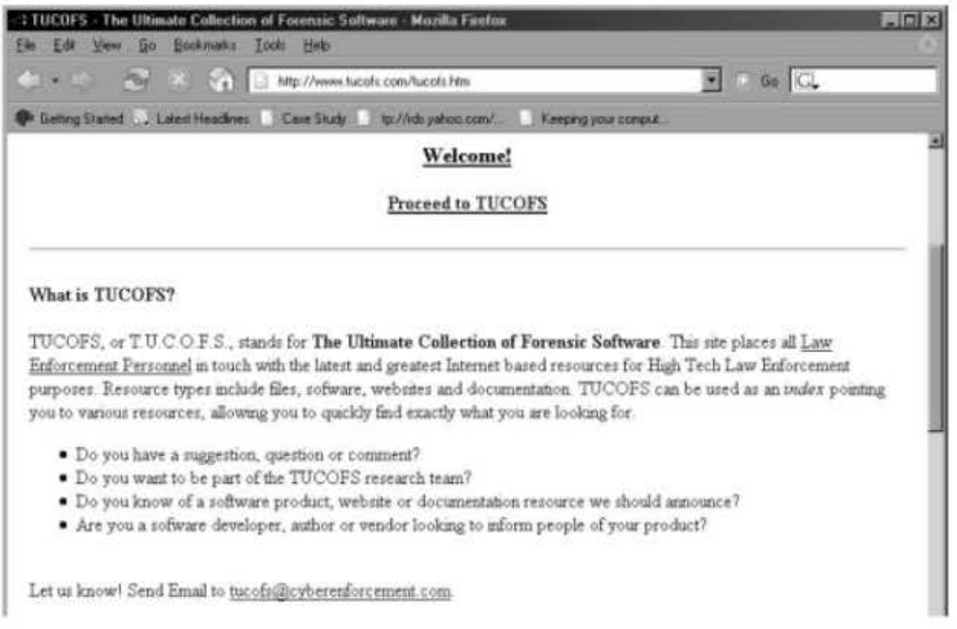
Gambar 2.13 Link:http://www.linux-forensics.com/forensics/pensleuth.html

Talisker Security Wizardry Portal http://www.networkintrusion.co.uk/

The Sleuth Kit

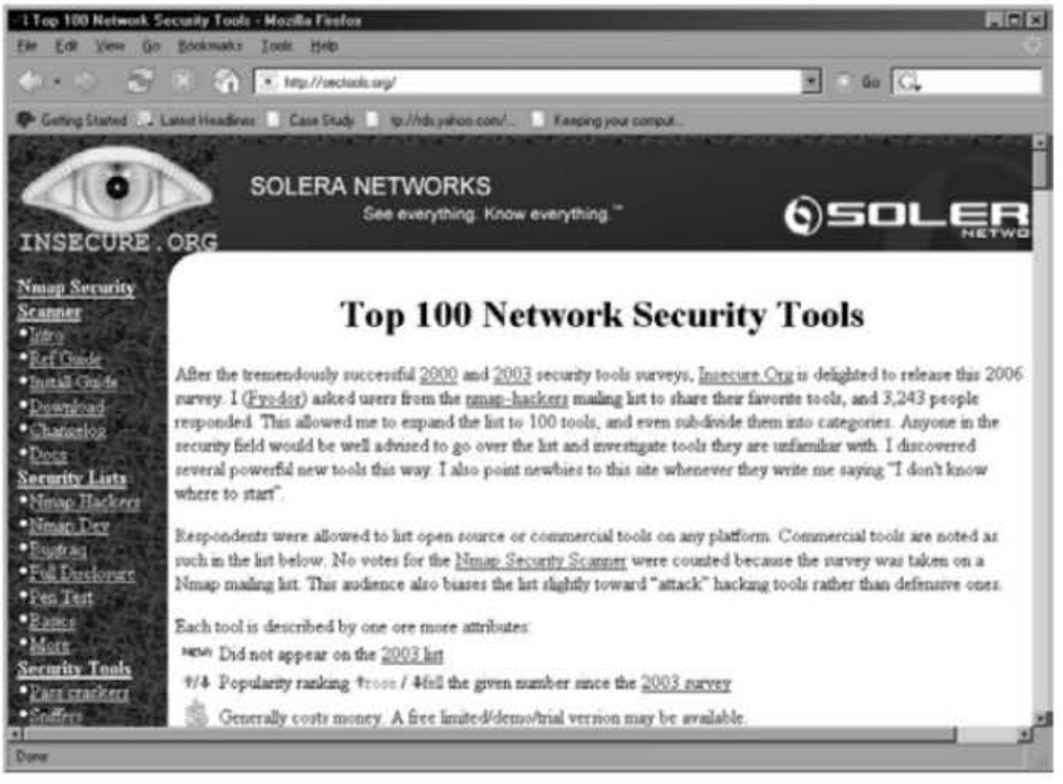
Link:http://www.sleuthkit.org/sleuthkit/tools.php

The Ultimate Collection of Forensic Software (TUCOFS)



Gambar 2.14 Link:http://www.tucofs.com/tucofs.htm

Top 75 Security Tools



Gambar 2.15 Link:http://www.insecure.org/tools.html

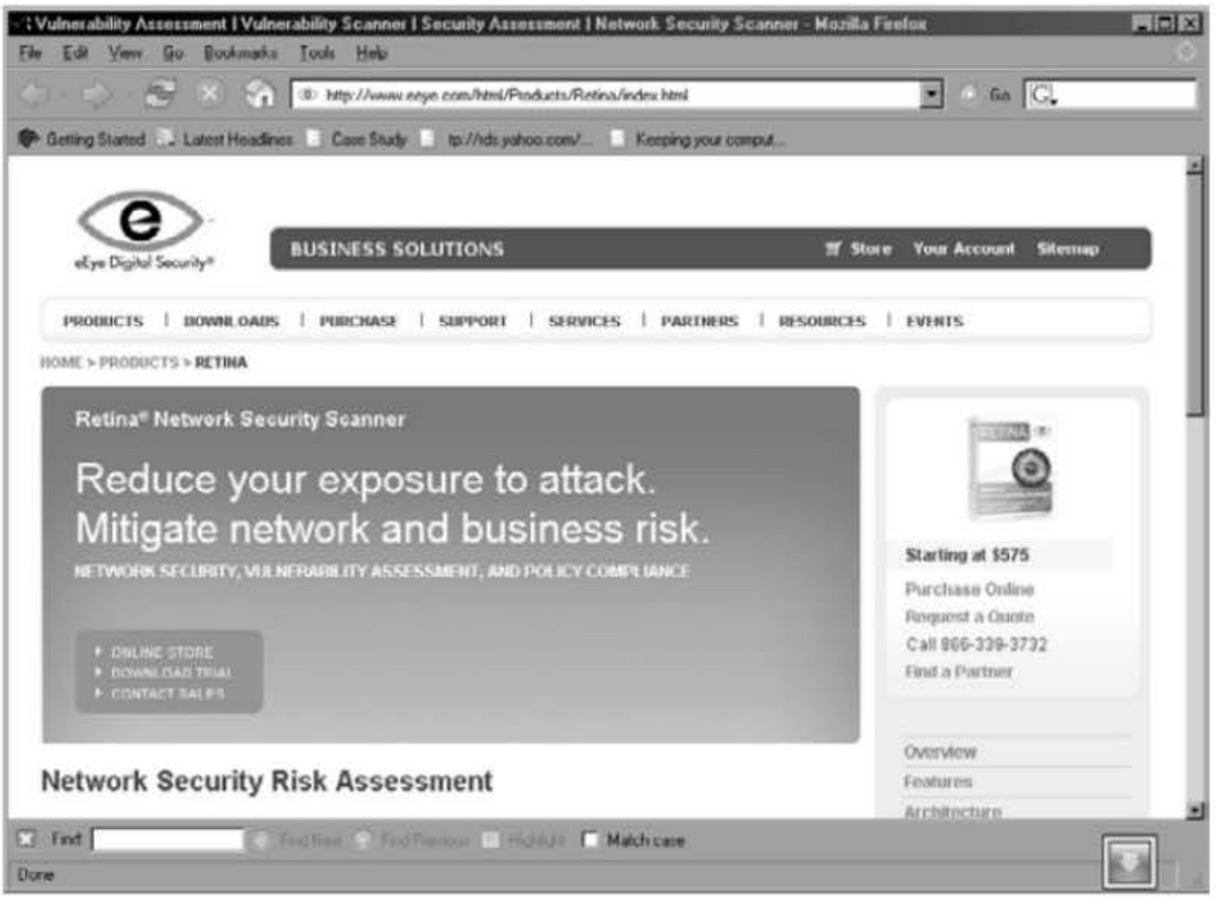
Trinux

Gambar 2.16 Link:http://trinux.sourceforge.net/

Ada banyak aplikasi yang ada dapat temukan pada Trinux, misalnya beberapa aplikasi berikut:

- Retina: Software komersial produksi eEye yang mampu men-scan lubang-lubang keamanan, mencakup hosts yang ada pada jaringan dan memberikan laporan jika ditemukan kelemahan sistem. Link sebagai berikut:

  (http://www.eeye.com/html/Products/Retina/index.html).



Gambar 2.17 http://www.eeye.com/html/Products/Retina/index.html

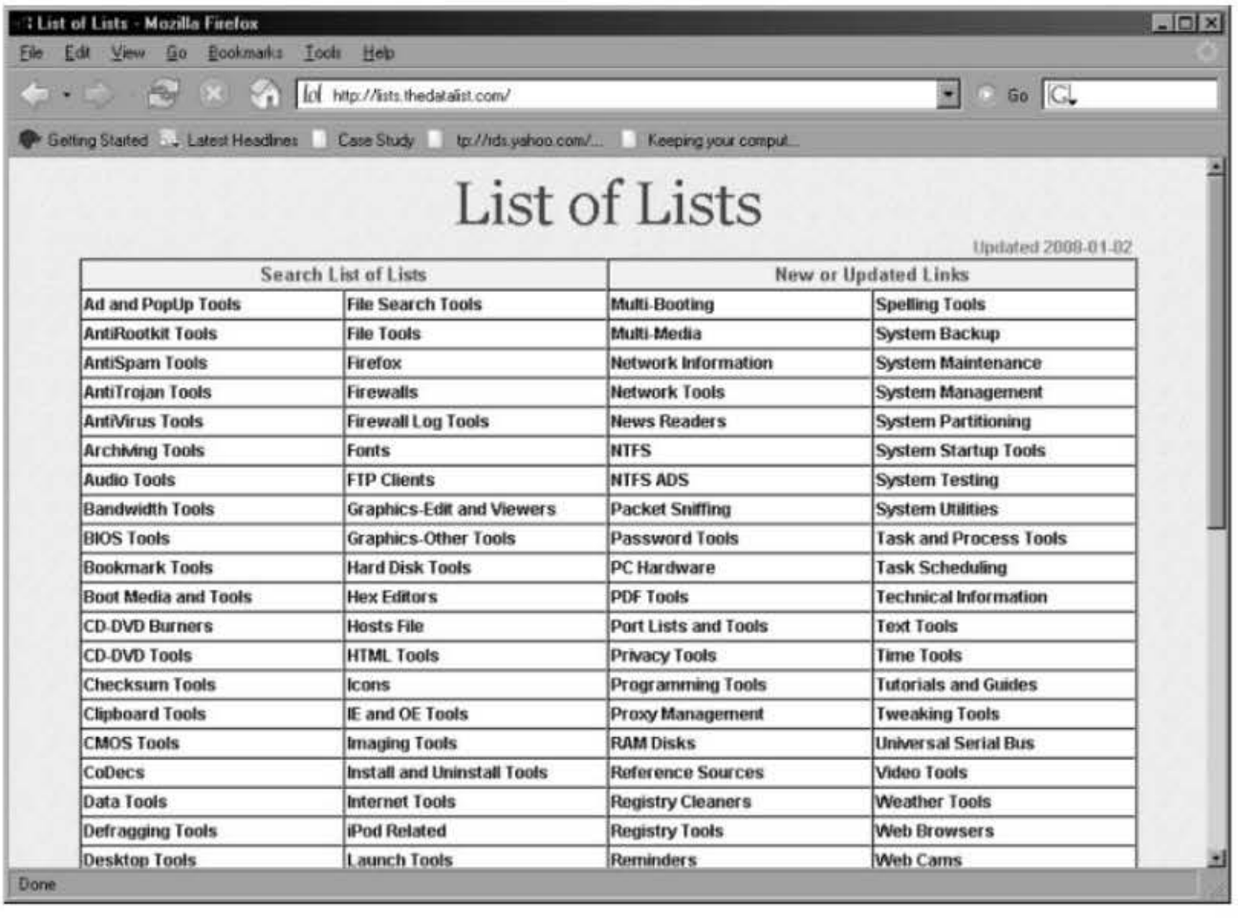
- NetStumbler: Free Windows 802.11 Sniffer. Aplikasi dengan platform sistem operasi Windows yang mampu untuk menemukan wireless access points yang didapati terbuka (wardriving), disediakan pula versi yang dapat dijalankan Platform a WinCE untuk PDA.

- WebInspect, salah satu Web Application Scanner yang tangguh. SPI Dynamics' WebInspect "application security assessment tool" membantu Anda dalam mengenali kelemahan pada lapisan application web. Menganalisa apakah Webserver dikonfigurasi dengan benar melalui serangkaiaan pengujian berupa serangan web seperti: parameter injection, cross-site scripting, directory traversal, dan lain sebagainya.

Berbagai Tool Komputer lainnya non kategori di atas:

Checksum Tools

Dalam website ini dapat Anda temukan banyak sekali list dari software yang dapat dijadikan sebagai alat forensik.

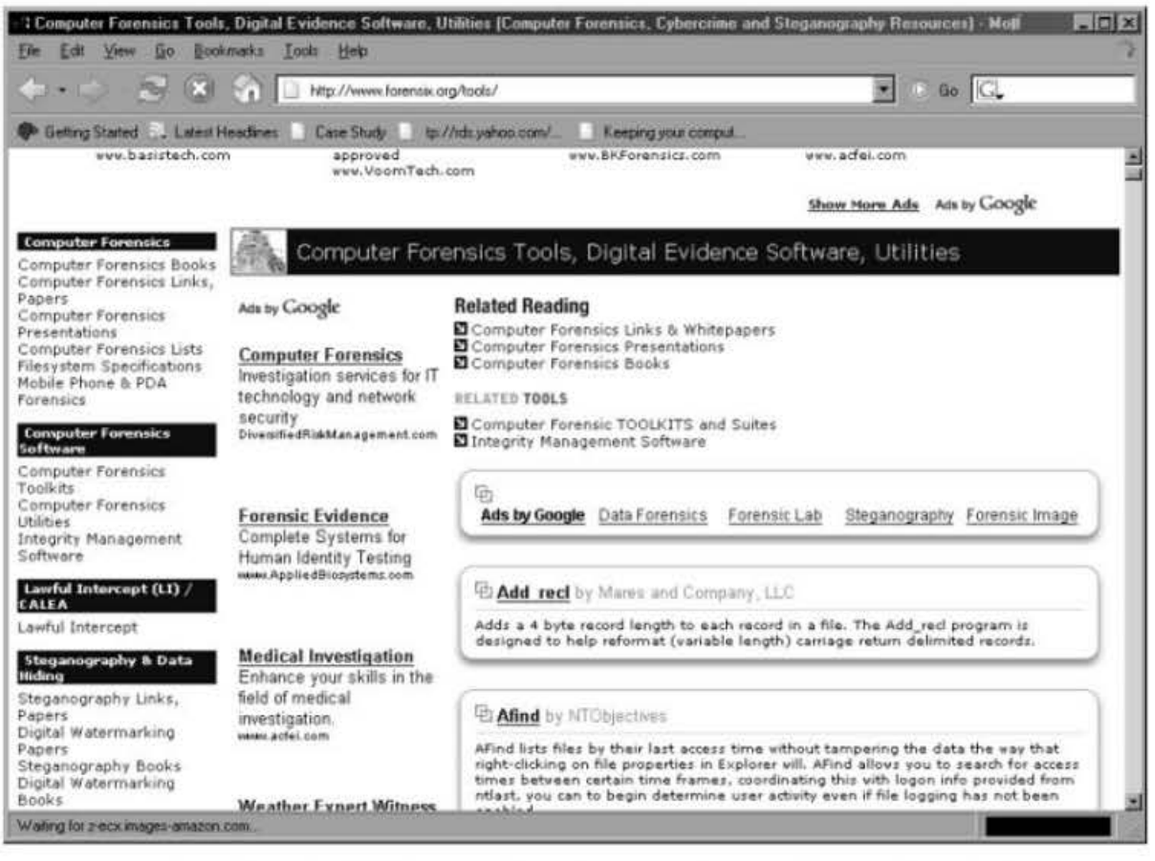


Gambar 2.18 http://lists.thedatalist.com/pages/Checksum_Tools.htm

Computer Forensics Tools, Software, Utilities

Dalam Website Forensix.org banyak dokumentasi, buku berbenaan forensik, termasuk software forensik yang dikeompokan ke dalam 3 bagian, antara lain:

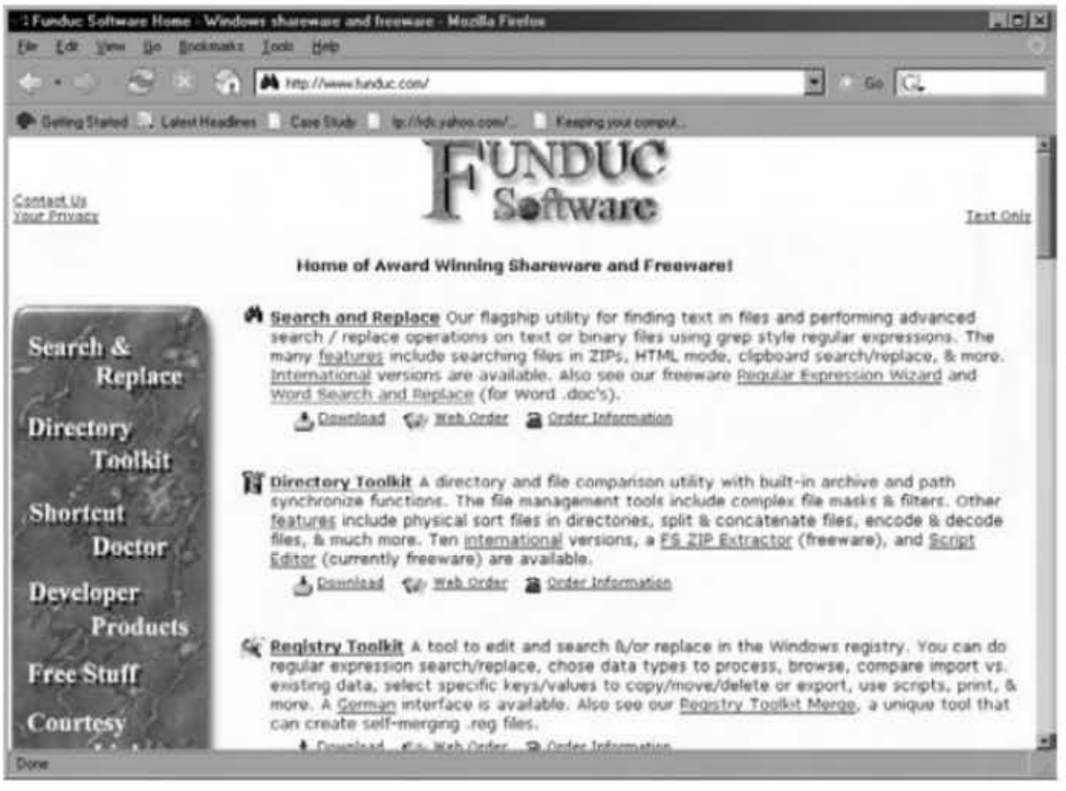
- Computer Forensics Toolkits.
- Computer Forensics Utilities.
- Integrity Management Software.



Gambar 2.19 Link:http://www.forensix.org/tools/

Funduc Software

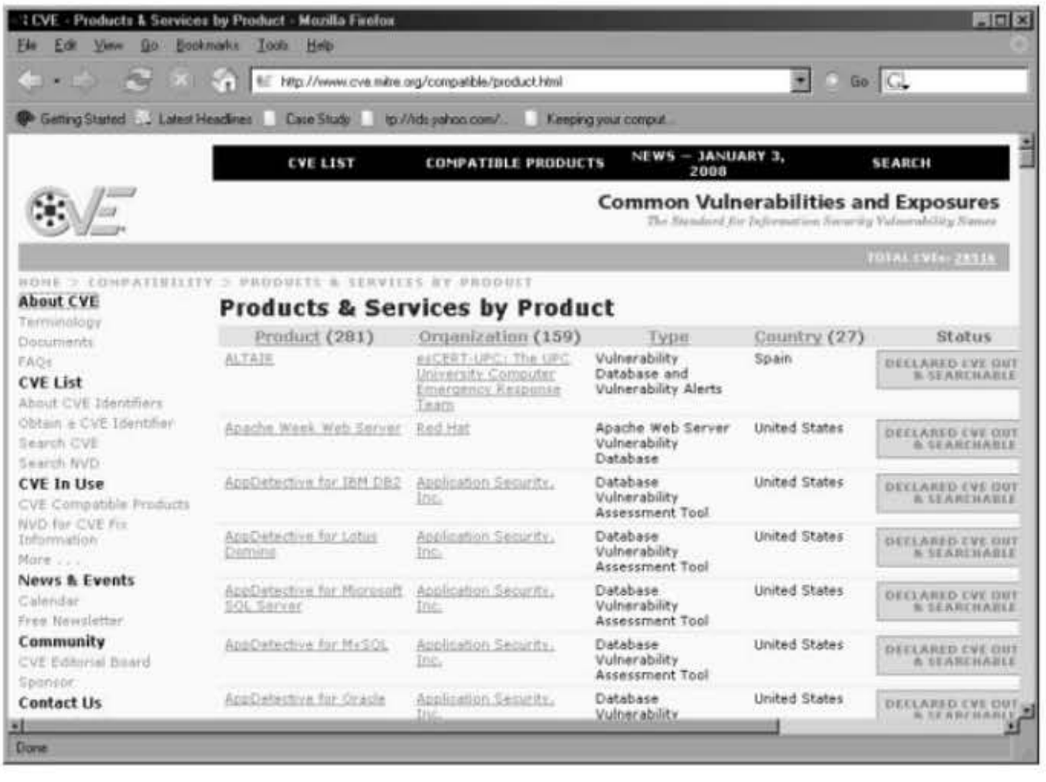
Di sini, Anda dapat temukan berbagai shareware dan freeware software forensik.



Gambar 2.20 Website FunDuc (Link:http://www.funduc.com/)

2.3.4 Berbagai Network Tool

Common Vulnerabilities and Exposures (CVE)



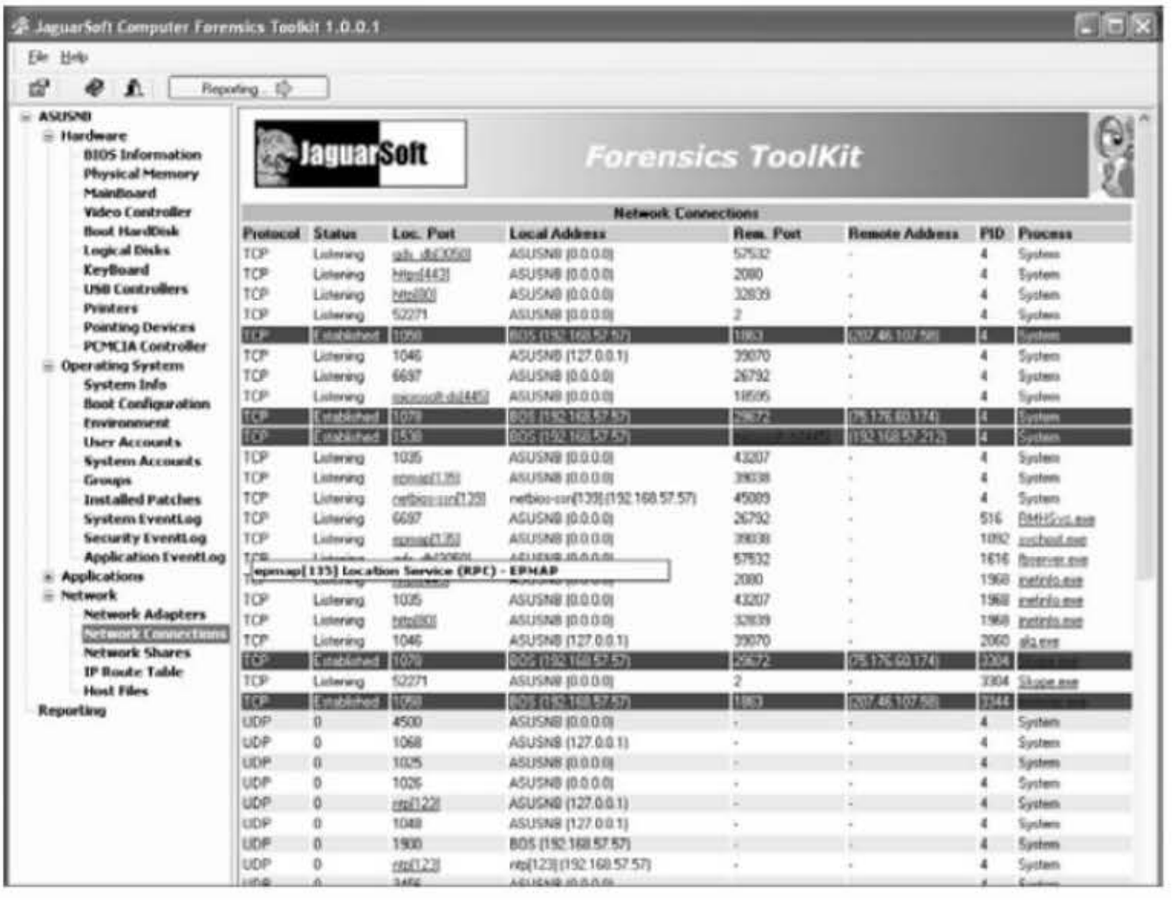
Gambar 2.21 Website CVE
(Link:http://www.cve.mitre.org/compatible/product.html)

Banyak sekali software spesifikasi forensik yang memiliki fitur yang mengakomodasi prosedur forensik, salah satunya Anda dapat menggunakan software komersial semisal Jaguar Forensics Toolkit.

Berdasarkan lansiran website-nya, Jaguar Forensics mampu membuat laporan HTML rinci Easly dengan analyzing terkenal BHO & Toolbar. Software ini dapat mendeteksi Rootkit & Hooks API, proses tersembunyi dan driver tersembunyi, memeriksa semua penggunaan & sumberdaya yang di-share pada jaringan, dan memverifikasi digital signature.

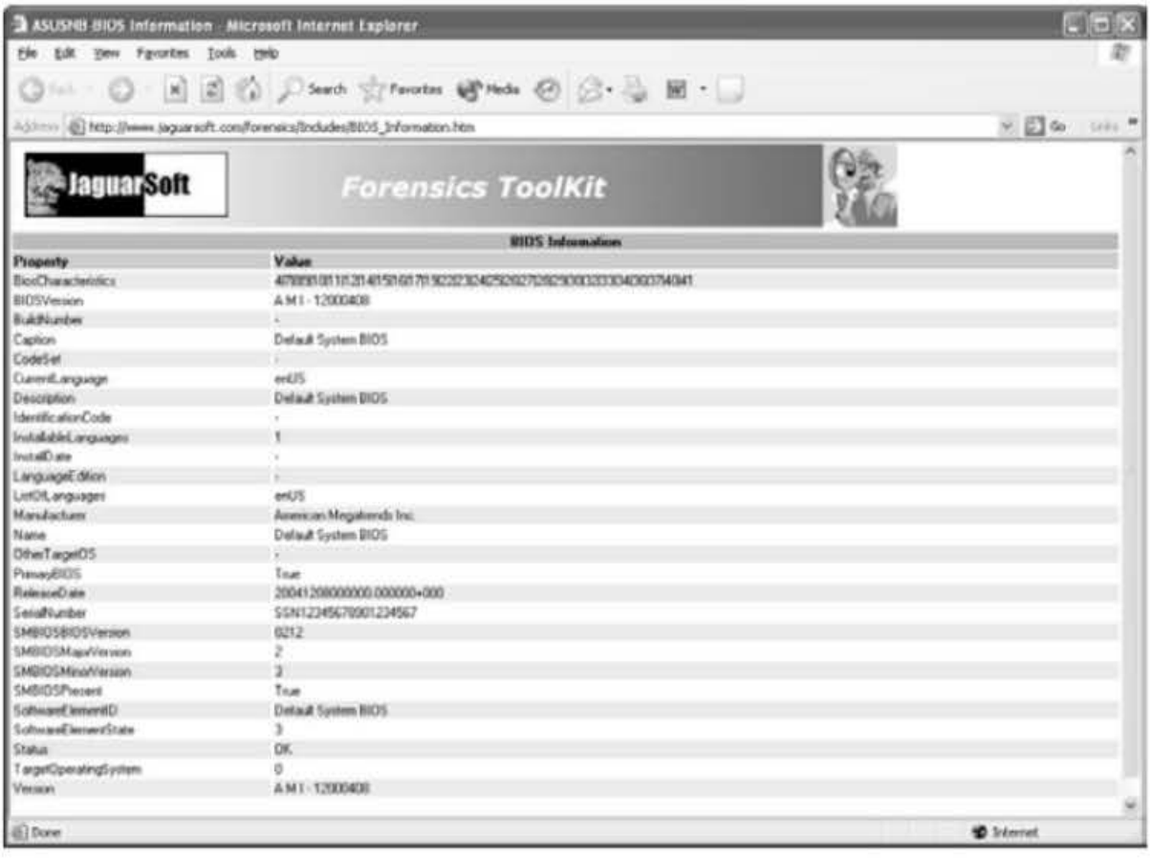
Dapat Anda perhatikan pada gambar-gambar berikut berdasarkan website yang disediakan, percontohan ditampilkan dalam website tersebut, dan Anda dapat men-download brosur untuk melihat spesifikasi software tersebut.

Gambar 2.22 Website JaguarSoft.com

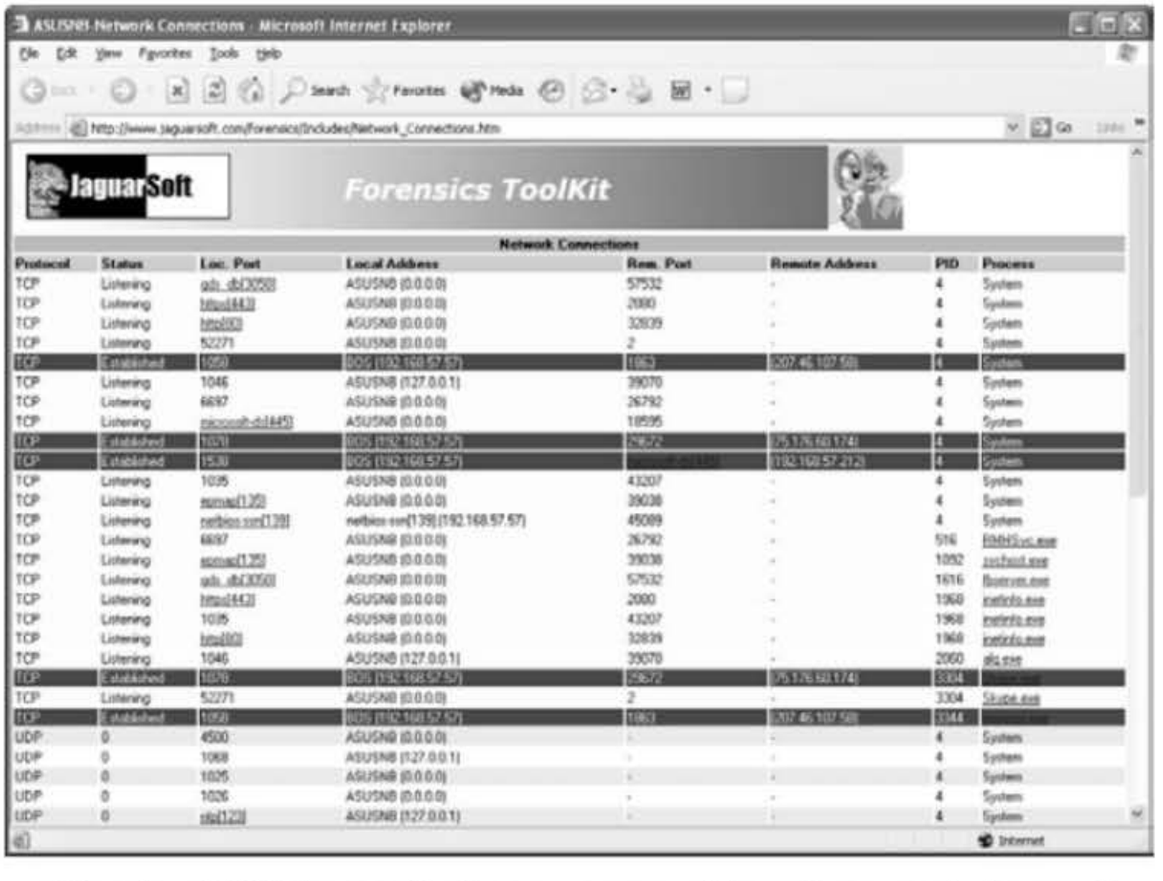


Gambar 2.23 Antarmuka Jaguar Forensics Toolkit

Gambar 2.24 Produk Jaguar Forensics Toolkit – memindai file yang sedang berjalan



Gambar 2.25 Website JaguarSoft.com – BIOS Information Report



Gambar 2.26 JaguarSoft yang menyajikan laporan informasi koneksi jaringan komputer

Gambar 2.27 Dokumentasi JaguarSoft yang dapat di-download pada website JaguarSoft.com

2.3 Fakta di Balik Forensik

Proses menemukan fakta melibatkan kemampuan dalam mengalamati sumber fakta. Pada komputer forensik, fakta potensial atau barang bukti dapat dialokasikan langsung pada komponen spesifik komputer yang berelasi dengan 'jenis' kejahatannya. Perhatikan beberapa sumber yang dapat dijadikan bukti potensial sebagai berikut:

Central Processing Unit (CPU)

Dikatakan sebagai otak dari komputer (processor) yang dialokasikan pada komputer/ kotak CPU.

Bukti Potensial:

- Bukti dari tindak pencurian.

- Pemalsuan.
- Remarking.

Memori (RAM)

Perangkat ini sering dikatakan sebagai primary storage device dan tergolong ke dalam media penyimpanan volatile, dan menjadi bagian penting dalam CPU untuk melakukan berbagai proses, termasuk sistem operasi dan program aplikasi.

Bukti potensial (perangkat itu sendiri):

- Bukti dari tindak pencurian.
- Pemalsuan.
- Tanda-tanda yang terlihat (Remarking).

Access Control Devices

Mencakup di dalamnya:

- SmartCard - Perangkat ini ringkas, maka dari itu dikategorikan sebagai handheld device, yang memiliki micropocessor terintegrasi, mermiliki keampuann seperti menyimpan nilai mata uang, kunci enkripsi, dan *authentication information* dengan penggunaan password, *digital certificate*, dan informasi lainya.
- Dongle, perangkat yang diintegrasikan pada port komputer.
- Biometric scanner, perangkat ini umumnya dikoneksikan dengan komputer, difungsikan untuk mengenali karakteristik fisik dari user seperti sidik jari, suara, bahkan retina. Hak akses untuk penggunaan program atau sistem komputer diberikan kepada user melalui identifikasi terlebih dahulu.

Bukti potensial:

- Identifikasi informasi user.
- Tingkat akses.
- Konfigurasi.
- Perizinan.
- Perangkat itu sendiri.

Mesin Penjawab (Answering Machine)

Perangkat ini diintegrasikan dengan telepon, dipasang sedemikian rupa antara line telepon dan telepon.

Pita Magnetis atau electronik (digital) recording system mungkin digunakan untuk menyimpan informasi audio.

Perangkat ini sangat mengandalkan baterai dengan kemampuan terbatas, dibutuhkan penanganan sedemikian rupa karena data dalam prosesnya mungkin terlebih jika kapasitas baterai sudah habis.

Untuk keperluan forensik, hal demikian harus diinformasikan kepada petugas (misalnya: evidence custodian, lab chief, forensic examiner).

Bukti potensial:

- Caller identification information.
- Pesan-pesan terhapus.
- Last number called.
- Memo.
- Nama dan nomor telepon.
- Tapes (media penyimpanan).

Kamera Digital

Perangkat ini difungsikan sebagai alat perekam image, video dalam format digital yang kemudian disimpan pada berbagai media penyimpanan dan memiliki kemampuan untuk tranfer data dan mengintegrasikan pada sistem komputer.

Bukti potensial yang terdapat pada kamera digital:

- Image.
- Informasi tanggal dan waktu.
- Removable cartridge.
- Video.
- Sound.

Handheld Devices (mencakup di dalamnya Personal Digital Assistants - PDA, Electronic Organizers)

Perangkat semacam ini disebut pula sebagai gadget, small device yang mengintegrasikan sistem komputer, telephone/ fax, paging, bahkan integrasi jaringan.

Kebutuhan organizer menjadi salah satu faktor yang memampukan perangkat sejenis ini. Terlebih saat ini gadget hadir dengan wujud yang ringkas, kapasitas memori yang besar, kemampuan komunikasi dan peningkatan kapasitas komputasi, membuat perangkat ini praktis dan banyak diminati.

Penanganan perangkat ini sebagai evidence punya banyak pertimbangan dan pemberlakukan, salah satunya karena power yang terbatas mengandalkan baterai, sehingga jika data terus 'berjalan' mungkin saja akan kehilangan karena power yang terbatas.

Bukti potensial:

- Buku alamat.
- Appointment calendars/information.
- Dokumen.
- E-mail.
- Handwriting (tulisan tangan).
- Password.
- Buku telepon.
- Pesan-pesan teks.
- Voice messages.

Hard Drive

Jika Anda berbicara mengenai hard drive, memaksudkan hard disk, di mana perangkat baca tulis terintegrasi dengan media penyimpanan berupa plat-plat magnetis yang adalah media penyimpanan populer saat ini, dan menjadi kebutuhan dari suatu sistem komputer.

Sampai saat ini, ketersediaan hard drive dengan kapasitas penyimpanan yang sangat besar merupakan hal yang umum. File-file yang banyak diakses pada sistem komputer dengan kapasitas yang besar pastinya disimpan pada hard disk, semisal berbagai file image, audio dan video, dokumen teks, dan lain sebagainya.

Bukti potensial yakni semua file yang tersimpan pada hard disk termasuk seluruh informasi sistem komputer yang juga tersimpan pada hard disk.

Memory Card

Memory card digunakan sebagai media penyimpanan yang removable, dan tergolong non-volatile (data tidak akan hilang walaupun listrik/power dimatikan).

Berbagai perangkat yang tergolong ke dalamnya antara lain:

- Memory stick.
- Smart card.
- Flash memory.
- Flash card.

Bukti Potensial yang ada tidak jauh berbeda dari bukti potesial dari sistem komputer, yakni semua data atau file yang terbaca dalam media tersebut.

Modem

Berbagai penggolongan modem mencakup:

- Internal.
- External:
    - Analog.
    - DSL.
    - ISDN.
    - Cable.
    - Wireless modem.
    - PC cards.

Merupakan perangkat komunikasi yang memungkinkan komputer mengakses komputer atau jaringan melalui kabel telepon, wireless, dan berbagai media komunikasi lainnya. Bukti potensial yakni perangkat itu sendiri.

Local Area Network (LAN) Card atau Network Interface Card (NIC)

Perangkat ini memungkinkan komputer untuk diintegrasikan dalam jaringan komputer, teknologi yang digunakan dalam mengusung perangkat

ini tergolong variatif, bahkan karena penggunaan teknologi spesifik, penamaannya mengikuti teknologi yang menyertainya, misalnya kita kenal istilah ethernet card.

Keunggulan dan keuntungan dari jaringan komputer dibangun karena perangkat ini, salah satu fitur yang umum dibangunnya jaringan komputer tidak lain adalah fasilitas sharing sumber daya yang mencakup media penyimpanan, file, printer, scanner, dan berbagai sumber daya komputer lainnya, serta berbagai fasilitas komunikasi.

Bukti potensial:

- Perangkat itu sendiri.
- MAC (Media Access Control) access address.

Routers, Hubs, and Switches

Komponen berikut mejadi kebutuhan dalam jaringin komputer seiring dengan perkembangan jaringan komputer yang dibangun.

Hubs dan Switches umumnya dibangun untuk membuat jaringan skala kecil (Local Area Network). Meskipun demikian, ada perbedaan kapan kita membutuhkan Switch atau Hub. Hub umumnya memiliki keterbatasan dalam membangun jaringan komputer jika dibandingkan Switch.

Router menjadi kebutuhan lain tergantung karakteristik jaringan komputer yang dibangun. Faktor pemampu dari komponen ini tidak lain adalah kemampuan pendistribusian data pada jaringan.

Bukti potensial: Perangakat itu sendiri.

Servers

Server adalah komputer yang digunakan dan dibangun karena kebutuhan spesifik untuk memberikan layanan bagi komputer-komputer lain yang ada dalam jaringan komputer.

Umumnya, komputer server digunakan untuk melayani pemakai terhadap kebutuhan akan:

- E-mail.
- File.
- Penyimpanan.
- Layanan web page.
- Layanan sumber daya printer pada jaringan komputer.

Bukti potensial yakni perangkat server secara keseluruhan.

Gambar 2.28 Komputer Server (Sumber: Wiki.Jahoe. GNU Free Documentation License)

Network Cables and Connectors

Kabel jaringan dan konektor merupakan atribut yang memfasilitasi dibangunnya jaringan komputer.

Ada banyak karakteristik dalam jaringan komputer yang berbeda bahkan untuk tiap developer, seperti warna, ketebalan, komposisi material yang digunakan, demikian pula istilah konektor, ada banyak konektor dengan bentuk dan cara penginstalasian yang berbeda, tergantung dari teknologi dan komponen yang terintegasi terhadapnya.

Bukti potensial: Perangakat itu sendiri.

Pagers

Bukti Potensial:

- Informasi alamat.
- Pesan teks.
- E-mail.
- Voice messages.
- Nomor telepon.

Printers

Perangkat output populer untuk menghasilkan/mentransalasikan informasi dalam media tercetak (gambar, teks).

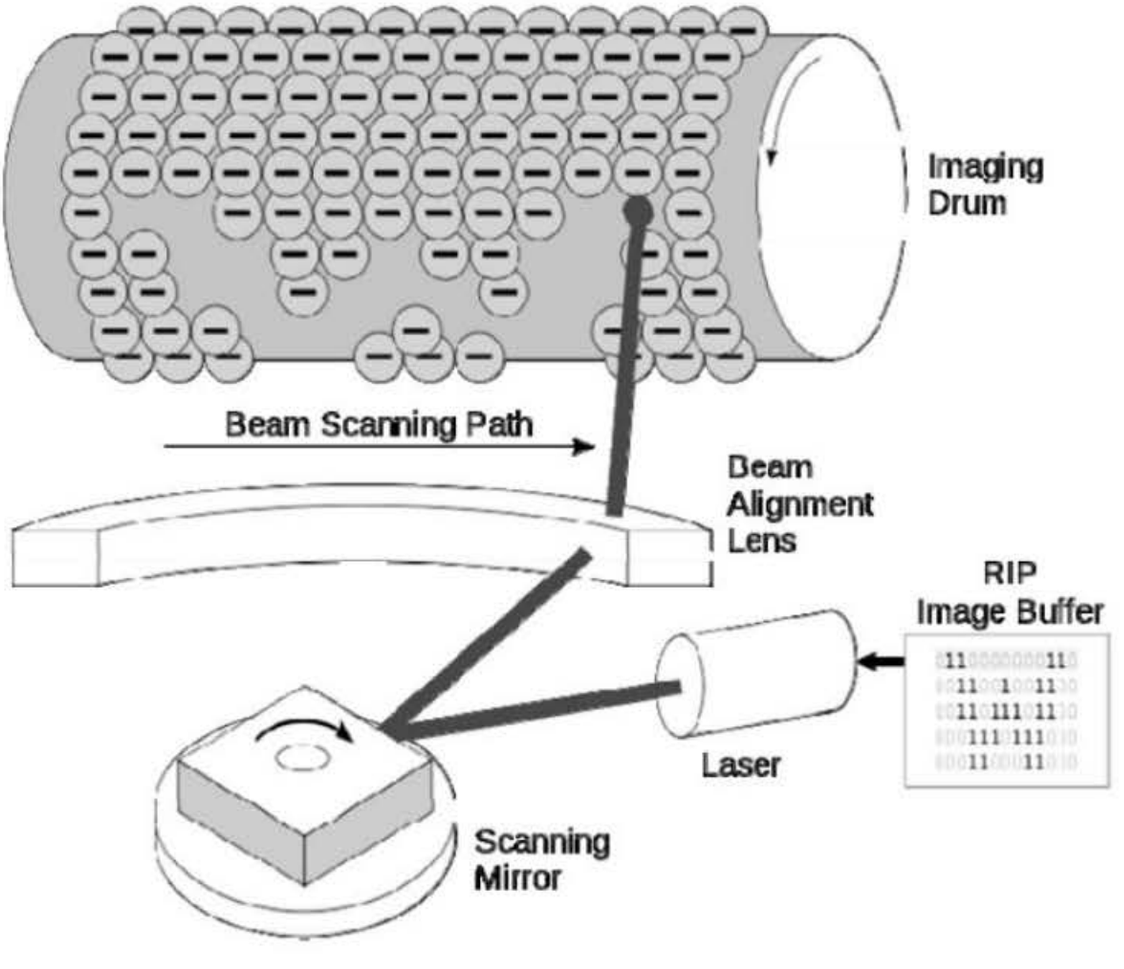
Banyak ragam printer yang dapat dijumpai, misalnya:

- Thermal printer.
- Laser printer.
- Inkjet printer.
- Impact printer.

Bentuk koneksi yang digunakan pun variatif, misalnya:

- Serial.
- Paralel.
- Universal Serial Bus (USB), firewire.
- Accessed via infrared port

Beberapa printer memiliki media penyimpanan tersendiri (memory buffer), terutama printer laser, ini memungkinkan printer menerima banyak dokumen walaupun dalam proses mencetak, inilah harus di-alamati dengan baik, ada informasi yang tersimpan pada memori printer, bahkan efektif digunakan sebagai evidence.



Gambar 2.29 Membangun image digital pada drum sebagai proses dalam membentuk image tercetak [Sumber: Dale Mahalko.Wikipedia. GNU Free Documentation License]

Bukti potensial:

- Dokumen.
- Hard drive.
- Ink cartridge.
- Network identity/information.
- Superimposed images pada roller (menyimpan image digital yang dibangkitkan secara elektrik).
- Waktu dan tanggal.
- Log penggunaan.

Removable Storage Devices and Media

Perangkat ini digunakan untuk menyimpan informasi dengan metode yang beragam mencakup: secara elektris, magnetik, atau melakukan 'burning' elemen plat kristal, ragam perangkat tersebut antara lain:

- Floppy disk.
- CD.
- DVD.
- Cartridge.
- Tape.

Komponen ini difungsikan sebagai media penyimpanan, file yang disimpan pada umumnya mencakup program komputer yang didistribusikan untuk keperluan komersial, dokumen teks, gambar, video/audio, berbagai multimedia files, dan lain sebagainya.

Bukti potensial: Media penyimpanan berikut juga file yang tersimpan didalamnya.

Scanner

Perangkat yang mampu mendigitalisasi dokumen fisik melalui proses scanning, sehingga dikenali komputer dalam bentuk file digital. File digital nantinya dapat berupa file gambar ataupun teks.

Scanner dapat menjadi bukti untuk menggali lebih dalam tindakan-tindakan kriminal semisal pornografi anak, check fraud, pencurian identitas (identity thef), counterfeiting, dan lain sebaginya. Bahkan kaca yang ada pada scanner mungkin saja didapati sidik jari yang tercecer.

Bukti potensial:

- Perangkat yang bersangkutan.

Telepon

Perangkat ini digunakan sebagai media komunikasi dua arah, berbagai media mungkin digunakan, antara lain:

- Kabel telepon.
- Transmisi radio.
- Cellular system.
- Kombinasi lainnya.

Kemampuan menyimpan informasi harus dialamati baik untuk keperluan evidence.

Bukti Potensial:

- Appointment calendars/information.
- Caller identification information.
- Electronic serial number.
- E-mail.

- Memo.
- Password.
- Buku telepon.
- Text messages.
- Voice mail.
- Web browsers.

Perangkat Elektronik Lainnya

Ada banyak perangkat elektronik lainnya yang dapat ditambahkan ke dalam daftar keperluan investigasi, bahkan banyak perangkat elektronik baru yang dapat digunakan sebagai sumber informasi yang sangat berharga, misalnya credit card skimmers, cell phone cloning equipment, caller ID boxes, audio recorders, web TV, fax machines, copiers, dan multifunction machines dengan banyak fitur yang terintegrasi di dalamnya, kemampuannya dalam menyimpan informasi menjadi bukti lebih lanjut yang sangat berharga.

Mesin Fotokopi (Copiers)

Mesin fotokopi mungkin menyimpan catatan penggunaan, bahkan beberapa dokumen mungkin masih disimpan dalam memori dan memungkinkan untuk dicetak kemudian, misalnya untuk jenis scan once/print.

Bukti Potensial:

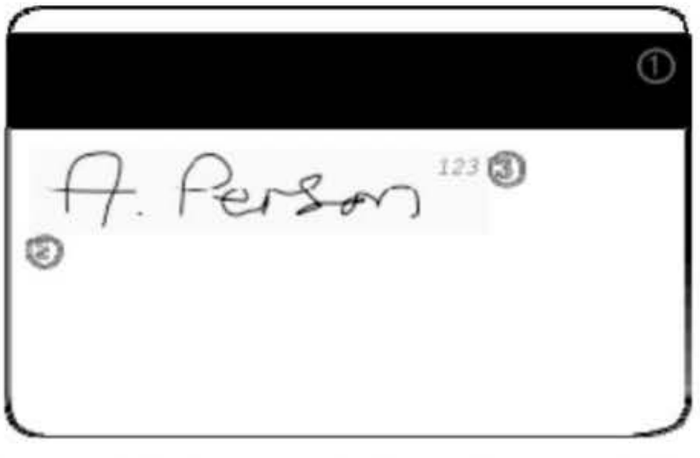
- Dokumen.
- Catatan penggunaan (user usage log).
- Catatan pelengkap berkenaan tanggal dan waktu.

Credit Card Skimmers

Credit card skimmers digunakan untuk membaca informasi yang ada pada magnetic stripe pada kartu plastik. Informasi untuk keperluan forensik didapat dengan melakukan pembacaan pada magnetic stripe.

Bukti Potensial:

- Tanggal kadaluarsa (masa berlaku).
- Alamat pemilik.
- Nomor kartu kredit.
- Nama pemilik.



Gambar 2.30 Penampang belakang dari kartu kredit (1) magnetic stripe (2) signature strip (3) CVC2 code

Jam Tangan Digital (Digital Watches)

Fitur digital watches tidak sesederhana namanya, kemampuan meng-organize address books, jadwal aktivitas, dan berbagai catatan yang bahkan dapat dikonversi, kemudian diakses via komputer.

Bukti Potensial:

- Buku alamat.
- Notes (buku catatan).

- Appointment calendars (agenda).
- Nomor telepon.
- E-mail.

Mesin Fax (Faximile Machines)

Mesin Fax memiliki fitur untuk menyimpan nomor telepon, catatan pengiriman dan penerimaan dokumen, bahkan memungkinkan untuk menyimpan banyak dokumen untuk dikirim kemudian, bukan hanya itu dokumen yang pernah dikirim dan diterima terdokumentasi dengan baik pada mesin fax.

Bukti potensial:

- Dokumen.
- Nomor telepon.
- Film cartridge.
- Log/catatan pengiriman dan penerimaan.

Global Positioning Systems (GPS)

Ada banyak informasi yang dapat dikumpulkan dari Global Positioning Systems, salah satunya adalah rute perjalanan.

Bukti potensial yang dimungkinkan antara lain:

- Rumah/tempat.
- Target selanjutnya (next destination).
- Catatan perjalanan.
- Jalur koordinat (way point coordinates).
- Jalur yang ditunjuk (way point name).

Gambar 2.31 Taksi yang dilengkapi dengan perangkat GPS (Sumber: Wiki.Paul Vlaar. GNU Free Documentation License)

2.4 Fakta Digital Terselubung

Fakta sifatnya tersembunyi dan dibutuhkan keahlian sang investigator untuk mengalamati di mana letak sumber-sumber potensial fakta yang dapat diajukan sebagai 'barang bukti'.

Banyak area 'tidak kasat mata' dalam penggunaan sistem komputer, justru di sinilah banyak celah yang sering dilewatkan user (sebagai tersangka) dalam memperlakukan komputer sedemikian rupa untuk menghilangkan jejak-jejak kejahatan yang ternyata tidak tersapu bersih seperti yang dilihat user pada layar komputernya.

Berikut beberapa pengetahuan penting yang harus dipahami oleh investigator untuk menangkap faktor tidak kasat mata dari teknologi komputer, berikut sistem yang terintegrasi di dalamnya:

- Anda sebenarnya tidak mutlak menghapus file, file yang terhapus masih tersimpan dalam recycle bin dengan aman, dan file yang dibuang dari recycle bin ternyata masih melekat pada hard disk dan masih sangat mudah untuk mendapatkannya kembali!
- Banyak jejak ditinggalkan dari program aplikasi.

- Data Volatile, meskipun tidak tersimpan pada hard disk secara permanen seperti Non-Volatile, ternyata daya lekatnya pada media penyimpanan semisal memori dapat melekat cukup lama bahkan setelah proses reboot.
- Data memang sangat sulit untuk dimusnahkan, maka dari itu pihak perbankan biasanya akan memusnahkan pula media penyimpanan meskipun sudah dilakukan penghapusan data. File yang dihapus dapat dengan mudah di-recover.
- File yang ditransmisikan melalui jaringan ternyata dengan mudah di-reassembled dan digunakan sebagai evidence.
- Formatting saja tidak cukup untuk menghapus data, masih banyak jejak lain yang ditinggalkan.
- Install aplikasi sangatlah mudah, tetapi tidak demikian untuk uninstall aplikasi, banyak jejak-jejak yang ditinggalkan, dengan demikian Anda tidak benar-benar membesihkan aplikasi dengan sekedar meng-uninstall.
- Menggunakan encryption tidaklah cukup, data dapat didapatkan kembali melalui decryption.
- Menggunakan magnet ternyata tidak membuang dan merusak data pada storage device.
- Me-rename file untuk mencegah deteksi ternyata tidak berarti.
- Mutilasi media penyimpanan tidak efektif, perlu melakukan mutilasi secara ekstrim.
- Software Anti-forensics belum maksimal, banyak software forensik dapat digunakan untuk merecovery data yang sudah dihapus.
- Web-based email ternyata dapat di-recover pada komputer asal.

BAB 3
METODA KOMPUTER FORENSIK

3.1 Komponen Utama Forensik

Model forensik melibatkan tiga komponen guna mencapai kelayakan dan hasil penyidikan yang berkualitas. Ketiga komponen tersebut adalah:

- Manusia (people).
- Peralatan (equipment).
- Aturan (protocol).

Manusia (people) sebagai penyidik harus memiliki kualifikasi. Mudah untuk sekedar belajar komputer forensik, tetapi untuk menjadi ahli ternyata dibutuhkan lebih dari sekedar pengetahuan, 'jam terbang' lah yang membuatnya dikatakan 'ahli'.

Hasil akhir dengan kualitas harus dibangun dengan keahlian, pengetahuan dan pengalaman. Pencapaian kualitas demikian bukan hanya semata-mata dalam menyajikan *evidence* untuk keperluan pengadilan dan investigasi kejahatan saja, tetapi melibatkan sisi hukum dan level-level tidak kasat mata semisal etika dan moral.

Apakah langkah - langkah yang diambil untuk menggali dan menemukan *evidence* dilakukan tanpa melanggar batasan hukum atau etika? Di sinilah kualitas diuji!

Ahli komputer forensik dapat dispesifikasi ke dalam beberapa ruang lingkup kerja. Meskipun demikian, ahli forensik sering disebut sebagai *investigator* saja bahkan ada yang menyebutnya sebagai *examiner*.

Berikut peran-peran terspesifikasi para i*nvestigator/examiner*, yaitu:

- **Computer Forensic Examiner**, memiliki kemampuan dan karakteristik sebagai berikut:
    - Pengujian perihal originalitas media.
    - Mengekstrak data untuk di-review.
    - Dibutuhkan empat sampai enam minggu pelatihan untuk mendapatan pengetahuan examiner.
- **Computer Investigator**, memiliki kemampuan dan karakteristik sebagai berikut:
    - Harus memiliki pengalaman yang teruji dan ahli.
    - Memahami jaringan komputer, internet, berbagai media komunikasi yang melibatkan teknologi komputer/ informasi.
    - Dibutuhkan satu sampai dua minggu pelatihan untuk mendapatan pengetahuan sebagai investigator.
- **Digital Evidence Collection Specialist**, memiliki kemampuan dan karakteristik sebagai berikut:
    - Spesifikasi pekerjaannya yakni mengumpulkan fakta digital, Digital Evidence Collection Specialist dapat dikatakan sebagai *First Responder*.

- Mendapatkan dan menghadirkan bukti komputer mencakup pula media penyimpanannya jika memang ada.
- Dibutuhkan dua sampai tiga hari pelatihan untuk mendapatan pengetahuan.

Jika diperhatikan, setiap spesifikasi keahlian memiliki standar, kecakapan, beban kerja, dan dan beban pelatihan yang yang berbeda-beda.

Peralatan yang digunakan pun harus melalui mekanisme dan prosedur tersendiri untuk mendapatkan bukti-bukti (evidence) yang berkulitas dan tidak kotor. Ada banyak peralatan yang dibutuhkan untuk melibatkan perangkat lunak spesifik, berbagai perangkat keras, dan berbagai media penyimpanan dalam menangai data-data/evidence.

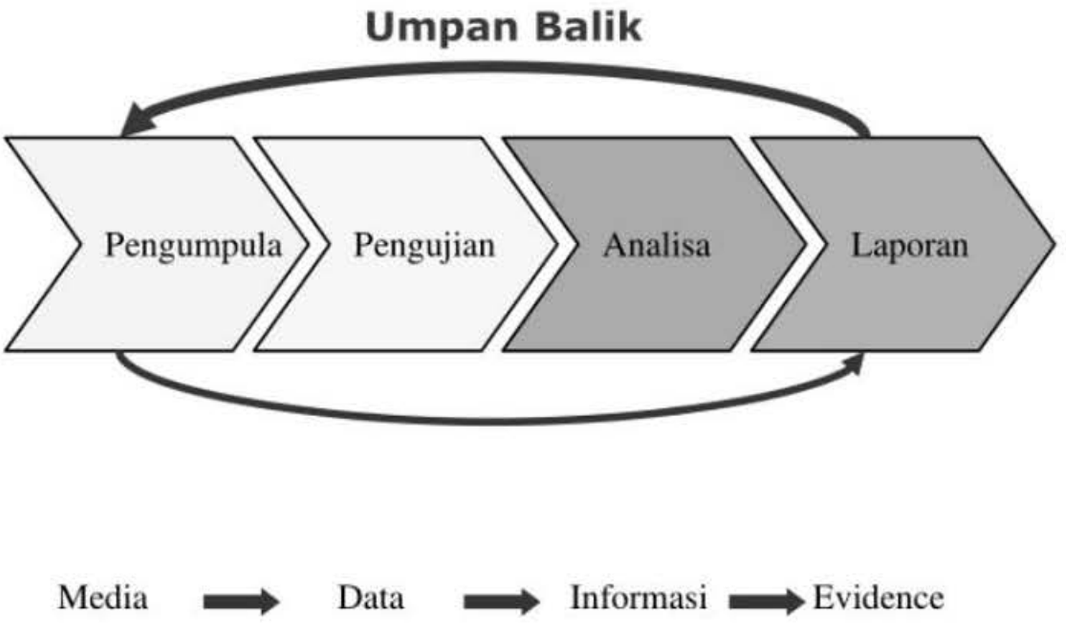
Di antara tiga komponen komputer forensik, aturan (protocol) memegang peranan paling penting. Protokol ditetapkan sebagai aturan dalam menggali, mendapatkan, menganalisa, dan menyajikan dalam laporan-laporan. Di sini, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam tindakannya diadakan peran-peran konsultasi yang mencakup pengetahuan akan teknologi informasi dan ilmu-ilmu hukum.

Pemampu komputer forensik yakni: Manusia (People), Peralatan (Equipment), dan Aturan (Protocol) akan melebur dan berkolaborasi untuk mengisi setiap fase-fase dalam proses komputer forensik.

Ada empat fase dalam komputer forensik, antara lain:

- Pengumpulan.
- Pengujian.
- Analisa.
- Laporan.

Ada objek yang dikelola dari proses setiap fase, dimuai dari media dan kemudian didapati evidence di akhir proses. Umpan balik diberlakukan untuk menganalisa kembali hasil yang didapat berdasarkan tujuan semula, hal ini dilakukan oleh examiner dengan me-review kembali proses forensik. Gambar 3.1.



Gambar 3.1 Tahap-tahap komputer forensik

3.2 Pengumpulan Data

Pengumpulan data adalah langkah pertama dalam proses forensik untuk mengidentifikasi sumber-sumber potensial dan menjelaskan langkah pengumpulan data.

Pengumpulan ini melibakan proses dan metode yang semakin kompleks dikarenakan perkembangan teknologi. Ada banyak komputer, ada banyak ragam media penyimpanan dan ada banyak jaringan komputer dengan segala teknologi dan kerumitan ini memerlukan penanganan yang berbeda-beda.

Data yang marak didapatkan umumnya berada pada personal komputer/ desktop Komputer, hal ini dijelaskan berdasarkan tren bahwa setiap orang ingin memiliki sendiri komputer satu untuk dirinya, demikian pula di perkantoran, setiap pegawai memiliki satu komputer untuk mengerjakan tugas-tugasnya.

Bukan hanya komputer desktop saja yang menjadi sumber data, server dan mencakup pula media penyimpanan yang dialokasikan pada jaringan komputer (file server, file sharing, dan lainnya) menjadi sumber daya, dan salah satu personal komputer portable dan bahkan fitur mobilitas tinggi dengan perangkat integrasi ke jaringan membuat laptop banyak diminati dan ada banyak sumber data bisa didapatkan.

Perangkat-perangkat demikian memiliki fitur penyimpanan, bahkan trennya perangkat demikian diberikan kapasitas penyimpanan yang cukup besar, bahkan penyimpanan-penyimpanan yang portable hadir dengan bentuk yang ringkas dengan biaya yang semakin murah.

Selain melibatkan drive untuk mengakses media beberapa perangkat mungkin mengintegrasikan media penyimpanan dengan drive (alat pengaksesannya), berikut misalnya perangkat yang dimaksud:

- CD ROM drive.
- DVD ROM drive
- USB (Universal Serial Bus) port.
- Firewire.
- PCMCIA (Personal Computer Memory Card International Association).

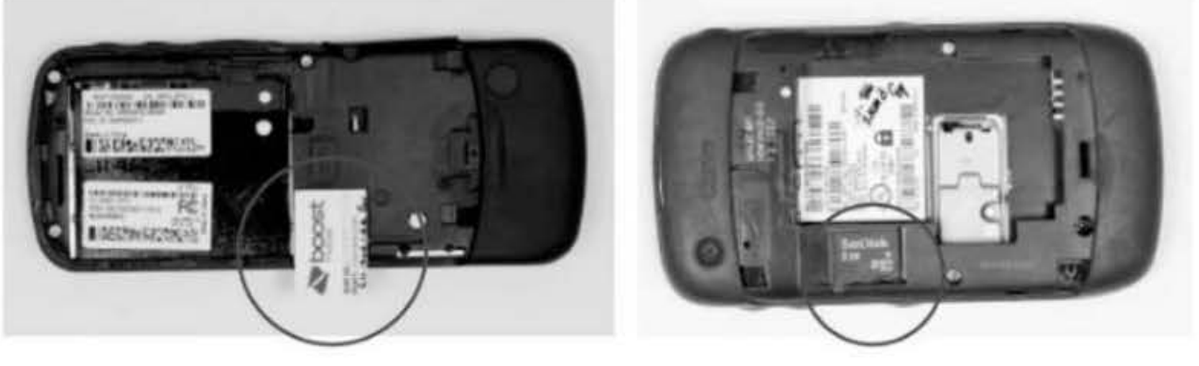
Dan ada banyak media penyimpanan eksternal lainnya, seperti:

- ThumbDrives.

- Memory Card.
- USB Flash Disk.
- Optical Disc.
- Magnetic Disk.

Tidak hanya komputer desktop, media yang memiliki penyimpanan data dapat ditemukan pula pada:

- PDA.
- Telepon selular.
- Kamera digital.
- Digital recorder.
- Audio player (iPOD, MP3 Player, dan lainnya)



Gambar 3.2 Penting untuk mengetahui jika perangkat tersimpan di SIM atau Micro SD. Keterangan: SIM Card dialokasikan secara internal (kiri) Micro SD dialokasikan secara eksternal (kanan) Sumber: Virginia Dept. Forensic Science

Perangkat penyimpanan dan data-data tadi mungkin dengan mudahnya kita dapat berkenaan organisasi yang dimaksud, tetapi akan ada banyak organisasi lain yang mungkin dapat diminta keterangan sehubungan dengan data dan informasi yang mungkin terelasi, misalnya saja jika melibatkan jaringan internet, mungkin dibutuhan log aktifitas jaring dari ISP (Internet Service Provider), untuk mendapatkan informasi/data

sedemikian diperlukan serangkaian prosedur, misalnya saja mungkin dibutuhkan surat keterangan resmi secara hukum untuk mendapatkan catatan/log demikian.

Tindakan pengumpulan data mungkin melibatkan perkara lain yang sulit teralamati, mencakup pula etika di dalamnya. Misalnya saja, akan sangat berguna untuk memonitoring pengguna komputer dalam beraktivitas tetapi privasi bisa dilanggar dan menimbulakan masalah lain lagi pada akhirnya.

Pengumpulan data ini mencakup aktivitas seperti:

- Identifikasi.
- Penamaan (Labeling).
- Perekaman (Recording).
- Mendapatkan data.

Data yang didapatkan harus dapat diandalkan dan relevan terhadap kasusnya. Data menjadi barang berharga yang rapuh, maka dari itu diberlakukan serangkaian prosedur untuk menjaga integritas data.

Lain peralatan maka lain penanganannya, misalnya PDA, telepon selular, laptop dan perangkat yang memiliki kapasitas power yang terbatas (baterai lithium), data yang berjalan akan sangat rapuh dan dibutuhkan penanganan segera.

Setelah melalui proses identifikasi sumber data, langkah selanjutnya tentu mendapatkan data tersebut. Ada tiga langkah yang dibutuhkan:

- Membuat perencanaan untuk mendapatkan data. (*Develop a plan to acquire data*).
    - Kemiripan nilai (Likely Value).
    - Karakteristik data (Volatility).

    - Upaya yang dibutuhkan untuk mendapatkan data (*Amount of Effort Required*).

- Mendapatkan data (*Acquire the data*).
- Analisa integritas data (*Verify the integrity of the data*).

Berikut dijabarkan penjelasan masing-masing prosesnya sebagai berikut:

Membuat perencanaan untuk mendapatkan data.

Membuat perencanaan dalam mendapatkan data adalah langkah paling penting, ada banyak sumber data yang potensial, di samping itu dalam mendapatkan data dibutuhkan analisa terhadap data yang layak diprioritaskan, mungkin membuat daftar berdasarkan tingkat prioritas.

Dalam menentukan prioritas, ada tiga faktor yang banyak ditawarkan untuk menjadi pertimbangan, antara lain:

- Kemiripan nilai (*likely value*). Tentu Examiner membutuhkan pemahaman akan situasi dan kondisi, mungkin berdasarkan pengalaman sebelumnya, perkiraan yang relevan diperlukan untuk menentukan justifikasi nilai suatu informasi.
- *Data Volatile.* Data kategori ini akan hilang begitu saja sewaktu listrik dimatikan, data-data yang di memori ada karena 'sistem berjalan' (runtime), dan akan hilang dengan mudahnya jika listrik mati. Karena alasan ini, data yang tergolong volatile mendapatkan prioritas dibandingkan data-data non volatile. Tetapi prioritas demikian tidaklah mutlak, banyak kasus yang ternyata data non volatile harus mendapatkan prioritas. Salah satu penyimpangan dalam bentuk lain, misalnya saja data yang non volatile pun dapat demikian 'liquid', seperti data log trans-aksi yang demikian dinamis berubah seiring sistem yang berjalan.

- Upaya dalam mendapatkan data (*Ammout of Effort Reqired a cquiring data*).

  Proses mendapatkan data tidak sekejap dapat dilakukan, belum tentu jika dipertimbangkan melalui kacamata hukum. Misalnya saja, akan lebih mudah mendapatkan data yang disumberkan pada network router daripada mendapatkannya dari ISP (Internet Service Provider).

  Telah kita lihat beberapa prioritas yang menjadi acuan dan cara menangani dalam mendapatkan data, meskipun demikian tidak semua sumber-sumber data potensial dapat dimanfaatkan.

  Diperlukan lebih dari sekedar menemukan sumber data dan mengambi kompleksitas priorits yang muncul, berbagai metode dokumentasi, penuntun praktis, dan prosedur dalam mencapai efektivitas dalam langkah ini.

Mendapatkan Data (Acquire the data)

Tidak selalu dibutuhkan upaya besar menggunakan serangkaian proses pemindaian data, seandainya data yang diperlukan memang sudah didapatkan dengan *security tools, analysis tools*, atau cara lain.

Pada banyak kasus, mungkin dibutuhkan tool spesifik forensik untuk mendapatkannya, mencakup mengumpulkan data-data yang tergolong volatile, mengambilnya dengan menduplikasi data sumber non volatile, mungkin mencakup mengamankan sumber data original non volatile .

Data yang diambil mungkin didapat via komputer lokal atau meng-aksesnya melalui jaringan komputer. Akan lebih baik jika data diambil pada komputer komputer lokal dikarenakan kontrol maksimum terhadap data, tetapi data lokal tidak sepenuhnya *feasible*, misalnya saja sistem komputer yang dialokasikan di tempat yang sulit untuk dijangkau/ dilokasi yang terpisah secara geografis.

Dikarenakan data dialokasikan di tempat yang terpisah, beberapa pertimbangan akan mucul, misalnya seberapa banyak data yang diperlukan, data-data apa saja yang perlu dikumpulkan. Pertimbangan demikian dibuat karena faktor sumber daya jaringan dengan berbagai kelebihan dan juga keterbatasannya terakit jangkauan.

Pertimbangan lain, apakah perlu mengambil data pada sistem yang berbeda atau cukup sistem tertentu saja. Kelayakan, kompleksitas, dan upaya yang dikerahkan akan mendasari pilihan yang akan diambil kemudian.

Analisa Integritas Data (Verify the integrity of the data)

Setelah data didapatkan, verifikasi penting untuk memeriksa integritas data, terlebih lagi jika nantinya diteruskan untuk keperluan hukum.

Verifikasi integritas data mencakup pengunaan tool dalam mengkalkulasi infomasi original dan kemudian mengkopinya, selanjutnya dilakukan analisa untuk membandingkan apakah data hasil pemindaian dan data original dapat dikatakan sama/identik.

3.3 Pengujian

Setelah melalui proses pengumpulan, langkah lebih lanjut yaitu dengan melakukan pengujian, mencakup di dalamnya menilai dan mengekstrak kepingan informasi yang relevan dari data-data yang dikumpulkan.

Tahap ini melibatkan *bypassing* atau miminimalisasi fitur-fitur sistem operasi dan sistem aplikasi yang akan mengaburkan data, seperti kompresi, enkripsi, dan akses mekanisme kontrol.

Hard drive berisi ribuan bahkan jutaan file, untuk mengidentifikasi data di dalamnya akan sangat menyita perhatian serta melelahkan. Filtrasi akan mengeliminir sebagian data yang tidak dibutuhkan, misalnya data log minggu lalu yang terdiri dari jutaan record dan didapati hanya ratusan record saja yang dinilai penting untuk pemeriksaan lebih lanjut.

Ada banyak peralatan dan teknik digunakan dalam melakukan eliminasi terhadap tumpukan data. Percarian data berbasis teks dan berbagai pola tertentu dapat digunakan untuk mengidentifikasi ketepatan suatu data, seperti pencarian terhadap dokumen yang berhubungan dengan seseorang atau pokok permasalahan tertentu, atau mengidentifikasi transaksi pada *e-mail log entries* untuk mendapatkan alamat e-mail tertentu.

Ada banyak tool lainnya yang digunakan dalam pengujian ini, semisal software yang mampu menentukan secara akurat jenis file yang berisi karakteristik data tertentu, mungkin berupa file teks, grafik, audio atau berbagai file kompresi lainnya.

Pengetahuan yang menyeluruh akan jenis dan tipe file dapat dijadikan acuan dalam menyingkirkan file yang tidak memiliki kelayakan/nilai lebih. Akan dijelaskan kemudian berkenaan proses ini lebih lanjut, secara mendasar, tahap ini mencakup mengalokasi file, mengekstrak file (mungkin melalui enskipsi, stenografi, dekompresi), pemeriksanan terhadap meta data, dan lain sebagainya.

3.4 Analisa

Setelah melalui tahap ekstraski informasi, Examiner akan melakukan analisa untuk merumuskan kesimpulan dalam menggambarkan data. Analisa yang dimaksud adalah mengambil pendekatan metodis dalam menghasilkan kesimpulan yang berkulitas berdasarkan pada ketersediaan data atau bahkan sebaliknya, dengan menyimpulkan bahwa tidak ada kesimpulan/ hasil yang didapat, maka hal itu mungkin bisa saja terjadi.

Tugas Examiner mencakup kegiatan seperti:

- Mengidentifikasi user atau orang di luar dari pengguna tetapi tidak terlibat secara langsung.
- Lokasi (melakukan observasi lokasi kejadian).

- Barang-barang (menentukan barang-barang yang berhubungan dengan kejadian).
- Kejadiaan (menelusuri rangkaian kejadian).
- Menentukan atau mempertimbangkan bagaimana komponen-komponen terelasi satu dengan yang lain, sehingga didapati kesimpulan akhir.

Misalnya saja, *network Intrusion Detection System (IDS) log* mungkin memiliki link ke banyak host, *the host audit logs* mungkin berisi banyak link dari aktivitas user dengan account pengguna, dan *thost IDS log* menjadi historis dari aktifitas dan aksi yang dilakukan oleh user.

Tool yang terintegrasi dengan sistem operasi ataupun tool spesifik lainnya seperti *centralized logging* dan *security event management software* mampu mengumpulkan data-data demikian.

Proses analisa akan dijelaskan dan dicontohkan lebih lanjut pada bab berikutnya.

3.5 Dokumentasi dan Laporan

Reporting adalah tahap akhir dari proses komputer forensik, dalam tahap ini kita akan merepresentasikan informasi yang merupakan hasil dari proses analisis.

Banyak faktor yang memengaruhi reporting, seperti di bawah ini:

- **Alternative Explanations (Penjelasan Alternatif)**

  Jika informasi yang mengacu pada suatu kasus dikategorikan tidak lengkap (incomplete), maka definisi akhir didapati tidak memadai dan tidak dapat diandalkan untuk mengalamati kejadian.

Bahkan jika didapati beberapa penjelasan lain yang masuk akal akan suatu kejadian, masing-masing informasi yang didapat harus dipertimbangakan dan diteruskan dalam proses reporting.

Apa pun yang terjadi, seorang examiner harus menggunakan pendekatan metodikal dalam menentukan untuk menyetujui atau menolak setiap penjelasan perihal duduk perkara yang mungkin untuk diteruskan/diajukan.

- **Audience Consideration. (Pertimbangan Audiensi/Pengamat)**

  Menyajikan data atau informasi pada audiensi sangatlah penting. Kasus yang melibatkan perundangan membutuhkan laporan detail/spesifik berkenaan informasi yang dikumpulkan, dan duplikasi setiap fakta (*evidentiary data*) yang diperoleh.

  Pertimbangan ini beralasan, misanya saja Administrator Sistem mungkin ingin melihat lebih jauh *network traffic* secara detail.

- **Actionable Information.**

  Proses Reporting mencakup pula mengidentifikasi actionable information yang didapat dari data-data terdahulu, darinya kita bisa mendapatkan informasi baru.

  Misalnya saja, daftar alamat seseorang (*contact list*) dapat dikembangkan lebih lanjut yang kemudian mengarah pada informsi lain mengenai suatu tindak kriminal/kejadian.

  Keuntungan lain dari *actionable information*, informasi yang didapatkan mungkin dapat digunakan untuk keperluan mendatang, misalnya tujuan pengamanan seperti *backdoor* yang mungkin bisa dieksploitasi, maka dibutuhkan penanganan segera.

Dalam prosesnya, mungkin didapati masalah yang harus diperbaiki sesegera mungkin seperti *policy shortcomings* atau *procedural errors.* Formal reviews dapat membantu dalam mengidentifikasi dan meningkatkan kualitas.

Sewaktu ada perubahan sedikit saja berkenaan guidelines atau prosedur semua anggota tim harus diinformasikan dan pengingat rutin mungkin diperlukan.

Tim Forensik mungkin memiliki metoda dan berbagai aktivitas formal lainnya untuk melakukan identifikasi dan menjejaki perubahan yang terjadi, perubahan ini menjadi suatu pola dan harus diawasi dengan seksama. Proses monitoring harusnya mudah akses, misalnya dengan menempelkan gambar, poster ataupun dokumen lainnya pada dinding atau apa pun yang dapat difungsikan, dengan demikian setiap tim dapat diingatkan dan melakukan monitoring dengan mudah.

Dari semua keahlian yang dimiliki, teknologi informasi cenderung liquid, perubahan dapat terjadi dengan cepat, demikian pula metode yang menyertai forensik, diperlukan pembelajaran dalam mengalamati setiap perubahan dengan cepat,.

Maka dari itu, untuk mememenuhi kualifikasi dengan tantangan perubahan demikian, maka dibutuhkan standar untuk membuktikan kelayakan seseorang sewaktu harus berkolaborasi dan bekerja dengan tim, dan skill masing-masing anggotanya perlu ditinjau ulang dalam rentang waktu satu tahun. Ini memastikan bahwa anggota tim memiliki skill yang terkini seiring perubahan teknologi dan hukum yang melingkupinya.

3.6 Tips Pemberlakuan Forensik

Hasil Forensik menjadi dapat diandalkan tergantung pada pedoman yang mengisi setiap langkah dan pelaksana, berikut beberapa tips yang dapat dipandang sebagai pedoman dalam melakukan proses forensik:

1. Konsistensi dalam setiap proses forensik.
2. Tahapan forensik yang mencakup pengumpulan(collection), pengujian (examination), analisa, dan laporan-laporan, perlu dipahami bahwa setiap tahap mungkin tidak memerlukan upaya atau kerja keras yang sama, kebutuhan akan detail pun bervariasi.
3. Analisa harus memerhatikan berbagai sumber data potensial, mencakup informasi non fisik (alokasi data) dan fisik (misalnya media penyimpana secara fisik).
4. Examiner harus jeli dalam mengalokasi sebaran data-data yang mungkin dibutuhkan, apakah hanya sebatas komputer desktop atau mencakup pula jaringan komputer yang bahkan merambah keluar organisasi.
5. Examiner harus mempertimbangkan setiap alternatif yang dapat diandalkan (reliable), seandainya didapati faktor rintangan secara fisik, konseptual, bahkan regulasi untuk men-dapatkan data.
6. Dibutuhkan tindakan proaktif dalam mengumpulkan data-data yang berharga. Tindakan proaktif membutuhkan effort yang besar, antara lain seperti: Melakukan audit terhadap sistem operasi, menerapkan logging, menjalankan sistem backup, dan security monitoring control yang suatu saat dapat digunakan untuk keperluan forensik.
7. Examiner harus menghadirkan data melalui standar yang sudah didefinisikan. Penyimpangan dan mengabaikan standar akan

membuat data menjadi tidak lagi berharga, bahkan bisa saja menimbulkan kasus baru yaitu pelanggaran hukum.

8. Pertimbangkan setiap tahapan, mulai dari mengidentifikasi sumber data, membuat perencanaan dalam mendapatkan data, dan menganalisa integritas dari data.

9. Buat prioritas untuk langkah kerja, misalnya: menentukan data yang perlu diberikan prioritas/penanganan segera, mencakup perkembangan karakteristik dari data, misalnya: likely value, data volatile atau non volatile, data dinamis atau non dinamis, dan mencakup pula upaya yang harus dikerahkan dalam mendapatkan data. Hal ini penting untuk mendapatkan kelengkapan dan kelayakan informasi, terutama bagi informasi yang sangat bergantung dengan waktu.

10. Sebelum data mulai dikumpulkan, keputusan harus dibuat yang mencakup kebutuhan dalam mengumpulkan data dan menangani evidence dengan serangkaian cara tertentu, pertimbangkan keutuhan dalam segi hukum yang mungkin suatu saat diperlukan atau untuk kebutuhan lainnya.

11. Pendefinisian yang jelas berkenaan prosesi penyerahan barang bukti (chain of custody), tentunya ditujukan untuk menghindari kesalahan penanganan barang bukti (mishandling evidence).

12. Examiner harus menggunakan pendekatan ilmiah dalam mempelajari data. Pendekatan demikian harus mengisi proses analisa kelayakan data dan keabsahannya, darinya Examiner membuat kesimpulan berdasarkan ketersediaan data atau mungkin saja tidak ada hasil sama sekali.

13. Jika evidence dibutuhkan untuk keperluan hukum/persidangan atau keperluan yang sifatnya internal disipliner, tentu detail dan

langkah-langkah mendapatkan harus didokumentasikan dengan terinci.

14. Examiner harus me-review kembali proses yang sudah dilaksanakan. Banyak keuntungan positif yang didapat dari tindakan ini yang membuat hasil forensik dapat dipertanggungjawabkan, misalnya:
    - Mengidentifikasi seandainya ada kebijakan yang dilanggar (policy shortcomings).
    - Mengalamati kesalahan prosedur (procedural errors).
    - Lain-lain masalah minor yang mungkin harus diperbaiki.
    - Mempertimbangkan kembali seberapa organisasi mengikuti arus dari teknologi dan perubahan di segi hukum.

Lebih lanjut dapat Anda perhatikan beberapa tips umum dalam menangani dan menganalisa evidence secara umum untuk menjaga keutuhan/integritas serta kelayakan data, berikut digariskan sebagai berikut:

- Jangan terlebih dulu menyalakan PC untuk alasan apa pun.
- Hubungi agen yang bersangkutan untuk melakukan analisa secepatnya, keuntungan berimbang didapatkan dengan mempertimbangkan sisi efisiensi, waktu yang terbatas, dan kebutuhan investigasi.
- Lekatkan/tandai evidence tape, melingkupi power supply dan disk drives.
- Memiliki surat perintah atau izin sangatlah penting dan ditujukan untuk memberikan kuasa untuk melakukan analisa terhadap komputer dan data di dalamnya.

- Laporan petugas/polisi, pernyataan tertulis yang sah ataupun ringkasan kasus menjadi kebutuhan yang melegalkan untuk examiner.
- Buat daftar kata-kata yang dibutuhkan dalam melakukan pencarian, ada baiknya disimpan dalam media ringkas semisal floppy disk dengan ukuran file yang kecil (misalnya: *.txt). Gunakan kata-kata yang unik bukan umum (misalnya jangan gunakan kata-kata: money, drugs, sex, mail, message, dan lainnya).
- Tidak ada istilah tepat waktu dalam komputer forensik, dibutuhkan upaya dan waktu yang tidak terbatas sewaktu Anda menelusuri 'hutan data' untuk mendapatkan bukti.
- Konsisten terhadap kasus dan identifikasi kepentingan/keperluan. Misalnya saja, jika menyangkut transaksi obat terlarang dan narkoba, tentu tidak menanyakan informasi untuk keperluan pengujian dalam mencari kasus pornografi anak.
- Jika ada beberapa orang yang mungkin menggunakan komputer atau dialokasikan di ruang komputer, indikasi terhadapnya perlu dilakukan, mencakup siapa kapan dan atribut lain yang berkaitan dengan kompuer, semisal password.
- Mengindikasi apakah komputer diintegrasikan (atau pernah diintegrasikan) ke jaringan komputer atau tidak.
- Dapatkan informasi sebanyak dan selengkap mungkin mencakup beberapa hal lainnya, seperti:
    - Jenis komputer dan jumlah komputer, termasuk pula sistem operasi yang digunakan.
    - Jenis software jaringan komputer, karakteristik jaringan dan lokasi server.

- Aktivitas jaringan yang berlangsung dan jenis koneksi, berikut sumbernya.

- Mengindikasi, apakah didapati encryption atau password protection.
- Mengidentifikasi skill komputer pengguna yang menggunakan komputer atau perangkat yang dijadikan taget forensik
- Tidak selamanya monitor dan peripheral ataupun perangkat lain harus disertakan, umumnya komputer dan media penyimpanan sudah cukup untuk diambil guna keperluan forensik.

3.7 Tips Bagi Pemula yang Sadar Forensik

Bagi pemula yang mungkin baru dengan istilah forensik dan ternyata mendapati adanya kasus-kasus yang membutuhkan penanganan forensik, beberapa yang layak diperhatikan:

1. Investigasi sederhana dapat dilakukan untuk mengalamati evidence.
2. Hubungi organisasi/pihak-pihak yang berwenang dalam meng-ambil keputusan.
3. Amankan lokasi, akan lebih baik jangan ada yang berada di daerah/meja kerja.
4. Minimalisasi interupsi terhadap lokasi, misalnya biarkan komputer apa adanya, jika komputer dalam keadaan menyala maka biarkan menyala atau dalam keadaan mati, biarkan seperti apa adanya, penanangan lebih lanjut diserahkan oleh profesional investigator.
5. Jangan menjalankan program apa pun pada komputer yang menjadi bagian dari evidence.

6. Jangan membiarkan user lain mengutak-atik komputer, termasuk atasan atau bahkan pemiliknya.
7. Kumpulkan dan dokumentasikan sumber data lainnya, misalnya CD backup, tape backup, dan log-log file.
8. Barang-barang non komputer yang dapat dijadikan evidence hendaknya diamankan, misalnya: notes, buku, dan berbagai peralatan kantor lainnya.
9. Mulailah dokumentasi *Chain of Custody*, dengan mencatat setiap evidence dan milik evidence yang adalah milik seseorang atau perusahaan, lengkapi data- datanya seperti di mana, kapan siapa yang menemukan evidence, siapa yang melakukan pemeriksaan terhadap evidence, waktu dan jam hendaknya dicatat.

Langkah-langkah demikian sangat efektif dan akan berguna kemudian untuk keperluan komputer forensik.

3.8 Berbagai Model Form Forensik

Berikut dicontohkan berbagai form yang digunakan dalam komputer forensik, mencakup pula form pada tahap forensik atau form lainnya yang digunakan sebagai langkah awal permintaan layanan forensik dan investigasi yang diajukan oleh pihak lain dengan banyak tujuan.

Beberapa form di bawah ini dikategorikan *public domain* dan dapat digunakan secara bebas, meskipun demikian form ini bukan menjadi standar baku. Anda dapat memodifikasi form sesuai kebutuhan.

Misalnya pada form yang tertera pada Gambar 3.3 dan Gambar 3.4 dirancang sangat sederhana, bahkan dapat memuat sekaligus beberapa item tetapi tergantung kebutuhan, form lainnya mungkin menghadirkan infromasi lebih rinci sesuai objek yang hendak ditinjau.

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page ___ of ___

Gambar 3.3 Sampel Form – Security Investigation

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page ___ of ___

Gambar 3.4 Sampel Form - Metropolis Police Bureau

Pada Gambar 3.5 sampai dengan Gambar 3.10, dicontohkan form yang berkaitan dengan proses forensik tahap awal, dispesifikasi berdasarkan perangkat, mungkin komputer secara umum (Gambar 3.5), detail dijabarkan berkenaan karakteristik komputer dan media penyimpanan dan konfigurasinya. Opsi yang ada sudah dibakukan sedemikian rupa untuk kemudahan.

Berikut pula untuk forensik terhadap hard drive dan media penyimpanan lainnya, opsi yang diberikan sangatlah variatif mengikuti karakteristik dari media tersebut.

Computer Evidence Worksheet

Case Number: _____ **Exhibit Number:** _____

Laboratory Number: _____ **Control Number:** _____

Computer Information

Manufacturer: _____ Model: _____

Serial Number: _____

Examiner Markings: _____

Computer Type: Desktop ☐ Laptop ☐ Other: _____

Computer Condition: Good ☐ Damaged ☐ **(See Remarks)**

Number of Hard Drives: _____ 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☐ Tape Drive ☐ Tape Drive Type: _____

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☐

DVD ☐ Other: _____

CMOS Information Not Available ☐

Password Logon: Yes ☐ No ☐ Password = _____

Current Time: _____ AM ☐ PM ☐ Current Date: ___/___/___

CMOS Time: _____ AM ☐ PM ☐ CMOS Date: ___/___/___

CMOS Hard Drive #1 Settings Auto ☐

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

CMOS Hard Drive #2 Settings Auto ☐

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

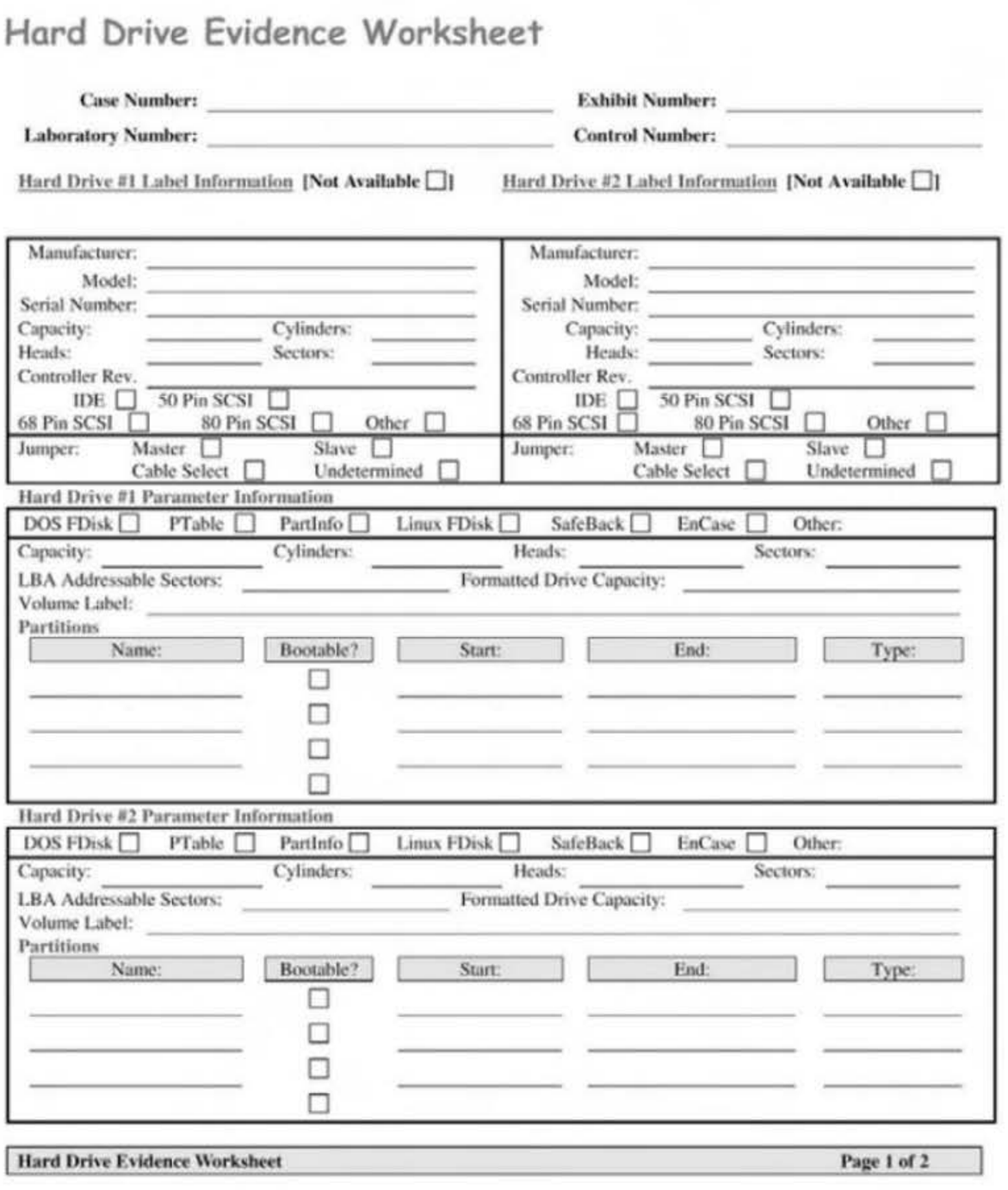
Computer Evidence Worksheet **Page 1 of 2**

Gambar 3.5 Sampel Form – Computer Evidence Worksheet (Lembar 1)

Exhibit # Sub-Exhibit #	Triage	Duplicated	Browse	Unerase	Keyword Search
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

Digital Evidence Removable Media Worksheet — **Page 2 of 2**

Gambar 3.6 Sampel Form – Computer Evidence Worksheet (Lembar 2)



Hard Drive Evidence Worksheet

Case Number: _____ Exhibit Number: _____

Laboratory Number: _____ Control Number: _____

Hard Drive #1 Label Information [Not Available ☐] Hard Drive #2 Label Information [Not Available ☐]

Hard Drive #1 Label Information	Hard Drive #2 Label Information
Manufacturer: _____	Manufacturer: _____
Model: _____	Model: _____
Serial Number: _____	Serial Number: _____
Capacity: _____ Cylinders: _____	Capacity: _____ Cylinders: _____
Heads: _____ Sectors: _____	Heads: _____ Sectors: _____
Controller Rev. _____	Controller Rev. _____
IDE ☐ 50 Pin SCSI ☐	IDE ☐ 50 Pin SCSI ☐
68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐	68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐
Jumper: Master ☐ Slave ☐	Jumper: Master ☐ Slave ☐
Cable Select ☐ Undetermined ☐	Cable Select ☐ Undetermined ☐

Hard Drive #1 Parameter Information

DOS FDisk ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

LBA Addressable Sectors: _____ Formatted Drive Capacity: _____

Volume Label: _____

Partitions

Name:	Bootable?	Start:	End:	Type:
_____	☐	_____	_____	_____
_____	☐	_____	_____	_____
_____	☐	_____	_____	_____
_____	☐	_____	_____	_____

Hard Drive #2 Parameter Information

DOS FDisk ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

LBA Addressable Sectors: _____ Formatted Drive Capacity: _____

Volume Label: _____

Partitions

Name:	Bootable?	Start:	End:	Type:
_____	☐	_____	_____	_____
_____	☐	_____	_____	_____
_____	☐	_____	_____	_____
_____	☐	_____	_____	_____

Hard Drive Evidence Worksheet Page 1 of 2

Gambar 3.7 Sampel Form – Hard Drive Evidence Worksheet (Lembar 1)

Image Archive Information

Archive Method: Direct to Tape ☐ NTBackup ☐ Tar ☐ Other :* _____ Compressed? ☐

Attach appropriate worksheet for backup method used.

Tape Type: DAT 24 ☐ Dat 40 ☐ DLT ☐* Other *: Number Used:

**Requires Lab Director Approval*

Analysis Platform Information

Operating Systems Used: DOS ☐ Windows ☐ Mac ☐ *nix ☐ Other: _____

Version: _____

Analysis Software Base: I-Look ☐ EnCase ☐ DOS Utilities ☐ *nix Utilities ☐ Other:*

Version: _____

Restored Work Copy/Image Validated:	Yes ☐ No ☐

List of utilities used other than base

Utility	Version	Purpose

Analysis Milestones

Milestone	Remarks	Initials
Run Anti-Virus Scan		
Full File List with Meta Data		
Identify Users/Logons/ISP Accounts, etc.		
Browse File System		
Keyword/String Search		
Web/E-mail Header Recovery		
Recover & Examine Free/Slack Space		
Examine Swap		
Unerase/Recover Deleted Files		
Execute Programs as Needed		
Examine/Recover Mail/Chat		
Crack Passwords		

Hard Drive Evidence Worksheet **Page 2 of 2**

Gambar 3.8 Sampel Form – Hard Drive Evidence Worksheet (Lembar 2)

Removable Media Worksheet

Case Number: _____ **Exhibit Number:** _____

Laboratory Number: _____ **Control Number:** _____

Media Type / Quantity

Diskette [ ]	LS-120 [ ]	100 MB Zip [ ]	250 MB Zip [ ]
1 GB Jaz [ ]	2 GB Jaz [ ]	Magneto-Optical [ ]	Tape [ ]
CD [ ]	DVD [ ]	Other [ ]	

Examination

Exhibit # Sub-Exhibit #	Triage	Duplicated	Browse	Unerase	Keyword Search
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

Examiner _____ Date _____ Supervisor Review _____ Date _____

Gambar 3.9 Sampel Form – Removable Media Evidence Worksheet (Lembar 1)

Exhibit # Sub-Exhibit #	Triage	Duplicated	Browse	Unerase	Keyword Search
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

Digital Evidence Removable Media Worksheet — **Page 2 of 2**

Gambar 3.10 Sampel Form – Removable Media Evidence Worksheet (Lembar 2)

Contoh form permintaan layanan forensik yang dilayangkan oleh penyidik ke sebuah lab komputer forensik di suatu negara bagian tertentu.

Example 1: Regional Computer Forensics Lab • 4455 Genesee Street, Cheektowaga, NY 14225

REQUEST FOR SERVICE

CASE INFORMATION:		***RCFL Case #:***
Submitting Person/ID#:	Date:	Agency Case #:
Submitting Agency:	Service: **Field Lab Tech**	Case Title:
Agency Property Tag #:	Suspect's Name:	
Case Agent:	Phone #:	
DDA/AUSA Assigned:	Phone #:	
Date Seized:	Case/Crime Type:	
Location Seized:	Pending Court Dates:	
Site #:	Date Analysis Needed:	
Suspect In Custody: **Yes/No**	Expected Evidence Return Date:	
Narcotics Related: **Yes/No**	Number of Computers Anticipated:	
Type of Seizure: (Circle) **Search Warrant Probation Parole Consent Admin Fed. Grand Jury Other:**		
Has this evidence been previously viewed and/or accessed by anyone? (Explain)		
Are you aware of any privileged information contained within evidence? (Explain)		
Do you want Standard Case Related Search Strings run against evidence? **Yes/No** (Circle Requested Searches) **Child Porn Narcotics Financial Crimes Internet Crimes Extortion Other:**		

SERVICE REQUESTED: ***(Requests for Field Service must be received at least 2 business days prior to the search.)***

INSTRUCTIONS:

a. Please prepare one form for each search site (address).
b. Please provide ***ALL*** requested information and note any unusual circumstances in the Service Request area.
c. Please attach an Evidence Custody Form listing each individual container or package of submitted evidence.

RCFL USE ONLY **Date Case**	**Received By:**
Case Priority:	**Priority Established By:**

Berikut ini dicontohkan form permintaan untuk layanan investigasi forensik yang di request oleh Departement of The Air Force kepada Department of Defences Computer Forensics Laboratory (Dod CFL).

Example 2: DoD Computer Forensics Laboratory (DCFL) Intake Form

(Form has been edited)

DEPARTMENT OF THE AIR FORCE

AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

(USE YOUR OWN LETTER HEAD)

MEMORANDUM FOR RECORD DoD Computer Forensics Laboratory
12 June 2000

TO: DoD Computer Forensics Laboratory (DCFL)
911 Elkridge Landing Road, Suite 300
Linthicum, MD 21090

FROM: Self-Explanatory

SUBJECT: Request Forensic Media Analysis (Complete Unit Investigation Number)

NOTE: Do not remove the captions (the bold face lettering only. Please remove the explanations.). If no information can be applied to a certain caption, then state N/A or unknown.

1. ***FULL NAME OF SUBJECT: (If unknown, then state "Unknown.")

JOHN JIM DOE

2. ***PRIORITY: Explain if there is publicity, high-level interest, or other reasons to justify placing this investigation ahead of others (e.g., court date, etc.).

3. CLASSIFICATION: Unclassified–Secret–Specialized Compartmented Information, as it pertains to the investigation, and properly mark all documents.

4. ***CASE AGENT: (This is the "Lead" investigator. For example, if this is a joint investigation, then provide the identification of the "Lead Investigator" of the "Lead Investigating Agency." Provide complete identification and where they are located.) SA Max Factor, AFOSI Detachment 998, Home AFB, WV, DSN: 234–2345 or Commercial: (234) 234–2345.

NOTE: The DCFL does not have DSN service yet. Please provide commercial telephone numbers.

5. ***SYNOPSIS OF THE CASE FACTS: (Brief description of allegation, situation, and background surrounding the investigation. Provide information that will be useful to the

examiner so they can better understand the investigation and provide a better examination). You can provide an already completed document or a pending report to cover this step.

6. ***ITEMS TO BE ANALYZED: (NOTE: IF NOT EVIDENCE, STATE THAT FACT)

NOTE: It is only required to list the items to be analyzed, not to answer all the questions.

This must be a complete list of all items that need analysis. An evidence listing must completely identify all items. The following is just a sample of how to list evidence:

Tag #'s	**Description**
Tag # XX	Western Digital Caviar 31600 Hard Drive, Serial #: WT2891586134 taken from AST Computer Serial # 186AUZ022348.
Tag # XX	Fujitsu M1636TAU Hard Drive, Serial #: 08613105, Size: 1226MB.
Tag # XX	Gateway 2000, 386/33 MHz, Serial #: 302557386-330XC. Computer System with a Western Digital 125 MB internal hard drive, a Seagate 107 MB internal hard drive, internal 3.5-inch high-density floppy drive, one internal 5.25-inch floppy drive, internal sound card. Gateway 2000 101 Keyboard, Serial #: 9208572226f7. Computer Mouse Device, Serial #: 850753.
Tag # XX	198 each 3.5-inch floppy diskettes 1 each 5.25-inch floppy diskettes

7. ***SUPPORT REQUESTED: (Specific and detailed request. Do not just cut and paste what is listed below. These are just some sample statements. If you do not know what one of these items is, then don't include it. Also, don't just say "give me everything" and expect DCFL to take it from there. List items you need the DCFL to find and how you need it produced and provided to you.)

e.g. **Computer Media**

Extract all system logs, graphic files, text, documents, etc.
Examine file system for modification to operating system software or configuration.
Examine file system for back doors, check for setuid and setgid files.
Examine file system for any sign of a sniffer program.
Extract data from this 8-mm tape and convert to readable format, cut to CD.
Backup hard drives and place backup on a CD, tape, or other format.
Analyze for deleted files and restore deleted files, cut findings to CD.
If possible, correlate sexually explicit images to the Internet history file.
Extract sexually explicit images from logical, slack space, free space, cut to CD.
Extract all pertinent text files of a sexual nature.
Provide an analysis report and cut all findings to CD (specify).
Conduct string search on physical level of media (provide list of words).

8. PERTINENT DATA: (e.g., provide passwords, keyword lists, operating system, nicknames, computer types, network information, Internet Protocol Address, and any other information that will assist with the analysis.)

NOTE: If network intrusion detection logs or other detection type logs are associated with the respective investigation (e.g., ASIM logs, Government Sniffer Logs, etc.), they should be provided (electronic form preferable, paper is acceptable). This will enhance the examiner's ability to provide a better product and to interpret the logs in an effort to search for the right items.

NOTE: The examiner will conduct only the specific tasks requested. If not specified, then it will not be done. If obvious items are left off the request, the DCFL will call to verify. The more detail you provide, the better and more analysis we conduct.

NOTE: Contact your servicing computer expert to aid in creation of this request, if necessary.

9. ***AUTHORITY: Please indicate the legal basis for DCFL conducting the search you are requesting. There are generally three bases in criminal cases that would allow DCFL to perform your request:

1. Search Warrant/Military Search Authority (include supporting affidavits).
2. Consent.
   - DoD Banner.
   - Unit User Agreement.
   - Written Consent Signed by Authorizer.
   - Written Record of the Designated Approval Authority or Other Official who has the Right to Consent to the Search of the Media.
   - Memorandum of oral consent with special emphasis as to the scope of the consent granted.
3. Written Memo from servicing legal office stating that there is no reasonable expectation of privacy in the media submitted.

Inclusion of a copy of documents listed above is mandatory along with the request and will speed the analysis. Failure to include the same will result in a delay until such time as DCFL is satisfied that there is a legal basis for conducting the analysis.

10. ***OTHER DOCUMENTS: Requestors **MUST** provide the form used to open the investigation within their organization (e.g., provide a copy of an ACISS report, Army Form 66, or Navy ALS, etc.).

11. INSTRUCTIONS: Let the DCFL know if you have specific instructions. Please send copy of analysis report to both ? and ? Please return all evidence to ?

12. ***POC is: (This is the Requestor's contacting information, i.e., the person who authored this request. It could be the same as the "Lead Agent," and, if so, just state "Same."). Provide complete identification and contacting information: SA Jane Doe, AFOSI Detachment 999 at DSN: 123–1234 or Commercial: (123) 123–1234.

NOTE: If the required information (marked by ***) is not outlined in or not with this request, then the request for examination will be placed on hold until ALL information is provided.

JANE DOE, SA, USAF
Computer Crime Investigations

Perhatikan Gambar 3.11, form permintaan layanan Department of Maryland State Police, Computer Forensic Laboratory. Form ini menjadi bagian dalam proses pertama komputer forensik, header informasi dijabarkan dengan sangat rinci dan pada sudut kanan bawah ditambahkan tingkat urgensinya melalui pilihan Case Priority.

Form yang dirancang pasti berbeda antara satu departmen dengan departmen lainnya, atau satu organisasi dengan organisasi lainnya, seperti yang ditampilkan pada Sample Form Miami Valley RCL atau Miami Valley RCFL, yakni kepentingan akan informasi dan rincian informasi dicantumkan berbeda.

Department of Maryland State Police
Computer Forensic Laboratory
TELEPHONE 410-290-1620 FAX 410-290-1831
7155 C Columbia Gateway Drive, Columbia, Maryland 21046

REQUEST FOR SERVICE

Date Submitted:					MSP Complaint Control #:
Submitting Agency:	Address:		County:		Agency Case #:
Submitting Officer	ID#:	E-mail Address:			Telephone:
Location Seized:		Date Seized:			Agency Property #:
Case Title:	Suspect's Last Name, First Name, MI:		Sex: M F	Age:	Tracking Number:
Crime:	Date of Offense:	Date Charges Filed:	Court Date:		Court / Location:
Owner of Property - Name:	Address:				Telephone:

Type of Seizure: (Circle) **Search Warrant** **Consent** **Administrative** **Federal Grand Jury** **Other:**

Number of Computers:	CCU Consulted Reference Seizure: ***(Attach a copy of the Search Warrant Affidavit and the Inventory/Return)***
Has this evidence been previously viewed, accessed, and/or examined by anyone? (Explain)	**Yes** **No**
Are you aware of any privileged information contained within the evidence being submitted for examination? Explain)	**Yes** **No**
Are you aware of any other information related to the evidence being submitted? (Explain)	**Yes** **No**

☐ **Urgent Request for Examination**

Date Request Received:	Person Making Request - Name / Title	Telephone # where you can be reached:	Date Analysis Needed:
Reason for Request: ***(Except for Imminent Court dates, ALL Urgent requests must be accompanied by a letter of justification.)***			

SERVICE REQUESTED: ***(Requests for field service must be received at least 2 business days prior to search)***

INSTRUCTIONS

☐ Please prepare one form for each search site (address).
☐ Please provide ***ALL*** requested information and note any unusual circumstance in the "Service Requested" area.
☐ Please attach a **Request for Laboratory Examination Chain of Custody Log** (MSP Form 67) and a copy of your agency /installation **Property Record** listing each container or package submitted as evidence.
☐ Please attach a **Detailed Summary** of suspect information, which includes personal data, e-mail addresses, nicknames, screen names, passwords, target websites, accomplices, and a list of unique keywords relevant to your investigation.

LABORATORY USE ONLY:		
LabCASE #:	**Date Case Received:**	**Case Priority:** 1 2 3 4 5
	Received by:	**Priority Established by:**

Gambar 3.11 Sampel Form – Permintaan Layanan Forensik pada Department of Maryland State Police Computer Forensic Laboratory

Secara general, forensik mencakup banyak bidang dan kasus, dan form global yang deskriptif diperlihatkan pada Gambar 3.12, kebutuhan yang berfokus pada proses analisa, seperti dipaparkan dalam form mencakup:

- Sidik jari (Fingerprint).
- Kimia dan obat-obatan (Chemistry).
- Komputer forensik (Computer Forensic), dan lain sebagainya.

MIAMI VALLEY REGIONAL CRIME LABORTORY

361 W. Third St., Dayton OH 45402 937-225-4660 FAX 937-496-7916

(x) New Case
( ) Additional Evidence
In an Old Case

Date Rec'd_____

D#:

Complainant/Victim(s): _____
Subject / Suspect(s) _____ DOB/SSN _____
Location of Offense _____
Offense _____ Date of Occurrence _____
Investigating Officer _____ Phone _____

Analysis Codes

Fingerprints
LP01 Search for Latent Prints
LP02 Latent Print Evaluation *retain at lab*
LP03 Latent Print Evaluation *return to department*
LP04 FP Comparison
LP05 AFIS Inquiry-print Marked?
LP06 AFIS Inquiry-enter best print?
LP07 Other Request**

Chemistry
C01 Drug analysis Juvenile ( )
C02 Blood Alcohol Anal.
C03 Urine Alcohol Anal.
C04 Drug Screen on Urine
C05 Alcoholic Beverage
C07 Arson Analysis
C08 Gunshot Residue Analysis (AA)
C09 Other Request**

Crime Scene ( )

Photographs ( )

Computer Forensics
CF01 Image/Exam*

Serology
S01 Blood Identification
S02 Semen Identification
S03 Other Request*

Trace Evidence
T01 Hair and Fiber Exam
T02 Paint Comparison
T03 Glass Comparison
T04 Footwear Comparison
T05 Soil Comparison
T06 Other Request**

Firearms/Toolmarks
F01 Firearms Identification
F02 Gunpowder Pattern
F03 Toolmark Comparison
F04 Serial Number Restoration
F05 Bullet/Cartridge Case Comparison
F06 Other Request**

Questioned Documents
QD01 Document Exam
QD02 Other QD Request**

*attach computer exam request form
** describe in synopsis

List of Evidence	Property Tag #	Analysis Code	Disposition

Synopsis of Case:

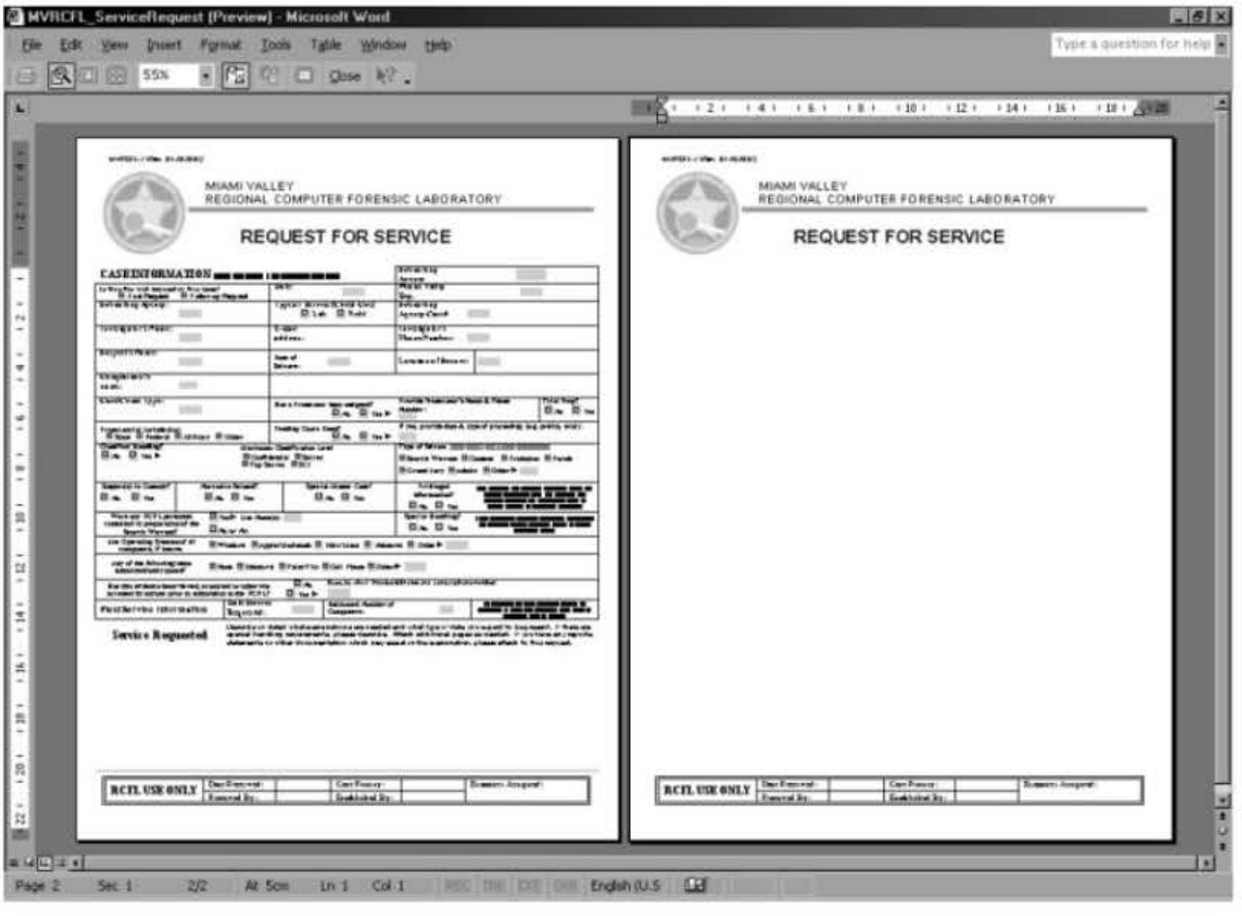
Submitting Officer _____ Department _____ Phone _____
Address _____ City _____ Zip _____ Fax _____

NATIONALLY ACCREDITED BY THE AMERICAN SOCIETY OF CRIME LABORATORY DIRECTORS

Gambar 3.12 Sampel Form Miami Valley Regional Crime Lab

Pada Gambar 3.13, perhatikan Form Layanan Miami Valley Regional Computer Forensic Laboratory, form ini dapat di-download di website yang bersangkutan.

Form tersebut digunakan hanya pada lingkungan terbatas, dan kemudian diteruskan untuk proses forensik lebih lanjut.



Gambar 3.13 Contoh template formulir permintaan layanan forensik yang dapat di download – Miami Valley

Anda dapat merancang form spesifik sesuai kebutuhan, atau organisasi/ perusahaan Anda. Beberapa form tadi dapat digunakan sebagai pembanding.

Lebih jauh lagi, Anda mungkin dapat menggunakan toolkit komersial, seperti yang ditampilkan pada website (http://computer-forensics.privacyresources.org) seperti terlihat Gambar 3.14, dicontohkan toolkit yang mencakup pula form dan template yang sudah siap digunakan.

Computer Forensic Forms

TOOLKIT CONTENTS

Introduction & Guide
A general guide and introduction on how to approach computer forensics .

A Management Presentation
An 86 full presentation introducing forensics and digital evidence to management.

Forensics Report Template
A template for your forensic examination report.

Manuals and Procedures
Detailed manuals and procedures.

Forensic Glossary
A comprehensive glossary of computer forensic Terms and Phrases

Miscellaneous Resources
Including:
- An FAQ
- A case cost estimator
- Tips for choosing a forensics expert
- Additional support items
- Summary of case studies

Checklists
For both the case and the investigation.

Tool Reference
A substantial reference log of publicly available software tools for computer forensics.

Computer Forensics requires the careful recording of data from all stages of the investigation. This is needed for both evidential, quality and referential reasons.

Look no further: the requisite forms are here. The toolkit contains a series of forms (MS-Word format), as used by established experts in the field. This even includes a log book form for exhibit movements.

Typical Form:

Hard Disk Details

Case No		Exhibit Ref. No.	
Make:		Model:	
Serial No:		Size:	
Cylinders:		Heads:	
Sectors:		Jumper setting :	
Volume Label		No of Partitions	
Partition Name 1		Partition Name 2	
Partition Name 3		Partition Name 4	
Imaging			
Software and Version (Image 1)		Write blocker type used	
Software and Version (Image 2)		Write blocker type used	
Time Corrected		Time Source	
Notes:			
Hashes Match Image 1		Hashes Match Image 2	
Hash verification attached)	Yes / No	If not attached, where can it be found	

Case Hard Drive Information		
Original Image located on Disk No (in safe)	Disk Reference No	
Backup Image located on Disk No (in safe)	Disk Reference No	
Backup Image located on Disk No (in server)	Disk Reference No	
Work Disk for case	Disk Reference No	

Gambar 3.14 Formulir keperluan komputer forensik

BAB 4
PROSEDUR DAN STANDARISASI KOMPUTER FORENSIK

4.1 Standarisasi Komputer Forensik

Standar dalam komputer forensik pada umumnya harus memenuhi kebutuhan standar pertukaran data atau informasi antarorganisasi, antarperusahaan, perorangan dengan organisasi atau bahkan lebih luas antarnegara yang melibatkan kebijakan setiap negara terhadap digital evidence.

Standar pada umumnya harus mengisi seluruh aktivitas dalam komputer forensik mencakup:

- Standar pendefinisian.
- Prinsip kerja.
- Proses dan metoda.
- Hasil (mencakup mengalamati dan memperlakukan setiap aktivitas dan hasil akhir).
- Bahasa.

Dari beberapa komponen yang menjadi standar tersebut harus dapat menjawab masalah inkompatibilitas semisal:

- Apakah layak untuk mengambil terlebih dahulu dan kemudian menganalisa suatu evidence?
- Bagaimana dengan proses mendapatkan dan mengorek informasi?
- Apakah proses forensik layak dalam sisi hukum, etika, dan teknologi informasi?

Dalam komputer forensik, diberlakukan standar yang mempertimbangkan lima faktor antara lain:

- Identifikasi subjek.
- Pemulihan komputer (Computer Recovered).
- Menyingkapkan jalur komunikasi (Reveal Communication Link).
- Permintaan investigasi.
- Pengumpulan digital evidence lainnya.

Kebutuhan akan standar ini ditindaklanjuti segera, ini terbukti dengan berbagai konferensi progresif yang diadakan, antara lain:

- Pada tahun 1993 diselenggarakan konferensi internasional pertama berkenaan komputer evidence.
- Pada tahun 1995-an dibentuk organisasi internasional komputer evidence (IOCE).
- Tahun 1997, G8 dan IOCE secara independen menentukan mengembangan standar berkenaan komputer evidence.
- Pada tahun 1998-an banyak organisasi lain yang ikut berpartisipasi, seperti SWG-DE, ACPO, FCG, ENSFI, dan INTERPOL.
- Akhir tahun 1999 ACPO, IOCE, FCG, dan ENSFI membahas mengenai standar komputer forensik di Eropa.

Dengan kebutuhan yang dialamati dengan cepat dan berkembangnya standar komputer forensik, ada kejelasan dan hasil-hasil positif yang didapat, ini mencakup perilaku terhadap komputer evidence, dilibatkannya komputer evidence terhadap tindak kriminal dan proses hukum, memperlengkapi para penegak hukum, dan masih banyak lagi hal-hal positif yang dicapai.

Kondisi tersebut memperlihatkan berkembangnya bidang komputer forensik, prinsip yang dihasilkan dari konferensi dan organisasi seputar komputer forensik misalnya: menangani evidence dan jenis serta berbagai pengertian dalam komputer forensik.

Pada bab ke tiga, Anda mendapatkan gambaran secara umum tahapan yang dilakukan pada komputer forensik.

Setiap organisasi dapat menerapkan tahapan secara berbeda mungkin beberapa tahap dilakukan terprosedur, atau beberapa tahap digabungkan menjadi satu atau satu atau lain tahap dihilangkan karena berdasarkan beberapa pertimbangan, hal itu sah-sah saja, tergantung dari kebijakan organisasi yang bersangkutan.

Tanpa mengabaikan standar, dan bahkan mengadopsi standar, bab ini akan membahas kembali langkah-langkah yang ada pada komputer forensik dengan pertimbangan faktor seperti kebijakan, etika dan kelayakan.

4.2 Organisasi SWG-DE

Organisasi ini dibentuk pada Februari 1998 oleh The Federal Crime Laboratory Directors dan berfokus pada forensik digital evidence.

SWG-DE ini dibentuk dan berada dalam naungan yang sama dengan organisasi lain yang melibatkan organisasi forensik seperti: *Scientific Working Groups on DNA* (SWGDAM), *Questioned Documents*

(SWGDOC), *Trace Evidence* (SWGMAT), *Drugs* (SWGDRUG), *Fire and Explosives* (SWGFEX), *Fingerprints* (SWGFAST), dan *Imaging* (SWGIT).

Keanggotaan SWG-DE mencakup organisasi pemerintahan, organisasi komersial, bahkan institusi pendidikan. Dapat Anda perhatikan keanggotaan yang tertera sebagai berikut:

Negara bagian dan Lokal

- California Highway Patrol.
- Charleston SC Police Department.
- Florida Department of Law Enforcement.
- Ft. Worth Police Dept (TX).
- Houston Police Department.
- Illinois State Police.
- Irving Police Department (TX).
- Lakewood Police Department.
- Lenexa Police Department (Kansas).
- Marshall University.
- Miami-Dade Police Department.
- North Carolina State Bureau of Investigation.
- Norwood Police Department (MA).
- Ocean City Police Department, MD.
- Philadelphia Police Department.
- Santa Clara Crime Lab.
- South Carolina Law Enforcement Division.

- State of South Dakota Forensic Laboratory.
- The University of Illinois at Chicago Police Department.

Federal

- Defense Cybercrime Center.
- Department of Defense Computer Forensics Laboratory.
- Federal Bureau of Investigation.
- Internal Revenue Service Criminal Investigation.
- United States Army Criminal Investigation Laboratory.
- United States Environmental Protection Agency - Criminal Investigation Division.
- United States Fish and Wildlife Service.
- United States Secret Service.
- US Customs & Border Protection.

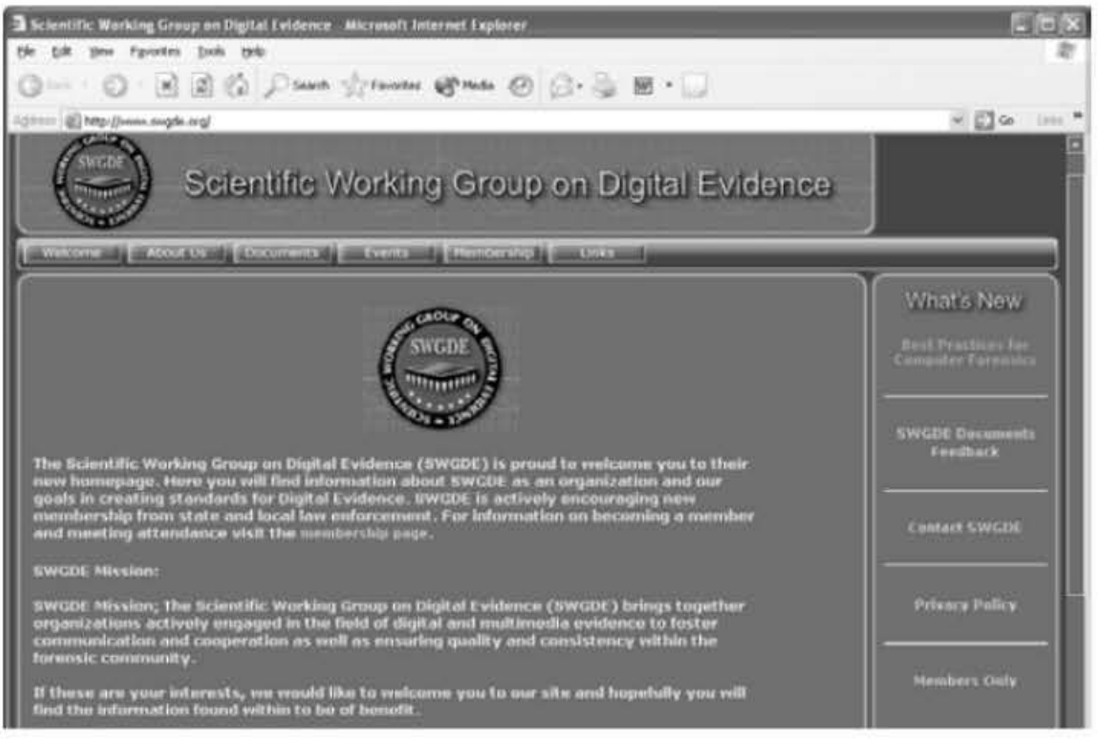
Internasional

- Australian Federal Police.
- Centre of Forensic Sciences (Ontario).
- Royal Canadian Mounted Police.

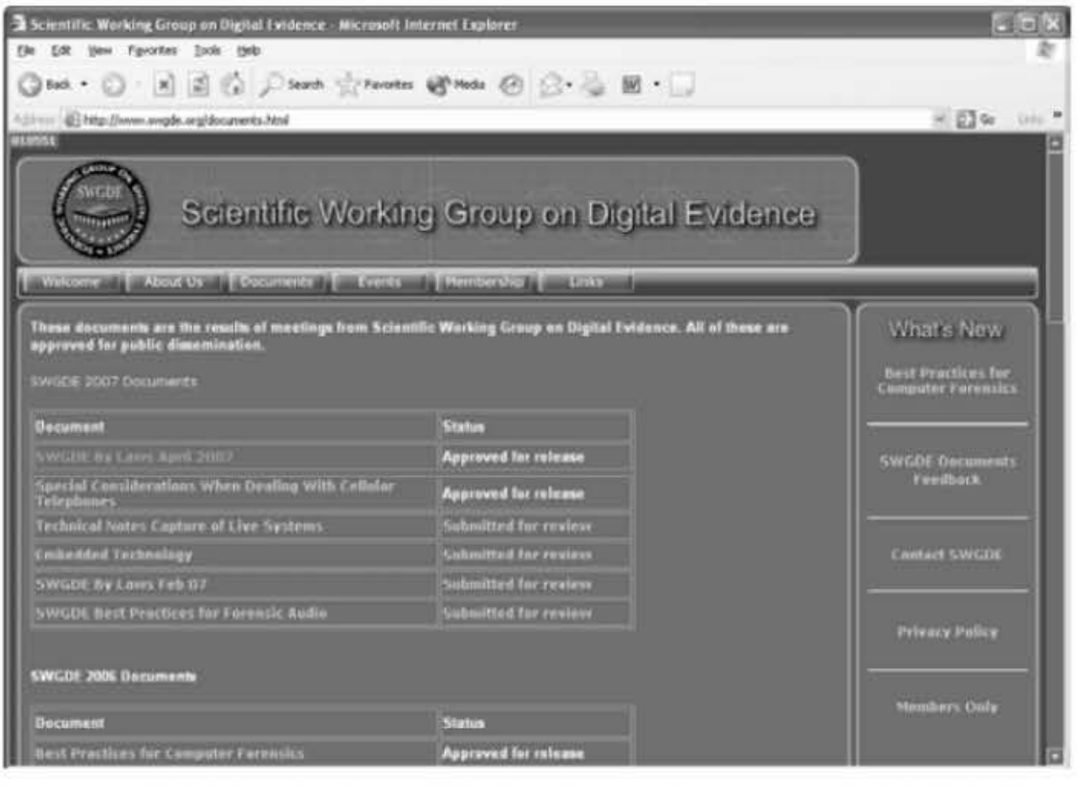
Associate Members

- Bank of America.
- Purdue University.
- National Center for Forensic Science.
- National Institute of Standards and Technology.

Untuk mendapatkan informasi lebih mendalam dan informasi forensik lainnya dari hasil kerja keras organisasi SWG-DE, Anda dapat mengakses website-nya (Gambar 4.1), men-download format pdf-nya (Gambar 4.2).



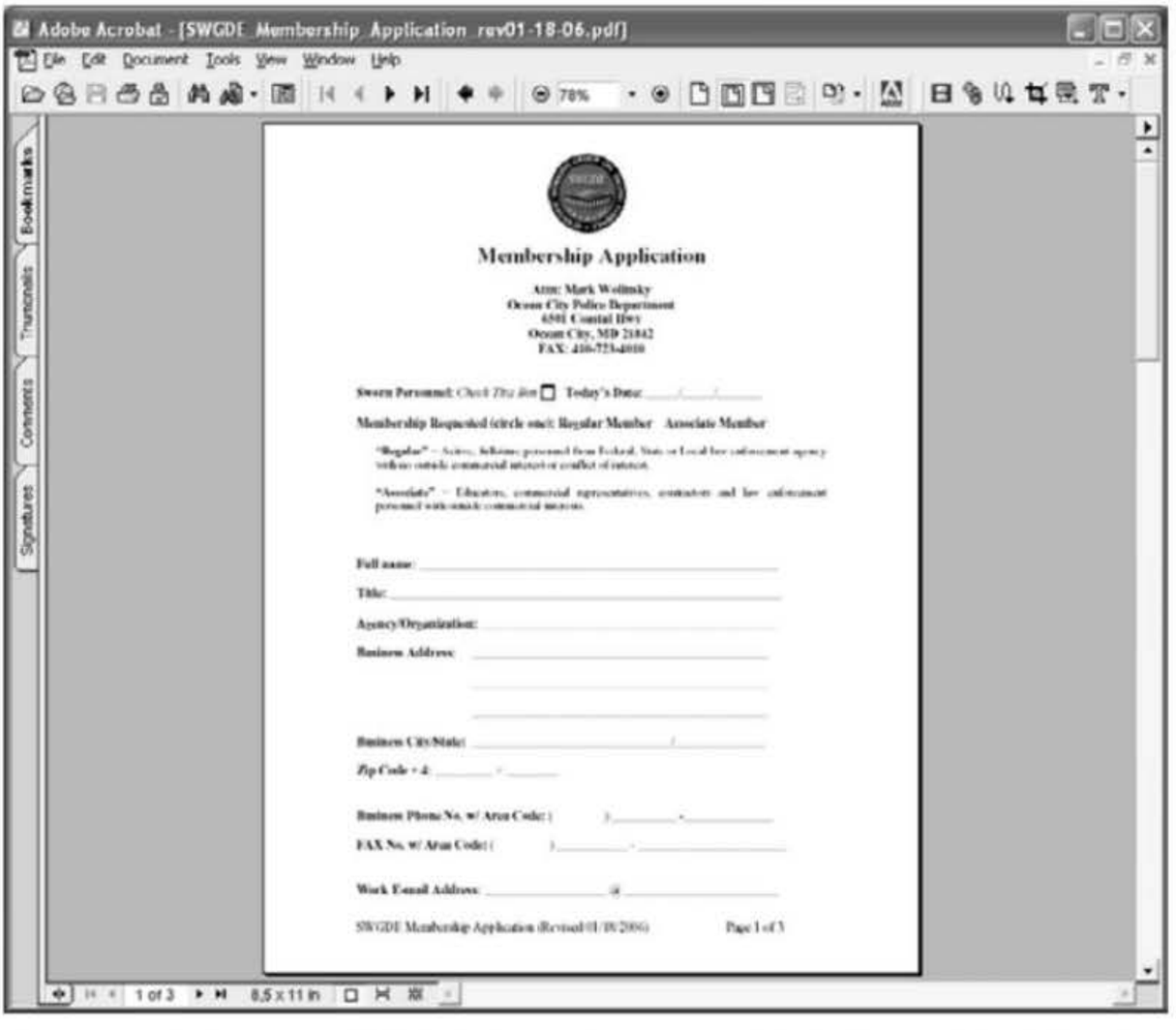
Gambar 4.1 Website Scientific Working Group on Digital Evidence (www.swgde.org)



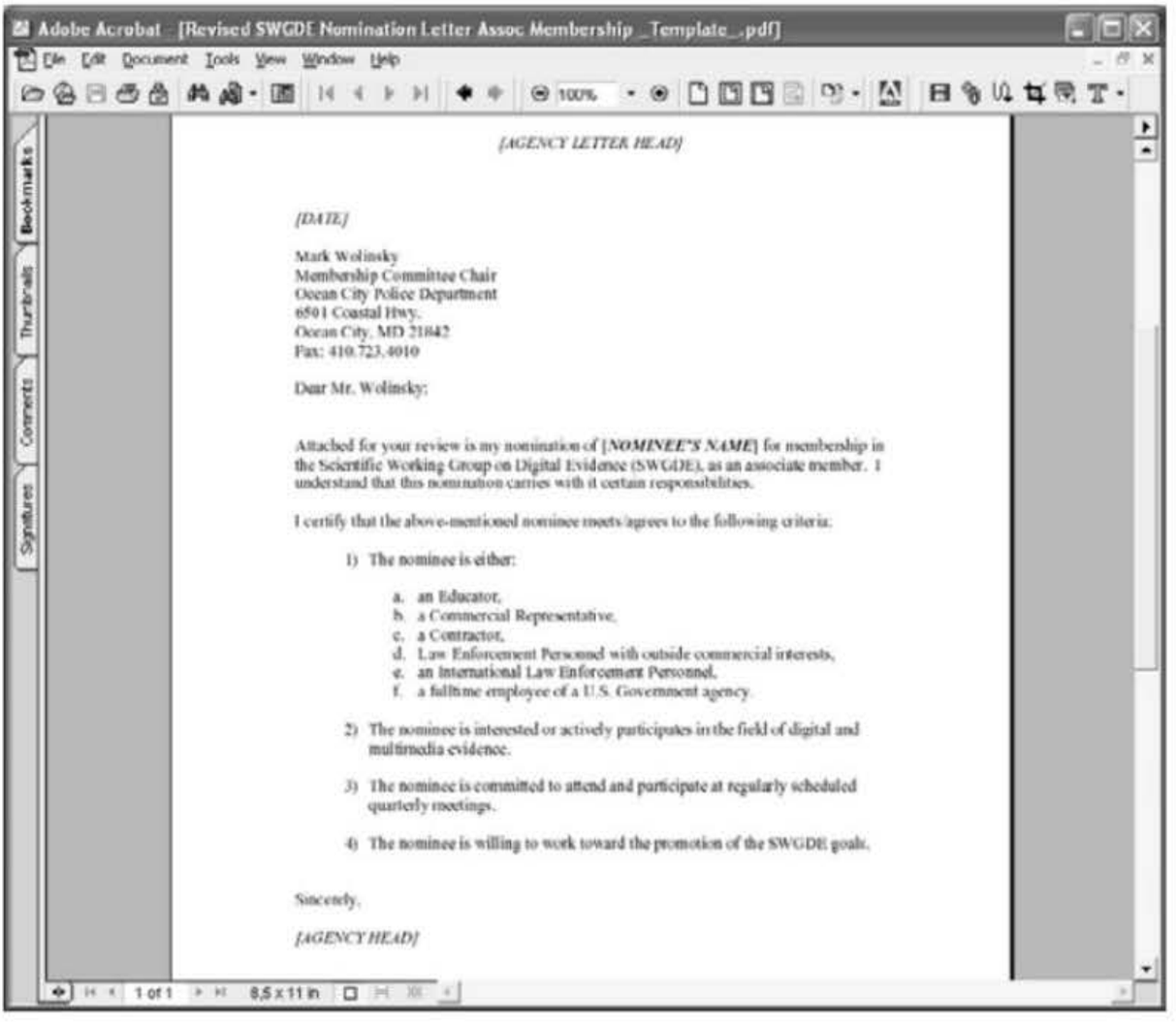
Gambar 4.2 Website Scientific Working Group on Digital Evidence (Dokumen Download)

Sedangkan untuk mengajukan keanggotaan, Anda dapat men-dowload formulir yang ada pada website tersebut dan mengirimkan kembali formulir yang sudah dilengkapi data yang relevan.

Perhatikan Gambar 4.3 dan Gambar 4.4, salahsatu contoh formulir dan template yang wajib diisikan untuk pengajuan keanggotaan.



Gambar 4.3 Website Scientific Working Group on Digital Evidence – Membership Application

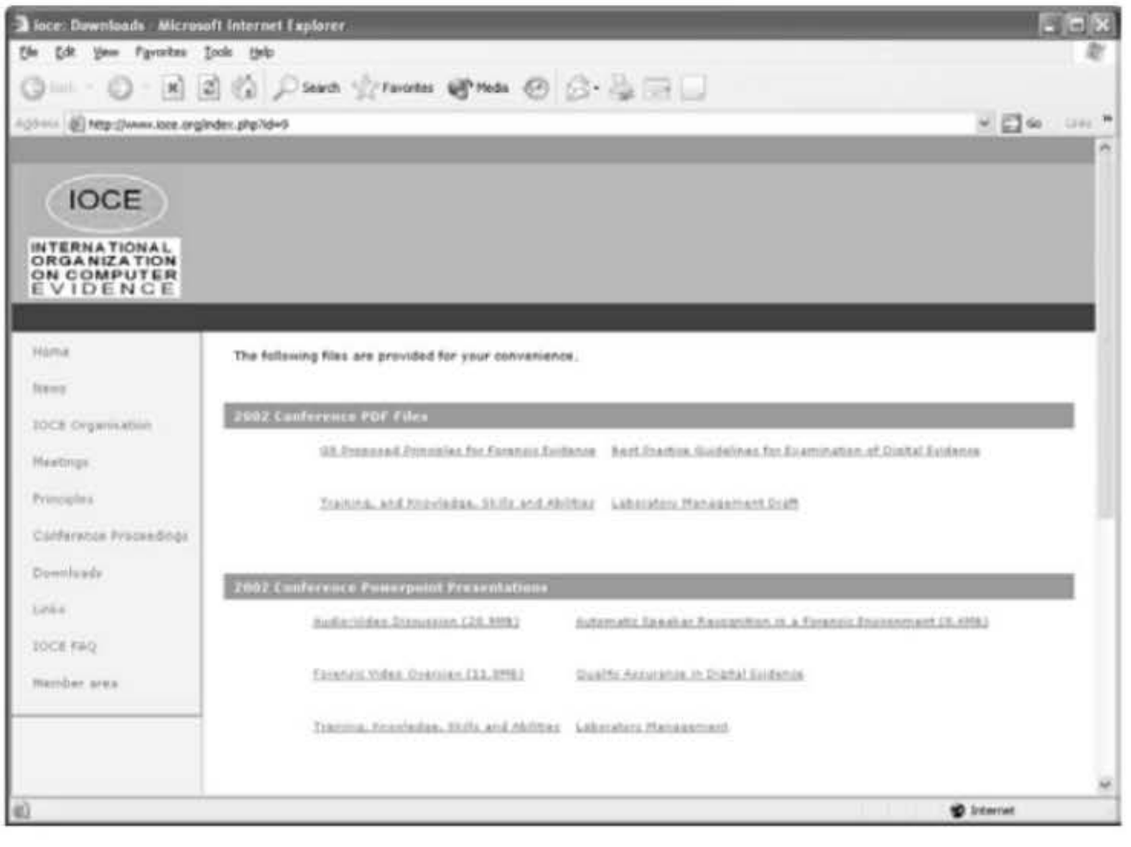


Gambar 4.4 Website Scientific Working Group on Digital Evidence – Revised Template

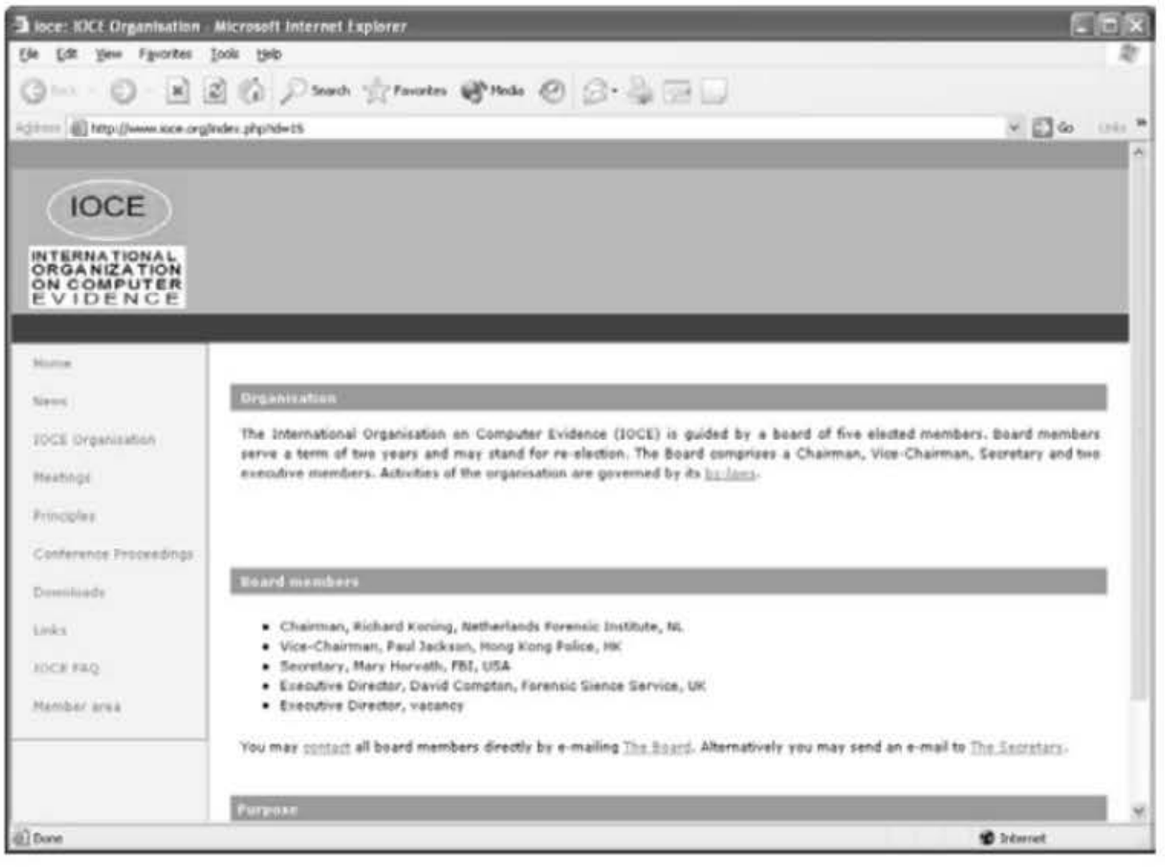
4.3 Organisasi IOCE

The International Organization on Computer Evidence (IOCE) yang didirikan pada tahun 1995 sebagai media/sarana pertukaran informasi bagi para penegak hukum skala internasional mengenai investigasi kejahatan komputer dan masalah-masalah forensik yang terkait.

Gambar 4.5 Website International Organization on Computer Evidence (IOCE) (www.ioce.org)



Gambar 4.6 Website International Organization on Computer Evidence (IOCE) – Conference PDF Dokumen Download



Gambar 4.7 Website International Organization on Computer Evidence (IOCE) - About

Beberapa prinsip IOCE:

- Konsisten terhadap sistem perundangan.
- Menggunakan bahasa yang umum.
- Berdaya tahan alias tangguh.
- Berkemampuan untuk melewati batas-batas internasional.
- Memastikan keabsahan evidence.
- Dapat diaplikasikan pada setiap *forensic evidence.*
- Aplikatif untuk setiap tingkatan, mencakup individual, organisasi, dan bahkan negara.

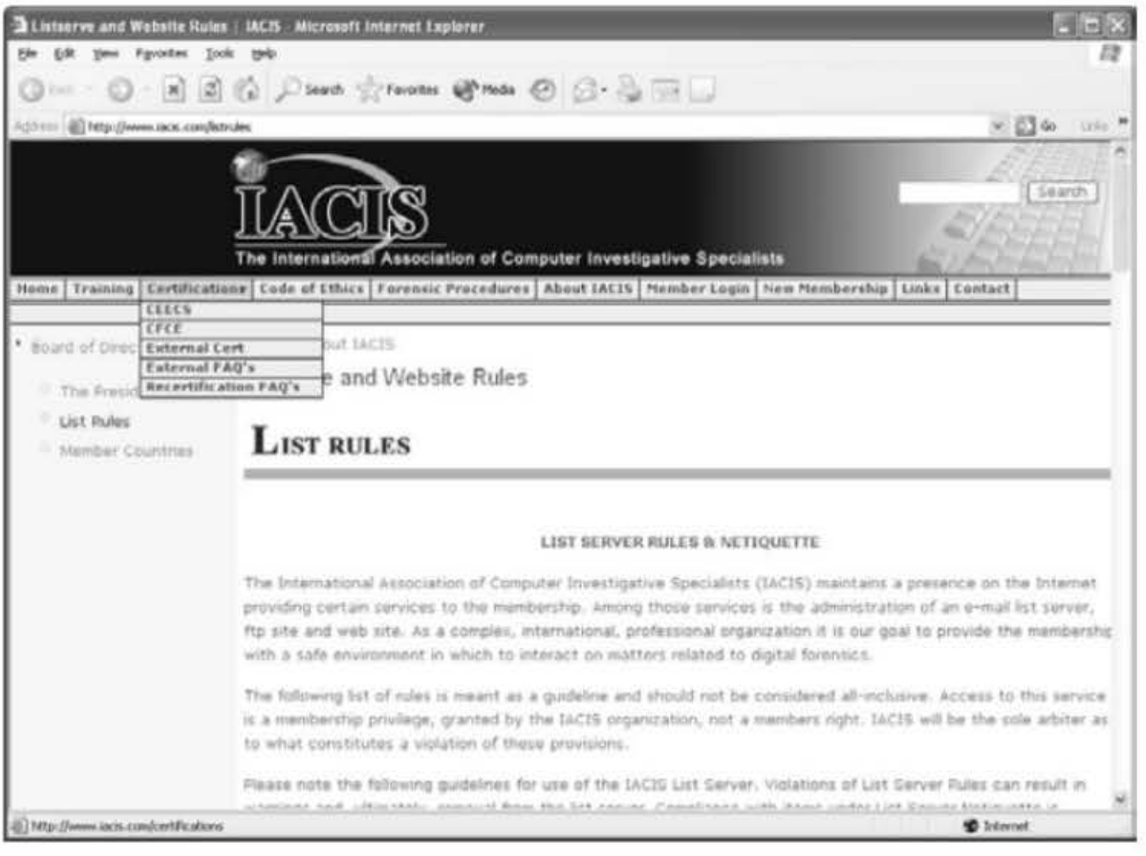
4.4 Organisasi IACIS

The International Association of Computer Investigative Specialist (IACIS) adalah organisasi internasional non komersial yang terdiri dari para penegak hukum profesional yang ditujukan untuk kepentingan edukasi spesifikasi ilmu komputer forensik.

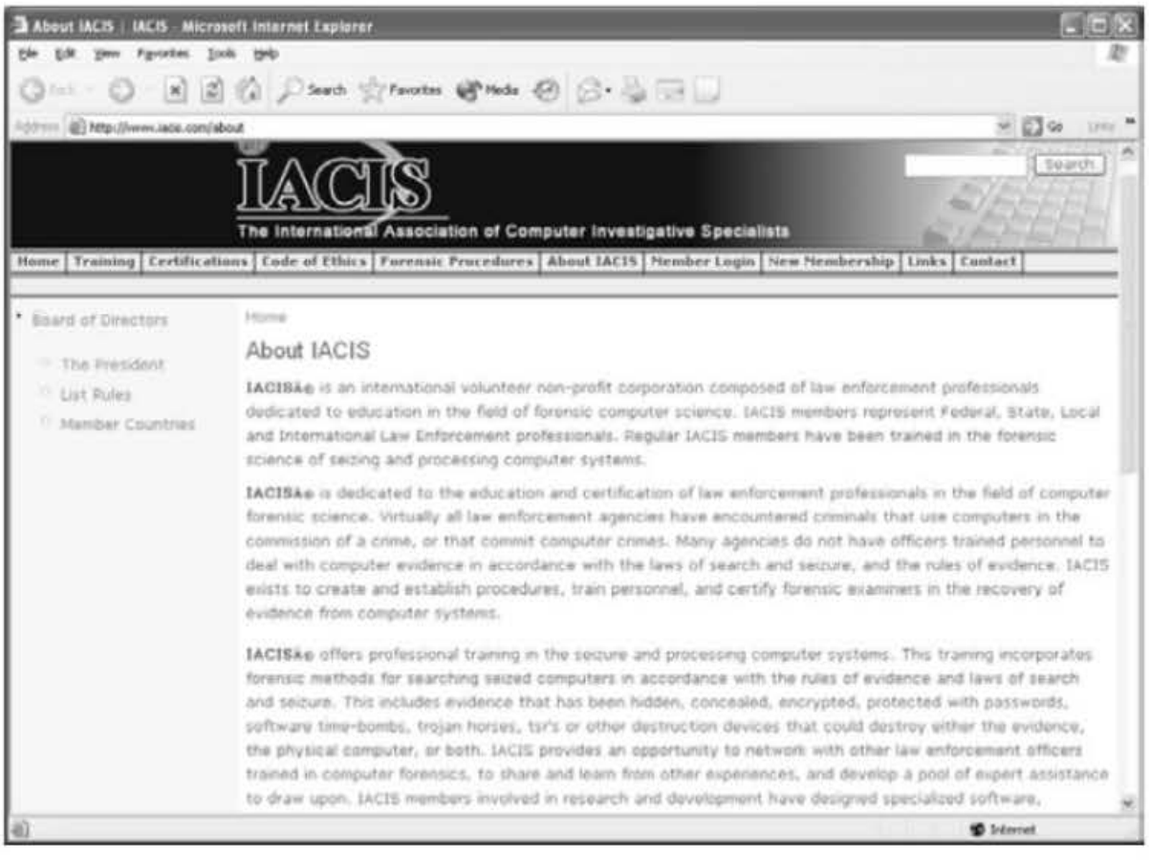
Keanggotaannya IACIS mencakup member di tingkat federal, negara bagian, lokal, dan penegak hukum profesional berskala internasional. Para anggota IACIS mendapatkan pelatihan ilmu forensik berkenaan penggunaan dan pemrosesan sistem komputer.

Organisasi ini menawarkan keanggotaan dengan berbagai keuntungan, akses informasi dapat dilakukan melalui newsletters, file library, dan juga list server, sehingga para anggotanya dapat berkomunikasi dan bertukar pengalaman dan kemampuan yang mencakup digital forensik, kemutakhiran teknologi, dan berbagai masalah kejahatan komputer

Beberapa informasi seputar IACIS ditampilkan pada beberapa gambar berikut. Perhatikan pula kode etik pada Gambar 4.10. Program sertifikasi diadakan pula oleh organisasi ini semisal Certified Forensic Computer Examiner (CFCE) dan the Certified Electronic Evidence Collection Specialist (CEECS) (Gambar 4.11).

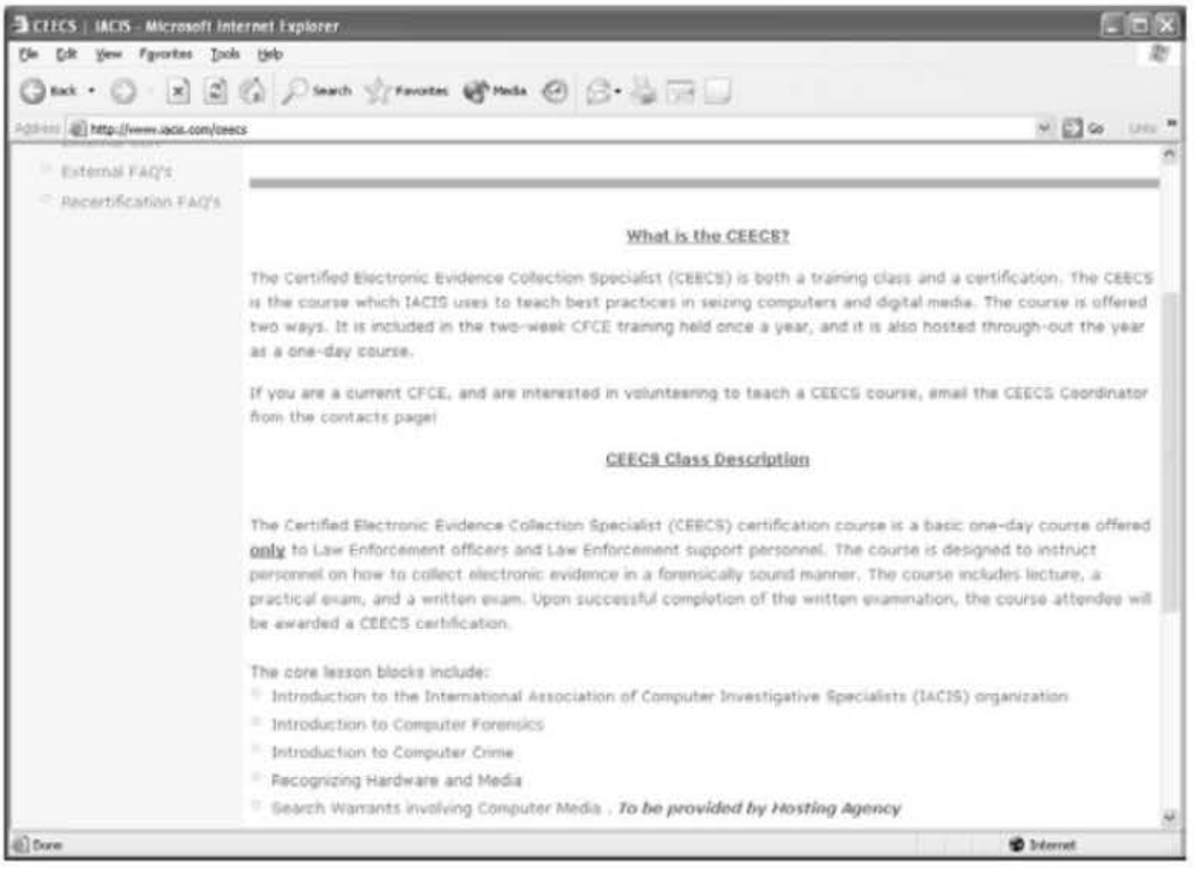


Gambar 4.8 Website The International Association of Computer Investigative Specialist (IACIS) (www.iacis.com)



Gambar 4.9 Website Website The International Association of Computer Investigative Specialist - About

Gambar 4.10 Website Website The International Association of Computer Investigative Specialist – Kode Etik Organisasi



Gambar 4.11 Website The International Association of Computer Investigative Specialist - Sertifikasi

Untuk menerapkan standarisasi komputer forensik, Anda dapat mengacu pada beberapa organisasi yang disebutkan pada subbab sebelumnya, mungkin Anda mengadopsi sebagian atau bahkan seluruhnya dan kemudian dirancang sesuai kebutuhan dan karakteristik organisasi atau perusahaan Anda.

Apa pun bentuk standarisasi yang diberlakukan, semuanya pasti melibatkan tiga komponen utama yang berkolaborasi untuk pencapaian satu tujuan, seperti yang dibahas pada bab terdahulu, yakni: tool/perangkat, manusianya, dan aturan/protokol.

Kolaborasi ketiganya harus mengisi setiap proses dan metoda komputer forensik, untuk lebih jelasnya perhatikan tahapan komputer forensik dan Anda dapat merasakan atmosfir yang melingkupinya

4.5 Kebijakan dan Prosedur

Pada prinsipnya, komputer forensik adalah salah satu bidang keilmuan yang membutuhkan keberadaan spesialis dan dikhususkan, ini tentunya berbeda dengan hanya semata-mata spesialis teknologi informasi secara umum. Keberadaan spesialis harus mendukung manajemen dan menjaga agar masing-masing komponen yang terkait (mencakup personel) dapat beroperasi secara berkualitas.

Kesemuanya dimampukan dengan adanya pelatihan yang komperhensif, menekankan pada teknik, kualitas, efisiensi, dan efektifitas yang harus mencirikan kinerja organisasi atau tim.

Misi dari organisasi berada dalam batasan protokol dan prosedur, dan ada tujuh hal yang perlu dipertimbangkan untuk mengalamati ptotokol dan prosedur:

1. Personel.

   Beberapa yang perlu dipertimbangkan akan keberadaan Personel, ini mencakup: deskripsi pekerjaan, kualifikasi minimum, waktu beroperasi, satus on-call duty, struktur, dan susunan tim.

2. Pertimbangan administratif, mencakup:

   a. Software.

      Software yang digunakan harus mendapatkan lisensi.

   b. Ketersediaan sumber daya.

      Sumber daya di sini memaksudkan biaya-biaya. Fasilitas yang meliputi gedung peralatan yang digunakan oleh examiner (penyidik), kebutuhan perangkat keras dan lunak, termasuk upgrade, training, dan skill update.

   c. Pelatihan.

      Pelatihan ditujukan untuk menambah pengetahuan/ skilll dan update. Training sangat penting direcanakan dan dijadwalkan kemudian. Penyediaan 'pendanaan khusus' hendaknya dialokasikan untuk kebutuhan ini.

3. Permintaan layanan.

   Pedoman dibentuk untuk mengalamati permintaan layanan dan berbagai rancangan formulir, pertimbangkan pula berbagai kebijakan.

4. Manajerial kasus.

   Merupakan tindak lanjut dari permintaan akan layanan yang diterima untuk proses lebih lanjut. Perlu ditentukan urgency (prioritas), dan bentuk pemeriksaan seperti apa yang dilakukan. Membuat prioritas harus mempertimbangkan faktor seperti:

a. Tindak kriminal.

b. Tanggal persidangan.

c. Batas waktu.

d. Pertimbangan hukum.

e. Ketersediaan sumber daya.

f. Korban potensial.

g. Volatile/non volatile evidence.

5. Penanganan dan memberlakukan Evidence.

   - Aturan demikian perlu dibuatkan pedomannya. Pedoman yang dibuat nantinya mencakup penerimaan, pemrosesan, dokumentasi, penanganan evidence, dan produk-produk atau alat yang digunakan untuk kebutuhan pemeriksaan. Kriteria penanganan digital evidence mungkin meluas, misalnya jika evidence diidentifikasi sebagai barang selundupan, tentu membutuhkan penanganan yang berbeda.

6. Pemrosesan kasus.

   - Tahap ini melibatkan SOP (Standard Operating Procedures), dan SOP harus mampu mengalamati kebutuhan dasar tahapan pemeriksaan rutin forensik.

7. Mengembangkan prosedur teknikal.

   a. Prosedur menjadi penuntun dalam memeriksa evidence. Untuk itu, prosedur yang dibuat/dikembangkan harus melalui uji kelayakan sebelum nantinya digunakan. Langkah-langkah pengembangan dan menilai kelayakan suatu prosedur adalah sebagai berikut :

i. Identifikasi tugas dan masalah.

ii. Mengajukan solusi.

iii. Pengetesan setiap solusi pada sample (sample dari tumpukan evidence).

iv. Mengevaluasi hasil pengetesan.

v. Menyempurnakan prosedur.

vi. Dalam kasus ini, tentunya bukan evidence asli yang digunakan dalam tahap ini, umumnya yang digunakan hanya berupa sample atau evidence buatan hasil duplikasi.

4.6 Menilai Evidence (Assesment)

Penilaiaan kelayakan terhadap digital evidence dilakukan dengan sepatutnya atas kasus yang melingkupinya dan kemudian menentukan langkah selanjutnya. Prosedur yang dilakukan melibatkan aturan dalam menilai detail kasus, keberadaan hardware dan software, potensial evidence yang teralamati, kondisi dan faktor-faktor lain yang memengaruhi/melingkupi adopsi evidence yang dianalisa.

Beberapa faktor yang menjadi pertimbangan mencakup antara lain:

- Menilai kasus.
- Membuat penalaran di lokasi (*Onsite Consideration*).
- Analisa lokasi pemrosesan.
- Pertimbangan hukum.
- Analisa evidence.
    - Lokasi diketemukannya evidence.

- Stabilitas media yang dilakukan pemeriksaan.
- Menentukan bagaimana evidence didokumentasikan nantinya (misalnya eviden berupa fotografi, image/gambar, sketsa, catatan, dan lainnya).
- Mengevaluasi lokasi media penyimanan (misalnya saja apakah ada inferensi elektromagnetik yang akan memengaruhi integritas data pada media).
- Memastikan kondisi dari evidence, misalnya evidence melalui proses pengemasan, proses pengiriman, dan bagaimana evidence disimpan.
- Analisa kebutuhan cadangan listrik, misal: baterai lithium.

4.7 Akuisisi Evidence

Pada prinsipnya Digital Evidence sangatlah rapuh, karena sifatnya yang mudah rusak (terkait dengan perangkat keras yang menyertainya), karakteristiknya rentan terhadap perubahan (sangat dimungkinkan untuk dimodifikasi, termasuk penambahan, penghapusan), bahkan kerusakan bisa saja terjadi karena kesalahan teknis/human error.

Penanganan yang sangat hati-hati perlu dilakukan, kesalahan dan kegagalan akan menyimpangkan hasil akhir bahkan menghilangkan evidence.

Penting untuk diperhatikan, dibutuhkan proteksi dan penanganan yang seksama akan otentisitas digital evidence, berikut beberapa langkah yang mungkin diambil:

1. Amankan digital evidence sesuai pedoman yang ditetapkan.
2. Mendokumentasi konfigurasi hardware dan software sistem yang digunakan oleh pemeriksa (Examiner).

3. Verifikasi operasi dari sistem komputer pemeriksa mencakup hardware dan software.

4. Men-disassembling komputer untuk keperluan pemeriksaan akses fisik media penyimpanan (jauhkan dari listrik statis dan medan magnet yang akan merusak data di dalamnya).

5. Mengidentifikasi media penyimpanan internal, eksternal, atau bahkan keduanya.

6. Mendokumentasi media penyimpanan internal (misalnya: jumpper setting, model, developer, kapasitas, kemampuan/ kecepatan, interface, dan lainnya).

7. Mendokumentasi konfigurasi hardware (misalnya: Network Interface Card, SoundCard, Graphic Card, MAC [Media Access Control], PCMCIA Card, dan lainnya).

8. Men-diskoneksikan media penyimpanan untuk mencegah terjadinya kerusakan, modifikasi/penambahan data, dan lainnya.

   Catatan: Khusus bagi hard disk, diskoneksi dilakukan dengan melepaskan kabel power dan kabel IDE.

9. Mendapatkan kembali konfigurasi informasi dari sistem *suspect* melalui kontrol boot (mendapatkan informasi dari CMOS BIOS, dengan boot yang dialokasikan dan mengakses Forensik Boot Disk, bukan pada media penyimpanan yang ada).

10. Matikan Power.

11. Pindahkan media penyimpanan yang ada dan instalasikan pada sistem milik examiner. Lakukan konfigurasi agar media penyimpanan dikenali oleh sistem.

12. Tahapan sebelumnya tidak mutlak, ada faktor-faktor lain yang perlu dipertimbangkan kelayakan akuisisi media penyimpanan, misalnya saja jika dihadapkan dengan:
    - Ketersediaan perangkat.
    - Ketergantungan hardware tertentu, bisa saja didapati drive terdahulu tidak dapat dibaca pada sistem yang lebih baru.
    - Sistem drive yang tidak mungkin dipindahkan dan akan banyak kesulitan jika dipisahkan dengan sistem tempat dia diintegrasikan, misalnya pada Laptop.
    - Network Storage.
    - RAID (Redundant Array of Inexpensive Disk).
13. Pertimbangkan kebutuhan write proteksi untuk melindungi original evidence.
14. Mendapatkan evidence subjek pada storgae device si examiner menggunakan berbagai tool hardware dan software (Gambar 4.13 s.d 4.15), misalnya:
    - Forensic Analysis Software.
    - Hardware device spesifik.
15. Menginvestigasi lebih lanjut karakteristik dari storage device (misalnya: tabel partisi dan karakteristik dan ruang -ruang pada storage device, dan lainnya).
16. Verifikasi hasil akuisisi dengan membandingkan hasil pengkopian, misalnya dengan membandingkan bahkan sektor-sektor dengan storage device yang didapat.

Gambar 4.12 Serial ATA hard disk yang akan didiskoneksi dari kotak CPU (Sumber: Wikipedia. Thomas Rosenau. Serial ATA hard disk connected)

Gambar 4.13 Portable tableau forensic write-blocker yang tersambung pada harddisk

Gambar 4.13. Perangkat *Tableau forensic write-blocker* digunakan untuk mengambil evidence tanpa melakukan modifikasi atau menambah

informasi apa pun terhadap data yang dipindai. Hal ini dilakukan sebatas pembacaan data dan menuliskan sebagaimana apa adanya tanpa menciptakan informasi baru, misalnya tidak melakukan modifikasi informasi kepemilikan atau modifikasi informasi penanggalan saat penulisan data.

Gambar 4.14 Pemindaian informasi akses halaman-halaman web menggunakan Xplico – Aplikasi Network Forensik OpenSource (sumber: xplico.org) [1]

Gambar 4.15 Pemindaian informasi akses halaman-halaman web menggunakan Xplico – Aplikasi Network Forensik OpenSource (sumber: xplico.org) [2]

4.8 Pemeriksaan Evidence

Pengujian dilakukan dengan tahapan sebagai berikut:

- Persiapan sebagai langkah awal.
- Ekstraksi.
- Menganalisa data terekstrak.
- Kesimpulan.

Tahap ini sudah dibahas pada bab sebelumnya, dan pada Bab 6 akan diberikan contoh secara nyata dari tahap ini.

4.9 Laporan dan Dokumentasi

Laporan, umumnya berisi catatan dan laporan-laporan yang dilakukan Examinator. Merupakan tanggung jawab Examinator untuk memberikan laporan yang lengkap dan akurat, bahkan langkah-langkah seperti apa yang diambil dalam pemeriksaan evidence harus tercatat dan didokumentasikan.

Berikut beberapa pertimbangan yang mungkin muncul dan umumnya menjadi catatan untuk lain waktu:

- Membawa catatan yang mungkin sewaktu-waktu digunakan ketika berkonsultasi dengan investigator ataupun jaksa penuntut (prosecutor).
- Copy dari dokumentasi *chain of custody*.
- Tanggal , waktu pencatatan, deskipsi, dan tindakan yang diambil.
- Topologi jaringan, nama dari para user, user agreement, password, dan lainnya.

- Dokumentasi perubahan yang dibuat pada sistem dan jaringan komputer atas pengaturan/perintah dari penegak hukum atau Examiner.
- Dokumentasi sistem operasi dan software mencakup pula versinya, patch yang diinstal, dan lainnya.
- Dokumentasi informasi lainnya, seperti remote user access, remote storage.

Laporan mungkin mencakup hal-hal seperti:

- Identitas dari organisasi yang melaporkan.
- Informasi kasus/submission number.
- Identitas dari orang yang melaporkan.
- Waktu diterima.
- Waktu dilaporkan.
- Penjelasan yang deskriptif berkenaan komponen yang diperiksa, mencakup pula serial number, developer, ataupun model.
- Identitas dan tanda tangan dari examiner/pemeriksa.
- Deskripsi singkat langkah-langkah yang diambil misalnya: melakukan pencarian terhadap potongan kata (string), me-recover file yang terhapus, dan lainnya.
- Hasil dan kesimpulan.

Laporan mencakup:

- Rumusan-rumusan penemuan.
- Detail penemuan, detail disajikan secara mendalam, antara lain:

- File spesifik yang diminta, file-file lainnya seperti file yang dihapus yang terelasi dengan penemuan.
- Pencarian 'string' tertentu.
- Pencarian kata-kata kunci.
- Evidence yang mungkin berhubungan dengan internet, misalnya: cache file, chat logs, e-mail , web traffic analysis, dan lainnya.
- Analisa image grafis.
- Meta data, property, dan kepemilikan file.
- Data program registrasi mengacu pada kepemilikan .
- Analisa data.
- Deskripsi dari program yang relevan pada subjek yang dianalisa.
- Teknik-teknik lain yang terelasi, semisal enkripsi, partisi tersembunyi, attribut tersembunyi (hidden attribute), dan lainnya.

- Material pendukung mencakup:
  - Dokumen/Catatan *Chain of Custody*.
  - Copy digital dari evidence.
  - Print out dari evidence, dan lainnya.
- Perbendaharaan kata, digunakan untuk kemudahan pembacanya sewaktu dihadapkan dengan istilah-istilah spesifik keilmuan dan teknis.

4.10 Kasus yang Mengandalkan Komputer Forensik

Berikut ini contoh ringkas pemberlakukan komputer forensik pada penyidikan:

Pornografi dalam Sistem Komputer Perusahaan

Selama pemeriksaan masalah yang dialami sistem perusahaan, Examiner menemukan beberapa sistem yang berisi gambar-gambar yang tergolong pornografi.

Proses Forensik:

Examiner kemudian melakukan pemeriksaan terhadap chace file, slack, dan free space hard disk untuk memastikan user terlibat dalam mengakses gambar-gambar tersebut.

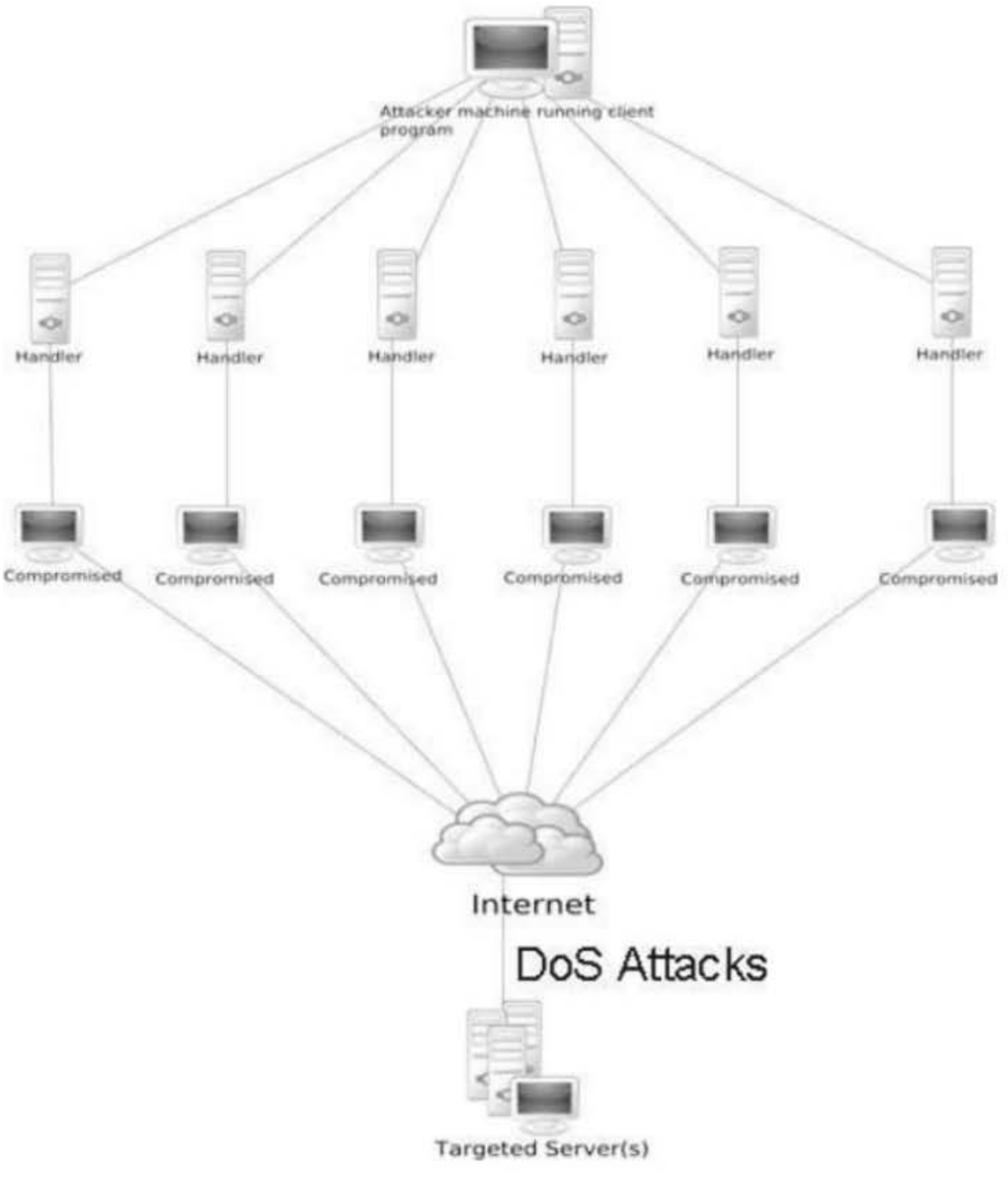
Sabotase layanan - Denial of Services

Berdasarkan temuan forensik, ternyata karyawan perusahaan meng-eksploitasi akses internet Denial of Services, di mana institusi keuangan menderita kerugian finansial yang diakibatkan karena kehilangan layanan dari komputer mainframe dalam jangka waktu lama

Proses Forensik:

Dari analisa forensik, diketahui bahwa: Adanya personal komputer (workstation) salah satu karyawan yang melakukan tindakan ilegal ter-hadap sistem.

Berdasarkan temuan forensik, karyawan yang bersangkutan meng-eksploitasi sistem yang rentan dan kemudian membatasi network auditing untuk melakukan sabotase mainframe.



Gambar 4.16 Diagram serangan DoS terhadap komputer server (Sumber:Wikipedia. NikNaks . DDos Attack. GNU Lesser General Public License)

BAB 5
SKILL INVESTIGASI KOMPUTER FORENSIK

5.1 Menilai Data

Pengetahuan investigasi berpedoman pada proses, dan proses ini yang menjadi acuan langkah kerja. Dengan demikian, seorang examiner dapat mengulang kembali ke proses sebelumnya jika proses yang dilakukannya tidak membuahkan hasil.

Mereka tidak bekerja semata-mata dengan intuisi, justru proses serta prosedur yang akan membatasi seorang examiner untuk tidak memuat asumsi dengan intuisi. Hal ini penting untuk memenuhi standar kelayakan data.

Bab ini akan membahas pengetahuan tentang penanganan data untuk keperluan investigasi komputer forensik.

5.1.1 Data Files

Data dalam komputer dikemas dalam file, maka dari itu disebut sebagai data file atau file saja.

Ada banyak sekali jenis dan ragam file yang mencakup file dokumen, aplikasi, file yang diciptakan dalam waktu sistem berjalan (runtime log file), dan ada banyak media penyimpanan dengan ragam fitur dan kapasitas penyimpanan.

Sebelum digunakan, media penyimpanan harus melalui proses format dan partisi. Partisi adalah tindakan untuk membagi media secara logika. Dan ada istilah logical volume, yang memaksudkan kumpulan partisi yang dipandang sebagai satu entitas dan telah diformat atas dasar system file. File system mendefinisikan bagaimana file diberi nama, disimpan, diakses, dan diorganisasi pada media penyimpanan secara logika.

Berikut pemahaman perihal file sistem:

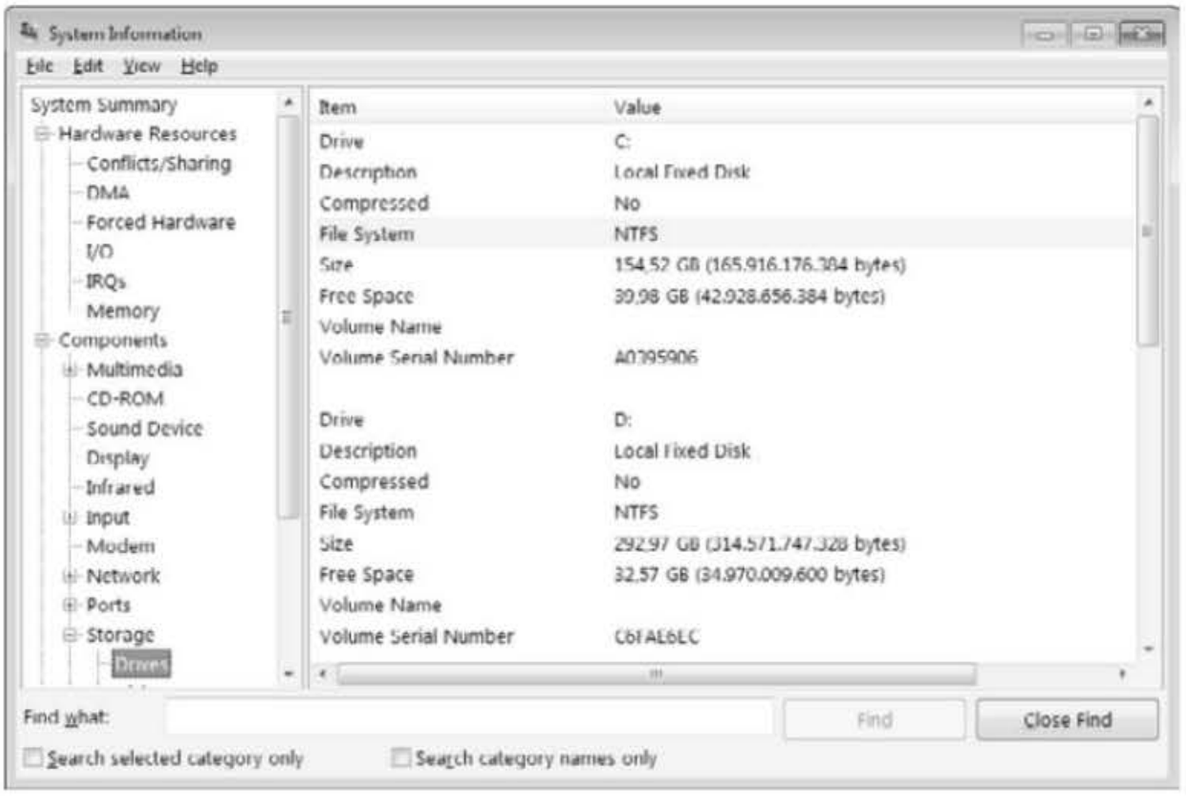
- File sistem menggunakan struktur data untuk mengacu pada lokasi file di media penyimpanan.
- File sistem memengaruhi bagaimana data disimpan, misalnya akan dismpan pada satu atau lebih file allocation units, ini mengacu pada blok dan cluster.
- File allocation unit merupakan kumpulan dari sektor-sektor, yang merupakan unit terkecil pada media penyimpanan dalam kacamata logika.

Berikut macam file system:

- FAT12 (umumnya digunakan pada floppy disk dan FAT volumes yang lebih kecil dari 16 MB).
- FAT16 (pada umumnya sistem operasi MS-DOS, Windows 95/98, Windows NT/2000, Windows XP, Windows Server 2003,

dan beberapa UNIX OSs mendukung FAT16. Digunakan pula pada perangkat multimedia, semisal digital camera. FAT16 menggunakan file allocation table entry 16-bit untuk mengalamati *entry system file.* FAT16 terbatas dengan kapasitas maksimum sampai 2 GB pada MS-DOS dan Windows 95/98).

- FAT32 (sistem operasi Windows 95 Original Equipment Manufacturer, Windows 98, Windows 2000, Windows XP, dan Windows Server 2003 mendukung FAT32, demikian pula dengan banyak perangkat multimedia. FAT32 menggunakan file allocation table 32-bit untuk mengalamati *entri ke file system*, kapasitas maksimum yang didukung sampai 2 Terabytes (TB)).
- NTFS (sistem operasi Windows NT/2000/XP dan Windows Server 2003 mendukung NTFS).
- High Performace File System (HPFS).
- Second Extended Filesystem (ext2fs), umumnya digunakan pada Linux OS.
- Third Extended Filesystem (ext3fs).
- Hierarchical File System (HFS), digunakan pada MAC OS.
- HFS Plus (Mac OS 8.1).
- UNIX File System (UFS).
- Compact Disk File System (CDFS), digunakan pada CD Media.
- International Organization for Standardization (ISO) 9660 The ISO 9660 file sistem yang pada umumnya digunakan bagi CD-ROMs.



Gambar 5.1 Informasi media penyimpanan mencakup informasi file sistem yang digunakan

Lalu bagaimana dengan penghapusan? Data-data yang ada pada media penyimpanan yang kemudian dihapus tidak sepenuhnya hilang begitu saja dari media penyimpanan. Meskipun proses penghapusan sudah dilalui, tetapi penghapusan hanya menandai file-file sebagai file yang terhapus secara logika dan bukan secara fisik, meskipun Anda sudah membersihkan recycle bin sekalipun.

Butuh waktu yang lama agar file sepenuhnya hilang dari media penyimpanan mungkin karena nantinya digunakan untuk menyimpanan file lain. Maka, file-file yang sudah dihapus masih memungkinkan untuk didapatkan kembali.

Salah satunya, program yang mampu mengkontruksi file yang sudah terhapus misalnya iCare, sebuah software data recovery terhadap ragam format data mencakupp image, dokumen, file audio, file arsip, folder atau direktori, bahkan media penyimpanan yang rusak.

Gambar 5.2 Aplikasi iCare

Slack Space dan Free Space

Sedangkan istilah *Slack Space* pada media penyimpanan memaksudkan lokasi yang tidak terpakai, ini ada hubungannya dengan file sistem.

Sedangkan *Free Space* merupakan lokasi penyimpanan yang dapat digunakan kemudian, tetapi tidak serta merta kosong, dimungkinkan ada data didalamnya mungkin karena proses *delete*. Dan masih dimungkinkan data diperoleh dari free space.

Dengan karakteristik media penyimpanan yang demikian, maka perlu penanganan khusus oleh examiner, yang diawali dengan proses pengumpulan (Collecting).

Sewaktu mengumpulkan data, examiner akan bekerja pada banyak data dan media hasil duplikasi, disini fungsinya membuat banyak duplikasi dari storage device termasuk pula datanya.

Mengkopi file dari media penyimpanan, pada umumnya menggunakan dua buah teknik:

- Logical Backup (mengkopi file dan direktori yang secara logika tersimpan pada media penyimpanan, ini tidak mencakup pengkopian file yang dinyatakan dihapus).
- Bit Stream Imaging (copy mencakup pula free space dan slack space).

Informasi lain yang dibutuhkan dan menjelaskan data file sewaktu user berartivitas melibatkan data file antara lain:

- Waktu modifikasi.
- Waktu pengaksesan (mencakup menampilkan (view), mengakses dan mencetak file).
- Waktu pembuatan suatu file.

Memeriksa Data.

Dalam pemeriksaan, dilakukan hanya terhadap *data hasil backup*, bukan data yang sesungguhnya. Dan akses read only akan menjaga konsistensi/ integritas data. Dalam proses ini, write bloker diperlukan dalam mencegah modifikasi terhadap data yang diperiksa.

Mengekstrak Data.

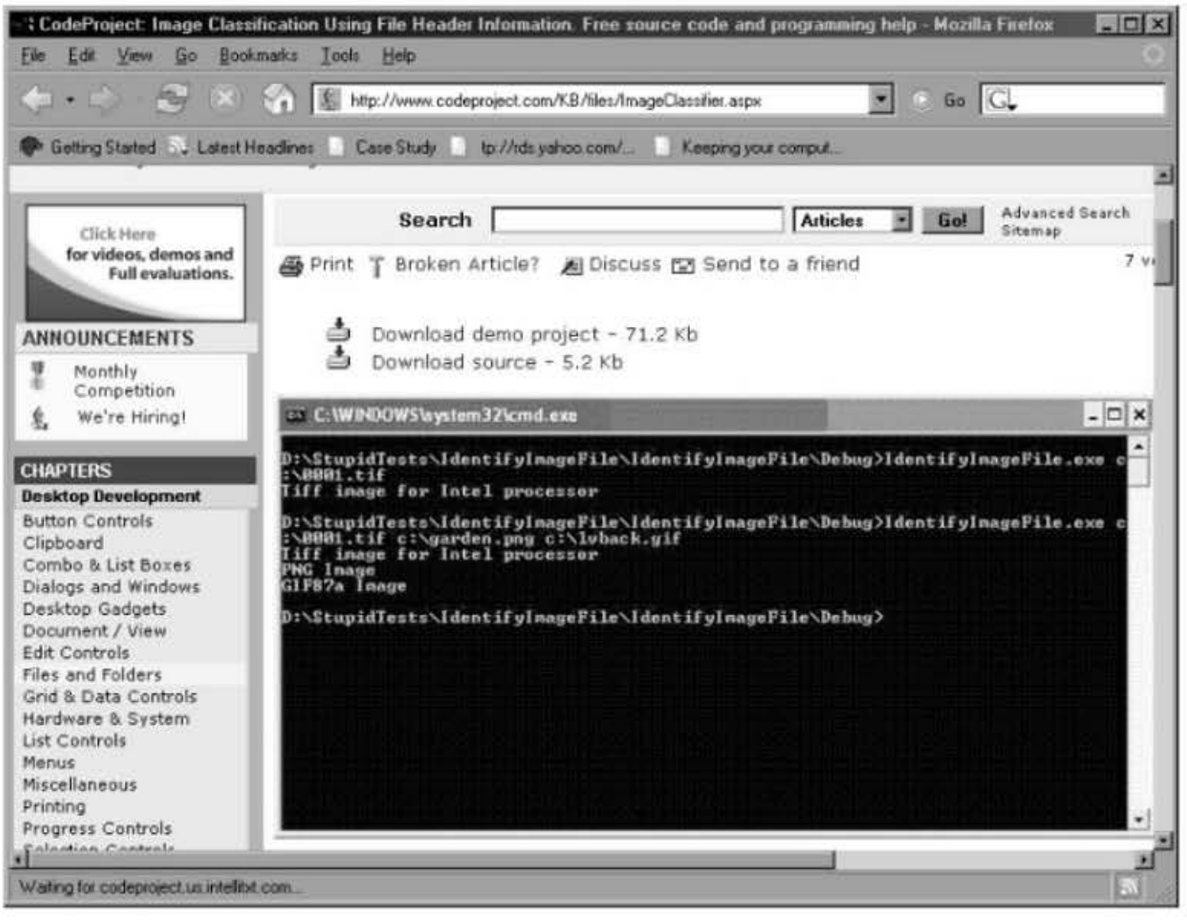
Dalam melakukan ekstraksi data, Anda harus tahu file-file apa saja yang ada di dalamnya (misal: file gambar, laku, dokumen). Untuk mengetahui karakteristik file, dapat kita lihat melalui exrtension file tersebut. Tetapi sayangnya, pengguna dapat saja memanipulasi extension file yang akan memberikan kesulitan tersendiri.

Cara paling jitu untuk mengetahui file tersebut dengan melihat file header information file tersebut.

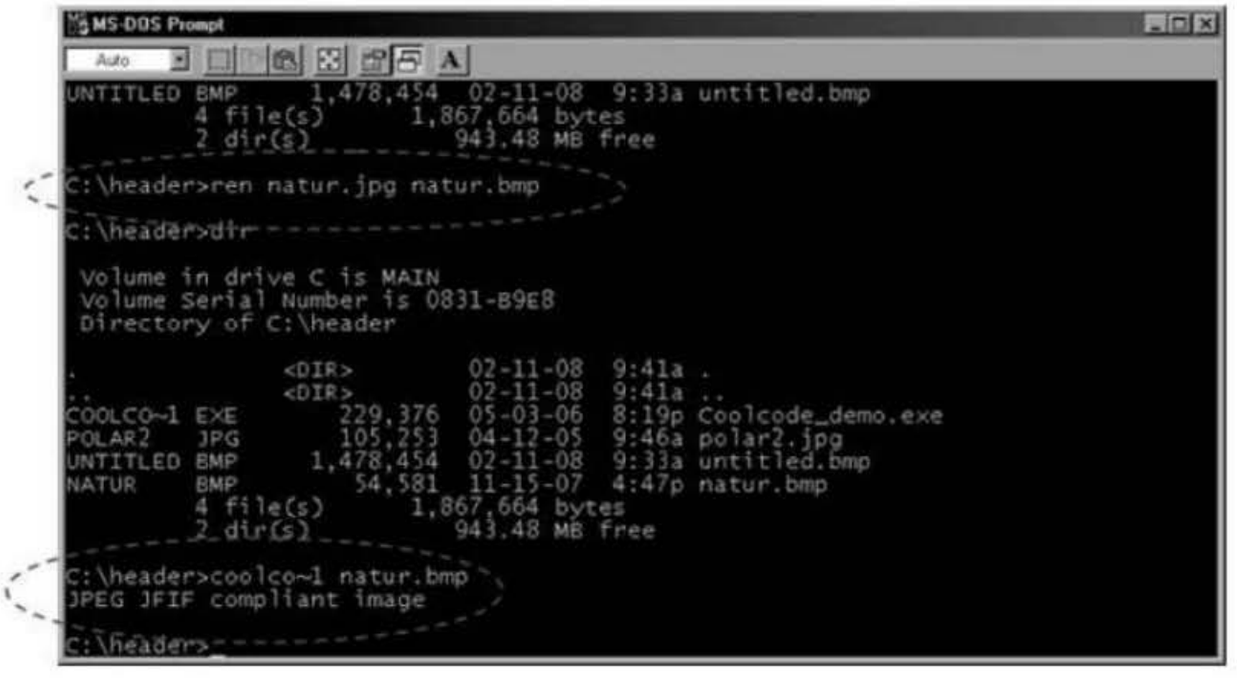
Salah satunya dicontohkan pada Gambar 5.4 menggunakan program Identify Image File. Program ini mampu menganalisa format file dari pembacaan header-nya.

Pada Gambar 5.4, penulis mengubah extension file tersebut yang seharusnya berekstensi *.jpg menjadi *.bmp, tetapi program tersebut tetap mengenali file dengan format *.jpg

Untuk mengeksplorasi lebih dalam bagaimana pembacaan header file, dapat Anda download source code-nya pada website yang tertera pada Gambar 5.3.



Gambar 5.3 CodeProject.com – Download demo project



Gambar 5.4 Program IdentifyImageFile.exe

Menggunakan software forensik, beberapa fungsi umum yang dimunculkan dari software forensik sehubungan penanganan data file, antara lain:

- File viewer.
- File non kompresi (Uncompressing Files).
- Menampilkan Struktur Direktori dalam interface grafis.
- Mengidentifikasi file yang tidak dikenal.
- Melakukan pencarian terhadap string atau pola tertentu.
- Mengakses metadata.

Analisa

Berbagai tool forensik dapat digunakan untuk proses analisa, sebagai pengingat, perhatikan file times dan waktu sistem. Temuan-temuan akan muncul sehubungan tahap ini, yakni: kapan kejadian terjadi, kapan waktu file dibuat atau dimodifikasi, serta kapan e-mail dikirimkan.

Tool-tool forensik yang melibatkan analisa mendalam akan memberikan kepada Anda gambar global dari serangkaian kejadian.

Tips:

Penting diketahui. Examinator bekerja menggunakan data-data duplikasi, dan bukan data sebenarnya yang menjadi evidence. Sehingga, kerusakan fisik atau perubahan terhadap data tidak akan menghilangkan evidence yang sebenarnya.

5.1.2 Data Sistem Operasi dan Data Software Aplikasi

Dalam memandang data Sistem Operasi, umumnya kita golongkan ke dalam dua bagian, yaitu data volatile dan non volatile.

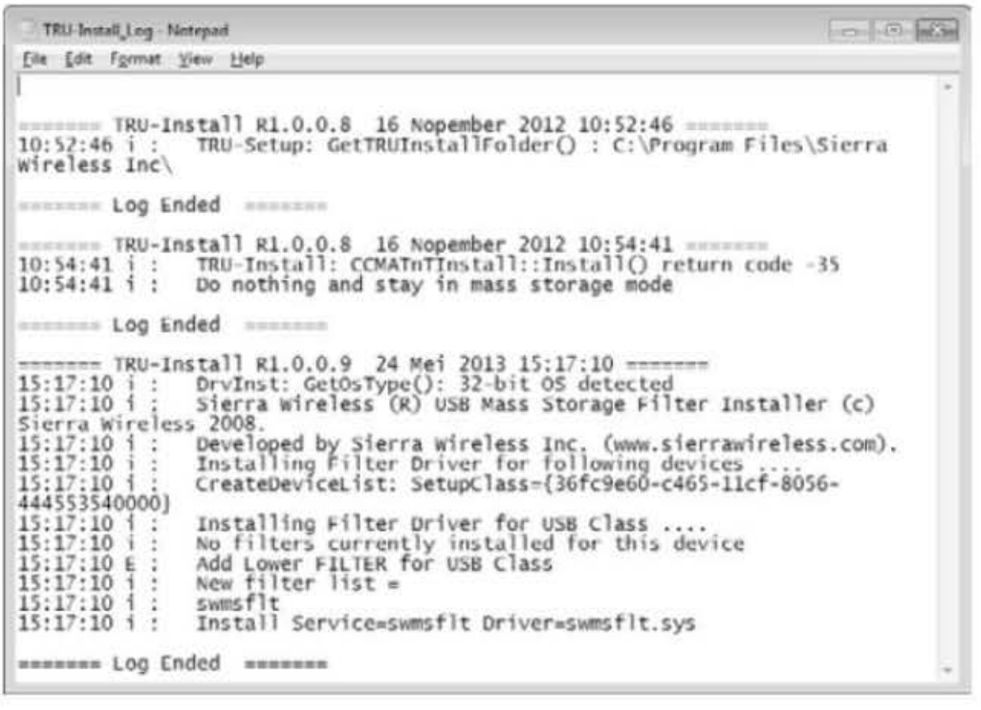
Yang tergolong dalam data non volatile yaitu:

- File konfigurasi (Digunakan dalam menyimpan informasi berkenaan setting sistem operasi dan program aplikasi, misalnya: resolusi layar, printer setting, connection setting, dan lainnya).
    - User dan Grup (Sistem operasi menyimpan catatan/ informasi berkenaan user account dan group account termasuk atribut penduduk lain, semisal karakteristik/ atribut dari user account).
    - File Password.
    - Schedule task (Informasi ini menjadi bagian dari konfigurasi sistem operasi dan akan ada beberapa aksi dijalankan berdasakan penjadwalan kerja, misalnya menjalankan program antivirus sebulan sekali).
- Log File (Log ini berisi aktivitas dari sistem operasi, bahkan menyimpan pula aktivitas spesifik dari program aplikasi, metode penyimpanannya beragam, mungkin disimpan pada: file teks atau database dan pada beberapa kasus bisa saja aktivitas disimpan pada log file yang berbeda).

- System Event (Merupakan kegiatan operasional sistem operasi, misalnya sewaktu sistem start-up atau proses shutdown. Kegagalan atau keberhasilan aktivitas yang dilakukan ini akan dicatat).
- Audit Record (Berisi serangkaian informasi yang berhubungan dengan sekuritas, misalnya saja keberhasilan dan kegagalan proses autentikasi).
- Application Events (Serangkaian kegiatan yang dilakukan oleh program aplikasi sewaktu aplikasi dijalankan, kemudian ditutup, atau bahkan kegagalan aplikasi).
- Command History (Umumnya ada log file lain terpisah untuk merncatat aktivitas ini, semisal perintah-perintah sistem operasi yang di-request oleh user).
- Recently Accesed File (Sistem operasi mungkin mencatat pula file-file dan program aplikasi yang diakses baru-baru ini).

- Application File (Program aplikasi terdiri dari banyak file yang terintgrasi, seperti file executable, file berisi skrip pemrograman, log file, file konfigurasi, grafik, audio, icon [format: *.ico]).
- Data file (Digunakan untuk menyimpan informasi dari program aplikasi, ada banyak macam, file ini umumnya dikenal oleh pengguna dan sering digunakan untuk menyimpan pekerjaan pengguna komputer).
- Swap file (Swap file digunakan untuk memperluas kemampuan memori komputer, tentunya akan dianggap sebagai memori yang temporer).
- Dump file (File yang menyimpan isi dari memori komputer).

- Hibernation Files (File yang diciptakan untuk menjelaskan sistem saat ini dan akan di restore saat sistem *turn on*).
- Temporary file (File ini diciptakan saat instalasi sistem operasi, instalasi program aplikasi, proses peng-update-an, dan bahakan diciptakan seraya program aplikasi berjalan, umumnya file tersebut dihapus segera setelah software aplikasi ditutup, meskipun demikian bisa saja karena lain kasus file tersebut masih tersimpan).



Gambar 5.5 Log file dari program aplikasi modem USB

Lebih lanjut perihal format file dapat dilihat pada bab terakhir, daftar format file dan jenis file.

Data Volatile

Yang termasuk dalam data volatile yaitu:

- Slack space.
- Free space.
- Network configuration.

- Network connection.
- Running process.
- Open files.
- Login session.
- Operating system time.

Dari karakterisik data sistem operasi, tentunya dibedakan dalam mengumpulkan data volatile dan non volatile.

Jenis data Volatile OS:

- Content of memory.
- Network configuration.
- Network connection.
- Running process.
- Open file.
- Login session.
- Operating system time.

Ternyata, tidak hanya melulu mengandalkan software forensik dalam prosesnya, beberapa aplikasi lain dapat digunakan, kita golongkan aplikasi ini ke dalam kategori software umum, misalnya:

- Os command prompt.
- Sha - 1 checksum.
- Directory list.
- String search.
- Text editor.

Prioritas dalam mengumpulkan data harus dicermati dengan baik, data yang lebih rapuh dan berpeluang hilang dan juga data harus mendapatkan penanganan segera.

Berikut daftar data-data berdasarkan prioritas:

1. Network connections.
2. Login sessions.
3. Contents of memory.
4. Running processes.
5. Open files.
6. Network configuration.
7. Operating system time.

Mengumpulkan data non volatile, umumnya dapat diberlakukan tahapan sebagai berikut:

- Melakukan shutdown sistem operasi.
- Remove power dari the system.

Kemampuan tool atau utilitas pada sistem operasi mampu meng-organisasi dan menyimpan informasi berharga yang sangat berguna untuk keperluan investigasi:

- Users and group.
- Password.
- Network share.
- Log.

Dalam prosesnya, analisa terhadap sistem operasi mungkin melibatkan perangkat spesifik lainnya.

Selain dari berbagai tool/utility yang secara langsung dapat mengakses dan menampilkan data/informasi, mungkin dibutuhkan tool-tool lainnya untuk menggali informasi, misalnya saja Hex Editor yang digunakan pada Swap File dan RAM Dumps.

Tips dan masalah yang muncul dalam mengumpulkan data:

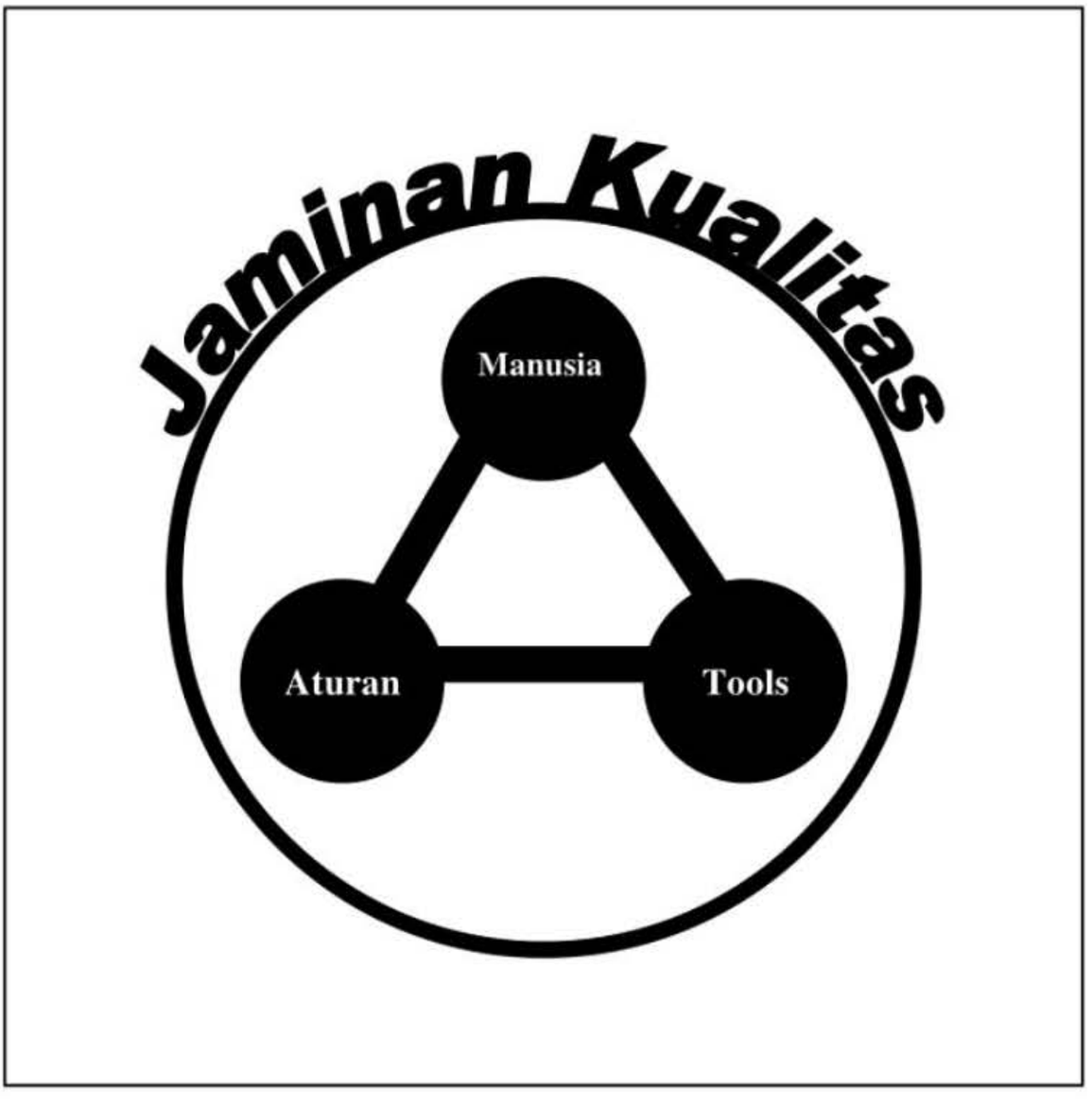
- OS Access. Bisa saja user munggunakan password screen saver yang menghalangi examiner untuk mengumpulakn data, terlebih lagi jika hendak mengumpulkan data-data volatile. Akan sangat mudah untuk mem-*baypass* proteksi password screensaver, cukup dengan me-restart, tetapi dengan demikian informasi data-data volatile akan hilang. Lalu apa yang harus disiasati? Dibutuhkan utility lain untuk meng-crack screensaver password tanpa harus melakukan reboot sistem.

- Log Modification. Pengguna komputer bisa saja men-disable program pencatatan aktivitas/log, tetapi dengan sentralisasi server, hal ini dapat diminimalisasi.

- Hard Drive dengan Flash Memory. Bisa saja password diterapkan pada Flash Memory Drive demikian, tentunya aksi password crack dilakukan untuk mengatasi masalah ini.

- Key Remmaping. Kombinasi individual berkenaan tombol-tombol keyboard dapat menjadi permasalahan dalam forensik, misalnya kombinasi tombol membuat komputer restart atau shutdown dan bahkan memformat hard disk. Cara terbaik adaah tidak menggunakan keyboard tersebut, mungkin cukup dengan menggunakan komputer lain yang dihubungkan melalui crossover kabel jaringan.

Kompleksitas penilaian data akan bertambah sewaktu melibatkan data aplikasi, data jaringan komputer, dan berbagai sumber lainnya dengan banyak lapisan dengan interface perangkat keras dan aplikasi.



Gambar 5.6 Konsep kelayakan forensik

5.2 Pemahaman yang Berkeahlian

Berikut ini poin penting yang menyangkut tindakan komputer forensik dan pola pikir ahli komputer forensik:

- Bukan efisiensi, tetapi efektivitas adalah nomor satu!
- Organisasi harus memerhatikan kompleksitas teknis yang logis dari analisis forensik.

- Organisasi/perusahaan harus mampu dalam menangani, bukan hanya semata-mata komputer forensik, tetapi mencakup pula network forensik
- Organisasi harus mampu menentukan siapa saja petugas yang menangani pekerjaan penyidikan, termasuk aspek forensiknya
- Examiner harus memiliki pengetahuan teknis yang memadai.
- Tim forensik harus memiliki kemampuan forensik yang kuat.
- Anggota tim harus berpartisipasi dalam proses forensik.
- Pertimbangan forensik harus melibatkan pula berbagai kebijakan.
- Organisasi harus membuat dan mengelola pedoman/prosedur untuk aktivitas forensik.
- Examiner harus memiliki *forensic toolkit* yang digunakan dalam pengumpulan data, pemeriksaan, dan analisa.
- Organisasi/perusahaan harus menyediakan sarana dan prasarana penyimpanan yang mencakup log dari aktivitas jaringan.
- Organisasi harus mampu menangani forensik secara konsisten.
- Organisasi secara proaktif mengumpulakan data-data yang berguna, bahkan untuk keperluan forensik sewaktu-waktu.
- Examiner harus memerhatikan bermacam sumber data dengan bermacam file format.
- Examiner harus mempertimbangkan semua data yang melibatkan aplikasi yang digunakan.
- Pengumpulan data hendaknya mengikuti proses yang sudah distandarisasi oleh organisasi/perusahaan.

- Examiner harus menangani data volatile sistem operasi, kerapuhan akan selalu menjadi ancaman, dan dalam kasus tertentu metoda tidaklah kaku dan selalu dapat diandalkan.
- Examiner menggunakan *forensic toolkit* yang tepat untuk mengumpulkan data volatile dari sistem operasi.
- Examiner harus menjalankan metode untuk mematikan sistem (shutdown) dengan tepat.
- Lakukanlah verifikasi integitas data.
- Pemeriksaan dilakukan hanya pada data hasil duplikasi dan bukan data sebenarnya.
- Examiner harus memerhatikan ketelitian dan keakuratan nilai dari data.
- Dalam analisa data, examiner mengandalkan pengenal berupa file header information, bukan sekedar file extension yang dapat dengan mudah diubah/dimanipulasi.
- Fokus terhadap karaktersitik dan berbagai perlakuan yang akan memengaruhi hasil forensik.
- Gunakan metodologi dalam mempelajari data dan bukan intuisi.
- Organisasi/perusahaan harus memahami bahwa hal teknis dan kompleksitas logis dapat muncul seiring dengan proses analisa.
- Examiner mampu menyajikan data dari berbagai sumber.
- Examiner harus meninjau ulang proses dan pengerjaan yang sudah dilakukan.
- Examiner harus mampu mengumpulan data apliasi dari macam sumber, hal ini ditujukan untuk keperluan akan rekonstruksi dan langkah dalam menjelaskan detail kasus komputer forensik.

5.3 Konsep Investigasi

Hanya sekedar memahami komputer, bagaimana data dan file komputer ditangani dan dikeloala tidaklah cukup. Mengerti hardware, software mencakup sistem operasi, dan berbagai aplikasi itupun belum cukup.

Pengalaman dalam menangani kasus membuat seorang examiner semakin matang. Tindak kriminal dengan segala macam aktivitas yang dilakukan tidak sebegitu mudahnya dipecahkan hanya berdasarkan pengalaman menggunakan komputer yang baik, di samping itu examiner harus berurusan dengan evidence yang tergolong rentan hilang/rusak.

Kerapuhan sangat dimungkinkan terjadi karena faktor antara lain:

- Pemakai melakukan perubahan terhadap evidence.
- Evidence sangat mudahnya dirusak ataupun dimodifikasi.
- Kesalahan dalam menanangani data dan media penyimpanan akan sangat berpengaruh terdapat data yang menjadi evidence.

Penalaran: Penanganan yang seksama dibutuhkan, banyak pertimbangan lain yang terlibat sewaktu kasus melibatkan lingkungan yang lebih luas, misalnya internet. Waktu, tanggal, dan wilayah waktu akan menjadi sangat diperhitungkan dan penting! Bukan itu saja, waktu server dan waktu komputer mungkin tidak akurat, itupun perlu dipertimbangkan.

Aksi kriminal pun semakin rapih dan terorganisasi, mungkin sudah direncanakan dengan sedemikian rupa. Banyak aktivitas yang dilakukan untuk menutupi aksi kriminal di samping memang tidaklah mudah menguak kejahatan, examiner harus jeli mengalamati aktivitas dan perilaku, misalnya saja yang dilakukan (dalam ruang lingkup internet) sebagai berikut:

- Berbagi informasi dan bertransaksi (melibatkakan dokumen, pornografi, perangkat lunak, dan lainnya).

- Memalsukan identitas.
- Menggunakan identitas lain.
- Sewaktu mendistribusikan informasi atau mendistribusikan informasi yang salah.
- Alokasi data pada workstation, server, atau organisasi lain.
- Bagaimana seandainya tindak kriminal melibatkan pula jalinan komunikasi. (teleconference, meeting, dan lainnya).
- Catatan pada Internet Service Provider.

Contohnya sewaktu investigasi melibatkan e-mail, apa-apa saja yang penting untuk dipertimbangkan, kita lihat deskripsi berikut.

Tentunya, bagaimana e-mail bekerja sudah menjadi pengetahuan yang harus dimiliki oleh examiner, salah satu yang tentunya tidak akan dilupakan adalah e-mail header.

Pesan e-mail mungkin dirutekan melalui satu atau lebih mail server dan setiap server menambahkan informasi pada mail header. Examiner dapat mengidentifikasi alamat ISP (Internet Service Provider) yang ada ada pada header dan menggunakan informasi tersebut untuk menentukan pengirim dari e-mail tersebut.

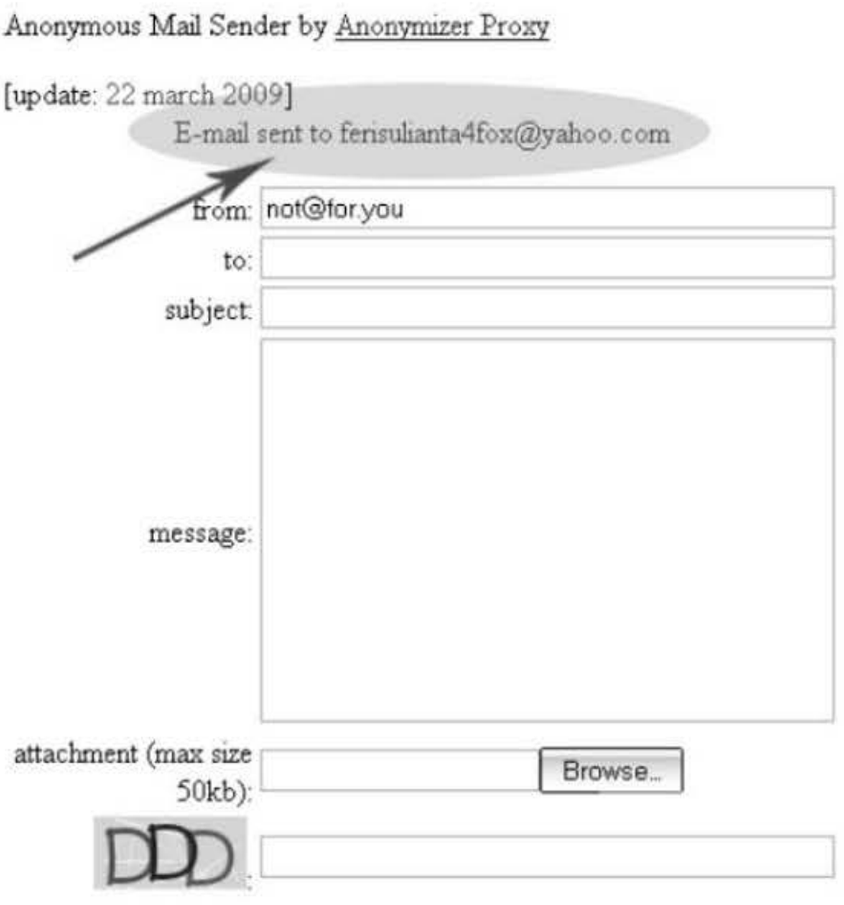
Examiner harus menggali inforamasi demi informasi, misalnya sewaktu dihadapkan pada e-mail tadi, tentunya si examiner tidak hanya memerhatikan attachment, atau body e-mail, meskipun konten e-mail tertumpu di sana, lebih jauh lagi header memunculkan banyak jejak yang dapat diungkap kemudian.

Bagaimana membaca dan menangani e-mail header tidaklah cukup, faktor-faktor yang menyimpangkan informasi bisa saja terjadi/dilakukan bahkan oleh orang yang membuat evidence akan menjadi tidak lagi berarti, misalnya:

- Spooofed e-mail header (Received pada e-mail header bisa saja palsu).
- Menggunakan akun anomim (anonymizer).
- Remote location (layanan internet/e-mail tersebar ditempat umum, tentunya akan sangat sulit menemukan pengirim yang sebenarnya).
- Lokasi e-mail.
- Pengiriman yang tertunda.

Berikut dicontohkan cuplikan dari mail spoofing pada Gambar 5.7 s.d. 5.10.

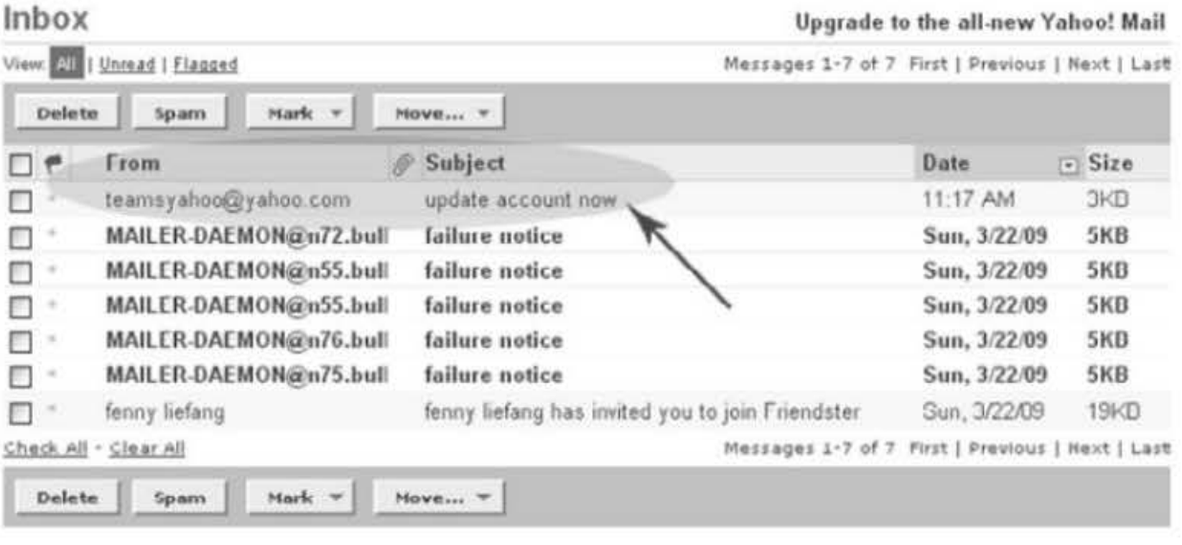
Gambar 5.7 Membuat mail jebakan untuk kebutuhan Spoofing



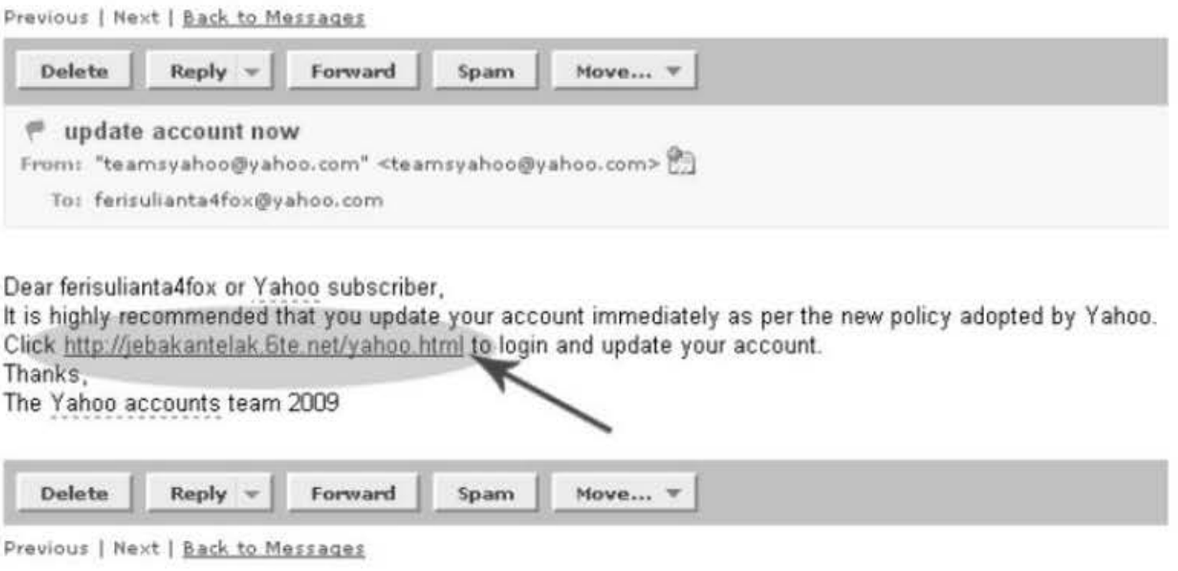
Gambar 5.8 E-mail jebakan terkirim

Si calon korban akan mendapatkan e-mail yang tampaknya sangat meyakinkan (dari: teamsyahoo@yahoo.com) pada inbox-nya.

(Gambar 5.9), dan isi mail tersebut dapat dilihat pada Gambar 5.10.



Gambar 5.9 E-mail jebakan diterima



Gambar 5.10 Isi dari E-mail jebakan

Examiner/Investigator mungkin membutuhkan informasi lain lagi, informasi yang dibutuhkan dan melibatkan banyak pihak termasuk masalah hukum. Maka dari itu, seseorang yang sudah terlatih barulah layak untuk melakukan komputer forensik yang sesungguhnya.

Informasi lain yang dibutuhkan misalnya saja:

- E-mail lain yang berhubungan dengan investigasi.
- Alamat e-mail lainnya.
- Log aplikasi yang akan memerlihatkan aksi spoofing.
- Informasi si pengirim.
- Isi dari komunikasi.
- IP Address.
- Password.
- File yang disertakan pada e-mail atau pesan (Attachment).
- Waktu.

Dalam tindakannya akan banyak didapati proses yang kemudian bersinggungan dengan peraturan dan kebijakan lainnya, misalnya ECPA (Electronic Communications Privacy Act) yang membatasi akses pemerintah akan evidence yang ada pada ISP.

Yang lain lagi, misalnya jika melibatkan Message Board (semisal Yahoo Groups). Ada beberapa pernyataan yang membutuhkan pertimbangan dan tindakan lebih lanjut dari examiner untuk menggali informasi sehubungan evidence, misalnya:

- Apa nama dari message board?
- Apa URL-nya?
- Message Board Host.
- Apakah dibutuhkan otoritas dalam keanggotaan?
- Apakah didapati password dan user ID?
- Apakah ada moderatornya?
- Apakah examiner dapat melakukan akses terhadapnya?
- Apakah guest account tersedia?
- Apa nama user si tersangka?
- Manajemen software seperti apa yang digunakan?
- Apakah arsip file tersedia? Jika ya, siapa yang mengkopi dan adakah partisipan lain yang berperan dalam file arsipan tersebut?
- Apakah waktu dan tanggal benar (sehubungan dengan hosting server)?
- Siapa anggota lain yang ada?

- Bagaimana pendakwa/penuntut/korban menemukan message board?
- Berapa lama si penuntut ini menggunakan message board?
- Apakah ada informasi lainnya yang didapat dari tersangka?
- Apakah si penuntut menggunakan sarana lain untuk berhubungan dengan tersangka?

Lain-lain mungkin ditambahkan sewaktu penemuan demi penemuan muncul ke permukaan.

Demikian skill investigasi ternyata kompleks, bukan hanya metoda/prosedur, tetapi pemahaman yang menyeluruh dan kematangan sangatlah penting!

BAB 6
MEMULAI BEDAH KOMPUTER FORENSIK

6.1 Mulai dari Hal Sederhana

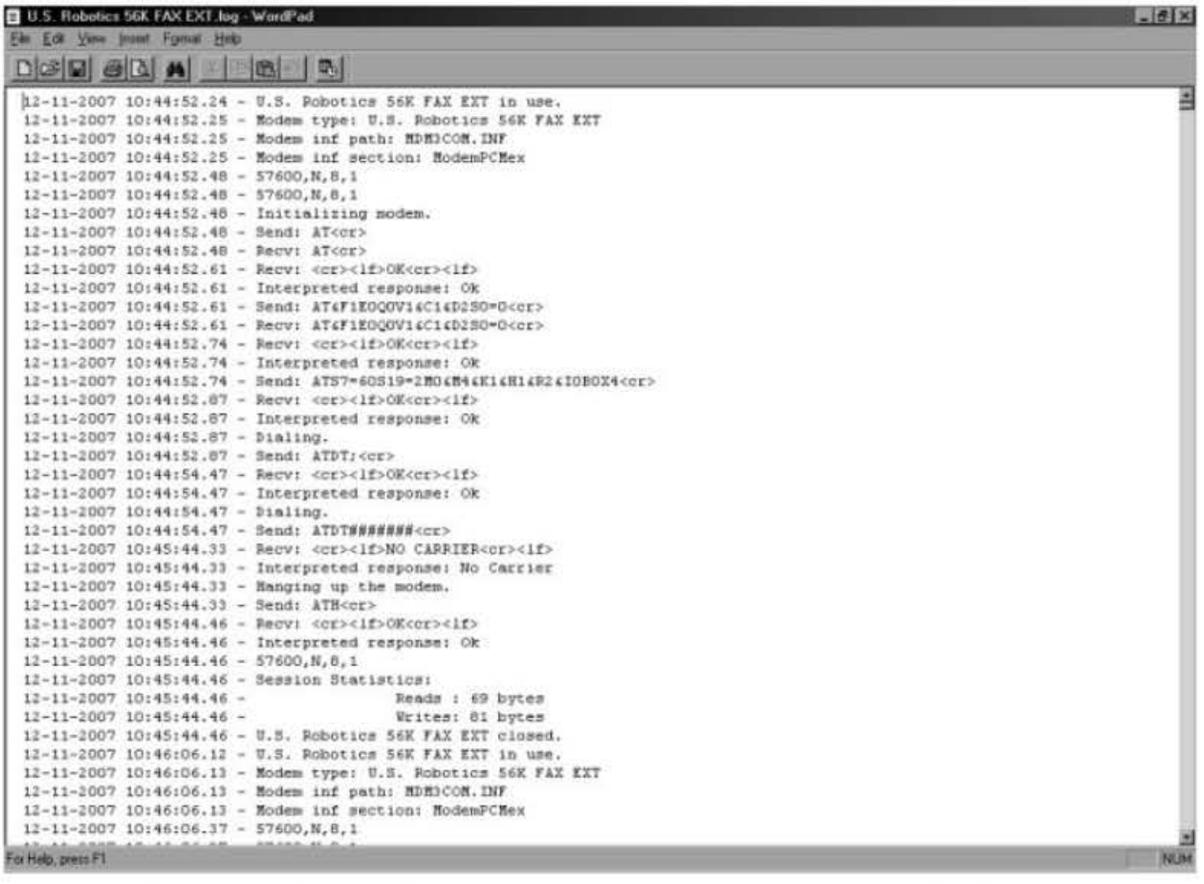
Memantau aktivitas sistem akan sangat menarik, terlebih lagi jika Anda mencurigai gerak-gerik seseorang yang mungkin memakai komputer yang sama dengan Anda. Anda dapat memulainya untuk menelusuri kejelian Anda dalam memonitoring secara tidak langsung. Maksudnya dengan memeriksa jejak-jejak apa saja yang tertinggal dari perilaku seseorang sewaktu beraktivitas dengan komputer.

Semakin Anda menelusuri dan mulai menemukan berbagai keanehan, misalnya saja beberapa website terlarang yang diakses, atau history dari file-file miring yang diunduh, bahkan pesan e-mail yang masih tersimpan dalam *temporary internet file*, pasti bisa membangkitkan rasa ingin tahu.

Dalam hal ini, penulis tidak mengajarkan atau mendukung tindakan demikian, Anda dapat mencobanya dari komputer Anda terhadap aktivitas Anda dan jejak-jejak yang Anda tinggalkan.

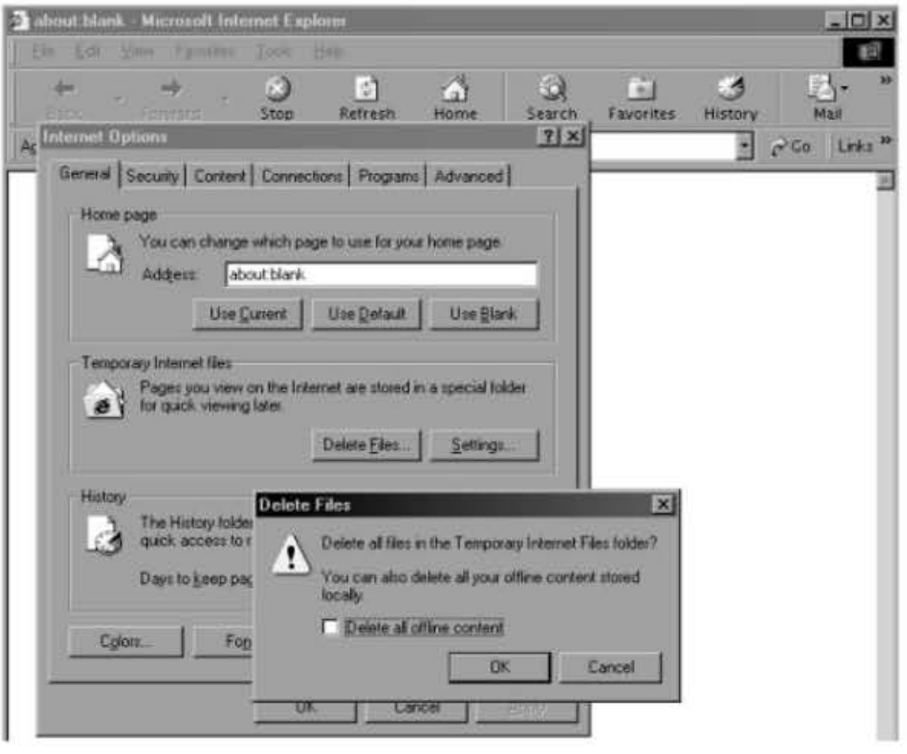
Perhatikan pada Gambar 6.1 ternyata aktivitas penggunaan modem dibuat pengaturannya dan transaksi yang terjadi terdokumentasi dan tersimpan dalam log file (Gambar 6.2).

Gambar 6.1 Mekanisme pengaturan koneksi modem

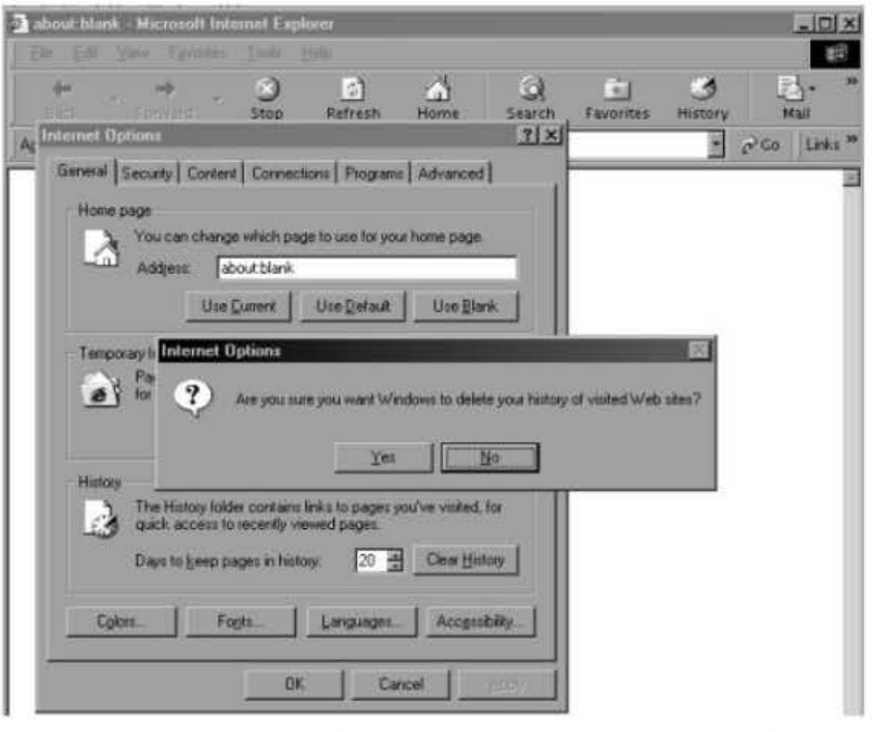


Gambar 6.2 Aktivitas penggunaan modem pada file log

Sewaktu mengakses internet, file-file temporer disimpan sementara pada komputer, dari sana tetunya akan terlihat aktivitas dan perilkau seseorang dalam berkomputer, seperti website apa saja yang diakses, dan lainnya. Perhatikan Gambar 6.3 dan Gambar 6.4.



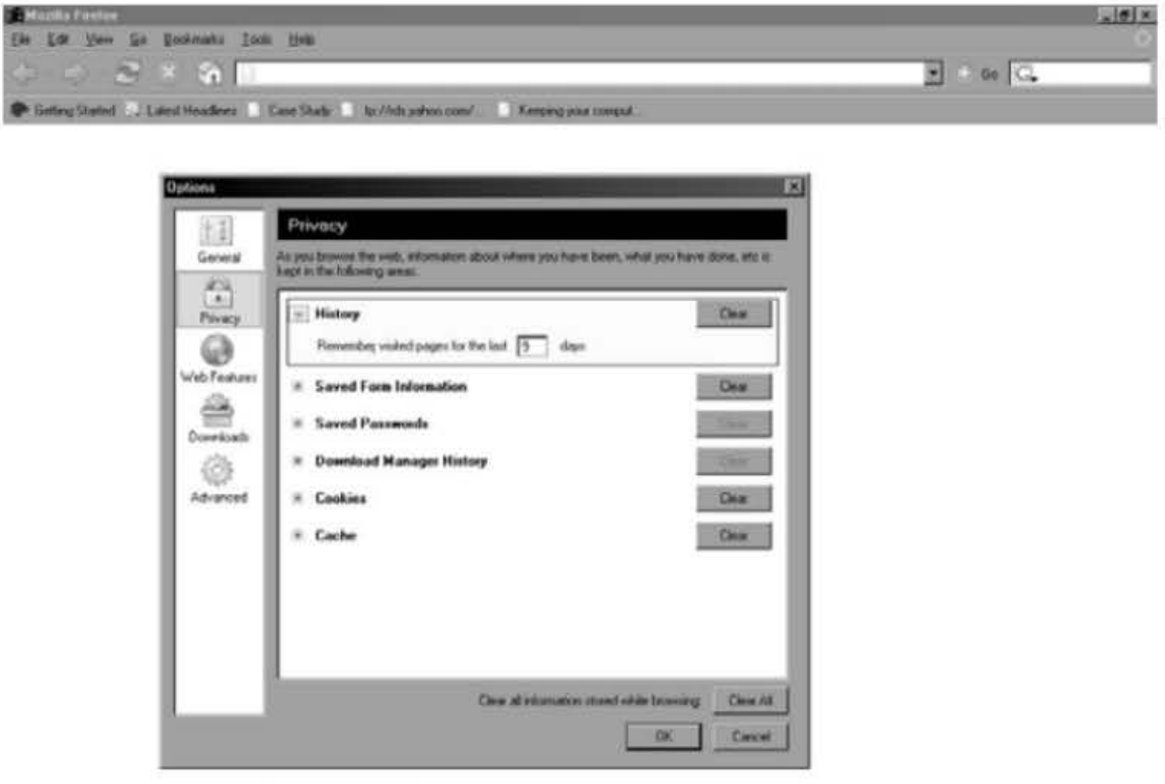
Gambar 6.3 Menghapus temporary internet files



Gambar 6.4 Menghapus history perihal website yang pernah dikunjungi

Mungkin pengguna komputer tidak menggunakan program Internet Explorer untuk mengakses internet, misalnya saja dengan menggunakan Mozilla FireFox, Netscape, Opera, dan lain sebagainya.

Dan informasi beraktivitas ini didokumentasikan secara tidak langsung. Manajerial informasi tersebut disimpan, ini dapat Anda lihat pada Gambar 6.5 yang menampilkan Mozilla sebagai web browser.



Gambar 6.5 Privasi Informasi – Mozilla

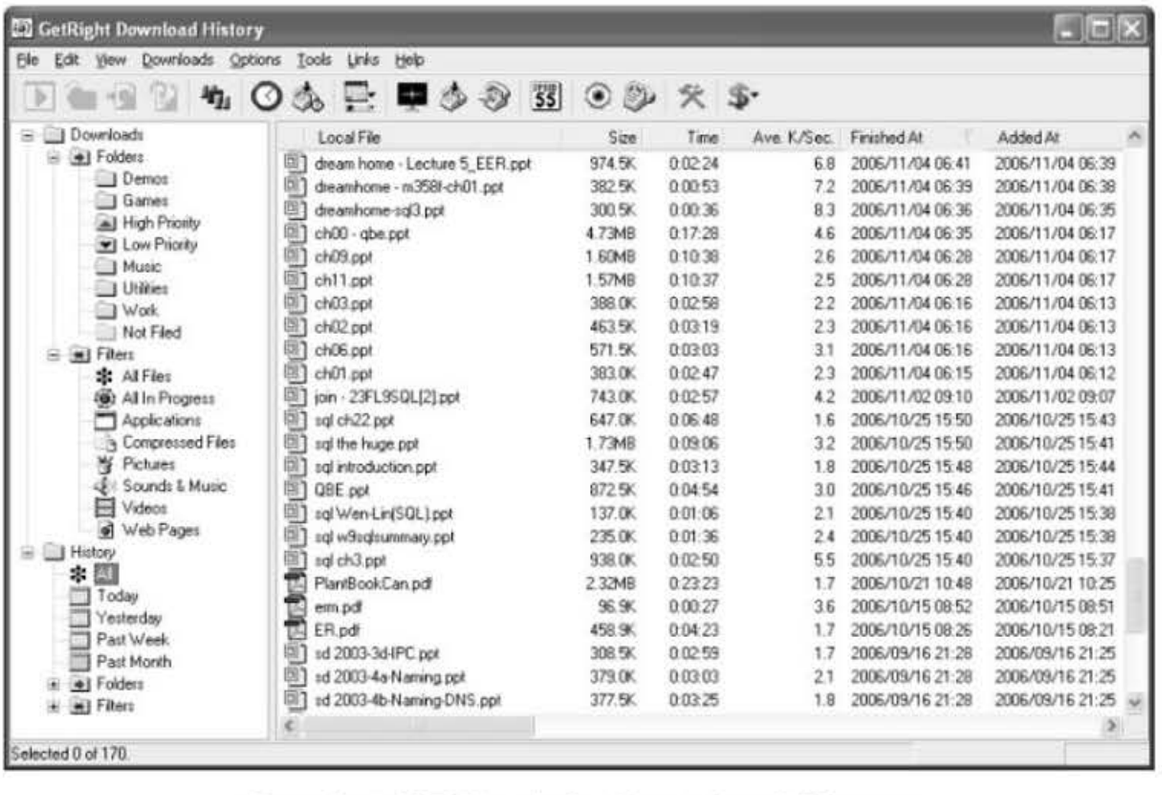
Tentu Anda pernah menghapus file dan bahkan membersihkan keranjang sampah (recyle bin), tetapi hati-hati, file tersebut tidak sepenuhnya hilang dalam hard disk, masih dimungkinkan untuk mendapatkan kembali informasi seperti itu meskipun recycle bin dalam keadaan bersih dari file-file yang sudah tidak lagi dibutuhkan.

Tidak harus menggunakan software forensik spesifik untuk mendapatkan informasi yang sudah terhapus, program utility yang dibuat symantec misalnya, mampu mendapatkan kembali file yang sudah terhapus karena data-data tersebut sebenarnya masih ada pada hard disk (file hanya ditandai sudah dihapus).

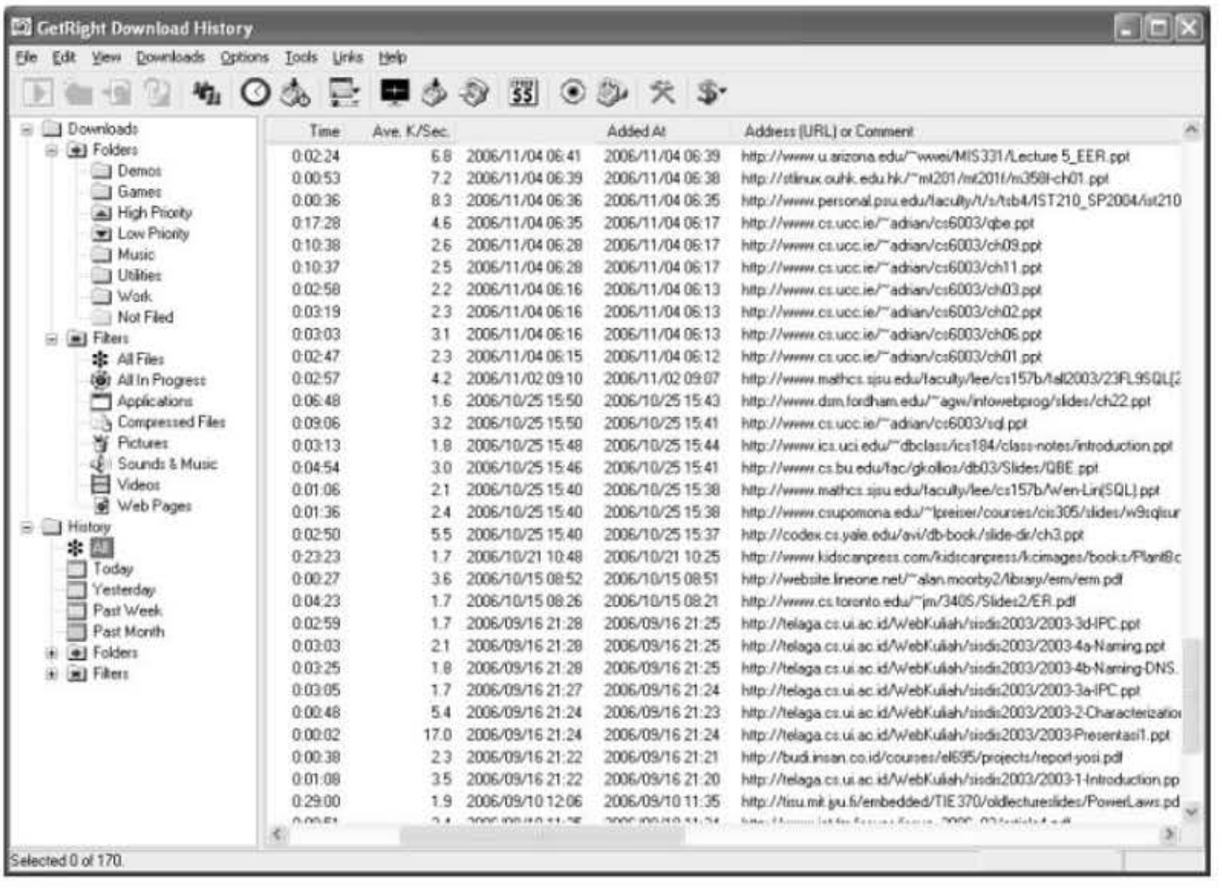
Gambar 6.6 File pada Recycle Bin

Anda juga mungkin sering men-download program dari internet, seperti file gambar, lagu, movie. Bukankah lebih nyaman jika menggunakan software khusus untuk men-download-nya?

Software demikian dapat mendokumentasikan secara rapih aktivitas Anda di dalamnya, coba perhatikan salah satu software download semisal Getright, pada Gambar 6.7 s.d. 6.8, url download pun akan tercatat, memudahkan Anda untuk redownload dan memudahkan pula bagi examiner untuk menelusuri aktivitas Anda!



Gambar 6.7 Getright Download History



Gambar 6.8 Getright Download History - URL

Hal sederhana lain yang dapat dijadikan parameter, misalnya data berkenaan dengan recently file used, file-file apa saja yang diakses terakhir kali yang menunjukan aktivitas Anda dalam menggunakan file dan program yang didokumentasikan. (Gambar 6.9).

6.2 Windows Registry

Sewaktu Anda mengakses registry windows dalam proses forensik, Anda sebenarnya sedang melakukan pembedahan komputer forensik.

Jika sistem operasi Windows yang Anda gunakan, penting memahami struktur windows registry, perilaku aplikasi, proses dari sistem operasi komponen lain yang terlibat seperti data, dan ragam aktifitas pengguna yang melibatkan perangkat keras dan perangkat lunak.

Pembongkaran registry akan terasa menarik dan menggelitik, menuntun Anda untuk melakuan pembedahan dan menelusuri area yang terelasi. Seraya itu, informasi sedikit demi sedikit memberikan titik terang.

Sebelum lebih jauh mengulas informasi yang ada pada registry, kita lihat pengertian yang mendasar dari registry itu sendiri.

Registry merupakan konfigurasi sistem yang substansial dan merupakan *single logical data store*, pada dasarnya dibagi ke dalam tiga database yang terpisah yang dialokasikan untuk menangani:

- User.
- Sistem.
- Pengaturan dan kebijakan pada jaringan komputer (network policies).

Berdasarkan apa yang dikatakan *The Microsoft Computer Dictionary, Fifth Edition*, registry adalah pusat database hirarkikal yang digunakan pada Microsoft Windows 9x, Windows CE, Windows NT, dan Windows 2000 untuk menyimpan informasi penting dalam mengonfigurasi sistem yang melibatkan user, aplikasi/software, dan hardware.

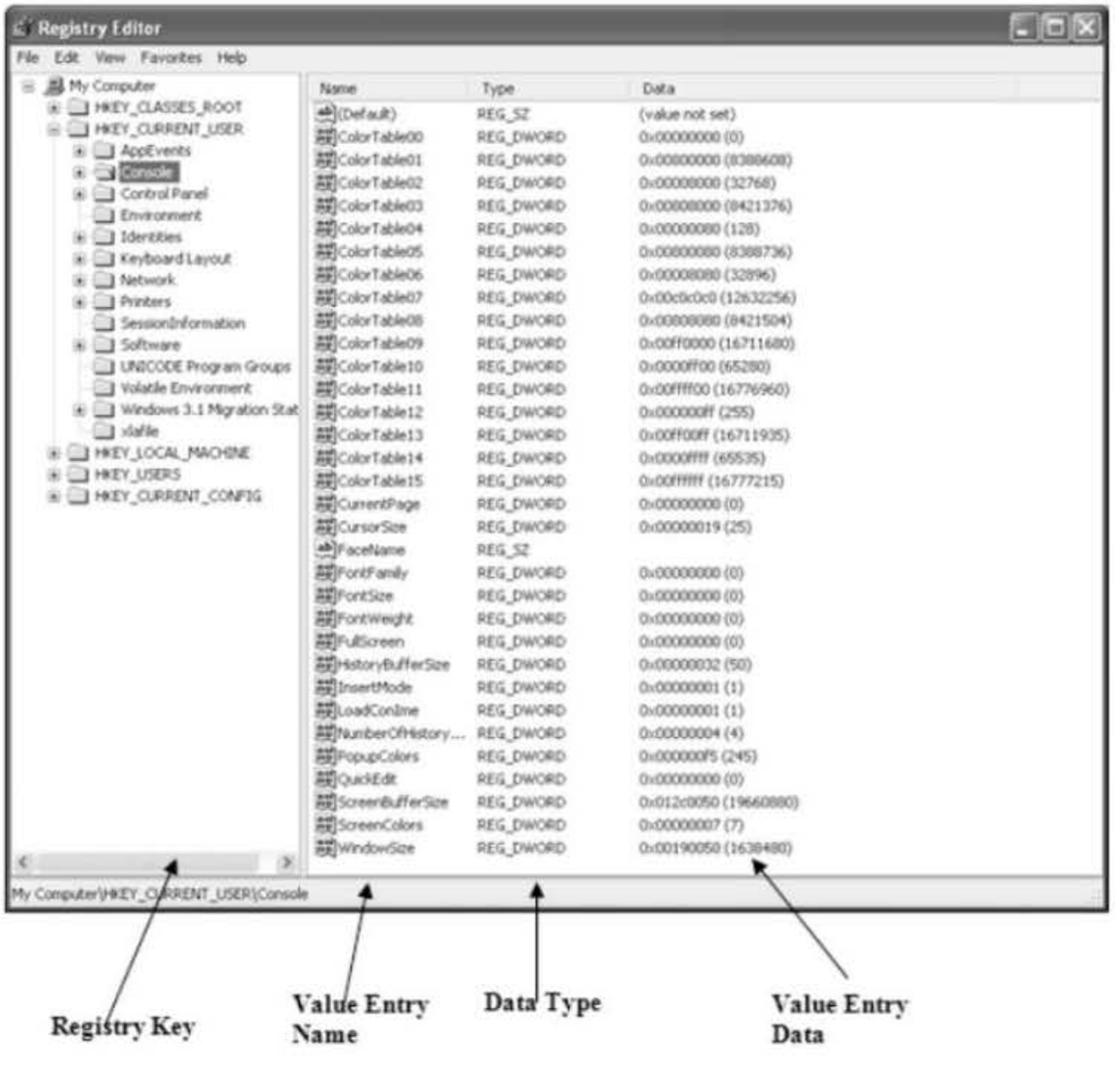
Berdasarkan pernyataan di atas, Microsoft memang menggunakan registry sebagai pusat dalam menyimpan informasi yang menyangkut sistem operasi. Di sinilah forensik bermain untuk menggali lebih dalam evidence yang mungkin ditemukan.

Registry terdiri dari tujuh *root key* atau *hives*. Dapat Anda lihat pada gambar bahwa key tersebut diawali dengan kata HKEY (*Handle to a Key*), dari key yang ada hanya dua saja yang dikatakan sebagai registry yang sebenarnya, yang lain hanyalah pengembangan yang merupakan shortcut yang mengacu pada dua hives ini.

Gambar 6.9 Recently Used

Untuk mengakses registry, Anda dapat mengetikkan kata Regedit pada command run yang disediakan Windows. Perhatikan lebih lanjut bahwa Anda dihadapkan dengan registry yang hierarkikal dan secara garis besar dibagi ke dalam empat bagian utama.

Sewaktu mengakses registry, Anda akan dihadapkan pada Gambar 6.10, perhatikan pembagian yang menjelaskan konten masing-masing kolom.



Gambar 6.10 Registry Editor - ROOT KEY (HIVES)

Tujuh key dalam registry ditampilkan dan dijelaskan sebagai berikut:

- **HKEY_USERS**. Berisi informasi mengenai user, mencakup pula *generic user*. Informasi yang disimpan pada hive ini antara lain: konfigurasi aplikasi dan setting visual.

- **HKEY_LOCAL_MACHINE**. Hive yang terdiri dari informasi spesifik komputer yang berhubungan langsung dengan sistem operasi, misalnya: daftar drive yang di gunakan, perangkat keras yang terintgrasi, dan konfigurasi dasar berkenaan aplikasi yang diinstal.

- **HKEY_CLASSES_ROOT**. Informasinya tergolong sama dengan Reg.dat. Berisi detail lebih jauh berkenaan aturan drag and drop,

shortcuts dan informasi user interface. HKEY_CLASSES_ROOT merupakan alias dari HKLM\Software\Classes.

- **HKEY_CURRENT_USER.** Key ini berisi informasi spesifik user yang diciptakan sewaktu user login ke sistem dan dibangun pada awalnya dengan informasi yang umum pada key HKEY_USERS. Key ini merupakan nama lain dari user-specific branch pada HKEY_USERS yang berisi konfigurasi data untuk user yang sedang login. Pada dasarnya, informasi umum yang diaplikasikan pada user adalah: HKU\.DEFAULT.
- **HKEY_CURRENT_CONFIG.** Key ini menyimpan informasi mengenai konfigurasi sistem saat ini yang merupakan nama lain dari: HKLM\Config\profile (konfigurasi hardware saat ini).
- **HKEY_DYN_DATA.** Berisi status dinamis informasi untuk perangkat/devices yang menggunakan arsitektur plug-and-play. Misalnya saja sewaktu mem-plug in (mengintgrasikan) USB flash disk drive.
- **HKEY_PERFORMANCE_DATA.** Key ini menyediakan dukungan untuk sistem monitoring didasarkan pada kernel Windows NT.

Perhatikan Tabel 6.1 berikut berkenaan dengan *root key* dan singkatan yang menyertainya.

SINGKATAN	ROOT KEY (HIVES)
HKU	HKEY_USERS
HKLM	HKEY_LOCAL_MACHINE
HKCR	HKEY_CLASSES_ROOT
HKCU	HKEY_CURRENT_USER
HKCC	HKEY_CURRENT_CONFIG
HKDD	HKEY_DYN_DATA
HKPD	HKEY_PERFORMANCE_DATA

Tabel 6.1 ROOT KEY (HIVES)

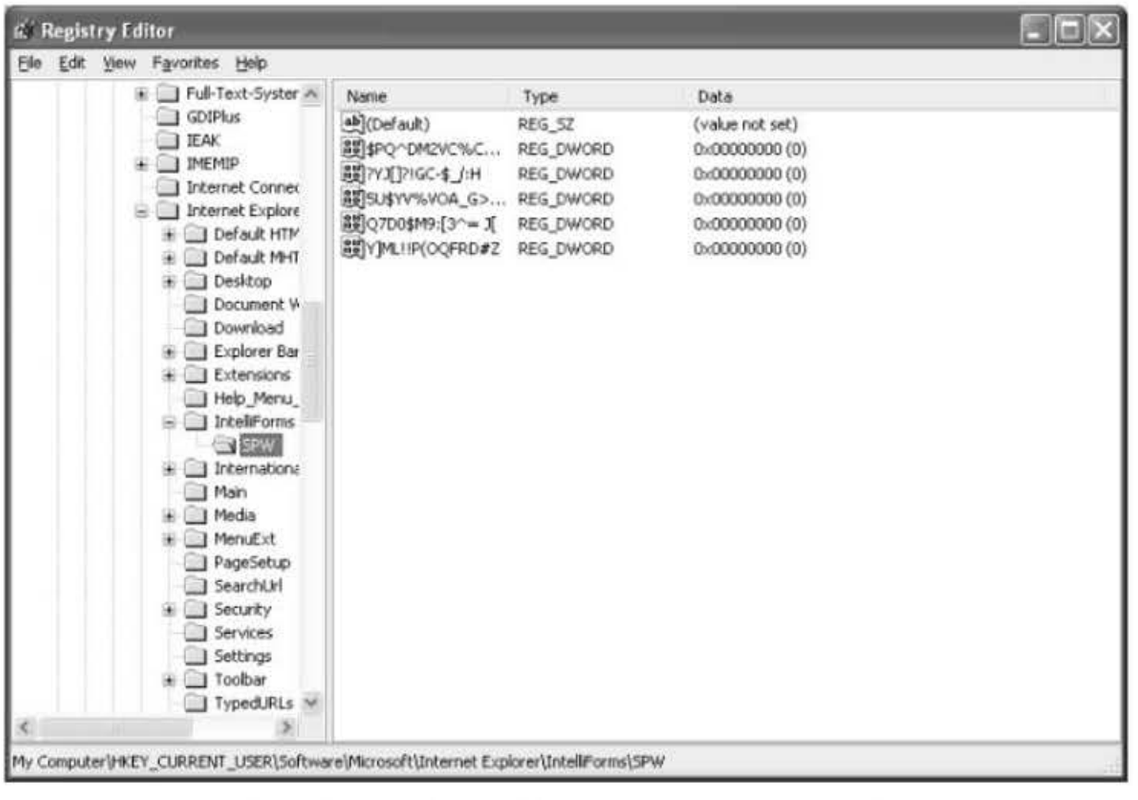
File registry disimpan pada lokasi yang berbeda, tergantung pada sistem operasi windows yang digunakan, misalnya saja:

- Sistem operasi Windows 3.x pada c:\windows\reg.dat.
- Sistem operasi Windows 98 pada c:\windows.
- Sistem operasi Windows NT pada c:\winnt\system32\config.
- Sistem operasi Windows XP pada c:\windows\system32\config.

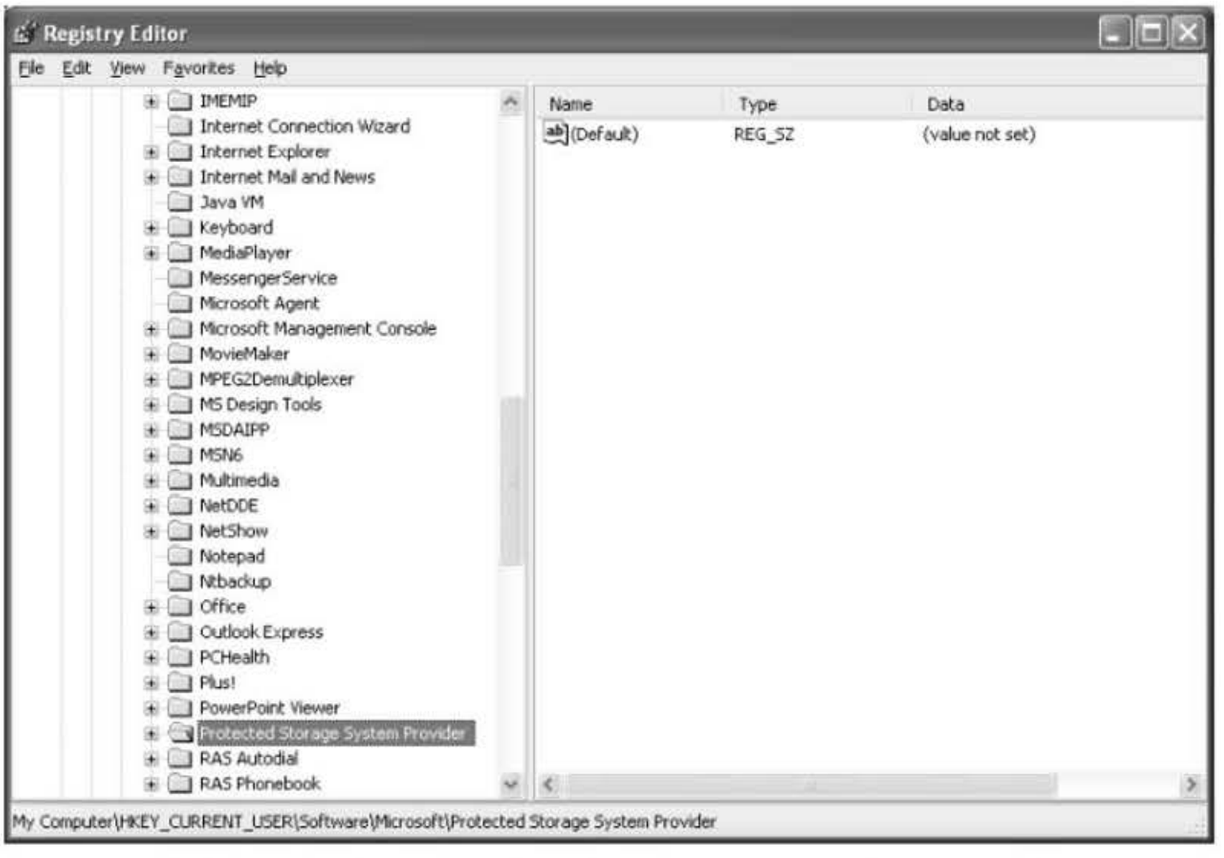
6.3 Informasi Esensial pada Registry

Kita langsung saja melihat apa saja yang disimpan pada registry, terlepas dari hal-hal teknis yang dapat Anda pelajari kemudian berkenaan registry dan masing-masing hive-nya.

Bagaimana password disimpan pada registry? Coba perhatikan Gambar 6.11 dan Gambar 6.12, ini mengacu pada informasi registry pada gambar berikut.



Gambar 6.11 HKCU\Software\Microsoft\Internet Explorer\Intel\Forms\SPW



Gambar 6.12 Registry – HKCU\Software\Microsoft\ Protected Storage System Provider

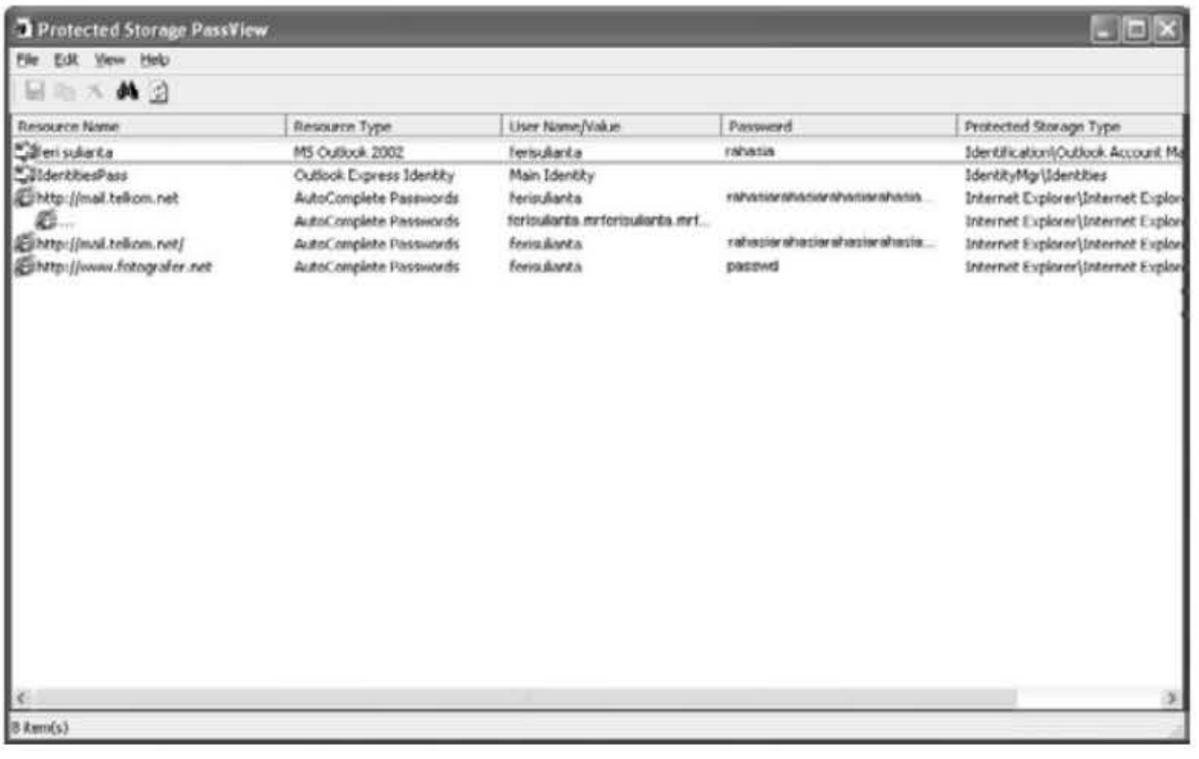
- HKCU\Software\Microsoft\Internet Explorer\Intel\Forms\SPW
- HKCU\Software\Microsoft\Protected Storage System Provider

Akan sangat membingungkan untuk memahami informasi demikian pada registry, tampaknya Anda membutuhkan interface lain yag memberikan kemudahan membaca informasi registry.

Untuk itu, penulis menggunakan PassView software yang mengeksplorasi informasi pada registry tadi. Dan software ini mampu memberikan informasi berikut:

- Outlook password.
- Password Autocomplete pada Internet Explorer.
- Password Protected pada Internet Explorer.
- Password MSN Explorer.

Penggunaannya relatif mudah, cukup dengan mengakses software tersebut untuk satu kali klik dan hasilnya adalah informasi password seperti terlihat pada Gambar 6.13.

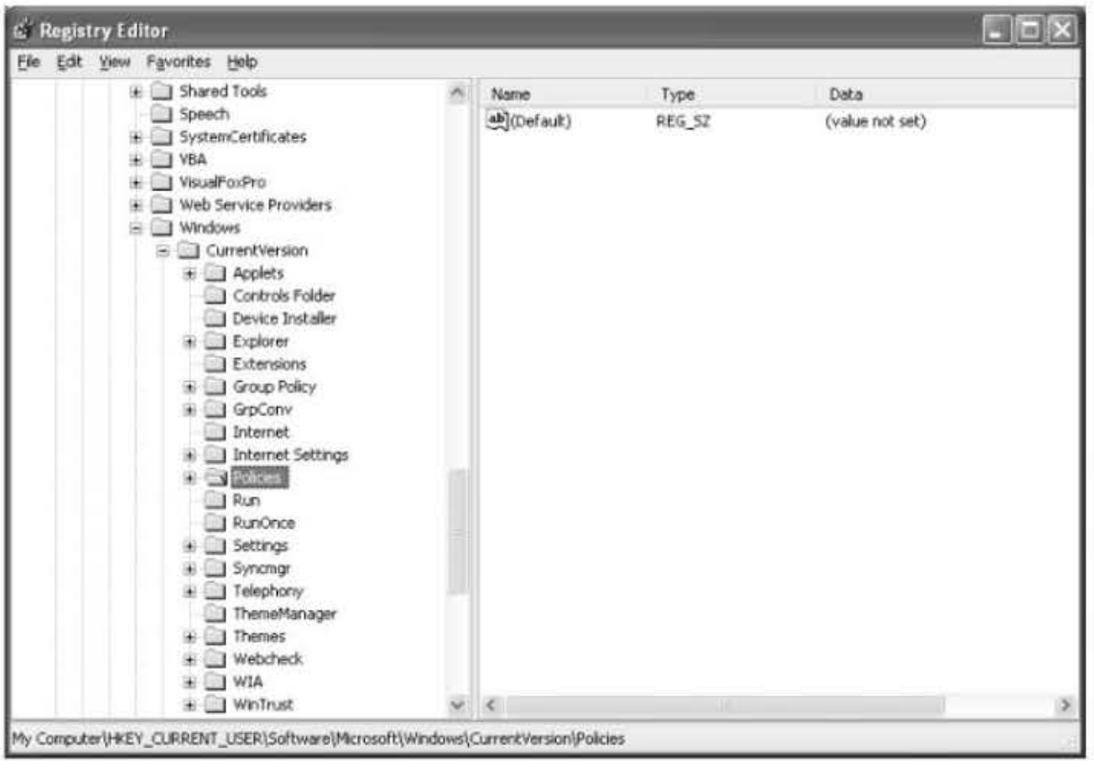


Gambar 6.13 Registry – PassView Program

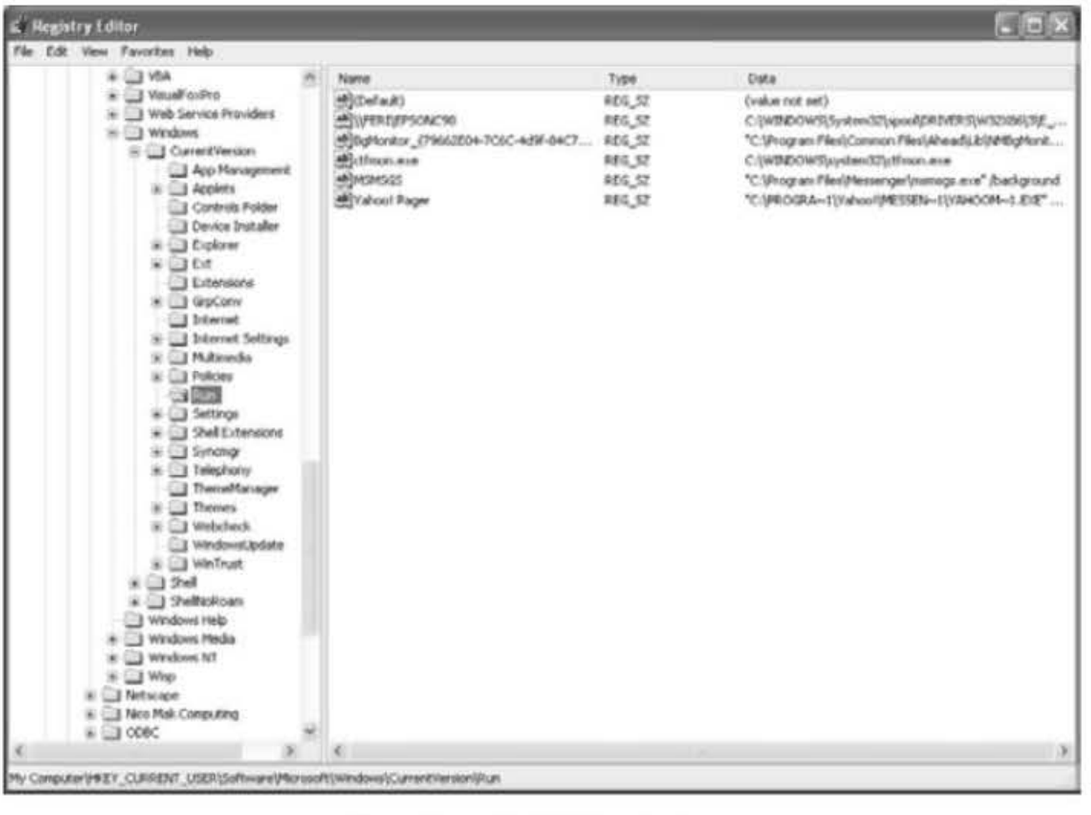
Untuk melihat aplikasi yang dijalankan sewaktu sistem operasi dijalankan (start up), informasinya tersimpan pada beberapa registry key sebagai berikut:

- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run`
- `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `ProfilePath\Start Menu\Programs\Startup\`

Contoh informasi yang tersimpan pada registry dapat dilihat pada Gambar 6.14 dan Gambar 6.15.

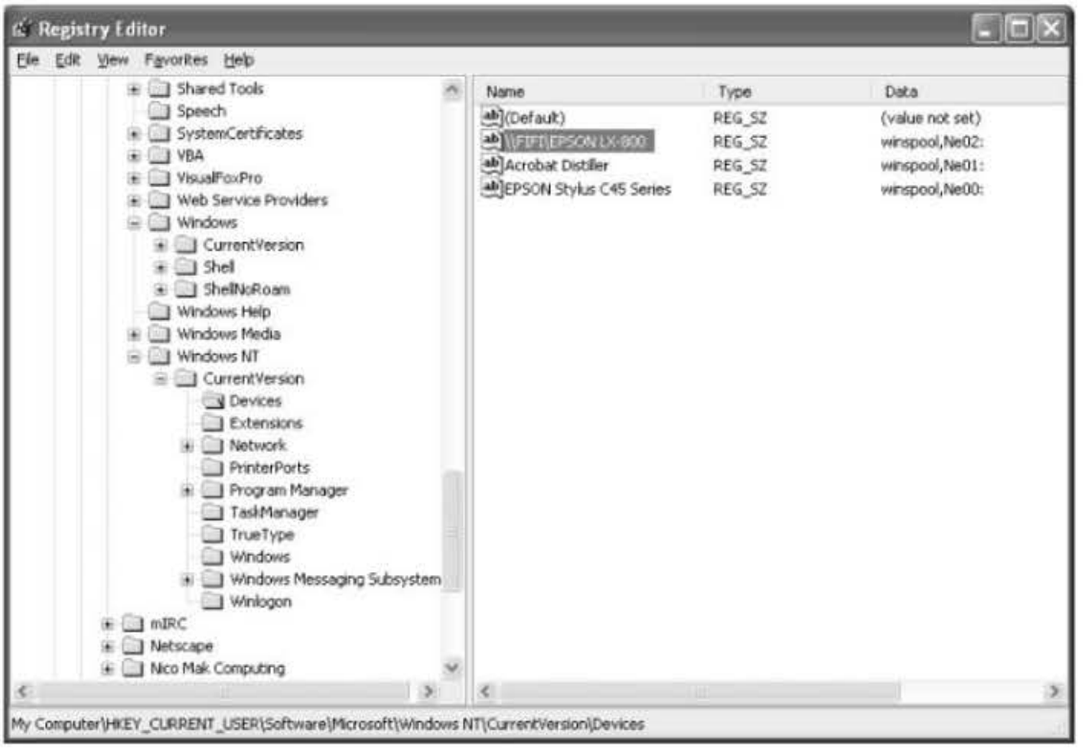


Gambar 6.14 Registry – HKCU\Software\Microsoft\Windows\CurrentVersion\Policies



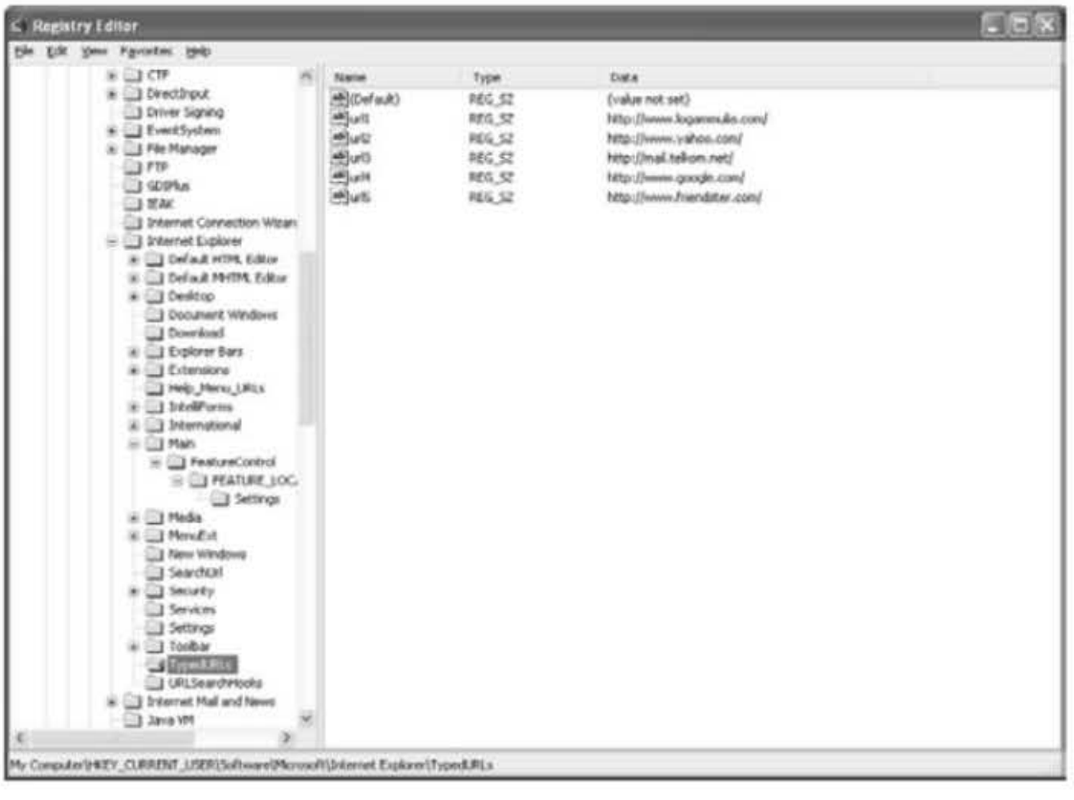
Gambar 6.15 Registry – HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Beberapa device yang saat ini terintegrasi pada sistem komputer dapat Anda lihat pada Gambar 6.16.



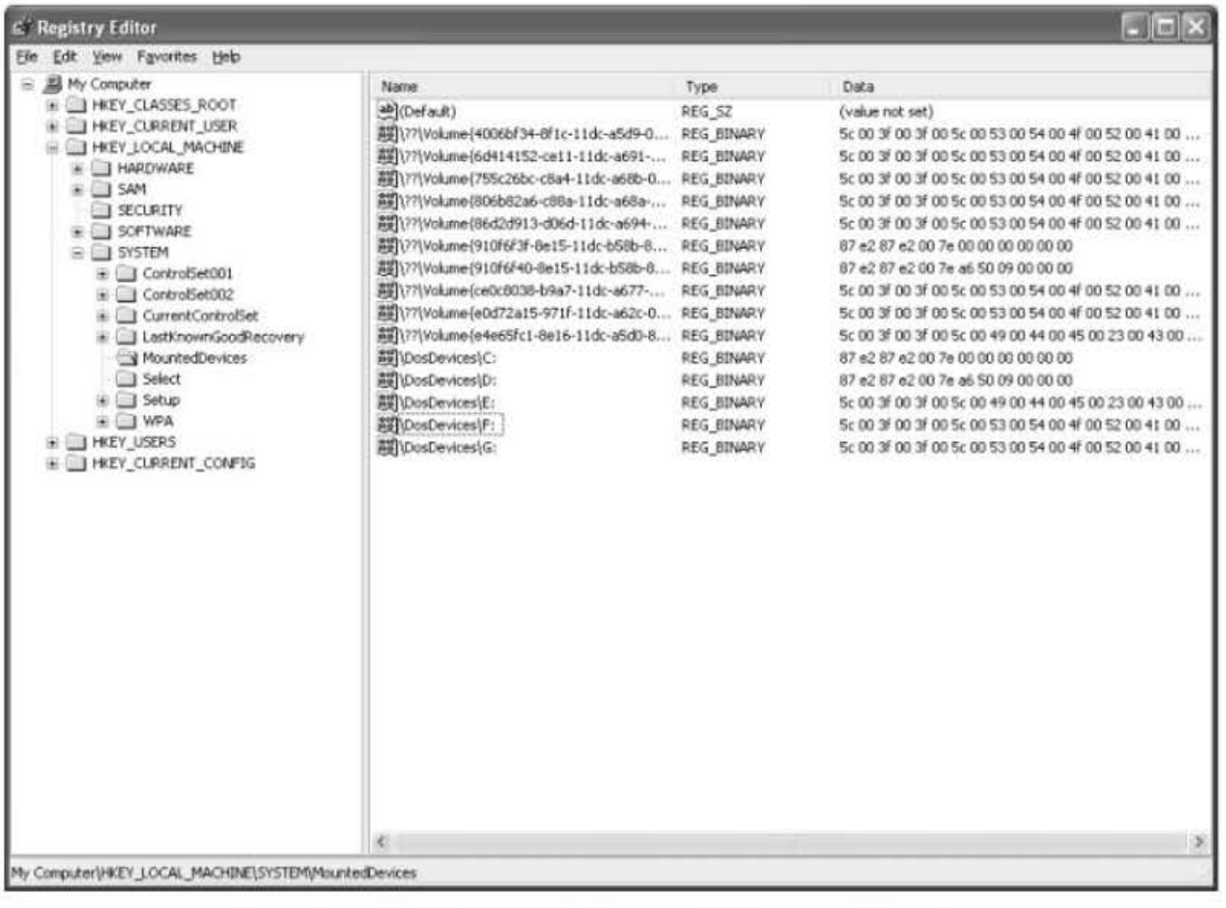
Gambar 6.16 HKCU\Software\Microsoft\Windows NT\CurrentVersion\Device

Sedangkan aktivitas Anda berinternet, dapat dicari dengan mengakases Windows Registry, perhatikan Gambar 6.17 yang menampilkan daftar informasi perihal URL yang baru-baru ini diakses.



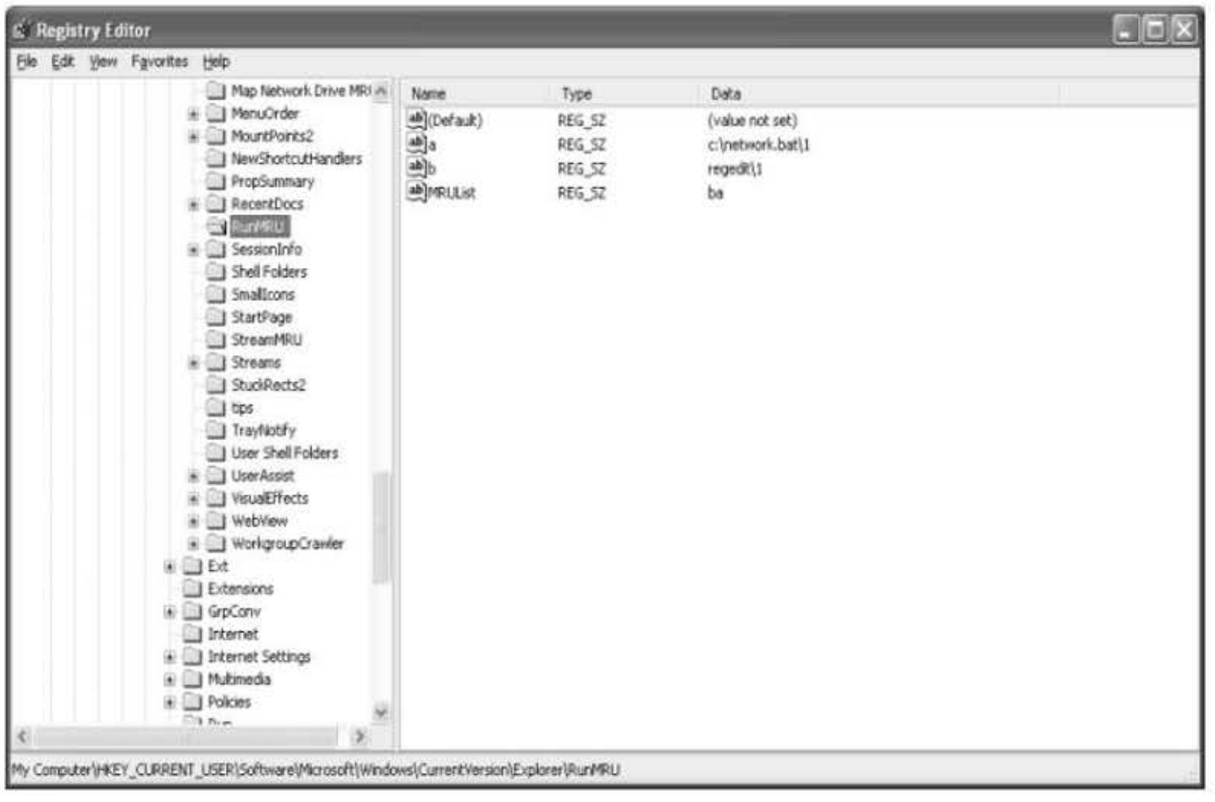
Gambar 6.17 HKCU\Software\Microsoft\Internet Explorer\TypedUrl

Hal lain lagi yang dapat dianalisa dari windows registry, misalnya berbagai media penyimpanan yang pernah diintegrasikan dengan sistem komputer, semisal Flash disk, Floppy, dan lainnya yang mungkin dapat saja berisi evidence. Riwayat perihal integrasi perangkat demikian dapat pula teralamati melalui registry. Perhatikan Gambar 6.18



Gambar 6.18 HKLM\System\MountedDevices

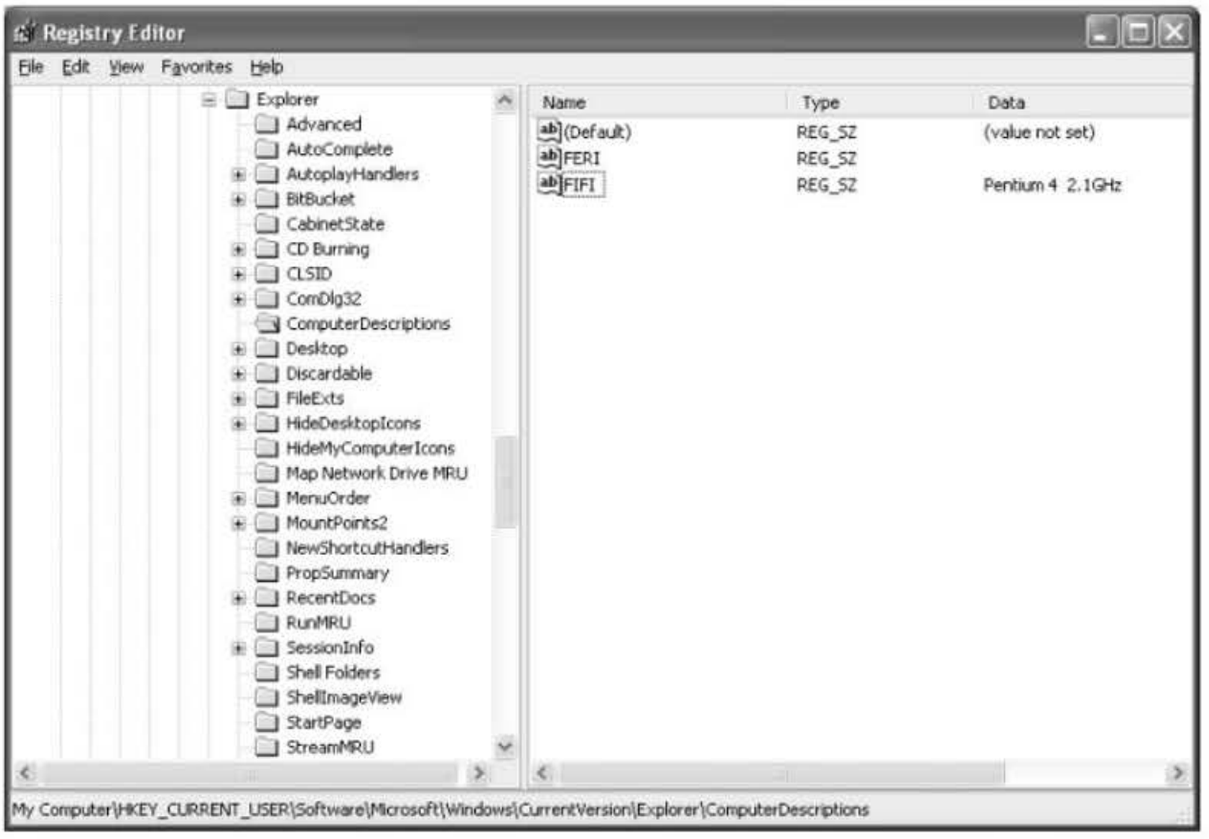
Mungkin Anda mengetikkan command pada Run Command Windows untuk mengakses executable aplikasi, maka aksi ini pun tercatat pada registry (Gambar 6.19).



Gambar 6.19 HKCU\Software\Microsoft\Windows \CurrentVersion\Explorer\RunMRU

Kompleksitas dari komputer forensik akan bertambah jika melibatkan cakupan yang lebih luas, misalnya sistem yang terletak/diintegrasikan dengan jaringan komputer, aktivitas user yang bersangkutan dijaringan pun menjadi demikian penting untuk dianalisa, bahkan berbagai komputer apa saja yang mungkin pernah terkoneksi dengan komputer suspect.

Coba perhatikan pada Gambar 6.20, diperlihatkan ada beberapa komputer yang berada dalam ruang lingkup jaringan komputer dengan komputer suspect, bagaimana user kemudian beraktivitas dapan di ekplorasi lebih dalam.



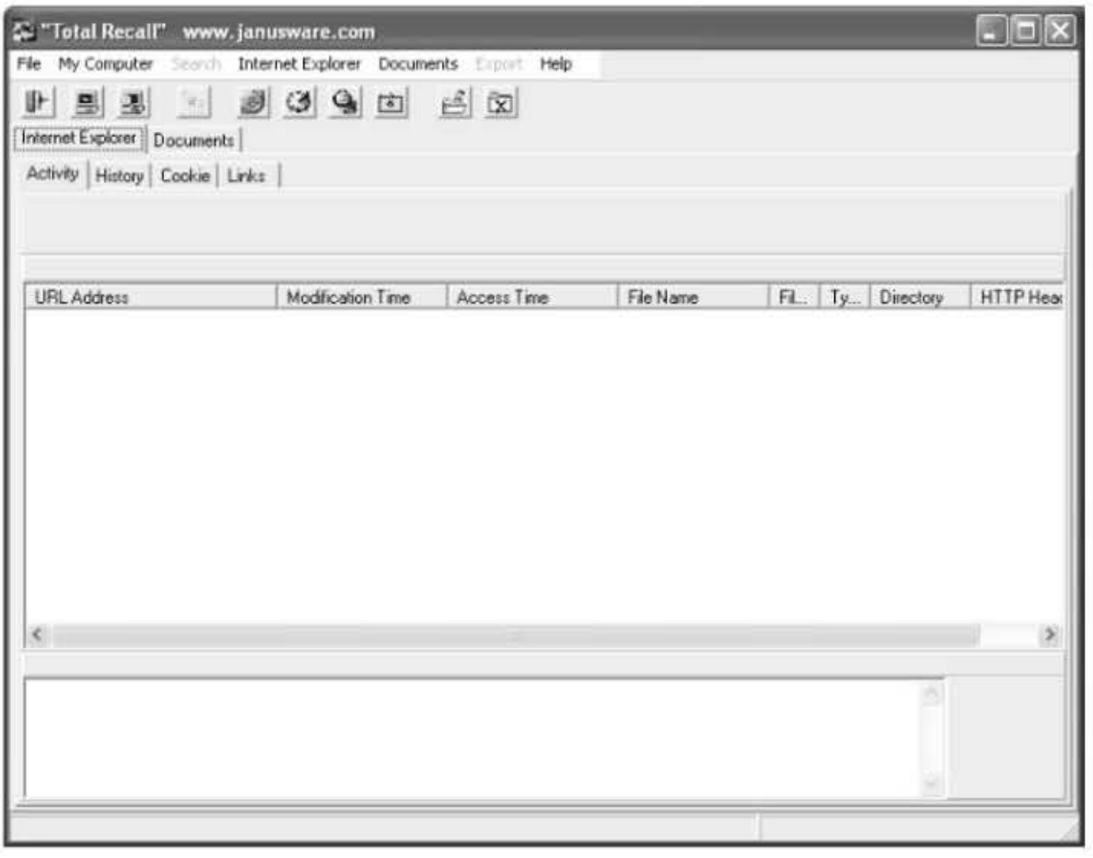
Gambar 6.20
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComputerDescriptions

6.4 Informasi dari Software Forensik

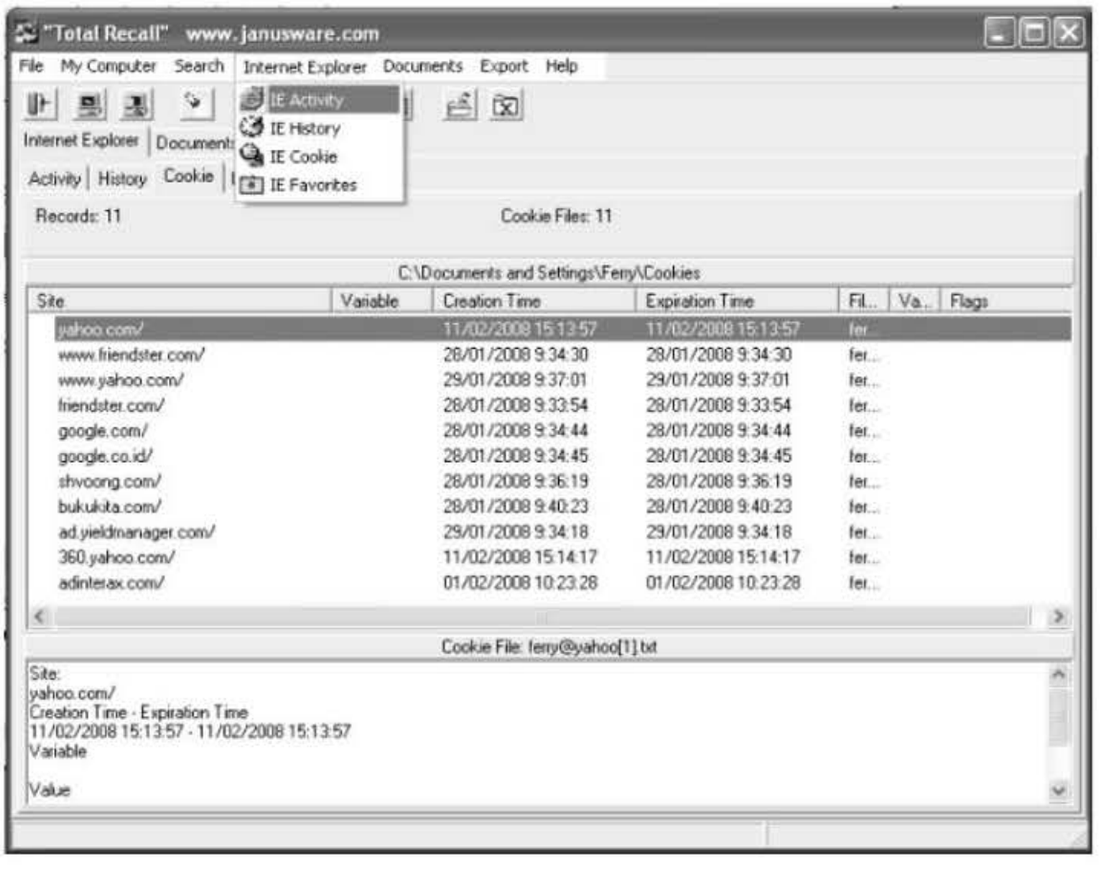
Komputer desktop sudah menjadi perangkat teknologi informasi dan komunikasi yang banyak digunakan, setiap orang mengingini satu bagi dirinya, ini terbukti dengan banyaknya pengguna computer rumahan dan perkantoran yang menggunakan komputer desktop dalam beraktifitas.

Ternyata, berbagai aktivitas yang dilakukan dan informasi yang terelasi lainnya didokumentasikan dengan sangat baik pada komputer yang bersangkutan dan pengguna tidak menyadari hal ini.

Salah satu aplikasi yang digunakan dalam mengakses informasi yang terdokumentasi demikian yaitu dengan menggunakan TotalRecall Software, (Gambar 6.21) salah satu *forensic analysis tool* gratis yang digunakan untuk merekonstruksi aktivitas.

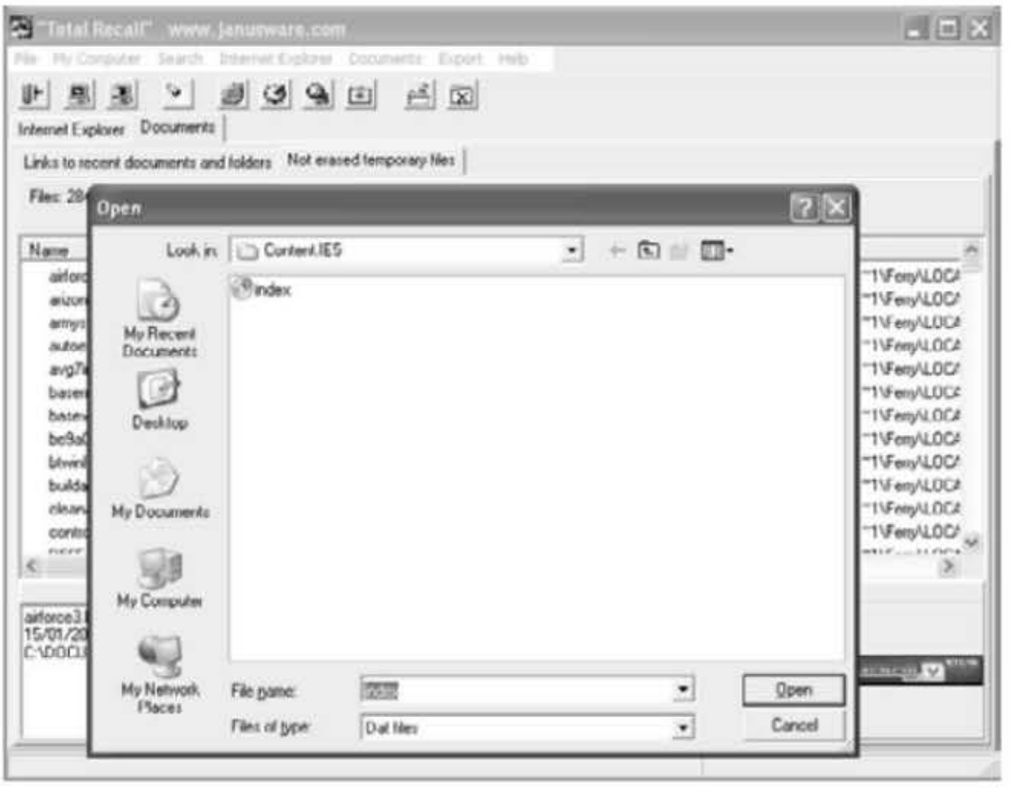


Gambar 6.21 Total Recall Software

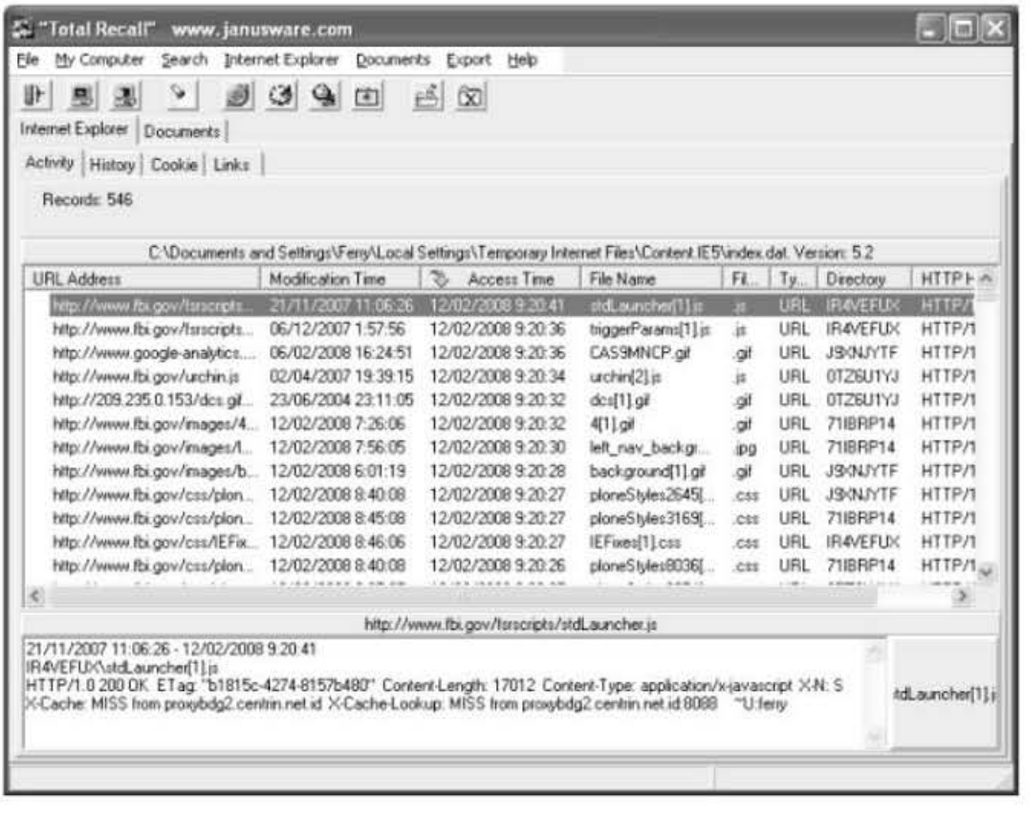


Gambar 6.22 Total Recall Software – Internet Activity

Total Recall mampu merekonstruksi aktivitas yang terjadi pada Microsoft Internet Explorer (MS IE), mencakup pula aktivitas pengguna komputer yang dimaksud. Gambar 6.24.



Gambar 6.23 Total Recall Software – Internet Activity – Akses Index.dat



Gambar 6.24 Total Recall Software – Internet Activity - List

Pada dasarnya, aktivitas internet disimpan oleh Microsoft Internet Explorer dan disimpan pada file index.dat (Gambar 6.23).

Informasi seputar user data, internet cookies, dan internet history dapat ditemukan pada folder di users profile. Aktivitas lain semisal browser activity file (aktivitas mengakses konten internet via web browser) disimpan dalam bentuk biner, maka dari itu dibutuhkan perangkat lunak khusus untuk membaca informasi tersebut.

Beberapa investigasi yang dimunculkan oleh program ini antara lain:

- Aktivitas user pada Internet Explorer.
- Internet Explorer history.
- Internet Explorer cookie.
- Favorites pada Internet Explorer.
- Aktivitas pemakai, yang mencakup:
    - File temporer yang tidak dihapus dan masih tersimpan di komputer (not erased temporary files).
    - File yang baru diakses (recent files and folders).

Informasi dapat diekspor dalam bentuk file .XML (extensible markup language) dan .TXT (teks).

Pembedahan forensik lebih lanjut dapat dilakukan terhadap e-mail dengan menganalisa struktur e-mail seperti header dan atribut lainnya, demikian pula pada sistem-sistem seperti Bulletin Board System, Newsgroup, ChatRoom, dan lain sebagainya.

6.5 Problem Komputer dengan Forensik Komputer?

Beberapa pengetahuan komputer forensik di atas dapat menjadi solusi efektif dalam hal misalnya: mengapa sistem komputer terkena virus, meskipun user mengatakan bahwa tidak ada aktivitas apa pun yang membuat virus bersarang di komputernya.

Kebanyakan user tidak menyadari bahwa virus hanya akan benar-benar teridentifikasi setelah program malicious ini merusak sistem komputer, user pun mungkin tidak menyadari bahwa ada orang-orang disekitar mereka yang juga pernah menggunakan komputer mereka secara diam-diam.

Informasi yang disimpan dalam registry perihal perangkat flash disk yang pernah terintgrasi ke komputer user dapat menjadi bagian dari evidence bahwa seseorang pernah menggunakan komputer tersebut dan virus yang menjangkiti USB flash disk pun menyebar ke sistem komputer.

Gambar 6.25 Integrasi media penyimpnanan portable di atas pun akan tercatat pada registry

Banyak hal lain sehubungan problematika komputer yang dapat dialamati, bahkan dicarikan solusinya dengan konsep komputer forensik. Lebih lanjut akan dibahas pada bab berikut.

BAB 7
KONSEP FORENSIK DALAM KELOLA IT?

7.1 Melihat Kasus Nyata Komputer Forensik

Berikut dicontohkan sebuah kasus dan proses forensik yang dilalui untuk mengungkap fakta sebubungan pornografi anak. Dan beginilah pada dasarnya ahli forensik bekerja dan mendokumentasi semua aktivitasnya.

Catatan: Material ini dibuat oleh U.S. Departement of Justice yang termasuk public domain yang dapat dipergunakan tanpa melanggar hak kekayaan intelektual.

Ringkasan kasus

SUBJECT: Seseorang yang merupakan pemilik perusahaan X, SUBJECT: memerintahkan karyawannya untuk mengirimkan komputer laptopnya kepada salah seoang karyawan untuk dibawa perusahaan service komputer Mom & Pop. Perbaikan ditujukan karena adanya masalah pada monitor.

Untuk memastikan bahwa laptop berhasil diperbaiki, maka sudah menjadi prosedur pada Mom & Pop untuk melakukan pengecekan dengan terlebih dahulu mengakses Start Bar dari Windows 98 dan file untuk ditampilkan.

Alhasil, salah satu file yang dilihat adalah gambar anak-anak yang memperlihatkan aksi seks.

Lalu perusahaan Mom & Pop segera melaporkannya dengan menelepon ke pihak yang berwajib. Seorang petugas yang ditunjuk menangani serta mengamati gambar yang dilaporkan oleh perusahaan Mom & Pop, yang kemudian memastikan bahwa gambar digital ini merupakan pelanggaran terhadap undang-undang negara.

Laptop itu disita petugas dengan keberadaan material seks, dan ini adalah langkah pertama sebagai aksi dari investigasi aksi kriminal.

Laptop dijadikan barang bukti sesuai dengan kebijakan lembaga hukum, dan surat perintah penggeledahan dibuat untuk pemeriksaan komputer.

Komputer diserahkan untuk pemeriksaan.

Tujuan (Objectives): Untuk menentukan apakah SUBJECT memiliki pornografi anak. Hal ini tidak mudah dikarenakan banyak orang yang pernah menangani atau menggunakan laoptop tersebut.

Jenis komputer(Computer type): laptop Generik, serial # 123456789.

Sistem operasi(Operating System): Microsoft Windows 98.

Pelanggaran (Offense): Memiliki pornografi anak.

Petugas (Case agent): Investigator Johnson.

Nomor Bukti (Evidence number): 012345.

Chain of custody: Lihat formulir terlampir.

Lokasi pemeriksaan berlangsung (Where examination took place:): Unit investigasi kriminal.

Peralatan yang digunakan(Tools used): Disk acquisition utility, universal graphic viewer, command line.

<u>Prosedur pemrosesan</u>

Penilaian (Assesment):

Dilakukan peninjauan permintaan penyidik dan surat perintah penyidikan diberikan. Penyidik mencari informasi yang berkaitan pornografi anak, tanggal akses, dan kepemilikan komputer. Hal ini dimungkinkan dengan adanya peralatan yang tersedia di laboratorium forensik.

Akuisisi (Acquisition):

Konfigurasi hardware didokumentasikan dan duplikat pada hard drive laptop yang menjadi evidence, hal ini dilakukan untuk melindungi barang bukti sewaktu proses penyidikan berlangsung.

Mendokumentasikan kelengkapan informasi yang dibutuhkan seperti: informasi CMOS, waktu, dan tanggal.

Pemeriksaan (Examination):

Merekam direktori file dan struktur file, mencakup pula tanggal dan waktu.

Dilakukan proses pencarian file header terhadap semua image grafis. Melakukan peninjauan untuk setiap file image yang tampaknya menggambarkan pornografi anak.

Ditemukan shortcut file yang menunjuk pada file di disket dengan nama file eksplisit secara seksual yang melibatkan anak-anak.

Didapati informasi bahwa waktu terakhir akses file, yakni 10 hari sebelum laptop diberikan kepada Mom & Pop untuk diperbaiki.

Dokumentasi dan pelaporan (Documentation and reporting):

Laporan hasil pemereriksaan diberikan kepada sang investigator. Penyidik memutuskan untuk diadakan wawancara terhadap orang yang menyerahkan laptop ke jasa service Mom & Pop.

Langkah selanjutnya (Next Step):

Mewawancarai karyawan yang memberikan komputer laptop ke Mom & Pop. Sang karyawan dinyatakan tidak pernah mengoperasikan komputer.

SUBJECT pernah memerlihatkan pada sang karyawan perihal gambar seksual yang melibatkan anak-anak pada laptopnya.

SUBJECT mengatakan kepada karyawan bahwa dia menyimpan gambar-gambar serupa pada disket di rumah; SUBJECT lupa bahwa ada satu gambar masih tersimpan pada laptop.

Kantor Pengacara Negara bagian berupaya mendapatkan surat perintah penggeledahan rumah milik SUBJECT, hal ini didasarkan pada pemeriksaan bukti digital dan wawancara karyawan.

Surat perintah dibuat dan disampaikan kepada petugas pengadilan untuk kemudian disahkan.

Selama proses pencarian bukti selanjutnya, floppy disk ditemukan di rumah SUBJECT. Hasil pemeriksaan disket mengungkapkan tambahan pornografi anak, termasuk gambar yang memerlihatkan bahwa SUBJECT terlibat secara fisik. Bukti ini menjadi dasar kuat untuk penangkapan SUBJECT.

Hasil laporan perihal kasus di atas dapat dilihat sebagai berikut.

Case brief 1 report

REPORT OF MEDIA ANALYSIS

MEMORANDUM FOR: County Sheriff's Police
Investigator Johnson
Anytown, USA 01234

SUBJECT: Forensic Media Analysis Report
SUBJECT: DOE, JOHN
Case Number: 012345

1. Status: Closed.

2. Summary of Findings:

- 327 files containing images of what appeared to be children depicted in a sexually explicit manner were recovered.
- 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children were recovered.

3. Items Analyzed:

TAG NUMBER:	**ITEM DESCRIPTION:**
012345	One Generic laptop, Serial # 123456789

4. Details of Findings:

- Findings in this paragraph related to the Generic Hard Drive, Model ABCDE, Serial # 3456ABCD, recovered from Tag Number 012345, One Generic laptop, Serial # 123456789.

1) The examined hard drive was found to contain a Microsoft® Windows® 98 operating system.

2) The directory and file listing for the media was saved to the Microsoft® Access Database TAG012345.MDB.

3) The directory C:\JOHN DOE\PERSONAL\FAV PICS\, was found to contain 327 files containing images of what appeared to be children depicted in a sexually explicit manner. The file directory for 327 files disclosed that the files' creation date and times are 5 July 2001 between 11:33 p.m. and 11:45 p.m., and the last access date for 326 files listed is 27 December 2001. In addition, the file directory information for one file disclosed the last access date as 6 January 2002.

4) The directory C:\JOHN DOE\PERSONAL\FAV PICS TO DISK\ contained 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children. The file directory information for the 34 shortcut files disclosed the files' creation date and times are 5 July 2001 between 11:23 p.m. and 11:57 p.m., and the last access date for the 34 shortcut files was listed as 5 July 2001.

5) The directory C:\JOHN DOE\LEGAL\ contained five Microsoft® Word documents related to various contract relationships John Doe Roofing had with other entities.

6) The directory C:\JOHN DOE\JOHN DOE ROOFING\ contained files related to operation of John Doe Roofing.

7) No further user-created files were present on the media.

5. Glossary:

Shortcut File: A file created that links to another file.

6. Items Provided: In addition to this hard copy report, one compact disk (CD) was submitted with an electronic copy of this report. The report on CD contains hyperlinks to the above-mentioned files and directories.

IMA D. EXAMINER
Computer Forensic Examiner

Released by_____

*Catatan: dikarenakan istilah komputer bukan istilah yang general, maka diperlukan daftar kata-kata (glossary) yang dideskripsikan untuk menjelaskan istilah spesifik komputer.

Dalam kasus ini, dapat dialamati bahwa proses forensik adalah proses bertahap dan berkesinambungan, setiap proses selalu memunculkan informasi baru yang menjadi landasan kuat untuk mencari sejumlah fakta lain. Dan fakta diperlakukan amat sangat hati-hati agar setiap penelusuran terhadap fakta atau bukti tidak merusak keabsahannya.

Pola bernalar dan cara bekerja seperti inilah yang penting untuk diterapkan bagi pengguna komputer terutama departemen IT dalam mengelola sumber daya IT.

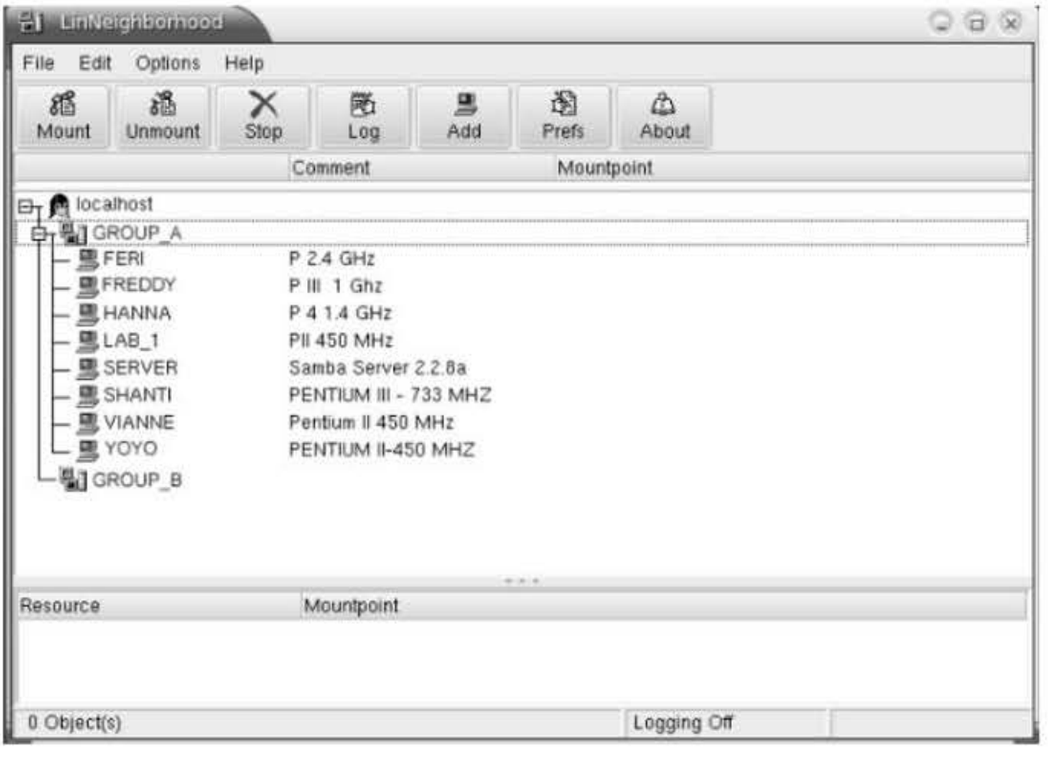
7.2 Fakta Unik Departemen IT yang Teridentifikasi dengan Penalaran Forensik

Kerap kali, Departemen IT atau Personel IT berkehendak langsung memberikan solusi tanpa memilikirkan dengan seksama apa penyebab dan akibat dari tindakannya. Alhasil tidakannya justru menyita lebih banyak waktu dan sumber daya yang tidak perlu. Perhatikan beberapa kasus solusi IT yang penting dengan memberlakukan penalaran forensik.

Aksi Ping of Death

Seorang user mendapati komputernya mengalami restart dan menampilkan pesan kerusakan pada windows kernel. Sewaktu komputer dinyalakan beberapa saat, maka komputer berjalan me-load sistem operasi tetapi beberapa saat layar menampilkan blue screen yang menginformasikan bahwa terjadi kerusakan dari sistem operasi.

Si user menyatakan bahwa tampaknya komputer terkena virus karena beberapa bulan yang lalu komputernya pun kerap kali terkena virus dan harus diinstal ulang.



Gambar 7.1 Lingkungan jaringan komputer perusahaan dengan konfigurasi Windows dan Linux saat itu

Staf IT mengambil komputer tersebut untuk diinstal ulang, dan hampir saja diinstal ulang.

Tetapi berdasarkan saran dari IT manajer, komputer tersebut dilakukan cek menyeluruh, dan tidak didapati virus bahkan komputer baik-baik saja. Kondisi ini dimungkinkan setelah komputer tidak lagi terkoneksi ke jaringan komputer.

Setelah dilakukan penyelidikan, ada komputer tertentu yang berada di jaringan dengan sistem operasi Linux yang sengaja melakukan aksi ping untuk mengganggu komputer user yang bersangkutan, yakni dengan mengirimkan sejumlah paket non fragmentasi berukuran besar, sehingga komputer yang dikenai aksi ping tersebut kewalahan menangani datangnya paket yang dikirimkan via jaringan. Kondisi ini terjadi pada sistem operasi Windows terdahulu, dan sistem operasi Windows terkini sudah mampu melakukan manajerial aksi ping ini.

Listing ping relatif sederhana seperti tertera pada perintah berikut: di mana 192.168.1.10 adalah IP Address komputer korban:

```
$ sudo ping -f -s 65500 192.168.1.10
```

Sintaks:

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
 [-r count] [-s count] [[-j host-list] | [-k host-list]]
 [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
-t Ping the specified host until stopped.
 To see statistics and continue - type Control-Break;
 To stop - type Control-C.
-a Resolve addresses to hostnames.
-n count Number of echo requests to send.
-l size Send buffer size.
-f Set Don't Fragment flag in packet (IPv4-only).
-i TTL Time To Live.
-v TOS Type Of Service (IPv4-only. This setting has been
deprecated
 and has no effect on the type of service field in the IP
Header).
-r count Record route for count hops (IPv4-only).
-s count Timestamp for count hops (IPv4-only).
-j host-list Loose source route along host-list (IPv4-only).
-k host-list Strict source route along host-list (IPv4-only).
-w timeout Timeout in milliseconds to wait for each reply.
-R Use routing header to test reverse route also (IPv6-only).
-S srcaddr Source address to use.
-4 Force using IPv4.
-6 Force using IPv6.
```

Kegagalan RAM (Random Access Memory)

Kasus menarik lainnya yakni sewaktu seorang staf IT hendak merakit ulang komputer, ternyata didapati RAM tidak berfungsi dan RAM dicobakan pula di beberapa komputer lain dan didapati tidak juga berfungsi, kondisi ini dialamati dengan adanya beep yang menginformasikan kerusakan pada RAM. Staf IT berupaya membeli RAM baru.

*Catatan: RAM (Random Access Memori) adalah tempat untuk menyimpan informasi tetapi hanya bisa menyimpan jika ada sumber daya listrik, maka dari itu disebut sebagai volatile memori.

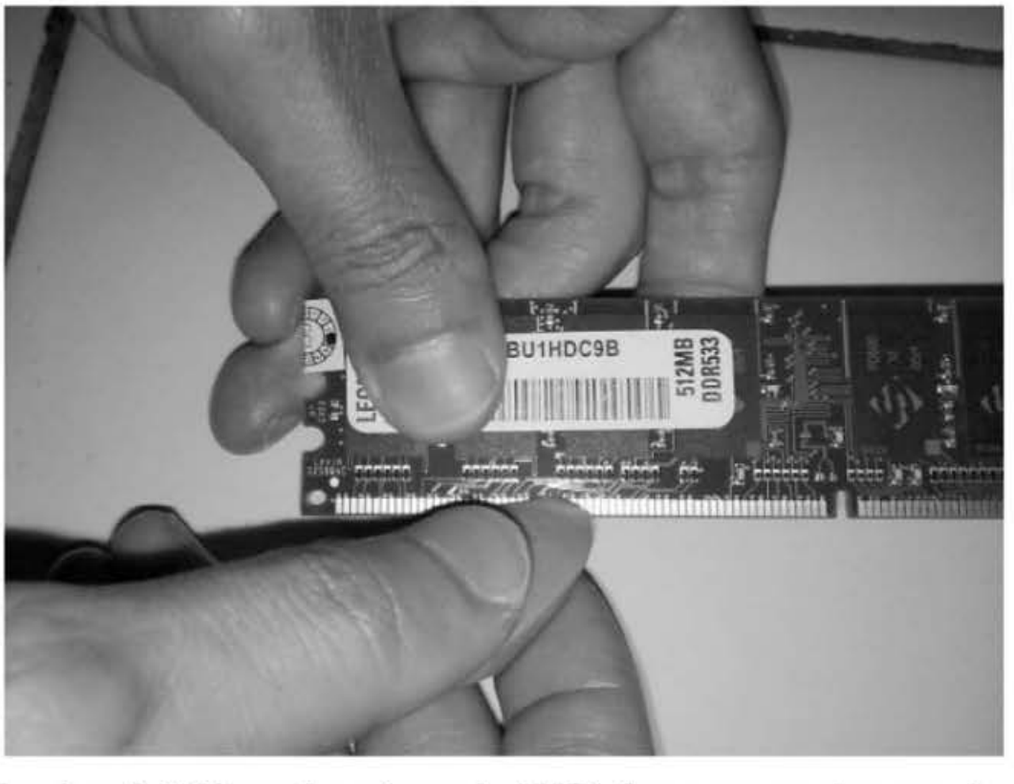
Ternyata setelah ditelusuri duduk perkaranya, kondisi ini dikarenakan adanya muatan listrik statis pada RAM. Karena sebelumnya staf IT

melakukan pembongkaran perangkat keras dengan bertelanjang tangan tanpa menggunakan gelang anti listrik statis.

Lalu bagaimana mengatasinya? Yakni dengan melakukan pembersihan secara fisik yang akan mengeliminasi keberadaan listrik statis. Listrik statis bisa terjadi karena ada gesekan, sehingga RAM tersebut mengandung muatan listrik.

Untuk menghilangkan listrik statis pada RAM, dapat menggunakan alat yang mudah didapatkan. Alat ini adalah penghapus. Penggunaannya cukup mudah tapi perlu ketelitian. Caranya yaitu menyeka penghapus ke pin RAM:

- Seka bagian depan dan belakang RAM dengan hati-hati agar tidak mengenai komponen sirkuit disekitarnya.
- Bersihkan bekas dari sisa penghapus yang menempel pada pin tersebut dengan cara meniupnya dengan blower.



Gambar 7.2 Menyeka pin pada RAM dengan penghapus akan membebaskan RAM dari listrik statis

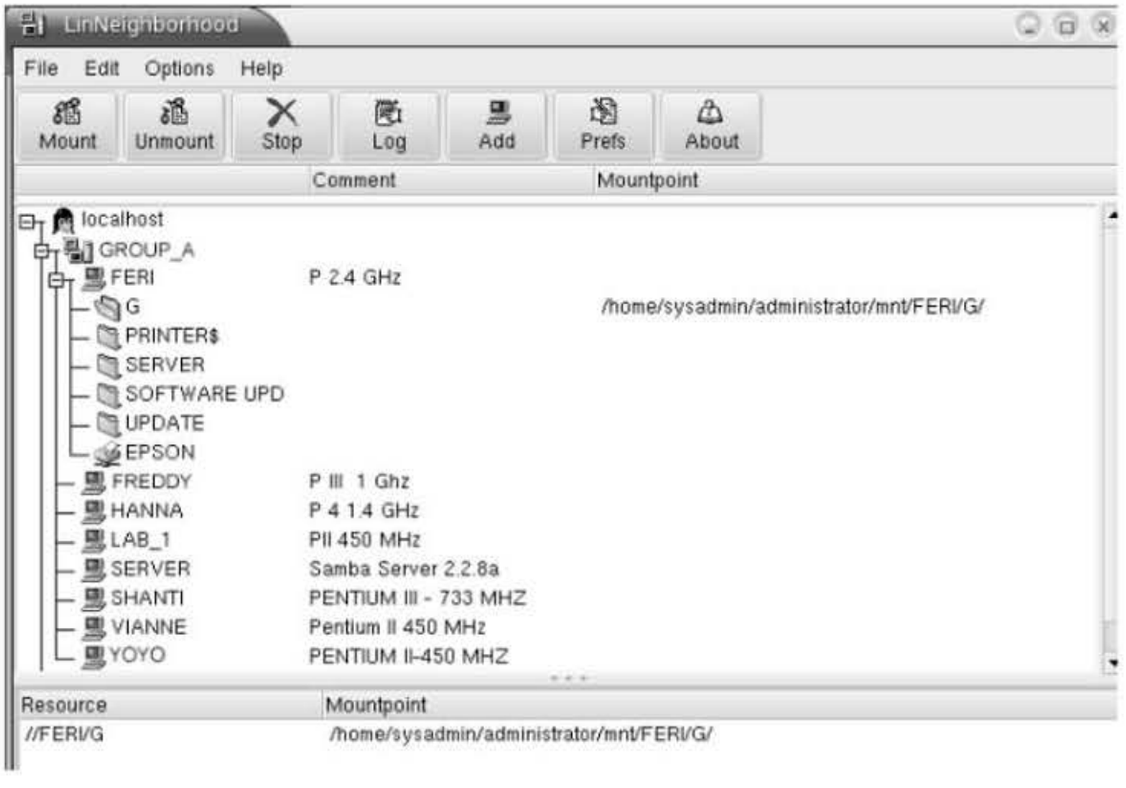
Server Down?

Kasus lain lagi yang unik adalah server yang tiba-tiba hilang koneksi dari jaringan komputer. Kecurigaan muncul dengan asumsi ada yang salah dengan LAN Card dan merembet keberbagai asumsi lain bahkan kerusakan pada Sistem Operasi Server.

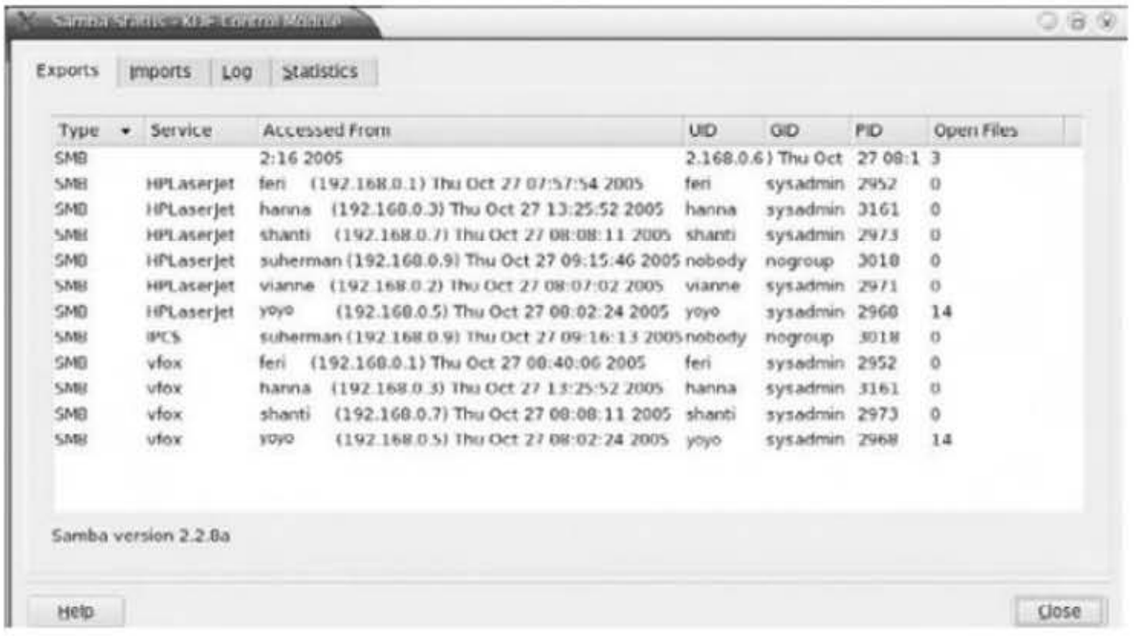
Lalu bagaimana kasus ini ditangani? Sederhananya, seharusnya jika mengandalkan konsep forensik, investigasi dimulai dari server (sebagai pemberi layanan ke jaringan komputer).

Hal ini dilakukan dengan mendisintegrasikan komputer server dari jaringan komputer dan membiarkannya menyala seharian. Bahkan dalam jangka waktu 12 jam dan pernah didapati 4 jam saja, maka server mengalami kegagalan operasi atau HANG.

Penyelidikan berlanjut pada perangkat keras komputer server dan setelah dilakukan pengujian menyeluruh, didapati bahwa RAM mengalami kerusakan.



Gambar 7.3 Kondisi jaringan komputer dengan server linux sewaktu kasus kegagalan server terjadi



Gambar 7.4 Kondisi jaringan komputer dengan server linux sewaktu kasus kegagalan server terjadi – Aplikasi jaringan menggunakan samba server

7.3 Bentuk Manajerial Bagian dari Forensik

Apakah Anda ingat bahwa komputer forensik memampukan evidence dalam rekonstruksi dan seharusnya dapat diambil dengan mudah, hal ini dimungkinkan dengan manajemen IT, sehingga aktivitas apa pun yang melibatkan IT dapat ditelusuri.

Akan didapati banyak pertentangan dan konflik sewaktu departemen IT yang memang dipandang sebagai departemen yang tidak memiliki kegiatan administrasi mulai menerapkan manajemen, bahkan untuk beberapa orang, tindakan administrasi demikian tampak mengada-ada.

Harus pula ada pencetus sewaktu IT mulai menerapkan admnistrasi yang rapi, bukan sekedar birokrasi yang bertele-tele, tetapi lebih mengacu pada pertanggungjawaban dan historis sumber daya teknologi informasi dan kegiatan perihal IT.

Pencetus tentunya akan lebih tegas jika dimotori dan dipelopori oleh manajer level puncak perusahaan. Meskipun demikian, benturan-benturan sosial berupa penolakan dan ketakutan tentu akan ada. Tapi ini

akan hilang seiring berjalannya waktu, bahkan manajer level puncak merasakan manfaatnya meskipun tidak dalam waktu singkat.

Faktor efisiensi dan efektivitas akan berperan sewaktu diberlakukan minimalisasi pemakaian sumber daya pilihan produk, merk, dan lain-lain.

Administrasi IT

Kegiatan administrasi IT seperti apa? Anda tentu setuju bahwasannya administrasi memaksudkan suatu kegiatan yang melibatkan aturan mencakup pekerjaan yang sistematis dan terarah.

Keunggulan yang didapat dari kegiatan administrasi antara lain:

- Sistematis dan jelas aktivitas kerja.
- Kerapihan yang memungkinkan informasi dapat dikelola dan didapatkan kembali sewaktu dibutuhkan.
- Meminimalisasi kesalahan karena rutin yang sudah terstruktur.
- Menyederhanakan kerumitan dan problematika yang muncul.

Kegiatan administrasi dapat diimplementasikan pada:

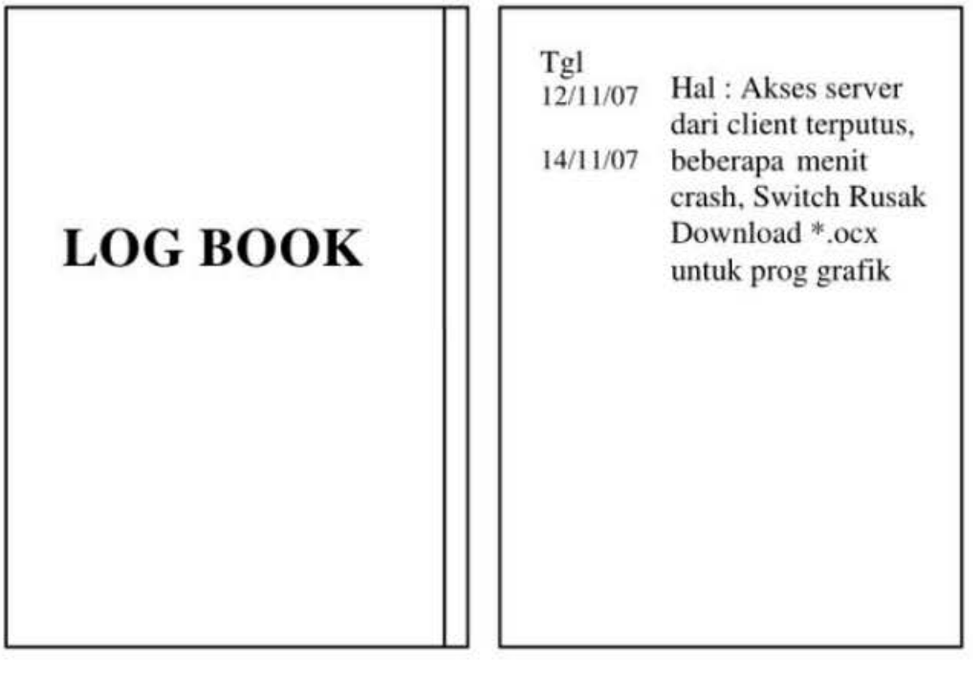
- Proses pengadaan perangkat IT.
- Pemeliharaan sistem informasi (Memperbaiki kesalahan, Cross Checking Database, dokumentasi perubahan sistem).
- Atribut perusahaan yang dibutuhkan oleh sistem informasi (NPWP perusahaan, logo perusahaan, dsb).
- Pembuatan surat keterangan yang berhubungan dengan departement IT (misal: tanda terima barang, keterangan kerja, dan lainnya)
- Dokumentasi pengembangan dan pemeliharaan sistem informasi.

Panduan ini dapat dijadikan referensi bagi departemen IT sewaktu harus berurusan dengan beberapa kegiatan IT yang sifatnya administrasi.

Log Book

Bukan hanya database saja yang memiliki log (log file, yang digunakan sebagai catatan transaksi basis data dan menjadi acuan dalam memperlakukan database di kemudian hari seandainya diperlukan, misalnya sewaktu melihat user mana yang menginput data tertentu pada waktu tertentu), staf IT sebaiknya dibekali dengan log book atau buku catatan khusus untuk kegiatan departemen IT.

Buku catatan ini diperlukan seandainya staf IT melakukan aktivitas kesehariannya, misalnya saja menemukan bug pada modul sistem. Tentu informasi tersebut hendaknya dicatat, dan ciri-ciri dari perilaku program yang janggal pun dicatat, atau bahkan memperbaiki program karena kesalahan logika. Alamat website tempat men-download driver tertentu, metode memperbaiki program yang membutuhkan trik spesifik atau kebutuhan beberapa file ataupun objek file, ada baiknya semua itu dicatat dalam log book.



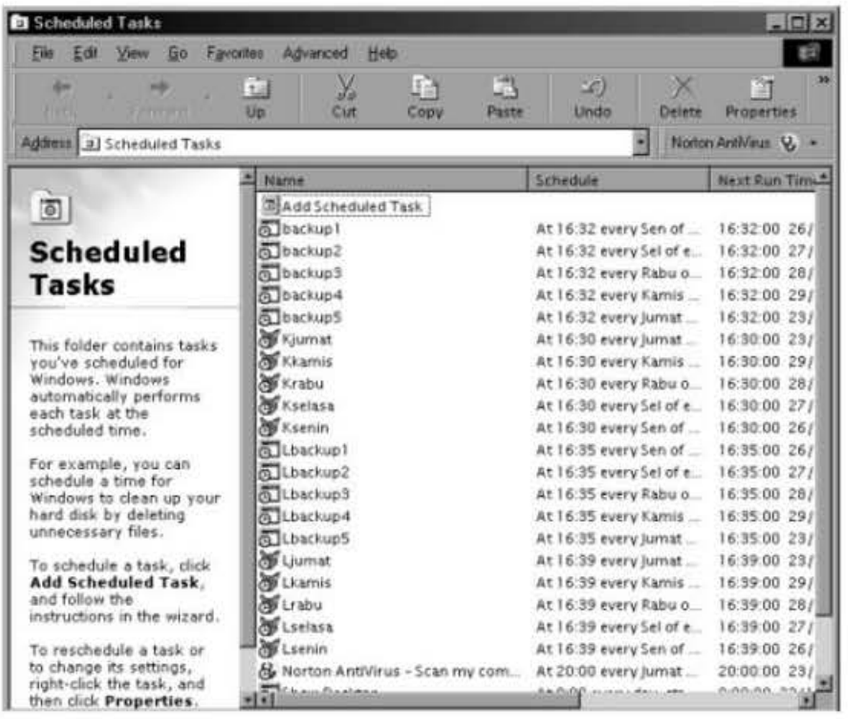
Gambar 7.5 Contoh Log Book

Backup, Backup dan Backup

Backup menjadi salah satu rutin esensial dalam departemen IT. Tidak ada yang lebih buruk dari kehilangan data/informasi bagi departemen IT. Data memiliki bebagai alasan mengapa harus di-backup, ini pun dipengaruhi oleh struktur dari sistem informasi. Beberapa hal yang berhubungan dengan kebutuhan backup data adalah:

- Pemampatan data.
- Data sudah tidak diperlukan untuk proses transaksi dan hanya dibutuhkan sewaktu-waktu untuk kasus tertentu.
- Me-retrive kembali data (mendapatkan kembali data).
- Pencegahan seandainya didapati masalah berupa kerusakan fisik dan logika.
- Mengisolasi data dari sistem yang ëberjalaní, karena alasan keamanan, kerahasiaan, dan lainnya

Berbagai ancaman terhadap data, misalnya kerusakan hardware (Hard disk, USB Flash Disk, dan berbagai media penyimpanan) dan kerusakan software yang umumnya merusak struktur database yang akan memengaruhi informasi yang ada di dalamnya, misalnya saja file indeks yang rusak. Manajemen backup data tentu berbeda antara satu departemen IT dengan departemen IT lainnya, kebutuhan dan karakteristik sistem informasi menjadi salah satu faktor pembeda utama dari beragamnya manajemen backup data.



Gambar 7.6 Schedule Task – Backup Program

RECEIVABLE DEPT.
(*note : backup per month)

2001	1	2	3	4	5	6
	7	8	9	10	11	12
2002	1	2	3	4	5	6
	7	8	9	10	11	12
2003	1	2	3	4	5	6
	7	8	9	10	11	12
2004	1	2	3	4	5	6
	7	8	9	10	11	12
2005	1	2	3	4	5	6
	7	8	9	10	11	12
2006	1	2	3	4	5	6
	7	8	9	10	11	12
2007	1	2	3	4	5	6
	7	8	9	10	11	12

SALES DEPT.
(*note : backup per month)

1999	1	2	3	4	5	6
	7	8	9	10	11	12
2000	1	2	3	4	5	6
	7	8	9	10	11	12
2001	1	2	3	4	5	6
	7	8	9	10	11	12
2002	1	2	3	4	5	6
	7	8	9	10	11	12

Gambar 7.7 Dokumentasi Backup

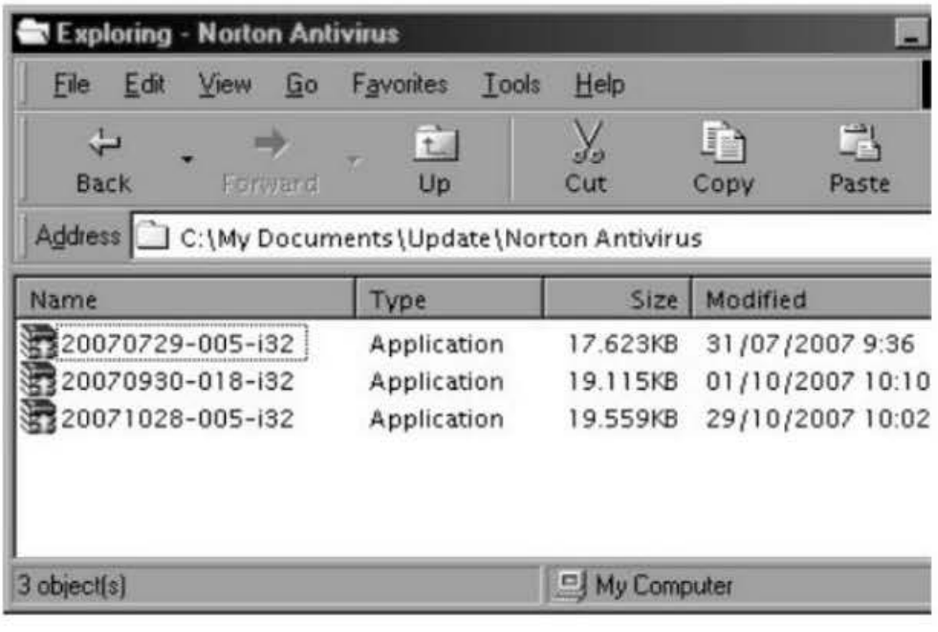
Daftar Sumber Daya IT

Akan sangat berguna membuat daftar sumber daya informasi dengan spesifik, misalnya saja mendata komponen perangkat keras penyusun konfigurasi sistem komputer dan sumber daya jaringan komputer. Mungkin Anda perlu membuat denah jaringan komputer perusahaan, berikut pula komponen atau perangkat lain yang terintgrasi ke jaringan komputer.

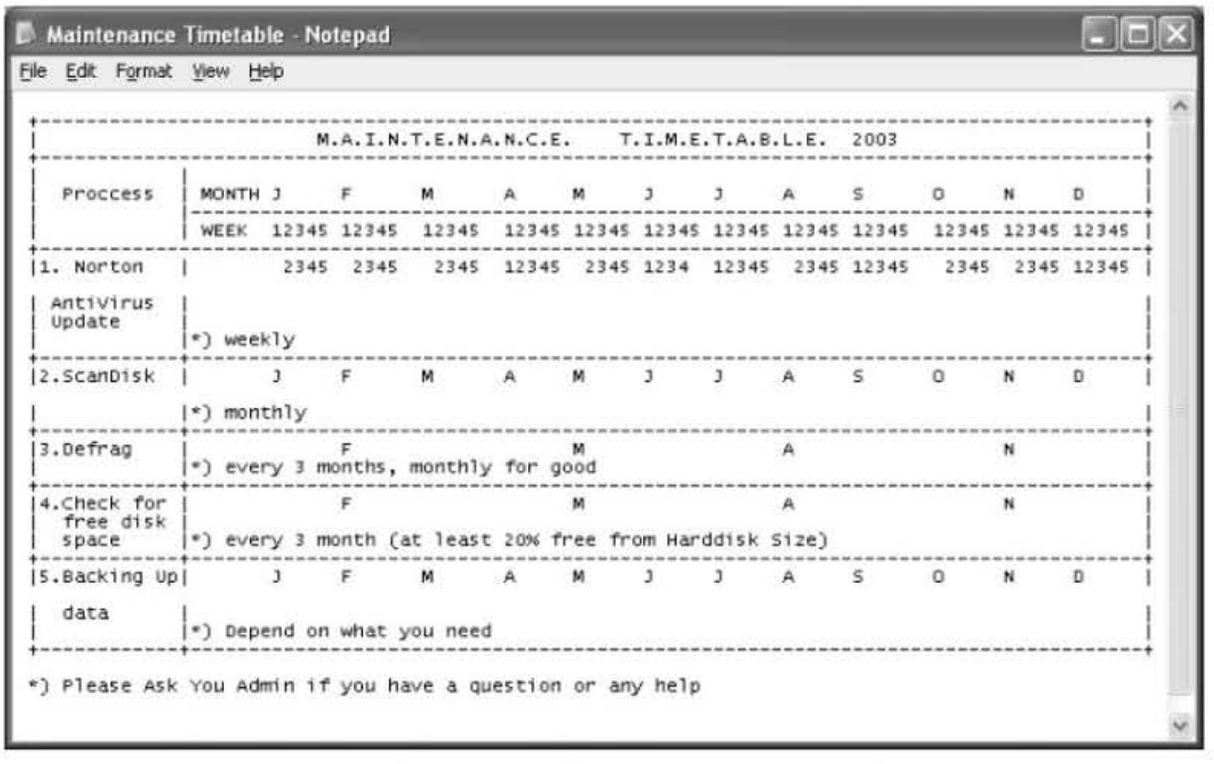
Up to Date - Bagian dari Manajerial

Update merupakan salah satu kegiatan mencakup administrasi rutin dalam memelihara sistem perusahaan. Ada banyak kegiatan yang termasuk ke dalam peng-update-an, misalnya update software dengan mendownload plug-in, patch (umumnya digunakan untuk menutup celah keamanan software aplikasi atau sistem).

Aktivitas update hendaknya didokumentasi untuk menginformasikan kondisi sistem atau perangkat lunak saat ini.



Gambar 7.8 File Update Norton Antivirus



Gambar 7.9 Jadwal Maintenance Sistem Komputer

Bahkan akan lebih baik jika membuat jadwal untuk me-maintenance komputer masing-masing, diharapkan user lebih *well educated* dan peduli dengan perangkat yang digunakannya.

Yang lain dari dokumentasi dan pelabelan

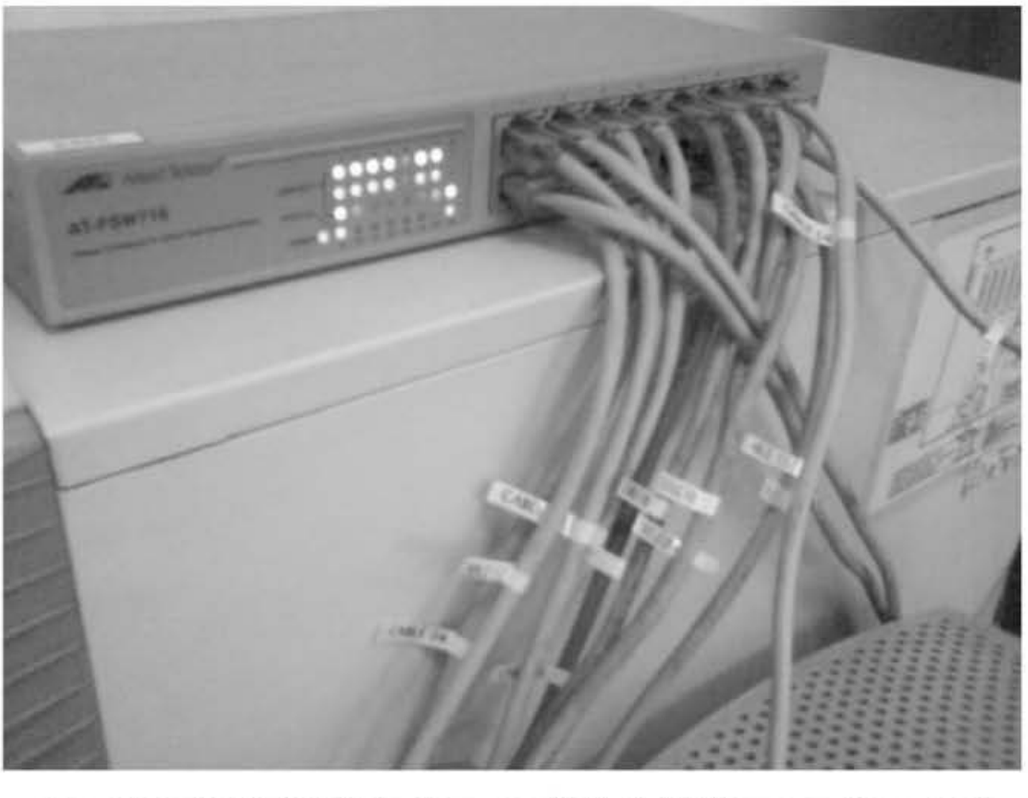
Tujuan jangka pendek manajemen IT dalam departemen IT adalah mengelola sumber daya informasi yang menjadi bagian dalam kegiatan jangka panjang manajerial IT yang akan lebih kompleks, dengan melibatkan banyak departemen lain yang terkait dengan sistem informasi perusahaan.

Banyak hal-hal teknis dan komponen sumber daya yang perlu Anda siapkan dalam mengelola sumber daya jaringan komputer perusahaan, misalnya kebutuhan untuk menambah komputer pada jaringan (LAN). Manajemen akan terasa penting dan memudahkan dalam kelola departemen IT.

Misalnya saja, akan sangat sulit menentukan mana kabel jaringan yang rusak untuk diganti seandainya hal nomor kabel yang terkoneksi ke switch dan LAN Card hilang atau bahkan tidak pernah diberi label.

Hal lagi misalnya, stiker COA (Certificate Of Analysis) yang harus dilekatkan di masing-masing komputer yang memerlihatkan legalitas dari penggunaan sistem operasi.

Hal remeh? Tidak juga. Bagaimana seandainya dalam satu pabrik terdapat beberapa komputer rusak, beberapa monitor rusak, atau beberapa CPU rusak? Untuk memperbaiki dan me-replace lagi ke masing-masing user dengan tepat diperlukan pengenal untuk masing-masing komputer, di sinilah hal kecil menjadi penting bukan? Dan di sinilah konsep kerja komputer forensik bermanfaat.



Gambar 7.10 Switch dengan Kabel UTP yang dinomori

Gambar 7.11 COA Label Windows pada CPU Case

Jika ditelaah, ternyata beberapa konsep forensik pernah diterapkan oleh departemen IT, meskipun kebanyakan mengabaikannya dan baru memikirkan setelah harus merekonstruksi dan mendapatkan informasi dengan susah payah.

BAB 8
ATASI MASALAH DENGAN PENALARAN KOMPUTER FORENSIK

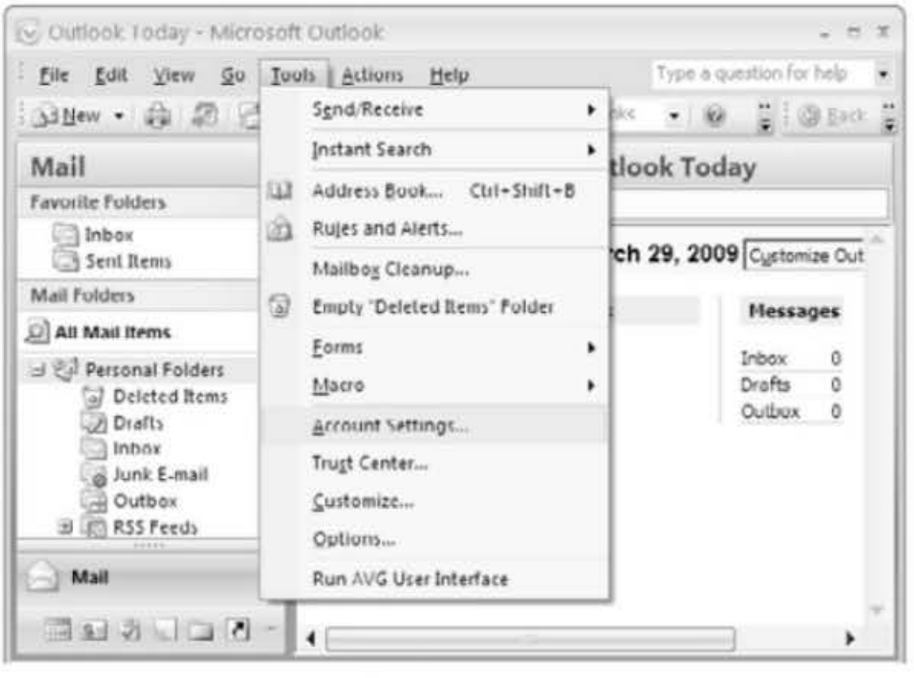
8.1 Men-generate Kembali E-mail Password via Outlook Scanner

Sebenarnya, aplikasi penyadapan kadang dapat digunakan pula sebagai tool forensik. Yang terpenting adalah seberapa terpercaya lembaga yang melakukan komputer forensik.

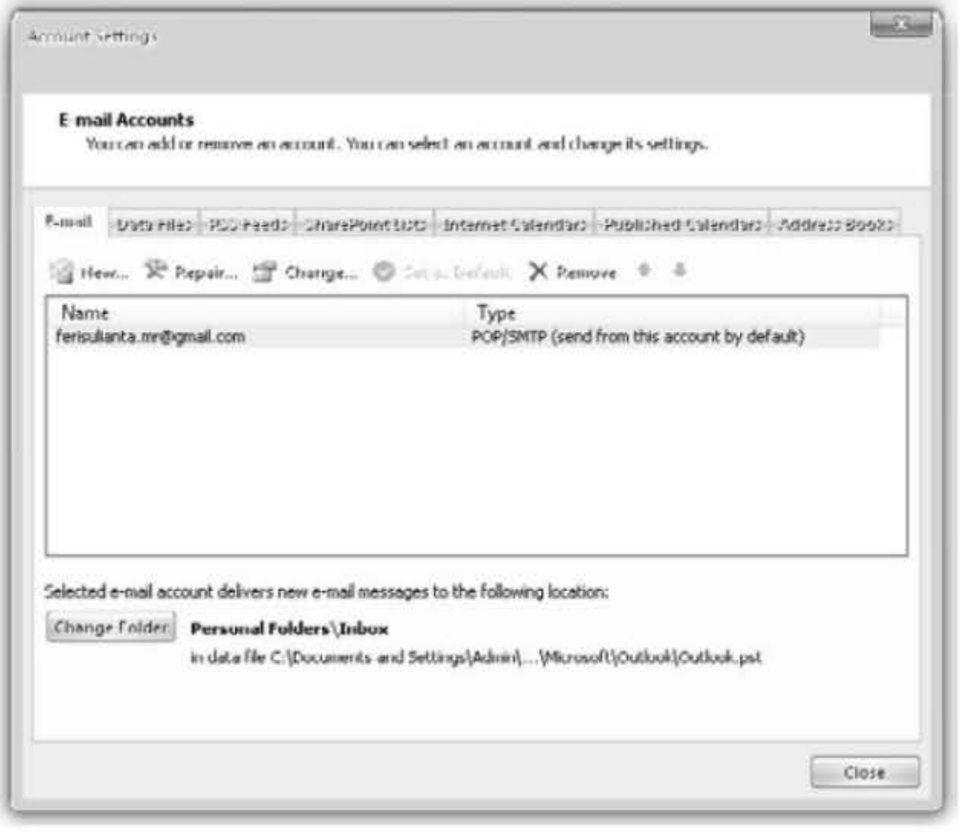
Misalnya saja dalam kasus ini, digunakan Freeware MailPassView versi 1.50 buatan Nir Soft, program ini mampu me-recover password yang ada pada software Mail Client (Gambar 8.1).

Untuk mengakses e-mail (upload dan download) via e-mail client pada komputer PC diperlukan konfigurasi terlebih dahulu, misalnya pada Microsoft Outlook. Yaitu dengan mengakses Tool > Account Setting (Gambar 8.1) hingga tampil informasi e-mail account (Gambar 8.2), klik ganda e-mail account tersebut (dalam hal ini: ferisulianta.mr@gmail.com), maka Internet e-mail setting terbuka, dan di sinilah sebenarnya informasi rahasia disimpan.

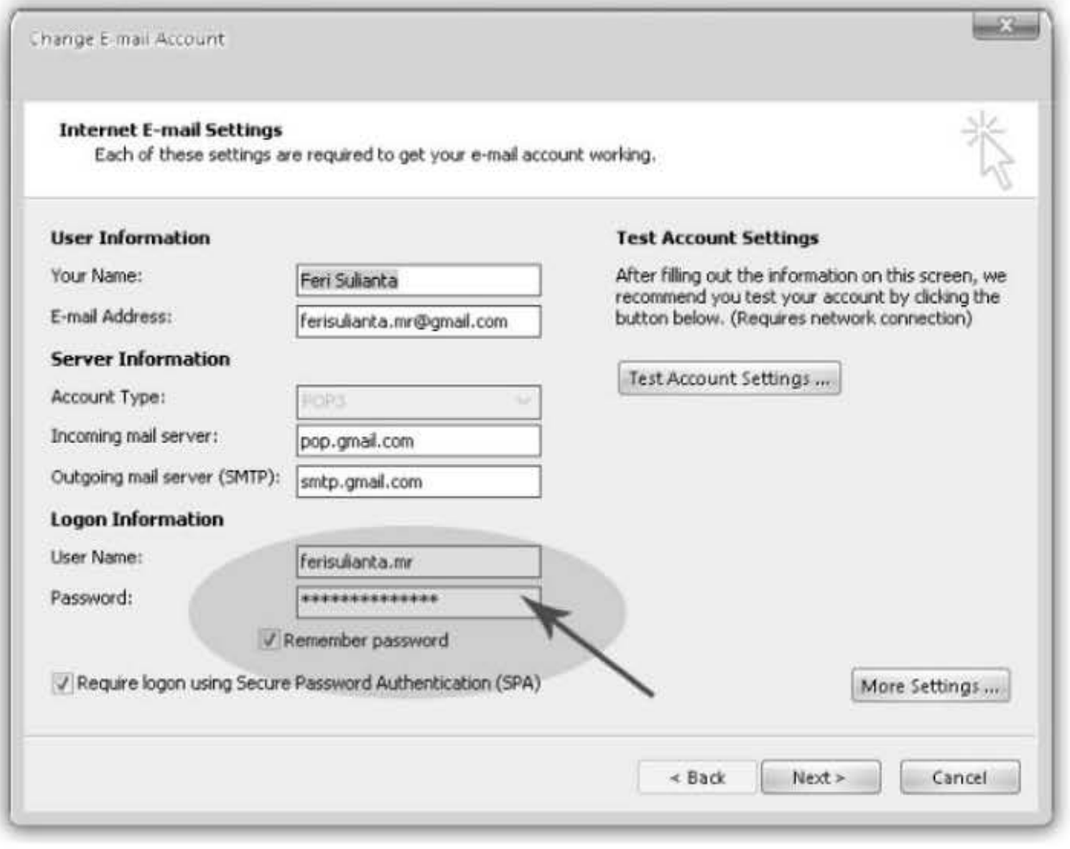
Perhatikan pada informasi password yang diwakilkan dengan simbol asterisk. Anda tidak dapat menebak-nebak begitu saja karakter di balik simbol asterik tersebut, tetapi dengan program Mail PassView, password tersebut dapat kita ketahui.



Gambar 8.1 Microsoft Outlook 2007



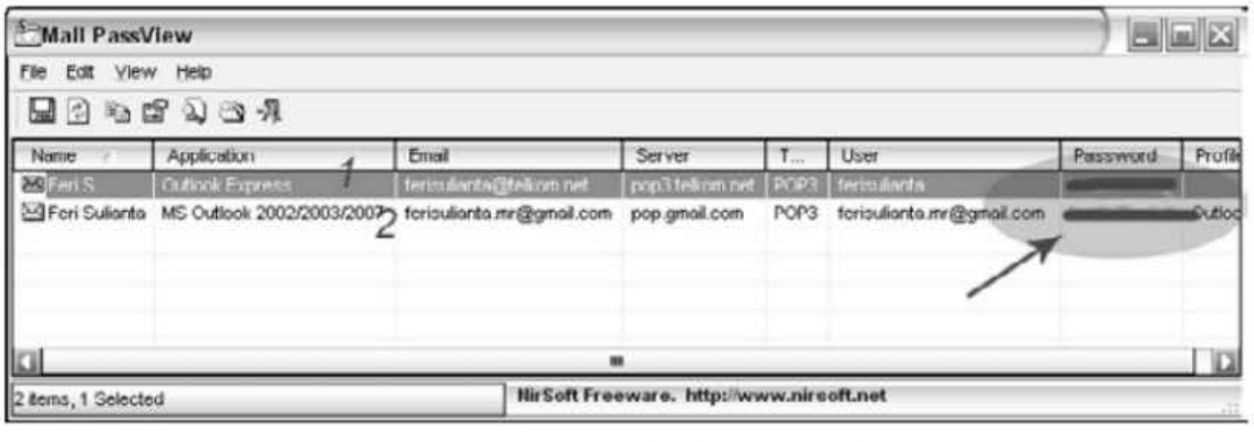
Gambar 8.2 E-mail Account pada Microsoft Outlook 2007



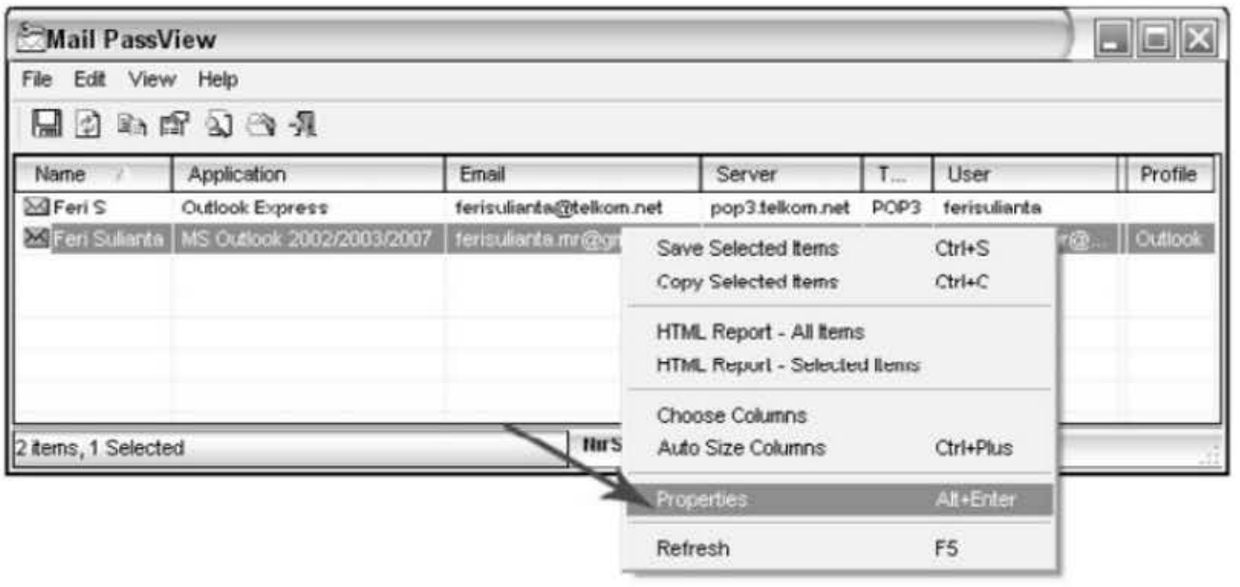
Gambar 8.3 Internet e-mail setting pada Outlook 2007

Caranya mudah saja, yaitu dengan menjalankan file Mailpv.exe, dan otomatis jendela program langsung terbuka dengan informasi mail user dan password-nya. Perhatikan Gambar 8.4, ditampilkan dua account yang ada pada Microsoft Outlook dan Outlook Express.

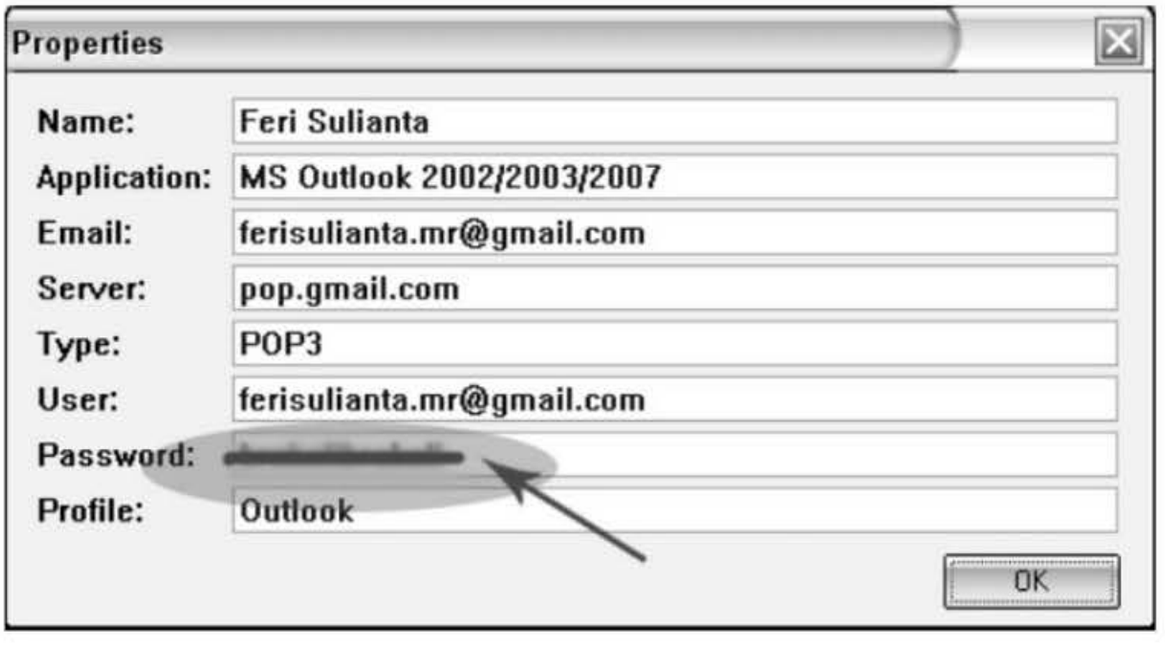
Untuk melihat info detail terhadap masing-masing account yang terjaring, arahkan kursor ke account tersebut > klik kanan > properties (Gambar 8.5), dan hasilnya dapat dilihat pada Gambar 8.6.



Gambar 8.4 Mail PassView ver 1.50



Gambar 8.5 Mail PassView – Pilih Properties



Gambar 8.6 Mail PassView – Info Properties

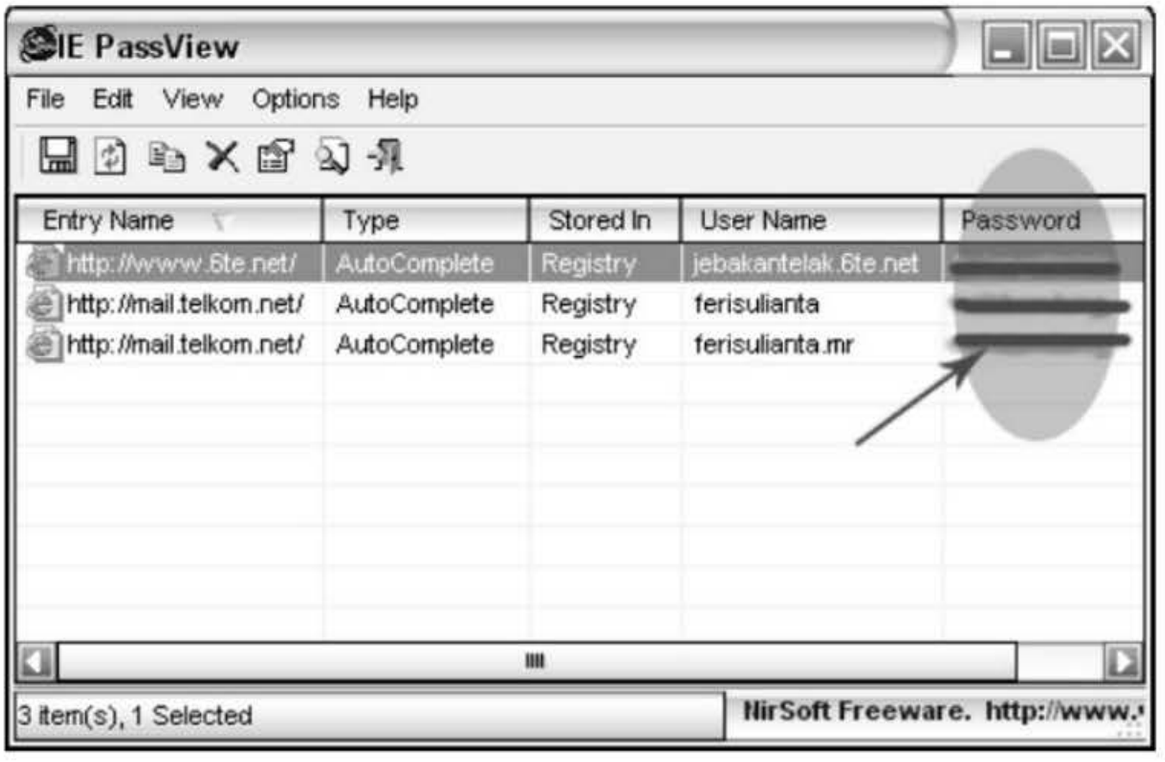
Selain mampu me-recovery password pada Outlook Express dan Microsoft Outlook, Mail PassView juga mampu me-recover email client seperti: Windows Mail, Windows Live Mail, IncrediMail, Eudora, Netscape 6.x/7.x , Mozilla Thunderbird, Hotmail/MSN, dan Gmail.

8.2 Mengungkap Password Internet via Browser Scanner

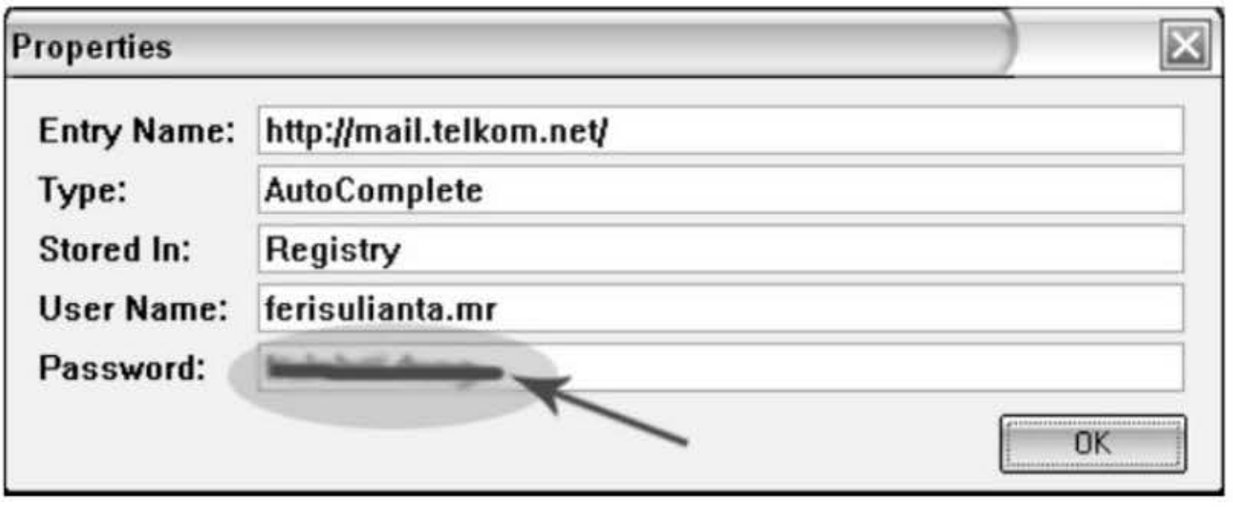
Rekonstruksi password yang digunakan user dalam berselancar dapat dilakukan dengan cara sederhana. Misalnya dengan melakukan scanning terhadap password Internet Explorer, gunakanlah IE PassView. Tidak dibutuhkan proses instalasi untuk menjalankannya, cukup klik ganda fileiepv.exe, maka IE PassView akan melakukan scanning semua password Internet Explorer dan ditampilkan pada jendela program.

Sebenarnya, ada tiga jenis password yang di recover oleh IE PassView, antara lain:

- Password AutoComplete Passwords (catatan: website seperti Yahoo, men-disable fitur AutoComplete untuk menghindari pencurian password user).
- Password HTTP Authentication Password.
- Password FTP Passwords (password pada alamat FTP).



Gambar 8.7 Mail PassView – Menjaring Informasi



Gambar 8.8 Mail PassView – Info Properties

8.3 Cari Tahu Fake E-mail?

Penting untuk mengetahui apakah e-mail yang dialamati pada Anda merupakan e-mail yang berisi informasi yang benar. Karena e-mail kerap kali dijadikan alat hacking. Dan rasa curiga merupakan awal yang baik dalam melatih keahlian forensik.

Misalnya saja, diperlihatkan step by step terhadap aksi hacking terhadap Yahoo!Mail.

Umumnya mereka yang melakukan aksi hacking ini nama account yang tampaknya terpercaya, kalau memungkinkan tambahkan kata-kata Yahoo di bagian lastname atau firstname-nya, atau Anda dapat memakai kata-kata semisal: supervisor, administrator, backup, recovery, dan lainnya.

Dengan demikian, korban akan mempercayai bahwa e-mail tersebut memang adalah e-mail Tim Yahoo! Misalnya dengan: Account_id (firstname) dan Update (lastname), dengan e-mail ID sebagai berikut:

- Update_your_account@yahoo.com
- Accountupdate@yahoo.com
- UpdateAccount2009@yahoo.com
- Administrator2009@yahoo.com

Mereka yang mengirimkan e-mail dengan account tersebut akan merangkai kata-kata untuk meyakinkan bahwa user harus me-reply e-mail tersebut dan mengirimkan passwordnya untuk keperluan update.

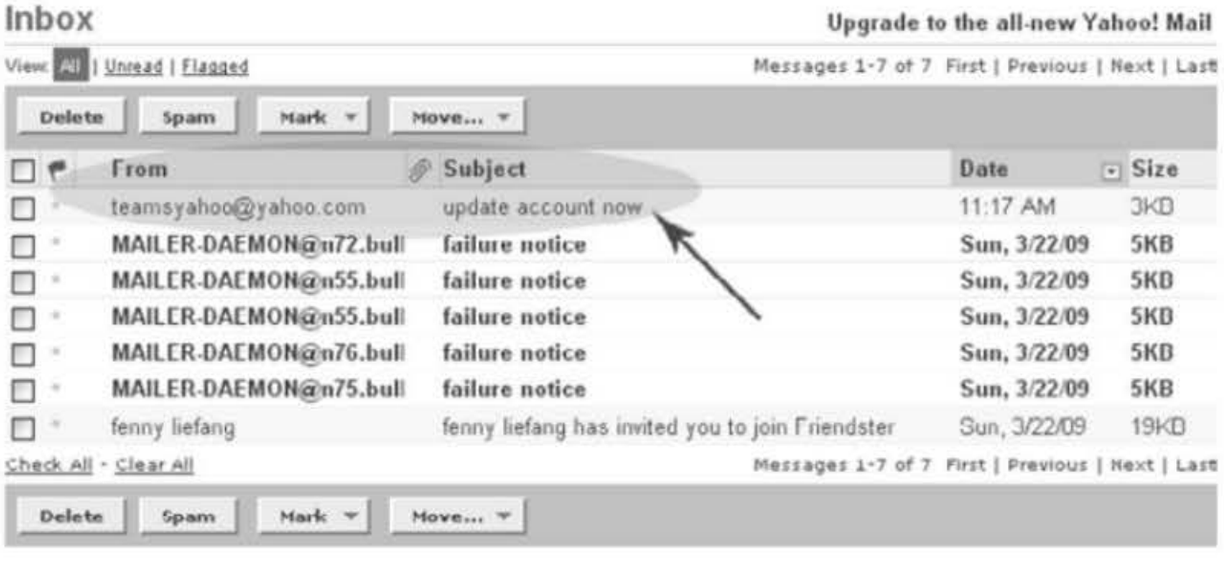
Selain menggunakan hanya sekedar e-mail, mereka pun menggunakan layanan web, aksi ini dikenal dengan istilah Website Spoofing.

Melakukan penelusuran Website Spoofing

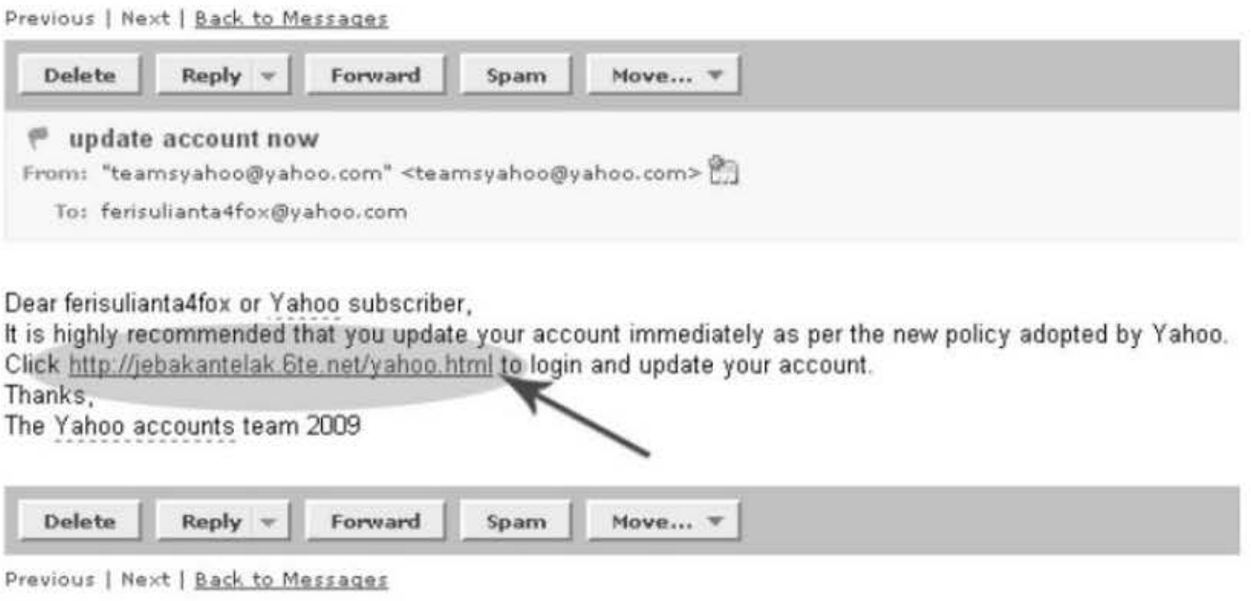
Website spoofing, merupakan suatu aksi membuat website yang ditujukan untuk membuat user tertipu dan salah arah, website ini memiliki antarmuka yang mirip dengan website aslinya, mungkin desain yang mirip dan URL yang juga mirip.

Hacking e-mail menggunakan fake login page terbilang jauh lebih ampuh daripada metode lainnya. Cara ini memang menjadi cara yang digunakan banyak hacker untuk mendapatkan password e-mail.

Si calon korban akan mendapatkan e-mail yang tampaknya sangat meyakinkan (misalnya dari: teamsyahoo@yahoo.com) pada inboxnya.(Gambar 8.9) , dan isi mail tersebut dapat dilihat pada Gambar 8.10.

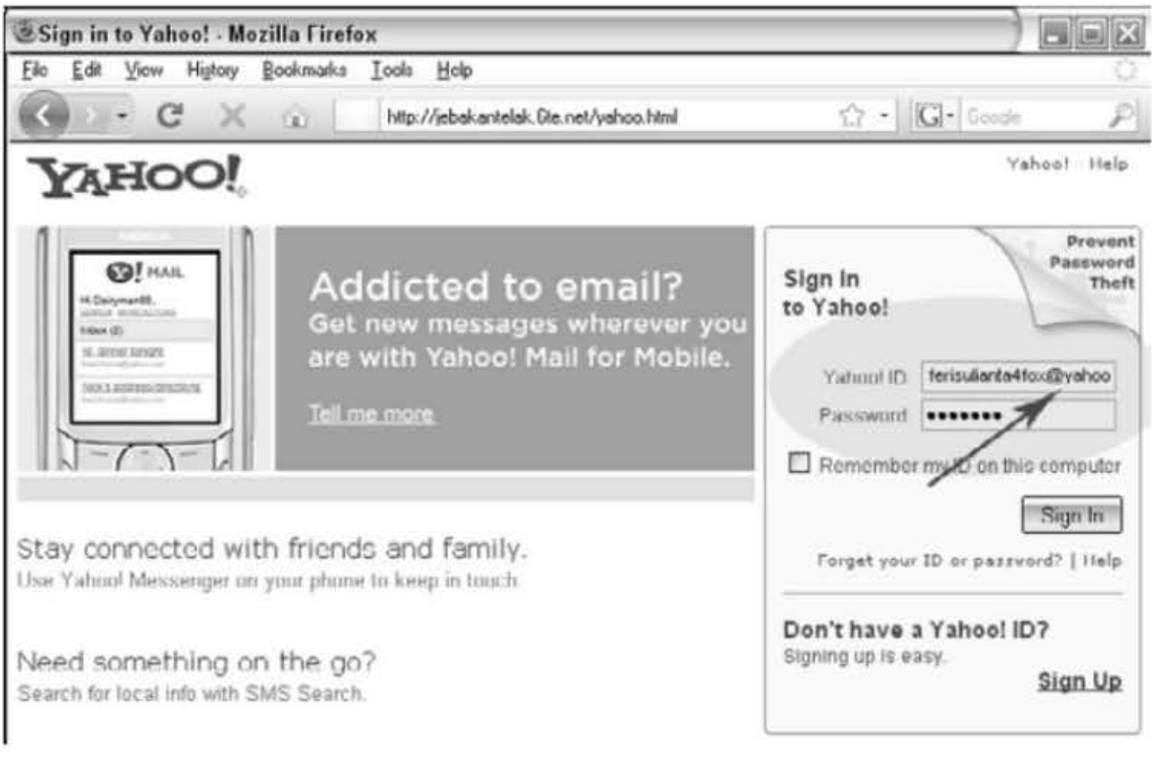


Gambar 8.9 E-mail jebakan diterima



Gambar 8.10 Isi dari E-mail jebakan

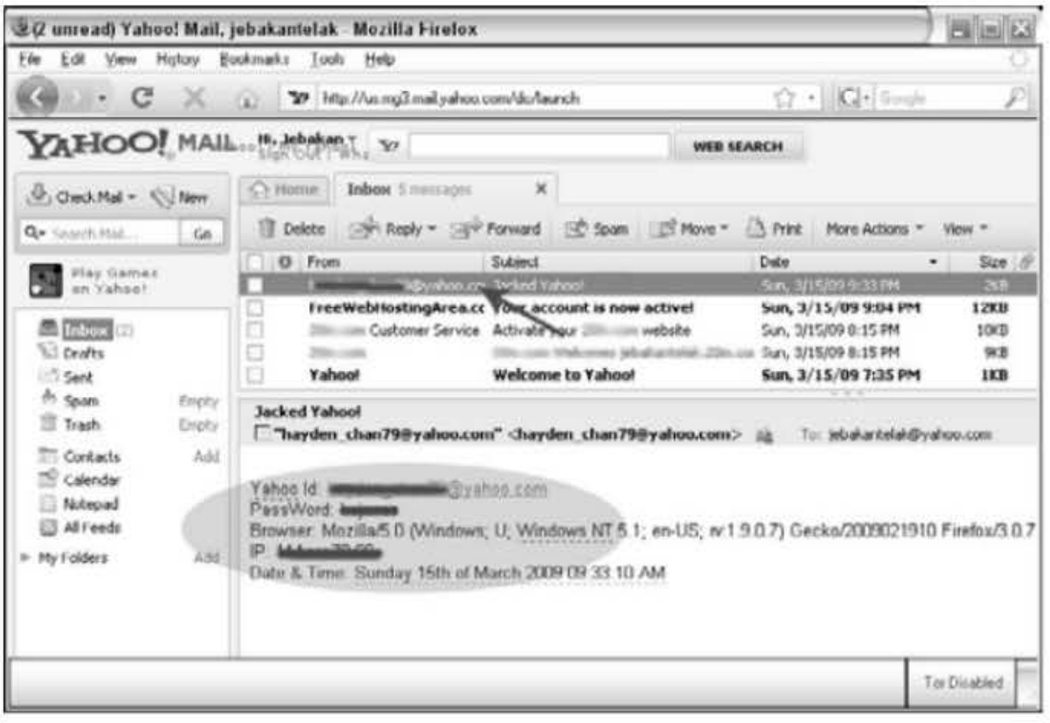
Jika si calon korban terperdaya dan mengklik link tersebut, maka ia akan dibawa ke website yang sudah dibuat dan ternyata si korban melakukan login di website yang palsu (Gambar 8.11), setelahnya korban akan dibawa ke website yahoo asli (Gambar 8.12), korban mungkin tidak menyadarinya.



Gambar 8.11 Web Spoofing – Yahoo!Mail

Gambar 8.12 Website Yahoo!Mail Asli

Sekarang password korban dikirimkan ke e-mail si hacker (Gambar 8.13).



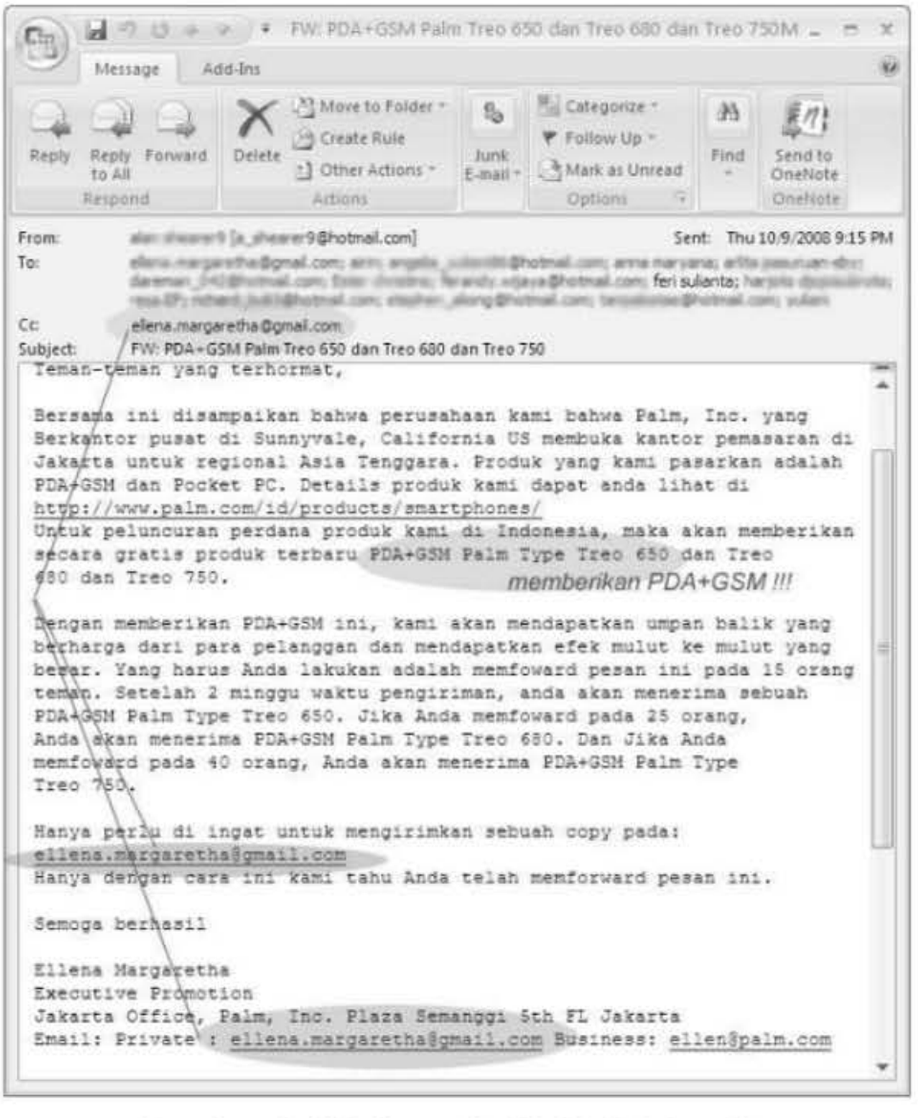
Gambar 8.13 Mail PassView

Lantas, bagaimana melakukan penelusuran aksi kejahatan ini secara teknis? Pada subbab selanjutnya akan diperkenalkan cara membaca mail dalam menilai keabsahan sebuah e-mail.

8.4 Mail Tipuan Sebagai Aksi Mail Flooding?

Cara lain untuk melakukan hack mail adalah dengan membanjiri mail box target dengan e-mail hingga pada akhirnya mailbox si user tidak akan lagi bisa menerima e-mail.

Konsepnya sebenarnya sangat sederhana, yaitu dengan menipu agar orang-orang mau mengirimkan pesan ke banyak teman-temannya, demikian pula teman-teman ke teman-temannya lagi.



Gambar 8.14 Contoh (1) Mail Flooding

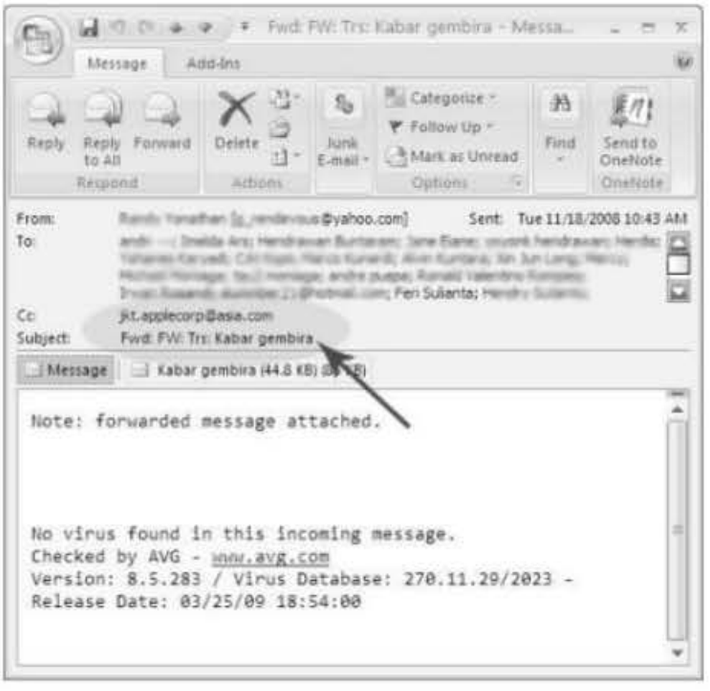
Perhatikan Gambar 8.14 di atas, isi e-mail tersebut untuk mengajak penerimanya agar mengirimkan atau mem-forward e-mail tersebut ke teman-teman dan teman-teman ke teman-temannya lagi, begitu seterusnya.

Isi e-mail tersebut formal dan cukup meyakinkan bahwa jika mem-forward ke 15 orang teman, dalam jangka waktu relatif singkat si pengirim e-mail akan mendapatkan secara gratis produk terbaru PDA + GSM Palm Type Treo 650, Treo 680, dan Treo 750.

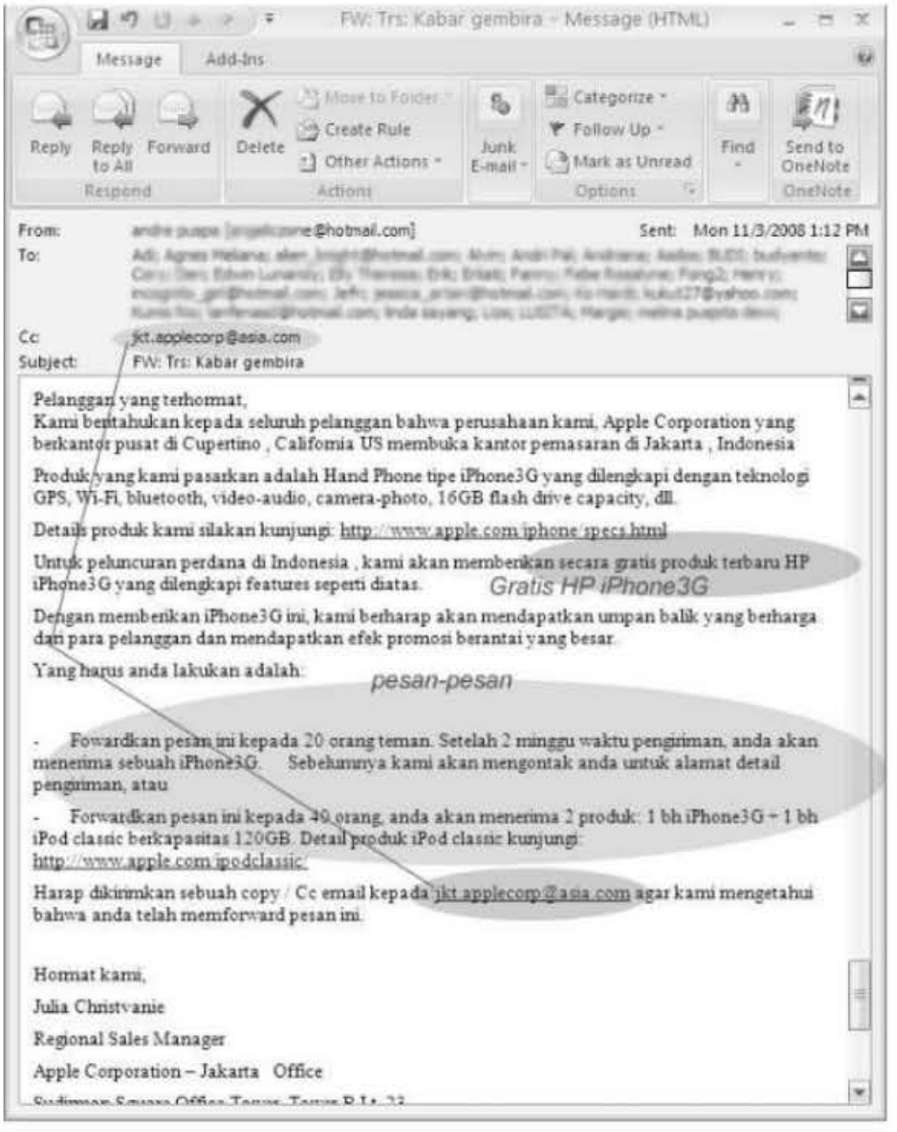
Padahal, barang yang dijanjikan tidak akan pernah didapatkan, tetapi teman-teman dari teman-teman Anda terus mengirimkan pesan diikuti CC ke alamat e-mail target.

Dapat dipastikan dalam jangka waktu tidak berapa lama mail box target (alamat e-mail pada CC) meskipun berkapasitas 1 GB akan overload dan tidak bisa menerima e-mail yang sebenarnya ia butuhkan/tunggu. Inilah Mail Flooding, suatu aksi untuk membanjiri mail box seseorang, sehingga tidak lagi bisa difungsikan untuk menerima e-mail.

Lain lagi dengan Gambar 8.15 dan Gambar 8.16, yang menawarkan gratis produk terbaru HP iPhone3G, padahal domain e-mail target (@asia.com)-perusahaan travel, tidak ada sedikitpun yang berhubungan dengan perusahaan Apple. Tetapi, e-mail tersebut tampak menyakinkan dan banyak orang tertipu! Amat mudah mengalamati aksi penipuan ini, tetapi yang menarik adalah penelusuran terhadap dampak pada target terkait aksi ini.



Gambar 8.15 Contoh (2a) Mail Flooding

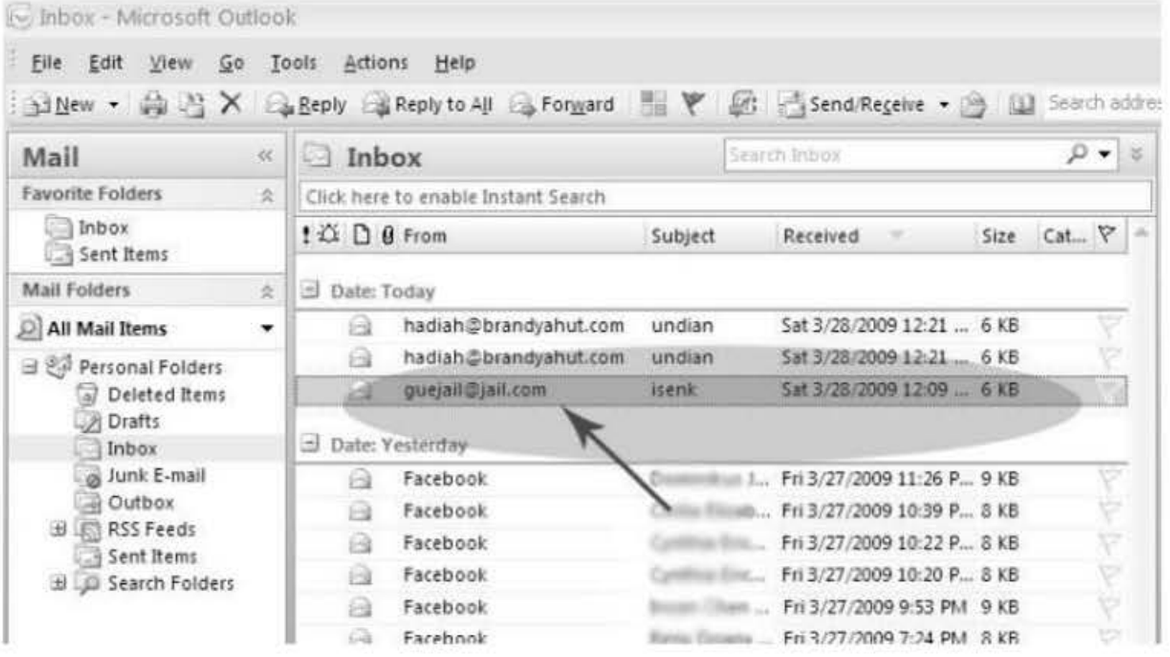


Gambar 8.16 Contoh (2b) Mail Flooding

Melakukan penelurusan E-mail (Tracing E-mail):

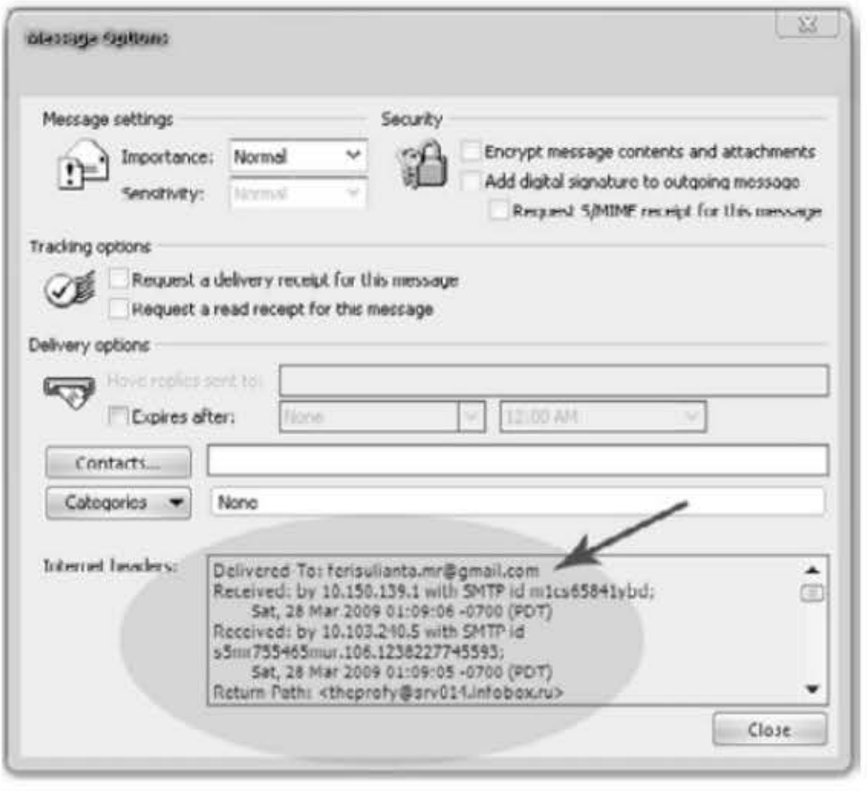
E-Mail Header-karena alamat e-mail bisa menipu, apalagi informasi yang terkandung di dalamnya sangatlah minim, maka dari itu Anda harus membacanya pada e-mail header.

Misalnya saja, ingin tahu perihal asal usul e-mail yang diterima (Gambar 8.17 dan Gambar 8.18), siapa sebenarnya pengirimnya? Alamat E-mail address-nya pun tampak aneh dan mencurigakan. E-mail berikut diterima oleh ferisulianta.mr@gmail.com dan kita akan melihat siapa pengirimnya.



Gambar 8.17 Mail pada Inbox

Gambar 8.18 Isi E-mail



Gambar 8.19 Melihat E-mail Header

Anggap saja e-mail header telah dibuka (Gambar 8.19), sebagai berikut:

```
Delivered-To: ferisulianta.mr@gmail.com

Received: by 10.150.139.1 with SMTP id m1cs65841ybd;

 Sat, 28 Mar 2009 01:09:06 -0700 (PDT)

Received: by 10.103.240.5 with SMTP id
s5mr755465mur.106.1238227745593;

 Sat, 28 Mar 2009 01:09:05 -0700 (PDT)

Return-Path: <theprofy@srv014.infobox.ru>

Received: from out-relay-02.mailcluster.net (out-relay-
02.mailcluster.net [77.221.130.195])

 by mx.google.com with ESMTP id
b9si4863959mug.32.2009.03.28.01.09.05;

 Sat, 28 Mar 2009 01:09:05 -0700 (PDT)

Received-SPF: neutral (google.com: 77.221.130.195 is
neither permitted nor denied by best guess record for
domain of theprofy@srv014.infobox.ru) client-
ip=77.221.130.195;

Authentication-Results: mx.google.com; spf=neutral
(google.com: 77.221.130.195 is neither permitted nor
denied by best guess record for domain of
theprofy@srv014.infobox.ru)
smtp.mail=theprofy@srv014.infobox.ru
```

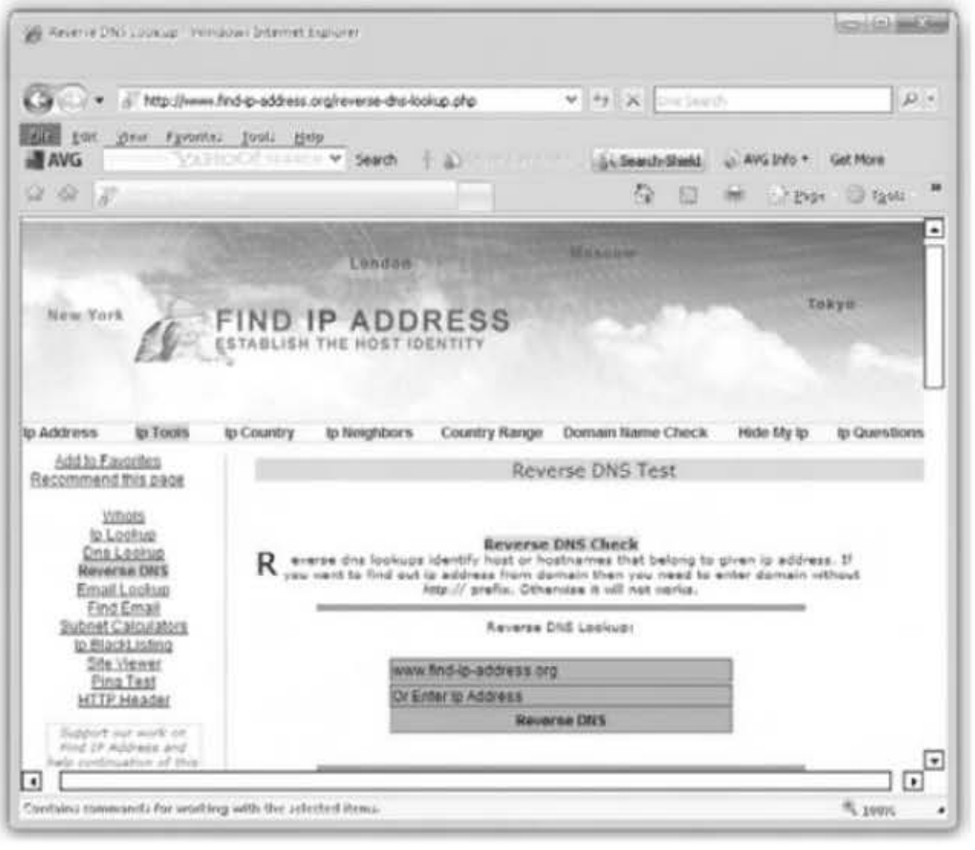
```
Received: from srv014.infobox.ru (srv014.infobox.ru
[77.221.130.14])
      by out-relay-02.mailcluster.net (Postfix) with
ESMTP id 89727400EF06
      for <ferisulianta.mr@gmail.com>; Sat, 28 Mar 2009
11:08:52 +0300 (MSK)
Received: by srv014.infobox.ru (Postfix, from userid
1075)
      id 96ABC50003E5; Sat, 28 Mar 2009 11:09:00 +0300
(MSK)
To: ferisulianta.mr@gmail.com
Subject: =?UTF-8?b?aXNlbms=?=
X-Mailer: mail.anonymizer.name
From: <guejail@jail.com>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="123822773449cddb1685e22"
Message-Id:
<20090328080901.96ABC50003E5@srv014.infobox.ru>
Date: Sat, 28 Mar 2009 11:09:00 +0300 (MSK)
```

Ada beberapa paragraf yang diawali dengan Received Tag, masing-masing tag tersebut ditambahkan pada e-mail header oleh e-mail server seiring e-mail yang bersangkutan ditransmisikan dari **sender (pengirim) ke (receiver) penerima.**

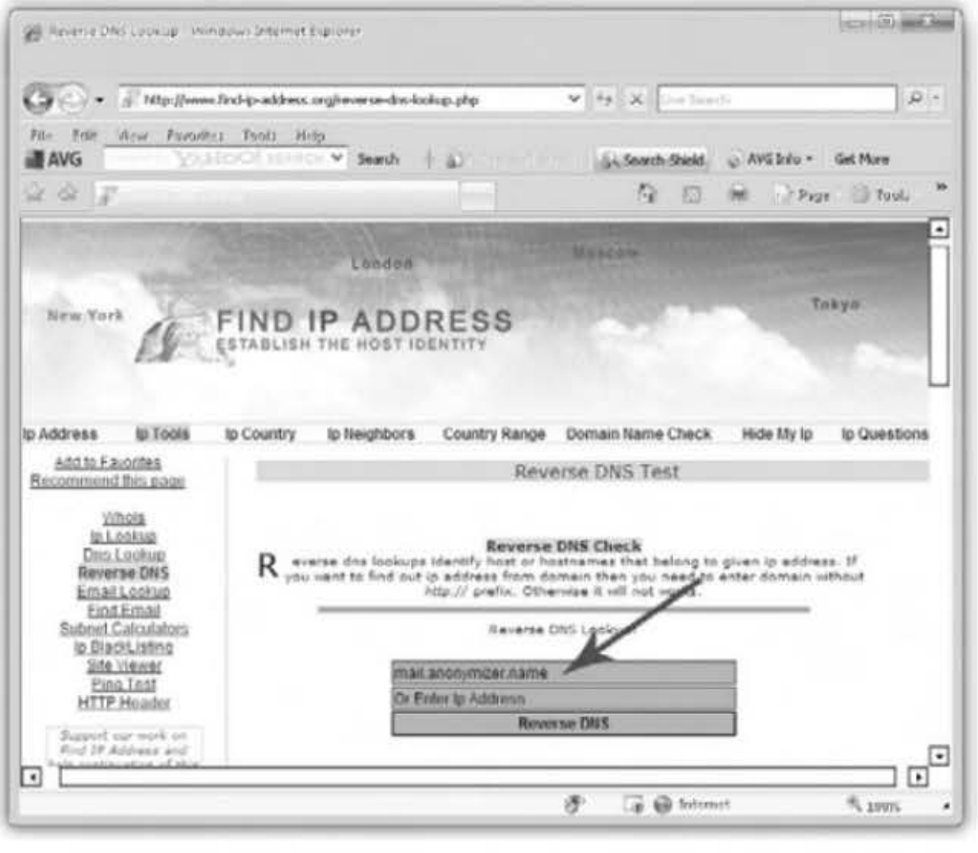
Perhatikan saja tag Received yang ditulis miring, dapat dilihat bahwa e-mail dikirim via **srv014.infobox.ru** yang **IP nya adalah 77.221.130.14** . E-mail tersebut dikirim menggunakan SMTP < with ESMTP id > dari e-mail Server ini: out-relay-02.mailcluster.net. Perhatikan **tag X-Mailer**, e-mail tersebut dikirim menggunakan: **mail.anonymizer.name.**

Tetapi apa IP Addressnya, Anda dapat mengunakan layanan pada website **http://www.find-ip-address.org/reverse-dns-lookup.php**, yang akan melakukan modus reverse dalam mencari IP Address via Domain Name. (Gambar 8.20)

Masukkan 'mail.anonymizer.name' dan klik Reverse DNS (Gambar 8.21).



Gambar 8.20 Website find-ip-address.org



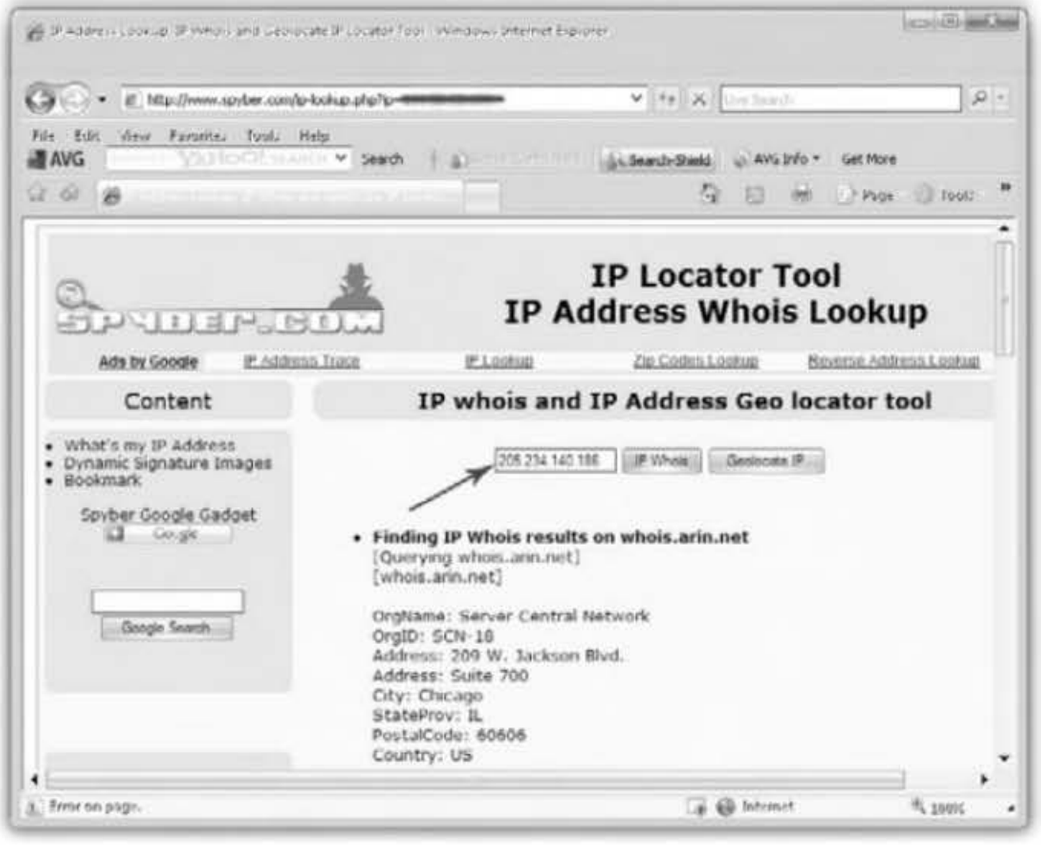
Gambar 8.21 Website find-ip-address.org - Input Domain

Gambar 8.22 Website find-ip-address.org – resolve IP

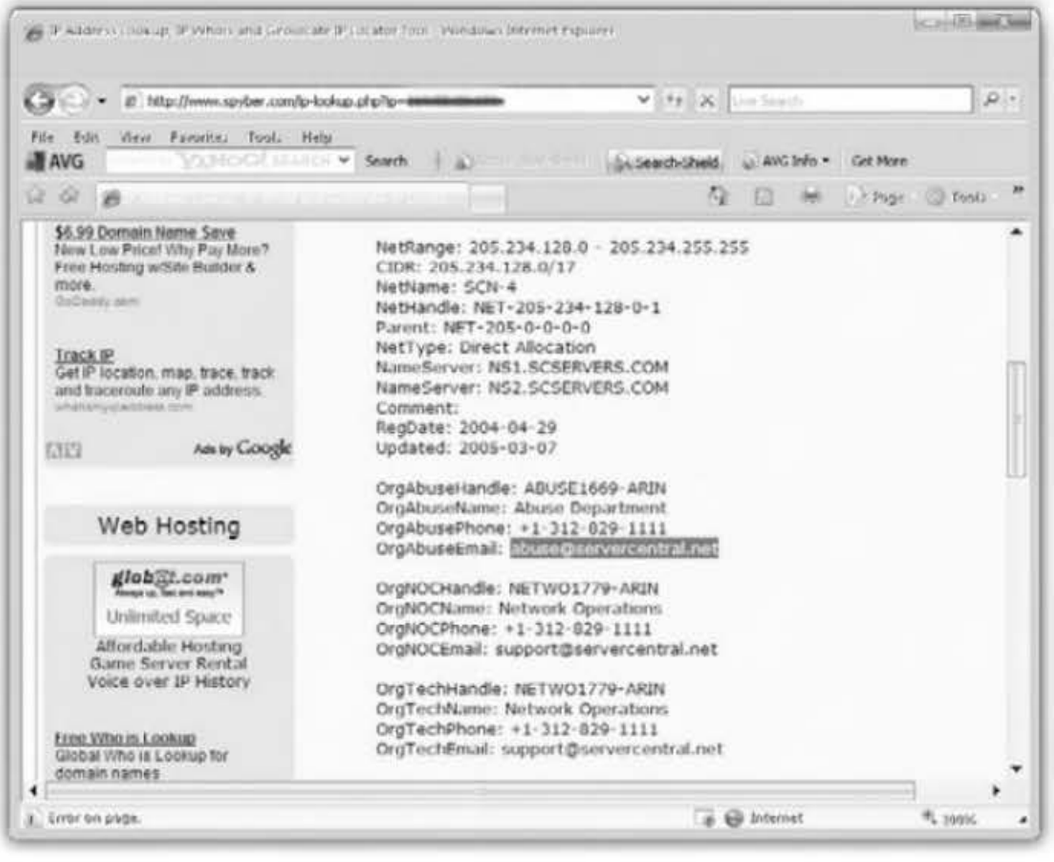
Hingga diketahui bahwa Domain Name **mail.anonymizer.name** mengacu pada **Ip Address 205.234.140.186** (Gambar 8.22). Untuk melacak lebih jauh siapa yang bertanggung jawab terhadap IP tersebut, gunakan layanan pada spyber.com. Input-kan IP Address-nya dan klik tombol IP Whois, hasilnya adalah: **Server Central Network** yang berlokasi di **Chicago**, di sana pun tertera informasi kontaknya (Gambar 8.23 dan Gambar 8.24).

Anda dapat mengontak alamat e-mail tersebut (Gambar 8.24) untuk pengaduan lebih lanjut. Tetapi sebelum bertindak jauh, berdasarkan pembacaan e-mail header, ternyata website mail.anomymizer.name-lah yang digunakan oleh si pelaku (Gambar 8.25), di sana ada juga e-mail kontak yang dapat Anda gunakan sebagai langkah awal untuk pelaporan.

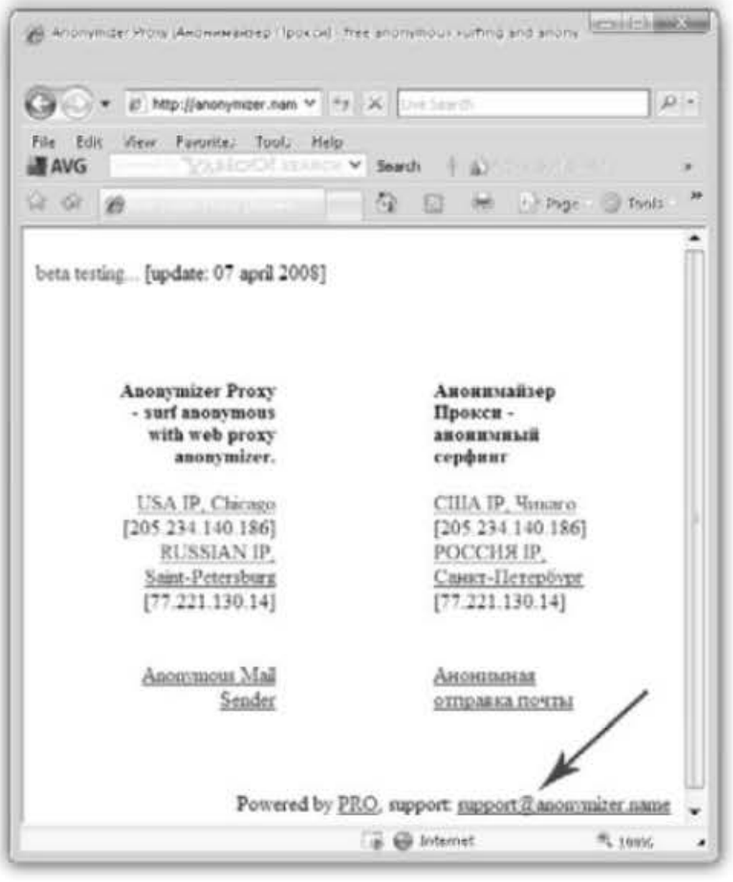
Karena pastinya Alamat IP si pengirim tercatat dan dapat digunakan untuk pelacakan jika memang kasusnya sangat 'krusial'. Jadi, apa pun itu yang Anda lakukan, pengguna internet, atau para Hacker atau apa pun itu, ada jejak-jejak yang selalu ditinggalkan! Disinilah penelusuran forensik semakin terasa menarik.



Gambar 8.23 Website Spyber.com – Hasil IP whois (1)



Gambar 8.24 Website Spyber.com– Hasil IP whois (2)



Gambar 8.25 Website Anonymizer.name

8.5 Tracing Aksi Spy

Mata-mata bisa didapati di manapun, tanpa kita sadari komputer yang digunakan sudah terpasang program pengintaian. Terlebih lagi jika menggunakan komputer di tempat umum, resiko pengintaian semakin tinggi.

Salah jika Anda segera membuang aplikasi yang menurut Anda adalah Spyware tanpa mengidentifikasi aplikasi yang diduga spyware dengan seksama.

Kiat pengamanan spy yang penting diketahui!

Sebenarnya ada beberapa tips praktis agar kita lebih waspada dan terhindar dari modus pengintaian, antara lain:

- Tidak pernah menggunakan komputer publik untuk keperluan personal, misalnya mengakses e-mail, jejaring sosial, aplikasi perbankan, dan lainnya.

- Selalu waspada jika didapati perangkat keras terpasang tanpa fungsi yang kita ketahui.
- Perhatikan dengan seksama aplikasi apa saja yang terinstal di komputer, termasuk pula aplikasi yang berjalan di-background. Jika ada yang mencurigakan, maka jangan gunakan komputer tersebut.
- Melakukan pengecekan dengan menginstal program Anti-Spy atau Anti-Keylogger terlebih dahulu sebelum menggunakan komputer orang lain atau komputer publik.

Kiat pengamanan tersebut akan efektif untuk diterapkan, tetapi kita tidak dapat menghindar untuk tidak menggunakan komputer publik pada saat-saat tertentu.

Komputer bekas yang kita beli pun bisa terinstall banyak *software spy*. Pilihan termudah adalah proses install ulang yang menyita waktu lama. Bahkan komputer kita pun bisa saja terpasang software spy tanpa kita sadari, misalnya melalui *spyware* yang ter-download sewaktu berselancar di internet atau *malware* yang menjangkiti komputer.

Bahkan jika tidak memungkinkan, install ulanglah terhadap komputer yang sudah digunakan orang lain sebelumnya, maka analisa akan perangkat lunak yang terinstal tampaknya perlu diperiksa keabsahannya.

Memeriksa sistem yang berisi spyware

Untuk mencari tahu keberadaan software spy berada, ada beberapa lokasi yang dapat dijadikan taget pencarian. Sebagai langkah awal, identifikasi dapat dilakukan menggunakan utilitas bawaan Windows yang akan menampilkan aplikasi yang menggunakan sumber daya sistem komputer. Jika didapati program yang asing, maka penelusuran lebih lanjut dapat dilakukan.

Biasanya, *software spy* bisa menempel pada systray, terlihat pada proses page frame windows task manager dan resource monitor. Pada resource monitor akan terlihat sumber daya processor serta memori yang digunakan oleh aplikasi spy dalam memata-matai.

Mari kita mencari aplikasi spy pada komputer dengan mengikuti langkah-langkah berikut.

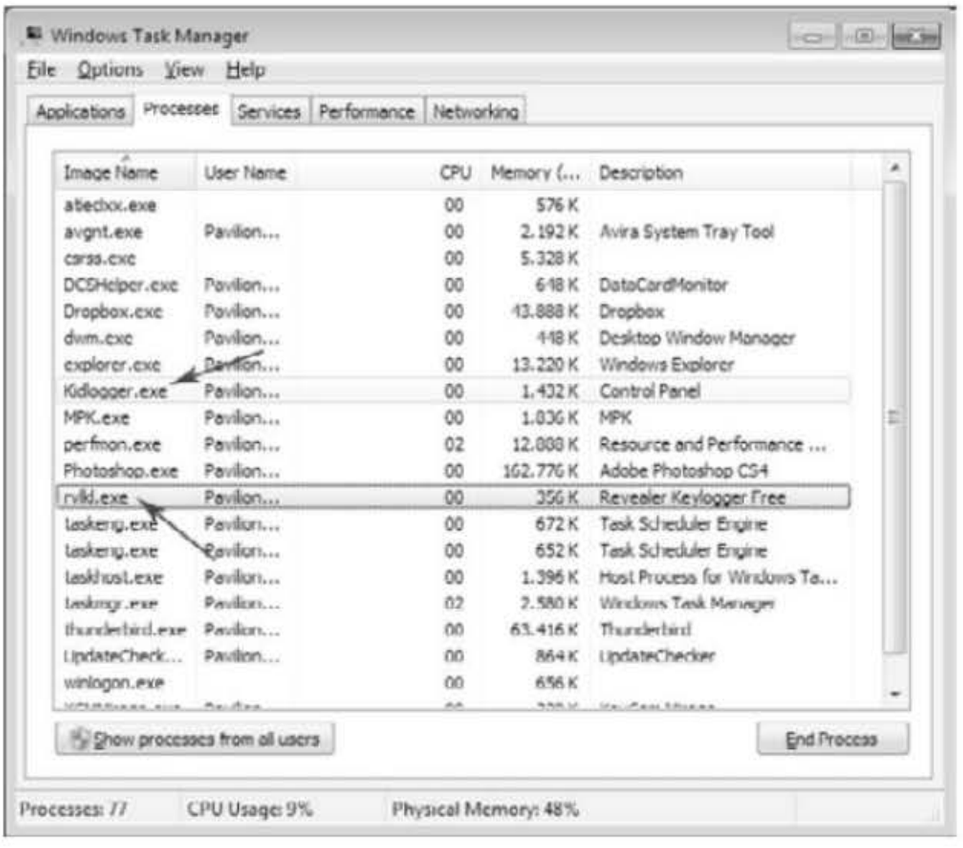
Gambar 8.26 Aplikasi keylogger pada systray

Kadang aplikasi spy yang tidak terpasang rapi, amat mudah terlihat pada systray. Untuk melihatnya klik saja icon segitiga pada taskbar di sudut kanan. Gambar 8.26.

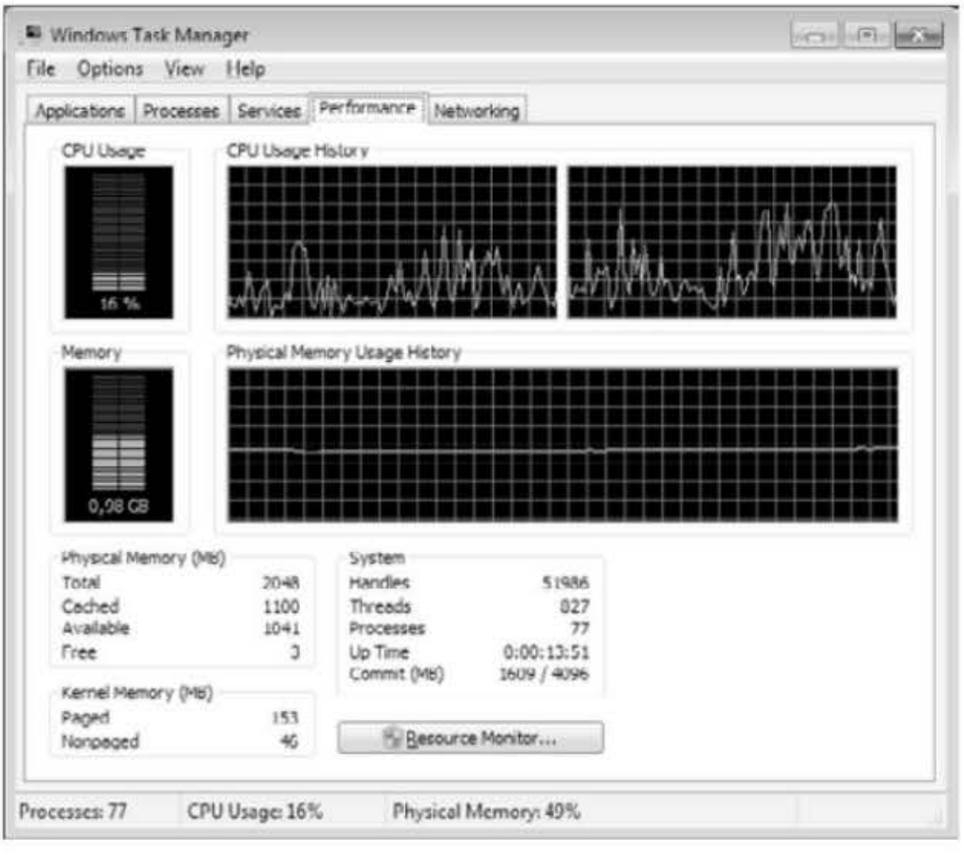
Jika keylogger atau aplikasi pengintai tidak didapati pada systray, cara lain yang biasanya efektif yaitu dengan mengakses task manager. Perhatikan langkahnya sebagai berikut:

Gambar 8.27 Tekan Ctrl+Alt+Del > Start Task Manager

Dengan mengakses Windows Task Manager, dapat terlihat berbagai aplikasi yang berjalan dalam sistem, termasuk pula aplikasi pengintaian.

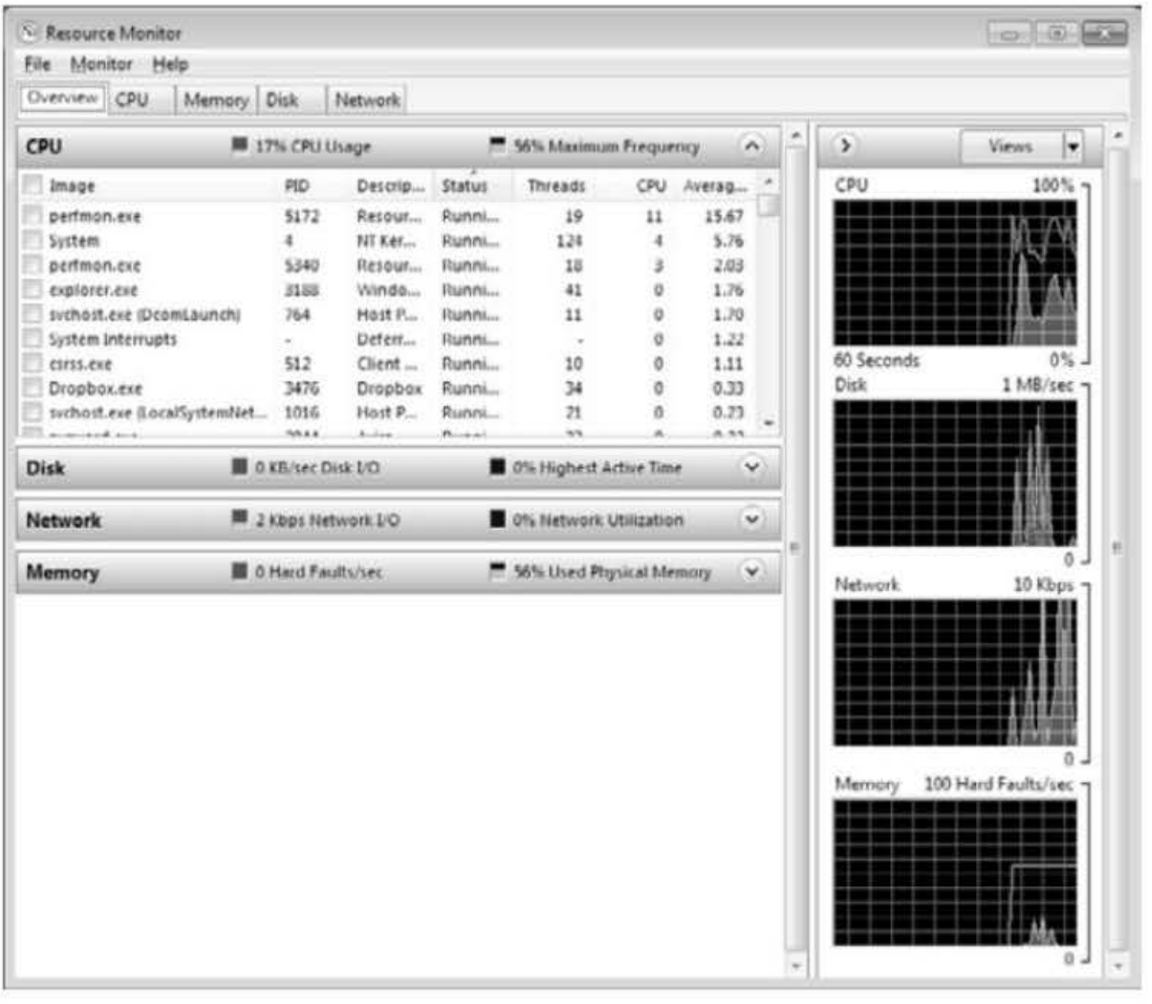


Gambar 8.28 Aplikasi Spy KidLogger dan Revealer pada Task Manager



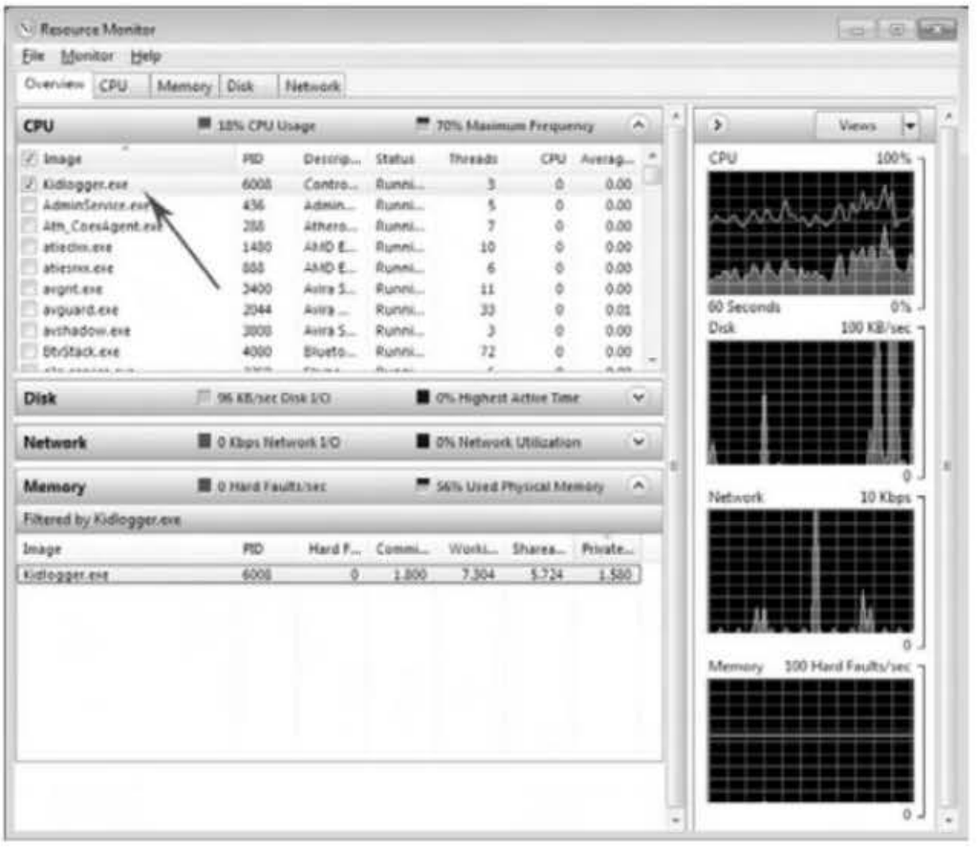
Gambar 8.29 Pageframe Performance untuk melihat penggunaan processor oleh program komputer

Gambar 8.29. Klik Tombol Resource Monitor untuk melihat beberapa sumber daya komputer yang digunakan oleh software spy.



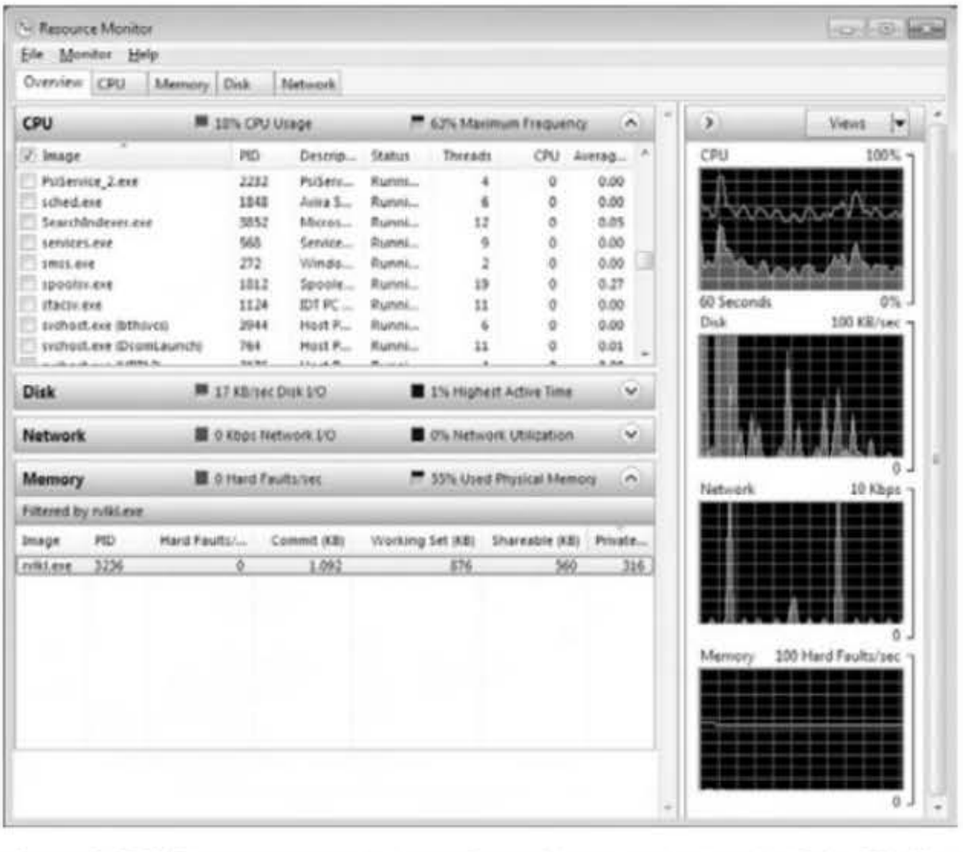
Gambar 8.30 Kotak dialog Resource Monitor

Pada kolom image, akan diidentifikasi aplikasi pengintaian yang ditemukan pada windows task manager. Antara lain: KidLogger dan Revealer KeyLogger.



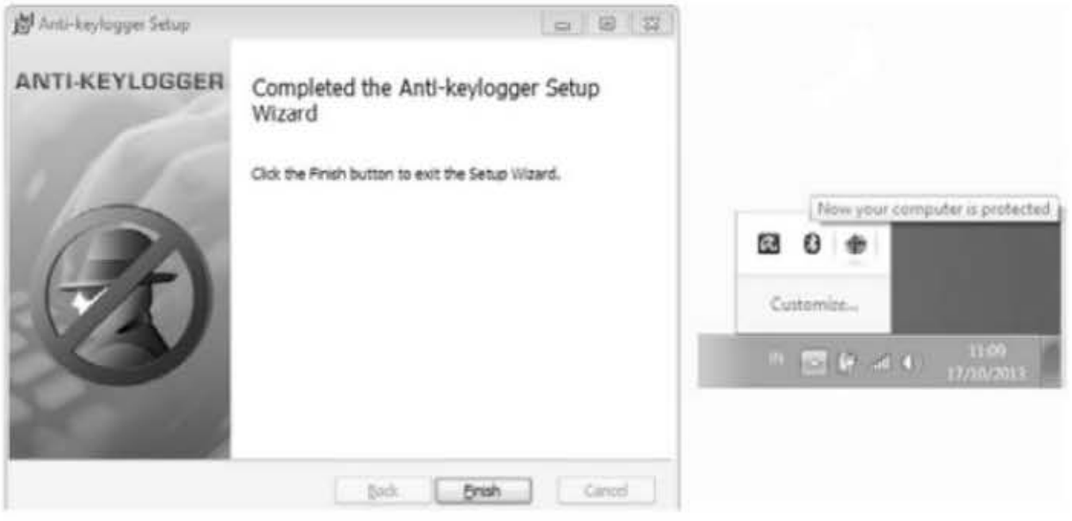
Gambar 8.31 Aplikasi KidLogger pada Resouce Monitor yang menggunakan sumber daya processor sistem komputer

Untuk melihat kapasitas memori yang dipakai, klik kolom bar Memory.

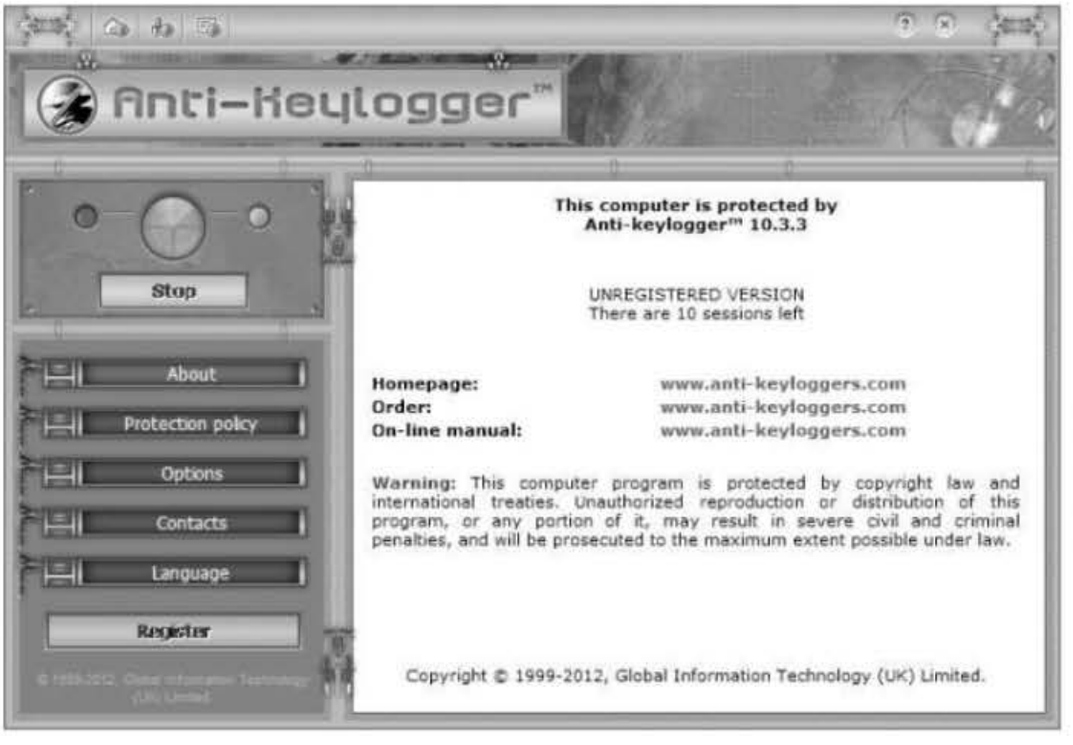


Gambar 8.32 Penggunaan sumber daya memori oleh KidLogger

Jika tadi diperlihatkan cara untuk menemukan aplikasi pengintaian secara manual, maka ada aplikasi khusus Anti-KeyLogger yang dapat digunakan untuk mendeteksi software spy secara otomatis dan mudah. Berikut ini adalah cara menggunakan aplikasi Anti-KeyLogger.



Gambar 8.33 Aplikasi Anti-KeyLogger sudah terinstalasi dan ditampilkan pada systray



Gambar 8.34 Antarmuka aplikasi Anti-KeyLogger

Selanjutnya, aplikasi ini akan digunakan untuk memantau keberadaan aplikasi pengintaian pada sistem komputer, serta menonaktifkan aplikasi pengintaian yang ditemukan.

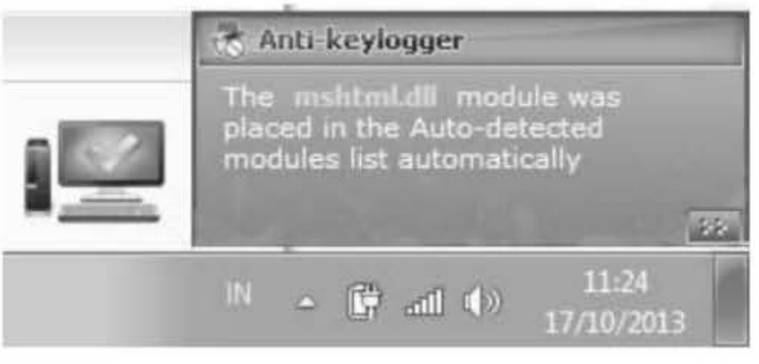
Gambar 8.35 Klik Options untuk melakukan konfigurasi Anti-KeyLogger

Pada Gambar 8.35, pengguna dapat membuat pengaturan modus deteksi dan perilaku Anti-KeyLogger sewaktu menemukan aplikasi pengintaian dan keberadaan aplikasi Anti-KeyLogger, misalnya aplikasi Anti-KeyLogger tetap ingin dimunculkan pada systray.

Gambar 8.36 Klik Protection Policy yang akan menampilkan modul yang diduga aplikasi pengintaian

Modul aplikasi pengintaian ini dapat dinonaktifkan, dengan mencentang modul pengintaian yang ditemukan. Secara default, aplikasi yang diduga spy akan di-disabled. Gambar 8.36.

Gambar 8.37 Dengan mengklik tombol disabled maka Aplikasi KidLogger akan kembali beroperasi (enabled)



Gambar 8.38 Warning dari Anti-Key Logger yang mendapati adanya aplikasi spy

Dalam kasus-kasus yang di atas, cara bernalar komputer forensik akan diimplementasikan pada rekonstruksi informasi dan caranya menangani problematika dan proses mengidentifikasi kejadian. Tidak ada tindakan 'breaking dan entering' yang akan mengobrak-abrik sistem, bahkan tidak diperlukan software forensik khusus dalam merekonstruksi informasi.

Hal inilah yang menjadi dasar bagaimana keahlian seorang ahli forensik dilatih. Yakni memahami perangkat serta proses teknologi informasi, dan bagaimana menangani kasus yang melibatkan proses forensik yang tidak merusak evidence.

BAB 9
KAMUS KOMPUTER FORENSIK

Akronim Komputer Forensik:

A

ADS: Alternate Data Stream

ARIN: American Registry for Internet Numbers

ARP: Address Resolution Protocol

ASCII: American Standard Code for Information Interchange

ATA: Advanced Technology Attachment

B

BIOS: Basic Input/Output System

C

CCIPS: Computer Crime and Intellectual Property Section

CD: Compact Disc

CD-R: CD-Recordable

CD-ROM: CD-Read Only Memory

CD-RW: CD-Rewritable

CDFS CD: File System

CFI: Computer and Financial Investigations

CFRDC: Computer Forensics Research and Development Center CFTT Computer Forensics Tool Testing

CMOS: Complementary Metal Oxide Semiconductor

CSI: Crime Scene Investigator

CVE: Common Vulnerabilities and Exposures

D

DBMS: Database Management System

DDoS: Distributed Denial of Service

DHCP: Dynamic Host Configuration Protocol

DLL: Dynamic Link Library

DNS: Domain Name System

DoD: Department of Defense

DVD: Digital Video Disc or Digital Versatile Disc

DVD-R: DVD-Recordable

DVD-ROM: DVD Read Only Memory

DVD-RW: DVD Rewriteable

E

ESP: Encapsulating Security Payload

ext2fs: Second Extended Filesystem

ext3fs: Third Extended Filesystem

FACCI: Florida Association of Computer Crime Investigators

F

FAT: File Allocation Table

FBI: Federal Bureau of Investigation FIPS Federal Information Processing Standards

F.I.R.E.: Forensic and Incident Response Environment

FISMA: Federal Information Security Management Act

Forensic Science: Pengaplikasian ilmu pengetahuan pada perundangan/ hukum

FLETC: Federal Law Enforcement Training Center

FTP: File Transfer Protocol

G

GB: Gigabyte

GUI: Graphical User Interface

D-1GUIDE TO INTEGRATING FORENSIC TECHNIQUES INTO INCIDENT RESPONSE

H

HFS: Hierarchical File System

HPA: Host Protected Area

HPFS: High-Performance File System

HTCIA: High Technology Crime Investigation Association

HTTP: Hypertext Transfer Protocol

I

IACIS: International Association of Computer Investigative Specialists

ICMP: Internet Control Message Protocol

ICS: Internet Connection Sharing

ID: Identification

IDE: Integrated Drive Electronics

IDS: Intrusion Detection System

IGMP: Internet Group Management Protocol

IM: Instant Messaging

IMAP: Internet Message Access Protocol

IOS: Internetwork Operating System IP Internet Protocol

IPsec: Internet Protocol Security

IR: Interagency Report

IRC: Internet Relay Chat

IRQ: Interrupt Request Line

ISO: International Organization for Standardization

ISP: Internet Service Provider

IT: Information Technology

ITL: Information Technology Laboratory

J

JPEG: Joint Photographic Experts Group

K

KB: Kilobyte

L

LACNIC: Latin American and Caribbean IP Address Regional Registry

M

MAC: Media Access Control

MAC: Modification, Access, and Creation

MB: Megabyte

MD: Message Digest

MISTI: MIS Training Institute

MMC: Multimedia Card

MO: Magneto Optical

MS-DOS: Microsoft Disk Operating System

N

NAT: Network Address Translation

NFAT: Network Forensic Analysis Tool

NFS: Network File Sharing

NIC: Network Interface Card

NIJ: National Institute of Justice

NIST: National Institute of Standards and Technology

NLECTC-NE: National Law Enforcement and Corrections Technology Center.North East

NSRL: National Software Reference Library

NTFS: Windows NT File System

NTI: New Technologies Inc.

D-2GUIDE TO INTEGRATING FORENSIC TECHNIQUES INTO INCIDENT RESPONSE

NTP: Network Time Protocol

NW3C: National White Collar Crime Center

O

OEM: Original Equipment Manufacturer

OMB: Office of Management and Budget

OS: Operating System

OSI: Open Systems Interconnection

OSR2: OEM Service Release 2

P

PCMCIA: Personal Computer Memory Card International Association

PDA: Personal Digital Assistant

POP3: Post Office Protocol 3

R

RAID: Redundant Arrays of Inexpensive Disks

RAM: Random Access Memory

RCFL: Regional Computer Forensics Laboratory

RFC: Request for Comment

RIPE NCC: RÈseaux IP EuropÈens Network Coordination Centre

S

SAM: Security Account Manager

SCSI: Small Computer System Interface

SD: Secure Digital

SDMI: Secure Digital Music Initiative SEM Security Event Management SFTP Secure FTP

SHA-1: Secure Hash Algorithm 1

SIP: Session Initiation Protocol

SMB: Server Message Block

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SP: Special Publication

SSH: Secure Shell

SSL: Secure Sockets Layer

Steganography: Menumpangkan data dengan data lain untuk penyembunyian.

T

TB: Terabytes

TCP: Transmission Control Protocol TCP/IP Transmission Control Protocol/Internet Protocol

TUCOFS: The Ultimate Collection of Forensic Software

U

UDF: Universal Disk Format

UDP: User Datagram Protocol

UFS: UNIX File System

UPS: Uninterruptible Power Supply URL Uniform Resource Locator

USB: Universal Serial Bus

V

VoIP: Voice Over IP

VPN: Virtual Private Network

Z

ZIF: Zero Insertion Force

Istilah Komputer Forensik:

Berikut ini adalah perbendaharaan kata perihal teknologi informasi dan beberapa kata lainnya yang berkembang dikarenakan kebutuhan dalam dunia komputer forensik.

A

Alamat: Atau disebut sebagai Address, umumnya digunakan dalam Internet Address, E-mail Address (Alamat E-mail), Web Page Address/ Alamat Web Page (URL).

Akuisisi: Prosesi duplikasi media untuk keperluan forensik.

Analisis: Langkah ketiga dalam proses komputer forensik, menyangkut pula metode dan teknik yang berkaitan dengan perundangan/hukum.

Anti Forensik: Teknik yang dilakukan untuk menghilangkan data dan fakta, sehingga menutup kemungkinan didapatkannya fakta dari proses Forensik, misalnya menghapus file pada recycle bin, memformat media penyimpanan atau merusak media penyimpanan secara fisik.

B

Best Evidence Rule: berbagai konten mencakup dokumen tertulis, rekaman audio, video, foto yang digunakan sebagai bukti.

BIOS: Basic Input Output System.

Bit: Unit terkecil dari data yang direpresentasikan dalam digit biner.

Bit Stream Imaging: Bit-Bit Copy dari original media, mencakup free space, slack space. Dikenal pula dengan disk Imaging.

C

Cache: Dikenal pula sebagai Cache Memory/memori penyangga, yang menjadi penyangga data. Komponen ini adalah bagian dari CPU.

Chain of Custody: Menelaah bukti-bukti yang didapat dari sumber yang dikatakan original yang nantinya diajukan untuk proses hukum.

C/S Arsitektur: Client/Server Arsitektur, salah satu arsitektur jaringan di mana komputer yang difungsikan menjadi server memberikan layanan sumber daya jaringan terhadap komputer Client.

Cluster: Kumpulan sektor (sector) pada track yang sama.

Collection: Fase pertama dalam komputer forensik, mencakup identifikasi, pelabelan, recording/pencatatan, dan usaha mendapatkan data dari sumber-sumber yang dapat diandalkan dan didasarkan pada panduan dan prosedur.

Copy: Penggandaan yang akurat, bentuk dari reproduksi dari informasi.

Cyberspace: Ruang maya yang terbentuk dari interkoneksi komputer.

CyberCrime: Kejahatan dalam dunia Cyber/Maya. Investigasi yang dilakukan sebagai upaya pencegahan dan mengalamati kejahatan yang menggunakan Cyberscape sebagai medianya, pelaku dikenal dengan sebutan Hacker. Metode yang digunakan mencakup: Tracing, analisa E-mail atau membuat berbagai perangkap.

D

Data: Sebagian kecil dari informasi digital dengan format yang berbeda-beda.

Data File: Lihat File.

Denial of Services Attack (DoS Attcak): Serangan yang ditujukan pada website yang mengakibatkan website tersebut tidak lagi berkemampuan memberikan layanan, tentunya website tidak dapat dikunjungi user lagi.

Digital Forensic: Pengaplikasian ilmu pengetahuan dalam meng-identifikasi, mengumpulkan, menguji, dan menganalisa data, kemudian menghadirkan informasi yang dapat diandalkan, mencakup pula chain of custody sehubungan data. (lihat Chain of Custody).

Direktori: Metoda Pengorganisasian file-file (dikatakan pula sebagai Folder).

Disk to Disk Copy: Mengkopi file yng ada pada suatu media secara langsung ke media lain.

Disk to File Copy: Mengkopi file yng ada pada suatu media ke satu data file logika.

Dongle: Berbagai perangkat keras eksternal, merangkat tambahan seperti memory pada perangkat tertentu. Misalnya: printer laser dengan 8 MB memory terintegasi.

Duplicate Digital Evidence: Penggandaan akurat dari bukti digital.

E

Evidence: Bukti atau Fakta.

F

False Positive: Kesalahan dalam mengklasifikasi kegiatan tidak berbahaya ke dalam tindakan yang dikategorikan ke dalam malicious (malicious: kejahatan atau pengrusakan).

False Negative: Salah dalam pengklasifikasi aktivitas yang tergolong malicious sebagai tindakan yang tidak berbahaya .

File Aktif: File yang dialokasikan pada personal komputer disk drive, server disk drive, dan perangkat keras lainnya semisal laptop. File backup yang di-generate oleh software aplikasi termasuk di dalamnya.

File Arsip: File yang disimpan untuk keperluan pengarsipan, misalnya: File backup dan file arsip disimpan di lokasi/media penyimpanan yang berbeda dari file induknya (Misalnya pada: floppy disk, CD media, hard disk terpisah, dan lainnya).

File backup: File yang diduplikasi untuk keperluan jaga-jaga/darurat seandainya sesuatu terjadi . File backup umumnya disimpan terpisah dari file induk, dalam hal ini file tersebut dibuat manual oleh user. Kadang file backup dibentuk otomatis oleh perangkat lunak aplikasi dan sistem operasi.

File signature: Atribut yang mendefiniskan karakteristik file, mencakup pula file format.

Files: Berbagai data dan informasi yang dikemas dan kemudian disimpan dalam komputer. Lebih lanjut, File-File diorganisasi sedemikian rupa dalam suatu direktori atau folder.

File Allocation Table (FAT): Peta yang memungkinkan sistem operasi menyimpan, mengalokasikan dan mendapatkannya kembali data/ informasi pada media penyimpanan (hard disk). Berbagai sistem operasi memiliki penanganan yang berbeda akan media penyimpanan.

Filename: Nama file yang unik, mengacu pada suatu file tertentu.

Forensically Clean: Media digital dalam kondisi bersih dari berbagai data, bebas malware dan sudah diuji kelayakannya sebelum digunakan.

Free Space: Area pada media penyimpana atau pada memori yang tidak terpakai (belum teralokasi).

H

Hersay Evidence: Pernyataan yang mengajukan fakta dan pembuktian atau kebenaran.

K

Kejahatan Komputer: Lihat Cyber Crime.

KeyLogger: Program komputer yang digunakan untuk memindai informasi secara sembunyi-sembunyi perihal aktivitas user.

Komputer Forensik: Keilmuan yang difungsikan untuk mendapatkan, menyelamatkan data/informasi, dan mendokumentasikan bukti dari berbagai perangkat elektronik, mencakup komputer, pager, PDA (Personal Digital Assistance), kamera digital, telepon selular, dan berbagai media penyimpanan. Ada aturan bagaimana disajikan dan dikumpulkan, untuk dikatakan layak untuk diajukan lebih lanjut ke dalam proses hukum.

Komputer Forensik: Metode mencakup mengumpulkan, penyelamatan informasi, analisa, pengajuan pengadilan/hukum berkenaan bukti yang berhubungan dengan komputer, metode demikian dikembangkan karena kebutuhan eksklusif akibat dari berkembangnya abad komputer/abad dari informasi.

M

MainFrame Architecture: Komputer berkemampuan sangat besar dan diakses melaui terminal-terminal yang tersebar. Mainframe terdahulu hanya menyediakan terminal-terminal tanpa kemampuan pemrosesan, lain halnya sekarang di mana terminal diberikan kemampuan untuk melakukan pemrosesan.

Malware: Malicious software, program-program berbahaya yang dapat mengganggu dan merusak sistem komputer.

Memory card: Dikenal dengan flash memory card, diartikan juga sebagai media penyimpanan yang removeable. Falsh memory tersedia beragam dengan berbagai vendornya, misalnya: Complact Flash (CF), Smart Media (SM), Memory Stick (MS), Multimedia Card (MMC), Secure Digital (SD Card), xD-Picture Card, PCMCIA Type I dan Type II.

Media: Istilah yang tergolong umum dalam menjelaskan perangkat penyimpanan data pada komputer. Yang tergolong media pada kategori ini antara lain: Floppy Disk, Internal Hard disk, CD Media, Tape Backup, Microchips, dan lainnya.

Metadata: Data yang menjelaskan data. Misalnya: pada File System, metadata yang dimaksud menyediakan informasi mengenai isi suatu file.

N

Network Traffic: Komunikasi antar komputer yang terintegrasi pada jaringan melalui suatu media, misalnya via kabel dan nirkabel (wirreless).

Non-Printing Information: Informasi yang di-*embed* pada dokumen elektronik dan tidak disajikan tercetak dalam bentuk hardcopy. Misalnya, perangkat pengolah kata semisal Miscosoft Word atau spreadsheet elektronik semisal Excel yang memungkinkan Anda untuk menyisipkan informasi (misalnya: komentar dan catatan).

Network: Kombinasi perangkat lunak dan perangkat keras yang memungkinkan komputer yang terintegrasi dapat saling berkomunikasi, arsitektur network umumnya digolongkan ke dalam 2 bagian: Peer-to-Peer dan Client/Server Network.

Non-Volatile Data: Data yang ada pada komputer akan hilang jika listrik dipadamkan.

Normalize: Proses dalam mengonversi data ke dalam format tertentu yang lebih kompatibel dengan parameter standar yang telah ditetapkan.

O

Operating System (OS): (i) Perangkat lunak kategori software sistem yang mengendalikan kinerja perangkat keras komputer, sehingga user dapat memanfaatkan sumber daya perangkat keras. Sistem Operasi berada di-lapisan atas dari fisik komputer. (ii) Perangkat lunak komputer yang memungkinkan perangkat keras menjadi satu kesatuan sistem yang bekerja. (iii) Adalah perangkat lunak minimum pembangun sistem komputer.

Original Digital Evidence: Komponen komputer fisik dan data di dalamnya, mungkin didapatkan dari aksi penyitaan.

P

Packet: Unit logika pada jaringan komunikasi (komputer) yang dibuat pada lapisan transport (transport layer OSI).

Packet Sniffer: Perangkat lunak yang melakukan monitoring terhadap lalulintas jaringan dan mampu meng-capture paket-paket yang ditransmisikan, terlepas apakah tergolong jaringan kabel atau wireless.

Partition: Bagian yang dipilah-pilah secara logika dan kemudian diberlakukan seakan-akan media penyimpanan yang terpisah secara fisik.

Peer-to-Peer Network: Salah satu arsitektur jaringan komputer di mana setiap user dengan masing-masing komputernya mengelola file-file miliknya tanpa manajemen terpusat.

Probative Value: Bukti penting yang sangat berguna dalam pemeriksaan.

Prima Facie Evidence: Asusmsi yang dianggap layak berkenaan fakta.

Proses: Program yang dieksekusi.

Q

Query: Statement yang dipakai sebagai ungkapan untuk pencarian atau pertanyaan, istilah ini mengacu pada proses sewaktu meminta informasi pada basis data, search engine, atau direktori indeks pada layanan website.

QWERTY: Jenis keyboard dengan komposisi tombol keyboard yang memiliki susunan tombol beruntun Q-W-E-R-T-Y.

R

RAM: Random Access Memory - media penyimpanan sementara yang volatile (informasi akan hilang jika listrik mati), dan digunakan sebagai komponen utama pemrosesan komputer.

Real Evidence: Bukti yang didapatkan dari objek komputer, dan digunakan untuk inspeksi dan pengujian di pengadilan.

Residual Data: Data-data yang dihapus, tetapi data tersebut tidak sepenuhnya hilang pada media penyimpanan. Karena sewaktu Anda menghapus data dan disimpan pada recycle bin atau sewaktu Anda membersihkan recycle bin, file tersebut masih ada di hard disk, dan ditandai sebagai file yang dihapus saja. File fragmentasi kadang disebut sebagai Residual Data.

Removable Media: Berbagai media yang dengan mudahnya dipasang dan dilepas tanpa kerumitan yang berarti, mencakup media penyimpanan digital seperti: Floppy Disk, CD, DVD, Cartridge, Tape, Multimedia Card.

Reporting: Tahap akhir dalam proses komputer forensik, mencakup pelaporan hasil analisa, penjelasan deskriptif pada tindakan yang diambil, bagaimana perangkat dan prosedur dipilih, menentukan tindakan lain yang mungkin dilakukan (forensik pada data tambahan yang muncul), merekomendasikan pula peningkatan terhadap kebijakan, penuntun, prosedur, peralatan dan hal-hal lain pada proses forensik.

S

Sector: Unit terkecil pada media penyimpanan yang dapat diakses oleh sistem terkomputerisasi.

Software Aplikasi: Perangkat lunak dengan tujuan spesifik bagi user, misalnya perangkat lunak olah kata, perangkat lunak basis data, perangkat lunak lembar kerja elektronik, dan lainnya.

Shareware: Software yang didistribusikan dengan bebas, dan digunakan dengan syarat dan ketentuan berlaku, misalnya untuk keperluan demo dan digunakan dengan rentang waktu yang terbatas.

Sistem Komputer: Mencakup sekumpulan ruang lingkup komputer, secara umum memaksudkan korelasi perangkat keras, perangkat lunak dan user sebagai pengguna, dan lebih spesifik mengacu pada komputer dan komponen yang terintegrasi, seperti komputer dengan berbagai peripheral/device (printer, modem, media penyimpanan, scanner) dan jaringan komputer.

Slack Space: Ruang penyimpanan yang tidak digunakan dan tercipta karena standar serta pembatasan sistem file.

Slack Space: (i) Bagian yang tidak digunakan pada disk cluster, atau (ii) ruang-ruang penyimpanan yang tidak digunakan pada file allocation block atau pada memory page yang mungkin berisi data-data residu.

Standalone: Komputer yang tidak terkoneksi ke jaringan komputer.

System Unit: Memaksudkan CPU (Central Processing Unit), Anda dapat mengalokasikannya pada kontak CPU, komponen utama di dalamnya terdiri dari processor, motherboard, memori komputer, dan berbagai port serta konektor yang memungkinkan

Smart Card: Kartu plastik yang terintegrasi dengan chip elektronik, misalnya ditujukan sebagai kartu identitas.

Subdirectory: Direktori yang berada pada direktori lain.

T

Tape: Pita magnetik yang diperuntukan sebagai media penyimanan pada komputer.

Trojan Horse: Digolongkan ke dalam malicious software, dan umumnya dikemas sehingga mirip dengan program yang berguna, tetapi pada akhirnya malah menjalankan aksi yang merugikan.

U

URL: Uniform Resource Locator.

V

Virus: Digolongkan dalam malicious software, memiliki ciri-ciri seperti virus biologis pada umumnya. Virus mampu memperbanyak dirinya dengan menumpangi program target, dan melakukan berbagai aksi merugikan yang tak terduga.

Volatile Data: Data yang ada pada sistem komputer dan akan hilang jika listrik dimatikan.

W

Wiping: Meng-overwrite seluruh atau sebagain media penyimpanan untuk merusak kumpulan data/informasi yang dilakukan secara random atau konstan.

Word Processor: Program Aplikasi pengolah kata, misalnya: Microsoft Word dan OpenOffice Writer.

Worm: Digolongkan ke dalam malicious software, worm dapat me-replikasi dirinya tanpa program host, yang terkenal adalah aksinya dalam memacetkan jaringan komputer.

Write-Blocker: Tool yang mencegah penulisan atau modifikasi terhadap media penyimpanan yang terkoneksi.

Z

Zip: Salah satu format kompresi data yang cukup populer.

Lampiran Berbagai Format File:

ABK	CorelDRAW auto backup
ACL	CorelDRAW keyboard accelerator
AFM	Adobe font metrics (Type 1)
AG4	Access G4 document imaging
AI	Adobe Illustrator graphics,
AI	Encapsulated PostScript header
ALB	JASC Image Commander
ANI	Animated cursor
ANS	ANSI text
ARC	ARC, ARC+ compressed archive
ARJ	Compressed archive (Jung)
ART	Xara Studio drawing
ASAX	ASP.NET file
ASC	ASCII file
ASCX	ASP.NET file
ASD	Word temporary document
ASF	NetShow file
ASM	Assembly source code
ASMX	ASP.NET file
ASP	Active Server Page
ASPX	ASP.NET file
ASX	NetShow file
ATT	AT&T Group IV fax
AU	Digital audio (Sun)

AVI	Microsoft movie format
AXD	Actrix drawing
BAK	Backup
BAS	BASIC source code
BAT	DOS, OS/2 batch file
BFC	Windows briefcase document
BIN	Driver, overlay
BM1	Apogee BioMenace file
BML	Bookmark library (SyncURL)
BMP	Windows & OS/2 bitmap
BMK	Windows help bookmarks
C	C source code
CAB	Microsoft compressed format for distribution
CAL	Windows calendar
CAL	SuperCalc spreadsheet
CAL	CALS raster and vector formats
CAP	Ventura Pub. captions
CAL	CALS raster and vector formats
CCB	Visual Basic animated button
CCH	Corel Chart
CDA	CD audio track
CDR	CorelDRAW vector graphics
CDT	CorelDRAW template
CDX	CorelDRAW compressed drawing
CDX	FoxPro and Clipper index
CFG	Configuration

CGM	CGM vector graphics
CH3	Harvard Graphics chart
CHP	Ventura Pub. chapter
CHK	DOS/Windows corrupted file (Chkdsk)
CIF	Ventura Pub. chapter info
CIT	Intergraph scanned image
COB	COBOL source code
COB	Truespace 3-D file
CLP	Windows clipboard
CLS	Visual Basic class module
CMF	Corel metafile
CMP	JPEG bitmap, LEAD bitmap
CMP	RichLink composed format
CMX	Corel clip art
CMV	Corel Presentation Exchange
CNT	Windows help contents
COM	Executable program
CPL	Windows control panel applets
CPL	Corel color palette
CPP	C++ source code
CPR	Knowledge Access bitmap
CPR	Corel Presents presentation
CPT	Corel Photopaint image
CPX	Corel Presentation Exchange
CRD	Cardfile file
CRP	Corel Presents runtime presentation

CSC	Corel script
CSV	Comma delimited
CT	Scitex CT bitmap
CUR	Cursor
DAT	Data
DAT	WordPerfect merge data
DB	Paradox table
DBF	dBASE database
DBT	dBASE text
DBX	DATABEAM bitmap
DCA	IBM text
DCT	Dictionary
DEF	Definition
DG	Autotrol vector graphics
DGN	Intergraph vector graphics
DIB	Windows DIB bitmap
DIC	Dictionary
DIF	Spreadsheet
DISCO	Publishing and Discovering Web Services
DLG	Dialogue script
DLL	Dynamic link library
DOC	Document (MS Word 2003-2007)
DOCX	Document (MS Word 2008)
DOT	Word template
DOX	MultiMate V4.0 document
DPI	Pointline bitmap

DRV	Driver
DRW	Designer vector graphics (Version 2.x, 3.x)
DS4	Designer vector graphics (Version 4.x)
DSF	Designer vector graphics (Version 6.x)
DWG	AutoCAD vector format
DX	Autotrol document imaging
DXF	AutoCAD vector format
ED5	EDMICS bitmap (DOD)
EMF	Enhanced Windows metafile
EPS	Encapsulated PostScript
ESI	Esri plot file (vector)
EVY	Envoy document
EXE	Executable program
FAX	Various fax formats
FDX	Force index
FH3	Freehand 3
FLC	Autodesk animation
FLD	Hijaak thumbnail folder
FLI	Autodesk animation
FLT	Graphics conversion filter
FMT	dBASE Screen format
FNT	Windows font
FON	Windows bitmapped font
FOR	FORTRAN source code
FOT	Windows TrueType font info.
FOX	FoxBase compiled program

FM3	Format info for 1-2-3 Version 3
FP1	Flying Pigs for Windows data
FPX	FlashPix bitmap
FRM	dBASE report layout
FTG	Windows help file links
FTS	Windows help text search index
GAL	Corel Multimedia Manager album
GCA	IBM MO:DCA - GOCA vector graphics
GID	Windows help global index
GIF	CompuServe bitmap
GP4	CALS Group IV - ITU Group IV
GRA	Microsoft graph
GRF	Micrografx Charisma vector graphics
GRP	Windows ProgMan Group
GWX	Genigraphics presentation link
GWZ	Genigraphics presentation link
GX1	Show Partner bitmap
GX2	Show Partner bitmap
GZ	UNIX Gzip
H	C header
HED	HighEdit document
HGL	HP Graphics language
HLP	Help text
HPJ	Visual Basic help project
HPP	C++ program header
HPL	HP Graphics language

HQX	BinHex format
HT	HyperTerminal
HTM	HTML document (Web page)
HTML	HTML document (Web page)
HTX	HTML extension file
HYC	WordPerfect hypen list
ICA	IBM MO:DCA - IOCA bitmap
ICB	Targa bitmap
ICO	Windows icon
IDC	Internet Database Connector
IDD	MIDI instrument definition
IDE	Development environment configuration
IDX	FoxBase index
IFF	Amiga bitmap
IGF	Inset Systems (Hijaak) raster & vector graphics
IL	Icon library (hDC Computer)
IMG	ISO 9660 CD-ROM image
IMG	Macintosh image file
IMG	GEM Paint bitmap
INF	Setup information
INI	Initialization
JFF	JPEG bitmap
JIF	JPEG bitmap
JPG	JPEG bitmap
JS	JavaScript file
JT	JT Fax

JTF	JPEG bitmap
KDC	Kodak Photo bitmap
KFX	Kofax Group IV fax
KYE	Kye game program data
LBL	dBASE label
LBM	Deluxe Paint graphics
LEG	Legacy text
LIB	Function library
LIT	Microsoft Reader file
LOG	Log file
LNK	Windows 9x/NT shortcut
LST	List
LV	LaserView Group IV
LZH	LHARC compressed
LZS	Skyroads program data
M1V	MPEG file
M3U	MPEG file
MAC	MacPaint bitmap
MAK	Visual Basic/MS C++ project
MAP	Link editor map
MB1	Apogee Moster Bash file
MBX	Mailbox (e-mail)
MCS	MathCAD format
MCW	Word for Macintosh document
MDB	Access database
MEL	Maya script

MET	OS/2 Metafile
MEU	Menu items
MDX	dBASE IV multi-index
MID	MIDI sound file
MID	Eudora script file
MIL	Same as GP4
MIX	PhotoDraw file
MME	MIME-encoded file
MMF	Microsoft mail file
MMM	Macromind animation format
MOD	Eudora script file
MOV	QuickTime movie
MPA	MPEG file
MP2	MPEG file
MP2V	MPEG file
MP3	MPEG-1 Layer 3 audio
MPE	MPEG file
MPEG	MPEG file
MPG	MPEG file
MPP	Microsoft Project
MRK	Informative Graphics markup file
MSG	Message file
MSP	Microsoft Paint bitmap
MUS	Music
MVB	Microsoft Multimedia Viewer
M1V	MPEG file

M3D	Corel Motion 3-D
NAP	NAPLPS format
NAV	Eudora script file
NDX	dBASE index
NDX	CDE index
NG	Norton Guides text
NLM	NetWare NLM program
O	UNIX machine language
OAZ	OAZ Fax
OBD	Microsoft Office binder
OBJ	Machine language,
OBJ	Wavefront 3-D file
OBZ	Microsoft Office wizard
OEB	Open eBook publication
OLB	OLE object library
OLE	OLE object
OPF	Open package file
ORG	Organizer file
OTF	OpenType font
OVL	Overlay module
OVR	Overlay module
PAL	Windows palette
PAS	Pascal source code
PAT	CorelDRAW pattern
PBD	PowerBuilder dynamic library
PBK	Microsoft Phonebook

PBM	Portable Bitmap
PCL	HP LaserJet series
PCD	Photo CD bitmap
PCM	LaserJet cartridge info.
PCT	Macintosh PICT bitmap & vector graphics
PCW	PC Write document
PCX	PC Paintbrush bitmap
PDF	Portable Document Format (Acrobat),
PDF	Printer driver,
PDF	Printer description (QuarkXpress)
PDV	PC Paintbrush printer driver
PDW	HiJaak vector graphics
PFA	Type 1 font (ASCII)
PFB	Type 1 font (encrypted)
PFM	Windows Type 1 font metrics
PIC	Various vector formats:
PIC	Lotus 1-2-3,
PIF	Windows info. for DOS programs,
PIF	IBM Picture Interchange
PLT	AutoCAD plotter file
PLT	HPGL plotter file
PNG	PNG bitmap
PPS	PowerPoint Slideshow
PPT	PowerPoint
PRD	Microsoft Word printer driver
PRG	dBASE source code

PRN	Temporary print file
PRS	Harvard Graphics
PRT	Formatted text
PS	PostScript page description
PSD	Photoshop native format
PSR	Powersoft report
PUB	Microsoft Publisher publication
PUB	Ventura Publisher publication
PUZ	Across puzzle
PVK	Private Key
PWL	Windows password list
QBW	QuickBooks
QLB	Quick programming library
QLC	ATM font info
QT	QuickTime movie
QTM	QuickTime movie
RA	Real Audio file
RAM	Real Audio file
RAS	Sun bitmap
RAW	3-D file (open standard)
RC	Resource script
REC	Recorder file
REG	Registration file
RES	Programming resource
RFT	DCA/RFT document
RGB	SGI bitmap

RIA	Alpharel Group IV bitmap
RIB	Renderman graphics
RIC	Roch FaxNet
RIX	RIX virtual screen
RLC	CAD Overlay ESP (Image Systems)
RLE	Compressed (run length encoded)
RLF	RichLink compiled format
RM	Real Media file
RMI	MIDI music
RMM	Real Media file
RND	AutoShade rendering format
RNL	GTX Runlength bitmap
RTF	Microsoft text/graphics
R8P	LaserJet portrait font
R8L	LaserJet landscape font
RV	Real Video file
SAM	Ami Pro document
SAT	ACIS 3-D model
SAV	Saved file
SC	Paradox source code
SCP	Dial-up Networking script
SCR	Windows screen saver
SET	Setup parameters
SFP	LaserJet portrait font
SFL	LaserJet landscape font
SFS	PCL 5 scalable font

SGI	SGI bitmap
SHB	Corel Show
SHW	Corel Show
SLD	AutoCAD slide
SMI	SMIL multimedia
SND	Digital audio
SPD	Speedo scalable font
STY	Ventura Pub. style sheet
SUN	Sun bitmap
SVX	Amiga sound file
SWF	Shockwave file
SY3	Harvard Graphics symbol
SYS	DOS, OS/2 driver
TAL	Adobe Type Align shaped text
TAR	Tape archive
TAZ	UNIX Gzip archive
TDF	Speedo typeface definition
TFM	Intellifont font metrics
TGA	TARGA bitmap
TGZ	UNIX Gzip archive
TIF	TIFF bitmap
TLB	OLE type library
TMP	Temporary
TOC	Table of contents
TRM	Terminal file
TTC	TrueType font compressed

TTF	TrueType font
TXT	ASCII text
USP	LaserJet portrait font
USL	LaserJet landscape font
VBP	Visual Basic project
VBX	Visual Basic custom control
VBS	Visual Basic script
VCF	vCard file
VDA	Targa bitmap
VGR	Ventura Pub. chapter info.
VOC	Sound Blaster sound
VOX	Voxware compressed audio
VP	Ventural Publisher publication
VSD	Visio drawing
VST	Targa bitmap
VUE	dBASE relational view
WAV	Digital Audio (Windows)
WAX	WMA metafile (location of WMA file)
WB?	Quattro Pro spreadsheet (?Memaksudkan versi)
WBK	Microsoft Word backup
WBT	WinBatch file
WCM	WordPerfect macro
WDB	Microsoft works data file
WGP	Wild Board games data
WID	Font width table
WIF	Wavelet image

WIZ	Microsoft Word wizard
WKQ	Quattro spreadsheet
WK1	Lotus versi 2.x
WK3	Lotus versi 3.x & Windows
WK4	Lotus versi 4.x
WKS	Lotus 1-2-3 versi 1a spreadsheet
WMA	Windows Media Audio (ASF file)
WMF	Windows Metafile
WMV	Windows Media video (ASF file)
WPD	Corel WordPerfect,
WPD	Windows printer description
WP?	WordPerfect document (? Memaksudkan versi)
WPG	WordPerfect raster & vector graphics
WPM	WordPerfect macro
WPT	WordPerfect template
WPS	Microsoft Works document
WRI	Windows Write document
WRK	Sympohony spreadsheet
WRL	VRML page
WS?	WordStar for Windows
WSD	WordStar 2000 document
WVX	WMV metafile
XBM	X Window bitmap
XFX	JetFax
XLA	Excel add-in
XLB	Excel toolbar

XLC	Excel chart
XLD	Excel dialogue
XLK	Excel backup
XLM	Excel macro
XLS	Excel spreadsheet
XLT	Excel template
XLW	Excel project
XML	XML file
Z	UNIX Gzip archive
ZIP	PKZIP compressed
$$$	Temporary

Tentang Penulis

Feri Sulianta, ST. MTI. Mengawali karirnya pada tahun 2001 sebagai *Chief Information Officer* dan saat ini aktif mengajar sebagai dosen di beberapa perguruan tinggi. Berbagai aktivitas lain yang dilakoninya antara lain: memberikan pelatihan dan seminar, motivator, life coaching, dan aktif dalam beberapa komunitas profesi.

Sampai saat ini, Feri Sulianta sudah memublikasikan lebih dari 50 judul buku dengan ragam kategori, seperti buku teknologi informasi & komputer, manajemen bisnis, manajemen karier, seni, biologi, true story, dan buku lainnya.

Email penulis: writer@ferisulianta.com

Catatan:

- Untuk melakukan pemesanan buku, hubungi
  Layanan Langsung PT Elex Media Komputindo:
  Gramedia Direct
  Jl. Palmerah Barat No. 33, Jakarta 10270
  Telemarketing/CS: 021-53650110/111 ext: 3901/3902
  Email: **endang@gramediapublishers.com**

Banyak yang tidak mengetahui bahwa segudang fakta dapat diungkap melalui teknik forensik. Bahkan, Anda sanggup menangani problematika komputer termasuk tindak kejahatan melalui teknik hebat yang aplikatif ini, untuk segala masalah yang melibatkan komputer.

Buku ini menarik karena berisi ilmu kombinasi baru berupa metoda, penggagas, penalaran, dan penyampaian deskriptif yang berguna bagi masyarakat dalam memanfaatkan dan menangani IT/komputer dengan pemahaman yang lebih baik.

Materi utama yang dibahas:

- Pemahaman komputer forensik serta korelasinya dengan teknologi komputer.
- Berbagai proses, metode, pola berpikir yang mendasari komputer forensik.
- Penanganan 'bukti' atau evidence yang melibatkan peralatan komputer forensik.
- Perangkat dan software forensik toolkit yang digunakan dan dipindai untuk keperluan komputer forensik.
- Penalaran forensik yang membuat seorang IT menjadi ahli di bidangnya.
- Solusi efektif untuk problematika komputer dengan penalaran forensik.

PT ELEX MEDIA KOMPUTINDO
Kompas Gramedia Building
Jl. Palmerah Barat 29-37, Jakarta 10270
Telp. (021) 53650110-53650111, Ext 3214
Webpage: http://elexmedia.co.id

Kelompok
Utiliti
Keterampilan
☑ Tingkat Pemula
☑ Tingkat Menengah
☐ Tingkat Mahir
Jenis Buku
☑ Referensi
☑ Tutorial
☐ Latihan

gramediana
ISBN 978-602-02-5496-8
9 786020 254968
121142623
001/I/2014