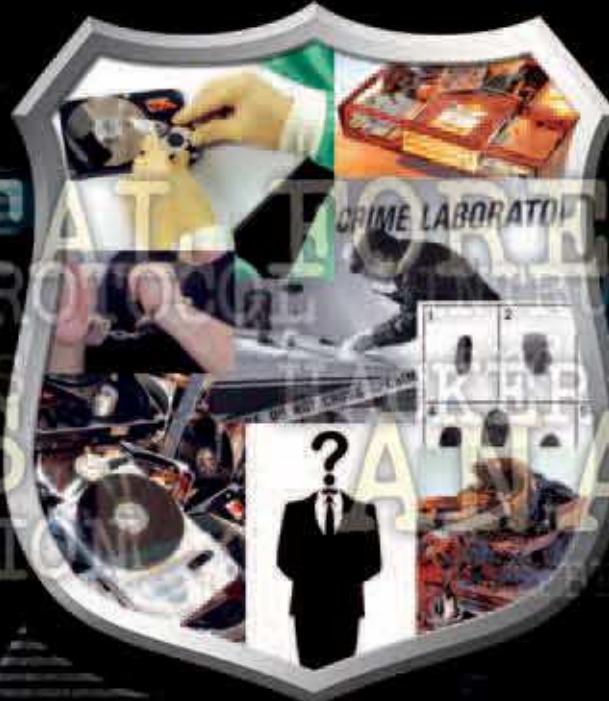


KOMPUTER FORENSIK



Feri Sulianta

KOMPUTER FORENSIK

Sanksi Pelanggaran Pasal 22:

Undang-Undang Nomor 19 Tahun 2002
Tentang Hak Cipta

1. Barangsiapa dengan sengaja melanggar 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 Rp 1.000.000,00 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 5.000.000.000,00 (lima milyar 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 Rp 500.000.000,00 (lima ratus juta rupiah).

KOMPUTER FORENSIK

Feri Sulianta

Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Jakarta

Komputer Forensik

Feri Sulianta

© 2008, PT Elex Media Komputindo, Jakarta
Hak cipta dilindungi undang-undang
Diterbitkan pertama kali oleh
Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Anggota IKAPI, Jakarta 2008

Editor: Whindy Yoevestian

EMK121080994
ISBN: 978-979-27-2771-5

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit.

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

Kata Pengantar

Selama berkecimpung dalam dunia IT dan mengajar, penulis melihat perkembangan yang signifikan dan matang akan keilmuan forensik pada umumnya, tetapi tidak demikian dengan komputer forensik. Bahkan tiga tahun yang lalu, istilah 'Komputer Forensik' terdengar asing dalam benak penulis.

Oleh karena itu, buku dengan tema **Komputer Forensik** sengaja dipilih penulis dengan maksud mengisi kekosongan akan pengetahuan komputer forensik dan diharapkan dapat menginspirasi profesional IT dan penegak hukum untuk mengembangkan metode bahkan pedoman yang berlaku.

Penulis tentunya mengucapkan banyak terima kasih kepada semua pihak (keluarga, rekan, sahabat, saudara) yang banyak memberikan dukungan moril kepada penulis. Terima kasih pula kepada Bapak Whindy Yoevestian yang sudah menjadi mediator yang baik antara penulis dengan penerbit Elex Media Komputindo.

Kritik dan saran dengan senang hati penulis terima untuk meningkatkan kualitas buku ini pada cetakan berikutnya dan menjadi bahan bakar mental untuk terus berkarya.

Bandung, 13 Februari 2008

Feri Sulianta

BAB 1

Hal-Hal Mendasar Komputer Forensik

- ✓ Apa Itu Komputer Forensik?
- ✓ Bidang Keilmuan Forensik
- ✓ Hanya Melulu Komputer?
- ✓ Autopsi – Digital Forensik

Apa Itu Komputer Forensik?

Forensik memiliki arti “membawa ke pengadilan”. Istilah forensik adalah suatu proses ilmiah (didasari oleh ilmu pengetahuan) dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.

Kekuatan dari forensik adalah memungkinkan analisa dan mendapatkan kembali fakta dari kejadian dan lingkungan. Tentu tidaklah mudah mendapatkan (atau lebih tepatnya menemukan) fakta, karena fakta itu tersembunyi adanya.

Berbagai fakta dan bukti tersembunyi yang melingkupi forensik secara umum misalnya: darah, struktur gigi seseorang, riwayat kesehatan, sidik jari, dan lainnya harus dianalisa sedemikian rupa sehingga didapatkan fakta yang layak untuk diajukan sebagai pembuktian.

Metodologi dalam forensik pasti berubah, mengingat ilmu pengetahuan yang mendasarinya pun berubah. Apapun itu perubahannya, pastinya membawa kepada pembaruan dan metode yang lebih baik dengan dimunculkannya bidang keilmuan dan pengetahuan baru.

Bidang forensik sudah berkembang lama, dan ini diawali oleh seorang tabib yang bernama Hi Duan Yu yang dapat mengkategorikan bagaimana seseorang didapati meninggal, misalnya saja karena faktor alami (usia tua), tenggelam, akibat benturan, atau bahkan mati dicekik.

Metode forensik pun berkembang sampai pada akhirnya menggunakan DNA. Meskipun DNA menjadi suatu pembuktian yang sangat kuat dewasa ini dalam forensik, namun tidak demikian dulu adanya.

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

Bukan hanya subjek yang berubah dan meluas, prosesnya pun banyak mengalami perubahan. Ini pun meluas ke bidang-bidang teknologi baru. Bahkan saat ini terdapat istilah **Komputer Forensik** yang mulai mencuat akhir-akhir ini.

Anda tentu setuju bahwa metode, peralatan dan ilmu pengetahuan yang melengkapi komputer forensik masihlah belum matang (*immature*), sangat tidak berimbang dengan perkembangan teknologi informasi itu sendiri.

Berbeda dari forensik pada umumnya, komputer forensik adalah pengumpulan dan analisa data dari berbagai sumber daya komputer. Ini mencakup: Sistem Komputer, Jaringan Komputer, Jalur Komunikasi (mencakup secara fisik dan *wireless*), dan juga berbagai media penyimpanan yang dikatakan layak untuk diajukan dalam sidang pengadilan. Komputer forensik menjadi bidang ilmu baru yang mengawinkan dua buah bidang keilmuan, hukum dan komputer.

Berbagai perilaku digital dan digitalisasi yang sudah merambah dalam setiap aktivitas manusia menjadi perilaku yang harus dialami 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. 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 akan kerusakan sistem.
- Troubleshooting yang melibatkan hardware ataupun software.

- Keperluan memahami sistem ataupun berbagai perangkat digital dengan lebih baik.

Sadar atau tidak, seorang profesional IT pastinya mengasah kemampuan mereka berkomputer bukan hanya pada level pengoperasian umum sistem komputer, tetapi meluas dan kemudian terspesifikasi sesuai kebutuhan. Ini mencakup bagaimana internal sistem operasi bekerja.

Berikut beberapa pokok yang mungkin pernah dilalui oleh profesional IT:

- Seorang profesional IT pastinya berperan dalam pengembangan sistem pada level-level strategis.
- Bukan hanya mengerti sistem secara umum tetapi memahami sistem keseluruhan, ini melibatkan perangkat keras dan perangkat lunak yang digunakan.
- Memiliki keahlian untuk mempertimbangkan dan membuat pilihan yang terasa dari pengalaman dengan problematika yang pernah dihadapi. Problematis ini mencakup user, kerusakan perangkat keras, ataupun masalah yang berhubungan dengan perangkat lunak.
- Profesional IT dengan spesifikasi tertentu, pasti memahami cara kerja perangkat keras dan perangkat lunak secara detail, dan tahu bagaimana sistem operasi bekerja.

- Penjadwalan dan kegiatan administrasi yang rapi pasti diterapkan.
- Tanggung jawab yang diembannya dalam memelihara sistem dan terlibat dalam setiap keputusan yang mempengaruhi sistem menjadi bukti dari kemampuannya.
- Penanganan backup dan bagaimana mendapatkan kembali informasi, tentu membuatnya demikian menghargai betapa berharganya data dan informasi, terlebih bagi komputer forensik yang harus mengambil dan menambah informasi yang minim.

Bidang Keilmuan Forensik

Ada banyak bidang-bidang yang dicakup dan dikombinasikan dalam forensik, berikut contohnya:

Bidang Keilmuan Fisiologi:

- Forensik pathology
- Forensik dentistry
- Forensik anthropology
- Forensik entomology

Bidang Ilmu Sosial:

- Psikologi Forensik
- Forensik Kejiwaan

Lain-Lain:

- *Fingerprint analysis*
- *Forensik Accounting*
- *Ballistics*
- *Bloodstain pattern analysis*

Analisa DNA

- *Forensik toxicology*
- *Forensik footwear evidence*
- *Questioned document examination*
- *Explosion analysis*

Forensik yang Melibatkan Teknologi Cyber:

- Forensik Teknologi Informasi
- Komputer Forensik

Kita lihat beberapa diantaranya, misalnya analisa terhadap pola darah yang tertinggal dalam suatu kejadian, berbagai sifat dari darah, bagaimana darah itu mengisi tubuh manusia, kondisi kesehatan/fisik seseorang, dan lain sebagainya menjadi parameter yang dilekatkan dalam analisa.

Misalnya saja seseorang yang terjatuh, tentu kejadiannya dapat dianalisa dari darah yang ditinggalkan atau tercecer, dan ini akan menjelaskan apakah seseorang memang terjatuh dari gedung yang cukup

tinggi atau tidak, lalu bagaimana posisinya sebelum terjatuh, lalu apakah ini aksi bunuh diri atau bahkan pembunuhan. Jejak dari cipratan darah mampu menceritakan kronologisnya. (*Bloodstain Pattern Analysis*).

Anda mungkin pernah menonton film “Criminal Mind”, dimana salah satu divisi dari FBI yang dikenal dengan BAU (Behavioral Analysis Unit) melakukan berbagai investigasi kriminal dari sisi perilaku dan psikologis.

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

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

- Forensik Disk
- Forensik System
- Forensik Jaringan Komputer
- Forensik Internet

Dari beberapa bagian ini beberapa mungkin sudah demikian berkembang, misalnya Disk Forensik yang melibatkan berbagai media penyimpanan. Ilmu forensik tersebut sudah terdokumentasi dengan baik, bahkan profesional IT pun bisa menangani masalah Disk Forensik ini.

Misalnya saja mendapatkan file-file yang sudah dihapus, mengubah partisi harddisk, mencari jejak *bad sector*, dan lainnya.

Sistem Forensik tentunya dekat dengan sistem operasi, dan akan sangat sulit menyamaratakan, karena setiap sistem operasi memiliki karakteristik dan perilaku yang berbeda, misalnya saja berbagai file sistem.

Berbagai keperluan sistem operasi untuk diimplementasikan pada Workstation saja atau untuk server saja, tentunya memiliki karakteristik, penanganan, dan perilaku yang berbeda.

Jika Anda berbicara tentang Network Forensik, pastinya ini melibatkan OSI (Open System InterConnection) layer yang menjelaskan bagaimana komputer berkomunikasi dalam diagram OSI tujuh lapis.

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

Mari kita lihat apa-apa saja yang dilakukan dalam bidang forensik dan apa yang ditanganinya secara umum:

Disk Foresik mencakup kemampuan dalam:

- Mendapatkan “bit-stream” image. Hal ini mencakup: *slack*, *unallocated space* dan file fragments yang dihapus.
- Penyidik harus mampu mendemonstrasikan pelaksanaan investigasi dengan aturan dan bukti yang layak.
- Integritas informasi harus disajikan sedemikian rupa sehingga terbukti keabsahannya, ini identik dengan sidik jari digital.

Beberapa hal yang bisa dilakukan dengan adanya Disk Forensik:

- Me-recover file-file yang terhapus, mendapatkan password dan kunci *Cryptographic*.
- Menganalisa akses file, perihal memodifikasi dan menciptakan file.
- Menganalisa dan memanfaatkan System Logs dan Log software aplikasi (misalnya: monitoring akses file di jaringan atau penggunaan software aplikasi dan Utility). Dengan demikian aktivitas pengguna dapat dilacak.

Tentunya untuk mendapatkan informasi demikian kita mengandalkan software-software yang 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 lain yang dapat digunakan, misalnya Linux DD yang pernah digunakan oleh FBI dalam kasus Zacarias Moussaoui, lalu Coroners Tool Kit (CTK) untuk Unix Sistem.

Hanya Melulu Komputer?

Komputer Forensik mencakup banyak hal yang harus dipertimbangkan, dikarenakan ilmu baru yang dibangun karena kebutuhan dan didasari pada kompleksitas.

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 sumber daya Teknologi Informasi yang melibatkan komputer forensik.

Prinsip (Principle): Pada prakteknya melibatkan peralatan (*special tools and equipment*) untuk mengumpulkan *electronic evidence*. Yang terpenting bukanlah tool-nya, tetapi keahlian yang sudah teruji lewat pengalaman. Bahkan tool akan disesuaikan berdasarkan cara kerja nantinya.

Kebijakan (Policy): Pertimbangkan kebijakan dalam menggunakan peralatan, mencakup perihal mendiskoneksikan media penyimpanan yang berisi *evidence* untuk keperluan investigasi, mengirimkan *digital evidence*, akase ke dokumen, dan lain sebagainya.

Prosedur dan Metode (Procedure): Harus dirancang sedemikian rupa terhadap peralatan dan mendapatkan/mengumpulkan *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 komputer. Perangkat-perangkat forensik pada umumnya (*general crime scene processing tools*) mungkin digunakan dalam komputer forensik, sebagai cara pemberlakukan terhadap suatu bukti, misalnya seperti digunakan-

nya notepad (buku catatan), kamera, sketsa (*sketchpads*), formulir (*evidence forms*), *crime scene tape*, dan *markers*.

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

Peralatan Dokumentasi (Documentation Tools):

- Cable tags.
- Indelible felt tip markers.
- Stick-on labels.

Disassembly and Removal Tools:

- Flat-blade and Philips-type screwdrivers.
 - Hex-nut drivers.
 - Needle-nose pliers.
 - Secure-bit drivers.
 - Small tweezers.
 - Specialized screwdrivers (yang dibuat secara spesifik oleh misalnya: Compaq, Macintosh).
 - Standard pliers.
 - Star-type nut drivers.
 - Pemotong kabel
- ### Package and Transport Supplies:
- Antistatic bags.
 - Antistatic bubble wrap.

- Cable ties.
- Evidence bags.
- Evidence tape.
- Packing materials (untuk menghindarkan dari material yang dapat menghasilkan listrik statis, seperti misalnya *styrofoam*).
- Packing tape.
- Sturdy boxes dengan berbagai ukuran.

Perlengkapan lain yang digunakan:

- Sarung tangan.
- Hand truck.
- Large rubber bands.
- Daftar kontak telpon asisten/staf.
- Magnifying glass.
- Printer paper.
- Seizure disk.
- Small flashlight (lampu senter).
- Floppy disk kosong atau tidak terpakai ($3\frac{1}{2}$ and $5\frac{1}{4}$ inch).

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 daripada sekedar spesialis informasi. Memang keilmuan Teknologi Informasi dan Komputer menjadi keharusan, tetapi pada prakteknya apa yang dilakukan dalam komputer forensik lebih dari itu, karena mereka mungkin melakukan bukan hanya *data recovery* biasa, bahkan luar biasa, melebihi batas-batas normal *data recovery*, dan masih banyak lagi hal-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 tentunya akan melalui serangkaian tes.

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 bukti demikian, mereka harus bekerja pada sistem yang terbukti keabsahannya, sistem yang terpercaya dan hanya mereka

saja yang dapat mengaksesnya, dan pastinya dalam laboratorium yang tingkat keamanannya tidak diragukan, bebas virus dan terisolasi.

Si *examiner* harus melalui serangkaian metode, seperti memfoto perangkat yang dimaksud sebelum nantinya dipindahkan untuk keperluan forensik. Ini mencakup dokumentasi pengkabelan, *peripheral* atau *device* yang diintegrasikan, sehingga nantinya dapat di *reassembling* di laboratorium forensik.

Belum cukup sampai di situ saja, bagaimana mereka memindahkan perangkat tersebut juga harus diperhatikan, jangan sampai panas dan jangan biarkan benda-benda magnetis ataupun faktor fisik merusaknya.

Pastinya mereka tidak menyentuh atau memperlakukan harddisk dan floppy dengan ceroboh, karena perubahan sekecil apaun akan mengubah laporan akhir. Maka dari itu mereka menduplikasi data yang ada ke media yang tidak dapat dimodifikasi kemudian, misalnya pada CD.

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

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 tentunya menyimpangkan log sebenarnya.

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

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

Dalam prakteknya si *examiner* mungkin melakukan pencarian dan pemeriksaan mendalam terhadap e-mail, file temporer, melibatkan pula basis data, *logical file structure*, space harddisk tersisa, setting-an perangkat keras dan perangkat lunak, *cache file* pada web browser, bookmark, dan hal lainnya.

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

Lebih jauh lagi Anda akan melihat ruang lingkup dari kasus forensik yang beragam, dimana karakteristik dari kategori tindak kriminal tentunya akan melibatkan bukti-bukti spesifik.

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

- Audio Recorder
- Mesin Penjawab
- Kabel
- Peralatan Caller ID
- Telpon Selular
- Chips (jumlah yang banyak berkenaan chip ini, tentunya akan menjadi bukti terhadap tindak pencurian)
- Mesin Fotokopi
- Databank/Digital Organizer
- Kamera digital
- Dongle
- Hardware Protection Devices (keys)
- Drive duplicators
- External drives
- Fax machines
- Flash memory cards
- Floppy (diskettes)
- CD-ROM
- Perangkat GPS
- Pagers
- Palm Pilots/electronic organizers
- PCMCIA cards
- Printers (dalam keadaan aktif)
- Removable media
- Scanners (film scanner, flatbed scanner, dan lainnya)
- Smart cards/secure ID tokens
- Telpon (mencakup pula speed dialers, dan lainnya)
- VCR
- Wireless access point

Dari kesemuanya, ternyata berbagai perangkat yang ada hanyalah sebagian kecil dari banyak ragam komponen yang akan ditambahkan kemudian, seiring bentuk tindak kejahatan, misalnya seandainya kejadian melibatkan internet dan jaringan komputer, tentu ruang lingkup akan meluas, bahkan harus melibatkan rangkaian kegiatan yang demikian teknis.

Berikut diberikan daftar yang akan membantu petugas investigasi mengidentifikasi berbagai bukti dan atribut yang dibagi dalam konteks kejahatan yang terjadi:

Auction Fraud (Online):

- Account data (online auction sites)
- Accounting/bookkeeping software

- Buku Alamat
- Kalendar
- Chat logs
- Customer information/credit card data
- Basis Data
- Digital camera software
- E-mail/surat/catatan
- Financial/asset records
- Image/files grafis
- Log aktivitas ber-internet
- Internet browser history/cache files
- Online financial institution access software
- Records/documents of “testimonials”
- Catatan pengunaantelpon

Eksplorasi dan Pelecehan Anak-Anak:

- Chat logs
- Tanggal dan waktu
- Digital camera software
- E-mail/surat/catatan
- Games
- Graphic editing dan viewing software
- Image

- Log aktivitas ber-internet
- File Movie
- User-created directory dan nama file yang mengklasifikasi image

Kejahatan Komputer:

- Buku alamat
- Configuration files
- E-mail/surat/catatan
- Program Executable
- Log aktivitas ber-internet
- Internet protocol address dan user name
- Internet relay chat (IRC) logs
- Source code
- File-file teks (user names dan passwords)

Investigasi Penyebab Kematian:

- Buku alamat
- Buku harian (diary)
- E-mail/surat/catatan
- Catatan keuangan dan perbedahan
- Images
- Log aktivitas ber-internet
- Legal documents
- Riwayat kesehatan dan pengobatan
- Catatan penggunaan telpon

Kekerasan Rumah Tangga:

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

Penipuan Keuangan (Melibatkan Penipuan Online dan Pemalsuan):

- Buku alamat
- Kalender
- Cek, mata uang, dan money order images
- E-mail/surat/catatan
- Form transaksi keuangan palsu
- Identifikasi palsu
- Catatan keuangan dan perben daharaan
- Log aktivitas ber-internet
- Online financial institution access software
- Credit card skimmers
- Informasi konsumen
- Data kartu kredit
- Basis Data

E-Mail (Berupa Ancaman/Memper malukan/Mengganggu):

- Buku alamat
- Buku harian (diary)
- E-mail/surat/catatan
- Catatan keuangan dan perben daharaan
- Image
- Log aktivitas ber-internet
- Dokumen/berkas-berkas hukum
- Catatan pengunaan telpon
- Catatan latar belakang korban

Pemerasan:

- Date and time stamps
- E-mail/surat/catatan
- Log Historis
- Log aktivitas ber-internet
- Temporary internet files
- 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 perben-daharaan
- Gambar/wajah para pemain
- Log aktivitas ber-internet
- Online financial institution access software
- Statistik taruhan

Pencurian Identitas:

- Tool hardware dan software
- Backdrops
- Credit card generators
- Credit card reader/writer
- Kamera digital
- Scanner
- Identification templates
- Surat kelahiran
- Check cashing cards
- Digital photo images untuk ke-perluan identifikasi
- SIM
- KTP
- Electronic signatures
- Registrasi kendaraan fiktif
- Bukti dokumen asuransi
- Tanda tangan yang di-scan

Aktivitas Internet Terkait Pencurian ID:

- E-mails dan newsgroup postings

- Dokumen terhapus
- Online orders
- Online trading information
- System files dan file slack

Aktivitas Internet pada Forgery Sites Narkotik:

- Buku alamat
- Kalender
- Basis data
- Resep obat-obatan
- E-mail/surat/catatan
- False identification
- Catatan keuangan dan perben-daharaan
- Log aktivitas ber-internet

Prostitusi:

- Buku alamat
- Biografi
- Kalender
- Database dan catatan konsumen
- E-mail/surat/catatan
- False identification
- Catatan keuangan dan perben-daharaan
- Log aktivitas ber-internet
- Riwayat kesehatan dan pengobat-an
- Iklan pada web page

Software Piracy

- Chat logs
 - E-mail/catatan/surat
 - Image files of software certificates
 - Log aktivitas ber-internet
 - Serial numbers
 - Software cracking information dan software utility
 - User-created directory dan nama file yang diklasifikasikan dalam software ber-copyright
- Ringkasan kasus
 - Internet Protocol (IP) Address
 - Daftar kata-kata kunci
 - Nickname/Alias
 - Password
 - Points of contact
 - Dokumen pendukung lainnya
 - Jenis kejahatan

Telecommunications Fraud:

- Cloning software
- Database dan catatan konsumen
- Electronic Serial Number (ESN) atau Mobile Identification Number (MIN) pair records
- E-mail/surat/catatan
- Catatan keuangan dan perben-daharaan
- Buku manual mengenai cara *phreaking*
- Aktivitas ber-internet
- Catatan penggunaan telpon

Sebagai catatan, informasi tadi harus didokumentasikan jika memung-kinkan. Beberapa informasi lain yang ditambahkan kemudian untuk membantu dalam uji forensik antara lain:

BAB 2

Perangkat Teknologi Forensik

- Komponen Komputer dan Informasi
- *Digital Evidence*
- Peralatan Komputer Forensik
- Fakta di Balik Forensik
- *Uncover Digital Evidence*

Komponen Komputer dan Informasi

Sama halnya dengan sumber daya informasi yang kita kenal, komponen dalam komputer forensik dibangun dari komponen sumber daya informasi, hanya saja pengimplementasianya berbeda. Tentu penanganan yang diberikan pun berbeda.

Komponen yang dimaksud identik dengan sumber daya informasi dalam era komputer antara lain:

- Hardware
- Software
- Database (Basis Data)
- Data/Informasi
- Brainware (User, Profesional IT)

Semakin ke bawah urutannya, maka semakin dekat dengan user/pengguna, semakin ke atas (hardware) maka semakin sulit kita berurusan dan mengerti perilakunya. Oleh karena itu diperlukan lapisan-lapisan lain yang memungkinkan kita memanfaatkan kemampuan sistem komputer.

Hardware mencakup:

- Perangkat Input (masukan)
- Perangkat Output (keluaran)
- Storage Device (penyimpanan)
- Komponen Pengolahan

Perangkat masukan dikenal pula dengan istilah Input Device, adalah perangkat yang diintegrasikan dalam sistem komputer yang memungkinkan kita memberikan intruksi pada komputer.

Beberapa yang dikategorikan ke dalam perangkat input:

- Keyboard
- Mouse
- Trackball
- Trackpoint
- Trackpad/Touchpad
- Touch Screen
- Joystick
- Source Data Automation (Optical Character Recognition, Bar Code Reader, Handwritten Recognition)
- Scanner (Flatbed Scanner, Handy Scanner, Medium Size Scanner)
- WebCam
- Kartu (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 output/keluaran.

Beberapa yang dikategorikan ke dalam perangkat output:

- Monitor: yang paling umum untuk komputer adalah Cathode Ray Tube (CRT). Sementara itu jenis monitor Liquid Crystal Display (LCD) umumnya digunakan pada laptop dan PDA.
- Printer
 - Impact Printer: dikatakan Impact karena bekerja dengan sistem "ketukan". Contoh printer ini antara lain dot matrix dan 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 dan external).
- Video Output (Proyektor Multi-media).
- MicroFilm

Storage Device atau media penyimpanan. Istilah ini mengacu pada media penyimpanan sekunder (Secondary Storage Device). Ada banyak istilah yang mengacu pada media penyimpanan sekunder, antara lain:

- Mass Storage

- Simpanan Luar
- Auxiliary Storage
- Permanen Storage
- Backing Storage
- Computer Data Bank

Secondary Storage umumnya digolongkan ke dalam dua bagian:

- Sequential Access Storage Device (SASD). Prosesnya lambat karena untuk mencari data tertentu harus selalu dimulai dari awal. Contoh: magnetic tape. Sudah jarang dipakai, umumnya hanya untuk backup, karena murah dan kapasitas yang besar.
- Direct Access Storage Device (DASD). Prosesnya lebih cepat dibanding SASD, karena untuk mengambil data tertentu tidak perlu dicari dari awal berurutan. Terdiri dari:
 - 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 yang lama akan ditinggalkan dan digantikan dengan teknologi yang lebih baik dan berdaya guna. Coba Anda perhatikan variasi dari teknologi penyimpanan seputar disk storage berikut:

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

Kemampuan menyimpannya pun berbeda:

- CD-ROM Media (650-700 MB) dengan kapasitas 60 menit dan kemampuan penyimpanan 553 MB. Kapasitas 79 menit dan 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 kapasitas penyimpanan antara CD jika dibandingkan dengan kapasitas DVD yang mencapai 26 kali kapasitas CD media.

Kita kembali ke CD media dengan CD-ROM drive-nya, dimana CD-ROM mampu melakukan transfer data untuk setiap putarannya per detiknya sedemikian:

- 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 metode CLV (Constant Linear Velocity) yang diterapkan pada CD-ROM terdahulu, sehingga semakin dekat head pada pusat piringan, maka semakin cepat putaran untuk menghantar data.

Sedangkan metode CAV memungkinkan CDROM berputar pada putaran yang konstan per menitnya, sehingga pembacaan data yang ada di piringan terluar akan dibaca sedemikian cepat dan melambat di pusat.

Perubahan berkenaan teknologi memang tidak selalu berpengaruh terhadap forensik, seperti percontohan dua metode pada CD-ROM. Hal demikian hanya menjadi ilmu tambahan yang mungkin tidak akan terlalu bermanfaat dalam bidang forensik.

Dalam forensik kita menguak fakta, bukan teknologi. Sama halnya dengan profesional IT bidang lain, seperti Sistem Analist, ataupun Database Administrator, forensik bukan bidang yang penuh dengan segi teknis belaka.

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 keseluruhan sistem. CPU dalam konteks ini sering disebut sebagai micro processor karena minimnya processor yang menyusun komputer mikro.

Sekali lagi, jika Anda berbicara mengenai CPU, tentunya ini mengacu pada processor (otak komputer), maka dari itu komponen ini menjadi komponen inti dari sistem komputer, karena pemrosesan terjadi di sini.

CPU dapat kita golongkan 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: Control Unit mengambil instruksi dari RAM, kemudian menerjemahkan instruksi tersebut, dan memerintahkan data yang diperlukan dipindahkan dari RAM ke ALU. ALU melakukan perhitungan dan perbandingan dan menyimpan hasilnya di RAM/Register.

Beberapa faktor yang sangat mempengaruhi kinerja CPU antara lain:

- Register, umumnya dapat menyimpan 2 bytes informasi, masing-masing dapat terdiri dari 16, 32, atau 64 bits. Ukuran penyimpanan informasi dalam register disebut wordsize. Semakin besar wordsize, semakin tinggi kecepatan prosesornya.
- Memori, yang dapat digolongkan kedalam dua bagian:
 - ROM (Read Only Memory). Berisi perintah yang diisi oleh pembuat chip. Isinya tidak dapat diubah/dihapus 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 dan 32 bit. Semakin besar ukuran bus, semakin cepat informasi mengalir, proses semakin cepat.
- Perkembangan bus: ISA, EISA, MCA, PCI.
- Jenis-jenis sistem BUS:
 - ISA (Industrial Standard Architecture)
 - PCI (Peripheral Component Interconnect)
 - AGP (Accelerate Graphic Port)
 - USB (Universal Serial Bus)
 - ISA dengan kecepatan transfer data 5 MB/s, memiliki lebar data 8/16 Bit
 - PCI dengan kecepatan transfer data 132 MB/s, lebar data 64 Bit. Digunakan untuk card kecepatan tinggi (misalnya pada LAN card, SoundCard)
 - AGP System Bus untuk Video Display. AGP 1X: 266 MB/s, AGP 2X: 532 MB/s, AGP 4X: 1064 MB/s
- Cache Memory, berikut pernyataan tentang 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 tentunya adalah menyangga data untuk keperluan pemrosesan, dan jika dilihat lebih jauh, ternyata konsep menyangga data ini melibatkan komponen di luar dari CPU: Cache Level 1 (L1 Cache) menyangga L2 Cache, RAM, Harddisk, dan CD-ROM.

Sedangkan L2 Cache menyangga RAM, Harddisk, CD-ROM. L3 Cache menyangga RAM, Harddisk, CD-ROM.

Sementara itu Harddisk menyangga CD-ROM. Perhatikan rantai yang terjadi, yang difungsikan untuk mendongkrak kinerja sistem komputer.

- Faktor lain yang mempengaruhi kinerja motherboard:
 - Expansion Slot (slot untuk komponen/card tambahan).

- Port (hubungan motherboard dengan alat Input-Output, misalnya keyboard, mouse, dan lainnya).
- CPU Fan (berfungsi sebagai pendingin).
- Casing (kotak CPU).

Penting bagi Anda untuk memahami dengan baik komponen-komponen berikut dengan berbagai penamaan atau istilah. Komputer forensik berada di level atas dari hanya sekedar mengerti komputer. Profesional komputer forensik harus memiliki ketertarikan yang luar biasa dalam bidang komputer, faktor-faktor yang menggelitik akan memicunya untuk menggali dan menganalisa lebih dalam. Jadi, adalah hal yang biasa jika Anda harus dihadapkan dengan berbagai istilah dan penamaan di bidang komputer.

Meskipun demikian Anda diajak untuk memahami dan mengeksplorasi bidang-bidang forensik ini, termasuk ragam istilah dasar dan spesifik. Salah pemahaman dalam merujuk pada komponen tertentu akan menimbulkan persepsi yang sama sekali berbeda. Oleh karena itu, upayakan untuk memperkaya pembendaharaan kata Anda (lebih jauh Anda dapat melihat kamus forensik yang ada pada Bab 8).

Software

Umumnya software atau dikenal dengan perangkat lunak digunakan sebagai mediator dan pemberi instruksi terhadap sumber daya hardware sehingga dapat dikatakan sebagai satu kesatuan sistem komputer yang bekerja.

Perangkat lunak umumnya digolongkan ke dalam dua bagian:

- Perangkat Lunak Sistem

Dikatakan perangkat lunak sistem, karena fungsi dan relasinya yang demikian dekat dengan perangkat keras. Perangkat keras umumnya tidak dapat bekerja tanpa adanya software sistem untuk menjadi suatu sistem komputer yang bekerja.

- Perangkat Lunak Aplikasi

Perangkat lunak aplikasi digunakan oleh user untuk mengakses sumber daya komputer. Perkembangan yang pesat akan software dikarenakan kebutuhan user yang terus meningkat dan beragam dalam memanfaatkan komputer.

Sedemikian beragamnya perangkat lunak, sehingga menimbulkan kesulitan dalam pengklasifikasianya. Tidak ada pembagian batu berkenaan perangkat lunak.

Berikut contoh pembagian perangkat lunak berdasarkan 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

Memang sangat sulit mengkategorikan seluruh perangkat lunak aplikasi yang ada karena perkembangan dan kebutuhan yang terus berubah. Coba perhatikan pembagian lebih lanjut pada <http://www.software-list.com/> yang membagi software dalam kategori berikut:

- Audio & Multimedia
- Communications
- Business
- Desktop
- Education
- Games & Entertainment
- Graphics
- Home & Hobby
- Network & Internet
- Security
- Servers
- Development
- System Utilities
- Web Development

Brainware

Profesi bidang Teknologi Informasi terus berkembang dan memiliki kecenderungan meluas. Meskipun demikian tidak menutup adanya perubahan, dalam arti, bidang yang satu hilang dan digantikan dengan yang lain.

Misalnya beberapa bahasa pemrograman yang terbilang *obsolete* akhirnya digantikan dengan programming "bertemakan visual" dengan konsep pemrograman yang sama sekali berbeda.

Beberapa software aplikasi akhirnya tidak dipakai lagi seiring meningkatnya kebutuhan pasar akan program aplikasi yang user friendly, demikian pula dengan perangkat keras. Tentunya hal ini akan berdampak langsung atas kualifikasi dari Brainware.

Umumnya Brainware yang terlatih akan sangat mudah mencerna ilmu-ilmu komputer forensik. Bahkan dalam berkegiatan, mungkin konsep-konsep komputer forensik digunakan. Misalnya saja untuk mendapatkan kembali data yang hilang karena terhapus tidak sengaja. Dibutuhkan tidak hanya sekedar pengetahuan, tetapi pengalaman yang membuat Brainware bisa memiliki "cita rasa" yang berbeda dalam memandang komputer dan segala problematika yang ada.

Lebih jauh lagi, Brainware dalam ruang lingkup komputer forensik tidak melulu dimaksudkan Investigator karena Ilmu Komputer Forensik dibutuhkan pula pada organisasi lain semisal organisasi perusahaan dalam mengelola sistem informasi yang ada. Jadi, pembagian sehubungan Brainware kategori forensik didasarkan atas kebutuhan dan seberapa besar intensitas dan kepentingan terhadap teknik forensik digunakan.

Umumnya Brainware dalam konteks ini dapat digolongkan ke dalam tiga bagian, yaitu (pembagian ini tidak

baku, hanya didasarkan pada sudut pandang yang berbeda):

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

Profesional IT di sini adalah profesional IT pada umumnya, mencakup bermacam deretan istilah seperti Technical Support, Network Administrator, Database Administrator, Sistem Analyst, Programmer, dan lain sebagainya.

Mereka-mereka ini pasti mengetahui dasar-dasar penanganan komputer forensik, yang berbeda mungkin hanya proses dan jenis kebutuhan. Brainware kategori ini tentunya sangat sedikit menerapkan konsep-konsep komputer forensik dalam pekerjaannya, meskipun demikian sedikit banyak mereka menerapkan komputer forensik secara tidak langsung sewaktu didapati masalah.

Incident Handler memiliki kedekatan dengan keilmuan forensik meskipun karakteristik pekerjaannya tidak melulu mencakup tindak kriminal dan pelanggaran. Mereka banyak menangani masalah keamanan, misalnya DoS Attack (Denial of Services), perangkat lunak yang berbahaya (Malicious), bahkan akan banyak menggunakan perangkat lunak komputer forensik dalam pekerjaannya.

Yang terakhir adalah Investigator, umumnya Investigator difungsikan dalam menangani kejadian sehubungan tindak kriminal. Disinilah komputer forensik diperlukan dan diterapkan sepenuhnya.

Database

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

Database umumnya dikelompokkan ke dalam dua bagian digolongkan berdasarkan ketahanannya 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 menjadi sumber yang bernilai dalam komputer forensik untuk menyukseskan fakta.

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, adalah data yang ada dalam sistem komputer yang sedang berjalan, misalnya saja dalam memori komputer (RAM).
- Berbagai komputer portabel dengan media penyimpanan di dalamnya.
- Peripheral, semisal printer dapat menyimpan data, misalnya saja printer laser dengan memori 8 Mb yang digunakan menampung data untuk keperluan cetak.
- Berbagai media penyimpanan, misalnya: USB Flash Disk, Multi-Media Card, Portable Harddisk, dan lainnya.

Digital Evidence

Evidence yang dimaksud dalam kasus forensik pada umumnya tidak lain adalah informasi dan data. Cara pandangnya sama saja, tetapi dalam kasus komputer forensik, kita mengenal subjek tersebut sebagai Digital Evidence.

Semakin kompleks konteks digital evidence dikarenakan faktor media yang melekatkan data. Format pun akan mempengaruhi cara pandang kita terhadap digital evidence, misalnya digital evidence berupa dokumen, yang umumnya dikategorikan ke dalam tiga bagian, antara lain:

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

File yang tergolong arsip adalah karena kebutuhannya dalam fungsi pengarsipan, mencakup penanganan dokumen untuk disimpan dan format yang ditentukan, proses mendapatkan kembali dan pendistribusian untuk lain kebutuhan, misalnya beberapa dokumen yang didigitalisasi disimpan dalam format TIFF untuk menjaga kualitas dokumen.

File Aktif adalah file yang memang digunakan untuk berbagai kepentingan yang berakitan erat dengan

kegiatan yang sedang dilakukan, misalnya file-file gambar saja, file-file dokumen teks, dan lain-lain.

Sedangkan file yang tergolong Residual mencakup file-file yang diproduksi seiring proses komputer dan user beraktivitas, misalnya catatan user dalam menggunakan internet, database log, berbagai temporary file, dan lain sebagainya.

Digital evidence tersebar dalam berbagai media dan konteks-nya, untuk itu diperlukan kejelian yang lebih daripada sekedar mengklasifikasi data untuk tujuan forensik. Secara umum akan disajikan dalam paragraf selanjutnya.

Sistem Komputer

Sistem komputer merupakan berbagai 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, misalnya: monitor, keyboard, dan mouse.

Bahkan akan lain halnya cara pandang kita terhadap sistem komputer seandainya komputer ditempatkan dalam suatu jaringan yang bersisisian dengan komputer-komputer lain yang memungkinkannya untuk saling berkomunikasi.

Demikian pula untuk sekedar sistem komputer, ada banyak komputer yang dikatakan sebagai sistem komputer dan range-nya pun sangat beragam , mulai dari mainframe/super komputer, komputer mini, dan akhirnya komputer mikro semisal: laptop, komputer desktop, PDA, dan berbagai *ubiquitous computer*.

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

Meskipun demikian, evidence umumnya ditemukan dalam file-file yang disimpan dalam media penyimpanan, misalnya pada harddisk.

Jadi, kembali lagi kepada data dan informasi yang terkandung dalam suatu file, terlepas apapun itu bentuk sistem komputer dan media penyimpanan yang digunakan. Banyak file dapat dijadikan acuan untuk memulai penyaringan evidence, file yang diciptakan user secara langsung tentunya 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 menjadi salah satu evidence yang sangat penting, dimana seiring dengan aktivitasnya dalam menggunakan komputer, akan ada data yang ditambahkan dan diciptakan, misalnya user mengorganisasi aktivitasnya dalam e-calendar, file-file grafik yang disimpan, dan sebagainya.

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

Berikut beberapa yang dikategorikan dalam user-created files:

- Address books
- Audio/video files
- E-Calendars
- Database files
- Dokumen dan file teks

- File-file e-mail
- Image/file grafik
- Internet bookmarks/favorites
- File Spreadsheet
- User-Protected Files

Tentunya file-file ini akan dijaga kerahasiannya dan akses yang dimungkinkan terhadapnya mengingat file tersebut diciptakan langsung untuk kepentingan pelaku.

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 didiskoneksikan dari komputer.

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

- File terkompres
- Salah menamakan file secara disengaja atau tidak.
- Salah dalam memberikan file format, secara disengaja atau tidak
- File yang diproteksi 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 tentunya dapat dijadikan evidence.

Ini mencakup pada berbagai catatan dan laporan dari aktivitas sistem komputer, sistem operasi tentunya berperan dalam memunculkan evidence jenis ini. Misalnya saja: password, aktivitas ber-internet, dan *temporary backup files* atau *temporary installation files* sangat mudah dianalisa dan didapatkan kembali untuk berbagai kepentingan.

Kita katakan evidence jenis ini ke dalam Computer-Created Files, mencakup aktivitas semisal: waktu dan jam menyangkut file tertentu, modifikasi yang mungkin dilakukan terhadap suatu file, penghapusan waktu pengaksesan, pemilik dari file tersebut, dan berbagai atribut file. Pada akhirnya dapat dikatakan ini adalah mengenai data atau dikenal dengan istilah metadata yang akan sangat berguna dalam komputer forensik. Berikut ini ditampilkan Computer Created-Files:

Computer-Created Files

- File Backup
- Registry (Windows Registry)
- File Log
- File Configuration
- 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, dan 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 dipercontohkan sebagian dari penggalian terhadap *computer created file* dalam kasus Windows Registry keperluan forensik pada bab-bab selanjutnya.

Kemampuan seperti ini tentunya tidak harus Anda dapatkan dalam komputer forensik, Anda sebagai user yang memiliki minat yang besar akan komputer tentunya memahami konsep dan penanganannya.

Peralatan Komputer Forensik

Software Forensik

Berbagai software forensik dibuat untuk menangani spesifik kebutuhan komputer forensik, meskipun pada prakteknya Anda dapat saja menggunakan berbagai utility yang banyak digunakan untuk keperluan performa komputer, keamanan, dan berbagai utility non spesifik forensik.

Berikut disajikan untuk Anda berbagai software yang digunakan mencakup website yang memungkinkan Anda mendapatkan informasi yang menyeluruh akan software tersebut:

Intrusion Detection and Prevention Systems

Honeypots.net

<http://www.honeypots.net/ids/products/>

The screenshot shows a search results page for 'Intrusion Detection and Prevention Software, IDS Software, IPS Software'. The results include links to various products and services:

- Related Reading:**
 - Honeypot Books
 - Honeypot & Honeysoft
 - Honeypot & Honeysoft Books
 - Honeypot & Honeysoft Software
 - Honeypot & Honeysoft Projects
- Related Tools:**
 - Blessing Access Server
 - The Leading Bluetooth Access Point Platform for Integrating Developers
 - Courses
 - Integrity
 - Honeypot Software
 - Honeypot Detection
 - SniffIt! and fida**
 - Cast effective alternatives for SmartBEE IP packet sniffing software.
- ActiveScout** by FireCloud Technologies.
- AirDefense Guard** by AirDefense, Inc.
- SnifferIt!** and **fida**
- MOXA串行網通選購**
- BroMan** for BroMan

Bro Intrusion Detection System

<http://www.bro-ids.org/Features.html>

The screenshot shows the 'Bro Features' section of the Bro Intrusion Detection System website. It includes:

- Bro Features and Benefits**
 - Network Based**: Bro is a network-based IDS. It collects, filters, and analyzes traffic that passes through a specific network location. A single Bro sniffer, strategically placed at a key network junction, can be used to monitor all incoming and outgoing traffic for the entire area. Bro does not use or require installation of client software on each individual, networked computer.
 - Custom Scripting Language**: Bro policy scripts are programs written in the Bro language. They

ISS Proventia Enterprise Protection by Internet Security Systems (ISS)

<http://www.iss.net/products/index.html>

The screenshot shows the 'Products' section of the IBM Internet Security Systems website. It lists several product categories:

- Network Protection**
 - IDS
 - Intrusion Prevention
 - Intrusion Detection
 - UTM Appliances
 - Anomaly Detection
 - Web Content Filtering
 - E-Mail Security Solutions
 - Desktop Protection
 - Server Protection
 - Vulnerability Management
 - Security Management
- Intelligent Monitoring**
 - IBM Proventia Network Intrusion Prevention
 - IBM Proventia Network Intrusion Prevention System (NIPS)
 - IBM Proventia Network Intrusion Prevention System (NIPS)
 - IBM Proventia Network Intrusion Prevention System (NIPS)
 - IBM Proventia Network Endpoint Security
 - IBM Proventia Server Intrusion Prevention
 - IBM Proventia Multi-Format Security
 - IBM Proventia Device Endpoint Security
 - IBM Proventia Server Endpoint Security
 - IBM Proventia Device Prevention
 - IBM Proventia Device Prevention
- Desktop Protection**
 - IBM Proventia Desktop Endpoint Security
 - IBM Proventia Desktop Endpoint Security
 - IBM Proventia Desktop Endpoint Security
 - IBM Proventia Desktop Endpoint Security
- Server Protection**
 - IBM Proventia Server Intrusion Prevention
 - IBM Proventia Server Endpoint Security
 - IBM Proventia Server Defense
- Vulnerability Management**
 - IBM Impact Scanner Software
 - IBM Proventia Network Enterprise Scanner

Network Packet Sniffers and Protocol Analyzers Packet Storm

<http://packetstormsecurity.org/defense/sniff/>

The screenshot shows the 'Sniff!' section of the Packet Storm website. It displays a list of files and advisories:

- # Directory: /sniff/**
 - Description: Immense packet sniffer collection written in C/C++.
 - Last Modified: Sep 6 02:51 05 2007
- # Directory: /sniff/**
 - Description: Sniff is a powerful suite of utilities based on network sniffing that are useful for penetration testing.
 - Last Modified: Sep 6 02:51 18 2007
- # Directory: /ethereal/**
 - Description: Ethereal is a Windows and UNIX-based sniffer with a nice GUI that makes it easy to view protocol information.
 - Last Modified: Sep 6 02:51 25 2007
- # Directory: /fiddler/**

Network Protocol Analyzers Softpedia

<http://www.softpedia.com/get/Network-Tools/Protocol-Analyzers-Sniffers/>

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

- **WinPcap 4.1 Beta 2**
- **WinPcap** memungkinkan Anda meng-capture dan mentransmisikan network packets 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 ini mampu menganalisa protocol yang menggunakan sistem operasi XP/2K Raw Socket, ukuran file download: 5.97 MB, dan dapat dijalankan pada berbagai Windows family OS.
- **SniffPass 1.03.** Mampu meng-capture password yang melewati network adapter komputer Anda. File download: 41 KB 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, dijalankan pada 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 tracing dalam menemukan informasi URL yang lalu lalang pada LAN. Berukuran 1.39 MB dan dapat dijalankan dalam lingkungan Windows.



Computer and Network Tools

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

<http://fire.dmzs.com/?section=tools>

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



Foundstone

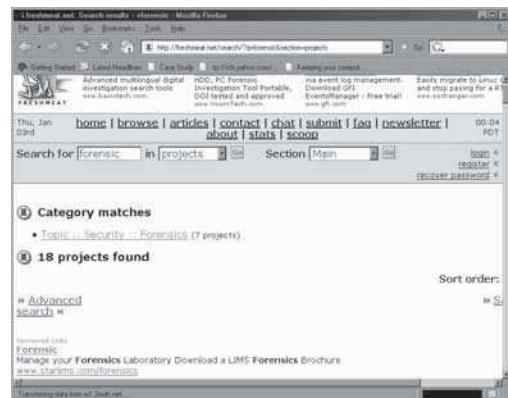
<http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm>

Anda dapat temukan berbagai software gratis kategori software forensik, misalnya **The Forensic Toolkit TM 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
- NTLast™ v3.0
- ShoWin™ v2.0
- PatchIt™ v2.0
- Vision™ v1.0
- BinText

Freshmeat

<http://freshmeat.net/search/?q=forensic§ion=projects>



Open Source Digital Forensics Analysis Tool Categories

(<http://www.opensourceforensics.org/tools/categories.html>)

Software yang Anda dapatkan di sini diorganisasi ke dalam beberapa spesifikasi sebagai berikut:

- Bootable Environments:** Anda dapat mem-boot sistem *suspect* dalam tingkat kelayakan yang terpercaya.
- Data Acquisition/IR Tools:** Software ini memungkinkan Anda untuk mengumpulkan berbagai data pada sistem *suspect*.
- Media Management Analysis Tools:** Software ini memungkinkan Anda untuk melakukan pemeriksaan terhadap struktur data, media semisal tabel partisi.
- File System Analysis Tools:** Pemeriksaan file sistem dan disk image, menampilkan konten file dan metadata 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 lalu lintas jaringan.

The screenshot shows the homepage of the Open Source Digital Forensics Analysis Tool Categories. It features a navigation bar at the top with links for Home, Contact Us, News, Merchandise, Links, and Chat. Below the navigation is a large banner for "Penguin Sleuth Kit". The main content area is titled "Open Source Forensic Tool Categories" and lists six categories with brief descriptions:

- Bootable Environments:** Software that you can use to boot a suspect system into a trusted state.
- Data Acquisition / IR Tools:** Software that you can use to collect data from a suspect system.
- Media Management Tools:** Software that you can use to examine the data structures that organize media, such as partition tables and disk labels.
- File System Analysis Tools:** Software that you can use to examine a file system or disk image and extract files.
- Application Analysis Tools:** Software that you can use to analyze the file content.
- Network Analysis Tools:** Software that you can use to analyze network packets and traffic. This does not include tools from network devices.

At the bottom of the page, there is a copyright notice for 2004-2007 by Brian Carrier and a link to www.openforensics.org.

Penguin Sleuth Kit

<http://www.linux-forensics.com/forensics/pensleuth.html>



Talisker Security Wizardry Portal

<http://www.networkinfiltration.co.uk/>

The Sleuth Kit

<http://www.sleuthkit.org/sleuthkit/tools.php>

The Ultimate Collection of Forensic Software (TUCOFS)

<http://www.tucofs.com/tucofs.htm>

The screenshot shows the homepage of the TUCOFS website. At the top, there is a banner with the text "Welcome!" and "Proceed to TUCOFS". Below the banner, there is a section titled "What is TUCOFS?". The main content area has a heading "TUCAFS, or TUCOFS, stands for The Ultimate Collection of Forensic Software. This site places all free information pertaining to tools used by the latest and greatest Internet based researchers for High Tech Law Enforcement purposes. Resource types include files, software, websites and documentation. TUCAFS can be used as an index pointing you to various resources, allowing you to quickly find exactly what you are looking for." followed by a list of bullet points. At the bottom, there is a "Let us know! Send Email to tucofs@verizonforensics.com" and a "How are information resources added to the site?" section.

Top 75 Security Tools

<http://www.insecure.org/tools.html>



Trinux

<http://trinux.sourceforge.net/>



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

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

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



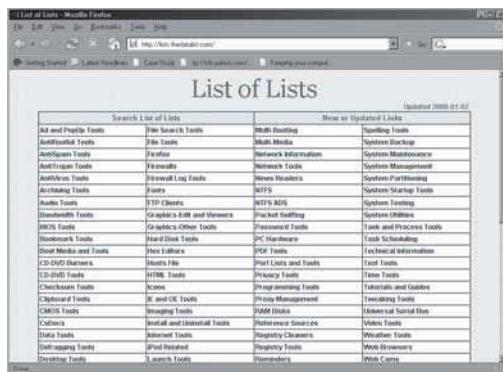
- **NetStumbler:** Free Windows 802.11 Sniffer. Aplikasi dengan platform sistem operasi Windows yang mampu untuk menemukan *wireless access points* yang didapati terbuka ("wardriving"), disediakan pula versi yang dapat dijalankan oleh platform WinCE untuk PDA.
- **WebInspect.** Salah satu Web Application Scanner yang tangguh. SPI Dynamics' WebInspect "application security assessment tool" membantu Anda dalam mengetahui kelemahan pada lapisan application web. Menganalisa apakah webserver dikonfigurasi dengan benar melalui serangkaian pengujian berupa serangan web seperti: parameter injection, cross-site scripting, directory traversal, dan lain sebagainya.

Berbagai Tool Komputer Lainnya

Checksum Tools

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

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



Computer Forensics Tools, Software, Utilities

<http://www.forensix.org/tools/>

Dalam website forensix.org, banyak dokumentasi berkenaan dengan forensik, termasuk software forensik yang dikelompokkan ke dalam tiga bagian, antara lain:

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

The screenshot shows a Google search results page for 'Computer Forensics Tools'. The top result is a link to 'Computer Forensics Tools, Digital Evidence software, Utilities' which includes a sidebar for 'Computer Forensics' and 'Computer Forensics Software'. Other results include links to 'Computer Forensics Tools & Suites' and 'Integrity Management Software'.

Funduc Software

<http://www.funduc.com/>

Di sini Anda dapat menemukan berbagai shareware dan freeware software forensik.

The screenshot shows the homepage of Funduc Software. It features a large logo for 'FUNDUC Software' and a banner for 'Home of Award Winning Shareware and Freeware'. Below the banner, there are sections for 'Search & Replace', 'Directory Toolkit', 'Shortcut Doctor', 'Developer Products', and 'Free Stuff'. A sidebar on the right provides information about their software products like 'File Doctor', 'File Doctor Home', 'File Doctor Business', and 'File Doctor Home Business'.

Berbagai Network Tools

Common Vulnerabilities and Exposures (CVE)

<http://www.cve.mitre.org/compatible/product.html>

Product ID	Description	Type	Country	Status
NSA/I4F	rec28740 - The NSA's Linux Security Updates, Announcements, and Advisories	Vulnerability Database	Spain	DECLARED EXIST & VERIFIABLE
Apache SSL/TLS Scanner	Apache SSL/TLS Scanner	Apache Web Server Vulnerability Database	United States	DECLARED EXIST & VERIFIABLE
Apache SSL/TLS Scanner	Apache SSL/TLS Scanner	Apache Web Server Vulnerability Assessment Tool	United States	DECLARED EXIST & VERIFIABLE
Apache SSL/TLS Scanner	Apache SSL/TLS Scanner	Database Vulnerability Assessment Tool	United States	DECLARED EXIST & VERIFIABLE
Apache SSL/TLS Scanner	Apache SSL/TLS Scanner	Database Vulnerability Assessment Tool	United States	DECLARED EXIST & VERIFIABLE
Apache SSL/TLS Scanner	Apache SSL/TLS Scanner	Database Vulnerability Assessment Tool	United States	DECLARED EXIST & VERIFIABLE

JaguarSoft - Internet Security, Anti-Spy, Anti-Fraud, One-Time-Password, Parental Control,SMPP - Microsoft Internet Explorer

ISEMARKET Consultancy & Developments

Products

- JaguarEditControl
- JaguarI4FD
- JaguarOTP
- JaguarForensics
- JaguarPasswords
- JaguarDeviceLock
- JaguarSMPP
- Financial Products
- JaguarChildLock
- JaguarIPRecorder
- JaguarGRS
- Mobile Developments

About us

Founded in Istanbul at 1999, ISEMARKET Consultancy & Developments LTD, provides High Quality & Robust solutions On Software development and consultancy services. Develops solutions on Internet & Computers security, Real-time market feeds & User Interfaces and Telephone & Camera & Iphone recording systems. JaguarControls for Web - JaguarEdit & JaguarI4FD protects millions of users for Secure On-line Banking.

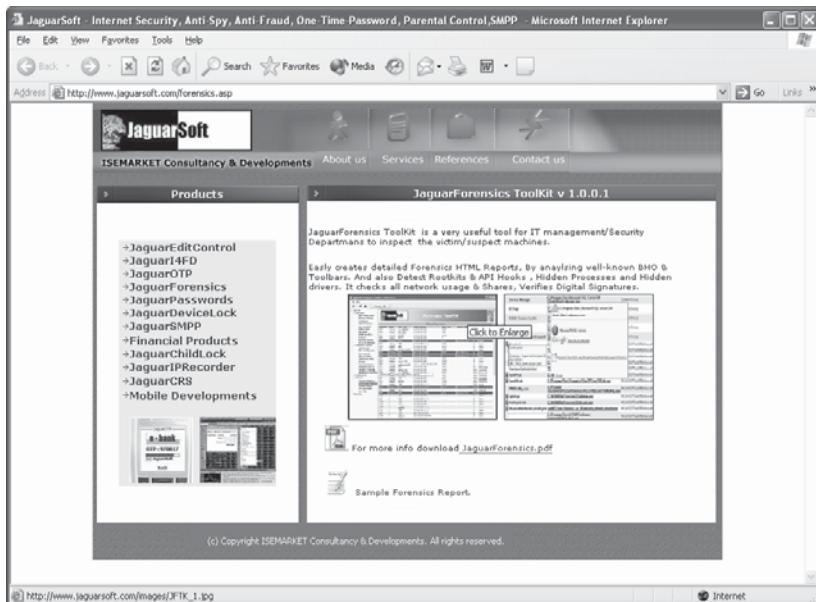
News & Events

- + **JaguarEditControl**
implemented in Cyprus TurkishBank On-line Banking Site, May 2006
- + **JaguarSMPP** implemented in UAE ,AbuDhabi COC Oct 2005
- + **JaguarEditControl**
implemented in T.ISBANK On-line Banking Site, March 2005
- + **JaguarEditControl**
implemented in TurkishBank On-line Banking Site, July 2004
- + **JaguarPasswords**
implemented on YAPIKREDİ BANK Network, April 2004
- + **JaguarEdit & I4FD Control**
implemented in Anadolulmians On-line Banking Site, June 2004
- + **JaguarEdit & I4FD Control**
implemented in GARANTIBANK On-line Banking Site, Dec 2003

Gambar 2.1 Website JaguarSoft.com

Banyak sekali software spesifikasi forensik yang memiliki fitur sangat baik, Anda dapat menggunakan software komersial semisal Jaguar Forensics Toolkit. Penulis melihat bahwa software ini sangat kaya fitur, salah satunya adalah *report generator* yang baik untuk memenuhi kebutuhan forensik.

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



Gambar 2.2 Website JaguarSoft.com – Produk JaguarForensics Toolkit

The screenshot shows a Microsoft Internet Explorer window displaying a sample forensics report at <http://www.jaguarsoft.com/forensics/>. The report includes sections for 'Computer Info' (Computer Name: ASUSNB, Description: Password Captured), 'Inspected by' (Support 1, JaguarSoft, Security Department, 111 2222 333, support@jaguarsoft.com), 'Owner's Contact Info' (E-BANK 1), 'Inspector Comments', and 'Reported Items'. The 'Reported Items' section is a large list of system components including BIOS Information, Video Controller, Keyboard, Pointing Devices, Boot Configuration, System Accounts, System EventLog, Installed Applications, Running Services, Browser Helper Objects, Hidden Processes, Network Adapters, and IP Route Table on the left, and Physical Memory, Boot HardDisk, USB Controllers, PCMCIA Controller, Environment, Groups, Security EventLog, Installed Services, System Drivers, ToolBars, Hidden Drivers, Network Connections, and Host Files on the right.

Gambar 2.3 Website JaguarSoft.com – Report Generator Sample

This screenshot shows a Microsoft Internet Explorer window displaying BIOS information. The title bar reads "ASUSN BIOS Information - Microsoft Internet Explorer". The address bar shows the URL "http://www.jaguarsoft.com/forensics/includes/BIOS_Information.htm". The main content area is titled "Forensics ToolKit" and "BIOS Information". A table lists various BIOS properties with their values:

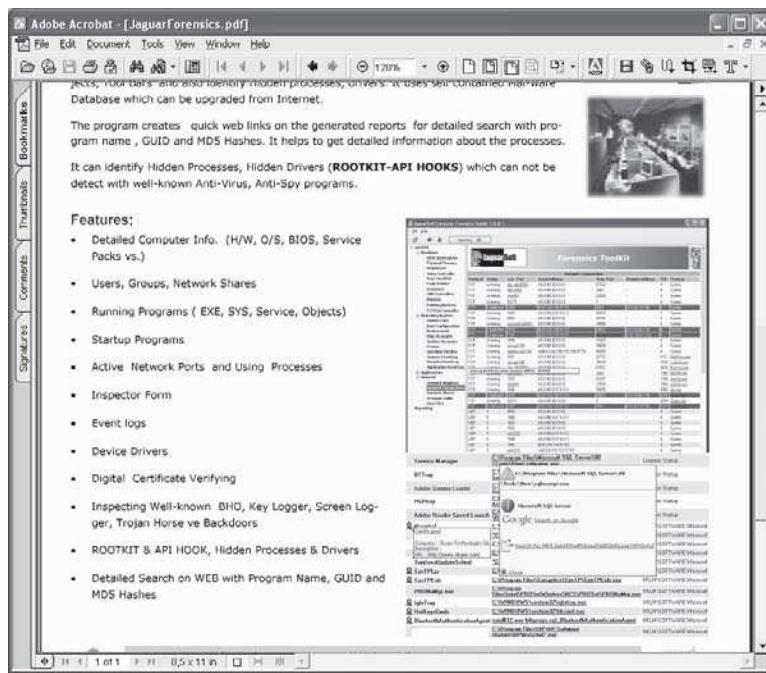
Property	Value
BioCharacteristics	407891011121415161719222324252627128293003203406074041
BIOSVersion	A M I - 12000408
BuildNumber	-
Caption	Default System BIOS
CodeSet	Default System BIOS
CurrentLanguage	enUS
Description	Default System BIOS
IdentificationCode	1
InstallableLanguages	-
InstallDate	-
LanguageEdition	-
LnfLanguages	enUS
Manufacturer	American Megatrends Inc.
Name	Default System BIOS
OtherTargetOS	-
PrimaryBIOS	True
ReleaseDate	20041208000000.000000+000
SerialNumber	SSN12345678901234567
SMBIOSBIOSVersion	0212
SMBIOSMajorVersion	2
SMBIOSMinorVersion	3
SMBIOSPresent	True
SoftwareElementID	Default System BIOS
SoftwareElementState	3
Status	OK
TargetOperatingSystem	0
Version	A M I - 12000408

Gambar 2.4 Website JaguarSoft.com – BIOS Information Report

This screenshot shows a Microsoft Internet Explorer window displaying network connection information. The title bar reads "ASUSN Network Connections - Microsoft Internet Explorer". The address bar shows the URL "http://www.jaguarsoft.com/forensics/includes/Network_Connections.htm". The main content area is titled "Forensics ToolKit" and "Network Connections". A table lists network connections with columns for Protocol, Status, Loc. Port, Local Address, Rem. Port, Remote Address, PID, and Process:

Protocol	Status	Loc. Port	Local Address	Rem. Port	Remote Address	PID	Process
TCP	Listening	4d1:db[3050]	ASUSN (0.0.0.0)	57532	-	4	System
TCP	Listening	Http[443]	ASUSN (0.0.0.0)	2080	-	4	System
TCP	Listening	Http[80]	ASUSN (0.0.0.0)	32329	-	4	System
TCP	Listening	52271	ASUSN (0.0.0.0)	2	-	4	System
TCP	Established	1058	B05 [192.168.57.57]	1863	[207.46.107.58]	4	System
TCP	Listening	1046	ASUSN (127.0.0.1)	39070	-	4	System
TCP	Listening	6697	ASUSN (0.0.0.0)	26732	-	4	System
TCP	Listening	microsoft-ds[445]	ASUSN (0.0.0.0)	18959	-	4	System
TCP	Established	1078	B05 [192.168.57.57]	25672	[75.176.60.174]	4	System
TCP	Established	1538	B05 [192.168.57.57]	25672	[207.46.107.58]	4	System
TCP	Listening	1035	ASUSN (0.0.0.0)	43207	-	4	System
TCP	Listening	connec[135]	ASUSN (0.0.0.0)	39038	-	4	System
TCP	Listening	netbios-ssn[139]	netbios-ssn[139] (192.168.57.57)	45099	-	4	System
TCP	Listening	6697	ASUSN (0.0.0.0)	26732	-	516	RMIHvC.exe
TCP	Listening	connec[135]	ASUSN (0.0.0.0)	39038	-	1052	svchost.exe
TCP	Listening	4d1:db[3050]	ASUSN (0.0.0.0)	57532	-	1616	fbsvc.exe
TCP	Listening	Http[443]	ASUSN (0.0.0.0)	2080	-	1968	inetinfo.exe
TCP	Listening	1035	ASUSN (0.0.0.0)	43207	-	1968	inetinfo.exe
TCP	Listening	Http[80]	ASUSN (0.0.0.0)	32329	-	1968	inetinfo.exe
TCP	Listening	1046	ASUSN (127.0.0.1)	39070	-	2060	glu.exe
TCP	Established	1078	B05 [192.168.57.57]	25672	[75.176.60.174]	3304	Java.exe
TCP	Listening	52271	ASUSN (0.0.0.0)	2	-	3304	Skype.exe
TCP	Established	1058	B05 [192.168.57.57]	1863	[207.46.107.58]	3344	Java.exe
UDP	0	4500	ASUSN (0.0.0.0)	-	-	4	System
UDP	0	1068	ASUSN (127.0.0.1)	-	-	4	System
UDP	0	1025	ASUSN (0.0.0.0)	-	-	4	System
UDP	0	1038	ASUSN (0.0.0.0)	-	-	4	System
UDP	0	65124	ASUSN (127.0.0.1)	-	-	4	System

Gambar 2.5 Website JaguarSoft.com – Network Connections Information Report



Gambar 2.6 Website JaguarSoft.com – pdf Download

Gambar 2.6 adalah deskripsi program tersebut dalam file pdf yang dapat Anda download.

Fakta di Balik Forensik

Sebenarnya dalam menemukan fakta yang sesungguhnya, ini melibatkan kemampuan Anda membaca dan menganalisa data. Meskipun demikian, secara umum Anda sudah dapat dikatakan jeli dalam mengalami fakta dari data dan informasi yang terbungkus dalam file atau dokumen.

Dalam hal ini beberapa komponen sudah tersaji di depan Anda dan digolongkan berdasarkan perangkat komputer yang digunakan, tinggal bagaimana Anda menanggapi kumpulan data/informasi spesifik untuk dikelola lebih lanjut.

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:

- Bukti dari tindak pencurian
- Pemalsuan
- *Remarking*

Access Control Devices

Mencakup di dalamnya:

- Smart Card
- Dongles
- Biometric Scanners

Smart Card - Perangkat ini ringkas, maka dari itu dikategorikan sebagai *handheld device*, tentunya memiliki micro processor terintegrasi, memiliki kemampuan seperti menyimpan nilai mata uang, kunci enkripsi dan authentication information dengan penggunaan password, digital certificate, dan informasi lainnya.

Dongle - perangkat yang dipasangkan pada port komputer, dan informasi yang dimungkinkan disimpan mirip dengan Smart Card.

Biometric scanner - perangkat ini umum 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 telpon, mungkin dipasang sedemikian rupa antara line telpon dan telpon.

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

Perangkat ini sangat mengandalkan baterai dengan kemampuan terbatas, tentunya dibutuhkan penanganan sedemikian rupa karena data dalam prosesnya mungkin hilang atau tidak tersimpan dengan baik. 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 telpon
- Tapes

Kamera Digital

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

Bukti potensial yang dimungkinkan pada kamera digital:

- Images
- Informasi tanggal dan waktu
- Removable cartridges
- Video
- Sound

Handheld Devices (Personal Digital Assistants, Electronic Organizers)

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

Kebutuhan organizer menjadi salah satu faktor yang berpengaruh pada perangkat sejenis ini. Sarana kemudahan komunikasi yang mirip dengan *smart phone* menjadi fitur tambahan yang membuatnya menjadi sedemikian menarik.

Penanganan perangkat ini sebagai evidence tentunya punya banyak pertimbangan dan pemberlakuan, salah satunya karena power yang terbatas mengandalkan baterai, data "berjalan" mungkin saja hilang karena power yang terbatas.

Bukti potensial:

- Buku alamat
- Appointment calendars/information
- Dokumen
- E-mail
- Handwriting (tulisan tangan)
- Password
- Buku telpon
- Pesan teks
- Pesan suara

Hard Drives

Jika Anda berbicara mengenai hard-drive, tentu yang dimaksudkan adalah harddisk, dimana perangkat baca tulis terintegrasi dengan media penyimpanan berupa plat-plat magnetis, yang menjadi media penyimpanan populer saat ini dan menjadi kebutuhan dari 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 harddisk, semisal berbagai file image, file audio dan video, teks, dan lain sebagainya.

Bukti potensial yang ada tentunya sangat berkaitan dengan sistem komputer secara keseluruhan.

Memory Cards

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 sticks
- Smart Cards
- Flash memory
- Flash cards.

Bukti potensial yang ada tidak jauh dari bukti potensial sistem komputer, karena fungsinya sebagai media penyimpanan dan hubungannya dengan sistem komputer secara umum.

Modems

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 telpon, wireless, dan berbagai media komunikasi lainnya.

Bukti potensial: 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 spesi-

fik, 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 dari dibangunnya jaringan komputer tidak lain adalah fasilitas sharing sumber daya yang mencakup media penyimpanan, file sharing, printer sharing, scanner, dan berbagai sumber daya komputer lainnya dan fasilitas komunikasi.

Bukti potensial:

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

Router, Hub, dan Switch

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

Hub dan Switch 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 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: perangkat itu sendiri.

Server

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 pemakaian terhadap kebutuhan akan:

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

Bukti potensial memiliki karakteristik yang mirip dengan sistem komputer pada umumnya.

Network Cable dan Connector

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, dan 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: perangkat komponen itu sendiri.

Pager

Bukti potensial:

- Informasi alamat
- Pesan teks
- E-mail
- Pesan suara
- Nomor telpom

Printer

Perangkat output populer untuk menghasilkan 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
- Parallel

- 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 yang harus dialami dengan baik, ada informasi yang tersimpan yang bahkan efektif digunakan sebagai evidence.

Bukti potensial:

- Dokumen
- Harddrive
- Ink cartridges
- Network identity/information.
- Superimposed images pada roller
- Waktu dan tanggal
- Log penggunaan

Removable Storage Devices dan Media

Perangkat ini digunakan untuk menyimpan informasi dengan metode yang beragam, mencakup secara elektris, magnetis, atau digital. Ragam perangkatnya antara lain:

- Floppy disk
- CD

- DVD
- Cartridges
- 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 file multimedia, dan lain sebagainya.

Bukti potensial: sudah didefinisikan.

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 theft), counterfeiting, dan lain sebagainya. Bahkan kaca yang ada pada scanner mungkin saja didapati sidik jari yang tercecer.

Bukti potensial: perangkat yang bersangkutan.

Telpon

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

- Kabel telpon
- Transmisi radio
- *Cellular systems*
- 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 telpon
- Text messages
- Voice mail
- Web browser

Perangkat Elektronik Lainnya

Ada banyak perangkat elektronik lainnya yang dapat kemudian ditambahkan 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

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. Informasi untuk keperluan forensik didapat dengan melakukan pembacaan pada *magnetic stripe*.

Bukti potensial:

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

Digital Watches

Fitur digital watches tidak sesederhana namanya, memiliki kemampuan meng-organisasi address books, jadwal aktivitas, berbagai catatan, yang bahkan dapat dikonversi dengan sangat kompatibel untuk diconnect dengan komputer.

Bukti potensial:

- Address book
- Notes
- Appointment calendars
- Phone numbers
- E-mail

Mesin Fax

Mesin fax memiliki fitur untuk menyimpan nomor telpon, catatan pengiriman dan penerimaan dokumen, bahkan memungkinkan untuk menyimpan banyak dokumen untuk dikirim kemudian.

Bukan hanya itu, dokumen yang pernah dikirim dan diterima terdokumentasi baik pada mesin fax.

Bukti potensial:

- Dokumen
- Nomor telpo
- Film cartridge
- Log atau catatan pengiriman dan penerimaan

Global Positioning System (GPS)

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

Bukti potensial yang dimungkinkan antara lain:

- Rumah
- Previous destinations
- Catatan perjalanan
- Way point coordinates
- Way point name

Uncover Digital Evidence

Fakta berkata dan fakta berbicara, tetapi kapan fakta muncul ke permukaan tergantung dari keahlian investigator dalam olah forensik dan menyajikannya sedemikian rupa.

Kerumitan dan komponen komputer yang tidak kasat mata yang seharusnya dimanfaatkan dengan baik oleh investigator, justru di sinilah banyak celah-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 yang harusnya 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 harddisk dan masih sangat mudah untuk mendapatkannya kembali!
- File yang dihapus dapat dengan mudah di-recover.
- Me-rename file untuk mencegah deteksi, ternyata sama sekali tidak berarti.
- Formatting saja tidak cukup untuk menghapus data-data, masih banyak jejak lain yang ditinggalkan.

- Web-based email ternyata dapat di-recover pada komputer yang bersangkutan.
- File yang ditransmisikan melalui jaringan ternyata dengan mudah di-reassembled dan digunakan sebagai evidence.
- Install aplikasi sangatlah mudah, tetapi tidak demikian untuk un-install aplikasi, banyak jejak-jejak yang ditinggalkan.
- Data “Volatile” meskipun tidak tersimpan pada harddisk secara permanen seperti *non-volatile*, ternyata daya lekatnya pada media penyimpanan semisal memori, melekat cukup lama bahkan setelah proses reboot.
- Banyak jejak ditinggalkan dari program aplikasi.
- Menggunakan *encryption* tidaklah cukup, data dapat didapatkan kembali melalui *decryption*.
- Software anti-forensic masih saja belum maksimal, banyak software forensik untuk mengalami data dan informasi.
- Menggunakan magnet ternyata tidak membuang dan merusak data pada storage device.
- Mutilasi media penyimpanan ternyata tidak efektif, perlu melakukan mutilasi secara ekstrim.
- Data memang sangat sulit untuk dimusnahkan.

BAB 3

Metode Komputer Forensik

- Pemodelan Forensik
- Tip Pemberlakuan Forensik
- Tip Bagi Pemula yang Sadar Forensik
- Berbagai Model Form Forensik

Pemodelan Forensik

Model forensik melibatkan tiga komponen yang dirangkai, diberdayakan, dan dikelola sedemikian rupa menjadi tujuan akhir dengan segala kelayakan dan kualitas.

Tiga komponen ini mencakup:

- Manusia (*People*)
- Peralatan (*Equipment*)
- Aturan (*Protocol*)

Manusia (Brainware) yang kita bahas di bab lalu, tentunya diperlukan kualifikasi tertentu untuk mencapai kualitas yang diinginkan. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahli lain ceritanya, dibutuhkan lebih dari sekedar pengetahuan. Pengalaman yang membuatnya dikatakan "ahli".

Hasil akhir dengan kualitas yang menyertainya tentu 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 paling tipis semisal etika dan moral.

Apakah langkah-langkah yang diambil untuk menggali evidence dan menemukannya melanggar batasan hukum atau etika? Disinilah kualitas diuji!

Seperti digariskan, umumnya keahlian komputer forensik dispesifikasi ke dalam beberapa bagian, dan diperlukan kriteria untuk dapat memenuhi standar yang diharapkan. Mungkin bisa diperbandingkan di sini, spesifikasi dengan keahlian mengiringi rentang pembelajaran yang diperlukan, tetapi komposisinya tidaklah baku, bahkan sering disebut sebagai Examiner atau Investigator. Meskipun demikian, informasi ini dapat menjadi pembanding secara umum saja. Berikut kriteria yang dimaksud:

- Computer Forensic Examiner, memiliki kemampuan dan karakteristik sebagai:
 - ✓ Melakukan pengujian terhadap media original.
 - ✓ Mengekstrak data bagi Investigator untuk di-review.
 - ✓ Dibutuhkan 4 sampai 6 minggu pelatihan.
- Computer Investigator
 - ✓ Harus memiliki pengalaman yang teruji dan "ahli".
 - ✓ Memahami jaringan komputer, internet, berbagai komunikasi yang melibatkan teknologi komputer/informasi.
 - ✓ Dibutuhkan satu sampai dua minggu pelatihan.

- Digital Evidence Collection Specialist
 - ✓ Dikarenakan spesifikasi pekerjaannya, dapat dikatakan sebagai first responder.
 - ✓ Dibutuhkan 2 sampai 3 hari pelatihan.
 - ✓ Mendapatkan dan menghadirkan bukti komputer mencakup pula media penyimpanan jika memang ada.

Anda perhatikan, ada spesialisasi, spesifikasi, dan beban pelatihan yang tentunya berdampak pada pencapaian kualitas.

Peralatan pun harus digunakan sedemikian rupa untuk mendapatkan bukti-bukti (evidence) yang berkualitas dan tidak "kotor". Ada banyak perlatatan yang dibutuhkan melibatkan perangkat lunak spesifik dan berbagai perangkat keras dan berbagai media penyimpanan dalam menangani data-data/evidence nantinya.

Yang terpenting adalah aturan (protocol), aturan dalam menggali, mendapatkan, menganalisa, dan akhirnya menyajikan dalam laporan-laporan tentunya melibatkan aturan. Di sini

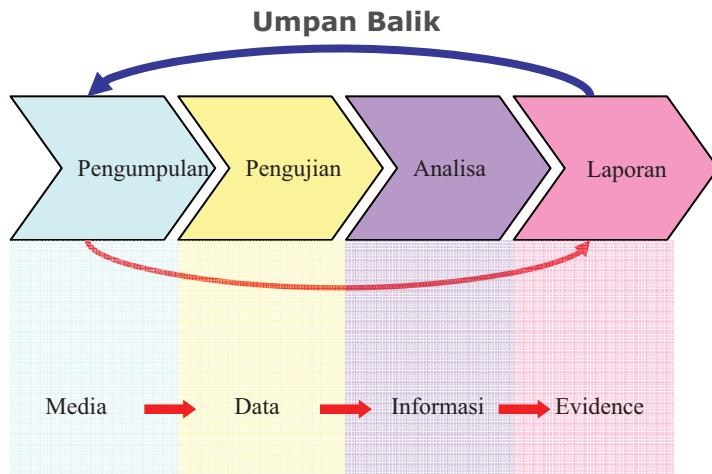
diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam tindakannya diadakan peran-peran konsultasi, mencakup pengetahuan akan teknologi informasi dan ilmu-ilmu hukum.

Triniti antara manusia (people), peralatan (equipment), dan aturan (protocol) akan melebur dan berkolaborasi untuk mengisi setiap fase-fase dalam komputer forensik.

Ada empat fase dalam komputer forensik, antara lain:

- Pengumpulan
- Pengujian
- Analisa
- Laporan

Ada objek yang dikelola dari proses setiap fase, dimulai dari media dan kemudian didapati "evidence" di akhir proses. Tentunya umpan balik diberlakukan untuk menganalisa kembali hasil yang didapat dengan tujuan semula. Anda dapat perhatikan konektivitas yang terjalin mencakup proses dan hasil pada Gambar 3.1.



Gambar 3.1 Tahap-tahap komputer forensik

Pengumpulan Data

Ini adalah langkah pertama dalam proses forensik untuk mengidentifikasi sumber-sumber potensial dan bagaimana kemudian data dikumpulkan.

Pengumpulan ini melibatkan proses dan metode yang semakin kompleks karena perkembangan teknologi yang demikian pesat. Ada banyak komputer, ada banyak ragam media penyimpanan, dan ada banyak jaringan komputer dengan segala teknologi yang dilekatkan terhadapnya. Tentunya kerumitan ini memerlukan penanganan berbeda-beda.

Data yang marak didapatkan bertumpu pada *personal computer* atau *desktop computer*. Anda perhatikan

bahwa setiap orang ingin memiliki sendiri satu komputer 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-sumber daya. Salah satu *personal computer* yang sangat populer dewasa ini yang demikian portable dan bermobilitas tinggi yang dapat terintegrasi ke jaringan, membuat laptop banyak diminati dan tentunya banyak sumber-sumber data bisa didapatkan.

Perangkat-perangkat tadi tentunya harus dan pasti memiliki fitur penyimpanan, bahkan tren-nya perangkat demikian diberikan kapasitas penyimpanan yang cukup besar, serta penyimpanan yang portable hadir dengan bentuk yang ringkas dan 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:

- Thumb Drives
- Memory Card
- USB Flash Disk
- Optical Disc
- Magnetic Disc

Tidak hanya komputer desktop yang memiliki media penyimpanan dan memungkinkan integrasi penyimpanan di dalamnya, ternyata ini pun meluas pada:

- PDA
- Telpon Selular
- Kamera Digital
- Digital Recorder
- Audio Player (iPod, MP3 Player, dan lainnya)

Perangkat penyimpanan dan data-data tadi mungkin dengan mudahnya kita dapatkan di suatu organisasi atau perusahaan, tetapi akan ada banyak organisasi lain yang mungkin dapat dimintai keterangan sehubungan dengan data dan informasi yang mungkin terelasi, misalnya saja jika melibatkan jaringan internet, mungkin dibutuhkan log aktivitas jaring dari ISP (Internet Service Provider). Tentunya untuk mendapatkan informasi/data sedemikian akan ada serangkaian prosedur, misalnya saja mungkin dibutuhkan surat keterangan resmi secara hukum untuk mendapatkan catatan-catatan/log demikian.

Atau bagaimana kalau organisasi yang lain menyangkut peralatan milik pribadi/pegawai perusahaan atau rekan bisnis perusahaan (kontraktor, perusahaan oursourcing), tentunya tidak mudah untuk dengan begitu saja mengumpulkan data darinya.

Tindakan pengumpulan data mungkin melibatkan perkara lain yang paling halus, mencakup pula etika di dalamnya, mungkin akan sangat

berguna untuk memonitoring pengguna komputer dalam beraktivitas, tetapi privasi bisa dilanggar dan menimbulkan masalah lain lagi pada akhirnya.

Pengumpulan data ini mencakup aktivitas seperti:

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

Tentu saja daya yang didapatkan harus dapat diandalkan dan relevan terhadap kasus. Data menjadi barang berharga yang rapuh, maka dari itu dengan serangkaian prosedur diharapkan integritas data dapat terpelihara.

Lain lagi penanganan data yang melibatkan peralatan, misalnya dengan PDA, telpon 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*).
 - ✓ Likely Value

- ✓ Volatility
- ✓ Amount of Effort Required
- Mendapatkan data (*Acquire the data*).
- Analisa integritas data (*Verify the integrity of the data*).

Berikut dijabarkan masing-masing prosesnya:

Membuat Perencanaan untuk Mendapatkan Data

Membuat perencanaan dalam mendapatkan data adalah langkah paling penting, ada banyak titik-titik 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 perlu menjadi pertimbangan, antara lain:

Kemiripan nilai (*Likely Value*). Untuk mengacu pada nilai yang mirip, tentu Examiner membutuhkan pemahaman akan situasi dan kondisi, mungkin berdasarkan pengalaman sebelumnya, perkiraan yang relevan diperlukan untuk menentukan *likely value*.

Volatile, data kategori ini tentunya akan hilang begitu saja sewaktu listrik dimatikan, data-data yang menetap di memori dan ada karena

sistem berjalan akan hilang dengan mudahnya jika listrik mati. Karena alasan inilah data yang tergolong Volatile mendapatkan prioritas dibandingkan data-data non-volatile.

Tetapi prioritas demikian tidaklah mutlak, akan didapat 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 transaksi yang demikian dinamis berubah seiring sistem berjalan.

Upaya dalam mendapatkan data (*Amount of effort required acquiring data*). Untuk mendapatkan data dari sumber yang ada tidaklah begitu saja dapat dilakukan, meskipun secara teknik sangat dimungkinkan, belum tentu jika mempertimbangkan melalui kacamata hukum. Misalnya saja, akan lebih mudah mendapatkan data yang disumberkan pada network router daripada mendapatkan data yang disumberkan pada ISP (Internet Service Provider).

Kita lihat tadi beberapa prioritas yang menjadi acuan dan cara menangani dalam mendapatkan data, meskipun demikian, pada kenyataannya tidak semua sumber-sumber data yang tergolong data sumber potensial dapat dimanfaatkan.

Diperlukan lebih dari sekedar menemukan sumber data dan mengambil kompleksitas prioritas yang muncul, berbagai metode dokumentasi, penuntun praktis, dan prosedur untuk dapat mencapai efektivitas yang tinggi dalam langkah ini.

Mendapatkan Data (Acquire the data)

Tidak selalu dibutuhkan "kekuatan" yang besar dalam mendapatkan data, seandainya data yang diperlukan memang sudah didapatkan dengan security tools, analysis tools, atau lain caranya.

Lain halnya jika cara-cara tersebut tidak dimungkinkan, Anda mungkin membutuhkan tool spesifik forensik. Ini mencakup mengumpulkan data-data yang tergolong volatile, mengambilnya dengan menduplikasi data sumber non-volatile, dan mungkin dapat mencakup pula mengamankan sumber data original non-volatile.

Data yang diambil mungkin berasal dari komputer lokal atau mengaksesnya melalui jaringan komputer. Memang akan lebih baik jika data diambil pada komputer yang bersangkutan/komputer lokal dikarenakan kontrol maksimum terhadap data yang dilekatkan padanya. Tetapi lokal data tidak sepenuhnya *feasible*, misalnya saja sistem/komputer yang dialokasikan di tempat yang sulit

untuk dijangkau atau di lokasi yang terpisah secara geografis.

Dikarenakan data dialokasikan di tempat yang terpisah, tentunya beberapa pertimbangan akan muncul, misalnya seberapa banyak data yang diperlukan dan data-data apa saja yang perlu dikumpulkan. Pertimbangan demikian dibuat karena sumber daya jaringan memiliki kelebihan dan juga keterbatasannya.

Lebih jauh lagi dipertimbangkan, apakah perlu mengambil data yang ada pada sistem yang berbeda atau cukup sistem tertentu saja. Kelayakan, kompleksitas, dan upaya yang dikerahkan akan mempengaruhi 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 penggunaan tool dalam mengkalkulasi infomasi orisinil dan kemudian meng-copy-nya. Selanjutnya dilakukan analisa yang membandingkan apakah data hasil dan orisinil sama atau identik.

Pengujian

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

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

Harddrive berisi ribuan bahkan jutaan file, untuk mengidentifikasi data di dalamnya akan sangat menghabiskan konsentrasi dan melelahkan. Filtrasi akan mengeliminir sebagian data yang tidak dibutuhkan, misalnya data log minggu lalu yang terdiri dari jutaan record dan didapat belasan record yang kemudian digunakan untuk pemeriksaan lebih lanjut.

Ada banyak peralatan dan teknik digunakan dalam melakukan eliminasi terhadap tumpukan data. Pencarian basis 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, musik, atau berbagai file kompresi lainnya.

Pengetahuan yang menyeluruh akan jenis dan tipe file dapat dijadikan acuan dalam meng-exclude file yang mungkin memiliki persentase kelayakan/interest lebih.

Akan dijelaskan proses ini lebih lanjut, secara mendasar tahap ini mencakup mengalokasi file, mengekstrak file (mungkin melalui enkripsi, stenografi, uncompress, dan lainnya), atau mungkin melakukan pemeriksaan terhadap metadata, dan lain sebagainya.

Analisa

Begini informasi diekstrak, Examiner melakukan analisa untuk merumuskan kesimpulan dalam menggambarkan data. Analisa yang dimaksud tentunya mengambil pendekatan metodis dalam menghasilkan kesimpulan yang berkualitas didasarkan pada ketersediaan data. Atau bahkan sebaliknya, dengan menyimpulkan bahwa tidak ada hasil yang didapat, itu dimungkinkan!

Tugas Examiner mencakup pula kegiatan seperti mengidentifikasi user atau orang di luar dari pengguna,

(tetapi terlibat secara tidak langsung), mengidentifikasi lokasi, barang-barang, kejadian, dan menentukan bagaimana komponen-komponen tadi terelasi satu dengan yang lain sehingga didapati kesimpulan pada akhirnya, tentunya kompleksitas memunculkan banyak sumber data.

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 tentunya *host IDS log* menjadi histori dari aktivitas 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 sedemikian.

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

Dokumentasi dan Laporan

Reporting adalah tahap akhir dari proses komputer forensik, dalam tahap ini kita merepresentasikan informasi yang merupakan hasil dari proses analisis. Banyak faktor mempengaruhi Reporting, seperti berikut ini:

- **Alternative Explanations** (Penjelasan alternatif)

Jika informasi yang mengacu pada suatu kasus dikategorikan *incomplete*, tentunya hasil akhir didapatkan tidak memadai dan tidak dapat diandalkan untuk menelusuri kejadian. Bahkan jika didapatkan beberapa penjelasan yang masuk akal akan suatu kejadian, masing-masing harus dipertimbangkan dan diteruskan dalam proses *reporting*.

Apapun yang terjadi, analist harus menggunakan pendekatan dalam menentukan setuju atau menolak setiap penjelasan duduk perkara yang mungkin untuk diajukan.

- **Audience Consideration** (Pertimbangan peserta)

Menyajikan data atau informasi pada hadirin/audience sangat penting. Kasus yang melibatkan perundangan tentunya membutuhkan laporan detail/spesifik berkenaan informasi yang dikumpulkan, dan membutuhkan pula copy dari setiap fakta (*evidentiary data*) yang diperoleh.

Pertimbangan ini beralasan, misalnya saja administrator sistem mungkin ingin melihat lebih jauh *network traffic* lebih mendetail.

- **Actionable Information**

Proses reporting mencakup pula identifikasi *actionable information* yang didapat dari data-data terdahulu,

lu, darinya kita bisa mendapatkan informasi baru.

Misalnya saja daftar alamat seseorang (contact list) dapat dikembangkan lebih lanjut, yang kemudian menujukkan pada informasi lain tentang suatu tindak kriminal/kejadian.

Keuntungan lain dari *actionable information*; informasi yang didapatkan mungkin dapat digunakan untuk keperluan-keperluan mendatang, misalnya tujuan pengamanan seperti *backdoor* yang mungkin bisa dieksplorasi. Ini membutuhkan penanganan segera tentunya.

Dalam prosesnya, mungkin akan 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 metode dan berbagai aktivitas formal lainnya untuk melakukan identifikasi dan menjajaki perubahan yang terjadi. Perubahan ini menjadi suatu pola dan harus dimonitoring dengan seksama, tentunya proses monitoring harus mudah diakses, misalnya dengan menempelkan gambar, poster ataupun dokumen lainnya pada dinding atau apapun 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 juga metode yang menyertai forensik. Diperlukan pembelajaran dan menangkap perubahan dengan cepat, untuk itu dibutuhkan standar dan penyaringan untuk membuktikan kelayakan seseorang agar tergabung dengan tim. Skill perlu di-review kembali dalam rentang waktu satu tahun.

Ini memastikan bahwa anggota tim memiliki skill yang ter-update seiring perubahan teknologi dan hukum yang melingkupinya.

Tip Pemberlakuan Forensik

Hasil forensik menjadi dapat diandalkan tergantung pada pedoman yang mengisi setiap langkah dan pelaksana. Berikut beberapa tip yang dapat dipandang sebagai pedoman dalam melakukan proses forensik:

- Konsistensi menjadi suatu keharusan dalam setiap proses forensik.
- Tahapan forensik yang mencakup pengumpulan (collection), pengujian (examination), analisa,

dan laporan-laporan mungkin tidak seluruhnya mendapatkan *effort* yang sama. Kebutuhan akan detail pun variatif untuk setiap tahapan.

- Analisa tentunya harus memperhatikan berbagai sumber data potensial, mencakup lapisan logika dan fisik (misalnya media penyimpanan secara fisik).
- Examiner harus memiliki kejelian dalam mengalokasi sebaran data-data yang mungkin, apakah hanya sebatas komputer desktop atau mencakup pula jaringan komputer yang bahkan merambah keluar organisasi.
- Examiner harus mempertimbangkan setiap alternatif yang *reliable* seandainya didapati faktor berupa “rintangan” untuk mendapatkan data.
- Dibutuhkan tindakan proaktif dalam mengumpulkan data-data yang berharga. Tindakan proaktif tentunya membutuhkan *effort* yang besar, antara lain seperti: Melakukan audit terhadap sistem operasi, menerapkan *logging*, performa sistem backup pada umumnya, dan *security monitoring control* yang suatu saat nanti dapat digunakan untuk keperluan forensik.

- 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 “pelanggaran hukum”.
- Pertimbangkan setiap tahapan, mulai dari mengidentifikasi sumber data, membuat perencanaan dalam mendapatkan data dan menganalisa integritas dari data. Faktor prioritas harus berperan dalam menentukan mana data yang perlu diberikan prioritas 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.
- Sebelum data mulai dikumpulkan, keputusan harus dibuat 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. Pedefinisian yang jelas berkenaan *chain of custody* tentunya ditujukan untuk menghindari *mishandling evidence*.
- Examiner harus menggunakan pendekatan ilmiah dalam mempelajari data. Pendekatan demikian harus mengisi proses analisa kelayakan data dan keabsahannya, darinya Examiner dapat membuat kesimpulan berdasarkan ketersediaan data, atau mungkin saja tidak ada hasil sama sekali.
- Jika evidence mungkin dibutuhkan untuk keperluan hukum atau persidangan atau keperluan yang sifatnya internal disipliner, tentunya detail dan langkah-langkah mendapatkan dan dokumentasi harus sangat diperhatikan.
- 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 *policy shortcomings*
 - ✓ Mengalami procedural error
 - ✓ Masalah minor lain-lain yang mungkin harus diperbaiki
 - ✓ Mempertimbangkan kembali seberapa organisasi mengikuti arus dari teknologi dan perubahan dalam segi hukum

Lebih lanjut dapat Anda perhatikan beberapa tip umum dalam menangani dan menganalisa evidence secara umum untuk menjaga keutuhan/integritas serta kelayakan data. Berikut tip-tipnya:

- Jangan terlebih dahulu menyalakan komputer untuk alasan apapun.
- 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 dan bukannya umum.

- Lupakan kata tepat waktu dalam komputer forensik, ini karena Anda menelusuri hutan data sewaktu mengekplorasi.
- Konsistenlah terhadap kasus dan identifikasi kepentingan, misalnya saja jika menyangkut transaksi obat terlarang dan narkoba, tentu Anda tidak menanyakan informasi untuk keperluan pengujian dalam kasus pornografi anak.
- Jika ada beberapa orang yang mungkin menggunakan komputer atau dialokasikan di ruang komputer, indikasi terhadapnya perlu dilakukan. Ini mencakup siapa, atau atribut lain yang berkaitan dengan komputer, seperti password.
- Mengindikasikan apakah komputer diintegrasikan dalam 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.
- Mengindikasikan apakah terdapat *encryption* atau *password protection*.
- Mengindikasi skill komputer user yang komputernya diambil untuk keperluan forensik.
- Tidak selamanya monitor dan peripheral ataupun perangkat lain harus disertakan, umumnya komputer dan media penyimpanan sudah cukup guna keperluan forensik.

Tip Bagi Pemula yang Sadar Forensik

Bagi user atau pemula yang mungkin baru dengan istilah forensik dan ternyata mendapati adanya kasus-kasus yang membutuhkan penanganan forensik. Beberapa yang layak diperhatikan:

- Investigasi sederhana mungkin dapat Anda lakukan untuk mengalami evidence.
- Hubungi organisasi/pihak-pihak yang berwenang dalam mengambil keputusan.
- Amankan lokasi, akan lebih baik jangan ada yang berada di daerah atau meja kerja.

- Minimalisasi interupsi terhadap lokasi, misalnya biarkan komputer apa adanya. Jika komputer dalam keadaan menyala, maka biarkan menyala atau dalam keadaan mati, maka biarkan seperti itu. Penanganan lebih lanjut diserahkan oleh profesional investigator.
- Jangan menjalankan program apapun pada komputer yang dimaksud.
- Jangan membiarkan user lain mengutak-atik komputer, termasuk manajer Anda atau bahkan pemiliknya.
- Kumpulkan dan dokumentasikan sumber data lainnya, misalnya CD backup, tape backup, dan log-log file.
- Barang-barang non komputer yang memang dapat dijadikan evidence hendaknya diamankan, misalnya: notes, buku, dan berbagai peralatan kantor lainnya.
- Mulailah dokumentasi Chain of Custody, dengan mencatat setiap evidence dan milik evidence yang adalah milik seseorang atau perusahaan. Lengkapi datanya seperti di mana, kapan, dan siapa yang menemukan evidence, serta siapa yang melakukan pemeriksaan terhadap evidence, waktu dan jam hendaknya dicatat.

Metropolis Police Bureau High-tech Investigations Unit			
<i>This form is to be used for only one piece of evidence. Fill out a separate form for each piece of evidence.</i>			
Case No.:			
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 3.3 Sample Form - Metropolis Police Bureau

Pada Gambar 3.4 sampai dengan Gambar 3.9 dipercontohkan form-form yang berkaitan dengan proses forensik tahap awal, dispesifikasi berdasarkan perangkat, mungkin komputer secara umum (Gambar 3.4). Detail dijabarkan berkenaan karakteristik komputer dan media

penyimpanan dan konfigurasinya. Opsi-opsi sudah dibakukan sedemikian rupa untuk kemudahan.

Berikut pula untuk forensik terhadap Harddrive 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 <input type="checkbox"/> Laptop <input type="checkbox"/> Other: _____
Computer Condition:	Good <input type="checkbox"/> Damaged <input type="checkbox"/> (See Remarks)
Number of Hard Drives:	3.5" Floppy Drive <input type="checkbox"/> 5.25" Floppy Drive <input type="checkbox"/>
Modem <input type="checkbox"/>	Network Card <input type="checkbox"/> Tape Drive <input type="checkbox"/> Tape Drive Type: _____
100 MB Zip <input type="checkbox"/>	250 MB Zip <input type="checkbox"/> CD Reader <input type="checkbox"/> CD Read/Write <input type="checkbox"/>
DVD <input type="checkbox"/>	Other: _____
CMOS Information	
Not Available <input type="checkbox"/>	
Password Layout:	Yes <input type="checkbox"/> No <input type="checkbox"/> Password #: _____
Current Time:	AM <input type="checkbox"/> PM <input type="checkbox"/> Current Date: / /
CMOS Time:	AM <input type="checkbox"/> PM <input type="checkbox"/> CMOS Date: / /
CMOS Hard Drive #1 Settings	
Auto <input type="checkbox"/>	
Capacity:	Cylinders: _____ Heads: _____ Sectors: _____
Mode:	LBA <input type="checkbox"/> Normal <input type="checkbox"/> Auto <input type="checkbox"/> Legacy CHS <input type="checkbox"/>
CMOS Hard Drive #2 Settings	
Auto <input type="checkbox"/>	
Capacity:	Cylinders: _____ Heads: _____ Sectors: _____
Mode:	LBA <input type="checkbox"/> Normal <input type="checkbox"/> Auto <input type="checkbox"/> Legacy CHS <input type="checkbox"/>
Computer Evidence Worksheet	
Page 1 of 2	

Gambar 3.4 Sample Form – Computer Evidence Worksheet (Lembar 1)

Sub Exhibits Split From This Computer		
Sub Number	Type	Where Found
Remarks		
Computer Evidence Worksheet		
Page 2 of 2		

Gambar 3.5 Sample Form – Computer Evidence Worksheet (Lembar 2)

Hard Drive Evidence Worksheet

Case Number: _____	Exhibit Number: _____																																																														
Laboratory Number: _____	Control Number: _____																																																														
<input type="checkbox"/> Hard Drive 41 Label Information [Not Available <input type="checkbox"/>] <input type="checkbox"/> Hard Drive 42 Label Information [Not Available <input type="checkbox"/>]																																																															
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Manufacturer: _____ Model: _____ Part Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev: _____ IDE: <input type="checkbox"/> 30 Pin SCSI: <input type="checkbox"/> Other: <input type="checkbox"/> 68 Pin SCSI: <input type="checkbox"/> 50 Pin SCSI: <input type="checkbox"/> Auger: <input type="checkbox"/> Master: <input type="checkbox"/> Slave: <input type="checkbox"/> Cache Select: <input type="checkbox"/> Undetermined: <input type="checkbox"/></td> <td style="width: 50%;">Manufacturer: _____ Model: _____ Part Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev: _____ IDE: <input type="checkbox"/> 30 Pin SCSI: <input type="checkbox"/> Other: <input type="checkbox"/> 68 Pin SCSI: <input type="checkbox"/> 50 Pin SCSI: <input type="checkbox"/> Auger: <input type="checkbox"/> Master: <input type="checkbox"/> Slave: <input type="checkbox"/> Cache Select: <input type="checkbox"/> Undetermined: <input type="checkbox"/></td> </tr> </table>		Manufacturer: _____ Model: _____ Part Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev: _____ IDE: <input type="checkbox"/> 30 Pin SCSI: <input type="checkbox"/> Other: <input type="checkbox"/> 68 Pin SCSI: <input type="checkbox"/> 50 Pin SCSI: <input type="checkbox"/> Auger: <input type="checkbox"/> Master: <input type="checkbox"/> Slave: <input type="checkbox"/> Cache Select: <input type="checkbox"/> Undetermined: <input type="checkbox"/>	Manufacturer: _____ Model: _____ Part Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev: _____ IDE: <input type="checkbox"/> 30 Pin SCSI: <input type="checkbox"/> Other: <input type="checkbox"/> 68 Pin SCSI: <input type="checkbox"/> 50 Pin SCSI: <input type="checkbox"/> Auger: <input type="checkbox"/> Master: <input type="checkbox"/> Slave: <input type="checkbox"/> Cache Select: <input type="checkbox"/> Undetermined: <input type="checkbox"/>																																																												
Manufacturer: _____ Model: _____ Part Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev: _____ IDE: <input type="checkbox"/> 30 Pin SCSI: <input type="checkbox"/> Other: <input type="checkbox"/> 68 Pin SCSI: <input type="checkbox"/> 50 Pin SCSI: <input type="checkbox"/> Auger: <input type="checkbox"/> Master: <input type="checkbox"/> Slave: <input type="checkbox"/> Cache Select: <input type="checkbox"/> Undetermined: <input type="checkbox"/>	Manufacturer: _____ Model: _____ Part Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev: _____ IDE: <input type="checkbox"/> 30 Pin SCSI: <input type="checkbox"/> Other: <input type="checkbox"/> 68 Pin SCSI: <input type="checkbox"/> 50 Pin SCSI: <input type="checkbox"/> Auger: <input type="checkbox"/> Master: <input type="checkbox"/> Slave: <input type="checkbox"/> Cache Select: <input type="checkbox"/> Undetermined: <input type="checkbox"/>																																																														
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="6" style="text-align: center;">Hard Drive 41 Parameter Information</td> </tr> <tr> <td>DOS: <input type="checkbox"/> Plate: <input type="checkbox"/> Parallel: <input type="checkbox"/> Linux/FD: <input type="checkbox"/> SafeDisk: <input type="checkbox"/> Enclose: <input type="checkbox"/> Other: <input type="checkbox"/></td> </tr> <tr> <td colspan="6" style="text-align: center;">Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____</td> </tr> <tr> <td colspan="6" style="text-align: center;">LBA Addressable Sectors: _____ Formatted Drive Capacity: _____</td> </tr> <tr> <td colspan="6" style="text-align: center;">Volume Label: _____</td> </tr> <tr> <td colspan="6" style="text-align: center;">Partitions:</td> </tr> <tr> <td colspan="6" style="text-align: center;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th>Name</th> <th>Bootable</th> <th>Start</th> <th>End</th> <th>Type</th> </tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table> </td> </tr> </table>		Hard Drive 41 Parameter Information						DOS: <input type="checkbox"/> Plate: <input type="checkbox"/> Parallel: <input type="checkbox"/> Linux/FD: <input type="checkbox"/> SafeDisk: <input type="checkbox"/> Enclose: <input type="checkbox"/> Other: <input type="checkbox"/>	Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____						LBA Addressable Sectors: _____ Formatted Drive Capacity: _____						Volume Label: _____						Partitions:						<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th>Name</th> <th>Bootable</th> <th>Start</th> <th>End</th> <th>Type</th> </tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table>						Name	Bootable	Start	End	Type																				
Hard Drive 41 Parameter Information																																																															
DOS: <input type="checkbox"/> Plate: <input type="checkbox"/> Parallel: <input type="checkbox"/> Linux/FD: <input type="checkbox"/> SafeDisk: <input type="checkbox"/> Enclose: <input type="checkbox"/> Other: <input type="checkbox"/>																																																															
Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____																																																															
LBA Addressable Sectors: _____ Formatted Drive Capacity: _____																																																															
Volume Label: _____																																																															
Partitions:																																																															
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th>Name</th> <th>Bootable</th> <th>Start</th> <th>End</th> <th>Type</th> </tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table>						Name	Bootable	Start	End	Type																																																					
Name	Bootable	Start	End	Type																																																											
Hard Drive Evidence Worksheet																																																															
Page 1 of 2																																																															

Gambar 3.6 Sample Form – Harddrive Evidence Worksheet (Lembar 1)

Initial Analysis Information																																								
Archiving Method: Direct to Tape <input type="checkbox"/> NTBackup <input type="checkbox"/> Tar <input type="checkbox"/> Other: _____ Compressed: <input type="checkbox"/> (Each aggregate workload for backup method and: Tape Type: DAT: <input type="checkbox"/> 1/2": <input type="checkbox"/> 1/4": <input type="checkbox"/> Other: <input type="checkbox"/> Number Tapes: _____)																																								
Media Recovery Requested																																								
Copying System Used: DOS: <input type="checkbox"/> Windows: <input type="checkbox"/> Mac: <input type="checkbox"/> Unix: <input type="checkbox"/> Other: _____ Version: _____ Archive Software Used: Toolkit: <input type="checkbox"/> Lazarus: <input type="checkbox"/> DOS/Windows: <input type="checkbox"/> Self-Extracting: <input type="checkbox"/> Other: _____ Version: _____																																								
Recovered Work Copy/Tape Validated: Yes: <input type="checkbox"/> No: <input type="checkbox"/>																																								
List of software and other than law																																								
Form																																								
Audit Matrix																																								
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Milestone</th> <th>Bonus</th> <th>Initials</th> </tr> </thead> <tbody> <tr><td>Review VNC Scan</td><td></td><td></td></tr> <tr><td>Print Review VNC Scan</td><td></td><td></td></tr> <tr><td>Archive Unallocated/Temporary Files</td><td></td><td></td></tr> <tr><td>Print Log Session</td><td></td><td></td></tr> <tr><td>Export Data Scan</td><td></td><td></td></tr> <tr><td>Print Log Report</td><td></td><td></td></tr> <tr><td>Review & Log File Protection</td><td></td><td></td></tr> <tr><td>Log File Log</td><td></td><td></td></tr> <tr><td>Unarchive Deleted Files</td><td></td><td></td></tr> <tr><td>Extract Programs or Scripts</td><td></td><td></td></tr> <tr><td>Extract Recovery Mail/Out</td><td></td><td></td></tr> <tr><td>Cook Passwords</td><td></td><td></td></tr> </tbody> </table>		Milestone	Bonus	Initials	Review VNC Scan			Print Review VNC Scan			Archive Unallocated/Temporary Files			Print Log Session			Export Data Scan			Print Log Report			Review & Log File Protection			Log File Log			Unarchive Deleted Files			Extract Programs or Scripts			Extract Recovery Mail/Out			Cook Passwords		
Milestone	Bonus	Initials																																						
Review VNC Scan																																								
Print Review VNC Scan																																								
Archive Unallocated/Temporary Files																																								
Print Log Session																																								
Export Data Scan																																								
Print Log Report																																								
Review & Log File Protection																																								
Log File Log																																								
Unarchive Deleted Files																																								
Extract Programs or Scripts																																								
Extract Recovery Mail/Out																																								
Cook Passwords																																								
Hard Drive Evidence Worksheet																																								
Page 2 of 2																																								

Gambar 3.7 Sample Form – Harddrive 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

Form dengan opsi
spesifikasi storage

Exhibit # Sub-Exhibit #	Triage	Duplicated				Keyword Search
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					
	<input type="checkbox"/>					

Examiner _____

Date _____

Supervisor Review _____

Date _____

Digital Evidence Removable Media Worksheet

Page 1 of 2

Gambar 3.8 Sample Form – Removable Media Evidence Worksheet (Lembar 1)

dapat Anda bandingkan dengan Sample Form Miami Valley RCL atau Miami Valley RCFL, dimana

spesifikasi, rincian dan kepentingan menjadi pembedanya.

Department of Maryland State Police
Computer Forensic Laboratory

TELEPHONE 410-200-1620 FAX 410-200-1831
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 Search (Circle):	Search Warrant:	Consent:	Administrative:	Federal Grand Jury: Other:
Number of Computers: (CDU Computer Reference Seizure) <input type="checkbox"/> (Attach a copy)				
Has this evidence been previously viewed, accessed, and/or examined by anyone?				
Are you aware of any privileged information contained within the evidence being submitted? (Explain) <input type="checkbox"/> Yes <input type="checkbox"/> No				
<input type="checkbox"/> Urgent Request for Examination				
Data Requested:	Person Making Request - Name / Title:	Telephone # where you can be reached:	Data 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				
<input type="checkbox"/> Please prepare one form for each search site (address). <input type="checkbox"/> Please provide ALL requested information and note any unusual circumstance in the "Service Requested" area. <input type="checkbox"/> 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. <input type="checkbox"/> Please attach a Detained 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 3.10 Sampel Form – Permintaan Layanan Forensik

Secara umum forensik mencakup banyak bidang dan kasus, dan form global yang deskriptif digambarkan pada Gambar 3.11. Kebutuhan ana-

lis difokuskan, seperti dipaparkan dalam form (Fingerprint, Chemistry, Computer Forensic, dan lain sebagainya) spesifikasi dibuat kemudian.

MIAMI VALLEY REGIONAL CRIME LABORTORY
361 W. Third St., Dayton OH 45402 937-225-4980 FAX 937-495-7916

<input checked="" type="checkbox"/> New Case <input type="checkbox"/> 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																																		
<table border="0" style="width: 100%;"> <tr> <td style="width: 33%;">Fingerprints</td> <td style="width: 33%;">Chemistry</td> <td style="width: 33%;">Computer Forensics</td> </tr> <tr> <td>LP01 Search for Latent Prints</td> <td>C01 Drug analysis</td> <td>CF01 Image/Exam*</td> </tr> <tr> <td>LP02 Latent Print Evaluation return at lab</td> <td>C02 Blood Alcohol Anal.</td> <td></td> </tr> <tr> <td>LP03 Latent Print Evaluation return to department</td> <td>C03 Urine Alcohol Anal.</td> <td></td> </tr> <tr> <td>LP04 FP Comparison</td> <td>C04 Drug Screen on Urine</td> <td></td> </tr> <tr> <td>LP05 AFIS Inquiry-print Marked?</td> <td>C05 Alcoholic Beverage</td> <td></td> </tr> <tr> <td>LP06 AFIS Inquiry-enter best print?</td> <td>C07 Arson Analysis</td> <td></td> </tr> <tr> <td>LP07 Other Request**</td> <td>C08 Gunshot Residue</td> <td></td> </tr> <tr> <td></td> <td>C09 Other Request**</td> <td></td> </tr> <tr> <td></td> <td>Crime Scene ()</td> <td></td> </tr> <tr> <td></td> <td>Photographs ()</td> <td></td> </tr> </table>		Fingerprints	Chemistry	Computer Forensics	LP01 Search for Latent Prints	C01 Drug analysis	CF01 Image/Exam*	LP02 Latent Print Evaluation return at lab	C02 Blood Alcohol Anal.		LP03 Latent Print Evaluation return to department	C03 Urine Alcohol Anal.		LP04 FP Comparison	C04 Drug Screen on Urine		LP05 AFIS Inquiry-print Marked?	C05 Alcoholic Beverage		LP06 AFIS Inquiry-enter best print?	C07 Arson Analysis		LP07 Other Request**	C08 Gunshot Residue			C09 Other Request**			Crime Scene ()			Photographs ()	
Fingerprints	Chemistry	Computer Forensics																																
LP01 Search for Latent Prints	C01 Drug analysis	CF01 Image/Exam*																																
LP02 Latent Print Evaluation return at lab	C02 Blood Alcohol Anal.																																	
LP03 Latent Print Evaluation return to department	C03 Urine Alcohol Anal.																																	
LP04 FP Comparison	C04 Drug Screen on Urine																																	
LP05 AFIS Inquiry-print Marked?	C05 Alcoholic Beverage																																	
LP06 AFIS Inquiry-enter best print?	C07 Arson Analysis																																	
LP07 Other Request**	C08 Gunshot Residue																																	
	C09 Other Request**																																	
	Crime Scene ()																																	
	Photographs ()																																	
<table border="0" style="width: 100%;"> <tr> <td style="width: 33%;">Serology</td> <td style="width: 33%;">Trace Evidence</td> <td style="width: 33%;">Firearms/Toolmarks</td> </tr> <tr> <td>S01 Blood Identification</td> <td>T01 Hair and Fiber Exam</td> <td>F01 Firearms Identification</td> </tr> <tr> <td>S02 Semen Identification</td> <td>T02 Paint Comparison</td> <td>F02 Gunpowder Pattern</td> </tr> <tr> <td>S03 Other Request*</td> <td>T03 Glass Comparison</td> <td>F03 Toolmark Comparison</td> </tr> <tr> <td></td> <td>T04 Footwear Comparison</td> <td>F04 Serial Number Restoration</td> </tr> <tr> <td></td> <td>T05 Soil Comparison</td> <td>F05 Bullet/Cartridge Case Comparison</td> </tr> <tr> <td></td> <td>T06 Other Request**</td> <td>F06 Other Request**</td> </tr> </table>		Serology	Trace Evidence	Firearms/Toolmarks	S01 Blood Identification	T01 Hair and Fiber Exam	F01 Firearms Identification	S02 Semen Identification	T02 Paint Comparison	F02 Gunpowder Pattern	S03 Other Request*	T03 Glass Comparison	F03 Toolmark Comparison		T04 Footwear Comparison	F04 Serial Number Restoration		T05 Soil Comparison	F05 Bullet/Cartridge Case Comparison		T06 Other Request**	F06 Other Request**												
Serology	Trace Evidence	Firearms/Toolmarks																																
S01 Blood Identification	T01 Hair and Fiber Exam	F01 Firearms Identification																																
S02 Semen Identification	T02 Paint Comparison	F02 Gunpowder Pattern																																
S03 Other Request*	T03 Glass Comparison	F03 Toolmark Comparison																																
	T04 Footwear Comparison	F04 Serial Number Restoration																																
	T05 Soil Comparison	F05 Bullet/Cartridge Case Comparison																																
	T06 Other Request**	F06 Other Request**																																
Questioned Documents QD01 Document Exam QD02 Other QD Request** <small>*attach computer exam request form **describe in synopsis</small>																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">List of Evidence</th> <th style="text-align: left; padding: 2px;">Property Tag #</th> <th style="text-align: left; padding: 2px;">Analysis Code</th> <th style="text-align: left; padding: 2px;">Disposition</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table>		List of Evidence	Property Tag #	Analysis Code	Disposition																													
List of Evidence	Property Tag #	Analysis Code	Disposition																															

Synopsis of Case:

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

NATIONALLY ACCREDITED BY THE AMERICAN SOCIETY OF CRIME LABORATORY DIRECTORS

Gambar 3.11 Sample Form - Miami Valley Regional Crime Lab

Pada Gambar 3.12 dapat Anda perhatikan form layanan Miami Valley Regional Computer Forensic Laboratory, form ini dapat Anda download di website yang bersangkutan.

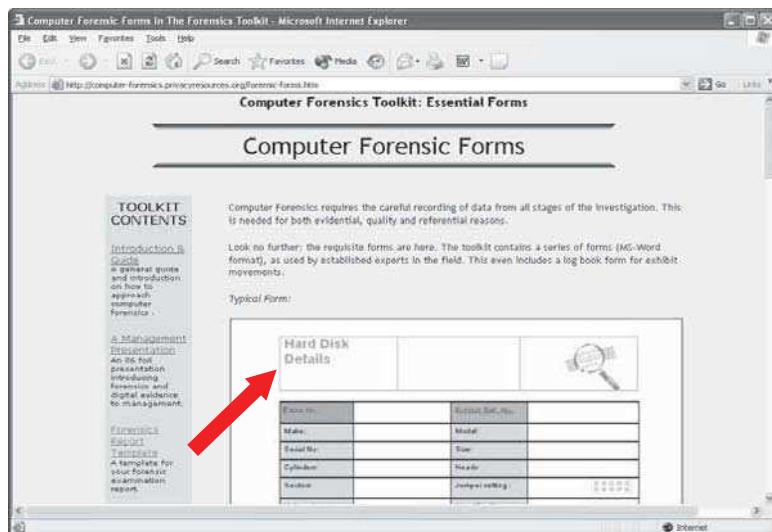
Form tersebut digunakan hanya pada lingkungan terbatas, dan kemudian diteruskan untuk proses forensik lebih lanjut.

The screenshot displays two Microsoft Word windows side-by-side. Both windows show a 'REQUEST FOR SERVICE' form from the 'MIAMI VALLEY REGIONAL COMPUTER FORENSIC LABORATORY'. The left window contains the original form with fields like 'Case Information', 'Case Status', 'Case Type', 'Case Priority', 'Case Established By', 'Case Received By', and 'Case Assigned To'. Many of these fields contain placeholder text such as 'Case ID: [REDACTED]', 'Case Status: [REDACTED]', 'Case Type: [REDACTED]', etc. The right window shows the same form but with all sensitive information redacted, leaving only the header and footer visible.

Gambar 3.12 Sample Form Download – Miami Valley

Anda dapat merancang form spesifik sesuai kebutuhan Anda, atau organisasi/perusahaan Anda. Beberapa form tadi dapat digunakan sebagai pembanding (penulis menilai bahwa form tadi sangat sederhana dan mudah dimengerti, layak dijadikan model untuk kebutuhan forensik).

Lebih jauh lagi mungkin Anda dapat menggunakan toolkit komersial, seperti yang ditampilkan pada website (<http://computer-forensics.privacyresources.org>) pada Gambar 3.13 dan Gambar 13.4, di sana dipercontohkan toolkit yang mencakup pula form dan template yang sudah siap Anda gunakan.



Gambar 3.13 Website <http://computer-forensics.privacyresources.org> – Form



Gambar 3.14 Website <http://computer-forensics.privacyresources.org> – Report Template

BAB 4

Standarisasi Komputer Forensik

- Perlukah Standardisasi Komputer Forensik?
- Kebijakan dan Prosedur
- Analisa Evidence
- Akuisisi Evidence
- Pengujian Evidence
- Laporan dan Dokumentasi
- Kasus yang Mengandalkan Komputer Forensik

Perlukah Standarisasi Komputer Forensik?

Seberapa perlu standarisasi dalam komputer forensik? Apakah tidak cukup menggunakan komputer yang adalah universal?

Bukankah bahasa pemrograman adalah universal? Bukankah bahasa Inggris menjadi bahasa pengantar yang paling '*reliable*' untuk komputer dan penggunanya? Bukankah perangkat keras dan perangkat lunak sudah ada standarnya? Lalu, bukankah itu sudah cukup dalam memenuhi kebutuhan dan implementasinya kemudian?

Setiap organisasi mungkin memiliki prosedur, metode, aturan, dan berbagai proses yang berbeda satu dengan yang lain. Masalah inkompatibilitas tidak akan pernah tenggelam seiring dengan perkembangan dan penggunaan komputer.

Buktinya? Inkompatibilitas dalam menangani data yang di-create oleh aplikasi yang sama tetapi beda versi, terlebih lagi aplikasi yang sejenis tetapi berbeda developer kerap kali memunculkan banyak masalah inkompatibilitas.

Lalu di level yang lebih dekat ke perangkat keras misalnya, berbagai printer dengan ragam versi PCL (Printer Control Language) kadang

menimbulkan masalah yang sering berikut di perbedaan yang tidak mungkin dijembatani.

Kebutuhan standar di level manapun sudah menjadi kebutuhan karena pengoperasian dan aktivitas yang berlangsung; di level perangkat keras, perangkat lunak, bahkan di level organisasi. Ternyata standarisasi bukan hanya milik teknologi, ini dikarenakan ada banyak metode dan proses yang mencakup cara-cara manual/tradisional.

Anda mungkin pernah mendengar istilah Electronic Data Interchange (EDI) yang diterapkan sebagai interface komunikasi data (mencakup pula transaksi, transfer data) antar dua sistem yang mungkin sama atau berbeda sama sekali.

Kemudahan inilah yang menjadi kekuatan, dan masalah inkompatibilitas dapat dieliminir sehingga bahkan dua organisasi dengan sistem yang berbeda dapat menggunakan data satu dengan yang lainnya. Bahkan penerapan ini menjadi strategi bisnis yang andal dalam mengikat konsumen. Tentunya EDI sangat mengandalkan standarisasi dengan format data yang tentunya 'standar'.

Standar dalam komputer forensik pada umumnya harus memenuhi kebutuhan akan pertukaran yang mencakup antar organisasi, antar perusahaan, perorangan dengan organisasi, atau bahkan lebih luas

antar negara yang melibatkan pula kebijakan setiap negara terhadap digital evidence.

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

- Pendefinisian
- Prinsip
- Proses dan metode
- Hasil
- Bahasa

Dari beberapa komponen tersebut tentunya harus dapat menjawab masalah inkompatibilitas semisal: Apakah layak untuk mengambil dan kemudian mendapatkannya lalu menganalisa suatu evidence? Bagaimana dengan proses mendapatkan dan mengorek keterangan, layakkah dalam sisi hukum, etika, dan teknologi informasi/komputer?

Dalam komputer forensik diberlakukan standar yang umumnya mengacu pada lima faktor yang dipertimbangkan, antara lain:

- Identifikasi Subjek
- “Memperbaiki” Komputer
- Mengungkap Jalur Komunikasi
- Permintaan Investigasi
- Pengumpulan Digital Evidence Lainnya

Buku ini bukan menjadi standar yang ‘baku’ ataupun pedoman kaku dalam menerapkan komputer forensik, Anda ataupun organisasi dapat mengembangkan metode yang cocok dan relevan terhadap kebutuhan. Jadikan buku ini media inspirasi dalam memandang komputer forensik.

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

- Pada tahun 1993 konferensi internasional pertama berkenaan dengan Computer Evidence diselenggarakan.
- Disusul dengan dibentuknya IOCE (International Organization of Computer Evidence) pada tahun 1995.
- Lalu tahun 1997, G8 dan IOCE secara independen menentukan pengembangan standar computer evidence.
- Sedangkan pada tahun 1998 banyak organisasi lain yang tanggap dan kemudian berpartisipasi, seperti SWG-DE, ACPO, FCG, ENSFI, dan INTERPOL.
- Akhir tahun 1999, ACPO, IOCE, FCG, dan ENSFI membahas mengenai standar di Eropa.

Dengan kebutuhan yang dialami dengan cepat dan berkembangnya standar komputer forensik, tentunya ada kejelasan dan hasil-hasil positif

yang didapat, ini mencakup perilaku terhadap computer evidence, dilibatkannya computer evidence terhadap tindak kriminal dan proses hukum, dan masih banyak lagi hal-hal positif yang dicapai.

‘Kejelasan’ menjadi wujud nyata dari perkembangan akan komputer forensik. Prinsip yang dihasilkan dari konferensi dan organisasi seputar komputer forensik misalnya: mencakup menangani evidence serta berbagai pengertian dalam komputer forensik.

Pada Bab 3 Anda mendapat gambaran secara umum tahapan yang dilakukan pada komputer forensik.

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

Lebih jauh berkenaan standar, Anda dapat mengeksporasi secara detail organisasi yang menyertakan komputer forensik, seperti dipercontohkan dalam paragraf sebelumnya.

Dan tanpa mengabaikan standar, dan bahkan merangkul standar, bab ini akan membahas kembali langkah-langkah yang ada pada komputer forensik, tetapi dengan pertimbangan faktor seperti kebijakan, etika, dan

kelayakan. Mudah-mudahan hal ini dapat memunculkan konsep yang nantinya akan Anda buat dan kembangkan.

SWG-DE

Organisasi ini dibentuk pada bulan Februari 1998 oleh The Federal Crime Laboratory Directors Group dan fokus kerjanya adalah pada forensik digital evidence.

SWG-DE ini dibentuk dan berada dalam naungan yang sama dengan organisasi lain yang melibatkan forensik yang sejenis, seperti: Scientific Working Groups on DNA (SWGDAM), Questioned Documents (SWGDOC), Trace Evidence (SWGMAT), Drugs (SWGDRUG), Fire and Explosives (SWGTEX), Fingerprints (SWGFAST), dan Imaging (SWGIT).

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

State and Local

- 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

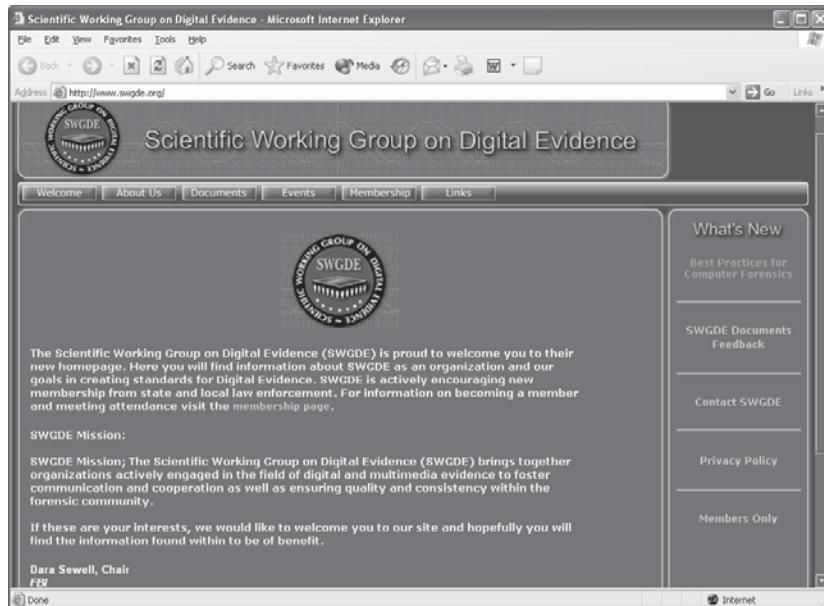
Internasional

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

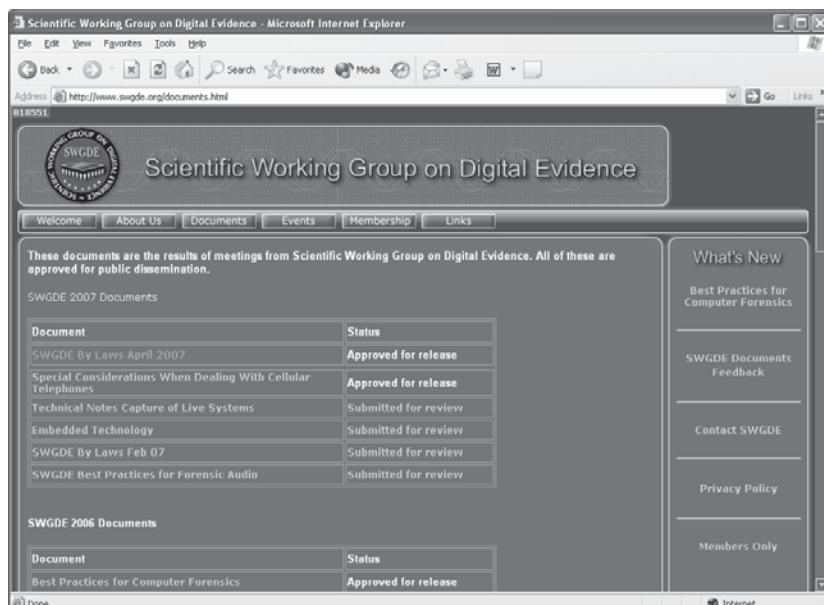
Associate Members

- 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 yang sudah dicapai oleh SWG-DE, Anda dapat mengakses websitenya. Perhatikan Gambar 4.1. Anda juga dapat men-download dokumen dalam format pdf (Gambar 4.2).



Gambar 4.1 Website Scientific Working Group on Digital Evidence



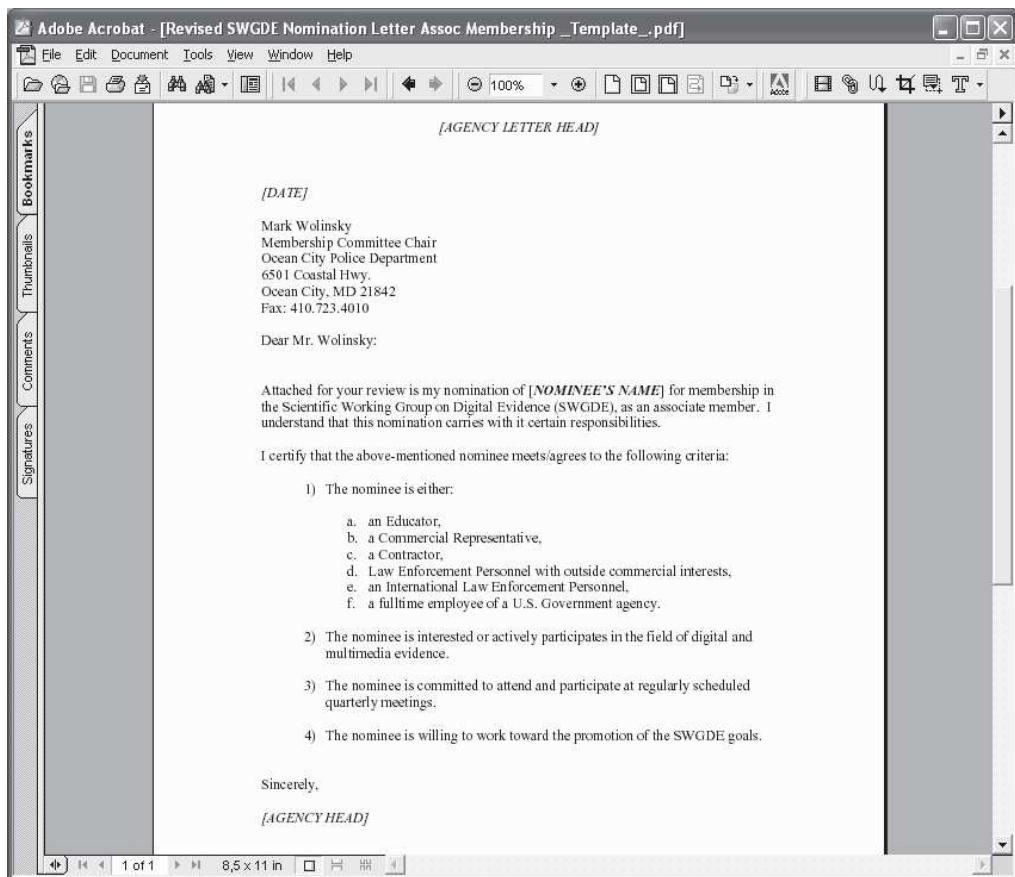
Gambar 4.2 Download Dokumen

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

Perhatikan Gambar 4.3 dan Gambar 4.4, salah satu percontohan formulir dan template yang wajib diisikan untuk pengajuan keanggotaan.

The screenshot shows a PDF document titled "Membership Application" from the "Scientific Working Group on Digital Evidence". The document includes a logo at the top, followed by the title "Membership Application". It contains several fields for personal information, such as "Full name:", "Title:", "Agency/Organization:", "Business Address:", "Business City/State:", "Zip Code + 4:", "Business Phone No. w/ Area Code:", "FAX No. w/ Area Code:", and "Work E-mail Address:". There are also sections for "Sworn Personnel" and "Membership Requested (circle one)". At the bottom, it says "SWGDE Membership Application (Revised 01/18/2006)" and "Page 1 of 3". The left sidebar of the Acrobat interface shows bookmarks like "Bookmarks", "Signatures", "Comments", "Thumbnails", and "File".

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



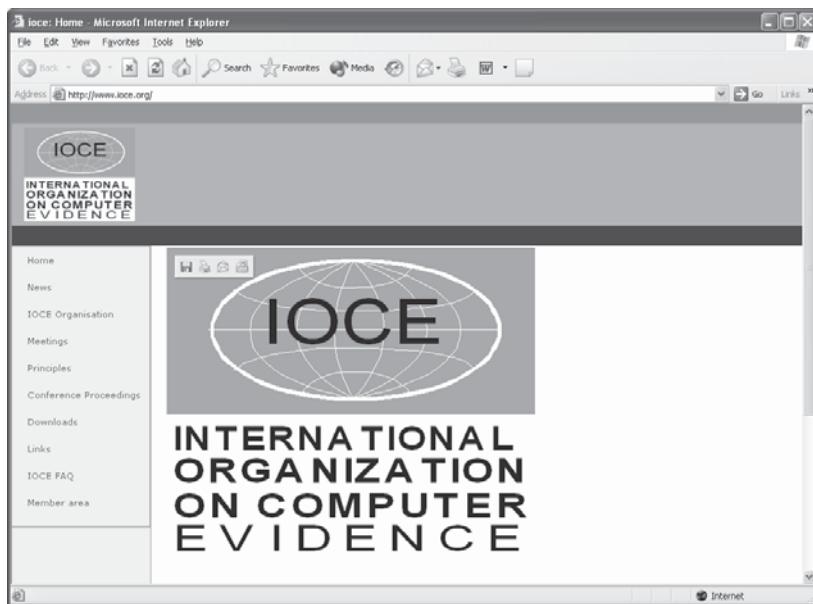
Gambar 4.4 Website Scientific Working Group on Digital Evidence – Revised Template

IOCE

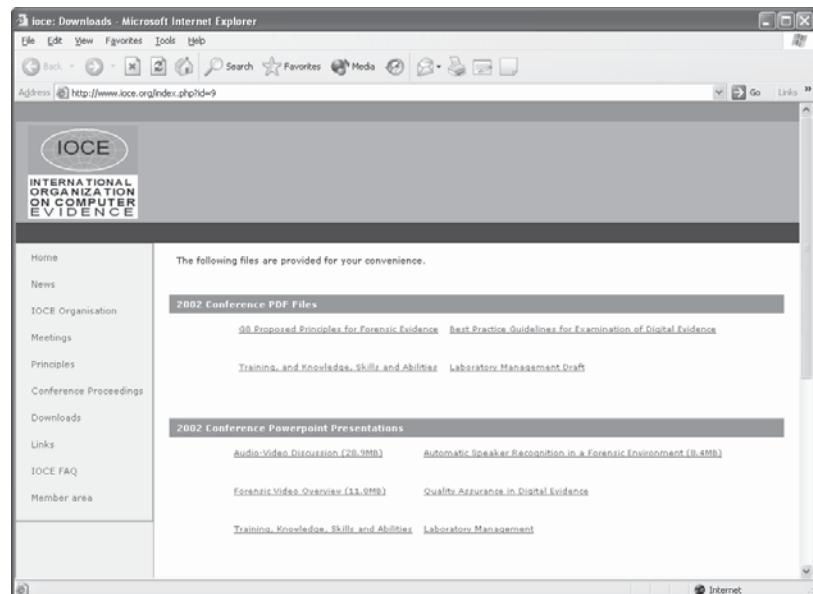
The International Organization on Computer Evidence (IOCE) didirikan pada tahun 1995 sebagai media atau sarana pertukaran informasi bagi para penegak hukum skala internasional mengenai investigasi

kejahatan komputer dan masalah-masalah forensik yang terkait.

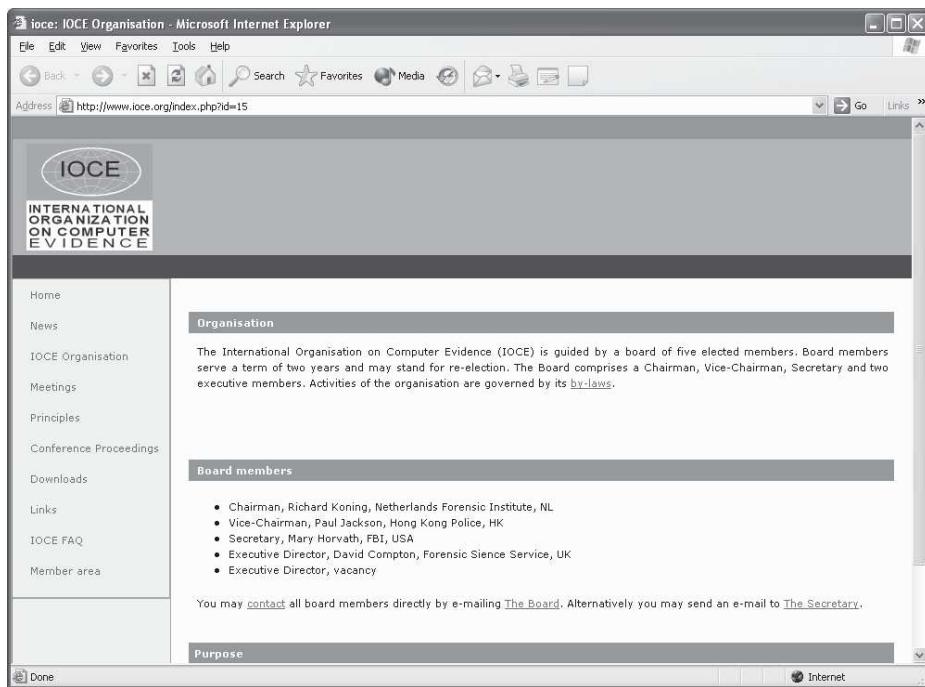
Website yang dimaksud tertera pada Gambar 4.5. Untuk mendapatkan informasi lebih dalam berkenaan organisasi ini Anda dapat mengaksesnya. Beberapa dokumen yang informatif dapat Anda temukan di sana.



Gambar 4.5 Website International Organization on Computer Evidence (IOCE)



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



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

Beberapa prinsip IOCE:

- Konsisten terhadap sistem perundangan
- Menggunakan bahasa umum
- Berdaya tahan (tangguh)
- Berkemampuan untuk melewati batas-batas internasional
- Mampu menanamkan ‘keyakinan’ terhadap integritas evidence
- Dapat diaplikasikan pada setiap *forensic evidence*

- Aplikatif untuk setiap tingkatan; mencakup individual, organisasi, dan bahkan negara

IACIS

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

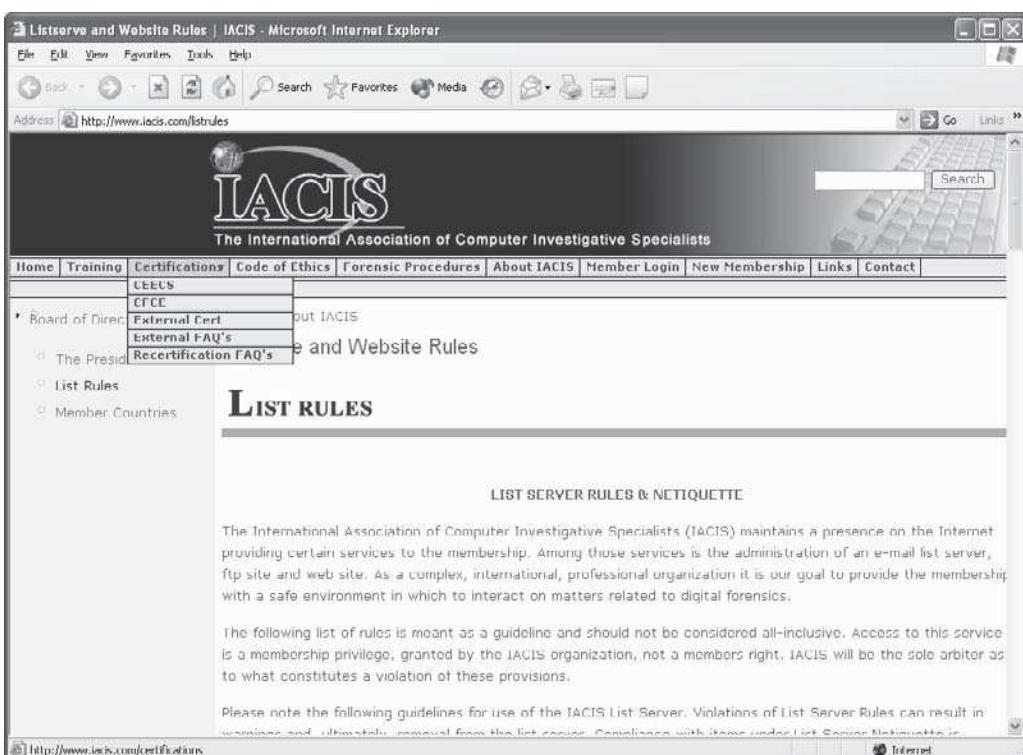
Keanggotaan IACIS melibatkan pula Federal, State, Local, dan penegak hukum profesional berskala internasional.

Anggota-anggota IACIS tentunya mendapatkan pelatihan ilmu forensik berkenaan penggunaan dan pemrosesan sistem komputer.

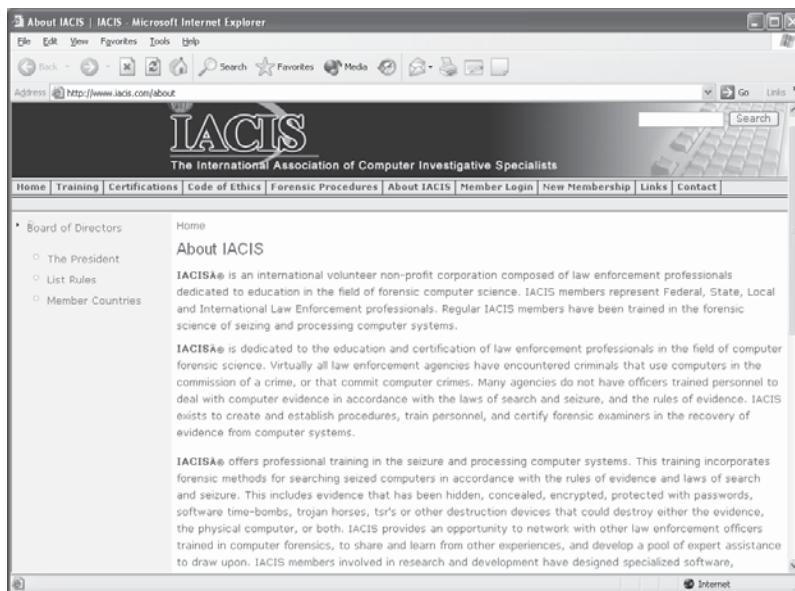
Organisasi ini menawarkan keanggotaan dengan berbagai keuntungan: akses informasi dapat dilakukan melalui newsletters, file libraries, dan juga list servers, sehingga para anggotanya dapat berkomunikasi dan

bertukar pengalaman dan kemampuan yang mencakup digital forensics, kemutakhiran teknologi, dan berbagai masalah kejahatan komputer.

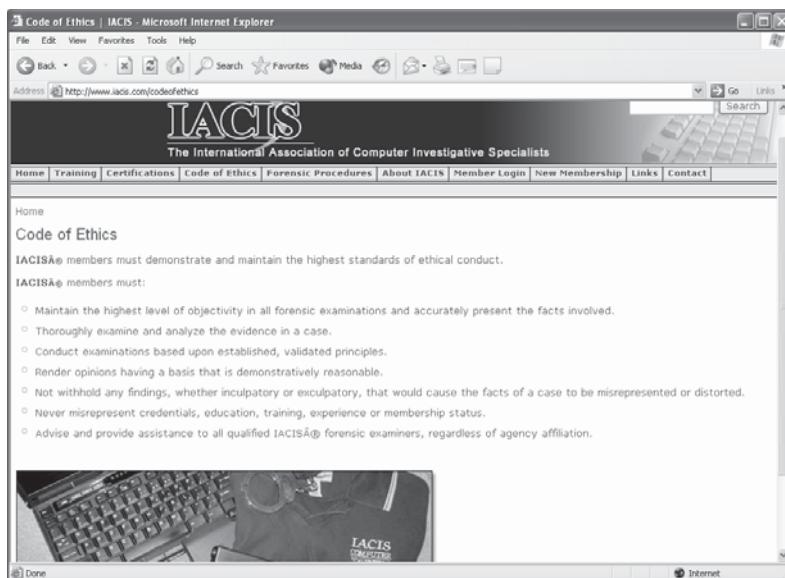
Beberapa informasi seputar IACIS ditampilkan pada beberapa gambar berikut. Perhatikan pula kode etik pada Gambar 4.10. Program sertifikasi diadakan pula oleh organisasi ini, seperti Certified Forensic Computer Examiner (CFCE) dan the Certified Electronic Evidence Collection Specialist (CEECS).



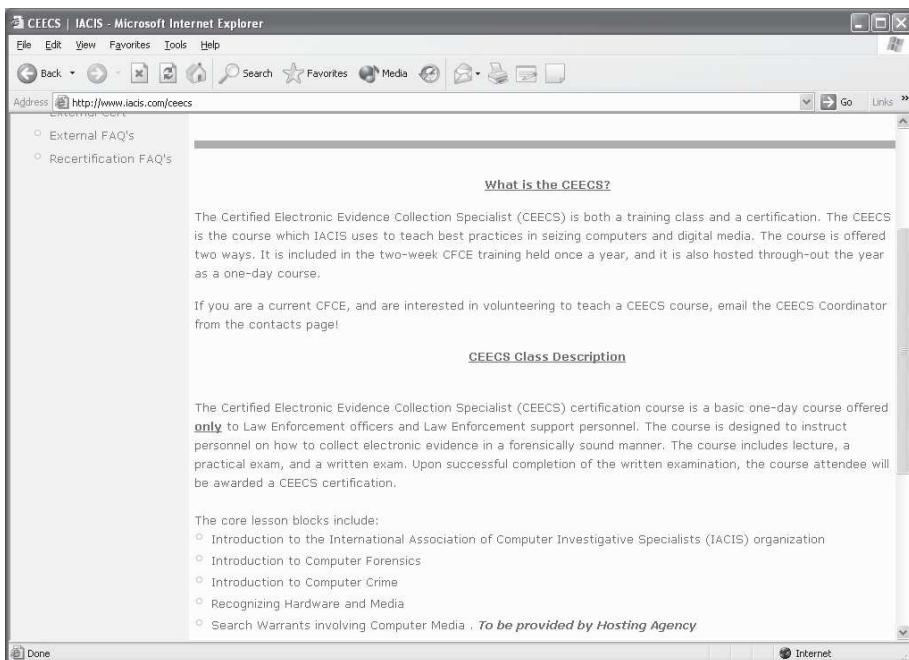
Gambar 4.8 Website The International Association of Computer Investigative Specialist (IACIS)



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 selentur mungkin dengan kebutuhan dan karakteristik organisasi atau perusahaan Anda.

Apapun bentuk standarisasi yang diberlakukan, semuanya pasti melibatkan tiga komponen utama yang berkolaborasi untuk pencapaian satu tujuan, seperti yang digariskan pada bab-bab terdahulu. Yang dimaksudkan adalah tool/perangkat, manusia, dan aturan/protokol.

Kolaborasi ketiganya harus mengisi setiap proses dan metode komputer forensik. Untuk lebih jelasnya perhatikan tahapan komputer forensik, Anda dapat merasakan ‘atmosfir’ yang melingkupinya.

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 dengan kualitas.

Tentu kesemuanya ini dimampukan dengan adanya pelatihan yang komprehensif, menekankan pada teknik dan kualitas, serta efisiensi dan efektivitas yang harus mewarnai organisasi/tim.

Misi dari organisasi tentunya berada dalam batasan protokol dan prosedur. Ada 7 hal yang perlu dipertimbangkan untuk protokol dan prosedur:

1. **Personel.** Beberapa yang perlu dipertimbangkan akan keberadaan personel ini mencakup: deskripsi pekerjaan, kualifikasi minimum, waktu beroperasi, status on-call duty, struktur tim, dan susunannya.

2. **Pertimbangan Administratif:**

- ✓ Software: harus mendapatkan lisensi yang sepatutnya.
- ✓ Ketersediaan sumber daya: yang dimaksud adalah biaya. Fasilitas gedung peralatan yang digunakan Examiner, kebutuhan perangkat keras dan lunak, termasuk pula keperluan upgrade, training,

dan skill update termasuk di dalam pembiayaan.

✓ Pelatihan: ditujukan untuk menambah pengetahuan dan skill. Training sangat penting direncanakan dan dijadwalkan kemudian. Dana khusus hendaknya dialokasikan untuk kebutuhan ini.

3. **Permintaan Layanan.** Pedoman tentunya dibentuk untuk mengalami permintaan layanan dan berbagai form input. Pertimbangkan pula kebijakan lainnya.

4. **Manajerial Kasus.** Ini merupakan tindak lanjut dari permintaan akan layanan yang diterima untuk proses lebih lanjut. Di sini perlu ditentukan tingkat prioritas dan bentuk penmeriksaan seperti apa yang dilakukan. Membuat prioritas tentunya dengan mempertimbangkan faktor seperti:

- ✓ Tindak kriminal
- ✓ Tanggal persidangan
- ✓ Batas waktu
- ✓ Pertimbangan hukum
- ✓ Ketersediaan sumber daya
- ✓ Korban potensial
- ✓ Volatile/non-volatile evidence

5. **Penanganan dan Pemberlakuan Evidence.** Untuk membuat pengaturan demikian, tentunya pedoman dibuat. Pedoman yang dibuat

nantinya mencakup penerimaan, pemrosesan, dokumentasi, penanganan evidence, dan produk-produk yang digunakan untuk kebutuhan pemeriksaan. Kriteria penanganan digital evidence mungkin meluas, misalnya jika evidence diidentifikasi sebagai barang selundupan, tentunya ada penanganan tersendiri.

6. **Pemrosesan Kasus.** Tahap ini melibatkan SOP (Standard Operating Procedures). SOP tentunya harus mampu mengalami kebutuhan dasar tahapan pemeriksaan rutin forensik.
7. **Mengembangkan Prosedur Teknikal.** Prosedur tentunya menjadi penuntun dalam memeriksa evidence. Untuk itu prosedur yang dibuat/dikembangkan tentunya harus melalui uji kelayakan sebelum nantinya digunakan. Langkah-langkah pengembangan dan menilai kelayakan suatu prosedur adalah:
 - ✓ Identifikasi tugas dan masalah
 - ✓ Mengajukan solusi
 - ✓ Pengetesan setiap solusi pada sample (sample dari tumpukan evidence)
 - ✓ Evaluasi hasil pengetesan
 - ✓ Menyempurnakan prosedur

Dalam kasus ini tentunya bukan evidence asli yang digunakan untuk tahap ini, umumnya yang digunakan hanya berupa sample atau evidence ‘buatan’.

Menilai Evidence (Assessment)

Penilaian kelayakan terhadap digital evidence dilakukan dengan sepututnya atas kasus yang melingkapinya dan kemudian menentukan langkah selanjutnya.

Prosedur yang dilakukan tentunya aturan dalam menilai detail kasus, keberadaan hardware dan software, potensial evidence yang teralamati, serta kondisi dan faktor-faktor lain yang mempengaruhi pengakuisisian evidence yang dianalisa.

Beberapa faktor yang menjadi pertimbangan antara lain:

- Penilaian Kasus
- *Onsite Consideration*
- Analisa Lokasi Pemrosesan
- Pertimbangan Hukum
- Analisa Evidence
 - ✓ Lokasi ditemukan evidence
 - ✓ Stabilitas media yang dilakukan pemeriksaan

- ✓ Menentukan bagaimana evidence didokumentasikan nantinya (misalnya evidence berupa: fotografi, image, sketsa, catatan, dan lainnya)
- ✓ Mengevaluasi lokasi media penyimpanan (misalnya saja apakah ada *electromagnetic interference* yang akan mempengaruhi integritas data yang ada pada media)
- ✓ Memastikan kondisi dari evidence; proses pengiriman, bagaimana evidence disimpan, dan hal lainnya.
- ✓ Menganalisa kebutuhan akan cadangan listrik (misalnya: baterai lithium)

Akuisisi Evidence

Pada prinsipnya digital evidence sangatlah rapuh karena sifatnya yang mudah rusak (terkait dengan perangkat keras yang menyertainya), integritasnya sangatlah rentan terhadap perubahan (sangat mungkin untuk dimodifikasi), 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 menghilangkannya.

Dibutuhkan proteksi dan penanganan yang seksama akan otentitas digital evidence. Berikut beberapa langkah yang mungkin diambil:

- Amankan digital evidence sesuai pedoman yang sudah ditetapkan.
- Mendokumentasi konfigurasi hardware dan software sistem si pemeriksa (Examiner).
- Verifikasi operasi dari sistem komputer pemeriksa, mencakup hardware dan software-nya.
- Men-disassembling komputer untuk keperluan pemeriksaan akses fisik media penyimpanan (jauhkan dari listrik statis dan medan magnet yang akan merusak data di dalamnya).
- Mengidentifikasi media penyimpanan internal, eksternal, atau bahkan keduanya.
- Mendokumentasi media penyimpanan internal (misalnya: jumper setting, model, developer, kapasitas, kemampuan/kecepatan, interface, dan lainnya).
- Mendokumentasi konfigurasi hardware, misalnya: Network Interface Card, Sound Card, Graphic Card, MAC (Media Access Control), PCMCIA Card jika ada, dan lainnya.
- Mendiskoneksi media penyimpanan untuk mencegah terjadinya kerusakan, modifikasi data, dan

- lainnya (untuk harddisk, lepas-kan kabel power dan kabel IDE).
- 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).
 - Matikan power.
 - Pindahkan media penyimpanan yang ada dan instalasikan pada sistem milik Examiner. Lakukan konfigurasi agar media penyimpanan dikenali oleh sistem.
 - Tahapan sebelumnya tentunya tidak mutlak, ada faktor-faktor lain yang perlu dipertimbangkan mengenai kelayakan akuisisi media penyimpanan, misalnya saja jika dihadapkan dengan:
 - ✓ Ketersediaan perangkat.
 - ✓ Ketergantungan hardware tertentu. Bisa saja didapat drive yang terdahulu tidak dapat dibaca pada sistem yang lebih baru.
 - ✓ Sistem drive yang tidak mungkin dipindahkan, dan akan banyak kesulitan jika dipisahkan dengan sistem tempatnya diintegrasikan, misalnya pada laptop.
 - ✓ Network storage.
 - ✓ RAID (Redundant Array of Inexpensive Disk).
 - Pertimbangkan kebutuhan *write protection* untuk melindungi data evidence orisinal.
 - Mendapatkan evidence subjek pada storage device si Examiner menggunakan berbagai tool hardware dan software, misalnya:
 - ✓ Software Forensic Analysis
 - ✓ Hardware device spesifik
 - Menginvestigasi lebih lanjut karakteristik dari storage device (misalnya: tabel partisi dan karakteristik dan ruang-ruang pada storage device, dan lainnya).
 - Verifikasi hasil akuisisi dengan membandingkan hasil peng-copy-an, misalnya dengan membandingkan sektor-sektor dengan storage device yang didapat.

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 percontohan rillnya.

Laporan dan Dokumentasi

Laporan umumnya berisi catatan si Examiner. Ini adalah tanggung jawabnya 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:

- Membawa catatan yang mungkin sewaktu-waktu digunakan ketika berkonsultasi dengan investigator ataupun prosecutor.
- Copy dari dokumentasi chain of custody.
- Tanggal, waktu pencatatan, deskripsi, dan tindakan yang diambil.
- Topologi jaringan, nama para user, user agreement, password, dan hal lainnya.
- Dokumentasi perubahan yang dibuat pada sistem dan jaringan komputer atas pengaturan atau perintah dari penegak hukum atau Examiner.

- Dokumentasi sistem operasi dan software, mencakup pula versi, patch yang diinstal, dan lainnya.
- Dokumentasi informasi lain, seperti remote user access, remote storage, dan lainnya.

Laporan mungkin mencakup hal-hal seperti:

- Identitas dari organisasi yang melaporkan
- Informasi kasus atau submission number
- Identitas dari si submitter
- 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-laporan tentunya akan mencakup:

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

- ✓ File spesifik yang diminta, dan file-file lainnya seperti file yang dihapus yang terelasi dengan penemuan, dan lainnya
- ✓ 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
- ✓ Metadata, property, dan kepemilikan file
- ✓ Data program registrasi mengacu pada kepemilikan
- ✓ Analisa data
- ✓ Deskripsi dari program yang relevan pada subjek yang dianalisa
- ✓ Teknik-teknik yang melengkapi, semisal enkripsi, partisi hidden, atribut hidden, dan lainnya.
- Material pendukung, mencakup:
 - ✓ Catatan chain of custody
 - ✓ Copy digital dari evidence
 - ✓ Print-out dari evidence
- Perbendaharaan kata, digunakan untuk kemudahan pembacanya sewaktu dihadapkan dengan istilah-istilah spesifik keilmuan dan teknis

Kasus yang Mengandalkan Komputer Forensik

Pornografi dalam Sistem Komputer Perusahaan

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

Examiner kemudian melakukan pemeriksaan terhadap cache file, slack, dan free space harddisk untuk memastikan user terlibat dalam mengakses gambar-gambar tersebut. Berdasarkan temuan forensik, ternyata karyawan perusahaan meng-exploitasi akses internet dengan tidak bertanggung jawab.

Denial of Services

Institusi keuangan menderita kerugian, kehilangan layanan dari mainframe dalam jangka waktu lama.

Dari analisa forensik diketahui bahwa adanya PC salah satu karyawan yang melakukan tindakan ilegal terhadap sistem.

Berdasarkan temuan forensik, karyawan tersebut mengeksploitasi sistem yang rentan dan kemudian membatasi *network auditing* untuk mekakukan sabotase mainframe.

BAB 5

Kemampuan Investigasi

- Menilai Data
- Pemahaman dengan Skill
- Investigasi!

Menilai Data

Data File

Data dalam komputer dikemas dalam bentuk file, oleh karena itu disebut sebagai data file atau file saja.

Ada banyak sekali jenis dan ragam file, mencakup file dokumen, aplikasi, file yang diciptakan waktu sistem berjalan (runtime log file), dan lain sebagainya.

Tentunya file disimpan pada media penyimpanan, dan ada banyak media penyimpanan dengan ragam fitur dan kapasitas penyimpanan.

Namun sebelum media penyimpanan digunakan, kita perlu langkah yang dinamakan format dan partisi. Partisi adalah tindakan untuk membagi media secara logika. Dan ada istilah *logical volume*, yang adalah kumpulan partisi yang dipandang sebagai satu entitas nantinya dan telah diformat atas dasar file system.

File system mendefinisikan bagaimana file dinamai, disimpan, diakses, dan diorganisasi pada *logical volume*.

File system menggunakan struktur data untuk mengacu pada lokasi file di media. File system data file ke media pada satu atau lebih file *allocation units*, ini mengacu pada

blok dan cluster. Sedangkan File Allocation Unit merupakan kumpulan sektor-sektor, merupakan unit terkecil pada media penyimpanan dalam kacamata logika.

Berikut berbagai jenis file system:

- FAT12 (umumnya digunakan pada floppy disk dan FAT volumes yang lebih kecil dari 16 MB).
- FAT16 (umumnya pada sistem operasi MS-DOS, Windows 95/98, Windows NT/2000, Windows XP, Windows Server 2003, dan beberapa OS UNIX). Digunakan pula pada perangkat multimedia semisal kamera digital. FAT16 menggunakan file allocation table entry 16-bit untuk meng-address 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, and Windows Server 2003, demikian pula dengan banyak perangkat multimedia). FAT32 menggunakan file allocation table 32-bit untuk mengalami entri ke file system. Kapasitas maksimum yang didukung sampai 2 Terabytes (TB).

- NTFS (sistem operasi Windows NT/2000/XP dan Windows Server 2003).
- 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 media CD.
- International Organization for Standardization (ISO) 9660 The ISO 9660 filesystem yang pada umumnya digunakan bagi CD-ROM.

Lalu bagaimana dengan penghapusan? Data-data yang ada pada media penyimpanan yang kemudian dihapus tidak sepenuhnya hilang begitu saja dari media penyimpanan.

Memang proses penghapusan sudah dilalui, tetapi penghapusan hanyalah menandai file-file tersebut, meskipun Anda sudah membersihkan recycle bin sekalipun.

Akan membutuhkan waktu yang lama bagi file untuk benar-benar hilang dari media penyimpanan, mungkin karena nantinya digunakan untuk menyimpan file lain. Oleh karena itu file-file yang sudah dihapus masih memungkinkan untuk didapatkan kembali.

Istilah *Slack Space* pada media penyimpanan adalah lokasi yang tidak terpakai, ini ada hubungannya dengan file system.

Sedangkan *Free Space* merupakan lokasi penyimpanan yang masih dapat digunakan, tetapi belum tentu kosong, karena kemungkinan masih ada data di dalamnya karena proses delete. Oleh karena itu masih memungkinkan data diperoleh dari free space.

Dengan karakteristik media penyimpanan yang demikian, tentunya ada penanganan khusus yang harus diberlakukan oleh si Examiner, yang diawali dengan proses pengumpulan (Collecting).

Sewaktu mengumpulkan data, Examiner akan bekerja pada banyak data dan media hasil duplikasi. Fungsinya adalah membuat banyak duplikasi dari storage device termasuk pula datanya.

Meng-copy file dari media penyimpanan pada umumnya menggunakan dua buah teknik berikut:

1. **Logical Backup.** Meng-copy file dan direktori, yang tentunya hanya meng-copy file-file yang secara logika tersimpan pada media penyimpanan. Ini tidak mencakup peng-copy-an file yang dinyatakan ‘dihapus’, dan lainnya.
2. **Bit Stream Imaging.** Copy mencakup pula free space dan slack space.

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

- Waktu modifikasi
- Waktu pengaksesan (mencakup melihat, mengakses, dan mencekat file)
- Waktu pembuatan

Memeriksa Data

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

Mengekstrak Data

Dalam melakukan ekstraksi data, tentunya Anda harus tahu file-file apa saja yang ada di dalamnya. File gambarkah, file lagukah? Untuk mengetahui karakteristik file, dapat kita lihat melalui extension file tersebut. Tetapi sayangnya pengguna dapat saja memanipulasi extension file yang akan memberikan kesulitan tersendiri.

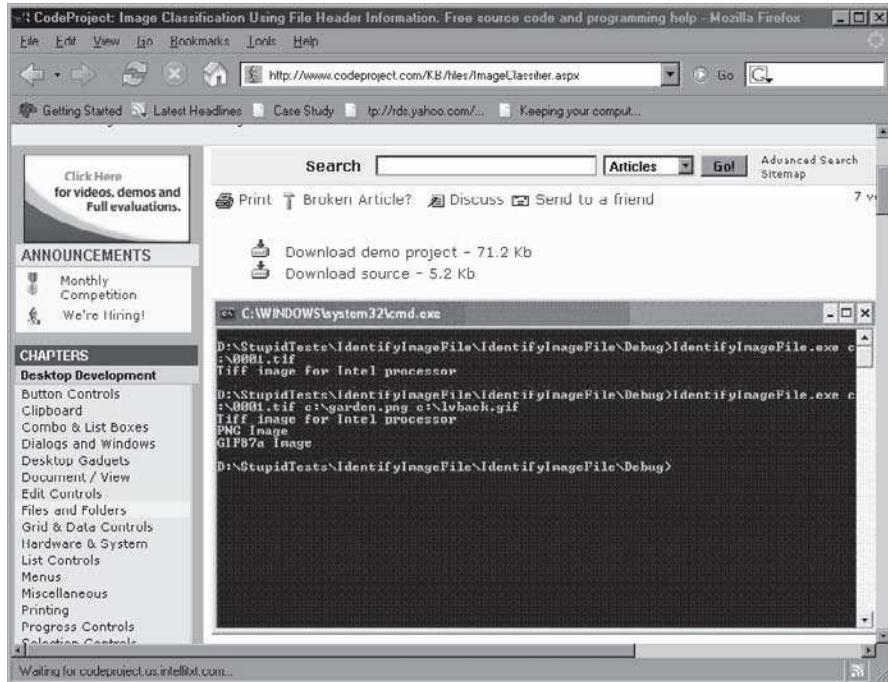
Cara paling jitu untuk mengetahui file tersebut adalah dengan melihat header information file tersebut.

Salah satunya dicontohkan pada Gambar 5.2 menggunakan program IdentifyImageFile. Program ini mampu menganalisa format file dari pembacaan header-nya.

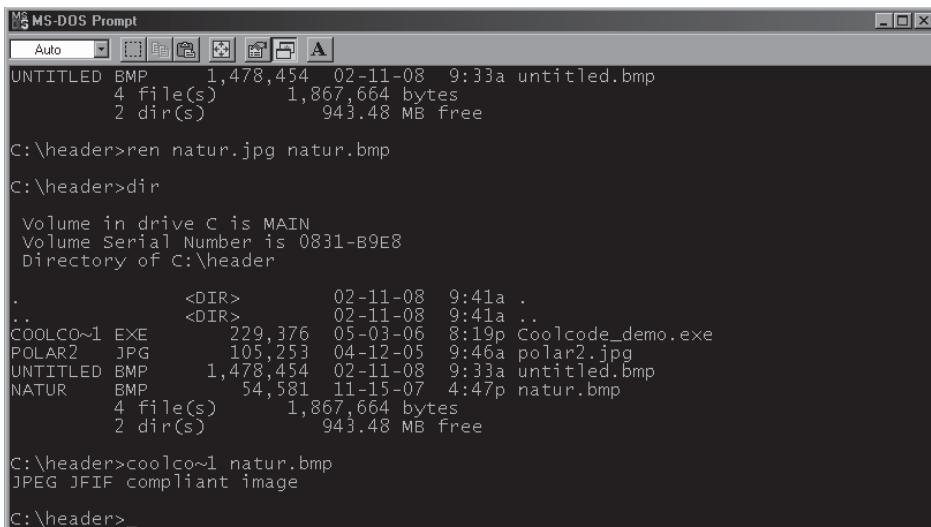
Pada Gambar 5.2 penulis mengubah extension fie tersebut yang seharusnya *.jpg menjadi *.bmp, tetapi program tersebut tetap mengenali-nya sebagai file berformat *.jpg.

Untuk mengeksplorasi lebih dalam bagaimana pembacaan header file, dapat Anda download source code-nya pada website yang tertera pada Gambar 5.1.

.



Gambar 5.1 CodeProject.com – Download demo project



Gambar 5.2 Program IdentifyImageFile.exe

Menggunakan Software Forensik

Beberapa fungsi umum yang dimunculkan dari software forensik sehubungan penanganan data file antara lain:

- File viewer
- 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, seperti kapan kejadian terjadi, kapan waktu file dibuat atau dimodifikasi, kapan e-mail dikirim, dan lain sebagainya.

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

Tip

Examiner bekerja menggunakan data-data duplikasi, bukan data sebenarnya yang menjadi evidence.

Data Sistem Operasi

Dalam memandang data-data dalam 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 informasi user account dan group account, termasuk atribut lain semisal karakteristik user account).
 - ✓ Password Files
 - ✓ Schedule Task (informasi ini menjadi bagian dari konfigurasi sistem operasi dan akan ada beberapa aksi dijalankan berdasarkan penjadwalan kerja, misalnya menjalankan program antivirus sebulan sekali.)
- Logs File (log ini berisi aktivitas dari sistem operasi, bahkan menyimpan pula aktivitas spesifik dari program aplikasi. Metode penyimpanannya cukup beragam, mungkin hanya menggunakan file teks, database, atau lainnya. Pada beberapa kasus bisa saja

- aktivitas disimpan pada log file yang berbeda).
- ✓ System Events (merupakan kegiatan operasional sistem operasi, misalnya sewaktu sistem startup atau proses shutdown. Kegagalan atau keberhasilan aktivitas yang dilakukan ini tercatat).
 - ✓ Audit Records (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, bahkan kegagalan aplikasi).
 - ✓ Command History (umumnya ada log file lain terpisah untuk mencatat aktivitas ini, semisal perintah-perintah sistem operasi yang di-request oleh user).
 - ✓ Recently Accessed Files (sistem operasi mungkin mencatat pula file-file dan program aplikasi yang diakses baru-baru ini).
 - Application Files (program aplikasi terdiri dari banyak file yang terintegrasi, seperti file executable, file berisi skrip pemrograman, log file, file konfigurasi, grafik, audio, icon (*.ico), dan lainnya).
 - Data Files (digunakan untuk menyimpan informasi dari program aplikasi. Ada banyak macam file data yang Anda kenal dan sering Anda gunakan).
 - Swap Files (digunakan untuk memperluas kemampuan memori komputer, tentunya akan dianggap sebagai memori yang temporer).
 - Dump Files (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 Files (file ini diciptakan saat instalasi sistem operasi, instalasi program aplikasi, proses peng-update-an, dan bahkan diciptakan saat program aplikasi berjalan. Umumnya file tersebut dihapus setelah software aplikasi ditutup, meskipun demikian, bisa saja karena kasus tertentu file tersebut masih tersimpan).
- Yang termasuk dalam data volatile yaitu:**
- Slack Space
 - Free Space
 - Network Configuration

- Network Connection
- Running Process
- Open Files
- Login Session
- Operating System Time

Dari karakteristik data sistem operasi, tentunya cara pengumpulan data volatile dan non volatile dibedakan.

Jenis data volatile OS:

- Content of Memory
- Network Configuration
- Network Connections
- 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 ke dalam software umum, misalnya:

- OS Command Prompt
- SHA-1 Checksum
- Directory List
- String Search
- Text Editor

Prioritas dalam mengumpulkan data harus dialamati dengan baik. Data yang lebih rapuh dan berpeluang hilang tentunya 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 non-volatile data umumnya melalui tahapan sebagai berikut:

- Men-shutdown sistem operasi
- Mematikan power dari sistem

Tool pada sistem operasi mampu mengorganisasi dan menyimpan informasi berharga yang sangat berguna untuk keperluan investigasi:

- Users and Groups
- Passwords
- Network Shares
- Logs

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, misal-

nya saja Hex Editor yang digunakan pada Swap File dan RAM Dumps.

Tip dan masalah yang muncul dalam pengumpulan data:

- **Pengaksesan OS**

Bisa saja user menggunakan password screensaver yang menghalangi examiner untuk mengumpulkan data, terlebih lagi data-data volatile. Akan sangat mudah untuk mem-bypass proteksi password screensaver, cukup dengan me-restart-nya, tetapi dengan demikian informasi dalam bentuk data-data volatile tentunya ikut hilang. Tentu dibutuhkan utility lain untuk meng-crack screensaver password tanpa harus me-reboot sistem.

- **Log Modification**

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

- **Hard Drive dengan Flash Memory**

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

- **Key Remapping**

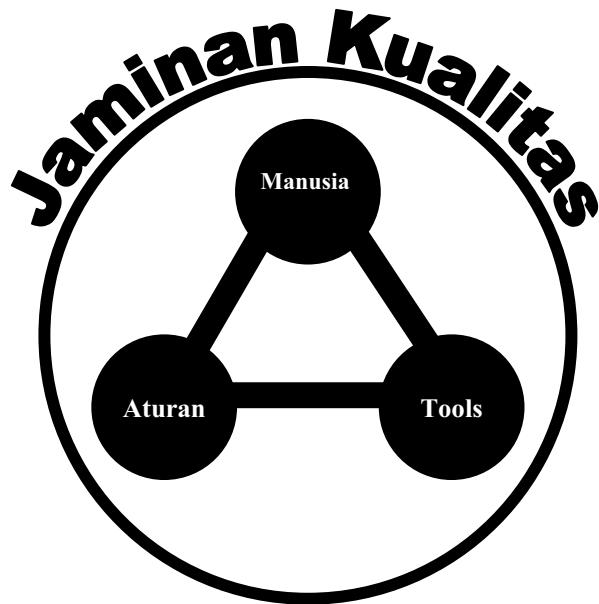
Kombinasi tombol-tombol keyboard dapat menjadi permasalahan dalam forensik, misalnya kombinasi tombol bisa membuat komputer restart atau

shutdown dan bahkan memformat harddisk. Cara terbaik adalah dengan tidak menggunakan keyboard tersebut. Gunakan komputer lain yang dihubungkan dengan cross over menggunakan 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. Lihat Gambar 5.3.

Pemahaman dengan Skill

- Bukan efisiensi, tetapi efektivitas adalah nomor satu!
- Organisasi harus memperhatikan kompleksitas teknis yang logis dari analisis forensik.
- Organisasi harus mampu dalam menangani bukan hanya semata-mata komputer forensik, tetapi mencakup pula network forensik.
- Organisasi harus mampu menentukan siapa-siapa saja yang harus menangani masing-masing aspek forensiknya.
- Examiner harus memiliki pengetahuan teknis yang memadai.
- Tim forensik harus memiliki kemampuan forensik yang mantap.



Gambar 5.3 Konsep Kelayakan Forensik

- Anggota tim harus berpartisipasi dalam proses forensik.
- Pertimbangan forensik harus melibatkan kebijakan-kebijakan.
- Organisasi harus menciptakan dan me-maintain panduan dan prosedur untuk menjalankan pekerjaan forensik.
- Examiner harus memiliki forensic toolkit yang digunakan dalam pengumpulan data, pemeriksaan, dan analisa.
- Organisasi harus menyediakan sarana dan prasarana penyimpanan yang mencakup log dari aktivitas jaringan.
- Organisasi harus mampu menangani forensik dengan konsisten.
- Organisasi secara proaktif mengumpulkan data-data yang berguna nantinya.
- Examiner harus memperhatikan bermacam sumber data dengan bermacam file format yang mungkin.
- Examiner harus mempertimbangkan semua data aplikasi sumber yang mungkin.
- Pengumpulan data hendaknya mengikuti proses yang sudah di standarisasi oleh organisasi.
- Examiner harus menangani data volatile sistem operasi, kerapuh-

- an akan selalu melingkupi, metode tidak selalu harus kaku.
- Examiner menggunakan forensic toolkit yang tepat untuk mengumpulkan data volatile sistem operasi.
 - Examiner harus menjalankan metode untuk mematikan sistem (shutdown) dengan tepat.
 - Lakukanlah versifikasi integritas data.
 - Pemeriksaan tentunya dilakukan hanya pada data hasil duplikasi dan bukan data sebenarnya.
 - Examiner harus memperhatikan ketelitian dan keakuratan nilai dari data.
 - Dalam analisa data, Examiner tentunya mengandalkan pengenal berupa file header information, bukan sekedar file extension yang dapat dengan mudah dimanipulasi.
 - Fokus terhadap karakteristik dan berbagai perlakuan yang berpengaruh kemudian.
 - Gunakan pendekatan dengan metodologi dalam mempelajari data.
 - Organisasi harus memahami bahwa perihal teknis dan kompleksitas logis akan muncul seiring dengan analisa yang dilakukan.
 - Examiner mampu menyajikan data dari berbagai sumber.
 - Examiner harus meninjau ulang proses dan pengeraaan yang sudah dilakukan.
 - Examiner tentunya harus mempertimbangkan sumber data aplikasi yang mungkin.
 - Examiner harus mampu mengumpulkan data aplikasi dari bermacam sumber, nantinya keperluan akan rekonstruksi dan menjelaskan detail tentangnya dibutuhkan.

Investigasi!

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

Keahlian yang melibatkan komputer forensik didapatkan bukan bertumpu melulu pada hal-hal teknis, justru pengalaman dan waktulah yang membuat seseorang memiliki ‘skill investigasi’.

Tentunya kasus per kasus membuat seorang examiner semakin matang. Tindak kriminal dengan segala macam aktivitas yang dilakukan tidak sebegitu mudahnya dipecahkan ha-

nya berdasarkan pengalaman komputer yang baik. Disamping itu examiner harus berurusan dengan evidence yang tergolong rentan.

Kerapuhan evidence sangat dimungkinkan terjadi karena faktor:

- Pemakai melakukan perubahan terhadapnya.
- Sangat mudahnya dirusak ataupun dimodifikasi.
- Kesalahan dalam menangani data dan media penyimpanan akan sangat berpengaruh terhadap data yang adalah evidence.

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, waktu komputer mungkin tidaklah akurat, tapi itupun perlu dipertimbangkan.

Aksi kriminal pun semakin rapi dan terorganisasi, mungkin sudah direncanakan dengan sedemikian rupa. Banyak aktivitas yang dilakukan untuk menutupi aksi kriminal, disamping memang tidak mudah untuk menguak kejahatan. Examiner harus jeli mengalami aktivitas dan perilaku, misalnya saja (dalam ruang lingkup internet):

- Berbagi informasi dan bertransaksi (melibatkan dokumen, pornografi, perangkat lunak, dan lainnya).
- Memalsukan identitas.
- Menggunakan identitas lain.
- Mendistribusikan informasi yang salah.
- Data pada workstation, server, atau organisasi lain.
- Bagaimana seandainya tindak kriminal melakukan pertemuan. (teleconference, dan lainnya).
- Catatan ISP (Internet Service Provider).
- Dan hal lainnya.

Kita ambil contoh sewaktu investigasi melibatkan e-mail, 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 boleh luput 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 pada header dan menggunakan informasi tersebut untuk menentukan pengirim dari e-mail tersebut.

Examiner harus menggali informasi demi informasi, misalnya sewaktu dihadapkan pada e-mail tadi, tentunya si examiner tidak hanya memperhatikan *Attachment*, atau *Body* e-mail, meskipun konten e-mail tertumpu di sana. Lebih jauh lagi header memunculkan banyak jejak yang dapat diungkap.

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

- Spooofed e-mail header (Received pada e-mail header bisa saja palsu).
- Anonymizer.
- Remote location (layanan e-mail tersebar di tempat umum, tentunya akan sangat sulit menemukan pengirim yang sebenarnya).
- Lokasi e-mail.
- Pengiriman yang tertunda.

Dan ternyata, lagi-lagi itu pun belum-lah cukup. Examiner/Investigator mungkin membutuhkan informasi lain lagi. Informasi dibutuhkan dan melibatkan banyak pihak termasuk masalah hukum. Oleh karena itu hanya seseorang yang sudah terlatih layak untuk melakukan komputer forensik yang sesungguhnya.

Informasi yang lain lagi dibutuhkan misalnya saja:

- E-mail lain yang berhubungan dengan investigasi.
- Alamat e-mail lainnya.
- Log aplikasi yang akan memperlihatkan aksi spoofing.
- Informasi si pengirim.
- Isi dari komunikasi yang terjadi.
- IP Address.
- Password.
- Attachment.
- Waktu dan tanggal.

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 (misalnya YahooGroups). Ada beberapa pernyataan yang membutuhkan pertimbangan dan tindakan lebih lanjut dari examiner untuk menggali informasi tentang 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 meng-copy dan adakah user lain yang berperan dalam file arsip tersebut?
- Apakah waktu dan tanggal benar (dengan hosting server)?
- Siapa member lain yang ada?
- Bagaimana pendakwa/pelapor menemukan message board?
- Berapa lama si pelapor ini menggunakan message board?
- Apakah ada informasi lainnya yang didapat tentang tersangka?
- Apakah si pelapor menggunakan sarana lain untuk berhubungan dengan tersangka?

Lainnya mungkin bisa ditambahkan sewaktu penemuan demi penemuan muncul ke permukaan.

Skill investigasi ternyata demikian kompleks, bukan hanya mengenai

metode atau prosedur, tetapi pemahaman yang menyeluruh dan kematangan menjadi sangat utama keberadaannya!

BAB 6

Bedah Komputer Forensik

- Berawal dari Hal Sederhana
- Windows Registry
- Informasi Esensial pada Registry
- Informasi dari Software Forensik

Berawal dari Hal Sederhana

Memantau aktivitas sistem akan sangat menarik, terlebih lagi jika Anda mencurigai gerak-gerik seseorang yang mungkin memakai komputer bersamaan dengan Anda. Anda dapat mulai 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 "ter-

larang" yang diakses, atau history dari file-file "miring" yang di-download, bahkan pesan e-mail yang masih tersimpan dalam temporary internet files, pasti ini membangkitkan rasa ingin tahu.

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

Perhatikan pada Gambar 6.1, ternyata aktivitas penggunaan modem ada pengaturannya dan kegiatan yang terjadi terdokumentasi, ini tersimpan dalam log file (perhatikan Gambar 6.2).



Gambar 6.1 Modem Connection Setting

```
U.S. Robotics 56K FAX EXT.log - WordPad
File Edit View Insert Format Help
[Windows icons]
[WordPad icons]
[Search icon]
[Print icon]
[Save icon]
[Open icon]
[New icon]
[Close icon]
[Minimize icon]
[Maximize icon]
[Close icon]

12-11-2007 10:44:52.24 - U.S. Robotics 56K FAX EXT in use.
12-11-2007 10:44:52.25 - Modem type: U.S. Robotics 56K FAX EXT
12-11-2007 10:44:52.25 - Modem inf path: MDM3COM.INF
12-11-2007 10:44:52.25 - Modem inf section: ModemPCMext
12-11-2007 10:44:52.48 - 57600,N,8,1
12-11-2007 10:44:52.48 - Initializing modem.
12-11-2007 10:44:52.48 - Send: AT<cr>
12-11-2007 10:44:52.48 - Recv: AT<cr>
12-11-2007 10:44:52.61 - Recv: <cr><lf>OK<cr><lf>
12-11-2007 10:44:52.61 - Interpreted response: Ok
12-11-2007 10:44:52.61 - Send: AT&F1E0Q0V1&C1&D2S0=0<cr>
12-11-2007 10:44:52.61 - Recv: AT&F1E0Q0V1&C1&D2S0=0<cr>
12-11-2007 10:44:52.74 - Recv: <cr><lf>OK<cr><lf>
12-11-2007 10:44:52.74 - Interpreted response: Ok
12-11-2007 10:44:52.74 - Send: AT&T=60319=2M0&K1&H1&R2&I0BOX4<cr>
12-11-2007 10:44:52.87 - Recv: <cr><lf>OK<cr><lf>
12-11-2007 10:44:52.87 - Interpreted response: Ok
12-11-2007 10:44:52.87 - Dialing.
12-11-2007 10:44:52.87 - Send: ATDT<cr>
12-11-2007 10:44:54.47 - Recv: <cr><lf>OK<cr><lf>
12-11-2007 10:44:54.47 - Interpreted response: Ok
12-11-2007 10:44:54.47 - Dialing.
12-11-2007 10:44:54.47 - Send: ATD#####<cr>
12-11-2007 10:45:44.33 - Recv: <cr><lf>NO CARRIER<cr><lf>
12-11-2007 10:45:44.33 - Interpreted response: No Carrier
12-11-2007 10:45:44.33 - Hanging up the modem.
12-11-2007 10:45:44.33 - Send: ATH<cr>
12-11-2007 10:45:44.46 - Recv: <cr><lf>OK<cr><lf>
12-11-2007 10:45:44.46 - Interpreted response: Ok
12-11-2007 10:45:44.46 - 57600,N,8,1
12-11-2007 10:45:44.46 - Session Statistics:
12-11-2007 10:45:44.46 - Reads : 69 bytes
12-11-2007 10:45:44.46 - Writes : 81 bytes
12-11-2007 10:45:44.46 - U.S. Robotics 56K FAX EXT closed.
12-11-2007 10:46:06.12 - U.S. Robotics 56K FAX EXT in use.
12-11-2007 10:46:06.13 - Modem type: U.S. Robotics 56K FAX EXT
12-11-2007 10:46:06.13 - Modem inf path: MDM3COM.INF
12-11-2007 10:46:06.13 - Modem inf section: ModemPCMext
12-11-2007 10:46:06.37 - 57600,N,8,1
```

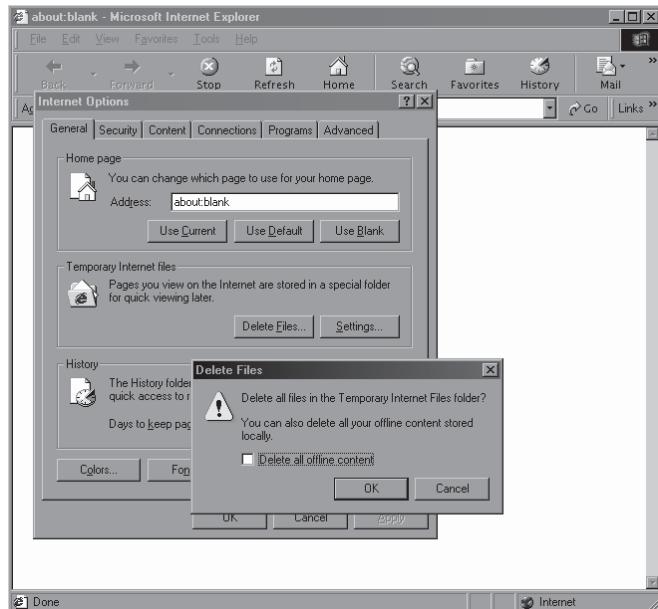
Gambar 6.2 Modem – Log File

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

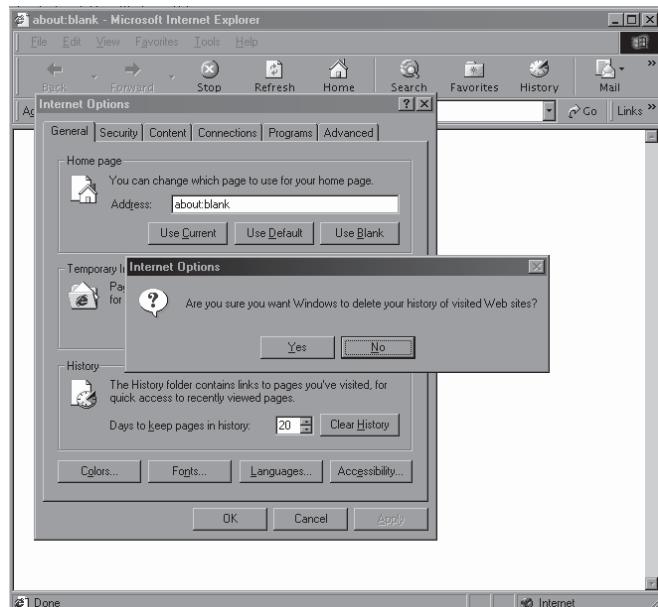
Mungkin pengguna komputer tidak menggunakan program Internet Explorer untuk mengakses internet, tetapi misalnya saja menggunakan Mozilla FireFox, Netscape, Opera, dan lain sebagainya. Informasi beraktivitas ini didokumentasikan seca-

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

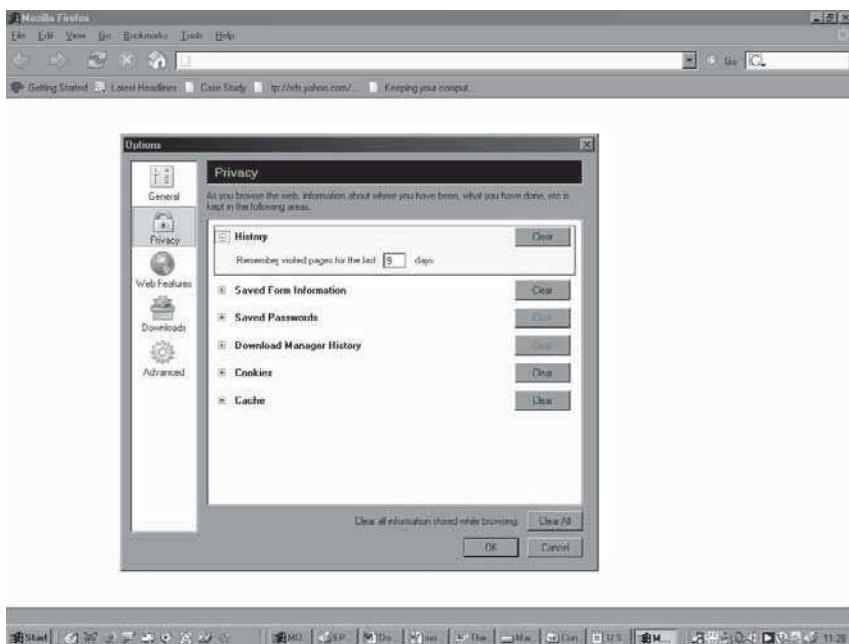
Tentunya Anda pernah menghapus file dan bahkan membersihkan ke ranjang sampah (recycle bin) Anda, tetapi hati-hati, file tersebut tidak sepenuhnya hilang dalam harddisk. Masih dimungkinkan untuk mendapatkan kembali informasi seperti itu meskipun recycle bin Anda dalam keadaan bersih dari sampah.



Gambar 6.3 Temporary Internet Files



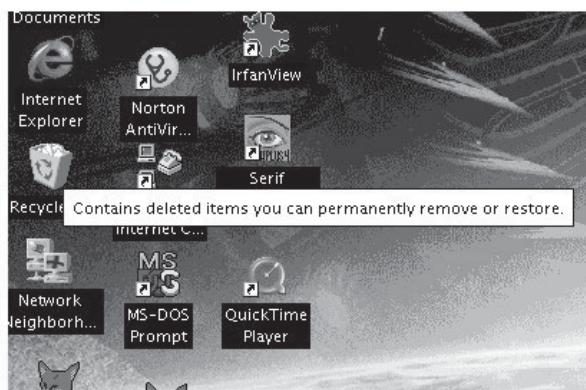
Gambar 6.4 Visited Website History



Gambar 6.5 Privasi Informasi – Mozilla

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 harddisk Anda (hanya ditandai sudah dihapus).

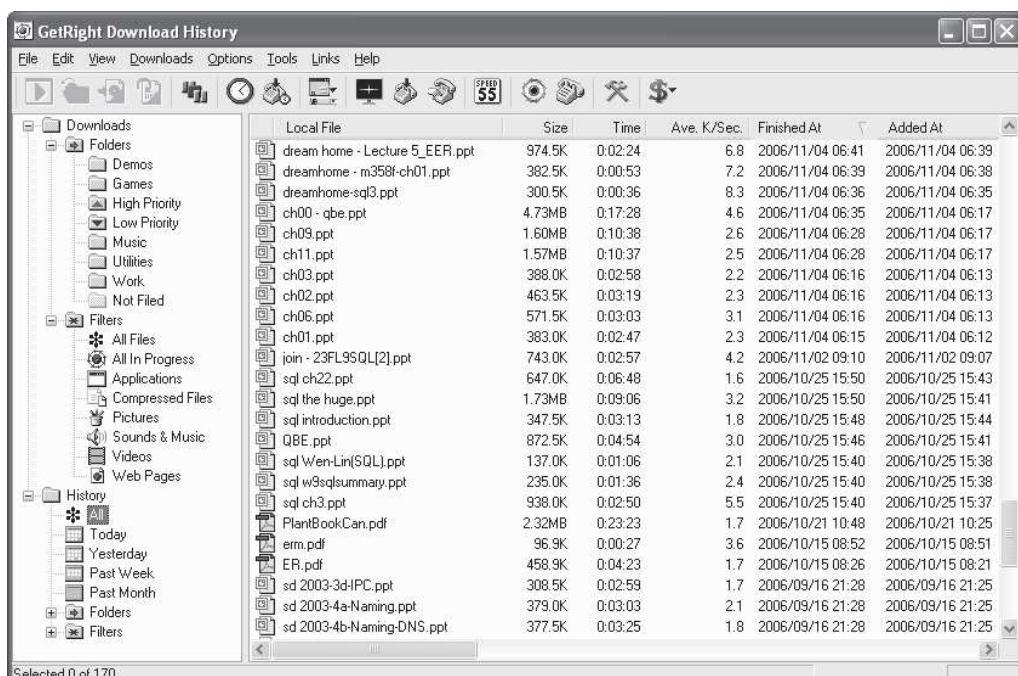


Gambar 6.6 File pada Recycle Bin

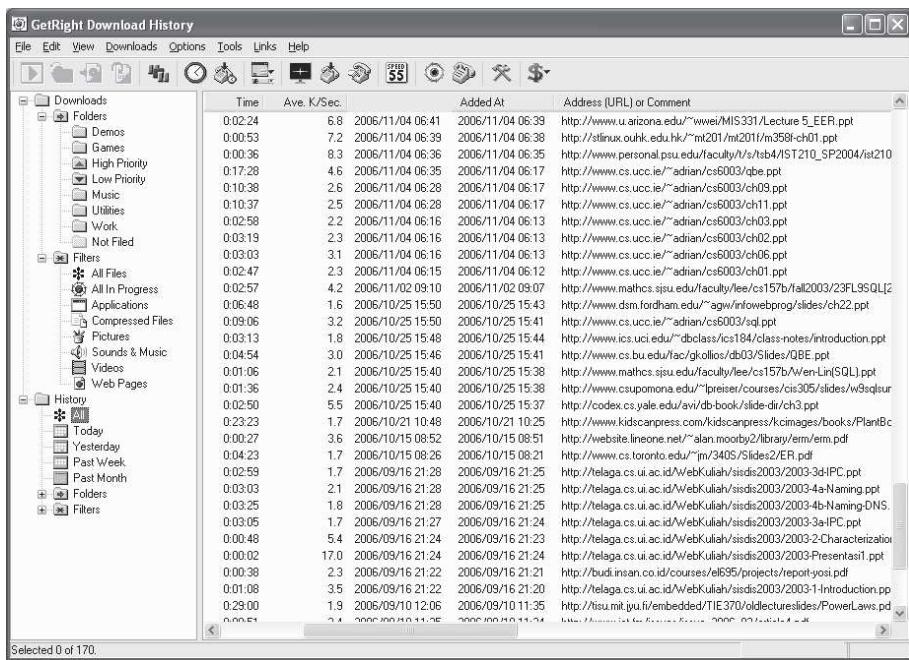
Anda juga pastinya sering men-download program dari internet, seperti file-file gambar, lagu, atau file movie. Bukankah lebih nyaman jika menggunakan software khusus untuk men-download-nya? Namun, software demikian dapat mendokumentasikan secara rapi aktivitas Anda di dalamnya. Coba perhatikan salah satu software download semisal Getright pada Gambar 6.7 dan Gambar 6.8. Website mana saja tempat Anda men-download file pun

tercatat. Ini memudahkan Anda untuk men-download kembali dan memudahkan pula bagi examiner untuk menelusuri aktivitas Anda!

Hal sederhana lain yang pada satu atau lain kasus dapat dijadikan parameter misalnya data berkenaan recently file used. File-file apa saja yang Anda akses terakhir kali yang menunjukkan aktivitas Anda dalam menggunakan file dan program didokumentasikan (Gambar 6.9).



Gambar 6.7 Getright Download History



Gambar 6.8 Getright Download History - URL



Gambar 6.9 Recently Used

Windows Registry

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

Untuk itu Anda harus memahami struktur registry windows, perilaku aplikasi, sistem operasi komponen lain yang terlibat seperti data, dan ragam aktivitas. Tentunya sama seperti pembedahan, Anda membutuhkan tool-tool spesifik sebagai interface bagi Anda, yang membantu Anda dalam pembedahan.

Pembongkaran registry yang Anda lakukan akan terasa menarik dan menggelitik, menuntun Anda untuk melakukan pembedahan yang lain, area lain, dan peralatan yang lain. Bersamaan dengan itu, Anda mulai melihat informasi yang sedikit demi sedikit memberikan titik terang.

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

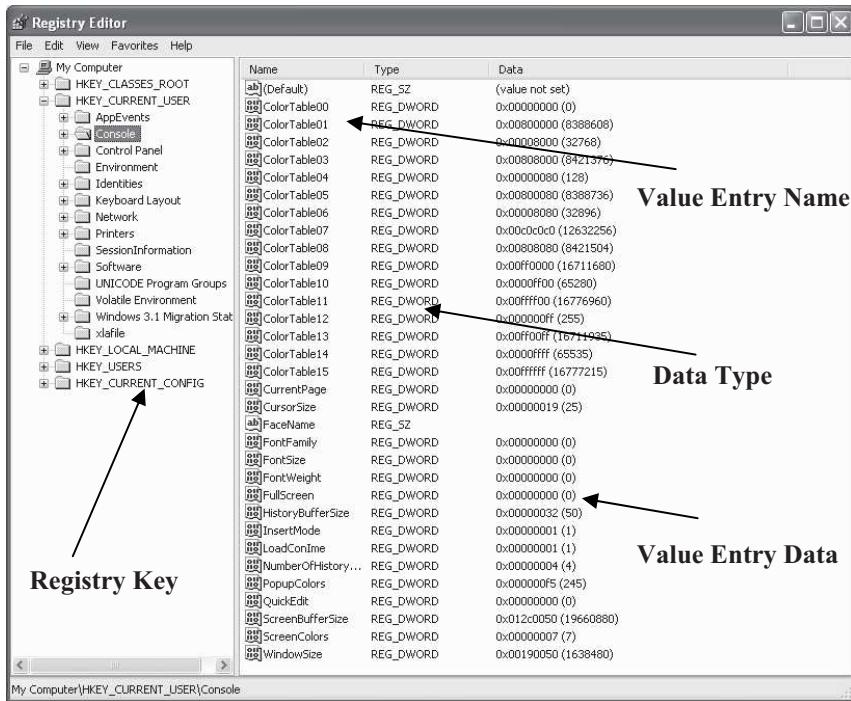
Registry merupakan konfigurasi sistem yang substansial dan merupakan single logical data store. Pada dasarnya registry dibagi ke dalam tiga database yang terpisah dialokasikan untuk menangani user, sistem, dan pengaturan jaringan (*network policies*).

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

Berdasarkan pernyataan di atas, Microsoft memang menggunakan registry sebagai ‘hub’ dalam menyimpan informasi yang berhubungan dengan sistem operasi. Disinilah 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 lainnya hanya pengembangan yang merupakan shortcut yang mengacu pada dua hives ini. Perhatikan Gambar 6.10.

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



Gambar 6.10 Registry Editor - ROOT KEY (HIVES)

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

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 visual settings.

- **HKEY_LOCAL_MACHINE.** Hive yang terdiri dari informasi spesifik komputer yang berhubungan langsung dengan sistem operasi, misalnya: daftar drive yang digunakan, perangkat keras yang terintegrasi dan konfigurasi dasar aplikasi yang diinstalasi.
- **HKEY_CLASSES_ROOT.** Informasinya tergolong sama dengan Reg.dat. Berisi detail lebih jauh berkaitan aturan *drag-and-drop*, shortcut, 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 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: 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 yang menggunakan arsitektur plug-and-play. Misalnya saja sewaktu mem-plug in 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 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

File registry disimpan pada lokasi yang berbeda, bergantung pada sistem operasi Windows yang digunakan, misalnya saja:

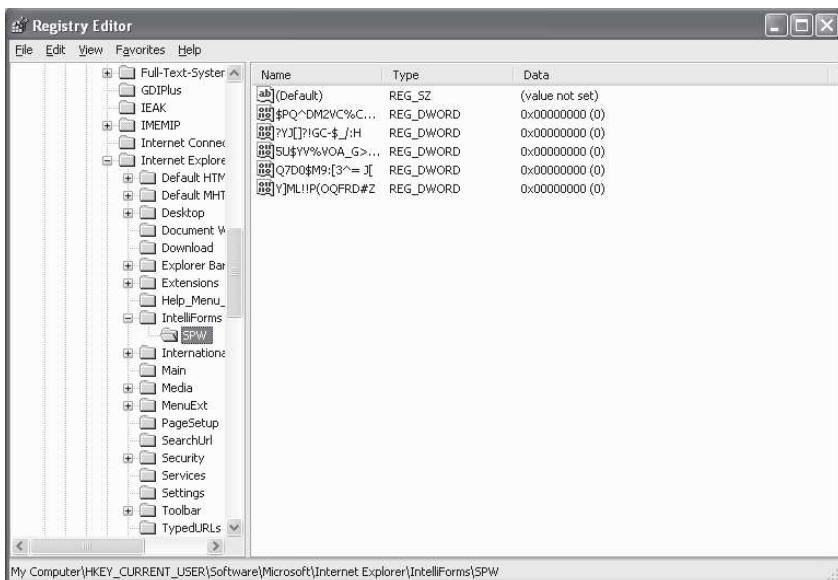
- Windows 3.x pada c:\windows\reg.dat
- Windows 98 pada c:\windows
- Windows NT pada c:\winnt\system32\config
- Windows XP pada c:\windows\system32\config

Informasi Esensial pada Registry

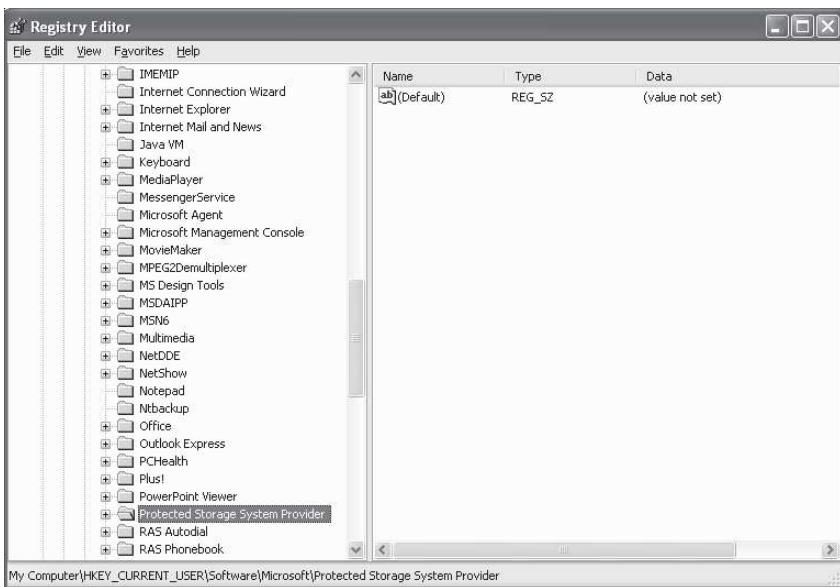
Kita langsung saja melihat apa-apa yang disimpan pada registry Anda, terlepas dari hal-hal teknis yang dapat Anda pelajari kemudian berkenaan registry dan masing-masing *hive*-nya.

Bagaimana password disimpan pada registry? Coba Anda perhatikan Gambar 6.11 dan Gambar 6.12, ini mengacu pada informasi registry:

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



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



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

Akan sangat membingungkan untuk memahami informasi demikian. Anda membutuhkan interface lainnya. Pergunakanlah software aplikasi yang mampu membaca informasi yang tersimpan di dalamnya.

Untuk itu penulis menggunakan software PassView yang mengeksplorasi informasi pada registry tadi. Software ini mampu memberikan informasi berikut kepada Anda:

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

Anda tinggal menjalankan saja software tersebut dengan satu kali klik, dan hasilnya dapat Anda lihat pada Gambar 6.13 pada kolom password.

Untuk start up aplikasi, Anda bisa mengakses 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\

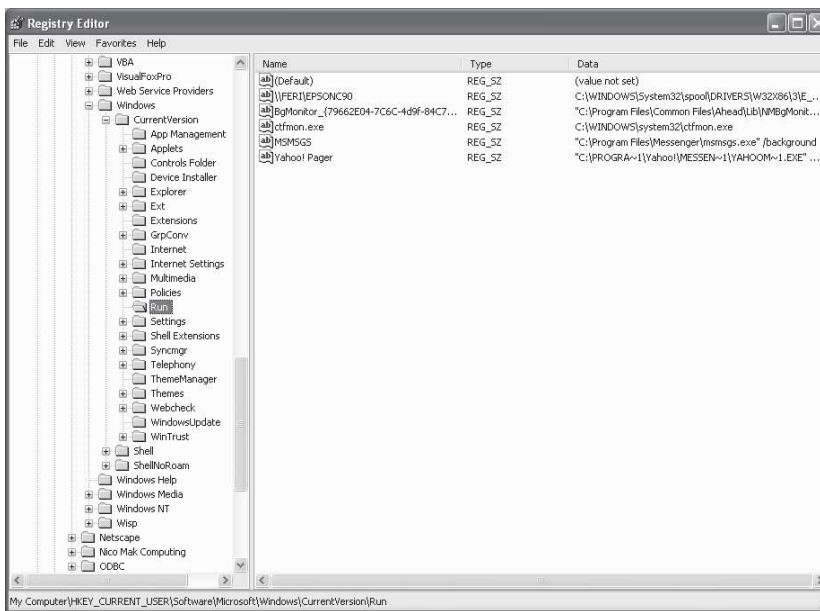
Salah satunya dapat Anda lihat pada Gambar 6.14, Gambar 6.15.

Protected Storage PassView				
Resource Name	Resource Type	User Name/Value	Password	Protected Storage Type
ferisulanta	MS Outlook 2002	Ferisulanta	rahasia	Identification\Outlook Account Management
IdentityPass	Outlook Express Identity	Main Identity		IdentityManager\Identities
http://mail.telkom.net	AutoComplete Passwords	Ferisulanta	rahasiarahasiarahasiarahasia...	Internet Explorer\Internet Explorer
...	AutoComplete Passwords	ferisulanta.mrifferisulanta.mrf...	rahasiarahasiarahasiarahasia...	Internet Explorer\Internet Explorer
http://mail.telkom.net/	AutoComplete Passwords	Ferisulanta	rahasiarahasiarahasiarahasia...	Internet Explorer\Internet Explorer
http://www.facebook.net/	AutoComplete Passwords	Ferisulanta	password	Internet Explorer\Internet Explorer

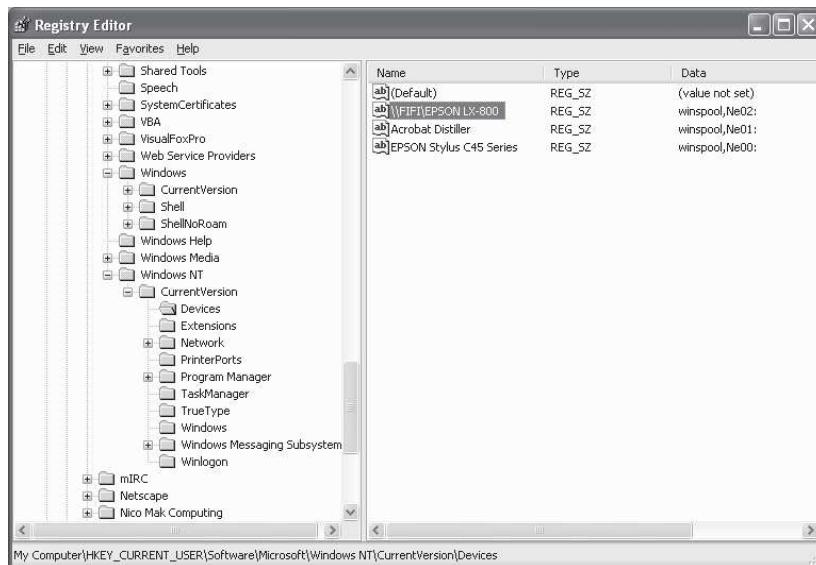
Gambar 6.13 Registry – PassView Program

Registry Editor		
File	Edit	View
Shared Tools		
Speech		
SystemCertificates		
VBA		
VisualFoxPro		
Web Service Providers		
windows		
CurrentVersion		
Applets		
Controls Folder		
Device Installer		
Explorer		
Extensions		
Group Policy		
GrpConv		
Internet		
Internet Settings		
Policies		
Run		
RunOnce		
Settings		
Syncmgr		
Telephony		
ThemeManager		
Themes		
Webcheck		
WIA		
WinTrust		

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



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

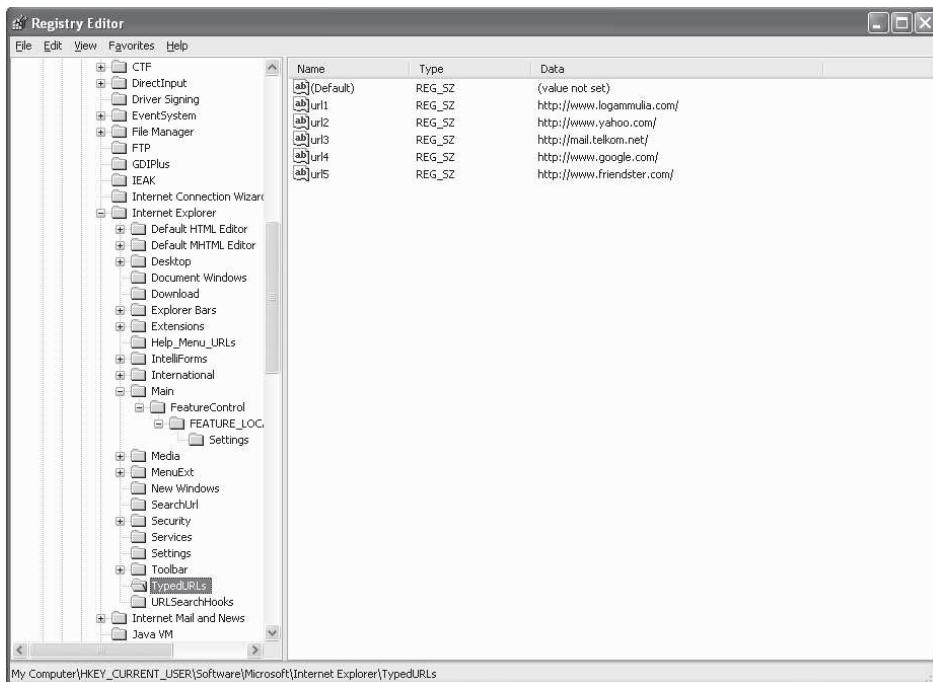


Gambar 6.16 HKCU\Software\Microsoft\Windows NT\CurrentVersion\Device

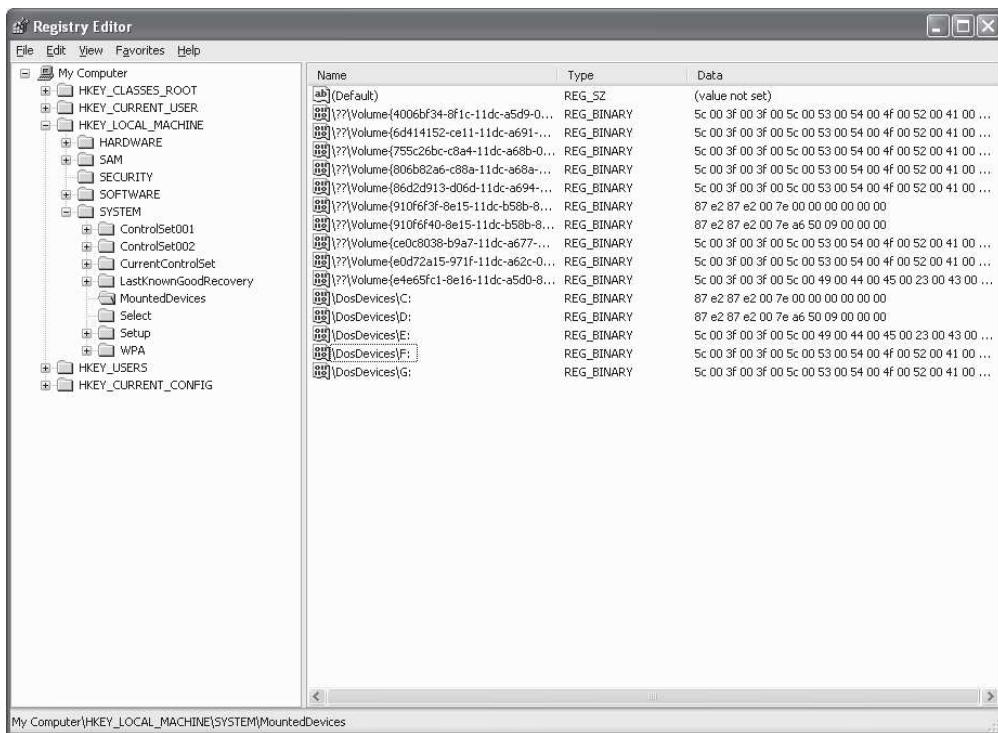
Beberapa device yang saat ini terintegrasi dapat Anda lihat pada Gambar 6.16.

Lalu aktivitas Anda berinternet dapat dilihat dengan mengakses Windows Registry, coba perhatikan Gambar 6.17. Ditampilkan list dari URL yang baru-baru ini Anda akses.

Hal lain lagi yang dapat dianalisa dari registry Windows, misalnya berbagai media penyimpanan yang pernah diintegrasikan dengan sistem komputer, semisal USB Flashdisk, Floppy dan lainnya yang tentunya dapat menaungi informasi yang adalah evidence. Riwayatnya dapat terlihat melalui registry. Anda perhatikan Gambar 6.18.



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



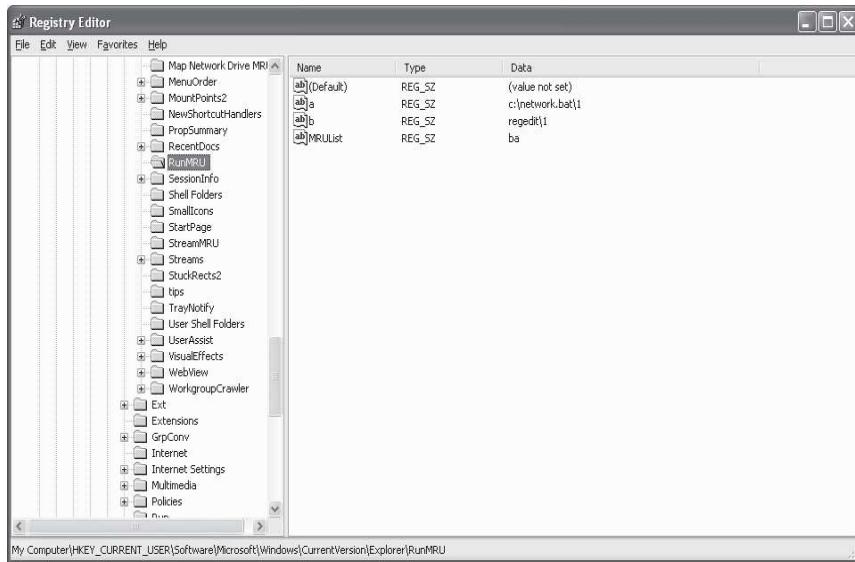
Gambar 6.18 HKLM\System\MountDevices

Mungkin juga Anda mengetikkan command pada Run Command Windows, ini pun tercatat pada registry (Gambar 6.19).

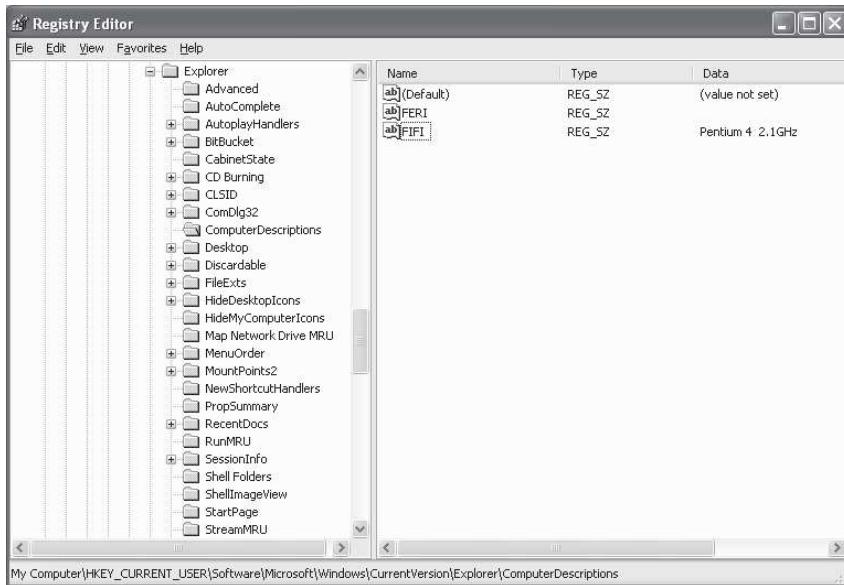
Kompleksitas komputer forensik akan bertambah jika melibatkan cakupan yang lebih luas, misalnya sistem yang terletak/diintegrasikan dengan jaringan komputer, aktivitas user yang bersangkutan di jaringan

pun menjadi demikian penting untuk dianalisa, bahkan komputer-komputer apa saja yang mungkin pernah terkoneksi dengan komputer *suspect*.

Coba perhatikan pada Gambar 6.20, diperlihatkan ada beberapa komputer yang bersisi-sisian dengan komputer suspect, bagaimana user kemudian beraktivitas dapat diekplorasi lebih dalam.



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



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

Informasi dari Software Forensik

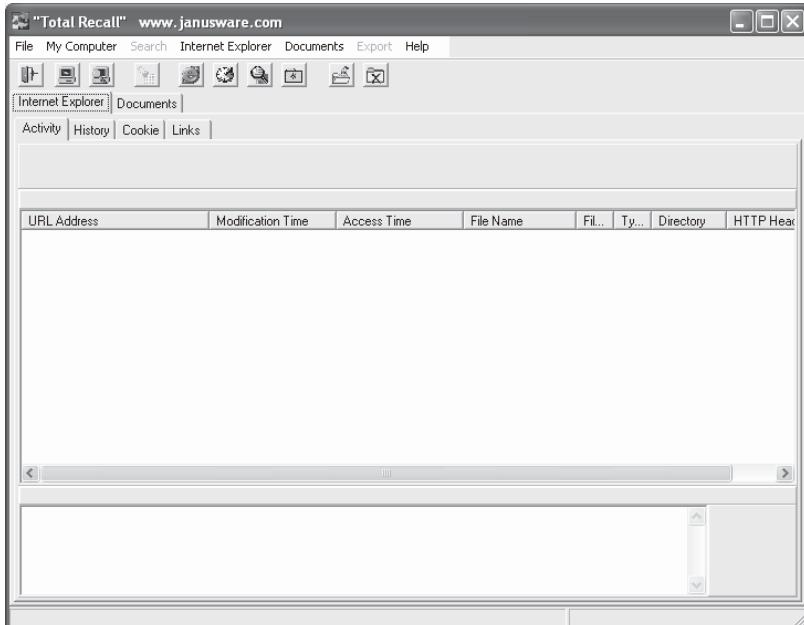
Komputer desktop sudah menjadi perangkat teknologi informasi dan komunikasi yang banyak digunakan, setiap orang menginginkan satu bagi dirinya, ini terbukti banyaknya pengguna komputer rumahan dan perkantoran yang menggunakan komputer desktop dalam beraktivitas.

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

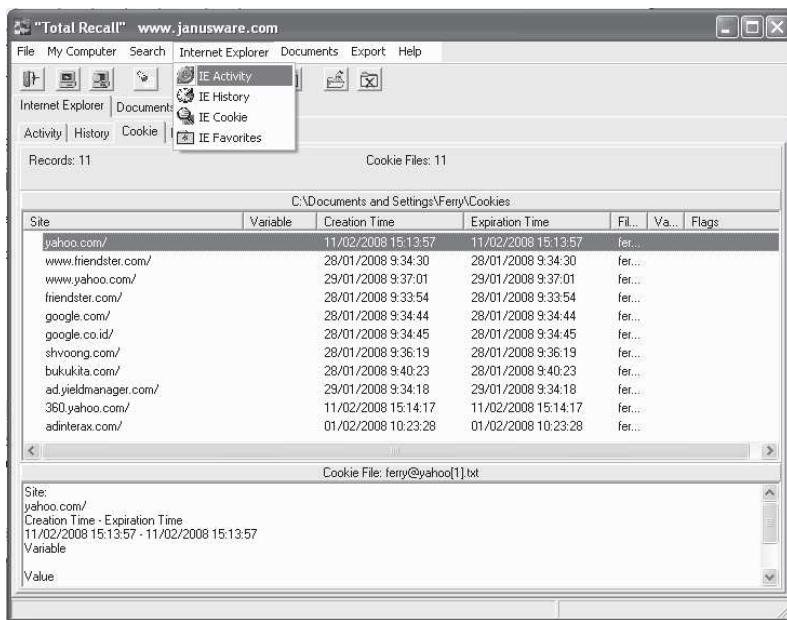
Salah satu aplikasi yang digunakan dalam mengakses informasi yang terdokumentasi demikian adalah Total Recall Software (Gambar 6.21), salah satu forensic analysis tool gratis yang digunakan untuk merekonstruksi aktivitas.

Total Recall mampu merekonstruksi aktivitas yang terjadi pada Microsoft Internet Explorer, mencakup pula aktivitas pengguna komputer tersebut. Perhatikan Gambar 6.24.

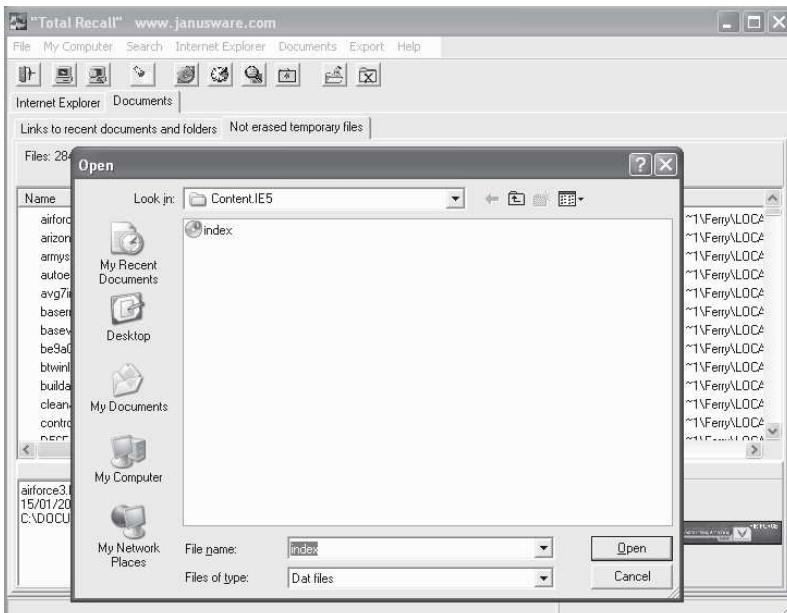
Pada dasarnya aktivitas internet disimpan oleh Microsoft Internet Explorer dan disimpan pada file **index.dat** (Gambar 6.23).



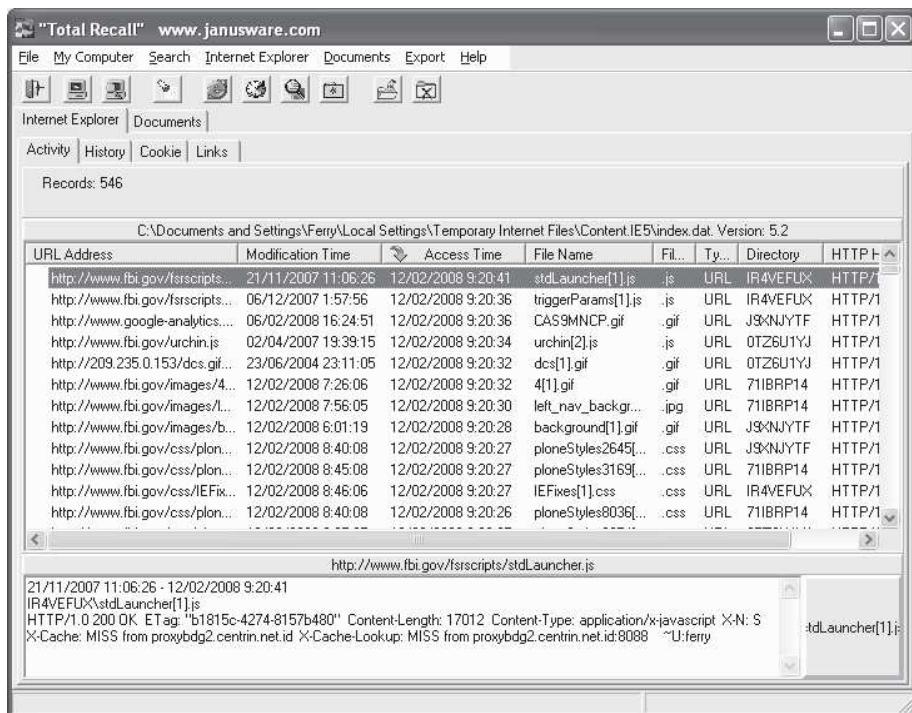
Gambar 6.21 Total Recall Software



Gambar 6.22 Total Recall Software – Internet Activity



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



Gambar 6.24 Total Recall Software – Internet Activity - List

Informasi seputar user data, *internet cookies*, dan *internet history* berada tersebar dan dapat ditemukan pada folder di *users profile*. Aktivitas lain semisal *Browser activity files* disimpan dalam bentuk biner, maka dari itu dibutuhkan software khusus untuk membaca informasi tersebut.

Beberapa investigasi yang dimunculkan oleh program ini antara lain:

- Aktivitas pada Internet Explorer
- Internet Explorer history
- Internet Explorer cookie
- Favorites pada Internet Explorer

- Aktivitas pemakai, yang mencakup: not erased temporary files, recent files and folders.

Informasi dapat diekspos dalam bentuk file .XML (Extensible Markup Language) dan .TXT (teks).

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

Buku ini tidak memberikan Anda bentuk riil dari komputer forensik, akan banyak kasus, organisasi atau-pun perangkat dengan developer masing-masing yang terlibat nantinya, dan akan sangat tidak etis untuk mempersepsikan kasus yang tentunya harus berurusan dengan sebagian bahkan seluruh bukti otentik.

Di samping itu, tidak ada pedoman mutlak dalam menerapkan komputer forensik. Meskipun proses, metode, dan prosedur dibuat, semuanya hanyalah sebagai percontohan yang seharusnya menggagas Anda untuk mengembangkan dan mengadaptasinya kemudian.

Anda dapat mencoba berbagai software komputer forensik yang disajikan dalam buku ini, termasuk pula merancang berbagai form, report, proses, dan metode tanpa harus mengorbankan kualitas dari makna forensik sesungguhnya.

BAB 7

Training Komputer Forensik

- Metode dan Silabus
- Training Online
- Komponen Training Forensik Komputer

Keahlian akan menjadi inti dari berkembangnya standarisasi dan diterimanya suatu tingkah laku komputer forensik pada akhirnya.

Memang pengaruhnya akan terasa lama melalui pemberlakuan standarisasi yang mencakup sertifikasi di tingkat profesional teknologi informasi, tetapi jika memang dilihat secara mengglobal, akan banyak hasil positif yang membenarkan pentingnya sertifikasi-standarisasi.

Tentunya mutu dan kualitas menjadi tujuan dari pemberlakuan sertifikasi yang nyata-nyatanya adalah standarisasi.

Metode dan Silabus

Berbagai organisasi komersial dan non-komersial banyak memberikan pelatihan untuk mengalami kebutuhan akan profesi bidang komputer forensik.

Ada salah satu bidang yang dikenal dengan Seized Computer Evidence Recovery Specialist (SCERS). Program pelatihan SCERS yang diadakan oleh salah satu organisasi (www.fletc.gov) mengajarkan dasar dan teknik komputer forensik untuk menganalisa *electronic data* pada komputer desktop dan perangkat komputer tertentu. Bagi yang ‘baru’ dengan komputer forensik, mereka dapat mulai mengenal dan mempe-

lajarinya, atau bagi mereka yang ingin meng-update pengetahuan di bidang komputer forensik, ini pun dimungkinkan.

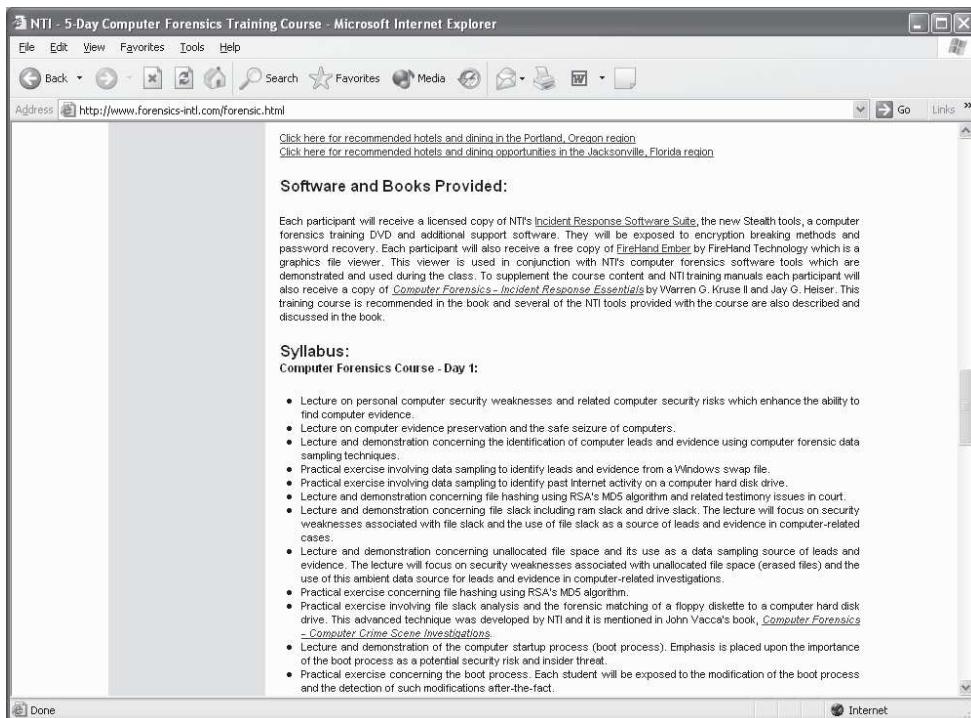
Perhatikan kurikulum/silabus yang diberikan berkenaan jasa training oleh website www.fletc.gov:

- Menyeting komputer forensik
- Istilah dan konsep digital forensik
- Analisa mendalam terhadap struktur sistem operasi Windows yang mencakup antara lain:
 - ✓ Recycle Bin
 - ✓ File Dates/Times
 - ✓ Graphik
 - ✓ Registry
 - ✓ Internet Explorer
 - ✓ Print Spools
 - ✓ Metadata
 - ✓ Link Files
 - ✓ Kompresi File
 - ✓ Alternate Data Streams
 - ✓ Thumbs.db
 - ✓ EFS

Penulis perhatikan apa yang disajikan dalam silabus cukup efektif untuk membangun pola pikir dan cara pandang komputer forensik, terlebih salah satu topik eksplorasi sistem operasi populer (Windows).

Kursus semacam ini tidak sertamerta membuat Anda menjadi ahli komputer forensik. Untuk menjadi terampil dibutuhkan pengalaman dan waktu. Belajar komputer memang mudah, tetapi untuk menjadi ahli dan terampil itu yang sulit!

Material training yang dibutuhkan umumnya mencakup berbagai macam hardware, software, berbagai peralatan lain termasuk pula buku dan software penuntun lainnya.



Gambar 7.1 Website NTI – Computer Forensics and Security Training - Silabus

Perhatikan komposisi training silabus yang disusun dalam NTI Website (<http://www.forensics-intl.com/forensic.html>) yang komposisi dan sebaran materinya sangat baik. Anda dapat melihat lebih jelas pada Gambar 7.1 yang mendeskripsikan perihal materi training.

Berbagai software utility komputer forensik orisinal diberikan mencakup perangkat lunak yang kompatibel dengan sistem operasi populer (misalnya: DOS, Windows 95, Windows 98, Windows NT, Windows 2000, dan Windows XP).

Diharapkan (dalam website tersebut) Anda akan mendapatkan pemahaman yang menyeluruh akan beberapa konsep dan skill berikut:

- Risiko keamanan komputer dan pemulihannya.
- Respon akan terjadi insiden, menentukan prioritas dan kebutuhan dalam membangun suatu tim kerja.
- Kesiapan evidence komputer.
- Ketepatan waktu dalam menganalisa file komputer berdasarkan aktivitas file seperti penciptaan file, modifikasi, dan akses file.
- Program malware semisal trojan horse.
- Perbedaan dan membedakan antara sistem operasi DOS dan Windows, mencakup berbagai Windows Family, diantaranya: Windows NT/2000/XP dalam sudut pandang komputer forensik.
- Metode dan prosedur baku komputer forensik dan proses yang dilibatkan.
- Dokumentasi berdasarkan temuan dari komputer forensik yang nantinya digunakan pada pemeriksaan dalam kasus pengadilan atau untuk me-review kebutuhan manajemen.
- Mengidentifikasi historis dari penggunaan internet, mencakup

browsing internet, download file, dan komunikasi via e-mail.

- Menggunakan *forensic search tools* untuk mengidentifikasi *data leakage* dan mencakup pula berbagai risiko keamanan. Setiap peserta nantinya akan diberikan software NTI berlisensi.
- Menggunakan testing dan *data elimination tool* Departeman Pertahanan US untuk eliminasi komputer yang teridentifikasi atas dasar faktor risiko keamanan. Setiap peserta nantinya akan diberikan pula software NTI berlisensi.
- Menggunakan software komputer forensik untuk pengecekan berbagai penemuan berkenaan *computer evidence* yang berelasi dengan kasus yang dimaksud.
- Penggunaan software komputer forensik dalam pengecekan dan menentukan eliminasi *data leakage*, tentunya mempertimbangkan pula *government security risk assessments*. Setiap peserta nantinya akan diberikan pula software NTI berlisensi.
- Masalah relevan dalam menanggulangi *legal junk science attack* (masalah hukum dan teknis komputer yang bersinggungan).

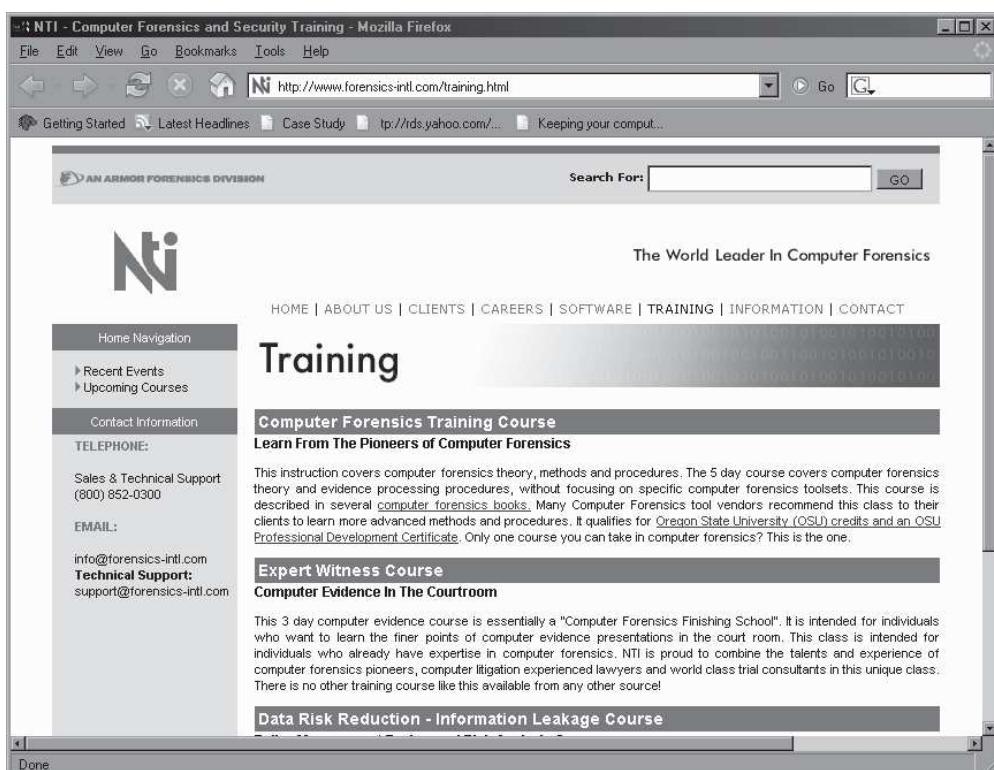
Masih banyak pelatihan dengan berbagai spesifikasi forensik yang dapat Anda temukan dalam berbagai website, lebih lanjut dapat Anda perhatikan pada gambar terakhir Bab 7.

Anda dapat mendapatkan banyak pengetahuan ‘cuma-cuma’ dari berbagai website yang tersebar dalam internet, Anda dapat men-download berbagai format file yang disediakan

atau dengan mengikuti serangkaian tes gratis untuk menguji keahlian komputer Anda.

Training Online

Berikut website training online komputer forensik populer yang dapat Anda eksplorasi lebih dalam.



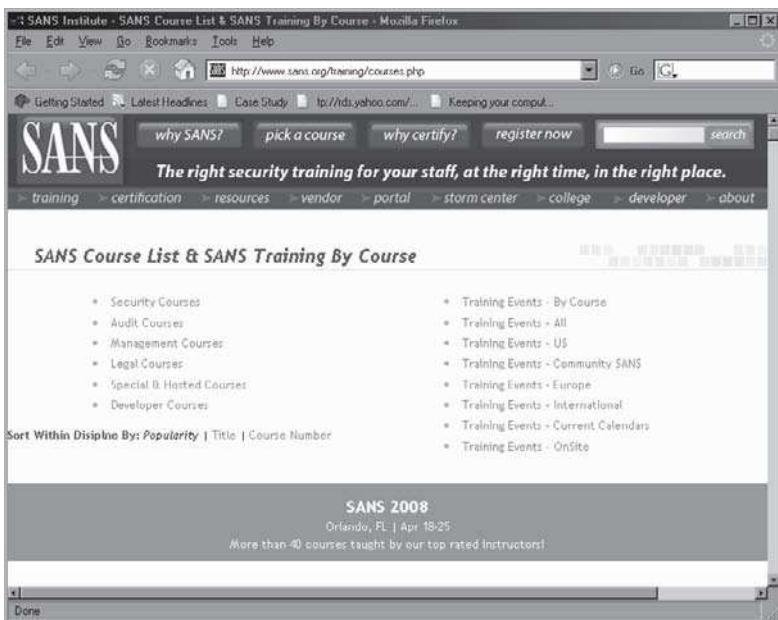
Gambar 7.2 Website NTI – Computer Forensics and Security Training



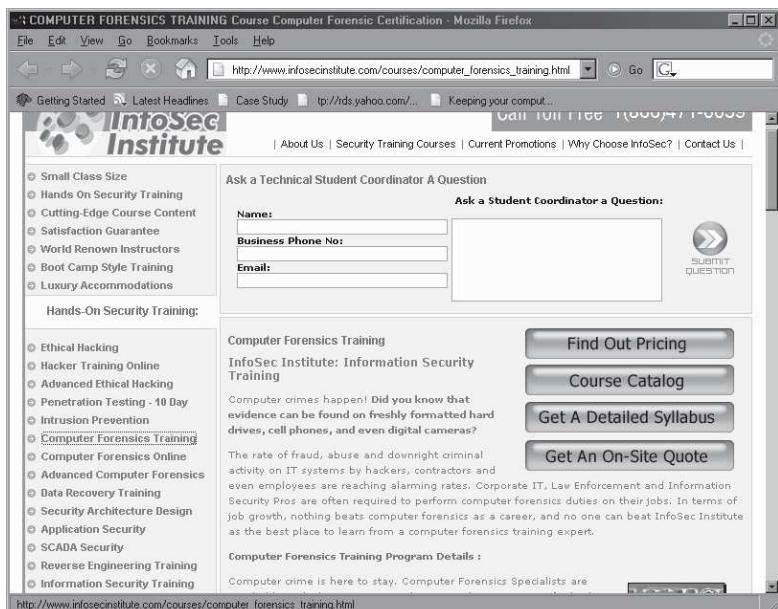
Gambar 7.3 Website NWC3 – National White Collar Crime Center



Gambar 7.4 Website SANS Institute



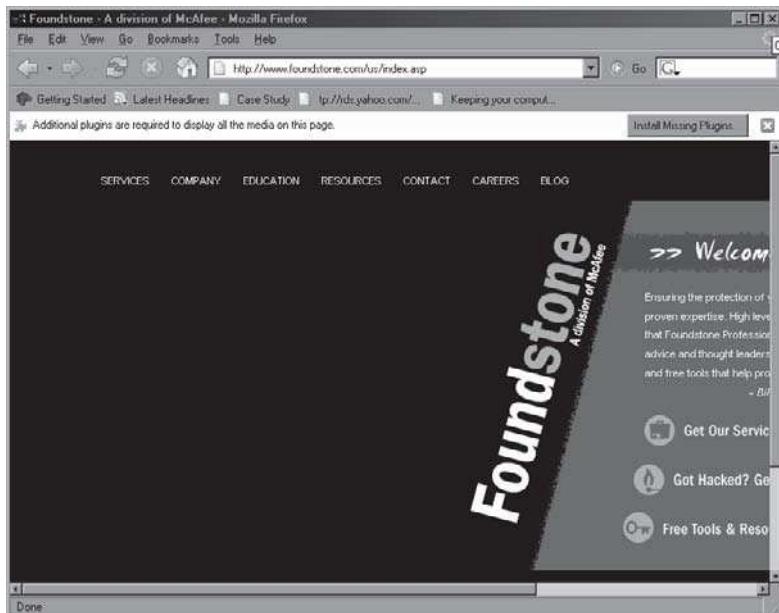
Gambar 7.5 Website SANS Institute – Training by Course



Gambar 7.6 Website InfoSec Institute



Gambar 7.7 Website MIS – Training Institute



Gambar 7.8 Website Foundstone.com

The screenshot shows a Mozilla Firefox browser window displaying the CompuForensics website at <http://www.computorensics.com/training.htm>. The page title is "CompuForensics for Computer Forensics Examiner Training". Below the title is a navigation bar with tabs: HOME, QUESTIONS, SYLLABUS, ANALYSIS, and LINKS. The "QUESTIONS" tab is selected. Underneath the navigation bar are four course options:

- Computer Forensics Examiner Basic Course** (Live On-line)
 - Length: 8 Week (48 hour)
 - Tuition: \$995
 - Included: Books & software
 - Requirements: MS Windows
 - Summary: Prerequisites needed to begin doing forensic analysis of Windows stand-alones as well as clients and servers; includes Internet crime 9 hour option.
- Computer Forensics Examiner 12-Week Course** (Live On-line)
 - Length: 12 Week (72 hour)
 - Tuition: \$1195
 - Included: Books & software
 - Requirements: MS Windows
 - Summary: Best of Basic and Advanced analysis of Windows using Windows inside SuSE Linux) courses; \$300 discount for Basic graduates since 2004.
- Windows & Linux Counter Forensics** (on-site & live on-line)
 - Length: 5 Weeks (20 hours)
 - Tuition: \$995
 - Included: Books & software
 - Requirements: MS Windows
 - Summary: An intermediate user's guide to computer privacy (end user anonymous surfing; partition and file eradication; and encryption).
- Computer Forensics Introduction** (on-site & live on-line)
 - Length: 1 day (8 hours)
 - Tuition: Call
 - Included: Note Guide
 - Requirements: None
 - Summary: An introduction to computer forensics (CF) is intended for managers and staff involved with the market for CF services. Contact for group pricing and scheduling.

A note below the courses states: "CompuForensics courses have become increasingly popular among law enforcement, government intelligence and corporate security professionals. Previously restricted to full-time government employees, our courses are now available to anyone who wants to learn computer forensics."

Gambar 7.9 Website ComputerForensics.com

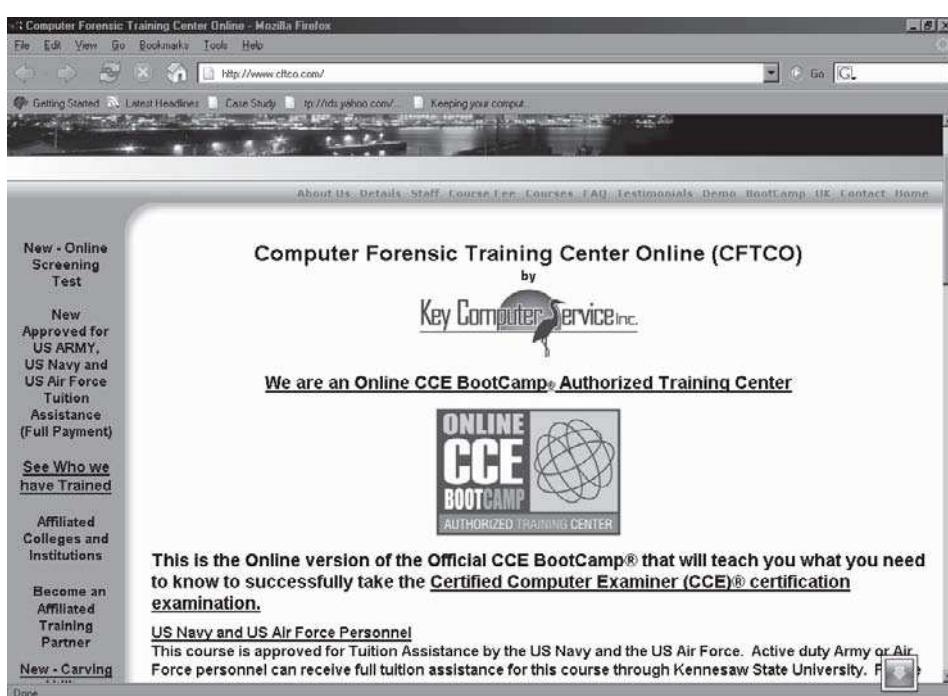
The screenshot shows a Mozilla Firefox browser window displaying the Computer Forensic Services (CFS) website at <http://www.computer-forensic.com/training.html>. The page title is "Training". The main content area features an article titled "Training" by Warren Kruse. The article discusses the benefits of his course, mentioning a humorous reference to past investigative experiences with computer forensics. It also quotes Susan Ballou from NIST and refers to a book by Warren G. Kruse and Jay G. Miller. To the right of the article is a sidebar for "Computer Forensics Incident Response Essentials" by Warren G. Kruse and Jay G. Miller, featuring a thumbnail image of the book cover.

Gambar 7.10 Website ComputerForensics.com - Training

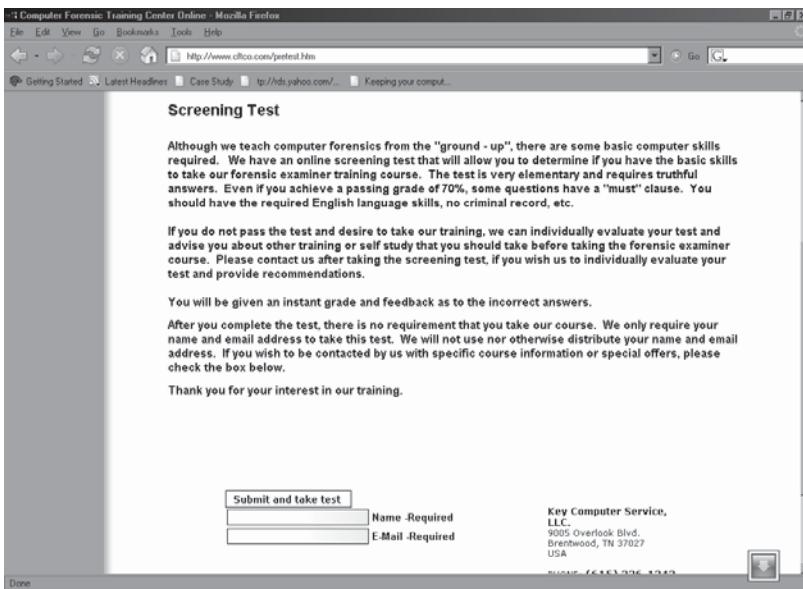
Dalam website yang tertera pada Gambar 7.11, Anda perhatikan salah satu fitur untuk tes gratis komputer forensik, umumnya keahlian yang diujikan mencakup pula penggunaan command-command sistem operasi MS-DOS. Sebelumnya Anda diwajibkan melakukan registrasi (Gambar 7.12 dan Gambar 7.13) dengan memberikan informasi dan

e-mail. Anda dapat mengeksplorasi lebih dalam website tersebut.

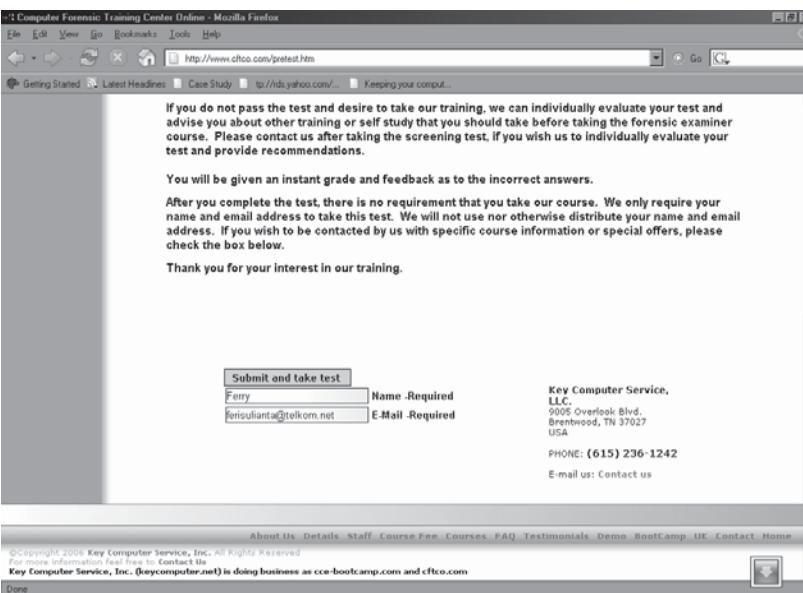
Pada Gambar 7.14 sampai Gambar 7.16 dapat Anda lihat beberapa contoh tes komputer forensik pada website tersebut. Hasil tes akan ditampilkan bagi Anda setelah mengisi semua pertanyaan yang ada. Perhatikan Gambar 7.17.



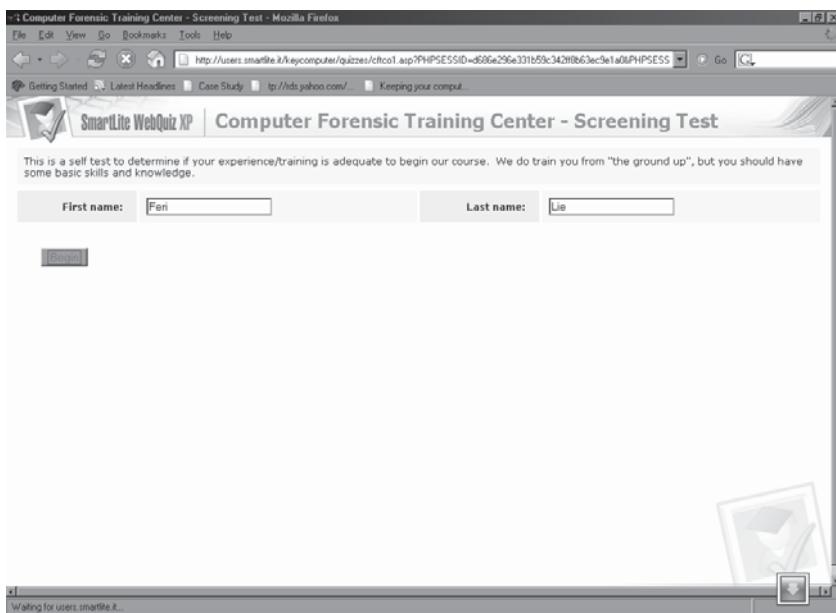
Gambar 7.11 Website Computer Forensic Training Center Online



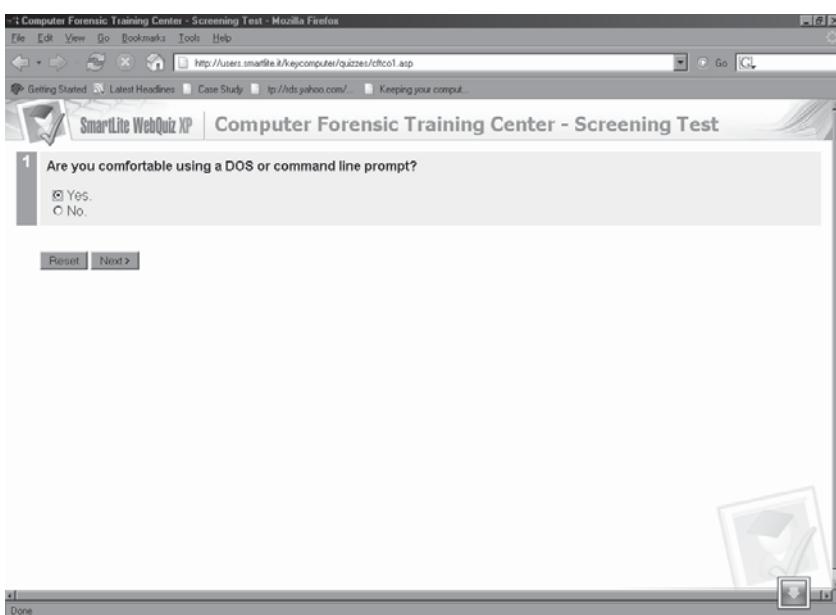
Gambar 7.12 Website Computer Forensic Training Center Online (Screening Test)



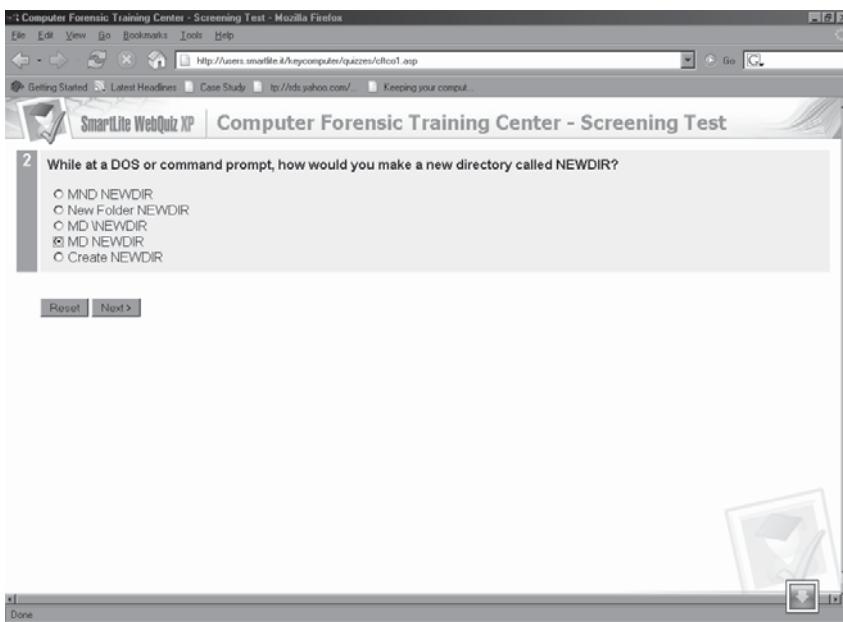
Gambar 7.13 Website Computer Forensic Training Center Online (Submit Test)



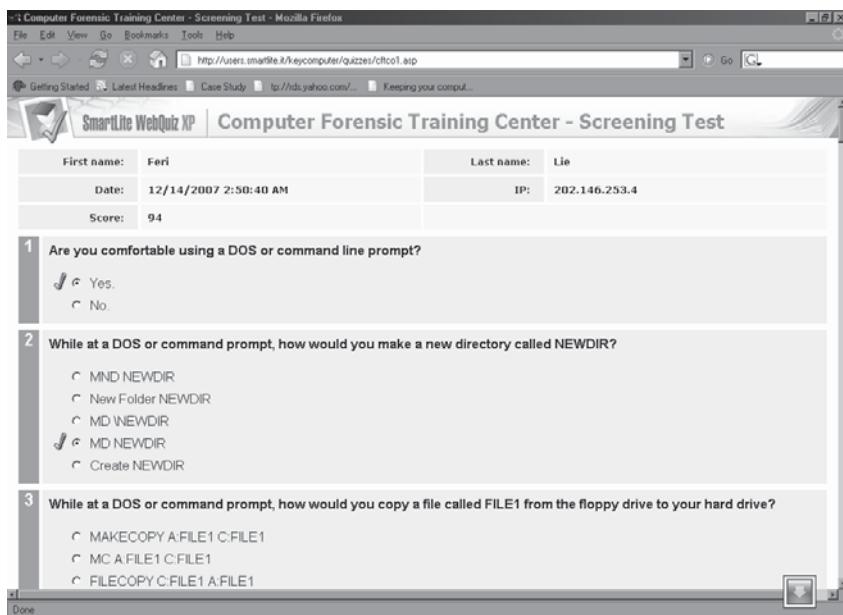
Gambar 7.14 Website Computer Forensic Training Center Online (Cont)



Gambar 7.15 Website Computer Forensic Training Center Online (cont.2)



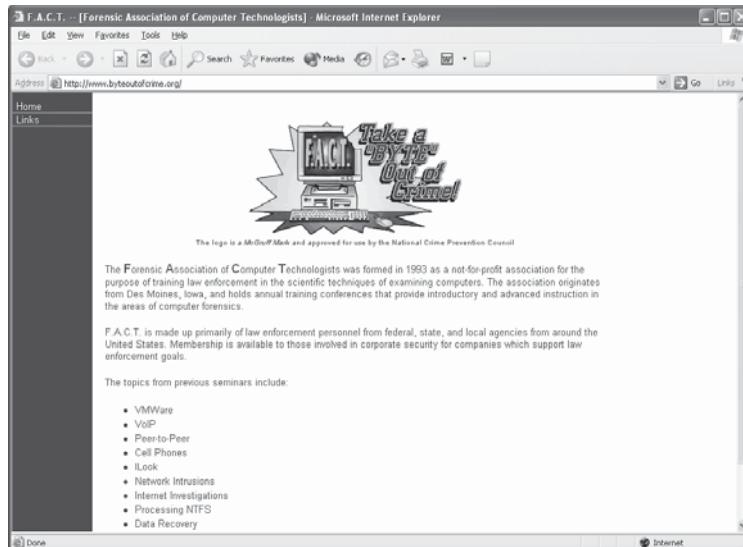
Gambar 7.16 Website Computer Forensic Training Center Online (cont. 3)



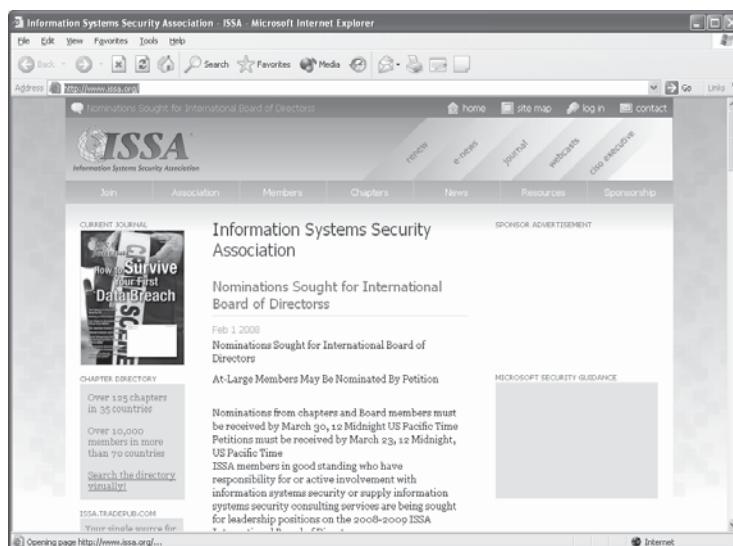
Gambar 7.17 Website Computer Forensic Training Center Online (Hasil Test)

Masih banyak organisasi non-profit, organisasi pemerintahan, ataupun organisasi komersial lain yang me-

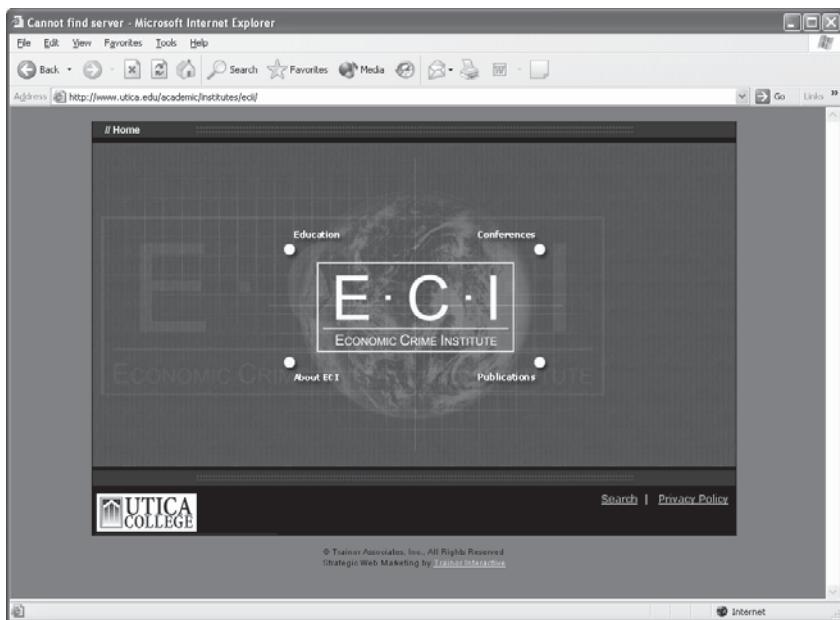
nyediakan layanan training, misalnya dapat Anda perhatikan dalam gambar selanjutnya.



Gambar 7.18 Website The Forensic Association of Computer Technologists



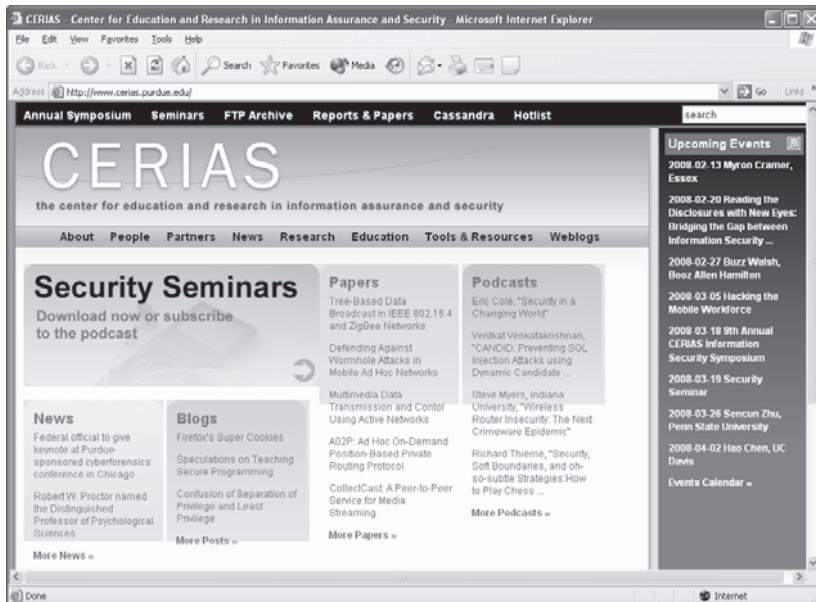
Gambar 7.19 Website Information Systems Security Association



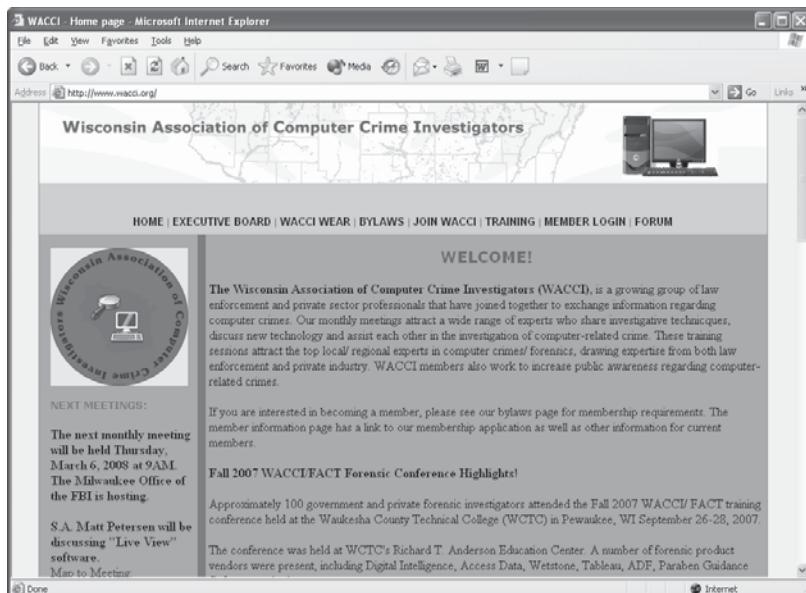
Gambar 7.20 Website <http://www.utica.edu/academic/institutes/ecii/>



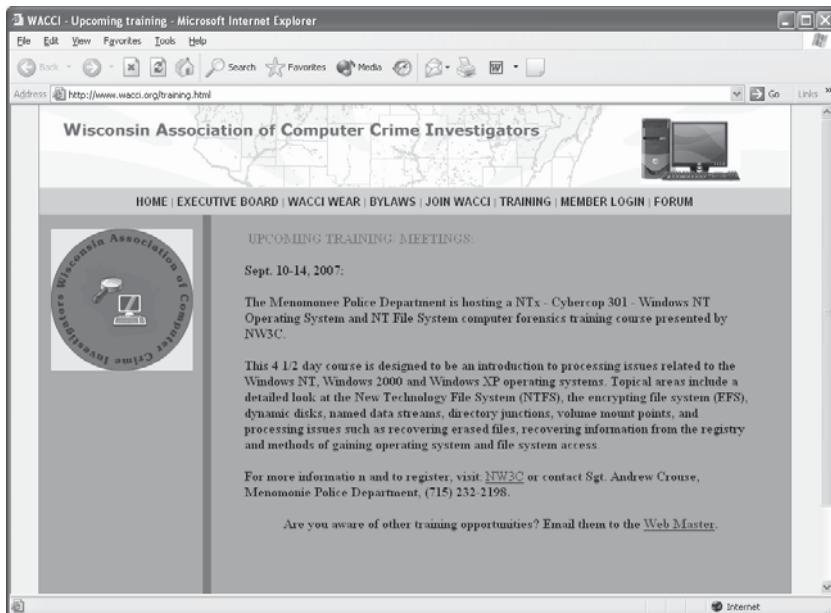
Gambar 7.21 Website The National Center for Forensic Science



Gambar 7.22 Website CERIAS



Gambar 7.23 Website The Wisconsin Association of Computer Crime Investigators (WACCI)



Gambar 7.24 Website The Wisconsin Association of Computer Crime Investigators (WACCI) - Training

Komponen Training Komputer Forensik

Ternyata tidak mudah untuk membuat pelatihan dan layanan training komputer forensik, disamping bidang ini sangat baru dan terus harus mengikuti perkembangan dari perangkat teknologi komputer yang melingkupinya.

Apalagi bukan hal yang mudah untuk menempatkan komputer forensik sejajar dengan bidang forensik lainnya mengingat ketertinggalan dalam segi perkembangan dan kematangan,

meskipun demikian bukan hal yang tidak mungkin untuk mengisi kekosongan dan kebutuhan akan komputer forensik. Ini karena komputer forensik pada dasarnya berangkat dari teknologi komputer dan informasi, dan karakteristiknya umumnya mirip dengan skill spesialis komputer meskipun ada kekhususan tersendiri dan terkait dengan kebutuhan forensik.

Ada beberapa faktor yang perlu dipertimbangkan dalam pelatihan yang akan dibuat/diberikan, ini mengacu pada ketersediaan sumber daya antara lain:

- Peralatan. Ini mencakup keberadaan software dan hardware. Peralatan yang dibutuhkan tentunya bervariasi sejalan dengan kebutuhan training, misalnya saja forensik bagi komputer desktop, forensik terhadap laptop, berbagai media penyimpanan dan backup eksternal, dan lain sebagainya yang tentunya melibatkan pula software forensik khusus.
- Sumber daya manusia. SDM harus mampu dalam membuat modul training yang *up to date*, termasuk pula terus meningkatkan kemampuan mereka.
- Training material yang mencakup pula:
 - ✓ Ruang Lingkup. Material yang diujikan tentunya dispesifikasi sedemikian rupa bergantung pada kebutuhan, misalnya storage device tertentu atau sistem operasi Windows, Linux, dan lainnya.
 - ✓ Trainee yang tergolong baru atau kebutuhan upgrade keahlian.
 - ✓ Macam ragam, misalnya banyaknya kasus yang dipercontohkan dan diujikan.
 - ✓ Permintaan organisasi lain untuk training. Misalnya perusahaan membutuhkan program training terhadap beberapa spesialis informasi, ten-

tunya diperlukan kesiapan dari trainer untuk merombak modul untuk kebutuhan spesifik, penyesuaian kasus dengan kondisi perusahaan *trainee*, atau dibutuhkan usaha lain seperti traveling, dan lainnya.

BAB 8

Suplemen Komputer Forensik

- Kamus Komputer Forensik
- Organisasi yang Menyertakan Komputer Forensik

Kamus Komputer Forensik

A

Alamat: Atau disebut sebagai Address, umumnya digunakan dalam alamat internet, alamat e-mail, alamat web (URL).

Analisis: Langkah ketiga dalam proses komputer forensik, menyangkut pula metode dan teknik yang berkaitan dengan perundangan atau hukum.

Anti forensik: Teknik yang dilakukan untuk menghilangkan data dan fakta sehingga menutup kemungkinan di-dapatkannya fakta dari proses forensik, misalnya menghapus file pada recycle bin dan media penyimpanan lainnya.

B

Best Evidence Rule: berbagai konten mencakup dokumen tertulis, rekaman audio, video, atau foto yang digunakan sebagai bukti.

BIOS: Basic Input Output System.

Bit Stream Imaging: Bit-bit copy dari media orisinalnya, mencakup free space dan slack space. Dikenal pula dengan disk imaging.

C

Cache: Dikenal pula sebagai cache memory/memori penyangga, yang menjadi penyangga dan bagian dari CPU.

Chain of Custody: Penelaahan dari bukti-bukti yang didapat dari sumber yang dikatakan orisinil yang nantinya dimajukan untuk proses hukum.

C/S Arsitektur: arsitektur client/server, salah satu arsitektur jaringan dimana komputer yang difungsikan menjadi server memberikan layanan sumber daya jaringan terhadap komputer client yang terintegrasi.

Cluster: Kumpulan sektor (sector) pada track yang sama.

Collection: Fase pertama dalam komputer forensik, mencakup identifikasi, pelabelan, pencatatan, dan usaha mendapatkan data dari sumber-sumber yang dapat diandalkan dan didasarkan pada panduan dan prosedur yang menghadirkan integritas.

Copy: Penggandaan yang akurat, bentuk dari reproduksi informasi.

Cyberspace: Ruang maya yang dimungkinkan terbentuk dari interkoneksi komputer.

Cyber Crime: Kejahatan dalam dunia cyber. Investigasi yang dilakukan sebagai upaya pencegahan dan

mengalami kejahatan yang menggunakan cyberspace 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.

Denial of Services Attack (DoS Attack): Serangan yang ditujukan pada website, yang mengakibatkan website tidak lagi mampu memberikan layanan, tentunya website tidak dapat dikunjungi user lagi.

Digital Forensic: Pengaplikasian ilmu pengetahuan dalam mengidentifikasi, mengumpulkan, menguji, dan menganalisa data, kemudian menghadirkan informasi yang dapat diandalkan, mencakup pula *chain of custody* data.

Direktori: Metoda pengorganisasian file-file (dikatakan pula sebagai folder).

Disk to Disk Copy: Meng-copy file yang ada pada suatu media secara langsung ke media lain.

Disk to File Copy: Meng-copy file yang ada pada suatu media ke satu data file logika.

Dongle: Berbagai perangkat keras eksternal dan memory disertakan di dalamnya, misalnya: printer laser dengan 8 MB memory terintegrasi.

Duplicate Digital Evidence: Penggandaan akurat dari bukti digital.

F

False Positive: Kesalahan dalam mengklasifikasi kegiatan tidak berbahaya ke dalam tindakan yang dikategorikan *malicious*.

False Negative: Salah dalam mengklasifikasi aktivitas yang tergolong *malicious* sebagai tindakan yang tidak berbahaya.

File Aktif: File yang dialokasikan pada personal komputer, disk drive, server disk drive, 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.

Terkadang file backup dibentuk otomatis oleh perangkat lunak aplikasi dan sistem operasi.

Files: Berbagai data dan informasi yang dikemas dan kemudian disimpan dalam komputer. Lebih lanjut, file-file diorganisasi sedemikian rupa dalam direktori atau folder.

File Allocation Table (FAT): “Peta” yang memungkinkan sistem operasi menyimpan, mengalokasikan, dan mendapatkannya kembali data/informasi pada media penyimpanan (harddisk). Berbagai sistem operasi memiliki penanganan yang berbeda akan media penyimpanan.

File Name: Nama file yang adalah harus unik, mengacu pada suatu file tertentu.

Forensically Clean: Media digital dalam kondisi “bersih” dari berbagai data, bebas malware dan sudah diuji kelayakannya sebelum nantinya digunakan.

Free Space: Area pada media penyimpanan atau pada memori yang tidak terpakai (belum teralokasi).

H

Hersay Evidence: Pernyataan yang mengajukan fakta dan pembuktian kebenaran.

K

Kejahatan Komputer: Lihat Cyber Crime.

Komputer Forensik: Suatu keilmuan yang difungsikan untuk mendapatkan, menyelamatkan data/informasi, dan mendokumentasikan bukti dari berbagai perangkat elektronik, mencakup komputer, pager, PDA, kamera digital, telpon selular, dan berbagai media penyimpanan. Ada tata cara bagaimana itu disajikan dan dikumpulkan sehingga dikatakan layak untuk dimajukan lebih lanjut ke dalam proses hukum.

Komputer Forensik: Suatu metode pengumpulan, penyelamatan informasi, analisa, pengajuan pengadilan berkenaan bukti yang berhubungan dengan komputer, dimana metode demikian dikembangkan karena kebutuhan eksklusif akibat dari berkembangnya abad komputer/abad informasi.

M

Mainframe Architecture: Komputer berkemampuan sangat besar dan diakses melalui terminal-terminal yang tersebar. Mainframe terdahulu hanya menyediakan terminal tanpa kemampuan pemrosesan, lain halnya sekarang, dimana terminal diberikan kemampuan untuk melakukan pemrosesan.

Malware: Malicious software, program berbahaya yang dapat mengganggu dan merusak sistem komputer.

Memory Card: Dikenal dengan flash memory card, digunakan sebagai media penyimpanan yang *removable*. Flash memory tersedia beragam dengan berbagai vendornya: Compact Flash (CF), Smart Media (SM), Memory Stick (MS), MultimediaCard (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, harddisk internal, 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 beberapa komputer yang terintegrasi pada jaringan melalui media komunikasi, misalnya kabel dan nirkabel (wireless).

Non-Printing Information: Informasi yang di-*embeded* pada dokumen elektronik dan tidak disajikan terce-

tak dalam bentuk hardcopy. Misalnya perangkat pengolah kata semisal Microsoft Word atau spreadsheet elektronik semisal Excel memungkinkan Anda menyisipkan informasi (misalnya: komentar, catatan).

Networks: Kombinasi perangkat lunak dan perangkat keras yang memungkinkan komputer yang terintegrasi dapat saling berkomunikasi. Arsitektur network umumnya digolongkan ke dalam dua bagian: Peer-to-Peer dan Client/Server.

Non-Volatile Data: Data yang ada pada komputer dan akan hilang jika listrik dipadamkan.

Normalize: Proses dalam mengkonversi data ke dalam format tertentu yang lebih kompatibel dengan parameter standar yang telah ditetapkan.

O

Operating System (OS): Perangkat lunak kategori software system yang mengendalikan kinerja perangkat keras komputer, sehingga user dapat memanfaatkan sumber daya perangkat keras. Sistem Operasi berada di lapisan atas dari fisik 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 (the transport layer OSI).

Packet Sniffer: Perangkat lunak yang melakukan monitoring terhadap lalu lintas 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 dimana setiap user dengan masing-masing komputernya mengelola file-file miliknya tanpa menajerial terpusat.

Probative Value: Bukti penting yang sangat berguna dalam pemeriksaan.

Prima Facie Evidence: Asumsi yang dianggap layak berkenaan fakta.

Proses: Program yang dieksekusi.

Q

QUERY: Statement yang digunakan sebagai ungkapan untuk pencarian atau pertanyaan, istilah ini mengacu pada proses sewaktu meminta informasi pada basis data, search engine, atau direktori index.

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 harddisk, 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 berarti, mencakup media penyimpanan digital seperti: floppy disk, CD, DVD, cartridge, tape, dan removable media card.

Reporting: Tahap akhir dalam proses komputer forensik, yang mencakup pelaporan hasil analisa, menyangkut pula penjelasan deskriptif terhadap tindakan yang diambil, bagaimana perangkat dan prosedur dipilih, menentukan tindakan lain

yang mungkin dilakukan (forensik terhadap 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 yang dapat diakses.

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. Didistribusikan dan bebas digunakan dengan syarat dan ketentuan berlaku, misalnya untuk keperluan demo dan digunakan dengan rentang waktu terbatas.

Shareware: Software yang bebas digunakan untuk interkoneksi device dan peripheral.

Sistem Komputer: Mencakup sekumpulan ruang lingkup komputer. Secara umum adalah korelasi perangkat keras, perangkat lunak, dan user sebagai pengguna, serta lebih spesifik mengacu pada komputer dan komponen yang terintegrasi, misanya komputer, berbagai device (contoh: printer, modem, media penyimpanan, scanner, dan lainnya) dan jaringan komputer.

System Unit: Adalah CPU (Central Processing Unit). Anda dapat mengalokasikannya pada kotak CPU. Komponen utama di dalamnya terdiri dari prosesor, motherboard, memori komputer, dan berbagai port serta konektor yang memungkinkan.

Slack Space: Bagian yang tidak digunakan pada disk cluster, atau ruang-ruang penyimpanan yang tidak digunakan pada *file allocation block* atau pada memory page yang mungkin berisi data-data residu.

Smart Card: Kartu plastik yang diintegrasikan chip elektronik untuk berbagai keperluan, misalnya kartu identitas.

Subdirectory: Direktori yang berada pada direktori lain.

T

Tape: Pita magnetik yang diperuntukkan sebagai media penyimpanan 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 sebagian 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 mereplikasi 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.

Organisasi yang Menyertakan Komputer Forensik

Federal Bureau of Investigation (FBI)

<http://www.fbi.gov/>



Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice.

<http://www.cybercrime.gov/>

High Technology Crime Investigation Association (HTCIA)

<http://www.htcia.org/>

International Association of Computer Investigative Specialists (IACIS)

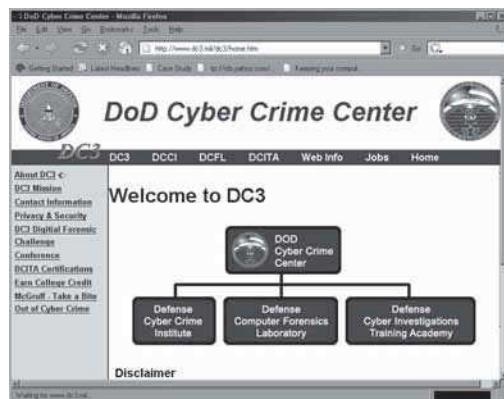
<http://www.cops.org/>

National Law Enforcement and Corrections Technology Center .North East (NLECTC-NE)

<http://www.nlectc.org/nlectcne/>

Regional Computer Forensics Laboratory (RCFL)

<http://www.rcfl.gov/>



SEARCH: National Consortium for Justice Information and Statistics

<http://www.search.org/>



U.S. Department of Defense Cyber Crime Center

<http://www.dc3.mil/dc3/home.htm>

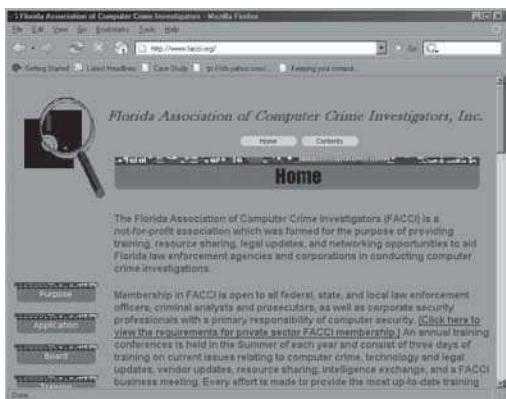
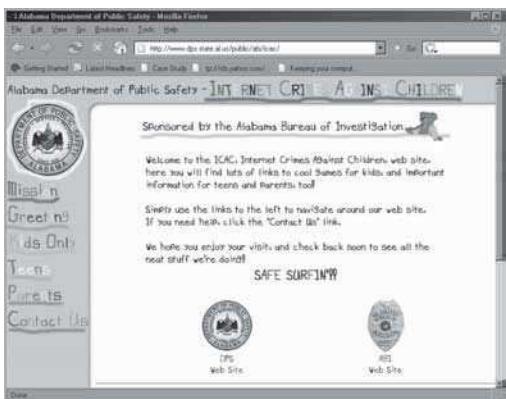
U.S. Secret Service Electronic Crimes Task Force

<http://www.ectaskforce.org/>



Alabama Bureau of Investigation Internet Crimes Against Children Unit

http://www.dps.state.al.us/public/ab_icac/



Phoenix Police Department

<http://www.ci.phoenix.az.us/POLICE>

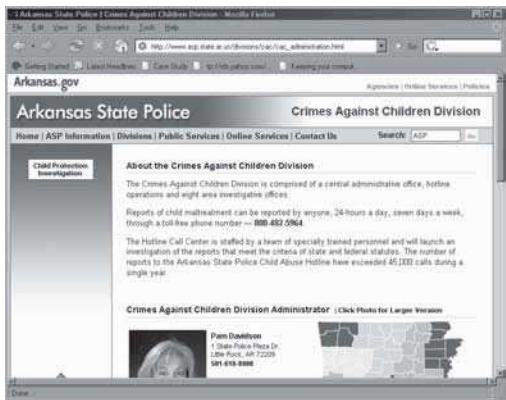


Florida Association of Computer Crime Investigators (FACCI)

<http://www.facci.org/>

Arkansas State Police Crimes Against Children Division

http://www.asp.state.ar.us/divisions/cac/cac_administration.html



Computer and Technology Crime High-Tech Response Team

<http://www.catchteam.org/>



Los Angeles Police Department - Computer Crime Unit

<http://www.lapdonline.org/>



Regional Computer Forensic Laboratory at San Diego

<http://www.rcfl.org>

Sacramento County Sheriff's Office - Internet Crimes Against Children Task Force

<http://www.sachitechcops.org/children.htm>



Connecticut Department of Public Safety - Division of Scientific Services Forensic Science Laboratory Computer Crimes and Electronic Evidence Unit

<http://www.state.ct.us/dps/>



Institute of Police Technology and Management - Computer Forensics Laboratory University of North Florida

<http://www.iptm.org/crim.htm#026119>



New Hampshire State Police Forensic Laboratory - Computer Crimes Unit

<http://www.state.nh.us/safety/infotech/index.html>

New Jersey Regional Computer Forensic Laboratory Office - NJSP Technology Center -

<http://www.njrcfl.org/>



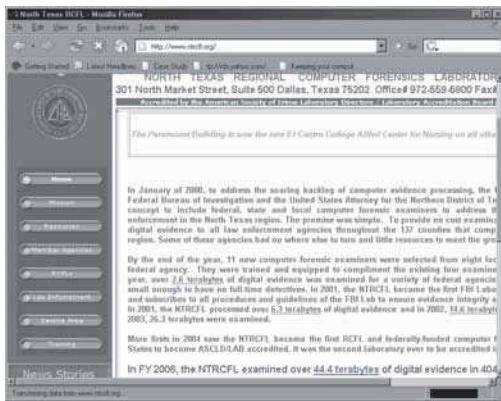
New York State Police - Computer Crime Unit Forensic Investigation Center

http://www.troopers.state.ny.us/Criminal_Investigation/Computer_Crimes/



North Texas Regional Computer Forensic Laboratory Office

<http://www.ntrcfl.org/>



Intermountain West Regional Computer Forensic Laboratory Office

<http://www.iwrcfl.org/>

Utah Department of Public Safety - Criminal Investigations Bureau Forensic Computer Lab

<http://sbi.utah.gov/compforensic/>



King County Sheriff's Office - Fraud/Computer Forensic Unit

http://www.metrokc.gov/sheriff/wha/t_investigations/fraud.aspx



Regional Computer Forensic Laboratory National Program Office - Engineering Research Facility

<http://www.rcfl.gov/>



Daftar Pustaka

Anders Svensson. Computer Forensics Applied to Windows NTFS Computers.3 January 2008.

<<http://www.dsv.su.se/research/seclab/pages/pdf-files/2005-x-268.pdf>>

Antonio Robinson, President Pioneer Technology. Computer and Network Forensics, The First Step Preservation of Evidence Commercial and Litigation support, .1 January 2008.<<http://www.pioneer technology.com/downloads/forensics-presentation.pdf>>

Arne Vidström. Computer Forensics and the ATA Interface.2 January 2008. <<http://www.foi.se/upload/rapporter/foi-computer-forensics.pdf>>

CAL STATE FULLERTON. Certificate in Computer Forensics..1 January 2008.
<<http://www.csufextension.org/ueeimages/Certificates/ComputerForensics.pdf>>

Champlain College.Computer & Digital Forensics.3 January 2008<http://digitalforensics.champlain.edu/CC_Digital_Forensics.pdf>

Chris Malinowski, Computer Science and Management Engineering CW Post, Long Island University.Workshop:Computer Forensics .10 January 2008.<<http://isedj.org/isecon/2006/1122/ISECON.2006.Malinowski.pdf>>

Computer Forensics Consultant Impact Forensics, LLC Chicago, IL.3 January 2008.<http://www.impactforensics.com/pdf/Computer_Forensics_Constant.pdf>

- Computer Forensics Essentials. 3 January 2008.
<http://www.charlesriver.com/resrcs/chapters/1584504056_1stChap.pdf>
- Cornell Walker. Computer Forensics: Bringing the Evidence to Court . 2 January 2008.
<http://infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf>
- Computer Forensics Training, ECC, .3 January 2008.<http://www.strategicintel.com/Computer_Forensic_Pamphlet.pdf>
- Computer Forensics Option, .1 January 2008.
<<http://www.edisonohio.edu/programs/ProgramBrochures/compforen.pdf>>
- Donald Wochna, Esq. Chief Legal Officer, COMPUTER FORENSICS: NON-ADVERSARIAL DISCOVERYSM OF FACTS.10 January 2008.
<<http://www.vestigeltd.com/resources/Non-AdversarialDiscoveryOfFacts.pdf>>
- Dr. Bruce V. Hartley, CISSP, Deloitte Financial Advisory Services LLP, Computer Forensics and Electronic Discovery .3 January 2008.
<<http://www.certconf.org/presentations/2006/files/TC2.pdf>>
- Daphyne Saundres Thomas, James Madison University, Harrisonburg,Virginia, Karen A. Forcht, Utah State University,Logan Utah.Legal Methods of Using Computer Forensics Techniques for Computer Crime Analysis and Investigation.3 January.
<http://www.iacis.org/iis/2004_iis/PDFfiles/ThomasForcht.pdf>
- Dr. Neal Krawetz, Hacker Factor Solutions,Non-Classical Computer Forensics.1 January 2008.<<http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Krawetz.pdf>>
- Dr. Hilton Chan Technology Crime Division Commercial Crime Bureau .How Secure is Secure?.3 January 2008.
<<http://www.e21magicmedia.com.hk/esecurity2002/pdf/closing.pdf>>
- Edmonds Community College. Computer Information Systems Digital Forensics Certificate Program Requirements 2007-2008.3 January 2008. <<http://requirements.edcc.edu/current/506h.pdf>>

Elytra Enterprises . Computer Forensics Inc.3 January 2008.
<http://www.elytra.com/Documents/Elytra_Computer_Forensics.pdf>

eVestigations Inc.Computer Forensics Computer .3 January 2008.
<<http://www.iacwcu.com/powerpoint/IAC Techies Day Presentation.pdf>>

Flashback Data. Computer Forensics Service Agreement..3 January 2008. <<http://www.911forensicdata.com/Forensic Services Agreement 2004.pdf>>

Forentech BEST PRACTICES series. Forensic Lifecycle An effective and repeatable process for computer forensic investigations.1 January 2008.
<<http://www.forentech.com/documents/ForensicLifeCycleWhitePaper.pdf>>

Hall Dillon, A career in forensic, .3 January.
<<http://www.bls.gov/opub/ooq/1999/Fall/art01.pdf>>

International Council of E-Commerce Consultants.CyberLaw..3 January 2008<<http://www.eccouncil.org/docs/CyberLaw.pdf>>

ISEMARKET Consultancy and developments Ltd, Computer Forensics Toolkit v 1.0.0.1, .10 January 2008.<<http://www.jaguarsoft.com/pdf/JaguarForensics.pdf>>

Jerry Grant, Acting Chief, National IT LAN Application and Policy Support Team

& Troy Schnack, CSA, Western District of Missouri. Computer Forensics..2 January 2008.
<http://www.fd.org/pdf_lib/ComLitCompForensics.pdf>

Jim Lyle and Doug White Information Technology Laboratory. Computer Forensics:

Tool Testing & National Software Reference Computer Forensics: Computer Forensics:

Tool Testing Tool Testing & National Software Reference National Software Reference Library. 3 January 2008.
<<http://www.nsrl.nist.gov/documents/techno2003/cftt-nsrl-techno.pdf>>

LAKE WASHINGTON TECHNICALCOLLEGE, Information Assurance & Computer Forensics, .3 January.
<<http://www.lwtc.edu/future/programs/list/iacf.pdf>>

LLC Chicago, IL.Computer Forensics Technician Impact Forensics. 3 January 2008.<<http://www.impactforensics.com/pdf/ComputerForensicsTechnician.pdf>>

Linda Volonino. Information Systems and Telecommunications Canisius College, Electronic Evidence and Computer Forensics.3 January 2008. <<http://cais.isworld.org/articles/12-27/article.pdf>>

MANDIANT COMPUTER FORENSICS - Intelligent Information Security.3 January 2008.<<http://www.mandiant.com/documents/MANDIANTComputerForensicsDatasheet.pdf>>

Matthew Meyers and Marc Rogers,CERIAS ,Purdue University. Computer Forensics: The Need for Standardization and Certification.1 January 2008
<http://media.wiley.com/product_data/excerpt/67/07645263/0764526367.pdf>

MIAMI VALLEY REGIONAL CRIME LABORTORY. 1 January 2008
<http://miamivalleyrcfl.org/Downloads/Documents/MVRCFL_ServiceRequest.doc>

MIAMI VALLEY REGIONAL CRIME LABORTORY. 1 January 2008
<<http://miamivalleyrcfl.org/Downloads/Documents/LabSheetnew.pdf>>

MIAMI VALLEY REGIONAL CRIME LABORTORY. Recommended Guidelines for Computer Forensic Analysis Evidence Submission.1 January 2008
<<http://miamivalleyrcfl.org/Downloads/Documents/guidelines.pdf>>

Mile 2 - IT Security Training. Computer Forensics & Electronic Discovery.3 January 2008.<http://www.mile2.com/CFTB_Computer_Forensics_Training_Bootcamp.pdf>

Netlingo.List of File Extensions.10 February 2008.<<http://www.netlingo.com/more/fileextensions.cfm>>

Northumbria University.Computer Forensics Workshop - Consideration of Computer Ethics in Computer Forensics Alastair Irons Northumbria University.3 January.
<http://www.ics.heacademy.ac.uk/events/presentations/71_ComputerForensicsWorkshop-Ethics.ppt>

Orin S. Kerr. SEARCHES AND SEIZURES IN A DIGITAL WORLD.3 January
2008<<http://www.harvardlawreview.org/issues/119/Dec05/Kerr.pdf>>

Lisa Oseles . Computer Forensics: The Key to Solving the Crime. 3 January
2008.<http://faculty.ed.umuc.edu/~meinkej/inss690/oseles_2.pdf>

Overview of Computer Forensics Technology, .3 January
2008.<http://www.charlesriver.com/resrcs/chapters/1584503890_1stCap.pdf>

Panell Kerr Forster of Texas, P.C. Computer Forensics - go behind the screen to investigation , .3 January 2008.

<<http://www.pkftexas.com/images/pkf/Documents/FullMagVol4Iss3.pdf>>

Peter Davies - 05004306 MSc Information Security & Computer Crime, Forensic Analysis of the Windows Registry .10 January 2008.
<http://pkdavies.co.uk/documents/Computer_Forensics/registry_examination.pdf>

Pueblo High-Tech Crimes Unit. Computer Forensics Processing Checklist..10 January 2008.<http://crime-research.org/library/Computer_Forensics_Processing_Checklist.pdf>

Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits.First Responders

Guide to Computer Forensics.1 January 2008.
<http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf>

RARITAN VALLEY COMMUNITY COLLEGE

COURSE OUTLINE.CISY-274 – Privacy, Ethics & Computer Forensics.2 January. <http://www.raritanval.edu/course_outlines/CISY274.pdf>

Scott Stevens,Forensics Early to Find the Smoking Gun.2 January 2008.

<http://www.dataforensics.com/articles/deploy_computer_forensics_early.pdf>

Simson L. Garfinkel,Forensic Corpora: A Challenge for Forensic Research.10 January 2008.<http://www.simson.net/ref/2007/Forensic_Corpora.pdf>

Simson L. Garfinkel ,Computer Science and Artificial Intelligence Laboratory, Remembrance of Data Passed: Used Disk Drives and Computer Forensics.10 January 2008.<<http://www.usenix.org/events/lisa04/tech/talks/garfinkel.pdf>>

Technology Administration I.S. Dept. of Commerce.Guide to Integrating Forensic Techniques into Incident Response, NIST National Institute of Standard and Technology. 10 January 2008.<<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>>

THE IEEE COMPUTER SOCIETY. Computer Forensics Education..3 January 2008.<<http://www.cs.albany.edu/~erbacher/publications/ForensicsEducationPaper.pdf>>

U.S. Department of Justice Office of Justice Programs National Institute of Justice. Forensic Examination of Digital Evidence: Guide for Law Enforcement..1 January 2008.
<<http://www.ncjrs.org/pdffiles1/nij/199408.pdf>>

Minutiae.Computer Computer Forensics..1 January 2008.
<<http://www.redwop.com/minutiae/min80.pdf>>

U.S. Department of Justice Office of Justice Programs National Institute of Justice, Investigations Involving the Internet and Computer Networks.2 January 2008.
<<http://www.ncjrs.gov/pdffiles1/nij/210798.pdf>>

U.S. Department of Justice Office of Justice Programs National Institute of Justice. Electronic Crime Scene Investigation.A Guide for First Responders.1 January 2008.
<<http://www.ncjrs.gov/pdffiles1/nij/187736.pdf>>

Veritect, Inc. What Lawyers and Managers Should Know About Computer Forensics..2 January 2008.
<http://isis.poly.edu/kulesh/forensics/comp_forensics.pdf>

Warren G. Kruse II, CISSP, CFCE. Computer Forensics "Top 10 List" - Things to avoid.1 January 2008. <http://www.computer-forensic.com/old_site/presentations/Info_Security.pdf>

Tentang Penulis



Feri Sulianta bekerja sebagai Manajer IT di salah satu perusahaan swasta dan dosen di salah satu perguruan tinggi swasta bidang Informatika. Beliau mendapatkan gelar Sarjana Teknik Jurusan Teknik Informatika Fakultas Teknik Industri, Universitas Gunadarma pada tahun 2001.

Berbagai aktivitas yang pernah dilakukan antara lain mengadakan seminar IT, aktif dalam komunitas programmer, membuat diktat, serta menulis jurnal dan buku-buku IT. Spesialisasi dan bidang-bidang yang diminatinya: Database Programming, IT dengan konsep korelasi Sosial Masyarakat dan Bisnis, serta Manajemen dan Administrasi Informasi.

Penulis dapat dihubungi melalui email ferisulianta@telkom.net

Buku komputer hasil karya Feri Sulianta:

ID	JUDUL	PENULIS	HARGA
121071972	Seri Referensi Praktis: Konten Internet	Feri Sulianta	39,800
121080441	Seri Referensi Praktis: Manajemen IT	Feri Sulianta	44,800

Buku-buku komputer terbaru PT Elex Media Komputindo:

ID	JUDUL	PENULIS	HARGA
121080624	Build and Hack Your Blogger Now!	Adam Pahlevi Baihaqi	34,800
121080661	101 Tip & Trik Photoshop CS3	Dominikus Juju & MataMaya Studio	32,800
121080663	Most Wanted Blogging Tips	Ridwan Sanjaya	24,800
121080592	20 Aplikasi Portable Paling Dicari!	Jubilee Enterprise	42,800
121080601	101 Tip & Trik Hotmail dan Yahoo Mail	Jubilee Enterprise	26,800
121080534	Education Game with Flash 8.0 + CD	Wirawan Istiono, S.Kom	38,800
121080512	Redesigning Joomla Template + CD	Adhicipta R. Wirawan	44,800
121080513	Seri Penuntun Praktis Data Recovery	Dominikus Juju & MataMaya Studio	23,800
121080420	Koleksi Program VB 6.0 Konsep ADO untuk Tugas Akhir dan Skripsi + CD	Uus Rusmawan	54,800
121080481	Teknik Menjebol Password untuk Pemula	Dominikus Juju & MataMaya Studio	41,800
121080421	Desain Presentasi Cantik dengan Photoshop CS3 & PowerPoint 2007 + CD	Jubilee Enterprise	56,800

Catatan:

- ✓ Untuk melakukan pemesanan, hubungi Layanan Langsung Elex Media, telp. (021) 5851473-1474, email: desy@elexmedia.co.id, wisnu@elexmedia.co.id
- ✓ Harga di atas dapat berubah sewaktu-waktu tanpa pemberitahuan terlebih dahulu.

KOMPUTER FORENSIK

Meskipun komputer sudah menjadi kebutuhan fundamental manusia dalam berkegiatan, ternyata masih banyak bidang lain yang miskin pengalaman dalam menangani komputer, salah satunya dalam bidang investigasi — Komputer Forensik.

Diharapkan buku ini mampu menjembatani kebutuhan yang ada berkenaan investigasi yang melibatkan teknologi informasi dengan metode serta komputer sains. Disamping membuka wawasan masyarakat secara umum dan penegak hukum serta profesional IT secara khusus, buku ini akan menarik karena berisi ilmu kombinasi baru, metode, penggagas, penalaran, dan penyampaian deskriptif yang akan berguna pula bagi masyarakat umum dalam memanfaatkan dan menangani IT/komputer dengan pemahaman yang lebih baik.

Materi utama yang disajikan dalam buku ini:

- ◊ Apa sebenarnya komputer forensik, korelasinya dengan teknologi komputer dan keilmuan forensik yang lain.
- ◊ Berbagai proses, metode, pola pikir, dan pemahaman yang mendasari komputer forensik.
- ◊ Cara Anda memandang sumber daya komputer, mencakup data yang tersebar dalam sistem komputer, serta penanganan evidence yang melibatkan peralatan fisik pada umumnya dan berbagai software forensik toolkit!

Kelompok

Internet

Ketrampilan

- Tingkat Pemula
- Tingkat Menengah
- Tingkat Mahir

Jenis Buku

- Referensi
- Tutorial
- Latihan

ISBN 978-979-27-2771-5



9 78979 2727715

EMK121080994

Penerbit PT Elex Media Komputindo

Jl Palmerah Selatan 22

Jakarta 10270

Telp. (021) 5483008 ext. 3323

Web Page: <http://www.elexmedia.co.id>