Etika dan Profesionalisme TSI - IT Forensik

Audit teknologi informasi (Inggris: *information technology (IT) audit atau information systems (IS) audit*) adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis. Pada mulanya istilah ini dikenal dengan audit pemrosesan data elektronik, dan sekarang **audit teknologi informasi** secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu. Istilah lain dari audit teknologi informasi adalah **audit komputer** yang banyak dipakai untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya.

Jejak audit atau log audit adalah urutan kronologis catatan audit, yang masing-masing berisi bukti langsung yang berkaitan dengan dan yang dihasilkan dari pelaksanaan suatu proses bisnis atau fungsi sistem.

Catatan Audit biasanya hasil dari kegiatan seperti transaksi atau komunikasi oleh orang-orang individu, sistem, rekening atau badan lainnya. Audit IT sendiri berhubungan dengan berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science. Audit IT bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan keutuhan (integrity) dari sistem informasi organisasi yang bersifat online atau real time.

Audit trail sebagai "yang menunjukkan catatan yang telah mengakses sistem operasi komputer dan apa yang dia telah dilakukan selama periode waktu tertentu".

Dalam telekomunikasi, istilah ini berarti catatan baik akses selesai dan berusaha dan jasa, atau data membentuk suatu alur yang logis menghubungkan urutan peristiwa, yang digunakan untuk melacak transaksi yang telah mempengaruhi isi record. Dalam informasi atau keamanan komunikasi, audit informasi berarti catatan kronologis kegiatan sistem untuk memungkinkan rekonstruksi dan pemeriksaan dari urutan peristiwa dan / atau perubahan dalam suatu acara.

Dalam penelitian keperawatan, itu mengacu pada tindakan mempertahankan log berjalan atau jurnal dari keputusan yang berkaitan dengan sebuah proyek penelitian, sehingga membuat jelas langkah-langkah yang diambil dan perubahan yang dibuat pada protokol asli.

Dalam akuntansi, mengacu pada dokumentasi transaksi rinci mendukung entri ringkasan buku. Dokumentasi ini mungkin pada catatan kertas atau elektronik.

Proses yang menciptakan jejak audit harus selalu berjalan dalam mode istimewa, sehingga dapat mengakses dan mengawasi semua tindakan dari semua pengguna, dan user normal tidak bisa berhenti / mengubahnya. Selanjutnya, untuk alasan yang sama, berkas jejak atau tabel database dengan jejak tidak boleh diakses oleh pengguna normal.

Dalam apa yang berhubungan dengan audit trail, itu juga sangat penting untuk mempertimbangkan isu-isu tanggung jawab dari jejak audit Anda, sebanyak dalam kasus sengketa, jejak audit ini dapat dijadikan sebagai bukti atas kejadian beberapa.

Perangkat lunak ini dapat beroperasi dengan kontrol tertutup dilingkarkan, atau sebagai sebuah 'sistem tertutup, "seperti yang disyaratkan oleh banyak perusahaan ketika menggunakan sistem Audit Trail.

Ada beberapa pendapat mengenai **real time audit (RTA)** dari dua sumber yang saya dapatkan. Ada yang mengartikan real time audit merupakan suatu sistem yang berfungsi untuk mengawasi kegiatan teknis dan keuanagan sehingga dapat memberikan penilaian yang transparan status saat ini dari semua kegiatan, di mana pun mereka berada. Ada juga yang berpendapat bahwa real time audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal secara online atau bisa dikatakn real time bisa disamakan dengan audit IT lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer.

Cara kerja Audit Trail

Audit Trail yang disimpan dalam suatu table

1. Dengan menyisipkan perintah penambahan record ditiap query Insert, Update dan Delete
2. Dengan memanfaatkan fitur trigger pada DBMS. Trigger adalah kumpulan SQL statement, yang secara otomatis menyimpan log pada event INSERT, UPDATE, ataupun DELETE pada sebuah tabel.

Fasilitas Audit Trail

Fasilitas Audit Trail diaktifkan, maka setiap transaksi yang dimasukan ke Accurate, jurnalnya akan dicatat di dalam sebuah tabel, termasuk oleh siapa, dan kapan. Apabila ada sebuah transaksi yang di-edit, maka jurnal lamanya akan disimpan, begitu pula dengan jurnal barunya.

Hasil Audit Trail

Record Audit Trail disimpan dalam bentuk, yaitu :

1. Binary File – Ukuran tidak besar dan tidak bisa dibaca begitu saja
2. Text File – Ukuran besar dan bisa dibaca langsung
3. Tabel.

Tools yang Digunakan Untuk IT Audit

Tool-Tool Yang Dapat Digunakan Untuk Mempercepat Proses Audit Teknologi Informasi, antara lain:

1.ACL

ACL (Audit Command Language) merupakan sebuah software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber. http://www.acl.com/

2.Picalo

Picalo merupakan sebuah software CAAT (Computer Assisted Audit Techniques) seperti halnya ACL yang dapat dipergunakan untuk menganalisa data dari berbagai macam sumber. http://www.picalo.org/

3.Powertech Compliance Assessment

Powertech Compliance Assessment merupakan automated audit tool yang dapat dipergunakan untuk mengaudit dan mem-benchmark user access to data, public authority to libraries, user security, system security, system auditing dan administrator rights (special authority) sebuah server AS/400. http://www.powertech.com/

4.Nipper

Nipper merupakan audit automation software yang dapat dipergunakan untuk mengaudit dan mem-benchmark konfigurasi sebuah router. http://sourceforge.net/projects/nipper/

5.Nessus

Nessus merupakan sebuah vulnerability assessment software. http://www.nessus.org/

6.Metasploit

Metasploit Framework merupakan sebuah penetration testing tool. http://www.metasploit.com/

7.NMAP

NMAP merupakan open source utility untuk melakukan security auditing. http://www.insecure.org/nmap/

8.Wireshark

Wireshark merupakan network utility yang dapat dipergunakan untuk meng-capture paket data yang ada di dalam jaringan komputer. http://www.wireshark.org/

IT Forensik

Keamanan komputer merupakan hal yang menarik untuk disimak. Perkembangan dunia IT yang sangat cepat telah melahirkan dimensi lain dari teknologi, yaitu kejahatan dengan peran computer sebagai alat utamanya. Istilah yang populer untuk modus ini disebut dengan *cybercrime*.

Adanya kecenderungan negative dari teknologi computer tersebut telah memunculkan berbagai permasalahan baru, baik secara *mikro* karena hanya berefek pada tingkatan personal/perseorangan, sampai kepada persoalan *makro* yang memang sudah pada wilayah komunal, publik, serta memiliki *efek domino* kemana-mana. Untuk negara yang sudah maju dalam IT-nya, pemerintahan setempat atau Profesional swasta bahkan telah membentuk polisi khusus penindak kejahatan yang spesifik menangani permasalahan-permasalahan ini. Cyber Police adalah polisi cyber yang diberikan tugas untuk menindak pelaku-pelaku kriminalitas di dunia cyber, yang tentu saja agak sedikit berbeda dengan polisi 'konvensional', para petugas ini memiliki kemampuan dan perangkat khusus dalam bidang komputerisasi. Sejarah IT

Perkembangan IT bermula apabila Generasi Komputer Digital wujud. Generasi pertama wujud pada tahun 1951-1958. Pada ketika itu tiub vakum telah digunakan sebagai elemen logik utama. Input terhadap komputer menggunakan kad tebuk dan data disimpan dengan menggunakan storan luaran. Storan dalamannya pula menggunakan drum magnetik. Aturcara ditulis dalam bahasa mesin dan bahasa himpunan.

Generasi Kedua (1959-1963) menggantikan tiub vakum dengan transistor sebagai elemen logik utama. Pita magnetik dan cakera pula telah menggantikan kat tebuk dan bertindak sebagai peralatan storan luaran. Bahasa pengaturcaraan aras tinggi digunakan untuk membuat aturcara seperti FORTRAN dan COBOL.

Transistor pula telah digantikan dengan litar bersepadu pada era Generasi Ketiga (1964-1979). Pita magnetik dan cakera menggantikan kad tebuk sepenuhnya dan ingatan metal oksida semikonduktur (MOS) diperkenalkan. Bahasa lebih tinggi telah dibangunkan seperti BASIC.

Komputer Generasi Keempat seperti hari ini menggunakan litar bersepadu berskala (LSI dan VLSI). Mikroprosessor mengandungi litar ingatan, logik dan kawalan direka dalam satu cip sahaja. Komputer

pribadi mula diperkenalkan oleh Apple (1984) dan IBM (1981) untuk kegunaan di rumah. Sistem pengoperasian MS-DOS digunakan secara meluas. Bahasa pengaturcaraan generasi keempat yang dibangunkan adalah seperti Visual C++ dan Visual Basic dengan ciri-ciri pengguna antaramuka bergrafik

Untuk Menganalisis Barang Bukti dalam Bentuk Elektronik atau Data seperti :

• NB/Komputer/Hardisk/MMC/CD/Camera Digital/Flash Disk dan SIM Card/HP

• Menyajikan atau menganalisis Chart Data Komunikasi Target

• Menyajikan atau Analisis Data isi SMS Target dari HP

• Menentukan Lokasi/Posisi Target atau Maping

• Menyajikan Data yg ada atau dihapus atau Hilang dari Barang Bukti Tersebut
Data atau barang bukti tersebut diatas diolah dan dianalisis menggunakan software dan alat khusus untuk dimulainya IT Forensik, Hasil dari IT Forensik adalah sebuah Chart data Analisis komunikasi data Target.

Berikut prosedur forensik yang umum di gunakan antara lain :

1. Membuat copies dari keseluruhan log data, files, daln lain-lain yang dianggap perlu pada media terpisah

2. Membuat finerptint dari data secara matematis.

3. Membuat fingerprint dari copies secvara otomatis.

4. Membuat suatu hashes masterlist

5. Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan.

Sedangkan menurut metode Search dan Seizure adalah :

1. Identifikasi dan penelitian permasalahan.
2. Membaut hipotesa.
3. Uji hipotesa secara konsep dan empiris.
4. Evaluasi hipotesa berdasarkan hasil pengujian dan pengujian ulang jika hipotesa tersebut jauh dari apa yang diharapkan.
5. Evaluasi hipotesa terhadap dampak yang lain jika hipotesa tersebut dapat diterima.

Sejarah IT Forensik

Barang bukti yang berasal dari komputer telah muncul dalam persidangan hampir 30 tahun. Awalnya, hakim menerima bukti tersebut tanpa melakukan pembedaan dengan bentuk bukti lainnya. Sesuai dengan kemajuan teknologi komputer, perlakuan serupa dengan bukti tradisional menjadi ambigu. *US Federal Rules of Evidence* 1976 menyatakan permasalahan tersebut sebagai masalah yang rumit. Hukum lainnya yang berkaitan dengan kejahatan komputer:

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

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

Tools dalam Forensik IT

1. Antiword

Antiword merupakan sebuah aplikasi yang digunakan untuk menampilkan teks dan gambar dokumen Microsoft Word. Antiword hanya mendukung dokumen yang dibuat oleh MS Word versi 2 dan versi 6 atau yang lebih baru.

2. Autopsy

The Autopsy Forensic Browser merupakan antarmuka grafis untuk tool analisis investigasi diginal perintah baris The Sleuth Kit. Bersama, mereka dapat menganalisis disk dan filesistem Windows dan UNIX (NTFS, FAT, UFS1/2, Ext2/3).

3. Binhash

Binhash merupakan sebuah program sederhana untuk melakukan hashing terhadap berbagai bagian file ELF dan PE untuk perbandingan. Saat ini ia melakukan hash terhadap segmen header dari bagian header segmen obyek ELF dan bagian segmen header obyekPE.

4. Sigtool

Sigtcol merupakan tool untuk manajemen signature dan database ClamAV. sigtool dapat digunakan untuk rnenghasilkan checksum MD5, konversi data ke dalam format heksadesimal, menampilkan daftar signature virus dan build/unpack/test/verify database CVD dan skrip update.

5. ChaosReader

ChaosReader merupakan sebuah tool freeware untuk melacak sesi TCP/UDP/… dan mengambil data aplikasi dari log tcpdump. la akan mengambil sesi telnet, file FTP, transfer HTTP (HTML, GIF, JPEG,…), email SMTP, dan sebagainya, dari data yang ditangkap oleh log lalu lintas jaringan. Sebuah file index html akan tercipta yang berisikan link ke seluruh detil sesi, termasuk program replay realtime untuk sesi telnet, rlogin, IRC, X11 atau VNC; dan membuat laporan seperti laporan image dan laporan isi HTTP GET/POST.

6. Chkrootkit

Chkrootkit merupakan sebuah tool untuk memeriksa tanda-tanda adanya rootkit secara lokal. la akan memeriksa utilitas utama apakah terinfeksi, dan saat ini memeriksa sekitar 60 rootkit dan variasinya.

7. Dcfldd

Tool ini mulanya dikembangkan di Department of Defense Computer Forensics Lab (DCFL). Meskipun saat ini Nick Harbour tidak lagi berafiliasi dengan DCFL, ia tetap memelihara tool ini.

8. Ddrescue

GNU ddrescue merupakan sebuah tool penyelamat data, la menyalinkan data dari satu file atau device blok (hard disc, cdrom, dsb.) ke yang lain, berusaha keras menyelamatkan data dalam hal kegagalan pembacaan. Ddrescue tidak memotong file output bila tidak diminta. Sehingga setiap kali anda menjalankannya kefile output yang sama, ia berusaha mengisi kekosongan.

9. Foremost

Foremost merupakan sebuah tool yang dapat digunakan untuk me-recover file berdasarkan header, footer, atau struktur data file tersebut. la mulanya dikembangkan oleh Jesse Kornblum dan Kris Kendall dari the United States Air Force Office of Special Investigations and The Center for Information Systems Security Studies and Research. Saat ini foremost dipelihara oleh Nick Mikus seorang Peneliti di the Naval Postgraduate School Center for Information Systems Security Studies and Research.

10. Gqview

Gqview merupakan sebuah program untuk melihat gambar berbasis GTK la mendukung beragam format gambar, zooming, panning, thumbnails, dan pengurutan gambar.

11. Galleta

Galleta merupakan sebuah tool yang ditulis oleh Keith J Jones untuk melakukan analisis forensic terhadap cookie Internet Explorer.

12. Ishw

Ishw (Hardware Lister) merupakan sebuah tool kecil yang memberikan informasi detil mengenai konfigurasi hardware dalam mesin. la dapat melaporkan konfigurasi memori dengan tepat, versi firmware, konfigurasi mainboard, versi dan kecepatan CPU, konfigurasi cache, kecepatan bus, dsb. pada sistem t>MI-capable x86 atau sistem EFI.

13. Pasco

Banyak penyelidikan kejahatan komputer membutuhkan rekonstruksi aktivitas Internet tersangka. Karena teknik analisis ini dilakukan secara teratur, Keith menyelidiki struktur data yang ditemukan dalam file aktivitas Internet Explorer (file index.dat). Pasco, yang berasal dari bahasa Latin dan berarti “browse”, dikembangkan untuk menguji isi file cache Internet Explorer. Pasco akan memeriksa informasi dalam file index.dat dan mengeluarkan hasil dalam field delimited sehingga dapat diimpor ke program spreadsheet favorit Anda.

14. Scalpel

Scalpel adalah sebuah tool forensik yang dirancang untuk mengidentifikasikan, mengisolasi dan merecover data dari media komputer selama proses investigasi forensik. Scalpel mencari hard drive, bit-stream image, unallocated space file, atau sembarang file komputer untuk karakteristik, isi atau atribut tertentu, dan menghasilkan laporan mengenai lokasi dan isi artifak yang ditemukan selama proses pencarian elektronik. Scalpel juga menghasilkan (carves) artifak yang ditemukan sebagai file individual.

Elemen kunci IT Forensik

Empat Elemen Kunci Forensik yang harus diperhatikan berkenaan dengan bukti digital dalam Teknologi Informasi, adalah sebagai berikut:

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

Merupakan tahapan paling awal dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah penyelidikan. *Network Administrator*merupakan sosok pertama yang umumnya mengetahui keberadaan *cybercrime*, atau Tim Respon *cybercrimecybercrime*diusut oleh *cyberpolice*. Ketika *cyberpolice* telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemen-elemen vital yang lainnya, antara lain: (jika perusahaan memilikinya) sebelum sebuah kasus

1. Petugas Keamanan (Officer/*as a First Responder*), Memiliki tugas-tugas yakni : ((i) Mengidentifikasi Peristiwa, (ii)Mengamankan Bukti dan (iii) Pemeliharaan bukti yang temporer dan Rawan Kerusakan.
2. Penelaah Bukti (Investigator), Memiliki Tugas-tugas yakni : (i) Menetapkan instruksi-instruksi sebagai sosok paling berwenang, (ii) Melakukan pengusutan peristiwa kejahatan,(iii) Pemeliharaan integritas bukti.
3. Teknisi Khusus, Memiliki tugas-tugas (dihindari terjadi*overlaping job* dengan Investigator), yakni (i) Pemeliharaan bukti yang rentan kerusakan dan menyalin *storageshuting down*) sistem yang sedang berjalan,(iii) Membungkus / memproteksi bukti-bukti,(iv)Mengangkut bukti,(v) Memproses bukti bukti,(ii) Mematikan(

Elemen-elemen vital diatas inilah yang kemudian nantinya memiliki *otoritas* penuh dalam penuntasan kasus kriminal yang terjadi.

- Penyimpanan bukti digital *(Preserving Digital Evidence)*

Bentuk, isi, makna bukti digital hendaknya disimpan dalam tempat yang *steril*. Untuk benar-benar memastikan tidak ada perubahan-perubahan, hal ini vital untuk diperhatikan. Karena sedikit perubahan saja dalam bukti digital, akan merubah juga hasil penyelidikan. Bukti digital secara alami bersifat sementara (*volatile*), sehingga keberadaannya jika tidak teliti akan sangat mudah sekali rusak, hilang, berubah, mengalami kecelakaan. Step pertama untuk menghindarkan dari kondisi-kondisi demikian adalah salahsatunya dengan mengcopy data secara *Bitstream Image* pada tempat yang sudah pasti aman.

Bitstream image adalah methode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk File yang tersembunyi (*hidden files*), File temporer (temp file), File yang terfragmentasi (*fragmen file*), file yang belum ter-*ovverwrite*. Dengan kata lain, setiap biner digit demi digit terkopi secara utuh dalam media baru. Tekhnik pengkopian ini menggunakan teknik ***Komputasi CRC***. Teknik ini umumnya diistilahkan dengan *Cloning DiskGhosting*. atau

Software-software yang dapat digunakan dalam aktivitas ini antara lain adalah:

- Safe Back. Dipasarkan sejak tahun 1990 untuk penegakan Hukum dan Kepolisian. Digunakan oleh FBI dan Divisi Investigasi Kriminal IRS. Berguna untuk pemakaian partisi tunggal secara virtual dalam segala ukuran. File Image dapat ditransformasikan dalam format SCSI atau media storage magnetik lainnya.
- EnCase. Seperti SafeBack yang merupakan program berbasis karakter, EnCase adalah program dengan fitur yang relatif mirip, dengan Interface GUI yang mudah dipakai oleh tekhnisi secara umum. Dapat dipakai dengan Multiple Platform seperti Windows NT atau Palm OS. Memiliki fasilitas dengan *Preview* Bukti, Pengkopian target,*SearchingAnalyzing.* dan
- Pro Discover[5]. Aplikasi berbasis Windows yang didesain oleh tim *Technology Pathways forensics.* Memiliki kemampuan untuk me-*recover* file yang telah terhapus dari *space storage* yang longgar, mengalanalisis Windows 2000/NT *data stream* untuk data yang

ter*hidden,*menganalisis data image yang diformat oleh kemampuan*dd UNIX* dan menghasilkan laporan kerja.

- Analisa bukti digital *(Analizing Digital Evidence)*

Barang bukti setelah disimpan, perlu diproses ulang sebelum diserahkan pada pihak yang membutuhkan. Pada proses inilah skema yang diperlukan akan fleksibel sesuai dengan kasus-kasus yang dihadapi. Barang bukti yang telah didapatkan perlu di*explore* kembali beberapa poin yang berhubungan dengan tindak pengusutan, antara lain: *(a)* Siapa yang telah melakukan. *(b)* Apa yang telah dilakukan (Ex. Penggunaan software apa),*(c)* Hasil proses apa yang dihasilkan. *(d)* Waktu melakukan.

Setiap bukti yang ditemukan, hendaknya kemudian dilist bukti-bukti potensial apa sajakah yang dapat didokumentasikan. Contoh kasus seperti kejahatan foto pornografi-anak ditemukan barang bukti gambar a.jpg, pada bukti ini akan dapat ditemukan data Nama file, tempat ditemukan, waktu pembuatan dan data properti yang lain. Selain itu perlu dicatat juga seperti *space*dari *storage,* format partisi dan yang berhubungan dengan alokasi lainnya.

Tiap-tiap data yang ditemukan sebenarnya merupakan informasi yang belum diolah, sehingga keberadaannya memiliki sifat yang vital dalam kesempatan tertentu. Data yang dimaksud antara lain :

- Alamat URL yang telah dikunjungi (dapat ditemukan pada Web cache, History, temporary internet files)
- Pesan e-mail atau kumpulan alamat e-mail yang terdaftar (dapat ditemukan pada e-mail server)
- Program Word processing atau format ekstensi yang dipakai (format yang sering dipakai adalah .doc, .rtf, .wpd, .wps, .txt)
- Dokumen spreedsheat yang dipakai (yang sering dipakai adalah .xls, .wgl, .xkl)
- Format gambar yang dipakai apabila ditemukan (.jpg, .gif, .bmp, .tif dan yang lainnya)
- Registry Windows (apabila aplikasi)
- Log Event viewers
- Log Applications
- File print spool
- Dan file-file terkait lainnya.

Analisis kemungkinan juga dapat diperoleh dari motif/latar belakang yang ada sebelum didapatkan kesimpulan. Bahwa setiap **sebab**, tentu saja akan memiliki potensi besar untuk menghasilkan **akibat** yang relatif seragam.

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

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

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

Pada tahapan *final* ini ada beberapa hal yang mutlak diperhatikan, karena memang pada level ini ukuran kebenaran akan ditetapkan oleh pengadilan sebagai pemilik otoritas. Hal-hal yang dimaksud adalah :

- Cara Presentasi
- Keahlian Presentasi
- Kualifikasi Presenter
- Kredibilitas setiap tahapan pengusutan

Tujuan IT Forensik

Adalah untuk mengamankan dan menganalisa bukti digital. Dari data yang diperoleh melalui survey oleh FBI dan The Computer Security Institute, pada tahun 1999 mengatakan bahwa 51% responden mengakui bahwa mereka telah menderita kerugian terutama dalam bidang finansial akibat kejahatan komputer. Kejahatan Komputer dibagi menjadi dua, yaitu:

1.Komputer fraud Kejahatan atau pelanggaran dari segi sistem organisasi komputer.

2.Komputer crime Merupakan kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Contoh kasus IT Forensik

Diawali dengan meningkatnya kejahatan di dunia computer khususnya di Internet, saat ini terdapat banyak sekali tingkat kriminalitas di Internet, seperti ; pencurian data pada sebuah site, pencurian informasi dari computer, Dos, Deface sites, carding, software bajakan, CC Cloning,

Kita tau ada banyak sekali kasus di dunia computer, dan pada umumnya kita sebagai orang awam kesusahan untuk membuktikan telah terjadinya penyalahgunaan sistem kita oleh orang lain. Lain halnya dengan pihak kepolisian yang saat ini telah berbenah diri untuk dapat mengungkap kasus demi kasus di dunia cyber dan computer ini.

Komputer forensik, suatu disiplin ilmu baru di dalam keamanan komputer, yang membahas atas temuan bukti digital setelah suatu peristiwa keamanan komputer terjadi., Komputer forensik akan lakukan analisa penyelidikan secara sistematis dan harus menemukan bukti pada suatu sistem digital yang nantinya dapat dipergunakan dan diterima di depan pengadilan, otentik, akurat, komplit, menyakinkan dihadapan juri, dan diterima didepan masyarakat.

Hal ini dilakukan oleh pihak berwajib untuk membuktikan pidana dari tindak suatu kejahatan. Maka saat ini menjadi seorang detective tidak hanya didunia nyata tapi juga didunia cyber. Coba kita bayangkan seorang hacker telah berhasil masuk ke system kita atau merubah data kita, baik itu menyalin, menghapus, menambah data baru, dll, Susah untuk kita buktikan karena keterbatasan alat dan tools. Dengan metode computer forensic kita dapat melakukan analisa seperti layaknya kejadian olah TKP.

Adapun contoh nyata yang berhubungan dengan IT Forensik antara lain:

-Contoh bagaimana melakukan aksi kejahatan di ATM (pembobolan ATM).

-Kasus kejahatan foto pornografi

-Penyelidikan dalam kasus nurdin M top (penyelidikan laptop nurdin M Top)

-Pembobolan E-banking paypal,CCards

Guna mengungkap kejahatan tersebut di butuhkan digital forensik sebagai metode mengungkap kejahatan tersebut dan beberapa alasan mengapa menggunakan digital forensik, antara lain:

-Dalam kasus hukum, teknik digital forensik sering digunakan untuk meneliti sistem komputer milik terdakwa (dalam perkara pidana) atau tergugat (dalam perkara perdata).

-Memulihkan data dalam hal suatu hardware atau software mengalami kegagalan/kerusakan (failure).

-Meneliti suatu sistem komputer setelah suatu pembongkaran/ pembobolan, sebagai contoh untuk menentukan bagaimana penyerang memperoleh akses dan serangan apa yang dilakukan.

-Mengumpulkan bukti menindak seorang karyawan yang ingin diberhentikan oleh suatu organisasi.

-Memperoleh informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimisasi kinerja, atau membalikkan rancang-bangun.

Tools yang Digunakan dalam IT Forensik

Secara garis besar tools untuk kepentingan komputer forensik dapat dibedakan secara hardware dan software.

Hardware:

- Harddisk IDE & SCSI kapasitas sangat besar, CD-R, DVR Drives.

- Memory yang besar (1-2GB RAM).
- Hub, Switch, keperluan LAN.
- Legacy Hardware (8088s, Amiga).
- Laptop forensic workstation.
- Write blocker

Software:

- Viewers (QVP, http://www.avantstar.com/)
- Erase/unerase tools (Diskscrub/Norton Utilities)
- Hash utility (MD5, SHA1)
- Forensic toolkit
- Forensic acquisition tools
- Write-blocking tools
- Spy Anytime PC Spy