Jelaskan perbedaan antara IT Audit dan IT Forensic, dari segi apa saja dan bagaimana pengaruhnya terhadap dampak dan tujuannya

IT FORENSIK

IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital. IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile. * Menurut Noblett, yaitu berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer. * Menurut Judd Robin, yaitu penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin. * Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa. Alasan mengapa menggunakan IT 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. Siapa yang menggunakan IT forensic ? Network Administrator merupakan sosok pertama yang umumnya mengetahui keberadaan cybercrime sebelum sebuah kasus cybercrime diusut oleh pihak yang berwenang. Ketika pihak yang berwenang telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemenelemen vital lainnya, antara lain: a. Petugas Keamanan (Officer/as a First Responder), Memiliki kewenangan tugas antara lain : mengidentifikasi peristiwa,mengamankan bukti, pemeliharaan bukti yang temporer dan rawan kerusakan. b. Penelaah Bukti (Investigator), adalah sosok yang paling berwenang dan memiliki kewenangan tugas antara lain: menetapkan instruksi-instruksi, melakukan pengusutan peristiwa kejahatan, pemeliharaan integritas bukti. c. Tekhnisi Khusus, memiliki kewenangan tugas antara lain : memeliharaan bukti yang rentan kerusakan dan menyalin storage bukti, mematikan(shuting down) sistem yang sedang berjalan, membungkus/memproteksi buktibukti, mengangkut bukti dan memproses bukti. IT forensic digunakan saat mengidentifikasi tersangka pelaku tindak kriminal untuk penyelidik, kepolisian, dan kejaksaan.

Tujuan IT Forensik

Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
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 :
Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

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

calpel 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.

Prodesur IT Forensik
Prosedur forensik yang umum digunakan, antara lain :Membuat copies dari keseluruhan log data, file, dan lain-lain yang dianggap perlu pada suatu media yang terpisah. Membuat copies secara matematis.Dokumentasi yang baik dari segala sesuatu yang dikerjakan.
Bukti yang digunakan dalam IT Forensics berupa :Harddisk.Floopy disk atau media lain yang bersifat removeable.Network system.
Metode/prosedure IT Forensik yang umum digunakan pada komputer ada dua jenis yaitu :
Search dan seizure : dimulai dari perumusan suatu rencana.
Identifikasi dengan penelitian permasalahan.
Membuat hipotesis.
Uji hipotesa secara konsep dan empiris.
Evaluasi hipotesa berdasarkan hasil pengujian dan pengujian ulang jika hipotesa tersebut jauh dari apa yang diharapkan.
Evaluasi hipotesa terhadap dampak yang lain jika hipotesa tersebut dapat diterima.
Pencarian informasi (discovery information). Ini dilakukan oleh investigator dan merupakan pencarian bukti tambahan dengan mengendalikan saksi secara langsung maupun tidak langsung.
Membuat copies dari keseluruhan log data, files, dan lain-lain yang dianggap perlu pada media terpisah.
Membuat fingerprint dari data secara matematis.
Membuat fingerprint dari copies secara otomatis.
Membuat suatu hashes masterlist
Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan.

IT Audit
Audit teknologi informasi 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.

B. Sejarah singkat Audit IT
Audit IT yang pada awalnya lebih dikenal sebagai EDP Audit (Electronic Data Processing) telah mengalami perkembangan yang pesat. Perkembangan Audit IT ini didorong oleh kemajuan teknologi dalam sistem keuangan, meningkatnya kebutuhan akan kontrol IT, dan pengaruh dari komputer itu sendiri untuk menyelesaikan tugas-tugas penting. Pemanfaatan teknologi komputer ke dalam sistem keuangan telah mengubah cara kerja sistem keuangan, yaitu dalam penyimpanan data, pengambilan kembali data, dan pengendalian. Sistem keuangan pertama yang menggunakan teknologi komputer muncul pertama kali tahun 1954. Selama periode 1954 sampai dengan 1960-an profesi audit masih menggunakan komputer. Pada pertengahan 1960-an terjadi perubahan pada mesin komputer, dari mainframe menjadi komputer yang lebih kecil dan murah.
Pada tahun 1968, American Institute of Certified Public Accountants (AICPA) ikut mendukung pengembangan EDP auditing. Sekitar periode ini pula para auditor bersama-sama mendirikan Electronic Data Processing Auditors Association (EDPAA). Tujuan lembaga ini adalah untuk membuat suatu tuntunan, prosedur, dan standar bagi audit EDP. Pada tahun 1977, edisi pertama Control Objectives diluncurkan. Publikasi ini kemudian dikenal sebagai Control Objectives for Information and Related Technology (CobiT). Tahun 1994, EDPAA mengubah namanya menjadi Information System Audit (ISACA). Selama periode akhir 1960-an sampai saat ini teknologi TI telah berubah dengan cepat dari mikrokomputer dan jaringan ke internet. Pada akhirnya perubahan-perubahan tersebut ikut pula menentukan perubahan pada audit IT.

C. Jenis Audit IT.
1. Sistem dan aplikasi.
Memeriksa apakah sistem dan aplikasi sesuai dengan kebutuhan organisasi, berdayaguna, dan memiliki kontrol yang cukup baik untuk menjamin keabsahan, kehandalan, tepat waktu, dan keamanan pada input, proses, output pada semua tingkat kegiatan sistem.

2. Fasilitas pemrosesan informasi.
Memeriksa apakah fasilitas pemrosesan terkendali untuk menjamin ketepatan waktu, ketelitian, dan pemrosesan aplikasi yang efisien dalam keadaan normal dan buruk.
3. Pengembangan sistem.
Memeriksa apakah sistem yang dikembangkan mencakup kebutuhan obyektif organisasi.
4. Arsitektur perusahaan dan manajemen TI
Memeriksa apakah manajemen TI dapat mengembangkan struktur organisasi dan prosedur yang menjamin kontrol dan lingkungan yang berdaya guna untuk pemrosesan informasi.
5. Client/Server, telekomunikasi, intranet, dan ekstranet
Memeriksa apakah kontrol-kontrol berfungsi pada client, server, dan jaringan yang menghubungkan client dan server.

D. Metodologi Audit IT.
Dalam praktiknya, tahapan-tahapan dalam audit IT tidak berbeda dengan audit pada umumnya, sebagai berikut :
1. Tahapan Perencanaan.
Sebagai suatu pendahuluan mutlak perlu dilakukan agar auditor mengenal benar obyek yang akan diperiksa sehingga menghasilkan suatu program audit yang didesain sedemikian rupa agar pelaksanaannya akan berjalan efektif dan efisien.
2. Mengidentifikasikan reiko dan kendali.
Untuk memastikan bahwa qualified resource sudah dimiliki, dalam hal ini aspek SDM yang berpengalaman dan juga referensi praktik-praktik terbaik.
3. Mengevaluasi kendali dan mengumpulkan bukti-bukti.
Melalui berbagai teknik termasuk survei, interview, observasi, dan review dokumentasi.
4. Mendokumentasikan.
Mengumpulkan temuan-temuan dan mengidentifikasikan dengan auditee.
5. Menyusun laporan.
Mencakup tujuan pemeriksaan, sifat, dan kedalaman pemeriksaan yang dilakukan.

E. Alasan dilakukannya Audit IT.
Ron Webber, Dekan Fakultas Teknologi Informasi, monash University, dalam salah satu bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :
1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

F. Manfaat Audit IT.
1. Manfaat pada saat Implementasi (Pre-Implementation Review)
– Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
– Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
– Mengetahui apakah outcome sesuai dengan harapan manajemen.
2. Manfaat setelah sistem live (Post-Implementation Review)
– Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
– Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya.
– Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
– Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
– Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
– Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

G. Pengertian Audit Trail

Audit Trail merupakan salah satu fitur dalam suatu program yang mencatat semua kegiatan yang dilakukan tiap user dalam suatu tabel log. secara rinci. Audit Trail secara default akan mencatat waktu , user, data yang diakses dan berbagai jenis kegiatan. Jenis kegiatan bisa berupa menambah, merungubah dan menghapus. Audit Trail apabila diurutkan berdasarkan waktu bisa membentuk suatu kronologis manipulasi data.Dasar ide membuat fitur Audit Trail adalah menyimpan histori tentang suatu data (dibuat, diubah atau dihapus) dan oleh siapa serta bisa menampilkannya secara kronologis. Dengan adanya Audit Trail ini, semua kegiatan dalam program yang bersangkutan diharapkan bisa dicatat dengan baik.

1. Cara Kerja Audit Trail

a. Audit Trail yang disimpan dalam suatu tabel

b. Dengan menyisipkan perintah penambahan record ditiap query Insert, Update dan Delete

c. 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.

2. 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.

3. Hasil Audit Trail

Record Audit Trail disimpan dalam bentuk, yaitu :

a. Binary File – Ukuran tidak besar dan tidak bisa dibaca begitu saja

b. Text File – Ukuran besar dan bisa dibaca langsung

c. Tabel.

Perbedaan audit around computer dan through the computer

Audit around computer

adalah suatu pendekatan audit yang berkaitan dengan komputer, lebih tepatnya pendekatan audit disekitar komputer. dalam pendekatan ini auditor dapat melangkah kepada perumusan pendapatdengan hanya menelaah sturuktur pengendalian dan melaksanakan pengujian transaksi dan prosedur verifikasi saldo perkiraan dengan cara sama seperti pada sistem manual(bukan sistem informasi berbasis komputer).

Audit around computer dilakukan pada saat :

1. Dokumen sumber tersedia dalam bentuk kertas (bahasa non-mesin), artinya masih kasat mata dan dilihat secara visual.
2. Dokumen-dokumen disimpan dalam file dengan cara yang mudah ditemukan
3. Keluaran dapat diperoleh dari daftar yang terinci dan auditor mudah menelusuri setiap transaksi dari dokumen sumber kepada keluaran dan sebaliknya.

keunggulan metode Audit around computer :

1. Pelaksanaan audit lebih sederhana.
2. Auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilihat dengan mudah untuk melaksanakan audit.

Audit Through the computer

Audit ini berbasis komputer, dimana dalam pendekatan ini auditor melakukan pemeriksaan langsung terhadap program-program dan file-file komputer pada audit sistem informasi berbasis komputer. Auditor menggunakan komputer (software bantu) atau dengan cek logika atau listing program untuk menguji logika program dalam rangka pengujian pengendalian yang ada dalam komputer.

Pendekatan Audit Through the computer dilakukan dalam kondisi :

1. Sistem aplikasi komputer memroses input yang cukup besar dan menghasilkan output yang cukup besar pula, sehingga memperuas audit untuk meneliti keabsahannya.
2. Bagian penting dari struktur pengendalian intern perusahaan terdapat di dalam komputerisasi yang digunakan.

Keunggulan pendekatan Audit Through the computer :

1. Auditor memperoleh kemampuasn yang besar dan efketif dalam melakukan pengujian terhadap sistem komputer.
2. Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.
3. Auditor dapat melihat kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan.

Resume:

Audit IT merupakan urutan kronologis catatan audit, yang masing-masing berisikan bukti langsung yang berkaitan

dengan yang dihasilkan dari pelaksanaan suatu proses bisnis atau fungsi sistem. Catatan audit biasanya hasil kerja dari kegiatan seperti transaksi atau komunikasi oleh orang-orang individu, sistem, rekening atau badan lainnya. Dengan adanya Audit IT diharapkan semua kronologis/kegiatan program dapat terekam dengan baik.
Audit IT juga sangat membantu dalam IT forensik jika pengguna IT menderita kerugian terutama dalam bidang finansial akibat kejahatan komputer seperti Komputer fraud (Kejahatan atau pelanggaran dari segi sistem organisasi komputer) dan Komputer crime. (menggunakan media komputer dalam melakukan pelanggaran hukum). Sehingga memudahkan Penyidik IT forensik dalam menganalisa.

IT Audit

Audit menurut Arens, et al. (2003) yang diterjemahkan oleh kanto Santoso Setiawan dan Tumbur Pasaribu adalah proses pengumpulan dan pengevaluasian bukti-bukti tentang informasi ekonomi untuk menentukan tingkat kesesuaian informasi tersebut dengan criteria-kriteria yang telah ditetapkan, dan melaporkan hasil pemeriksaan tersebut. IT Audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.IT audit lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. IT Audit merupakan gabungan dari berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science. (Laporan) IT Audit bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan kebutuhan (integrity) dari sistem informasi organisasi.

IT Forensik

IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital. IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile.

IT FORENSIK

IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital.

IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile. * Menurut Noblett, yaitu berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer. * Menurut Judd Robin, yaitu penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin. * Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa. Alasan mengapa menggunakan IT 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. Siapa yang menggunakan IT forensic ? Network Administrator merupakan sosok pertama yang umumnya mengetahui keberadaan cybercrime sebelum sebuah kasus cybercrime diusut oleh pihak yang berwenang. Ketika pihak yang berwenang telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemenelemen vital lainnya, antara lain: a. Petugas Keamanan (Officer/as a First Responder), Memiliki kewenangan tugas antara lain : mengidentifikasi peristiwa,mengamankan bukti, pemeliharaan bukti yang temporer dan rawan kerusakan. b. Penelaah Bukti (Investigator), adalah sosok yang paling berwenang dan memiliki kewenangan tugas antara lain: menetapkan instruksi-instruksi, melakukan pengusutan peristiwa kejahatan, pemeliharaan integritas bukti. c. Tekhnisi Khusus, memiliki kewenangan tugas antara lain : memeliharaan bukti yang rentan kerusakan dan menyalin storage bukti, mematikan(shuting down) sistem yang sedang berjalan, membungkus/memproteksi buktibukti, mengangkut bukti dan memproses bukti. IT forensic digunakan saat mengidentifikasi tersangka pelaku tindak kriminal untuk penyelidik, kepolisian, dan kejaksaan.

Tujuan IT Forensik

Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
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 : Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.

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

IT Audit

Audit teknologi informasi 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.

Alasan dilakukannya Audit IT

Ron Webber, Dekan Fakultas Teknologi Informasi, monash University, dalam salah satu bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :
1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Manfaat Audit IT.
1. Manfaat pada saat Implementasi (Pre-Implementation Review) Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria. Mengetahui apakah pemakai telah siap menggunakan sistem tersebut. Mengetahui apakah outcome sesuai dengan harapan manajemen.
2. Manfaat setelah sistem live (Post-Implementation Review) Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya. Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya. Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang. Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan. Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan. Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

sumber : http://pietrajayaramadhan.blogspot.com/2015/06/it-forensic-it-audit-dan-perbedaan.html

Nama : Mifathul Fallah

Nim : 182420132

Kelas : MTI 20A

Jawaban :

Audit IT adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal. Audit IT lebih dikenal dengan istilah *EDP Auditing* (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. Salah satu penggunaan istilah tersebut adalah untuk menjelaskan proses penelahan dan evaluasi pengendalian-pengendalian internal dalam EDP. Audit IT bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan keutuhan (integrity) dari sistem informasi organisasi.

Proses IT Audit

Mengumpulkan dan mengevaluasi bukti-bukti bagaimana system informasi dikembangkan, dioperasikan, diorganisasikan, serta bagaimana praktek dilaksanakan:

a. Apakah IS melindungi aset institusi: asset protection, availability

b. Apakah integritas data dan sistem diproteksi secara cukup (security, confidentiality)

c. Apakah operasi sistem efektif dan efisien dalam mencapai tujuan organisasi, dan lain-lain (coba cari pertanyaan2 lain).

Salah satu software yang dapat dijadikan alat bantu dalam pelaksanaan audit teknologi informasi

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. ACL for Windows (sering disebut ACL) adalah sebuah software TABK (TEKNIK AUDIT BERBASIS KOMPUTER) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektro.

IT Forensik yaitu penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. 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.

Tujuan IT Forensik

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 :
    - Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
    - Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Metode yang sering digunakan dalam pendekatan Audit Forensik IT yaitu, Audit around the computer adalah pendekatan audit dimana auditor menguji keandalan sebuah informasi yang dihasilkan oleh komputer dengan terlebih

dahulu mengkalkulasikan hasil dari sebuah transaksi yang dimasukkan dalam sistem. Kemudian, kalkulasi tersebut dibandingkan dengan output yang dihasilkan oleh sistem. Apabila ternyata valid dan akurat, diasumsikan bahwa pengendalian sistem telah efektif dan sistem telah beroperasi dengan baik. Jenis audit ini dapat digunakan ketika proses yang terotomasi dalam sistem cukup sederhana. Kelemahan dari audit ini adalah bahwa audit around the computer tidak menguji apakah logika program dalam sebuah sistem benar. Selain itu, jenis pendekatan audit ini tidak menguji bagaimana pengendalian yang terotomasi menangani input yang mengandung error. Dampaknya, dalam lingkungan IT yang komplek, pendekatan ini akan tidak mampu untuk mendeteksi banyak error.

Nama: Moh Fajri Al Amin

NIM : 182420121

IT AUDIT

jawaban:

IT FORENSIK
IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital. IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile. * Menurut Noblett, yaitu berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer. * Menurut Judd Robin, yaitu penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin. * Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa. Alasan mengapa menggunakan IT 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. Siapa yang menggunakan IT forensic ? Network Administrator merupakan sosok pertama yang umumnya mengetahui keberadaan cybercrime sebelum sebuah kasus cybercrime diusut oleh pihak yang berwenang. Ketika pihak yang berwenang telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemenelemen vital lainnya, antara lain: a. Petugas Keamanan (Officer/as a First Responder), Memiliki kewenangan tugas antara lain : mengidentifikasi peristiwa,mengamankan bukti, pemeliharaan bukti yang temporer dan rawan kerusakan. b. Penelaah Bukti (Investigator), adalah sosok yang paling berwenang dan memiliki kewenangan tugas antara lain: menetapkan instruksi-instruksi, melakukan pengusutan peristiwa kejahatan, pemeliharaan integritas bukti. c. Tekhnisi Khusus, memiliki kewenangan tugas antara lain : memeliharaan bukti yang rentan kerusakan dan menyalin storage bukti, mematikan(shuting down) sistem yang sedang berjalan, membungkus/memproteksi buktibukti, mengangkut bukti dan memproses bukti. IT forensic digunakan saat mengidentifikasi tersangka pelaku tindak kriminal untuk penyelidik, kepolisian, dan kejaksaan.

Tujuan IT Forensik
Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
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 :
Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

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
calpel 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.

Prodesur IT Forensik
Prosedur forensik yang umum digunakan, antara lain :Membuat copies dari keseluruhan log data, file, dan lain-lain yang dianggap perlu pada suatu media yang terpisah. Membuat copies secara matematis.Dokumentasi yang baik dari segala sesuatu yang dikerjakan.
Bukti yang digunakan dalam IT Forensics berupa :Harddisk.Floopy disk atau media lain yang bersifat removeable.Network system.
Metode/prosedure IT Forensik yang umum digunakan pada komputer ada dua jenis yaitu :
Search dan seizure : dimulai dari perumusan suatu rencana.
Identifikasi dengan penelitian permasalahan.
Membuat hipotesis.
Uji hipotesa secara konsep dan empiris.
Evaluasi hipotesa berdasarkan hasil pengujian dan pengujian ulang jika hipotesa tersebut jauh dari apa yang diharapkan.
Evaluasi hipotesa terhadap dampak yang lain jika hipotesa tersebut dapat diterima.
Pencarian informasi (discovery information). Ini dilakukan oleh investigator dan merupakan pencarian bukti tambahan dengan mengendalikan saksi secara langsung maupun tidak langsung.
Membuat copies dari keseluruhan log data, files, dan lain-lain yang dianggap perlu pada media terpisah.
Membuat fingerprint dari data secara matematis.
Membuat fingerprint dari copies secara otomatis.
Membuat suatu hashes masterlist
Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan.

IT Audit
Audit teknologi informasi 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.

B. Sejarah singkat Audit IT
Audit IT yang pada awalnya lebih dikenal sebagai EDP Audit (Electronic Data Processing) telah mengalami perkembangan yang pesat. Perkembangan Audit IT ini didorong oleh kemajuan teknologi dalam sistem keuangan, meningkatnya kebutuhan akan kontrol IT, dan pengaruh dari komputer itu sendiri untuk menyelesaikan tugas-tugas penting. Pemanfaatan teknologi komputer ke dalam sistem keuangan telah mengubah cara kerja sistem keuangan, yaitu dalam penyimpanan data, pengambilan kembali data, dan pengendalian. Sistem keuangan pertama yang menggunakan teknologi komputer muncul pertama kali tahun 1954. Selama periode 1954 sampai dengan 1960-an profesi audit masih menggunakan komputer. Pada pertengahan 1960-an terjadi perubahan pada mesin komputer, dari mainframe menjadi komputer yang lebih kecil dan murah.
Pada tahun 1968, American Institute of Certified Public Accountants (AICPA) ikut mendukung pengembangan EDP auditing. Sekitar periode ini pula para auditor bersama-sama mendirikan Electronic Data Processing Auditors Association (EDPAA). Tujuan lembaga ini adalah untuk membuat suatu tuntunan, prosedur, dan standar bagi audit EDP. Pada tahun 1977, edisi pertama Control Objectives diluncurkan. Publikasi ini kemudian dikenal sebagai Control Objectives for Information and Related Technology (CobiT). Tahun 1994, EDPAA mengubah namanya menjadi Information System Audit (ISACA). Selama periode akhir 1960-an sampai saat ini teknologi TI telah berubah dengan

cepat dari mikrokomputer dan jaringan ke internet. Pada akhirnya perubahan-perubahan tersebut ikut pula menentukan perubahan pada audit IT.

C. Jenis Audit IT.
1. Sistem dan aplikasi.
Memeriksa apakah sistem dan aplikasi sesuai dengan kebutuhan organisasi, berdayaguna, dan memiliki kontrol yang cukup baik untuk menjamin keabsahan, kehandalan, tepat waktu, dan keamanan pada input, proses, output pada semua tingkat kegiatan sistem.
2. Fasilitas pemrosesan informasi.
Memeriksa apakah fasilitas pemrosesan terkendali untuk menjamin ketepatan waktu, ketelitian, dan pemrosesan aplikasi yang efisien dalam keadaan normal dan buruk.
3. Pengembangan sistem.
Memeriksa apakah sistem yang dikembangkan mencakup kebutuhan obyektif organisasi.
4. Arsitektur perusahaan dan manajemen TI
Memeriksa apakah manajemen TI dapat mengembangkan struktur organisasi dan prosedur yang menjamin kontrol dan lingkungan yang berdaya guna untuk pemrosesan informasi.
5. Client/Server, telekomunikasi, intranet, dan ekstranet
Memeriksa apakah kontrol-kontrol berfungsi pada client, server, dan jaringan yang menghubungkan client dan server.

D. Metodologi Audit IT.
Dalam praktiknya, tahapan-tahapan dalam audit IT tidak berbeda dengan audit pada umumnya, sebagai berikut :
1. Tahapan Perencanaan.
Sebagai suatu pendahuluan mutlak perlu dilakukan agar auditor mengenal benar obyek yang akan diperiksa sehingga menghasilkan suatu program audit yang didesain sedemikian rupa agar pelaksanaannya akan berjalan efektif dan efisien.
2. Mengidentifikasikan reiko dan kendali.
Untuk memastikan bahwa qualified resource sudah dimiliki, dalam hal ini aspek SDM yang berpengalaman dan juga referensi praktik-praktik terbaik.
3. Mengevaluasi kendali dan mengumpulkan bukti-bukti.
Melalui berbagai teknik termasuk survei, interview, observasi, dan review dokumentasi.
4. Mendokumentasikan.
Mengumpulkan temuan-temuan dan mengidentifikasikan dengan auditee.
5. Menyusun laporan.
Mencakup tujuan pemeriksaan, sifat, dan kedalaman pemeriksaan yang dilakukan.

E. Alasan dilakukannya Audit IT.
Ron Webber, Dekan Fakultas Teknologi Informasi, monash University, dalam salah satu bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :
1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

F. Manfaat Audit IT.
1. Manfaat pada saat Implementasi (Pre-Implementation Review)
– Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
– Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
– Mengetahui apakah outcome sesuai dengan harapan manajemen.
2. Manfaat setelah sistem live (Post-Implementation Review)
– Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
– Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran

pada periode berikutnya.
– Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
– Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
– Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
– Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

G. Pengertian Audit Trail
Audit Trail merupakan salah satu fitur dalam suatu program yang mencatat semua kegiatan yang dilakukan tiap user dalam suatu tabel log. secara rinci. Audit Trail secara default akan mencatat waktu , user, data yang diakses dan berbagai jenis kegiatan. Jenis kegiatan bisa berupa menambah, merungubah dan menghapus. Audit Trail apabila diurutkan berdasarkan waktu bisa membentuk suatu kronologis manipulasi data.Dasar ide membuat fitur Audit Trail adalah menyimpan histori tentang suatu data (dibuat, diubah atau dihapus) dan oleh siapa serta bisa menampilkannya secara kronologis. Dengan adanya Audit Trail ini, semua kegiatan dalam program yang bersangkutan diharapkan bisa dicatat dengan baik.
1. Cara Kerja Audit Trail
a. Audit Trail yang disimpan dalam suatu tabel
b. Dengan menyisipkan perintah penambahan record ditiap query Insert, Update dan Delete
c. 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.
2. 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.
3. Hasil Audit Trail
Record Audit Trail disimpan dalam bentuk, yaitu :
a. Binary File – Ukuran tidak besar dan tidak bisa dibaca begitu saja
b. Text File – Ukuran besar dan bisa dibaca langsung
c. Tabel.
Perbedaan audit around computer dan through the computer
Audit around computer
adalah suatu pendekatan audit yang berkaitan dengan komputer, lebih tepatnya pendekatan audit disekitar komputer. dalam pendekatan ini auditor dapat melangkah kepada perumusan pendapatdengan hanya menelaah sturuktur pengendalian dan melaksanakan pengujian transaksi dan prosedur verifikasi saldo perkiraan dengan cara sama seperti pada sistem manual(bukan sistem informasi berbasis komputer).
Audit around computer dilakukan pada saat :
1. Dokumen sumber tersedia dalam bentuk kertas (bahasa non-mesin), artinya masih kasat mata dan dilihat secara visual.
2. Dokumen-dokumen disimpan dalam file dengan cara yang mudah ditemukan
3. Keluaran dapat diperoleh dari daftar yang terinci dan auditor mudah menelusuri setiap transaksi dari dokumen sumber kepada keluaran dan sebaliknya.
keunggulan metode Audit around computer :
1. Pelaksanaan audit lebih sederhana.
2. Auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilihat dengan mudah untuk melaksanakan audit.
Audit Through the computer
Audit ini berbasis komputer, dimana dalam pendekatan ini auditor melakukan pemeriksaan langsung terhadap program-program dan file-file komputer pada audit sistem informasi berbasis komputer. Auditor menggunakan komputer (software bantu) atau dengan cek logika atau listing program untuk menguji logika program dalam rangka pengujian pengendalian yang ada dalam komputer.
Pendekatan Audit Through the computer dilakukan dalam kondisi :
1. Sistem aplikasi komputer memroses input yang cukup besar dan menghasilkan output yang cukup besar pula, sehingga memperuas audit untuk meneliti keabsahannya.

2. Bagian penting dari struktur pengendalian intern perusahaan terdapat di dalam komputerisasi yang digunakan.

Keunggulan pendekatan Audit Through the computer :
1. Auditor memperoleh kemampuasn yang besar dan efketif dalam melakukan pengujian terhadap sistem komputer.
2. Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.
3. Auditor dapat melihat kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan.

Resume:
Audit IT merupakan urutan kronologis catatan audit, yang masing-masing berisikan bukti langsung yang berkaitan dengan yang dihasilkan dari pelaksanaan suatu proses bisnis atau fungsi sistem. Catatan audit biasanya hasil kerja dari kegiatan seperti transaksi atau komunikasi oleh orang-orang individu, sistem, rekening atau badan lainnya. Dengan adanya Audit IT diharapkan semua kronologis/kegiatan program dapat terekam dengan baik.
Audit IT juga sangat membantu dalam IT forensik jika pengguna IT menderita kerugian terutama dalam bidang finansial akibat kejahatan komputer seperti Komputer fraud (Kejahatan atau pelanggaran dari segi sistem organisasi komputer) dan Komputer crime. (menggunakan media komputer dalam melakukan pelanggaran hukum). Sehingga memudahkan Penyidik IT forensik dalam menganalisa.

Definisi

IT Forensic Yaitu penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal.

IT Audit adalah adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.

Perbedaannya

IT Forensic : untuk mengamankan dan menganalisa bukti digital sedangkan

IT Audit : untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan keutuhan (integrity) dari sistem informasi organisasi.

Prinsip IT Forensik

1. Forensik bukan proses Hacking
2. Data yang didapat harus dijaga jangan berubah
3. Membuat image dari HD / Floppy / USB-Stick / Memory-dump adalah prioritas tanpa merubah isi, kadang digunakan hardware khusus
4. Image tsb yang diotak-atik (hacking) dan dianalisis – bukan yang asli
5. Data yang sudah terhapus membutuhkan tools khusus untuk merekonstruksi
6. Pencarian bukti dengan: tools pencarian teks khusus, atau mencari satu persatu dalam image

Alasan Dilakukannya IT Audit

Ron Webber, Dekan Fakultas Teknologi Informasi, monash University, dalam salah satu bukunya *Information System Controls and Audit* (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Sumber : https://bambangsuhartono.wordpress.com/2013/09/10/pentingnya-it-forensic-dan-it-audit/

IT Audit

- Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
- Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
- Mengukur tingkat efektifitas dari sistem
- Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang
- Menyediakan informasi untuk proses peningkatan
- Meningkatkan saling memahami antar departemen dan antar individu
- Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen

Keterampilan yang dibutuhkan

- Audit skill : sampling, komunikasi, melakukan interview, mengajukan pertanyaan, mencatat
- Generic knowledge : pengetahuan mengenai prinsip2 audit, prosedur dan teknik, sistem manajemen dan dokumen2 referensi, organisasi, peraturan2 yang berlaku
- Specific knowledge : background IT/IS, bisnis, specialist technical skill, pengalaman audit sistem manajemen, perundangan

IT Forensik

Komputer Forensik adalah cabang dari ilmu forensik berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik.

Tujuan dari komputer forensik adalah untuk menjelaskan keadaan artefak digital saat ini . Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan komputer. ” Penjelasannya dapat secara langsung sebagai “informasi apa yang ada di sini?” dan sama detailnya dengan “apa urutan kejadian-kejadian yang bertanggung jawab atas situasi sekarang?”

Bidang komputer forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile.

Terima kasih, salam.

IT Audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.IT audit lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. IT Audit merupakan gabungan dari berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science. (Laporan) IT Audit bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan kebutuhan (integrity) dari sistem informasi organisasi.

IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile.

Alasan Penggunakan IT Audit

Ron Webber (Dekan Fakultas Teknologi Informasi, Monash University) dalam bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Manfaat IT Audit

1. Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
2. Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
3. Mengetahui apakah outcome sesuai dengan harapan manajemen.

Alasan Penggunaan IT Forensik

1. Dalam kasus hukum, teknik komputer forensik sering digunakan untuk menganalisis sistem komputer milik terdakwa (dalam kasus pidana) atau milik penggugat (dalam kasus perdata).
2. Untuk memulihkan data jika terjadi kegagalan atau kesalahan hardware atausoftware.
3. Untuk menganalisa sebuah sistem komputer setelah terjadi perampokan, misalnya untuk menentukan bagaimana penyerang memperoleh akses dan apa yang penyerang itu lakukan.
4. Untuk mengumpulkan bukti untuk melawan seorang karyawan yang ingin diberhentikan oleh organisasi.
5. Untuk mendapatkan informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimasi kinerja, atau reverse-engineering.

Tujuan IT Forensik

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 :

Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.

- Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Perbedaan	IT Audit	IT Forensik
Definisi	**suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.IT audit lebih dikenal dengan istilah *EDP Auditing* (*Electronic Data Processing*), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. IT Audit merupakan gabungan dari berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.**	**prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal.**
Tujuan	**meninjau dan mengevaluasi faktor-faktor ketersediaan (*availability*), kerahasiaan (*confidentiality*), dan kebutuhan (*integrity*) dari sistem informasi organisasi.**	**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.**
Tools	**1 ACL (Audit Command Language): software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber.** **2 Picalo : software CAAT (Computer**	1. Antiword. Aplikasi untuk menampilkan teks dan gambar dokumen Microsoft Word. 1. Autopsy. The Autopsy Forensic Browser merupakan antarmuka

Assisted Audit Techniques) seperti halnya ACL yang dapat dipergunakan untuk menganalisa data dari berbagai macam sumber.

3 Powertech Compliance Assessment Powertech: 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 serverAS/400.

4 Nipper : audit automation software yang dapat dipergunakan untuk mengaudit dan mem-benchmark konfigurasi sebuah router.

5 Nessus: sebuah vulnerability assessment software.

6 Metasploit Framework : sebuah penetration testing tool.

7 NMAP: utility untuk melakukan security auditing.

8 Wireshark: network utility yang dapat dipergunakan untuk meng-capture paket data yang ada di dalam jaringan komputer.

grafis untuk tool analisis investigasi diginal perintah baris The Sleuth Kit.

2. Binhash. Program sederhana untuk melakukan hashing terhadap berbagai bagian file ELF dan PE untuk perbandingan.
3. Sigtool. 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.
4. ChaosReader. 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
5. Chkrootkit. 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.
6. 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.
7. GNU Ddrescue. Tool penyelamat data, la menyalinkan data dari satu file atau device blok (hard disc, cdrom, dsb.)
8. Foremost. Tool yang dapat digunakan untuk me-recover file berdasarkan

		header, footer, atau struktur data file tersebut. 9. Gqview. Program untuk melihat gambar berbasis GTK la mendukung beragam format gambar, zooming, panning, thumbnails, dan pengurutan gambar. 10. Galleta. Tool yang ditulis oleh Keith J Jones untuk melakukan analisis forensic terhadap cookie Internet Explorer. 11. Ishw (Hardware Lister). Tool kecil yang memberikan informasi detil mengenai konfigurasi hardware dalam mesin.. 12. Pasco. Banyak penyelidikan kejahatan komputer membutuhkan rekonstruksi aktivitas Internet tersangka. 13. Scalpel. Tool forensik yang dirancang untuk mengidentifikasikan, mengisolasi dan merecover data dari media komputer selama proses investigasi forensik.
Dampak Pengunaannya	1. **Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.** 2. **Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.** 3. **Mengetahui apakah outcome sesuai dengan harapan manajemen.** 4. **Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.** 5. **Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang**	1. Untuk memulihkan data jika terjadi kegagalan atau kesalahan hardware atausoftware. 2. Untuk menganalisa sebuah sistem komputer setelah terjadi perampokan, misalnya untuk menentukan bagaimana penyerang memperoleh akses dan apa yang penyerang itu lakukan. 3. Untuk mengumpulkan bukti untuk melawan seorang karyawan yang ingin diberhentikan oleh organisasi. 4. Untuk mendapatkan informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimasi kinerja, atau reverse-engineering.

	melakukan pemeriksaan. 6. **Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.** 7. **Untuk memulihkan data jika terjadi kegagalan atau kesalahan hardware atausoftware.** 8. **Untuk menganalisa sebuah sistem komputer setelah terjadi perampokan, misalnya untuk menentukan bagaimana penyerang memperoleh akses dan apa yang penyerang itu lakukan.** 9. **Untuk mengumpulkan bukti untuk melawan seorang karyawan yang ingin diberhentikan oleh organisasi.** 10. **Untuk mendapatkan informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimasi kinerja, atau reverse-engineering.**	

Perbedaan IT Audit da IT Forensik

IT AUDIT

IT Audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.IT audit lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. IT Audit merupakan gabungan dari berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science. (Laporan) IT Audit bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan kebutuhan (integrity) dari sistem informasi organisasi.

Manfaat penggunaan IT Audit dapat dikelompokkan menjadi 2 yaitu:

A. Manfaat pada saat Implementasi (Pre-Implementation Review)

1. Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
2. Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
3. Mengetahui apakah outcome sesuai dengan harapan manajemen.

B. Manfaat setelah sistem live (Post-Implementation Review)

1. Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
2. Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya.
3. Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
4. Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
5. Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
6. Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

IT FORENSIK

IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital. IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile.

Tujuan IT Forensik

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 :
    - Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
    - Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Audit teknologi informasi atau information systems (IS) audit adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh.

IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal.

Kesimpulan ;

Menurut saya IT forensic itu di ibaratkan seperti seorang detektif yang bertugas mencari tau kebenaran dari suatu kasus. Khusus untuk IT forensic ini adalah untuk mencari tau dan menganalisa bukti-bukti pelanggaran atau kejahatan sistem informasi sehingga dapat di pertanggungjawabkan secara hukum di pengadilan. IT audit itu sendiri bertujuan untuk meninjau atau mengevaluasi masalah audit financial ataupun audit internal suatu perusahaan dengan menggunakan berbagai macam ilmu seperti audit tradisional, manajemen sistem informasi, sistem informasi akuntansi ataupun ilmu computer. Kemudian tujuan lainnya adalah untuk mengurangi kerugian akibat kehilangan data, mengurangi kesalahan dalam pengambilan keputusan serta untuk meminimalisasi dampak penyalahgunaan computer oleh orang yang tidak bertanggung jawab. Audit arround the computer lebih mengacu terhadap audit bidang IT dengan menguji sebuah informasi dalam sebuah sistem apakah seluruh transaksi yang ada pada system sudah valid dan akurat apa belum kemudian dibandingkan dengan output yang dihasilkan. Dan audit through the computer audit ini menguji sebuah system dan pengecekan pemrograman apakah terjadi error atau sudah berjalan sesuai yang diinginkan, audit ini lebih ke pemeriksaan tekhnik pembuatan dengan memeriksa logika pemrograman dan pengendalianny

1. **1. IT Audit**- adalah bentuk pengawasan dan pengendalian dari infrastrukturteknologi 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.

1.2. Tujuan IT Audit - Menjalankan pengelolaan IT dengan lebih efektif dan efisien, Meningkatkan kepuasan pelanggan, Peningkatan kinerja yang berkesinambungan, Meningkatkan nilai jual (competitive advanced) produk layanan contact center perbankan, Meningkatkan tingkat kepatuhan terhadap ketentuan / peraturan pemerintah dan bidang usaha, Meningkatkan pengawasan (controling) terhadap pengelolaan IT yang digunakan sebagai pendukung proses bisnis dan produk solusi layanan DRC perbankan perusahaan.

1. **2. IT Forensik -** adalah suatu disiplin ilmu turunan keamanan komputer yang membahas tentang temuan bukti digital setelah suatu peristiwa terjadi. Kegiatan forensik komputer sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa, dan mempergunakan bukti digital menurut hukum yang berlaku.

Sedangkan definisi forensik IT menurut para ahli diantaranya :

• Menurut Noblett, yaitu berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer.

• Menurut Judd Robin, yaitu penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin.

• Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

2.1. Tujuan IT Forensik - Tujuan utama dari kegiatan forensik IT adalah untuk mengamankan dan menganalisa bukti digital dengan cara menjabarkan keadaan terkini dari suatu artefak digital. Istilah artefak digital dapat mencakup sebuah sistem komputer, media penyimpanan (harddisk, flashdisk, CD-ROM), sebuah dokumen elektronik (misalnya sebuah email atau gambar), atau bahkan sederetan paket yang berpindah melalui jaringan komputer.

Nama : Rio Permata

NIM : 182420108

Kelas : MTI B

IT Forensik

Ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat); Memerlukan keahlian dibidang IT (termasuk diantaranya hacking) dan alat bantu (tools) baik hardware maupun software.

IT Audit

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria berlaku, dan mengkomunikasikan hasilnya kepada pihak terkait.

Ada beberapa aspek yang diperiksa pada audit sistem teknologi informasi: Audit secara keseluruhan menyangkut efektifitas, efisiensi, availability system, reliability, confidentiality, dan integrity, serta aspek security. Selanjutnya adalah audit atas proses, modifikasi program, audit atas sumber data, dan data file. Audit IT sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

Perbedaan IT-Forensik dan IT-Audit
perbedaan antara IT Forensik dan IT-Audit terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya.

IT Audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.IT audit lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. IT Audit merupakan gabungan dari berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science. (Laporan) IT Audit bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan kebutuhan (integrity) dari sistem informasi organisasi.

Manfaat IT Audit

Manfaat penggunaan IT Audit dapat dikelompokkan menjadi 2 yaitu:

A. Manfaat dan tujuan pada saat Implementasi (Pre-Implementation Review)

1. Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
2. Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
3. Mengetahui apakah outcome sesuai dengan harapan manajemen.

B. Manfaat dan tujuan setelah sistem live (Post-Implementation Review)

1. Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
2. Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya.
3. Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
4. Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
5. Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
6. Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

sedangkan IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile.

Tujuan IT Forensik

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 :
    - Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
    - Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran

hukum.

IT Forensik

Definisi IT Forensik Ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat); Memerlukan keahlian dibidang IT (termasuk diantaranya hacking) dan alat bantu (tools) baik hardware maupun software.

Tujuan dari komputer forensik adalah untuk menjelaskan keadaan artefak digital saat ini . Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan komputer.

IT Audit

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria berlaku, dan mengkomunikasikan hasilnya kepada pihak terkait.

Ada beberapa aspek yang diperiksa pada audit sistem teknologi informasi: Audit secara keseluruhan menyangkut efektifitas, efisiensi, availability system, reliability, confidentiality, dan integrity, serta aspek security. Selanjutnya adalah audit atas proses, modifikasi program, audit atas sumber data, dan data file. Audit IT sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

Perbedaan IT-Forensik dan IT-Audit

Dari beberapa definisi di atas, dapat disimpulkan bahwa perbedaan antara IT Forensik dan IT-Audit terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya.

1. Pengertian

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.

1.1. Keuntungan Audit

Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
Mengukur tingkat efektifitas dari sistem Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang Menyediakan informasi untuk proses peningkatan
Meningkatkan saling memahami antar departemen dan antar individu Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen Keterampilan yang dibutuhkan

Audit skill : sampling, komunikasi, melakukan interview, mengajukan pertanyaan, mencatat
Generic knowledge : pengetahuan mengenai prinsip2 audit, prosedur dan teknik, sistem manajemen dan dokumen2 referensi, organisasi, peraturan2 yang berlaku
Specific knowledge : background IT/IS, bisnis, specialist technical skill, pengalaman audit sistem manajemen, perundangan

1.2. IT Forensik

Komputer Forensik adalah cabang dari ilmu forensik berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik.

Tujuan dari komputer forensik adalah untuk menjelaskan keadaan artefak digital saat ini . Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan komputer. ” Penjelasannya dapat secara langsung sebagai “informasi apa yang ada di sini?” dan sama detailnya dengan “apa urutan kejadian-kejadian yang bertanggung jawab atas situasi sekarang?”

Bidang komputer forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile .

1.3. Ada banyak alasan-alasan untuk menggunakan teknik komputer forensik:
/* Style Definitions */

table.MsoNormalTable
{mso-style-name:”Table Normal”;

mso-tstyle-rowband-size:0;
mso-tstyle-colband-size:0;
mso-style-noshow:yes;
mso-style-priority:99;
mso-style-qformat:yes;
mso-style-parent:””;

mso-padding-alt:0cm 5.4pt 0cm 5.4pt;

mso-para-margin-top:0cm;
mso-para-margin-right:0cm;
mso-para-margin-bottom:10.0pt;
mso-para-margin-left:0cm;
line-height:115%;
mso-pagination:widow-orphan;
font-size:11.0pt;
font-family:”Calibri”,”sans-serif”;
mso-ascii-font-family:Calibri;
mso-ascii-theme-font:minor-latin;
mso-hansi-font-family:Calibri;
mso-hansi-theme-font:minor-latin;}

Dalam kasus hukum, teknik komputer forensik sering digunakan untuk menganalisis sistem komputer milik terdakwa (dalam kasus pidana) atau milik penggugat (dalam kasus perdata).
Untuk memulihkan data jika terjadi kegagalan atau kesalahan hardware atau software.
Untuk menganalisa sebuah sistem komputer setelah terjadi perampokan, misalnya untuk menentukan bagaimana penyerang memperoleh akses dan apa yang penyerang itu lakukan.
Untuk mengumpulkan bukti untuk melawan seorang karyawan yang ingin diberhentikan oleh organisasi.
Untuk mendapatkan informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimasi kinerja, atau reverse-engineering.

1.4. Langkah-langkah khusus harus diambil ketika melakukan penyelidikan forensik jika diinginkan untuk menggunakan hasil dalam pengadilan hukum . Salah satu langkah yang paling penting adalah untuk memastikan bahwa bukti telah dikumpulkan secara akurat dan bahwa ada rantai yang jelas dengan tempat kejadian kepada penyidik — dan akhirnya ke pengadilan. Dalam rangka memenuhi kebutuhan untuk mempertahankan integritas dari bukti digital, pemeriksa-pemeriksa dari Inggris mengikuti pedoman-pedoman Association of Chief Police Officers (ACPO).

Perbedaan IT Audit dan IT Forensic dari segi tujuan

Tujuan IT Forensic :

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden/pelanggaran sistem infomasi yan setelah di verifikasi akan menjadi bukti yang akan digunakan dalam proses hukum.

2. Mengamankan dan menganalisa bukti digital dari kejahatan komputer

Tujuan IT Audit :

1. Ketersediaan informasi, apakah informasi dapat dengan mudah tersedia setiap saat

2. Kerahasiaan informasi, apakah informasi yang dihasilkan oleh sistem informasi dapat diakses oleh pihak-pihak yang berwenang

3. Integrity , apakah informasi yang dihasilkan akurat, handal dan tepat waktu

keduanya berpengaruh terhadap dampak dan tujuannya dalam mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi kriteria yang telah ditentukan

Perbedaan antara IT Audit dan IT Forensic

IT FORENSIK

IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital.

IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan. Bidang IT Forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile. * Menurut Noblett, yaitu berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer. * Menurut Judd Robin, yaitu penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin. * Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa. Alasan mengapa menggunakan IT 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. Siapa yang menggunakan IT forensic ? Network Administrator merupakan sosok pertama yang umumnya mengetahui keberadaan cybercrime sebelum sebuah kasus cybercrime diusut oleh pihak yang berwenang. Ketika pihak yang berwenang telah dilibatkan dalam sebuah kasus, maka juga akan melibatkan elemenelemen vital lainnya, antara lain: a. Petugas Keamanan (Officer/as a First Responder), Memiliki kewenangan tugas antara lain : mengidentifikasi peristiwa,mengamankan bukti, pemeliharaan bukti yang temporer dan rawan kerusakan. b. Penelaah Bukti (Investigator), adalah sosok yang paling berwenang dan memiliki kewenangan tugas antara lain: menetapkan instruksi-instruksi, melakukan pengusutan peristiwa kejahatan, pemeliharaan integritas bukti. c. Tekhnisi Khusus, memiliki kewenangan tugas antara lain : memeliharaan bukti yang rentan kerusakan dan menyalin storage bukti, mematikan(shuting down) sistem yang sedang berjalan, membungkus/memproteksi buktibukti, mengangkut bukti dan memproses bukti. IT forensic digunakan saat mengidentifikasi tersangka pelaku tindak kriminal untuk penyelidik, kepolisian, dan kejaksaan.

Tujuan IT Forensik

Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.

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 :

Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.

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

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

calpel 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.

Prodesur IT Forensik

Prosedur forensik yang umum digunakan, antara lain :Membuat copies dari keseluruhan log data, file, dan lain-lain yang dianggap perlu pada suatu media yang terpisah. Membuat copies secara matematis.Dokumentasi yang baik dari segala sesuatu yang dikerjakan.

Bukti yang digunakan dalam IT Forensics berupa :Harddisk.Floopy disk atau media lain yang bersifat removeable.Network system.

Metode/prosedure IT Forensik yang umum digunakan pada komputer ada dua jenis yaitu :

Search dan seizure : dimulai dari perumusan suatu rencana.

Identifikasi dengan penelitian permasalahan.

Membuat hipotesis.

Uji hipotesa secara konsep dan empiris.

Evaluasi hipotesa berdasarkan hasil pengujian dan pengujian ulang jika hipotesa tersebut jauh dari apa yang diharapkan.

Evaluasi hipotesa terhadap dampak yang lain jika hipotesa tersebut dapat diterima.

Pencarian informasi (discovery information). Ini dilakukan oleh investigator dan merupakan pencarian bukti tambahan dengan mengendalikan saksi secara langsung maupun tidak langsung.

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

Membuat fingerprint dari data secara matematis.

Membuat fingerprint dari copies secara otomatis.

Membuat suatu hashes masterlist

Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan.

IT Audit

Audit teknologi informasi 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.

B. Sejarah singkat Audit IT

Audit IT yang pada awalnya lebih dikenal sebagai EDP Audit (Electronic Data Processing) telah mengalami perkembangan yang pesat. Perkembangan Audit IT ini didorong oleh kemajuan teknologi dalam sistem keuangan, meningkatnya kebutuhan akan kontrol IT, dan pengaruh dari komputer itu sendiri untuk menyelesaikan tugas-tugas penting. Pemanfaatan teknologi komputer ke dalam sistem keuangan telah mengubah cara kerja sistem keuangan, yaitu dalam penyimpanan data, pengambilan kembali data, dan pengendalian. Sistem keuangan pertama yang menggunakan teknologi komputer muncul pertama kali tahun 1954. Selama periode 1954 sampai dengan 1960-an profesi audit masih menggunakan komputer. Pada pertengahan 1960-an terjadi perubahan pada mesin komputer, dari mainframe menjadi komputer yang lebih kecil dan murah.

Pada tahun 1968, American Institute of Certified Public Accountants (AICPA) ikut mendukung pengembangan EDP auditing. Sekitar periode ini pula para auditor bersama-sama mendirikan Electronic Data Processing Auditors Association (EDPAA). Tujuan lembaga ini adalah untuk membuat suatu tuntunan, prosedur, dan standar bagi audit EDP. Pada tahun 1977, edisi pertama Control Objectives diluncurkan. Publikasi ini kemudian dikenal sebagai Control

Objectives for Information and Related Technology (CobiT). Tahun 1994, EDPAA mengubah namanya menjadi Information System Audit (ISACA). Selama periode akhir 1960-an sampai saat ini teknologi TI telah berubah dengan cepat dari mikrokomputer dan jaringan ke internet. Pada akhirnya perubahan-perubahan tersebut ikut pula menentukan perubahan pada audit IT.

C. Jenis Audit IT.

1. Sistem dan aplikasi.

Memeriksa apakah sistem dan aplikasi sesuai dengan kebutuhan organisasi, berdayaguna, dan memiliki kontrol yang cukup baik untuk menjamin keabsahan, kehandalan, tepat waktu, dan keamanan pada input, proses, output pada semua tingkat kegiatan sistem.

2. Fasilitas pemrosesan informasi.

Memeriksa apakah fasilitas pemrosesan terkendali untuk menjamin ketepatan waktu, ketelitian, dan pemrosesan aplikasi yang efisien dalam keadaan normal dan buruk.

3. Pengembangan sistem.

Memeriksa apakah sistem yang dikembangkan mencakup kebutuhan obyektif organisasi.

4. Arsitektur perusahaan dan manajemen TI

Memeriksa apakah manajemen TI dapat mengembangkan struktur organisasi dan prosedur yang menjamin kontrol dan lingkungan yang berdaya guna untuk pemrosesan informasi.

5. Client/Server, telekomunikasi, intranet, dan ekstranet

Memeriksa apakah kontrol-kontrol berfungsi pada client, server, dan jaringan yang menghubungkan client dan server.

D. Metodologi Audit IT.

Dalam praktiknya, tahapan-tahapan dalam audit IT tidak berbeda dengan audit pada umumnya, sebagai berikut :

1. Tahapan Perencanaan.

Sebagai suatu pendahuluan mutlak perlu dilakukan agar auditor mengenal benar obyek yang akan diperiksa sehingga menghasilkan suatu program audit yang didesain sedemikian rupa agar pelaksanaannya akan berjalan efektif dan efisien.

2. Mengidentifikasikan reiko dan kendali.

Untuk memastikan bahwa qualified resource sudah dimiliki, dalam hal ini aspek SDM yang berpengalaman dan juga referensi praktik-praktik terbaik.

3. Mengevaluasi kendali dan mengumpulkan bukti-bukti.

Melalui berbagai teknik termasuk survei, interview, observasi, dan review dokumentasi.

4. Mendokumentasikan.

Mengumpulkan temuan-temuan dan mengidentifikasikan dengan auditee.

5. Menyusun laporan.

Mencakup tujuan pemeriksaan, sifat, dan kedalaman pemeriksaan yang dilakukan.

E. Alasan dilakukannya Audit IT.

Ron Webber, Dekan Fakultas Teknologi Informasi, monash University, dalam salah satu bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.

2. Kesalahan dalam pengambilan keputusan.

3. Resiko kebocoran data.

4. Penyalahgunaan komputer.

5. Kerugian akibat kesalahan proses perhitungan.

6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

F. Manfaat Audit IT.

1. Manfaat pada saat Implementasi (Pre-Implementation Review)

– Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.

– Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.

– Mengetahui apakah outcome sesuai dengan harapan manajemen.

2. Manfaat setelah sistem live (Post-Implementation Review)

– Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.

– Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya.

– Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.

– Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.

– Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.

– Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

G. Pengertian Audit Trail

Audit Trail merupakan salah satu fitur dalam suatu program yang mencatat semua kegiatan yang dilakukan tiap user dalam suatu tabel log. secara rinci. Audit Trail secara default akan mencatat waktu , user, data yang diakses dan berbagai jenis kegiatan. Jenis kegiatan bisa berupa menambah, merungubah dan menghapus. Audit Trail apabila diurutkan berdasarkan waktu bisa membentuk suatu kronologis manipulasi data.Dasar ide membuat fitur Audit Trail adalah menyimpan histori tentang suatu data (dibuat, diubah atau dihapus) dan oleh siapa serta bisa menampilkannya secara kronologis. Dengan adanya Audit Trail ini, semua kegiatan dalam program yang bersangkutan diharapkan bisa dicatat dengan baik.

1. Cara Kerja Audit Trail

a. Audit Trail yang disimpan dalam suatu tabel

b. Dengan menyisipkan perintah penambahan record ditiap query Insert, Update dan Delete

c. 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.

2. 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.

3. Hasil Audit Trail

Record Audit Trail disimpan dalam bentuk, yaitu :

a. Binary File – Ukuran tidak besar dan tidak bisa dibaca begitu saja

b. Text File – Ukuran besar dan bisa dibaca langsung

c. Tabel.

Perbedaan IT Audit dan IT Forensic

Nama : Arie Ansyah

NIM : 182420117

Mata Kuliah : IT AUDIT

Perbedaan IT Audit dan IT Forensik

IT Forensik

Definisi IT Forensik Ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat); Memerlukan keahlian dibidang IT (termasuk diantaranya hacking) dan alat bantu (tools) baik hardware maupun software.

Sumber: http://renianggraeniblog.blogspot.com/2010/06/it-forensik.html

IT Audit

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria berlaku, dan mengkomunikasikan hasilnya kepada pihak terkait.

Ada beberapa aspek yang diperiksa pada audit sistem teknologi informasi: Audit secara keseluruhan menyangkut efektifitas, efisiensi, availability system, reliability, confidentiality, dan integrity, serta aspek security. Selanjutnya adalah audit atas proses, modifikasi program, audit atas sumber data, dan data file. Audit IT sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

Sumber: http://www.scribd.com/doc/13263189/Audit-Sistem-Informasi

Perbedaan IT-Forensik dan IT-Audit

Dari beberapa definisi di atas, dapat disimpulkan bahwa perbedaan antara IT Forensik dan IT-Audit terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya.

IT Forensik

Definisi IT Forensik Ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat); Memerlukan keahlian dibidang IT (termasuk diantaranya hacking) dan alat bantu (tools) baik hardware maupun software.

IT Audit

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria berlaku, dan mengkomunikasikan hasilnya kepada pihak terkait.

Ada beberapa aspek yang diperiksa pada audit sistem teknologi informasi: Audit secara keseluruhan menyangkut efektifitas, efisiensi, availability system, reliability, confidentiality, dan integrity, serta aspek security. Selanjutnya adalah audit atas proses, modifikasi program, audit atas sumber data, dan data file. Audit IT sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

Perbedaan IT-Forensik dan IT-Audit
Dari beberapa definisi di atas, dapat disimpulkan bahwa perbedaan antara IT Forensik dan IT-Audit terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya.

IT Forensik :

Definisi IT Forensik Ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat); Memerlukan keahlian dibidang IT (termasuk diantaranya hacking) dan alat bantu (tools) baik hardware maupun software.

IT Audit :

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria berlaku, dan mengkomunikasikan hasilnya kepada pihak terkait.

Ada beberapa aspek yang diperiksa pada audit sistem teknologi informasi: Audit secara keseluruhan menyangkut efektifitas, efisiensi, availability system, reliability, confidentiality, dan integrity, serta aspek security. Selanjutnya adalah audit atas proses, modifikasi program, audit atas sumber data, dan data file. Audit IT sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

Perbedaan IT-Forensik dan IT-Audit
Dari beberapa definisi di atas, dapat disimpulkan bahwa perbedaan antara IT Forensik dan IT-Audit terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya.

JAWAB :

Perbedaan IT Audit dan IT Forensic

IT Audit

Pengertian IT 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. Audit menurut Arens, et al. (2003) yang diterjemahkan oleh kanto Santoso Setiawan dan Tumbur Pasaribu adalah proses pengumpulan dan pengevaluasian bukti-bukti tentang informasi ekonomi untuk menentukan tingkat kesesuaian informasi tersebut dengan criteria-kriteria yang telah ditetapkan, dan melaporkan hasil pemeriksaan tersebut.

Tujuan dilakukan IT Audit untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan kebutuhan (integrity) dari sistem informasi organisasi. Menurut Ron Webber (Dekan Fakultas Teknologi Informasi, Monash University) dalam bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Manfaat penggunaan IT Audit dapat dikelompokkan menjadi 2 yaitu:

1. Manfaat pada saat Implementasi (Pre-Implementation Review)

Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.

1. Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
2. Mengetahui apakah outcome sesuai dengan harapan manajemen.
3. Manfaat setelah sistem live (Post-Implementation Review)
    1. Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
    2. Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya.
    3. Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
    4. Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
    5. Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
    6. Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

IT Forensic

Pengertian IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital. Menurut Ruby Alamsyah (salah seorang ahli forensik IT Indonesia), digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggung jawabkan di

pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Tujuan dalam IT Forensik ialah

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 : Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi computer dan komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Manfaat mengapa menggunakan IT 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.

Perbedaan IT-Forensik dan IT-Audit

Dari beberapa definisi di atas, dapat disimpulkan bahwa perbedaan antara IT Forensik dan IT-Audit terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya. Audit IT merupakan urutan kronologis catatan audit, yang masing-masing berisikan bukti langsung yang berkaitan dengan yang dihasilkan dari pelaksanaan suatu proses bisnis atau fungsi sistem. Catatan audit biasanya hasil kerja dari kegiatan seperti transaksi atau komunikasi oleh orang-orang individu, sistem, rekening atau badan lainnya. Dengan adanya Audit IT diharapkan semua kronologis/kegiatan program dapat terekam dengan baik. Audit IT juga sangat membantu dalam IT forensik jika pengguna IT menderita kerugian terutama dalam bidang finansial akibat kejahatan komputer seperti Komputer fraud (Kejahatan atau pelanggaran dari segi sistem organisasi komputer) dan Komputer crime. (menggunakan media komputer dalam melakukan pelanggaran hukum). Sehingga memudahkan Penyidik IT forensik dalam menganalisa.

Nama : Dini Rahmadia

Nim : 182420134

IT Audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.IT audit lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer.. Salah satu Contohnya

IT Baseline Protection Manual (IT- Grundschutzhandbuch)

Dikembangkan oleh GISA: German Information Security Agency

Digunakan: evaluasi konsep keamanan & manua

Sedangkan

IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal.

IT Forensik

Definisi IT Forensik Ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat); Memerlukan keahlian dibidang IT (termasuk diantaranya hacking) dan alat bantu (tools) baik hardware maupun software.

Sumber: **http://renianggraeniblog.blogspot.com/2010/06/it-forensik.html**

IT Audit

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria berlaku, dan mengkomunikasikan hasilnya kepada pihak terkait.

Ada beberapa aspek yang diperiksa pada audit sistem teknologi informasi: Audit secara keseluruhan menyangkut efektifitas, efisiensi, availability system, reliability, confidentiality, dan integrity, serta aspek security. Selanjutnya adalah audit atas proses, modifikasi program, audit atas sumber data, dan data file. Audit IT sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

Sumber: **http://www.scribd.com/doc/13263189/Audit-Sistem-Informasi**

Perbedaan IT-Forensik dan IT-Audit

Dari beberapa definisi di atas, dapat disimpulkan bahwa perbedaan antara IT Forensik dan IT-Audit terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya.

IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. IT forensik dapat menjelaskan keadaan artefak digital terkini. Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan

Nama : Fajar Prayoga

Nim : 182420136

Kelas : MTI 20A

Jawaban :

Audit IT 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 organisasiny

Proses IT Audit

Mengumpulkan dan mengevaluasi bukti-bukti bagaimana system informasi dikembangkan, dioperasikan, diorganisasikan, serta bagaimana praktek dilaksanakan:

a. Apakah IS melindungi aset institusi: asset protection, availability

b. Apakah integritas data dan sistem diproteksi secara cukup (security, confidentiality)

c. Apakah operasi sistem efektif dan efisien dalam mencapai tujuan organisasi, dan lain-lain (coba cari pertanyaan2 lain).

Salah satu software yang dapat dijadikan alat bantu dalam pelaksanaan audit teknologi informasi

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. ACL for Windows (sering disebut ACL) adalah sebuah software TABK (TEKNIK AUDIT BERBASIS KOMPUTER) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektro.

IT Forensik yaitu penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal. 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.

Tujuan IT Forensik

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 :
    - Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
    - Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Metode yang sering digunakan dalam pendekatan Audit Forensik IT yaitu, Audit around the computer adalah pendekatan audit dimana auditor menguji keandalan sebuah informasi yang dihasilkan oleh komputer dengan terlebih dahulu mengkalkulasikan hasil dari sebuah transaksi yang dimasukkan dalam sistem. Kemudian, kalkulasi tersebut dibandingkan dengan output yang dihasilkan oleh sistem. Apabila ternyata valid dan akurat, diasumsikan bahwa pengendalian sistem telah efektif dan sistem telah beroperasi dengan baik. Jenis audit ini dapat digunakan ketika proses yang terotomasi dalam sistem cukup sederhana. Kelemahan dari audit ini adalah bahwa audit around the computer tidak menguji apakah logika program dalam sebuah sistem benar. Selain itu, jenis pendekatan audit ini tidak menguji bagaimana pengendalian yang terotomasi menangani input yang mengandung error. Dampaknya, dalam lingkungan IT yang komplek, pendekatan ini akan tidak mampu untuk mendeteksi banyak error.

IT AUDIT adalah proses sistematis dan obyektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan & infrastruktur IT/SI yang menjadi obyek audit, guna mencari asersi, temuan kesalahan/misimplementasi pada proses, menilai seberapa jauh tindakan dan proses sudah sesuai dengan standar operasional dan ketentuan yang berlaku, kemudian mengkomunikasikan hasilnya dengan pihak terkait yang membutuhkan.

IT FORENSIK adalah cabang dari ilmu forensik yang berhubungan dengan pengumpulan data, fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (biasanya menggunakan *cause-effect relationship*) dimana prosesnya memerlukan keahlian IT (termasuk diantaranya *hacking*) dan alat bantu baik *hardware* maupun *software*.

Perbedaan dasarnya terletak pada cara pengumpulan dan evaluasi bukti-bukti bagaimana SI/TI dikembangkan, dioperasikan, diorganisasikan, serta dilaksanakan dalam prakteknya.

Tujuan IT Audit lebih kepada menggali informasi dan melakukan penilaian kesesuaian proses dan infrastruktur IT yang ada dengan standar yang sudah ditetapkan sebelumnya, sehingga diharapkan visi dan misi dari target audit mampu terlaksana tanpa hambatan. Kata kunci IT audit adalah bisnis. Sedangkan IT Forensik bertujuan menggali fakta & informasi dari artefak/struktur/komponen IT/IS yang sudah rusak, terhapus, termanipulasi dan semuanya berkaitan dengan proses dan barang bukti hukum (*evidence*). Kata kunci IT forensik adalah penegakan hukum dan investigasi.

Disarikan dari :

http://ndaysen.blogspot.com/2011/04/perbedaan-it-forensik-dengan-it-audit.html

https://tommykur.wordpress.com/2011/04/12/perbedaan-it-audit-dan-it-forensik/

Nama : **Hari Febriadi**
NIM : **182420127**
Kelas : **MTI.20A**

Sebelum saya menjelas kan beberapa **perbedaan, dampak dan tujuan dari IT Audit dan IT Forensic** saya akan memaparkan nya dalam beberapa sub bagian secara detail :

- **PENGERTIAN SECARA UMUM IT AUDIT**

IT Audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.IT audit lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer

- **JENIS IT AUDIT**

1. Sistem dan aplikasi
2. Fasilitas pemrosesan informasi
3. Pengembangan sistem
4. Arsitektur perusahaan dan manajemen TI
5. Client/Server, telekomunikasi, intranet, dan ekstranet

- **DAMPAK PENGUNAAN IT AUDIT**
  Ron Webber (Dekan Fakultas Teknologi Informasi, Monash University) dalam bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

- **TUJUAN IT AUDIT**

Manfaat penggunaan IT Audit dapat dikelompokkan menjadi 2 yaitu:

1. Manfaat pada saat Implementasi (**Pre-Implementation Review**)

- Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
- Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
- Mengetahui apakah outcome sesuai dengan harapan manajemen.

1. Manfaat setelah sistem live (**Post-Implementation Review**)

- Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
- Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan

anggaran pada periode berikutnya.
- Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
- Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
- Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
- Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.
- **CONTOH METODOLOGI IT AUDIT**

BSI (Bundesamt for Sicherheit in der Informationstechnik)

1. IT Baseline Protection Manual (IT- Grundschutzhandbuch)
2. Dikembangkan oleh GISA: German Information Security Agency
3. Digunakan: evaluasi konsep keamanan & manual
4. Metodologi evaluasi tidak dijelaskan
5. Mudah digunakan dan sangat detail sekali
6. Tidak cocok untuk analisis resiko
7. Representasi tidak dalam grafik yg mudah dibaca

- **IT AUDIT TOOLS**

Beberapa tool yang dipergunakan dalam IT Audit adalah:

- ACL (Audit Command Language)
- Picalo
- Powertech Compliance Assessment Powertech
- Nipper
- Nessus
- Metasploit Framework
- NMAP
- Wireshark

- **PENGERTIAN UMUM IT FORENSIC**

IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital

- **Tujuan IT Forensik**

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 :
3. Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
4. Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

- **Alasan Penggunaan IT Forensik**

1. Dalam kasus hukum, teknik komputer forensik sering digunakan untuk menganalisis sistem komputer milik terdakwa (dalam kasus pidana) atau milik penggugat (dalam kasus perdata).
2. Untuk memulihkan data jika terjadi kegagalan atau kesalahan hardware atausoftware.
3. Untuk menganalisa sebuah sistem komputer setelah terjadi perampokan, misalnya untuk menentukan bagaimana penyerang memperoleh akses dan apa yang penyerang itu lakukan.
4. Untuk mengumpulkan bukti untuk melawan seorang karyawan yang ingin diberhentikan oleh organisasi.
5. Untuk mendapatkan informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimasi kinerja, atau reverse-engineering.

- **Terminologi IT Forensik**

A. Bukti digital (digital evidence)

Bukti digital (digital evidence) adalah informasi yang didapat dalam bentuk atau format digital, contohnya e-mail.

B. Elemen kunci forensik

Elemen kunci forensik dalam teknologi informasi, antara lain :

1. Identifikasi dari bukti digital. Tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya.
2. Penyimpanan bukti digital. Ttahapan yang paling kritis dalam forensik. Bukti digital dapat saja hilang karena penyimpanannya yang kurang baik.
3. Analisa bukti digital. Tahapan pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital.
4. Presentasi bukti digital. Proses persidangan dimana bukti digital akan diuji dengan kasus yang ada. Presentasi disini berupa penunjukkan bukti digital yang berhubungan dengan kasus yang disidangkan.

- **Investigasi Kasus Teknologi Informasi**
  - Prosedur forensik yang umum digunakan, antara lain :Membuat copies dari keseluruhan log data, file, dan lain-lain yang dianggap perlu pada suatu media yang terpisah. Membuat copies secara matematis.Dokumentasi yang baik dari segala sesuatu yang dikerjakan.
  - Bukti yang digunakan dalam IT Forensics berupa :Harddisk.Floopy disk atau media lain yang bersifat removeable.Network system.
  -
- **Tools IT Forensik**

1. Antiword.
2. Autopsy.
3. Binhash.
4. Sigtool.
5. ChaosReader.
6. Chkrootkit.
7. Dcfldd.
8. GNU Ddrescue
9. Foremost.
10. Gqview.
11. Galleta.
12. Ishw (Hardware Lister).
13. Pasco.

14. Scalpel.

Definisi IT Forensik
*Definisi sederhana y*aitu penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal.
*Menurut Noblett "*berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer"
*Menurut Judd Robin "*penerapan secara sederhana dari penyidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin"

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, yaitu kejahatan atau pelanggaran dari segi sistem organisasi komputer.
2. Komputer Crime, merupakan kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Terminologi IT Forensik
A. Bukti digital (digital evidence), adalah informasi yang didapat dalam bentuk atau format digital, contohnya e-mail.
B. Empat elemen kunci forensik dalam teknologi informasi, antara lain :
   1. Identifikasi dari bukti digital, merupakan tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya.
   2. Penyimpanan bukti digital, termasuk tahapan yang paling kritis dalam forensik. Bukti digital dapat saja hilang karena penyimpanannya yang kurang baik.
   3. Analisa bukti digital, pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital.
   4. Presentasi bukti digital, proses persidangan dimana bukti digital akan diuji dengan kasus yang ada. Presentasi disini berupa penunjukkan bukti digital yang berhubungan dengan kasus yang disidangkan.

Prinsip IT Forensik
1. Forensik bukan proses Hacking
2. Data yang didapat harus dijaga jangan berubah
3. Membuat image dari HD / Floppy / USB-Stick / Memory-dump adalah prioritas tanpa merubah isi, kadang digunakan hardware khusus
4. Image tsb yang diotak-atik (hacking) dan dianalisis – bukan yang asli
5. Data yang sudah terhapus membutuhkan tools khusus untuk merekonstruksi
6. Pencarian bukti dengan: tools pencarian teks khusus, atau mencari satu persatu dalam image

IT AUDIT
adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal. Audit IT lebih dikenal dengan istilah *EDP Auditing* (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. Salah satu penggunaan istilah tersebut adalah untuk menjelaskan proses penelahan dan evaluasi pengendalian-pengendalian internal dalam EDP. Jenis aktivitas ini disebut sebagai auditing melalui komputer. Penggunaan istilah lainnya adalah untuk

menjelaskan pemanfaatan komputer oleh auditor untuk melaksanakan beberapa pekerjaan audit yang tidak dapat dilakukan secara manual. Jenis aktivitas ini disebut audit dengan komputer.
Audit IT sendiri merupakan gabungan dari 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.

Proses IT Audit
Mengumpulkan dan mengevaluasi bukti-bukti bagaimana system informasi dikembangkan, dioperasikan, diorganisasikan, serta bagaimana praktek dilaksanakan:
a. Apakah IS melindungi aset institusi: asset protection, availability
b. Apakah integritas data dan sistem diproteksi secara cukup (security, confidentiality)?
c. Apakah operasi sistem efektif dan efisien dalam mencapai tujuan organisasi, dan lain-lain (coba cari pertanyaan2 lain).

Alasan Dilakukannya IT Audit
Ron Webber, Dekan Fakultas Teknologi Informasi, monash University, dalam salah satu bukunya *Information System Controls and Audit* (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :
1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Manfaat IT Audit
A. Manfaat pada saat Implementasi (Pre-Implementation Review)
   1. Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
   2. Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
   3. Mengetahui apakah outcome sesuai dengan harapan manajemen.
B. Manfaat setelah sistem live (Post-Implementation Review)
   1. Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
   2. Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya.
   3. Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
   4. Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
   5. Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
   6. Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

IT Audit

- Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
- Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
- Mengukur tingkat efektifitas dari sistem
- Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang
- Menyediakan informasi untuk proses peningkatan
- Meningkatkan saling memahami antar departemen dan antar individu
- Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen

Keterampilan yang dibutuhkan

- Audit skill : sampling, komunikasi, melakukan interview, mengajukan pertanyaan, mencatat
- Generic knowledge : pengetahuan mengenai prinsip2 audit, prosedur dan teknik, sistem manajemen dan dokumen2 referensi, organisasi, peraturan2 yang berlaku
- Specific knowledge : background IT/IS, bisnis, specialist technical skill, pengalaman audit sistem manajemen, perundangan

IT Forensik

Komputer Forensik adalah cabang dari ilmu forensik berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik.

Tujuan dari komputer forensik adalah untuk menjelaskan keadaan artefak digital saat ini . Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan komputer. ” Penjelasannya dapat secara langsung sebagai “informasi apa yang ada di sini?” dan sama detailnya dengan “apa urutan kejadian-kejadian yang bertanggung jawab atas situasi sekarang?”

Bidang komputer forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile.

Terima kasih, salam.

Perbedaan IT Audit dan 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.

Tujuan Audit teknologi informasi adalah untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya.

Keuntungan Audit

- Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
- Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
- Mengukur tingkat efektifitas dari sistem
- Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang
- Menyediakan informasi untuk proses peningkatan
- Meningkatkan saling memahami antar departemen dan antar individu
- Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen

Keterampilan yang dibutuhkan

- Audit skill : sampling, komunikasi, melakukan interview, mengajukan pertanyaan, mencatat
- Generic knowledge : pengetahuan mengenai prinsip2 audit, prosedur dan teknik, sistem manajemen dan dokumen2 referensi, organisasi, peraturan2 yang berlaku
- Specific knowledge : background IT/IS, bisnis, specialist technical skill, pengalaman audit sistem manajemen, perundangan

IT Forensik

Komputer Forensik adalah cabang dari ilmu forensik berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik.

Tujuan dari IT Forensik adalah untuk menjelaskan keadaan artefak digital saat ini . Artefak Digital dapat mencakup sistem komputer, media penyimpanan (seperti hard disk atau CD-ROM, dokumen elektronik (misalnya pesan email atau gambar JPEG) atau bahkan paket-paket yang secara berurutan bergerak melalui jaringan komputer. ” Penjelasannya dapat secara langsung sebagai “informasi apa yang ada di sini?” dan sama detailnya dengan “apa urutan kejadian-kejadian yang bertanggung jawab atas situasi sekarang?”

Bidang komputer forensik juga memiliki cabang-cabang di dalamnya seperti firewall forensik, forensik jaringan , database forensik, dan forensik perangkat mobile .

Ada banyak alasan-alasan untuk menggunakan teknik komputer forensik:

Dalam kasus hukum, teknik komputer forensik sering digunakan untuk menganalisis sistem komputer milik terdakwa (dalam kasus pidana) atau milik penggugat (dalam kasus perdata).
Untuk memulihkan data jika terjadi kegagalan atau kesalahan hardware atau software.
Untuk menganalisa sebuah sistem komputer setelah terjadi perampokan, misalnya untuk menentukan bagaimana penyerang memperoleh akses dan apa yang penyerang itu lakukan.
Untuk mengumpulkan bukti untuk melawan seorang karyawan yang ingin diberhentikan oleh organisasi.
Untuk mendapatkan informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimasi kinerja, atau reverse-engineering.

Langkah-langkah khusus harus diambil ketika melakukan penyelidikan forensik jika diinginkan untuk menggunakan hasil dalam pengadilan hukum . Salah satu langkah yang paling penting adalah untuk memastikan bahwa bukti telah dikumpulkan secara akurat dan bahwa ada rantai yang jelas dengan tempat kejadian kepada penyidik — dan akhirnya ke pengadilan. Dalam rangka memenuhi kebutuhan untuk mempertahankan integritas dari bukti digital, pemeriksa-pemeriksa dari Inggris mengikuti pedoman-pedoman Association of Chief Police Officers (ACPO).

Nama : Laiatur Rahmi

Nim :182420118

Mata Kuliah : IT AUDIT

Dosen : Dr. Widya Cholil

Perbedaan IT audit dan IT forensic

Dari segi Pengertian

IT Audit adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.

IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital. Komputer forensik juga dikenal sebagai Digital Forensik yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital. IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal.

Dari segi tujuan

IT Audit bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan kebutuhan (integrity) dari sistem informasi organisasi. Sedangkan

Tujuan IT Forensik :

1. Mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.
2. 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 :

- Komputer fraud : kejahatan atau pelanggaran dari segi sistem organisasi komputer.
- Komputer crime: kegiatan berbahaya dimana menggunakan media komputer dalam melakukan pelanggaran hukum.

Dari segi alasan penggunaan

Alasan Penggunakan IT Audit

Ron Webber (Dekan Fakultas Teknologi Informasi, Monash University) dalam bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan.
3. Resiko kebocoran data.
4. Penyalahgunaan komputer.
5. Kerugian akibat kesalahan proses perhitungan.
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

Alasan Penggunaan IT Forensik

1. Dalam kasus hukum, teknik komputer forensik sering digunakan untuk menganalisis sistem komputer milik terdakwa (dalam kasus pidana) atau milik penggugat (dalam kasus perdata).
2. Untuk memulihkan data jika terjadi kegagalan atau kesalahan hardware atausoftware.
3. Untuk menganalisa sebuah sistem komputer setelah terjadi perampokan, misalnya untuk menentukan bagaimana penyerang memperoleh akses dan apa yang penyerang itu lakukan.
4. Untuk mengumpulkan bukti untuk melawan seorang karyawan yang ingin diberhentikan oleh organisasi.
5. Untuk mendapatkan informasi tentang bagaimana sistem komputer bekerja untuk tujuan debugging, optimasi kinerja, atau reverse-engineering