IT AUDIT TRAIL, REAL TIME AUDIT, DAN IT FORENSIK

Audit IT lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing) yang 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. Pada audit IT sendiri berhubungan dengan berbagai macam-macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science. Tujuan dari audit IT adalah untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan keutuhan (integrity) dari sistem informasi organisasi yang bersifat online atau real time. Pada Real Time Audit (RTA) dapat juga menyediakan teknik ideal untuk memungkinkan mereka yang bertanggung jawab untuk meningkatkan kinerja karena sistem ini tidak mengganggu atau investor dapat memperoleh informasi yang mereka butuhkan tanpa menuntut waktu manajer.

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

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

Catatan Audit biasanya hasil dari kegiatan seperti transaksi atau komunikasi oleh orang-orang individu, sistem, rekening atau badan lainnya. Audit IT sendiri berhubungan dengan berbagai macam ilmu, antara lain Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science. Audit IT bertujuan untuk meninjau dan

mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan keutuhan (integrity) dari sistem informasi organisasi yang bersifat online atau real time.

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

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

Dalam penelitian keperawatan, itu mengacu pada tindakan mempertahankan log berjalan atau jurnal dari keputusan yang berkaitan dengan sebuah proyek penelitian, sehingga membuat jelas langkah-langkah yang diambil dan perubahan yang dibuat pada protokol asli. Dalam akuntansi, mengacu pada dokumentasi transaksi rinci mendukung entri ringkasan buku. Dokumentasi ini mungkin pada catatan kertas atau elektronik. Proses yang menciptakan jejak audit harus selalu berjalan dalam mode istimewa, sehingga dapat mengakses dan mengawasi semua tindakan dari semua pengguna, dan user normal tidak bisa berhenti / mengubahnya. Selanjutnya, untuk alasan yang sama, berkas jejak atau tabel database dengan jejak tidak boleh diakses oleh pengguna normal.

Dalam apa yang berhubungan dengan audit trail, itu juga sangat penting untuk mempertimbangkan isu- isu tanggung jawab dari jejak audit Anda, sebanyak dalam kasus sengketa, jejak audit ini dapat dijadikan sebagai bukti atas kejadian beberapa.Perangkat lunak ini dapat beroperasi dengan kontrol tertutup dilingkarkan, atau sebagai sebuah 'sistem tertutup, "seperti yang disyaratkan oleh banyak perusahaan ketika menggunakan sistem Audit Trail.

Tools yang Digunakan Untuk IT Audit

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

1. ACL

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

2. Picalo

Picalo merupakan sebuah software CAAT (Computer Assisted Audit Techniques) seperti halnya ACL

yang dapat dipergunakan untuk menganalisa data dari berbagai macam sumber. http://www.picalo.org/

3. Powertech Compliance Assessment

Powertech Compliance Assessment merupakan automated audit tool yang dapat dipergunakan untuk mengaudit dan mem-benchmark user access to data, public authority to libraries, user security, system

security, system auditing dan administrator rights (special authority) sebuah server AS/400.

http://www.powertech.com/

4. Nipper

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

5. Nessus

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

6. Metasploit

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

7. NMAP

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

8. Wireshark

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

Real Time Audit merupakan suatu sistem yang berfungsi untuk mengawasi kegiatan teknis dan keuanagan sehingga dapat memberikan penilaian yang transparan status saat ini dari semua kegiatan, di mana pun mereka berada.

Dari sumber lain yang dilihat dari penerapan Real Time Audit dalam transaksi:

transaksi secara individual dientri melalui peralatan terminal, divalidasi dan digunakan untuk meng-update dengan segera filekomputer. Hasil pengolahan ini kemudian tersedia segera untuk permintaan keterangan atau laporan. Jadi dapat disimpulkan bahwa Real time audit adalah suatu kegiatan evaluasi dan pemeriksaan dokumen, transaksi dalam suatu sistem organisasi yang dilakukan secara langsung atau realtime secara online, hal ini berbeda dengan internal audit yang memiliki pengertian yaitu audit yang pelaksanaan nya dilakukan oleh pegawai pemeriksa yang berada dalam organisasi tersebut.

Namun ada juga yang mendefinisikan Real Time Audit adalah sebuah sistem manajemen kegiatan online yang menggabungkan sistem kegiatan manajemen dengan sistem monitoring dan evaluasi. Dalam penggunaannya, Real Time Audit sangat membantu dalam penghematan biaya overhead administrasi yang timbul dari penggunaan Real Time Audit yang signifikan, seiring dengan meningkatnya kemajuan teknologi, teknik kualitas dari pelaporan dan kontrol manajemen meningkatkan menyediakan kedua manajer dan pemilik modal dengan cara untuk mencari kegiatan yang dibiayai dari sudut pandang beberapa manfaat dengan minimum atau tidak ada konsumsi waktu di bagian aktivitas manajer. Oleh karena itu Real Time Audit sangat berguna sekali dalam membantu kita mengaudit suatu administrasi. Real Time Audit menggabungkan logis prosedural merekam dan sederhana dari perencanaan dan komitmen dana. prosedur analitik yang sedang berlangsung memberikan alert tepat waktu untuk mencegah pengeluaran yang tidak sesuai. Dan ilmu yang mempelajari audit sistem informasi yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya disebut IT Forensik. Dan metode audit yang bisa digunakan adalah COBIT.

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.

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

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

o 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).

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

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

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

o 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.

Pengertian dari Komputer Forensik adalah :

Definisi sederhana : penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem computer dengan menggunakan software dan tool untuk mengambil dan memelihara barang bukti tindakan kriminal.

Menurut Judd Robin, seorang ahli komputer forensik : “Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin”.

New Technologies memperluas definisi Judd Robin dengan: “Komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi bukti-bukti komputer yang tersimpan dalam wujud informasi magnetik”.

Menurut Dan Farmer & Wietse Venema : “Memperoleh dan menganalisa data dengan cara yang bebas dari distorsi atau sebisa mungkin, untuk merekonstruksi data atau apa yang telah terjadi pada waktu sebelumnya di suatu sistem”.

Prosedur dalam Forensik IT

Prosedur Forensik yang umum digunakan adalah :

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

2. Membuat finerptint dari data secara matematis.

3. Membuat fingerprint dari copies secvara otomatis.

4. Membuat suatu hashes masterlist

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

Sedangkan menurut metode Search dan Seizure adalah :

1. Identifikasi dan penelitian permasalahan.

2. Membaut hipotesa.

3. Uji hipotesa secara konsep dan empiris.

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

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

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.

Daftar Pustaka

http://ibenuh.blogspot.com/2013/03/pengertian-tentang-it-audit-trail-real.html

http://rainzacious.blogspot.com/2013/03/penulisan-pengertian-audit-trail-real.html

http://kuncungku.wordpress.com/2012/05/01/definisi-it-forensik/