Jurnal Ilmiah Akuntansi
Vol.V No.2, November 2006
Hal 65-80

# AUDIT FORENSIK: STRATEGI UNTUK MEMINIMALKAN *INTERNET FRAUD*

**Meythi**
*Dosen Fakultas Ekonomi Jurusan Akuntansi, Univ.Kristen Maranatha*

**ABSTRAK**. *Internet fraud* sangat meresahkan dunia e-commerce karena kejahatan ini menggangu keamanan transaksi. Hal ini mengakibatkan keraguan konsumen dalam melakukan transaksi di internet dan mempengaruhi bisnis yang dilakukan di internet. Di Indonesia masalah ini mengakibatkan pemblokiran terhadap transaksi–transaksi yang dilakukan oleh orang Indonesia di internet karena ditakutkan bahwa transaksi tersebut dilakukan oleh orang yang tidak berhak. Strategi untuk meminimalkan internet fraud maka digunakan audit forensik.

**Kata Kunci**: *Internet fraud*, audit forensik.

## PENDAHULUAN

Akhir-akhir ini, media massa seakan-akan tidak pernah berhenti dalam menyuguhkan potret *internet fraud*, mulai dari pencurian kartu kredit, *hacking* beberapa situs, penyadapan transmisi data orang lain, misalnya email, dan pemanipulasian data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program komputer.

Merajalelanya *internet fraud* juga tidak lepas dari lemahnya *control system* di negara ini, yang antara lain meliputi undang-undang atau hukum, sistem pengendalian internal, dan akuntan publik. Hukum merupakan bagian integral dari *control system* yang berfungsi represif tetapi juga preventif, tidak lagi menjadi hal yang menakutkan bagi pelaku *internet fraud*. Ganjaran hukuman yang diberikan terhadap hacker sering jauh lebih ringan dibanding pelaku kejahatan jenis lain. Kemungkinan lain, adalah tidak takutnya hacker terhadap akuntan publik. Apabila ditelusuri lebih lanjut, hal tersebut dapat terjadi karena keberhasilan hacker berulang kali mampu mengelabui dan lolos dari pemeriksaan akuntan publik. Ahli kriminologi berteori bahwa hacker menerima penguatan positif, berupa bertambahnya kepercayaan diri, apabila kecurangan yang dilakukannya tidak terdeteksi. Karena hasil yang diperoleh melalui tindakan *internet fraud* sering melebihi risiko penahanan dan hukuman yang akan diterimanya, tidaklah mengherankan apabila hacker memiliki kepercayaan diri untuk mengulangi perbuatannya.

Lalu dimanakah tanggung jawab dan peran akuntan sebagai pihak yang berkompeten? Apakah *internet fraud* yang dilakukan oleh pelaku-pelaku kecurangan terlalu sulit untuk dideteksi ataukah audit memang tidak ditujukan untuk mengungkap suatu kecurangan?

Tujuan dari penulisan artikel ini adalah untuk memaparkan *internet fraud* dan audit forensik sebagai strategi untuk meminimalkan *internet fraud*. MetodE ini dilakukan melalui studi kepustakaan, yaitu dengan cara mengumpulkan dan menganalisa *text book* dan artikel-artikel terkait.

## PERMASALAHAN

Akuntan publik memiliki tanggung jawab untuk mendeteksi kecurangan sebagaimana dirumuskan di PSA 32. Tanggung jawab tersebut dapat diartikan sebagai kewajiban hukum akuntan publik. Yang dimaksud kewajiban hukum akuntan publik adalah bahwa dalam melaksanakan tugas profesionalnya kepada pihak lain, akuntan memiliki kewajiban untuk melaksanakan kemahiran profesionalnya dengan hati-hati dan penuh tanggung jawab. Akuntan harus menyadari bahwa jasa yang diberikan diandalkan oleh pihak lain untuk keputusan bisnisnya. Karena disebut kewajiban hukum, maka itu berarti akuntan publik dapat dimintai pertanggungjawaban secara hukum apabila pihak pemakai jasa akuntan merasa dirugikan karena mengandalkan laporan akuntan publik.

Hal ini juga berlaku dalam masalah pendeteksian *internet fraud*. Artinya, akuntan publik dapat dituntut secara hukum apabila lalai atau gagal menemukan *internet fraud*. Meskipun tanggung jawab akuntan hanya sebatas SPAP, namun cukup riskan apabila akuntan tidak berusaha untuk menambah pengetahuannya tentang *internet fraud*. Padahal *internet fraud* sendiri semakin hari semakin meningkat baik dari segi kuantitas maupun kualitas.

## TINJAUAN PUSTAKA

**Apakah Internet Fraud itu?**

Confederation Asian and Pasific Accountants (CAPA) mendefinisikan *internet fraud* sebagai "*...any act of dishonesty or deception carried out through the use of the internet, or directed at the technologies that support the internet*" (CAPA, 2002). US Department of Justice mendefinisikan *internet fraud* sebagai "*...any type of fraud scheme that uses one or more components of the internet-such as chat room, e-mail, massage boards, or web sites-to present fraudelent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme*" (US Department of Justice, 2001). Jadi *internet fraud* adalah suatu peluang bagi individu atau sekelompok orang yang memiliki tingkat keahlian tertentu untuk memperoleh keuntungan finansial dengan cara melakukan *fraud* lewat internet.

*Internet fraud* ini bisa dilakukan oleh orang yang berada di wilayah suatu negara dan bisa juga dilakukan oleh orang yang berada di luar wilayah suatu negara yang berkolaborasi dengan pihak yang berada di wilayah negara itu. Kemampuan global dari internet dan ekspansi yang cepat dari *e-commerce* membuat kita tidak dapat mengelak dari pengaruh *internet fraud*. Risiko ini akan sangat berdampak terutama bagi negara-negara yang tingkat keahlian teknologinya rendah dan negara-negara yang tidak memiliki cukup dana untuk melakukan pencegahan terhadap *fraud* tersebut.

**Jenis-Jenis Internet Fraud**

Menurut US Department of Justice (2001) jenis-jenis *internet fraud* antara lain:

a. Skema lelang dan *retail online*
   Skema ini berisi penawaran item-item bernilai tinggi yang mungkin menarik perhatian konsumen. Skema ini membujuk korbannya untuk mengirimkan sejumlah uang untuk mendapatkan item-item yang dijanjikan, tetapi kemudian pelaku tidak mengirimkan apa-apa atau mengirim hanya suatu item yang nilainya jauh lebih rendah dari yang dijanjikan.
b. Skema peluang bisnis/"*work-at-home*" *online*
   Skema ini menggunakan internet untuk mempromosikan peluang bisnis yang memungkinkan seseorang memperoleh ribuan dolar dalam sebulan dengan "*work-at-home*". Skema ini umumnya mensyaratkan korbannya untuk membayar dari US$35 sampai ratusan dolar atau lebih, akan tetapi kemudian pelaku tidak mengirimkan material atau informasi yang dibutuhkan untuk membuat peluang "*work-at-home*" itu berjalan.

c. Pencurian identitas dan *fraud*
Skema ini melibatkan pencurian identitas, yaitu memperoleh dan menggunakan data personal orang lain untuk melakukan *fraud* atau penipuan demi keuntungan ekonomis. Sebagai contoh, seorang pelaku memperoleh nama dan nomor *social security* sejumlah pejabat militer US dari *web sites*, dan kemudian menggunakan lebih dari seratus nama dan nomor tersebut untuk membuat aplikasi *credit card* via internet pada Delaware Bank.

d. Skema investasi online.
Skema investasi online ini umumnya berupa skema manipulasi pasar. Pelaku menggunakan dua metode untuk mencoba memanipulasi *security market* untuk kepentingan pribadi. Metode pertama disebut "*pump-and-dump*". Metode ini dilakukan dengan menyebarkan informasi yang salah sebagai usaha untuk menaikkan secara dramatis harga saham yang sedikit diperdagangkan atau saham dari *shell companies* (*the* "*pump*"). Kemudian dengan segera pelaku menjual saham-saham yang mereka miliki (*the* "*dump*") untuk merealisasikan profit substansial sebelum harga saham tersebut kembali pada tingkat yang rendah. Pembeli lain yang tidak sadar akan kesalahan informasi akan menjadi korban ketika harga saham kembali turun. Metode kedua disebut metode "*scalping*". Metode ini menggunakan pendekatan sejenis dengan metode pertama, yaitu dengan menyebarkan informasi yang salah dalam usaha untuk menurunkan harga saham perusahaan tertentu. Umumnya penyebaran informasi itu dilakukan dengan mengirimkan email ke sejumlah buletin internet.

e. Skema kartu kredit
Skema ini melibatkan penggunaan nomor kartu kredit yang diperoleh secara ilegal untuk memesan sejumlah barang atau jasa secara *online*.

f. Pembajakan informasi
*Fraud* jenis ini dilakukan dengan membuat copy data ilegal dengan melanggar hak cipta. Data yang dibajak dapat berupa data audio dan data visual seperti musik dan film. Data-data tersebut kemudian "dipajang" di internet yang kemudian bisa diakses dan di-*download* secara gratis. Sebagai contoh copy film James Bond "*The World is Not Enough*" sudah tersedia di internet secara gratis sebelum *release* resmi film tersebut.
Selain data audio dan visual, pembajakan *software* juga sering terjadi. Secara global kerugian yang dialami perusahaan software akibat pembajakan ini mencapai 11,7 miliar dolar Amerika pada tahun 2000. Kerugian perusahaan software di Asia Pasifik mencapai lebih dari 4 miliar dolar Amerika pada tahun 2000 atau naik 1 miliar dolar Amerika dari tahun 1999. Memang tidak semua pembajakan terjadi lewat internet, tetapi pencurian material hak cipta dengan men-*download* dari internet merupakan masalah yang perlu diperhatikan.

g. Skema Lain

Masih ada skema-skema lain yang merupakan *internet fraud* seperti *multilevel marketing* dan lain-lain.

Berikut ini Tabel sepuluh jenis *internet fraud* yang paling sering dilakukan pada tahun 1999 dan 2000.

**Tabel 1 Top 10 Jenis Internet Fraud tahun 1999-2000**

| Top 10 fraud types 1999 Type | % | Top 10 fraud types 2000 Type | % |
|---|---|---|---|
| Online auction | 87 | Online auction | 78 |
| General merchandise sales | 7 | General merchandise sales | 10 |
| Internet access services | 2 | Internet access services | 3 |
| Computer equipment/software | 1 | Work-at-Home | 3 |
| Work-at-Home | 1 | Advanced fee loans | 2 |
| Advanced fee loans | 0.2 | Computer equipment/software | 1 |
| Magazine sales | 0.2 | Nigerian money offers | 1 |
| Information adult service | 0.2 | Credit card offers | 0.5 |
| Travel/vacation | 0.1 | Travel/vacation | 0.5 |
| Multilevel market/pyramids | 0.1 | | |
| Total | 98.8 | | 99 |

Sumber: Internet fraud watch (2000) seperti dikutip oleh Confederation Asian and Pasific Accountants dalam "Controlling Fraud on Internet: A CAPA Perspective". http:/capa.tmsasia.com/article.cfm?id=l. Malaysia. 2002.

**Kesulitan Dalam Penanganan Internet Fraud**

Menurut Prasojo (2002) ada beberapa aspek yang menyebabkan terjadinya kesulitan dalam menangani *internet fraud*. Aspek-aspek itu antara lain:

a. Kebijakan Pemerintah

Negara-negara di dunia umumnya telah mengeluarkan kebijakan untuk mengembangkan teknologi informasi dan penggunaan internet. Ada satu karakteristik kebijakan negara-negara berkembang yang membedakannya dengan negara-negara maju. Beberapa pemerintah negara berkembang berusaha mengendalikan akses ke internet dan mengatur isinya. Akan tetapi pengendalian itu sebagian besar hanya berhubungan dengan hal-hal yang tidak disetujui oleh pemerintah seperti subjek seksual dan potensi subversif atau tindakan anti pemerintah. Sedangkan hal-hal yang bisa menyebabkan terjadinya *fraud* kurang mendapat perhatian serius dari pemerintah.

b. Masalah Penyelidikan

Umumnya aparat penegak hukum di negara-negara berkembang mempunyai masalah yang sama dalam menghadapi *internet fraud* ini, yaitu kurangnya pendanaan yang memadai untuk bisa mempekerjakan staf yang terlatih dan untuk memperoleh teknologi yang sesuai dalam penanganan *internet fraud*.

Masalah lain yang menghalangi upaya penyelidikan ialah masalah *mutual assistance*, ekstradisi tersangka, prosedur forensik yang rumit, dan panjangnya masa persidangan. Masalah khusus mengenai *anonimity* dan *pseudonimity* juga menimbulkan kesulitan bagi penyelidik apabila tersangka pelaku *internet fraud* menyangkal keterlibatannya dalam tindak kejahatan tersebut.

c. Masalah Hukum
Karakteristik teknologi internet yang global dan kompleks juga membawa beragam masalah hukum dalam penuntutan pelaku *internet fraud*. Masalah ini timbul dari keberagaman aturan yang ada di berbagai yurisdiksi dan adanya fakta bahwa beberapa aturan itu sangat kompleks, tidak jelas, dan kontradiksi. Beberapa definisi istilah hukum juga perlu ditinjau ulang seperti definisi "dokumen", "tulisan", dan "tanda tangan".

**Upaya Penanganan Masalah Internet Fraud**

Berbagai usaha telah dilakukan oleh berbagai negara untuk mengatasi masalah di atas dan mencegah terjadinya *internet fraud*. Usaha ini meliputi penerapan berbagai strategi mulai dari cara pengendalian kejahatan tradisional sampai penggunaan alat berbasis teknologi mutakhir yang bisa membuktikan pengguna komputer dan melacak bagaimana mereka menggunakan komputer. Penggunaan prosedur pembuktian yang lebih canggih pun diperkenalkan, termasuk penggunaan teknologi biometrik yang akan memecahkan masalah yang sulit dalam mengidentifikasi pelaku *fraud*.

Penggunaan jasa sertifikasi *web site*, seperti *Web Trust*, juga diekstensifkan untuk memperbaiki tingkat kepercayaan dalam penggunaan *e-commerce*. Banyak perusahaan juga telah menggunakan alat keamanan elektronik dalam *e-commerce* mereka. Sebagai contoh Citibank telah menerapkan sistem antisipasi *fraud* yang dinamai *Fraud Early Warning System* (FEWS). Sejauh ini FEWS cukup efektif untuk menekan *fraud*. Beberapa produk sejenis FEWS memang sesuai untuk menghadapi risiko *internet fraud*. Tetapi ada juga produk-produk yang tidak dapat diandalkan, terlalu mahal, dan tidak sesuai dengan kebutuhan.

Upaya penanganan lain ialah pendidikan kepada pengguna internet agar mereka mempunyai pengetahuan yang lengkap mengenai risiko *fraud* dan cara menghadapinya. Usaha ini telah dilakukan oleh sejumlah media masa dan institusi pendidikan.

Dalam upaya pencegahan dan pengendalian *fraud*, Confederation Asian and Pasific Accountants (CAPA, 2002) telah memberikan beberapa saran. Saran-saran itu antara lain:

a. Penerapan *guidelines*
CAPA telah menetapkan *Guidelines Fraud Minimization for Organization Engage in Electronic Commerce* yang dapat digunakan untuk membantu bisnis dan badan-badan pemerintah dalam mencegah dan mengendalikan *internet fraud*. Secara garis besar, *guidelines* itu berisi kewajiban bagi organisasi yang melakukan *e-commerce* untuk:

1. Menyediakan proteksi yang transparan dan efektif yang tidak lebih rendah dari tingkat perlindungan yang diberikan oleh bentuk perdagangan lainnya.
2. Melaksanakan praktik bisnis, periklanan, dan pemasaran yang fair.
3. Melakukan pengungkapan online (*online disclosure*) tentang organisasi, barang dan jasa, syarat, kondisi, dan biaya transaksi.
4. Menyediakan proses konfirmasi.
5. Menyediakan mekanisme pembayaran yang mudah dan aman.
6. Menjelaskan dan menetapkan proses penyelesaian perselisihan dan ganti rugi terutama tentang hukum dan yurisdiksi yang diterapkan serta alternatif-alternatif penyelesaian perselisihan dan ganti rugi.
7. Menjamin privasi.
8. Melakukan pendidikan tentang *e-commerce* untuk membantu pengambilan keputusan oleh pihak-pihak yang menggunakan *e-commerce*.

b. Pelaksanaan inventarisasi hukum dan kebijakan
Inventarisasi hukum ini diperlukan untuk melengkapi sarana hukum yang kurang dan untuk memperbaiki peraturan yang kurang sesuai dalam rangka menghadapi *internet fraud*. Inventarisasi ini juga diperlukan untuk melakukan harmonisasi hukum dengan hukum internasional.

c. Pembuatan database tentang *internet fraud* oleh pihak kepolisian
Database ini diperlukan agar penilaian tentang luas masalah *internet fraud* ini dapat dilakukan dengan tepat untuk bisa memprediksi trend *internet fraud* di masa datang dan untuk mengetahui respon kepolisian dan pengadilan tentang masalah ini.

d. Pembuatan database vonis
Database vonis kasus-kasus *internet fraud* perlu dibuat untuk membantu pengambil keputusan hukum dalam membuat keputusan yang konsisten.

e. Pembentukan *Regional Fraud Desk*
*Regional Internet Fraud Desk* dapat digunakan untuk mengumpulkan dan memeriksa laporan tentang *internet fraud* dan membagi informasi tersebut ke badan-badan penegak hukum.

f. Pelaksanaan inventarisasi layanan sertifikasi
Inventarisasi ini perlu dilakukan untuk memberi informasi tentang tingkat ke-dapat dipercaya-an dari bisnis yang melakukan *e-commerce*.

g. Registrasi profesional ahli
Register perlu dibuat untuk mendaftar individu-individu dan organisasi-organisasi yang memiliki kualifikasi dan keahlian dalam penanganan *internet fraud*.

h. Penilaian sumber daya
Berdasarkan informasi yang telah diperoleh dengan cara-cara di atas, suatu penilaian dapat dibuat untuk menilai tingkat sumber daya yang diperlukan pihak berwajib dalam menghadapi *internet fraud*.

i. Program edukasi
Usaha edukasi perlu dilakukan untuk mendidik pihak-pihak yang terlibat dalam penggunaan internet agar sadar tentang etika dan kewajiban hukum mereka.

j. Kerjasama penegakan hukum
Karena sifat internet yang tidak mengenal batas negara, maka kerja sama antarnegara perlu diciptakan untuk mendorong pembuatan hukum yang seragam dan memadai untuk menghadapi *internet fraud* dan untuk memberikan *mutual assistance* dalam melakukan penyelidikan.

## PEMBAHASAN

### Audit Forensik sebagai Strategi Meminimalkan Internet Fraud

Banyak orang termasuk auditor memandang auditing hanya sebagai auditing dan tidak pernah berpikir lebih jauh dari itu. Namun demikian sebagaimana profesi-profesi lain, ada begitu banyak praktek-praktek khusus yang hanya memiliki sedikit kemiripan baik di dalam program audit, teknik maupun tujuan.

Audit forensik merupakan salah satu spesialisasi dari auditing. Audit forensik diharapkan dapat memberikan *skill* dalam mengasah intuisi, melatih ketrampilan, serta melengkapi auditor dengan cara yang lebih efektif untuk menemukan ketidakberesan.

Seorang akuntan yang memiliki naluri audit forensik akan senantiasa bersikap was-was terhadap setiap situasi yang nampak "normal". Akuntan tersebut akan selalu mencoba untuk mengungkap apa yang ada dibalik setiap transaksi, bukan hanya membandingkan apakah suatu sistem akuntansi atau sistem pengendalian internal berjalan sesuai dengan ketentuan SAK atau tidak (Bologna dan Lindquist, 1987).

Menurut Bologna dan Lindquist (1987) audit forensik tidak dapat diajarkan tetapi dapat dipelajari. Audit forensik menyangkut kesadaran yang paling luas yang meliputi berbagai macam unsur yaitu:

1. Unsur manusia
2. Unsur tingkah laku yang berhubungan dengan suatu organisasi atau perusahaan.
3. Unsur pengetahuan tentang kecurangan
4. Standar-standar dari pelaksanaan pemeriksaan
5. Indikator kecurangan
6. Serta ilmu-ilmu lain yang dapat mendukung pendeteksian kecurangan

Audit forensik akan memandang setiap kecurangan secara kualitatif, tidak menjadi masalah berapa jumlah nominal uang yang tersangkut. Alasannya adalah bahwa setiap kecurangan, menurut sifatnya, dapat berkembang apabila tidak dicegah. Karena memandang secara kualitatif, maka akuntan dituntut untuk memiliki pola pikir yang jeli untuk menemukan setiap kejanggalan yang merupakan indikasi kecurangan, sekecil apapun sifat kejanggalan tersebut (Boatsman, 1996). Kepekaan untuk menangkap kejanggalan dan mendeteksi ketidakberesan tidak dapat dipelajari melalui buku teks. Mental penyelidik akan timbul didalam diri seorang auditor melalui suatu proses yang panjang dengan latihan, disiplin diri, pengalaman yang kesemuanya akan membentuk

kerangka pikir untuk mengetahui bahwa kecurangan dapat terjadi di lingkungan apapun, disegala waktu, oleh setiap orang.

Audit forensik lebih menyerupai suatu proses intuitif daripada suatu metodologi yang analitis dan baku. Audit forensik juga lebih berbentuk seni daripada suatu ilmu formal. Konsekuensinya audit forensik sulit untuk diajarkan. Ketrampilan tergantung pada kerangka pikir dan praktek yang tepat. Tidak ada petunjuk atau bukti sekecil apapun yang tidak memiliki relevansi tertentu. Yang penting adalah bagaimana mendapatkan informasi yang relevan, mengatur dan menyusunnya hingga membentuk suatu pola yang jelas. Untuk itu diperlukan standar yang baku serta tehnik-tehnik khusus (Durtschi, 2003).

Kriteria auditor forensik menurut Dougherty (2001): "Seorang auditor forensik yang baik harus mudah berkomunikasi dengan siapapun, dan sangat kritis. Berpikir lojik, objektif dan tidak bias, tanpa kontroversi. Kemampuan verbal dan tulisan sehingga setiap orang memahami apa yang terjadi, karena akan ditanyai saran dan kepakaran saat diperlukan."

Karakteristik berikut diperlukan oleh auditor forensik untuk bekerja secara profesional (Millan, 2000):

1. Pendidikan, pengalaman dan sertifikasi merupakan kualifikasi yang baik untuk profesi komputer forensik. Pendidikan dengan pengalaman memberikan kepercayaan yang diperlukan untuk membuat keputusan dan mengetahui keputusan yang tepat. Sertifikasi menunjukkan bahwa pendidikan dan pengalamannya merupakan standar yang tinggi dan dapat dipahami.
2. Yakinkan pada setiap tindakan dan keputusan, agar mencukupi untuk kesaksian di pengadilan
3. Semua proses dilakukan dengan menyeluruh
4. Memiliki pengetahuan yang banyak mengenai bagaimana *recover* data dari berbagai tipe media
5. Mampu memecah password dari aplikasi dan sistem operasi yang berbeda dan mempergunakannya untuk penyelidikan
6. Perlu pengetahuan yang memadai, tanpanya bisa terjadi kesalahan yang akan membuat barang bukti ditolak di pengadilan. Barang bukti bisa dirusak, diubah, atau informasi yang berharga terlewat.
7. Obyektif dan tidak bias, harus *fair* pada penyelidikan, dengan fakta yang akurat dan lengkap
8. Inovatif dan memiliki kemampuan interpersonal yang baik
9. Memiliki kemampuan verbal dan oral yang baik
10. Menggunakan penalaran dan logika yang tepat

Penyelidikan *internet fraud* memerlukan bantuan dari para profesional. Salah satunya ialah auditor forensik. Dalam pengusutan *internet fraud* ini tugas dari auditor forensik (Media Akuntansi, 1997) ialah:

1. Melakukan penyelidikan dan analisis bukti-bukti keuangan
2. Mengembangkan aplikasi komputerisasi untuk membantu dalam menganalisis dan menyajikan bukti-bukti keuangan
3. Mengkomunikasikan temuan mereka dalam bentuk laporan, bagan (peraga), dan pengumpulan dokumen
4. Membantu menyelesaikan proses peradilan. Auditor forensik hadir sebagai saksi ahli di pengadilan dan menyiapkan bantuan penerangan untuk mendukung penelusuran bukti.

Menurut Lunn (2001) strategi yang perlu dilakukan oleh audit forensik untuk meminimalkan *internet fraud*:

1. Perlindungan sistem komputer selama pengujian forensik dari semua kemungkinan perubahan, kerusakan, korupsi data, atau virus
2. Temukan semua file pada sistem. Termasuk file normal, terhapus, *hidden, pasword-protected*, dan terenkripsi.
3. *Recovering* file terhapus sebisa mungkin.
4. Ambil isi file *hidden* juga file *temporary* atau *swap* yang dipergunakan baik oleh sistem operasi atau program aplikasi
5. Lakukan akses (jika dimungkinkan secara legal) isi dari file terproteksi atau terenkripsi
6. Analisa semua data yang relevan pada area spesial di disk. Misal *unnalocated* (tidak terpakai, tapi mungkin menyimpan data sebelumnya), *slack space* (area di akhir file pada *last cluster* yang mungkin menyimpan data sebelumnya juga)
7. Cetak semua analisis keseluruhan dari sistem komputer, seperti halnya semua file yang relevan dan ditemukan. Berikan pendapat mengenai layout sistem, struktur file yang ditemukan, dan informasi pembuat, setiap usaha menyembunyikan, menghapus, melindungi, mengenkripsi informasi, dan lainnya yang ditemukan dan nampak relevan dengan keseluruhan pengujian sistem komputer.
8. Berikan konsultasi ahli dan kesaksian yang diperlukan

**Tantangan Bagi Auditor Forensik**

Audit forensik atas teknologi informasi berbeda dengan audit elektronik data processing (EDP). Atau audit teknologi informasi dalam hal tujuan audit (*objective*) dan pendekatan audit (*approach*). Tujuan audit teknologi informasi ialah untuk mendapatkan jaminan yang layak bahwa teknologi informasi akan menghasilkan informasi yang dapat diyakini keandalannya, sedangkan audit forensik teknologi informasi bertujuan untuk mendapatkan bukti-bukti hukum yang diperoleh dari teknologi informasi.

Perbedaan kedua menyangkut fokus audit. Audit teknologi informasi memfokuskan pada kualitas dari sistem, sedangkan audit forensik teknologi informasi memfokuskan pada data yang dihasilkan oleh teknologi informasi tersebut. Pada saat melakukan audit teknologi informasi auditor seringkali memfokuskan pada ketaatan (*compliance*), sedangkan audit forensik teknologi informasi memfokuskan pada bukti substantif.

Menurut Sofjan (2002) dalam melaksanakan audit forensik teknologi informasi untuk mengungkapkan *internet fraud* ini, seringkali auditor menghadapi hambatan sebagai berikut:

1. Kesadaran akan adanya perbedaan pendekatan (*different approach*)
2. Hilangnya bukti-bukti yang dapat diamati (*visible evidence*)
3. Hasil dari audit forensik teknologi informasi jarang dapat digunakan tanpa dukungan bukti-bukti lain
4. Audit forensik teknologi informasi bukan merupakan suatu kegiatan (usaha) tersendiri tetapi merupakan bagian dari investigasi forensik secara keseluruhan
5. Audit forensik teknologi informasi jarang dapat memberikan bukti-bukti yang cukup.

Menurut Prasojo (2002) untuk menghadapi kesulitan-kesulitan tersebut maka auditor forensik perlu memiliki karakteristik tertentu seperti memiliki rasa ingin tahu (*curiousity*), keras hati (*persistence*), kreatif, dapat bebas bertindak (*discretion*), mampu mengorganisasikan, percaya diri, dan mempunyai pertimbangan profesional yang baik. Seorang auditor forensik wajib memiliki keahlian dalam bidang akuntansi, auditing, dan investigasi. Selain itu, keahlian-keahlian bidang lain juga harus dimiliki, antara lain keahlian tentang:

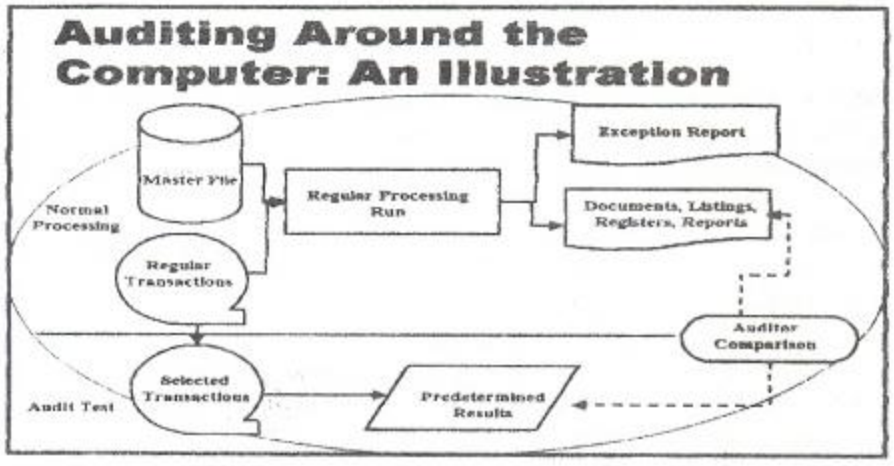
a. Teknologi informasi dan komputer

Karena *internet fraud* terjadi dalam lingkungan teknologi informasi maka auditor forensik harus memiliki pengetahuan tentang teknologi informasi. Auditor forensik harus juga menguasai teknik audit berbantuan komputer.

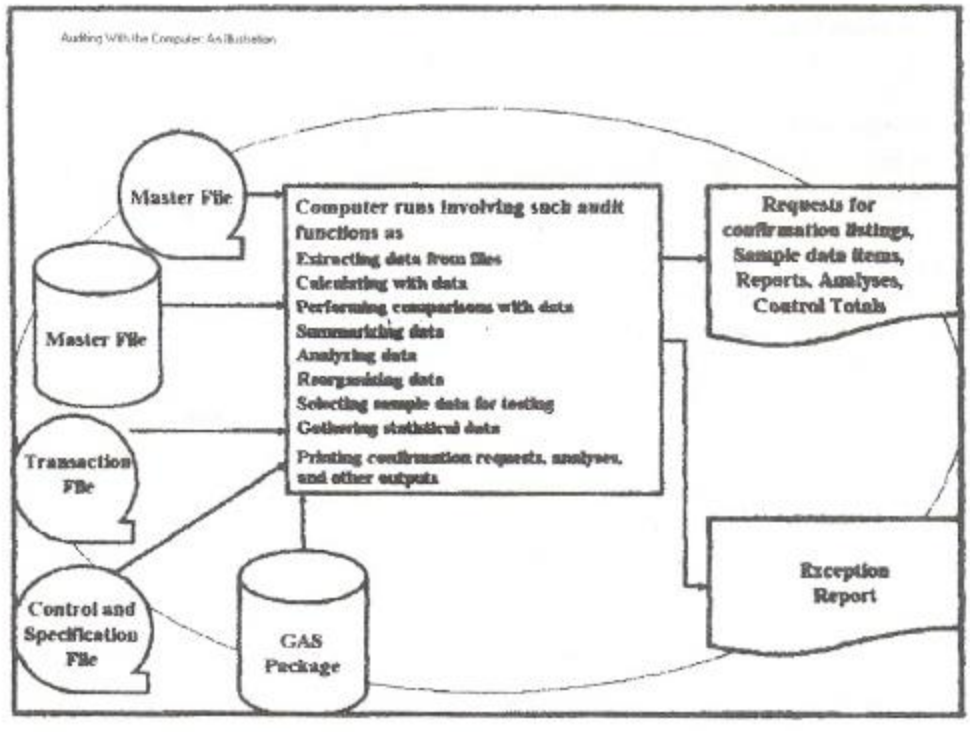
Audit forensik terhadap *internet fraud* berbeda dengan audit EDP, tetapi keduanya mempunyai persamaan, yaitu pelaksanaan auditnya berada di lingkungan pengolahan data elektronik. Dalam hal ini SPAP menghendaki auditor memiliki keahlian sebagai berikut.

Apabila melaksanakan audit di lingkungan Pengolahan Data Elektronik, auditor harus memiliki pemahaman yang memadai mengenai perangkat keras, perangkat lunak, dan sistem pengolahan komputer untuk merencanakan penugasan dan ia harus memahami bagaimana dampak pengolahan data elektronik terhadap prosedur yang digunakan oleh auditor dalam memperoleh pemahaman dan melakukan prosedur audit termasuk penggunaan teknik audit berbantuan komputer (*computer-assisted-audit techniques*).

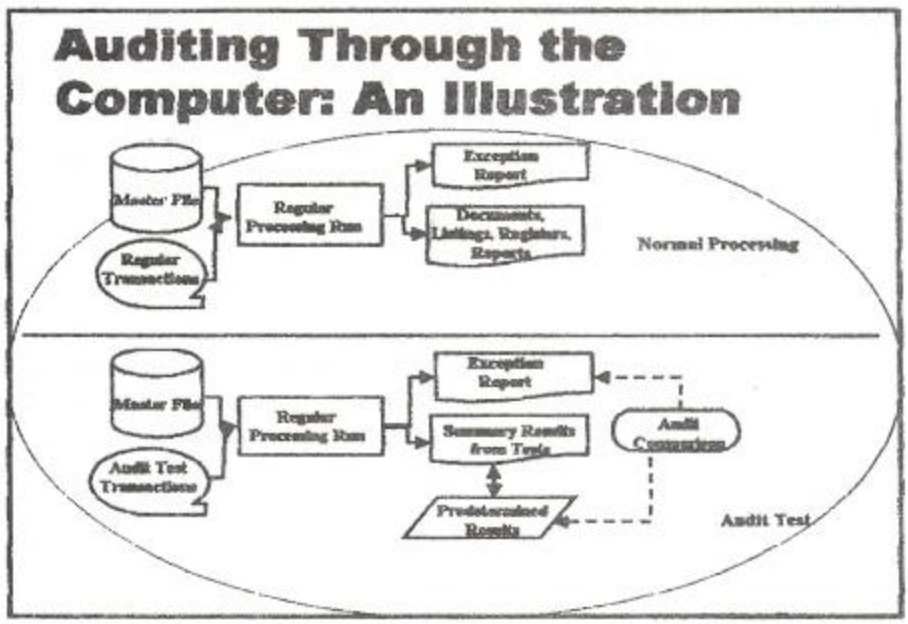
Auditor harus pula memiliki pengetahuan pengolahan data elektronik yang memadai untuk menerapkan prosedur audit yang digunakan (*audit around computer, audit with computer, atau audit through computer*).




Sumber: Wilkinson *et al.* (2000)




Sumber: Wilkinson *et al.* (2000)




Sumber: Wilkinson *et al.* (2000)

Standar Profesional Akuntan Publik, SA 335, paragraf 03-05 menyatakan bahwa auditor sama sekali tidak dapat mendelegasikan tanggung jawabnya dalam merumuskan kesimpulan atau merumuskan pernyataan pendapatnya atas informasi keuangan kepada pihak lain. Oleh karena itu, bila auditor mendelegasikan pekerjaan yang dilakukan oleh auditor lain atau tenaga ahli lainnya, auditor harus tetap memiliki pengetahuan yang memadai mengenai PDE untuk memungkinkannya mengarahkan, melakukan supervisi, dan mereview pekerjaan asisten yang berkeahlian pengolahan data elektronik atau memperoleh keyakinan memadai bahwa pekerjaan yang dilakukan oleh auditor lain atau tenaga ahli di bidang PDE telah cukup untuk memenuhi tujuan auditor (IAI, 2001)

Akan tetapi berbeda dengan sikap mental independen yang harus dimiliki oleh setiap auditor, keahlian ini boleh dimiliki oleh salah seorang dari tim audit. Oleh karena itu keahlian ini dapat diperoleh dengan salah satu cara atau kombinasi dari cara-cara berikut (Watne dan Peter, 1990):

1. Melatih masalah-masalah yang berkaitan dengan komputer kepada mereka yang telah mempelajari akuntansi dan auditing. Dengan kata lain mengajarkan konsep-konsep PDE kepada akuntan atau auditor
2. Melatih teknisi komputer dengan akuntansi dan auditing, atau melatih teknisi komputer menjadi auditor
3. Menggabungkan teknisi komputer dengan mereka yang mengetahui akuntansi dan auditing dalam satu tim audit, atau mempekerjakan teknisi komputer sebagai tenaga ahli membantu auditor. Dalam hal ini akuntan atau auditor berada dalam satu tim dengan teknisi komputer tersebut.

b. Hukum

*Internet fraud* terkadang melibatkan beberapa yurisdiksi hukum. Auditor forensik harus mengetahui hukum pada yurisdiksi yang diperiksanya agar bisa memfokuskan pemeriksaannya pada bukti-bukti pelanggaran hukum. Selain itu pengetahuan hukum, seperti kerahasiaan bank dan perlindungan privasi, juga perlu dimiliki auditor forensik agar dalam pelaksanaan audit, auditor forensik tidak melakukan pelanggaran terhadap hukum yang bisa menimbulkan penuntutan.

c. Manajemen Bisnis

Auditor harus mengetahui manajemen bisnis untuk bisa memprediksi tindakan-tindakan pengusaha dalam berbisnis dan untuk mengetahui tata cara dan kebiasaan-kebiasaan bisnis yang berlaku.

d. Kriminologi

Tujuan audit forensik *internet fraud* adalah untuk mengumpulkan bukti-bukti adanya *internet fraud*. Oleh karena itu kriminologi perlu diketahui auditor forensik untuk memprediksi tindakan-tindakan yang akan dilakukan pelaku kejahatan.

**Pertimbangan Dalam Pelaksanaan Audit**

Seperti kejahatan yang melibatkan komputer yang lain, *internet fraud* memerlukan penanganan secara khusus. Menurut Sofjan (2002) hal ini disebabkan oleh beberapa sifat khusus yang melekat pada komputer seperti:

1. Kemampuan untuk merekam segala jenis bukti dalam kuantitas yang besar
2. Kesalahan dalam prosedur penanganan akan menjadikan bukti yang ada tidak dapat diterima atau lemah
3. Tindakan yang tidak disengaja kemungkinan besar akan dapat menghancurkan bukti-bukti yang diperlukan
4. Data dapat dihancurkan dengan cepat oleh operator yang kompeten.

Menurut Basalamah (1995) dalam melaksanakan audit di dalam sistem online, auditor mau tidak mau harus bekerja pada sistem tersebut. Dengan kata lain, pendekatan audit dengan komputer (*audit with computer*) adalah suatu keharusan disamping pendekatan audit melalui komputer (*audit through computer*). Auditor dapat menggunakan terminal khusus untuk melakukan audit sehingga dapat mengembangkan dan menggunakan piranti lunak pemeriksaan.

Adapun sumber bukti-bukti audit yang perlu diperiksa antara lain adalah *accounts profile, access log, local storage device, free/slack space, deleted files, hidden files, system back up, service provider log files, swap files, printer/fax spooler files, internet log files, network server*, PABX *device, building access systems, dan e-mail server files* (Sofjan 2002).

## SIMPULAN

Kemajuan teknologi internet membuka peluang bagi seseorang atau sekelompok orang yang memiliki tingkat keahlian tertentu untuk memperoleh keuntungan finansial melalui *internet fraud*. Auditor forensik dibutuhkan dalam membantu menemukan bukti *internet fraud* tersebut. Karena kompleksitas yang ada dalam penanganan *internet fraud*, maka auditor forensik pun harus mempunyai keahlian yang memadai pada bidang auditing, akuntansi, investigasi, teknologi informasi dan komputer, hukum, manajemen bisnis, kriminologi, dan pengetahuan lain yang diperlukan.

Seperti kejahatan yang melibatkan komputer yang lain, *internet fraud* memerlukan penanganan secara khusus dan serius. Hal ini disebabkan oleh beberapa sifat khusus yang melekat pada komputer yang rawan terhadap penghilangan bukti.

## DAFTAR PUSTAKA


Basalamah, Anis SM. 1995.Auditing PDE Dengan Standar IAI. *Usaha Kami*. Depok.

Boatsman, James R. July 1996. Fraud Auditing and Forensic Accounting: New Tools and Techni. *The Accounting Review*, Vol. 71, No. 3, , pp. 433-437.

Bologna, Jack and Lindquist Robert. 1987.*Fraud Auditing dan Forensic Accounting, New Tools and Techniques*, John Wiley and Sons.

Confederation Asian and Pasific Accountants (CAPA). *Controlling Fraud on Internet: A CAPA Perspective*. http:/capa.tmsasia.com/article.cfm?id=l. Malaysia. 2002.

Dougherty, James J. 2001. "*Computer Forensics*", SANS Institute

Durtschi, Cindy. May 2003 .The Tallahassee BeanCounters: A Problem-Based Leearning Case in Forensic Auditing. *Issues in Accounting Education*, Vol. 18, No. 2 , pp. 137-173.

Ikatan Akuntan Indonesia. 2001.*Standar Profesional Akuntan Publik*, Salemba Empat, Jakarta.

Lunn, Dorothy A. 2001. "*Computer Forensics – An Overview*", SANS Institute.

Media Akuntansi No. 20/Th.IV/1997.

Millan, Jim Mc. 2000. "*Importance of a Standard Methodology in Computer Forensics*", SANS Institute

Prasojo, Widi. April 2002. Internet Fraud Suatu Tantangan Bagi Auditor. *Pemeriksa no. 84*, pp. 40-45.

Sofjan, Irwan. 14-25 Januari 2002.*Peranan Akuntansi Forensik dalam Mendeteksi Tindak Pidana Korupsi*. Pelatihan Fraud Auditing BPK-RI. Jakarta.

US Department of Justice. 2001. *Internet Fraud*. http:/www.usdoj.gov/criminal/fraud/jmh.htm Washington DC, 15 Mei

Watne, Donald A dan Peter BB Turney. 1990. *Auditing EDP System*, edisi kedua, Prentice Hall Inc. Englewood Cliffs. New Jersey.

Wilkinson, J.W., Cerullo M.J., Raval, V. dan Wong-On-Wing, B. 2000.*Accounting Information Systems: Essential Concepts and Applications*, 4th ed., New York: John Wiley and Sons, Inc., Danvers.