MODUL PERKULIAHAN

EDP Audit

Komputer Forensik

(Computer Forensics)

Abstract

Modul ini berisi seputar computer porensik bagaimana penerapannnya dan jenis-jenis computer foreksi serta tekni dari computer porensik. Modul ini juga membahsa tetang tahapan sistem forensic.

Kompetensi

Mahasiswa mampu pememahami tahapan dari proses sistem forensic dan bagaimana sebuah sistem forensic dilakukan.

Pengantar

Manusia sudah bergantung pada komputer untuk menyimpan dan memproses informasi pribadi, profesional, dan yang terkait dengan bisnis. Bahkan penjahat tidak bisa melawan kekuatan komputer untuk menjaga catatan kegiatan ilegal mereka. Jaringan prostitusi menjaga database "Johns" mereka; pengedar narkoba mengurus daftar pelanggan, distributor, dan pemasok utamanya; dan pembunuh, pemerkosa, penguntit, penyalahguna, dan pelaku kekerasan lainnya dapat menjaga akun rinci tentang perilaku obsesif dan kegiatan lain yang mereka lakukan. Bisnis dapat menghasilkan volume data dalam sistem mereka yang menjelaskan secara rinci kegiatan ilegal seperti diskriminasi, pelecehan seksual, pencemaran atau kerusakan lingkungan, kegiatan antitrust, penyuapan, pemerasan, dan sejumlah pelanggaran hukum dan peraturan lainnya. Lembaga pemerintah dan organisasi militer juga menjaga kekayaan informasi rahasia dan sangat rahasia mengenai kegiatan mereka sendiri serta orang-orang dari negara-negara lain. Saya berani menebak bahwa ada informasi lebih lanjut yang tersimpan pada semua hard drive, paket disk, disket floppy, compact disk, dan media elektronik lainnya di dunia selain yang ada di cetakan.

Definisi dan Gambaran

Manusia sudah bergantung pada komputer untuk menyimpan dan memproses informasi pribadi, profesional, dan yang terkait dengan bisnis. Bahkan penjahat tidak bisa melawan kekuatan komputer untuk menjaga catatan kegiatan ilegal mereka. Jaringan prostitusi menjaga database "Johns" mereka; pengedar narkoba mengurus daftar pelanggan, distributor, dan pemasok utamanya; dan pembunuh, pemerkosa, penguntit, penyalahguna, dan pelaku kekerasan lainnya dapat menjaga akun rinci tentang perilaku obsesif dan kegiatan lain yang mereka lakukan. Bisnis dapat menghasilkan volume data dalam sistem mereka yang menjelaskan secara rinci kegiatan ilegal seperti diskriminasi, pelecehan seksual, pencemaran atau kerusakan lingkungan, kegiatan antitrust, penyuapan, pemerasan, dan sejumlah pelanggaran hukum dan peraturan lainnya. Lembaga pemerintah dan organisasi militer juga menjaga kekayaan informasi rahasia dan sangat rahasia mengenai kegiatan mereka sendiri serta orang-orang dari negara-negara lain. Saya berani menebak bahwa ada informasi lebih lanjut yang tersimpan pada semua hard drive, paket disk, disket floppy, compact disk, dan media elektronik lainnya di dunia selain yang ada di cetakan.

Sebagian besar sistem hukum, dan terutama di Amerika Serikat, dibuat untuk mengandalkan kekayaan informasi yang tersimpan secara elektronik dalam membantu narapidana atau membebaskan tersangka dan untuk menentukan tingkat kerusakan dalam tindakan sipil. Tapi pengaksesan informasi ini sulit, kadang-kadang hampir mustahil. Untuk menyembunyikan atau membuat bukti yang memberatkan tidak dapat diakses, penjahat sering mencoba menghapus atau menghilangkan data dari media penyimpanan elektroniknya. Mereka juga dapat melindungi file datanya dengan menggunakan sandi, teknik enkripsi, atau perangkat lunak kompresi file. Data juga dapat dibagi menjadi potongan-potongan dan disimpan di berbagai lokasi di berbagai media. Penjahat yang putus asa mengatur disk komputernya dan juga komputernya dibakar, bahkan jika itu berarti membakar rumahnya untuk menghindari penuntutan. Yang lainnya membuang komputer mereka ke sungai, danau, dan lautan untuk merusakkan bukti. Para penjahat yang paling berbahaya dan berdarah dingin bahkan menggunakan bahan peledak pada komputernya sehingga jika kunci yang salah disentuh atau jika komputer tidak dimulai dengan urutan yang benar, komputer akan meledak, sehingga menghancurkan data dan orang yang mencoba mengaksesnya.

Para ahli di bidang forensik komputer berada di garis depan dari banyak pertempuran hukum untuk membantu penggugat, terdakwa, dan pengadilan dalam perpaduan fakta-fakta yang sebelumnya tersembunyi. *Komputer forensik* adalah ilmu yang terkait dengan hubungan fakta dan bukti komputer dalam masalah hukum. Ahli komputer forensik dapat memperoleh dan mengakses informasi komputer serta menjelaskannya di pengadilan dengan menggunakan metodologi dan prosedur yang berlaku secara hukum. Spesialis ini juga menawarkan pelatihan kursus untuk lembaga penegak hukum pada perolehan, penanganan, dan penyimpanan hukum atas bukti komputer yang tepat.

Salah satu dari perusahaan komputer forensik yang paling canggih di dunia adalah New Technologies, Inc (NTI), yang berkantor pusat di Gresham, Oregon. Organisasi ini didirikan pada tahun 1996 oleh beberapa ahli teknologi yang diakui secara internasional, termasuk Michael R. Anderson, seorang ahli kecerdasan buatan dan komputer forensik yang menghabiskan waktu 25 tahun untuk melakukan investigasi kriminal berteknologi tinggi dan pelatihan untuk badan-badan penegak hukum federal AS. Anggota lain dari NTI yaitu para ahli di bidang ilmu komputer forensik, pengembangan manfaat forensik dan perangkat lunak keamanan, tren teknologi, masalah jaringan, kriptografi, analisis risiko, dan penilaian risiko. Jasa perusahaan ini yaitu pelatihan dan konsultasi ilmu komputer forensik, penilaian keamanan komputer, dan kesaksian ahli dalam masalah bukti komputer. Untungnya bagi masyarakat, NTI bekerja pada sisi kanan hukum, membantu penegakan hukum sekaligus menghindari permintaan bantuan dari pengedar narkoba dan penjahat lainnya.

Apa yang dipelajari para ahli adalah hal tersebut tidak seperti pembakaran kertas, menghapus atau menghilangkan data pada media penyimpanan elektronik sering tidak sepenuhnya informasi terhapus. Dalam kasus sederhana, menghapus atau menghilangkan data hanya menghilangkan referensi komputer ke lokasi penyimpanan data. Data mungkin tetap utuh sepenuhnya sampai benar-benar ditimpa oleh kegiatan penyimpanan data kelak. Seringkali membutuhkan waktu beberapa tahun untuk menimpa data sepenuhnya, terlepas dari langkah-langkah pemilik data yang diperlukan untuk menyembunyikan atau menghapusnya. Misalnya, salah satu artikel yang lebih rinci mengenai masalah pemulihan data menyatakan bahwa "Ketika sebuah disk diformat, hanya data pada disk yang benar-benar dihapus yang merupakan informasi dalam catatan *boot*, FAT (tabel alokasi file), dan buku petunjuk. File pengguna tersebut masih ada".[1] Versi yang lebih baru dari sistem operasi dapat melakukan perintah tidak memformat untuk membantu pemulihan informasi

yang sengaja diformat ulang. Program perangkat lunak utilitas juga dapat digunakan dalam beberapa upaya pemulihan data. Dua dari aplikasi perangkat lunak utilitas yang lebih dikenal adalah Norton Utilities ™ dari Symantec Corporation dan PC Tools ™ dari Central Point Software.

Dalam kasus yang lebih sulit, hanya informasi file parsial yang mungkin tetap. Sebagai contoh, fragmen data atau "sidik jari elektronik" lainnya dapat ditemukan dalam area penyimpanan sementara dan *cache* data lain dalam komputer. Kadang-kadang fragmen ini bisa sangat besar. Misalnya, data yang "dihapus" atau "dihilangkan" mungkin berlokasi di daerah file slack. Anderson dari NTI mendefinisikan file slack sebagai "ruang penyimpanan antara akhir dari file dan akhir dari kelompok terakhir yang ditugaskan ke ruang khusus". Dalam kasus sistem operasi yang lebih baru, kelompok memori dapat sebesar 32 kilobyte. Jadi, jika bagian terakhir dari sebuah file yang disimpan hanya menggunakan 8 kilobyte kelompok, 24 kilobyte file slack tersedia dalam kelompok.[2] Ketika komputer beroperasi, hal itu akan terus melakukan pembuangan dari data yang berada dalam memori akses acak ke daerah file slack ini. Mengingat ukuran besarnya hard drive di komputer pribadi (PC) hari ini, volume potensi yang mengandung file slack yang berpotensi memberatkan data sangat besar.

Mengakses data ini membutuhkan perangkat lunak dan teknik yang lebih canggih. Sebuah program yang disebut SafeBack™ dikembangkan oleh Sydex Corporation. Menurut Anderson, "segmen data yang jelas mengandung data yang berpasangan (tidak dapat dibaca) yang sekarang dapat disaring (menggunakan SafeBack) membuat isinya dicetak atau ditampilkan dengan mudah menggunakan perangkat lunak pengolah kata sederhana".[2] Kantor Anderson juga menciptakan program perangkat lunak sendiri yang melakukan identifikasi data dan analisis fungsi yang sangat khusus yang dapat mengungkap informasi dimana pemikiran ahli komputer lain sudah lama menghilang.

Ahli forensik komputer bahkan dapat mencocokkan disket individu dalam PC yang digunakan untuk menyimpan data di dalamnya. Jenis informasi ini sangat berguna dalam kasus tersangka yang memiliki disket dalam kepemilikkannya yang bisa dihubungkan dengan PC yang terletak di rumah mereka atau yang dicurigai kriminal lain.

Micro Law Software, Inc. dari Troudale, Oregon, mengembangkan paket perangkat lunak yang unik dan menarik untuk membantu mengidentifikasi komputer yang dicuri. Paket perangkat lunak tersebut terdiri dari pasangan program yang disebut Micro-ID™ dan

Cop-Only™. Setelah pemilik komputer menginstal Micro-ID, perangkat lunak tersebut meminta pemilik asli untuk memasukkan informasi identifikasi pribadi, seperti nama, alamat, nomor telepon, dan tanggal laihr. Perangkat lunak ini juga akan mencatat tanggal penginstalan Micro-ID dan memindai perangkat peripheralnya dan komponen lain yang ada dalam komputer. Micro-ID membuat catatan atas fitur identifikasi yang unik ini dan menyimpan informasi tersebut dalam tempat rahasia dari hard drive komputer. Kemudian, jika komputer disita oleh oleh aparat penegak hukum dan diduga dicuri, program Cop-Only dapat digunakan untuk mengkonfirmasi kecurigaan mereka. Micro-ID merespon segera Cop-Only dan mengungkapkan informasi identitas pemilik asli, tanggal pemuatan Micro-ID, dan informasi perangkat peripheral yang dicatat. Jenis perangkat lunak ini dapat menyalahkan pencuri komputer yang tidak dicurigai dan orang-orang yang membeli komputer curian.[3] Perangkat lunak Micro-ID tersedia untuk umum dengan sedikit atau tanpa biaya. Perangkat lunak Cop-Only tersedia dengan biaya nominal untuk semua lembaga penegak hukum resmi dengan tanggung jawab dalam pemulihan barang curian.

Seperti kontrol lainnya, produk ini dapat dikalahkan oleh penjahat yang cerdas. Karena hard drive mudah untuk dihilangkan, pencuri bisa menginstal hard drive pengganti atau menukar satu dengan komputer lain. Meskipun informasi identitas asli mungkin masih dapat dibaca pada hard drive menggunakan Cop-Only atau beberapa perangkat lunak forensik lainnya, hal itu tidak terkait dengan komputer yang sekarang terinstal. Akibatnya, keakuratan informasi identifikasi bisa dikatakan dalam keraguan. Namun, jika ada contoh yang cukup atas hard drive yang teridentifikasi dalam "toko chop" komputer, juri mungkin menemukan bukti yang menunjukkan tanpa adanya keraguan bahwa komputer dicuri. Selain itu, ada kesempatan yang baik dimana penjahat tidak akan memotong atau menghancurkan hard drive, karena data yang ada pada mereka lebih berharga daripada hard drive itu sendiri. Seiring waktu, juri harus memutuskan kasus demi kasus apakah informasi Micro-ID dapat diandalkan. Berdasarkan hasil, produk tersebut bisa diinstal secara luas.

Organisasi dapat menyewa spesialis komputer forensik untuk melakukan berbagai layanan lain selain mengakses dan menguraikan data. Para ahli dapat memberikan pelatihan untuk auditor internal dan orang lain yang tertarik dalam meningkatkan keamanan lingkungan sistem informasi secara keseluruhan. Mereka dapat melakukan evaluasi keamanan dan penilaian sistem informasi lingkungan dan memberikan rekomendasi untuk membantu memastikan bahwa data cukup terlindungi dari invasi

elektronik oleh penjahat, pesaing, dan bahkan penyalahgunaan diri sendiri. Mereka juga dapat membantu organisasi mengembangkan pergudangan data dan penghapusan prosedur yang aman sehingga kelebihan data diminimalkan dan data yang tidak perlu tidak disimpan selamanya.

Semua masalah forensik yang disebutkan tadi berlaku untuk dunia pengintaian perusahaan semudah yang mereka terapkan untuk penjahat kekerasan. Dengan proaktif melaksanakan rekomendasi dari spesialis komputer forensik sebelum kejahatan atau pengintaian dilakukan, organisasi dapat meningkatkan keamanan sistem secara komputer signifikan dan data serta posisi hukum mereka dalam banyak potensi pertempuran pengadilan. Sekarang mari kita menguji apa yang dapat auditor SI lakukan dalam membantu mengamankan barang bukti untuk potensi penggunaan dalam investigasi kriminal.

INVESTIGASI[4]

Misalkan seorang administrator sistem (SA) melakukan pemindaian rutin atas perangkat jaringan dan menemukan bahwa pengguna telah menginstal program perangkat lunak yang tidak sah yang mampu mengekstrak ID pengguna dan sandi dari jaringan tersebut dan menggunakan kekuatan brutal secara sistematis dalam menetapkan sebagian besar sandi. Dugaan lebih lanjut bahwa pengguna mengakses masuk ke jaringan menggunakan ID pengguna dan sandi yang dikompromikan SA dan kemudian menggunakan hak-hak istimewa SA untuk mengekstrak segala macam informasi rahasia dari jaringan organisasi. Akankah SA tahu apa yang harus dilakukan? Setiap organisasi harus memiliki rencana aksi untuk penemuan tersebut. Rencana aksi yang memadai harus membahas bagaimana menangani bukti komputer yang sedemikian rupa sehingga tidak mencemari dan mencakup prosedur spesifik mengenai cara untuk menciptakan sebuah rantai bukti yang lengkap dan akurat. Sisa bab ini berfokus pada pertanyaan-pertanyaan untuk membantu organisasi lebih siap dalam menyelidiki adegan kejahatan elektronik sebelum hal itu terjadi.

Pemeriksaan Relistis

Skenario yang baru saja dijelaskan bukan fiksi. Sebuah program gratis yang disebut L0PHTCRACK (dengan angka 0, bukan huruf O), yang telah ada selama beberapa tahun, dapat mengekstrak file yang berisi ID dan sandi pengguna dari file server Windows NT dan menggunakan kekuatan brutal untuk menentukan banyaknya mereka, terutama yang lemah. File target pada sistem operasi NT dikenal sebagai file SAM. Dua mantan karyawan baru-baru ini dituduh menggunakan L0PHTCRACK untuk menyalin file SAM secara ilegal dari Epicor Software Corporation dimana tempat mereka bekerja dan kemudian menyalin daftar perusahaan pelanggan internasional. Kedua orang tersebut kemudian menyalin file SAM dari tempat kerja berikutnya, VP Projects, Inc.[5] Program yang mirip dengan L0PHTCRACK telah ada selama bertahun-tahun dan menggunakan pendekatan yang sama untuk menentukan sandi dalam sistem operasi jaringan umum lainnya seperti Unix.

Beberapa penjahat memiliki pornografi anak di komputernya, sementara yang lain menggunakan ruang obrol internet untuk bertemu anak-anak. Patrick Naughton, mantan eksekutif yang berbasis pencari info di Seattle, ditangkap oleh FBI pada tanggal 16 September 1999, karena melanggar undang-undang federal 1994 dimana hal tersebut adalah ilegal dalam melakukan perjalanan dari satu negara ke negara lain dengan maksud untuk berhubungan seks dengan anak di bawah umur. Dalam kasus ini, Naughton, saat itu 34 tahun, melakukan perjalan dari Seattle ke Santa Monica dengan maksud untuk memiliki hubungan seksual dengan anak di bawah umur yang ternyata agen FBI sedang melakukan penyamaran.[6] Sebagian besar percakapan elektronik Naughton selama tujuh bulan atas bujukannya direkam pada komputer laptop pribadinya.

Contoh lain dari karyawan yang dipercaya mencuri informasi sensitif yang terjadi pada tahun 1997 di General Motors (GM). Seorang perwira tinggi yang sedang bernegosiasi posisi yang lebih baik dengan Volkswagen (VW) di Jerman menyalin hampir 40.000 halaman gambar dan spesifikasi komponen CAD (desain berbantuan komputer).[7] Meskipun GM menemukan pencurinya sesaat setelah eksekutif memulai dengan VW, dan GM menerima penyelesaian yang sangat besar setelah tindakan hukum yang sukses terhadap VW, kejadian ini dipublikasikan secara luas, banyak yang merasa malu dari GM.

Hal ini dan banyak jenis lainnya dari kejahatan elektronik semua telah menjadi berita yang terlalu sering. Intinya adalah bahwa meskipun pelaksanaan berbagai jenis kontrol keamanan fisik dan logis bukan masalah jika namun *saat* sebuah organisasi akan

terkena dengan kejahatan elektronik. Seperti bencana apapun, semua organisasi harus siap untuk melakukan investigasi yang akan mengarah pada keyakinan atau penyelesaian yang menguntungkan jika kerusakan tersebut signifikan.

Meskipun sistem hukum secara bertahap menerapkan hukuman yang lebih berat untuk kejahatan elektronik, hukuman sejauh ini relatif ringan dan tidak ada jera yang signifikan. Masalah rumit yang lebih lanjut adalah kesulitan dalam mengamankan hukuman. Jika bukti disalahgunakan atau tercemar bahkan dengan cara yang sangat sedikit, risiko terdakwa yang ditemukan tidak bersalah meningkat secara substansial. Jadi apa yang harus dilakukan setelah potensi kejahatan elektronik diidentifikasi? Di sinilah forensik komputer datang ke garis terdepan.

Penanganan Bukti

Untungnya bagi mereka yang mencari bukti hukum, informasi pada komputer sangat sulit diberantas. Joan Feldman, pemilik Computer Forensic, Inc., perusahaan yang berbasis di Seattle yang membantu menyelidiki kasus Naughton, menggunakan analogi bahwa komputer seperti tape recorder yang selalu berjalan.[8] David Julian, manajer pemulihan data dari Northwest Computer Support, perusahaan lain yang berbasis di Seattle, mengatakan bahwa ia telah memulihkan data dari komputer yang telah didorong dengan mobil, dibuang ke sungai, dan ditembak dengan pistol. Bahkan melemparkan komputer ke laut tidak akan berhasil dalam menghancurkan data.[9]

Alan Brill, direktur praktik global untuk komputer forensik dan jasa investigasi teknologi tinggi dalam Kroll and Associates di New York, mengungkapkan bahwa "mana bagian yang digunakan dari hard drive (disebut kelompok) sebelumnya yang ditugaskan untuk file baru, ruang apa pun dalam kelompok tidak benar-benar digunakan untuk data baru yang mempertahankan data lama. File slack ini terlihat oleh sistem operasi. Dan ada file (termasuk file tukar, file-file sementara dan file penyangga) di mana informasi dapat disimpan bahkan jika pengguna tidak pernah meminta mesin untuk menyimpannya".[10]

Sebelum memulai analisis teknis data komputer, banyak langkah yang harus diambil dalam membantu menjamin penyelidikan dan penuntutan yang sukses, jika diperlukan. Konsep utama yang perlu diingat sepanjang penyelidikan adalah bahwa rantai bukti harus dipertahankan, jika tidak keberhasilan penuntutan apapun akan membahayakan. Ahli komputer forensik dari Ernst & Young, Admiral plc (Inggris), dan Datum eBS semua setuju

bahwa mempertahankan rantai bukti adalah "aturan emas" untuk penyelidikan forensik komputer.[11]

Pemeliharaan harus dilakukan untuk memastikan bahwa pendekatan terstandar yang dipikirkan dengan baik diterapkan. Profesional keamanan teknologi informasi (TI) internal memainkan peran penting dalam mengidentifikasi dan mengamankan bukti kejahatan elektronik. Namun, membolehkan profesional keamanan TI yang tidak terlatih untuk melakukan analisis forensik teknis bisa mencemari bukti yang tak tergantikan, yang kemudian tidak bisa diajukan di pengadilan. Walt Manning, direktur Techno-Crime Intitute memperingatkan, "Menjadi orang yang pintar komputer tidak sama dengan orang yang pintar komputer forensik."[12] Bahkan jika profesional keamanan TI internal memiliki keterampilan, nyatanya analisis komputer forensik bisa memakan waktu berhari-hari, berminggu-mingu, atau bahkan berbulan-bulan untuk membuatnya tidak praktis dan tidak realistis bagi individu tersebut dalam melakukan analisis forensik kecuali, tentu saja, manajemen memilih untuk menyewa pengganti sementara.

Selain itu, analis forensik komputer kemungkinan akan diminta untuk bersaksi jika kasus tersebut masuk ke pengadilan. Sekali lagi, pengalaman di ruang sidang dapat membuktikan malapetaka. Lalu ada masalah kebebasan. Seorang penyidik internal yang bersaksi di pengadilan atas nama organisasi secara otomatis akan dianggap menjadi bias dalam mendukung organisasi, sehingga membuat bukti kurang dapat dipertanggungjawabkan. Untuk alasan ini, organisasi harus secara serius mempertimbangkan penggunaan ahli forensik independen dalam kasus yang memungkinkan ke pengadilan.

Michael Anderson mengutip sebuah kasus di mana seorang karyawan internal diduga melakukan tindakan penggelapan besar dalam perusahaannya. Semua bukti ada di PC-nya. Perusahaan ini menyita PC dengan benar dan memasukkannya ke dalam kantor manajer TI. Sayangnya, manajer TI memutuskan untuk melakukan penyelidikan sendiri. Dia sibuk dan pergi keluar kantor selama dua minggu. Selama waktu ini, PC lain di kantor rusak. Asistennya, yang belum mendapat informasi dari penyelidikan tersebut, memindahkan komputer dalam kantor bosnya ke dalam produksi, percaya bahwa komputer tersebut sudah tidak terpakai. Semua bukti tercemar sehingga tidak layak untuk diajukan ke ruang sidang. Pemeliharaan yang sangat hati-hati harus dilakukan sehingga

bukti dipahami oleh hakim dan juri serta dapat dipertanggungjawabkan dan dapat dipertahankan.[13]

Langkah Investigasi yang Direkomendasikan oleh Para Ahli

Komputer forensik tidak harus dilihat dalam ruang hampa. Hal ini harus menjadi bagian dari program tanggapan insiden komputer organisasi secara keseluruhan. Bahkan hack "biasa" mungkin membutuhkan setidaknya beberapa analisis komputer forensik yang melaksanakan setelah peristiwa tersebut. Seorang manajer sistem menggambarkan kesalahan yang ia buat dalam insiden gangguan terbaru dalam organisasinya. Berdasarkan goresan perlawanannya, ia menyusun 10 langkah "resep untuk penanganan insiden yang sukses". Meskipun tidak spesifik untuk forensik komputer, resep ini memberikan panduan yang berguna bagi mereka yang mengembangkan atau menilai program tanggapan insiden komputer secara keseluruhan :

1. Tulis yang jelas, pernyataan singkat dari ruang lingkup, tujuan, dan kendala.
2. Tambahkan komputasi dan deskripsi sumber daya jaringan.
3. Lakukan penilaian dampak.
4. Delegasikan peran dan tanggung jawab.
5. Buat daftar informasi kontak staf dan penjual.
6. Uraikan tindakan, pemberitahuan, dan prioritas tanggapan insiden.
7. Identifikasi sumber daya tanggapan yang penting.
8. Tentukan investigasi insiden dan persyaratan dokumentasi.
9. Tentukan kebutuhan data yang mendukung.
10. Terus melakukan pelatihan dan mempertahankan rencana.[14]

Mark Bigler, auditor sistem informasi senior di Pacificorp, di Salt Lake city, Utah, memberikan petunjuk yang serupa. Enam langkah menurutnya yaitu :

1. Mengembangkan kebijakan perlindungan informasi dan prosedur forensik yang efektif.
2. Memberitahu kelompok hukum organisasi Anda dan kemungkinan penegakan hukum.
3. Menjaga rantai pemeliharaan untuk semua bukti.
4. Menyiapkan laporan dan kertas kerja rinci.
5. Menyita komputer tersangka.

6. Membuat salinan bayangan cermin dari hard drive.[15]

Bill Betts, seorang konsultan keamanan komputer swasta di Pleasanton, California, merincikan 11 langkah yang harus dilakukan dalam urutan beruntun ketika awal investigasi komputer forensik :

1. Mendapatkan otorisasi yang tepat untuk mengevaluasi sumber daya komputasi.
2. Mematikan komputer (sebaiknya dengan tarik steker saja).
3. Dokumentasikan konfigurasi hardware dari sistem (foto/video).
4. Bawa komputer ke lokasi yang aman.
5. Boot komputer dari disket boot DOS, atau hapus hard drive dan instal di komputer uji yang terisolasi. Langkah ini sangat penting dan hanya boleh dilakukan oleh para ahli.
6. Buat gambar cadangan aliran bit dari target drive.
7. Otentikasi data pada semua perangkat penyimpanan melalui total *hash*.
8. Dokumentasikan tanggal dan waktu sistem.
9. Buat daftar kata kunci pencarian.
10. Periksa ruang bebas.
11. Periksa ruang file slack.[16]

Mark Morris, seorang penyelidik dari Layanan Investigasi Forensik Komputer di Admiral plc di Inggris dan mantan detektif di Unit Kejahatan Komputer di New Scotland Yard, setuju bahwa melakukan backup aliran bit adalah penting. Morris menekankan bahwa mempertahankan jejak audit dan catatan yang komprehensif untuk setiap dan semua kegiatan adalah langkah-langkah yang tidak terpisahkan. "Tidak ada tindakan yang diambil oleh penyelidik yang harus mengubah data asli. Inilah sebabnya mengapa salinan gambar bit harus diambil dari hard drive asli, katanya".[17]

Menggabungkan Semuanya Bersama

Pertimbangan untuk mengambil 13 langkah berikut dalam kejadian kejahatan elektronik.

1. Bersiaplah sebelum ada kejahatan eletronik apapum. Menunjuk tim dasar tanggap darurat (ERT). ERT harus terdiri dari manajemen yang ditunjuk, profesional keamanan

TI (misalnya, administrator sistem jaringan), staf keamanan (dalam hal intervensi fisik), staf penyelidikan penipuan, staf audit internal, dan staf sumber daya manusia (jika seorang karyawan merupakan pelakunya). ERT harus terdiri dari manajemen senior dalam semua komunikasi.

2. Identifikasi satu atau dua konsultan komputer forensik, sebaiknya konsultan lokal, yang bersedia jika keterampilan teknisnya (dan memakan waktu) yang sangat tinggi diperlukan. Mereka harus membuktikan keahlian mereka pada kedua analisis komputer forensik teknis dan kesaksian ruang sidang. Penelitian klien mereka saat ini dan sebelumnya. Pastikan bahwa setidaknya ada beberapa perpindahan pengetahuan kepada keamanan SI dan staf audit internal Anda sehingga mereka mendapatkan pengalaman berharga selama proses tersebut. Biaya konsultan hingga $ 400 per jam, jadi buatlah uang Anda bermanfaat.[18] Pada titik tertentu, ketika anggota staf internal memiliki pengalaman yang cukup, konsultan eksternal mungkin hanya diperlukan dalam kasus penting yang memakan waktu di pengadilan.
3. Lindungi jaringan. Ini adalah tugas pertama administrator jaringan pada penemuan kejahatan elektronik yang potensial. Seringkali mereka harus mengambil langkah cepat dan kadang-kadang langkah ekstrim tanpa kenyamana kelompok konsultasi (misalnya, mematikan seluruh jaringan jika serangan berbahaya yang berlangsung terdeteksi atau segera menyetel ulang sandi atas semua pengguna jika menemukan file sandi jaringan telah disalin).

   Dengan cara yang sama, administrator sistem harus berhati-hati untuk tidak melompati pistol dan mewaspadai pelanggar, sehingga memberikan kesempatan bagi mereka untuk merusak atau menghilangkan bukti-bukti penting sebagian atau seluruhnya. Seperti salah satu manajer sistem yang mengatakannya, "Reaksi dengan cepat dapat menyebabkan kesalahan kecerobohan, yang bisa sangat menyakitkan".[19] Pada akhirnya, administrator sistem harus membuat panggilan penghakiman.
4. Sesegera mungkin setelah identifikasi awal (dalam jam), lakukan ERT tersebut. ERT harus melakukan penilaian risiko dalam menentukan potensi kerusakan yang mungkin atau tidak dilakukan dari hasil kejahatan, dimana sistem dan perangkat penyimpanan data mungkin berisi bukti-bukti, dan tindakan yang perlu dilakukan oleh setiap anggota tim.
5. Buka file kasus dan mulai membuat catatan fisik dari setiap langkah yang diambil selama penyelidikan, termasuk tanggal dan waktu setiap tugas dilakukan, alat apapun yang digunakan, orang yang melakukan tugasnya masing-masing, lokasi dan kontrol

atas setiap potongan bukti, dan informasi lainnya yang bersangkutan. Setiap anggota ERT harus mencatat kegiatannya, dan informasi ini harus disusun oleh anggota ERT tunggal yang ditunjuk untuk memastikan format yang konsisten dan lengkap.

6. Jika seorang karyawan diduga tersangka kejahatan: Departemen Sumber Daya Manusia harus memberitahukan karyawannya bahwa penyelidikan akan dimulai dan harus menempatkan orang tersebut untuk cuti administratif berbayar sampai ditentukan apakah ia tampaknya telah melakukan kejahatan. Kehati-hatian tinggi harus dilakukan agar tidak menyerang privasi karyawan.
7. Putuskan hubungan komputer tersangka dari jaringan sesegera mungkin.
8. Kumpulkan seger media elektronik penyimpanan di sekitar (misalnya, disket, CD-ROM dan CD-RW, kartrid zip-drive) serta bukti kertas potensial dan bawa ke ruang bukti yang ditunjuk, yang terkunci dan hanya dapat diakses oleh individu yang berwenang. Sekali lagi, kehatian-hatian tinggi untuk tidak menyerang privasi karyawan. Melalui dompet dan barang-barang pribadi lainnya dapat menyebabkan gugatan dan kerusakan jauh lebih besar daripada kejahatan elektronik yang sedang diselidiki.
9. Salin media penyimpanan elektronik jarak jauh yang mungkin berisi bukti (misalnya, perangkat penyimpanan disk yang terhubung ke jaringan file server yang terletak baik di tempat atau di sebuah pusat data jarak jauh, CD-ROM yang disimpan dalam perangkat jaringan "jukebox") menggunakan alat forensik yang cocok. Langkah ini merupakan langkah dimana ahli forensik komputer harus dimintai pendapat.
10. Gunakan perangkat lunak yang sesuai, lakukan backup aliran bit dari setiap potongan media penyimpanan elektronik tersangka. Sekali lagi, konsultan komputer forensik harus dimintai pendapat dan mungkin menjadi orang yang melakukan langkah ini.
11. Evaluasi hasil investigasi dengan tingkat yang tepat dari manajemen. Manajemen harus memutuskan apakah akan mengadili orang tersebut. Jika demikian, penasehat hukum harus diberitahu. Aparat penegak hukum yang tepat juga harus diberitahu, terutama dalam kasus-kasus pornografi anak atau kejahatan yang berpotensi kekerasan lainnya.
12. Tutup berkas kasus, dan arsipkan semua dokumen dan bukti untuk jangka waktu yang ditentukan oleh penasihat hukum organisasi.
13. Lakukan kasus pemeriksaan setelahnya untuk mengevaluasi bagaimana proses keseluruhan ditangani dan apakah ada perbaikan yang perlu dilakukan.

KESIMPULAN

Alat komputer forensik adalah, dengan ilmiah sendirinya. Penggunaan yang tepat dari berbagai alat komputer forensik dan analisis hasil merupakan seni maupun ilmu. Langkah-langkah kita sebagai orang awam dapat melakukan sejumlah pikiran praktis. Meskipun demikian, langkah-langkah pikiran praktis tersebut dapat berarti perbedaan antara keberhasilan penuntutan dan pelaku lolos dengan tindakan ilegal. Diharapkan pembaca akan menggunakan informasi dalam bab ini sebagai panduan untuk membantu organisasinya dalam mengembangkan prosedur yang akan meningkatkan kemungkinan hukuman pelaku kejahatan elektronik dan kejahatan lainnya. Tampilan 12.1 memperlihatkan daftar produk dan layanan perangkat lunak komputer forensik yang umum.

Tampilan 12.1 Produk dan Layanan Perangkat Lunak Komputer Forensik yang Umum

Kebanyakan alat forensik komputer telah dikembangkan untuk penggunaan pribadi oleh konsultan yang memungut biaya besar untuk membantu pengacara, perusahaan klien, dan lembaga penegak hukum. Hanya saja baru-baru ini alat tersebut telah tersedia secara komersial. Pendistribusian beberapa alat ini masih diatur oleh pembuatnya untuk membatasi jumlah penjahat dalam memperoleh teknologi tersebut. Saya telah mengumpulkan daftar alat berikut dari berbagai sumber. Beberapa tidak selalu forensik komputer tertentu dan hingga tersedia secara komersial sampai 10 tahun. Mereka dimasukkan karena mereka dapat membantu dalam penyelidikan forensik komputer.

ENCASE PRO Oleh Guidance Software, Inc., Pasadena, CA (*www.guidancesoftware.com*)

Kemungkinan merupakan perangkat lunak komputer forensik yang paling terkenal; awalnya tersedia pada tahun 1997; dijual seharga sekitar $ 1.000; bekerja pada Windows 95/98/NT dan memiliki interface pengguna grafis (GUI); empat hari kursus pelatihan tersedia dengan biaya $ 1.500; pelayanan forensik investigasi juga tersedia; fitur EnCase meliputi :

- Pemindaian drive pada tempat kejadian, kemudian melihat, menyalin, mencetak yang tidak terhapus, dan ekspor file dan folder tanpa mengubah data pada target drive.
- Pergantian antara jenis tampilan Windows Explorer dan tampilan database.

- Melihat dan mengekspor bagian dari hard drive, termasuk daerah antar partisi, ruang disk yang tidak terisi dan file slack, dan isi tempat sampah yang dihapus.
- Pemindaian seluruh disk dengan tampilan klaster dan sektor.
- Melakukan kemampuan kata kunci dan pencarian *wild-card*.

EnCase menciptakan total *hash* MD-5 128-bit dari data bit yang disalin. Hal ini memungkinkan pengguna untuk membuktikan apakah data telah diubah. Jika data diperiksa di lain waktu, EnCase dapat membuat hash baru. Jika data tidak berubah, kedua hash harus setuju.

FORENSIX Oleh Dr. Fred Cohen dan Rekan (*http://all.net*)

Dibuat oleh Dr Fred Cohen, seorang ahli yang diakui secara internasional dan instruktur forensik komputer sejak tahun 1970-an dan saat ini menjadi anggota utama dari staf teknis di US Department of Energy Sandia National Laboratories; versi CD-ROM dijual seharga $ 2.000; versi desktop $ 7.000; gambar dan analisis ForensiX Mac, DOS, Windows, Unix, disk, file, dan sumber data; memiliki interface pengguna grafis; berjalan dengan RedHat Linux atau sistem operasi Unix; pelatihan forensik ditawarkan melalui University of New Haven, CT.

Investigator Oleh WinWhatWhere Corp, Kennewick, WA (*www.winwhatwhere.com*)

Dibuat oleh Richard Eaton dan awalnya dirilis pada tahun 1993, Investigator memantau dan melaporkan semua aktivitas komputer, termasuk pemantauan waktu dan penggunaan, kombinasi kunci pencatatan, pelacakan proyek, dan penggunaan internet. Memiliki mode penipuan sehingga target pengguna tidak menyadari adanya pemantauan. Informasi ini dicatat untuk kemudian melihat oleh pengguna. Hanya $ 100.

Hukum Disk Imager, Genx, Gentext, Gentree, Dan Imager Oleh Vogon International, UK (*www.authentec.co.uk*)

Hukum Disk Imager menciptakan replika yang tepat dari media asli target, atau mesin tersangka. Proses pencitraan tidak akan mengubah informasi pada mesin target. GenX dan GenText berjalan secara otomatis untuk mengindeks dan mengambil teks dari semua bidang gambar target. Pilihan juga tersedia untuk melakukan ekstraksi file penuh dari gambar jika diperlukan. Utilitas investigasi, GenTree, menggabungkan Quick View Plus untuk melihat lebih dari 200 format file. "Hits" yang diidentifikasi dapat dilihat dalam format aslinya dan dicetak jika diperlukan, kemungkinan identifikasi yang cepat harus

dibuat dari bukti yang relevan. Harga tidak disediakan di website. Jasa konsultasi juga tersedia.

Rangkaian New Technologies, Inc (NTI), GRESHAM, OR (*www.forensics-intl.com*)

NTI diakuisisi oleh Armor Holdings, Inc pada tahun 2000 tetapi tetap anak perusahaan yang relatif otonom. Rangkaian NTI mengenai program perangkat lunak berbasis DOS dan tidak terintegrasi, membuat perangkat lunak yang kurang ramah untuk digunakan. Tapi karena berbasis DOS, itu sangat efisien dan membutuhkan ruang disk yang minim. NTI juga menawarkan berbagai pelatihan, termasuk kursus pelatihan intensif tiga hari mengenai perangkat lunak sebagai bagian dari biaya $ 2295 ($ 995 untuk kualifikasi lembaga penegak hukum).

Northon Ghost 2000 Oleh Symantec Corp,. Cupertino, CA (*www.symantec.com*)

Ghost dapat mengkloning dan menggambarkan sebagian atau seluruh hard drive untuk media atau PC lain yang tidak dapat dihapus melalui port paralel atau interface NetBIOS, kemudian mengembalikan seluruh gambar atau file individual dan daftar yang diperlukan. Memeriksa kesalahan yang ada dan kemampuan perbandingan gambar memberikan jaminan bahwa gambar yang tersimpan persis menduplikat yang aslinya; sesuai dengan semua sistem operasi Microsoft. Lisensi pengguna tunggal sebesar $ 70; lisensi perusahaan pada harga aplikasi.

SafeBack, ViewDisk, AnaDisk, Oleh Sydex Corp, Eugene, OR (*www.sydex.com*)

SafeBack menciptakan file backup gambar cermin dari hard disk dan dapat membuat salinan bayangan cermin dari seluruh hard disk atau partisi. File backup gambar dapat ditulis ke perangkat penyimpanan magnetik apapun yang dapat ditulis. ViewDisk menemukan data yang disembunyikan atau dihapus pada disket komputer terlepas dari format. AnaDisk mencari, menganalisis, dan menyalin hampir semua jenis disket tanpa memperhatikan jenis atau formatnya, dapat mengedit sektor data disket oleh sektor atau melakukan pembacaan diagnostik atas jejak disket tertentu, membuang data dari jejak kisaran yang dipilih dalam file DOS sehingga data dari disket yang bukan DOS dapat diperiksa dan dimanipulasi, dan membuat stempel tanggal dan waktu jejak audit dari semua operasi AnaDisk selama pembahasan. Harga harus diminta melalui website karena produk yang dibuat hanya tersedia untuk organisasi yang "sah". Jasa konsultasi juga tersedia.

Daftar Pustaka

1. Robert G. Bromley, "Data Recovery for Small Systems," *Information Systems Audit & Control Journal* (Volume 1, 1994): 45.
2. Michael R. Anderson, "Electronic Fingerprints, Computer Evidence Comes of Age," (1996): 1.
3. "A Stolen Computer As Star Witness," *Law Enforcement Technology* (May 1996): 58–59.
4. Parts of this section adapted from Jack J. Champlain, "Computer Forensics Investigation, "*The Audit Report* (Volume 9, Issue 3, 2000): 4–8.
5. Channel 4000, "Two Face Felony Charges In Software Theft," *www.channel4000.com* (February 17, 2000).
6. Greg Miller, "Impact of Internet Sex-Predator Stings Questioned," *Seattle Times* (September 26, 1999): A6.
7. Peter Ruber, "State of Seige," *IRM Magazine* (Summer/Fall 1999): 10–11.
8. Eric Lacitis, "Secrets on a Computer: Delete Key Doesn't Make Things Clear," *Seattle Times* (September 26, 1999): L1, L8.
9. *Id.*
10. Alan Brill, "Computer Forensics: Files from the Kroll Casebook," *IRM Magazine* (Summer/Fall 1999): 8–9.
11. "Computer Forensics," *SC Magazine* (April 2000): 20–24.
12. *Id.*
13. "Computer Forensics," *SC Magazine* (October 1998): 16–21.
14. Philip Jan Rothstein, "Incident Response: Now What?" *Information Security* (May 1999): 37–41.
15. Mark Bigler, "Computer Forensics," *Internal Auditor* (February 2000): 53–55.
16. Bill Betts, "Crime Seen," *Information Security* (March 2000): 33–39.
17. "Computer Forensics," *SC Magazine* (April 2000): 20–24.
18. Lacitis, "Secrets on a Computer."
19. Rothstein, "Incident Response: Now What?"