An Introduction to

COMPUTER FORENSICS

Oleh: ***Ahmad Syauqi Ahsan***

LATAR BELAKANG

- Penyalahgunaan komputer terbagi menjadi dua:
  - komputer digunakan untuk tindakan kriminal,
  - atau komputer sebagai target kriminal
- Saat ini komputer sudah menjadi barang yang selalu digunakan dalam organisasi2 modern, sehingga tak dapat dielakkan lagi kalau aktifitas2 ilegal akan melibatkan komputer
- Teknologi komputer berkembang dengan sangat pesat. Begitu pula kejahatan2 yang melibatkan komputer (dan internet), serta tool2 untuk keamanan komputer juga banyak dikembangkan.
- Kejahatan komputer melibatkan lebih banyak isu yang belum pernah ada dalam proses2 hukum konservatif,
- Ahli hukum dibidang komputer/internet harus berhadapan dengan lebih banyak ambigu daripada ahli2 hukum yang lain.

COMPUTER FORENSICS ?

- Computer Forensics melibatkan pemeliharaan (preservation), identifikasi (identification), ekstraksi (extraction), dokumentasi (documentation) dan interpretasi (interpretation) dari data komputer.
- Seringkali, Computer Forensics lebih dekat ke seni dari pada ke sains. Tetapi, seperti pada semua disiplin ilmu, ahli dalam computer forensics tetap mengikuti metodologi2 dan prosedur2 yang telah didefinisikan dengan baik dan jelas. Serta, fleksibilitas dibutuhkan dan disarankan ketika menghadapi sesuatu yang tidak biasa.

COMPUTER FORENSICS (2)

- Data digital dapat berupa sesuatu yang sangat mudah berubah → menjadikan computer forensics sebagai satu bidang yang sangat menantang.
- Langkah terbaik adalah dengan memperlakukan setiap kasus kejahatan komputer seakan kasus tersebut akan berakhir di pengadilan.
- Tujuan computer forensics tidak hanya untuk proses penuntutan tindakan kriminal. Kadangkala, computer forensics dilakukan untuk mencari akar permasalahan dari sesuatu guna memastikan bahwa hal itu tidak akan terjadi lagi.
- Forensics dapat juga digunakan untuk mencari jawaban tentang siapa yang bertanggung jawab.

METODOLOGI DASAR

- Metodologi dasar dari computer forensics terdiri dari 3 langkah utama, yaitu:
  1. Acquire the Evidence: Mendapatkan barang bukti tanpa merubah atau merusak aslinya.
  2. Authenticate: Membuktikan bahwa barang bukti yang didapat benar2 merupakan barang yang terlibat didalam kasus yang diselidiki.
  3. Analyze: Menganalisa data tanpa memodifikasinya.

CABUT ATAU TIDAK KABELNYA ?

- Sering terjadi pertentangan antara mencabut kabel listrik atau tidak, mana yang lebih baik.
- Mencabut kabel:
  - Keuntungan: Mem-***beku***-kan sistem. Menghindari kehilangan data karena program yang (mungkin) ditanam dalam sistem operasi yang akan menghapus data2 penting. Memungkinkan meng-clone sistem, sehingga dapat melakukan analisa dengan beberapa skenario tanpa menyentuh data aslinya.
  - Kerugian: Tidak bisa melihat data yang mungkin hanya ada dalam memory. Ada kemungkinan membuat harddisk 'corrupt'.

CABUT ATAU TIDAK KABELNYA ? (2)

- Tidak mencabut kabel:
  - Keuntungan: Bisa melihat informasi yang sedang aktif dalam memory. Opsi ini bisa jadi pilihan yang tepat untuk kasus seperti Internet Intrusion, dimana bukti2 bisa terdapat hanya dalam memory (RAM).
  - Kerugian: Ada kemungkinan sistem dapat mendeteksi kalau ada sesuatu yang ganjil dan akan menghapus data (barang bukti).

1. ACQUIRE THE EVIDENCE

- Satu yang jelas dalam Computer Forensics yaitu: **ketidakjelasan**.
- Pertimbangkan dengan teliti apakah akan mencabut atau tidak mencabut kabel listrik. Dalam beberapa situasi, khususnya pada penyusupan jaringan (network intrusion), barang bukti bisa berada hanya di RAM.
- Ada beberapa faktor yang harus diperhatikan dalam proses pengambilan barang bukti, yaitu: ***penanganan*** (handling), ***rantai penjagaan*** (chain of custody), ***proses pengumpulan*** (collection), ***identifikasi*** (identification), ***perpindahan*** (transportation), ***penyimpanan*** (storage), ***dokumentasi*** (documenting the investigation).

HANDLING THE EVIDENCE

- Penanganan barang bukti merupakan langkah pertama yang sangat crucial. Langkah yang salah akan membuat kacau segalanya.
- Data digital adalah rapuh. Kesalahan sedikit saja bisa membuat suatu data hilang. Handle with extra care.
- Penanganan data, terutama perpindahan dan penyimpanan, merupakan proses2 yang berulang selama masa investigasi.

CHAIN OF CUSTODY

- Tujuan dari pelaksanaan rantai penjagaan yang baik tidak hanya untuk menjaga integritas dari barang bukti, tetapi juga untuk menghindari pembela berargumentasi kalau barang bukti telah dirusak/diubah selama dalam penjagaan kita.
- Prosedur rantai penjagaan yang simpel dan efektif adalah dengan mendokumentasikan secara lengkap seluruh perjalanan dari barang bukti selama proses penyelidikan (persidangan).
- Informasi didalam dokumentasi harus bisa menjawab pertanyaan2 (terkait dengan barang bukti) berikut:
  - Siapa yang mengumpulkannya ?
  - Bagaimana dan dimana ?
  - Siapa (saja) yang bertanggungjawab ?
  - Bagaimana barang bukti itu tersimpan dan bagaimana penjagaannya ?
  - Siapa (saja) yang mengeluarkannya dari tempat penyimpanan dan kenapa?

CHAIN OF CUSTODY (2)

- Untuk memfasilitasi proses pencatatan, kita bisa menggunakan program spreadsheet dan membuat beberapa kolom (seperti terlihat pada gambar dibawah).
- Informasi yang disimpan bisa lebih detail lagi, walaupun data seperti pada gambar dibawah sudah cukup selama terisi secara lengkap.
- Semakin sedikit orang yang mengakses barang bukti semakin baik.

Item	Tanggal	Waktu	Lokasi	Nama	Alasan
Fujitsu P1610 Serial# 7212	3-May-10	11.30 WIB	Brankas di kamar no 232	Jono	Penyimpanan
Fujitsu P1610 Serial# 7212	4-May-10	08.00 WIB	Dikeluarkan dari brankas	Jono	Analisa
Fujitsu P1610 Serial# 7212	4-May-10	10.30 WIB	Dikembalikan ke brankas di kamar no 232	Jono	Penyimpanan

COLLECTION

- Dalam proses pengumpulan barang bukti, sebaiknya dikumpulkan semua benda yang secara hukum dapat dijadikan barang bukti. Komputer, harddisk, CD/DVD, flashdisk, backup tape, sampai pada sobekan kertas yang mungkin dapat berisi informasi penting.
- Ketika kita meninggalkan lokasi, maka tidak ada kemungkinan untuk kembali. Karena, sesuatu yang sebelumnya tidak terpikirkan mengandung informasi, bisa jadi telah hilang. Khususnya untuk log file.
- Ketika kita berurusan dengan ISP (internet service provider), perlu diingat bahwa mereka tidak dalam bisnis penyimpanan log file. Bertindaklah dengan cepat supaya log file tidak hilang.

IDENTIFICATION

- Setiap item yang keluar dari lokasi kejadian harus diidentifikasi dan diberi label.
- Dalam kasus besar, biasanya ada satu petugas khusus yang bertanggung jawab terhadap identifikasi dan pemberian label.
- Sebaiknya tidak mengumpulkan barang bukti sendirian. Ajak seseorang sebagai saksi dan minta partner kita untuk membuat dokumentasi.
- Label pada barang bukti harus cukup besar untuk berisi:
  - Nomor kasus
  - Keterangan singkat
  - Tanda tangan (pada setiap item)
  - Tanggal dan waktu barang bukti dikumpulkan.

IDENTIFICATION (2)

- Kita juga perlu untuk mengambil gambar (foto) lokasi kejadian. Mulai dari seluruh scene, secara bertahap lebih dekat ke komputer (atau barang bukti lain) yang dicurigai, sampai pada jarak yang cukup dekat sehingga bisa mengambil foto sehingga tampak dengan jelas bagian depan dan belakang ketika (hampir) semua kabel masih terhubung.
- Kecuali kita yakin bahwa ada program yang berjalan yang merusak barang bukti, biarkan kabel listrik masih terhubung ketika kita mengambil foto.
- Perlu juga memfoto serial number atau informasi lain yang bisa digunakan untuk identifikasi.

TRANSPORTATION

- Perlu diingat bahwa pada umumnya barang bukti tidak didesain untuk dipindahkan → hati2 ketika memindahkannya.
- Gunakan bungkus anti-static ketika membawa harddisk.
- Ketika menutup sebuah dus berisi barang bukti, segel dus tersebut dan beri tanda tangan disekitar segel. Sehingga akan terlihat bila ada orang lain yang membuka dus tersebut.
- Kalau kita perlu membuka dus yang telah tersegel, catat didalam laporan dan sebutkan alasannya. Setelah selesai, tutup dus dan segel kembali dengan label baru.
  Jika perlu, masukkan dus yang segelnya telah rusak kedalam dus yang lain, baru kemudian disegel lagi.

STORAGE

- Barang bukti, terutama untuk alat2 elektronik, harus disimpan didalam lingkungan yang dingin dan kering.
- Barang bukti harus berada didalam dus yang disegel dan diletakkan di area dengan akses yang terbatas.
- Mengontrol akses ke barang bukti sangatlah penting. Banyak pembela yang suka berargumentasi bahwa barang bukti telah diubah oleh seseorang. Batasi jumlah orang yang punya akses ke ruang penyimpanan.

DOCUMENTING THE INVESTIGATION

- Proses dokumentasi mungkin merupakan hal yang sangat susah bagi ahli komputer. Seorang yang sangat ahli dapat memperbaiki komputer dengan mata tertutup, tapi jika ditanya bagaimana melakukannya, mereka mungkin tidak mampu untuk menjelaskan.
- Bekerja dengan partner, satu orang bekerja pada komputer yang lain membuat catatan.
- Dokumentasikan setiap langkah secara seksama dengan informasi yang detail, termasuk nama software beserta versinya, alat yang digunakan untuk pengumpulan data, metode yang digunakan, serta penjelasan tentang mengapa kita melakukannya.

2. AUTHENTICATE THE EVIDENCE

- Menunjukkan bahwa suatu barang bukti yang kita kumpulkan sama dengan yang ditinggalkan merupakan hal yang sulit.
- Kita harus bisa menunjukkan bahwa tidak ada perubahan pada barang bukti. Seandainya ada, itu disebabkan karena faktor2 alami dan tidak mempengaruhi ‘fungsi’ dari barang bukti itu sendiri.
- Dalam dunia digital, kita mempunyai keuntungan yaitu kita bisa menunjukkan bahwa suatu barang bukti tidak berubah sama sekali semenjak kita kumpulkan.
- Sebuah teknik sederhana memungkinkan kita untuk merekam timestamp sekaligus untuk membuktikan integritas data.

AUTHENTICATE THE EVIDENCE (2)

- Sebuah teknik kriptografi sederhana dapat digunakan untuk menghitung suatu ‘nilai’ yang dapat berfungsi sebagai sidik jari elektronik untuk setiap file atau bahkan untuk seluruh harddisk. ‘Nilai’ ini disebut ***hash***.
- Nilai ***hash*** (atau biasa disebut ***message digest***) merupakan suatu nilai dengan panjang tetap yang dihasilkan oleh sebuah ***hash function*** yang dikenakan terhadap satu kelompok data (biasa disebut ***message***).
- Jika ada perubahan sedikit saja pada kelompok data tadi, maka nilai ***hash*** akan berubah.
- Dua algoritma ***hash*** yang sering digunakan saat ini adalah **MD5** dan **SHA**.

AUTHENTICATE THE EVIDENCE (3)

- Ketika pertama kali kita mengumpulkan data, kita harus segera men-generate nilai ***hash*** untuk setiap file (dan kalau perlu seluruh harddisk) serta mencatatnya.
- Dengan melakukan hal tersebut, kita bisa membuktikan bahwa data yang kita periksa/analisa adalah data yang identik dengan yang pertama kali kita kumpulkan.
- Ada baiknya kita men-generate nilai ***hash*** menggunakan dua algoritma. Sehingga jika dimasa depan ditemukan suatu metode untuk membobol satu algoritma hash, maka kita masih punya nilai ***hash*** yang dihasilkan oleh algoritma yang lainnya.

3. ANALYSIS

- Sedapat mungkin proses analisa data dilakukan tanpa merubah data aslinya.
- Buat copy identik dari harddisk (atau media lain) yang akan kita analisa. Kemudian, ketika kita ingin menganalisanya, copy identik yang biasa disebut image ini bisa kita gandakan lagi. Sehingga bila terjadi kesalahan, kita dapat dengan mudah menggandakan lagi dari copy identik yang pertama (tanpa harus menyentuh data aslinya).
- Jangan lupa untuk mengenerate nilai hash setiap kali kita membuat harddisk image baru. Hal ini diperlukan untuk memastikan integritas data yang terdapat dalam harddisk image tersebut.

TOOLS UNTUK ANALISA

- Ada banyak tool, baik gratis maupun berbayar, yang bisa kita gunakan untuk melakukan analisa.
- Diantaranya ada yang berupa ISO image yang berisi kumpulan dari tool2 untuk analisa forensik (misal *FCCU GNU/Linux Forensic Boot CD*). Dimana ISO image tersebut bisa kita burn ke CD/DVD dan berfungsi sebagai live CD.
- Live CD untuk keperluan analisa forensik ini biasanya sudah didesain khusus sehingga ketika kita menggunakannya tidak akan merubah barang bukti (harddisk) yang kita analisa tanpa disengaja.

TAHAPAN ANALISA

1. Lihat dan catat partition table dari harddisk yang kita periksa. Langkah ini selain diperlukan untuk dokumentasi, juga berguna untuk mengetahui tipe partisi (apakah NTFS, FAT, EXT3, dll) sehingga kita bisa memilih tool yang akan digunakan dengan tepat.
2. Jika tipe dari file system adalah FAT, lihat dalam File Allocation Table, tampilkan bad clusters menggunakan HEX editor. Ada kalanya data disimpan dalam bad blocks.
3. Simpan (atau cetak) daftar file dalam directory beserta sub-directory-nya, termasuk file2 yang *hidden*.

TAHAPAN ANALISA (2)

4. Kembalikan file yang sudah dihapus (un-delete).
   Selain menggunakan tool2 seperti *Norton Unerase*, proses un-delete ini juga bisa dilakukan (dengan penuh kesabaran) dengan bantuan HEX editor.
5. Cek space harddisk yang unallocated atau yang tidak dipartisi, karena ada kemungkinan suatu data disimpan disini.
6. Berikutnya, setelah kita mendapatkan semua file, mungkin kita perlu mulai meng-unzip-nya dan kalau perlu meng-crack password-nya,
   Tergantung pada kasusnya, langkah ini bisa jadi adalah akhir dari proses analisa, atau bahkan merupakan suatu permulaan.