Computer Forensic
23 November 2011, UNRIYO

Josua M Sinambela, M.Eng,
CEH, CHFI, ECSA|LPT, ACE, CCNP, CCNA, CompTIA Security+

About me

- Professional IT Security Trainer & Consultant
- Professional Lecturer (Teach PostGraduate Students)
- Leader Information System Integration Team UGM
- CEO RootBrain IT Security Training & Consulting

Agenda

- Definisi Computer Forensics
- Alasan Mengumpulkan Barang Bukti
- Siapa yang menggunakan Computer Forensics
- Tahapan dalam Computer Forensics
- Penanganan Barang Bukti (Evidence)
- Kebutuhan Pengetahuan Computer Forensic
- Anti-Forensics Tools
- Pedoman dalam memproses dan mengolah Bukti digital
- Metode Penyembunyian Informasi/Data
- Metode Recovery Informasi/Data

Definisi Computer Forensic

- Proses ilmiah dalam melakukan penemuan, pencarian, analisis dan pengumpulan barang bukti dari suatu sistem komputer dengan sebuah standard dan dokumentasi tertentu **untuk dapat diajukan sebagai bukti hukum yang sah**

Definisi Computer Forensic

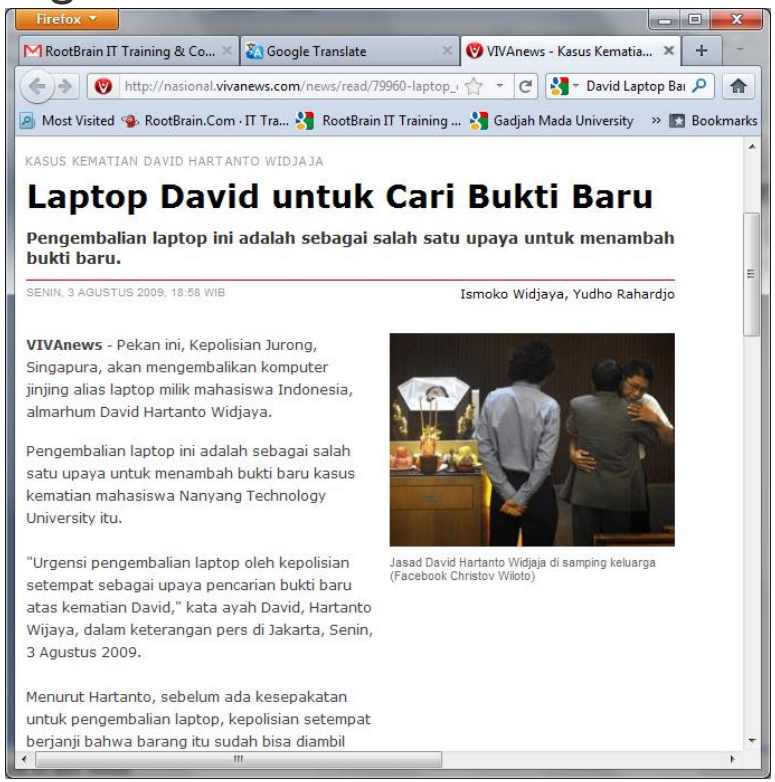
- Komputer forensik juga dapat diartikan setiap aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan – penyaringan dan dokumentasi serta interpretasi bukti pada media sistem komputer
- Investigator Forensic melakukan penyelidikan dan analisis komputer untuk menentukan potensi bukti legal
- Metode metode yang digunakan untuk
  - Penemuan informasi atau data pada sistem komputer
  - Pengembalian/Recovery file yang sudah di hapus, enkripsi, atau mengalami kerusakan.
  - Monitoring Aktifitas seseorang
  - Mendeteksi pelanggaran terhadap kebijakan (policy) perusahaan

Contoh Computer Forensic

- Pemulihan email-email yang terhapus
- Melakukan investigasi setelah pemutusan hubungan kerja
- Recovery barang bukti setelah media storage (harddisk) diformat
- Melakukan investigasi/penyelidikan setelah beberapa pengguna mengambil alih sistem

Kenapa butuh bukti

- Banyak kejadian kejahatan komputer dan penyalahgunaannya
  - Lingkungan Non Bisnis (spt Public Sector): bukti dikumpulkan oleh unsur pemerintahan (Kepolisian), di tingkat pusat maupun daerah untuk kejahatan yang berhubungan dengan :
    - Pencurian rahasia dagang
    - Penipuan
    - Pemerasan
    - Espionasi Industri
    - Pornografi
    - Investigasi SPAM
    - Penyebar Virus/Trojan
    - Penyelidikan Pembunuhan
    - Pelanggaran HAKI
    - Penyalahgunaan informasi pribadi
    - Pemalsuan



Kenapa butuh bukti (lanjutan)

- Kejahatan dan penyalahgunaan komputer
  - Pada Lingkungan Bisnis:
    - Pencurian atau perusakan kekayaan intelektual
    - Melakukan kegiatan yang tidak sah
    - Pelacakan aktivitas dari kebiasaan browsing
    - Rekonstruksi kejadian
    - Menyimpulkan Motif
    - Menjual bandwidth perusahaan
    - Kesalahan pemberhentian klaim
    - Pelecehan Seksual
    - Pembajakan Software

Siapa yang menggunakan Computer Forensic?

- Jaksa Penuntut pada kasus Pidana
- Masyarakat (Civil Ligitation)
- Perusahaan Asuransi
- Sektor Swasta
- Penegakan Hukum pada Pejabat
- Perorangan/Pribadi

Tahapan Computer Forensics

- Secara umum Forensik Komputer terdiri dari 4 tahap yakni
  - Akusisi (Acquisition)
    - Secara fisik atau jarak jauh memeroleh akses ke komputer, jaringan dan pemetaan dari sistem, atau perangkat penyimpanan fisik eksternal
  - Identifikasi (Identification)
    - Mengidentifikasi data apa saja yang dapat dipulihkan atau diperoleh secara elektronik dengan menggunakan tools atau software komputer forensik
  - Evaluasi (Evaluation)
    - Mengevaluasi informasi yang diperoleh atau data yang dapat direcovery untuk menentukan apakah tersangka pelaku benar pernah melakukan pelanggaran dan dapat dilakukan penuntutan di pengadilan
  - (Penyajian) Presentation
    - Tahapan penyajian bukti bukti yang telah didapatkan dengan cara atau istilah yang dapat dipahami oleh para pengacara, para staff dan management yang bukan orang teknis dan sesuai dengan kriteria alat bukti yang sah

Kebutuhan Pengetahuan dalam Komputer Forensik

- Hardware
- BIOS
- Operating Systems
  - Windows 3.1/95/98/ME/NT/2000/2003/XP/VISTA/7
  - DOS
  - UNIX
  - LINUX
  - VAX/VMS
  - Symbian, Blackberry, MAC, Android
- Software
- Forensic Tools
  - Forensic ToolKit (FTK)
  - EnCASE

Anti-Forensics

- Software yang digunakan untuk membatasi/mempersulit penemuan alat bukti oleh investigator dengan cara merusak alat bukti
- Melakukan penyembunyian data (data hiding) atau pengaburan inforamasi
- Memanfaatkan keterbatasan dari tool-tool atau alat komputer forensik.
- Bekerja menggunakan beberapa OS spt Windows dan LINUX

Pedoman dalam pemrosesan alat bukti

- Perusahaan jasa Forensic memiliki standar dan prosedur yang umumnya langkahnya berlaku secara umum
- Contoh Langkah memproses alat bukti digital berupa Komputer/Notebook (Sumber: New Technology Inc) sbb:
  - Step 1: Shut down the computer
    - Considerations must be given to volatile information
    - Prevents remote access to machine and destruction of evidence (manual or ant-forensic software)
  - Step 2: Document the Hardware Configuration of The System
    - Note everything about the computer configuration prior to re-locating

Pedoman dalam pemrosesan alat bukti (lanjutan)

- Step 3: Transport the Computer System to A Secure Location
  - Do not leave the computer unattended unless it is locked in a secure location
- Step 4: Make Bit Stream Backups of Hard Disks and Floppy Disks
- Step 5: Mathematically Authenticate Data on All Storage Devices
  - Must be able to prove that you did not alter any of the evidence after the computer came into your possession
- Step 6: Document the System Date and Time
- Step 7: Make a List of Key Search Words
- Step 8: Evaluate the Windows Swap File

Pedoman dalam pemrosesan alat bukti (lanjutan)

- Step 9: Evaluate File Slack
  - File slack is a data storage area of which most computer users are unaware; a source of significant security leakage.
- Step 10: Evaluate Unallocated Space (Erased Files)
- Step 11: Search Files, File Slack and Unallocated Space for Key Words
- Step 12: Document File Names, Dates and Times
- Step 13: Identify File, Program and Storage Anomalies
- Step 14: Evaluate Program Functionality
- Step 15: Document Your Findings
- Step 16: Retain Copies of Software Used

Metode metode penyembunyian Informasi/Data

- Covert Channels – Menyembunyikan saat transmisi
  - Memanfaatkan waktu dan media penyimpanan bersama (Shared Storage) untuk mentransmisikan data melalui channel/koneksi milik umum/pihak lain
- Teknik Enkoding
  - **Steganography**: Seni menyimpan informasi dengan berbagai bentuk bentuk tersembunyi yang tidak disadari oleh pihak lain

Metode metode penyembunyian Informasi/Data

- **Contoh pada informasi:**
- **T**o **h**uman **e**yes, **d**ata **u**sually **c**ontains **k**nown **f**orms, **l**ike **i**mages, **e**-mail, **s**ounds, **a**nd **t**ext. **M**ost **I**nternet **d**ata **n**aturally **i**ncludes **g**ratuitous **h**eaders, **t**oo. **T**hese **a**re **m**edia **e**xploited **u**sing **n**ew **c**ontroversial **l**ogical **e**ncodings: **s**teganography **a**nd **m**arking.

- ***The duck flies at midnight. Tame uncle Sam***
  - Sederhana dan sering tanpa disadari

Metode metode penyembunyian Informasi/Data

- **Watermarking**: Menyembunyikan informasi didalam data lain.
  - Informasi dapat disembunyikan dihampir semua format file
  - Format file yang digunakanuntuk watermarking
    - Image files (JPEG, GIF)
    - Sound files (MP3, WAV)
    - Video files (MPG, AVI)
  - Informasi yang disembunyikan dapat dienkripsi atau tidak dienkripsi
  - Banyak aplikasi tersedia online dan gratis untuk digunakan

Metode metode penyembunyian Informasi/Data

- Manipulasi Hard Drive/File System
  - Slack Space
  - Hidden Drive
  - Bad Sector
  - Extra Track
  - Mengubah Nama file dan Ekstensi

    (File data.doc dirubah menjadi data.dll, bukti.jpg menjadi bukti.txt)

Metode metode penyembunyian Informasi/Data

- Metode lain
  - Memanipulasi request HTTP dengan merubah urutan elemen
    - Saat ini belum ada software yang dapat digunakan untuk umum, hanya untuk kalangan tertentu (agen rahasia atau pemerintah)
    - Belum dapat atau Sulit untuk dideteksi, karena aksesnya sama seperti access http yang biasa
  - Enkripsi: Informasi tidak disembunyikan, tetapi dilakukan pengacakan sehingga tidak dapat dibaca selain pemilik.
    - Si pemilik data tidak peduli datanya diketahui atau tidak.

Metode deteksi dan recovery data

- Steganalysis – Seni dalam mendeteksi dan melakukan decoding data tersembunyi
  - Menyembunyikan informasi pada media digital/elektronik lain membutuhkan penambahan/perubahan bentuk pada properti data tersebut atau memunculkan karakteristik data yang berbeda
  - Bentuk-bentuk perubahan karakteristik data tersebut disebut dengan signature pada metode steganografi.
  - Software Steganalysis dapat digunakan untuk mencari dan mempelajari sebuah signature.

Metode deteksi dan recovery data

- Metode Steganalysis – Deteksi
  - Pengamatan User/Manusia
  - Software analysis
  - Tool Disk analysis dapat digunakan untuk mencari hidden tracks/sectors/data pada sebuah hard drive
  - RAM slack
  - Filter pada Firewall/Routing filters dapat digunakan untuk mencari data tersebunyi atau tidak falid dalam header IP datagram
  - Statistic Analysis
  - Frequency Scanning

Metode deteksi dan recovery data

- Metode Steganalysis – Recovery
  - Melakukan Recovery pada data watermarking sangat sulit
    - Saat ini hanya sedikit cara yang ditemukan untuk merecover informasi tersebunyi dan terenkripsi pada watermarking.
  - Data tersembunyi pada Hard Disk paling mudah didapatkan.
  - Data yang sudah dihapus dapat di rekonstruksi kembali, bahkan pada Hard Disk yang sudah secara magnetik diformat/wiped/low level format
  - Pada Swap File secara umum terdapat password dan kunci enkripsi yang tersimpan dalam kondisi plain text (unencrypted)
  - Tersedia banyak Software Tools untuk
    - Search/Scan dan reconstruksi data terhapus
    - Membongkar Enkripsi
    - Menghapus/destroy informasi tersembunyi (overwrite)