Yogyakarta, September 2017

Introduction to Digital Forensics

Achmad Syafaat

mailto: asyafaat@gmail.com

Lang: EN & ID (combined)

Agenda

- Introduction
- Definition
- Digital Evidence
- Triage Forensic
- Chain of Custody
- Procedures
- Forensic Tools
- Exercise (Hand on)

Introduction

In the early 1970s the US Congress seeking the latest solutions faster in solving computer crimes

Laws and Conventions

- US Federals Rules of Evidence 1976
- Economic Espionage Act 1996
- The Electronic Comunications Privacy Act 1986
- The Computer Security Act 1987 (Public Law 100-235)
- Convention on Cybercrime; Budapest, 23.XI.2001; http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Introduction

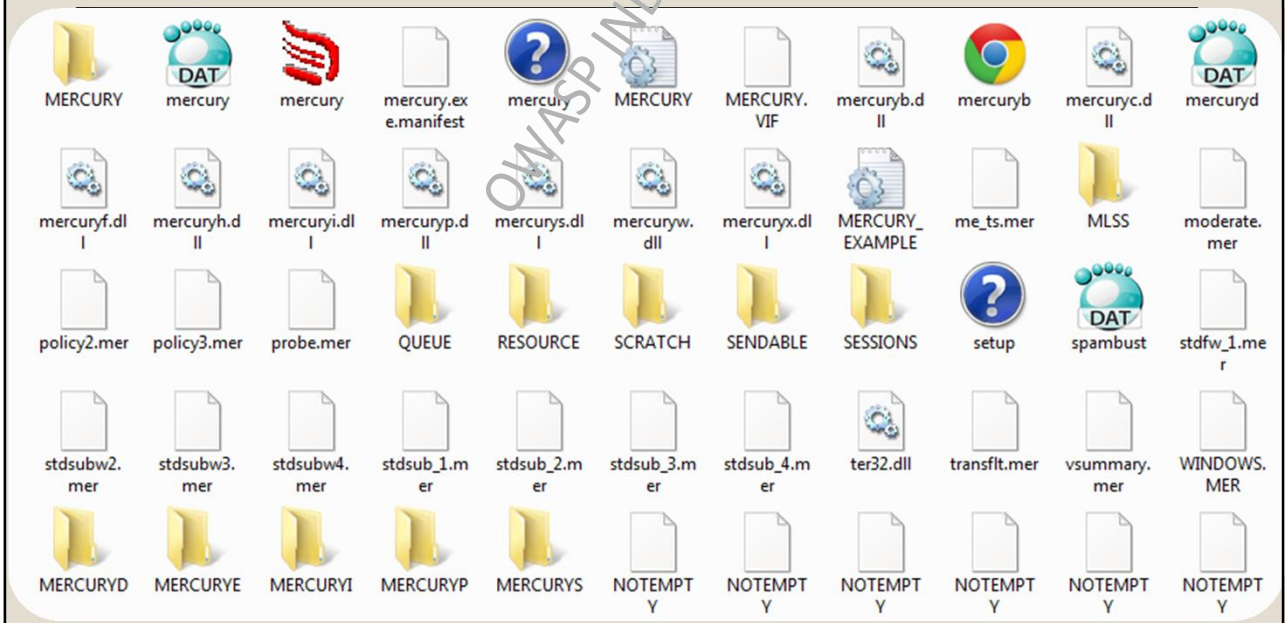
"Merupakan media yang dapat digunakan untuk analisis dan melakukan pengkajian dalam proses penyidikan untuk mengetahui bagaimana cara melakukannya, proses terjadinya, dimana pelaksanaannya dan siapa yang mungkin jadi pelakunya; sehingga dengan barang bukti diharapkan dapat memberikan informasi yang cukup ketika dibutuhkan dipengadilan."

Undang – Undang #Indonesia:

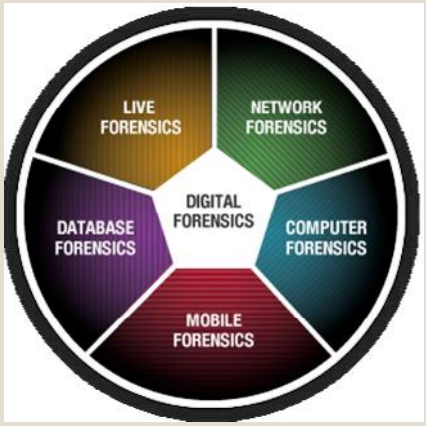
- UU No. 8/1997 tentang Dokumen Perusahaan, Pasal 15 jo. 12-13
- UU No. 20/2001 (TPK), Pasal 26A
- UU No 1 Tahun 2002 tentang Terorisme
- UU No. 15/2002 (TPPU), Pasal 38
- UU Perlindungan Anak No. 23/2002
- UU No. 30/2002 (KPK), Pasal 44 (2)
- UU No. 15/2003 (TP Terorisme), Pasal 27
- UU No 25 tahun 2003 tentang penyucian Uang
- UU No. 21/2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang, Pasal 29
- UU ITE No. 11/2008, Pasal 44
- UU KIP nomor 14/2008
- UU Pornografi No. 44/2008, Pasal 24-25

Introduction

- Komputer dapat digunakan sebagai alat bagi para pelaku kejahatan komputer: seperti pencurian, penggelapan uang dan lain sebagainya. Barang bukti yang berasal dari komputer telah muncul dalam persidangan hampir 30 tahun
- Bukti yang berasal dari komputer sulit dibedakan antara yang asli ataupun salinannya, karena berdasarkan sifat alaminya, data yang ada dalam komputer sangat mudah dimodifikasi. Proses pembuktian bukti tindak kejahatan tentunya memiliki kriteria-kriteria, demikian juga dengan proses pembuktian pada bukti yang didapat dari komputer.



Digital Forensics



Definition

- Secara sederhana: penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan menggunakan software dan tool untuk mengambil dan memelihara barang bukti tindakan kriminal.
- Judd Robin: "Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin".
- New Technologies memperluas definisi Judd Robin: "Komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstraksi, dan dokumentasi bukti-bukti komputer yang tersimpan dalam wujud informasi magnetik".

Definition

- Komputer Forensik berkaitan dengan pelestarian (menjaga keutuhan data), identifikasi, pengambilan (ekstraksi), dan dokumentasi bukti komputer.
- Komputer forensik dapat digambarkan sebagai otopsi dari harddisk komputer karena perangkat lunak khusus dan teknik yang diperlukan untuk menganalisis berbagai tingkat di mana data komputer disimpan setelah fakta
- Memulihkan Informasi tidak lagi dilihat

Definition

- Dan Farmer & Wietse Venema: "Memperoleh dan menganalisa data dengan cara yang bebas dari distorsi atau bias sebisa mungkin, untuk merekonstruksi data atau apa yang telah terjadi pada waktu sebelumnya di suatu sistem".
- CHFI: Penerapan ilmu fisika dengan UU dalam mencari kebenaran dalam perdata, pidana, dan sosial masalah perilaku sampai akhir bahwa ketidakadilan tidak akan dilakukan untuk setiap anggota masyarakat

Objective

- Menentukan nilai bukti dari TKP dan bukti terkait
- Untuk mengembalikan (*recover*), menganalisis, dan menjaga komputer serta material yang berkaitan dengan barang bukti untuk dihadirkan sebagai bukti (*evidence*) di pengadilan
- Untuk mengidentifikasi bukti secara cepat serta memperkirakan potensi dampak dari aktivitas berbahaya pada korban (*victim*), dan menilai maksud dan identitas pelaku

Digital Forensics

- **Dilakukan dengan HAK TERBATAS sesuai peraturan**
- **Mencari & mengumpulkan alat bukti digital**
  - Mengikuti standar & prosedur untuk menjamin integritas data
  - Menemukan (ambil alih) data yang disembunyikan, dihapus, disandikan
  - Mengakses dan memulihkan data yang disembunyikan, dihapus, disandikan

Digital Forensics

- **Analisis informasi, data, alat bukti digital**
  - Menemukan keterkaitan data dengan kejahatan yang dituduhkan
  - Tantangan: keterbatasan waktu analisis, keterbatasan alat/teknologi, jumlah material yang dianalisais tingkat kesulitan (*password*, *encryption*, *secure delete*, *steganography*)
- **Menyajikan hasil analisis & alat bukti digital**
  - Tantangan keterbatasan peraturan perundangan pendukung
  - Pemahaman pihak yang beracara, a.l. hakim, jaksa, pengacara
  - Saksi ahli kontra untuk menjatuhkan proses investigasi & analisis

Digital Evidence

- Any information in digital format
- email message, email address
- File Word processor / spreadsheet
- Source code from software / applications
- Picture (.jpeg, .Gif, .Tiff, etc)
- Bookmark web browser, cookies
- Calendar, Task
- Video (.mov, .3gp, .Mp4, etc)

Triage Forensic

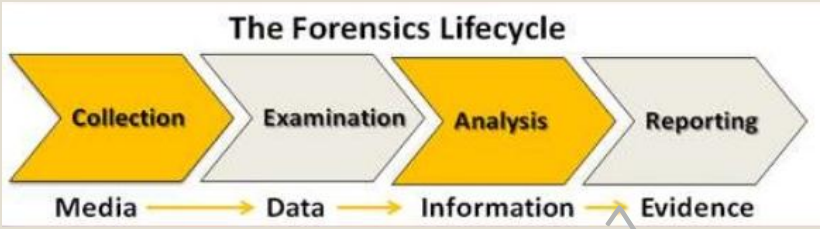
- Identification, where, which, how
- Memprioritaskan dan mendapatkan bukti digital (digital evidence)
- Pelestarian, integritas/keutuhan, chain of custody
- Menganalisis, proses, interpretasi
- Presentasi, pengujian, otentikasi, berhubungan dengan bukti lain non digital dan/atau informasi, saksi
- Dokumentasi dan cadangan bahan

Chain of Custody

- Sangat penting bahwa setiap barang bukti dapat ditelusuri dari TKP hingga ke ruang sidang, dan dimanapun di antara keduanya. Dikenal sebagai mempertahankan '*Chain of Custody*' atau 'kesinambungan bukti'.
- Membuktikan bahwa bagian tertentu dari bukti itu di tempat tertentu, pada waktu tertentu dan dalam kondisi tertentu. Hal ini berlaku untuk perangkat keras fisik serta informasi yang diambil dari *hardware* itu.

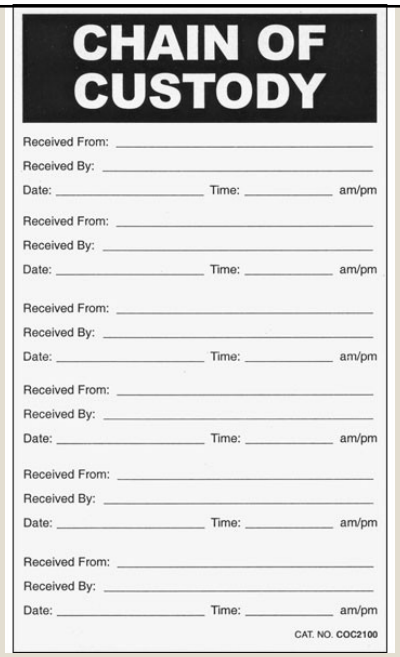
Chain of Custody

- *The Collection, labeling, and testing of evidence.*
- *There must be a documented trail of exactly who has handled the evidence form crime scene to court.*
- *if the chain of custody is broken because of improper handling or labeling of evidence, then the evidence may not be admissible in court.*



Example

- Evidence Form
  - Label everything, memulai mendapatkan bukti
  - Log make, model, and serial numbers
  - Copy stays with evidence at all times
- Chain of Custody
  - Who, What, Where, When, Why, How
  - Copy stays with evidence at all times
  - Always make copies, never work on original media/digital evidence



CHAIN OF CUSTODY

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

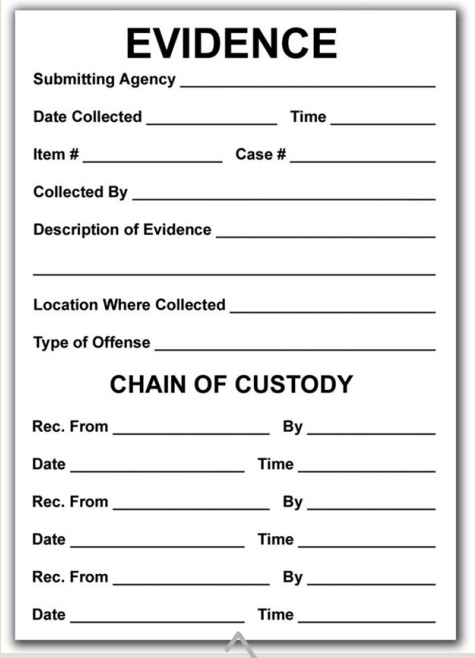
Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

Received From: _____
Received By: _____
Date: _____ Time: _____ am/pm

CAT. NO. COC2100



EVIDENCE

Submitting Agency _____

Date Collected _____ Time _____

Item # _____ Case # _____

Collected By _____

Description of Evidence _____

_____

Location Where Collected _____

Type of Offense _____

CHAIN OF CUSTODY

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Rules of Evidence

- Diterima, dapat diterima oleh pengadilan
- Asli, melindungi integritas data
- Lengkap, diterima oleh jaksa penuntut
- Terpercaya, tidak diragukan lagi, tepatnya
- Handal, mudah diakses

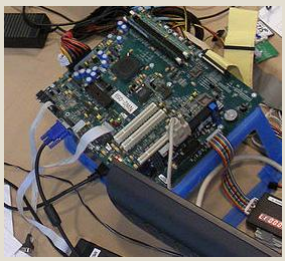
Imaging Evidence

- Mengambil salinan persis termasuk file dihapus dan daerah dari hard drive yang cadangan normal tidak akan menyalin
- Tidak pernah booting dari hard drive
- Gunakan perangkat lunak menulis perlindungan untuk melindungi bukti asli (sumber)
- Buatlah salinan bukti asli dan melakukan semua pekerjaan off dari salinan
- Mendokumentasikan semua aspek dari hard drive
- Tag dan menyimpan bukti asli
- Bukti terbaik adalah bukti asli

Analysis Area

- Email, Temporary Files, Recycle Bin, Info File Fragmen, Link File Terbaru, Spool (di cetak) file, History Internet (index.dat), Registry
- Tidak dapat dialokasikan ruang Ruang bebas pada hard drive
- File ruang Slack bebas antara akhir file logis dan akhir file fisik (cluster)
- RAM ruang Slack bebas antara akhir file logis dan akhir sektor
- Sektor kelompok terkecil yang dapat diakses pada disk. Sekelompok sektor disk ditugaskan oleh sistem operasi yang dikenal sebagai cluster.

Detail Observation



- Hardware: motherboards, power, RAM, printer, scanner, fax, mobile devices
- OS/Apps: Microsoft, Red Hat, UNIX, Forensic Tools, MS. Office, HTML etc.
- Butuh kesabaran dalam melakukan analisis data.

Procedures

- Membuat salinan “2 bit stream” identik
- Hanya melakukan analisa pada barang duplikat bukan aslinya (tetap disimpan)
- Pengembangan dan penggunaan MD5 checksum untuk memastikan tak ada kontaminasi ataupun intervensi
- Penyiapan rantai posesi barang bukti
- Menyimpan barang bukti asli aman
- Pembuatan detail laporan forensik

Tools: RoadMASSter-3 X2 Forensic Hard Drive Acquisiton/Duplicator/Analysis Lab

RoadMASSter-3 X2 is a forensic portable lab designed as a high-speed forensic data acquisition and analysis workstation. The RoadMASSter-3 X2 is ruggedized, built for the road and equipped with all the necessary tools to seize data from drives with today's common drive interface technologies. The RoadMASSter-3 X2 offers the forensic investigator a powerful and versatile platform for forensic data seizure and analysis.

Featuring:

- twice the CPU processing power
- SAS, SATA, SCSI, USB 2.0 and USB 3.0
- Advanced SATA-3 Acquisition Technology,
- 1Gbit Ethernet port for network connectivity
- Data from suspect drives can be uploaded during acquisition for archiving, sharing or future analysis.
- SHA-1, SHA-2 and MD5 Hashing algorithms and features built-in NIST approved AES-256 Hard Drive Encryption support to secure evidence data for the purpose of transporting or storing drives containing sensitive information.

URI: http://ics-iq.com/roadmasster-3-x2-forensic-hard-drive-acquisiton-duplicator-analysis-lab/

Tools: IM Solo-4 G3 PLUS Forensic Enterprise Super Kit

The Image MASSter Solo-4 G3 PLUS Forensic Enterprise Super Kit drive data acquisition unit configured with the i7 Processor and Expansion Box hardware, offers investigators the ability to capture simultaneously at SATA-3 speed from one "Suspect" hard drive to two" Evidence" hard drives. It can also capture from two separate" Suspect" hard drives to two individual "Evidence" hard drives. The unit features a built-in native support for SAS, SATA and USB 3.0drives. The Expansion Box adds support for SCSI drives, Express Card 34/54 Reader.

- Fiber Channel
- Authenticates the drive copies with SHA-1,SHA-2 and MD5.
- IDE, RAID, e-SATA drives and Micro Media flash drives.
- All the "Evidence" images can be saved as 100% copies, Linux DD images or E01 image files.
- All "Evidence" hard drives can be encrypted "on-the-fly" during the acquisition process to protect sensitive data during transportation or storage.
- This forensic hard drive data acquisition unit also offers a built-in Gigabit Ethernet connection allowing users to upload images to Storage Area Networks(SAN) for the purpose of processing and archiving. Write-Protected Ports: All Drive and USB ports are Write-Protected, eliminating the possibility of overwriting valuable data.

URI: http://ics-iq.com/im-solo-4-g3-plus-forensic-enterprise-super-kit/

Tools: Blu-Ray Duplicator

- Blu-Ray disc duplicator with up to 5 times more storage capacity (25Gb) than standard DVDs (4.7Gb).
- Fitted with 4x Blu-Ray drives.
- Includes 500Gb hard disc drive and USB.
- Records 25GB Blu-ray, DVD-R, DVD+R, CD-R, CD-RW

Tools: Cellebrite Mobile Synchronization

- Mobile Phone Forensics is a fast emerging branch of Digital Investigations
- SIM Card Forensic Investigation Tools
- Forensic clone of SIM Cards
- Damaged SIM Card recovery
- Mobile Phone memory extraction – over 1600 models – focused to wards the Indian market
- Mobile site Tower Survey

URI: www.cellebrite.com

Tools: Cellebrite Mobile Synchronization

Tools: Computer Forensic Hardware

- Forensic Workstations
- Password Decryption Hardware Accelerators
- High speed disk duplicators/ imagers
- Shadow (in-situ) forensic devices
- ATA Encrypted hard disk decryption hardware
- Secure Data Destruction Hardware
- Call Loggers etc. etc.
- Cyber Forensic Lab in a Van
- Portable Cyber Forensic Labs

Tools: Hammer, CPR Tools Forensic Hardware

Hammer™ is a hard disk drive erasure tool. The device will securely erase all data written to the attached drives, up to 4 drives at once. Both PATA and SATA interfaces are supported.

Tools: Autopsy

The Autopsy Forensic Browser merupakan antarmuka grafis untuk tool analisis investigasi digital perintah baris The Sleuth Kit. Dapat menganalisis disk dan filesistem Windows dan UNIX (NTFS, FAT, UFS1/2, Ext2/3).

Mode Analisis

- Analisis offline (dead analysis) terjadi ketika digunakan sistem analisis khusus untuk memeriksa data dari sistem tersangka.
- Autopsy dan The Sleuth Kit dijalankan dalam lingkungan terpercaya, biasanya dalam sebuah laboratorium.
- Analisis hidup (live analysis) terjadi ketika sistem tersangka di analisis/sedang berjalan. Dalam hal ini Autopsy dan The Sleuth Kit dijalankan dari sebuah CD (SLAX4). Hal ini sering dilakukan selama proses *incident response* ketika insiden sedang dikonfirmasi. Setelah ia dikonfirmasi, sistem dapat diambil dan dilakukan analisis *offline*.

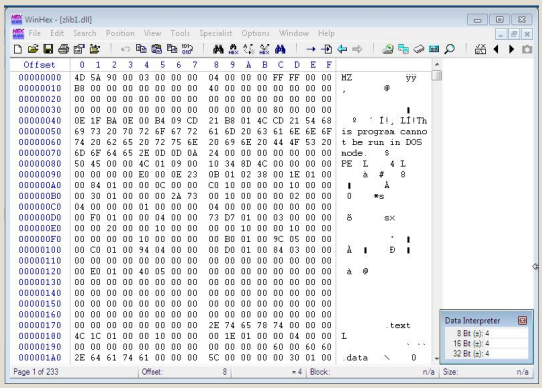
URI: https://www.sleuthkit.org/autopsy/

Tools: VirtualBOX

Digunakan untuk :

- Virtualisasi Sistem Operasi pada satu harddisk yang sama diatas suatu sistem operasi yang sedang berjalan
- Melakukan uji coba melakukan berbagai sistem operasi yg berbeda.

Tools: WinHex



Digunakan untuk :

- Melakukan analisis file dalam format Hexadecimal
- Clone Disk (Copy Sector)
- Analisis Main Memory (Edit Main Memory)

start the exercise (hand on)

ExIDF0. Tools

- Mention some digital forensics tools:
  1. _____
  2. _____
  3. _____
  4. _____
  5. _____

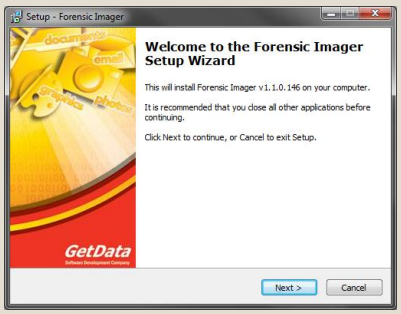
ExIDF1. : *Chain of Custody*

Make a Chain of Custody Form

- Case study: your cell phone or flash disk

ExIDF2. Image

- Write down the steps in creating the image file



ExIDF3. Autopsy

- Complete the case in the image file using Autopsy

ExIDF4. MOBILedit

- Do a forensic cell phone that you have prepared with MOBILedit

Q & A

Thank You