Keamanan Jaringan

85 . Digital Forensik

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Digital Forensik

Menurut Noblett

mengambil, menjaga, mengembalikan, menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer.

Pengertian

Menurut Ruby Alamsyah

ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan.

Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Digital Forensik

Digital forensic dipergunakan untuk :

mengungkap sebuah kasus,

mendapatkan alat bukti (*evidence*)

untuk proses audit dalam satu lembaga/perusahaan.

Barang Bukti Digital

Digital Evidence

- Bukti digital adalah informasi yang didapat dalam bentuk/format digital.

  (Scientific Working Group on Digital Evidence, 1999)

- Bukti digital ini bisa berupa bukti yang riil maupun abstrak

Contoh Bukti Digital

- Email, alamat email
- File Word processor/spreadsheet
- Source code dari software/apps
- Gambar (.jpeg, .gif, .tiff etc.)
- Web browser bookmarks, cookies
- Kalender, to-do list (task)
- Video (.mov, .3gp, .mp4 etc.)

Keamanan Jaringan

86. Elemen Forensik

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Empat Elemen Kunci Forensik

1. **Identifikasi** dari Bukti Digital
2. **Penyimpanan** Bukti Digital
3. **Analisa** Bukti Digital
4. **Pelaporan** Bukti Digital

Obyek forensik?

- Log file
- File yang telah terhapus
- Log IDS atau IPS
- Hard disk
- Email, mailing list, blog atau chat
- File (.tmp, .dat, .txt, .doc)

mekanisme the Chain of Custody CoC

1. Gunakan catatan yang lengkap mengenai keluar-masuk bukti dari penyimpanan
2. Simpan di tempat yang dianggap aman.
3. Akses yang terbatas dalam tempat penyimpanan.
4. Catat siapa saja yang dapat mengakses bukti tersebut.

Prosedur Forensik

1. Membuat *copies dari keseluruhan log data, files, dan lain-lain yang dianggap* perlu pada suatu media yang terpisah
2. Membuat *fingerprint dari data secara matematis (contoh hashing algorithm,* MD5)
3. Membuat *fingerprint dari copies secara matematis*
4. Membuat suatu *hashes masterlist*
5. Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan

Prosedur Digital Forensik

- Buat Kopi yang persis sama, termasik file yang sudah didelete
- Jangan gunakan hard disk
- Gunakan software write protection utk melindungi barang bukti
- Lakukan analisa hanya pada kopi dari barang bukti
- Catat semua aspek dari barang bukti
- Beri tag dan simpan barang bukti asli
- Barang bukti terbaik adalah barang bukti asli

Keamanan Jaringan

87. Windows Forensik

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Obyek Forensik

- File Tersembunyi
- Atribut File
- Registry
- Index.dat

Objek Forensik Windows

- Files
- Slack space
- Swap file
- Unallocated clusters
- Partisi yang tidak digunakan
- Hidden partisi

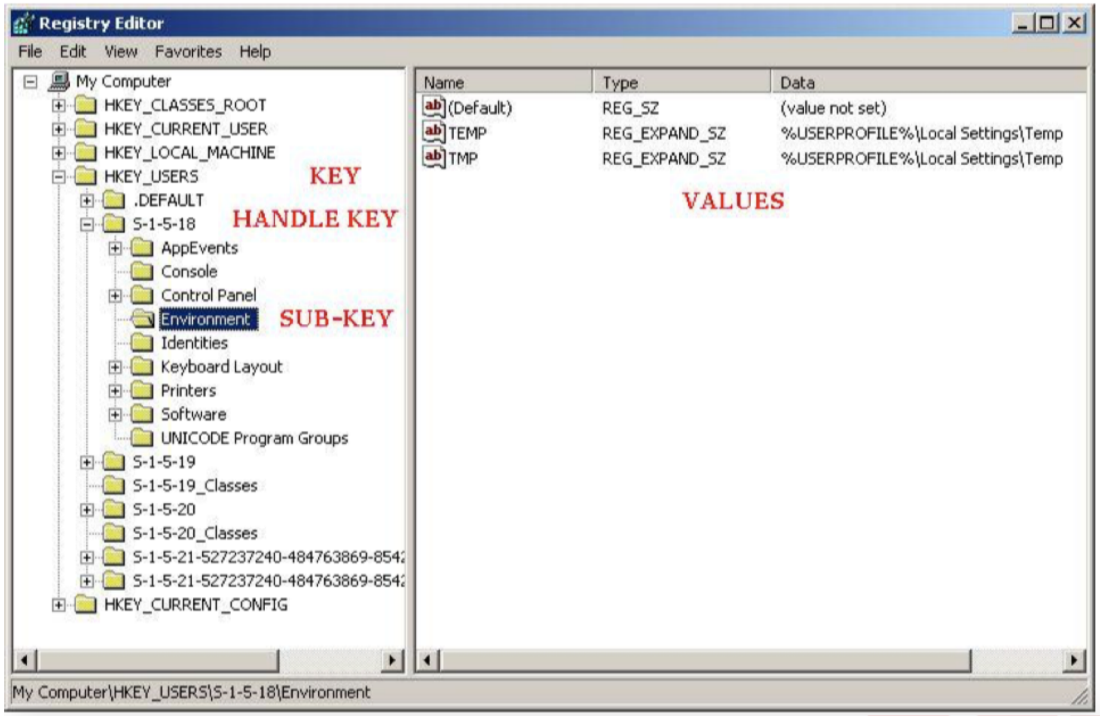
Objek Forensik Windows

- Memory
- Backup
- Jaringan
- Cookies
- History
- Cache

Registry

- Key→ Handle Key→ Subkey→ Value
- HKEY_LOCAL_MACHINE HKEY_CURRENT_USER • HKEY_USERS\.DEFAULT

- RegistryMonitor
- RegistryChecker



Windows Shellbag

- Tentang folder
- Ukuran, Posisi, views icon→ windows explorer
- Informasi tentang
- Mounted volume
- File yang telah dihapus
- Aktifitas user
- UsrClass.dat → HKEY_USERS\{USERID}\.

Keamanan Jaringan

88. Linux Forensik

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Boot Sequence

- */boot : kernel*
- */etc/lilo.conf* atau */etc/grub.conf : bootloader*
- */etc/inittab d*an */sbin/init : inisialisasi*

Perintah Linux

- **dd** -image.
- **sfdisk** and **fdisk** –struktur disk
- **grep** –mencari files text pola.
- **loop device** -mount image
- **md5sum** and **sha1sum** -hash
- **file** -file header ekstensi
- **xxd** - command line hexdump tool.
- **ghex** and **khexedit**

Contoh tahapan forensik menggunakan linux

- */mkdir evidence*
- *mkdir /mnt/investigation*
- *dd if=/dev/fd0 of=image.suspectdisk*
- *Chmod 444 image.suspectdisk*
- *mount -t vfat -o ro,noexec /dev/fd0 /mnt/investigations*
- *md5sum /evidence/md5.image.suspectfile*
- *ls –alR*

Tahapan Forensik Menggunakan Linux (2)

- *grep -i xxx suspectfiles.list*
- *file changedfile*
- *strings, cat, more* or *less*
- *cat /evidence/ suspectfiles.list | grep blackmailword*
  - */evidence/keywordlist.txt*.
- *grep –aibf keywordlist.txt image.suspectdisk > results.txt*
- *xxd -s (offset) image.suspectdisk | less*

Linux Tool

- Sleuthkit
- Autopsy
- SMART
- Penguin Sleuth
- White Glove Linux
- F.I.R.E

Keamanan Jaringan

89. Sistem File

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

file system Windwos

- FAT16 (File Allocation Table)
- FAT32
- NTFS

Linux File system

- EXT
- EXT2
- EXT3
- EXT4

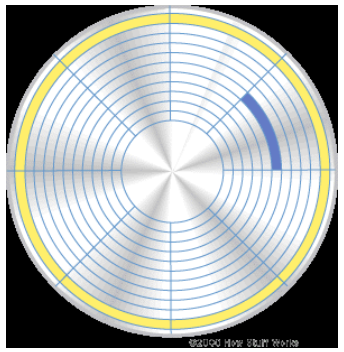
Mac OS X

- HFS
- UFS
- APFS

Media penyimpanan

- Cylinder
- Head
- Platter
- Track dari sektor

Track & Sector



- Tracks merupakan lingkaran yang konsentris dan Sector merupakan bagian dari track yang dibagi-bagi lagi sehingga membentuk pie.
- Track secara umum dapat dilihat dalam garis berwarna kuning, sedangkan Sector berwarna biru.
- Sector berisi fixed number of bytes (maksudnya jumlah byte yang tetap) biasanya 256 atau 512.
- Di dalam level drive maupun sistem operasi, sector sering di kelompokan bersama yang disebut sebagai clusters.

Keamanan Jaringan

90. Teknik Forensik

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Recover File yang dihapus

- Recycle Bin
- Recycle Hidden Folder
- Search & Recover; Zero Assumption Digital Image recovery
- E2undel; O&O Unerase
- File Scavenger; Acronis; restoration
- active@Uneraser

Image File forensik

- Bitmap Vs Vector
- File Header
- Viewer: Irfan View, ACDsee
- Steganografi: Hex Workshop, S-Tools
- Rekonstruksi: DriveSpy,
- Recovery: HDR_Find

Password

- Bypass Bios Password
- Reset Baterei CMOS
- Password Recovery
- Password Cracking
- Default Password

Log

- Events: Success, Failure
- Syslog
- Log Aplikasi
- Log Serangan:

Network

- Log IDS
- Log Router
- Log Firewall
- Log Switch
- Log ApplicationServer

Keamanan Jaringan

91 Tools Forensik

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Hardware

- Roadmasster-3 X2 Forensic Hard Drive Acquisiton/Duplicator/Analysis Lab

Software Forensik

- FTK IMAGING, HASH MYFILE,
- DISK, DEFT FORENSIC,
- WIPE DISK, JPEG SNOOP
- FILE INFO, WINAUDIT
- DRIVEMAN, TREE SIZE
- KALI LINUX DLL

Mobile Forensik

- MOBILE :
- SIM, Internal memori, External memori, Network Provider
- DISK DIGGER, ANDROID DEVICE MANAGER, MOBILE EDIT FORENSIC,
- PHONE COPIER, CPUZ, DLL

Email Forensik

- Header; Body
- Email Server
- Lacak Alamat
- EnCase
- FTK
- FINALeMAIL
- Sawmill-GroupWise
- AudimationforLogging

Web Forensik

- Nslookup, traceroute, neotrace
- Log
  - IDS, Database, Webserver, Firewall
- Deface
- FTP, IIS
- DNS, Apache
- DHCP

Referensi

Council, E. C. "Computer Forensics, Investigating Network Intrusion And Cyber Crime." *Computer Hacking Forensic Investigator (CHFI) Series (Cengage Learning*).