Disk Forensik

Gunadarma University
http://www.gunadarma.ac.id

Gunadarma UG University

Pengenalan Disk Forensik

- Disk Forensik adalah melakukan ekstraksi seluruh informasi pada media penyimpanan sebagai bahan pengembangan sistem maupun barang bukti digital

Jenis Data Dalam Disk Forensik

- Text file
- Multimedia File, contohnya *.mp3,*.mp4,*.wav, *.mpeg, *.avi
- Log File, contohnya:

*.log, *.snort, *.dll

Standar Tools Analisa Disk Forensik berdasarkan NIST

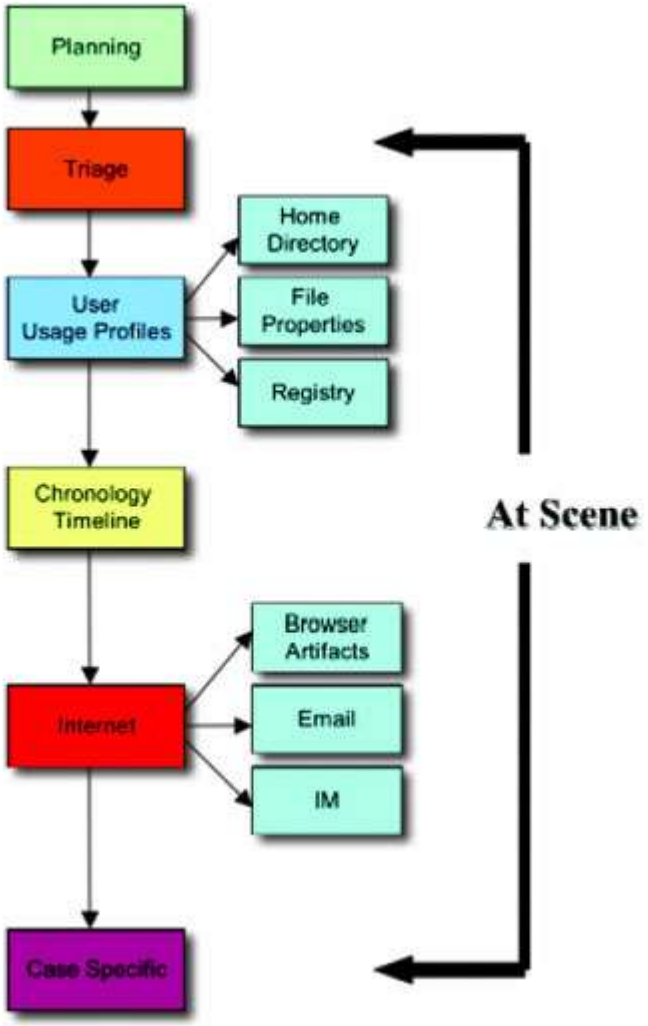
- Tool yang digunakan mampu menduplikasi atau mengclone secara bit-stream untuk seluruh barang bukti (storage devices)yang ada
- Tidak mengubah barang bukti
- Mampu untuk mengakses IDE dan SCSI disk
- Mampu untuk memperifikasi integritas dari sebuah image file
- Mencatat seluruh (I/O) erros

Tahapan Forensik

- Persiapan
- Pengumpulan bukti
- Persiapan Analisa Sistem
- Tahap Analisa
- Kesimpulan

Steps

- Preparation
- Snapshot
- Transport
- Preparation
- Examination



Persiapan

- Mendapatkan ijin/surat untuk mengambil bukti digital
- Wipe hardisk menggunakan...
  - Hal ini dilakakukan untuk memenuhi prasyarat dalam menjalankan forensik
- Memilih operating sistem sebagai alat lab
- Mempersiapkan seluruh tools yang digunakan untuk forensik

Pengumpulan Bukti

- Menggunakan tools yang sesuai dengan sebuah standard misalnya NIST
- Mengumpulkan informasi dari media penyimpanan (Media Acquisition)
- Pencarian bukti-bukti

Media Acquistion

- Menduplikasi individual file
  - Bukti yang terkumpul sedikit karena mengumpulkan isi dari file saja
  - Metadata tidak terekam yang terekam hanya data
  - Untuk lebih memaksimalkan informasi kita dapat menggunakan *grave-robber* utility dari TCT
- Membuat backup tergantung dari sistem yang di gunakan. Di UNIX biasanya menggunakan ekstensi `tar,cpio`, atau

Tools for registry

- RegMon <http://www.sys-internals.com>
- InCntrl5
- Backup registry : rdisk /s

Deleted file

- MS Windows :
  - Check recycle bin
  - EasyRecovery Professional by Ontrack
- Linux :
  - midnight commander (mc)
  - e2undel -d device -s path [-a] [-t]
  - tct

Examining swap file

- MS Windows
  - win386.swp : Win 95/98/ME
  - pagefile.sys : NT/2000/XP
  - Encase
  - Filter_1 by New Technologies Inc

Basic tools

- last
- ps, pstree (be carefull !!!)
- strings
- nm
- find
  - find /bin -ctime -7
  - find / -perm -4000 -print (find SETUID)
  - find / -perm -2000 -print (find SETGID)
  - find / -name ".*" (find hidden directory)
- grep (Ex: grep "uid=0" /var/log/*)
- netstat -a

unrm

- Useful for looking for something that you know is deleted , example for password file

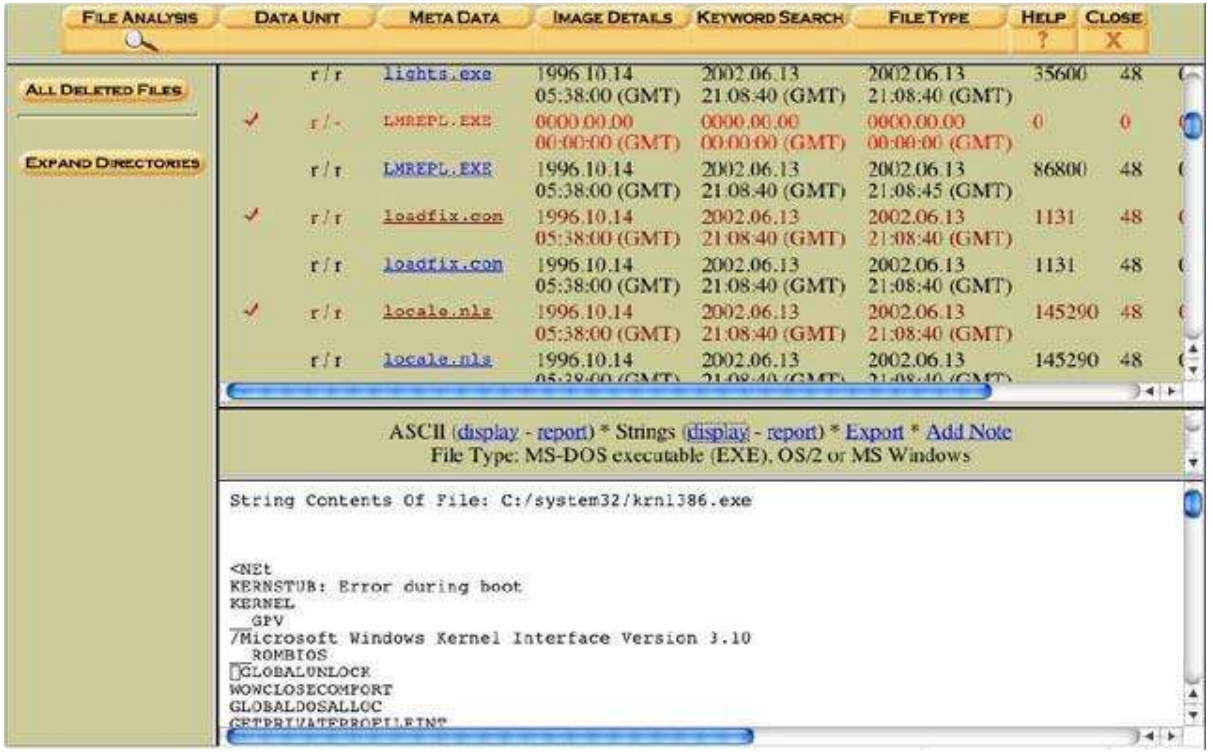
```
unrm /dev/raw/disk/device |

egrep '^.*:.*:[0-9]*:[0-
  9]*:.*:.*:' |

sort -u unrm-passwd file
```

Autospy and Sleuthkit

- <http://www.sleuthkit.org>
- Sleuthkit is based on TCT
- Autospy is forensic browser



pyFLAG

- Network forensics
- Disk forensics
- Support hash comparison (using NIST hast database).

Keyword search

- BinText by Foundstone
- <http://www.foundstone.com>
- Disk Investigator by Kevin Soloway
- <http://www.theabsolute.net/sware/>
- SectorSpyX by Nick McCamy
- <http://home.carolina.rr.com/lexunfreeware>

Apa yang dilog ?

- Proses (UID, GID, waktu eksekusi dsb)
- Filesystem (audit trail, time, label history)
- Network (address, port, ukuran paket, waktu)
- Security (log yang terkait)

Snapshot

- dd can be used

```
dd if=_source_  of=_destionation_
```

- example

```
dd if=/dev/hda  of=/dev/case10img1
```

- to read

```
mount -o ro,noexec,loop case10img1 /mnt/...
```

Analisa Bukti

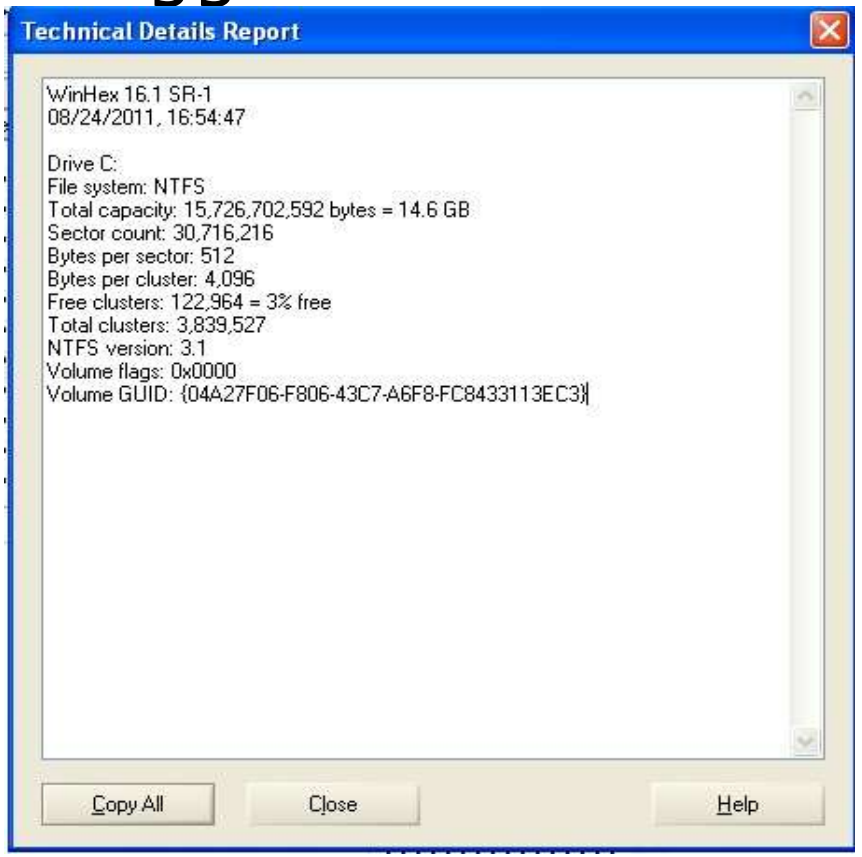
- Image verifikasi, dapat menggunakan `md5sum`, `sha1sum`

```
# md5sum usbkey.dd
# md5sum /dev/sda

# sha1sum usbkey.dd
# sha1sum /dev/hda
```

Metadata Filesystem

- Menunjukkan informasi cluster
  - Dapat menggunakan WinHex untuk windows,



File System

Pengertian File System

- File System merupakan struktur logika yang digunakan untuk mengendalikan akses terhadap data yang ada pada disk
- File System menyediakan mekanisme untuk penyimpanan data dan program yang dimiliki oleh sistem operasi serta seluruh pengguna dari sistem komputer
- File System terdiri dari dua bagian:
  - Kumpulan file yang masing-masingnya menyimpan data-data yang berhubungan
  - Struktur direktori yang mengorganisasi dan menyediakan informasi mengenai seluruh file dalam sistem
- Masing-masing Sistem Operasi menggunakan cara yang berbeda dalam mengatur dan mengendalikan akses data dalam disk.

Hubungan Sistem Operasi dengan File System

- File System merupakan interface yang menghubungkan sistem operasi dengan disk.
- Ketika program aplikasi yang sedang dijalankan memerlukan pembacaan file dari hard disk, sistem operasi meminta file system untuk membuka file yang diinginkan.
- File system harus mengetahui lokasi penyimpanan file yang dibaca. Setelah menemukan lokasinya, file system membaca data yang ada dan mengirimkan data tersebut pada sistem operasi.

Jenis-Jenis File System

- FAT
- NTFS
- EXT2
- EXT3
- Mac OS X

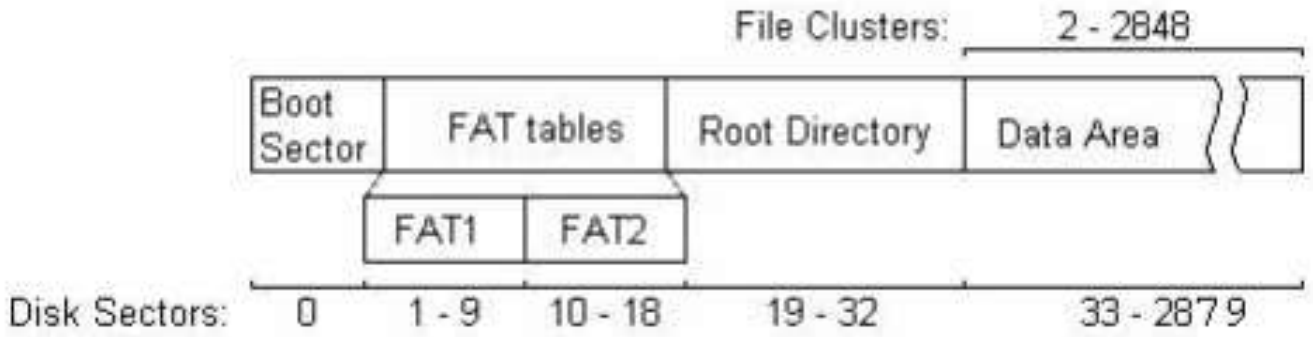
FAT

- FAT → File Allocation Table
- Jenis-jenis sistem file FAT:
  - FAT12
  - FAT16
  - FAT32

FAT12

- Menggunakan ukuran unit alokasi yang memiliki batas hingga 12 bit
- Merupakan file sistem asli dari FAT yang pertama kali digunakan dalam sistem operasi MS-DOS
- Batas kapasitas hingga 32 MB
- Bisa diakses oleh MS-DOS dan semua OS Windows

- Organisasi Disk pada FAT12 sistem file



FAT16

- Menggunakan ukuran unit alokasi yang memiliki batas hingga 16 bit
- Batas kapasitas hingga 4 GB
- Ukuran unit alokasi yang digunakan oleh FAT16 bergantung pada kapasitas partisi yang hendak diformat
- Bisa diakses oleh MS-DOS (versi 4.x ke atas) dan semua OS Windows

FAT32

- Menggunakan ukuran unit alokasi yang memiliki batas hingga 32 bit
- Batas kapasitas hingga 2 TB
- Diperkenalkan mulai Windows 95 OEM Service Release 2 (Windows 95 OSR2)
- Bisa diakses oleh semua OS Windows kecuali Windows 95 (versi awal), Windows NT 3.x dan Windows NT 4.0

FAT 12 or FAT 16 or FAT 32

Perbandingan	FAT 12	FAT 16	FAT 32
Unit Alokasi	Hingga 12 bit	Hingga 16 bit	Hingga 32 bit
Ukuran Volume Max	32 MB	4 GB	2 TB
Jumlah ClusterMax	4.085	65.525	268.435.445

NTFS

- NTFS → New Technology File System
- NTFS adalah Pengembangan yang dilakukan oleh Microsoft untuk memperbaiki kekurangan yang dimiliki sistem file FAT

Keunggulan & Tujuan NTFS

Beberapa tujuan spesifik dari NTFS adalah:

- **Reliability**:

  satu hal yang penting dari sebuah file system yang serius adalah bahwa file system tersebut harus dapat pulih kembali dari masalah tanpa kehilangan data hasil. Disini NTFS mencegah hilangnya data dan memperkecil toleransi dari kesalahan dalam *processing*.

- **Security dan Access Control**:

  Kelemahan dari FAT adalah ketidakmampuan mengontrol akses file atau folder dari hard disk, sehingga memungkinkan pihak luar untuk mengubah data pada suatu sistem jaringan.

- **Breaking Size Barriers**:

  karena pada sistem FAT dalam hal ini FAT16 tidak dapat mempartisi lebih dari 4GB, sedang NTFS didesain untuk partisi yang jauh lebih besar.

- **Storage Efficiency**:

  NTFS lagi-lagi memperbaiki kelemahan pada FAT16
  karena pada sistem ini memungkinkan terjadinya ketidak efisienan pada penyimpanan pada kapasitas hard disk. Untuk itu NTFS menggunakan metode lain dalam alokasi kapasitas hard disk tersebut.

- **Long File Names**:

  NTFS memungkinkan nama sebuah file hingga 255 karakter, dibandingkan dengan pada FAT adalah 8+3 karakter.

- **Networking**:

Saat ini networking berkembang pesat dengan NTFS memungkinkan networking dalam skala besar.

- **Storage Fault Tolerance**:

  Data-redundant storage methods dapat diterapkan pada NTFS. Hal ini berguna dalam menjamin dan melindungi jika suatu data/berkas mengalami kerusakan dengan mengkopi ulang data yang sama dari disk mirror.

- **Multiple Data Stream**:

  NTFS dapat terdiri dari lebih 1 stream. Stream tambahan ini dapat berisi berbagai jenis data, walau data itu hanya mendeskripsikan berkas atau **metadata.**

- **Unicode Names**:

  Unicode merupakan paket karakter standar yang digunakan pada NTFS dan menggantikan karakter older-single byte ASCII. Setiap karakter pada kebanyakan bahasa yang natural adalah direpresentasikan dengan double-byte number dalam paket karakter Unicode.

- **Improved File Attribute Indexing**:

  Dalam NTFS juga terdapat kemampuan untuk memberi indeks pada atribut berkas, fungsinya ialah sebagai penglokasian dan sorting.

- **Data Compression**:

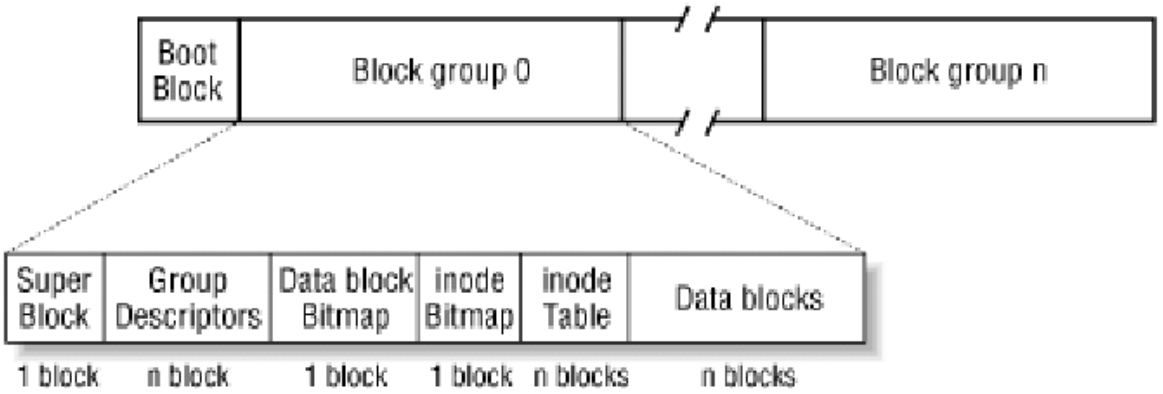
Dalam kompresi data metode yang digunakan adalah Lempel-Ziv Compression. Dengan algoritma ini dipastikan tidak ada data yang hilang pada proses kompresi.

EXT2 File System

- EXT2 menggunakan mekanisme yang mirip dengan BSD Fast File System (ffs) dalam mengalokasikan blok-blok data dari file. Hanya saja

EXT2 File System (Cont.)

- Layout dari partisi dan group block Ext2FS



EXT3 File System

- Ext3FS merupakan pengembangan dari Ext2FS.
- Ext3FS memiliki beberapa kelebihan antara lain:

✓Optimasi waktu pengecekan jika terjadi kegagalan sumber daya, kerusakan sisem atau *unclean shutdown*.

✓Integritas data dan kecepatan akses yang fleksibel.

METADATA

Pengertian Metadata

- Metadata adalah data tentang data.
- Terdapat beberapa jenis metadata yang sering digunakan pada komputer forensik:

✓ Metadata sistem file
✓ Metadata gambar digital
✓ Metadata dokumen

Metadata Gambar Digital

- Dari sebuah gambar digital dapat diambil data-data seperti berikut ini:
- Tanggal dan waktu pembuatan gambar
- Resulosi gambar
- Jenis kamera penghasil gambar
- Ekstensi gambar
- Iso, exposure time, focal length dan pengaturan lain yang digunakan pada saat penggambilan gambar

Metadata Dokumen

- Dari sebuah dokumen elektronik dapat diperoleh informasi seperti berikut ini:
- Tanggal dan waktu pembuatan dokumen
- Ekstensi atau jenis dokumen

Metadata Tools

- Sistem File
  - ✓ Winhex
- Gambar Digital
  - ✓ JPEGsnoop
  - ✓ ExifTool GUI
  - ✓ Jhead
  - ✓ Exif viewer
  - ✓ vinetto
- Dokumen elektronik
  - ✓ ID3 → File music (mp3)
  - ✓ Antiword
  - ✓ Catdoc
  - ✓ Laola
  - ✓ wvWare
  - ✓ FI Tools
  - ✓ Xpdf
  - ✓ Meta-extractor

Data Office

Data pdf

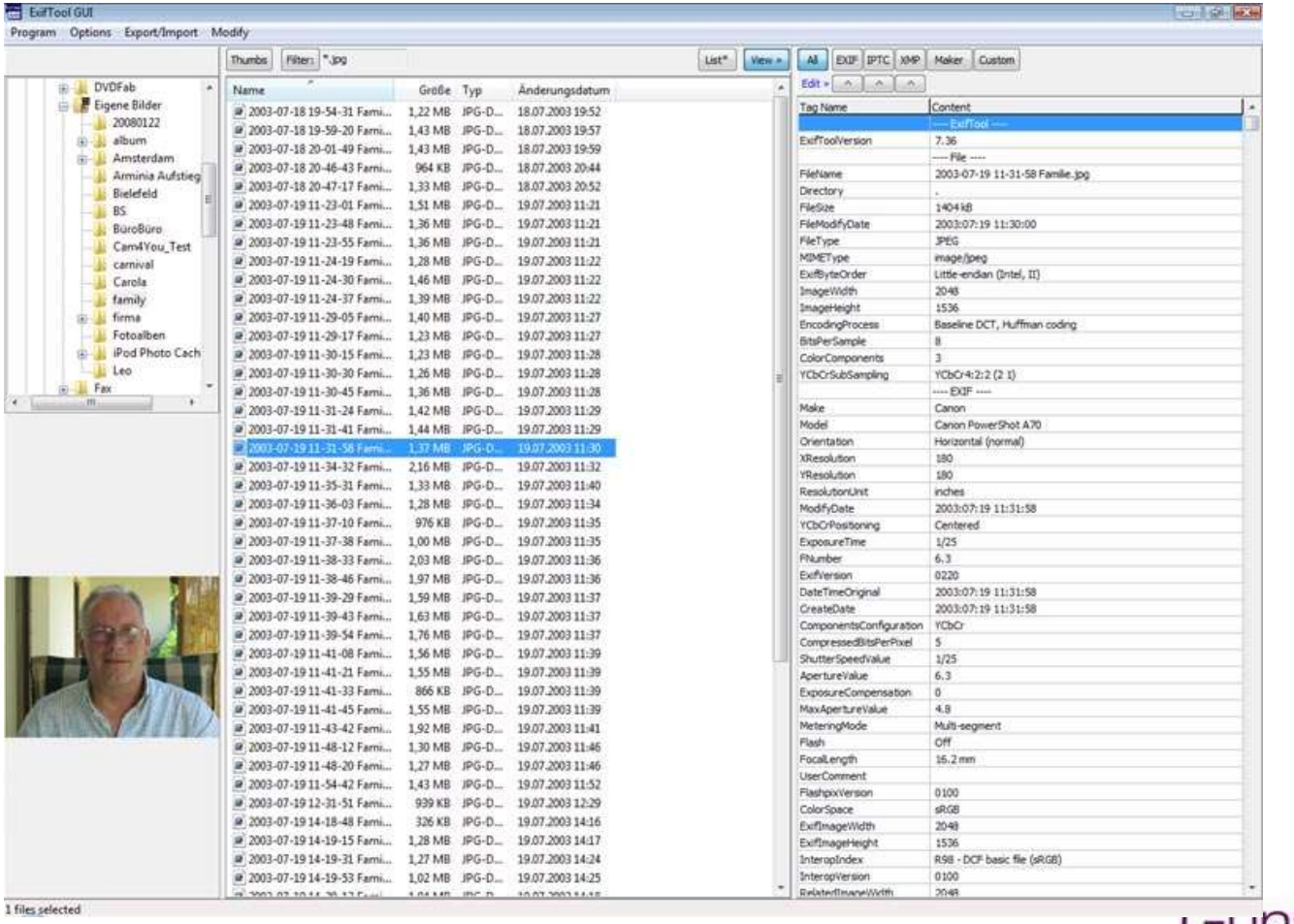
Contoh metadata tools

- JPEGsnoop

- Dengan aplikasi ini, pengguna hanya perlu membuka gambar yang ingin di observasi dan aplikasi ini akan menampilkan metadata dari gambar tersebut

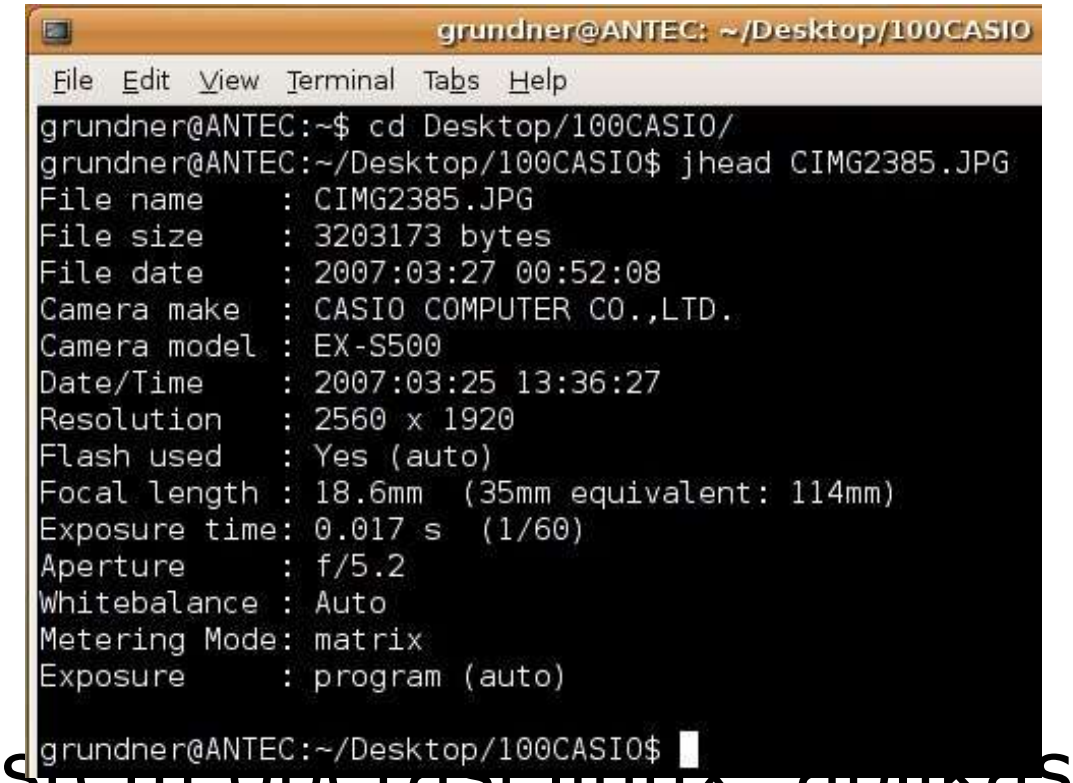
Contoh metadata tools (count.)

- ExifTool GUI



Contoh metadata tools (count.)

- Jhead



- Pada sistem operasi linux, aplikasi ini cukup dipanggil melalui terminal

Contoh metadata tools (count.)

- ID3

- Aplikasi ini digunakan untuk mengetahui metadata dari file musik .mp3

TOOLS DISK FORENSIK

Content :

- Disk Imaging
- Data Recovery
- File Analysis
- Document Metadata Extraction
- Memory Imaging
- Memory Analysis
- Network Forensics
- Logfile Analysis

Disk Imaging

1. **Hardware Imager**
   - Data Compass
   - DeepSpar Disk Imager
   - Data copy king
   - ICS Solo3
   - Logicube Talon
   - PSIClone
   - Voom HardCopy III

Disk Imaging (cont)

1. **Unix-based imagers**
   - guymager
   - ewfacquire
   - Adepto
   - aimage
   - AIR
   - dcfldd
   - dd
   - EnCase LinEn
   - GNU ddrescue
   - dd_rescue
   - iLook IXimager
   - MacQuisition Boot CD
   - rdd
   - sdd

Disk Imaging (cont)

1. **Windows-based imagers**
   - AccessData
   - ASR
   - DIBS
   - EnCase
   - FTK Imager by AccessData
   - Ghost
   - iLook
   - Paraben
   - ProDiscovery
   - X-Ways Replica

Data Recovery

1. **Partition Recovery**
   - NTFS Partition Recovery
   - CD/DVD Diagnostic
   - Partition Table Doctor
   - NTFS Recovery
   - gpart
   - TestDisk
   - Partition Recovery Software

Data Recovery (cont)

1. **Data Recovery**
   - Stellar Data Recovery
   - HD Doctor Suite
   - SalvationDATA
   - BringBack
   - RAID Reconstructor
   - e-ROL
   - Recuva
   - Restoration
   - Undelete Plus
   - R-Studio
   - DeepSpar Disk Imager
   - Adroit Photo Recovery
   - FreeRecover

Data Recovery (cont)

1. **Carving**
   - DataLifter® - File Extractor Pro
   - NFI Defraser
   - Simple Carver Suite
   - Foremost
   - Scalpel
   - EnCase
   - CarvFs
   - LibCarvPath

Data Recovery (cont)

1. **Carving (cont)**
   - midi-carver
   - PhotoRec
   - PhotoRescue
   - RevIt
   - Magic Rescue
   - FTK
   - X-Ways
   - Adroit Photo Forensics

File Analysis

1. **Image Analysis**
   - SurfRecon LE rapid image analysis tool
2. **Software Forensics**
   - CodeSuite
3. **File Sharing Analysis Tools**
   - eMule Reader
   - P2P Marshal
   - **NDA and scoped distribution tools**

File Analysis (cont)

1. **Open Source Tools**
   - PDF Miner
   - ltrace
   - strace
   - xtrace
   - Valgrind
   - DTrace
   - strings
   - The Open Computer Forensics Architecture
   - Rifiuti
   - Pasco
   - dumpster_dive.pl
   - cookie_cruncher.pl
   - yim2text
   - Hachoir
   - Cygwin
   - UnxUtils
   - GnuWin32
   - SUA

Document Metadata Extraction

1. **Office Files**
   - file
   - ldd
   - antiword
   - catdoc
   - laola
   - word2x
   - wvWare
   - Outside In
   - FI Tools

Document Metadata Extraction

1. **PDF Files**
   - Xpdf

2. **Images**
   - Exiftool
   - jhead
   - vinetto
   - libexif
   - Adroit Photo Forensics
   - Exif Viewer

Document Metadata Extraction

1. **Images**
   - exiftags
   - exifprobe
   - Exiv2
   - pngtools
   - pngmeta
2. **General**
   - Metadata Extraction Tool
   - Metadata Assistant
   - hachoir-metadata
   - file
   - GNU libextractor
   - Directory Lister Pro

Memory Imaging

1. **Memory Imaging Techniques**
   - Crash Dumps
   - LiveKd Dumps
   - Hibernation Files
   - Firewire
   - Virtual Machine Imaging

Memory Imaging (cont)

1. **Memory Imaging Tools**
   - **x86 Hardware**
   - **Windows Software**
   - **Linux/Unix**
   - **Mac OS X**
   - **Virtual**

Memory Analysis

1. **Memory Analysis Frameworks**
   - Volatility Framework
   - Second Look
2. **Browser Email Memory Tool**
   - Pdgmail
3. **Instant Messenger Memory Tool**
   - Belkasoft Evidence Center

Network Forensics

1. **Network Forensics Packages and Appliances**
2. **Command-line tools**
   - ARP and Ethernet MAC Tools
   - CISCO Discovery Protocol Tools
   - ICMP Layer Tests and Attacks
   - IP Layer Tests
   - UDP Layer Tests
   - TCP Layer

Logfile Analysis

1. **General Tools**
   - Log Parser 2.2
2. **Web Logfile Analytics**
   - Analog
   - Webalizer
   - phpMyVisites
   - AWStats
   - JasperReports
   - Open Web Analytics
   - Breadboard BI Web Analytics

Terima Kasih