

Proyek Akhir
EC 5010 Keamanan Sistem Informasi

Forensik Komputer:
Evaluasi Autopsy dan Sleuthkit

Oleh:
Daniel Widyanto
13200021



DEPARTEMEN TEKNIK ELEKTRO
INSTITUT TEKNOLOGI BANDUNG
2004

Semua gambar/ilustrasi versi cetak makalah ini telah dipotong
untuk menghemat tinta dan kertas. Mohon mengacu ke versi elektronik makalah ini.

*Anda akan lebih mudah membaca versi elektronik makalah ini sambil membuka dan mempelajari autopsy /
sleuthkit daripada membaca versi cetaknya. Jika Anda harus mencetak makalah ini, mohon gunakan kertas
bekas yang masih kosong lembar sebaliknya.*



Save Our Forest

ABSTRAK

Sleuthkit adalah *open source* forensik *toolkit* yang berlisensi GPL. Sleuthkit merupakan penerus TCT (*the coroner toolkit*) dan TCTUTILS. Sebagai penerus TCT / TCTUTILS, sleuthkit mempunyai banyak keunggulan. Diantaranya adalah analisis post-mortem terhadap file sistem lain, yang berbeda sistem operasi maupun arsitektur dengan host penganalisa. File sistem yang didukung oleh sleuthkit saat tulisan ini dibuat adalah NTFS, FAT16, FAT32, EXT2, EXT3, FFS, BSD, Mac, dan Sun partition.

Sleuthkit sebenarnya adalah kumpulan program-program *shell* kecil yang dapat digunakan untuk melakukan analisa forensik. Autopsy menyediakan *graphical interface* ke sleuthkit. Penggunaan autopsy mempermudah pengguna sleuthkit untuk menginterpretasikan data hasil analisa. Selain itu, autopsy juga menyediakan fasilitas manajemen kasus. Oleh karena itu, penggunaan autopsy sangat disarankan.

Makalah ini membahas hasil evaluasi penulis terhadap kedua program. Pembahasan meliputi instalasi, penggunaan fasilitas, dan konfigurasi.

Daftar Isi

ABSTRAK.....	i
1. Pendahuluan.....	1
2. Instalasi Sleuthkit.....	1
3. Instalasi Autopsy.....	2
4. Ekstraksi Image.....	2
Penggunaan dd di Linux.....	3
Penggunaan dd di Windows.....	3
Menganalisa Partisi Tertentu dari Image.....	4
6. Fasilitas Autopsy.....	4
Menjalankan Autopsy.....	4
Manajemen Kasus (Case Management).....	5
Struktur Case Management Autopsy.....	6
Autopsy.log.....	6
Case.aut.....	6
Case.log.....	6
Investigators.txt.....	7
Host.aut.....	7
Host.log.....	8
NamaInvestigator.log.....	8
NamaInvestigator.notes.....	8
NamaInvestigator.exec.log.....	8
Fungsi Utama Autopsy.....	8
File Analysis.....	9
File Type.....	9
Meta Data Analysis.....	9
Data Unit Analysis.....	10
Image Details.....	10
Keyword Search.....	10
Live Analysis.....	11
7. Fasilitas Sleuthkit.....	11
File System Tools.....	11
Data Unit Layer Tools.....	11
Meta Data Unit Layer.....	12
File Name Layer.....	13
Filesystem Layer.....	13
Media Management Tools.....	13
10. Kesimpulan.....	14
11. Daftar Pustaka.....	14

1. Pendahuluan

Sleuthkit dan autopsy adalah *open source* forensik *toolkit* penerus TCT / TCTUTILS. Sleuthkit merupakan kumpulan program shell untuk melakukan analisa forensik. Autopsy menyediakan *graphical user interface* sleuthkit. Sleuthkit dan autopsy dapat dijalankan di hampir semua varian UNIX (Linux, OS X, FreeBSD, OpenBSD, Solaris).

Sleuthkit, secara umum, terdiri dari dua bagian, yaitu *file system tools* dan *media management tools*. *File sistem tools* berguna untuk menganalisis file sistem. Hal ini memungkinkan sleuthkit untuk menganalisis file-file yang telah dihapus ataupun disembunyikan. *Media management tools* berguna untuk menganalisis *disk/media layout*. Versi terbaru sleuthkit mampu mengenali partisi DOS, BSD, Mac, dan Sun. Dengan bantuan *media management tools*, sebuah partisi dapat diekstrak dari media lalu dianalisis dengan *file system tools*..

Autopsy sebenarnya adalah sebuah mini web server dengan script CGI berbasis perl. Autopsy menggunakan perl untuk menjalankan program-program sleuthkit dan mengubah hasilnya ke HTML. Oleh karena itu, pengguna Autopsy membutuhkan web client untuk mengakses fungsi-fungsi Autopsy. Selain sebagai *user interface* sleuthkit, Autopsy menyediakan fungsi-fungsi administratif tambahan. Beberapa fungsi tersebut adalah *logging* (mencatat tindakan / perintah sleuthkit yang telah dijalankan), *notes* (mencatat keterangan tambahan yang diperoleh penyelidik), dan *report* (mencatat hasil analisa).

Keterangan lebih lanjut tentang autopsy dan sleuthkit dapat diperoleh di <http://sleuthkit.sourceforge.net> atau <http://www.sleuthkit.org/>

2. Instalasi Sleuthkit

Sleuthkit terbaru saat tulisan ini dibuat adalah Sleuthkit-1.70. *Source code* sleuthkit dapat diambil di <http://prdownloads.sourceforge.net/sleuthkit/sleuthkit-1.70.tar.gz?download>

Untuk menginstall sleuthkit, ekstrak *source code* sleuthkit ke direktori yang diinginkan, lalu kompilasi dengan make.

```
su
tar -xvzf sleuthkit-1.70.tar.gz -C /usr/local
make
```

Agar sleuthkit dapat digunakan oleh autopsy, buat softlink direktori *sleuthkit-versi* ke direktori *sleuthkit*.

```
ln -s /usr/local/sleuthkit-1.70 /usr/local/sleuthkit
```

Sleuthkit umumnya tidak perlu diinstall sebagai *user binaries* (diletakkan di `/usr/local/bin`), karena sleuthkit akan dipanggil oleh autopsy. Bila Anda menghendaki sleuthkit dapat digunakan sebagai *user binaries*, Anda harus mengkopikan hasil kompilasi secara manual ke direktori yang Anda inginkan.

3. Instalasi Autopsy

Versi terbaru autopsy saat ini adalah 2.01 dan dapat didownload di <http://prdownloads.sourceforge.net/autopsy/autopsy-2.01.tar.gz?download>. Instalasi autopsy hampir sama dengan instalasi sleuthkit.

```
su
tar -xvzf autopsy-2.01.tar.gz -C /usr/local
make
```

Setelah itu, autopsy akan menanyakan letak beberapa program yang diperlukan, letak direktori sleuthkit (jawab dengan direktori softlink `/usr/local/sleuthkit`), letak file NSRL, dan direktori yang akan digunakan untuk menyimpan file kasus yang akan diperiksa. File NSRL adalah file yang berisi *digital signature* dari program-program yang umum digunakan. File ini dapat didownload dari <http://www.nsrl.nist.gov/Downloads.htm>.

4. Ekstraksi Image

Sleuthkit dan autopsy selalu bekerja dengan kopi media asli. Hal ini dilakukan agar data di media asli tidak berubah. Selain itu, jika terjadi kesalahan prosedur pada data kopi, data asli bisa dikopi ulang. Untuk itu, diperlukan software tool yang dapat mengkopir isi media *bit by bit*. Di keluarga UNIX, tool yang dapat melakukan hal itu adalah dd.

Perhatian : Subbab ini hanya menjelaskan cara mendapatkan image yang valid untuk dianalisis sleuthkit. Ikuti prosedur forensik *incident handling* untuk analisis forensik sesungguhnya.

Penggunaan dd di Linux

dd adalah bagian dari paket coreutils (di Linux), dan umumnya terinstall di semua varian UNIX. Format perintah dd adalah :

```
$ dd if=/dev/namadevice of=namafile bs=besar_sektor count=banyak_sektor
```

Contoh penggunaan dd di Linux :

- Untuk mengambil partisi pertama di IDE kedua (hdb1) sebesar 650MB, ketikkan :

```
$ dd if=/dev/hdb1 of=image_hdb1 bs=1024k count=650
```

- Untuk mengambil image dari floppy disk A:\ (fd0), ketikkan

```
$ dd if=/dev/fd0 of=image_fd0 bs=1k count=1440
```

Penggunaan dd di Windows

Jika tidak terdapat komputer yang dapat menjalankan UNIX, dapat digunakan dd versi DOS/Windows. dd versi Windows/DOS dapat didownload dari <http://unxutils.sourceforge.net/>. Format perintah dd untuk DOS/Windows adalah :

```
$ dd if=\\.\namadevice of=namafile bs=besar_sektor count=banyak_sektor
```

Contoh penggunaan dd di Windows

- Untuk mengambil image dari floppy disk A:\, ketikkan

```
$ dd if=\\.\a: of=c:\temp\disk1.img bs=1440k count=1
```

- Untuk mengambil image CDROM pertama

```
$ dd if=\\?\Device\CdRom0 of=c:\temp\disc1.iso bs=1M
```

- Untuk mengambil image dari partisi tertentu di harddisk

```
$ dd if=\\.\Harddisk<n>\Partition<n> of=c:\temp\image
```

Keterangan : n=0 utk harddisk pertama, partition0 adalah seluruh harddisk.

Menganalisa Partisi Tertentu dari Image

Sleuthkit *file system tools* hanya dapat menganalisa file sistem. Artinya hanya sebuah partisi yang dapat diperiksa tiap saat. Bila terdapat banyak partisi dalam image (contohnya bila seluruh harddisk di-dd), tiap partisi harus dipisahkan dalam image tersendiri. Untuk mengekstrak partisi, gunakan bantuan `fdisk`.

```
$ fdisk -lu image (image adalah nama file image)
Disk image: 0 heads, 0 sectors, 0 cylinders
Units = sectors of 1 * 512 bytes

Device      Boot  Start      End      Blocks      Id      System
image1      *     63         16064999   8032468+    83     Linux
image2             16065000   32129999   8032500     7      NTFS
image3             32130000   40162499   4016250     83     Linux
image4             40162500   58621184   9229342+    5      Extended
image5             40162563   48194999   4016218+    83     Linux
image6             48195063   58621184   5213061     83     Linux
```

Untuk mengekstrak partisi tertentu, gunakan option `skip` di `dd`. Contohnya untuk mengekstrak `image2` dari file `image`, gunakan perintah :

```
$ dd if=image of=image2 bs=512 skip=16065000 \
    count=$((32129999-16065000+1))
```

Untuk mengekstrak `image3`, ketikkan :

```
$ dd if=image of=image3 bs=512 skip=32130000 \
    count=$((40162499-32130000+1))
```

Catatan : sesuaikan ukuran `bs` dengan besar unit hasil `fdisk` (`bs=512` karena `Units = sectors of 1 * 512 bytes`)

6. Fasilitas Autopsy

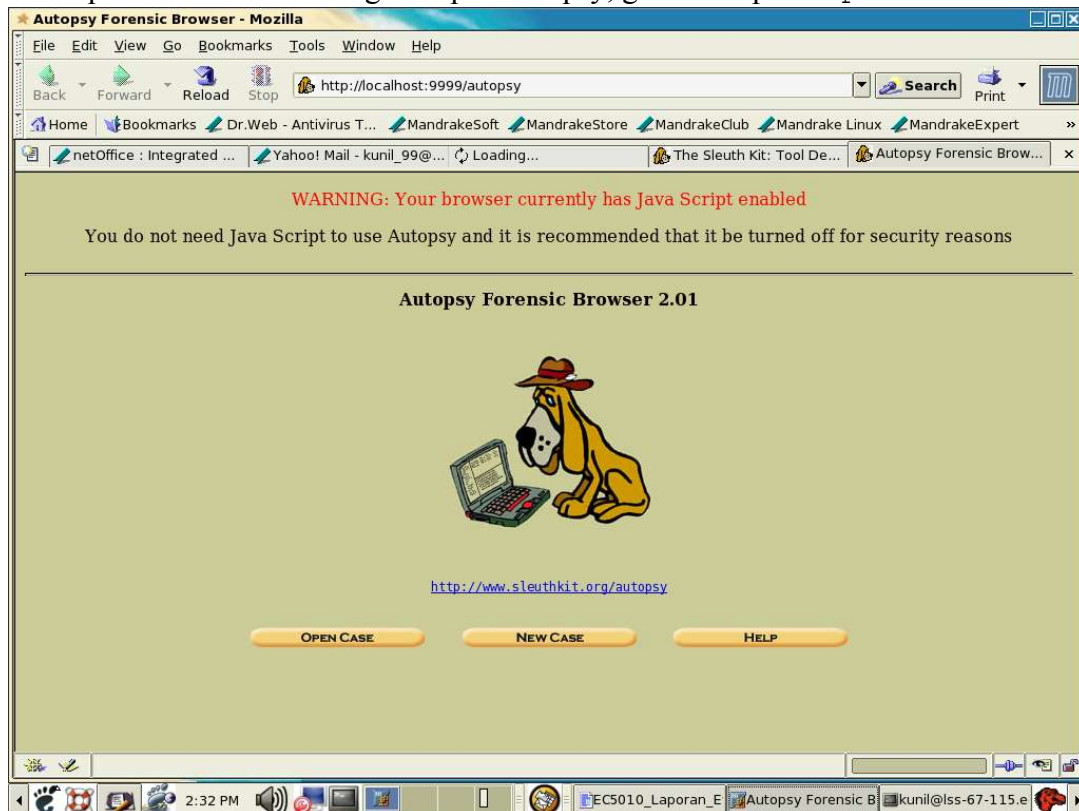
Menjalankan Autopsy

Untuk menjalankan autopsy, ketik :

```
$ /usr/local/autopsy-2.01/autopsy
```

Kopi URL yang diberikan ke HTML browser yang ada. Secara default autopsy akan

berjalan di port 9999. Untuk mengubah port autopsy, gunakan option `-p`



Gb 1 Autopsy Welcome Screen

```
$ /usr/local/autopsy-2.01/autopsy -p no_port
```

Autopsy hanya akan menerima sebuah koneksi dari sebuah host (defaultnya adalah localhost). Agar autopsy dapat diakses oleh host lain (selain localhost), ketikkan IP host yang bersangkutan.

```
$ /usr/local/autopsy-2.01/autopsy 167.205.67.115
```

Agar beberapa host dapat mengakses autopsy, gunakan kombinasi port dan alamat IP.

Contoh :

```
$ /usr/local/autopsy-2.01/autopsy -p 13221 167.205.67.115
```

```
$ /usr/local/autopsy-2.01/autopsy -p 9999 localhost
```

Tiap host harus menggunakan port terpisah. Autopsy menggunakan cookies untuk memvalidasi hal ini.

Manajemen Kasus (*Case Management*)

Case/kasus adalah investigasi yang sedang dilakukan. Untuk sebuah kasus terdapat satu atau beberapa penyelidik (*investigator*). Dalam sebuah kasus juga terdapat satu atau beberapa

host yang terlibat. *Case management* di autopsy di-implementasikan dengan hirarki direktori.

Struktur Case Management Autopsy

Berikut adalah struktur direktori yang dibuat autopsy untuk manajemen kasus.

```

/direktori EvidenceLocker ( didefinisikan di file conf.pl atau dengan option -d )
|-autopsy.log
|-NamaKasus/
    |-case.aut
    |-case.log
    |-investigators.txt
    |-NamaHost/
        |-host.aut
        |-images/ (menyimpan host image)
        |-output/ (menyimpan hasil output sleuthkit)
        |-logs/
            |-host.log
            |-NamaInvestigator.log
            |-NamaInvestigator.notes
            |-NamaInvestigator.exec.log
        |-report/ (menyimpan report dalam bentuk text/HTML)
        |-mnt/ (digunakan untuk loopback mounting di versi mendatang)

```

Keterangan :

Autopsy.log

Mencatat aktifitas umum autopsy. Meliputi waktu ketika autopsy dijalankan dan dihentikan, waktu dan tanggal kasus dibuat dan dibuka, dan *unauthorized connection*.

Case.aut

Case configuration file. Meliputi pencatatan kapan kasus dibuat, deskripsi kasus, dan lokasi direktori tempat menyimpan image, log, report, dan output hasil sleuthkit.

Case.log

Mencatat kapan kasus dibuat, dibuka, kapan host ditambahkan / dibuka, dan oleh siapa.

Investigators.txt

Nama-nama penyelidik. File ini hanya digunakan untuk keperluan logging (tidak untuk autentifikasi).

Host.aut

Host configuration file. Mencatat file-file yang digunakan oleh host dan timezone host. Berikut adalah beberapa entry konfigurasi dan artinya :

<i>Tipe</i>	<i>Deskripsi</i>	<i>Argumen</i>	<i>Contoh</i>
desc	Deskripsi host	String deskripsi	desc DNS server dari New York data center
image	Image file sistem	Path ke file sistem image, tipe file system, dan mounting point filesistem di host	image images/image1 ntfs C:
dls	Unallocated data from file system images	Path ke iange 'dls' dan path ke file system image asli	dls output/part1.dls images/part1.dd
strings	File berisi string yang ada di file system atau dls images	Path ke file string dan path ke original image	strings output/part1.str images/part1.dd
body	File body yang digunakan ketika membuat timelines	Path ke body file	body output/body
timeline	File aktivitas timeline	Path ke file timeline	timeline output/timeline.march15
timezone	Timezone tempat asal host yang dianalisa	Variabel Timezone (legal TZ values)	timezone EST5EDT

<i>Tipe</i>	<i>Deskripsi</i>	<i>Argumen</i>	<i>Contoh</i>
timeskew	Beda clock host yang dianalisa dengan host pemeriksa (dalam detik)	Bilangan bulat positif atau negatif	timeskew -24
alert_db	The 'known bad' hash database	Path ke database	alert_db /usr/local/forensics /database/linux-rootkits.md5
exclude_db	The 'known good' hash database	Path ke database	exclude_db /usr/local/forensics /database/redhat-8.0.md5

Host.log

Generic host log file. Mencatat kapan host dan image dibuka.

NamaInvestigator.log

Berisi tindakan yang dilakukan investigator (meliputi direktori/file yang dibuka).

NamaInvestigator.notes

Berisi catatan kecil yang dibuat oleh investigator.

NamaInvestigator.exec.log

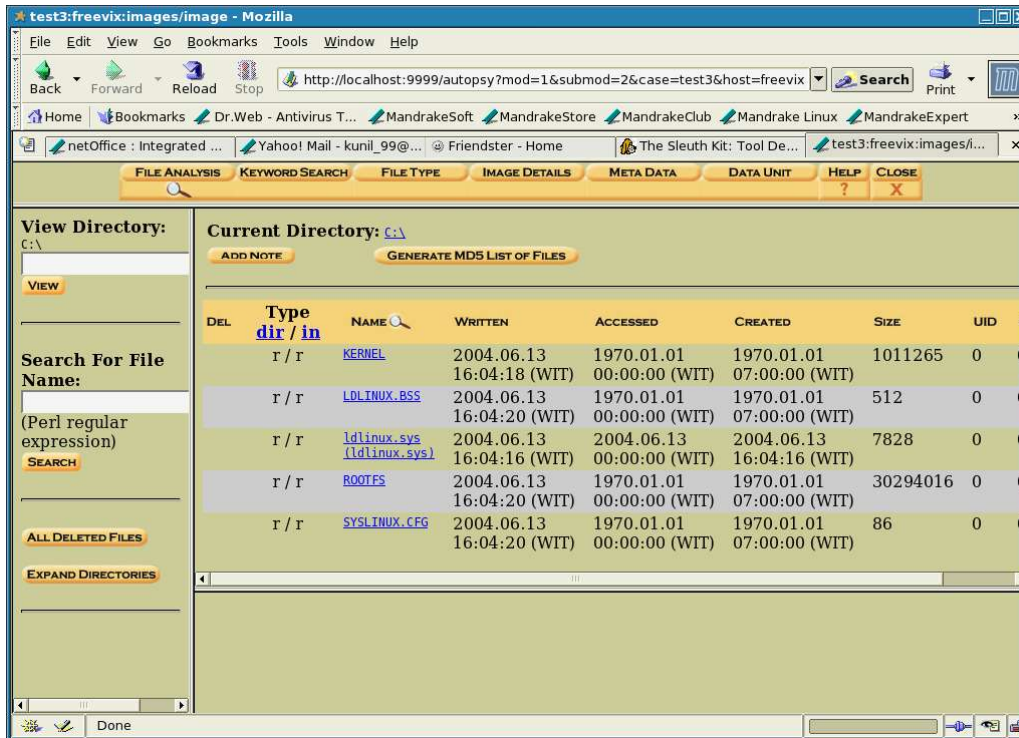
Mencatat perintah-perintah sleuthkit (yang dijalankan lewat autopsy) yang dilakukan oleh investigator.

Fungsi Utama Autopsy

Autopsy menggabungkan beberapa perintah sleuthkit untuk melakukan fungsi-fungsi utamanya. Berikut adalah penjelasan fungsi-fungsi utama autopsy.

File Analysis

Browsing image sebagai file system. Memberikan daftar direktori di kiri dan nama serta isi file di kanan frame.



Gb 2 File Analysis

Isi file dapat dilihat sebagai ASCII, raw, hex atau di-inputkan ke program strings (untuk mengekstrak string dari file). File-file yang terhapus ditandai dengan huruf merah.

Selain itu, isi direktori dapat diurutkan berdasar nama, ukuran, waktu, dsb. Isi file HTML akan di-sanitasi (javascript/vbscript dan link akan di-disable).

File Type

Mensortir file berdasarkan *internal signature*-nya. Dapat digunakan untuk mengidentifikasi jenis file (GIF, JPG, PDF, dst). Selain itu, extension file juga akan dibandingkan dengan *signature*, untuk mengetahui apakah sebuah file disembunyikan dengan mengubah jenis ekstensinya.

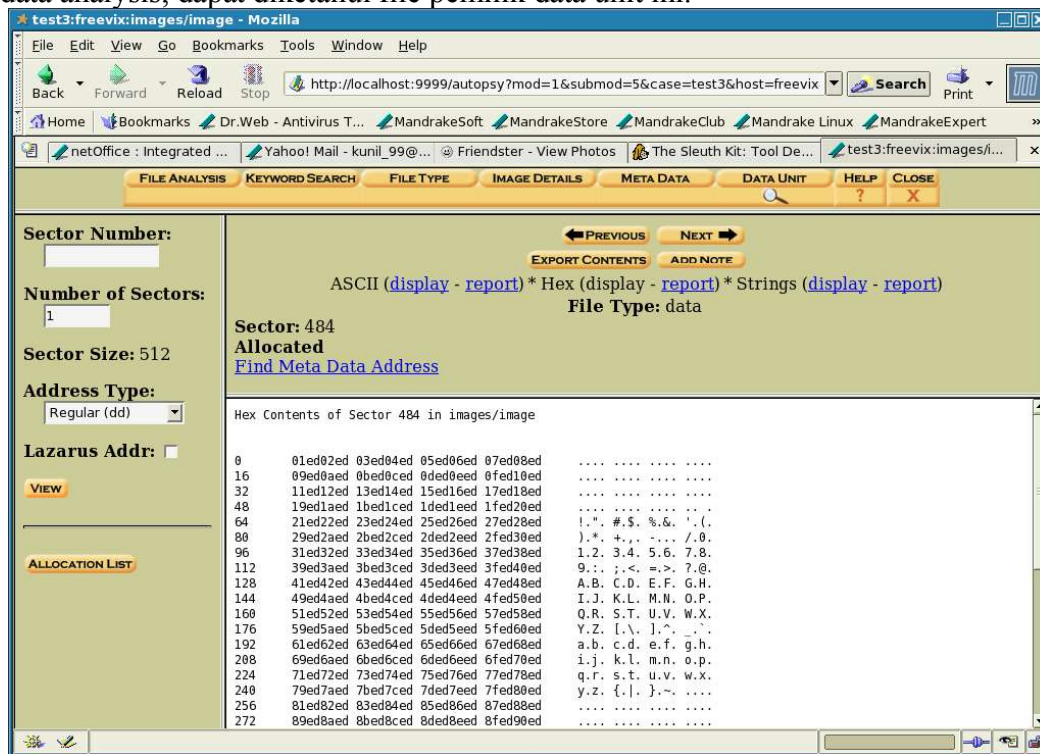
Meta Data Analysis

Meta data adalah struktur yang berisi detail file / direktori. Autopsy mampu

menampilkan struktur ini. Hal ini berguna untuk *me-recover* isi media yang telah dihapus.

Data Unit Analysis

Data unit adalah tempat isi file disimpan. Autopsy mampu menampilkan data unit dalam berbagai format, termasuk ASCII, hexdump, and strings. Selain itu, dengan bantuan meta-data analysis, dapat diketahui file pemilik data unit ini.



Gb 3 Data Unit Analysis

Image Details

Menampilkan detail file sistem, termasuk layout file sistem di media dan aktifitas.

Keyword Search

Mencari pola string tertentu di image file sistem. Pola yang dicari dapat berupa ASCII strings ataupun *grep regular expressions* (regex). Pencarian dapat dilakukan di seluruh image, atau bagian-bagian tertentu.

Live Analysis

Kelebihan lain autopsy-2.01 adalah kemampuan untuk melakukan *live analysis*. *Live analysis* adalah teknik analisa diatas host yang sedang berjalan (tanpa men-*shutdown* host dulu). Teknik ini tidak dianjurkan sebab menggunakan *software tools* yang terdapat di host (ada kemungkinan *software tools* tersebut merupakan trojan). Akan tetapi, teknik ini dapat digunakan untuk mem-*preserve* isi memori *volatile* (RAM).

Untuk mencegah agar trojan tersebut tidak digunakan dalam analisa, umumnya program-program yang digunakan untuk analisa dikompilasi secara statik (di host lain yang dijamin *secure*), lalu di-*burn* ke CD. Autopsy menyediakan fasilitas untuk ini.

Untuk membuat CD berisi autopsy dan sleuthkit yang independen (dikompilasi statik), ketikkan perintah ini di direktori *source* autopsy :

```
$ make live
```

Hasil dari perintah ini adalah direktori `live-cd` yang siap di-*burn* ke CD. Lebih lanjut dengan metode analisa live, dapat dilihat di file `README-LIVE.txt` (di direktori *source* autopsy) atau di <http://www.sleuthkit.org/informer/sleuthkit-informer-13.html>

7. Fasilitas Sleuthkit

Sebagaimana telah dijelaskan di atas, tool di sleuthkit dapat dibagi menjadi dua bagian besar, yaitu *file system tools* dan *media management tools*. *File system tools* kemudian dibagi lagi menjadi *data unit layer tools*, *meta data unit layer tools*, *file name layer tools*, dan *file system tools*.

File System Tools

Data Unit Layer Tools

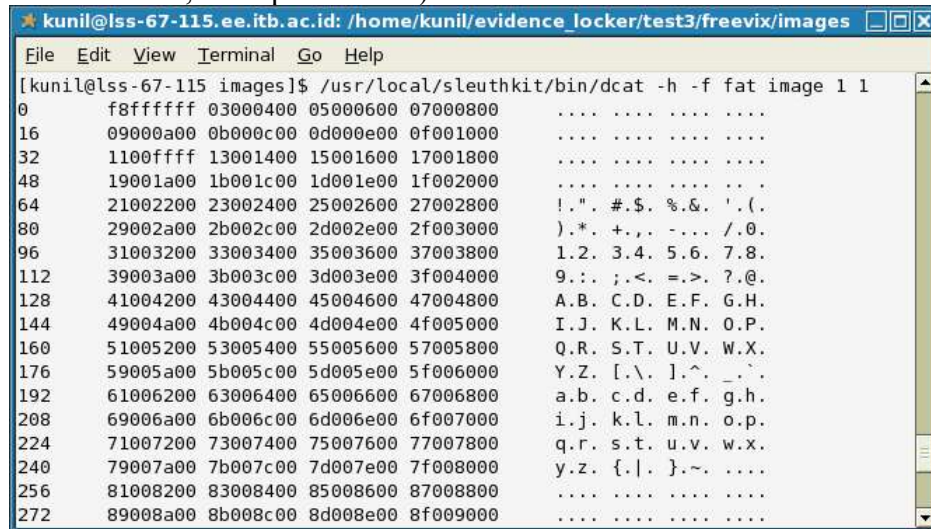
Data unit layer adalah lapisan/*layer* dari filesistem yang menyimpan isi file. Terdapat empat tool yang dapat digunakan di *layer* ini, yaitu

dcat : Mengekstrak isi dari data unit dan menampilkannya ke *stdout*.

dls : Menampilkan detail isi data unit dan mempunyai kemampuan untuk mengekstrak

unallocated space di filesystem

dstat: Menampilkan informasi tentang data unit (meliputi teralokasi atau tidak, cluster pemilik data unit, dan tipe data unit)



```

kunik@lss-67-115.ee.itb.ac.id: /home/kunik/evidence_locker/test3/freevix/images
File Edit View Terminal Go Help
[kunik@lss-67-115 images]$ /usr/local/sleuthkit/bin/dcat -h -f fat image 1 1
0      f8ffffff 03000400 05000600 07000800      ....
16     09000a00 0b000c00 0d000e00 0f001000      ....
32     1100ffff 13001400 15001600 17001800      ....
48     19001a00 1b001c00 1d001e00 1f002000      ....
64     21002200 23002400 25002600 27002800      !. " #. $ % & ' ( .
80     29002a00 2b002c00 2d002e00 2f003000      ) * + , - . / 0 .
96     31003200 33003400 35003600 37003800      1.2. 3.4. 5.6. 7.8.
112    39003a00 3b003c00 3d003e00 3f004000      9.: ; < = > ? @ .
128    41004200 43004400 45004600 47004800      A.B. C.D. E.F. G.H.
144    49004a00 4b004c00 4d004e00 4f005000      I.J. K.L. M.N. O.P.
160    51005200 53005400 55005600 57005800      Q.R. S.T. U.V. W.X.
176    59005a00 5b005c00 5d005e00 5f006000      Y.Z. [\ . ] ^ _ ` .
192    61006200 63006400 65006600 67006800      a.b. c.d. e.f. g.h.
208    69006a00 6b006c00 6d006e00 6f007000      i.j. k.l. m.n. o.p.
224    71007200 73007400 75007600 77007800      q.r. s.t. u.v. w.x.
240    79007a00 7b007c00 7d007e00 7f008000      y.z. { | } ~ .
256    81008200 83008400 85008600 87008800      ....
272    89008a00 8b008c00 8d008e00 8f009000      ....

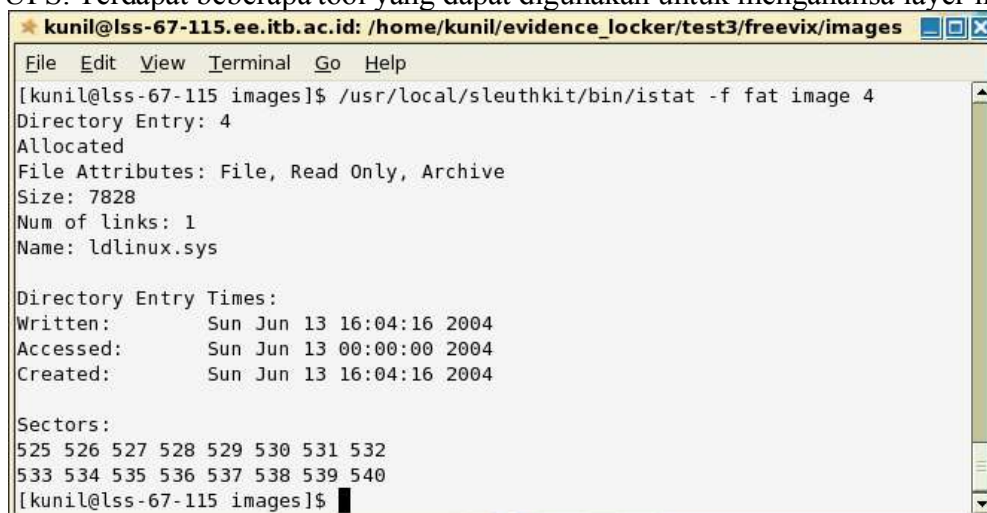
```

Gb 4 dcat result

dcalc: Menghitung posisi data unit di media.

Meta Data Unit Layer

Meta data unit layer adalah lapisan/layer filesystem yang menyimpan detail sebuah file. Contohnya adalah struktur hirarki direktori di FAT, MFT di NTFS, ataupun *inode* di EXT2 / EXT3 / UFS. Terdapat beberapa tool yang dapat digunakan untuk menganalisa layer ini, yaitu :



```

kunik@lss-67-115.ee.itb.ac.id: /home/kunik/evidence_locker/test3/freevix/images
File Edit View Terminal Go Help
[kunik@lss-67-115 images]$ /usr/local/sleuthkit/bin/istat -f fat image 4
Directory Entry: 4
Allocated
File Attributes: File, Read Only, Archive
Size: 7828
Num of links: 1
Name: ldlinux.sys

Directory Entry Times:
Written:      Sun Jun 13 16:04:16 2004
Accessed:    Sun Jun 13 00:00:00 2004
Created:     Sun Jun 13 16:04:16 2004

Sectors:
525 526 527 528 529 530 531 532
533 534 535 536 537 538 539 540
[kunik@lss-67-115 images]$

```

Gb 5 istat result

icat : Mengekstrak data unit yang ditunjuk oleh alamat meta data (*inode*). Dapat digunakan untuk merecover/undelete file

ifind: Untuk mencari alamat *meta data unit* yang menunjuk ke alamat data unit tertentu.

Dapat juga digunakan untuk mencari alamat meta data unit dengan nama file yang dicari sebagai input.

ils : menampilkan isi struktur *meta data* (MAC time, size allocated, dll.).

istat: menampilkan statistik dan detil meta data unit. Menampilkan nama/jenis file, MAC time, dan alamat data unit yang digunakan file tersebut.

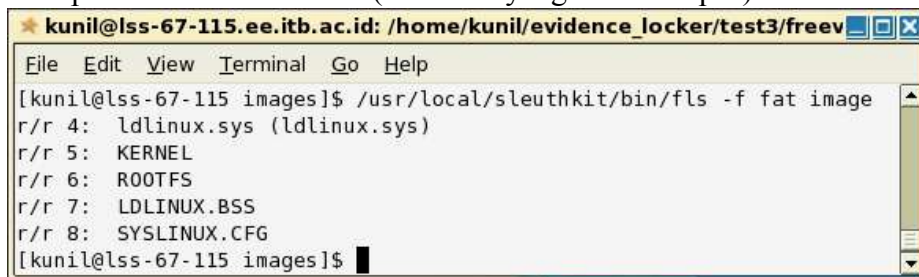
File Name Layer

Sesuai namanya, file name layer adalah bagian dari file sistem yang memuat nama file.

Beberapa tool yang dapat digunakan di layer ini antara lain adalah :

ffind: menampilkan nama file yang ditunjukkan oleh input meta data unit

fls : menampilkan semua nama file (termasuk yang telah dihapus)



```

kunil@lss-67-115.ee.itb.ac.id: /home/kunil/evidence_locker/test3/freew
File Edit View Terminal Go Help
[kunil@lss-67-115 images]$ /usr/local/sleuthkit/bin/fls -f fat image
r/r 4:  ldlinux.sys (ldlinux.sys)
r/r 5:  KERNEL
r/r 6:  ROOTFS
r/r 7:  LDLINUX.BSS
r/r 8:  SYSLINUX.CFG
[kunil@lss-67-115 images]$

```

Gb 6 fls result

Filesystem Layer

Tool yang tergabung di layer ini berguna untuk menampilkan data umum filesistem.

Satu-satunya *tool* yang tergabung di layer ini adalah **fstat**. **fstat** menampilkan tipe filesistem, volume label, volume ID, dan alokasi sektor.

Media Management Tools

Saat ini, satu-satunya *media management tools* yang ada saat ini adalah **mmls**. **mmls** menganalisa image dan menampilkan partisi yang terdapat dalam image tersebut. **mmls** dapat digunakan untuk menampilkan partisi tersembunyi dan sekaligus mengekstrak partisi tersebut sehingga dapat digunakan *file system tools*.

Mmls membutuhkan dua parameter input, tipe filesistem dan nama file image hasil dd. Tipe filesistem yang dikenali mmls adalah :

dos : partisi DOS-based (untuk DOS, Windows, dan Linux)

bsd : FreeBSD, OpenBSD, dan NetBSD disklabels dan slice

mac : partisi Macintosh

sun : Solaris Volume Table of Contents structures and slices

```

kunil@lss-67-115.ee.itb.ac.id: /home/kunil/workplace/freevix-0.72/output
File Edit View Terminal Go Help
[kunil@lss-67-115 output]$ /usr/local/sleuthkit/bin/mmls -t dos rawimage
DOS Partition Table
Units are in 512-byte sectors

   Slot   Start      End          Length      Description
00:  ----   0000000000  0000000000  0000000001  Primary Table (#0)
01:  ----   0000000001  0000000031  0000000031  Unallocated
02:  00:00  0000000032  0000063487  0000063456  DOS FAT16 (0x06)
[kunil@lss-67-115 output]$

```

Gb 7 mmls result

Hasil output yang ditampilkan mmls adalah sebagai berikut :

No. urut : Terletak di kolom pertama. Menunjukkan no. urut partisi yang ditemukan mmls

Slot : Menunjukkan lokasi tabel partisi yang memuat partisi tersebut. Contohnya : 00:00 adalah entry pertama untuk tabel partisi pertama, 01:00 adalah entry pertama untuk tabel partisi kedua (tabel partisi kedua = partisi ekstended).

Start : Sektor dimana partisi dimulai

End : Sektor dimana partisi berakhir

Length : Panjang partisi

Deskripsi : Jenis partisi

10. Kesimpulan

Sleuthkit dan Autopsy merupakan *open-source forensic toolkit* yang berjalan di atas *platform* UNIX. Sleuthkit menyediakan fungsi-fungsi forensik, sedangkan Autopsy menyediakan *user interface* untuk mempermudah analisa hasil sleuthkit. Pemisahan fungsi Sleuthkit dan Autopsy bertujuan untuk meningkatkan fleksibilitas penggunaan kedua tool tersebut.

Sleuthkit dan Autopsy memiliki banyak keunggulan, diantaranya adalah kemampuan

untuk menganalisa berbagai jenis filesistem. Kemampuan ini terus-menerus ditingkatkan berkat konsep *open-source development*. Kemampuan yang sedang dalam tahap *release* pada saat tulisan ini dibuat adalah *live-analysis*, penggunaan NIST NSRL database untuk autentifikasi file-file yang ada di filesistem, dan *sorter* untuk mensortir file berdasarkan tipe filenya.

Contoh penggunaan Sleuthkit / Autopsy di kasus nyata dapat dilihat di <http://sleuthkit.sourceforge.net/case/index.php>. Selain itu, Sleuthkit Informer (<http://sleuthkit.sourceforge.net/informer>) juga merupakan sumber yang baik untuk mengetahui fitur-fitur Sleuthkit/Autopsy beserta tip pemakaiannya.

11. Daftar Pustaka

- Carrier, Bryan, *The Sleuthkit Informer*, <http://sleuthkit.sourceforge.net/informer>
- Utdirartatmo, Firrar, *Tinjauan analisis forensik dan kontribusinya pada keamanan sistem komputer*, <http://budi.insan.co.id/courses/el695/projects/firar.rtf>
- Rahardjo, Budi, *Incident Handling (Penanganan Insiden)*, <http://budi.insan.co.id/courses/el695/IDCERT-incident-handling.ppt>