TUGAS

KEAMANAN JARINGAN KOMPUTER

DISUSUN OLEH :

NAMA : INDAH SARI

NIM : 09011181320011

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017 – 2018

HASIL TRAINING KOMPUTER FORENSICS DI LEB

DEFINISI KOMPUTER FORENSICS

Dari berbagai sumber, definisi komputer forensics secara garis besar adalah suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun piranti digital, agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan.

KASUS :

Telah tertangkap seorang pengedar narkoba kelas kakap, polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta bantuan oleh polisi untuk melakukan forensic terhadap file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut.

TOOLS YANG DIGUNAKAN :

- AutoPsy
- Foremost
- String
- Ghex

Berikut Langkah – Langkah Pengerjaan dari Komputer Forensics :

Lakukan penginstallan tools selain string dan buka alamat web dibawah ini:
http://old.honeynet.org/scans/scan24/

Dari alamat web tersebut muncul halaman utama dari The Honeynet Project dan download file: Image.Zip MD5 = b676147f63923e1f428131d59b1d6a72 (image.zip)

Konfig md5sum image.zip, dimana fungsi md5sum adalah sebuah file yang pasti ada md5sum yang fungsinya untuk mengecek keaslian dari file atau integritas file

```
# md5sum image.zip
b676147f63923e1f428131d59b1d6a72  image.zip
```

Konfig file image, untuk mengecek tipe file. Jika kita menemukan file yang tidak ada ekstensi, maka kita bisa menggunakannya

```
root@mahasiswa:/home/mahasiswa/Downloads# ls
image  image.zip
root@mahasiswa:/home/mahasiswa/Downloads# file image
image: DOS floppy 1440k, x86 hard disk boot sector
root@mahasiswa:/home/mahasiswa/Downloads#
```

Fungsi perintah file image di atas menampilkan image: DOS floppy 1440k, x86 hard disk boot sector, setelah mengetahui bahwa file tersebut file boot sector, maka selanjutnya bisa melakukan proses mounting.

Sebelum melakukan proses mounting buat folder kasus terlebih dahulu yaitu :

```
# mkdir /tmp/kasus
```

Konfig mount image /tmp/kasus

```
root@mahasiswa:/home/mahasiswa/Downloads# mount image /tmp/kasu
s
```

Konfig cd /tmp/kasus, untuk masuk ke folder kasus, lalu ls

```
root@mahasiswa:/home/mahasiswa/Downloads# cd /tmp/kasus
root@mahasiswa:/tmp/kasus# ls
cover page.jpgc             SCHEDU~1.EXE
root@mahasiswa:/tmp/kasus#
```

Dari gambar diatas setelah di ls akan tampil isi dari folder kasus yang telah dibuat sebelumnya, dimana folder tersebut berisi dua file yaitu cover page.jpgc dan SCHEDU~1.EXE

Konfig file * , yang berfungsi untuk mengecek keaslian semua file pada folder kasus

```
root@mahasiswa:/tmp/kasus# file *
cover page.jpgc           : ERROR: cannot read `cover page.jpgc
          ' (Input/output error)
SCHEDU~1.EXE:              Zip archive data, at least v2.0 to
extract
root@mahasiswa:/tmp/kasus#
```

Dimana file yang terbaca dalam folder kasus ini hanya SCHEDU~1.EXE Zip archive data, at least v2.0 to extract

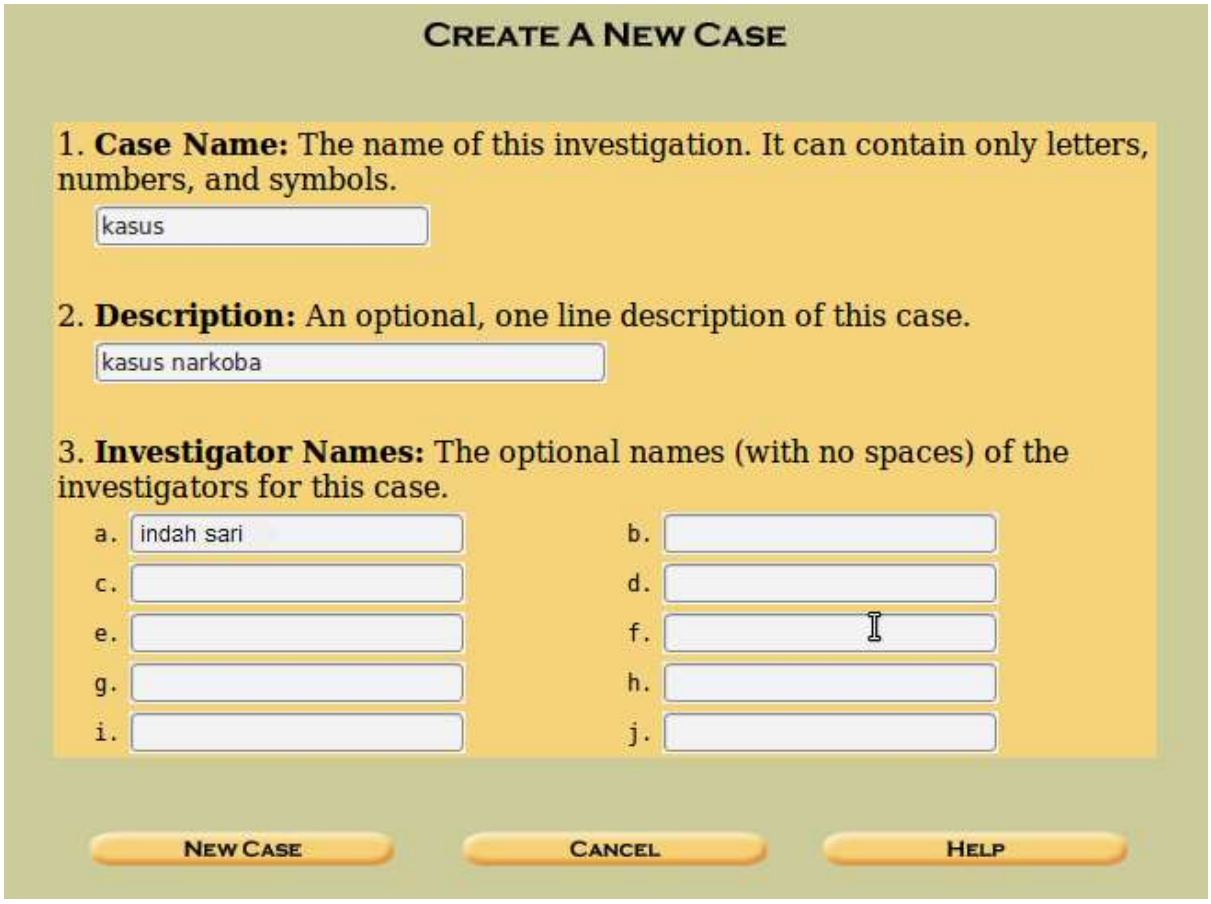
Konfig autopsy, dimana sebelumnya telah di install terlebih dahulu

```
root@mahasiswa:/tmp/kasus# autopsy
  I
================================================================
=============

                    Autopsy Forensic Browser
                http://www.sleuthkit.org/autopsy/
                           ver 2.24

================================================================
=============
Evidence Locker: /var/lib/autopsy
Start Time: Thu Mar 23 10:01:14 2017
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in i
t:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Konfigurasi dari autospy diatas menampilkan remote host dari autospy: localhost, dan memiliki local port 9999

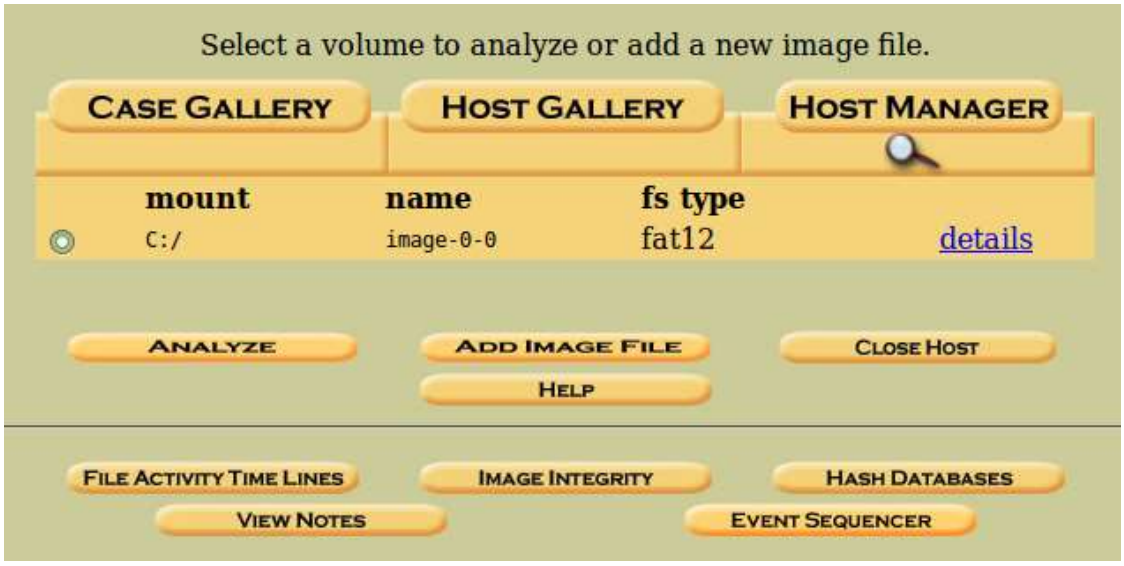
Setelah mengetahui autospy memiliki local host yang memiliki local port 9999, lalu search alamat web localhost.9999/autospy

Dari alamat web localhost.9999/autospy maka akan tampil halaman utama dari Autopsy Forensic Browser 2.24, dimana halaman ini berfungsi untuk mengatur hostname, siapa yang melakukan forensik pada komputer target. Klik New Care



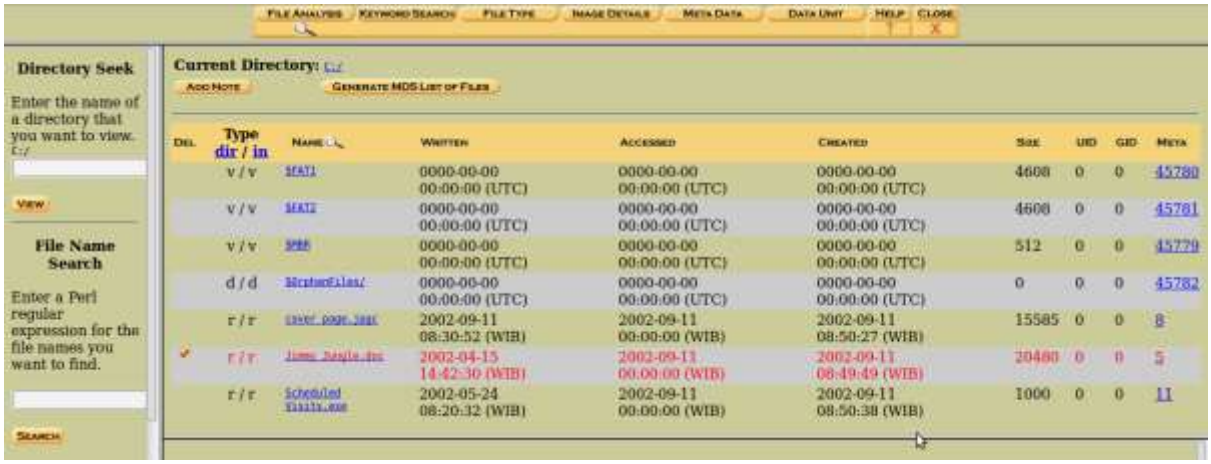
Isi Create A New Case, dengan case name: kasus, description: kasus narkoba, dan investigator names: nama user. Lalu New Case

Setelah pengisian dari beberapa case, akhirnya akan menampilkan gambar seperti berikut:

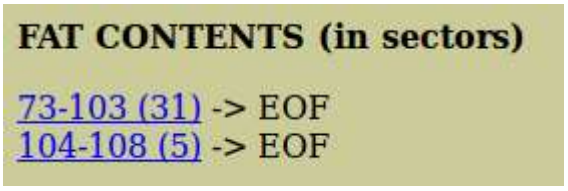


Gambar daitas menampilkan dimana letak data image.zib yang kita simpan sebelumnya

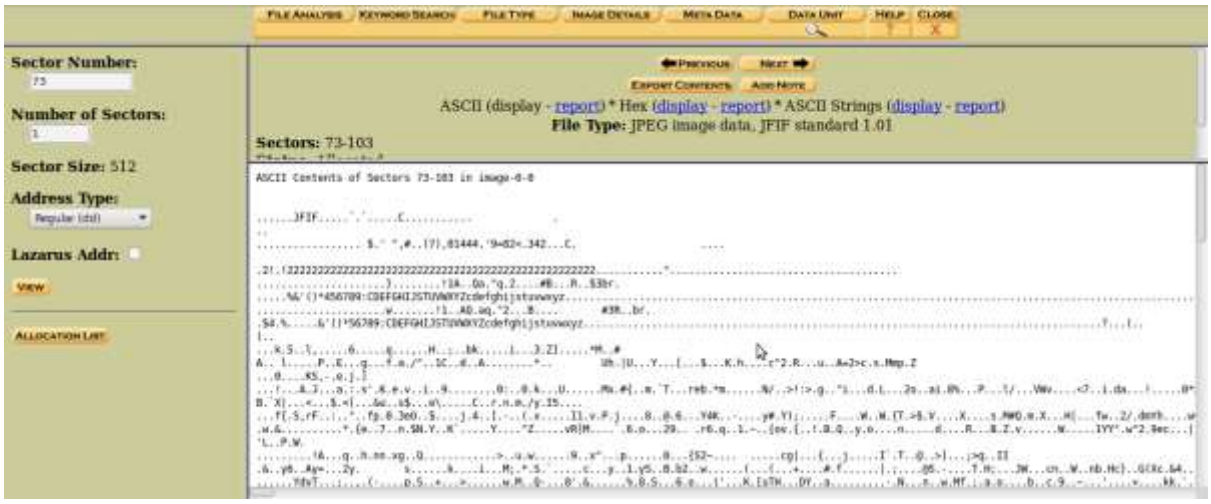
Lalu pilih r/r jimmy jungle.doc



Setelah itu akan ada dua file yang bisa kita ambil



FAT CONTENTS (in sector) untuk 73-103 (31) → EOF

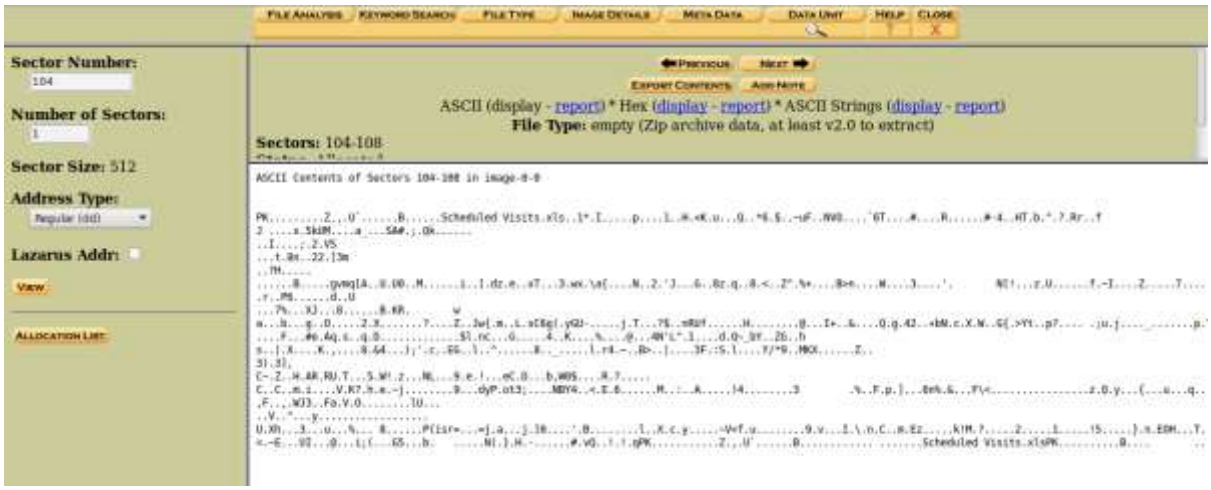


Dari gambar diatas file type dari 73-103 (31) → EOF adalah JPEG image data JFIF standard 1.01

Konfig file voli-sector73.raw

Dari perintah fungsi diatas menampilkan vol1-sector73.raw: JPEG image data, JFIF standard 1.01 dimana file tipe nya sama jika dilihat dari gambar FAT CONTENTS (in sector) untuk 73-103 (31) → EOF. Dan Rename jd jpg

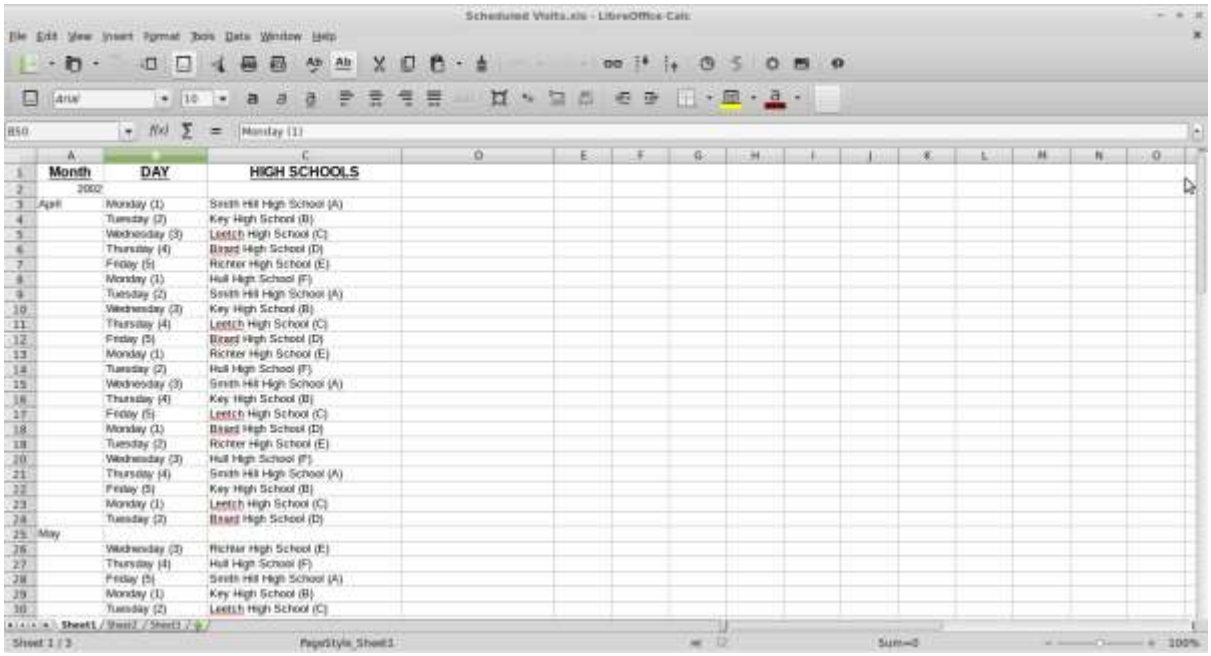
FAT CONTENTS (in sector) untuk 104-108 (5) → EOF



Dari gambar diatas file type dari 104-108 (5) → EOF adalah empty (Zip archive data, at least v2.0 to extract)

Konfig strings vol1-sector73.jpg

Menyimpan pw di dalam file gambar



Month	DAY	HIGH SCHOOLS
	2002	
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Board High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Board High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
	Monday (1)	Board High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)
	Tuesday (2)	Board High School (D)
May		
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)

Konfig foremost –v –i image –o recover

```
root@mahasiswa:/home/mahasiswa/Downloads# foremost -v -i image
-o recover
```

Perintan fungsi diatas berfungsi untuk merecover jika signature nya hilang

Kesimpulan: dengan adanya langkah langkah komputer forensic diatas dapat membantu menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki yang sah di pengadilan.