Keamanan Jaringan Komputer

Disusun Oleh

Nama : Kusuma Dwi Indriani

NIM : 09011181320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

COMPUTER FORENSIK

Secara garis besar computer forensik merupakan 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.

Tujuan dan fokus komputer forensik diantaranya untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki yang sah di pengadilan. Sedangkan fokus komputer forensik dibagii 3 yaitu Active Data, Archival Data dan Latent Data.

Beberapa tools yang diperlukan dalam komputer forensik seperti :

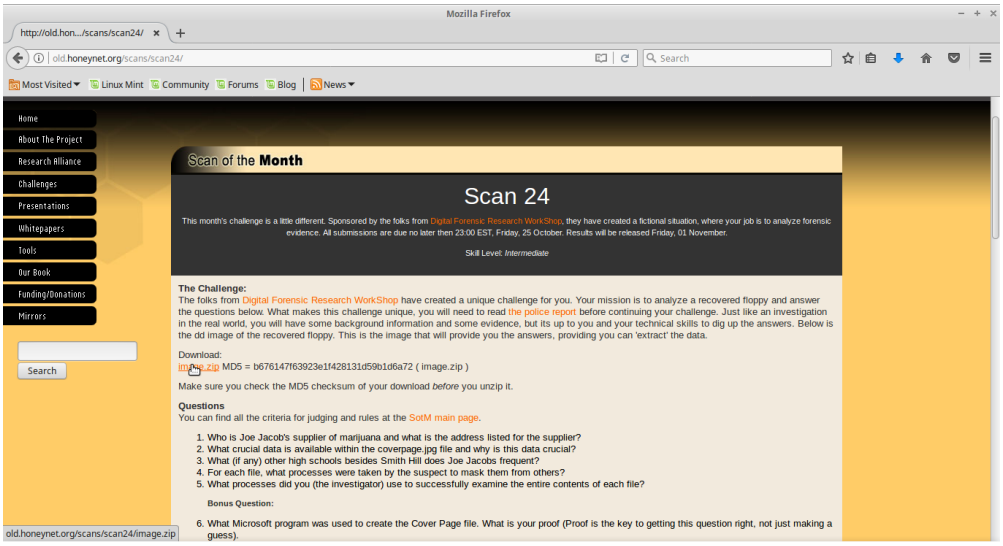
- AutoPsy
- Foremost
- Strings

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.

Berikut tahapan yang dilakukan pada saat hands di Laboratorium Jaringan Komputer:

1. Install tools Autopsy dan Foremost
2. Buka website http://old.honeynet.org/scans/scan24/ pada browser
   Download file Image.Zip
   (old.honeynet.org/scans/scan24/image.zip)
   md5 : b676147f63923e1f428131d59b1d6a72



Gambar 1. Tampilan website old.honeynet.org

3. mengecek tipe file lalu gunakan file yang tidak ada ekstensi

```
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#
```

Gambar 2. Hasil dari pengecekan file

Dari hasil proses pengecekan file diketahui file tersebut merupakan file boot sector.

4. Lakukan proses mounting pada file yang ditemukan tadi

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

Gambar 3. Perintah dalam melakukan proses mounting

5. Cek keaslian file

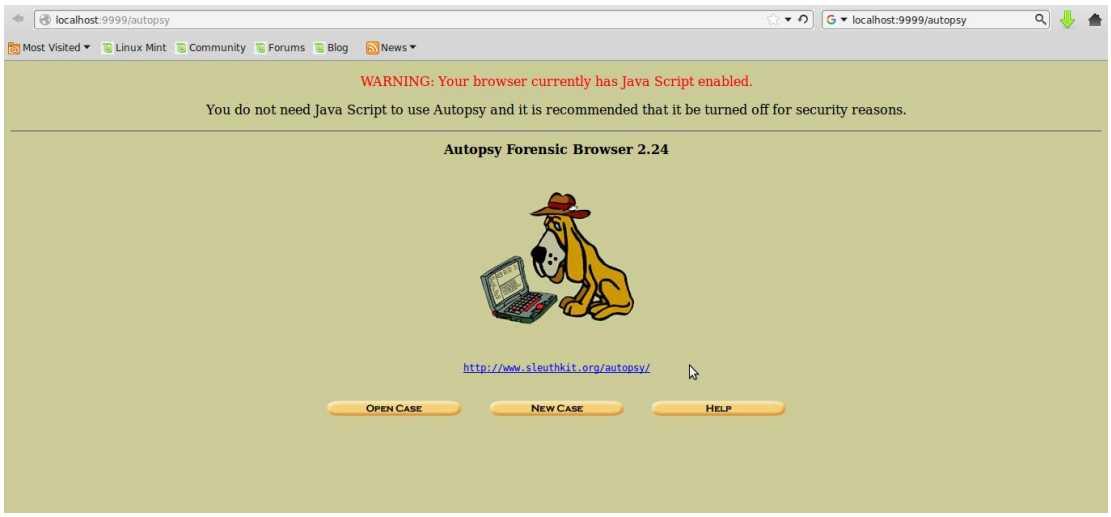
```
root@mahasiswa:/tmp/kasus# file *
cover page.jpgc           : ERROR: cannot read `cover page.jpgc
          ' (Input/output error)
SCHEDU~1.EXE:              Zip archive data, at least v2.0 to
extract
root@mahasiswa:/tmp/kasus#
```

Gambar 4. Perintah dalam cek keaslian file

6. Jalankan Autopsy dan atur hostname, siapa yang melakukan forensic komputer target

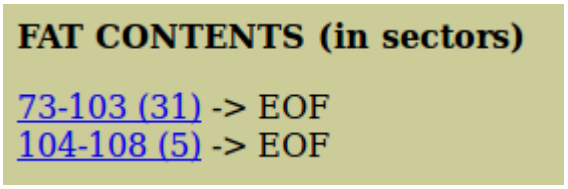
```
root@mahasiswa:/tmp/kasus# autopsy
  I
============================================================
=============

                    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
```

Gambar 5. Tools autopsy saat dijalankan



Gambar 6. akses autopsy dengan browser http://localhost:9999/autopsy

7. Pembuatan New case; case name dan decription sesuaikan dengan kasus yang akan diakses hal ini bertujuan agar dapat membedakan jika ingin ada kasus yang lainnya. lalu klik lagi New Case, setelah itu langsung saja klik Add Host pada Creating Case.
8. Buat host baru, Pada step ADD NEW HOST isi *Host Name* sesuai keinginan contoh nya Forensic1
9. Tambahkan file gambar dengan cara klik add image file
10. Pada tahapan setup autopsy ini isi dari setup tergantung yang dikehendaki. Saat proses setup telah selesai maka gunakan file sistem yang dibuat



Gambar 7. Ada 2 file yang dapa digunakan

11. Rename menjadi .JPG

```
root@mahasiswa:/home/mahasiswa# cd Downloads/
root@mahasiswa:/home/mahasiswa/Downloads# ls
image  image.zip  Link to image  vol1-Sector73.raw
root@mahasiswa:/home/mahasiswa/Downloads# file vol1-Sector73.ra
w
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
root@mahasiswa:/home/mahasiswa/Downloads#
```

Gambar 8. Perintah untuk merename

12. Gunakan string agar dapat menyimpan password di dalam file gambar

```
root@mahasiswa:/home/mahasiswa/Downloads# strings vol1-Sector73
.jpg
```

Gambar 9. Penggunaan string

	Month	DAY	HIGH SCHOOLS
2	2002		
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith Hill High School (A)
10		Wednesday (3)	Key High School (B)
11		Thursday (4)	Leetch High School (C)
12		Friday (5)	Birard High School (D)
13		Monday (1)	Richter High School (E)
14		Tuesday (2)	Hull High School (F)
15		Wednesday (3)	Smith Hill High School (A)
16		Thursday (4)	Key High School (B)
17		Friday (5)	Leetch High School (C)