

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

COMPUTER FORENSICS

Secara Garis Besar, di rangkum dari berbagai sumber :

"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."

Pada praktikum kali ini akan dilakukan sebuah kegiatan Computer Forensics . dapat dilihat diatas definisi dari Computer Forensics.

Tujuan dari Computer Forensics adalah sebagai berikut

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat bukti yang sah di pengadilan.
2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Fokus data yang di kumpulkan di bagi menjadi 3 kategori :

1. Active Data

yaitu informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi.

2. Archival Data

yaitu informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpanan seperti hardisk eksternal, CD ROM, backup tape, DVD, dan lain-lain.

Nama : Suci Anggraeni
Nim : 0901181320030
Keamanan Jaringan Komputer

3. Latent Data

yaitu informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya.

Tools yang digunakan adalah :

1. Autopsy
2. Foremost
3. 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.

Langkah –langkah melakukan Computer Forensics.

Install tools Autopsy dan Foremost

Buka website <http://old.honeynet.org/scans/scan24/> pada browser

Download file Image.Zip

(old.honeynet.org/scans/scan24/image.zip)

md5 : b676147f63923e1f428131d59b1d6a72

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



Fungsi md5sum : sebuah file pasti ada md5sum yang berfungsi untuk mengecek keaslian dari file atau integritas file.

```
Terminal
File Edit View Terminal Tabs Help
suci-Aspire-47362 suci # cd Documents
suci-Aspire-47362 Documents # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
suci-Aspire-47362 Documents #
```

```
Terminal
File Edit View Terminal Tabs Help
suci-Aspire-47362 suci # cd Documents
suci-Aspire-47362 Documents # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
suci-Aspire-47362 Documents # file image.zip
image.zip: Zip archive data, at least v2.0 to extract
suci-Aspire-47362 Documents # unzip image.zip
Archive: image.zip
  inflating: image
suci-Aspire-47362 Documents # file image
image: DOS floppy 1440k, x86 hard disk boot sector
suci-Aspire-47362 Documents #
```

Fungsi perintah di atas : untuk mengecek tipe file. Jika kita menemukan file yang tidak ada ekstensi, maka kita bisa menggunakannya.

Setelah tahu bahwa file tersebut file boot sector, maka akan melakukan proses mounting

```
suci-Aspire-47362 Documents # mkdir /tmp/kasus.narkoba
suci-Aspire-47362 Documents # mount image /tmp/kasus.narkoba/
```

Nama : Suci Anggraeni
Nim : 0901181320030
Keamanan Jaringan Komputer

```
Terminal
File Edit View Terminal Tabs Help
suci@suci-Aspire-4736Z ~ $ cd /tmp/kasus-narkoba
suci@suci-Aspire-4736Z /tmp/kasus-narkoba $ su
Password:
suci-Aspire-4736Z kasus-narkoba # ls
cover page.jpgc          SCHEDU-1.EXE
```

Perintah untuk Mengecek keaslian file

```
suci-Aspire-4736Z kasus-narkoba # file *
cover page.jpgc          : ERROR: cannot read `cover page.jpgc' (Inp
ut/output error)
SCHEDU-1.EXE:            Zip archive data, at least v2.0 to extract
suci-Aspire-4736Z kasus-narkoba #
```

Kemudian jalankan Autopsy dan Mengatur hostname, siapa yang melakukan forensik pada komputer target

```
Terminal
suci-Aspire-4736Z kasus-narkoba # autopsy

=====

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

=====

Evidence Locker: /var/lib/autopsy
Start Time: Fri Mar 24 11:13:04 2017
Remote Host: localhost
Local Port: 9999

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

http://localhost:9999/autopsy

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

akses autopsy dengan browser <http://localhost:9999/autopsy>

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



Pembuatan New Case

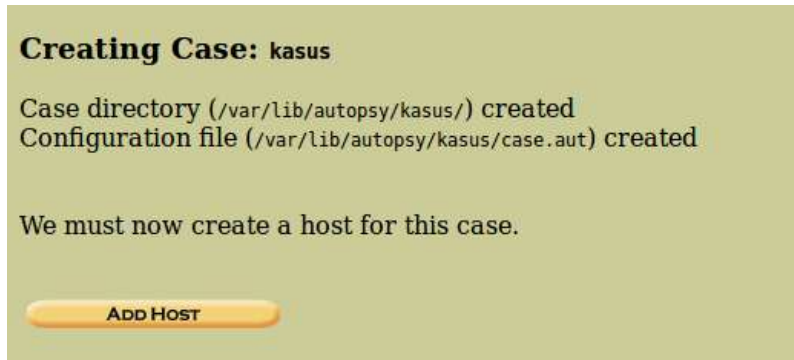
Tujuan pembuatan *New Case* adalah agar kita dapat mudah mengakses kasus kasus sehingga tidak tercampur dengan kasus forensic lain nya .Klik *New Case*

isikan Case Name hingga Investigator Name nya sesuai keinginan. lalu klik lagi New Case, setelah itu langsung saja klik Add Host pada Creating Case.

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

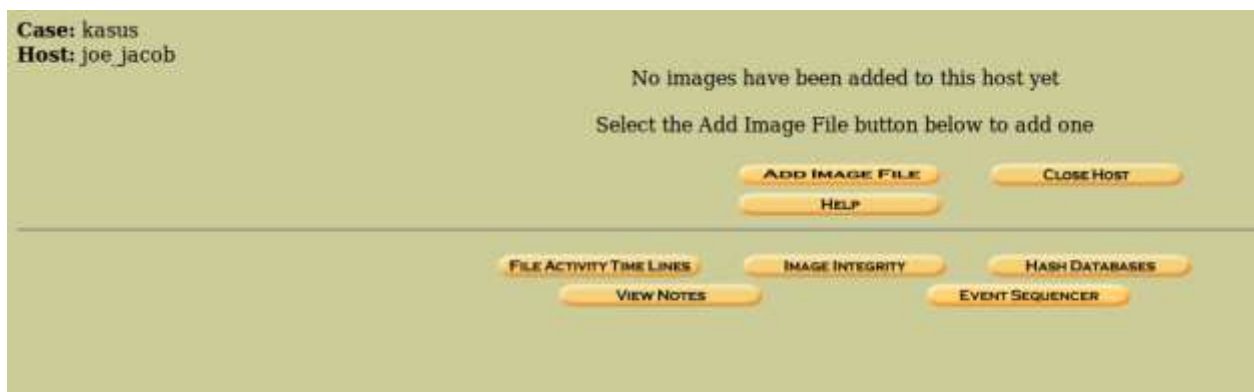
Membuat Host Baru

Pada step ADD NEW HOST isi *Host Name* terserah contoh nya Forensic1,



Menambahkan Image File

Klik Add Image file



Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

Pada form *Location* masukan lokasi dari image file yang ingin dilakukan forensi.

Case: kasus
Host: joe_jacob

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type /home/suci/Download/image
Please select if this image file is for a disk or a single partition.
 Disk Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
 Symlink Copy Move

NEXT

- `/home/suci/Downloads/image` : merupakan lokasi file image
- Pada Type masukan sesuai dengan type daei image file nya, apabila disk pilih disk apabila partisi pilih partition, pada kasus ini memilih disk.
- Pada bagian import method silahkan pilih sesuai keinginan . pada gambar diatas terlihat bahwa yang dipilih adalah symlink karena sudah punya salinan lain nya, jadi apabila file system tersebut rusak tidak menjadi masalah.

Setelah semuanya selesai langsung sakja *klik next*.

Maka akan muncul seperti gambar dibawah ini.

Nama : Suci Anggraeni
Nim : 0901181320030
Keamanan Jaringan Komputer

Image File Details

Local Name: images/image

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

Ignore the hash value for this image.

Calculate the hash value for this image.

Add the following MD5 hash value for this image:

Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat12)

Mount Point: C: File System Type: fat12

ADD **CANCEL** **HELP**

Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image Volume Image

Volume System Type (disk image only): dos

OK

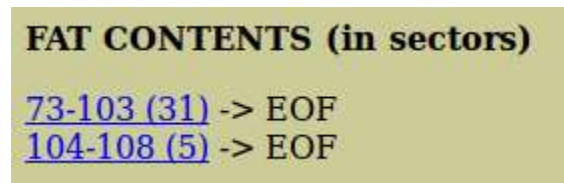
Lanjutkan saja dengan klik ADD->> OK.

Nama : Suci Anggraeni
Nim : 0901181320030
Keamanan Jaringan Komputer



Sampai tahap ini setup pada kasus autopsy sudah selesai, tinggal melakukan analisis terhadap file system dari kasus yang dibuat.

File yang dipakai



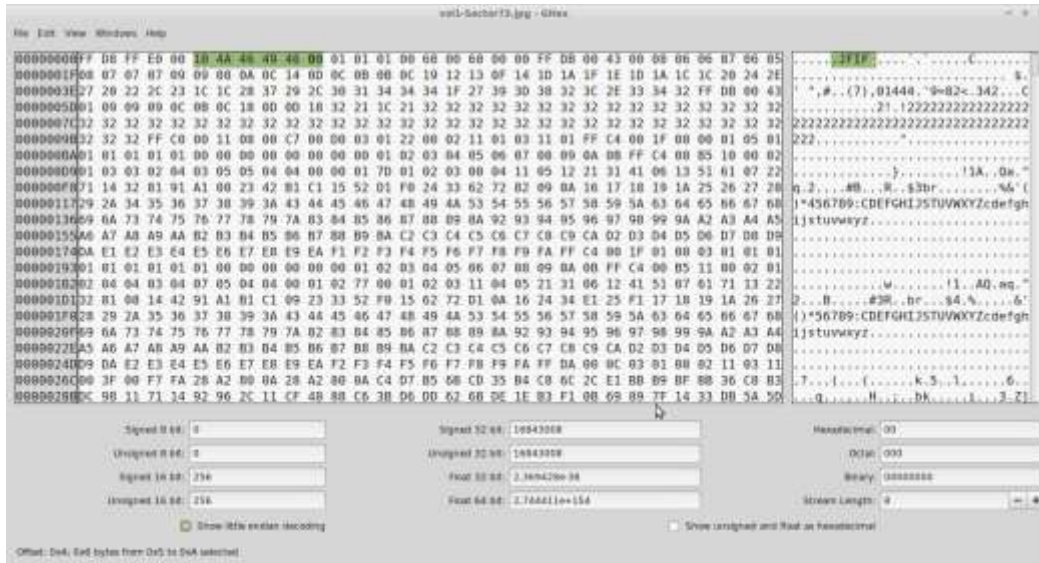
```
suci-Aspire-4736Z Documents # file vol1-Sector73.raw  
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
```

Rename file tersebut



Tampilan image vol1-sector73.jpg

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



Kemudian untuk Merecover jika signature nya hilang gunakan foremost

```
suci-Aspire-4736Z Documents # foremost -v -i image -o recover
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Mar 24 12:01:57 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/srisuryani/Unduhan/recover
Configuration file: /etc/foremost.conf
Processing: image
-----
File: image
Start: Fri Mar 24 12:01:57 2017
Length: 1 MB (1474560 bytes)

Num   Name (bs=512)      Size   File Offset   Comment
0:    00000073.jpg       8 KB   37376
1:    00000033.doc      21 KB   16896
Foundat=Scheduled Visits.xls001*01
0p00[?]00<K0uc0066*0050[?]uF00NV0000*6T[?]0.#00[?]
00030e-4[?]T0b0*070R00f
j 00 0x05KUP00000 00SA#0;00k0 00[?]
010[?]00;020VS
2:    00000104.zip       2 KB   53248
*|
Finish: Fri Mar 24 12:01:57 2017

3 FILES EXTRACTED

jpg:= 1
ole:= 1
zip:= 1
-----
Foremost finished at Fri Mar 24 12:01:57 2017
```

Nama : Suci Anggraeni
Nim : 0901181320030
Keamanan Jaringan Komputer

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)	Brand 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)	Brand 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)	Brand 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)	Brand 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)

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe