KEAMANAN JARINGAN KOMPUTER

“COMPUTER FORENSICS”

OLEH :

SAROS SAKIYANA

09011181320038

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Definisi Computer Forensics

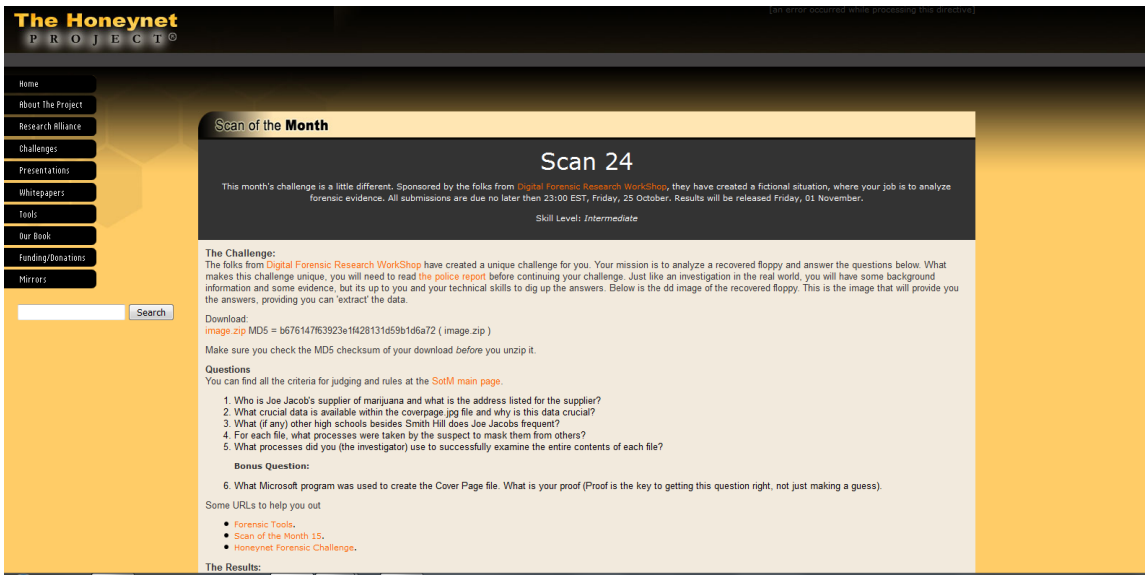
Komputer Forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital.

Tujuan

untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi

Langkah kerja :

1. Install tools, selain strings
2. Buka wesite berikut. File tersebut merupakan

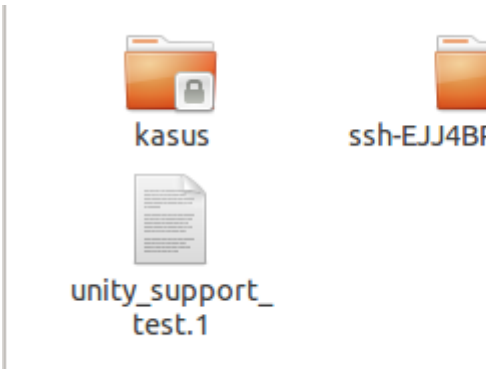


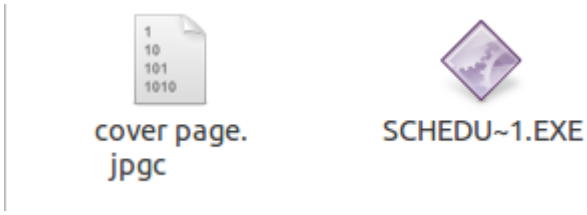

```
root@mahasiswa:/home/mahasiswa/Downloads# ls
image  image.zip
root@mahasiswa:/home/mahasiswa/Downloads# file image
image: DOS floppy 1440k, x86 hard disk boot sector
root@mahasiswa:/home/mahasiswa/Downloads#
```

Pada gambar diatas adalah untuk mengecek tipe file. Jika kita menemukan file yang tidak ada ekstensi, maka kita bisa menggunakannya

Terus kita masuk ke proses mount image /tmp/ksus

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



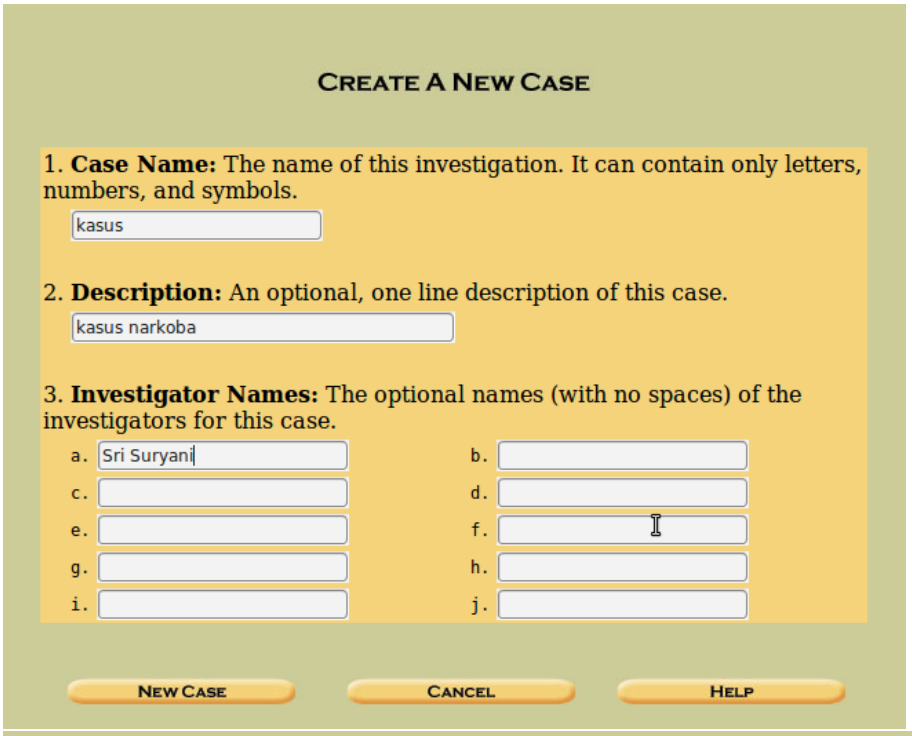


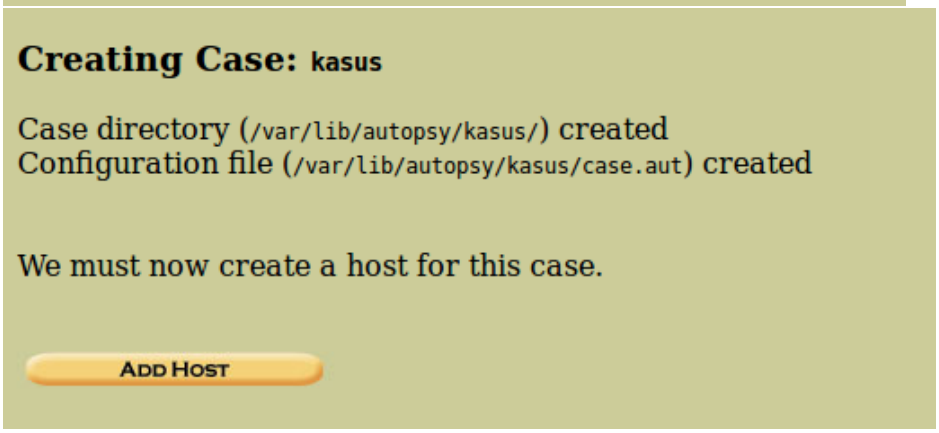

```
root@mahasiswa:/home/mahasiswa/Downloads# cd /tmp/kasus
root@mahasiswa:/tmp/kasus# ls
cover page.jpgc              SCHEDU~1.EXE
root@mahasiswa:/tmp/kasus#
```

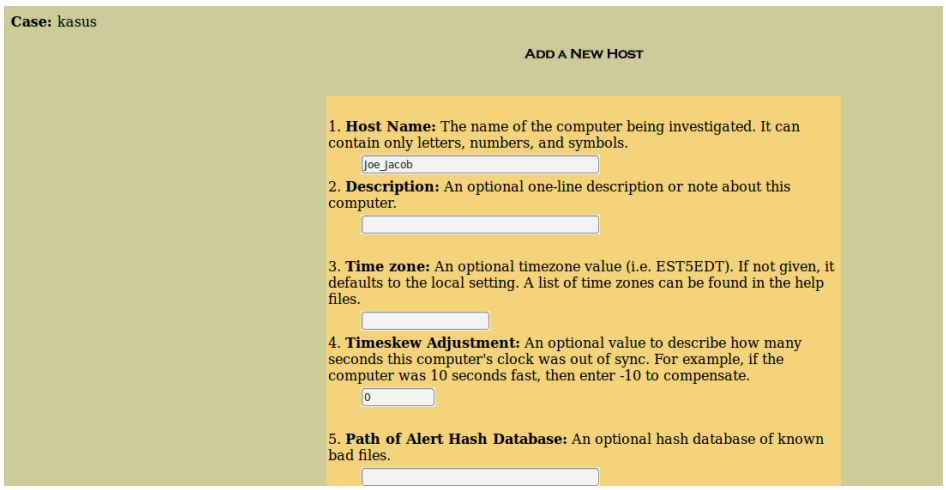
Mengecek keaslian file

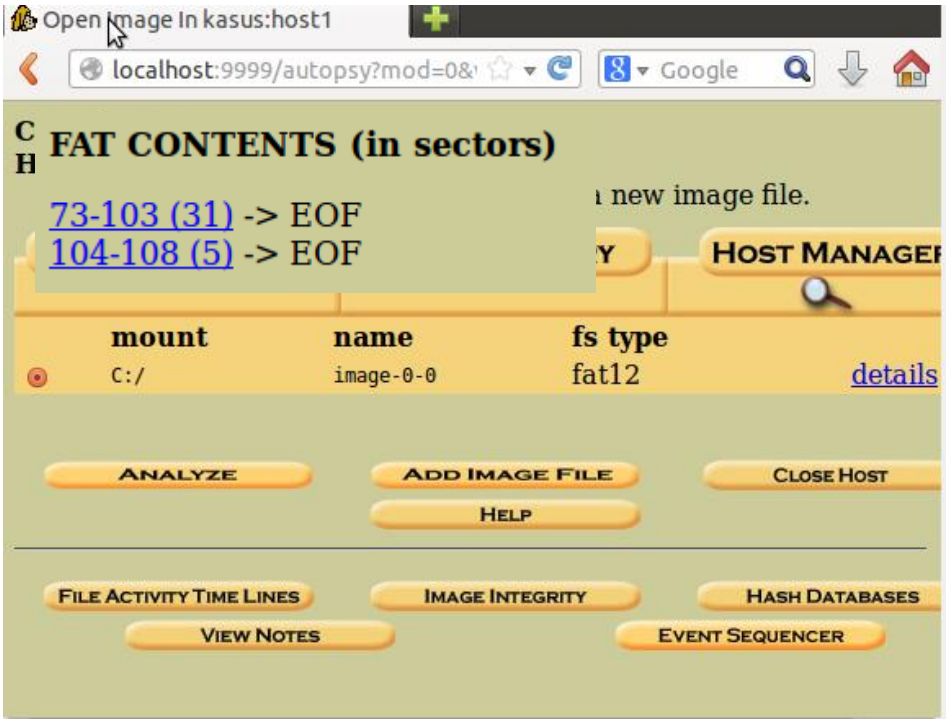
```
root@mahasiswa:/tmp/kasus# file *
cover page.jpgc           : ERROR: cannot read `cover page.jpgc
          ' (Input/output error)
SCHEDU~1.EXE:              Zip archive data, at least v2.0 to
extract
root@mahasiswa:/tmp/kasus#
```

```
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
```


CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
kasus
2. Description: An optional, one line description of this case.
kasus narkoba
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. Sri Suryani
b.
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP

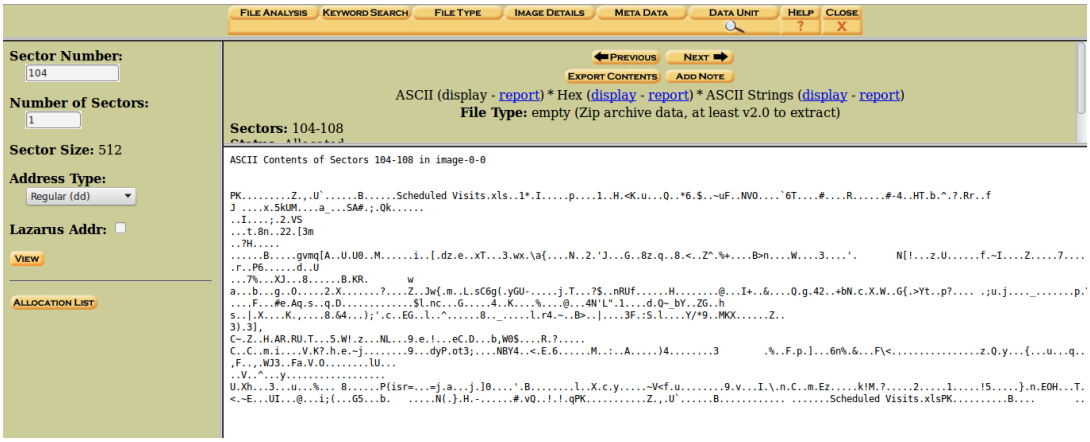

Creating Case: kasus
Case directory (/var/lib/autopsy/kasus/) created
Configuration file (/var/lib/autopsy/kasus/case.aut) created
We must now create a host for this case.
ADD HOST


Case: kasus
ADD A NEW HOST
1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
Joe_Jacob
2. Description: An optional one-line description or note about this computer.
3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0
5. Path of Alert Hash Database: An optional hash database of known bad files.



jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿØÿÛ	FF D8 FF DB
			ÿØÿà ..J F IF..	FF D8 FF E0 nn nn 4A 46 49 46 00 01
			ÿØÿá ..E x if..	FF D8 FF E1 nn nn 45 78 69 66 00 00

```
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#
```



	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)

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

Merecover jika signature nya hilang

```
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $ 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.xls��1*�I
                                  ]
R
J
2:      00000104.zip           2 KB           53248
*|
Finish: Fri Mar 24 12:01:57 2017

3 FILES EXTRACTED
```

Menggunakan GHex

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

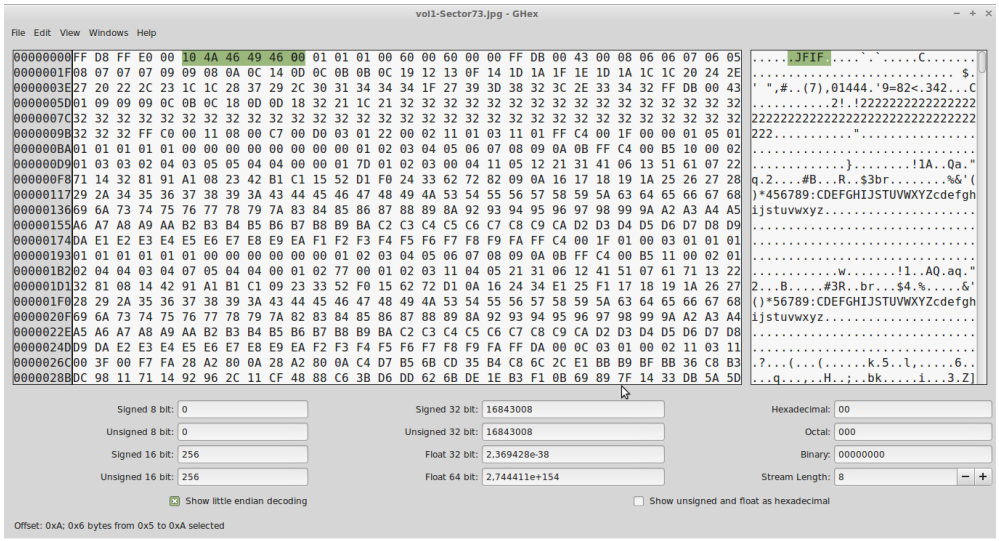
Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

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



dari gambar diatas terlihat ada beberapa string yang dienkripsi dan yang tidak dienkripsi. Debugger bisa digunakan untuk menjalankan virus dalam lingkungan yang dapat dimonitor.

```
srisuryani-Aspire-4739 Unduhan # md5sum image.zip
b676147f63923e1f428131d59b1d6a72  image.zip
srisuryani-Aspire-4739 Unduhan #
```