

KEAMANAN JARINGAN KOMPUTER
“COMPUTER FORENSICS”



OLEH :

SAROS SAKIYANA

09011181320038

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017

Definisi Computer Forensics

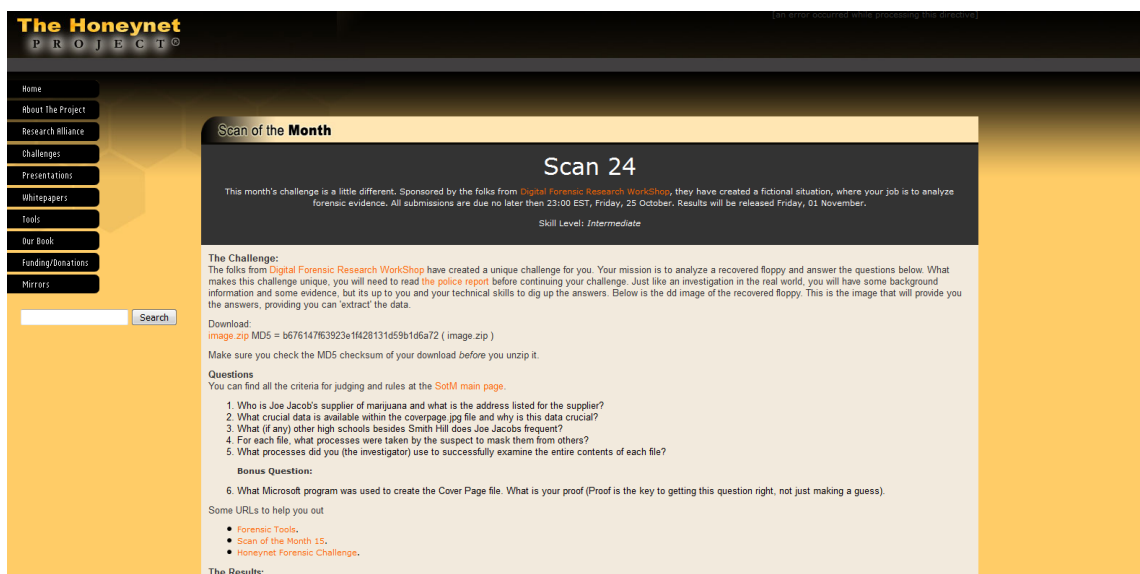
Komputer Forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital.

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



The HoneyNet PROJECT

Home
About The Project
Research Alliance
Challenges
Presentations
Whitepapers
Tools
Our Book
Funding/Donations
Mirrors

Search

Scan of the Month

Scan 24

This month's challenge is a little different. Sponsored by the folks from [Digital Forensic Research Workshop](#), they have created a fictional situation, where your job is to analyze forensic evidence. All submissions are due no later than 23:00 EST, Friday, 25 October. Results will be released Friday, 01 November.

Skill Level: *Intermediate*

The Challenge:
The folks from [Digital Forensic Research Workshop](#) have created a unique challenge for you. Your mission is to analyze a recovered floppy and answer the questions below. What makes this challenge unique, you will need to read [the police report](#) before continuing your challenge. Just like an investigation in the real world, you will have some background information and some evidence, but it's up to you and your technical skills to dig up the answers. Below is the dd image of the recovered floppy. This is the image that will provide you the answers, providing you can 'extract' the data.

Download:
[image.zip](#) MD5 = b676147f63923e1f428131d59b1d6a72 ([image.zip](#))
Make sure you check the MD5 checksum of your download before you unzip it.

Questions
You can find all the criteria for judging and rules at the [SoTM main page](#).

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the [coverpage.jpg](#) file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Bonus Question:

6. What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).

Some URLs to help you out

- [Forensic Tools](#).
- [Scan of the Month 15](#).
- [honeynet Forensic Challenge](#).

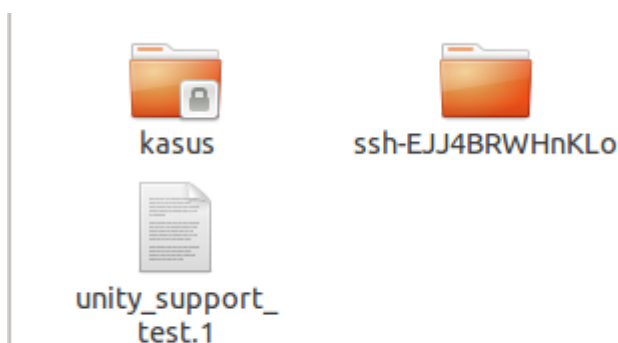
The Results:

```
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/ksus
S
```





cover page.
jpgc



SCHEDU~1.EXE

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

```
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 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.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	<input type="text" value="Sri Suryani"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

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

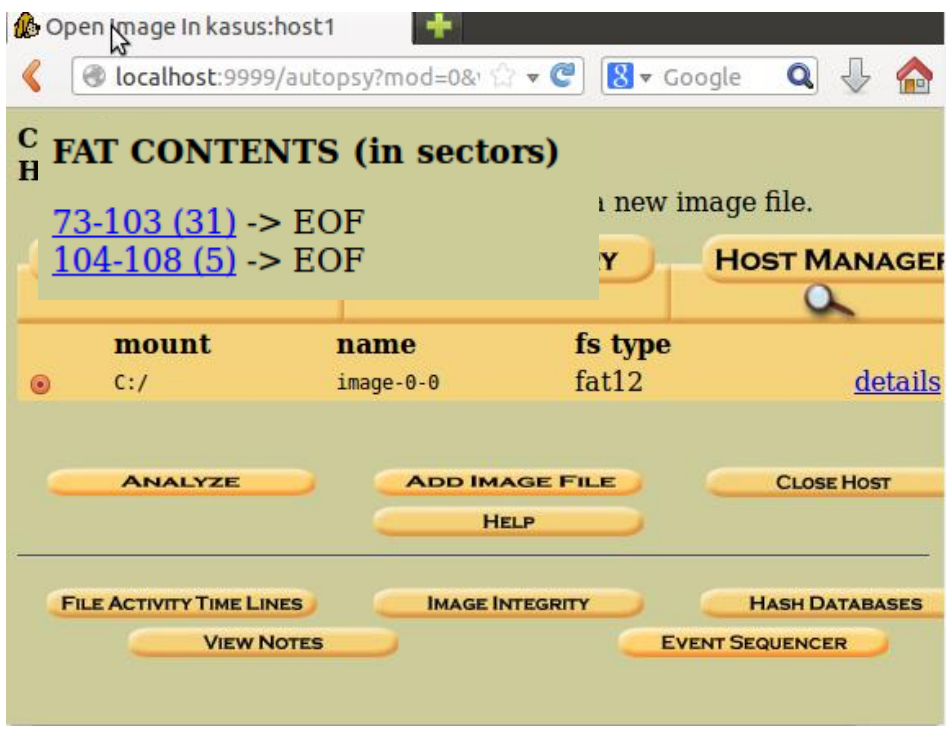
1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

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.

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	ÿøÿÜ	FF D8 FF DB
			ÿøÿá ..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#
  
```



FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

← PREVIOUS NEXT →
EXPORT CONTENTS ADD NOTE

Sector Number: 104
Number of Sectors: 1
Sector Size: 512
Address Type: Regular (dd)
Lazarus Addr:
View

ALLOCATION LIST

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: empty (Zip archive data, at least v2.0 to extract)

Sectors: 104-108
ASCII Contents of Sectors 104-108 in image 0-0

```
PK.....Z...U'.....B.....Scheduled Visits.xls..1*.I.....p.....1...H.<K.u...0.*6.S...uF...NV0...6T...#...R.....#-4...HT.b.^?7.Rr..f
J...X.SKUM...a...SA#;:0k.....
..I...;:2.VS
...t.Bn:22.[3m
..7H.....
.....B.....gvmq[A..U.U0..M.....i...[.dz.e..XT...3.wx\{...N..2.'J...G..8z.q..8.<.Z^%+...B>n...W...3.....' N[...z.U.....f.-I...Z...7....
.r.P6.....d..U
...7n...XJ...8.....B.KR.
a...b...g..0...2.X.....7...Z..Jw{m..L.sc6g(yGU+...j.T...7S...nRUF.....H.....@...I+..&...0.g.42...+BN.c.X.W..G(->Yt..p?...;u.j.....p?
...F...#e.Aq.s.q.D.....S.l.nc...G....4..K...%...@...4N"l...1...d..0..._b...ZG..h
s...[X...K...8.64...];'c..EG..l..^...8.....l.r4-<.B>...]...3F::S...L...Y/9..MKX...Z...
3)3)
C=Z..H.AR.RU.T...5.WI.z...NL...9.e.t...eC.D...b.WS...R.7.....
C..C..m.i...V.K7.h.e.-]...9...dyP.ot3;...NBV4.<.E.6.....M.....A.....)4.....3      %..F.p.]...6n%.6...F<.....z.0.y...{...u...q...
..W...Y...
U.Xh..3...u...%...8.....P(isr=...e].a...j].0...'.B.....l.X.C.y...-Vef.u.....9.v...I..n.C..m.Ez...KIM.7...2...1...5...}..n.EOH...T.
<-E...UI...@...i...[65..z..b. ....N(.).H.....#V0..f.l.qPK.....Z..U'.....B.....Scheduled Visits.xlsPK.....B.....
```

1	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.xls001*0I
0p00000100<K0uq0Q00*60$0[A]uF00NV0000`6T[00].#00[00]
0R0[00]#-4[00]T0b0^0?0Rr00f
J 00[00]x05kUM0000a_00SA#0;0Qk0[00]
0I0[00]:020VS
2:       00000104.zip           2 KB     53248
*|
Finish: Fri Mar 24 12:01:57 2017

3 FILES EXTRACTED
```

Menggunakan GHex

The screenshot shows the GHex application interface. At the top, there is a navigation bar with buttons for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. Below this, there are buttons for REPORT, VIEW CONTENTS, EXPORT CONTENTS, and ADD NOTE. The main window is divided into two panes. The left pane shows 'Dir Entry Number: 11' with a 'VIEW' button and an 'ALLOCATION LIST' button. The right pane displays file details for entry 11:

- Search for File Name**
- File Type:** empty (Zip archive data, at least v2.0 to extract)
- MD5 of content:** 082a5cc64deea22a3a589ffbb5a6fa66 -
- SHA-1 of content:** c8e7f25380d63c9034d9f27faab29de1f09240b5 -
- Details:**
 - Directory Entry: 11
 - Allocated
 - File Attributes: File, Archive
 - Size: 1000
 - Name: SCHEDU~1.EXE
 - Directory Entry Times:
 - Written: Fri May 24 08:20:32 2002
 - Accessed: Wed Sep 11 00:00:00 2002
 - Created: Wed Sep 11 08:50:38 2002
 - Sectors: [104](#) [105](#)

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

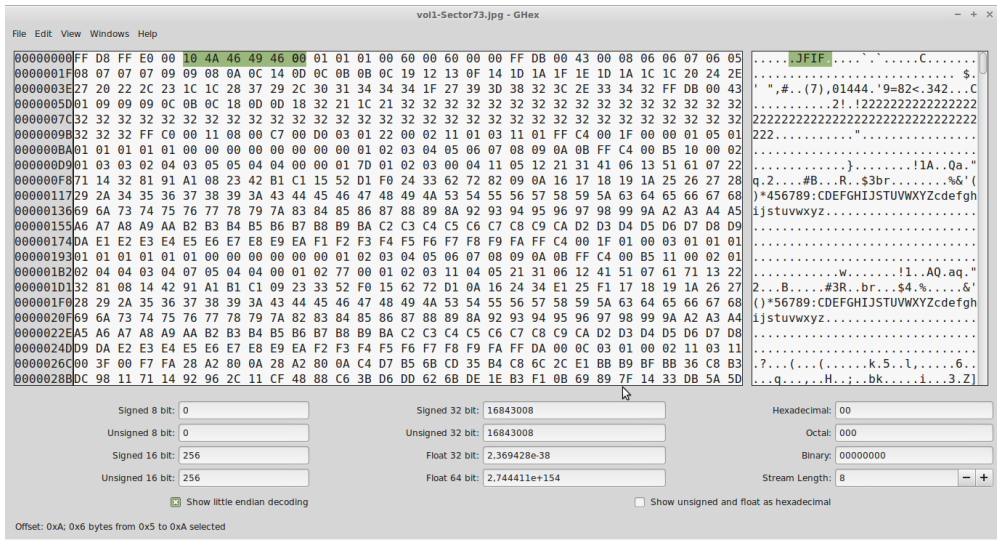
Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

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 #

```