TUGAS KEAMANAN JARINGAN

“ Komputer Forensik “

OLEH :

NAMA : MARDIAH

NIM : 09011281320005

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

INDERALAYA

2017

Komputer Forensik adalah cabang dari ilmu forensik berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital.

Maraknya tindakan kejahatan dalam dunia komputer, membutuhkan proses pembuktian yang tidaklah mudah, oleh karena itu, kajian bidang komputer forensik ini masih tergolong baru dan masih terus dikembangkan, sehingga nantinya, semua kasus-kasus kejahatan komputer mampu dibuktikan secara sah di pengadilan.

Saat ini, kajian komputer forensik dibagi menjadi beberapa bidang seperti Internet Forensik yang khusus membahas forensik dalam ranah internet dan aplikasinya, lalu ada Network Forensik, Disk Forensik, Database Forensik, Firewall Forensik, Mobile Device Forensik dan System Forensik yang kesemuanya secara umum berada dalam kontek komputer forensik.

Tujuan dari Komputer Forensik adalah untuk mengamankan dan menganalisa bukti digital. Selain itu juga bertujuan untuk mendapatkan fakta-fakta objektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.

KASUS :

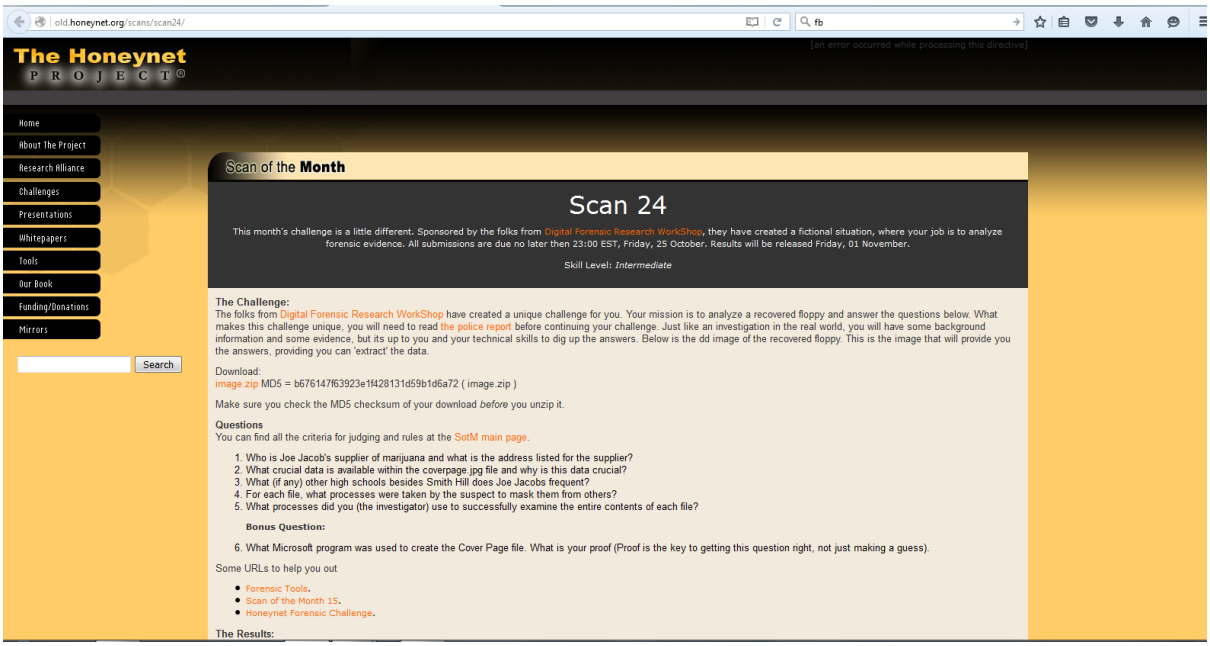
Ada seorang pengedar narkoba yang tertangkap polisi, polisi mendapatkan barang bukti berupa harddrive yang sudah korup dari tersangka. Bagaimana cara kita me- recover harddrive tersebut sehingga kita mendapatkan informasi di dalam nya.

Pada percobaan kali ini, menggunakan beberapa tools berikut :

1. Autopsy
   Merupakan sebuah antarmuka grafis yang menyediakan fungsi manajemen kasus, integritas gambar, pencarian kata kunci, dan operasi lainnya.
2. Foremost
   Foremost merupakan aplikasi berbasis console yang melakukan recovery file yang terhapus berdasarkan header file, footer file, data struktur data. Foremost dapat bekerja pada image file (.iiso, dll), seperti yang dihasilkan oleh dd, Safeback, Encase, dll, atau langsung pada drive.
3. Strings
   Adalah sebuah aplikasi yang digunakan untuk mengetahui password dalam suatu file. Pada percobaan ini yaitu file image

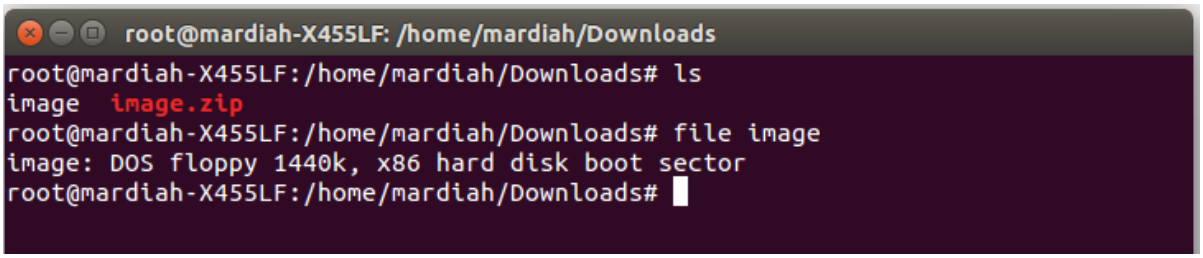
Langkah kerja :

1. Install tools, selain strings karena tools string sudah tersedia pada OS ubuntu
2. Buka wesite berikut http://old.honeynet.org/scans/scan24/. Kemudian download " file image.zip ". File tersebut merupakan bahan yang akan kita analisa menggunakan 3 tools diatas.
   Image.Zip (old.honeynet.org/scans/scan24/image.zip) md5 : b676147f63923e1f428131d59b1d6a72



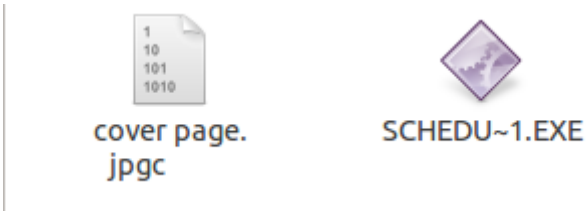
⇨ Fungsi md5sum : sebuah file pasti ada md5sum yang berfungsi untuk mengecek keaslian dari file atau integritas file

3. Fungsi perintah di bawah ini yaitu untuk mengecek tipe file. Jika kita menemukan file yang tidak ada ekstensi, maka kita bisa menggunakan perintah sintaks tersebut.



4. Setelah kita tahu bahwa file tersebut file boot sector, maka akan melakukan proses mounting. Lalu Mengecek keaslian file

```
root@mardiah-X455LF:/home/mardiah/Downloads# mkdir /tmp/Narkoba
root@mardiah-X455LF:/home/mardiah/Downloads# mount image /tmp/Narkoba
root@mardiah-X455LF:/home/mardiah/Downloads# cd /tmp/Narkoba
root@mardiah-X455LF:/tmp/Narkoba# ls
cover page.jpgc             SCHEDU~1.EXE
root@mardiah-X455LF:/tmp/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
root@mardiah-X455LF:/tmp/Narkoba#
```

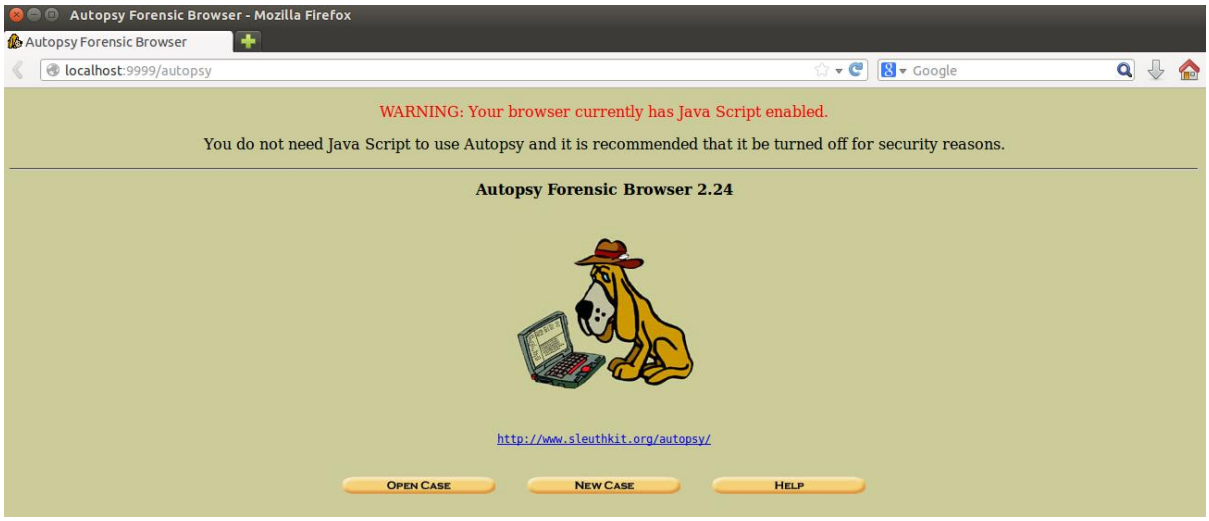


5. Kemudian menggunakan tools autopsy. Karena tools ini bekerja menggunakan search engine, jadi tools ini memberikan informasi yaitu :

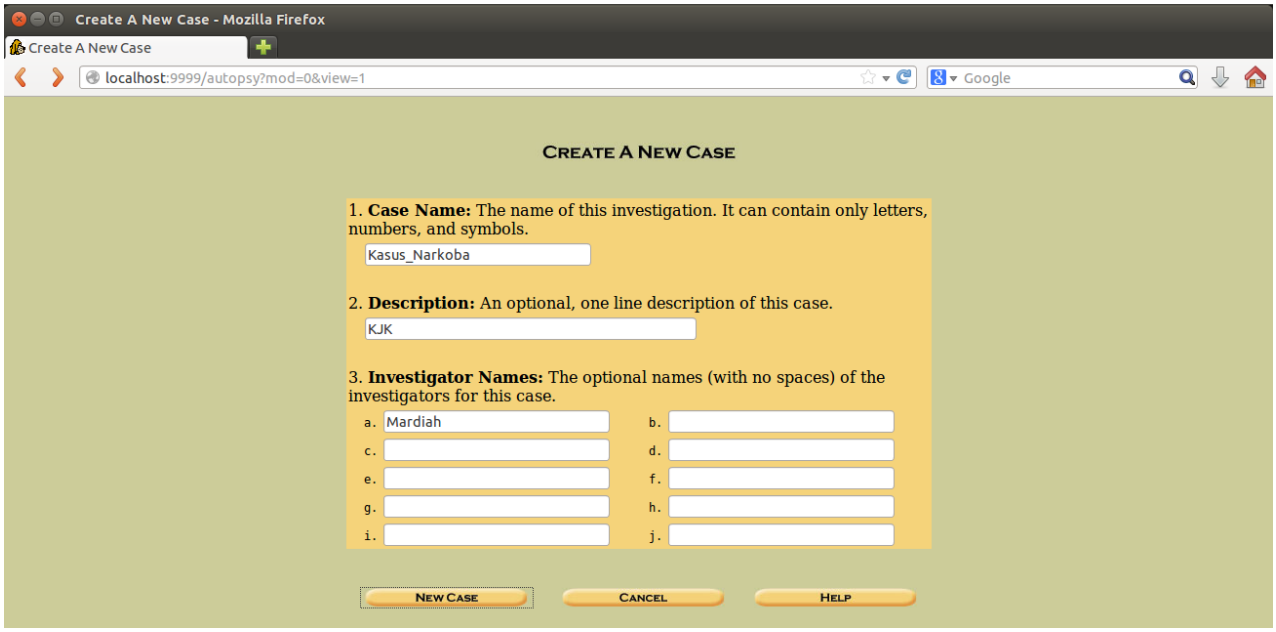
- Remote Host : localhost
- Local Port : 9999

```
root@mardiah-X455LF: /tmp/Narkoba
root@mardiah-X455LF:/tmp/Narkoba# autopsy

================================================================================

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

================================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Wed Mar 29 03:35:50 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
```

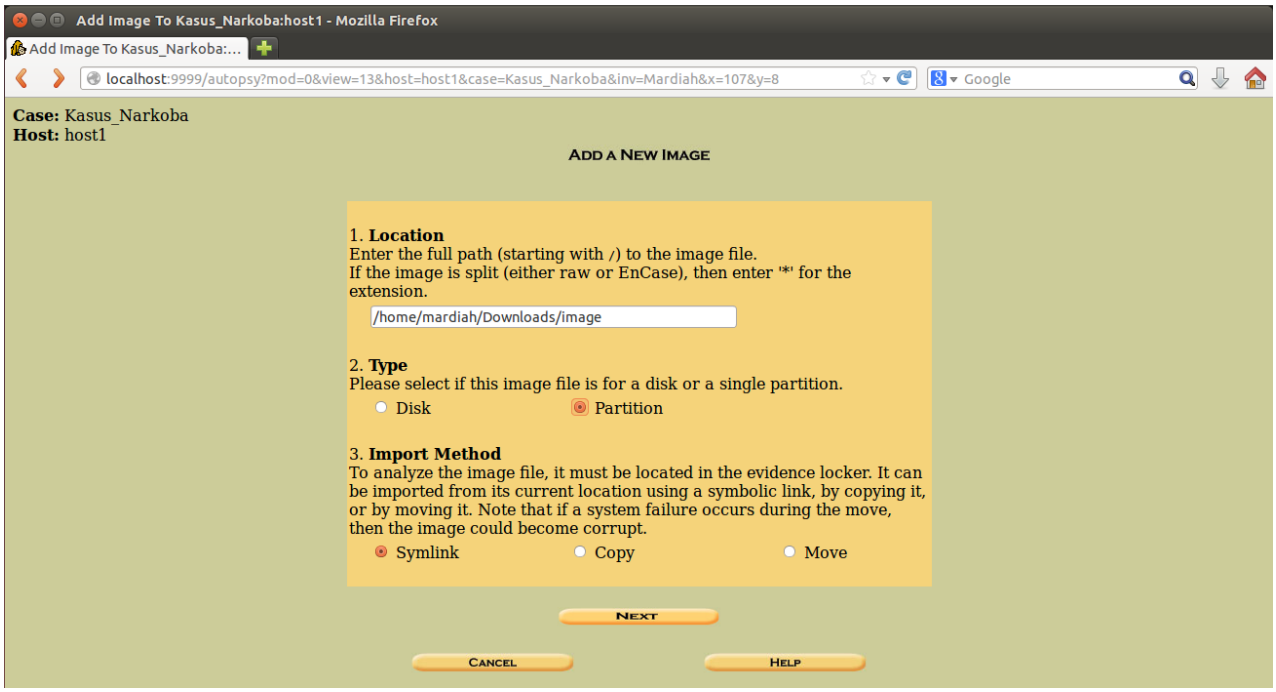
6. Buka search engine dengan alamat dari informasi diatas " localhost : 9999 / autopsy "

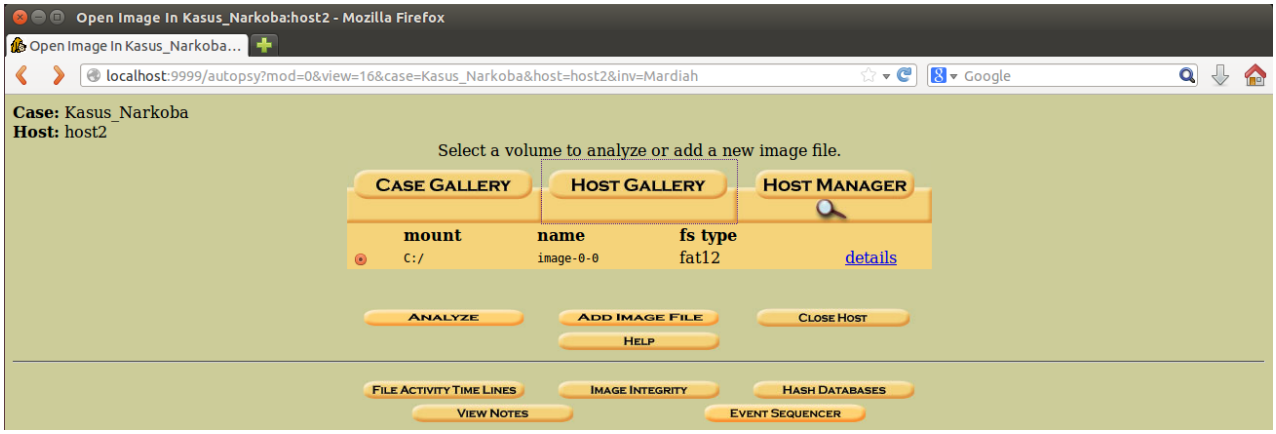


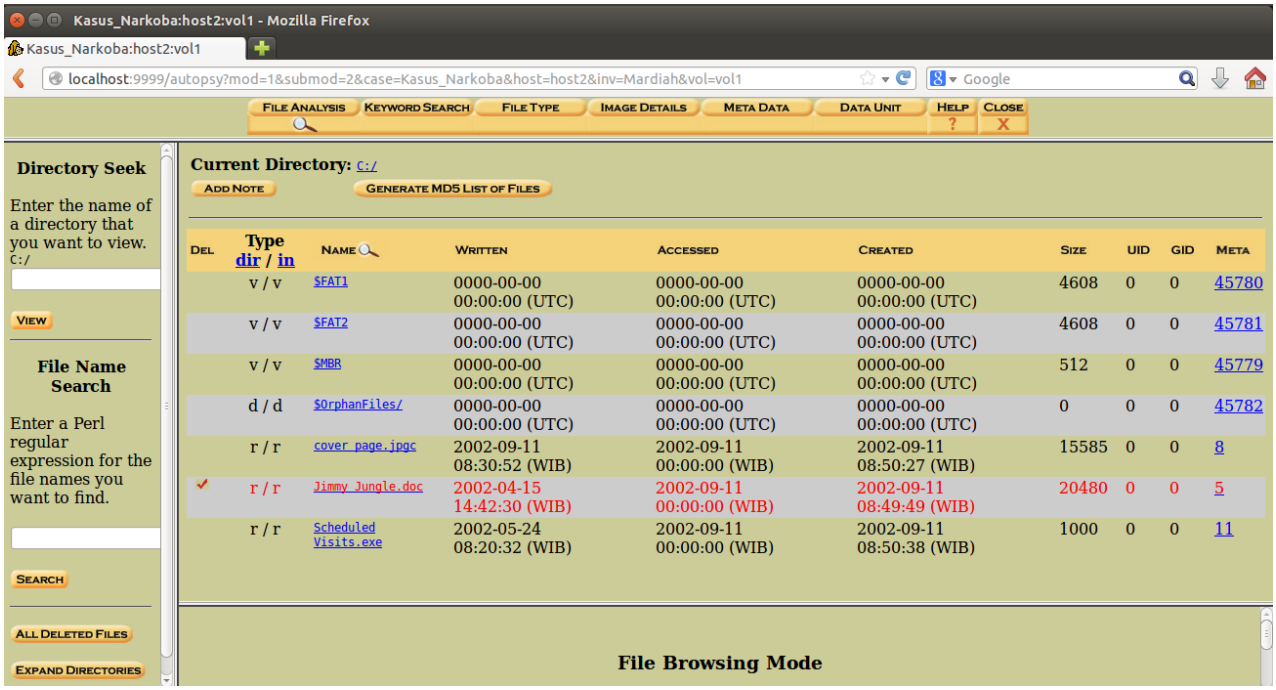
7. Mengatur hostname, siapa yang melakukan forensik pada komputer target



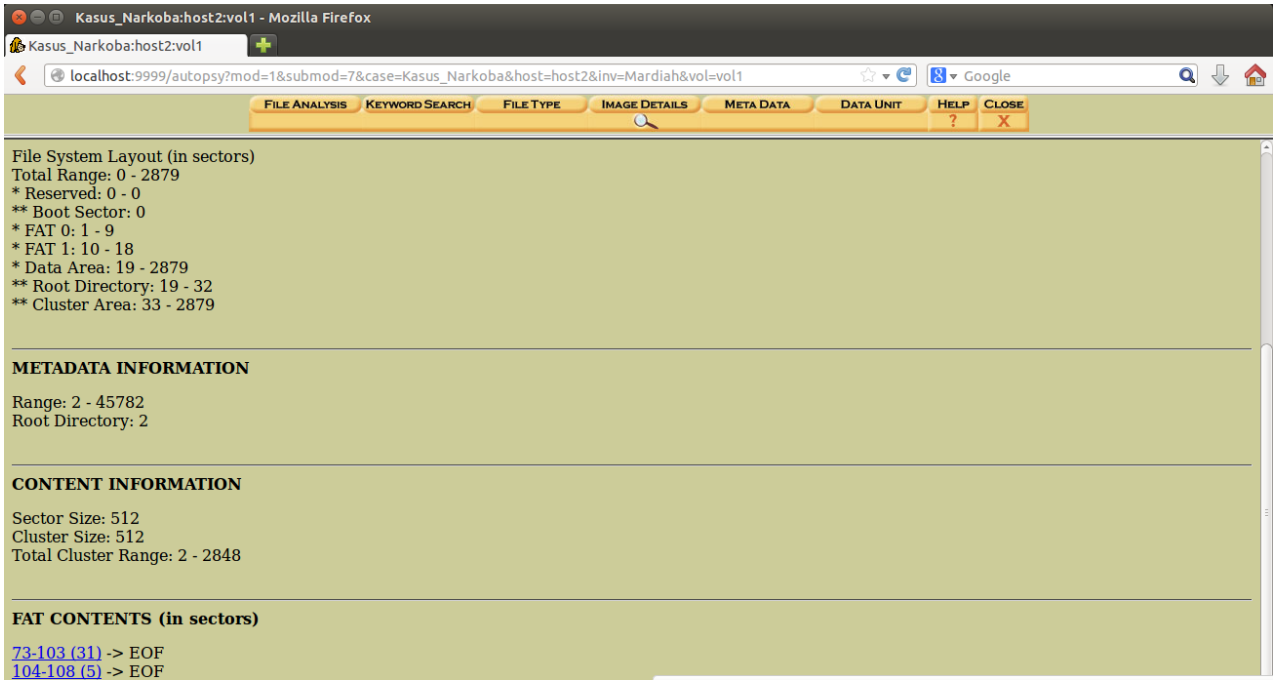
8. Menambahkan file yang akan di autopsy. Dalam percobaan ini menggunakan file image

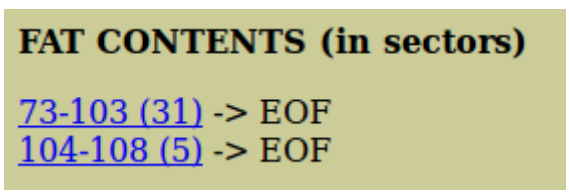




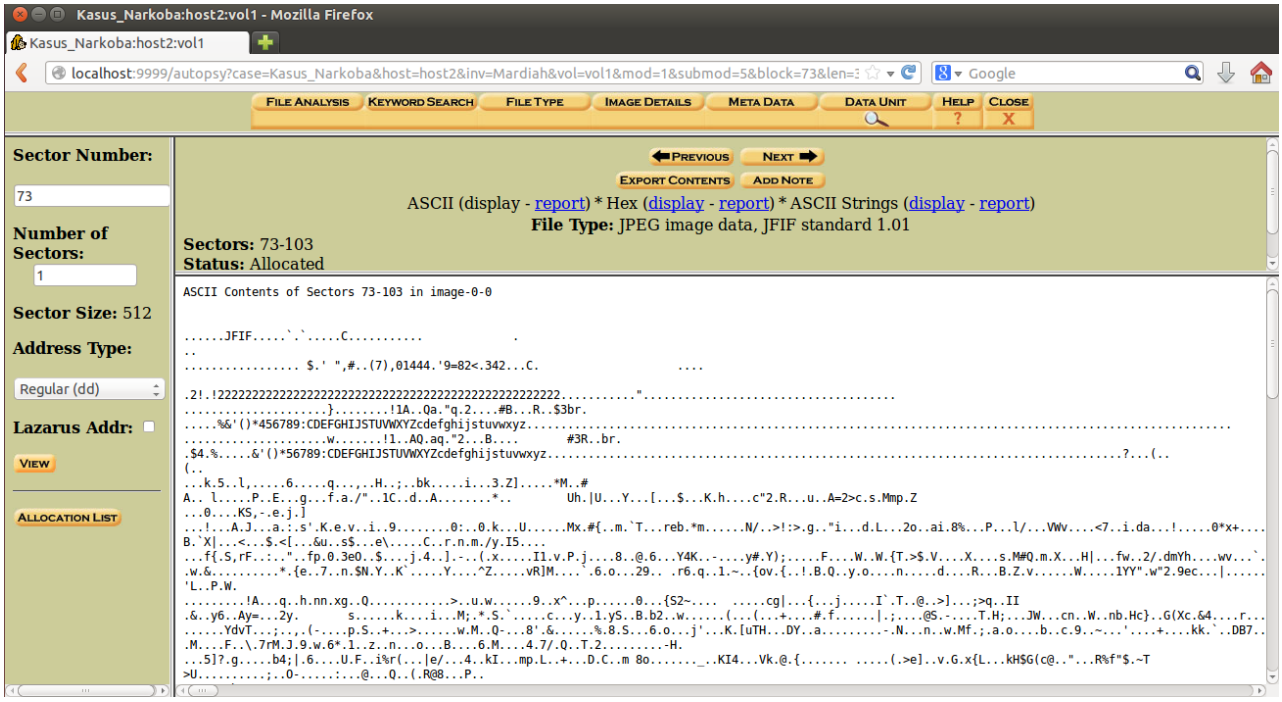


9. Dua konten dalam file image yang bisa kita gunakan untuk autopsy. Yaitu :

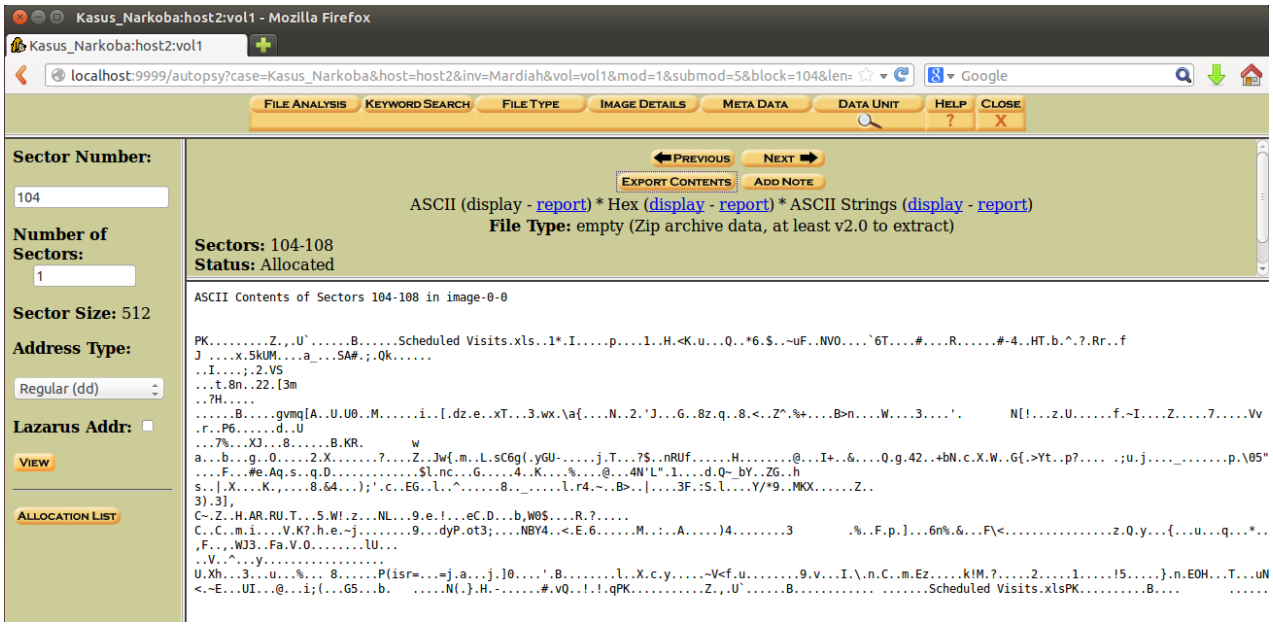




10. Tampilan isi konten pertama yaitu : 73 – 103 (31) .> EOF. Kemudian export contens lalu kita akan mendownload suatu file dari export contens tersebut



11. Tampilan isi konten kedua yaitu : 104 – 108 (5) .> EOF. Sama seperti contents pertama, pada contents kedua juga melakukan export contents dan mendownload suatu file



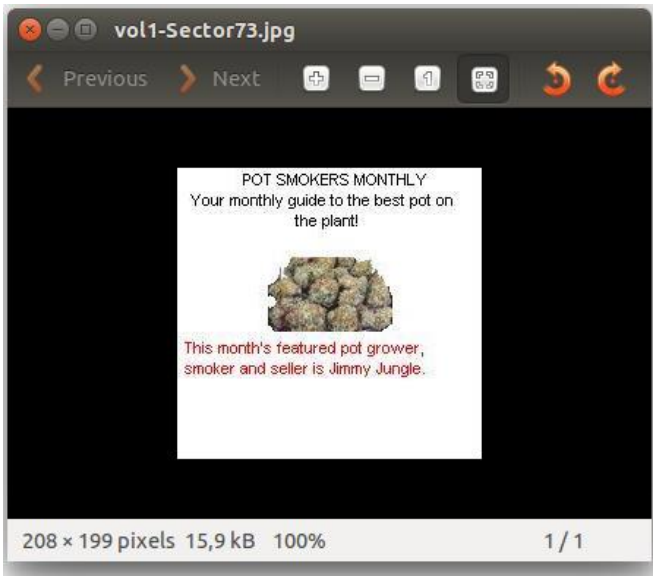
⇨ File yang didownload sebelumnya yaitu :

- Vol1-Sector73.raw
- Vol1-Sector104.raw

12. Lalu Mengecek ekstensi dari file tersebut. Disini merupakan file dari contents yang pertama. Setelah kita mengetahui bahwa ekstensi dari file tersebut yaitu JPEG maka kita rename file tersebut menjadi format JPG

```
root@mardiah-X455LF:/home/mardiah/Downloads# ls
image  image.zip  vol1-Sector104.raw  vol1-Sector73.raw
root@mardiah-X455LF:/home/mardiah/Downloads# file vol1-Sector73.raw
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
root@mardiah-X455LF:/home/mardiah/Downloads#
```

13. Tampilan gambar yang kita dapat pada contents pertama.

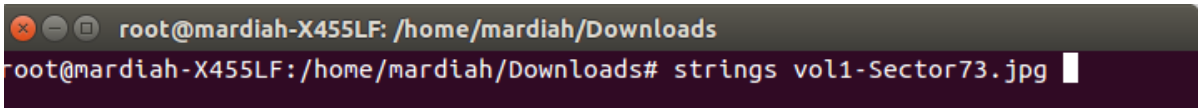


14. Lalu melakukan pengecekan ekstensi pada contens yang kedua

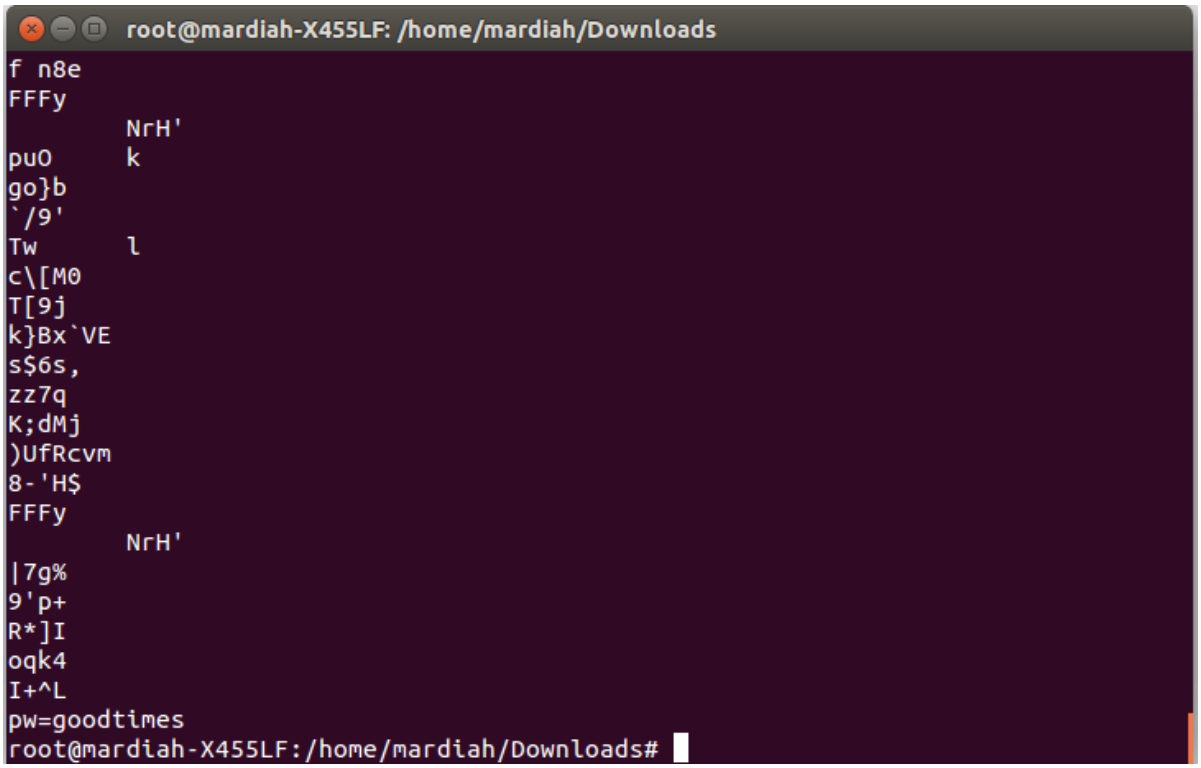
```
root@mardiah-X455LF: /home/mardiah/Downloads
root@mardiah-X455LF:/home/mardiah/Downloads# file vol1-Sector104.raw
vol1-Sector104.raw: Zip archive data, at least v2.0 to extract
root@mardiah-X455LF:/home/mardiah/Downloads#
```

⇨ Dan kita mengetahui ekstensi dari file tersebut, sama seperti langkah sebelumnya, kita rename file tersebut menjadi format zip. Dalam melakukan pengekstraksian, ternyata file tersebut mempunyai password untuk membuka nya, sehingga kita harus mencari tau apa passoword tersebut.

⇨ Ternyata pada contents pertama, diselipkan password pada gambar di atas sehingga kita akan mengetahui password tersebut dengan melakukan proses string pada file contens pertama



15. Lalu akan tampil bahwa password untuk melakukan ekstraksi yaitu : goodtimes



16. Dan isi dari file zip berupa file exel dengan isi sebagai berikut :

	A	B	C
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)
18		Monday (1)	Birard High School (D)
19		Tuesday (2)	Richter High School (E)
20		Wednesday (3)	Hull High School (F)
21		Thursday (4)	Smith Hill High School (A)
22		Friday (5)	Key High School (B)
23		Monday (1)	Leetch High School (C)
24		Tuesday (2)	Birard High School (D)

25	May		
26		Wednesday (3)	Richter High School (E)
27		Thursday (4)	Hull High School (F)
28		Friday (5)	Smith Hill High School (A)
29		Monday (1)	Key High School (B)
30		Tuesday (2)	Leetch High School (C)
31		Wednesday (3)	Birard High School (D)
32		Thursday (4)	Richter High School (E)
33		Friday (5)	Hull High School (F)
34		Monday (1)	Smith Hill High School (A)
35		Tuesday (2)	Key High School (B)
36		Wednesday (3)	Leetch High School (C)
37		Thursday (4)	Birard High School (D)
38		Friday (5)	Richter High School (E)
39		Monday (1)	Hull High School (F)
40		Tuesday (2)	Smith Hill High School (A)
41		Wednesday (3)	Key High School (B)
42		Thursday (4)	Leetch High School (C)
43		Friday (5)	Birard High School (D)
44		Monday (1)	Richter High School (E)
45		Tuesday (2)	Hull High School (F)
46		Wednesday (3)	Smith Hill High School (A)
47		Thursday (4)	Key High School (B)
48		Friday (5)	Leetch High School (C)

49	June		
50		Monday (1)	Birard High School (D)
51		Tuesday (2)	Richter High School (E)
52		Wednesday (3)	Hull High School (F)
53		Thursday (4)	Smith Hill High School (A)
54		Friday (5)	Key High School (B)
55		Monday (1)	Leetch High School (C)
56		Tuesday (2)	Birard High School (D)
57		Wednesday (3)	Richter High School (E)
58		Thursday (4)	Hull High School (F)
59		Friday (5)	Smith Hill High School (A)
60		Monday (1)	Key High School (B)
61		Tuesday (2)	Leetch High School (C)
62		Wednesday (3)	Birard High School (D)
63		Thursday (4)	Richter High School (E)
64		Friday (5)	Hull High School (F)
65		Monday (1)	Smith Hill High School (A)
66		Tuesday (2)	Key High School (B)
67		Wednesday (3)	Leetch High School (C)
68		Thursday (4)	Birard High School (D)
69		Friday (5)	Richter High School (E)

17. Kemudian melakukan recover jika signature nya hilang

```
root@mardiah-X455LF:/home/mardiah/Downloads# foremost -v -i image -o recover
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Mar 29 03:59:03 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/mardiah/Downloads/recover
Configuration file: /etc/foremost.conf
Processing: image
|------------------------------------------------------------------
File: image
Start: Wed Mar 29 03:59:03 2017
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000073.jpg           8 KB           37376
1:      00000033.ole          21 KB           16896
foundat=Scheduled Visits.xls◆◆1*◆I
                                  p◆◆  ◆◆<K◆uq◆Q◆◆*6◆$◆ uF◆◆NVO◆◆◆`6T .#◆◆
 ◆ ◆#-4 T◆b◆^◆?◆Rr◆◆f
J ◆◆ x◆5kUM◆◆◆◆a_◆◆SA#◆;◆Qk멎◆◆
```

```
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000073.jpg           8 KB           37376
1:      00000033.ole          21 KB           16896
foundat=Scheduled Visits.xls◆◆1*◆I
                                  p◆◆  ◆◆<K◆uq◆Q◆◆*6◆$◆ uF◆◆NVO◆◆◆`6T .#◆◆
 ◆ ◆#-4 T◆b◆^◆?◆Rr◆◆f
J ◆◆ x◆5kUM◆◆◆◆a_◆◆SA#◆;◆Qk멎◆◆
 I◆ ◆;◆2◆VS
2:      00000104.zip           2 KB           53248
*|
Finish: Wed Mar 29 03:59:03 2017

3 FILES EXTRACTED

jpg:= 1
ole:= 1
zip:= 1
----------------------------------------------------------------

Foremost finished at Wed Mar 29 03:59:03 2017
root@mardiah-X455LF:/home/mardiah/Downloads#
```

18. Berikut merupakan semua file yang kita dapatkan dari autopsy pada kasus narkoba diatas :