TUGAS KEAMANAN JARINGAN KOMPUTER

“Computer Forensik”

Devi Purnama

09011281320016

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Komputer forensik

Di dalam keamananan jaringan, pasti akan melakukan yang nama nya komputer forensik, komputer forensik adalah “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 untuk memecahkan suatu masalah.

Tujuan dan Fokus Komputer Forensik Adalah :

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki 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 motivitasi 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 penyimpan seperti hardisk eksternal, CD ROM, backup tape, DVD, dan lain-lain.
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

Manfaat dari komputer Foreksik:

1. organisasi/perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti2 pendukung yg di butuhkan.
2. seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut,dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir.
3. Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer;
4. Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya

Objek Forensik “Tidak Ada Kejahatan yang tidak meninggalkan Jejak” Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Contohnya adalah sebagai berikut: Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem, File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu, Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System), Hard disk yang berisi data/informasi backup dari sistem utama, Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya, Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain), Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya).

Secara metodologis, terdapat beberapa tahapan yang perlu dilakukan dalam aktivitas forensik yaitu sebagai berikut:

1. Pernyataan Terjadinya Kejahatan Komputer – merupakan tahap dimana secara formal pihak yang berkepentingan melaporkan telah terjadinya suatu aktivitas kejahatan berbasis komputer.
2. Pengmpulan Petunjuk atau Bukti Awal – merupakan tahap dimana ahli forensik mengumpulkan semua petunjuk atau bukti awal yang dapat dipergunakan sebagai bahan kajian forensik, baik yang bersifat tangible maupun intangible.
3. Penerbitan Surat Pengadilan – merupakan tahap dimana sesuai dengan peraturan dan perundang-undangan yang berlaku, pihak pengadilan memberikan ijin resmi kepada penyelidik maupun penyidik untuk melakukan aktiivitas terkait dengan pengolahan tempat kejadian perkara, baik yang bersifat fisik maupun maya.
4. Pelaksanaan Prosedur Tanggapan Dini – merupakan tahap dimana ahli forensik melakukan serangkaian prosedur pengamanan tempat kejadian perkara, baik fisik maupun maya, agar steril dan tidak tercemar/terkontaminasi, sehingga dapat dianggap sah dalam pencarian barang-barang bukti.
5. Pembekuan Barang Bukti pada Lokasi Kejahatan – merupakan tahap dimana seluruh barang bukti yang ada diambil, disita, dan/atau dibekukan melalui teknik formal tertentu.
6. Pemindahan Bukti ke Laboratorium Forensik – merupakan tahap dimana dilakukan transfer barang bukti dari tempat kejadian perkara ke laboratorium tempat dilakukannya analisa forensik.
7. Pembuatan Salinan “2 Bit Stream” terhadap Barang Bukti – merupakan tahap dimana dilakukan proses duplikasi barang bukti ke dalam bentuk salinan yang identik.

Contoh Kasus :

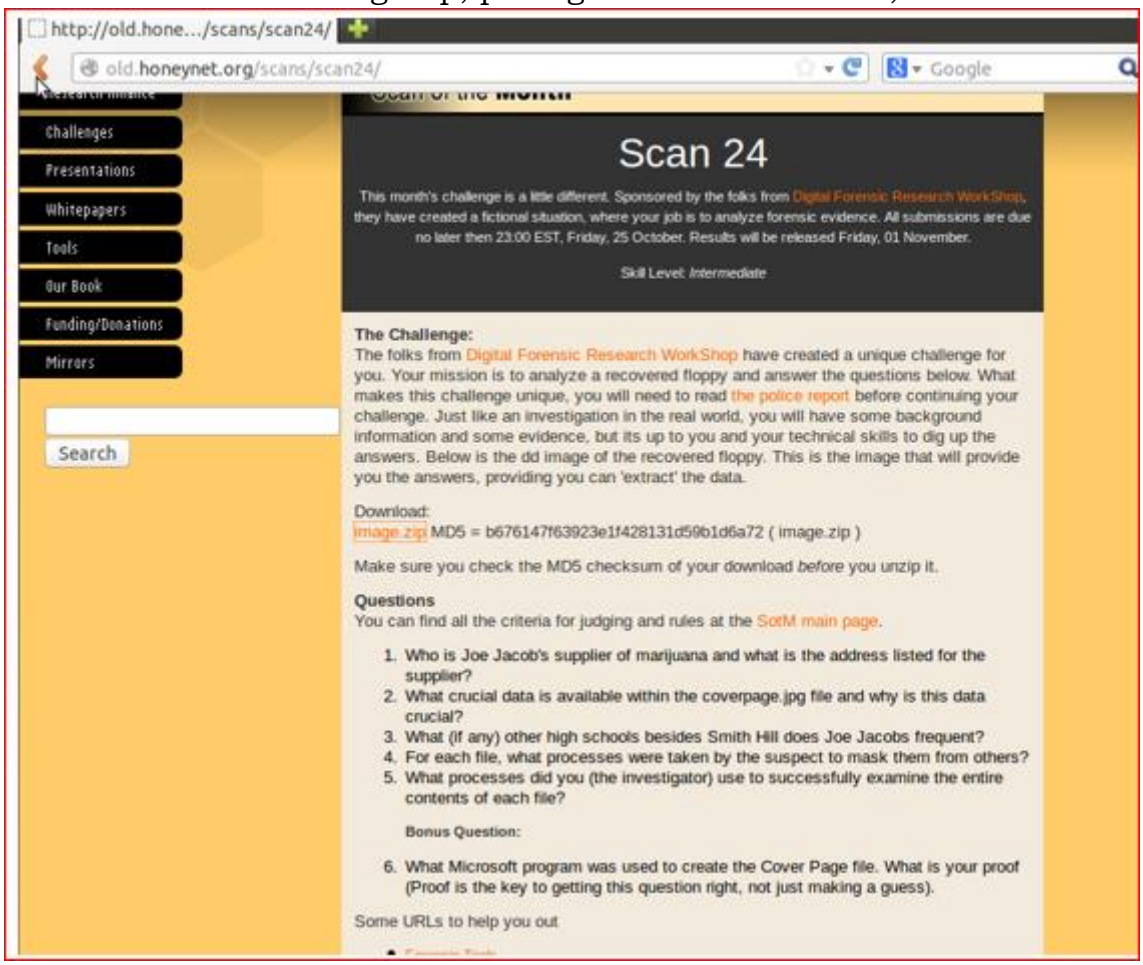
telah tertangkap seorang pengedar narkoba kelas kakap, polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta bantuan oleh polisi untuk melakukan forensic terhadap file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut.

Tool yang bisa digunakan yaitu :

- Autopsy
- Foremost
- Strings

Untuk menyelesaikan kasus di atas langah yang di lakukan yaitu :

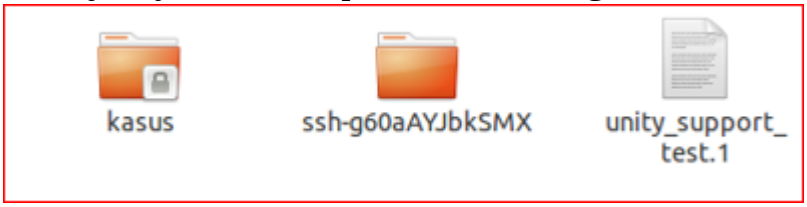
1. Pertama yang di lakukan Buka file old.honey.org/scans/scan24 untuk mendownload data image.zip, pada gambar di bawah ini,



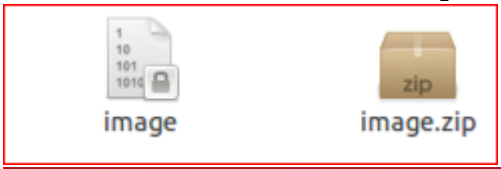
2. Setelah file di Download maka Untuk mengetahui keaslian file maka dapat dilihat dengan perintah berikut.

```
root@mahasiswa:/home/mahasiswa/Downloads# unzip image.zip
Archive:  image.zip
  inflating: image
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#
```

3. Selanjutnya lakukan proses mounting.



4. Di dalam folder kasus terdapat 2 file maka buka file tersebut.




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

5. Lalu cek file untuk melihat keasliannya.

```
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
```

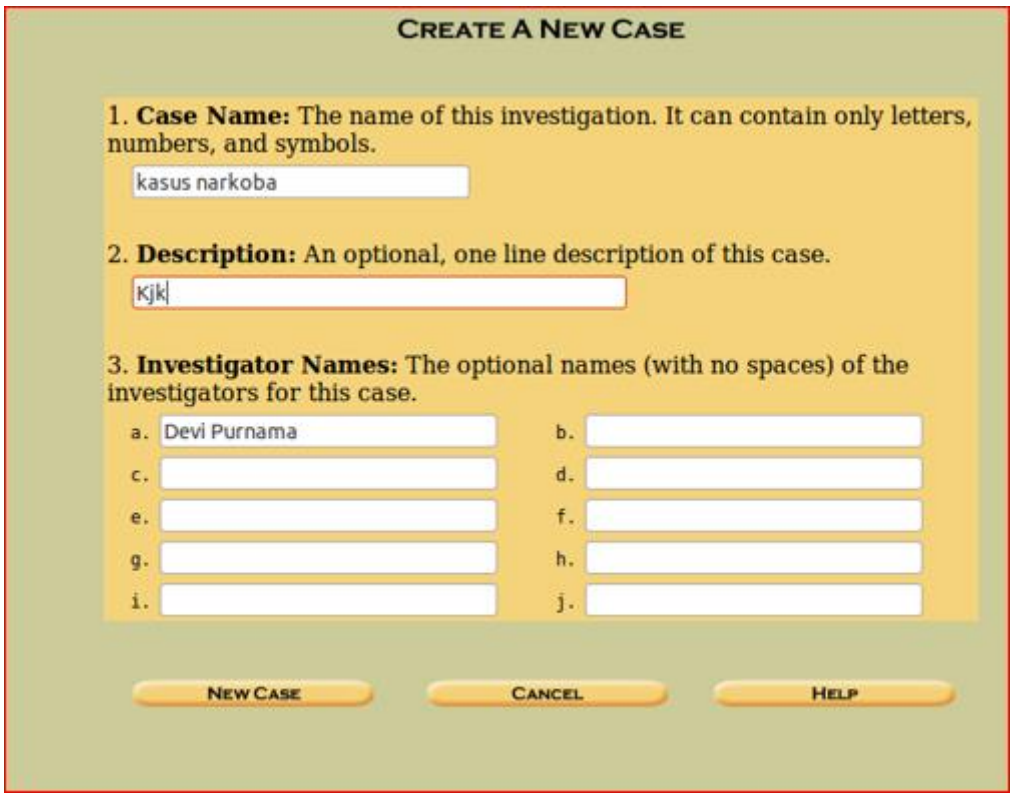
6. Jalankan Tools Psy

```
root@mahasiswa:/tmp/kasus# sudo auto psy
sudo: auto: command not found
root@mahasiswa:/tmp/kasus# autopsy

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

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

================================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Thu Mar 23 10:01:48 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
```

7. Mengatur hostname, siapa yang melakukan forensik pada komputer target, dengan membuka localhost:9999/auotopsy.

8. Pilih New Case

9. Pada jendela New Case isikan Case Name, Description dan Investigator Names

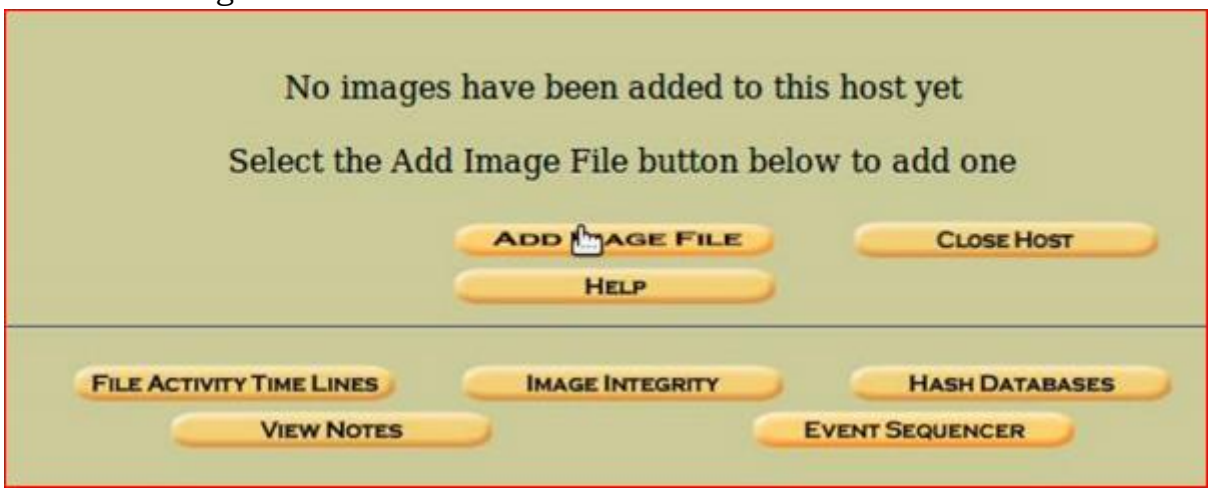


10. Untuk mengecek apakah Case yang kita buat tadi ada atau tidak ada dengan cara masuk ke jendela

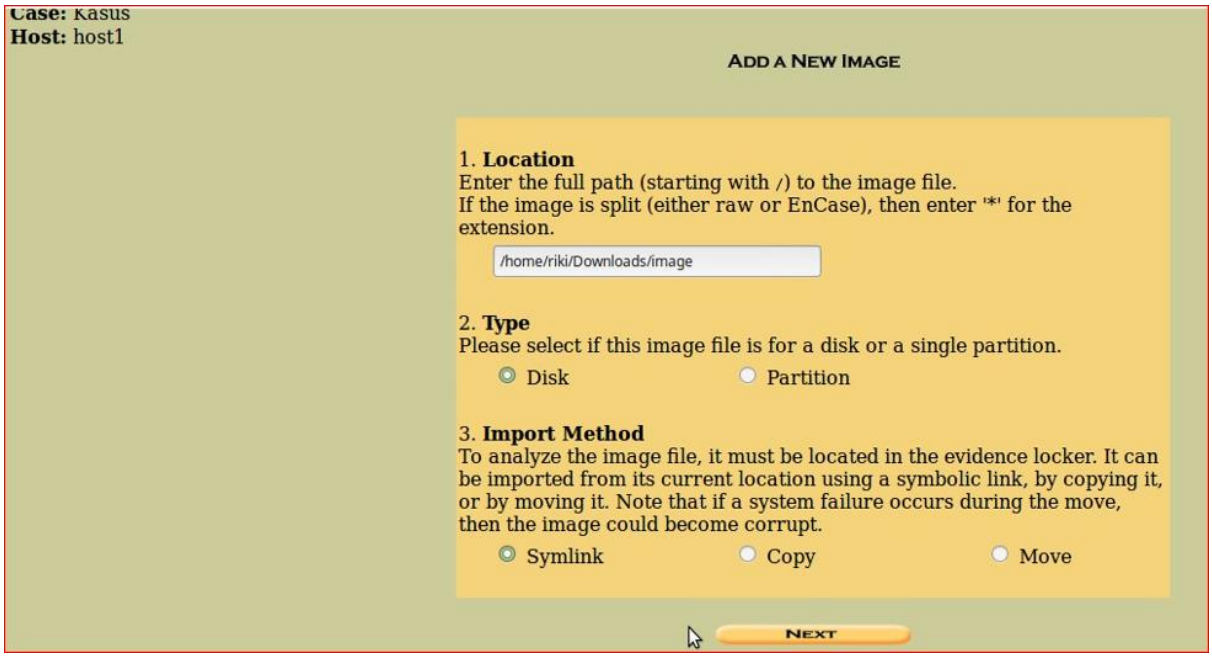
11. Masuk ke Jendela New Host

12. Disana terdapat host yang telah dibuat.

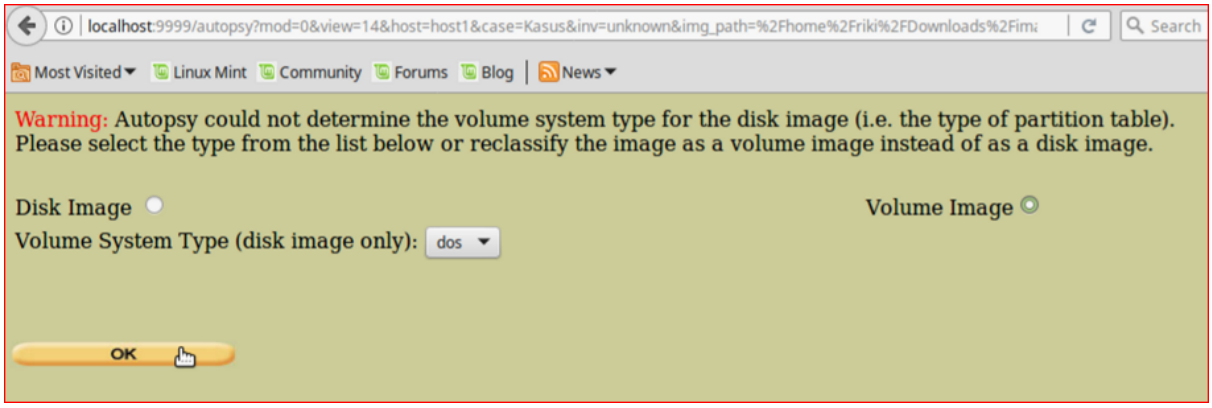
13. Pilih Add Image



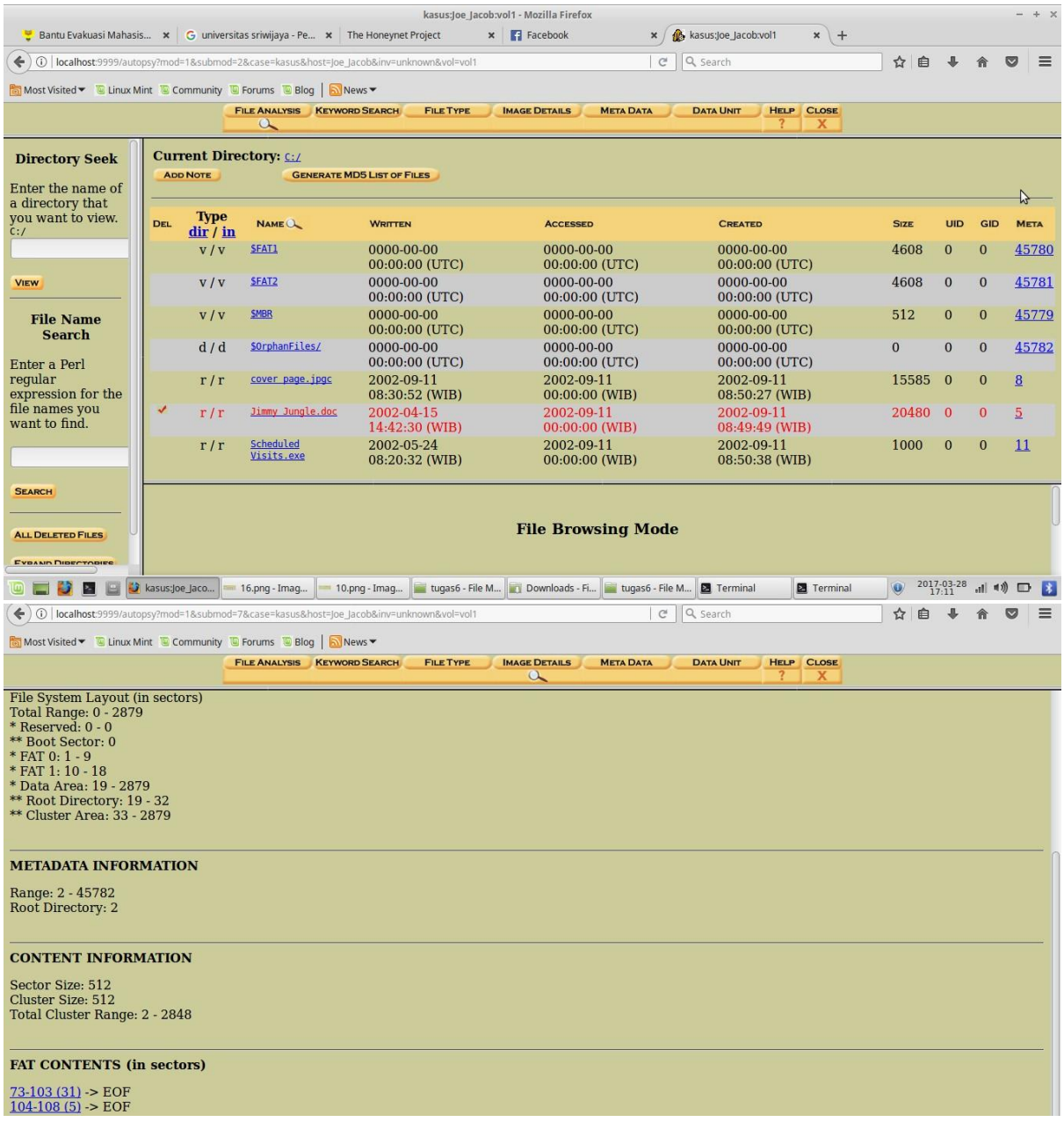
14. Pilih type Disk



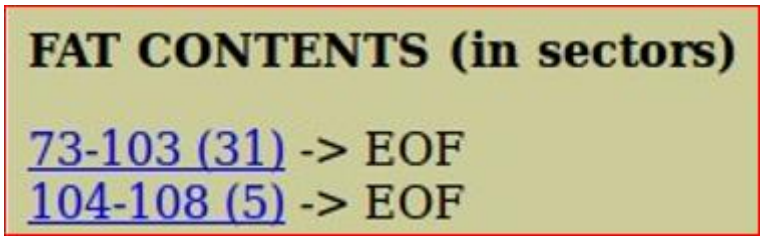
15. Pilih Dos



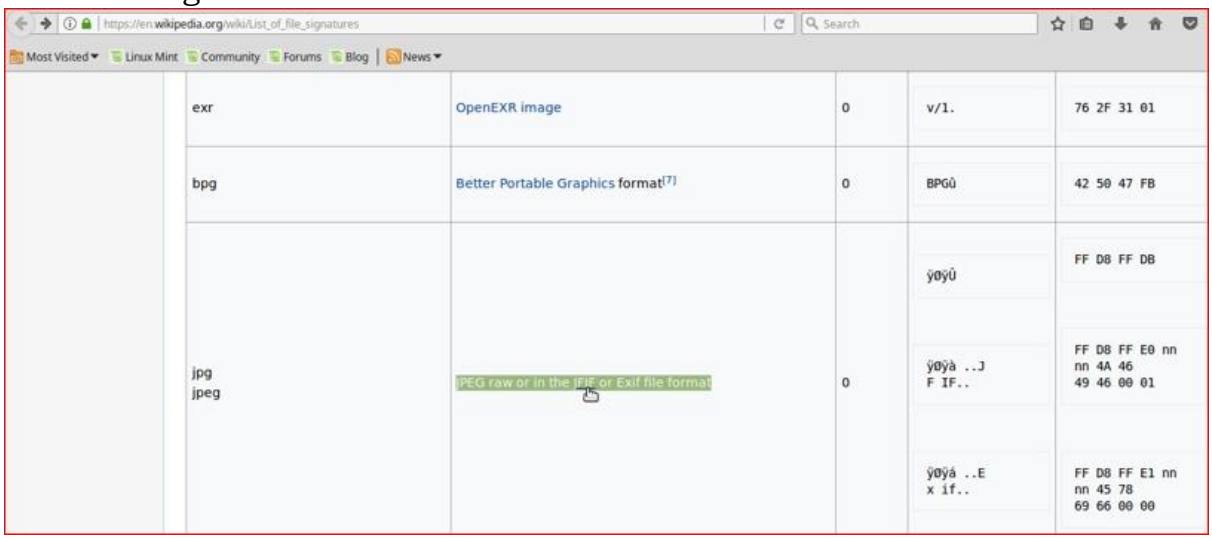
16. Maka Akan Muncul hasil



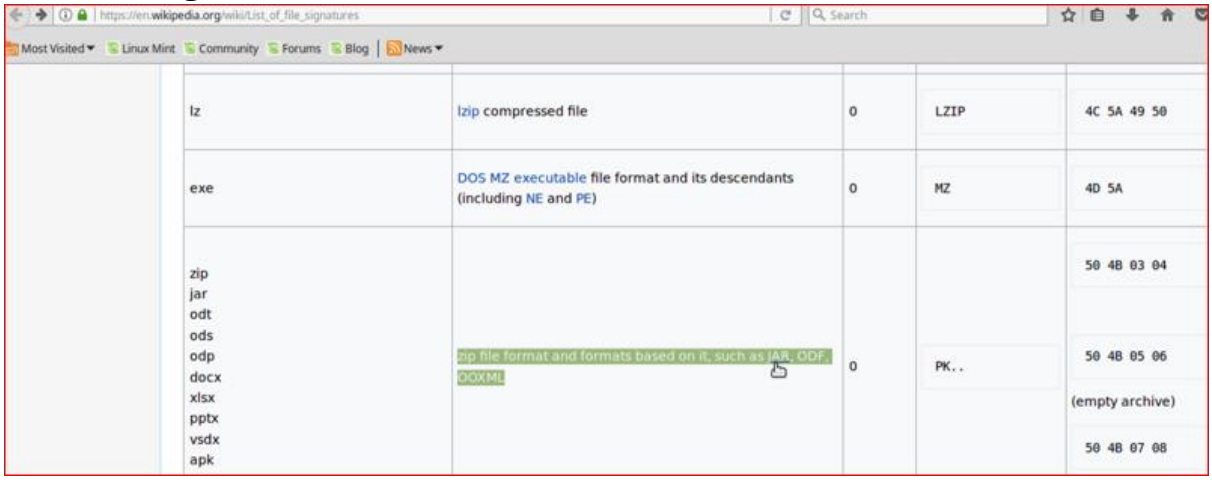
17. Terdapat 2 file yaitu JPG dan PK



18. Untuk mengecek file JPG



19. Untuk mengecek file PK



20. Untuk mengetahui password, rename file jadi JPG, maka hasilnya akan berubah

21. Menyimpan File PW di dalam file gambar dan mendowload file

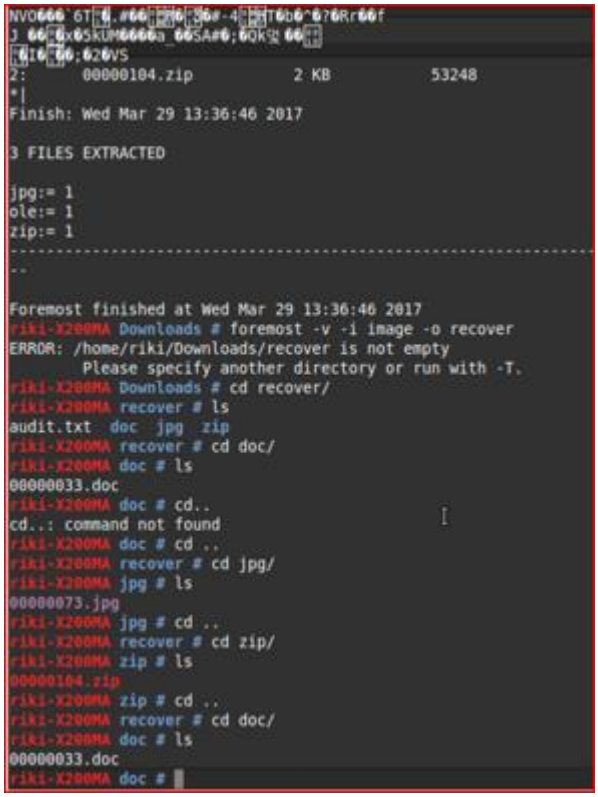
```
root@mahasiswa:/home/mahasiswa/Downloads# strings vol1-Sector73
.jpg
FFFy
        NrH'
puO     k
go}b
`/9'
Tw      l
c\[M0
T[9j
k}Bx`VE
s$6s,
zz7q
K;dMj
)UfRcvm
8-'H$
FFFy
        NrH'
|7g%
9'p+
R*]I
oqk4
I+^L
pw=goodtimes
```

22. Hasil file yang di download akan berbentuk seperti di bawah ini

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)

23. Recove

```
riki-X200MA 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 13:36:46 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/riki/Downloads/recover
Configuration file: /etc/foremost.conf
Processing: image
|------------------------------------------------------------
---
File: image
Start: Wed Mar 29 13:36:46 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.xls66l*6I
                                  [illegible]
NVO666`6T[illegible]
[illegible]
[illegible]
2:       00000104.zip           2 KB           53248
*|
Finish: Wed Mar 29 13:36:46 2017

3 FILES EXTRACTED

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

Foremost finished at Wed Mar 29 13:36:46 2017
```


2: 00000104.zip 2 KB 53248
Finish: Wed Mar 29 13:36:46 2017
3 FILES EXTRACTED
jpg:= 1
ole:= 1
zip:= 1
Foremost finished at Wed Mar 29 13:36:46 2017
riki-X200MA Downloads # foremost -v -i image -o recover
ERRDR: /home/riki/Downloads/recover is not empty
Please specify another directory or run with -T.
riki-X200MA Downloads # cd recover/
riki-X200MA recover # ls
audit.txt doc jpg zip
riki-X200MA recover # cd doc/
riki-X200MA doc # ls
00000033.doc
riki-X200MA doc # cd..
cd..: command not found
riki-X200MA doc # cd ..
riki-X200MA recover # cd jpg/
riki-X200MA jpg # ls
00000073.jpg
riki-X200MA jpg # cd ..
riki-X200MA recover # cd zip/
riki-X200MA zip # ls
00000104.zip
riki-X200MA zip # cd ..
riki-X200MA recover # cd doc/
riki-X200MA doc # ls
00000033.doc
riki-X200MA doc #