TUGAS KEAMANAN JARINGAN KOMPUTER

“ Computer Forensik “

NAMA : DESY MARITA

NIM : 09011281320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Di dalam keamananan jaringan, pasti akan melakukan yang nama nya komputer forensik. Dimana pada intinya forensik komputer 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."

Tujuan utama dari aktivitas forensik komputer, yaitu:

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat buti yang sah di pengadilan; dan
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.

Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi. Sementara itu fokus data yang dikumpulkan dapat dikategorikan menjadi 3 (tiga) domain utama, yaitu:

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.

Memiliki kemampuan dalam melakukan forensik komputer akan mendatangkan sejumlah manfaat, antara lain:

- Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan.
- Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir.
- Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer; dan

- Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Terlepas dari manfaat tersebut, teramat banyak tantangan dalam dunia forensik komputer, terutama terkait dengan sejumlah aspek sebagai berikut:

- Forensik komputer merupakan ilmu yang relatif baru, sehingga "Body of Knowledge"-nya masih sedemikian terbatas (dalam proses pencarian dengan metode "learning by doing");
- Walaupun berada dalam rumpun ilmu forensik, namun secara prinsip memiliki sejumlah karakteristik yang sangat berbeda dengan bidang ilmu forensik lainnya – sehingga sumber ilmu dari individu maupun pusat studi sangatlah sedikit;
- Perkembangan teknologi yang sedemikian cepat, yang ditandai dengan diperkenalkannya produk-produk baru dimana secara langsung berdampak pada berkembangnya ilmu forensik komputer tesebut secara pesat, yang membutuhkan kompetensi pengetahuan dan keterampilan sejalan dengannya;
- Semakin pintar dan trampilnya para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang;
- Cukup mahalnya harga peralatan canggih dan termutakhir untuk membantu proses forensik komputer beserta laboratorium dan SDM pendukungnya;
- Secara empiris, masih banyak bersifat studi kasus (happening arts) dibandingkan dengan metodologi pengetahuan yang telah dibakukan dimana masih sedikit pelatihan dan sertifikasi yang tersedia dan ditawarkan di masyarakat;
- Sangat terbatasnya SDM pendukung yang memiliki kompetensi dan keahlian khusus di bidang forensik komputer; dan
- Pada kenyataannya, pekerjaan forensik komputer masih lebih banyak unsur seninya dibandingkan pengetahuannya (more "Art" than "Science").

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);

- Absensi akses server atau komputer yang dikelola oleh sistem untuk merekam setiap adanya pengguna yang login ke piranti terkait; dan lain sebagainya.

Secara metodologis, terdapat paling tidak 14 (empat belas) tahapan yang perlu dilakukan dalam aktivitas forensik, 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;
8. Pengembangan “MD5 Checksum” Barang Bukti – merupakan tahap untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada;
9. Penyiapan Rantai Posesi Barang Bukti – merupakan tahap menentukan pengalihan tanggung jawab dan kepemilikan barang bukti asli maupun duplikasi dari satu wilayah otoritas ke yang lainnya;
10. Penyimpanan Barang Bukti Asli di Tempat Aman – merupakan tahap penyimpanan barang bukti asli (original) di tempat yang aman dan sesuai dengan persyratan teknis tertentu untuk menjaga keasliannya;
11. Analisa Barang Bukti Salinan – merupakan tahap dimana ahli forensik melakuka analisa secara detail terhadap salinan barang-brang bukti yang dikumpulkan untuk mendapatkan kesimpulan terkait dengan seluk beluk terjadinya kejahatan;
12. Pembuatan Laporan Forensik – merupakan tahap dimana ahli forensik menyimpulkan secara detail hal-hal yang terjadi seputar aktivititas kejahatan yang dianalisa berdasarkan fakta forensik yang ada;
13. Penyerahan Hasil Laporan Analisa – merupakan tahap dimana secara resmi dokumen rahasia hasil forensik komputer diserahkan kepada pihak yang berwajib; dan

14. Penyertaan dalam Proses Pengadilan – merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi.

KASUS :

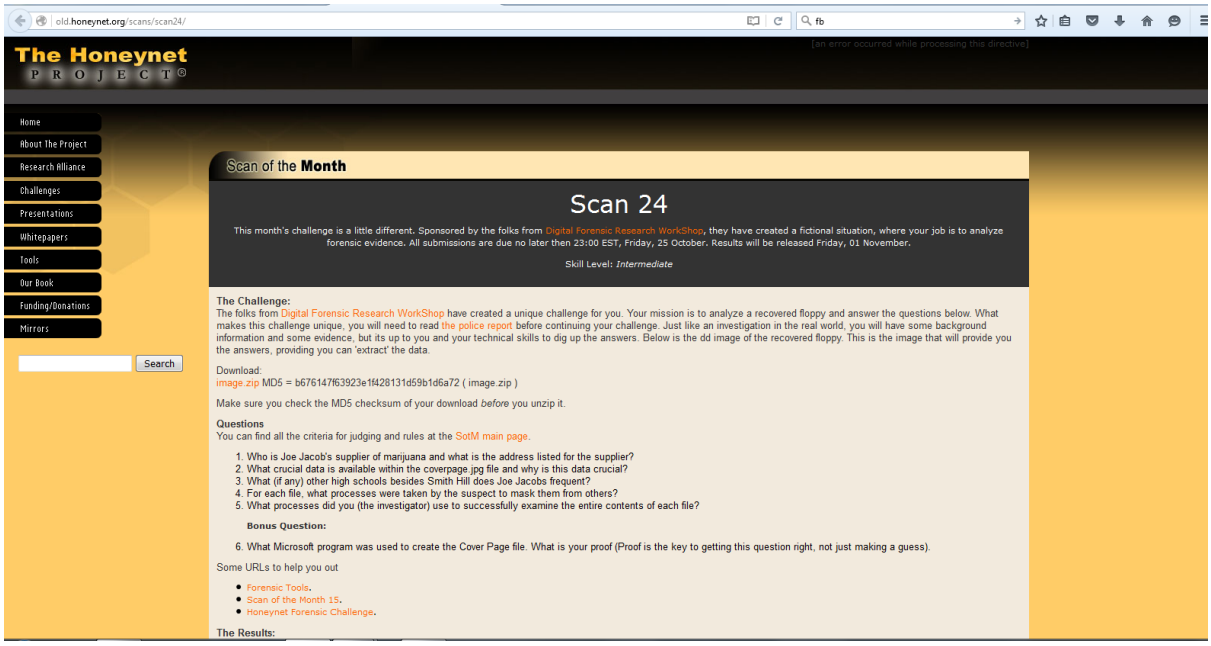
Ada seorang pengedar narkoba kelas kakap yang tertangkap, polisi hanya ada harddrive yang sdah korup dr tersangka. Bagaimana kita me recover nya ?

Tool yang bisa digunakan yaitu :

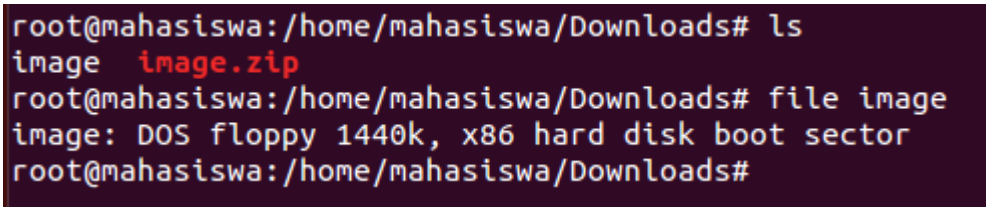
1. Autopsy
2. Foremost
3. Strings

Langkah yang dilakukan yaitu :

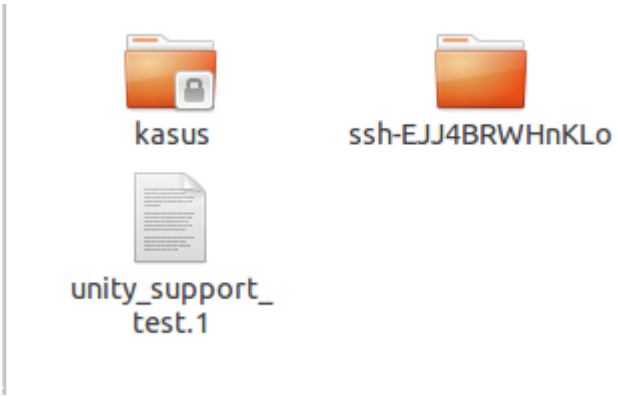
- Install tools yang akan digunakan
- Buka wesite berikut ini



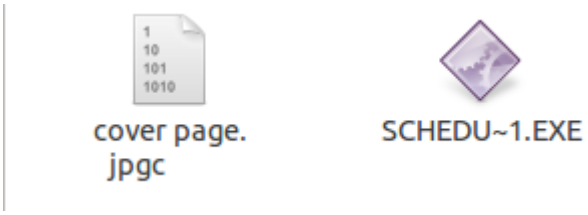
- sebuah file pasti ada md5sum yang berfungsi untuk mengecek keaslian dari file atau integritas file. Cek tipe file dengan perintah berkut



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



Di dalam folder Kasus terdapat 2 file yaitu :




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

- Lalu cek lagi keaslian file

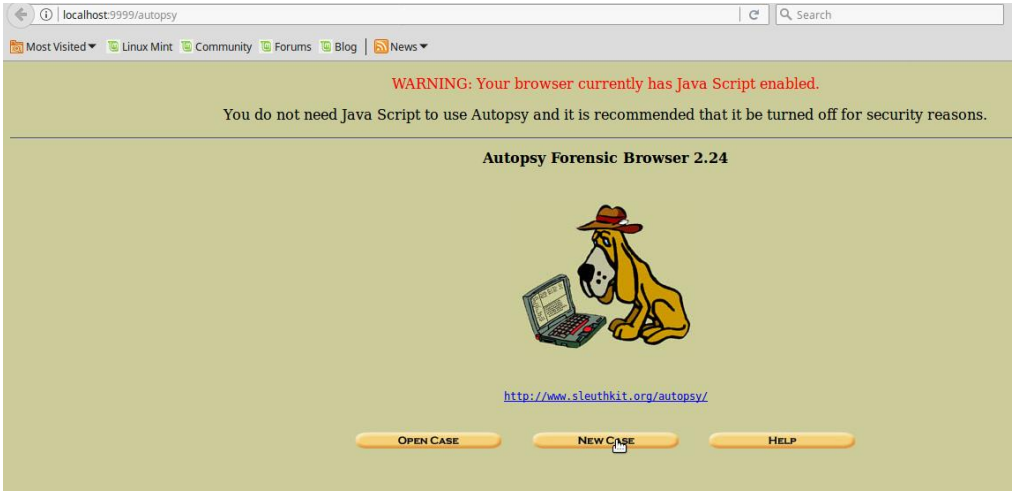
```
root@mahasiswa:/tmp/kasus# file *
cover page.jpgc           : ERROR: cannot read `cover page.jpgc
          ' (Input/output error)
SCHEDU~1.EXE:              Zip archive data, at least v2.0 to
extract
root@mahasiswa:/tmp/kasus#
```

- Jalankan Tools psy

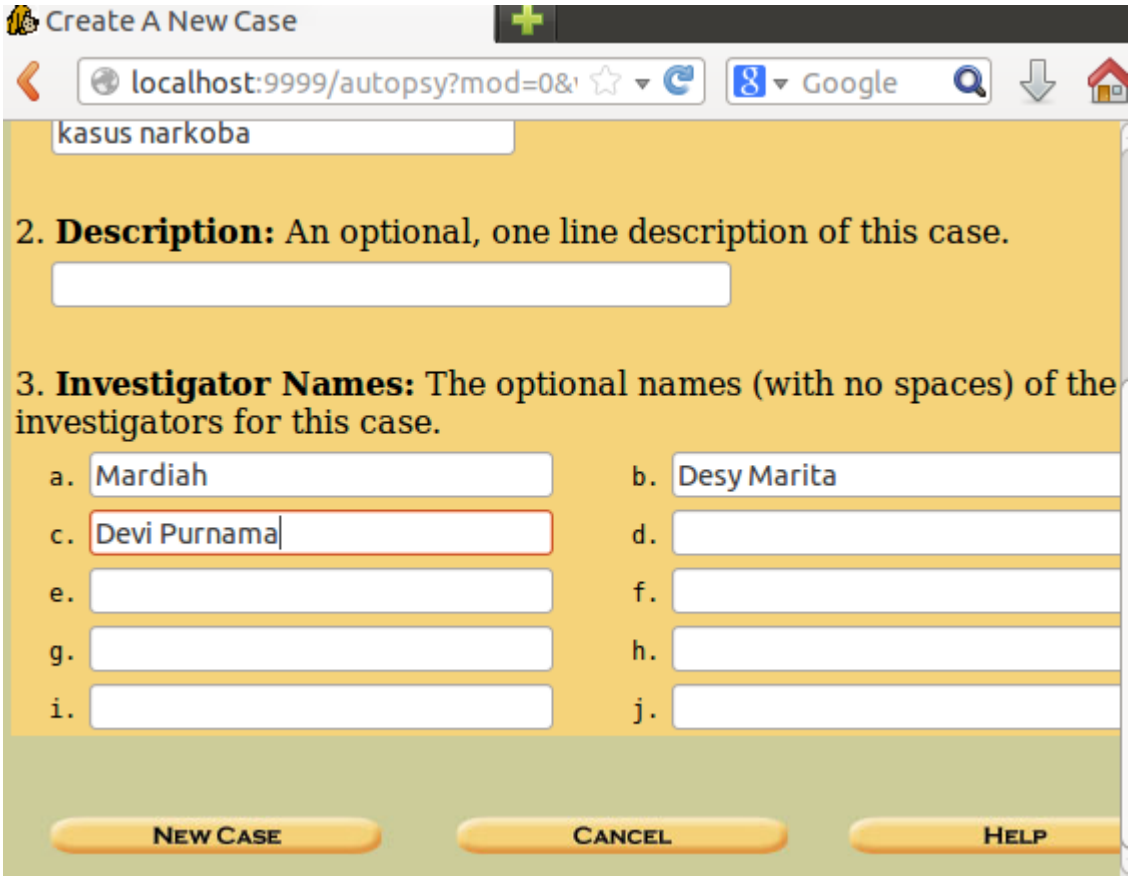
```
root@mahasiswa:/tmp/kasus# autopsy
  I
================================================================
=============

                       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
```

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

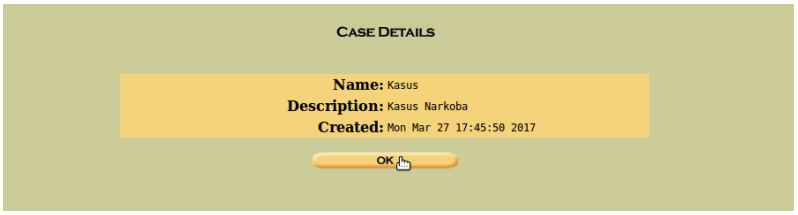
- Pilih New Case



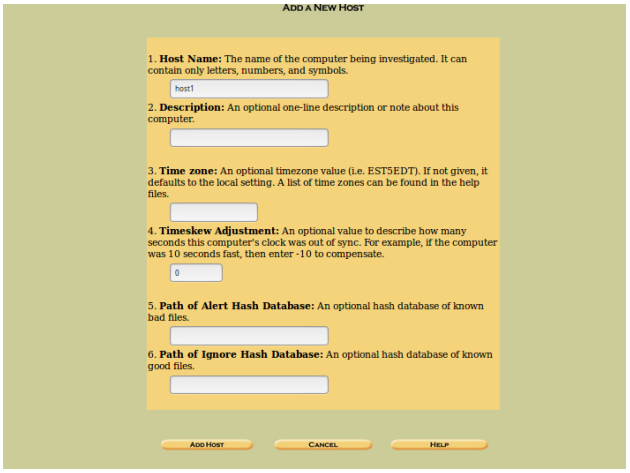
- Pada jendela New Case isikan Case Name, Description dan Investigator Names



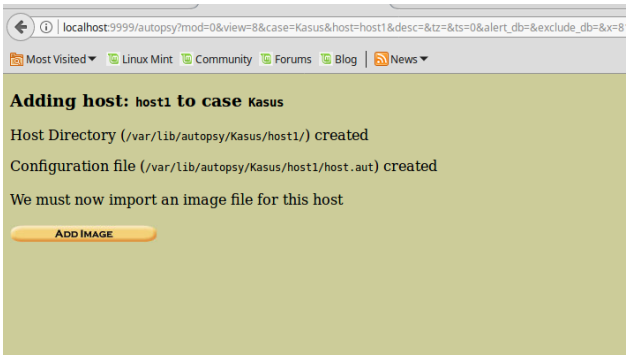
- Untuk mengecek apakah Case yang kita buat tadi ada atau tidak ada dengan cara masuk ke jendela



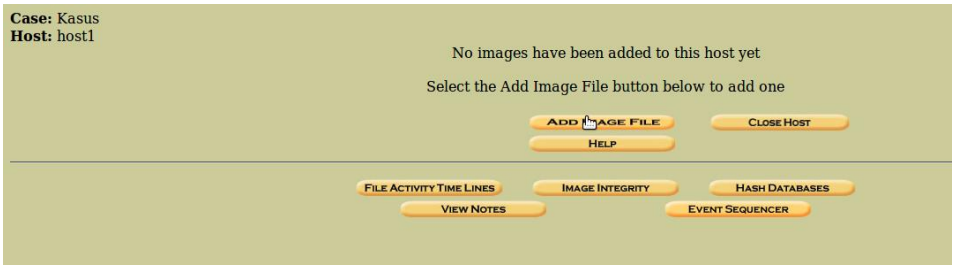
- Masuk ke jendela New Host



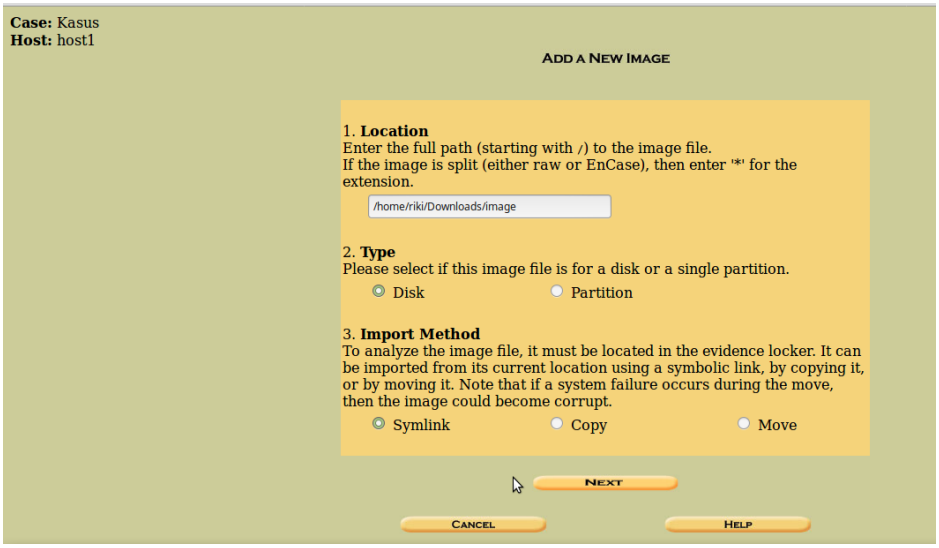
- Disana terdapat host yang telah dibuat



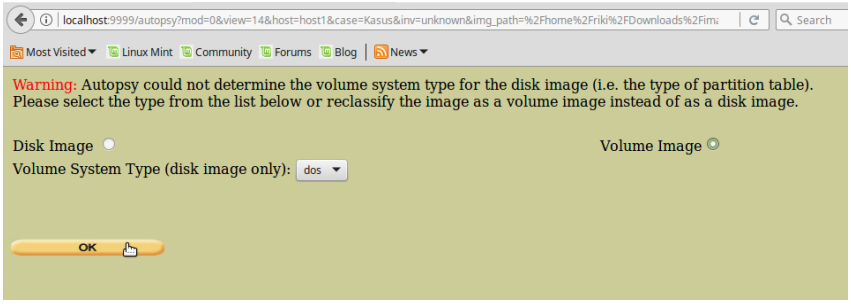
- Pilih Add Image File



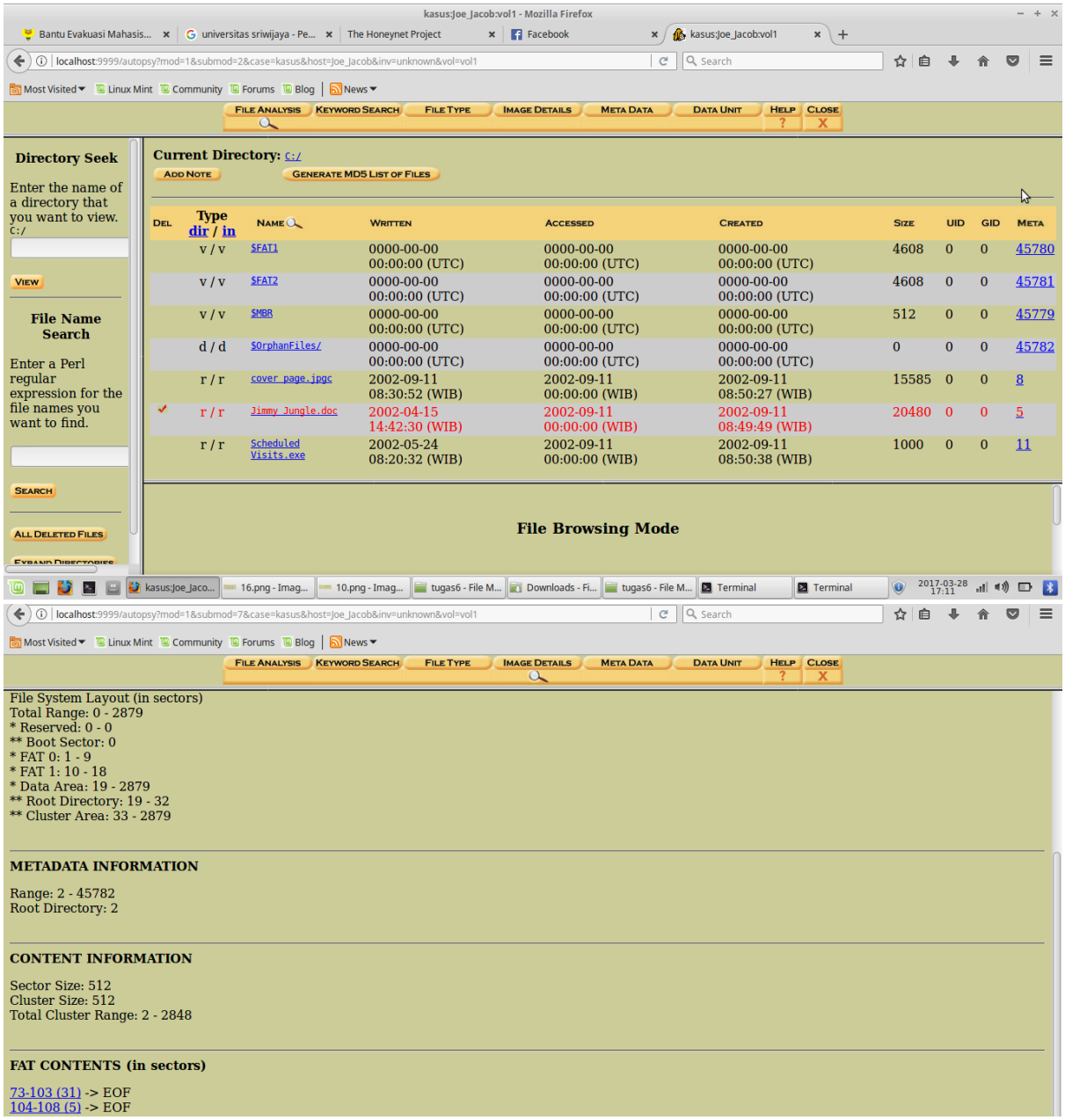
- pilih type Disk



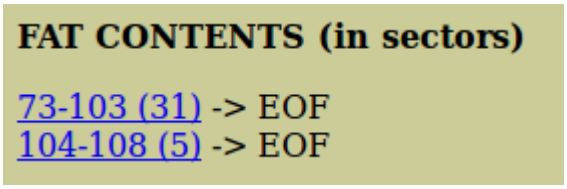
- Lalu pilih DOS



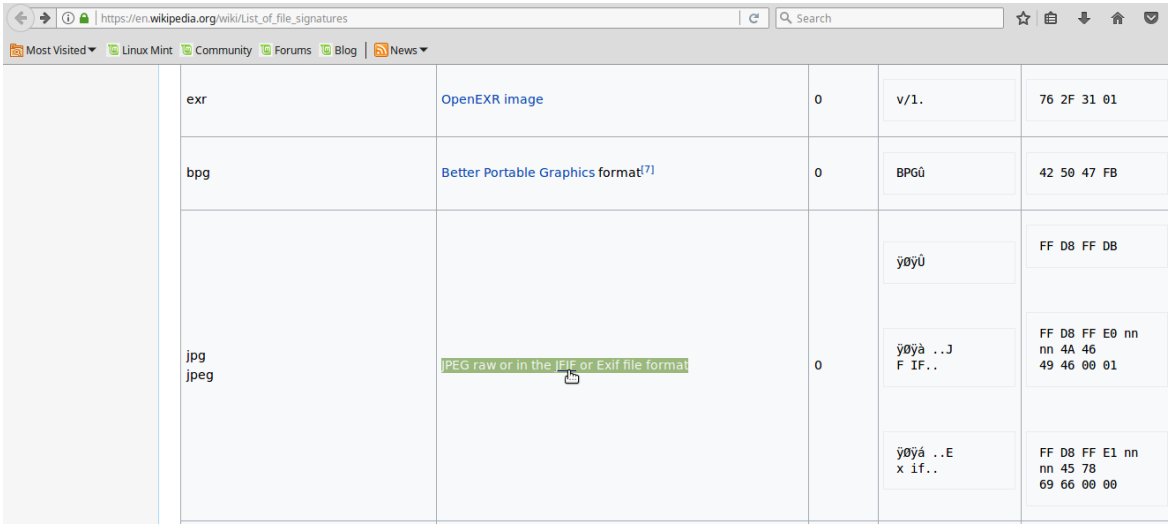
- di dapatlah hasil



- Terdapat 2 file yaitu JPG dan PK

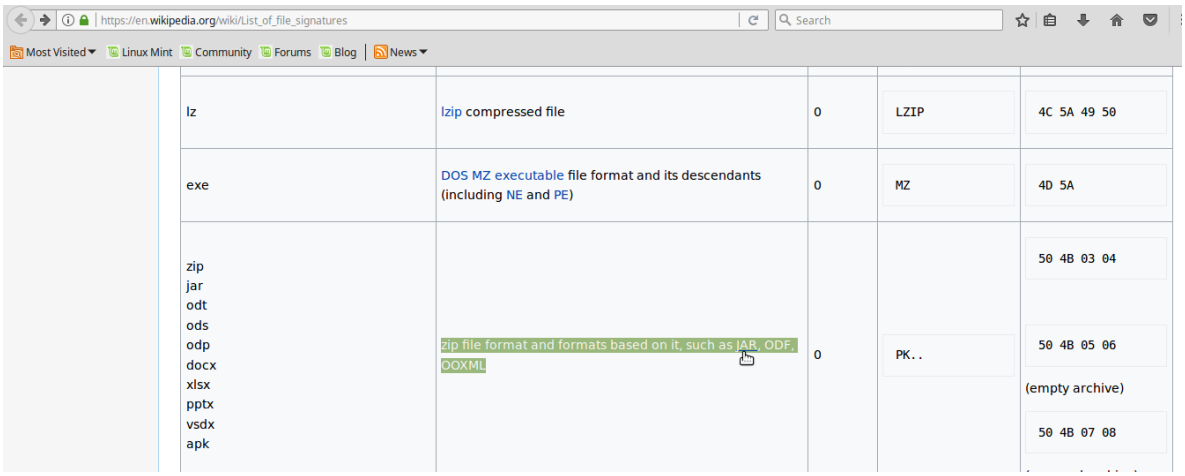


- Untuk mengecek file JPG



exr	OpenEXR image	0	v/1.	76 2F 31 01
bpg	Better Portable Graphics format[7]	0	BPGû	42 50 47 FB
jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿØÿÛ ÿØÿà ..J F IF.. ÿØÿá ..E x if..	FF D8 FF DB FF D8 FF E0 nn nn 4A 46 49 46 00 01 FF D8 FF E1 nn nn 45 78 69 66 00 00

- Untuk mengecek file PK



lz	lzip compressed file	0	LZIP	4C 5A 49 50
exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A
zip jar odt ods odp docx xlsx pptx vsdx apk	zip file format and formats based on it, such as JAR, ODF, OOXML	0	PK..	50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08

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

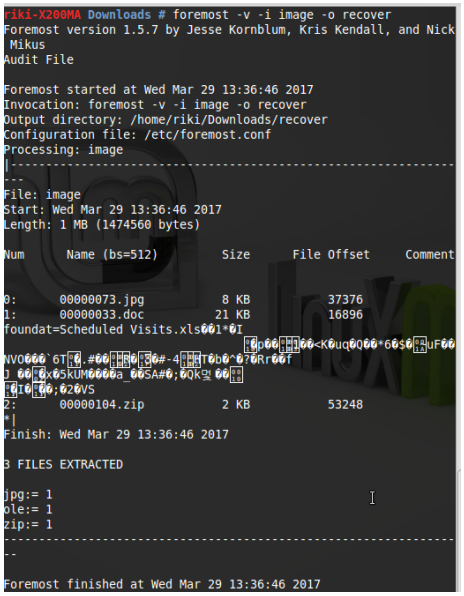
- Menyimpan pw di dalam file gambar dan men download file

```
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
root@mahasiswa:/home/mahasiswa/Downloads#
```

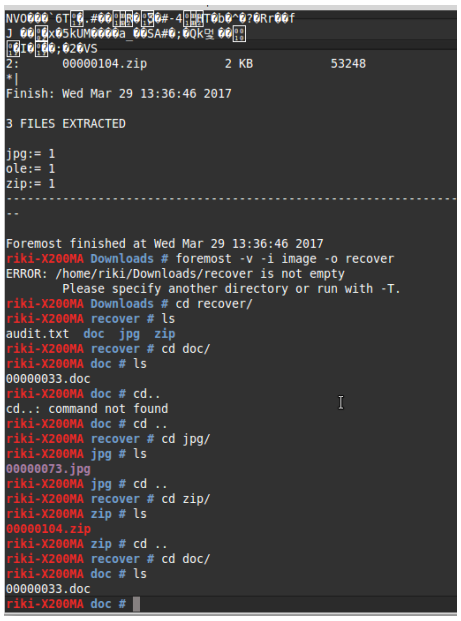
- Hasil file yang di download akan berbentuk seperti di bawah ini

	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)

- recover



```
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.xls▯▯1*▯I
                                  ▯▯p▯▯▯▯▯▯<K▯uq▯▯▯*6▯$▯▯uF▯▯
NVO▯▯▯`6T▯▯.#▯▯▯▯▯▯▯#-4▯▯▯T▯b▯^▯7▯Rr▯▯f
J ▯▯▯▯x▯5kUM▯▯▯▯a_▯▯SA#▯;▯▯k및 ▯▯▯▯
▯▯I▯▯▯;▯2▯VS
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
```



```
NVO▯▯▯`6T▯▯.#▯▯▯▯▯▯▯#-4▯▯▯T▯b▯^▯7▯Rr▯▯f
J ▯▯▯▯x▯5kUM▯▯▯▯a_▯▯SA#▯;▯▯k및 ▯▯▯▯
▯▯I▯▯▯;▯2▯VS
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
ERROR: /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 #
```