

KEAMANAN JARINGAN KOMPUTER



Ulan Purnama Sari

09011181320003

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

Task 6

computer forensics

Komputer forensik atau yang juga dikenal juga dengan istilah digital forensik, adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang dapat ditemukan pada komputer dan media penyimpanan digital lainnya. Forensik sendiri merupakan sebuah proses ilmiah dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti pada sidang pengadilan karena adanya suatu kasus hukum. Secara singkat tujuan dari komputer forensik adalah untuk menjabarkan keadaan terkini dari suatu catatan digital.

Tugas :

Diminta bantuan untuk mendapatkan informasi tentang kasus narkoba

- Tampilkan capture langkah langkahnya
- Jawab pertanyaan untuk memberikan informasi

Tools yang digunakan :

- AutoPsy
- Foremost
- Strings

TAMPILAN CAPTURE LANGKAH – LANGKAH

1. Langkah pertama kali kita melakukan perintah md5sum pada file zip, terlebih dahulu kita download dulu file nya. Gambar dibawah adalah perintah md5sum yang file image.zip nya berada di direktori Videos.

```
Videos
Terminal
dee-K46CB Videos # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
dee-K46CB Videos #
```

Gambar 1. Perintah md5sum

2. Kemudian kita lakukan perintah file image yang bertujuan untuk melihat tipe file yang digunakan. Dalam hal ini file yang digunakan adalah DOS.

```
Videos
Terminal
dee-K46CB Videos # file image
image: DOS floppy 1440k, x86 hard disk boot sector
dee-K46CB Videos #
```

Gambar 2. Perintah file image

3. Selanjutnya, kita membuat direktori baru dengan kasus narkoba setelahnya melakukan mount image kedalam direktori itu.

```
dee-K46CB Videos # mkdir /tmp/kasus.narkoba
dee-K46CB Videos # mount image /tmp/kasus.narkoba/
dee-K46CB Videos #
```

Gambar 3. Perintah mkdir dan mount image

4. Setelah kita membuat direktori kita masuk ke dalam direktori tersebut dan masukkan perintah ls, perintah ls tersebut bertujuan untuk kita bisa melihat didalam direktori tersebut telah terdapat isi

```
Videos
Terminal
dee-K46CB Videos # cd /tmp/kasus.narkoba/
dee-K46CB kasus.narkoba # ls
cover page.jpg          SCHEDU-1.EXE
dee-K46CB kasus.narkoba #
```

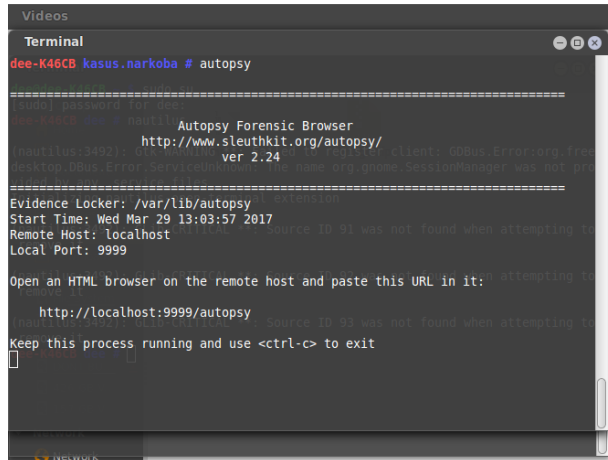
Gambar 4. Melihat isi direktori

5. Lalu kita mengekstrak semua file yang terdapat pada direktori kasus.narkoba dengan menggunakan perintah 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
```

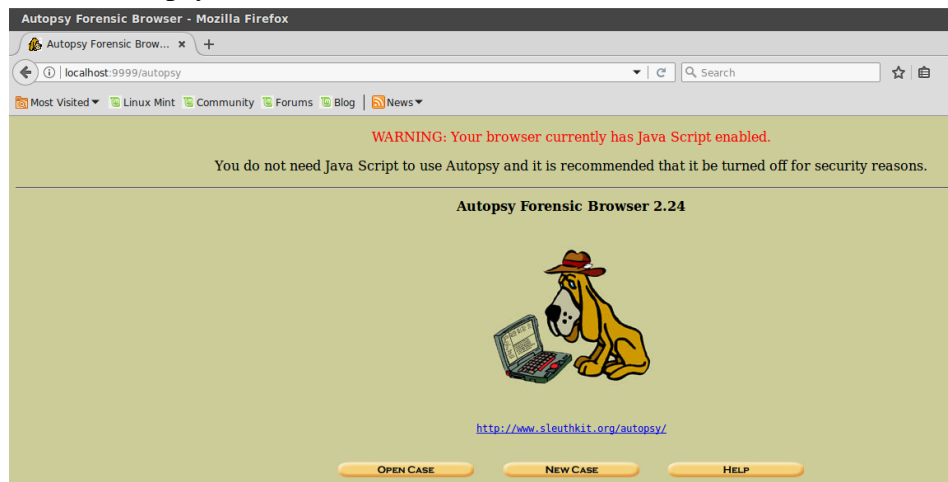
Gambar 5. Perintah ekstrak file

6. Membuka tools Autopsy



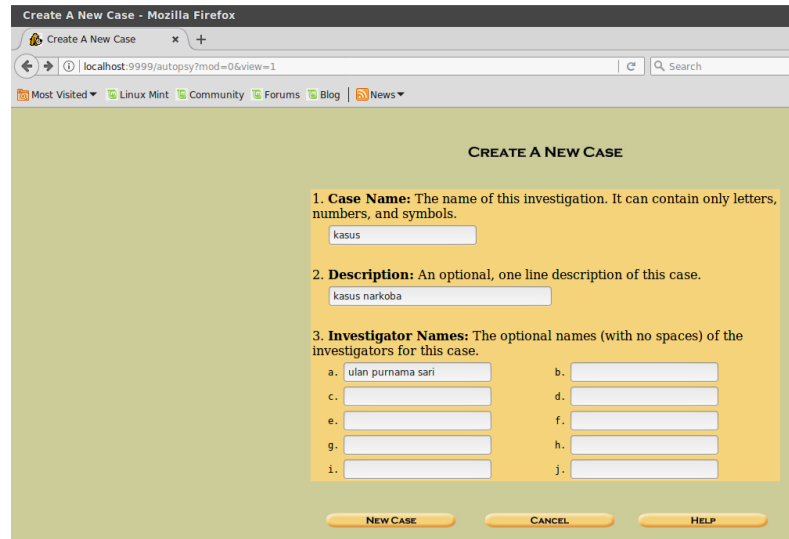
Gambar 6. Membuka tools Autopsy

7. Langkah ke-6 kita sudah membuka tools autopsy pada terminal biarkan agar tetap running terminal tersebut, lalu kita buka autopsy pada web dan menuliskan localhost:9999/autopsy



Gambar 7. Tampilan pada web Autopsy

8. Langkah berikutnya membuat kasus baru, untuk membuat kasus baru nya kita pilih New Case , inputkan sesuai kasus yang kita sedang tangani



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. ulan purnama sari	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

Gambar 8.1 Membuat kasus baru



Gambar 8.2 Tampilan Kasus berhasil dibuat

Lalu klik ADD HOST , kita akan disuruh menginputkan host name. Disini saya menginputkan host name Joe_Jacob sesuai dengan perintah yang dilakukan.

ADD A NEW HOST

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- Description:** An optional one-line description or note about this computer.
- 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.
- 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.
- Path of Alert Hash Database:** An optional hash database of known bad files.
- Path of Ignore Hash Database:** An optional hash database of known good files.

Gambar 8.3. Add New Host

Adding host: Joe_Jacob to case kasus

Host Directory (/var/lib/autopsy/kasus/Joe_Jacob/) created

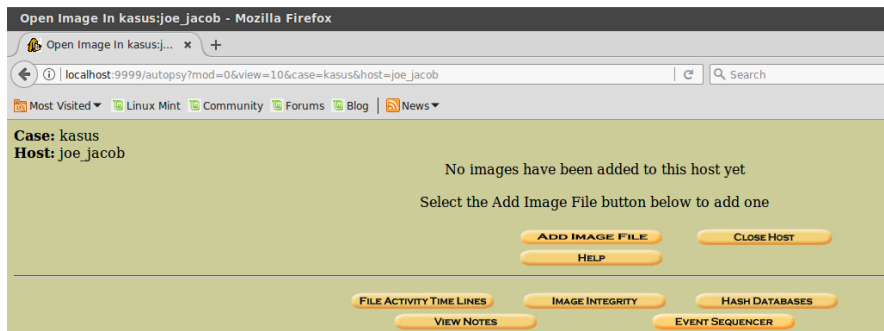
Configuration file (/var/lib/autopsy/kasus/Joe_Jacob/host.aut) created

We must now import an image file for this host

[ADD IMAGE](#)

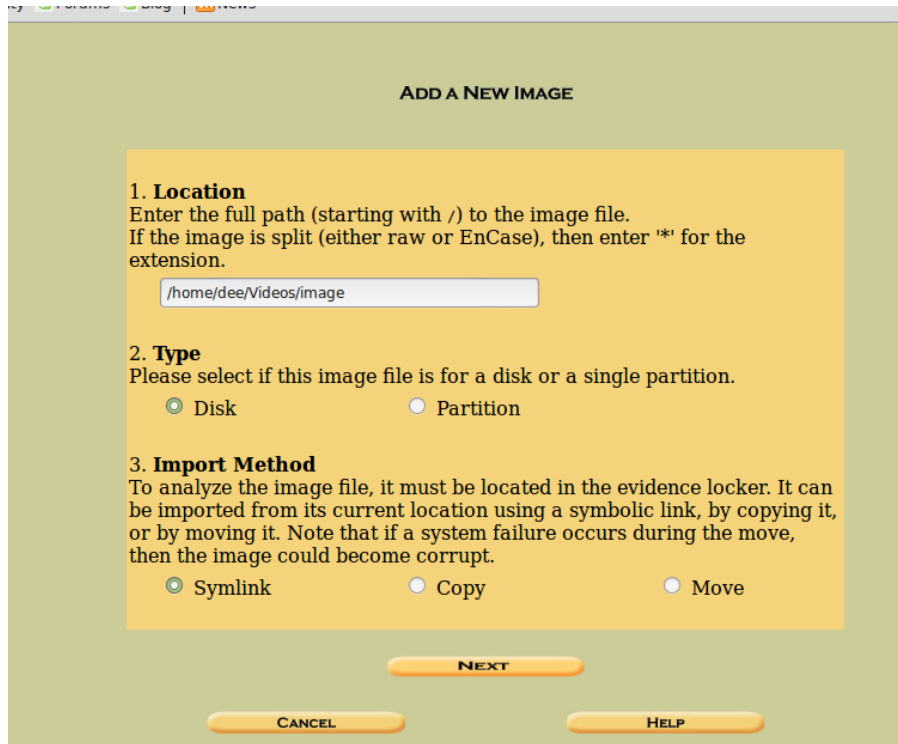
Gambar 8.4 Tampilan berhasil menambah Host

Lalu langkah selanjutnya memilih Add Image File



Gambar 8.5 Add Image File

Perintah selanjutnya kita diarahkan untuk memberikan lokasi penyimpanan dari gambar tersebut , saya letakkan di direktori `/home/dee/Videos/image`



ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type
Please select if this image file is for a disk or a single partition.

Disk Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink Copy Move

NEXT

CANCEL **HELP**

gambar 8.6 Menentukan lokasi penyimpanan



Collecting details on new image file - Mozilla Firefox

Collecting details on ne... x +

localhost:9999/autopsy?mod=0&view=14&host=joe_jacob&case=kasus&inv=unknown&img_path=%2Fhome%2F... | Search

Most Visited Linux Mint Community Forums Blog News

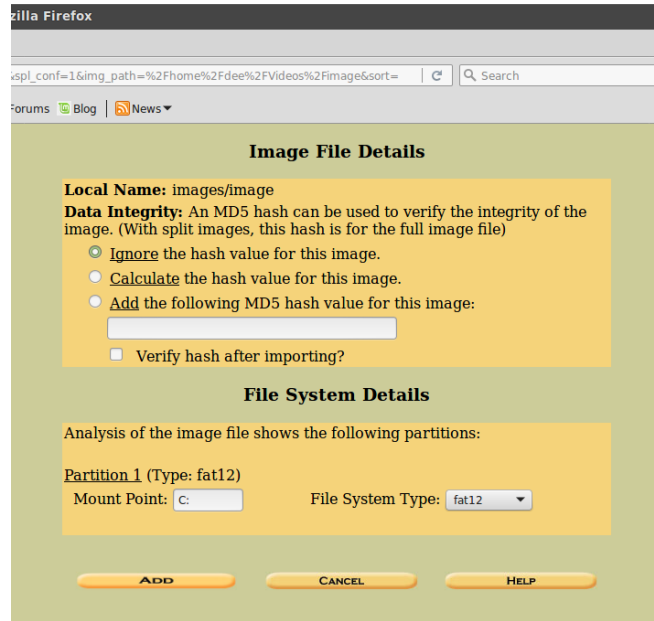
Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image Volume Image

Volume System Type (disk image only): dos

OK

Gambar 8.7 Volume Image Dos

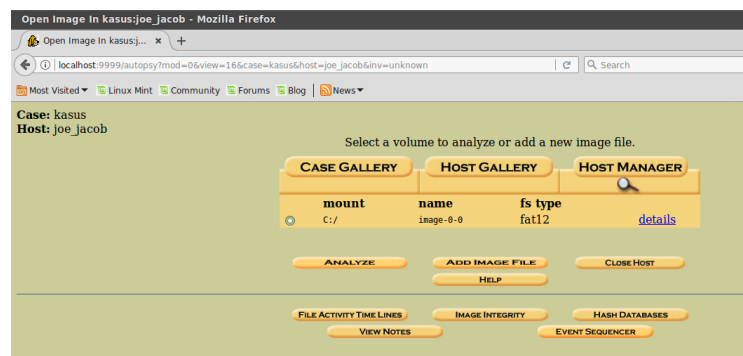


Gambar 8.8 Image file details

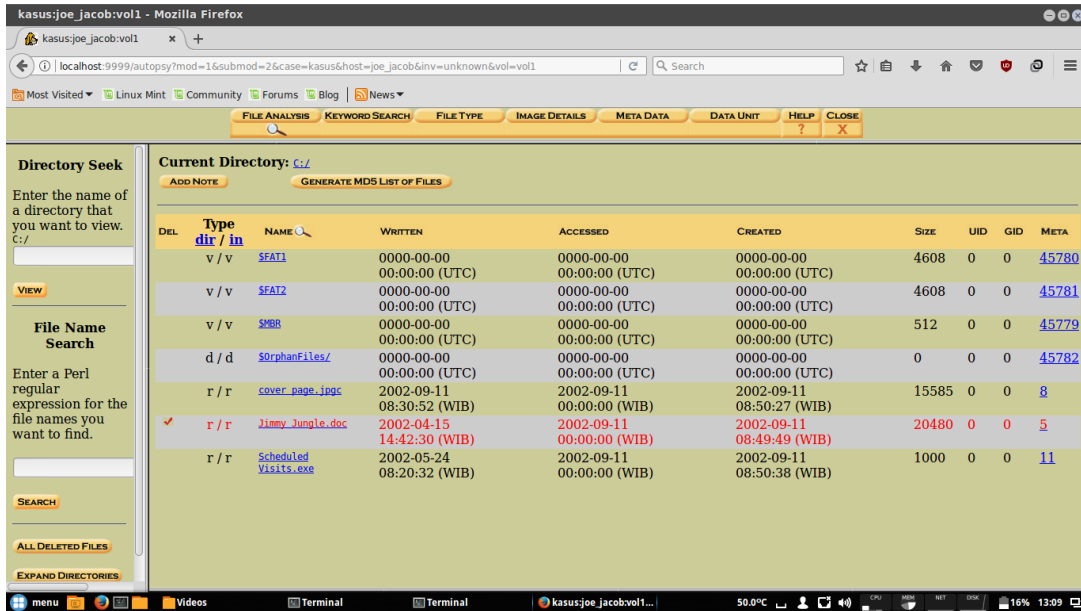


Gambar 8.9. Testing Partitions

Tampilan setelah kita memilih OK, akan muncul tampilan testing partition

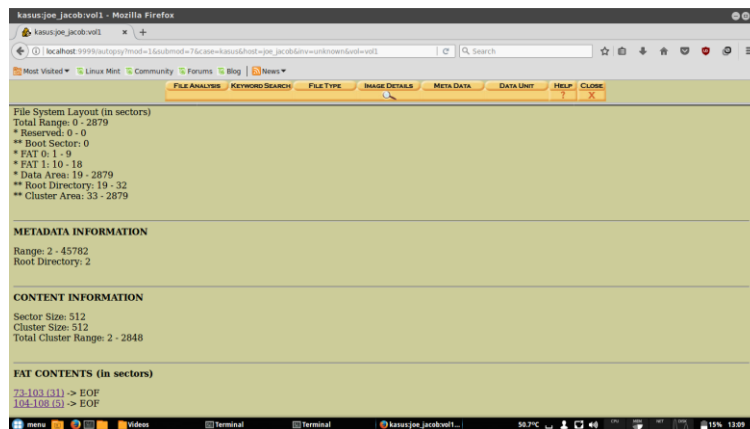


Gambar 8.10. Tampilan Volume Analyze

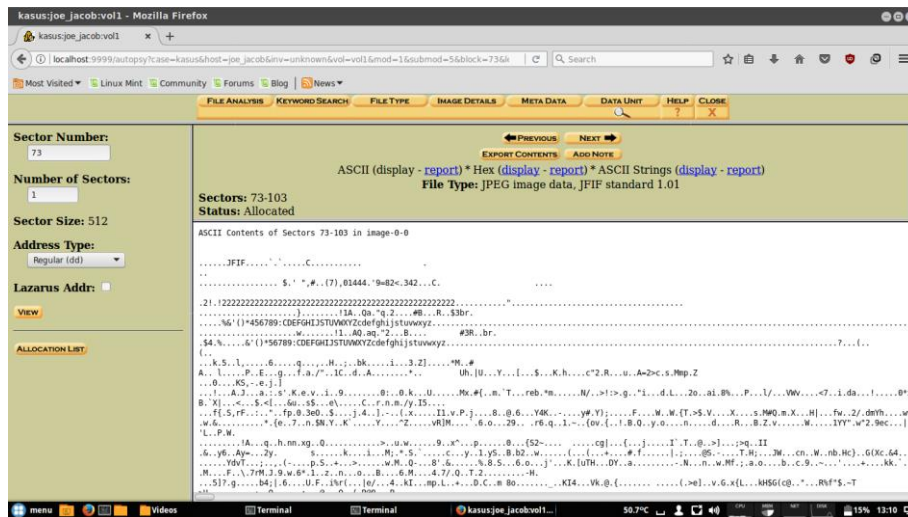


Gambar 8.11. Analyze details

Digambar bawah tersebut tampilan setelah kita memilih image detail , terdapat 2 FAT Contents. Kita membuka konten pertama 73-103



Gambar 8.12. Image Details



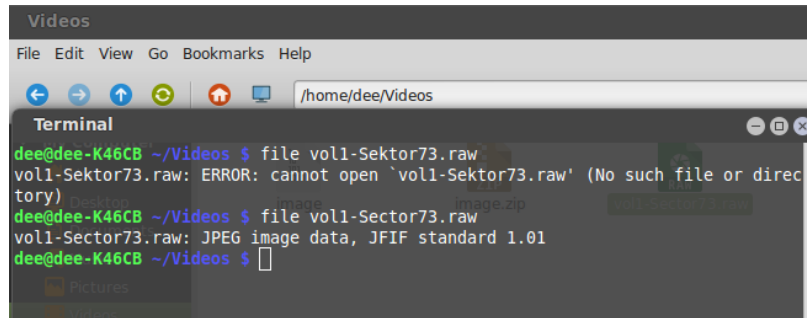
Gambar 8.13. Data Unit Image pertama

Dari gambar diatas konten pertama dgn sector 73-103 terdapat JFIF salah satunya adalah format dari image pertama. Format JFIF adalah format dari gambar jpg/jpeg, bisa saya buktikan pada gambar 8.14, informasi tersebut saya dapatkan dari wikipedia.

File Format	Description	Signature
bpg	Better Portable Graphics format ^[7]	0 BPGü 42 50 47 FB
jpg	JPEG raw or in the JFIF or Exif file format	FF D8 FF E0 nn 4A 46 49 46 80 01
jpeg		FF D8 FF E1 nn x 1F.. 69 66 00 00
ibm	IFF Interleaved Bitmap image	46 4F 52 4D nn nn nn nn 49 4C 42 4D
ibm		FORM... ILBM
iff		
Bsvx	IFF 8-BIT Sampled Voice	46 4F 52 4D nn nn nn nn 38 53 56 58
Bsv		FORM... BSVX
svx		
spd		

Gambar 8.14. Format JFIF

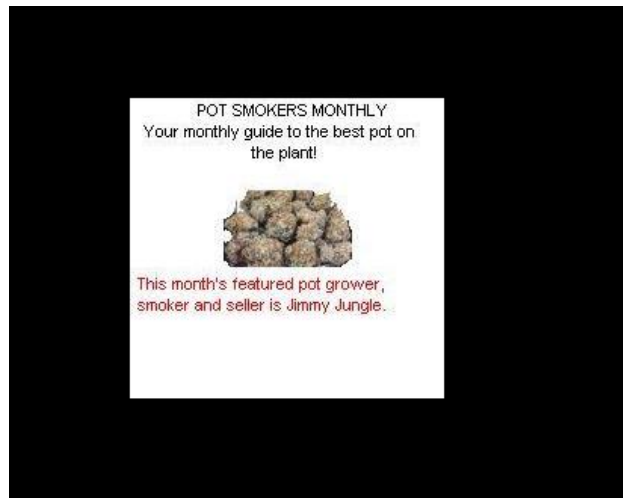
9. Masuk lagi ke terminal



```
deedee-K46CB ~/Videos $ file voll-Sektor73.raw
voll-Sektor73.raw: ERROR: cannot open `voll-Sektor73.raw' (No such file or directory)
deedee-K46CB ~/Videos $ file voll-Sektor73.raw
voll-Sektor73.raw: JPEG image data, JFIF standard 1.01
deedee-K46CB ~/Videos $
```

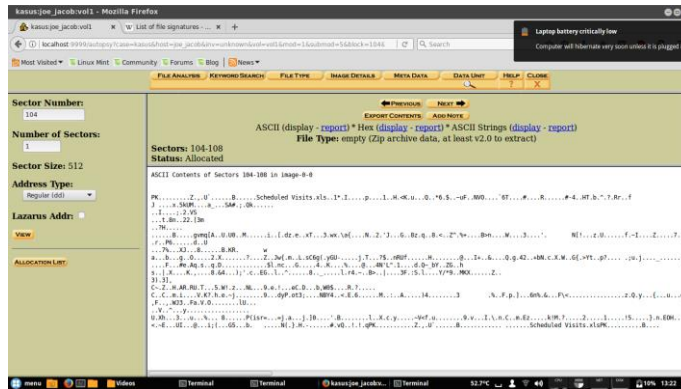
Gambar 9.1 Perintah Membuka Image

Melakukan perintah diatas tidak perlu kita masuk ke root. Setelah melakukan perintah di gambar 9, akan muncul gambar 9.2.

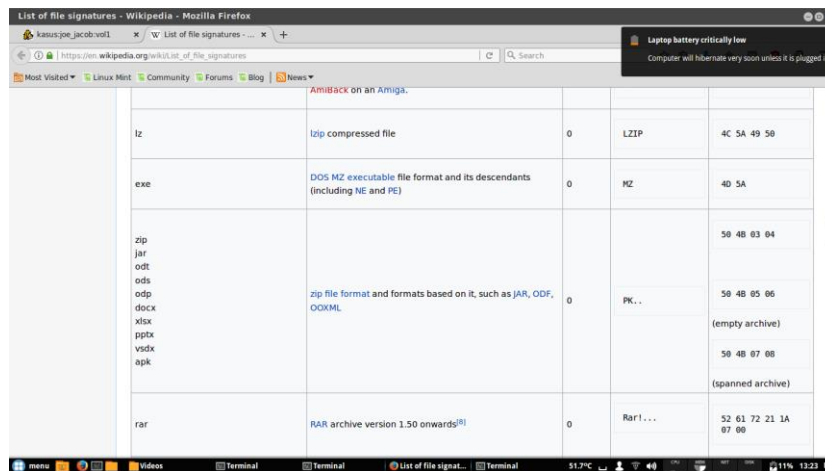


Gambar 9.2. Image Sector 73-103

10. Melakukan sector selanjutnya, yaitu sector yang kedua 104-108. Dimana isi sector 2 terdapat kata PK pada gambar 10.1 dan saya mencari tahu nya lagi dari wikipedia pada gambar 10.2

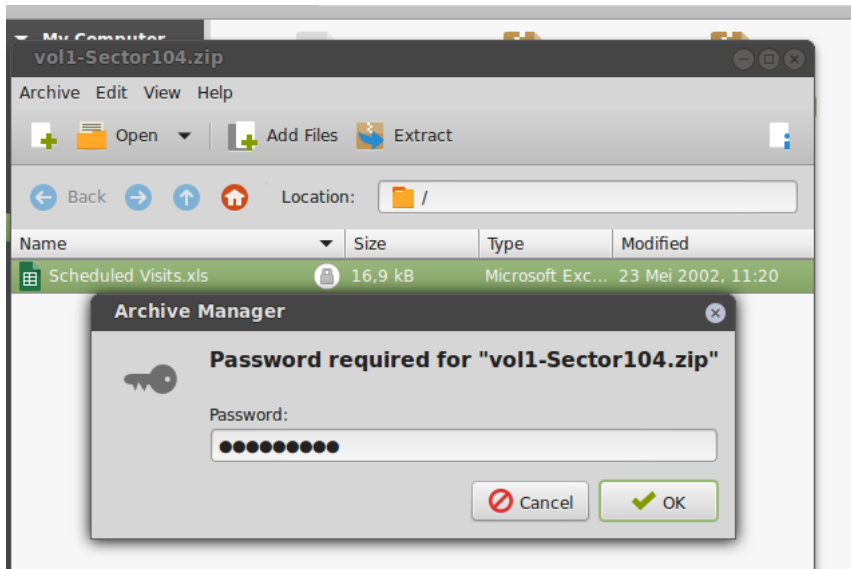


Gambar 10.1 data unit image kedua



Gambar 10.2 Wikedpedia

Setelah mencari informasi tentang format Pk didapatkan hasil bahwa format PK sama halnya dengan format ZIP. Seperti yang ditampilkan pada gambar 25.



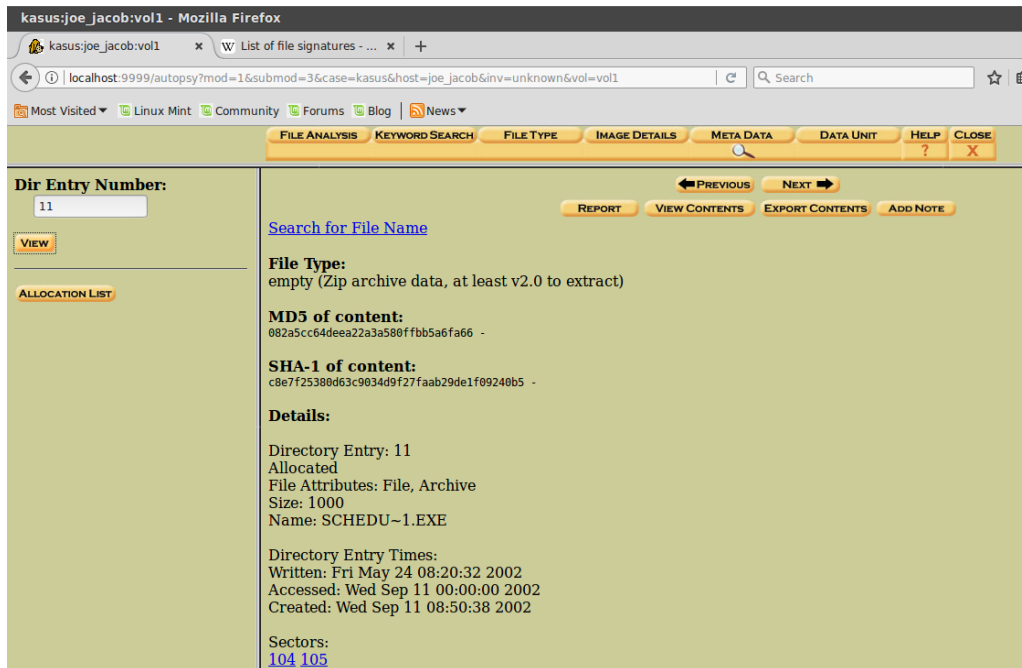
Gambar 10.5 buka password

Digambar 10.6 dibawah ini adalah isi informasi dari rentetan kegiatan untuk mempermudah melacak informasi.

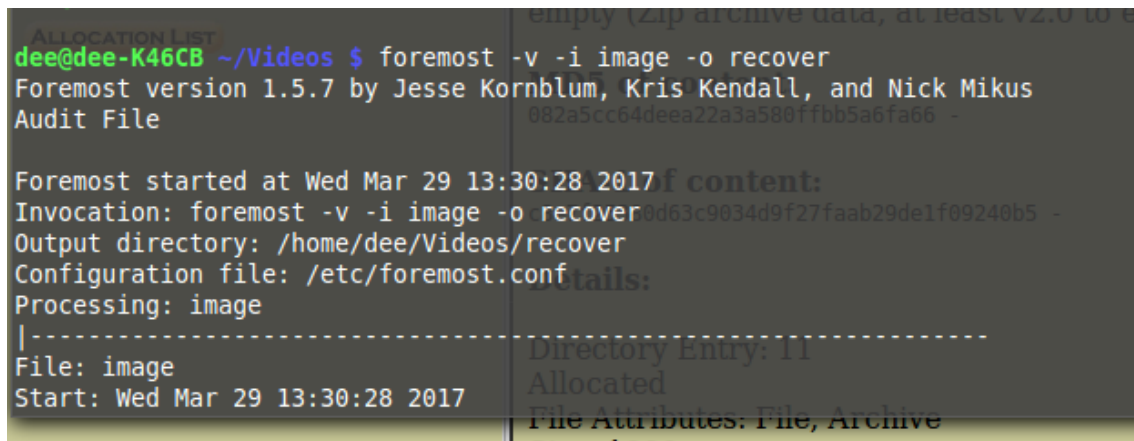
 A screenshot of a spreadsheet application window titled 'Scheduled Visits.xls - LibreOffice Calc'. The spreadsheet displays a schedule of visits to high schools from April to May 2002. The columns are labeled 'Month', 'DAY', and 'HIGH SCHOOLS'. The data is organized by month and day, listing specific high schools for each day.

Month	DAY	HIGH SCHOOLS
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leitch High School (C)
	Thursday (4)	Strand High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leitch High School (C)
	Friday (5)	Strand High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leitch High School (C)
	Monday (1)	Strand High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leitch High School (C)
	Tuesday (2)	Strand High School (D)
May	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leitch High School (C)

Gambar 10.6 File scheduled



Gambar 10.7 meta data



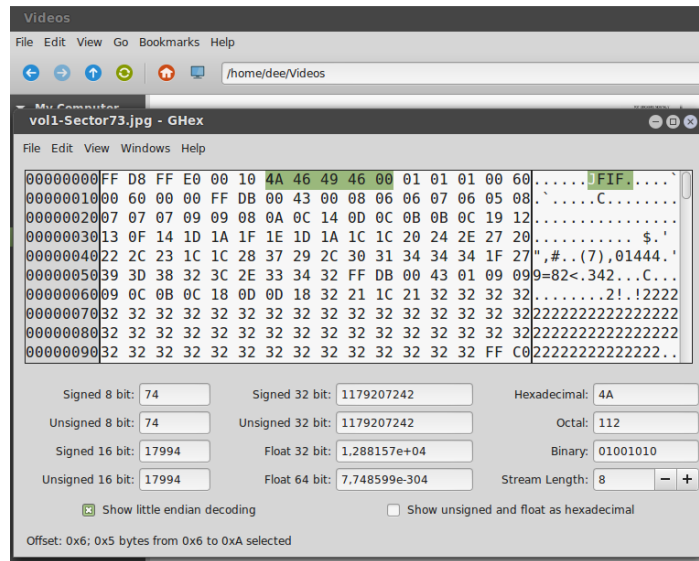
Gambar 10.8 perintah foremost

Perintah diatas adalah fungsinya untuk mengekstrak data yang tertimpa atau tertumpuk.



Gambar 10.9 file doc

Isi dari file doc adalah surat dari Joe untuk Jimmy.



Gambar 10.10 Konversi Ghex

Gambar 10.10 adalah langkah terakhir melakukan praktikum ini, langkah ini merupakan konveksi huruf ke binner menggunakan tools GHex.

Pertanyaan :

1. Siapa pemasok narkoba Joe Jacob dan apa alamatnya?
2. Data penting apa yang terdapat di file coverage.jpg dan mengapa data tersebut penting?
3. Nama sekolah selain smith hill yang sering menjadi tempat transaksi joe Jacob?
4. Untuk setiap file proses apa yang diambil oleh tersangka untuk mengelabui orang lain?
5. Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file?

Jawab :

1. - Pemasok adalah Jimmy Jungle
- alamat tinggalnya di 626 Jungle Ave Apt 2
2. file Scheduled Visit.xls tetapi dalam hal ini file tersebut dapat diakses dengan password. Kenapa didalam file tersebut terdapat data tentang nama – nama sekolah yang menjadi tempat transaksi joe jacob
3. nama sekolah
 - Key High School
 - Leetch High School
 - Birard High School
 - Richter High School
 - Hull High School
4. Mereka mengelabui dengan cara mengganti format zip menjadi raw dari file vollsector73 dan sector104
5. Dalam hal ini proses yang digunakan penyidik adalah dengan mencari informasi informasi penting menggunakan beberapa tools yaitu Autopsy, foremost dan GHex