**Tugas Mata Kuliah**

# KEAMANAN JARINGAN KOMPUTER


Nama : Faris Abdul Aziz

Nim : 09011181320020


**Jurusan Sistem Komputer**

**Fakultas Ilmu Komputer Universitas Sriwijaya**

**2017**

# TUGAS 6

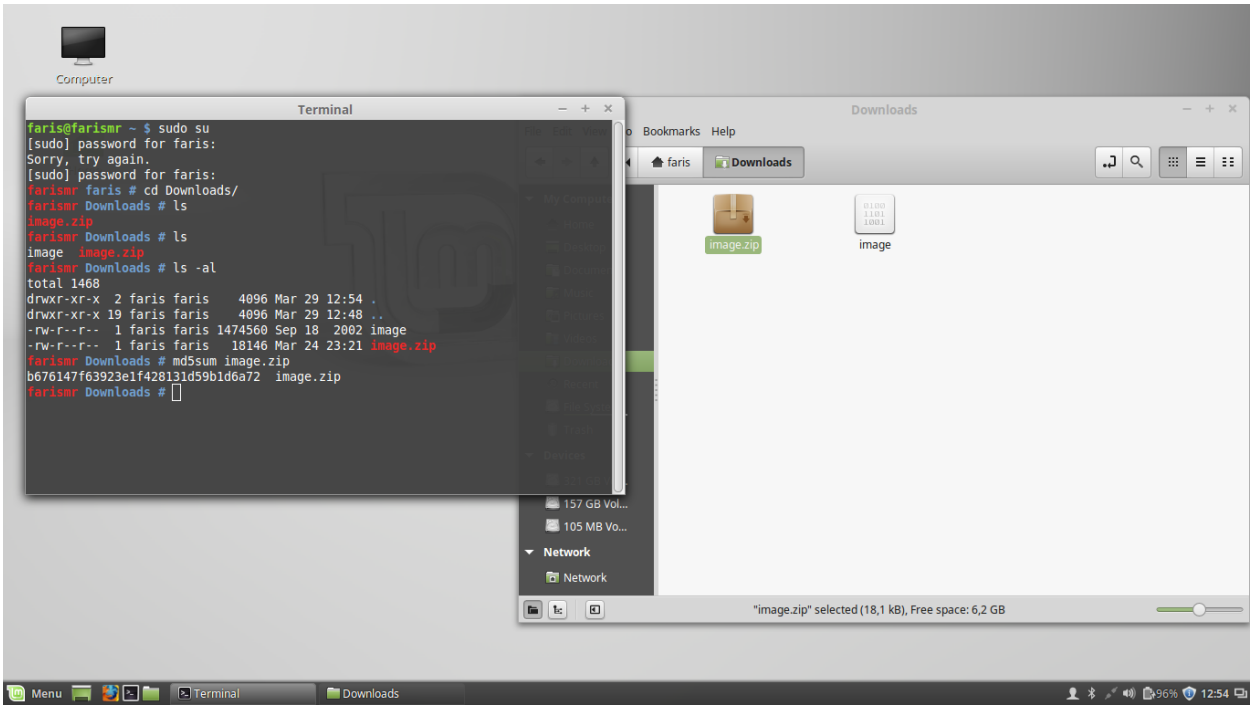
## KOMPUTER FORENSIK

Komputer Forensik adalah salah satu cabang ilmu dalam forensic yang berkaitan dengan bukti illegal yang ditemui pada computer dan media penyimpanan digital untuk dapat disajikan sebagai barang bukti yang sah dipengadilan nanti.

Tools yang digunakan adalah:

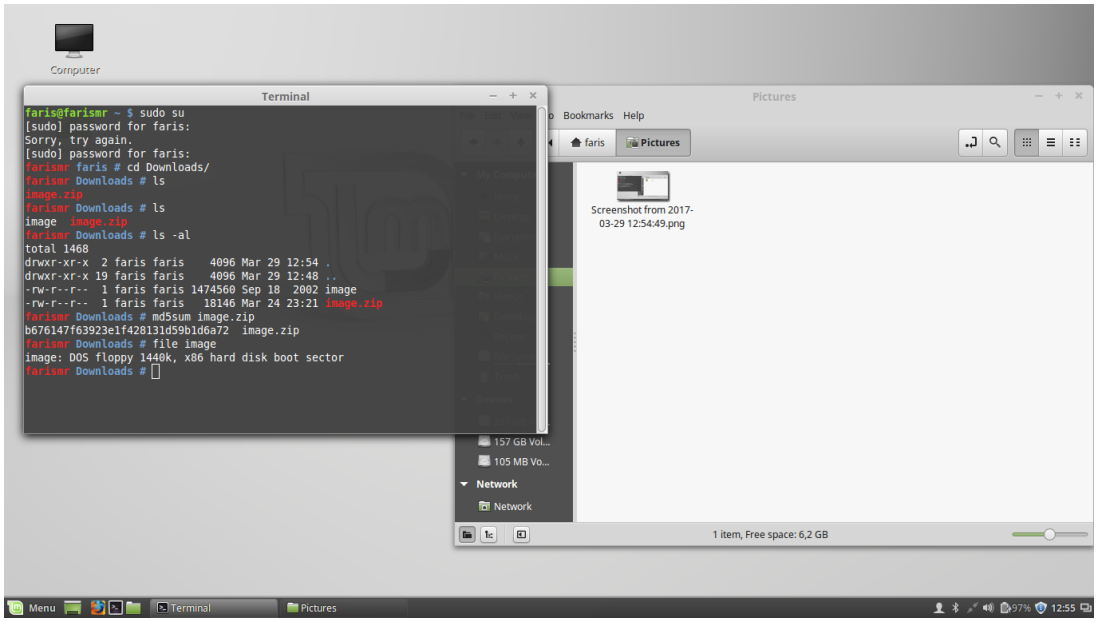
1. Autopsy
2. Foremost
3. Strings
4. GHex

Tahap pertama yang harus dilakukan ada mengekstrak file image.zip, setelah dilakukan ekstrak akan terdapat file image. Setelah itu masukkan perintah md5sum image.zip, md5sum sendiri digunakan untuk mengecek keaslian dari file tersebut. Dapat dilihat pada gambar 1.1 dibawah.



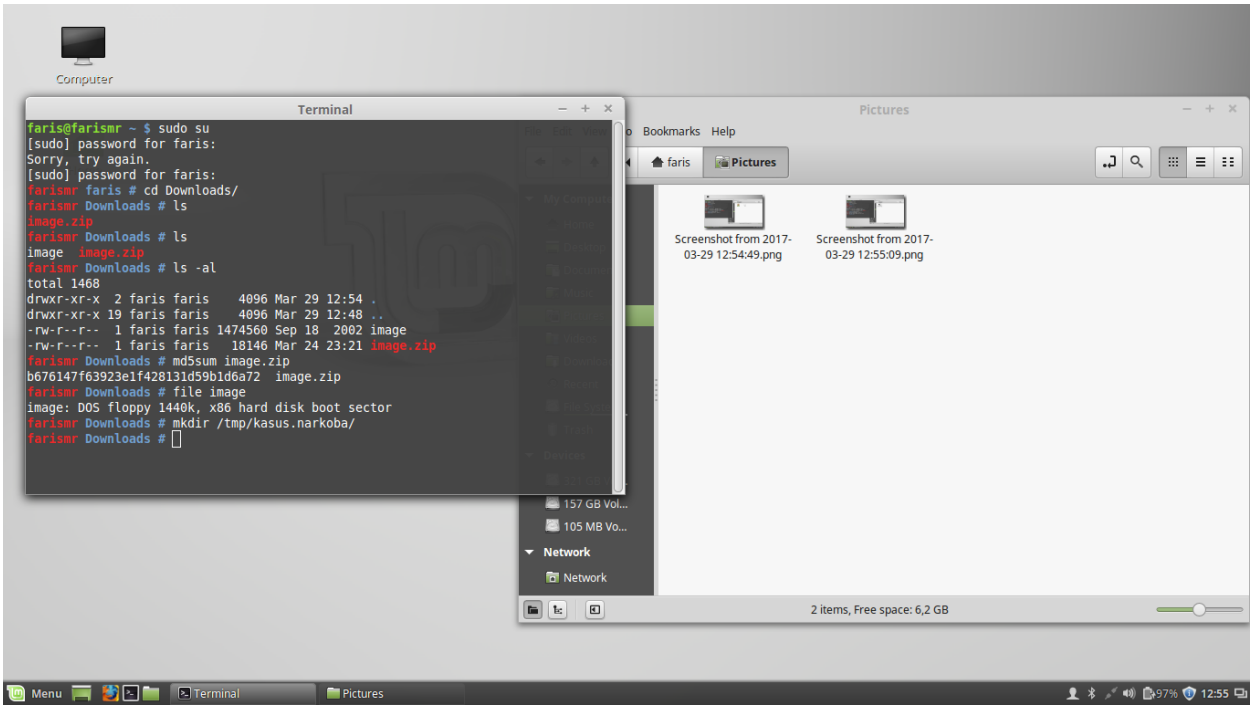

**Gambar 1.1.** Hasil perintah md5sum

Tahap selanjutnya adalah dengan memasukkan perintah file image, dimana file image berfungsi untuk melihat tipe filenya, dapat dilihat pada gambar 1.2 dibawah



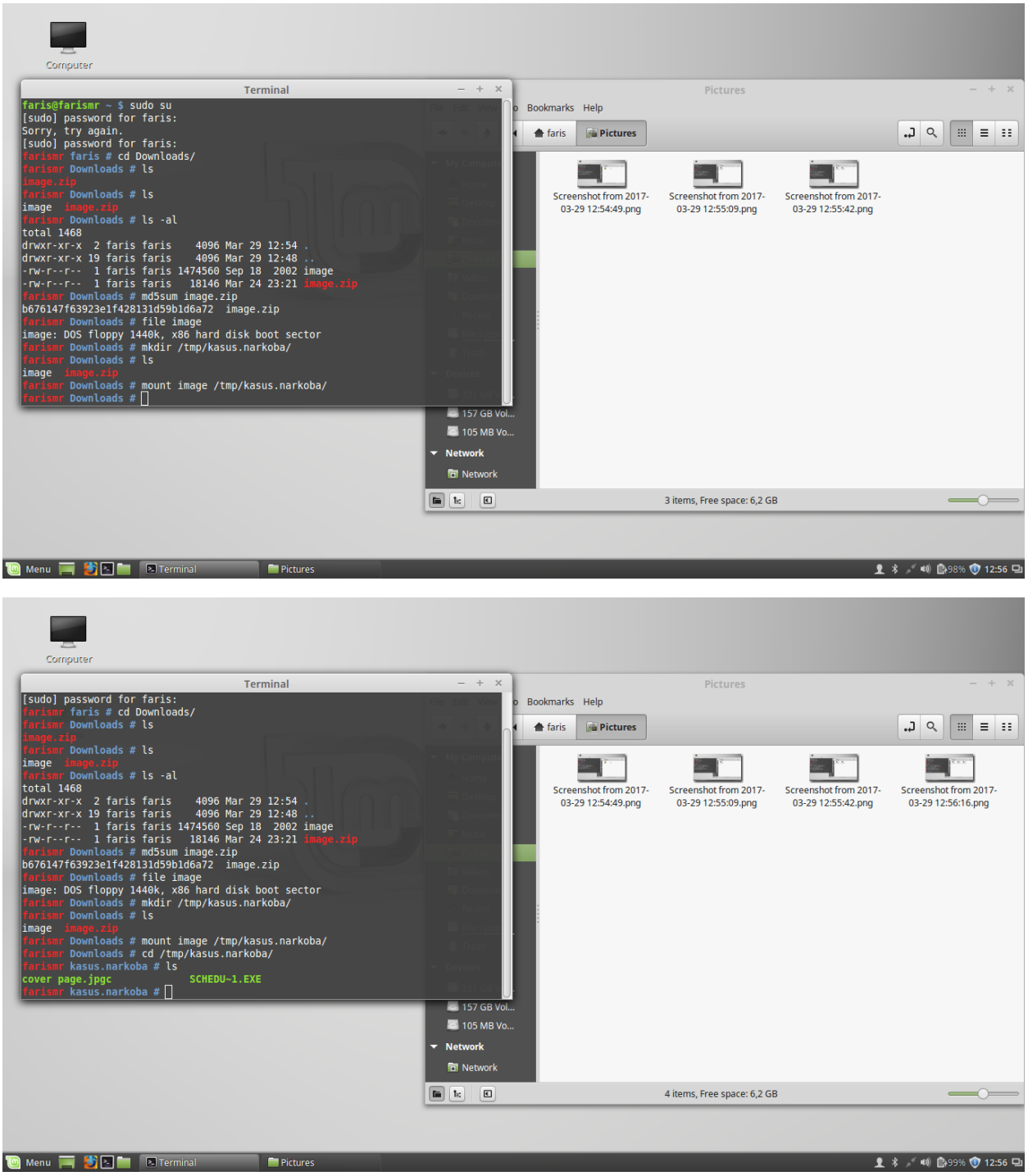

**Gambar 1.2.** File Image

Tahap selanjutnya membuat directory baru dengan nama kasus.narkoba, dapat dilihat pada gambar 1.3 dibawah.



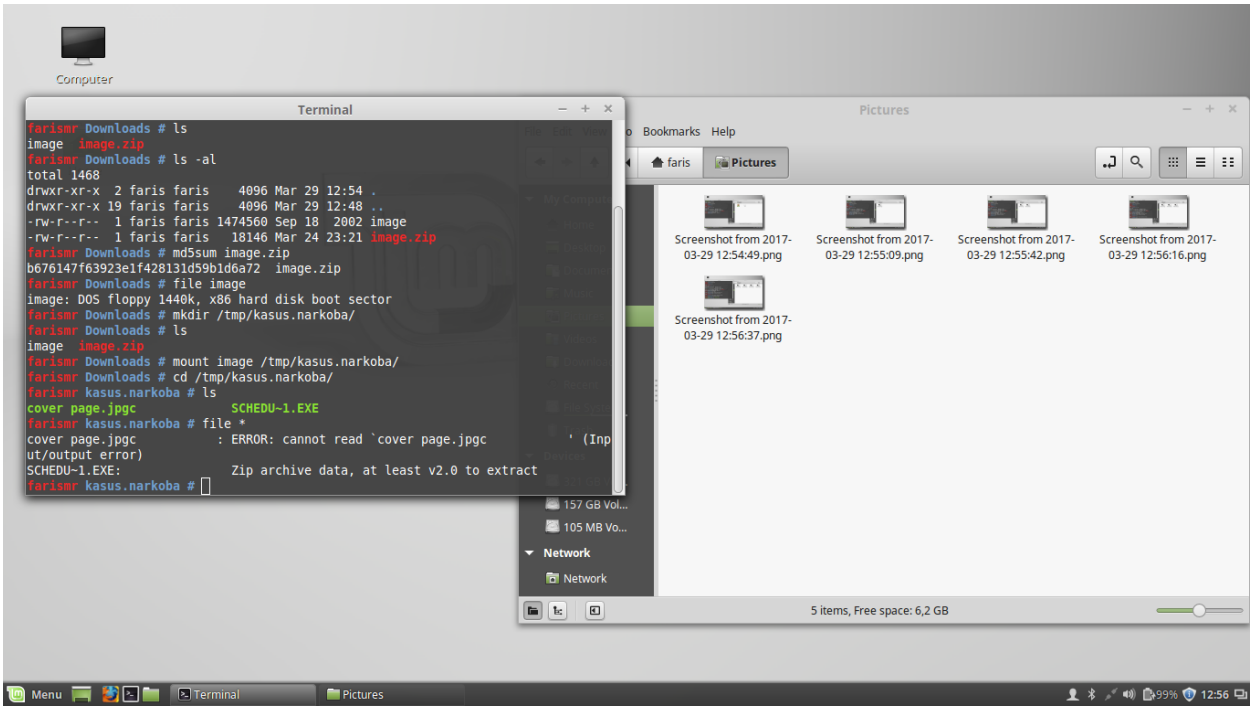

**Gambar 1.3.** Directory baru

Selanjutnya masukkan perintah mount image /tmp/kasus.narkoba/, yang dimana file image akan diekstrak pada directory kasus.narkoba, dan masuk ke dalam file kasus.narkoba dan dengan perintah ls kita dapat melihat file yang telah diekstrak. Dapat dilihat pada gambar 1.4 dibawah.



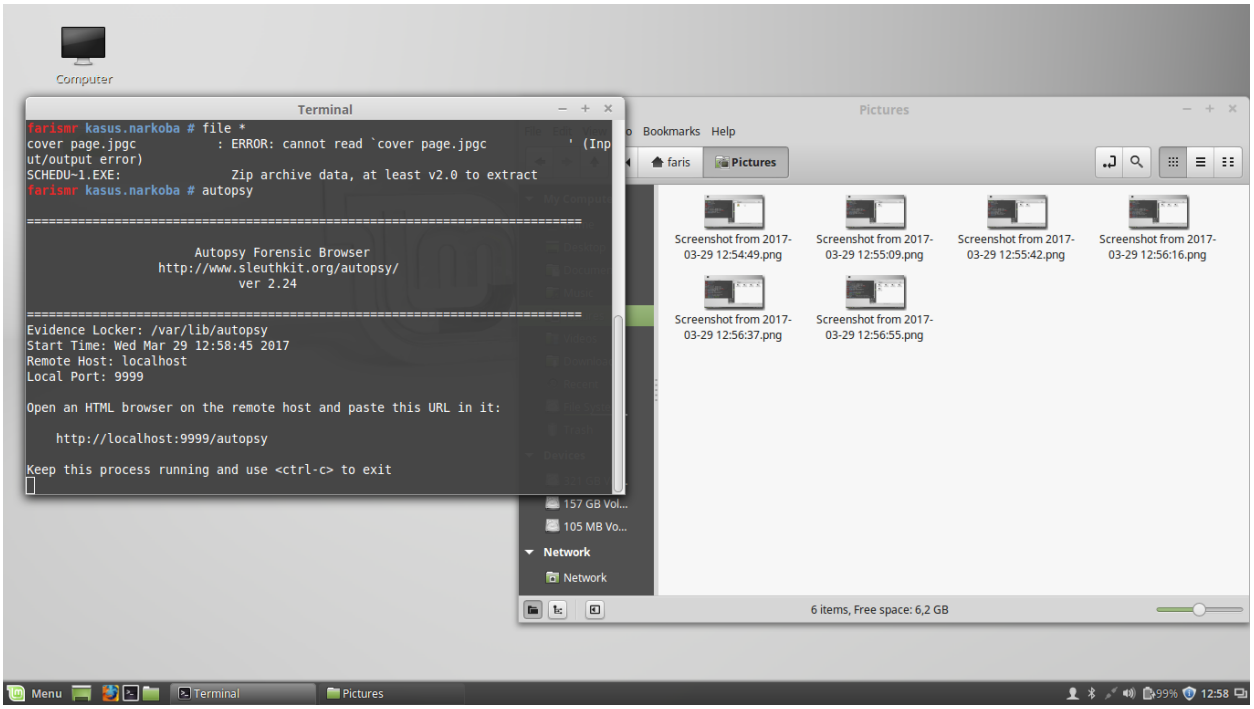

**Gambar 1.4.** Ekstrak file image

Selanjutnya masukkan perintah file * pada directory kasus.narkoba, yang dimana berfungsi sebagai perintah melihat tipe file secara keseluruhannya. Dapat dilihat pada gambar 1.5 dibawah.



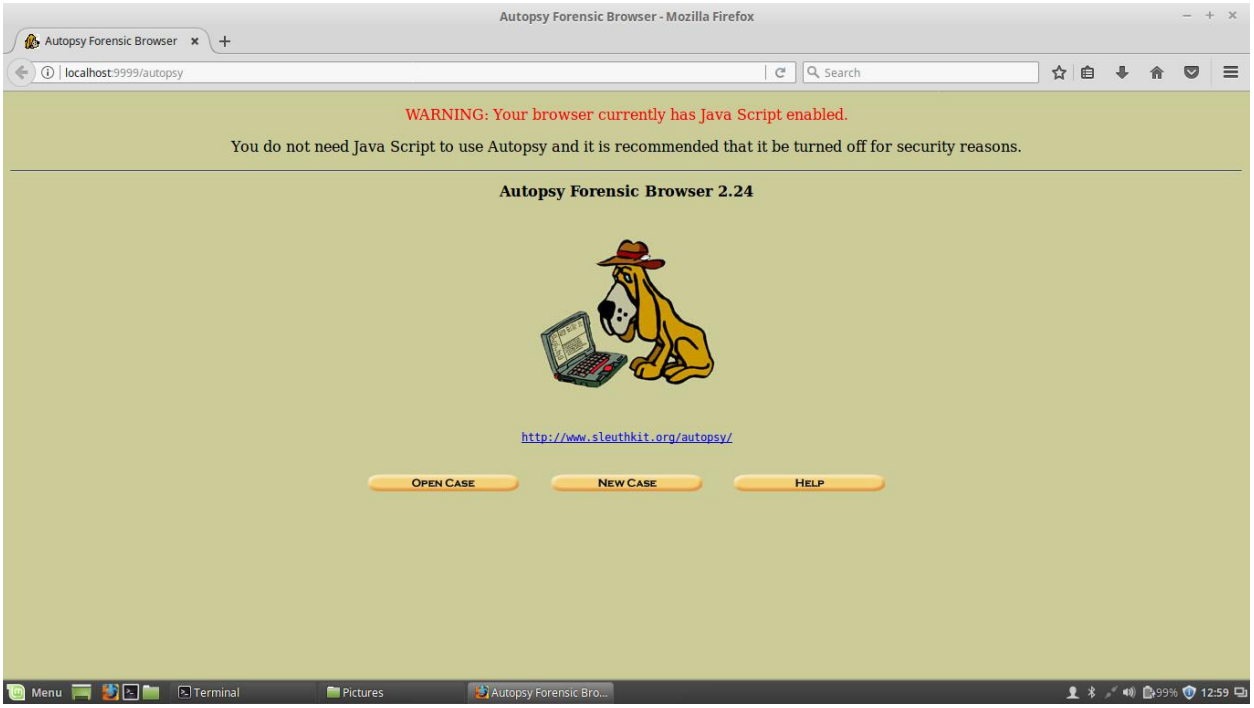

**Gambar 1.5.** File *

Tahap selanjutnya adalah memasukkan perintah autopsy, dan akan keluar seperti pada gambar 1.6.



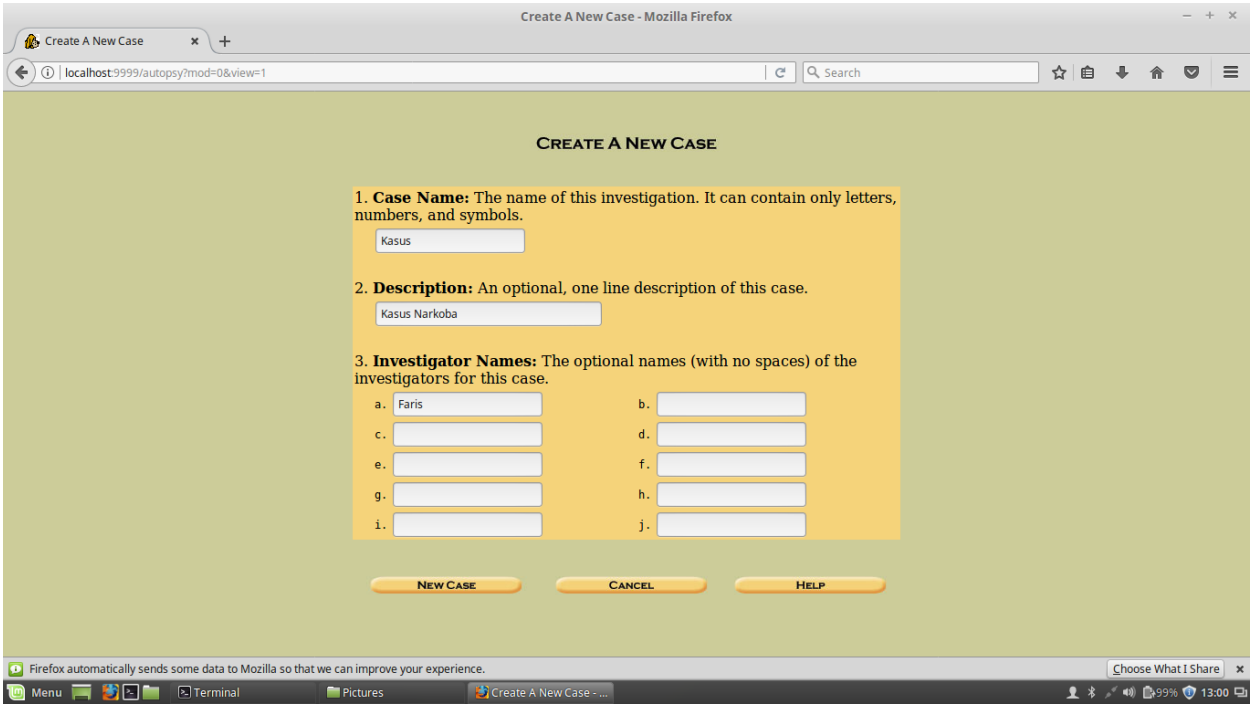

**Gambar 1.6.** Autopsy

Selanjutnya kita buka browser dan masukkan localhost yang didapat dari autopsy tadi, dan akan muncul interface seperti pada gambar 1.7 dibawah, lalu pilih new case.



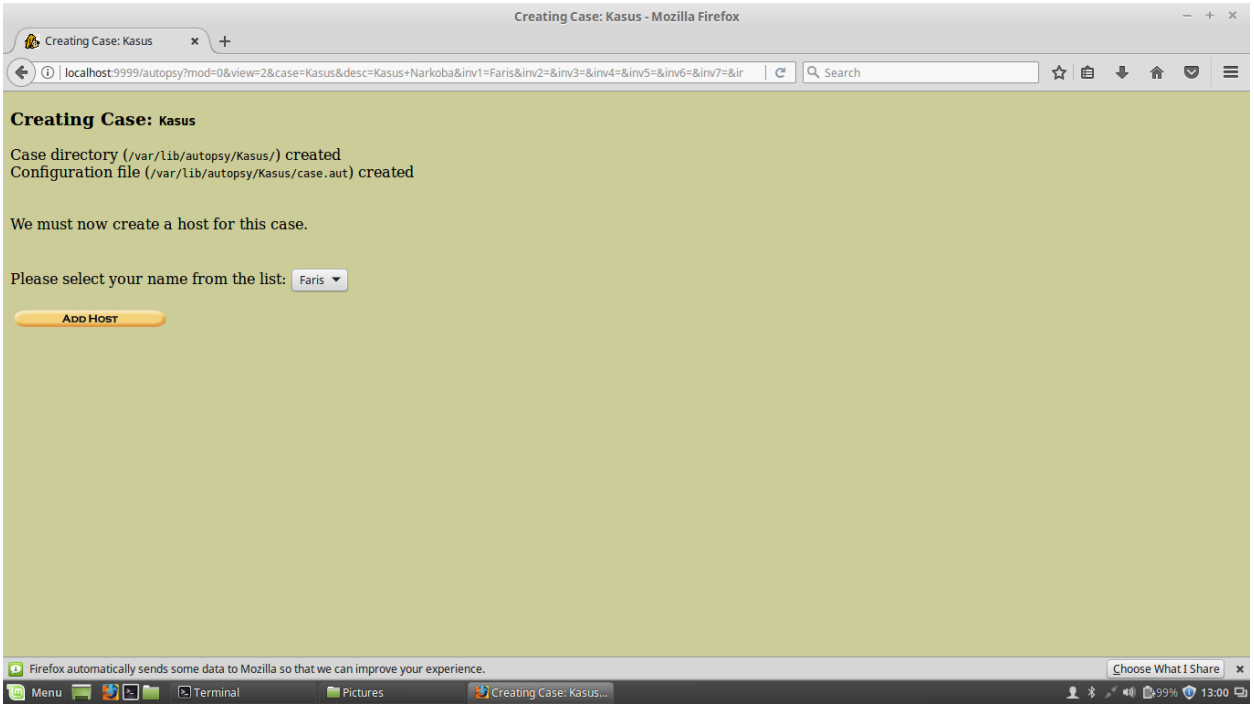

**Gambar 1.7.** Interface localhost autopsy

Selanjutnya masukkan data pada form create new case, dapat dilihat pada gambar 1.8 dibawah.



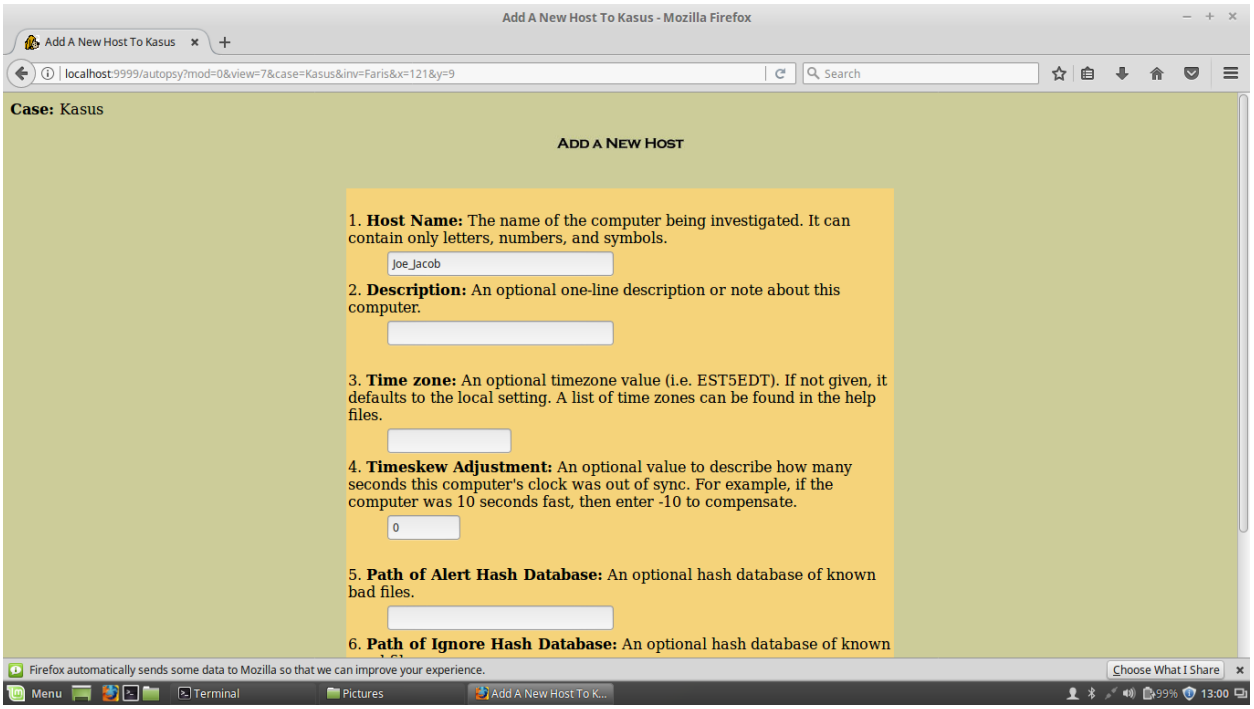

**Gambar 1.8.** Form Create New Case

Selanjutnya setelah membuat new case, akan muncul tampilan seperti gambar 1.9. lalu klik add host.



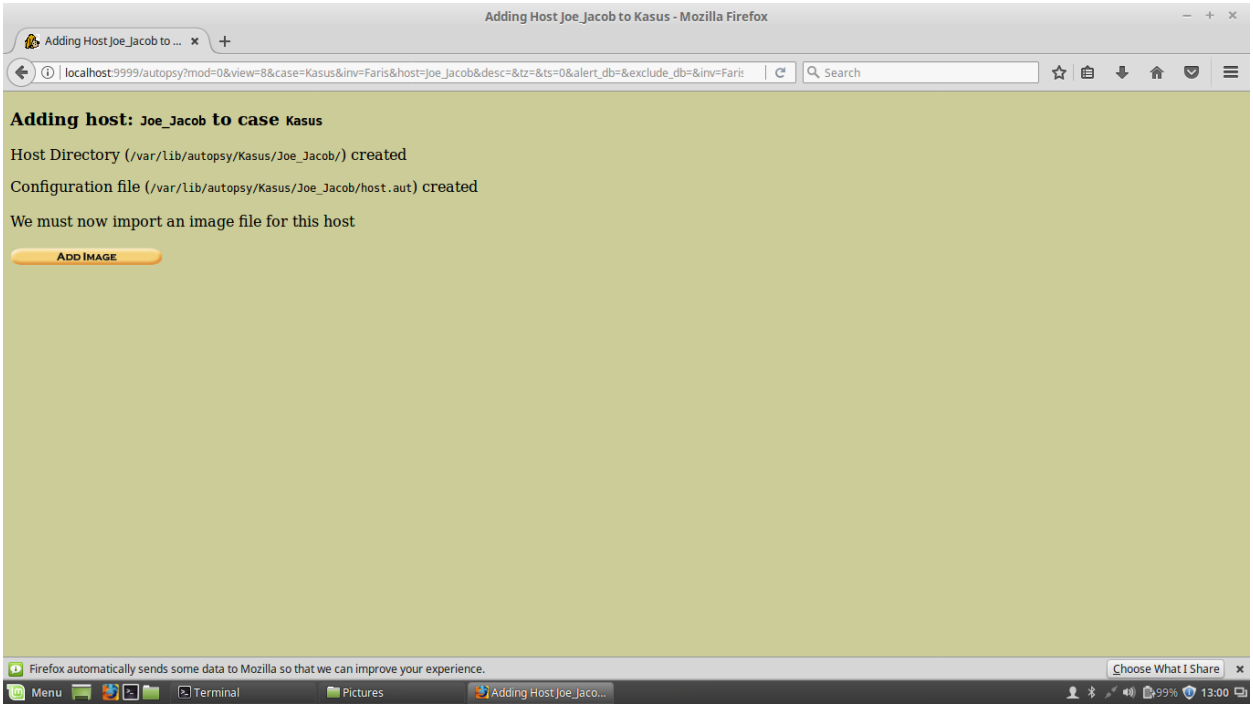

**Gambar 1.9** Add host

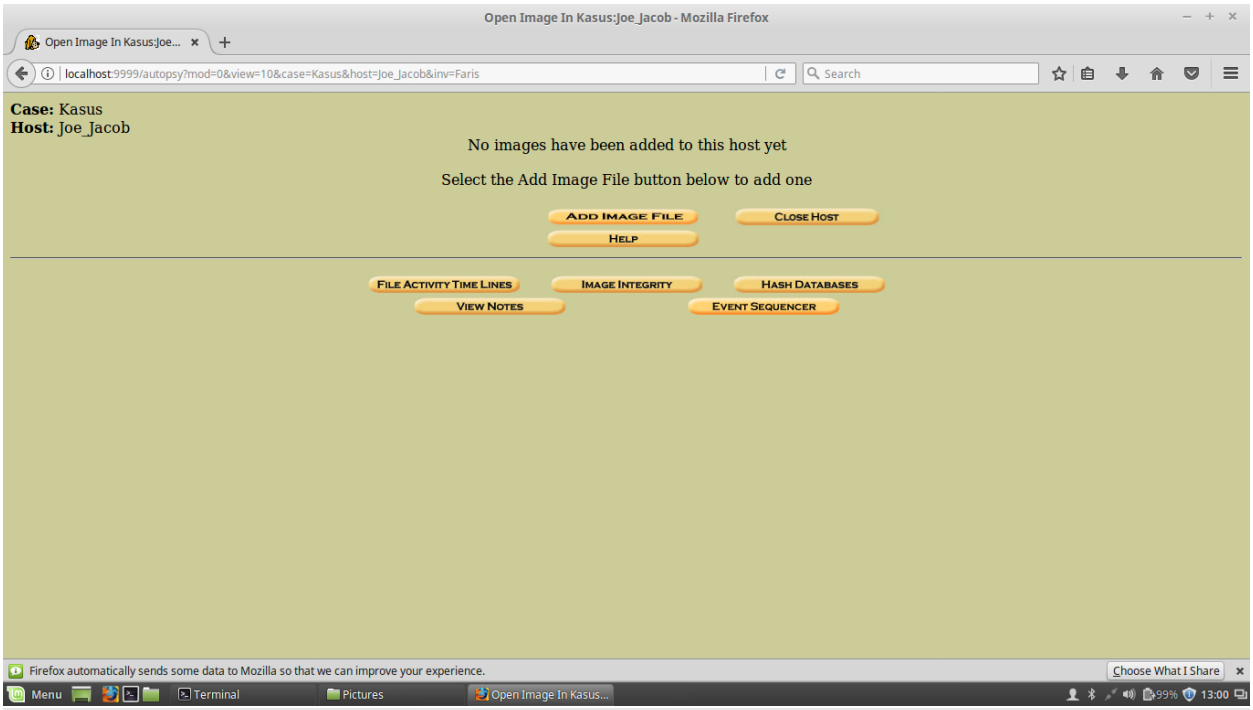
Setelah itu lakukan penambahan host ada case tadi, dan isikan hostname pada kolom form host name, dapat dilihat pada gambar 1.10 dibawah.

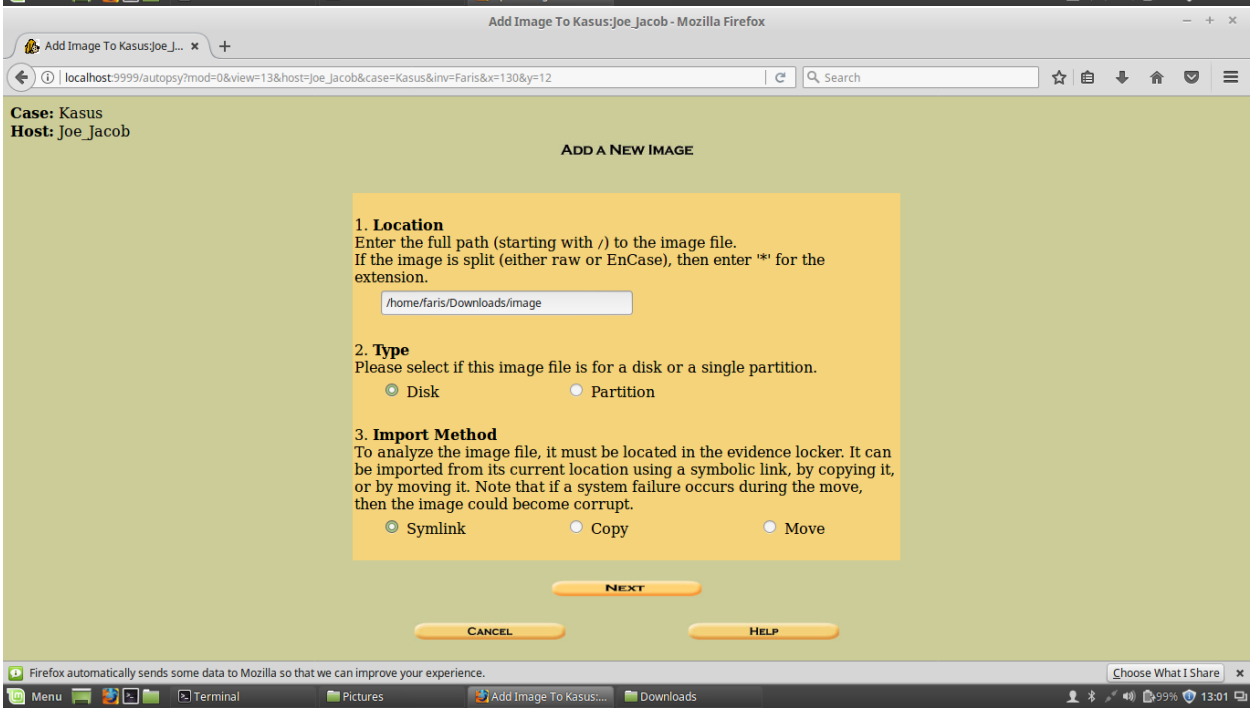


**Gambar 1.10.** Form Add New Host

Lalu klik add image untuk menbahkan image pada case tersebut. Lalu masukkan file image yang telah diekstrak sebelumnya kedalam kolom location. Lalu ganti dengan Volume Image dan tekan ok Dapat dilihat pada gambar 1.11 dibawah.

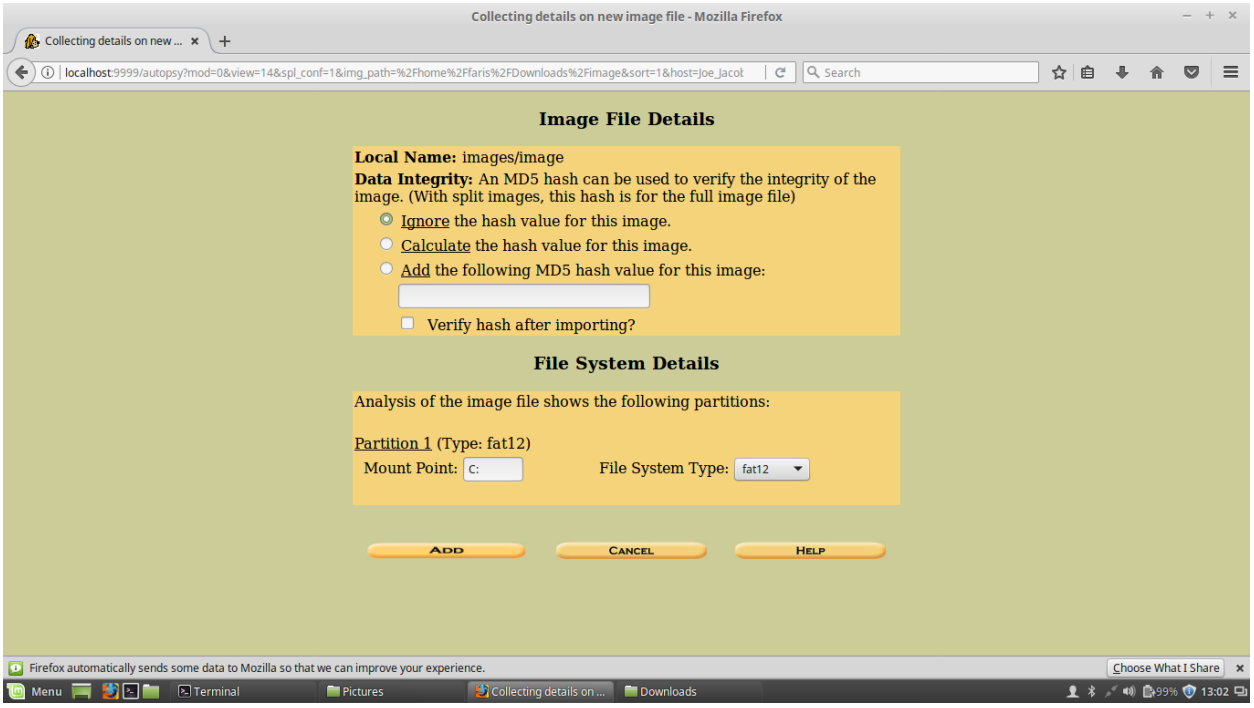



Open Image In Kasus:Joe_Jacob - Mozilla Firefox
Open Image In Kasus:Joe...
localhost:9999/autopsy?mod=0&view=10&case=Kasus&host=Joe_Jacob&inv=Faris
Search
Case: Kasus
Host: Joe_Jacob
No images have been added to this host yet
Select the Add Image File button below to add one
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Menu
Terminal
Pictures
Open Image In Kasus...
13:00


Add Image To Kasus:Joe_Jacob - Mozilla Firefox
Add Image To Kasus:Joe_J...
localhost:9999/autopsy?mod=0&view=13&host=Joe_Jacob&case=Kasus&inv=Faris&x=130&y=12
Search
Case: Kasus
Host: Joe_Jacob
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.
/home/faris/Downloads/image
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
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Menu
Terminal
Pictures
Add Image To Kasus:...
Downloads
13:01

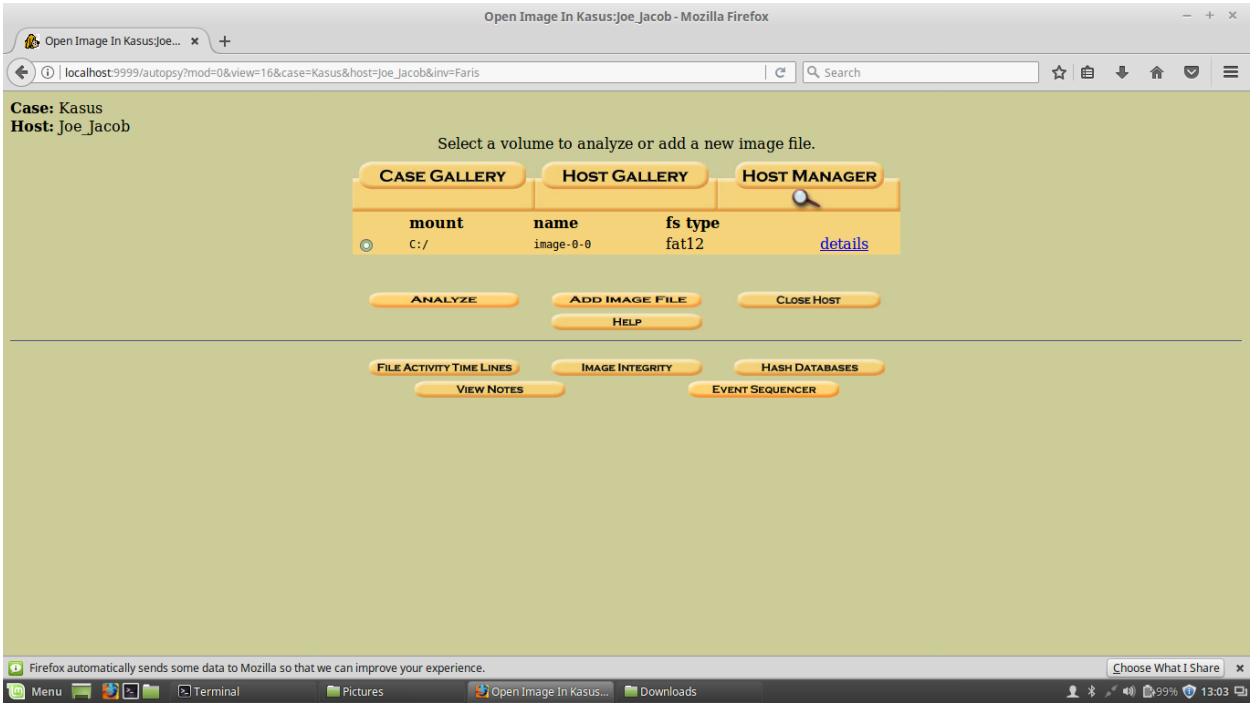

**Gambar 1.11.** Pengisian image

Seelah itu pilih opsi ignore the hash value for this image, lalu pilih add. Dan setelah itu klik lagi pilihan add. Dapat dilihat pada gambar 1.12 dibawah.



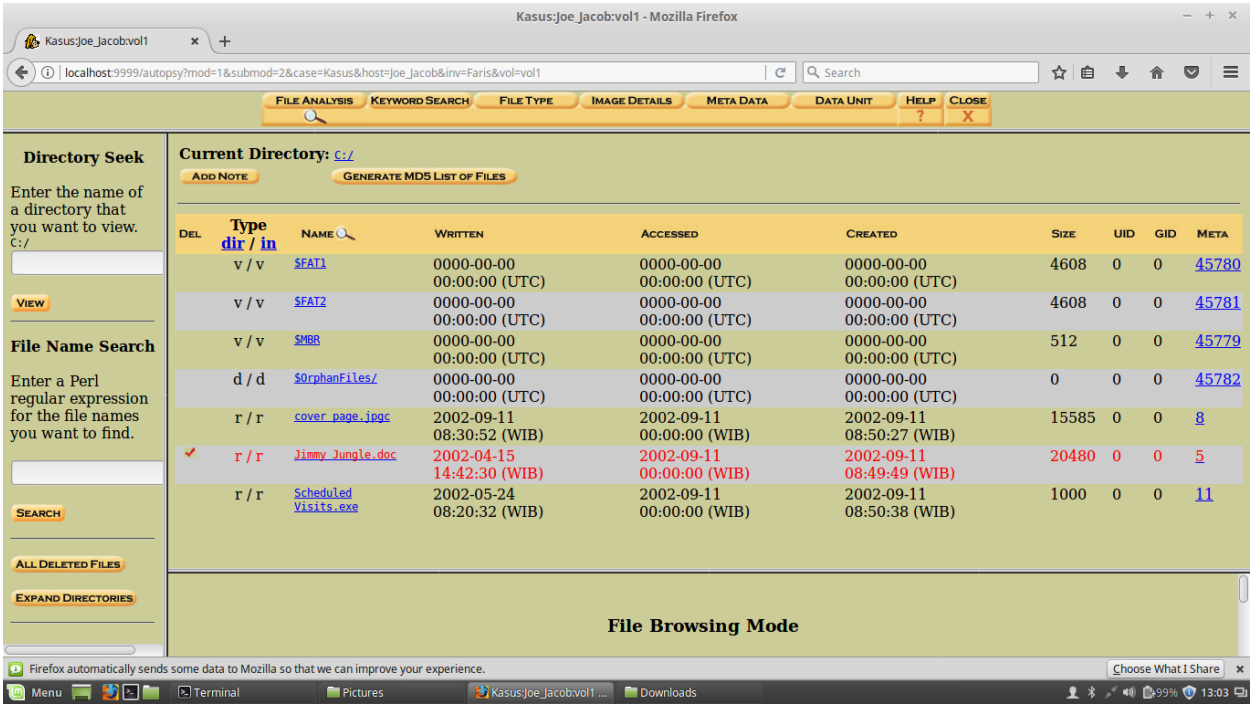

**Gambar 1.12.** Ignore image

Akan muncul tampilan seperti gambar 1.13, lalu klik details untuk melihat info dari case yang telah dibuat tadi, dan dapat dilihat pada gambar 1.13 dibawah.



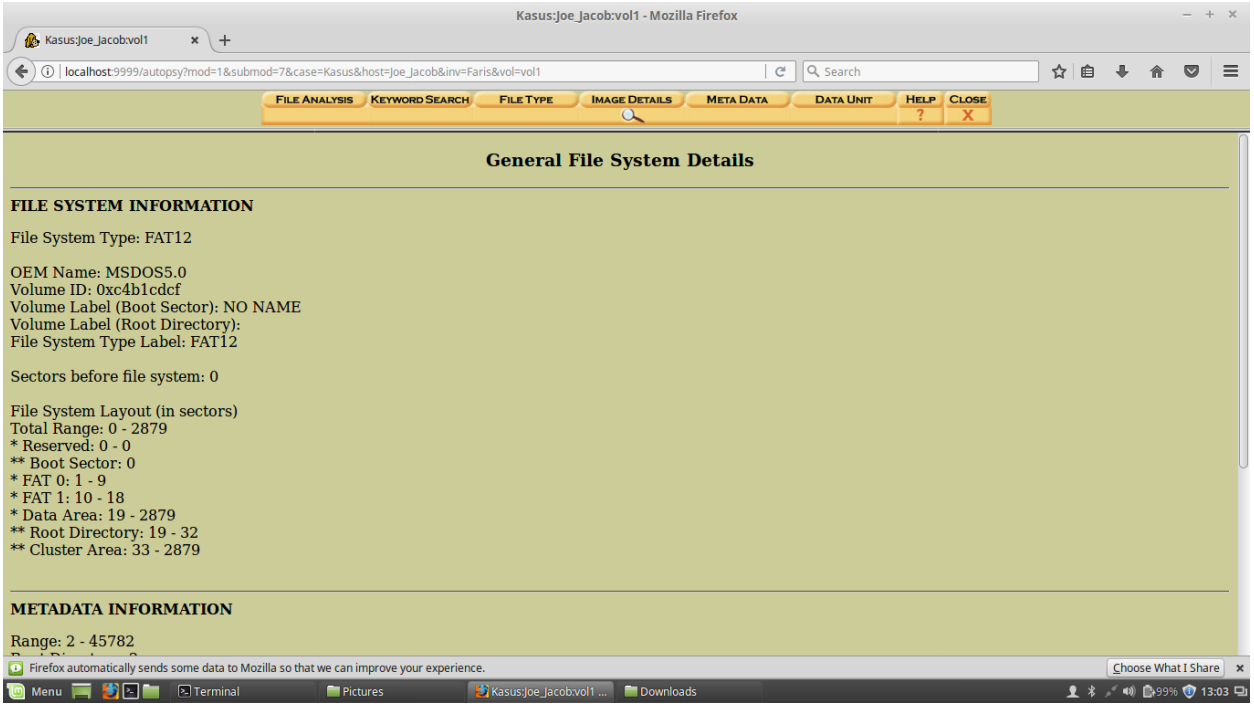

**Gambar 1.13.** Tampilan open image

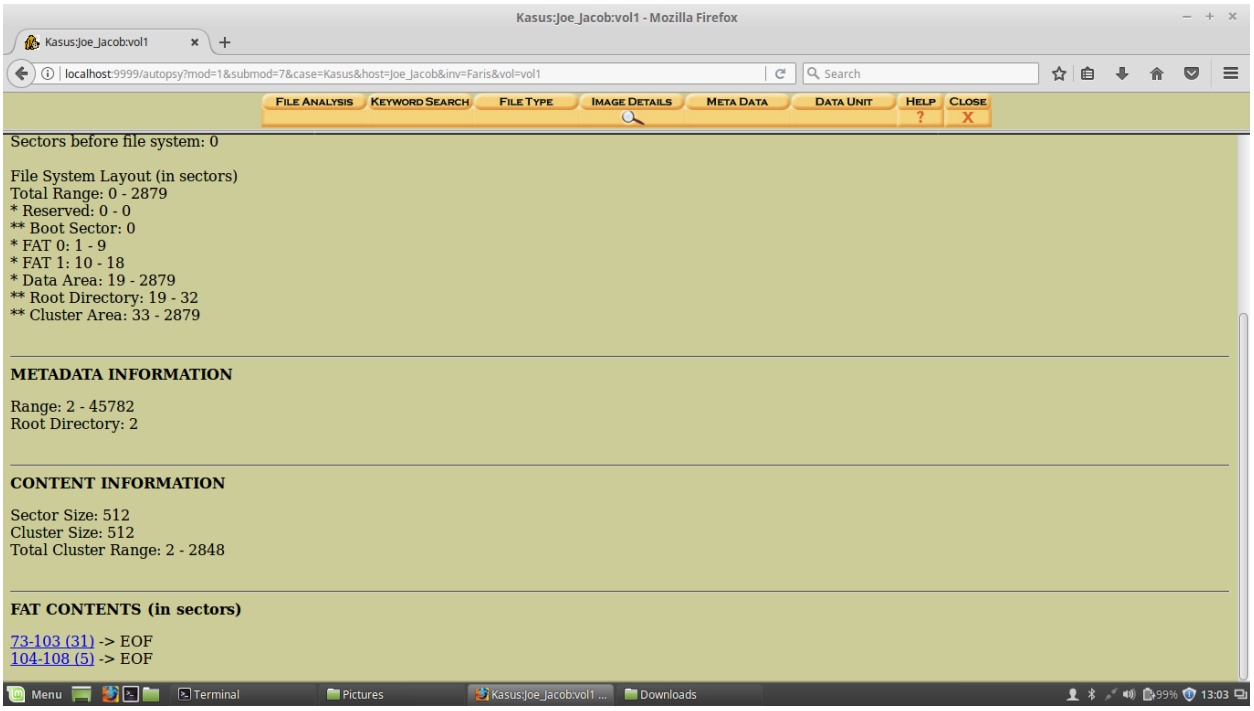
Pada tampilan ini terlihat file yang di analisis oleh autopsy pada case yang telah dibuat tadi, dapat dilihat pada gambar 1.14 dibawah.




**Gambar 1.14.** File Analisis

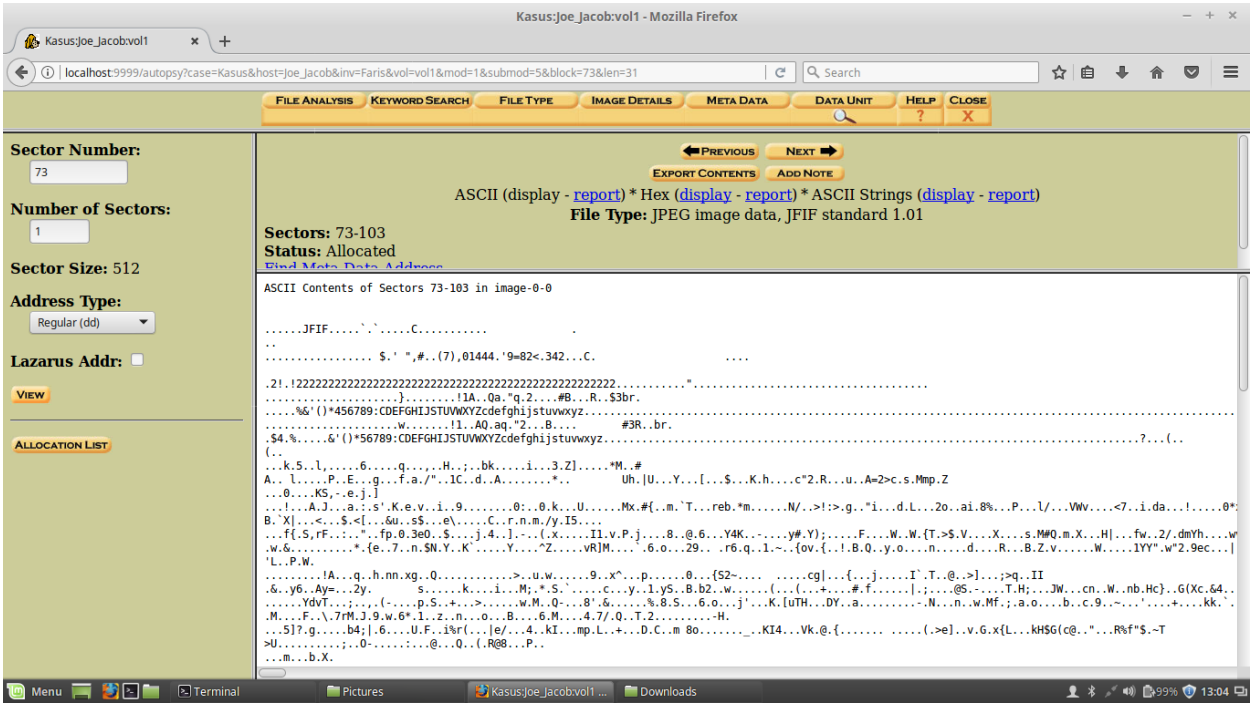
Pada tampilan ini terdapat isi image detail, yang dimana pada halaman ini terlihat seluruh detail dari image pada case yang telah dibuat tadi. Dan pada halaman ini terdapat 2 sektor, yaitu sektor 73 dan 104. Dapat dilihat pada gambar 1.15 dibawah.

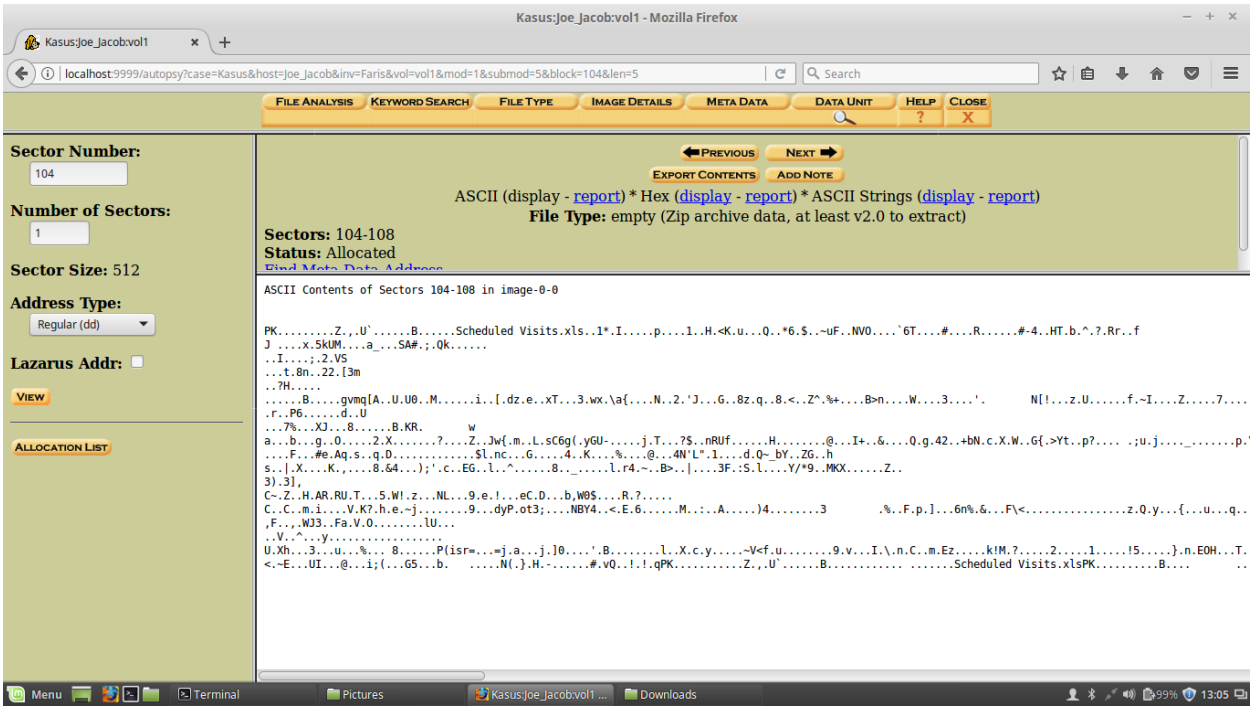





**Gambar 1.15.** Image Details

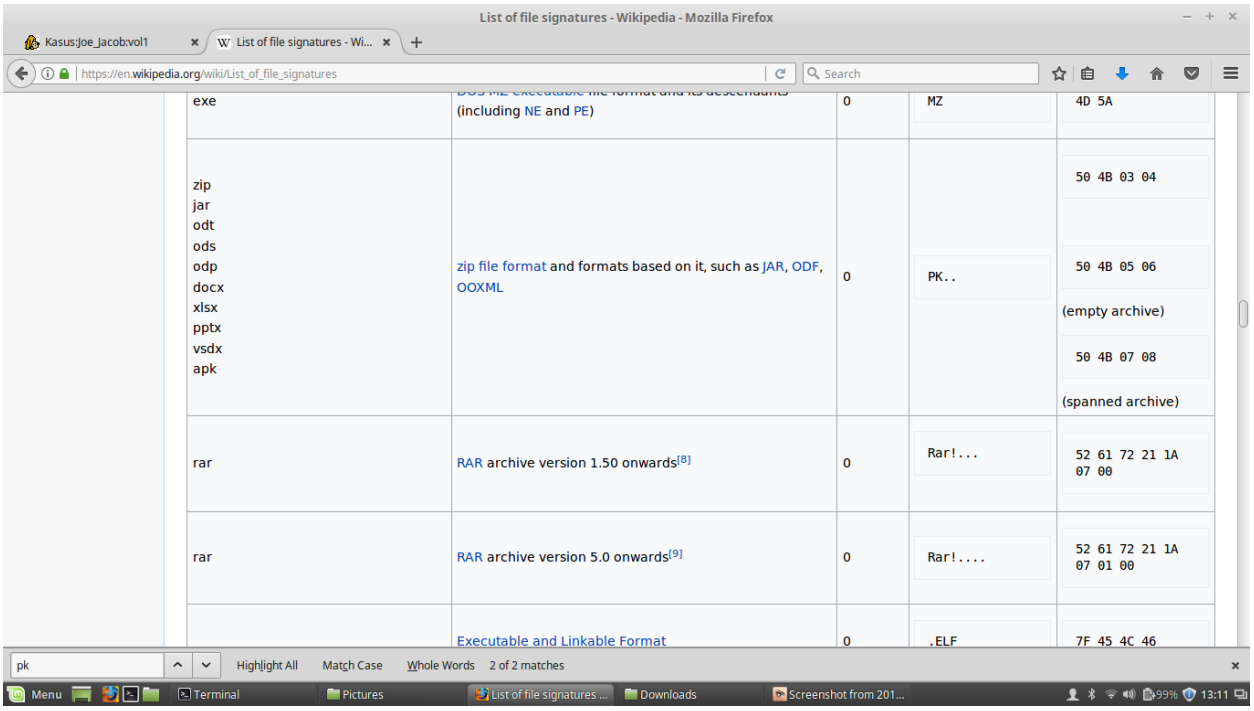
Lalu buka masing-masing sektor yang telah kita dapatkan tadi, makan tampilannya akan seperti pada gambar 1.16 dan dikategorikan sebagai data unit. Dapat dilihat pada gambar 1.16 dibawah.





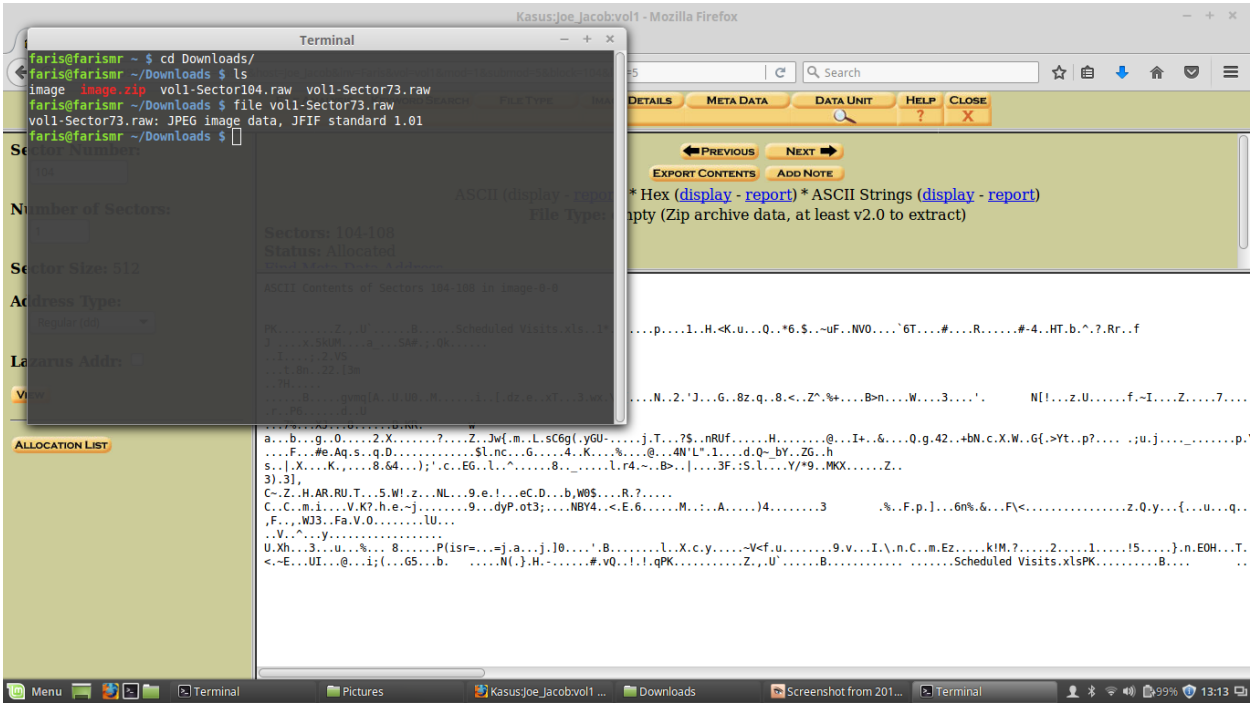

**Gambar 1.16.** Data Unit

Pada sektor pada gambar 1.16 terdapat kode di awal data unit tersebut, yaitu JFIF dan PK yang artinya JFIF itu adalah gambar, dan PK ada file berupa zip. Dapat dilihat pada gambar 1.17 dibawah.



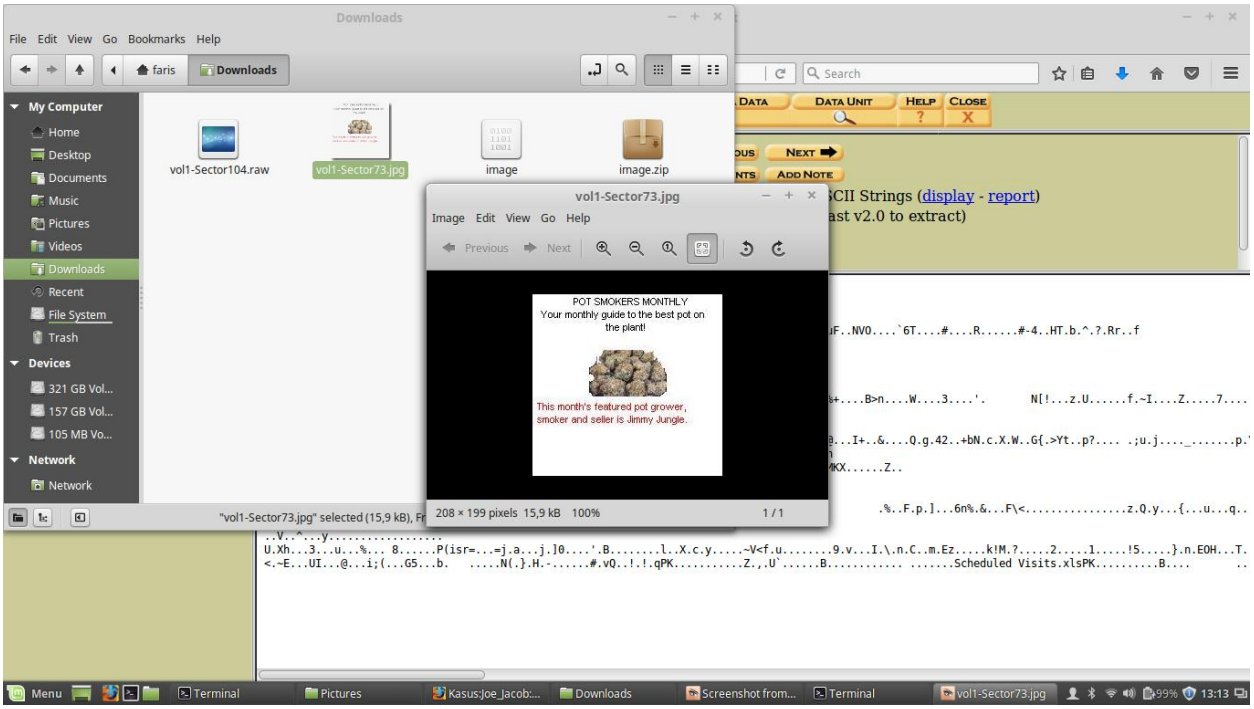

**Gambar 1.17.** Kode pada sektor

Lalu periksa file sektor yang telah didapatkan tadi dengan cara file vol1-sector73.raw, dan akan tampil seperti gambar 1.18 dibawah.



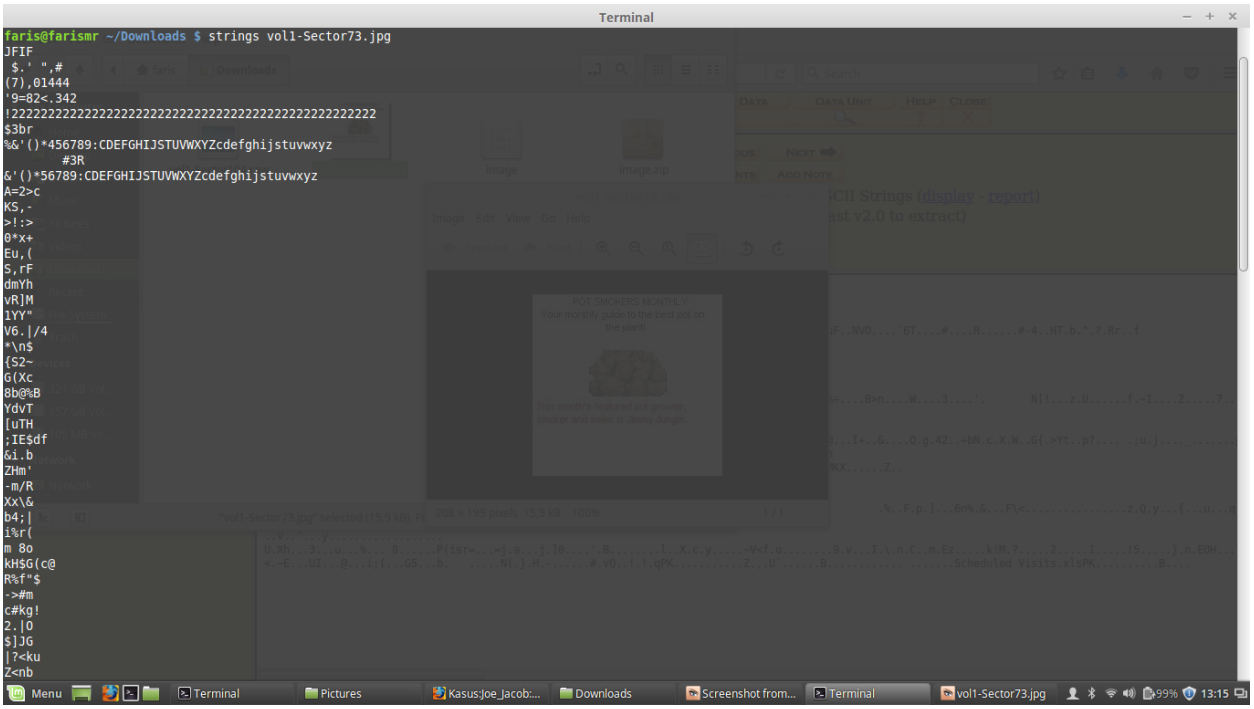

**Gambar 1.18.** File vol1-secotr73.raw

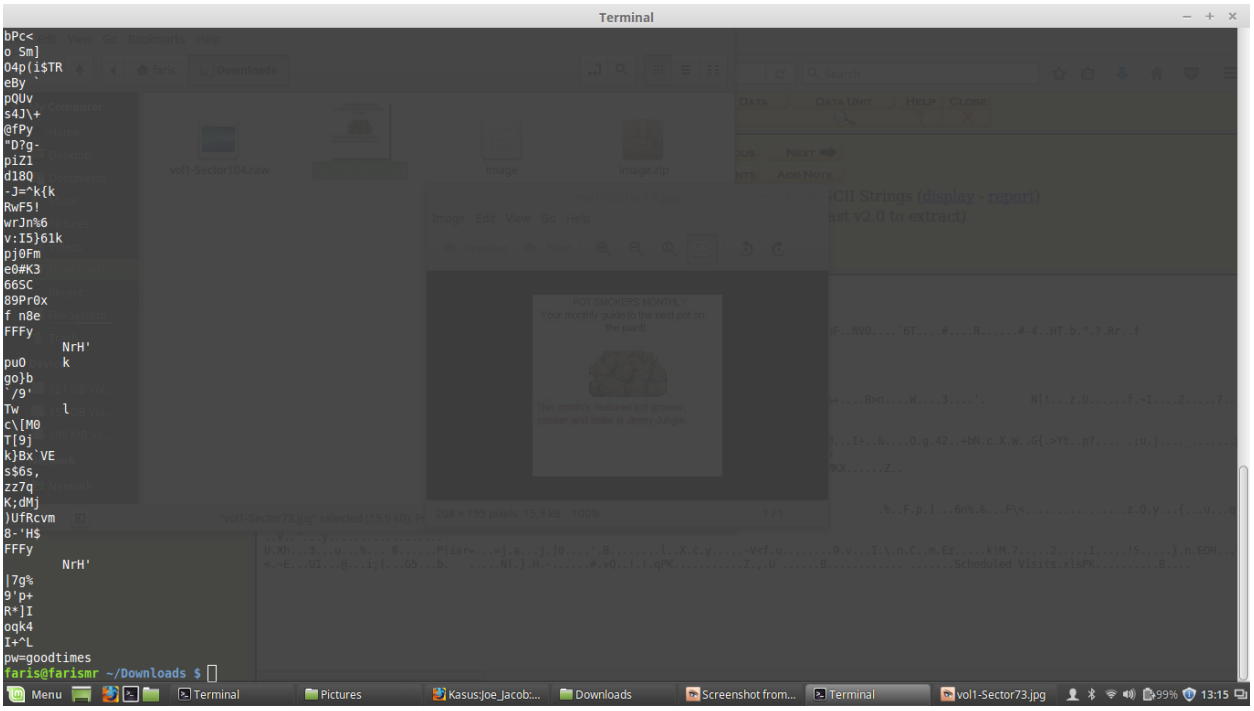
Format .raw pada sector73 diubah menjadi .jpg, dan akan berubah menjadi gambar. Dan kabar tersebut dapat dilihan pada gambar 1.19 dibawah.




**Gambar 1.19.** Gambar sector73

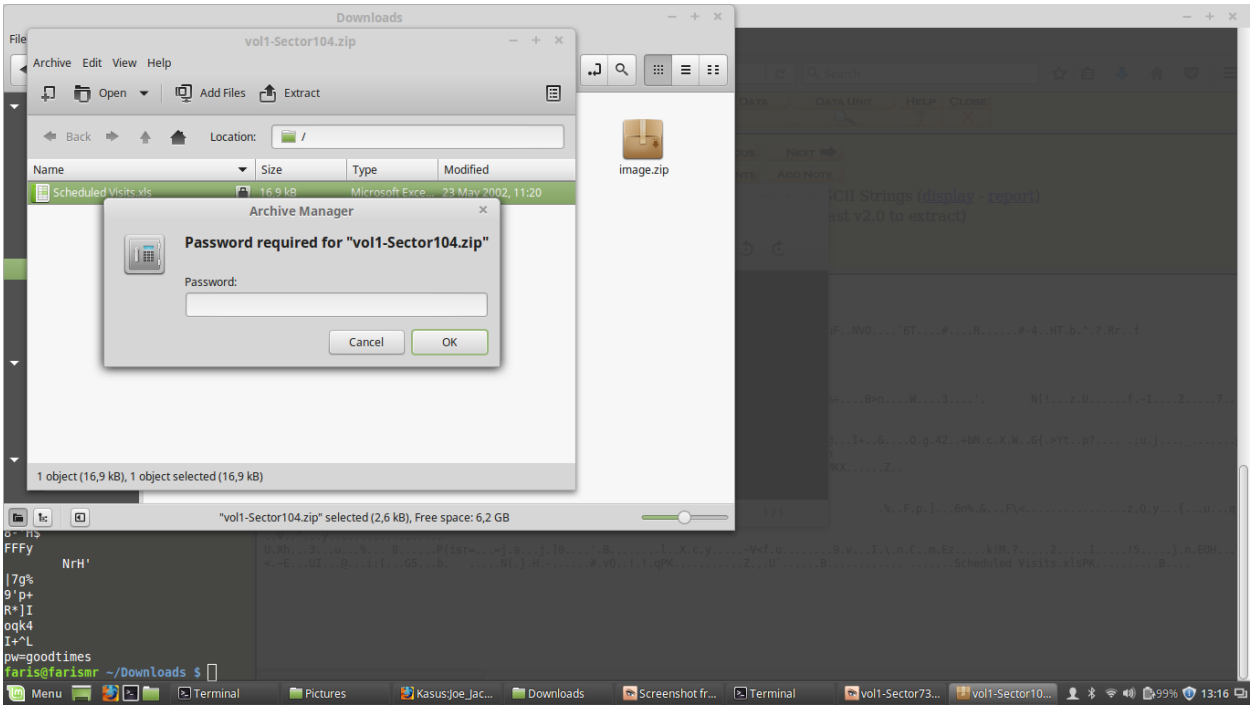
Lalu masukkan perintah String vol1-sector73.jpg, yang dimana string berguna untuk melihat readable pada sebuah file. Dan kita akan mendapatkan sebuah password untuk masuk pada .zip sector104.zip. Dapat dilihat pada gambar 1.20 dibawah,

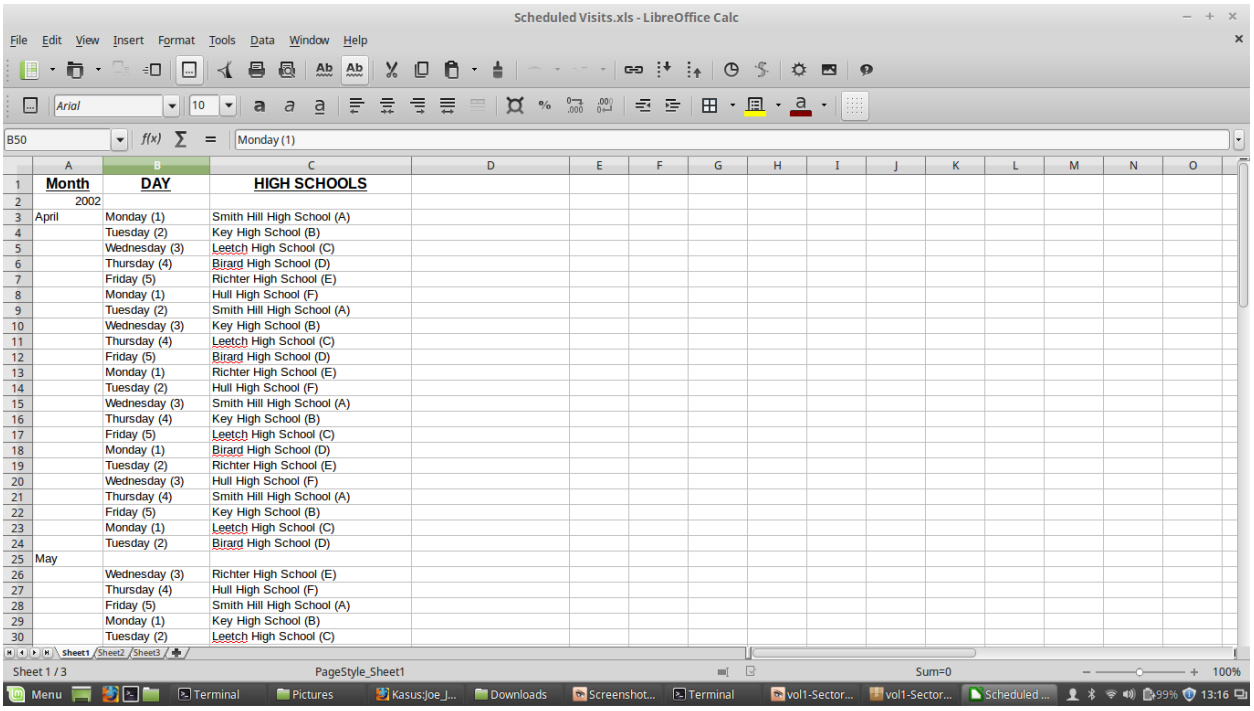





**Gambar 1.20.** String sector73

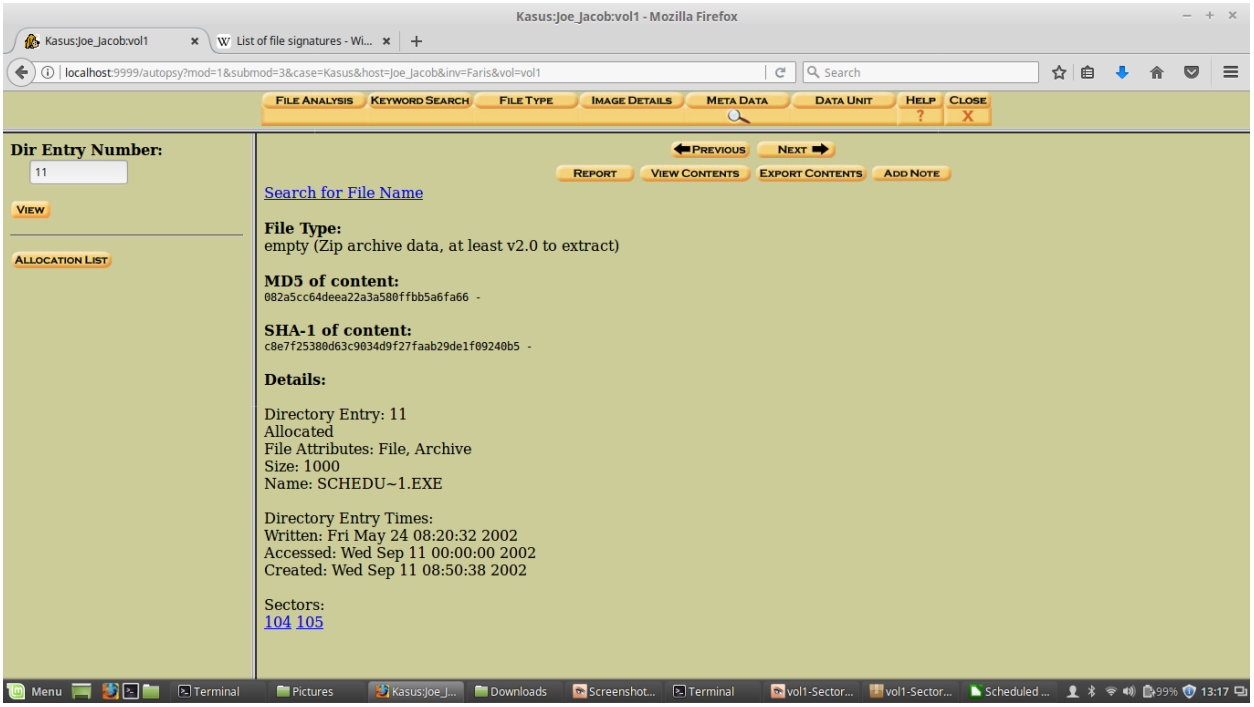
Masukkan password yang didapatkan dari perintah string pada gambar 1.20 kedalam file sector104.zip, setelah itu buka file yang ada didalam zip tersebut. Dapat dilihat pada gambar 1.21 dibawah.





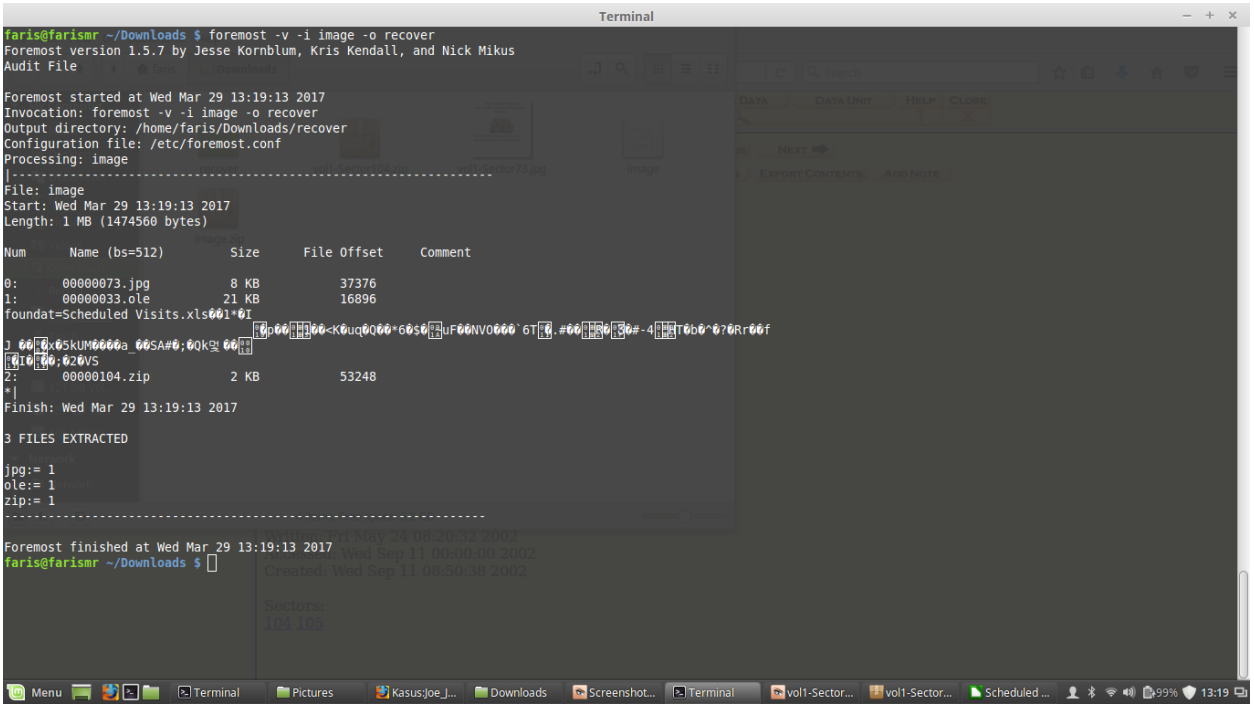

**Gambar 1.21.** File sector104.zip

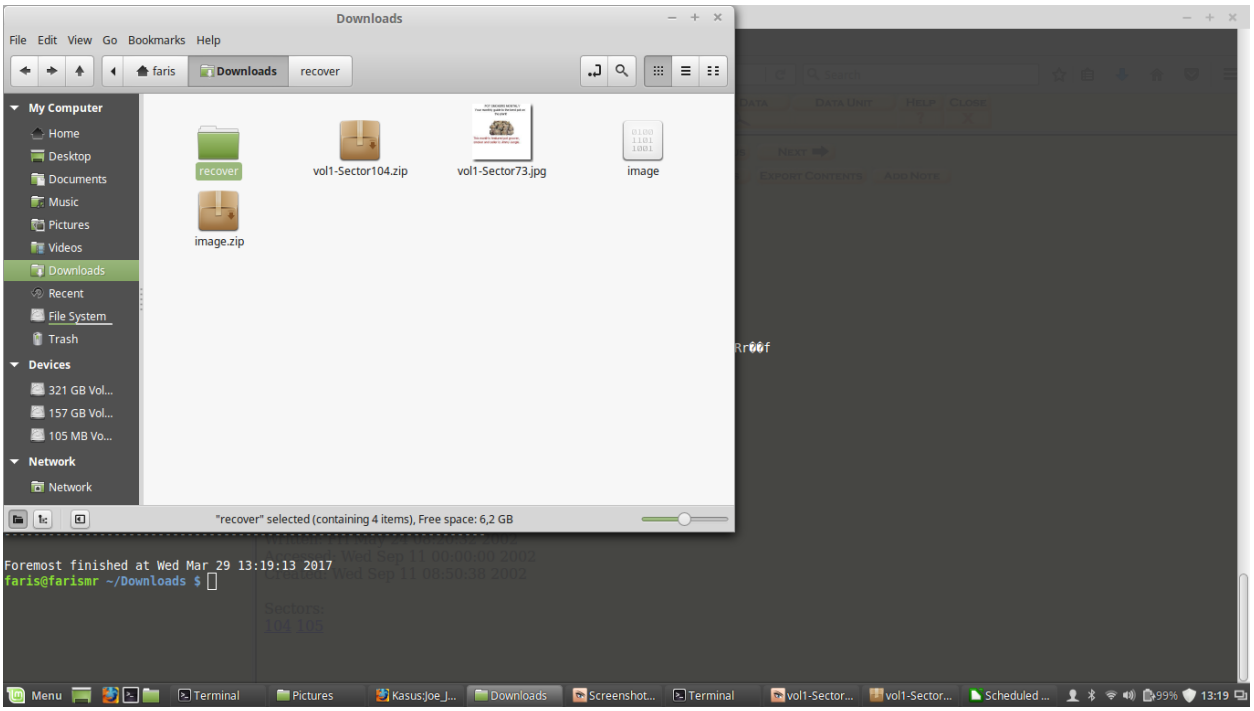
Kembali lagi pada localhost, lalu masukkan dir entry number dengan angka 11, dan akan muncul tampilan seperti gambar 1.22 dibawah.

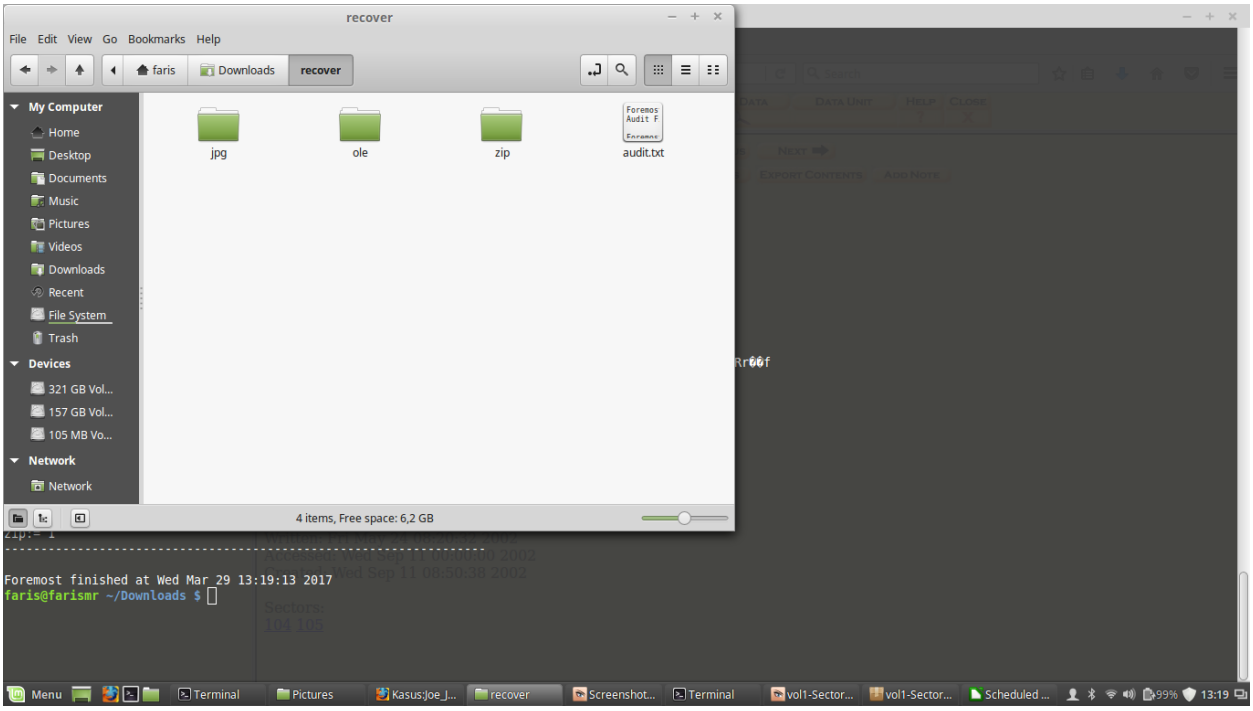


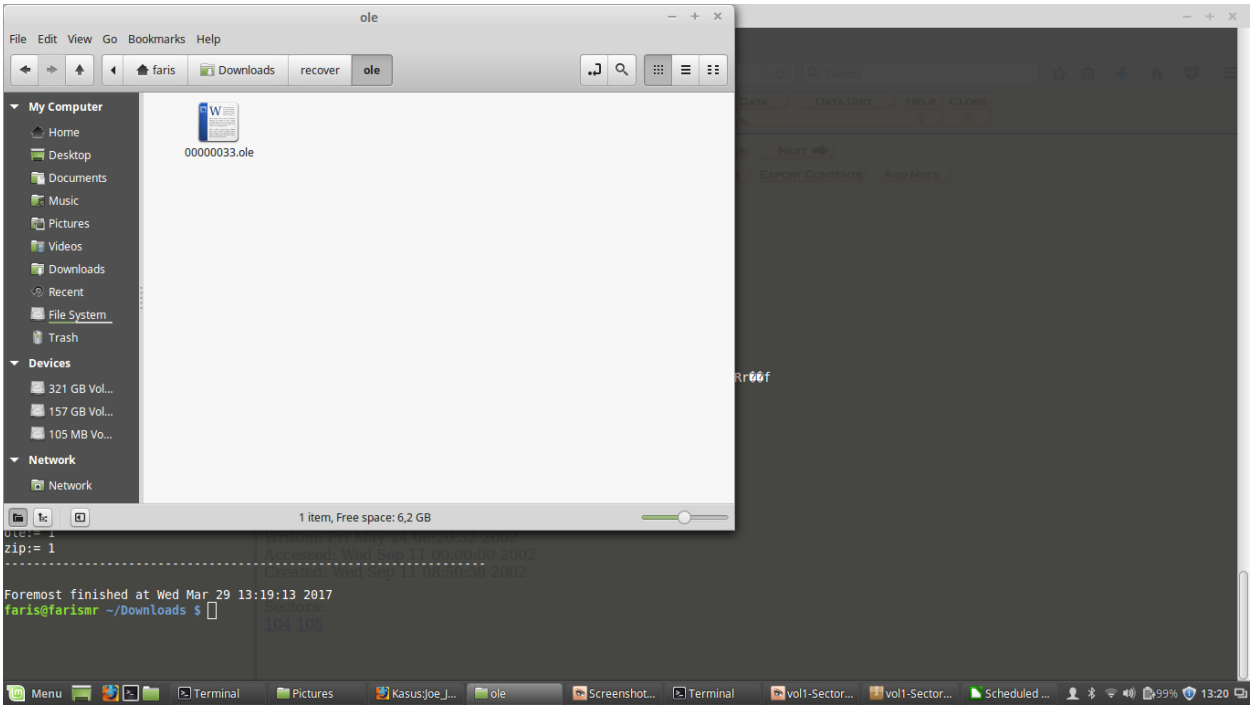

**Gambar 1.22.** Meta Data

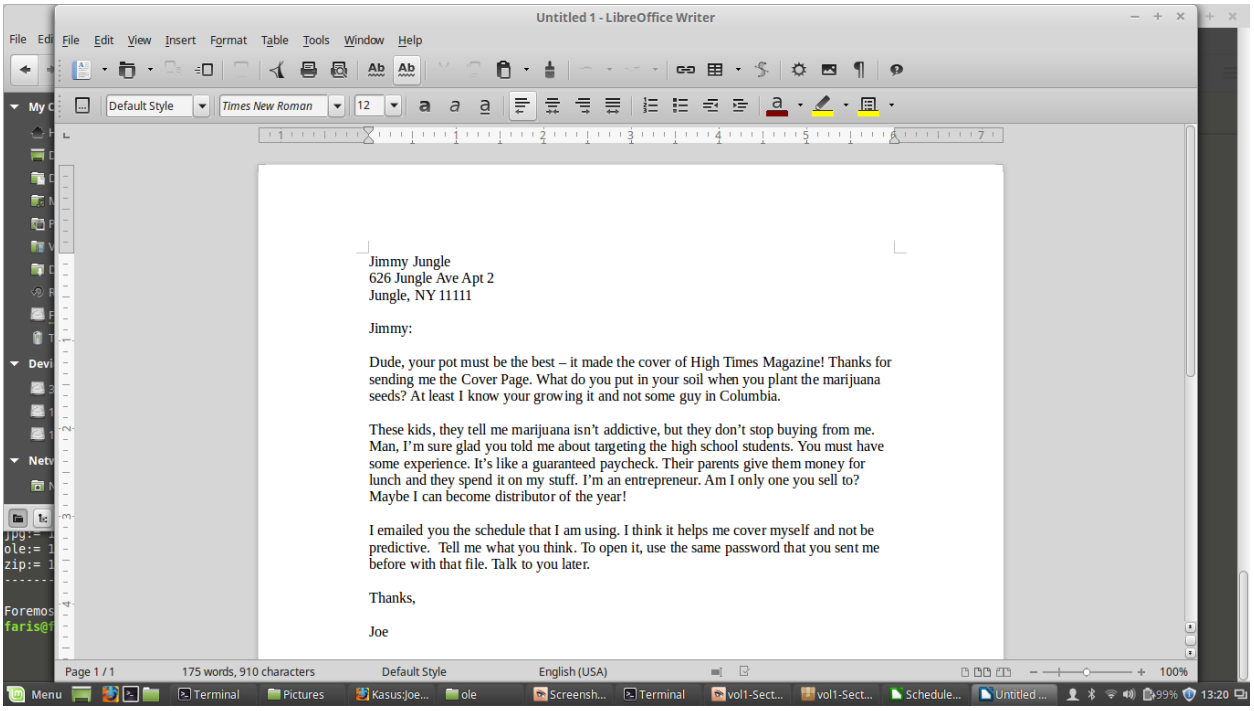
Lalu masukkan perintah foremost –v –i image –o recover, yang berfungsi untuk mengembalikan data yang tertimpa dan recover sebagi extrak file ini. Dapat dilihat pada gambar 1.23 dibawah.



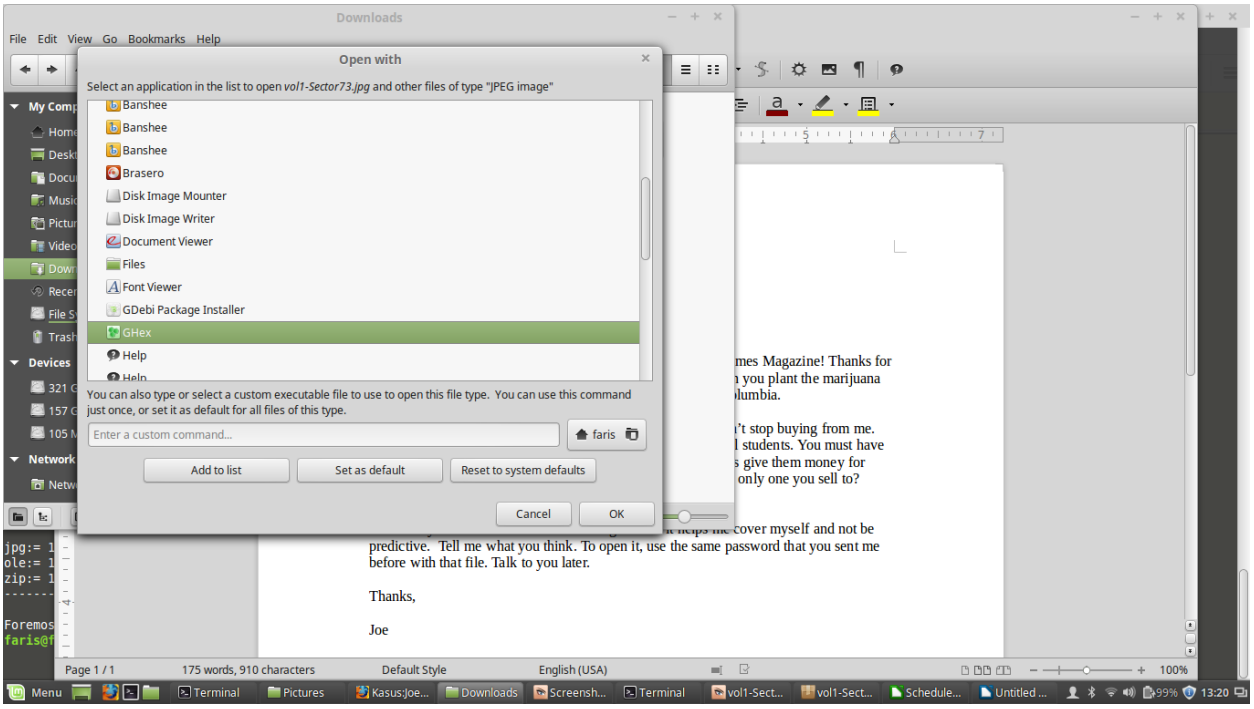

recover
File Edit View Go Bookmarks Help
faris
Downloads
recover
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Devices
321 GB Vol...
157 GB Vol...
105 MB Vo...
Network
Network
jpg
ole
zip
audit.txt
4 items, Free space: 6,2 GB
Foremost finished at Wed Mar 29 13:19:13 2017
faris@farismr ~/Downloads $
Menu
Terminal
Pictures
Kasus:Joe_J...
recover
Screenshot...
Terminal
vol1-Sector...
vol1-Sector...
Scheduled ...
99%
13:19

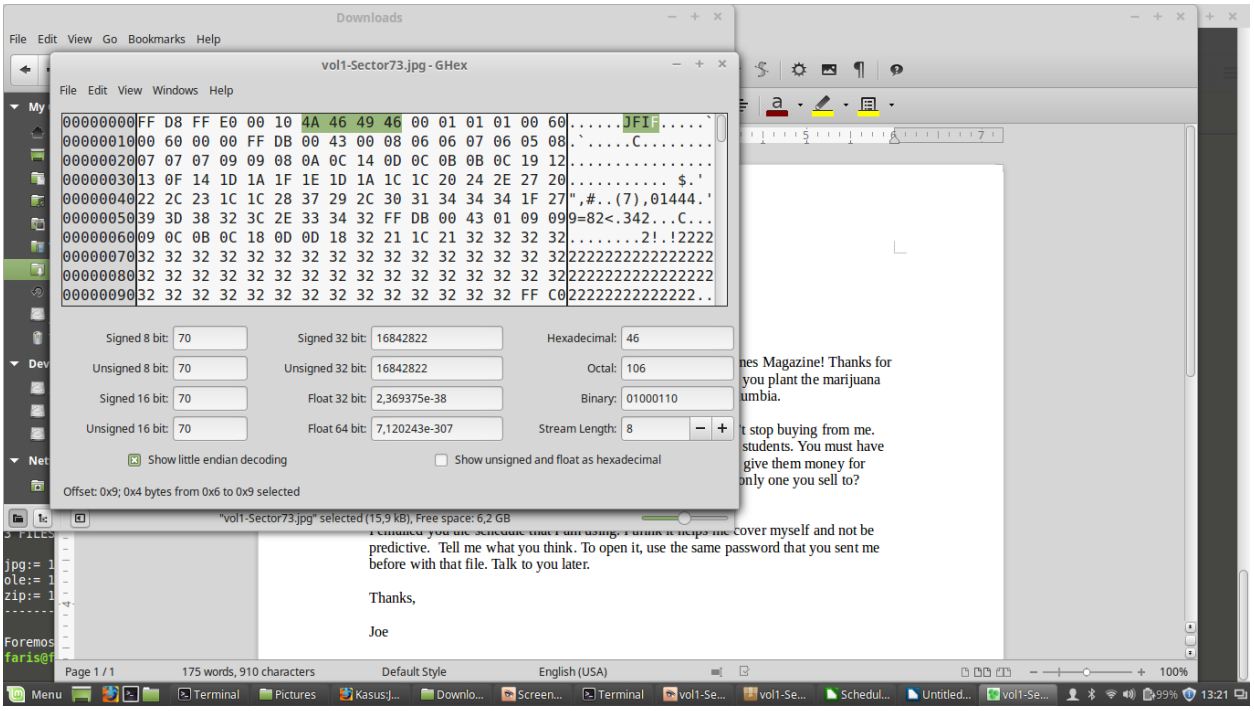

ole
File Edit View Go Bookmarks Help
faris
Downloads
recover
ole
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Devices
321 GB Vol...
157 GB Vol...
105 MB Vo...
Network
Network
00000033.ole
1 item, Free space: 6,2 GB
zip:= 1
Foremost finished at Wed Mar 29 13:19:13 2017
faris@farismr ~/Downloads $
Menu
Terminal
Pictures
Kasus:Joe_J...
ole
Screenshot...
Terminal
vol1-Sector...
vol1-Sector...
Scheduled ...
99%
13:20




**Gambar 1.23.** Foremost dan isi file recovery

Lalu open with pada sector73 dan ubah ke GHex. Dan akan muncul tampilan file tersebut setelah diubah menjadi format GHex, dapat dilihat pada gambar 1.24 dibawah.






**Gambar 1.24.** GHex

Setelah mendapatkan data yang dicari pada gambar-gambar diatas, maka kita dapat memberikan beberapa informasi yang diperlukan untuk bahan penyelidikan, Berikut beberapa pertanyaan yang diminta:

1. Siapa pemasok narkoba Joe Jacob dan apa alamatnya?
   **Jawab: Jimmy Jungle adalah pemasok narkoba pada Joe Jacob, dan beralamat pada 626 Jungle Ave Apt 2.**

2. Data penting apa yang terdapat di file coverage.jpg dan mengapa data tersebut penting?
   **Jawab: File Scheduled Visit.xls, tetapi file ini harus diakses menggunakan password yang telah diberikan sebelumnya. Informasi penting yang didapatkan pada file tersebut adalah dimana tempat-tempat yang mereka lakukan sebagai tempat transaksi kepada Joe Jacob.**

3. Nama sekolah selain Smith Hill yang sering menjadi tempat transaksi Joe Jacob?
   **Jawab: Key High School, Leetch High School, Birard High School, Richter High School dan Hull High School.**

4. Untuk setiap file proses apa yang diambil oleh tersangka untuk mengelabuhi orang lain?
   **Jawab: Dengan cara mengubah format .zip menjadi format .raw pada file vol1-sector73 dan sector104.**

5. Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file?
   **Jawab: Pada penyidikan ini digunakan beberapa tools, yaitu autopsy, foremost dan GHex. Yang dimana tools tersebut dapat melacak dan mendapatkan informasi dalam kasus ini. Seperti tempat transaksi yang dilakukan kepada Joe Jacob, serta surat yang diberikan oleh Jimmy Jungle kepada Joe Jacob.**