TUGAS

KEAMANAN JARINGAN KOMPUTER

Nama : Dede Triseptiawan

Nim : 09011181320001

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

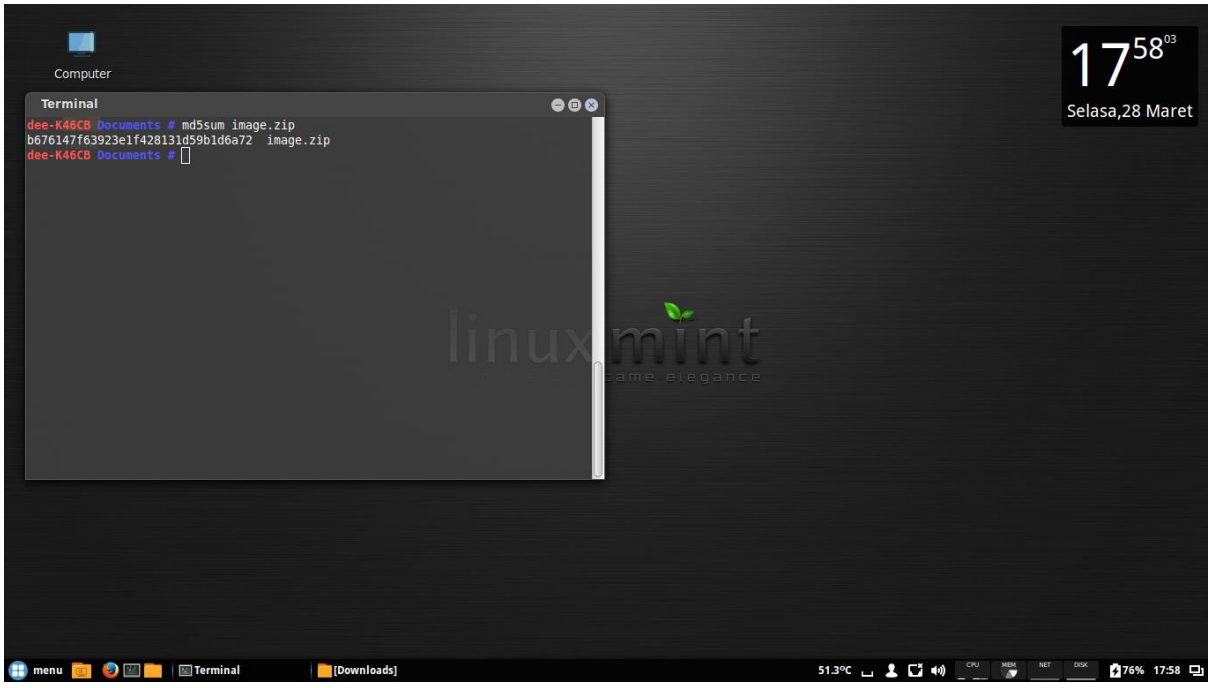
UNIVERSITAS SRIWIJAYA

2017

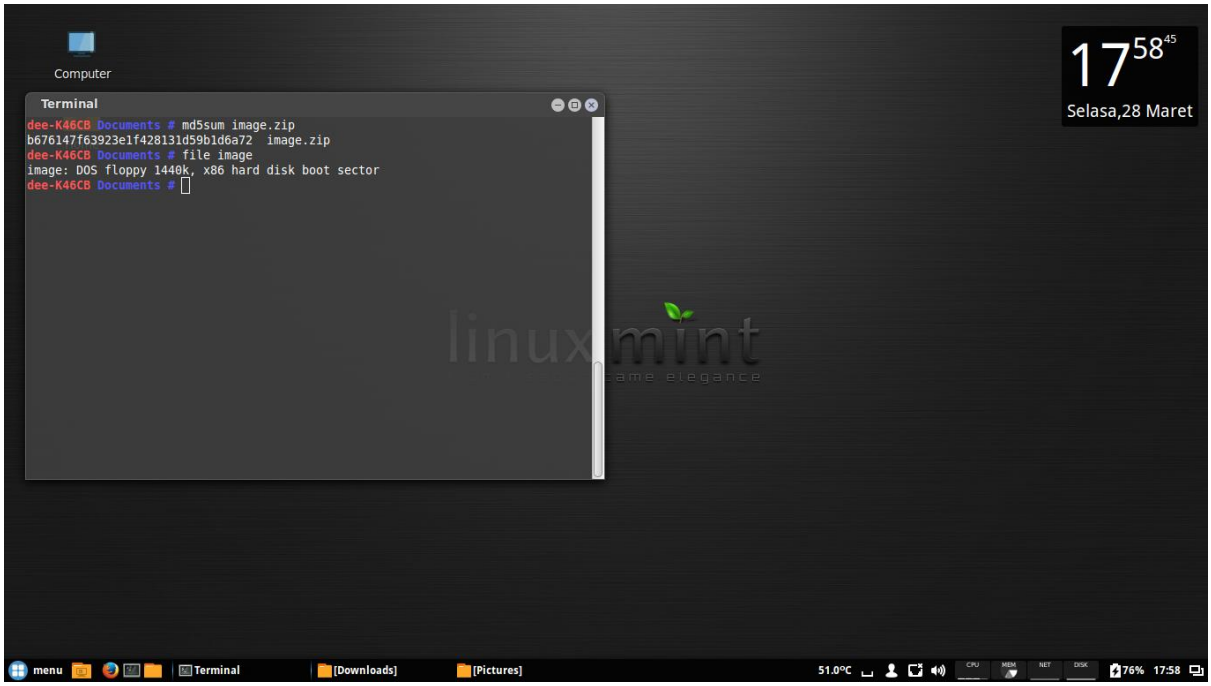
Forensik komputer adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan digital. Tujuannya untuk menjabarkan keadaan kini dari suatu artefak digital. Istilah artefak digital bisa mencangkup sebuah sistem komputer, media penyimpanan, sebuah dokumen elektronik atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Secara umum kebutuhan forensik komputer dapat digolongkan sebagai keperluan investigasi tindak kriminal dan perkara pelanggaran hukum, rekontruksi duduk perkara insiden keamanan komputer, dan lain-lain.

Pada tugas ini kita mencoba memecahkan kasus narkoba, dan didapatkan berupa file image, sebagai bahan investigasi kasus tersebut, tools yang dibutuhkan berupa, autopsy, foremost, strings, dan Ghex. Kegunaan autopsy untuk melakukan digital forensic, autopsy dapat melakukan analyze terhadap disk image serta partition, tujuannya agar dapat melakuan analyze terhadap file system yang dapat menjadi evidence atau bukti.

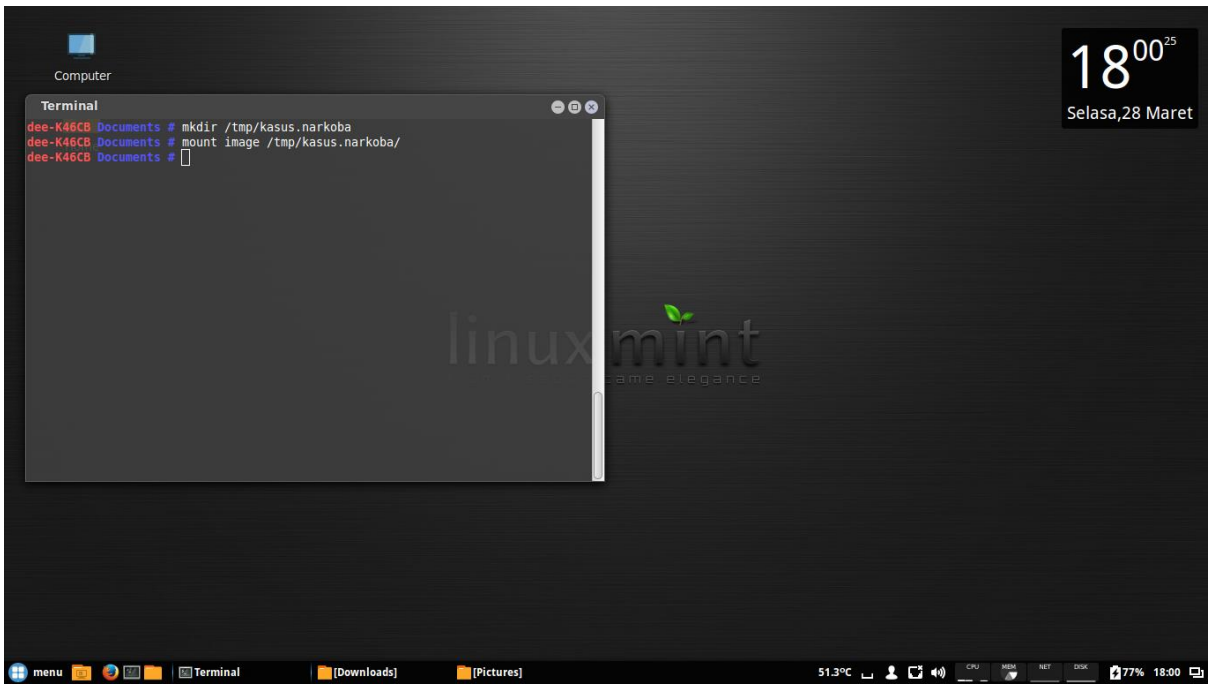
Berikut tahap-tahap dalam melakukan pemecahan kasus narkoba, pertama kita download file image.zip yang sebagai barang bukti yang ditemukan dalam kasus ini ((old.honeynet.org/scans/scan24/image.zip) md5 : b676147f63923e1f428131d59b1d6a72)



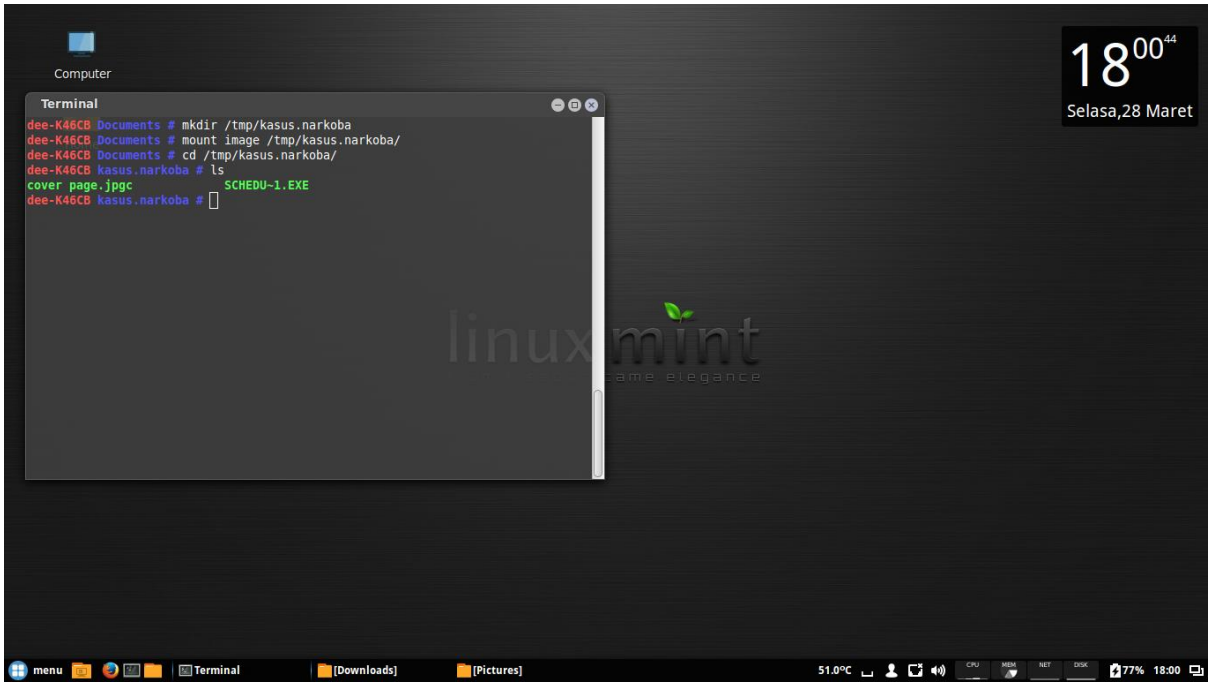
Setelah diunduh file image lalu di pindahkan di di folder documents agar lebih mudah, lalu buka terminal lalu masuk ke direktori documents, lalu ketik md5sum image.zip, perintah md5sum berfungsi untuk mengecek keaslian file, kemudian eksrak image.zip



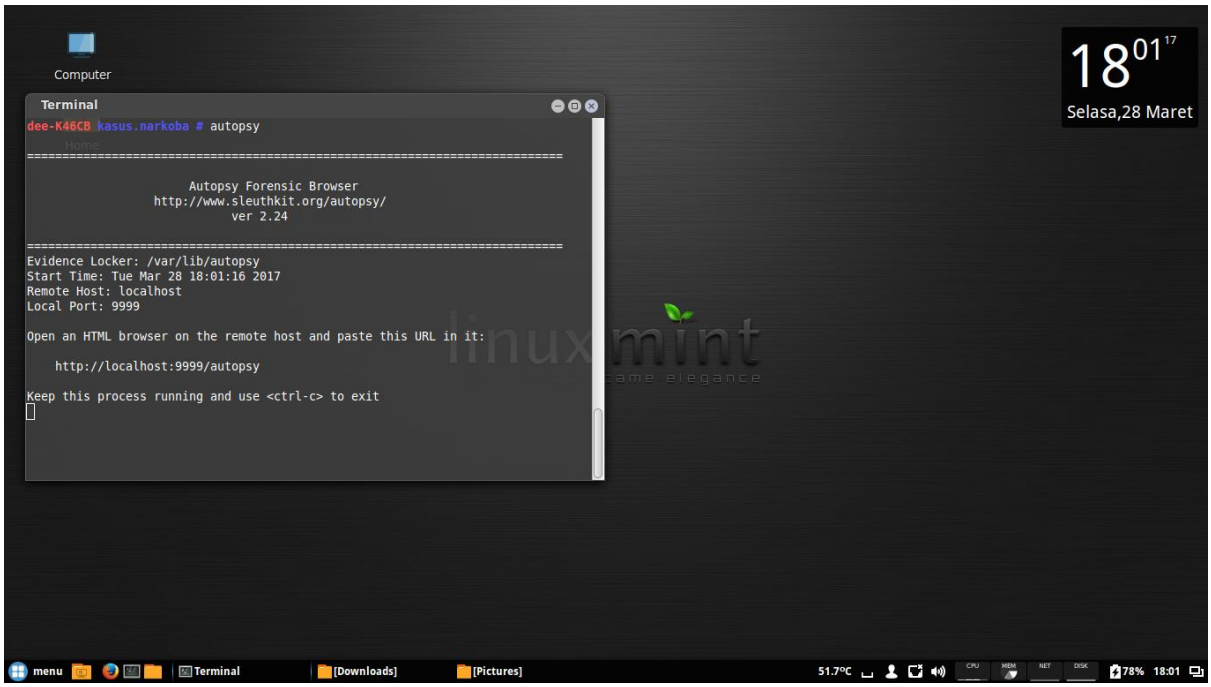
Setelah di ekstrak lalu ketik perintah file image, fungsi perintah file untuk melihat tipe filenya.



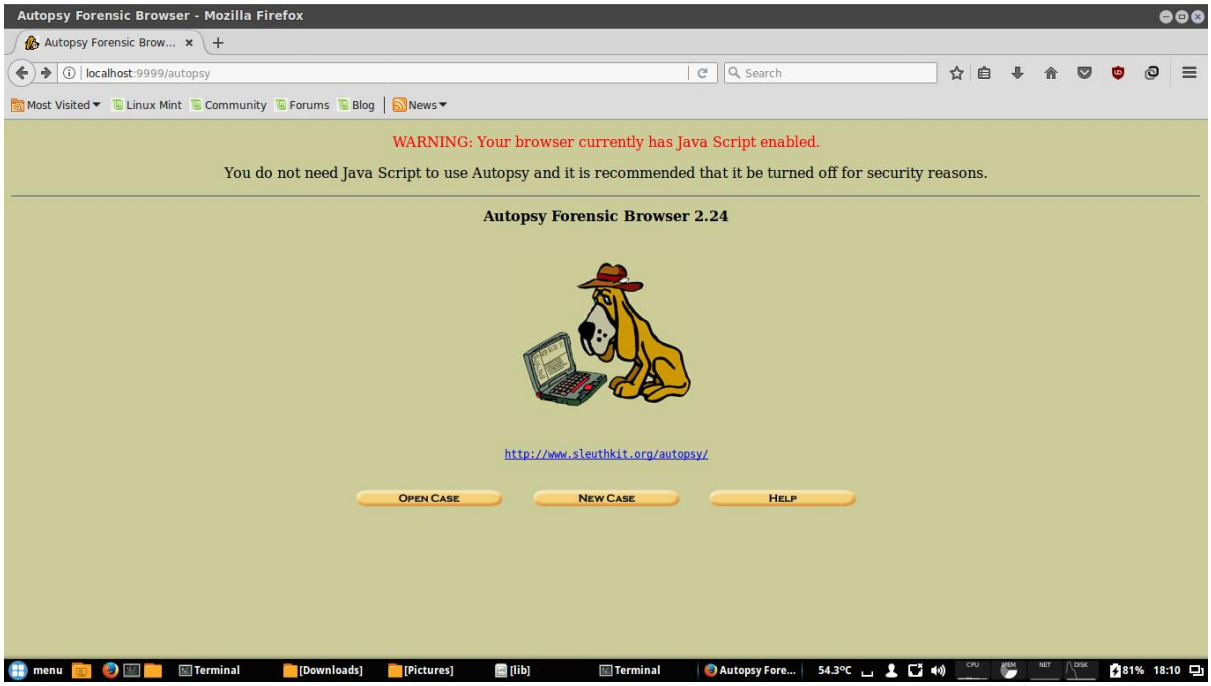
Kemudian buat folder kasus.narkoba di direktori root /tmp/ . kemudian ekstrak file image di folder yang kita buat di direktori root /tmp/kasus.narkoba.



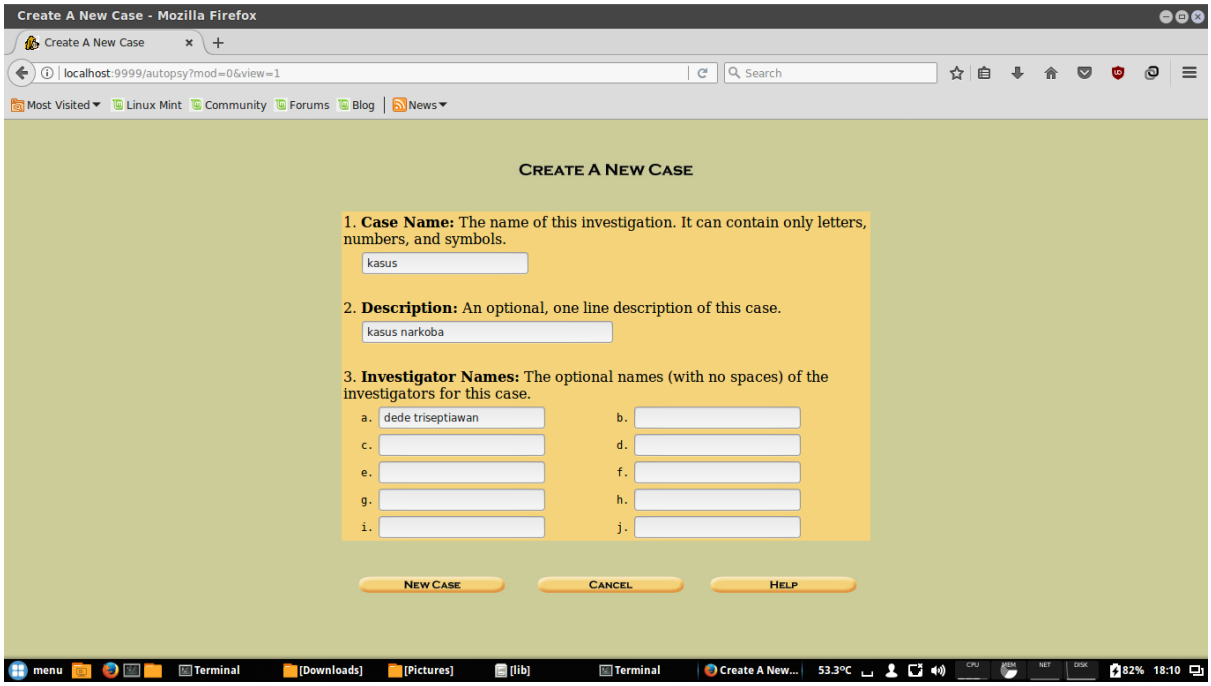
Kemudian kita masuk ke folder kasus.narkoba dengan perintah cd /tmp/kasus.narkoba/ , kemudian kita cek isi folder, dengan perintah ls.



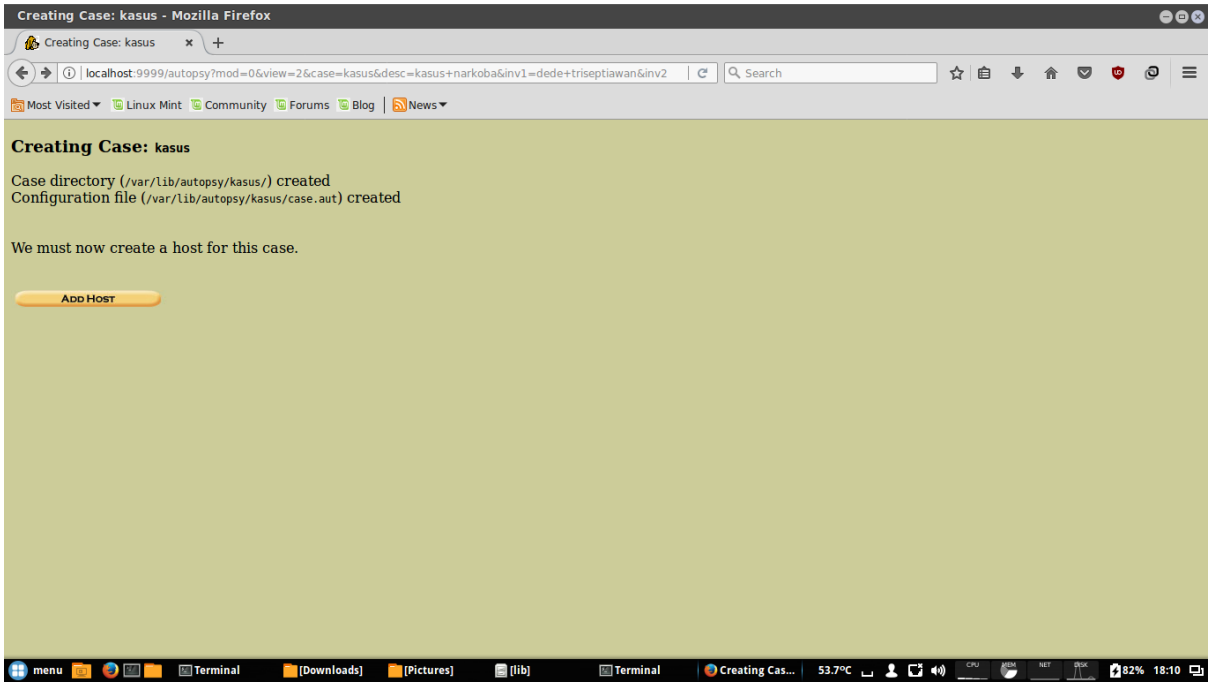
Kemudian kita buka tools autopsy di terminal, jangan di close terminal nya.



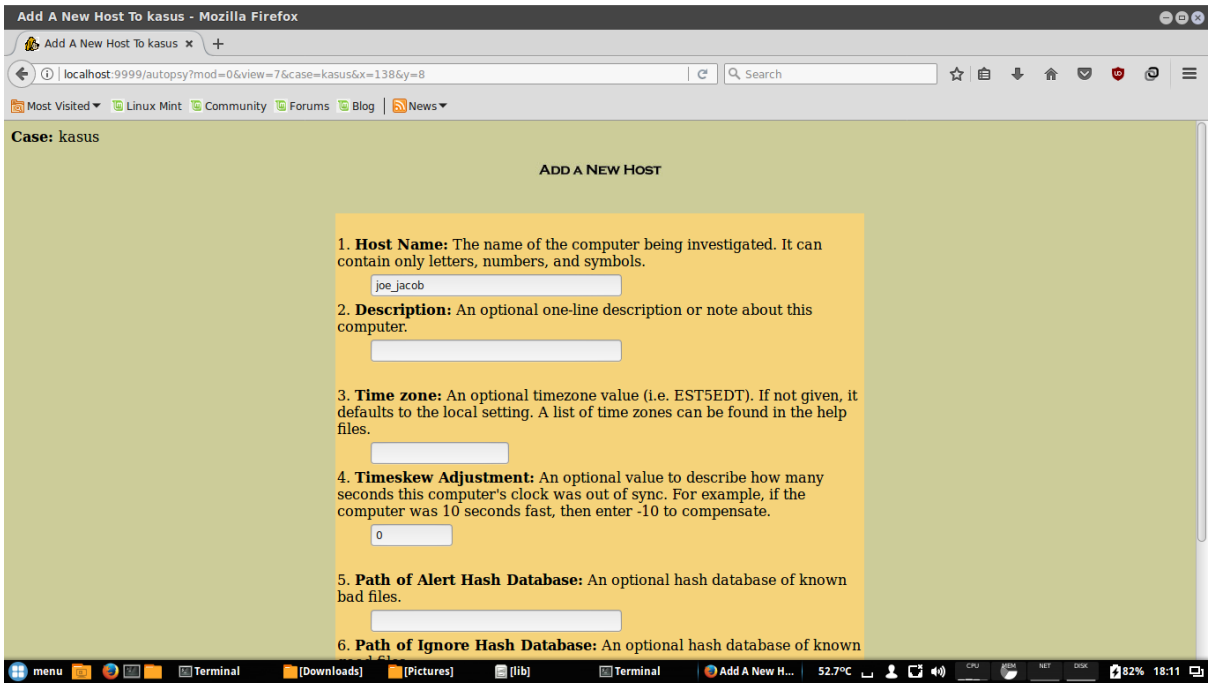
Kemudian buka browser masukkan alamat localhost:9999/autopsy maka akan terbuka tampilan dari tools autopsy, kemudian klik new case



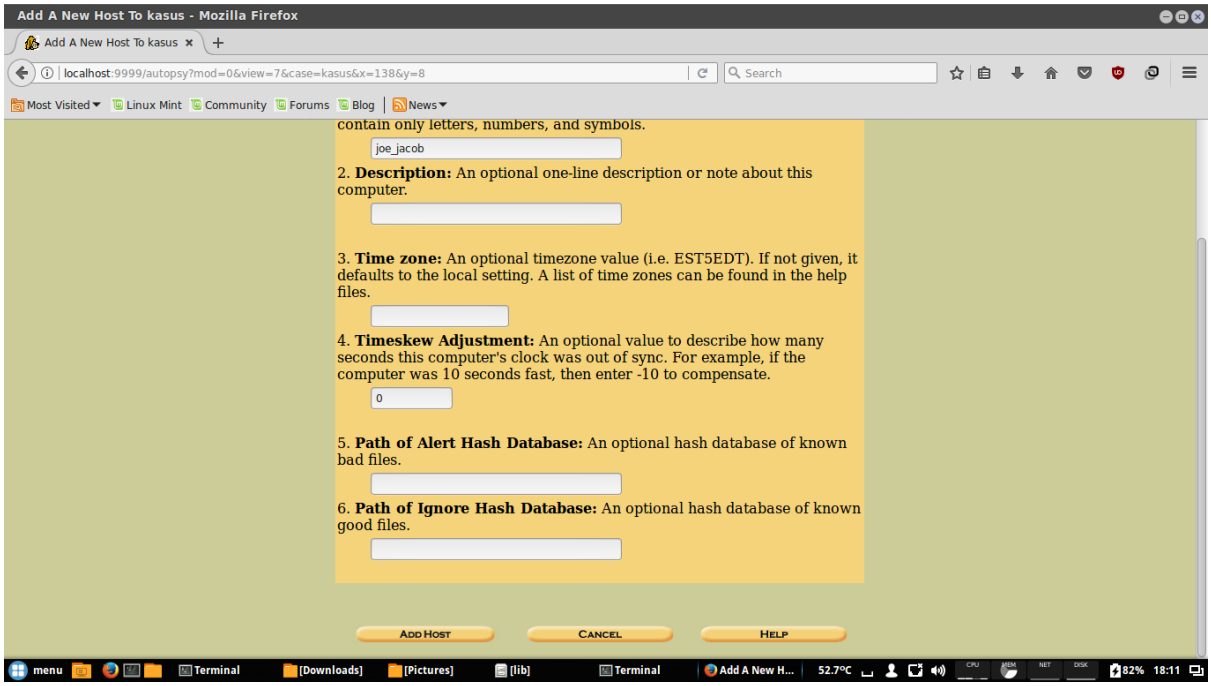
Kemudian kita buat case baru, dengan nama case kasus, dengan deskripsi kasus narkoba, dan nama investigasi nama kita, kemudian klik new case untuk melanjutkan



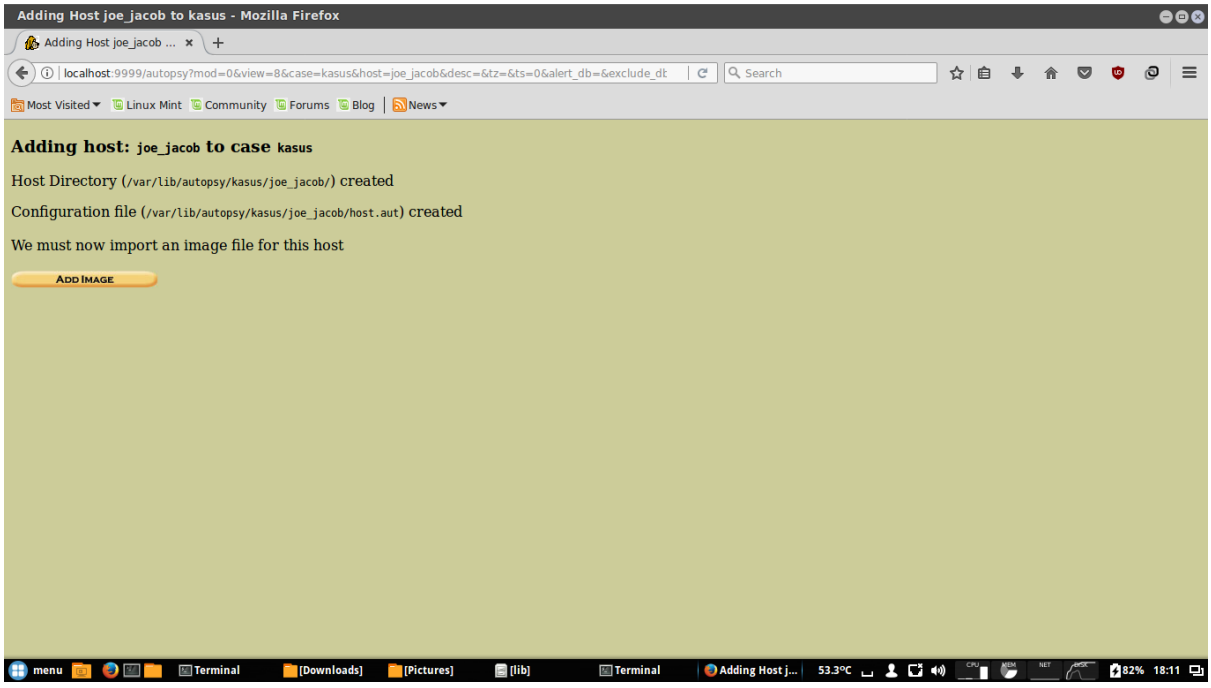
Case tersimpan di direktori root /var/lib/autopsy/kasus/ kemudian kita harus membuat host untuk case ini, klik add host



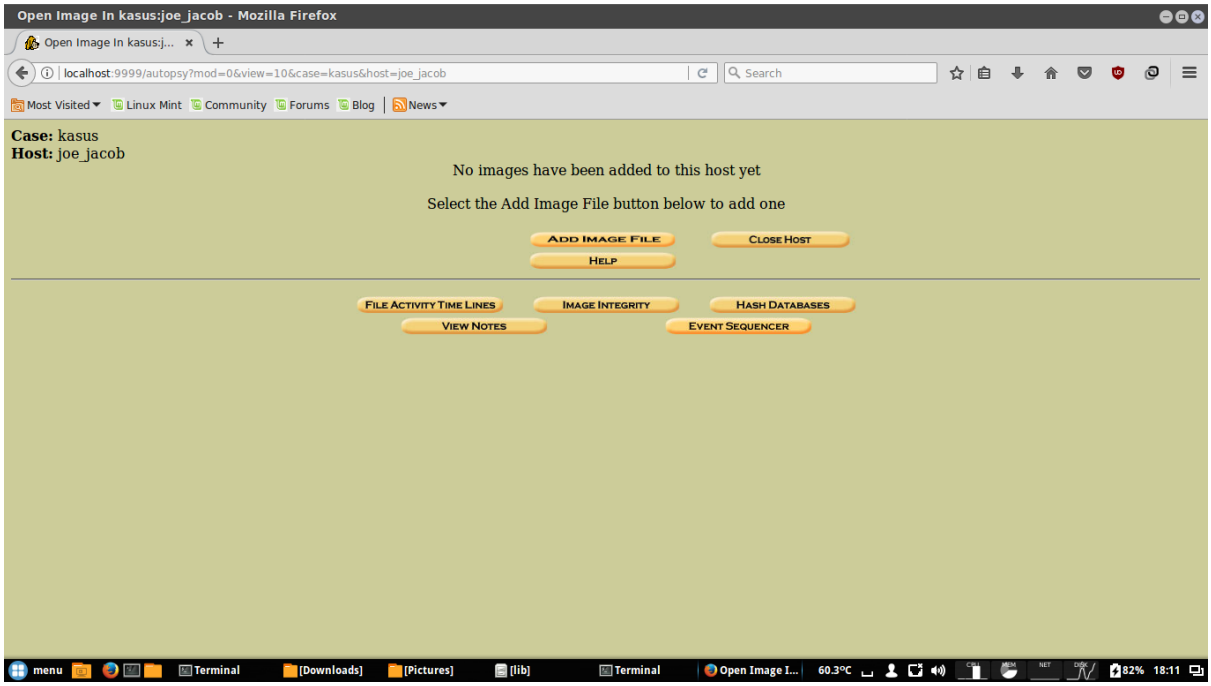
Kita buat host dengan nama joe_jacob



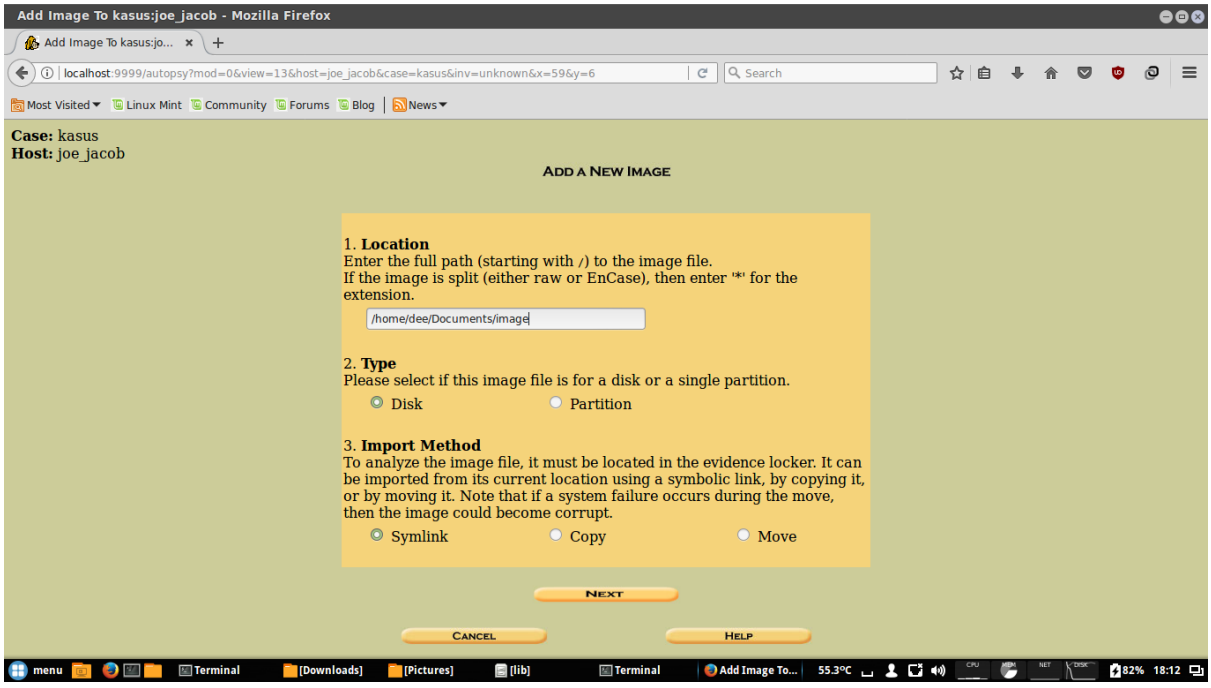
Kemudian klik add host



Host telah di buat, kemudian kita import file image, klik add image

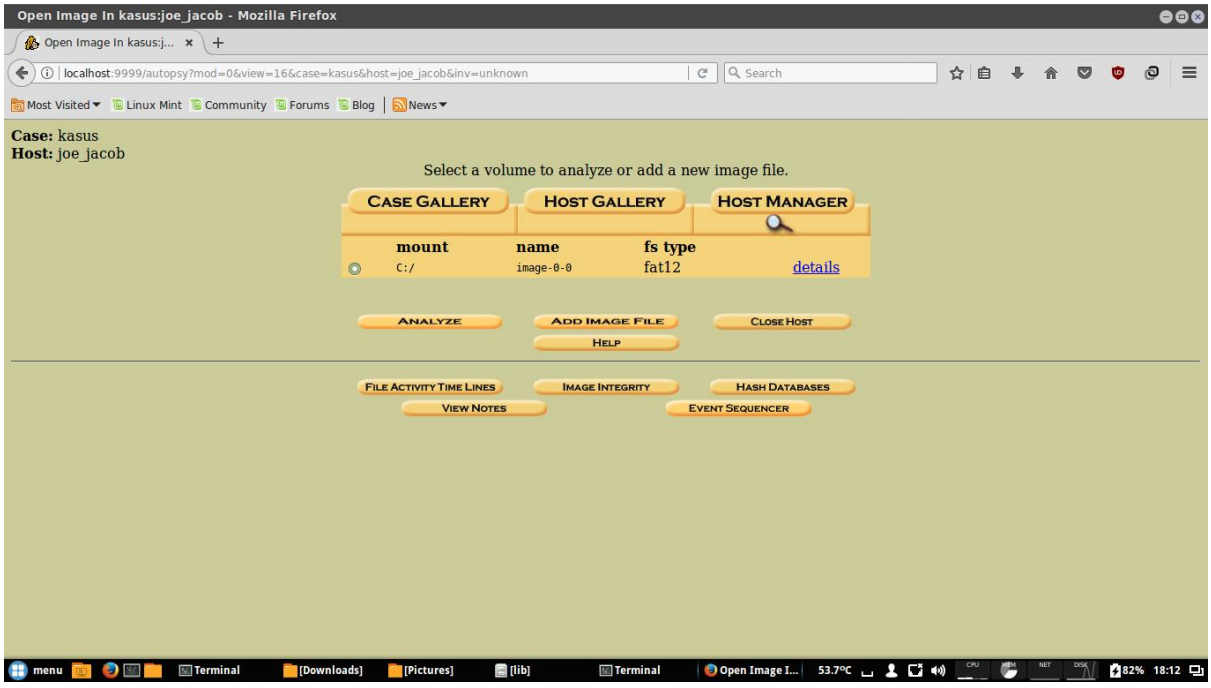


Kemudian klik add image file

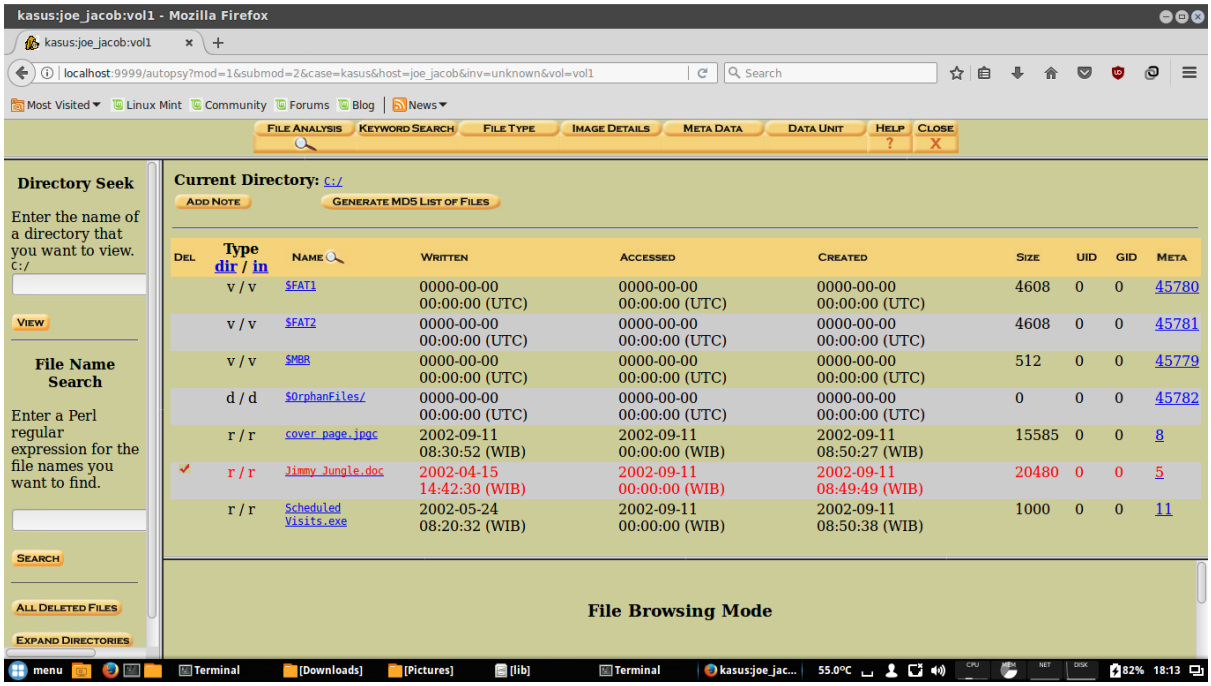


Masukkan lokasi file image yang telah di download tadi, lokasi file saya di direktori /home/dee/documents/image. Kemudian klik next

Kemudian centangkan pada volume image, lalu klik ok

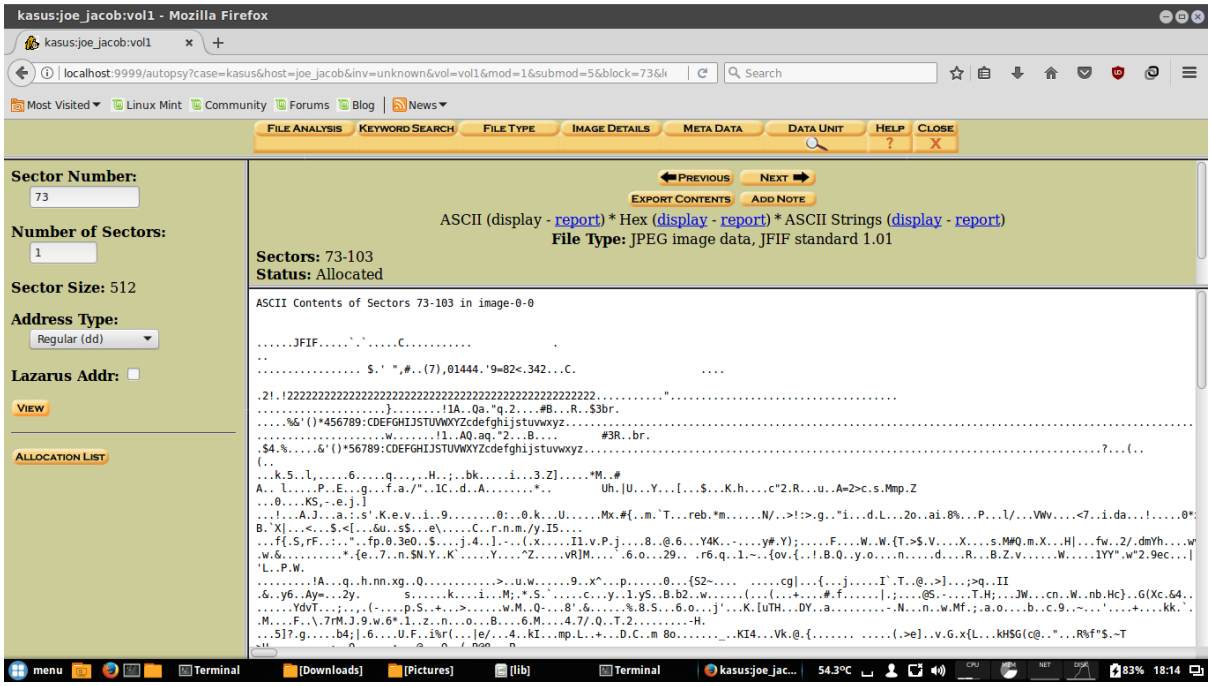


File image telah di tambahkan, kemudian klik analyze untuk melihat isi analisis file image

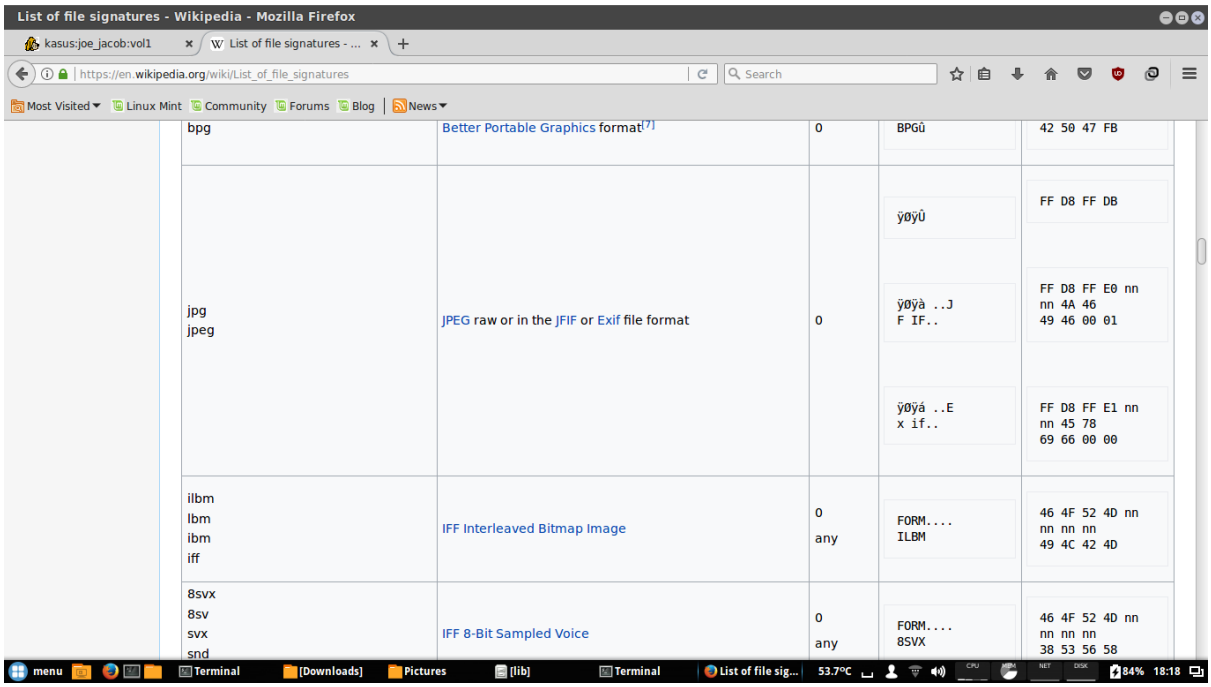


Setelah terbuka, klik file analysis, terdapat beberapa file di dalam file image

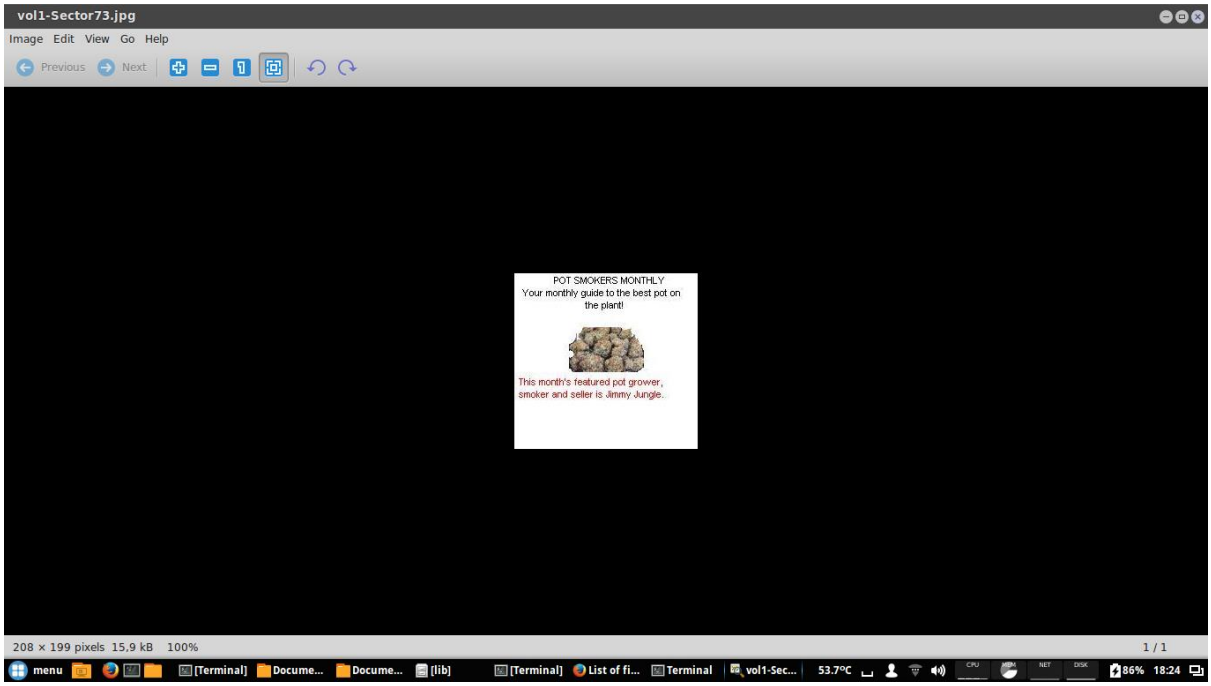
Kemudian klik image details, pada tab ini menjelaskan detail dari file image, kemudian paling bawah terdapat 2 file contents di dalam file image, kemudian klik 73-103 (31) -> EOF



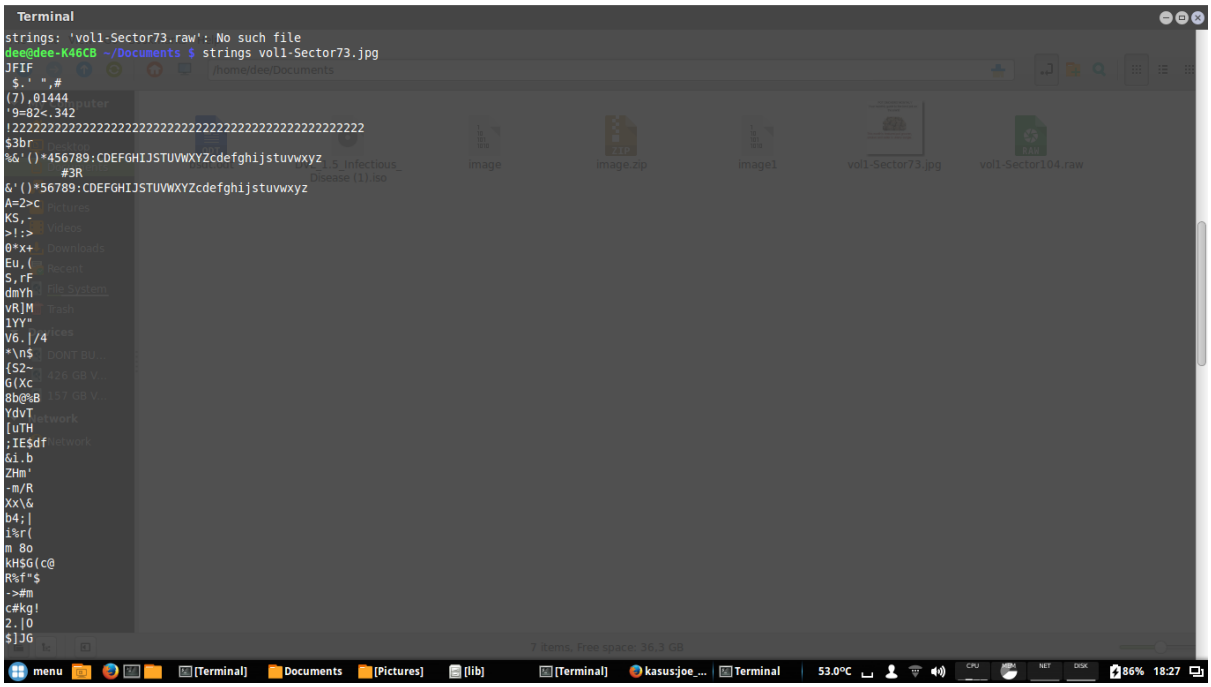
Setelah di klik akan muncul ASCII contents of sectors 73-103 dalam file image, pada awal kode tersebut ada kata JFIF. Kemudian kita export contents

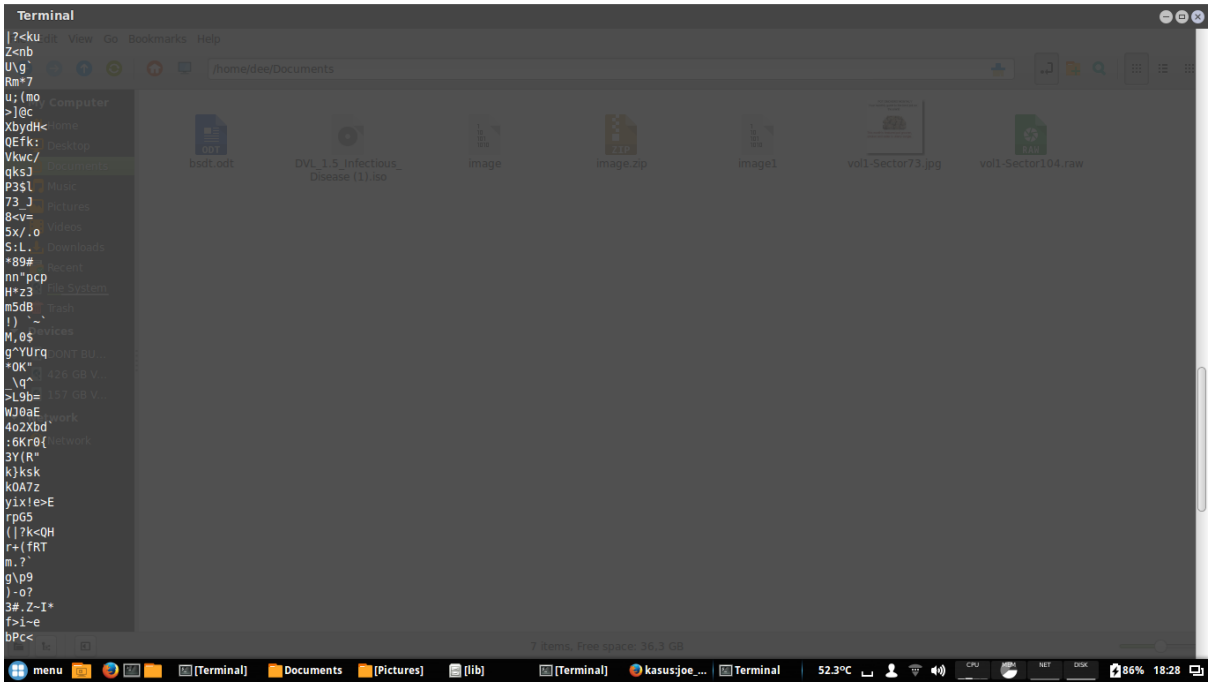


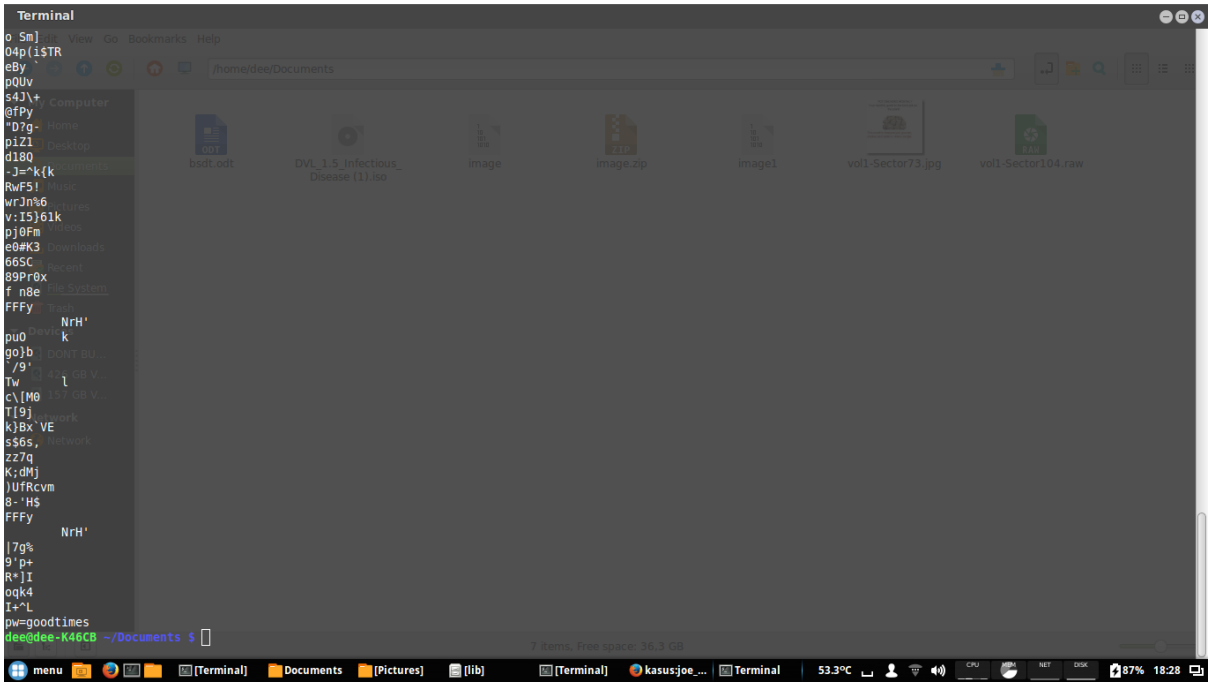
File JFIF adalah adalah format file tipe gambar



setelah kita export contents, maka akan otomatis terdownload file vol1-sector73.raw . kemudian kita ubah nama file tersebut menjadi vol1-sector73.jpg . maka akan terbuka file raw tersebut menjadi gambar diatas.

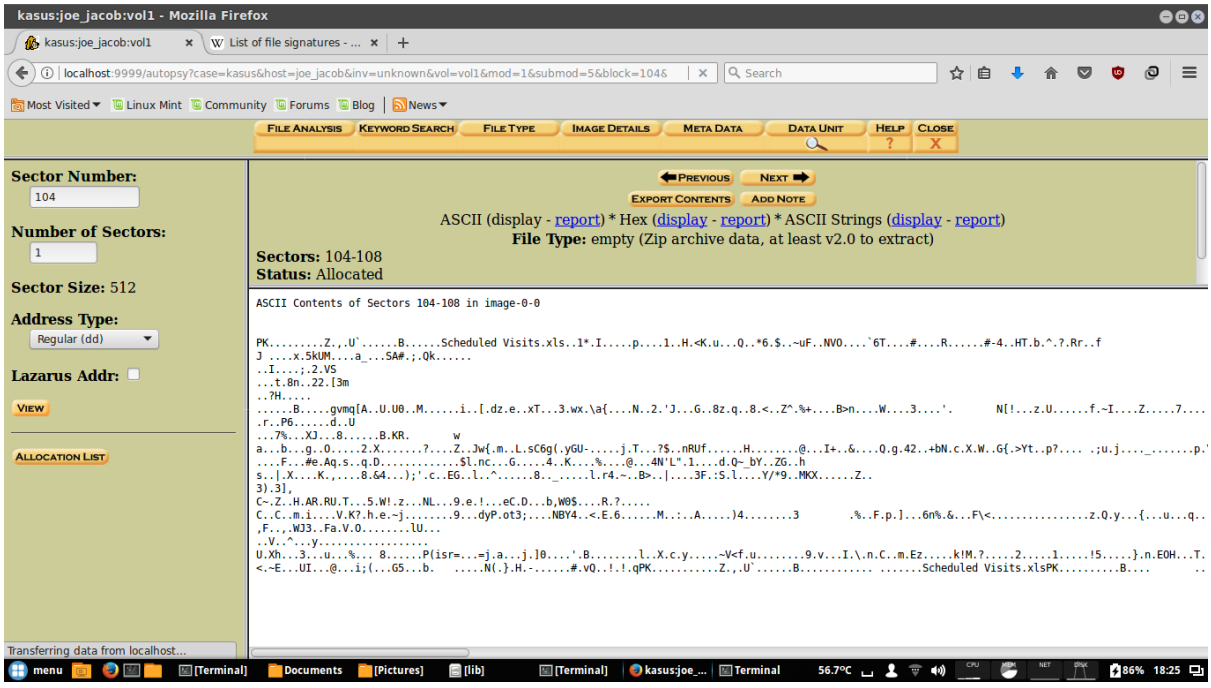




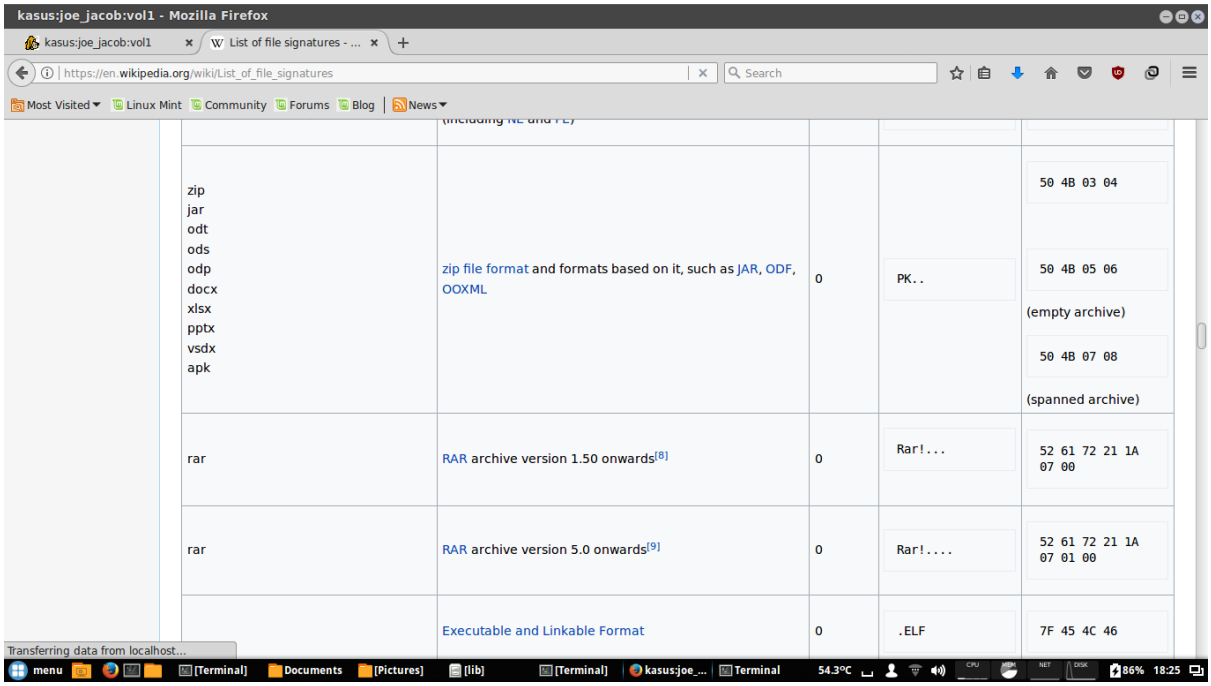


Kemudian kita buka folder tempat tersimpannya file vol1-sector73.jpg, kemudian buka terminal klik perintah strings vol1-sectors73.jpg maka terbuka seperti gambar diatas, pada paling bawah ada password “goodtimes” untuk membuka file vol1-sectors104.zip nantinya. Fungsi perintah strings untuk melihat karakter yang readable pada sebuah file.

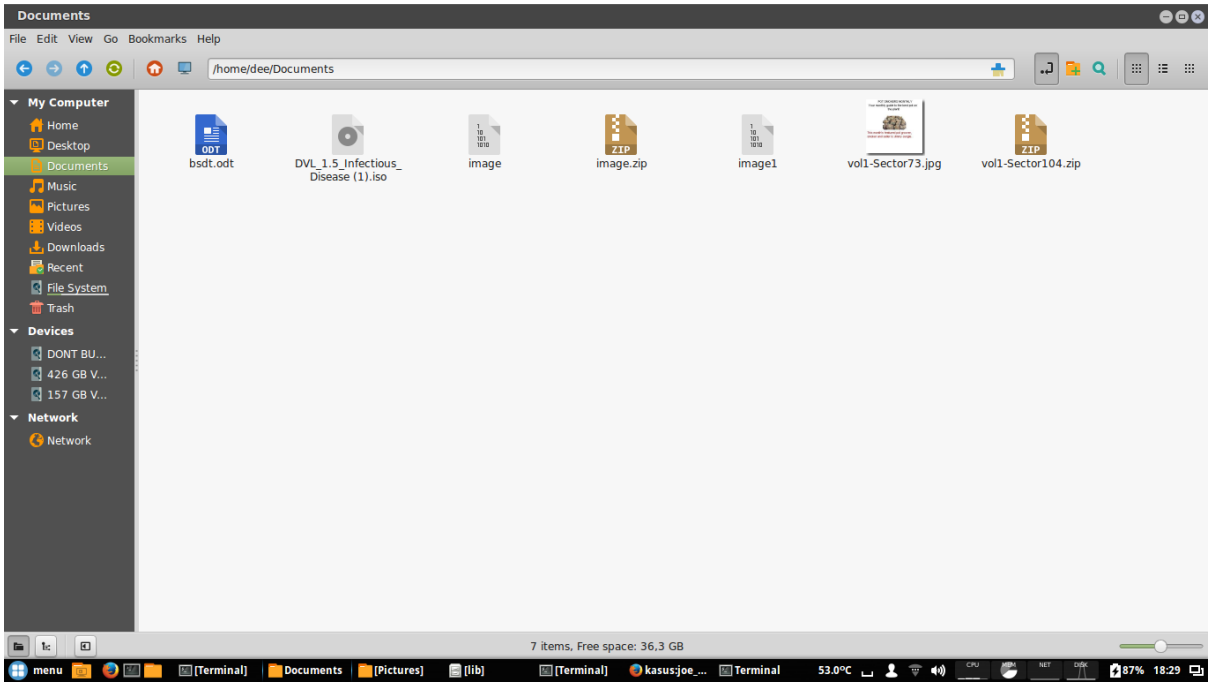
Kemudian kita back ke file image details, kemudian kita klik 104-108(5)-> EOF



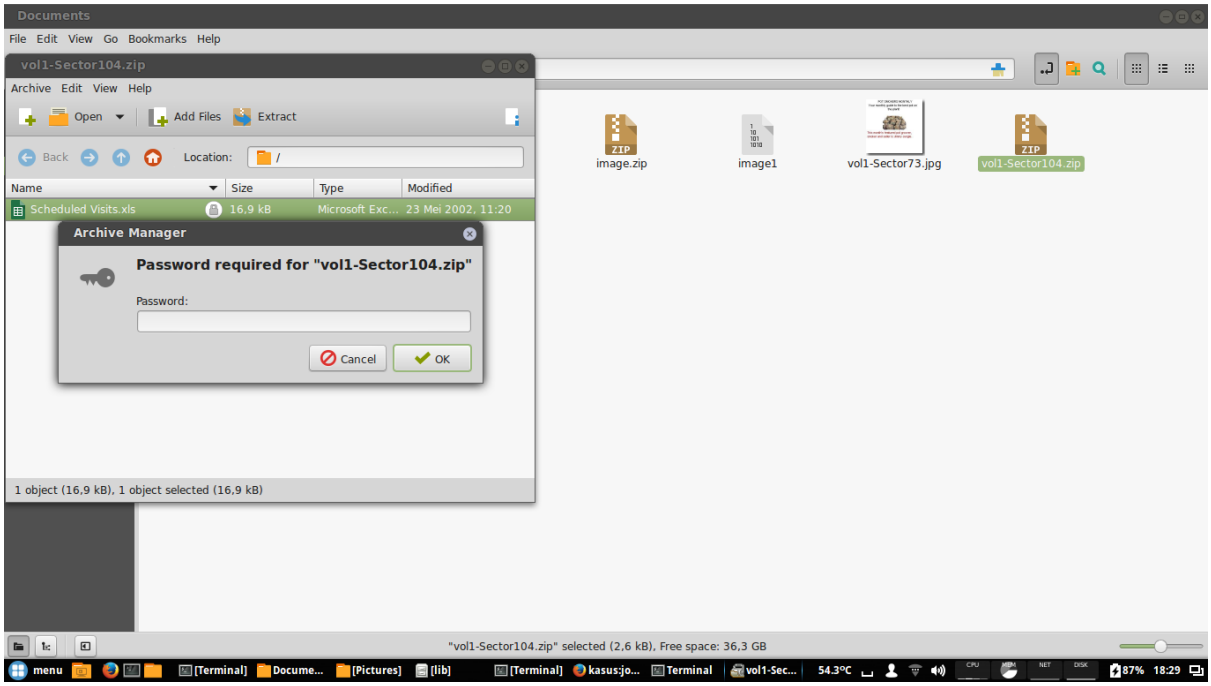
Maka akan muncul data unit ASCII contents of sector 104-108 di dalam file image, pada kode tersebut kata awal terdapat PK. Kemudian kita export contents.



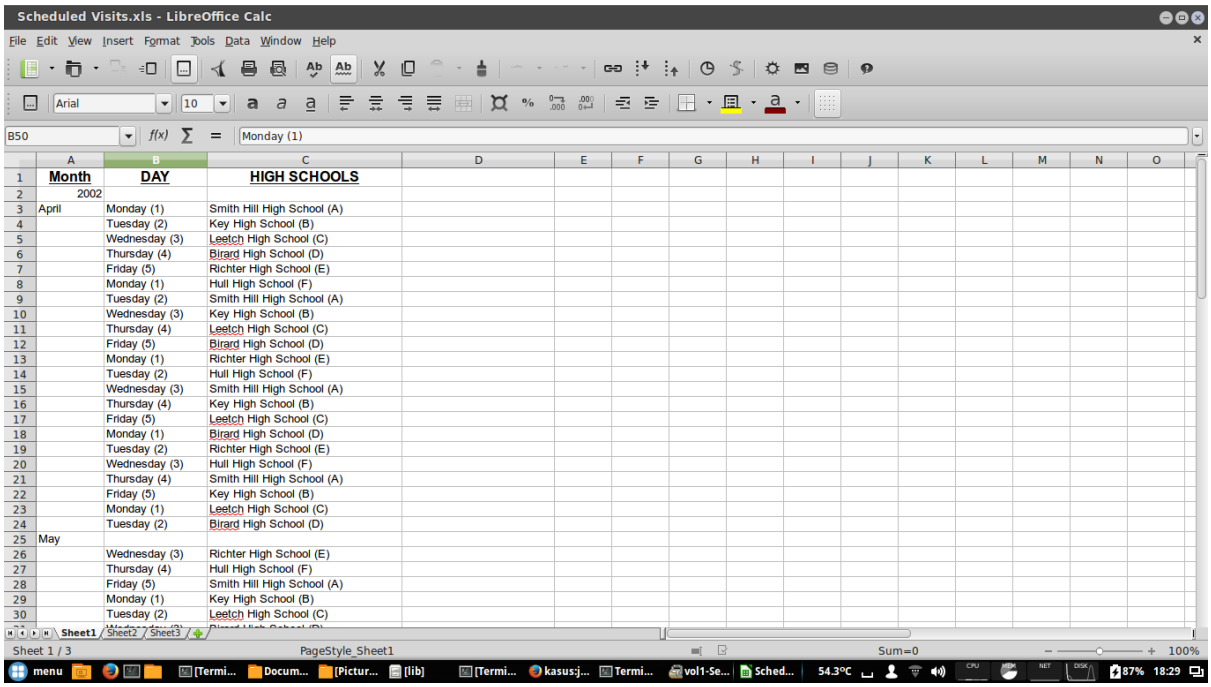
Kode PK adalah jenis format file zip



Kemudian kita ubah nama file yang didownload tadi vol1-sector104.raw menjadi vol1-sector104.zip agar file tersebut dapat dibuka

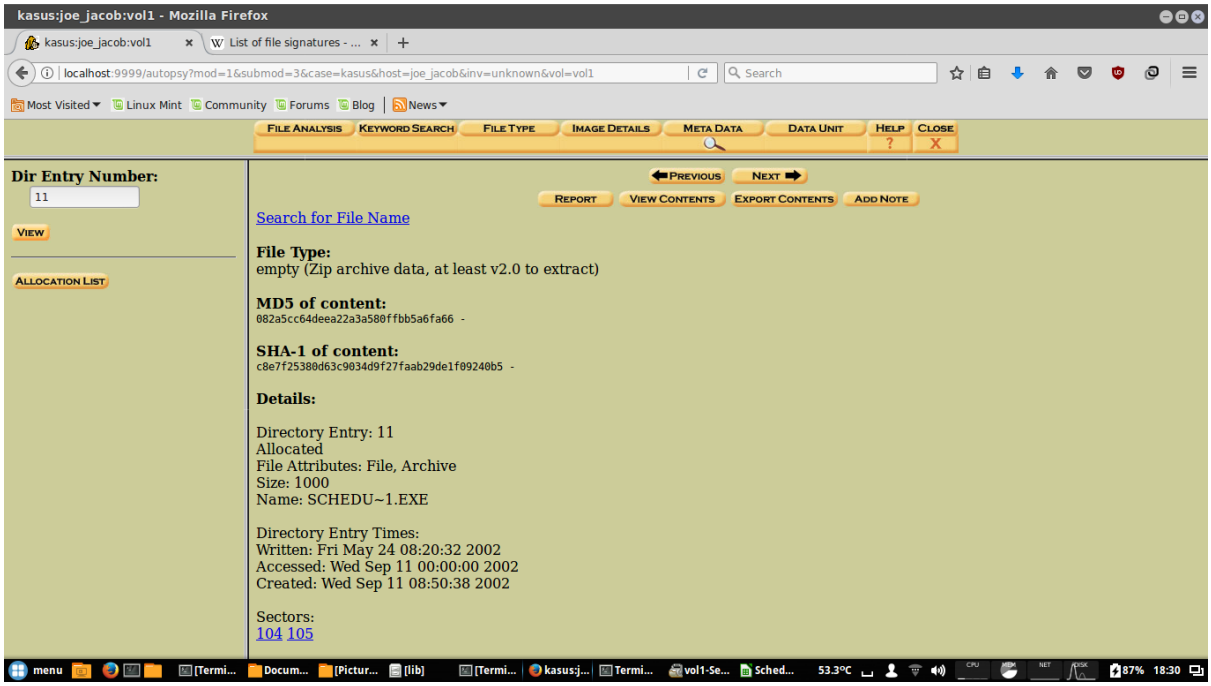


Kemudian kita buka file vol1-sector104.zip, lalu klik scheduled visits.xls, masukkan password yang didapatkan pada perintah strings vol1-sector73.jpg sebelumnya. Password “goodtimes”

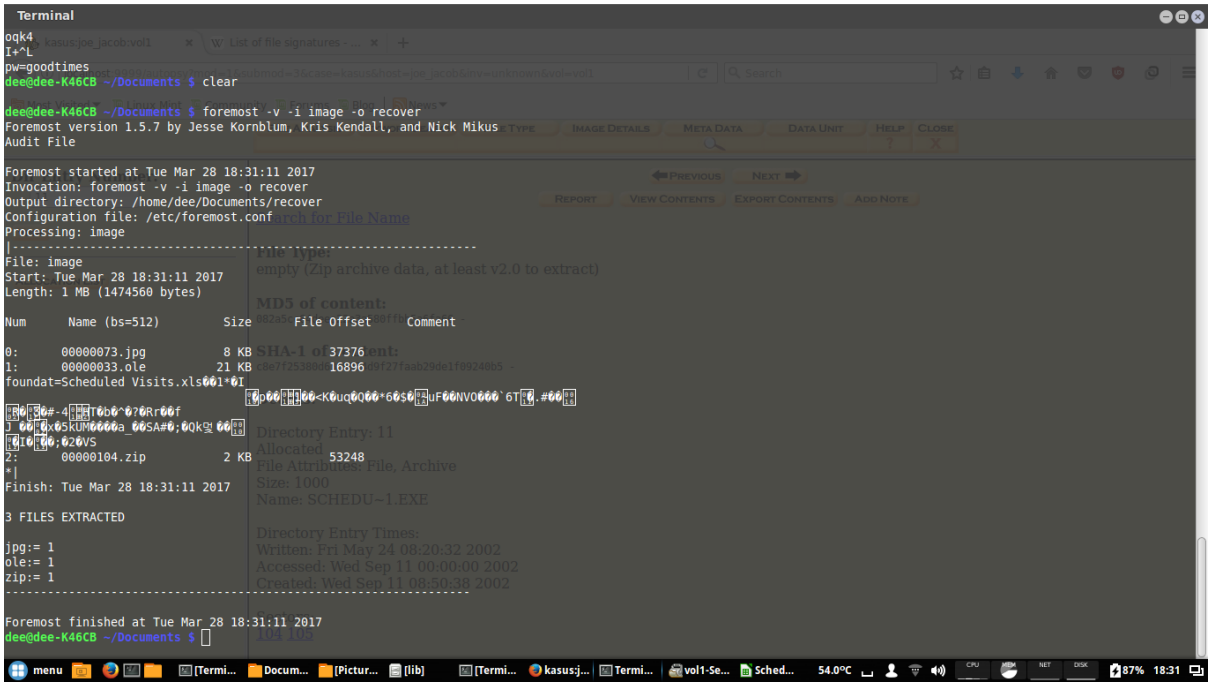


	A	B	C
1	Month	DAY	HIGH SCHOOLS
2	2002		
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith Hill High 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)

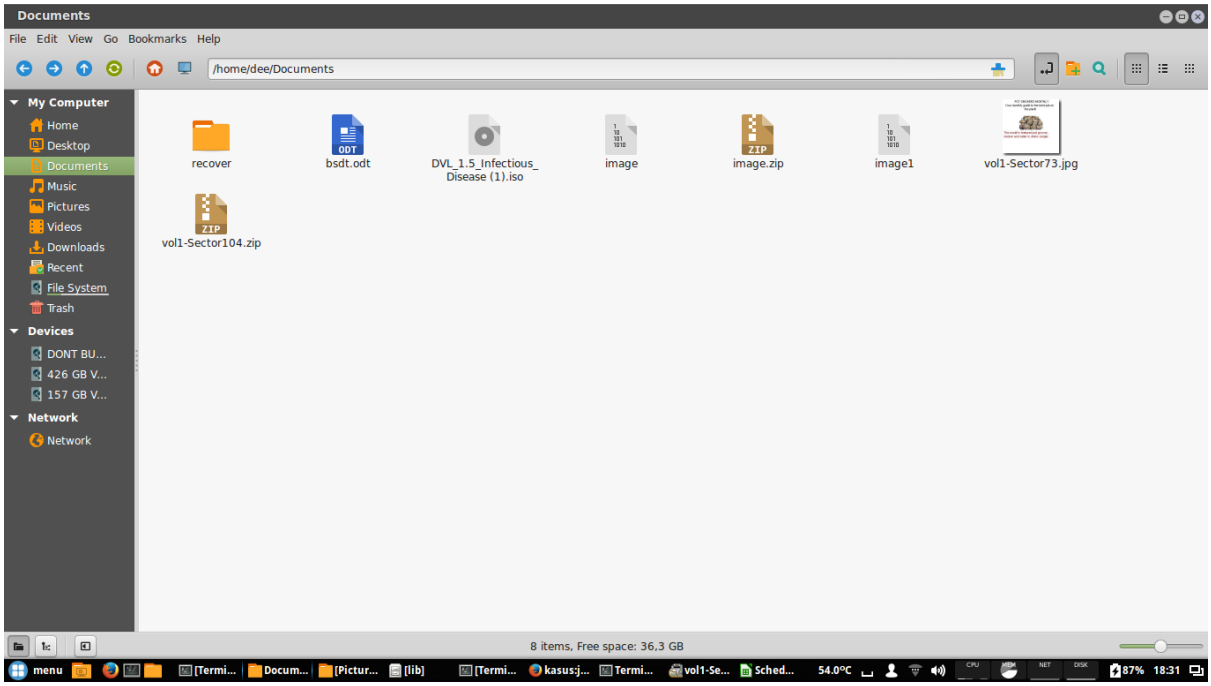
Maka akan terbuka file xls seperti gambar diatas



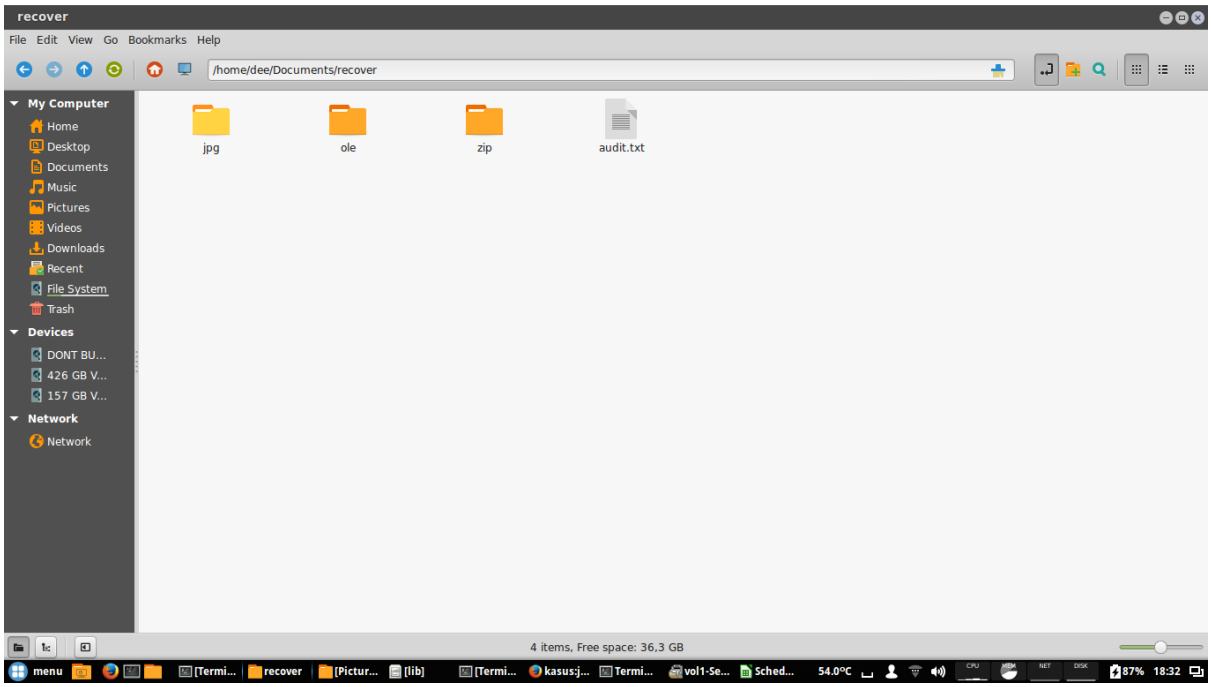
Kemudian kita buka browser kembali, klik tab meta data, dan masukkan dir entry number 11. Akan menampikan tipe file, md5 dari contents, SHA-1 dari contents, dan detail dari gambar tersebut.



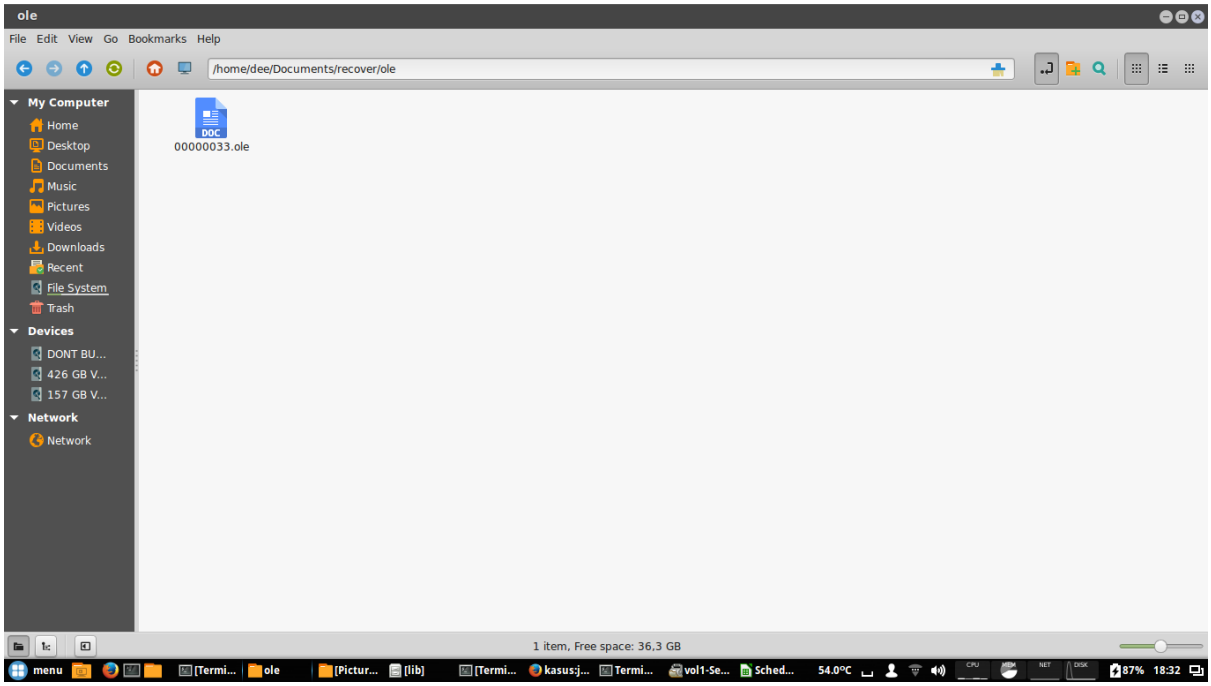
Kemudian buka terminal dengan perintah foremost –v –i image –o recover. Fungsi foremost untuk mengembalikan data yang tertimpa dan recover sebagai ekstrak file image.



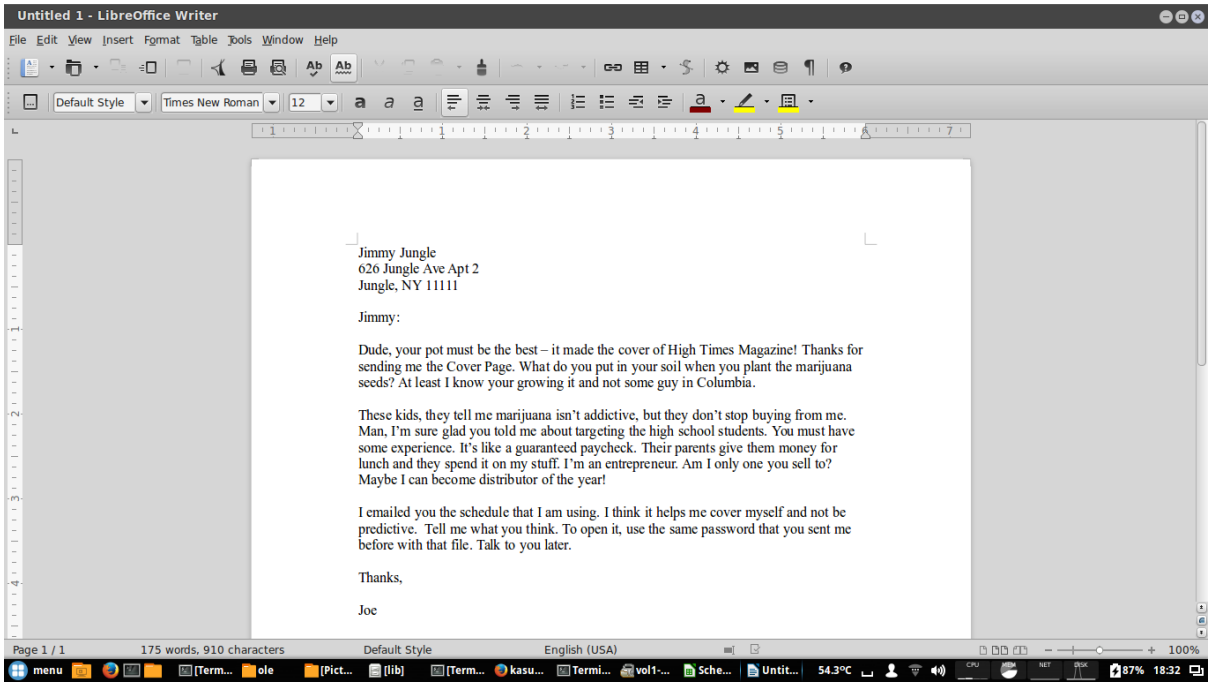
Hasil ekstrak recover foremost dapat dilihat pada gambar diatas dengan folder recover. Kemudian kita buka folder tersebut



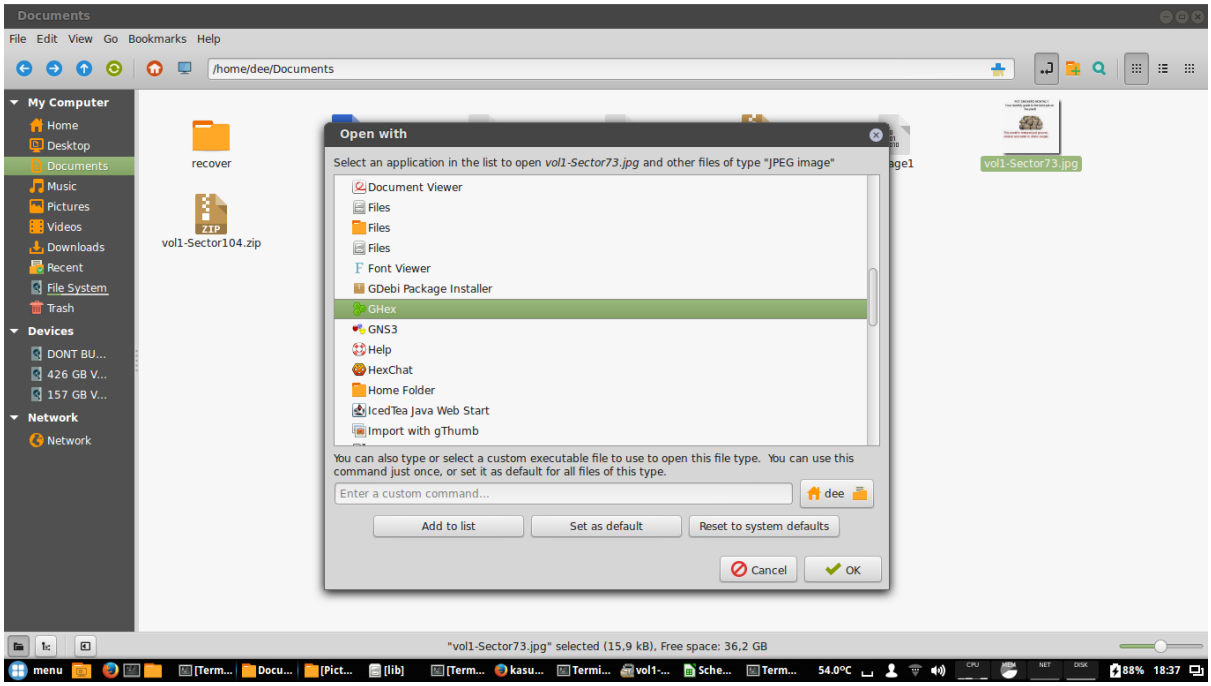
Terdapat folder jpg, ole, zip. Kemudian kita buka folder ole



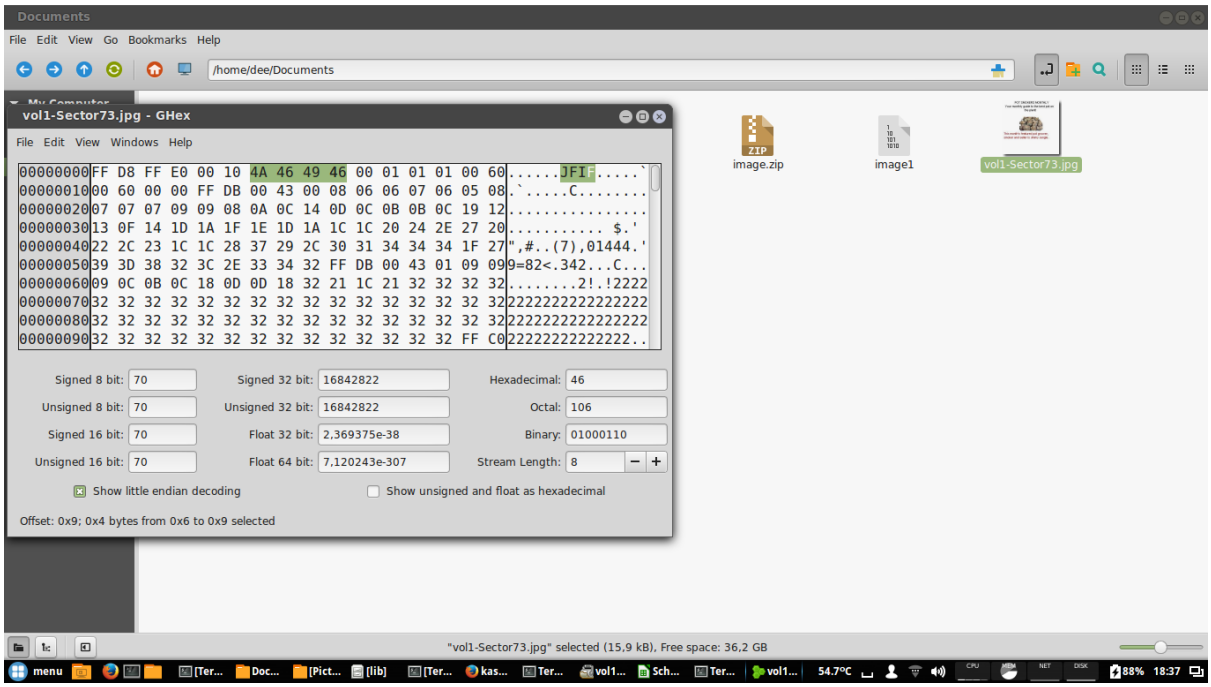
Terdapat file 00000033.ole. lalu buka file tersebut



Setelah terbuka, terdapat file dokumen berupa surat



Lalu buka folder documents kita klik kanan file vol1-sector73.jpg. lalu buka dengan Ghex. Klik ok



Tools ghex berfungsi untuk konversi gambar tersebut menjadi bilangan hex. Dapat ditebali kode JFIF, dapat dilihat bilangan hex dari JFIF yaitu 4A 46 49 46.

Pertanyaan yang diminta sebuah pemecahan kasus narkoba tersebut :

1. **Siapa pemasok narkoba joe jacob dan alamatnya?**

Jimmy jungle, dengan alamat 626 Jungle Ave Apt 2, Jungle, NY 11111

2. **Data penting apa yang terdapat di file coverage.jpg dan mengapa data tersebut penting ?**

Data penting berupa password, dikarenakan coverage.jpg atau vol1-sector73.jpg memberikan sebuah password untuk membuka file zip (vol1-sector104.zip) yang berupa dokumen jadwal kunjungan pengedar narkoba / scheduled visits.xls

3. **Nama sekolah selain smith hill yang sering menjadi tempat transaksi joe jacob?**

Smith Hill High School (A), Key High School (B), Leetch High School (C) , Birard High School (D), Richter High School (E), Hull High School (F)

4. **Untuk setiap file, proses apa yang diambil oleh tersangka untuk mengelabuhi orang lain ?**

Tersangka merubah file-file vol1-sector73.jpg dan vol1-sector104.zip menjadi format .raw dan tersangka menyembunyikan sebuah password untuk membuka vol1-sector104.zip pada gambar vol1-sector73.jpg

5. **Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file ?**

Penyidik melakukan pencarian data-data yang dianggap penting dalam mengungkapkan kasus ini, dan melakukan analisa data-data yang didapatkan, pada data yang didapat berupa file image, penyidik menggunakan tools berupa autopsy, foremost, strings, dan ghex yang berfungsi untuk menganalisa sebuah file yang nanti nya menjadi sebuah bukti dalam kasus ini. Dan terungkap ada file yang penting berupa jadwal pengedaran narkoba pada sekolah-sekolah yang menjadi target penjualan, dan surat dari pengedar narkoba(joe_jacob) untuk pemasok narkoba(jimmy jungle).