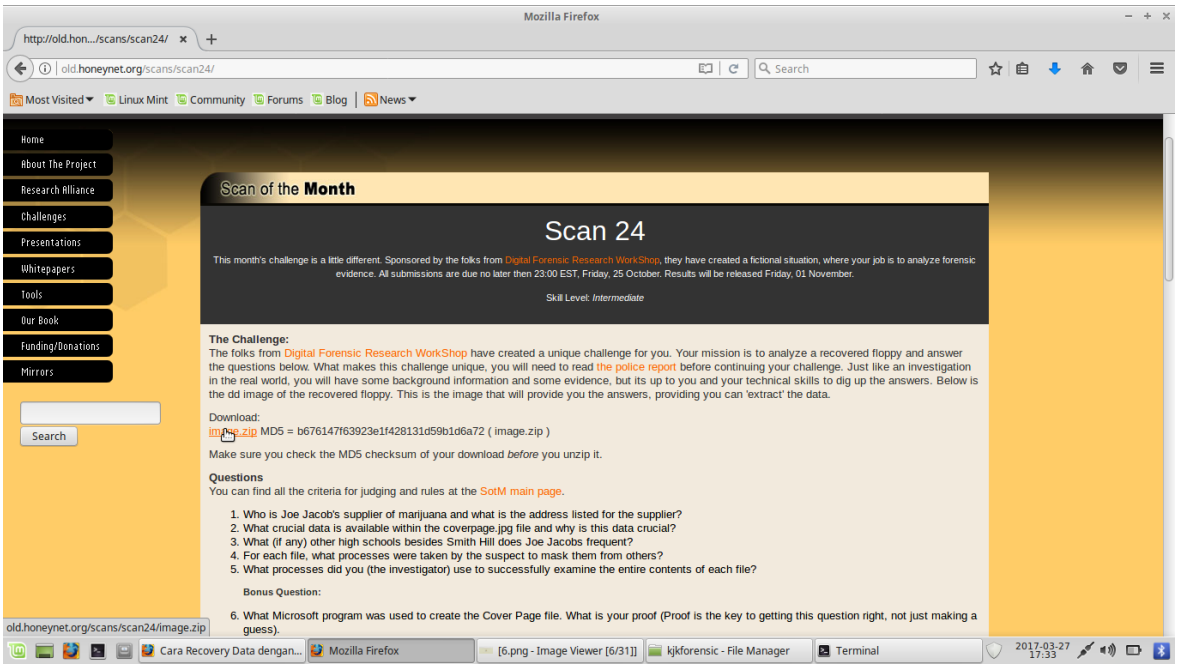
Nama : Muhammad Fachrurroji Ilham Saputra

Nim : 09011181320025

Computer Forensics

Penyelesaian langkah-langkah investigasi dari kasus yang telah diberikan, dengan langkah-langkah simulasi yang dilakukan dalam penyelesaian kasus narkoba tersebut sebagai berikut:

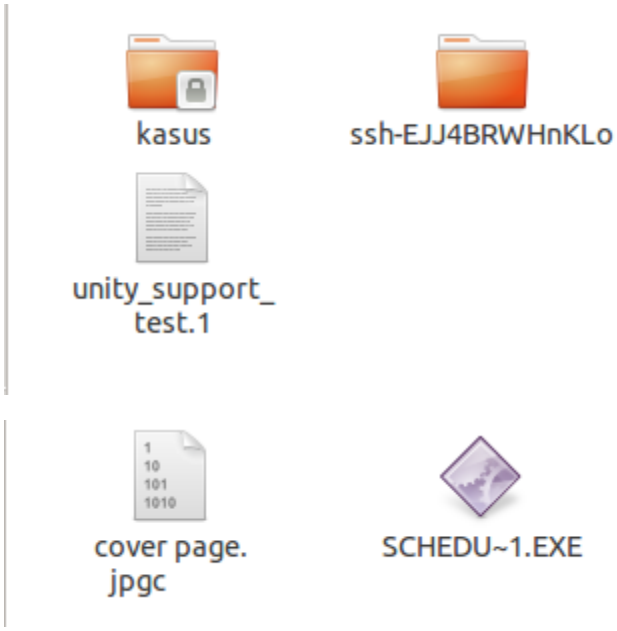


Fungsi perintah di bawah : untuk mengecek tipe file. Jika kita menenmukan file yang tidak ada ekstensi, maka kita bisa menggunakan.

```
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#
```

Gambar dibawah adalah hasil dari file system dalam folder yang telah dibuat dengan perintah mount image /tmpt/kasus.

```
root@mahasiswa:/home/mahasiswa/Downloads# mount image /tmp/kasu
s
```

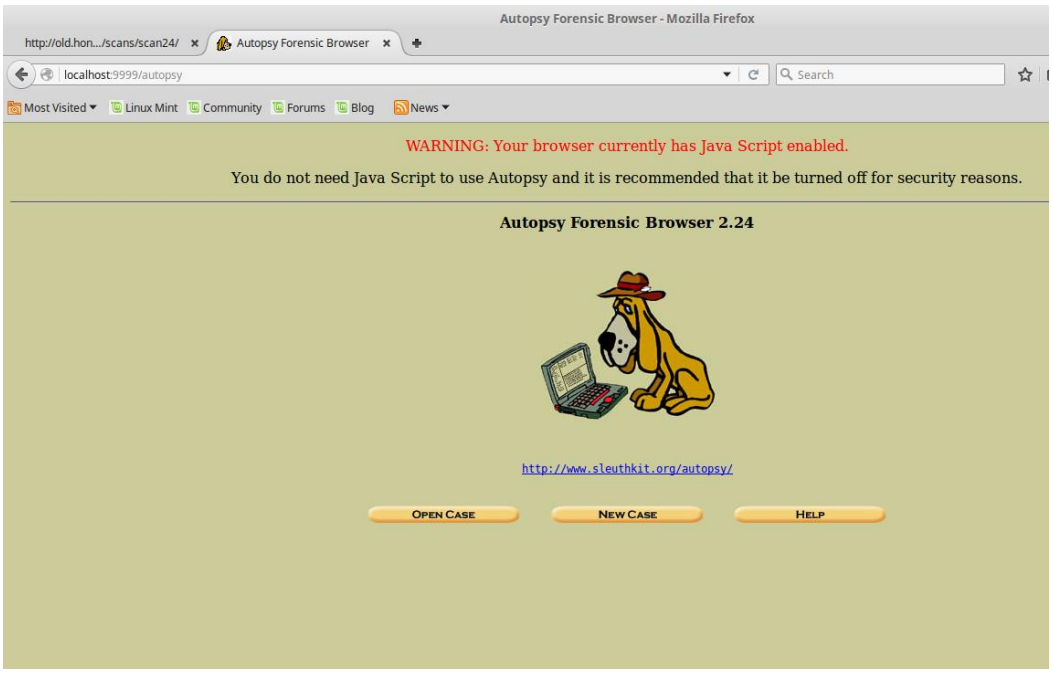


File yang ada dalam folder pada gambar diatas tmp/kasus/ dengan hasil mounting dari file image tersebut, untuk melakukan pengecekan utilitas file dengan perintah file *, yang berarti untuk mengecek semua utilitas dari file yang ada didalam folder kasus tersebut. Terlihat pada gambar dibawah perintahnya

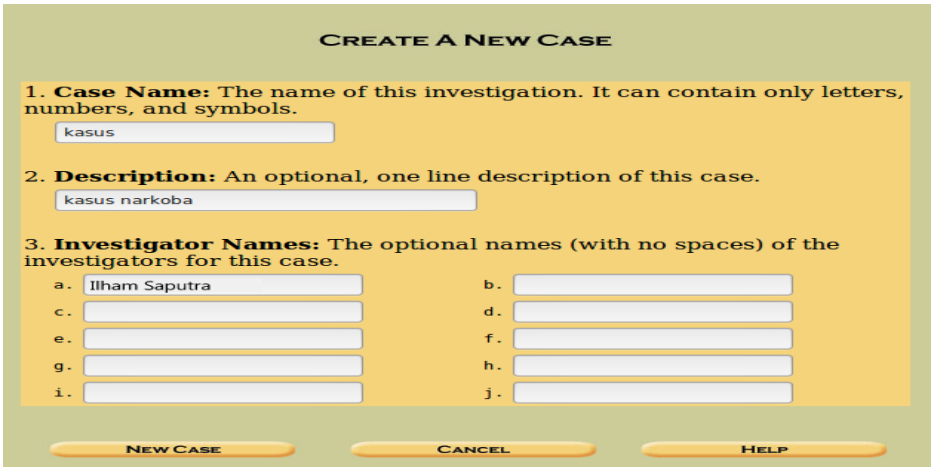
```
root@mahasiswa:/home/mahasiswa/Downloads# cd /tmp/kasus
root@mahasiswa:/tmp/kasus# ls
cover page.jpgc             SCHEDU~1.EXE
root@mahasiswa:/tmp/kasus#
```

```
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#
```

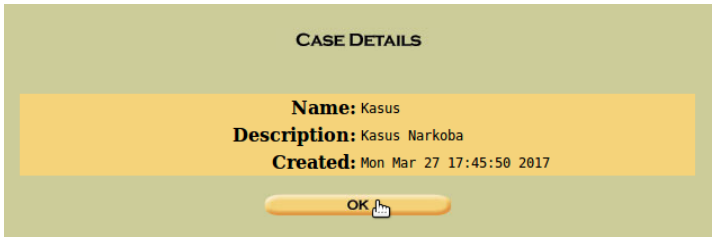
Langkah selanjutnya yaitu dengan menjalankan tools autopsy dan membuka local host dengan alamat localhost:9999/autopsy.



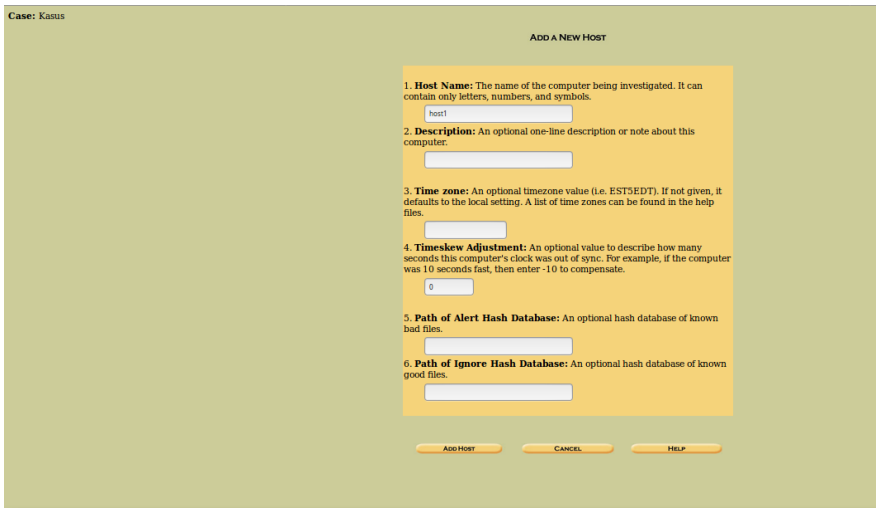
Setelah itu mengisi form yang ada pada gambar dibawah untuk menyelesaikan kasus yang diminta.

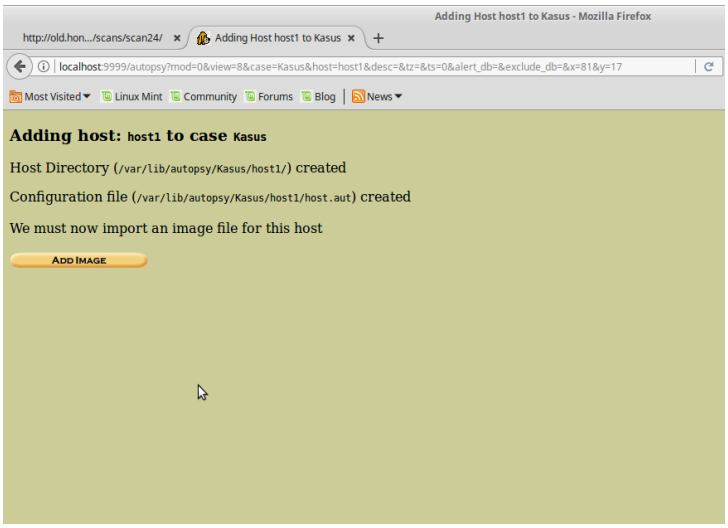


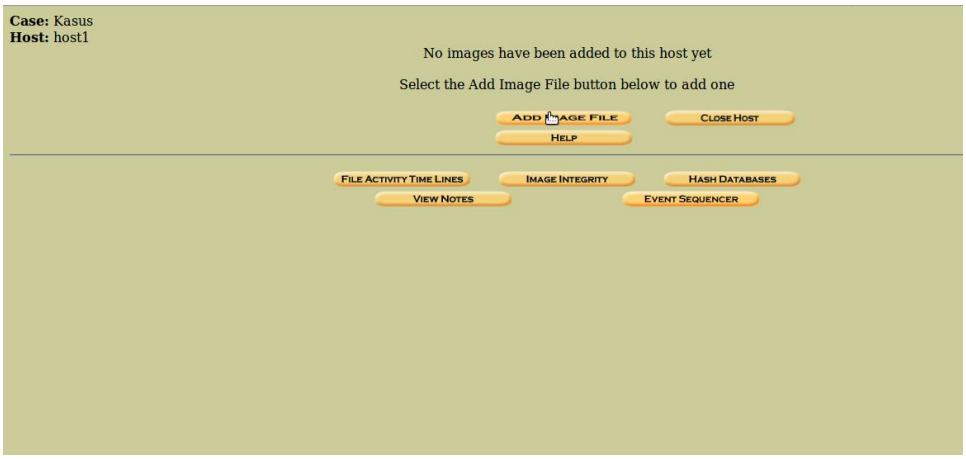
Maka akan muncul nama kasus yang telah kita isi tadi



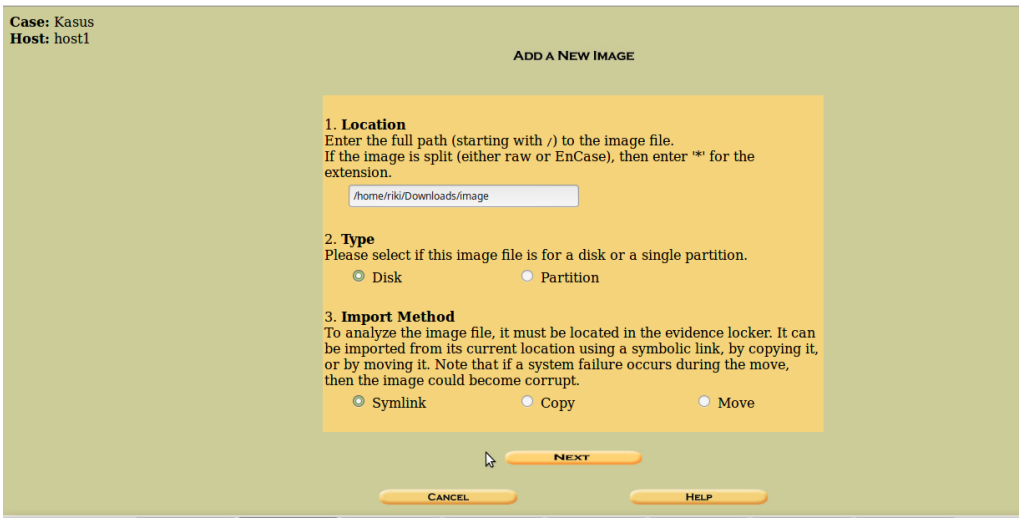
Setelah itu kita membuat kasus baru yang akan diselesaikan maka akan menampilkan dialog box yang dapat kita isi dengan menggunakan tools aoutospy untuk mengimport image yang akan diinvestigasi. Pada gambar dibawah contoh langkah – langkah yang dilakukan



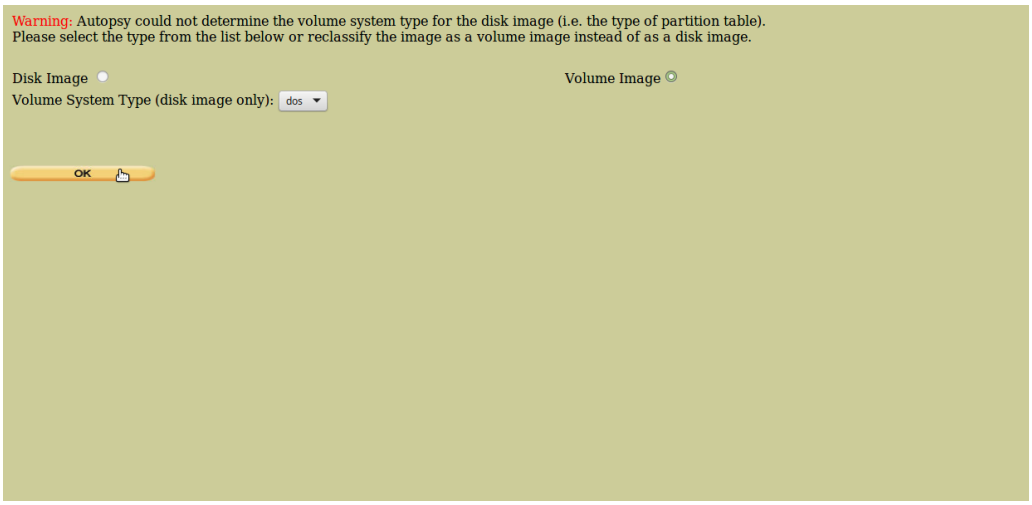


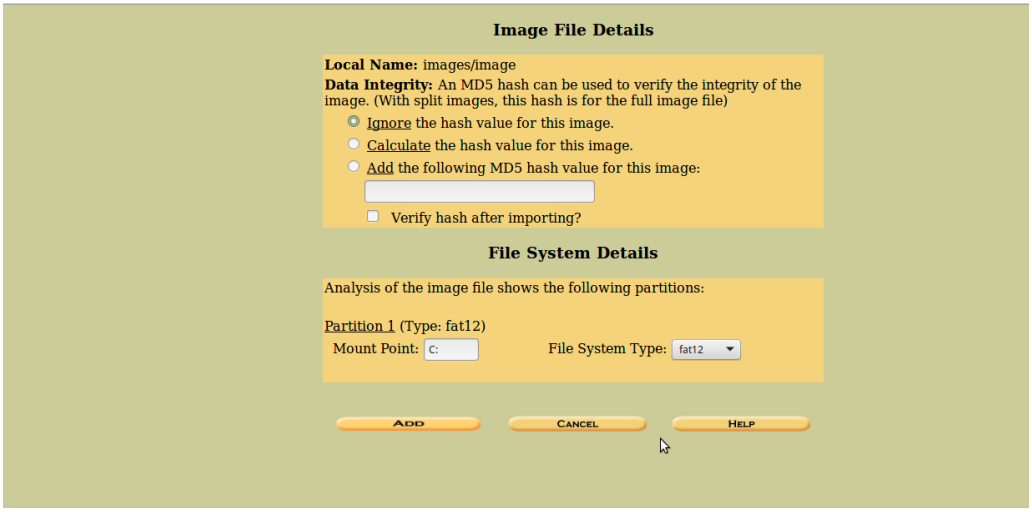


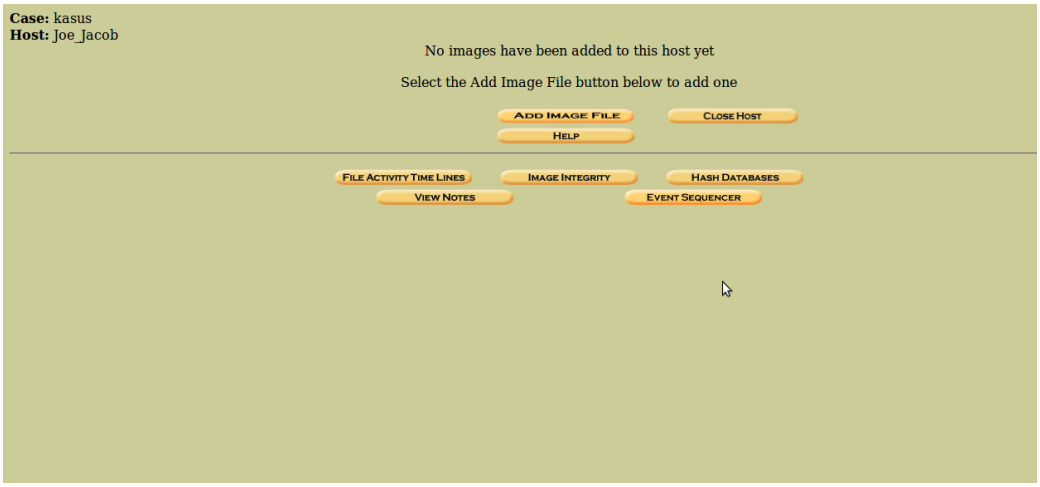
Setelah melewati bagian dari dialog box diatas maka langkah selanjutnya memasukkan alamat dari file image yang akan diinvestigasi pada gambar dibawah



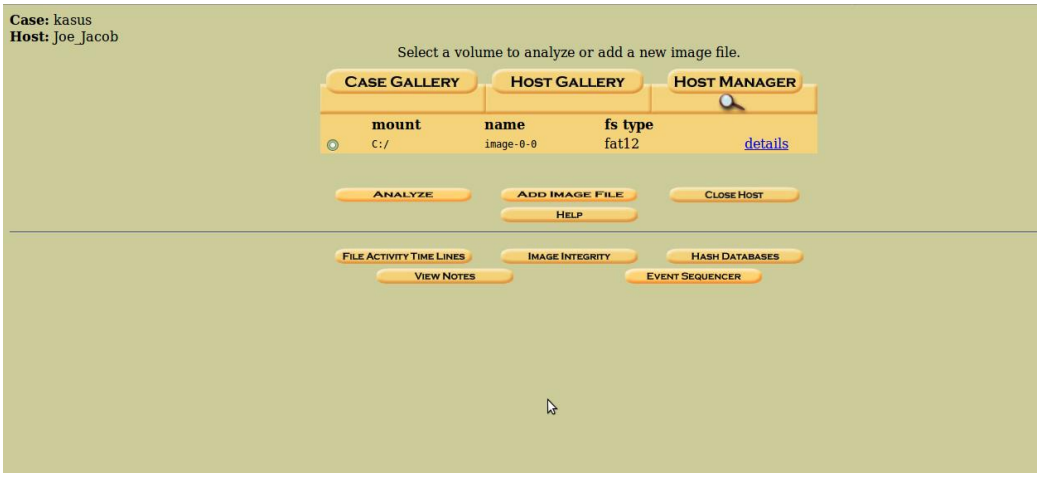
Terdapat langkah – langkah sebagai berikut yang akan mengarahkan keberhasilan dari file yang diupload kedalam tools autopsy untuk dilakukan forensic dari kasus narkoba untuk mencari informasi yang ada.



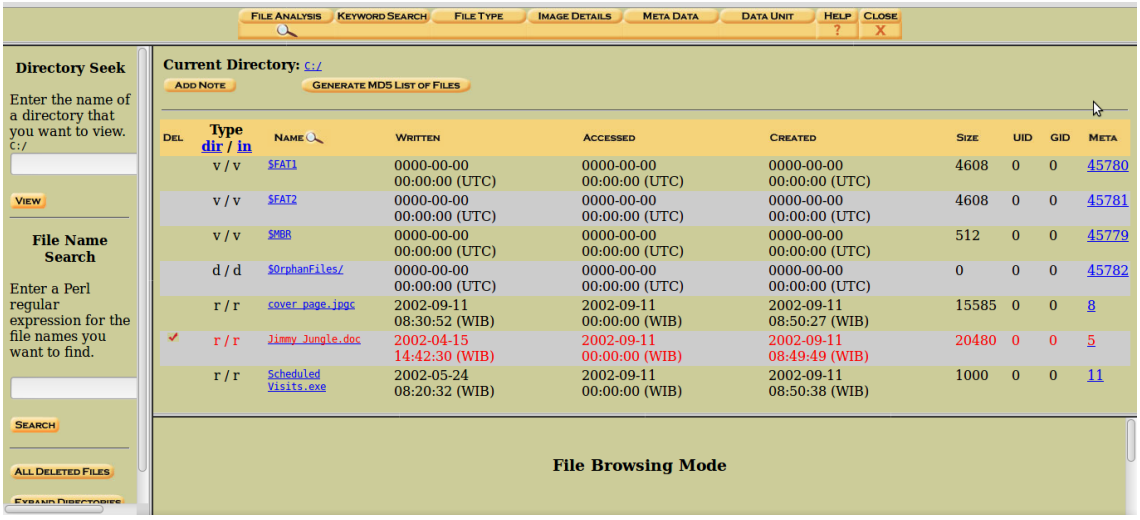




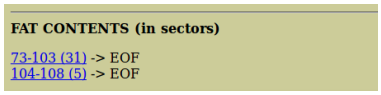
Pada gambar dibawah menunjukkan kasus yang telah dimasukkan dalam tools aoutospy dengan nama kasus yaitu kasus dan nama hostnya ialah Joe_Jacob.



Kemudian dari kasus yang telah dimasukkan lakukan analisa dengan mengklik tombol analyse, gambar dibawah merupakan isi dari informasi yang dimiliki oleh hardrive, dengan menampilkan hasil seperti pada gambar dibawah.

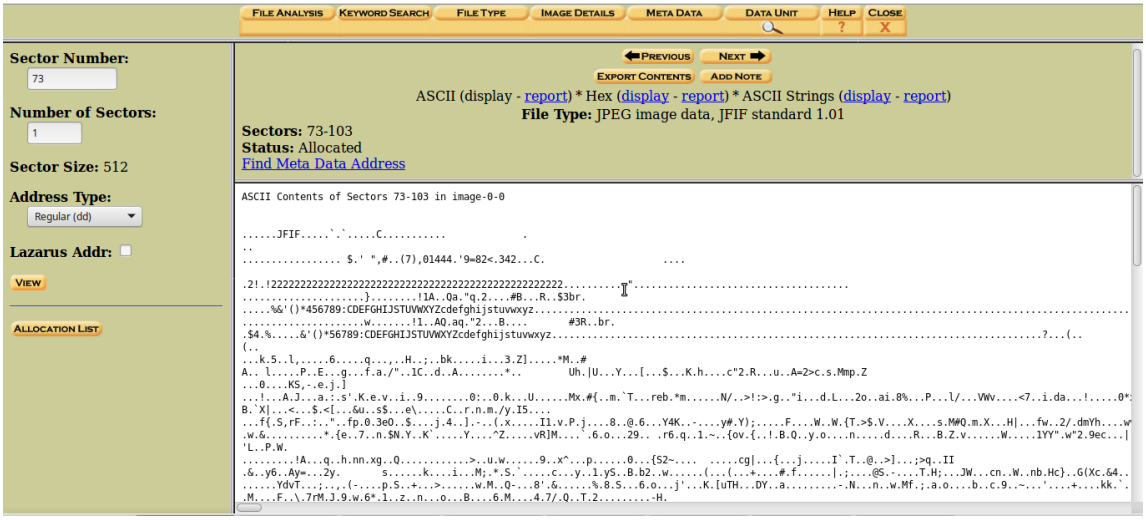


Pada gambar diatas terdapat list yang berwarna merah, yang merupakan isi dari list tersebut filenya sudah dihapus.



Dua file yang ada diatas merupakan jejak yang ditinggalkan dalam kasus narkoba, dengan nama file 73-103 (31) dengan maksud yaitu informasi yang disembunyikan didalam sector 73 sampai

dengan sektor 103 , begitu pula dengan yang kedua 104-108 (5) terdapat informasi yang disembunyikan dalam sector 104 sampai 108.

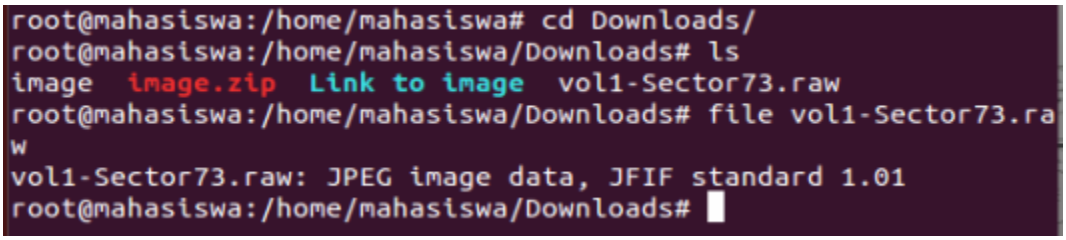


Gambar diatas menampilkan detail dari file 73-103 (31) dengan informasi yang dapat diambil yang terdapat pada baris pertama yaitu JFIF.

setelah informasi dari gambar diatas dapat dilihat dengan jelas, dengan mencari secara manual informasi di list of file singnature (wikipedia) seperti yang terilihat pada gambar dibawah, dan juga untuk file yang ada pada sector 104-108 (5).

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
ilbm lbm ibm	IFF Interleaved Bitmap Image	0 any	FORM.... ILBM	46 4F 52 4D nn nn nn nn 49 4C 42 4D

Jalankan perintah dibawah untuk mengecek utilitas dari file dengan sector 104-108 seperti pada gambar dibawah.



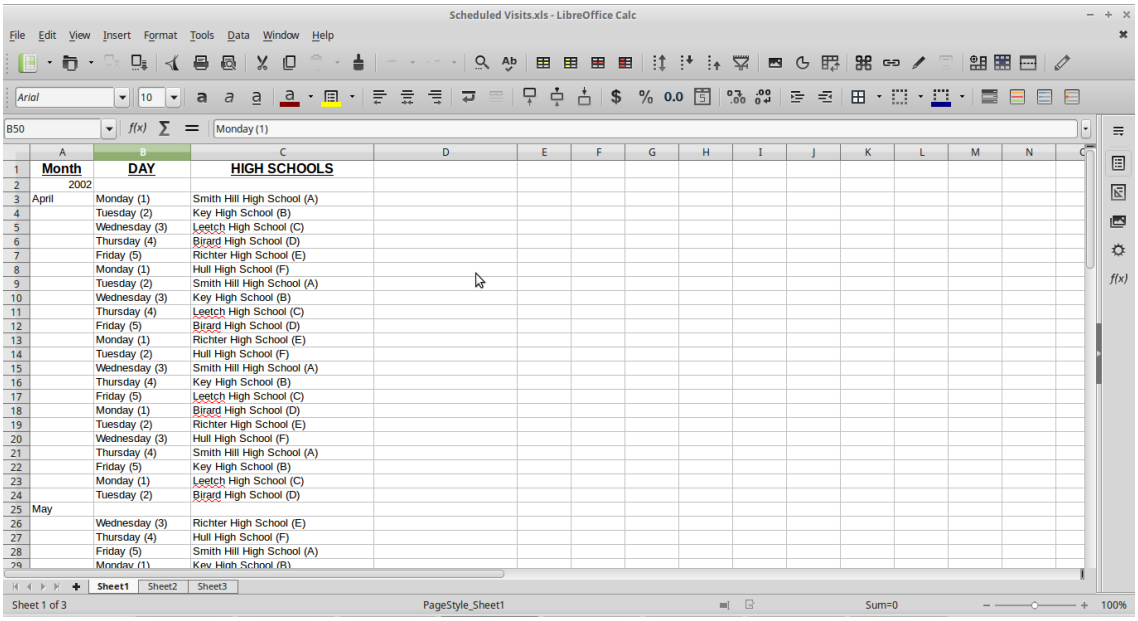
Dengan melakukan pengecekan utilitas dari file sector 104-108 (51) dengan nama file vol1-Sector73.raw, maka dapat dilakukan pencarian list of file signature (wikipedia) seperti pada gambar dibawah.

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 (spanned archive)
rar	RAR archive version 1.50 onwards[8]	0	Rar!...	52 61 72 21 1A 07 00

Untuk mendapatkan password dari file sector yang disimpan oleh pelaku kita menggunakan tools strings dan contoh perintahnya ada pada gambar dibwah.

```
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#
```

Dari hasil srtings diatas kita dapat mengetahui password yang disimpan oleh pelaku kedalam file sector pertama dengan password yang diperoleh ialah goodtimes yang dapat digunakan untuk membuaka file zip yang merupakan file sector kedua, dengan hasil terlihat pada gambar dibawah.



	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)

kasus ini juga dapat dipecahkan dengan menggunakan tools foremost, tools yang berfungsi berfungsi sebagai pengubah file tersebut menjadi folder, yang didalamnya terdapat informasi-informasi yang dibutuhkan, dengan perintah foremost –v –i nama_file –o recover, pada terminal, seperti yang terlihat pada gambar dibawah.

```
root@mahasiswa:/home/mahasiswa/Downloads# foremost -v -i image
-o recover
```

Folder yang aka nada didalam recover nantinya merupakkan informasi yang dibutuhkan dalam menangani kasus narkoba, contohnya untuk file yang ada didalam folder doc, berisi file 0000003.doc dengan info didalamnya yaitu surat dari pengedar narkoba dikasus tersebut, terlihat pada gambar dibawah.

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe