TUGAS

“KEAMANAN JARINGAN KOMPUTER”

Disusun Oleh :

Nama : Nova Dyati Pradista

Nim : 09011181320005

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

“Computer Forensik”

Tujuan dan Fokus Komputer Forensik :

Tujuan :

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

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.

Fokus data yang di kumpulkan di bagi menjadi 3 kategori :

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

Kasus :

Telah tertangkap seorang pengedar narkoba kelas kakap, polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta bantuan oleh polisi untuk melakukan forensic terhadap file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut.

kita di minta bantuan untuk mendapatkan beberapa informasi di bawah

1.Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

2.What crucial data is available within the coverpage.jpg file and why is this data crucial?

3.What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?

4.For each file, what processes were taken by the suspect to mask them from others?

5.What processes did you (the investigator) use to successfully examine the entire contents of each file?

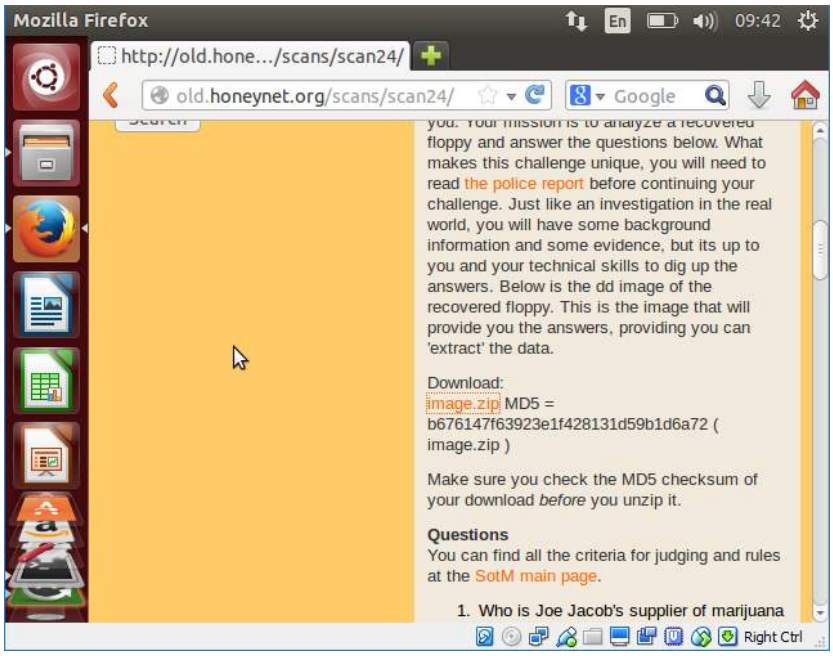
Tools yang digunakan adalah :

- AutoPsy
- Foremost
- Strings

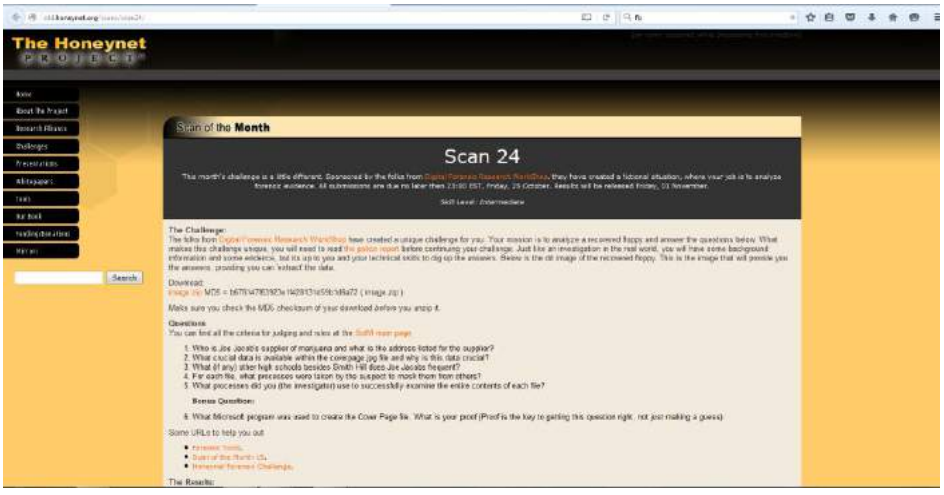
Langkah kerja :

Install tools, selain strings.

Buka website http://old.honeynet.org/scans/scan24,

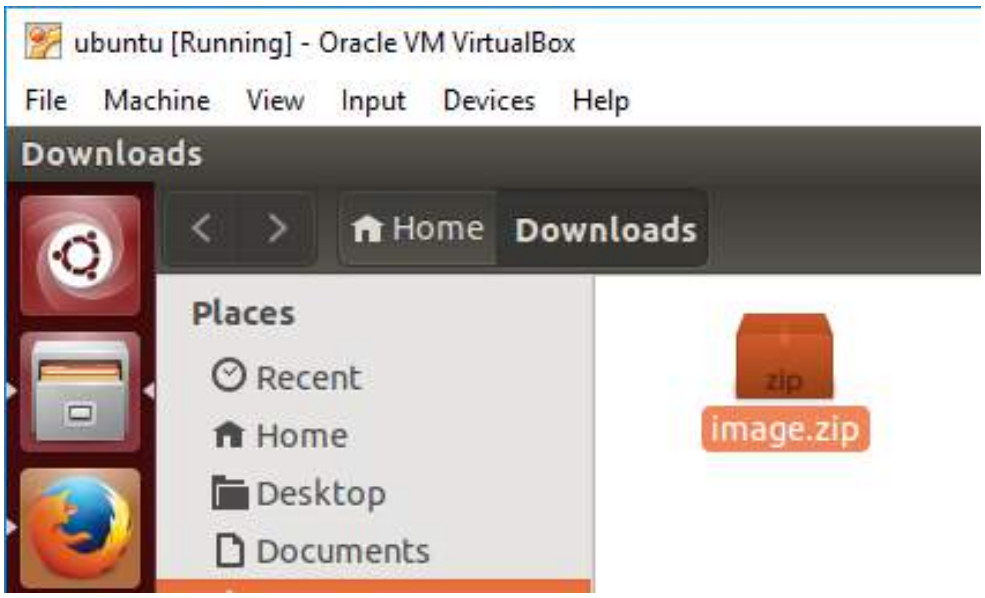


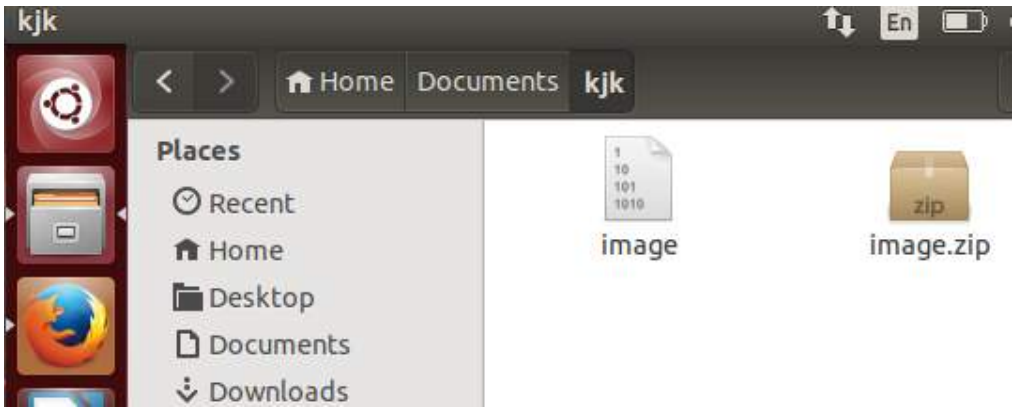
Maka akan tampil halaman website seperti gambar dibawah ini



Setelah itu download file dengan extention zib, dengan nama image.zib yang akan digunakan kemudian lakukan perintah md5sum image.zip untuk mengecek keaslian dari file atau integritas file yang telah didownload tadi.

```
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#
```

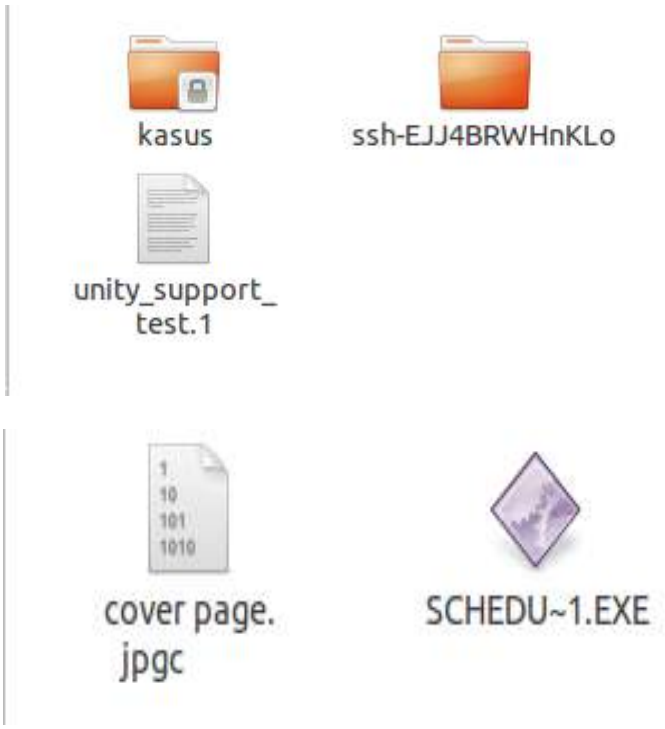




Setelah itu buat folder baru didalam folder tmp. Letakkan hasil mount dalam file system dalam folder yang telah dibuat dengan perintah mount image /tmp/kasus

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

Maka akan tampil hasil mounting dari perintah diatas



Setelah itu file yang ada di dalam folder tmp/kasus/ dengan hasil mounting dari file image tersebut akan dilakukan pengecekan utilitas file dengan perintah file *, yang artinya mengecek semua utilitas dari file yang ada didalam folder kasus tersebut.

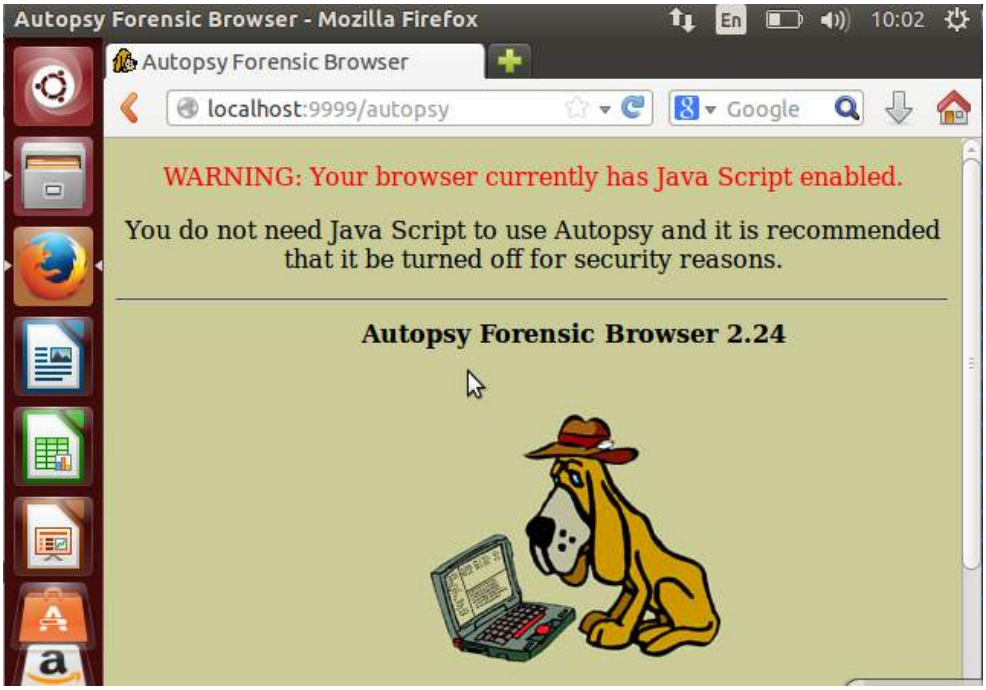
```
root@mahasiswa:/home/mahasiswa/Downloads# cd /tmp/kasus
root@mahasiswa:/tmp/kasus# ls
cover page.jpgc              SCHEDU~1.EXE
root@mahasiswa:/tmp/kasus#
```

```
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#
```

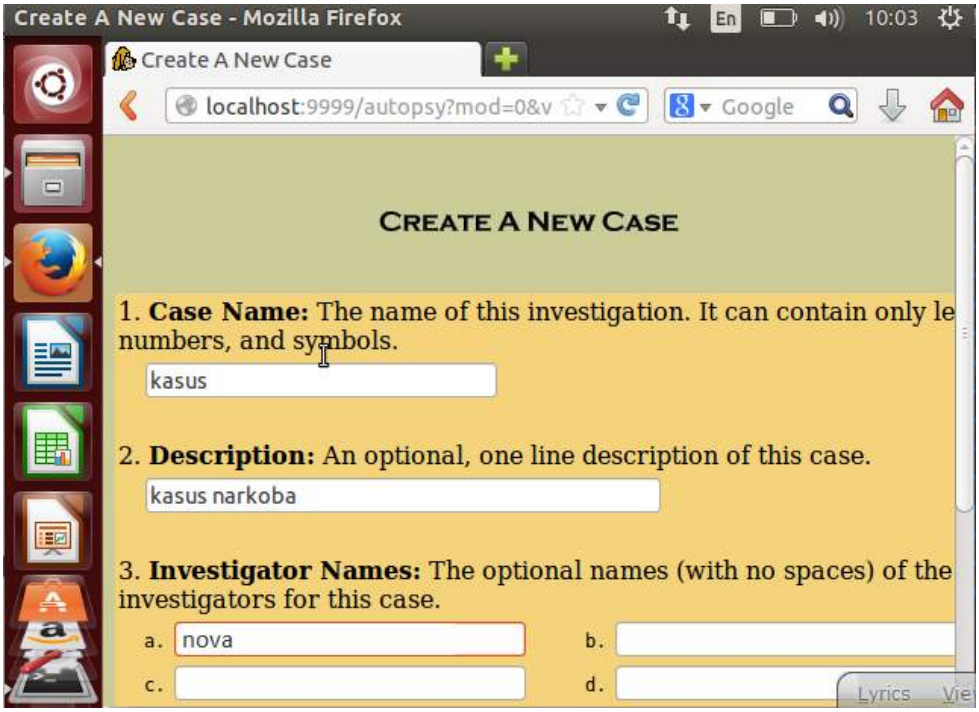
Selanjutnya lakukan perintah autopsy untuk mengatur hostname dan siapa saja yang melakukan forensik pada komputer target

```
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
```

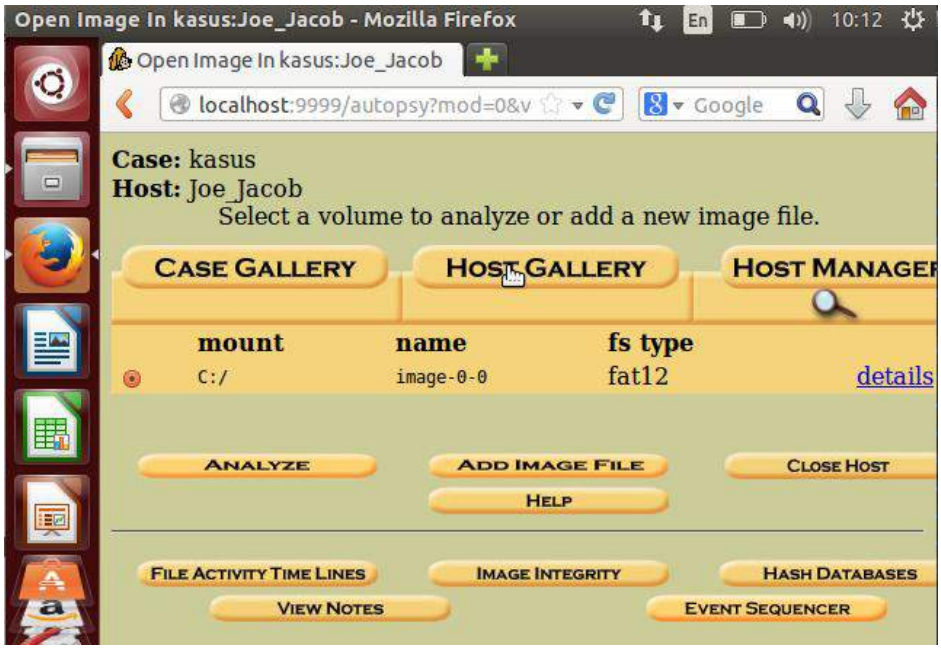
Setelah itu buka localhost dari tools The Autopsy Forensic dengan alamat localhost:9999/autopsy yang merupakan antarmuka grafis untuk tool analisis investigasi digital dengan perintah baris The Sleuth Kit, yang dapat menganalisis disk dan filesistem Windows dan UNIX (NTFS, FAT, UFS1/2, Ext2/3). Lalu akan tampil halaman depan tools autopsy seperti gambar dibawah ini



Setelah membuka alamat localhost dari tools autopsy tersebut, selanjutnya lakukan pengisian form dengan mengetikkan case name kasus, description kasus narkoba dan investigator names nova

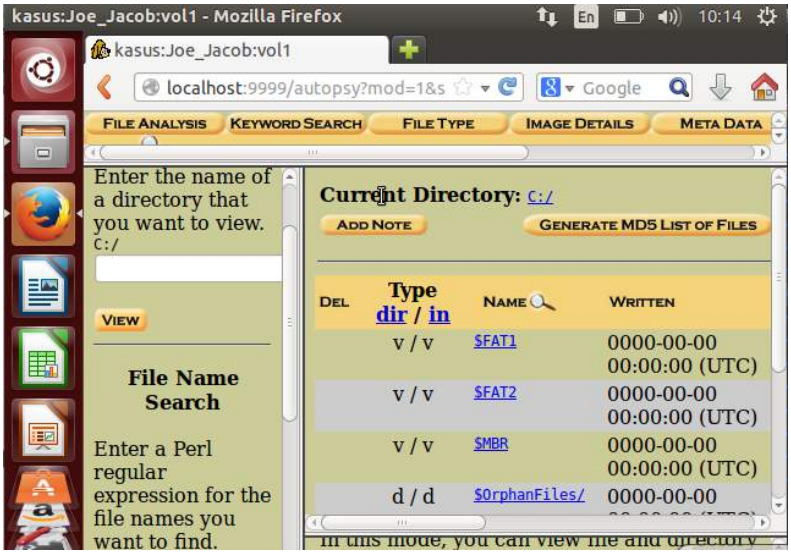


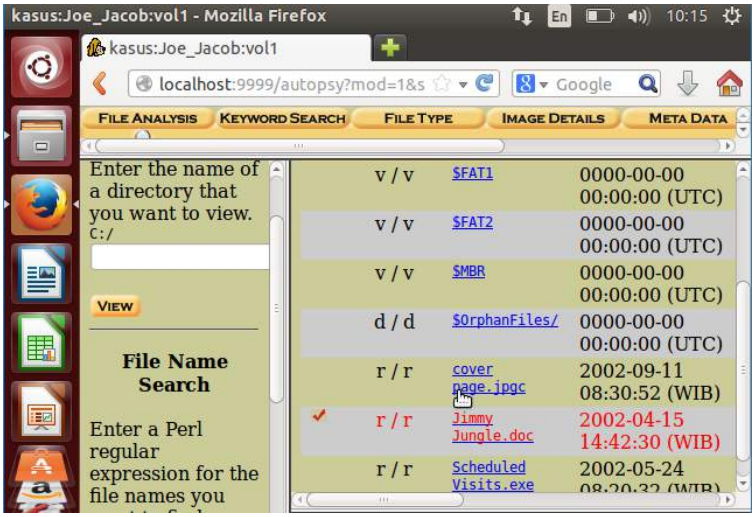
Selanjutnya akan menampilkan kasus yang telah dibuat dalam tools autopsy dengan nama kasus nya adalah kasus dan hostnya adalah Joe_Jacob.

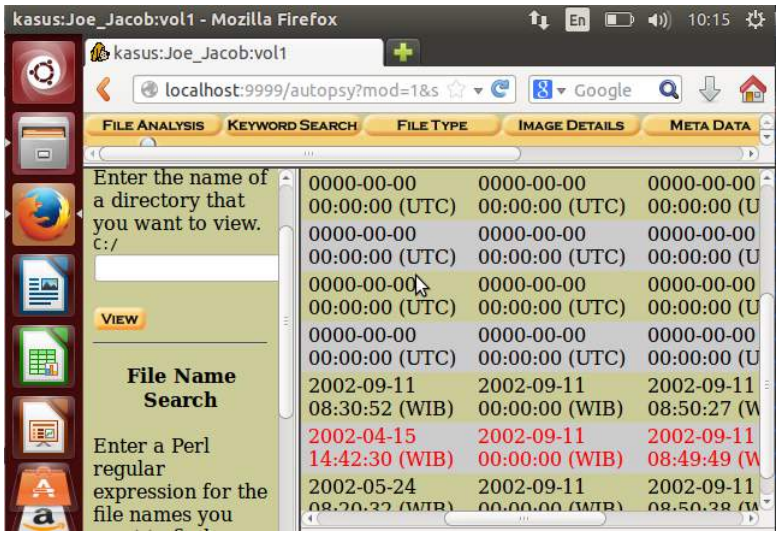


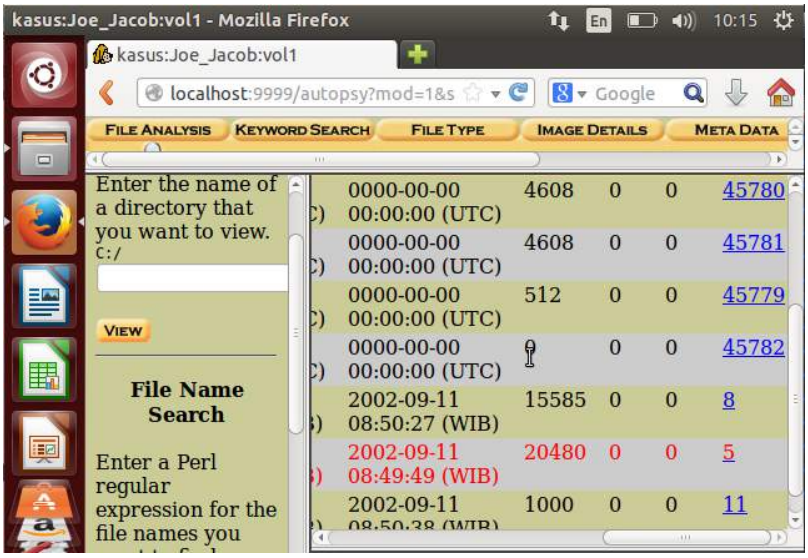
Kemudian dari kasus yang telah dimasukkan lakukan analisa dengan mengklik file analysis. Dapat dilihat bahwa isi dari informasi yang dimiliki oleh hardrive tersebut, yang

dapat dilihat dimana terdapat banyak kegiatan yang dilakukan, yang dimulai dari waktu palaku menulis, mengakses dan membuat file, juga terdapat tulisan dengan huruf berwarna merah yang memiliki arti bahwa isi dari list tersebut filenya sudah dihapus.

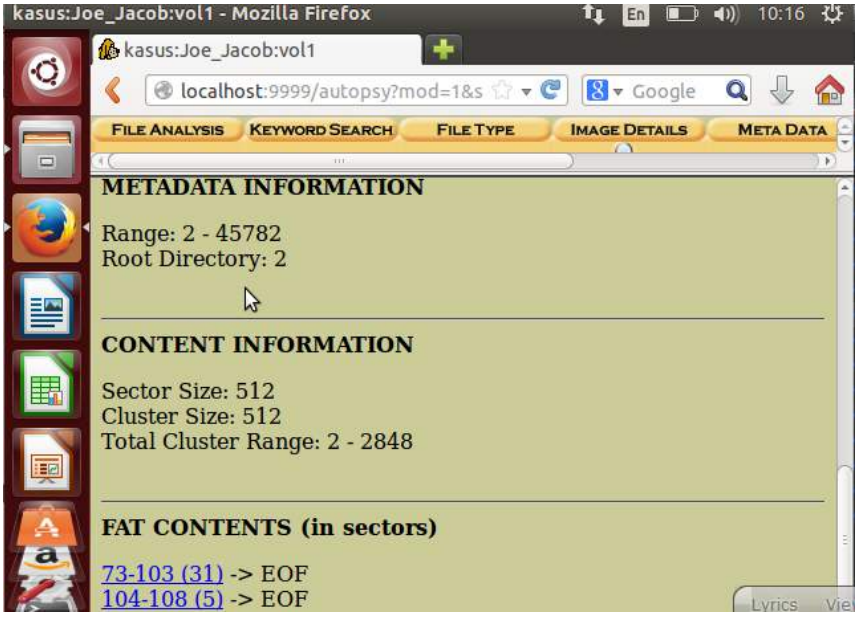




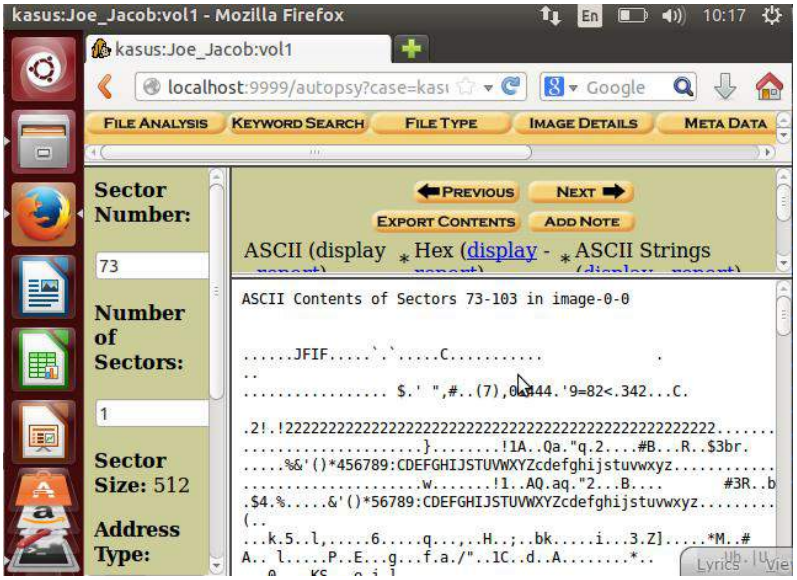




Terdapat dua file yang dapat didownlaod tersebut dengan nama file 73-103 (31) yang dimana di dalam file tersebut terdapat informasi yang disembunyikan didalam sector 73 sampai dengan sektor 103 , begitu pula dengan nama file 104-108 (5) terdapat informasi yang disembunyikan dalam sector 104 sampai 108. Pada sector 73-103 (31) yang dapat dilihat pada gambar dibawah ini, terdapat format yang sangat asing sehingga sulit untuk dimengerti.



Gambar dibawah ini menampilkan detail dari file 73-103 (31) dengan informasi yang dapat diambil yang terdapat pada baris pertama yaitu JFIF , dan kemudian informasi tersebut dapat dilihat dengan jelas, dengan mencari secara manual informasi di list of file singnature (wikipedia), dan Begitu pula sebaliknya untuk file yang ada pada sector 104-108 (5)



Selanjutnya file dengan sector 73-103 (31) dengan analisa format yang diperoleh ialah format JFIF tersebut adalah file dengan format JPEG, hal ini digunakan pelaku untuk menyembunyikan gambar dengan merubah format dari gambar tersebut menjadi raw.

```
root@mahasiswa:/home/mahasiswa# cd Downloads/
root@mahasiswa:/home/mahasiswa/Downloads# ls
image  image.zip  Link to image  vol1-Sector73.raw
root@mahasiswa:/home/mahasiswa/Downloads# file vol1-Sector73.ra
w
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
root@mahasiswa:/home/mahasiswa/Downloads#
```

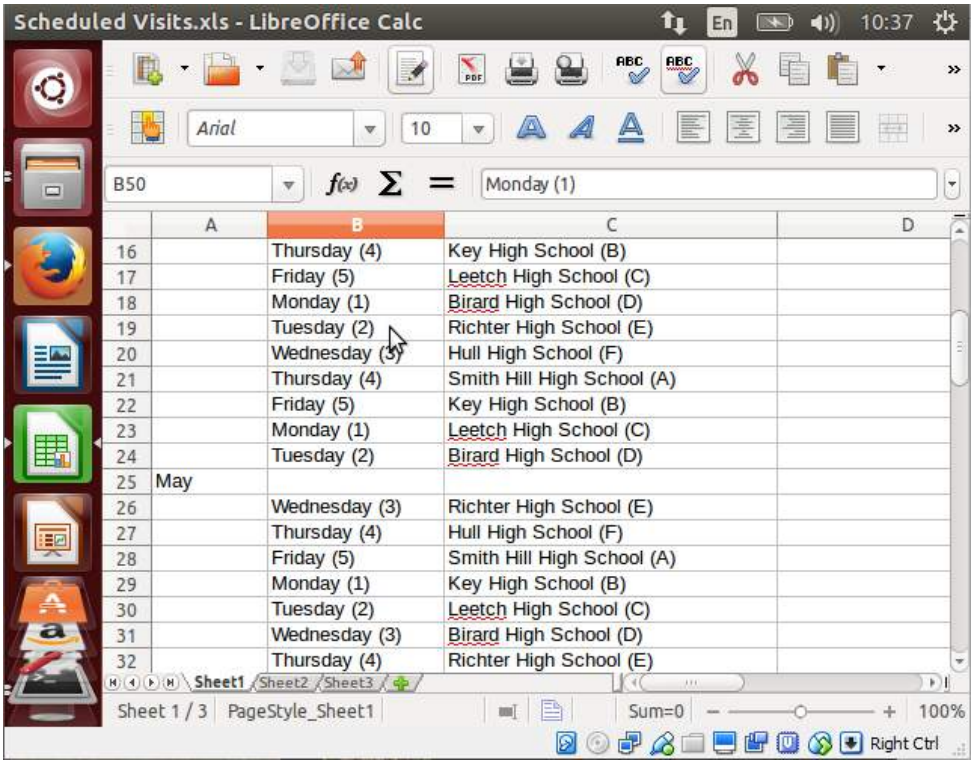
Untuk mengetahui kebenaran dan hasil dari forensics yang telah dilakukan dengan mengganti format dari file 73-103 (31) menjadi format JPEG, untuk mendapatkan informasi-informasi yang berhubungan kasus tersebut dapat dilihat pada gambar dibawah ini.

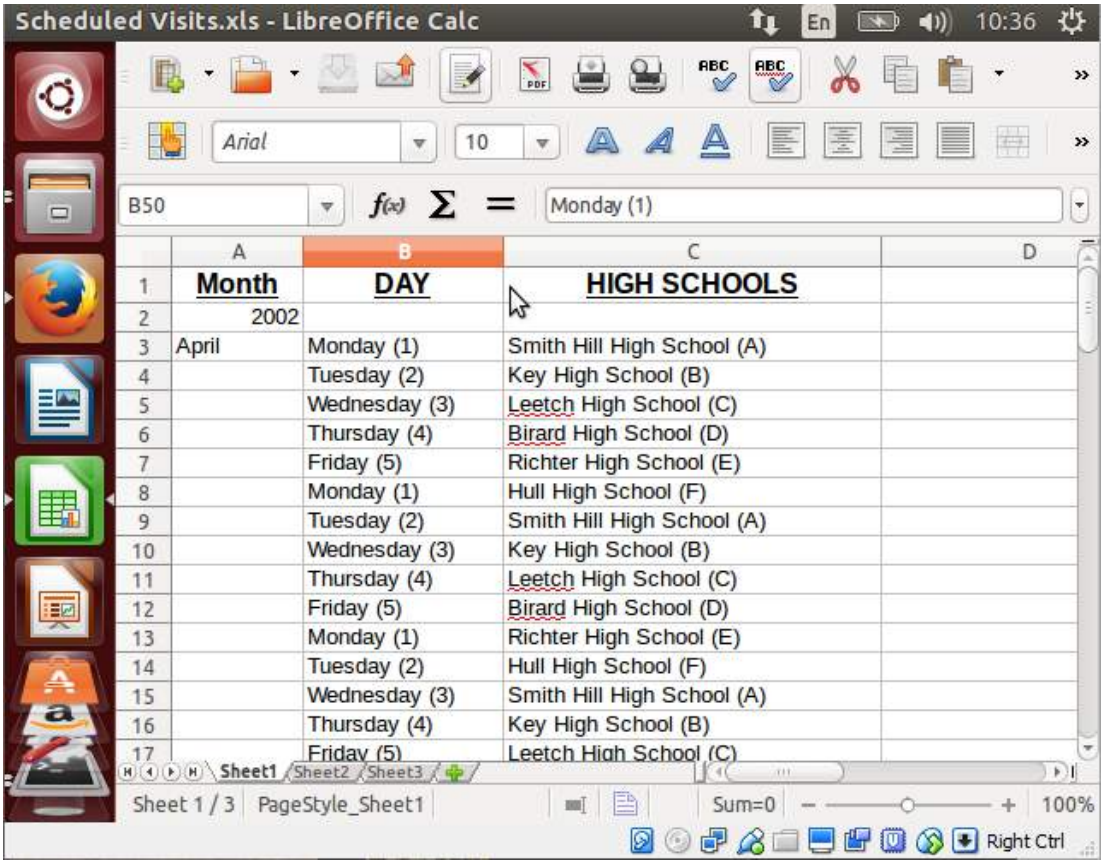
Selanjutnya untuk mendapatkan password tersebut pelaku menyimpan password didalam file sector 73-103 (31). Untuk mencari tahu password dari file tersebut menggunakan tools strings dengan mengetikkan perintah string vol1-Sector73.raw , yang dapat dilihat pada gambar dibawah ini.

```
root@mahasiswa:/home/mahasiswa/Downloads# strings vol1-Sector73
.jpg
```

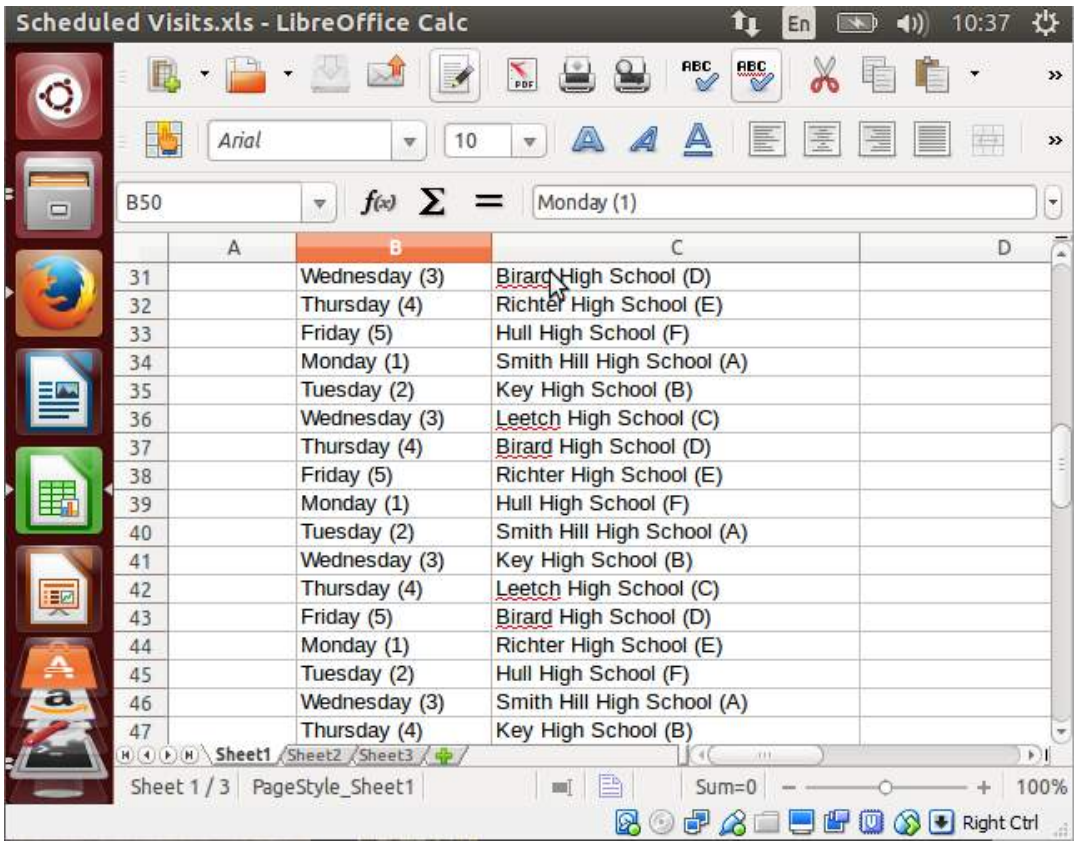
```
FFFy
        NrH'
puO     k
go}b
`/9'
Tw      l
c\[M0
T[9j
k}Bx`VE
s$6s,
zz7q
K;dMj
)UfRcvm
8-'H$
FFFy
        NrH'
|7g%
9'p+
R*]I
oqk4
I+^L
pw=goodtimes
root@mahasiswa:/home/mahasiswa/Downloads#
```

Dari hasil string yang telah dilakukan password disimpan 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 ini.

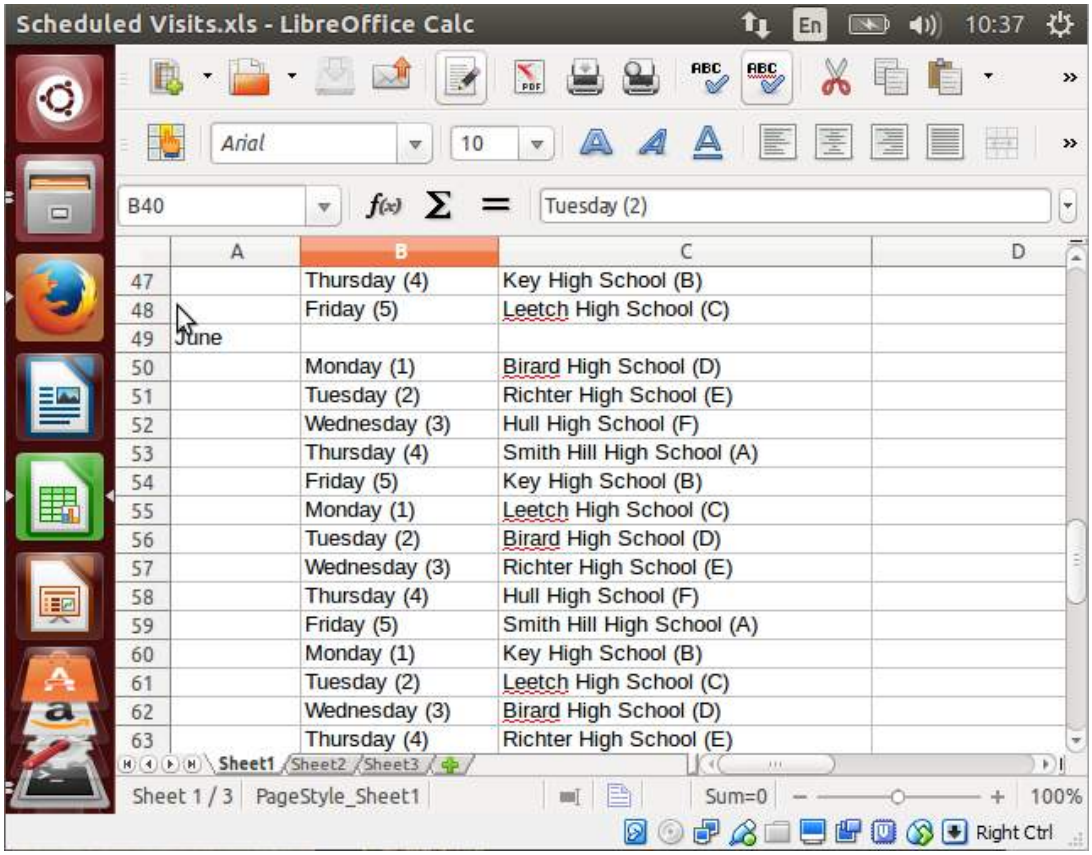


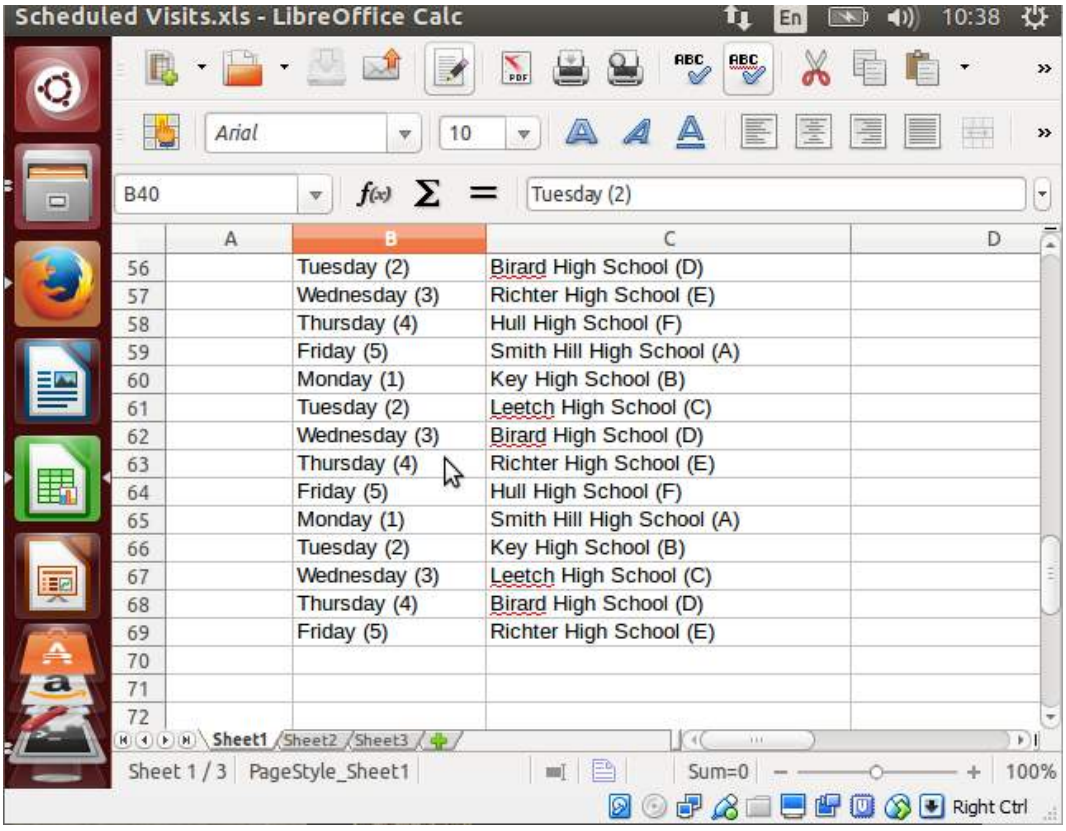


	A	B	C	D
1	**Month**	**DAY**	**HIGH SCHOOLS**	
2	2002			
3	April	Monday (1)	Smith Hill High School (A)	
4		Tuesday (2)	Key High School (B)	
5		Wednesday (3)	Leetch High School (C)	
6		Thursday (4)	Birard High School (D)	
7		Friday (5)	Richter High School (E)	
8		Monday (1)	Hull High School (F)	
9		Tuesday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

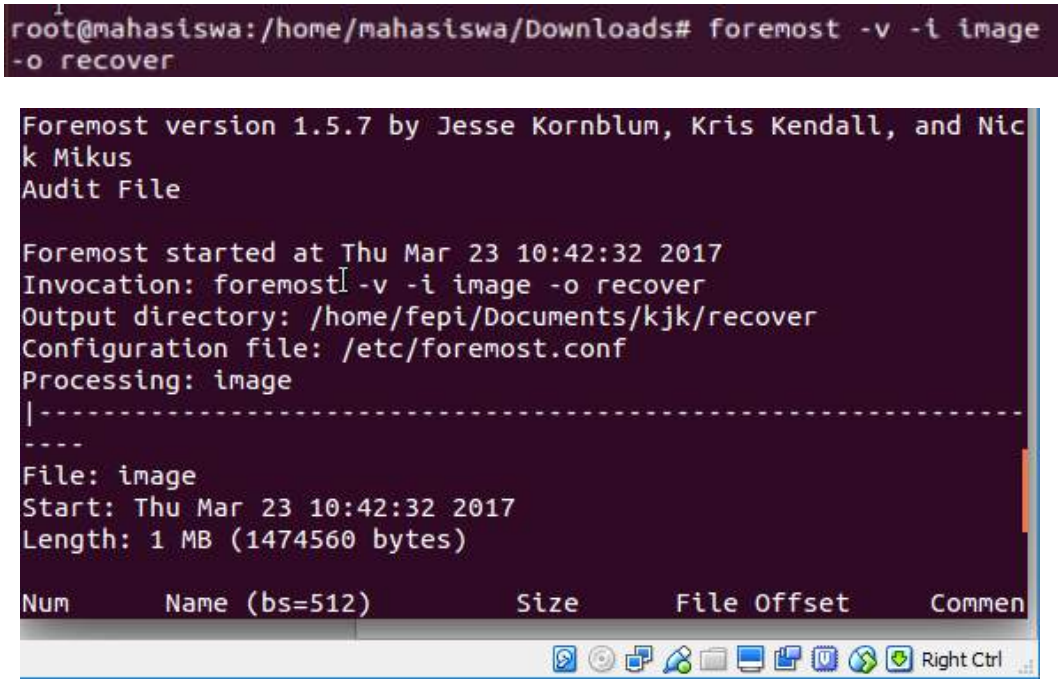


	A	B	C	D
31		Wednesday (3)	Birard High School (D)	
32		Thursday (4)	Richter High School (E)	
33		Friday (5)	Hull High School (F)	
34		Monday (1)	Smith Hill High School (A)	
35		Tuesday (2)	Key High School (B)	
36		Wednesday (3)	Leetch High School (C)	
37		Thursday (4)	Birard High School (D)	
38		Friday (5)	Richter High School (E)	
39		Monday (1)	Hull High School (F)	
40		Tuesday (2)	Smith Hill High School (A)	
41		Wednesday (3)	Key High School (B)	
42		Thursday (4)	Leetch High School (C)	
43		Friday (5)	Birard High School (D)	
44		Monday (1)	Richter High School (E)	
45		Tuesday (2)	Hull High School (F)	
46		Wednesday (3)	Smith Hill High School (A)	
47		Thursday (4)	Key High School (B)	

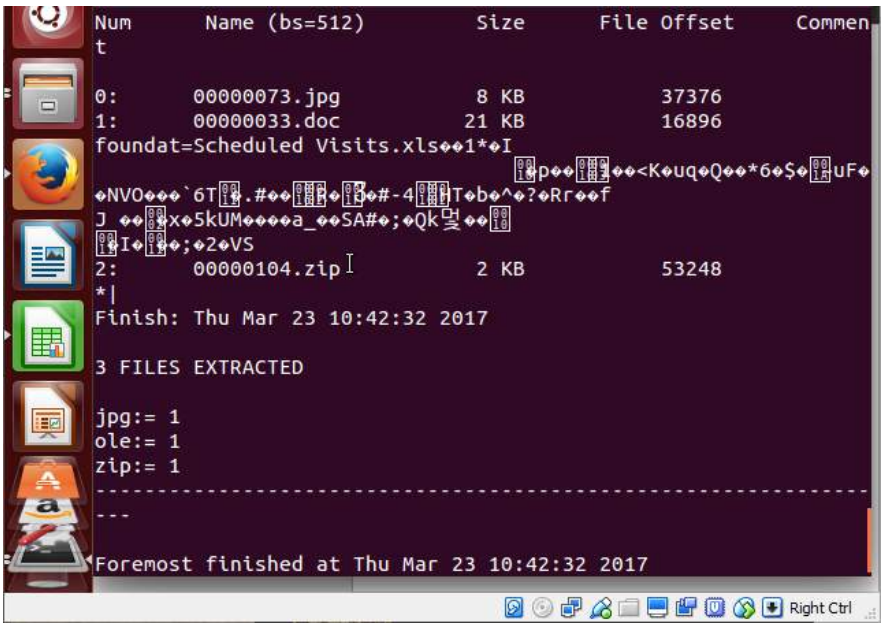

Scheduled Visits.xls - LibreOffice Calc
10:37
Arial
10
B40
Tuesday (2)
A
B
C
D
47 Thursday (4) Key High School (B)
48 Friday (5) Leetch High School (C)
49 June
50 Monday (1) Birard High School (D)
51 Tuesday (2) Richter High School (E)
52 Wednesday (3) Hull High School (F)
53 Thursday (4) Smith Hill High School (A)
54 Friday (5) Key High School (B)
55 Monday (1) Leetch High School (C)
56 Tuesday (2) Birard High School (D)
57 Wednesday (3) Richter High School (E)
58 Thursday (4) Hull High School (F)
59 Friday (5) Smith Hill High School (A)
60 Monday (1) Key High School (B)
61 Tuesday (2) Leetch High School (C)
62 Wednesday (3) Birard High School (D)
63 Thursday (4) Richter High School (E)
Sheet1 Sheet2 Sheet3
Sheet 1 / 3
PageStyle_Sheet1
Sum=0
100%
Right Ctrl

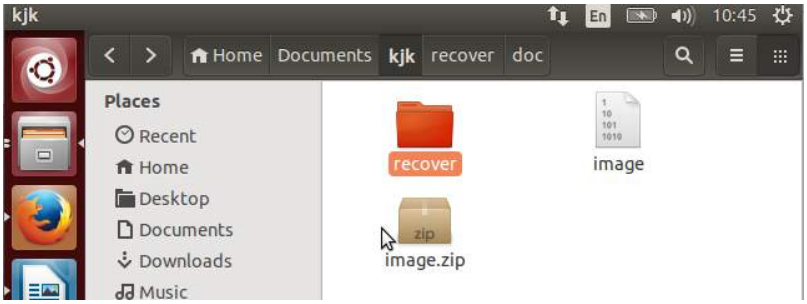

Scheduled Visits.xls - LibreOffice Calc
10:38
Arial
10
B40
Tuesday (2)
A
B
C
D
56 Tuesday (2) Birard High School (D)
57 Wednesday (3) Richter High School (E)
58 Thursday (4) Hull High School (F)
59 Friday (5) Smith Hill High School (A)
60 Monday (1) Key High School (B)
61 Tuesday (2) Leetch High School (C)
62 Wednesday (3) Birard High School (D)
63 Thursday (4) Richter High School (E)
64 Friday (5) Hull High School (F)
65 Monday (1) Smith Hill High School (A)
66 Tuesday (2) Key High School (B)
67 Wednesday (3) Leetch High School (C)
68 Thursday (4) Birard High School (D)
69 Friday (5) Richter High School (E)
70
71
72
Sheet1 Sheet2 Sheet3
Sheet 1 / 3
PageStyle_Sheet1
Sum=0
100%
Right Ctrl

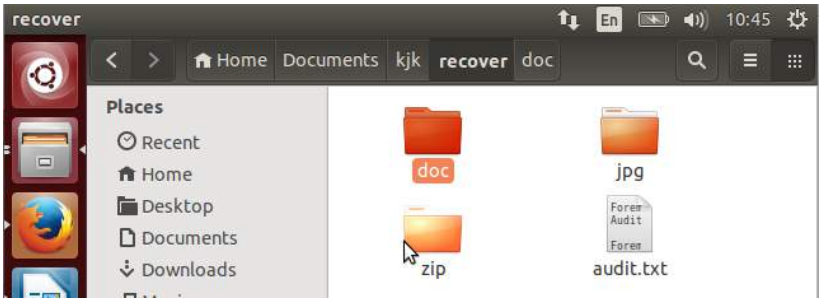
Kasus ini juga dapat dipecahkan dengan menggunakan tools foremost dengan perintah foremostyaitu –v –i image –o recover seperti yang terlihat pada gambar dibawah ini. Setelah melakukan perintah diatas maka akan menampilkan folder yang berisi tentang informasi yang berhubungan dengan kasus narkoba yang telah ditangani.

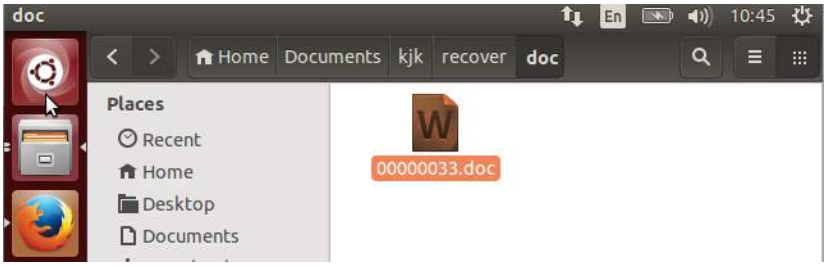


Folder yang ada didalam folder recover ini merupakkan informasi yang dibutuhkan dalam menangani kasus narkoba, sebagai contoh untuk file yang ada didalam folder doc, berisi file 0000003.doc dengan informasi yang ada didalammnya ialah surat pengedar narkoba dari kasus ini.









Berikut adalah tampilan surat pengedar narkoba dalam kasus ini. Jadi dapat disimpulkan bahwa Joe Jacob adalah jimmy jungle yaitu dapat dilihat pada informasi di bawah ini.