

Nama : Riki Andika NIM : 09011181320015
--

Hang on Training, Kamis 23 Maret 2017

Computer Forensics

Keamanan komputer merupakan hal yang menarik untuk dipelajari dan ikuti perkembangannya. Perkembangan dunia *Information Technology* (IT) yang sangat cepat telah melahirkan dimensi lain dari teknologi, yaitu kejahatan dengan peran komputer sebagai alat utamanya, istilah yang populer untuk modus ini disebut dengan *cybercrime*. Adanya kecenderungan negative dari teknologi komputer tersebut telah memunculkan berbagai permasalahan baru, baik secara mikro karena hanya berefek pada tingkatan personal/perseorangan, sampai kepada persoalan makro yang memang sudah pada wilayah komunal, publik, serta memiliki efek domino kemana-mana. Suatu Negara yang sudah maju dalam bidang *Information Technology* (IT) nya, pemerintahan setempat atau Profesional swasta bahkan telah membentuk polisi khusus yang bertugas untuk menindak kejahatan yang spesifik menangani permasalahan-permasalahan ini.

Cyber Police adalah polisi *cyber* yang diberikan tugas untuk menindak pelaku-pelaku kriminalitas di dunia *cyber*, yang tentu saja agak sedikit berbeda dengan polisi konvensional, para petugas ini memiliki kemampuan dan perangkat khusus dalam bidang komputerisasi, sehingga dapat dengan mudah dalam menindak setiap tindakan jahat yang berhubungan dengan *cyber crime* (kejahatan dunia maya). *Computer Forensics* merupakan suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun piranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan. Adapun tujuan dari *computer forensic* ini ialah sebagai berikut;

- a. Membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat bukti yang sah di pengadilan.
- b. 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 motivasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tersebut.

Terdapat 3 fokus data yang dilakukan dalam *Computer Forensics* yang dikategorikan sebagai berikut;

a. Active Data

Informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi.

b. Archival Data

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.

c. Latent Data

Informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya

Pemahaman mengenai Computer Forensics membutuhkan pembelajaran lebih mendalam, sehingga untuk lebih mengerti, sebagai contoh dilakukan pemecahan kasus melalui simulasi yang dilakukan, dengan contoh kasus yang diselesaikan ialah kasus penyebaran dan penggunaan narkoba, Kasus yang diselesaikan menggunakan tools pendukung sebagai software yang digunakan untuk membatu dalam penyelesaian kasus tersebut, dengan tools yang digunakan seperti autopsy, ghax dan foremost. Informasi yang ada berikut ulasannya “Telah tertangkap seorang pengedar narkoba yang telah memiliki banyak jaringan yang dapat dikatakan bos dari semua bos narkoba, polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta untuk membantuan pihak kepolisian untuk melakukan forensic terhadap file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut”.

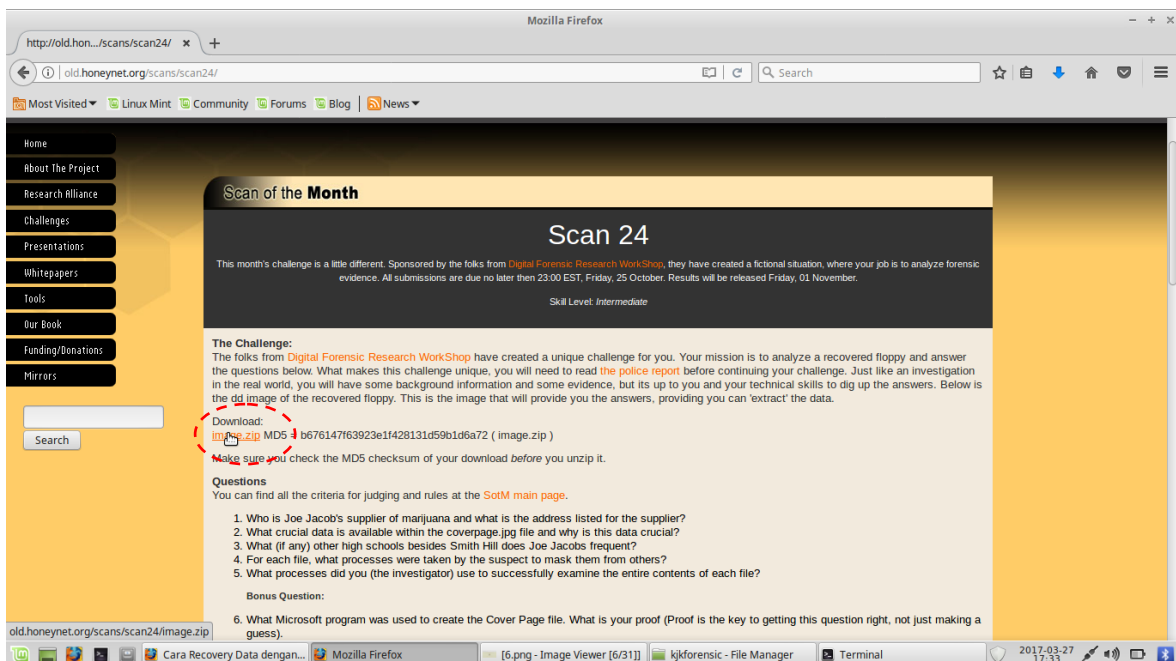
Dengan beberapa point informasi yang dicari sebagai berikut;

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?

Jawab:

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

Penyelesaian kasus atau langkah-langkah investigasi dari kasus ini menjawab pertanyaan nomor 5, dengan langkah-langkah simulasi yang dilakukan dalam penyelesaian kasus narkoba tersebut sebagai berikut;



Gambar 1. Website old.honeynet.org/scans/scan24/

Download file dengan extension zip, dengan nama image.zip yang akan digunakan sebagai bahan dalam menyelesaikan kasus narkoba tersebut, kemudian cek keaslian dari file yang telah didownload dengan menggunakan perintah md5sum image.zip. dengan hasil seperti pada gambar 2, sebagai berikut;

```
riki@riki-X200MA ~/Downloads $ su
Password:
riki-X200MA Downloads # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
```

Gambar 2. Mengecek keaslian file

Setelah melihat keaslian file yang didownload ekstrak file tersebut kemudian lihat rincian dari file image yang telah di ekstrak dengan perintah file image, maka akan kelihatan rincian dari file image, seperti yang terlihat pada gambar 3.

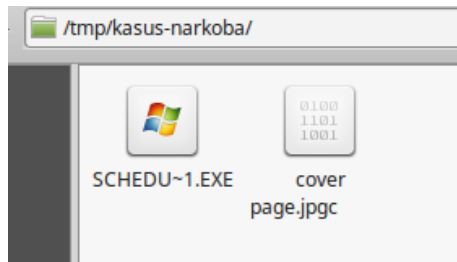
```
riki-X200MA Downloads # unzip image.zip
Archive: image.zip
  inflating: image
riki-X200MA Downloads # file image
image: DOS floppy 1440k, x86 hard disk boot sector
```

Gambar 3. Rincian file image

Dari rincian yang diperoleh, dapat dilihat file image yang diperoleh tersebut merupakan file dari hardisk yang telah rusak (*boot sector*). Setelah itu buat folder baru didalam folder tmp kemudian mount file image tersebut letakkan hasil mount dalam file system dalam folder yang telah dibuat dengan perintah mount image /tmp/kasus-narkoba/, dengan hasil screenshot yang dapat dilihat pada gambar 4 dengan hasil mounting yang telah dilakuakn dapat dilihat pada gambar 5.

```
riki-X200MA Downloads # mkdir /tmp/kasus-narkoba
riki-X200MA Downloads # mount image /tmp/kasus-narkoba/
```

Gambar 5. Mounting file image



Gambar 6. Hasil mounting

File yang ada didalam folder tmp/kasus-narkoba/ dengan hasil mounting dari file image tersebut lakukan pengecekan utilitas file dengan perintah file *, yang artinya mengecek semua utilitas dari file yang ada didalam folder kasus-narkoba, dengan hasil prenscren sebagai berikut;

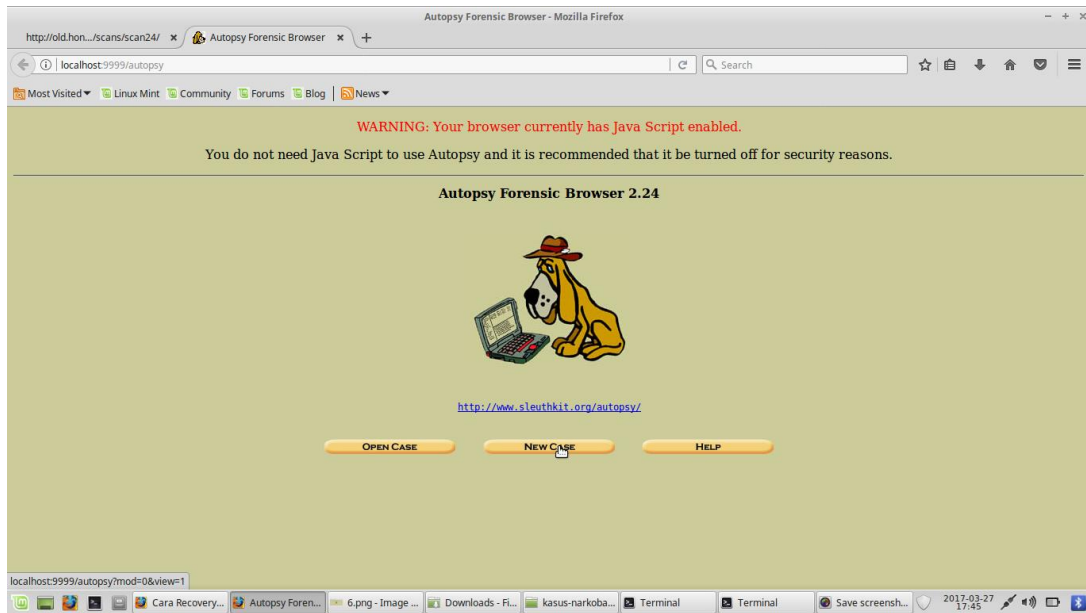
 A screenshot of a terminal window titled "Terminal". The terminal shows the following commands and output:


```

riki@riki-X200MA /tmp/kasus-narkoba $ su
Password:
riki-X200MA kasus-narkoba # ls
cover page.jpgc          SCHEDU~1.EXE
riki-X200MA kasus-narkoba # file *
cover page.jpgc: binary data
SCHEDU~1.EXE: Zip archive data, at least v2.0 to extract
riki-X200MA kasus-narkoba #
  
```

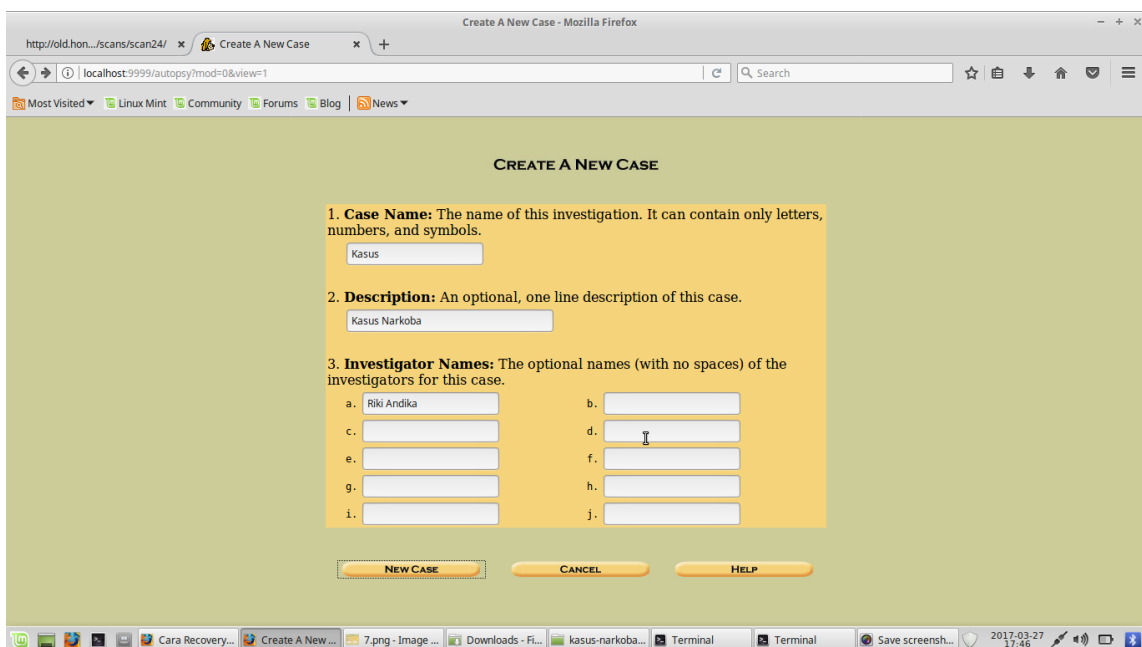
Gambar 6. Cek utilitas file

Setelah file image berhasil dimounting, buka localhost dari tools The Autopsy Forensic Browser 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). Langkah selanjutnya ialah dengan menjalankan tools autopsy dan membuka local host dengan alamat localhost:9999/autopsy, dengan hasil seperti pada gambar 7.



Gambar 7. Tampilan localhost autopsy

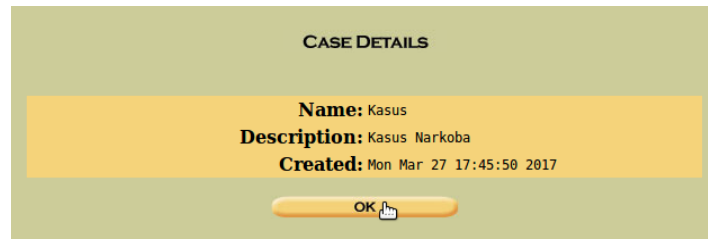
Setelah membuka alamat localhost dari tools autopsy tersebut, lakukan pengisian form untuk menyelesaikan kasus yang ditangani, dengan mengisi data-data, seperti pada gambar 8 berikut;



Gambar 8. Form create new case

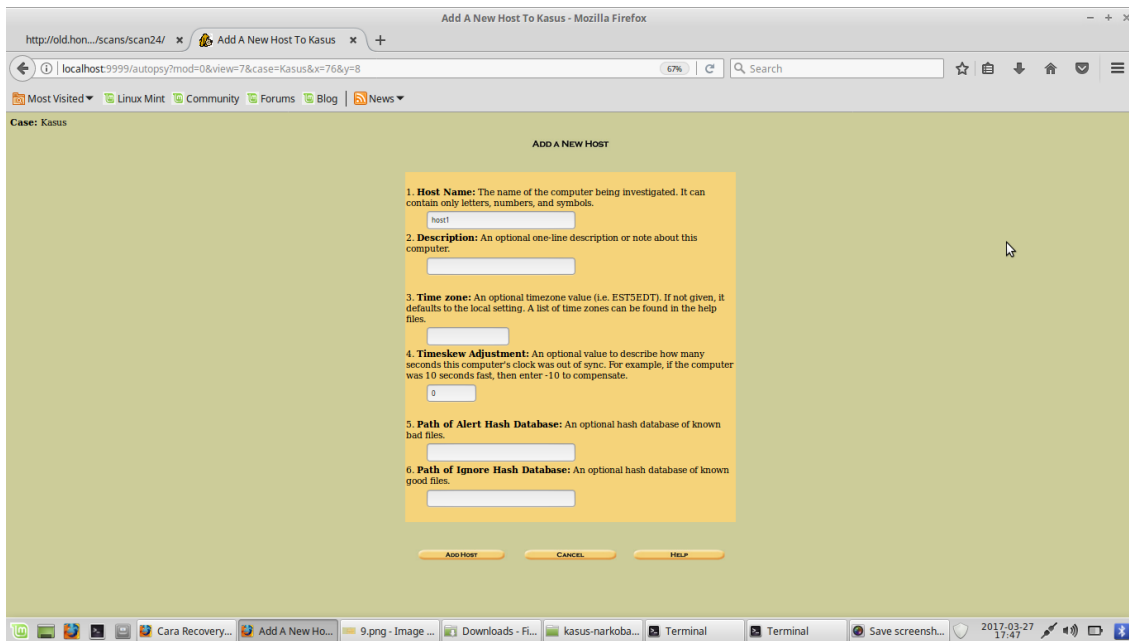
Setelah kasus dibuat maka akan muncul nama kasus yang telah dibuat dengan tampilan

seperti yang terlihat pada gambar 9 berikut;

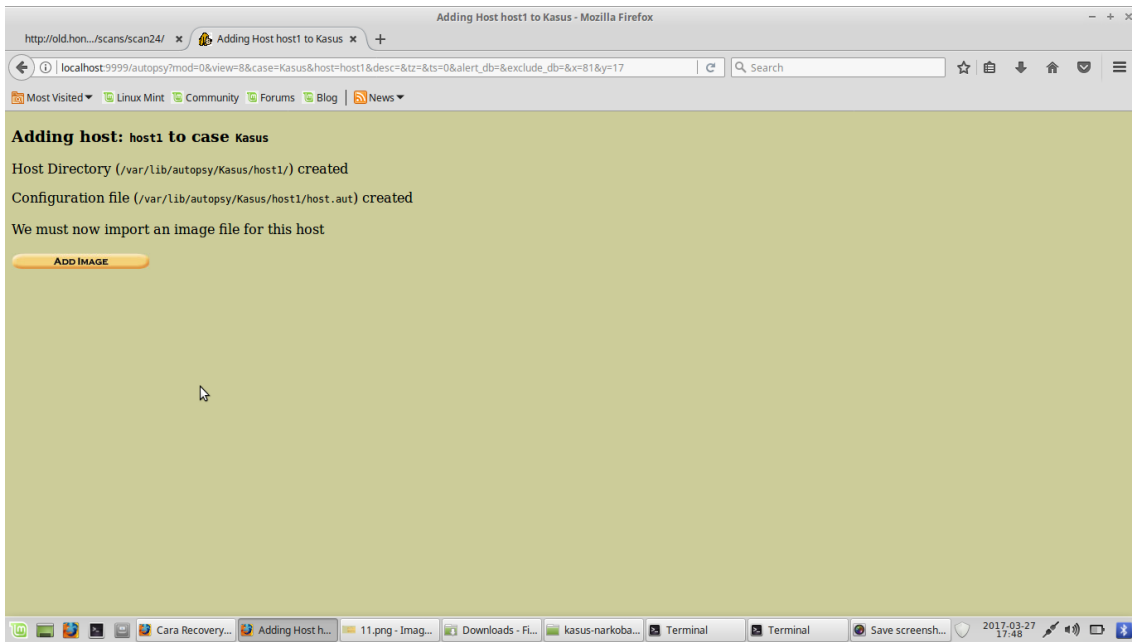


Gambar 9. Case Detail

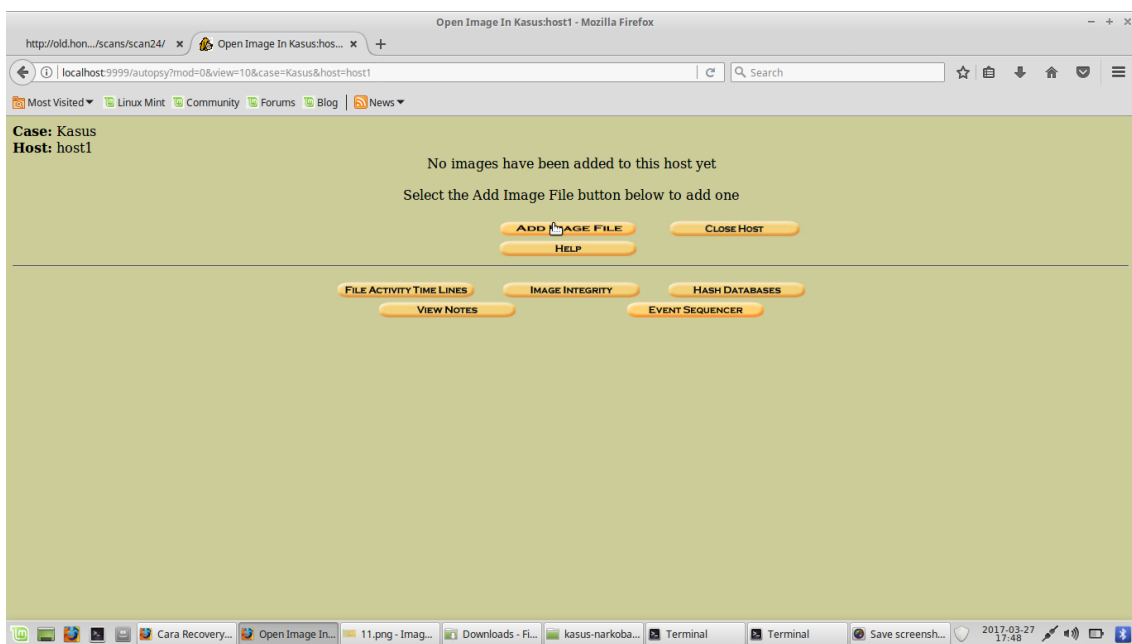
Setelah membuat kasus baru yang akan diselesaikan maka akan menampilkan dialog box yang akan menuju ke import image yang akan diinvestigasi dengan menggunakan tools autopsy, dengan menampilkan dialog box yang dapat dilihat pada gambar 10.a, 10.b, dan 10.c.



Gambar 10.a Dialog Box 1

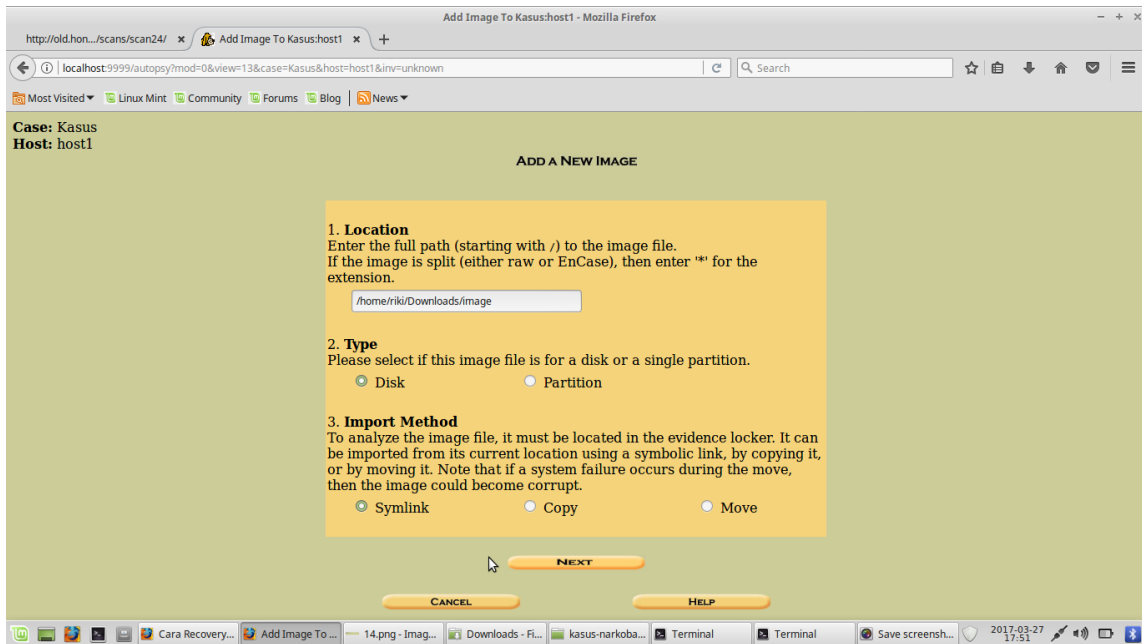


Gambar 10.b Dialog Box 2.



Gambar 10.c Dialog Box 3

Setelah melalui beberapa dialog box yang akan mengarahkan ke inport image yang akan diinvestivigasi, maka langkah selanjutnya memasukkan alamat dari file image yang akan diinvestivigasi, seperti pada gambar 11 berikut;

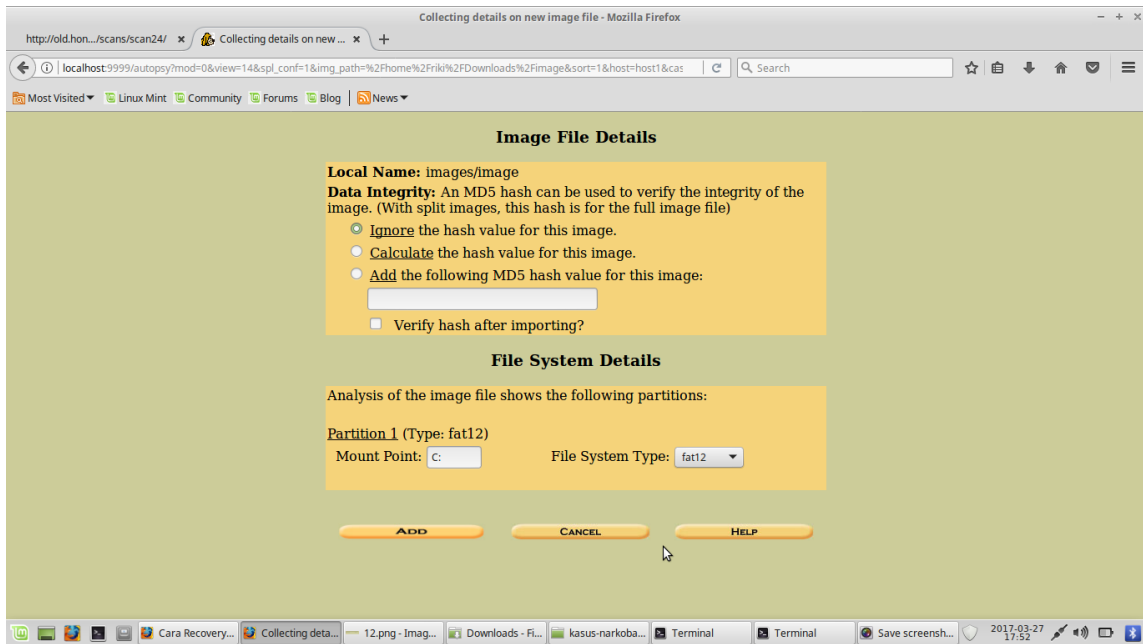


Gambar 11. Add a new image

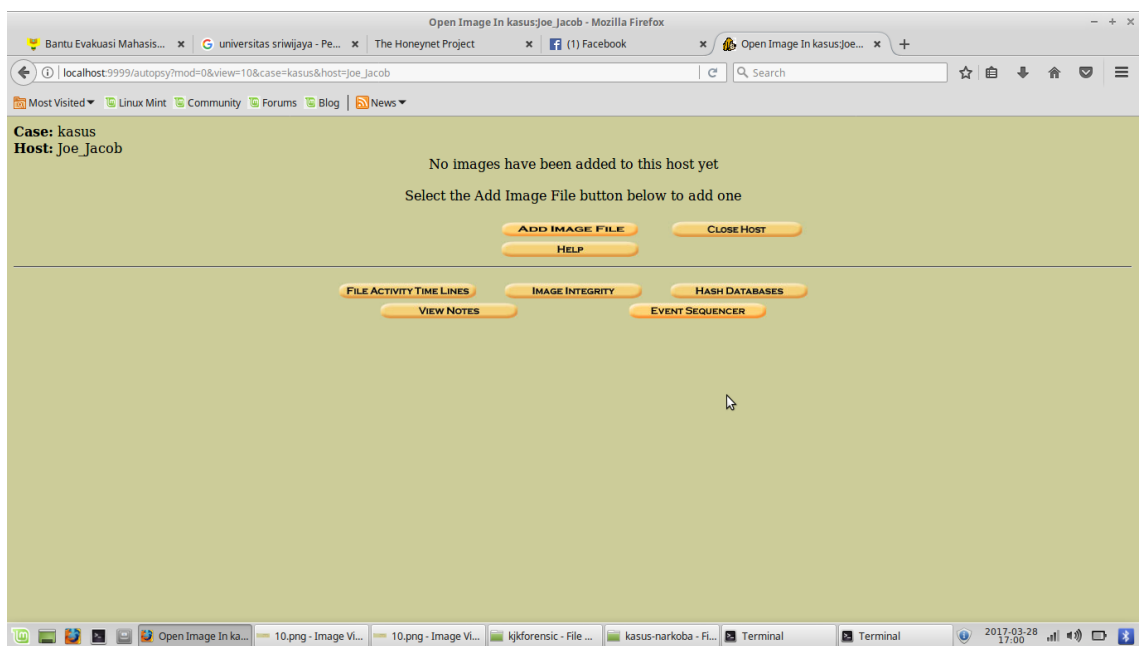
Setelah memasukkan image yang akan diinvestigasi, maka akan menampilkan beberapa dialog box yang akan mengarahkan keberhasilan dari file yang diupload kedalam tools autopsy untuk dilakukan forensic dari kasus narkoba untuk mencari informasi-informasi terkait.



Gambar 12.a

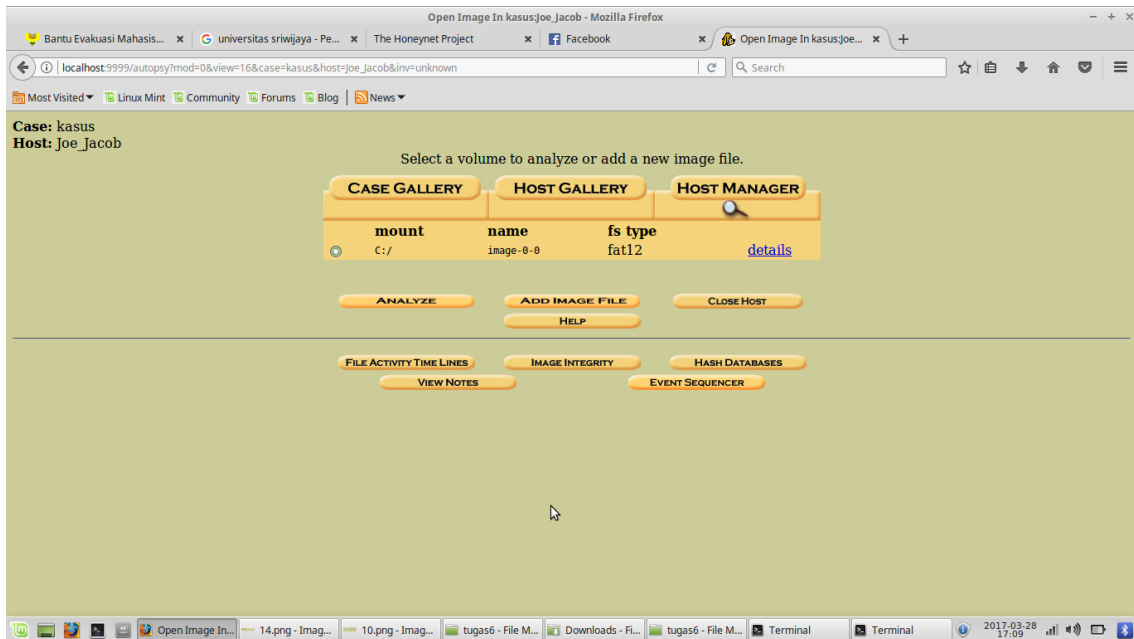


Gambar 12. B



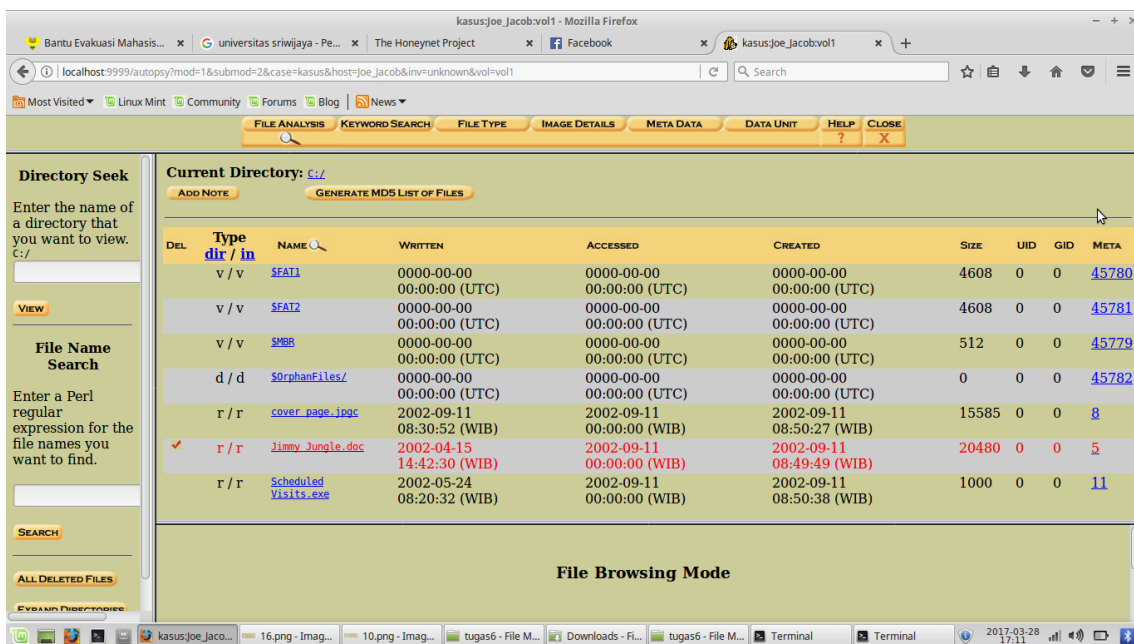
Gambar 12. c

Setelah dengan dialog box yang akan menuju ke kasus yang telah dibuat, maka kasus berhasil dibuat dengan menampilkan hasil seperti pada gambar 13 berikut;



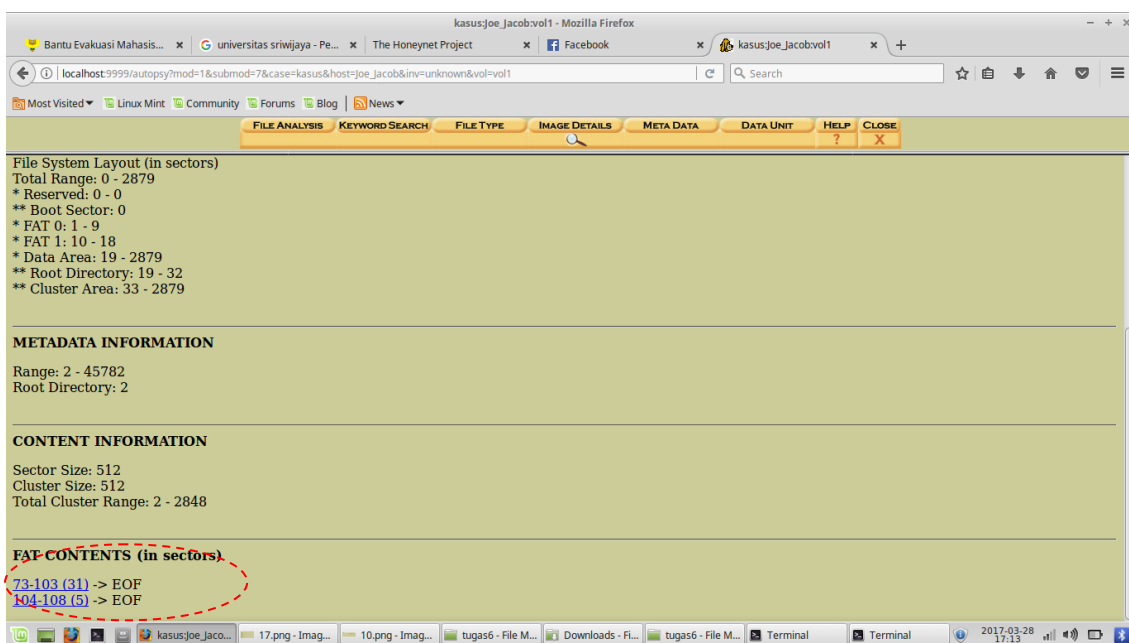
Gambar 13. Kasus yang telah dibuat pada tools autopsy

Pada gambar 13 menunjukkan kasus yang telah dimasukkan atau dibuat dalam tools autopsy dengan nama kasus ialah kasus dan hostnya adalah Joe_Jacob. Kemudian dari kasus yang telah dimasukkan lakukan analisa dengan mengklik tombol analyse, dengan menampilkan hasil seperti pada gambar 14 berikut;



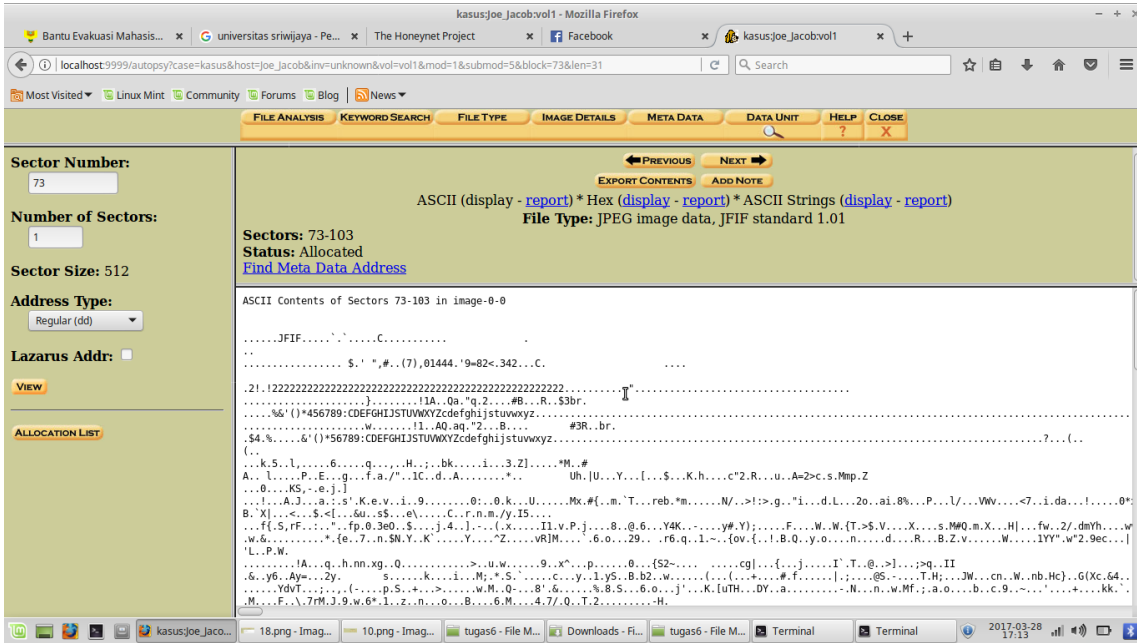
Gambar 14. Analisis File

Gambar 14 merupakan isi dari informasi yang dimiliki oleh harddrive tersebut, yang dapat dilihat dimana terdapat banyak kegiatan yang dilakukan, yang dimulai dari waktu palaku menulis, mengakses dan membuat file. Pada gambar 14 terdapat list dengan warna merah ayng memiliki arti bahwa isi dari list tersebut filenya sudah dihapus. Fakus pada dua file yang terdapat pada contet yang memiliki dua file yang dapat didownload dan untuk mendapatkan informasi-informasi yang berhubungan dengan kasus narkoba yang akan diselesaikan, dengan hasil screenshot yang dapat dilihat pada gambar 15 berikut:



Gambar 15. FAT Content yang ada didalam sektor

Dua file yang dapat didownload tersebut meruakan jejak yang ditinggalkan dalam kasus narkoba ini, dengan nama file 73-103 (31) dengan maksud terdapat informasi yang disembunyikan didalam sector 73 sampai dengan sector 103 , begitu pula dengan yang kedua 104-108 (5) terdapat informasi yang disembunyikan dalam sector 104 sampai 108. Pada sector 73-103 (31) hasil screenshot dapat dilihat pada gambar 16, terdapat format yang sangat asing sehingga sulit untuk dimengerti, untuk melakukan analisa dari file tersebut dilakukan secara manual dengan melihat bit pertama atau informasi hexa yang terdapat pada awal tulisan.



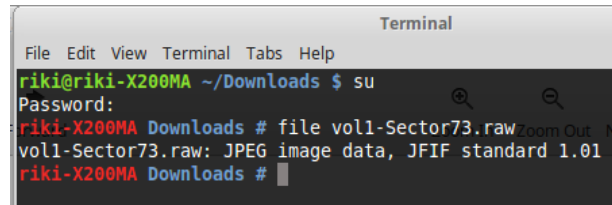
Gambar 16. Detail dari file 73-103 (31)

Gambar 16 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 signature (wikipedia) seperti yang terlihat pada gambar 17, Begitu juga untuk file yang ada pada sector 104-108 (5).

File Format	Description	Offset	Signature	Hex Signature
exr	OpenEXR image	0	v/1.	76 2F 31 01
bpg	Better Portable Graphics format ^[7]	0	BPGú	42 50 47 FB
jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿøÿ	FF D8 FF DB
			ÿøÿá ..J F IF..	FF D8 FF E0 nn nn 4A 46 49 46 00 01
			ÿøÿá ..E x 1f..	FF D8 FF E1 nn nn 45 78 69 66 00 00
ilbm ibm ibm	IFF Interleaved Bitmap Image	0 any	FORM... ILBM	46 4F 52 4D nn nn nn nn 49 4C 42 4D

Gambar 17. List of file signature format JFIF

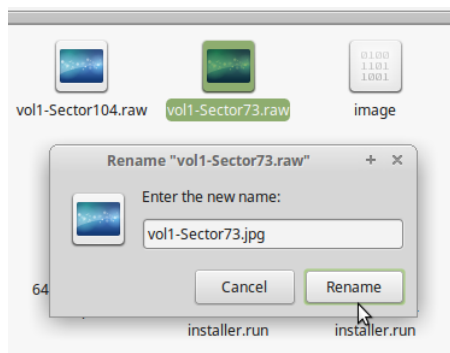
File dengan sector 73-103 (31) dengan analisa format yang diperoleh ialah format JFIF tersebut merupakan file dengan format JPEG, hal ini digunakan pelaku untuk menyembunyikan gambar dengan merubah format dari gambar tersebut menjadi raw.



```
Terminal
File Edit View Terminal Tabs Help
riki@riki-X200MA ~/Downloads $ su
Password:
riki-X200MA Downloads # file vol1-Sector73.raw
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
riki-X200MA Downloads #
```

Gambar 18. Mengecek utilitas file vol1-Sector73.raw

Sehingga untuk mengetahui kebenaran dan hasil dari forensics yang telah dilakukan dengan mengganti format dari file 73-103 (31) dengan nama vol1-Sector73.raw menjadi format JPEG, untuk mendapatkan informasi-informasi yang berhubungan kasus narkoba yang ditangani, dengan hasil screenshot yang dapat dilihat pada gambar 20.



Gambar 19. Mengganti format file menjadi JPEG



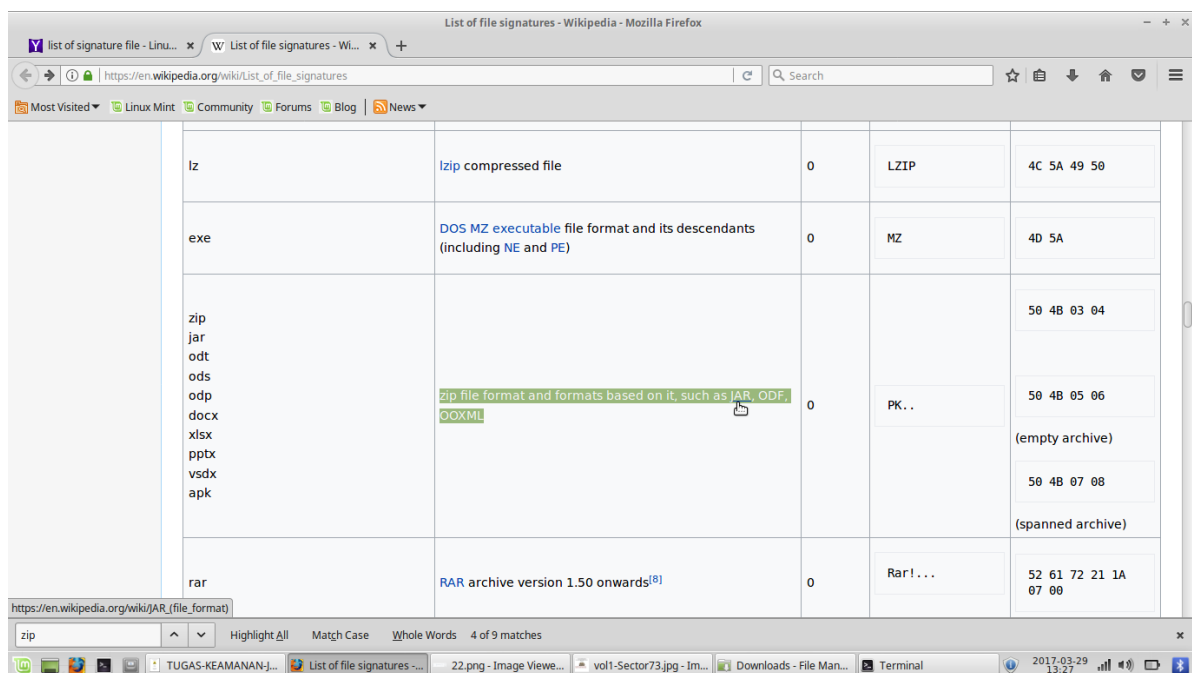
Gambar 20. File vol1-Sector73.raw setelah dirubah format JPEG

Begitu juga dengan file yang ada pada sector 104-108 (5) dilakukan hal yang sama dengan sector yang ada sebelumnya, dengan mengecek utilitas dari file dengan sector 104-108 (51) seperti pada gambar 21, dan mencari list of file signature (wikipedia) secara manual seperti pada gambar 22.

```
riki@riki-X200MA ~/Downloads $ su
Password: ns-allinone-3.21 vol1-Sector104.raw vol1-Sector73.jpg
riki-X200MA Downloads # file vol1-Sector104.raw
vol1-Sector104.raw: Zip archive data, at least v2.0 to extract
riki-X200MA Downloads #
```

Gambar 21. Utilitas file sector 104-108 (5)

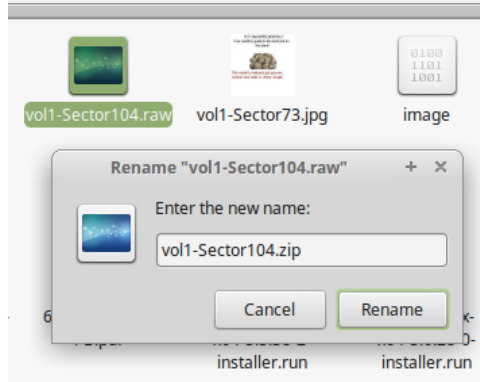
Dengan melakukan pengecekan utilitas dari file sector 104-108 (51) dengan nama file vol1-Sector104.raw, maka dapat dilakukan pencarian list of file signature (wikipedia) seperti pada gambar 22 berikut;



Gambar 22. File of signature dari sector 104-108 (51)

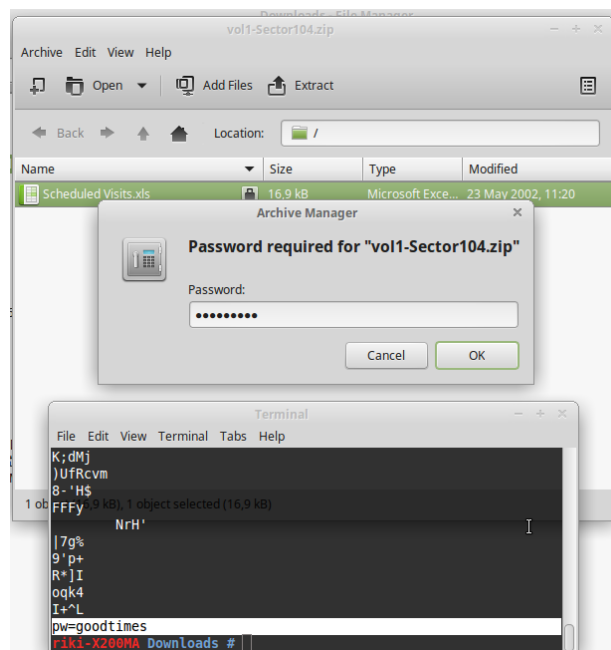
Setelah mendapat informasi yang berhubungan dengan file sector yang dicari, dengan menyembunyikan format file, dimana pada sector 104-108 (51) dengan nama file vol1-Sector104.raw pelaku menyembunyikan format zip dengan mengganti format menjadi raw, untuk membuktikan kebenaran dari analisa yang diperoleh dengan mengganti

format file tersebut menjadi zip, seperti yang terlihat pada gambar 23 dan dengan hasil yang diperoleh seperti pada gambar 24.



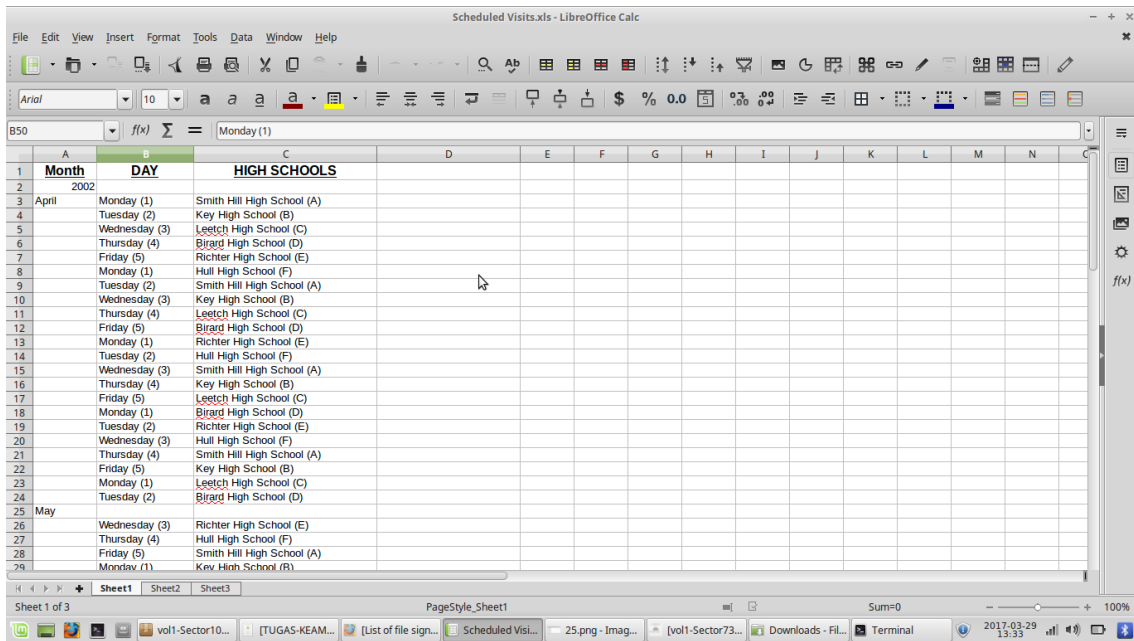
Gambar 23. Mengganti format file menjadi zip

Menghasilkan file dengan format zip, dimana didalam file dengan format zip tersebut terdapat file dengan format xls, tetapi file zip tersebut memiliki password untuk membuka isi dari file tersebut, untuk mendapatkan password tersebut pelaku menyimpan passwor didalam file sector 73-103 (31), jadi untuk membuka man cari tahu password dari file tersebut menggunakan tools strings dengan mengetikkan perintah string nama file yang akan string (string vol1-Sector73.raw) , yang dapat dilihat pada gambar 24.



Gambar 24. Strings vol1-Sector73.raw

Dari hasil string yang telah dilakukan dengan hasil screen yang terdapat pada gambar 25, merupakan password disimpan selaku kedalam file sector pertama dengan password yang diperoleh ialah goodtimes yang dapat digunakan untuk membuka file zip yang merupakan file sector kedua, dengan hasil terlihat pada gambar 25.



Gambar 25. File dengan format xls yang ada dalam sector kedua

Tidak hanya dengan menggunakan tools string dan autopsy 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 26, setelah melakukan perintah diatas maka akan menampilkan folder yang berisi tentang informasi yang berhubungan dengan kasus narkoba yang ditangani dengan hasil yang diperoleh seperti ada gambar 27.

```

Terminal
File Edit View Terminal Tabs Help
riki-X200MA Downloads # foremost -v -i image -o recover
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick
Mikus
Audit File
Foremost started at Wed Mar 29 13:36:46 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/riki/Downloads/recover
Configuration file: /etc/foremost.conf
Processing: image
|-----|
---
File: image
Start: Wed Mar 29 13:36:46 2017
Length: 1 MB (1474560 bytes)
Num      Name (bs=512)      Size      File Offset    Comment
0:      00000073.jpg       8 KB      37376
1:      00000033.doc       21 KB     16896
foundat=Scheduled Visits.xls01*0I
NVO000 6T0.#0000030#-400T0b0-070R00T
J 0000:05KUM0000a 00SA#0;00K0 000
000000:020VS
2:      00000104.zip       2 KB     53248
*|
Finish: Wed Mar 29 13:36:46 2017

3 FILES EXTRACTED

jpg:= 1
ole:= 1
zip:= 1
|-----|
Foremost finished at Wed Mar 29 13:36:46 2017
riki-X200MA Downloads #

```

Gambar 26. Menjalankan tools Foremost

Dengan hasilyang diperoleh dari menjalankan tools foremost ini ialah mendapat kan 3 folder dari image yang dianalisa, seperti yang terlihat pada gambar 27 berikut.

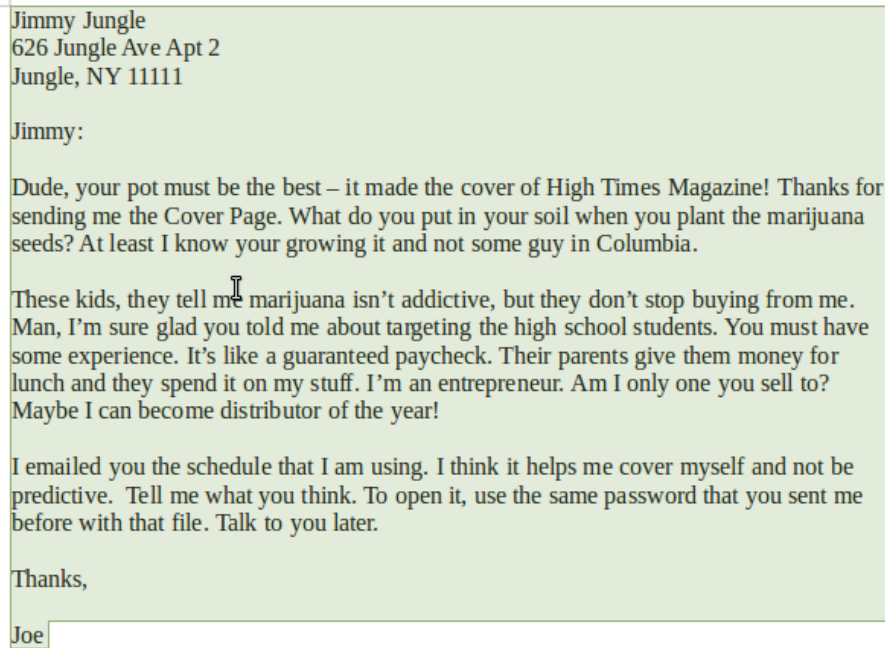
```

riki-X200MA Downloads # cd recover/
riki-X200MA recover # ls
audit.txt doc jpg zip
riki-X200MA recover # cd doc/
riki-X200MA doc # ls
00000033.doc
riki-X200MA doc # cd..
cd.: command not found
riki-X200MA doc # cd ..
riki-X200MA recover # cd jpg/
riki-X200MA jpg # ls
00000073.jpg
riki-X200MA jpg # cd ..
riki-X200MA recover # cd zip/
riki-X200MA zip # ls
00000104.zip

```

Gambar 27. Hasil dari foremost file image

Folder-folder yang ada didalam folder recover, ini merupakan informasi-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, seperti yang terlihat pada gambar 28.



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

Gambar 28. Isi folder doc setelah direcover

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

Joe Jacob adalah jimmy jungle, informasi tersebut terdapat pada sebuah email yang dikirimkan pada jimmy. (dapat dilihat pada gambar 28)

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

File gambar (jpg) yang diperoleh dari file sector 73-103 (31) adalah informasi password yang kita butuhkan untuk membuka isi dari file zip yang diperoleh dari file sector 104-108 (51). (dapat dilihat pada gambar 24)

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

Dari analisis yang telah dilakukan terdapat beberapa tempat yang dikunjungi oleh Joe Jacobs, untuk melakukan transaksi maupun pengedaran narkoba, seperti key high school ,leetch high school , berrard high school , richter high school dan hull high school. (dapat dilihat pada gambar 25)

4. For each file, what processes were taken by the suspect to mask them from others?
Strategi yang dilakukan oleh pelaku dengan menyembunyikan format file pada file sector pertama sector 73-103 (31) dan file sector kedua sector 104-108 (51) (dapat dilihat pada gambar 19 dan 23) serta password dari file zip yang ada pada file sector 104-108 (51) yang disembunyikan didalam file sector 73-103 (31) (dapat dilihat pada gambar 24)