

Tugas 6

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:

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 , birrard high school , richter high school dan hull high school. (dapat dilihat pada gambar 25)

Nim : 09011181320012

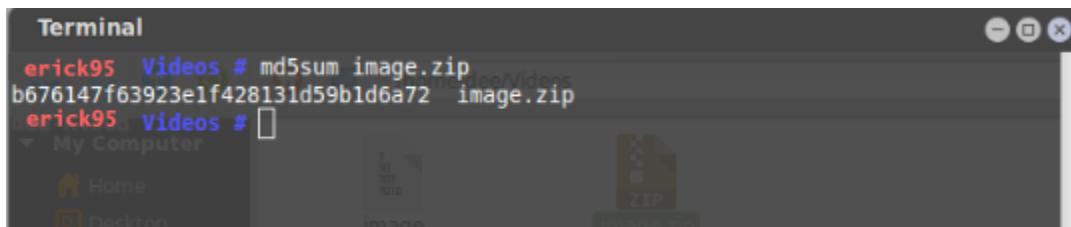
4. For each file, what processes were taken by the suspect to mask them from others?

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)

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

Penyelesaian kasus yang digunakan untuk melakukan investigasi denan contoh tersebut adalah melakukan simulasi yang dilakukan untuk penyelesaian kasus narkoba seperti dibawah ini.

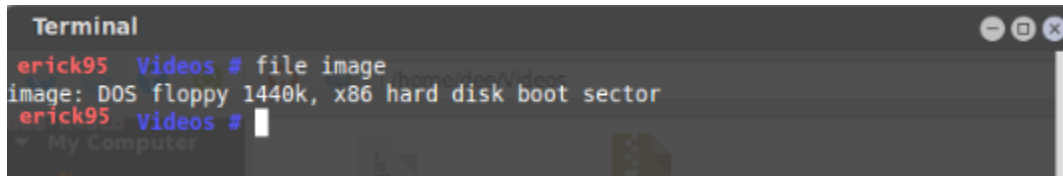
Download file dengan extention zip, dengan nama image.zip yang akan digunakan sebagai bahan dalam meyelesaikan kasus narkoba tersebut, kemudian cek keaslian dari file yang telah didownload dengan menggunakan perintah md5sum image.zip. dengan hasil seperti pada gambar 2, sebagai berikut;



```
Terminal
erick95 Videos # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
erick95 Videos #
```

Gambar.1 Mengecek originalitas File

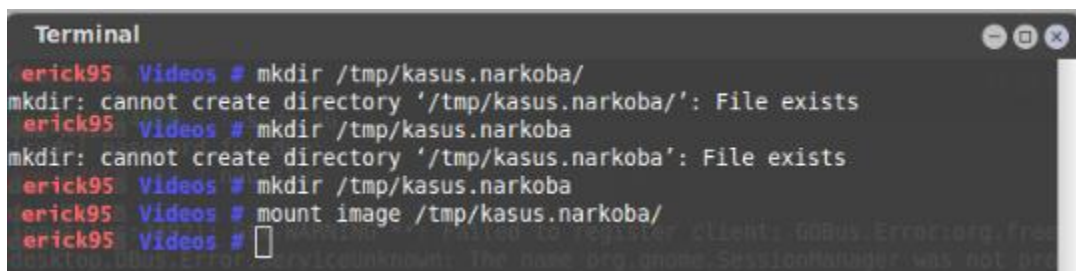
Setelah melihat keaslian file yang didownload ekstrak file tersebut kemudian lihat rincian dari file image yang telah di ekstrak dengan perintah file image, maka akan kelihatan rincian dari file image, seperti yang terlihat pada gambar 2.



```
Terminal
erick95 Videos # file image
image: DOS floppy 1440k, x86 hard disk boot sector
erick95 Videos #
```

Gambar.2 Rincian mengenai File Image

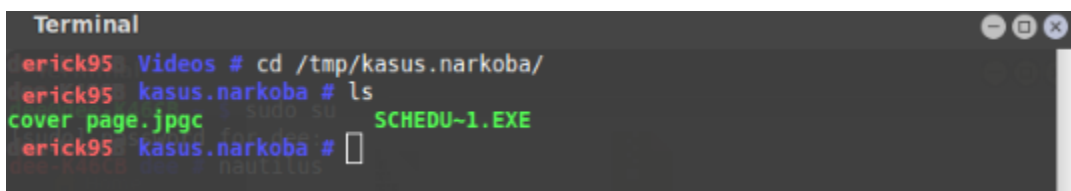
Dari rincian yang diperoleh, dapat dilihat file image yang diperoleh tersebut merupakan file dari hardisk yang telah rusak (*boot sector*). Setelah itu buat folder baru didalam folder tmp kemudian mount file image tersebut letakkan hasil mount dalam file system dalam folder yang telah dibuat dengan perintah `mount image /tmp/kasus-narkoba/`, dengan hasil screenshot yang dapat dilihat pada gambar 3 dengan hasil mounting yang telah dilakuakn dapat dilihat pada gambar 4.



```
Terminal
erick95 Videos # mkdir /tmp/kasus.narkoba/
mkdir: cannot create directory '/tmp/kasus.narkoba/': File exists
erick95 Videos # mkdir /tmp/kasus.narkoba
mkdir: cannot create directory '/tmp/kasus.narkoba': File exists
erick95 Videos # mkdir /tmp/kasus.narkoba
erick95 Videos # mount image /tmp/kasus.narkoba/
erick95 Videos #
```

Gambar.4 Proses Mount Image

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;



```
Terminal
erick95 Videos # cd /tmp/kasus.narkoba/
erick95 kasus.narkoba # ls
cover page.jpgc SCHEDU~1.EXE
erick95 kasus.narkoba #
```

Gambar.5 Menguji Utilitas

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,

Nama : Erick Okvanty Haris

Tugas 6 (Keamanan Jaringan Komputer)

Nim : 09011181320012

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 6.



Gambar.6 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;

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

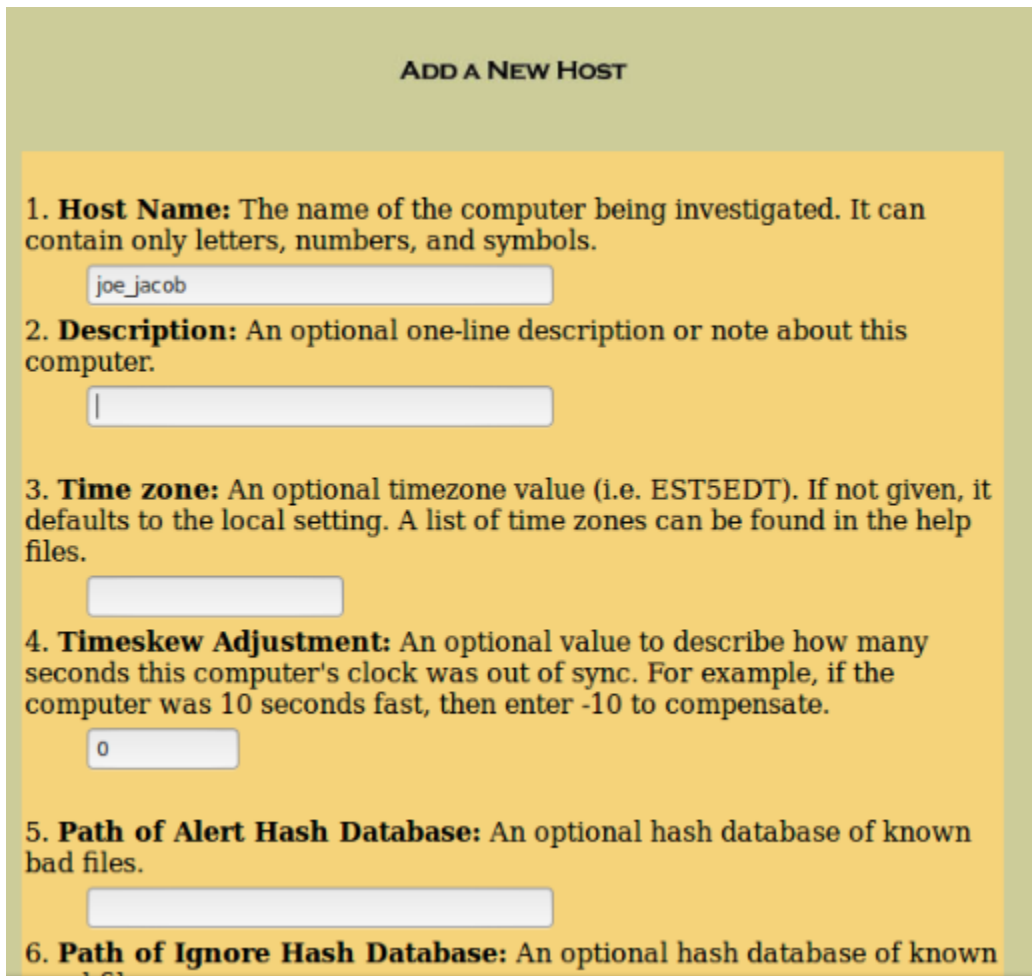
2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	<input type="text" value="Erick Okvanty Haris"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

Gambar.7 Create A New Case

Setelah membuat kasus baru yang akan diselesaikan maka akan menampilkan dialog box yang akan menuju ke import image yang akan diinvestivigasi dengan menggunakan tools autopsy, dengan menampilkan dialog box yang dapat dilihat pada gambar 8.a, 8.b, dan 8.c.



ADD A NEW HOST

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- Description:** An optional one-line description or note about this computer.
- Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
- Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
- Path of Alert Hash Database:** An optional hash database of known bad files.
- Path of Ignore Hash Database:** An optional hash database of known bad files.

Gambar.8.a Dialog Box



Adding host: joe_jacob to case kasus

Host Directory (/var/lib/autopsy/kasus/joe_jacob/) created

Configuration file (/var/lib/autopsy/kasus/joe_jacob/host.aut) created

We must now import an image file for this host

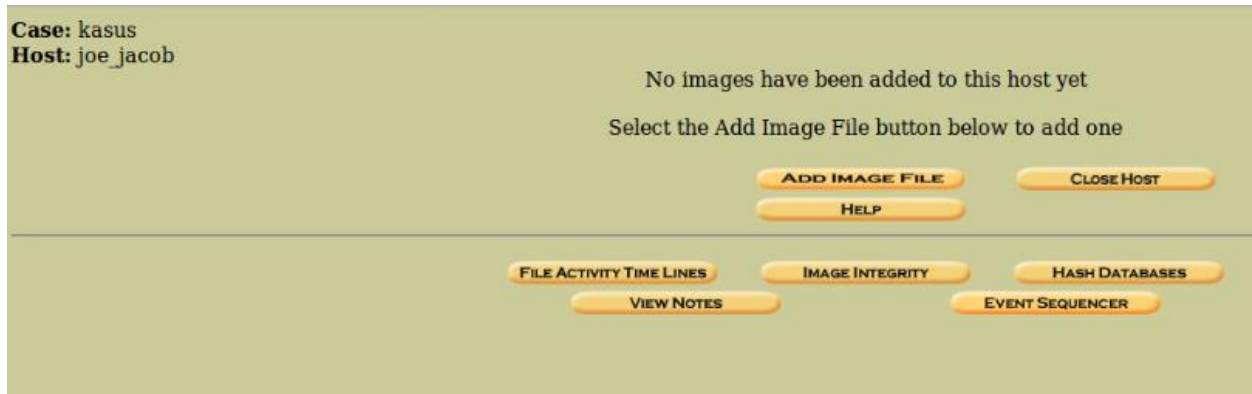
ADD IMAGE

Gambar.8.b Dialog Box

Nama : Erick Okvanty Haris

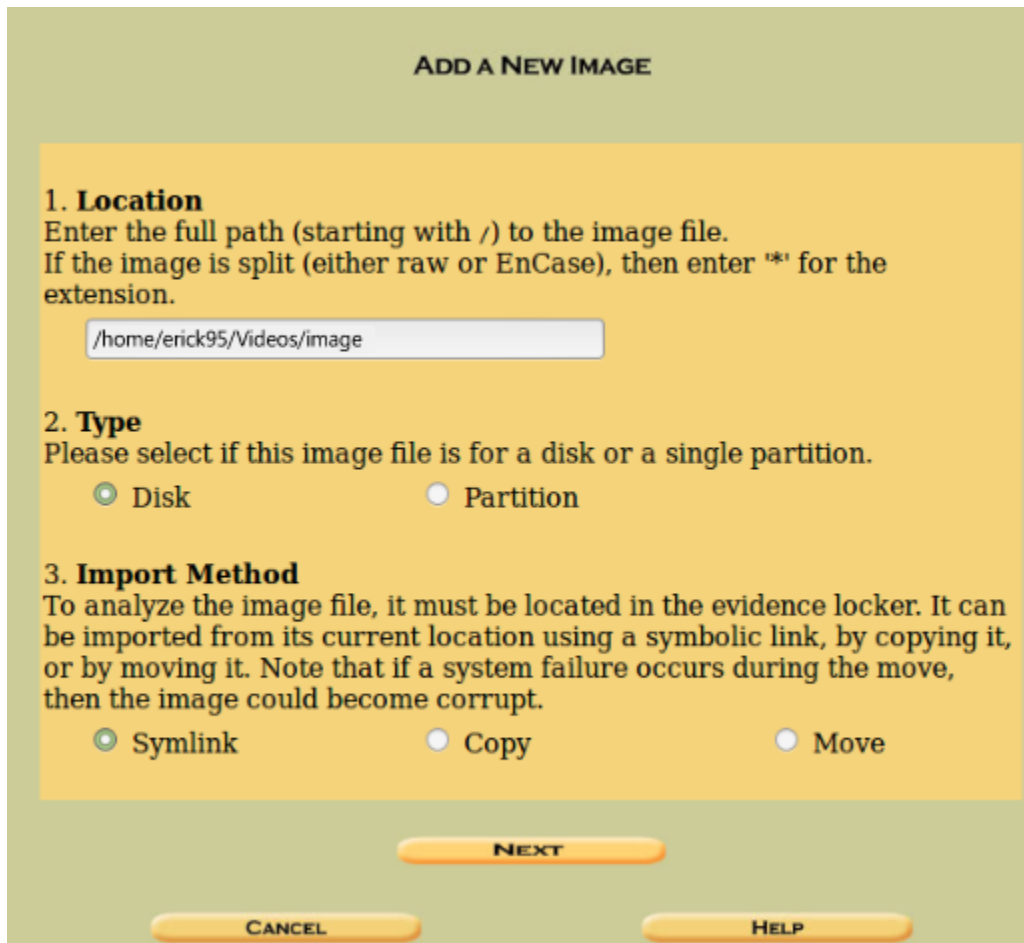
Tugas 6 (Keamanan Jaringan Komputer)

Nim : 09011181320012



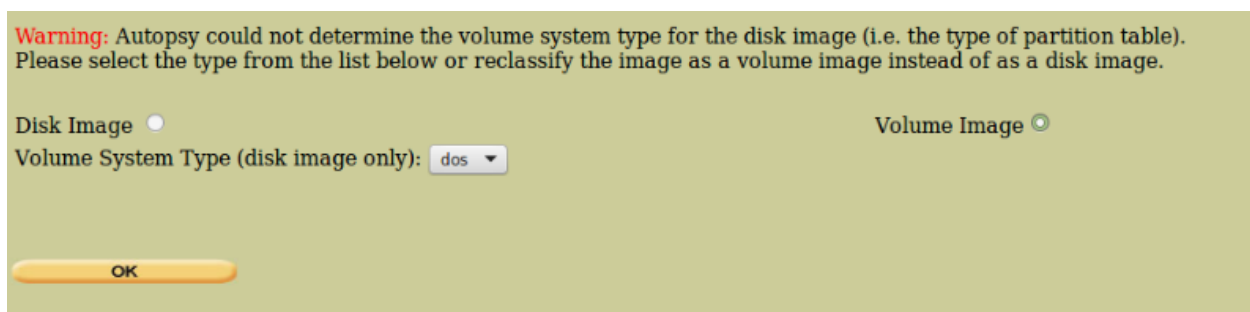
Gambar.8.c Dialog Box

Setelah melalui beberapa dialog box yang akan mengarahkan ke inport image yang akan diinvestigasi, maka langkah selanjutnya memasukkan alamat dari file image yang akan diinvestigasi, seperti pada gambar 9 berikut;

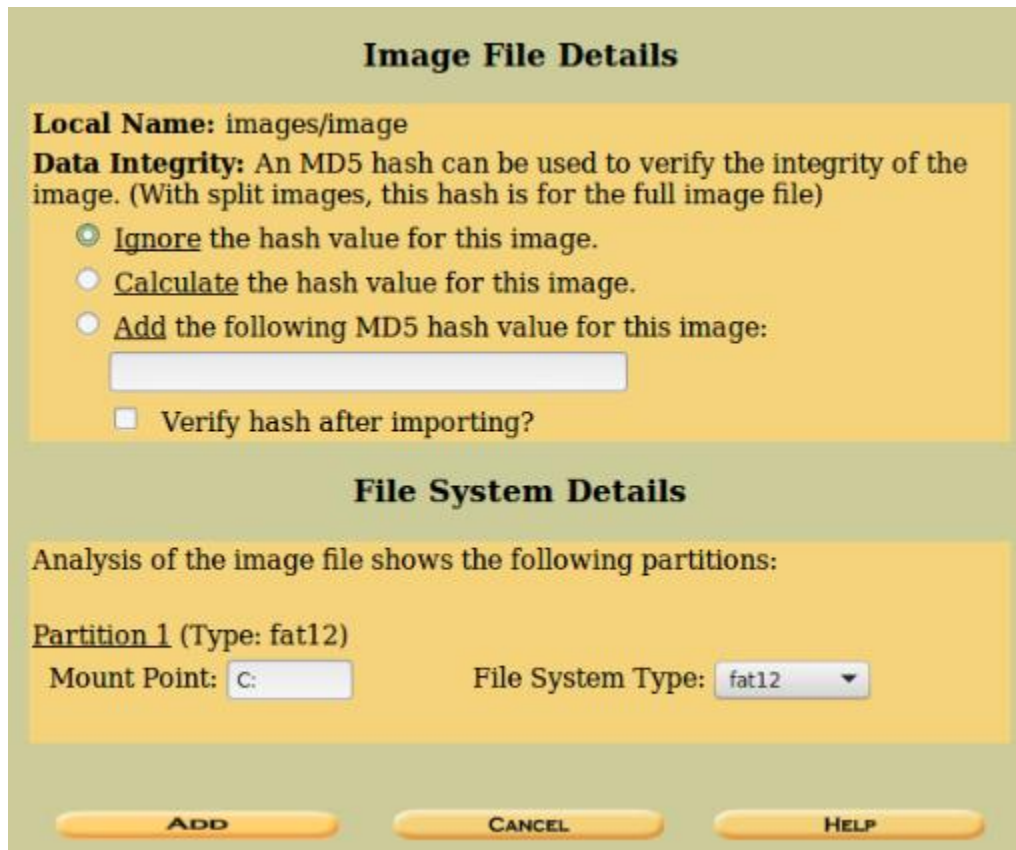


Gambar.9 Add a New Image

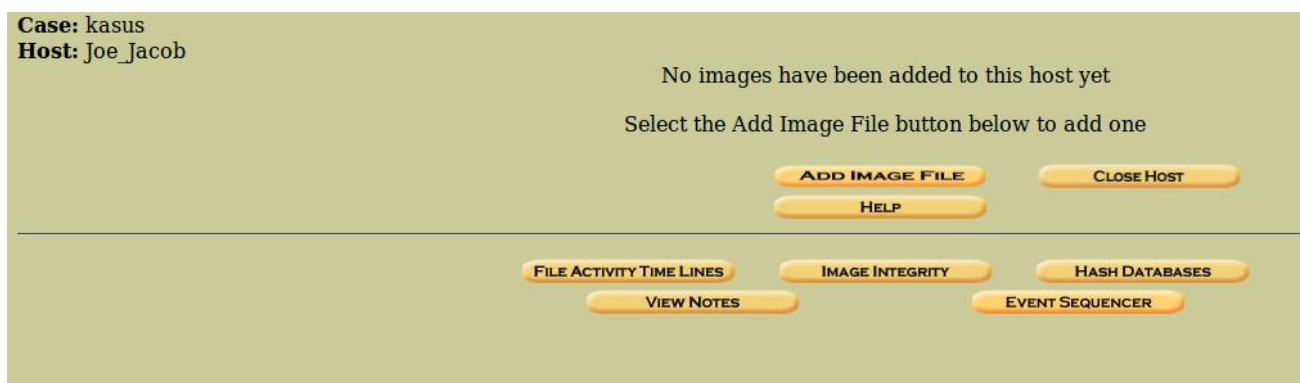
Setelah memasukkan image yang akan diinvestigasi, maka akan menampilkan beberapa dialog box yang akan mengarahkan keberhasilan dari file yang diupload kedalam tools autopsy untuk dilakukan forensic dari kasus narkoba untuk mencari informasi-informasi terkait.



Gambar 10.a

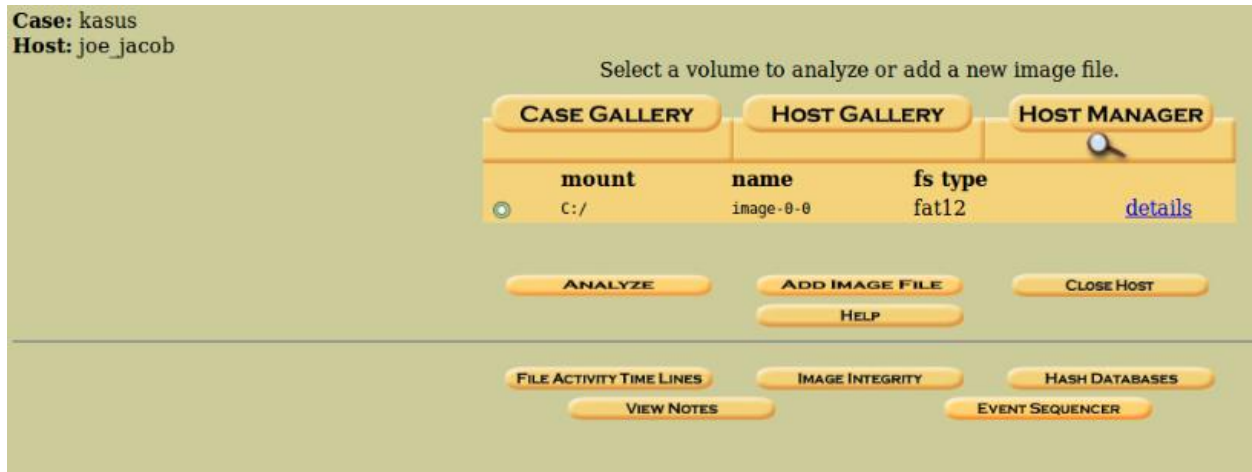


Gambar.10.b



Gambar.10.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 11. Kasus yang telah dibuat pada tools autopsy

Pada gambar 11 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 12 berikut;

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	SFAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45780
	v / v	SFAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
	v / v	SMBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
	d / d	\$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	45782
	r / r	cover_page.ipgc	2002-09-11 08:30:52 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:27 (WIB)	15585	0	0	8
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:49:49 (WIB)	20480	0	0	5
	r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:38 (WIB)	1000	0	0	11

Gambar.12 Analisis File

Gambar 12 merupakan isi dari informasi yang dimiliki oleh harddrive tersebut, yang dapat dilihat dimana terdapat banyak kegiatan yang dilakukan, yang dimulai dari waktu pelaku

Nim : 09011181320012

menulis, mengakses dan membuat file. Pada gambar 12 terdapat list dengan warna merah yang memiliki arti bahwa isi dari list tersebut filenya sudah dihapus. Fokus pada dua file yang terdapat pada content 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 13 berikut:

```
File System Layout (in sectors)
Total Range: 0 - 2879
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 9
* FAT 1: 10 - 18
* Data Area: 19 - 2879
** Root Directory: 19 - 32
** Cluster Area: 33 - 2879

METADATA INFORMATION
Range: 2 - 45782
Root Directory: 2

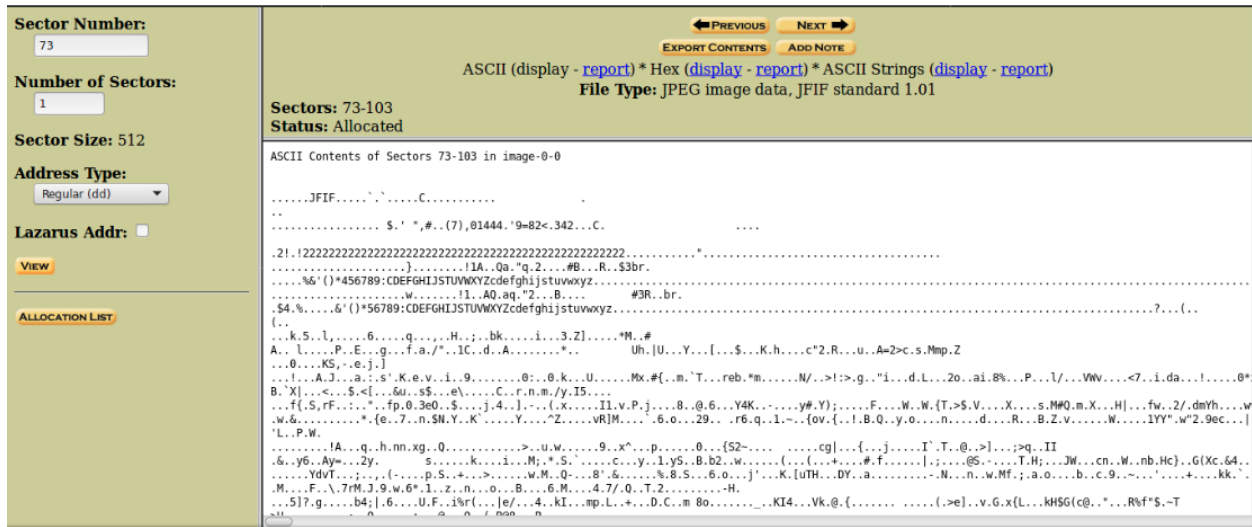
CONTENT INFORMATION
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 2848

FAT CONTENTS (in sectors)
73-103 (31) -> EOF
104-108 (5) -> EOF
```

Gambar.13 FAT content yang terdapat pada sector

Dua file yang dapat didownload tersebut merupakan jejak yang ditinggalkan dalam kasus narkoba ini, dengan nama file 73-103 (31) dengan maksud terdapat 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. Pada sector 73-103 (31) hasil screenshot dapat dilihat pada gambar 14, 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.14 Detail dari file 73-103 (31)

Gambar 14 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 15, Begitu juga untuk file yang ada pada sector 104-108 (5).

bpg	Better Portable Graphics format ^[7]	0	BPGú	42 50 47 FB
jpg jpeg	JPG raw or in the JFIF or Exif file format	0	ÿøÿ	FF D8 FF DB
			ÿøÿà ..J F IF..	FF D8 FF E0 nn nn 4A 46 49 46 00 01
			ÿøÿá ..E x if..	FF D8 FF E1 nn nn 45 78 69 66 00 00
ilbm lbm ibm iff	IFF Interleaved Bitmap Image	0 any	FORM.... ILBM	46 4F 52 4D nn nn nn nn 49 4C 42 4D
8svx 8sv svx snd	IFF 8-Bit Sampled Voice	0 any	FORM.... 8SVX	46 4F 52 4D nn nn nn nn 38 53 56 58

Gambar.15 List of file signature format JFIF

Nim : 09011181320012

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
erick95-x453M ~/Videos $ file vol1-Sektor73.raw
vol1-Sektor73.raw: ERROR: cannot open `vol1-Sektor73.raw' (No such file or directory)
erick95-x453M ~/Videos $ file vol1-Sektor73.raw
vol1-Sektor73.raw: JPEG image data, JFIF standard 1.01
erick95-x453M ~/Videos $
```

Gambar 16. Mengecek utilitas file vol1-Sektor73.raw

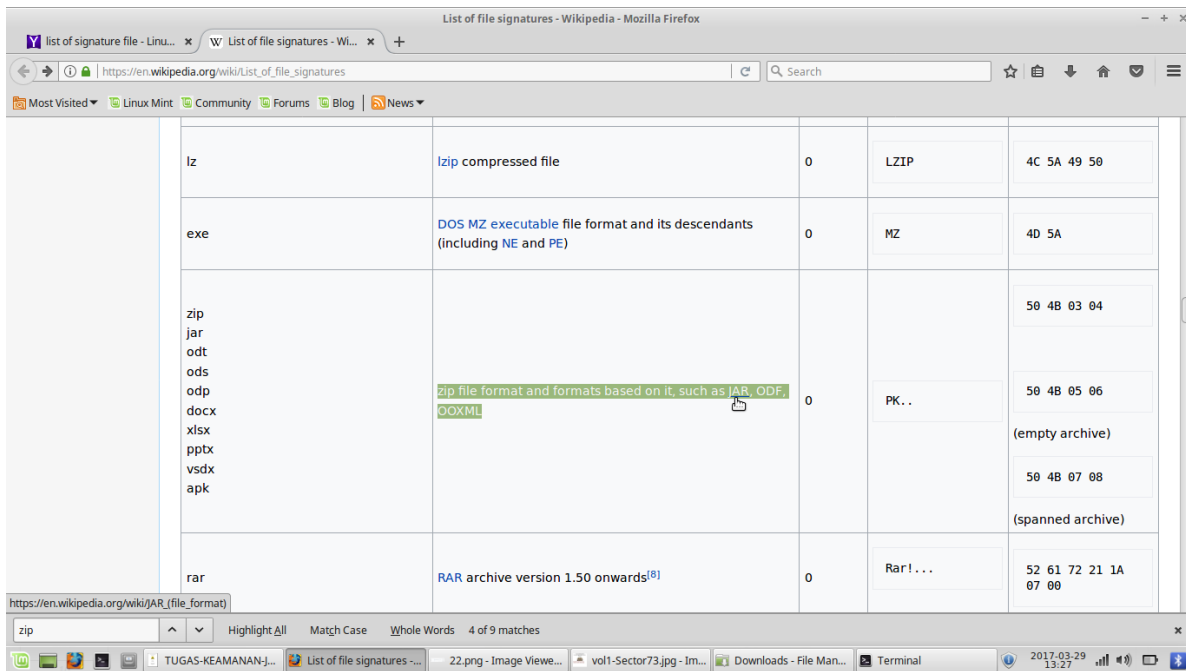
Sehingga untuk mengetahui kebenaran dan hasil dari forensics yang telah dilakukan dengan mengganti format dari file 73-103 (31) dengan nama vol1-Sektor73.raw menjadi format JPEG, untuk mendapatkan informasi-informasi yang berhubungan kasus narkoba yang ditangani,



Gambar.17 File vol1-Sektor73.raw setelah dirubah format JPEG

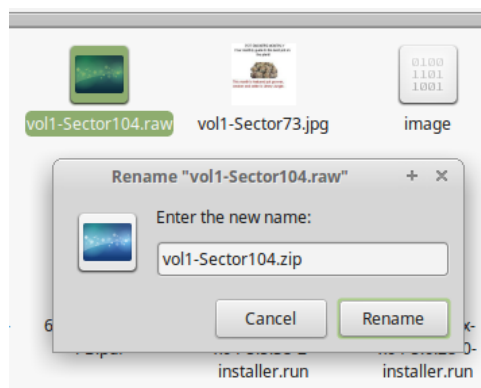
Begitu juga dengan file yang ada pada sector 104-108 (5) dilakukan hal yang sama dengan sector yang ada sebelumnya, dengan mengecek utilitas dari file dengan sector 104-108 (51)

Dengan melakukan pengecekan utilitas dari file sector 104-108 (51) dengan nama file vol1-Sektor104.raw, maka dapat dilakukan pencarian list of file signature (wikipedia) seperti pada gambar 18 berikut;



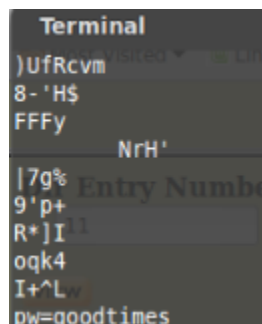
Gambar.18 . File of signature dari sector 104-108 (51)

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 19 dan dengan hasil yang diperoleh seperti pada gambar 20.



Gambar 19. 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 20.



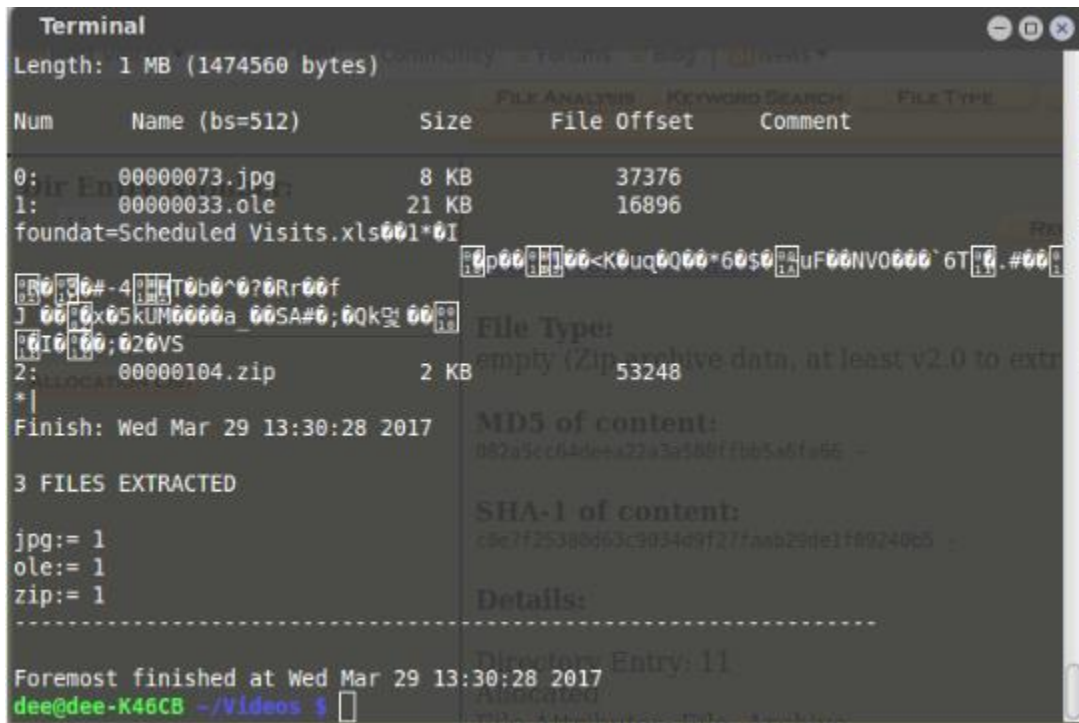
Gambar.20. Strings vol1-Sector73.raw

Dari hasil string yang telah dilakukan dengan hasil screen yang terdapat pada gambar 21, merupakan password disimpan pelaku 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 21.

	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)

Gambar.21 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 22, 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 23.



Gambar.22 Menjalankan tools Foremost

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 didalamnya ialah surat pengedar narkoba dari kasus ini, seperti yang terlihat pada gambar 28.

Nama : Erick Okvanty Haris

Tugas 6 (Keamanan Jaringan Komputer)

Nim : 09011181320012

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