TUGAS KEAMANAN JARINGAN KOMPUTER
(KOMPUTER FORENSIK)

NAMA : YAYANG PRAYOGA

NIM : 09011181320006

KELAS : SK8A

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

KOMPUTER FORENSIK

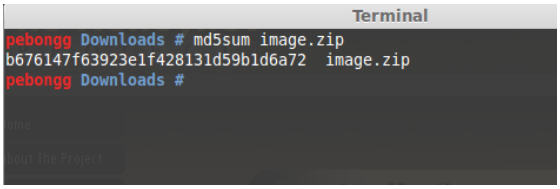
Komputer Forensik (Ilmu Komputer Forensik) adalah cabang dari ilmu forensic digital yang berkaitan dengan bukti yang ditemukan di computer dan media penyimpanan digital. Tujuan dari komputer forensik adalah untuk memeriksa media digital dengan tujuan mengidentifikasi, melestarikan, memulihkan, menganalisis dan menyajikan fakta dan opini tentang informasi digital.

PERCOBAAN DARI KOMPUTER FORENSIK

Pada percobaan dari komputer forensik berikut, berkaitan dengan kasus narkoba yaitu seseorang bernama Joe Jacobs yang ditangkap oleh polisi dengan tuduhan menjual obat-obatan terlarang ke anak sekolahan. Polisi memiliki file imaged.zip sebagai barang bukti untuk dilakukan investigasi.

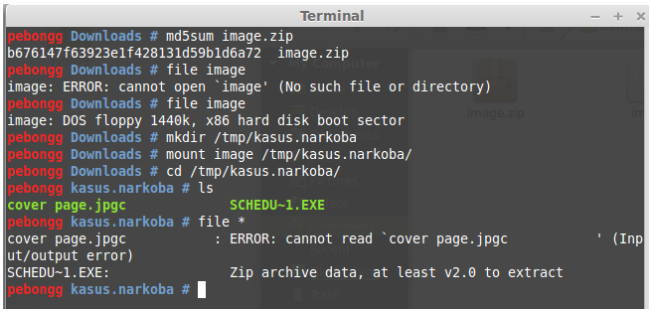
Berikut langkah-langkah untuk menganalisis file imaged.zip

1. Gunakan tool Message-Digest Algortihm 5



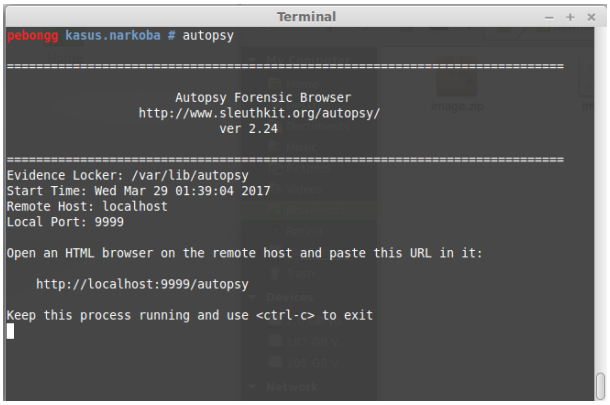
Tool Message-Digest Algortihm 5 (md5sun) ini digunakan untuk membaca file image.zip. Menggunakan md5 untuk mengacak password agar tidak disimpan sebagai plain text di database dan bisa juga digunakan untuk mengecek integritas file.

2. Ekstrak file imagezip



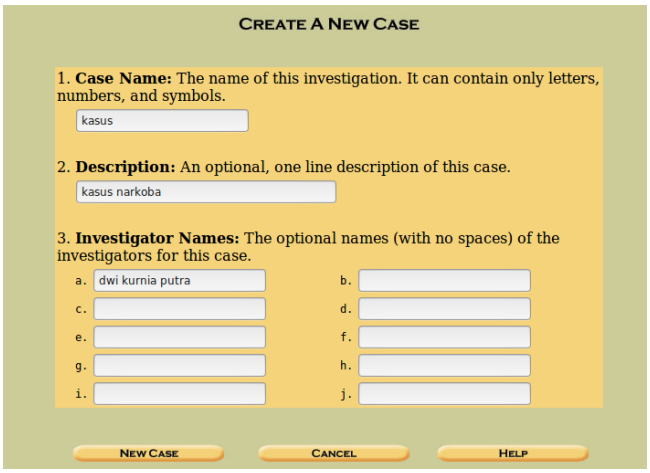
Ekstrak file imaged.zip, kemudian save pada direktori /tmp/kasus.narkoba/. Dari hasil ekstrak file imaged.zip tersebut, didapatkan 2 file yaitu cover page.jpgc dan SCHEDU-1.EXE

3. Menggunakan tool AutoPsy



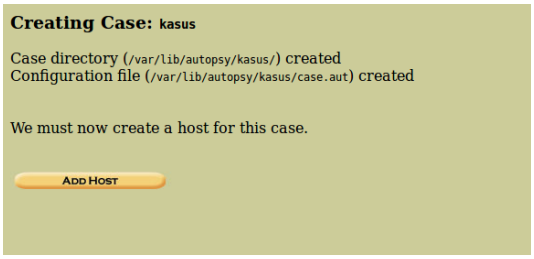
Tool autopsy atau Auto Forensic Browser adalah tool yang dibuat menggunakan bahasa perl yang berfungsi untuk melakukan digital forensic. Autopsy dapat melakukan analyze terhadapa disk image serta partition.

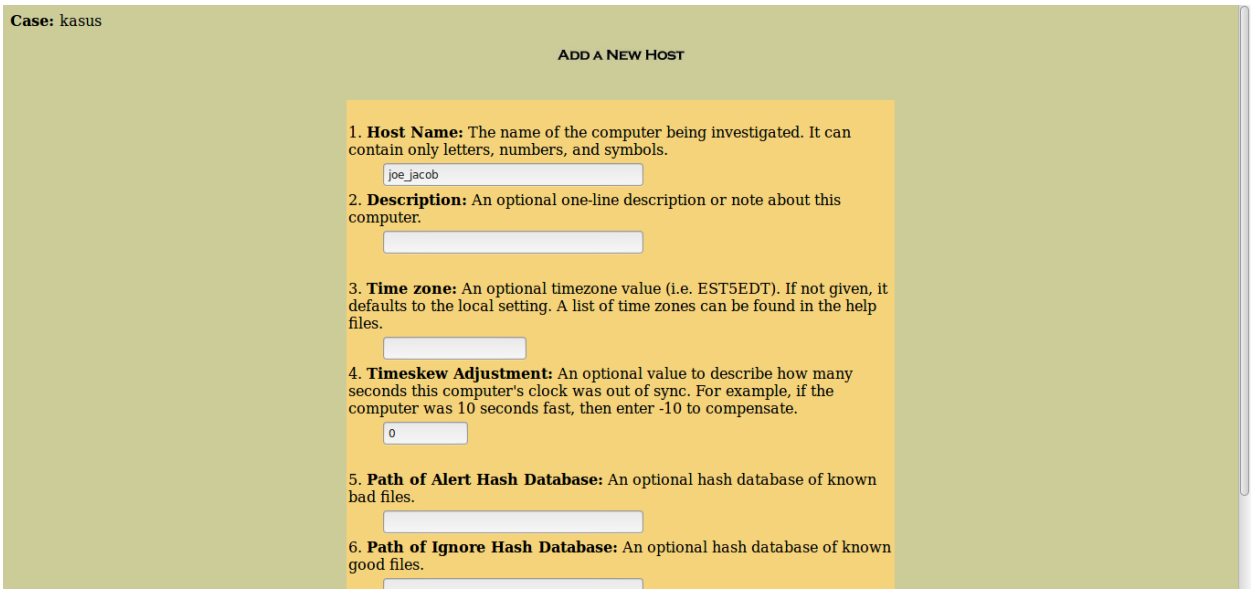
4. Membuat Case baru di AutoPsy



Pembuatan Case baru bertujuan untuk mempermudah akses kasus sehingga tidak tercampur dengan kasus forensic lainnya.

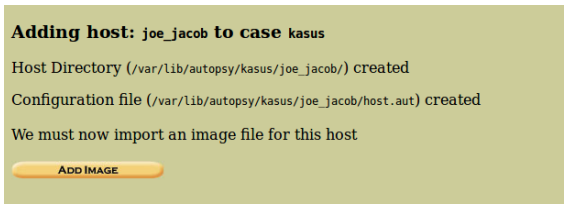
5. Membuat host baru

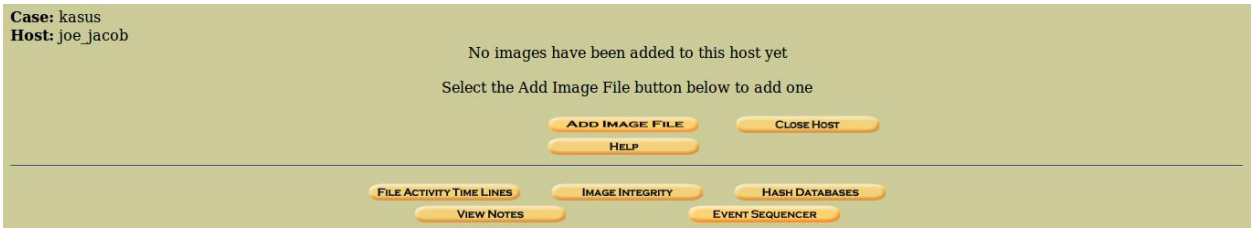


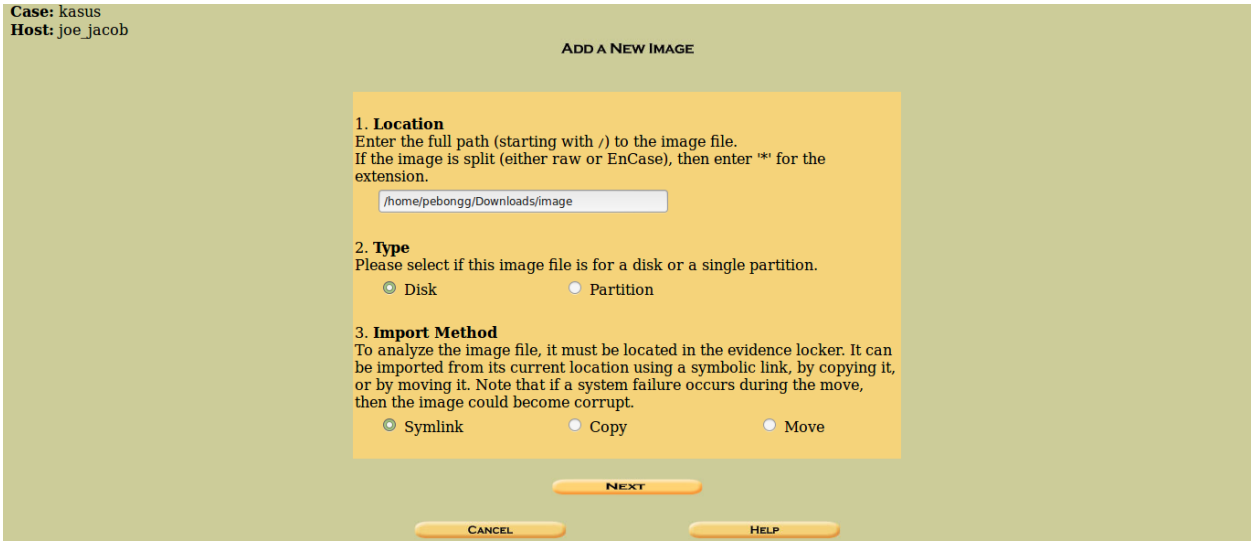


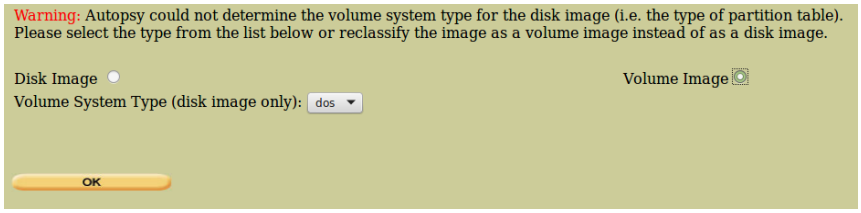
Pembuatan host baru dengan cara mengisi host name dengan nama joe_jacob dan untuk nomor 2-6 hanya optional.

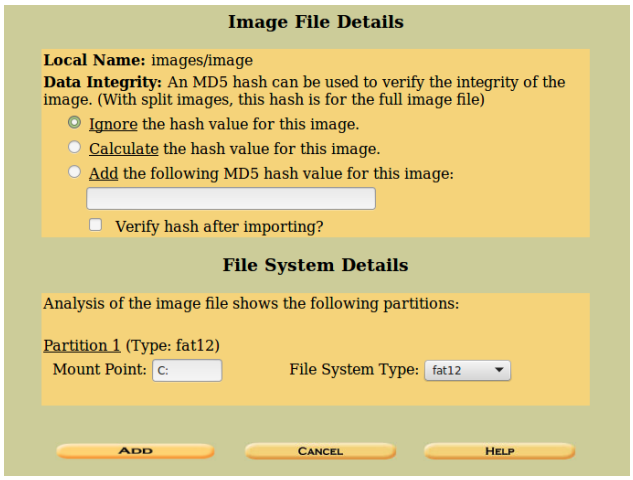
6. Proses Adding Image

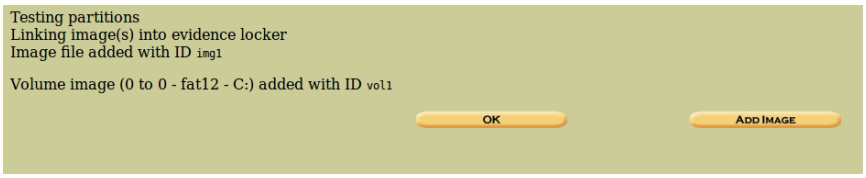


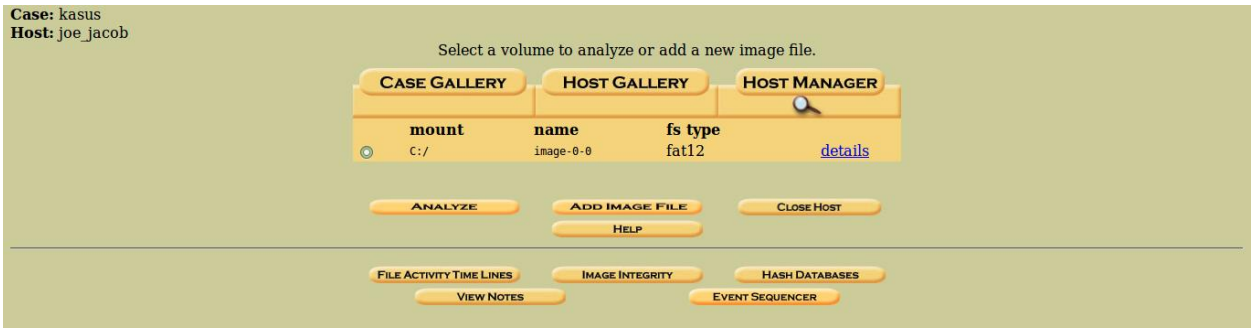






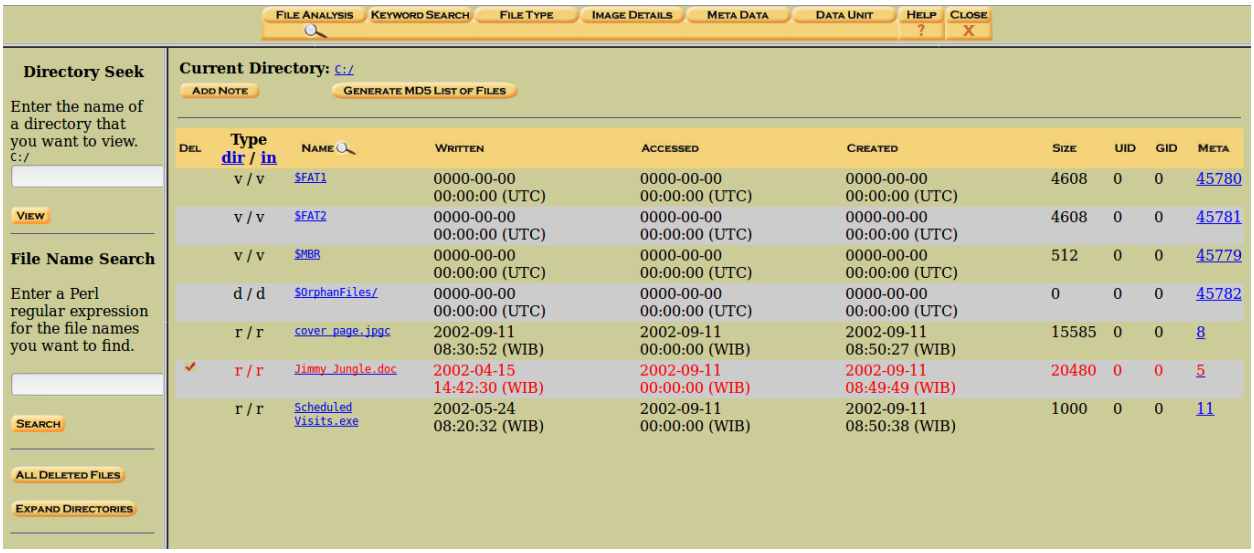


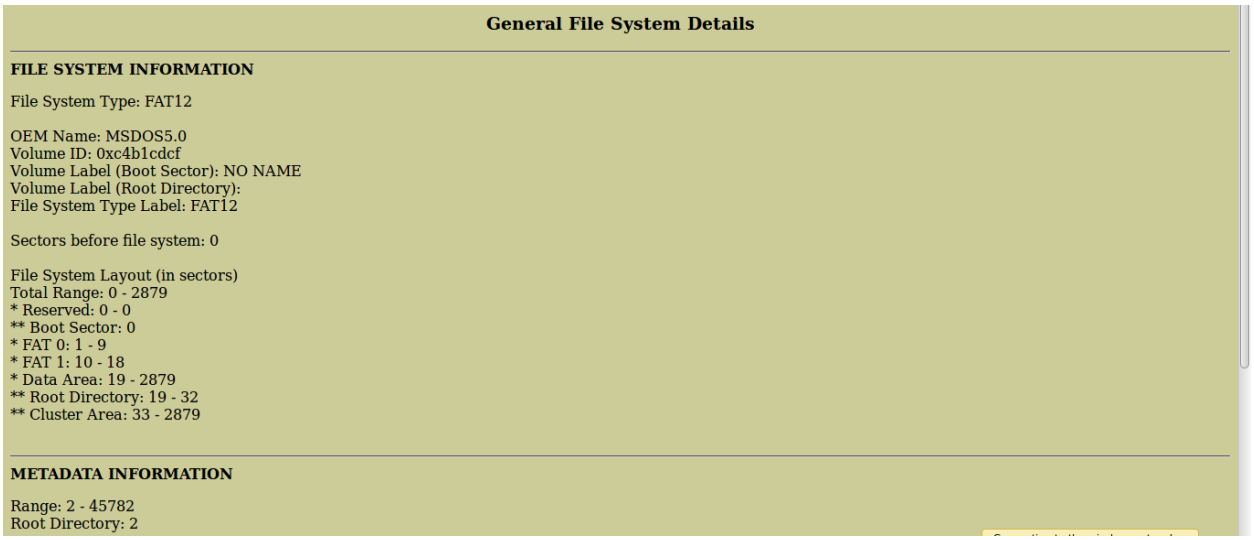


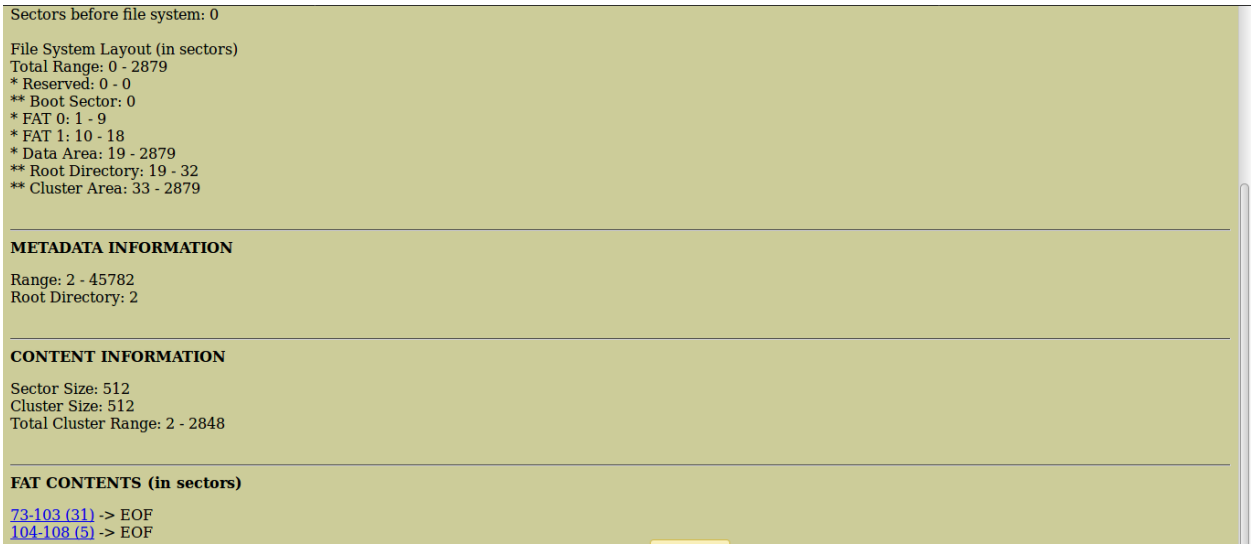


Proses adding image adalah proses yang berisikan location image file, type file yaitu disk, dan import method memilih symlink.

7. Analyze file system Fat12



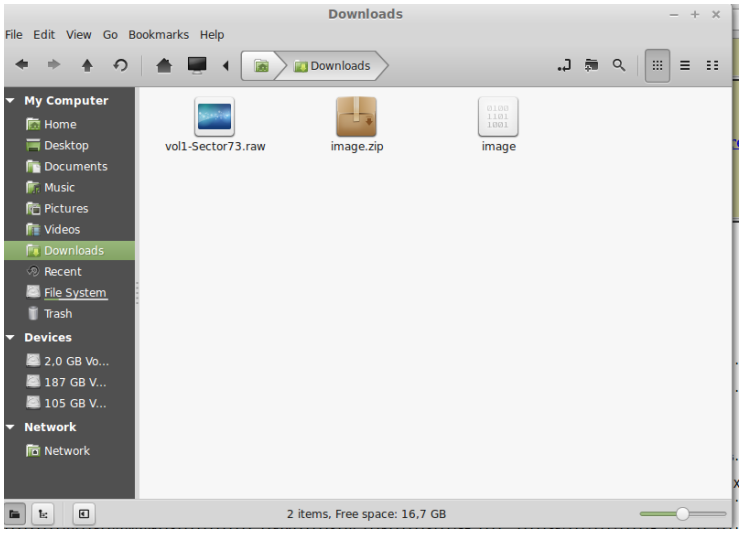


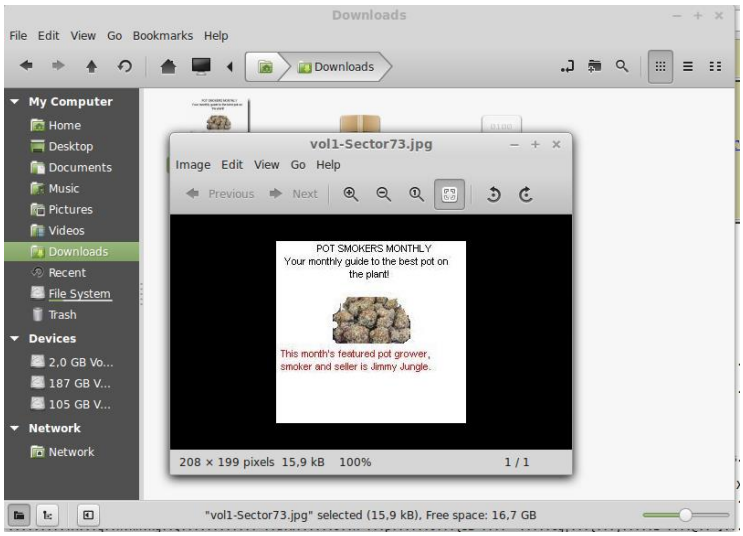


Analyze file system yang pertama adalah pada fat contents 73-103(31).

8. Analyze code JFIF

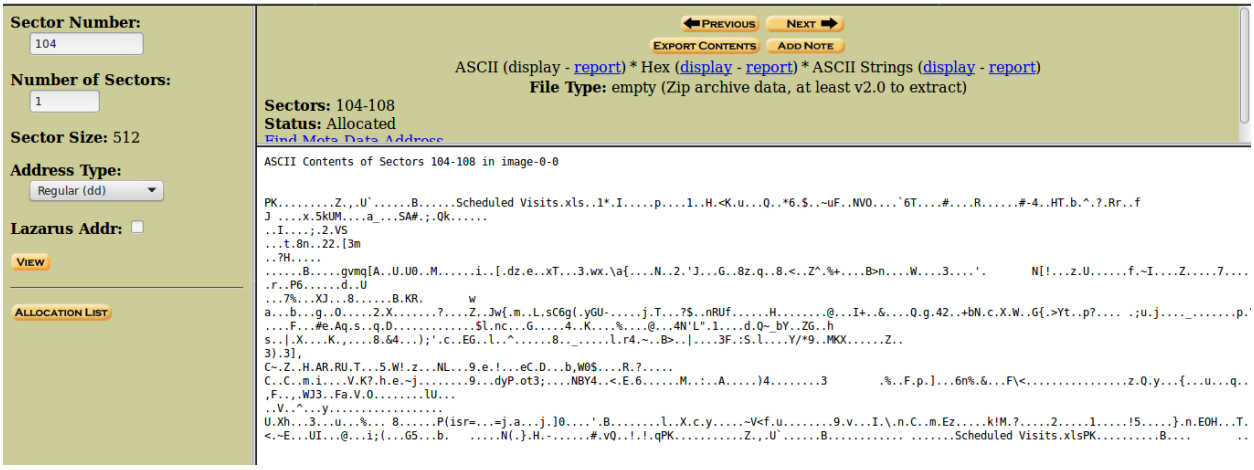
exr	OpenEXR image	0	v/1.	76 2F 31 01
bpg	Better Portable Graphics format[7]	0	BPGû	42 50 47 FB
jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿØÿÛ ÿØÿà ..J F IF.. ÿØÿá ..E x if..	FF D8 FF DB FF D8 FF E0 nn nn 4A 46 49 46 00 01 FF D8 FF E1 nn nn 45 78 69 66 00 00
ilbm lbm ibm iff	IFF Interleaved Bitmap Image	0 any	FORM.... ILBM	46 4F 52 4D nn nn nn nn 49 4C 42 4D



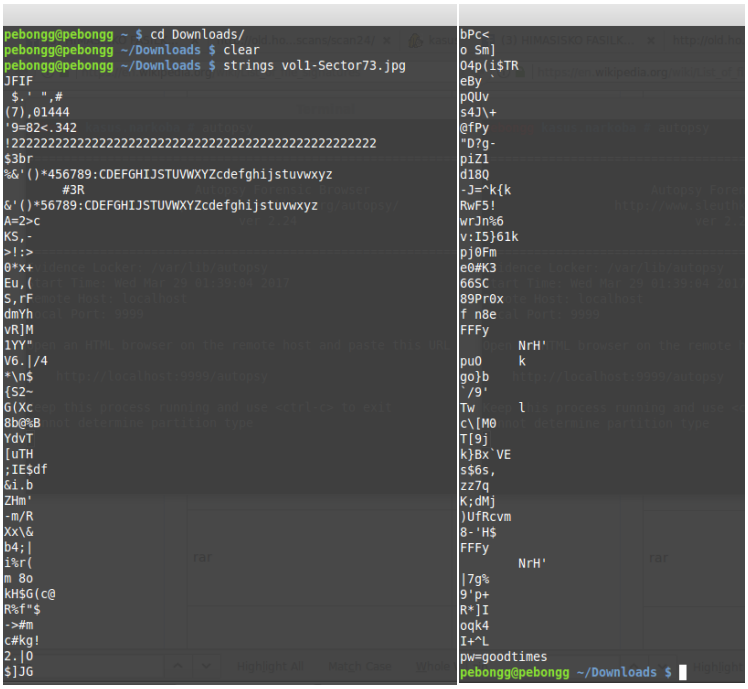


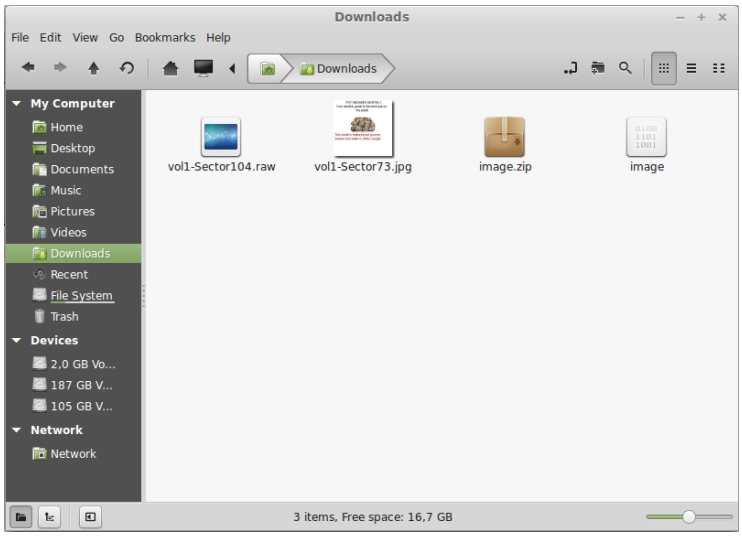
Analyze berupa code JFIF. JFIF itu sendiri merupakan format dari file .jpg.

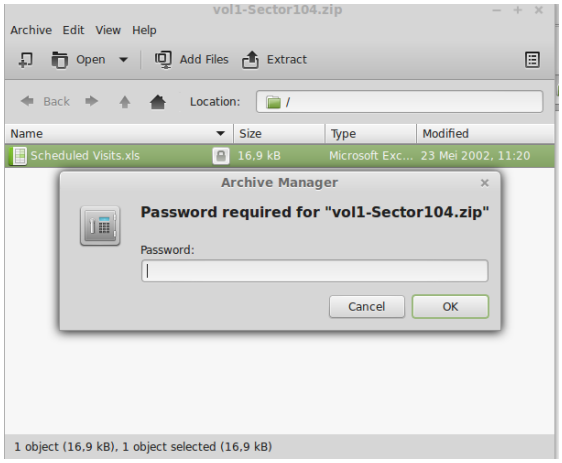
9. Analyze code PK

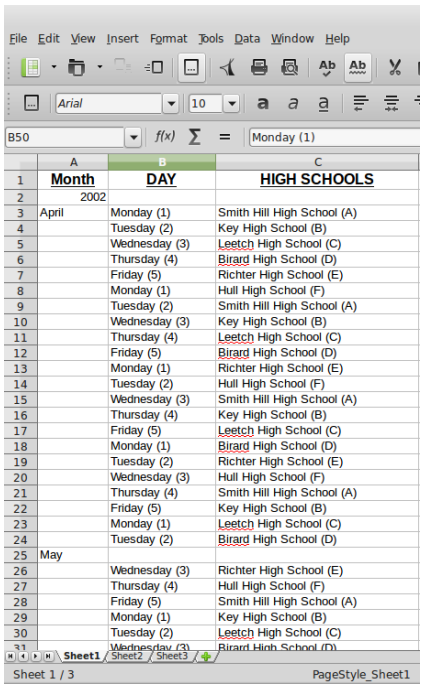


lz	lzip compressed file	0	LZIP	4C 5A 49 50
exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A
zip jar odt ods odp docx xlsx pptx vsdx apk	zip file format and formats based on it, such as JAR, ODF, OOXML	0	PK..	50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive)
rar	RAR archive version 1.50 onwards[8]	0	Rar!...	52 61 72 21 1A 07 00
				52 61 72 21 1A





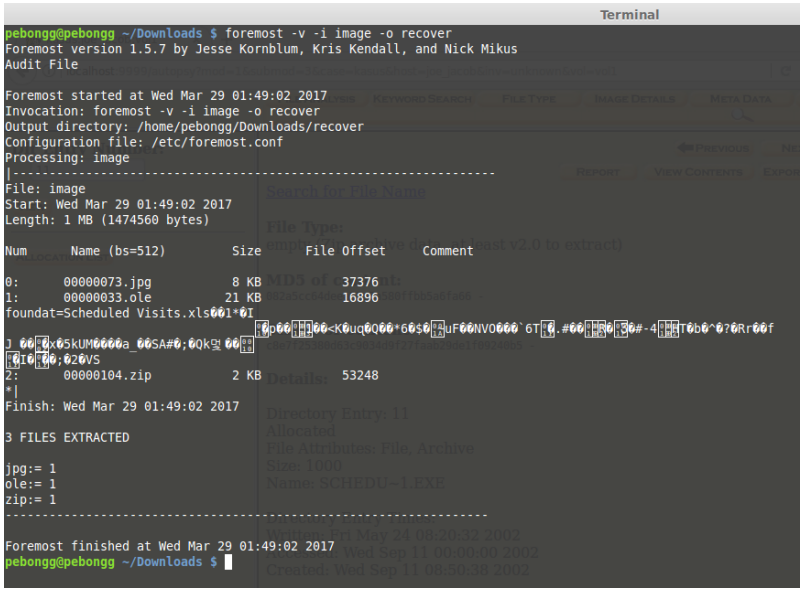


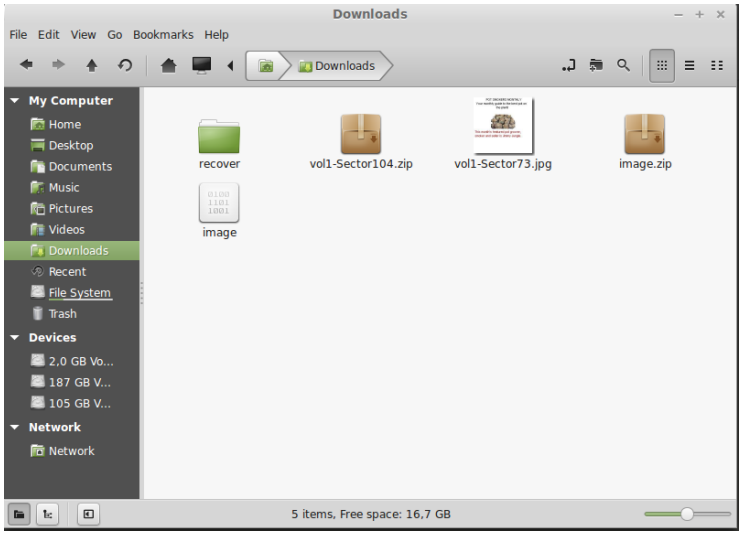


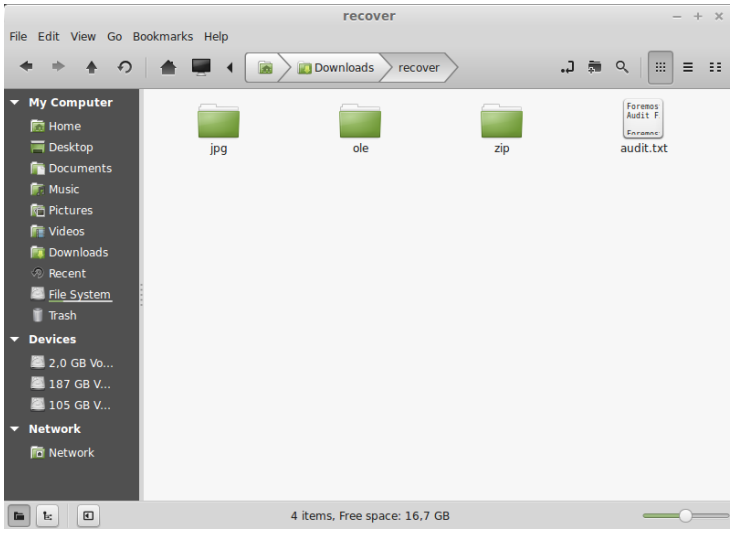
	A	B	C
1	**Month**	**DAY**	**HIGH SCHOOLS**
2	2002		
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith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

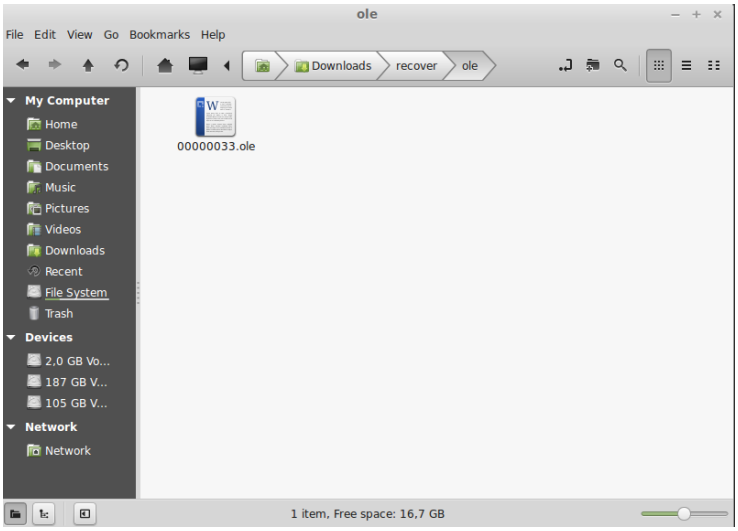
Analyze berupa code PK. PK merupakan format dari file .zip. Dari beberapa gambar di atas, terdapat file volt-sector104.raw kemudian ubah ekstensi filenya menjadi volt-sector104.zip, maka file tersebut dapat dibuka sebagai file archive. Sesuai perintah pada terminal yaitu string volt-sector73.jpg, didapatkan password file yaitu goodtimes dan digunakan untuk membuka file volt-sector104.zip. Dan didapatkan file Scheduled Visits.xls.

10. Menggunakan tool Foremost

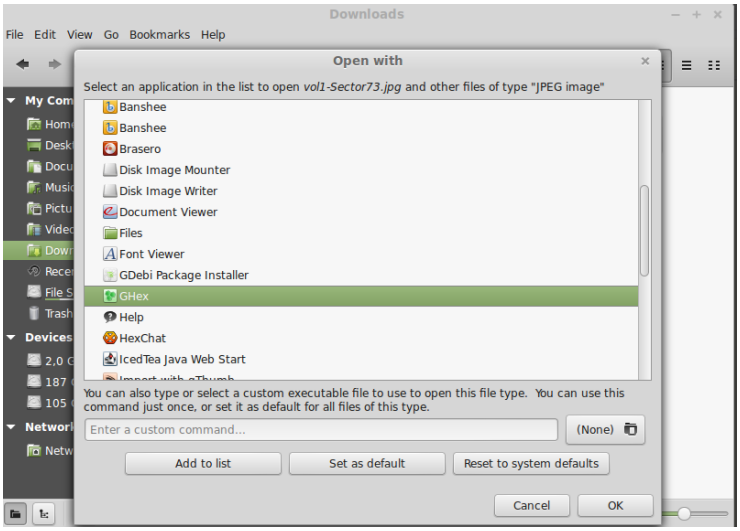


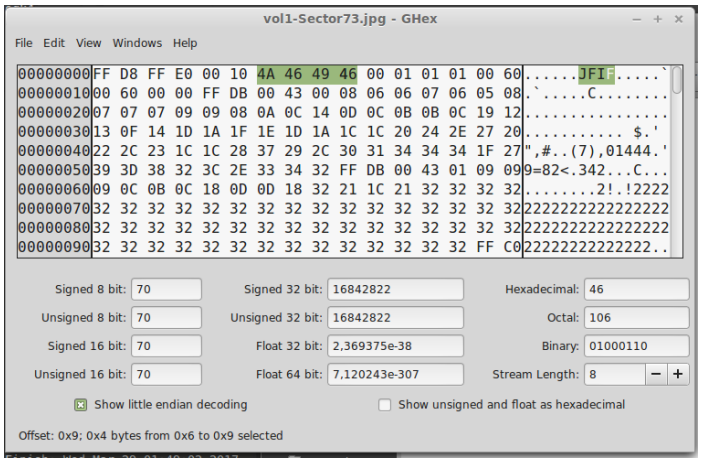

Downloads
File Edit View Go Bookmarks Help
Downloads
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Devices
2,0 GB Vo...
187 GB V...
105 GB V...
Network
Network
recover
vol1-Sector104.zip
vol1-Sector73.jpg
image.zip
image
5 items, Free space: 16,7 GB


recover
File Edit View Go Bookmarks Help
Downloads
recover
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Devices
2,0 GB Vo...
187 GB V...
105 GB V...
Network
Network
jpg
ole
zip
audit.txt
4 items, Free space: 16,7 GB


ole
File Edit View Go Bookmarks Help
Downloads
recover
ole
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Devices
2,0 GB Vo...
187 GB V...
105 GB V...
Network
Network
00000033.ole
1 item, Free space: 16,7 GB


Untitled 1 - LibreOffice Writer
File Edit View Insert Format Table Tools Window Help
Default Style
Times New Roman
12
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
Page 1 / 1
175 words, 910 characters
Default Style
English (USA)
100%


Downloads
File Edit View Go Bookmarks Help
Open with
Select an application in the list to open vol1-Sector73.jpg and other files of type "JPEG image"
Banshee
Banshee
Brasero
Disk Image Mounter
Disk Image Writer
Document Viewer
Files
Font Viewer
GDebi Package Installer
GHex
Help
HexChat
IcedTea Java Web Start
You can also type or select a custom executable file to use to open this file type. You can use this command just once, or set it as default for all files of this type.
Enter a custom command...
(None)
Add to list
Set as default
Reset to system defaults
Cancel
OK


vol1-Sector73.jpg - GHex
File Edit View Windows Help
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 ......JFIF.....`
00000010 00 60 00 00 FF DB 00 43 00 08 06 06 07 06 05 08 .`.....C........
00000020 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 ....
00000030 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 .... $.'
00000040 22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27 ",#..(7),01444.'
00000050 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 9=82<.342...C...
00000060 09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32 ....2!.!2222
00000070 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000080 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000090 32 32 32 32 32 32 32 32 32 32 32 32 32 32 FF C0 22222222222222..
Signed 8 bit: 70
Signed 32 bit: 16842822
Hexadecimal: 46
Unsigned 8 bit: 70
Unsigned 32 bit: 16842822
Octal: 106
Signed 16 bit: 70
Float 32 bit: 2,369375e-38
Binary: 01000110
Unsigned 16 bit: 70
Float 64 bit: 7,120243e-307
Stream Length: 8
Show little endian decoding
Show unsigned and float as hexadecimal
Offset: 0x9; 0x4 bytes from 0x6 to 0x9 selected

Foremost digunakan untuk mengembalikan data yang tertimpa dan diletakkan pada folder recover. Dari hasil ujicoba didapatkan 3 folder yaitu, jpg, ole dan zip. Ole merupakan file doc yang berisi surat dari Joe Jacob untuk Jimmy. Untuk mengkonversi huruf ke biner cek kembali file dari .jpg dan gunakan perintah ghex.

PERTANYAAN

Setelah berhasil mendapatkan data dari hasil uji coba, maka data tersebut dijadikan informasi untuk keperluan bahan penyelidikan. Dari informasi tersebut, hal yang menjadi pertanyaan adalah sebagai berikut :

1. Siapa pemasok narkoba Joe Jacob dan apa alamatnya ?
    - Pemasok narkoba Joe Jacob adalah Jimmy Jungle yang beralamatkan di 626 Jungle Ave Apt 2 Jungle, NY 1111
2. Data penting apa yang terdapat di file coverage .jpg dan mengapa data tersebut penting ?
    - Karena di dalam file coverage .jpg terdapat password untuk file Scheduled Visits.xls
3. Nama sekolah selain smith hill yang sering menjadi tempat transaksi Joe Jacob ?
    - Key High School
    - Leet High School
    - Birard High School
    - Ricter High School
    - Hull High School
4. Untuk setiap file proses apa yang diambil oleh tersangka untuk mengetahui orang lain ?
    - Yang dilakukan tersangka untuk menutupi kejahatannya adalah mengubah nama dan ekstensi file .zip menjadi .raw
5. Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file ?
    - Mengamati file imaged.zip menggunakan tool md5sum sebagai pengecekkan integritas file dan autopsy sebagai analyze file system forensic.