

**TUGAS KEAMANAN JARINGAN KOMPUTER
(KOMPUTER FORENSIK)**



NAMA : YAYANG PRAYOGA

NIM : 09011181320006

KELAS : SK8A

**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

KOMPUTER FORENSIK

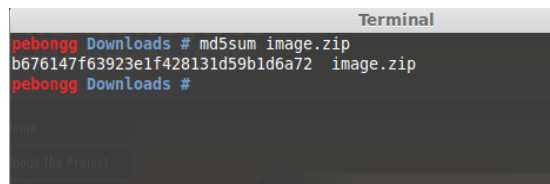
Komputer Forensik (Ilmu Komputer Forensik) adalah cabang dari ilmu forensic digital yang berkaitan dengan bukti yang ditemukan di computer dan media penyimpanan digital. Tujuan dari komputer forensik adalah untuk memeriksa media digital dengan tujuan mengidentifikasi, melestarikan, memulihkan, menganalisis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

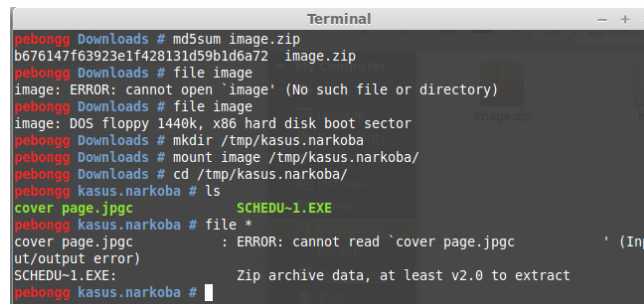
1. Gunakan tool Message-Digest Algoritim 5



```
Terminal
pebongg Downloads # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
pebongg Downloads #
```

Tool Message-Digest Algoritim 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.

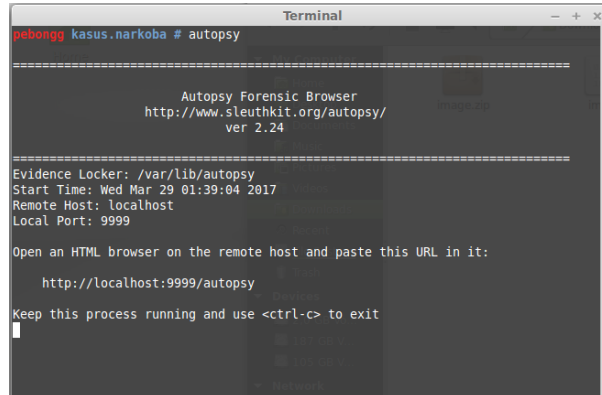
2. Ekstrak file imagezip



```
Terminal
pebongg Downloads # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
pebongg Downloads # file image
image: ERROR: cannot open 'image' (No such file or directory)
pebongg Downloads # file image
image: DOS floppy 1440k, x86 hard disk boot sector
pebongg Downloads # mkdir /tmp/kasus.narkoba
pebongg Downloads # mount image /tmp/kasus.narkoba/
pebongg Downloads # cd /tmp/kasus.narkoba/
pebongg kasus.narkoba # ls
cover page.jpgc          SCHEDU-1.EXE
pebongg kasus.narkoba # file *
cover page.jpgc          : ERROR: cannot read `cover page.jpgc' (Inp
ut/output error)
SCHEDU-1.EXE:            Zip archive data, at least v2.0 to extract
pebongg kasus.narkoba #
```

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



```
pebongg kasus.narkoba # autopsy
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /var/lib/autopsy
Start Time: Wed Mar 29 01:39:04 2017
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

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

4. Membuat Case baru di AutoPsy



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="dwi kurnia putra"/>	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"/>

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

5. Membuat host baru

Creating Case: kasus

Case directory (/var/lib/autopsy/kasus/) created
 Configuration file (/var/lib/autopsy/kasus/case.aut) created

We must now create a host for this case.

Case: kasus

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **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.

4. **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.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

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

6. Proses Adding Image

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

Case: kasus
Host: joe_jacob

No images have been added to this host yet
Select the Add Image File button below to add one

ADD IMAGE FILE

CLOSE HOST

HELP

FILE ACTIVITY TIME LINES

IMAGE INTEGRITY

HASH DATABASES

VIEW NOTES

EVENT SEQUENCER

Case: kasus
Host: joe_jacob

ADD A NEW IMAGE

1. Location

Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/home/pebongg/Downloads/image

2. Type

Please select if this image file is for a disk or a single partition.

Disk

Partition

3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink

Copy

Move

NEXT

CANCEL

HELP

Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image

Volume Image

Volume System Type (disk image only): dos

OK

Image File Details

Local Name: images/image
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

Ignore the hash value for this image.
 Calculate the hash value for this image.
 Add the following MD5 hash value for this image:

 Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat12)
 Mount Point: File System Type:

Testing partitions
 Linking image(s) into evidence locker
 Image file added with ID img1
 Volume image (0 to 0 - fat12 - C:) added with ID vol1

Case: kasus
Host: joe_jacob

Select a volume to analyze or add a new image file.

CASE GALLERY	HOST GALLERY	HOST MANAGER
mount	name	fs type
C:/	image-0-0	fat12
<input checked="" type="radio"/>		details

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

7. Analyze file system Fat12

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE ? X

Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

Current Directory: C:/

ADD NOTE GENERATE MDS LIST OF FILES

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	SEAT1	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	SEAT2	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	\$MBR	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.jpg	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

VIEW

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

General File System Details

FILE SYSTEM INFORMATION

File System Type: FAT12

OEM Name: MSDOS5.0
Volume ID: 0xc4b1cdef
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT12

Sectors before file system: 0

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

Sectors before file system: 0

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

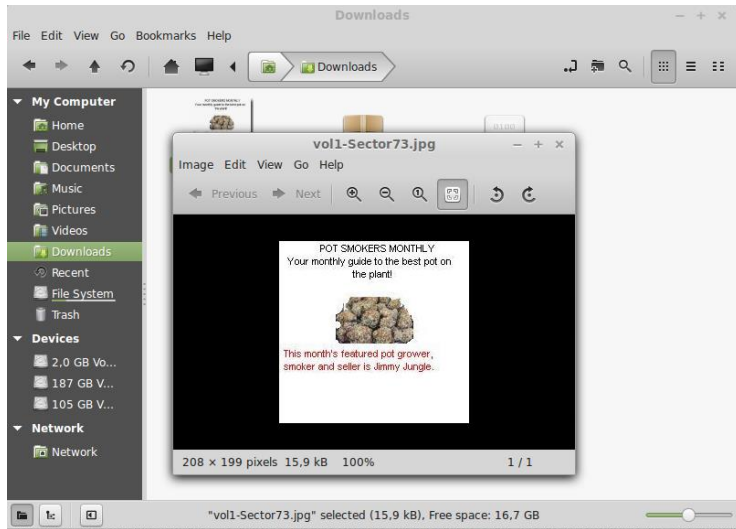
CONTENT INFORMATION

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

FAT CONTENTS (in sectors)

[73-103 \(31\)](#) -> EOF
[104-108 \(5\)](#) -> EOF

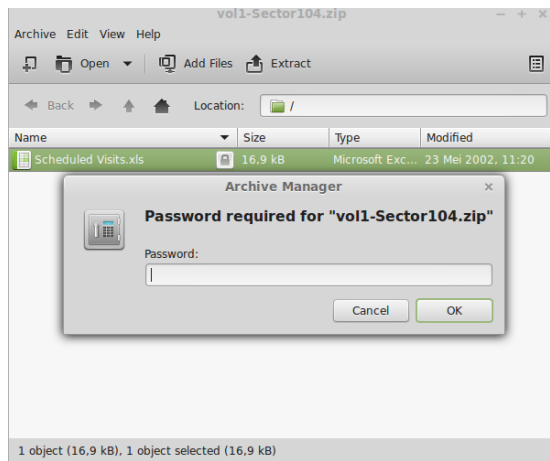
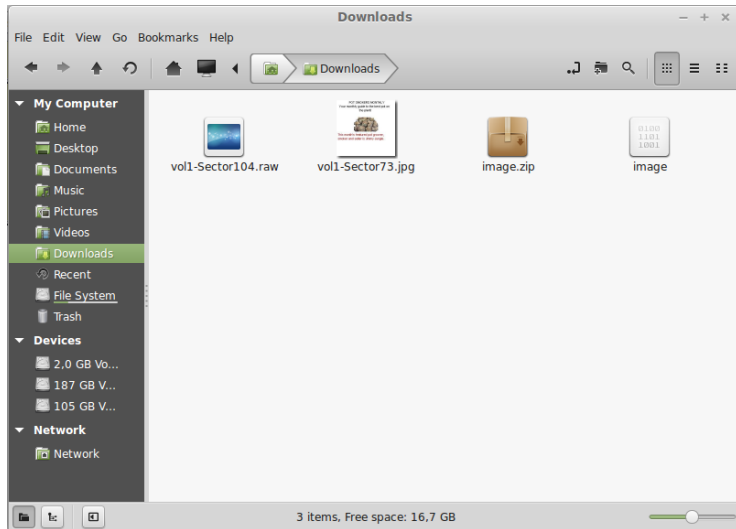
Analyze file system yang pertama adalah pada fat contents 73-103(31).



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

9. Analyze code PK

<p>Sector Number: 104</p> <p>Number of Sectors: 1</p> <p>Sector Size: 512</p> <p>Address Type: Regular (dd)</p> <p>Lazarus Addr: <input type="checkbox"/></p> <p>VIEW</p> <p>ALLOCATION LIST</p>	<p>◀ PREVIOUS NEXT ▶</p> <p>EXPORT CONTENTS ADD NOTE</p> <p>ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)</p> <p>File Type: empty (Zip archive data, at least v2.0 to extract)</p> <p>Sectors: 104-108 Status: Allocated Find Meta Data Address</p> <p>ASCII Contents of Sectors 104-108 in image-0-0</p> <pre>PK.....Z,,U'.....B.....Scheduled Visits.xls..1*.I....p...1..H.<K.u...0..*6.\$...uF..NW0...`6T...#...R.....#-4..HT.b.^?.Rr..f J...x.5kUM...a...SA#;:;0k..... ..I....;2.VS ...t.8n..22.[3m ..?H.....B.....gvmq[A..U.U0..M.....i..[.dz.e..XT...3.wx.\a{...N..2.'J...G..Bz.q..8.<..Z%.%*...B>n...W...3...'. N[!...z.U.....f.-I...Z...7... .r.P6.....0..U ..78...XJ...8.....B.KR. W a...b...g..0.....2.X.....?.....Z..Jw{m..L.sC6g{yGU.....j.T...?\$.nRUF.....H.....@...I+..6...0.g.42..+bN.c.X.W..6{>Yt...p7...;u.j.....p~ ...F...#e.Aq.s..q.d.....\$l.nc...G.....4..K...%...@..4N'L".1...d.0-..bY..Z6..h s...j.X...K...8.64...);'.c..EG..l..^.....8.....l.r4.>..B>...}...3F::S.l...Y/*9..MKX.....Z.. 3).3], C->.Z..H.AR.RU.T...5.Wf.z...NL...9.e.l...eC.D..b,W6S...R..?.... C..C..m.1...V.K7.h.e.-j.....9...dyP.ot3;...NB44.<.E.6.....M...A.....)4.....3 %..F.p.]...6n%.&...F\<.....z.0.y...{...u...q.. .F...W03...Fa.V.0.....LU... ..V...^..y..... U.Xh...3..u...%...8.....P(isr=...=j.a...j.]0...'.B.....l..X.c.y.....-Vcf.u.....9.v...I..n.C..m.Ez...kIM?...2...1...!S.....}.n.EOH...T. <-E...UI...@...;{...G5..b.N(.).H.....#..vQ..l.l.qPK.....Z,,U'.....B.....Scheduled Visits.xlsPK.....B.....</pre>
---	--



The screenshot shows a spreadsheet application window with a menu bar (File, Edit, View, Insert, Format, Tools, Data, Window, Help) and a toolbar. The spreadsheet content is as follows:

	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)

The spreadsheet footer shows 'Sheet 1 / 3' and 'PageStyle_Sheet1'.

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

The screenshot shows the Foremost web interface. On the left, there is a sidebar with 'Dir Entry Number: 11', a 'VIEW' button, and an 'ALLOCATION LIST' button. The main content area displays the following information:

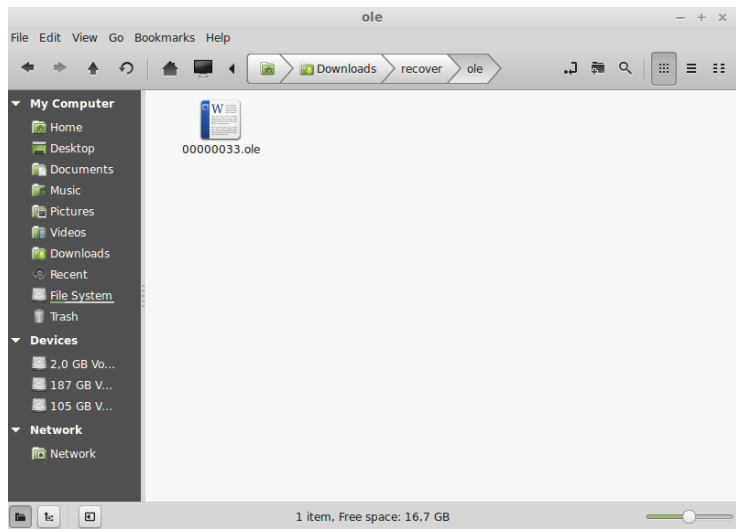
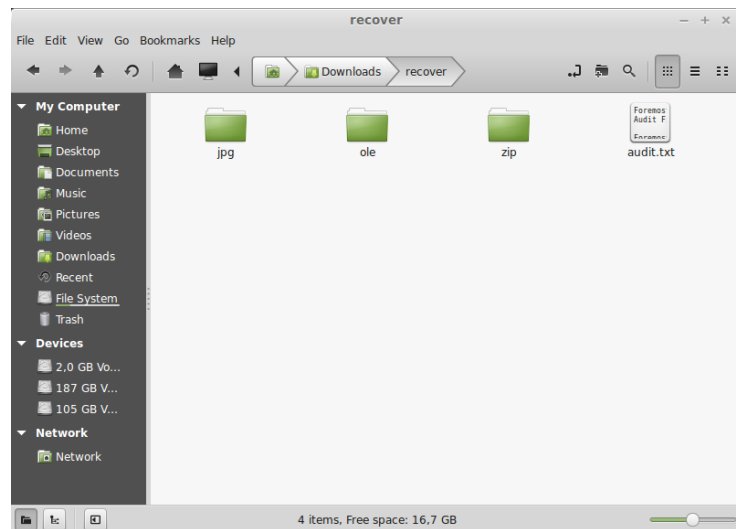
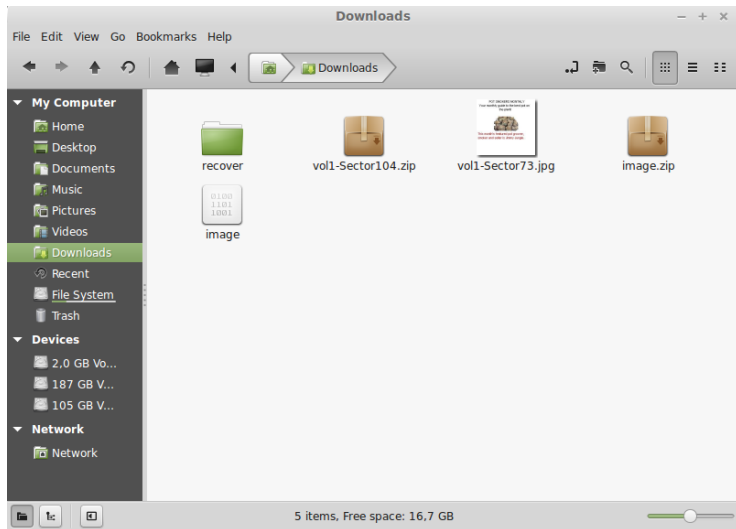
- Search for File Name**
- File Type:** empty (Zip archive data, at least v2.0 to extract)
- MD5 of content:** 082a5cc64deea22a3a580ffb5a6fa66 -
- SHA-1 of content:** c8e7f25380d63c9034d9f27faab29de1f09240b5 -
- Details:**
 - Directory Entry: 11
 - Allocated
 - File Attributes: File, Archive
 - Size: 1000
 - Name: SCHEDU~1.EXE
 - Directory Entry Times:
 - Written: Fri May 24 08:20:32 2002
 - Accessed: Wed Sep 11 00:00:00 2002
 - Created: Wed Sep 11 08:50:38 2002
 - Sectors: [104](#) [105](#)

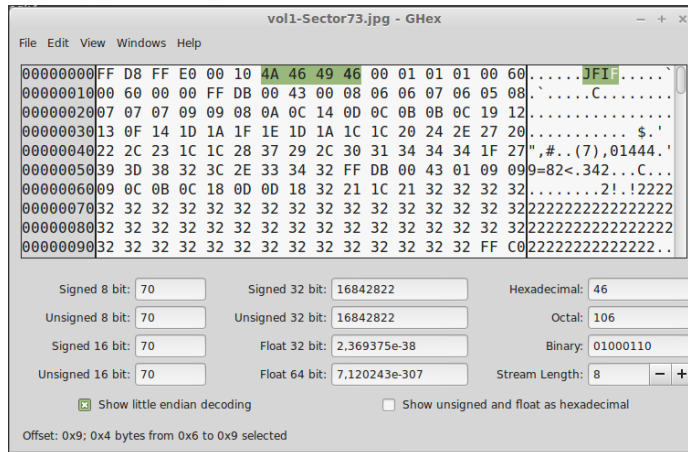
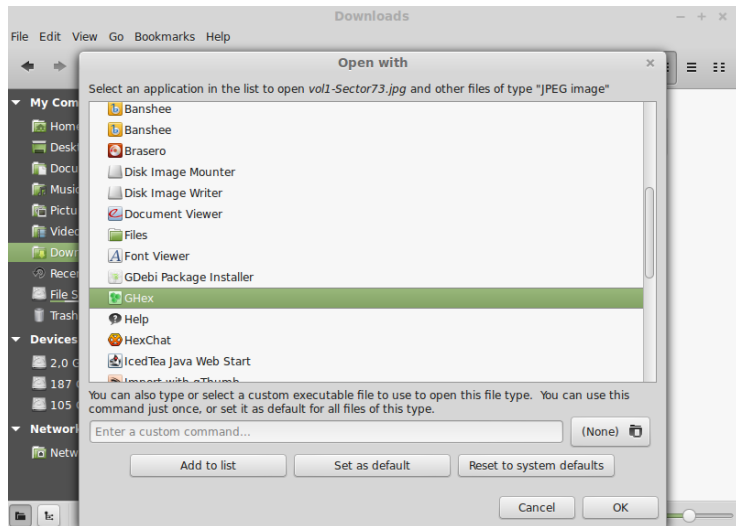
```

Terminal
pebongg@pebongg ~/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 01:49:02 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/pebongg/Downloads/recover
Configuration file: /etc/foremost.conf
Processing: image
-----
File: image
Start: Wed Mar 29 01:49:02 2017
Length: 1 MB (1474560 bytes)
-----
File Type: empty (Zip archive data, at least v2.0 to extract)
-----
Num   Name (bs=512)      Size  File Offset  Comment
-----
0:    00000073.jpg      8 KB  1123  37376
1:    00000033.ole      21 KB  16896
foundat=Scheduled Visits.xls
-----
2:    00000104.zip       2 KB  53248
-----
Finish: Wed Mar 29 01:49:02 2017
3 FILES EXTRACTED
-----
jpg:= 1
ole:= 1
zip:= 1
-----
Foremost finished at Wed Mar 29 01:49:02 2017
pebongg@pebongg ~/Downloads $

```





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
 - Rictor 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 pengecekan integritas file dan autopsy sebagai analyze file system forensic.