NAMA : DWI KURNIA PUTRA

NIM : 09011181320019

MK : KEAMANAN JARINGAN KOMPUTER

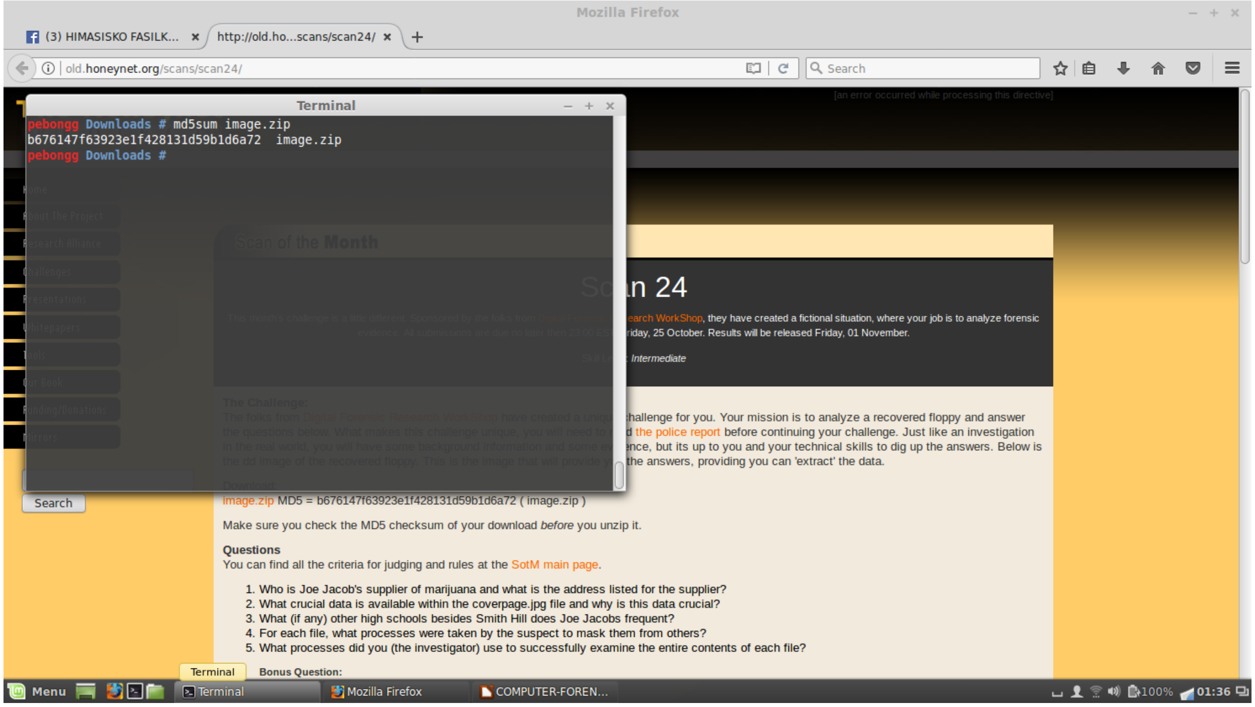
KOMPUTER FORENSIK

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 computer forensic 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 computer forensic 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



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

earch WorkShop, they have created a fictional situation, where your job is to analyze forensic evidence. ... riday, 25 October. Results will be released Friday, 01 November.

Skill Level: Intermediate

The Challenge:
... challenge for you. Your mission is to analyze a recovered floppy and answer the questions below. ... d the police report before continuing your challenge. Just like an investigation in the real world, you will have some background information and some evidence, but its up to you and your technical skills to dig up the answers. Below is ... the answers, providing you can 'extract' the data.

Download:
image.zip MD5 = b676147f63923e1f428131d59b1d6a72 (image.zip)

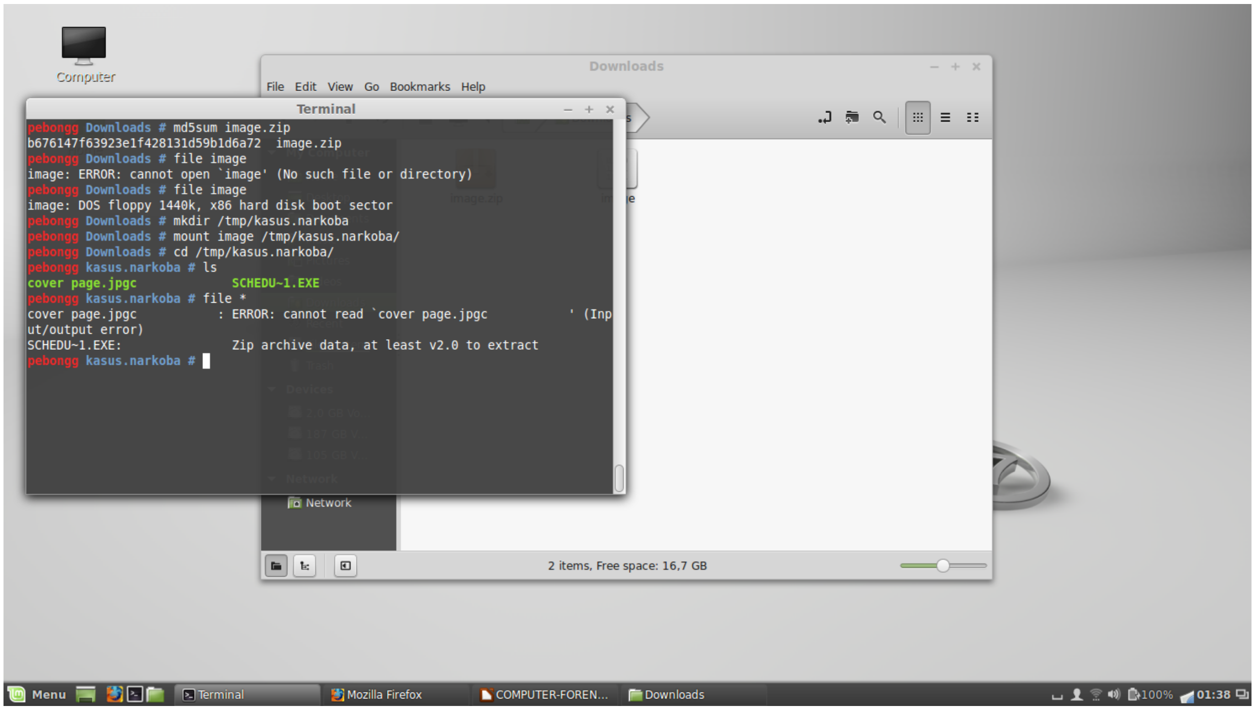
Make sure you check the MD5 checksum of your download *before* you unzip it.

Questions
You can find all the criteria for judging and rules at the SotM main page.

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?

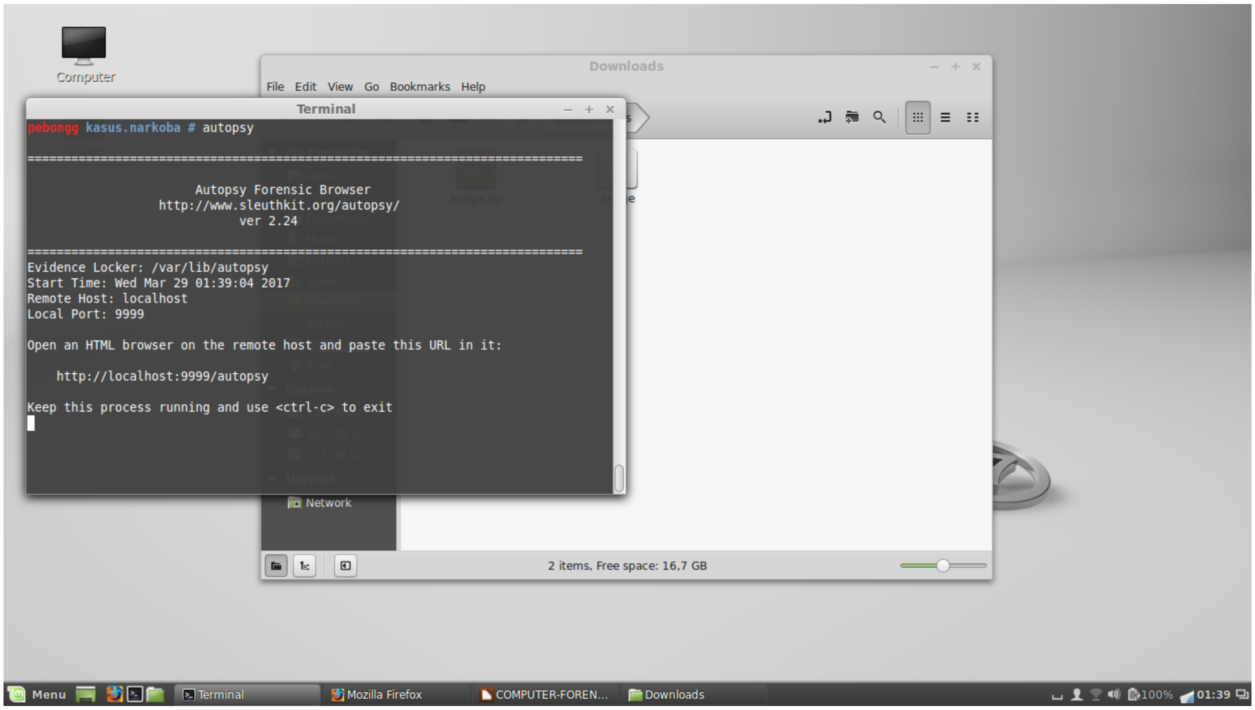
Bonus Question:

Menggunakan tool md5sun untuk membaca file image.zip. Tool md5sun (Message-Digest Algortihm 5) merupakan fungsi hash kriptografik untuk keperluan keamanan data. Menggunakan md5 untuk mengacak password agar tidak disimpan sebagai plaintext di database dan bisa juga digunakan untuk mengecek integritas file.



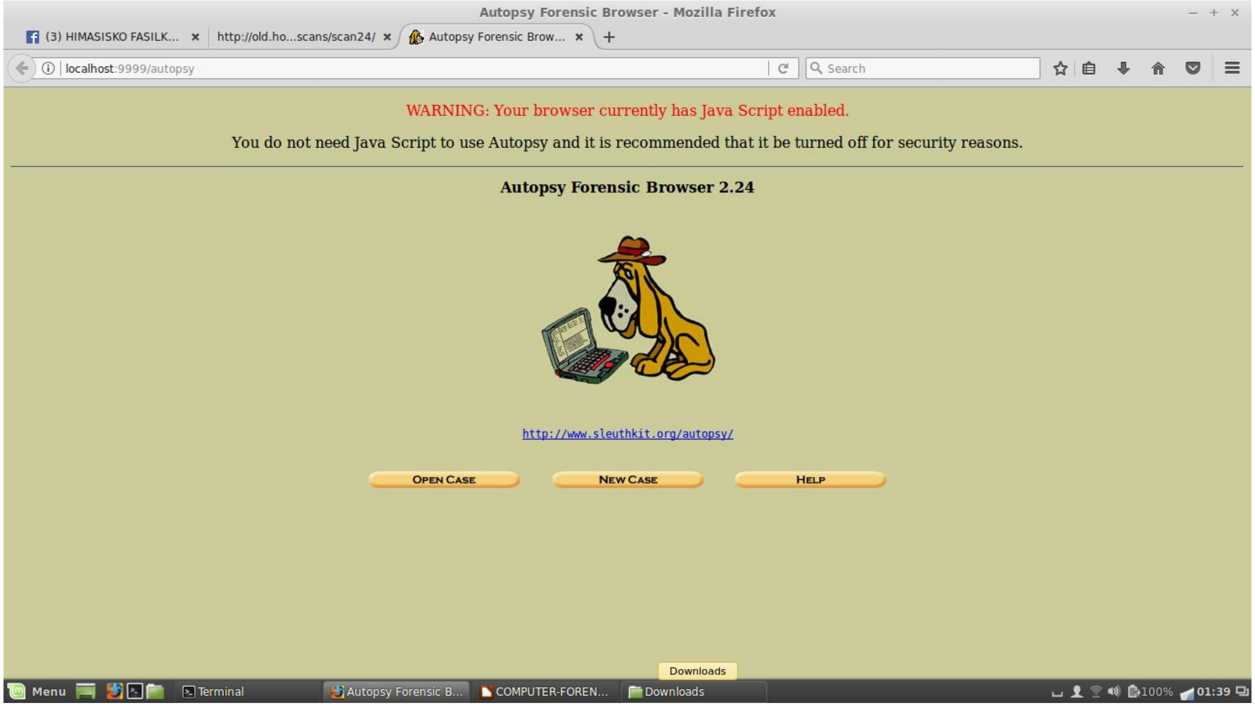
```
pebongg Downloads # md5sum image.zip
b676147f63923e1f428131d59b1d6a72  image.zip
pebongg Downloads # file image
image: ERROR: cannot open `image' (No such file or directory)
pebongg Downloads # file image
image: DOS floppy 1440k, x86 hard disk boot sector
pebongg Downloads # mkdir /tmp/kasus.narkoba
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 # 
```

Mengekstrak file imaged.zip, lalu disimpan dalam direktori /tmp/kasus.narkoba/. Dari hasil ekstrak file imaged.zip tersebut, didapatkan 2 file yaitu cover page.jpgc dan SCHEDU-1.EXE



```
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
```

Menggunakan tool autopsy atau Auto Forensic Browser yang mana merupakan tool yang dibuat menggunakan Bahasa perl berfungsi untuk melakukan digital forensic. Autopsy dapat melakukan analyze terhadapa disk image serta partition.

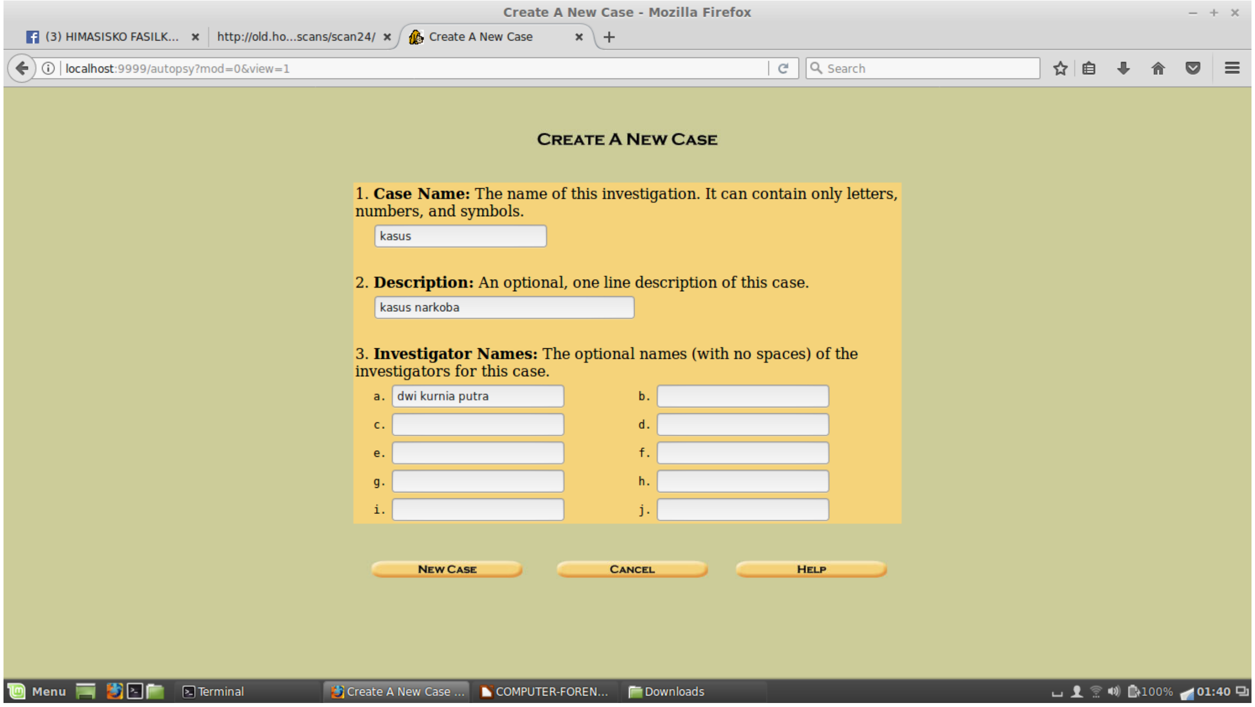


WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/


Create A New Case - Mozilla Firefox
(3) HIMASISKO FASILK...
http://old.ho...scans/scan24/
Create A New Case
localhost:9999/autopsy?mod=0&view=1
Search

CREATE A NEW CASE

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

kasus

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

kasus narkoba

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

a. dwi kurnia putra b.

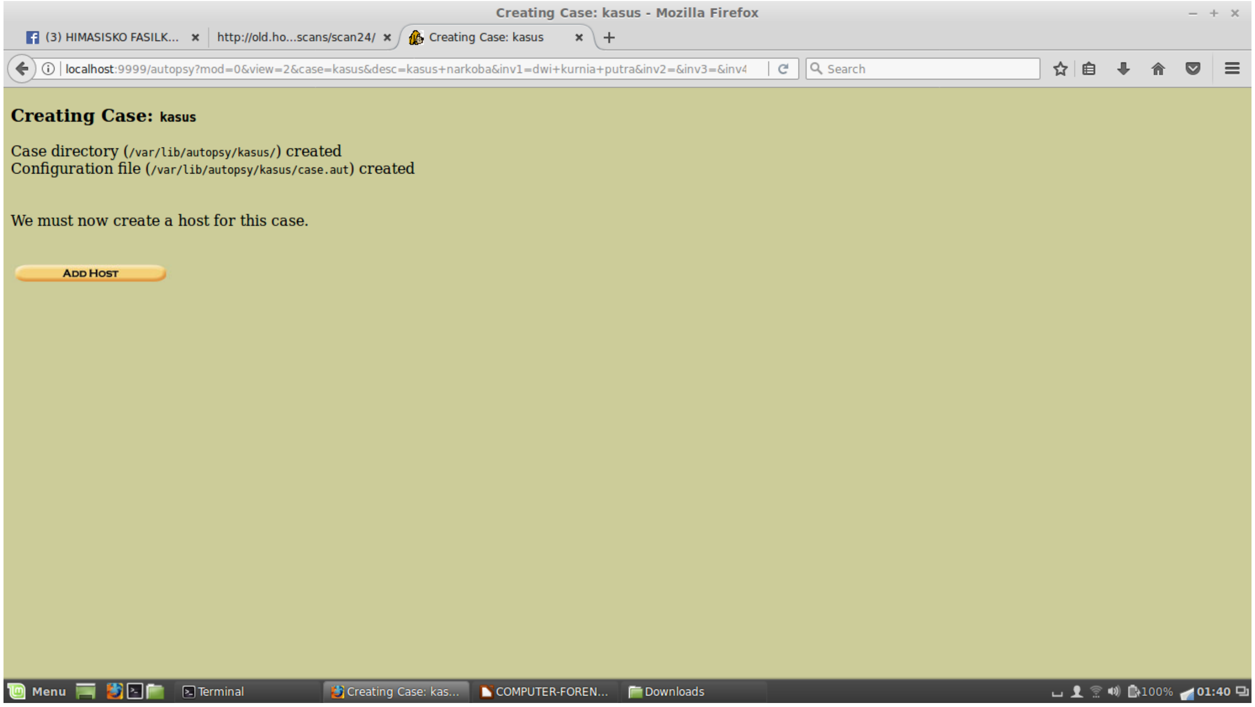
c. d.

e. f.

g. h.

i. j.

Gambar di atas merupakan langkah-langkah untuk pembuatan newcase, yang mana bertujuan mempermudah akses kasus sehingga tidak tercampur dengan kasus forensic lainnya.

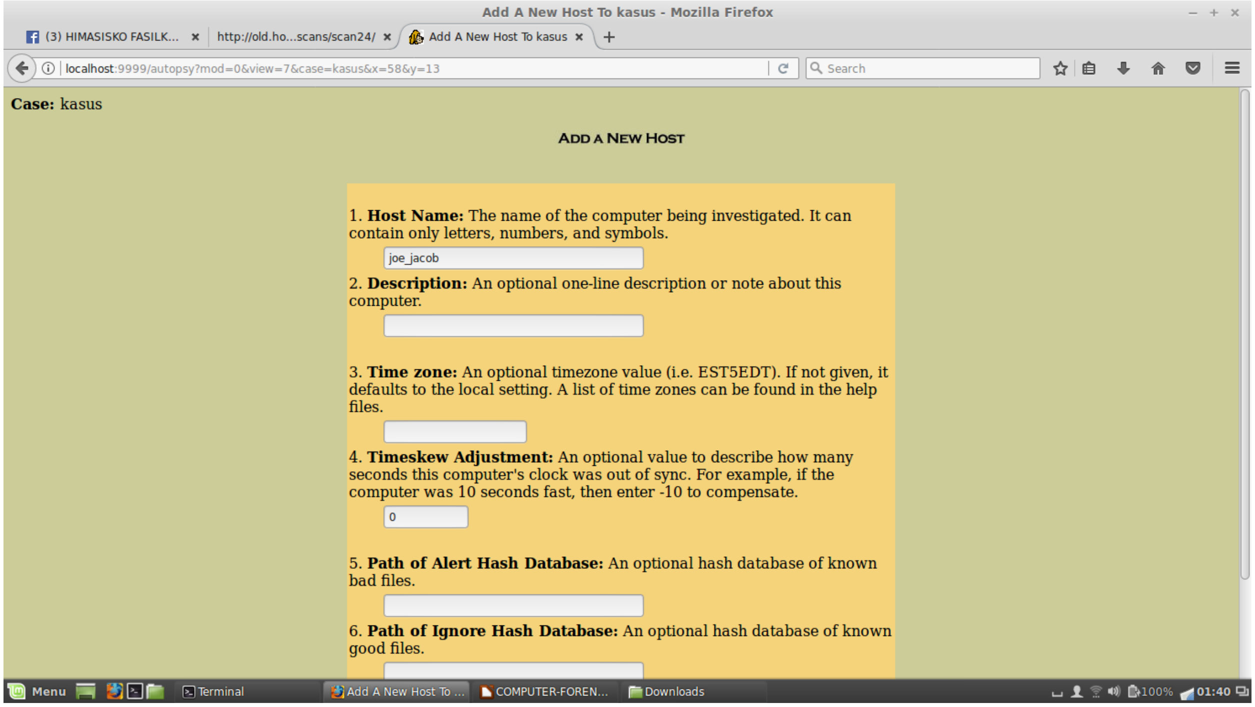


localhost:9999/autopsy?mod=0&view=2&case=kasus&desc=kasus+narkoba&inv1=dwi+kurnia+putra&inv2=&inv3=&inv4

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.



localhost:9999/autopsy?mod=0&view=7&case=kasus&x=58&y=13

Case: kasus

ADD A NEW HOST

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

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

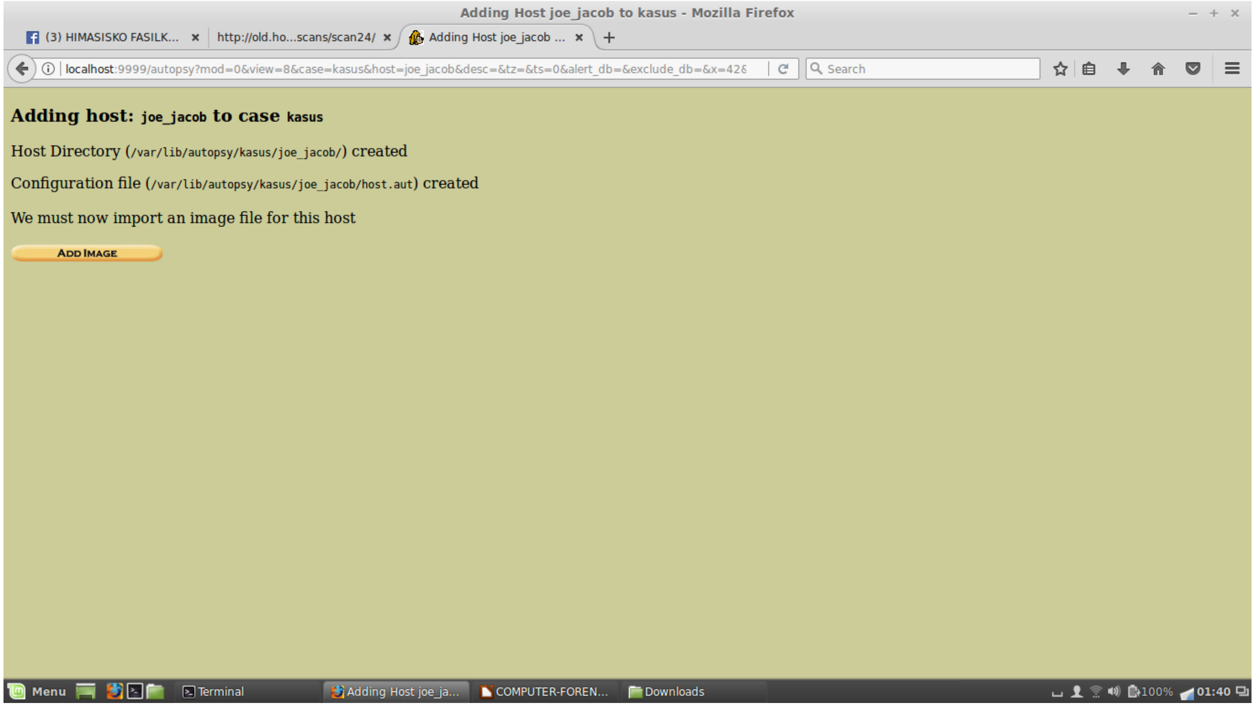
3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

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.
0

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.

Langkah selanjutnya yaitu membuat host baru, mengisi host name dengan nama joe_jacob dan untuk nomor 2-6 adalah optional, bisa tidak diisi. Setelah itu adding host.

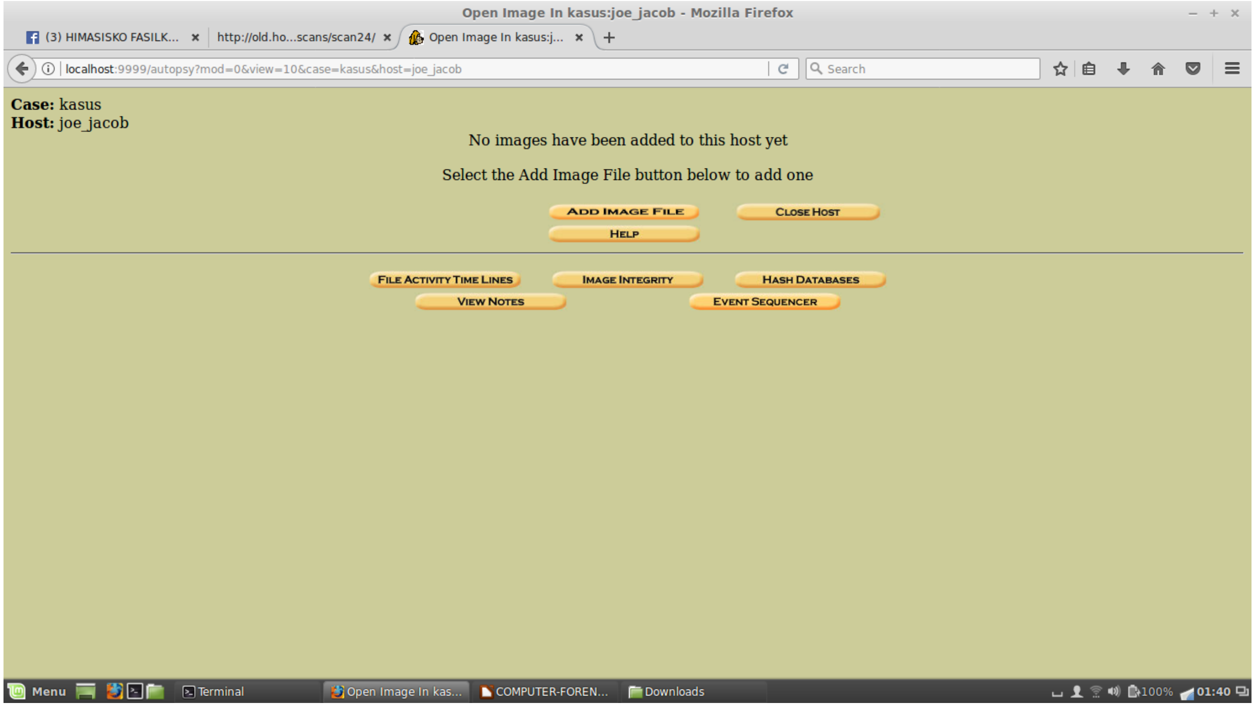

Adding Host joe_jacob to kasus - Mozilla Firefox
(3) HIMASISKO FASILK...
http://old.ho...scans/scan24/
Adding Host joe_jacob ...
localhost:9999/autopsy?mod=0&view=8&case=kasus&host=joe_jacob&desc=&tz=&ts=0&alert_db=&exclude_db=&x=42&
Search
Menu
Terminal
Adding Host joe_ja...
COMPUTER-FOREN...
Downloads
100%
01:40

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

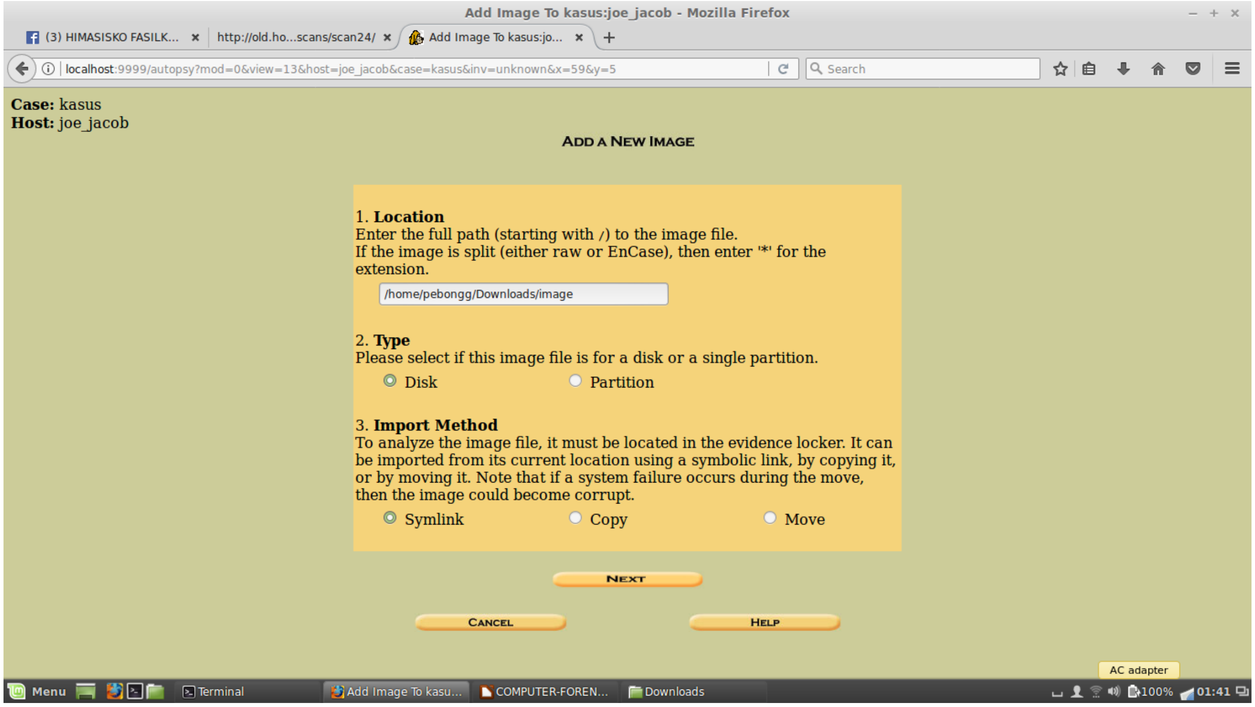
We must now import an image file for this host


Open Image In kasus:joe_jacob - Mozilla Firefox
(3) HIMASISKO FASILK...
http://old.ho...scans/scan24/
Open Image In kasus:j...
localhost:9999/autopsy?mod=0&view=10&case=kasus&host=joe_jacob
Search
Menu
Terminal
Open Image In kas...
COMPUTER-FOREN...
Downloads
100%
01:40

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 To kasus:joe_jacob - Mozilla Firefox
(3) HIMASISKO FASILK...
http://old.ho...scans/scan24/
Add Image To kasus:jo...
localhost:9999/autopsy?mod=0&view=13&host=joe_jacob&case=kasus&inv=unknown&x=59&y=5
Search
AC adapter
Menu
Terminal
Add Image To kasu...
COMPUTER-FOREN...
Downloads
100%
01:41

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.

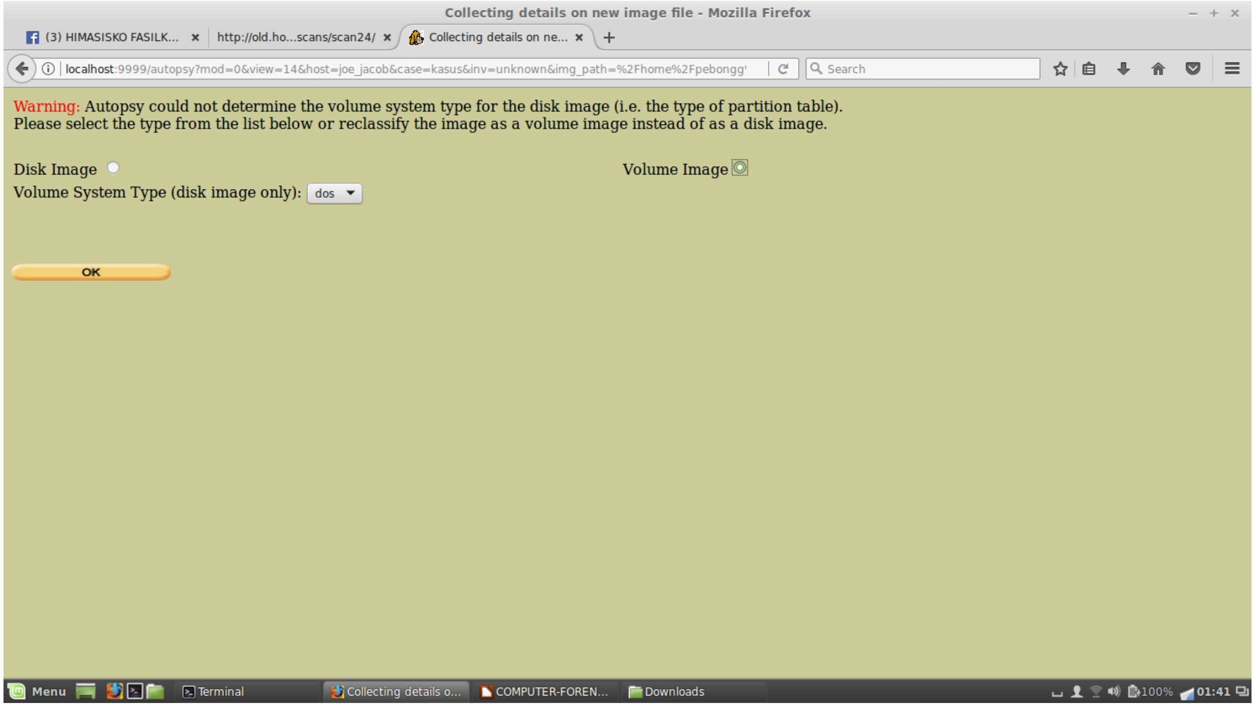
/home/pebongg/Downloads/image

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



Collecting details on new image file - Mozilla Firefox
(3) HIMASISKO FASILK...
http://old.ho...scans/scan24/
Collecting details on ne...
localhost:9999/autopsy?mod=0&view=14&host=joe_jacob&case=kasus&inv=unknown&img_path=%2Fhome%2Fpebongg'
Search
Menu
Terminal
Collecting details o...
COMPUTER-FOREN...
Downloads
100%
01:41

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

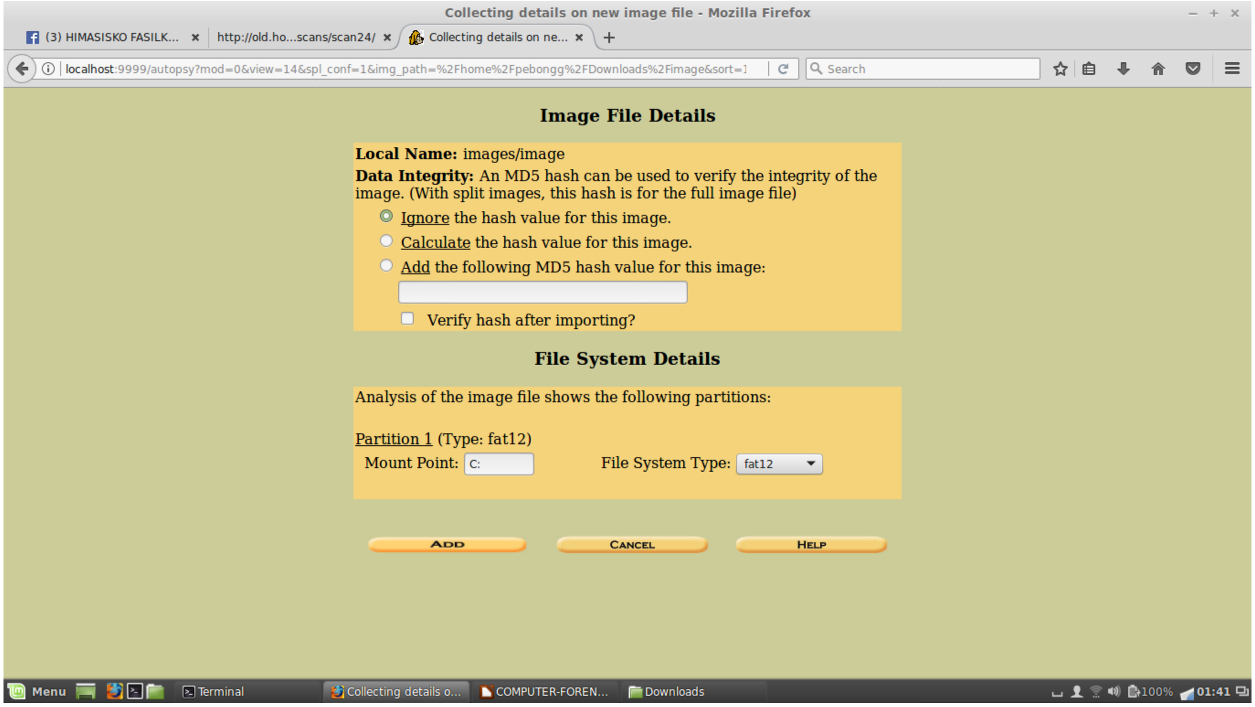

Collecting details on new image file - Mozilla Firefox
(3) HIMASISKO FASILK...
http://old.ho...scans/scan24/
Collecting details on ne...
localhost:9999/autopsy?mod=0&view=14&spl_conf=1&img_path=%2Fhome%2Fpebongg%2FDownloads%2Fimage&sort=1
Search
ADD
CANCEL
HELP
Menu
Terminal
Collecting details o...
COMPUTER-FOREN...
Downloads
100%
01:41

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:

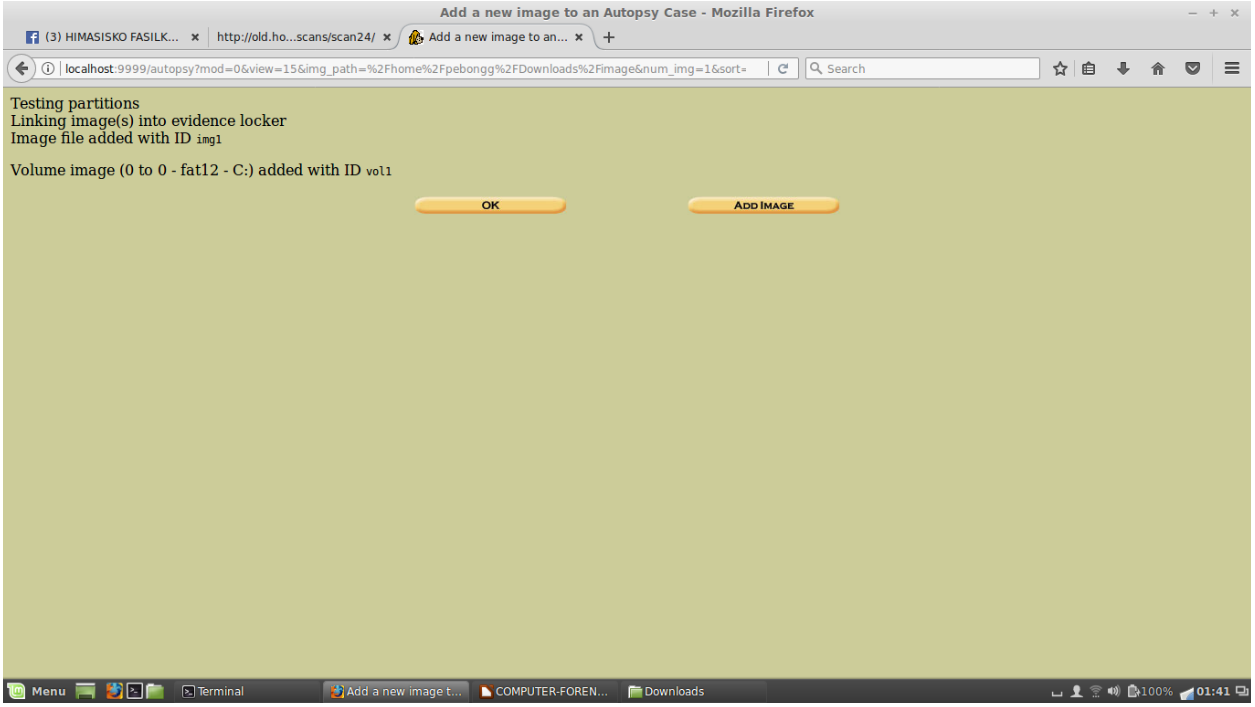
□ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

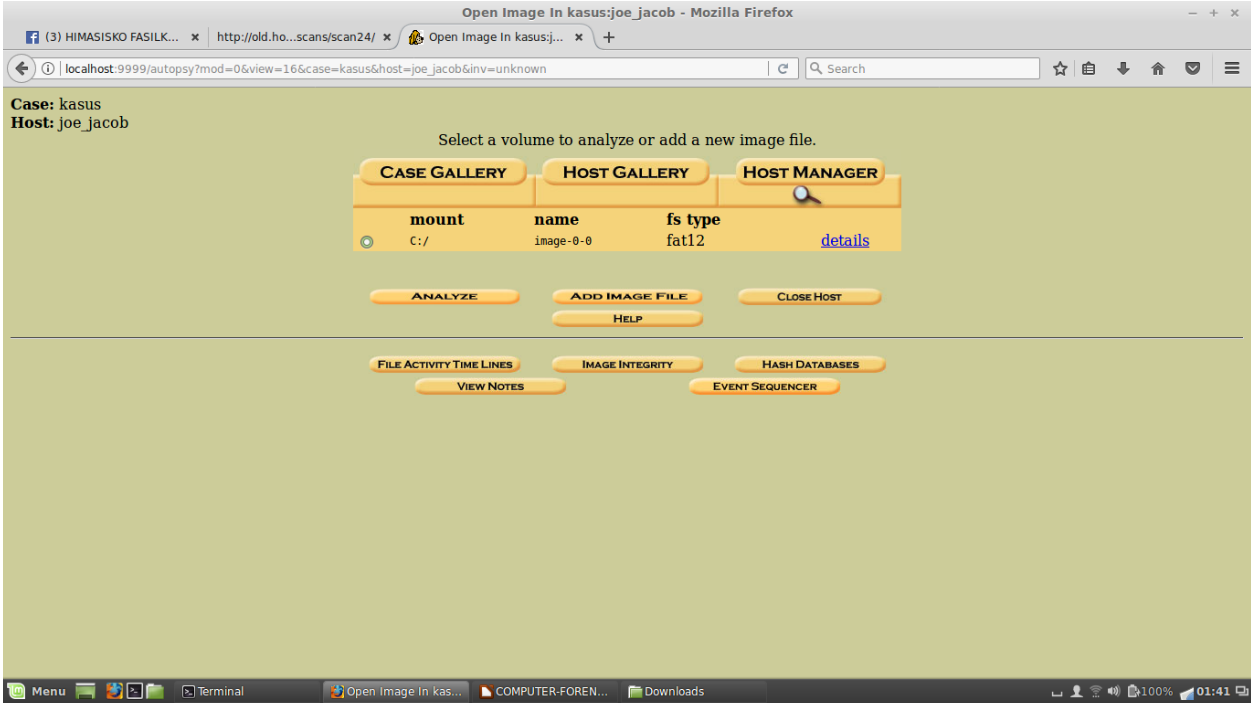
Partition 1 (Type: fat12)

Mount Point: C: File System Type: fat12


Add a new image to an Autopsy Case - Mozilla Firefox
(3) HIMASISKO FASILK...
http://old.ho...scans/scan24/
Add a new image to an...
localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fpebongg%2FDownloads%2Fimage&num_img=1&sort=
Search
OK
ADD IMAGE
Menu
Terminal
Add a new image t...
COMPUTER-FOREN...
Downloads
100%
01:41

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`

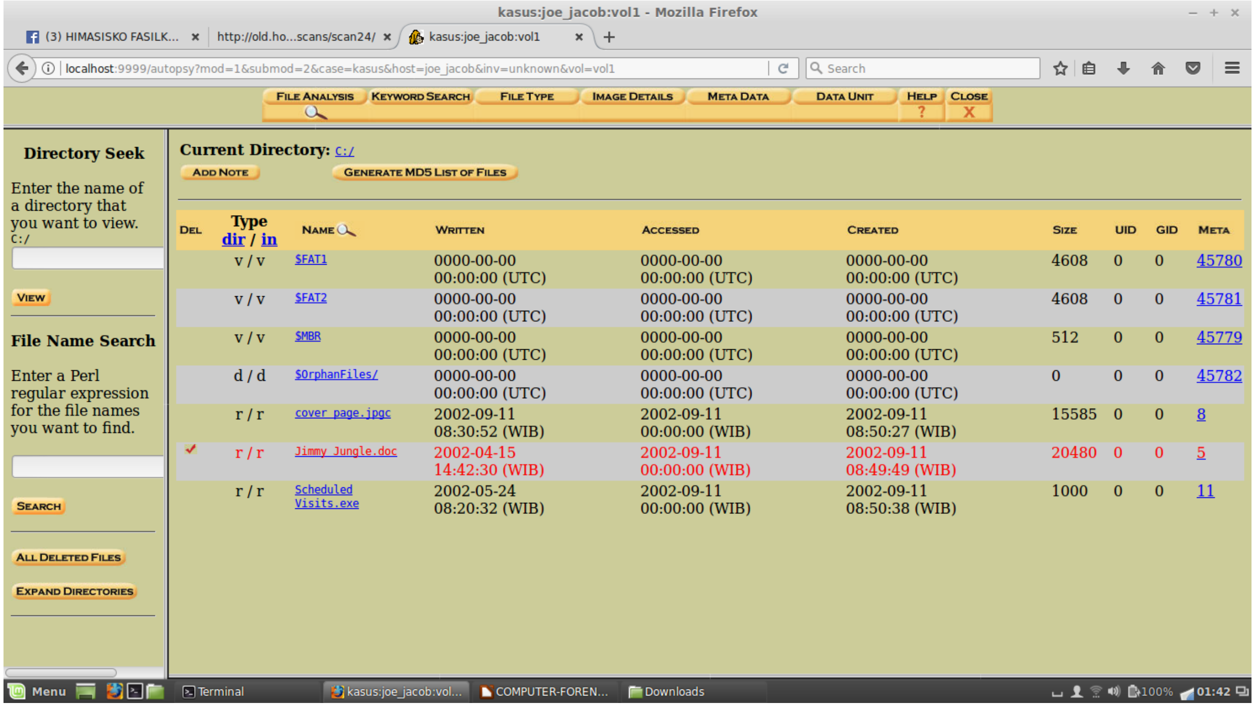


Case: kasus
Host: joe_jacob

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

	mount	name	fs type	
○	C:/	image-0-0	fat12	details

Dari 7 gambar di atas merupakan proses adding image, yaitu berupa location image file, type file yaitu disk, dan import method memilih symlink.



Directory Seek

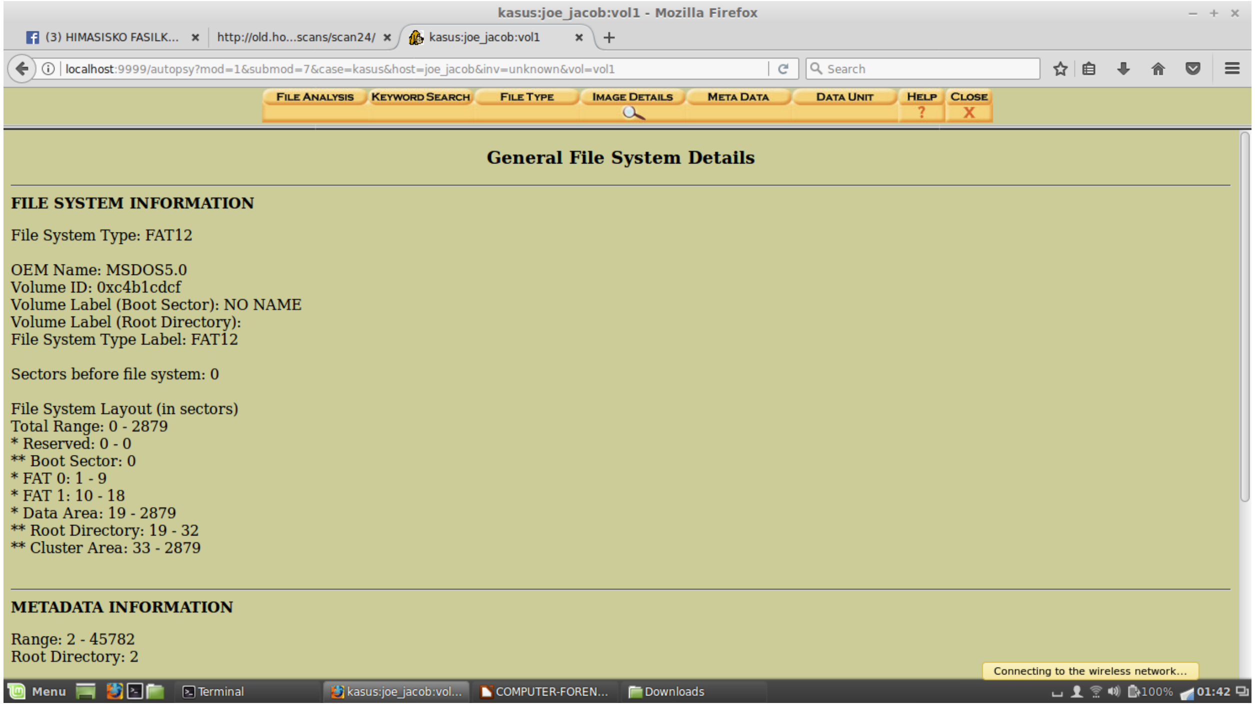
Enter the name of a directory that you want to view.
C:/

File Name Search

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

Current Directory: C:/

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	$FAT1	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	$FAT2	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.jpgc	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



General File System Details

FILE SYSTEM INFORMATION

File System Type: FAT12

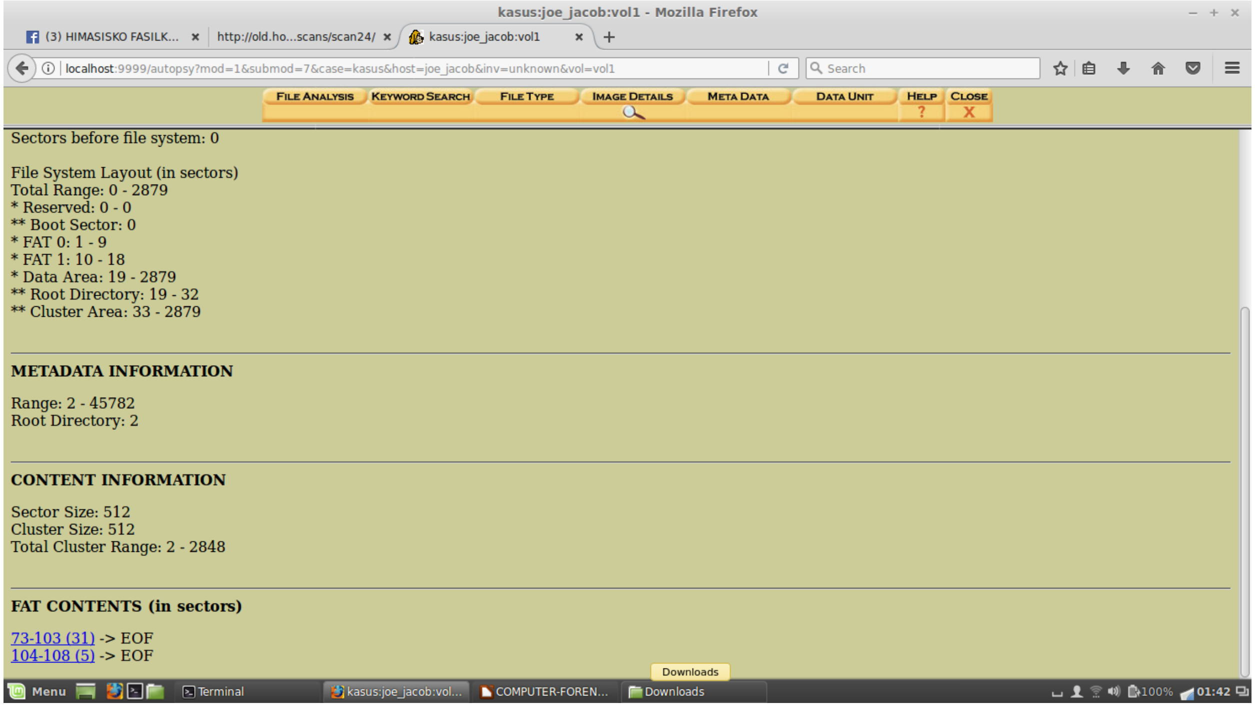
OEM Name: MSDOS5.0
Volume ID: 0xc4b1cdcf
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT12

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

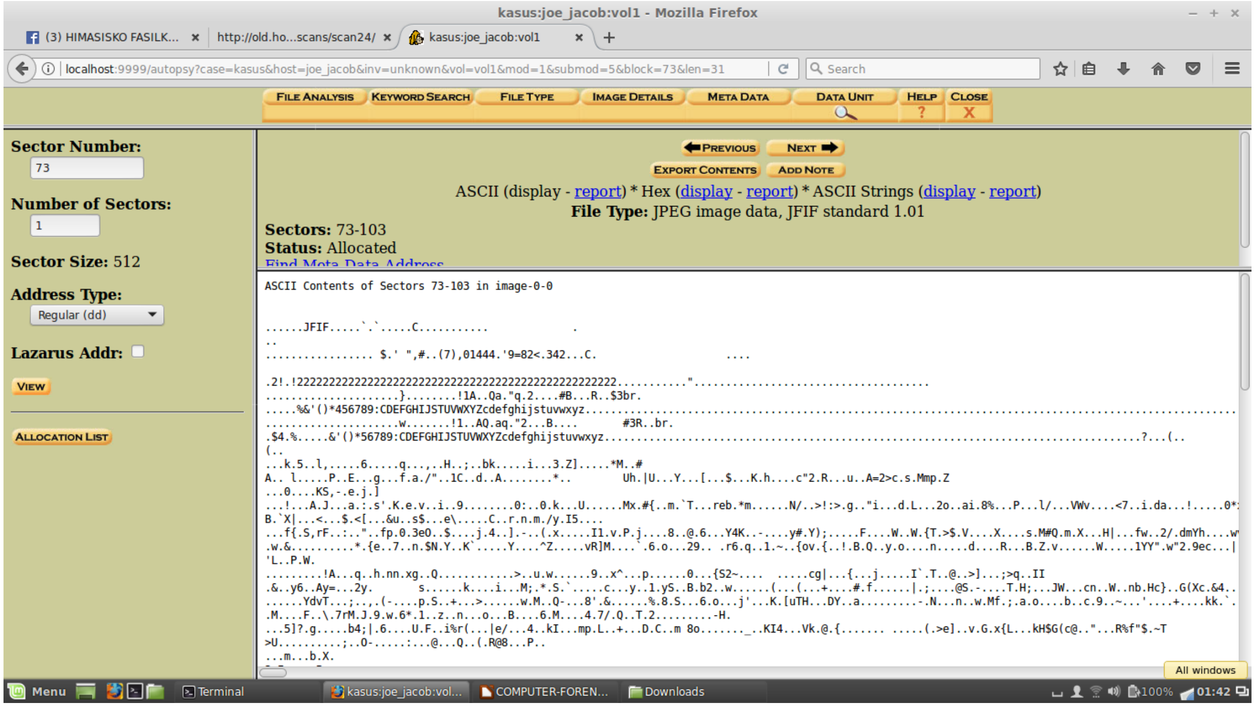
CONTENT INFORMATION

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

FAT CONTENTS (in sectors)

73-103 (31) -> EOF
104-108 (5) -> EOF

Selanjutnya melakukan analyze file system. Yang pertama melakukan analyze pada fat contents 73-103(31).



Sector Number: 73

Number of Sectors: 1

Sector Size: 512

Address Type: Regular (dd)

Lazarus Addr: □

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)

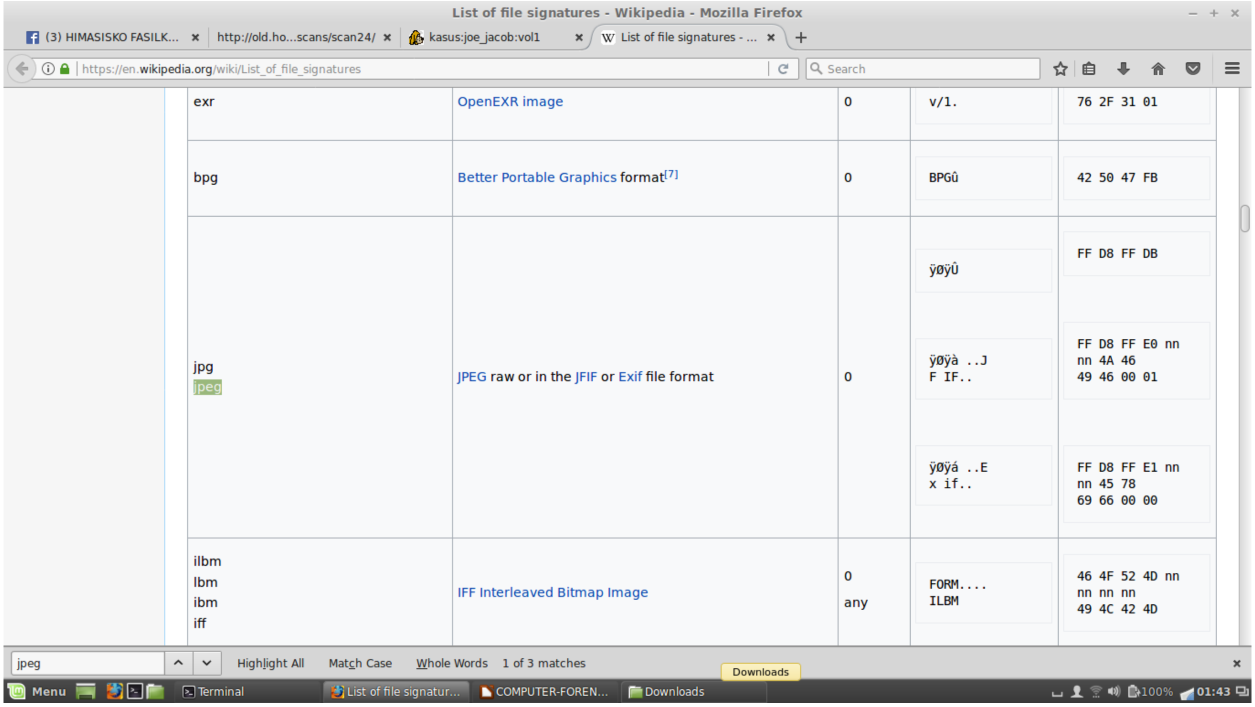
File Type: JPEG image data, JFIF standard 1.01

Sectors: 73-103

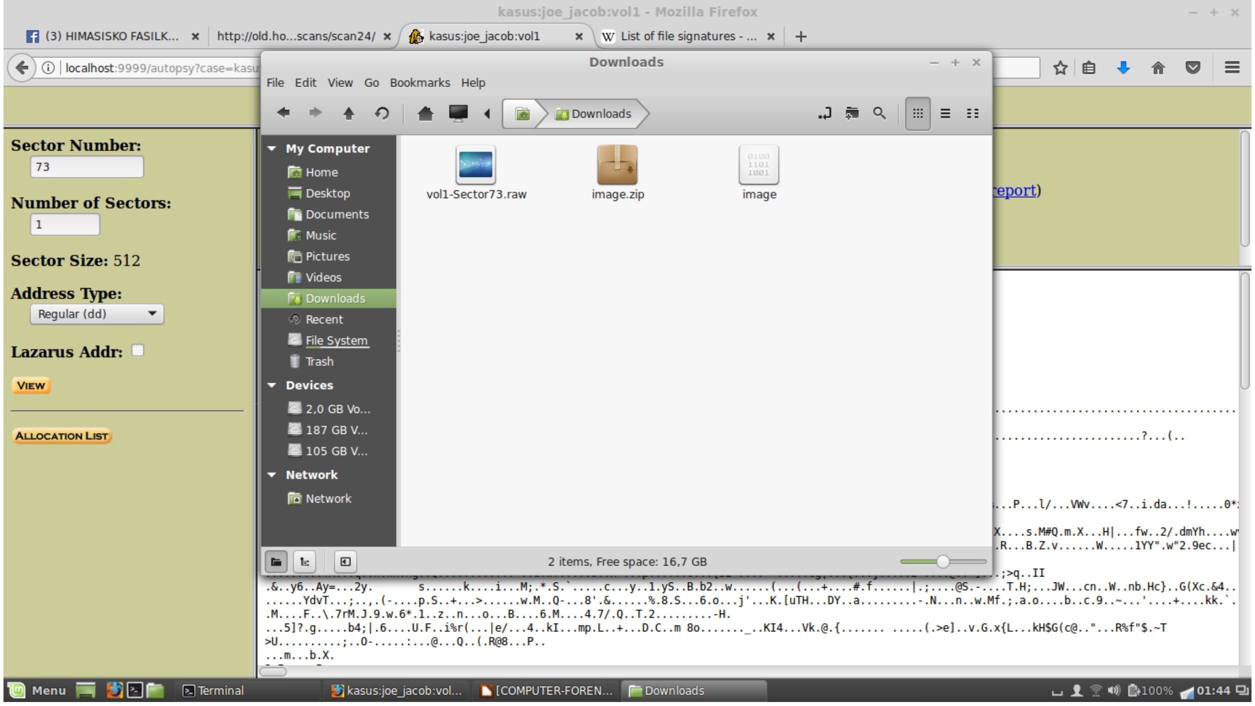
Status: Allocated

Find Meta Data Address

```
ASCII Contents of Sectors 73-103 in image-0-0


......JFIF.....`.`.....C...........                    .
..
................. $.' ",#..(7),01444.'9=82<.342...C.                    ....

.2!.!22222222222222222222222222222222222222222222222222...........".....................................
....................}........!1A..Qa."q.2....#B...R..$3br.
.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...................................................................................................
....................w.......!1..AQ.aq."2...B....       #3R..br.
.$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...........................................................................?...(..
(..
...k.5..l,.....6.....q...,..H..;..bk.....i...3.Z].....*M..#
A.. l.....P..E...g...f.a./"..1C..d..A........*..        Uh.|U...Y...[...$...K.h....c"2.R...u..A=2>c.s.Mmp.Z
...0....KS,-.e.j.]
...!...A.J...a.:.s'.K.e.v..i..9........0:..0.k...U......Mx.#{..m.`T...reb.*m......N/..>!:>.g.."i...d.L...2o..ai.8%...P...l/...VWv....<7..i.da...!.....0*
B.`X|...<...$.<[...&u..s$...e\.....C..r.n.m./y.I5....
...f{.S,rF..:..."..fp.0.3eO..$....j.4..].-..(.x.....I1.v.P.j....8..@.6...Y4K..-....y#.Y);.....F....W..W.{T.>$.V....X....s.M#Q.m.X...H|...fw..2/.dmYh....w
.w.&..........*.{e..7..n.$N.Y..K`.....Y....^Z.....vR]M....`.6.o...29.. .r6.q..1.~..{ov.{..!.B.Q..y.o....n.....d....R...B.Z.v......W.....1YY".w"2.9ec...|
'L..P.W.
.........!A...q..h.nn.xg..Q............>..u.w......9..x^...p......0...{S2~....  .....cg|...{...j.....I`.T..@..>]...;>q..II
.&..y6..Ay=...2y.       s......k....i...M;.*.S.`.....c...y..1.yS..B.b2..w......(...(...+....#.f......|.;....@S.-....T.H;...JW...cn..W..nb.Hc}..G(Xc.&4..
......YdvT...;..,.(-....p.S..+...>......w.M..Q-...8'.&......%.8.S...6.o...j'...K.[uTH...DY..a.........-.N...n..w.Mf.;.a.o....b..c.9..~...'....+....kk.`.
.M....F..\.7rM.J.9.w.6*.1..z..n...o...B....6.M....4.7/.Q..T.2.........-H.
...5]?.g.....b4;|.6....U.F..i%r(...|e/...4..kI...mp.L..+...D.C..m 8o......._..KI4...Vk.@.{....... .....(.>e]..v.G.x{L...kH$G(c@.."...R%f"$.~T
>U..........;..O-.....:...@...Q..(.R@8...P..
...m...b.X.
```



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



Sector Number: 73

Number of Sectors: 1

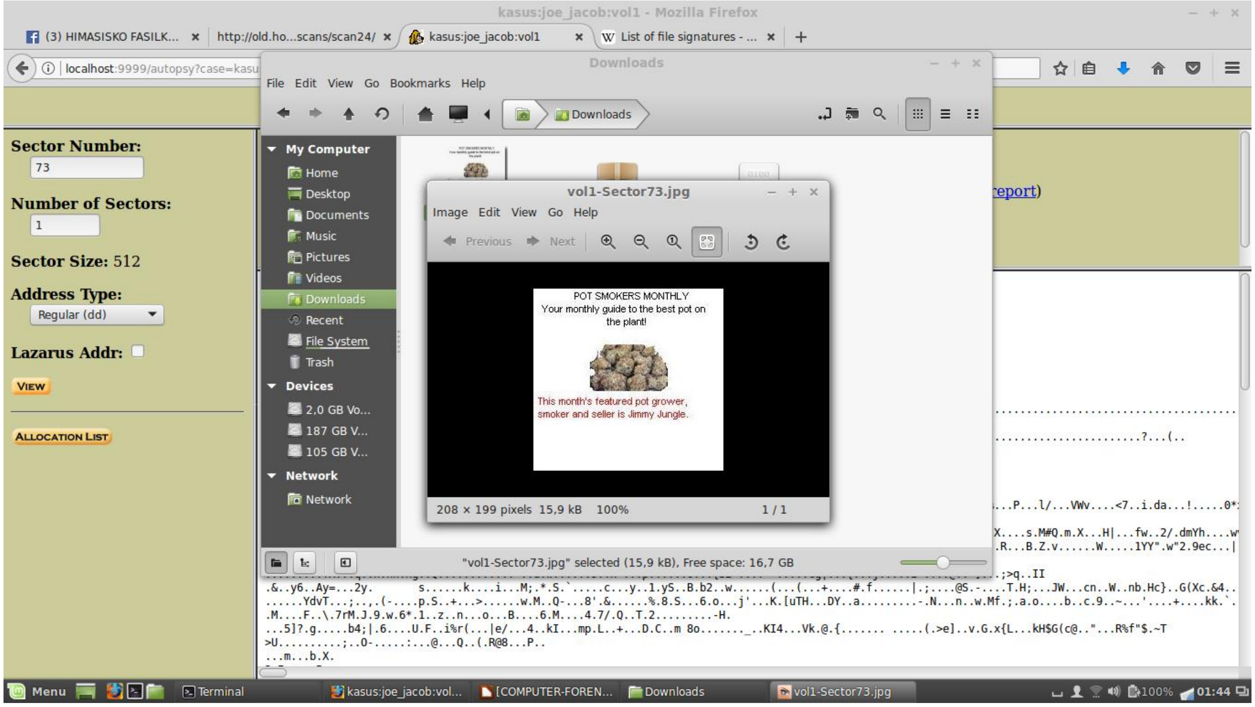
Sector Size: 512

Address Type: Regular (dd)

Lazarus Addr: □

```
..........................................
........................?...(..
...P...l/...VWv....<7..i.da...!.....0*
X....s.M#Q.m.X...H|...fw..2/.dmYh....w
.R...B.Z.v......W.....1YY".w"2.9ec...|
.;>q..II
.&..y6..Ay=...2y.        s......k....i...M;.*.S.`.....c...y..1.yS..B.b2..w......(...(...+....#.f......|.;....@S.-....T.H;...JW...cn..W..nb.Hc}..G(Xc.&4..
......YdvT...;..,.(-....p.S..+...>......w.M..Q-...8'.&......%.8.S...6.o...j'...K.[uTH...DY..a.........-.N...n..w.Mf.;.a.o....b..c.9..~...'....+....kk.`.
.M....F..\.7rM.J.9.w.6*.1..z..n...o...B....6.M....4.7/.Q..T.2.........-H.
...5]?.g.....b4;|.6....U.F..i%r(...|e/...4..kI...mp.L..+...D.C..m 8o......._..KI4...Vk.@.{....... .....(.>e]..v.G.x{L...kH$G(c@.."...R%f"$.~T
>U.........;..O-.....:...@...Q..(.R@8...P..
...m...b.X.
```

2 items, Free space: 16,7 GB



Sector Number: 73

Number of Sectors: 1

Sector Size: 512

Address Type: Regular (dd)

Lazarus Addr: □

vol1-Sector73.jpg

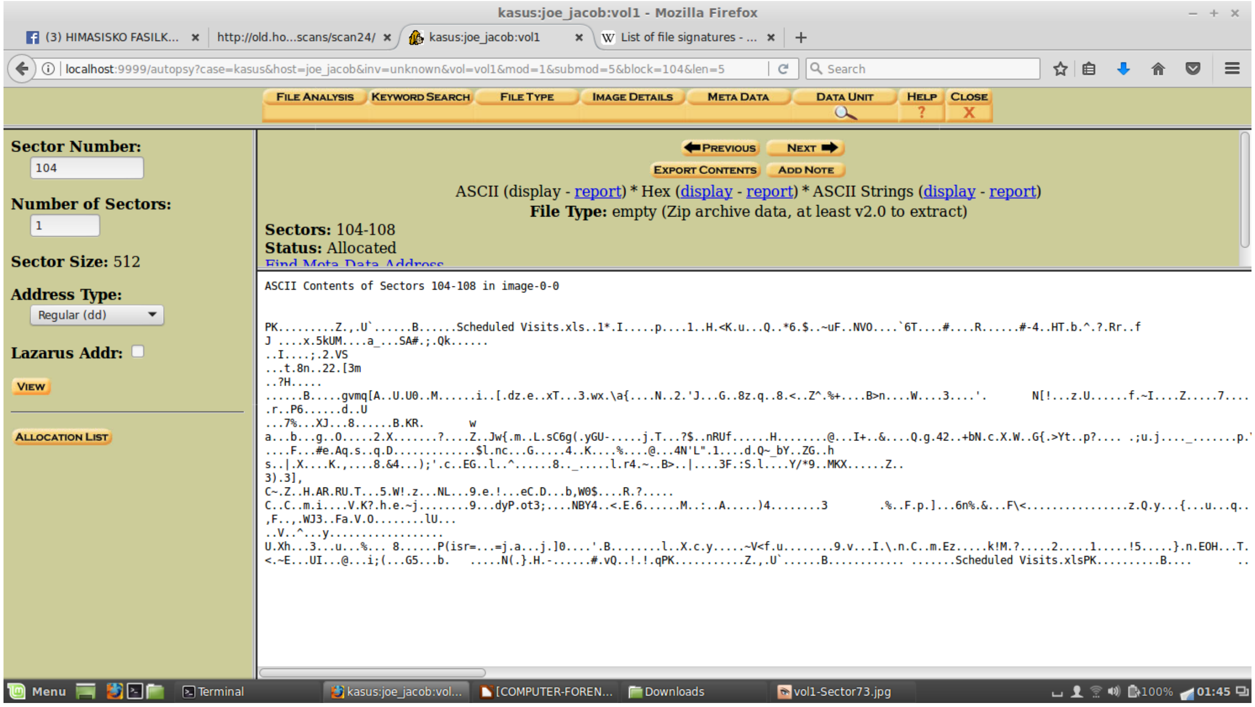
POT SMOKERS MONTHLY
Your monthly guide to the best pot on the plant!

This month's featured pot grower, smoker and seller is Jimmy Jungle.

208 × 199 pixels 15,9 kB 100% 1 / 1

"vol1-Sector73.jpg" selected (15,9 kB), Free space: 16,7 GB

Dari 4 gambar di atas, didapatkan analyze berupa code JFIF. Sesuai dengan list of signatures file .jpg, JFIF merupakan format dari file .jpg. Dan juga, dilihat dari gambar di atas, terdapat file volt-sector73.raw diubah ekstensi filenya menjadi volt-sector73.jpg, maka file tersebut dapat dilihat sesuai dengan ekstensi file .jpg yaitu berupa gambar.



Sector Number: 104

Number of Sectors: 1

Sector Size: 512

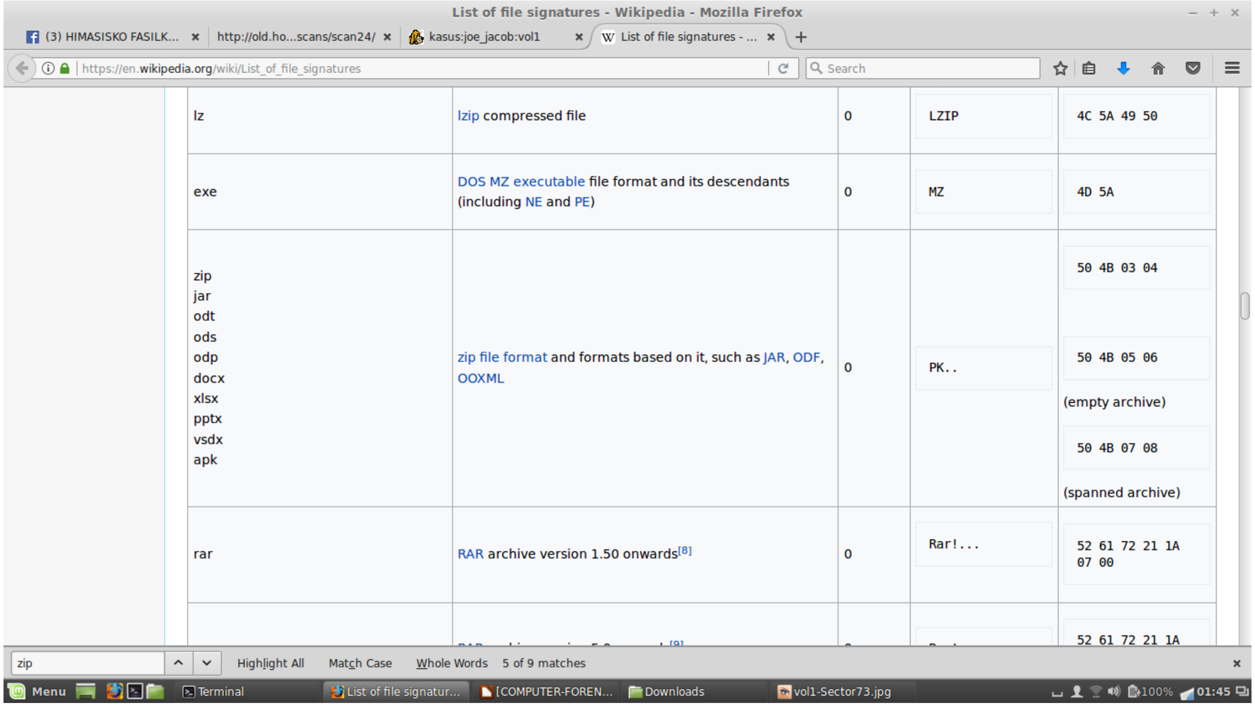
Address Type: Regular (dd)

Lazarus Addr: □

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: empty (Zip archive data, at least v2.0 to extract)

Sectors: 104-108
Status: Allocated
Find Meta Data Address

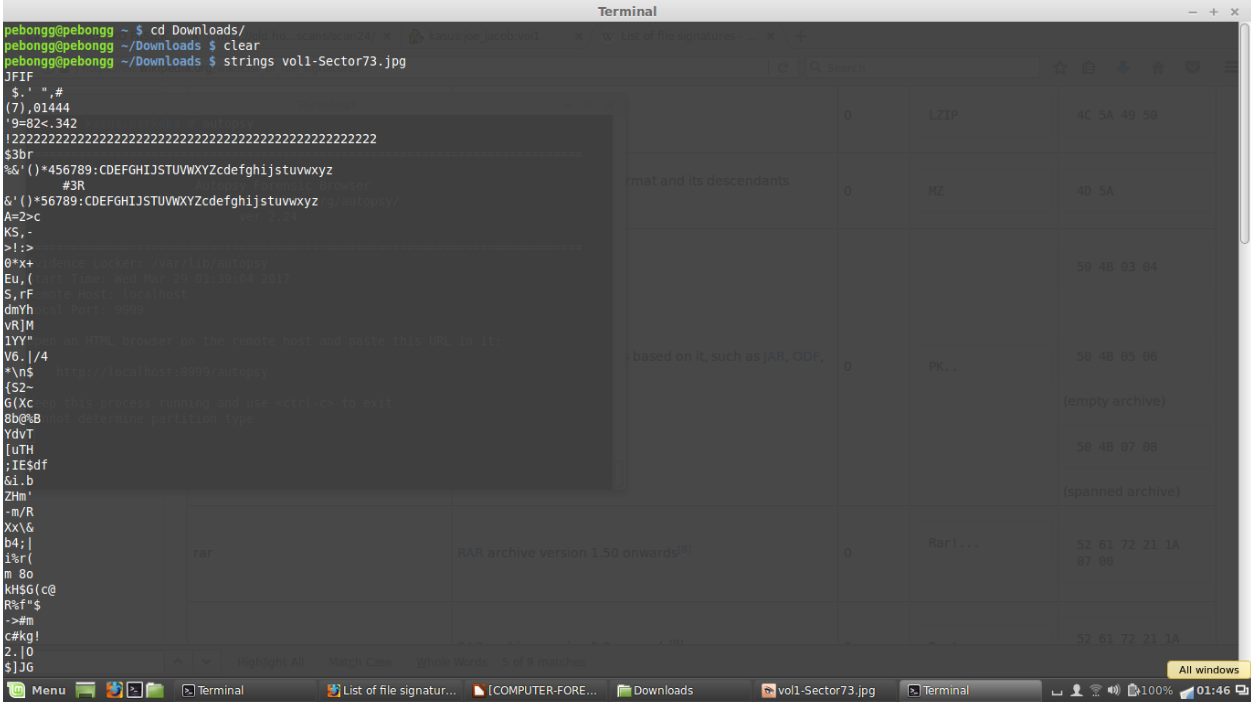
```
ASCII Contents of Sectors 104-108 in image-0-0


PK.........Z.,.U`......B......Scheduled Visits.xls..1*.I.....p....1..H.<K.u...Q..*6.$..~uF..NVO....`6T....#....R......#-4..HT.b.^.?.Rr..f
J ....x.5kUM....a_...SA#.;.Qk......
..I....;.2.VS
...t.8n..22.[3m
..?H.....
......B.....gvmq[A..U.U0..M......i..[.dz.e..xT...3.wx.\a{....N..2.'J...G..8z.q..8.<..Z^.%+....B>n....W....3....'.       N[!...z.U......f.~I....Z.....7....
.r..P6......d..U
...7%...XJ...8......B.KR.       w
a...b...g..O.....2.X.......?....Z..Jw{.m..L.sC6g(.yGU-.....j.T...?$..nRUf......H........@...I+..&....Q.g.42..+bN.c.X.W..G{.>Yt..p?.... .;u.j...._.......p.'
....F...#e.Aq.s..q.D.............$l.nc...G.....4..K....%....@...4N'L".1....d.Q~_bY..ZG..h
s..|.X....K.,....8.&4...);'.c..EG..l..^......8.._.....l.r4.~..B>..|....3F.:S.l....Y/*9..MKX......Z..
3).3],
C~.Z..H.AR.RU.T...5.W!.z...NL...9.e.!...eC.D...b,W0$....R.?.....
C..C..m.i....V.K?.h.e.~j........9...dyP.ot3;....NBY4..<.E.6......M..:..A.....)4........3       .%..F.p.]...6n%.&...F\<................z.Q.y...{...u...q..
,F..,.WJ3..Fa.V.O........lU...
..V..^...y..................
U.Xh...3...u...%... 8......P(isr=...=j.a...j.]0....'.B........l..X.c.y.....~V<f.u........9.v...I.\.n.C..m.Ez.....k!M.?.....2.....1.....!5.....}.n.EOH...T.
<.~E...UI...@...i;(...G5...b.   .....N(.}.H.-......#.vQ..!.!.qPK...........Z.,.U`......B............ .......Scheduled Visits.xlsPK..........B....      ..
```



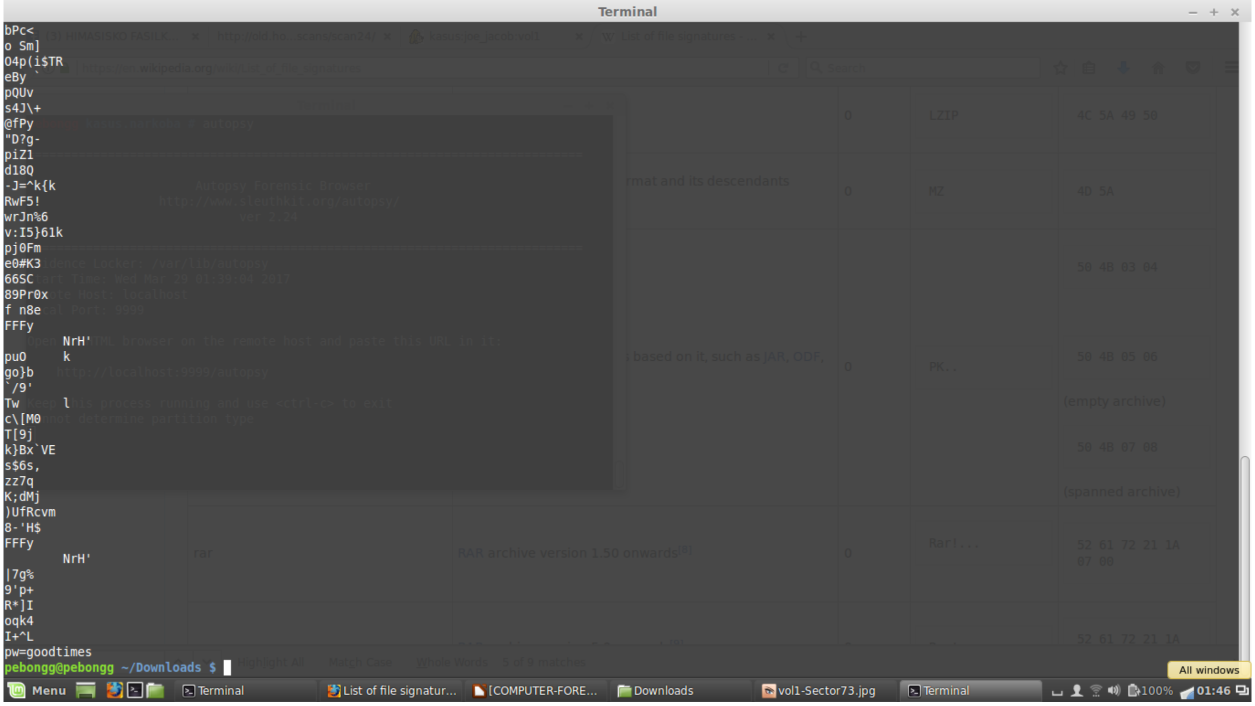
lz	lzip compressed file	0	LZIP	4C 5A 49 50
exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A
zip jar odt ods odp docx xlsx pptx vsdx apk	zip file format and formats based on it, such as JAR, ODF, OOXML	0	PK..	50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive)
rar	RAR archive version 1.50 onwards[8]	0	Rar!...	52 61 72 21 1A 07 00
	[9]			52 61 72 21 1A

zip

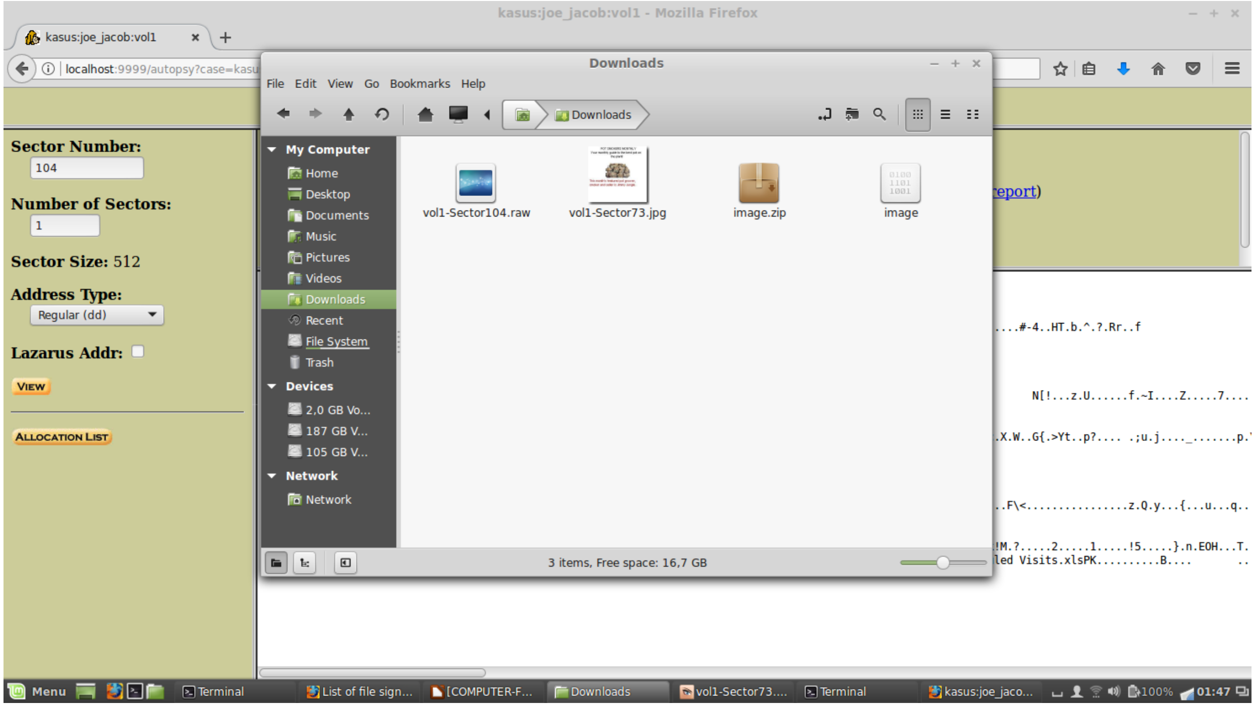
5 of 9 matches



```
pebongg@pebongg ~ $ cd Downloads/
pebongg@pebongg ~/Downloads $ clear
pebongg@pebongg ~/Downloads $ strings vol1-Sector73.jpg
JFIF
 $.' ",#
(7),01444
'9=82<.342
!22222222222222222222222222222222222222222222222222
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
        #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
A=2>c
KS,-
>!:>
0*x+
Eu,(
S,rF
dmYh
vR]M
1YY"
V6.|/4
*\n$
{S2~
G(Xc
8b@%B
YdvT
[uTH
;IE$df
&i.b
ZHm'
-m/R
Xx\&
b4;|
i%r(
m 8o
kH$G(c@
R%f"$
->#m
c#kg!
2.|O
$]JG
```



```
bPc<
o Sm]
O4p(i$TR
eBy `
pQUv
s4J\+
@fPy
"D?g-
piZ1
d18Q
-J=^k{k
RwF5!
wrJn%6
v:I5}61k
pj0Fm
e0#K3
66SC
89Pr0x
f n8e
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
pebongg@pebongg ~/Downloads $ 
```



Sector Number: 104

Number of Sectors: 1

Sector Size: 512

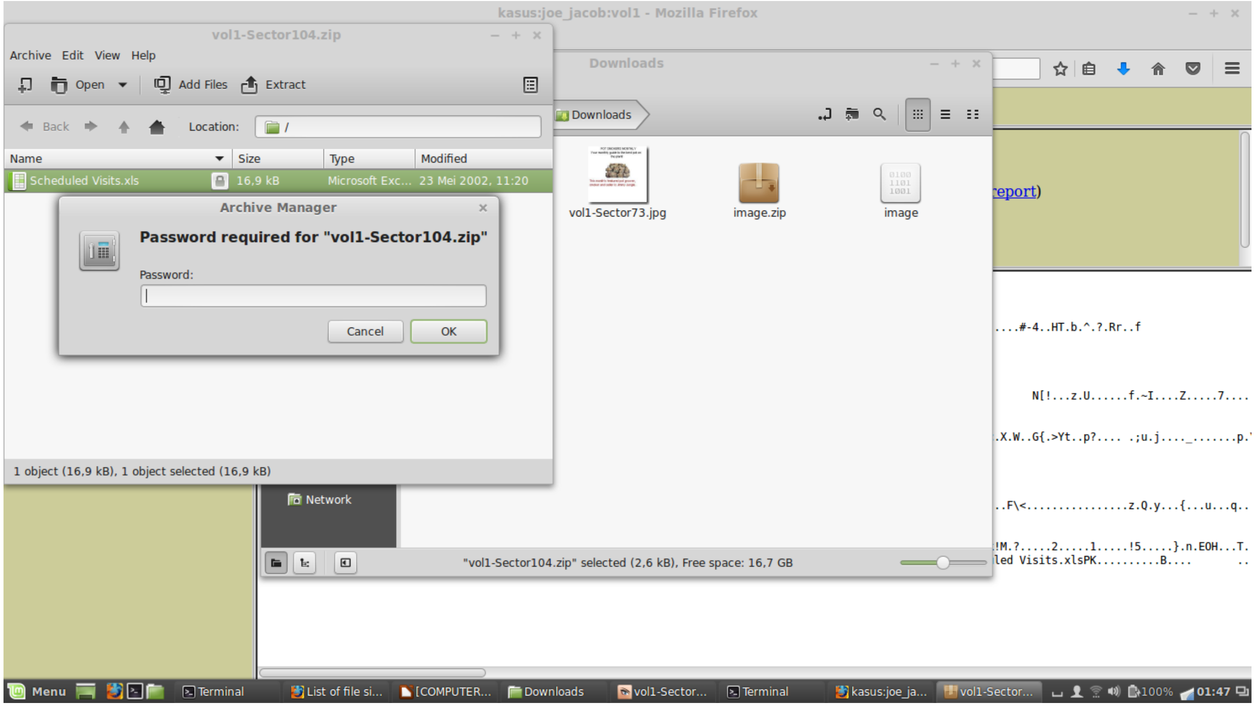
Address Type: Regular (dd)

Lazarus Addr: □

vol1-Sector104.raw vol1-Sector73.jpg image.zip image

3 items, Free space: 16,7 GB

```
....#-4..HT.b.^.?.Rr..f

      N[!...z.U......f.~I....Z.....7....

.X.W..G{.>Yt..p?.... .;u.j...._.......p.'

..F\<...............z.Q.y...{...u...q..

!M.?.....2.....1.....!5.....}.n.EOH...T.
led Visits.xlsPK..........B....      ..
```



Location: /

Name	Size	Type	Modified
Scheduled Visits.xls	16,9 kB	Microsoft Exc...	23 Mei 2002, 11:20

Password required for "vol1-Sector104.zip"

Password:

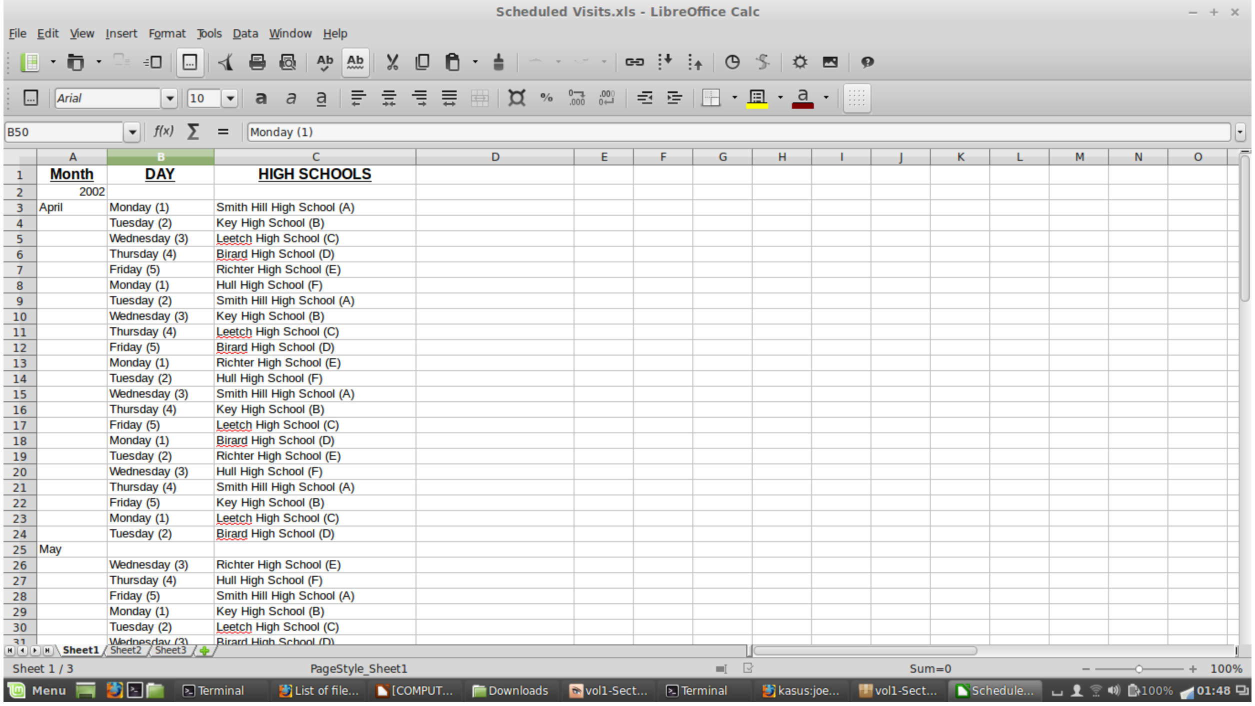
Cancel OK

1 object (16,9 kB), 1 object selected (16,9 kB)

vol1-Sector73.jpg image.zip image

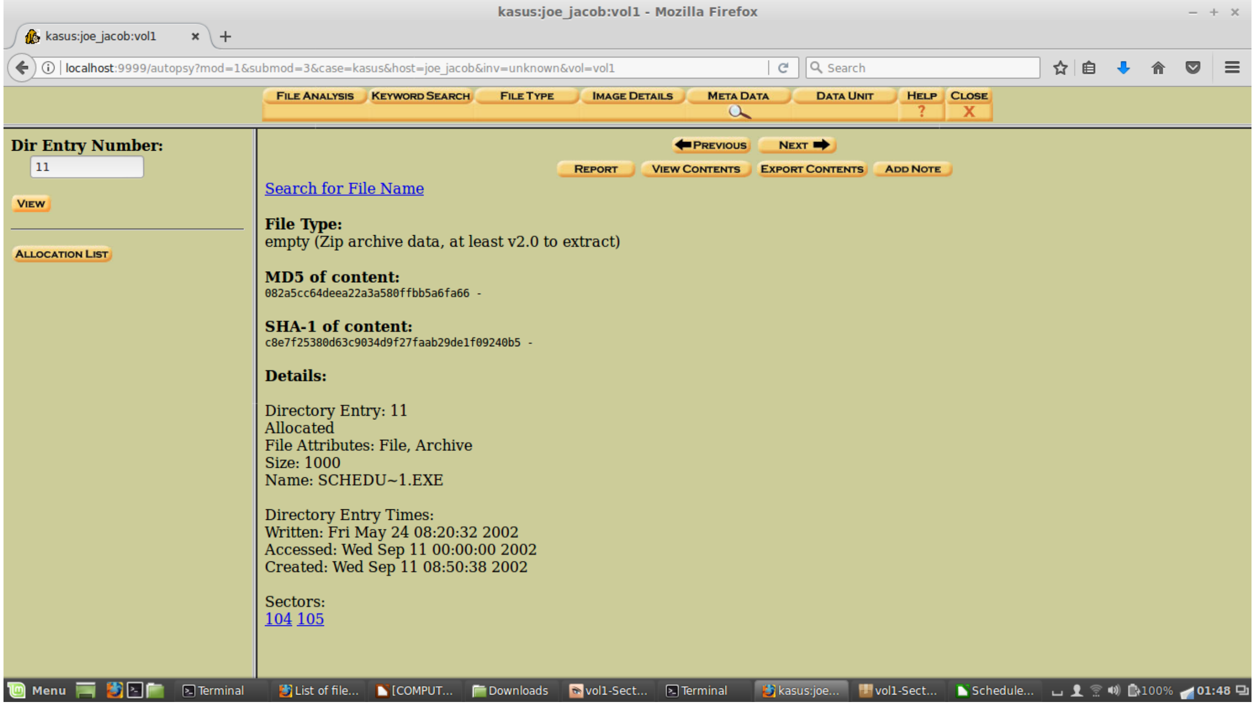
"vol1-Sector104.zip" selected (2,6 kB), Free space: 16,7 GB

```
....#-4..HT.b.^.?.Rr..f

      N[!...z.U......f.~I....Z.....7....

.X.W..G{.>Yt..p?.... .;u.j...._.......p.'

..F\<...............z.Q.y...{...u...q..

!M.?.....2.....1.....!5.....}.n.EOH...T.
led Visits.xlsPK..........B....      ..
```



	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)

Dari 7 gambar di atas, didapatkan analyze berupa code PK. Sesuai dengan list of signatures file .zip, PK merupakan format dari file .zip. Dan juga, dilihat dari gambar di atas, terdapat file volt-sector104.raw diubah 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.



Dir Entry Number:
11

Search for File Name

File Type:
empty (Zip archive data, at least v2.0 to extract)

MD5 of content:
082a5cc64deea22a3a580ffbb5a6fa66 -

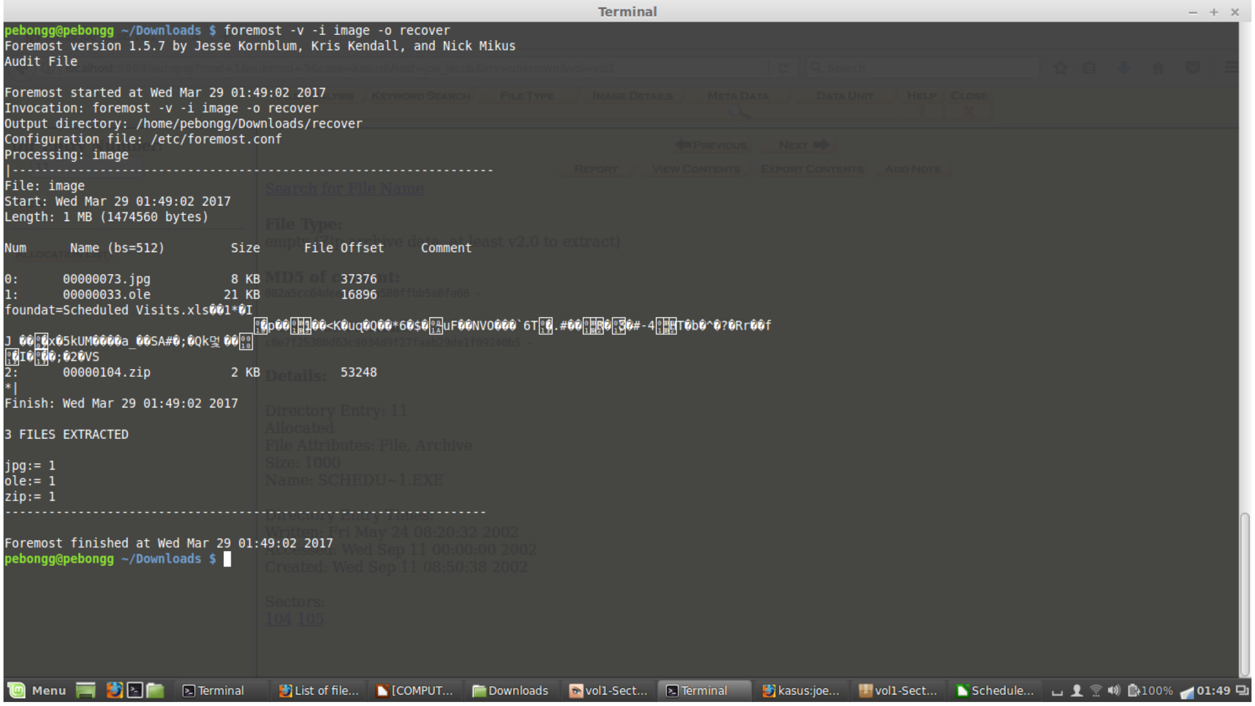
SHA-1 of content:
c8e7f25380d63c9034d9f27faab29de1f09240b5 -

Details:

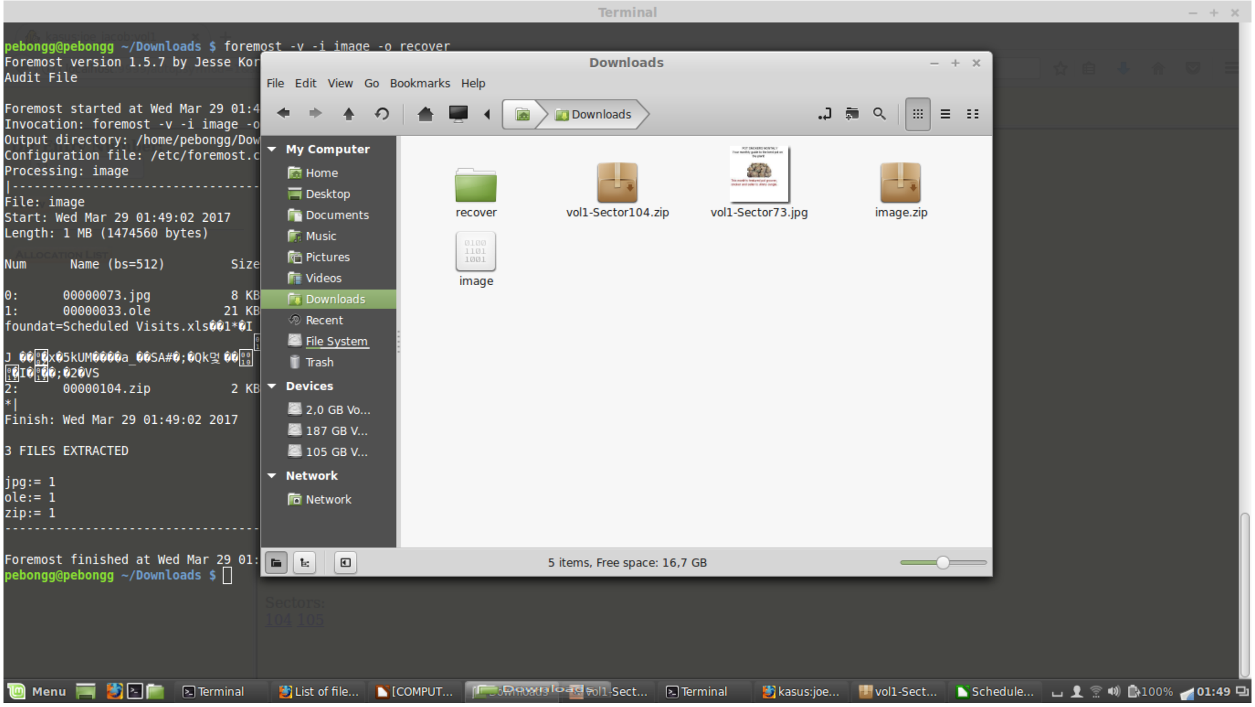
Directory Entry: 11
Allocated
File Attributes: File, Archive
Size: 1000
Name: SCHEDU~1.EXE

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



```
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)

Num      Name (bs=512)         Size      File Offset     Comment

0:       00000073.jpg           8 KB          37376
1:       00000033.ole          21 KB          16896
foundat=Scheduled Visits.xls��1*�I
                                                            ��p���1��<K�uq�Q��*6�$��uF��NVO���`6T��.#����R���3�#-4���T�b�^�?�Rr��f
J ����x�5kUM����a_��SA#�;�Qk멎 ���
��I���;�2�VS
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 $ 
```



recover

vol1-Sector104.zip

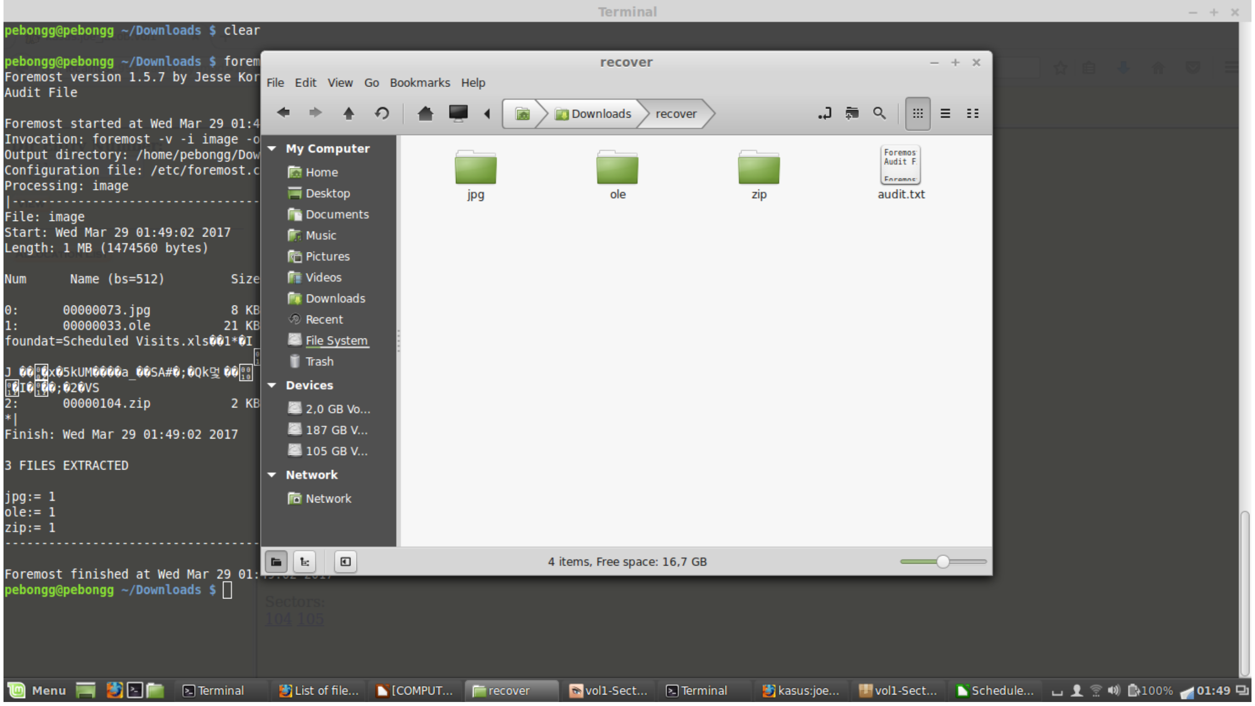
vol1-Sector73.jpg

image.zip

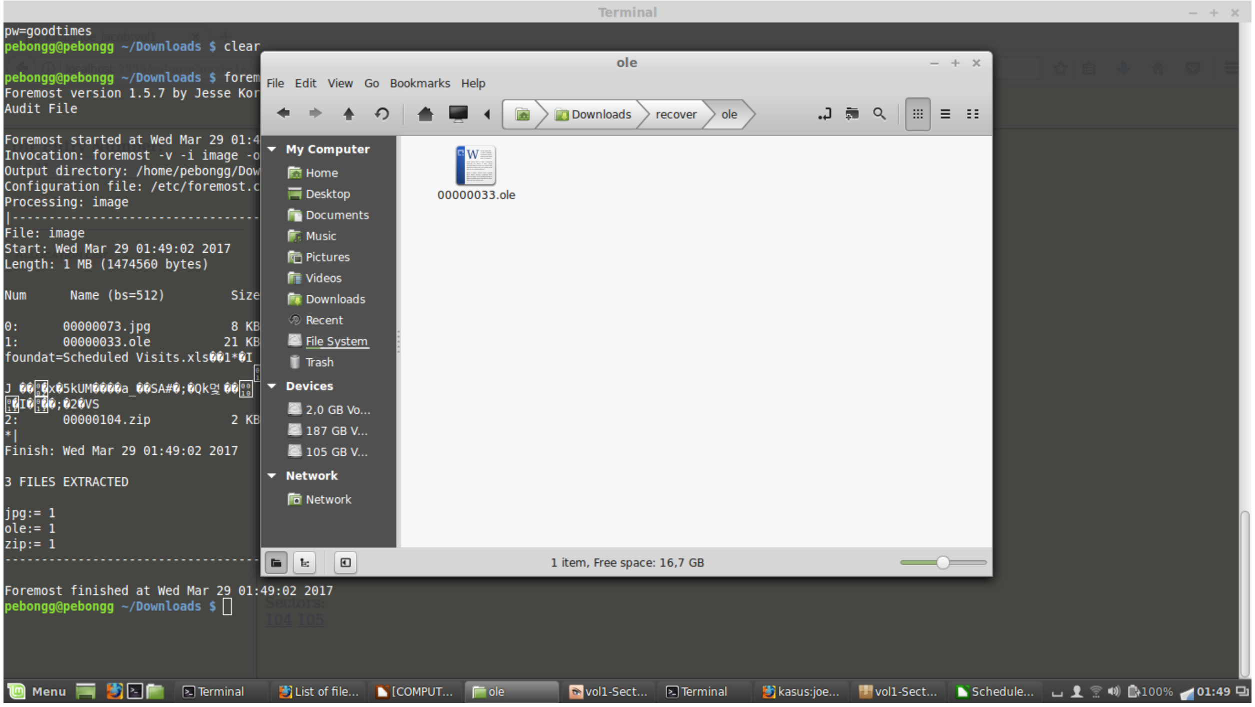
image

5 items, Free space: 16,7 GB

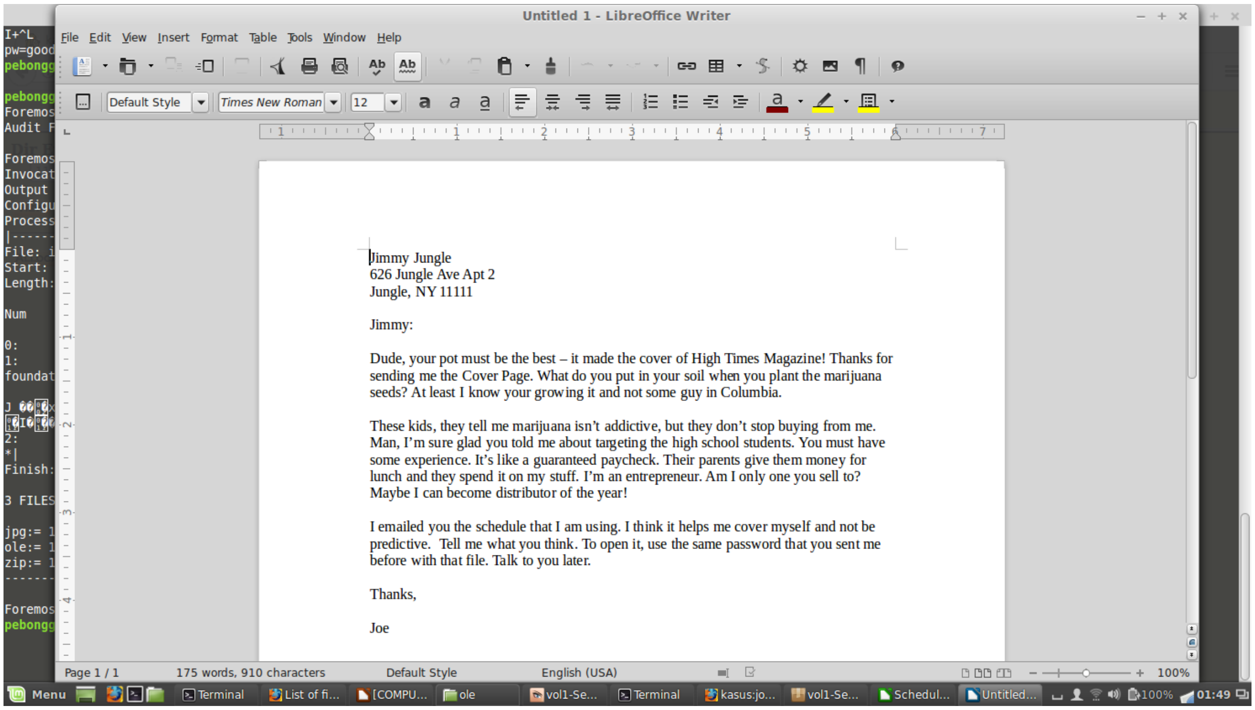
```
pebongg@pebongg ~/Downloads $ foremost -v -i image -o recover
Foremost version 1.5.7 by Jesse Kor
Audit File

Foremost started at Wed Mar 29 01:4
Invocation: foremost -v -i image -o
Output directory: /home/pebongg/Dow
Configuration file: /etc/foremost.c
Processing: image
|-----------------------------------
File: image
Start: Wed Mar 29 01:49:02 2017
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)         Size

0:       00000073.jpg           8 KB
1:       00000033.ole          21 KB
foundat=Scheduled Visits.xls��1*�I

J ����x�5kUM����a_��SA#�;�Qk멎 ���
��I���;�2�VS
2:       00000104.zip           2 KB
*|
Finish: Wed Mar 29 01:49:02 2017

3 FILES EXTRACTED

jpg:= 1
ole:= 1
zip:= 1
-----------------------------------

Foremost finished at Wed Mar 29 01:
pebongg@pebongg ~/Downloads $ 
```



```
pebongg@pebongg ~/Downloads $ clear

pebongg@pebongg ~/Downloads $ forem
Foremost version 1.5.7 by Jesse Kor
Audit File

Foremost started at Wed Mar 29 01:4
Invocation: foremost -v -i image -o
Output directory: /home/pebongg/Dow
Configuration file: /etc/foremost.c
Processing: image
|----------------------------------
File: image
Start: Wed Mar 29 01:49:02 2017
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)         Size

0:       00000073.jpg           8 KB
1:       00000033.ole          21 KB
foundat=Scheduled Visits.xls��1*�I

J ����x�5kUM����a_��SA#�;�Qk멎 ��
��I���;�2�VS
2:       00000104.zip           2 KB
*|
Finish: Wed Mar 29 01:49:02 2017

3 FILES EXTRACTED

jpg:= 1
ole:= 1
zip:= 1
-----------------------------------

Foremost finished at Wed Mar 29 01:
pebongg@pebongg ~/Downloads $ 
```



```
pw=goodtimes
pebongg@pebongg ~/Downloads $ clear

pebongg@pebongg ~/Downloads $ forem
Foremost version 1.5.7 by Jesse Kor
Audit File

Foremost started at Wed Mar 29 01:4
Invocation: foremost -v -i image -o
Output directory: /home/pebongg/Dow
Configuration file: /etc/foremost.c
Processing: image
|----------------------------------
File: image
Start: Wed Mar 29 01:49:02 2017
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)         Size

0:       00000073.jpg           8 KB
1:       00000033.ole          21 KB
foundat=Scheduled Visits.xls��1*�I

J ����x�5kUM����a_��SA#�;�Qk멎 ��
��I���;�2�VS
2:       00000104.zip           2 KB
*|
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 $ 
```



Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

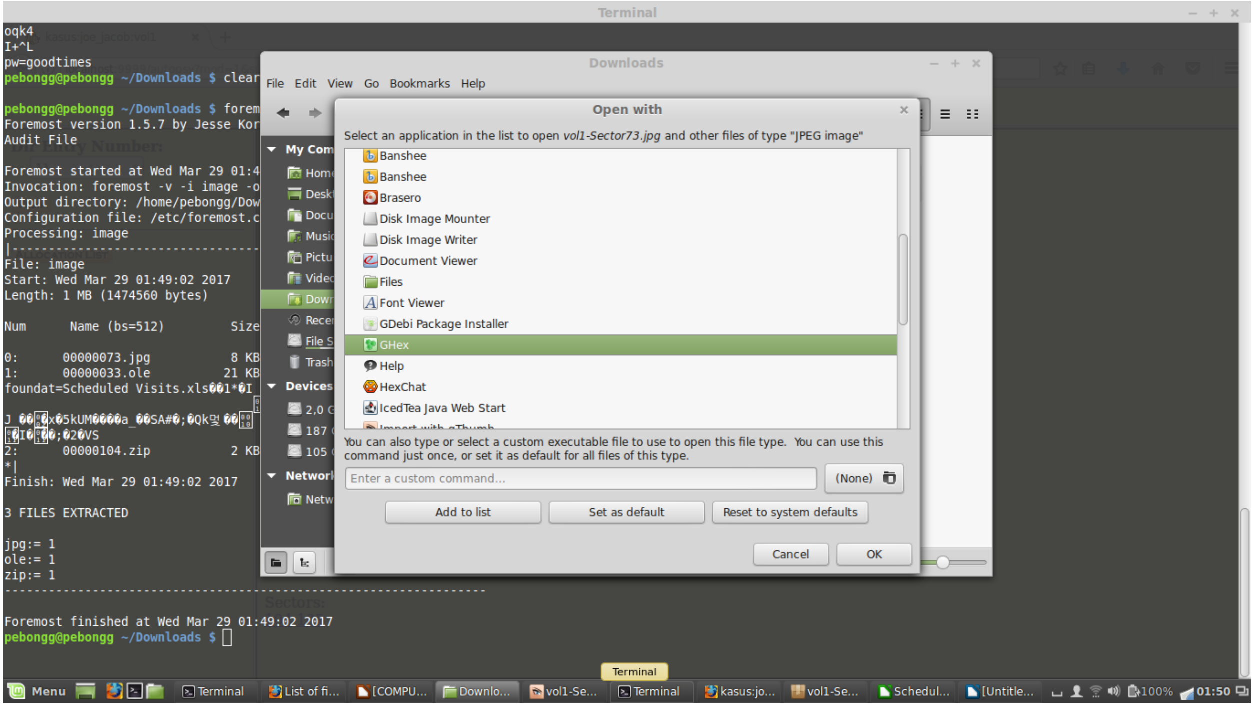
Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

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,

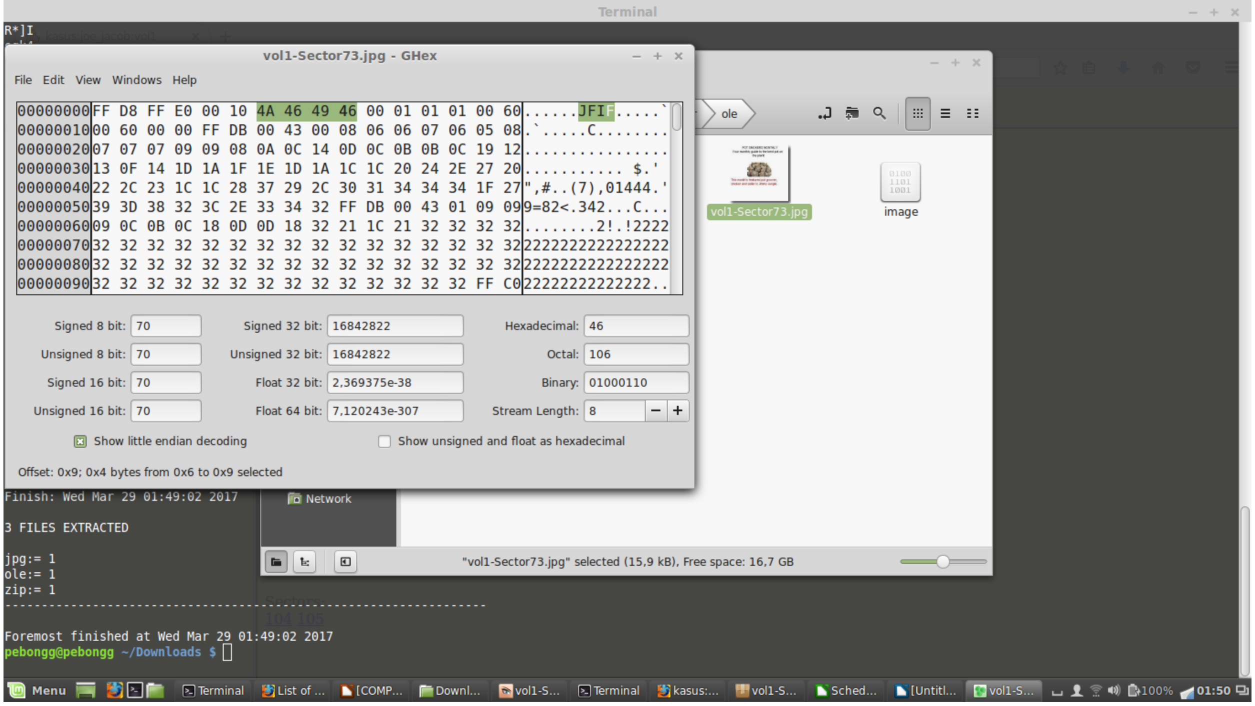
Joe



```
oqk4
I+^L
pw=goodtimes
pebongg@pebongg ~/Downloads $ clear

pebongg@pebongg ~/Downloads $ forem
Foremost version 1.5.7 by Jesse Kor
Audit File

Foremost started at Wed Mar 29 01:4
Invocation: foremost -v -i image -o
Output directory: /home/pebongg/Dow
Configuration file: /etc/foremost.c
Processing: image
|----------------------------------
File: image
Start: Wed Mar 29 01:49:02 2017
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)         Size

0:       00000073.jpg           8 KB
1:       00000033.ole          21 KB
foundat=Scheduled Visits.xls��1*�I

J ���x�5kUM����a_��SA#�;�Qk멎 ��
��I���;�2�VS
2:       00000104.zip           2 KB
*|
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 $ 
```

Select an application in the list to open *vol1-Sector73.jpg* and other files of type "JPEG image"

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.



```
00000000FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60......JFIF.....`
0000001000 60 00 00 FF DB 00 43 00 08 06 06 07 06 05 08.`.....C........
0000002007 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12................
0000003013 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20........... $.' 
0000004022 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27",#..(7),01444.'
0000005039 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 099=82<.342...C...
0000006009 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32........2!.!2222
0000007032 32 32 32 32 32 32 32 32 32 32 32 32 32 32 322222222222222222
0000008032 32 32 32 32 32 32 32 32 32 32 32 32 32 32 322222222222222222
0000009032 32 32 32 32 32 32 32 32 32 32 32 32 32 FF C022222222222222..
```

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

"vol1-Sector73.jpg" selected (15,9 kB), Free space: 16,7 GB

```
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 $ 
```

Sesuai 8 gambar di atas, perintah foremost digunakan untuk mengembalikan/mengesktrak data yang tertimpa dan diletakkan pada folder recover. Dan didapatkan 3 folder yaitu, jpg, ole dan zip. Ole merupakan file doc yang berisi surat dari Joe Jacob untuk Jimmy. Menggunakan perintah ghex untuk mengkonversi huruf ke biner sambal mengecek kembali file dari .jpg.

Setelah berhasil mendapatkan data dari percobaan, 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 ?**
   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 sekoolah 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.