KEAMANAN JARINGAN KOMPUTER

“COMPUTER FORENSICS”

OLEH :

LISA MARDALETA

09011181320032

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

- **Definisi Computer Forensics :**

Secara Garis Besar, di rangkum dari berbagai sumber :

"suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun piranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan."

- **Tujuan dan Fokus Komputer Forensik :**

Tujuan :

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki yang sah di pengadilan.

2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Fokus data yang di kumpulkan di bagi menjadi 3 kategori :

1. Active Data

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

2. Archival Data

yaitu informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpan seperti hardisk eksternal, CD ROM, backup tape, DVD, dan lain-lain.

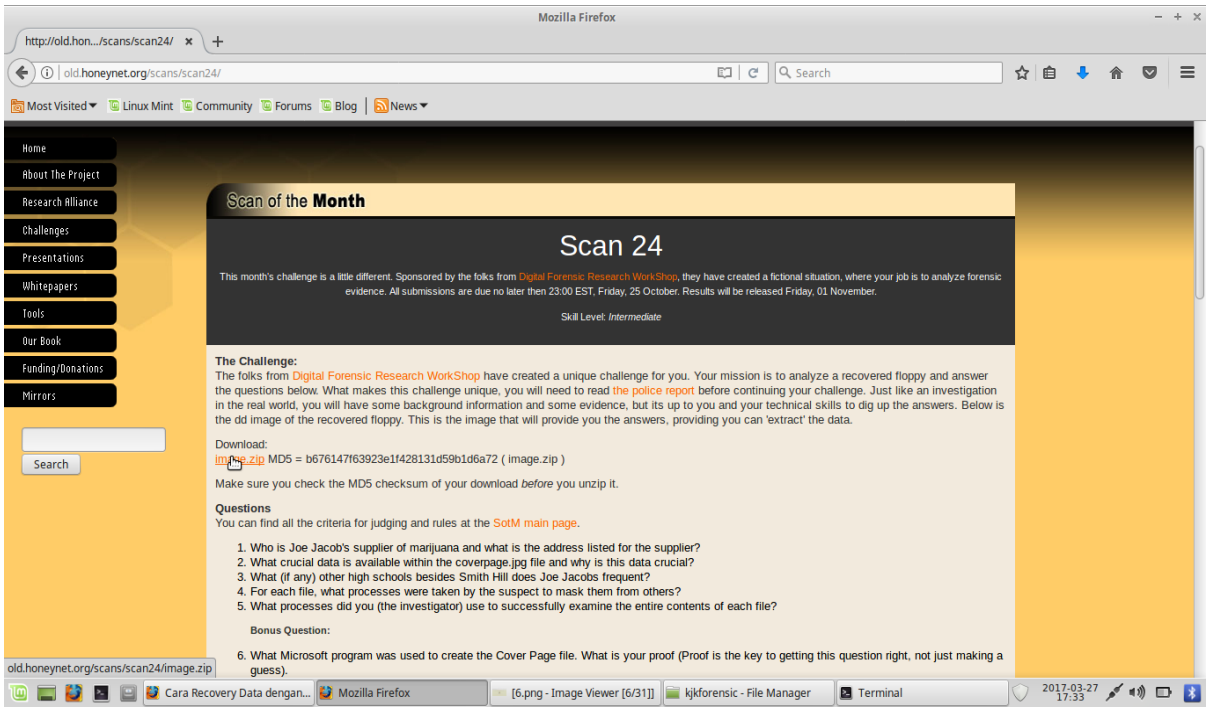
3. Latent Data

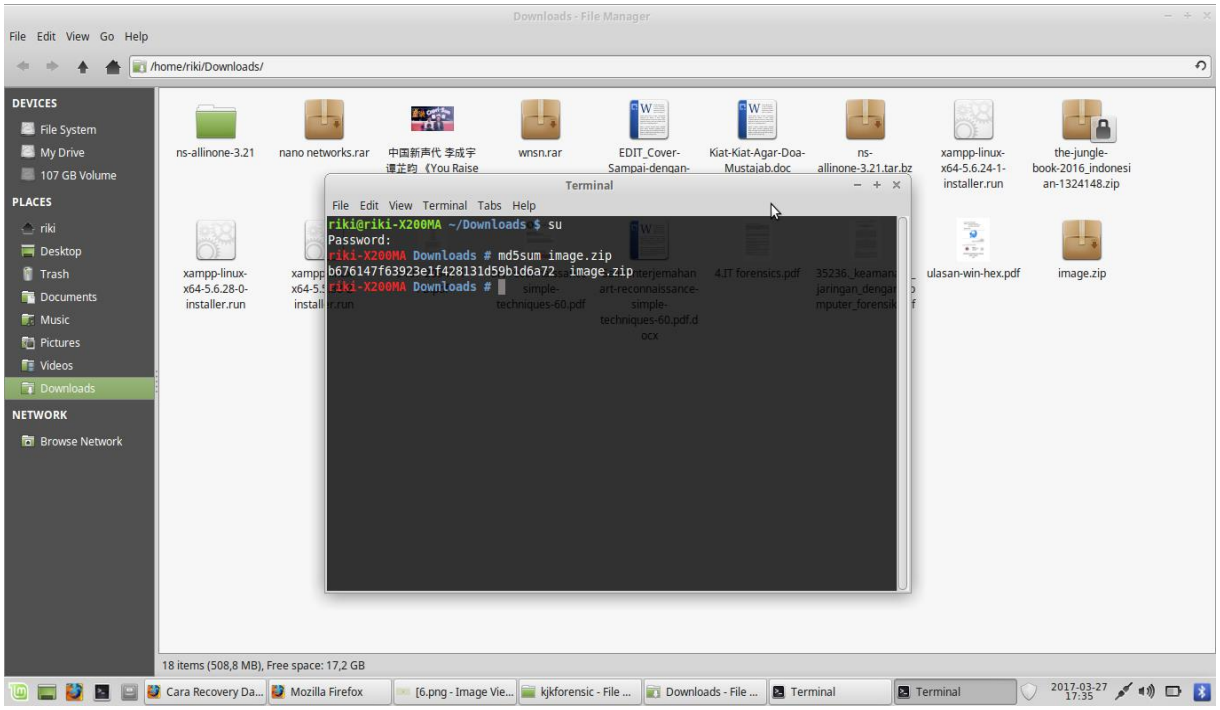
yaitu informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya.

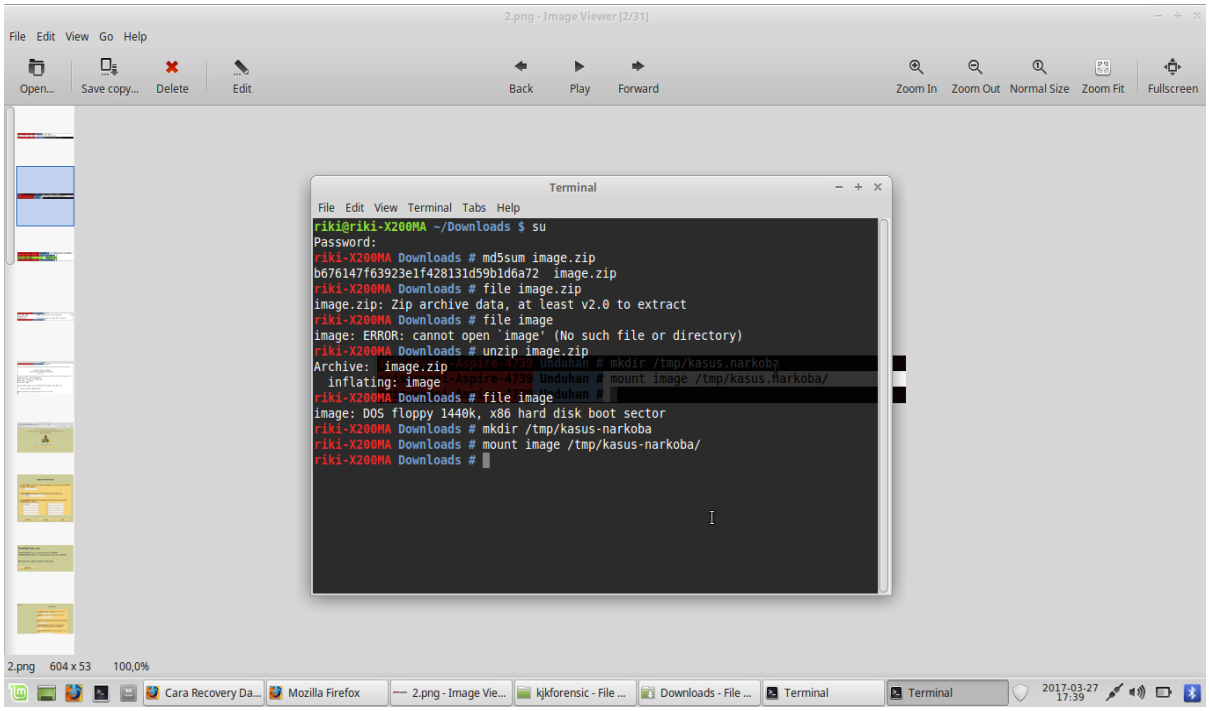
- Tools yang kita gunakan :

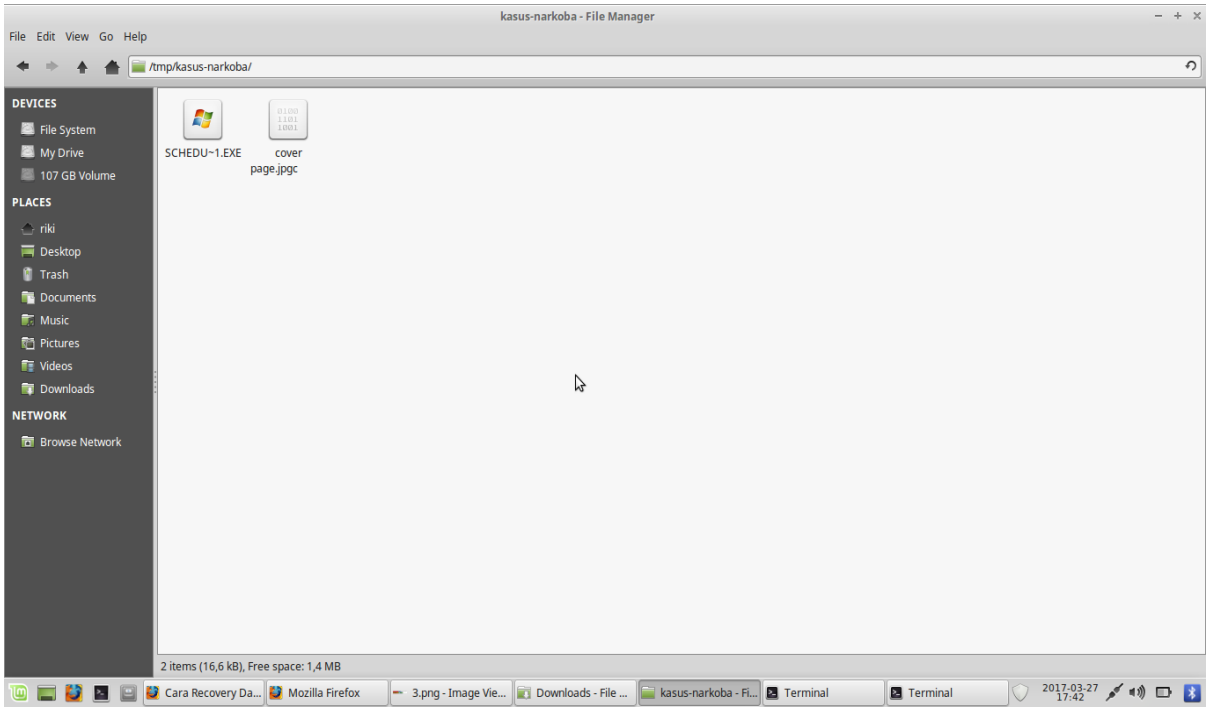
- AutoPsy
- Foremost

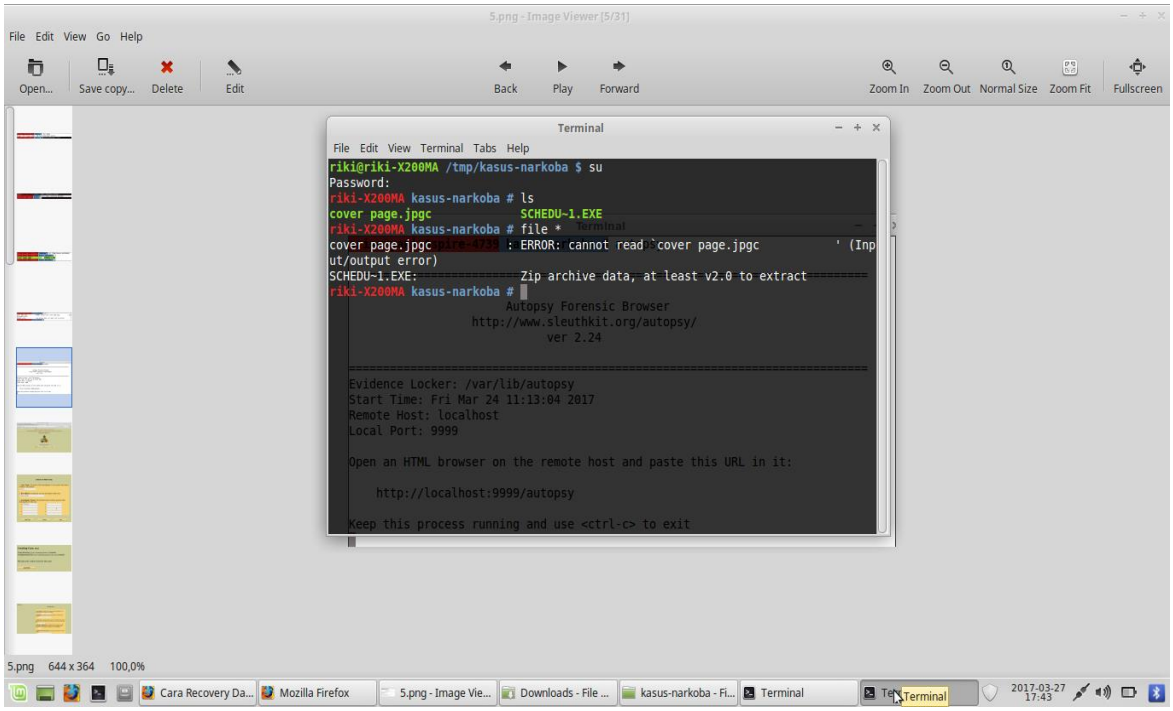
- Strings
- Ghex

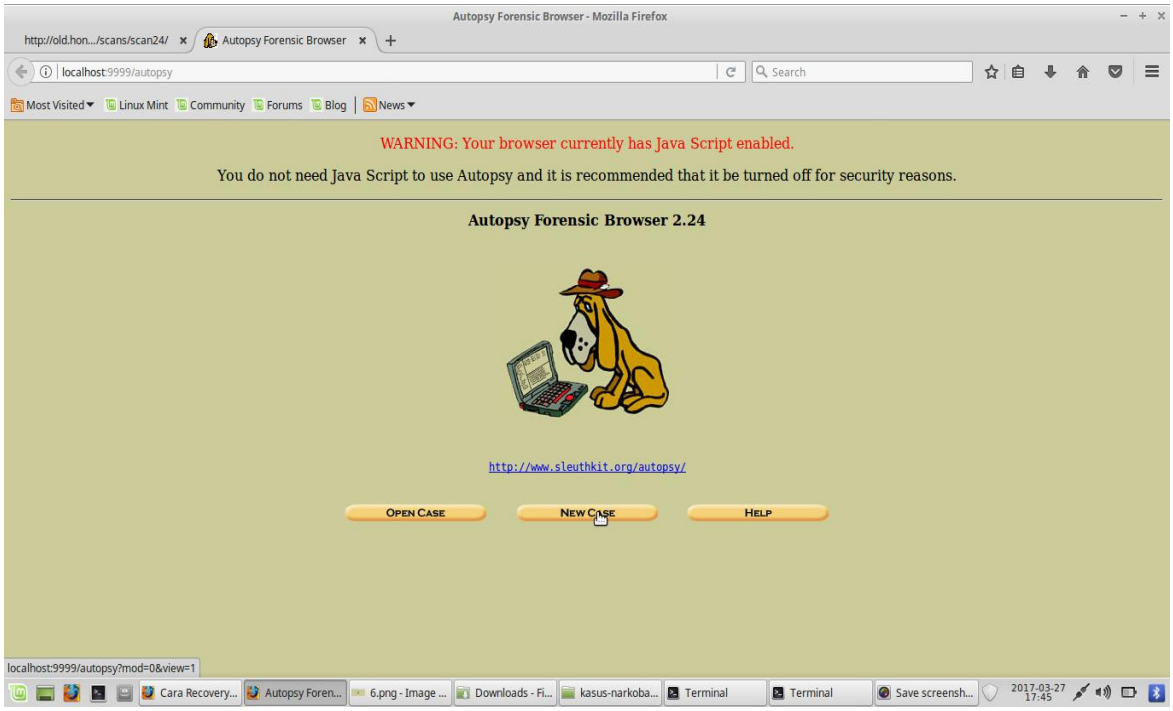


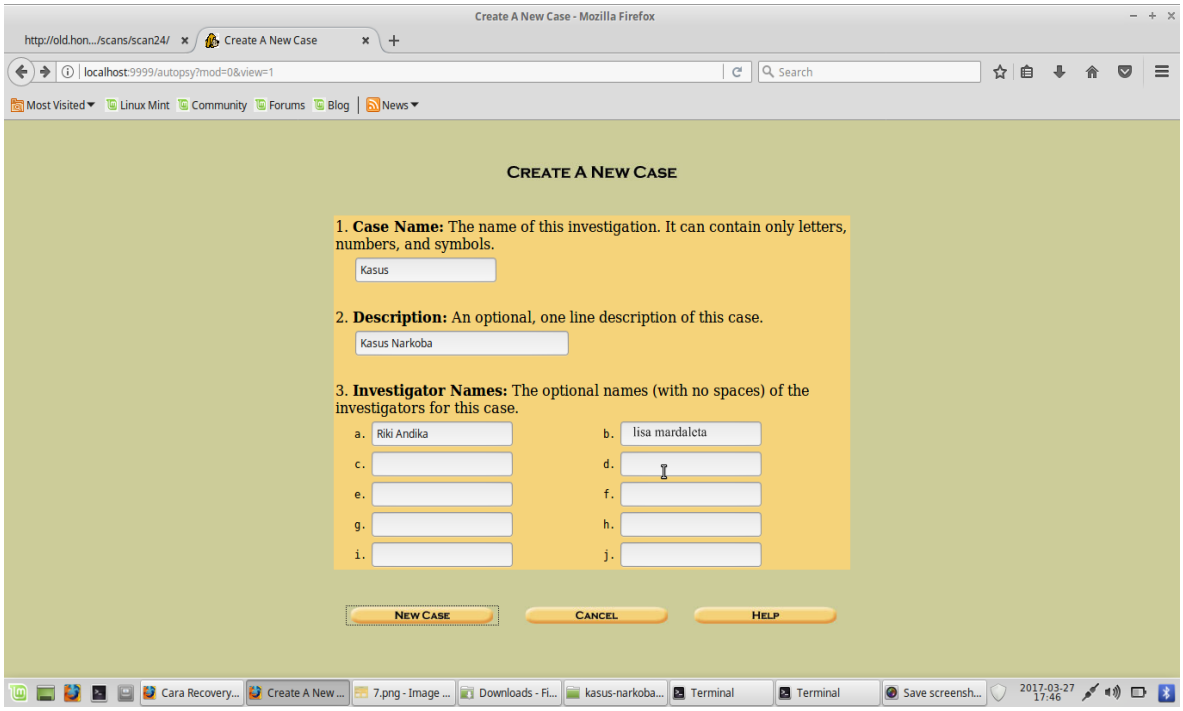


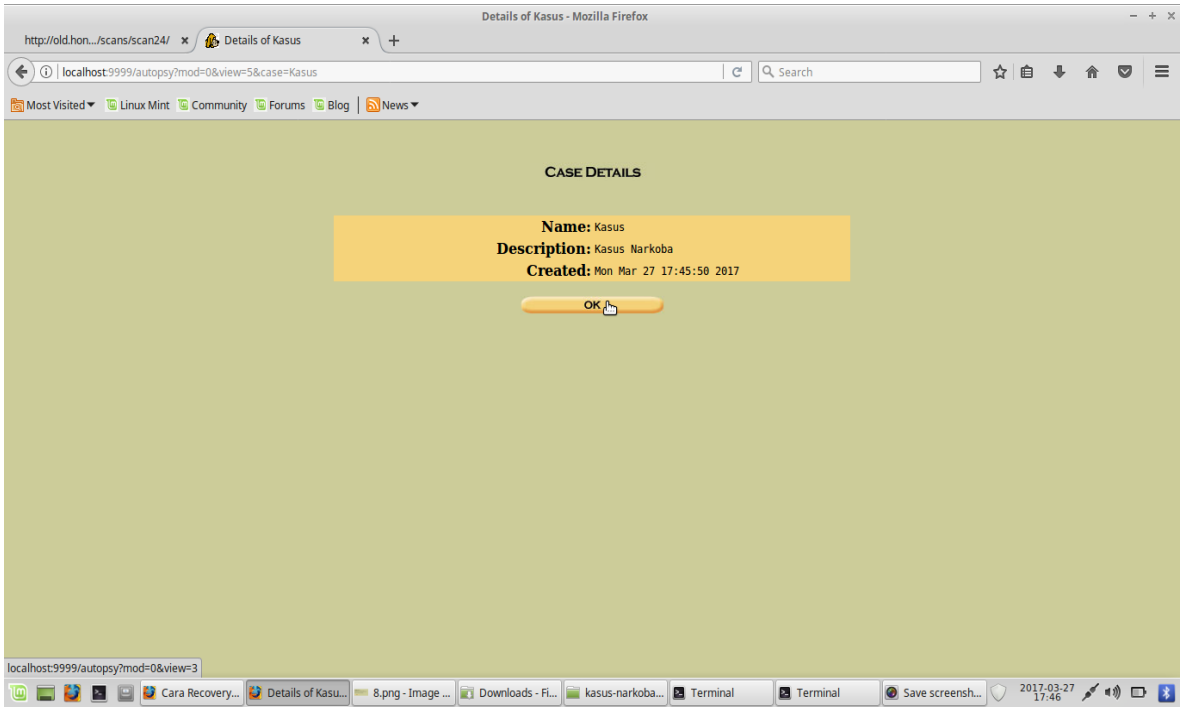

2.png - Image Viewer [2/31]
File Edit View Go Help
Open... Save copy... Delete Edit Back Play Forward Zoom In Zoom Out Normal Size Zoom Fit Fullscreen
Terminal
File Edit View Terminal Tabs Help
riki@riki-X200MA ~/Downloads $ su
Password:
riki-X200MA Downloads # md5sum image.zip
b676147f63923e1f428131d59b1d6a72 image.zip
riki-X200MA Downloads # file image.zip
image.zip: Zip archive data, at least v2.0 to extract
riki-X200MA Downloads # file image
image: ERROR: cannot open `image' (No such file or directory)
riki-X200MA Downloads # unzip image.zip
Archive: image.zip
inflating: image
riki-X200MA Downloads # file image
image: DOS floppy 1440k, x86 hard disk boot sector
riki-X200MA Downloads # mkdir /tmp/kasus-narkoba
riki-X200MA Downloads # mount image /tmp/kasus-narkoba/
riki-X200MA Downloads #
2.png 604 x 53 100,0%
Cara Recovery Da... Mozilla Firefox 2.png - Image Vie... kjkforensic - File ... Downloads - File ... Terminal Terminal
2017-03-27 17:39

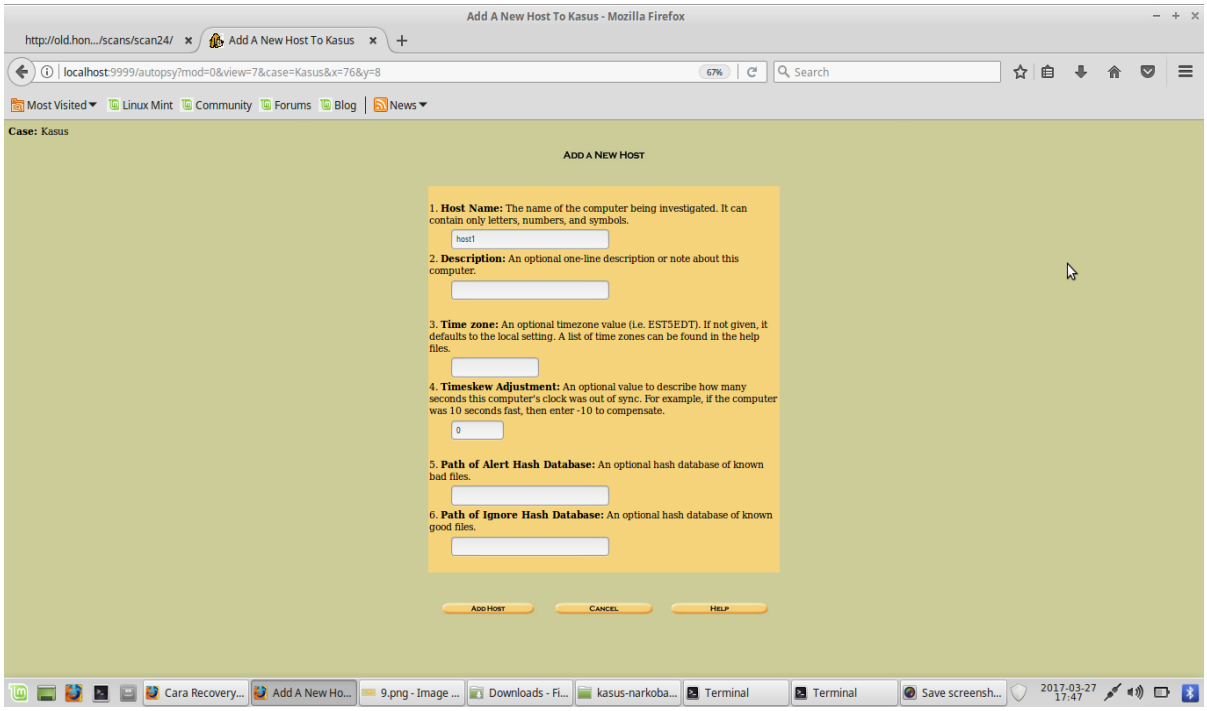

kasus-narkoba - File Manager
File Edit View Go Help
/tmp/kasus-narkoba/
DEVICES
File System
My Drive
107 GB Volume
PLACES
riki
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
SCHEDU~1.EXE
cover page.jpgc
2 items (16,6 kB), Free space: 1,4 MB
Cara Recovery Da... Mozilla Firefox 3.png - Image Vie... Downloads - File ... kasus-narkoba - Fi... Terminal Terminal
2017-03-27 17:42

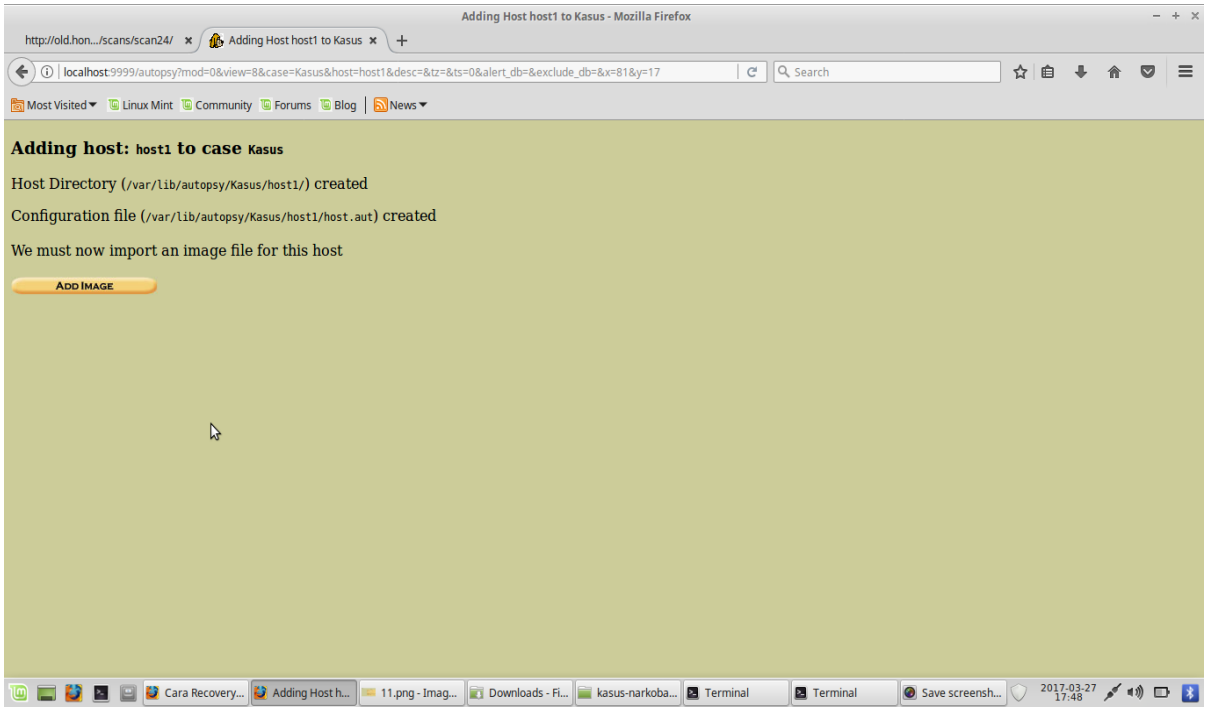

5.png - Image Viewer [5/31]
File Edit View Go Help
Open... Save copy... Delete Edit Back Play Forward Zoom In Zoom Out Normal Size Zoom Fit Fullscreen
Terminal
File Edit View Terminal Tabs Help
riki@riki-X200MA /tmp/kasus-narkoba $ su
Password:
riki-X200MA kasus-narkoba # ls
cover page.jpgc SCHEDU~1.EXE
riki-X200MA kasus-narkoba # file *
cover page.jpgc : ERROR: cannot read `cover page.jpgc ' (Input/output error)
SCHEDU~1.EXE: Zip archive data, at least v2.0 to extract
riki-X200MA kasus-narkoba #
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy
Start Time: Fri Mar 24 11:13:04 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
5.png 644 x 364 100,0%
Cara Recovery Da... Mozilla Firefox 5.png - Image Vie... Downloads - File ... kasus-narkoba - Fi... Terminal Terminal
2017-03-27 17:43

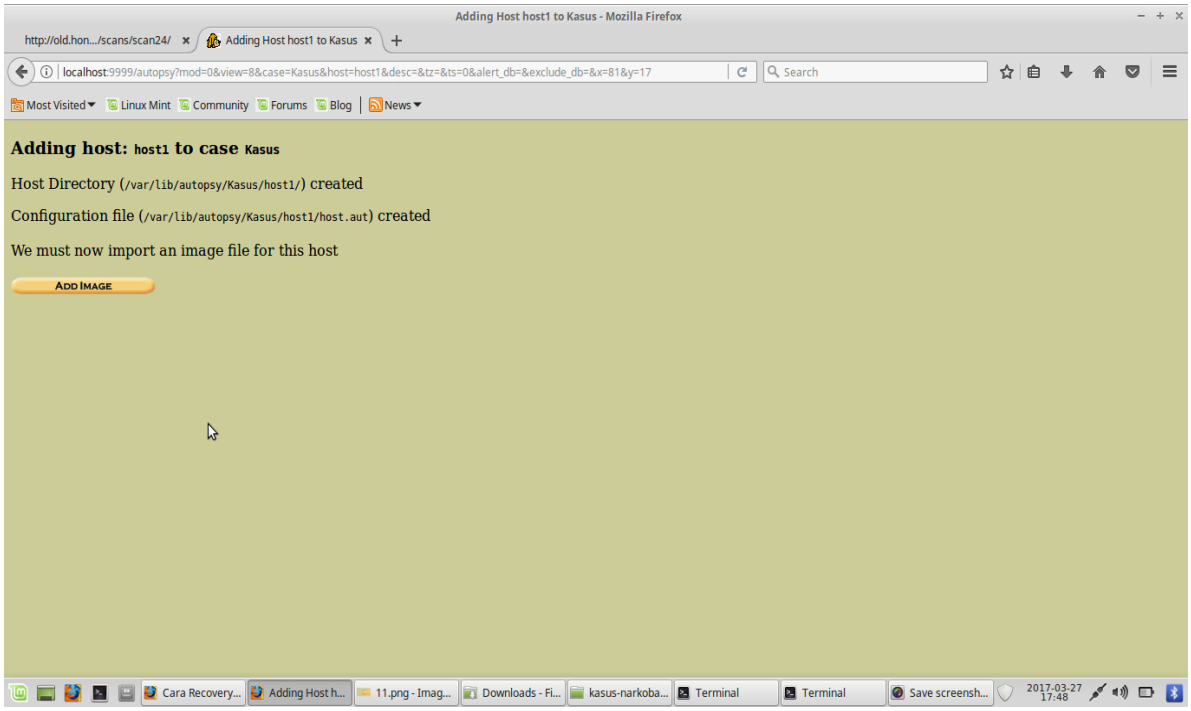

Autopsy Forensic Browser - Mozilla Firefox
http://old.hon.../scans/scan24/ Autopsy Forensic Browser
localhost:9999/autopsy
Search
Most Visited Linux Mint Community Forums Blog News
WARNING: Your browser currently has Java Script enabled.
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.
Autopsy Forensic Browser 2.24
http://www.sleuthkit.org/autopsy/
OPEN CASE NEW CASE HELP
localhost:9999/autopsy?mod=0&view=1
Cara Recovery... Autopsy Foren... 6.png - Image ... Downloads - Fi... kasus-narkoba... Terminal Terminal Save screensh...
2017-03-27 17:45

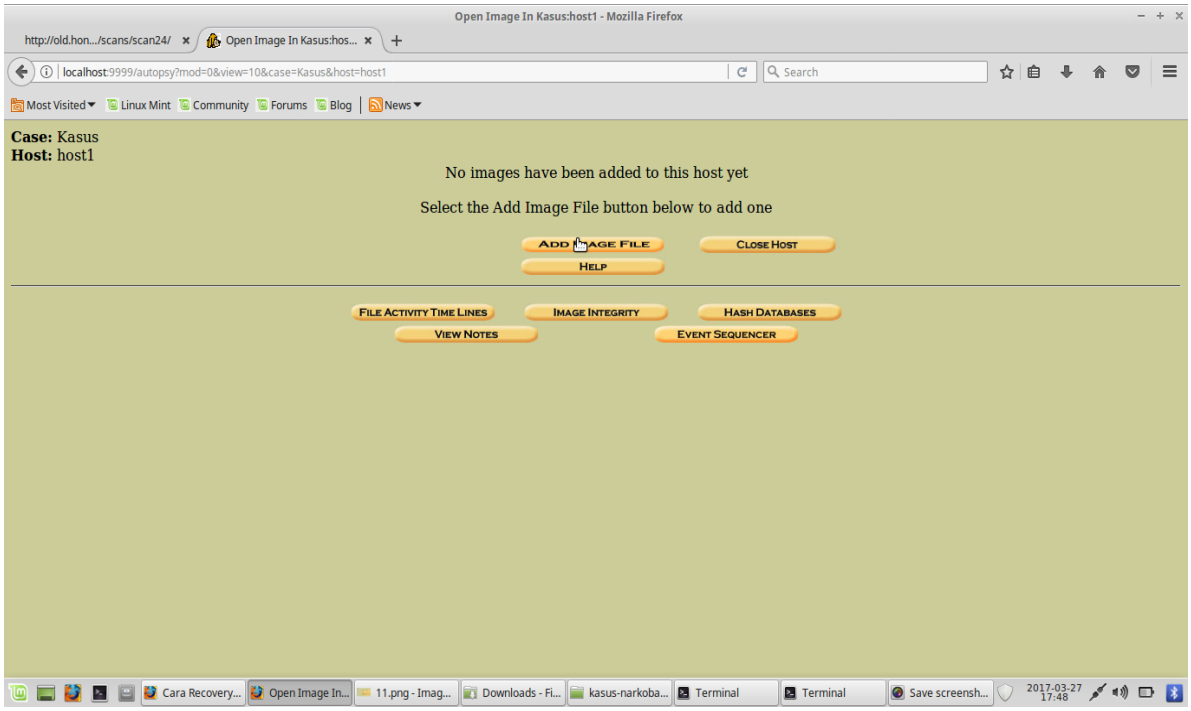

Create A New Case - Mozilla Firefox
http://old.hon.../scans/scan24/
Create A New Case
localhost:9999/autopsy?mod=0&view=1
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
Kasus
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. Riki Andika
b. lisa mardaleta
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP
Cara Recovery...
Create A New ...
7.png - Image ...
Downloads - Fi...
kasus-narkoba...
Terminal
Terminal
Save screensh...
2017-03-27 17:46


Details of Kasus - Mozilla Firefox
http://old.hon.../scans/scan24/
Details of Kasus
localhost:9999/autopsy?mod=0&view=5&case=Kasus
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
CASE DETAILS
Name: Kasus
Description: Kasus Narkoba
Created: Mon Mar 27 17:45:50 2017
OK
localhost:9999/autopsy?mod=0&view=3
Cara Recovery...
Details of Kasu...
8.png - Image ...
Downloads - Fi...
kasus-narkoba...
Terminal
Terminal
Save screensh...
2017-03-27 17:46


Add A New Host To Kasus - Mozilla Firefox
http://old.hon.../scans/scan24/
Add A New Host To Kasus
localhost:9999/autopsy?mod=0&view=7&case=Kasus&x=76&y=8
Most Visited
Linux Mint
Community
Forums
Blog
News
Case: Kasus
ADD A NEW HOST
1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
host1
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.
ADD HOST
CANCEL
HELP

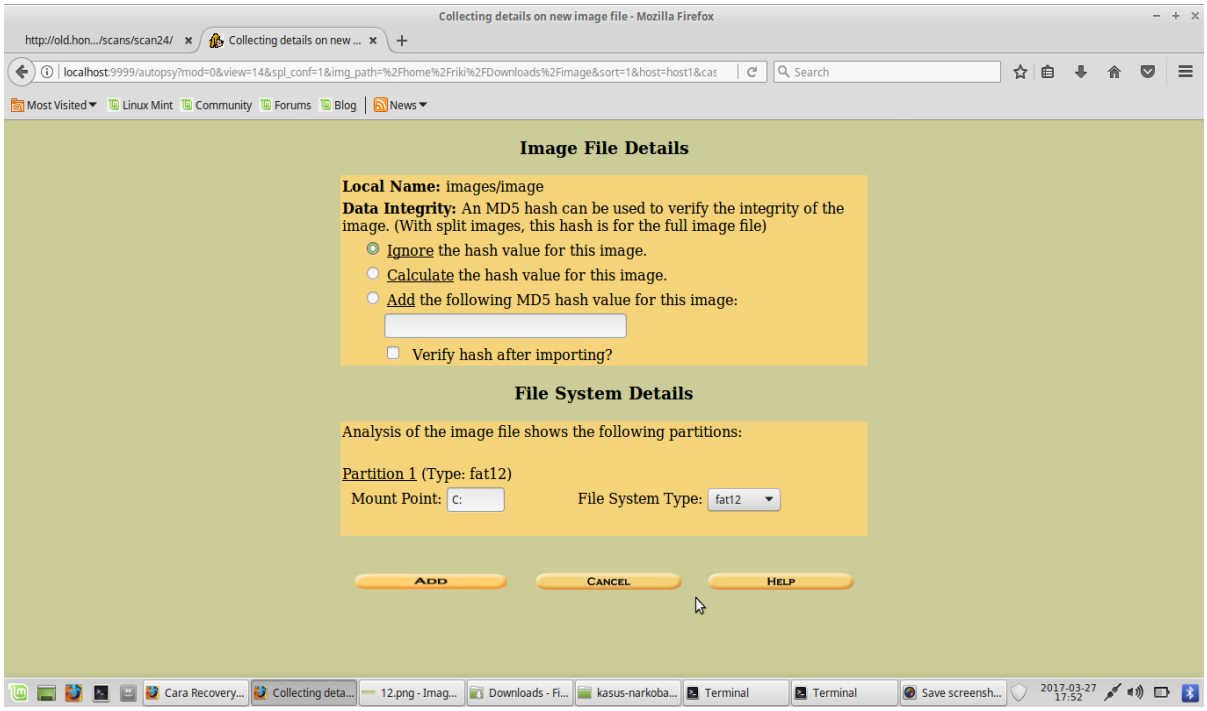

Adding Host host1 to Kasus - Mozilla Firefox
http://old.hon.../scans/scan24/
Adding Host host1 to Kasus
localhost:9999/autopsy?mod=0&view=8&case=Kasus&host=host1&desc=&tz=&ts=0&alert_db=&exclude_db=&x=81&y=17
Most Visited
Linux Mint
Community
Forums
Blog
News
Adding host: host1 to case Kasus
Host Directory (/var/lib/autopsy/Kasus/host1/) created
Configuration file (/var/lib/autopsy/Kasus/host1/host.aut) created
We must now import an image file for this host
ADD IMAGE

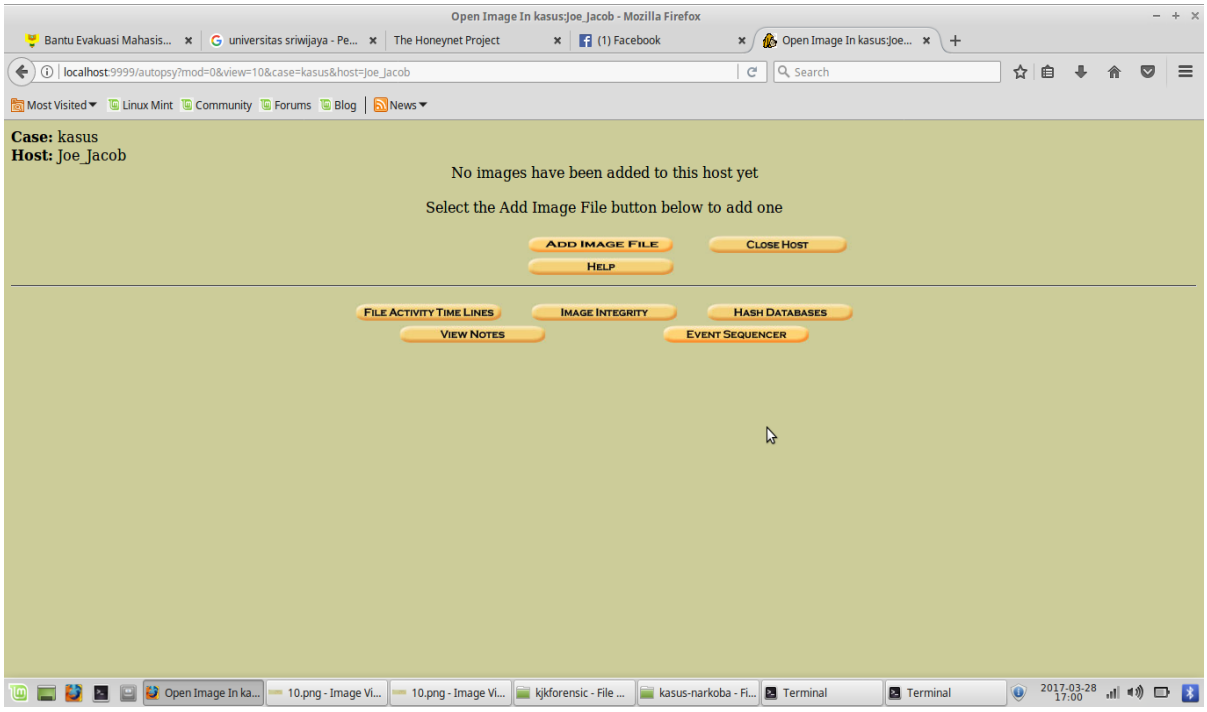

Adding Host host1 to Kasus - Mozilla Firefox
http://old.hon.../scans/scan24/
Adding Host host1 to Kasus
localhost:9999/autopsy?mod=0&view=8&case=Kasus&host=host1&desc=&tz=&ts=0&alert_db=&exclude_db=&x=81&y=17
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
Adding host: host1 to case Kasus
Host Directory (/var/lib/autopsy/Kasus/host1/) created
Configuration file (/var/lib/autopsy/Kasus/host1/host.aut) created
We must now import an image file for this host
ADD IMAGE
Cara Recovery...
Adding Host h...
11.png - Imag...
Downloads - Fi...
kasus-narkoba...
Terminal
Terminal
Save screensh...
2017-03-27
17:48

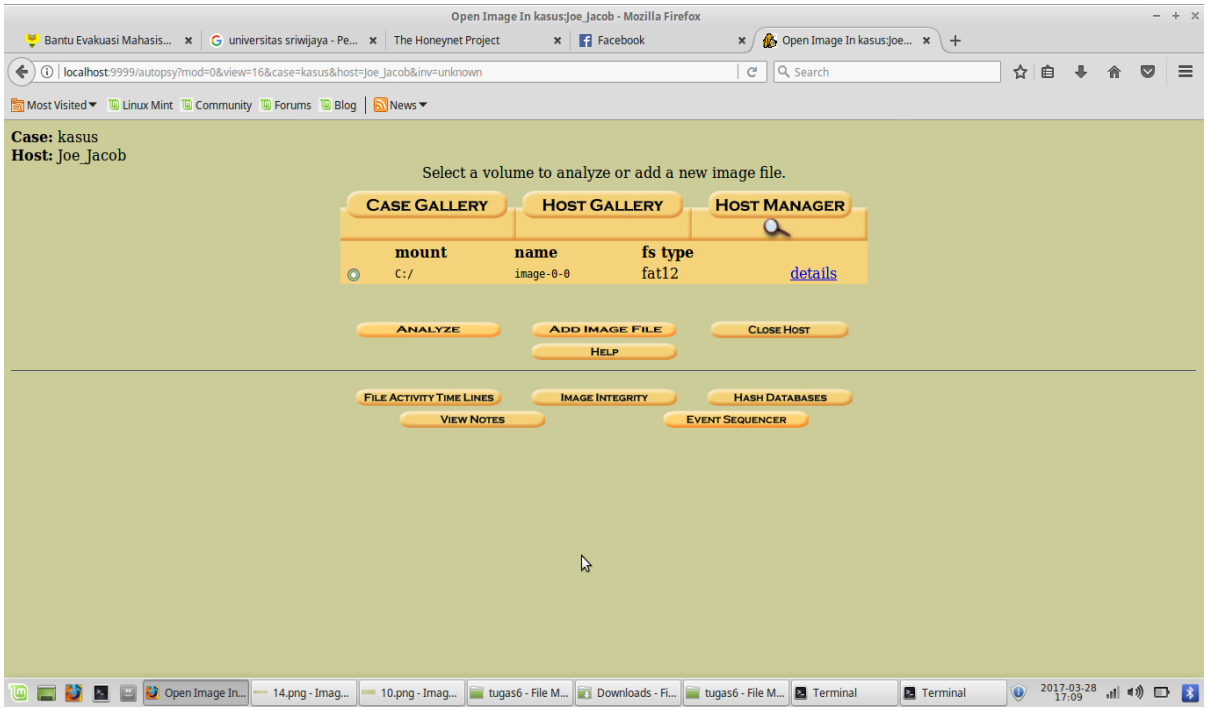

Open Image In Kasus:host1 - Mozilla Firefox
http://old.hon.../scans/scan24/
Open Image In Kasus:hos...
localhost:9999/autopsy?mod=0&view=10&case=Kasus&host=host1
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
Case: Kasus
Host: host1
No images have been added to this host yet
Select the Add 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
Cara Recovery...
Open Image In...
11.png - Imag...
Downloads - Fi...
kasus-narkoba...
Terminal
Terminal
Save screensh...
2017-03-27
17:48

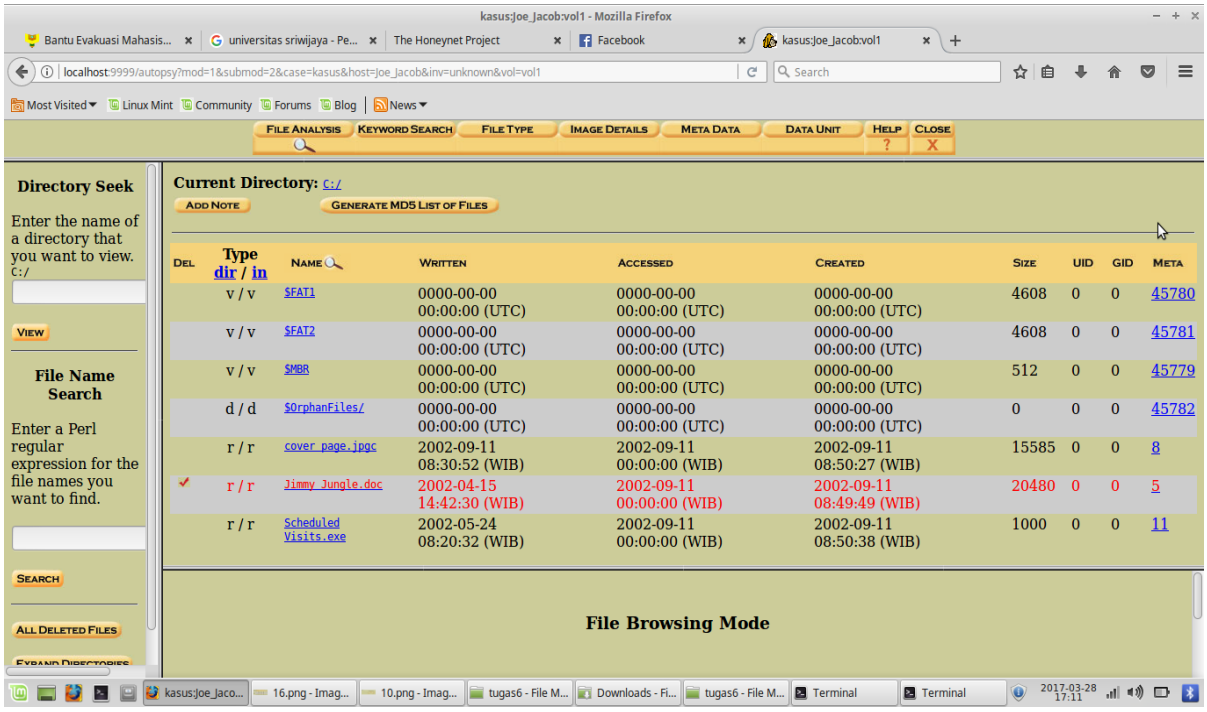

Add Image To Kasus:host1 - Mozilla Firefox
http://old.hon.../scans/scan24/
Add Image To Kasus:host1
localhost:9999/autopsy?mod=0&view=13&case=Kasus&host=host1&inv=unknown
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
Case: Kasus
Host: host1
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/riki/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
Cara Recovery...
Add Image To ...
14.png - Imag...
Downloads - Fi...
kasus-narkoba...
Terminal
Terminal
Save screensh...
2017-03-27 17:51

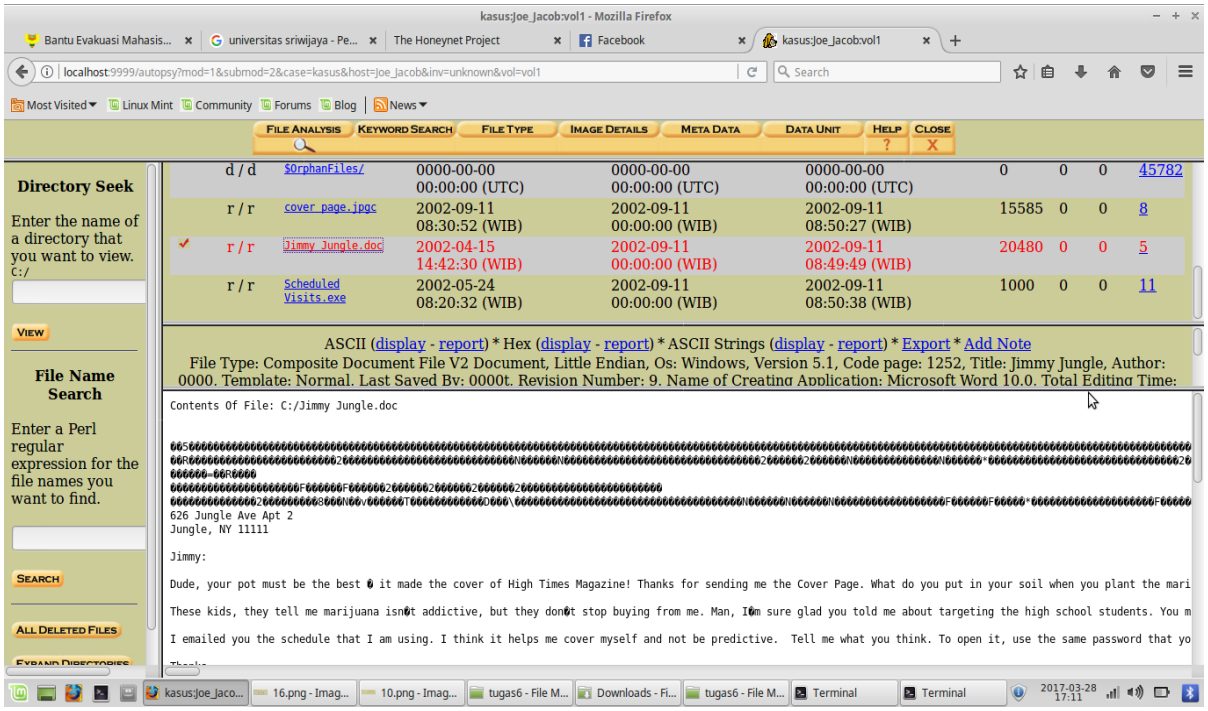

Collecting details on new image file - Mozilla Firefox
http://old.hon.../scans/scan24/
Collecting details on new ...
localhost:9999/autopsy?mod=0&view=14&host=host1&case=Kasus&inv=unknown&img_path=%2Fhome%2Friki%2FDownloads%2Fim
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
Warning: Autopsy 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
Cara Recovery...
Collecting deta...
14.png - Imag...
Downloads - Fi...
kasus-narkoba...
Terminal
Terminal
Save screensh...
2017-03-27 17:51

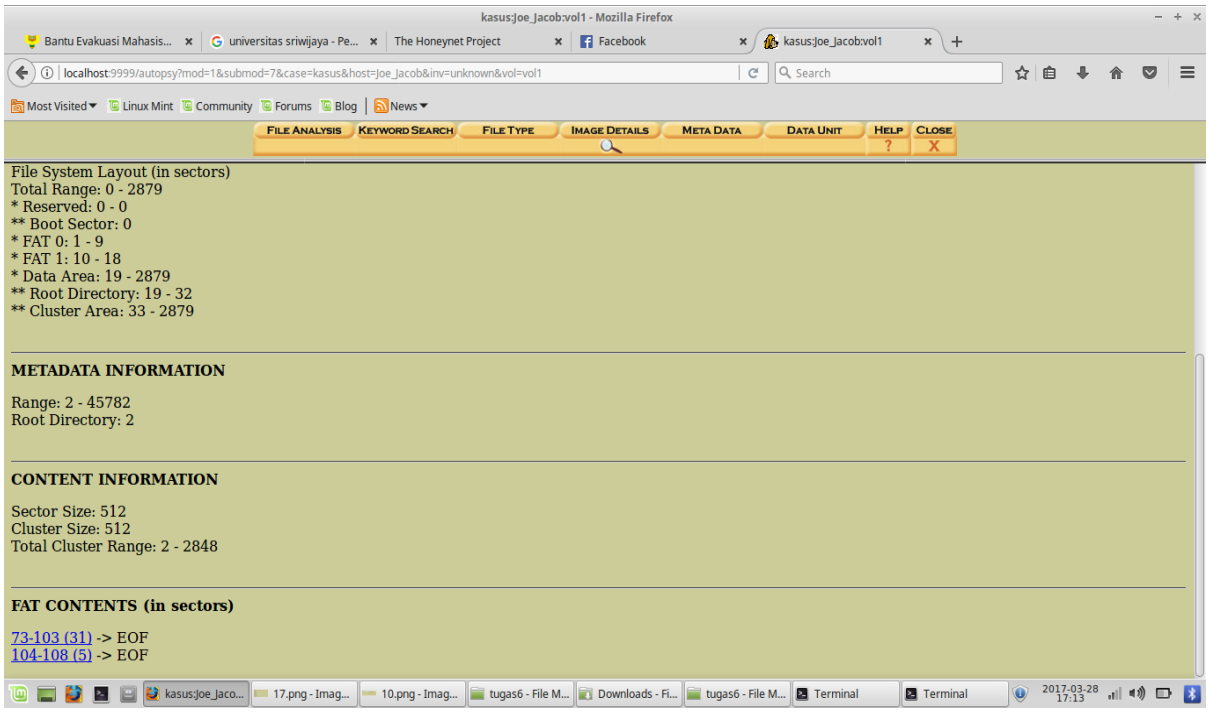

Collecting details on new image file - Mozilla Firefox
Image File Details
Local Name: images/image
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for 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
CANCEL
HELP

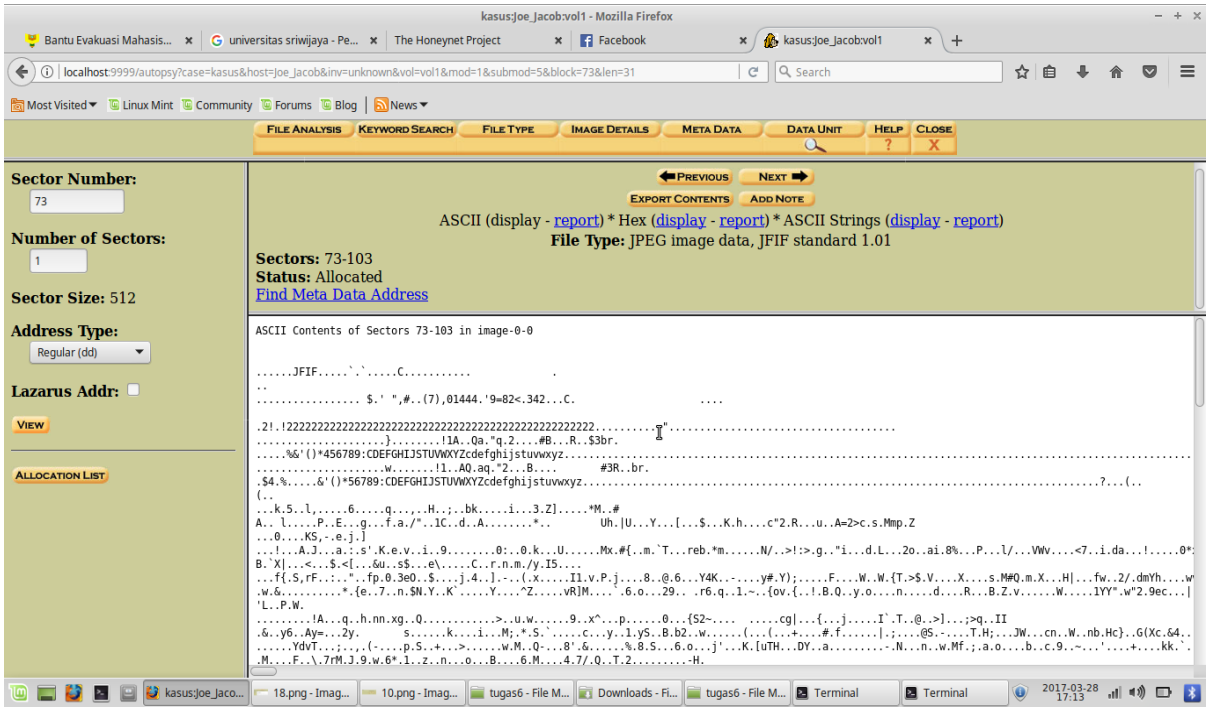

Open Image In kasus:Joe_Jacob - Mozilla Firefox
Case: kasus
Host: Joe_Jacob
No images have been added to this host yet
Select the Add Image File button below to add one
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER

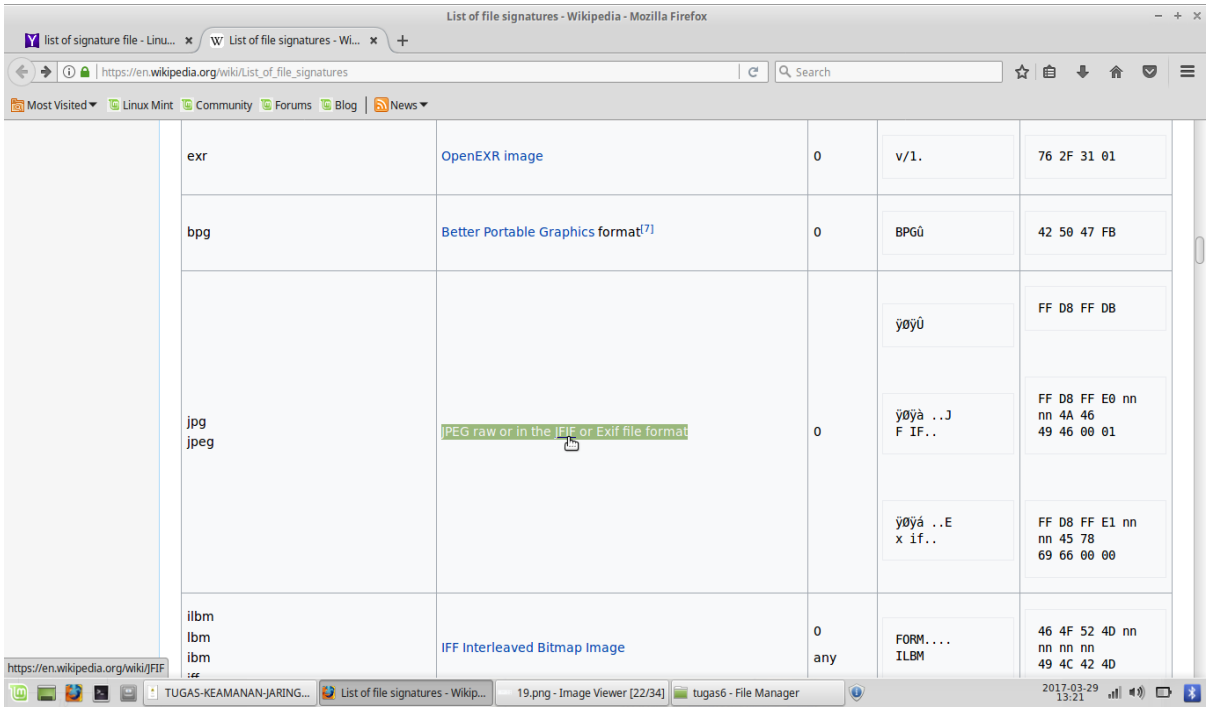

Open Image In kasus:Joe_Jacob - Mozilla Firefox
localhost:9999/autopsy?mod=0&view=16&case=kasus&host=Joe_Jacob&inv=unknown
Case: kasus
Host: Joe_Jacob
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
image-0-0
fat12
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER

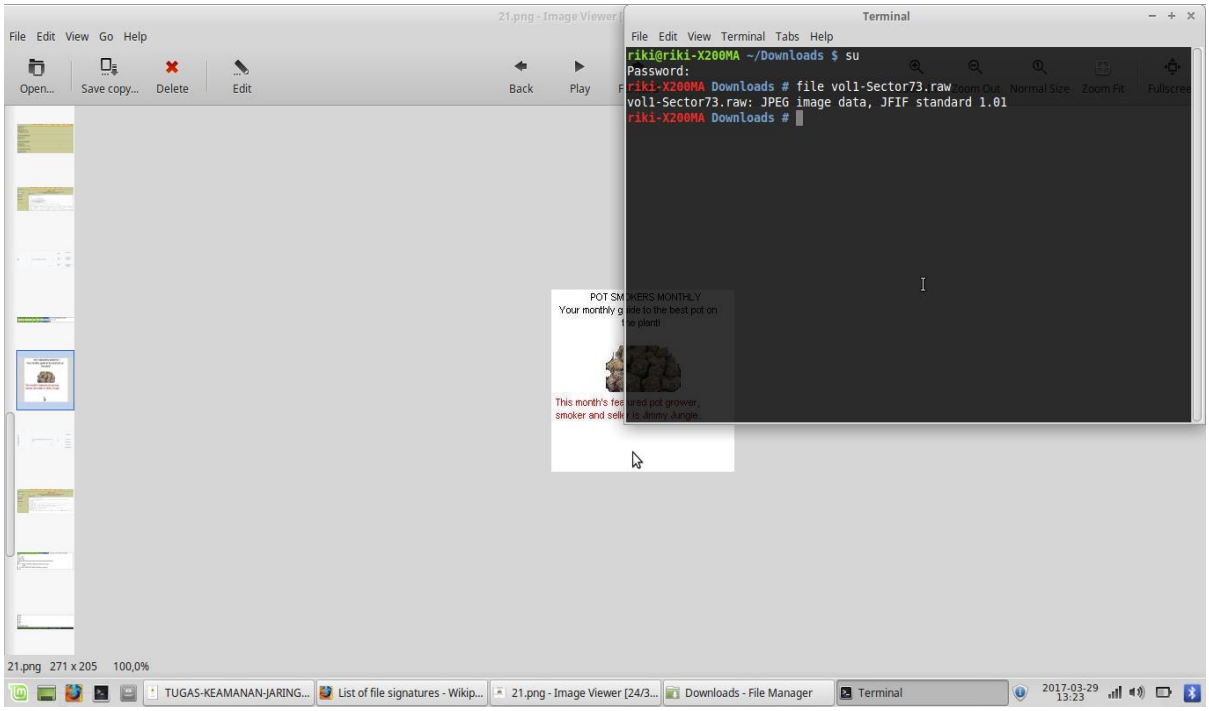

kasus:Joe_Jacob:vol1 - Mozilla Firefox
localhost:9999/autopsy?mod=1&submod=2&case=kasus&host=Joe_Jacob&inv=unknown&vol=vol1
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
Current Directory: C:/
ADD NOTE
GENERATE MD5 LIST OF FILES
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
File Browsing Mode

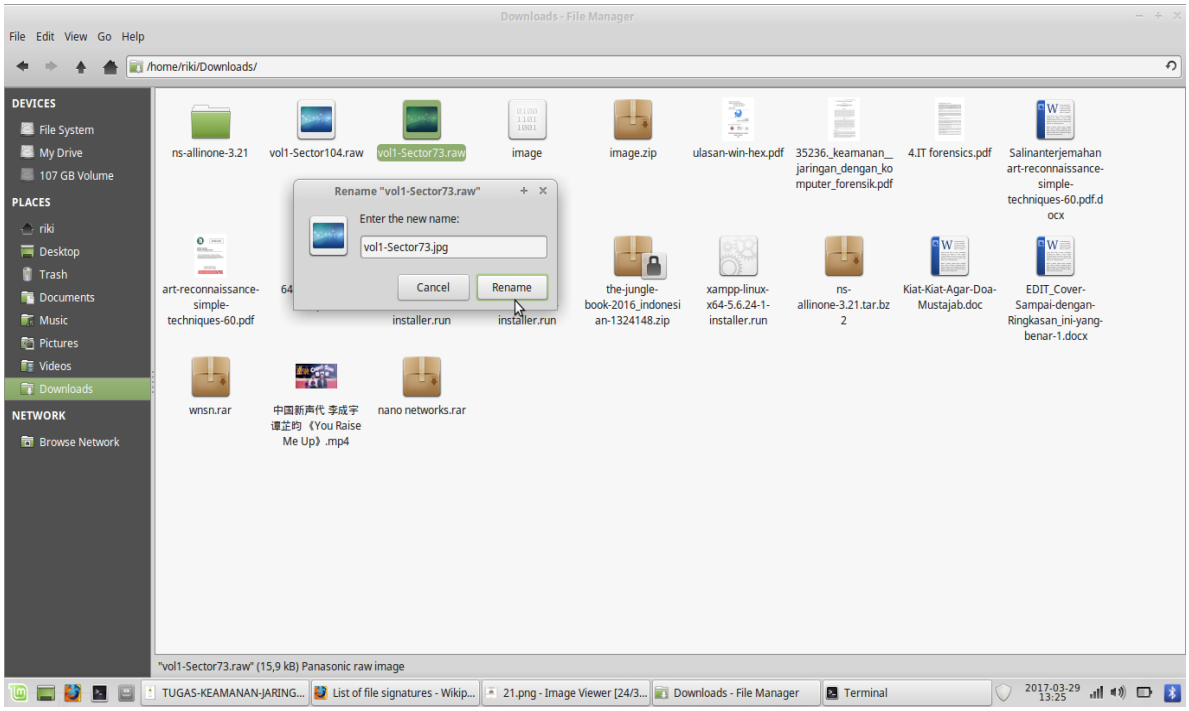

kasus:Joe_Jacob:vol1 - Mozilla Firefox
localhost:9999/autopsy?mod=1&submod=2&case=kasus&host=Joe_Jacob&inv=unknown&vol=vol1
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
$OrphanFiles/
cover_page.jpgc
Jimmy_Jungle.doc
Scheduled Visits.exe
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: Jimmy Jungle, Author: 0000, Template: Normal, Last Saved By: 0000t, Revision Number: 9, Name of Creating Application: Microsoft Word 10.0, Total Editing Time:
Contents Of File: C:/Jimmy Jungle.doc
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 mari
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 m
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 yo

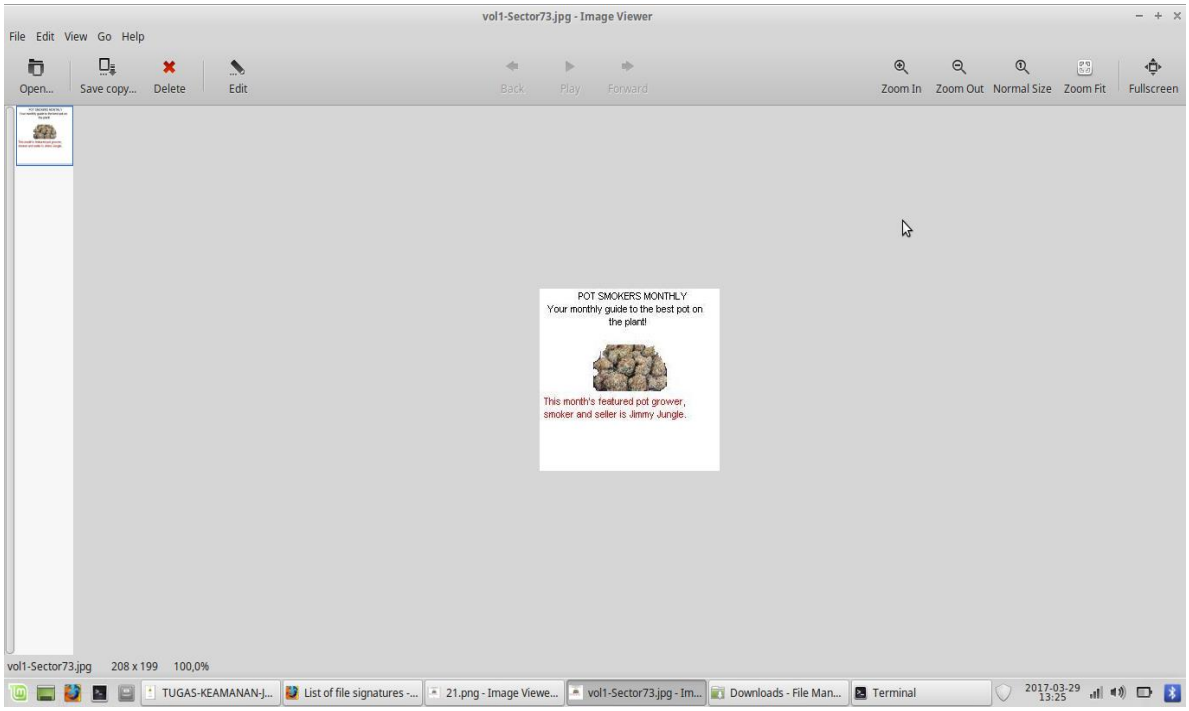

kasus:Joe_Jacob:vol1 - Mozilla Firefox
localhost:9999/autopsy?mod=1&submod=7&case=kasus&host=Joe_Jacob&inv=unknown&vol=vol1
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
File System Layout (in sectors)
Total Range: 0 - 2879
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 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

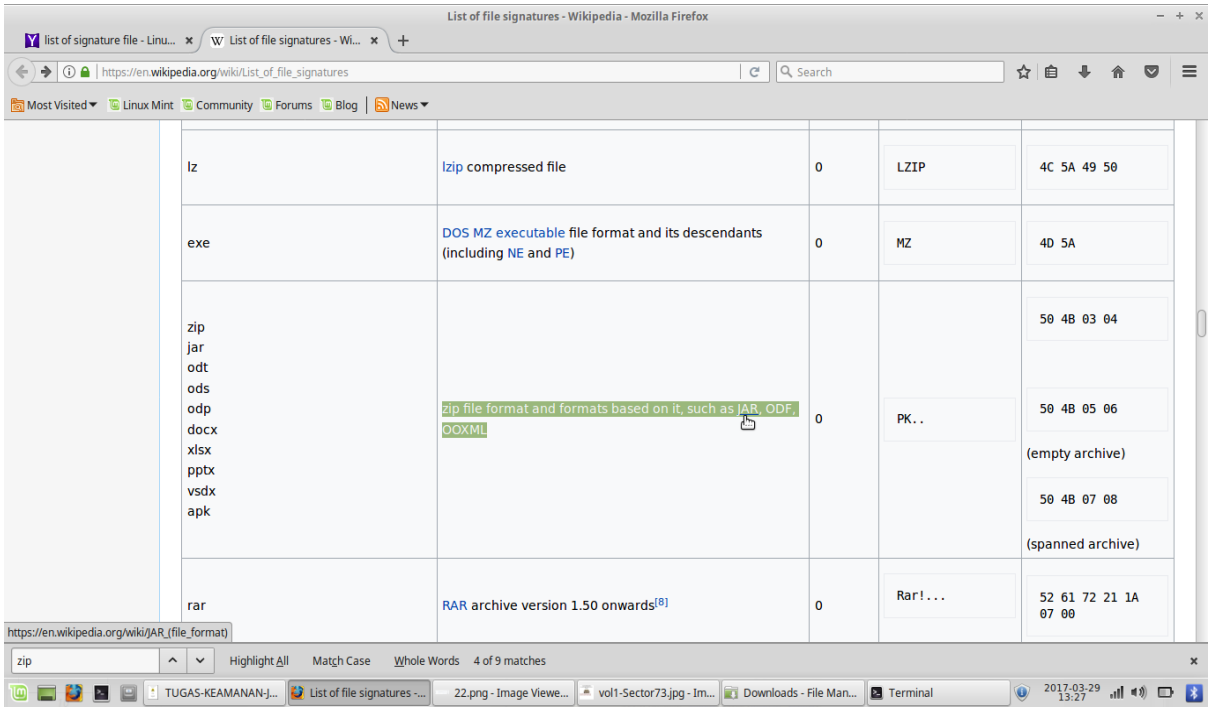

kasus:Joe_Jacob:vol1 - Mozilla Firefox
Bantu Evakuasi Mahasis...
universitas sriwijaya - Pe...
The Honeynet Project
Facebook
kasus:Joe_Jacob:vol1
localhost:9999/autopsy?case=kasus&host=Joe_Jacob&inv=unknown&vol=vol1&mod=1&submod=5&block=73&len=31
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Sector Number:
73
Number of Sectors:
1
Sector Size: 512
Address Type:
Regular (dd)
Lazarus Addr:
VIEW
ALLOCATION LIST
PREVIOUS
NEXT
EXPORT CONTENTS
ADD NOTE
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.....
.2!.!2222222222222222222222222222222222222222222222222222.....
.....%&'()*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.
kasus:Joe_Jaco...
18.png - Imag...
10.png - Imag...
tugas6 - File M...
Downloads - Fi...
tugas6 - File M...
Terminal
Terminal
2017-03-28 17:13

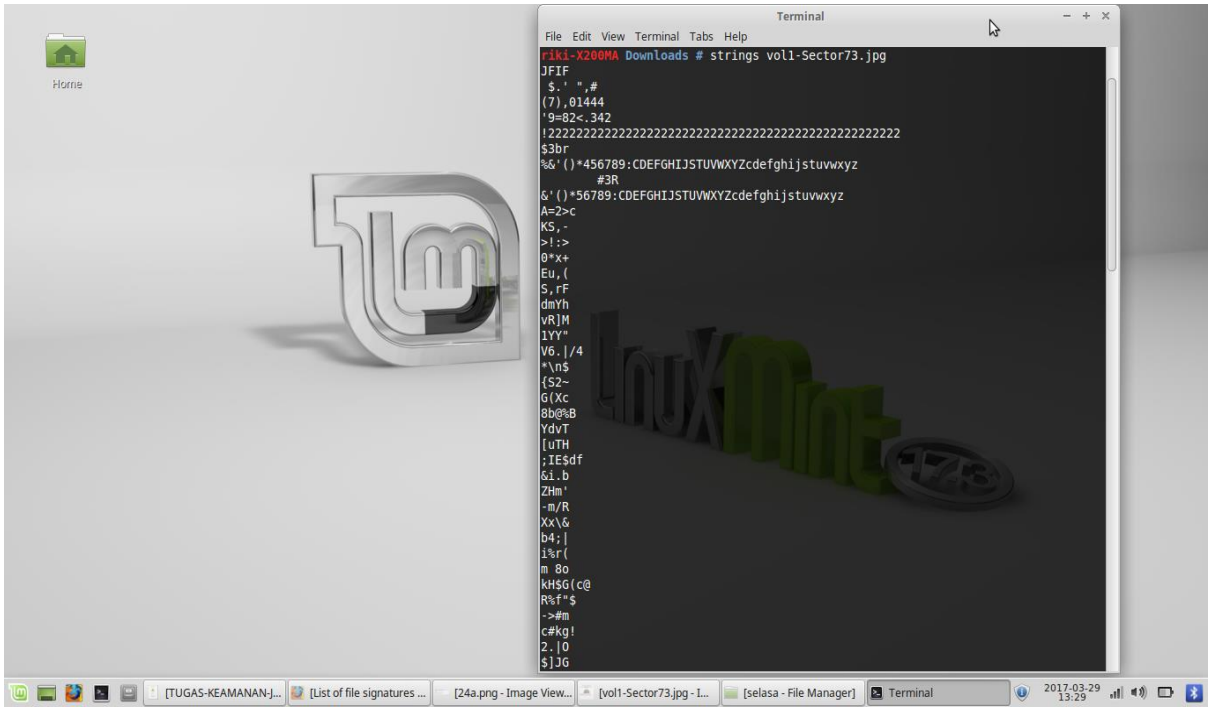

List of file signatures - Wikipedia - Mozilla Firefox
list of signature file - Linu...
List of file signatures - Wi...
https://en.wikipedia.org/wiki/List_of_file_signatures
Search
Most Visited
Linux Mint
Community
Forums
Blog
News
exr | OpenEXR image | 0 | v/1. | 76 2F 31 01
bpg | Better Portable Graphics format[7] | 0 | BPGû | 42 50 47 FB
jpg
jpeg | JPEG raw or in the JFIF or Exif file format | 0 | ÿØÿÛ | 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 Interleaved Bitmap Image | 0
any | FORM....
ILBM | 46 4F 52 4D nn
nn nn nn
49 4C 42 4D
https://en.wikipedia.org/wiki/JFIF
TUGAS-KEAMANAN-JARING...
List of file signatures - Wikip...
19.png - Image Viewer [22/34]
tugas6 - File Manager
2017-03-29 13:21

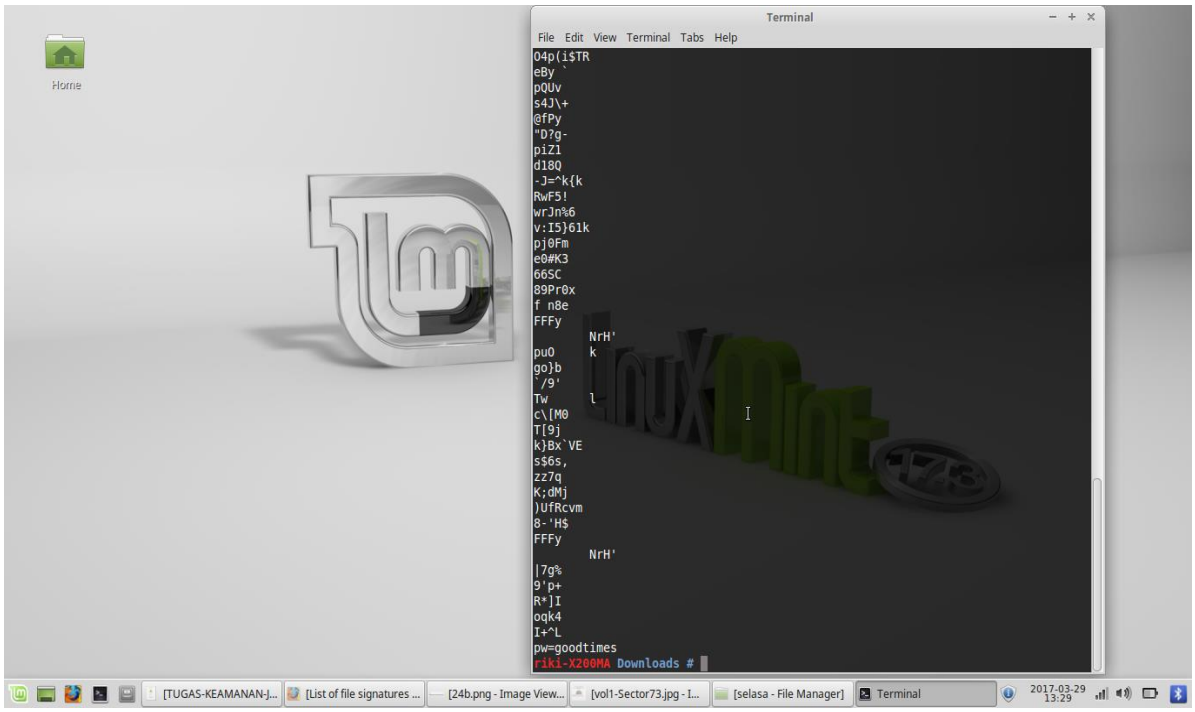

Terminal
File Edit View Terminal Tabs Help
riki@riki-X200MA ~/Downloads $ su
Password:
riki-X200MA Downloads # file vol1-Sector73.raw
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
riki-X200MA Downloads #
21.png - Image Viewer
File Edit View Go Help
Open... Save copy... Delete Edit Back Play
21.png 271 x 205 100,0%
TUGAS-KEAMANAN-JARING...
List of file signatures - Wikip...
21.png - Image Viewer [24/3...
Downloads - File Manager
Terminal
2017-03-29 13:23

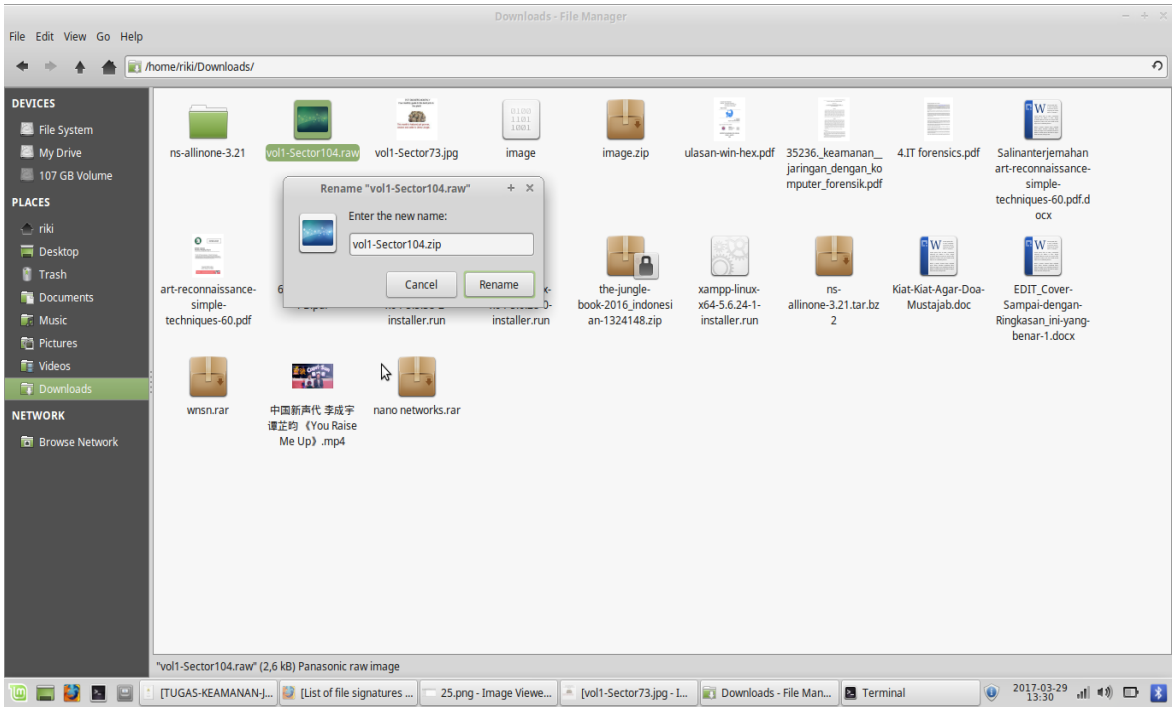

Downloads - File Manager
File Edit View Go Help
/home/riki/Downloads/
DEVICES
File System
My Drive
107 GB Volume
PLACES
riki
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
ns-allinone-3.21
vol1-Sector104.raw
vol1-Sector73.raw
image
image.zip
ulasan-win-hex.pdf
35236._keamanan__jaringan_dengan_komputer_forensik.pdf
4.IT forensics.pdf
Salinanterjemahan art-reconnaissance-simple-techniques-60.pdf.docx
art-reconnaissance-simple-techniques-60.pdf
Rename "vol1-Sector73.raw"
Enter the new name:
vol1-Sector73.jpg
Cancel
Rename
installer.run
installer.run
the-jungle-book-2016_indonesian-1324148.zip
xampp-linux-x64-5.6.24-1-installer.run
ns-allinone-3.21.tar.bz2
Kiat-Kiat-Agar-Doa-Mustajab.doc
EDIT_Cover-Sampai-dengan-Ringkasan_ini-yang-benar-1.docx
wnsn.rar
中国新声代 李成宇 谭芷昀 《You Raise Me Up》.mp4
nano networks.rar
"vol1-Sector73.raw" (15,9 kB) Panasonic raw image
TUGAS-KEAMANAN-JARING...
List of file signatures - Wikip...
21.png - Image Viewer [24/3...
Downloads - File Manager
Terminal
2017-03-29 13:25

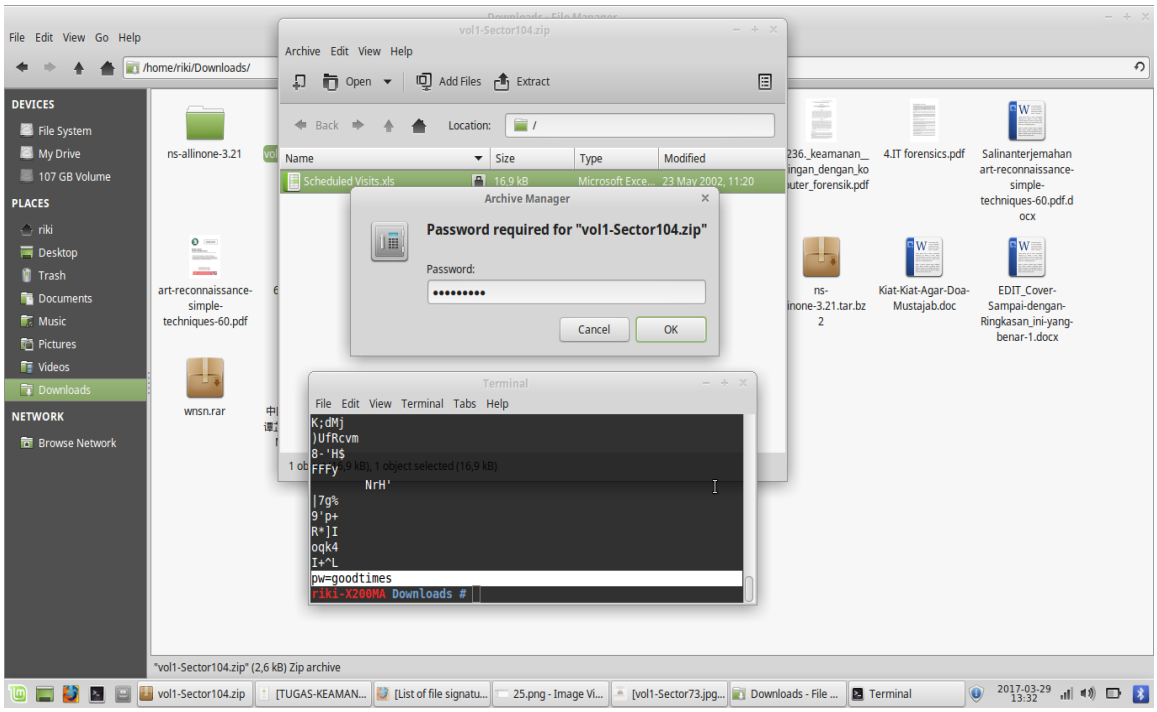

vol1-Sector73.jpg - Image Viewer
File Edit View Go Help
Open... Save copy... Delete Edit Back Play Forward Zoom In Zoom Out Normal Size Zoom Fit Fullscreen
POT SMOKERS MONTHLY
Your monthly guide to the best pot on the plant!
This month's featured pot grower, smoker and seller is Jimmy Jungle.
vol1-Sector73.jpg 208 x 199 100,0%
TUGAS-KEAMANAN-J... List of file signatures -... 21.png - Image Viewe... vol1-Sector73.jpg - Im... Downloads - File Man... Terminal
2017-03-29 13:25

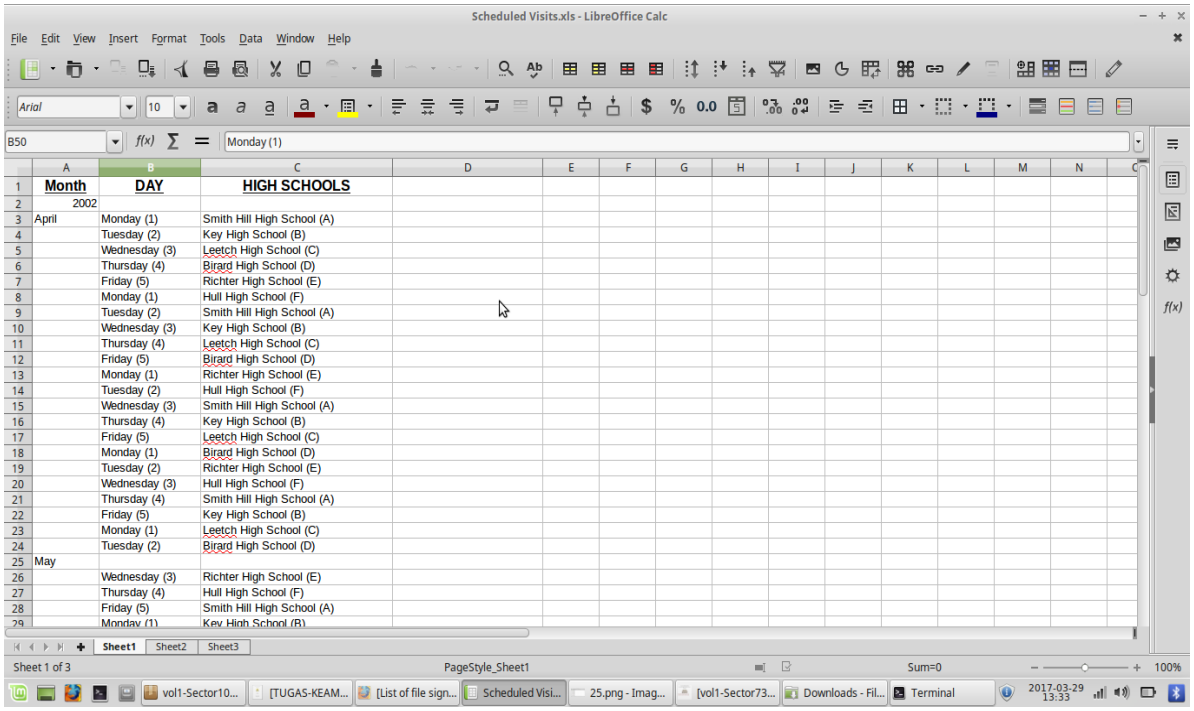

List of file signatures - Wikipedia - Mozilla Firefox
list of signature file - Linu... List of file signatures - Wi...
https://en.wikipedia.org/wiki/List_of_file_signatures
Search
Most Visited Linux Mint Community Forums Blog News
lz
lzip compressed file
0
LZIP
4C 5A 49 50
exe
DOS MZ executable file 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
https://en.wikipedia.org/wiki/JAR_(file_format)
zip
Highlight All Match Case Whole Words 4 of 9 matches
TUGAS-KEAMANAN-J... List of file signatures -... 22.png - Image Viewe... vol1-Sector73.jpg - Im... Downloads - File Man... Terminal
2017-03-29 13:27


Terminal
File Edit View Terminal Tabs Help
riki-X200MA Downloads # strings vol1-Sector73.jpg
JFIF
$.' ",#
(7),01444
'9=82<.342
!2222222222222222222222222222222222222222222222222222
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
#3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
A=2>c
KS,-
>!:>
0*x+
Eu,(
S,rF
dmYh
vR]M
1YY"
V6.|/4
*\n$
{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
Home
[TUGAS-KEAMANAN-J...
[List of file signatures ...
[24a.png - Image View...
[vol1-Sector73.jpg - I...
[selasa - File Manager]
Terminal
2017-03-29 13:29

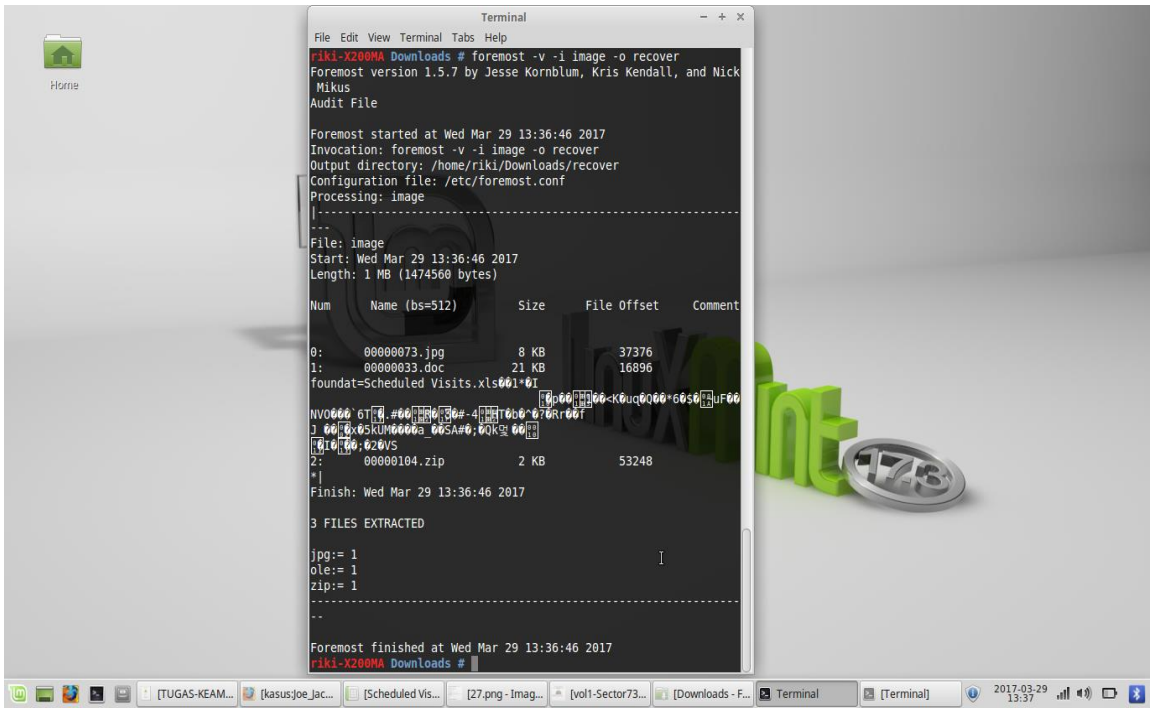

Terminal
File Edit View Terminal Tabs Help
O4p(i$TR
eBy `
pQUv
s4J\+
@fPy
"D?g-
piZ1
d18Q
-J=^k{k
RwF5!
wrJn%6
v:I5}61k
pj0Fm
e0#K3
66SC
89Pr0x
f n8e
FFFy
NrH'
puO k
go}b
`/9'
Tw l
c\[M0
T[9j
k}Bx`VE
s$6s,
zz7q
K;dMj
)UfRcvm
8-'H$
FFFy
NrH'
|7g%
9'p+
R*]I
oqk4
I+^L
pw=goodtimes
riki-X200MA Downloads #
Home
[TUGAS-KEAMANAN-J...
[List of file signatures ...
[24b.png - Image View...
[vol1-Sector73.jpg - I...
[selasa - File Manager]
Terminal
2017-03-29 13:29

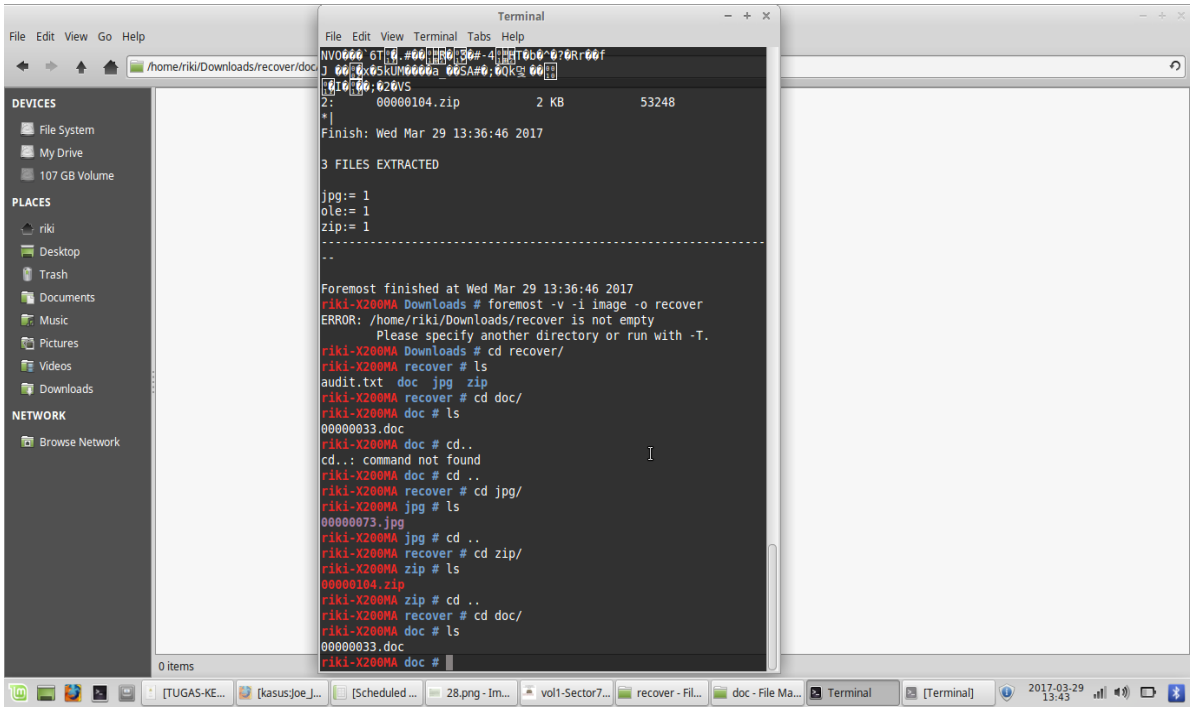

Downloads - File Manager
File Edit View Go Help
/home/riki/Downloads/
DEVICES
File System
My Drive
107 GB Volume
PLACES
riki
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
ns-allinone-3.21
vol1-Sector104.raw
vol1-Sector73.jpg
image
image.zip
ulasan-win-hex.pdf
35236._keamanan__jaringan_dengan_komputer_forensik.pdf
4.IT forensics.pdf
Salinanterjemahan art-reconnaissance-simple-techniques-60.pdf.docx
art-reconnaissance-simple-techniques-60.pdf
Rename "vol1-Sector104.raw"
Enter the new name:
vol1-Sector104.zip
Cancel
Rename
installer.run
the-jungle-book-2016_indonesian-1324148.zip
xampp-linux-x64-5.6.24-1-installer.run
ns-allinone-3.21.tar.bz2
Kiat-Kiat-Agar-Doa-Mustajab.doc
EDIT_Cover-Sampai-dengan-Ringkasan_ini-yang-benar-1.docx
wnsn.rar
中国新声代 李成宇 谭芷昀 《You Raise Me Up》.mp4
nano networks.rar
"vol1-Sector104.raw" (2,6 kB) Panasonic raw image
[TUGAS-KEAMANAN-J...
[List of file signatures ...
25.png - Image Viewe...
[vol1-Sector73.jpg - I...
Downloads - File Man...
Terminal
2017-03-29 13:30


vol1-Sector104.zip
Archive Edit View Help
Open
Add Files
Extract
Back
Location: /
Name
Size
Type
Modified
Scheduled Visits.xls
16,9 kB
Microsoft Exce...
23 May 2002, 11:20
Archive Manager
Password required for "vol1-Sector104.zip"
Password:
Cancel
OK
Terminal
File Edit View Terminal Tabs Help
K;dMj
)UfRcvm
8-'H$
FFFy
NrH'
|7g%
9'p+
R*]I
oqk4
I+^L
pw=goodtimes
riki-X200MA Downloads #
"vol1-Sector104.zip" (2,6 kB) Zip archive
vol1-Sector104.zip
[TUGAS-KEAMAN...
[List of file signatu...
25.png - Image Vi...
[vol1-Sector73.jpg...
Downloads - File ...
Terminal
2017-03-29 13:32



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





ANALISA :

Dapat dianalisa bahwa computer forensics sebagai proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud. Secara garis besar bahwa computer forensics ini untuk membantu memulihkan. Proses diatas mencari file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut. Dari percobaan yang dilakukan diatas dapat dilihat proses demi proses yang dilakukan mulai dari memasukkan alamat kasus yang menggunakan Tools :

- AutoPsy
- Foremost
- Strings
- Ghex