Dimas Wahyudi – 09011281320004 | Sistem Komputer | Fakultas Ilmu Komputer | Universitas Sriwijaya
mail.dimaswahyudi@gmail.com

Forensik Komputer

Dasar Teori : Forensik Komputer

Menurut beberapa sumber, forensik komputer adalah 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. Secara umum tujuan dari komputer forensik adalah sebagai berikut :

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.

Secara umum kebutuhan forensik komputer dapat digolongkan sebagai : keperluan investigasi tindak kriminal dan perkara pelanggaran hukum, rekonstruksi duduk perkara insiden keamanan komputer, upaya–upaya pemulihan akibat kerusakan sistem, troubleshooting yang melibatkan hardware ataupun software, Keperluan memahami sistem ataupun berbagai perangkat digital dengan lebih baik.

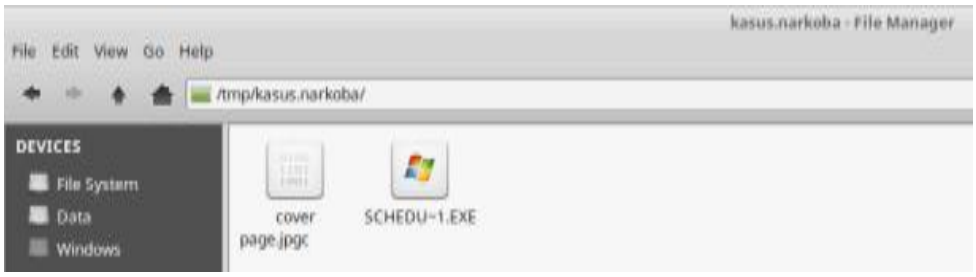
Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi. Sementara itu fokus data yang dikumpulkan dapat dikategorikan menjadi 3 (tiga) domain utama, yaitu : 1) *Active Data* : informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun *file* yang dikendalikan oleh sistem operasi. 2) *Archival Data* : 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* : informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya.

Contoh Kasus : Narkoba

“Telah tertangkap seorang pengedar narkoba kelas kakap (Joe Jacob’s), polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta bantuan oleh polisi untuk melakukan *forensic* terhadap file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut”.

Tahap : Forensik Komputer

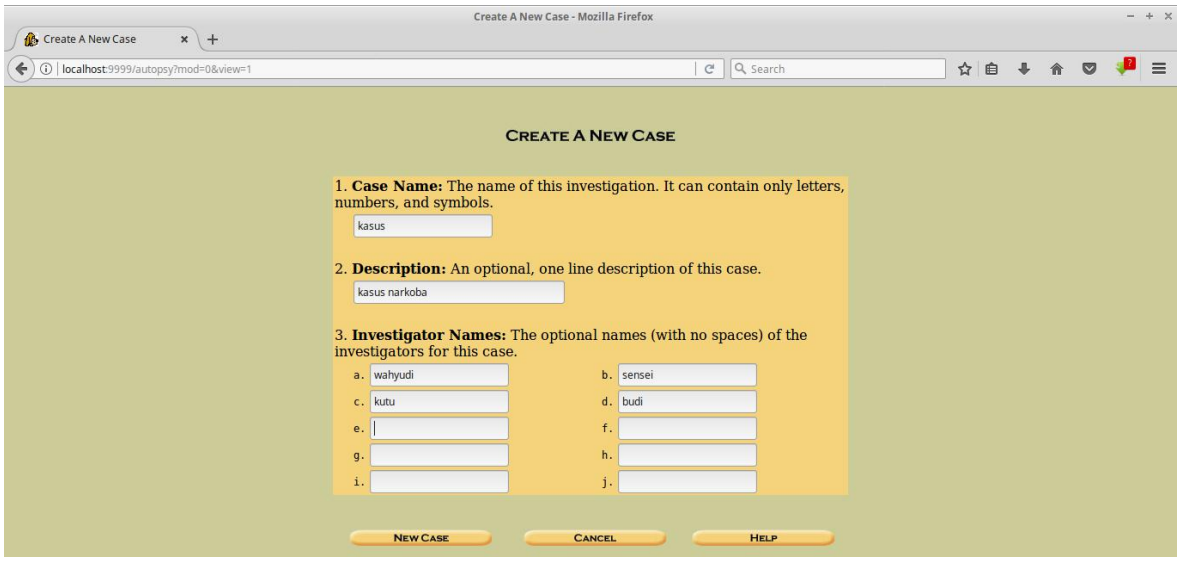
```
Terminal - root@dimaswahyudi /home/dimaswahyudi/Downloads/KJK
File  Edit  View  Terminal  Tabs  Help
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ ls
image  image.zip
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ file image
image: DOS/MBR boot sector, code offset 0x3c+2, OEM-ID "MSDOS5.0", root entries
224, sectors 2880 (volumes <=32 MB) , sectors/FAT 9, sectors/track 18, serial nu
mber 0xc4b1cdcf, unlabeled, FAT (12 bit), followed by FAT
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ mkdir /tmp/kasus.narkoba
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ sudo su
[sudo] password for dimaswahyudi:
dimaswahyudi KJK # mount image /tmp/kasus.narkoba/
dimaswahyudi KJK #
```

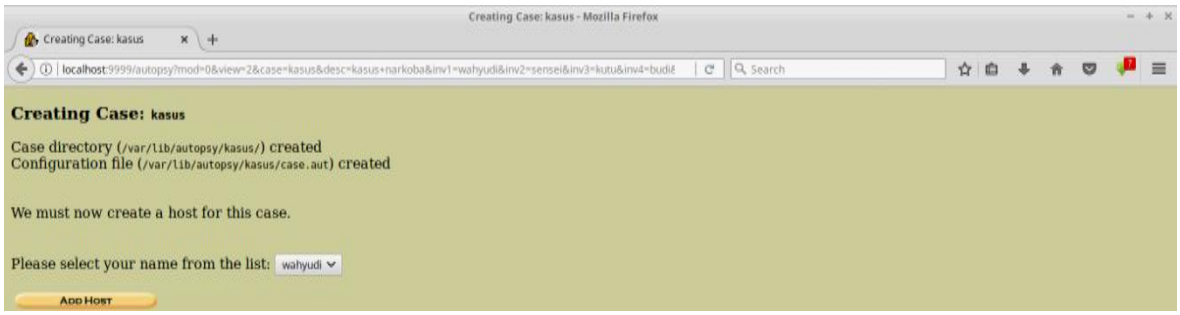


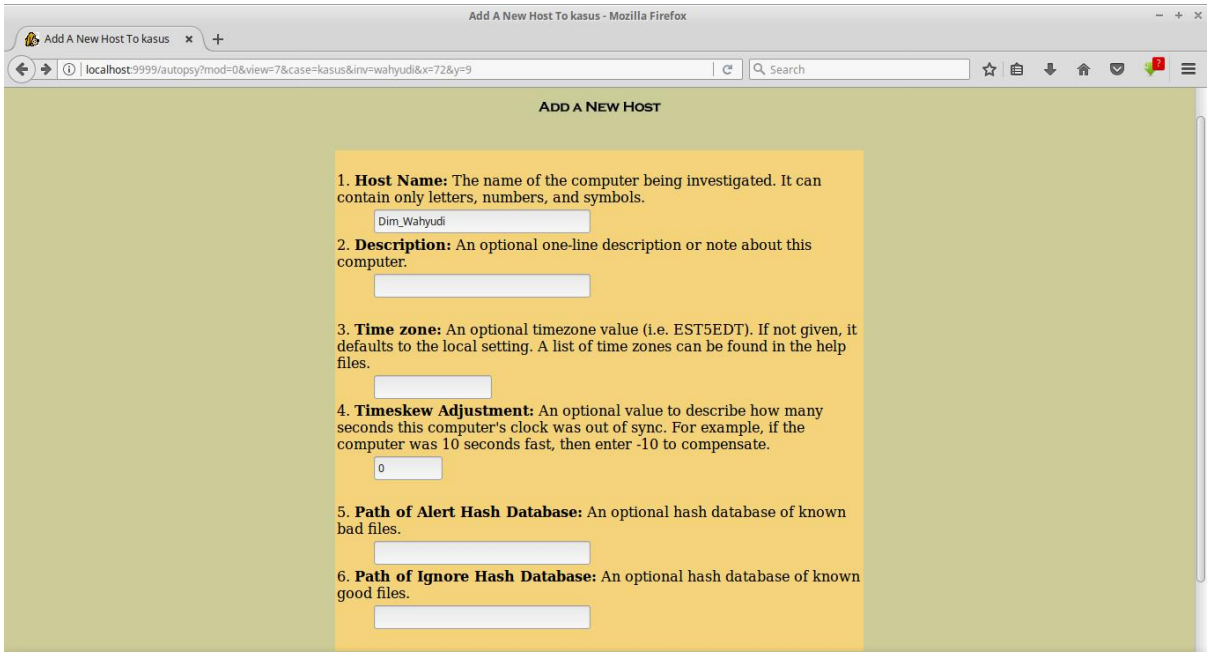

```
Terminal - root@dimaswahyudi /tmp/kasus.narkoba
File  Edit  View  Terminal  Tabs  Help
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ ls
image  image.zip
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ file image
image: DOS/MBR boot sector, code offset 0x3c+2, OEM-ID "MSDOS5.0", root entries
224, sectors 2880 (volumes <=32 MB) , sectors/FAT 9, sectors/track 18, serial nu
mber 0xc4b1cdcf, unlabeled, FAT (12 bit), followed by FAT
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ mkdir /tmp/kasus.narkoba
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ sudo su
[sudo] password for dimaswahyudi:
dimaswahyudi KJK # mount image /tmp/kasus.narkoba/
dimaswahyudi KJK # ls
image  image.zip
dimaswahyudi KJK # cd /tmp/kasus.narkoba/
dimaswahyudi kasus.narkoba # ls
cover page.jpgc              SCHEDU~1.EXE
dimaswahyudi kasus.narkoba #
```

```
Terminal - root@dimaswahyudi /tmp/kasus.narkoba
File  Edit  View  Terminal  Tabs  Help
dimaswahyudi 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
dimaswahyudi kasus.narkoba # autopsy

================================================================================

                    Autopsy Forensic Browser
                http://www.sleuthkit.org/autopsy/
                           ver 2.24

================================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Mon Mar 27 00:00:47 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
```

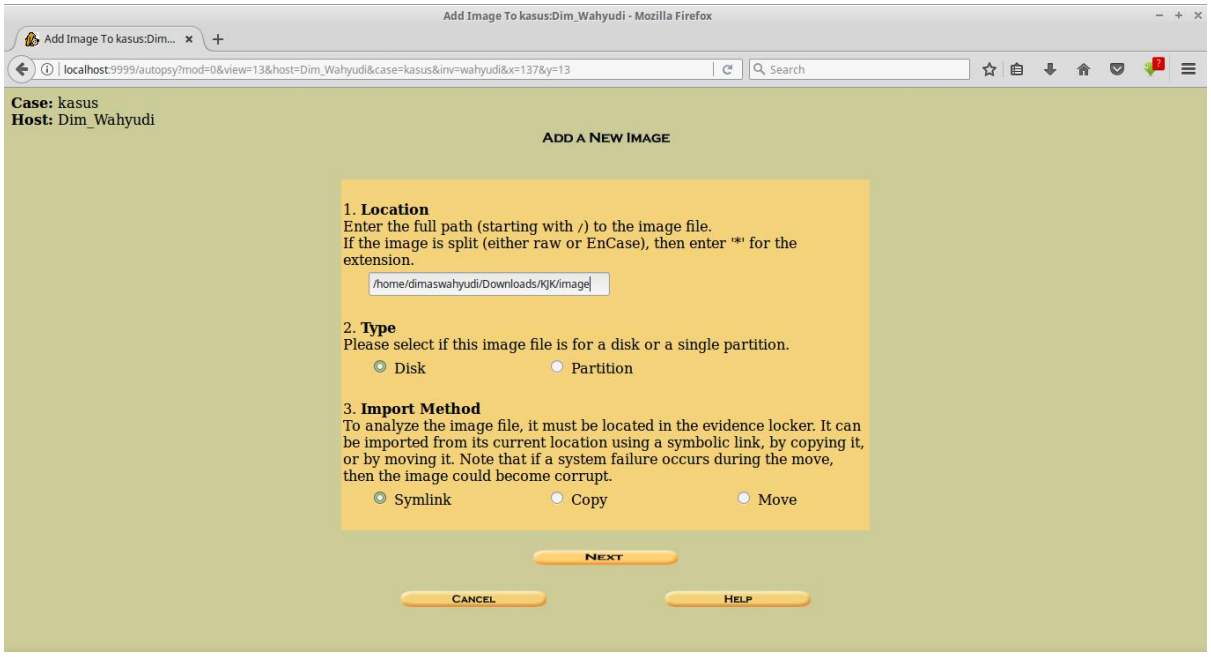
Pada tahapan diatas adalah menjalankan tools autospy. Autospy adalah sebuah antarmuka grafis untuk tool-tool di dalam Sleuth Kit, yang memudahkan pengguna dalam melakukan investigasi. Autopsy menyediakan fungsi manajemen kasus, integritas gambar, pencarian kata kunci, dan operasi lainnya. Autopsy menggunakan Perl untuk menjalankan program-program Sleuth Kit dan mengubah hasilnya ke HTML, oleh karena itu, pengguna Autopsy membutuhkan web client untuk mengakses fungsi-fungsinya. Sleuth Kit dan Autopsy memiliki banyak keunggulan, diantaranya adalah kemampuan untuk proses analisis dari berbagai jenis file sistem yang berbeda. Selain itu, karena merupakan sebuah tool open source, keduanya dapat dikembangkan sesuai dengan kebutuhan masing-masing pengguna. Pada tahap ini, kita akan melalukan forensik terhadap sebuah file gambar (*image*)



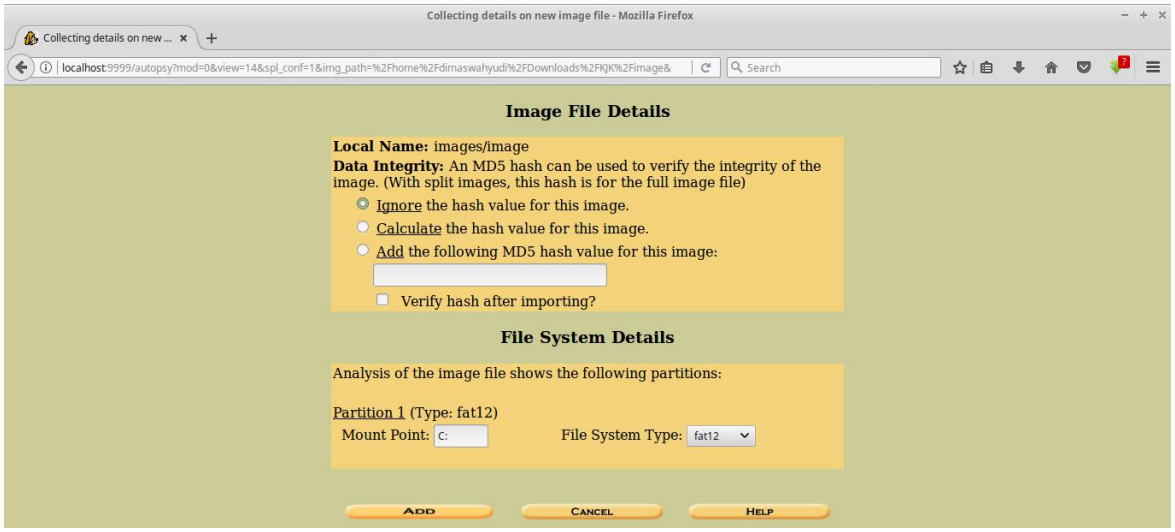


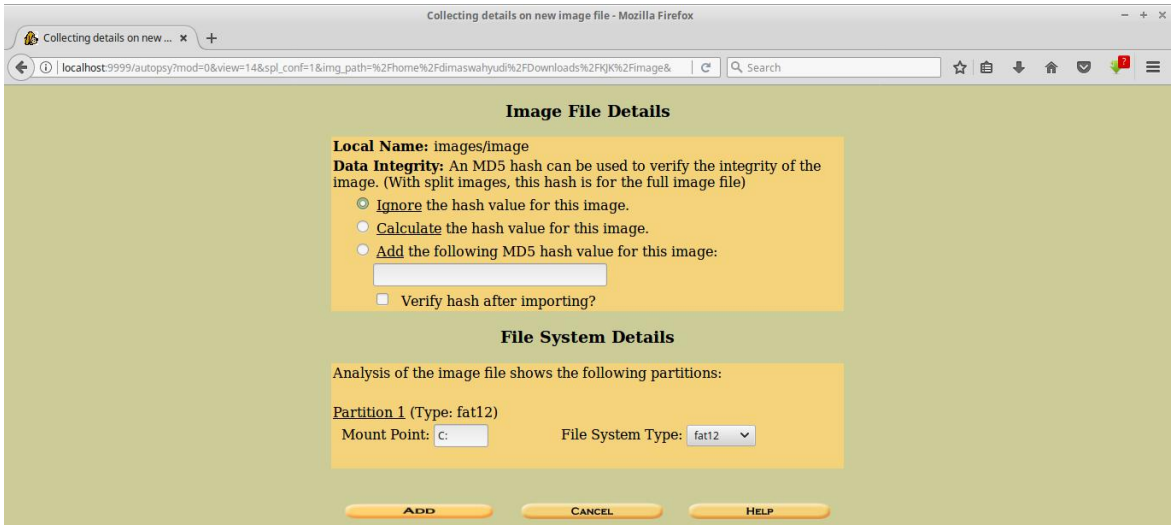

Add A New Host To kasus - Mozilla Firefox
Add A New Host To kasus
localhost:9999/autopsy?mod=0&view=7&case=kasus&inv=wahyudi&x=72&y=9
Search
ADD A NEW HOST
1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
Dim_Wahyudi
2. Description: An optional 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.


Open Image In kasus:Dim_Wahyudi - Mozilla Firefox
Open Image In kasus:Di...
localhost:9999/autopsy?mod=0&view=10&case=kasus&host=Dim_Wahyudi&inv=wahyudi
Search
Case: kasus
Host: Dim_Wahyudi
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

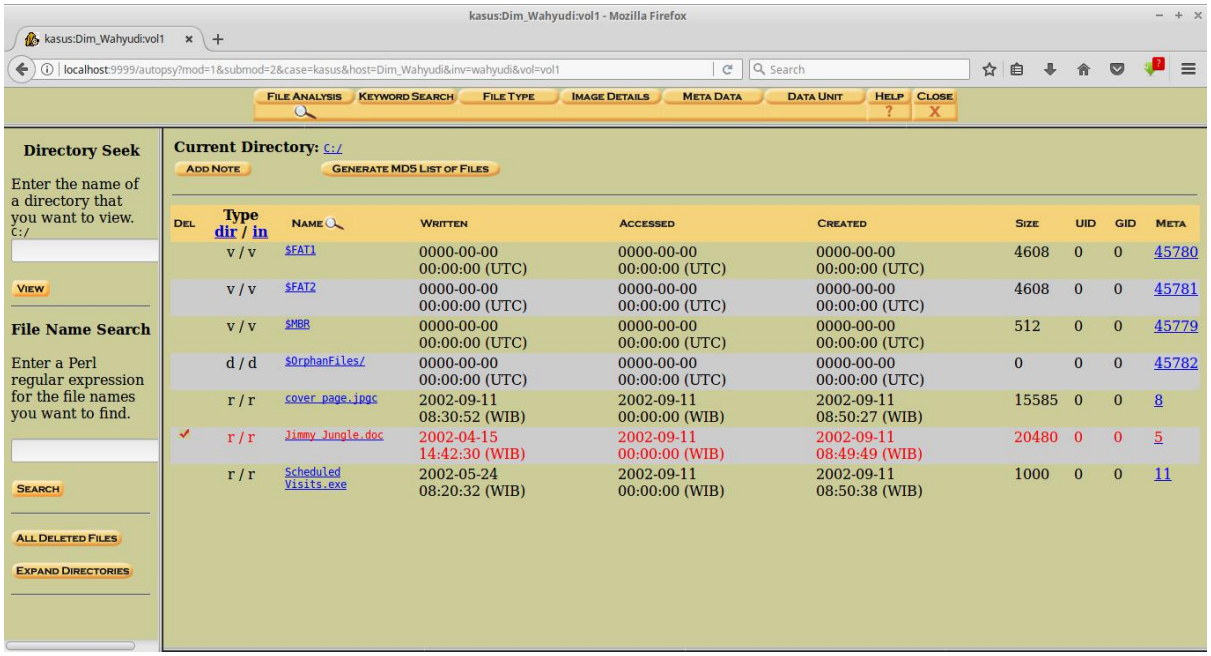

Add Image To kasus:Dim_Wahyudi - Mozilla Firefox
Add Image To kasus:Dim...
localhost:9999/autopsy?mod=0&view=13&host=Dim_Wahyudi&case=kasus&inv=wahyudi&x=137&y=13
Search
Case: kasus
Host: Dim_Wahyudi
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/dimaswahyudi/Downloads/KJK/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

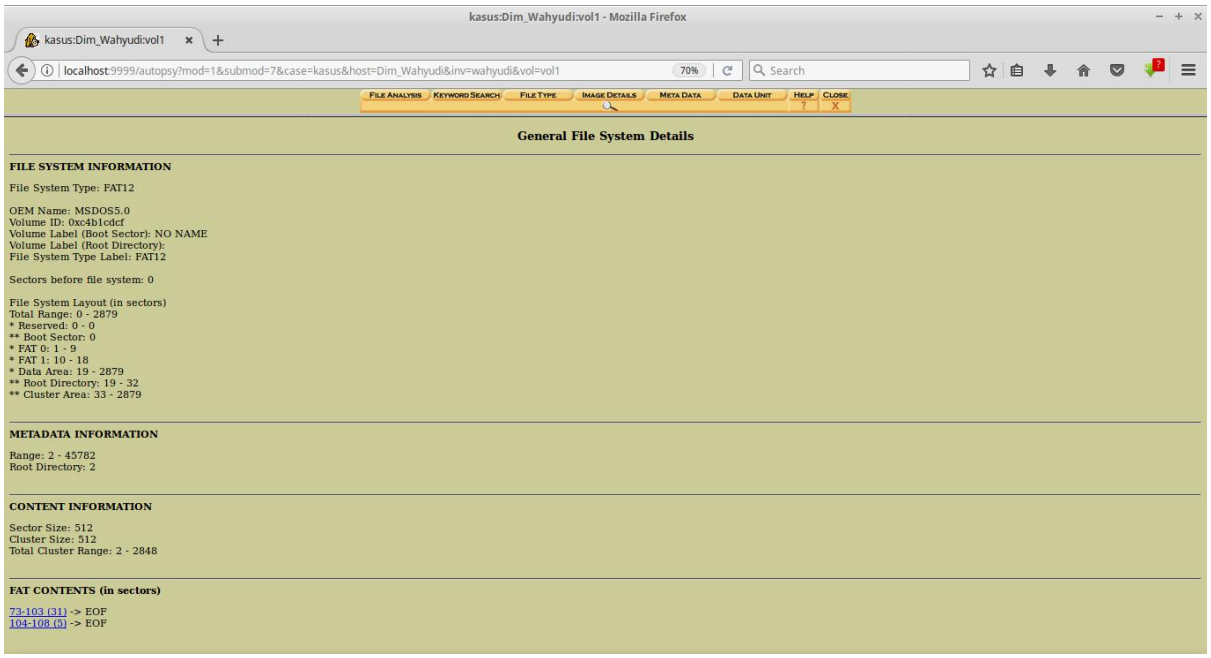

Collecting details on new image file - Mozilla Firefox
Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table).
Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.
Disk Image
Volume Image
Volume System Type (disk image only): dos
OK

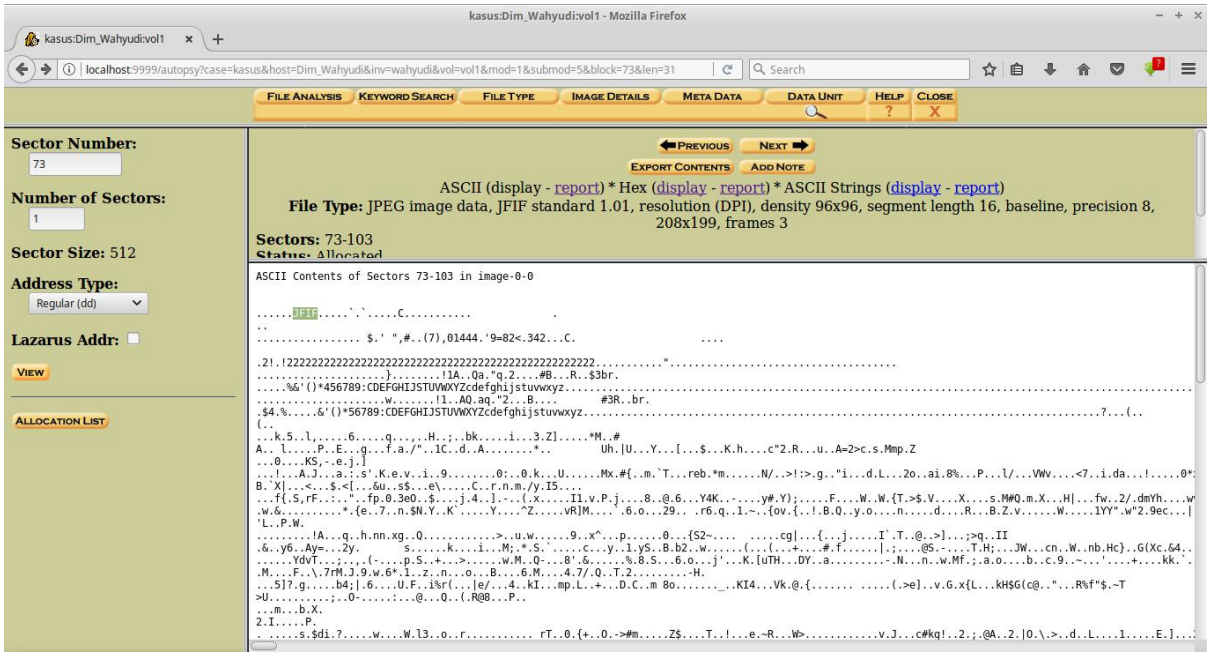

Collecting details on new image file - Mozilla Firefox
Image File Details
Local Name: images/image
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for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

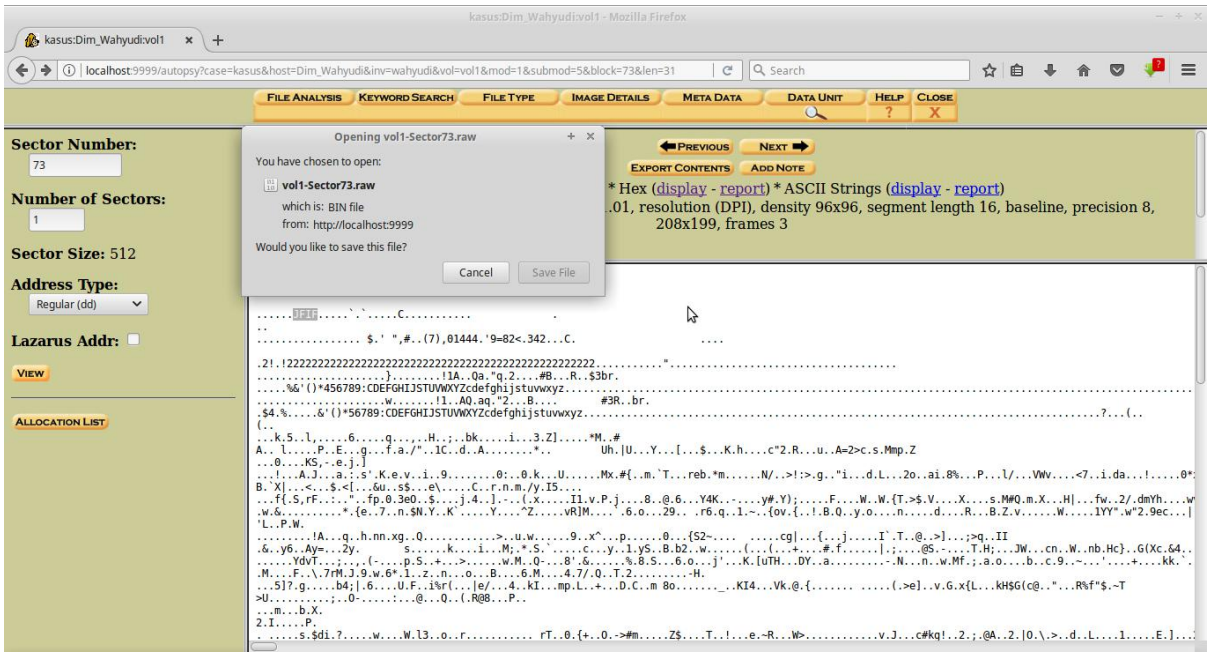

Collecting details on new image file - Mozilla Firefox
Image File Details
Local Name: images/image
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for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

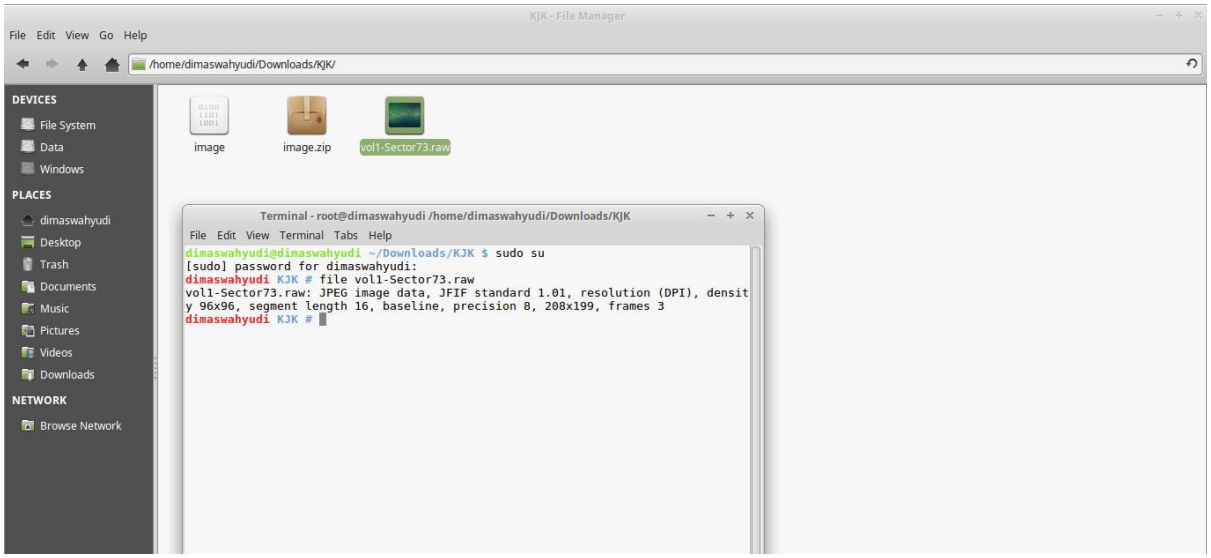

Open Image In kasus:Dim_Wahyudi - Mozilla Firefox
Case: kasus
Host: Dim_Wahyudi
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
image-0-0
fat12
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER

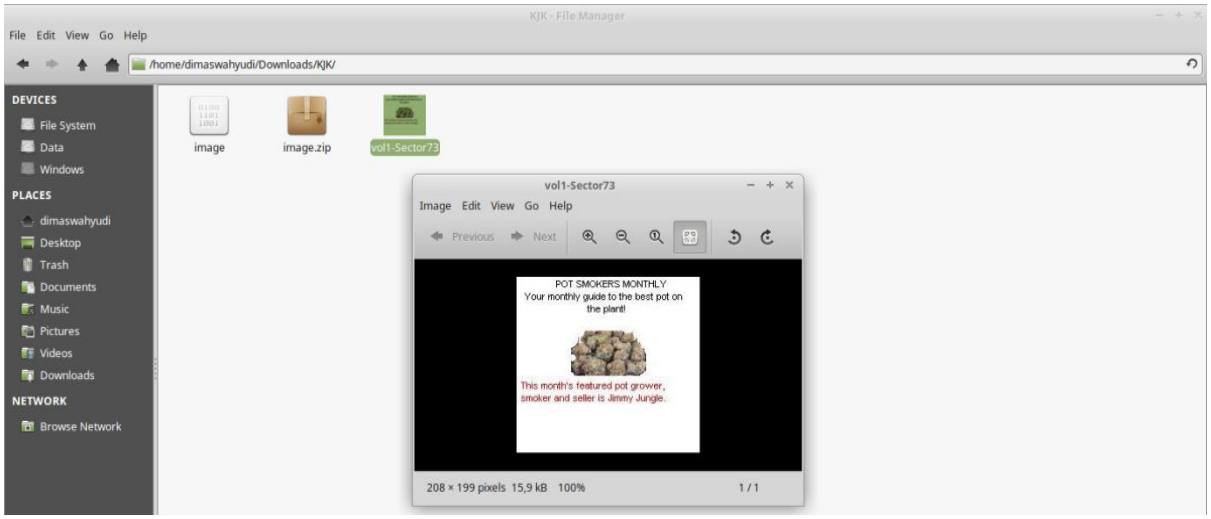

kasus:Dim_Wahyudi:vol1 - Mozilla Firefox
kasus:Dim_Wahyudi:vol1
localhost:9999/autopsy?mod=1&submod=2&case=kasus&host=Dim_Wahyudi&inv=wahyudi&vol=vol1
Search
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Directory Seek
Enter the name of a directory that you want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

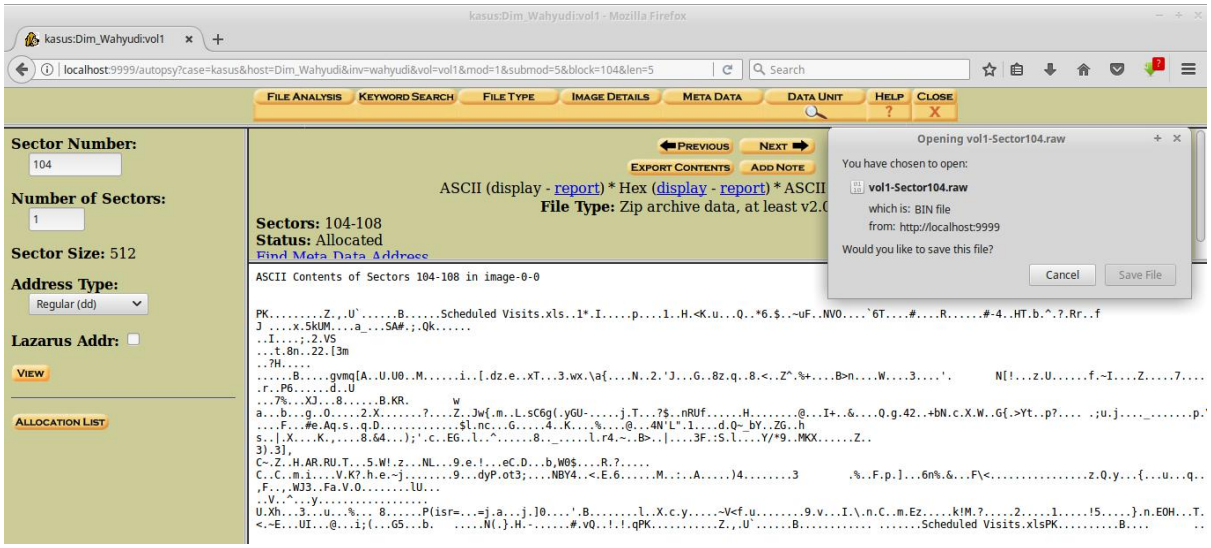

kasus:Dim_Wahyudi:vol1 - Mozilla Firefox
kasus:Dim_Wahyudi:vol1
localhost:9999/autopsy?mod=1&submod=7&case=kasus&host=Dim_Wahyudi&inv=wahyudi&vol=vol1
70%
Search
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
General File System Details
FILE SYSTEM INFORMATION
File 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
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

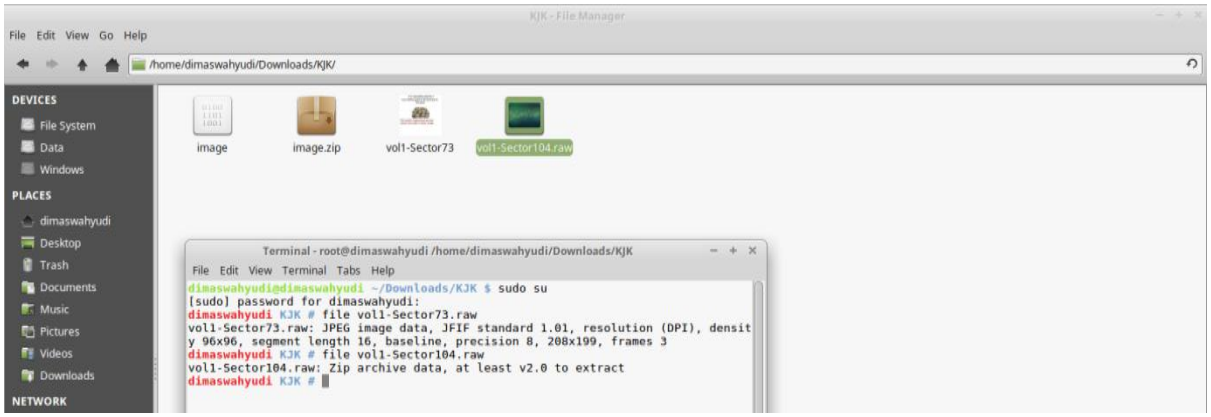

kasus:Dim_Wahyudi:vol1 - Mozilla Firefox
kasus:Dim_Wahyudi:vol1
localhost:9999/autopsy?case=kasus&host=Dim_Wahyudi&inv=wahyudi&vol=vol1&mod=1&submod=5&block=73&len=31
Search
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Sector Number:
73
Number of Sectors:
1
Sector 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, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 208x199, frames 3
Sectors: 73-103
Status: Allocated
ASCII Contents of Sectors 73-103 in image-0-0

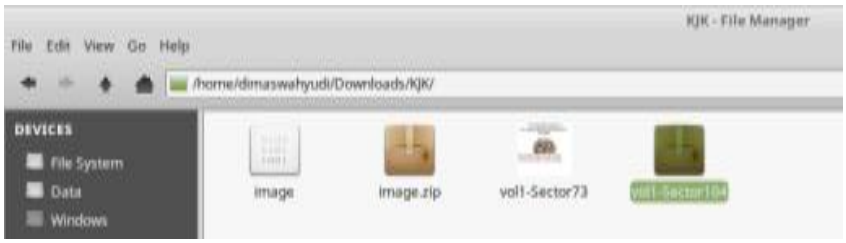

Opening vol1-Sector73.raw
You have chosen to open:
vol1-Sector73.raw
which is: BIN file
from: http://localhost:9999
Would you like to save this file?
Cancel
Save File


KJK - File Manager
File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
image
image.zip
vol1-Sector73.raw
Terminal - root@dimaswahyudi /home/dimaswahyudi/Downloads/KJK
File Edit View Terminal Tabs Help
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ sudo su
[sudo] password for dimaswahyudi:
dimaswahyudi KJK # file vol1-Sector73.raw
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01, resolution (DPI), densit
y 96x96, segment length 16, baseline, precision 8, 208x199, frames 3
dimaswahyudi KJK #

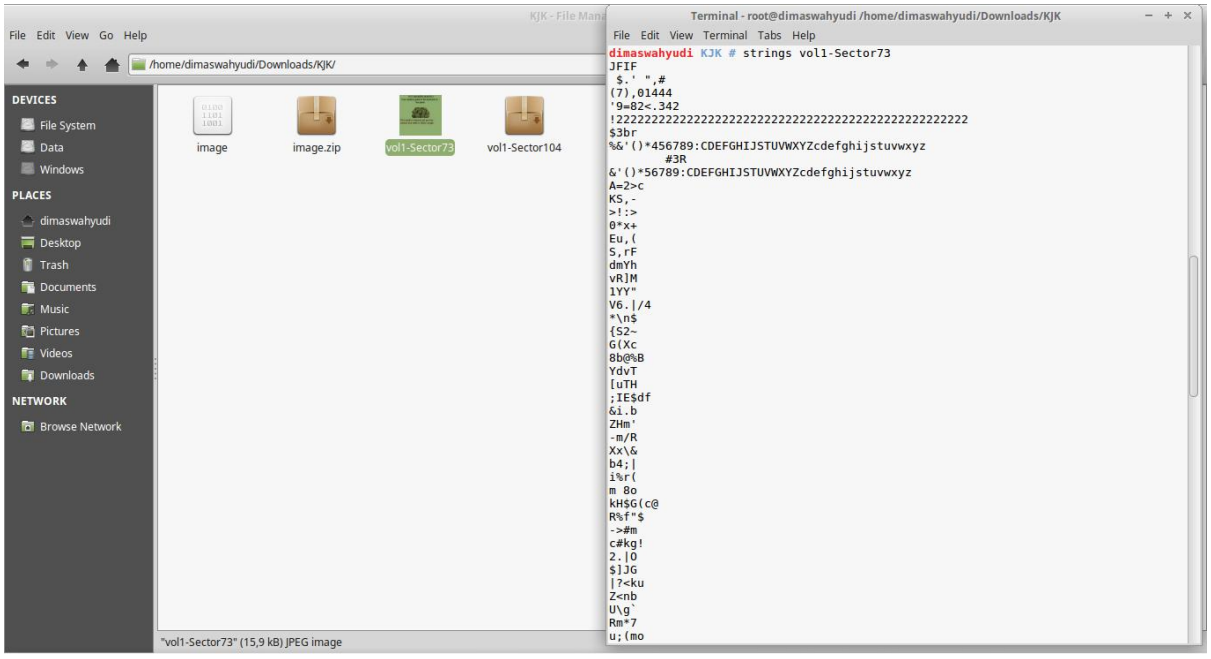

KJK - File Manager
File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
image
image.zip
vol1-Sector73
vol1-Sector73
Image Edit View Go Help
Previous
Next
POT SMOKERS MONTHLY
Your monthly guide to the best pot on the planet!
This month's featured pot grower, smoker and seller is Jimmy Jungle.
208 × 199 pixels 15,9 kB 100%
1 / 1

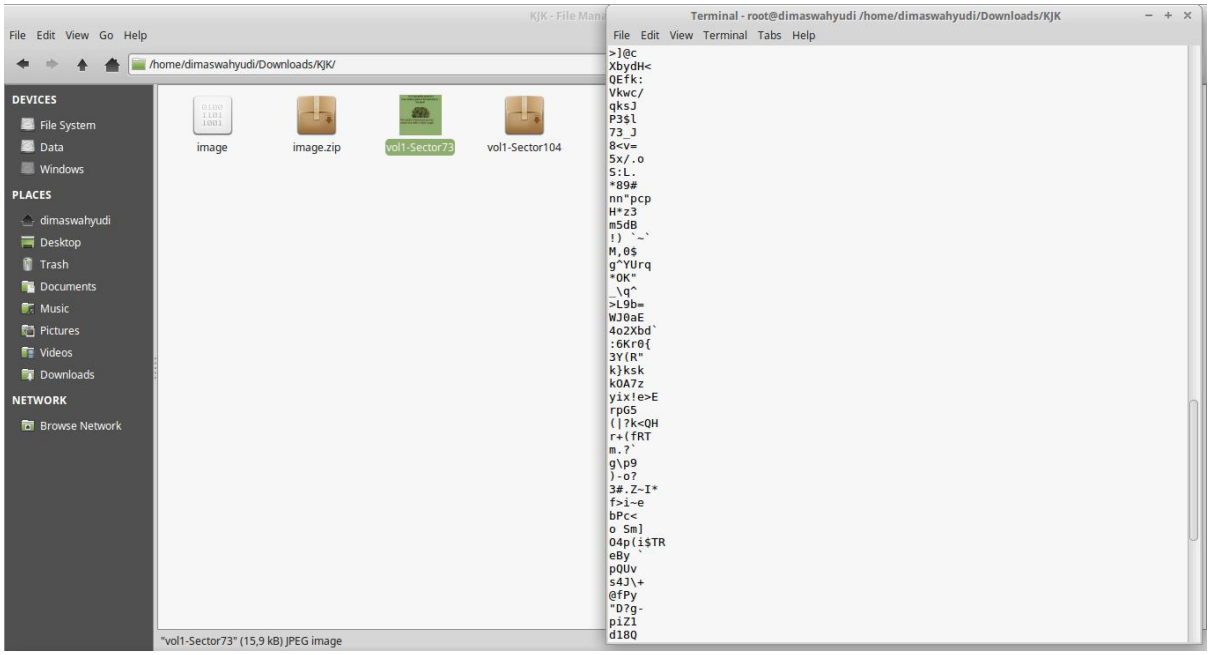

kasus:Dim_Wahyudi:vol1 - Mozilla Firefox
kasus:Dim_Wahyudi:vol1
localhost:9999/autopsy?case=kasus&host=Dim_Wahyudi&inv=wahyudi&vol=vol1&mod=1&submod=5&block=104&len=5
Search
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Sector Number:
104
Number of Sectors:
1
Sector Size: 512
Address Type:
Regular (dd)
Lazarus Addr:
VIEW
ALLOCATION LIST
PREVIOUS
NEXT
EXPORT CONTENTS
ADD NOTE
ASCII (display - report) * Hex (display - report) * ASCII
File Type: Zip archive data, at least v2.0
Sectors: 104-108
Status: Allocated
Find Meta Data Address
ASCII Contents of Sectors 104-108 in image-0-0
Opening vol1-Sector104.raw
You have chosen to open:
vol1-Sector104.raw
which is: BIN file
from: http://localhost:9999
Would you like to save this file?
Cancel
Save File

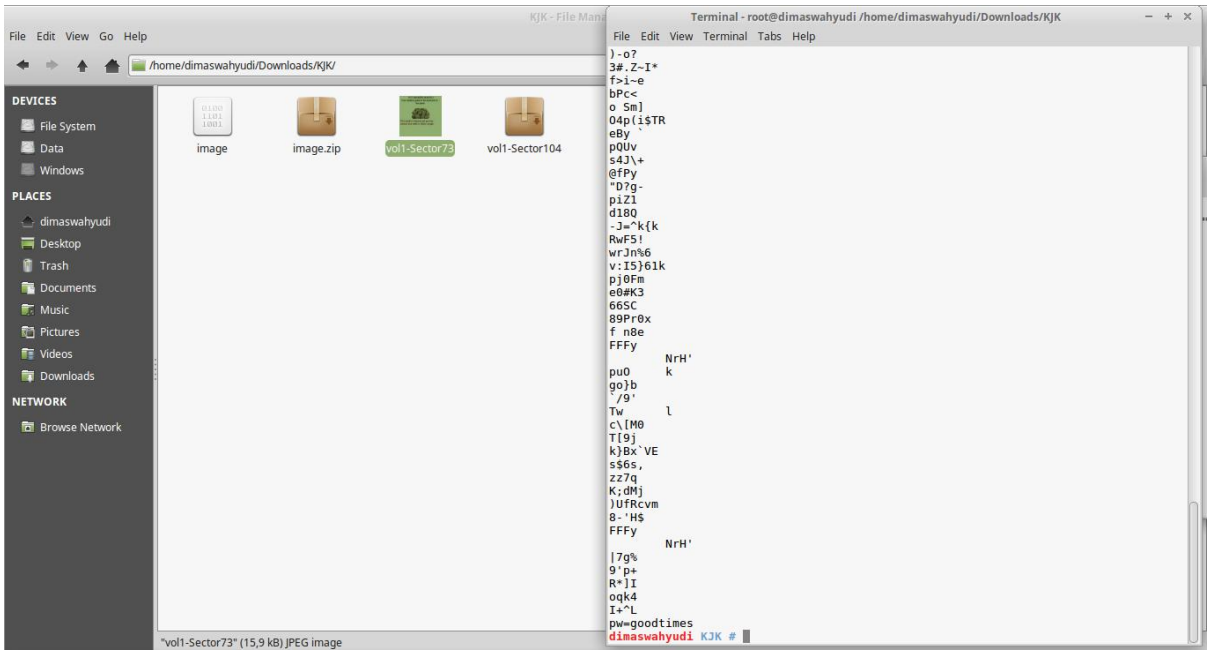

KJK - File Manager
File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
image
image.zip
vol1-Sector73
vol1-Sector104.raw
Terminal - root@dimaswahyudi /home/dimaswahyudi/Downloads/KJK
File Edit View Terminal Tabs Help
dimaswahyudi@dimaswahyudi ~/Downloads/KJK $ sudo su
[sudo] password for dimaswahyudi:
dimaswahyudi KJK # file vol1-Sector73.raw
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01, resolution (DPI), densit
y 96x96, segment length 16, baseline, precision 8, 208x199, frames 3
dimaswahyudi KJK # file vol1-Sector104.raw
vol1-Sector104.raw: Zip archive data, at least v2.0 to extract
dimaswahyudi KJK #

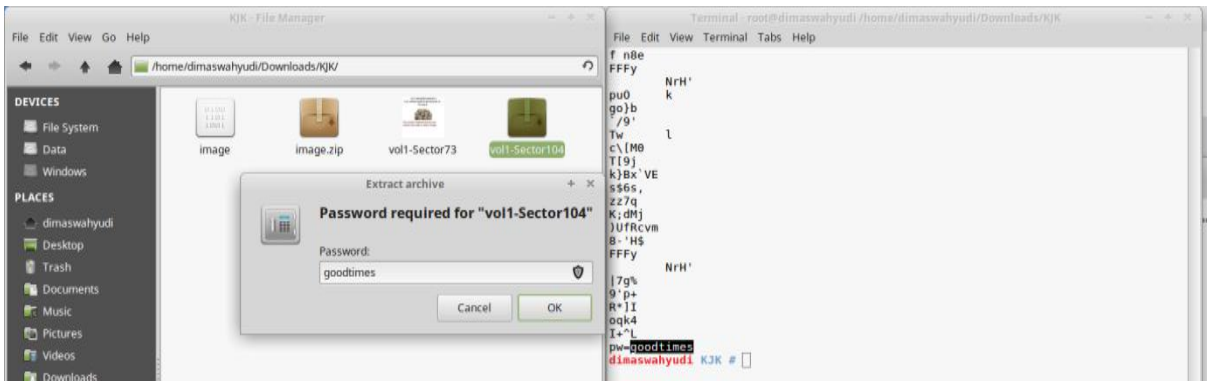

KJK - File Manager
File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
image
image.zip
vol1-Sector73
vol1-Sector104

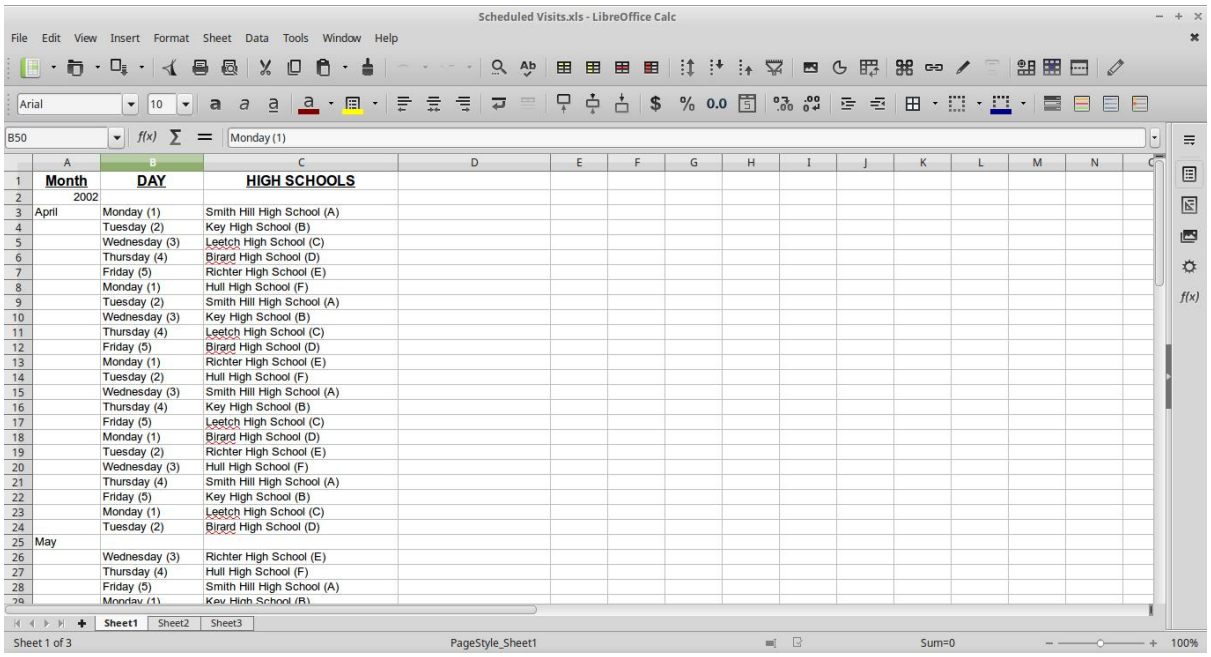

KJK - File Manager
File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
image
image.zip
vol1-Sector73
vol1-Sector104
Extract archive
Password required for "vol1-Sector104"
Password:
Cancel
OK


File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
image
image.zip
vol1-Sector73
vol1-Sector104
"vol1-Sector73" (15,9 kB) JPEG image
Terminal - root@dimaswahyudi /home/dimaswahyudi/Downloads/KJK
File Edit View Terminal Tabs Help
dimaswahyudi KJK # strings vol1-Sector73
JFIF
$.' ",#
(7),01444
'9=82<.342
!2222222222222222222222222222222222222222222222
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
#3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
A=2>c
KS,-
>!:>
0*x+
Eu,(
S,rF
dmYh
vR]M
1YY"
V6.|/4
*\n$
{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.|0
$]JG
|?<ku
Z<nb
U\g`
Rm*7
u;(mo

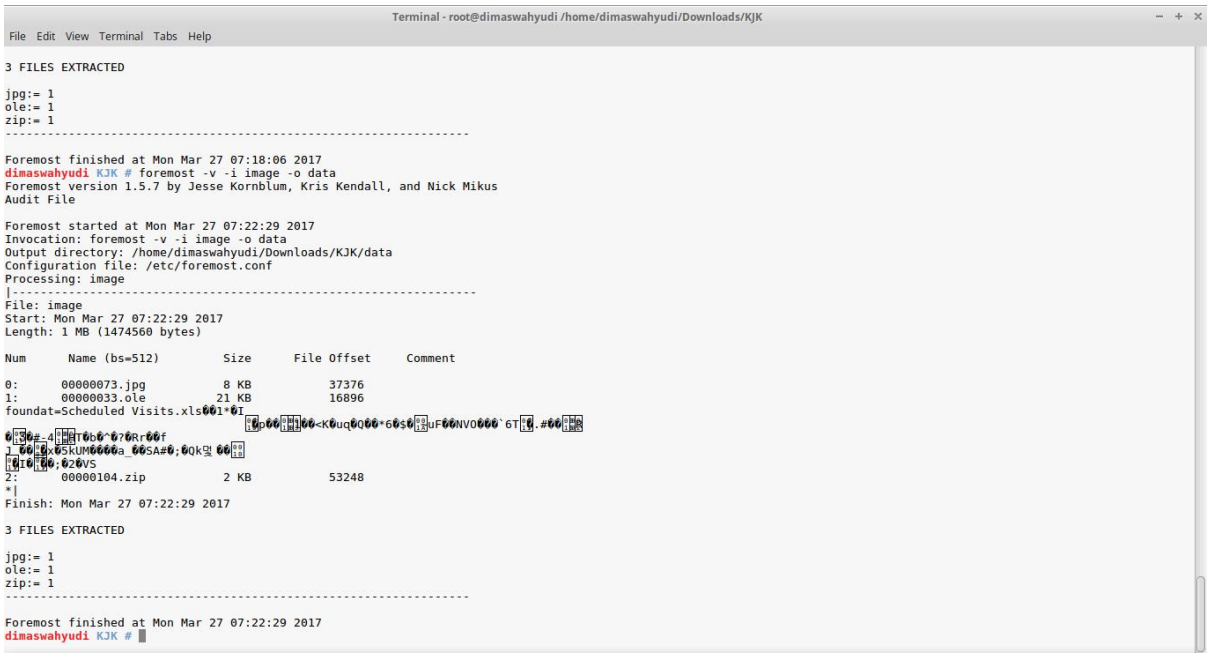

File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
image
image.zip
vol1-Sector73
vol1-Sector104
"vol1-Sector73" (15,9 kB) JPEG image
Terminal - root@dimaswahyudi /home/dimaswahyudi/Downloads/KJK
File Edit View Terminal Tabs Help


File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
image
image.zip
vol1-Sector73
vol1-Sector104
"vol1-Sector73" (15,9 kB) JPEG image
Terminal - root@dimaswahyudi /home/dimaswahyudi/Downloads/KJK
File Edit View Terminal Tabs Help
pw=goodtimes
dimaswahyudi KJK #

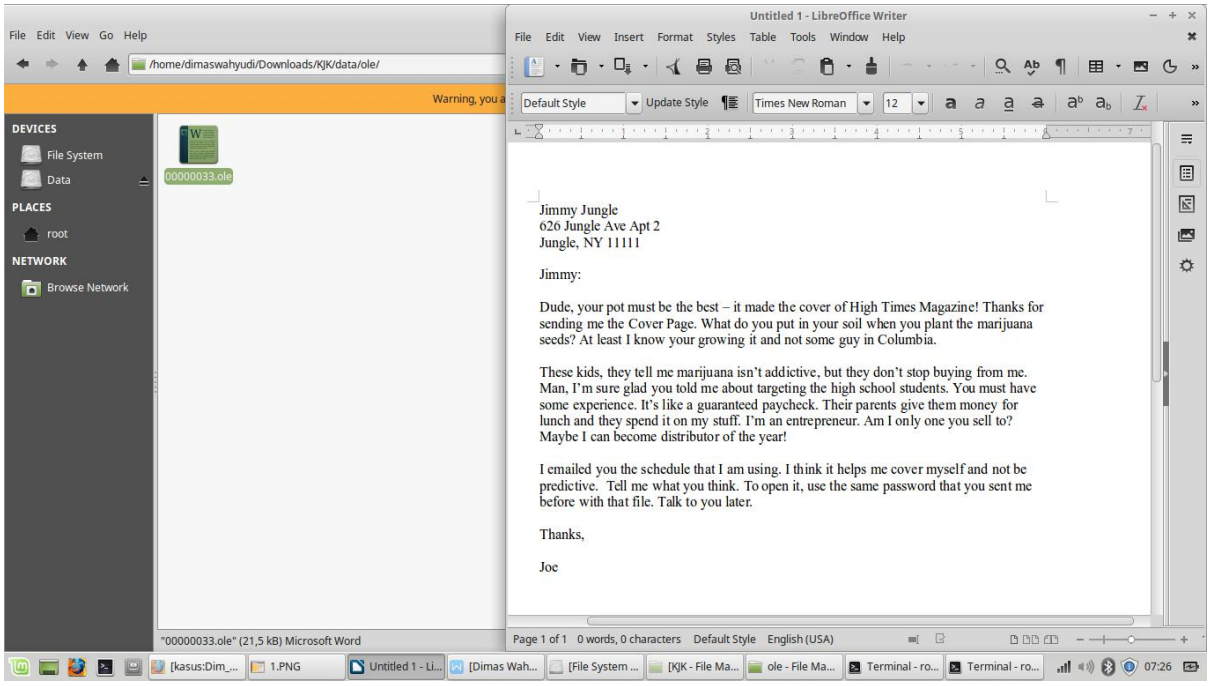

File Edit View Go Help
/home/dimaswahyudi/Downloads/KJK/
DEVICES
File System
Data
Windows
PLACES
dimaswahyudi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
image
image.zip
vol1-Sector73
vol1-Sector104
Extract archive
Password required for "vol1-Sector104"
Password:
goodtimes
Cancel
OK
Terminal - root@dimaswahyudi /home/dimaswahyudi/Downloads/KJK
File Edit View Terminal Tabs Help
pw=goodtimes
dimaswahyudi KJK #



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)



Pada tahapan ini, kita menggunakan tools foremost. Foremost adalah ebuah tool yang dapat digunakan untuk me-recover file berdasarkan header, footer, atau struktur data file (image) tersebut.



Dalam dunia kriminal dikenal istilah "tidak ada kejahatan yang tidak meninggalkan jejak". Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Dalam hal ini terbukti bahwa kegiatan diatas merupakan informasi yang didapat melalui serangkaian kegiatan foreksi komputer.

Daftar Pustaka

[1] A. H. Abdullah, "Cyber-Attack Penetration Test and Vulnerability Analysis," vol. 13, no. 1, pp. 125–132.

[2] I. C. of E.-C. C. (EC-Council), "Footprinting and Reconnaissance," *Certif. Ethical Hacker V8.00*.

[3] R. E. Indrajit, "Forensik Komputer," *Artikel*, vol. 1, no. C, pp. 1–11, 2011.