Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

COMPUTER FORENSICS

Computer Forensic 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.

- **Tujuan dan Fokus Computer Forensic**

Selaras dengan definisinya, secara prinsip ada tujuan utama dari aktivitas forensik komputer, yaitu :

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.

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 – 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.

- **Manfaat dan Tantangan Computer Forensic**

Memiliki kemampuan dalam melakukan forensik komputer akan mendatangkan sejumlah manfaat, antara lain :

1. Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan.
2. Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir.
3. Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer.
4. Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Terlepas dari manfaat tersebut, teramat banyak tantangan dalam dunia forensik komputer, terutama terkait dengan sejumlah aspek sebagai berikut :

1. Forensik komputer merupakan ilmu yang relatif baru, sehingga “Body of Knowledge”-nya masih sedemikian terbatas (dalam proses pencarian dengan metode “learning by doing”).
2. Walaupun berada dalam rumpun ilmu forensik, namun secara prinsip memiliki sejumlah karakteristik yang sangat berbeda dengan bidang ilmu forensik lainnya – sehingga sumber ilmu dari individu maupun pusat studi sangatlah sedikit.
3. Perkembangan teknologi yang sedemikian cepat, yang ditandai dengan diperkenalkannya produk-produk baru dimana secara langsung berdampak pada berkembangnya ilmu forensik komputer tesebut secara pesat, yang membutuhkan kompetensi pengetahuan dan keterampilan sejalan dengannya.
4. Semakin pintar dan trampilnya para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang.

5. Cukup mahalnya harga peralatan canggih dan termutakhir untuk membantu proses forensik komputer beserta laboratorium dan SDM pendukungnya.
6. Secara empiris, masih banyak bersifat studi kasus (happening arts) dibandingkan dengan metodologi pengetahuan yang telah dibakukan dimana masih sedikit pelatihan dan sertifikasi yang tersedia dan ditawarkan di masyarakat.
7. Sangat terbatasnya SDM pendukung yang memiliki kompetensi dan keahlian khusus di bidang forensik komputer.
8. Pada kenyataannya, pekerjaan forensik komputer masih lebih banyak unsur seninya dibandingkan pengetahuannya (more "Art" than "Science").

- **Objek Forensik**

1. Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem.
2. File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu.
3. Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System).
4. Hard disk yang berisi data/informasi backup dari sistem utama.
5. Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya.
6. Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain).
7. Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya).

- **Tahapan Aktivitas Forensik**

Secara metodologis, terdapat paling tidak 14 (empat belas) tahapan yang perlu dilakukan dalam aktivitas forensik, sebagai berikut :

1. Pernyataan Terjadinya Kejahatan Komputer – merupakan tahap dimana secara formal pihak yang berkepentingan melaporkan telah terjadinya suatu aktivitas kejahatan berbasis komputer.
2. Pengumpulan Petunjuk atau Bukti Awal – merupakan tahap dimana ahli forensik mengumpulkan semua petunjuk atau bukti awal yang dapat dipergunakan sebagai bahan kajian forensik, baik yang bersifat tangible maupun intangible.

3. Penerbitan Surat Pengadilan – merupakan tahap dimana sesuai dengan peraturan dan perundang-undangan yang berlaku, pihak pengadilan memberikan ijin resmi kepada penyelidik maupun penyidik untuk melakukan aktiivitas terkait dengan pengolahan tempat kejadian perkara, baik yang bersifat fisik maupun maya.
4. Pelaksanaan Prosedur Tanggapan Dini – merupakan tahap dimana ahli forensik melakukan serangkaian prosedur pengamanan tempat kejadian perkara, baik fisik maupun maya, agar steril dan tidak tercemar/terkontaminasi, sehingga dapat dianggap sah dalam pencarian barang-barang bukti.
5. Pembekuan Barang Bukti pada Lokasi Kejahatan – merupakan tahap dimana seluruh barang bukti yang ada diambil, disita, dan/atau dibekukan melalui teknik formal tertentu.
6. Pemindahan Bukti ke Laboratorium Forensik – merupakan tahap dimana dilakukan transfer barang bukti dari tempat kejadian perkara ke laboratorium tempat dilakukannya analisa forensik.
7. Pembuatan Salinan "2 Bit Stream" terhadap Barang Bukti – merupakan tahap dimana dilakukan proses duplikasi barang bukti ke dalam bentuk salinan yang identik.
8. Pengembangan "MD5 Checksum" Barang Bukti – merupakan tahap untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada.
9. Penyiapan Rantai Posesi Barang Bukti – merupakan tahap menentukan pengalihan tanggung jawab dan kepemilikan barang bukti asli maupun duplikasi dari satu wilayah otoritas ke yang lainnya.
10. Penyimpanan Barang Bukti Asli di Tempat Aman – merupakan tahap penyimpanan barang bukti asli (original) di tempat yang aman dan sesuai dengan persyaratan teknis tertentu untuk menjaga keasliannya.
11. Analisa Barang Bukti Salinan – merupakan tahap dimana ahli forensik melakukan analisa secara detail terhadap salinan barang-brang bukti yang dikumpulkan untuk mendapatkan kesimpulan terkait dengan seluk beluk terjadinya kejahatan.
12. Pembuatan Laporan Forensik – merupakan tahap dimana ahli forensik menyimpulkan secara detail hal-hal yang terjadi seputar aktivititas kejahatan yang dianalisa berdasarkan fakta forensik yang ada.
13. Penyerahan Hasil Laporan Analisa – merupakan tahap dimana secara resmi dokumen rahasia hasil forensik komputer diserahkan kepada pihak yang berwajib.
14. Penyertaan dalam Proses Pengadilan – merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi.

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

KASUS

Telah tertangkap seorang pengedar narkoba kelas kakap, 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.

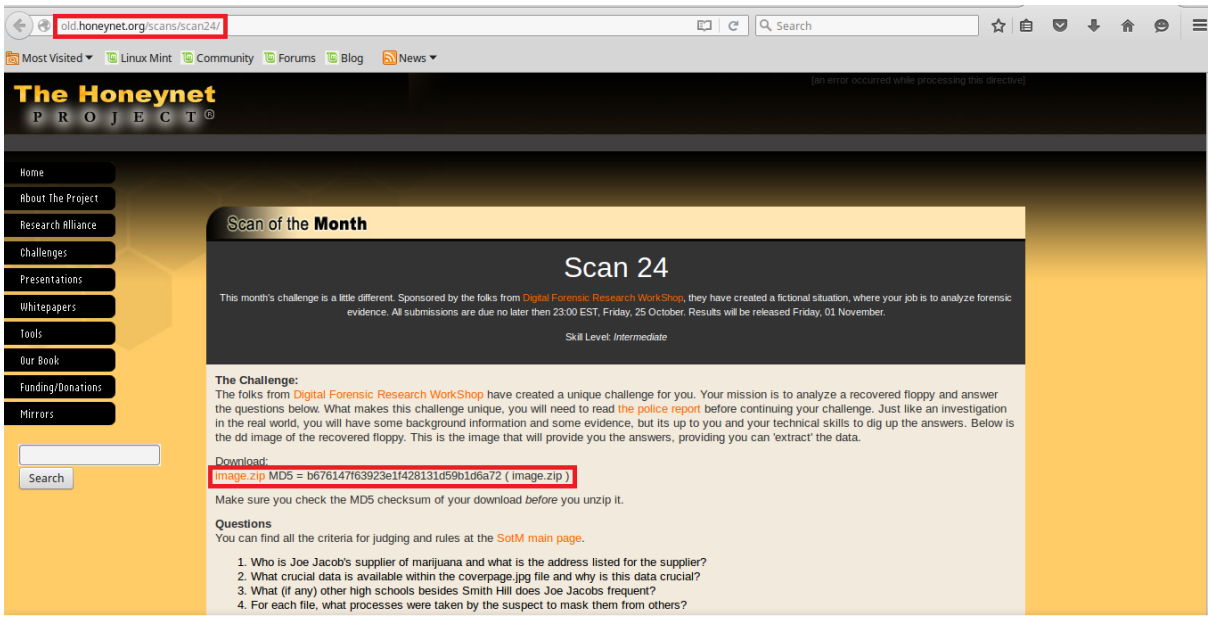
Kita di minta bantuan untuk mendapatkan beberapa informasi di bawah ini :

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?

Tools yang digunakan untuk mendapatkan beberapa informasi yang diinginkan di atas:

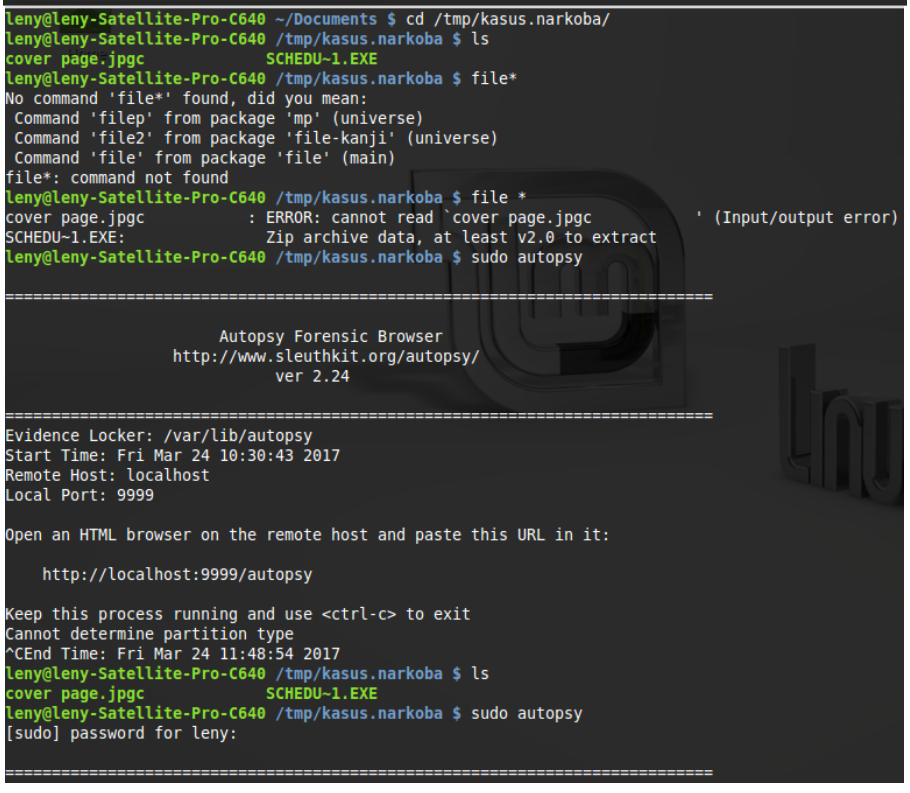
- Autopsy
- Foremost
- Strings (*tidak perlu di install karena telah tersedia strings default pada linux/ubuntu)
- Ghex

Download file Image.zip pada situs (old.honeynet.org/scans/scan24/image.zip) dengan md5 : b676147f63923e1f428131d59b1d6a72 untuk memastikan bahwa file yang telah di download adalah file yang asli maka gunakan opsion : `md5ceksum image.zip` pada terminal dan samakan dengan md5 file diatas.



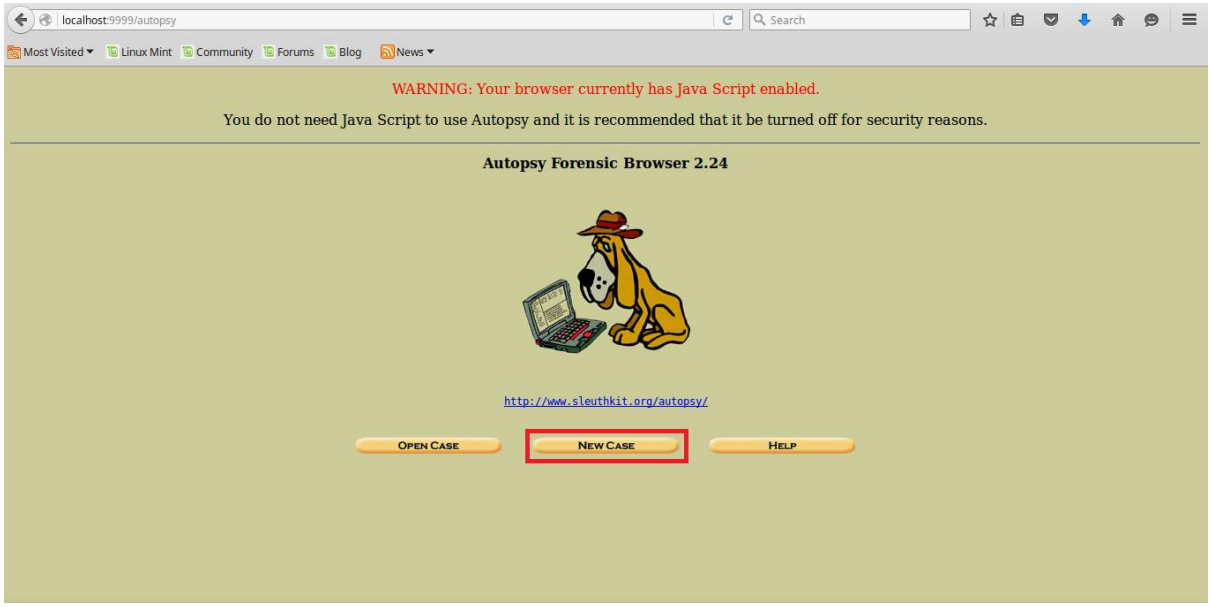
Gambar.1 old.honeynet.org/scans/scan24/image.zip

Setelah file selesai di download, buka terminal pada direktori tempat file image.zip disimpan. Buat folder dengan option : `mkdir /tmp/kasus.narkoba` lalu image di maunting menggunakan option : `#maunt image /tmp/kasus.narkoba/`, masuk pada direktori folder yang telah dibuat `cd /tmp/kasus.narkoba` jika dijalankan option `-ls` akan tampak dua file yaitu cover page.jpgc dan SCEDU~1.EXE. Kita coba untuk mengekstrak file tersebut dengan option `file *`, maka hasilnya akan tampil seperti pada Gambar.2. Tampak bahwa file cover page.jpgc tidak bisa terbaca sedangkan SCEDU~1.EXE ternyata merupakan zip archive data.

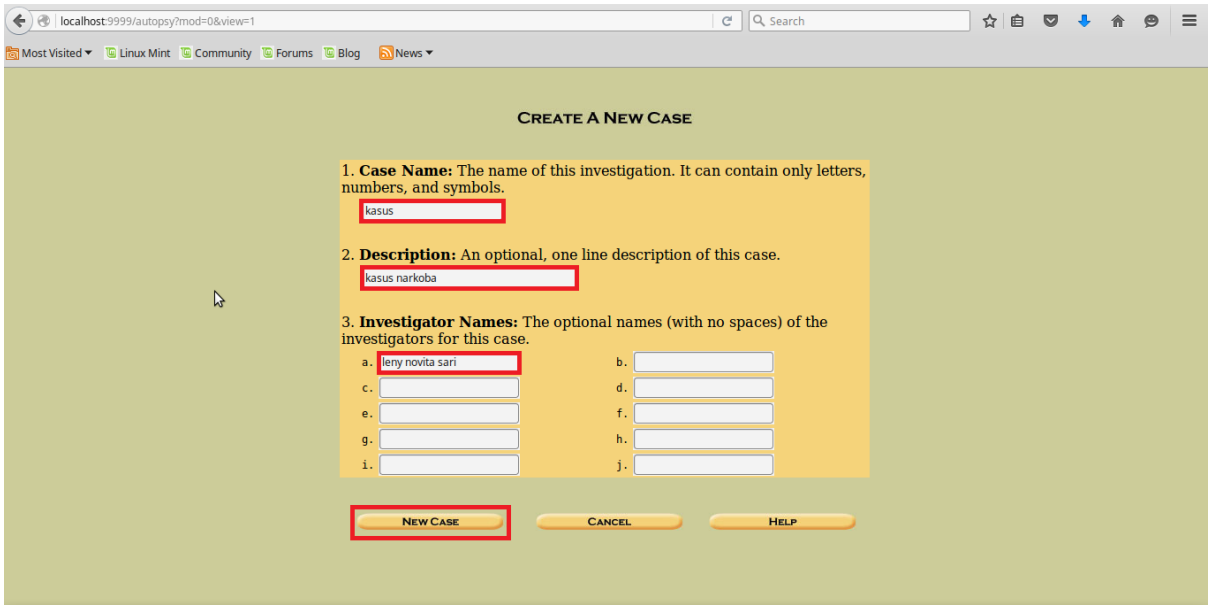


Gambar.2 Ekstrak File Image.zip

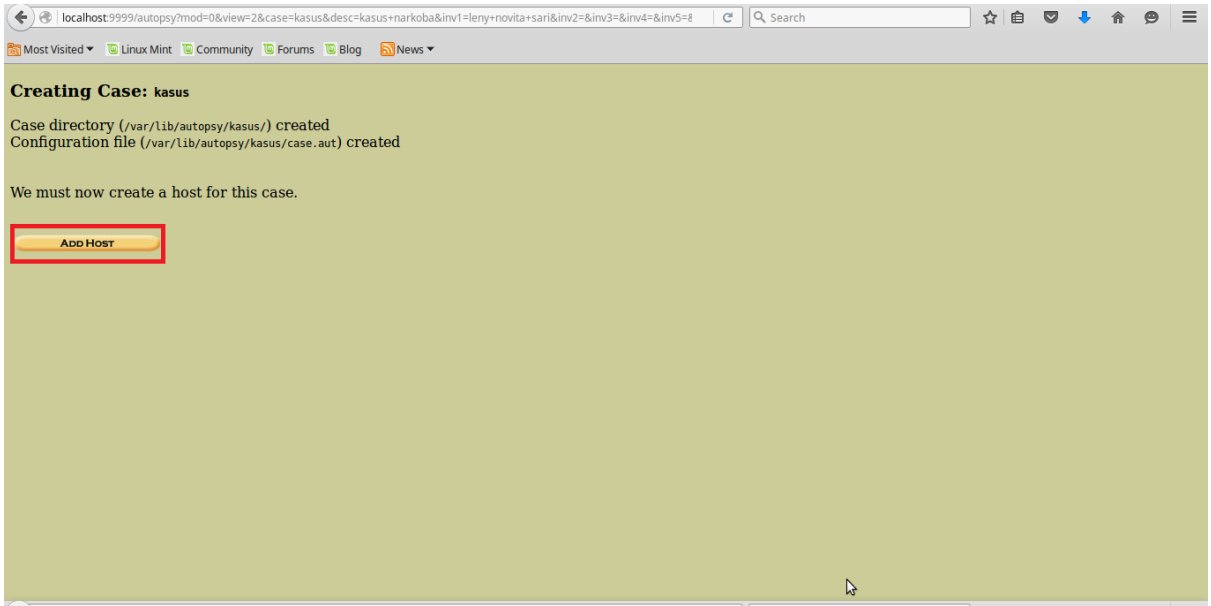
Sampai pada langkah di atas, kita belum mendapatkan informasi apapun dari kasus yang kita tangani. Langkah selanjutnya fokus pada Latent Data karena data yang kita dapatkan sifatnya khusus (telah ditimpa data lain, dilakukan rename yang tidak sesuai dengan tipe file sesungguhnya). Jalankan tool autopsy sesuai gambar-gambar dibawah ini untuk mengidentifikasi file.

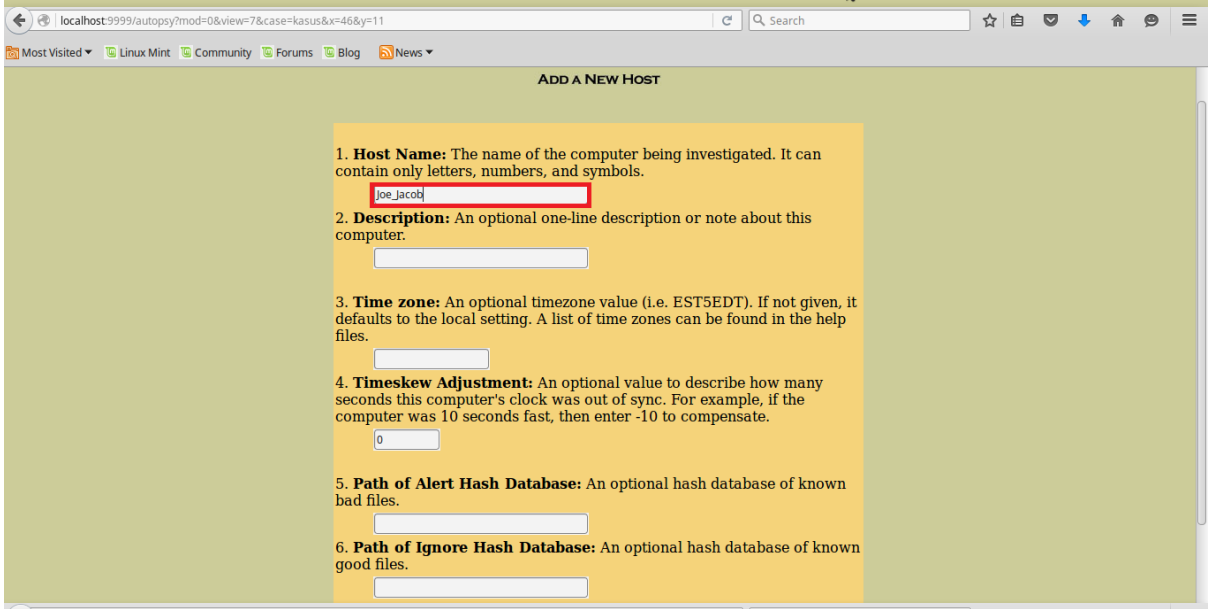


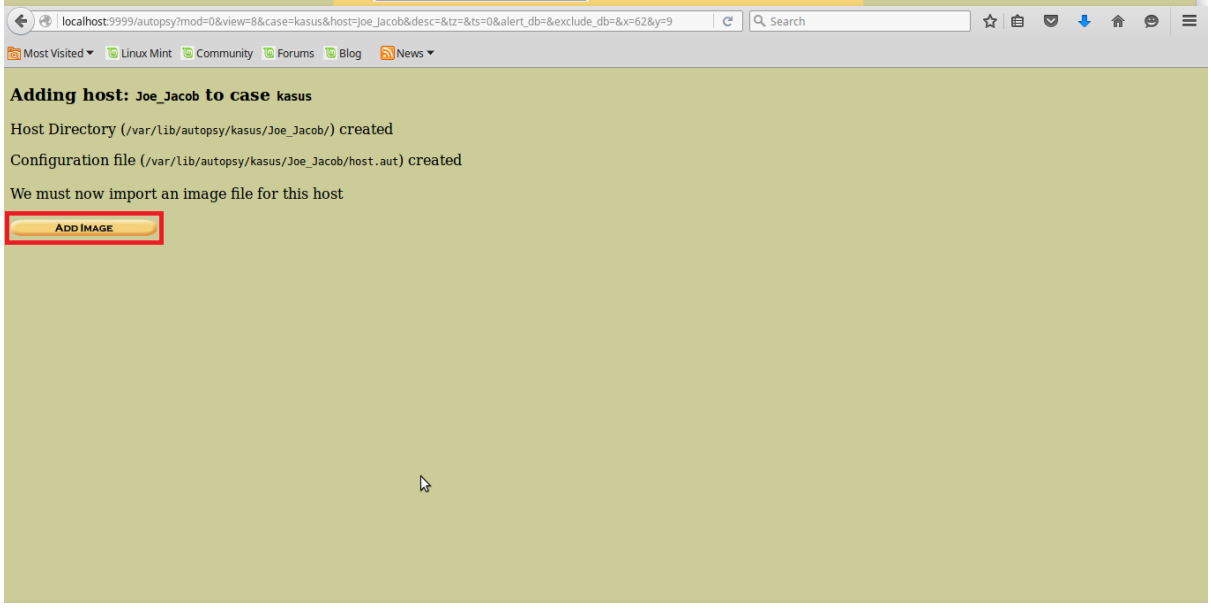
Gambar.3 Autopsy Forensic Browser 2.24



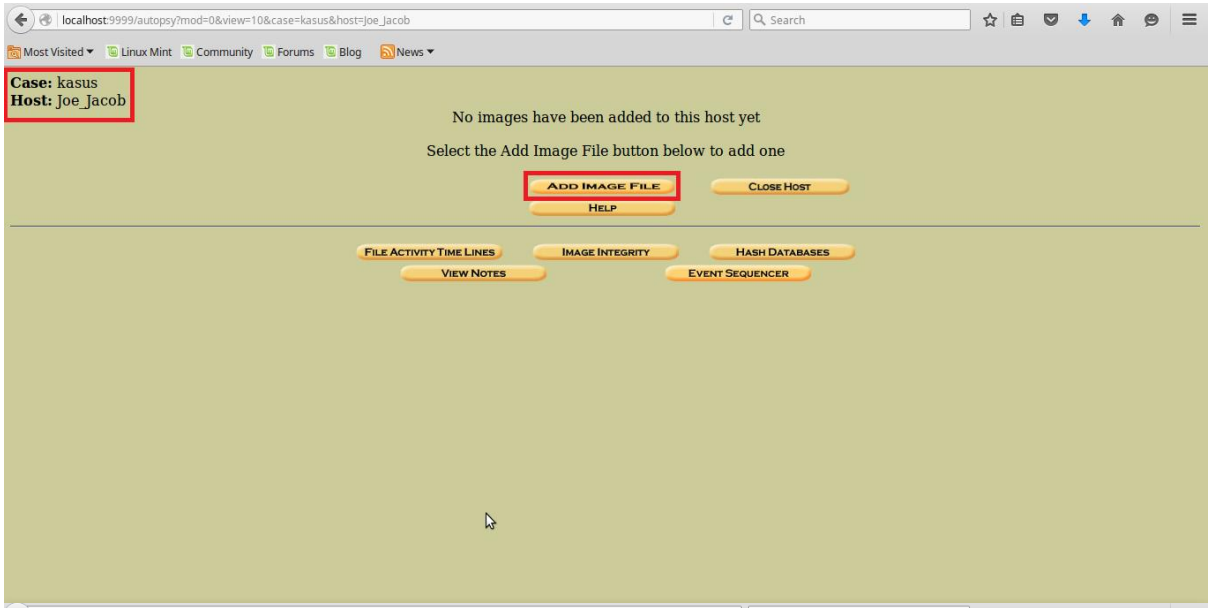
Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

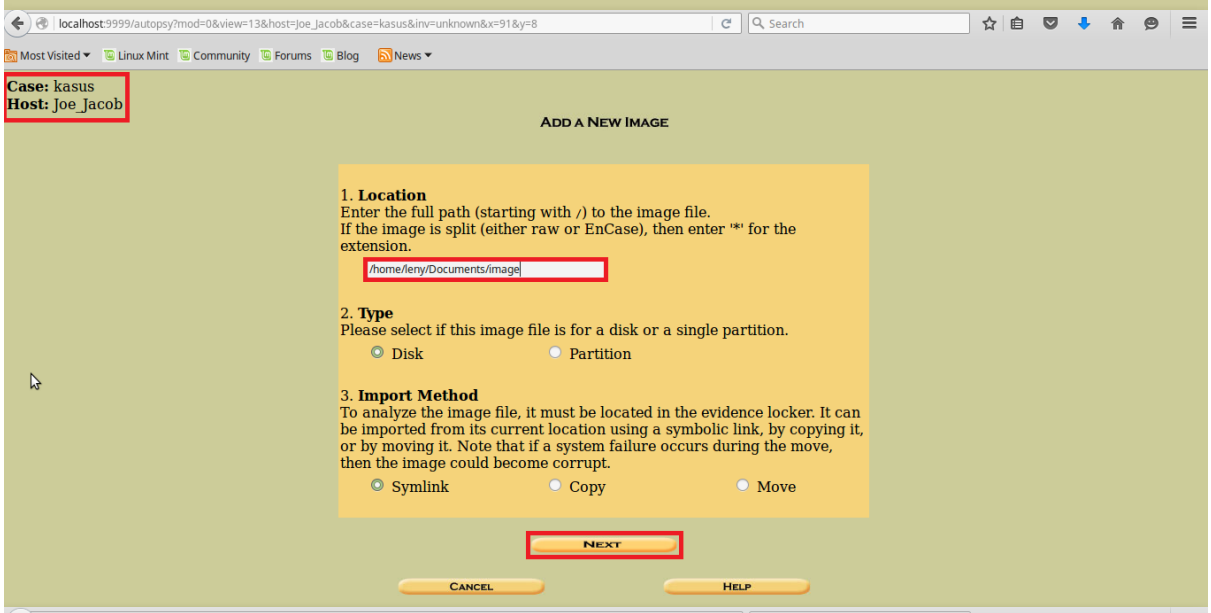


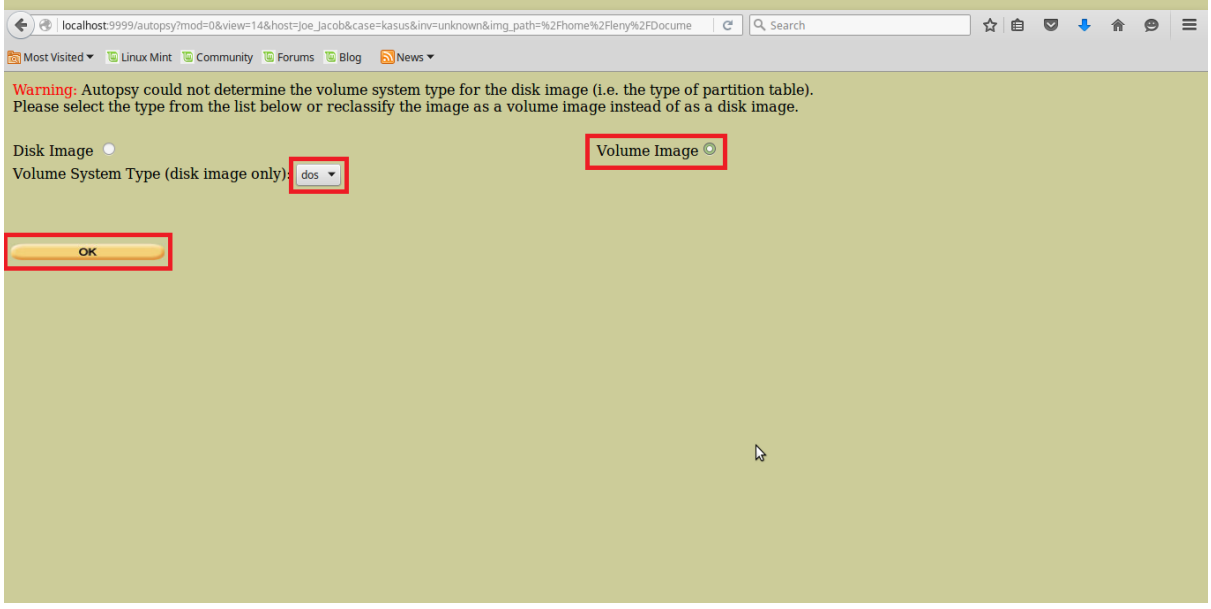




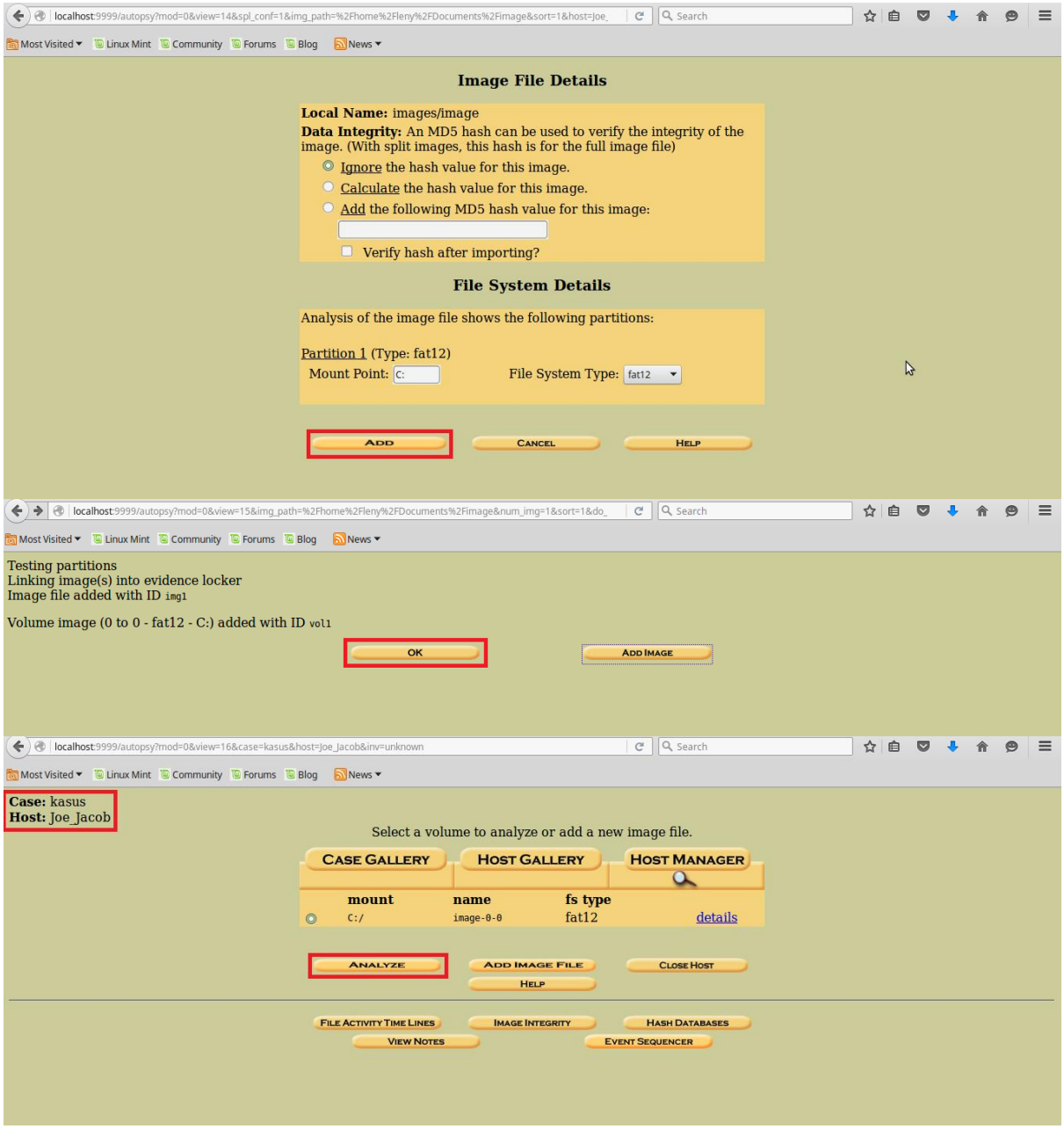
Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer







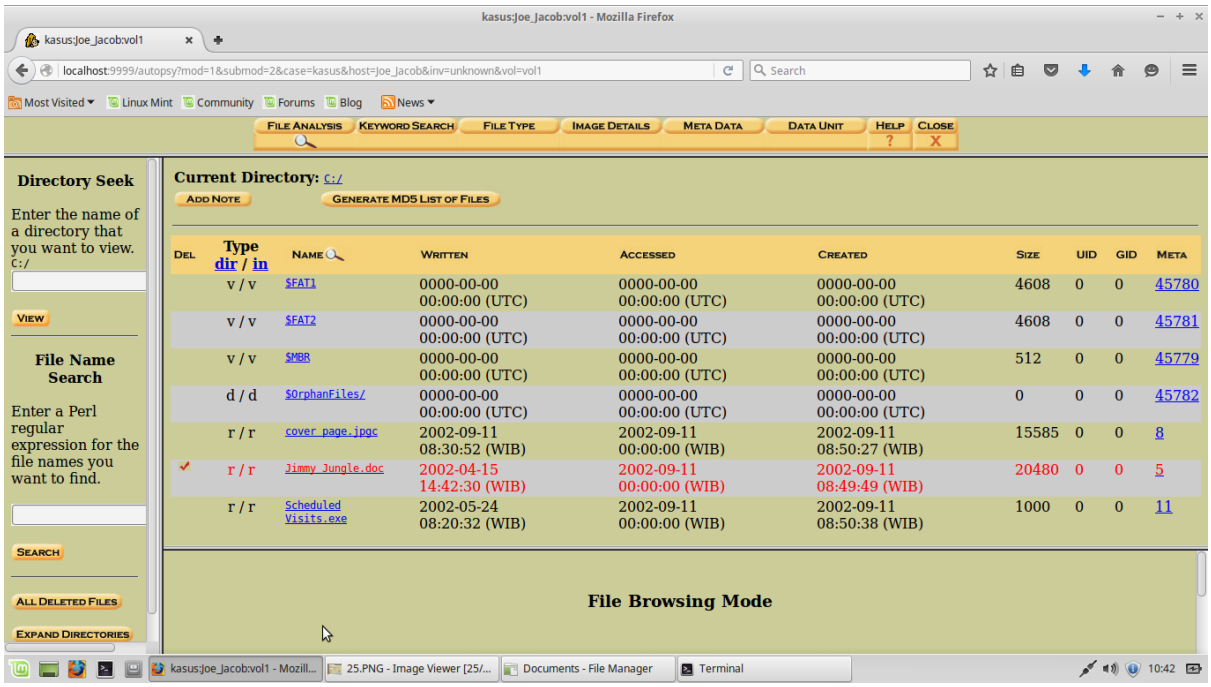
Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



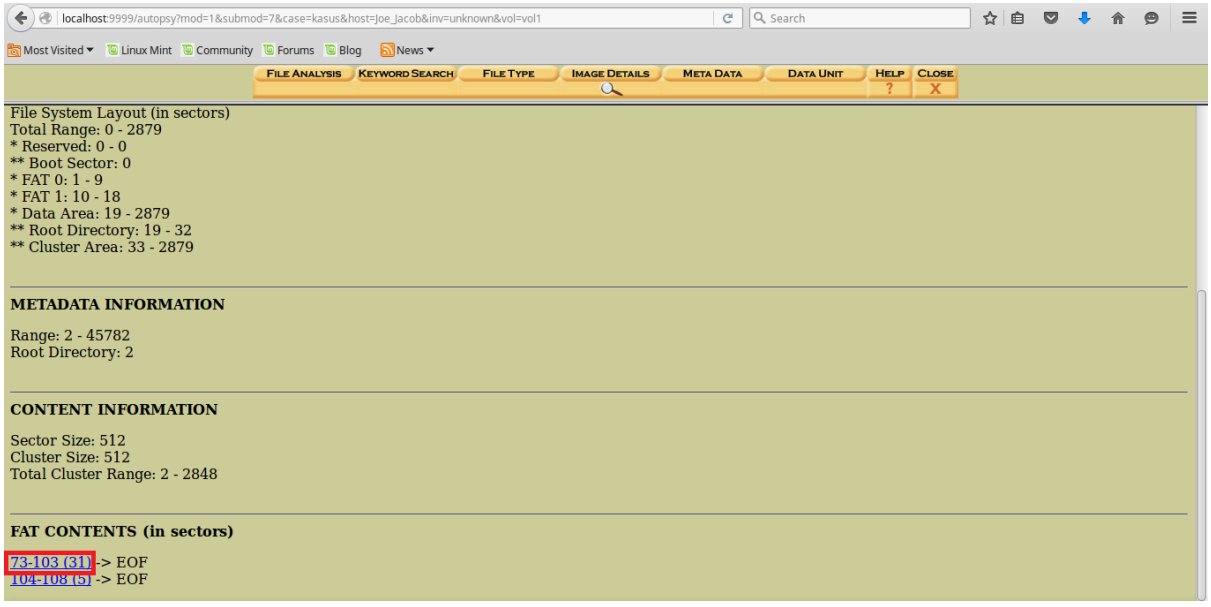
Gambar.4 Running Tool Autopsy

Setelah file image selesai diinputkan pada autopsy, maka akan didapatkan file analisis seperti pada Gambar.5. Pada menu meta data seperti Gambar.6, jika dilihat terdapat 2 FAT Content dalam sektor yaitu 73-103 dan 104-108 yang jika dibuka akan terdapat kumpulan kode ASCII baik yang redable ataupun yang tidak bisa di redable seperti pada Gambar.7 dan Gambar.12.

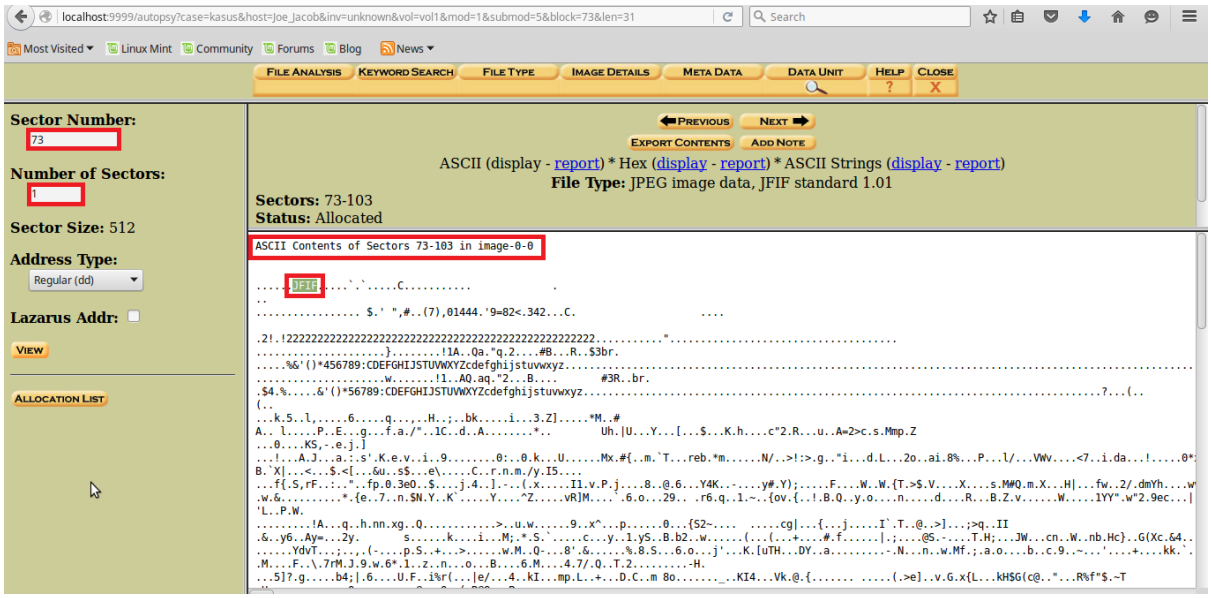
Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



Gambar.5 File Analisis Image.zip

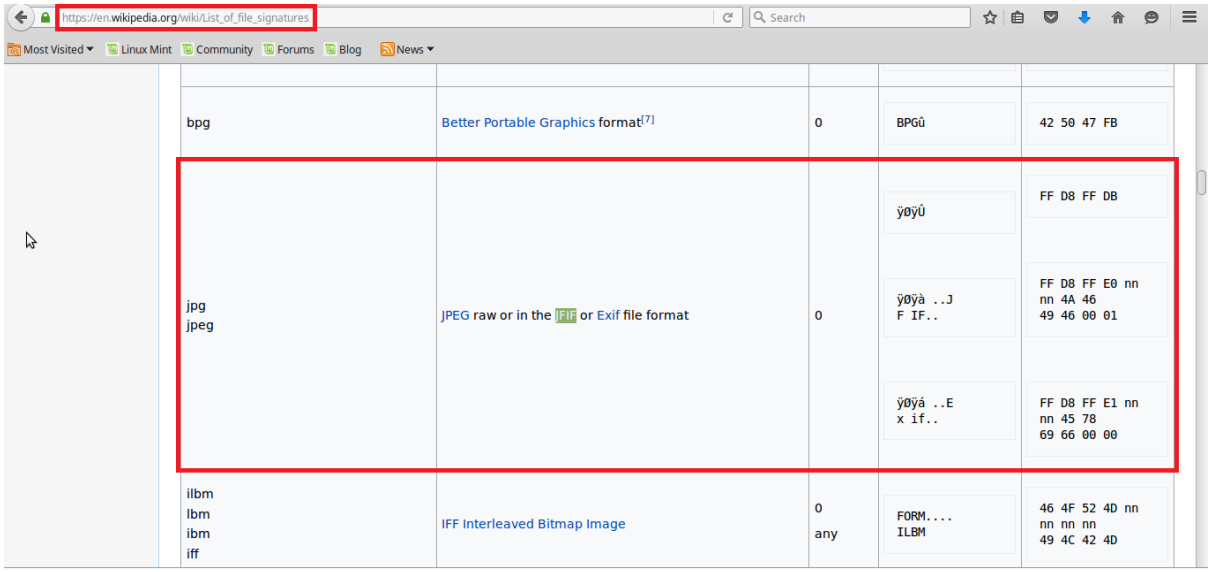


Gambar.6 Meta Data



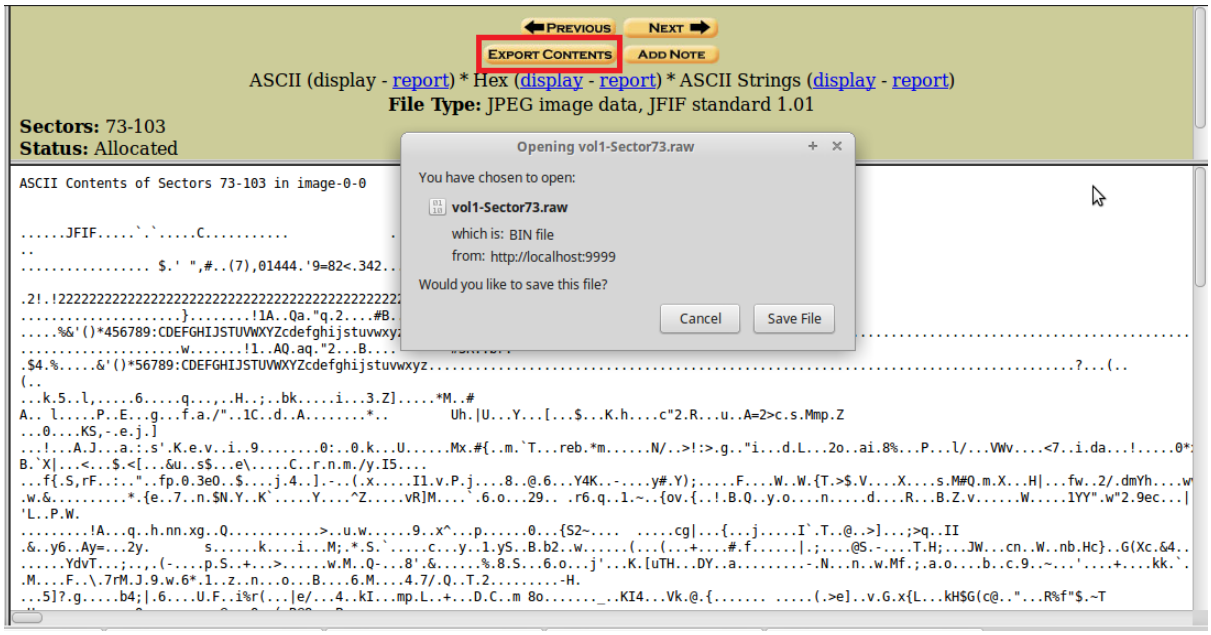
Gambar.7 ASCII dari sektor 73-103

Coba ambil salah satu header konten ASCII pada sektor 73-103, kemudian cek tipe file dengan menggunakan sample header yang telah ditentukan pada *List of File Signatures*. Dari file signature didapatkan bahwa sektor 73-103 dengan header JFIF ternyata merupakan tipe file gambar (jpg/jpeg). Eksport contents seperti Gambar.9 kemudian lakukan rename pada file yang telah di eksport, dari .raw menjadi .jpg atau .jpeg maka akan tampil gambar seperti Gambar.11.

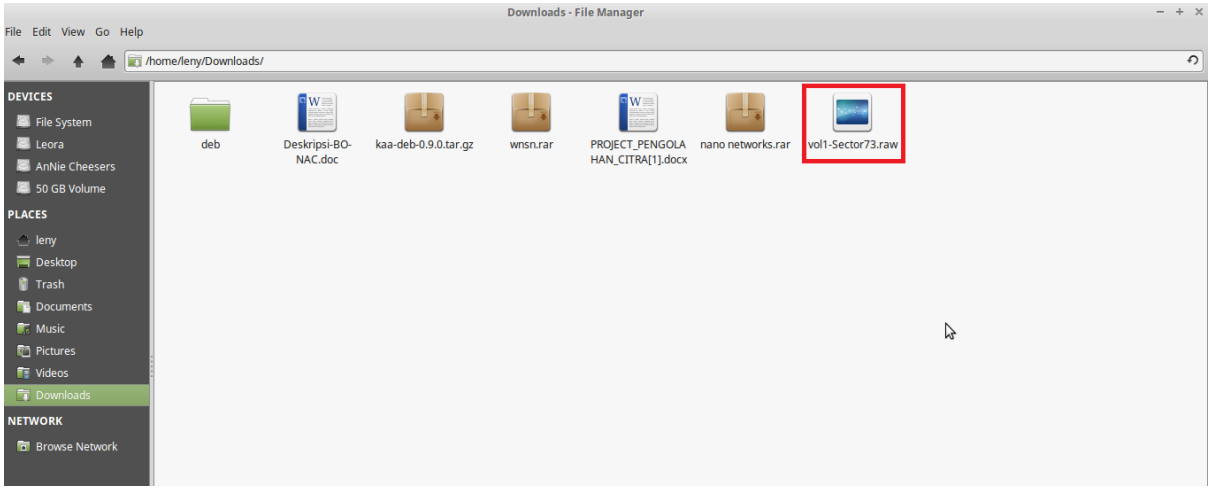


Gambar.8 File Signature Header JFIF

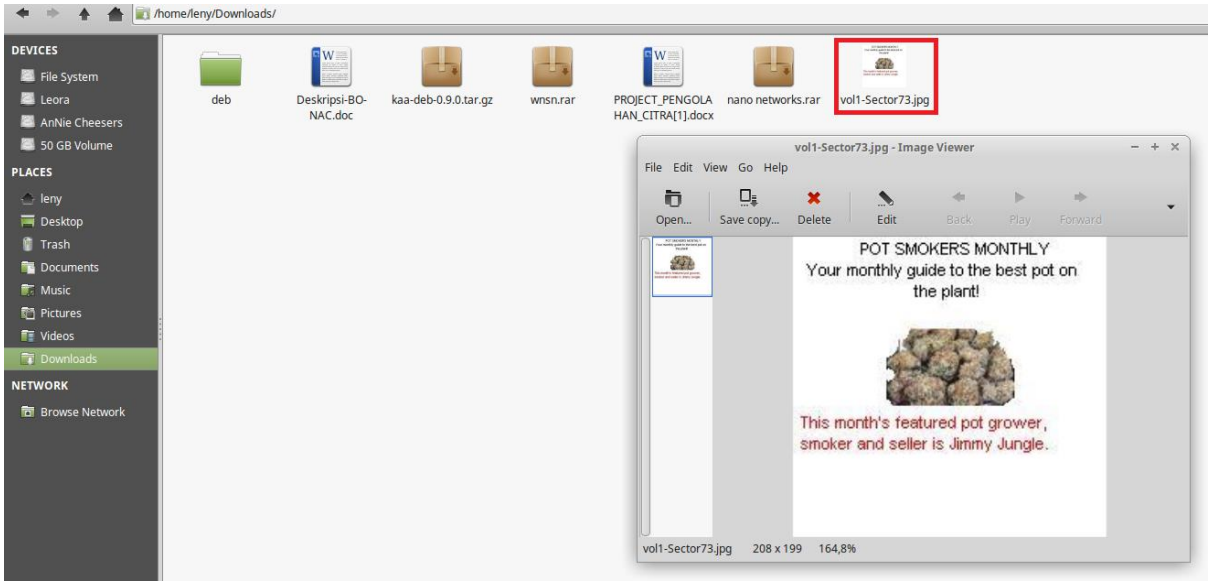
Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



Gambar.9 Eksport File pada Sektor 73

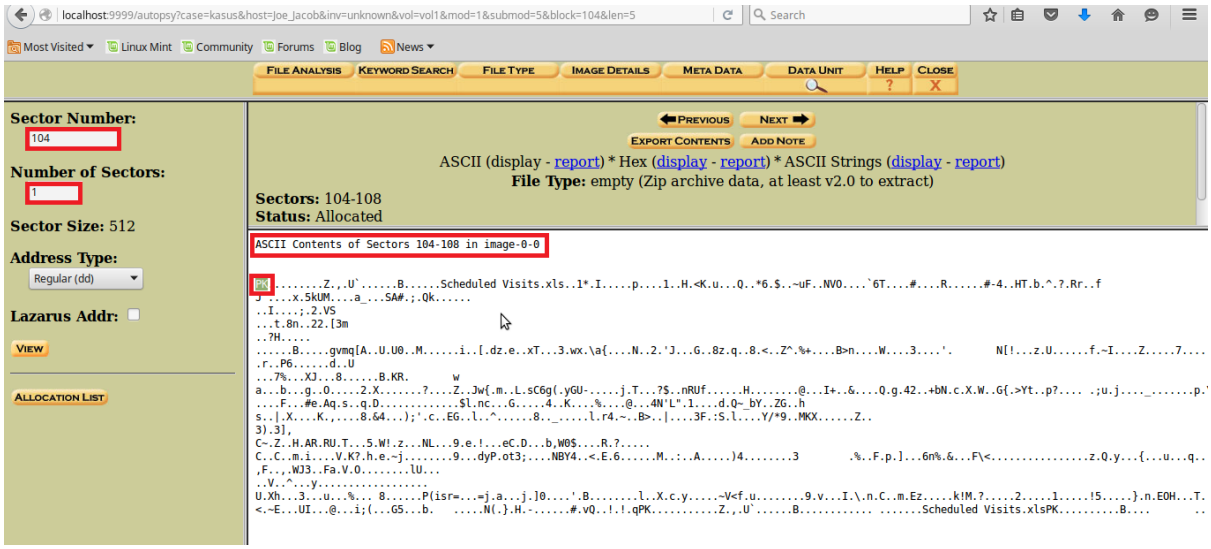


Gambar.10 File Sektor73.raw



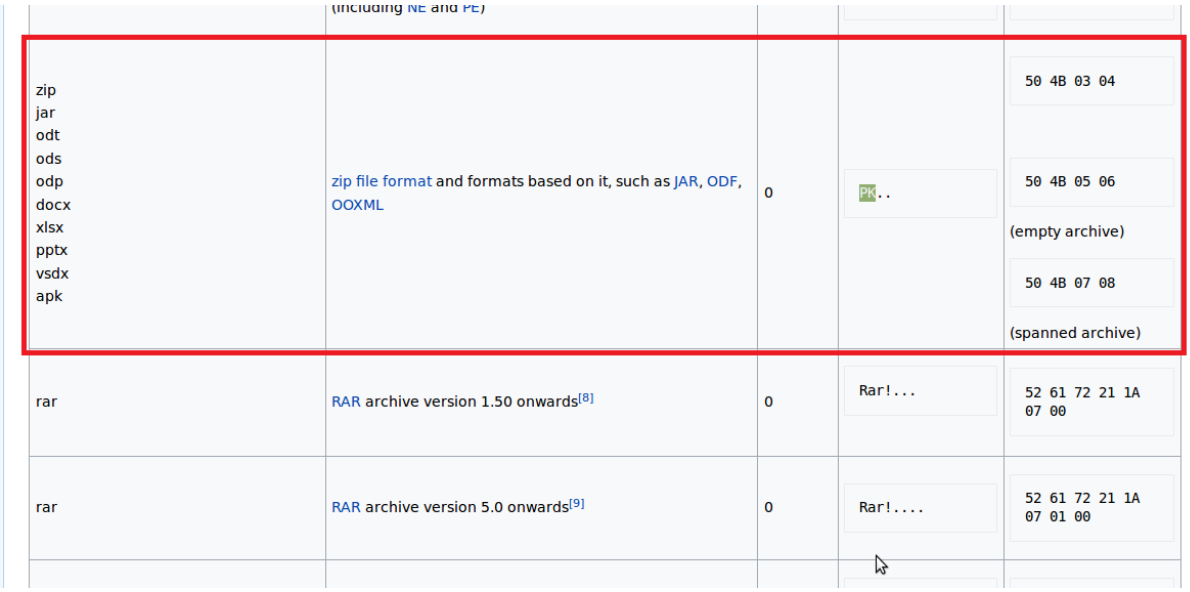
Gambar.11 File Sektor73.jpg

Lakukan hal yang sama untuk pengolahan sektor 104-108. Coba ambil salah satu header konten ASCII, kemudian cek tipe file dengan menggunakan sample header yang telah ditentukan pada *List of File Signatures*. Dari file signature didapatkan bahwa sektor 104-108 dengan header PK ternyata merupakan tipe file zip/jar/odt/ods/odp/docx/xlsx/pptx/vsdx/apk. Eksport contents seperti Gambar.14 kemudian lakukan rename pada file yang telah di eksport, dari .raw menjadi .zip maka akan tampil gambar seperti Gambar.16, yang ternyata setelah dibuka didalamnya terdapat sebuah dokumen bertipe .xls, untuk mebuka file tersebut dibutuhkan sebuah password.



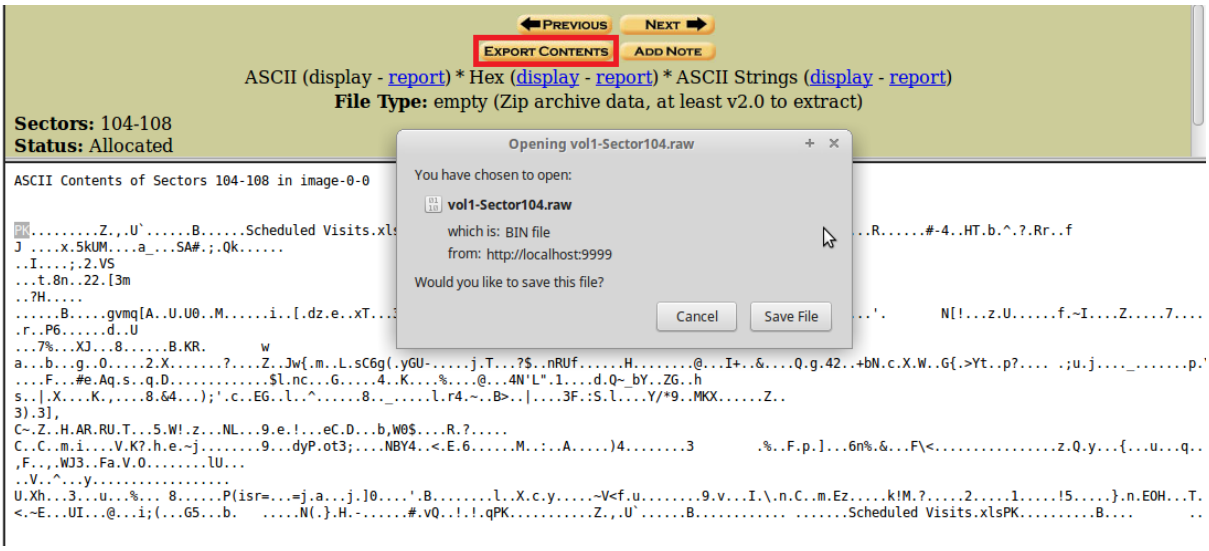
Gambar.12 ASCII dari sektor 104-108

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

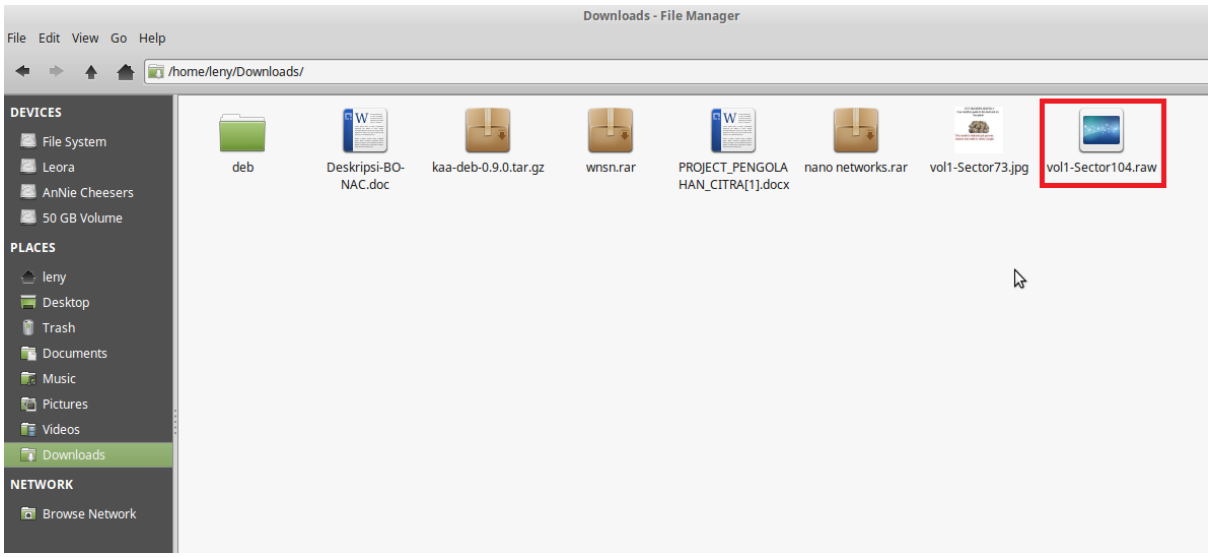


zip jar odt ods odp docx xlsx pptx vsdx apk	zip file format and formats based on it, such as JAR, ODF, OOXML	0	PK..	50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive)
rar	RAR archive version 1.50 onwards[8]	0	Rar!...	52 61 72 21 1A 07 00
rar	RAR archive version 5.0 onwards[9]	0	Rar!....	52 61 72 21 1A 07 01 00

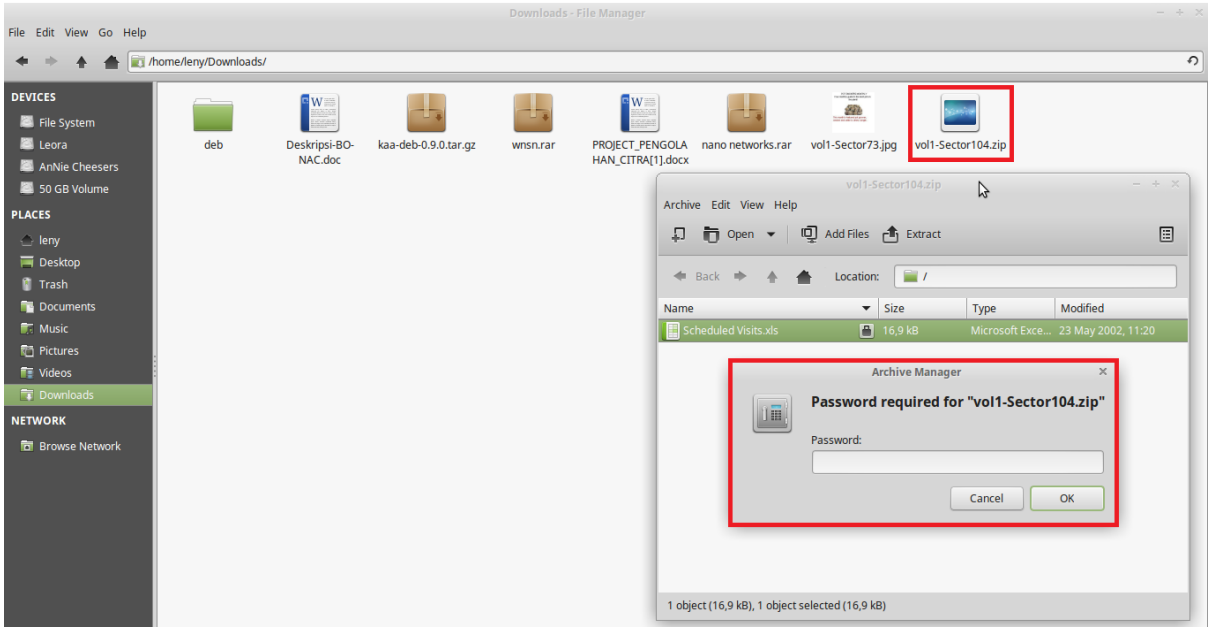
Gambar.13 File Signature Header PK



Gambar.14 Eksport File pada Sektor 104



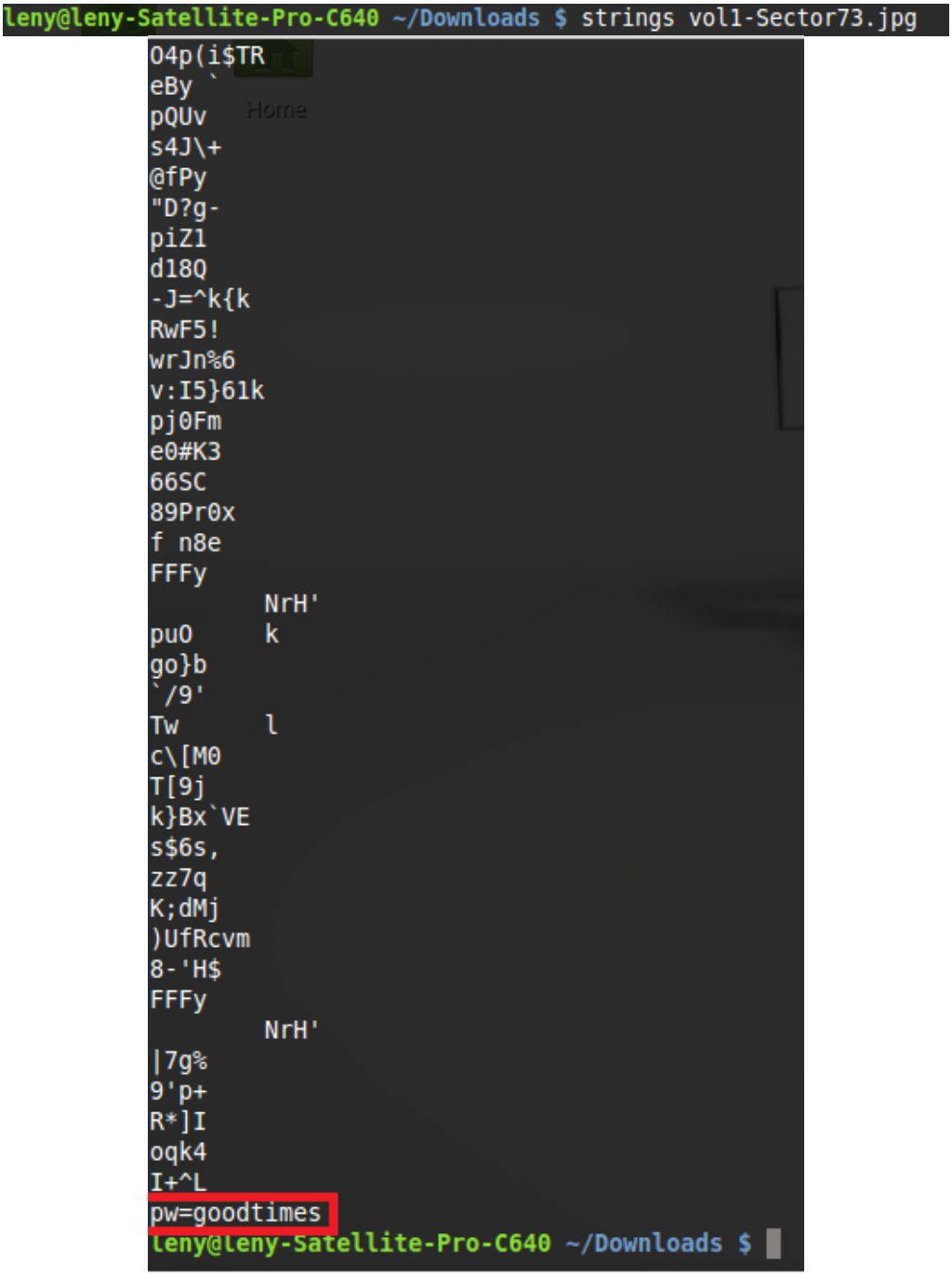
Gambar.15 File Sektor104.raw



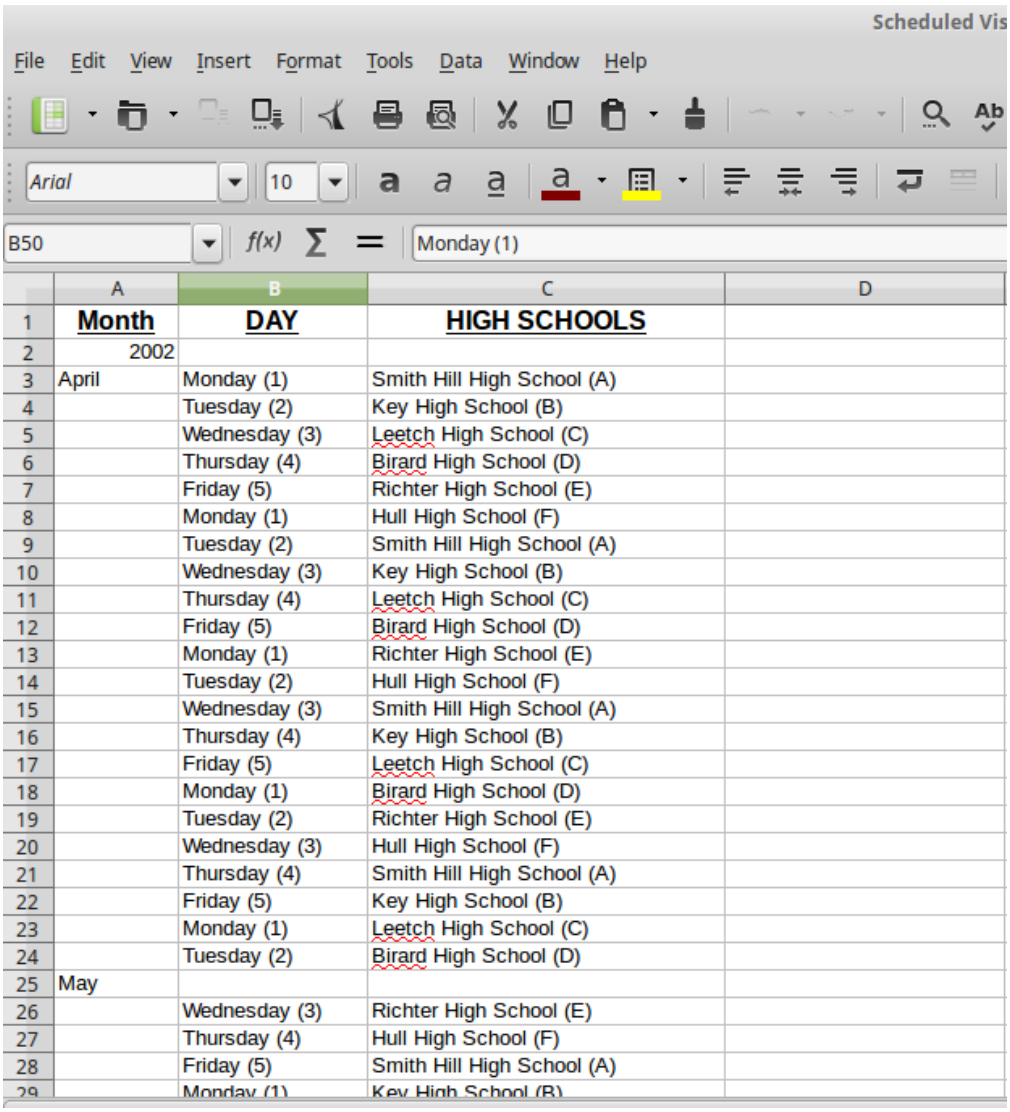
Gambar.16 File Sektor104.zip

Untuk mendapatkan password hingga bisa membuka dokumen bertipe .xls diatas, kita menjalankan tool strings dengan option `strings vol1-sector73.jpg` hingga didapatkan

password : goodtimes seperti Gambar.17. Inputkan password pada vol1-Sector104.zip untuk membuka file xls yang terdapat didalamnya, setelah file xls terbuka ternyata didalamnya berisikan bulan, hari dan nama-nama sekolah yang dikunjungi pelaku seperti pada Gambar.18.



Gambar.17 Running tool Strings untuk Mendapatkan Password



Scheduled Vis

File Edit View Insert Format Tools Data Window Help

Arial 10

B50 f(x) Σ = Monday (1)

	A	B	C	D
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)	

Gambar.18 File xls pada Sektor104.zip

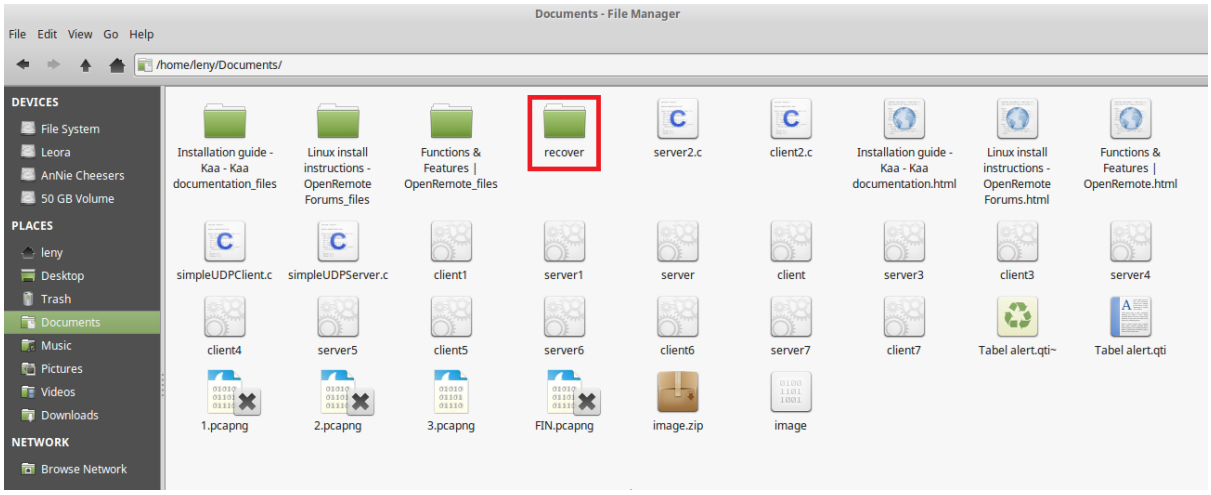
Kita tidak tahu apa yang dilakukan pelaku pada file image.zip yang ada, maka kita gunakan tool foremost untuk merecover file berdasarkan header dengan option `foremost -v -i image -o recover`. Cek folder recover pada direktori penyimpanan file image.zip seperti Gambar.20. Pada folder recover terdapat folder lagi, yaitu : folder doc/ole, jpg dan zip. Buka folder doc, di dalamnya terdapat dokumen .doc yang ternyata isinya adalah sebuah surat untuk Jimmy Jungle.

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

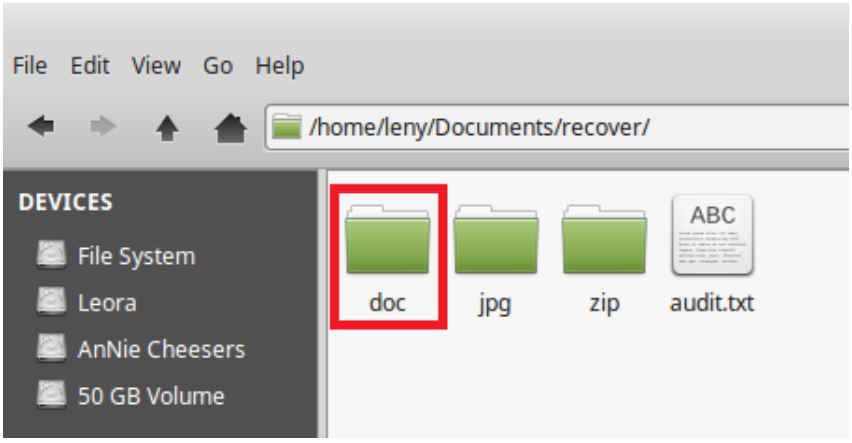
```
leny@leny-Satellite-Pro-C640 ~/Documents $ ls
1.pcapng
2.pcapng
3.pcapng
client
client1
client2.c
client3
client4
client5
client6
client7
FIN.pcapng
Functions & Features | OpenRemote_files
Functions & Features | OpenRemote.html
image
image.zip
Installation guide - Kaa - Kaa documentation_files
Installation guide - Kaa - Kaa documentation.html
Linux install instructions - OpenRemote Forums_files
Linux install instructions - OpenRemote Forums.html
server
server1
server2.c
server3
server4
server5
server6
server7
simpleUDPClient.c
simpleUDPServer.c
Tabel alert.qti
Tabel alert.qti~
leny@leny-Satellite-Pro-C640 ~/Documents $ foremost -v -i image -o recover
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Mar 24 11:51:02 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/leny/Documents/recover
```

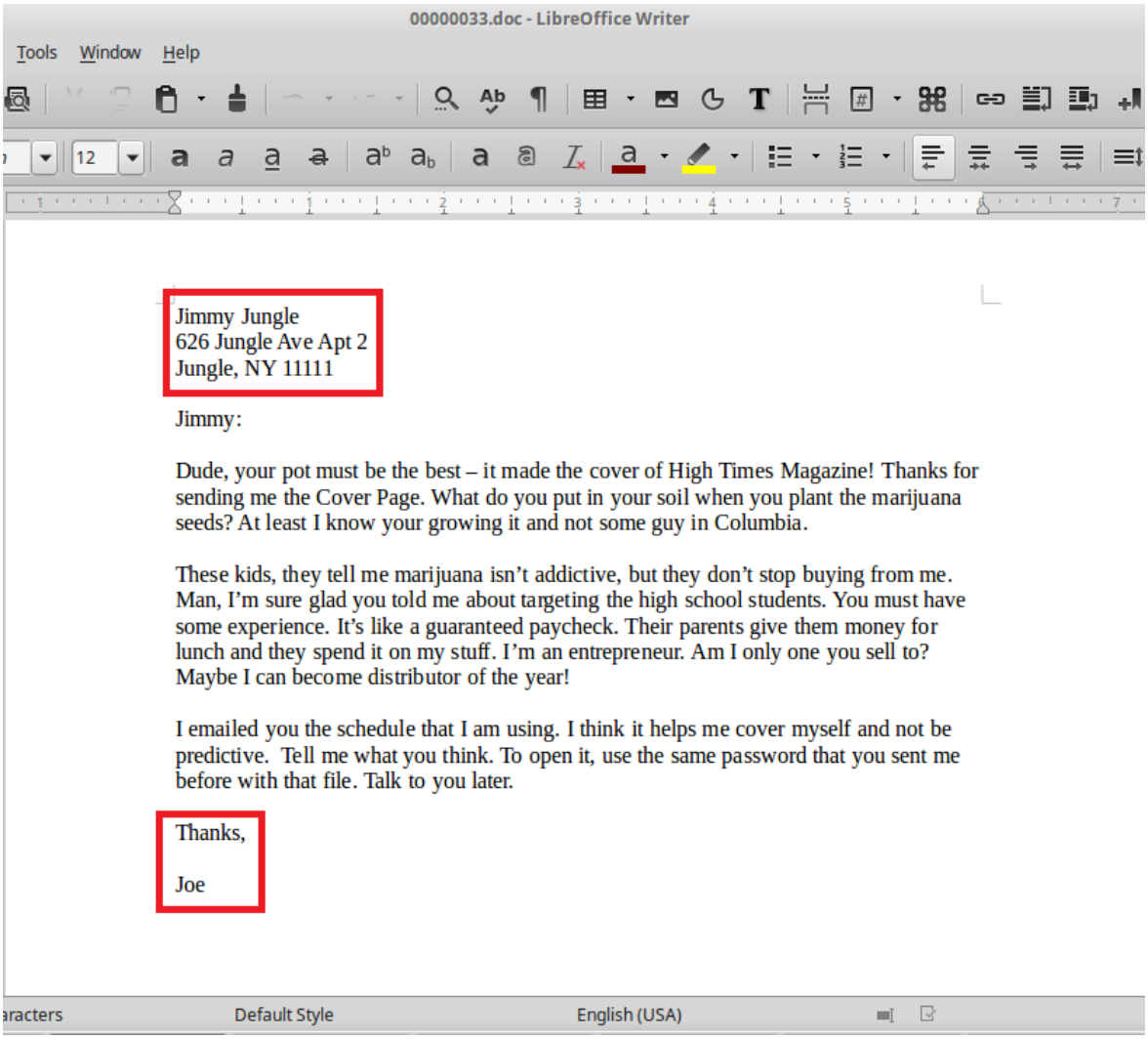
Gambar.19 Running Tool Foremost



Gambar.20 Folder Recover

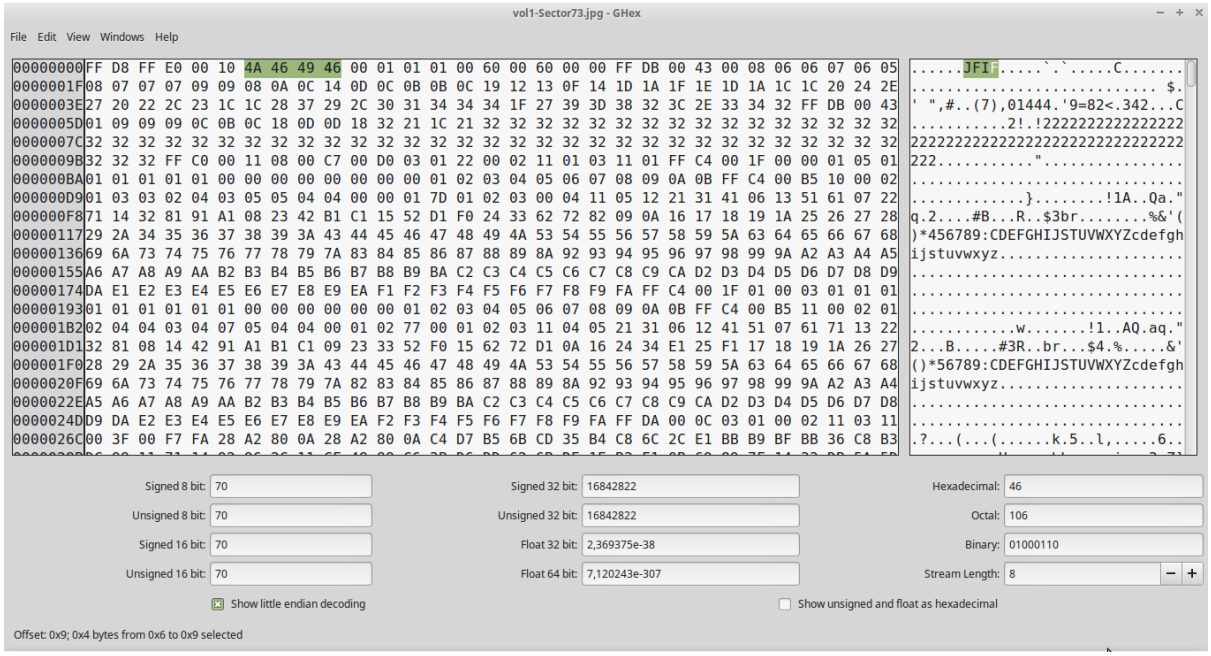


Gambar.21 Folder Doc



Gambar.22 Surat Dari Joe untuk Jimmy Jungle

Terakhir, running tool ghex untuk editor hexa dari Vol1-Sector73.JPG.



Gambar.23 Running Tool Ghex

Dari apa yang kita lakukan diatas, kita bisa menjawab beberapa informasi yang dibutuhkan pihak berwenang untuk penyelidikan lebih lanjut.

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
   → Jimmy Jungle, alamat : 626 Jungle Ave Apt 2 Jugle NY 11111
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
   → password dari file zip yang diembedd ke cover page menggunakan steganografi.
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
   → Key High School, Leetch High School, Birard High School, Richter High School, Hull High School.
4. For each file, what processes were taken by the suspect to mask them from others?
   → Melakukan rename file zip menjadi file EXE dan menyembunyikan password dengan menggunakan file.jpg.
5. What processes did you (the investigator) use to successfully examine the entire contents of each file? (proses apa yang kamu lakukan sebagai investigator untuk memeriksa secara keseluruhan konten dari setiap file)

→ pertama-tama melakukan “MD5 Checksum” pada barang bukti untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada, kemudian mengekstrak file dari file yang ada, kemudian barulah diolah dengan menggunakan bantuan tool sehingga didapatkanlah beberapa file. Untuk file JPG, image.zip di identifikasi menggunakan autopsy sehingga didapatkan vol1-sector73.raw kemudian direname menjadi vol1-sector73.jpg sehingga menjadi sebuah gambar. Untuk file ZIP, sama seperti identifikasi file JPG hanya saja vol1-sector104.raw direname menjadi vol1-sector104.zip sehingga didapatkan file berbentuk XLS yang didalamnya terdapat informasi penting tentang sekolah-sekolah yang sering dikunjungi pengedar narkoba untuk melakukan aksinya. Sedangkan untuk file DOC didapatkan dari hasil recovery image.zip berdasarkan header dengan menggunakan foremost.