Network Security: Computer Forensics

Menurut Dr. HB Wolfre, definisi dari forensik komputer adalah sebagai berikut [1]:

"*A methodological series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format.*"

Serangkaian metodologis teknik dan prosedur untuk mengumpulkan bukti-bukti, dari peralatan dan berbagai perangkat penyimpanan dan media digital komputasi, yang dapat disajikan di pengadilan hukum dalam format yang koheren dan bermakna

Tujuan dan Fokus Forensik Komputer, yaitu [1]:

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.

Berikut adalah manfaat dari forensik komputer [1]:

1. Organisasi/perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang di butuhkan.
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

Fokus data yang di kumpulkan pada bidang forensik di bagi menjadi tiga kategor, 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 *tools* khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (*corrupted file*), dan lain sebagainya

Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Contohnya adalah sebagai berikut [1]:

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

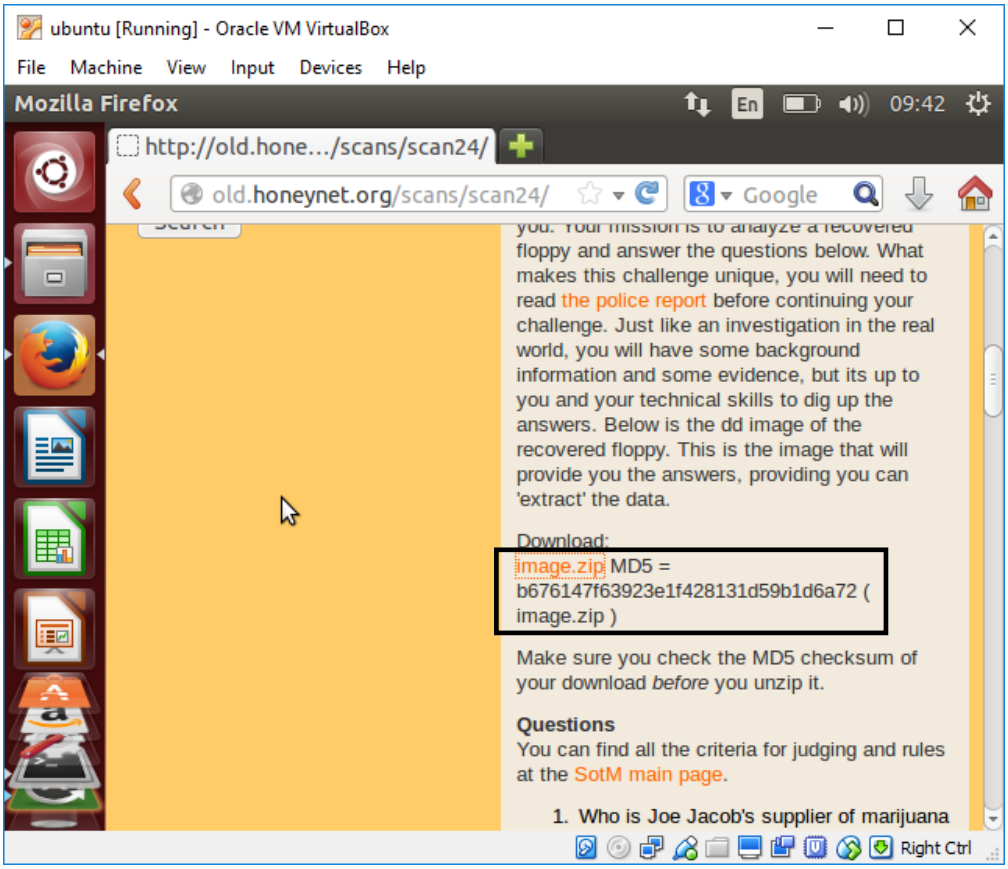
Pada tugas 6 tentang forensic, terdapat sebuah contoh kasus yang harus diselesaikan. Berikut adalah contoh kasus forensik yang dilakukan pada percobaan tugas 6 :

> 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 :
>
> 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?

Solusi untuk memecahkan kasus narkoba pada kotak diatas, berikut adalah tools yang digunakan :

- Autopsy
- Foremost
- Strings
- Ghex

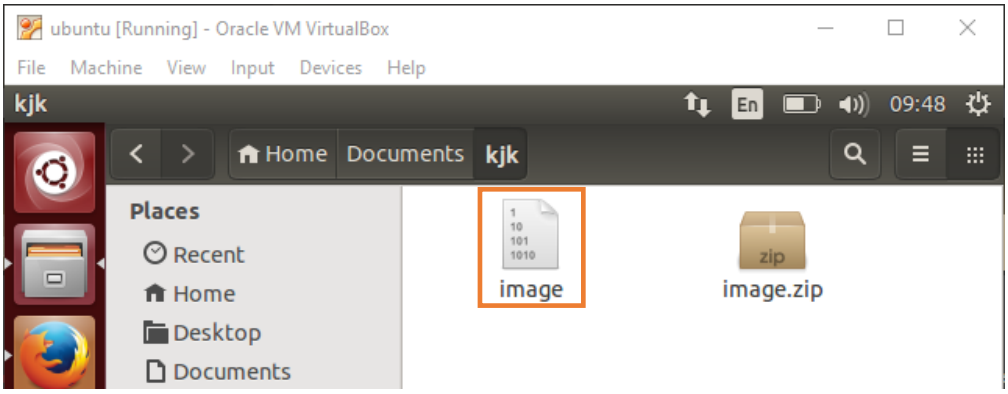
Hal yang harus kita lakukan untuk melakukan computer forensic untuk menyelidiki kasus narkoba diatas, kita download terlebih dahulu file zip pada url : http://old.honeynet.org/scans/scan24



Gambar 1: url tempat download file zip untuk kasus narkoba

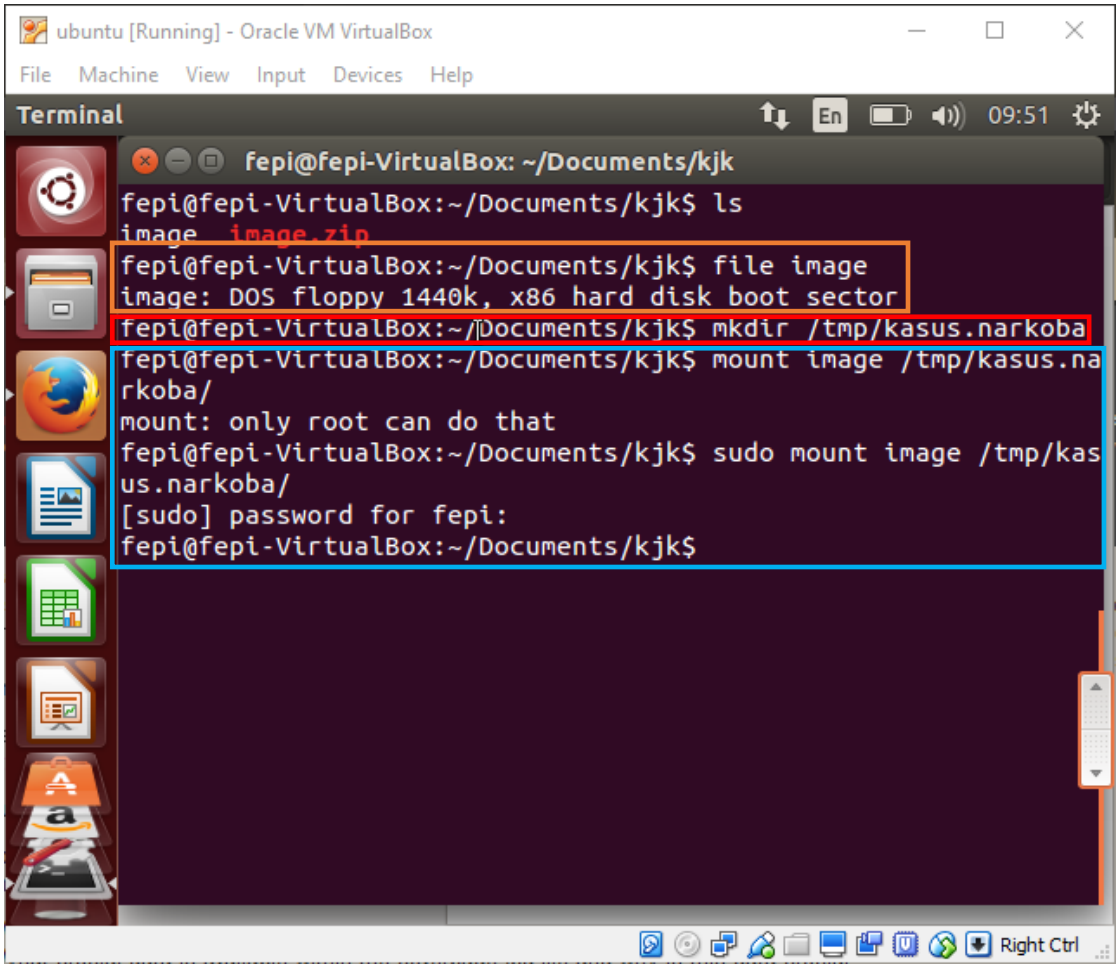
Pada gambar 1 dapat kita lihat terdapat file yang bernama image.zip. MD5 berfungsi untuk mengecek keaslian dari file. Setelah download kita extrak file image.zip yang terdapat pada direktori Download.

Agar memudahkan pada saat mencari file, penulis memindahkan file image.zip dalam direktori kjk, dengan path yaitu : /home/fepi/Documents/kjk.



Gambar 2: file image.zip setelah diekstrak

Setelah kita melakukan proses ekstrak, dapat kita lihat file image.zip berisi sebuah file image yang belum diketahui tipe filenya. Agar dapat mengetahui tipe file tersebut kita gunakan *command* : **file (spasi) nama_file**.



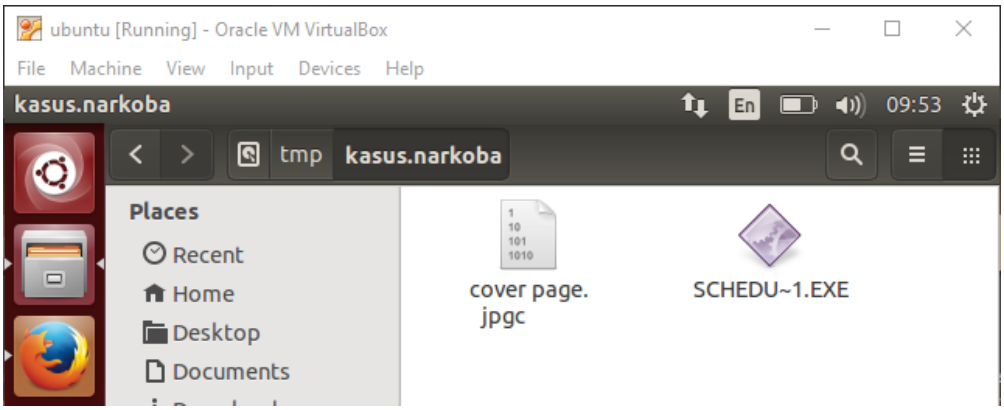
Gambar 3: image

Berdasarkan kotak yang berwarna oren dapat kita lihat hasil dari file image berupa **DOS floppy 1440k, x86 hard disk boot sector.** Boot sector adalah bagian dari hard disk atau floppy disk yang memiliki kode yang tersimpan di dalamnya program boot khusus, dan untuk referensi fitur kunci lain untuk menjaga disk bekerja.

Setelah mengetahui tipe file image,kita buat direktori baru yang dapat dilihat pada kotak berwarna merah pada gambar 3. **$mkdir /tmp/kasus.narkoba,** mkdir artinya perintah untuk membuat direktori baru. Direktori tersebut dibuat pada /tmp/kasus.narkoba. tmp artinya *temporary* yang bersifat sementara jika kita restart, direktori yang dibuat tadi akan hilang. Kasus.narkoba merupakan nama direktori yang akan dibuat.

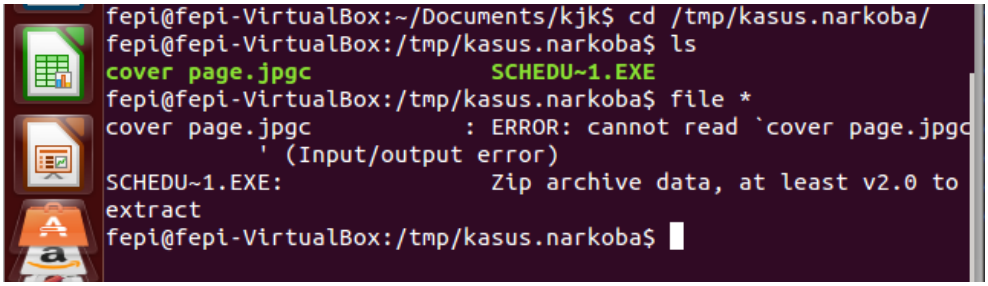
Kotak warna biru yang terdapat pada gambar 3 merupakan proses mount file image dengan direktori yang telah kita buat. Mount merupakan perintah yang akan me-mount filesystem ke suatu direktori atau mount-point yang telah ditentukan. Hanya superuser yang bisa menjalankan perintah ini.

Setelah melakukan mount, kita lihat isi direktori tmp/kasus.narkoba (gambar 4).



Gambar 4: isi direktori /tmp/kasus.narkoba

Pada direktori kasus.narkoba, dapat kita lihat pada gambar 4 terdapat file yang bernama **cover page.jpgc** dan **SCHEDU~1.EXE.** Kedua file tersebut kita belum mengetahui tipe filenya. Untuk mengecek tipe file kita gunakan kembali *command* **file *.** Tanda bintang artinya mengecek semua tipe file dalam direktori kasus.narkoba.

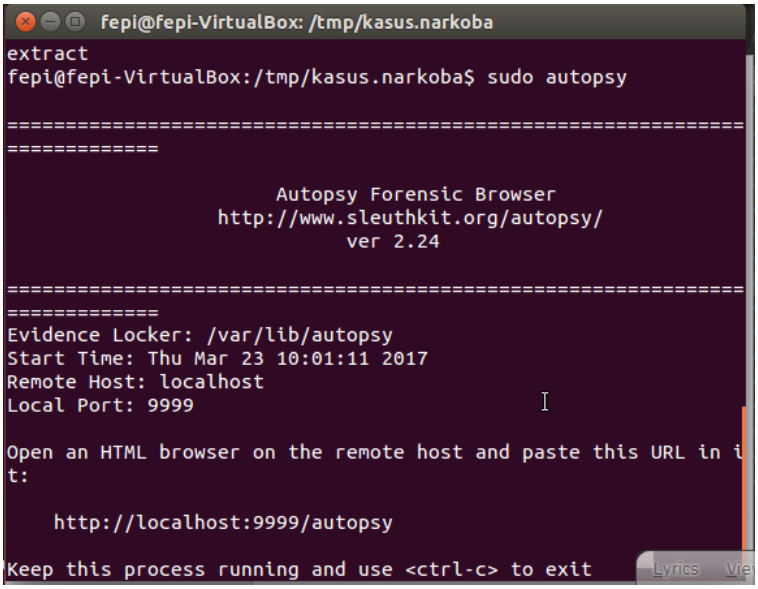


Gambar 5: proses pengecekan tipe file pada direktori kasus.narkoba

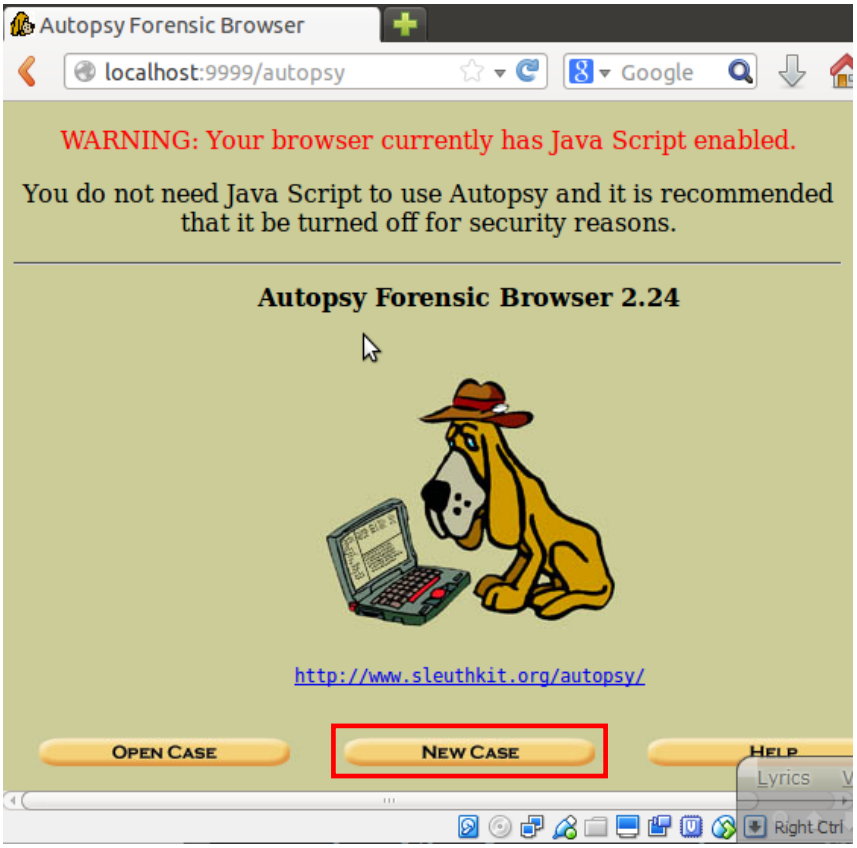
Pada gambar 5 dapat kita lihat bahwa **cover page.jpgc** merupakan file ERROR tidak bisa dibaca. File **cover page.jpgc** tidak dapat dibaca, dapat kita analisa kemungkinan file tersebut telah dihapus sebelumnya oleh tersangka. Untuk melihat file **cover page.jpgc** kita gunakan tools untuk forensic. Sedangkan file **SCHEDU~1.EXE** bertipe zip.

Untuk melakukan forensic terhadap file **cover page.jpgc** dan **SCHEDU~1.EXE** kita gunakan tools **autopsy, foremost, strings,** dang hex [2]**.**

- **Autopsy :** merupakan antarmuka grafis untuk tool analisis investigasi diginal perintah baris The Sleuth Kit. Tools tersebut dapat menganalisis disk dan filesistem Windows dan UNIX (NTFS, FAT, UFS1/2, Ext2/3). The Sleuth Kit dan Autopsy bersifat Open Source dan berjalan pada platform UNIX. Karena Autopsy berbasis HTML, kita dapat koneksi ke server Autopsy dari sembarang platform dengan menggunakan browser HTML.
- **Foremost** : merupakan sebuah tool yang dapat digunakan untuk me-recover file berdasarkan header, footer, atau struktur data file tersebut. Header dan footer dapat diberikan dalam sebuah file konfigurasi atau anda dapat memberikan opsi perintah baris untuk menentukan tipe file built-in. Tipe built-in ini mencari struktur data format file yang diberikan sehingga memberikan recovery yang cepat dan handal. Jika tidak tersedia tipe built-in untuk format yang anda inginkan, anda dapat mendefisikan formatnya dalam file konfigurasi foremost.conf. Beberapa format yang didukung secara built-in adalah gif, jpg, png, bmp, avi, mov, doc, html, pdf, wav, zip, rar, wmv, ppt, xls, sxw, sxc, dan sxi.
- **Strings :** merupakan *tools* aplikasi yang berfungsi untuk melihat karakter pada sebuah file.
- **Ghex :** merupakan *tools* aplikasi yang digunakan untuk mengkonvert atau mengubah file teks ke file hexa.

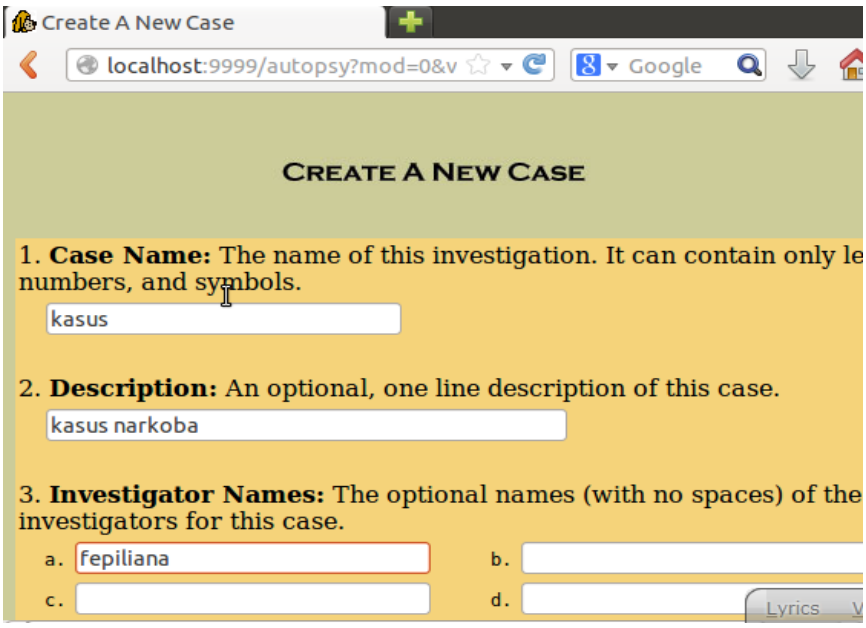


Gambar 6: proses menjalankan **autopsy**

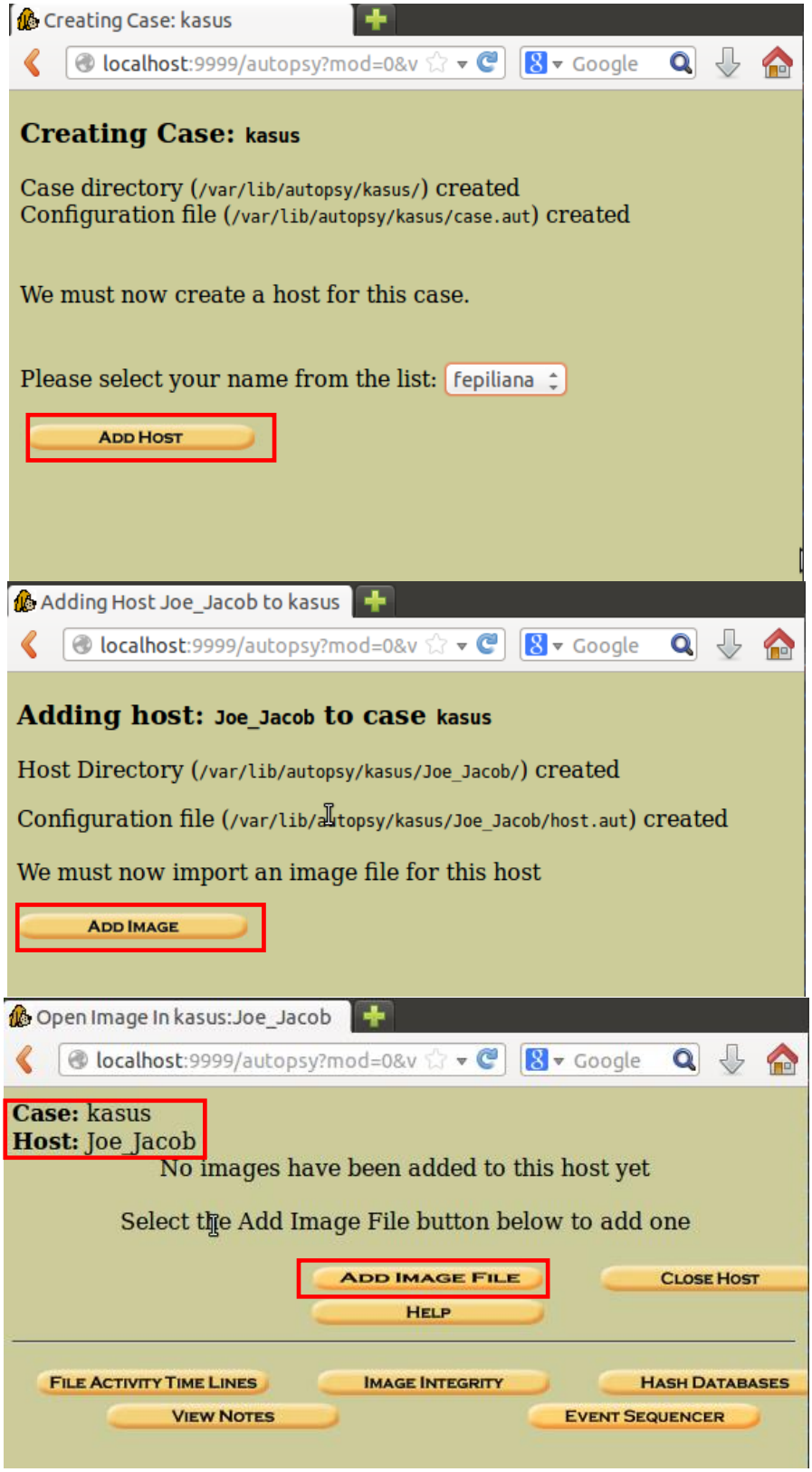


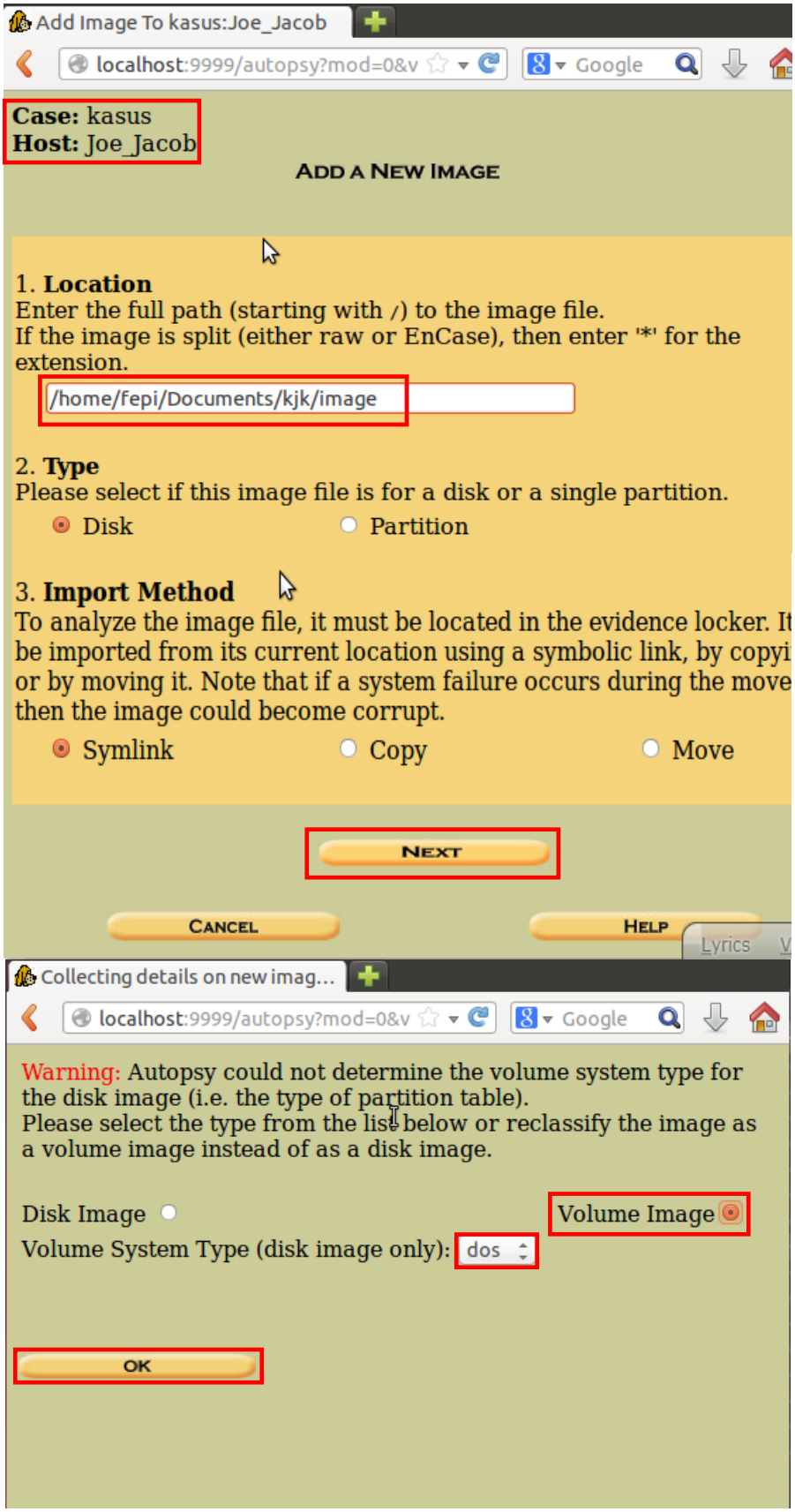
Gambar 7: *interfaces* Autopsy Forensic Browser

Untuk melakukan forensic kita klik **New Case. New** Case berguna untuk menambahkan kasus penyelidikan baru.

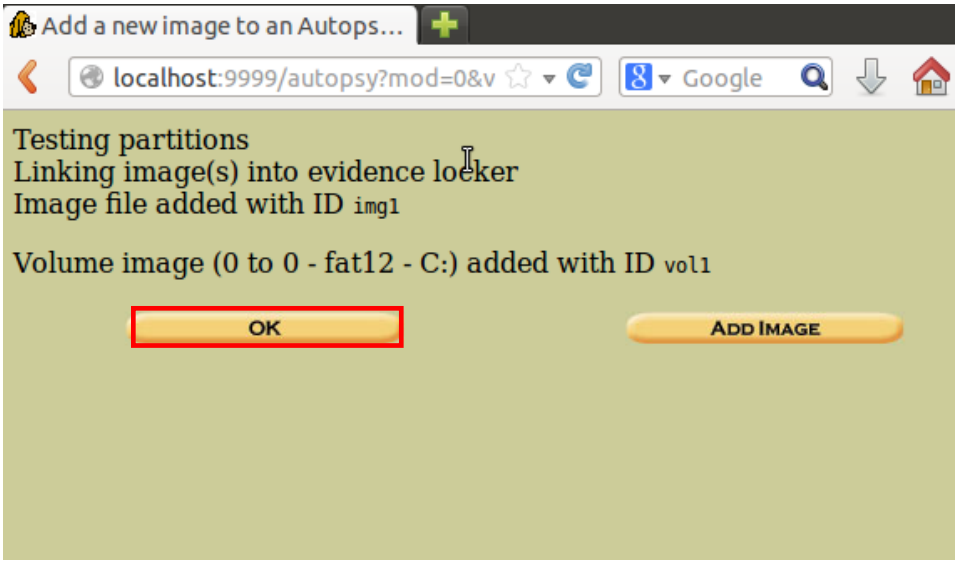


Gambar 8: tampilan laman New Case

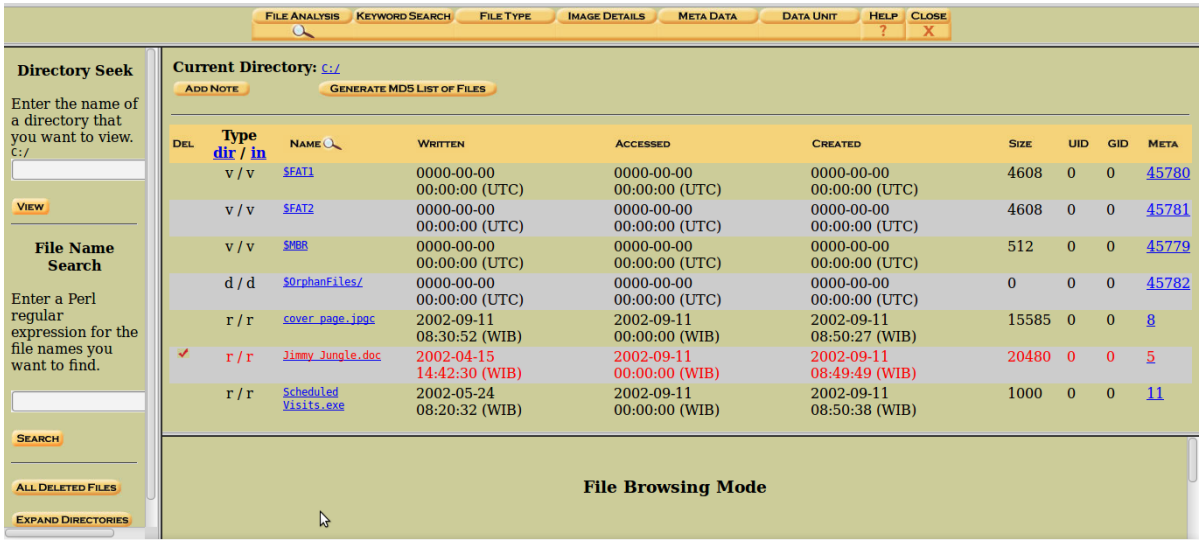

Creating Case: kasus
localhost:9999/autopsy?mod=0&v
Google
Creating Case: kasus
Case directory (/var/lib/autopsy/kasus/) created
Configuration file (/var/lib/autopsy/kasus/case.aut) created
We must now create a host for this case.
Please select your name from the list: fepiliana
ADD HOST
Adding Host Joe_Jacob to kasus
localhost:9999/autopsy?mod=0&v
Google
Adding host: Joe_Jacob to case kasus
Host Directory (/var/lib/autopsy/kasus/Joe_Jacob/) created
Configuration file (/var/lib/autopsy/kasus/Joe_Jacob/host.aut) created
We must now import an image file for this host
ADD IMAGE
Open Image In kasus:Joe_Jacob
localhost:9999/autopsy?mod=0&v
Google
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

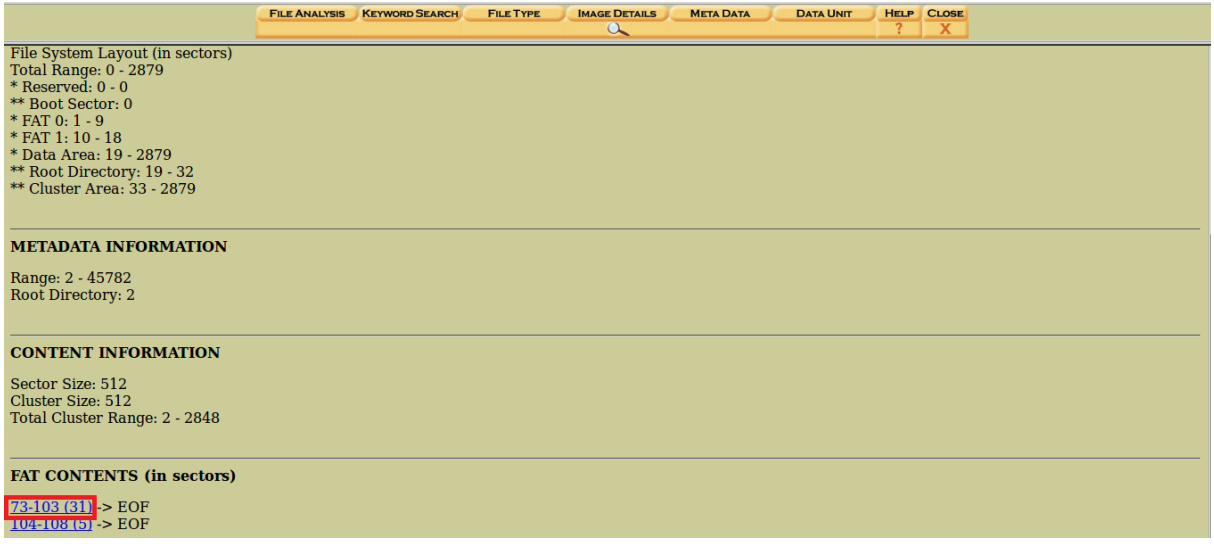

Add Image To kasus:Joe_Jacob
localhost:9999/autopsy?mod=0&v
Google
Case: kasus
Host: Joe_Jacob
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/fepi/Documents/kjk/image
2. Type
Please 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 be imported from its current location using a symbolic link, by copyi 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 imag...
localhost:9999/autopsy?mod=0&v
Google
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

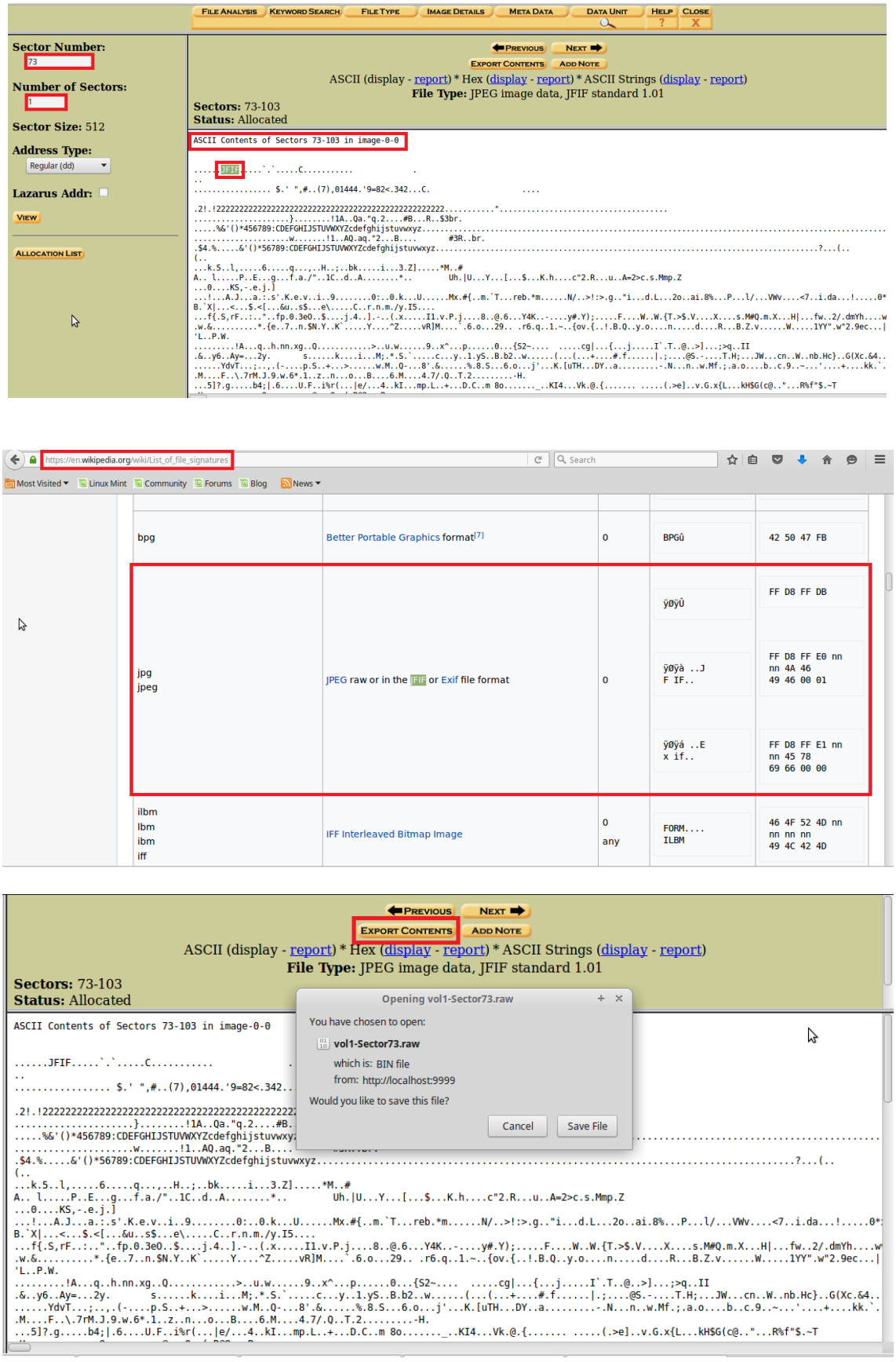

Collecting details on new imag...
localhost:9999/autopsy?mod=0&v
Google
Image File Details
Local Name: images/image
Data Integrity: An MD5 hash can be used to verify the integrity of t
image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the 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


Add a new image to an Autops...
localhost:9999/autopsy?mod=0&v
Google
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
OK
ADD IMAGE

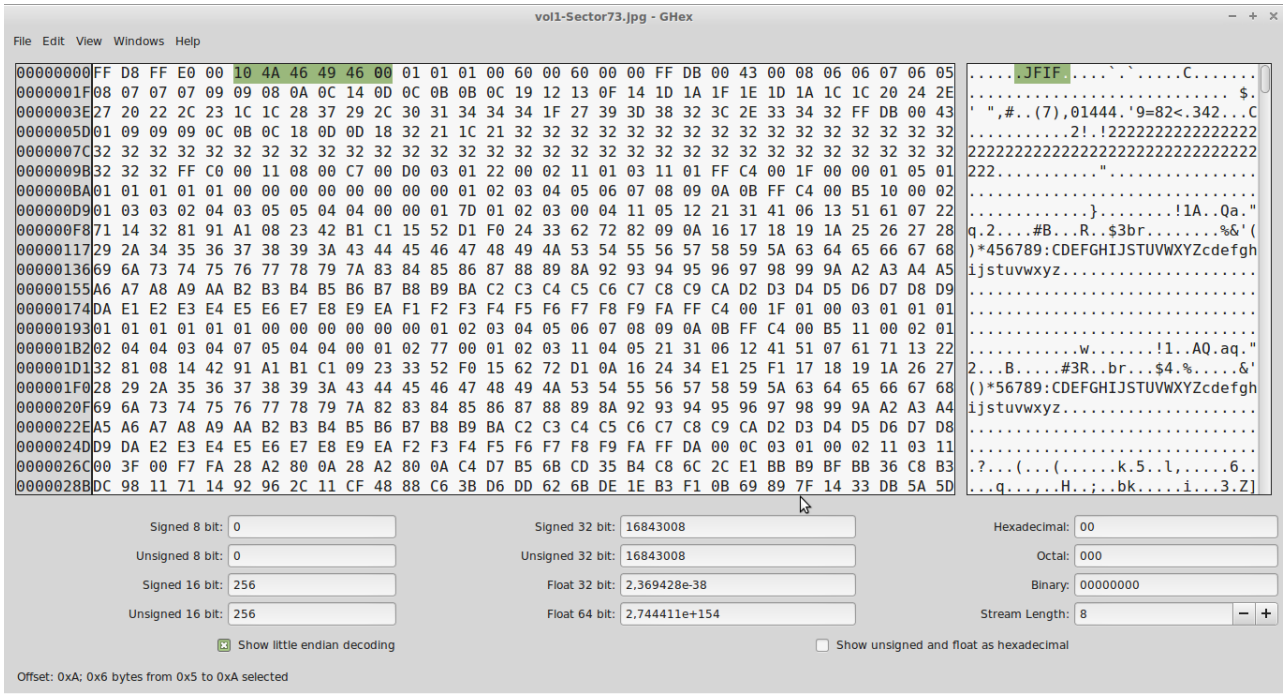

Open Image In kasus:Joe_Jacob
localhost:9999/autopsy?mod=0&v
Google
Case: kasus
Host: Joe_Jacob
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
image-0-0
fat12
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE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


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
File Browsing Mode


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



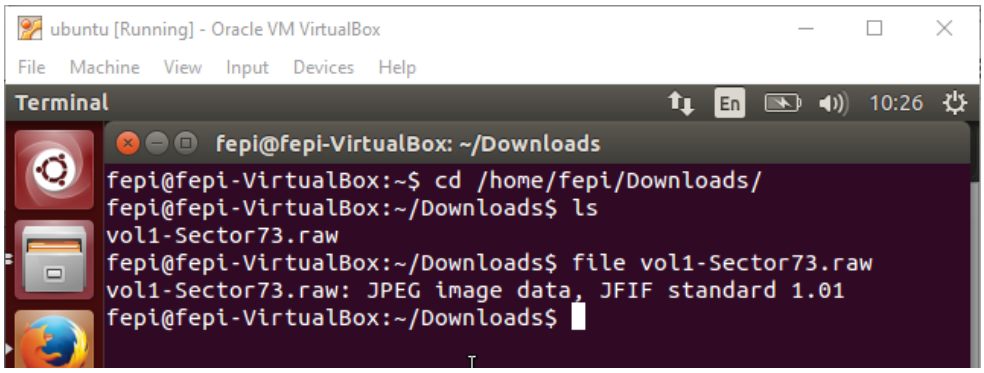
Gambar 9: proses melakukan forensic menggunakan *tools* autopsy



Gambar 10: Tampilan file image ketika dibuka dengan *tools* Ghex.

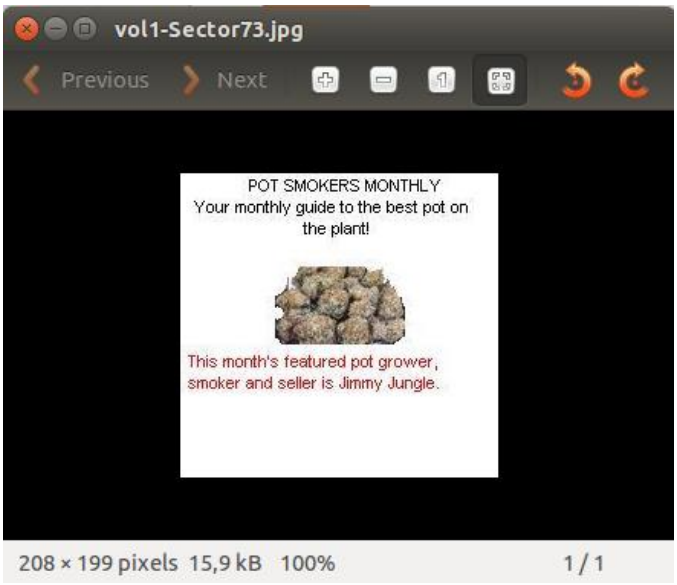
Tools Ghex digunakan untuk melihat file hexa.Berdasarkan dari hasil Fat Contents 73-103 (31) yang telah dilakukan forensic, kita dapat mengetahui bahwa file tersebut memiliki *signature* berupa JFIF (berdasakan kode ASCII). Jika kita telusuri, *signature* JFIF merupakan file yang berekstensi JPG atau JPEG, yang berarti file tersebut merupakan file gambar. Ketika kita klik tombol Export Contents, kita dapat menyimpan file tersebut yang berformat .raw.

Untuk memastikan kembali file **vol1-sector73.raw** tersebut tipenya apa, kita dapat mengetik *command* file **vol1-sector73.raw** pada CMD (lihat gambar 11).



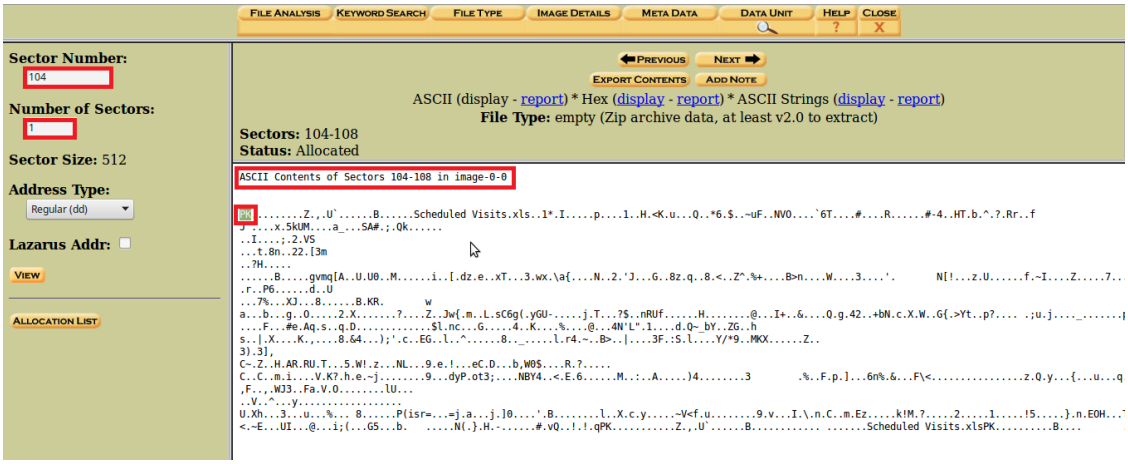
Gambar 11: file **vol1-sector73.raw**

Dari hasil gambar 11, kita dapat mengetahui bahwa memang benar file **vol1-sector73.raw** berekstensi JPEG atau JPG. Untuk melihat gambar dari file **vol1-sector73.raw** kita harus mengubah format file tersebut menjadi vol1-sector73.jpg, agar gambar dari file tersebut dapat kita lihat.

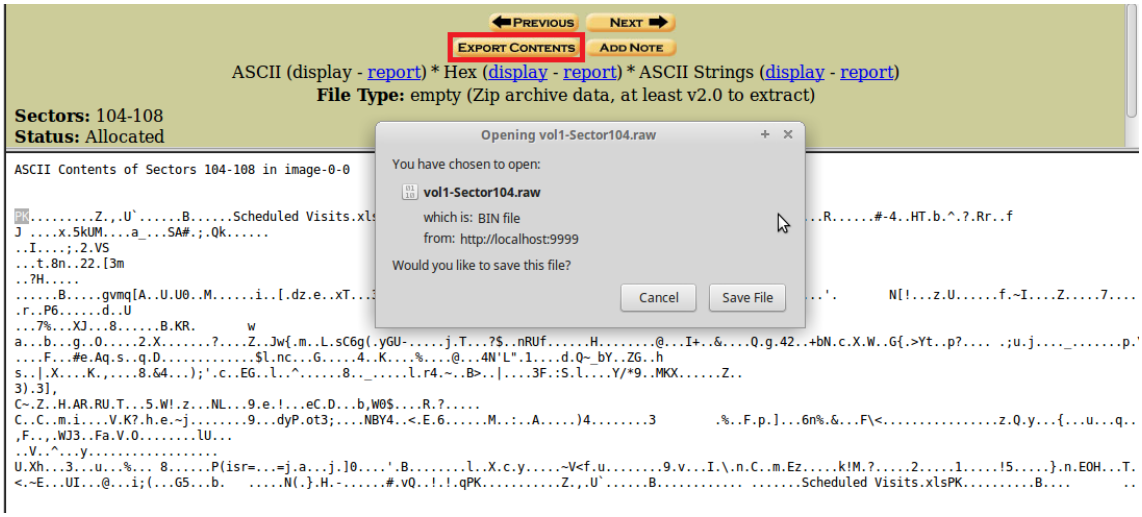


Gambar 12: tampilan **vol1-sector73.jpg**

Setelah melakukan forensic pada Fat Contents 73-103 (31), maka langkah selanjutnya adalah kita lakukan juga forensic pada Fat Contents 104-108 (5) yang masih menggunakan *tools* autopsy. Berikut adalah proses forensic yang dilakukan:

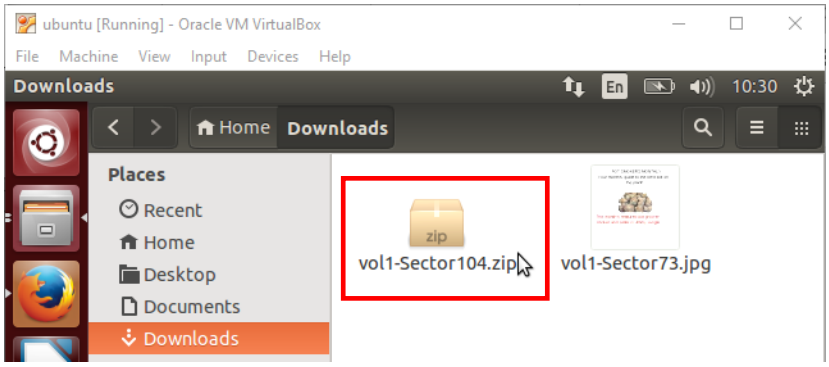


zip jar odt ods odp docx xlsx pptx vsdx apk	zip file format and formats based on it, such as JAR, ODF, OOXML	0	PK..	50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive)
rar	RAR archive version 1.50 onwards[8]	0	Rar!...	52 61 72 21 1A 07 00
rar	RAR archive version 5.0 onwards[9]	0	Rar!....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



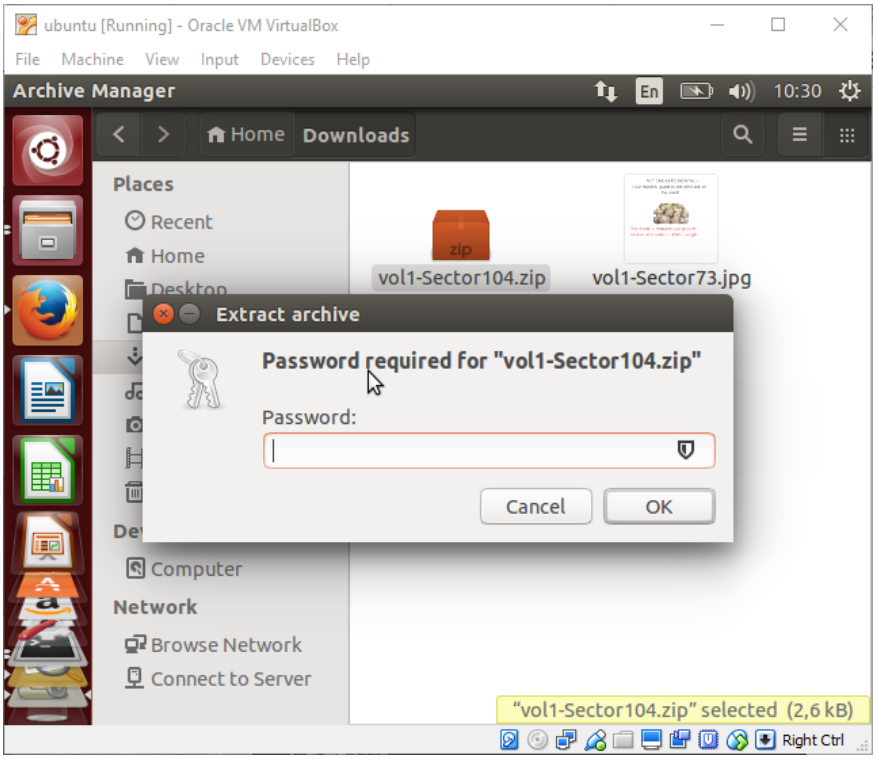
Gambar 13: proses forensic Fat Contents 104-108 (5)

Berdasarkan gambar 13, dapat kita ketahui bahwa file Fat Contents 104-108 (5) memiliki file *signature* berupa PK. Jika kita telusuri, file dengan *signature* PK tersebut merupakan file ekstensi zip, jar, odt, ods, odp, docx, xlxs, pptx, vsdx, dan apk. Untuk mengetahui berupa apa fat contents 104-108 (5), maka kita lakukan export contents. Ketika di export, maka akan muncul file dengan nama **vol1-sector104.raw.** Setelah file **vol1-sector104.raw** kita simpan, tahap selanjutnya adalah kita langsung saja mengubah ekstensi file **vol1-sector104.raw** menjadi **vol1-sector104.zip.**



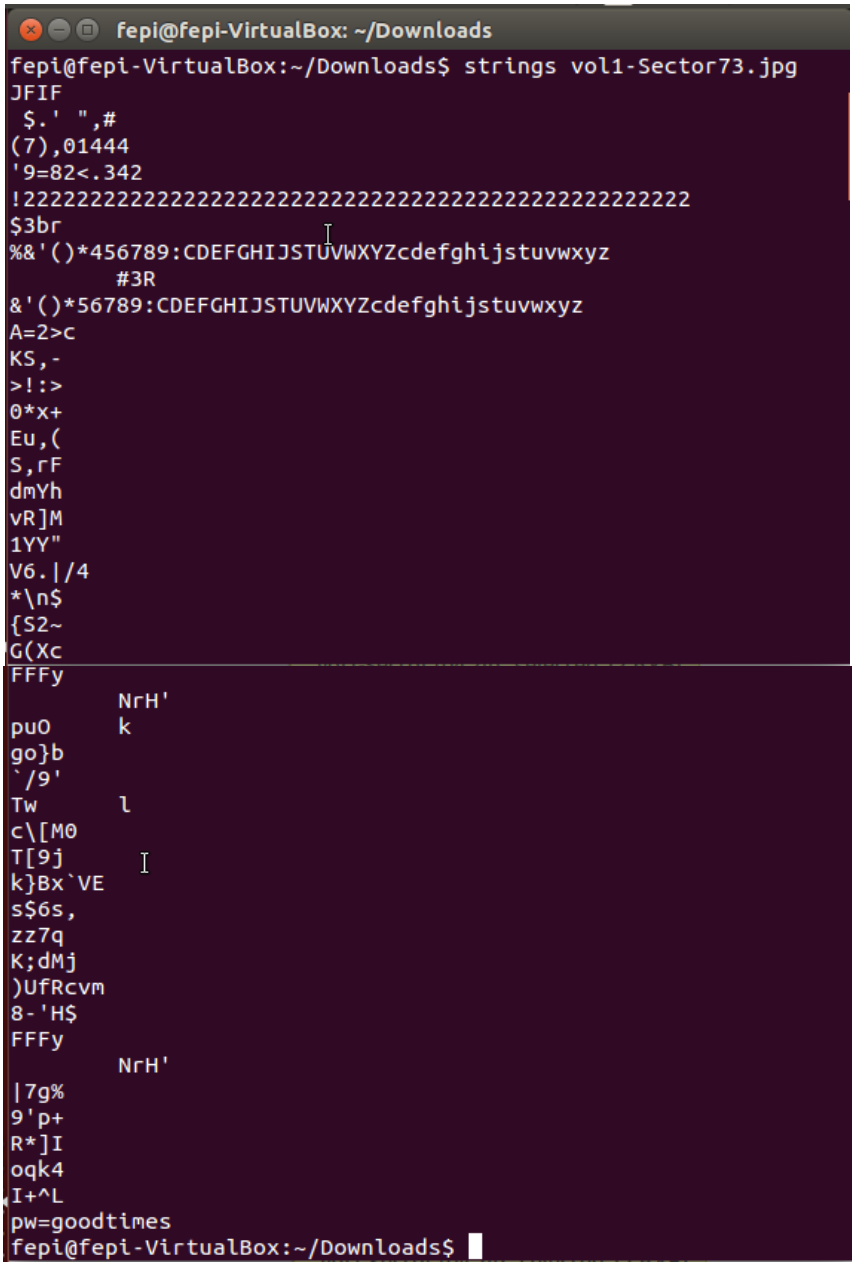
Gambar 14: file **vol1-sector104.zip**

Pada saat file **vol1-sector104.zip** ingin kita ekstrak, maka vol1-sector104.zip tidak dapat kita ekstrak karena file tersebut diamankan dengan password.



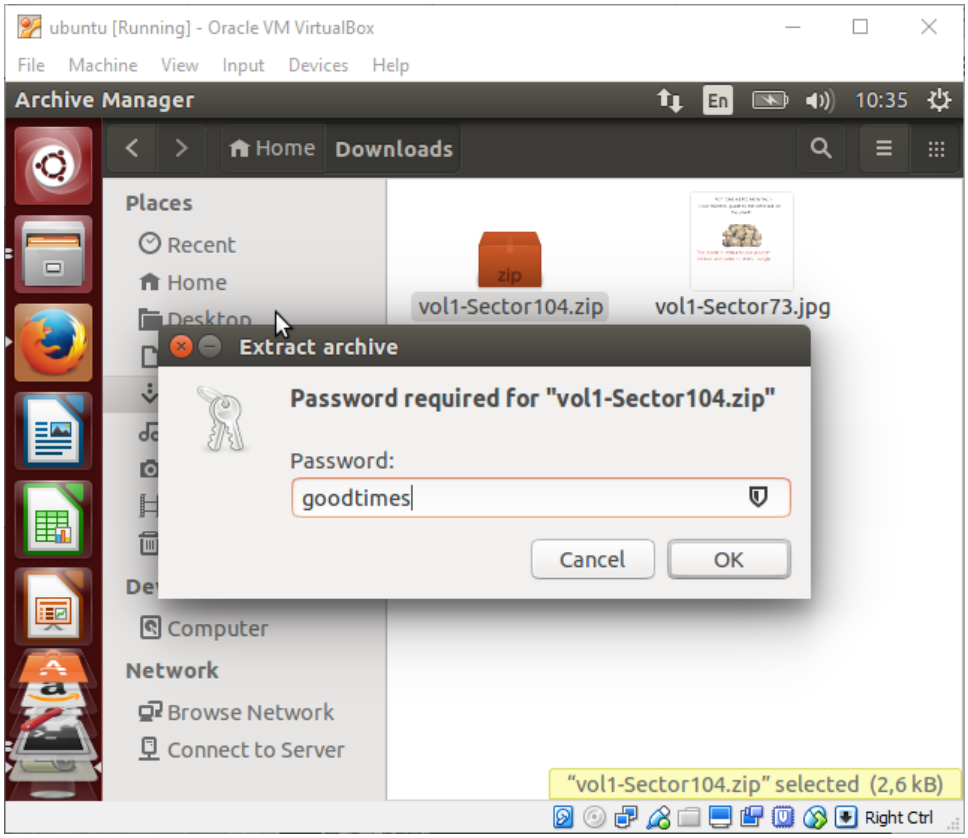
Gambar 15: file **vol1-sector104.zip** diamankan menggunakan password.

Kita tidak dapat mengetahui apa password dari file **vol1-sector104.zip** tersebut, tetapi kita dapat menganalisa bahwa ada kemungkinan tersangka bandar narkoba menyembunyikan passwordnya pada gambar **vol1-sector73.jpg.** Untuk mengetahui apakah ada karakter unik atau tidak pada gambar tersebut, maka kita gunakan *tools* strings. Untuk menjalankan strings kita ketik *command* pada CMD : **$ strings vol1-sector73.jpg.** Strings merupakan *tools* aplikasi yang berfungsi untuk melihat karakter pada sebuah file.

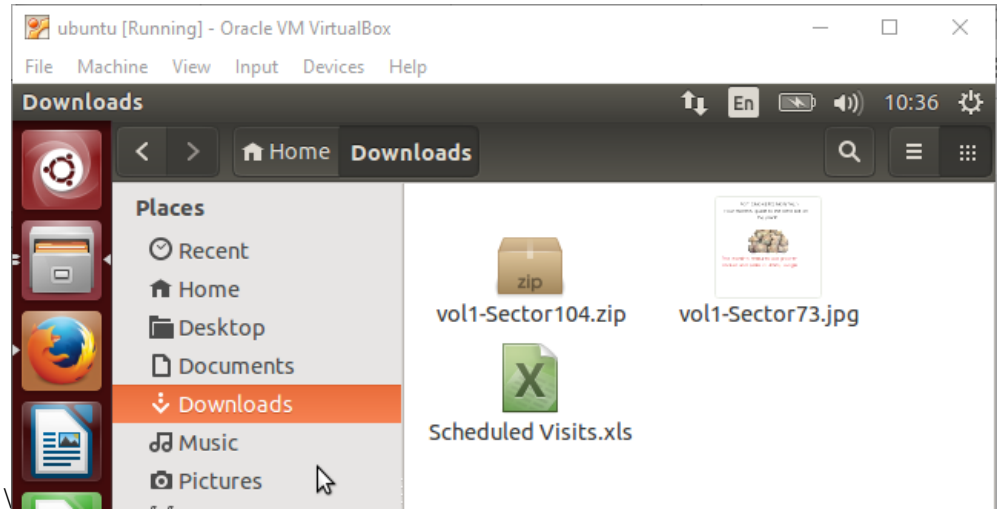


Gambar 16: proses menjalankan *tools* stings.

Berdasarkan gambar 16, kita telah mendapatkan klue bahwa pw=goodtimes. Jika kita ketik di file **vol1-sector104.zip,** dapat kita lihat bahwa file tersebut berisi file excel **Scheduled Visit.xls.**

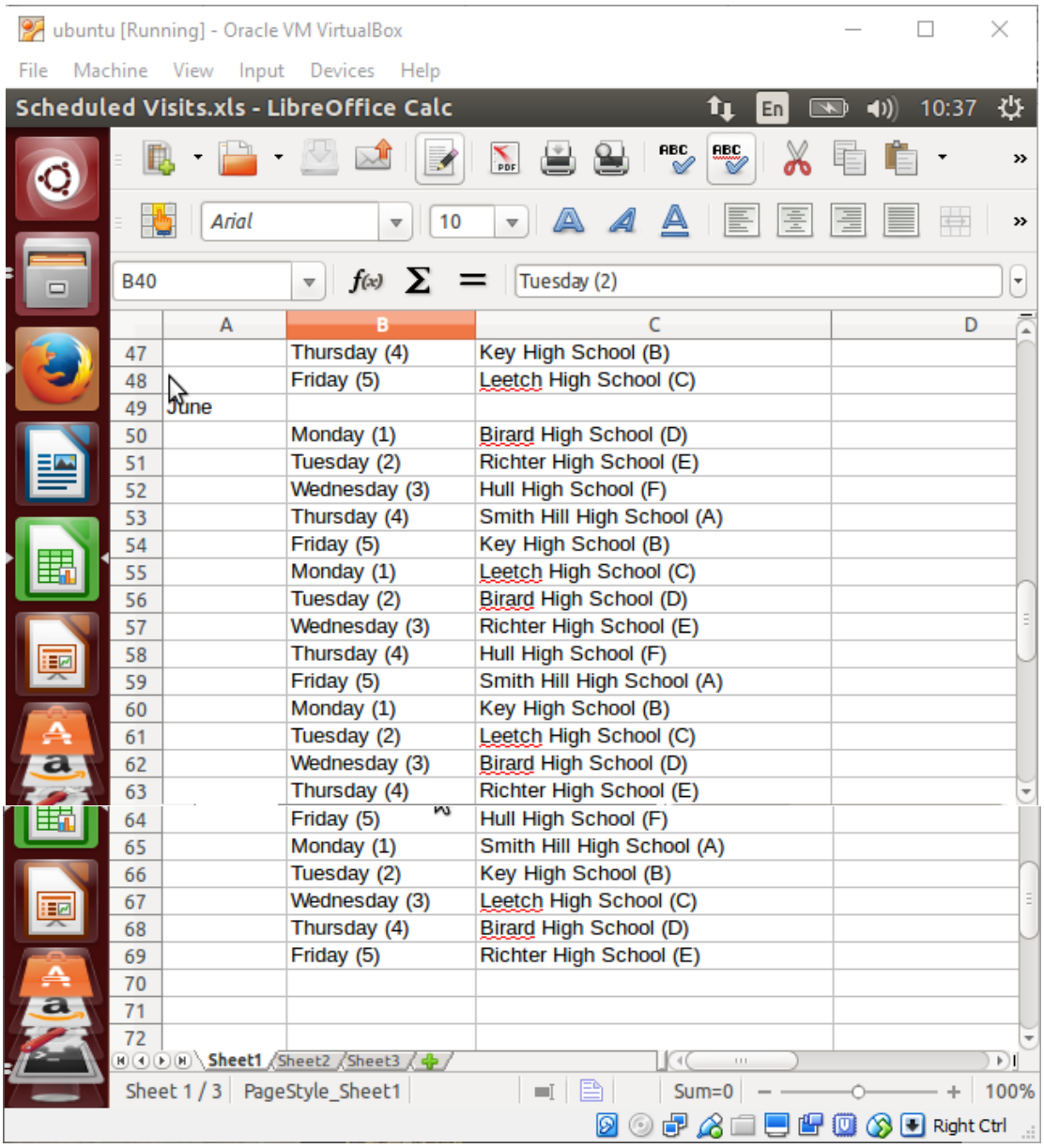


Gambar 17: memasukan password “goodtimes”



Gambar 18: file excel **Scheduled Visit.xls** hasil ekstrak vol-sector104.zip

	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)	
30		Tuesday (2)	Leetch High School (C)	
31		Wednesday (3)	Birard High School (D)	
32		Thursday (4)	Richter High School (E)	
33		Friday (5)	Hull High School (F)	
34		Monday (1)	Smith Hill High School (A)	
35		Tuesday (2)	Key High School (B)	
36		Wednesday (3)	Leetch High School (C)	
37		Thursday (4)	Birard High School (D)	
38		Friday (5)	Richter High School (E)	
39		Monday (1)	Hull High School (F)	
40		Tuesday (2)	Smith Hill High School (A)	
41		Wednesday (3)	Key High School (B)	
42		Thursday (4)	Leetch High School (C)	
43		Friday (5)	Birard High School (D)	
44		Monday (1)	Richter High School (E)	
45		Tuesday (2)	Hull High School (F)	
46		Wednesday (3)	Smith Hill High School (A)	
47		Thursday (4)	Key High School (B)	



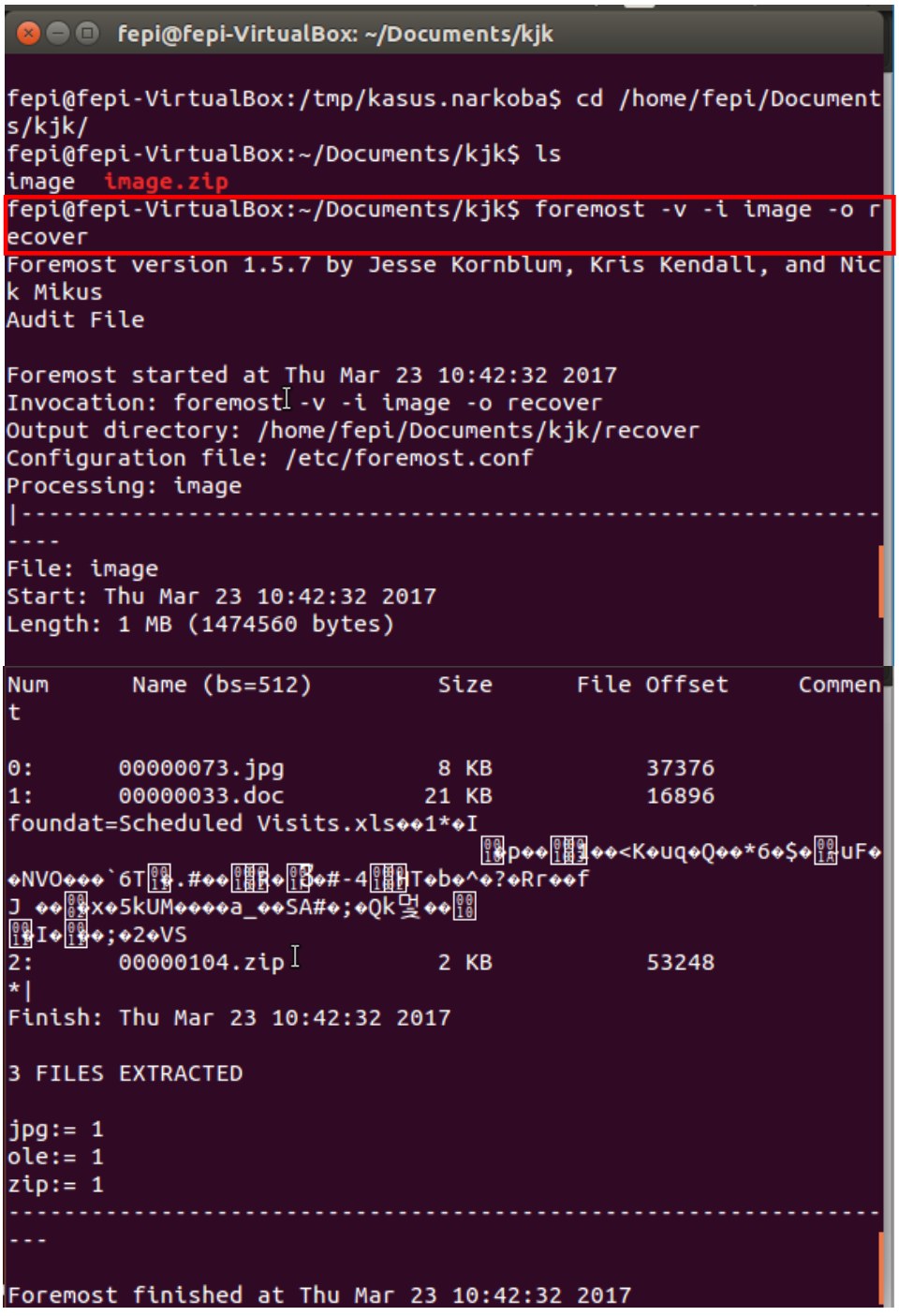
	A	B	C	D
47		Thursday (4)	Key High School (B)	
48		Friday (5)	Leetch High School (C)	
49	June			
50		Monday (1)	Birard High School (D)	
51		Tuesday (2)	Richter High School (E)	
52		Wednesday (3)	Hull High School (F)	
53		Thursday (4)	Smith Hill High School (A)	
54		Friday (5)	Key High School (B)	
55		Monday (1)	Leetch High School (C)	
56		Tuesday (2)	Birard High School (D)	
57		Wednesday (3)	Richter High School (E)	
58		Thursday (4)	Hull High School (F)	
59		Friday (5)	Smith Hill High School (A)	
60		Monday (1)	Key High School (B)	
61		Tuesday (2)	Leetch High School (C)	
62		Wednesday (3)	Birard High School (D)	
63		Thursday (4)	Richter High School (E)	
64		Friday (5)	Hull High School (F)	
65		Monday (1)	Smith Hill High School (A)	
66		Tuesday (2)	Key High School (B)	
67		Wednesday (3)	Leetch High School (C)	
68		Thursday (4)	Birard High School (D)	
69		Friday (5)	Richter High School (E)	
70				
71				
72				

Gambar 19: isi file **Scheduled Visit.xls**

Dari hasil gambar 19, kita dapat mengetahui bahwa Joe Jacob mengedarkan narkoba diberbagai sekolah. Data yang disajikan merupakan data dari bulan april s.d. juni 2002.

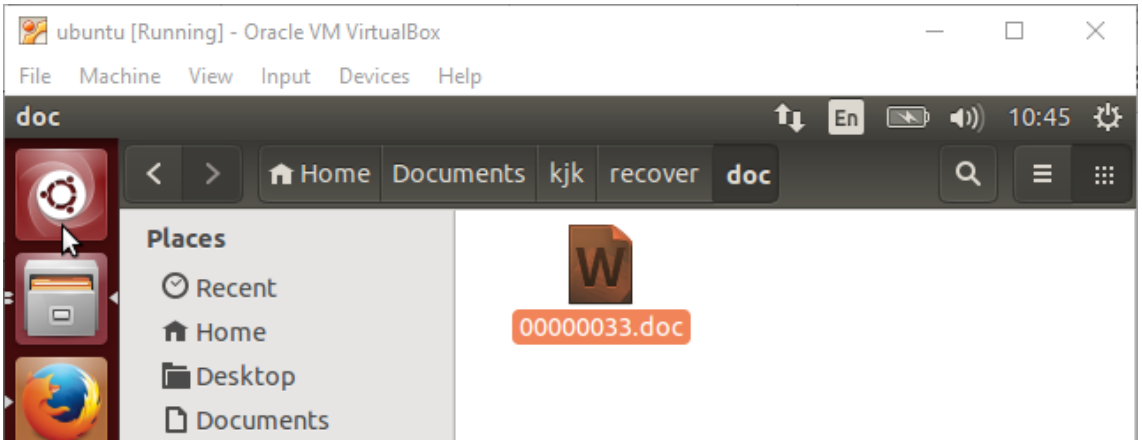
Sebelumnya kita telah mengetahui bahwa terdapat file yang telah dihapus, untuk melakukan forensic selanjutnya kita gunakan *tools* **foremost** untuk merecover file yang telah dihapus itu. Berikut adalah langkah-langkah menggunakan *tools* foremost :

Menjalankan perintah foremost, kita gunakan perintah **$ foremost –v –l image –o recover.**



Gambar 20: proses menjalankan *tools* foremost.

Setelah menjalankan *tools* foremost, pada direktori **kjk,** terdapat direktori baru yang bernama recover. Dalam direktori tersebut terdapat sebuah dokumen .doc.



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

Gambar 21: isi dokumen yang berektensi .doc pada direktori recover.

Berdasarkan gambar 21, kita dapat mengetahui bahwa dokumen tersebut merupakan sebuah surat yang ditujukan untuk Jimmy Jungle dari Joe Jacob.

Untuk informasi penyidikan, berikut adalah informasi-informasi yang diperlukan berdasarkan hasil forensic.

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, Jungle, NY 11111

2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
   - Data penting tersebut ada pada file **vol-Sector73.jpg** dan **vol-Sector104.zip**, dimana file-file berisi informasi list sekolah-sekolah yang terdapat konsumen narkoba.

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?
   - File yang berisi jadwal kunjungan Joe Jacob ke sekolah-sekolah dibuat dalam file **vol-sector104.zip**, kemudian file tersebut diamankan menggunakan password yang diselipkannya pada gambar **vol-sector73.jpg**.

5. What processes did you (the investigator) use to successfully examine the entire contents?
   - file **vol1-sector73.raw** berekstensi JPEG atau JPG. Untuk melihat gambar dari file **vol1-sector73.raw** kita harus mengubah format file tersebut menjadi **vol1-sector73.jpg,** agar gambar dari file tersebut dapat kita lihat.

tampilan **vol1-sector73.jpg**

- Menggunakan *tools* String **$ strings vol1-sector73.jpg** untuk mendapatkan password: goodtimes, dimana password tersebut digunakan untuk mengamankan file **vol1-sector104.zip.** Setelah diekstrak, file **vol1-sector104.zip** berisikan dokumen tentang list sekolah tempat transaksi narkobanya. Isi dokumen dapat dilihat pada gambar 19.
- Menggunakan *tools* foremost untuk merecovery file yang telah dihapus. Hasil dari recovery tersebut berisi sebuah surat yang ditulis Joe Jacob untuk Jimmy Junggle.

DAFTAR PUSTAKA

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

[2] F. Sulianta, "Komputer Forensik," 2008.