

Komputer Forensik

Komputer forensik dapat didefinisikan sebagai 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 dari komputer forensik ini sendiri yaitu :

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi atau entitas berbasis digital atau elektronik sehingga dapat dipergunakan sebagai alat bukti 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 motivasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan yang melanggar hukum tersebut.

Sedangkan beberapa manfaat komputer forensik ini sendiri adalah :

1. Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yg 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 di bagi menjadi 3 kategori, diantaranya :

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 penyimpanan 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: file yang telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya.

Dalam melakukan forensik atau penyelidikan harus memiliki ketentuan objek, objek forensik diantaranya :

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 atau informasi backup dari sistem utama
5. Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya
6. Beraneka ragam jenis 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)
8. Absensi akses server atau komputer yang dikelola oleh sistem untuk merekam setiap adanya pengguna yang login ke piranti terkait; dan lain sebagainya.

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 penyidik 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 atau 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. Pemindehan 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-barang 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 aktivitas 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; dan
14. Penyertaan dalam proses pengadilan merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi.

Pada tugas komputer forensik ini, kami diberi kasus dan cara memecahkan kasus tersebut. Dibawah ini merupakan kasus yang diberikan pada tugas ini :

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 forensik 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?

Tools yang digunakan ada empat, diantaranya :

1. Autopsy
2. Foremost
3. Strings
4. Ghex

Langkah-langkah dalam menyelesaikan kasus diatas dan untuk mendapatkan informasinya adalah sebagai berikut:

1. Menginstall tools yang digunakan, dimana tools yang digunakan adalah :
 - Autopsy browser : merupakan antarmuka grafis yang digunakan untuk tool analisis investigasi digital perintah baris The Sleuth Kit.
 - Foremost : merupakan aplikasi berbasis terminal yang berfungsi untuk mengembalikan (recover) file yang hilang (terhapus maupun tertimpa dengan file lain).
 - Strings : merupakan aplikasi yang berfungsi untuk melihat karakter readable pada sebuah file.
 - Ghex : merupakan aplikasi yang digunakan untuk mengkonvert atau mengubah file teks ke file hexa.
2. Download file di (<http://old.honeynet.org/scans/scan24>) , setelah file image.zip didownload maka dicek keaslian file tersebut seperti yang ditampilkan pada gambar 1.

```
srisuryani-Aspire-4739 Unduhan # md5sum image.zip  
b676147f63923e1f428131d59b1d6a72 image.zip  
srisuryani-Aspire-4739 Unduhan # █
```

Gambar 1. Tampilan ketika mengecek keaslian file image.zip

3. Langkah selanjutnya melihat type file pada image.zip seperti gambar 2. Dimana pada gambar 2 terlihat type file tersebut adalah DOS floppy 1440k, x86 hard disk boot sector.

```
srisuryani-Aspire-4739 Unduhan # file image  
image: DOS floppy 1440k, x86 hard disk boot sector  
srisuryani-Aspire-4739 Unduhan # █
```

Gambar 2. Tampilan ketika melihat type file image

4. Membuat folder dengan nama kasus.narkoba seperti yang ditampilkan pada gambar 3, setelah itu file image pada folder di mounting.

```
srisuryani-Aspire-4739 Unduhan # mkdir /tmp/kasus.narkoba/
srisuryani-Aspire-4739 Unduhan # mount image /tmp/kasus.narkoba/
srisuryani-Aspire-4739 Unduhan #
```

Gambar 3. Tampilan ketika membuat folder dan mounting file image pada folder tersebut.

5. Selanjutnya masuk dalam direktori folder yang telah dibuat, dan mengecek isi folder tersebut seperti yang ditampilkan pada gambar 4. Dimana pada folder kasus.narkoba terdapat dua tipe file yaitu file jpg dan file exe.

```
srisuryani-Aspire-4739 Unduhan # cd /tmp/kasus.narkoba/
srisuryani-Aspire-4739 kasus.narkoba # ls
cover page.jpgc          SCHEDU~1.EXE
srisuryani-Aspire-4739 kasus.narkoba #
```

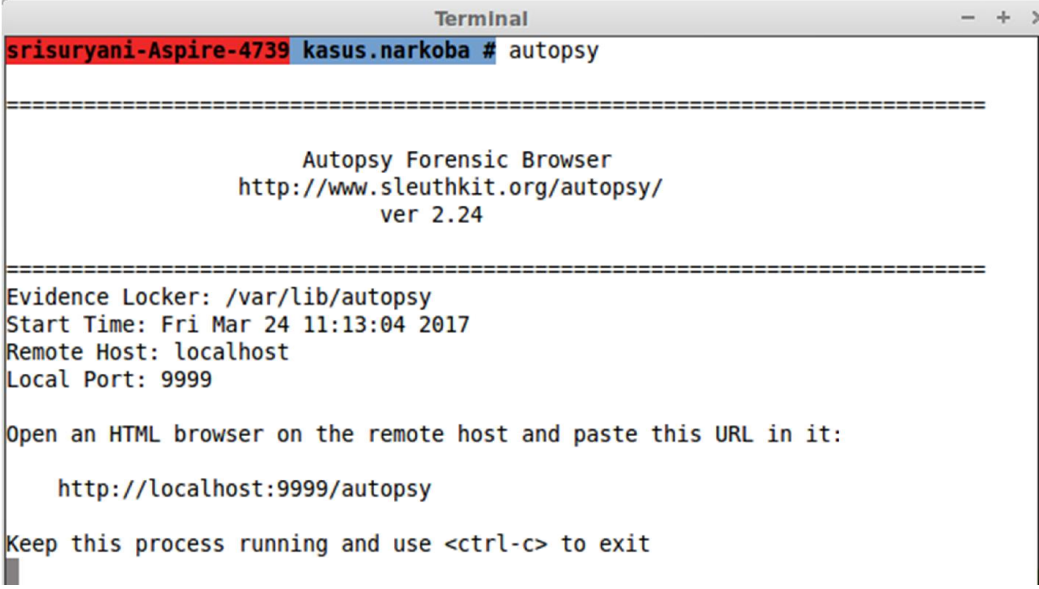
Gambar 4. Tampilan ketika melihat isi file pada folder kasus.narkoba

6. Melakukan pengecekan semua isi file, gambar 5 merupakan tampilan ketika melihat semua isi pada direktori.

```
srisuryani-Aspire-4739 kasus.narkoba # file *
cover page.jpgc          : ERROR: cannot read `cover page.jpgc' (Inp
ut/output error)
SCHEDU~1.EXE:           Zip archive data, at least v2.0 to extract
srisuryani-Aspire-4739 kasus.narkoba #
```

Gambar 5. Tampilan ketika melihat isi file pada direktori folder kasus.narkoba

- Langkah selanjutnya me-running autopsy pada terminal agar localhost:9999/autopsy dapat diakses pada browser. Gambar 6 dan 7 merupakan tampilan autopsy diterminal dan tampilan awal pada saat akses di browser.



```
Terminal
srisuryani-Aspire-4739 kasus.narkoba # autopsy

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

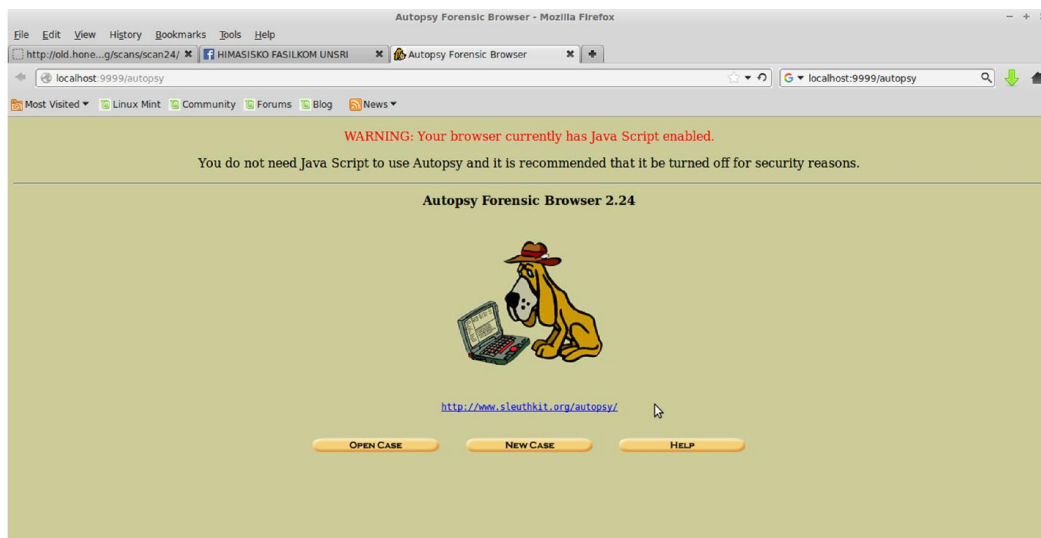
Evidence Locker: /var/lib/autopsy
Start Time: Fri Mar 24 11:13:04 2017
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

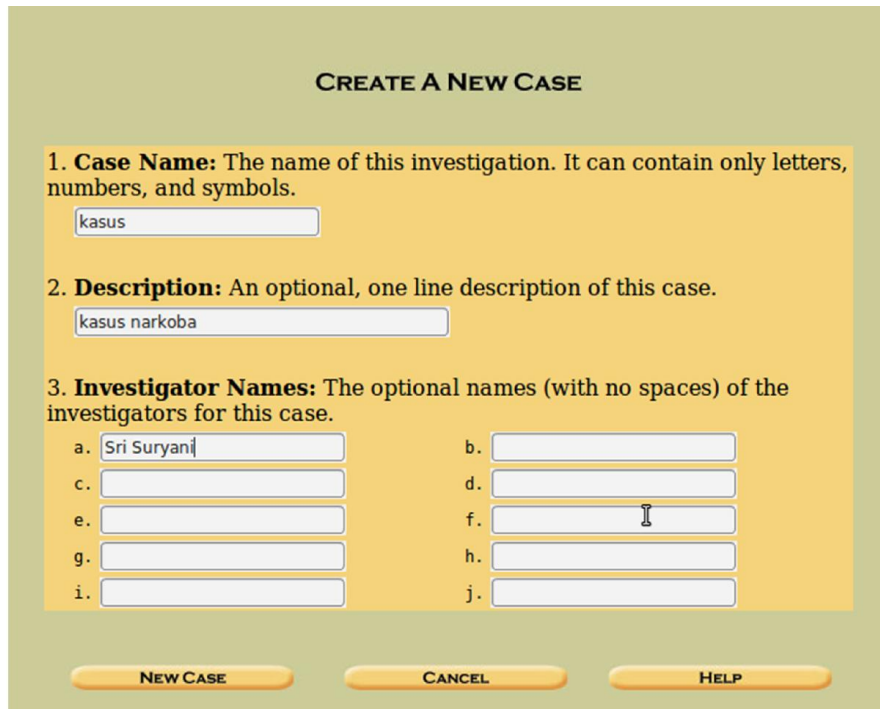
Keep this process running and use <ctrl-c> to exit
```

Gambar 6. Tampilan ketika akses autopsy diterminal



Gambar 7. Tampilan awal autopsy ketika dibrowser.

8. Selanjutnya membuat case baru atau klik *new case*, dan mengisi *case name*, *description* serta *investigator names* seperti gambar 8. Gambar 9 merupakan tampilan ketika telah berhasil membuat case baru dan langkah selanjutnya membuat host atau menambahkan host.



CREATE A NEW CASE

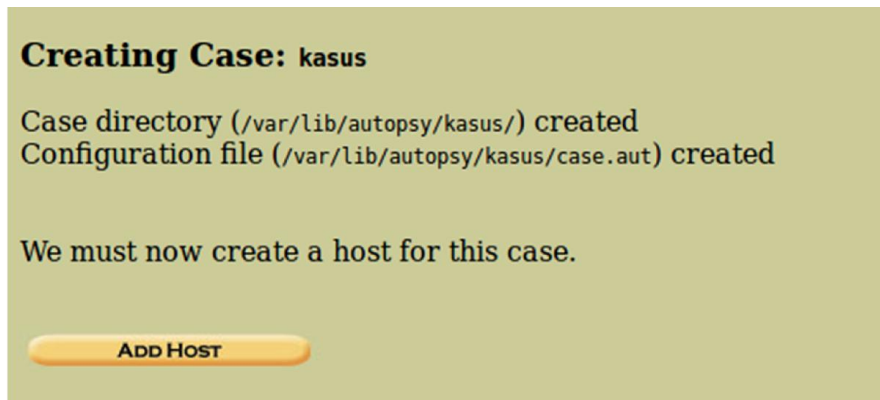
1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

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

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

a.	<input type="text" value="Sri Suryani"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

Gambar 8. Tampilan ketika membuat *new case*



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.

Gambar 9. Tampilan ketika berhasil membuat case baru dan selanjutnya *add host*.

9. Gambar 10 merupakan tampilan ketika akan menambahkan host, dan pada tugas ini nama hostnya adalah joe jacob.

ADD A NEW HOST

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

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

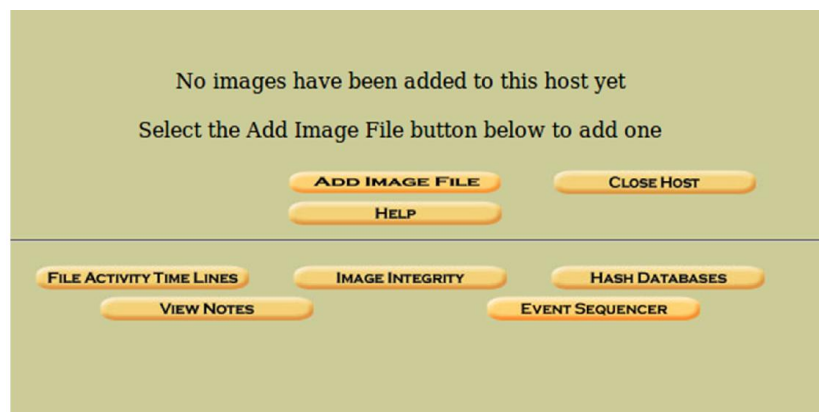
3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

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.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

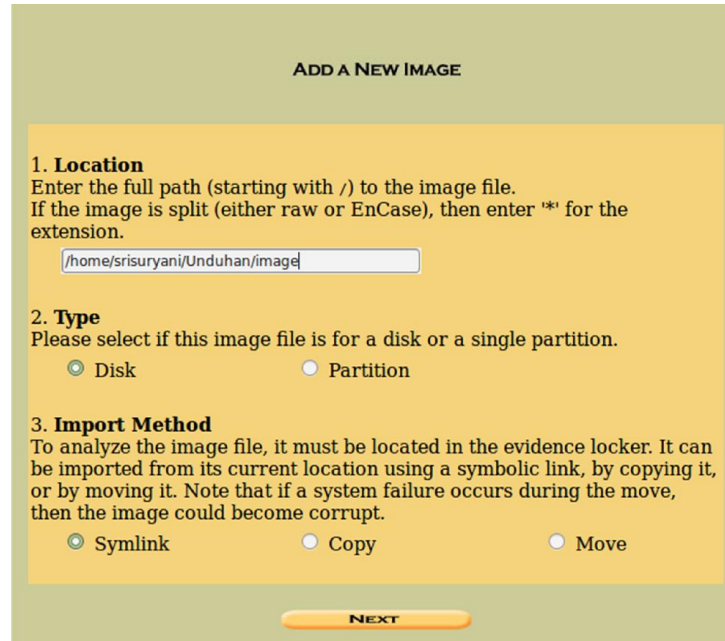
Gambar 10. Tampilan ketika menambahkan host pada autopsy browser.

10. Gambar 11 tampilan ketika telah berhasil menambahkan host dan selanjutnya klik add image file.

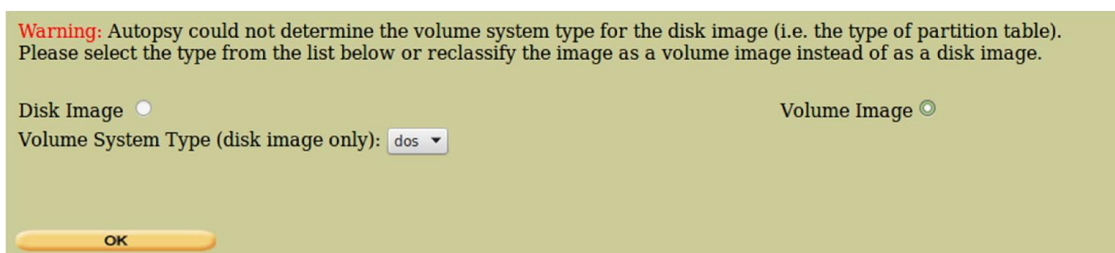


Gambar 11. Tampilan ketika telah berhasil menambahkan host

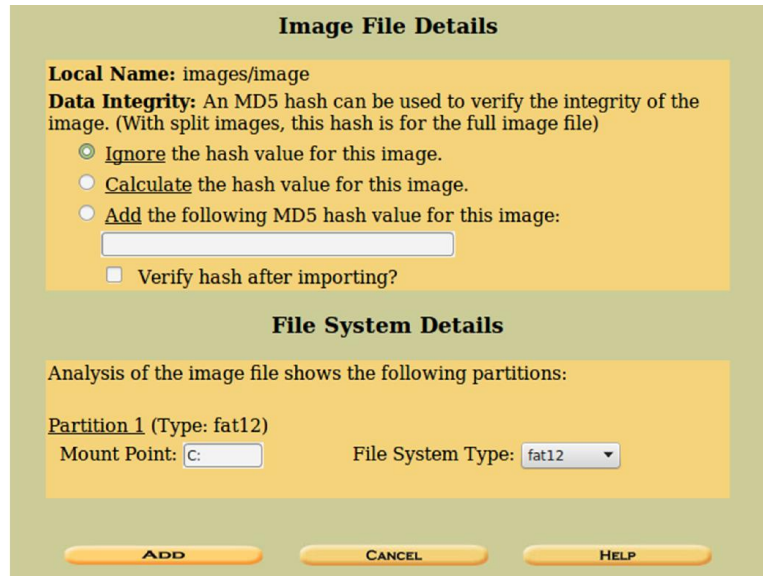
11. Gambar 12, 13, 14, 15, dan 16 merupakan langkah ketika menambahkan file image dan telah selesai membuat *new case*.



Gambar 12. Tampilan ketika menambahkan file image



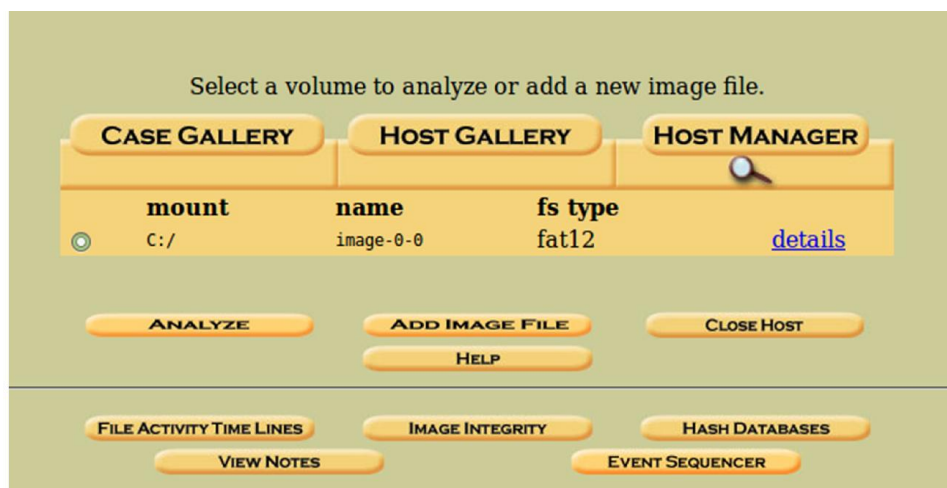
Gambar 13. Tampilan ketika memilih type file



Gambar 14. Tampilan ketika telah menambahkan file image dan pada tahap ini tidak ada yang diubah atau ditambahkan.

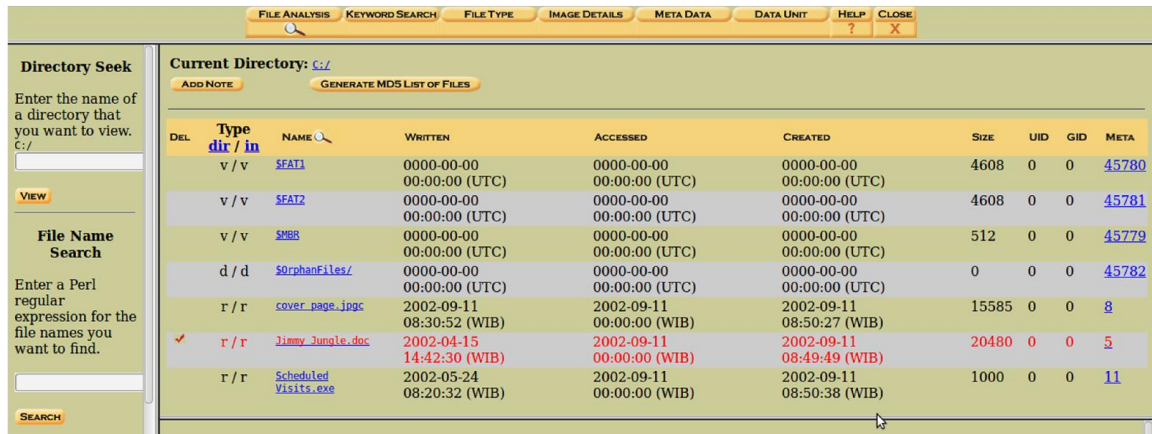


Gambar 15. Tampilan ketika telah selesai menambahkan file image dan klik OK.



Gambar 16. Tampilan ketika telah selesai membuat case baru.

12. Pada gambar 17 dan 18 terdapat tampilan file analisis, dimana file analisis tersebut memiliki nilai-nilai yang berbeda, misalnya waktu file dibuat, dimodifikasi, dihapus, diakses, identifikasi pengguna (user), dan atribut filenya.



The screenshot shows a file analysis tool interface with a menu bar (FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, CLOSE) and a toolbar (ADD NOTE, GENERATE MDS LIST OF FILES). The main area displays a table of file analysis results for the current directory C:/.

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	SEAT1	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	SEAT2	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	SMBR	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	SorphanFiles/	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

Gambar 17. Tampilan file analisis pada autopsy



The screenshot shows the metadata details for file entry 11. The interface includes a menu bar (FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, CLOSE) and a toolbar (REPORT, VIEW CONTENTS, EXPORT CONTENTS, ADD NOTE). The main area displays the following information:

Dir Entry Number: 11

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

MD5 of content: 082a5cc64deea22a3a580ffb5a6fa66 -

SHA-1 of content: c8e7f25380d63c9034d9f27faab29de1f09240b5 -

Details:

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

Directory Entry Times:
 Written: Fri May 24 08:20:32 2002
 Accessed: Wed Sep 11 00:00:00 2002
 Created: Wed Sep 11 08:50:38 2002

Sectors:
[104](#) [105](#)

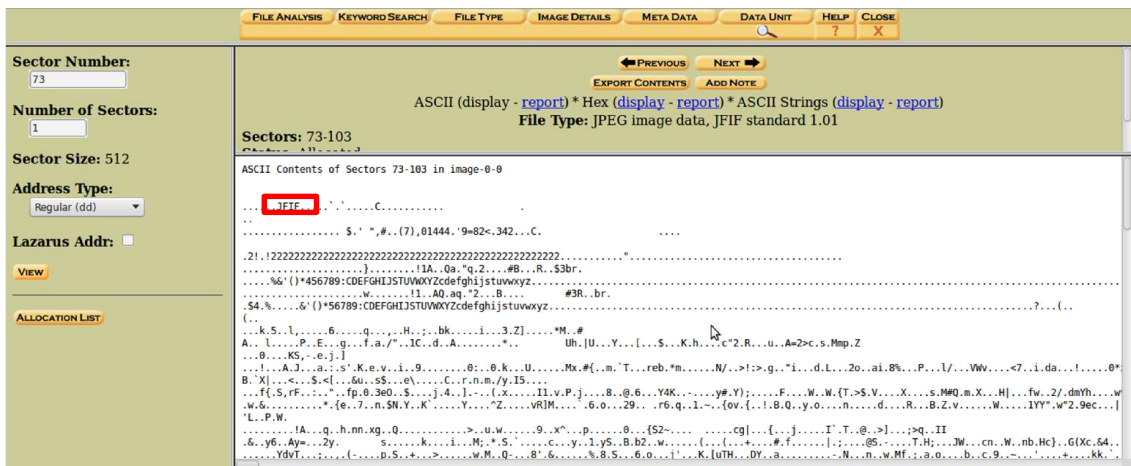
Gambar 18. Tampilan ketika melihat metadata 11 pada file analisis

13. Metadata Analysis merupakan penjelajahan untuk mencari variabel yang tidak terlihat, sehingga mendapatkan penjelasan meta secara detail dari file (document / gambar / audio / video) dan mengakses variabel tidak terlihat untuk terakhir kali saat data diakses jika saja data tersebut direvisi atau diproduksi sampai dengan penggunaan aplikasi untuk produksi file tersebut. Gambar 19 merupakan tampilan dari metadata analisis, dimana pada metadata analisis terdapat dua file yang akan dianalisa.



Gambar 19. Tampilan metadata pada autopsy

14. File 73-103 (31) -> EOF merupakan file jpg, karena isi pada file tersebut terdapat JFIF, dimana ketika JFIF tersebut dicari pada list of file signature (wikipedia) maka akan terindikasi file jpg atau jpeg seperti pada gambar 20 dan 21.



Gambar 20. Tampilan isi pada file 73-103 (31) pada autopsy

jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿøÿÜ	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

Gambar 21. Tampilan list of file signature pada wikipedia untuk melihat type file JFIF.

15. Langkah selanjutnya adalah mengekspor konten pada file 73-103 (31), dan melihat tipe file pada voll-sector73.raw seperti yang ditampilkan pada gambar 22 dan 23.

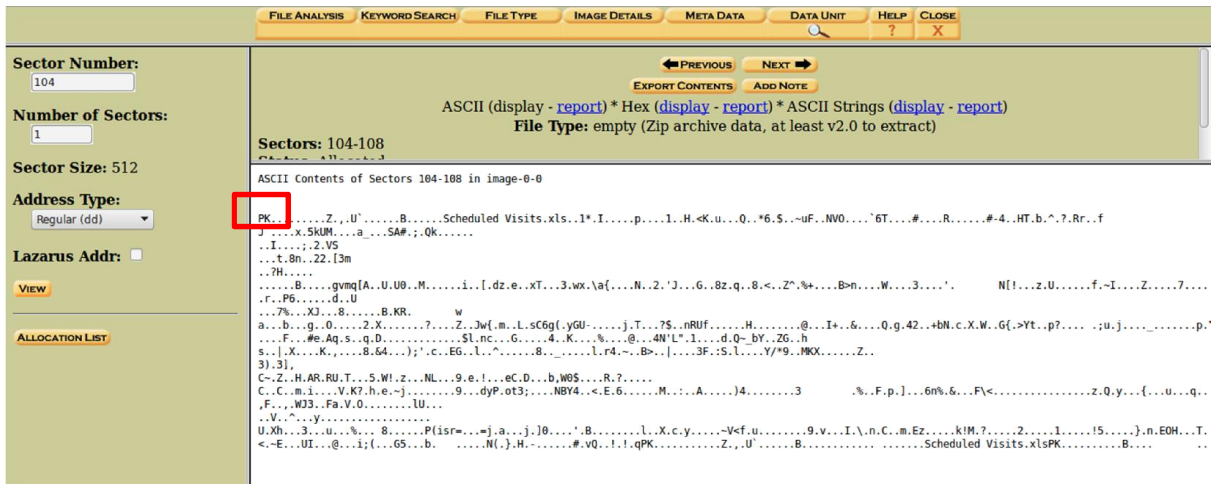
```
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $ file voll-Sector73.raw
voll-Sector73.raw: JPEG image data, JFIF standard 1.01
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $
```

Gambar 22. Tampilan ketika melihat tipe file 73-103 (31) yang telah di ekspor.

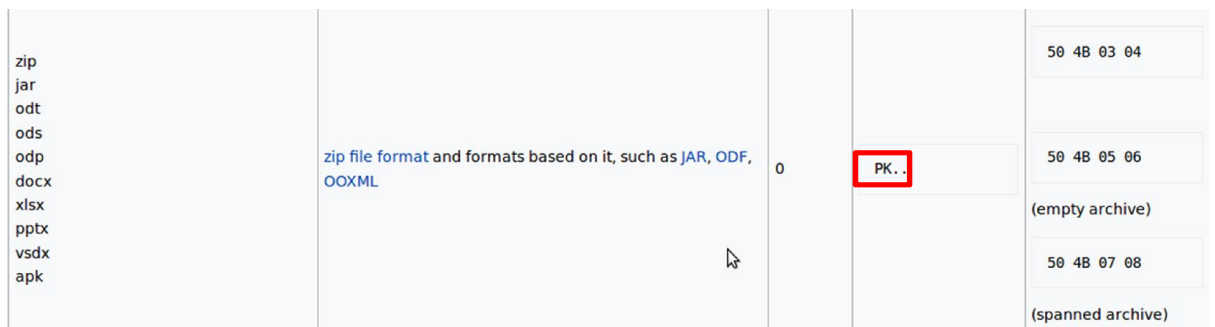


Gambar 23. Tampilan ketika file image.zip di rename menjadi file jpg.

16. Selanjutnya melihat isi file yang kedua untuk dianalisa tipe filenya, file 104-108 (5)-> EOF merupakan file dengan format zip karena pada isi filenya terdapat PK (seperti yang ditampilkan pada gambar 24), yang ketika dicari pada list of file signature di wikipedia maka hasilnya akan seperti gambar 25.



Gambar 24. Tampilan isi file 104-108 (5) pada autopsy.



Gambar 25. Tampilan ketika melihat list untuk file 104-108 (5) pada autopsy.

19. Gambar 28 merupakan tampilan ketika melakukan command foremost -v -i image -o recover
recover

```
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $ 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 12:01:57 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/srisuryani/Unduhan/recover
Configuration file: /etc/foremost.conf
Processing: image
|-----
File: image
Start: Fri Mar 24 12:01:57 2017
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)          Size      File Offset   Comment
0:       00000073.jpg           8 KB      37376
1:       00000033.doc           21 KB     16896
foundat=Scheduled Visits.xls*0I
:0p00:0H:00<K0uq0Q00*60$0:0AUF00NV0000`6T:0.#00:00
0R0:00#-40H0T0b0^0?0Rr00f
J 00:00x05kUM0000a_00SA#0;0Qk00 00:00
00I0:00;020VS
2:       00000104.zip           2 KB      53248
*|
Finish: Fri Mar 24 12:01:57 2017

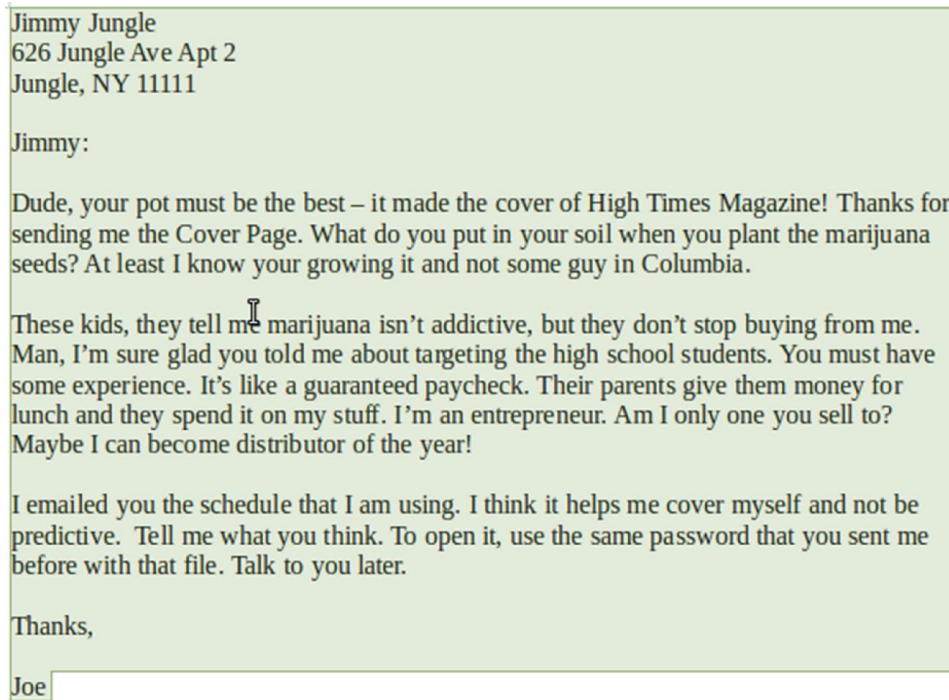
3 FILES EXTRACTED

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

Foremost finished at Fri Mar 24 12:01:57 2017
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $
```

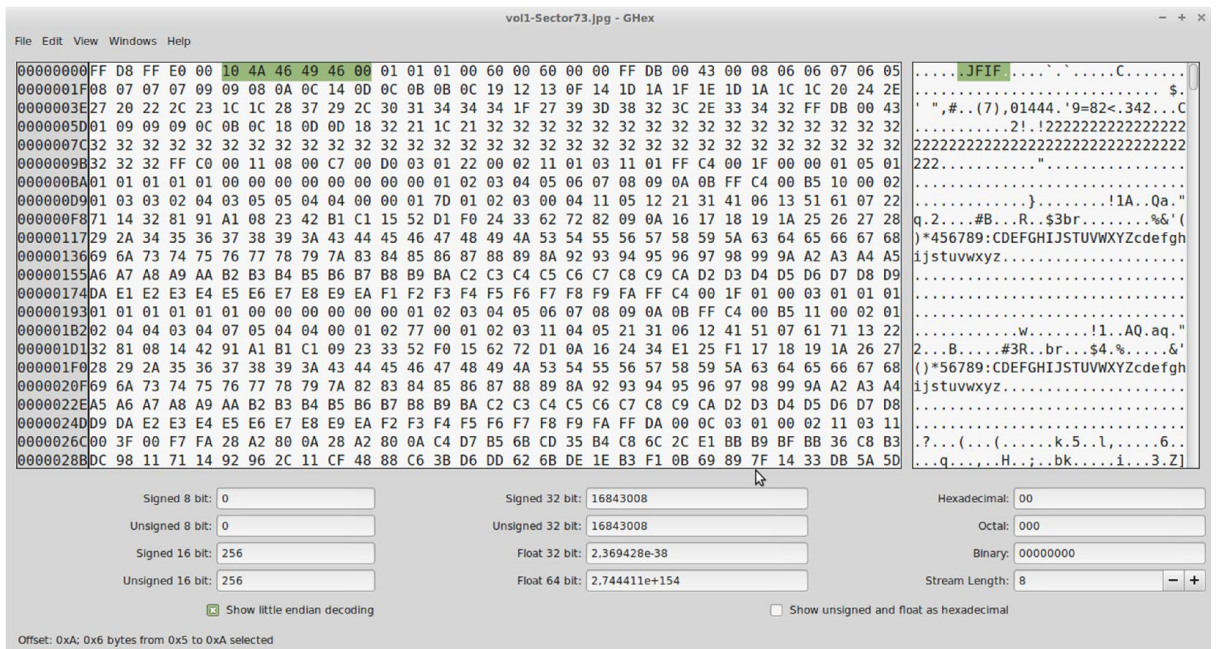
Gambar 28. Tampilan ketika melakukan perintah untuk mengembalikan file image yang telah dihapus

- 20. Gambar 29 merupakan isi dari file coverpage dimana isinya tersebut memiliki informasi nama penyuplier berserta alamatnya.



Gambar 29. Tampilan isi file pagecover

- 21. Gambar 30 merupakan tampilan ketika membuka file image menggunakan aplikasi Ghex.



Gambar 30. Tampilan file image ketika dibuka dengan aplikasi Ghex

Berikut merupakan informasi yang dibutuhkan oleh penyidik :

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

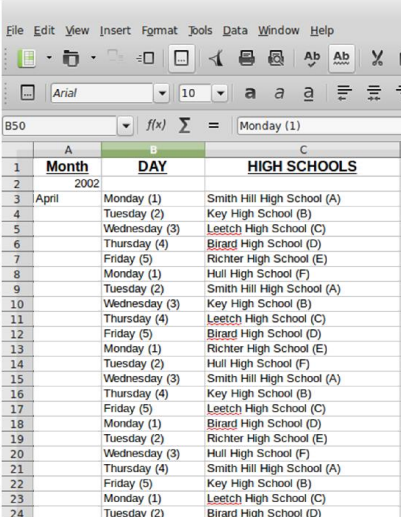
2. What crucial data is available within the coverage.jpg file and why is this data crucial?

Isinya dari coverage adalah password untuk membuka file yang berisi list sekolah sebagai tempat transaksi.

```
pw=goodtimes
```

```
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $
```

3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?



	A	B	C
1	Month	DAY	HIGH SCHOOLS
2		2002	
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith Hill High School (A)
10		Wednesday (3)	Key High School (B)
11		Thursday (4)	Leetch High School (C)
12		Friday (5)	Birard High School (D)
13		Monday (1)	Richter High School (E)
14		Tuesday (2)	Hull High School (F)
15		Wednesday (3)	Smith Hill High School (A)
16		Thursday (4)	Key High School (B)
17		Friday (5)	Leetch High School (C)
18		Monday (1)	Birard High School (D)
19		Tuesday (2)	Richter High School (E)
20		Wednesday (3)	Hull High School (F)
21		Thursday (4)	Smith Hill High School (A)
22		Friday (5)	Key High School (B)
23		Monday (1)	Leetch High School (C)
24		Tuesday (2)	Birard High School (D)

4. For each file, what processes were taken by the suspect to mask them from others?
 - Merename file format zip ke format exe.
 - Menyembunyikan password dengan menggunakan file format jpg.

5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

- Rename file zip menjadi jpg untuk melihat hasil gambar dibawah ini



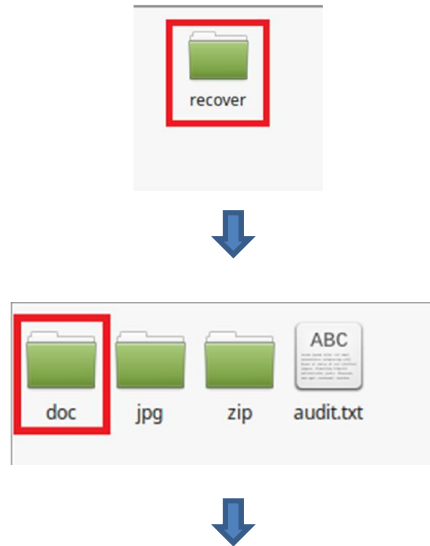
- Melakukan strings pada file voll-sector73.jpg untuk mendapatkan password dan password tersebut digunakan untuk membuka file schedule.exe seperti gambar dibawah

```
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $ strings voll-Sector73.jpg
pw=goodtimes
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $
```



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)

- Melakukan perintah command foremost -v -i image -o recover untuk membuka folder recover dan membuka folder dokumen, dimana file dokumen tersebut terdapat isi surat untuk jimmy (penyuplaier narkoba).



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