UJIAN AKHIR SEMESTER

KOMPUTER FORENSIK

DISUSUN OLEH:

AJRUL AMILIN M

09021381520071

JURUSAN TEKNIK

INFORMATIKA FAKULTAS

ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA 2018

1. Analisa Forensik Image File

STUDI KASUS

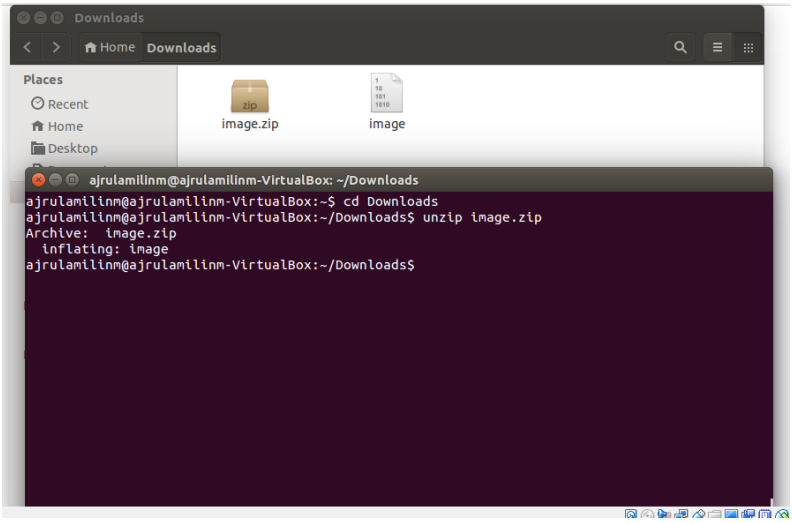
Telah tertangkap seorang pengedar narkoba kelas kakap, polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta bantuan oleh polisi untuk melakukan forensic terhadap file yang di temukan pada harddrive pelaku guna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

Ada beberapa yang harus di selesaikan atau mendapatkan informasi antara lain yaitu:

a) image file download url : http://old.honeynet.org/scans/scan24/image.zip
b) Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
c) What crucial data is available within the coverpage.jpg file and why is this data crucial?
d) What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
e) For each file, what processes were taken by the suspect to mask them from others?
f) What processes did you (the investigator) use to successfully examine the entire contents of each file?

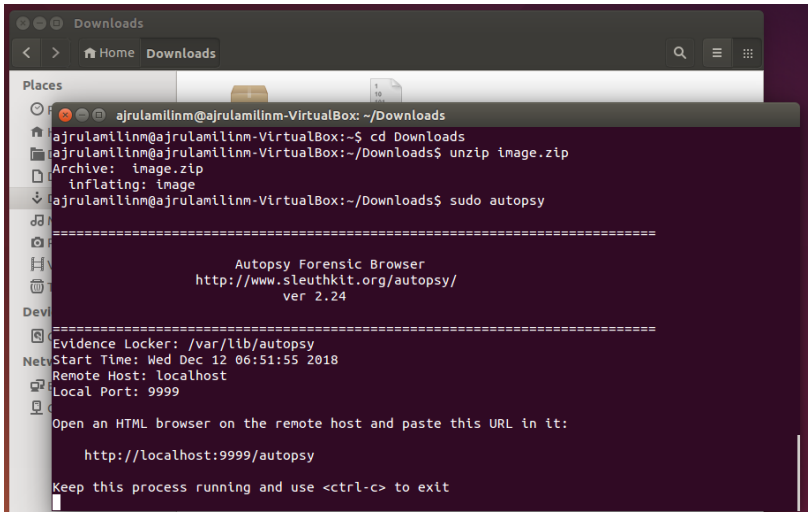
Investigasi ini dilakukan di Linux Ubuntu 14.04 dalam Virtual Box dan Tools yang digunakan Autopsy, Foremost, dan Strings. Sebelumnya kita menjawab **bagian (f)** terlebih dahulu untuk dapat mengetahui bagian-bagian diatasnya. Proses yang dilakukan untuk menginvestigasi kasus ini sehingga dapat dengan berhasil menemukan informasi yang terdapat pada file tersebut.

Proses pertama, pada file yang ditemukan pada hardrive pelaku sebaiknya kita melakukan rincian atau melihat jenis apakah file tersebut dengan cara ketikan "**file nama_file**" pada terminal. Setelah mengetahui bahwa file yang ditemukan itu berjenis zip, maka untuk membuka file tersebut harus di unzip terlebih dengan cara "**unzip nama_file.zip**" pada terminal dan kita akan mendapatkan file hasil unzip yang terlihat pada gambar 1.

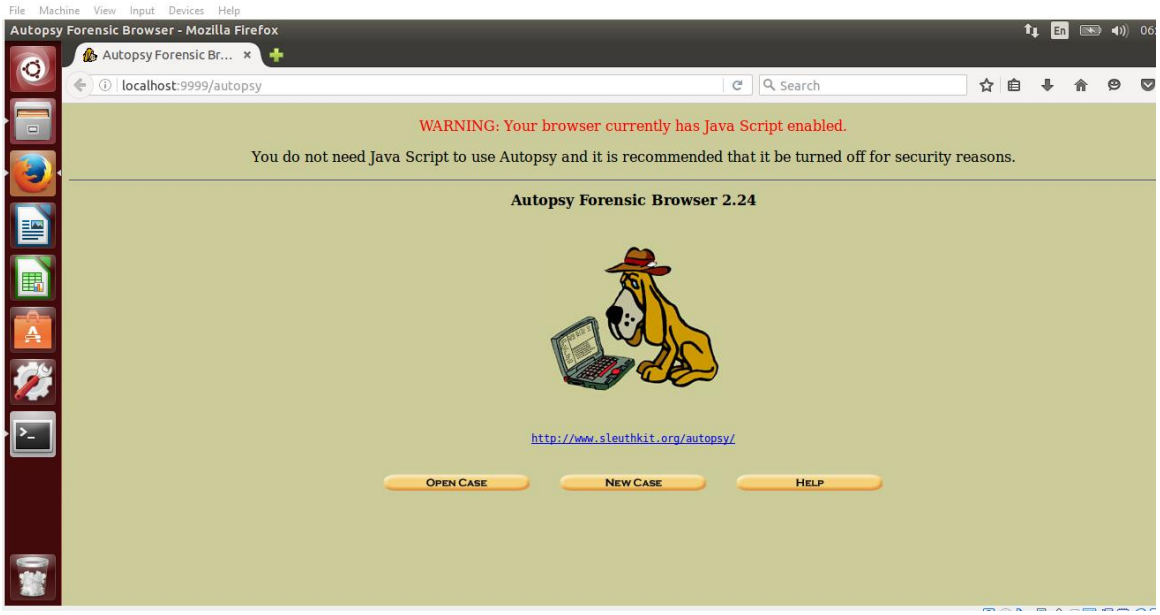


Gambar 1 : Hasil unzip

Setelah mendapatkan hasil unzip ,yaitu berupa raw data bernama image, untuk mengetahui lebih lanjut mengenai file tersebut maka akan digunakan tools autopsy. Dapat dilihat pada gambar 2 tampilan jika menggunakan tools tersebut , autopsy dapat diakses secara local pada alamat http://localhost:9999/autopsy

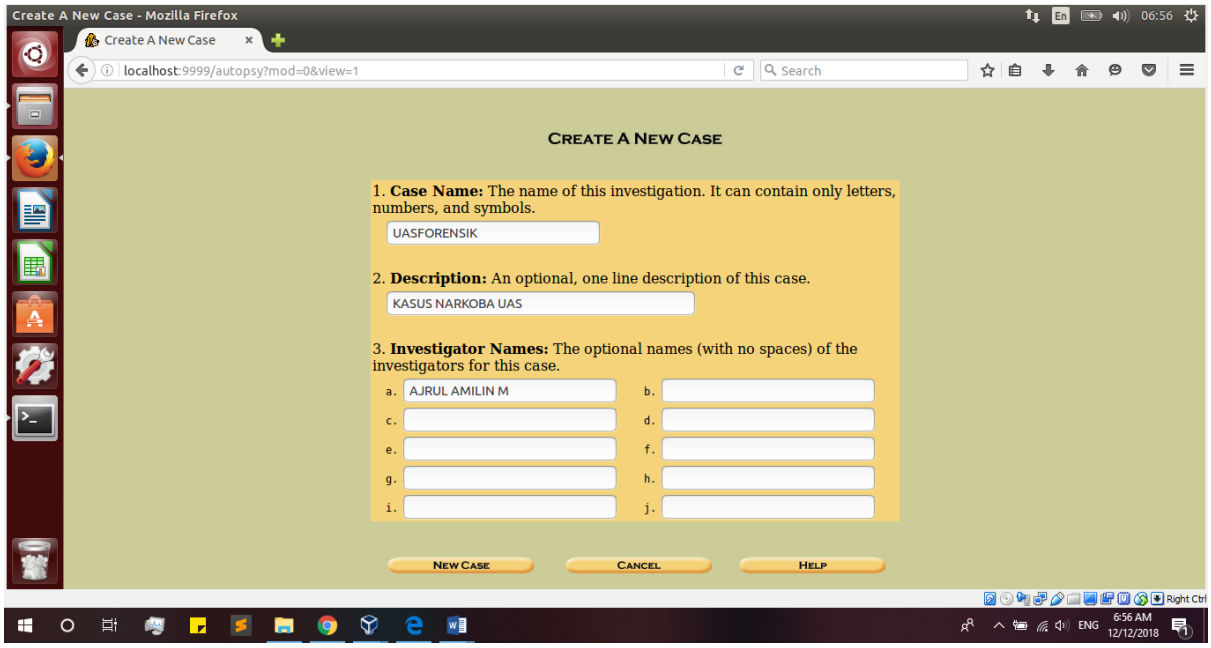


Gambar 2 : Tampilan Autopsy ketika di Terminal



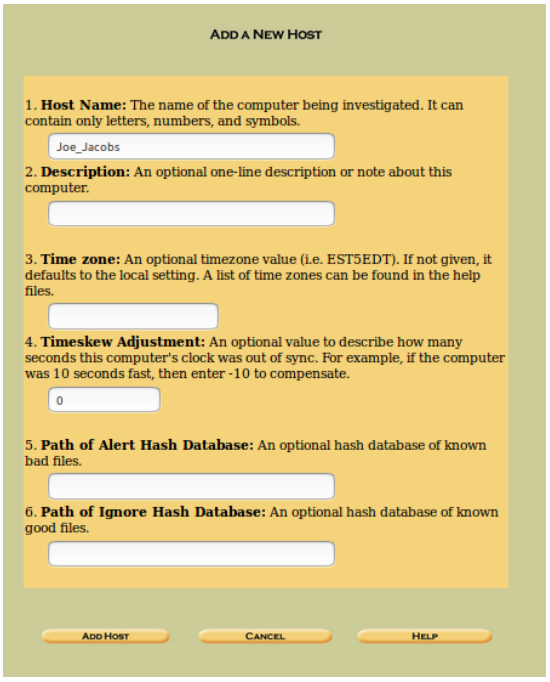
Gambar 3 : Start Autopsy

Pada alamat tools tersebut pilih ***New Case,*** kemudian isi kolom *case name* , *description dan investigator name*.



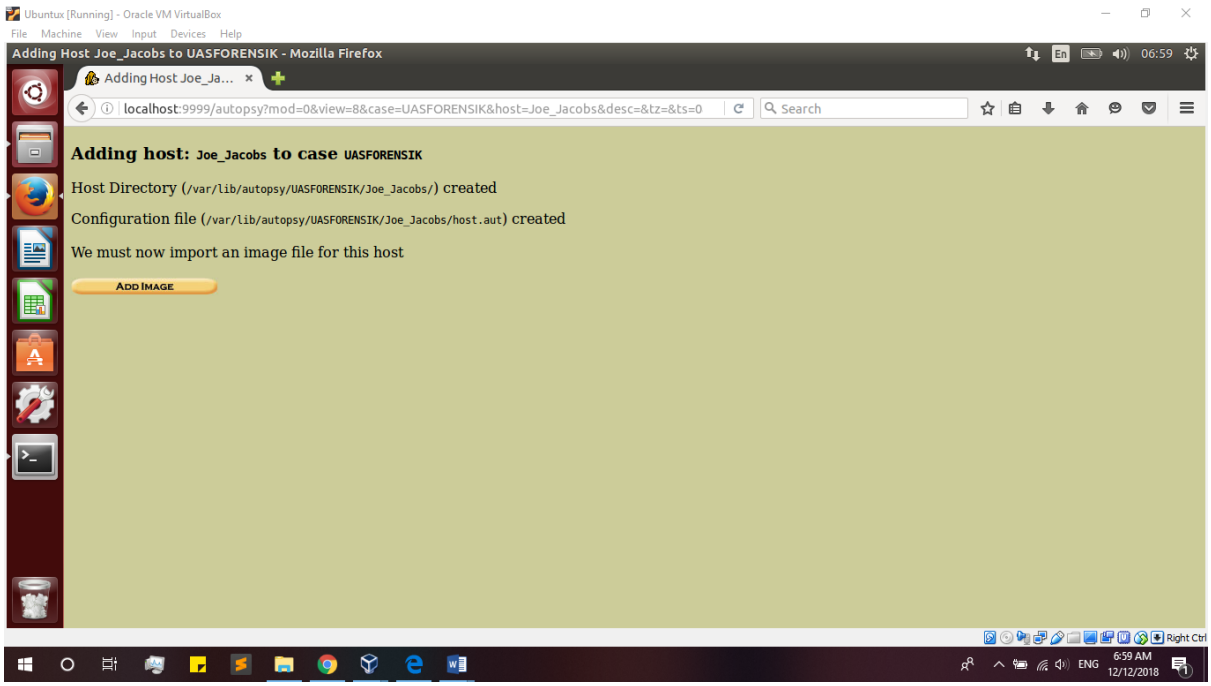
Gambar 4 : Create A New Case

Setelah selesai diisi maka pilih ***new case***, pada gambar 5 kemudian lakukan lagi pengisisan kolom pada *host name* saja.

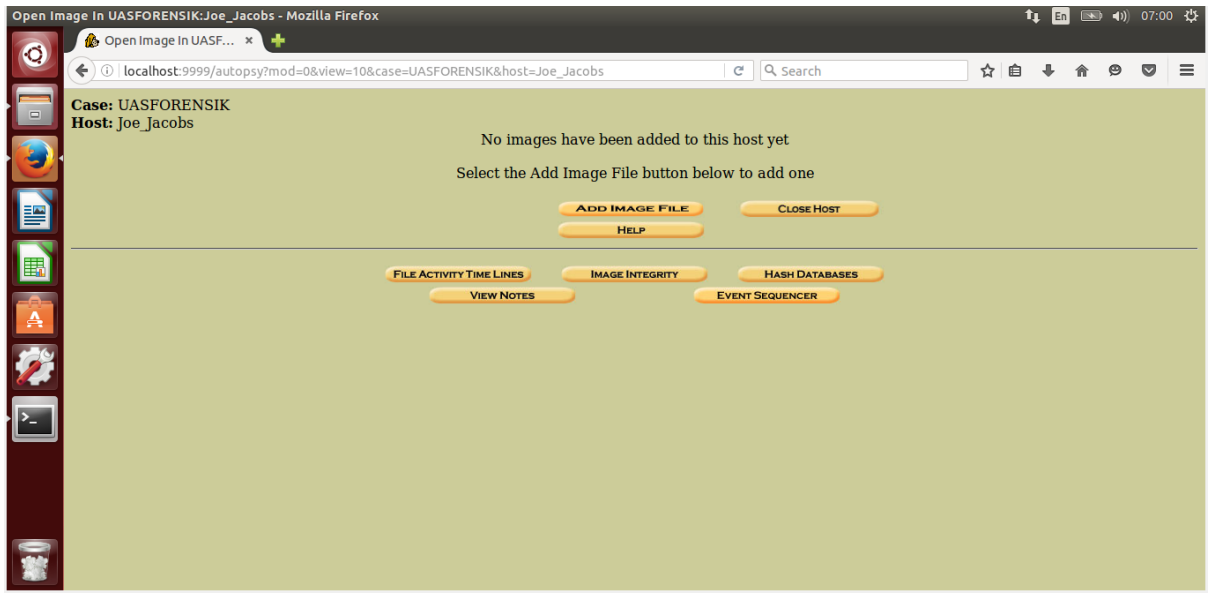


Gambar 5 : Add A New Host

Pada gambar selanjutnya yaitu gambar 6, pilih *add image* maka akan menuju home dari apa yang telah kita lakukan sebelumnya lihat pada gambar 7.

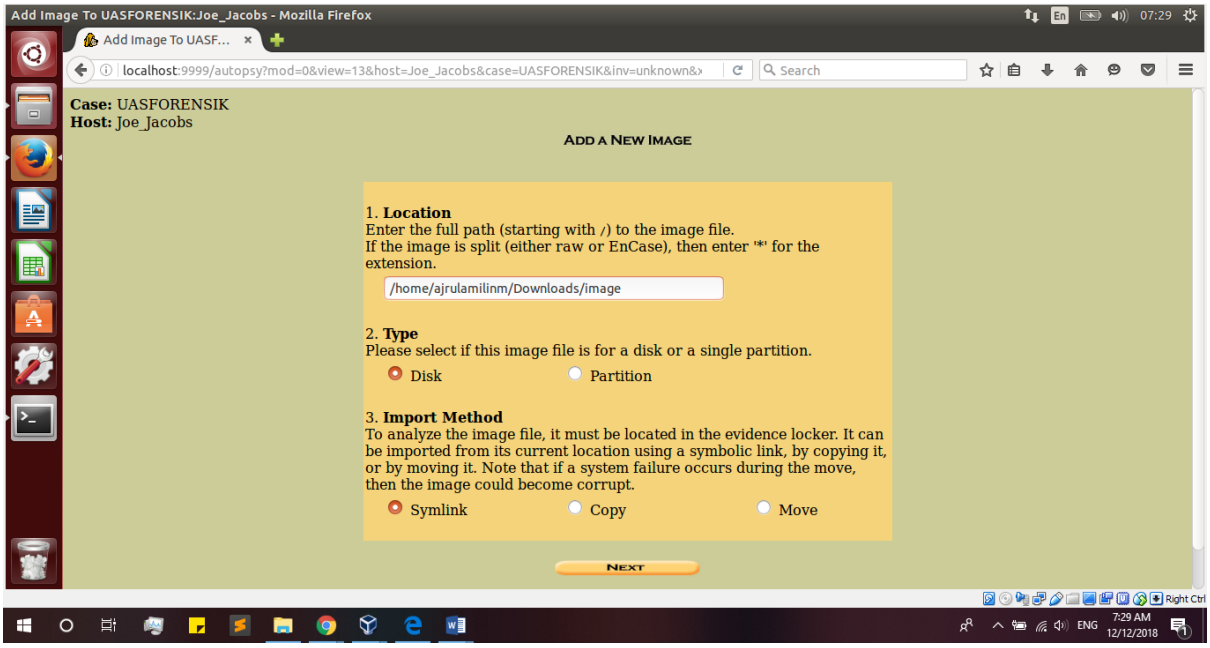


Gambar 6 : Add Image (File)

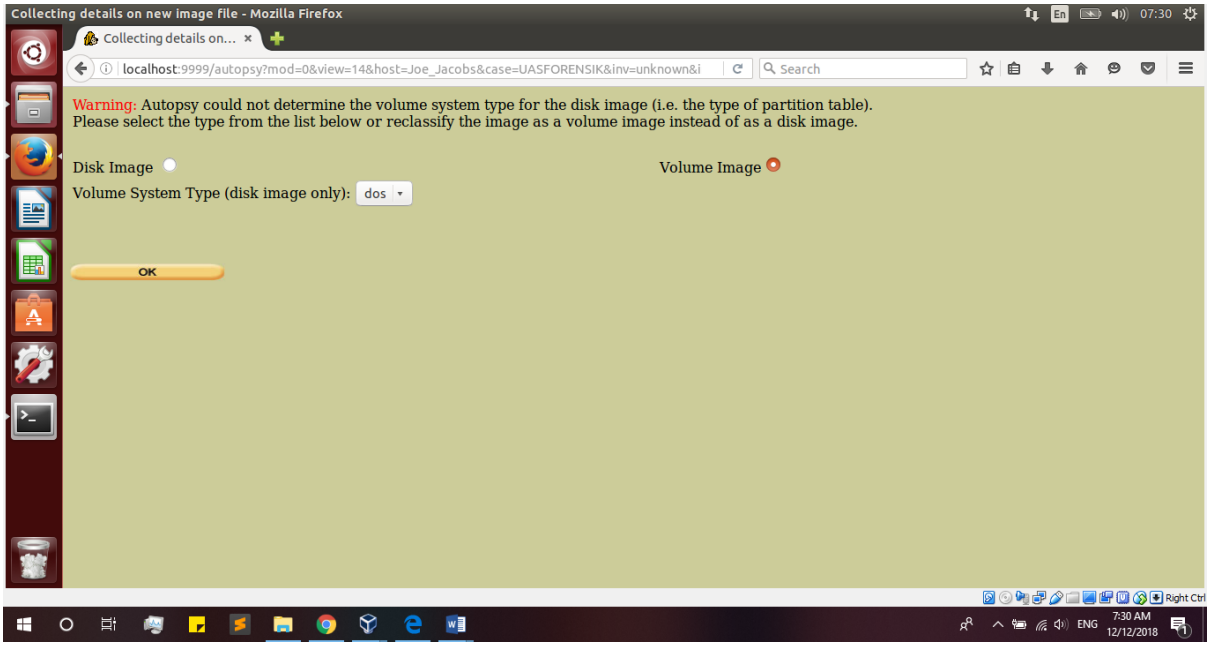


Gambar 7 : Home Case

Pilih *add image file* , hal ini bertujuan untuk melihat informasi dan bagian rincian isi file yang yang masih ada atau pun telah dihapus. Pada gambar 8 terdapat kolom location lalu isilah kolom tersebut berdasarkan file yang telah tersimpan sebelumnya, Pilih Type **Disk** dan Import Method **Symblink** kemudian *Next*.

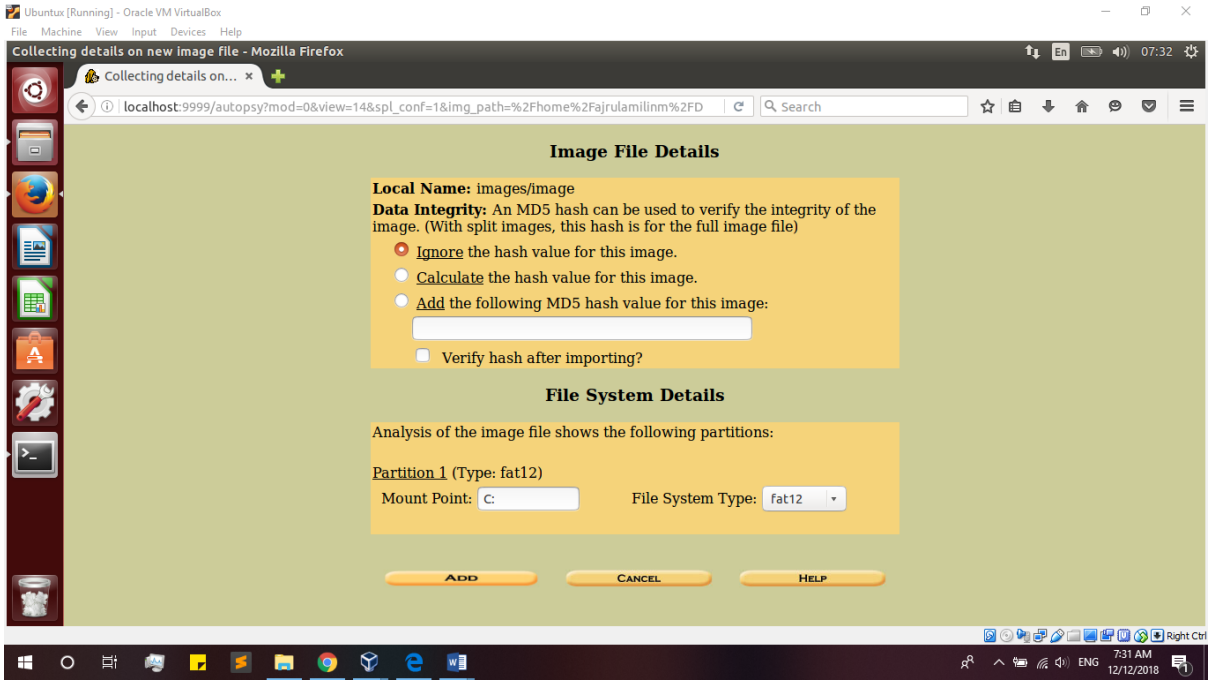


Gambar 8 : Pengaturan File Image



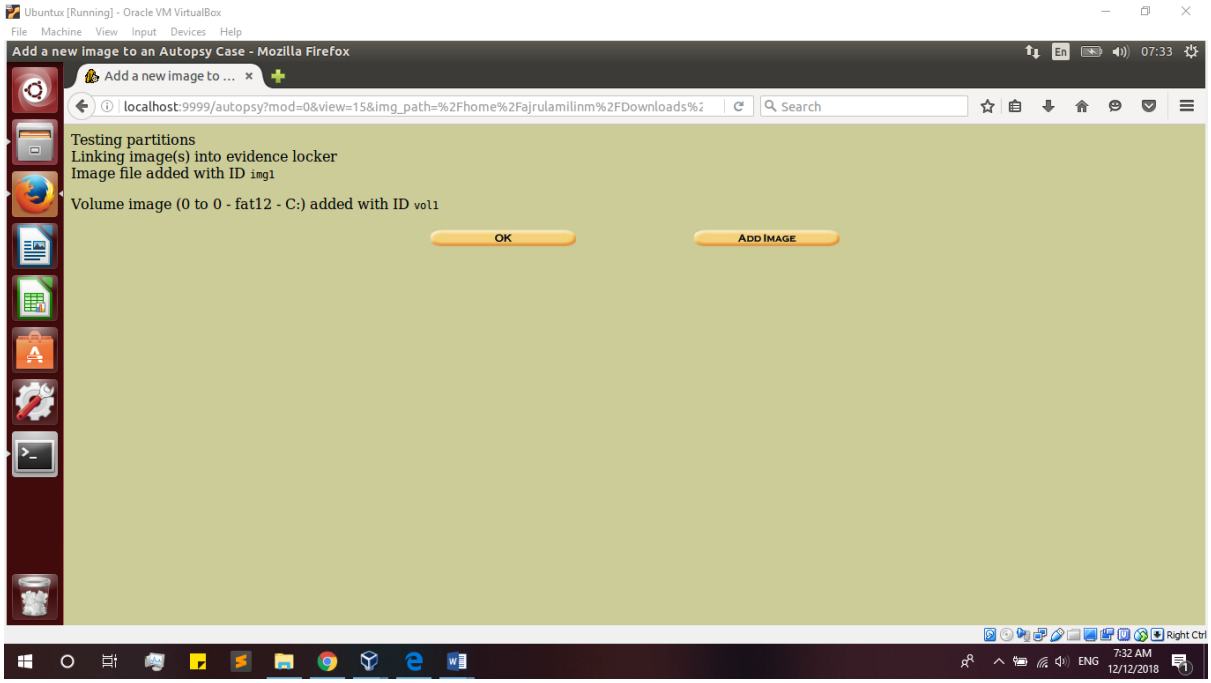
Gambar 9 : Tipe File

Pada gambar 9 terdapat dua opsi untuk tipe file yang akan dilakaukan pada tools autopsy ini. Pilih ***volume image***, dikarenakan file tersebut merupakan jenis dos dan corrupt atau untuk reclassify.

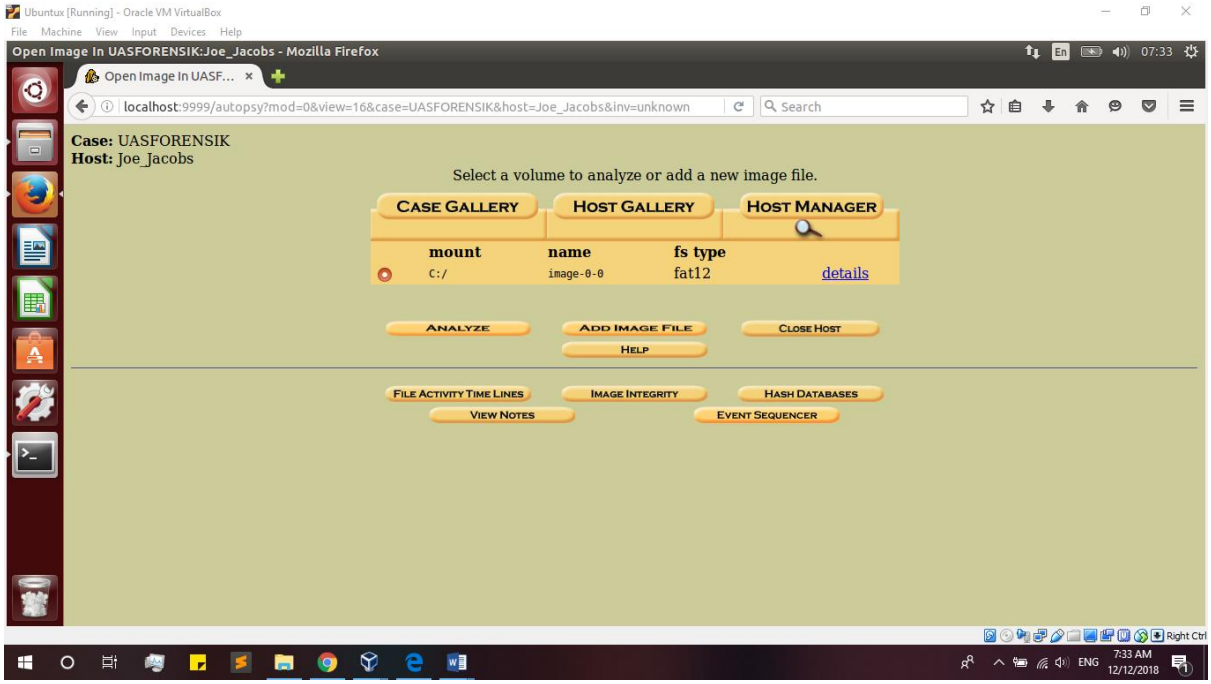


Gambar 10 : Image File Details

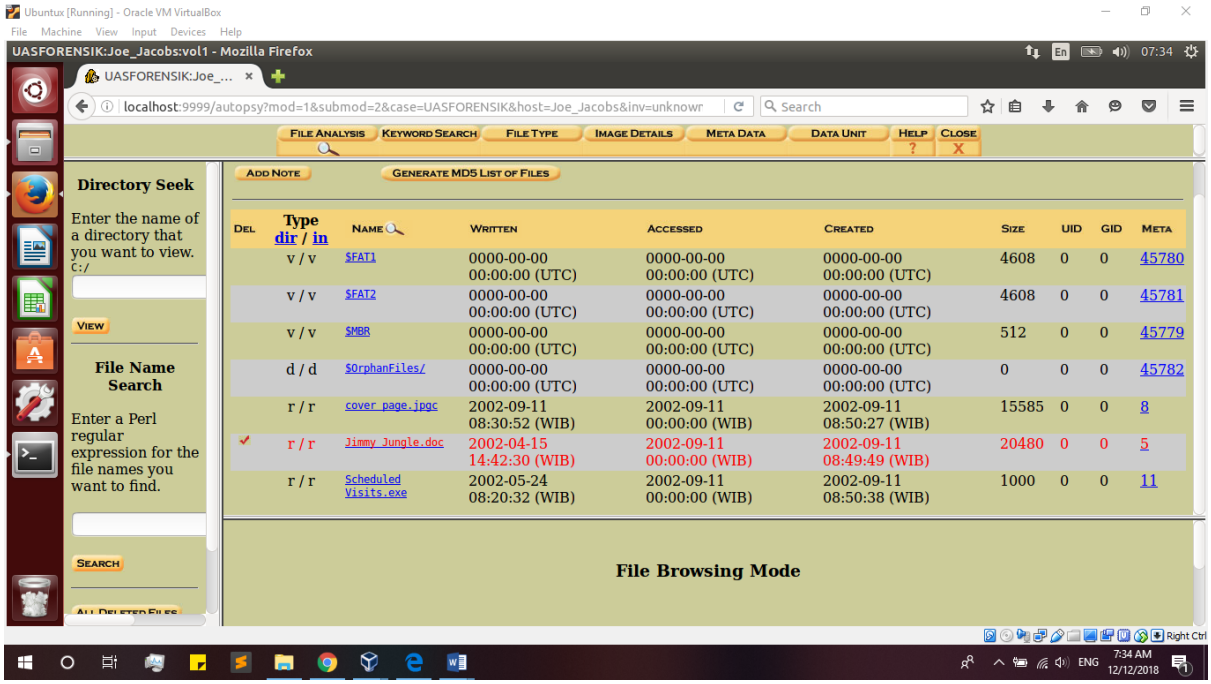
Biarkan secara default lalu pilih **ADD**



Gambar 11 : Testing Partitions



Gambar 12 : Tampilan setelah dibuat partisi



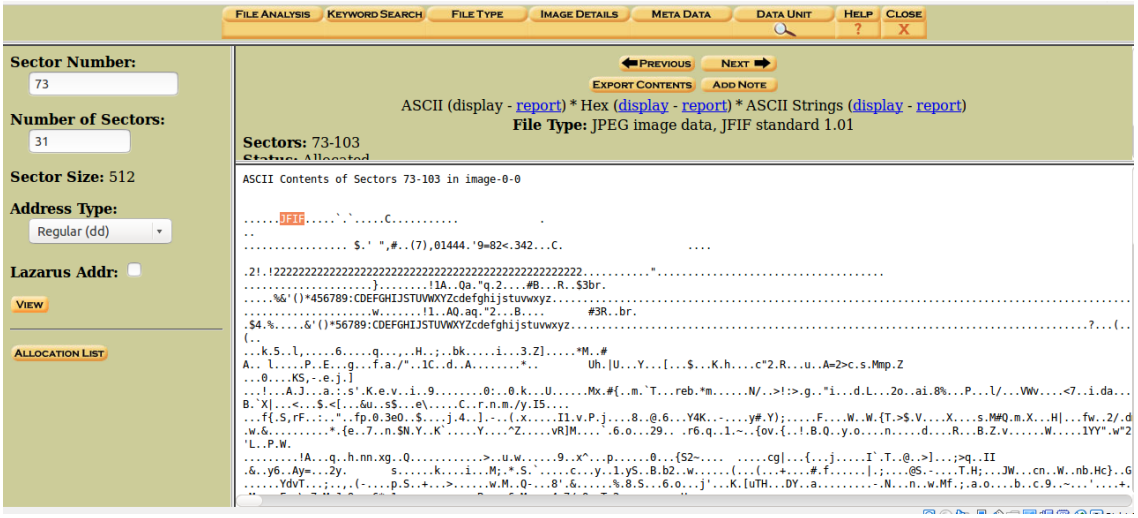
Gambar 13 : Tab File Analyze

Setelah diklik ***ANALYZE*** maka akan muncul seperti gambar 13 yang merupakan isi dari informasi dari hardrive tersebut. Terdapat banyak kegiatan mulai dari kapan palaku menulis mengakses serta membuat file. Pada list terdapat warna merah berarti file tersebut telah dihapus.

Gambar 14 : Tab image details bagian Fat Contents

Setelah melihat isi dari aktivitas pelaku ,lihat bagian *image details* dan dibagian *FAT CONTETNTS* dimana terdapat dua pilihan yaitu 73-103 (31) maksudnya terdapat informasi yang disembunyikan dalam sector 73 sampai 103 , begitu pula dengan yang kedua 104-108(5) terdapat informasi yang disembunyikan dalam sector 104 sampai 108.

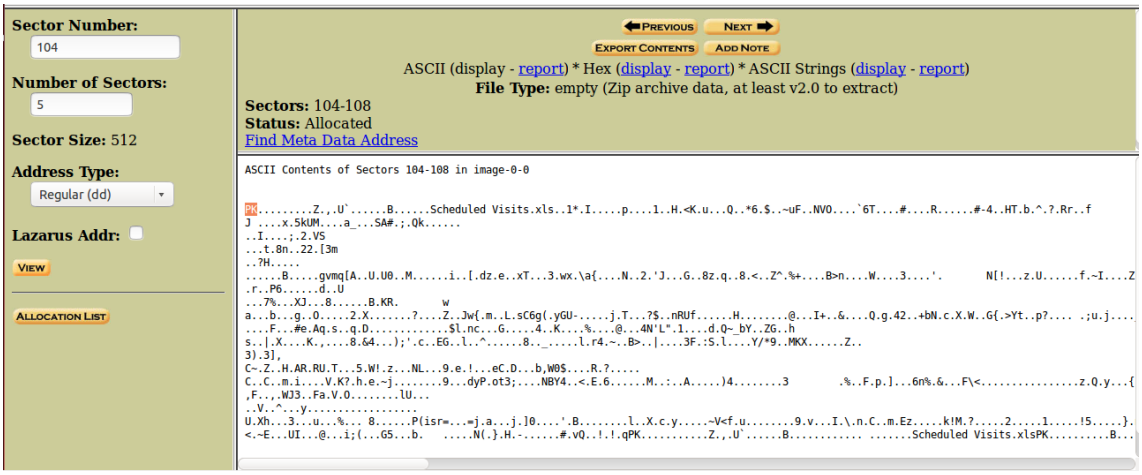
Pada sector 73 – 103 terdapat format yang sulit dimengerti bagi yang tidak mengetahuinya kita dapat mengidentifikasikan dengan cara melihat bit pertama atau informasi hexa yang terdapat pada awal tulisan. Yang dapat pada baris pertama yaitu JFIF , dan kemudian informasi tersebut dapat dilihat jenis dan dan informasi di *list of file singnature* seperti yang terilihat pada gambar 16 (Wikipedia). Lakukan hal yan sama pada sector 104-108.



Gambar 15 : Sector 73-103

FF D8 FF DB	ÿØÿÛ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà..JFIF..			
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá..Exif..			

Gambar 16 : *List of file signature for* JFIF

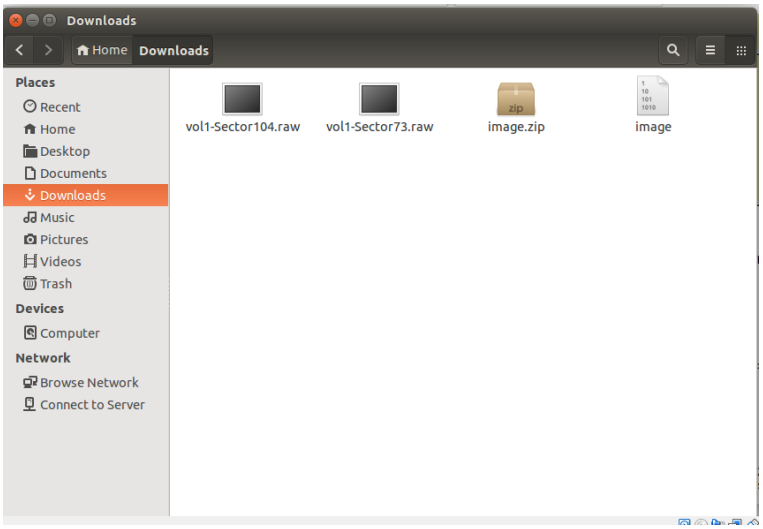


Gambar 17 : Sector 104-108

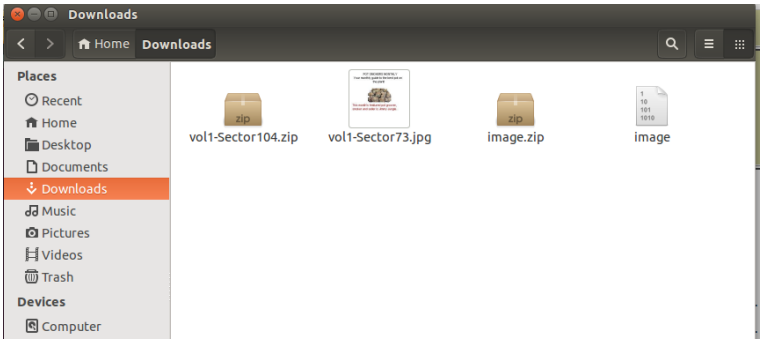
50 4B 03 04	PK..	0	zip jar odt ods odp docx xlsx pptx vsdx apk aar	zip file format and formats based on it, such as JAR, ODF, OOXML
50 4B 05 06 (empty archive)				
50 4B 07 08 (spanned archive)				

Gambar 18 : *List of file signature for PK*

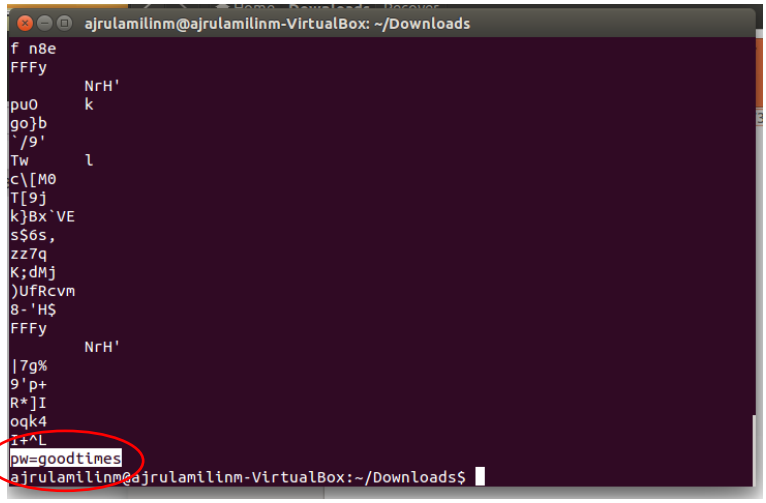
Setelah mengetahui jenis file yang terdapat dalam sector tersebut maka pilih *export contens* ,dan secara otomatis akan menguduh file, kemudian ubah format file yang telah terunduh sesuai dengan informasi yang didapat dari *list of file signature*.



Gambar 19 : Hasil Export File



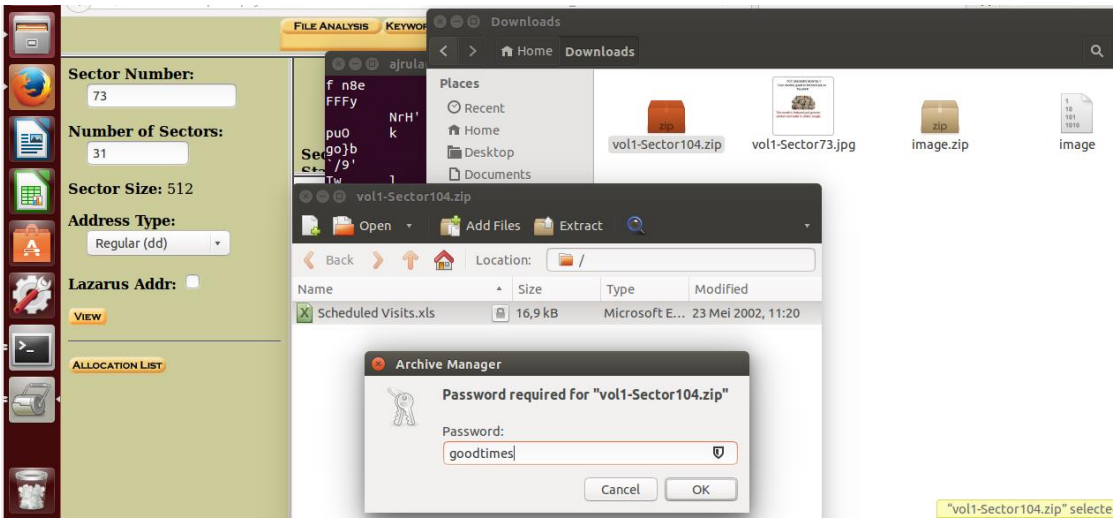
Gambar 20 : Hasil kedua file export setelah disesuaikan format file aslinya



Gambar 21 : Informasi Password (1)

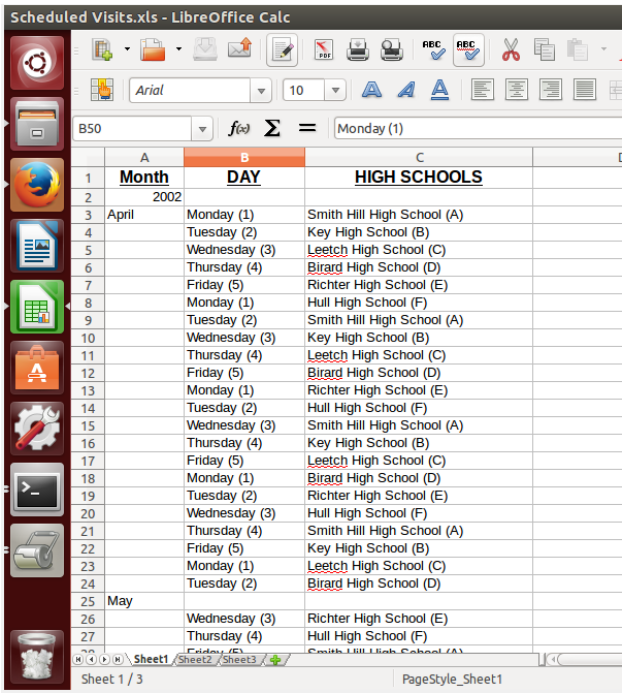
Gambar 22 : Informasi Password (2)

Dari file sector yang telah di rename sebelumnya, dengan menggunakan tools string kita telah mendapatkan informasi yang terdapat pada file tersebut. Pada gambar 21 telah dilakukan string , informasi yang terdapat pada file tersebut adalah password **"pw=goodtimes",** password tersebut digunakan untuk membuka file zip pada file sector 104.zip. Selain dari string ternyata kita juga bisa menemukan informasi password tersebut dari hasil Data Unit namun haruslah teliti dan seksama dalam menemukannya.



Gambar 23 : Isi File vol1-Sector104.zip

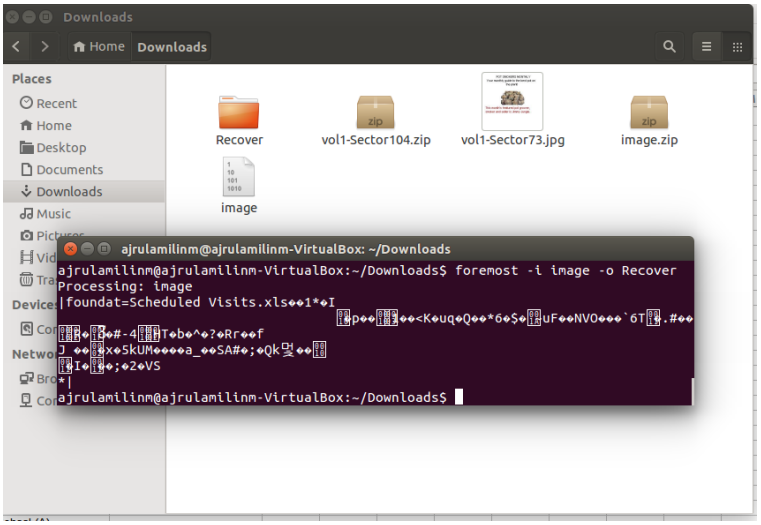
Ketika akan membuka File vol1-Sector104.zip kita menemukan terdapat sebuah file **Scheduled Visits.xls** namun untuk membukanya diperlukan password yang mana tadi kita telah menemukan password tersembunyi di dalam file gambar. Lalu masukkan password tersebut (Gambar 23).



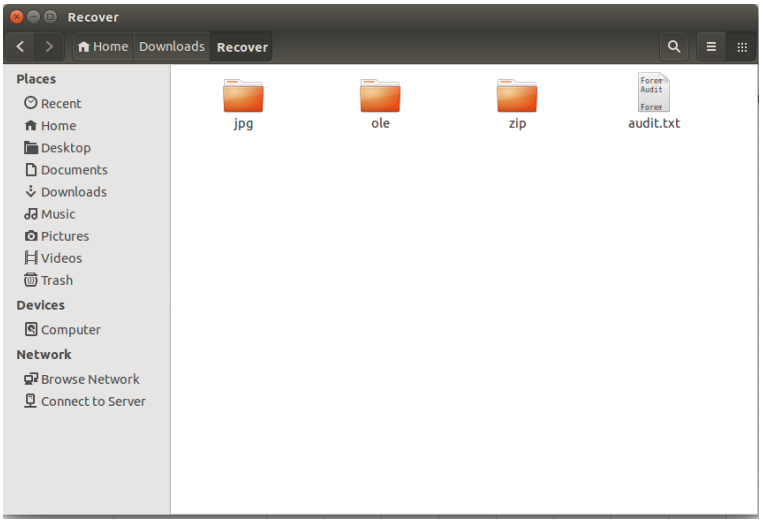
	A	B	C
1	Month	DAY	HIGH SCHOOLS
2	2002		
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith Hill High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

Gambar 24 : Isi File Scheduled.xls

Selain dengan menggunakan tools autopsy, kita juga dapat mnggunakan tools Foremost , tools ini berfungsi seperti mengubah file tersebut menjadi folder , yang didalamnya ada informasi yang penting. Dengan perintah "***foremost –i [nama_file] –o [nama_folder]***" pada terminal. Dapat dilihat pada gambar 25, setelah melakukan perintah diatas maka akan menampilkan folder yang berisi tentang informasi yang bersangkutan seperti yang terlihat pada gambar 26.

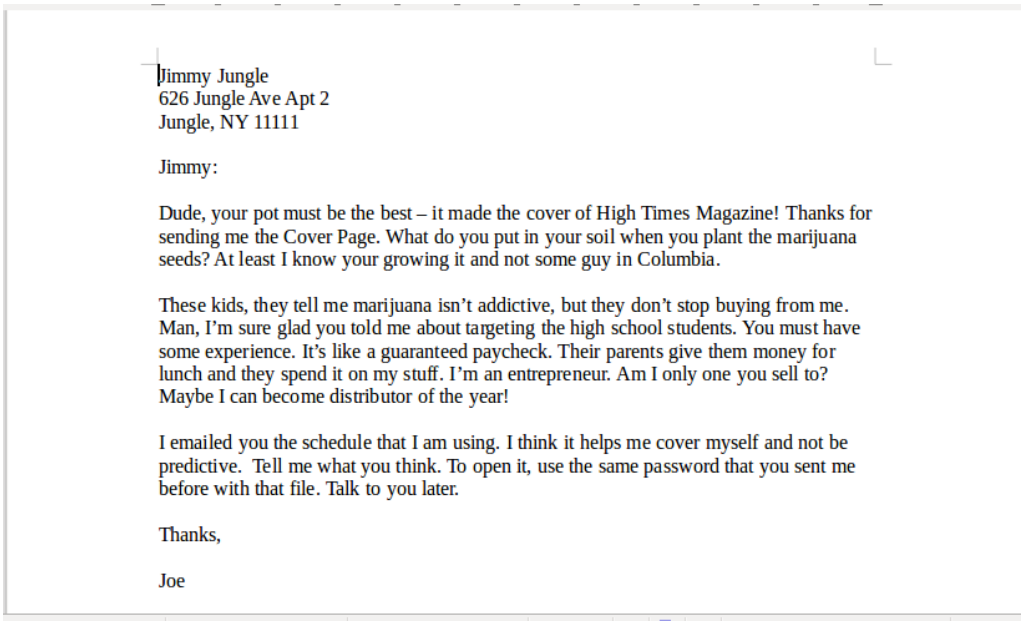


Gambar 25 : Menggunakan Foremost



Gambar 26 : Isi folder Recover

Didalam file recover terdapat folder ole, jpg, zip. Folder jpg berisi file yang sama seperti File vol1-Sector73.jpg dan Folder zip berisi file yang sama seperti File vol1-Sector104.zip (Gambar 20). Namun folder ole memiliki file yang berisi informasi seperti surat (email) yang telah dikirimkan untuk orang yang bersangkutan , isi file tersebut dapat dilihat pada gambar 27 yang mana file tersebut merupakan file yang telah dihapus ketika kita melakukan analisis di Autopsy (Jimmy Junggle.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 27 : isi file di folder ole

Jawaban bagian (b) yang menjadi pemasok (supplier) Joe Jacob adalah **Jimmy Jungle**, informasi tersebut terdapat pada sebuah email yang dikirimkan pada jimmy. Dapat dilihat pada gambar 27 yang beralamatkan . **626 Jungle Ave Apt 2, Jungle, NY 11111.**

Jawaban bagian (c) yang didapatkan dalam file gambar (jpg) adalah informasi password "**pw=goodtimes**" yang kita butuhkan untuk membuka atau mengekstrak file zip. Jadi informasi dalam file gambar (jpg) ini sangatlah penting, jika tidak ditemukan maka kita akan kesulitan untuk mengetahui informasi yang ada didalam file zip.

Jawaban bagian (d) , terdapat beberapa sekolah yang dikunjungi oleh Joe Jacobs (pelaku), seperti **Key High School**, **Leetch High School**, **Birrard High School** , **Richter High School** dan **Hull High School**, dan terdapat informasi yang menunjukan agenda atau kegiatan yang telah dilakukan oleh pelaku seperti yang terlihat pada gambar 24.

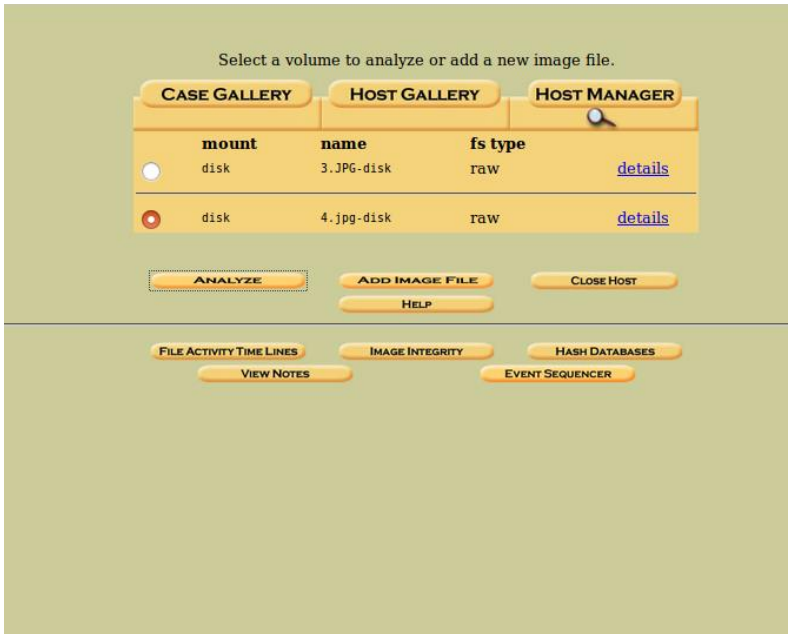
Jawaban bagian (e) , proses yang dilakukan tersangka untuk menyembunyikan informasi tersebut agar tidak diketahui oleh orang lain adalah pertama file.xls yaitu semua kegiatan yang dilakukan oleh tersangka di letakan dalan file zip dan diberikan kunci (password) untuk mengaksesnya , dan password tersebut disembunyikan pada sebuah gambar (jpg) , kemudian masing- masing file yang berisi informasi tersebut di ubah format (rename) dan hasil perubahan format tersebut diletakan pada sebuah file yang bernama **image**, file image ini pula di letakan dalam file zip.

Jawaban bagian (f) merupakan hasil investigasi dan analisis dari awal (Telah dijelaskan sebelumnya di awal) setelah pertanyaan.

2. Analisa Forensik Gambar / Foto

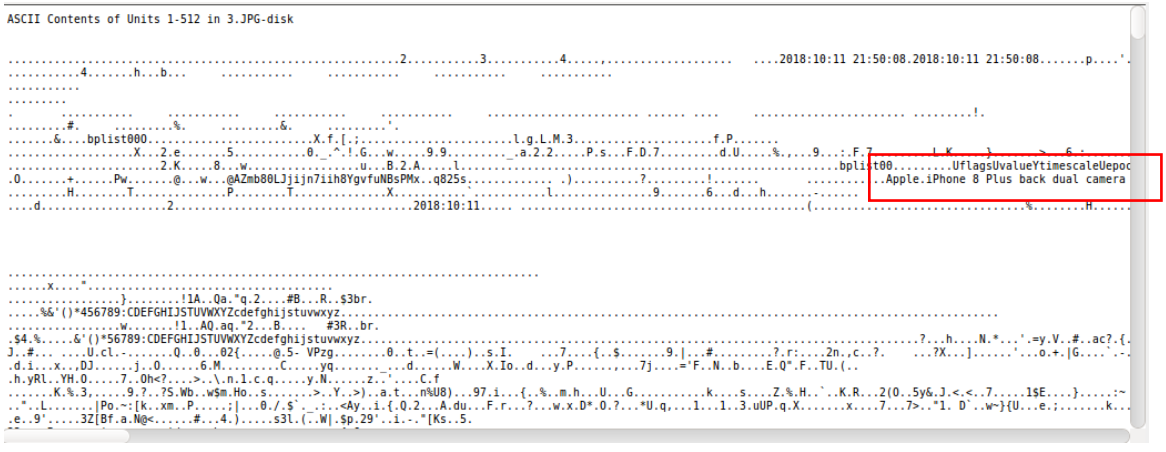
Melakukan forensic pada 2 gambar/foto dengan melakukan analisa pada metadata gambar/foto, membandingkan yang mana asli dan yang mana palsu.

Tambahkan data/file yang akan dianalisis seperti cara yang sebelumnya (Gambar 2.1)



Gambar 2.1

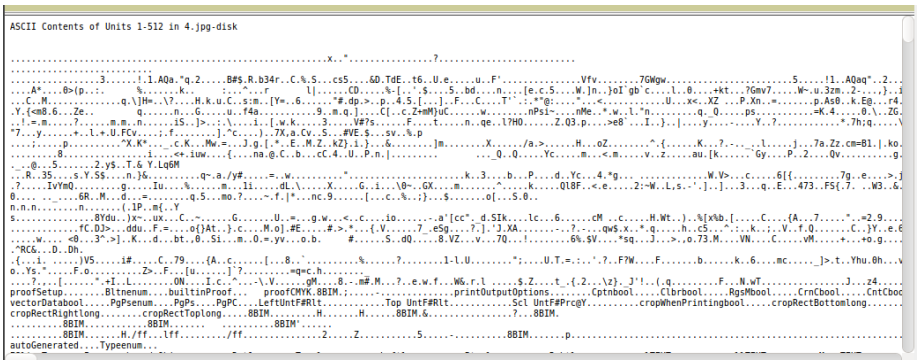
Hasil Metadata dari file 3.JPG menunjukkan hasil berikut (Gambar 2.2)



Gambar 2.2

Dari gambar bias ketahui bahwa gambar/photo diambil dari Merek **Apple. iPhone 8 Plus Dual Camera 3.99mm f/1.8**

Hasil Metadata dari file 4.jpg menunjukkan hasil berikut (Gambar 2.3) dan (Gambar 2.4)

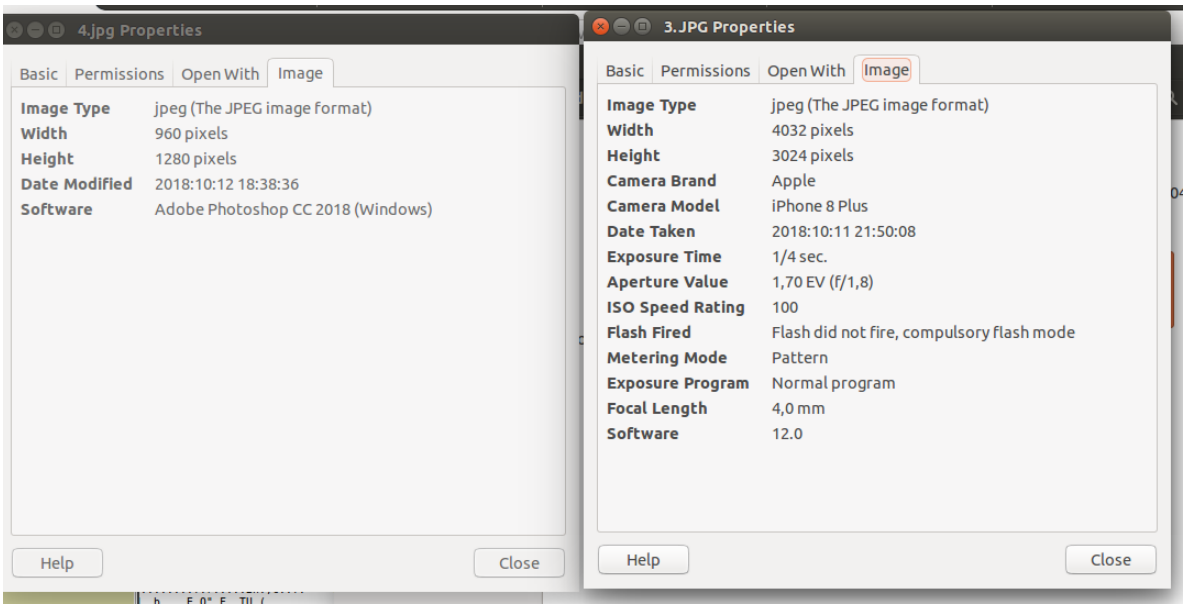


Gambar 2.3

Gambar 2.4

Dari hasil meta data di atas dinyatakan file photo 4.jpg telah mengalami editan menggunakan software **Adobe Photoshop CC 2018 (Windows)**

Kita juga bisa mengetahui mana file original atau sudah mengalami perubahan (editan) dengan cara melihat properties file (Gambar 2.5)



Gambar 2.5