TUGAS KEAMANAN JARINGAN KOMPUTER

COMPUTER FORENSIC

DISUSUN OLEH:

NAMA : Fahrul Rozi

NIM : 09011181320022

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Komputer Forensic

Definisi komputer forensic secara garis besar , dan telah dirangkum dari berbagai sumber 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.

Adapun tujuan dari sesorang yang melkukan komputer forensic yaitu pertama, untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki yang sah di pengadilan. Kedua, 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.

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:

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?

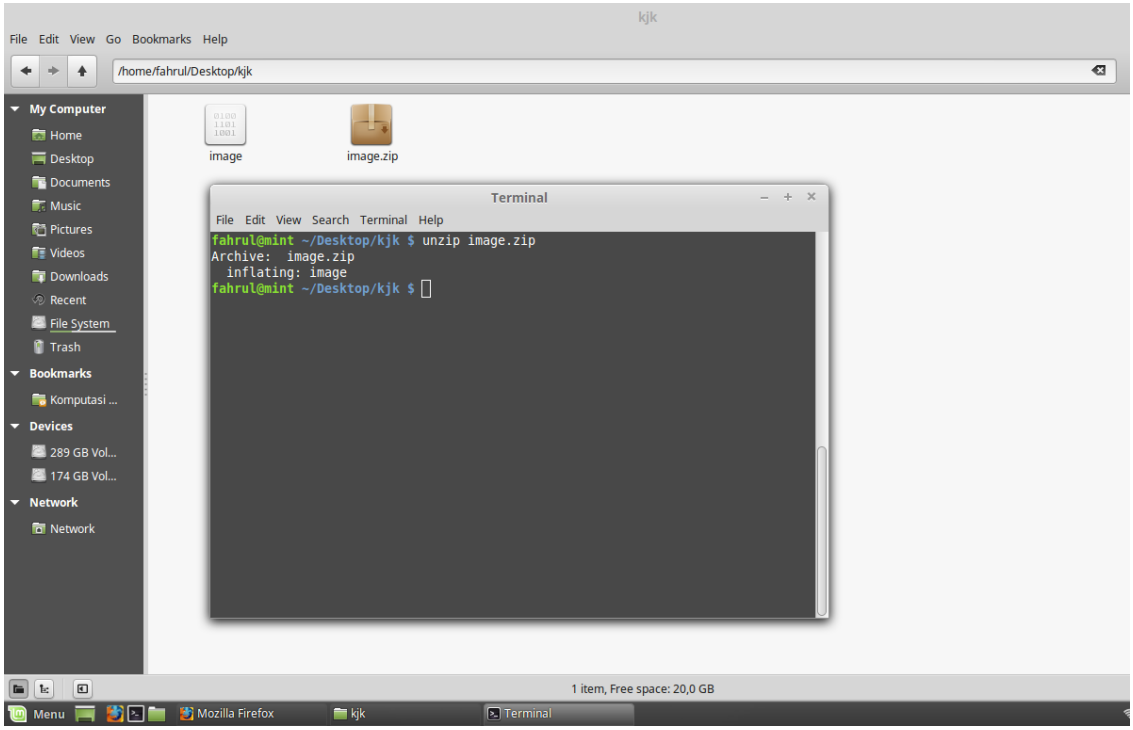
4.For each file, what processes were taken by the suspect to mask them from others?

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

File tersebut berada pada http://old.honeynet.org/scans/scan24 . Tools yang digunakan Autopsy, foremost, dan strings.

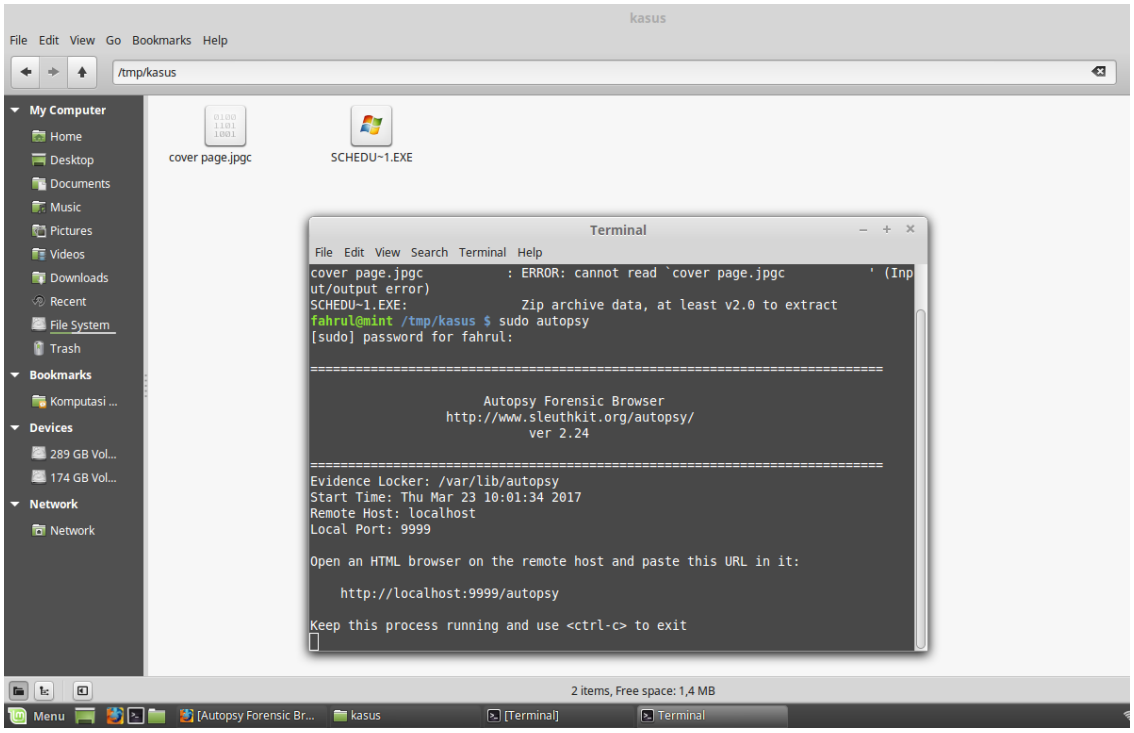
Sebelumnya kita menjawab bagian no 5 terlebih dahulu untuk dapat mengetahui bagian-bagian diatasnya. Proses yang dilakukan untuk menginvestigasi kasus ini sehingga dapat dengan berhasil menemukan informasi yang terdapat pada file tersebut.

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.

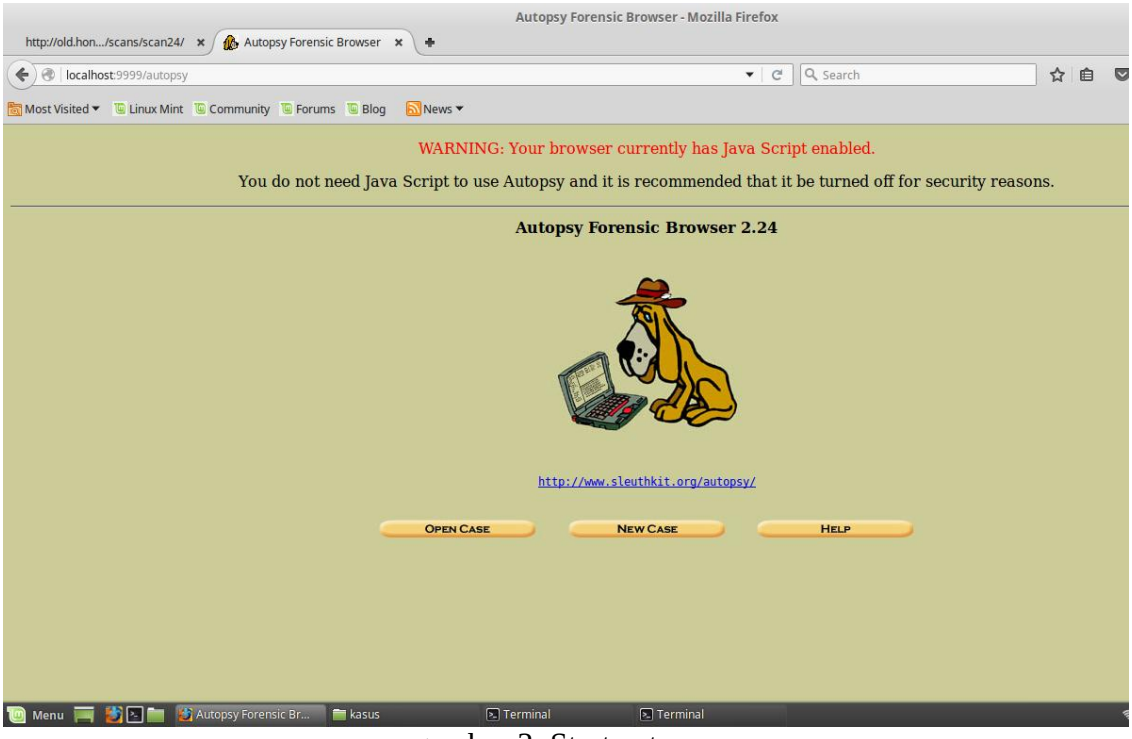


Gambar 1 : Hasil unzip

Setelah mendapatkan hasil unzip ,yaitu berupa file makal lakukan proses restore dan akan mendapatkan 2 file seperti yang terlihat pada gambar 2. Untuk mengetahui jenis file tersebut maka lakukan kembali perintah "**file nama_file**" pada terminal. Untuk mengetahui lebih lanjut mengenai 2 file tersebut maka akan digunakan tools autopsy. Dapat dilihat pada gambar 3 tampilan jika menggunakan tools tersebut , autopsy dapat diakses secara local pada alamat http://127.0.0.1:9999/autopsy

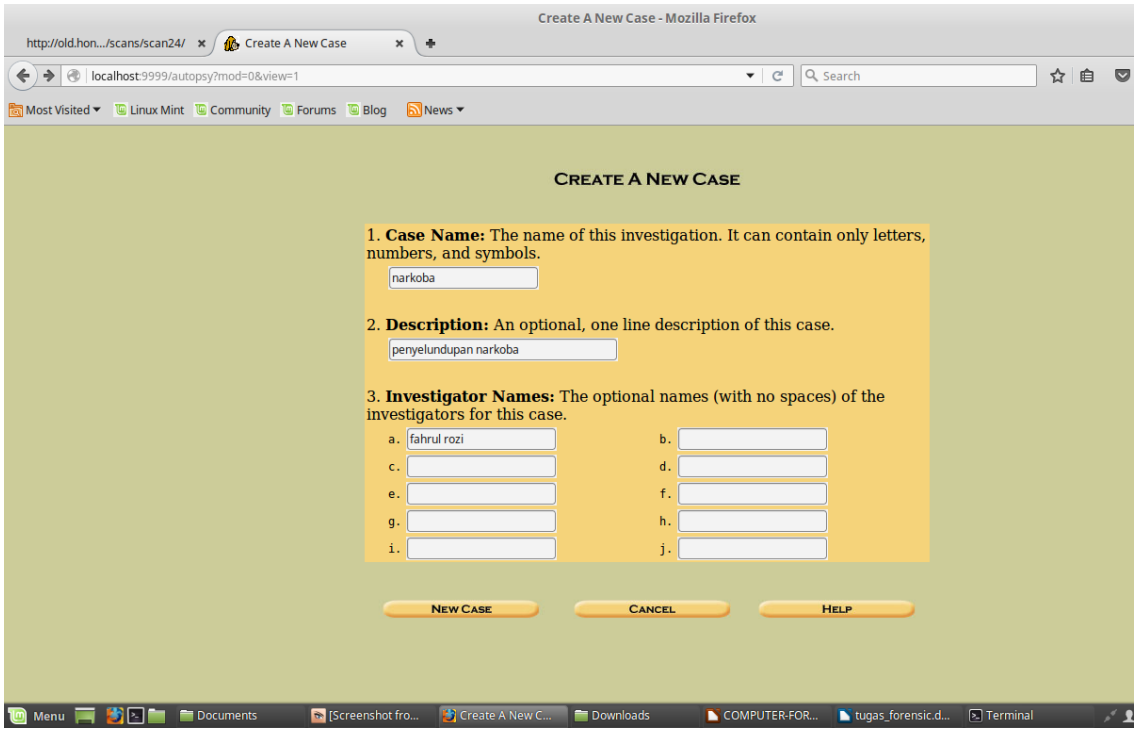


Gambar 2: Hasil restore file image



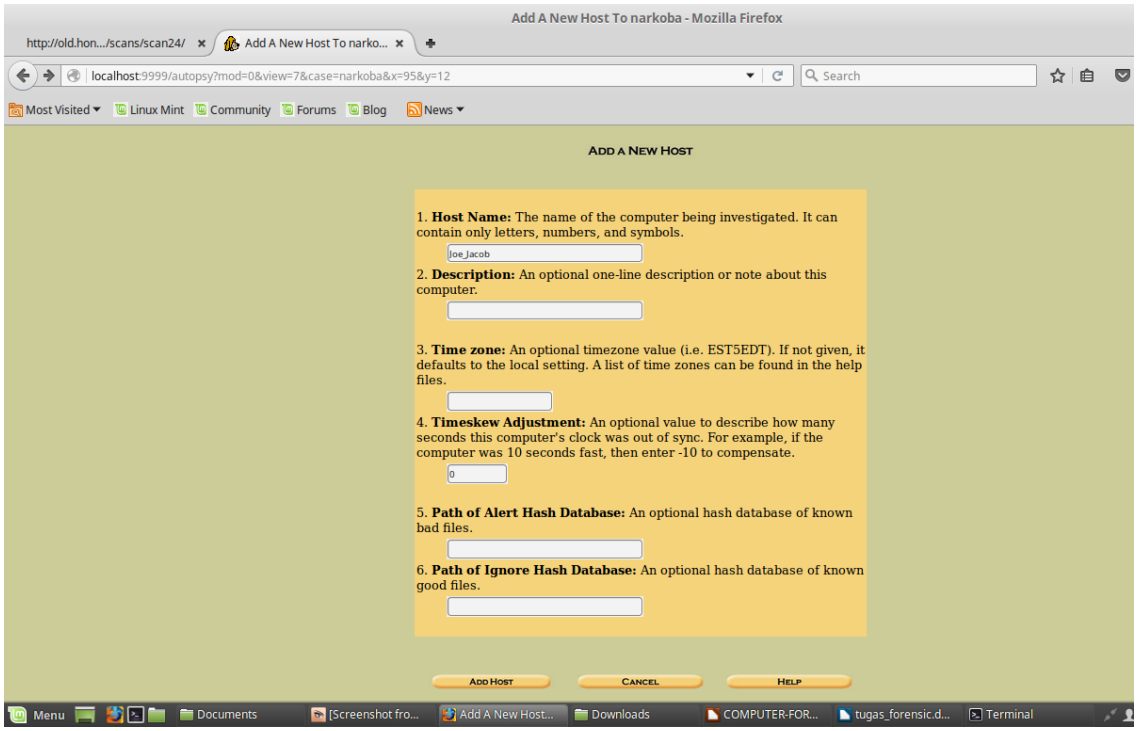
gambar 3: Start autopsy

pada alamat tools tersebut pilih ***new case,*** kemudian isi kolom *case name* , *description dan investigator name*. cohtoh dapat dilihat pada gambar 4.



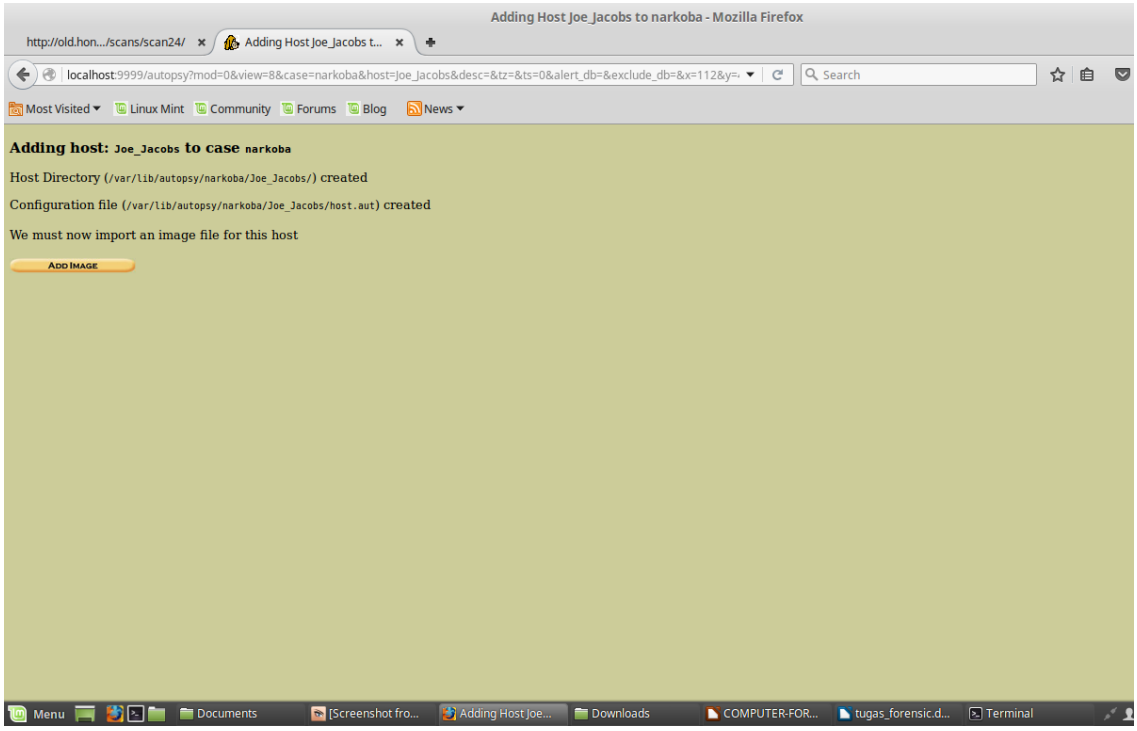
Gambar 4 : Create komponen case

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

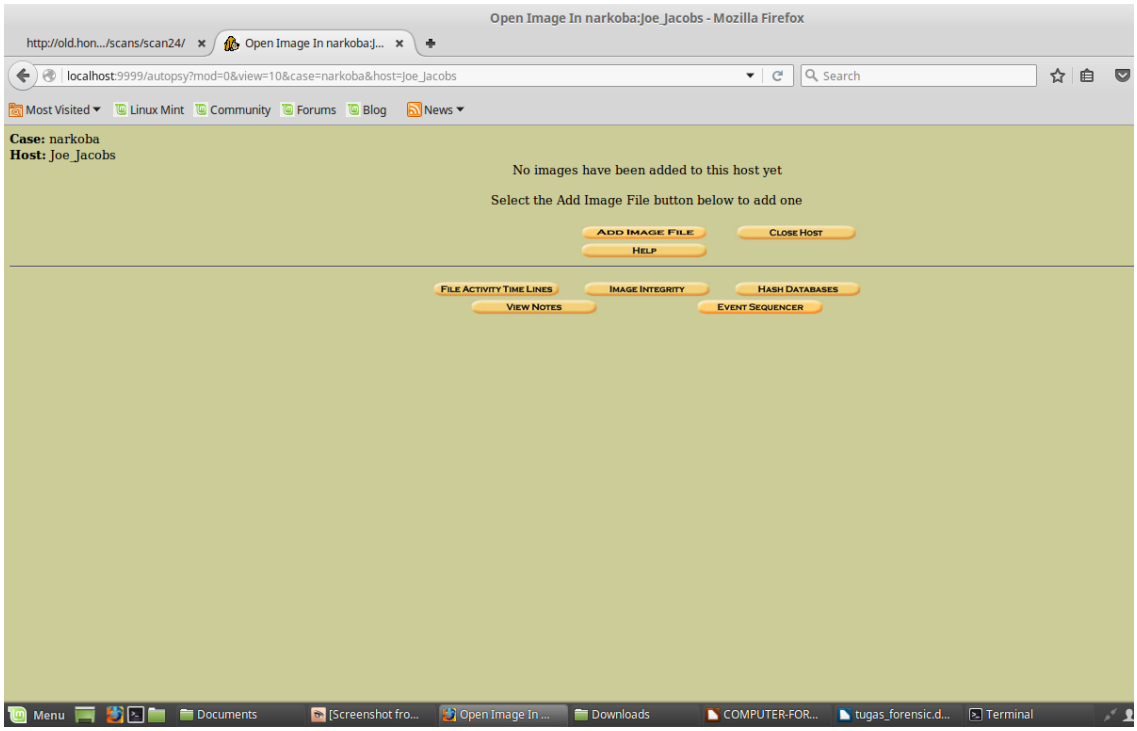


Gambar 5 : Add host

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

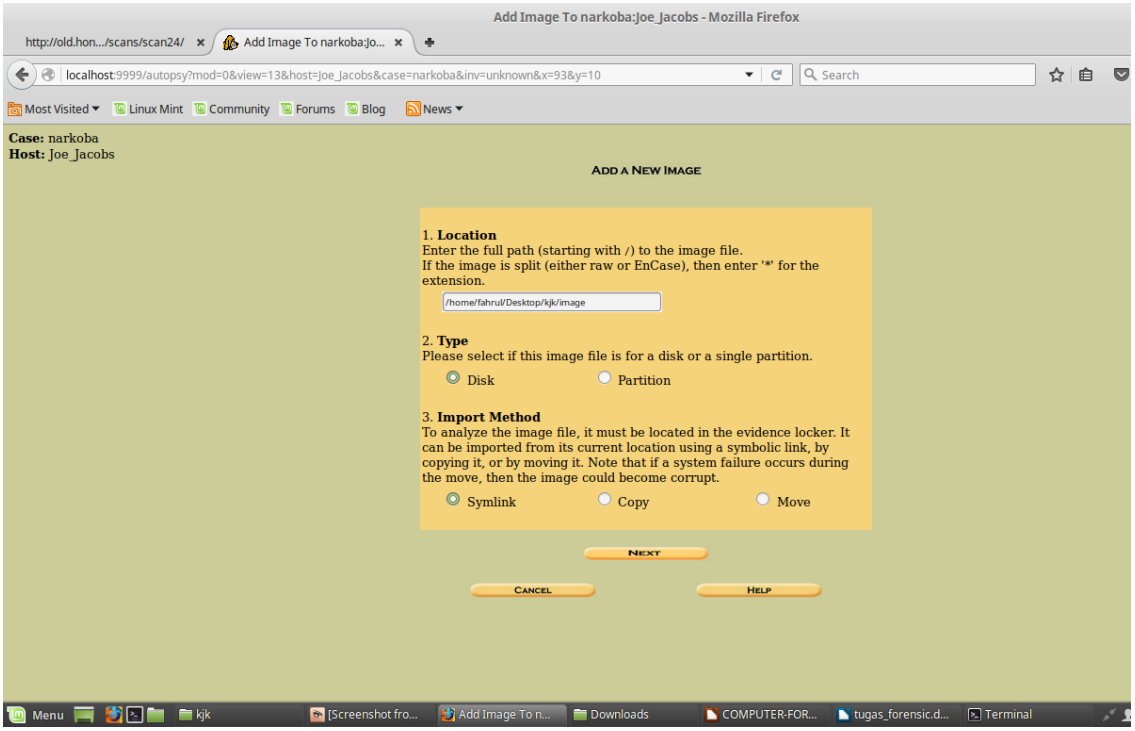


Gambar 6 : Add image (file)

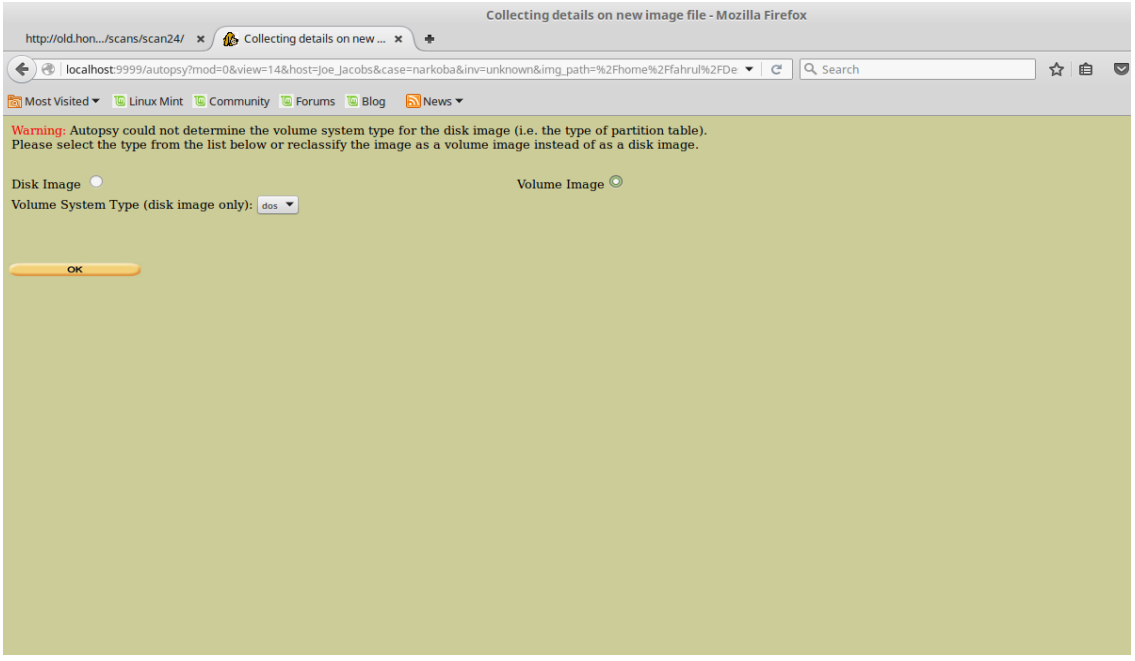


Gambar 7 : Home case

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, kemudian *next*.

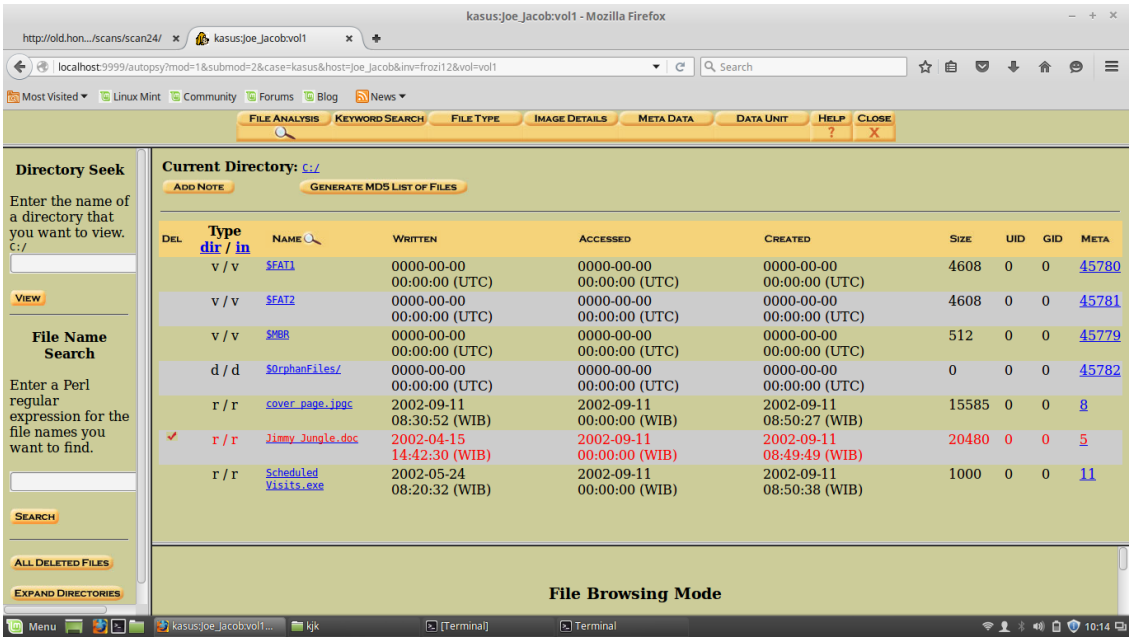


Gambar 8 : Options file image

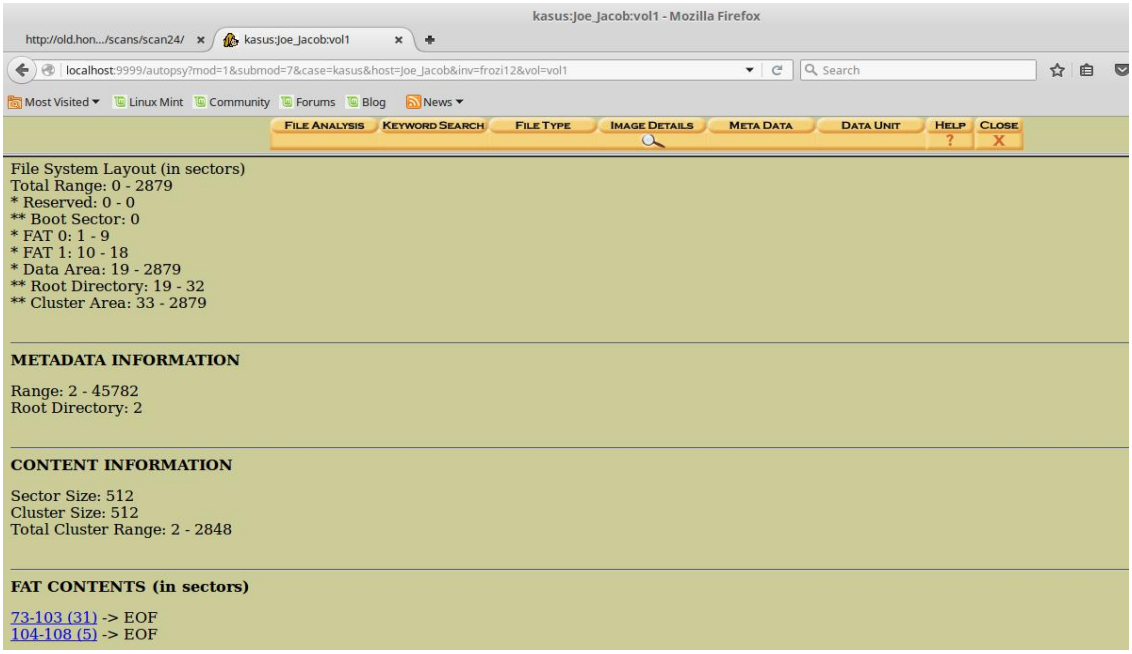


Gambar 9 : Type file

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. Pada gamber 10 merupakan isi dari informasi dari hardrive tersebut. Terdapat banyak kegiatan mulai dari kapan palaku menulis mengakses serta membuat file. Pada list terdapat werna merah berarti file tersebut telah dihapus.



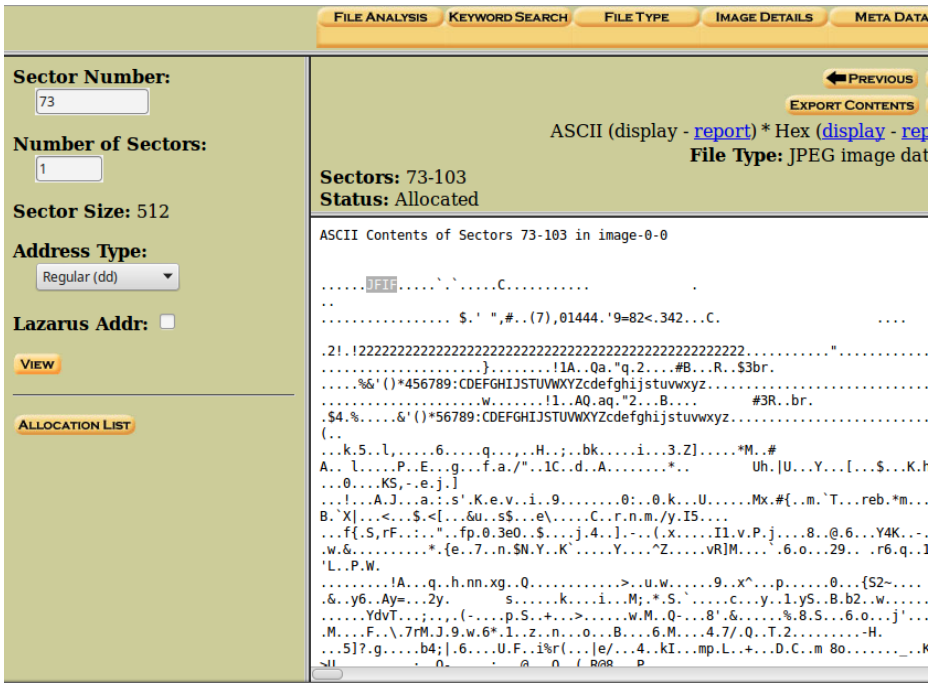
Gambar 10 : Tab file analyze



Gambar 11 : Tab image details

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.

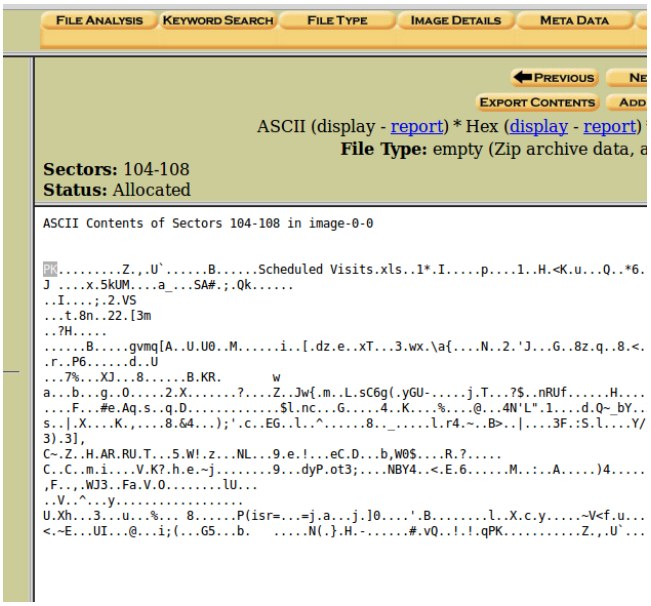
Pada sector 73 – 103 terdapat format yang sulit dimengerti bagi yang tidak mengetahuinya kita dapat mengidentifikasikan dengan cara melihat bit pertama atau informasi hexa yang terdapat pada awal tulisan. Yang dapat pada baris pertama yaitu JFIF , dan kemudian informasi tersebut dapat dilihat jenis dan dan informasi di *list of file singnature* seperti yang terilihat pada gambar 13. Lakukan hal yan sama pada sector 104-108.



Gambar 12 : Sector 73-103

jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿØÿÛ	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 13 : *List of file signature for* JFIF

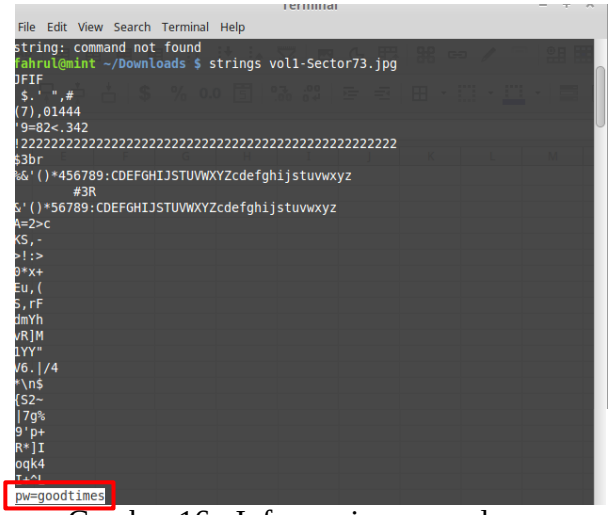


Gambar 14 : Sector 104-108

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)

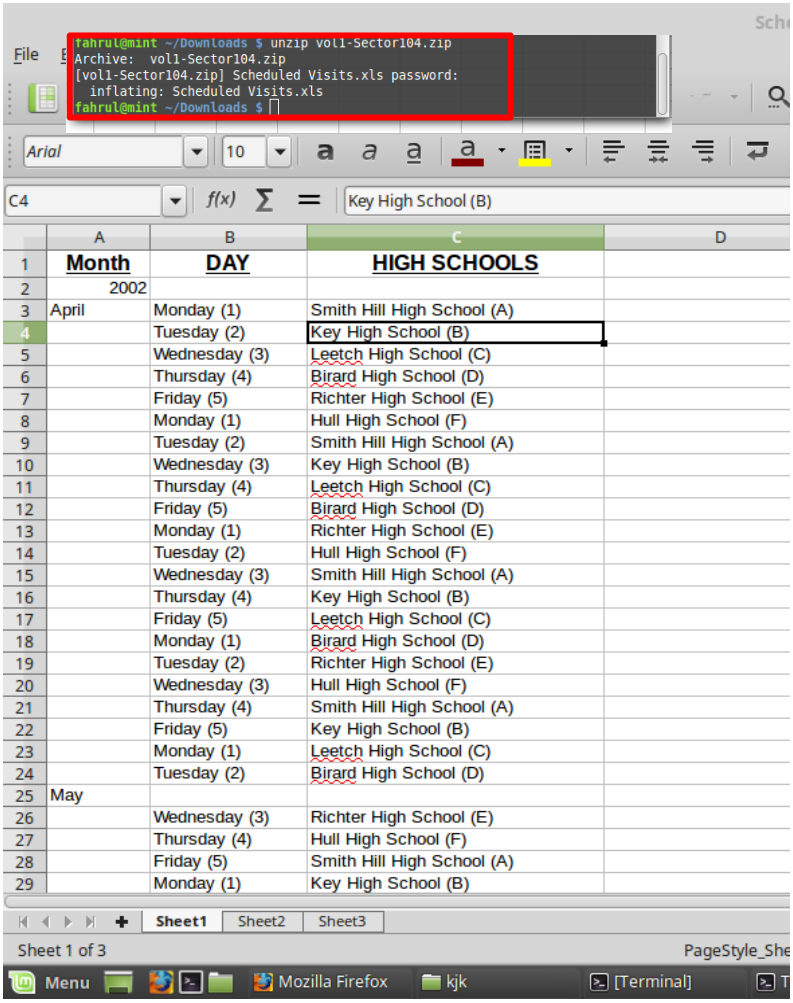
Gambar 15 : *List of file signature for PK*

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 16 : Informasi password

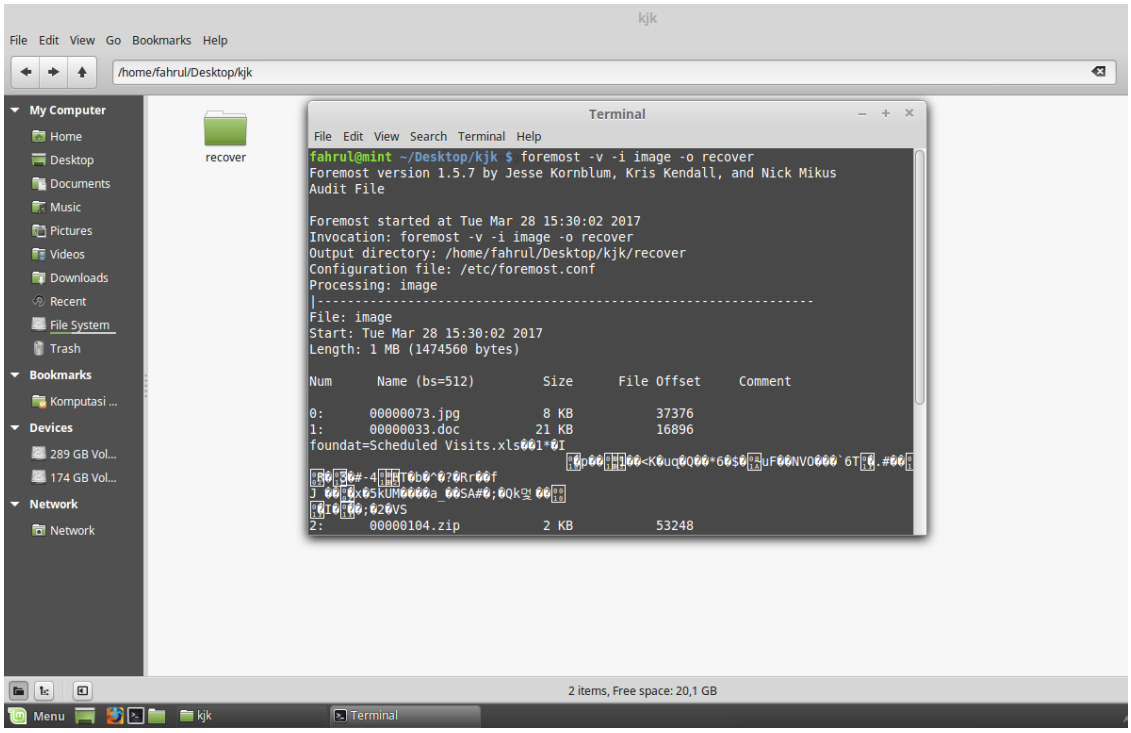
Dari file sector yang telah di rename sebelumnya, dengan menggunakan tools string kita telah mendapatkan informasi yang terdapat pada file tersebut. Pada gambar 16 telah dilakukan string , informasi yang terdapat pada file tersebut adalah password **“pw=goodtimes”,** password tersebut digunakan untuk membuka file zip pada file sector 104.zip



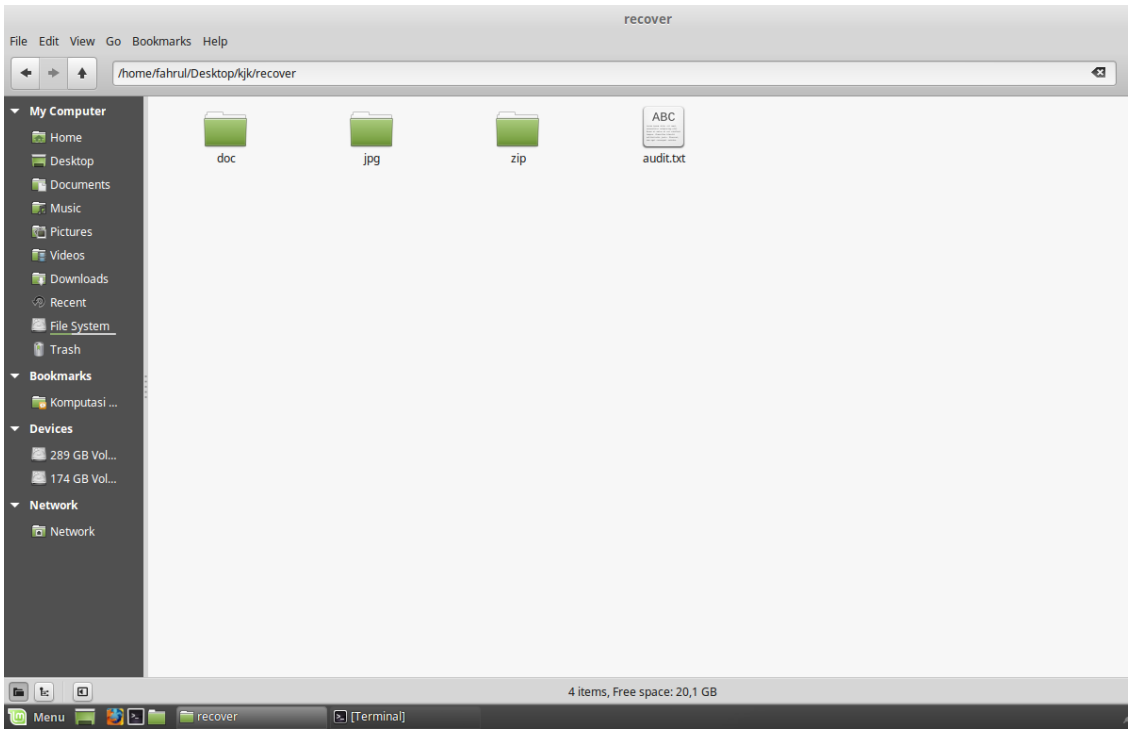
	A	B	C	D
1	**Month**	**DAY**	**HIGH SCHOOLS**	
2	2002			
3	April	Monday (1)	Smith Hill High School (A)	
4		Tuesday (2)	Key High School (B)	
5		Wednesday (3)	Leetch High School (C)	
6		Thursday (4)	Birard High School (D)	
7		Friday (5)	Richter High School (E)	
8		Monday (1)	Hull High School (F)	
9		Tuesday (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 17: Isi file sector 104.zip setelah di extract

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 –v –i nama_file –o recover***” pada terminal. Dapat dilihat pada gambar 18, setelah melakukan perintah diatas maka akan menampilkan folder yang berisi tentang informasi yang bersangkutan seperti yang terlihat pada gambar 19.

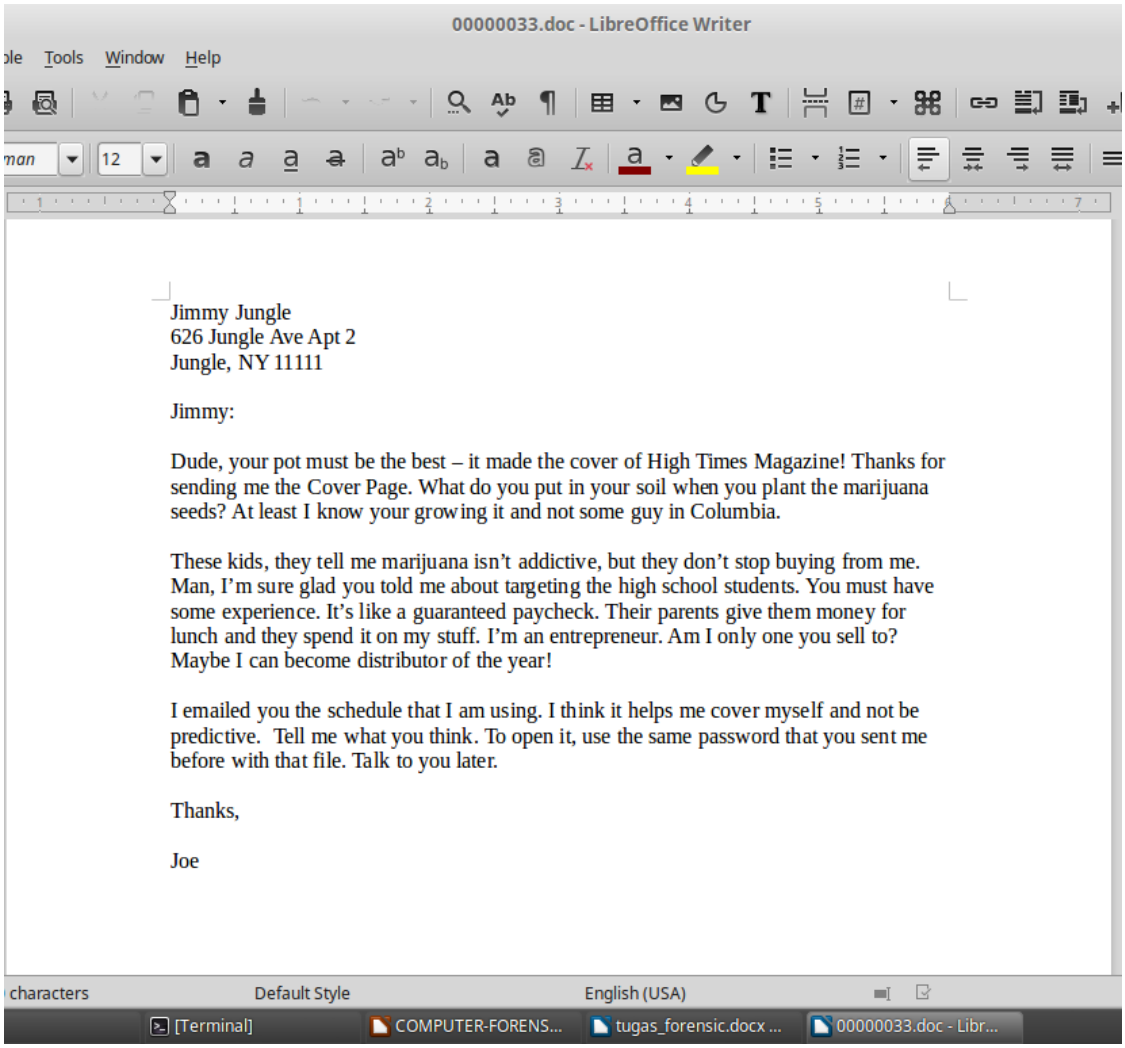


Gambar 18 : Menggunakan Foremost



Gambar 19 : Isi folder recover

Didalam file recover terdapat folder doc yang berisi informasi seperti surat (email) yang telah dikirimkan untuk orang yang bersangkutan , isi file tersebut dapat dilihat pada gambar 20.



Gambar 20: isi file doc

Jawaban no 1 yang menjadi pemasok (supplier) joe Jacob adalah jimmy jungle, informasi tersebut terdapat pada sebuah email yang dikirimkan pada jimmy. Dapat dilihat pada gambar 20.

Jawaban no 2 yang didapatkan dalam file gambar (jpg) adalah informasi password yang kita butuhkan untuk membuka atau mengekstrak file zip. Jadi informasi dalam file gamba (jpg) ini sangatlah penting, jika tidak ditemukan maka kita akan kesulitan untuk mengetahui informasi yang ada didalam file zip.

Jawaban no 3 , terdapat beberapa sekolah yang di kunjungi 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 17.

Jawaban no 4 , 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 prubahan format tersebut diletakan pada sebuah file yang bernama **image**, file image ini pula di letaka dalam file zip.