KEAMANAN JARINGAN KOMPUTER

Eko Pratama

09011181320004

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

TUGAS 6

KOMPUTER FORENSIK

Komputer Forensik adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan digital untuk dapat disajikan sebagai barang bukti yang sah di pengadilan.

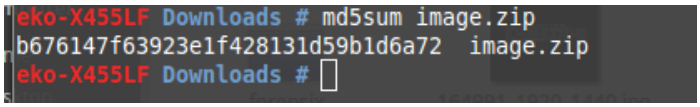
Tugas : Diminta bantuan untuk mendapatkan informasi tentang kasus narkoba

- Tampilkan capture langkah langkahnya
- Jawab pertanyaan untuk memberikan informasi

Tools yang digunakan :

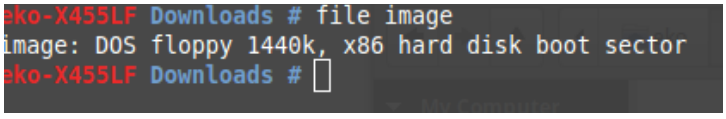
- AutoPsy
- Foremost
- Strings

Langkah pertama yang harus dilakukan adalah ketikan perintah md5sum pada file zip yang telah di downloads untuk memeriksa keaslian dari file, yang perlu diingat kita harus masuk kedalam direktori dari file penyimpanan image.zip tersebut



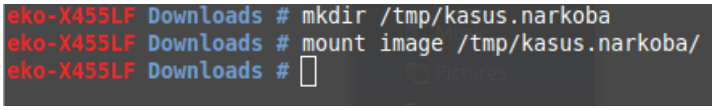
Gambar 1. Perintah md5sum

Kemudian ketika kita telah memastikan file yang didownload adalah file asli maka langkah berikutnya adalah masukan perintah file image yang bertujuan untuk melihat tipe file yang digunakan. Dalam hal ini file yang digunakan adalah DOS



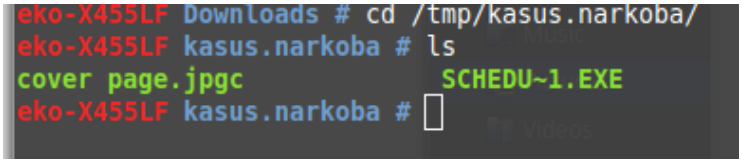
Gambar 2. Perintah file image

Langakah berikutnya adalah membuat direktori baru yaitu kasus.narkoba lalu, lakukan mount image kedalam direktori tersebut.



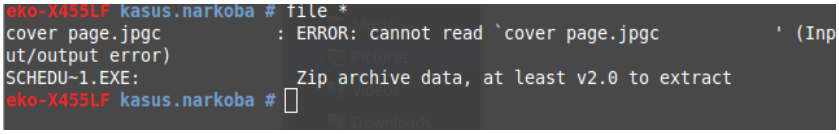
Gambar 3. Perintah mount image

Setelah berhasil kita masuk ke direktori yang sudah kita buat tadi lalu masukkan perintah ls untuk melihat apakah dalam direktori kasus.narkoba tersebut telah terdapat isi

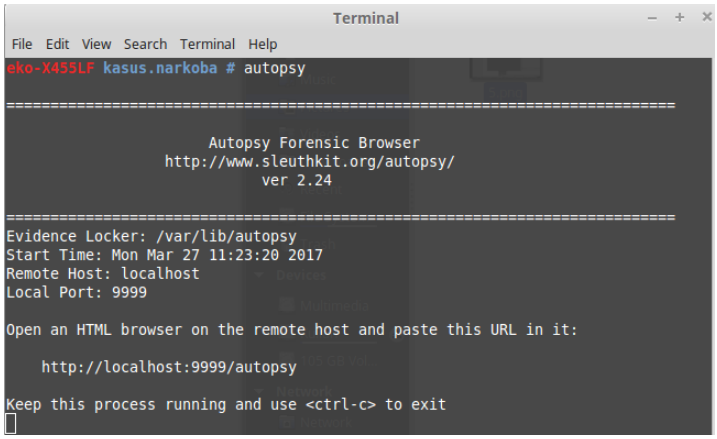


Gambar 4. Melihat isi Direktori

Masukkan perintah File * dimana maksudnya adalah untuk mengekstrak semua file yang terdapat pada direktori kasus.narkoba tersebut

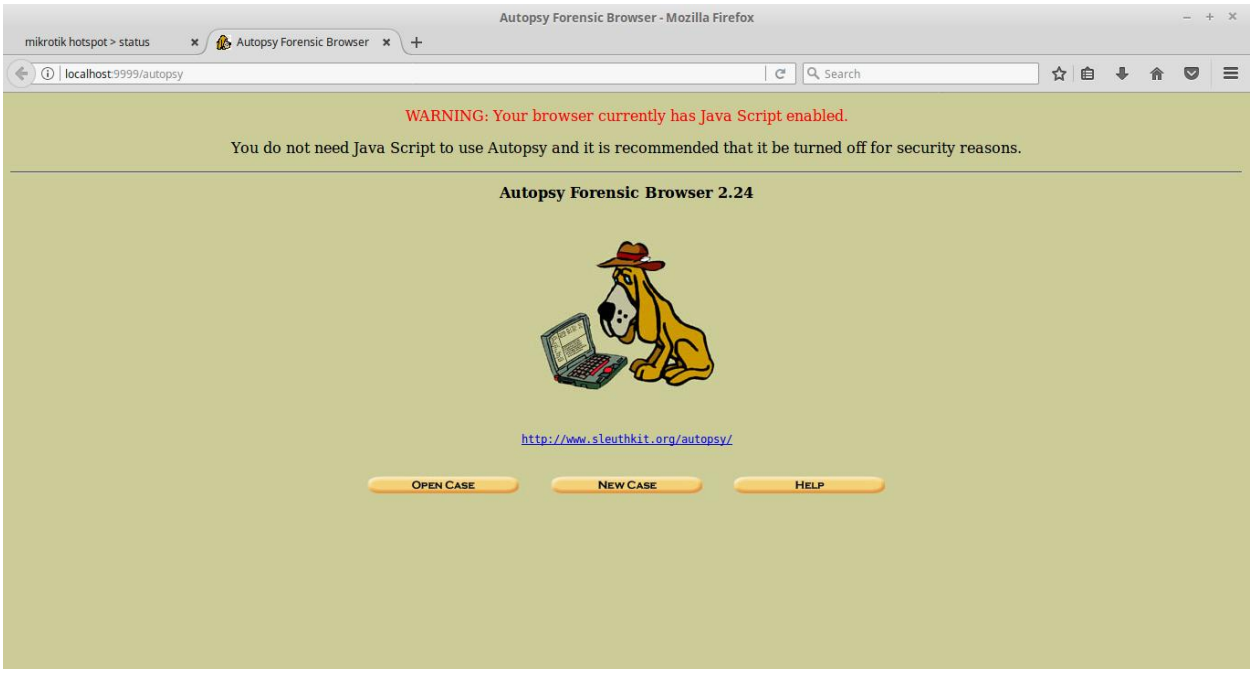


Gambar 5. Perintah ekstrak



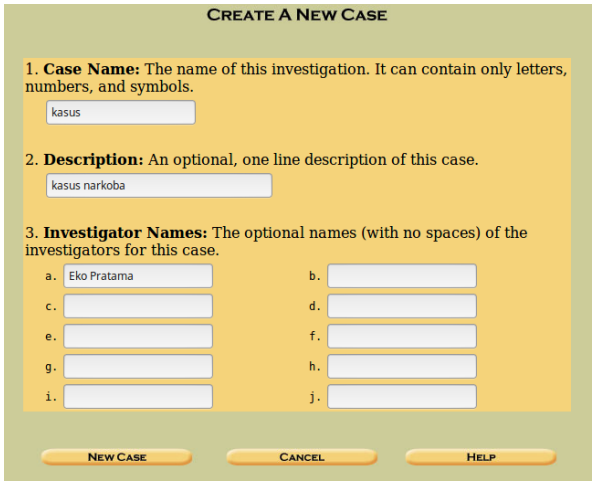
Gambar 6. Buka Tools Autopsy

Perintah berikutnya adalah buka tools autopsy pada terminal seperti pada gambar 6 lalu biarkan tetap running pada terminal dan jangan di tutup. Kemudian buka autopsy pada web dengan memasukkan localhost sesuai dengan localhost yang diberikan oleh autopsy diterminal. Tampilan web autopsy dapat dilihat pada gambar 7



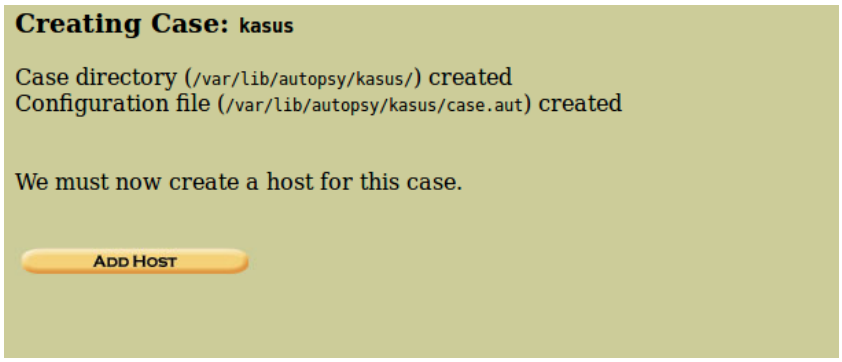
Gambar 7. Tampilan web Autopsy

Untuk membuat kasus baru pilih New Case lalu, inputkan sesuai kasus yang sedang ditangani.



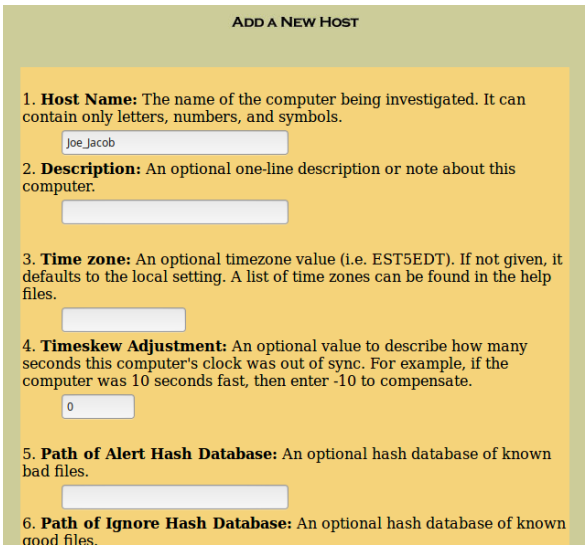
Gambar 8. Membuat kasus baru

Pada gambar 9 kasus telah brhasil dibuat dengan nama kasus. Lalu, pilih ADD HOST



Gambar 9. Kasus berhasil Dibuat

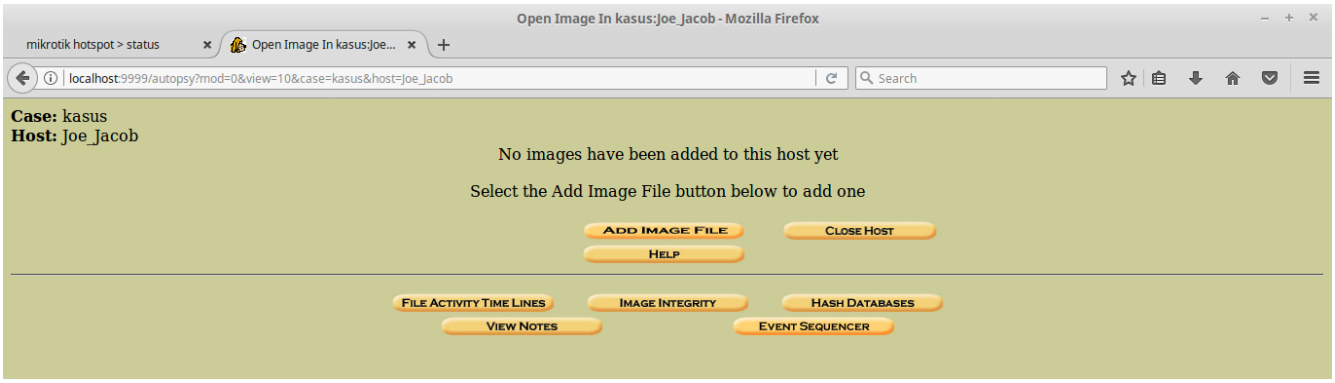
Setelah masuk kedalam add host kita akan disuruh menginputkan host name. dalam hal ini saya menginputkan host namenya adalah Joe_Jacob sesuai dengan pratikum yang dilakukan.



Gambar 10. Add New Host

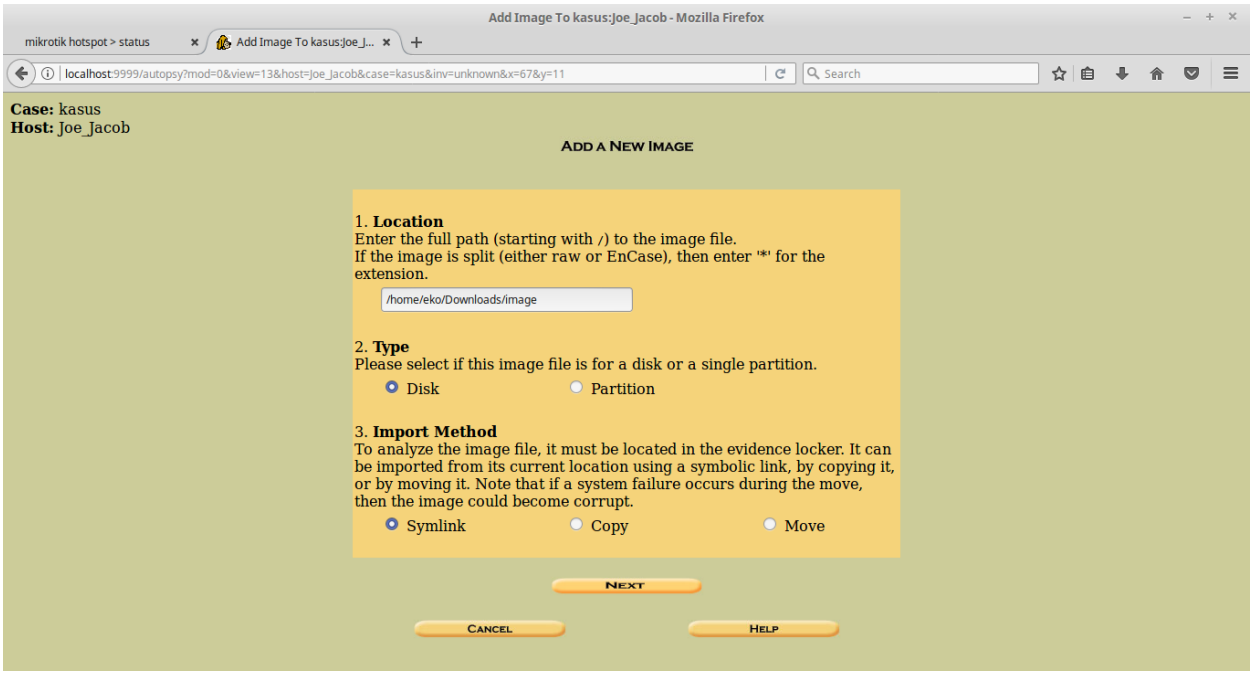
Gambar 11. Berhasil menambah Host

Setelah berhasil membuat case dengan nama kasus dan Host dengan nama host Joe_Jacob langkah selanjutnya adalah dengan memilih Add Image File



Gambar 12. Add Image File

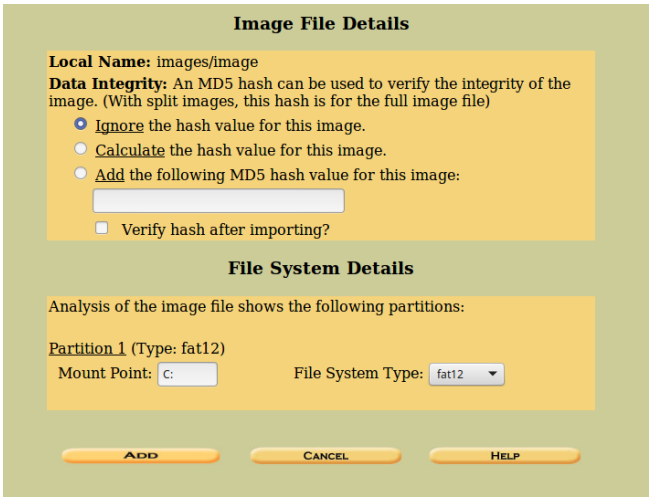
Setelah memilih Add Image File kita akan diarahkan untuk memberikan lokasi penyimpanan dari gambar tersebut dalam hal ini saya letakan di direktori ***/home/eko/Downloads/image*** kemudian untuk Type tetap pilih Disk dan symlink untuk Import Method lalu tekan next



Gambar 13. Menentukan lokasi penyimpanan

Pilih Volume Image untuk menentukan Tipe sistem Volume yaitu DOS sesuai dengan file yang digunakan dalam kasus ini

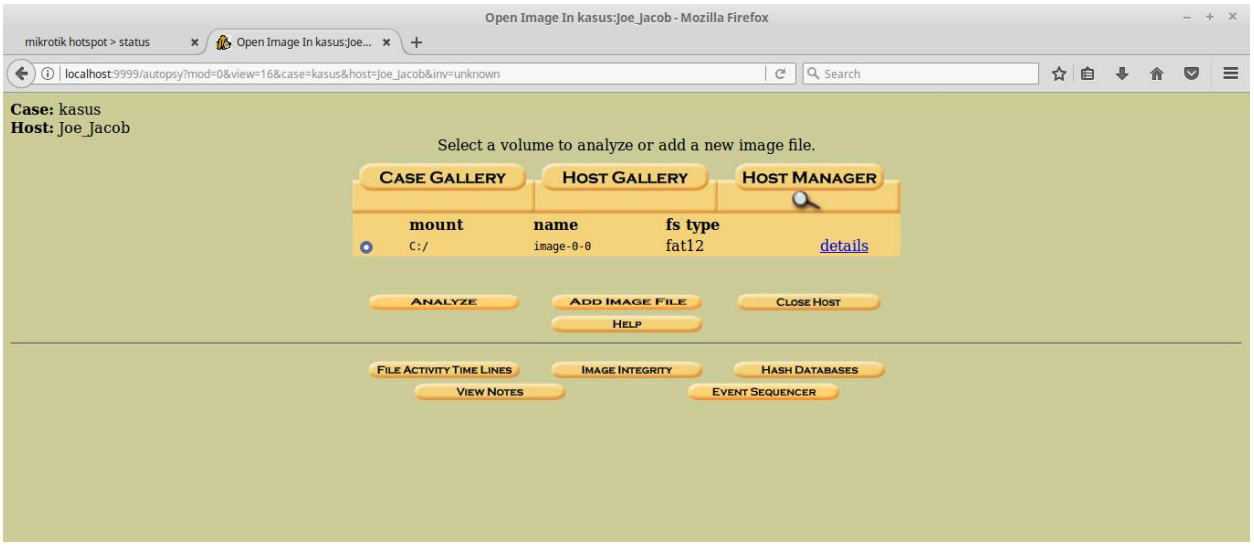
Gambar 14. Volume Image DOS



Gambar 15. Image File Details

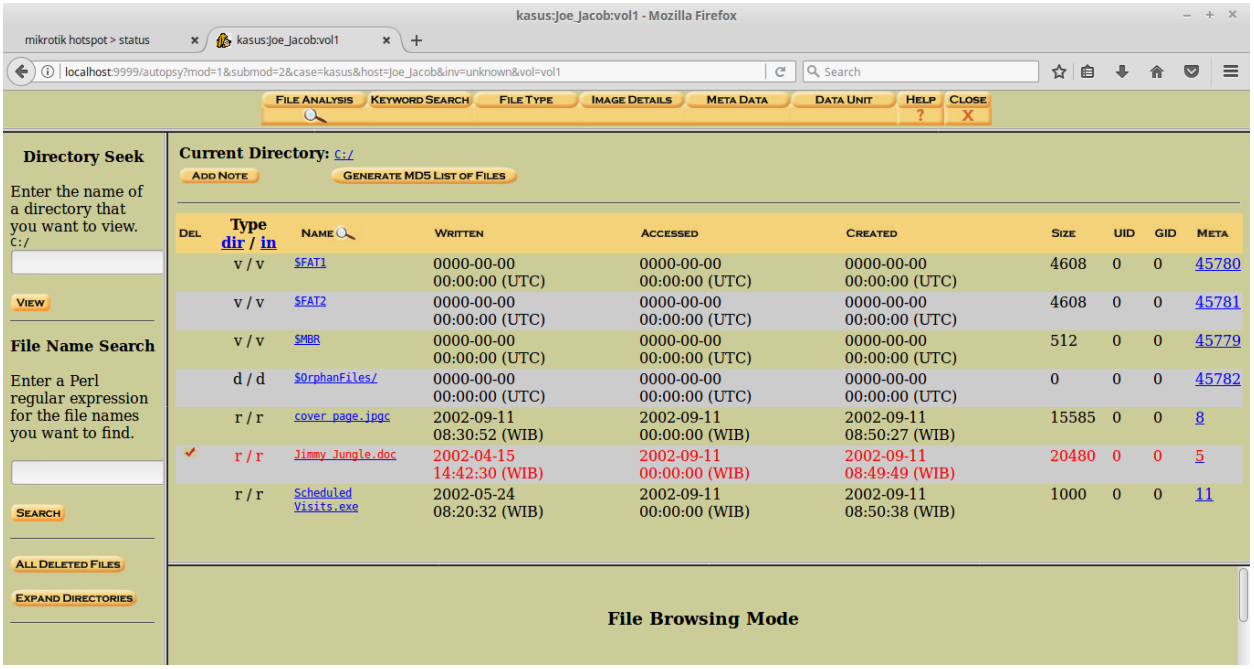
Gambar 16. Testing Partitions

Pada Gambar 16 setelah kita melakukan ADD Image File Details, maka akan mucul tampilan testing partition dan klik OK, kemudian akan masuk ke tampilan seperti Gambar 17.



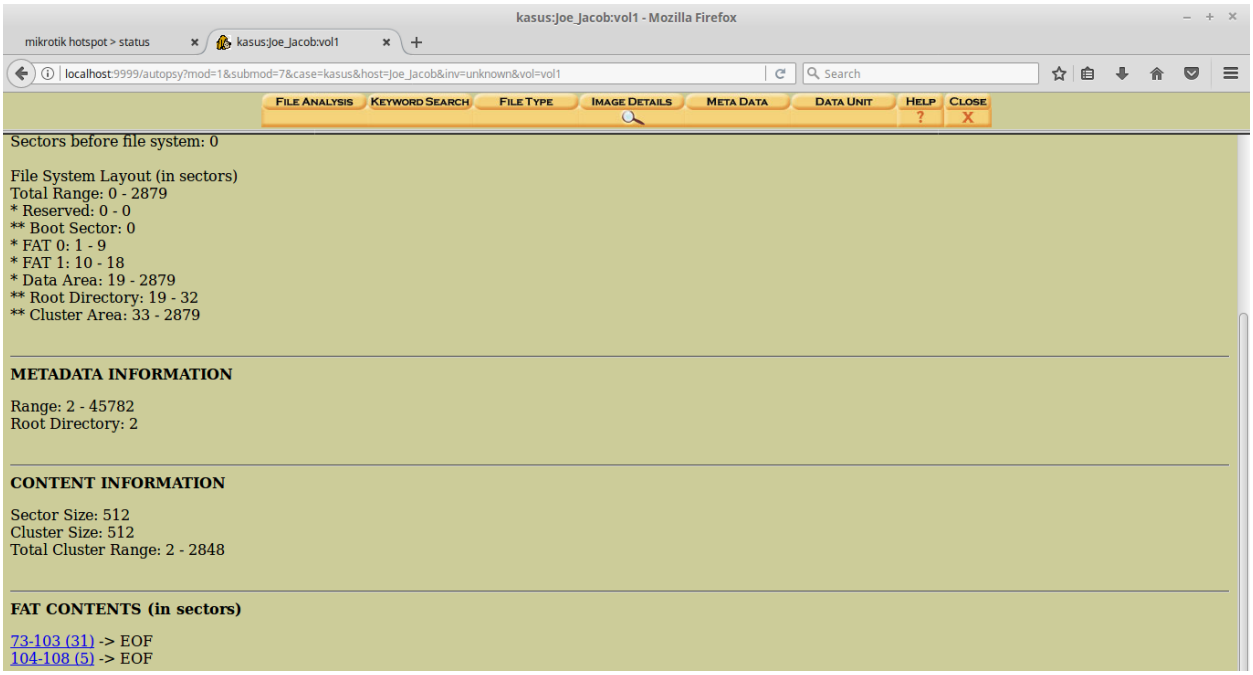
Gambar 17. Tampilan Volume Analyze

Dari gambar 17 ini pilih ANALYZE untuk melihat file analyzenya dan akan muncul tampilan seperti pada gambar 18 dan ketika kita memilih image detail akan muncul tampilan seperti pada gambar 19

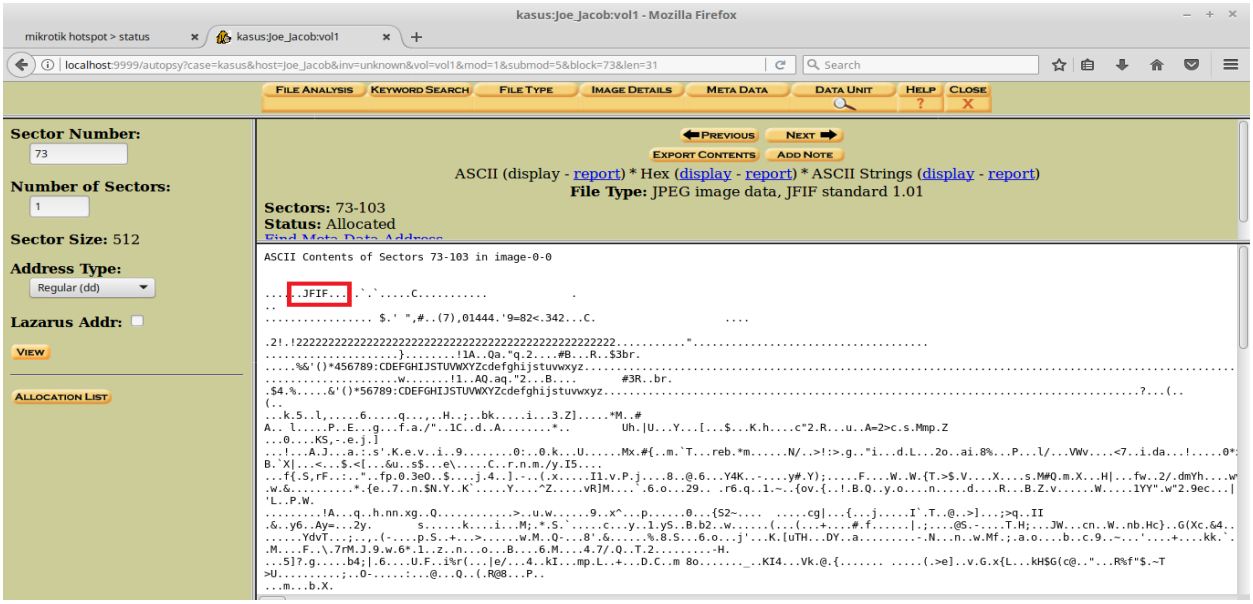


Gambar 18. Analyze Details

Pada Gambar 19 dibawah ketika kita memilih image detail kita dapatkan 2 FAT Contens yaitu konten yang berisi Sector dan status yang merupakan isi dari file image yang pertama. Kita buka conten yang pertama dengan sector 73-103.



Gambar 19. Image Details

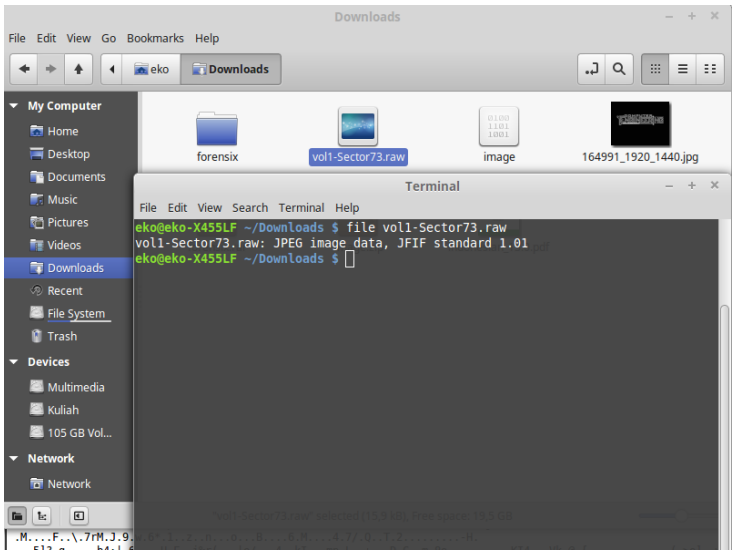


Gambar 20. Data Unit Image pertama

Setelah kita buka konten gambar pertama dengan sector 73-103 didapatkan hasil Pada Gambar 20, dimana pada gambar tersebut terdapat sebuah kotak yang saya tandai yaitu JFIF salah satu format dari image pertama. Dan pada gambar 21 saya mencoba mencari apa itu format JFIF dan saya berhasil mendapatkan informasi dari Wikipedia bahwa JFIF merupakan salah satu dari Format gambar jpg/jpeg.

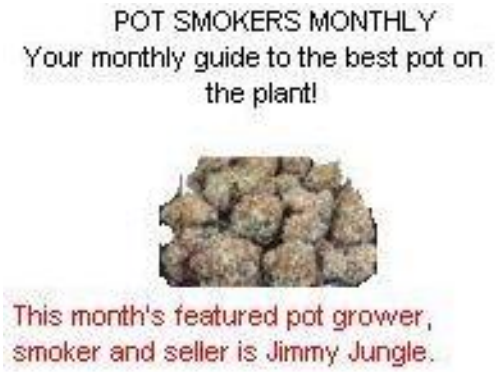
exr	OpenEXR image	0	v/1.	76 2F 31 01
bpg	Better Portable Graphics format[7]	0	BPGû	42 50 47 FB
jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿØÿÛ ÿØÿà ..J F IF..	FF D8 FF DB FF D8 FF E0 nn nn 4A 46 49 46 00 01

Gambar 21. Format JFIF



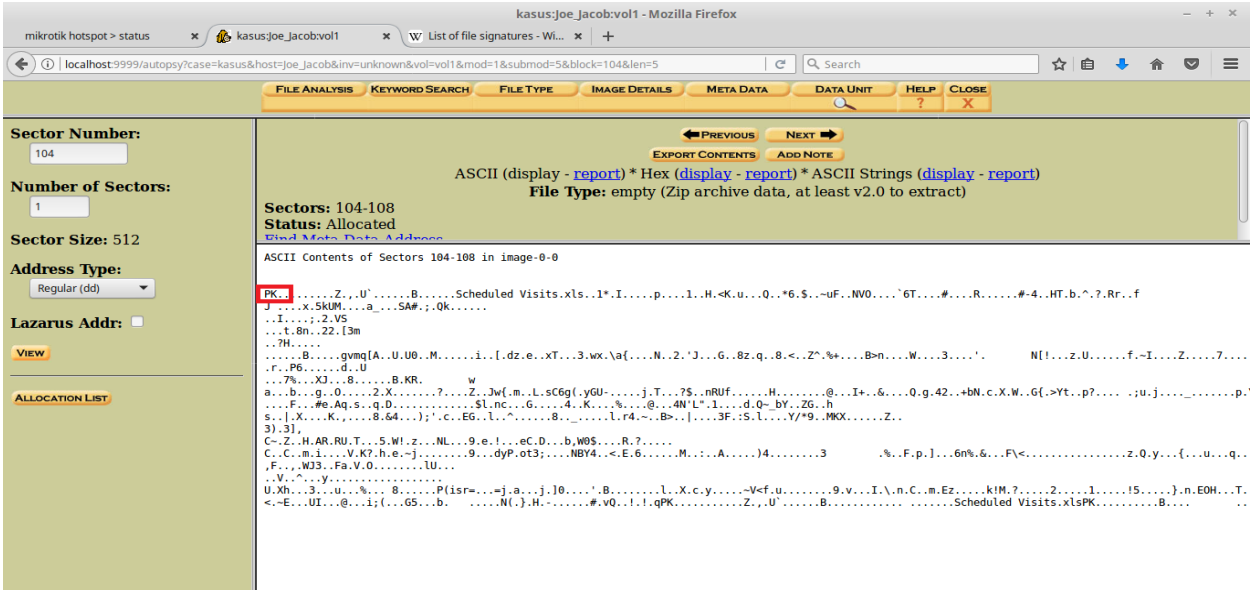
Gambar 22. Perintah Membuka Image

Setelah kita mengetahui bahwa JFIF merupakan format JPG/JPEG maka langkah selanjutnya yang akan kita lakukan adalah kita masukan perintah seperti gambar 22. Perlu diingat perintah diinputkan tanpa masuk ke root. Lalu kita buka file tersebut dan akan muncul gambarnya seperti pada gambr 23



Gambar 23. Image Sector 73-103

Setelah kita mengetahui format apa dan isi pada data unit image pertama dengan sector 73-103, selanjutnya kita akan melakukan hal yang sama pada gambar kedua yaitu sector 104-108. Seperti gambar 24. Dimana digambar ini saya memberi kotak warna merah terhadap kata PK. Lakukan hal yang sama seperti yang pertama tadi dengan mencari tahu informasi PK dari wikipedia

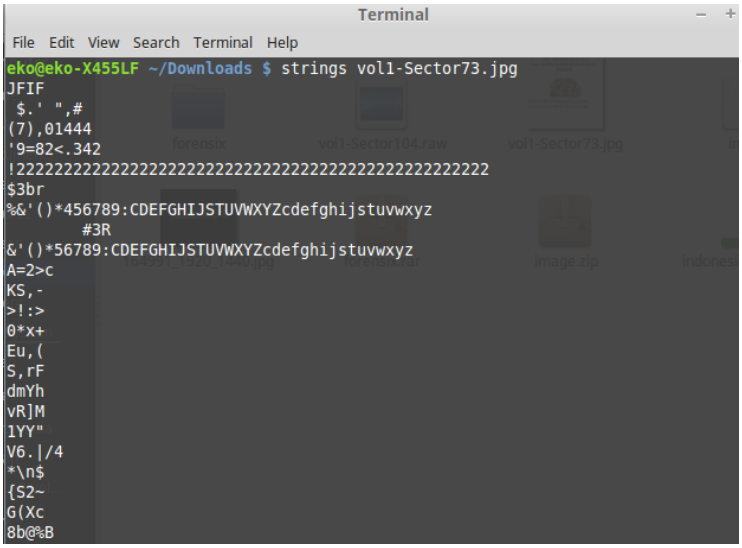


Gambar 24. Data Unit Image kedua

lz	lzip compressed file	0	LZIP	4C 5A 49 50
exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A
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 25. Format PK

Setelah mencari informasi tentang format Pk didapatkan hasil bahwa format PK sama halnya dengan format ZIP. Seperti yang ditampilkan pada gambar 25.

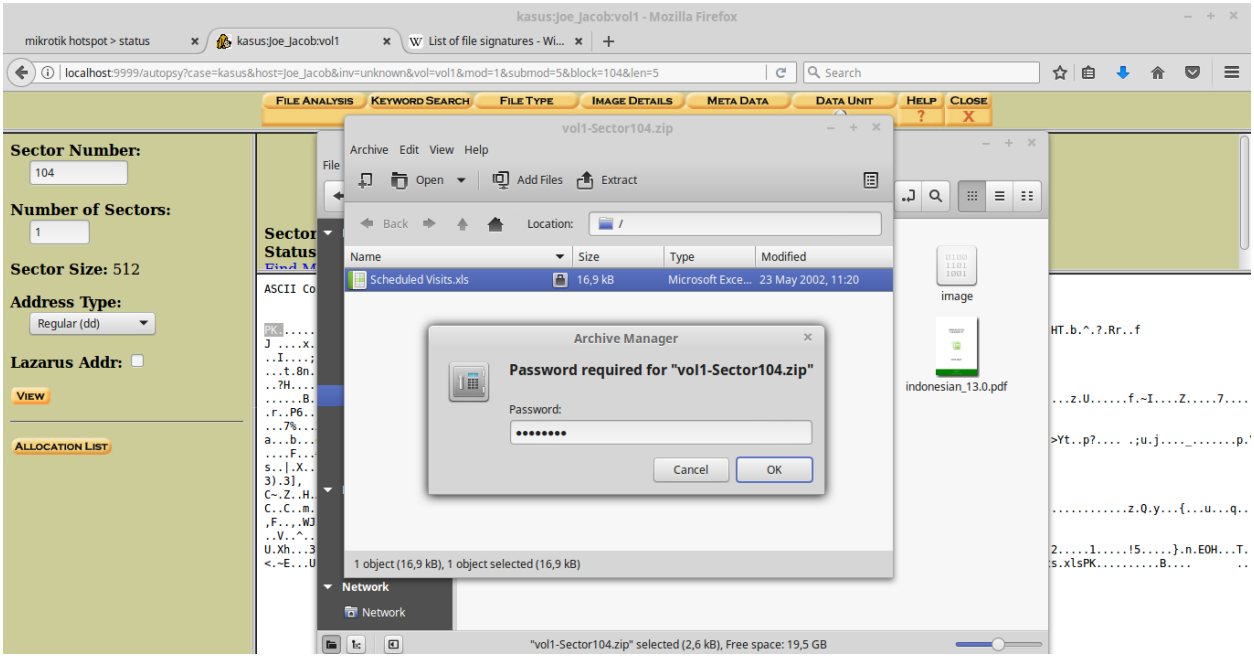


Gambar 26. Perintah Strings Image

Setelah mencari tahu informasi tentang PK maka yang harus dilakukan adalah melakukan strings terhadap file image sector 73-103 untuk mendapatkan password. Pada gambar 27 password berhasil didapatkan yaitu goodtimes. Password inilah yang digunakan untuk mengakses file pada file image sector 104.

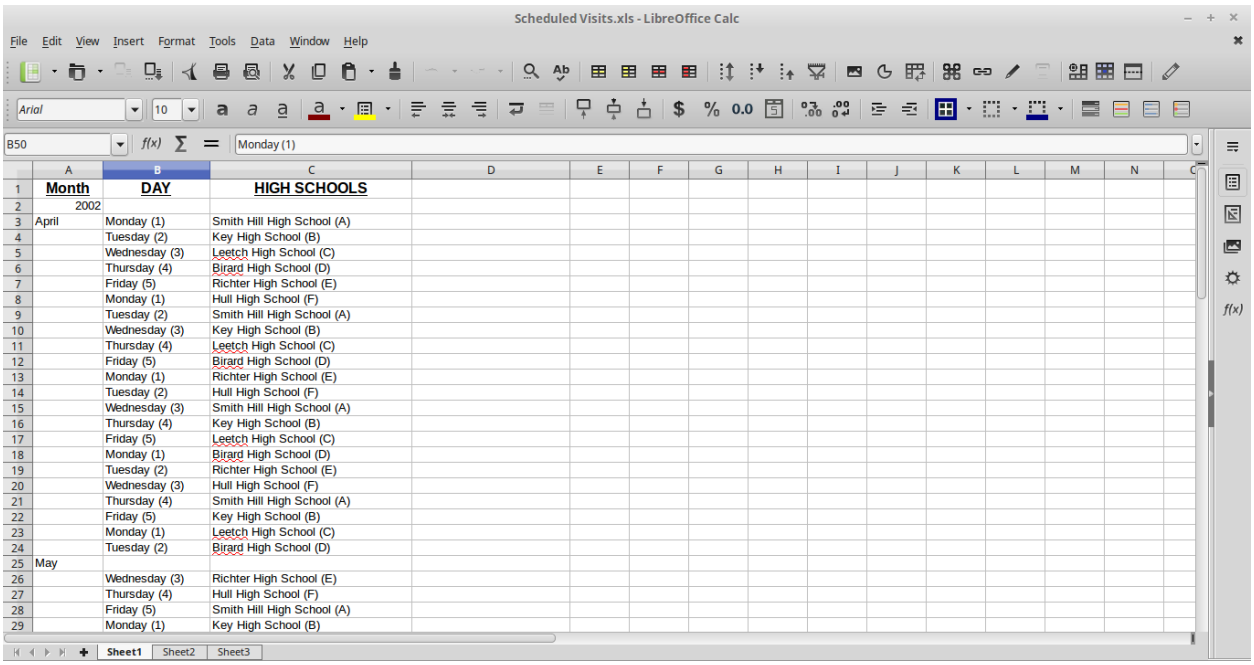
Gambar 27. Mendapatkan Password

Gambar 28. Sector 104



Gambar 29. Open Password

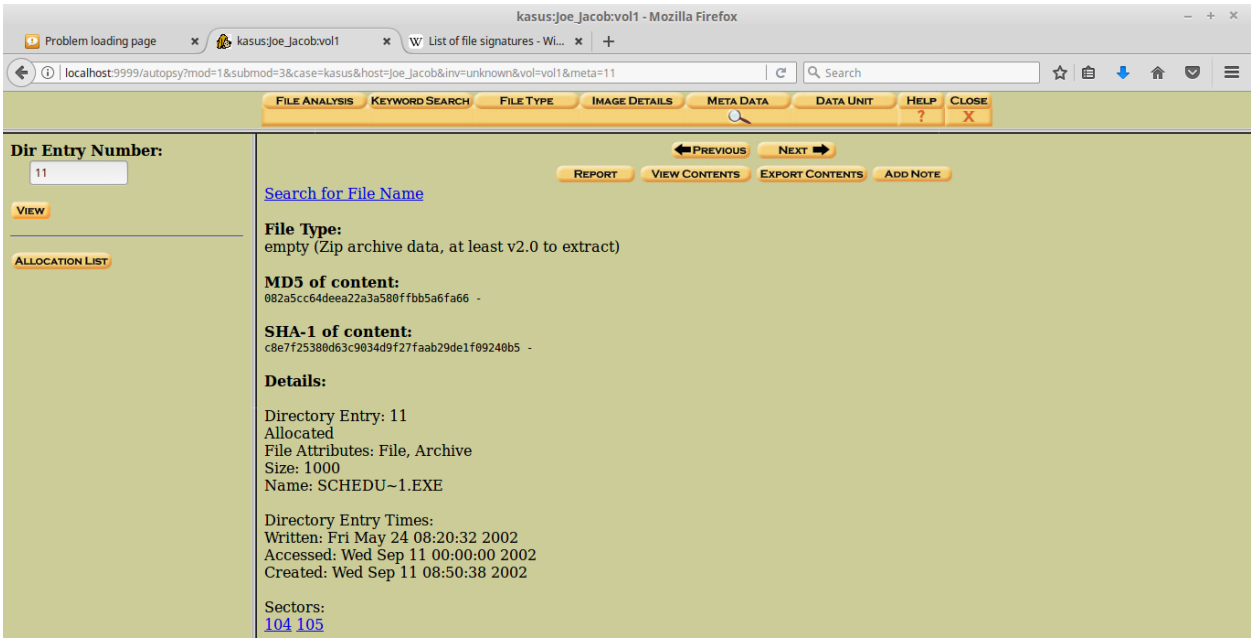
Pada gambar 28 dan gambar 29 dinsini saya mencoba melakukan akses membuk file tersebut tetapi diminta password. Lalu, saya memasukan password yang telah saya dapatkan tadi untuk masuk ke akses tersebut. Dan saya berhasil mendapatkan file Scheduled seperti pada gambar 30.



	Month	DAY	HIGH SCHOOLS
1			
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)

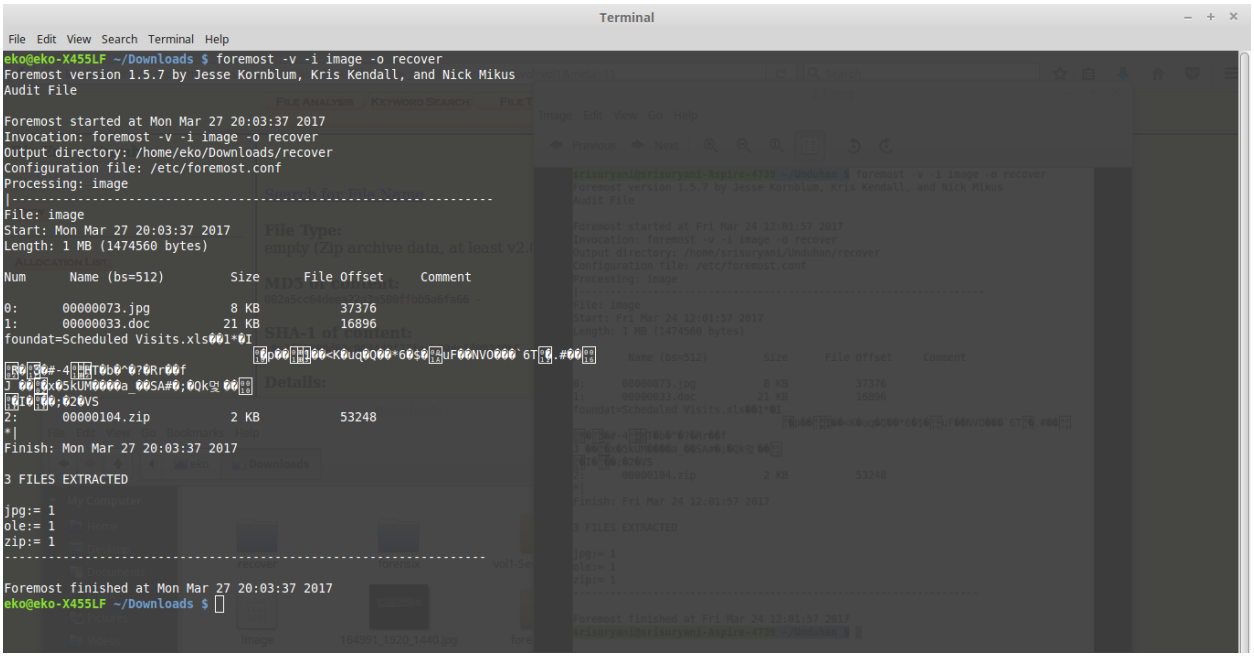
Gambar 30. File scheduled

Digambar 30 ini saya berhasil mendapatkan info tentang rentetan kegitan untuk mempermudah melacak informasi.

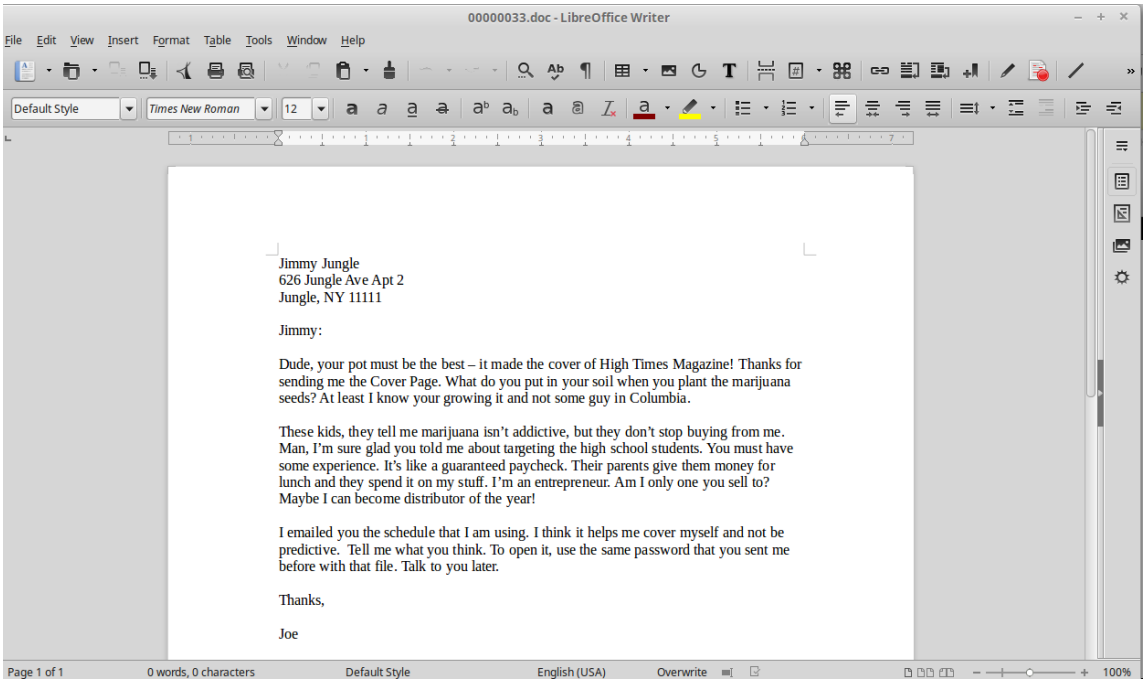


Gambar 31. Meta Data

Pada gambar 32 memasukan perintah foremost dimana perintah ini berfungsi untuk mengembalikan/mengekstrak data yang tertimpa. Dalam hal ini saya memindahkan file tersebut kedalam file recover. Saya berhasil memindahkan 3 file berbentuk jpg,ole dan zip

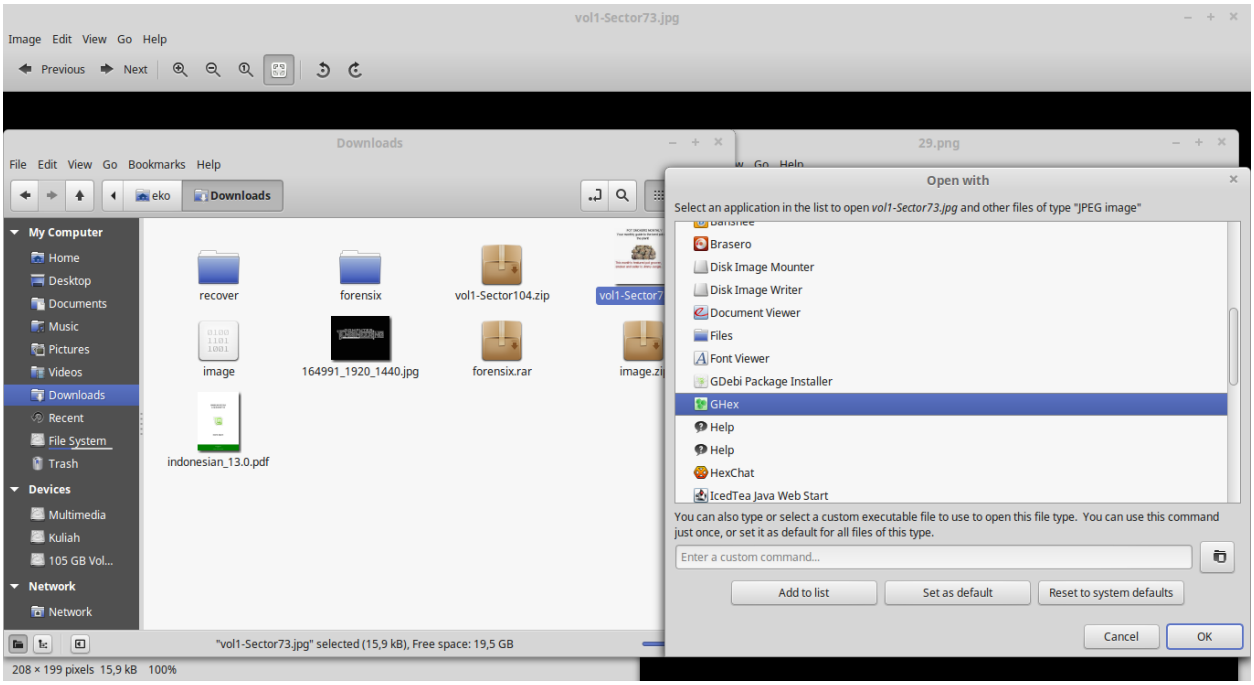


Gambar 32. Perintah Foremost

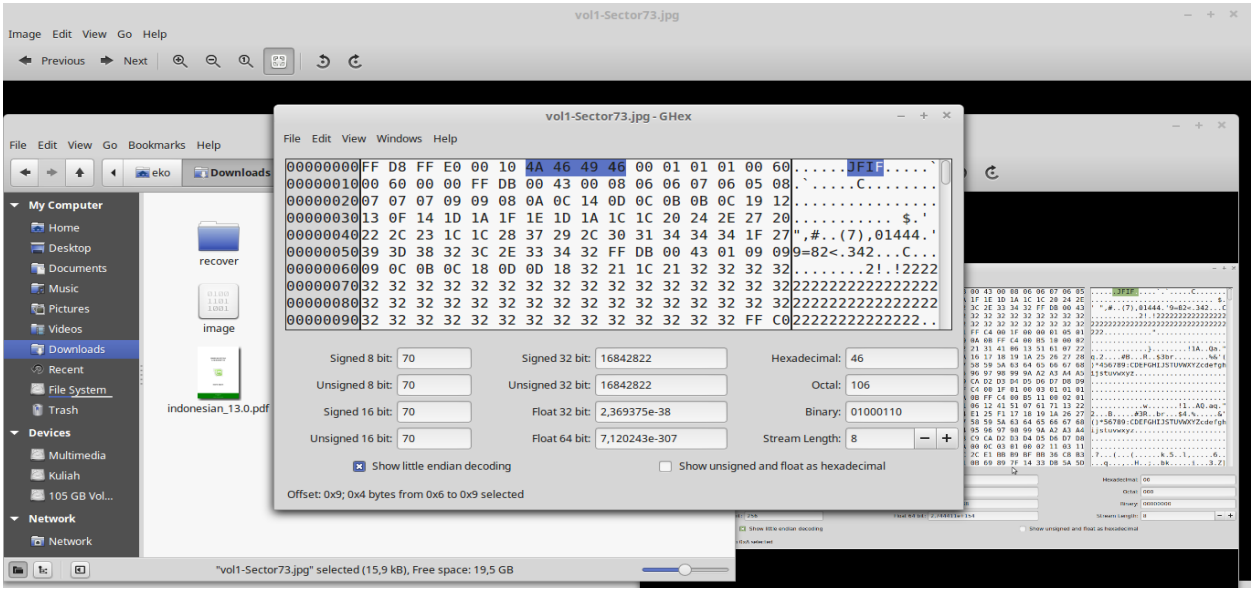


Gambar 33. File .Doc

Setelah itu terdapat file berbentuk Doc yang isinya adalah surat dari joe untuk Jimmy dari sinilah kita dapat menganalisa dan mencari informasi tentang kasus narkoba tersebut. Untuk lebih jelasnya surat tersebut ada pada gambar 33



Gambar 34. Tools GHex



Gambar 35. Konversi Ghex

Pada gambar 34 dan 35 merupakan langkah terakhir saat melakukan pratikum dimana langkah ini merupakan konversi huruf ke biner menggunakan tools GHex. Kita lihat pada gambar 35 saya mencoba menkonversikan JFIF dimana ketika kita blok huruf tersebut maka dengan bantuan tools GHex angka biner dari huruf tersebut akan terblok secara otomatis

Setelah berhasil mendapatkan data maka kita bias memberikan beberapa informasi yang diperlukan untuk bahan penyelidikan. Berikut beberapa pertanyaan yang diminta

1. Siapa pemasok narkoba Joe Jacob dan apa alamatnya?

   Jawab: Pemasok adalah Jimmy Jungle dan alamat tinggalnya di 626 Jungle Ave Apt 2

2. Data penting apa yang terdapat di file coverage.jpg dan mengapa data tersebut penting?

   Jawab: file Scheduled Visit.xls tetapi dalam hal ini file tersebut dapat diakses dengan password. Kenapa penting karena didalam file tersebut terdapat data tentang nama nama sekolah yang menjadi tempat transaksi joe jacob

3. Nama sekolah selain smith hill yang sering menjadi tempat transaksi joe Jacob?

   Jawab: (A) Key High School, (B) Leetch High School, (C) Birard High School, (D) Richter High School dan (E) Hull High School

4. Untuk setiap file proses apa yang diambil oleh tersangka untuk mengelabuhi orang lain?

   Jawab: Mereka mengelabui dengan cara mengganti format zip menjadi raw dari file vol1sector73 dan sector104

5. Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file?

   Jawab: Dalam hal ini proses yang digunakan penyidik adalah dengan mencari informasi informasi penting menggunakan beberapa tools yaitu Autopsy,foremost dan GHex yang memiliki peran masing masing dalam membaca atau mendapatkan data yang kongkrit untuk menjadi barang bukti di persidangan. Diantaranya data yang didapatkan adalah nama nama list sekolah untuk pasokan narkoba serta surat dari pemasok narkoba ke joe Jacob.