TUGAS

KEAMANAN JARINNGAN KOMPUTER

“Komputer Forensik”

DISUSUN OLEH :

MEILINDA EKA SURYANI (09011181320033)

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Komputer Forensik

Menurut Dr. HB Wolfre, definisi dari forensik komputer adalah sebagai berikut: “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.” Sementara senada dengannya, beberapa definisi dikembangkan pula oleh berbagai lembaga dunia seperti:

- The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found; atau
- The science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law. Dimana pada intinya forensik komputer 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.”

Tujuan dari Komputer Forensik :

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.

Fokus Komputer Forensik dibagi menjadi 3 kategori:

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 alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya

Manfaat dari Komputer Forensik:

1. organisasi/perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti2 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.

Objek Forensik

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/informasi backup dari sistem utama.

5. Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya.

6. Beraneka ragam jeis 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).

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. 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?

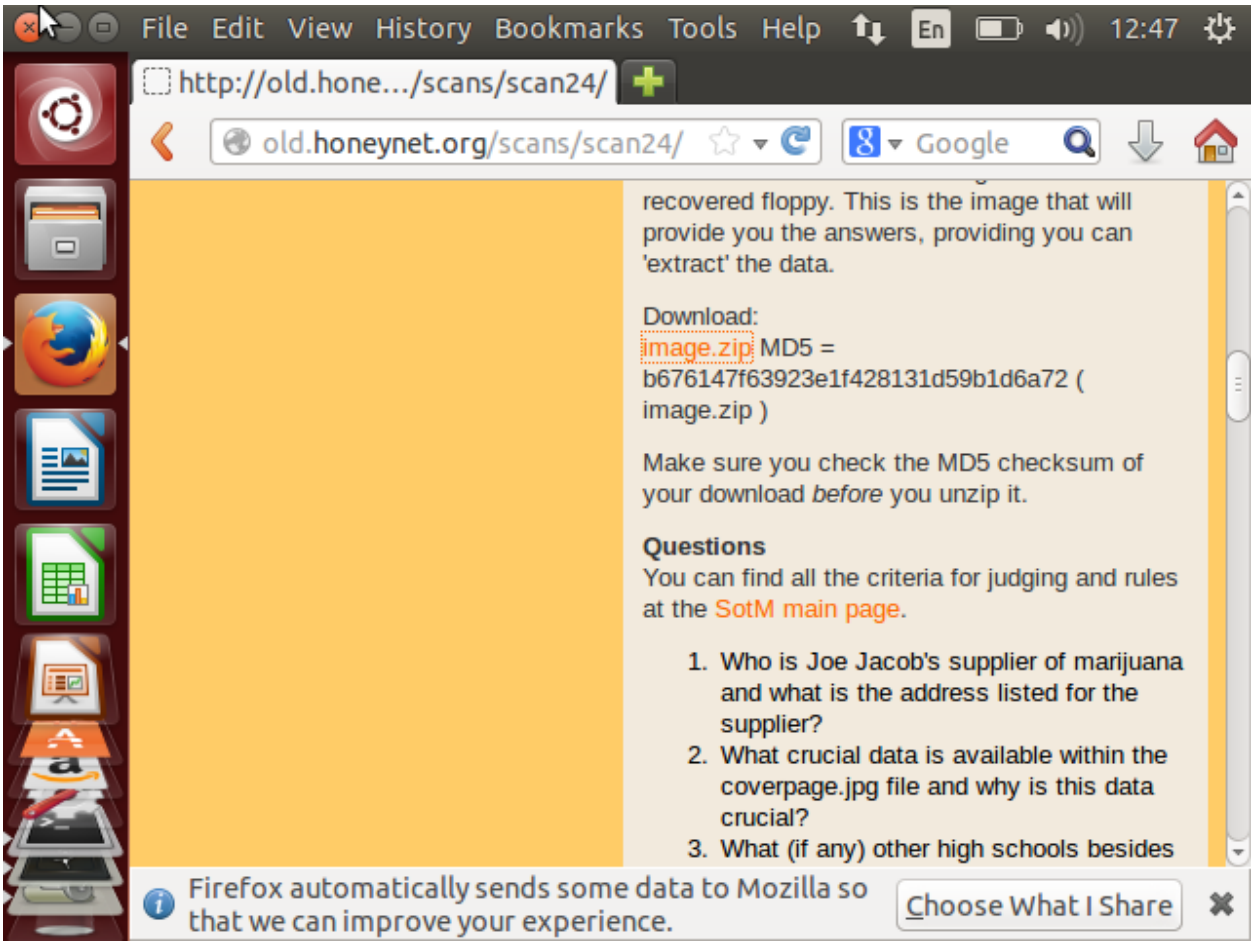
4.For each file, what processes were taken by the suspect to mask them from others?

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

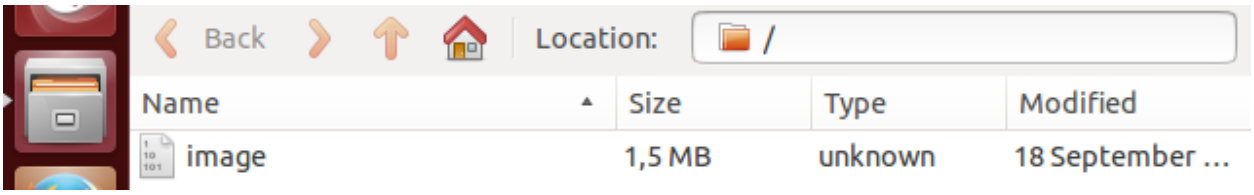
Tools yang diperlukan ialah sebagai berikut:

1. Autopsy
2. Foremost
3. String
4. GHEX

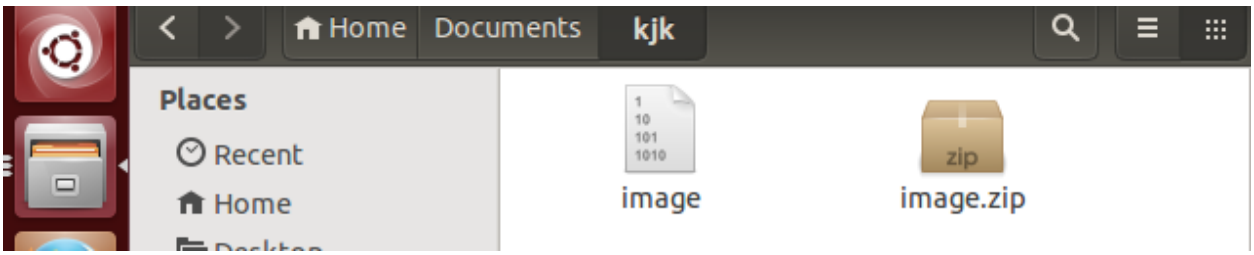
Langkah pertama yang perlu dilakukan adalah dengan mengakses alamat old.honeynet.org/scans/scan24. Dalam situs itu, terdapat file image.zip dengan ukuran 1,5 MB, download file tersebut, lalu ekstrak. Di sini saya memindahkan file image.zip dan file yang telah diekstraknya kedalam folder kjk dalam Documents. Dari terminal, masuk ke direktori kjk, untuk melihat jenis file image tersebut dengan memasukkan merintah *file image.* Dari perintah tersebut akan menampilkan jenis file image tersebut, yaitu image: DOS floppy 1440k, x86 hard disk boot sector. Langka selanjutnya adalah membuat direktori baru di /tmp/ dengan nama kasus.narkoba, lalu mount file image tadi ke direktori kasus.narkoba. ketika masuk ke direktori tersebut, akan terdapat 2 buah file, yaitu cover page.jpgc dan dan SCHEDU~1.exe



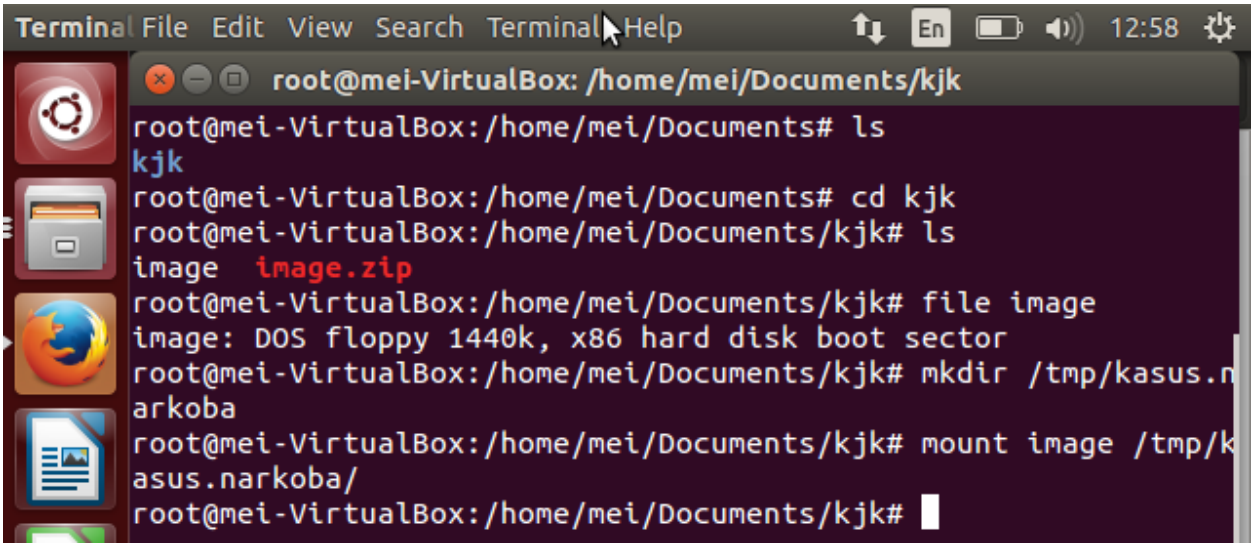
Gambar 1. Tampilan old.honeynet.org/scans/scan24



Gambar 2. Hasil ekstrak file image.zip

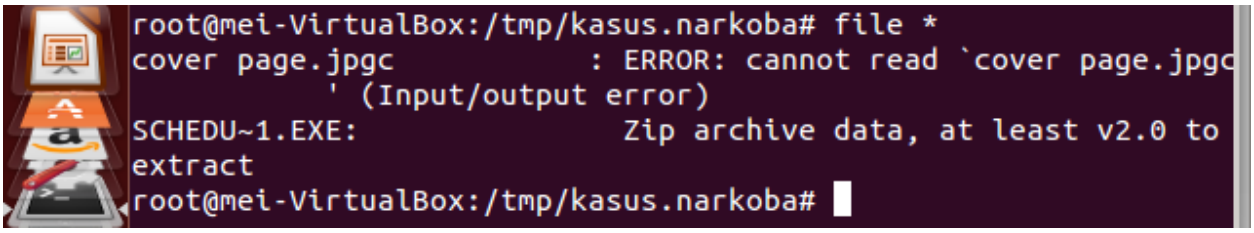


Gambar 3. File image.zip dan hasil ekstraknya diletakkan pada folder kjk



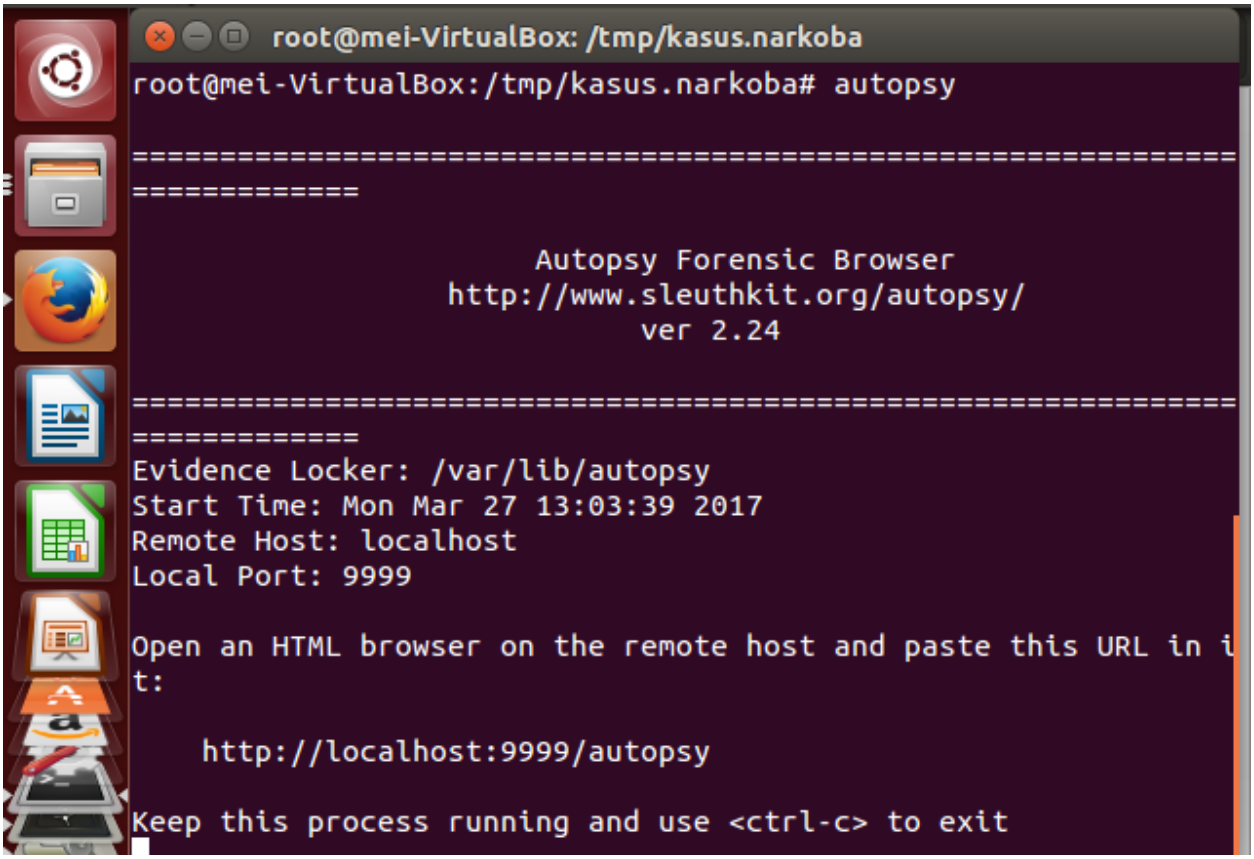
Gambar 4. Melihat jenis file image, membuat direktorikasus.narkoba, da melakukan mount file image ke kasus.narkoba

Gambar 5. File dalam kasus.narkoba



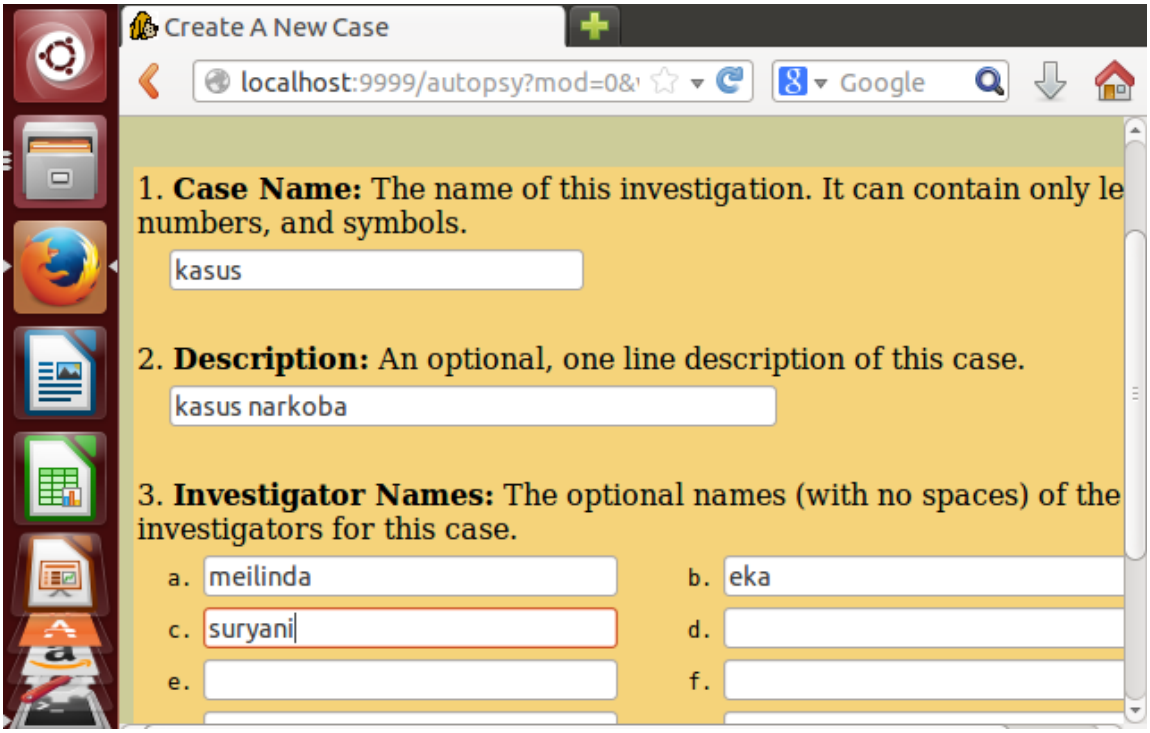
Gambar 6. Melihat semua file yang ada pada direktori kasus.narkoba

Selanjutnya jalankan autopsy pada terminal, maka akan menapilkan hasil seperti Gambar 7, di sana terdapat alamat http://localhost:9999/autopsy. Akses alamat tersebut ke browser, maka akan menampilkan hasil seperti pada Gambar 8. Lalu pilih New Case. Masukkan kasus pada name case, kasus narkoba pada description, dan masukkan nama investigator, dalam hal ini saya memasukkan nama a.)Meilinda b.)Eka dan c.)Suryani seperti pada Gambar 9 lalu klik add. Selanjutnya akan tampil seperti pada Gambar 10, pilih add host. Lalu pada tampilan seperti pada Gambar 11, kita diminta untuk memasukkan nama host, masukkan nama 'Joe_Jacob". Setelah proses add host selesai, masukkan file image yang tadi sudah didownload dan diekstrak, lalu add image seperti pada Gambar 13. Untuk langkah selanjutnya dapat dilihat pada gambar 14 sampai dengan gambar 16.



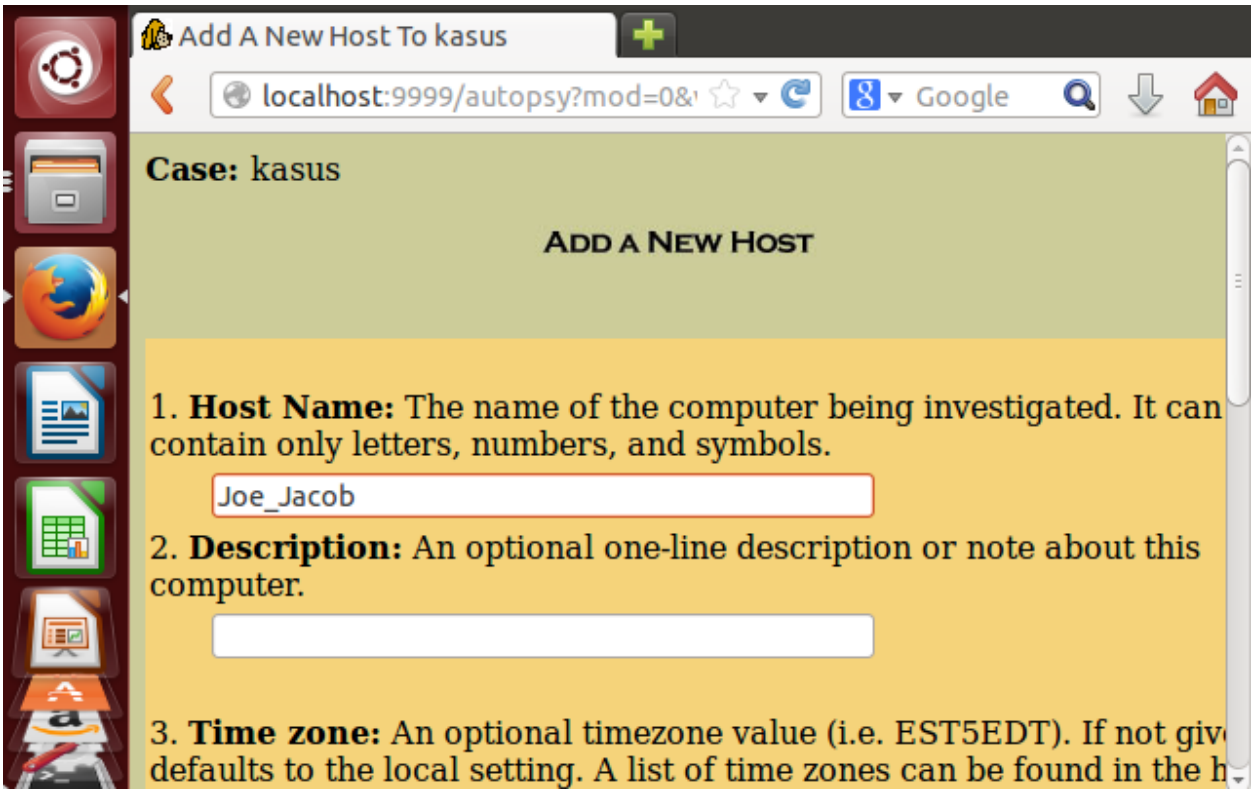
Gambar 7. Menjalankan autopsy

Gambar 8. Localhost:9999/autopsy



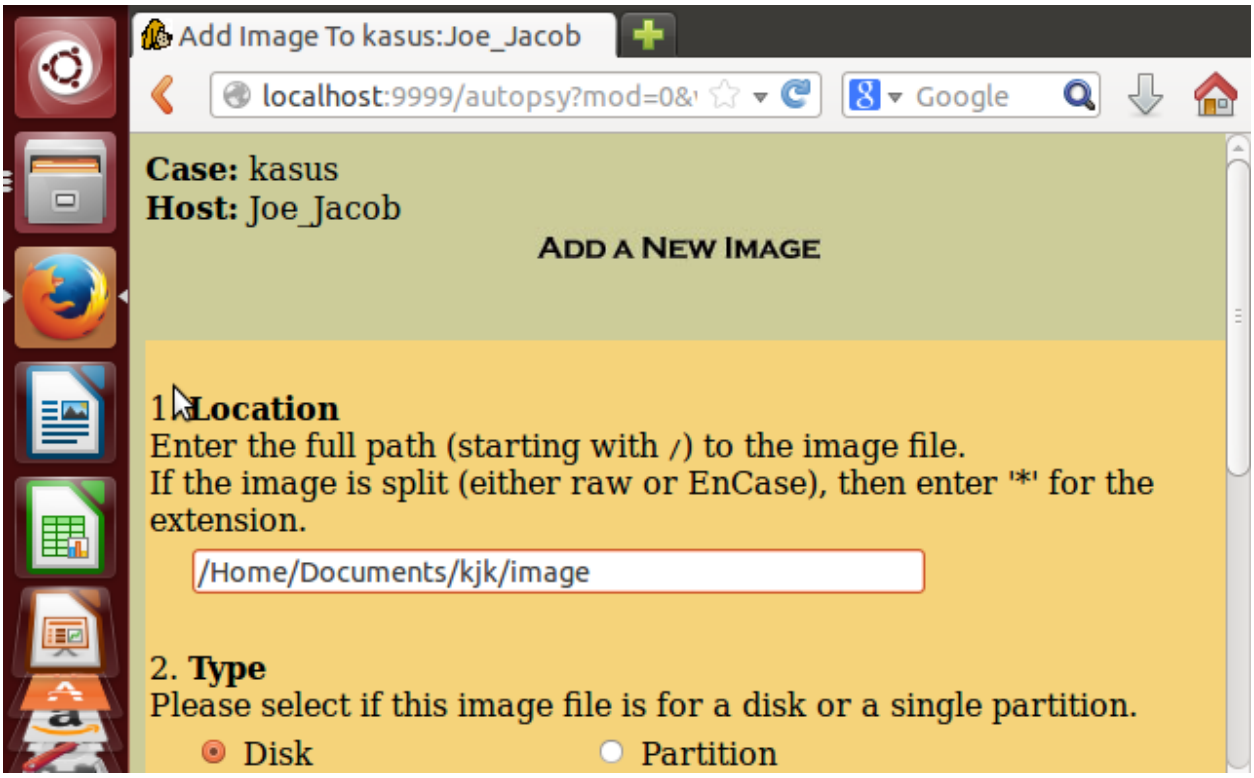
Gambar 9. Membuat kasus baru

Gambar 10. Membuat case: kasus

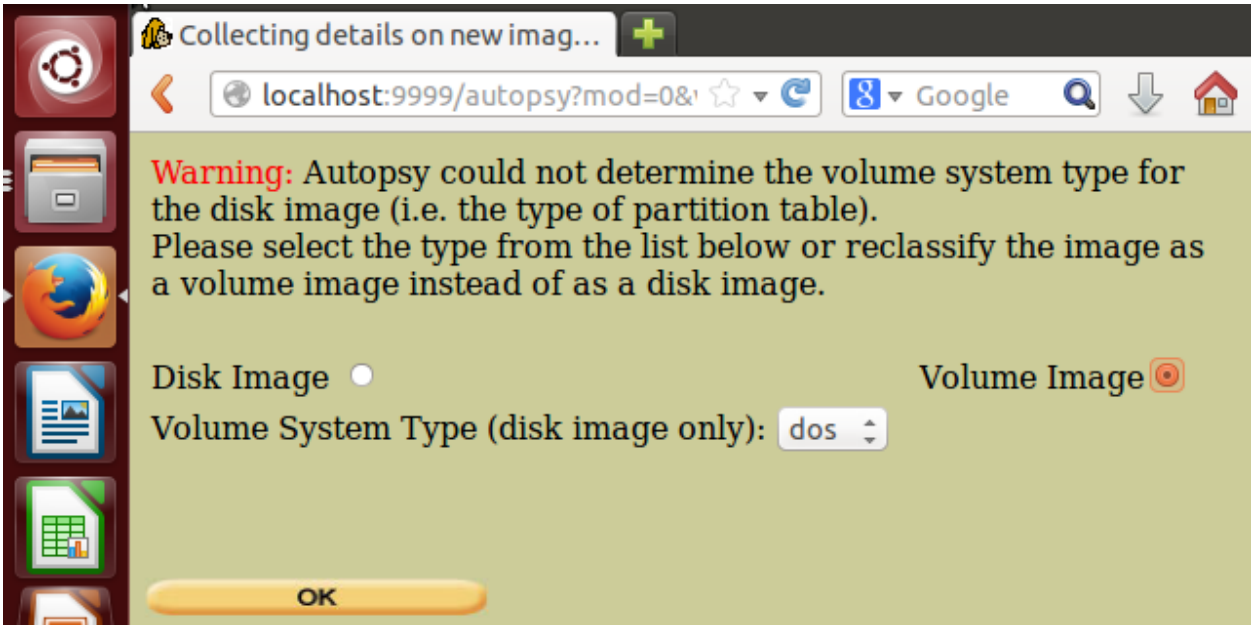


Gambar 11. Menambah host baru

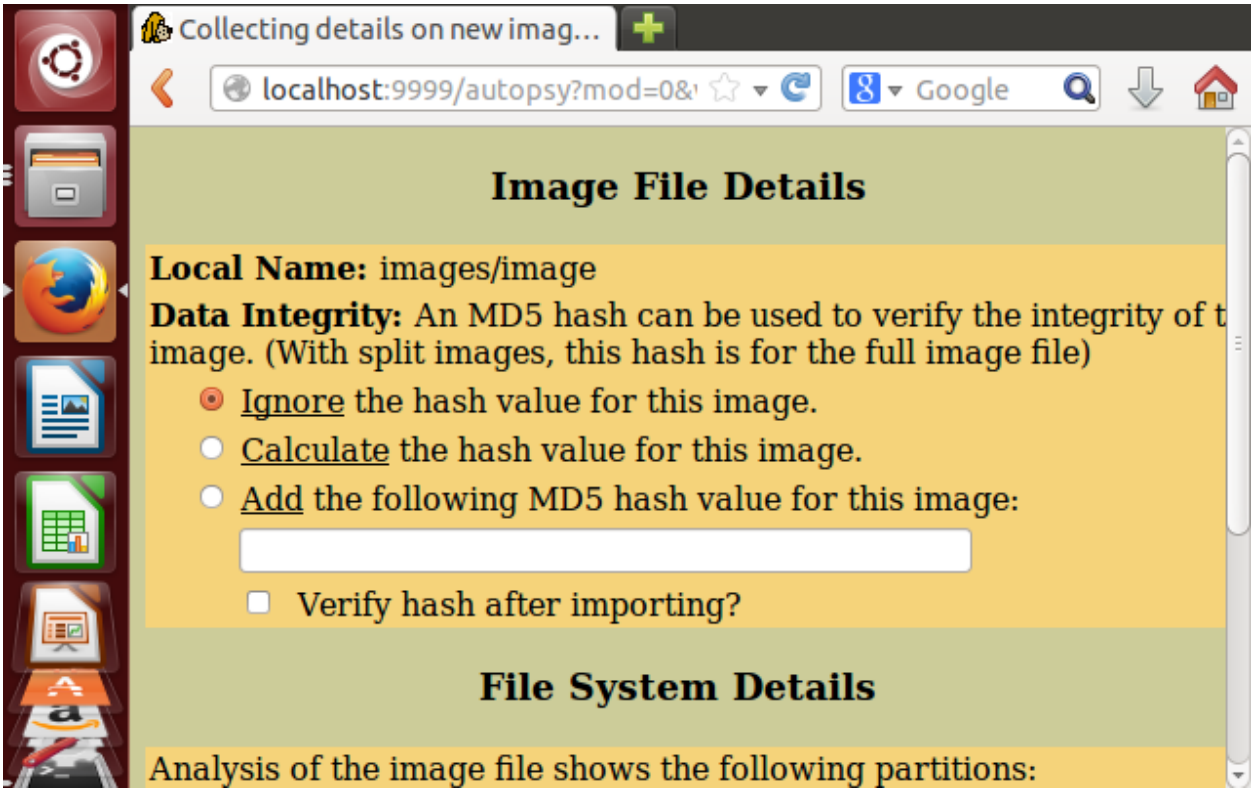
Gambar 12. Setelah host ditambahkan



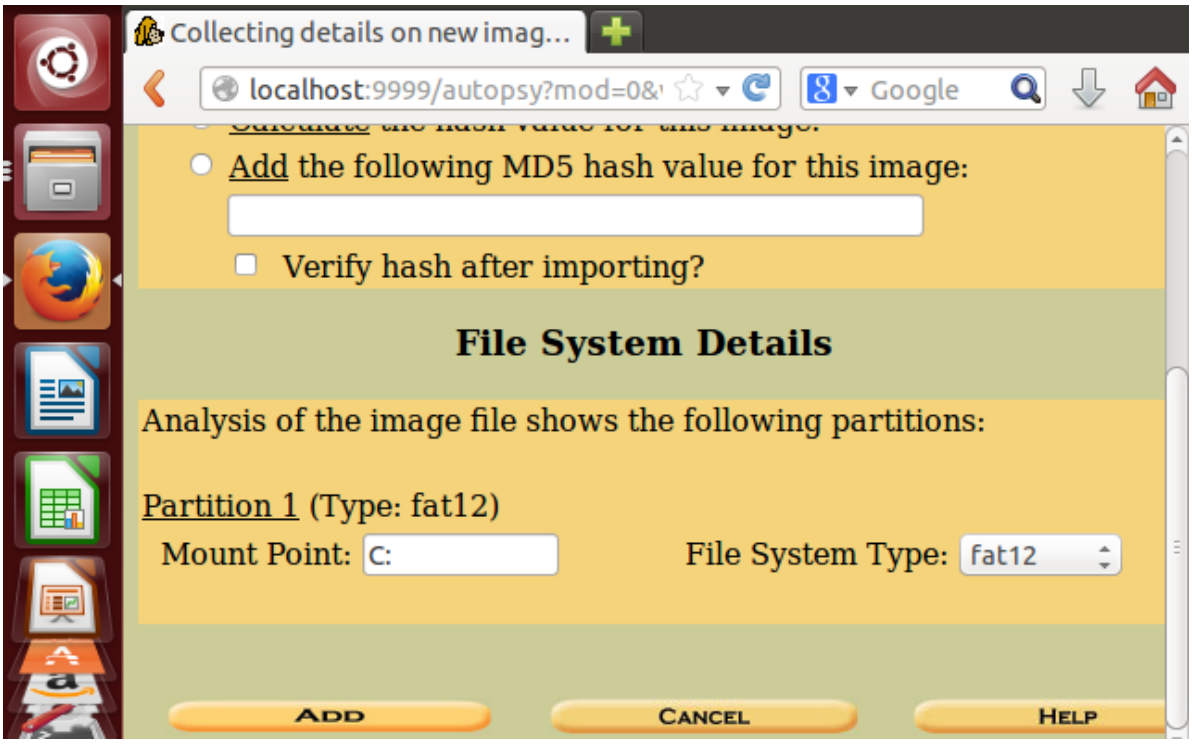
Gambar 13. Memasukkan gambar



Gambar 14. Mengklasifi volume imange

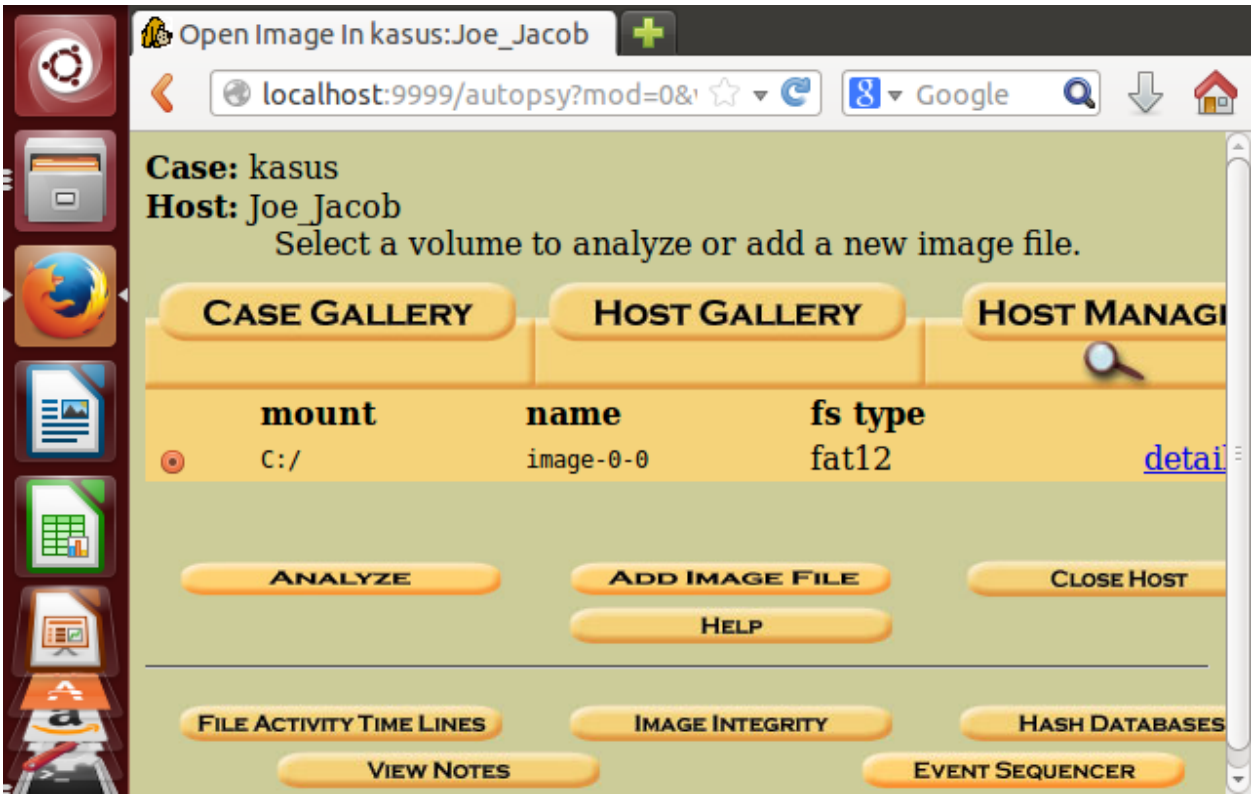


Gambar 15. Image file details

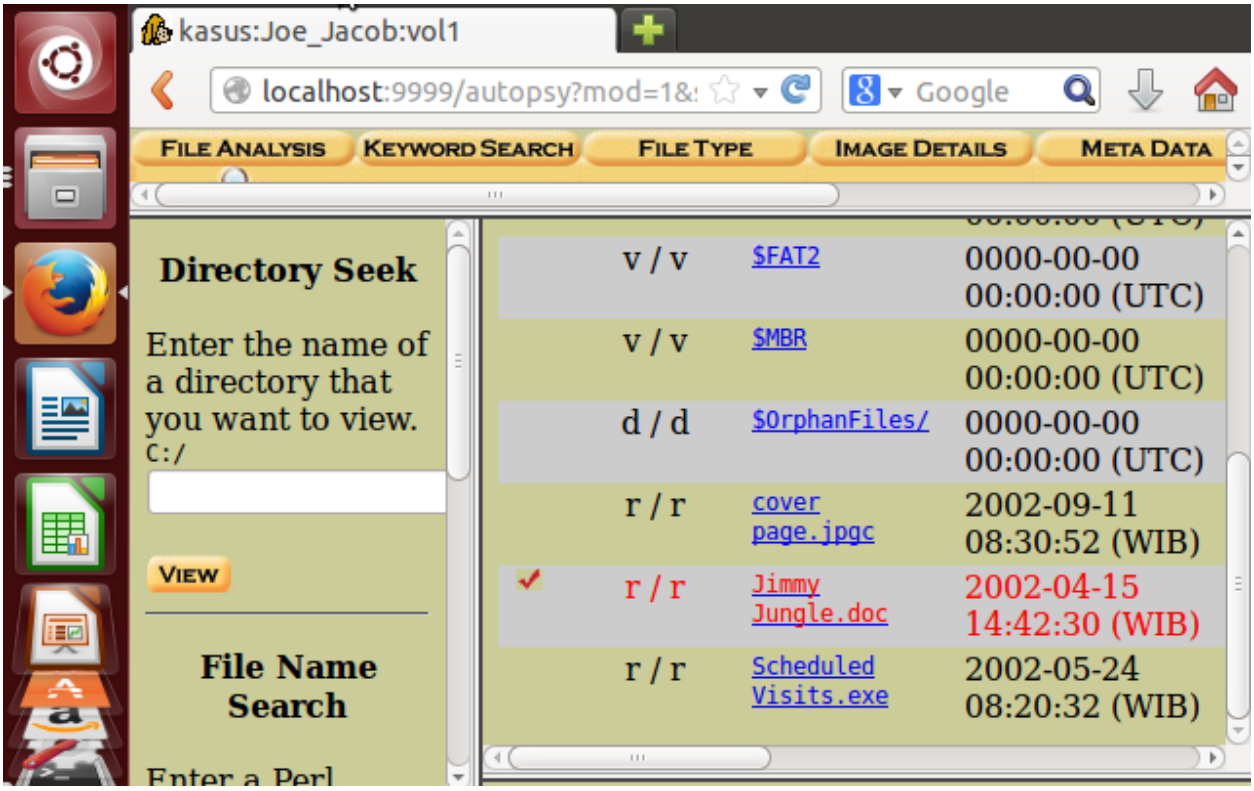


Gambar 16. File system details

Berikut merupakan tampilan kasus yang telah dibuat pada http://localhost:9999/autopsy. Klik analyze untuk melihat analisa kasus, seperti pada gambar 18.

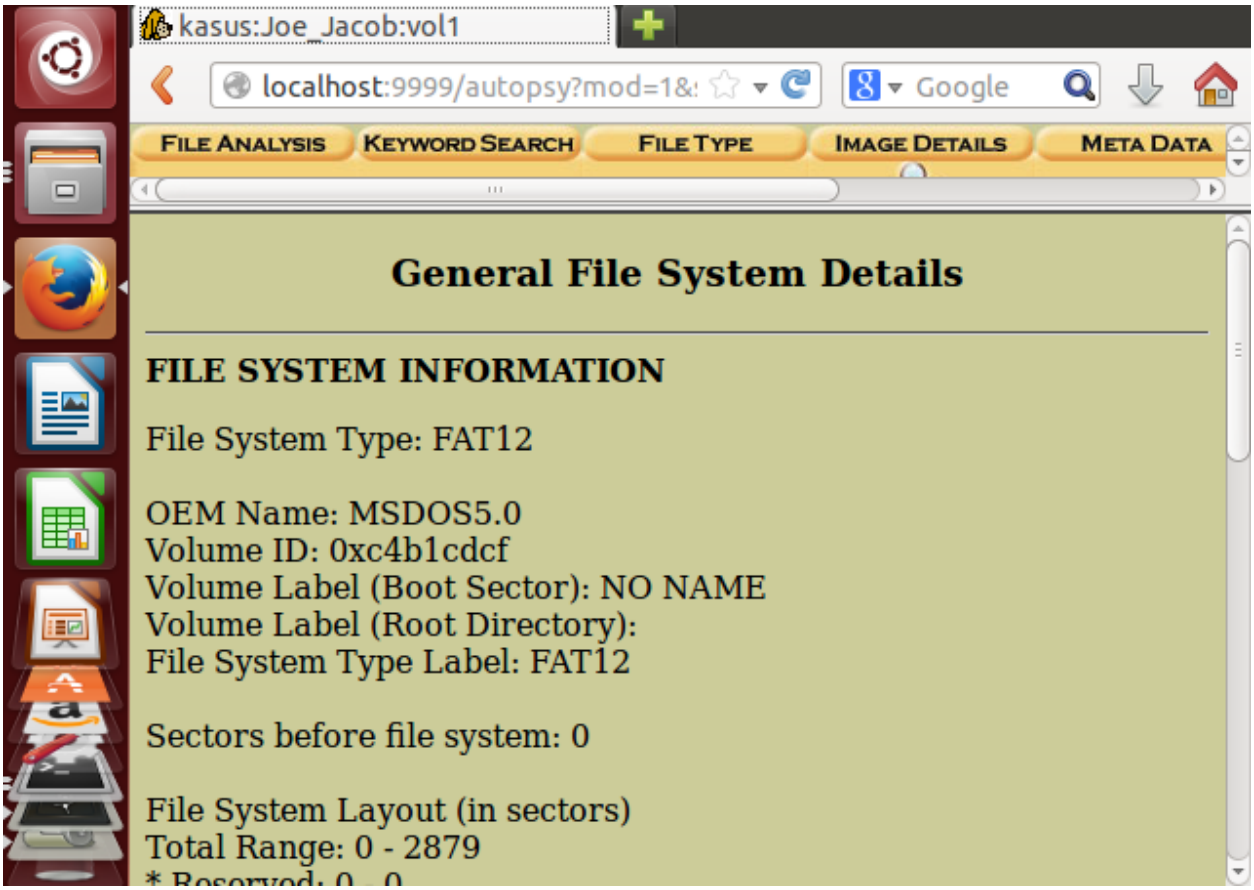


Gambar 17. Tampilan kasus yang telah ditambahkan

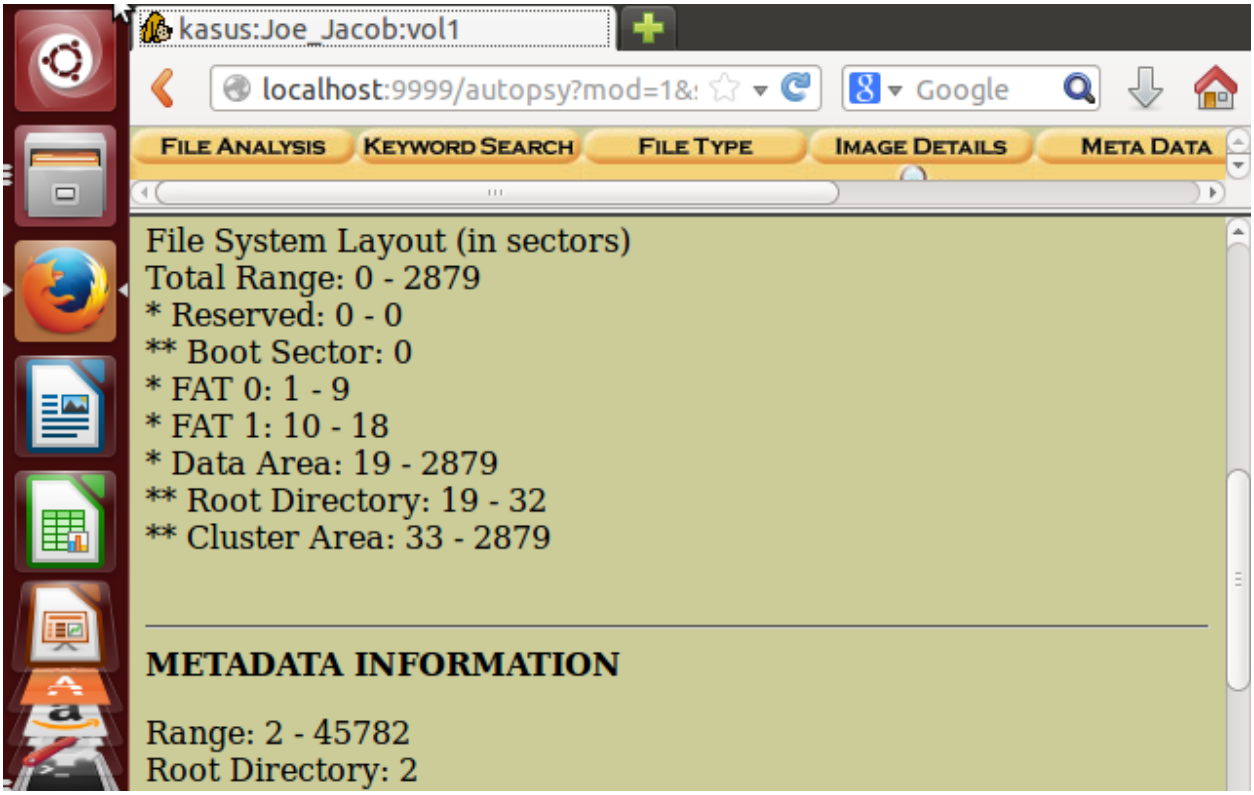


Gambar 18. Analyze kasus

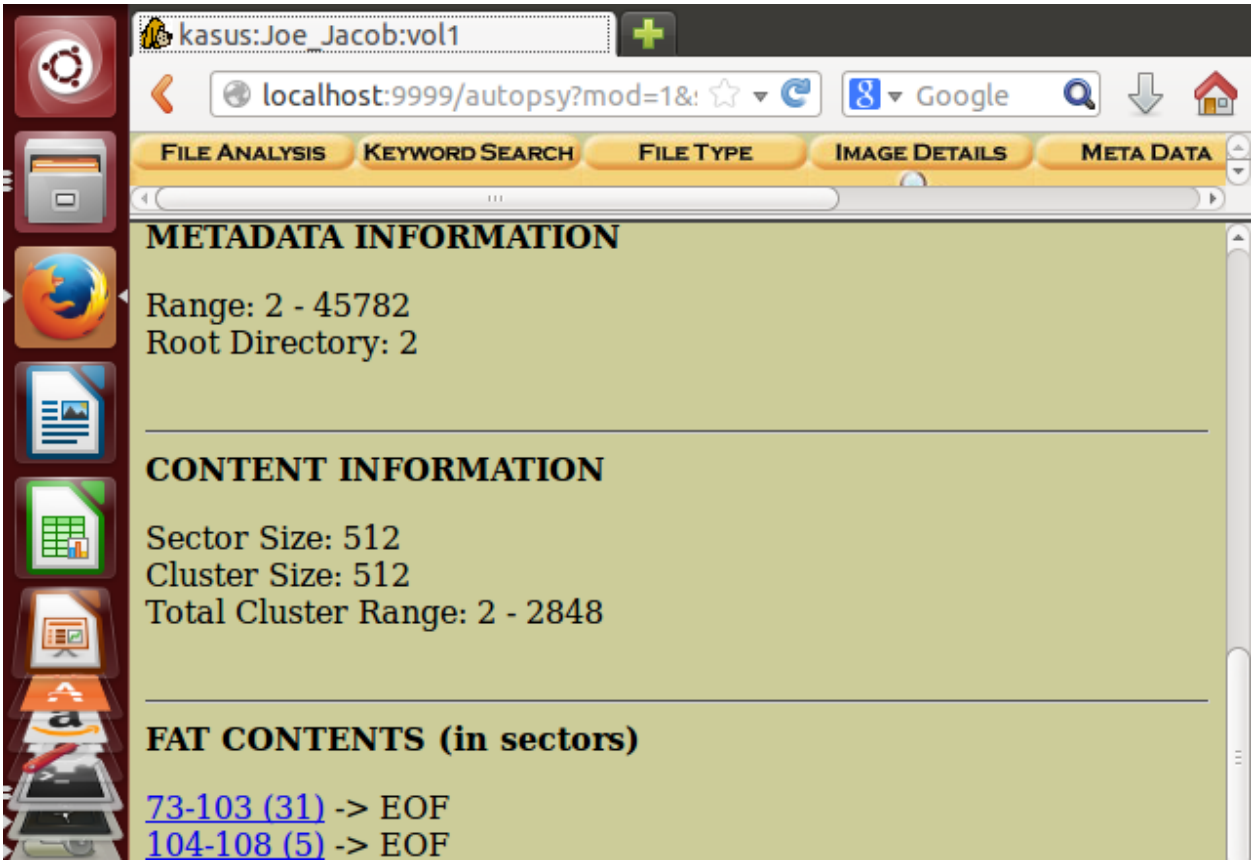
Pilih metada untuk mengetahui general file system details seperti pada gambar 19 sampai gambar 21.



Gambar 19. File system information

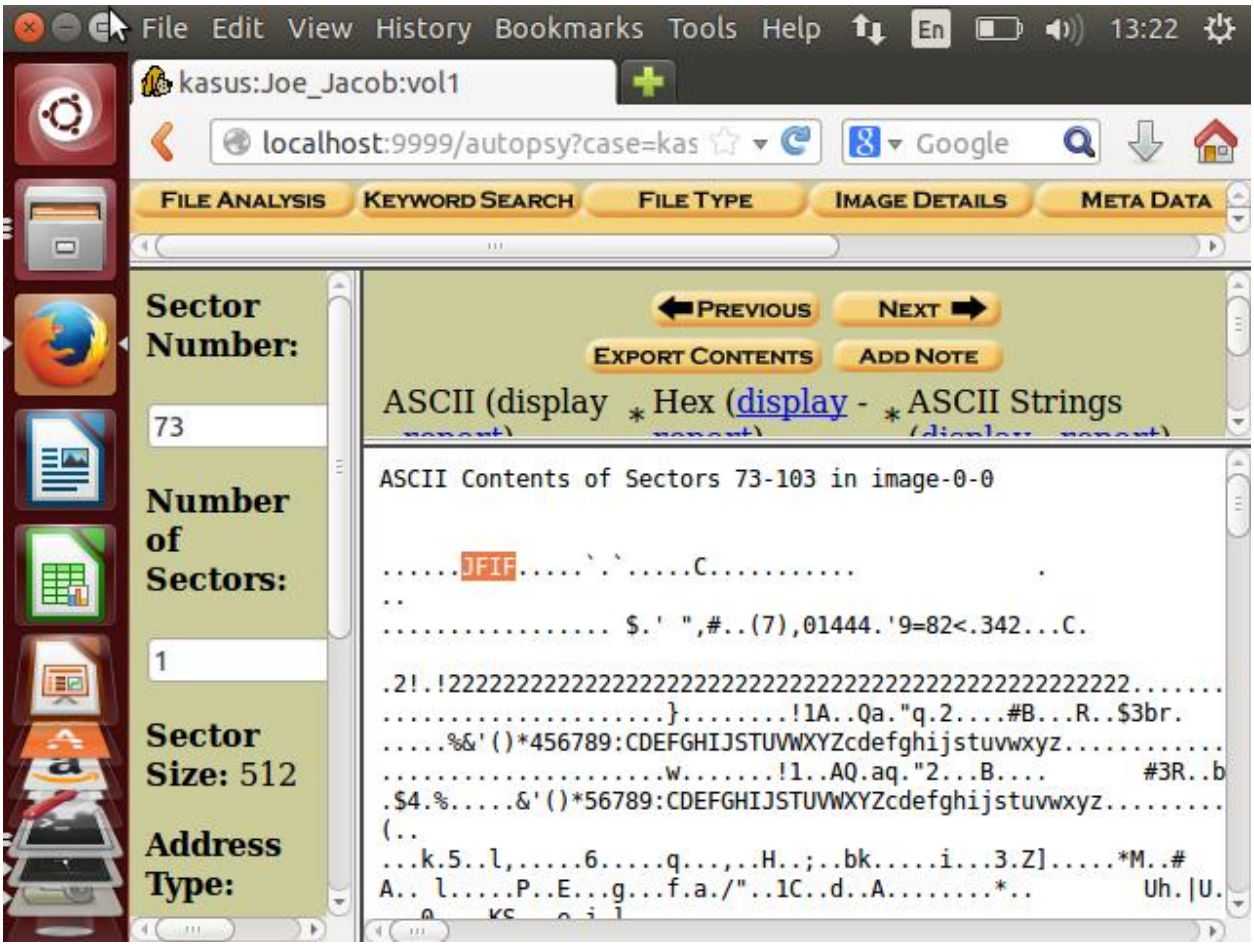


Gambar 20. Metadata information

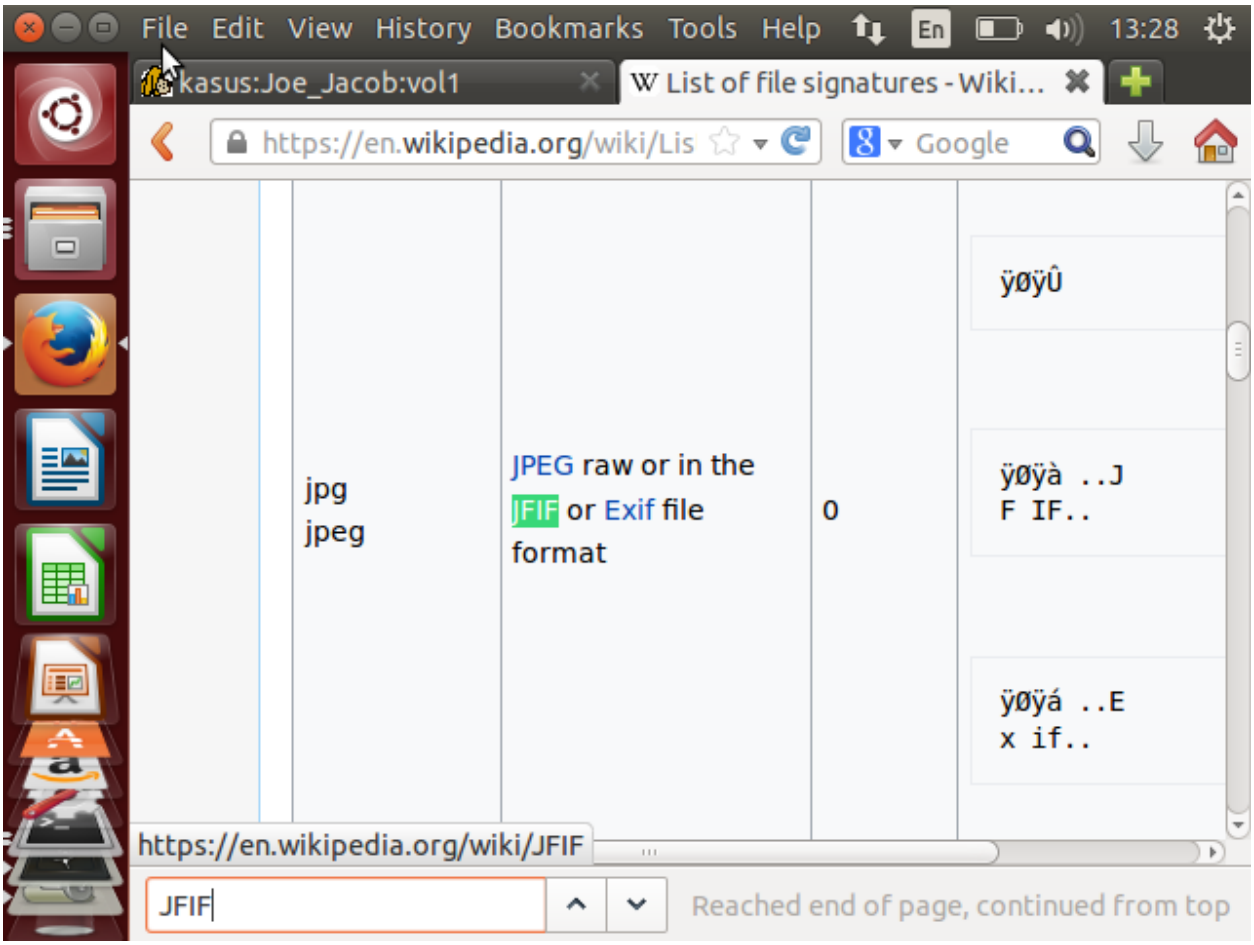


Gambar 21. Content information dan FAT contents

Pada FAT CONTETNS di gambar 21 terdapat 73-103 (31) dan 104-108 (5). Pertama kita pilih 73-103 (31). Maka akan tampil hasil seperti pada gambar 22. Di sana terlihat headernya adalah JFIF. Setelah mendapatkan header, kita periksa jenis extensi dari header tersebut pada list of signature seperti pada gambar 23..

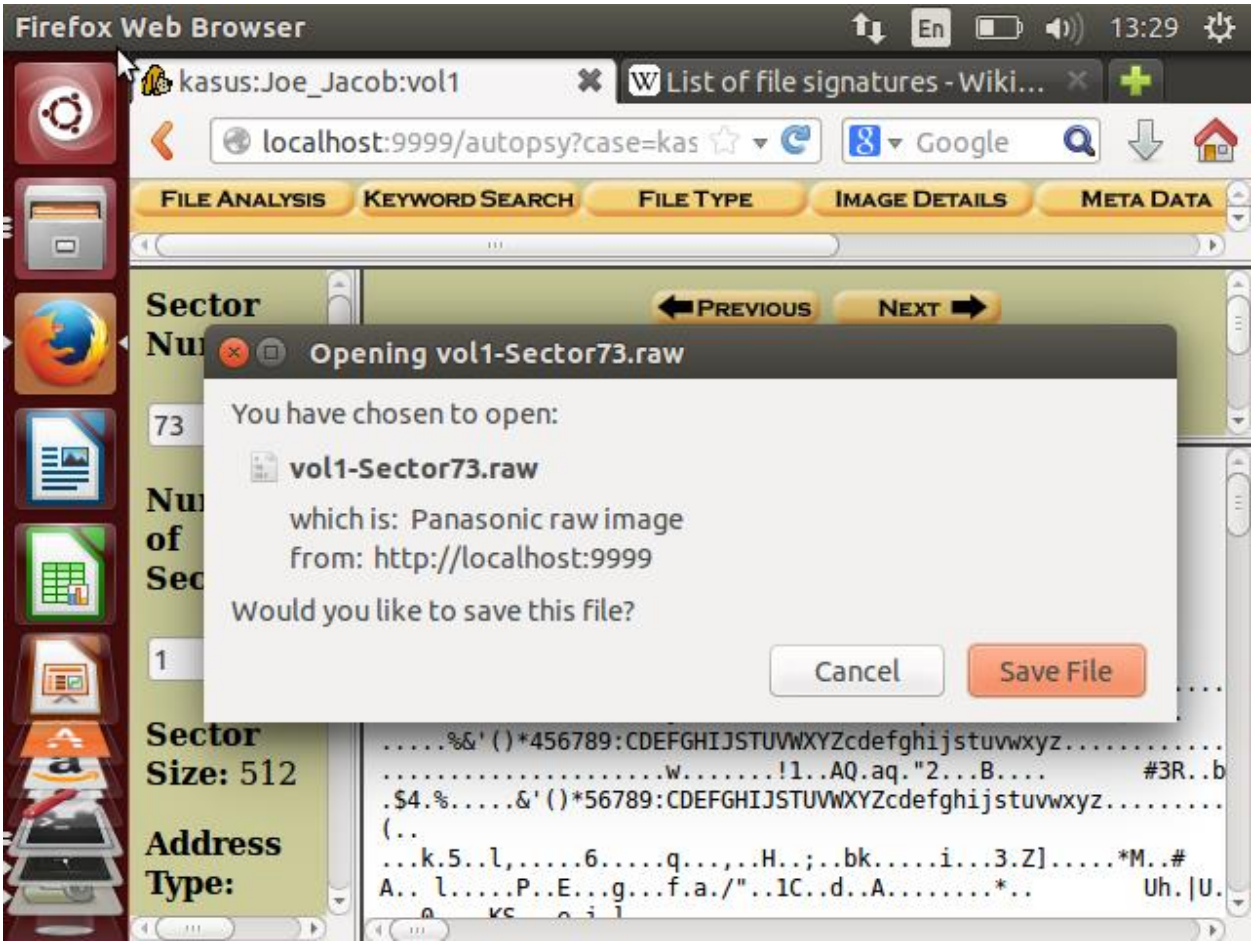


Gambar 22. 73-103 (31)

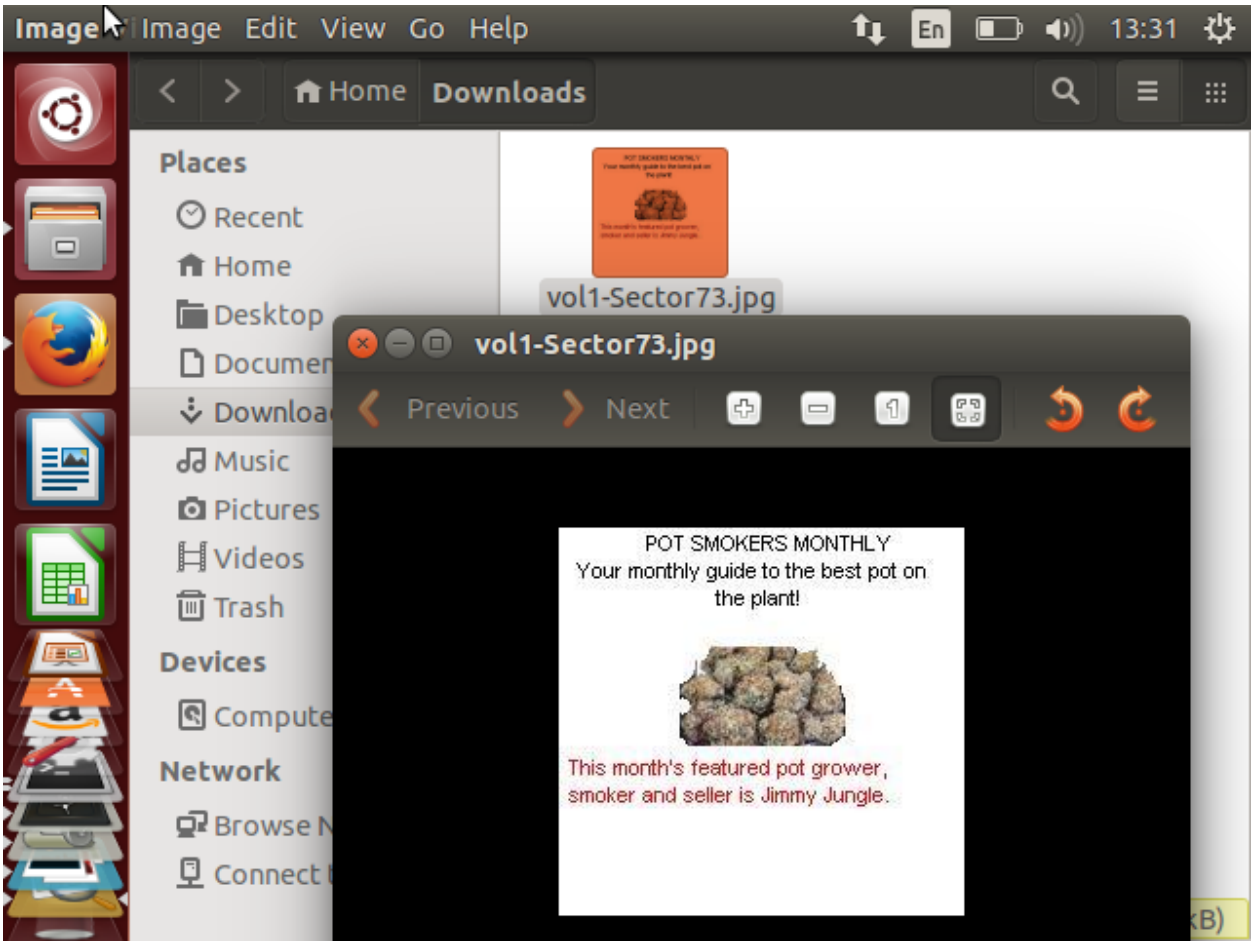


Gambar 23. List of signature

Setelah mendapat extensi dari header, kembali lagi ke localhost:9999/autopsy, lalu klik export contets, lalu save file seperti yang ditampilkan pada gambar 24. Hasilnya berupa file raw, karena extensi dari JFIF merupakan jpg, maka, ganti extensi raw tersebut menjadi jpg. Lalu buka file tersebut, maka akan menampilkan gambar seperti pada gambar 25.

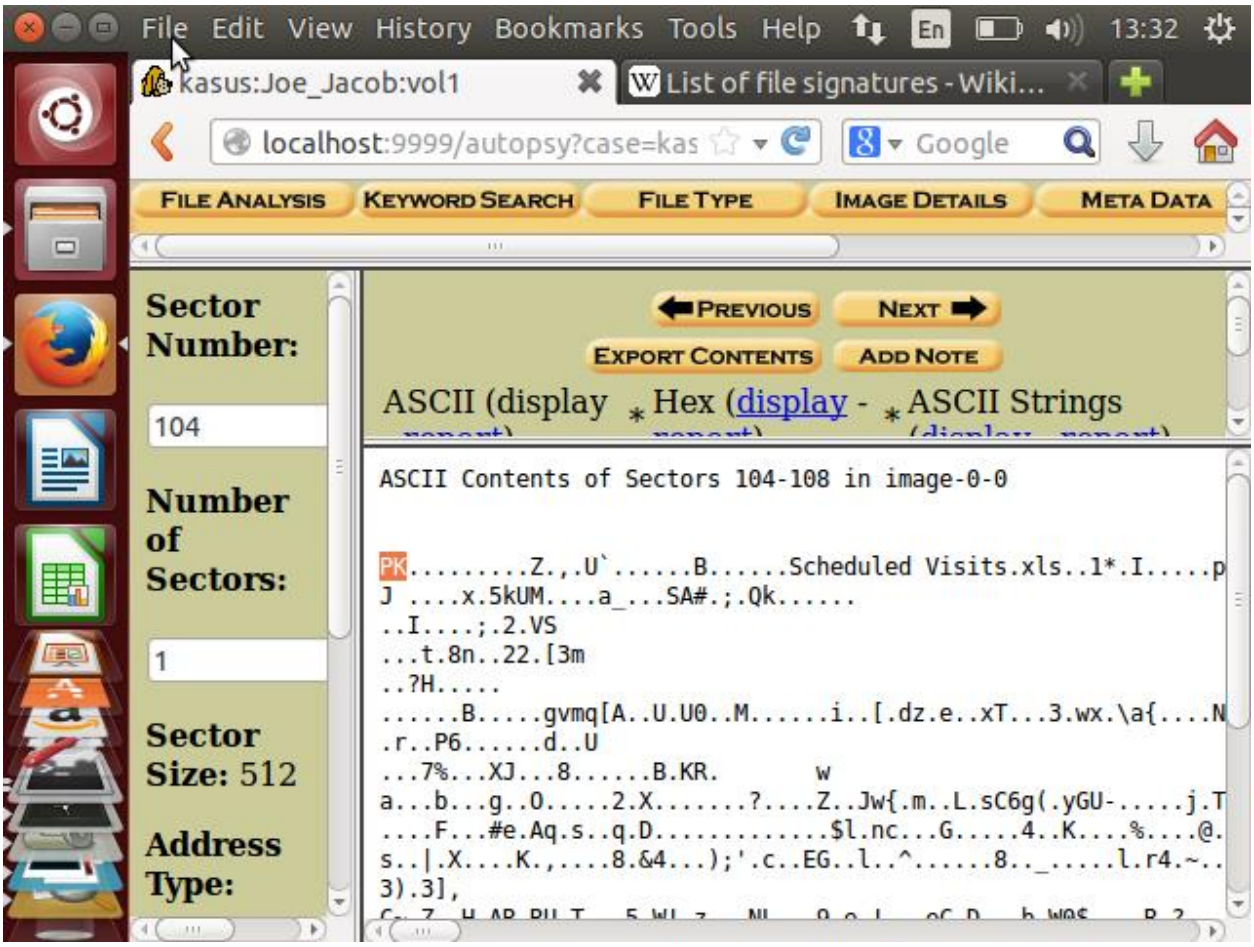


Gambar 24. Export file



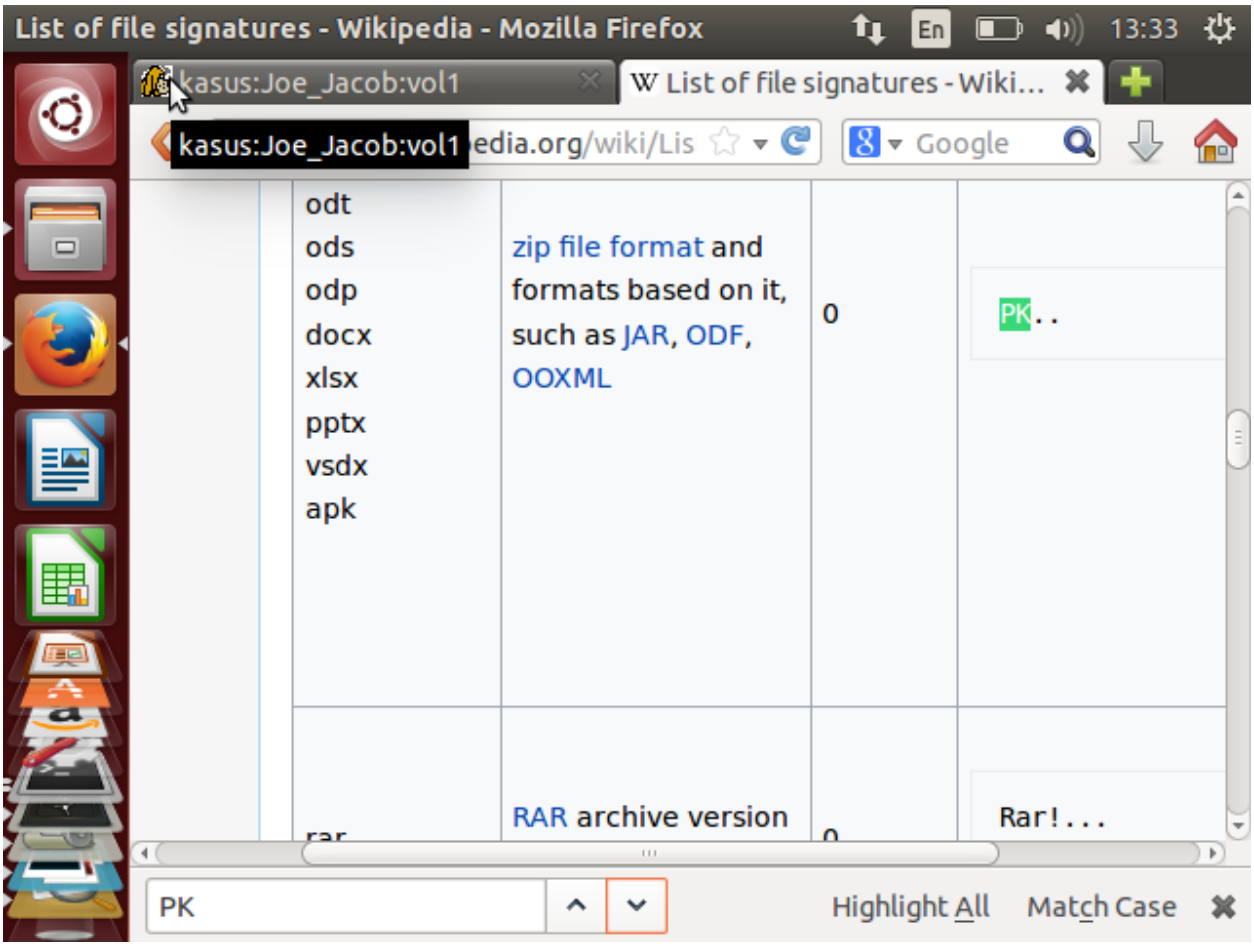
Gamabr 25.tampilan file jpg

Selanjutnya kembali ke FAT CONTENTS dan klik pada 104-108(5) maka akan menampilkan hasil seperti pada gambar 26 berikut. Dapat dilihat bahwa headernya adalah PK. Maka seperi yang telah dilakukan sebelumnya, kita akan mencari extensi dari header PK di list of signature, seperti pada gambar 27.

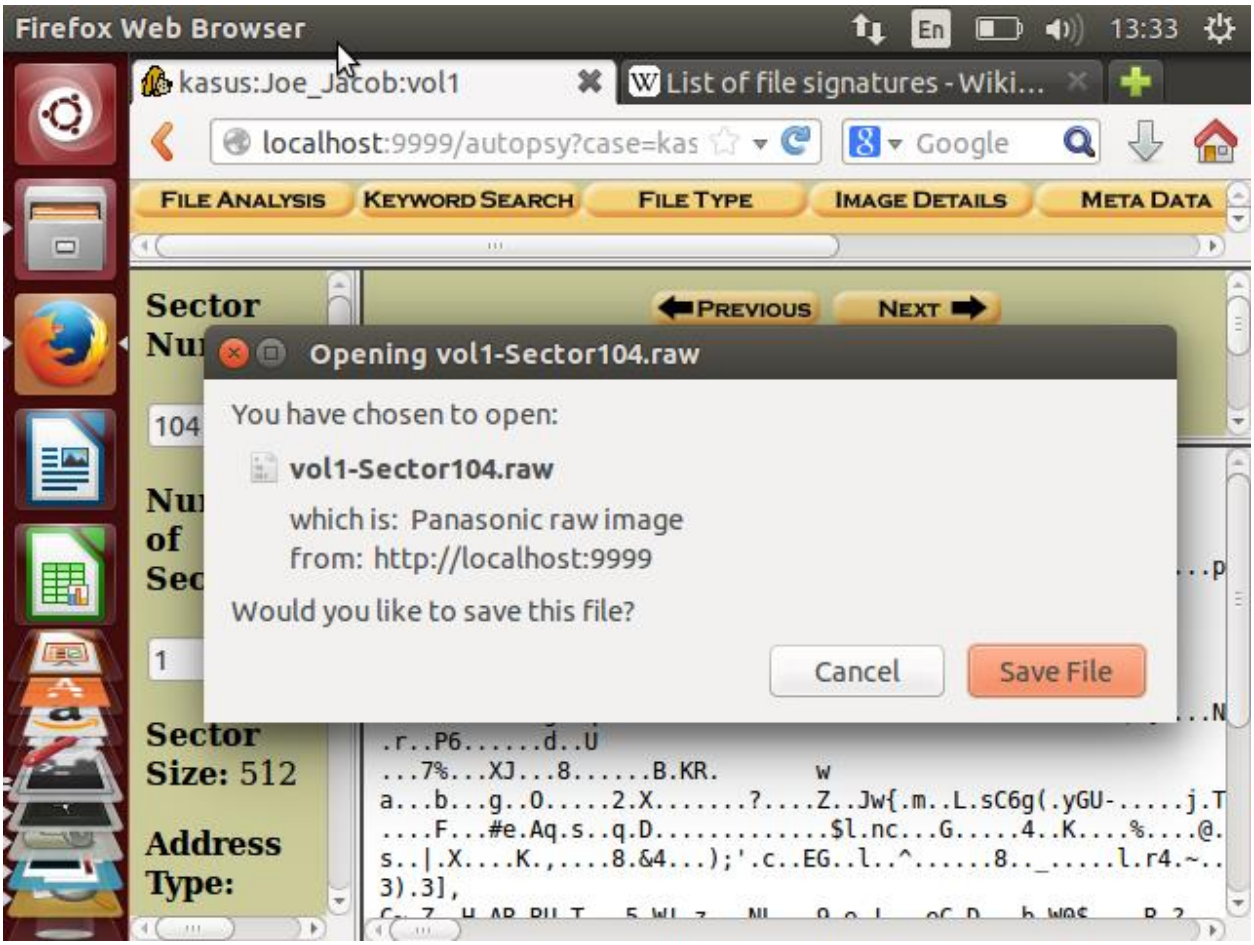


Gambar 26. 104-108(5)

Dari gambar 27 ini dapat diketahui bahwa PK memiliki existansi zip. Setelah mengetahui ini, kembali ke localhost:9999/autopsy, lalu pilih export contents, dan save. Sama seperti sebelumnya, content yang diexport berupa raw, maka ganti dulu menjadi zip.

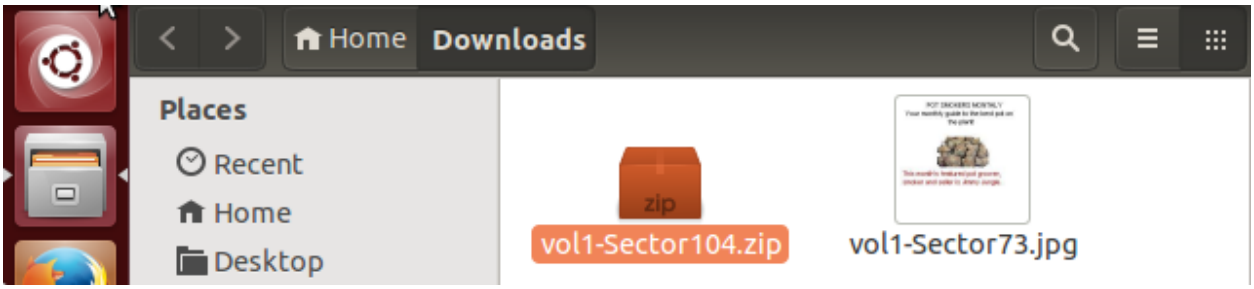


Gambar 27. List of signature PK



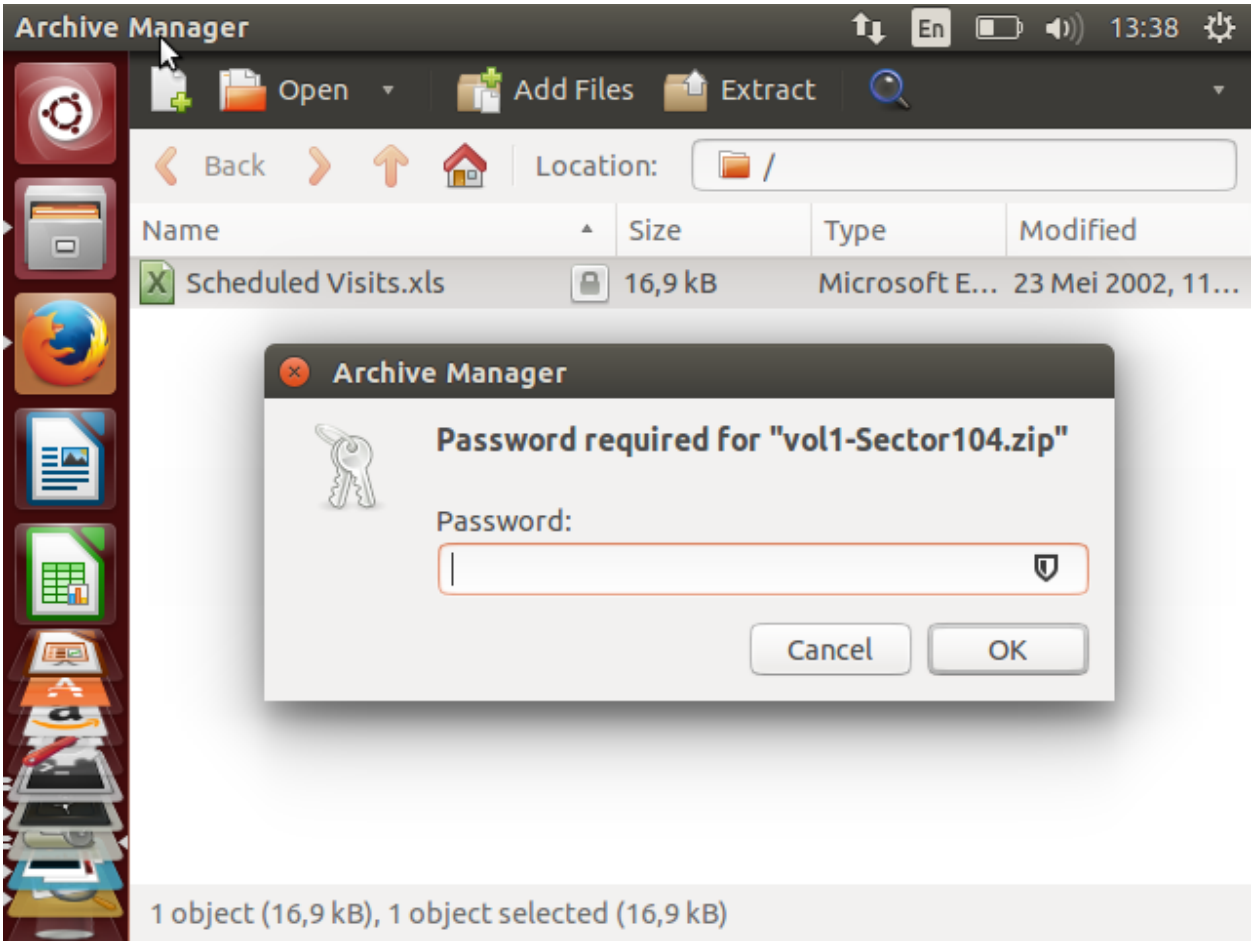
Gambar 28. Export content PK

Gambar 29. File raw PK



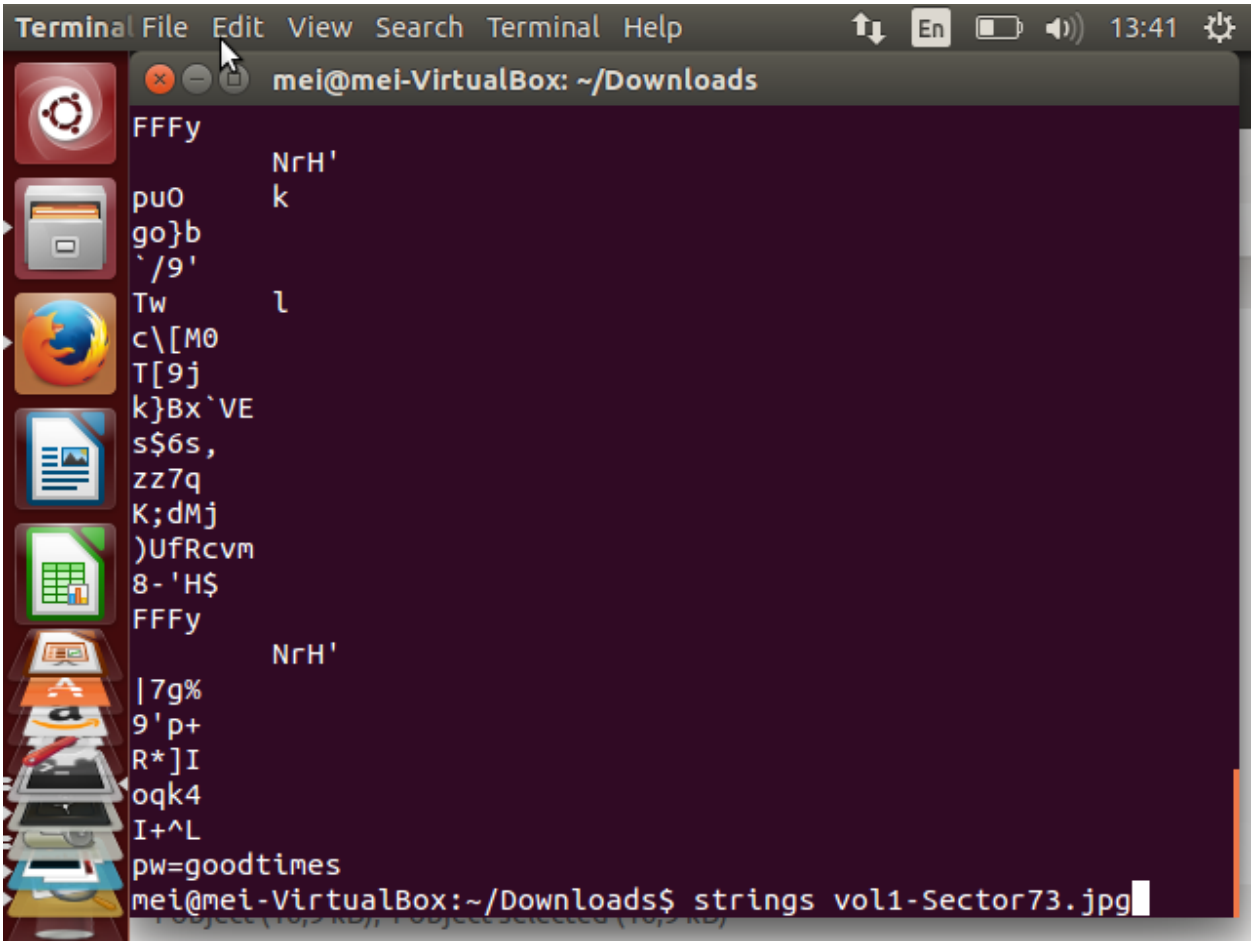
Gambar 30. File zip PK

Saat membuka file zip tersebut, terdapat sebuah file .xls, ketika dibuka, maka kita diminta untuk memasukkan password, seperti yang terlihat pada gambar 31.



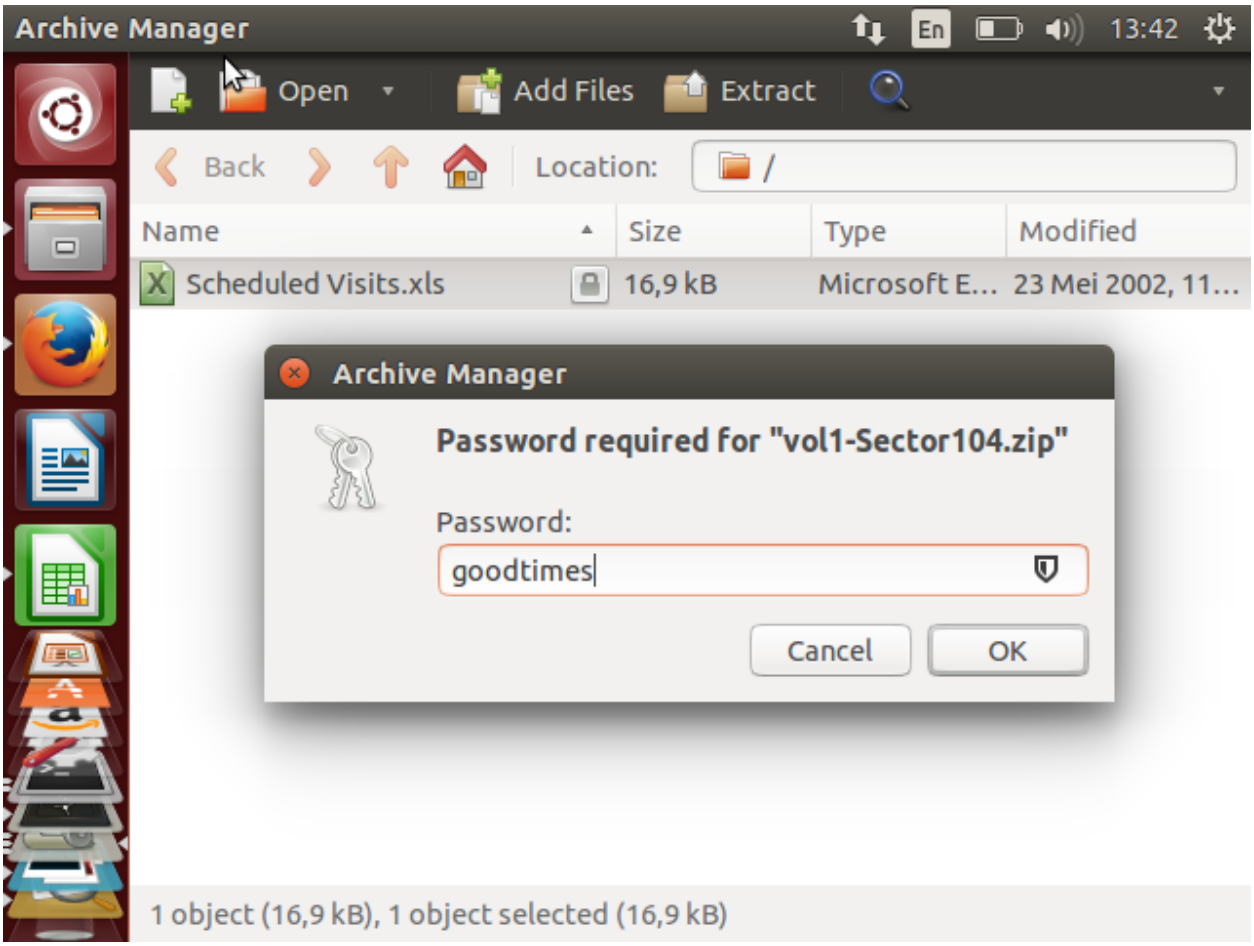
Gambar 31. Isi file zip PK

Untuk mengetahui password yang digunakan untuk membuka file xls tersebut ialah dengan memasukkan perintah strings vol1-sector73.jpg dalam direktori yang memuat file tersebut. Strings digunakan untuk mengetahui karakter yang dapat dibaca pada suatu file. Maka akan menampilkan hasil seperti pada gambar 32 berikut. Di dini, diketahui bahwa passwordnya adalah goodtimes.

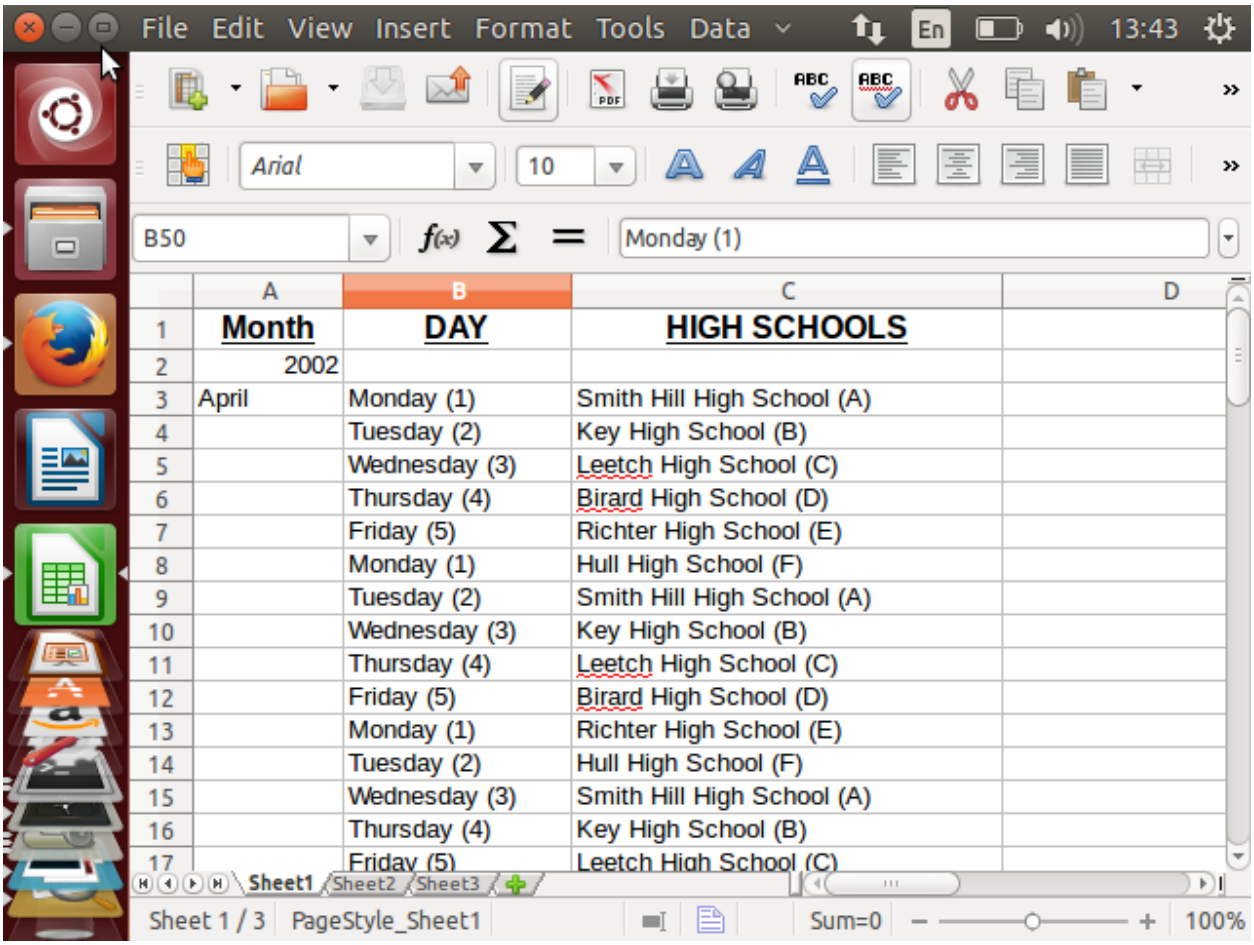


Gambar 32. Mencari password dengan strings

Setelah menemukan password, masukkan password tersebut pada file yang ingin dibuka tadi, seperti pada gambar 33. Maka terbukalah file tersebut yang memuat nama-nama sekolah serta hari dan tanggal si pengedar beroperasi, seperti yang terlihat pada gambar 34.



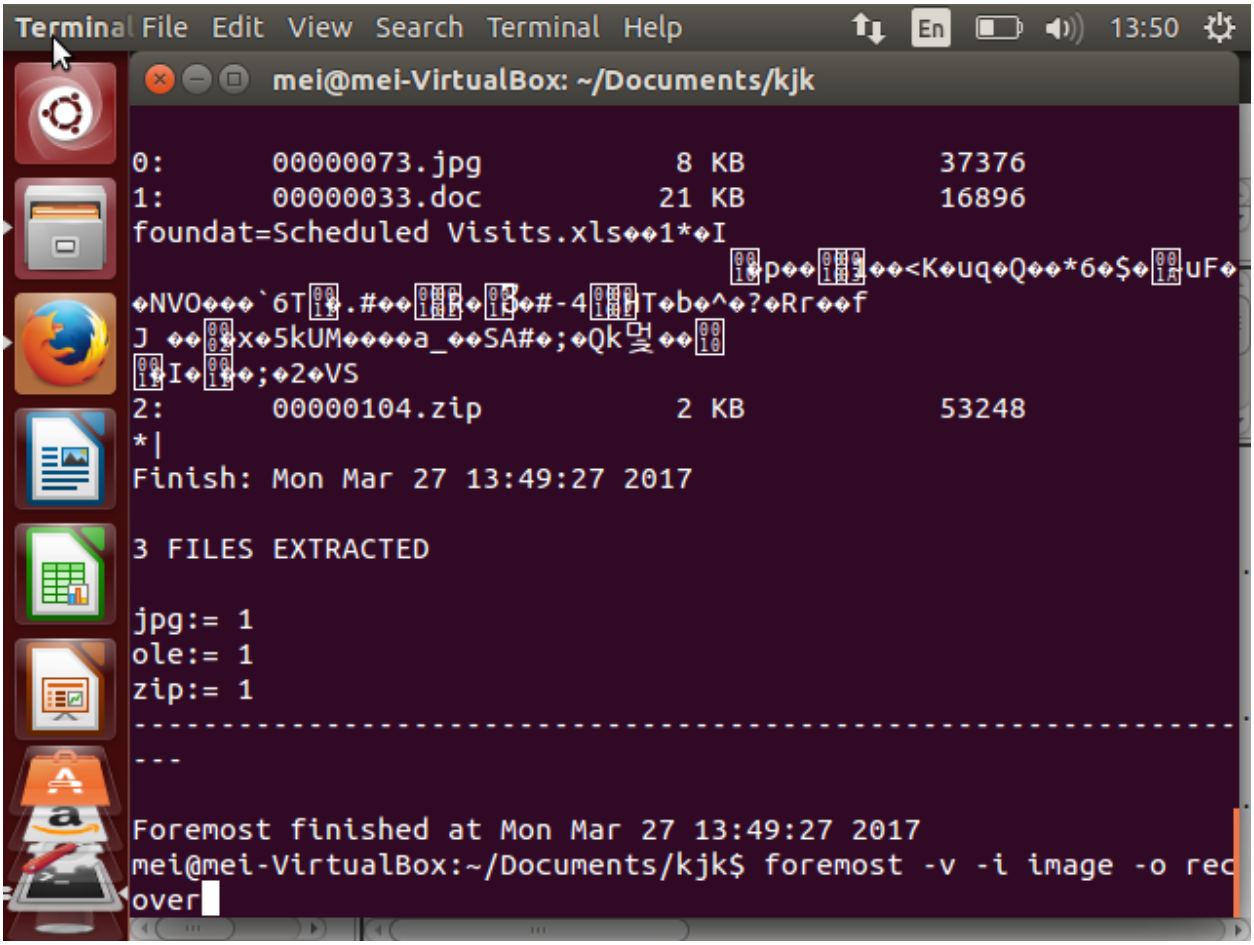
Gambar 33. Memasukkan password



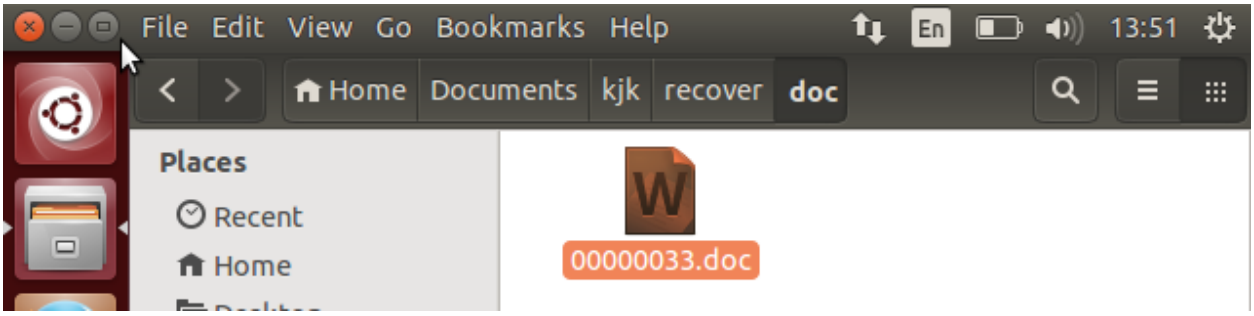
	A	B	C	D
1	**Month**	**DAY**	**HIGH SCHOOLS**	
2	2002			
3	April	Monday (1)	Smith Hill High School (A)	
4		Tuesday (2)	Key High School (B)	
5		Wednesday (3)	Leetch High School (C)	
6		Thursday (4)	Birard High School (D)	
7		Friday (5)	Richter High School (E)	
8		Monday (1)	Hull High School (F)	
9		Tuesday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

Gambar 34. Isi fil .xls

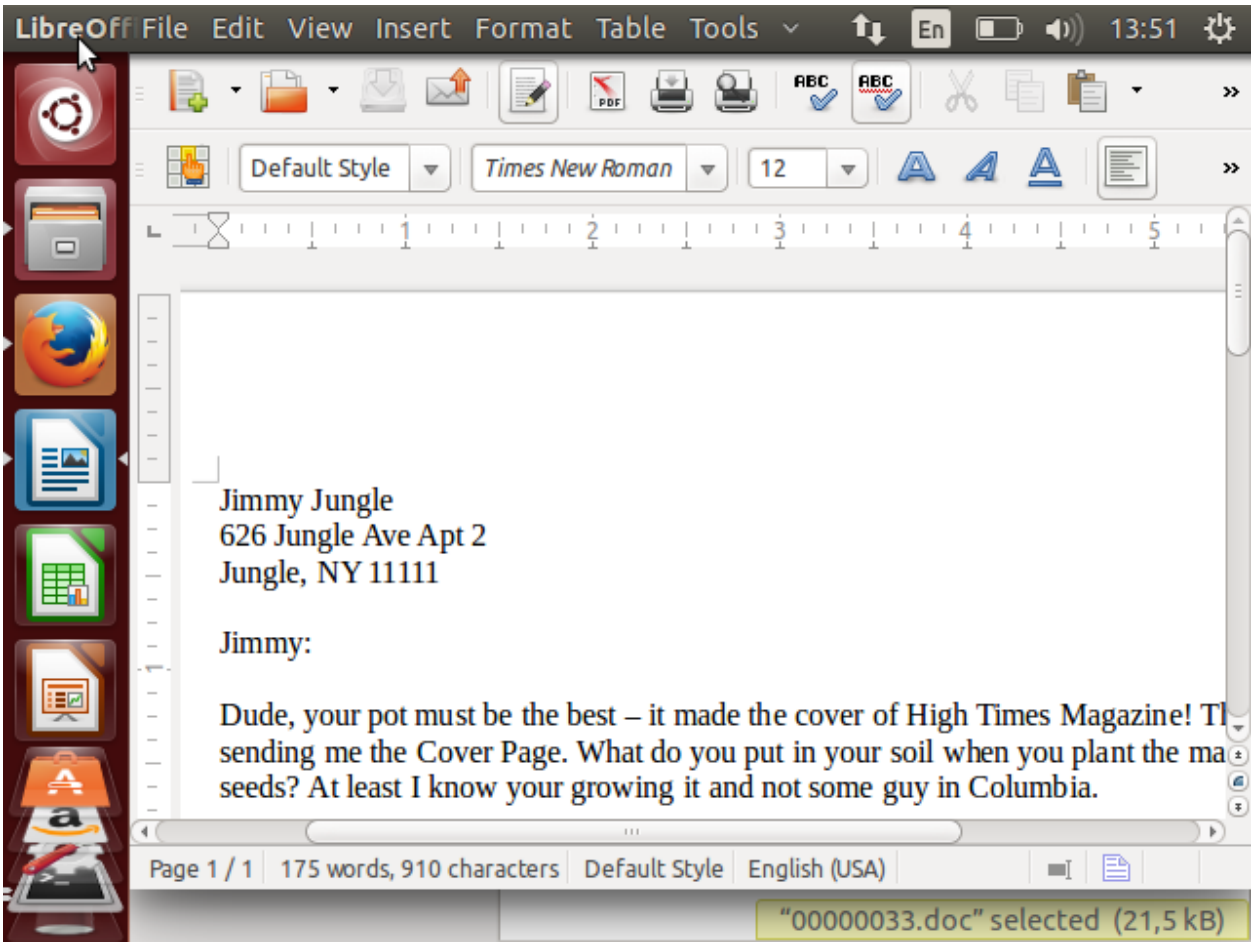
Untuk menngetahui data yang tersembunyi pada image, masukkan perintah firemost –v –I image –o recover, maka aka menghasilkan seperti pada gambar 35 berikut. Maka akan menghasilkan file seperti pada gambar 36. Kitika dibuka, file itu tenyata adalah sebuah surat yang ditulis oleh Joe, untuk Jimmy Jungle seperti yang terlihat pada gambar 37 dan gambar 38. Dari surant itu dapat disimpulkan bahwa Joe adalah seorang pengedar narkoba dan Jimmy adalah suppliernya.



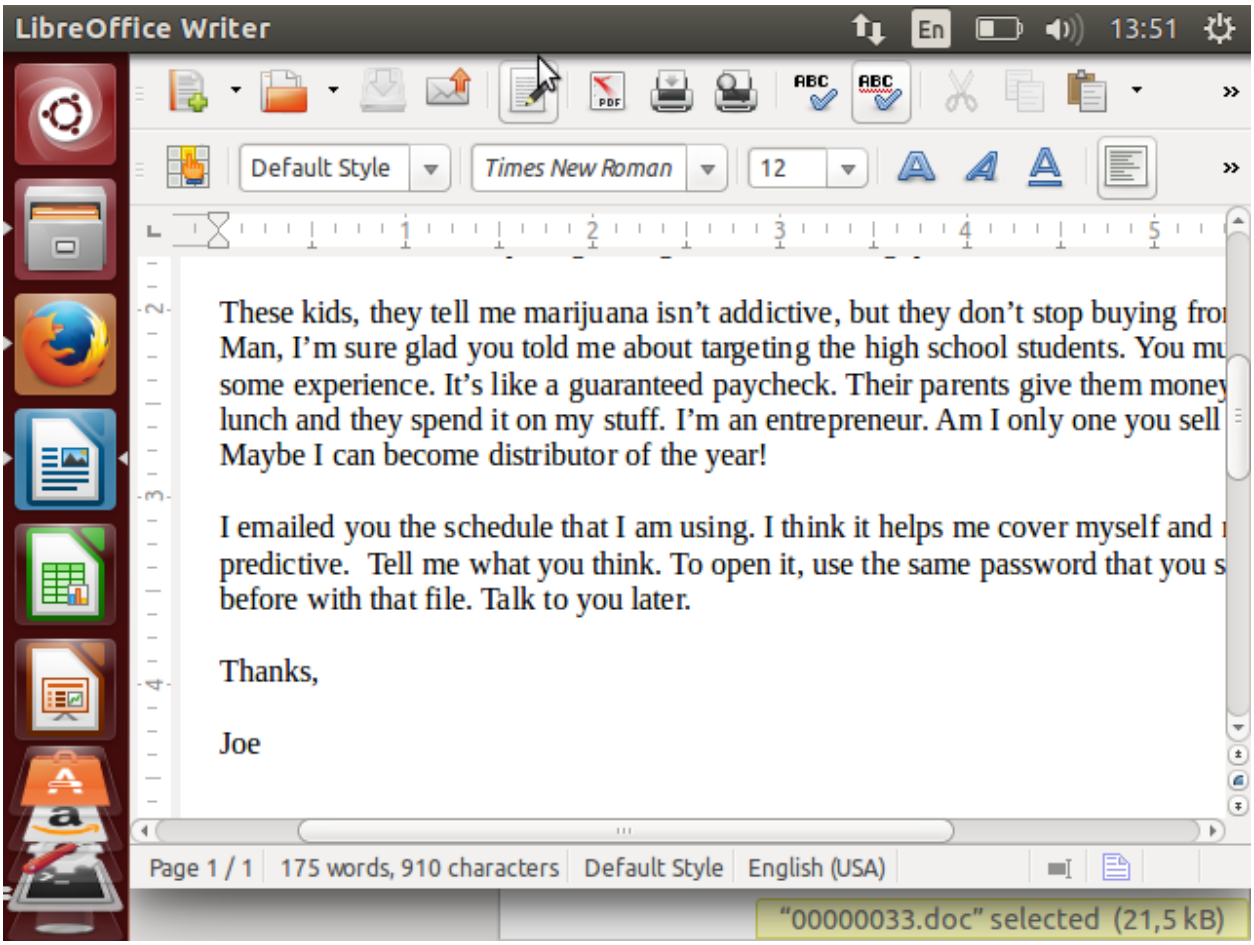
Gambar 35. Menjalankan perintah foremost



Gambar 36. File hasil recover



Gambar 37. Isi file recover



Gambar 38. Isi file recover

Dari penjelasan diatas, kita dapat mengetahui informasi-informasi yang dibutuhkan oleh polisi, bahwa:

1. Supplier marijuana langganan Joe Jacob adalah Jimmy Jungle. Dan daftar alamat di sini adalah nama-nama sekolah yang muridnya mengkonsumsi marijuana.
2. Data-data penting yang terdapat pada file coverpage.jpg adalah vol-Sector73.jpg dan vol-Sector104.zip. file-file tersebut penting karena berisi informasi nama pengedar dan supplier narkoba serta alamat targetnya.
3. Selain Smith Hill, masih ada sekolah lain yang sering dikunjungi oleh Joe Jacob, yaitu Key High School, Leetch High School, Birard High School, Richter High School, dan Hull High School.
4. Untuk merahasiakan isi file, file yang berisi jadwal kunjungan Joe ke sekolah-sekolah di masukkan ke sebuah zip vol-sector104.zip, dengan diamankan menggunakan password yang diselipkannya pada gambar vol-sector73.jpg. yang mana keduanya diubah kedalam ASCII kemudian digabungkan menjadi satu menjadi file 'image'.

5. Untuk memeriksa seluruh konten dalam setiap file (vol-Sector73.jpg dan vol-Sector104.zip) investigator melakukan perubahan ekstensi file berdasarkan headernya, setelah itu membuka file-file tersebut, ketika menemukan file berpassword, maka langkah yang dilakukan adalah mencari password dari file tersebut, setelah menemukan passwordnya, maka investigator menggunakannya untuk membuka file berpassword tersebut. Langkah-langkah ini dapat dilihat pada gambar 17 sampai dengan gambar 38.