Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

COMPUTER FORENSICS

Secara Garis Besar, di rangkum dari berbagai sumber :

"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."

Pada praktikum kali ini akan dilakukan sebuah kegiatan Computer Forensics . dapat dilihat diatas definisi dari Computer Forensics.

Tujuan dari Computer Forensics adalah sebagai berikut

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 data yang di kumpulkan di bagi 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.

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

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.

Tools yang digunakan adalah :

1. Autopsy
2. Foremost
3. Strings

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.

Langkah –langkah melakukan Computer Forensics.

Install tools Autopsy dan Foremost

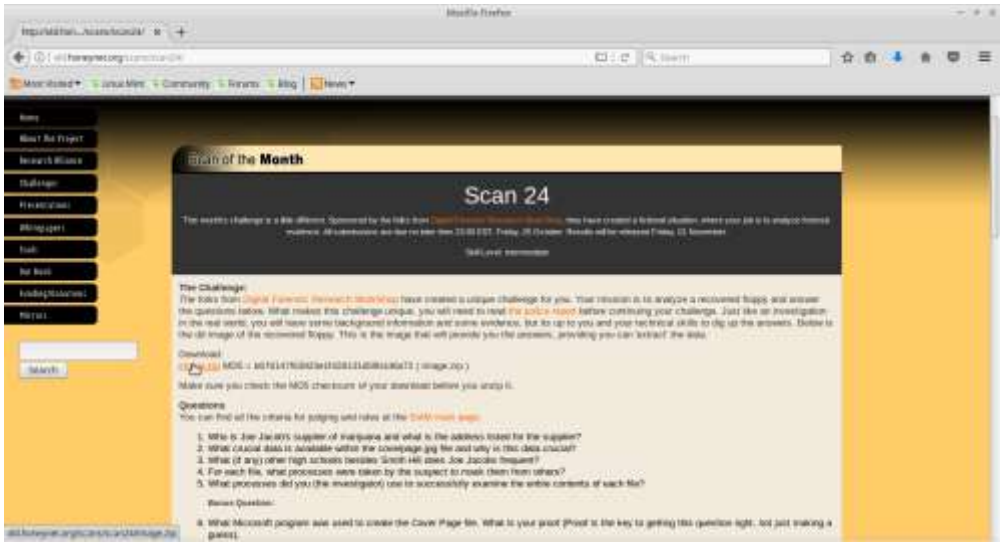
Buka website http://old.honeynet.org/scans/scan24/ pada browser

Download file Image.Zip

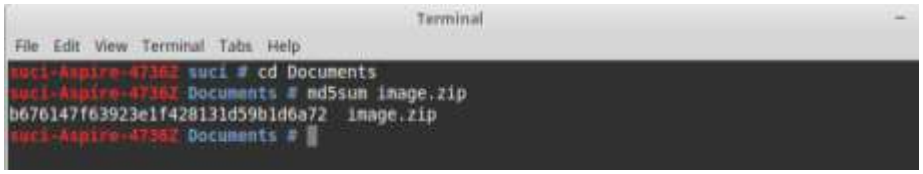
(old.honeynet.org/scans/scan24/image.zip)

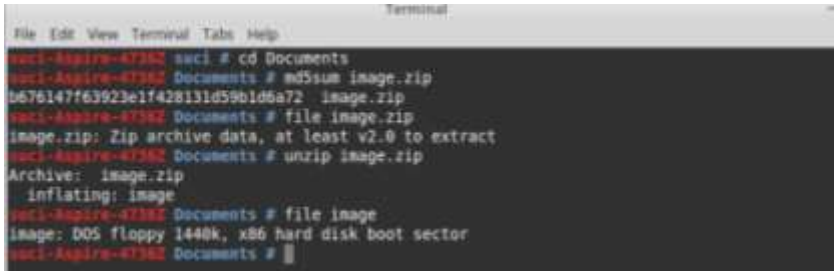
md5 : b676147f63923e1f428131d59b1d6a72

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



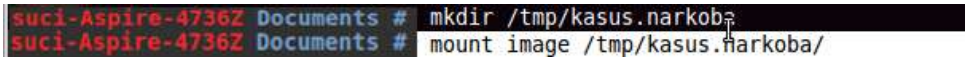
Fungsi md5sum : sebuah file pasti ada md5sum yang berfungsi untuk mengecek keaslian dari file atau integritas file.



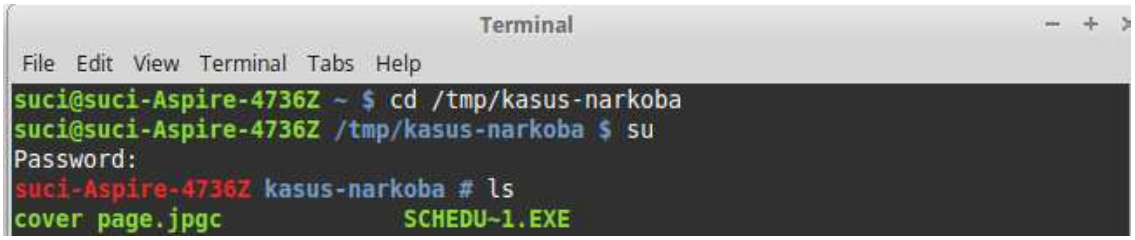


Fungsi perintah di atas : untuk mengecek tipe file. Jika kita menenmukan file yang tidak ada ekstensi, maka kita bisa menggunakannya.

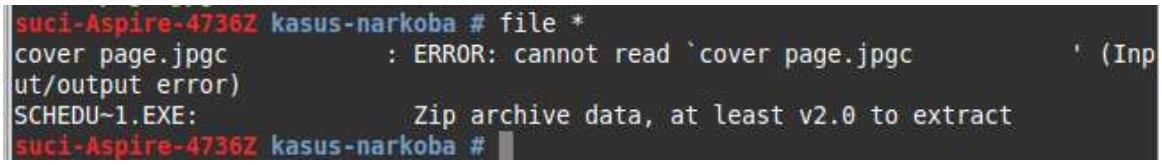
Setelah tahu bahwa file tersebut file boot sector, maka akan melakukan proses mounting



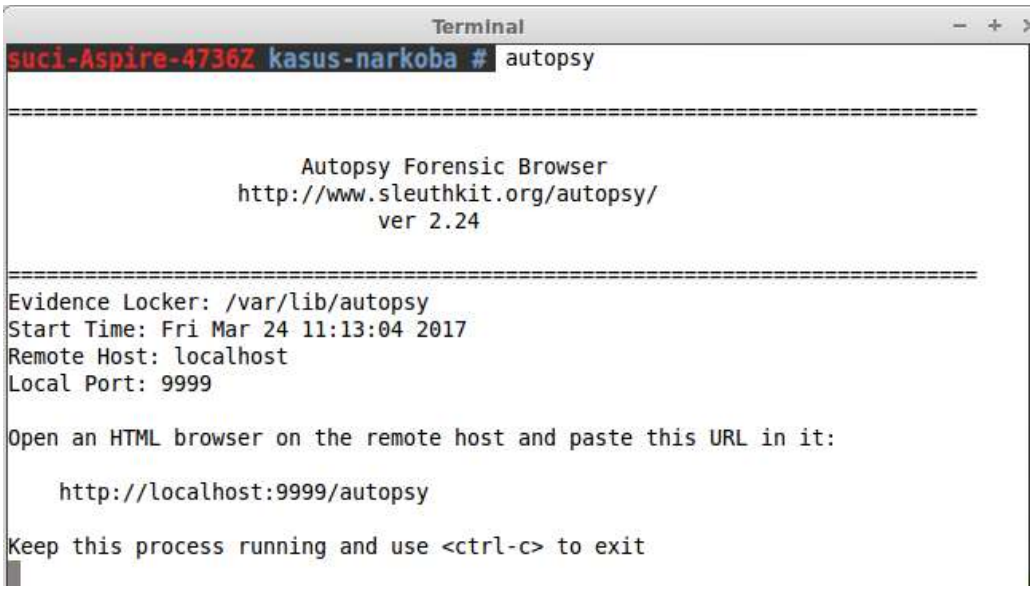
Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



Perintah untuk Mengecek keaslian file



Kemudian jalankan Autopsy dan Mengatur hostname, siapa yang melakukan forensik pada komputer target

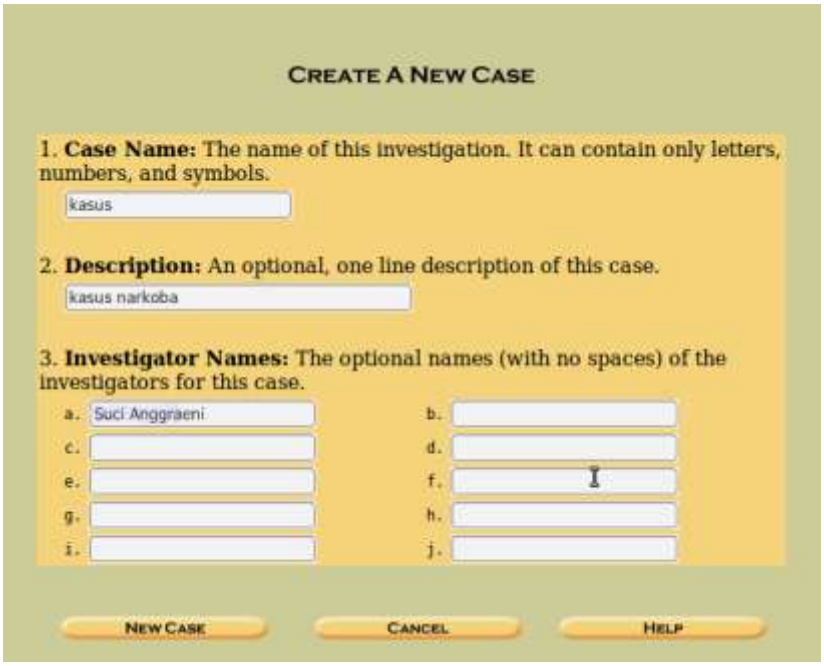


akses autopsy dengan browser http://localhost:9999/autopsy

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

Pembuatan New Case

Tujuan pembuatan *New Case* adalah agar kita dapat mudah mengakses kasus kasus sehingga tidak tercampur dengan kasus forensic lain nya .Klik *New Case*

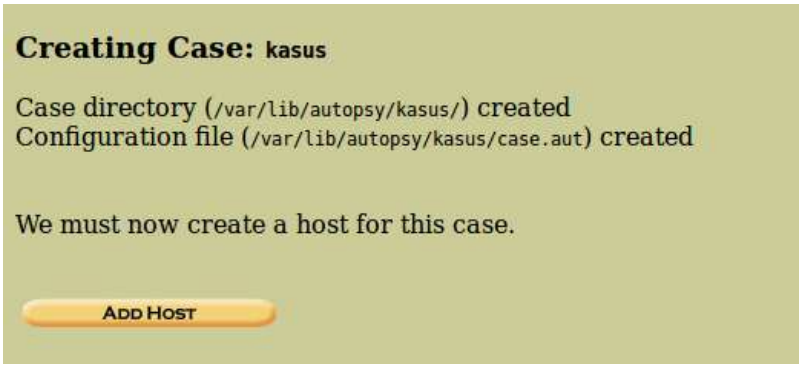


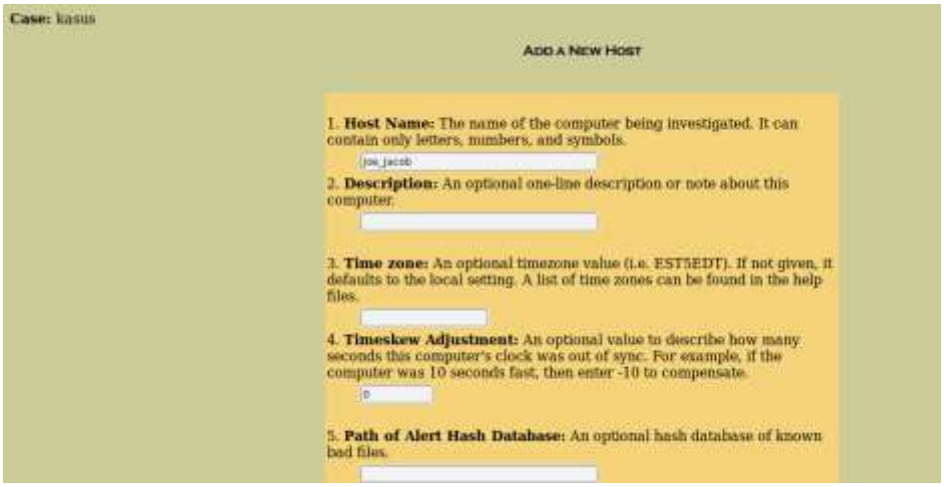
isikan Case Name hingga Investigator Name nya sesuai keinginan. lalu klik lagi New Case, setelah itu langsung saja klik Add Host pada Creating Case.

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

Membuat Host Baru

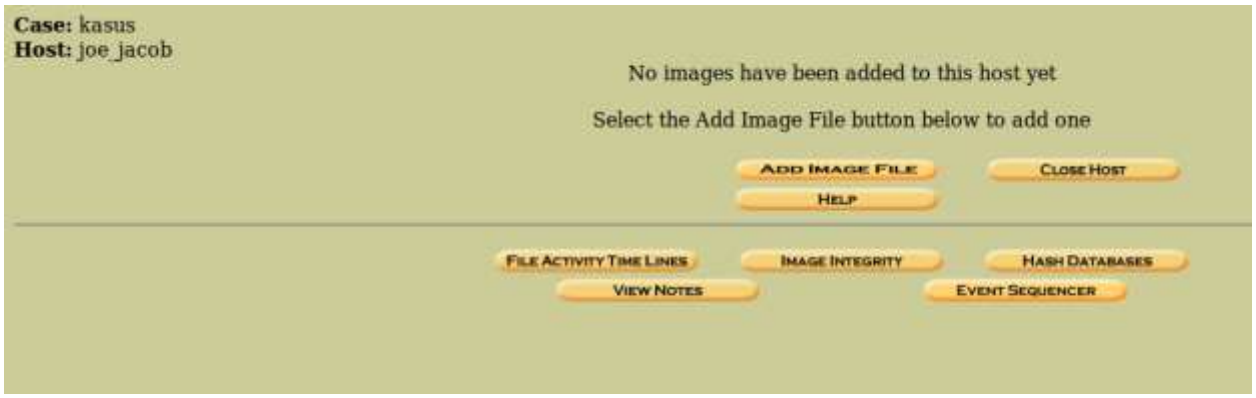
Pada step ADD NEW HOST isi *Host Name* terserah contoh nya Forensic1,





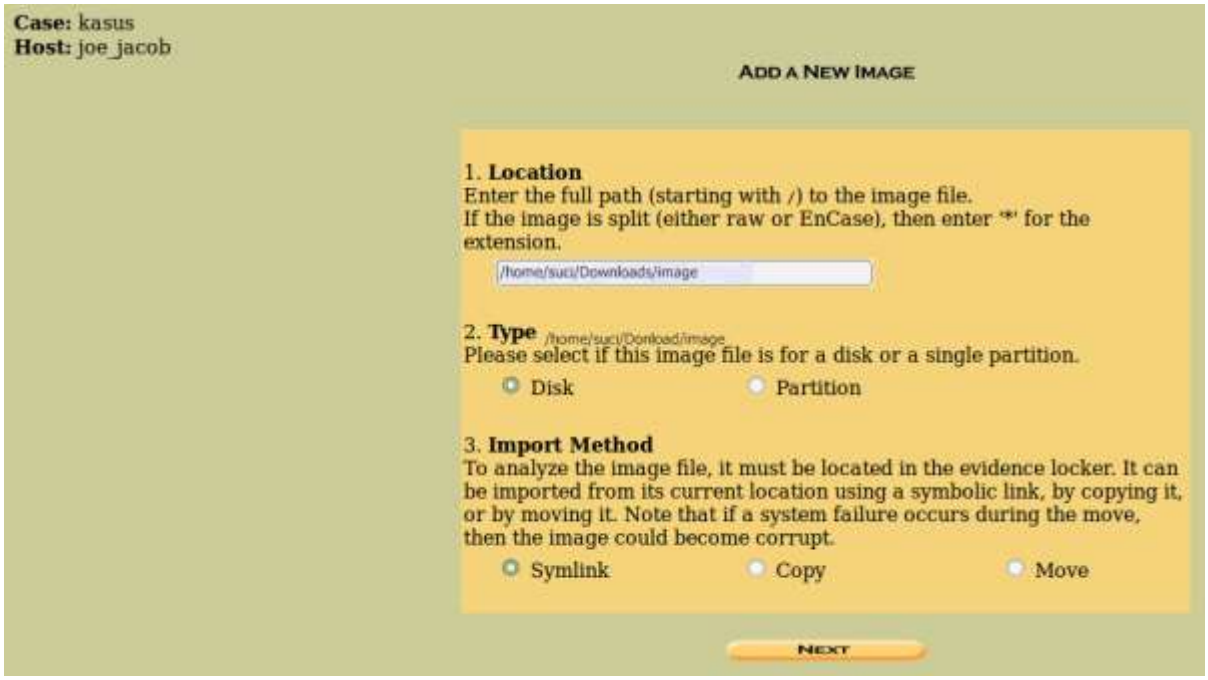
Menambahkan Image File

Klik Add Image file



Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

Pada form *Location* masukan lokasi dari image file yang ingin dilakukan forensi.

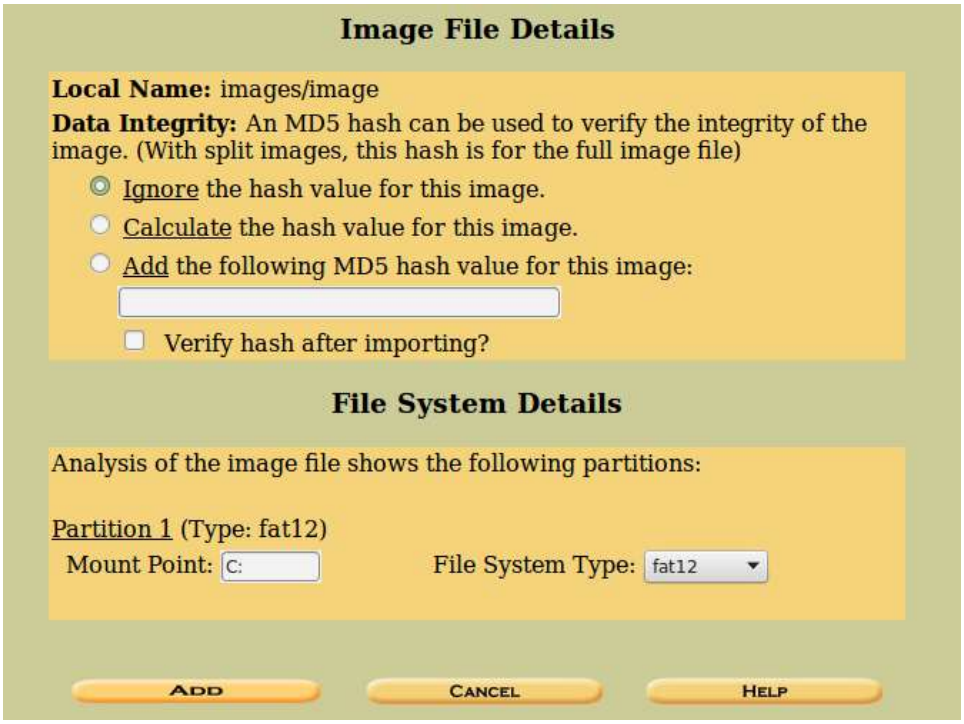


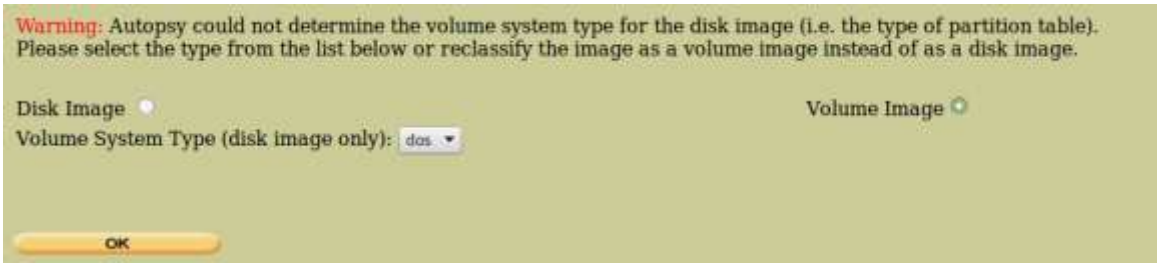
- /home/suci/Downloads/image : merupakan lokasi file image
- Pada Type masukan sesuai dengan type daei image file nya, apabila disk pilih disk apabila partisi pilih partition, pada kasus ini memilih disk.
- Pada bagian import method silahkan pilih sesuai keinginan . pada gambar diatas terlihat bahwa yang dipilih adalah symlink karena sudah punya salinan lain nya, jadi apabila file system tersebut rusak tidak menjadi masalah.

  Setelah semuanya selesai langsung sakja *klik next*.

Maka akan muncul seperti gambar dibawah ini.

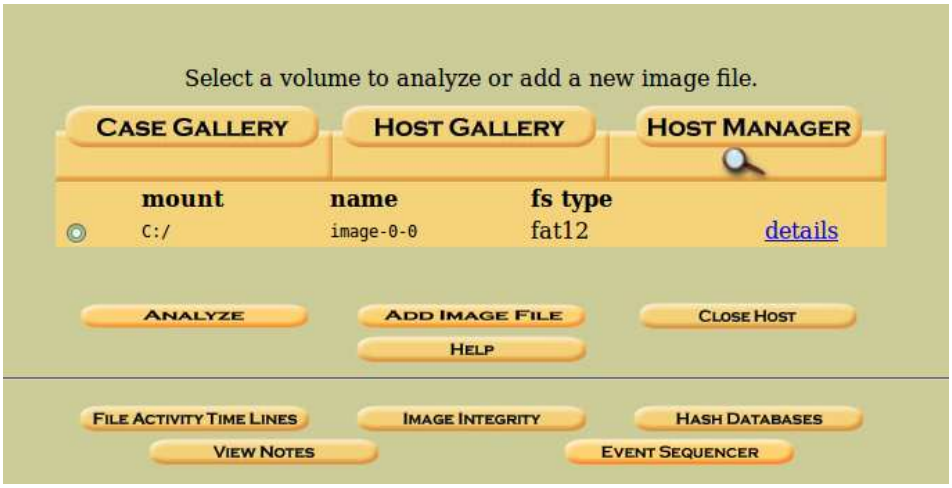
Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer





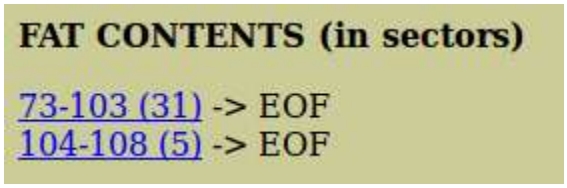
Lanjutkan saja dengan klik ADD->> OK.

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



Sampai tahap ini setup pada kasus autopsy sudah selesai, tinggal melakukan analis terhadap file system dari kasus yang dibuat.

File yang dipakai




```
suci-Aspire-4736Z Documents # file vol1-Sector73.raw
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
```

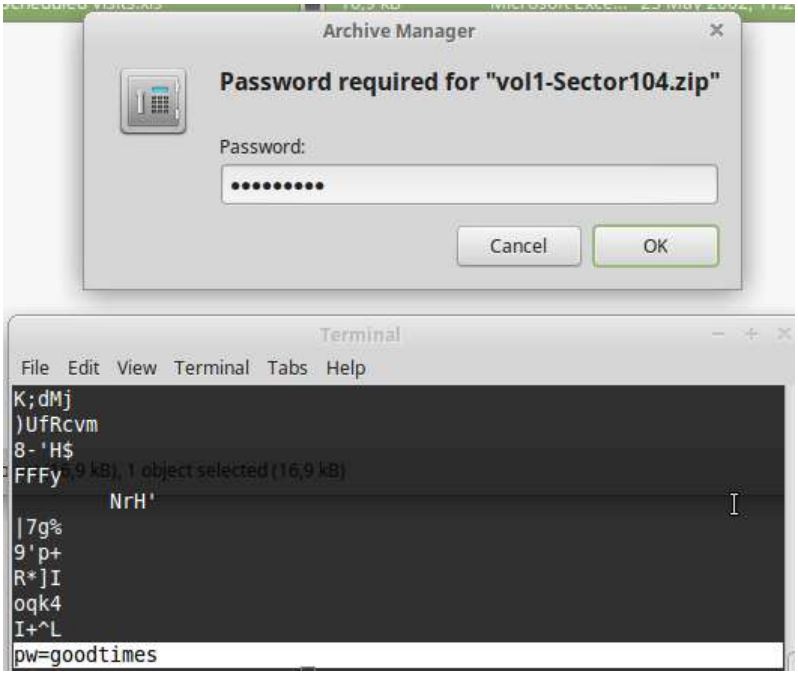
Rename file tersebut

Tampilan image vol1-sector73.jpg

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer

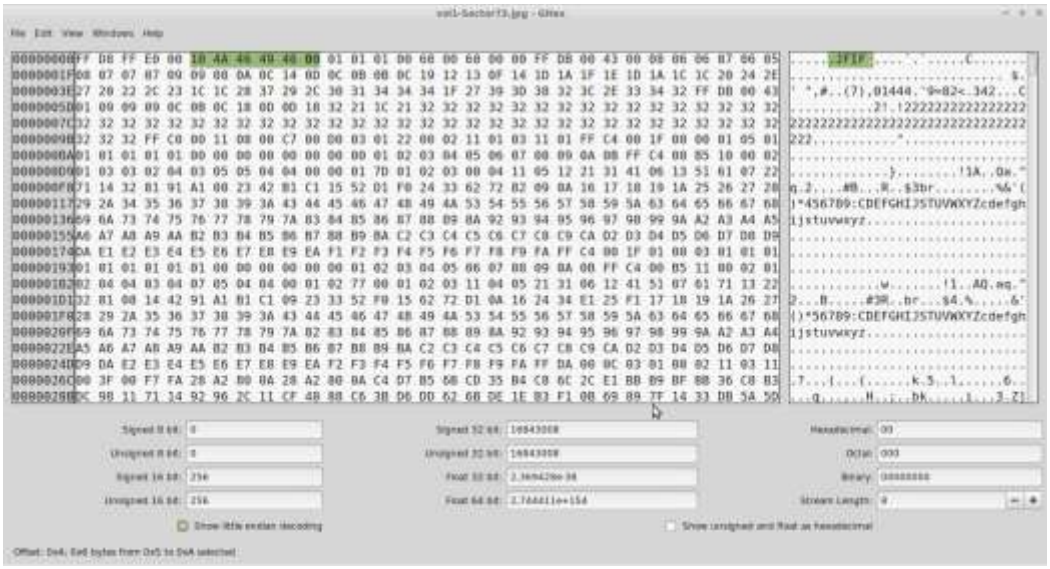
Selanjutnya gunakan string untuk menyimpan password di dalam file gambar

```
suci-Aspire-4736Z Documents # strings vol1-Sector73.jpg
JFIF
 $.' ",#
(7),01444
'9=82<.342
!2222222222222222222222222222222222222222222222222
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
        #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
A=2>c
```



Dapat dilihat pada terminal password yang didapatkan adalah “goodtimes”

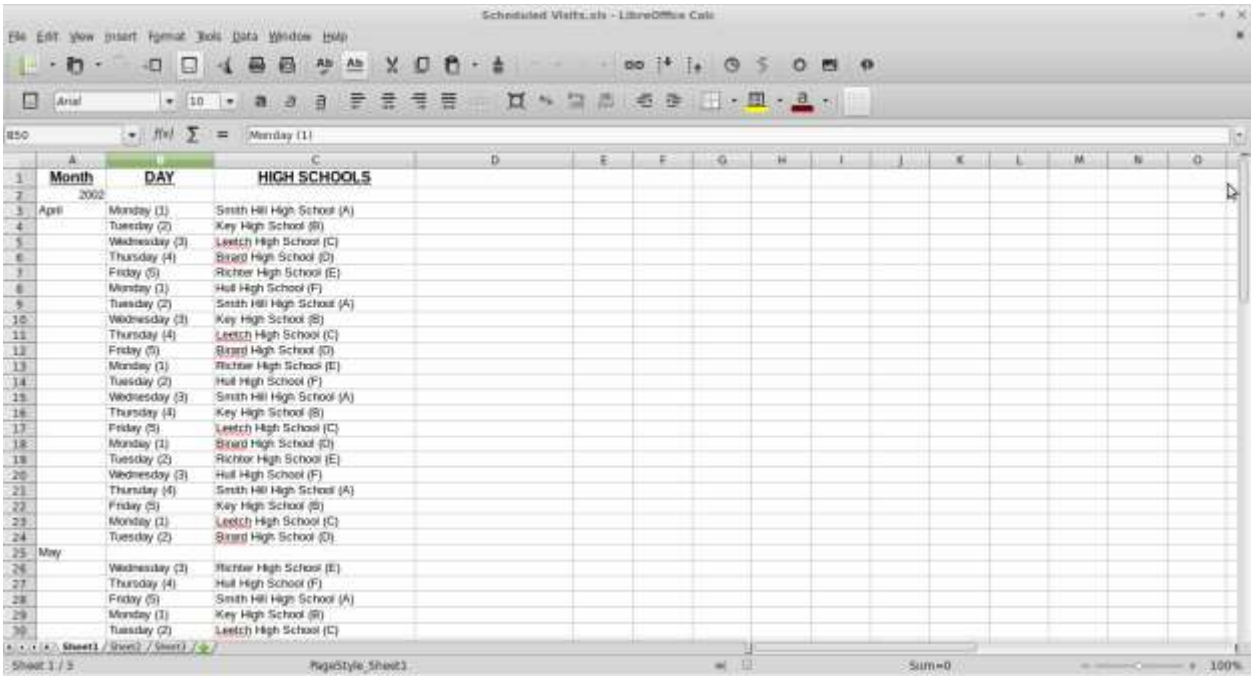
Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



Kemudian untuk Merecover jika signature nya hilang gunakan foremost

```
suci-Aspire-4736Z Documents # 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
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
```

Nama : Suci Anggraeni
Nim : 09011181320030
Keamanan Jaringan Komputer



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)	Brand 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)	Brand 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)	Brand 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)	Brand High School (D)
May		
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)

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