TUGAS KEAMANAN JARINGAN KOMPUTER
ANALISA COMPUTER FORENSIK

NAMA: EDI SUKRISNO
NIM: 09011181320043

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Computer Forensik

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."

Tujuan :

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.

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

Percobaan yang di lakukan dilab jaringan komputer yaitu:

KASUS :

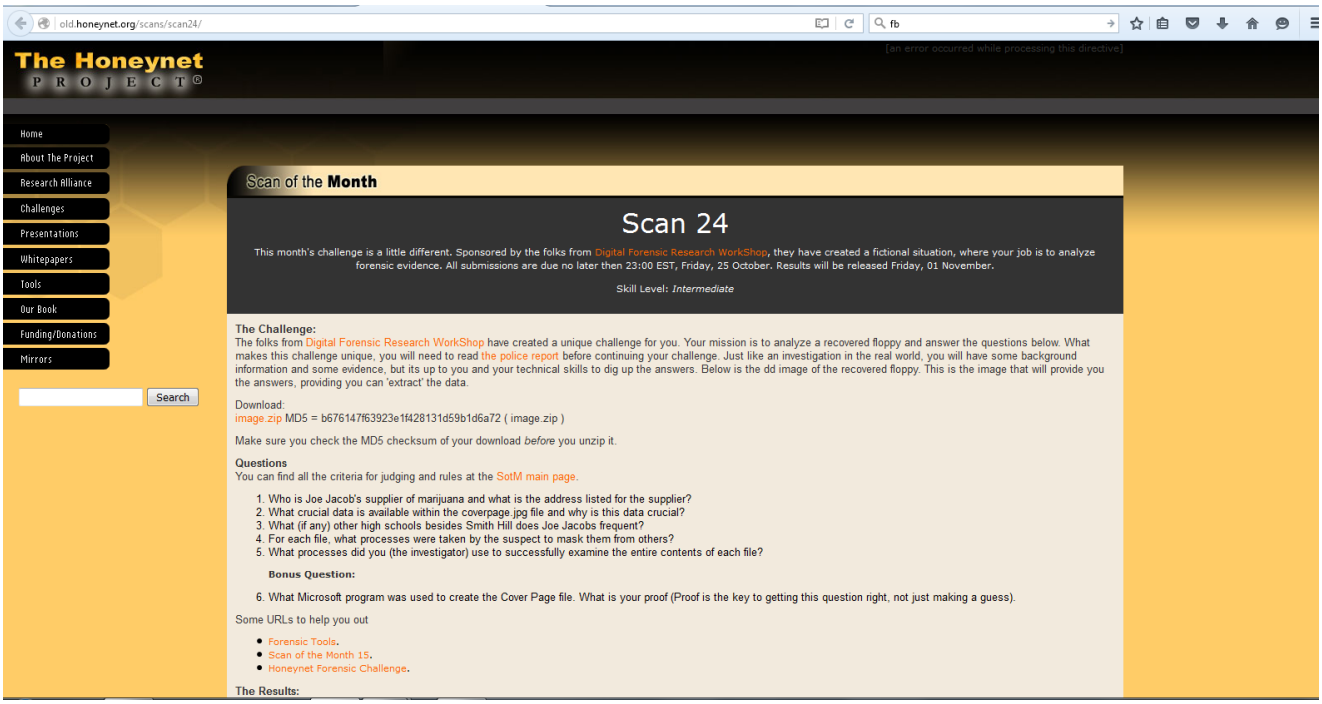
Ada seorang penegdar narkoba yang tertangkap, polisi ada harddrive yang sdah korup dr tersangka. Bagaimana kita me recover nya.

Tools :

1. Autopsy
2. Foremost
3. Strings

Langkah kerja :

1. Install tools, selain strings
2. Buka wesite berikut.



Gambar 1. Tampilan website

```
root@kali:~/Downloads# file image
image: DOS/MBR boot sector, code offset 0x3c+2, OEM-ID "MSDOS5.0", root entries
224, sectors 2880 (volumes <=32 MB) , sectors/FAT 9, sectors/track 18, serial nu
mber 0xc4b1cdcf, unlabeled, FAT (12 bit), followed by FAT
root@kali:~/Downloads#
```

Gambar 2. Tipe File yang di download dari website

Fungsi perintah di atas : untuk mengecek tipe file. Jika kita menemukan file yang tidak ada ekstensi, maka dapat menggunakan perintah tersebut.

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

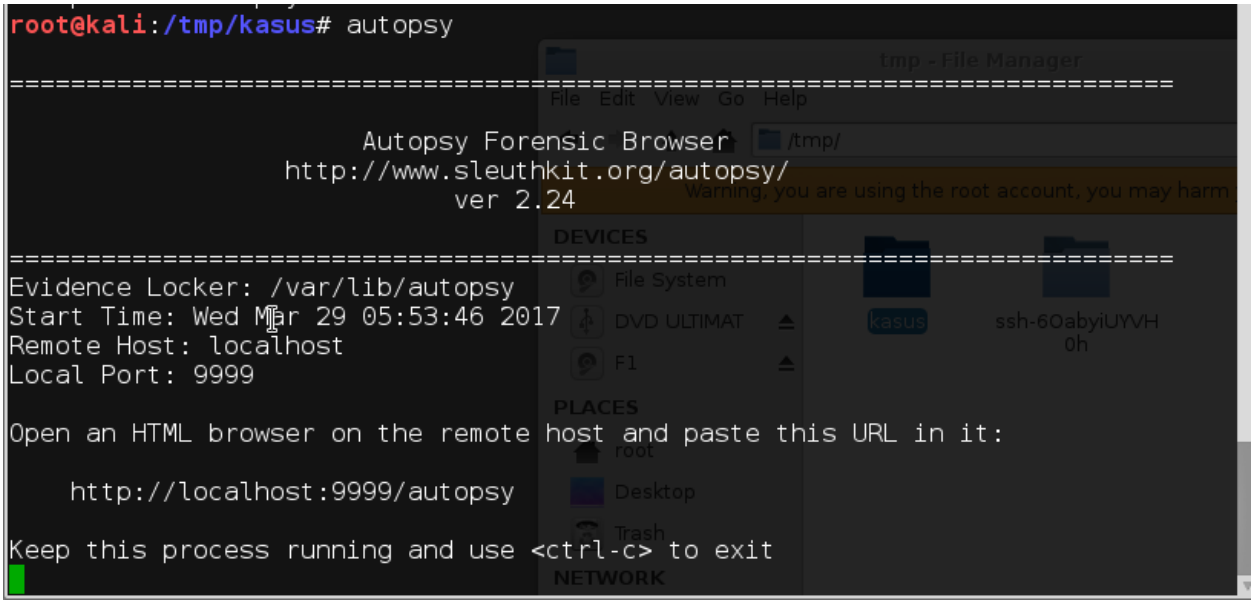
Setelah kita tahu bahwa file tersebut file boot sector, maka akan melakukan proses mounting pada file tersebut.

```
root@kali:~/Downloads# mount image /tmp/kasus
root@kali:~/Downloads# cd /tmp/kasus/
root@kali:/tmp/kasus# ls
cover page.jpgc          SCHEDU~1.EXE
root@kali:/tmp/kasus#
```

Gambar 3. Proses mouting

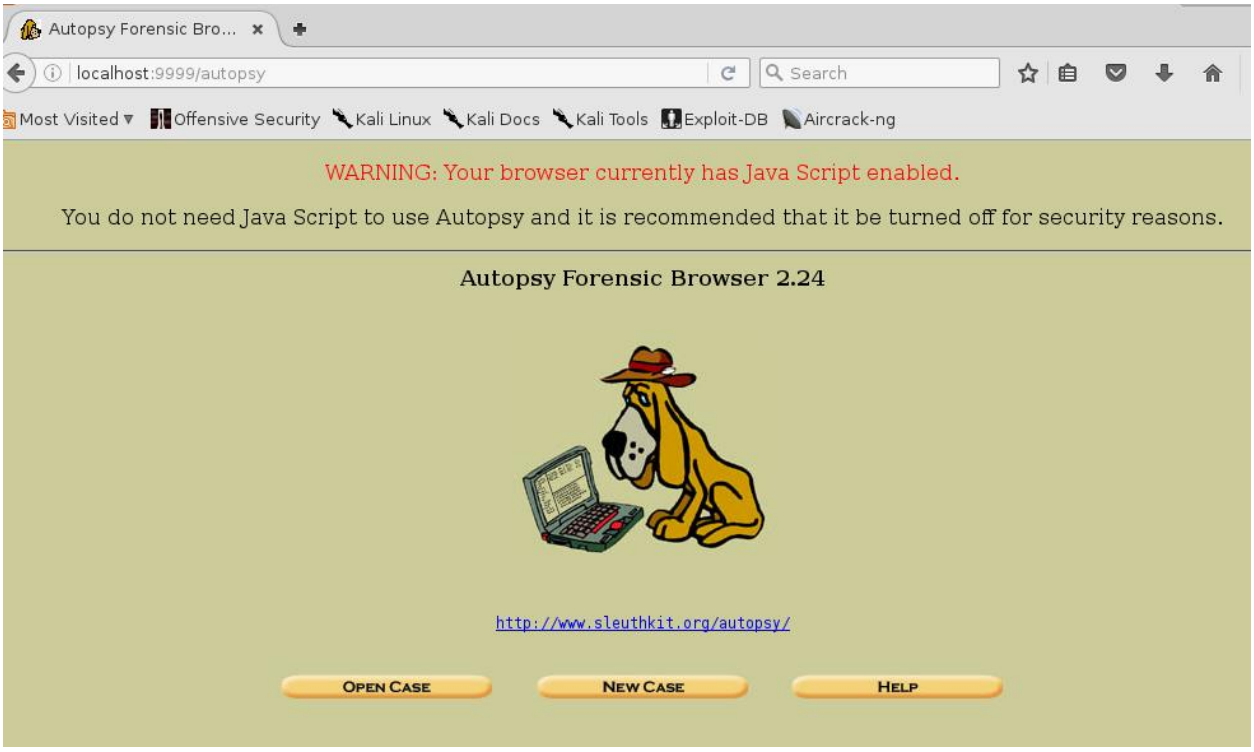
```
root@kali:/tmp/kasus# file *
cover page.jpgc          : ERROR: cannot read `cover page.jpgc          ' (Inp
ut/output error)
SCHEDU~1.EXE:              Zip archive data, at least v2.0 to extract
root@kali:/tmp/kasus#
```

Gambar 4. Mengecek keaslian file

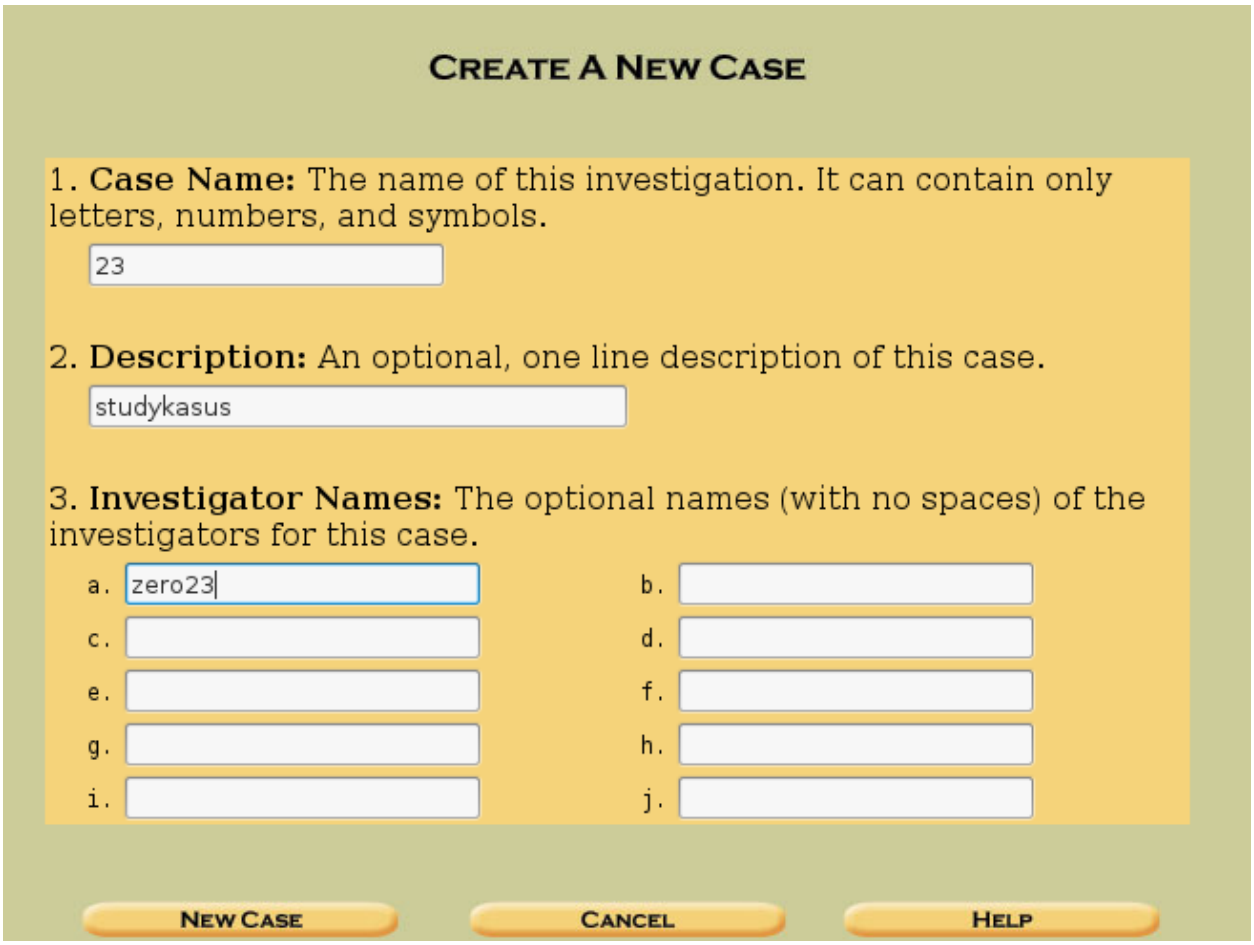


Gambar 5. Proses running autopsy

Setelah itu mengatur hostname untuk melakukan computer forensic

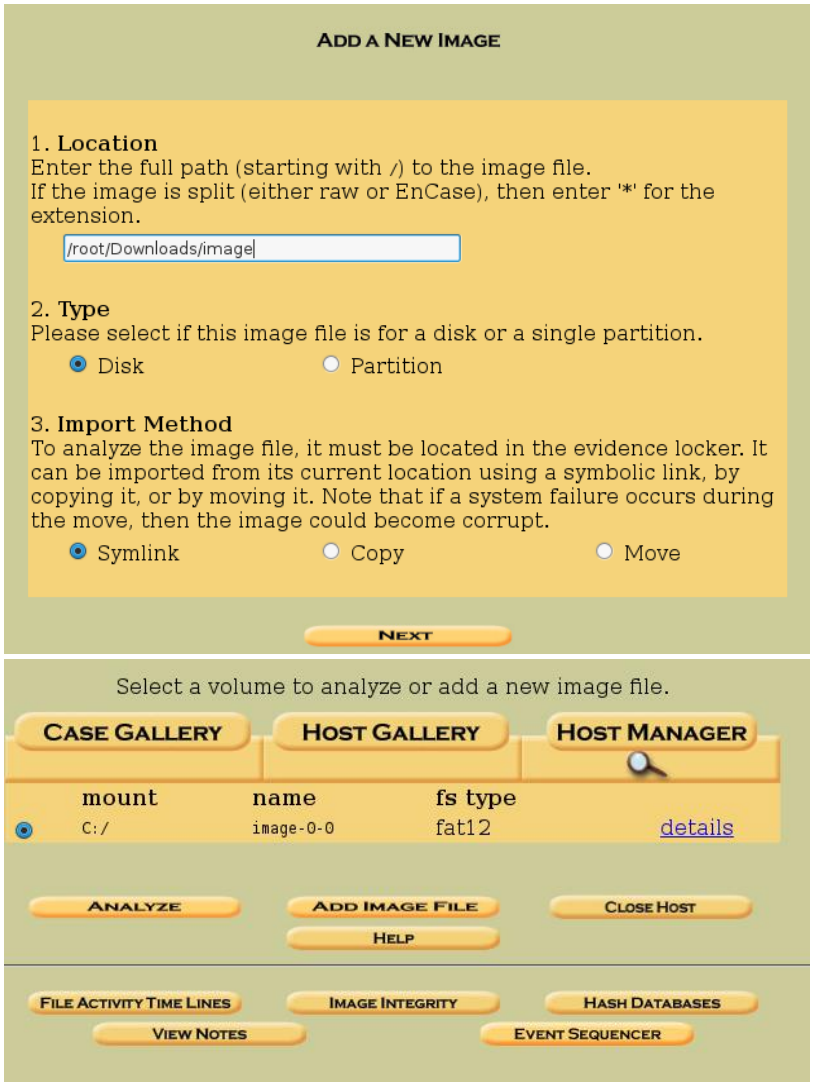


Gambar 6. Tampilan localhost pada autopsy

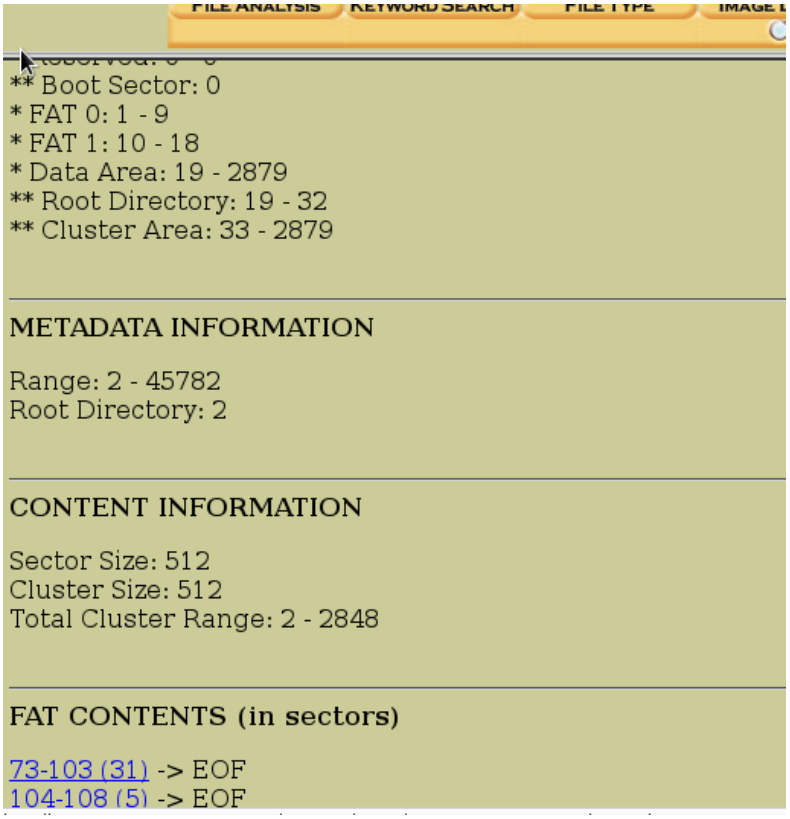


Gambar 7. Tampilan pembuatan host di dalam autopsy

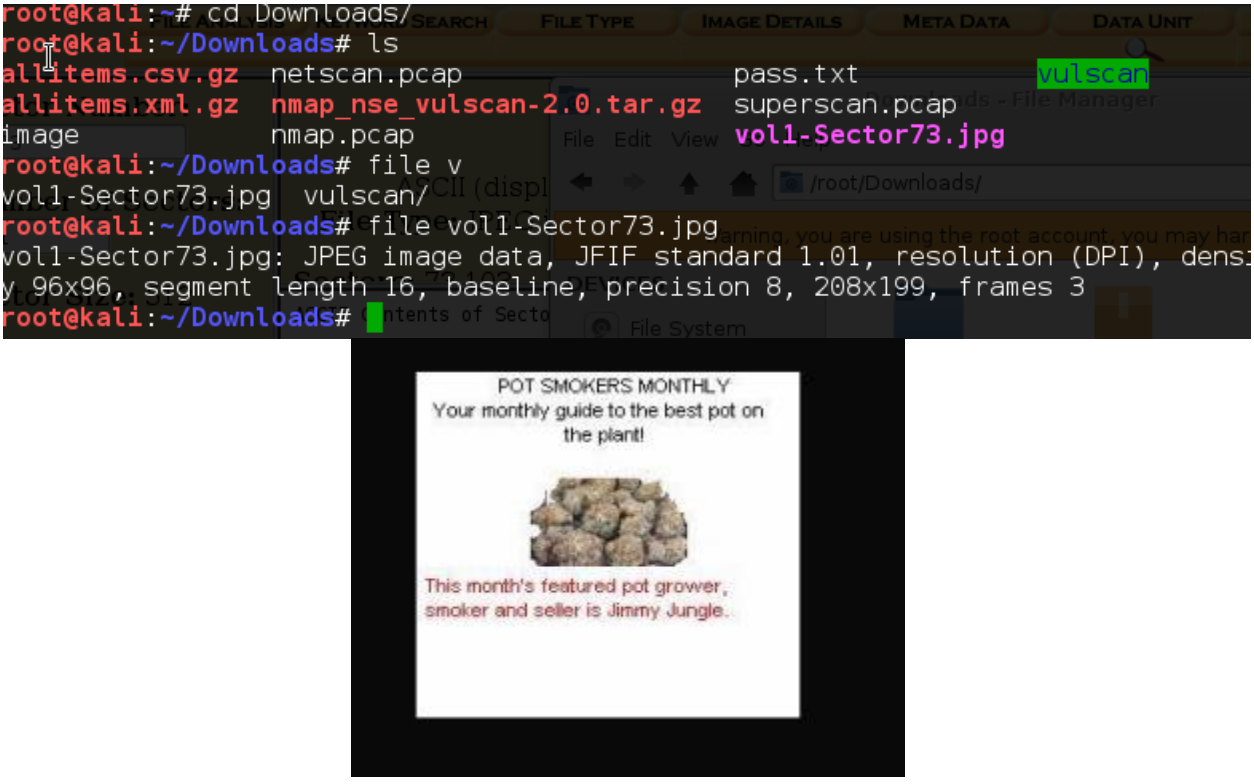
Gambar 7. Tampilan hasil pembuatan host di dalam autopsy



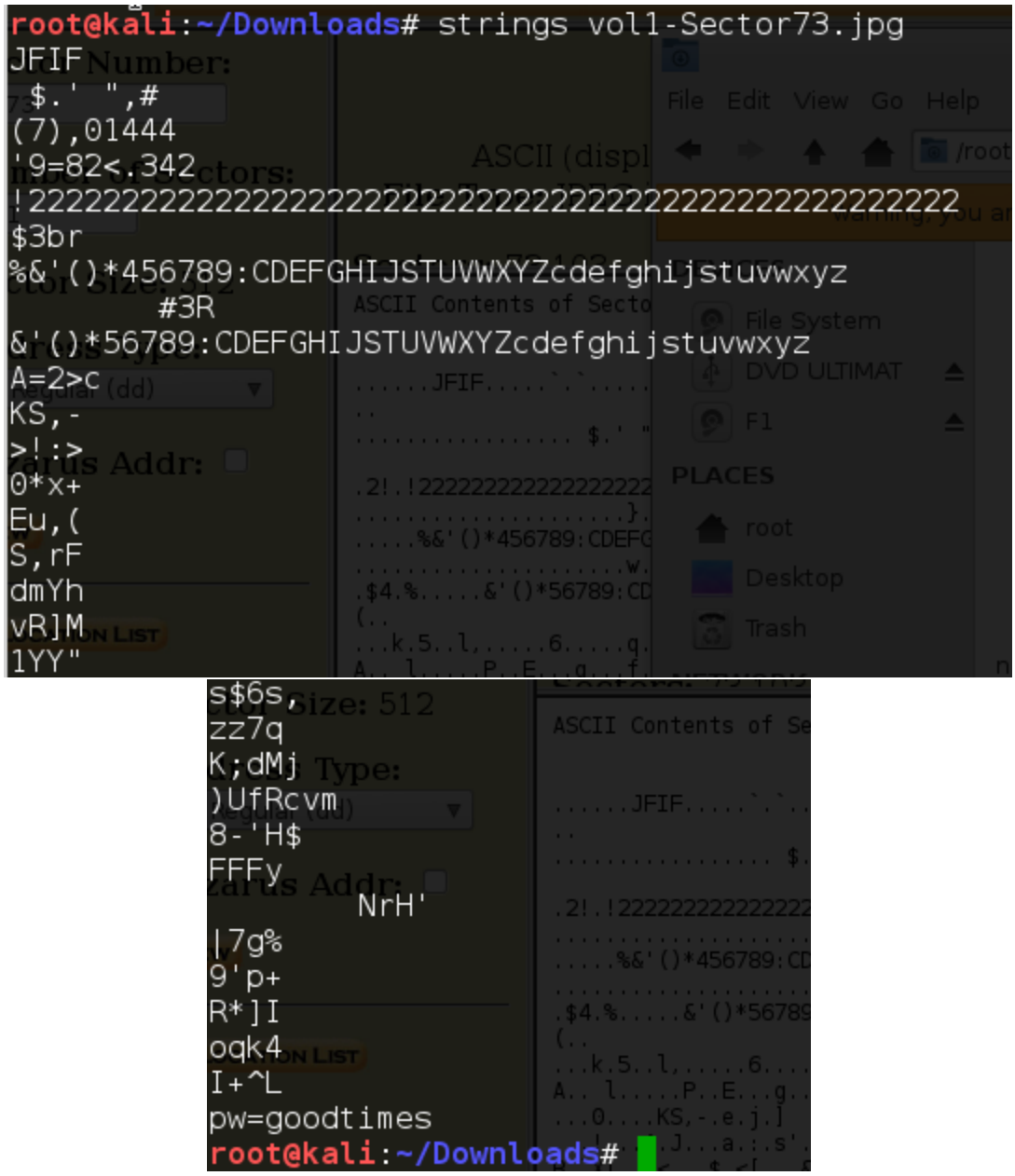
Gambar 8. Proses analyze file dengan autopsy



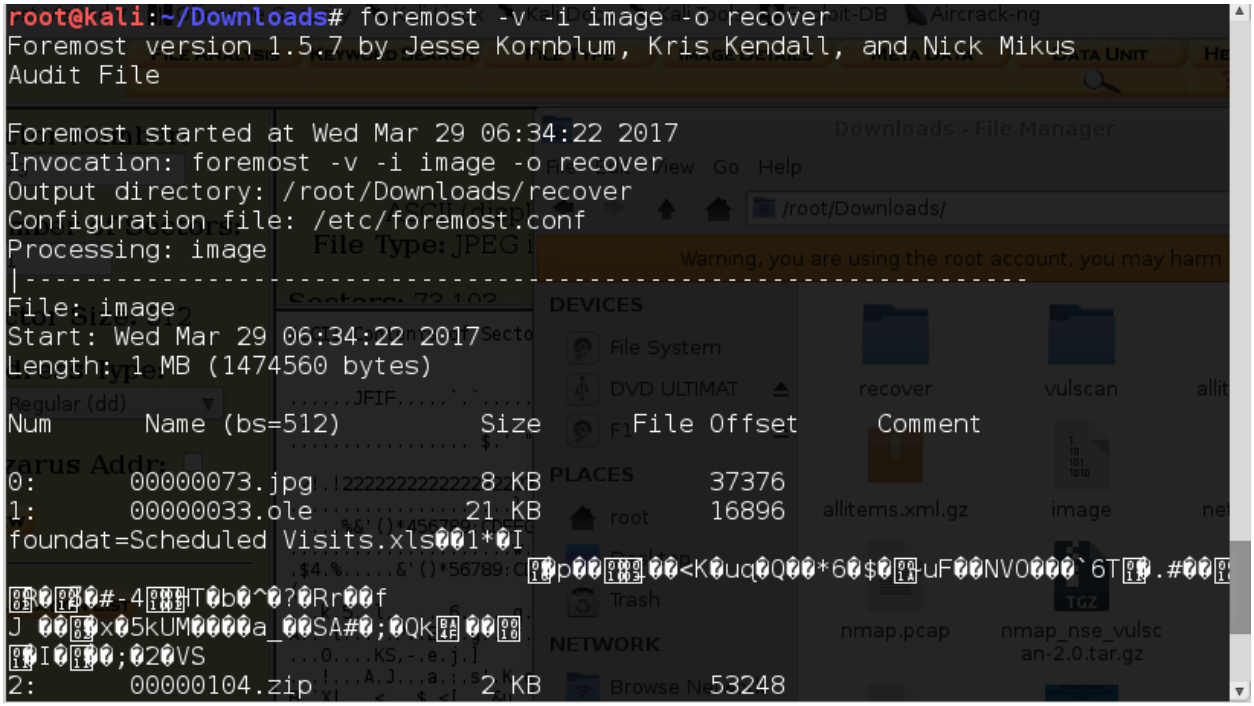
Gambar 9. Hasil analyze pada software autopsy



Gambar 10. File yang telah di download dari localhost autopsy



Gambar 11. Hasil analisa dengan software strings sehingga dapat di ketahui bahwa terdapat password di dalam file tersebut.



Gambar 12. Proses recover file image menggunakan software foremost