Proj 16: Sleuthkit dan Autopsy (15 pts.)

Kebutuhan Project

- Komputer Linux Backtrack 5 R3. Bisa menggunakan DEFT atau Kali Linux.

Menjalankan Komputer BackTrack Virtual

1. Masuk ke komputer Backtrack, Log in dengan user name **root** dan password **toor**. Masukkan perintah berikut diikuti dengan tombol Enter:
   `startx`

Meletakkan Evidence pada komputer Backtrack VM

2. Pada Linux Backtrack, buka elearning dan download file **anon-dd.7z** di elearning simpan di desktop. Buka jendela Terminal dan jalankan perintah berikut.

```
cd Desktop    (untuk ke direktori desktop tempat file anon1.dd)
7z x anon-dd.7z  (untuk mengekstrak)
cd dd             (pindah ke direktori dd)
mv anon1.dd.001 anon1.dd  (merubah nama anon1.dd.001 menjadi dd)
md5sum anon1.dd         (memeriksa nilai hash file)
```

   Perintah di atas masuk ke direktori tempat mendownload file anon, mengekstraknya, merubah namanya untuk meremove file ekstensi .001, dan menghitung nilai MD5 hash dari evidence disk. Nilai MD5 harus sama seperti di bawah, berakhiran dengan 4419:

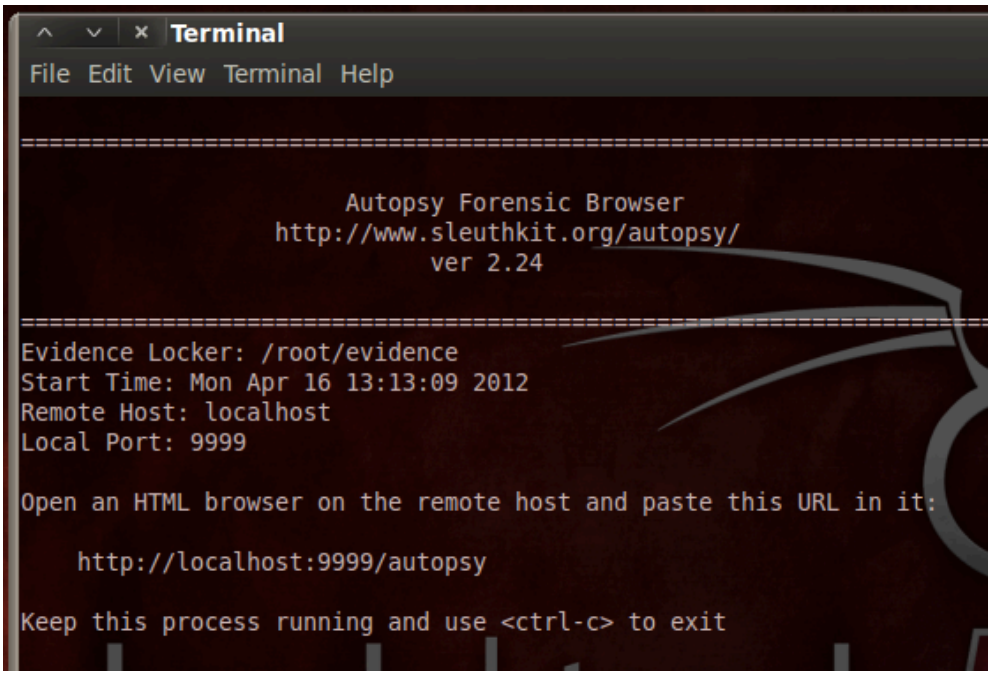
```
root@bt:/anon/dd# md5sum anon1.dd
0ca61246ac61c628ed98daa863354419  anon1.dd
root@bt:/anon/dd#
```

3. Jalankan perintah berikut untuk mengetahui informasi tentang file
   `file anon1.dd`
   akan keluar informasi tentang lokasi file di hardisk.

Menjalankan Autopsy

4. Di BackTrack, pada jendela Terminal, jalankan perintah berikut:
   `cd /pentest/forensics/autopsy`
   `./autopsy`

   Maka program akan berjalan, menampilkan teks sperti berikut. Biarkan jendelanya terbuaka.

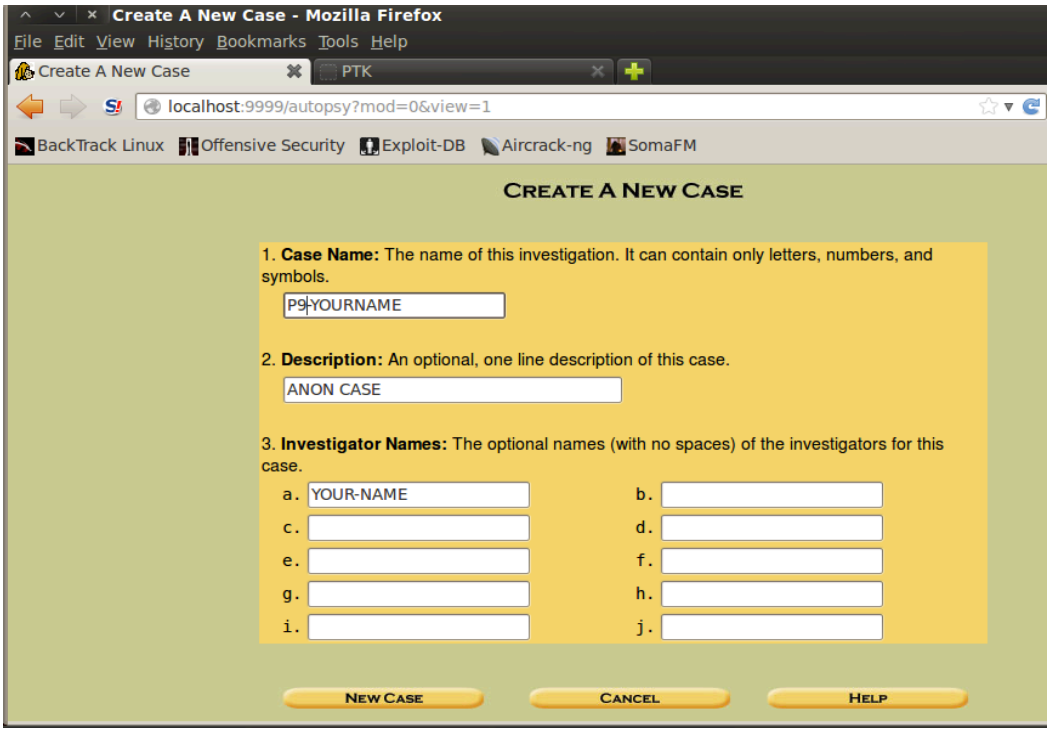


5. Dari menu BackTrack menu, click **Applications**, **Internet**, "**Firefox Web Browser**".
Ketika Firefox terbuka, arahkan ke alamat berikut:
http://localhost:9999/autopsy

Autopsy terbuka, sperti pada gambar di bawah ini. Akan terlihat pesan peringatan "Javascript is enabled". Abaikan saja.

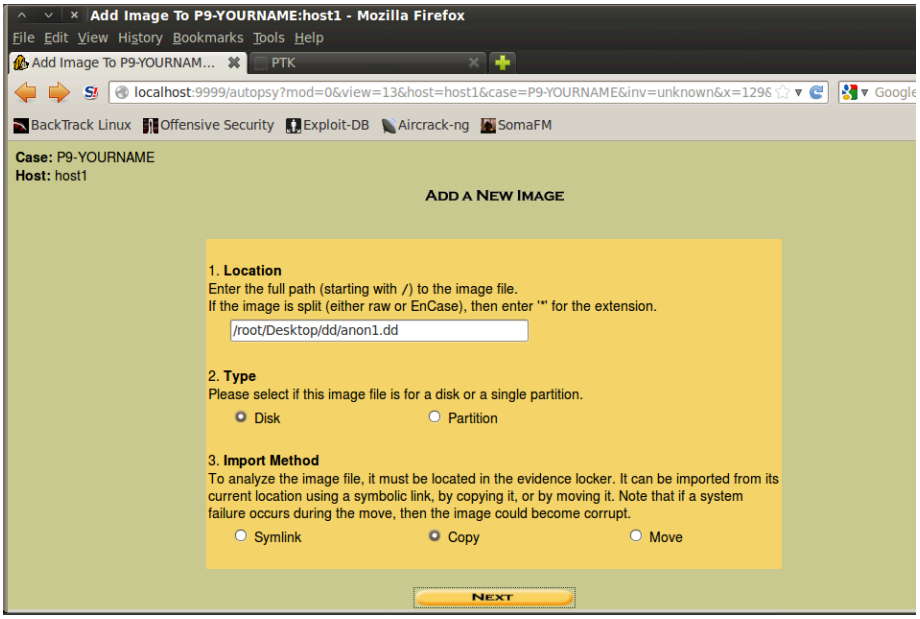
Membuka Case Baru dengan Autopsy

6. Pada jendela Autopsy, click tombol "**New Case**".
Isi form seperti gambar di bawah ini, ganti "Your-Name" dengan nama masing-masing.

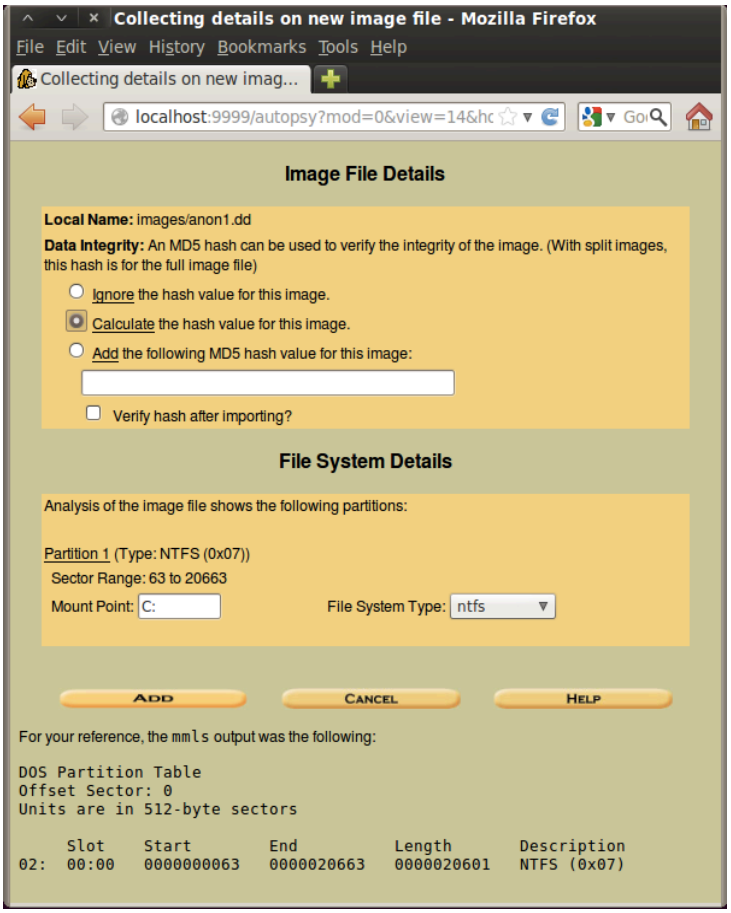


Click tombol "**New Case**". Pada window "Creating Case", click tombol "**Add Host**". Pada jendela "Add a New Host", accept default options dan click tombol "**Add Host**". Pada jendela "Adding host", click tombol "**Add Image**".

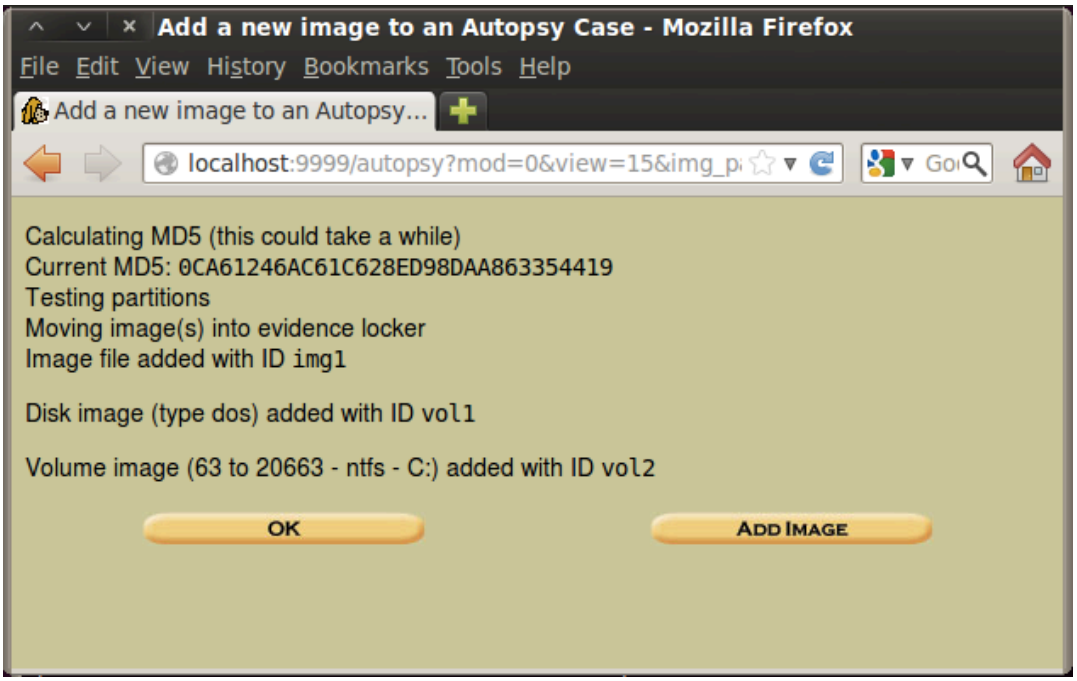
7. Pada next window, click tombol "**Add Image File**".
Pada jendela "Add a New Image", masukkan options berikut, seperti terlihat di bawah ini:
   - Location: **/root/Desktop/dd/anon1.dd**
   - Type: **Disk**
   - Import Method: **Copy**



Click **Next**.
Pada bagian "Image File Details", click tombol "**Calculate the hash value for this image**", seperti terlihat di bawah ini. Click **Add**.



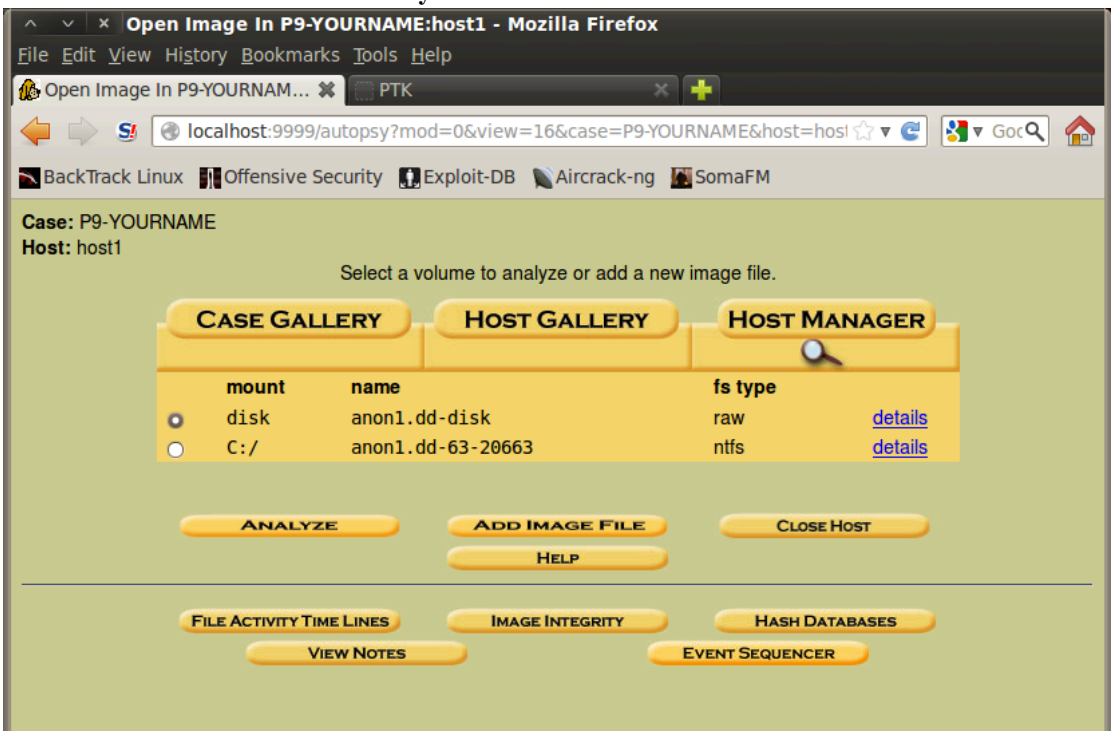
Maka akan tampil MD5 hash, yang berakhiran dengan 4419, seperti terlihat di gambar bawah.



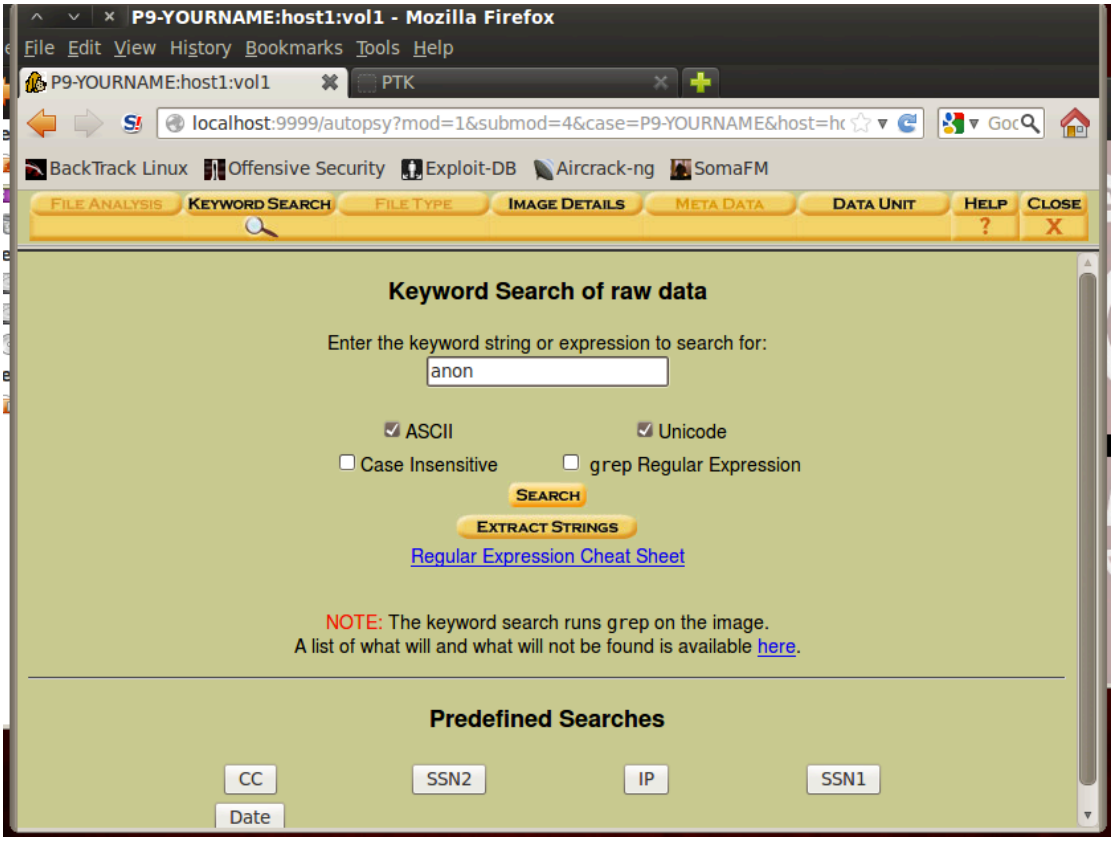
Click **OK**.

Pencarian di Autopsy

8. Jendela "Select a volume to analyze or add a new image file" terbuka, seperti pada gambar di bawah ini. Click tombol **Analyze**.

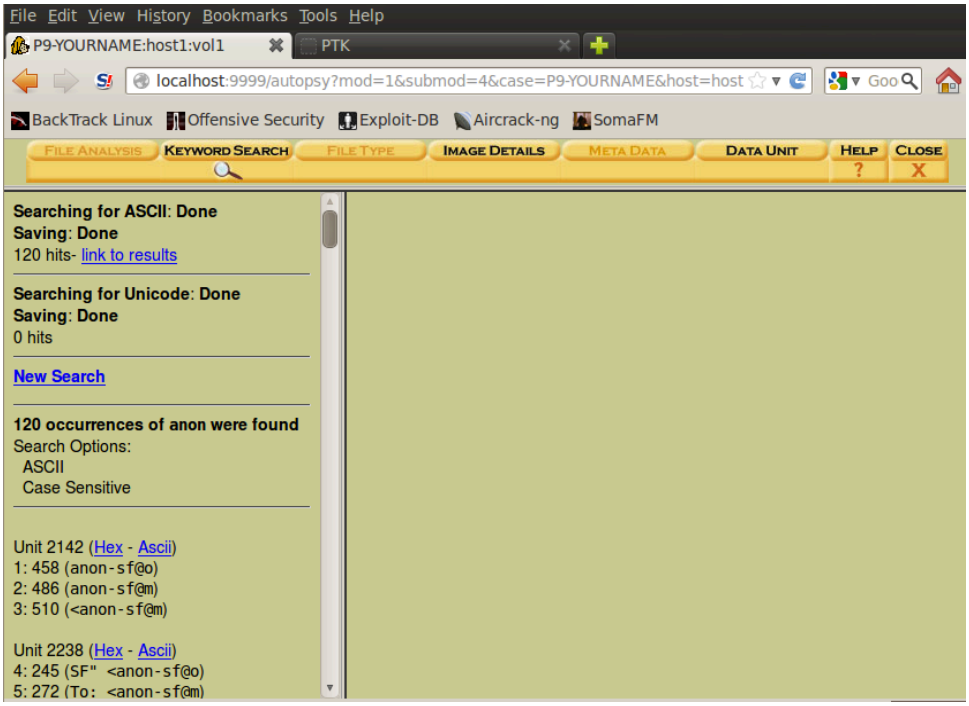


9. Pada next window, click tab "Keyword Search".
Pada kotak pencarian, ketikkan **anon** seperti terlihat di bawah ini. Click tombol **Search**.



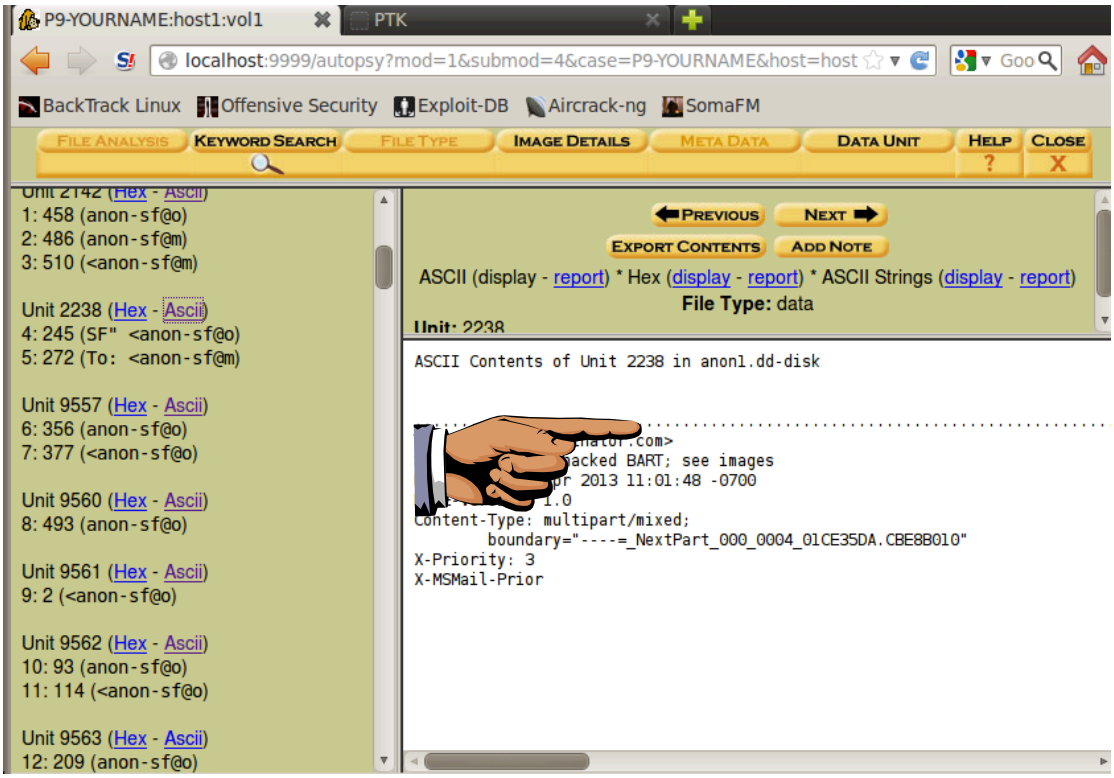
Hasil Pencarian

10. Terdapat "120 hits", seperti terlihat di bawah ini:



Memeriksa Hits

11. Pada sisi kiri, click link biru **Ascii** pertama yang terllihat untuk melihat details hits pada panel sebelah kanan, seperti terlihat di bawah ini.
    Perhatikan bagaimana merepotkan—gunakan mouse untuk mengclick tiap item; mereka tidak dikelompokkan dalam 22 files seperti FTK, dan tampilannya formatnya sangat minim sehingga kita hanya bisa meihat sebagian kecil dari horizontal line.



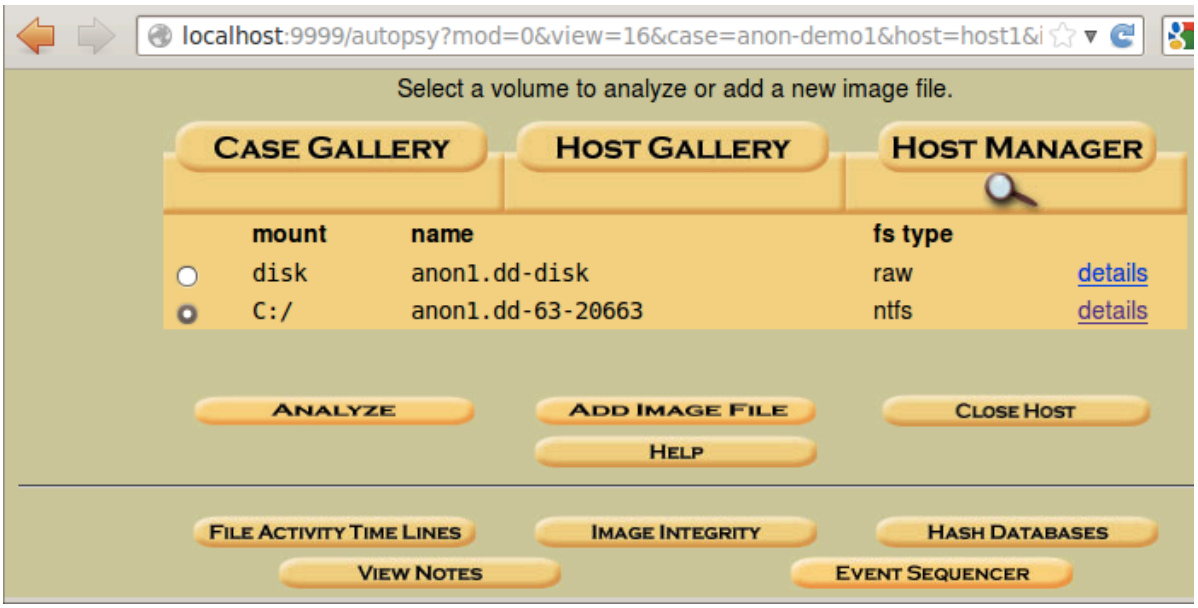
Meskipun dengan keterbatasannya, saudara masih bisa mencari incriminating email message – untuk membuktikan kejahatan. Ketika ditemukan file incriminating email message, simpan screen image.

Simpan Screen Image

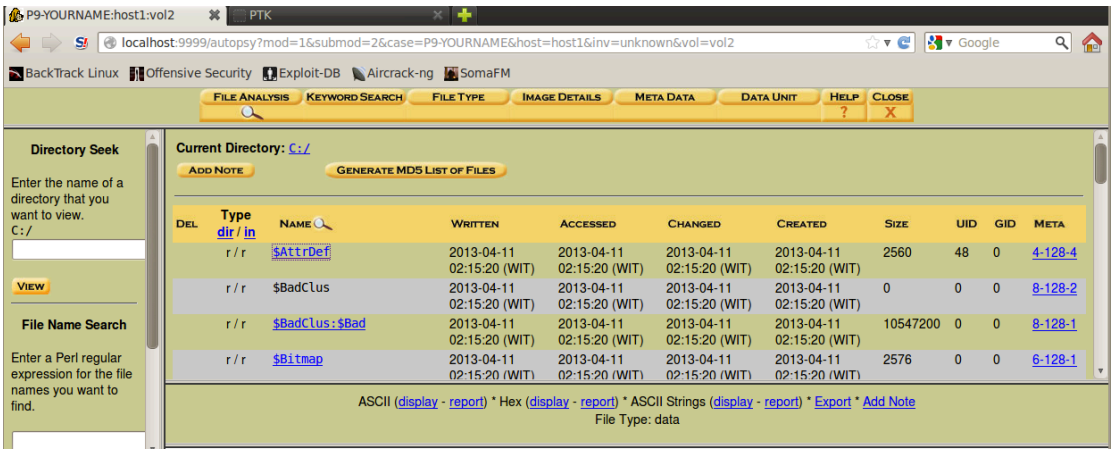
12. Pastikan layar yang ditampilkan berisi incriminating email message. Tekan tombol Printscreen.
    UNTUK MENDAPATKAN POIN MAKSIMAL SUBMIT WHOLE-DESKTOP IMAGE.
    Simpan dengan nama filename "**NamaKamu_Proj16**".

File Analysis

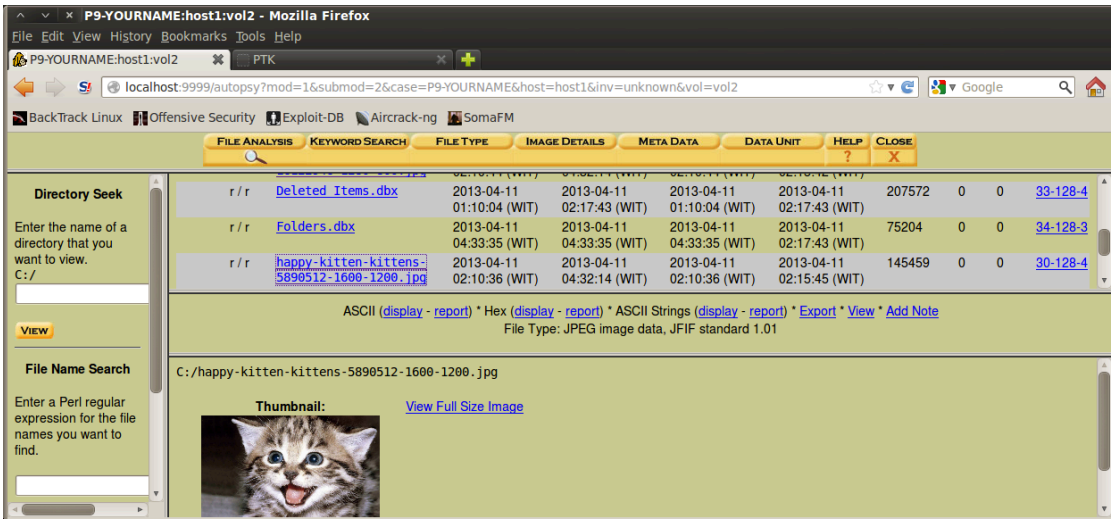
13. Pada halaman pencarian, di sisi kanan atas, click **Close**.
    Pada halaman Case Gallery, click **C:**, seperti terlihat di bawah ini:



14. Di sisi bawah kiri, click tombol **Analyze**.
Di sisi kiri atas next screen, click tombol "**File Analysis**".
Sejumlah file akan terlihat seperti pada gambar di bawah ini.
Perhatikan empat timestamps di tiap file: Written, Accessed, Changed, and Created. Inilah Keunggulan Autopsy: karena autopsy menginformasikan ke empat timestamps, sementara FTK hanya tiga.



15. Coba cari file gambar. Bisa terlihat ada file anak kucing I was able to view the kittens, seperti terlihat di bawah ini, tapi tidak bisa ditemukan incriminating image, karena filenya sudah di deleted.



Sebenarnya Sleuthkit bisa melakukan file carving, untuk merekonstruksi files yang sudah didelete, tapi tentu saja sangat ribet dibandingkan FTK atau ProDiscover.

Mengumpulkan Project

16. Kirim melalui elearning

Last modified 18-4-2013