MODUL PRAKTIKUM



DIGITAL FORENSIK

UNIVERSITAS TEKNOLOGI MATARAM

2019

Jl. Kampus Universitas Teknologi Mataram, Kekalik, Mataram

KATA PENGANTAR

Puji syukur kehadirat Allah SWT rahmat dan karunianya sehingga Modul Praktikum Forensik Digital Program Studi Teknik Informatika tahun 2018/2019 dapat diselesaikan, sebagai pedoman bagi mahasiswa Program Studi Rekayasa Sistem Komputer Universitas Teknologi Mataram dalam praktikum digital forensic agar mahasiswa mendapatkan gambaran secara jelas materi praktikum yang akan disampaikan tersebut.

Terimakasih disampaikan kepada semua pihak yang telah membatu dalam penyusunan modul ini sehingga dapat terselesaikan tepat waktu. Kami menyadari masih terdapat kekurangan dalam modul ini untuk itu kritik dan saran terhadap penyempurnaan buku ini sangat diharapkan. Semoga buku ini dapat memberi maanfaat bagi mahasiswa mahasiswa Program Studi Rekayasa Sistem Komputer Universitas Teknologi Mataram terutama bagi yang mengambil praktikum forensic digital dan bagi semua pihak yang membutuhkan.

Mataram,01 Juli 2019

DAFTAR ISI

KATA PENGANTAR i
DAFTAR ISI ii
Praktikum 1 (Digital Imaging) *FTK Imager Windows Base* 1
Praktikum 2 (Digital Imaging) *dd linux Base* 9
Praktikum 3 Explore Investigasi File .DD 12
Praktikum 4 Wireshark 28
Praktikum 5 Sosial Chat Forensics 42
Praktikum 6 Email Forensics "Tools NetworkMiner" 55
Praktikum 7 Data Carving 65
Praktikum 8 Report Investigation 70

Praktikum 1

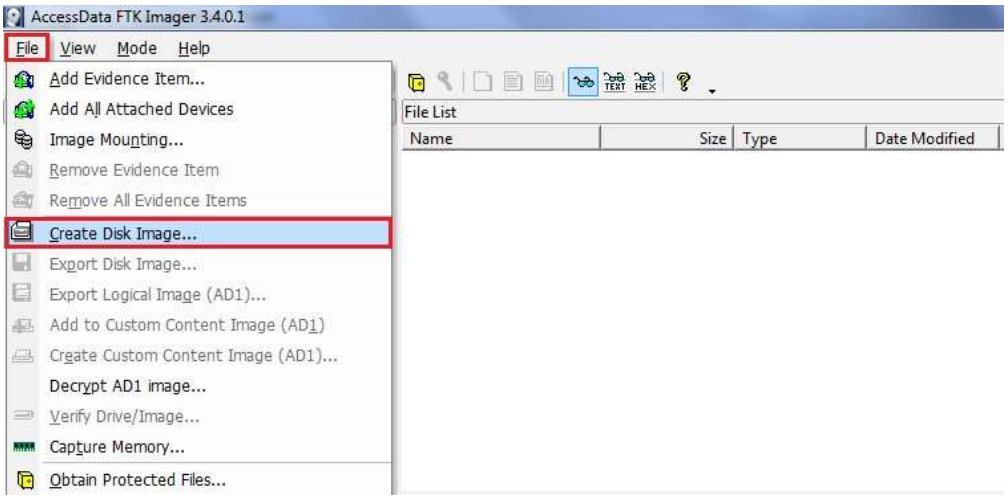
(Digital Imaging) *FTK Imager Windows Base*

Pretest:

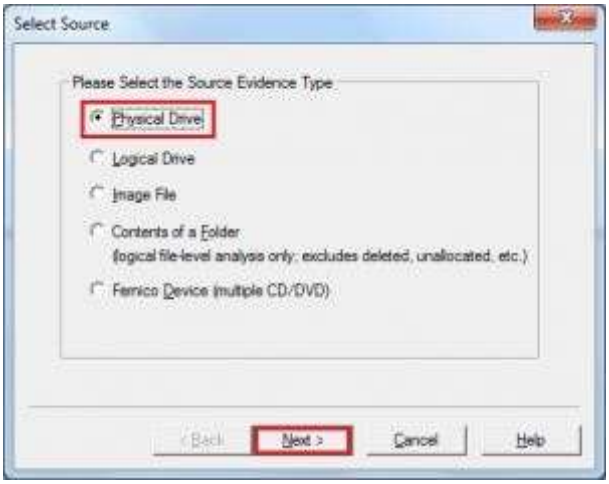
1. Sebutkan definisi dari Digital Imaging!
2. Apa fungsi utama tool imaging FTK dalam kaitannya investigastion barang bukti?

Langkah Praktikum:

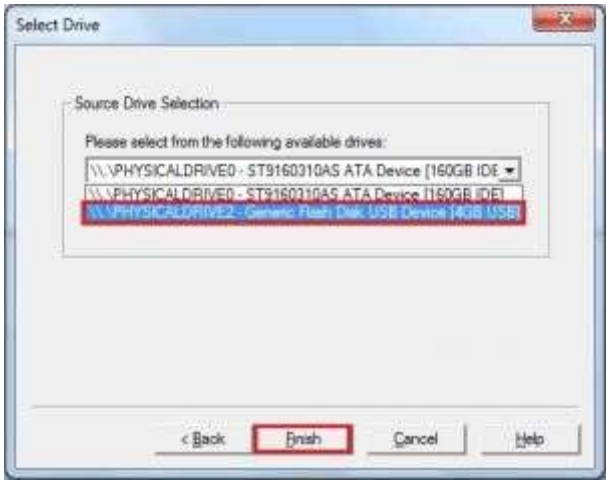
- Buka aplikasi FTK Imager yang sudah di-*install* . Klik **Start** –> **All Programs** –>**AccessData** –> **FTK Imager**. Atau lewat *shortcut* di Desktop jika ada.
- Pilih menu **File** –> **Create Disk Image…**



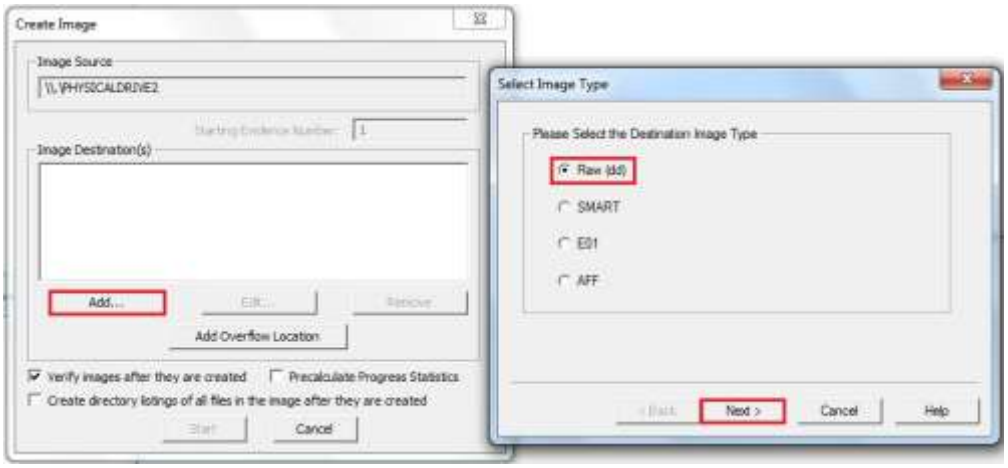
- Pilih **Physical Drive**, kemudian klik **Next**.



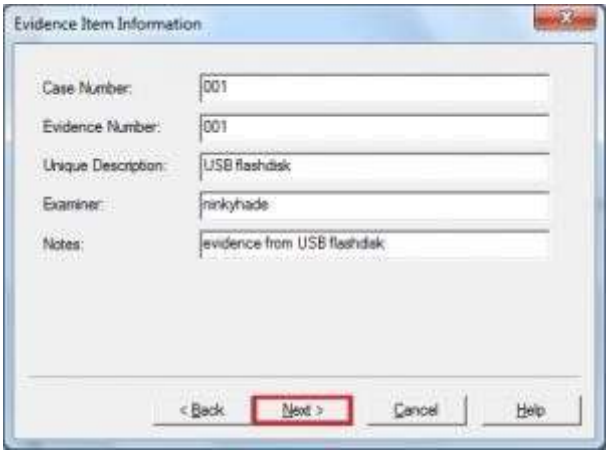
- Pilih *device* yang akan dibuat *physical image*-nya. Dalam hal ini, pilih yang tadi sudah terbaca sistem, kemudian klik tombol **Finish**.



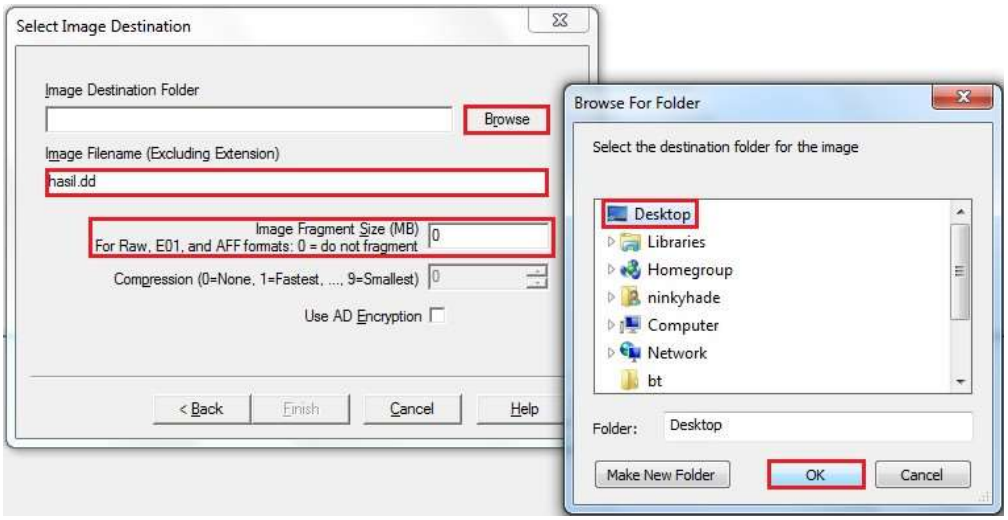
- Atur setting *destination folder* dengan klik tombol **Add**. Lalu pilih format **Raw (dd)** agar hasilnya sama dengan hasil pada praktikum linux yang juga menggunakan format *raw*. Klik tombol **Next**.



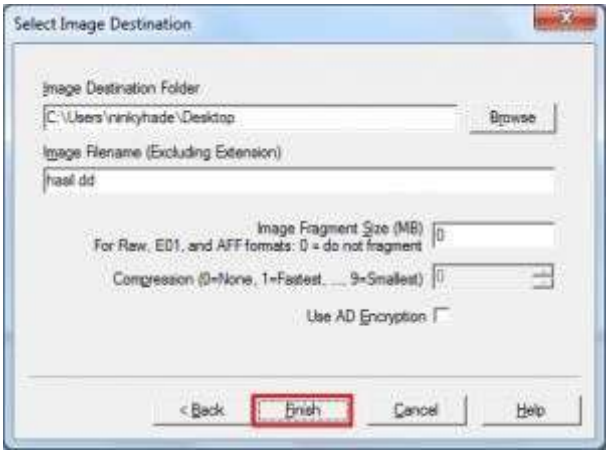
- Isikan informasi tambahan, sesuaikan dengan kondisi praktikan. tombol **Next**.



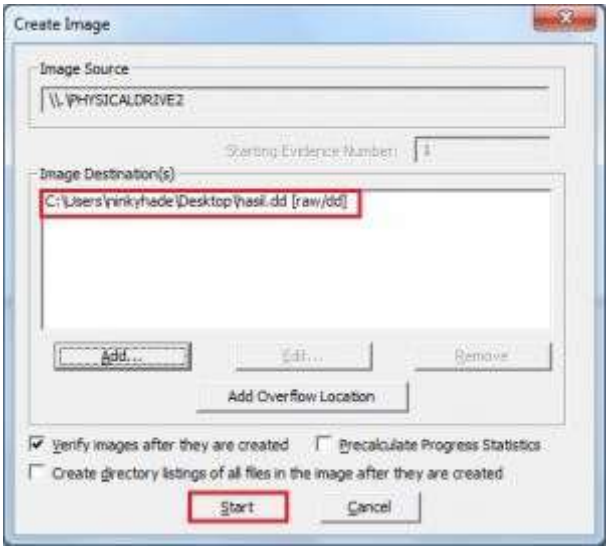
- Pilih *destination folder* dengan klik tombol **Browse**. Dalam hal ini dipilihlah **Desktop** sebagai *destination folder* agar lebih memudahkan Klik tombol **OK** Kemudian isikan nama file *image* berikut ekstensi file-nya. Pada praktikum kali ini, nama file yang digunakan adalah **hasil.dd**. Isikan angka **0** (nol) pada bagian **Image Fragment Size** agar hasil *imaging* tidak dipecah-pecah menjadi beberapa file.



- Klik tombol **Finish**.



- Nanti akan muncul *window* berisi informasi *destination folder*. Klik tombol **Start**.

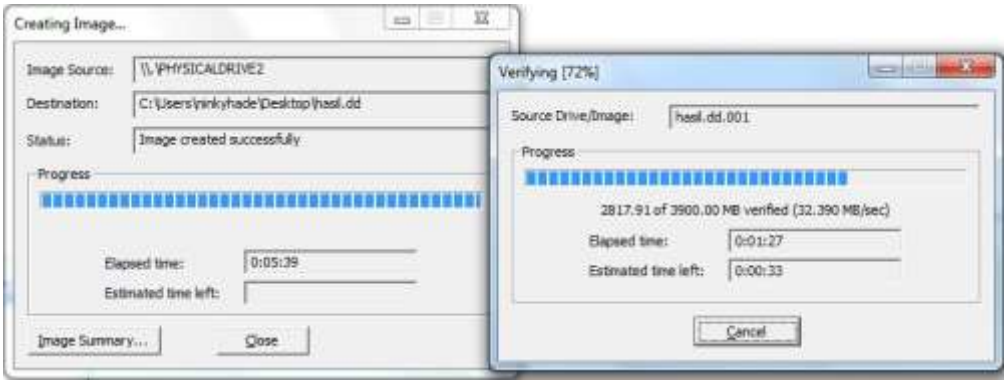


- Tunggu *progress*-nya sampai proses *imaging* selesai.

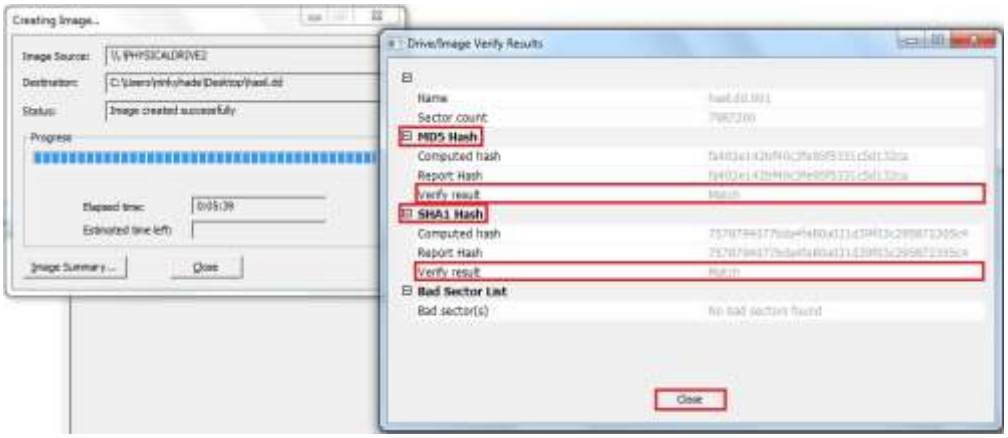


- Setelah selesai proses *imaging*, akan muncul *window* verifikasi (*integrity check*)

file *image* apakah telah sama persis nilai *hash*-nya dengan yang asli.



- Setelah dilakukan verifikasi file, hasil akhirnya akan muncul pada sebuah *window* yang berisi nilai *hash* dan kecocokan nilai *hash* file *image* dengan aslinya. Silakan diamati, jika sudah OK, klik tombol **Close**.



- Setelah itu, akan muncul *window* notifikasi bahwa proses *imaging* telah berhasil. Klik tombol **Close**.

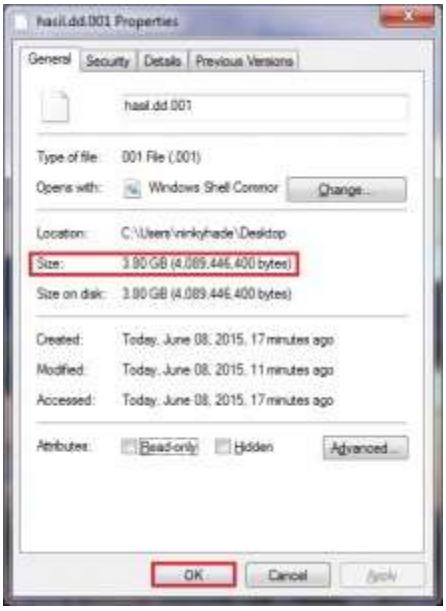


Nah, proses *physical imaging* terhadap flashdisk telah berhasil dilakukan. Sekarang saatnya mengecek file *image*yang tadi sudah di-setting agar *destination folder*-nya ada di Desktop.

- *Minimize* semua *window* untuk menampilkan Desktop.
- Cek file *image* bernama **hasil.dd**. Nanti akan ditemukan 2 file, yaitu 1 file *image* dan 1 file teks (berisi informasi proses *imaging* dan hasil verifikasi/*integrity check*). Pilih file *image*, klik kanan –> **Properties**untuk melihat *size* file *image*-nya.



• Kemudian akan muncul *window* berupa informasi mengenai *size* dari file *image* hasil.dd tersebut. Bandingkan *size* file *image* dengan kapasitas flashdisk yang telah dicek pada awal praktikum ini.



menggunakan aplikasi imaging, cara menggunakan ftk imager, cara mount file dd di ftk imager, download ftk imager terbaru, imaging flasgdisk, imaging flashdisk, praktiktum digital forensik, tutorial menggunakan ftk imager

Praktikum 2
(Digital Imaging) *dd linux Base*

Pretest:

1. Sebutkan definisi dari Digital Imaging!
2. Mengapa perlu dilakukan Digital Imaging pada barang bukti temuan?

Langkah Praktikum:

Seperti telah diketahui bersama, bahwa cara untuk mendapatkan bukti digital adalah dengan melakukan akuisisi barang bukti elektronik. **Akuisisi** yang dimaksud adalah dengan mengidentifikasi, mengumpulkan, membuat *image*(*imaging*) atau menyalin (*cloning*/*copy bit by bit*), dan mengamankan barang bukti elektronik.

Untuk proses *imaging* sendiri dapat dilakukan dengan 2 cara:

1. *Physical*
Membuat *image* disk secara utuh. Dilakukan apabila terindikasi ada folder/file yang telah dihapus, sehingga membutuhkan *recovery* file.
2. *Logical*
Hanya membuat *image* pada partisinya saja.
Pada postingan kali ini akan dibahas mengenai cara untuk melakukan ***physical imaging*** sebuah **flashdisk**menggunakan *command* Linux. Distro Linux yang digunakan pada praktikum kali ini adalah **Kali Linux**.

<u>Langkah-langkah:</u>

1. Tancapkan flashdisk ke komputer.

2. Cek apakah flashdisk sudah terbaca oleh sistem Linux. Cari baris yang mengandung "/dev/sd…"

 # fdisk -l
/dev/sdb …

3. Lakukan proses *imaging* terhadap flashdisk dan langsung lakukan *hashing*. ***Hashing*** adalah metode untuk melakukan ***integrity check***, yaitu membandingkan hasil *imaging* apakah sama persis dengan aslinya.

 # dc3dd if=/dev/sdb of=/root/Desktop/hasil.dd hash=md5

Keterangan :

- *if=/dev/sdb –> media input adalah **/dev/sdb** di mana flashdisk ditancapkan*
- *of=/root/Desktop/hasil.dd –> hasil imaging diletakkan di direktori **/root/Desktop**dengan nama file-nya adalah **hasil.dd** (format raw)*
- *hash=md5 –> algoritma hashing yang digunakan adalah **MD5***

Cara lain menggunakan DD
 # sudo dd if=/dev/sdb of=/root/Desktop/hasil.dd bs=512

Keterangan :

- **sudo -> menjalankan perintah dengan permission ROOT**
- **if=/dev/sdb -> media input /dev/sdb dimana flashdisk ditancapkan**
- **of=/root/Desktop/hasil.dd -> hasil imaging diletakan di direktori /root/Desktop/ dengan nama file hasil.dd**
- **bs=512 -> adalah bytes yang ada pada flashdisk**

4. Tunggu sampai selesai. Output di layar akan memberitahukan bahwa proses *imaging* telah berhasil dan menampilkan nilai *hash* MD5-nya.

c105a26e214939091239f949fd0c9aba (md5)

5. Lakukan *integrity check*.

 # md5sum /dev/sdb
c105a26e214939091239f949fd0c9aba (/dev/sdb)

atau:

 # md5sum /root/Desktop/hasil.dd
c105a26e214939091239f949fd0c9aba (/root/Desktop/hasil.dd)

6. Cocokkan nilai *hash* MD5 pada md5sum dengan nilai *hash* MD5 pada proses *imaging*. Jika sama, maka hasil*imaging* sudah OK.

Demikian praktikum kali ini. Sampai jumpa insya Allah di praktikum-praktikum selanjutnya ☺

Praktikum 3
Explore Investigasi File .DD

Pretest:

1. Apa itu Autopsy dalam pengertian umum?
2. Sebutkan kegunaan tool investigasi Autopsy kaitannya dalam mengolah barang bukti digital!
3. Download image pada *bit.ly/evidence03dd* !

Langkah Praktikum:

Pembahasan kali ini sebenarnya merupakan pembahasan dari forensicscontest.com. dengan menganalisis sebuah file *image* berekstensi .dd dan diminta untuk menjawab 4 pertanyaan (*challenge*) yang ada, jawaban dari keempat *challenge* tersebut akan ditemukan jika sudah berhasil menganalisis file *image* berekstensi .dd tersebut.

WHAT TO DO?

File *raw image* yang dimaksud adalah file bernama "**quarter-SDHC-snippet.dd**". File ini akan coba dibuka dengan program Autopsy yang merupakan bawaan dari OS Kali Linux. Mungkin saja akan ditemukan file-file yang telah dihapus, jika ini terjadi maka akan dibutuhkan proses *recovery* file.

Asumsi:

File "**quarter-SDHC-snippet.dd**" berada di folder **/root/Desktop**.

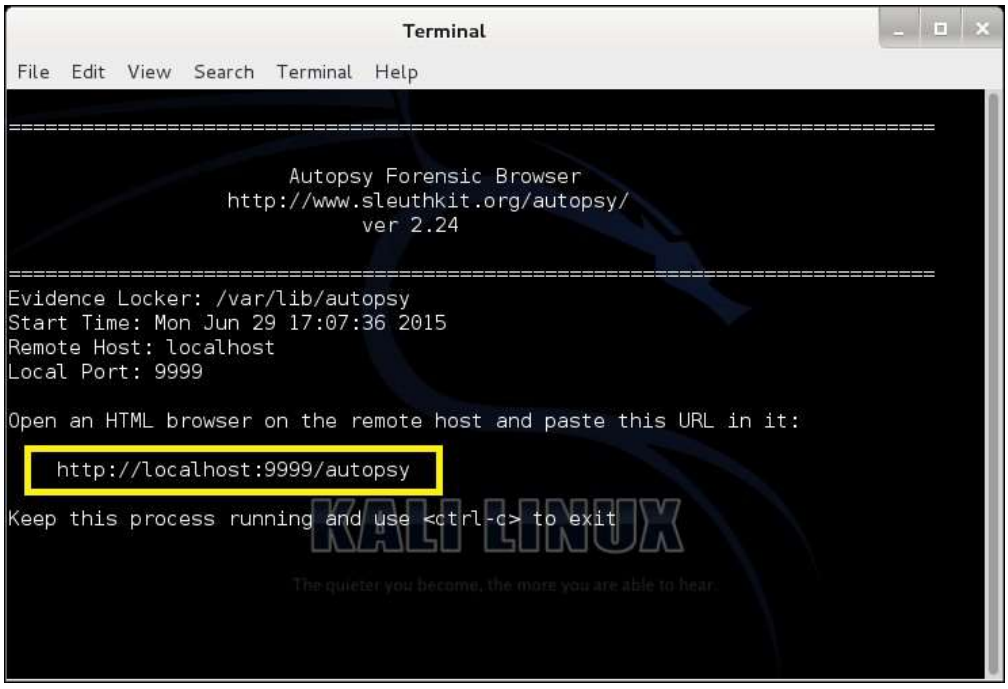
CHALLENGE

1. *In his conversation with juniorkeyy, how old does Larry initially say he is?*
2. *What was the filename of the file that had the following SHA256 sum?*
3. *What is the SHA256sum of the photo from the "dd" image that shows Larry taking a bite out of a wireless router?*
4. *What is the SHA256sum of the image that shows zombie Larry taking a bite out of a cat?*

LANGKAH-LANGKAH

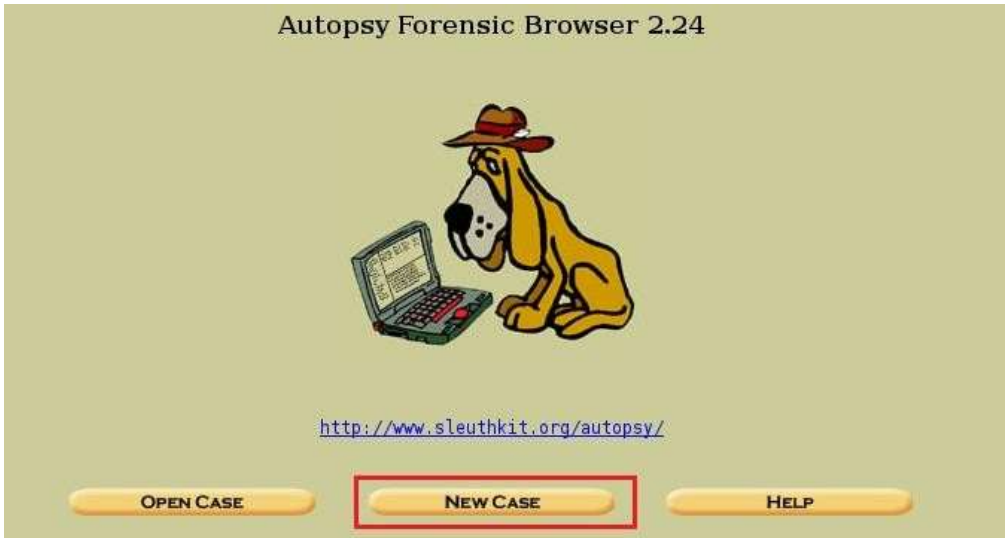
1. Buka program **Autopsy** dari menu **Applications** –> **Kali Linux** –> **Forensics** –> **Forensic Suites** –> **Autopsy**

Akan muncul terminal sebagai berikut:



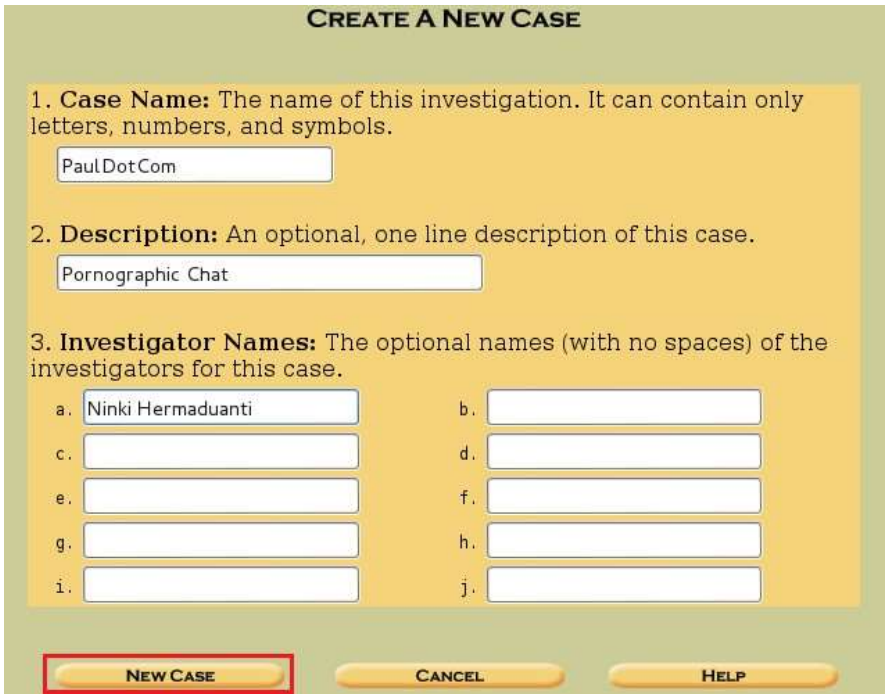
- Buka *address* **http://localhost:9999/autopsy** menggunakan *web browser*.
- **INGAT!!!** Selama program Autopsy dijalankan, jangan *close* terminal tersebut.
- Semua file yang digunakan oleh kasus dalam program Autopsy ini akan disimpan di ***Evidence Locker***dengan *path*-nya adalah **/var/lib/autopsy**.

2. Tambahkan kasus baru dengan cara klik tombol **Add Case**.



Isikan informasi sebagai berikut (seusaikan dengan kondisi Anda):

- *Case Name* : PaulDotCom
- *Description* : *Pornographic Chat*
- *Investigator Name* : Ninki Hermaduanti



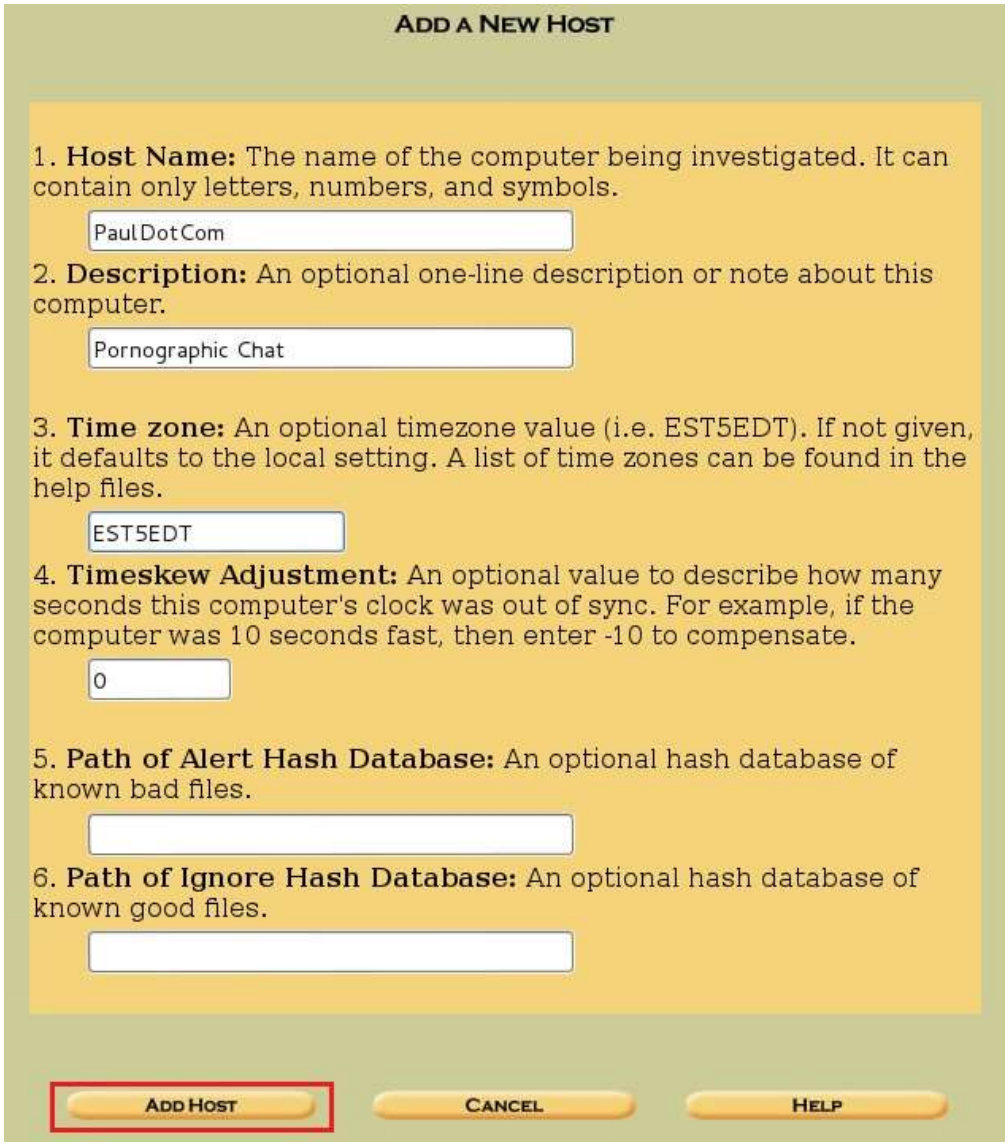
Jika sudah, klik tombol **New Case**. Maka folder **PaulDotcom** akan otomatis ditambahkan ke dalam folder **/var/lib/autopsy**, sehingga *path* lengkapnya adalah di **/var/lib/autopsy/PaulDotCom**.

3. Langkah selanjutnya adalah menambahkan *host* untuk kasus PaulDotCom ini. Klik pada tombol **Add Host.**



Lalu isikan informasi sebagai berikut:

- *Host Name* : PaulDotCom
- *Description* : *Pornographic Chat*
- *Timezone* : EST5EDT



Field yang lain biarkan *default*. Untuk bantuan pemilihan *timezone*, dapat dilihat pada halaman HELP dari program Autopsy ini.

Jika sudah, klik tombol **Add Host**. *Host* bernama **PaulDotCom** akan ditempatkan pada *case folder***/var/lib/autopsy/PaulDotCom**, sehingga path lengkapnya akan menjadi **/var/lib/autopsy/PaulDotCom/PaulDotCom**.

4. Tambahkan file *raw image* **quarter-SDHC-snippet.dd** yang akan dianalisis. File ini berada di folder **/root/Desktop**. Klik tombol **Add Image** lalu klik tombol **Add Image File**.



Dan isikan informasi sebagai berikut:

- *Location* : /root/Desktop/quarter-SDHC-snippet.dd
- *Type* : *Disk*
- *Import Method* : *Move*



Untuk mengecek *Type* yang akan digunakan, jalankan perintah di terminal Linux sebagai berikut:

root@kali:~# file /root/Desktop/quarter-SDHC-snippet.dd

quarter-SDHC-snippet.dd: x86 boot sector; partition 1: ID=0xb, starthead 2, startsector 8192, 7618560 sectors, extended partition table (last)\011, code offset 0x0

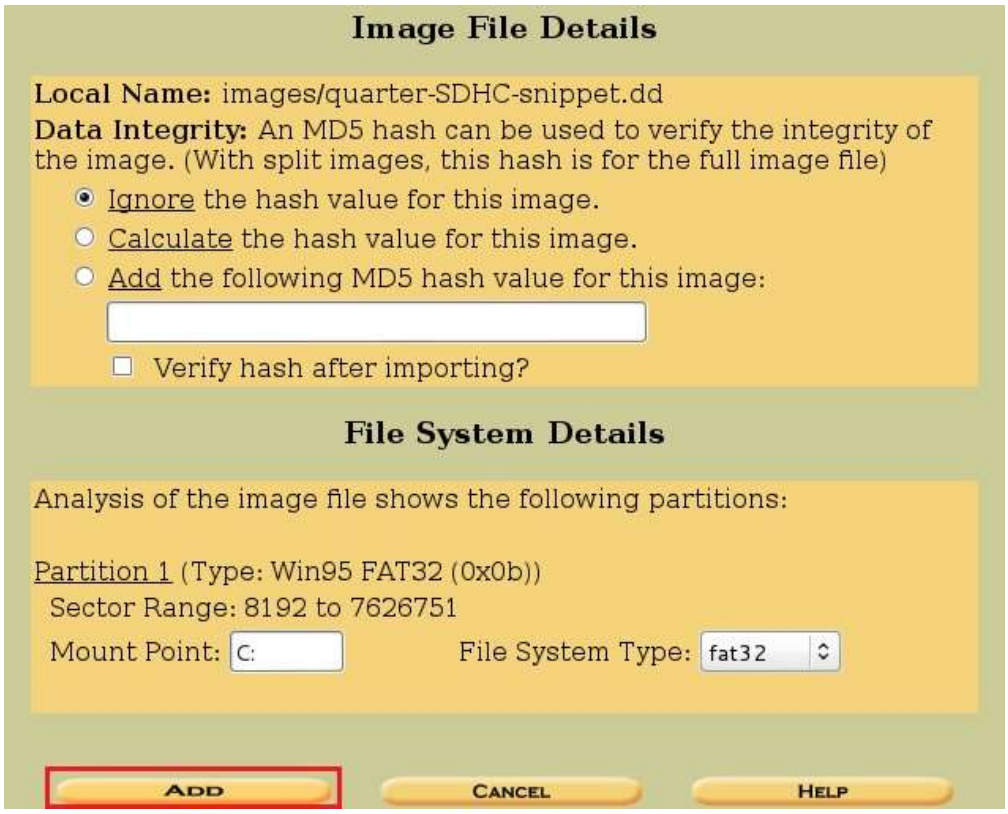
Jika ada lebih dari 1 partisi, maka gunakan *Type*: *Disk*.

Untuk penjelasan *Import Method* adalah sebagai berikut:

- ***Symlink*** : untuk menghemat *space*, maka dibuatlah *symbolic link* (*shortcut*) dengan tidak memindahkan file *image* yang asli ke dalam *Evidence Locker*
- **Copy** : melakukan *copy* terhadap file *image* asli ke dalam *Evidence Locker*
- ***Move*** : untuk menghemat *space* dan juga memindahkan file *image* ke dalam *Evidence Locker* (*cut* file *image*)

Jika sudah, klik tombol **Next**.

5. Tambahkan detail dari file *image* dengan mengisikan informasi sebagai berikut:
   - *Data Integrity* : *Ignore*

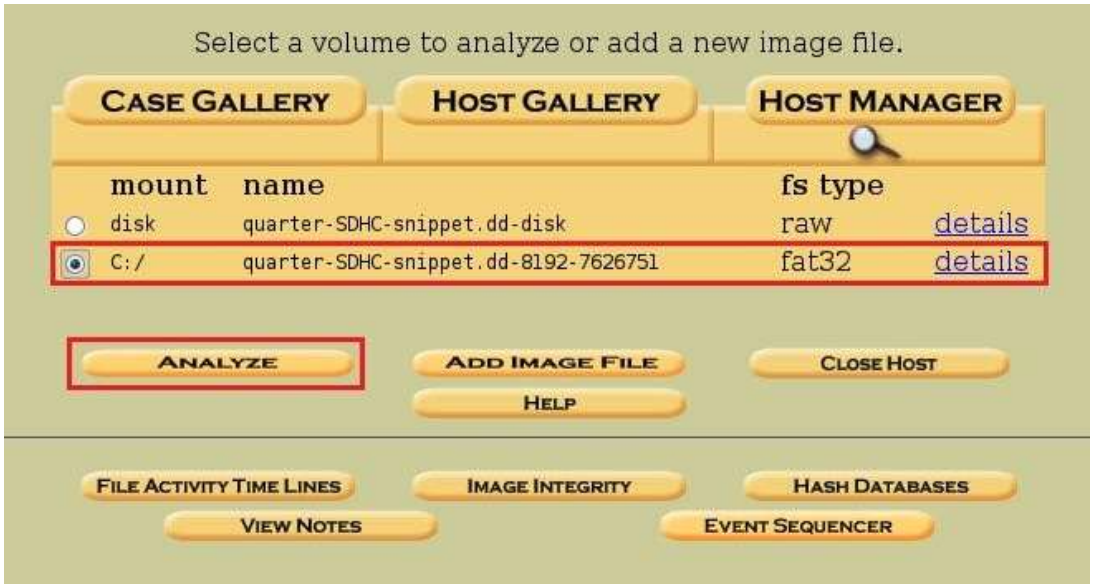


Opsi *Ignore* dipilih karena Autopsy hanya support MD5 *hash*, sedangkan file *raw image* yang dianalisis menggunakan SHA256 *hash*.
Field lain dibiarkan *default*, kemudian klik tombol **Add**. Pada halaman konfirmasi, klik tombol **OK**.



File *image* di dalam *Evidence Locker* pada kasus ini, akan diletakkan di folder **/var/lib/autopsy/PaulDotCom/PaulDotCom/images**.

6. Untuk *file system*, pilih **FAT32** dan klik tombol **Analyze**.



7. Klik pada tab **File Analysis**, maka akan muncul semua file yang ada di dalam *image* **quarter-SDHC-snippet.dd**.



8. *Scroll* ke bawah pada panel *evidence item*, maka akan ditemukan file-file yang bertuliskan warna merah.



File-file ini merupakan file yang sudah dihapus (*deleted files*), sehingga untuk menganalisisnya akan dibutuhkan proses *recovery*.

9. *Recovery* file pada Kali Linux dapat dilakukan dengan 2 cara melalui *command* di terminal Linux. Cara tersebut adalah:
   - **foremost** : dapat memisahkan file ter-*recover* sesuai dengan tipenya
   - **photorec** : file ter-*recover* tidak dipisahkan sesuai tipenya

   Untuk mempermudah, maka yang akan digunakan adalah *command* **foremost**. Jalankan perintah berikut di terminal Linux.

```
root@kali:~# cd /var/lib/autopsy/PaulDotCom/PaulDotCom/
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom# ls -l
total 24
-rw-r–r– 1 root root  271 Jun 29 17:28 host.aut
drwxr-xr-x 2 root root 4096 Jun 29 17:28 images
drwxr-xr-x 2 root root 4096 Jun 29 17:27 logs
drwxr-xr-x 2 root root 4096 Jun 29 17:19 mnt
drwxr-xr-x 4 root root 4096 Jun 29 17:36 output
drwxr-xr-x 2 root root 4096 Jun 29 17:19 reports
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom# ls -l images/
total 26624
-rw-r–r– 1 root root 27262976 Jun 29 17:27 quarter-SDHC-snippet.dd
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom#     foremost
images/quarter-SDHC-snippet.dd
Processing: images/quarter-SDHC-snippet.dd
|*|
```

Semua file ter-*recover* dari *command* **foremost** akan diletakkan di folder **/var/lib/autopsy/PaulDotCom/PaulDotCom/output**.

```
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom# ls -l output/
total 12
-rw-r–r– 1 root root 1328 Jun 29 17:36 audit.txt
drwxr-xr– 2 root root 4096 Jun 29 17:36 jpg
drwxr-xr– 2 root root 4096 Jun 29 17:36 mov
```

Dapat terlihat bahwa file ter-*recover* diletakkan ke dalam 2 folder berbeda sesuai tipenya, yaitu file JPG dan file *movie*.

```
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom# ls -l output/jpg/
total 7728
-rw-r–r– 1 root root   28083 Jun 29 17:36 00026304.jpg
-rw-r–r– 1 root root 2005871 Jun 29 17:36 00026368.jpg
-rw-r–r– 1 root root  212411 Jun 29 17:36 00030336.jpg
-rw-r–r– 1 root root   31660 Jun 29 17:36 00030784.jpg
-rw-r–r– 1 root root  127671 Jun 29 17:36 00030848.jpg
-rw-r–r– 1 root root   97676 Jun 29 17:36 00031104.jpg
-rw-r–r– 1 root root 3873991 Jun 29 17:36 00031296.jpg
-rw-r–r– 1 root root  116985 Jun 29 17:36 00038912.jpg
-rw-r–r– 1 root root   71619 Jun 29 17:36 00039168.jpg
-rw-r–r– 1 root root  103338 Jun 29 17:36 00039360.jpg
-rw-r–r– 1 root root  105202 Jun 29 17:36 00039616.jpg
-rw-r–r– 1 root root 1121475 Jun 29 17:36 00050880.jpg
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom# ls -l output/mov/
total 10236
-rw-r–r– 1 root root 4858802 Jun 29 17:36 00016768.mov
-rw-r–r– 1 root root 5617411 Jun 29 17:36 00039872.mov
```

INGAT!!!

Yang perlu diperhatikan dari recovery file ini adalah, ***file tidak di-recover dengan nama aslinya****. Sehingga dalam proses pengecekan nanti untuk menjawab challenge yang ada, perlu dicocokkan antara gambar dari file ter-recover dan gambar dari file aslinya.*

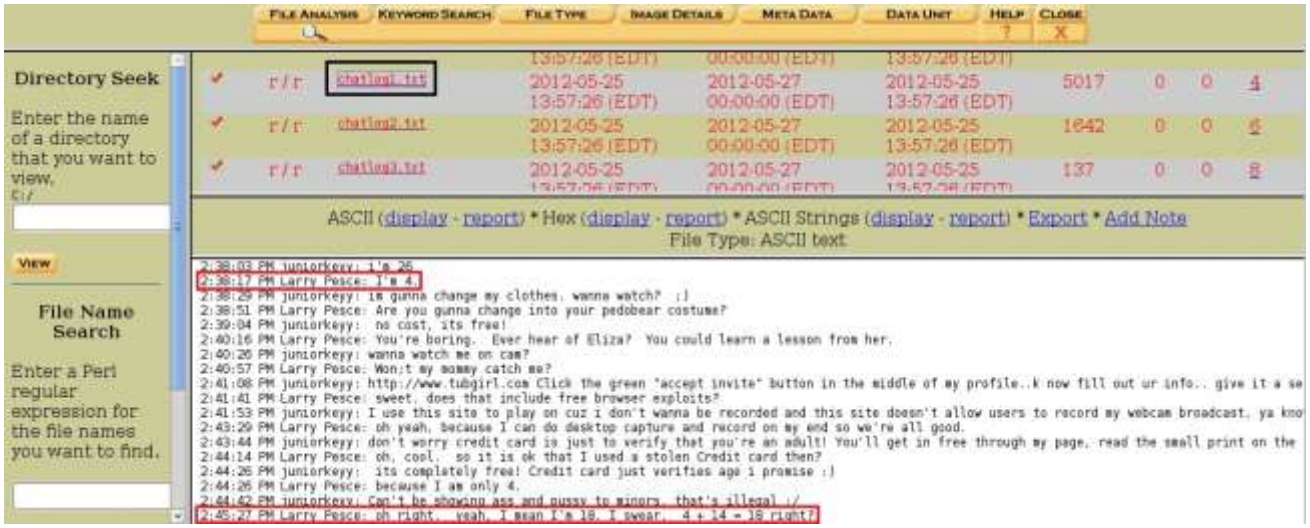
*Yang menjadi **masalah** adalah **jika file-nya berjumlah ratusan bahkan ribuan**, maka diperlukan waktu yang cukup banyak untuk mencocokkan gambar file ter-recover dengan gambar file aslinya.*

10. Untuk menjawab *challenge* nomor 2,3, dan 4 maka diperlukan pengecekan nilai *hash* dengan algoritma SHA256. Jalankan perintah berikut di terminal Linux.

```
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom# cd output/jpg/
root@kali:/var/lib/autopsy/PaulDotCom/PaulDotCom/output/jpg# sha256sum *
fc4fec579db37ffaec516be4cfff1a669fba3a3cbf09f6706a8328b766ed729a  00026304.jpg
a51649b8f2af41f71c6bf22b30e0691bf104a3d7014977f38ecc7c80699ab690  00026368.jpg
e4e2fac9fc41546239d4e534bfe6588e4796f3799befc09b2787f5ad6c75faca  00030336.jpg
1bdfd9d7445d38fdb7ba5acbb58669cf31c7c568c7aa6e6fcf0c961628f4c32e  00030784.jpg
67788573a013ce0e59400800ddd765132a44fdf5ba3931f3295dc76cc28b8adf  00030848.jpg
9c0a8bc6c3baa2ad7f390ef4e41c3edf3d98a543f492afb50a4bab8700af5766  00031104.jpg
8c1c8e97a8a37b6b7b6942bd17a3eb5ecae79e315cc04f7e857c011f3e4dca28  00031296.jpg
dd244a31908037d439c2095391b3f46a1820059c91af31369b5f6c4522e8fa3d  00038912.jpg
0f5ac5eff6aeda2eeef8dec60d588d28899959a31d27e9a5c24d65accc5f18ca  00039168.jpg
c08af53ce151fd454dcfc642b81406f57aec522ad9cfc44dcb921d5be26d60b6  00039360.jpg
e56931935bc60ac4c994eabd89b003a7ae221d941f1b026b05a7947a48dc9366  00039616.jpg
6b55985144d6535b192b5b4a679b116ce7e48cc91e9f96909d4a721ade218c21  00050880.jpg
```

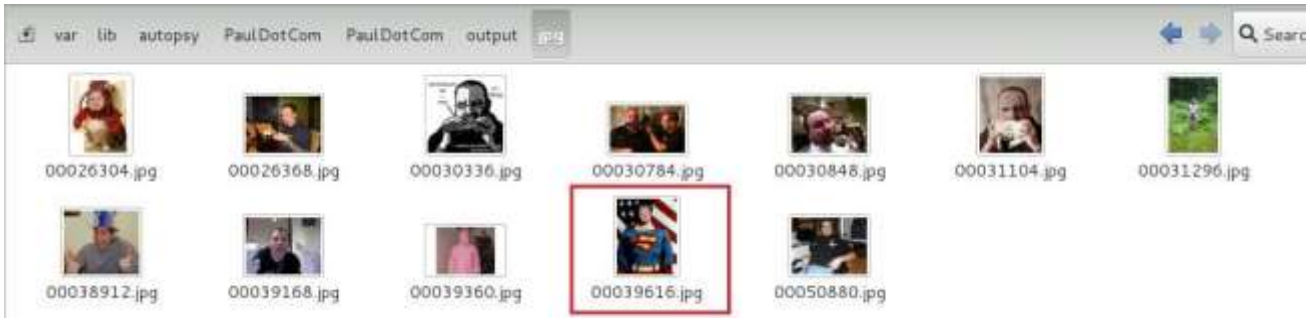
JAWABAN *CHALLENGE*

1. *In his conversation with juniorkeyy, how old does Larry initially say he is?*
Asumsinya jika disebut *conversation*, maka yang dicek adalah log dari percakapan yang ada. Cek file *chatlog* untuk mengetahui jawaban dari *challenge* tersebut. Dimulai dari file **chatlog1.txt**. Ditemukan *evidence* sebagai berikut:



Jawabannya adalah **4 tahun** karena yang ditanyakan adalah "*initially*" yang berarti "pada awalnya".

2. *What was the filename of the file that had the following SHA256 sum:*e56931935bc60ac4c994eabd89b003a7ae221d941f1b026b05a7947a48dc9366
Cocokkan dengan hasil sha256sum yang telah dijalankan di terminal Linux. Maka ditemukan nama file "**00039616.jpg**" (file ter-*recover*). Kemudian buka folder **/var/lib/autopsy/PaulDotCom/PaulDotCom/output/jpg**melalui *explorer* unt uk melihat gambarnya.



Setelah ditemukan, cocokkan gambarnya dengan gambar file aslinya. Klik 1 per 1 gambar JPG pada program Autopsy sampai ditemukan gambar yang sama sebagai berikut:



Jawabannya adalah "**superstrand.jpg**".

3. *What is the SHA256sum of the photo from the "dd" image that shows Larry taking a bite out of a wireless router?*

Cek 1 per 1 gambar JPG yang ada pada program Autopsy, cari gambar Larry yang sedang menggigit sebuah *wireless router*.





Ditemukan 2 file yaitu "**haxorthematrix-has-a-posse.jpg**" dan "**larryeatswrt.jpg**". Kedua file ini kemudian dicocokkan dengan nama file ter-*recover* pada folder **/var/lib/autopsy/PaulDotCom/PaulDotCom/output/jpg**, maka ditemukan nama file:

- "**00030336.jpg**" untuk file "**haxorthematrix-has-a-posse.jpg**"
- "**00030784.jpg**" untuk file "**larryeatswrt.jpg**"



Kemudian cek nilai *hash* SHA256-nya untuk file "**00030336.jpg**" dan file "**00030784.jpg**".
Jawabannya adalah:

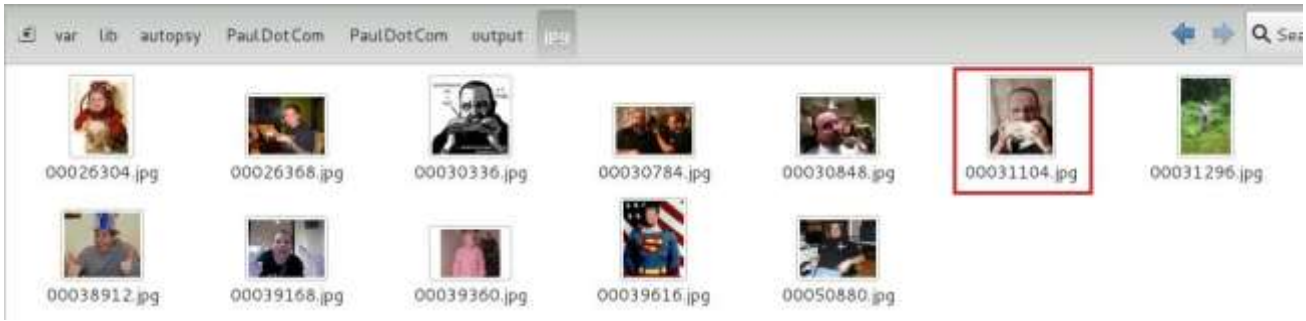
- **e4e2fac9fc41546239d4e534bfe6588e4796f3799befc09b2787f5ad6c75faca** (0003 0336.jpg)
- **1bdfd9d7445d38fdb7ba5acbb58669cf31c7c568c7aa6e6fcf0c961628f4c32e** (000 30784.jpg)

4. *What is the SHA256sum of the image that shows zombie Larry taking a bite out of a cat?*

Langkah yang dilakukan sama dengan nomor 3. Cek 1 per 1 gambar JPG yang ada pada program Autopsy, cari gambar Larry yang sedang menggigit seekor kucing.



Ditemukan 1 file yaitu "**Larry_zombie_cat.jpg**". File ini kemudian dicocokkan dengan nama file ter-*recover* pada folder **/var/lib/autopsy/PaulDotCom/PaulDotCom/output/jpg**, maka ditemukan nama file "**00031104.jpg**".



Kemudian cek nilai *hash* SHA256-nya untuk file "00031104.jpg".
Jawabannya adalah:

- **9c0a8bc6c3baa2ad7f390ef4e41c3edf3d98a543f492afb50a4bab8700af5766** (00031104.jpg)

Demikian jawaban *challenge* dari nomor 1-4. Sebenarnya masih ada lanjutan *challenge*-nya sih.. Tetapi yang buat UTS itu saja. Jadi, sekian dulu yaa… Oiya, ada sedikit tips nih..

TIPS!!!

Kalau misal ditemukan kendala dalam melihat konten file *evidence* di Autopsy, seperti misalnya sudah klik file "**chatlog1.txt**" atau "**Larry_zombie_cat.jpg**", namun tidak muncul apa-apa, bahkan ada *warning* "**File Type: no read permission**", silakan lakukan langkah berikut.

1. Cek log di terminal Autopsy yang sedang *running* (itu lho, terminal yang berjalan ketika program Autopsy dibuka dan gak boleh di-*close* selama program Autopsy *running*).
2. Apabila ditemukan kata-kata "**sh: 1: /usr/bin/icat-sleuthkit: not found**", maka lakukan langkah seperti yang disebutkan di web bugs.kali.org, yaitu menjalankan perintah berikut di terminal Linux:

root@kali:~# ln -s /usr/bin/icat /usr/bin/icat-sleuthkit

*Hal ini dikarenakan command yang digunakan untuk melihat konten file evidence dalam program Autopsy adalah "**icat-sleuthkit**", sementara yang diinstall di Kali Linux adalah command "**icat**" yang ada di folder **/usr/bin**. Jadi, perlu dibuatkan symbolic link (shortcut) untuk menghubungkan command **/usr/bin/icat** ke **/usr/bin/icat-sleuthkit**.*

This will do the trick

Praktikum 4
Wireshark

Pretest:

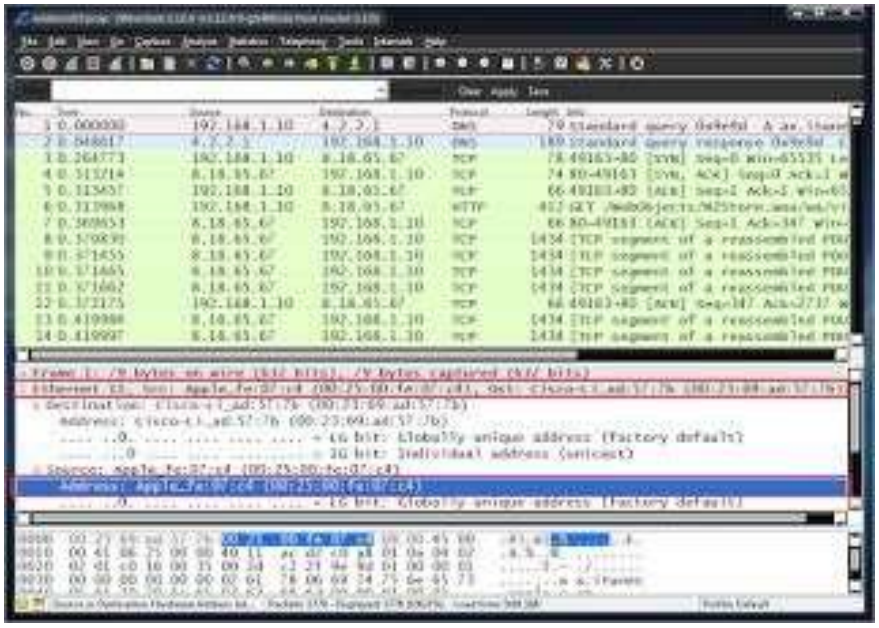
1. Apa itu Wireshark?
2. Sebutkan Fungsi-Fungsi dari Wireshark!
3. Download capture an wireshark pada *bit.ly/evidence04pcap* !

Langkah Praktikum:

1. What is the MAC address of Ann's AppleTV?

Untuk menjawabnya, kita dapat melakukan langkah-langkah berikut :

Diketahui Ann merupakan *source* yang memiliki IP address 192.168.1.10, maka kita dapat melihat detail dari *header* frame pertama file tersebut, dari jendela detail frame tersebut kita dapat merujuk pada *Ethernet II, Src: Apple_fe:07:c4 (**00:25:00:fe:07:c4**), Dst: Cisco-Li_ad:57:7b (00:23:69:ad:57:7b)*, secara detail kita dapat melihat *address* dari *source: Address: Apple_fe :07:c4 (00:25:00:fe:07c4)*

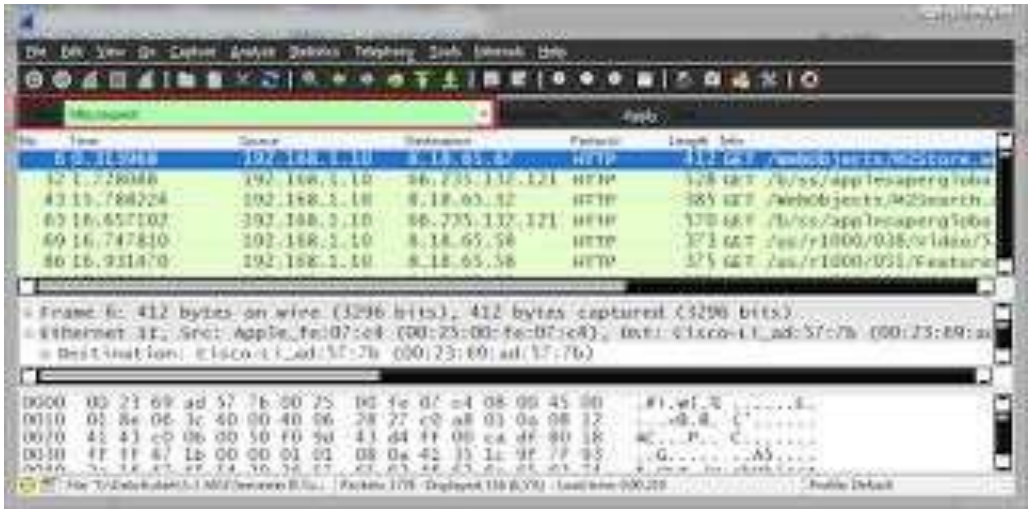


Dari penjelasan poin a diatas maka jawaban dari pertanyaan *What is the MAC address of Ann's AppleTV* adalah ***00:25:00:fe:07:c4***.

2. What User-Agent string did Ann's AppleTV use in HTTP requests?

Untuk menjawabnya, kita dapat melakukan langkah-langkah berikut :

a. Pertama-tama kita harus menemukan frame-frame mana yang dilakukan *HTTP requests* yaitu dengan mengetik perintah *http.request* pada kotak *Filter* kemudian tekan tombol *Enter* pada*keyboard*, sehingga akan ditemukan deretan frame yang dilakukan *HTTP requests*, seperti pada gambar berikut :



b. Langkah selanjutnya menemukan *string User-Agent* dari Ann yaitu dengan menggunakan perintah *Find Packet* caranya adalah klik menu *Edit* kemudian klik *Find Packet* atau dengan menekan tombol kombinasi Ctrl + F secara bersamaan.

Selanjutnya pada jendela *Find Packet* atur seperti berikut :

a. Pada pada perintah *Find* klik/ceklis perintah *String*
b. Pada perintah *Filter* ketik User-Agent
c. Pada perintah *Search In* klik/ceklis *Packet details*
d. Selanjutnya klik perintah Find, perhatikan gambar berikut :

c. Setelah melakukan perintah diatas maka secara otomatis akan tampil string dari User-Agent yang dicari, perhatikan gambar berikut :

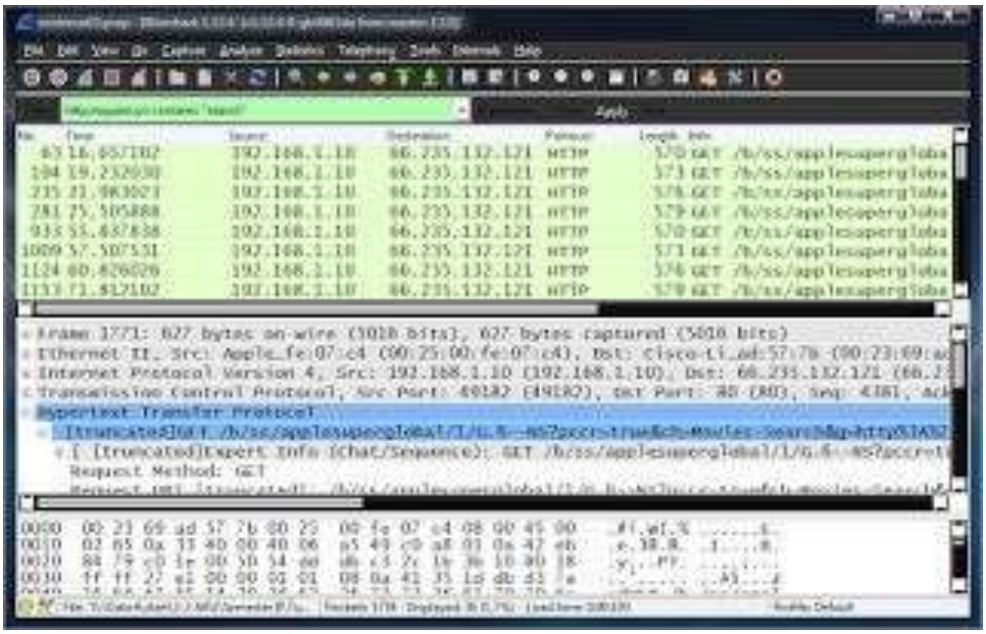


Berdasarkan gambar diatas maka dapat dilihat pada detail *Hypertext Transfer Protocol* terdapat string *User-Agent* dari Ann yaitu AppleTV/2.4. Jadi jawaban dari pertanyaan *what User-Agent string did Ann's AppleTV use in HTTP requests* adalah ***AppleTV/2.4***.

3. What were Ann's first four search terms on the AppleTV (all incremental searches count)?

Untuk menjawabnya, kita dapat melakukan langkah-langkah berikut :

Pertama-tama kita harus menemukan frame-frame mana yang dilakukan *search terms* yaitu dengan mengetik perintah *http.request.uri contains "search"* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame yang dilakukan *search*, seperti pada gambar berikut :



Dari gambar diatas terdapat 30 frame yang melakukan *search*, dari pertanyaan diatas ditanyakan empat istilah pertama yang dicari oleh Ann, maka untuk menemukan jawabannya adalah dengan cara berikut :

Diketahui *frame* pertama yang melakukan perintah *search* adalah *frame* ke 63, maka untuk mencari empat istilah pertama yang dilakukan oleh Ann Apple TV adalah :

a. Aktifkan *frame* ke 63 yaitu *frame* pertama dari gambar diatas, kemudian klik menu *Analyze*kemudian klik *Follow TCP Stream*.
b. Dari perintah *Follow TCP Stream* diatas maka akan tampil jendela *Stream Content* dalam bentuk bentuk *Raw*. Dari *Stream Content* tersebut kita dapat melihat *detail search* yang dilakukan oleh Ann serta balasan dari *server destination*, maka keempat istilah yang pertama dicari oleh Ann adalah :

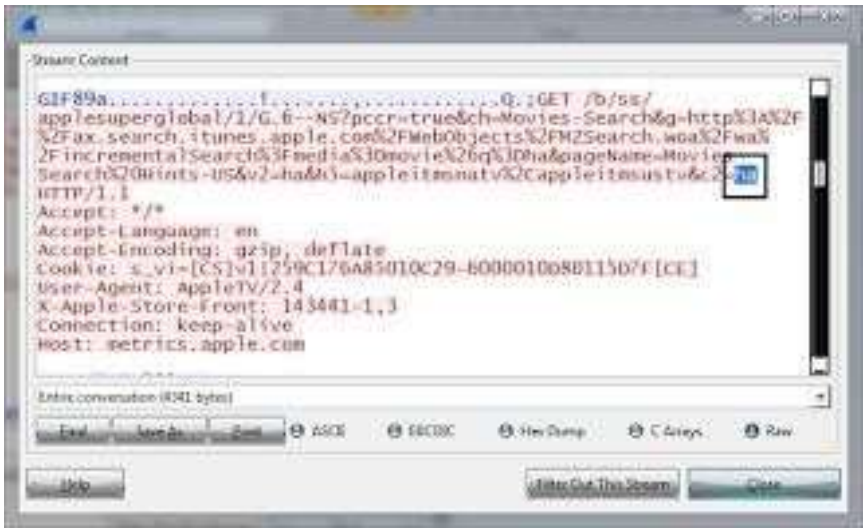
1. Pada alamat URI yaitu :
   */b/ss/applesuperglobal/1/G.6--NS?pccr=true&ch=Movies-Search&g=http%3A%2F%2Fax.search.itunes.apple.com%2FWebObjects%2FMZSearch.woa%2Fwa%2FincrementalSearch%3Fmedia%3Dmovie%26q%3Dh&pageName=Movies-Search%20Hints-US&v2=h&h5=appleitmsnatv%2Cappleitmsustv&c2=**h**,*

kita dapat melihat istilah yang diakses oleh Ann adalah huruf ***h***. Perhatikan huruf ***h*** yang di blok dan di beri kotak hitam dari gambar berikut :



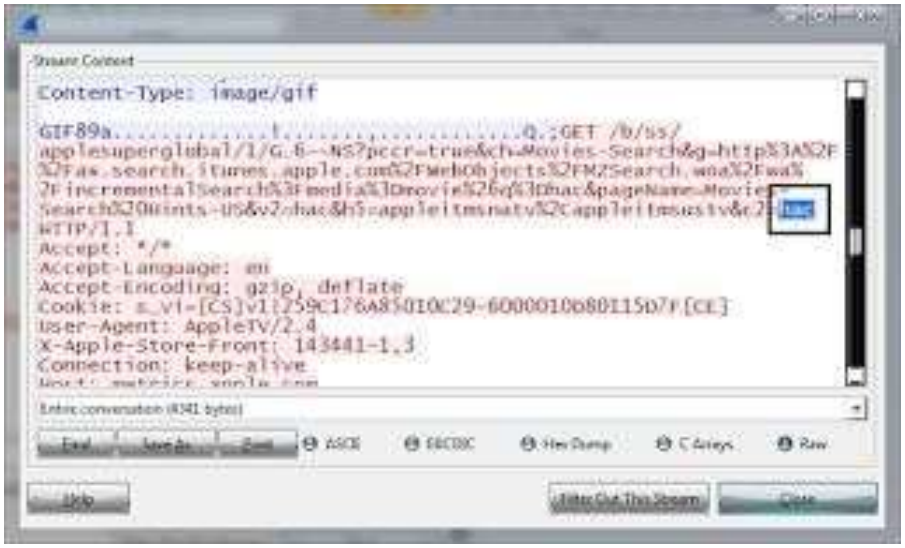
2. Pada alamat URI yaitu :
   */b/ss/applesuperglobal/1/G.6--NS?pccr=true&ch=Movies-Search&g=http%3A%2F%2Fax.search.itunes.apple.com%2FWebObjects%2FMZSearch.woa%2Fwa%2FincrementalSearch%3Fmedia%3Dmovie%26q%3Dha&pageName=Movies-Search%20Hints-US&v2=ha&h5=appleitmsnatv%2Cappleitmsustv&c2=**ha**,*

kita dapat melihat istilah yang diakses oleh Ann adalah huruf ***ha***. Perhatikan huruf ***ha*** yang di blok dan di beri kotak hitam dari gambar berikut :



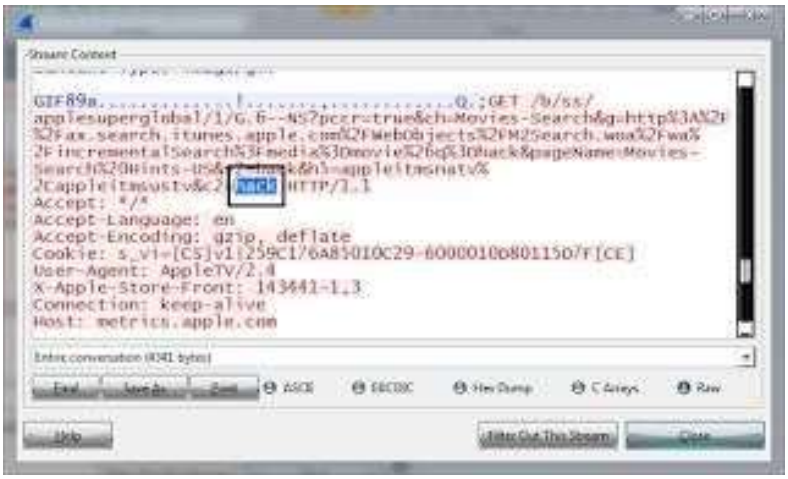
3. Pada alamat URI yaitu :
   */b/ss/applesuperglobal/1/G.6--NS?pccr=true&ch=Movies-Search&g=http%3A%2F%2Fax.search.itunes.apple.com%2FWebObjects%2FMZSearch.woa%2Fwa%2FincrementalSearch%3Fmedia%3Dmovie%26q%3Dhac&pageName=Movies-Search%20Hints-US&v2=hac&h5=appleitmsnatv%2Cappleitmsustv&c2=**hac**,*

kita dapat melihat istilah yang diakses oleh Ann adalah huruf ***hac***. Perhatikan huruf ***hac*** yang di blok dan di beri kotak hitam dari gambar berikut :



4. Pada alamat URI yaitu :
   */b/ss/applesuperglobal/1/G.6--NS?pccr=true&ch=Movies-Search&g=http%3A%2F%2Fax.search.itunes.apple.com%2FWebObjects%2FMZSearch.woa%2Fwa%2FincrementalSearch%3Fmedia%3Dmovie%26q%3Dhack&pageName=Movies-Search%20Hints-US&v2=hack&h5=appleitmsnatv%2Cappleitmsustv&c2=**hack**,*

kita dapat melihat istilah yang diakses oleh Ann adalah huruf ***hack***. Perhatikan huruf ***hack***yang di blok dan di beri kotak hitam dari gambar berikut :



Berdasarkan penjelasan point b diatas maka jawaban pertanyaan dari *What were Ann's first four search terms on the AppleTV (all incremental searches count)* adalah ***h, ha, hac,*** dan ***hack****.*

4. What was the title of the first movie Ann clicked on?

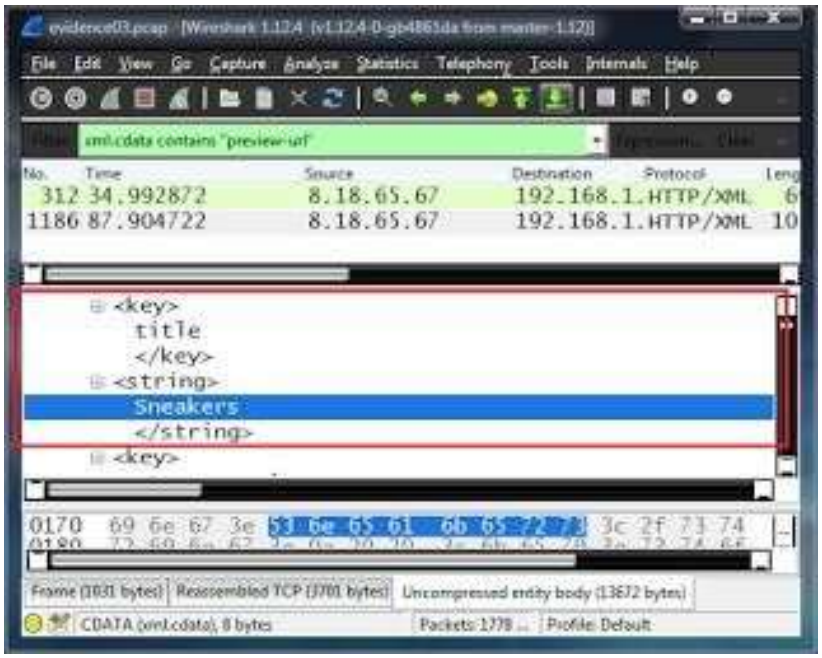
Untuk menjawabnya, kita dapat melakukan langkah-langkah berikut :

a. Pertama-tama kita harus menemukan frame-frame mana yang memiliki *preview-url* yaitu dengan mengetik perintah *xml.cdata contains "preview-url"* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame, seperti pada gambar berikut:



b. klik menu *Edit* kemudian klik *Find Packet* atau dengan menekan tombol kombinasi Ctrl + F secara bersamaan, selanjutnya pada jendela *Find Packet* atur seperti berikut:

1. Pada pada perintah *Find* klik/ceklis perintah *String*
2. Pada perintah *Filter* ketik *title*
3. Pada perintah *Search In* klik/ceklis *Packet details*
4. Selanjutnya klik perintah Find, maka secara otomatis akan tampil string dari *title* yang dicari. Perhatikan gambar berikut :

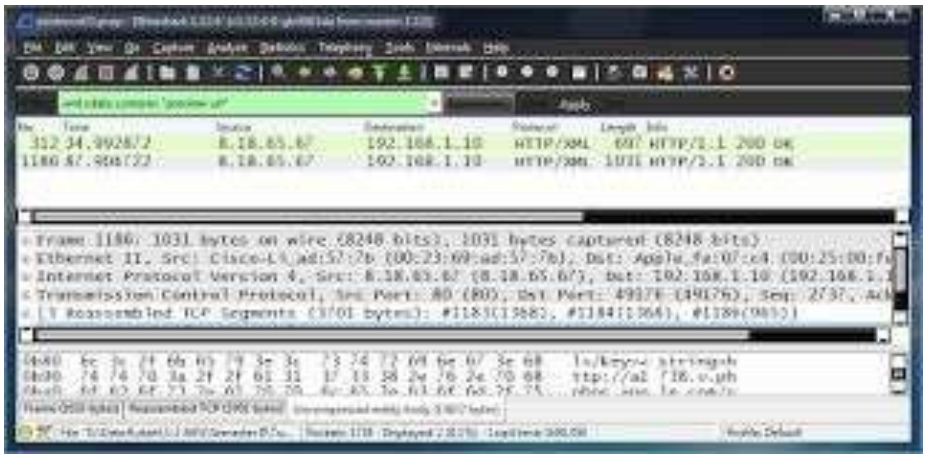


Berdasarkan gambar diatas maka jawaban pertanyaan dari *What was the title of the first movie Ann clicked on* adalah ***sneakers***.

5. What was the full URL to the movie trailer (defined by "preview-url")?

Untuk menjawabnya, kita dapat melakukan langkah-langkah berikut :

a. Pertama-tama kita harus menemukan frame-frame mana yang memiliki *preview-url* yaitu dengan mengetik perintah *xml.cdata contains "preview-url"* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame, seperti pada gambar berikut:



b. Klik menu Edit kemudian klik *Find Packet* atau dengan menekan tombol kombinasi Ctrl + F secara bersamaan, selanjutnya pada jendela *Find Packet* atur seperti berikut :

1. Pada pada perintah *Find* klik/ceklis perintah *String*
2. Pada perintah *Filter* ketik *preview-url*
3. Pada perintah *Search In* klik/ceklis *Packet details*

4 Selanjutnya klik perintah Find, maka secara otomatis akan tampil string dari *preview-url* yang dicari, perhatikan gambar berikut :



Berdasarkan gambar diatas maka jawaban dari pertanyaan:
What was the full URL to the movie trailer (defined by "preview-url") adalah

http://a227.v.phobos.apple.com/us/r1000/008/Video/62/bd/1b/mzm.plqacyqb..640x278.h264lc.d2.p.m4v dan *http://a1738.v.phobos.apple.com/us/r1000/011/Video/7f/9d/ce/mzm.gbctwnmq..640x352.h264lc.D2.p.m4v*

6. What was the title of the second movie Ann clicked on?

Untuk menjawabnya, kita dapat melakukan langkah-langkah berikut :

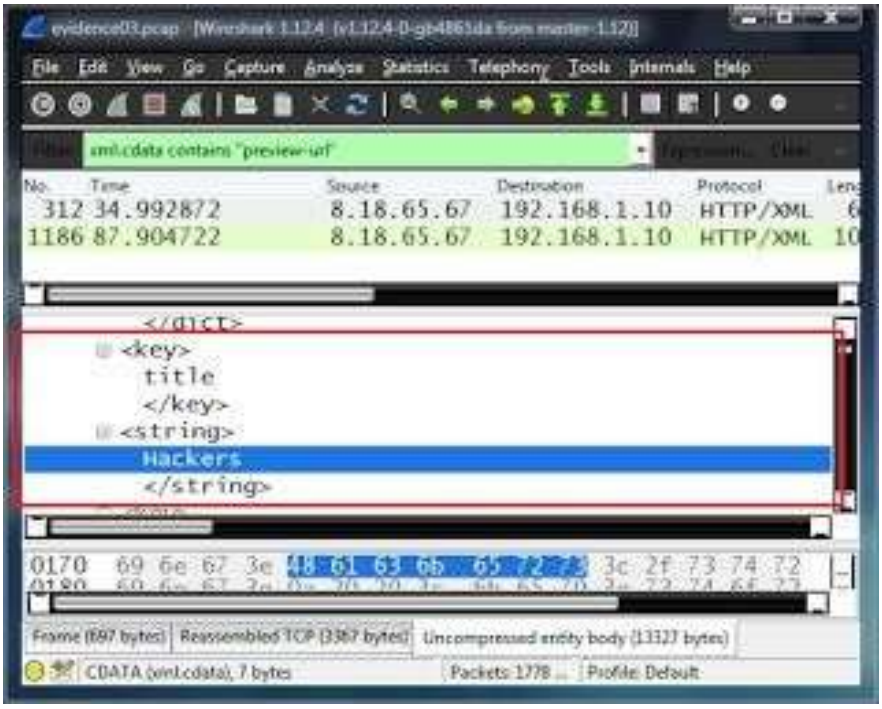
a. Pertama-tama kita harus menemukan frame-frame mana yang memiliki *preview-url* yaitu dengan mengetik perintah *xml.cdata contains "preview-url"* pada kotak *Filter* kemudian tekan tombol*Enter* pada *keyboard*.



b. Klik menu *Edit* kemudian klik *Find Packet* atau dengan menekan tombol kombinasi Ctrl + F secara bersamaan, selanjutnya pada jendela *Find Packet* atur seperti berikut :

1. Pada pada perintah *Find* klik/ceklis perintah *String*
2. Pada perintah *Filter* ketik *title*
3. Pada perintah *Search In* klik/ceklis *Packet details*
4. Selanjutnya klik perintah Find, maka secara otomatis akan tampil string dari *title* yang dicari. Title yang pertama adalah judul movie yang pertama.

5. Selanjutnya klik menu Edit kemudian klik Find Next atau dengan menekan kombinasi tombol Ctrl + N untuk menemukan judul movie yang ke dua, perhatikan gambar berikut :

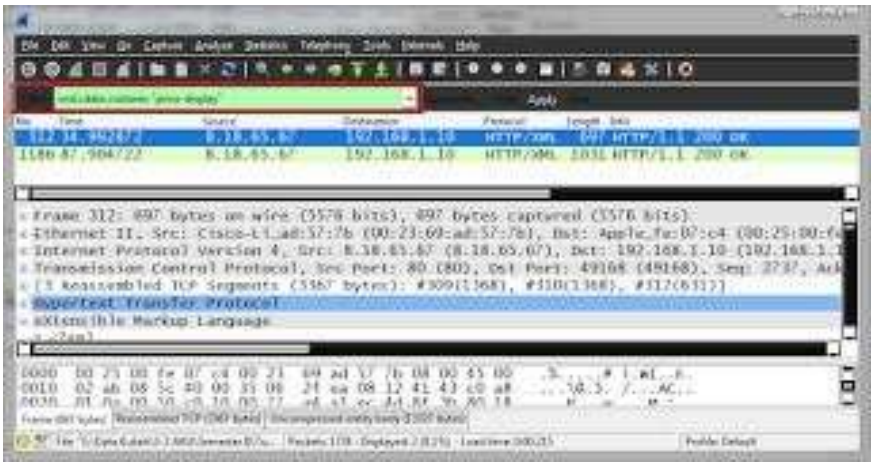


Berdasarkan gambar diatas maka jawaban pertanyaan dari *What was the title of the second movie Ann clicked on* adalah ***Hackers.***

7. What was the price to buy it (defined by "price-display")?

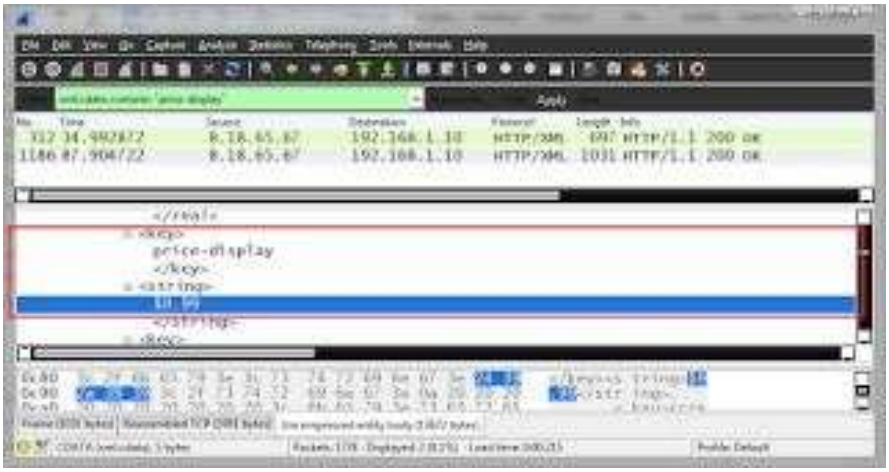
Untuk menjawabnya, kita dapat melakukan langkah-langkah berikut :

a. Pertama-tama kita harus menemukan frame-frame mana yang memiliki *price-display* yaitu dengan mengetik perintah *xml.cdata contains "price-display"* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame, seperti pada gambar berikut:



b. Klik menu *Edit* kemudian klik *Find Packet* atau dengan menekan tombol kombinasi Ctrl + F secara bersamaan, selanjutnya pada jendela *Find Packet* atur seperti berikut :

1. Pada pada perintah *Find* klik/ceklis perintah *String*
2. Pada perintah *Filter* ketik *price-display*
3. Pada perintah *Search In* klik/ceklis *Packet details*
4. Selanjutnya klik perintah Find, maka secara otomatis akan tampil string dari *preview-url* yang dicari, perhatikan gambar berikut :



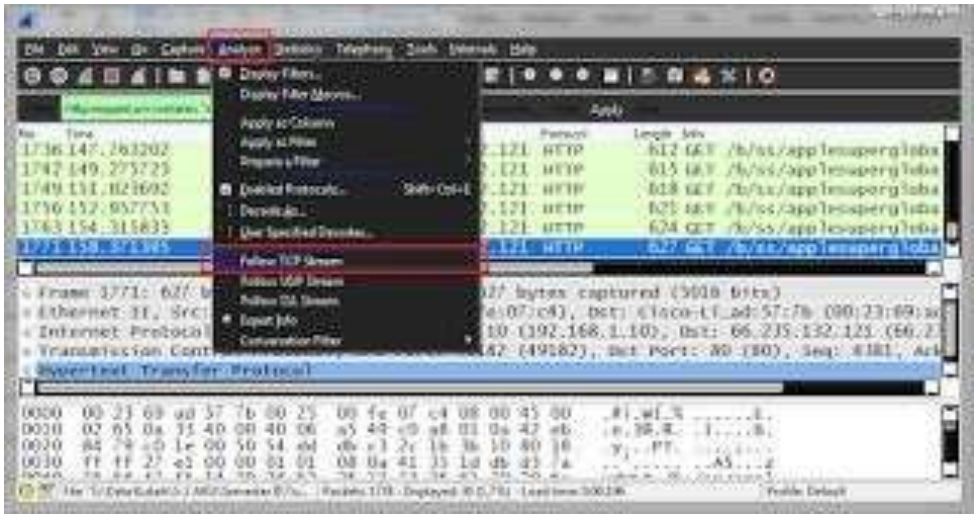
Berdasarkan gambar diatas maka jawaban dari pertanyaan *What was the price to buy it (defined by "price-display")* adalah **$9.99**.

8. What was the last full term Ann searched for?

Untuk menjawabnya kita bisa melakukannya seperti pada cara yang nomor 3, perbedaannya kita mencari istilah penuh yang terakhir dicari oleh Ann. Adapun langkah-langkahnya adalah sebagai berikut :

a. Pertama-tama kita harus menemukan frame-frame mana yang dilakukan *search terms* yaitu dengan mengetik perintah *http.request.uri contains "search"* pada kotak *Filter* kemudian tekan tombol *Enter* pada *keyboard*, sehingga akan ditemukan deretan frame yang dilakukan *search*. Dari hasil *filter* tersebut terdapat 30 frame yang melakukan *search* dan diketahui *frame* terakhir yang melakukan *search* adalah *frame* ke 1771.

b. Aktifkan *frame* ke 1771, kemudian klik menu *Analyze* kemudian klik *Follow TCP Stream*, seperti gambar berikut :

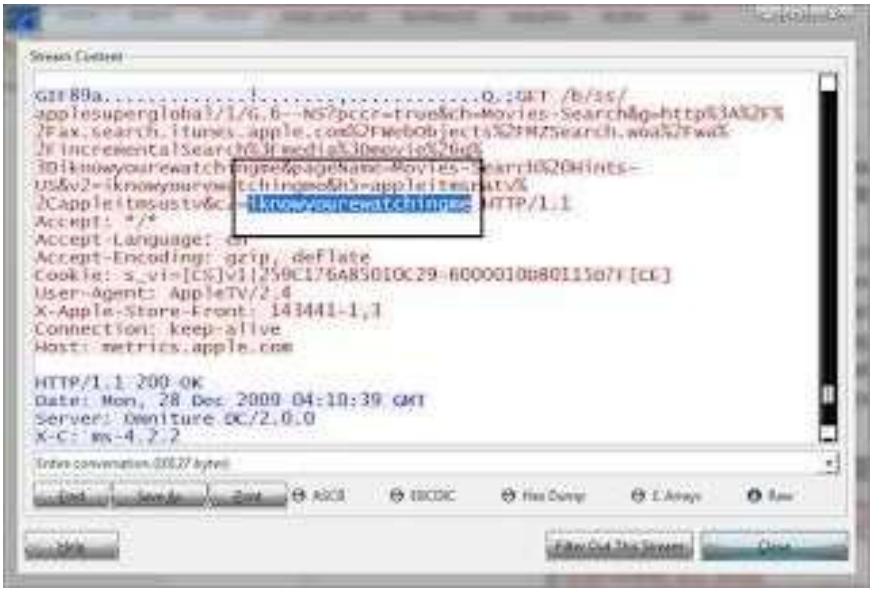


c. Dari perintah *Follow TCP Stream* diatas maka akan tampil jendela *Stream Content* dalam bentuk bentuk *Raw*. *Scroll* dan perhatikan bagian terakhir dari *Stream Content* tersebut kita dapat melihat *detail search* terakhir yang dilakukan oleh Ann yaitu pada alamat :

URI*/b/ss/applesuperglobal/1/G.6--NS?pccr=true&ch=Movies-Search&g=http%3A%2F%2Fax.search.itunes.apple.com%2FWebObjects%2FMZSearch.woa%2Fwa%2FincrementalSearch%3Fmedia%3Dmovie%26q%3Diknowyourewatchingme&pageName=Movies-Search%20Hints-*

US&v2=iknowyourewatchingme&h5=appleitmsnatv%2Cappleitmsustv&c2=iknowyourewatchingme,

kita dapat melihat istilah yang diakses oleh Ann adalah huruf *h*. Perhatikan huruf*iknowyourewatchingme* yang di blok dan di beri kotak hitam dari gambar berikut :



Berdasarkan penjelasan diatas maka jawaban dari pertanyaan *What was the last full term Ann searched for* adalah ***iknowyourewatchingme***.

Praktikum 5
Sosial Chat Forensics

Pretest:

1. Apa itu Wireshark?
2. Sebutkan Fungsi-Fungsi dari Wireshark!
3. Download capture an wireshark pada *bit.ly/evidence05pcap* !

Langkah Praktikum:

Ada seseorang bernama Ann Dercover bekerja pada perusahaan yang bernama Anarchy-R-Us, Inc. Namun, perusahaan menaruh curiga kepada Ann. Ann memiliki akses ke resep rahasia perusahaan. Staff keamanan mencurigai Ann kalau kalau si Ann membocorkan rahasia perusahaan. Staff keamanan memonitor perlakuan Ann, tapi tidak ada hal mencurigakan sampai saat ini. Hingga tiba – tiba ada sebuah laptop yang muncul di jaringan perusahaan, dan IP Ann (**192.168.1.158**) mengirim IMs ke laptop tersebut. Laptop tersebut tiba – tiba menghilang sesaat setelah IMs selesai dikirim. Staff keamanan berhasil mengcapture paket yang dikirim dari komputer Ann, dan mereka meminta penulis untuk menganalisis paket tersebut.

evidence file include modul

Pertanyaan:

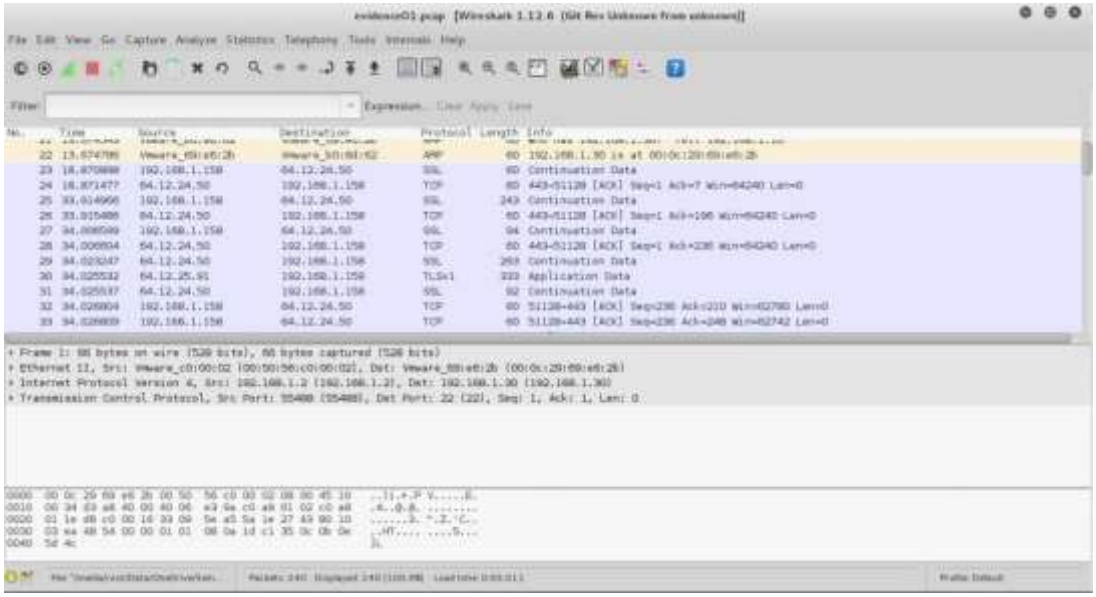
1. Apa nama dari teman IM Ann?
2. Apa komentar pertama dalam percakapan IM ditangkap?
3. Apa nama file Ann yang ditransfer?
4. Apa magic number dari file yang ingin Anda ekstrak (4 byte pertama)?
5. Apa md5sum file?
6. Apa resep rahasia?

Pembahasan

Pertanyaan 1

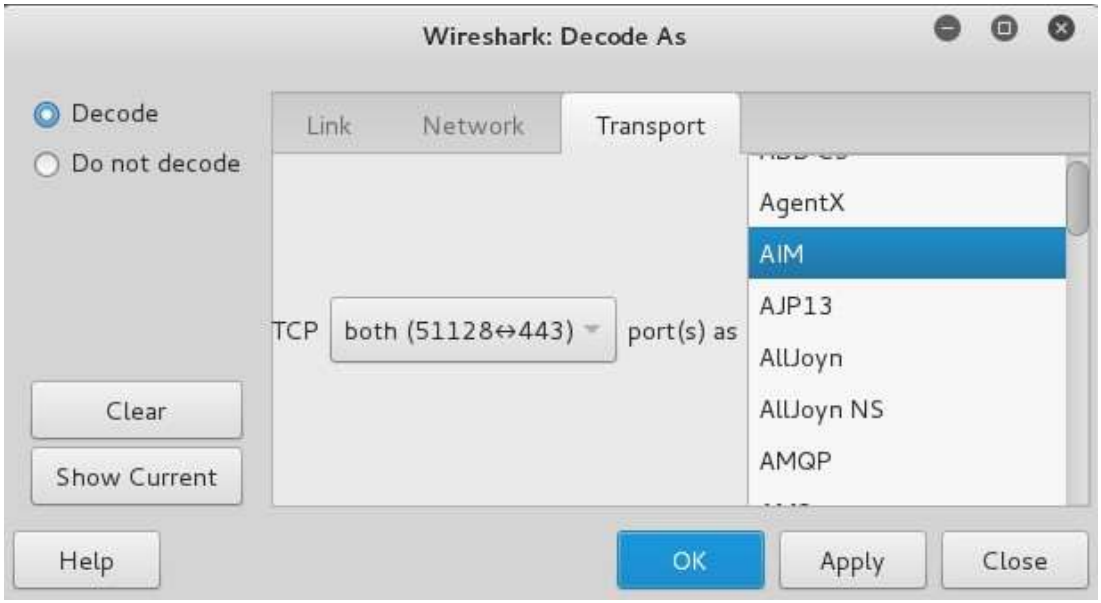
Hal pertama yang harus dilakukan adalah melihat jenis paket apa saja yang ada di wireshark. Ketika kita scroll, akan terlihat tampilan berikut

Pada kolom Protocol, ada protokol ARP, TCP, dan SSL.

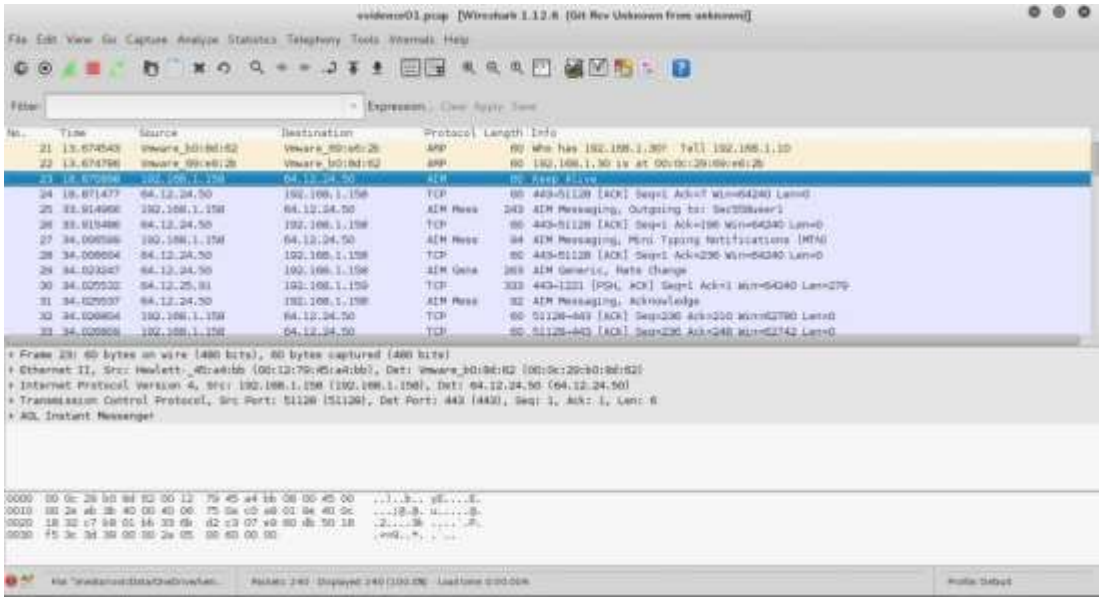


Dari analisis staff keamanan, diketahui bahwa protokol yang dipakai adalah AIM yang bekerja di port 443. Secara default, wireshark akan menganggap port 443 adalah port SSL. Oleh karena itu, kita ganti dulu SSL di wireshark menjadi protokol AIM dengan cara:

1. Klik kanan paket SSL nya
2. Klik Decode As
3. Pilih AIM



Setelah di klik apply, maka tampilan wireshark akan menjadi seperti berikut



Terlihat pada kolom protokol, SSL telah berubah menjadi AIM. Tujuan perubahan ini agar paket AIM dapat terbaca.

Kita perhatikan paket nomor 25….



Terlihat ada kata – kata **Outgoing to: Sec558user1**. **Sec558user1** adalah user AIM dari Ann. Terjawab pertanyaan nomor 1

Pertanyaan 2

Pada paket yang sama, kita dapat melihat text message yang ada pada paket tersebut. Lihat screenshoot di bawah ini.



Ada kalimat **Here's the secret recipe….** Kalimat tersebut adalah kalimat yang dikirim Ann ke pelaku. Terjawab pertanyaan 2

Pertanyaan 3

Untuk mencari nama file yang dikirim, ketikkan perintah berikut di terminal

strings evidence01.pcap | grep -A 2 'OFT2'

Adapun penjelasan fungsi dari perintah di atas sebagai berikut:

1. strings: Untuk memunculkan semua string yang ada di file evidence01.pcap
2. grep -A 2 'OFT2': untuk memunculkan 2 string sebelum dan sesudah baris string yang mengandung kata **'OFT2'**

Ketika perintah dijalankan, maka akan dihasilkan output berikut:

OFT2
Cool FileXfer
recipe.docx
–
OFT2
7174647
Cool FileXfer
–
OFT2
7174647
Cool FileXfer

Dari hasil tersebut, terlihat ada nama file **recipe.docx**. Nama file tersebut adalah nama file yang dikirim oleh Ann. Terjawab pertanyaan 3

Pertanyaan 4

Untuk mencari magic number, kita search di mesin pencari, apakah magic number dari docx. Magic number tersebut dapat ditemukan di website : http://www.garykessler.net/library/file_sigs.html

Magic number tersebut adalah **50 4B 03 04**. Terjawab pertanyaan 4

Pertanyaan 5

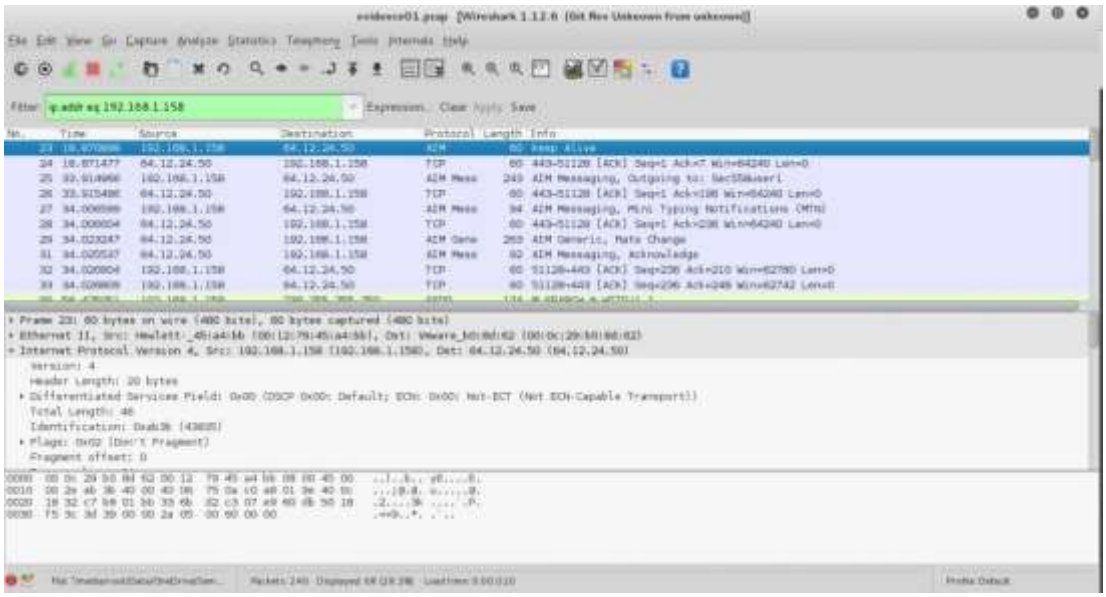
Untuk mencari file yang diinginkan, ada 2 cara yang dapat dilakukan.

Cara pertama adalah langkah berikut dijalankan melalui terminal:

1. tshark -Y 'ip.addr eq 192.168.1.158' -r evidence.pcap -w newev.pcap
2. ngrep -I newev.pcap 'OFT2.*Cool FileXfer' src port 5190 | grep 'T '

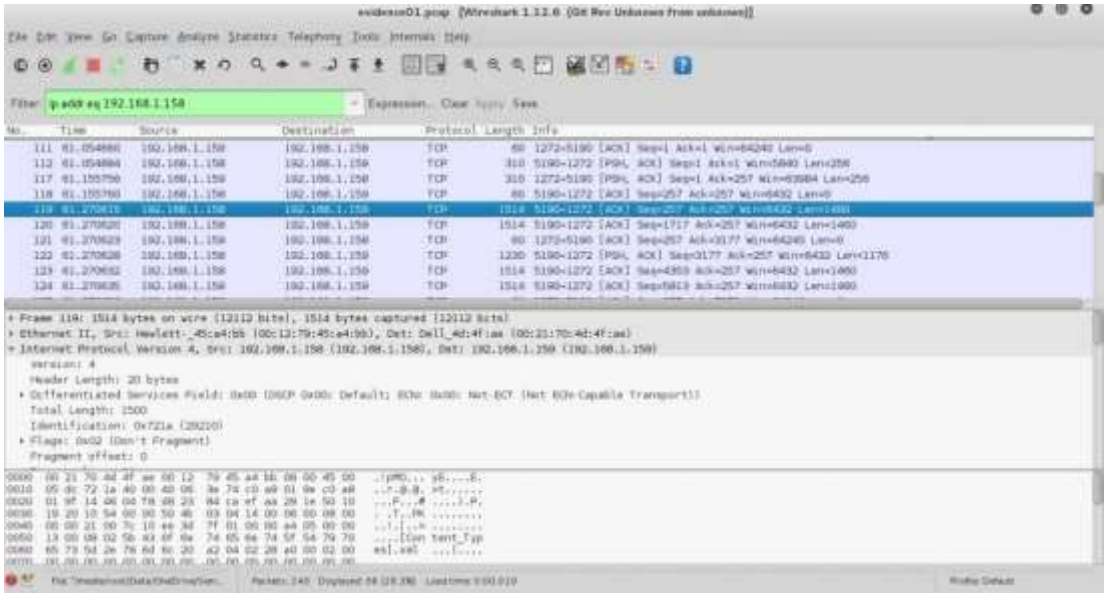
3. tshark -Y '(ip.addr eq 192.168.1.159 and ip.addr eq 192.168.1.158) and (tcp.port eq 1272 and tcp.port eq 5190)' -r newev.pcap -w OFT2CONV.pcap
4. tcpflow -r OFT2CONV.pcap 'src port 5190'
5. mv 192.168.001.158.05190-192.168.001.159.01272 payload1
6. xxd -ps payload1 > hex1
7. search for "504b0304" yang pertama, dan hapus semua huruf sebelum 504b, lalu simpan
8. xxd -r -ps hex1 > recipe.docx
9. md5sum recipe.docx

Cara di atas adalah cara yang ada di video. namun berhubung terlalu panjang jika dijelaskan 1 per 1, maka ada lagi cara yang kedua yang memakai wireshark GUI. Hal pertama yang harus dilakukan adalah menemukan paket yang berasal dari IP 192.168.1.158. IP tersebut adalah IP dari komputer Ann. Untuk mencarinya, ketikkan ip.addr eq 192.168.1.158 di filter wireshark seperti berikut:

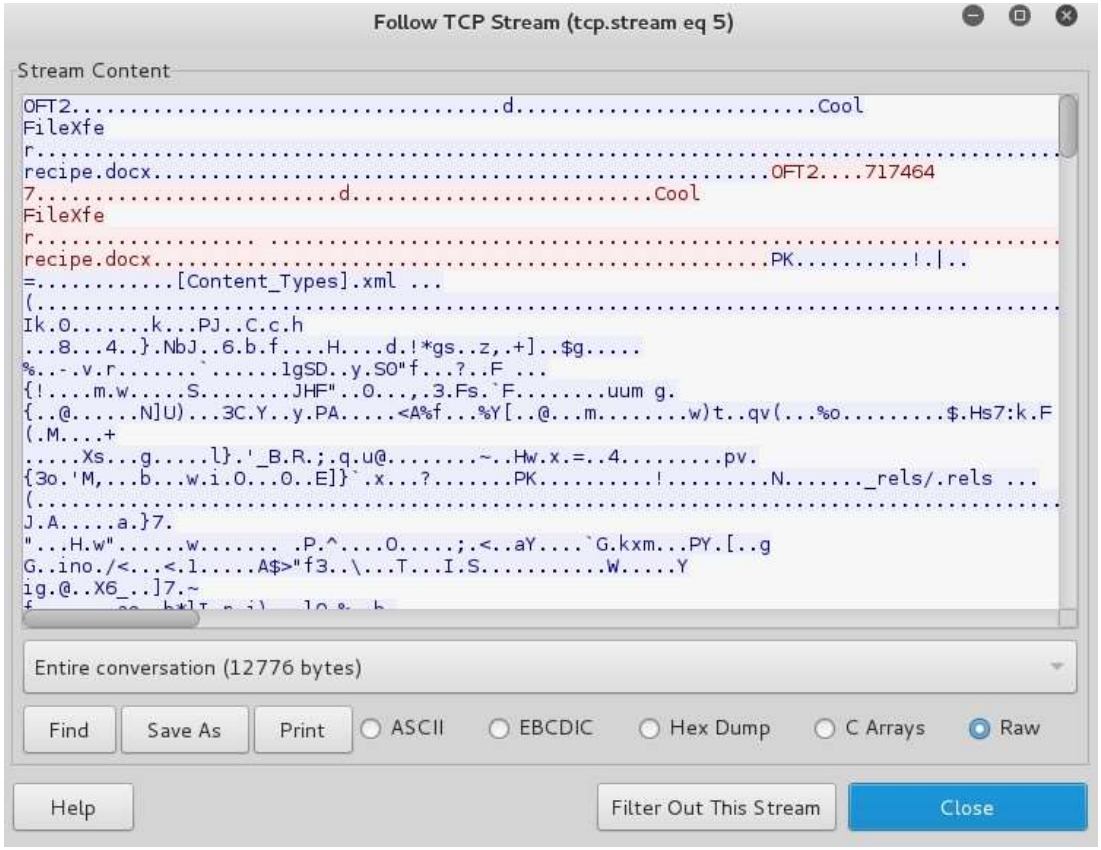


Setelah kita mendapatkan hasil filternya, hal berikutnya adalah kita cari paket yang kolom **length** nya cukup besar. Hal ini dikarenakan yang kita cari adalah paket yang mengirim file. Oleh karena itu, kita butuh panjang paket yang besar juga.

Setelah kita scroll hasil filter, maka akan ditemukan paket nomor 119 dengan panjang paket 1514 seperti gambar berikut:



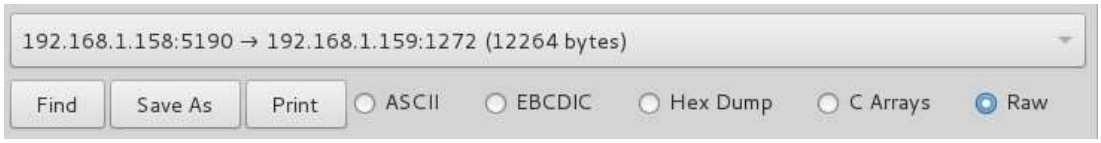
Kita klik kanan file tersebut, dan klik **Follow TCP Stream.** Hasilnya seperti berikut.



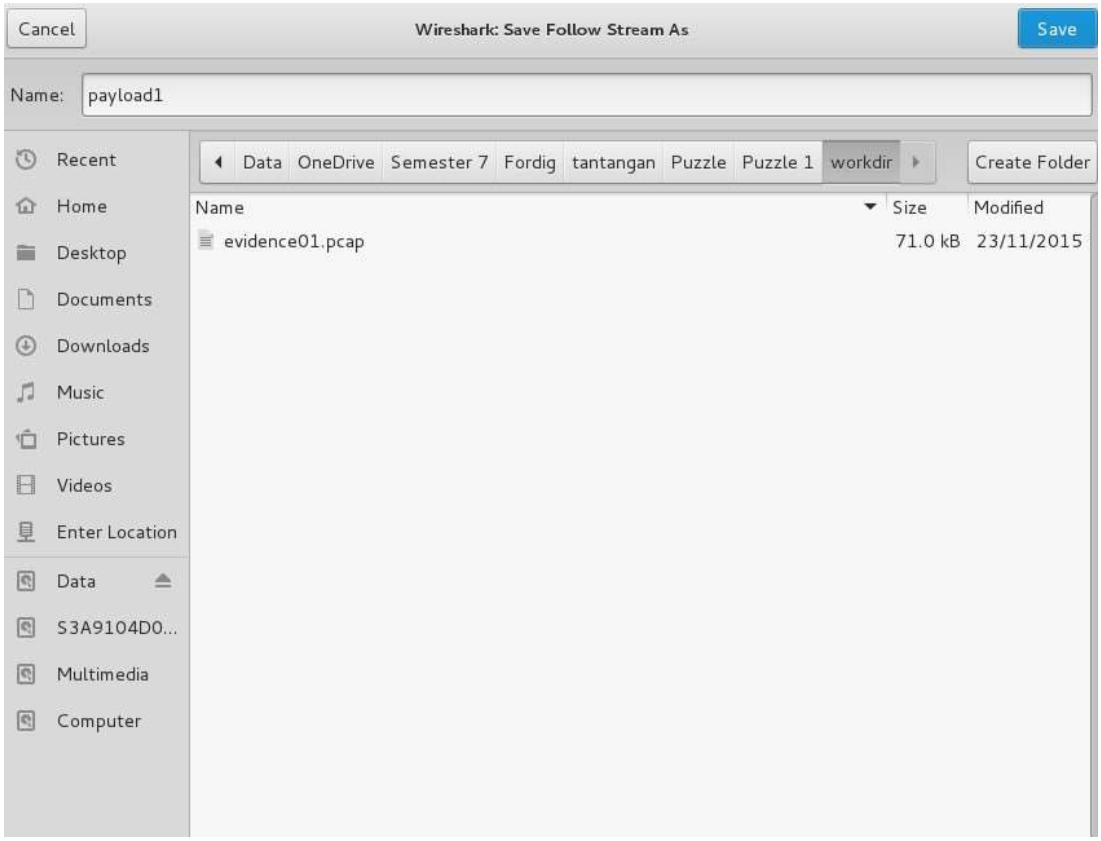
Pada dropdown Entire conversation, kita ganti dari



menjadi berikut



klik save as, dan kita simpan dengan nama **payload1**



File payload1 adalah file binary dari paket yang dikirim. Untuk membacanya sebagai docx, maka kita harus menghapus “binary sampah” yang ada di file payload1. Untuk melakukannya, ada beberapa langkah di terminal hingga file docx berhasil didapat. Ikuti langkah berikut: xxd -ps payload1 > hex1

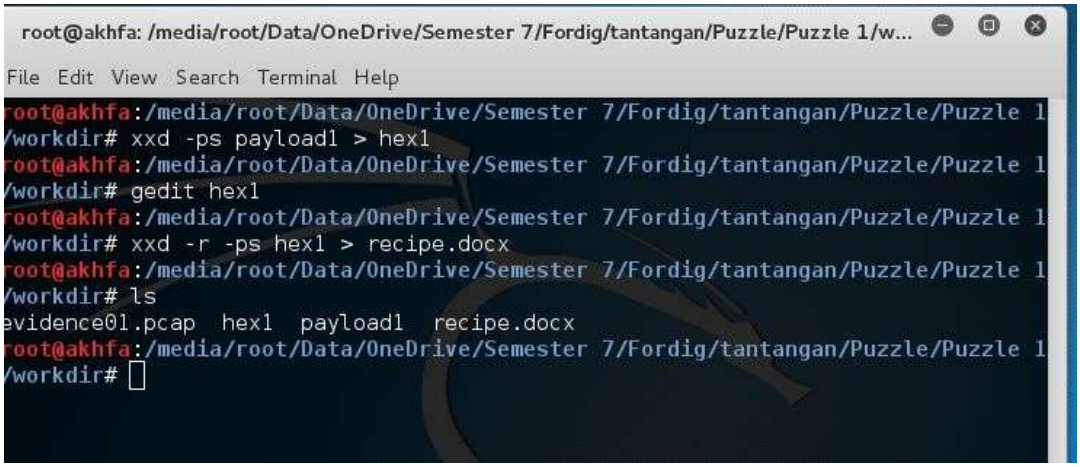
Untuk mengubah file binary menjadi file txt yang dapat dibaca gedit

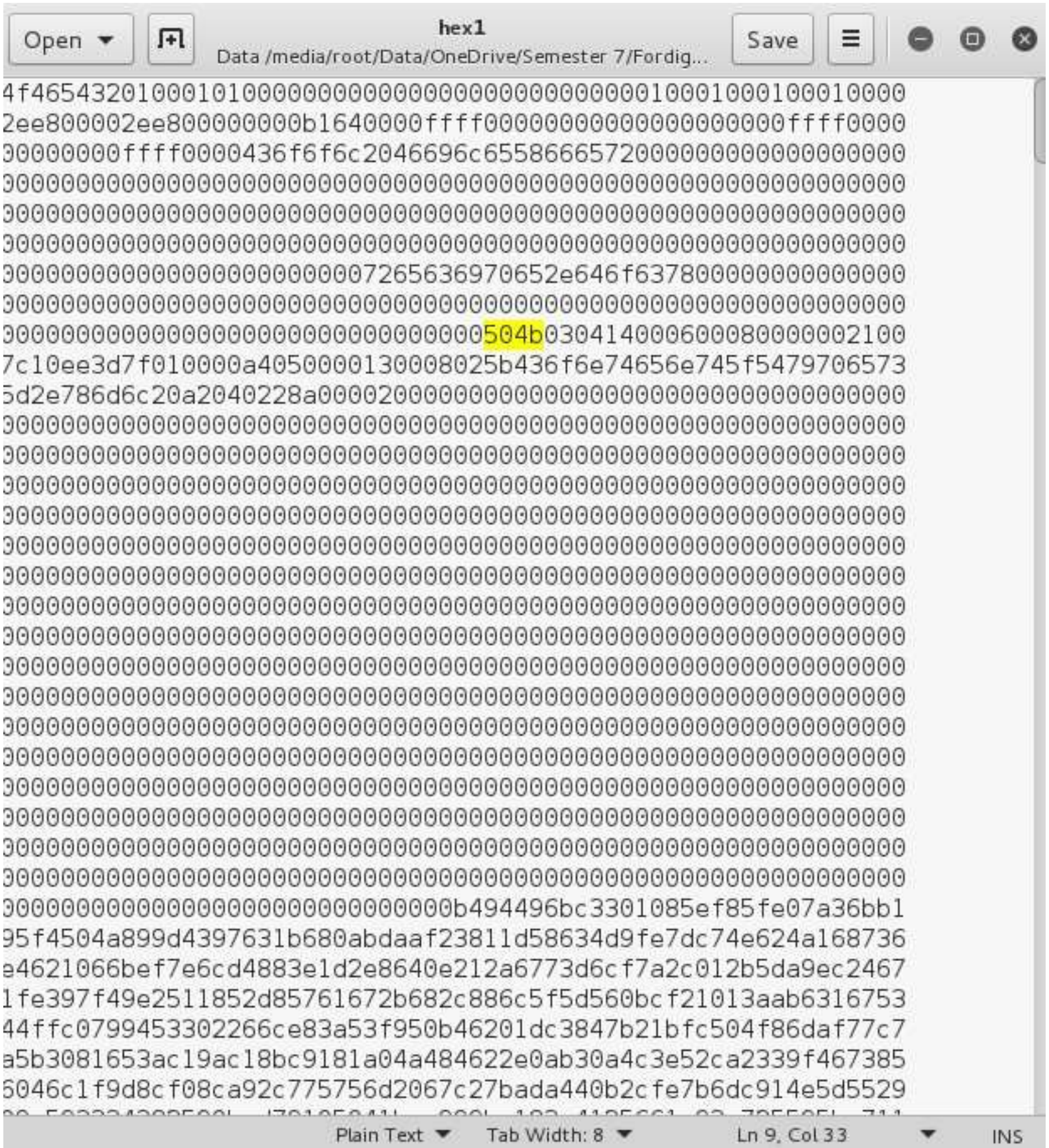
- gedit hex1
- Buka aplikasi gedit yang muncul
- Cari 504b yang pertama kali dari file hex1
- Hapus semua karakter sebelum 504b

Bertujuan untuk menghapus binary yang tidak diperlukan

- simpan filenya
- Kembali ke terminal
- xxd -r -ps hex1 > recipe.docx

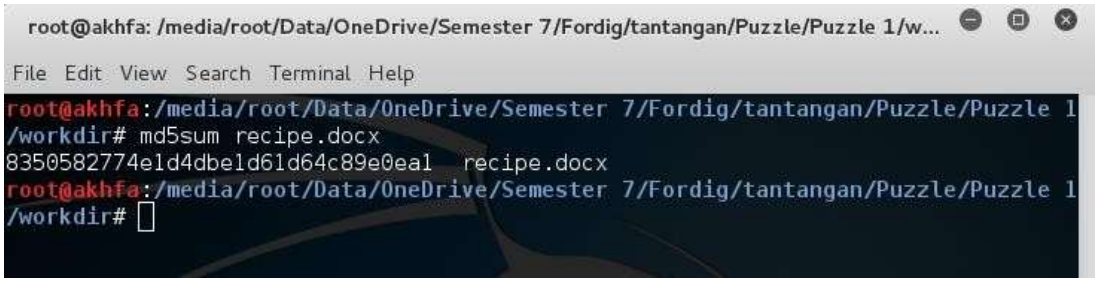
Untuk mengubah file txt menjadi binary kembali, yang mana binary kali ini adalah file docx yang kita cari.




Open
hex1
Data /media/root/Data/OneDrive/Semester 7/Fordig...
Save
7c10ee3d7f010000a405000013000802 5b436f6e74656e745f5479706573
95f4504a899d4397631b680abdaaf23811d58634d9fe7dc74e624a168736
e4621066bef7e6cd4883e1d2e8640e212a6773d6cf7a2c012b5da9ec2467
1fe397f49e2511852d85761672b682c886c5f5d560bcf21013aab6316753
44ffc0799453302266ce83a53f950b46201dc3847b21bfc504f86daf77c7
a5b3081653ac19ac18bc9181a04a484622e0ab30a4c3e52ca2339f467385
6046c1f9d8cf08ca92c775756d2067c27bada440b2cfe7b6dc914e5d5529
Plain Text
Tab Width: 8
Ln 9, Col 33
INS



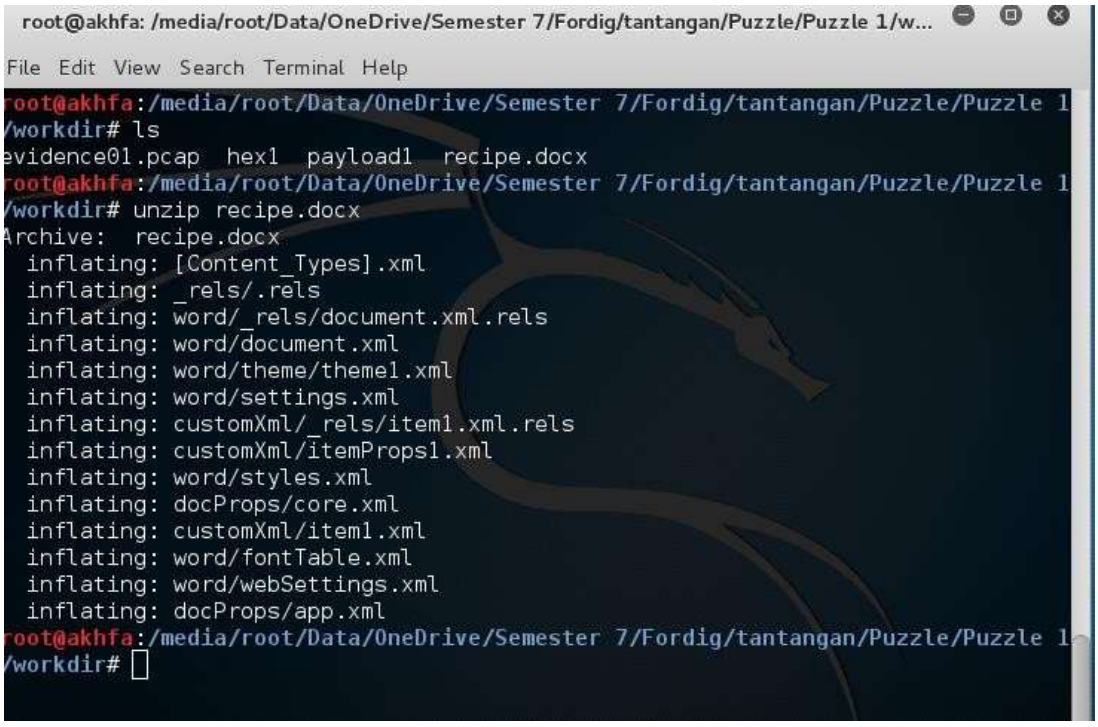
Sampai pada langkah ini, file docx berhasil kita dapatkan. Lakukan **md5sum recipe.docx,** dan terjawablah soal 5



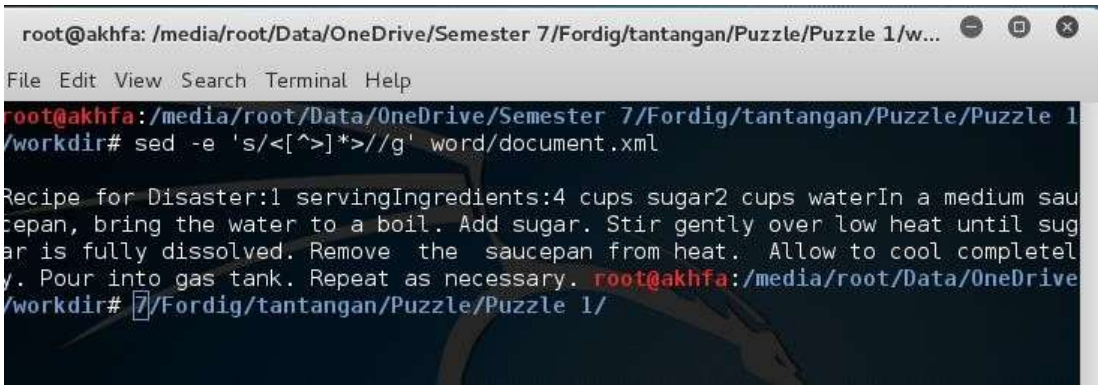
Pertanyaan 6

Untuk melihat isi dari recipe.docx, sebenarnya bisa saja file tersebut langsung dibuka menggunakan aplikasi office, namun cara ini kurang aman. Lebih aman jika kita memakai cara berikut untuk mengetahui isi dari file docx.

Perlu diketahui bahwa file docx sebenarnya adalah file zip biasa. Maka untuk membukanya, tinggal kita unzip seperti gambar berikut:



dan jalankan perintah **sed -e ‘s/<[^>]*>//g’ word/document.xml di terminal**



Terjawablah pertanyaan terakhir

Praktikum 6

Email Forensics "Tools NetworkMiner"

Pretest:

1. Apa fungsi networkminer dalam kaitannya dengan investigasi email *forensics*?
2. Apa saja yang dapat di explorasi dr tools tsb!

capture image (.pcap)
http://bit.ly/2m1oHAp

network miner windows
http://bit.ly/2Ajhez3

Langkah Praktikum:

Gunakan pendekatan 5w + 1H untuk menjawab dari 8 daftar pertanyaan yang harus kita pecahkan. Ke delapan pertanyaan tersebut yaitu :

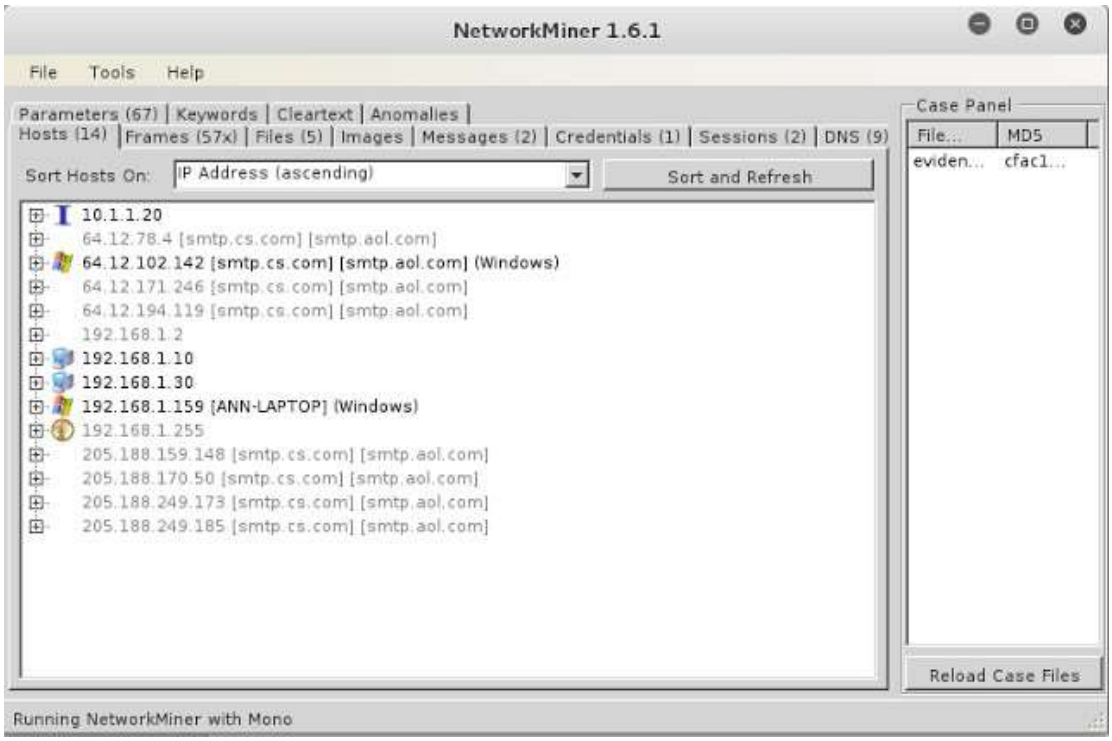
- *What is Ann's email address?*
- *What is Ann's email password?*
- *What is Ann's secret lover's email address?*
- *What two items did Ann tell her secret lover to bring?*
- *What is the NAME of the attachment Ann sent to her secret lover?*
- *What is the MD5sum of the attachment Ann sent to her secret lover?*
- *In what CITY and COUNTRY is their rendez-vous point?*
- *What is the MD5sum of the image embedded in the document?*

What data do you need to answer that question?

Data apa saja yang dibutuhkan untuk menjawab pertanyaan yang ada? Jawaban dari pertanyaan ini yaitu data berupa file *packet capture* dari aktivitas jaringan yang dilakukan oleh Ann yaitu file yang bernama "evidence02.pcap".

How do you extract/analyze that data?

Bagaimana cara mengkestrak atau menganalisis data? Jawaban dari pertanyaan ini yaitu menganalisis menggunakan *NetworkMiner* yang ada di *kali linux* 2.0.

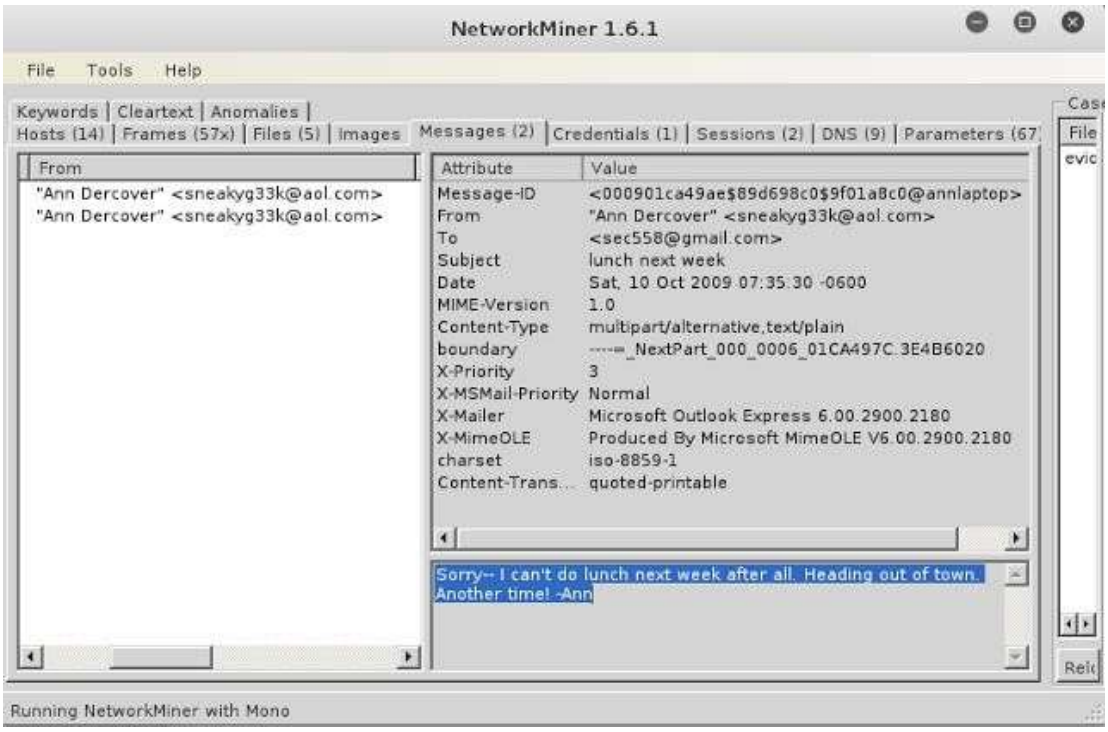


What does the data tell you?

Apa yang dijelaskan data tersebut? Nah untuk menjawab pertanyaan ini, maka kita lakukan analisis hasil ekstraksi data tadi. Yang akan dijelaskan data tersebut dan yang akan kita cari yaitu 8 pertanyaan diawal tadi yaitu :

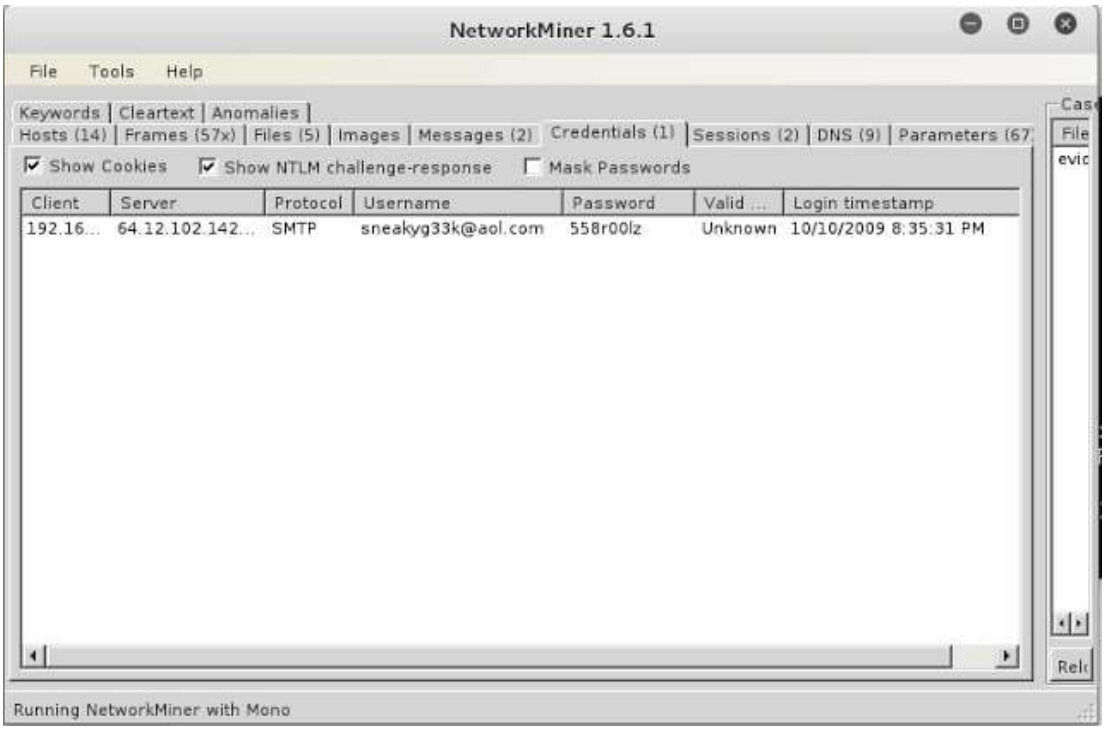
- *What is Ann's email address?*

Hasil analisis mendapatkan data bahwa *email address* Ann's yaitu sneakyg33k@aol.com. Hal ini dapat dilihat dari menu *Messages* yang ada pada *NetworkMiner* maka akan terlihat email yang ada dalam *log*jaringan tersebut. Hasil analisis *screenshot NetworkMiner* dibawah ini.



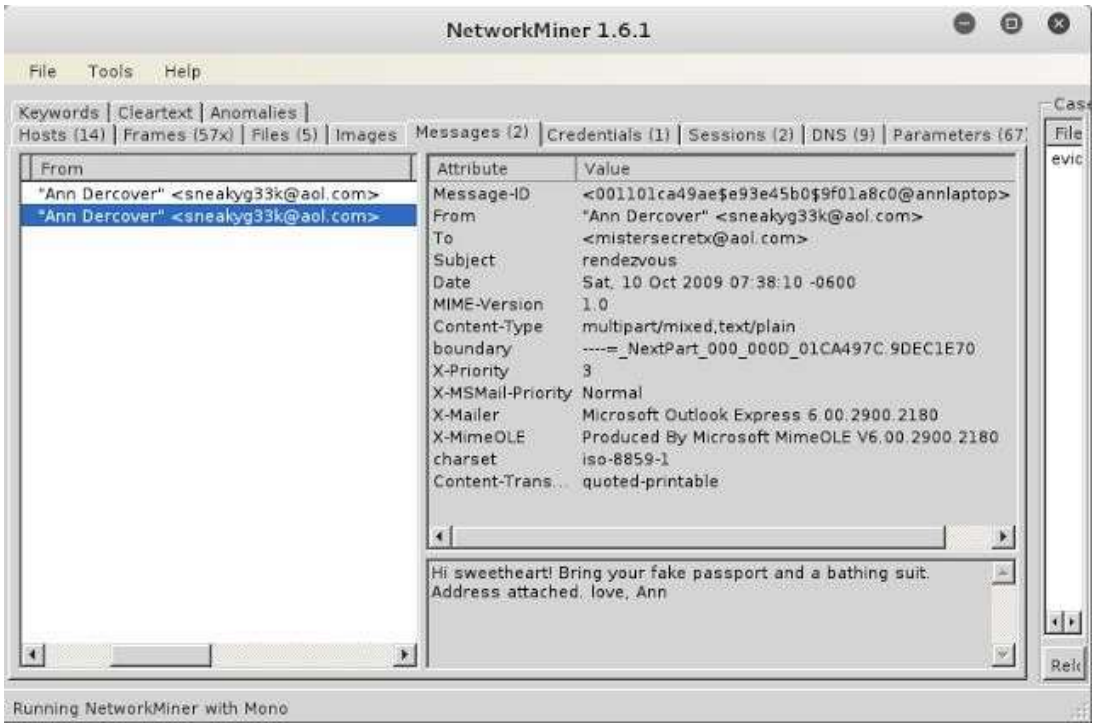
- *What is Ann's email password?*

Hasil analisis juga berhasil mendapatkan *password* email tersebut yaitu 558r00lz. *Password* tersebut didapatkan dari menu *Credentials* di *NetworkMiner*. Screenshoot ditemukannya *password* tersebut dapat dilihat pada gambar dibawah ini.



- *What is Ann's secret lover's email address?*

Email address "*secret lover's*" si Ann yaitu mistersecretx@aol.com. Hal ini terungkap dari email yang dikirimkan oleh Ann ke pasangannya. Untuk mendapatkan data ini, kita kembali lagi ke menu *Messages*, dan membuka *Messages* yang kedua, dimana isi emailnya dapat dilihat pada gambar dibawah ini.

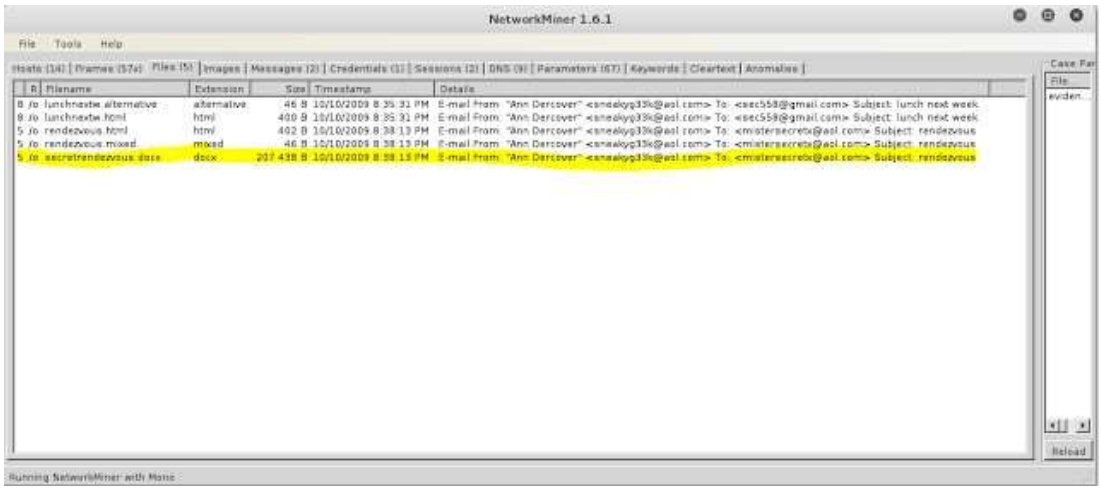


- *What two items did Ann tell her secret lover to bring?*

Jawaban atas pertanyaan ini dapat dilihat pada gambar diatas dimana Ann mengirimkan email ke pasangannya untuk membawa Pasport Palsu dan Baju Renang.

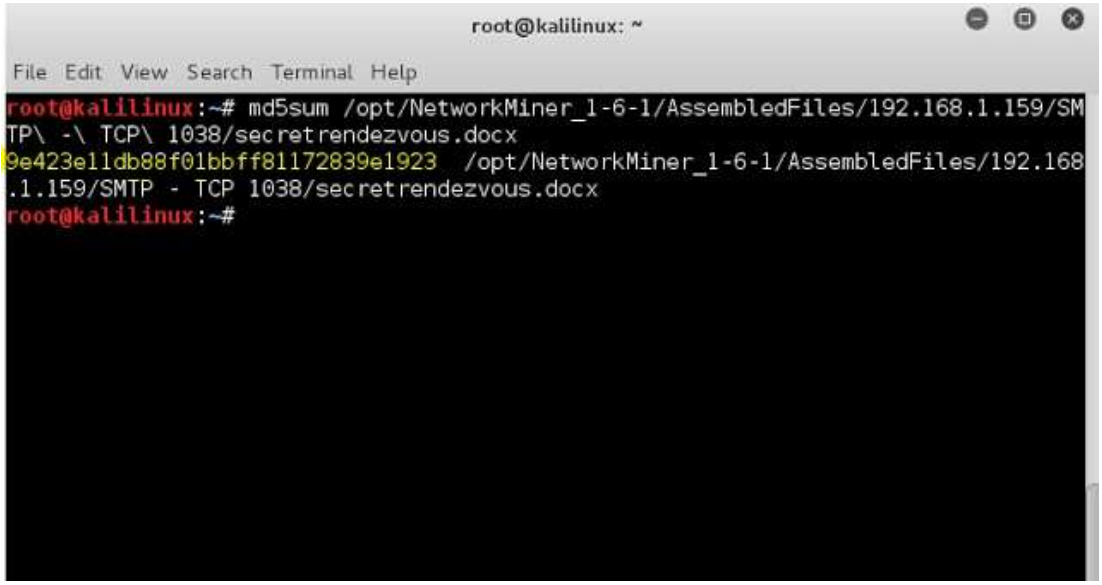
- *What is the NAME of the attachment Ann sent to her secret lover?*

Hasil analisis juga mendapatkan data attachment ini. File attachment tersebut bernama secretrendezvous.docx. File ini didapatkan dari menu *Files* yang ada di *NetworkMiner*, hasil *screenshot*ditemukannya file tersebut dapat dilihat pada gambar dibawah ini.



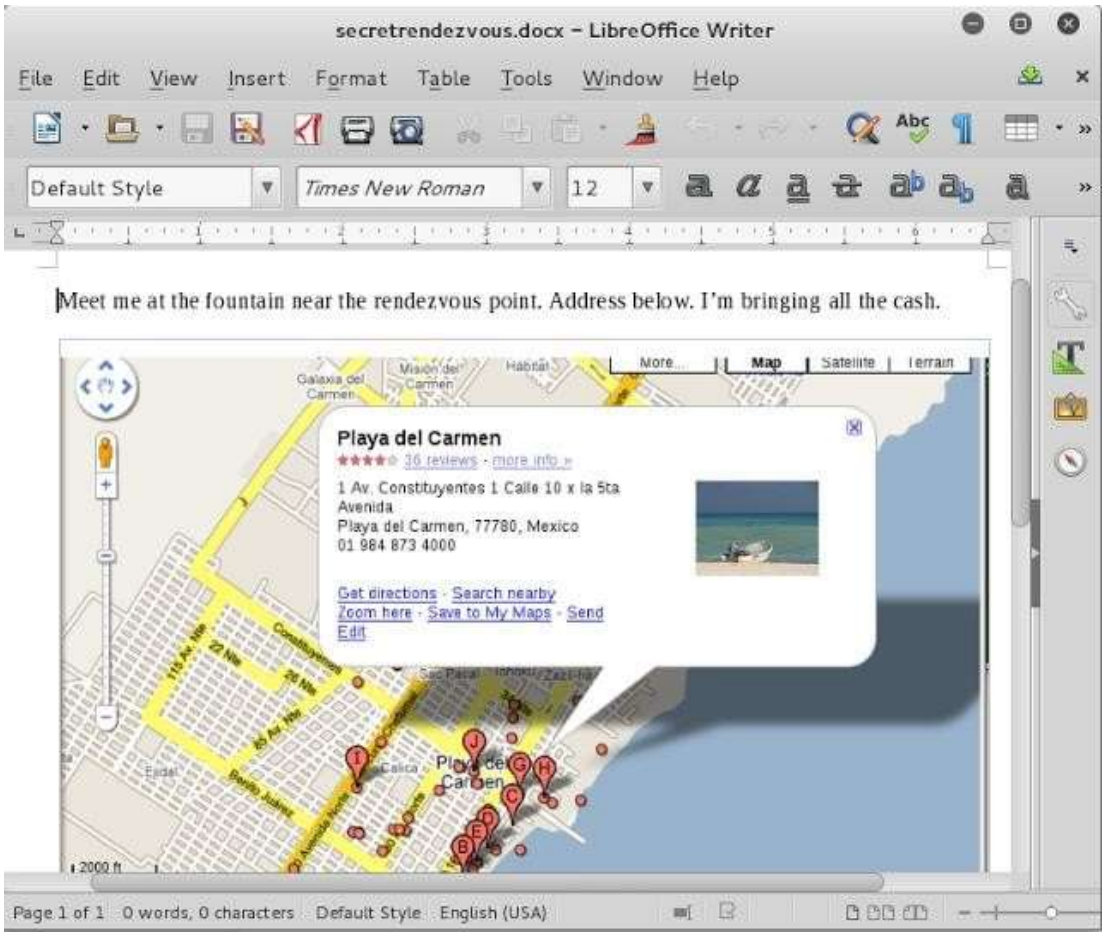
- *What is the MD5sum of the attachment Ann sent to her secret lover?*

Untuk menjawab pertanyaan ini, maka file yang ditemukan tadi kita *generate* kode md5 nya seperti gambar dibawah ini. Adapun hasil *generate* kode MD5 nya dengan menggunakan perintah md5sum yaitu *9e423e11db88f01bbff81172839e1923*



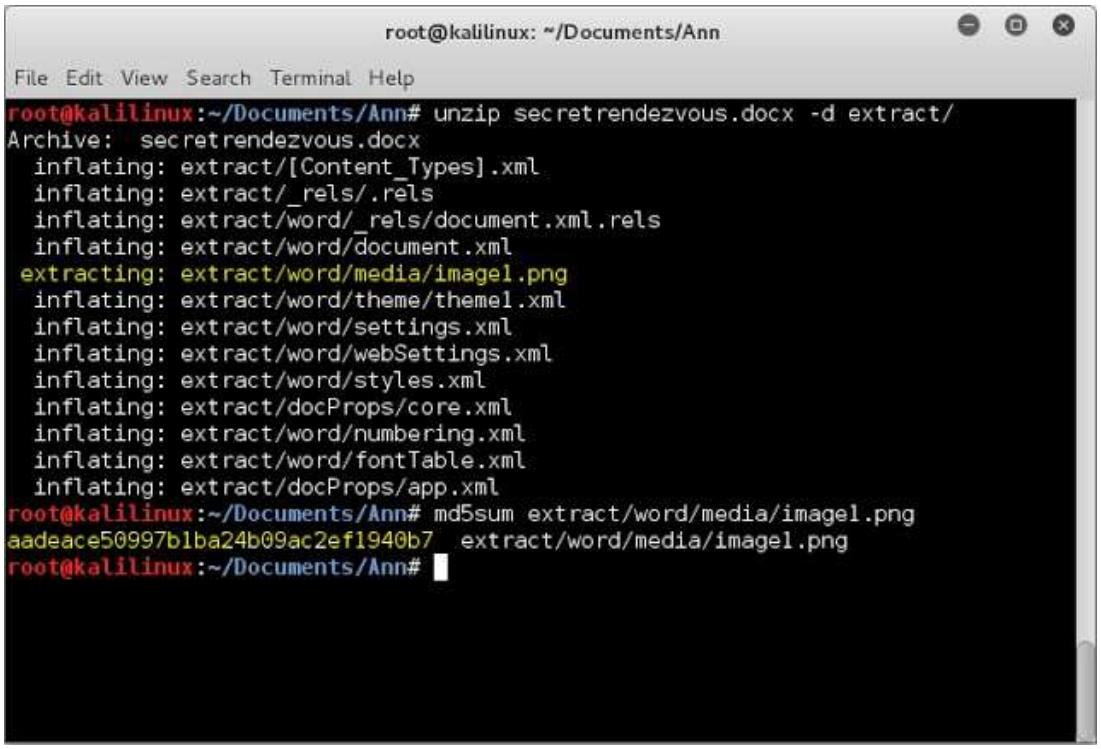
- *In what CITY and COUNTRY is their rendez-vous point?*

Untuk menjawab pertanyaan ini, maka file tadi harus dibuka terlebih dahulu dan dianalisis lagi. Dari hasil analisis terhadap file secretrendezvous.docx tadi ditemukan jawaban bahwa mereka akan bertemu di Playa del Carmen, Mexico.



- *What is the MD5sum of the image embedded in the document?*

Untuk mengetahui nilai md5 dari gambar yang ada dalam dokumen tersebut, maka dokumen tersebut harus di ekstrak terlebih dahulu untuk "mengeluarkan" gambarnya. Langkah dan prosedur yang dilakukan dapat dilihat pada gambar dibawah ini.



Akhirnya selesai terjawab semua pertanyaan-pertanyaan tadi. Setelah semua proses analisis selesai dilakukan, tahapan selanjutnya yaitu merekonstruksi kasus tersebut menggunakan model pertanyaan 5W + 1H. Pertanyaan apa saja dalam model 5W + 1H tersebut? Pertanyaannya yaitu *What, When, Where, Who, Why, dan How*.

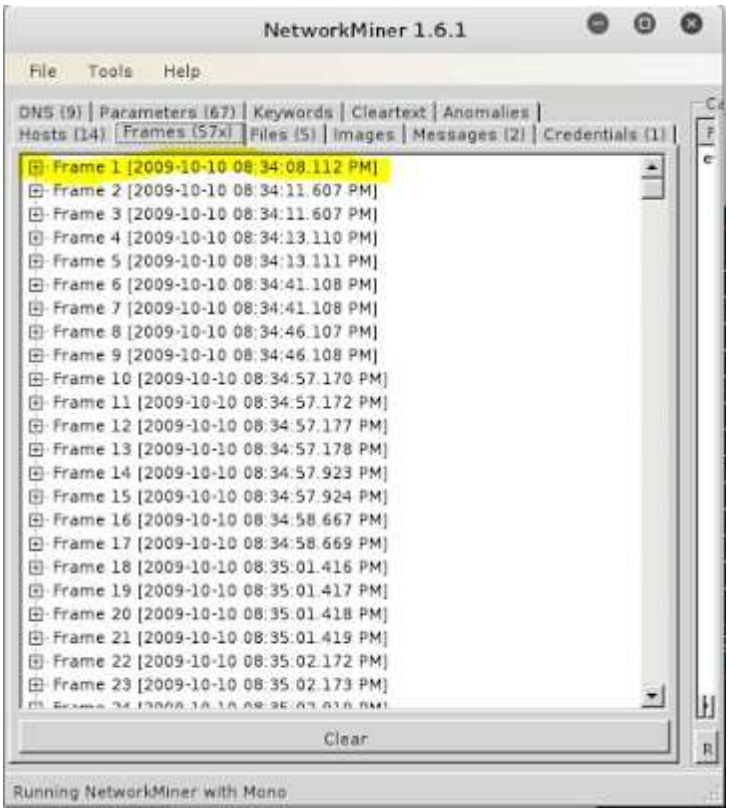
WHAT

Pada pertanyaan ini, yang ditanyakan yaitu apa kasusnya? Berdasarkan data dari forensicsontest.com diceritakan bahwa si Ann Dercover pernah tertangkap oleh polisi, tapi sudah dibebaskan dengan jaminan. Namun tidak lama setelah itu, si Ann menghilang. Tapi penyidik telah memonitoring aktivitas jaringan yang digunakan oleh Ann dan mencurigai ada komunikasi yang dilakukannya dengan kekasihnya sebelum menghilang.

WHEN

Kapan kasus ini terjadi? Berdasarkan hasil analisis terhadap file aktivitas jaringan si Ann, ditemukan bahwa si Ann merencanakan kepergian dan menghilang pada

tanggal 10 Oktober 2009. Si Ann berkomunikasi dengan kekasihnya antara pukul 08:34:112 PM berdasarkan awal mula aktivitas jaringannya.



WHERE

Dimana si Ann berada? Setelah komunikasi yang dilakukan Ann dengan kekasihnya, dapat dipastikan bahwa dia akan berada di Playa del Carmen, Mexico.

WHO

Siapa saja yang terlibat dalam kasus ini? Yaitu Ann Dercover dengan akun email sneakyg33k@aol.com dan kekasihnya dengan akun email mistersecretx@aol.com.

WHY

Kenapa Ann melarikan diri? Kemungkinan Ann tidak ingin kembali dipenjara apabila nantinya kasusnya selesai disidangkan dan ternyata Ann terbukti bersalah, sehingga dia merencanakan untuk melarikan diri.

HOW

Bagaimana Ann melarikan diri? Hal ini telah kita bahas diatas, yaitu Ann melarikan diri dengan menghubungi kekasihnya dan menyuruhnya membawakan passport palsu dan baju renang yang kemudian mereka merencanakan untuk bertemu di kota Playa dl Carmen, Mexico.

Kesimpulan

Kesimpulan yang dapat kita ambil dalam pembahasan yang panjang ini yaitu, prinsip *Occam Razor* dan *Alexiou Principle*sangat membantu dalam hal melakukan pencarian untuk menganalisis sebuah kasus. Karena dengan adanya prinsip tersebut, kita mempunyai semacam panduan apa yang akan mulai dikerjakan. Kemudian berdasarkan prinsip pencarian tersebut, dan kita selesai menemukan barang bukti yang diinginkan, maka rekonstruksi kasus menggunakan 5W+1H sangat membantu untuk melihat motif pelaku melakukan kejahatan berdasarkan bukti bukti yang dikumpulkan.

Sources: *http://forensicscontest.com/2009/10/10/puzzle-2-ann-skips-bail*

Praktikum 7
Data Carving

Pretest:

1. What is Data Carving?
2. Explain every command in Foremost Tool!

Goal

This exercise will illustrate some of the concepts learned in this brief introduction to data carving. You will use Foremost to carve different files from an image of a thumbdrive.

Your instructor will guide you through this exercise. This will prepare you for performing this module's casework on your own.

Requirements

- Foremost (linux/Windows)
- Formatted_thumb.dd
  (*bit.ly/formatted_thumb*)

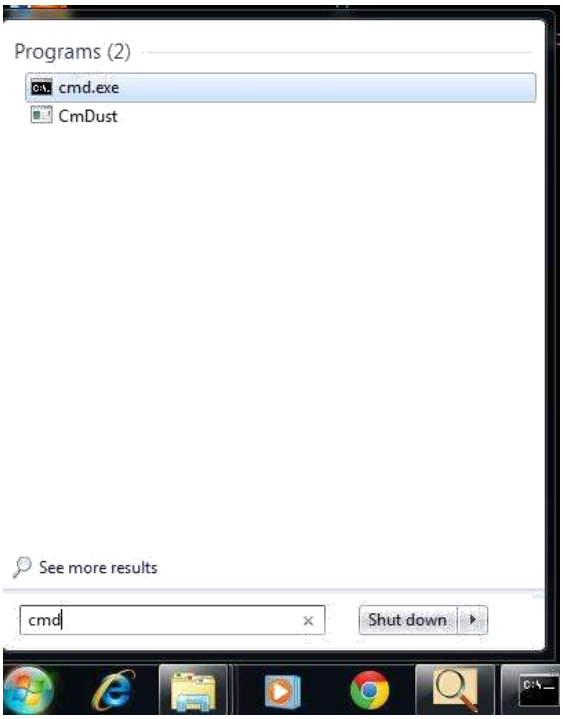
Review

Recall from the lecture that when a file is deleted the filesystem marks it as being free space to be written over. The filesystem still maintains a record of deleted file, just will write over it if space is needed. When a storage device is reformatted the old filesystem is wiped out and a new one is created. All the files on the previous device still exist but there is no structure which knows where these files are located.

In this exercise we will look at an image of a thumbdrive which was reformatted. You cannot see the files on the image of the thumbdrive, but we will be able to retrieve them in this exercise.

Steps

1. Open the command prompt.
    a. Go to start menu. (Windows Icon bottom left)
    b. In search box type **cmd** and hit enter.



2. Navigate to the folder where the image we will use is located.
    a. In command prompt go to data carving folder by **cd c:\Advanced\DataCarving**.

3. Use foremst to pull information from the image file.
    a. Whenever we use a tool, it is always a good idea to see if there is any help information. This is done by typing **foremost.exe –h**. This will give us a listing of some of the some of the commands we can use for the tool.



b. We are going to try and see if there are and pdfs on the image. We do this by typing **foremost.exe –t pdf –T –i Formatted_thumb.dd.**

By calling **foremost.exe** we are calling the program to use. By looking at the help information above we use the **–t** flag to specify the file we are looking for (multiple files can all be typed together by separating them by commas). By specifying the **–i** we tell the program what image file we will be carving. The last flag is not mentioned in the help file but there is another flag used, **-T**. When foremost runs it will put all of the files it finds into an output folder. If the folder already exists, then it will not run. This command creates an output folder with a time stamp. This is useful because a different folder is created each time and the time and date is associated with it.

Note

We specify which files we are going to be carving for with the **–t** command. If we are unsure what we want to look for and tell it to gives us every file foremost knows about, we simply

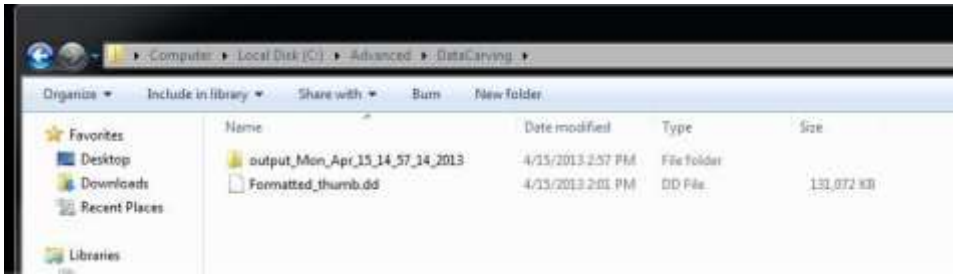
exclude the flag from the command. In the above example if we wanted to carve everything from the image we would type: **foremost.exe –T –i**

Formatted_thumb.dd.

c. Let the program run until complete. This could take a while depending on how big the image being carved is and how many different files you are looking for.

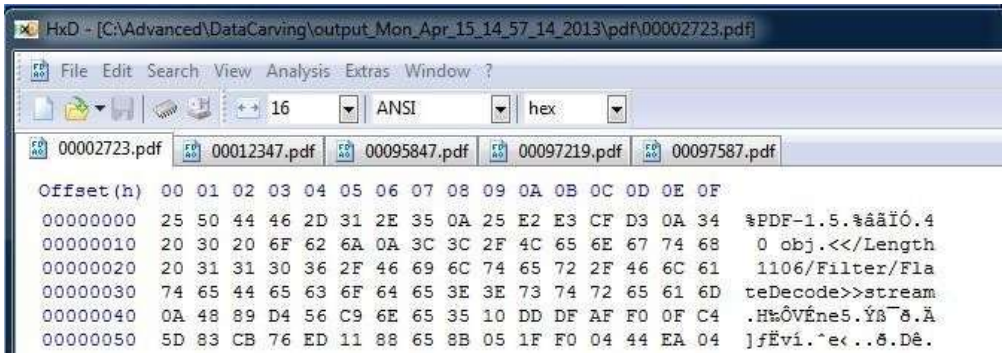
4. Navigate to the data carving folder in any file window. It is under Computer > C:

> Advanced > DataCarving. Once in there we see an output folder and if we used **–T** then it has a date associated with it.



5. Go into the output folder and we will see a folder for each file we searched for. In this example it is called pdf. Search in the folder and look at the pdfs found in the image.

6. Open HxD (the hex editor we use) and use it to open any of the pdfs.



By seeing the first couple of bytes we can see the header for the pdf files. Recall from the config file that foremost looks for the signature of bytes that gives us the ascii **%PDF**.

Take some time to carve out different types of files from the image and see what is contained on the thumbdrive.

Review:

The image is a thumbdrive which contained files on it. The thumbdrive was then reformatted without being wiped. This gives us an image which cannot be viewed through normal means, but the files still exist. We used foremost to pull files from the image to be viewed later.

Praktikum 8
Report Investigation

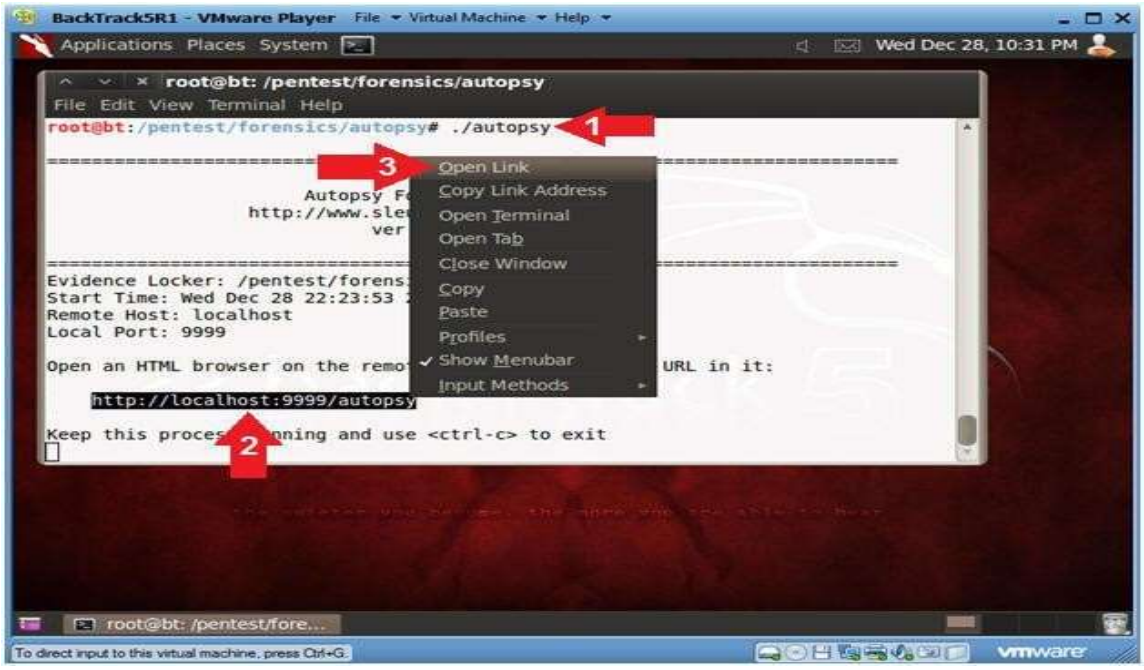
Pretest:

1. Tulislah alasan mengapa kita perlu membuat report forensik!

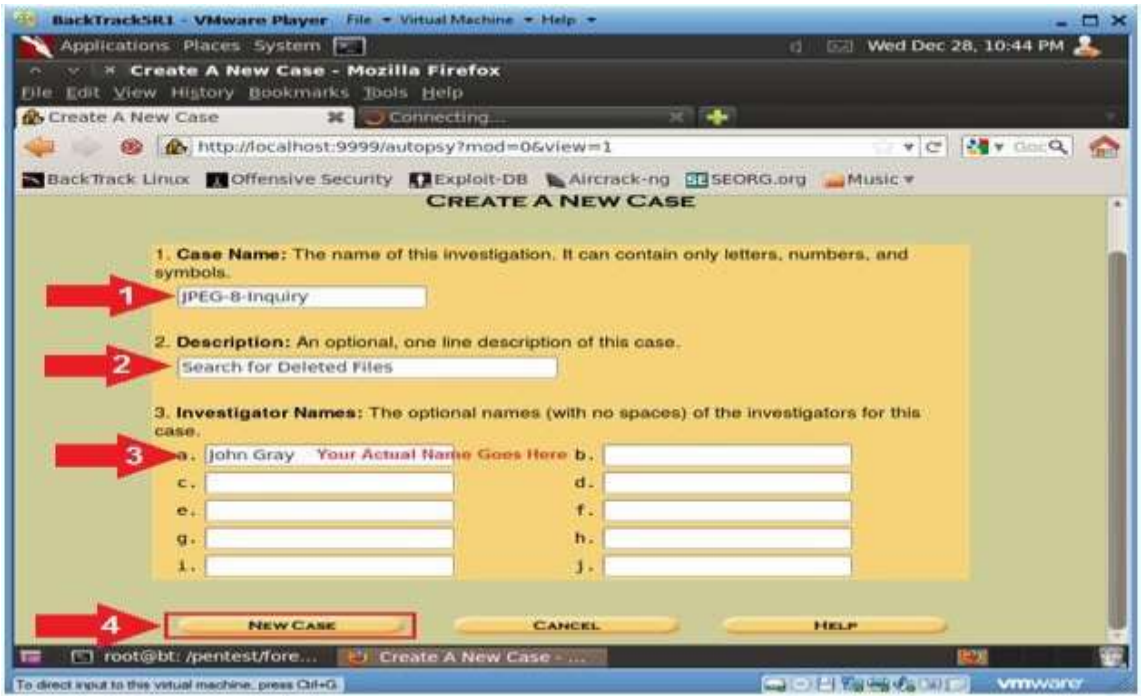
Download panduan lengkap pada *bit.ly/panduanlengkap08*
Referensi pada *http://bit.ly/referensi08*

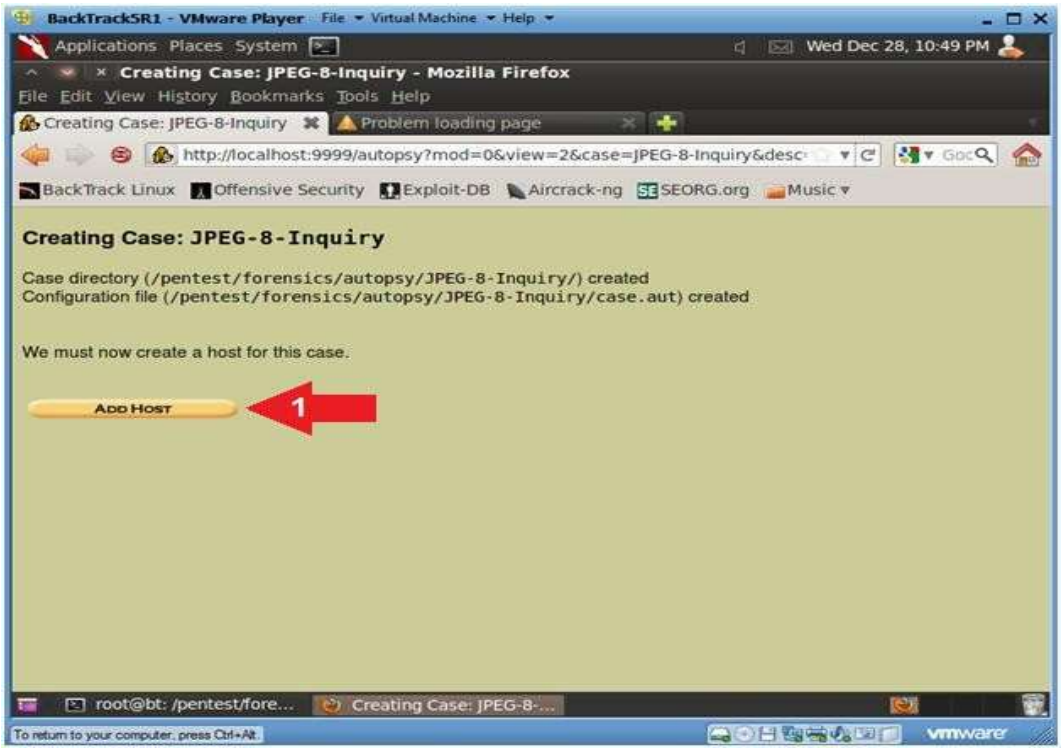
Langkah Praktikum:

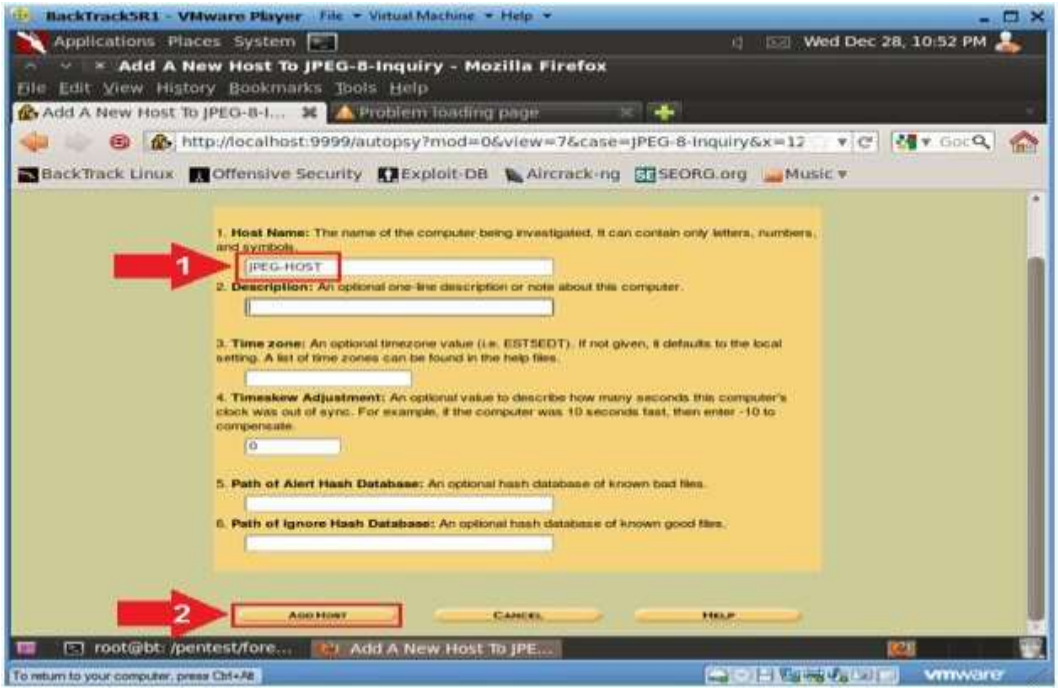
The Autopsy Forensic Browser enables you to conduct a digital forensic investigation. It is a graphical interface to The Sleuth Kit and other tools. This guide covers information about using Autopsy version 3 on Windows. This manual is for users with above average computer skills who have a basic understanding of digital forensics concepts.

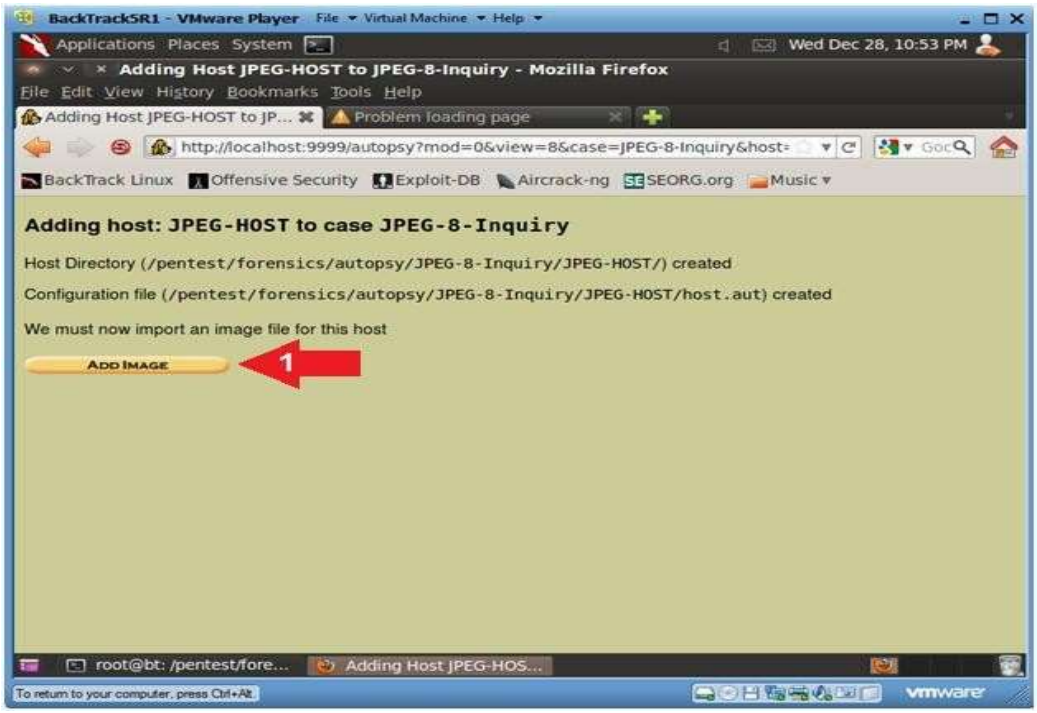


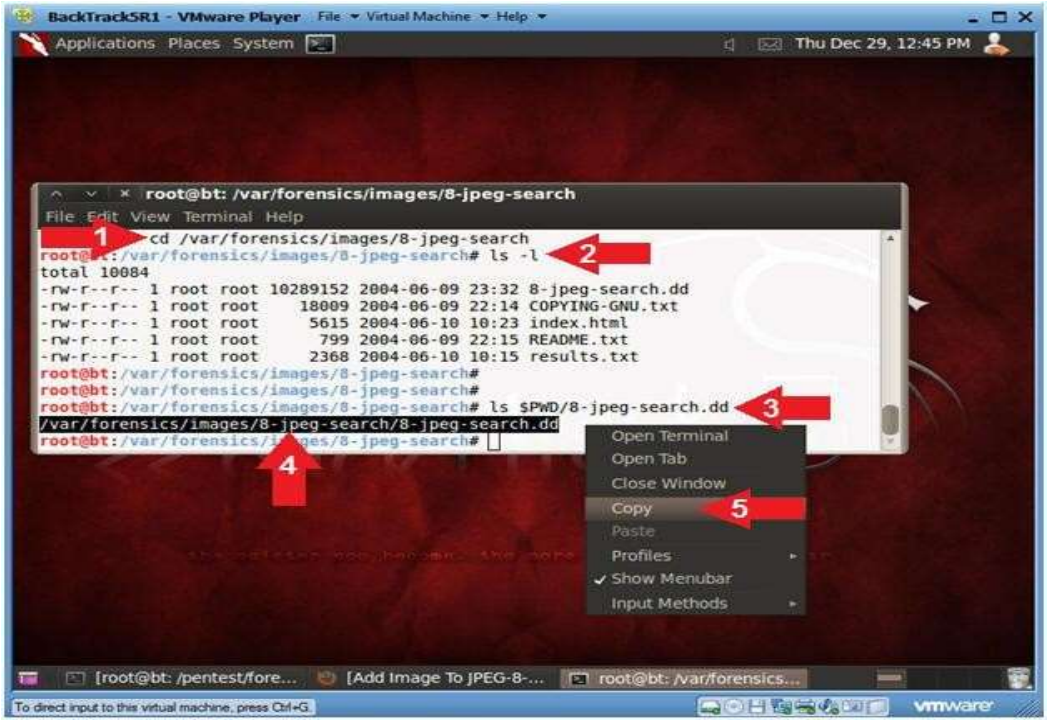

BackTrackSR1 - VMware Player File Virtual Machine Help
Applications Places System
Wed Dec 28, 10:34 PM
Autopsy Forensic Browser - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Autopsy Forensic Browser
http://localhost:9999/autopsy
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
Autopsy Forensic Browser 2.24
http://www.sleuthkit.org/autopsy/
OPEN CASE
NEW CASE
HELP
1
root@bt: /pentest/fore...
Autopsy Forensic
To direct input to this virtual machine, press Ctrl+G
vmware

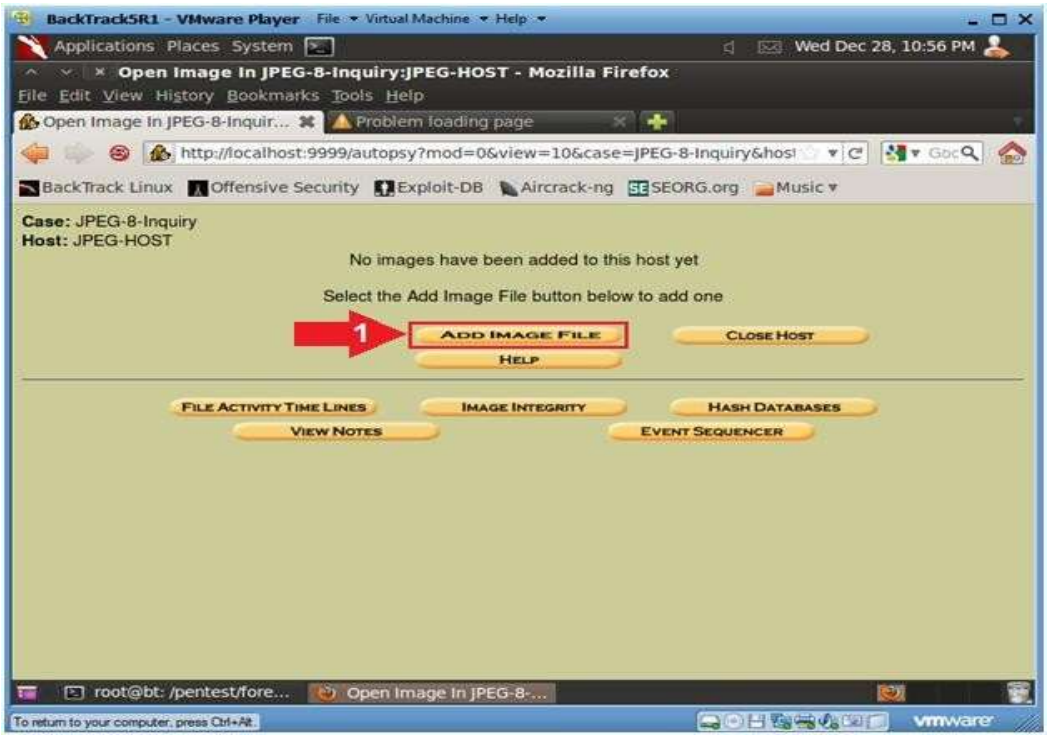

BackTrackSR1 - VMware Player File Virtual Machine Help
Applications Places System
Wed Dec 28, 10:44 PM
Create A New Case - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Create A New Case
Connecting...
http://localhost:9999/autopsy?mod=06&view=1
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
1
JPEG-8-Inquiry
2. Description: An optional, one line description of this case.
2
Search for Deleted Files
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
3
a. John Gray Your Actual Name Goes Here
b.
c.
d.
e.
f.
g.
h.
i.
j.
4
NEW CASE
CANCEL
HELP
root@bt: /pentest/fore...
Create A New Case - ...
To direct input to this virtual machine, press Ctrl+G
vmware

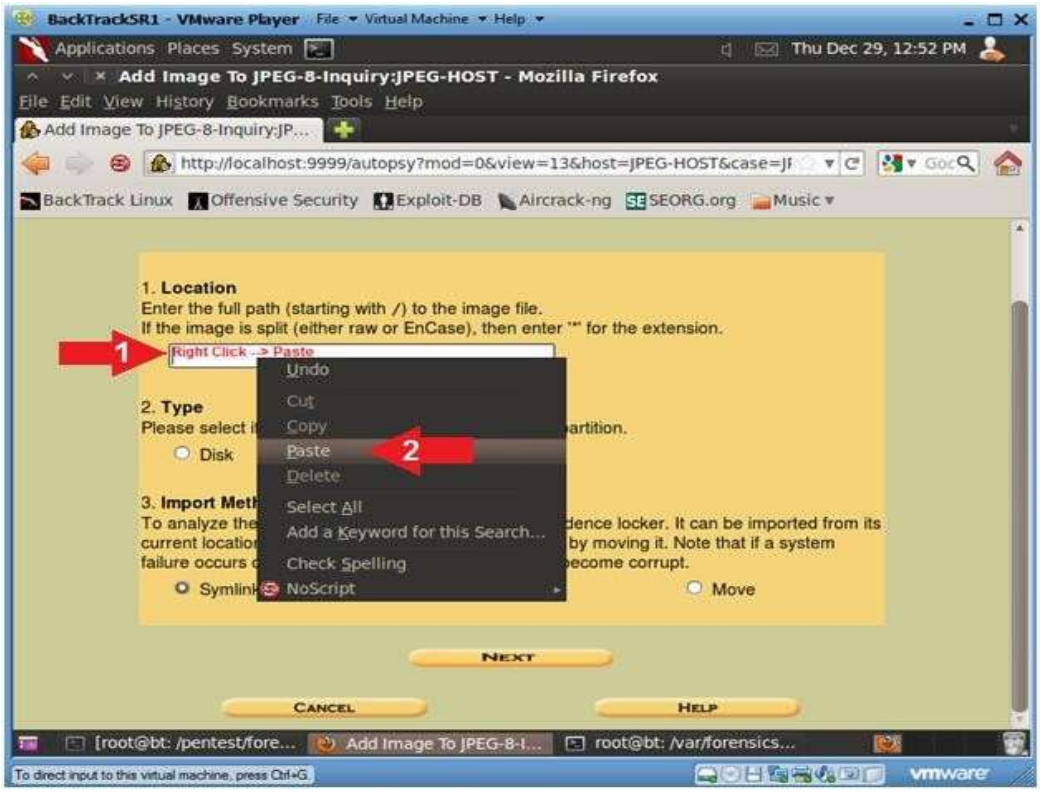

BackTrack5R1 - VMware Player
Applications Places System
Wed Dec 28, 10:49 PM
Creating Case: JPEG-8-Inquiry - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Creating Case: JPEG-8-Inquiry
Problem loading page
http://localhost:9999/autopsy?mod=0&view=2&case=JPEG-8-Inquiry&desc
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Creating Case: JPEG-8-Inquiry
Case directory (/pentest/forensics/autopsy/JPEG-8-Inquiry/) created
Configuration file (/pentest/forensics/autopsy/JPEG-8-Inquiry/case.aut) created
We must now create a host for this case.
ADD HOST
1
root@bt: /pentest/fore...
Creating Case: JPEG-8-...
To return to your computer, press Ctrl+Alt
vmware

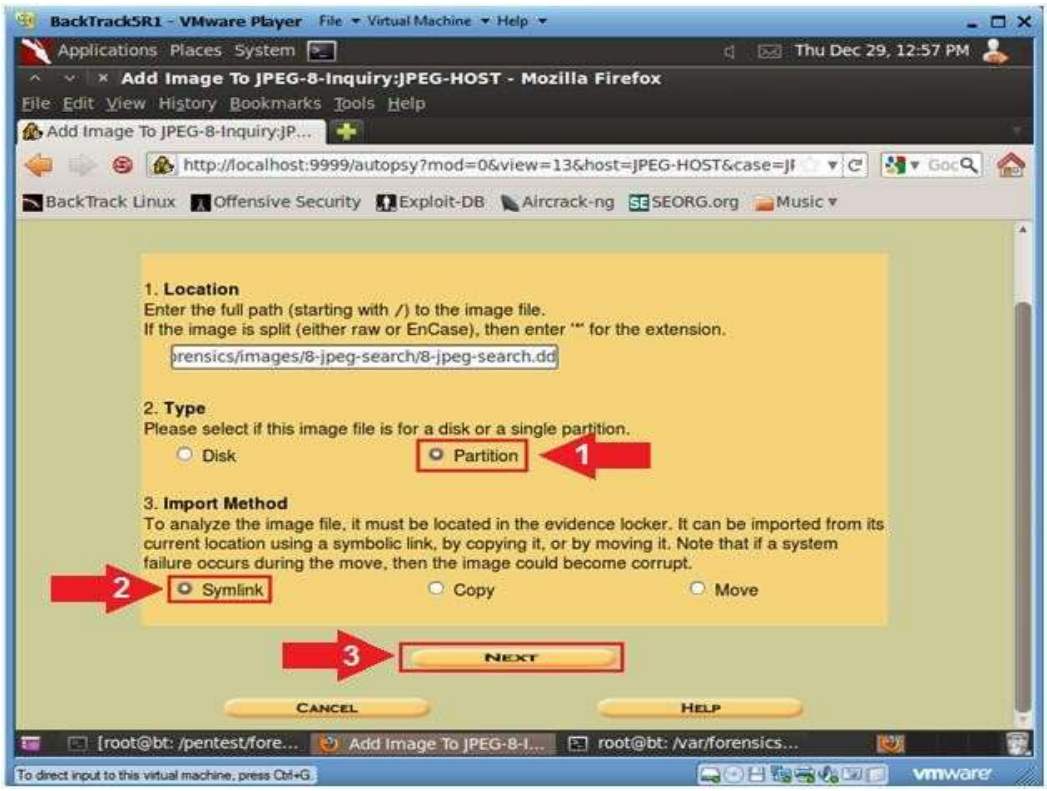

BackTrack5R1 - VMware Player
Applications Places System
Wed Dec 28, 10:52 PM
Add A New Host To JPEG-8-Inquiry - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Add A New Host To JPEG-8-I...
Problem loading page
http://localhost:9999/autopsy?mod=0&view=7&case=JPEG-8-Inquiry&x=12
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
1
JPEG-HOST
2. Description: An optional one-line description or note about this computer.
3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0
5. Path of Alert Hash Database: An optional hash database of known bad files.
6. Path of Ignore Hash Database: An optional hash database of known good files.
2
ADD HOST
CANCEL
HELP
root@bt: /pentest/fore...
Add A New Host To JPE...
To return to your computer, press Ctrl+Alt
vmware

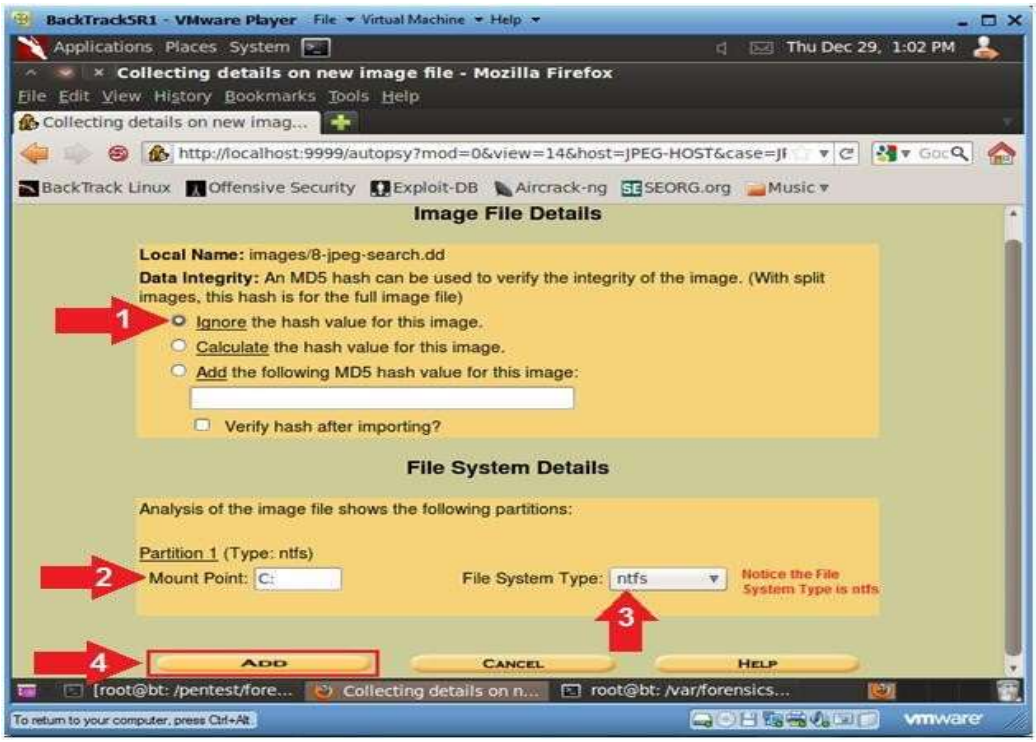

BackTrack5R1 - VMware Player
Applications Places System
Wed Dec 28, 10:53 PM
Adding Host JPEG-HOST to JPEG-8-Inquiry - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Problem loading page
http://localhost:9999/autopsy?mod=0&view=8&case=JPEG-8-Inquiry&host=
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Adding host: JPEG-HOST to case JPEG-8-Inquiry
Host Directory (/pentest/forensics/autopsy/JPEG-8-Inquiry/JPEG-HOST/) created
Configuration file (/pentest/forensics/autopsy/JPEG-8-Inquiry/JPEG-HOST/host.aut) created
We must now import an image file for this host
ADD IMAGE
1
root@bt: /pentest/fore...
Adding Host JPEG-HOS...
To return to your computer, press Ctrl+Alt.
vmware

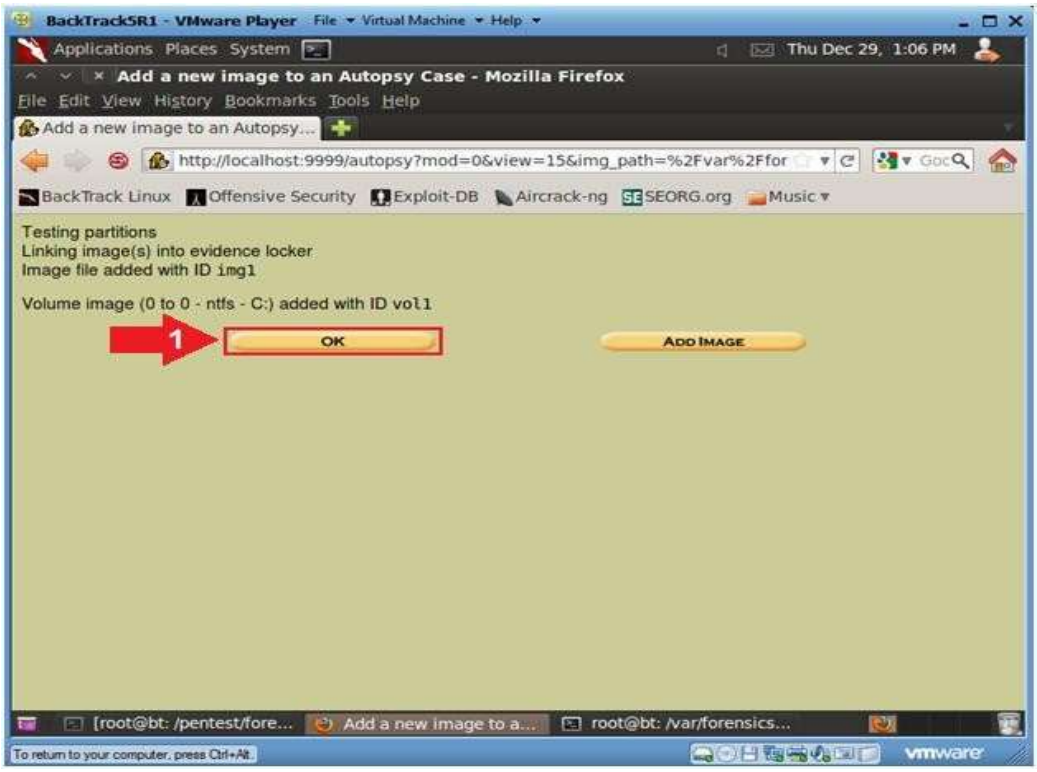

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 12:45 PM
root@bt: /var/forensics/images/8-jpeg-search
File Edit View Terminal Help
1
cd /var/forensics/images/8-jpeg-search
root@bt:/var/forensics/images/8-jpeg-search# ls -l
2
total 10084
-rw-r--r-- 1 root root 10289152 2004-06-09 23:32 8-jpeg-search.dd
-rw-r--r-- 1 root root 18009 2004-06-09 22:14 COPYING-GNU.txt
-rw-r--r-- 1 root root 5615 2004-06-10 10:23 index.html
-rw-r--r-- 1 root root 799 2004-06-09 22:15 README.txt
-rw-r--r-- 1 root root 2368 2004-06-10 10:15 results.txt
root@bt:/var/forensics/images/8-jpeg-search#
root@bt:/var/forensics/images/8-jpeg-search#
root@bt:/var/forensics/images/8-jpeg-search# ls $PWD/8-jpeg-search.dd
3
/var/forensics/images/8-jpeg-search/8-jpeg-search.dd
root@bt:/var/forensics/images/8-jpeg-search#
4
Open Terminal
Open Tab
Close Window
Copy
5
Paste
Profiles
Show Menubar
Input Methods
[root@bt: /pentest/fore...
[Add Image To JPEG-8-...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G.
vmware


BackTrack5R1 - VMware Player
Applications Places System
Wed Dec 28, 10:56 PM
Open Image In JPEG-8-Inquiry:JPEG-HOST - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Problem loading page
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Case: JPEG-8-Inquiry
Host: JPEG-HOST
No images have been added to this host yet
Select the Add Image File button below to add one
1
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
root@bt: /pentest/fore...
To return to your computer, press Ctrl+Alt.
vmware

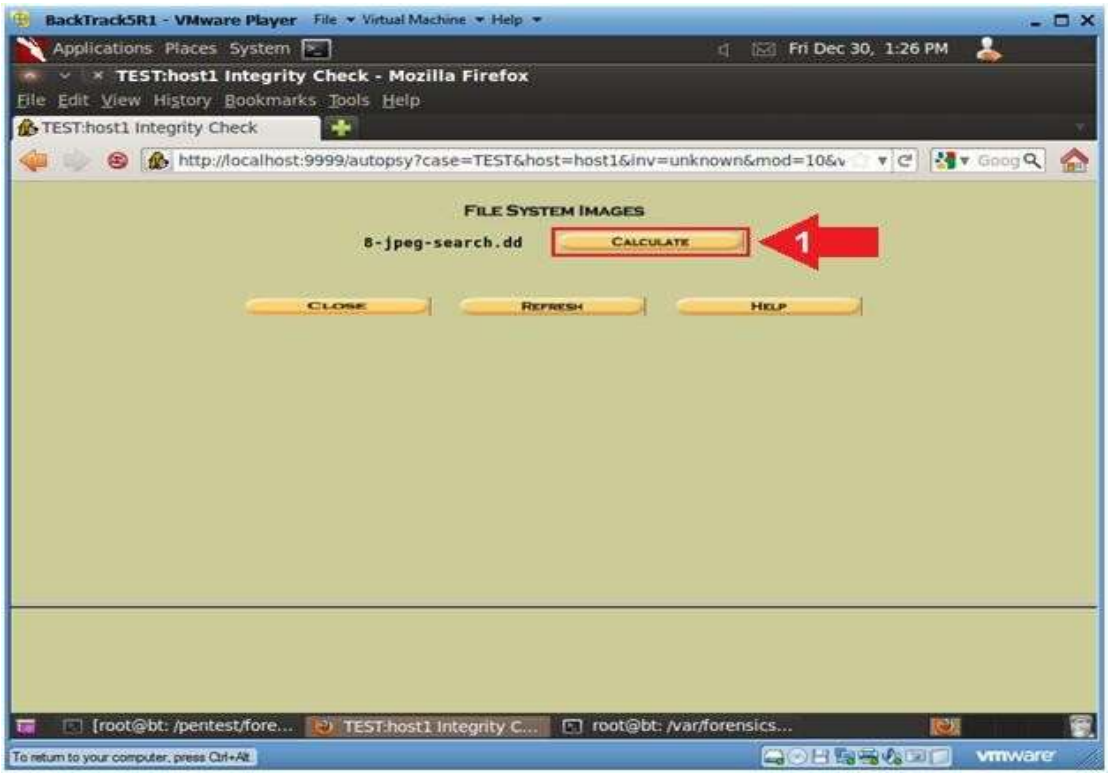

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 12:52 PM
Add Image To JPEG-8-Inquiry:JPEG-HOST - Mozilla Firefox
File Edit View History Bookmarks Tools Help
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
1
Right Click --> Paste
Undo
Cut
Copy
Paste
2
Delete
Select All
Add a Keyword for this Search...
Check Spelling
NoScript
2. Type
Disk
Move
NEXT
CANCEL
HELP
[root@bt: /pentest/fore...
Add Image To JPEG-8-I...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G.
vmware

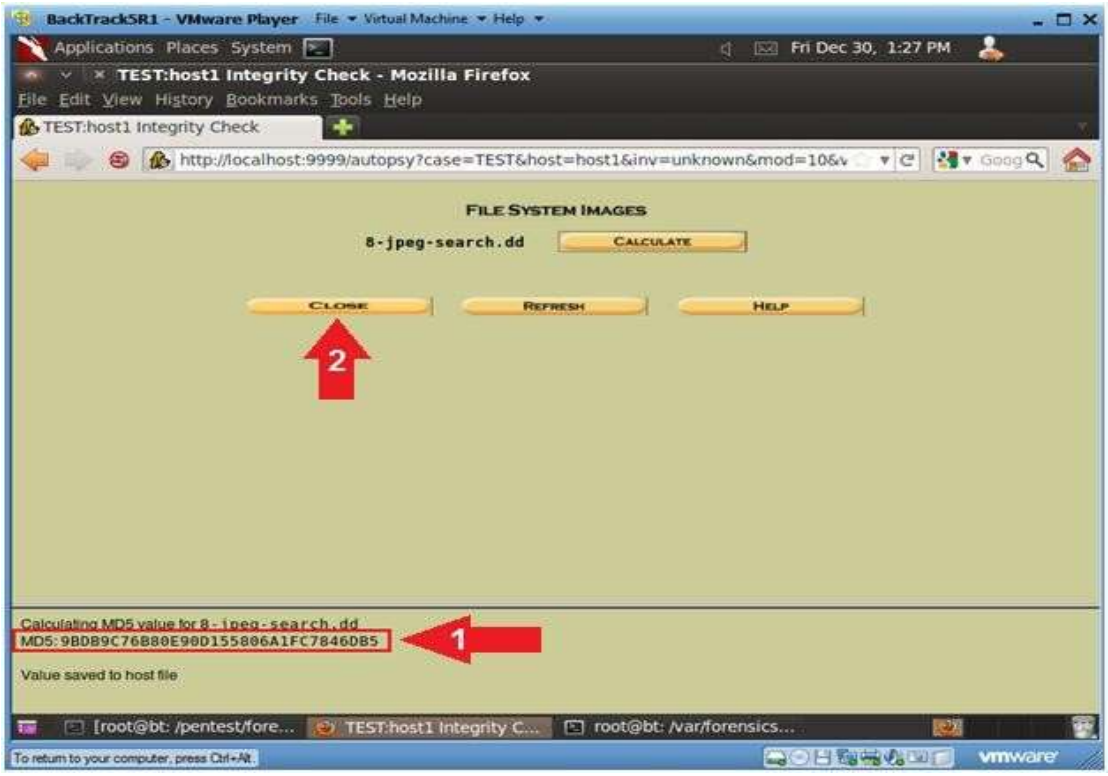

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 12:57 PM
Add Image To JPEG-8-Inquiry:JPEG-HOST - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=13&host=JPEG-HOST&case=J
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
orensics/images/8-jpeg-search/8-jpeg-search.dd
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
1
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
2
Symlink
Copy
Move
3
NEXT
CANCEL
HELP
[root@bt: /pentest/fore...
Add Image To JPEG-8-I...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G
vmware

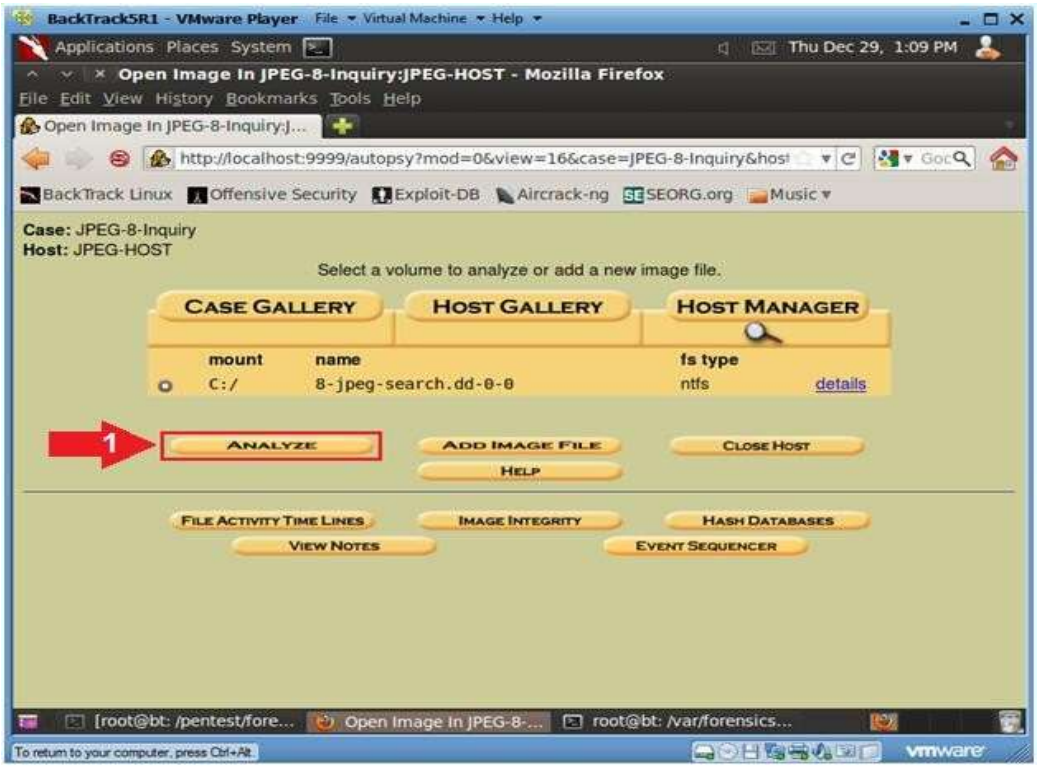

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:02 PM
Collecting details on new image file - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=14&host=JPEG-HOST&case=J
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Image File Details
Local Name: images/8-jpeg-search.dd
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
1
Ignore the hash value for this image.
Calculate the hash value for this image.
Add the following MD5 hash value for this image:
Verify hash after importing?
File System Details
Analysis of the image file shows the following partitions:
Partition 1 (Type: ntfs)
2
Mount Point: C:
File System Type: ntfs
Notice the File System Type is ntfs
3
4
ADD
CANCEL
HELP
[root@bt: /pentest/fore...
Collecting details on n...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware

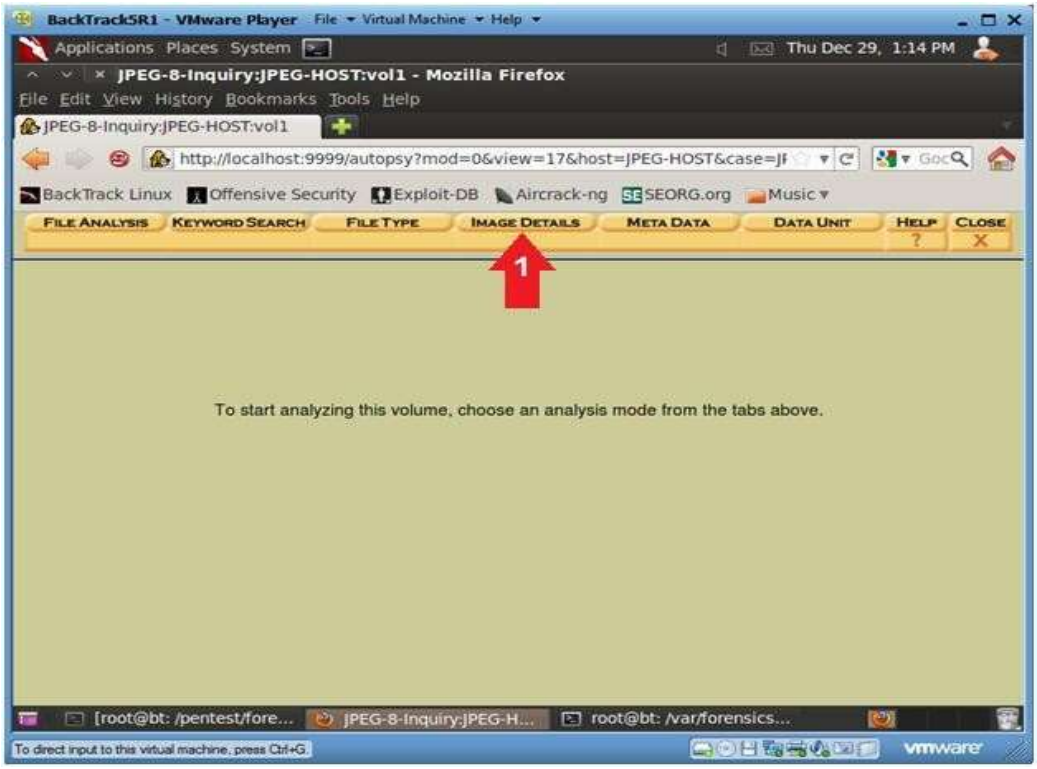

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:06 PM
Add a new image to an Autopsy Case - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Add a new image to an Autopsy...
http://localhost:9999/autopsy?mod=0&view=15&img_path=%2Fvar%2Ffor
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Volume image (0 to 0 - ntfs - C:) added with ID vol1
1
OK
ADD IMAGE
[root@bt: /pentest/fore...
Add a new image to a...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

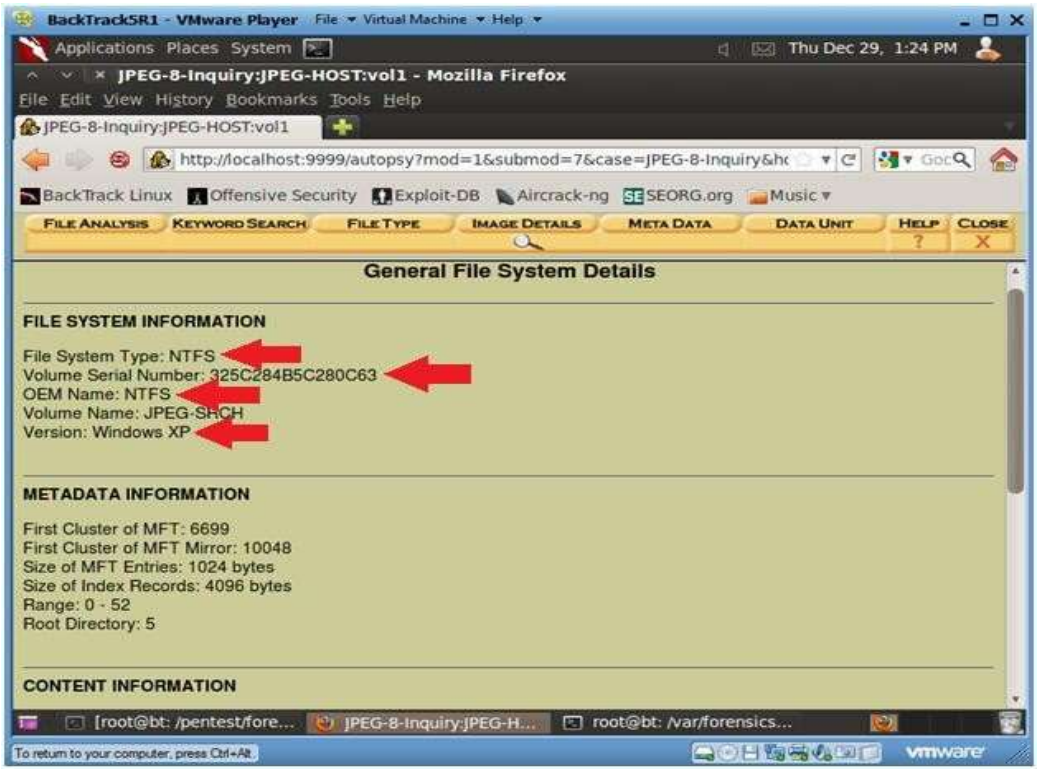

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 12:03 PM
Open Image In JPEG-8-Inquiry:JPEG-HOST - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Open Image In JPEG-8-Inquiry:J...
http://localhost:9999/autopsy?mod=0&view=10&case=JPEG-8-Inquiry&host=JPEG
Case: JPEG-8-Inquiry
Host: JPEG-HOST
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
8-jpeg-search.dd-0-0
ntfs
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
1
[root@bt: /pentest/fore...
Open Image In JPEG-8-...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware


BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 1:26 PM
TEST:host1 Integrity Check - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TEST:host1 Integrity Check
http://localhost:9999/autopsy?case=TEST&host=host1&inv=unknown&mod=10&v
FILE SYSTEM IMAGES
8-jpeg-search.dd
CALCULATE
1
CLOSE
REFRESH
HELP
[root@bt: /pentest/fore...
TEST:host1 Integrity C...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware

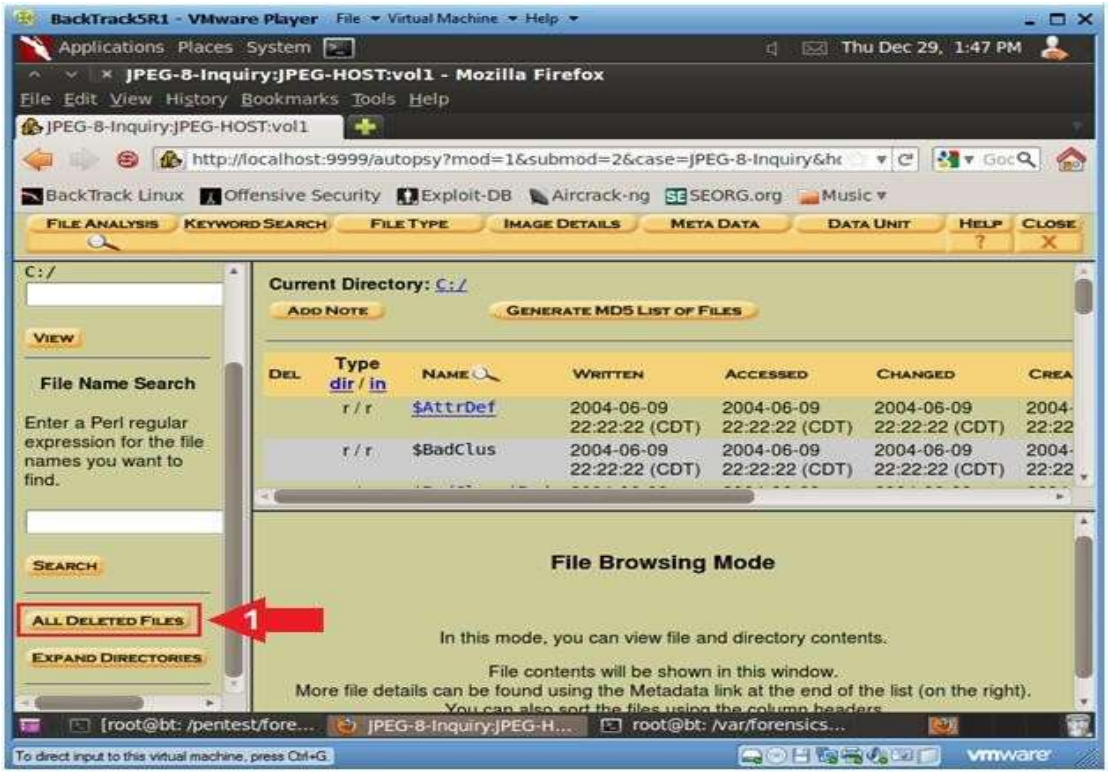

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 1:27 PM
TEST:host1 Integrity Check - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TEST:host1 Integrity Check
http://localhost:9999/autopsy?case=TEST&host=host1&inv=unknown&mod=10&v
FILE SYSTEM IMAGES
8-jpeg-search.dd
CALCULATE
CLOSE
REFRESH
HELP
2
Calculating MD5 value for 8-jpeg-search.dd
MD5: 9BDB9C76B80E90D155806A1FC7846DB5
1
Value saved to host file
[root@bt: /pentest/fore...
TEST:host1 Integrity C...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware


BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:09 PM
Open Image In JPEG-8-Inquiry:JPEG-HOST - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=16&case=JPEG-8-Inquiry&host
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Case: JPEG-8-Inquiry
Host: JPEG-HOST
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
8-jpeg-search.dd-0-0
ntfs
details
1
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
[root@bt: /pentest/fore...
Open Image In JPEG-8-...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware


BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:14 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=17&host=JPEG-HOST&case=J
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
1
To start analyzing this volume, choose an analysis mode from the tabs above.
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G
vmware

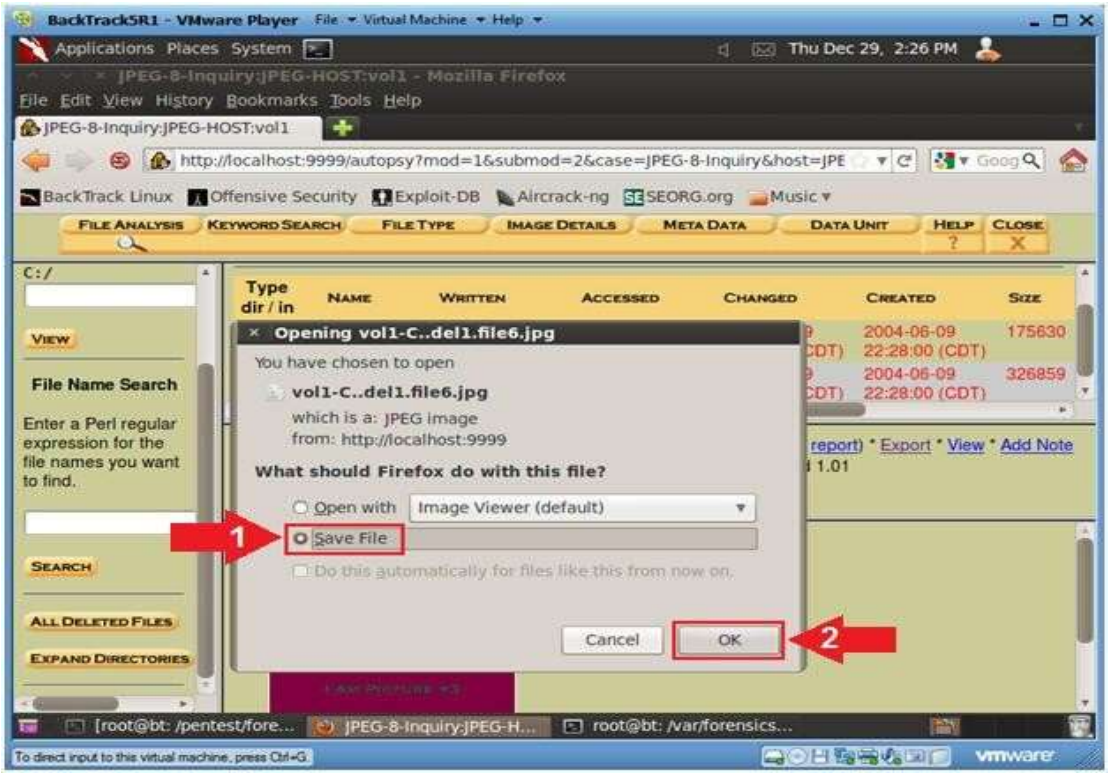

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:24 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=1&submod=7&case=JPEG-8-Inquiry&hc
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
General File System Details
FILE SYSTEM INFORMATION
File System Type: NTFS
Volume Serial Number: 325C284B5C280C63
OEM Name: NTFS
Volume Name: JPEG-SRCH
Version: Windows XP
METADATA INFORMATION
First Cluster of MFT: 6699
First Cluster of MFT Mirror: 10048
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 52
Root Directory: 5
CONTENT INFORMATION
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware

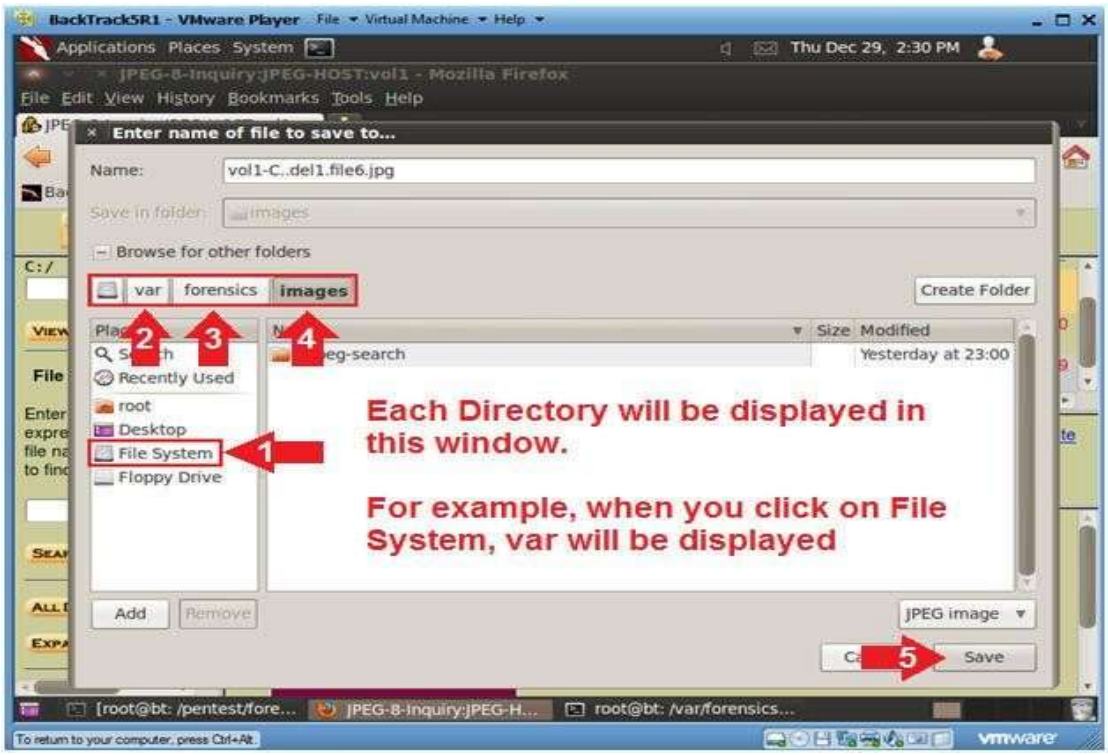

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:47 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&hc
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
1
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
Current Directory: C:/
ADD NOTE
GENERATE MD5 LIST OF FILES
DEL
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREA
r / r
$AttrDef
2004-06-09 22:22:22 (CDT)
2004-06-09 22:22:22 (CDT)
2004-06-09 22:22:22 (CDT)
r / r
$BadClus
2004-06-09 22:22:22 (CDT)
2004-06-09 22:22:22 (CDT)
2004-06-09 22:22:22 (CDT)
File Browsing Mode
In this mode, you can view file and directory contents.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G
vmware

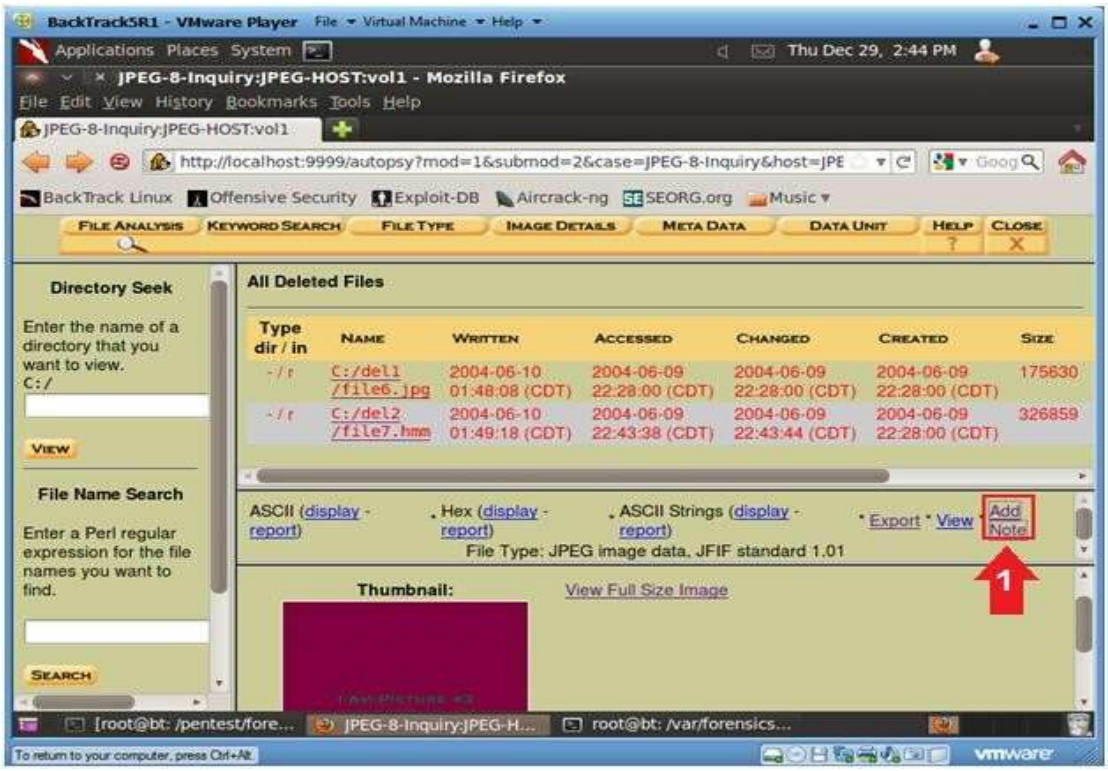

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:47 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
Current Directory: C:/
ADD NOTE
GENERATE MD5 LIST OF FILES
DEL
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
$AttrDef
$BadClus
2004-06-09 22:22:22 (CDT)
File Browsing Mode
In this mode, you can view file and directory contents.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
1
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G
vmware

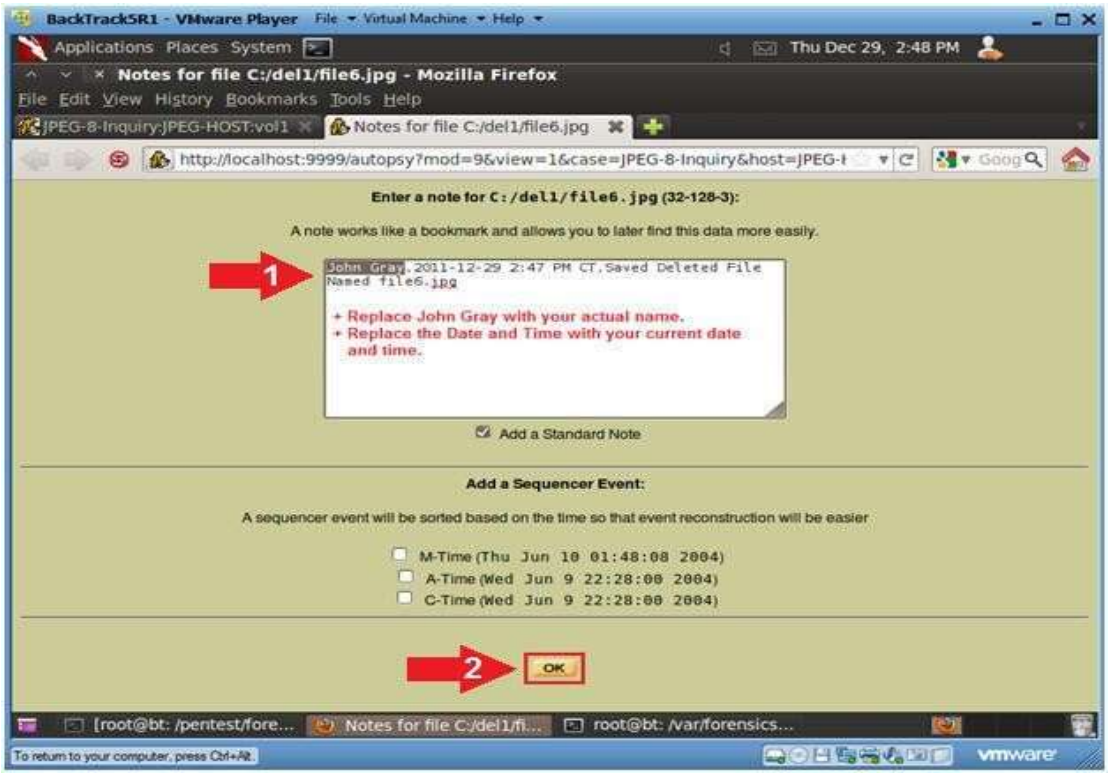

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 1:57 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
All Deleted Files
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREATED
SIZE
UID
GID
C:/del1 /file6.jpg
2004-06-10 01:48:08 (CDT)
2004-06-09 22:28:00 (CDT)
175630
C:/del2 /file7.hmm
2004-06-10 01:49:18 (CDT)
2004-06-09 22:43:38 (CDT)
2004-06-09 22:43:44 (CDT)
326859
File Browsing Mode
In this mode, you can view file and directory contents.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
1
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

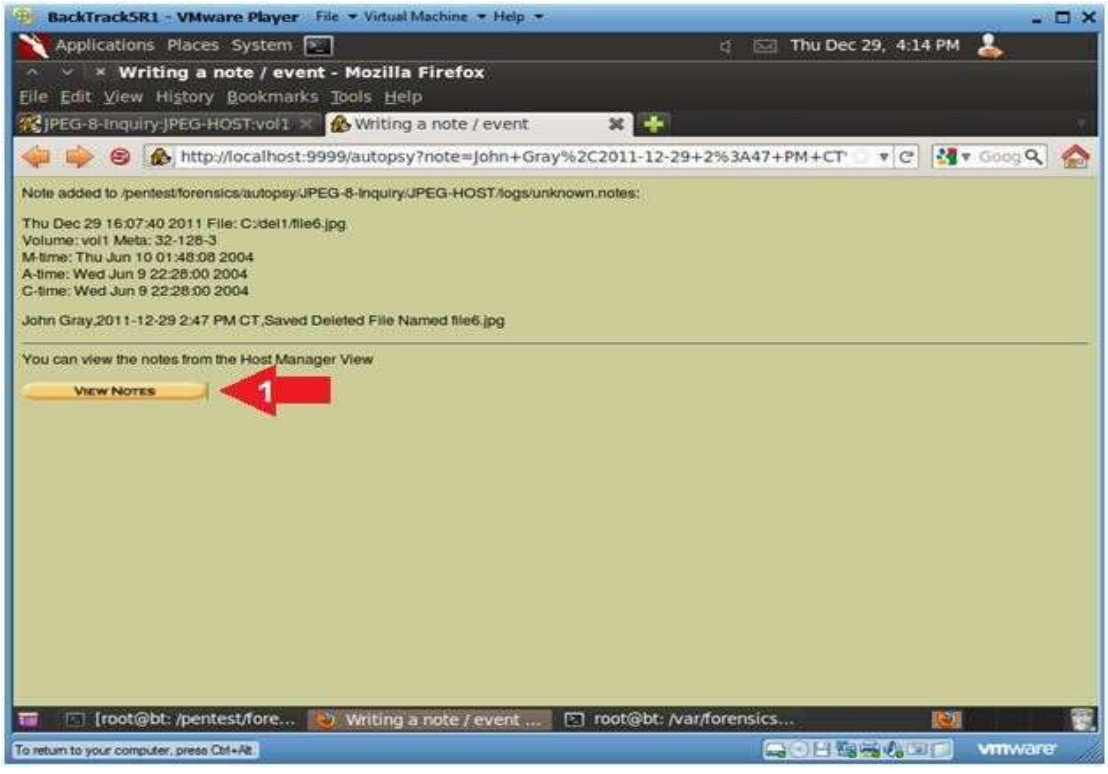

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 2:04 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPEG-HOST&inv=
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREATED
SIZE
UID
GID
C:/del1/file6.jpg
2004-06-10 01:48:08 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
175630
C:/del2/file7.hmm
2004-06-10 01:49:18 (CDT)
2004-06-09 22:43:38 (CDT)
2004-06-09 22:43:44 (CDT)
2004-06-09 22:28:00 (CDT)
326859
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01
Deleted File Recovery Mode
1
Click on the Export link to undelete and save the deleted file.
C:/del1/file6.jpg
Thumbnail:
View Full Size Image
Notice Autopsy tries to display a thumbnail of the file selected.
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware


BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 2:26 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREATED
SIZE
2004-06-09 22:28:00 (CDT)
175630
2004-06-09 22:28:00 (CDT)
326859
Opening vol1-C..del1.file6.jpg
You have chosen to open
vol1-C..del1.file6.jpg
which is a: JPEG image
from: http://localhost:9999
What should Firefox do with this file?
Open with
Image Viewer (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK
1
2
report) * Export * View * Add Note
1.01
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G.
vmware

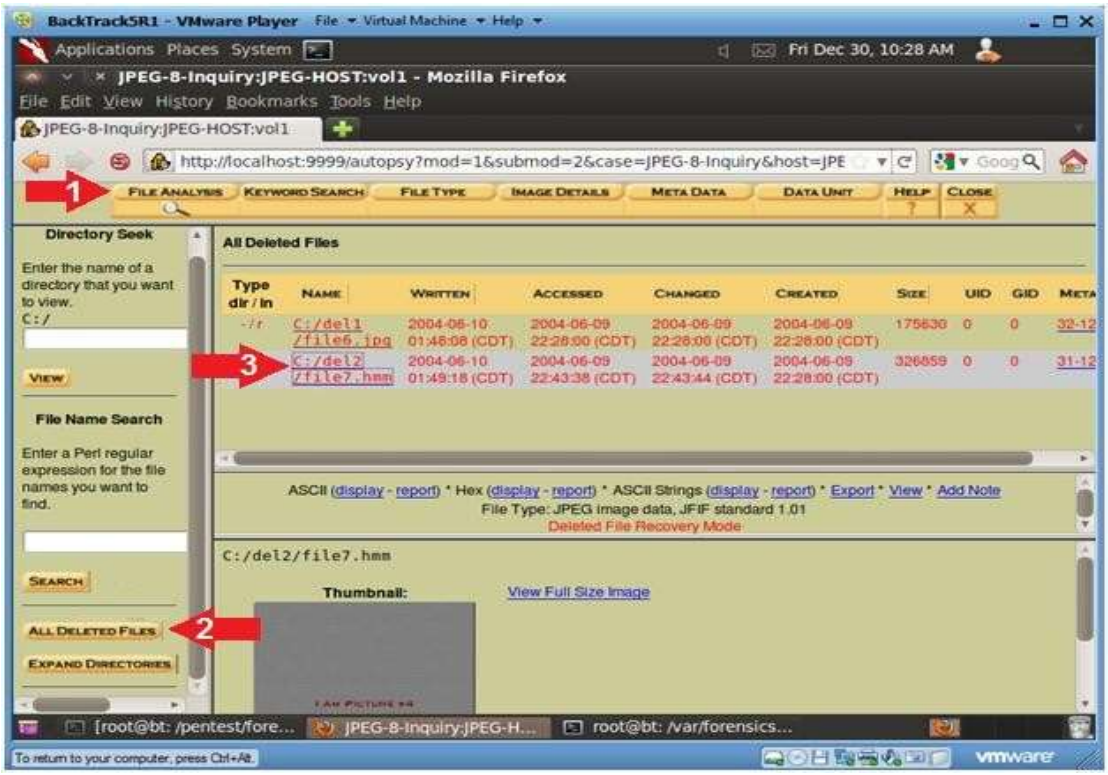

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 2:30 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Enter name of file to save to...
Name:
vol1-C..del1.file6.jpg
Save in folder:
images
Browse for other folders
var
forensics
images
Create Folder
Recently Used
root
Desktop
File System
Floppy Drive
Size
Modified
Yesterday at 23:00
Each Directory will be displayed in this window.
For example, when you click on File System, var will be displayed
Add
Remove
JPEG image
Save
1
2
3
4
5
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

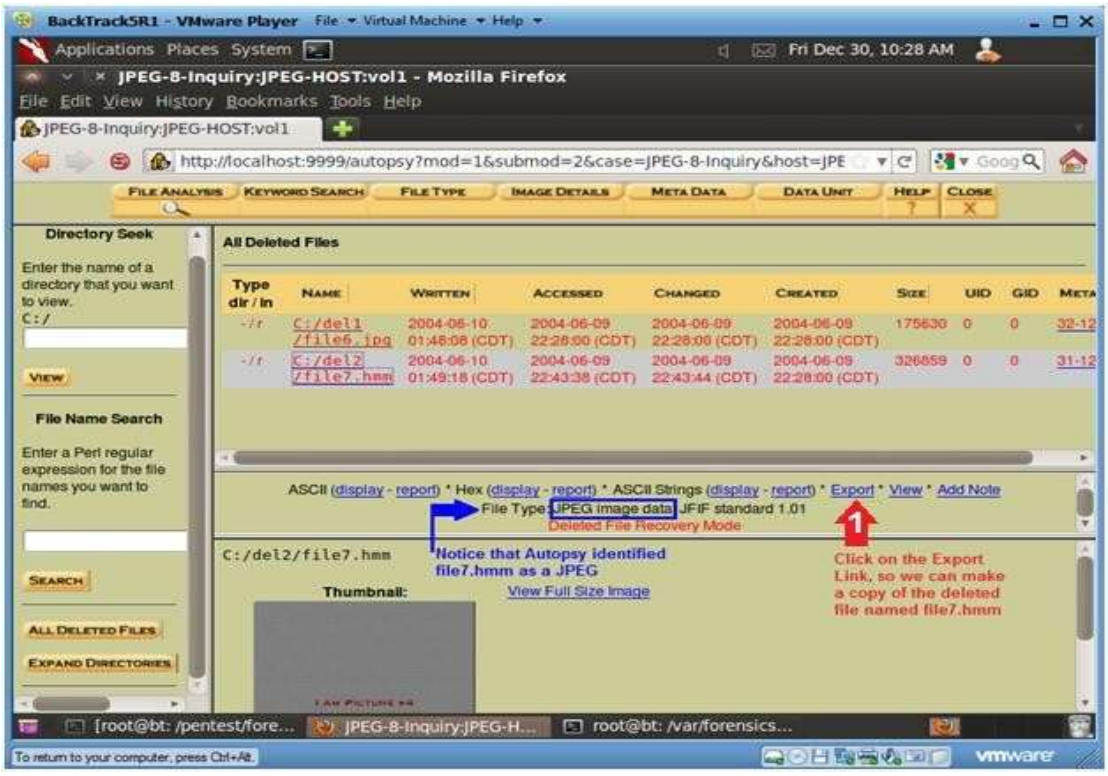

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 2:44 PM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
All Deleted Files
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREATED
SIZE
-/r
C:/del1 /file6.jpg
2004-06-10 01:48:08 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
175630
-/r
C:/del2 /file7.hmm
2004-06-10 01:49:18 (CDT)
2004-06-09 22:43:38 (CDT)
2004-06-09 22:43:44 (CDT)
2004-06-09 22:28:00 (CDT)
326859
ASCII (display - report)
Hex (display - report)
ASCII Strings (display - report)
Export
View
Add Note
File Type: JPEG image data, JFIF standard 1.01
Thumbnail:
View Full Size Image
1
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

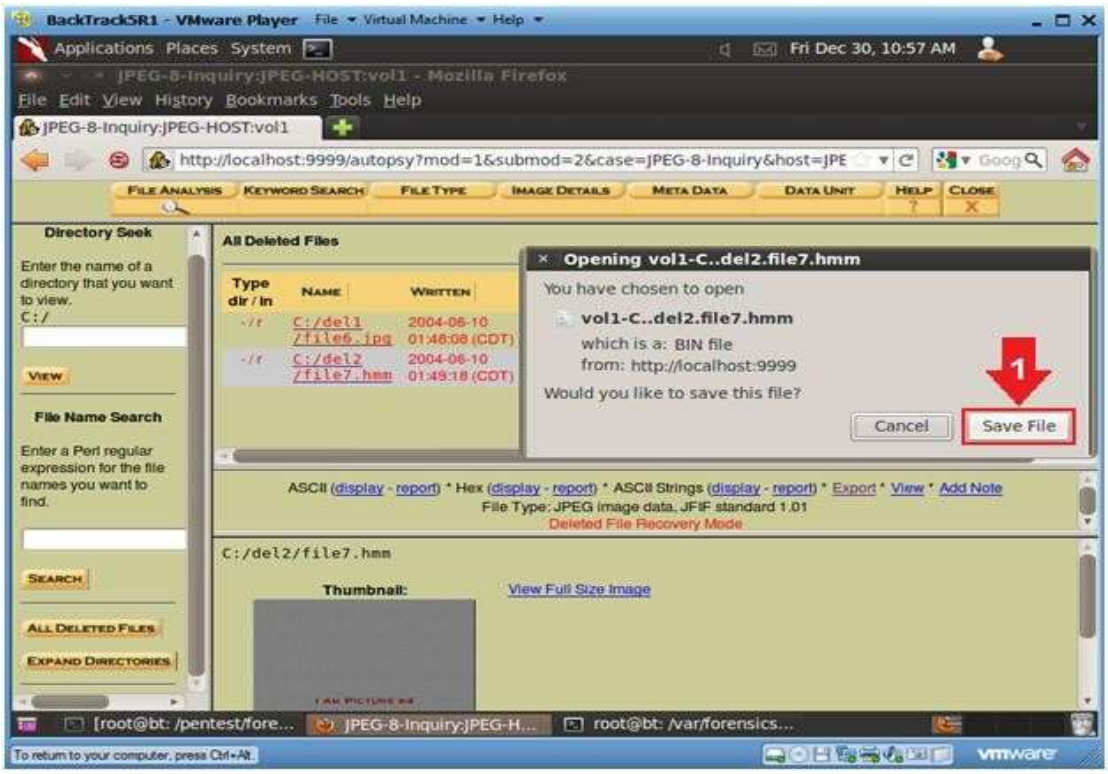

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 2:48 PM
Notes for file C:/del1/file6.jpg - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
Notes for file C:/del1/file6.jpg
http://localhost:9999/autopsy?mod=9&view=1&case=JPEG-8-Inquiry&host=JPEG-I
Enter a note for C:/del1/file6.jpg (32-128-3):
A note works like a bookmark and allows you to later find this data more easily.
1
John Gray,2011-12-29 2:47 PM CT,Saved Deleted File Named file6.jpg
+ Replace John Gray with your actual name.
+ Replace the Date and Time with your current date and time.
Add a Standard Note
Add a Sequencer Event:
A sequencer event will be sorted based on the time so that event reconstruction will be easier
M-Time (Thu Jun 10 01:48:08 2004)
A-Time (Wed Jun 9 22:28:00 2004)
C-Time (Wed Jun 9 22:28:00 2004)
2
OK
[root@bt: /pentest/fore...
Notes for file C:/del1/fi...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware

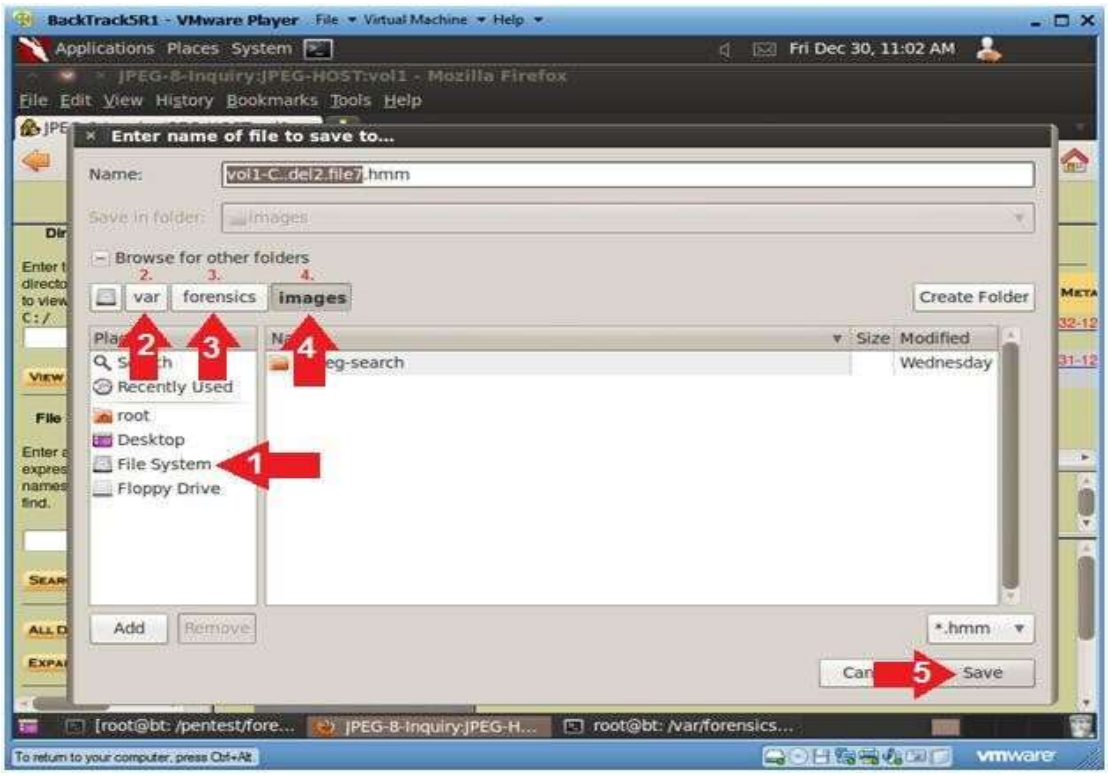

BackTrack5R1 - VMware Player
Applications Places System
Thu Dec 29, 4:14 PM
Writing a note / event - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
Writing a note / event
http://localhost:9999/autopsy?note=John+Gray%2C2011-12-29+2%3A47+PM+CT
Note added to /pentest/forensics/autopsy/JPEG-8-Inquiry/JPEG-HOST/logs/unknown.notes:
Thu Dec 29 16:07:40 2011 File: C:/del1/file6.jpg
Volume: vol1 Meta: 32-128-3
M-time: Thu Jun 10 01:48:08 2004
A-time: Wed Jun 9 22:28:00 2004
C-time: Wed Jun 9 22:28:00 2004
John Gray,2011-12-29 2:47 PM CT,Saved Deleted File Named file6.jpg
You can view the notes from the Host Manager View
VIEW NOTES
1
[root@bt: /pentest/fore...
Writing a note / event ...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware

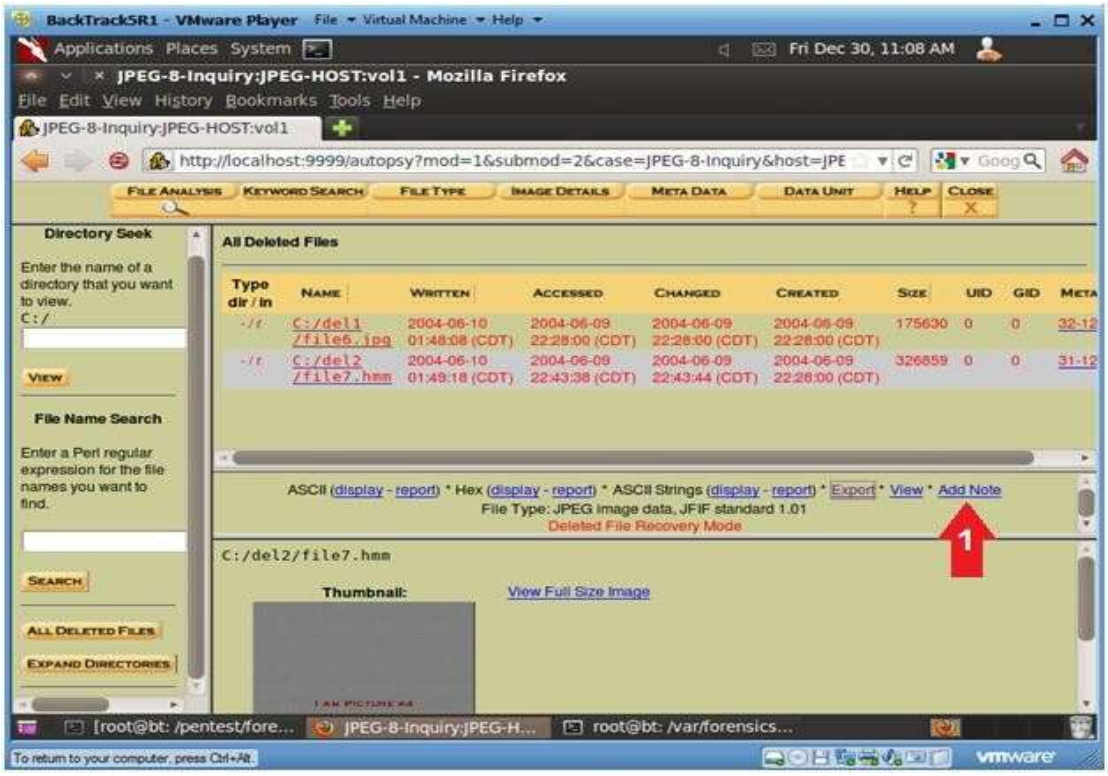

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 10:13 AM
Contents of Notes File - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
Contents of Notes File
Thu Dec 29 16:07:40 2011
File: C:/del1/file6.jpg
Volume: vol1 Meta: 32-128-3
M-time: Thu Jun 10 01:46:08 2004
A-time: Wed Jun 9 22:28:00 2004
C-time: Wed Jun 9 22:28:00 2004
This is the parent window tab.
Do NOT close this tab.
This is the child window tab.
Close this tab window.
John Gray,2011-12-29 2:47 PM CT,Saved Deleted File Named file6.jpg
CLOSE
REFRESH
1
[root@bt: /pentest/fore...
Contents of Notes File ...
root@bt: /var/forensics...
1 Item in Trash
To direct input to this virtual machine, press Ctrl+G
vmware

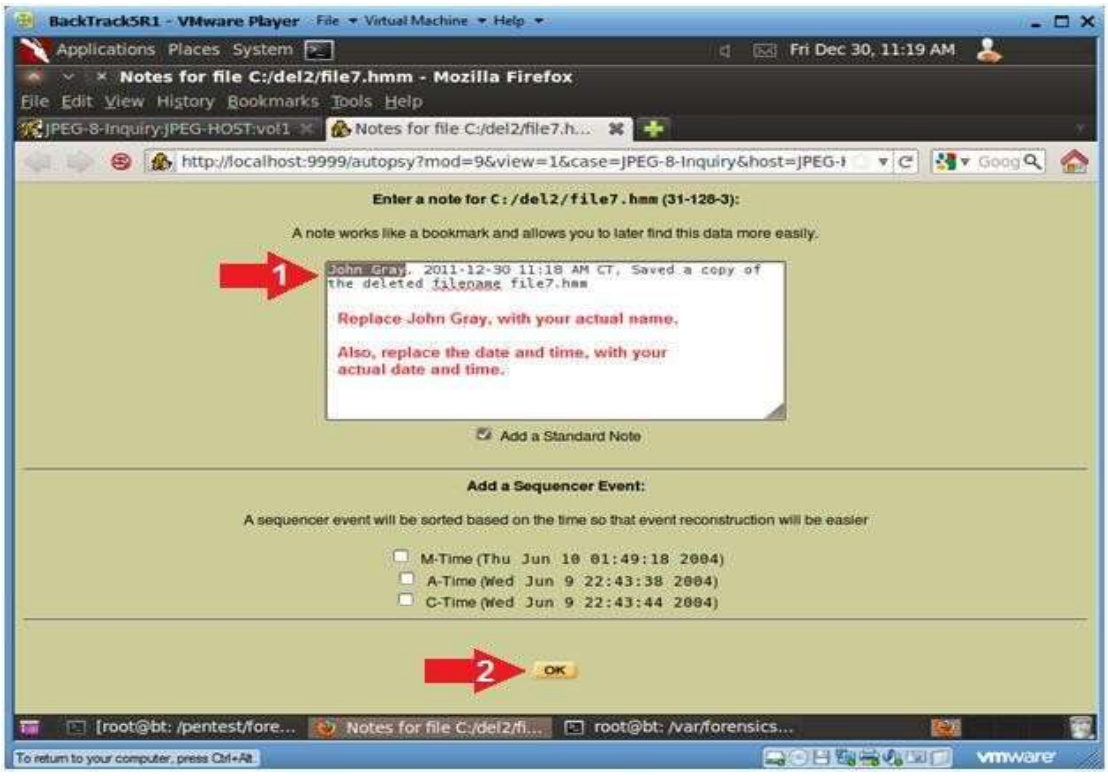

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 10:28 AM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
1
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
2
EXPAND DIRECTORIES
All Deleted Files
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREATED
SIZE
UID
GID
C:/del1 /file6.jpg
2004-06-10 01:46:08 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
175830
C:/del2 /file7.hmm
2004-06-10 01:49:18 (CDT)
2004-06-09 22:43:38 (CDT)
2004-06-09 22:43:44 (CDT)
2004-06-09 22:28:00 (CDT)
326859
3
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01
Deleted File Recovery Mode
C:/del2/file7.hmm
Thumbnail:
View Full Size Image
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

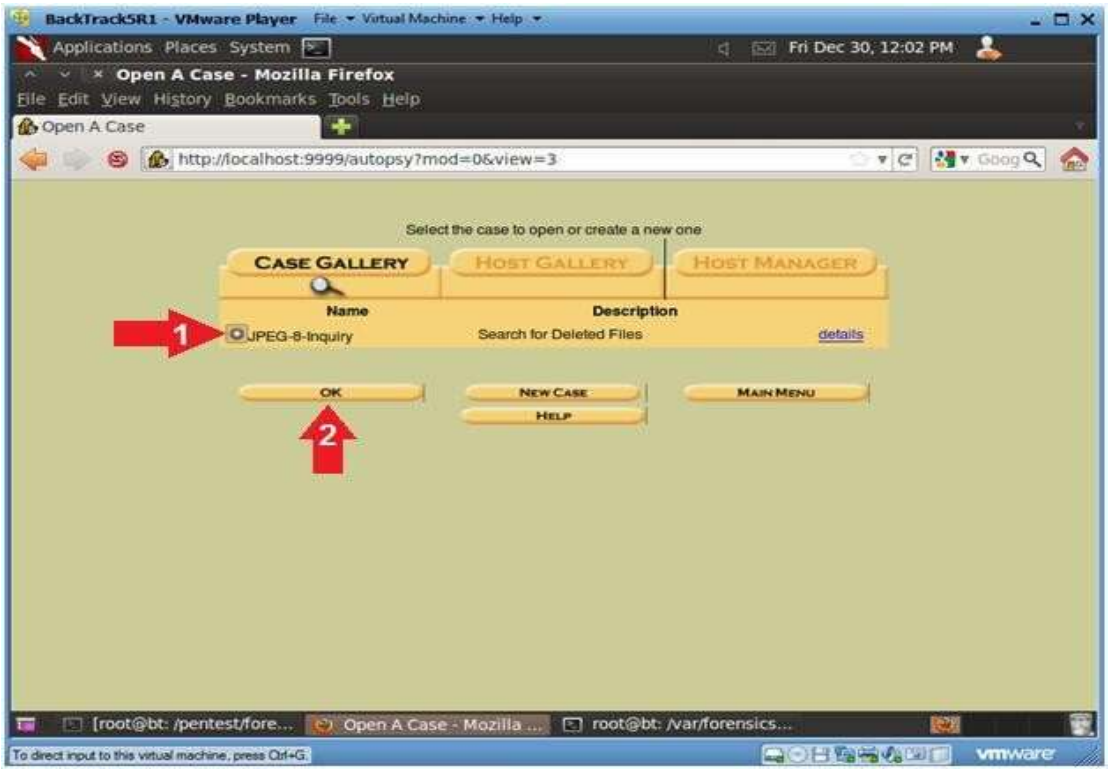

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 10:28 AM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
All Deleted Files
Type dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREATED
SIZE
UID
GID
META
C:/del1 /file6.jpg 2004-06-10 01:48:08 (CDT) 2004-06-09 22:28:00 (CDT) 2004-06-09 22:28:00 (CDT) 2004-06-09 22:28:00 (CDT) 175630 0 0 32-12
C:/del2 /file7.hmm 2004-06-10 01:49:18 (CDT) 2004-06-09 22:43:38 (CDT) 2004-06-09 22:43:44 (CDT) 2004-06-09 22:28:00 (CDT) 326859 0 0 31-12
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01
Deleted File Recovery Mode
C:/del2/file7.hmm
Notice that Autopsy identified file7.hmm as a JPEG
Click on the Export Link, so we can make a copy of the deleted file named file7.hmm
Thumbnail:
View Full Size Image
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware


BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 10:57 AM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
ALL DELETED FILES
EXPAND DIRECTORIES
All Deleted Files
Type dir / in
NAME
WRITTEN
C:/del1 /file6.jpg 2004-06-10 01:48:08 (CDT)
C:/del2 /file7.hmm 2004-06-10 01:49:18 (CDT)
Opening vol1-C..del2.file7.hmm
You have chosen to open
vol1-C..del2.file7.hmm
which is a: BIN file
from: http://localhost:9999
Would you like to save this file?
Cancel
Save File
1
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01
Deleted File Recovery Mode
C:/del2/file7.hmm
Thumbnail:
View Full Size Image
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt.
vmware

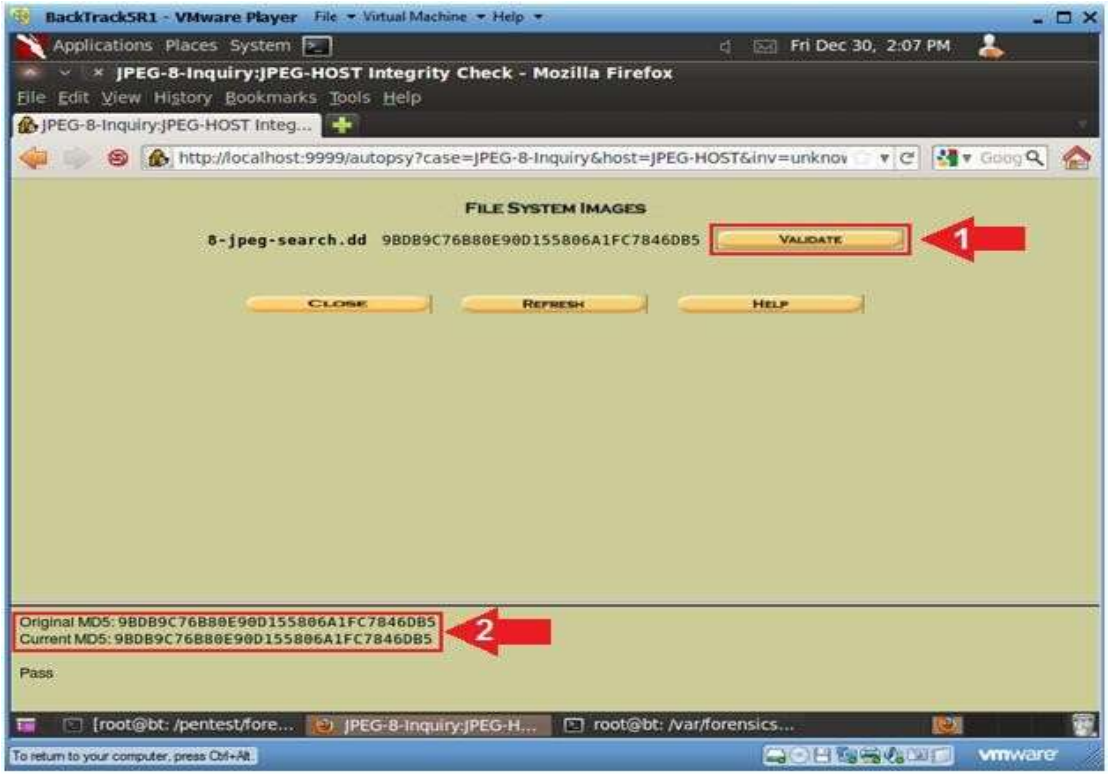

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 11:02 AM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Enter name of file to save to...
Name:
vol1-C..del2.file7.hmm
Save in folder:
images
Browse for other folders
2.
3.
4.
var
forensics
images
Create Folder
Recently Used
root
Desktop
File System
Floppy Drive
Size
Modified
Wednesday
Add
Remove
*.hmm
Save
1
2
3
4
5
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware

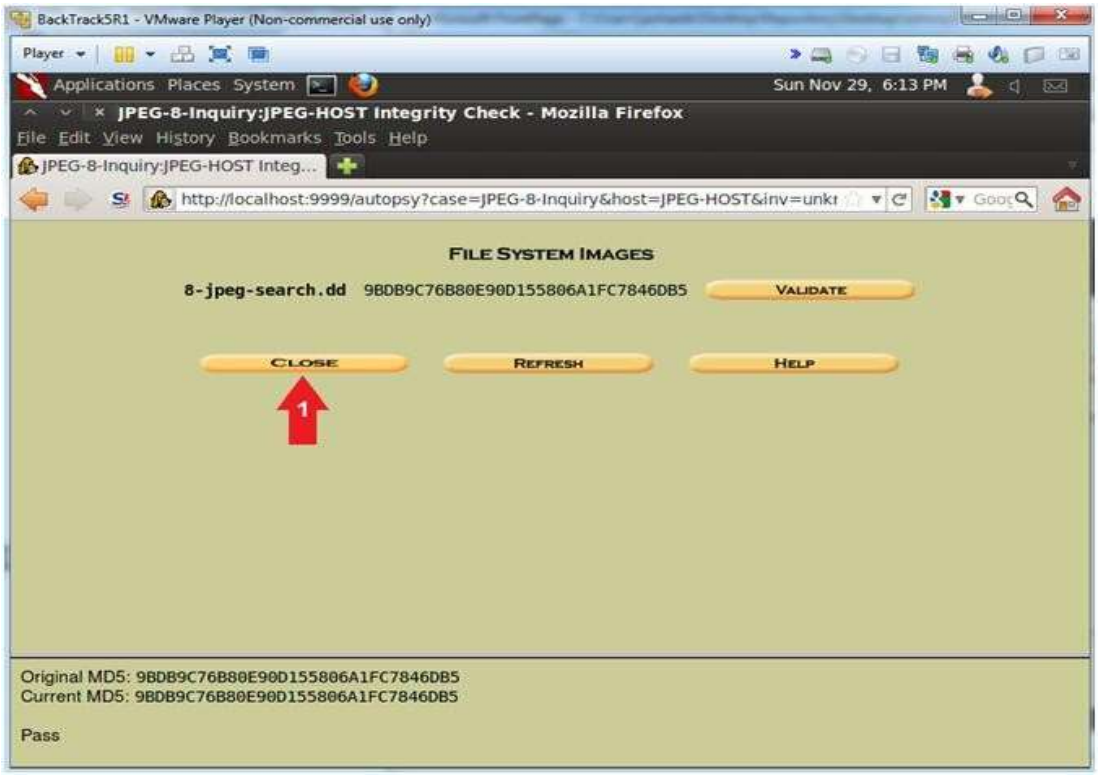

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 11:08 AM
JPEG-8-Inquiry:JPEG-HOST:vol1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST:vol1
http://localhost:9999/autopsy?mod=1&submod=2&case=JPEG-8-Inquiry&host=JPE
File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
Directory Seek
Enter the name of a directory that you want to view.
C:/
View
File Name Search
Enter a Perl regular expression for the file names you want to find.
Search
All Deleted Files
Expand Directories
All Deleted Files
Type dir / in
Name
Written
Accessed
Changed
Created
Size
UID
GID
Meta
C:/del1 /file6.jpg
2004-06-10 01:48:08 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
2004-06-09 22:28:00 (CDT)
175630
C:/del2 /file7.hmm
2004-06-10 01:49:18 (CDT)
2004-06-09 22:43:38 (CDT)
2004-06-09 22:43:44 (CDT)
2004-06-09 22:28:00 (CDT)
326859
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01
Deleted File Recovery Mode
1
C:/del2/file7.hmm
Thumbnail:
View Full Size Image
[root@bt: /pentest/fore...
JPEG-8-Inquiry:JPEG-H...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware


BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 11:19 AM
Notes for file C:/del2/file7.hmm - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=9&view=1&case=JPEG-8-Inquiry&host=JPEG-I
Enter a note for C:/del2/file7.hmm (31-128-3):
A note works like a bookmark and allows you to later find this data more easily.
1
John Gray, 2011-12-30 11:18 AM CT, Saved a copy of the deleted filename file7.hmm
Replace John Gray, with your actual name.
Also, replace the date and time, with your actual date and time.
Add a Standard Note
Add a Sequencer Event:
A sequencer event will be sorted based on the time so that event reconstruction will be easier
M-Time (Thu Jun 10 01:49:18 2004)
A-Time (Wed Jun 9 22:43:38 2004)
C-Time (Wed Jun 9 22:43:44 2004)
2
OK
[root@bt: /pentest/fore...
Notes for file C:/del2/fi...
root@bt: /var/forensics...
To return to your computer, press Ctrl+Alt
vmware

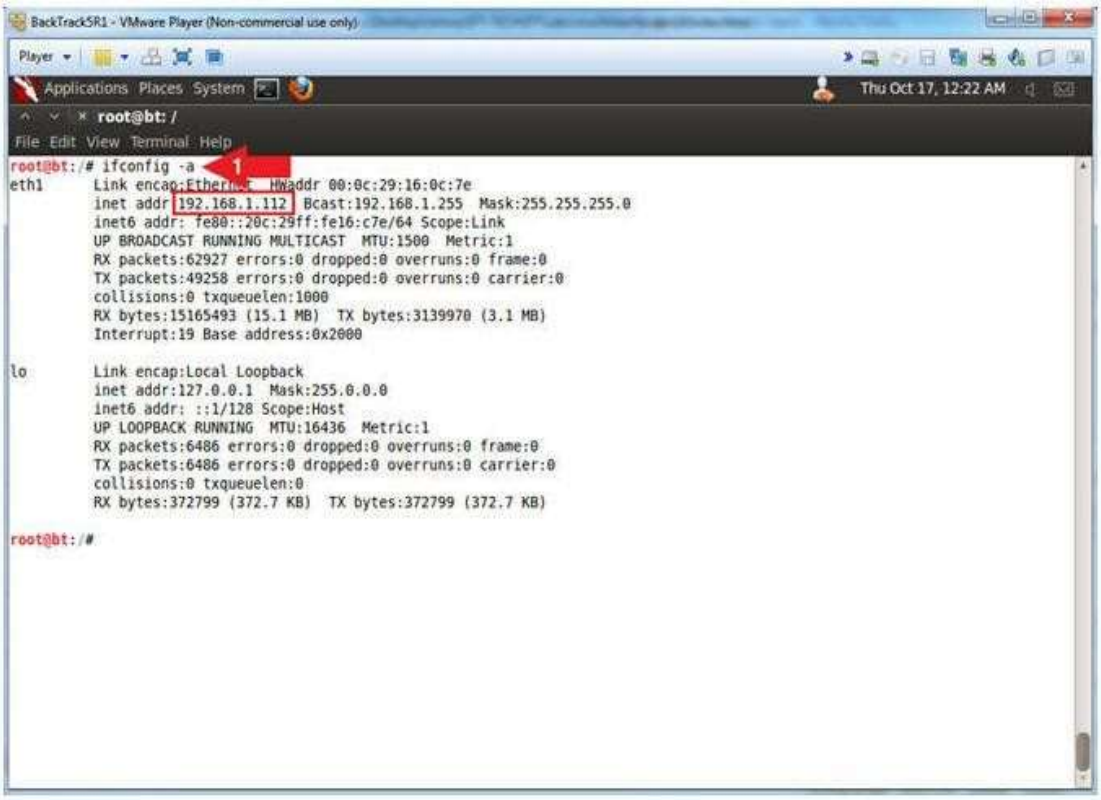

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 12:02 PM
Open A Case - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Open A Case
http://localhost:9999/autopsy?mod=0&view=3
Select the case to open or create a new one
CASE GALLERY
HOST GALLERY
HOST MANAGER
Name
Description
1
JPEG-8-Inquiry
Search for Deleted Files
details
OK
NEW CASE
MAIN MENU
HELP
2
[root@bt: /pentest/fore...
Open A Case - Mozilla ...
root@bt: /var/forensics...
To direct input to this virtual machine, press Ctrl+G
vmware

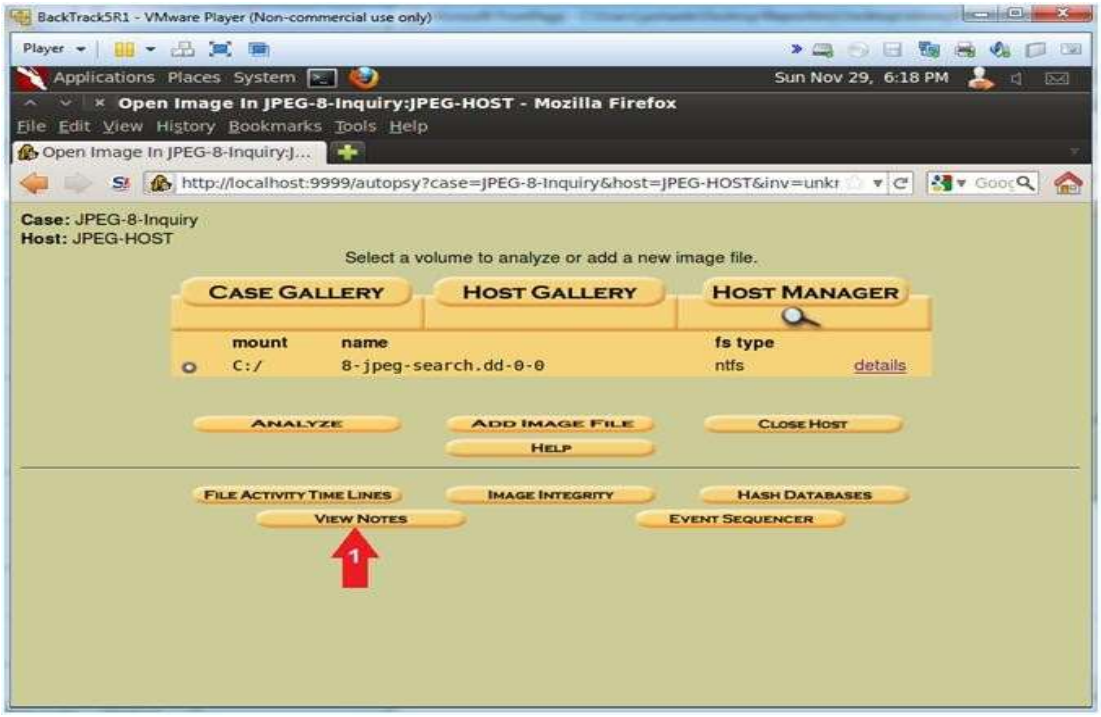

BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 12:03 PM
Open Image In JPEG-8-Inquiry:JPEG-HOST - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Case: JPEG-8-Inquiry
Host: JPEG-HOST
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
8-jpeg-search.dd-0-0
ntfs
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
1


BackTrack5R1 - VMware Player
Applications Places System
Fri Dec 30, 2:07 PM
JPEG-8-Inquiry:JPEG-HOST Integrity Check - Mozilla Firefox
File Edit View History Bookmarks Tools Help
FILE SYSTEM IMAGES
8-jpeg-search.dd
9BDB9C76B80E90D155806A1FC7846DB5
VALIDATE
1
CLOSE
REFRESH
HELP
Original MD5: 9BDB9C76B80E90D155806A1FC7846DB5
Current MD5: 9BDB9C76B80E90D155806A1FC7846DB5
2
Pass

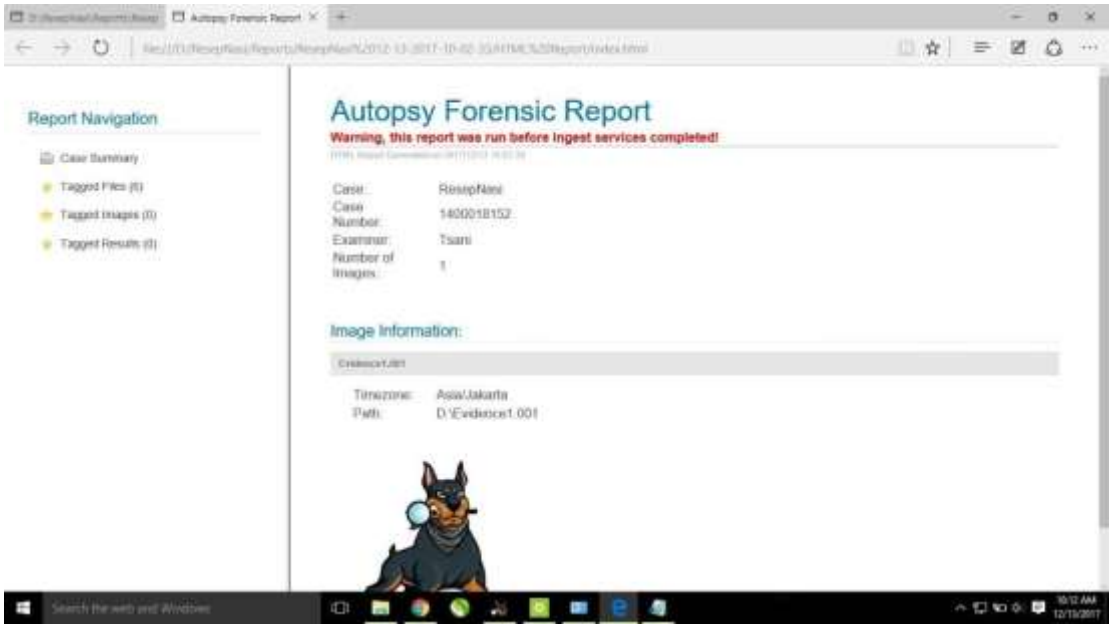

BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
Sun Nov 29, 6:13 PM
JPEG-8-Inquiry:JPEG-HOST Integrity Check - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JPEG-8-Inquiry:JPEG-HOST Integ...
http://localhost:9999/autopsy?case=JPEG-8-Inquiry&host=JPEG-HOST&inv=unkr
FILE SYSTEM IMAGES
8-jpeg-search.dd 9BDB9C76B80E90D155806A1FC7846DB5
VALIDATE
CLOSE
REFRESH
HELP
1
Original MD5: 9BDB9C76B80E90D155806A1FC7846DB5
Current MD5: 9BDB9C76B80E90D155806A1FC7846DB5
Pass


Programs (1)
VMware Player
3
See more results
vmware player
2
Shut down
1


BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
Thu Oct 17, 12:22 AM
root@bt: /
File Edit View Terminal Help
root@bt:/# ifconfig -a
1
eth1 Link encap:Ethernet HWaddr 00:0c:29:16:0c:7e
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe16:c7e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:62927 errors:0 dropped:0 overruns:0 frame:0
TX packets:49258 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:15165493 (15.1 MB) TX bytes:3139970 (3.1 MB)
Interrupt:19 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:6486 errors:0 dropped:0 overruns:0 frame:0
TX packets:6486 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:372799 (372.7 KB) TX bytes:372799 (372.7 KB)
root@bt:/#


BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
Sun Nov 29, 6:18 PM
Open Image In JPEG-8-Inquiry:JPEG-HOST - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Open Image In JPEG-8-Inquiry:J...
http://localhost:9999/autopsy?case=JPEG-8-Inquiry&host=JPEG-HOST&inv=unkr
Case: JPEG-8-Inquiry
Host: JPEG-HOST
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
8-jpeg-search.dd-0-0
ntfs
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
1


BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
Sun Nov 29, 6:22 PM
Contents of Notes File - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Contents of Notes File
http://localhost:9999/autopsy?case=JPEG-8-Inquiry&host=JPEG-HOST&inv=unkr
Sun Nov 29 17:23:33 2015
File: C:/del1/file6.jpg
Volume: vol1 Meta: 32-128-3
M-time: Thu Jun 10 01:48:08 2004
A-time: Wed Jun 9 22:28:00 2004
C-time: Wed Jun 9 22:28:00 2004
John Gray 2011-12-29 2:47 PM CT. Saved Deleted Fle Named file6.jpg.
Sun Nov 29 17:27:25 2015
File: C:/del2/file7.hmm
Volume: vol1 Meta: 31-128-3
M-time: Thu Jun 10 01:49:18 2004
A-time: Wed Jun 9 22:43:38 2004
C-time: Wed Jun 9 22:43:44 2004
John Gray 2011-12-30 11:18 AM CT. Saved a copy of the deleted filename file7.hmm.
CLOSE
REFRESH
1
2


Report Navigation
Autopsy Forensic Report
Warning, this report was run before ingest services completed!
Image Information:

Selesai.