PRAKTIKUM 3: (DIGITAL IMAGING) DD LINUX BASE

Pertemuan ke : 3

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Skor Penilaian : 100 %
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK

CPL-04	Mampu berpikir logis, kritis, sistematis dan inovatif, dan mampu mengambil keputusan secara tepat dibidang keahliannya
CPMK-01	Mahasiswa memahami tahapan investigasi digital forensik

3.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu melakukan akuisisi digital evidence dengan tools unix
2. Mampu mengidentifikasi jenis-jenis digital evidence dan autentikasinya

3.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-04	CPMK-01	Kemampuan mahasiswa dalam menerapkan Proses akuisisi digital evidence & Analisisi digital evidence md5 sha

3.3. TEORI PENDUKUNG

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. Proses imaging sendiri dapat dilakukan dengan 2 cara:

1. *Physical*

   Membuat *image* dari *physical drive* yang biasanya berupa hard disk atau flash disk, atau dapat dikatakan drive secara fisik. Jika kapasitas drive adalah 500 GB, maka *image* yang dihasilkan juga akan memiliki ukuran sebesar 500 GB (kecuali jika dikompres). Jadi proses *physical imaging* ini akan meng*clone* hard disk atau flash disk secara fisik, tidak peduli apakah ada isinya atau tidak. Biasanya proses akuisisi ini dilakukan untuk melihat apakah ada file-file yang di*delete*.

2. *Logical*

   Membuat *image* dari *logical drive*, berupa drive di komputer, yaitu biasanya A:, C:, D:, dst. Bisa saja satu harddisk dipartisi menjadi 2 atau lebih *logical drive*, misalnya C: untuk system dan D: untuk data. Jika membuat *image* dari *logical drive* berarti satu drive utuh termasuk bagian yang kosong/tidak ada datanya.

3.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:
1. Komputer.
2. OS Kali Linux.

3. Flashdisk/Partisi Tersedia

3.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-04	CPMK-01	Apa perbedaan imaging dengan platform windows dan opensource?	50
2.	CPL-04	CPMK-01	Jelaskan kelebihan dan kekurangan aplikasi ftk imager windows dan dd linux?	50

3.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-04	CPMK-01	Selesaikan langkah praktikum berikut ini	Screen Shot Hasil praktikum	100

Pada praktikum 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.

Ikuti langkah berikut ini:

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 *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 dimana flashdisk ditancapkan*
   - ***Of=/root/Desktop/hasil.dd*** *hasil imaging diletakkan di direktori* ***/root/Desktop*** *dengan nama file 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 diletakkan 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 selesai.

3.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-04	CPMK-01	Buat analisis perbandingan imaging yang telah anda lakukan pada praktikum ke-2 dengan hasil dari imaging menggunakan dd linux!	100

3.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-04	CPMK-01	20%		
2.	Praktik	CPL-04	CPMK-01	30%		
3.	Post-Test	CPL-04	CPMK-01	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 4: ANALISIS FILE RAW DENGAN AUTOPSY

Pertemuan ke : 4

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Skor Penilaian : 100 %
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK

CPL-06	Memahami tanggung jawab profesional dan menerapkan pengetahuan serta berkomunikasi efektif dalam melakukan penilaian berdasar informasi dan praktek computing dengan berpedoman pada prinsip-prinsip legal dan etika
CPMK-02	Mahasiswa mampu merekontruksi skenario kasus menggunakan tools forensik

4.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu melakukan analisisi digital evidence dengan tools autopsy
2. Mampu mengekplorasi digital evidence

4.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-06	CPMK-02	Kemampuan mahasiswa dalam melakukan Proses autopsy dan Analisisi temuan digital evidence

4.3. TEORI PENDUKUNG

Pembahasan kali ini sebenarnya merupakan pembahasan dari forensicscontest.com, dengan menganalisis sebuah file imager 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.

4.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:
1. Komputer.
2. OS Kali Linux
3. Autopsy

4.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-02	Apa perbedaan antara hasil imaging menggunakan FTK Imager dengan DD Linux ?	50
2.	CPL-06	CPMK-02	Jelaskan apa saja hasil jenis file extention dan cakupan tools investigasinya?	50

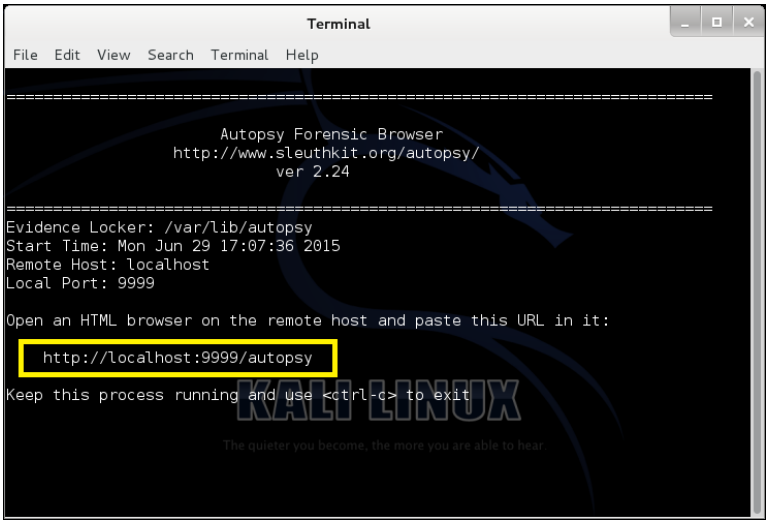
4.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-06	CPMK-02	Selesaikan langkah praktikum berikut?	Screen Shot Hasil praktikum	100

Ikuti langkah berikut ini:

1. Download kasus dilink berikut http://bit.ly/forensik3
2. Buka program **Autopsy** dari menu **Applications Kali Linux Forensics Forensic Suites Autopsy**
   Akan muncul terminal sebagai berikut:



Gambar 4.1 Tampilan Kali Linux

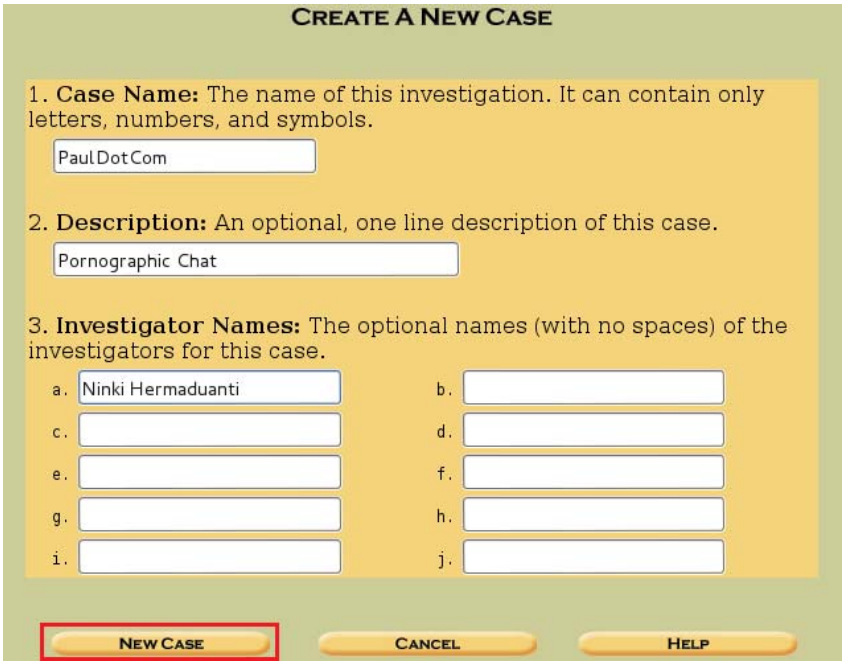
- Buka address **http://localhost:99/autopsy** menggunakan *web browser*.
- **INGAT!!!** Selamam program Autopsy dijalankan, jangan *close* terminal tersebut
- Semua file yang digunakan oleh kasus dalam program Autopsy ini akan disimpan di ***Evidence Locker*** dengan path-nya adalah **/var/lib/autopsy**.

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

Gambar 4.2 Tampilan Autopsy

4. Isikan informasi sebagai berikut (sesuai dengan kondisi Anda):

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



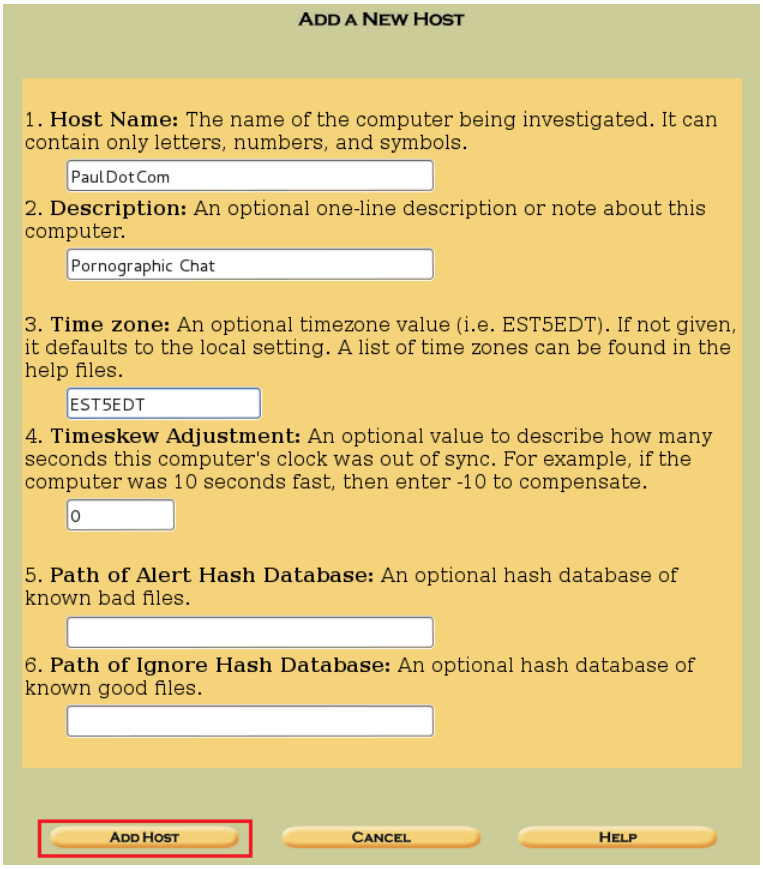
Gambar 4.3 Tampilan Autopsy Create New Case

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**

5. Langkah selanjutnya adalah menambahkan host untuk kasus PaulDotCom ini.

Gambar 4.4 Tampilan Autopsy Add Host

6. Isikan informasi sebagai berikut:
   - *Host Name* : PaulDotCom
   - *Description* : *Pornographic Chat*
   - *Timezone* : EST5EDT



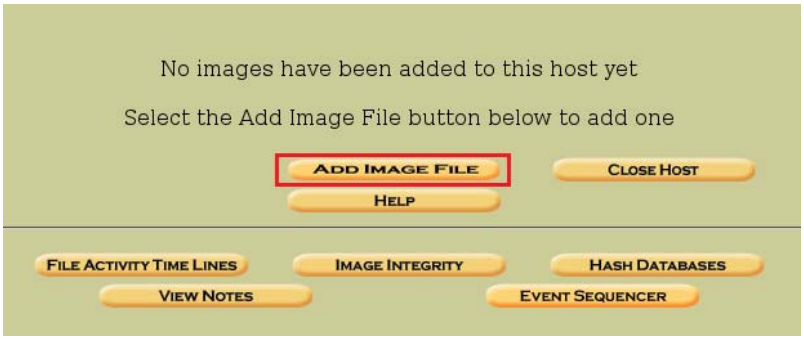
Gambar 4.5 Tampilan Autopsy Add Host Atribut

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**

7. 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**.

Gambar 4.6 Tampilan Autopsy Add Host Directory File



Gambar 4.7 Tampilan Autopsy Add Image File

8. Isikan Informasi sebagai berikut:
   - *Location* : /root/Desktop/quarter-SDHC-snippet.dd
   - *Type* : *Disk*
   - *Import Method* : *Move*

Gambar 4.8 Tampilan Autopsy Add Image File

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

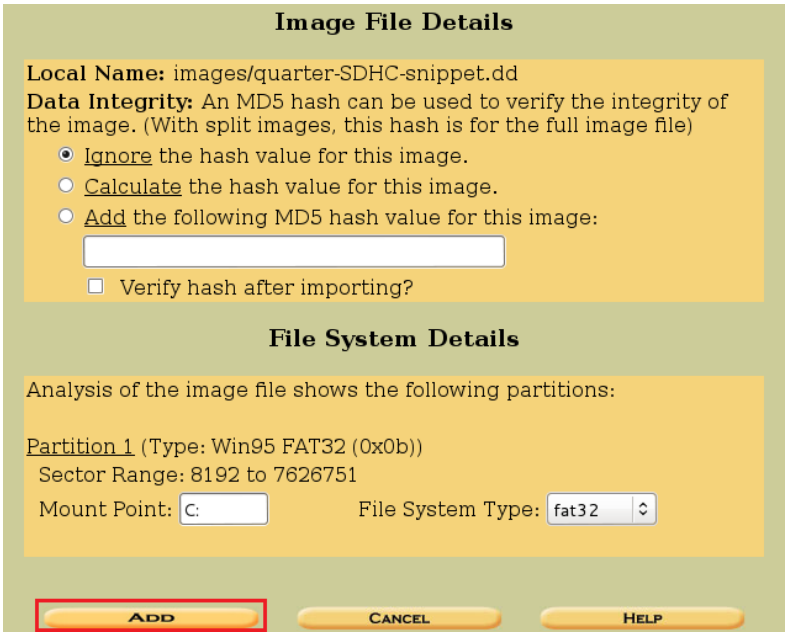
Jika ada lebih dari 1 partisi, maka gunakan *Type*: *Disk*.

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*)

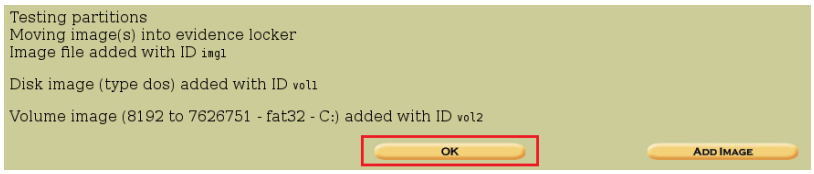
  Jika sudah, klik tombol **Next.**

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



Gambar 4.9 Tampilan Autopsy Add Image File Details

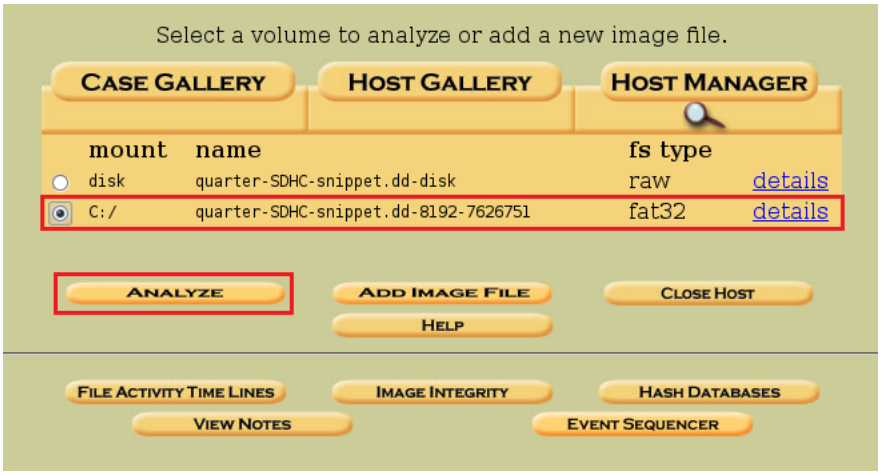
Opsi *Ignore* dipilih karena Autopsy hanya support MD5 *hash*, sedangkan file *raw image* yang dianalisis menggunakan SHA256 *hash*.
Field lain dibiarkan *default*, kemudian klik tombol **Add**. Pada halaman konfirmasi, klik tombol **OK.**



Gambar 4.10 Tampilan Autopsy Add Konfirmasi

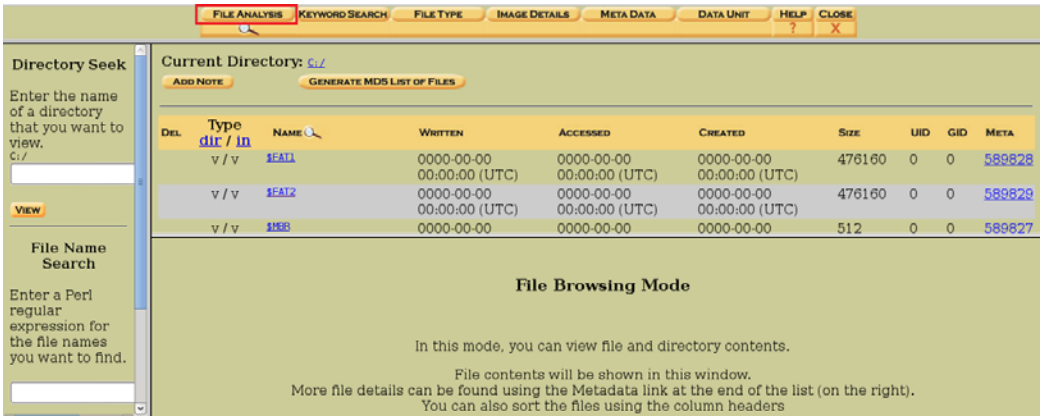
File *image* di dalam *Evidence Locker* pada kasus ini, akan diletakkan di folder **/var/lib/autopsy/PaulDotCom/PaulDotCom/images.**

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



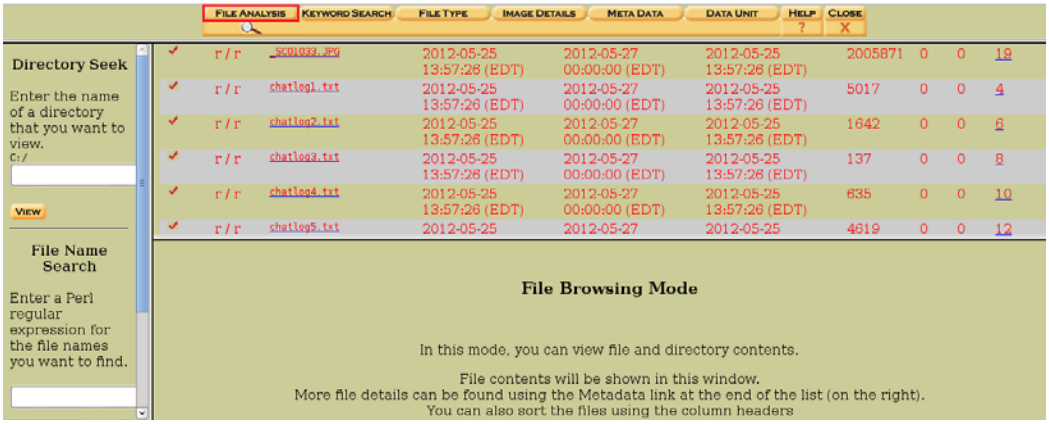
Gambar 4.11 Tampilan Autopsy Directory Volume

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



Gambar 4.12 Tampilan Autopsy File Analisis

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



Gambar 4.13 Tampilan Autopsy Evidence

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

13. *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-*rocover* 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*

14. 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 *

4.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-06	CPMK-02	Buatlah analisis menggunakan tools autopsy dengan menggunakan hasil akuisisi image.dd barang bukti yang telah anda lakukan pada praktikum ke-2 klasifikasikan temuan yang anda peroleh	100

4.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-06	CPMK-02	20%		
2.	Praktik	CPL-06	CPMK-02	30%		
3.	Post-Test	CPL-06	CPMK-02	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**