

LAPORAN PRAKTIKUM

EXPLORE INVESTIGASI FILE .DD



Disusun Oleh:

Nama : L Hafidl Alkhair
NIM : 2023903430060
Kelas : TRKJ 2.C
Jurusan : Teknologi Informasi dan Komputer
Program Studi : Teknologi Rekayasa Komputer Jaringan
Dosen Pembimbing : Umri Erdiansyah, S.Kom., M.Kom



JURUSAN TEKNOLOGI INFORMASI KOMPUTER
PRODI TEKNOLOGI REKAYASA KOMPUTER JARINGAN
POLITEKNIK NEGERI LHOKSEUMAWE
TAHUN AJARAN 2024-2025

LEMBAR PENGESAHAN

No Praktikum : 03/TIK/TRKJ-2C/Analisis Forensik Pertahanan Cyber
Judul : Laporan Praktikum Explore Investigasi File .DD
Nama : L Hafid Alkhair
NIM : 2023903430060
Kelas : TRKJ 2.C
Jurusan : Teknologi Informasi dan Komputer
Prodi : Teknologi Rekayasa Komputer Jaringan
Tanggal Praktikum : Kamis, 12 Juni 2025
Tanggal Penyerahan : Sabtu, 16 Juni 2025

Buketrata, 16 Juni 2025

Dosen Pembimbing,

Umri Erdiansyah, S.Kom., M.Kom

NIP. 19901013 202203 1 003

DAFTAR ISI

LEMBAR PENGESAHAN	i
DAFTAR ISI.....	ii
BAB I PENDAHULUAN	1
A. Tujuan Praktikum.....	1
B. Dasar Teori.....	1
C. Alat dan Bahan.....	2
D. Challenge	2
BAB II LANGKAH PRAKTIKUM.....	3
A. Membuka Program Autopsy	3
B. Membuat Kasus Baru	4
C. Menambahkan Host ke Kasus	5
D. Menambahkan Image Disk.....	7
E. Data Integrity	9
F. Menganalisis File System.....	10
G. Recovery File	12
H. Jawaban Challenge.....	15
BAB III PENUTUP	21
A. Kesimpulan	21

BAB I

PENDAHULUAN

A. Tujuan Praktikum

1. Mahasiswa mampu memahami dasar-dasar forensik digital, terutama dalam menganalisis file image dengan format .dd.
2. Mahasiswa dapat menjalankan proses mounting dan menyelidiki file bukti menggunakan alat bantu forensik seperti Autopsy dan Foremost.
3. Mahasiswa bisa mengenali dan mengekstrak berbagai jenis file yang terdapat di dalam image disk digital dengan teknik file carving.
4. Mahasiswa mampu mengecek keaslian data hasil ekstraksi dengan menghitung nilai hash (SHA256), sebagai bentuk verifikasi integritas file.

B. Dasar Teori

Digital forensik adalah salah satu cabang ilmu forensik yang berfokus pada proses mengidentifikasi, mengumpulkan, menganalisis, dan melaporkan bukti-bukti digital. Salah satu jenis data yang sering dianalisis dalam bidang ini adalah file image berformat .dd, yaitu salinan bit-per-bit dari media penyimpanan seperti hard disk atau flashdisk. File image ini digunakan agar analisis bisa dilakukan tanpa mengubah atau merusak data asli.

Salah satu alat bantu yang sering digunakan adalah Autopsy, sebuah software open source yang menyediakan tampilan grafis (GUI) dari Sleuth Kit. Autopsy memudahkan penyidik dalam menjelajahi isi file image, seperti struktur sistem file, metadata, file yang sudah dihapus, serta berbagai artefak digital lainnya.

Selain itu, ada juga Foremost, sebuah alat berbasis command-line yang digunakan untuk melakukan file carving. Teknik ini memungkinkan pengguna untuk mengekstrak file dari image disk berdasarkan struktur internal file (seperti header dan footer), tanpa harus bergantung pada sistem file. Foremost sangat berguna terutama saat sistem file rusak atau ketika file sudah terhapus tetapi masih bisa ditemukan secara fisik.

Dalam proses forensik digital, menjaga keaslian file yang dianalisis sangat penting. Salah satu cara untuk memastikannya adalah dengan menghitung nilai hash—misalnya dengan algoritma SHA256. Nilai hash ini bisa dianggap sebagai sidik jari digital dari sebuah file, yang dapat membantu memastikan bahwa file tersebut tidak mengalami perubahan selama proses investigasi.

C. Alat dan Bahan

1. Laptop atau Komputer
2. Kali Linux
3. Autopsy
4. Foremost
5. quarter-SDHC-snippet.dd

D. Challenge

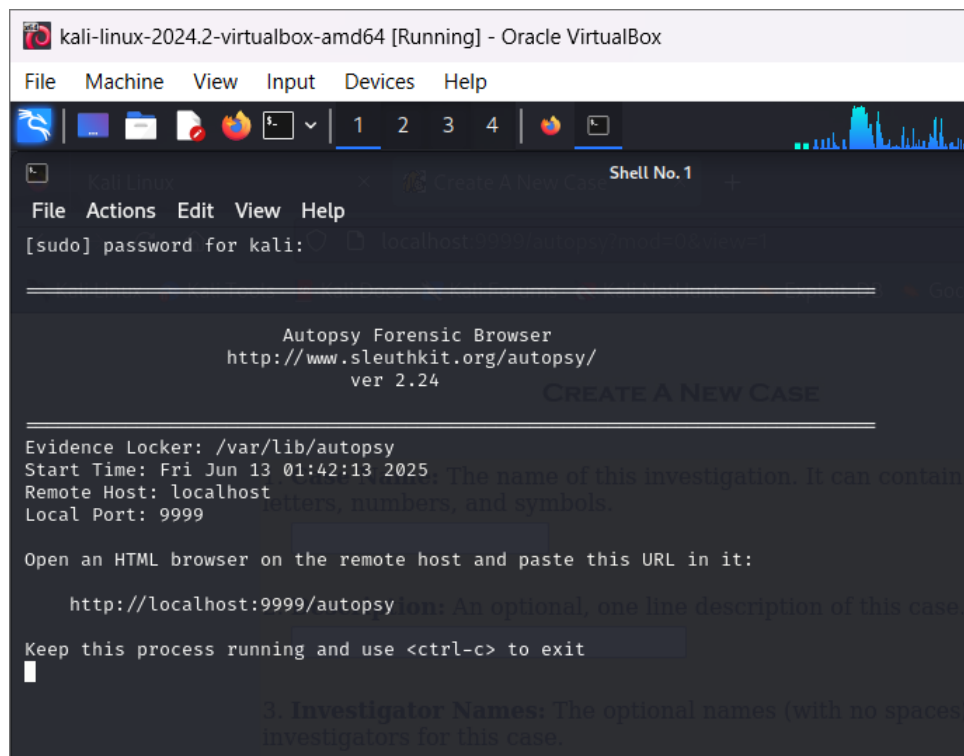
1. In his conversation with juniorkeyy, how old does Larry initially say he is?
2. What was the filename of the file that had the following SHA256 sum?
3. What is the SHA256sum of the photo from the “dd” image that shows Larry taking a bite out of a wireless router?
4. What is the SHA256sum of the image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

BAB II

LANGKAH PRAKTIKUM

A. Membuka Program Autopsy

1. Buka program Autopsy melalui menu → Applications → Kali Linux → Forensics → Forensic Suites → Autopsy.
2. Setelah terbuka, akan muncul terminal Autopsy. Jangan menutup terminal selama program Autopsy berjalan.



3. Kemudian buka address **http://localhost:9999/autopsy** menggunakan web browser.

```
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

Evidence Locker: /var/lib/autopsy
Start Time: Fri Jun 13 01:52:12 2025
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
```

4. Semua file yang digunakan oleh kasus dalam program Autopsy ini akan disimpan di Evidence Locker dengan path-nya adalah **/var/lib/autopsy**.

B. Membuat Kasus Baru

1. klik tombol **Add Case**.



2. Sesuaikan pada gambar

99/autopsy?mod=0&view=1&x=111&y=13

Kali NetHunter Exploit-DB Google Hacking DB OffSec

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="Hafid Alkhair"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

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.

C. Menambahkan Host ke Kasus

1. Selanjutnya adalah menambahkan host untuk kasus PaulDotCom ini.
2. Klik pada tombol Add Host.

Creating Case: PaulDotCom

Case directory (/var/lib/autopsy/PaulDotCom/) created
Configuration file (/var/lib/autopsy/PaulDotCom/case.aut) created

We must now create a host for this case.

3. Kemudian isi data host sebagai berikut:

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

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.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

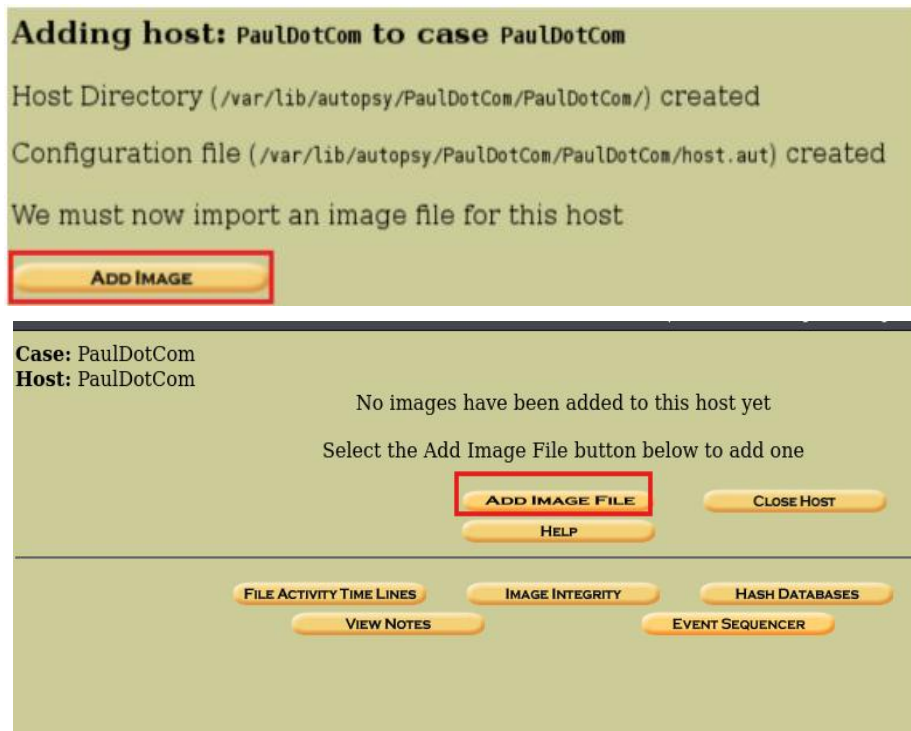
6. **Path of Ignore Hash Database:** An optional hash database of known good files.

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

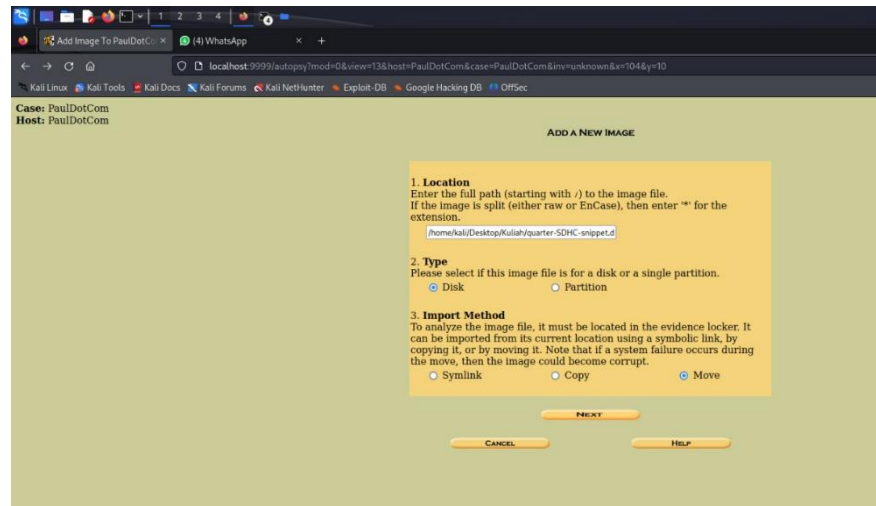
Setelah itu, tekan tombol Add Host. Host dengan nama PaulDotCom akan disimpan di dalam folder case `/var/lib/autopsy/PaulDotCom`, sehingga jalur lengkapnya menjadi `/var/lib/autopsy/PaulDotCom/PaulDotCom`

D. Menambahkan Image Disk

1. Tambahkan file raw image bernama quarter-SDHC-snippet.dd yang akan dianalisis. File ini terletak di folder /root/Desktop. Klik tombol Add Image, lalu klik tombol Add Image File.



2. Isi informasi berikut:



ADD A NEW IMAGE

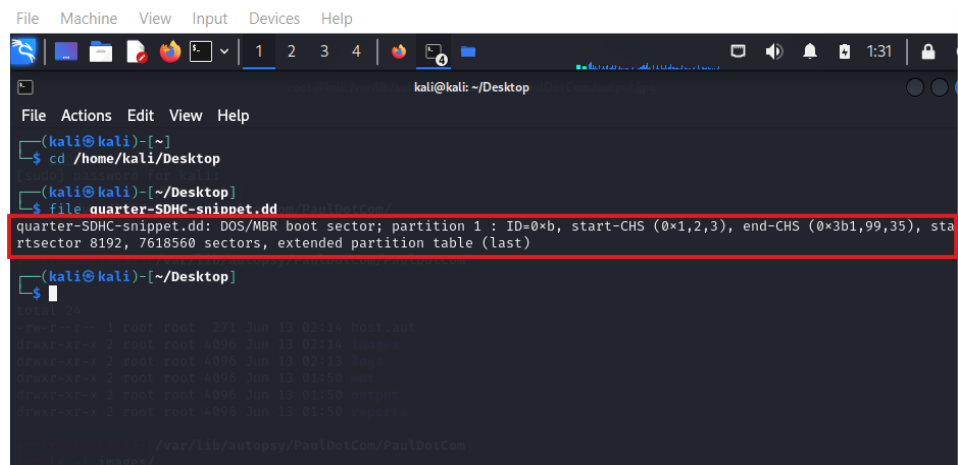
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type
Please select if this image file is for a disk or a single partition.
☒ Disk ☐ Partition

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.
☐ Symlink ☐ Copy ☒ Move

NEXT **CANCEL** **HELP**

3. Untuk memeriksa Type yang akan digunakan, jalankan perintah berikut di terminal Linux:



```
File Machine View Input Devices Help
kali@kali: ~/Desktop

File Actions Edit View Help
(kali@kali)-[~]
$ cd /home/kali/Desktop
(kali@kali)-[~/Desktop]
$ file quarter-SDHC-snippet.dd
quarter-SDHC-snippet.dd: DOS/MBR boot sector; partition 1 : ID=0xb, start=CHS (0x1,2,3), end=CHS (0x3b1,99,35), startsector 8192, 7618560 sectors, extended partition table (last)
(kali@kali)-[~/Desktop]
$
```

Jika terdapat lebih dari satu partisi, pilih Type: Disk. Berikut penjelasan mengenai Import Method:

- a. Symlink: Membuat tautan simbolik (seperti shortcut) ke file image tanpa perlu menyalin file aslinya ke dalam Evidence Locker. Metode ini hemat ruang karena file aslinya tetap berada di lokasi awal.

- b. Copy: Menyalin file image asli ke dalam Evidence Locker. Cara ini membuat salinan baru sehingga file asli tetap aman di tempat semula, namun membutuhkan ruang penyimpanan tambahan.
 - c. Move: Memindahkan file image langsung ke dalam Evidence Locker (seperti melakukan cut-paste). Cara ini menghemat ruang penyimpanan karena hanya ada satu salinan file, tapi file aslinya akan berpindah dari lokasi awal.
4. Setelah itu, klik tombol Next.

E. Data Integrity

- 1. Tambahkan detail dari file image dengan mengisi informasi berikut:
 - a. Data Integrity: Ignore

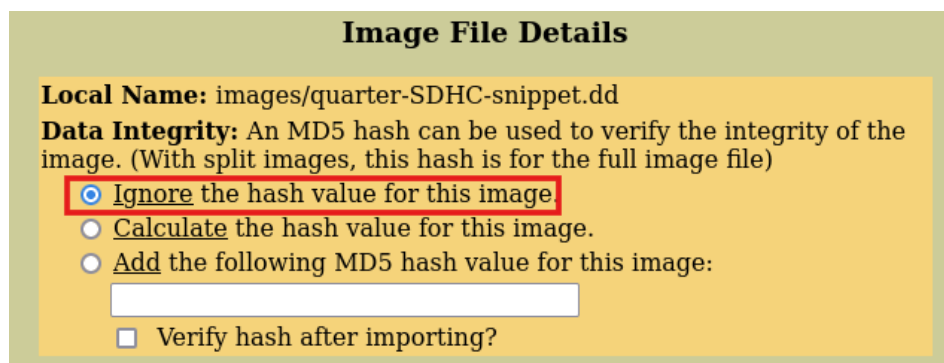


Image File Details

Local Name: images/quarter-SDHC-snippet.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)

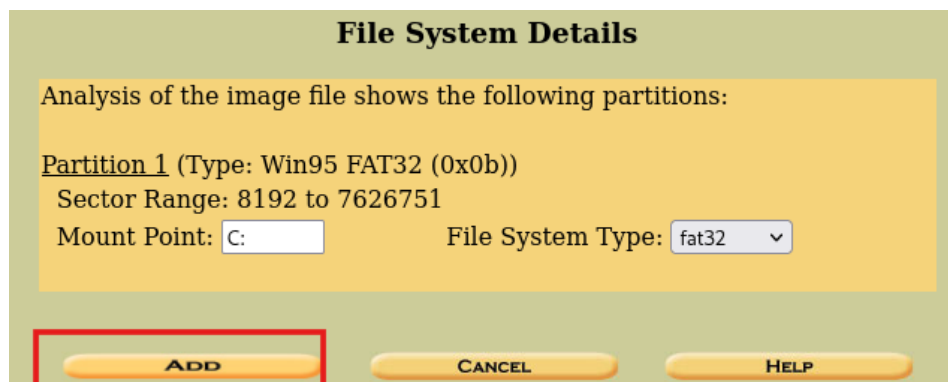
☒ Ignore the hash value for this image.

☐ Calculate the hash value for this image.

☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

- 2. Opsi Ignore dipilih karena Autopsy hanya mendukung MD5 hash, sementara file raw image yang dianalisis menggunakan SHA256 hash.



File System Details

Analysis of the image file shows the following partitions:

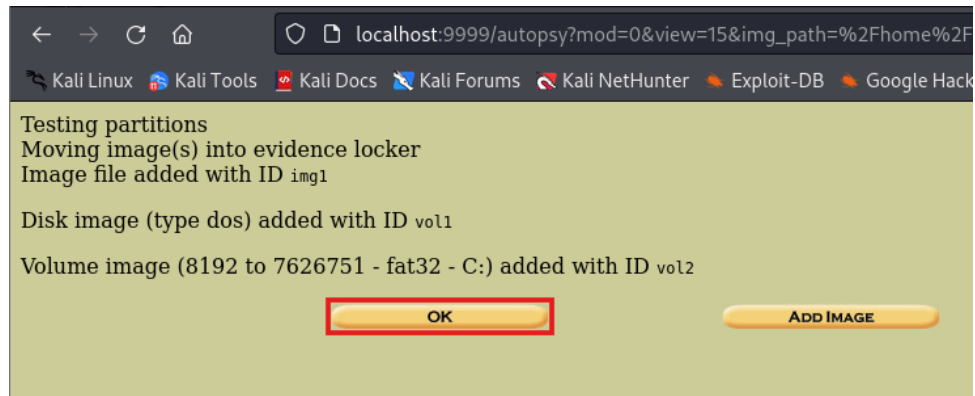
Partition 1 (Type: Win95 FAT32 (0x0b))

Sector Range: 8192 to 7626751

Mount Point: C: File System Type: fat32

ADD CANCEL HELP

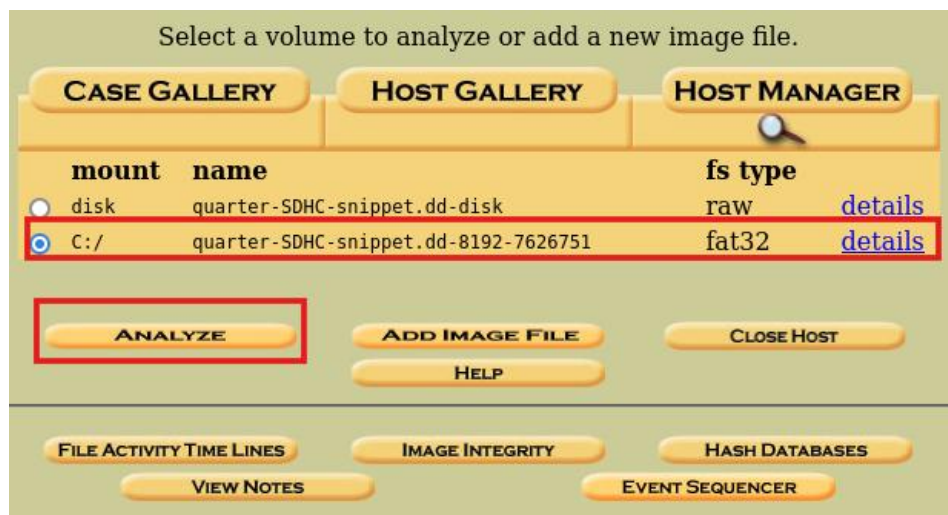
3. Biarkan field lainnya pada pengaturan default, lalu klik tombol Add. Di halaman konfirmasi, tekan tombol OK.



File image dalam Evidence Locker untuk kasus ini akan disimpan di folder `/var/lib/autopsy/PaulDotCom/PaulDotCom/images`.

F. Menganalisis File System

1. Untuk file system, pilih FAT32 dan klik tombol Analyze.



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



- Scroll ke bawah pada panel evidence item, dan temukan file-file yang tertulis dengan warna merah.



File-file ini merupakan file yang telah dihapus (deleted files), sehingga proses recovery diperlukan untuk menganalisisnya.

G. Recovery File

1. Melakukan Recovery File di Kali Linux
Ada dua cara untuk mengembalikan file yang terhapus di Kali Linux menggunakan terminal:
 - a. foremost: Mengembalikan file dan mengelompokkannya berdasarkan jenis file.
 - b. photorec: Juga bisa mengembalikan file, tapi semua jenis file dicampur tanpa pemisahan berdasarkan tipe.
2. Agar prosesnya lebih mudah, kita akan menggunakan perintah foremost. Pertama, masuk dulu ke direktori tempat data disimpan dengan mengetik perintah: bash Copy Edit
3. Tampilkan daftar file di direktori. Setelah berada di direktori tersebut, tampilkan semua file yang ada untuk memverifikasi isi folder:

```
(root@kali)-[/var/lib/autopsy/PaulDotCom/PaulDotCom]
# ls -l
total 24
-rw-r--r-- 1 root root 271 Jun 13 02:14 host.aut
drwxr-xr-x 2 root root 4096 Jun 13 02:14 images
drwxr-xr-x 2 root root 4096 Jun 13 02:13 logs
drwxr-xr-x 2 root root 4096 Jun 13 01:50 mnt
drwxr-xr-x 2 root root 4096 Jun 13 01:50 output
drwxr-xr-x 2 root root 4096 Jun 13 01:50 reports
```

Penjelasan output:

- c. total 24: Total ukuran file dalam direktori.
- d. File dan folder yang ditampilkan mencakup:
 - host.aut: File konfigurasi Autopsy.
 - images: Folder yang berisi file image yang akan dianalisis.
 - logs, mnt, output, reports: Folder untuk menyimpan log, mounting point, hasil recovery, dan laporan.
4. Masuk ke folder images untuk melihat file image yang akan dianalisis.

```
(root@kali)-[/var/lib/autopsy/PaulDotCom/PaulDotCom]
# ls -l images/

total 26624
-rw-r--r-- 1 kali kali 27262976 May 31 2012 quarter-SDHC-snippet.dd
```

Penjelasan output:

Proses recovery akan dimulai, dan hasilnya akan disimpan di folder output.

5. Jalankan Perintah Foremost. Gunakan perintah foremost untuk melakukan recovery file dari image.

```
(root@kali)-[/var/lib/autopsy/PaulDotCom/PaulDotCom]
# foremost images/quarter-SDHC-snippet.dd

Processing: images/quarter-SDHC-snippet.dd
|*|
```

Penjelasan output:

Proses recovery akan dimulai, dan hasilnya akan disimpan di folder output.

6. Tampilkan daftar file di folder output. Setelah proses recovery selesai, tampilkan hasil recovery di folder output.

```
(root@kali)-[/var/lib/autopsy/PaulDotCom/PaulDotCom]
# ls -l output/

total 12
-rw-r--r-- 1 root root 1328 Jun 13 08:21 audit.txt
drwxr-xr-- 2 root root 4096 Jun 13 08:21 jpg
drwxr-xr-- 2 root root 4096 Jun 13 08:21 mov
```

Penjelasan output:

- a. Terdapat file audit.txt dan dua folder: jpg dan mov.
- b. jpg berisi file gambar yang berhasil direcovery, sedangkan mov berisi file video.

7. Tampilkan daftar file gambar ter-recovery. Masuk ke folder jpg untuk melihat file gambar yang telah direcovery.

```
(root@kali)-[/var/lib/autopsy/PaulDotCom/PaulDotCom]
# ls -l output/jpg/

total 7728
-rw-r--r-- 1 root root 28083 Jun 13 08:21 00026304.jpg
-rw-r--r-- 1 root root 2005871 Jun 13 08:21 00026368.jpg
-rw-r--r-- 1 root root 212411 Jun 13 08:21 00030336.jpg
-rw-r--r-- 1 root root 31660 Jun 13 08:21 00030784.jpg
-rw-r--r-- 1 root root 127671 Jun 13 08:21 00030848.jpg
-rw-r--r-- 1 root root 97676 Jun 13 08:21 00031104.jpg
-rw-r--r-- 1 root root 3873991 Jun 13 08:21 00031296.jpg
-rw-r--r-- 1 root root 116985 Jun 13 08:21 00038912.jpg
-rw-r--r-- 1 root root 71619 Jun 13 08:21 00039168.jpg
-rw-r--r-- 1 root root 103338 Jun 13 08:21 00039360.jpg
-rw-r--r-- 1 root root 105202 Jun 13 08:21 00039616.jpg
-rw-r--r-- 1 root root 1121475 Jun 13 08:21 00050880.jpg
```

Penjelasan output:

Daftar file dengan ekstensi .jpg, menunjukkan berbagai file gambar yang berhasil ter-recovery dengan ukuran yang bervariasi.

8. Tampilkan daftar file video ter-recovery. Masuk ke folder mov untuk melihat file video yang telah direcovery

```
(root@kali)-[/var/lib/autopsy/PaulDotCom/PaulDotCom]
# ls -l output/mov/

total 10236
-rw-r--r-- 1 root root 4858802 Jun 13 08:21 00016768.mov
-rw-r--r-- 1 root root 5617411 Jun 13 08:21 00039872.mov
```

Penjelasan output:

Daftar file dengan ekstensi .mov, menunjukkan file video yang berhasil ter-recovery.

9. Periksa nilai hash untuk file gambar. Agar bisa membandingkan file ter-recovery dengan file aslinya, periksa nilai hash menggunakan algoritma sha256.

```
(root@kali)-[/var/lib/autopsy/PaulDotCom/PaulDotCom]
# cd output/jpg/
```

Kemudian, jalankan perintah berikut.

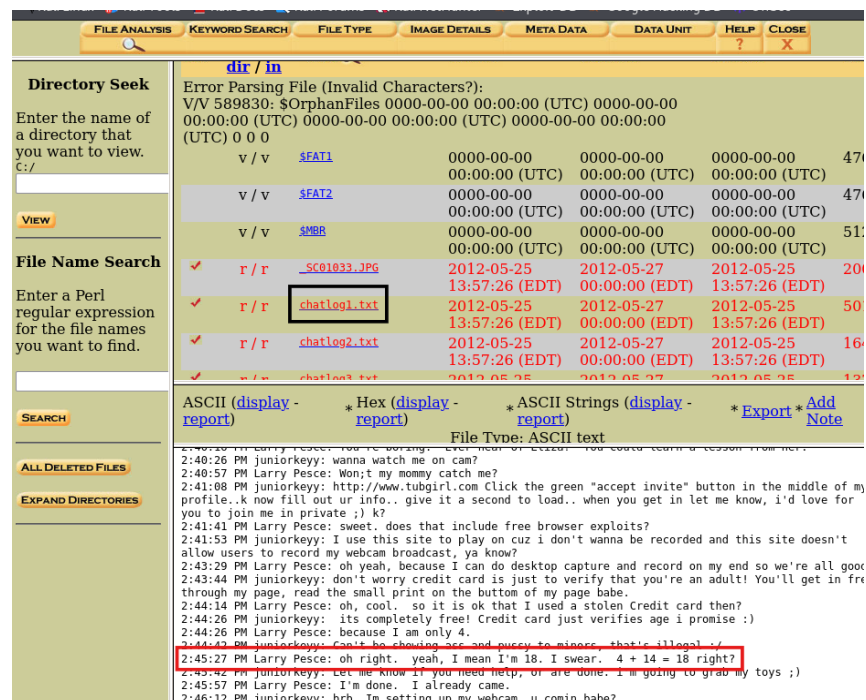
```
(root@kali)-[/var/www/PaulDotCom/PaulDotCom/output/jpg]
# sha256sum *
fc4fec579db37ffaec516be4cfff1a669fba3a3cbf09f6706a8328b766ed729a 00026304.jpg
a51649b8f2af41f71c6bf22b30e0691bf104a3d7014977f38ecc7c80699ab690 00026368.jpg
e4e2fac9fc41546239d4e534bfe6588e4796f3799befc09b2787f5ad6c75faca 00030336.jpg
1bdfd9d7445d38fdb7ba5acbb58669cf31c7c568c7aa6e6fcf0c961628f4c32e 00030784.jpg
67788573a013ce0e59400800ddd765132a44fdf5ba3931f3295dc76cc28b8adf 00030848.jpg
9c0a8bc6c3baa2ad7f390ef4e41c3edf3d98a543f492afb50a4bab8700af5766 00031104.jpg
8c1c8e97a8a37b6b7b6942bd17a3eb5ecae79e315cc04f7e857c011f3e4dca28 00031296.jpg
dd244a31908037d439c2095391b3f46a1820059c91af31369b5f6c4522e8fa3d 00038912.jpg
0f5ac5eff6aada2eeef8dec60d588d28899959a31d27e9a5c24d65acc5f18ca 00039168.jpg
c08af53ce151fd454dcfc642b81406f57aec522ad9cfc44dc921d5be26d60b6 00039360.jpg
e56931935bc60ac4c994eabd89b003a7ae221d941f1b026b05a7947a48dc9366 00039616.jpg
6b55985144d6535b192b5b4a679b116ce7e48cc91e9f96909d4a721ade218c21 00050880.jpg
```

Penjelasan output:

- Menampilkan nilai hash SHA256 untuk setiap file gambar.
- Nilai hash ini berguna untuk memastikan integritas file dan mencocokkan dengan file aslinya.

H. Jawaban Challenge

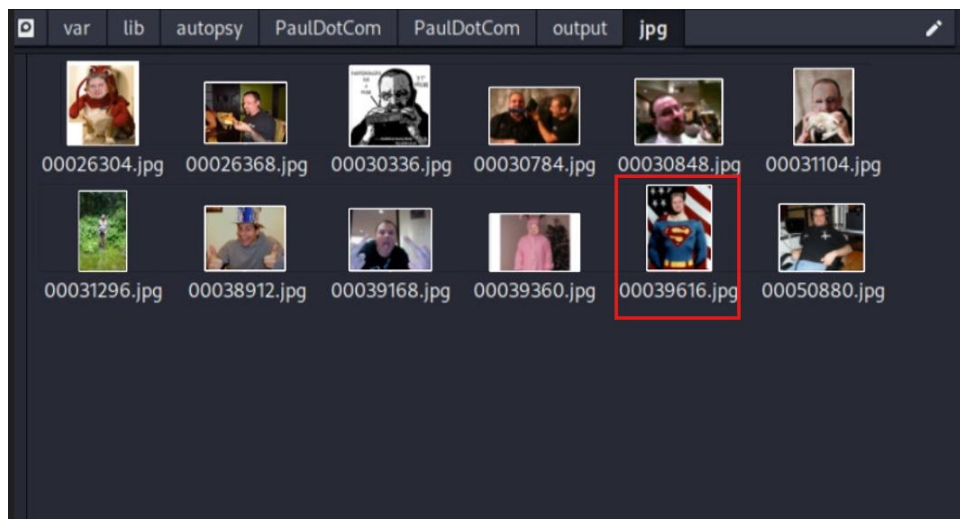
- In his conversation with juniorkeyy, how old does Larry initially say he is? Asumsinya, jika disebut "conversation," maka yang perlu diperiksa adalah log dari percakapan yang ada. Untuk mengetahui jawaban dari challenge tersebut, cek file chatlog dimulai dari chatlog1.txt.



Ditemukan bahwa 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.

Setelah mencocokkan dengan hasil sha256sum yang telah dijalankan di terminal Linux, ditemukan bahwa nama file tersebut adalah 00039616.jpg (file ter-recover). Selanjutnya, buka folder /var/lib/autopsy/PaulDotCom/PaulDotCom/output/jpg melalui explorer untuk melihat gambar tersebut.



Setelah ditemukan, lakukan pencocokan gambar dengan gambar file aslinya dengan mengklik satu per satu gambar JPG di program Autopsy hingga menemukan gambar yang sama.

✓	r / r	strandbunny.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	10
✓	r / r	superstrand.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	10
✓	r / r	trapped.mp4	2012-05-25 13:57:26 (EDT)	2012-05-25 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	56
✓	r / r	x_marks_the_spot.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	11

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [View](#) * [Add Note](#)
 File Type: IPEG image data. IFIF standard 1.01. resolution (DPI). densitv 96x96. segment

C:/superstrand.jpg

Thumbnail:



[View Full Size Image](#)

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


Periksa satu per satu gambar JPG yang ada di program Autopsy.

✓	r / r	haxorthematrix-has-a-posse.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	2124
✓	r / r	Larry_zombie_cat.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	9767
✓	r / r	larryeatswrt.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	3166
✓	r / r	LarryPlus40.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	1276
✓	r / r	ohnoeswrt.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	3873
✓	r / r	paul2.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	1169

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [View](#) * [Add Note](#)
 File Type: IPEG image data. IFIF standard 1.02. aspect ratio. densitv 100x100. segment

C:/haxorthematrix-has-a-posse.jpg

Thumbnail:




[View Full Size Image](#)

✓	r / r	Larry_zombie_cat.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	9767
✓	r / r	larryeatswrt.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	3166
✓	r / r	LarryPlus40.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	1276
✓	r / r	ohnoeswrt.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	3873
✓	r / r	paul2.jpg	2012-05-25 13:57:26 (EDT)	2012-05-27 00:00:00 (EDT)	2012-05-25 13:57:26 (EDT)	1169

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [View](#) * [Add Note](#)
 File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment

C:/larryeatswrt.jpg

Thumbnail: [View Full Size Image](#)



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

- 00030336.jpg untuk haxorthematrix-has-a-posse.jpg
- 00030784.jpg untuk larryeatswrt.jpg

Selanjutnya, cek nilai hash SHA256 untuk masing-masing file tersebut. Hasilnya adalah.

- 00030336.jpg:
e4e2fac9fc41546239d4e534bfe6588e4796f3799befc09b2787f5ad6c75
faca
- 00030784.jpg:
1bdfd9d7445d38fdb7ba5acbb58669cf31c7c568c7aa6e6fcf0c961628f4
c32e

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. Periksa satu per satu gambar JPG yang ada di program Autopsy untuk mencari gambar Larry yang sedang menggigit seekor kucing.

		a-posse.jpg	13:57:26 (EDT)	00:00:00 (EDT)	13:57:26 (EDT)	
✓	r / r	Larry_zombie_cat.jpg	2012-05-25	2012-05-27	2012-05-25	9767
			13:57:26 (EDT)	00:00:00 (EDT)	13:57:26 (EDT)	
✓	r / r	Larryeatswrt.jpg	2012-05-25	2012-05-27	2012-05-25	3166
			13:57:26 (EDT)	00:00:00 (EDT)	13:57:26 (EDT)	
✓	r / r	LarryPlus40.jpg	2012-05-25	2012-05-27	2012-05-25	1276
			13:57:26 (EDT)	00:00:00 (EDT)	13:57:26 (EDT)	
✓	r / r	ohnoeswrt.jpg	2012-05-25	2012-05-27	2012-05-25	3873
			13:57:26 (EDT)	00:00:00 (EDT)	13:57:26 (EDT)	
✓	r / r	paul2.jpg	2012-05-25	2012-05-27	2012-05-25	1169
			13:57:26 (EDT)	00:00:00 (EDT)	13:57:26 (EDT)	

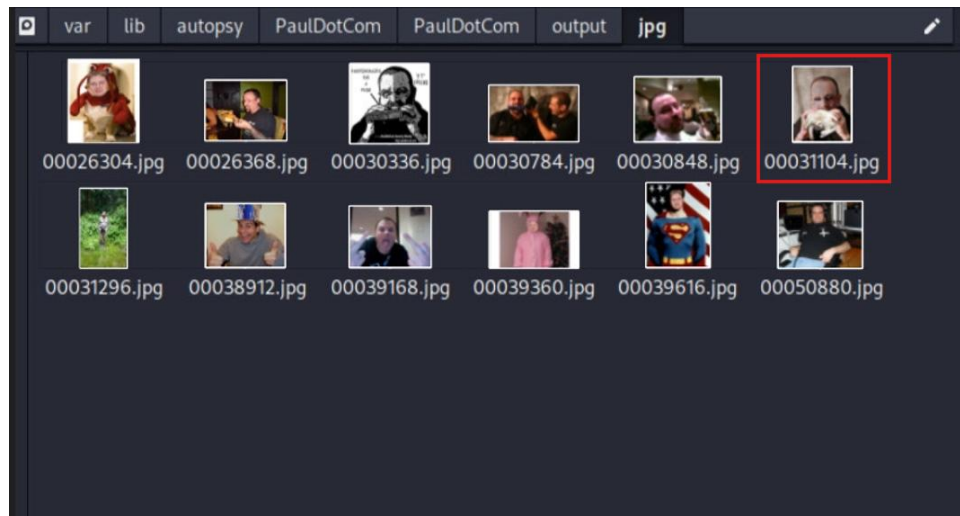
ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [View](#) * [Add Note](#)

File Type: JPEG image data. Exif standard: [TIFF image data, big-endian, direntries=10.

Thumbnail: [View Full Size Image](#)



Ditemukan satu file, yaitu Larry_zombie_cat.jpg. File ini kemudian dicocokkan dengan nama file ter-recover di folder /var/lib/autopsy/PaulDotCom/PaulDotCom/output/jpg, dan ditemukan nama file 00031104.jpg.



Selanjutnya, cek nilai hash SHA256 untuk file 00031104.jpg. Hasilnya adalah:

a. 00031104.jpg:

9c0a8bc6c3baa2ad7f390ef4e41c3edf3d98a543f492afb50a4bab8700af
5766

BAB III

PENUTUP

A. Kesimpulan

Dengan bantuan tools seperti Autopsy dan Foremost, data yang tersimpan di dalam image berhasil diekstraksi—baik itu berupa file gambar, video, maupun log percakapan. Setelah diekstrak, setiap file dianalisis lebih lanjut dan dicek keasliannya menggunakan metode hash SHA256 untuk memastikan file tersebut tidak berubah.

Selama proses analisis, ditemukan beberapa bukti digital penting yang bisa digunakan untuk menjawab tantangan atau soal yang diberikan. Dari file percakapan misalnya, kita bisa mengetahui informasi seperti usia Larry saat pertama kali ngobrol, nama file yang cocok dengan hash tertentu, hingga mengenali gambar-gambar yang sesuai dengan petunjuk soal.

Dari kegiatan ini bisa disimpulkan bahwa proses forensik digital membutuhkan ketelitian, pemahaman tentang cara kerja tools forensik, serta kemampuan menganalisis data secara mendalam. Teknik ini sangat berguna dalam penyelidikan kasus digital, karena meskipun data tampak sudah hilang atau tersembunyi, nyatanya tetap bisa dilacak dan dibuktikan dengan cara yang sah dan akurat.