**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/Analis Forensik Pertahanan Cyber

Judul : Laporan Praktikum Explore Investigasi File .DD

Nama : L Hafidl 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](#_Toc200928746)

[DAFTAR ISI ii](#_Toc200928747)

[BAB I PENDAHULUAN 1](#_Toc200928748)

[A. Tujuan Praktikum 1](#_Toc200928749)

[B. Dasar Teori 1](#_Toc200928750)

[C. Alat dan Bahan 2](#_Toc200928751)

[D. Challenge 2](#_Toc200928752)

[BAB II LANGKAH PRAKTIKUM 3](#_Toc200928753)

[A. Membuka Program Autopsy 3](#_Toc200928754)

[B. Membuat Kasus Baru 4](#_Toc200928755)

[C. Menambahkan Host ke Kasus 5](#_Toc200928756)

[D. Menambahkan Image Disk 7](#_Toc200928757)

[E. Data Integrity 9](#_Toc200928758)

[F. Menganalisis File System 10](#_Toc200928759)

[G. Recovery File 12](#_Toc200928760)

[H. Jawaban Challenge 15](#_Toc200928761)

[BAB III PENUTUP 21](#_Toc200928762)

[A. Kesimpulan 21](#_Toc200928763)

# BAB I PENDAHULUAN

## 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.

## 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.

## Alat dan Bahan

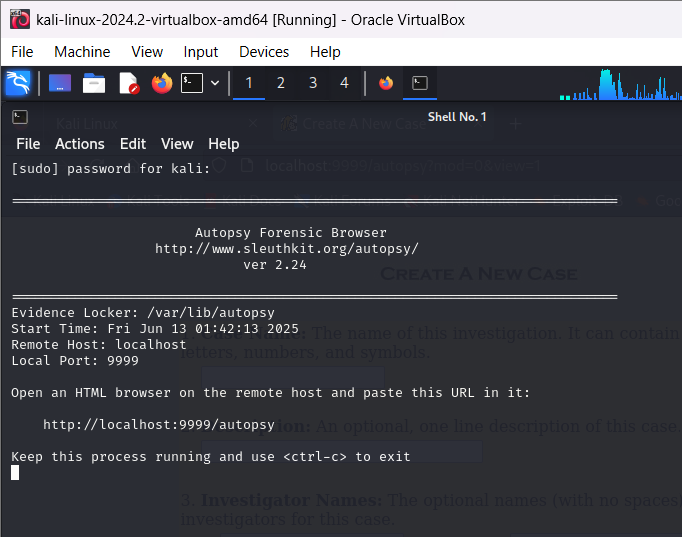
1. Laptop atau Komputer
2. Kali Linux
3. Autopsy
4. Foremost
5. quarter-SDHC-snippet.dd

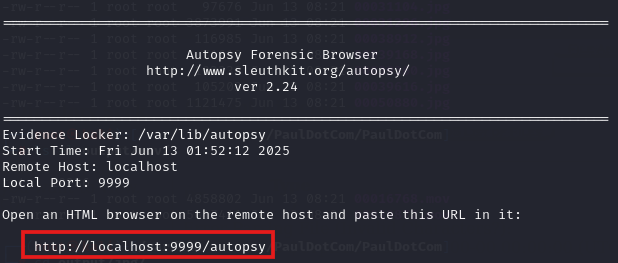
## Challenge

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

## Membuka Program Autopsy

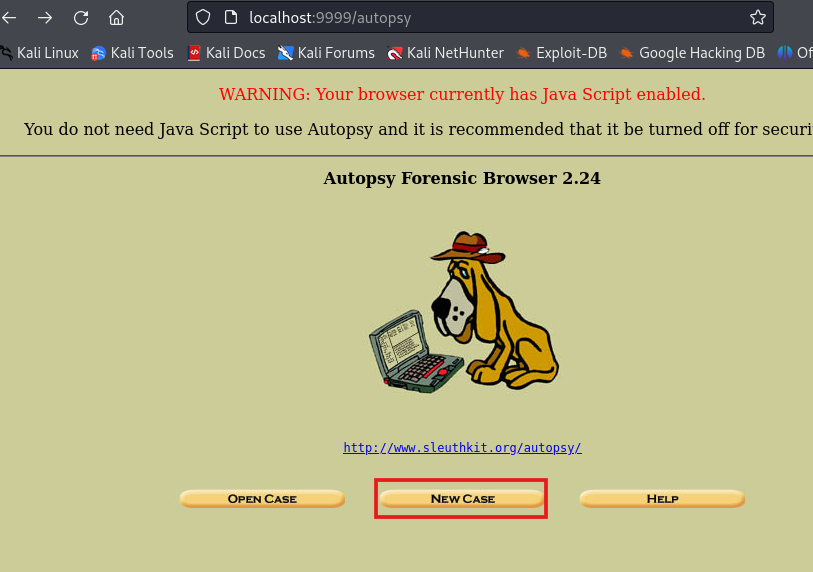
1. Buka program Autopsy melalui menu → Applications → Kali Linux → Forensics → Forensic Suites → Autopsy.
2. Setelah terbuka, akan muncul terminal Autopsy. Jangan menutup terminal selama program Autopsy berjalan.
3. Kemudian buka address **http://localhost:9999/autopsy** menggunakan web browser.

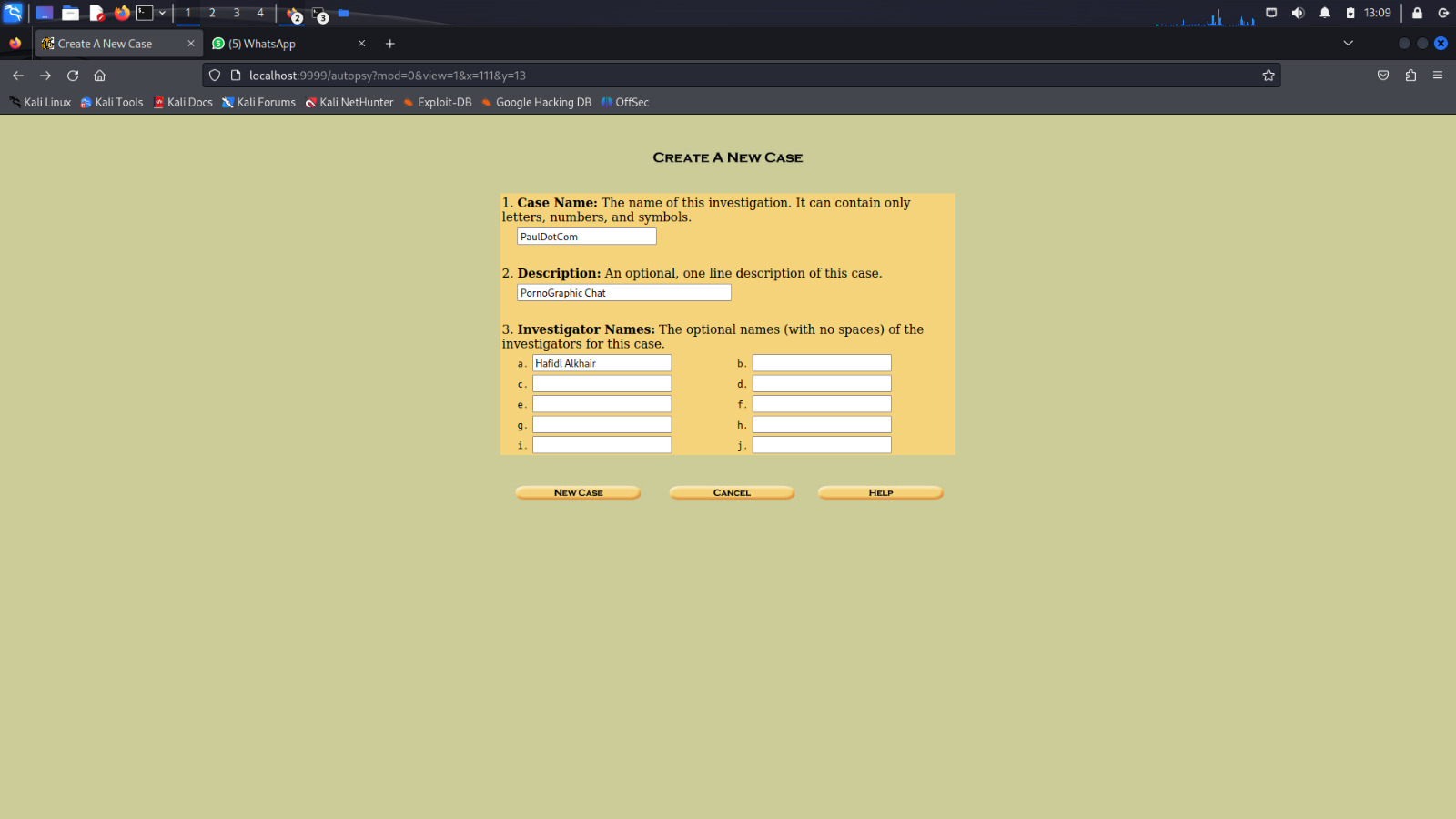


1. Semua file yang digunakan oleh kasus dalam program Autopsy ini akan disimpan di Evidence Locker dengan path-nya adalah **/var/lib/autopsy**.

## Membuat Kasus Baru

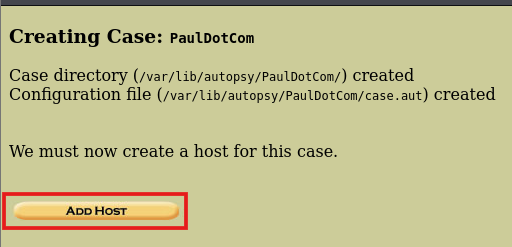
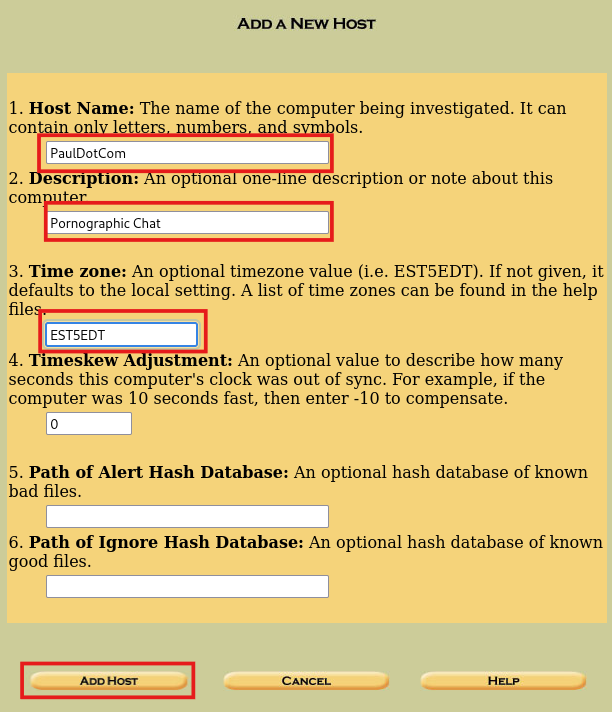
1. klik tombol **Add Case**.



1. Sesuikan pada gambar

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.

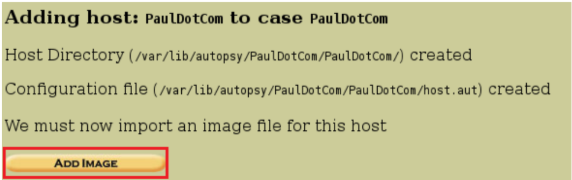
## Menambahkan Host ke Kasus

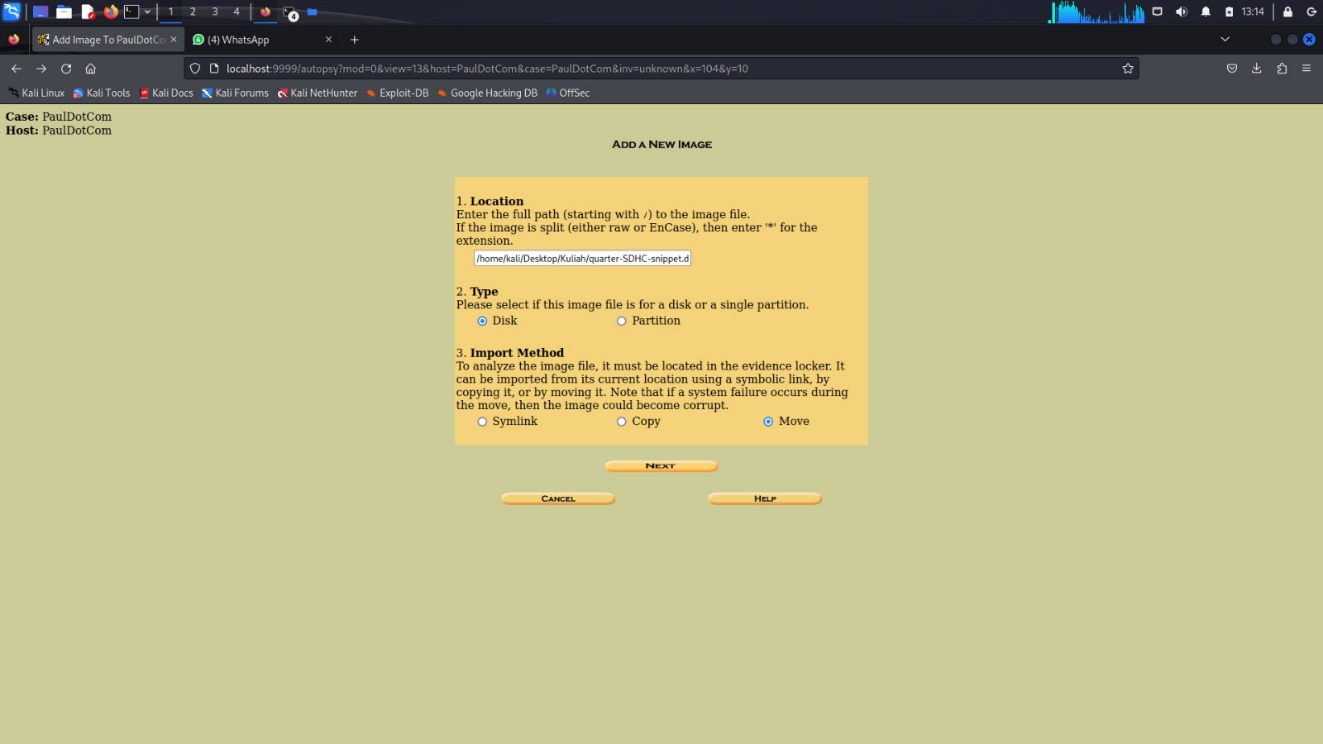
1. Selanjutnya adalah menambahkan host untuk kasus PaulDotCom ini.
2. Klik pada tombol Add Host.
3. Kemudian isi data host sebagai berikut:

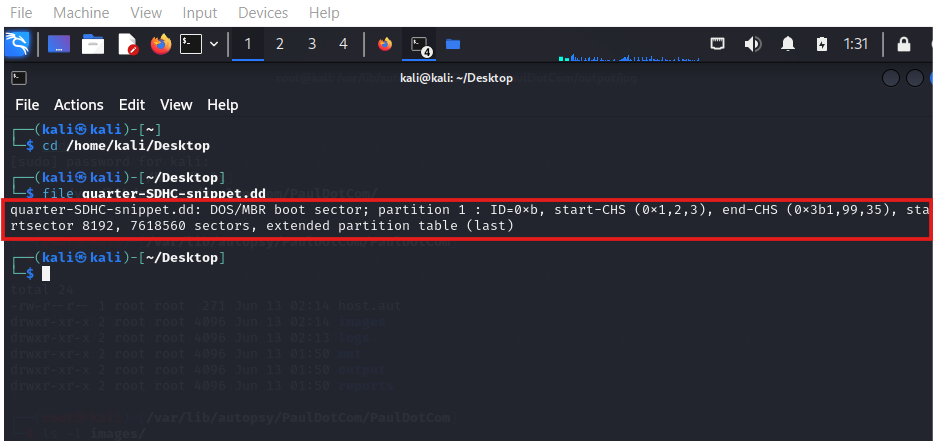
Field yang lain biarkan default. Untuk bantuan pemilihan *timezone*, dapat dilihat pada halaman *HELP* dari program *Autopsy* ini.

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

## 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:



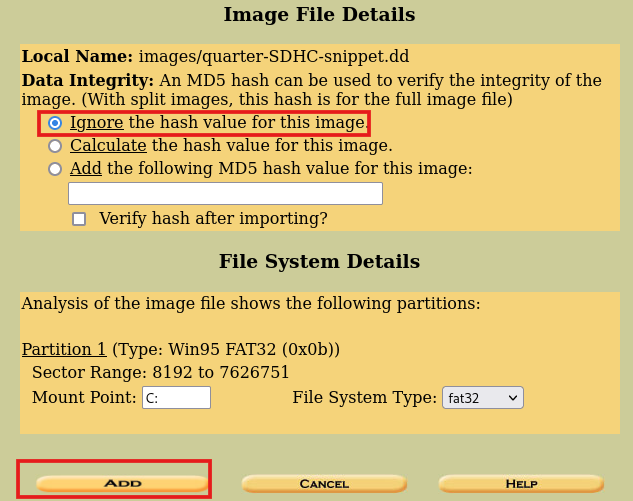
1. Untuk memeriksa Type yang akan digunakan, jalankan perintah berikut di terminal Linux:

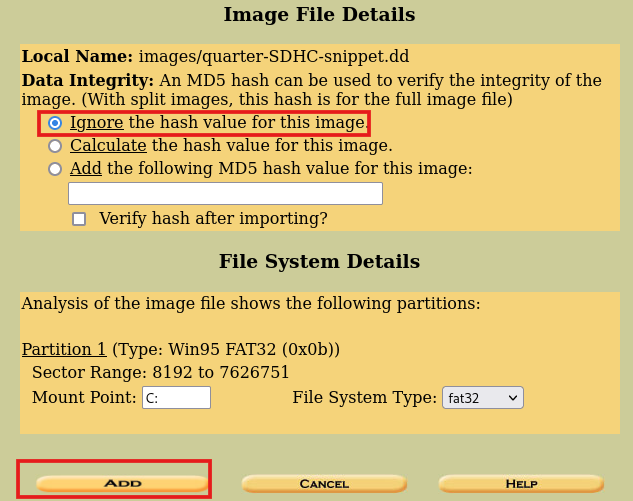
Jika terdapat lebih dari satu partisi, pilih Type: Disk. Berikut penjelasan mengenai Import Method:

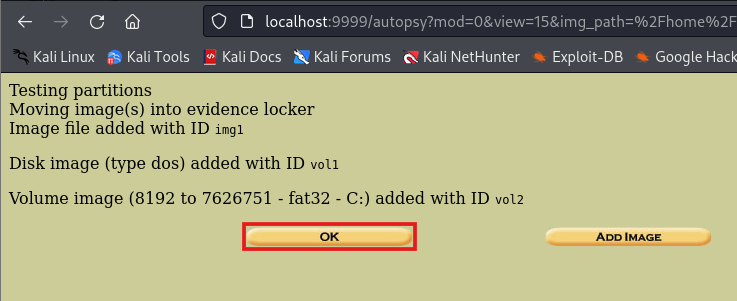
1. Symlink: Membuat tautan simbolik (seperti shortcut) ke file image tanpa perlu menyalin file aslinya ke dalam Evidence Locker. Metode ini hemat ruang karena file aslinya tetap berada di lokasi awal.
2. Copy: Menyalin file image asli ke dalam Evidence Locker. Cara ini membuat salinan baru sehingga file asli tetap aman di tempat semula, namun membutuhkan ruang penyimpanan tambahan.
3. 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.

## Data Integrity

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



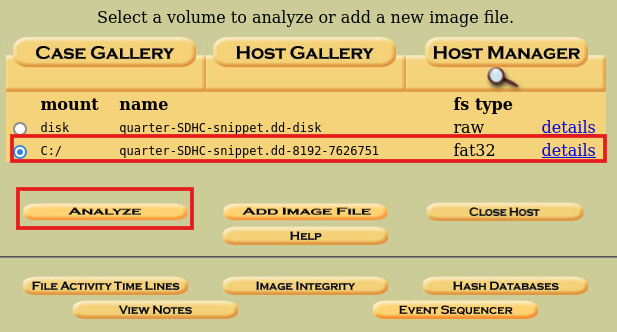
1. Opsi Ignore dipilih karena Autopsy hanya mendukung MD5 hash, sementara file raw image yang dianalisis menggunakan SHA256 hash.
2. Biarkan field lainnya pada pengaturan default, lalu klik tombol Add. Di halaman konfirmasi, tekan tombol OK.

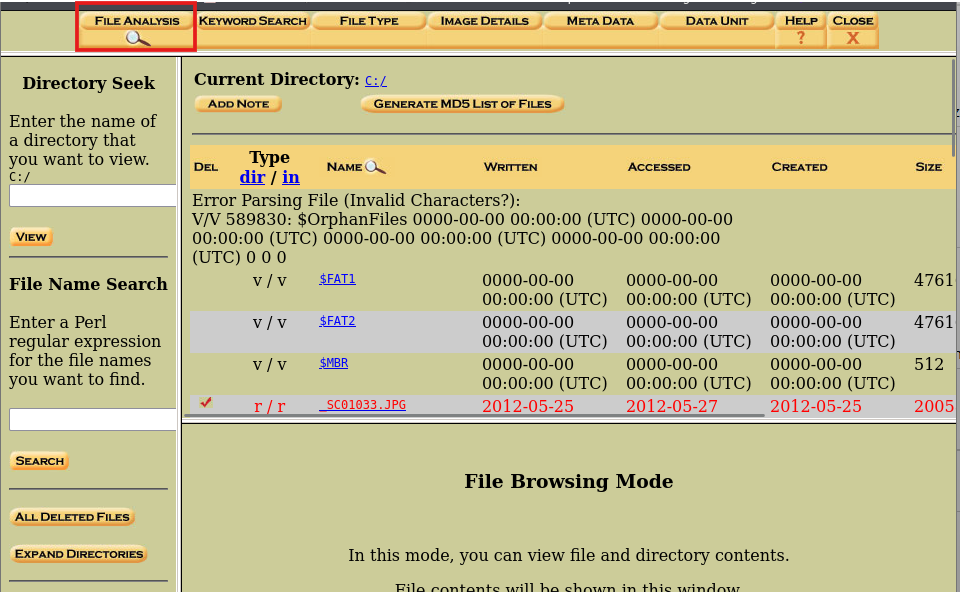


File image dalam Evidence Locker untuk kasus ini akan disimpan di folder /var/lib/autopsy/PaulDotCom/PaulDotCom/images.

## Menganalisis File System

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

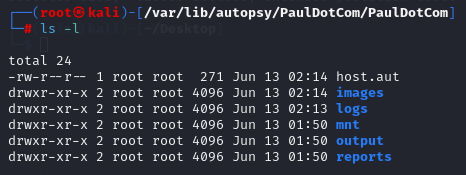


1. Klik pada tab File Analysis, maka semua file yang ada dalam image quarter-SDHC-snippet.dd akan muncul.
2. Scroll ke bawah pada panel evidence item, dan temukan file-file yang tertulis dengan warna merah.



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

## Recovery File

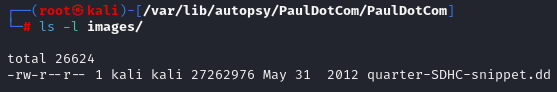
1. Melakukan Recovery File di Kali Linux  
   Ada dua cara untuk mengembalikan file yang terhapus di Kali Linux menggunakan terminal:
2. foremost: Mengembalikan file dan mengelompokkannya berdasarkan jenis file.
3. photorec: Juga bisa mengembalikan file, tapi semua jenis file dicampur tanpa pemisahan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

Penjelasan output:

1. total 24: Total ukuran file dalam direktori.
2. File dan folder yang ditampilkan mencakup:

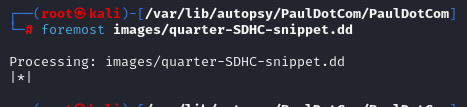
* host.aut: File konfigurasi Autopsy.
* images: Folder yang berisi file image yang akan dianalisis.
* logs, mnt, output, reports: Folder untuk menyimpan log, mounting point, hasil recovery, dan laporan.

1. Masuk ke folder images untuk melihat file image yang akan dianalisis.



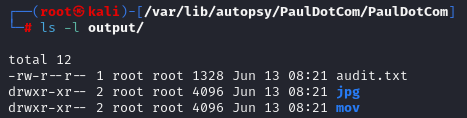
Penjelasan output:

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

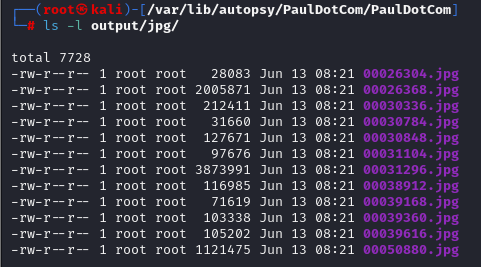
1. Jalankan Perintah Foremost. Gunakan perintah foremost untuk melakukan recovery file dari image.

Penjelasan output:

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

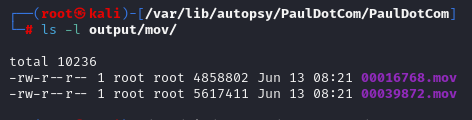
1. Tampilkan daftar file di folder output. Setelah proses recovery selesai, tampilkan hasil recovery di folder output.

Penjelasan output:

1. Terdapat file audit.txt dan dua folder: jpg dan mov.
2. jpg berisi file gambar yang berhasil direcovery, sedangkan mov berisi file video.
3. Tampilkan daftar file gambar ter-recovery. Masuk ke folder jpg untuk melihat file gambar yang telah direcovery.

Penjelasan output:

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

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

Penjelasan output:

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

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



Kemudian, jalankan perintah berikut.

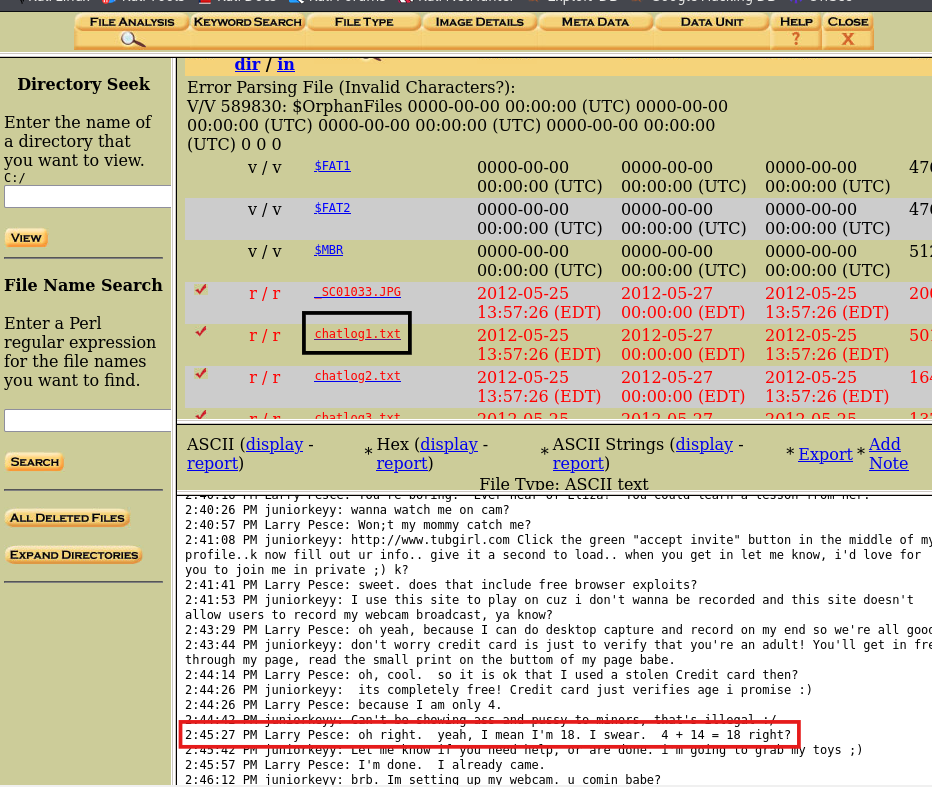
Penjelasan output:

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

## Jawaban Challenge

1. In his conversation with juniorkeyy, how old does Larry initially say he is?

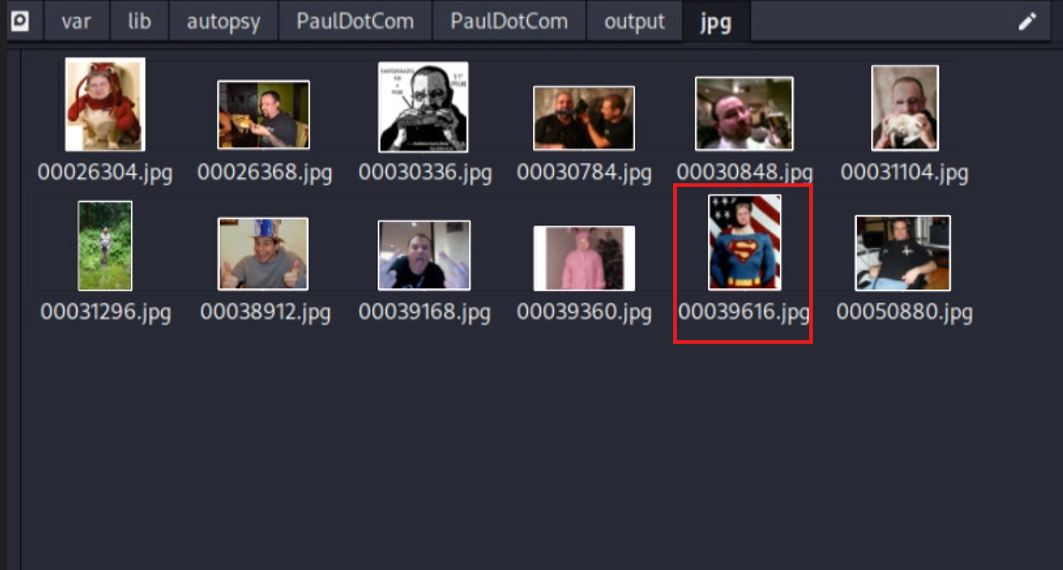
Asumsinya, jika disebut "conversation," maka yang perlu diperiksa adalah log dari percakapan yang ada. Untuk mengetahui jawaban dari challenge tersebut, cek file chatlog dimulai dari chatlog1.txt.



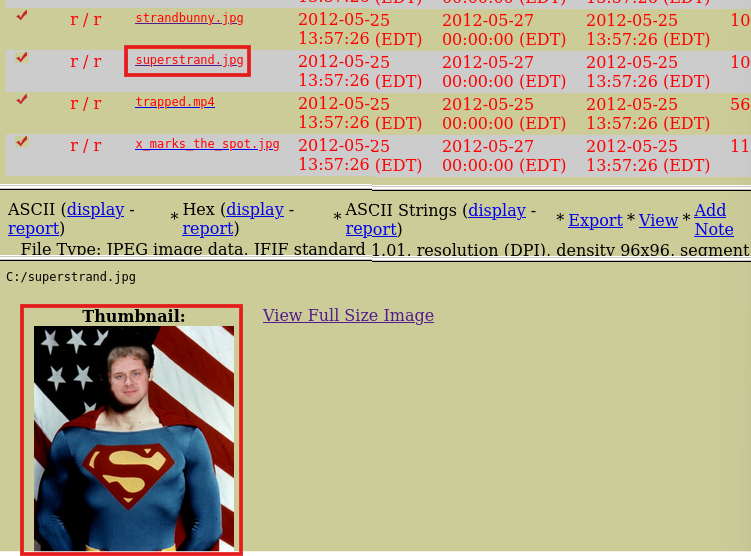
Ditemukan bahwa jawabannya adalah 4 tahun, karena yang ditanyakan adalah “initially,” yang berarti “pada awalnya.”

1. What was the filename of the file that had the following SHA256 sum:e56931935bc60ac4c994eabd89b003a7ae221d941f1b026b05a7947a48dc9366.

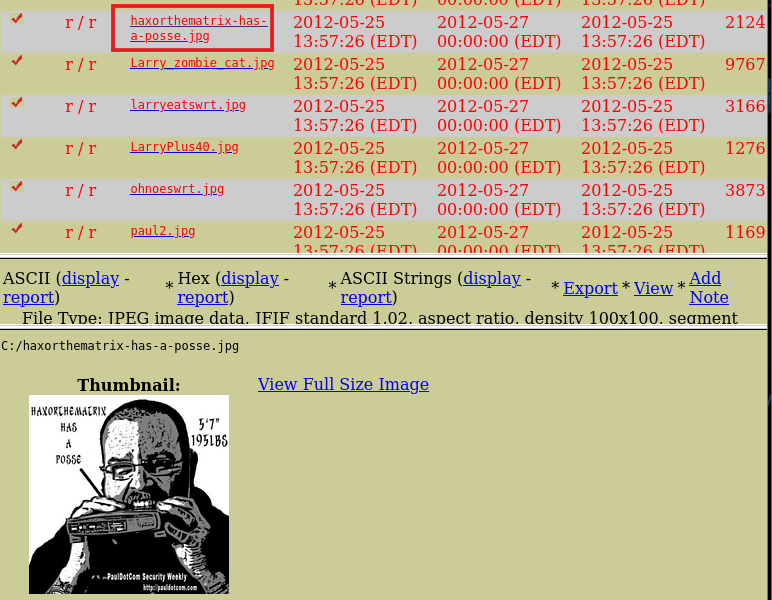
Setelah mencocokkan dengan hasil sha256sum yang telah dijalankan di terminal Linux, ditemukan bahwa nama file tersebut adalah 00039616.jpg (file ter-recover). Selanjutnya, buka folder /var/lib/autopsy/PaulDotCom/PaulDotCom/output/jpg melalui explorer untuk melihat gambar tersebut.

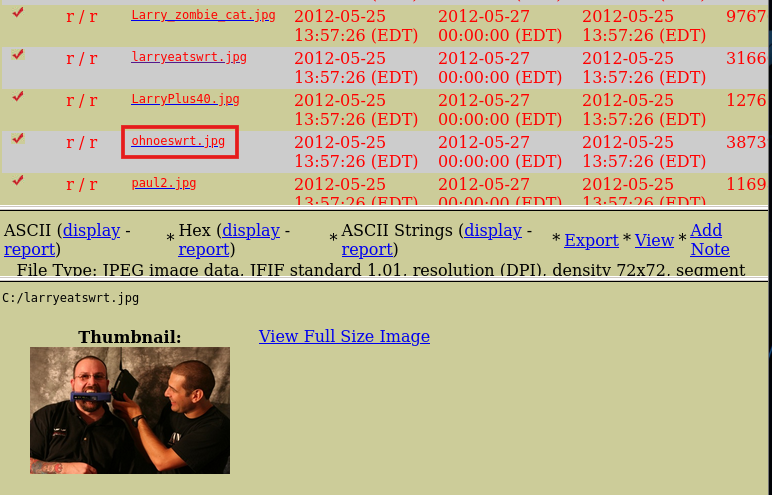


Setelah ditemukan, lakukan pencocokan gambar dengan gambar file aslinya dengan mengklik satu per satu gambar JPG di program Autopsy hingga menemukan gambar yang sama.



1. 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.



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:

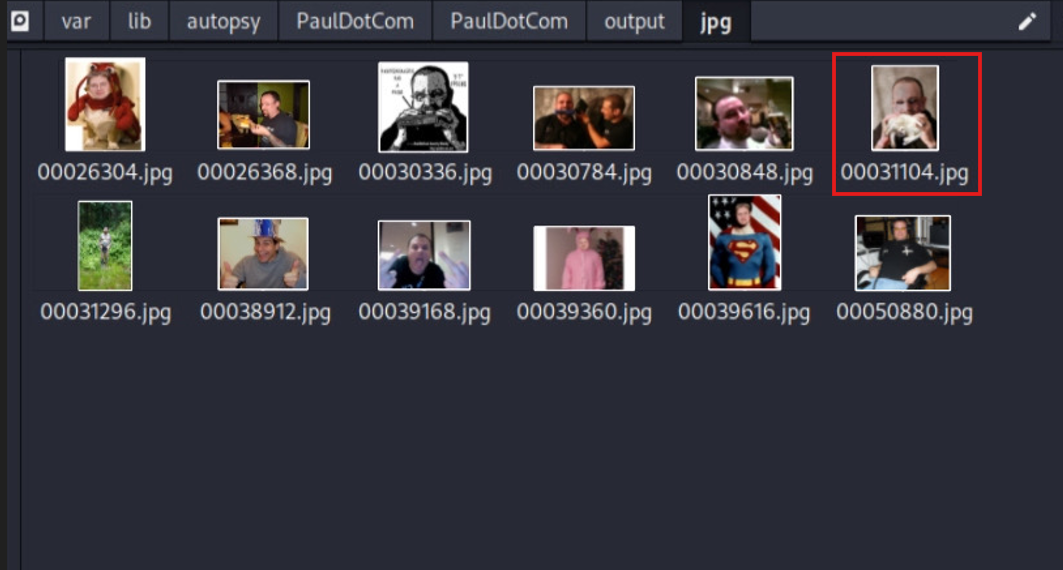
1. 00030336.jpg untuk haxorthematrix-has-a-posse.jpg
2. 00030784.jpg untuk larryeatswrt.jpg

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

1. 00030336.jpg: e4e2fac9fc41546239d4e534bfe6588e4796f3799befc09b2787f5ad6c75faca
2. 00030784.jpg: 1bdfd9d7445d38fdb7ba5acbb58669cf31c7c568c7aa6e6fcf0c961628f4c32e
3. 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.

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:

1. 00031104.jpg: 9c0a8bc6c3baa2ad7f390ef4e41c3edf3d98a543f492afb50a4bab8700af5766

# BAB III PENUTUP

## 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.