



# PERTEMUAN 8

STUDI KASUS PADA AUTOPSY



# TOOLS

- Autopsy (Software)

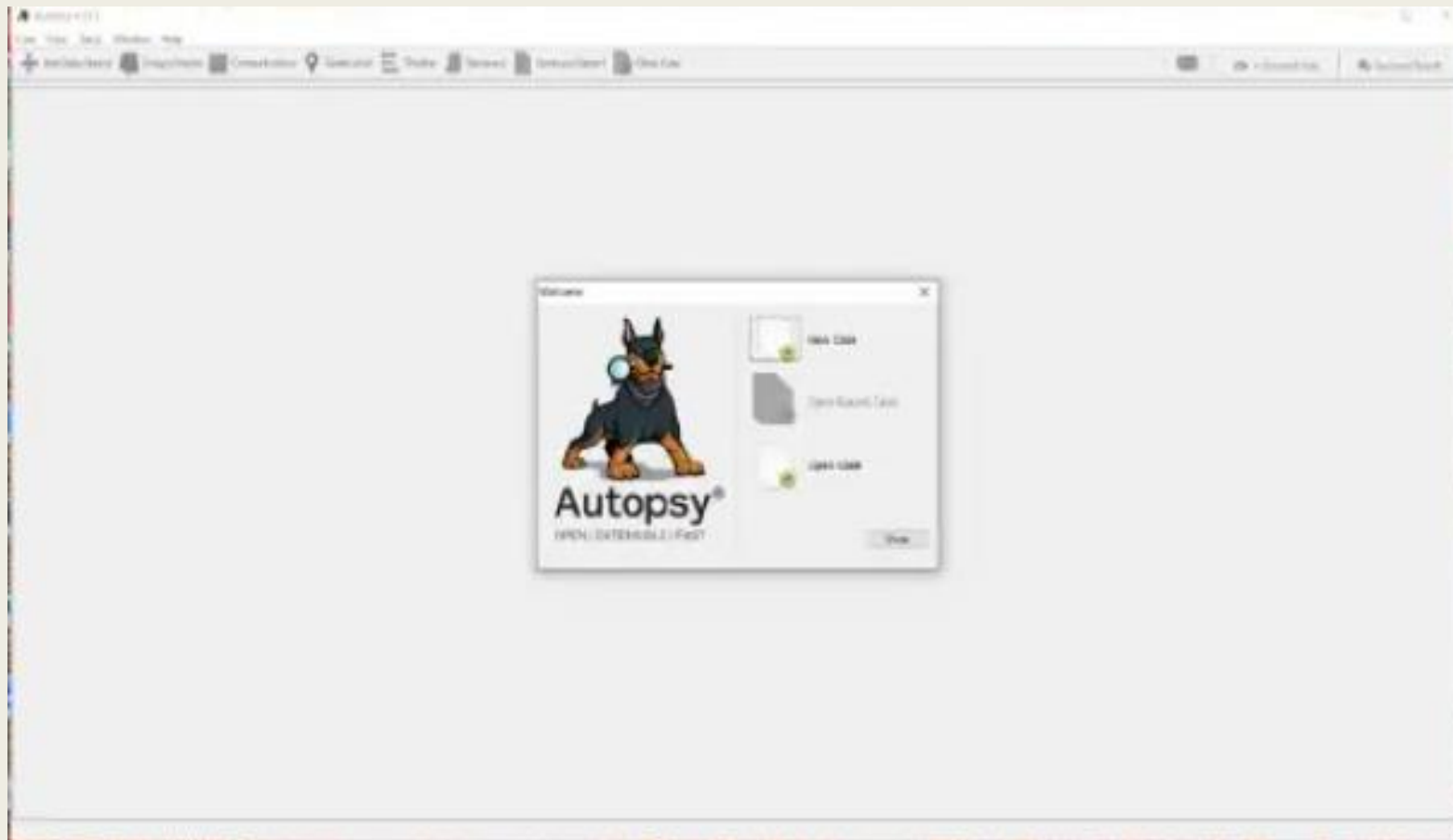
Aplikasi yang dibuat khusus untuk menganalisa atau membaca file yang tersimpan di dalam disk. Aplikasi Autopsy tidak hanya bisa untuk membaca file saja, bahkan, bisa digunakan untuk mencari dan mengembalikan file yang telah terhapus dari sistem. Digunakan Untuk Menganalisa Data & Recovery Beberapa Ekstensi File Yang Terhapus seperti PDF, Foto, Text.

Biasanya Digunakan Untuk Praktek Akuisisi Data Untuk Forensic Data Digital.

- File Imager (Sample)

Disk Image adalah suatu proses dari file tunggal atau suatu perangkat media penyimpanan yang mengandung isi lengkap dengan strukturnya yang kemudian di perbanyak / duplikat / penggandaan dengan isi dan struktur yang sama persis/sempurna dari yang asli tanpa selisih ukuran se-bit pun di dalamnya.

- New Case = Membuat Case Autopsy Yang Baru
- Open Recent Case = Membuka Case Yang Pernah Dibuka atau dibuat
- Open Case = Membuka Case Yang Tersimpan Dalam Komputer



# Database Autopsy

**New Case Information**

**Steps**

1. **Case Information**
2. Optional Information

**Case Information**

Case Name: Kasus Pencurian Motor

Base Directory: D:\Bram\Semester 7\Autopsy 1 Browse

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

D:\Bram\Semester 7\Autopsy 1\Kasus Pencurian Motor

< Back Next > Finish Cancel Help

- Case Name : Nama Case Tersebut
- Base Directory : Pilih Direktori Yang Mau Digunakan Untuk Menyimpan Database Autopsy
- Case Type : Single-User

# Database Autopsy

New Case Information

**Steps**

1. Case Information
2. Optional Information

**Optional Information**

Case

Number: CN-01

Examiner

Name: Ibrahim Asshabirin

Phone: 081286293669

Email: Bramrambramtut@gmail.com

Notes: Kasus Pencurian Motor

Organization

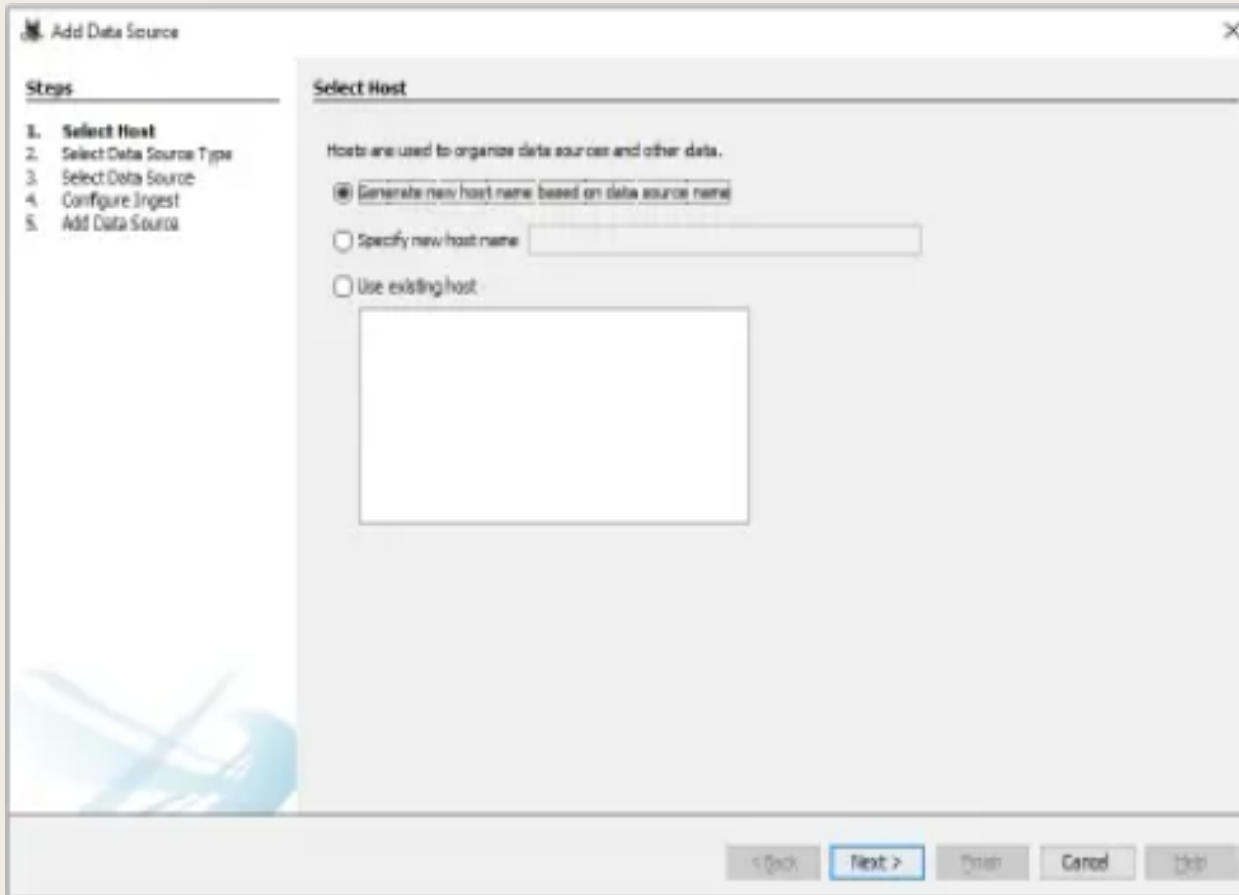
Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

Merupakan informasi mengenai kasus tersebut secara umum, serta informasi examiner atau penguji kasus tersebut.

- Data Yang Diisi Yaitu Case Number, Examiner Data (Nama, Phone, Email, Notes)

# Data Source Yang Akan Di Analisa & Diakuisisi.

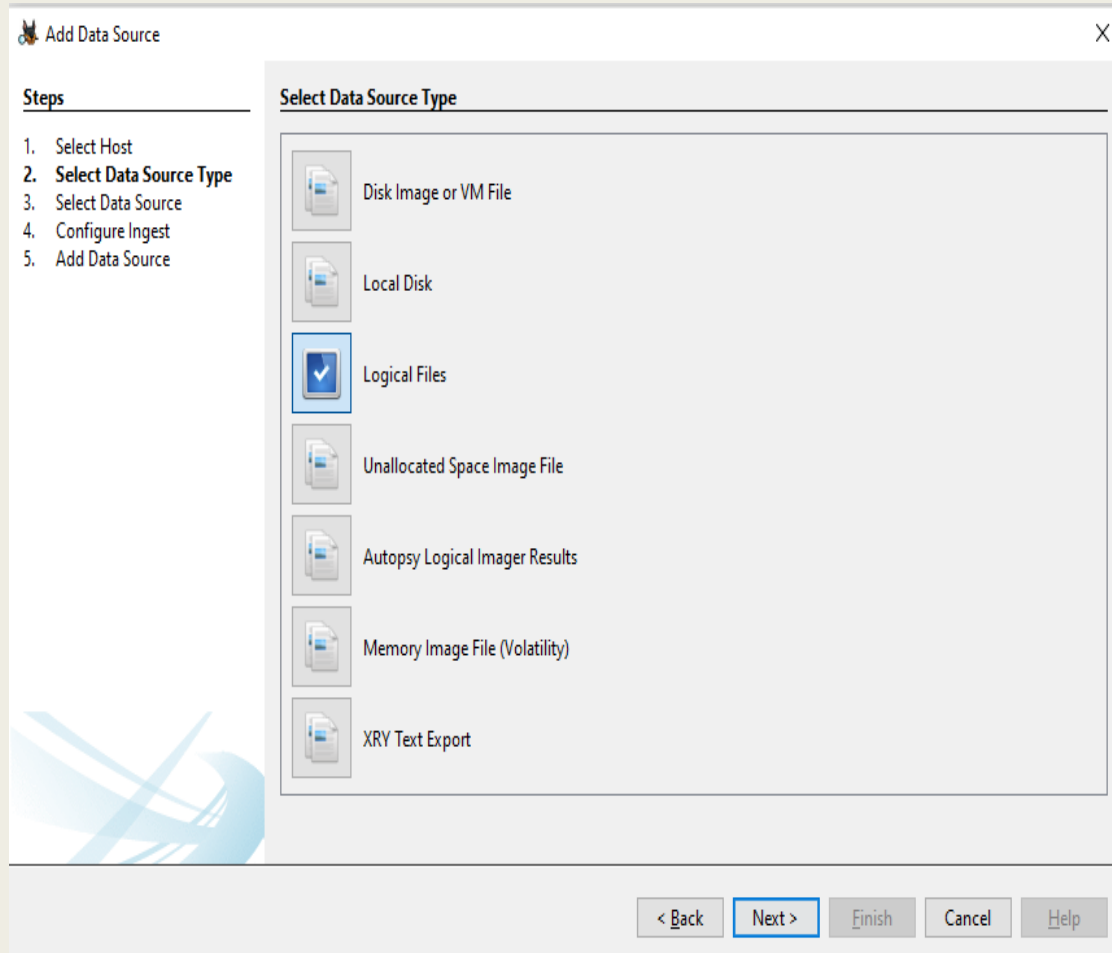


The screenshot shows a software window titled "Add Data Source" with a close button in the top right corner. On the left, a "Steps" sidebar lists five steps: 1. Select Host (highlighted), 2. Select Data Source Type, 3. Select Data Source, 4. Configure Ingest, and 5. Add Data Source. The main area is titled "Select Host" and contains the text "Hosts are used to organize data sources and other data." Below this, there are three radio button options: "Generate new host name based on data source name" (which is selected), "Specify new host name" (with an adjacent text input field), and "Use existing host" (with an adjacent empty rectangular box). At the bottom of the window, there are five buttons: "< Back", "Next >" (highlighted in blue), "Finish", "Cancel", and "Help".

1. Select Host Data Source keterangan:

- ☐ Generate New Host name based on datasource name: digunakan untuk membuat otomatis nama host baru pada data source
- ☐ Specify new host name: digunakan untuk menentukan nama host secara manual
- ☐ Use Existing host: digunakan untuk memilih host yang sudah ada atau pernah dibuat.

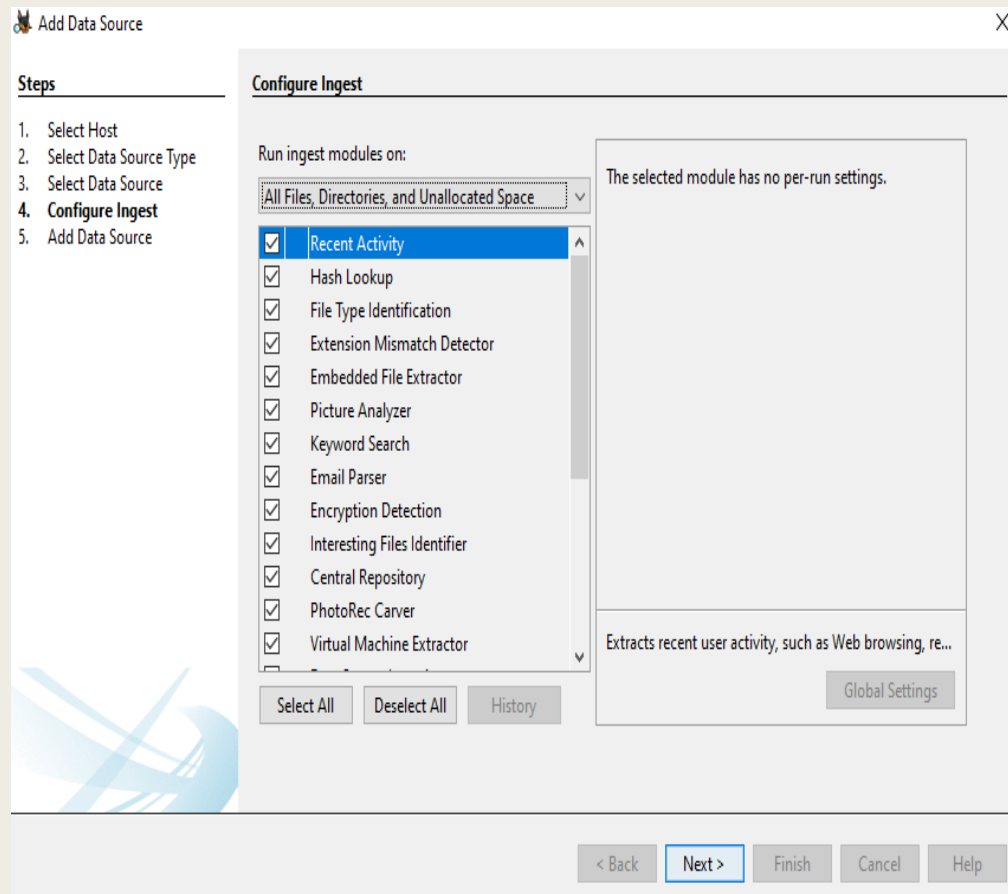
# Data Source Yang Akan Di Analisa & Diakuisisi.



## 2. Select Data Source Type keterangan:

- ☐ Disk Image or VM File: jika perangkat tersebut berupa imaging atau virtual (VM)
- ☐ Local Disk: jika perangkat tersebut berupa Physical Drive Seperti FlashDisk, HardDisk, SSD
- ☐ Logical Files: jika perangkat tersebut berupa Logical File seperti CD, DVD
- ☐ Unallocate Space Image File: jika perangkat tersebut merupakan space kosong pada suatu komputer yangdigunakansebagai harddisk yang sudah di imager.
- ☐ Autopsy Logical Imager Results: jika perangkat tersebut berupa File Dengan Ektensi (.Aut) dari Autopsy
- ☐ Memory Image File (Volatility): semua jenis file yang tidak berisi sistem file tetapi ingin menjalankannya melalui ingest.
- ☐ XRY Text Export: jika perangkat tersebut hasil dari mengekspor file teks dari XRY.

# Data Source Yang Akan Di Analisa & Diakuisisi.

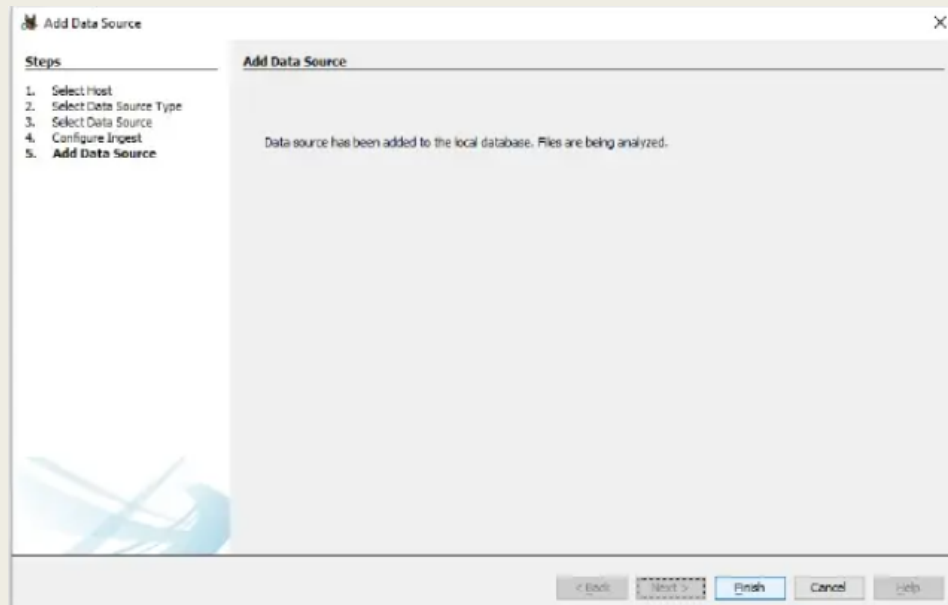
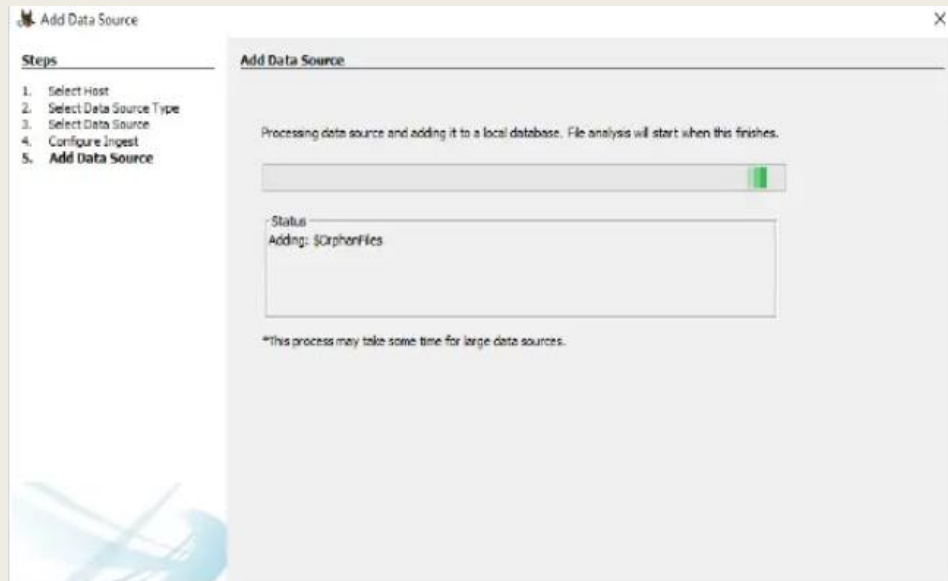


Configure Ingest “Checklist Semua” : Digunakan untuk Mencari File atau User Konten Dengan Cepat



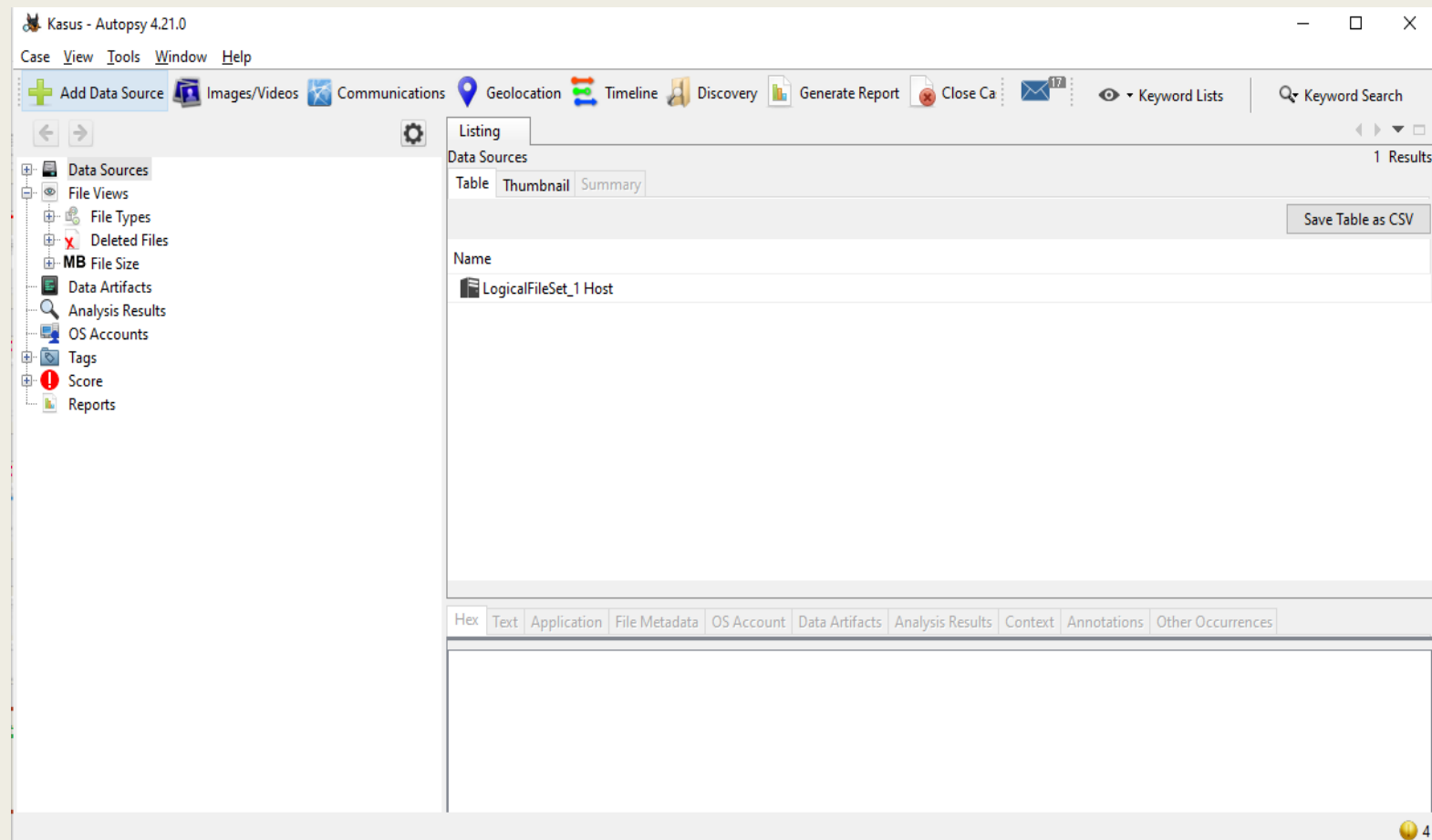
# Data Source Yang Akan Di Analisa & Diakuisisi.

Add Data Source: Tunggu Proses Add Data Source Ke Software Autopsy

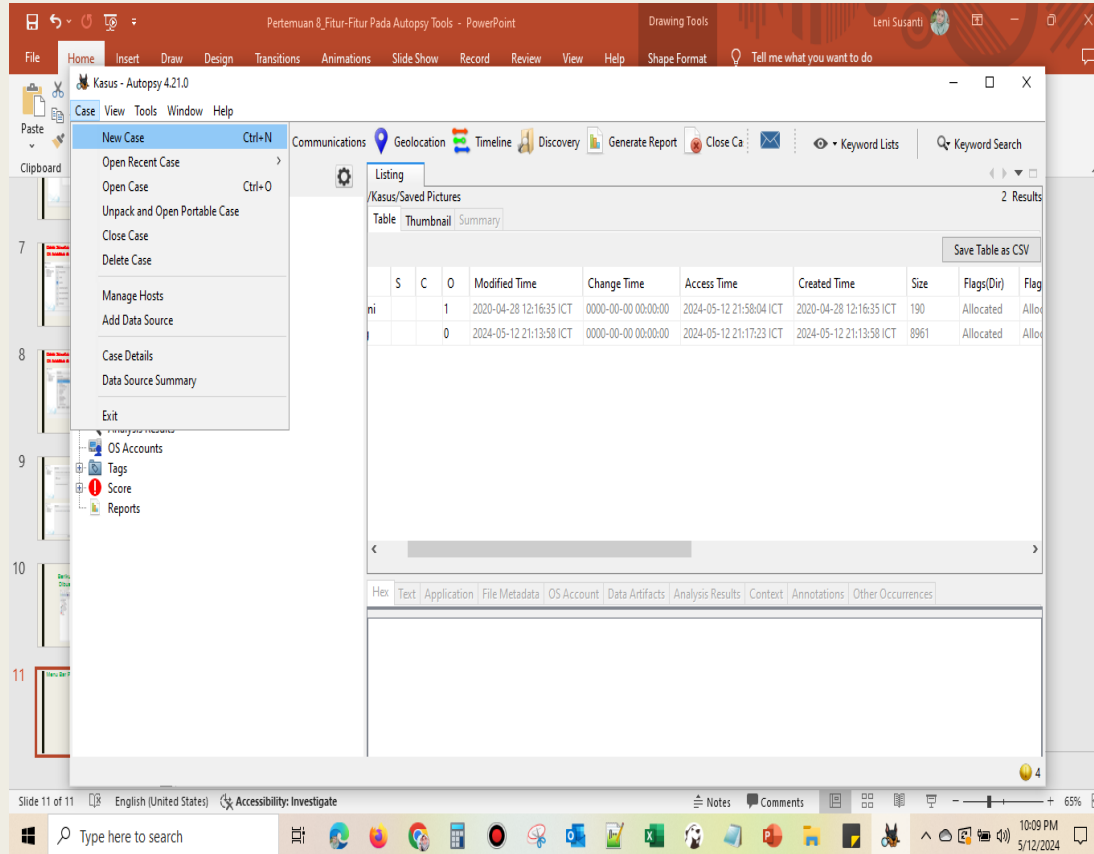


Klik Finish & Tunggu Data Selesai Diproses

# Berikut tampilan Autopsy Setelah Dibuat Database & Data Source



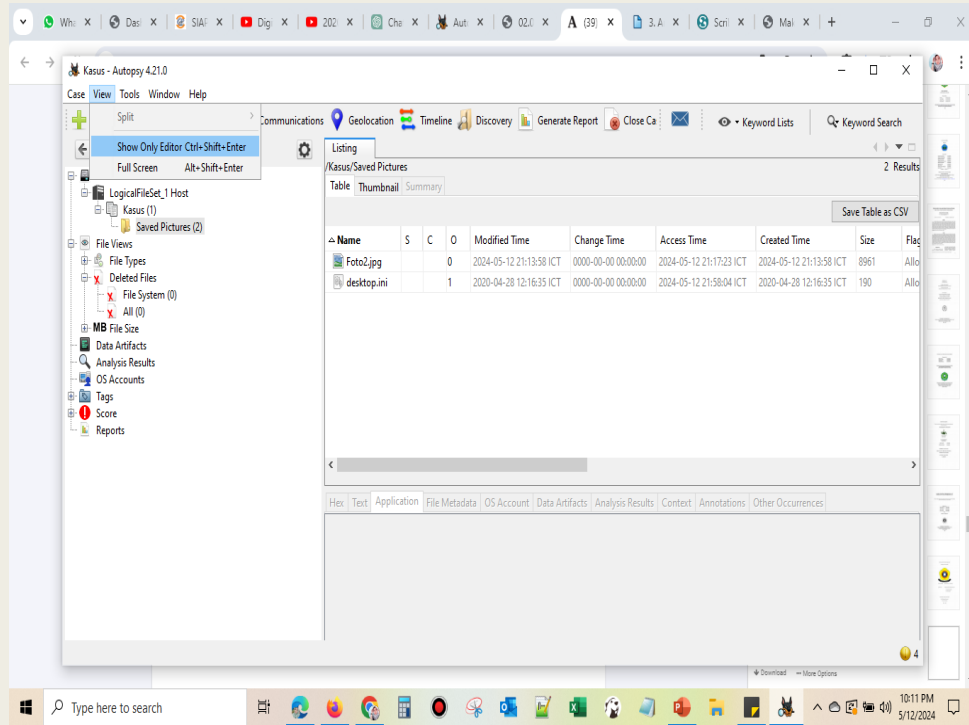
# Menu Bar Pada Autopsy



## CASE

- New case untuk membuat case baru.
- Open case untuk membuka case.
- Open recent untuk membuka case yang telah terbuka sebelumnya.
- Close case untuk keluar dari case.
- Add data source untuk memasukkan data source.
- Case details untuk melihat isi dari case.
- Exit untuk keluar.

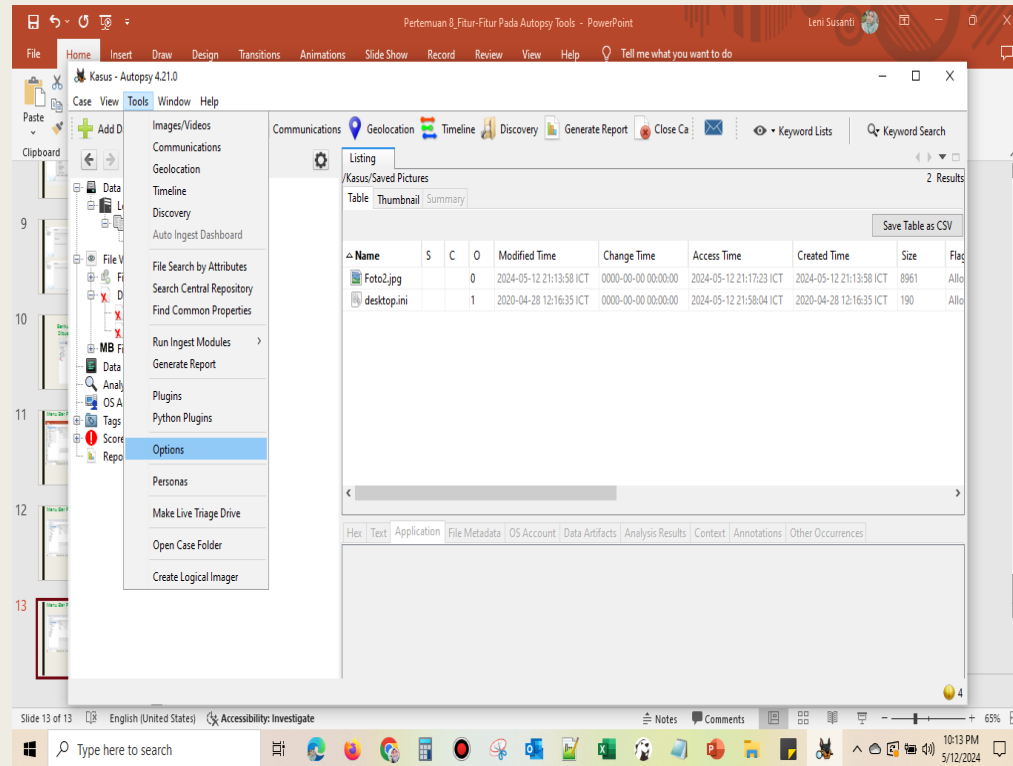
# Menu Bar Pada Autopsy



## VIEW

- Split untuk melihat case yang tertukar.
- Show only editor untuk melihat case yang hanya di edit
- Full screen untuk melihat bentuk window full.

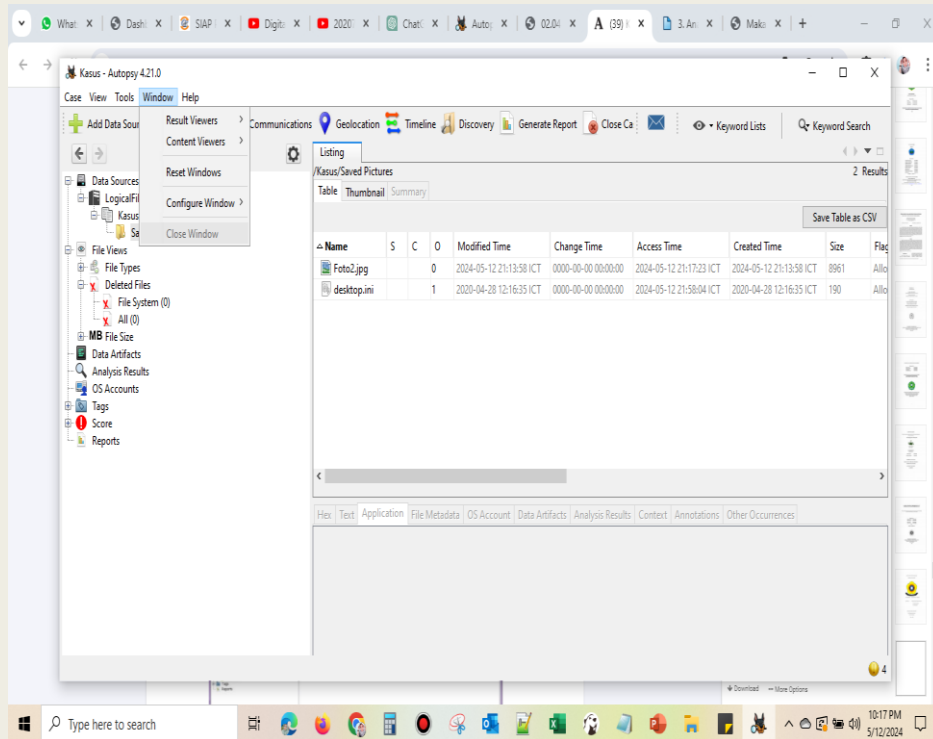
# Menu Bar Pada Autopsy



## TOOLS

- View Images/videos untuk melihat gambar atau vidio.
- Timeline melihat garis masa case.
- Generate report untuk mereport case yang diinginkan.
- File search by attributes untuk mencari file dari atribut.
- Run ingest modules untuk menjalankan case yang sudah di pilih.
- Plugins konten untuk mengetahui fungsional case.
- Pyton plugins mirip dengan plugins tapi ini lebih merujuk ke file-nya.
- Options pengaturan.
- Open output folder untuk membuka keluaran folder

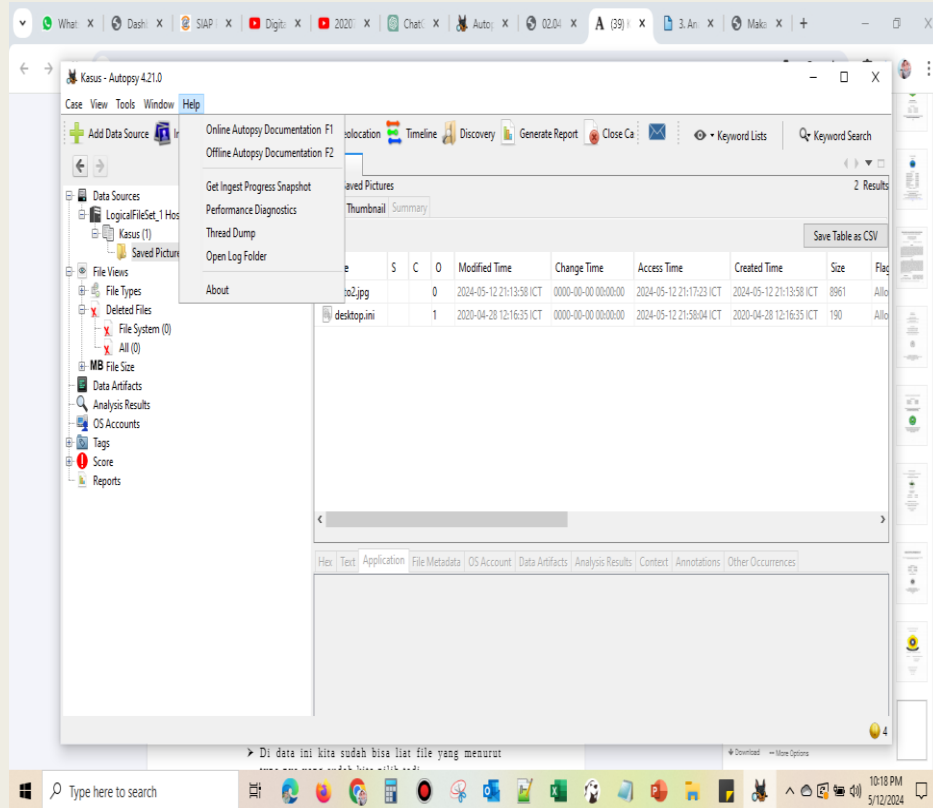
# Menu Bar Pada Autopsy



## WINDOWS

- Directory listing untuk melihat listing yang ada
- Data result untuk melihat hasil listing directory.
- Data content adalah konten-konten data.
- Configure window untuk mensetting window yang di inginkan.
- Close window tools perintah untuk keluar dari window.

# Menu Bar Pada Autopsy



## HELP

- Online autopsy documention untuk membantu mengoperasikan autopsy secara online
- Offline autopsy documention untuk membantu mengoprasikan autopsy secara offline.
- Image/vedio gallery help untuk membantu membuka file gambar atau vedio.
- Get ingest progress snapshot: mendapatkan informasi tentang proses yang berlangsung.
- Performance dianostics: untuk melihat performa yang di diagnosa.
- Open log folder: untuk membuka folder.
- About: informasi tentang autopsy.

# STUDI KASUS

Ditemukan sebuah kasus kejahatan dan ditemukan barang bukti dari smartphone yang sudah diamankan dalam format file, untuk kemudian dilakukan proses analisa.

[https://drive.google.com/file/d/1AJm9B0-otp5W1IvoEx6dbbGQAF9o4AsB/view?usp=drive\\_link](https://drive.google.com/file/d/1AJm9B0-otp5W1IvoEx6dbbGQAF9o4AsB/view?usp=drive_link)

Pertanyaan setelah proses analisa yang dilakukan adalah sebagai berikut:

1. Siapa saja nama-nama yang terlibat dalam kasus ini, dan selidiki profesi mereka?
2. Apa nama file dari file yang memiliki jumlah SHA256 berikut:  
e56931935bc60ac4c994eabd89b003a7ae221d941f1b026b05a7947a48dc9366?
3. Berapa jumlah SHA256 foto dari gambar "dd" yang menunjukkan Larry menggigit routernirkabel? Lakukan checksum dengan powershell setelah mengextract file tersebut, lalutampilkan metadatanya !
4. Berapa jumlah SHA256 dari gambar yang menunjukkan zombie Larry menggigit seekor kucing?



# Proses Analisa Barang Bukti

- Buatlah New Case pada kasus tersebut dengan menggunakan aplikasi Autopsy, ikuti Langkah-Langkah yang sudah dijelaskan di atas.
- Hal-hal yang perlu dilakukan untuk menjawab pertanyaan kasus di atas adalah sebagai berikut:

# 1. Siapa saja nama-nama yang terlibat dalam kasus ini, dan selidiki profesi mereka?

LANGKAH 1. Cari Tau Lebih Lanjut Hasil Autopsy & Analisa Apakah Ada Yang Bisa Digunakan Untuk Menentukan Nama-nama yang terlibat dalam kasus tersebut.

#Ada Ekstensi Plain text Yang Termuat Dalam File Ini Sebagai Bukti. Terdapat Beberapa File chatlog1.txt – chatlog5.txt

LANGKAH 2. Export Kelima File Tersebut Untuk Melihat Isinya. Klik Kanan > Export File(s). Kemudian Buktikan File Metadatanya Apakah Sesuai Dengan File Autopsy

LANGKAH 3. Telaah atau Analisa Isi File tersebut.

# 1. Siapa saja nama-nama yang terlibat dalam kasus ini, dan selidiki profesi mereka?

LANGKAH 1. Cari Tau Lebih Lanjut Hasil Autopsy & Analisa Apakah Ada Yang Bisa Digunakan Untuk Menentukan Nama-nama yang terlibat dalam kasus tersebut.

#Ada Ekstensi Plain text Yang Termuat Dalam File Ini Sebagai Bukti. Terdapat Beberapa File chatlog1.txt – chatlog5.txt

LANGKAH 2. Export Kelima File Tersebut Untuk Melihat Isinya. Klik Kanan > Export File(s). Kemudian Buktikan File Metadatanya Apakah Sesuai Dengan File Autopsy

LANGKAH 3. Telaah atau Analisa Isi File tersebut.

2. Apa nama file dari file yang memiliki jumlah SHA256 berikut:  
e56931935bc60ac4c994eabd89b003a7ae221d941f1b026b0  
5a7947a48dc9366?

LANGKAH 1. Cari Per-Ekstensi File, Kemudian Cari Hingga Sesuai SHA256 Checksum Dengan soal Yang Disampaikan. Dengan Mengecek Metadata Tersebut.

LANGKAH 2. Lihat File Tersebut Melalui Application > Klik Kanan > Eksport file (s)# Cari Letak File Yang akan disimpan hasil exportnya

LANGKAH 3. Buka File Yang Sudah Dieksport Tadi , Kemudian Jalankan Windows PowerShell Di Komputer Untuk Mencocokkan Hash Autopsy dengan Yang Telah Diexport

Di Windows PowerShell Ketikkan Seperti Dibawah Ini :

- `get-filehash <Tarik File Yang Diexport Tadi > -algorithm md5` kemudian enter
- `get-filehash <Tarik File Yang Diexport Tadi > -algorithm SHA256` kemudian enter

### 3. Berapa jumlah SHA256 foto dari gambar "dd" yang menunjukkan Larry menggigit router nirkabel? Lakukan checksum dengan powershell setelah mengextract file tersebut, lalu tampilkan meta datanya !

LANGKAH 1. Cari Per-Ekstensi File, Kemudian Cari Hingga Sesuai Dengan Ketentuan Yaitu“Larry Menggigit Router Nirkabel” Dengan Soal Yang Disampaikan. Dengan Mengecek MetadataTersebut.

**Foto 1 (Larry Menggigit Router Hitam Putih)**

**Foto 2 (Larry Menggigit Router Ditemani Temannya Dikanan Memegang Router)**

LANGKAH 2. Lihat File Tersebut Melalui Application > Klik Kanan > Eksport file (s)# Cari Letak File Yang akan disimpan hasil exportnya

LANGKAH 3. Buka File Yang Sudah Dieksport Tadi , Kemudian Jalankan Windows PowerShellDi Komputer Untuk Mencocokkan Hash Autopsy dengan Yang Telah Diexport.

Di Windows PowerShell Ketikkan Seperti Dibawah Ini :

- `get-filehash <Tarik File Yang Diexport Tadi > -algorithm md5` kemudian enter
- `get-filehash <Tarik File Yang Diexport Tadi > -algorithm SHA256` kemudian enter

## 4. Berapa jumlah SHA256 dari gambar yang menunjukkan zombie Larry menggigit seekor kucing?

LANGKAH 1. Cari Per-Ekstensi File, Kemudian Cari Hingga Sesuai Dengan Ketentuan Yaitu “Zombie Larry Menggigit Seekor Kucing” Dengan Soal Yang Disampaikan. Dengan Mengecek Metadata Tersebut.

LANGKAH 2. Lihat File Tersebut Melalui Application > Klik Kanan > Eksport file (s)# Cari Letak File Yang akan disimpan hasil exportnya.

LANGKAH 3. Buka File Yang Sudah Dieksport Tadi , Kemudian Jalankan Windows PowerShell Di Komputer Untuk Mencocokkan Hash Autopsy dengan Yang Telah Diexport.

Di Windows PowerShell Ketikkan Seperti Dibawah Ini :

- `get-filehash <Tarik File Yang Diexport Tadi > -algorithm md5` kemudian enter
- `get-filehash <Tarik File Yang Diexport Tadi > -algorithm SHA256` kemudian enter

# TUGAS

## PERTEMUAN 09 dan 10

- Buatlah 6 kelompok (anggota bebas)
- Carilah studi kasus kejahatan forensic yang diselesaikan dengan menggunakan tools Autopsy (Praktekan dengan tools Autopsy)
- Kelompok 1, 2 dan 3 presentasi di minggu ke-09, sedangkan kelompok 4, 5, dan 6 presentasi di pertemuan ke-10
- Pada akhir presentasi buatlah 5 soal, ditujukan kepada kelompok yang tidak presentasi (1 kelompok jawab 1 soal)
- 5 Kelompok yang tidak presentasi akan memberikan penilaian untuk performa kelompok yang melakukan presentasi.

