

Autopsy Exercise



Oleh :

1203210015 – Enrico Sulfriando Sinaga

Mata Kuliah Forensik Digital

Program Studi Informatika

Fakultas Teknologi Informasi dan Bisnis

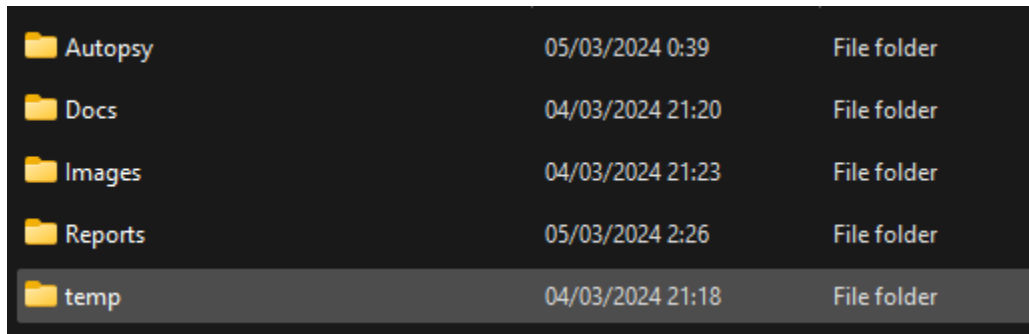
Institut Teknologi Telkom Surabaya

2024

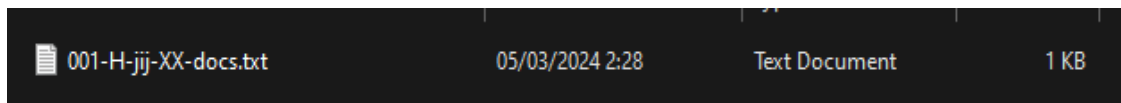
1. Mengunduh Autopsy dari autopsy.com dan menginstalnya
2. Mengunduh dan menginstal HxD (hex editor) untuk membantu proses investigasi
3. Membuat folder cases dengan nomor kasus, indikator jenis kasus, dan inisial investigator



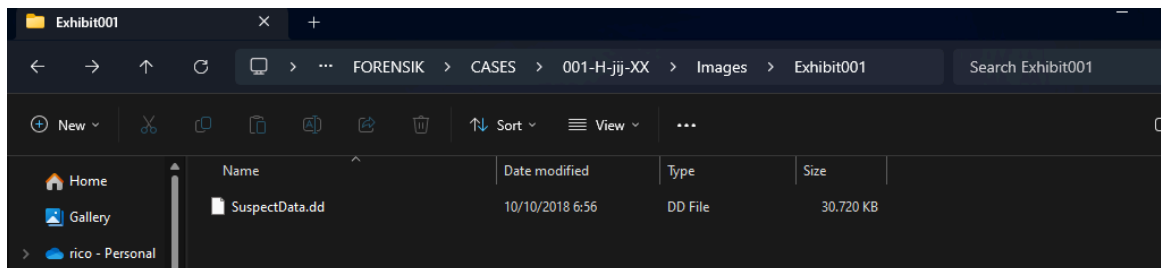
4. Membuat subfolder dokumen docs, images, temp, autopsy, reports



5. Membuat dokumen docs/casenumbers-docs.txt untuk mencatat log aktivitas



6. Memindahkan data target ke folder images/exhibit001



7. Membuka autopsy dan membuat kasus baru dengan nama sesuai folder kasus

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: 001-H-jjj-XX

Base Directory: E:\FORENSIK\CASES\001-H-jjj-XX\Autopsy\ Browse

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

E:\FORENSIK\CASES\001-H-jjj-XX\Autopsy\001-H-jjj-XX

< Back **Next >** Finish Cancel Help

8. Menyimpan data kasus di lokasi folder kasus
9. Mencatat detail kasus seperti nomor kasus, nama investigator, organisasi
10. Menambahkan host baru dengan nama Exhibit001

001-H-jjj-XX - Autopsy 4.21.0

Case View Tools Window Help

+ Add Data Source + Images/Videos + Communications + Geolocation + Timeline + Discovery + Generate Report + Close Case + Keyword Lists + Keyword Search

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

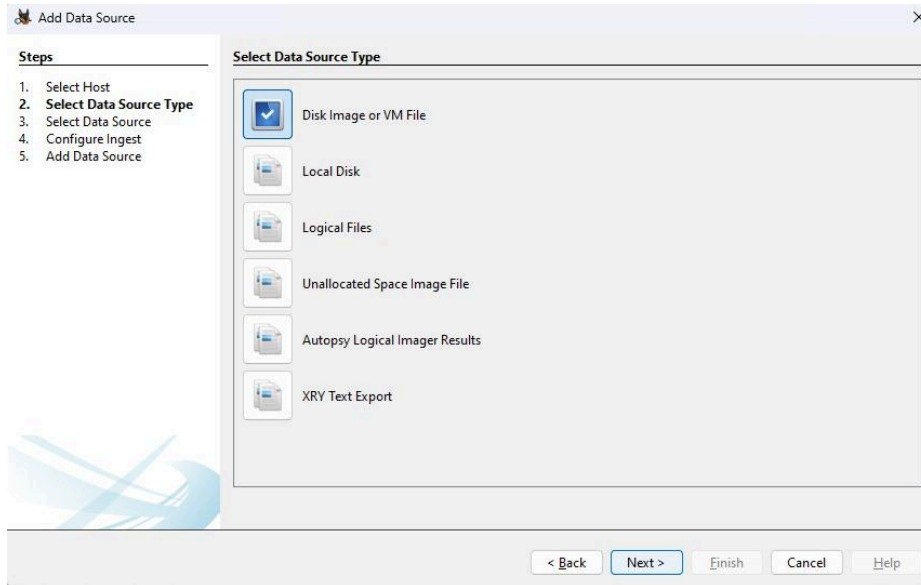
☐ Generate new host name based on data source name

☒ Specify new host name Exhibit001

☐ Use existing host

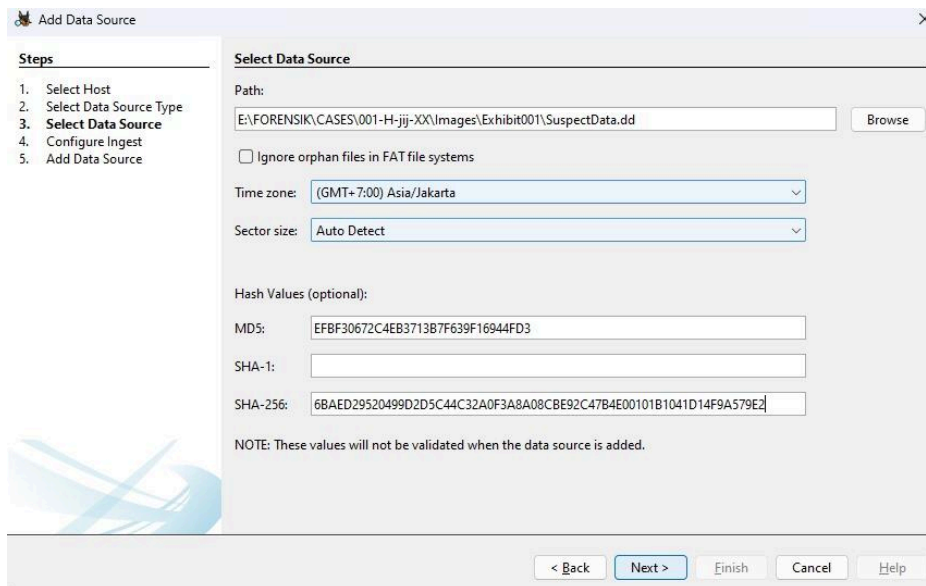
< Back **Next >** Finish Cancel Help

11. Select Data Source Type



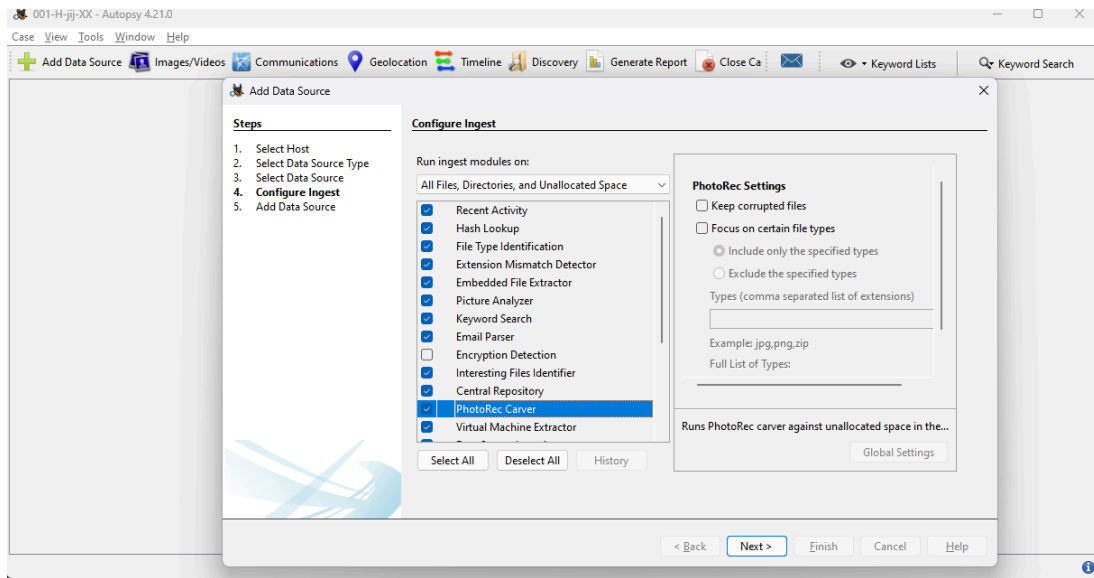
Disk image adalah salinan bit-per-bit dari disk fisik atau partisi. Biasanya berformat .dd. Disk image lebih baik daripada menganalisis disk fisik langsung karena dapat merusak hardware. Disk image dapat disimpan di berbagai lokasi seperti folder kasus di Autopsy.

12. Mengisi data source



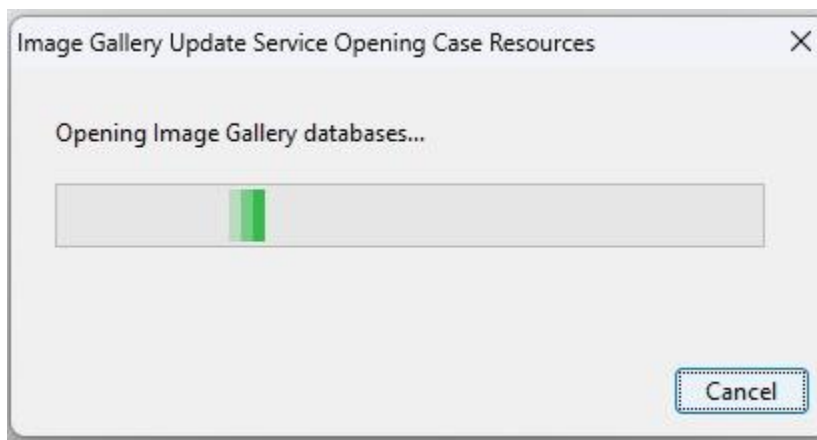
Waktu zona disk image harus diketahui untuk analisis yang tepat. Jika tidak diketahui, gunakan UTC. Hash nilai seperti MD5 dan SHA-256 digunakan untuk verifikasi disk image

13. Memilih modul

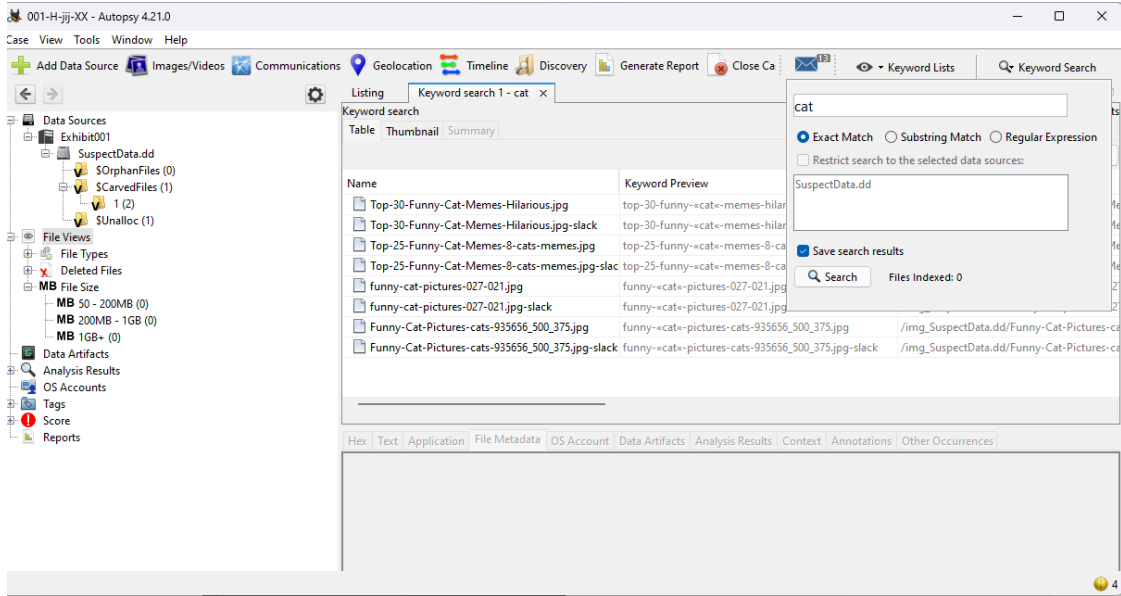


- File type identification
- Extension Mismatch Detector: mengekstrak file di dalam file terkompresi seperti zip
- Picture Anyzer: menganalisis gambar dan mengekstrak informasi seperti lokasi, timestamp, program editing
- Keyword search: mencari nomor telepon, alamat IP, email, URL, nomor kartu kredit secara default
- Photorec Carver: mengorek data yang dihapus atau tidak teralokasi
- Virtual Machine Extractor: mengekstrak mesin virtual sebagai cakram terpisah
- Data Source Integrity: memverifikasi hash sumber data

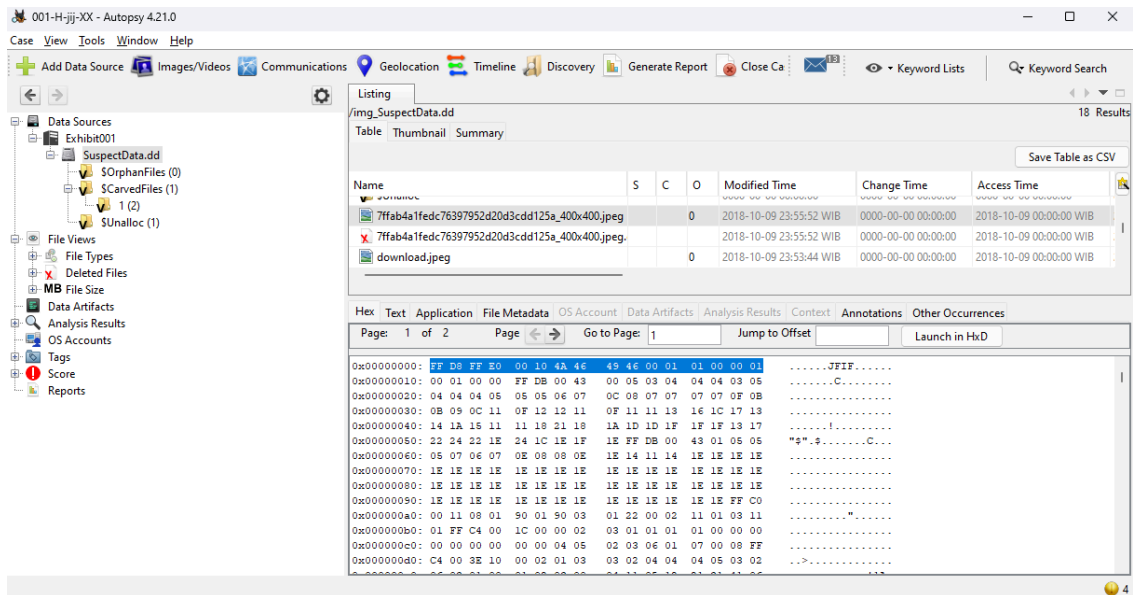
14. Lalu next untuk memproses data



15. Setelah data sudah selesai di proses kita dapat melakukan pencarian kata kunci khusus kasus untuk menemukan bukti relevan. Misalnya mencari kata kunci "cat".



16. Kita dapat melihat beberapa tampilan detail berkas seperti Hex, Strings, dan Metadata. Gunakan tampilan yang tepat untuk menganalisis bukti tertentu.



Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings **Extracted Text** Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

-----METADATA-----

Component 1: Y component: Quantization table 0, Sampling factors 2 horiz/2 vert
 Component 2: Cb component: Quantization table 1, Sampling factors 1 horiz/1 vert
 Component 3: Cr component: Quantization table 1, Sampling factors 1 horiz/1 vert
 Compression Type: Baseline
 Content-Type: image/jpeg
 Data Precision: 8 bits
 File Modified Date: Tue Mar 05 02:01:15 +07:00 2024
 File Name: apache-tika-5075495670123016365.tmp
 File Size: 30286 bytes

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Metadata

Name: /img_SuspectData.dd/7ffab4a1fedc76397952d20d3cdd125a_400x400.jpeg
 Type: File System
 MIME Type: image/jpeg
 Size: 30286
 File Name Allocation: Allocated
 Metadata Allocation: Allocated
 Modified: 2018-10-09 23:55:52 WIB
 Accessed: 2018-10-09 00:00:00 WIB
 Created: 2018-10-09 23:55:53 WIB
 Changed: 0000-00-00 00:00:00
 MD5: dcc7290913e8fb0abd4f8bfc3899853a
 SHA-256: 791b652056104b115c82274d40960bfbb55fe13e431525d8f98d68744235d6f1

17. Generate Report

Generate Report

Select and Configure Report Modules

Report Modules:

- ☒ HTML Report
- ☐ Excel Report
- ☐ Files - Text
- ☐ Data Source Summary Report
- ☐ Save Tagged Hashes
- ☐ Extract Unique Words
- ☐ TSK Body File
- ☐ Google Earth KML
- ☐ CASE-UCO
- ☐ Portable Case

A report about results and tagged items in HTML format.

Header:

Footer:

< Back Next > Finish Cancel Help

Generate Report

Select which data source(s) to include

☒ SuspectData.dd

Uncheck All Check All

< Back Next Finish Cancel Help

Generate Report

Configure Report

Select which data to report on:

☒ All Results

☐ All Tagged Results

☐ Specific Tagged Results

Select All Deselect All

Choose Result Types...

< Back Next > Finish Cancel Help

