Autopsy Exercise

Oleh :

1203210015 – Enrico Sulfriando Sinaga

Mata Kuliah Forensik Digital

Program Studi Informatika

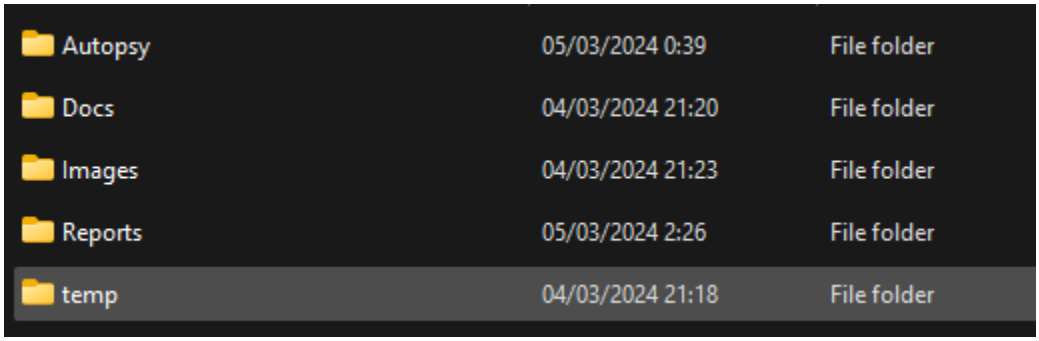
Fakultas Teknologi Informasi dan Bisnis

Institut Teknologi Telkom Surabaya

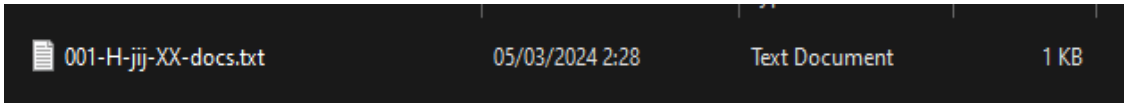
2024

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

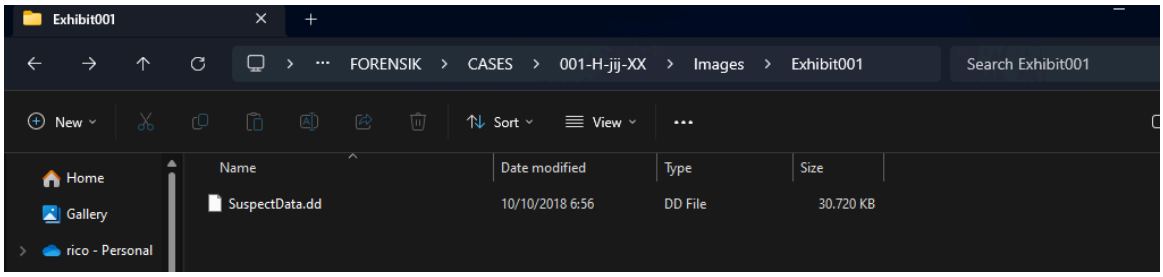
4. Membuat subfolder dokumen docs, images, temp, autopsy, reports



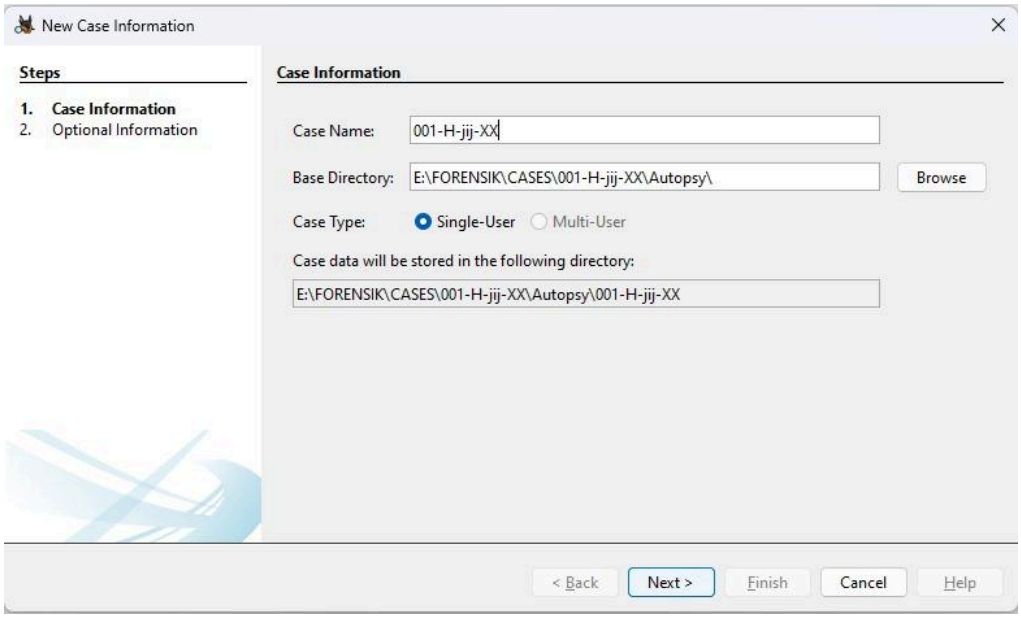
5. Membuat dokumen docs/casenumber-docs.txt untuk mencatat log aktivitas



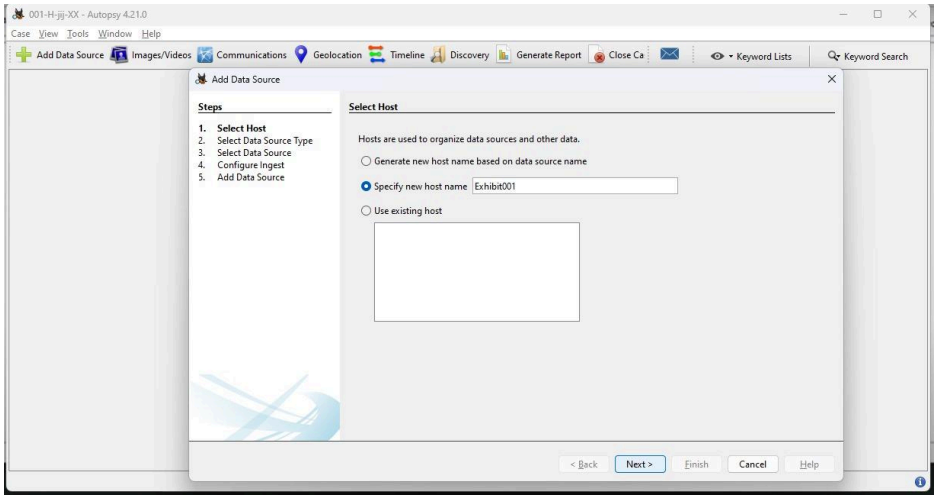
6. Memindahkan data target ke folder images/exhibit001



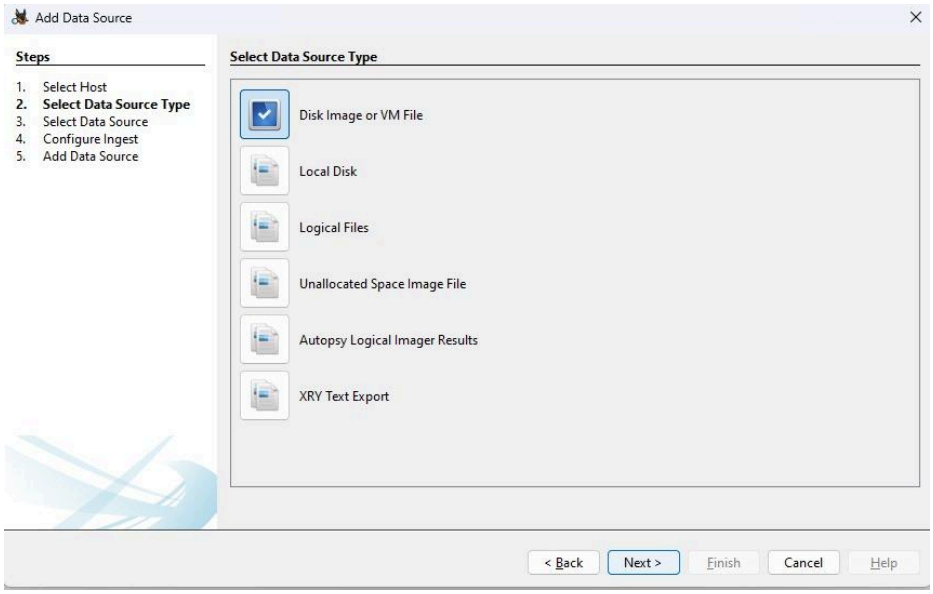
7. Membuka autopsy dan membuat kasus baru dengan nama sesuai folder kasus



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

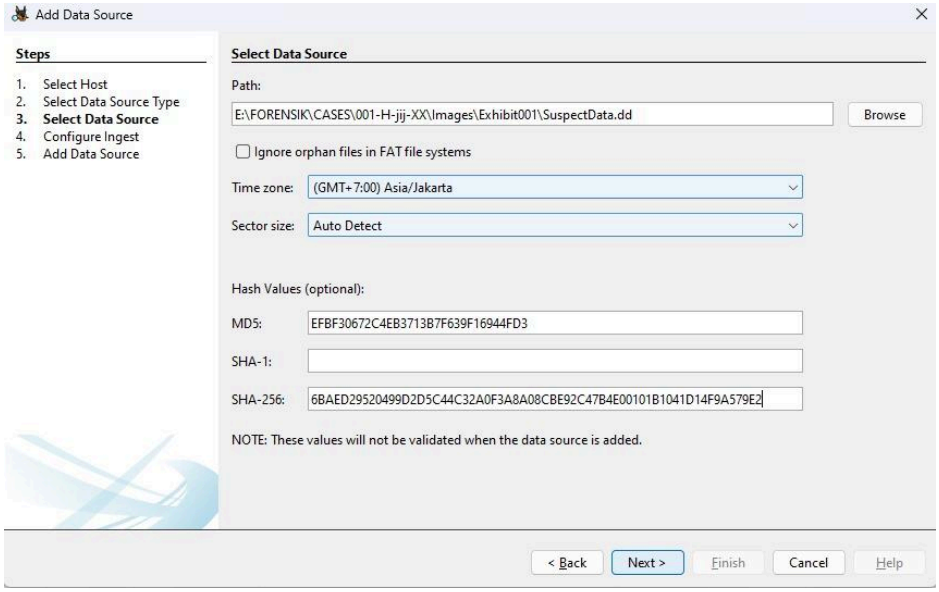


11. Select Data Source Type



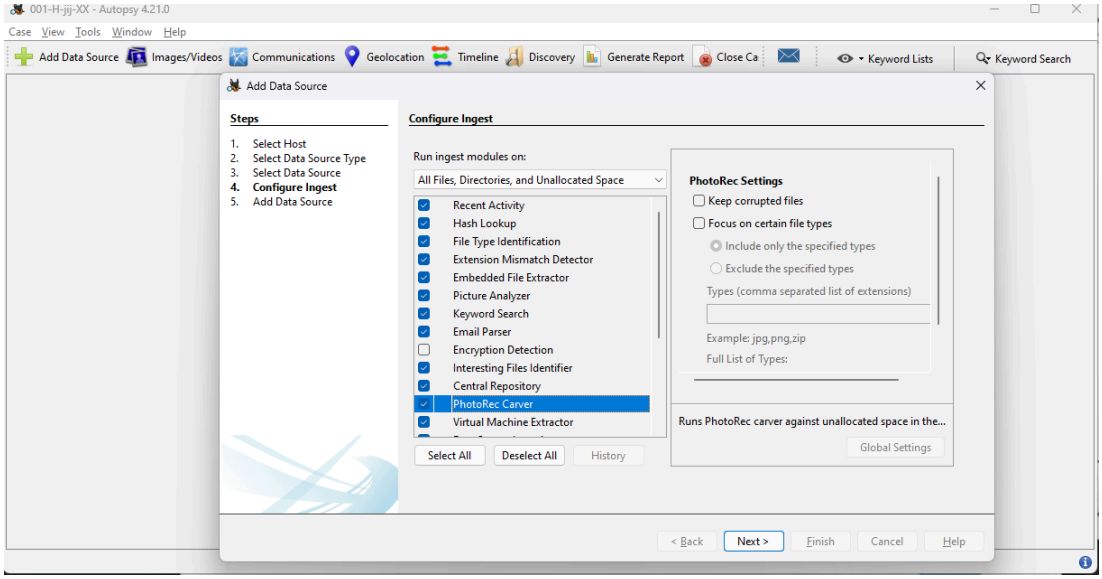
Disk image adalah salinan bit-per-bit dari disk fisik atau partisi. Biasanya berformat .dd. Disk image lebih baik daripada menganalisis disk fisik langsung karena dapat merusak hardware. Disk image dapat disimpan di berbagai lokasi seperti folder kasus di Autopsy.

12. Mengisi data source



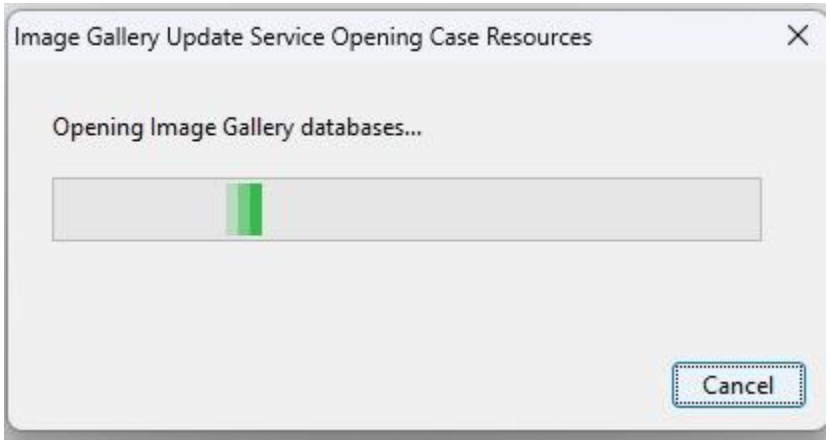
Waktu zona disk image harus diketahui untuk analisis yang tepat. Jika tidak diketahui, gunakan UTC. Hash nilai seperti MD5 dan SHA-256 digunakan untuk verifikasi disk image

13. Memilih modul

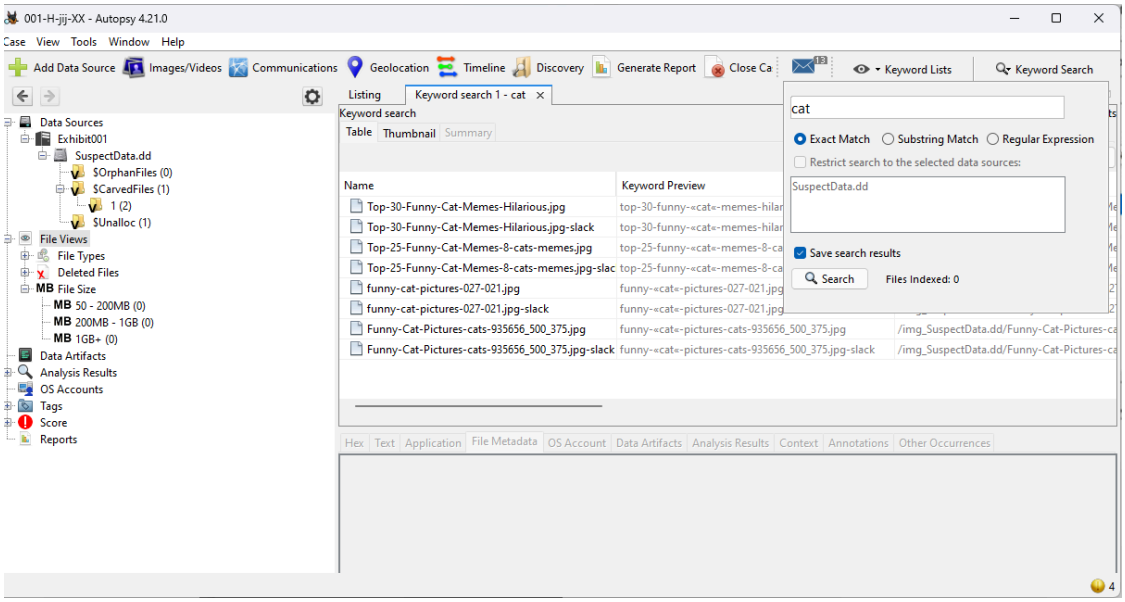


- File type identifation
- Extension Mismatch Detector: mengekstrak file di dalam file terkompresi seperti zip
- Picture Anlyzer: menganalisis gambar dan mengekstrak informasi seperti lokasi, timestamp, program editing
- Keyword search: mencari nomor telepon, alamat IP, email, URL, nomor kartu kredit 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

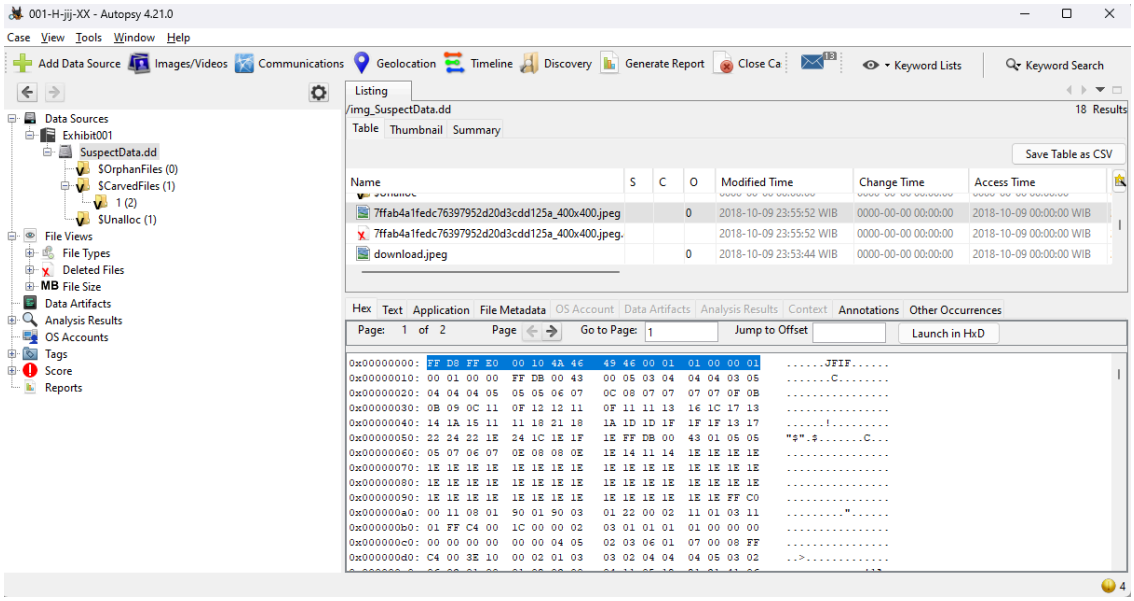
14. Lalu next untuk memproses data

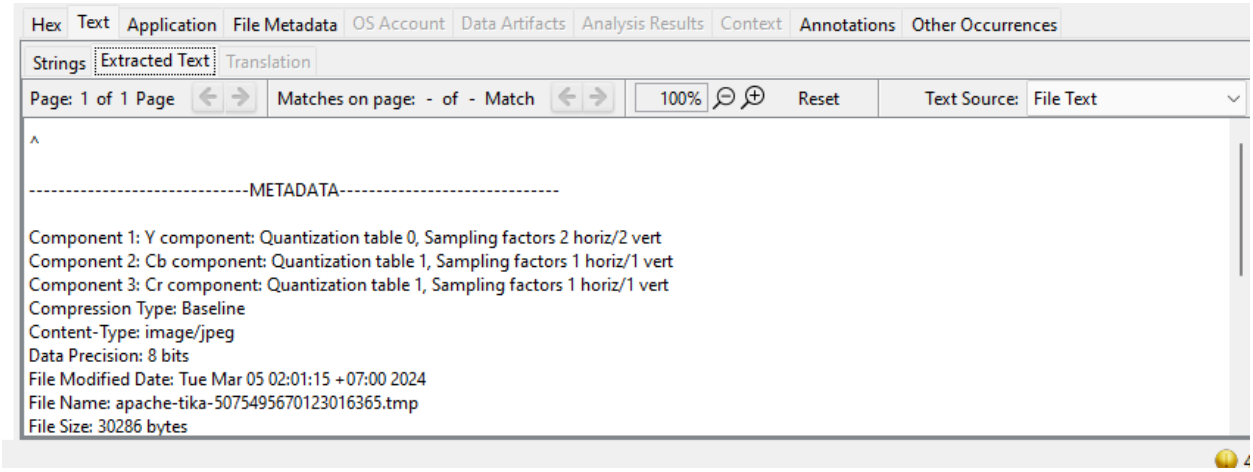


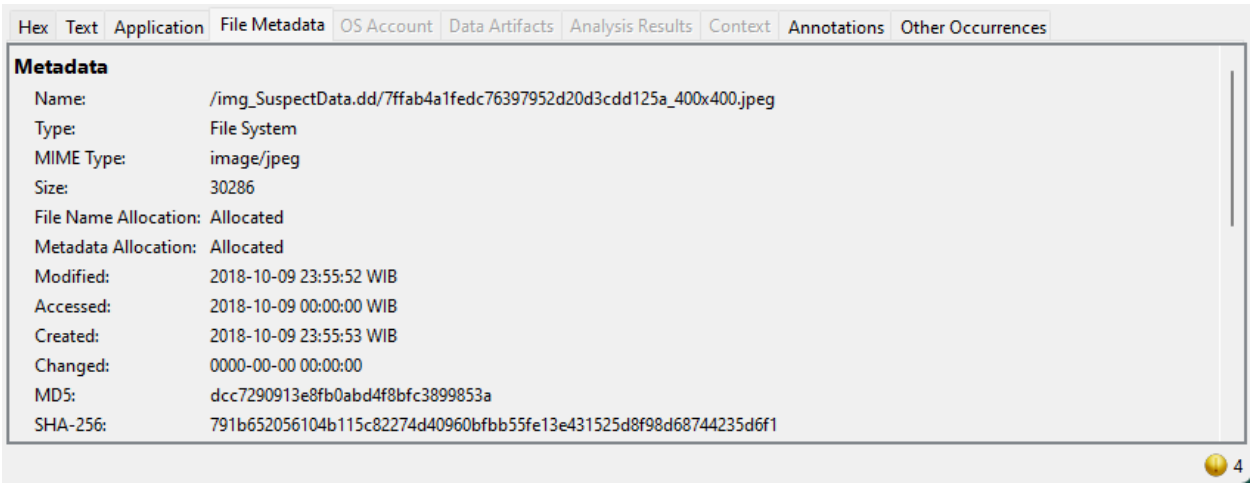
15. Setelah data sudah selesai di proses kita dapat melakukanpencarian kata kunci khusus kasus untuk menemukan bukti relevan. Misalnya mencari kata kunci "cat".



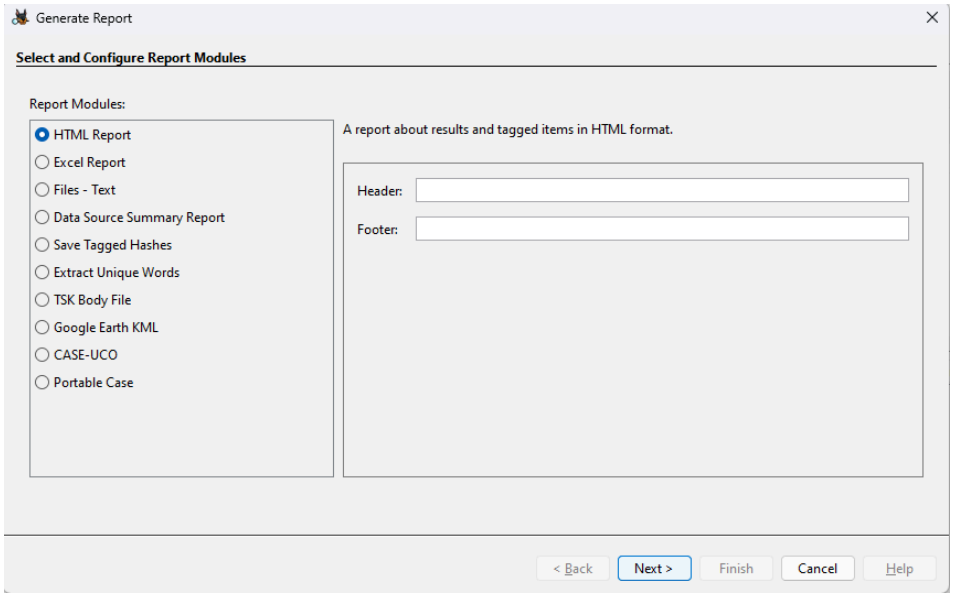
16. Kita dapat melihat beberapa tampilan detail berkas seperti Hex, Strings, dan Metadata. Gunakan tampilan yang tepat untuk menganalisis bukti tertentu.

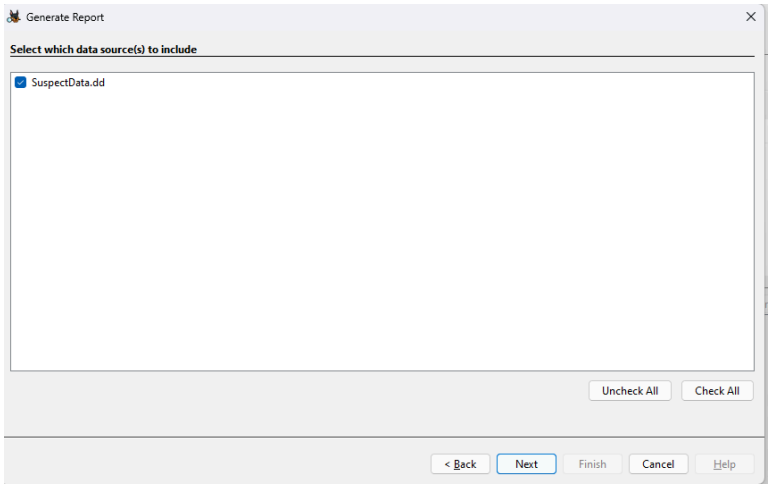


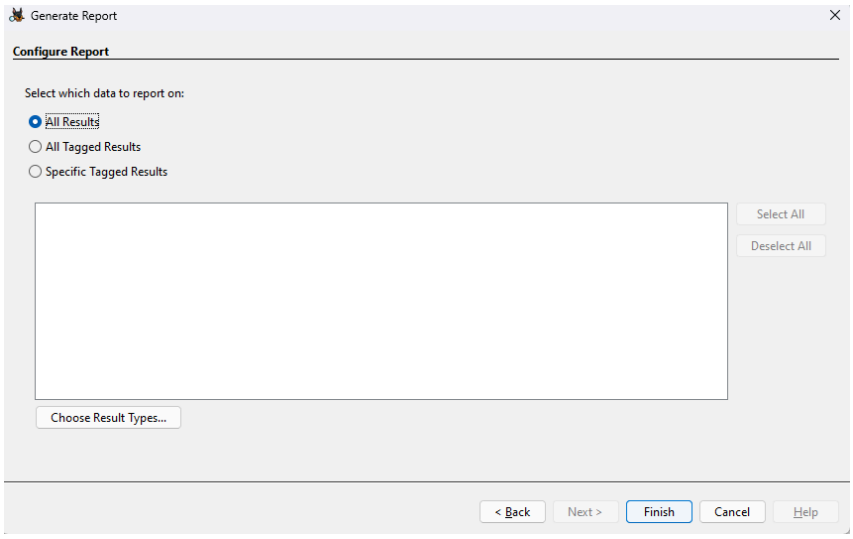


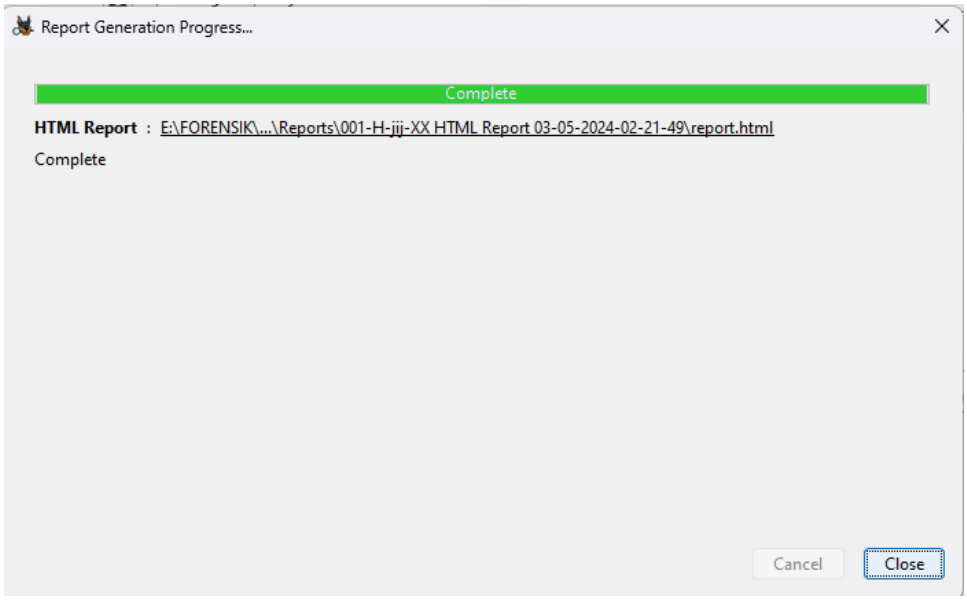


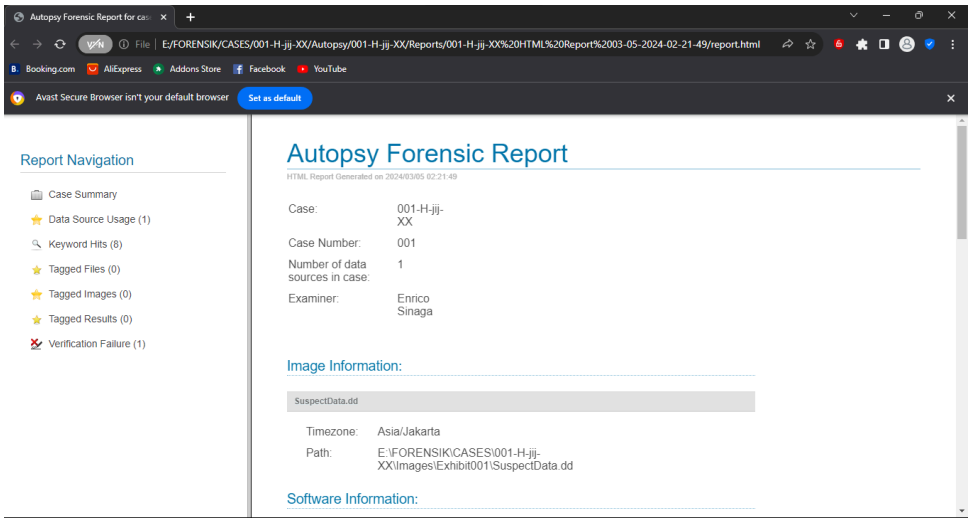
17. Generate Report




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


Report Generation Progress...
Complete
HTML Report : E:\FORENSIK\...\Reports\001-H-jij-XX HTML Report 03-05-2024-02-21-49\report.html
Complete
Cancel
Close


Autopsy Forensic Report for cas
E:/FORENSIK/CASES/001-H-jij-XX/Autopsy/001-H-jij-XX/Reports/001-H-jij-XX%20HTML%20Report%2003-05-2024-02-21-49/report.html
Booking.com
AliExpress
Addons Store
Facebook
YouTube
Avast Secure Browser isn't your default browser
Set as default
Report Navigation
Case Summary
Data Source Usage (1)
Keyword Hits (8)
Tagged Files (0)
Tagged Images (0)
Tagged Results (0)
Verification Failure (1)
Autopsy Forensic Report
HTML Report Generated on 2024/03/05 02:21:49
Case: 001-H-jij-XX
Case Number: 001
Number of data sources in case: 1
Examiner: Enrico Sinaga
Image Information:
SuspectData.dd
Timezone: Asia/Jakarta
Path: E:\FORENSIK\CASES\001-H-jij-XX\Images\Exhibit001\SuspectData.dd
Software Information: