EXPERIMENT--05

Aim:
To examine a disk image or folder with Autopsy, extract digital artifacts, and generate a forensic report.

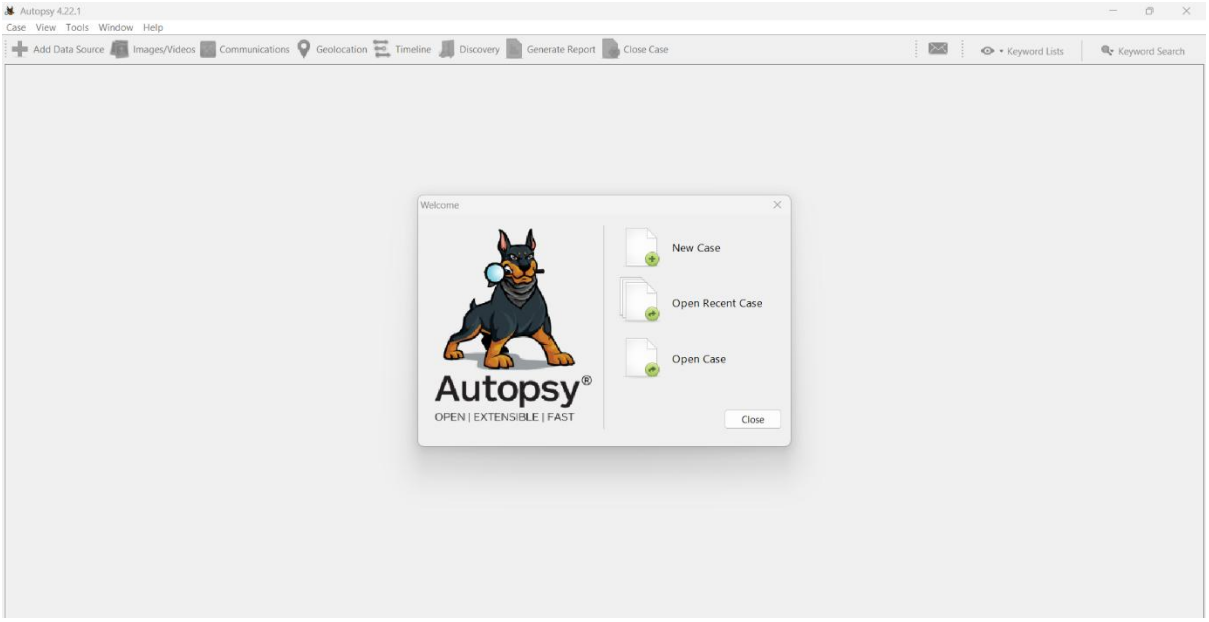
Tools Used:

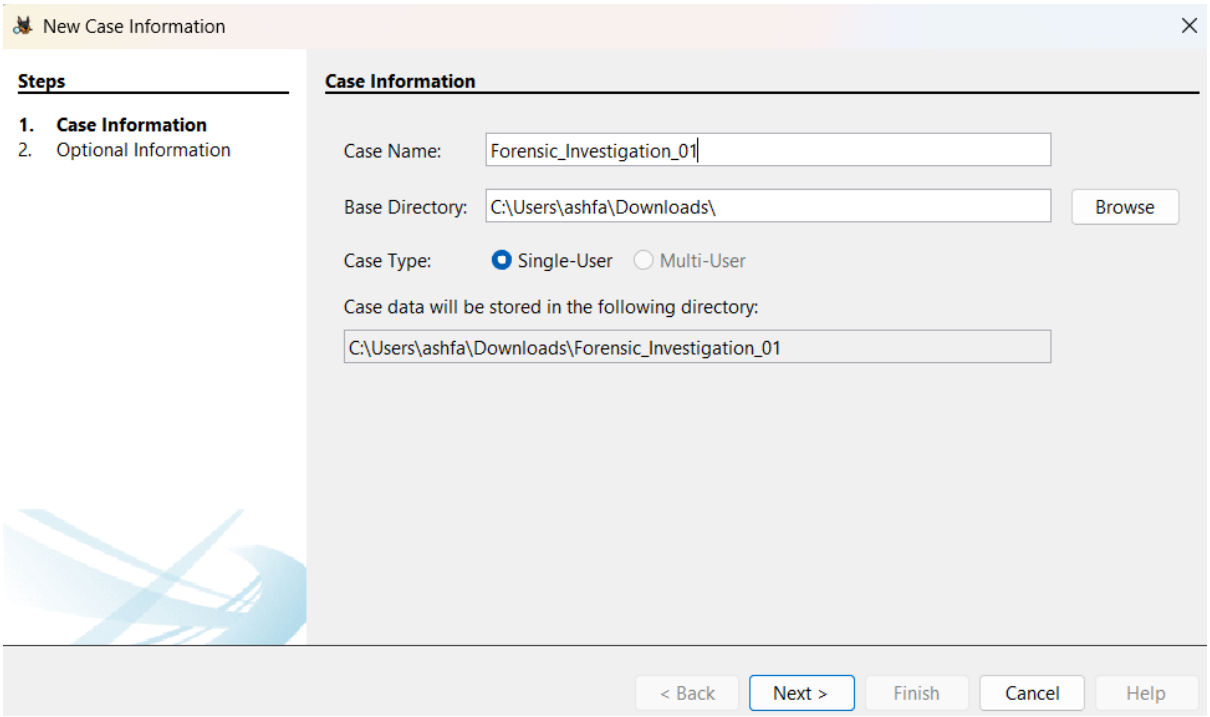
- Autopsy (open-source DFIR suite)
- Windows/Linux system
- Evidence source: disk image (E01/RAW/VHD) or folder
-

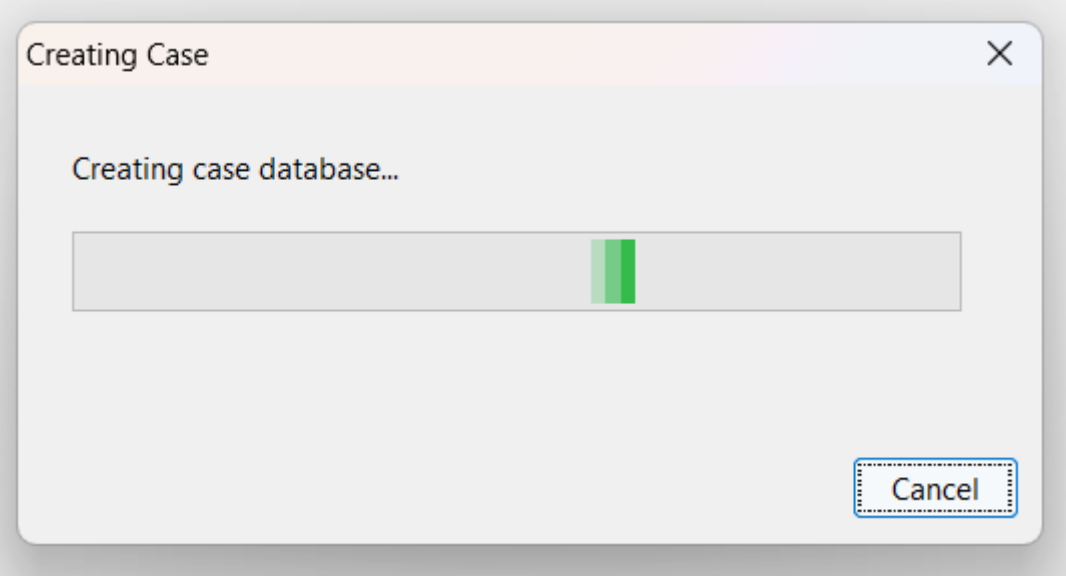
Procedure:

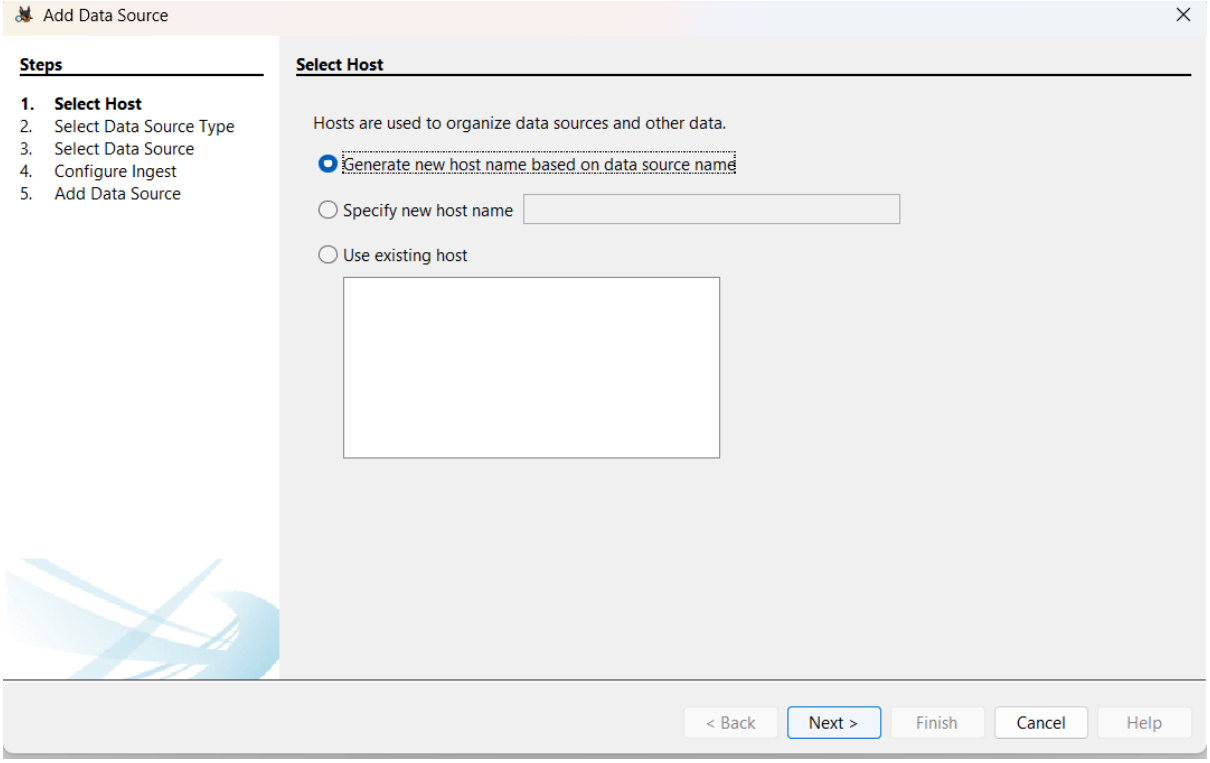
1. Launch Autopsy → Create New Case (enter case name, base directory, investigator).
2. Add Data Source → choose Disk Image/VM file, Local Disk, or Logical Files, then browse to the evidence.
3. In Ingest Modules, select: File Type Identification, Embedded File Extractor, Recent Activity (web artifacts), EXIF Parser/Metadata, Keyword Search (add terms if needed), and Hash Lookup (optional).
4. Start Ingest and monitor progress/messages until processing completes.
5. Review results in the left tree: Recent Activity, Web History/Downloads, Documents/Images/Videos, Deleted Files, Installed Programs, etc.
6. Use Timeline and Filters to focus on relevant activity; preview items and Export artifacts if required.
7. Go to Tools → Generate Report → choose HTML/PDF/CSV, select result types, and save the report to the case folder.

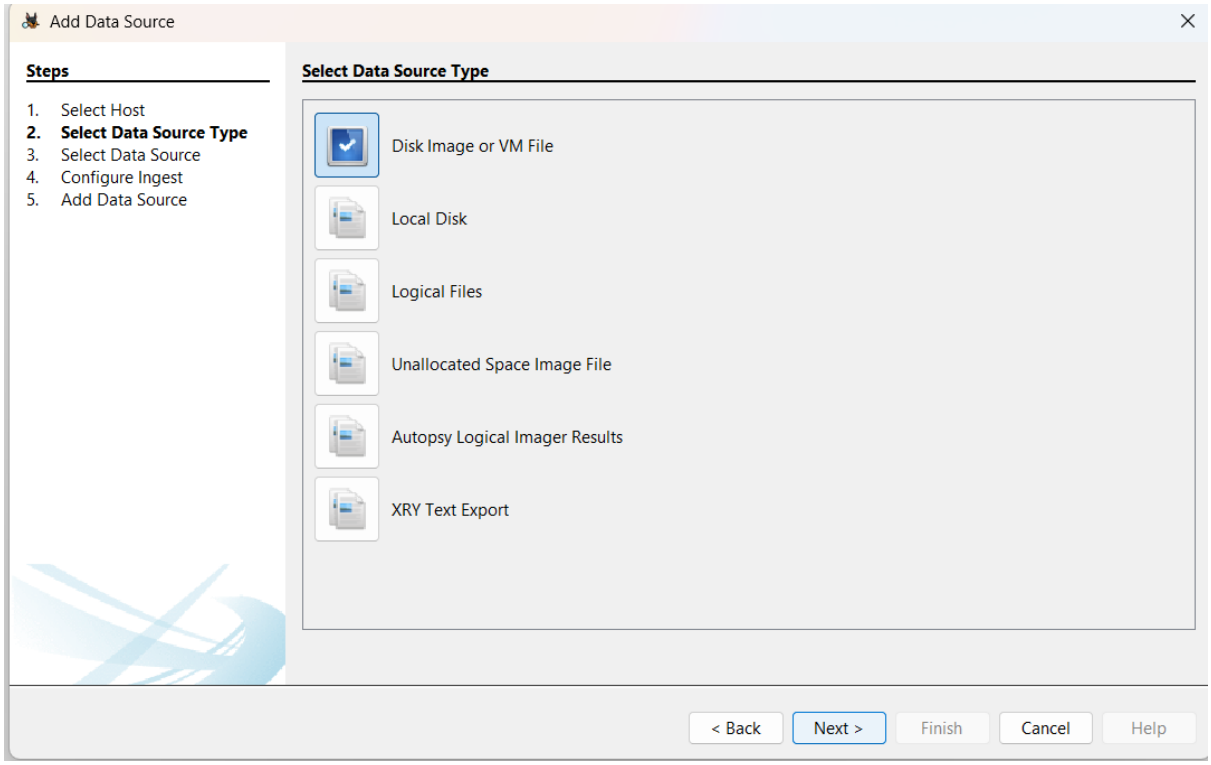
Outputs:

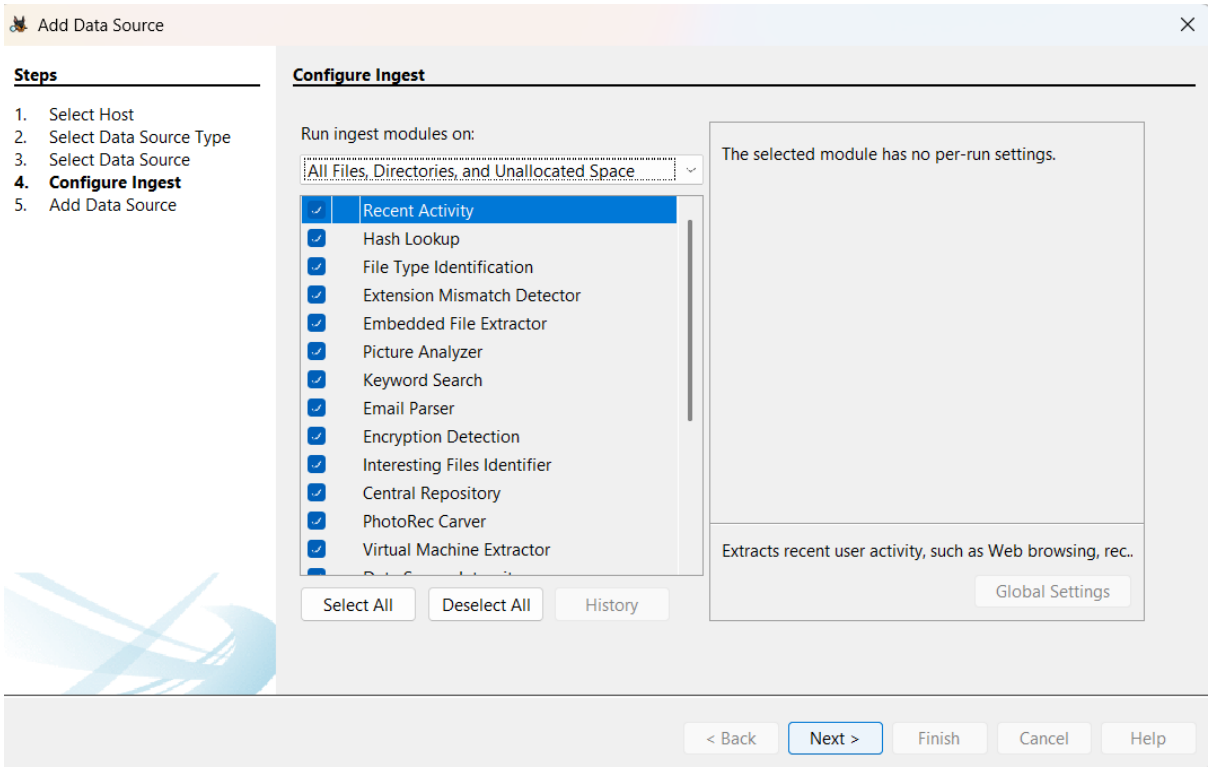

Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Welcome
New Case
Open Recent Case
Open Case
Close
Autopsy®
OPEN | EXTENSIBLE | FAST

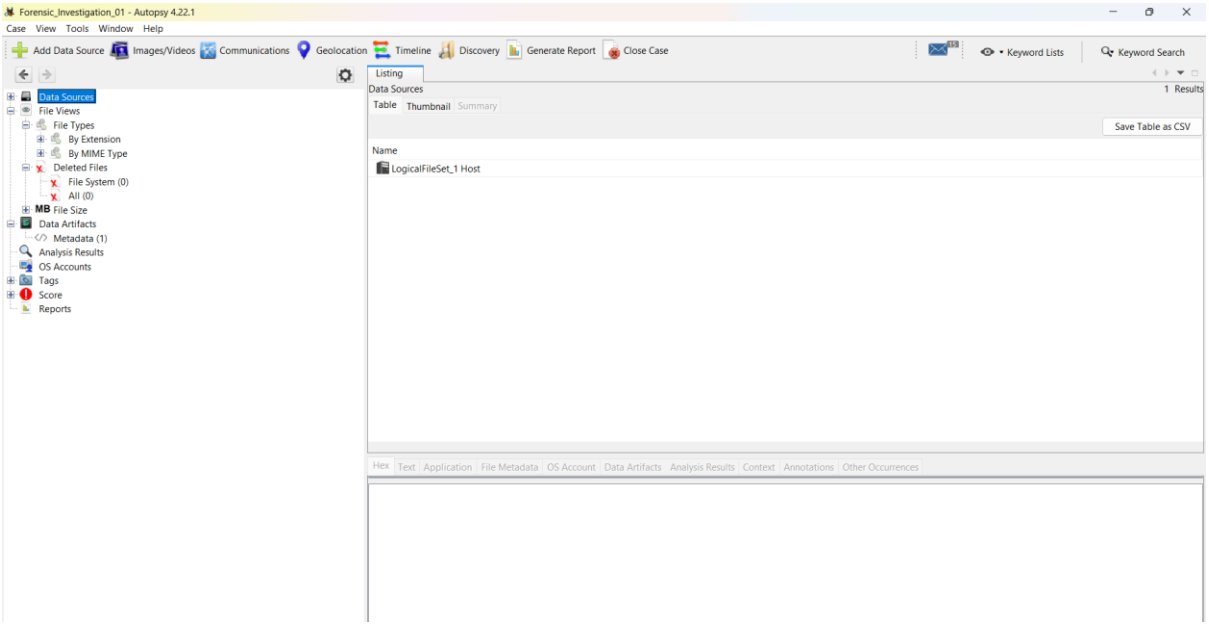

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: Forensic_Investigation_01
Base Directory: C:\Users\ashfa\Downloads\
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
C:\Users\ashfa\Downloads\Forensic_Investigation_01
< Back
Next >
Finish
Cancel
Help

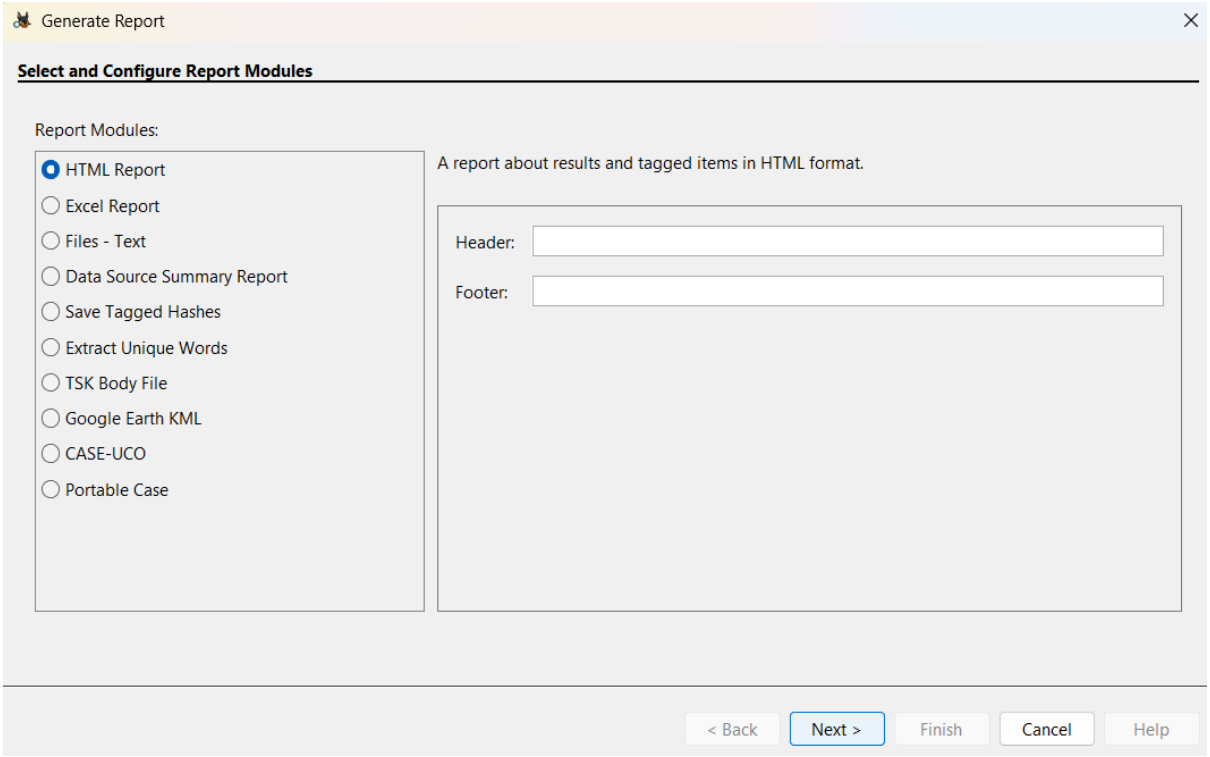

Creating Case
Creating case database...
Cancel

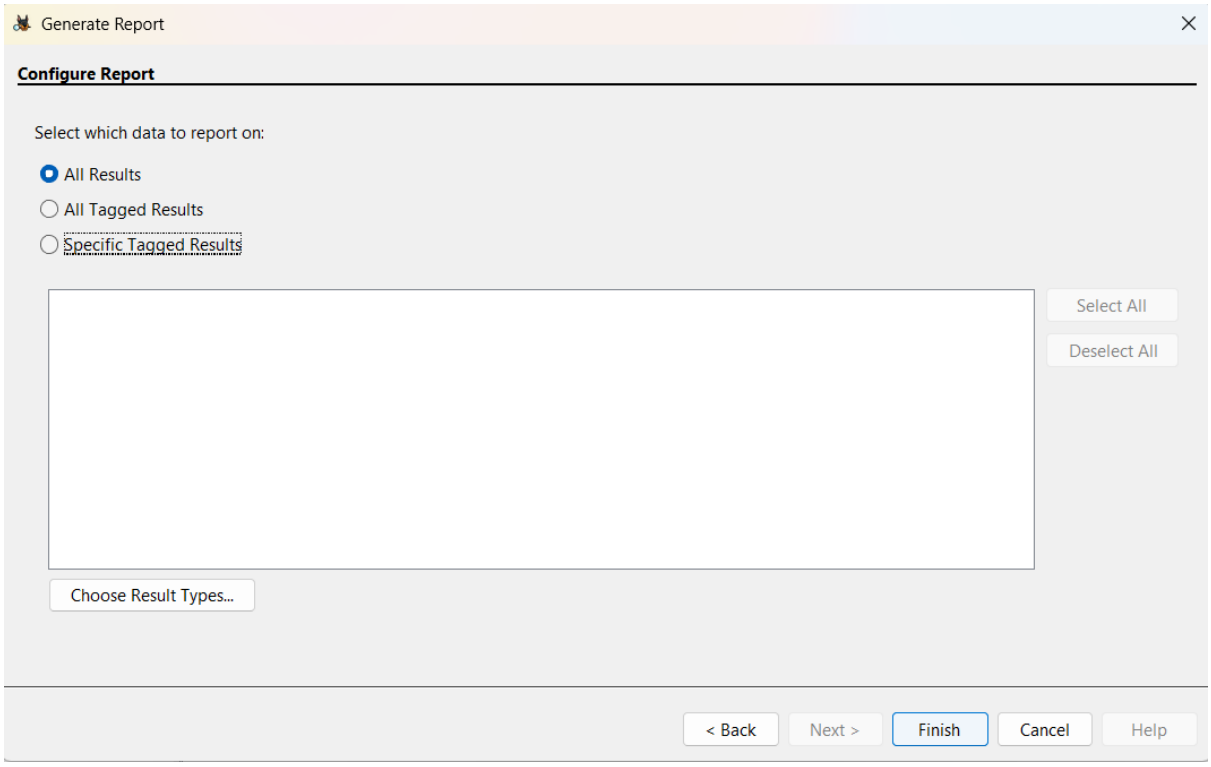

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help

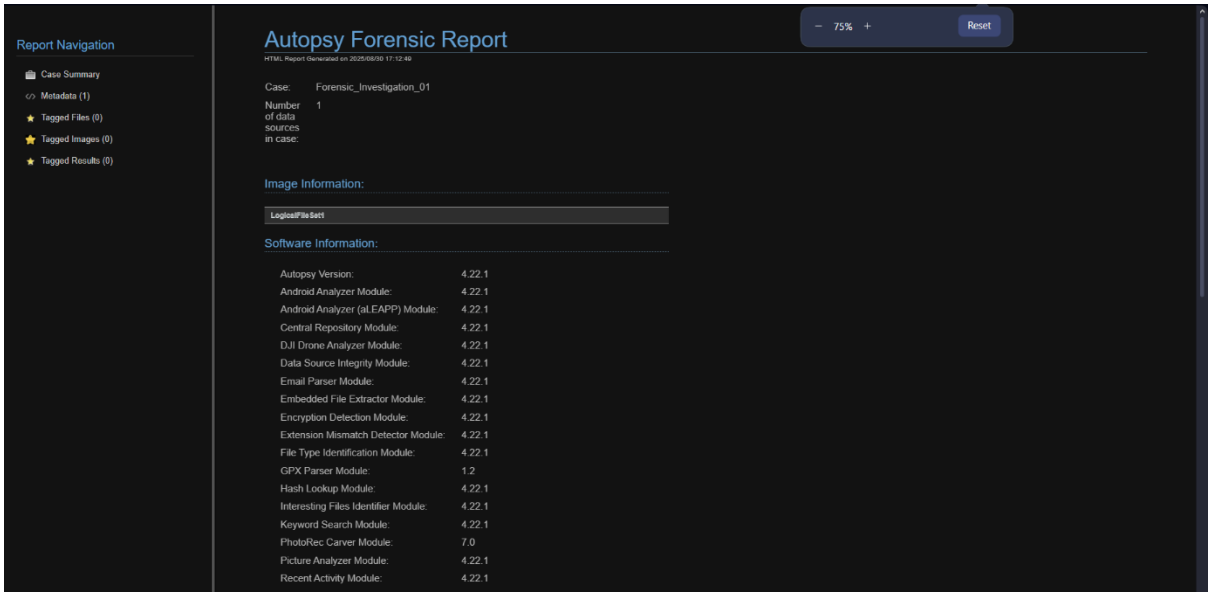

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, rec..
Global Settings
< Back
Next >
Finish
Cancel
Help


Forensic_Investigation_01 - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
By Extension
By MIME Type
Deleted Files
File System (0)
All (0)
File Size
Data Artifacts
Metadata (1)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Data Sources
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
LogicalFileSet_1 Host
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


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





Result:

Autopsy successfully parsed the evidence, recovered key artifacts (files, metadata, web/browser activity, keyword hits), and produced a structured forensic report.