Title: Use Autopsy to recover file from the given data source. Present your details accordingly

Objective:

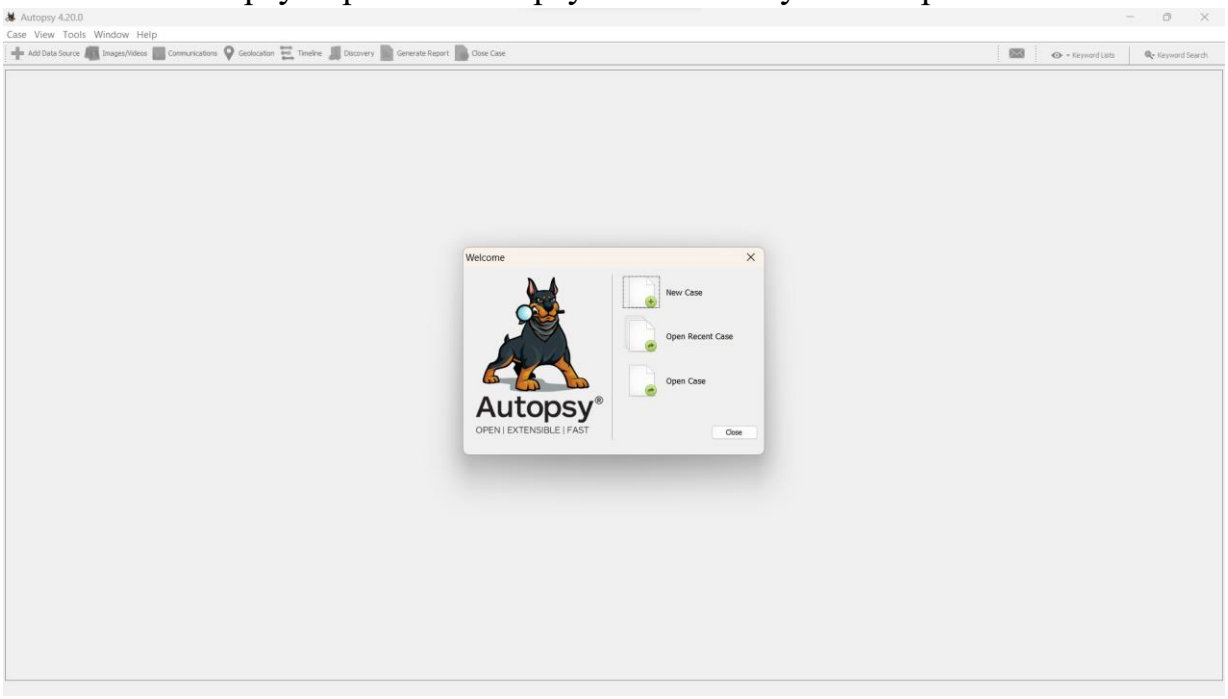
The objective of this experiment is to utilize Autopsy, a digital forensics tool, to recover a file from a specific data source.

Requirements:

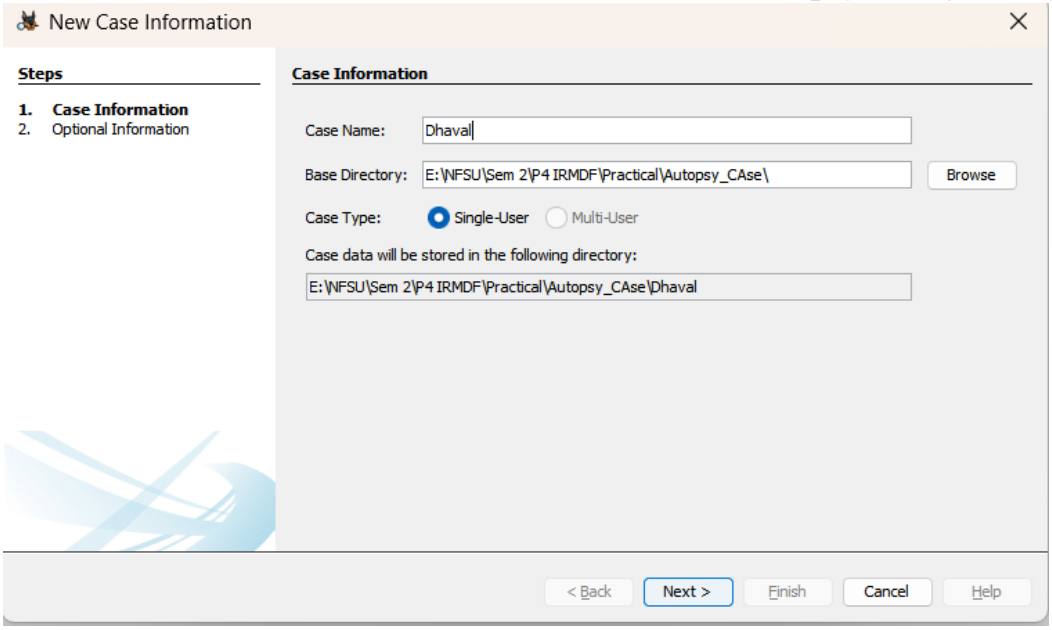
- Autopsy software installed
- Data source containing the target file for recovery (e.g., a storage device, disk image, or forensic image)

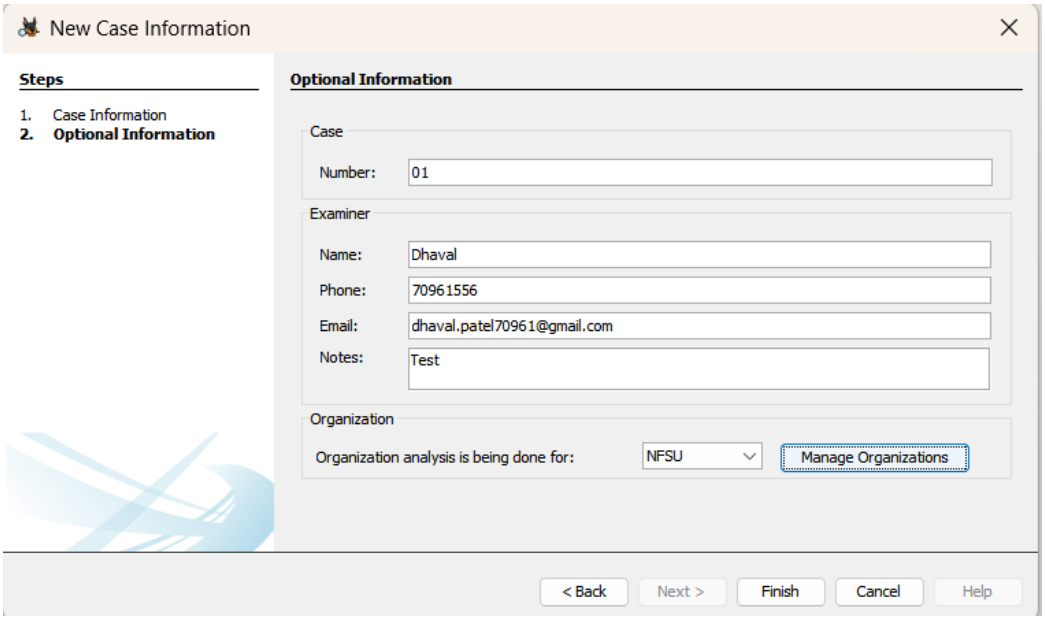
Procedure/Experiment Steps:

1. Launch Autopsy: Open the Autopsy software on your computer.

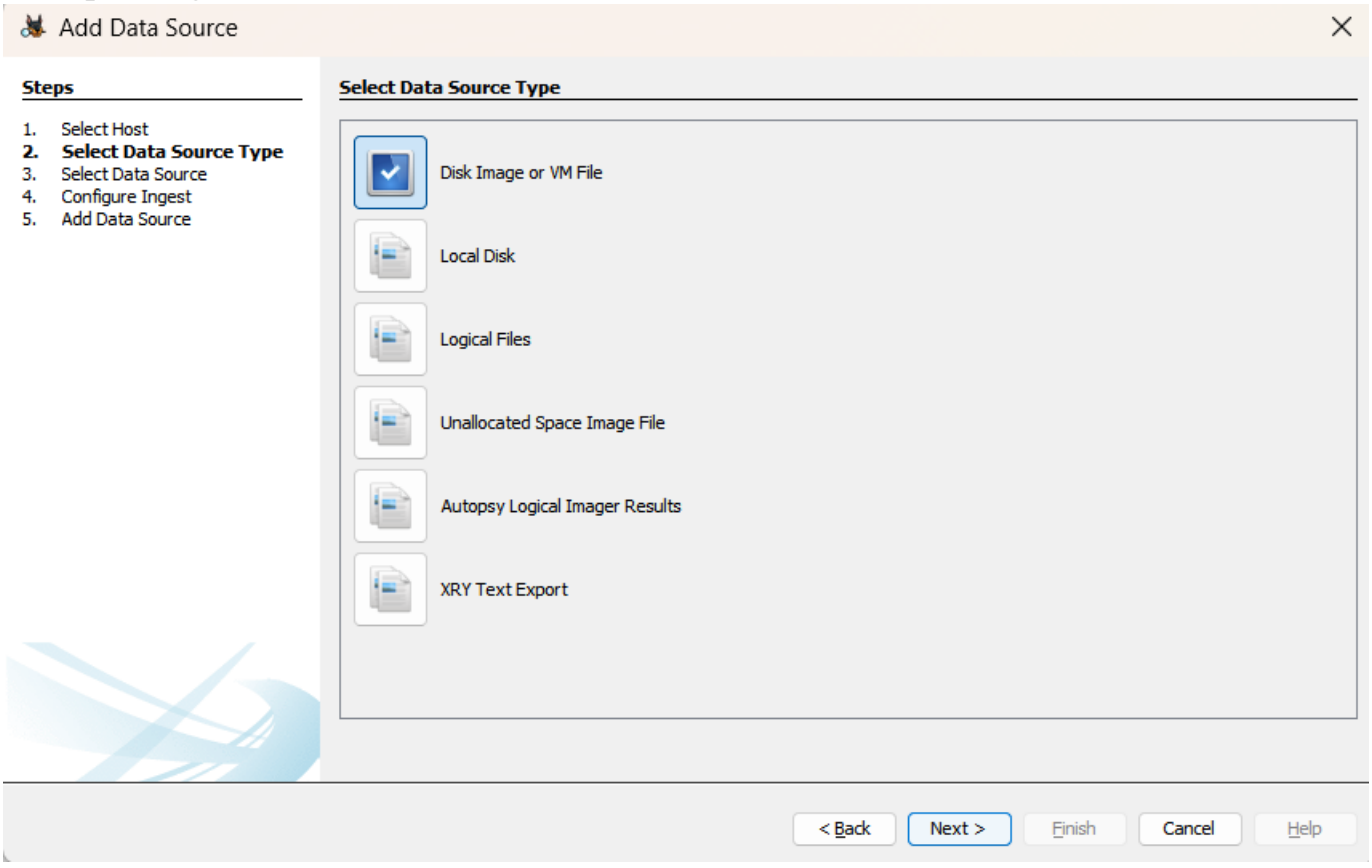


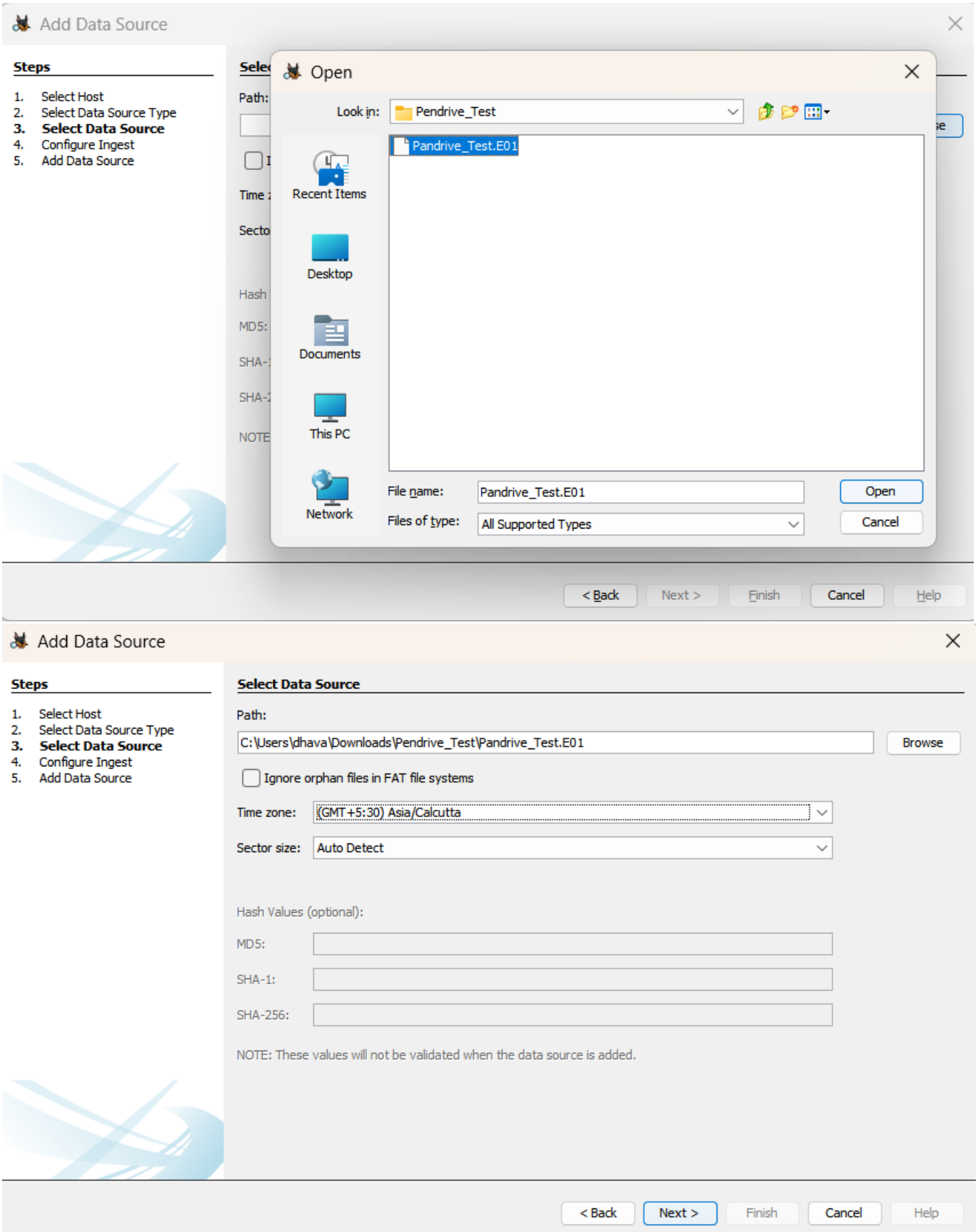
2. Create a New Case: Create a new case within Autopsy to organize your investigation.



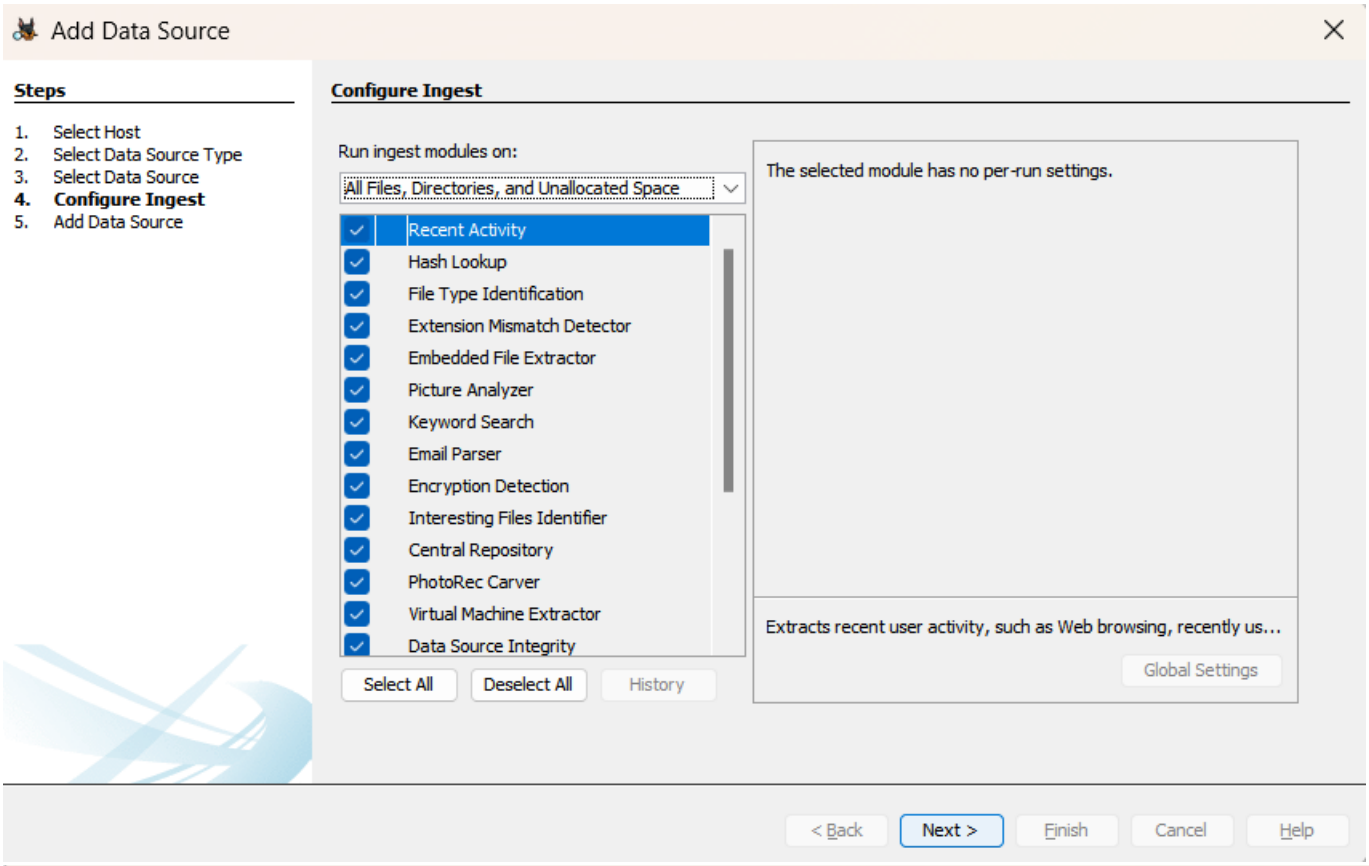


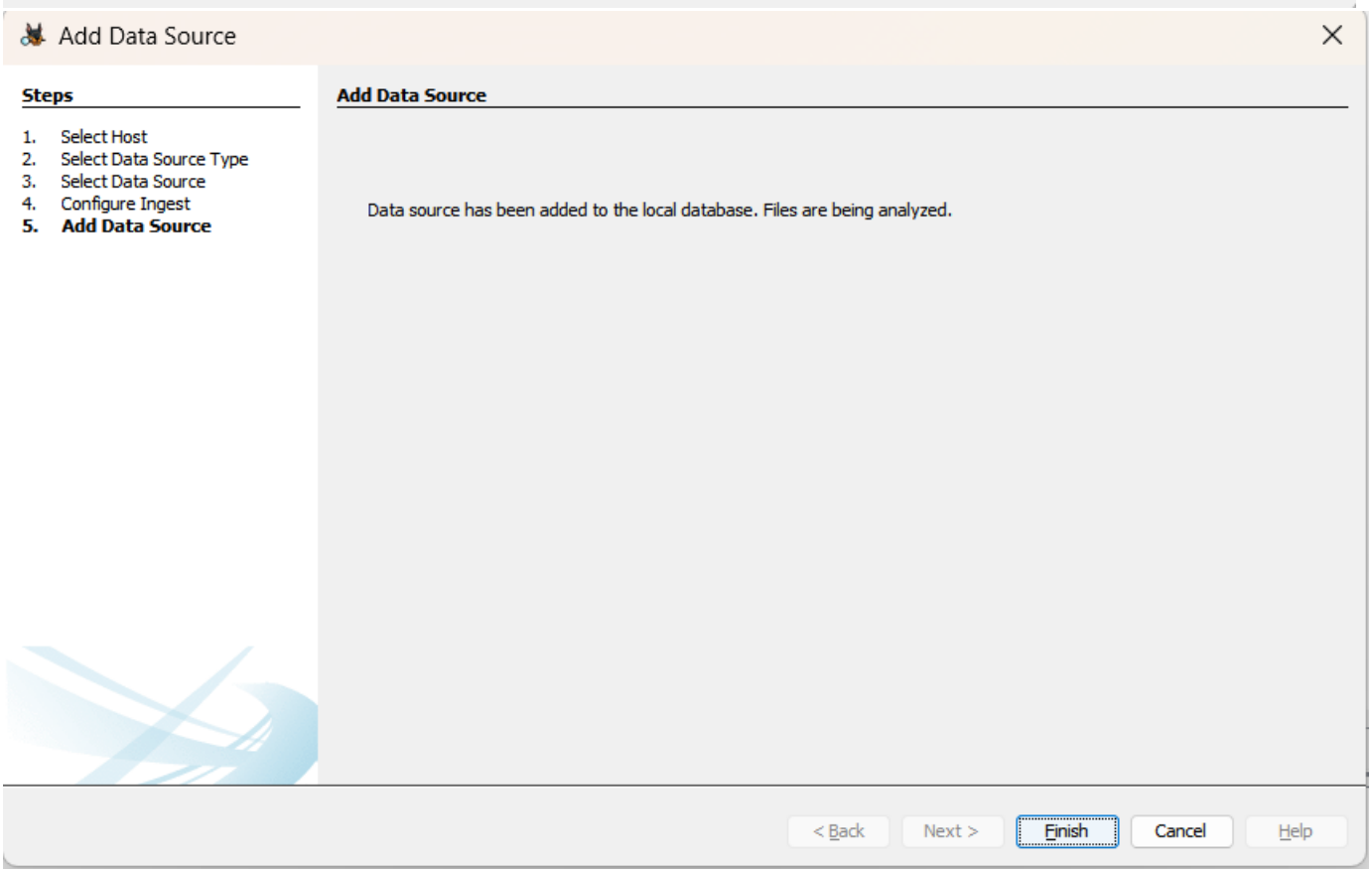
3. Add Data Source: Import the given data source, which contains the target file, into the Autopsy case. This can be done by selecting the "Add Image" or "Add Device" option, depending on the nature of the data source.

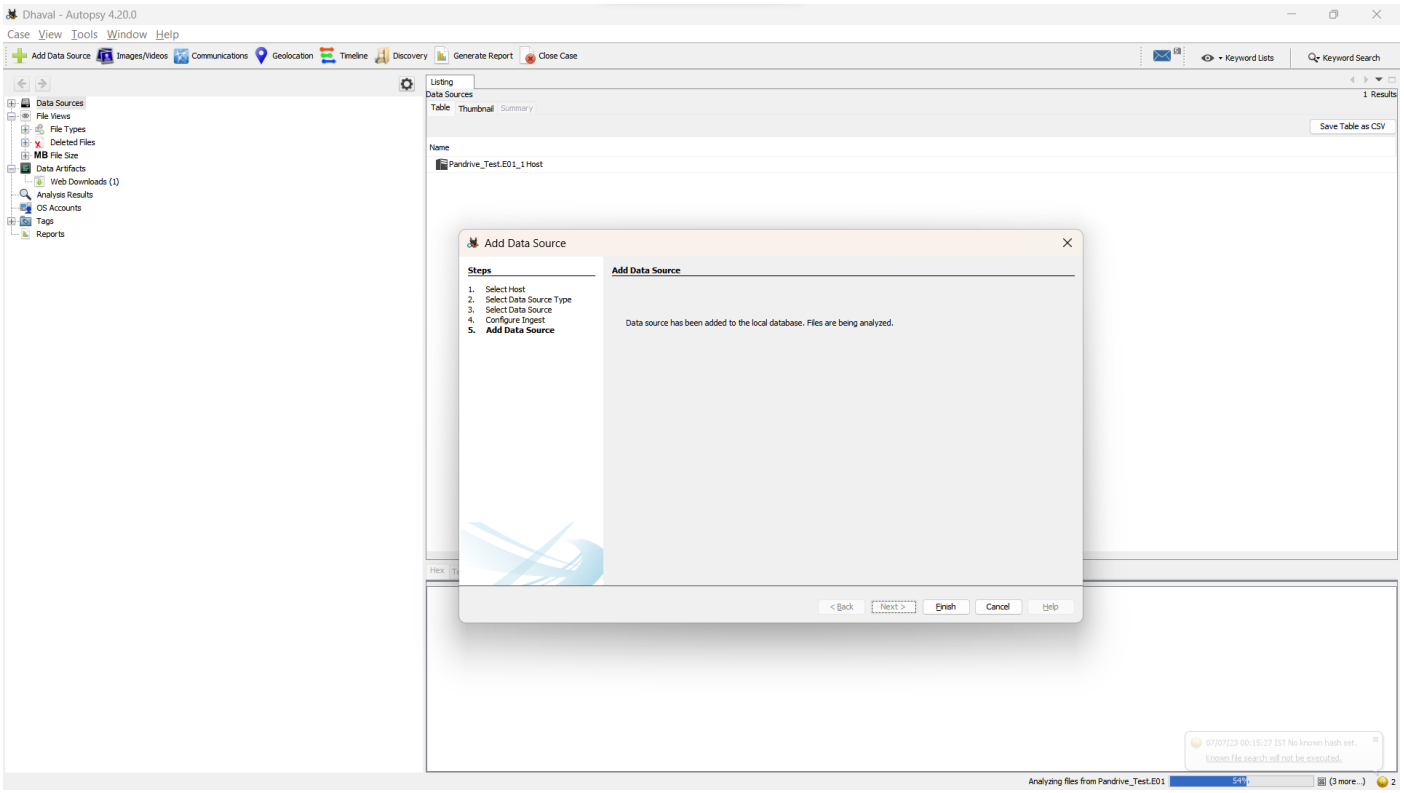




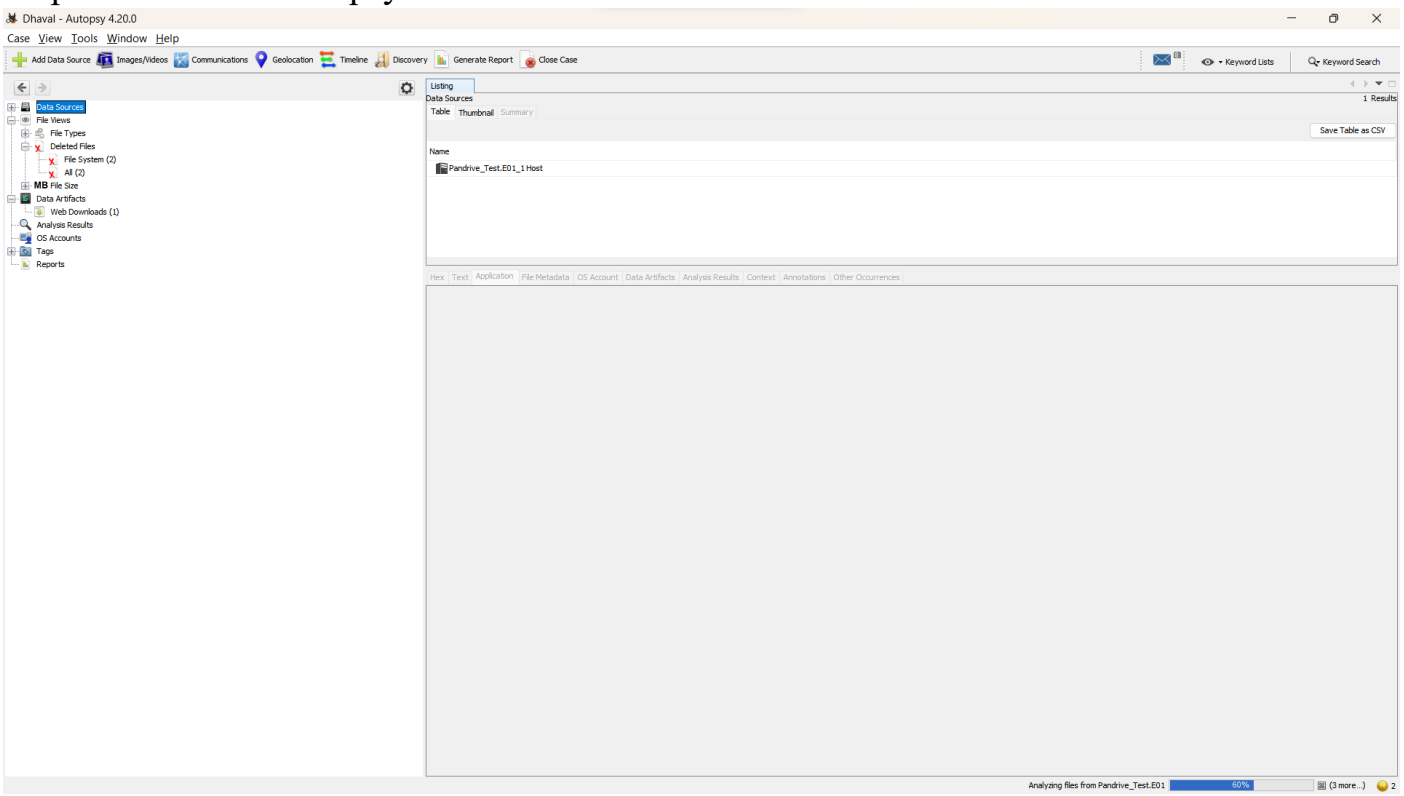
4. Configure Data Source: Provide necessary information about the data source, such as the image file or device details, during the configuration process.


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
Data Source Integrity
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
< Back
Next >
Finish
Cancel
Help

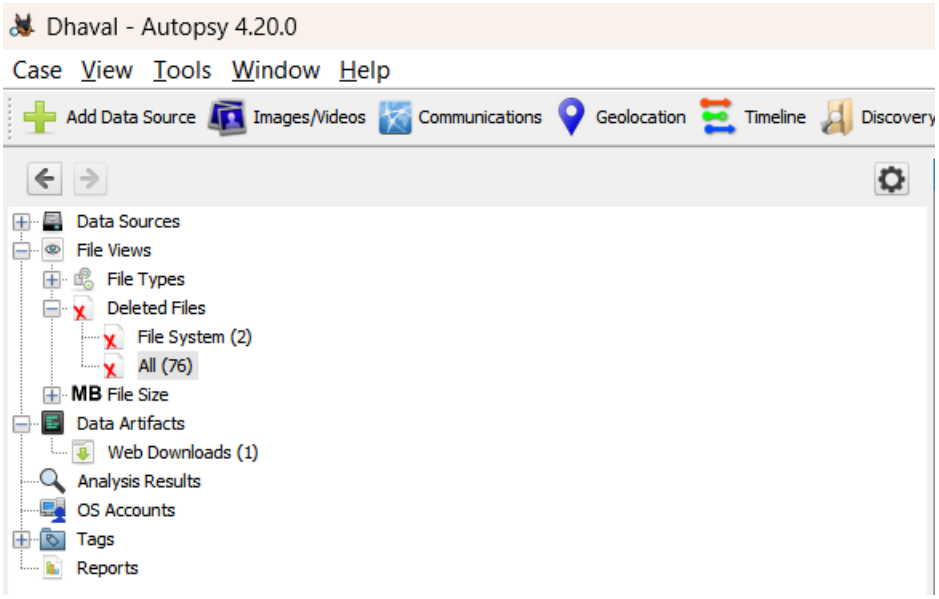

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

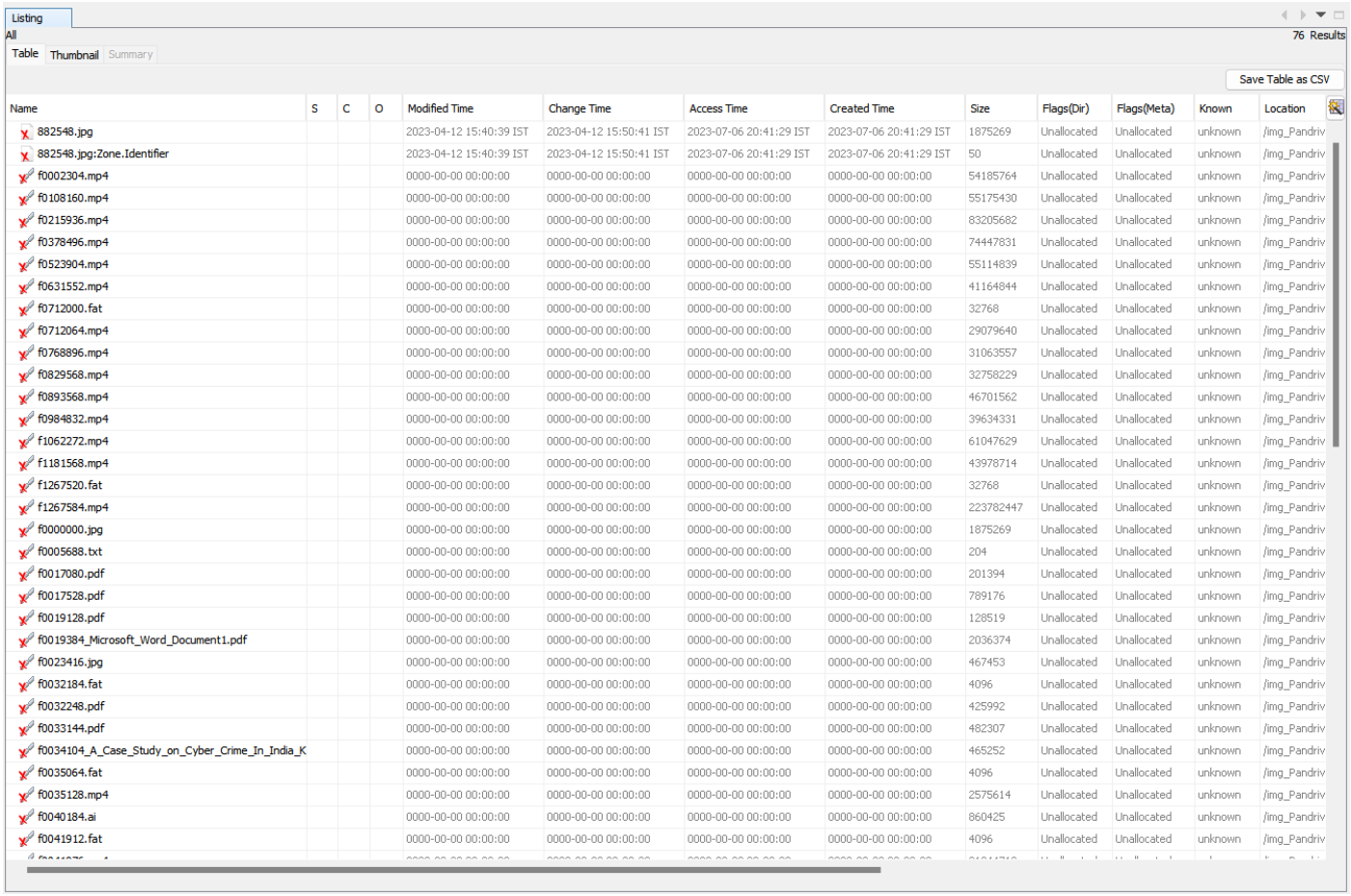


5. Start Analysis: Once the data source is added and configured, initiate the analysis process within Autopsy.

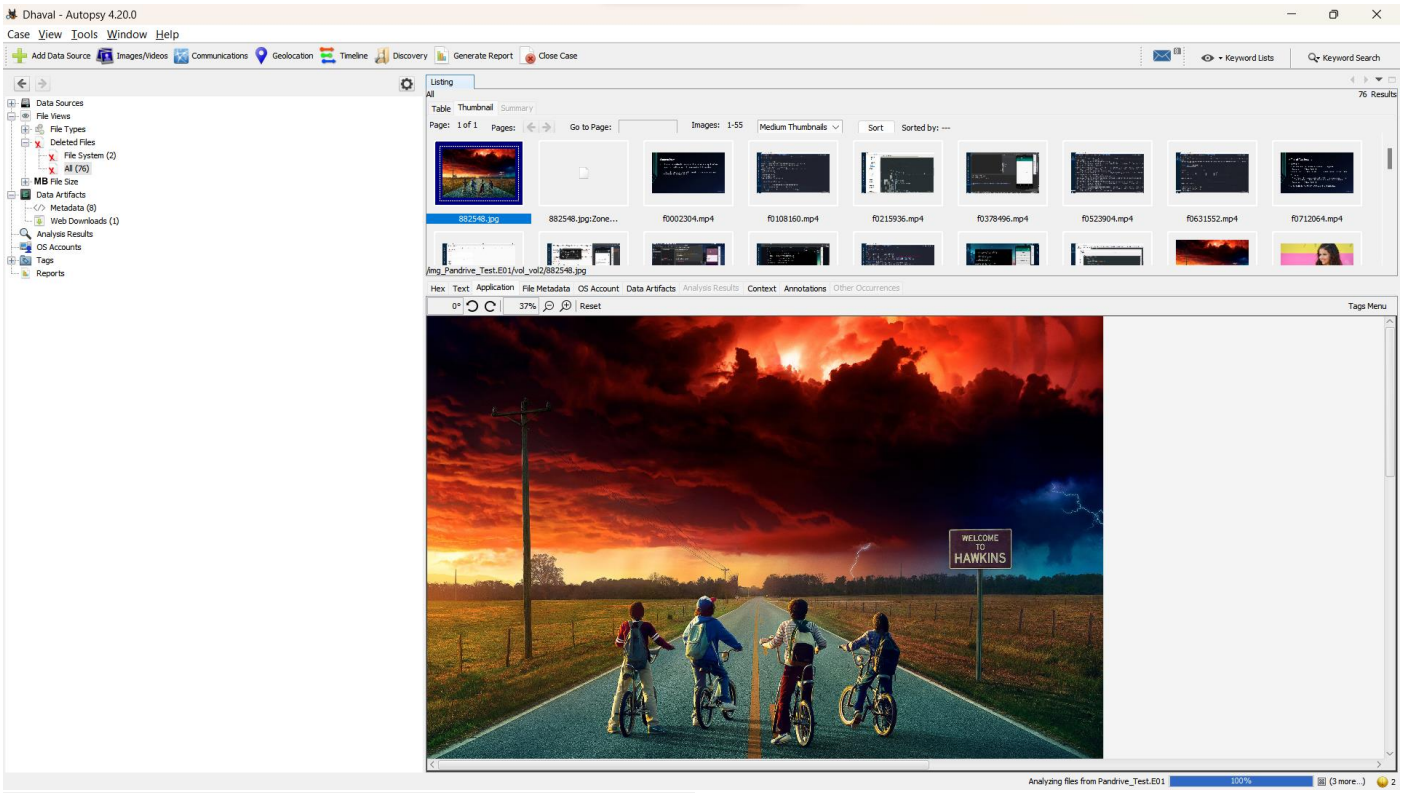


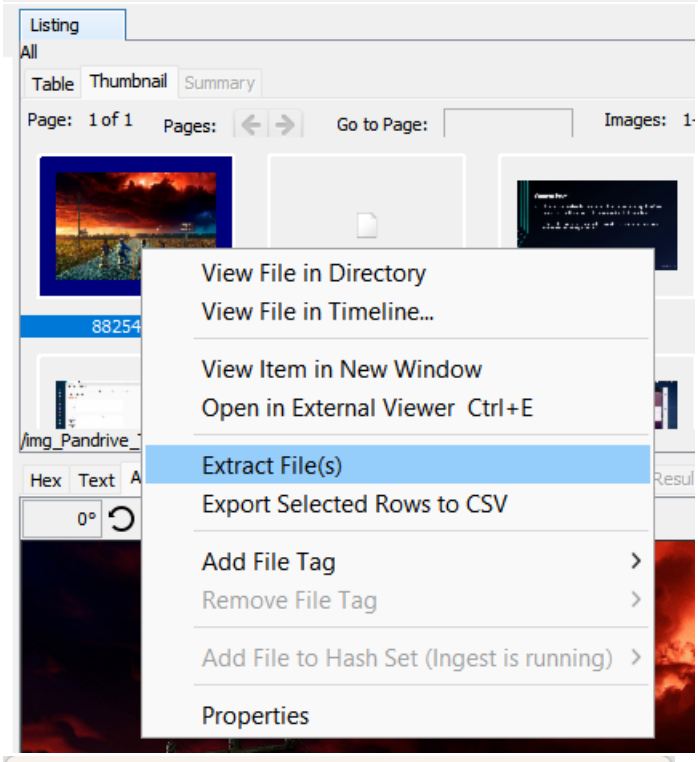
6. Search for File: Utilize Autopsy's search functionality to locate the target file within the data source. You can specify the file name or use file metadata to narrow down the search results.

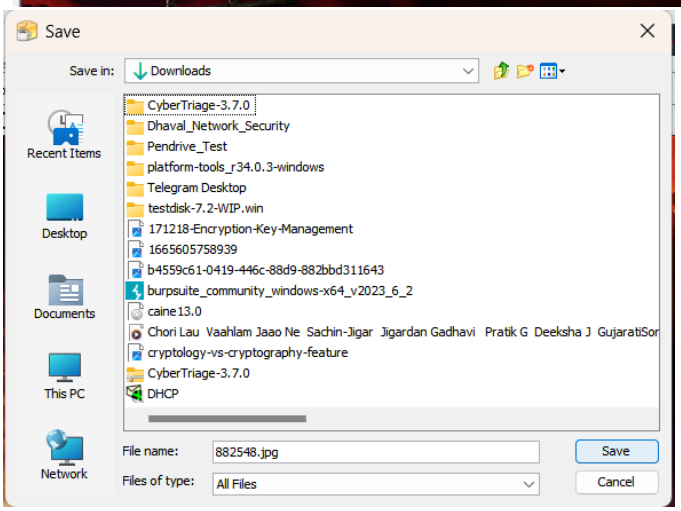


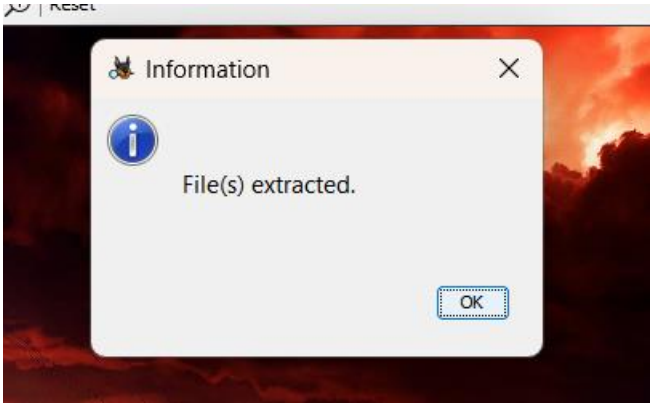


7. Recover File: Once the target file is located, select the file and choose the recovery option provided by Autopsy. Follow the prompts to specify the destination for the recovered file.


Dhaval - Autopsy 4.20.0
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
Deleted Files
File System (2)
All (76)
MB File Size
Data Artifacts
Metadata (8)
Web Downloads (1)
Analysis Results
OS Accounts
Tags
Reports
Listing
All
76 Results
Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Images: 1-55
Medium Thumbnails
Sort
Sorted by: ---
882548.jpg
882548.jpg:Zone...
f0002304.mp4
f0108160.mp4
f0215936.mp4
f0378496.mp4
f0523904.mp4
f0631552.mp4
f0712064.mp4
/img_Pandrive_Test.E01/vol_vol2/882548.jpg
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Reset
Tags Menu
WELCOME TO HAWKINS
Analyzing files from Pandrive_Test.E01
100%
(3 more...)


Listing
All
Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Images: 1-
View File in Directory
View File in Timeline...
View Item in New Window
Open in External Viewer Ctrl+E
Extract File(s)
Export Selected Rows to CSV
Add File Tag
Remove File Tag
Add File to Hash Set (Ingest is running)
Properties
Hex
Text
0°


Save
Save in:
Downloads
Recent Items
Desktop
Documents
This PC
Network
CyberTriage-3.7.0
Dhaval_Network_Security
Pendrive_Test
platform-tools_r34.0.3-windows
Telegram Desktop
testdisk-7.2-WIP.win
171218-Encryption-Key-Management
1665605758939
b4559c61-0419-446c-88d9-882bbd311643
burpsuite_community_windows-x64_v2023_6_2
caine13.0
Chori Lau Vaahlam Jaao Ne Sachin-Jigar Jigardan Gadhavi Pratik G Deeksha J GujaratiSor
cryptology-vs-cryptography-feature
CyberTriage-3.7.0
DHCP
File name:
882548.jpg
Save
Files of type:
All Files
Cancel



8. Verify Recovery: After the recovery process is complete, verify the recovered file's integrity and accessibility to ensure a successful recovery.
9. Document Findings: Record the details of the recovery process, including the file name, location, and any additional observations or notes.

Result:

Using Autopsy, we successfully recovered the target file from the given data source. After adding and configuring the data source within the Autopsy case, we initiated the analysis and performed a search to locate the file. The file was successfully recovered, and its integrity and accessibility were verified. The details of the recovery, including the file name, location, and any relevant observations, were documented for further analysis.

Conclusion:

Autopsy proved to be an effective digital forensics tool for file recovery from the given data source. Its comprehensive search capabilities, combined with the recovery functionality, allowed us to successfully locate and recover the target file. Autopsy can be a valuable asset in forensic investigations, data recovery processes, and digital evidence analysis.

Future Scope:

1. Advanced file carving techniques: Explore Autopsy's advanced file carving capabilities to recover files even in fragmented or damaged states.
2. Timeline analysis: Utilize Autopsy's timeline feature to establish a chronological order of events related to the recovered file and other artifacts.
3. Metadata extraction and analysis: Extract and analyze file metadata using Autopsy to gain further insights into the recovered file's origin, timestamps, and associated attributes.
4. Hash analysis: Perform hash analysis on the recovered file to determine its integrity and check against known hash databases for potential matches.
5. Integration with other forensic tools: Explore integrating Autopsy with other digital forensics tools for a more comprehensive analysis and cross-validation of findings.