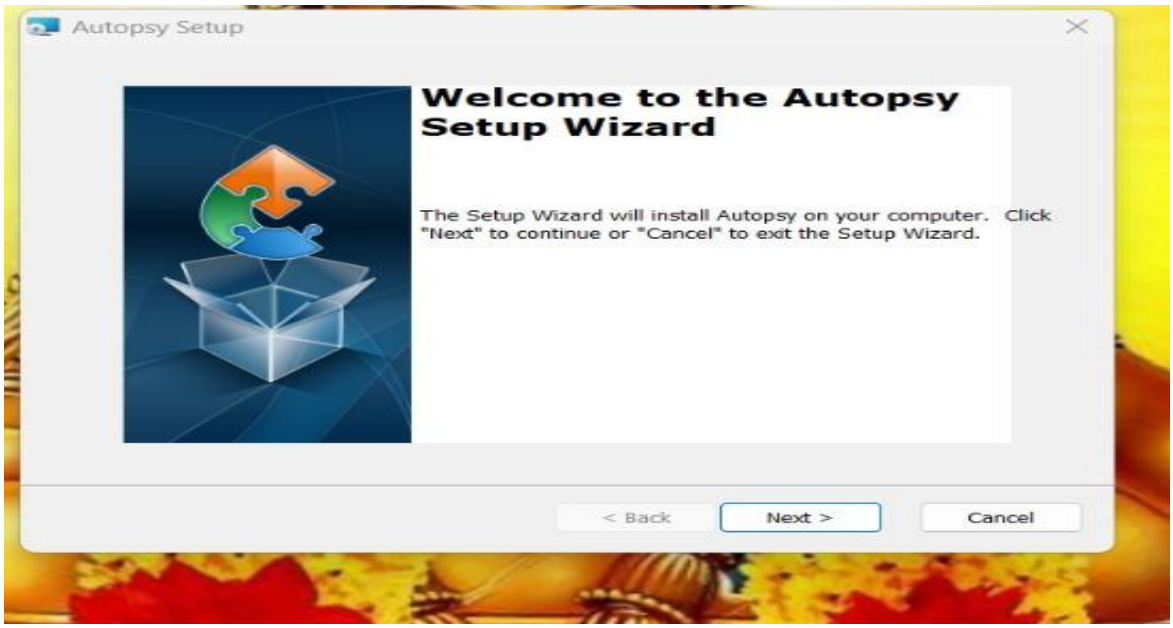
Hands-On Lab: Image Analysis Using Autopsy

Report By :

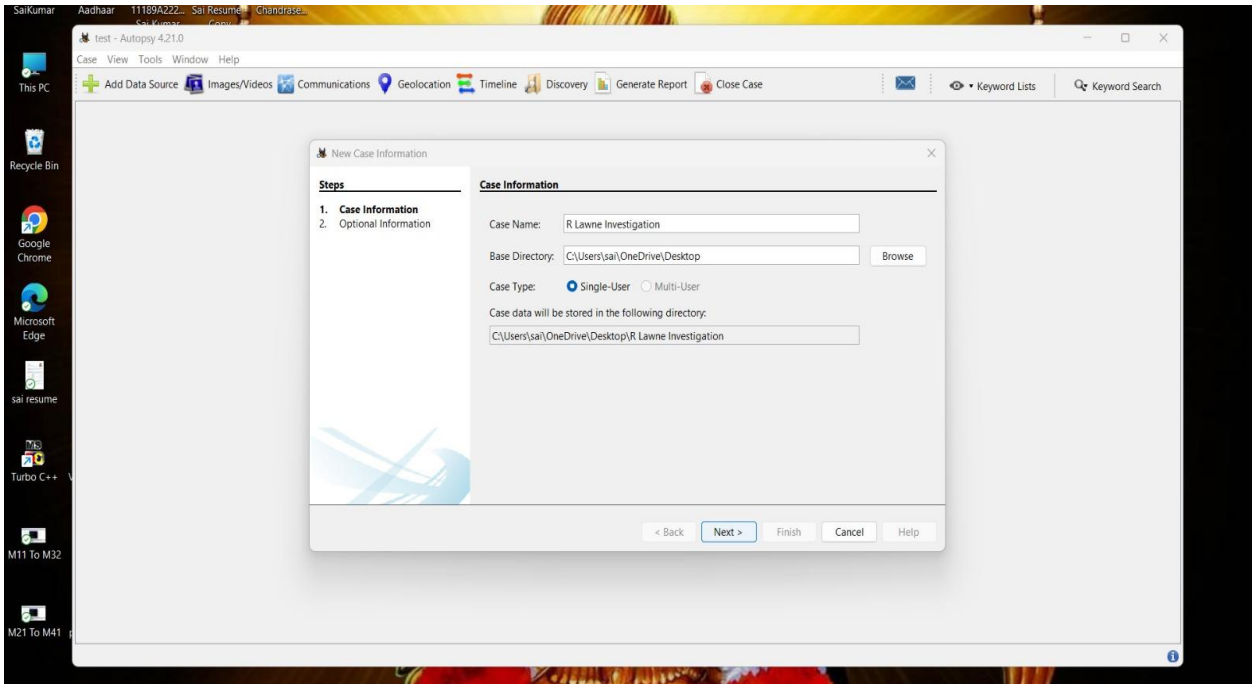
Prathyusha Kesireddygari

Downloading and Installing Autopsy

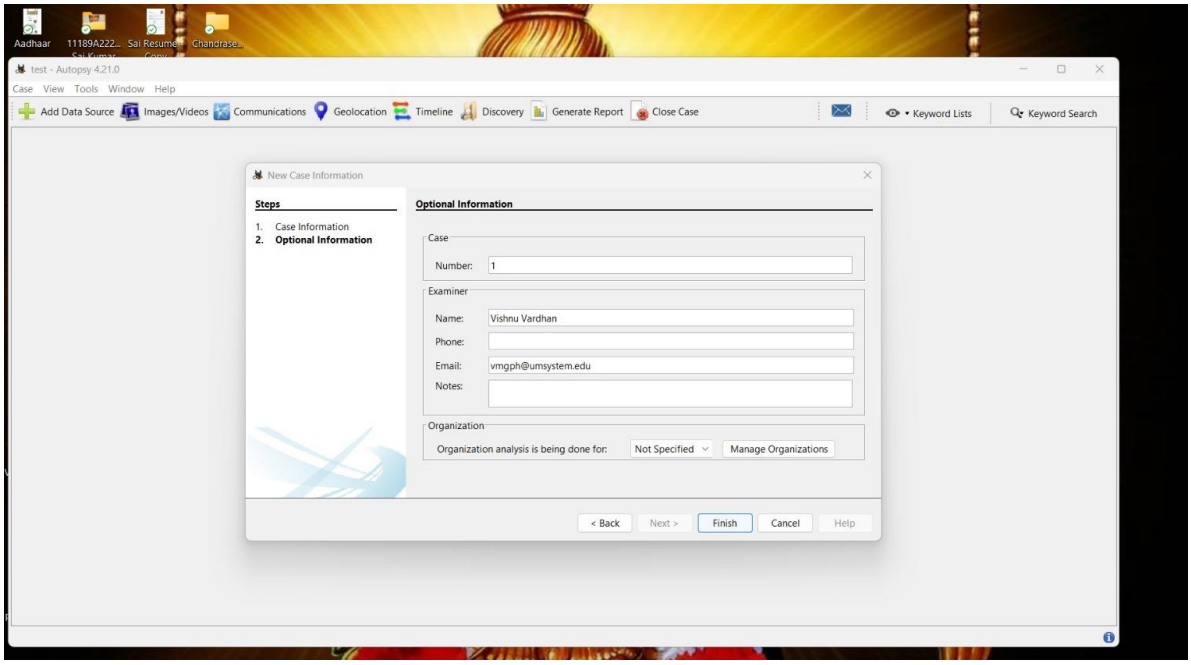
- Downloading and running the Autopsy.msi file

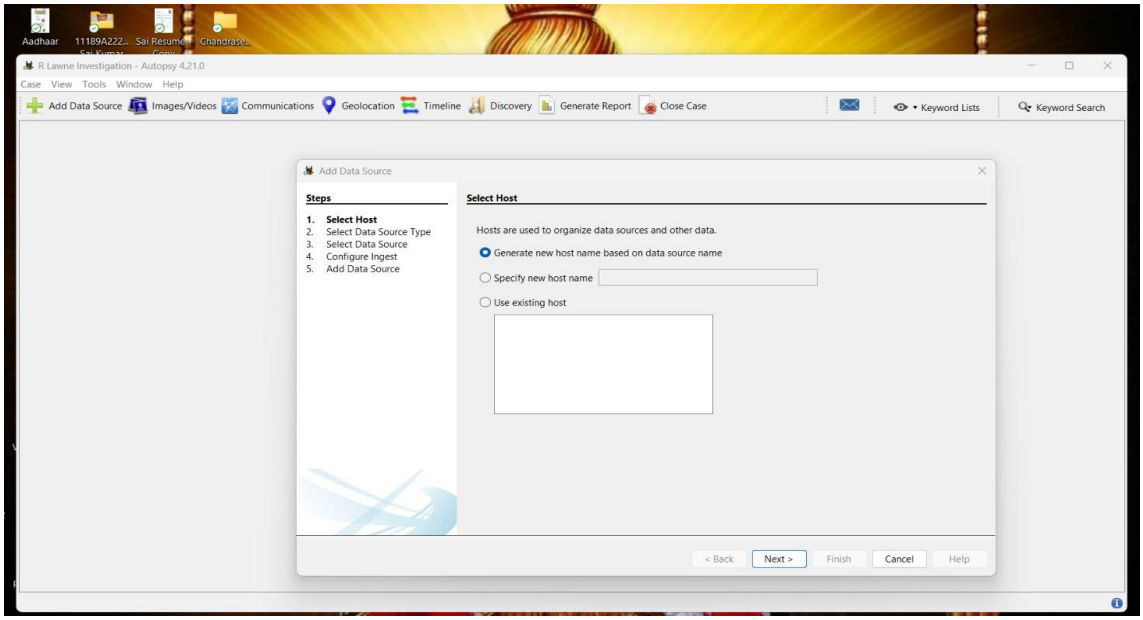


- Providing installation path

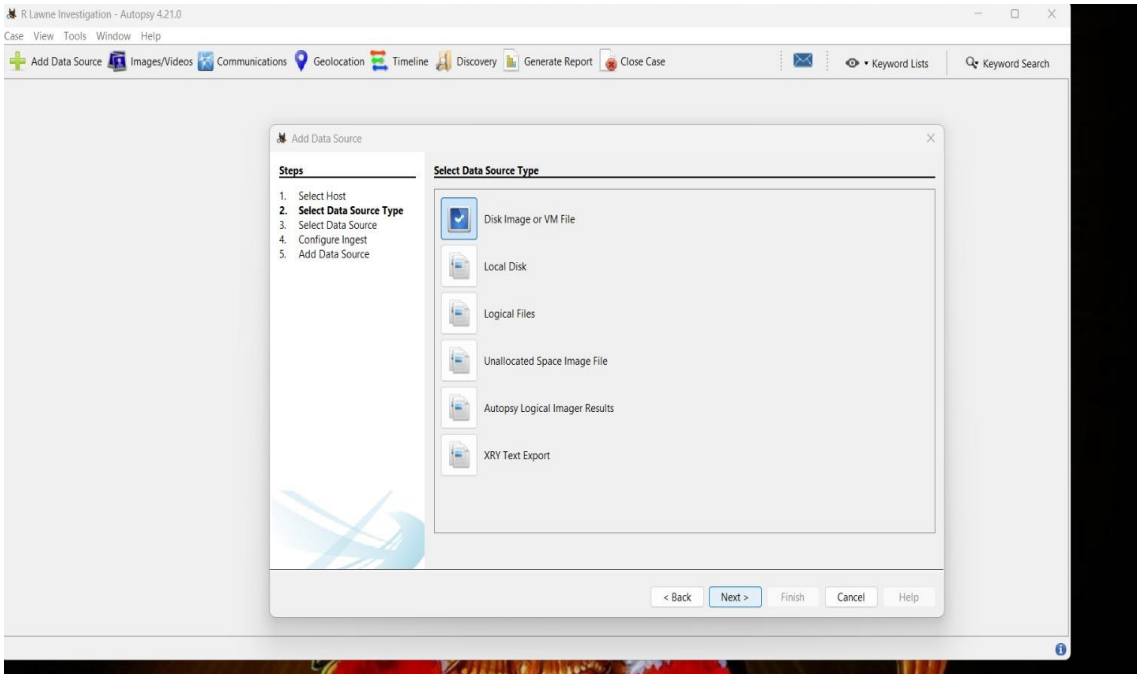


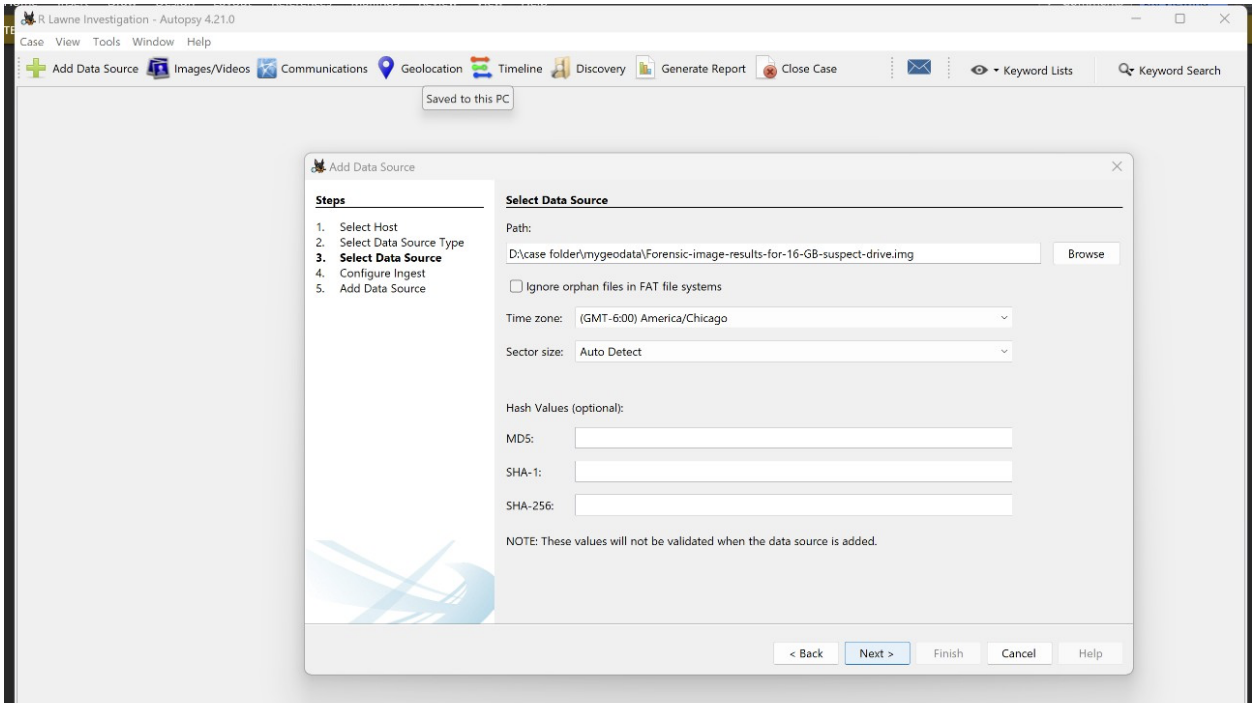
- Providing case number and other details



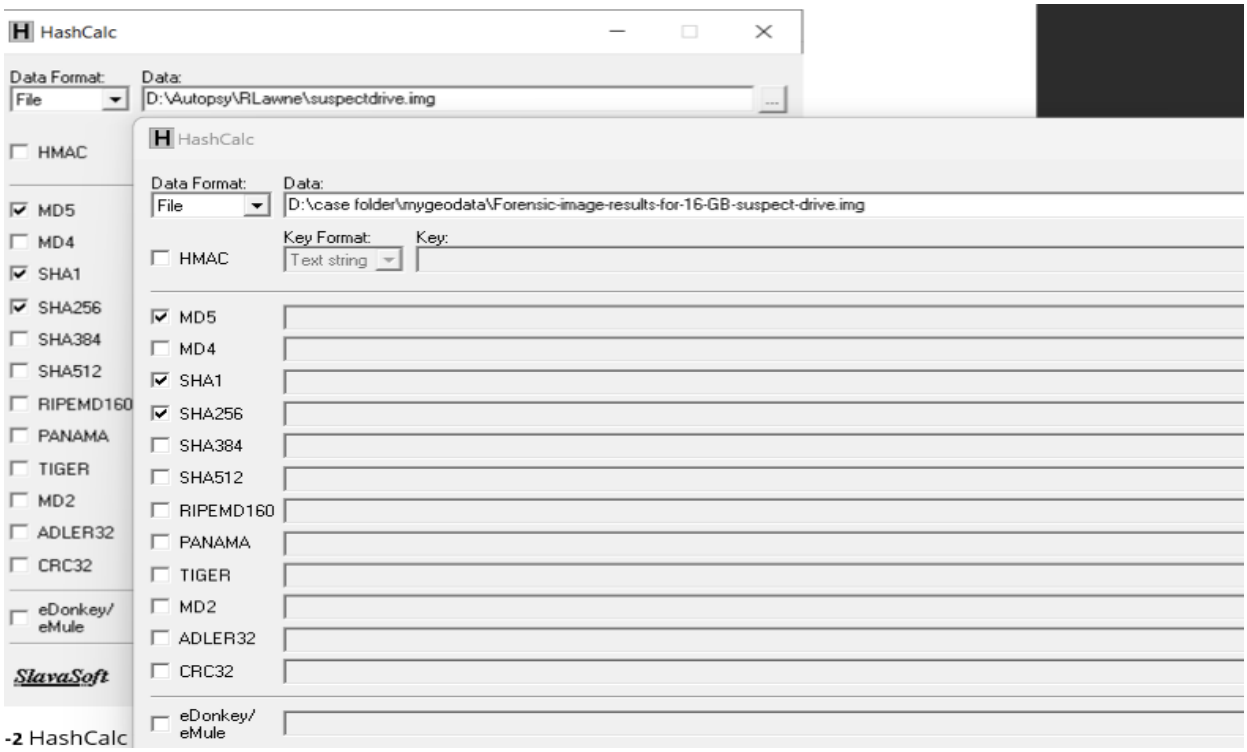


- Importing a Suspect Image File Using Autopsy

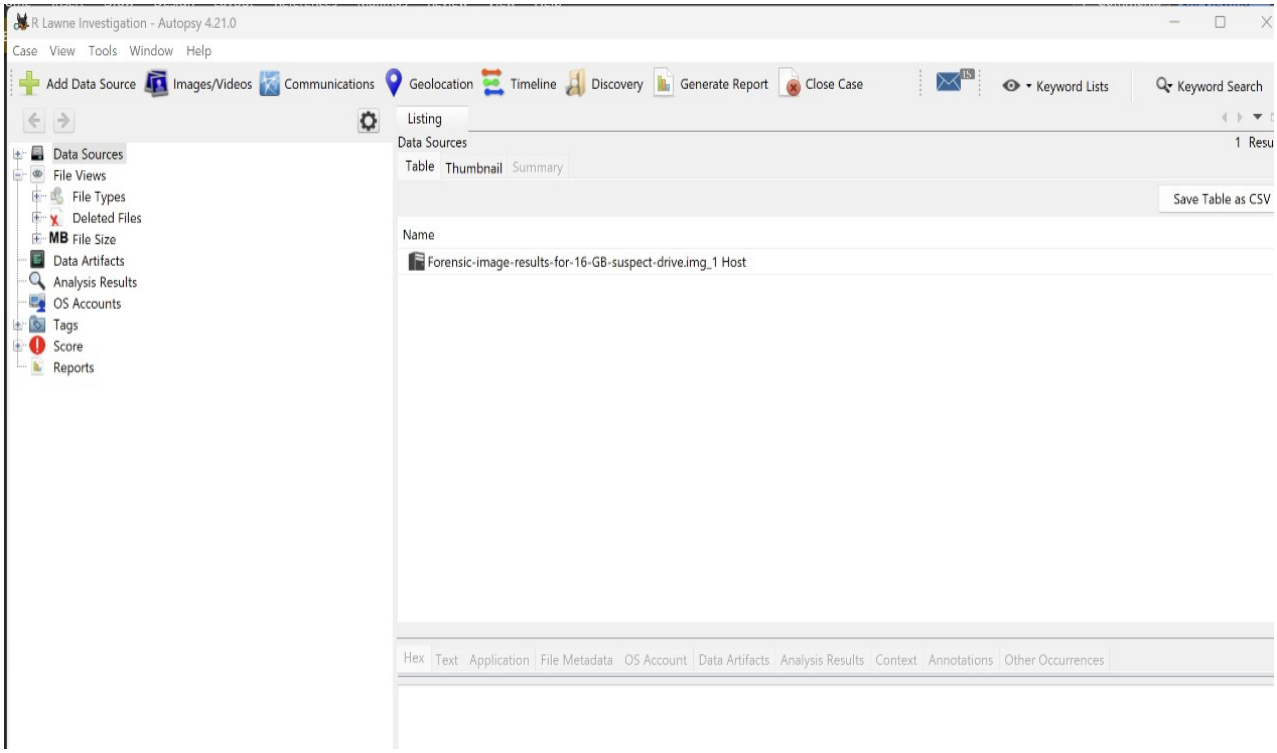




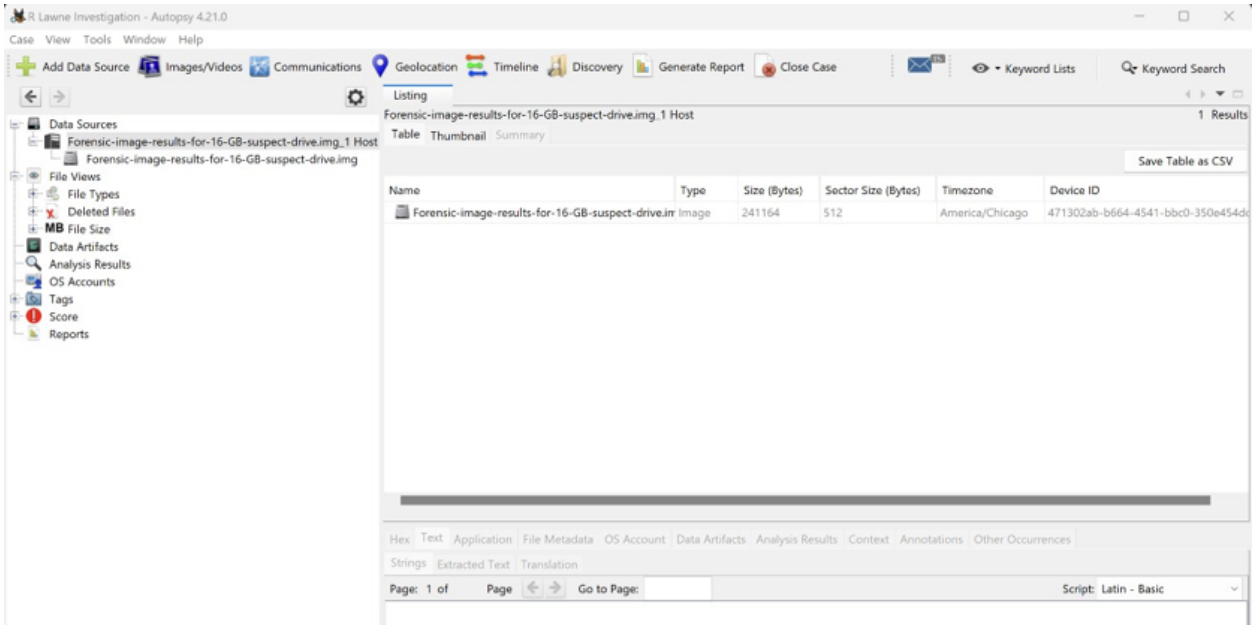
- Using hashcalc tool to generate hash values

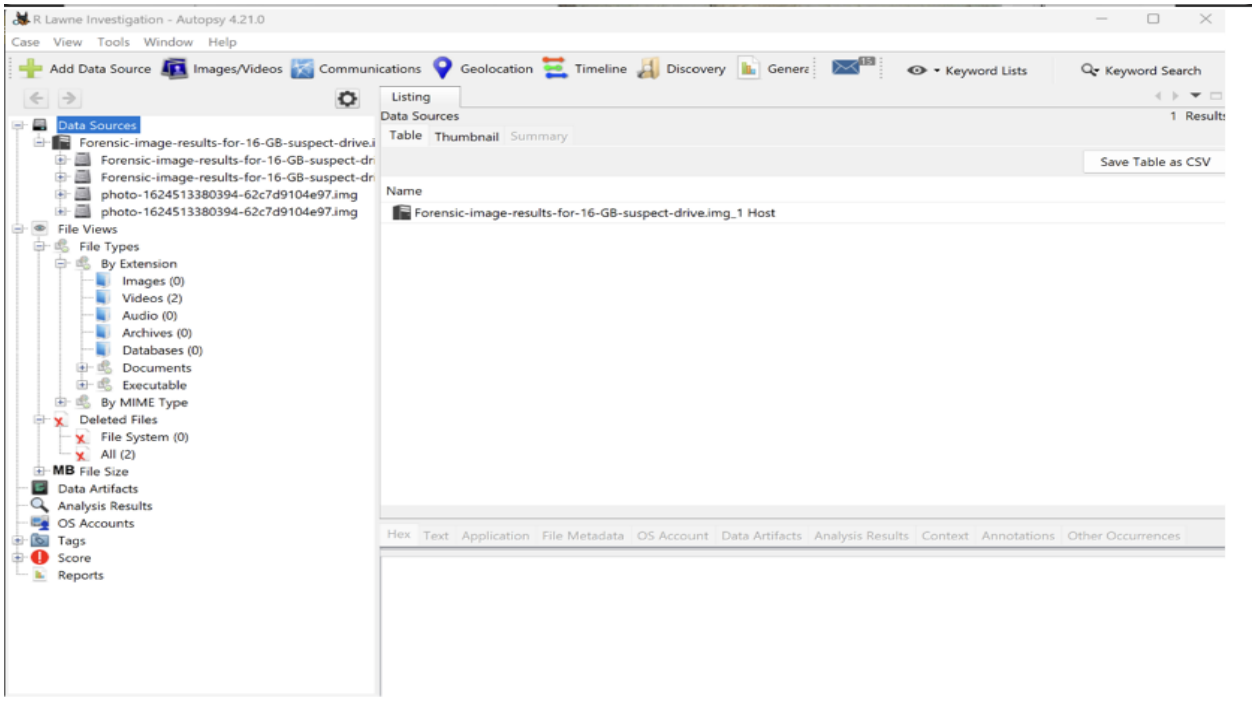


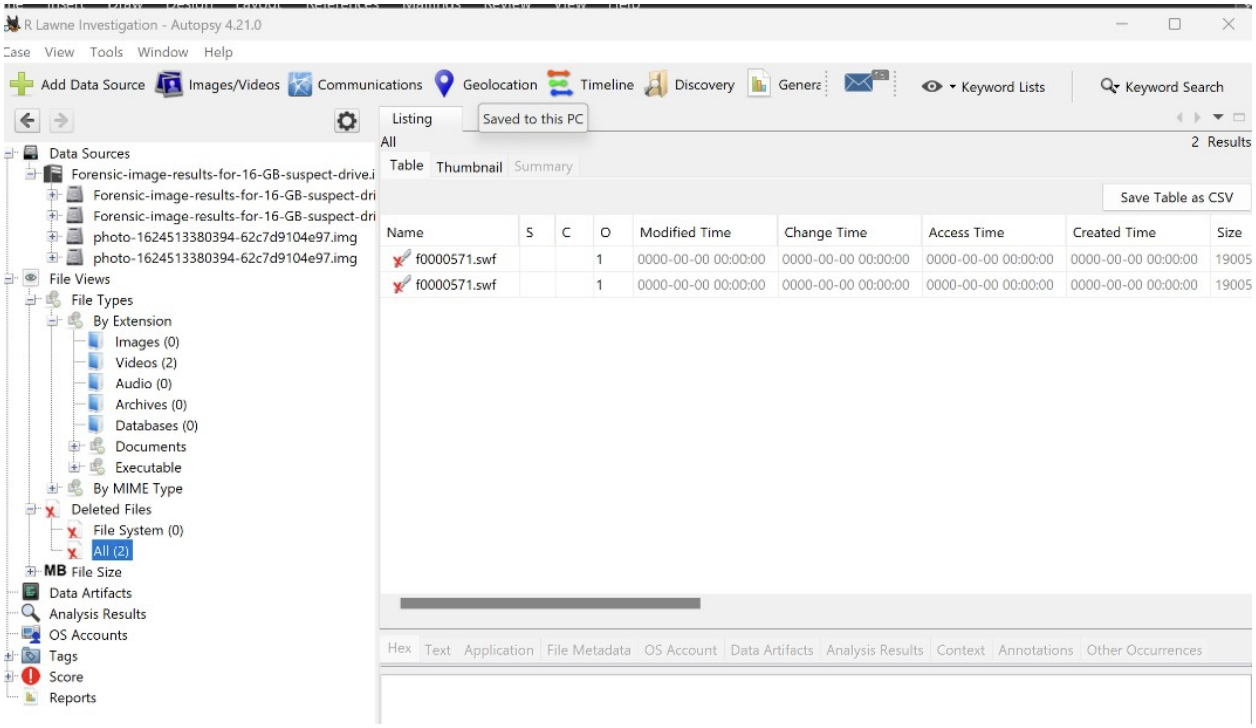
- Examining the Suspect Image File Using Autopsy

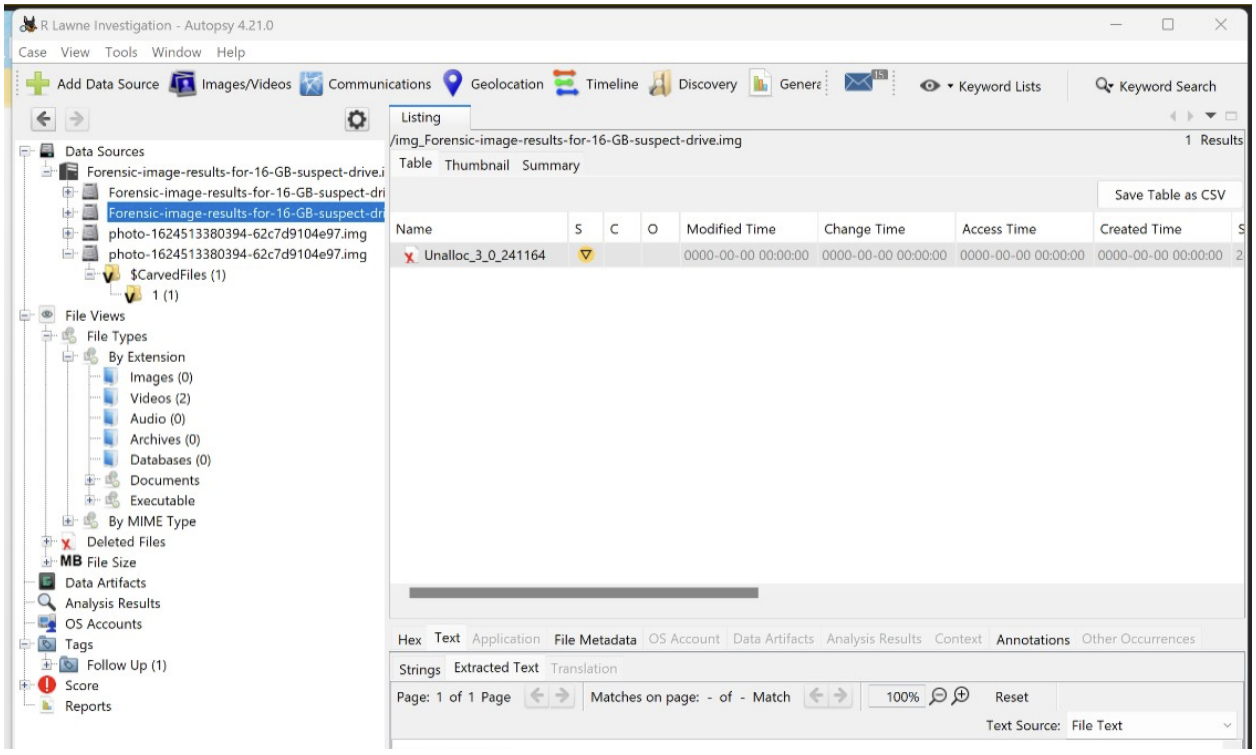


- Examining the contents of suspectdrive.img file

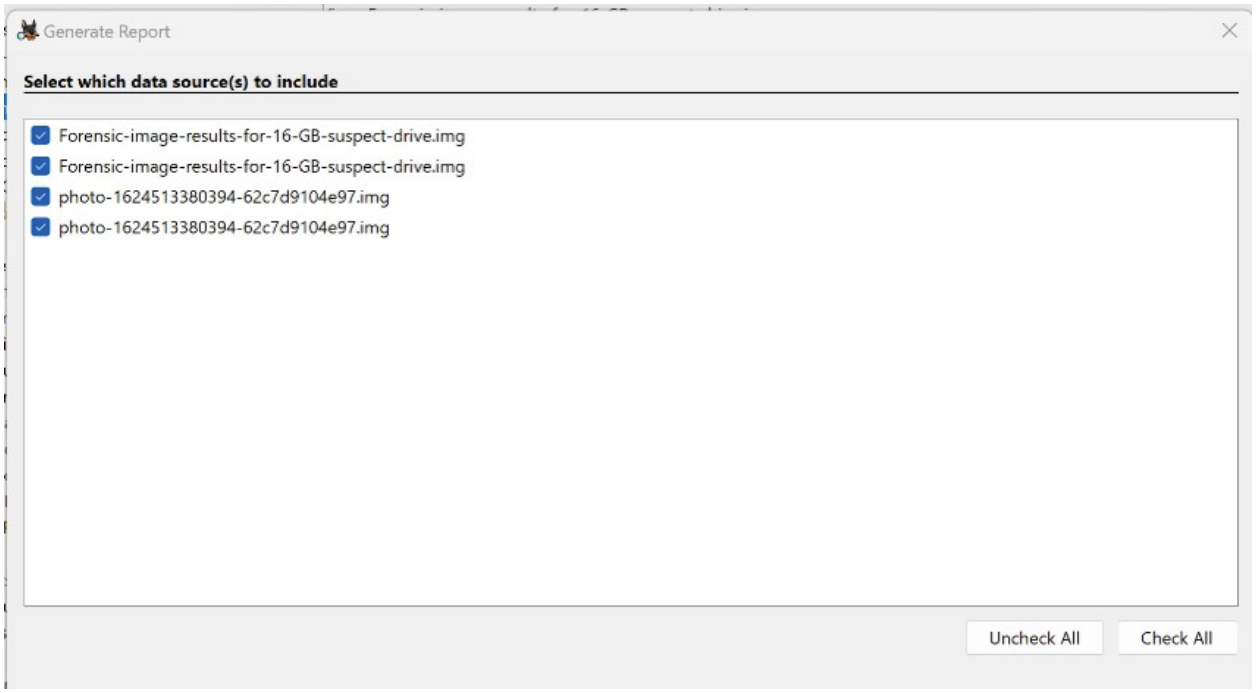


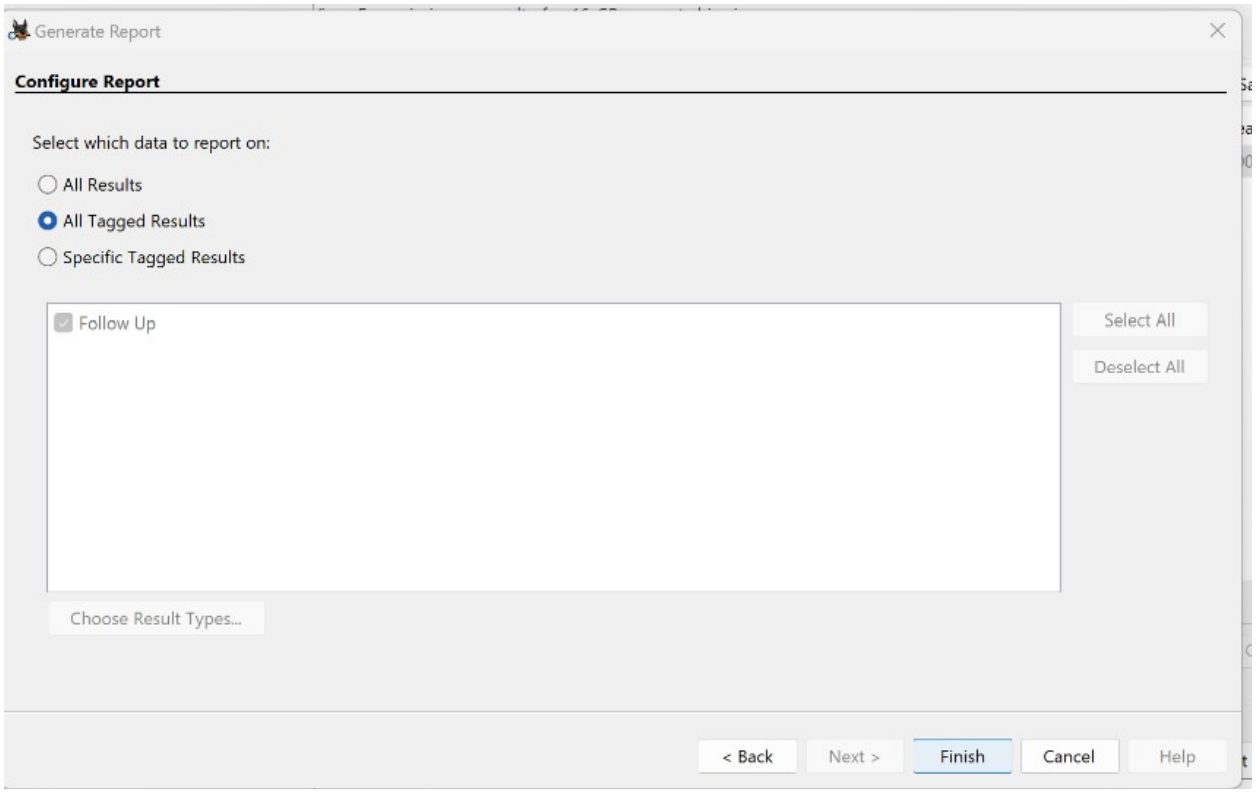



R Lawne Investigation - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Keyword Lists
Keyword Search
Listing
Saved to this PC
All
2 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
f0000571.swf
f0000571.swf
0000-00-00 00:00:00
19005
Data Sources
Forensic-image-results-for-16-GB-suspect-drive.i
photo-1624513380394-62c7d9104e97.img
File Views
File Types
By Extension
Images (0)
Videos (2)
Audio (0)
Archives (0)
Databases (0)
Documents
Executable
By MIME Type
Deleted Files
File System (0)
All (2)
File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

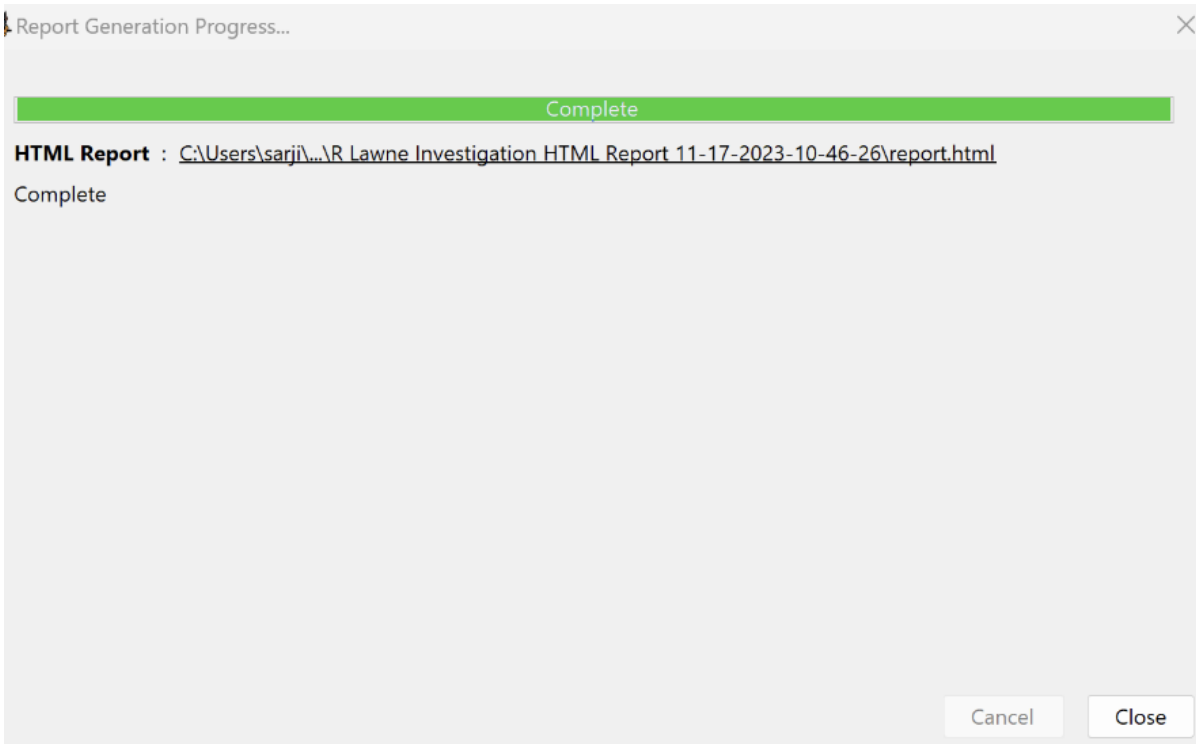

R Lawne Investigation - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Keyword Lists
Keyword Search
Listing
/img_Forensic-image-results-for-16-GB-suspect-drive.img
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Unalloc_3_0_241164
0000-00-00 00:00:00
Data Sources
Forensic-image-results-for-16-GB-suspect-drive.i
photo-1624513380394-62c7d9104e97.img
$CarvedFiles (1)
1 (1)
File Views
File Types
By Extension
Images (0)
Videos (2)
Audio (0)
Archives (0)
Databases (0)
Documents
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Follow Up (1)
Score
Reports
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

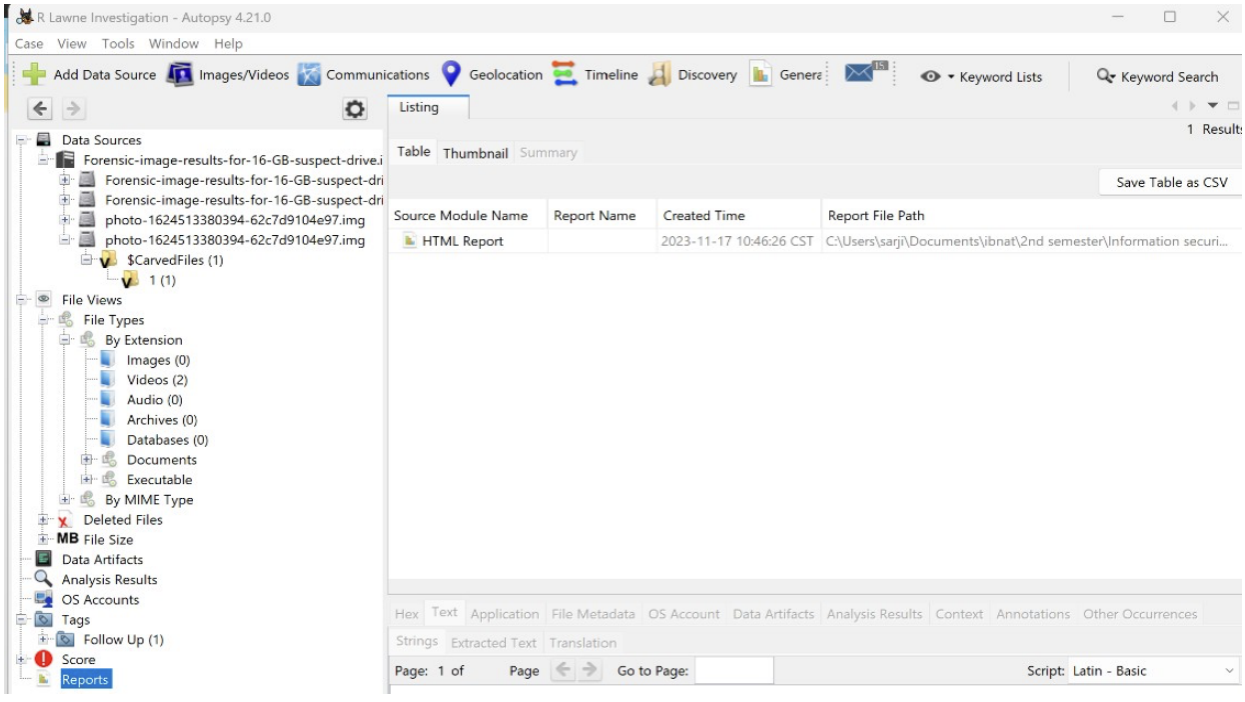
- Adding File tags





- Generating HTML report and viewing in web browser


Report Generation Progress...
Complete
HTML Report : C:\Users\sarji\...\R Lawne Investigation HTML Report 11-17-2023-10-46-26\report.html
Complete
Cancel
Close


R Lawne Investigation - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Keyword Lists
Keyword Search
Listing
Table
Thumbnail
Summary
Save Table as CSV
Source Module Name
Report Name
Created Time
Report File Path
HTML Report
2023-11-17 10:46:26 CST
Data Sources
File Views
File Types
By Extension
Images (0)
Videos (2)
Audio (0)
Archives (0)
Databases (0)
Documents
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Follow Up (1)
Score
Reports
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Extracted Text
Translation
Page: 1 of
Page
Go to Page:
Script: Latin - Basic

Recent Activity Module:	4.21.0
Virtual Machine Extractor Module:	4.21.0
YARA Analyzer Module:	4.21.0
iOS Analyzer (iLEAPP) Module:	4.21.0

Ingest History:

Job 1:

Data Source:	Forensic-image-results-for-16-GB-suspect-drive.img
Status:	COMPLETED
Enabled Modules:	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 Android Analyzer (aLEAPP) DJI Drone Analyzer YARA Analyzer iOS Analyzer (iLEAPP) GPX Parser

Report Navigation

- Case Summary
- Tagged Files (1)
- Tagged Images (0)
- Tagged Results (0)

GPX Parser
Android Analyzer

Job 2:

Data Source:	Forensic-image-results-for-16-GB-suspect-drive.img
Status:	COMPLETED
Enabled Modules:	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 Android Analyzer (aLEAPP) DJI Drone Analyzer YARA Analyzer iOS Analyzer (iLEAPP) GPX Parser Android Analyzer

Job 3:

Data Source:	photo-1624513380394-62c7d9104e97.img

Report Navigation

- Case Summary
- Tagged Files (1)
- Tagged Images (0)
- Tagged Results (0)

Job 3:

Data Source:	photo-1624513380394-62c7d9104e97.img
Status:	COMPLETED
Enabled Modules:	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 Android Analyzer (aLEAPP) DJI Drone Analyzer YARA Analyzer iOS Analyzer (iLEAPP) GPX Parser Android Analyzer

Job 4:

Data Source:	photo-1624513380394-62c7d9104e97.img
Status:	COMPLETED
Enabled Modules:	Recent Activity Hash Lookup

Report Navigation

- Case Summary
- Tagged Files (1)
- Tagged Images (0)
- Tagged Results (0)

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
Android Analyzer (aLEAPP)
DJI Drone Analyzer
YARA Analyzer
iOS Analyzer (iLEAPP)
GPX Parser
Android Analyzer

Self-Reflection and Response

Q 1 : Were you able to complete the setup, configuration, and use of Autopsy?
A : Yes, I was able to complete the setup, configuration, and use of Autopsy for digital forensics analysis.

Q2 : If you were not able to complete the setup and configuration, explain what went wrong.
A: I managed to complete all the steps successfully but encountered an issue while displaying the image.