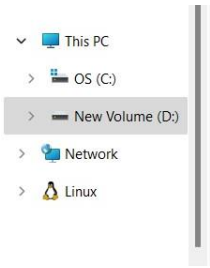
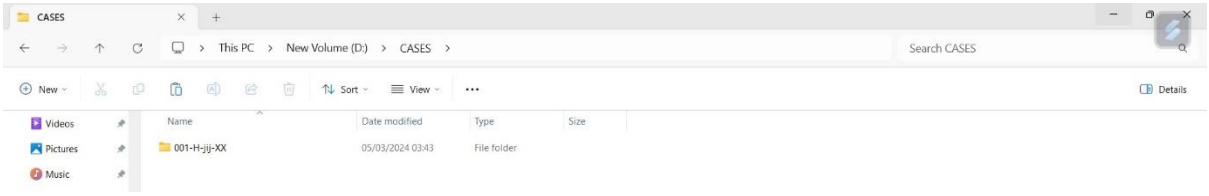
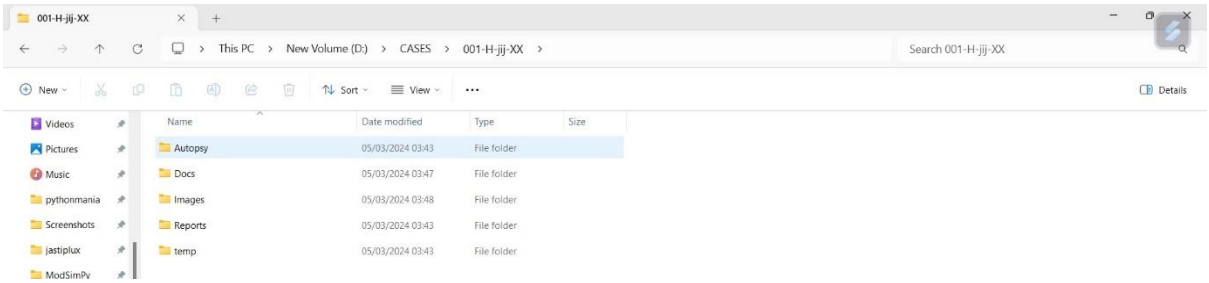
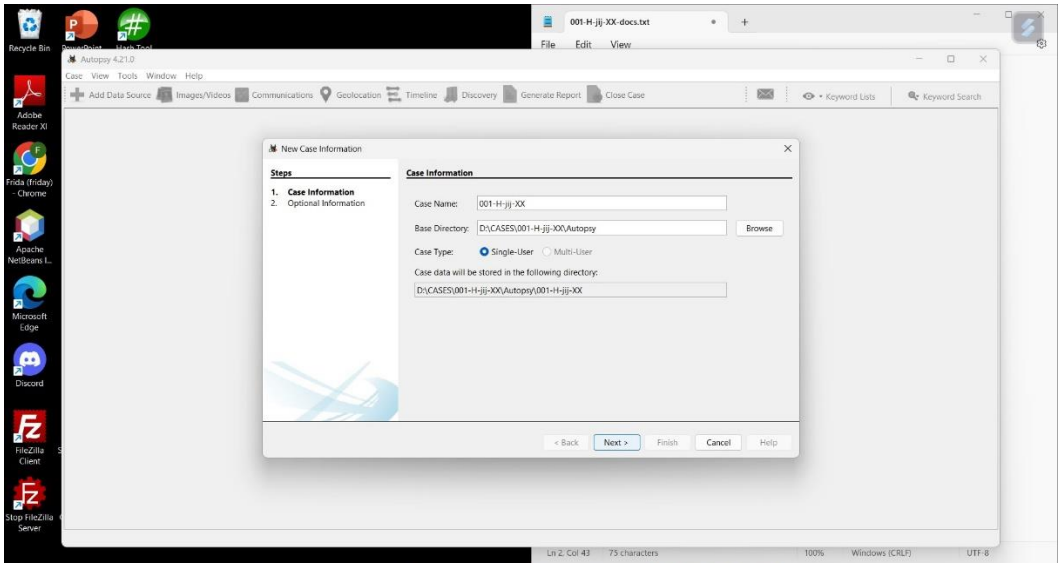
Autopsy Exercise – 1203210098

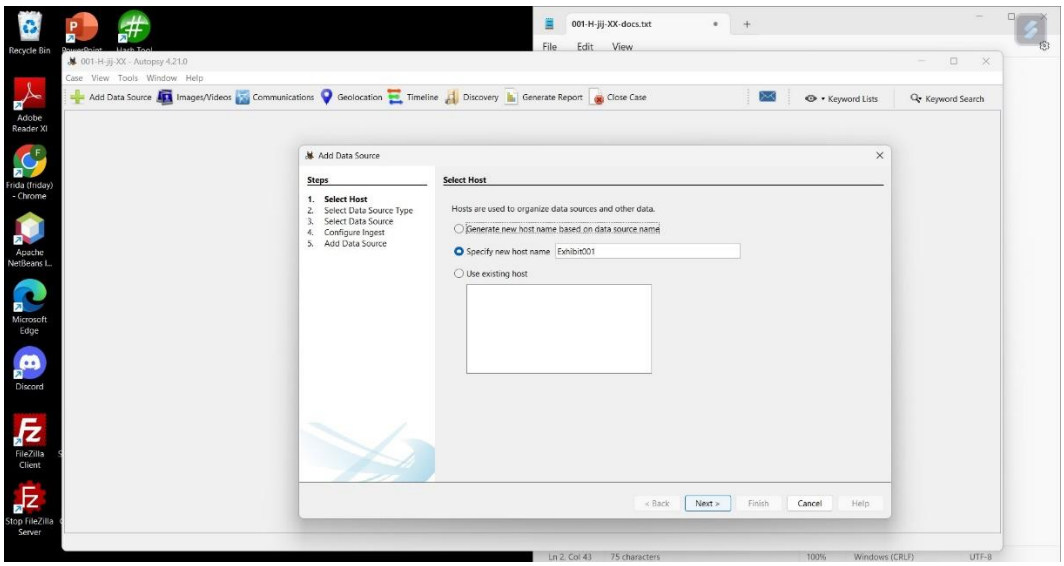
Muatan dokumentasi gambar untuk “Langkah-langkah Percobaan Digital Forensic Investigation dengan menggunakan Autopsy”.

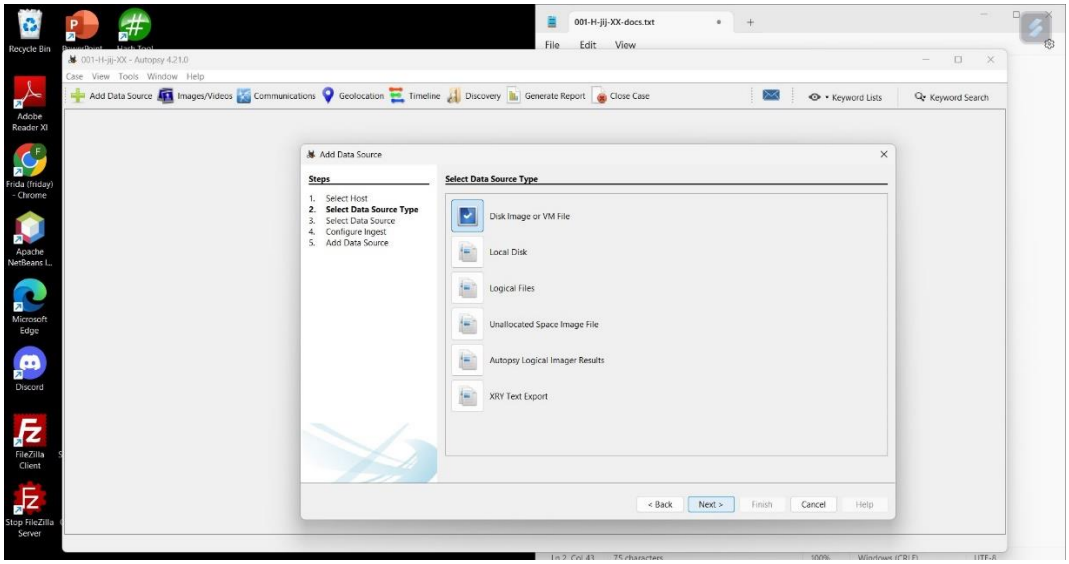
1. 

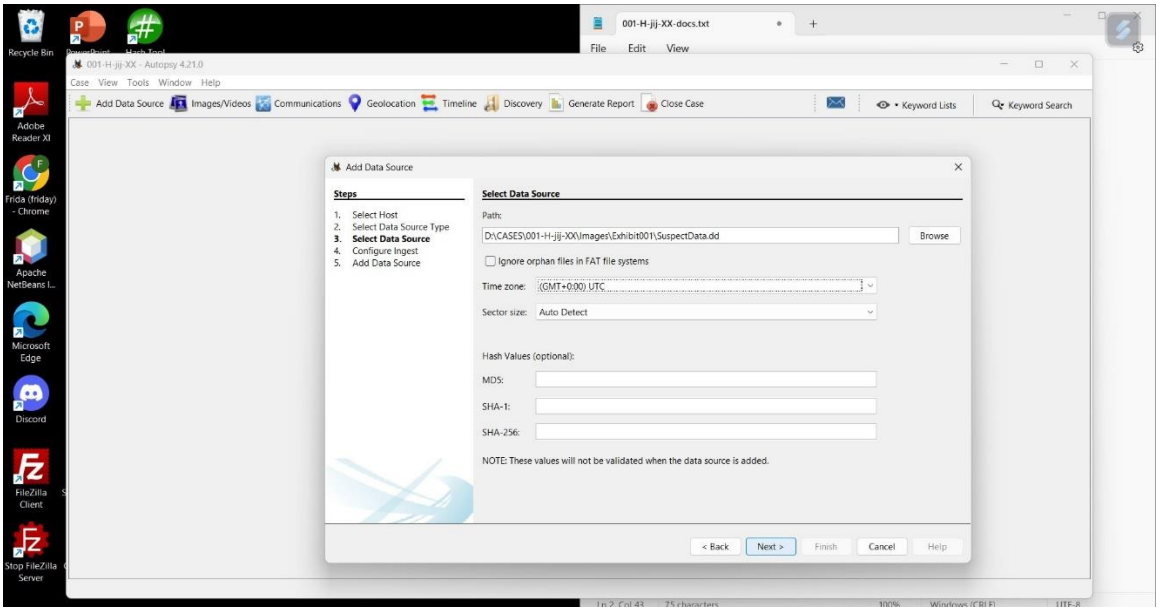
2. 

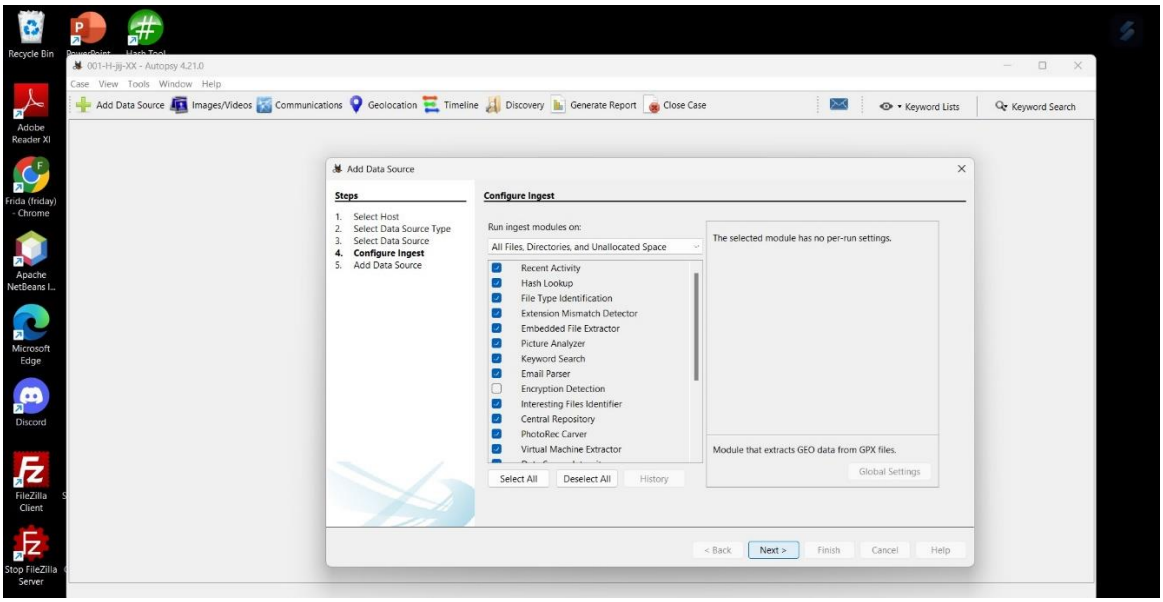
3. 

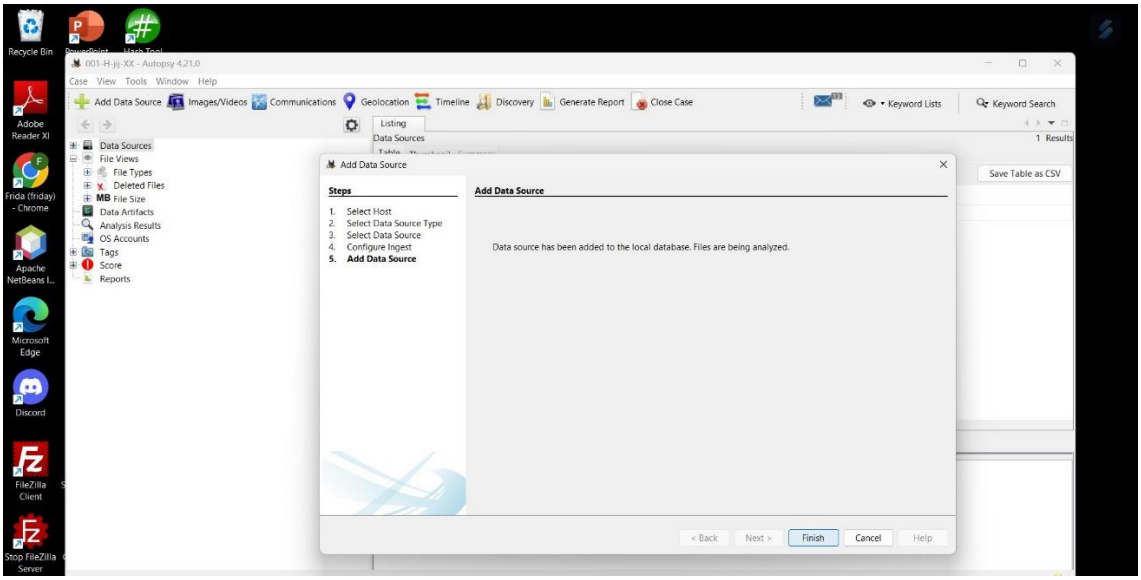
4. 
001-H-jij-XX-docs.txt
Autopsy 4.21.0
New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: 001-H-jij-XX
Base Directory: D:\CASES\001-H-jij-XX\Autopsy
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
D:\CASES\001-H-jij-XX\Autopsy\001-H-jij-XX
< Back
Next >
Finish
Cancel
Help

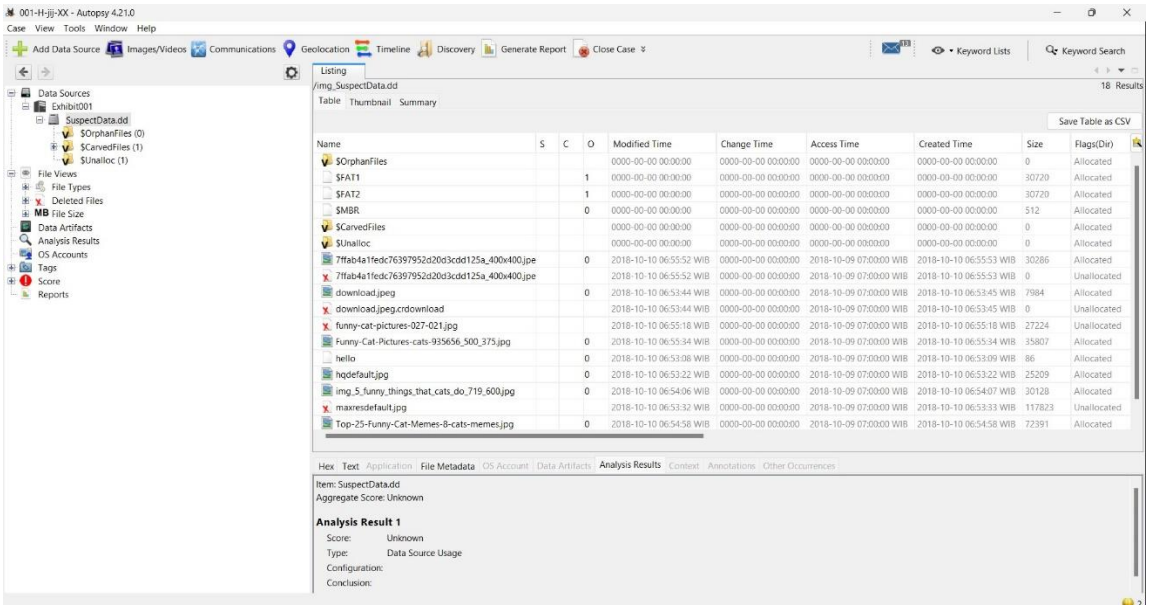
5. 
001-H-jij-XX-docs.txt
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name Exhibit001
Use existing host
< Back
Next >
Finish
Cancel
Help

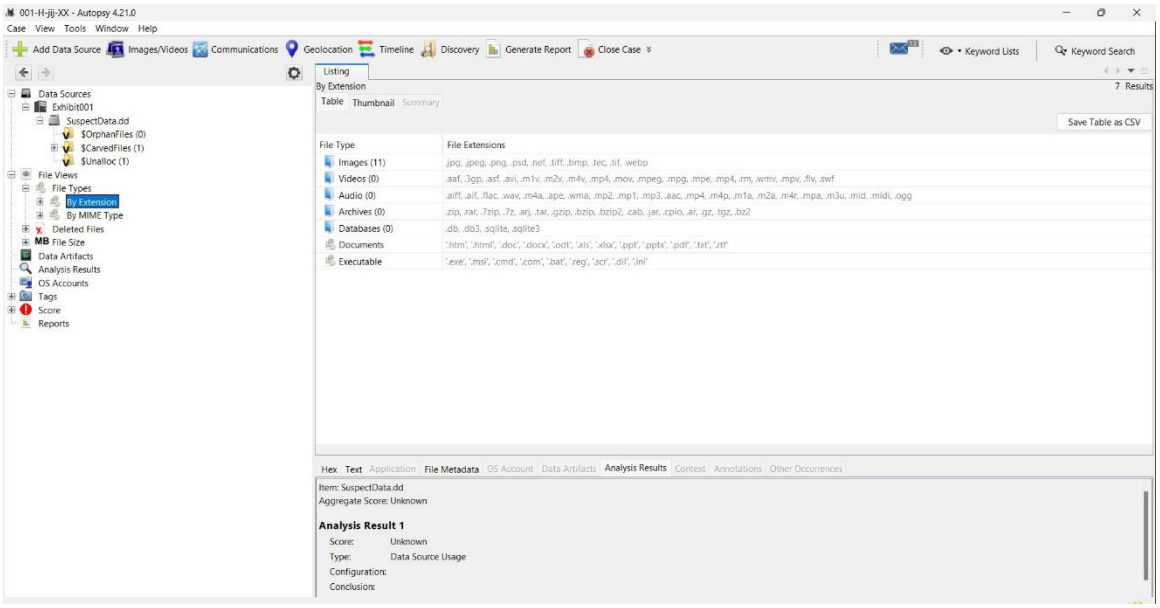

001-H-jij-XX-docs.txt
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back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

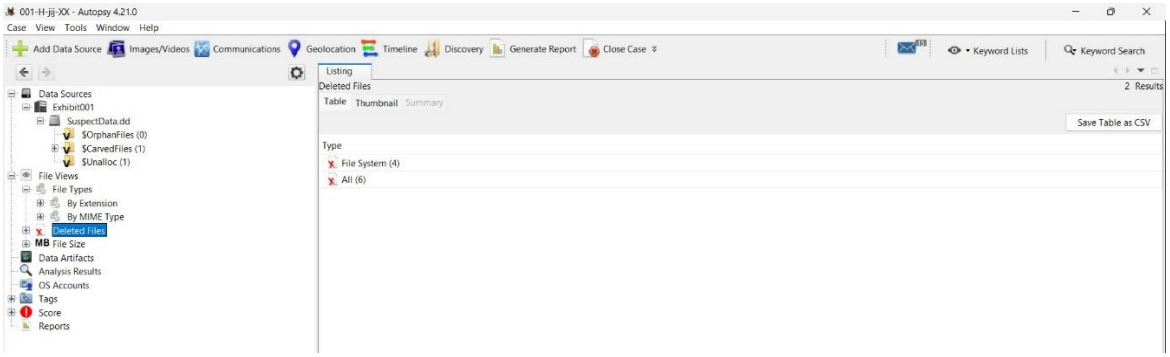

001-H-jij-XX-docs.txt
File Edit View
001-H-jij-XX - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
D:\CASES\001-H-jij-XX\Images\Exhibit001\SuspectData.dd
Browse
Ignore orphan files in FAT file systems
Time zone: (GMT+0:00) UTC
Sector size: Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back Next > Finish Cancel Help
Recycle Bin
Adobe Reader XI
Frida (friday) - Chrome
Apache NetBeans I...
Microsoft Edge
Discord
FileZilla Client
Stop FileZilla Server

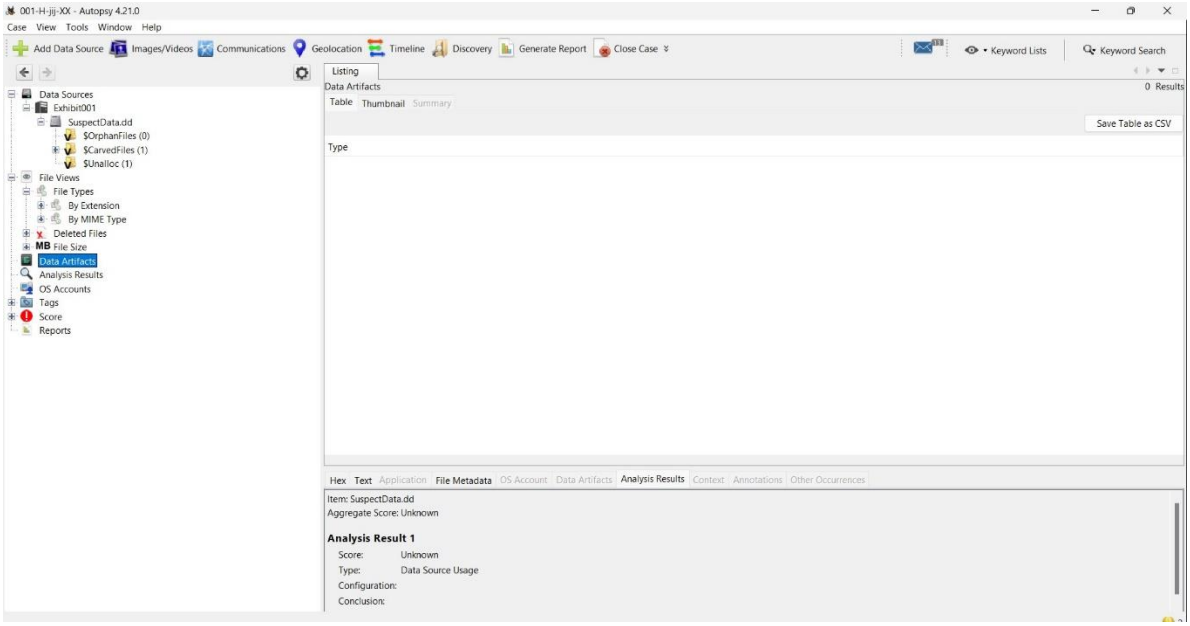

001-H-jij-XX - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
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
The selected module has no per-run settings.
Module that extracts GEO data from GPX files.
Global Settings
Select All Deselect All History
< Back Next > Finish Cancel Help
Recycle Bin
Adobe Reader XI
Frida (friday) - Chrome
Apache NetBeans I...
Microsoft Edge
Discord
FileZilla Client
Stop FileZilla Server

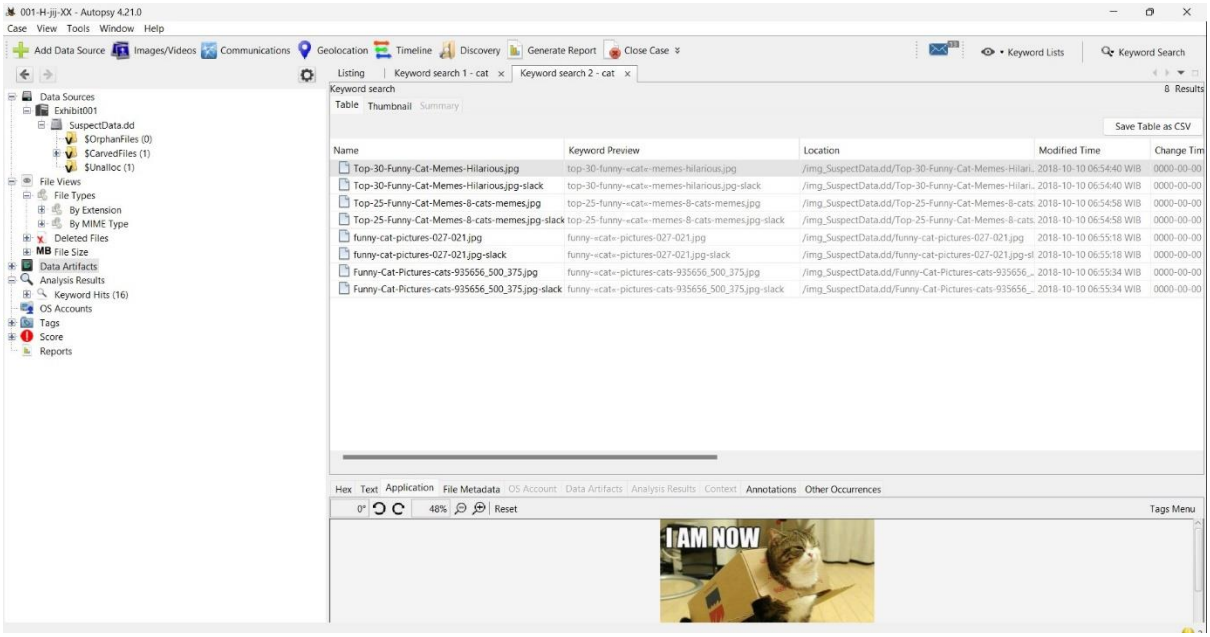
6. 
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

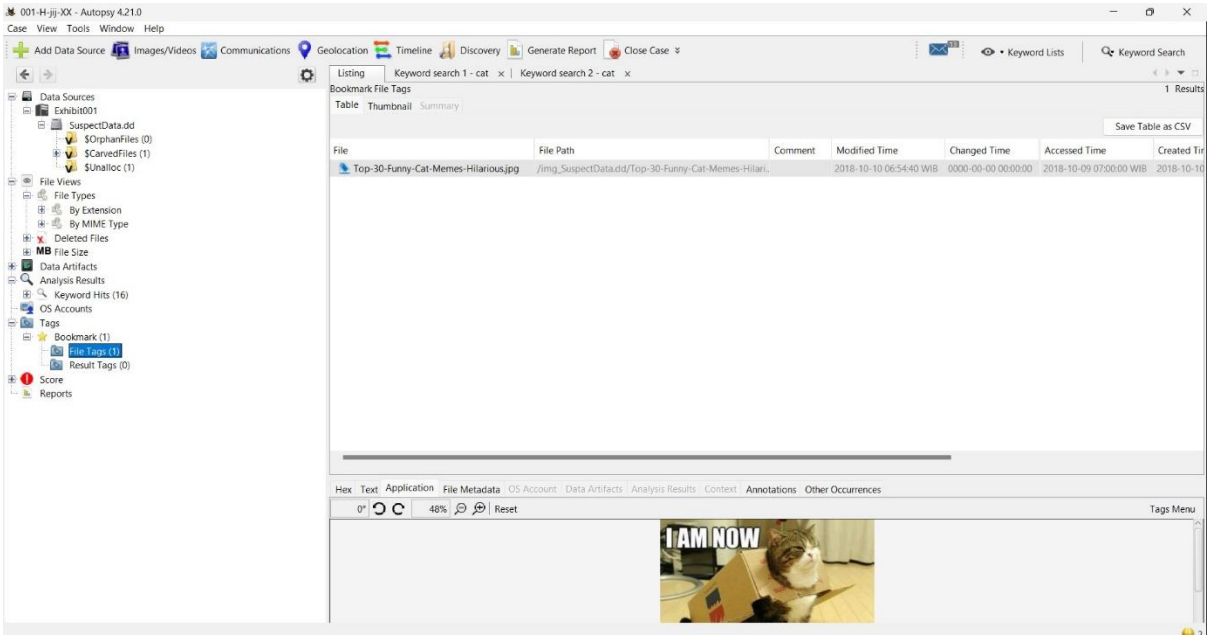
7. 
001-H-jij-XX - Autopsy 4.21.0
Item: SuspectData.dd
Aggregate Score: Unknown
Analysis Result 1
Score: Unknown
Type: Data Source Usage
Configuration:
Conclusion:

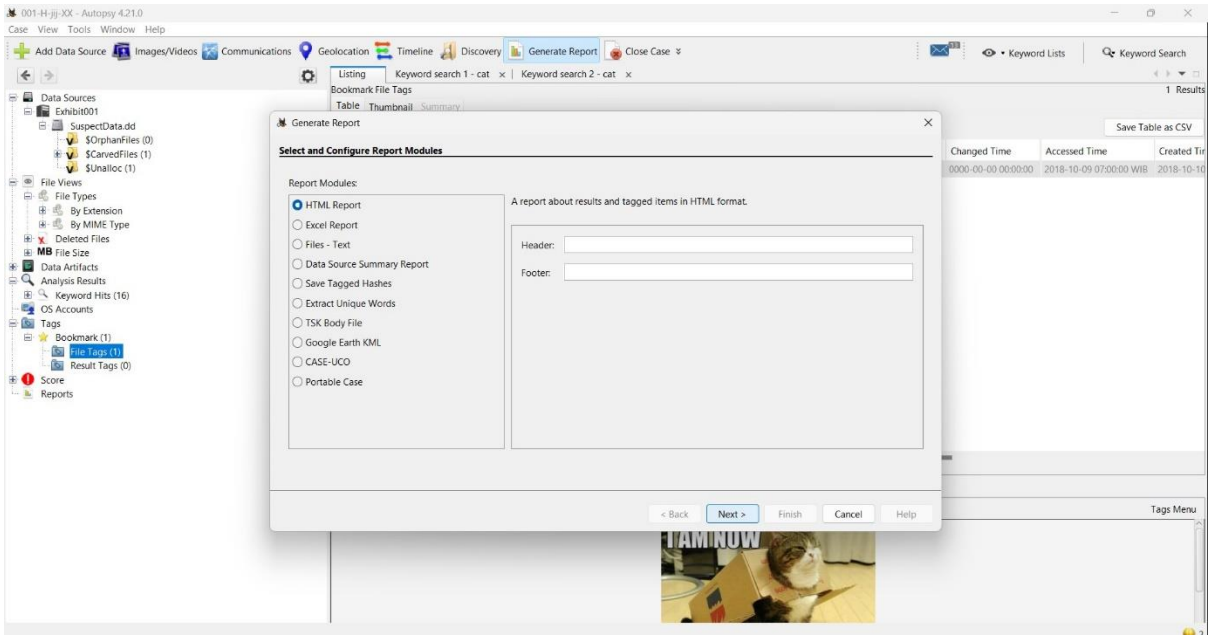
8. 
001-H-jij-XX - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
Exhibit001
SuspectData.dd
$OrphanFiles (0)
$CarvedFiles (1)
$Unalloc (1)
File Views
File Types
By Extension
By MIME Type
Deleted Files
MB File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
By Extension
7 Results
Table Thumbnail Summary
Save Table as CSV
File Type
File Extensions
Images (11)
Videos (0)
Audio (0)
Archives (0)
Databases (0)
Documents
Executable
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Item: SuspectData.dd
Aggregate Score: Unknown
Analysis Result 1
Score: Unknown
Type: Data Source Usage
Configuration:
Conclusion:

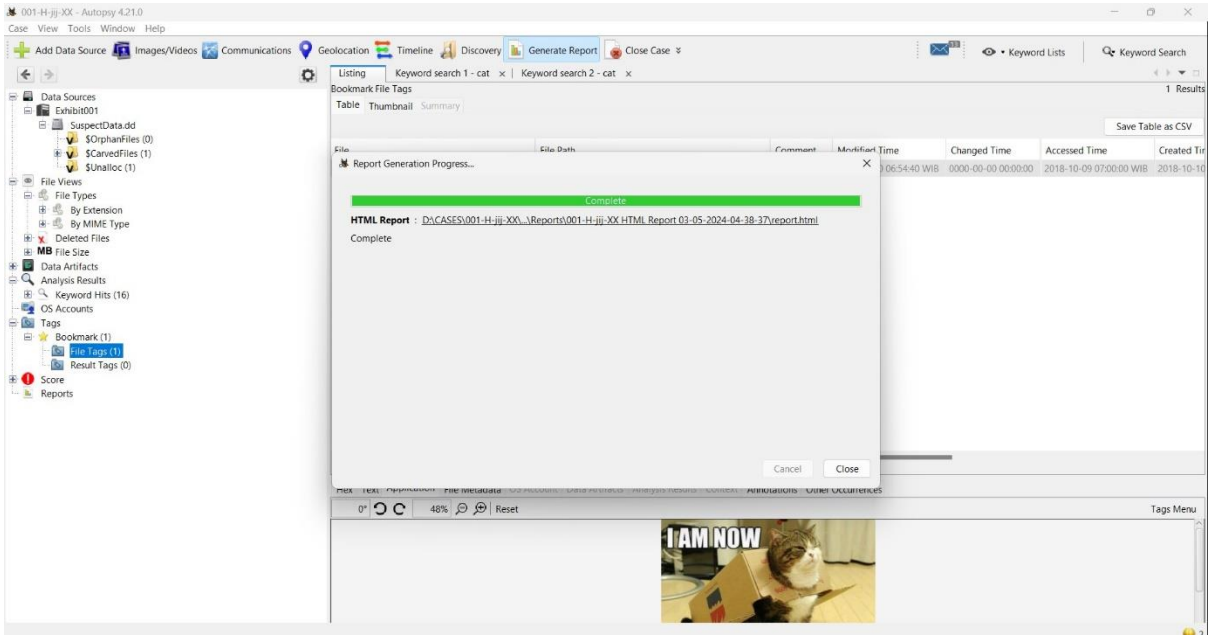
9. 
001-H-jij-XX - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
Exhibit001
SuspectData.dd
$OrphanFiles (0)
$CarvedFiles (1)
$Unalloc (1)
File Views
File Types
By Extension
By MIME Type
Deleted Files
MB File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Deleted Files
2 Results
Table Thumbnail Summary
Save Table as CSV
Type
File System (4)
All (6)

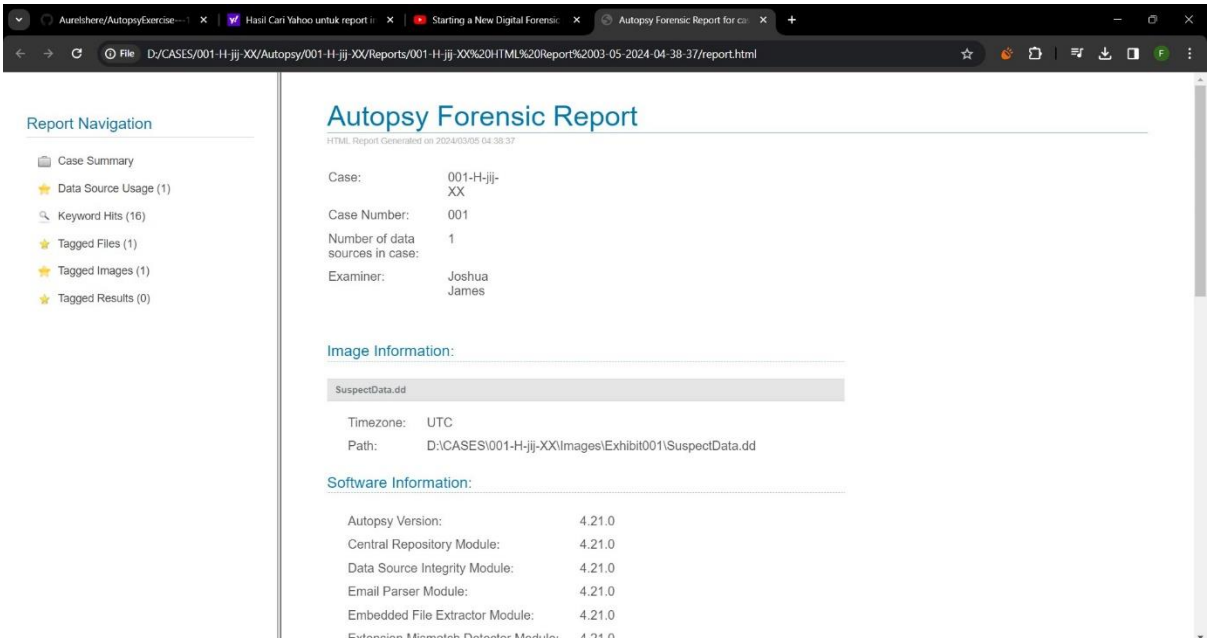
10. 
001-H-jij-XX - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
Exhibit001
SuspectData.dd
$OrphanFiles (0)
$CarvedFiles (1)
$Unalloc (1)
File Views
File Types
By Extension
By MIME Type
Deleted Files
MB File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Data Artifacts
0 Results
Table Thumbnail Summary
Save Table as CSV
Type
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Item: SuspectData.dd
Aggregate Score: Unknown
Analysis Result 1
Score: Unknown
Type: Data Source Usage
Configuration:
Conclusion:

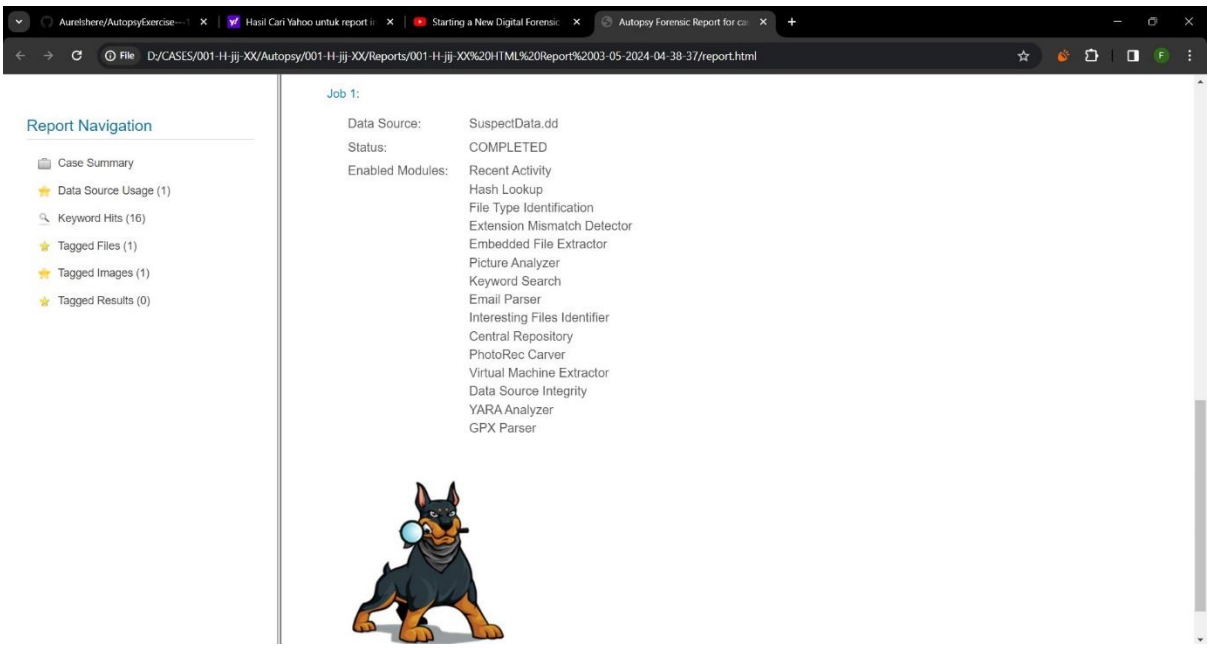
11. 
001-H-jij-XX - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Keyword search 1 - cat
Keyword search 2 - cat
Keyword search
8 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
Keyword Preview
Location
Modified Time
Change Tim
Top-30-Funny-Cat-Memes-Hilarious.jpg
Top-30-Funny-Cat-Memes-Hilarious.jpg-slack
Top-25-Funny-Cat-Memes-8-cats-memes.jpg
Top-25-Funny-Cat-Memes-8-cats-memes.jpg-slack
funny-cat-pictures-027-021.jpg
funny-cat-pictures-027-021.jpg-slack
Funny-Cat-Pictures-cats-935656_500_375.jpg
Funny-Cat-Pictures-cats-935656_500_375.jpg-slack
Data Sources
Exhibit001
SuspectData.dd
$OrphanFiles (0)
$CarvedFiles (1)
$Unalloc (1)
File Views
File Types
By Extension
By MIME Type
Deleted Files
File Size
Data Artifacts
Analysis Results
Keyword Hits (16)
OS Accounts
Tags
Score
Reports
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Reset
Tags Menu
I AM NOW


001-H-jij-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
Listing
Keyword search 1 - cat
Keyword search 2 - cat
Bookmark File Tags
1 Results
Table
Thumbnail
Summary
Save Table as CSV
File
File Path
Comment
Modified Time
Changed Time
Accessed Time
Top-30-Funny-Cat-Memes-Hilarious.jpg
2018-10-10 06:54:40 WIB
0000-00-00 00:00:00
2018-10-09 07:00:00 WIB
Data Sources
Exhibit001
SuspectData.dd
$OrphanFiles (0)
$CarvedFiles (1)
$Unalloc (1)
File Views
File Types
By Extension
By MIME Type
Deleted Files
File Size
Data Artifacts
Analysis Results
Keyword Hits (16)
OS Accounts
Tags
Bookmark (1)
File Tags (1)
Result Tags (0)
Score
Reports
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Reset
Tags Menu
I AM NOW

12. 
001-H-jij-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
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
I AM NOW


001-H-jij-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
Report Generation Progress...
Complete
HTML Report : D:\CASES\001-H-jij-XX\...\Reports\001-H-jij-XX HTML Report 03-05-2024-04-38-37\report.html
Complete
Cancel
Close
I AM NOW


Aurelshere/AutopsyExercise---1
Hasil Cari Yahoo untuk report ir
Starting a New Digital Forensic
Autopsy Forensic Report for ca
File
D:/CASES/001-H-jij-XX/Autopsy/001-H-jij-XX/Reports/001-H-jij-XX%20HTML%20Report%2003-05-2024-04-38-37/report.html
Report Navigation
Case Summary
Data Source Usage (1)
Keyword Hits (16)
Tagged Files (1)
Tagged Images (1)
Tagged Results (0)
Autopsy Forensic Report
HTML Report Generated on 2024/03/05 04:38:37
Case: 001-H-jij-XX
Case Number: 001
Number of data sources in case: 1
Examiner: Joshua James
Image Information:
SuspectData.dd
Timezone: UTC
Path: D:\CASES\001-H-jij-XX\Images\Exhibit001\SuspectData.dd
Software Information:
Autopsy Version: 4.21.0
Central Repository Module: 4.21.0
Data Source Integrity Module: 4.21.0
Email Parser Module: 4.21.0
Embedded File Extractor Module: 4.21.0


Aurelshere/AutopsyExercise---1
Hasil Cari Yahoo untuk report ir
Starting a New Digital Forensic
Autopsy Forensic Report for ca
File
D:/CASES/001-H-jij-XX/Autopsy/001-H-jij-XX/Reports/001-H-jij-XX%20HTML%20Report%2003-05-2024-04-38-37/report.html
Report Navigation
Case Summary
Data Source Usage (1)
Keyword Hits (16)
Tagged Files (1)
Tagged Images (1)
Tagged Results (0)
Job 1:
Data Source: SuspectData.dd
Status: COMPLETED
Enabled Modules: Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
YARA Analyzer
GPX Parser