Software and Cybersecurity (CS/IT 445)

Lab Assignment 4

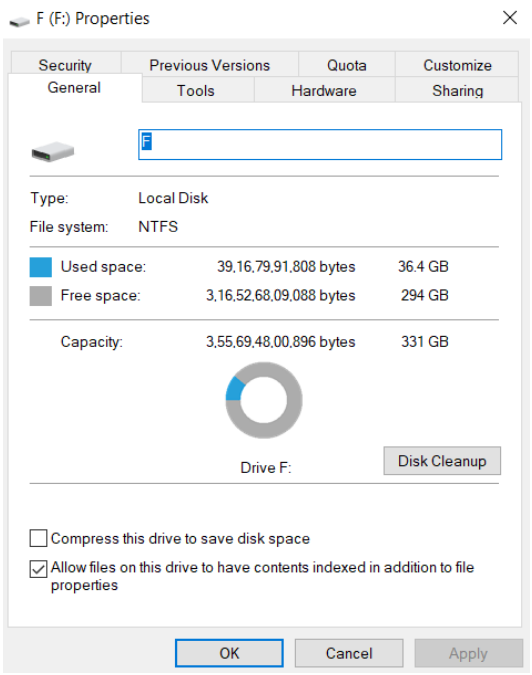
ROLL NO - 202051051

Objective: The objective of this experiment is to introduce students or participants to the fundamental principles and techniques used in a post-mortem examination (autopsy) in a controlled,educational context.

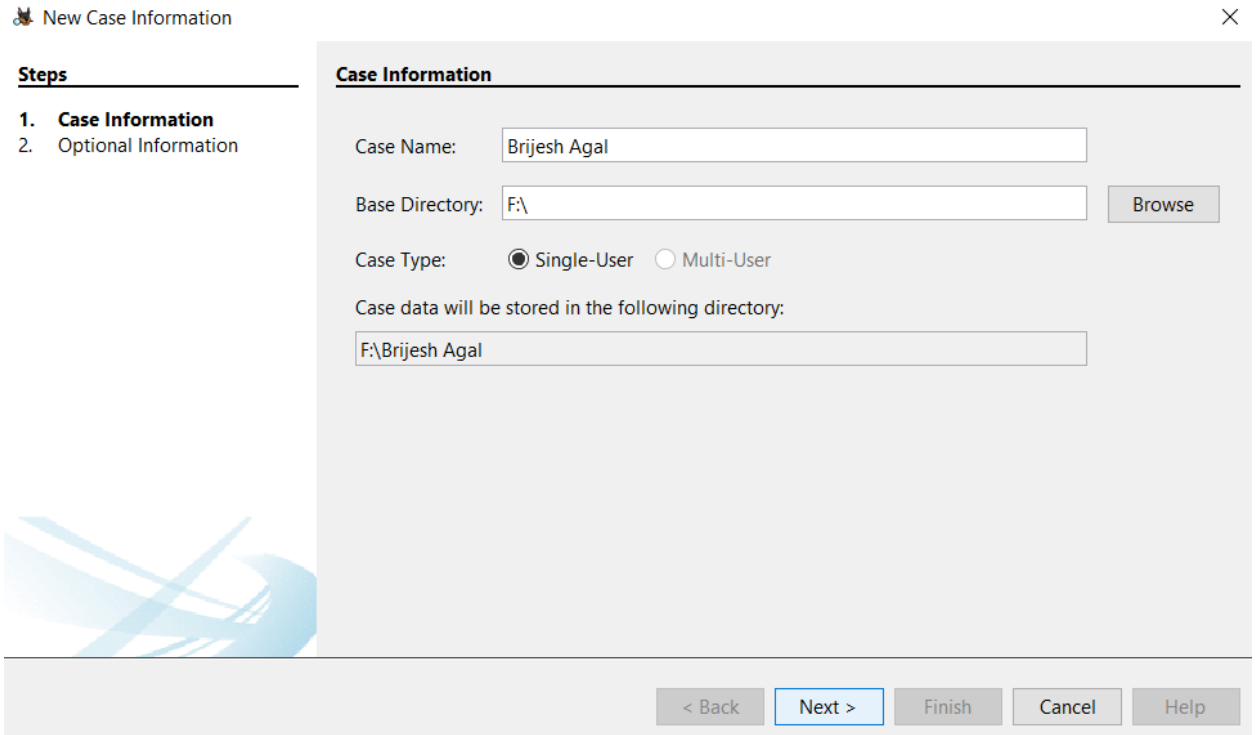
Task 1: Data Acquisition : -

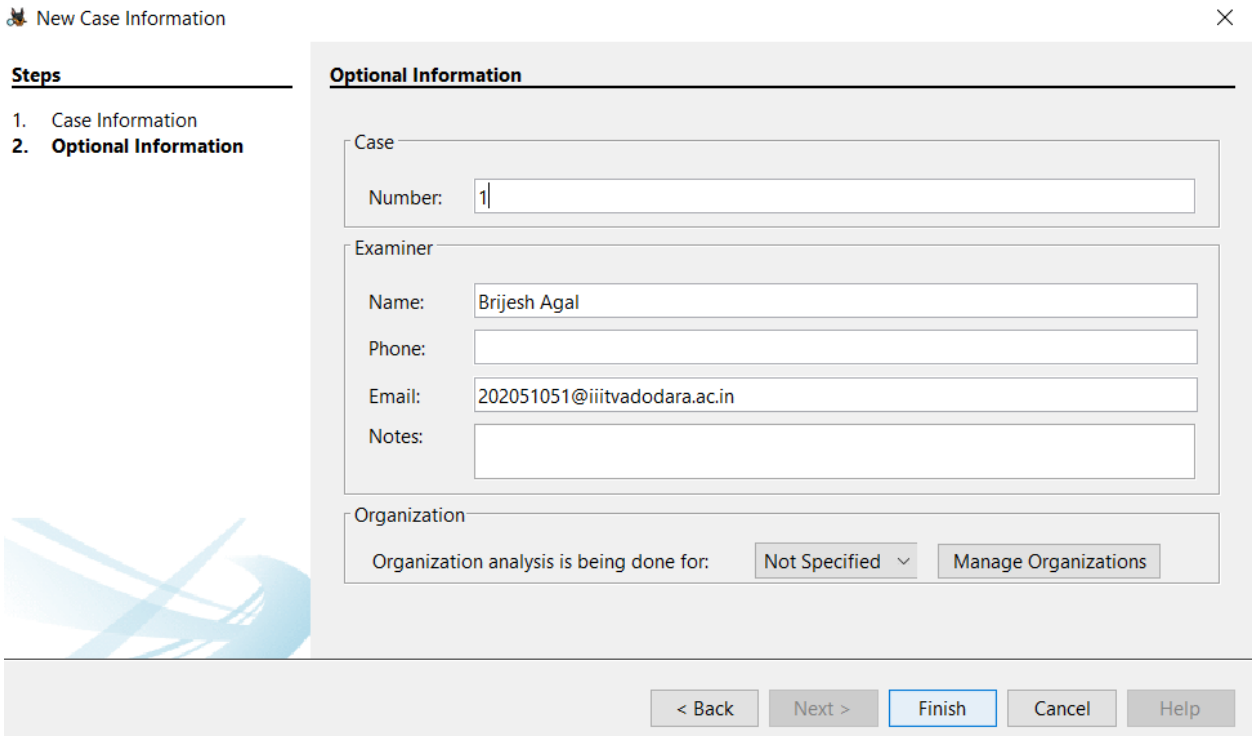
The objective of this task was to acquire a forensic image of a physical hard drive provided for a digital investigation, maintaining the integrity of the original evidence.

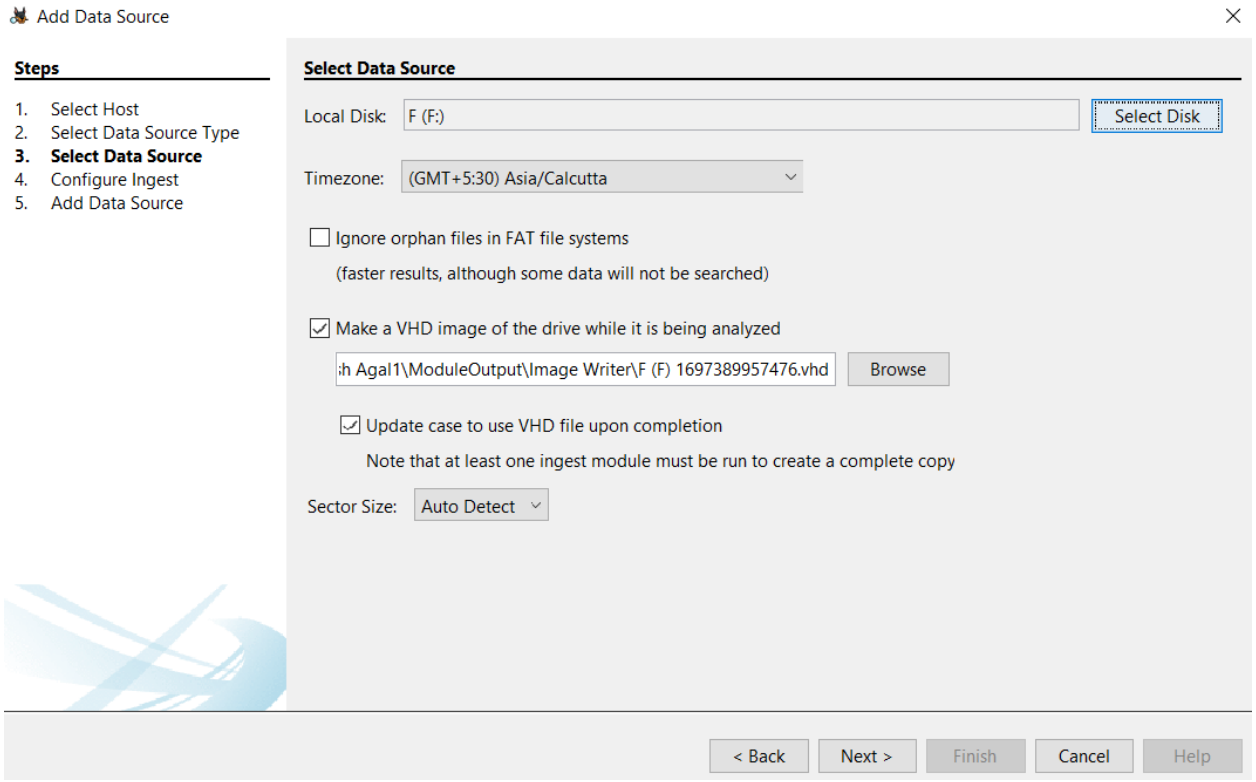
Examine Hard Drive :



1. **Create a new case.**






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
Local Disk: F (F:)
Select Disk
Timezone: (GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
Make a VHD image of the drive while it is being analyzed
:h Agal1\ModuleOutput\Image Writer\F (F) 1697389957476.vhd
Browse
Update case to use VHD file upon completion
Note that at least one ingest module must be run to create a complete copy
Sector Size: Auto Detect
< Back
Next >
Finish
Cancel
Help

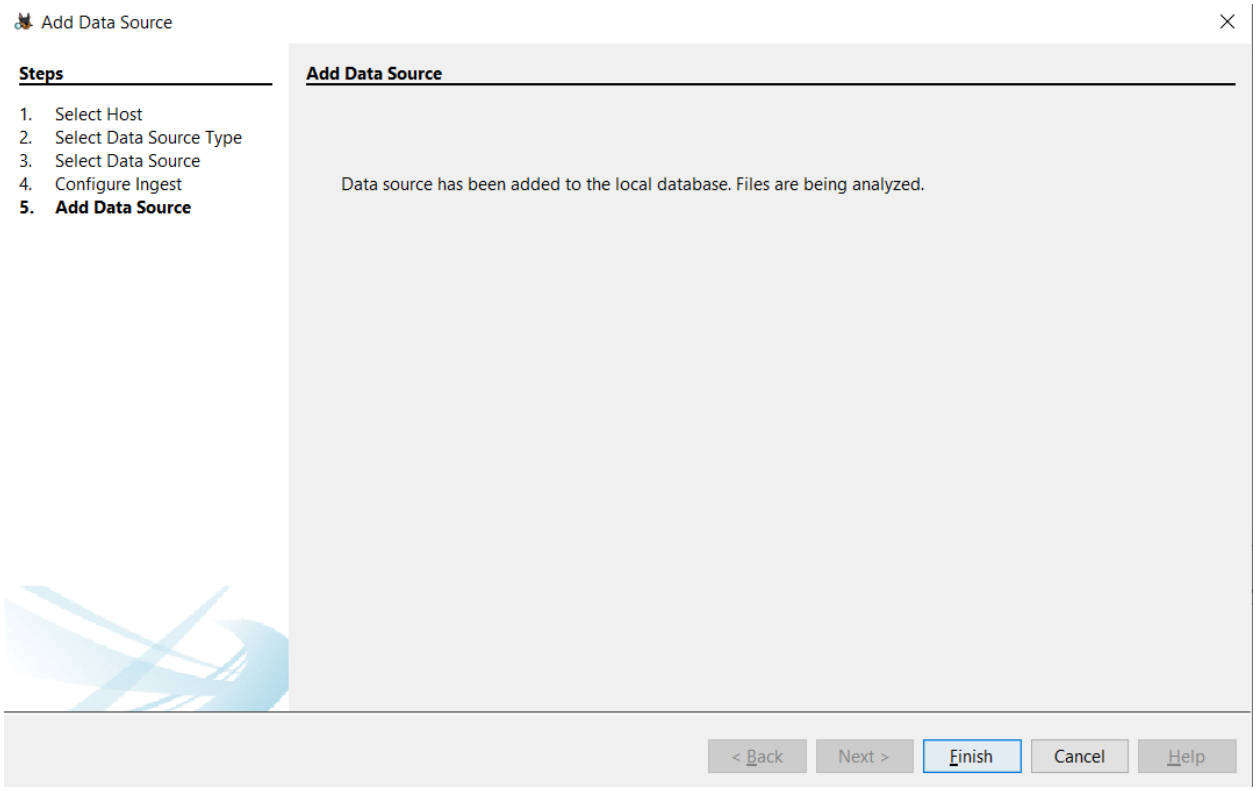
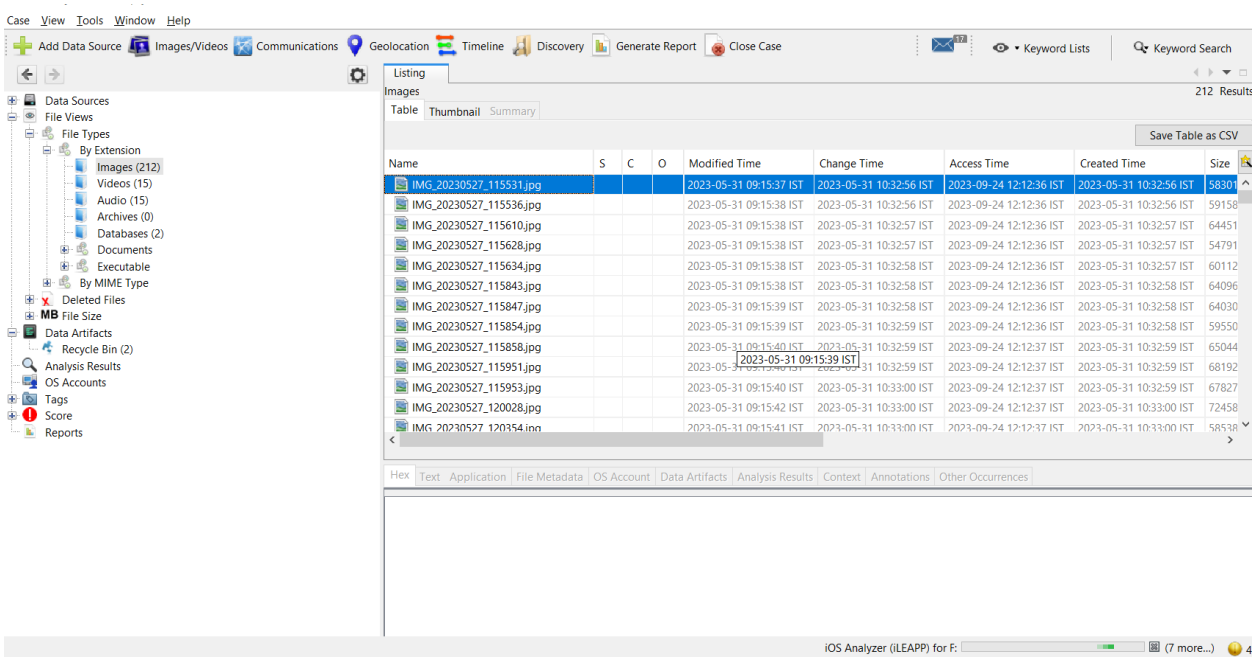
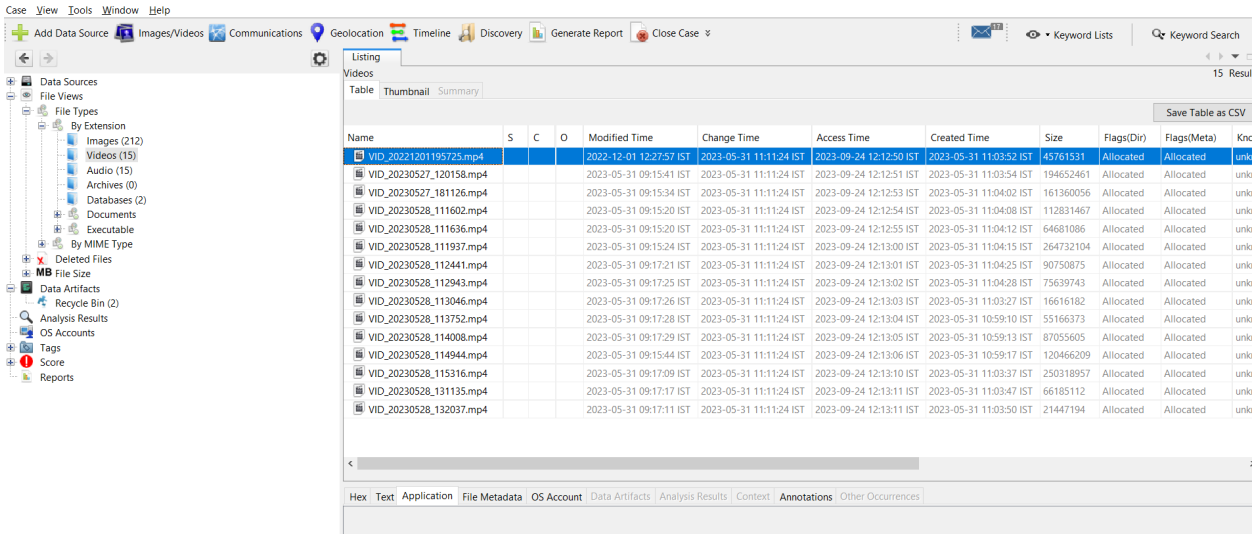

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

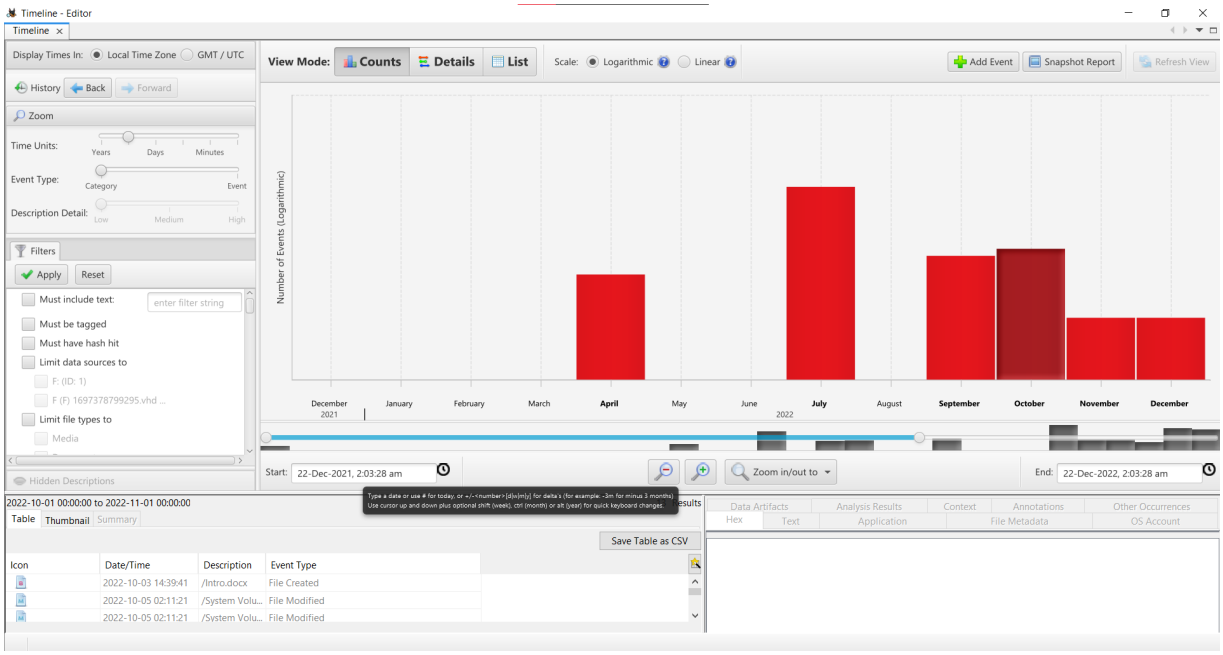
Image :


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
Images (212)
Videos (15)
Audio (15)
Archives (0)
Databases (2)
Documents
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Recycle Bin (2)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Images
212 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
IMG_20230527_115531.jpg
IMG_20230527_115536.jpg
IMG_20230527_115610.jpg
IMG_20230527_115628.jpg
IMG_20230527_115634.jpg
IMG_20230527_115843.jpg
IMG_20230527_115847.jpg
IMG_20230527_115854.jpg
IMG_20230527_115858.jpg
IMG_20230527_115951.jpg
IMG_20230527_115953.jpg
IMG_20230527_120028.jpg
2023-05-31 09:15:39 IST
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
iOS Analyzer (iLEAPP) for F:
(7 more...)

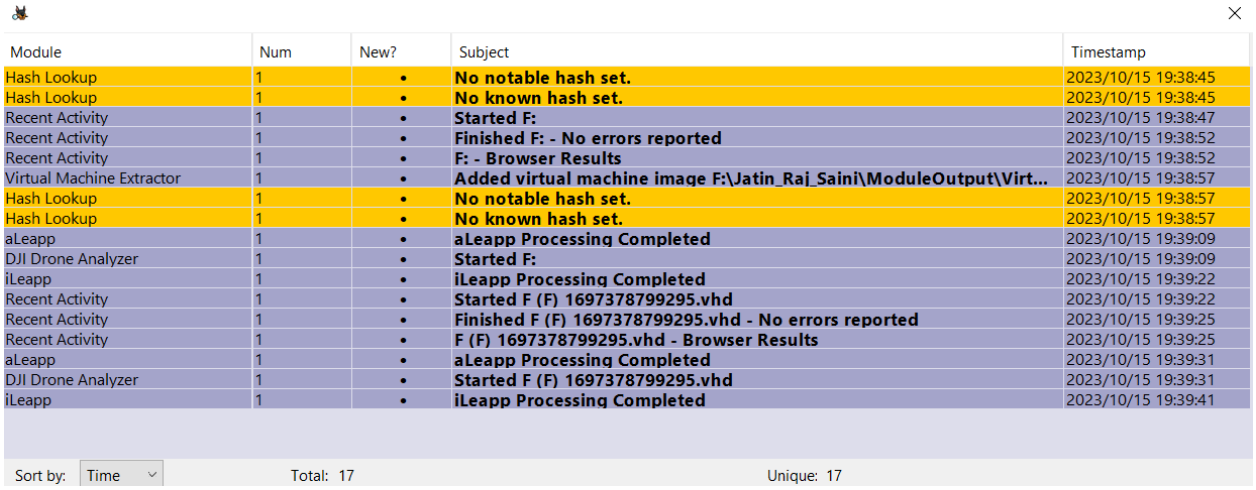
Video :


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
Images (212)
Videos (15)
Audio (15)
Archives (0)
Databases (2)
Documents
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Recycle Bin (2)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Videos
15 Resul
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
VID_20221201195725.mp4
VID_20230527_120158.mp4
VID_20230527_181126.mp4
VID_20230528_111602.mp4
VID_20230528_111636.mp4
VID_20230528_111937.mp4
VID_20230528_112441.mp4
VID_20230528_112943.mp4
VID_20230528_113046.mp4
VID_20230528_113752.mp4
VID_20230528_114008.mp4
VID_20230528_114944.mp4
VID_20230528_115316.mp4
VID_20230528_131135.mp4
VID_20230528_132037.mp4
Allocated
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

TimeLine :

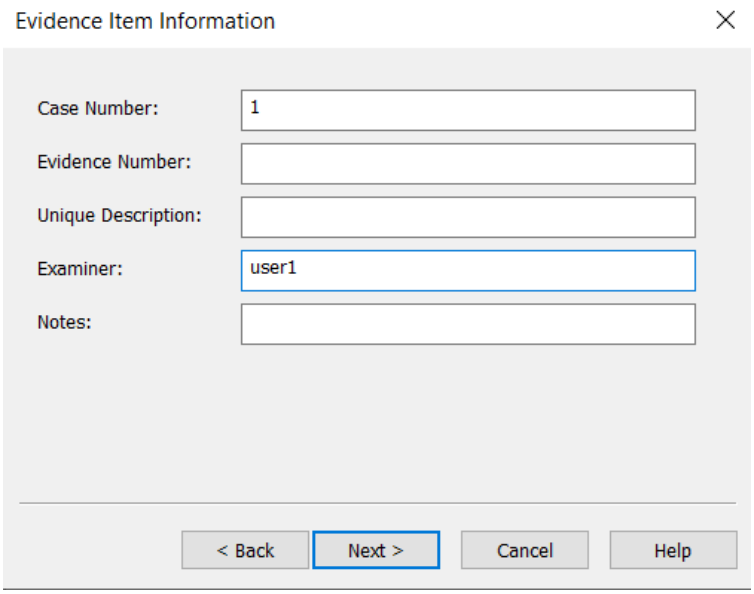


Details of the forensic imaging process after Image Integrity:

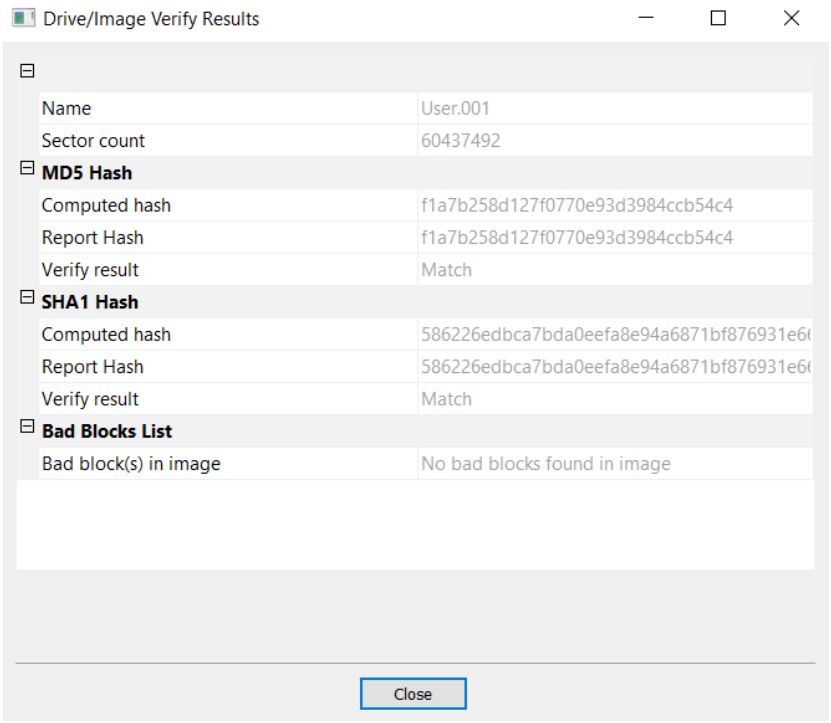


Module	Num	New?	Subject	Timestamp
Hash Lookup	1	•	No notable hash set.	2023/10/15 19:38:45
Hash Lookup	1	•	No known hash set.	2023/10/15 19:38:45
Recent Activity	1	•	Started F:	2023/10/15 19:38:47
Recent Activity	1	•	Finished F: - No errors reported	2023/10/15 19:38:52
Recent Activity	1	•	F: - Browser Results	2023/10/15 19:38:52
Virtual Machine Extractor	1	•	Added virtual machine image F:\Jatin_Raj_Saini\ModuleOutput\Virt...	2023/10/15 19:38:57
Hash Lookup	1	•	No notable hash set.	2023/10/15 19:38:57
Hash Lookup	1	•	No known hash set.	2023/10/15 19:38:57
aLeapp	1	•	aLeapp Processing Completed	2023/10/15 19:39:09
DJI Drone Analyzer	1	•	Started F:	2023/10/15 19:39:09
iLeapp	1	•	iLeapp Processing Completed	2023/10/15 19:39:22
Recent Activity	1	•	Started F (F) 1697378799295.vhd	2023/10/15 19:39:22
Recent Activity	1	•	Finished F (F) 1697378799295.vhd - No errors reported	2023/10/15 19:39:25
Recent Activity	1	•	F (F) 1697378799295.vhd - Browser Results	2023/10/15 19:39:25
aLeapp	1	•	aLeapp Processing Completed	2023/10/15 19:39:31
DJI Drone Analyzer	1	•	Started F (F) 1697378799295.vhd	2023/10/15 19:39:31
iLeapp	1	•	iLeapp Processing Completed	2023/10/15 19:39:41

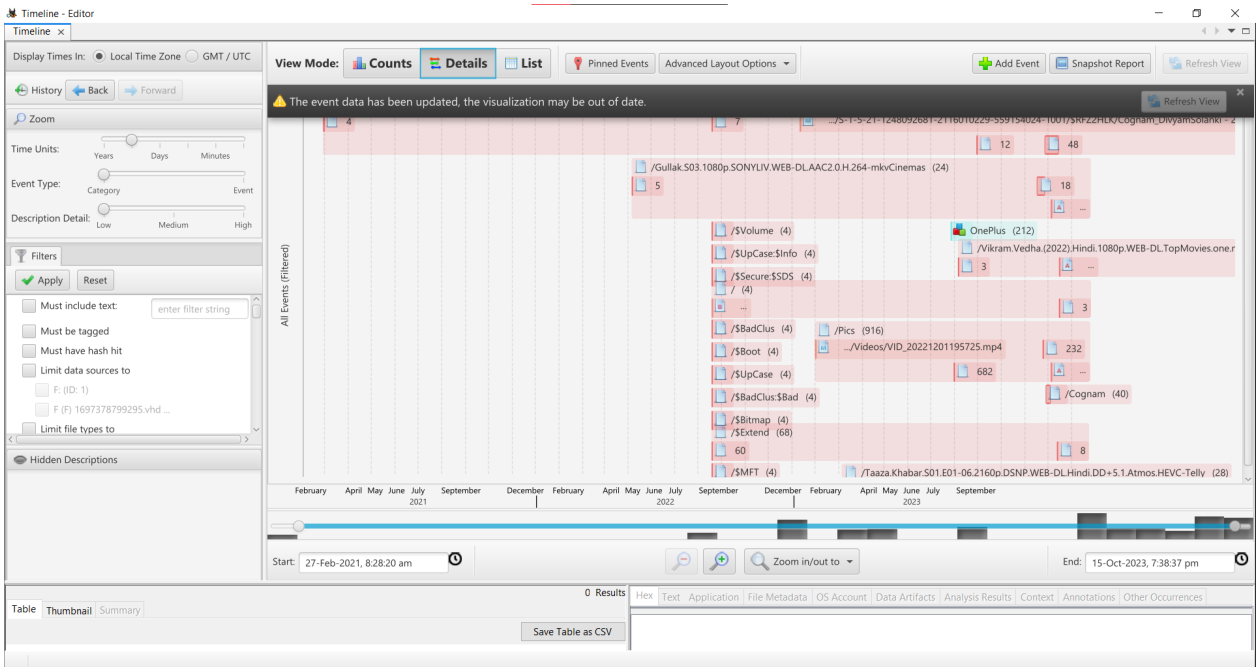
Sort by: Time Total: 17 Unique: 17



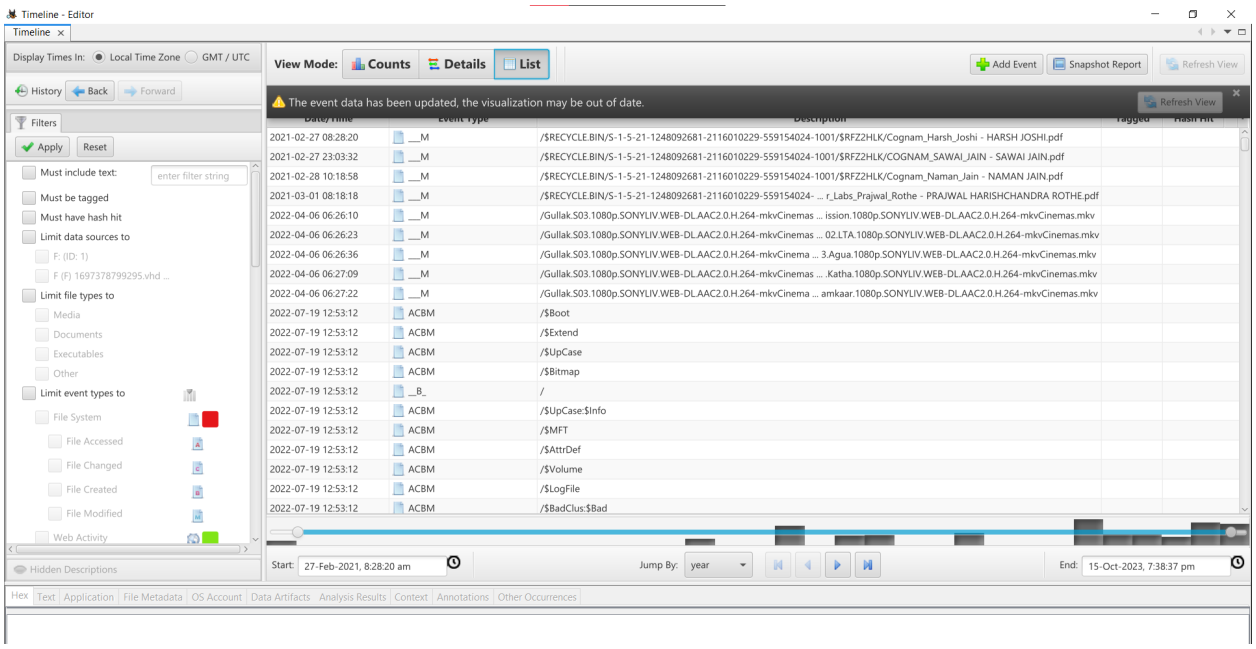
To affirm the integrity of the acquired image, a MD5 hash value was computed for both the original hard drive and the image.



Details :



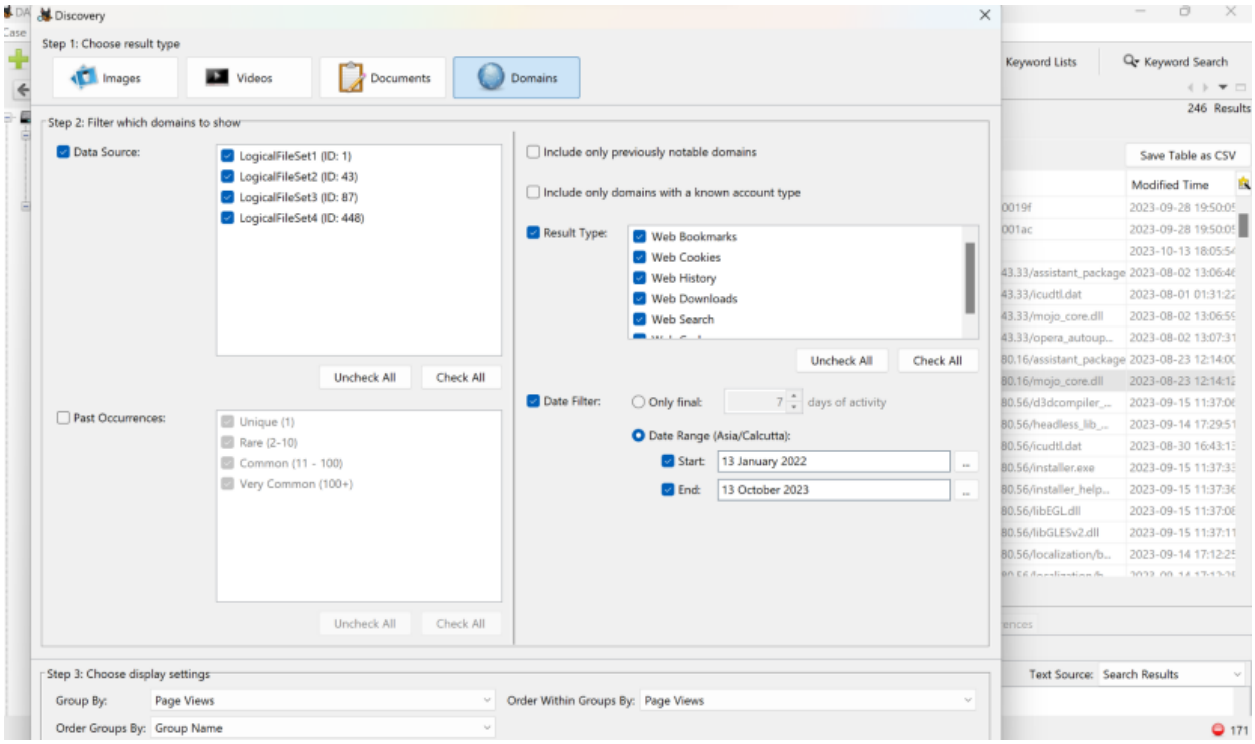
List:



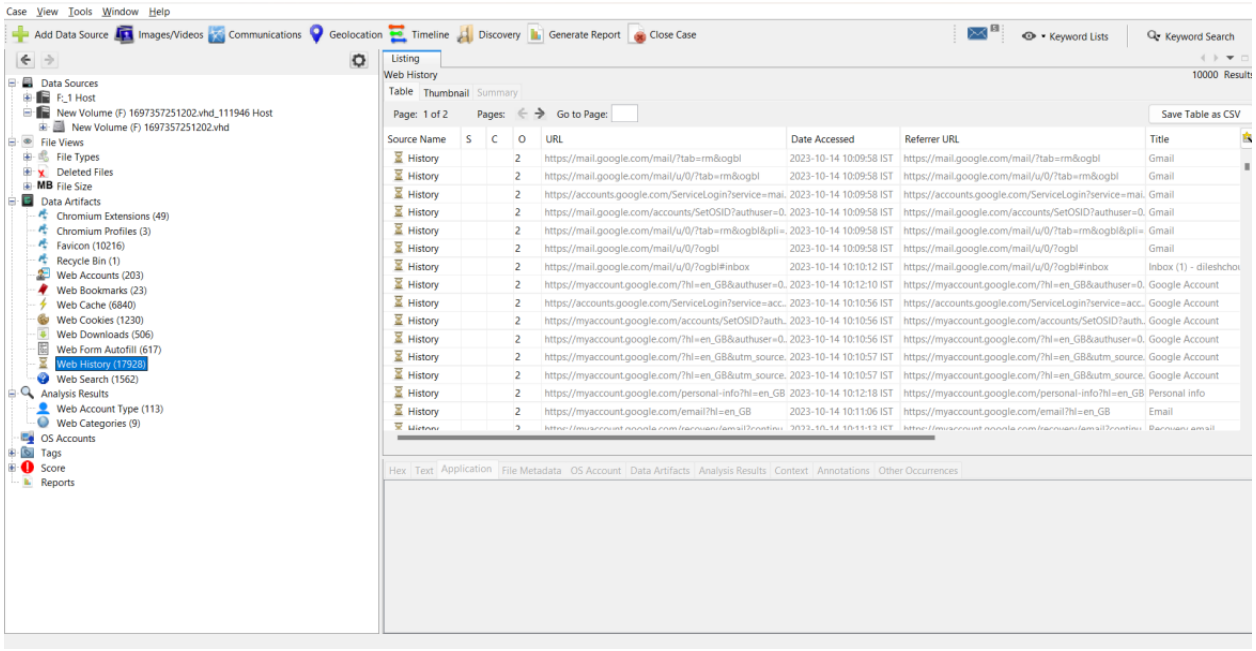
TASK 2- File Analysis :

The purpose of this task was to analyse the file system of a suspect's computer using the acquired forensic image to retrieve specific pieces of information relevant to the Investigation.

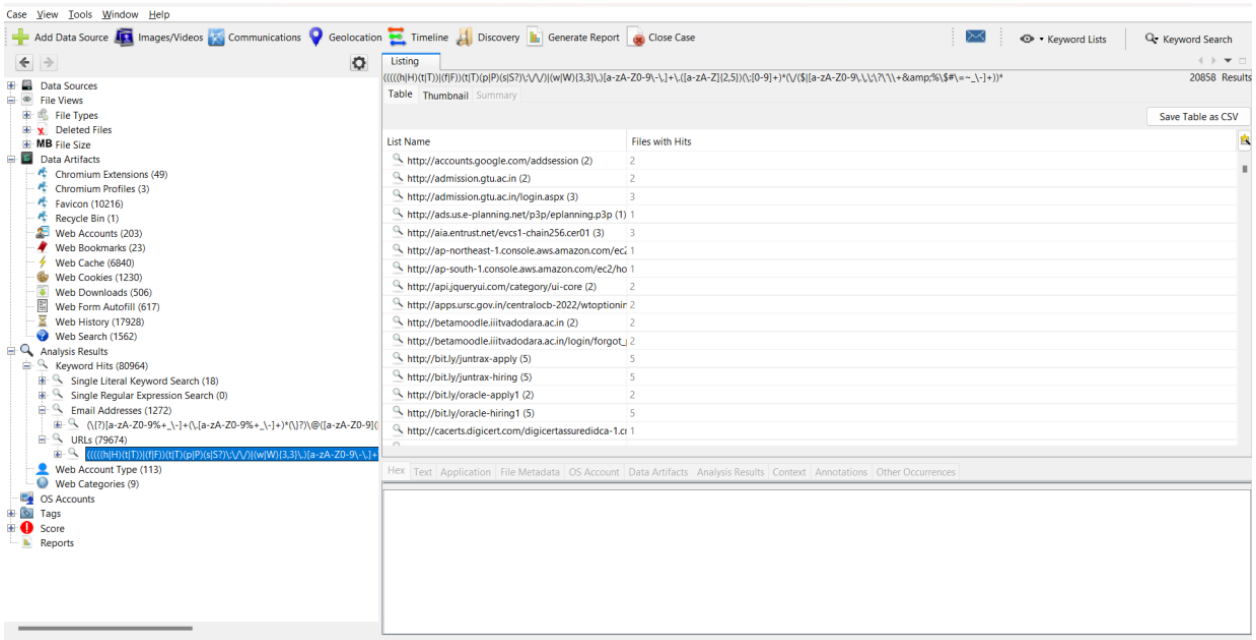
1. Analyse data files

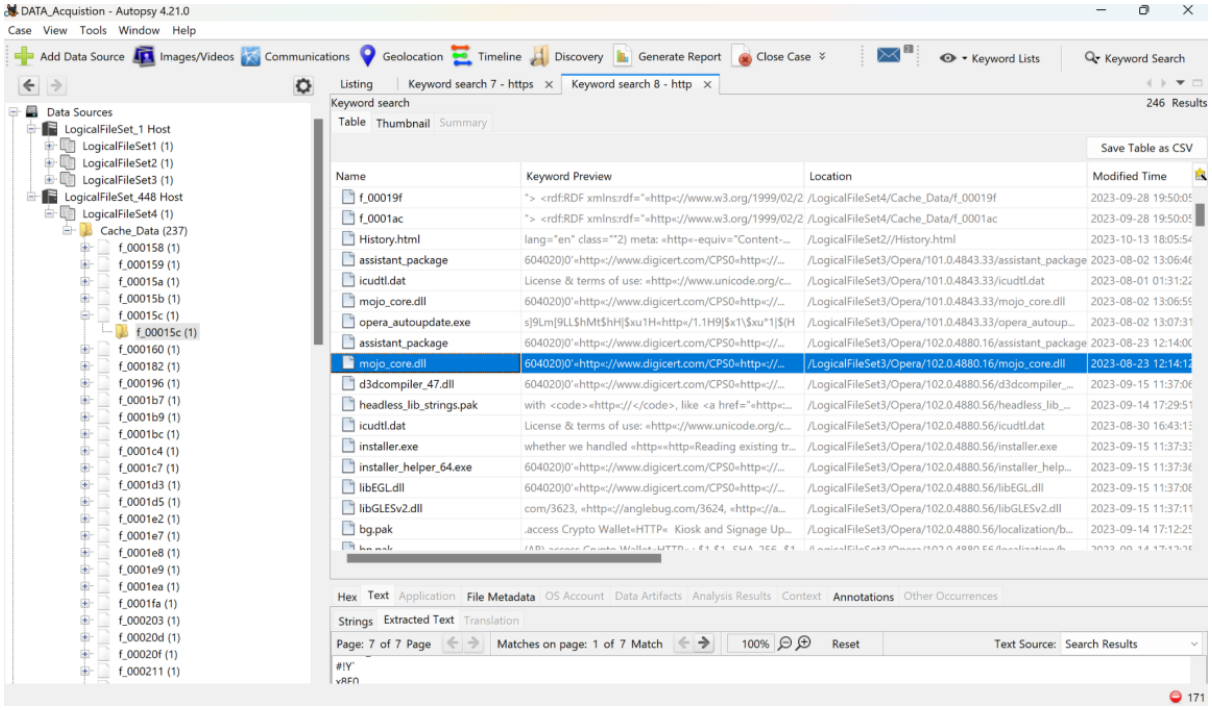


2. Web Browser History

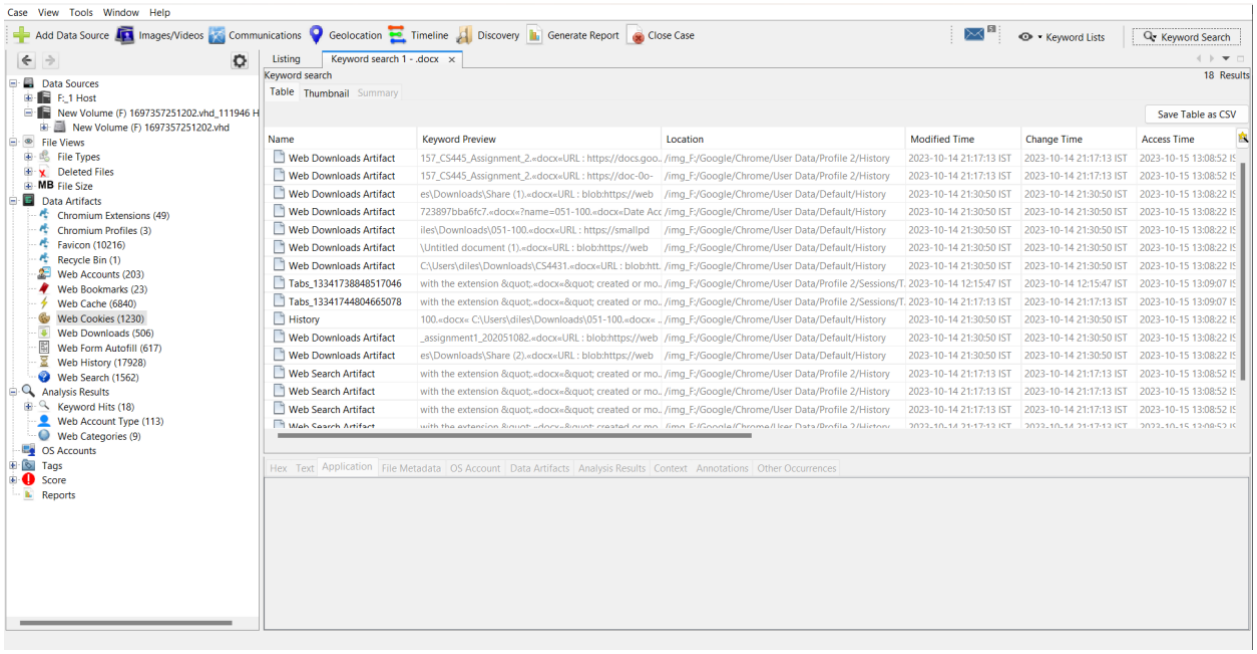


3. Url searches

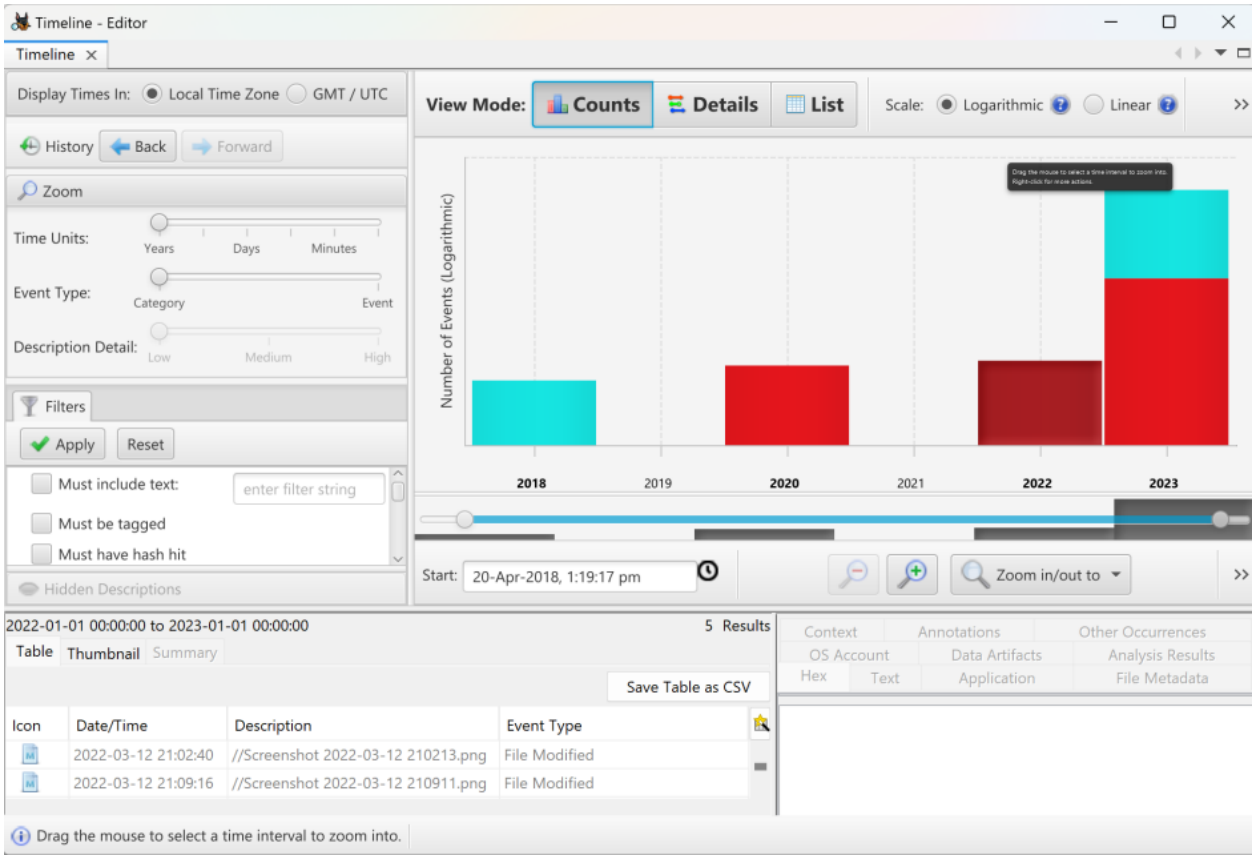


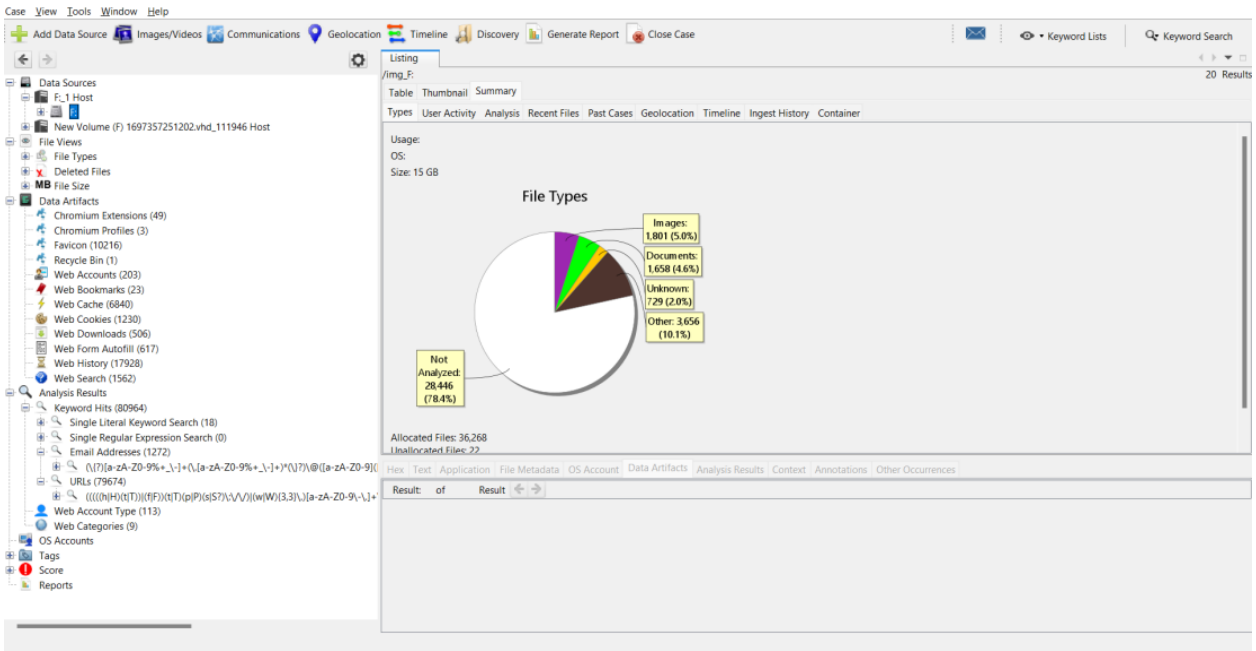

DATA_Acquistion - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search
Listing Keyword search 7 - https Keyword search 8 - http
Keyword search 246 Results
Table Thumbnail Summary
Save Table as CSV
Name Keyword Preview Location Modified Time
Data Sources
LogicalFileSet_1 Host
LogicalFileSet1 (1)
LogicalFileSet2 (1)
LogicalFileSet3 (1)
LogicalFileSet_448 Host
LogicalFileSet4 (1)
Cache_Data (237)
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 7 of 7 Page Matches on page: 1 of 7 Match 100% Reset Text Source: Search Results

4. Keyword :

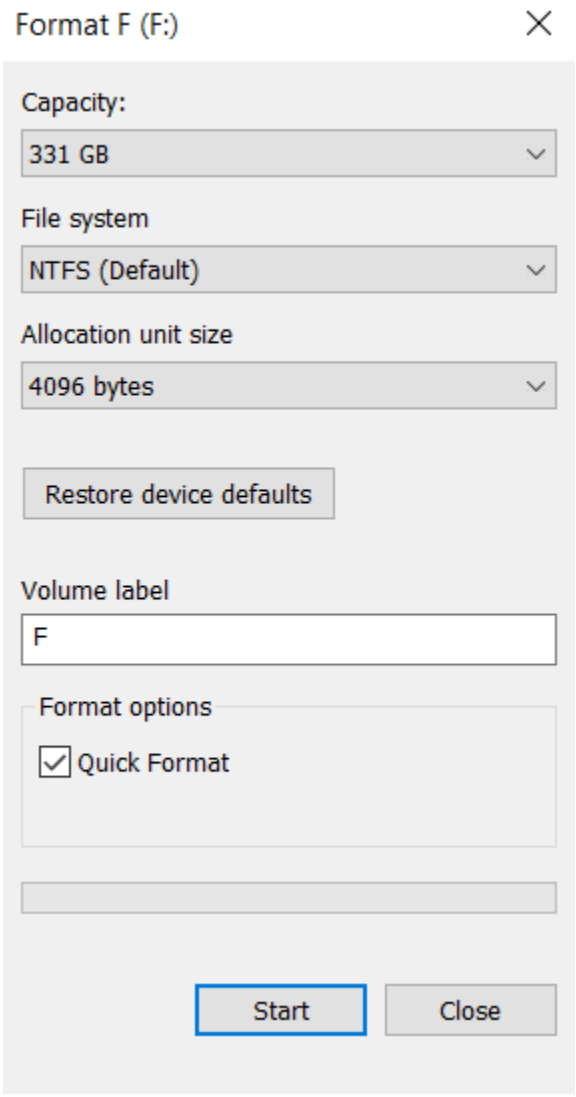

Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search
Listing Keyword search 1 - .docx
Keyword search 18 Results
Table Thumbnail Summary
Save Table as CSV
Name Keyword Preview Location Modified Time Change Time Access Time
Data Sources
File Views
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

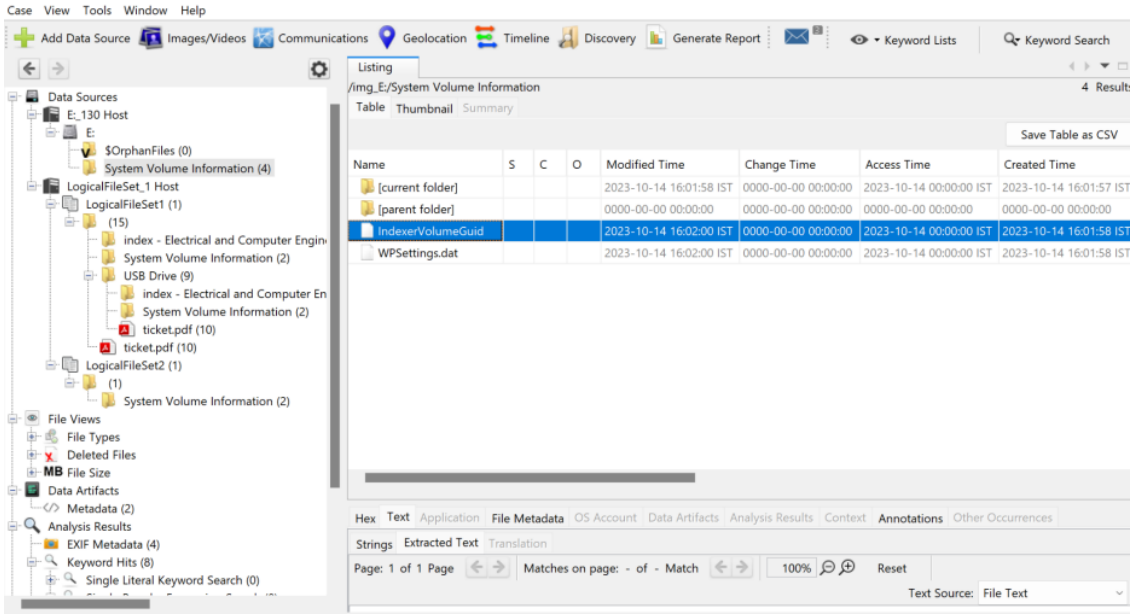
TimeLine :

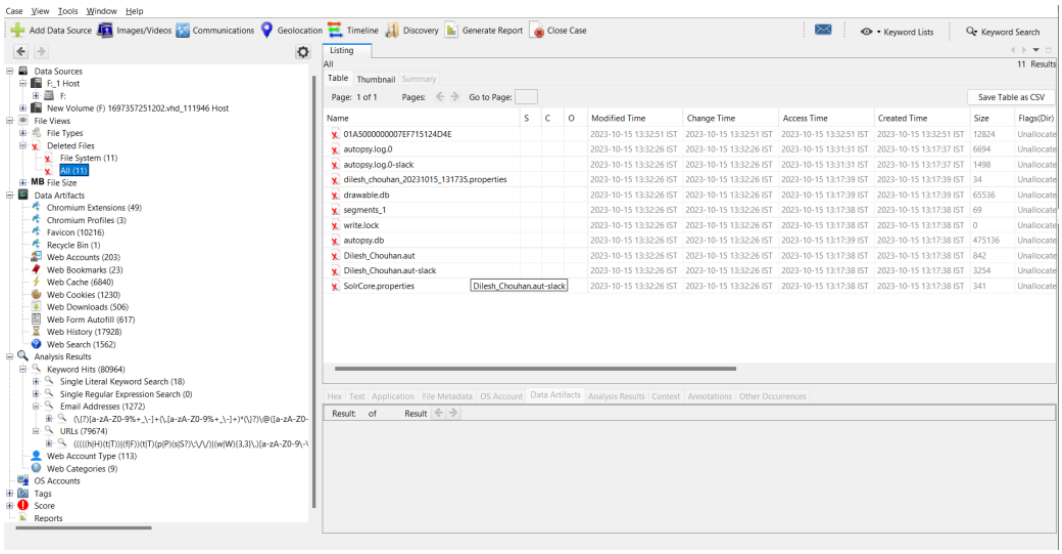

Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail: Low Medium High
Filters
Apply Reset
Must include text: enter filter string
Must be tagged
Must have hash hit
Hidden Descriptions
View Mode: Counts Details List
Scale: Logarithmic Linear
Number of Events (Logarithmic)
2018 2019 2020 2021 2022 2023
Start: 20-Apr-2018, 1:19:17 pm
Zoom in/out to
2022-01-01 00:00:00 to 2023-01-01 00:00:00
5 Results
Table Thumbnail Summary
Save Table as CSV
Icon Date/Time Description Event Type
2022-03-12 21:02:40 //Screenshot 2022-03-12 210213.png File Modified
2022-03-12 21:09:16 //Screenshot 2022-03-12 210911.png File Modified
Context Annotations Other Occurrences
OS Account Data Artifacts Analysis Results
Hex Text Application File Metadata
Drag the mouse to select a time interval to zoom into.

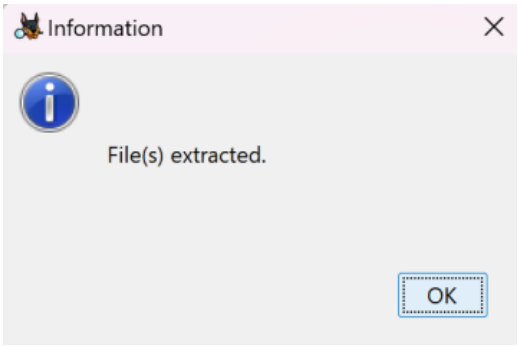

Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
File Views
Data Artifacts
Analysis Results
Tags
Score
Reports
Listing
Table Thumbnail Summary
Types User Activity Analysis Recent Files Past Cases Geolocation Timeline Ingest History Container
Usage:
OS:
Size: 15 GB
File Types
Images: 1,801 (5.0%)
Documents: 1,658 (4.6%)
Unknown: 729 (2.0%)
Other: 3,656 (10.1%)
Not Analyzed: 28,446 (78.4%)
Allocated Files: 36,268
Unallocated Files: 22
20 Results

Recovery of data :




Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Keyword Lists
Keyword Search
Listing
/img_E:/System Volume Information
4 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
[current folder]
2023-10-14 16:01:58 IST
0000-00-00 00:00:00
2023-10-14 00:00:00 IST
2023-10-14 16:01:57 IST
[parent folder]
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
IndexerVolumeGuid
2023-10-14 16:02:00 IST
0000-00-00 00:00:00
2023-10-14 00:00:00 IST
2023-10-14 16:01:58 IST
WPSettings.dat
2023-10-14 16:02:00 IST
0000-00-00 00:00:00
2023-10-14 00:00:00 IST
2023-10-14 16:01:58 IST
Data Sources
E:_130 Host
E:
$OrphanFiles (0)
System Volume Information (4)
LogicalFileSet_1 Host
LogicalFileSet1 (1)
(15)
index - Electrical and Computer Engin
System Volume Information (2)
USB Drive (9)
index - Electrical and Computer En
System Volume Information (2)
ticket.pdf (10)
ticket.pdf (10)
LogicalFileSet2 (1)
(1)
System Volume Information (2)
File Views
File Types
Deleted Files
File Size
Data Artifacts
Metadata (2)
Analysis Results
EXIF Metadata (4)
Keyword Hits (8)
Single Literal Keyword Search (0)
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

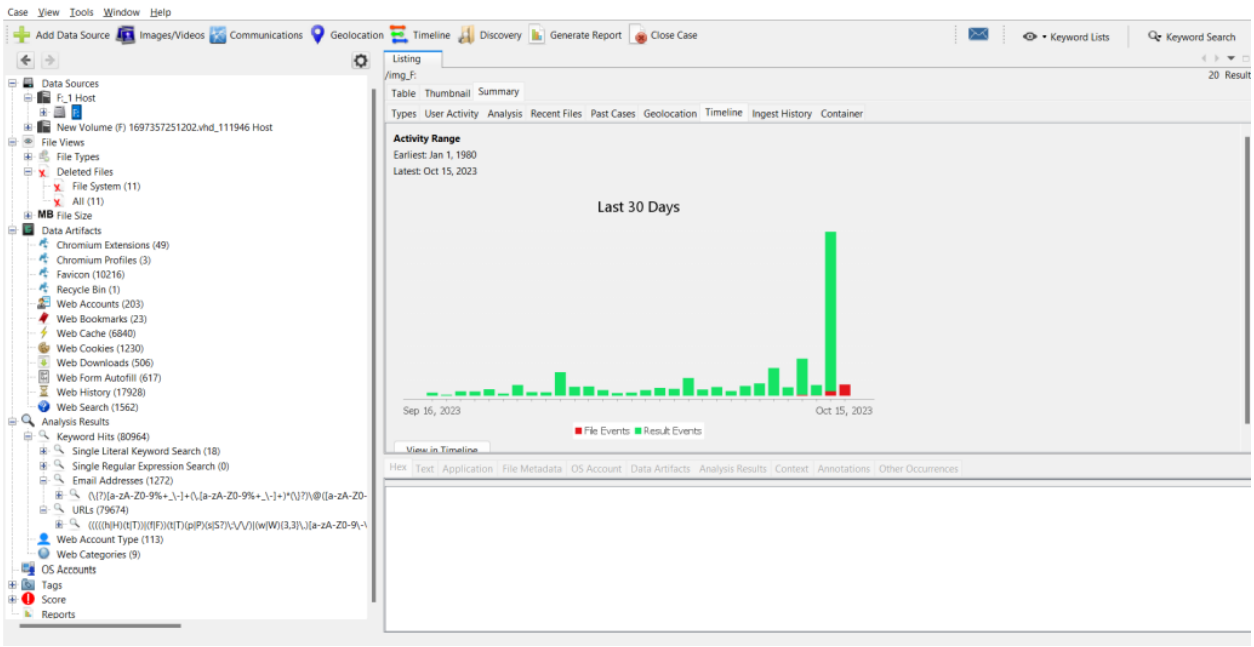

Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
All
11 Results
Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
01A5000000007EF715124D4E
autopsy.log.0
autopsy.log.0-slack
dilesh_chouhan_20231015_131735.properties
drawable.db
segments_1
write.lock
autopsy.db
Dilesh_Chouhan.aut
Dilesh_Chouhan.aut-slack
SolrCore.properties
Dilesh_Chouhan.aut-slack
Data Sources
F:_1 Host
New Volume (F) 1697357251202.vhd_111946 Host
File Views
File Types
Deleted Files
File System (11)
All (11)
File Size
Data Artifacts
Chromium Extensions (49)
Chromium Profiles (3)
Favicon (10216)
Recycle Bin (1)
Web Accounts (203)
Web Bookmarks (23)
Web Cache (6840)
Web Cookies (1230)
Web Downloads (506)
Web Form Autofill (617)
Web History (17928)
Web Search (1562)
Analysis Results
Keyword Hits (80964)
Single Literal Keyword Search (18)
Single Regular Expression Search (0)
Email Addresses (1272)
URLs (79674)
Web Account Type (113)
Web Categories (9)
OS Accounts
Tags
Score
Reports
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: of
Result


Information
File(s) extracted.
OK

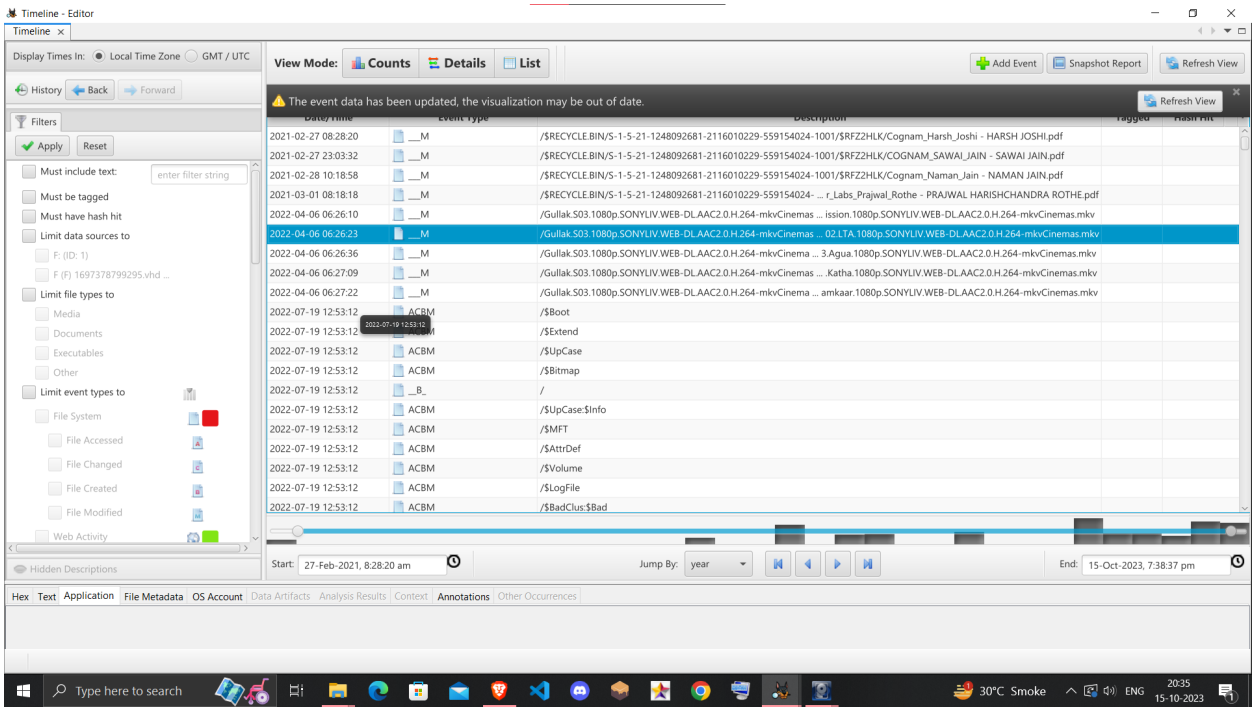
TASK 3-

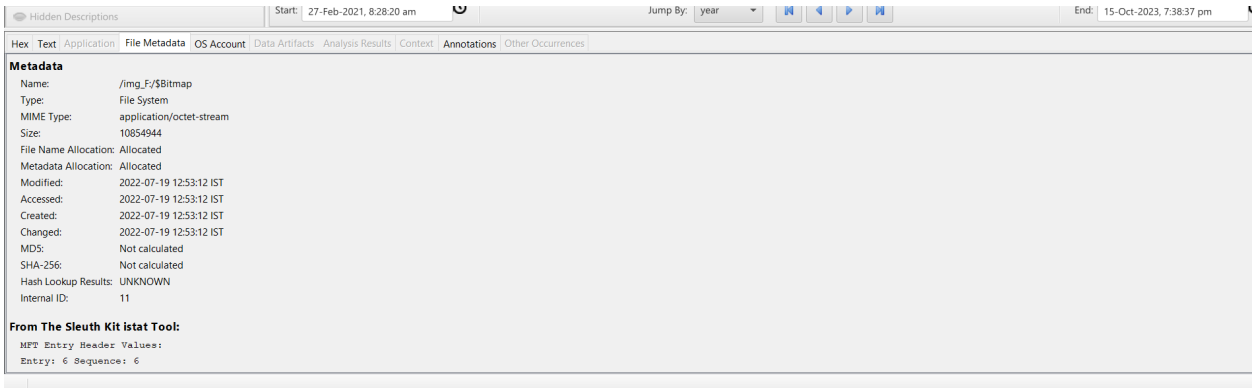
The primary aim of this task was to create a chronological timeline of events related to the usage and activity on the suspect's computer. This timeline would offer a chronological overview of actions and events on the system.

Generate Timeline :




Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail: Low Medium High
Filters
Apply Reset
Must include text: enter filter string
Must be tagged
Must have hash hit
Limit data sources to
F: (ID: 1)
F (F) 1697378799295.vhd ...
Limit file types to
Hidden Descriptions
View Mode: Counts Details List
Pinned Events
Advanced Layout Options
Add Event
Snapshot Report
Refresh View
The event data has been updated, the visualization may be out of date.
Refresh View
All Events (Filtered)
Document Last Saved (3)
Document Created (3)
OnePlus (212)
/Cognam (40)
/Vikram.Vedha.(2022).Hindi.1080p.WEB-DL.TopMovies.one.r
/Gullak.S03.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas (24)
/$UpCase:$Info (4)
/Jatin_Raj_Saini (100)
/$Secure:$SDS (4)
/ (4)
/$BadClus (4)
/Pics (916)
.../Videos/VID_20221201195725.mp4
/$Boot (4)
/$UpCase (4)
February April May June July September December February April May June July September December February April May June July September
2021
2022
2023
Start: 27-Feb-2021, 8:28:20 am
Zoom in/out to
End: 15-Oct-2023, 7:38:37 pm
0 Results
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences


Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
History Back Forward
Filters
Apply Reset
Must include text: enter filter string
Must be tagged
Must have hash hit
Limit data sources to
F: (ID: 1)
F (F) 1697378799295.vhd ...
Limit file types to
Media
Documents
Executables
Other
Limit event types to
File System
File Accessed
File Changed
File Created
File Modified
Web Activity
Hidden Descriptions
View Mode: Counts Details List
Add Event
Snapshot Report
Refresh View
The event data has been updated, the visualization may be out of date.
Refresh View
2021-02-27 08:28:20 __M /$RECYCLE.BIN/S-1-5-21-1248092681-2116010229-559154024-1001/$RFZ2HLK/Cognam_Harsh_Joshi - HARSH JOSHI.pdf
2021-02-27 23:03:32 __M /$RECYCLE.BIN/S-1-5-21-1248092681-2116010229-559154024-1001/$RFZ2HLK/COGNAM_SAWAI_JAIN - SAWAI JAIN.pdf
2021-02-28 10:18:58 __M /$RECYCLE.BIN/S-1-5-21-1248092681-2116010229-559154024-1001/$RFZ2HLK/Cognam_Naman_Jain - NAMAN JAIN.pdf
2021-03-01 08:18:18 __M /$RECYCLE.BIN/S-1-5-21-1248092681-2116010229-559154024- ... r_Labs_Prajwal_Rothe - PRAJWAL HARISHCHANDRA ROTHE.pdf
2022-04-06 06:26:10 __M /Gullak.S03.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas ... ission.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas.mkv
2022-04-06 06:26:23 __M /Gullak.S03.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas ... 02.LTA.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas.mkv
2022-04-06 06:26:36 __M /Gullak.S03.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinema ... 3.Agua.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas.mkv
2022-04-06 06:27:09 __M /Gullak.S03.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas Katha.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas.mkv
2022-04-06 06:27:22 __M /Gullak.S03.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinema ... amkaar.1080p.SONYLIV.WEB-DL.AAC2.0.H.264-mkvCinemas.mkv
2022-07-19 12:53:12 ACBM /$Boot
2022-07-19 12:53:12 ACBM /$Extend
2022-07-19 12:53:12 ACBM /$UpCase
2022-07-19 12:53:12 ACBM /$Bitmap
2022-07-19 12:53:12 _B_ /
2022-07-19 12:53:12 ACBM /$UpCase:$Info
2022-07-19 12:53:12 ACBM /$MFT
2022-07-19 12:53:12 ACBM /$AttrDef
2022-07-19 12:53:12 ACBM /$Volume
2022-07-19 12:53:12 ACBM /$LogFile
2022-07-19 12:53:12 ACBM /$BadClus:$Bad
Start: 27-Feb-2021, 8:28:20 am
Jump By: year
End: 15-Oct-2023, 7:38:37 pm
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Type here to search
30°C Smoke
ENG
20:35
15-10-2023


Hidden Descriptions
Start: 27-Feb-2021, 8:28:20 am
Jump By: year
End: 15-Oct-2023, 7:38:37 pm
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Metadata
Name: /img_F:/$Bitmap
Type: File System
MIME Type: application/octet-stream
Size: 10854944
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-07-19 12:53:12 IST
Accessed: 2022-07-19 12:53:12 IST
Created: 2022-07-19 12:53:12 IST
Changed: 2022-07-19 12:53:12 IST
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 11
From The Sleuth Kit istat Tool:
MFT Entry Header Values:
Entry: 6 Sequence: 6