

Software and Cybersecurity (CS/IT 445)

Lab Assignment 4

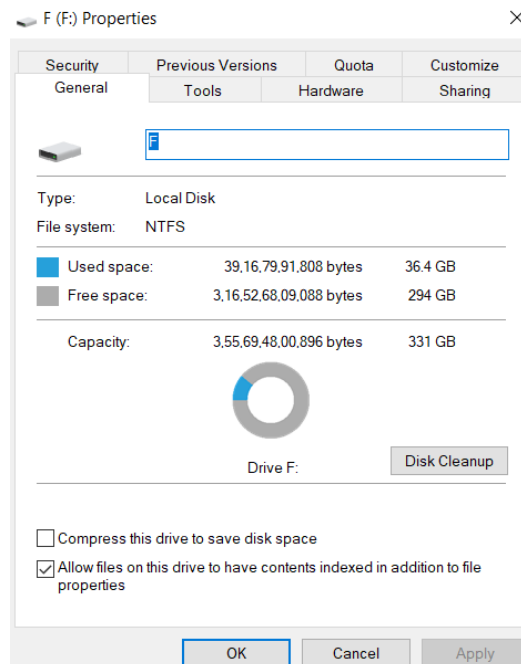
ROLL NO - 202051051

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.

New Case Information ×

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

New Case Information ×

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for:

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

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

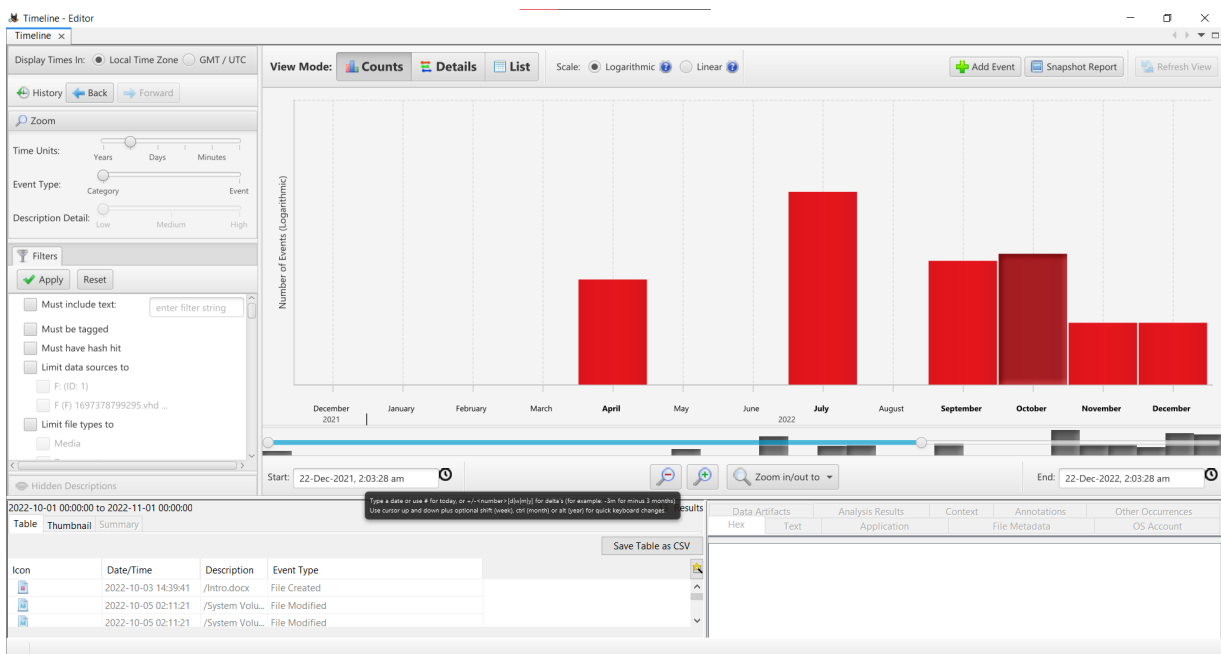
Next >

Finish

Cancel

Help

TimeLine :



Details of the forensic imaging process after Image Integrity:

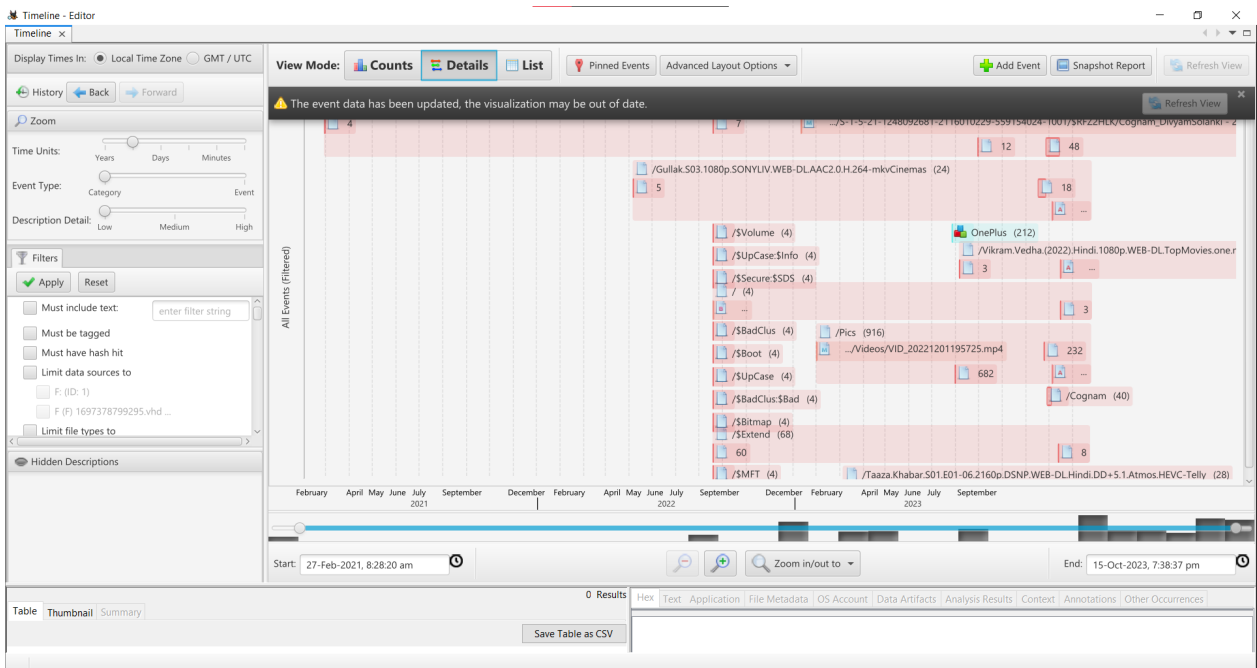
| Module | Num | New? | Subject | Timestamp |
|---------------------------|-----|------|---------------------------------------------------------------------|---------------------|
| Hash Lookup | 1 | • | No notable hash set. | 2023/10/15 19:38:45 |
| Hash Lookup | 1 | • | No known hash set. | 2023/10/15 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

Details :



List:

Timeline - Editor

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

Media Documents Executables Other

Limit event types to

File System File Accessed File Changed File Created File Modified Web Activity

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

| Timestamp | Event type | Description | Tagged | Hash hit |
|---------------------|------------|-------------------------------------------------------------------------------------------------------------------------------|--------|----------|
| 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-1-5-21-1248092681-2116010229-559154024-1001/\$RFZ2HLK\Cognam_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 End: 15-Oct-2023, 7:38:37 pm

Jump By: year

Table Thumbnail Summary

Save Table as CSV

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

The screenshot displays the Discovery tool interface, which is used for analyzing forensic data. The interface is divided into several sections:

- Step 1: Choose result type**: This section includes tabs for Images, Videos, Documents, and Domains. The Domains tab is currently selected.
- Step 2: Filter which domains to show**: This section contains several filters:
 - Data Source**: A list of logical file sets (LogicalFileSet1 (ID: 1), LogicalFileSet2 (ID: 43), LogicalFileSet3 (ID: 87), LogicalFileSet4 (ID: 448)) with checkboxes. The 'Uncheck All' and 'Check All' buttons are at the bottom.
 - Past Occurrences**: A section with checkboxes for Unique (1), Rare (2-10), Common (11 - 100), and Very Common (100+).
 - Date Filter**: A section with a radio button for 'Only final' and a dropdown for 'days of activity' (set to 7). There is also a 'Date Range (Asia/Calcutta)' section with 'Start' and 'End' date pickers (13 January 2022 and 13 October 2023).
 - Result Type**: A list of result types (Web Bookmarks, Web Cookies, Web History, Web Downloads, Web Search) with checkboxes. The 'Uncheck All' and 'Check All' buttons are at the bottom.
- Step 3: Choose display settings**: This section includes dropdown menus for 'Group By' (set to Page Views), 'Order Within Groups By' (set to Page Views), and 'Order Groups By' (set to Group Name).

On the right side of the interface, there is a 'Keyword Lists' section with a 'Keyword Search' input field and a 'Save Table as CSV' button. Below this is a table of results with columns for 'Keyword' and 'Modified Time'. The table shows 246 results, with the first few rows visible:

| Keyword | Modified Time |
|-------------------------|---------------------|
| 0019f | 2023-09-28 19:50:00 |
| 001ac | 2023-09-28 19:50:00 |
| | 2023-10-13 18:05:54 |
| 43.33/assistant_package | 2023-08-02 13:06:46 |
| 43.33/icudt1.dat | 2023-08-01 01:31:26 |
| 43.33/mojo_core.dll | 2023-08-02 13:06:55 |
| 43.33/opera_autoup... | 2023-08-02 13:07:31 |
| 80.16/assistant_package | 2023-08-23 12:14:00 |
| 80.16/mojo_core.dll | 2023-08-23 12:14:12 |
| 80.56/d3dcompiler_... | 2023-09-15 11:37:06 |
| 80.56/headless_lib_... | 2023-09-14 17:29:51 |
| 80.56/icudt1.dat | 2023-08-30 16:43:10 |
| 80.56/installer.exe | 2023-09-15 11:37:30 |
| 80.56/installer_help... | 2023-09-15 11:37:36 |
| 80.56/libEGL.dll | 2023-09-15 11:37:06 |
| 80.56/libGLESv2.dll | 2023-09-15 11:37:11 |
| 80.56/localization/b... | 2023-09-14 17:12:25 |
| 80.56/localization/b... | 2023-09-14 17:12:25 |

At the bottom right, there is a 'Text Source' dropdown menu set to 'Search Results' and a red circle icon with the number 171.

2. Web Browser History

The screenshot shows a web browser history analysis tool interface. The left sidebar contains a tree view with categories like Data Sources, File Views, Data Artifacts, and Analysis Results. The main panel displays a table of web history results. The table has columns for Source Name, S, C, O, URL, Date Accessed, Referrer URL, and Title. The results are sorted by Date Accessed, showing a list of 10000 results. The table includes various URLs from mail.google.com, accounts.google.com, and myaccount.google.com, with dates ranging from 2023-10-14 10:09:58 IST to 2023-10-14 10:11:06 IST. The bottom of the interface shows a search bar and a list of tags.

| Source Name | S | C | O | URL | Date Accessed | Referrer URL | Title |
|-------------|---|---|---|------------------------------------------------------|-------------------------|------------------------------------------------------|-----------------------|
| History | 2 | | | https://mail.google.com/mail/?tab=rm&ogbl | 2023-10-14 10:09:58 IST | https://mail.google.com/mail/?tab=rm&ogbl | Gmail |
| History | 2 | | | https://mail.google.com/mail/u/0/?tab=rm&ogbl | 2023-10-14 10:09:58 IST | https://mail.google.com/mail/u/0/?tab=rm&ogbl | Gmail |
| History | 2 | | | https://accounts.google.com/ServiceLogin?service=mai | 2023-10-14 10:09:58 IST | https://accounts.google.com/ServiceLogin?service=mai | Gmail |
| History | 2 | | | https://mail.google.com/accounts/SetOSID?authuser=0 | 2023-10-14 10:09:58 IST | https://mail.google.com/accounts/SetOSID?authuser=0 | Gmail |
| History | 2 | | | https://mail.google.com/mail/u/0/?tab=rm&ogbl&pli= | 2023-10-14 10:09:58 IST | https://mail.google.com/mail/u/0/?tab=rm&ogbl&pli= | Gmail |
| History | 2 | | | https://mail.google.com/mail/u/0/?ogbl | 2023-10-14 10:09:58 IST | https://mail.google.com/mail/u/0/?ogbl | Gmail |
| History | 2 | | | https://mail.google.com/mail/u/0/?ogbl#inbox | 2023-10-14 10:10:12 IST | https://mail.google.com/mail/u/0/?ogbl#inbox | Inbox (1) - dilishcho |
| History | 2 | | | https://myaccount.google.com/?hl=en_GB&authuser=0 | 2023-10-14 10:12:10 IST | https://myaccount.google.com/?hl=en_GB&authuser=0 | Google Account |
| History | 2 | | | https://accounts.google.com/ServiceLogin?service=acc | 2023-10-14 10:10:56 IST | https://accounts.google.com/ServiceLogin?service=acc | Google Account |
| History | 2 | | | https://myaccount.google.com/accounts/SetOSID?auth | 2023-10-14 10:10:56 IST | https://myaccount.google.com/accounts/SetOSID?auth | Google Account |
| History | 2 | | | https://myaccount.google.com/?hl=en_GB&authuser=0 | 2023-10-14 10:10:56 IST | https://myaccount.google.com/?hl=en_GB&authuser=0 | Google Account |
| History | 2 | | | https://myaccount.google.com/?hl=en_GB&utm_source | 2023-10-14 10:10:57 IST | https://myaccount.google.com/?hl=en_GB&utm_source | Google Account |
| History | 2 | | | https://myaccount.google.com/?hl=en_GB&utm_source | 2023-10-14 10:10:57 IST | https://myaccount.google.com/?hl=en_GB&utm_source | Google Account |
| History | 2 | | | https://myaccount.google.com/personal-info?hl=en_GB | 2023-10-14 10:12:18 IST | https://myaccount.google.com/personal-info?hl=en_GB | Personal info |
| History | 2 | | | https://myaccount.google.com/email?hl=en_GB | 2023-10-14 10:11:06 IST | https://myaccount.google.com/email?hl=en_GB | Email |

3. Url searches

The screenshot shows the same web browser history analysis tool interface, but with a search filter applied. The search bar at the top contains a complex regular expression: `((([H]([tT])?([F])?([tT])?([P])?([sS])?([V])?([wW])?([33])?([a-zA-Z0-9-~\.\!/:'@])?)+)*V($([a-zA-Z0-9\.\!/:'@])?)+)*`. The results table shows a list of 20858 results, with columns for List Name and Files with Hits. The results are sorted by Files with Hits, showing a list of 20858 results. The table includes various URLs from accounts.google.com, admission.gtu.ac.in, and other domains, with hits ranging from 1 to 5. The bottom of the interface shows a search bar and a list of tags.

| List Name | Files with Hits |
|-----------------------------------------------------|-----------------|
| http://accounts.google.com/adsession (2) | 2 |
| http://admission.gtu.ac.in (2) | 2 |
| http://admission.gtu.ac.in/login.aspx (3) | 3 |
| http://adsuse-planning.net/p3p/planning.p3p (1) | 1 |
| http://aia.entrust.net/evcs1-chain256.cer01 (3) | 3 |
| http://ap-northeast-1.console.aws.amazon.com/ec | 1 |
| http://ap-south-1.console.aws.amazon.com/ec2/ho | 1 |
| http://api.jqueryui.com/category/ui-core (2) | 2 |
| http://apps.usrc.gov.in/centralocb-2022/wtoptionin | 2 |
| http://betamoodle.iitvadodara.ac.in (2) | 2 |
| http://betamoodle.iitvadodara.ac.in/login/forgot_L | 2 |
| http://bit.ly/juntrax-apply (5) | 5 |
| http://bit.ly/juntrax-hiring (5) | 5 |
| http://bit.ly/oracle-apply1 (2) | 2 |
| http://bit.ly/oracle-hiring1 (5) | 5 |
| http://cacerts.digicert.com/digicertassuredidca-1.c | 1 |

DATA_Acquisition - 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 x Keyword search 8 - http x

Keyword search 246 Results

Table Thumbnail Summary

Save Table as CSV

| Name | Keyword Preview | Location | Modified Time |
|--------------------------|----------------------------------------------------------|--------------------------------------------------------|---------------------|
| f_00019f | "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/2 | /LogicalFileSet4/Cache_Data/f_00019f | 2023-09-28 19:50:05 |
| f_0001ac | "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/2 | /LogicalFileSet4/Cache_Data/f_0001ac | 2023-09-28 19:50:05 |
| History.html | lang="en" class="" meta: http-equiv="Content-... | /LogicalFileSet2/History.html | 2023-10-13 18:05:54 |
| assistant_package | 604020f0 http://www.digicert.com/CP50=http://... | /LogicalFileSet3/Opera/101.0.4843.33/assistant_package | 2023-08-02 13:06:46 |
| icudtl.dat | License & terms of use: http://www.unicode.org/c... | /LogicalFileSet3/Opera/101.0.4843.33/icudtl.dat | 2023-08-01 01:31:22 |
| mojo_core.dll | 604020f0 http://www.digicert.com/CP50=http://... | /LogicalFileSet3/Opera/101.0.4843.33/mojo_core.dll | 2023-08-02 13:06:56 |
| opera_autoupdate.exe | s]9Lm[9LL\$Hm\$H\$Xu1H=http://1.1H9[\$xu*1]\$(H | /LogicalFileSet3/Opera/101.0.4843.33/opera_autoup... | 2023-08-02 13:07:31 |
| assistant_package | 604020f0 http://www.digicert.com/CP50=http://... | /LogicalFileSet3/Opera/102.0.4880.16/assistant_package | 2023-08-23 12:14:00 |
| mojo_core.dll | 604020f0 http://www.digicert.com/CP50=http://... | /LogicalFileSet3/Opera/102.0.4880.16/mojo_core.dll | 2023-08-23 12:14:11 |
| d3dcompiler_47.dll | 604020f0 http://www.digicert.com/CP50=http://... | /LogicalFileSet3/Opera/102.0.4880.16/d3dcompiler_... | 2023-09-15 11:37:06 |
| headless_lib_strings.pak | with <code>http://</code>, like <a href="http:... | /LogicalFileSet3/Opera/102.0.4880.16/headless_lib... | 2023-09-14 17:29:51 |
| icudtl.dat | License & terms of use: http://www.unicode.org/c... | /LogicalFileSet3/Opera/102.0.4880.16/icudtl.dat | 2023-08-30 16:43:12 |
| installer.exe | whether we handled http=http-Reading existing tr... | /LogicalFileSet3/Opera/102.0.4880.16/installer.exe | 2023-09-15 11:37:35 |
| installer_helper_64.exe | 604020f0 http://www.digicert.com/CP50=http://... | /LogicalFileSet3/Opera/102.0.4880.16/installer_help... | 2023-09-15 11:37:36 |
| libEGL.dll | 604020f0 http://www.digicert.com/CP50=http://... | /LogicalFileSet3/Opera/102.0.4880.16/libEGL.dll | 2023-09-15 11:37:06 |
| libGLESv2.dll | com/3623, http://anglebug.com/3624, http://a... | /LogicalFileSet3/Opera/102.0.4880.16/libGLESv2.dll | 2023-09-15 11:37:11 |
| bg.pak | .access Crypto Wallet+HTTP= Kiosk and Signage Up... | /LogicalFileSet3/Opera/102.0.4880.16/localization/b... | 2023-09-14 17:12:25 |
| baseb... | (API) server Crypto Wallet+HTTP= Kiosk and Signage Up... | /LogicalFileSet3/Opera/102.0.4880.16/localization/b... | 2023-09-14 17:12:25 |

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

#IY vRF0

171

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 x

Keyword search 18 Results

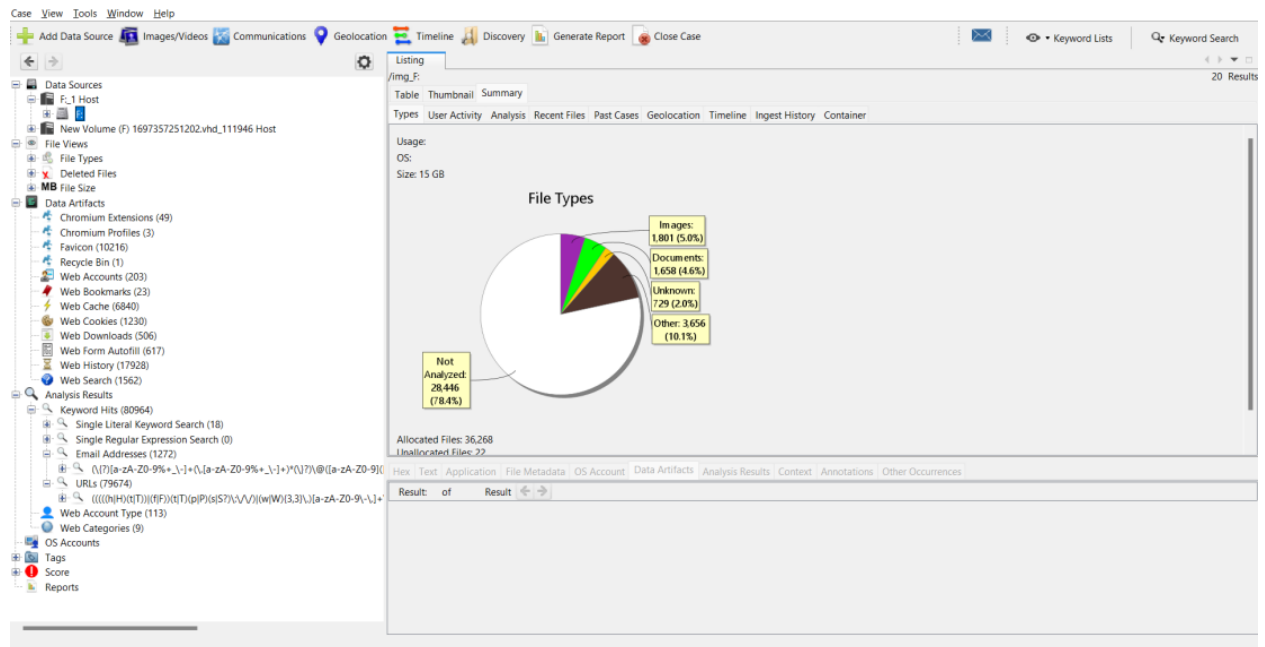
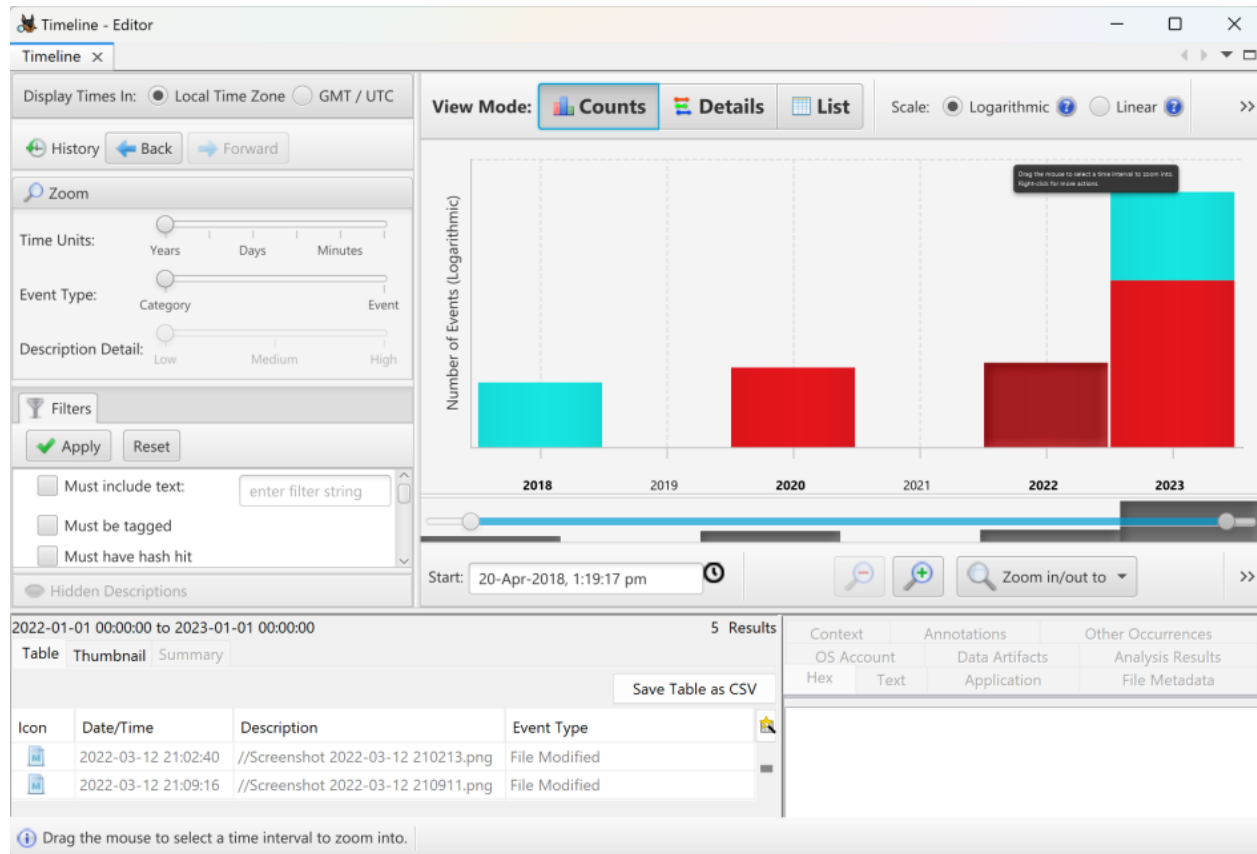
Table Thumbnail Summary

Save Table as CSV

| Name | Keyword Preview | Location | Modified Time | Change Time | Access Time |
|------------------------|-------------------------------------------------------|--------------------------------------------------------|-------------------------|-------------------------|-------------------------|
| Web Downloads Artifact | 157_C5445_Assignment_2.docx URL : https://docs.goo... | /img_F/Google/Chrome/User Data/Profile 2/History | 2023-10-14 21:17:13 IST | 2023-10-14 21:17:13 IST | 2023-10-15 13:08:52 IST |
| Web Downloads Artifact | 157_C5445_Assignment_2.docx URL : https://doc-0o... | /img_F/Google/Chrome/User Data/Profile 2/History | 2023-10-14 21:17:13 IST | 2023-10-14 21:17:13 IST | 2023-10-15 13:08:52 IST |
| Web Downloads Artifact | es/Downloads/Share (1).docx URL : blobhttps://web... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Web Downloads Artifact | 723897bba6fc7.docx name=051-100.docx Date Act... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Web Downloads Artifact | ies/Downloads/051-100.docx URL : https://smallpd... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Web Downloads Artifact | [Untitled document (1).docx URL : blobhttps://web... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Web Downloads Artifact | C:\Users\diles\Downloads\CS4431.docx URL : blobhtt... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Tabs,13341738840517046 | with the extension ".docx" created or mo... | /img_F/Google/Chrome/User Data/Profile 2/Sessions/T... | 2023-10-14 12:15:47 IST | 2023-10-14 12:15:47 IST | 2023-10-15 13:09:07 IST |
| Tabs,13341744804665078 | with the extension ".docx" created or mo... | /img_F/Google/Chrome/User Data/Profile 2/Sessions/T... | 2023-10-14 21:17:13 IST | 2023-10-14 21:17:13 IST | 2023-10-15 13:09:07 IST |
| History | 100.docx C:\Users\diles\Downloads\051-100.docx... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Web Downloads Artifact | _assignment1_202051082.docx URL : blobhttps://web... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Web Downloads Artifact | es/Downloads/Share (2).docx URL : blobhttps://web... | /img_F/Google/Chrome/User Data/Default/History | 2023-10-14 21:30:50 IST | 2023-10-14 21:30:50 IST | 2023-10-15 13:08:22 IST |
| Web Search Artifact | with the extension ".docx" created or mo... | /img_F/Google/Chrome/User Data/Profile 2/History | 2023-10-14 21:17:13 IST | 2023-10-14 21:17:13 IST | 2023-10-15 13:08:52 IST |
| Web Search Artifact | with the extension ".docx" created or mo... | /img_F/Google/Chrome/User Data/Profile 2/History | 2023-10-14 21:17:13 IST | 2023-10-14 21:17:13 IST | 2023-10-15 13:08:52 IST |
| Web Search Artifact | with the extension ".docx" created or mo... | /img_F/Google/Chrome/User Data/Profile 2/History | 2023-10-14 21:17:13 IST | 2023-10-14 21:17:13 IST | 2023-10-15 13:08:52 IST |
| Web Search Artifact | with the extension ".docx" created or mo... | /img_F/Google/Chrome/User Data/Profile 2/History | 2023-10-14 21:17:13 IST | 2023-10-14 21:17:13 IST | 2023-10-15 13:08:52 IST |

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

TimeLine :



Recovery of data :

Format F (F:) ×

Capacity:
331 GB ▼

File system
NTFS (Default) ▼

Allocation unit size
4096 bytes ▼

Restore device defaults

Volume label
F

Format options
☒ Quick Format

Start Close

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 |

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

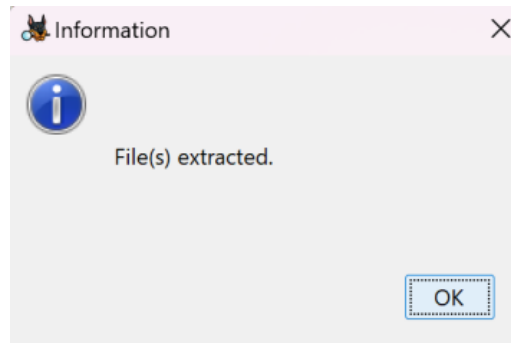
Page: 1 of 1 Pages: Go to Page:

Save Table as CSV

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) |
|-------------------------------------------|---|---|---|-------------------------|-------------------------|-------------------------|-------------------------|--------|-------------|
| 01A500000007E7F15124D4E | | | | 2023-10-15 13:32:51 IST | 2023-10-15 13:32:51 IST | 2023-10-15 13:32:51 IST | 2023-10-15 13:32:51 IST | 12824 | Unallocated |
| autopsy.log.0 | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:31:31 IST | 2023-10-15 13:17:37 IST | 6694 | Unallocated |
| autopsy.log.0-slack | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:31:31 IST | 2023-10-15 13:17:37 IST | 1498 | Unallocated |
| dilesh_chouhan_20231015_131735.properties | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:39 IST | 2023-10-15 13:17:39 IST | 34 | Unallocated |
| drawable.db | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:39 IST | 2023-10-15 13:17:39 IST | 65536 | Unallocated |
| segments_1 | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:38 IST | 2023-10-15 13:17:38 IST | 69 | Unallocated |
| write.lock | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:38 IST | 2023-10-15 13:17:38 IST | 0 | Unallocated |
| autopsy.db | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:39 IST | 2023-10-15 13:17:38 IST | 475136 | Unallocated |
| Dilesh_Chouhan.aut | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:38 IST | 2023-10-15 13:17:38 IST | 842 | Unallocated |
| Dilesh_Chouhan.aut-slack | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:38 IST | 2023-10-15 13:17:38 IST | 3254 | Unallocated |
| SqlCore.properties | | | | 2023-10-15 13:32:26 IST | 2023-10-15 13:32:26 IST | 2023-10-15 13:17:38 IST | 2023-10-15 13:17:38 IST | 341 | Unallocated |

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

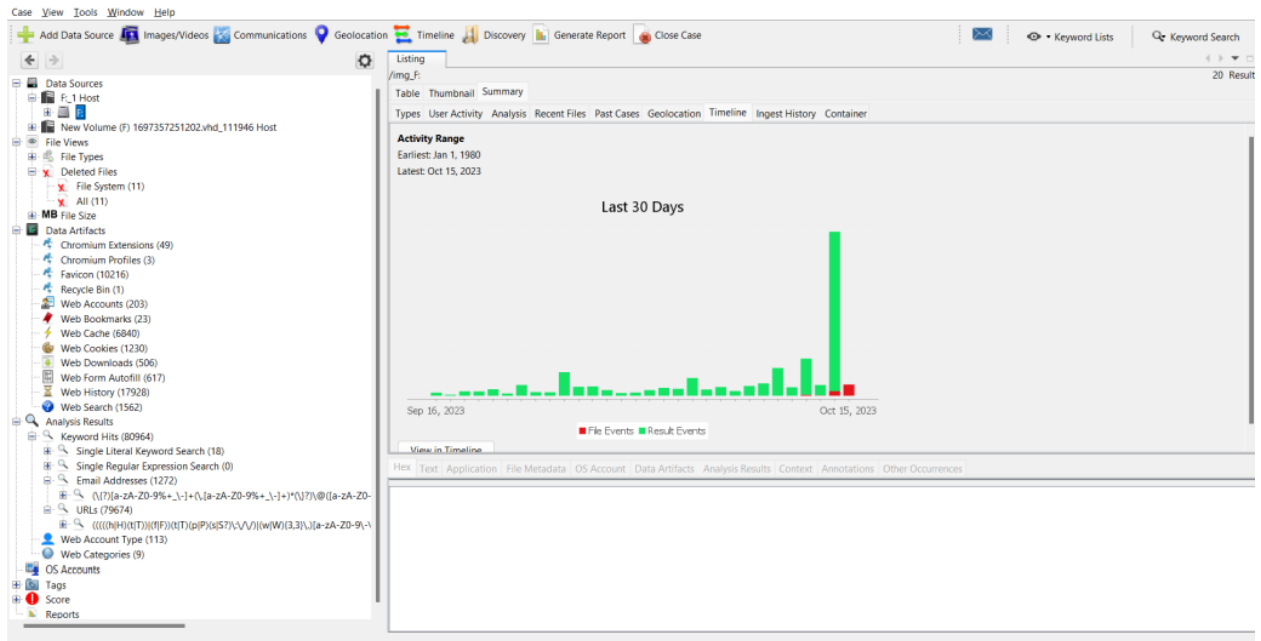
Result: of Result

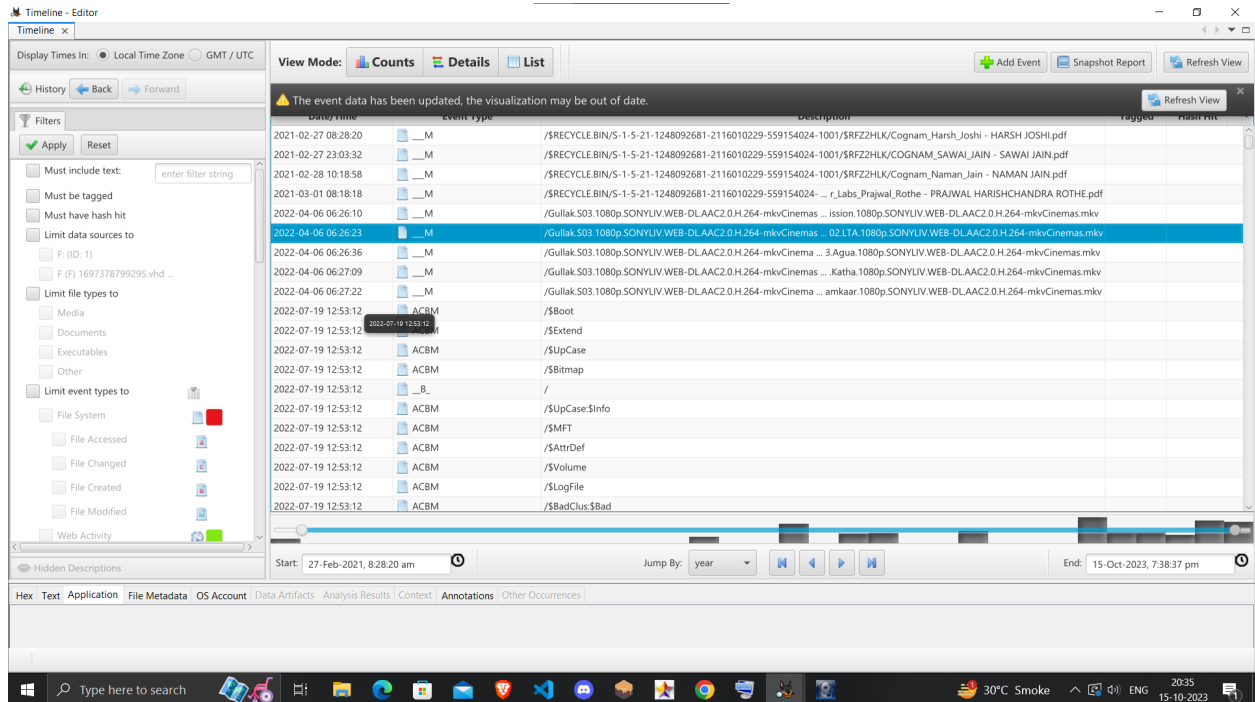
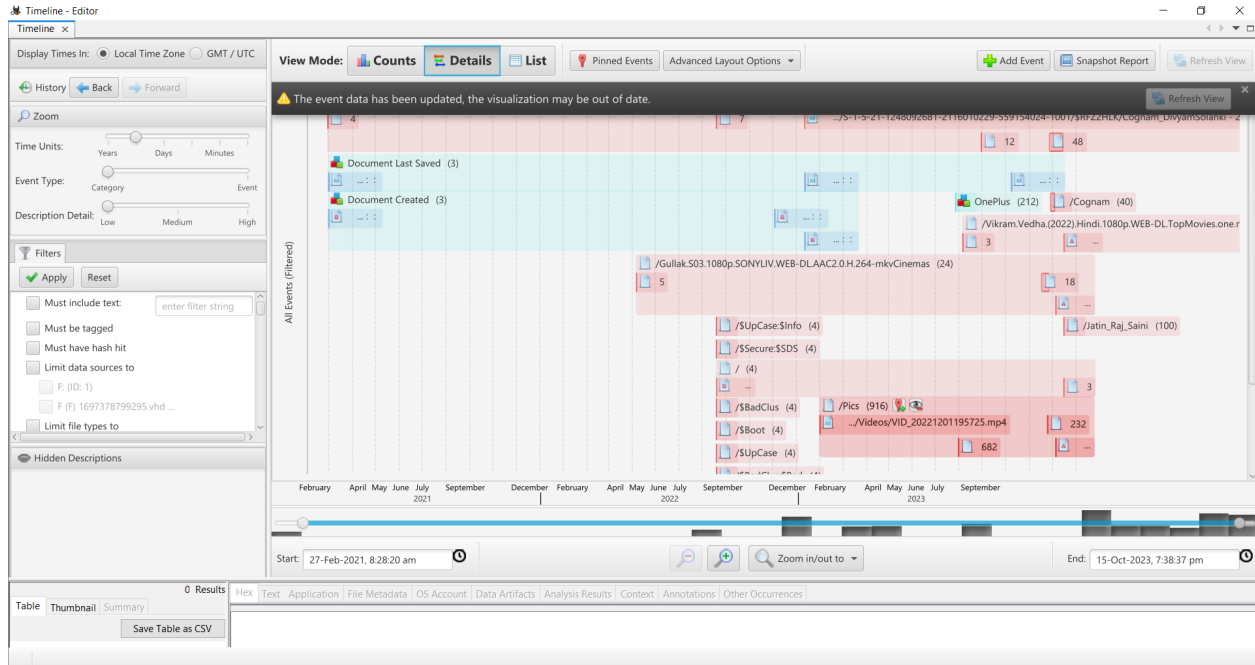


TASK 3-

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 :





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

MDS: 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