LOVELY PROFESSIONAL UNIVERSITY

INT 301

CA-3

OPEN-SOURCE TECHNOLOGIES

Extract Data from Disk drives and other Storage so as to Facilitate the Forensic Analysis

Name : Dipraj Daripa

Reg No. : 11911828

Program : B.Tech CSE

Semester : 8Th Sem

School : Computer Science and Engineering

Faculty : Manpreet Singh

Date of submission : 6h April 2023

1. INTRODUCTION

1.1 OBJECTIVE OF THE PROJECT :

The project is aimed at utilizing open-source software to extract data from various storage media, like hard drives, memory cards, and uSB drives in a forensically sound manner. This data could include files, email, chat logs, browser history, and other information that might, be relevant to a forensic investigation.

1.2 DESCRIPTION OF THE PROJECT :

Autopsy, a widely-used open source software for data extraction and forensic analysis of digital systems, offers examiners a comprehensive platform to conduct investigations on various media types such as memory cards, hard drives, and USB drives. The platform facilitates digital forensics, providing users the opportunity to explore and conduct thorough analyses.

1) In order to dutifully delve into forensic investigations, using Autopsy or a comparable software would be the intended route to effectively dissect data from storage media and disk drives. Extracted from this process would be files, emails, browser history, chat logs and other noteworthy data.
2) To uncover any relevant findings, the data will be analyzed once it has been extracted.
3) This analysis could include identifying deleted files or hidden data, searching for keywords or patterns, and examining metadata to determine file creation, modification, or access times.
4) In essence, the primary objective of this endeavor is to furnish law enforcement agencies, forensic examiners, and other practitioners with a potent means of carrying out digital investigations and collecting evidence while maintaining forensic integrity and legal acceptability. Furthermore, through the implementation of open-source software, this undertaking would foster transparency, and actively encourage broader utilization of digital forensics tools.

About Autopsy :

Autopsy is the graphical user interface (GUI) utilized in conjunction with The Sleuth Kit, a set of command-line tools and a library. Together, they enable the exploration of disk images for forensic purposes. All outcomes from analysis of the images are visualized in Autopsy. Digital devices can have deleted data recovered using this tool. It's utilized in various fields, such as corporate examining, military and law enforcement investigations. The investigator's work is assisted by these findings, as relevant sections of data regarding their investigation is located.

1.3 SCOPE OF THE PROJECT

Utilizing open source software to forensically extract data from storage media such as hard drives, USB drives, and memory cards is the project's focus. Relevant information that may aid in a forensic investigation, such as files, chat logs, email, and browsing history, is included in this data.

Some of the areas

- Data Extraction: In a forensically sound manner, data will be extracted from various storage media, including hard drives, USB drives, and memory cards, as part of the project.
- Digital Forensic Analysis: Extracted data will be thoroughly examined using Autopsy as the main methodology for conducting digital forensic analysis, which happens to be the main objective of the project.

- Open Source Software: An open source software, Autopsy, is the chosen tool for this project's digital forensic analysis efforts. The software's transparency promotes widespread usability for users.
- Preservation of Evidence: During the extraction process, it is crucial to prioritize maintaining the authenticity of the original data, as this allows for its potential use as evidence in a legal setting. Emphasis is placed on this aspect within the scope of the project.

- Keyword Searching: The extracted data can be easily searched for specific terms or phrases using Autopsy's impressive keyword search feature, a tool that holds immense power for investigators.
- Data Carving: Utilizing Autopsy's data carving tool, the endeavor incorporates the retrieval of pertinent files or file fragments that have been eradicated.

- Hash Matching: Matching a file's hash value to a known value is made possible through Autopsy's hash matching tool, which assists investigators in identifying any files that could have been tampered with or altered.

- Timeline Analysis: Using Autopsy's timeline analysis tool, the project aims to establish a sequence of events and unveil any potential culprits by examining

- the creation, modification, and access times of particular files.

- Exporting Reports: Various formats like PDF, HTML, and CSV are utilized by the project in exporting Autopsy's generated reports. As evidence in court, these reports present a thorough analysis of the data extracted.

Overall, the scope of the project to use Autopsy for forensic analysis is extensive and covers a wide range of tools and techniques that investigators can use to uncover evidence and build a strong case.

2. SYSTEM DESCRIPTION

2.1 TARGET SYSTEM DESCRIPTION :

For successfully downloading Autopsy, it's imperative to ensure that the software's system requirements are met. Below is a breakdown of the system specifications that are necessary to download Autopsy:

- Operating System: Meet the minimum system requirements of your operating system before downloading Autopsy on Windows, MacOS, or Linux.

- Java: To properly run an autopsy, ensure that your computer boasts the latest Java iteration.

- Download Source: The Sleuth Kit, who is responsible for Autopsy's development, provides the open source software for download on their official website. To acquire Autopsy, you must head to the website's download page and select the version suitable for your OS.

- Installation: Autopsy can be installed to your computer once the download is finished. Be sure to follow the instructions given by the software to properly install it. The process of installation may differ depending on your computer's operating system.

- Configuration: After installation, configure Autopsy to suit your needs. This includes setting up case management, data sources, and other preferences.
- Usage: Once configured, Autopsy is ready for use. Open the software and start using its features to extract, analyze, and report on digital media.

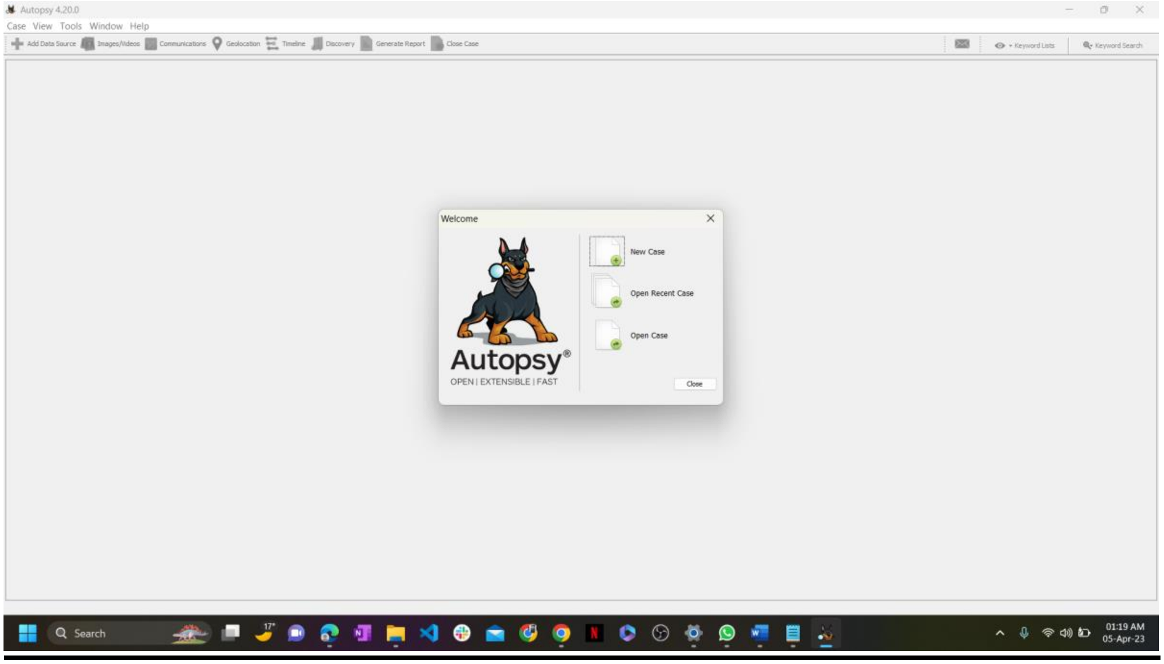
Overall, downloading Autopsy requires a computer that meets the minimum system requirements for the operating system you are using, Java installed, and downloading the software from the official website of The Sleuth Kit. Once installed, configure Autopsy to suit your needs and start using its features to perform digital forensic analysis.

3. ANALYSIS REPORT

3.1 Getting Started :

Open Autopsy and create a new case.

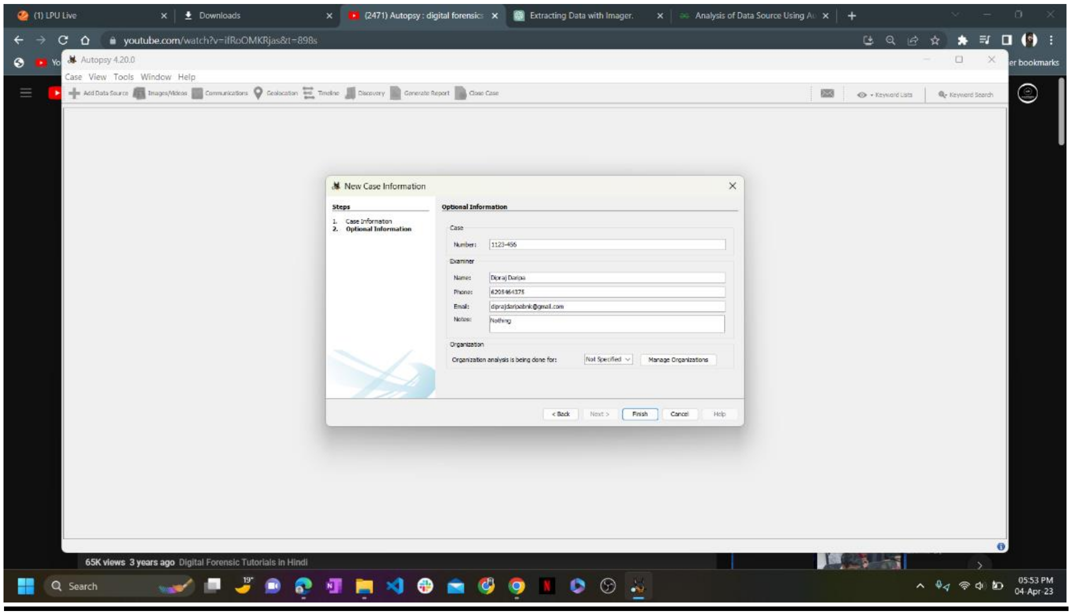
You can Open a recent case or open any case.



3.2 Optional System Information:

First you need to create a case Number for this.

Then Put the detail of the exminner.



New Case Information

Steps

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

Optional Information

Case

Number: 1123-456

Examiner

Name: Dipraj Daripa

Phone: 6205464375

Email: diprajdaripabnk@gmail.com

Notes: Nothing

Organization

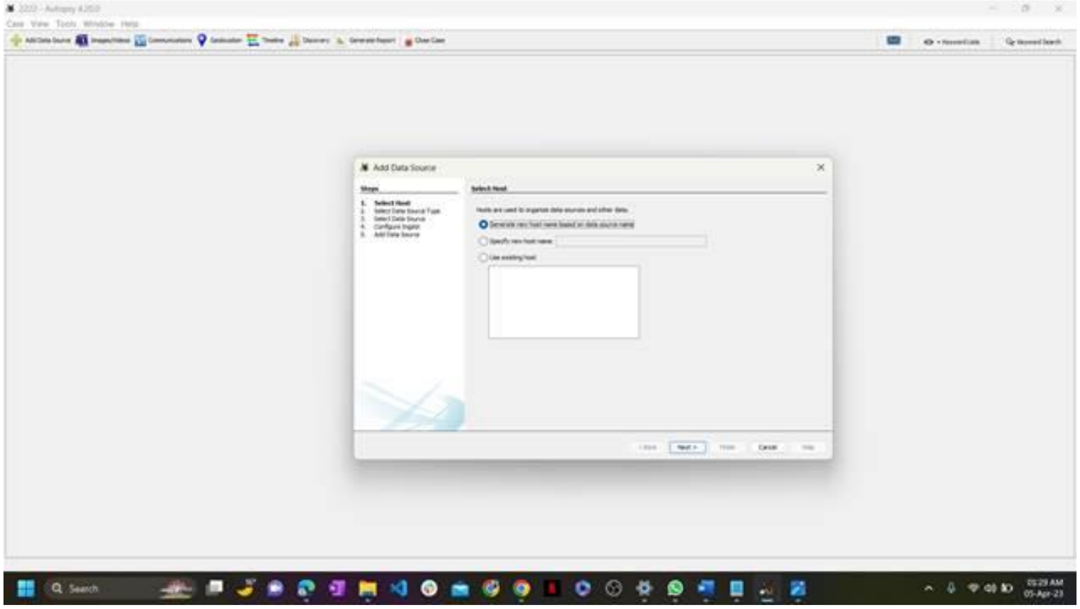
Organization analysis is being done for: Not Specified

3.3 Add Data Source:

Select the appropriate data source .

Step 1)

Select the host :



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

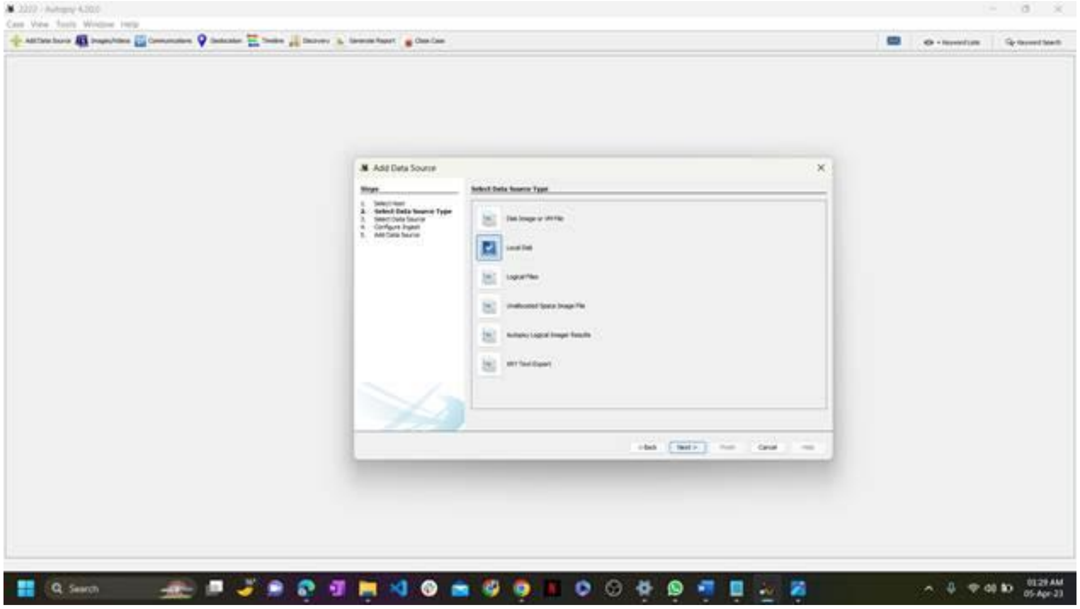
○ Specify new host name

○ Use existing host

Step 2)

Select the data Source Type.

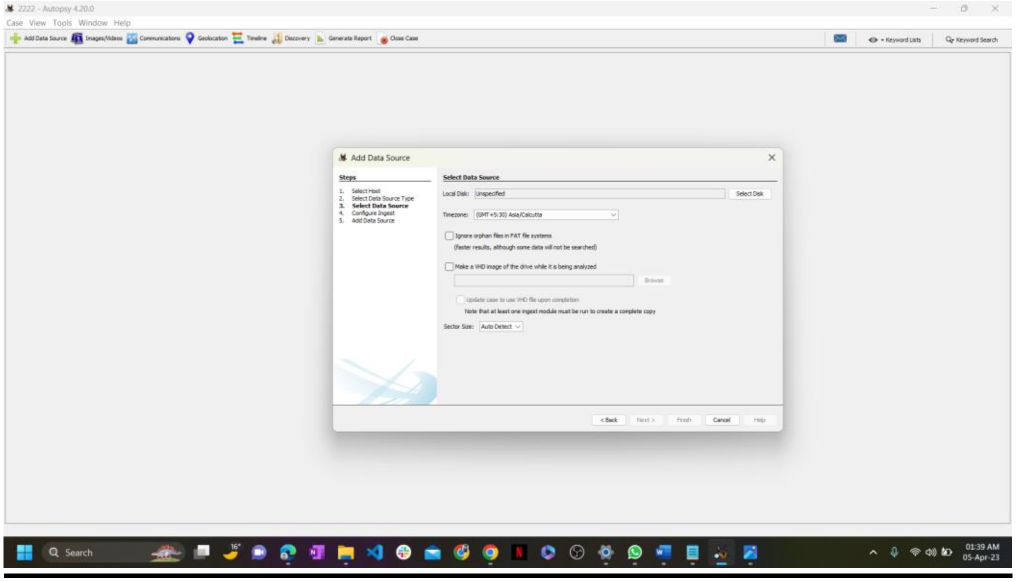
- Disk Image or VM file: These are files that contain an exact copy of a hard drive, media card, or a virtual machine image.
- Local Disk: This category includes various types of physical storage devices such as hard disks, pendrives, memory cards, and so on.
- Logical Files: These are local files and folders that are stored on your computer's physical storage devices.
- Unallocated Space Image File: This type of file includes data that is not organized into a file system, but still needs to be processed during the data ingestion process.



Step 3)

Select the data Source

Which data Source You want to analysis.



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: Unspecified

Timezone: (GMT+5:30) Asia/Calcutta

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

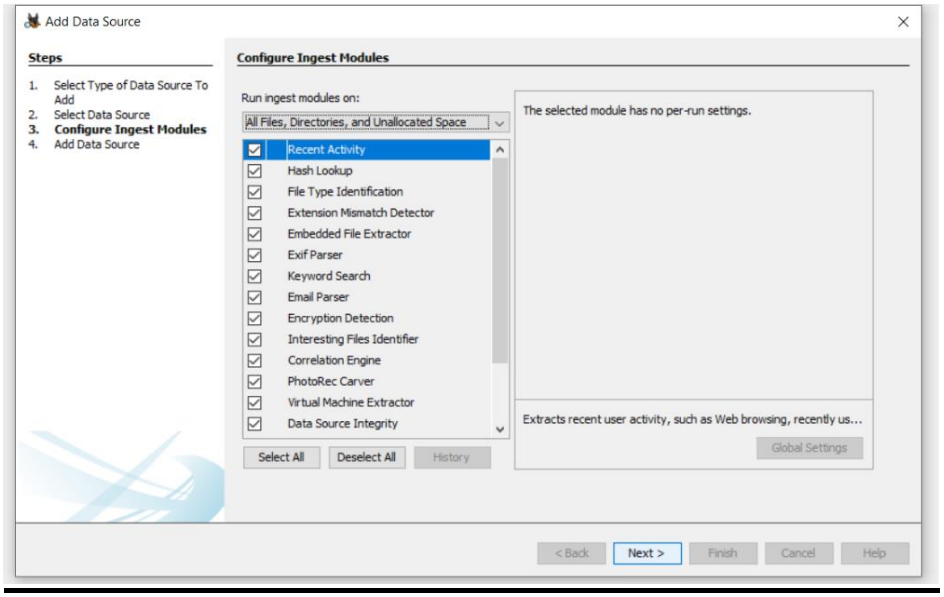
☐ Make a VHD image of the drive while it is being analyzed

☐ 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

Step 4)

Configure ingest modules.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Encryption Detection
☑ Interesting Files Identifier
☑ Correlation Engine
☑ PhotoRec Carver
☑ Virtual Machine Extractor
☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Autopsy ingest modules:

- Recent Activity: Shows the most recent operations performed on the disk.
- Hash Lookup: Identifies files using their unique hash values.
- File Type Identification: Identifies files based on their internal signatures.
- Extension Mismatch Detector: Identifies files with tampered extensions.
- Embedded File Extractor: Extracts files that are embedded within other files, such as .zip or .rar archives.

- EXIF Parser: Retrieves metadata about image files.
- Keyword Search: Searches for specific keywords or patterns within the data.
- Email Parser: Extracts information from email databases.
- Encryption Detection: Detects and identifies encrypted or password-protected files.
- Interesting File Identifier: Allows users to set custom rules to filter data.
- Correlation Engine: Displays correlated properties to help identify patterns and relationships within the data.
- PhotoRec Carver: Recovers files from unallocated space.
- Virtual Machine Extractor: Extracts and analyzes virtual machines.
- Data Source Integrity: Calculates hash values and verifies data integrity.
- Plaso: Extracts timestamps for various types of files.
- Android Analyzer: Analyzes SQLite and other files from an Android device.

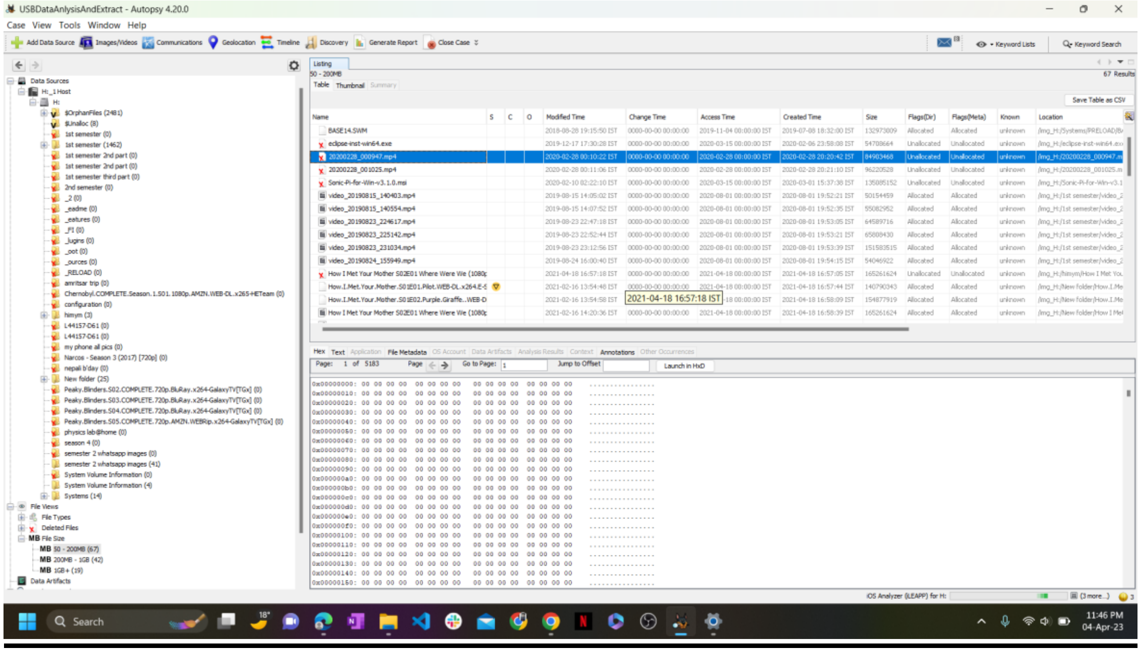
Step 4)

To begin the investigation, select all relevant data sources and click "Next". Once the data sources are added, click "Finish". The tool will require some buffer time to extract and analyze the data, depending on the size of the data source.

3.4 Exploring the Data Source:

- The Data Source information: In this section, you can view basic metadata about the selected data source. The bottom section provides a more detailed analysis, and you can extract additional information in various formats, such as Hex values, Results, and File Metadata.

Hex value:



50 - 200MB

67 Results

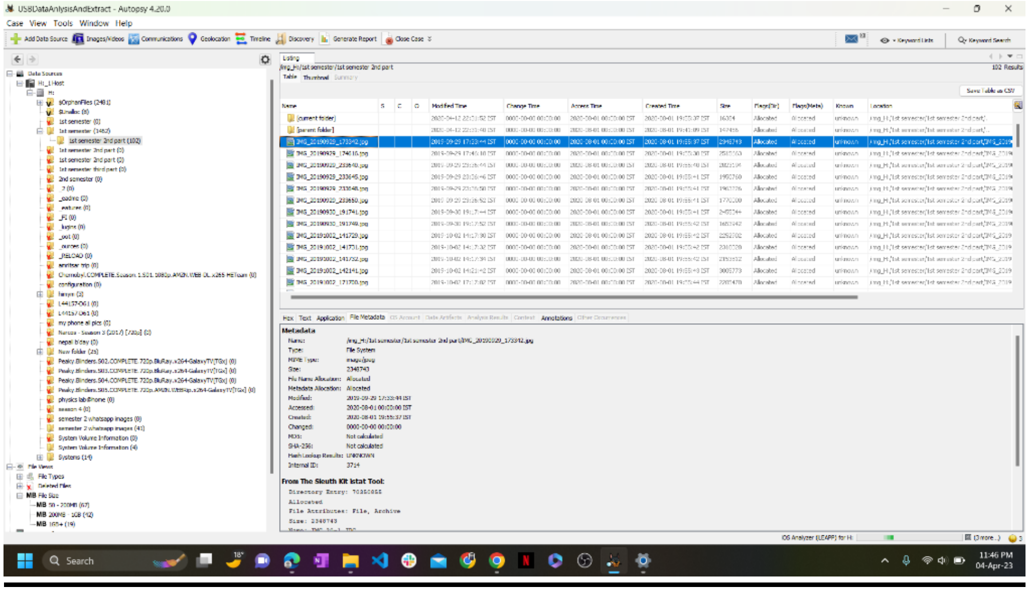
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
BASE14.SWM				2018-08-28 19:15:50 IST	0000-00-00 00:00:00	2019-11-04 00:00:00 IST	2019-07-08 18:32:00 IST	132973009	Allocated	Allocated	unknown	/img_H:/Systems/PRELOAD/B
☒ eclipse-inst-win64.exe				2019-12-17 17:30:28 IST	0000-00-00 00:00:00	2020-03-15 00:00:00 IST	2020-02-06 23:58:08 IST	54708664	Unallocated	Unallocated	unknown	/img_H:/eclipse-inst-win64.ex
☒ 20200228_000947.mp4				2020-02-28 00:10:22 IST	0000-00-00 00:00:00	2020-02-28 00:00:00 IST	2020-02-28 20:20:42 IST	84903468	Unallocated	Unallocated	unknown	/img_H:/20200228_000947.m
☒ 20200228_001025.mp4				2020-02-28 00:11:06 IST	0000-00-00 00:00:00	2020-02-28 00:00:00 IST	2020-02-28 20:21:10 IST	96220528	Unallocated	Unallocated	unknown	/img_H:/20200228_001025.m
☒ Sonic-Pi-for-Win-v3.1.0.msi				2020-02-10 02:22:10 IST	0000-00-00 00:00:00	2020-03-15 00:00:00 IST	2020-03-01 15:37:38 IST	135085152	Unallocated	Unallocated	unknown	/img_H:/Sonic-Pi-for-Win-v3.1
video_20190815_140403.mp4				2019-08-15 14:05:02 IST	0000-00-00 00:00:00	2020-08-01 00:00:00 IST	2020-08-01 19:52:21 IST	50154459	Allocated	Allocated	unknown	/img_H:/1st semester/video_2
video_20190815_140554.mp4				2019-08-15 14:07:52 IST	0000-00-00 00:00:00	2020-08-01 00:00:00 IST	2020-08-01 19:52:35 IST	55082952	Allocated	Allocated	unknown	/img_H:/1st semester/video_2
video_20190823_224617.mp4				2019-08-23 22:47:18 IST	0000-00-00 00:00:00	2020-08-01 00:00:00 IST	2020-08-01 19:53:05 IST	64589716	Allocated	Allocated	unknown	/img_H:/1st semester/video_2
video_20190823_225142.mp4				2019-08-23 22:52:44 IST	0000-00-00 00:00:00	2020-08-01 00:00:00 IST	2020-08-01 19:53:21 IST	65808430	Allocated	Allocated	unknown	/img_H:/1st semester/video_2
video_20190823_231034.mp4				2019-08-23 23:12:56 IST	0000-00-00 00:00:00	2020-08-01 00:00:00 IST	2020-08-01 19:53:39 IST	151583515	Allocated	Allocated	unknown	/img_H:/1st semester/video_2
video_20190824_155949.mp4				2019-08-24 16:00:40 IST	0000-00-00 00:00:00	2020-08-01 00:00:00 IST	2020-08-01 19:54:15 IST	54046922	Allocated	Allocated	unknown	/img_H:/1st semester/video_2
☒ How I Met Your Mother S02E01 Where Were We (1080p				2021-04-18 16:57:18 IST	0000-00-00 00:00:00	2021-04-18 00:00:00 IST	2021-04-18 16:57:05 IST	165261624	Unallocated	Unallocated	unknown	/img_H:/himym/How I Met You
How.I.Met.Your.Mother.S01E01.Pilot.WEB-DL.x264.E-S	▽			2021-02-16 13:54:48 IST	0000-00-00 00:00:00	2021-04-18 00:00:00 IST	2021-04-18 16:57:44 IST	140790343	Allocated	Allocated	unknown	/img_H:/New folder/How.I.Me
How.I.Met.Your.Mother.S01E02.Purple.Giraffe..WEB-D				2021-02-16 13:54:58 IST	2021-04-18 16:57:18 IST	-18 00:00:00 IST	2021-04-18 16:58:09 IST	154877919	Allocated	Allocated	unknown	/img_H:/New folder/How.I.Me
How I Met Your Mother S02E01 Where Were We (1080p				2021-02-16 14:20:36 IST	0000-00-00 00:00:00	2021-04-18 00:00:00 IST	2021-04-18 16:58:39 IST	165261624	Allocated	Allocated	unknown	/img_H:/New folder/How I Me

Page: 1 of 5183 Page Go to Page: 1 Jump to Offset

```
0x00000000: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000010: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000020: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000030: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000040: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000050: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000060: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000070: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000080: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000090: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x000000a0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x000000b0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x000000c0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x000000d0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x000000e0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x000000f0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000100: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000110: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000120: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000130: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000140: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000150: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
```

11:46 PM
04-Apr-23

Meta data:



/img_H:/1st semester/1st semester 2nd part

102 Results

Metadata

Name: /img_H:/1st semester/1st semester 2nd part/IMG_20190929_173342.jpg
Type: File System
MIME Type: image/jpeg
Size: 2348743
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2019-09-29 17:33:44 IST
Accessed: 2020-08-01 00:00:00 IST
Created: 2020-08-01 19:55:37 IST
Changed: 0000-00-00 00:00:00
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 3714

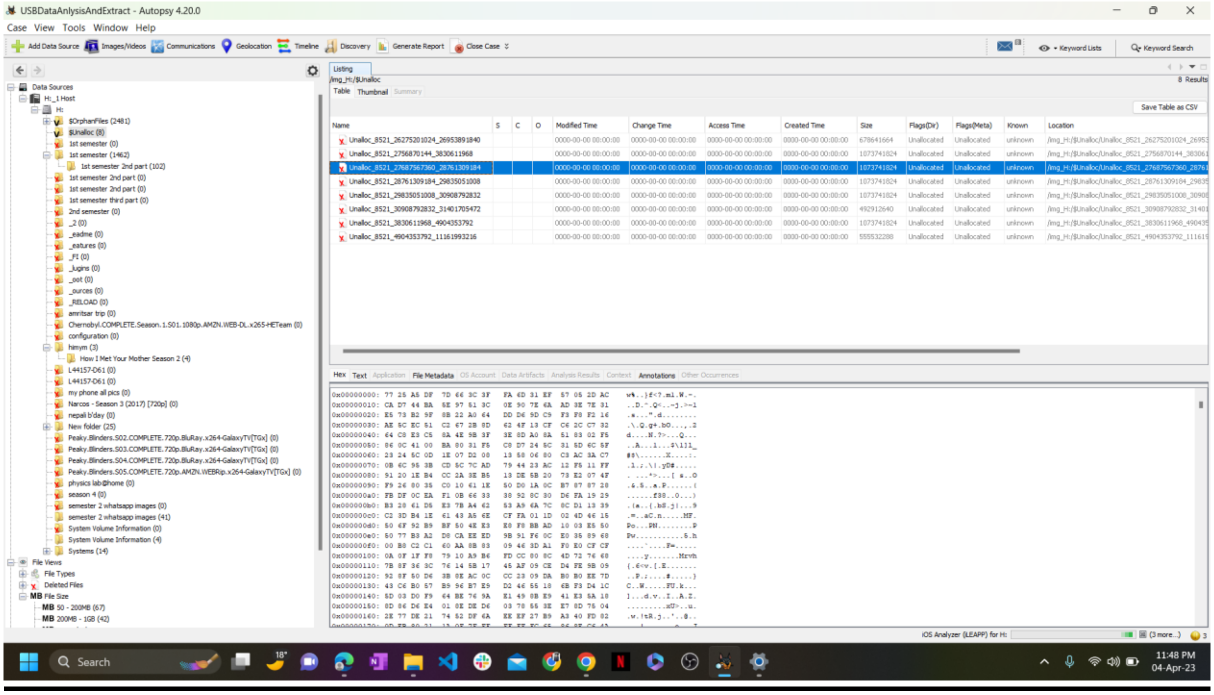
From The Sleuth Kit istat Tool:

```
Directory Entry: 70250055
Allocated
File Attributes: File, Archive
Size: 2348743
```

11:46 PM
04-Apr-23

- **<u>Extracted Deleted File Data</u>**: Additionally, it is possible to extract metadata and Hex values of deleted files and gather information about them using this tool.

In The file Which have Cross Symbol means Its was Deleted.



USBDataAnlysisAndExtract - Autopsy 4.20.0

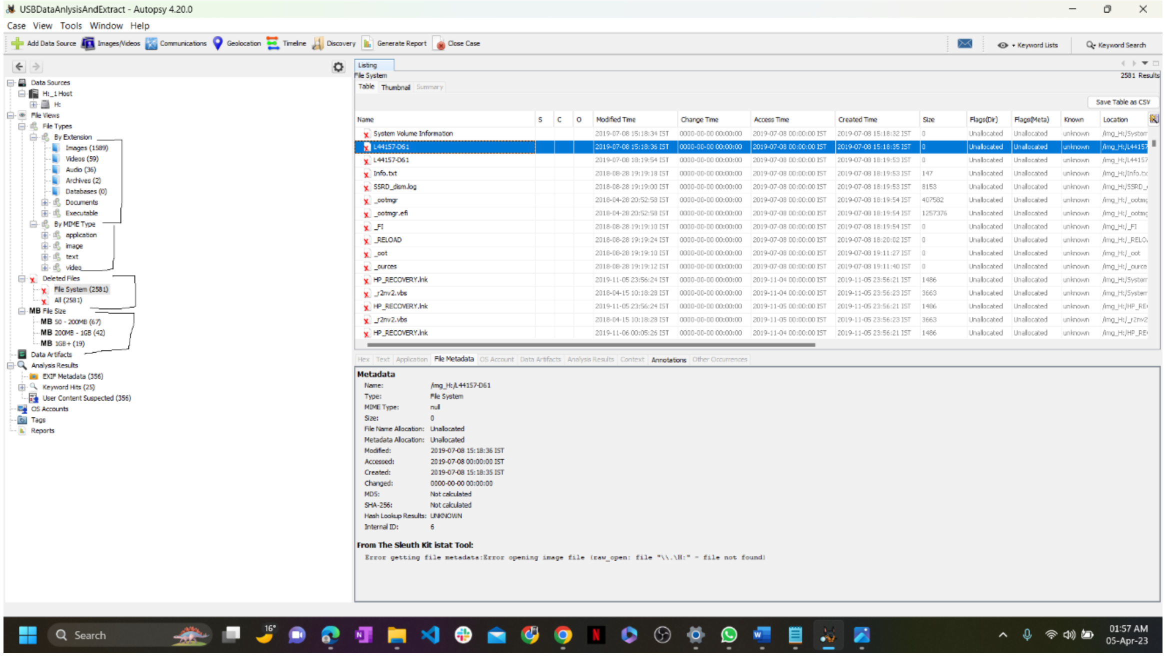
Listing

/img_H:/$Unalloc — 8 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Unalloc_8521_26275201024_26953891840				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	678641664	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_26275201024_2695
Unalloc_8521_2756870144_3830611968				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_2756870144_38306
Unalloc_8521_27687567360_28761309184				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_27687567360_2876
Unalloc_8521_28761309184_29835051008				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_28761309184_2983
Unalloc_8521_29835051008_30908792832				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_29835051008_3090
Unalloc_8521_30908792832_31401705472				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	492912640	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_30908792832_3140
Unalloc_8521_3830611968_4904353792				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_3830611968_49043
Unalloc_8521_4904353792_11161993216				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	555532288	Unallocated	Unallocated	unknown	/img_H:/$Unalloc/Unalloc_8521_4904353792_11161

```
0x00000000: 77 25 A5 DF  7D 66 3C 3F  FA 6D 31 EF  57 05 2D AC   w%..}f<?.m1.W.-.
0x00000010: CA D7 44 BA  5E 97 51 3C  0E 90 7E 6A  AD 3E 7E 31   ..D.^.Q<..~j.>~1
0x00000020: E5 73 B2 9F  8B 22 A0 64  DD D6 9D C9  F3 F8 F2 16   .s...".d........
0x00000030: AE 5C EC 51  C2 67 2B 8D  62 4F 13 CF  C6 2C C7 32   .\.Q.g+.bO...,.2
0x00000040: 64 C8 E3 C5  8A 4E 9B 3F  3E 8D A0 8A  51 83 02 F5   d....N.?>...Q...
0x00000050: 86 0C 41 00  BA 80 31 F5  C8 D7 24 5C  31 5D 6C 5F   ..A...1...$\1]l_
0x00000060: 23 24 5C 0D  1E 07 D2 08  13 58 06 80  C3 AC 3A C7   #$\......X....:.
0x00000070: 0B 6C 95 3B  CD 5C 7C AD  79 44 23 AC  12 F5 11 FF   .l.;.\|.yD#.....
0x00000080: 91 20 1E B4  CC 2A 3E B5  13 DE 5B 20  73 E2 07 4F   . ...*>...[ s..O
0x00000090: F9 26 80 35  C0 10 61 1E  50 D0 1A 0C  B7 87 87 28   .&.5..a.P......(
0x000000a0: FB DF 0C EA  F1 0B 66 33  38 92 8C 30  D6 FA 19 29   ......f38..0...)
0x000000b0: B3 28 61 D5  E3 7B A4 62  53 A9 6A 7C  8C D1 13 39   .(a..{.bS.j|...9
0x000000c0: C2 3D B4 1E  61 43 A5 6E  CF FA 01 1D  02 4D 46 15   .=..aC.n.....MF.
0x000000d0: 50 6F 92 B9  BF 50 4E E3  E8 F8 BB AD  10 03 E5 50   Po...PN........P
0x000000e0: 50 77 B3 A2  D8 CA EE ED  9B 91 F6 0C  E0 35 89 68   Pw...........5.h
0x000000f0: 00 B8 C2 C1  60 AA 8B 83  09 46 3D A1  F0 E0 CF CF   ....`....F=.....
0x00000100: 0A 0F 1F F8  79 10 A9 B6  FD CC 80 8C  4D 72 76 68   ....y.......Mrvh
0x00000110: 7B 8F 36 3C  76 14 5B 17  45 AF 09 CE  D4 FE 9B 09   {.6<v.[.E.......
0x00000120: 92 8F 50 D6  3B 8E AC 0C  CC 23 09 DA  B0 B0 EE 7D   ..P.;....#.....}
0x00000130: 43 C6 B0 57  B9 96 B7 E9  D2 46 55 18  6B F3 D4 1C   C..W.....FU.k...
0x00000140: 5D 03 D0 F9  64 BE 76 9A  E1 49 8B E9  41 E3 5A 18   ]...d.v..I..A.Z.
0x00000150: 8D 86 D6 E4  01 8E DE D6  03 78 55 3E  E7 8D 75 04   .........xU>..u.
0x00000160: 2E 77 DE 21  74 52 DF 6A  EE EF 27 B9  A3 40 FD 82   .w.!tR.j..'..@..
```

- **List View :** Its Gives a List View, Like how many Image file, how many Deleted file, and listed file according to its size.



USBDataAnlysisAndExtract - Autopsy 4.20.0

Listing

File System — 2581 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
System Volume Information				2019-07-08 15:18:34 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 15:18:32 IST	0	Unallocated	Unallocated	unknown	/img_H:/System
L44157-D61				2019-07-08 15:18:36 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 15:18:35 IST	0	Unallocated	Unallocated	unknown	/img_H:/L44157
L44157-D61				2019-07-08 18:19:54 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 18:19:53 IST	0	Unallocated	Unallocated	unknown	/img_H:/L44157
Info.txt				2018-08-28 19:19:18 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 18:19:53 IST	147	Unallocated	Unallocated	unknown	/img_H:/Info.tx
SSRD_dism.log				2018-08-28 19:19:00 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 18:19:53 IST	8153	Unallocated	Unallocated	unknown	/img_H:/SSRD_
_ootmgr				2018-04-28 20:52:58 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 18:19:54 IST	407582	Unallocated	Unallocated	unknown	/img_H:/_ootmg
_ootmgr.efi				2018-04-28 20:52:58 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 18:19:54 IST	1257376	Unallocated	Unallocated	unknown	/img_H:/_ootmg
_FI				2018-08-28 19:19:10 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 18:19:54 IST	0	Unallocated	Unallocated	unknown	/img_H:/_FI
_RELOAD				2018-08-28 19:19:24 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 18:20:02 IST	0	Unallocated	Unallocated	unknown	/img_H:/_RELO
_oot				2018-08-28 19:19:10 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 19:11:27 IST	0	Unallocated	Unallocated	unknown	/img_H:/_oot
_ources				2018-08-28 19:19:12 IST	0000-00-00 00:00:00	2019-07-08 00:00:00 IST	2019-07-08 19:11:40 IST	0	Unallocated	Unallocated	unknown	/img_H:/_ource
HP_RECOVERY.lnk				2019-11-05 23:56:24 IST	0000-00-00 00:00:00	2019-11-04 00:00:00 IST	2019-11-05 23:56:21 IST	1486	Unallocated	Unallocated	unknown	/img_H:/System
_r2nv2.vbs				2018-04-15 10:18:28 IST	0000-00-00 00:00:00	2019-11-04 00:00:00 IST	2019-11-05 23:56:23 IST	3663	Unallocated	Unallocated	unknown	/img_H:/System
HP_RECOVERY.lnk				2019-11-05 23:56:24 IST	0000-00-00 00:00:00	2019-11-05 00:00:00 IST	2019-11-05 23:56:21 IST	1486	Unallocated	Unallocated	unknown	/img_H:/HP_RE
_r2nv2.vbs				2018-04-15 10:18:28 IST	0000-00-00 00:00:00	2019-11-05 00:00:00 IST	2019-11-05 23:56:23 IST	3663	Unallocated	Unallocated	unknown	/img_H:/_r2nv2
HP_RECOVERY.lnk				2019-11-06 00:05:26 IST	0000-00-00 00:00:00	2019-11-04 00:00:00 IST	2019-11-05 23:56:21 IST	1486	Unallocated	Unallocated	unknown	/img_H:/HP_RE

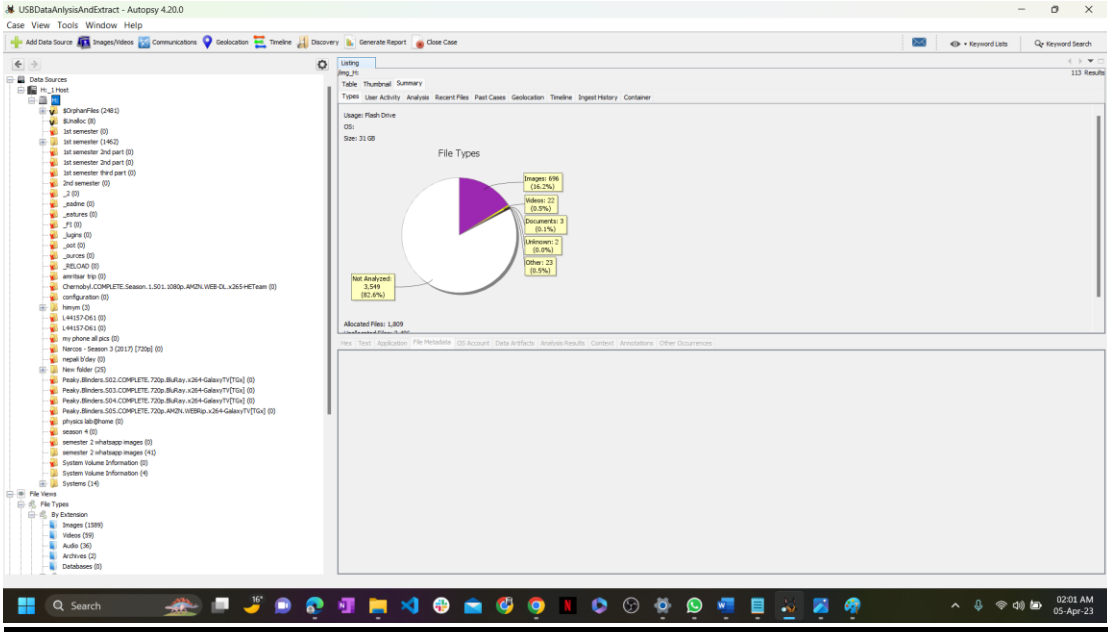
Metadata

Name:	/img_H:/L44157-D61
Type:	File System
MIME Type:	null
Size:	0
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2019-07-08 15:18:36 IST
Accessed:	2019-07-08 00:00:00 IST
Created:	2019-07-08 15:18:35 IST
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	6

From The Sleuth Kit istat Tool:

```
Error getting file metadata:Error opening image file (raw_open: file "\\.\H:" - file not found)
```

- **Summry Data:** I can clearly See The Pie table View of the Summary of the Data Source.



```
Data Sources
  H:_1 Host
    H:
      $OrphanFiles (2481)
      $Unalloc (8)
      1st semester (0)
      1st semester (1462)
      1st semester 2nd part (0)
      1st semester 2nd part (0)
      1st semester third part (0)
      2nd semester (0)
      _2 (0)
      _eadme (0)
      _eatures (0)
      _FI (0)
      _lugins (0)
      _oot (0)
      _ources (0)
      _RELOAD (0)
      amritsar trip (0)
      Chernobyl.COMPLETE.Season.1.S01.1080p.AMZN.WEB-DL.x265-HETeam (0)
      configuration (0)
      himym (3)
      L44157-D61 (0)
      L44157-D61 (0)
      my phone all pics (0)
      Narcos - Season 3 (2017) [720p] (0)
      nepali b'day (0)
      New folder (25)
      Peaky.Blinders.S02.COMPLETE.720p.BluRay.x264-GalaxyTV[TGx] (0)
      Peaky.Blinders.S03.COMPLETE.720p.BluRay.x264-GalaxyTV[TGx] (0)
      Peaky.Blinders.S04.COMPLETE.720p.BluRay.x264-GalaxyTV[TGx] (0)
      Peaky.Blinders.S05.COMPLETE.720p.AMZN.WEBRip.x264-GalaxyTV[TGx] (0)
      physics lab@home (0)
      season 4 (0)
      semester 2 whatsapp images (0)
      semester 2 whatsapp images (41)
      System Volume Information (0)
      System Volume Information (4)
      Systems (14)
File Views
  File Types
    By Extension
      Images (1589)
      Videos (59)
      Audio (36)
      Archives (2)
      Databases (0)
```

/img_H:

113 Results

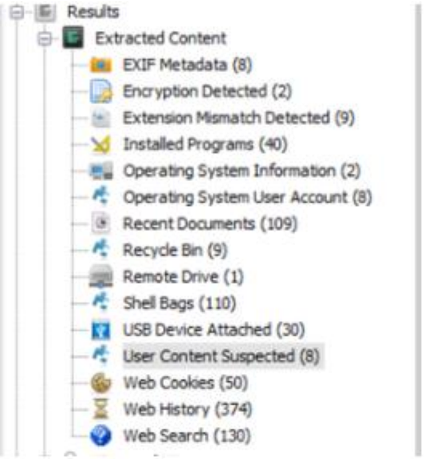
Usage: Flash Drive

OS:

Size: 31 GB

Allocated Files: 1,809

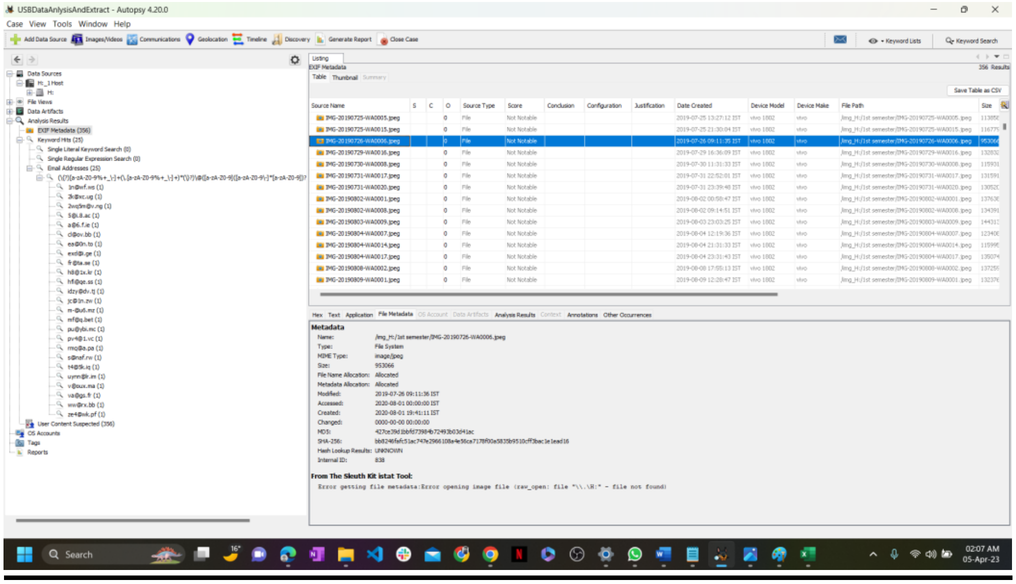
- **<u>Result</u>**



```
Results
  Extracted Content
    EXIF Metadata (8)
    Encryption Detected (2)
    Extension Mismatch Detected (9)
    Installed Programs (40)
    Operating System Information (2)
    Operating System User Account (8)
    Recent Documents (109)
    Recycle Bin (9)
    Remote Drive (1)
    Shell Bags (110)
    USB Device Attached (30)
    User Content Suspected (8)
    Web Cookies (50)
    Web History (374)
    Web Search (130)
```

- Encryption Detection: Identifies files that are password-protected or encrypted.
- Extension Mismatch Detection: Identifies files whose extensions do not match their MIME types, which may indicate suspicious activity.
- Installed Programs: Displays information about the software used on the system, extracted from the Software Registry hive.

- Operating System Information: Provides details about the operating system, gathered from the Windows Registry hive and the Software Registry hive.
- Recent Documents: Lists all documents accessed around the time the disk image was captured.
- Recycle Bin: Displays files that were temporarily stored on the system before being permanently deleted.
- Remote Drives: Shows information about all remote drives accessed using the system.
- Web Cookies: Reveals cookies that store user information from websites, providing insights into the user's online activities.
- Web History: Displays details about the user's browser history.
- EXIF Metadata: Contains all .jpg images with associated EXIF metadata that can be analyzed further.



EXIF Metadata

356 Results

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	Device Model	Device Make	File Path	Size
IMG-20190725-WA0005.jpeg			0	File	Not Notable				2019-07-25 13:27:12 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190725-WA0005.jpeg	11385
IMG-20190725-WA0015.jpeg			0	File	Not Notable				2019-07-25 21:30:04 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190725-WA0015.jpeg	11677
IMG-20190726-WA0006.jpeg			0	File	Not Notable				2019-07-26 09:11:35 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190726-WA0006.jpeg	95306
IMG-20190729-WA0016.jpeg			0	File	Not Notable				2019-07-29 16:36:09 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190729-WA0016.jpeg	13283
IMG-20190730-WA0008.jpeg			0	File	Not Notable				2019-07-30 11:31:33 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190730-WA0008.jpeg	115931
IMG-20190731-WA0017.jpeg			0	File	Not Notable				2019-07-31 22:52:01 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190731-WA0017.jpeg	131591
IMG-20190731-WA0020.jpeg			0	File	Not Notable				2019-07-31 23:39:48 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190731-WA0020.jpeg	13052
IMG-20190802-WA0001.jpeg			0	File	Not Notable				2019-08-02 00:58:47 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190802-WA0001.jpeg	13763
IMG-20190802-WA0008.jpeg			0	File	Not Notable				2019-08-02 09:14:51 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190802-WA0008.jpeg	134391
IMG-20190803-WA0009.jpeg			0	File	Not Notable				2019-08-03 23:03:25 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190803-WA0009.jpeg	14431
IMG-20190804-WA0007.jpeg			0	File	Not Notable				2019-08-04 12:19:36 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190804-WA0007.jpeg	12340
IMG-20190804-WA0014.jpeg			0	File	Not Notable				2019-08-04 21:31:33 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190804-WA0014.jpeg	11599
IMG-20190804-WA0017.jpeg			0	File	Not Notable				2019-08-04 23:31:43 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190804-WA0017.jpeg	13507
IMG-20190808-WA0002.jpeg			0	File	Not Notable				2019-08-08 17:55:13 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190808-WA0002.jpeg	13725
IMG-20190809-WA0001.jpeg			0	File	Not Notable				2019-08-09 12:28:47 IST	vivo 1802	vivo	/img_H:/1st semester/IMG-20190809-WA0001.jpeg	13237

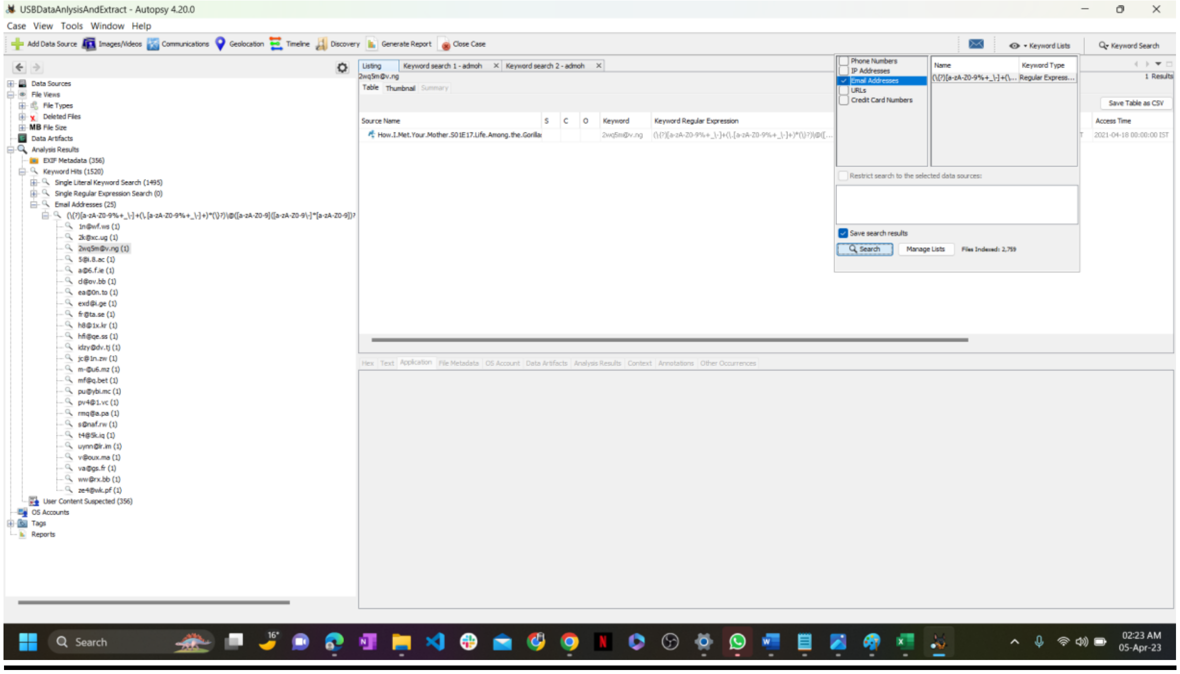
Metadata

Name:	/img_H:/1st semester/IMG-20190726-WA0006.jpeg
Type:	File System
MIME Type:	image/jpeg
Size:	953066
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2019-07-26 09:11:36 IST
Accessed:	2020-08-01 00:00:00 IST
Created:	2020-08-01 19:41:11 IST
Changed:	0000-00-00 00:00:00
MD5:	427ce39d1bbfd73984b72493b03d41ac
SHA-256:	bb8246fafc51ac747e2966108a4e56ca7178f00a5835b9510cff3bac1e1ead16
Hash Lookup Results:	UNKNOWN
Internal ID:	838

From The Sleuth Kit istat Tool:

```
Error getting file metadata:Error opening image file (raw_open: file "\\.\H:" - file not found)
```

- Keyword Hits: The disk image can be searched for specific keywords using this tool. Multiple data sources can be selected for the lookup, and the search can be narrowed down by specifying whether an exact match, substring match, or regular expression is desired. This feature can be particularly useful for finding emails or IP addresses, for example.



☐ Phone Numbers
☐ IP Addresses
☑ Email Addresses
☐ URLs
☐ Credit Card Numbers

Name	Keyword Type
(\{?)[a-zA-Z0-9%+_\-]+(\...	Regular Express...

☐ Restrict search to the selected data sources:

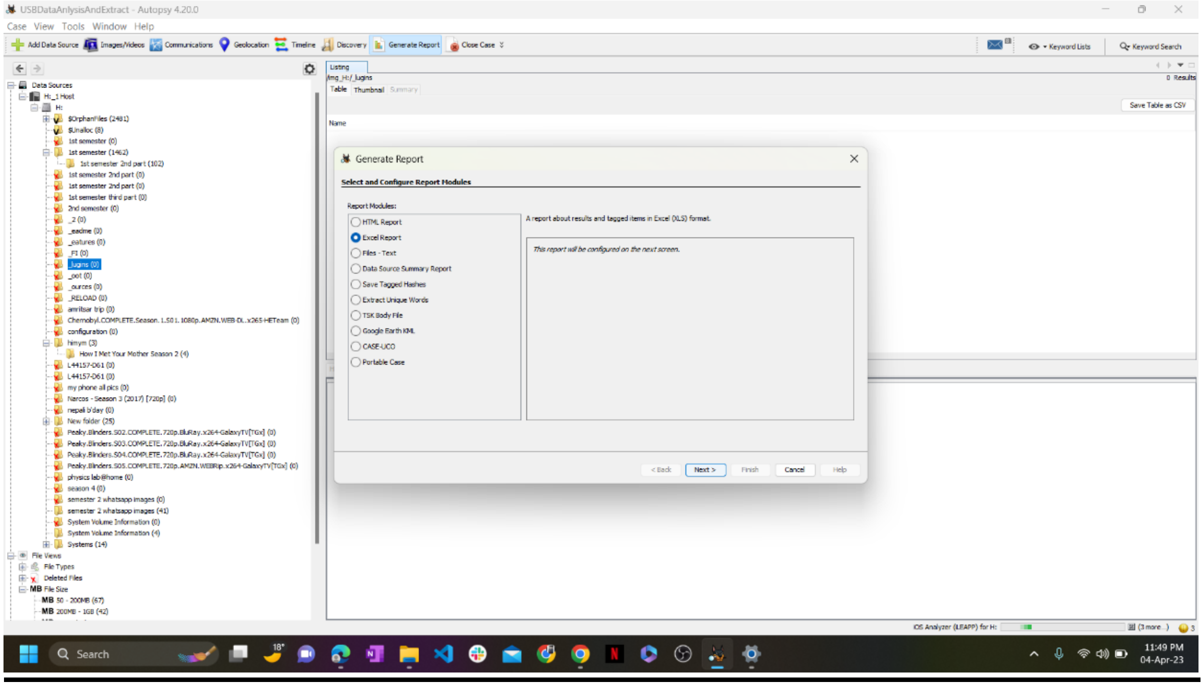
☑ Save search results

Search | Manage Lists | Files Indexed: 2,759

Source Name	S	C	O	Keyword	Keyword Regular Expression	Access Time
How.I.Met.Your.Mother.S01E17.Life.Among.the.Gorilla				2wq5m@v.ng	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...	2021-04-18 00:00:00 IST

- ## Reports:

  Reports about the entire analysis of the data source can be generated and exported in many formats.


USBDataAnlysisAndExtract - 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
H:_1 Host
H:
$OrphanFiles (2481)
$Unalloc (8)
1st semester (0)
1st semester (1462)
1st semester 2nd part (102)
1st semester 2nd part (0)
1st semester 2nd part (0)
1st semester third part (0)
2nd semester (0)
_2 (0)
_eadme (0)
_eatures (0)
_F1 (0)
_lugins (0)
_oot (0)
_ources (0)
_RELOAD (0)
amritsar trip (0)
Chernobyl.COMPLETE.Season.1.S01.1080p.AMZN.WEB-DL.x265-HETeam (0)
configuration (0)
himym (3)
How I Met Your Mother Season 2 (4)
L44157-D61 (0)
L44157-D61 (0)
my phone all pics (0)
Narcos - Season 3 (2017) [720p] (0)
nepali b'day (0)
New folder (25)
Peaky.Blinders.S02.COMPLETE.720p.BluRay.x264-GalaxyTV[TGx] (0)
Peaky.Blinders.S03.COMPLETE.720p.BluRay.x264-GalaxyTV[TGx] (0)
Peaky.Blinders.S04.COMPLETE.720p.BluRay.x264-GalaxyTV[TGx] (0)
Peaky.Blinders.S05.COMPLETE.720p.AMZN.WEBRip.x264-GalaxyTV[TGx] (0)
physics lab@home (0)
season 4 (0)
semester 2 whatsapp images (0)
semester 2 whatsapp images (41)
System Volume Information (0)
System Volume Information (4)
Systems (14)
File Views
File Types
Deleted Files
MB File Size
MB 50 - 200MB (67)
MB 200MB - 1GB (42)
Listing
/img_H:/_lugins
Table
Thumbnail
Summary
Name
0 Results
Save Table as CSV
OS Analyzer (iLEAPP) for H:
Search
11:49 PM
04-Apr-23

Generate Report

Select and Configure Report Modules

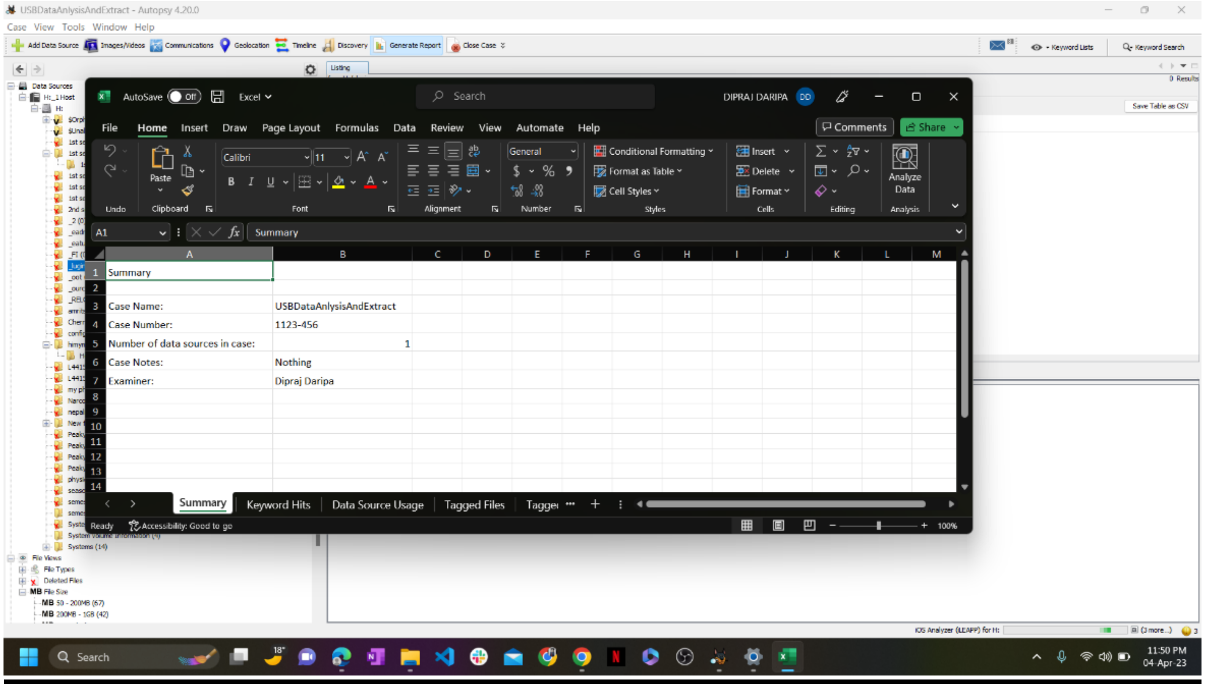
Report Modules:

○ 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 Excel (XLS) format.

This report will be configured on the next screen.

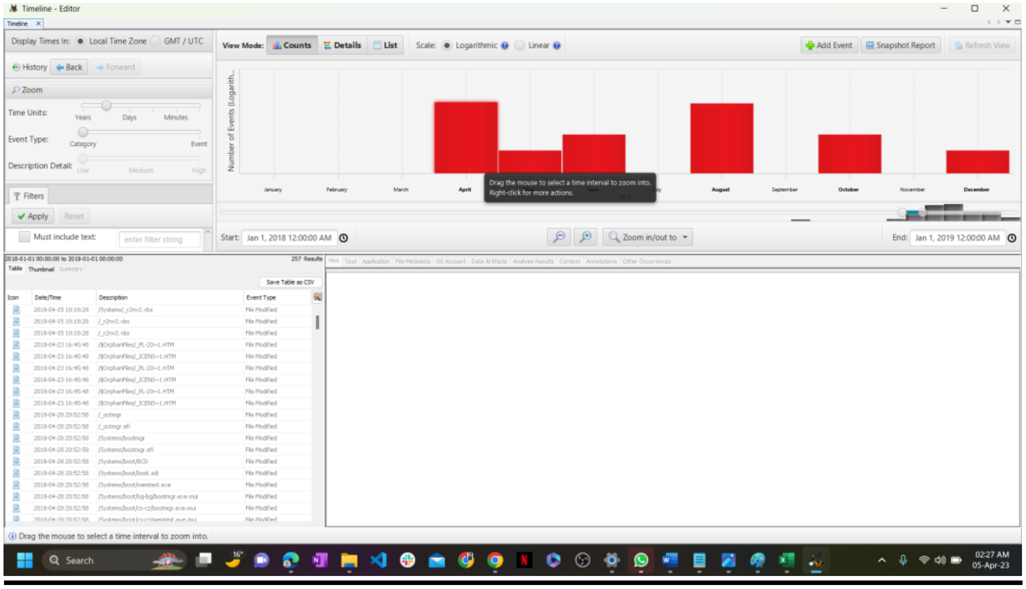
< Back | Next > | Finish | Cancel | Help



	A	B
1	Summary	
2		
3	Case Name:	USBDataAnlysisAndExtract
4	Case Number:	1123-456
5	Number of data sources in case:	1
6	Case Notes:	Nothing
7	Examiner:	Dipraj Daripa

• Additional Information :

✓ Timeline Viewer: This tool allows investigators to find information about when the computer was used and what events occurred before or after a specific event, which can be valuable in investigating events that occurred around a particular time. By analyzing the system logs and other relevant data sources, investigators can gain insight into the activities that took place on the computer leading up to and following a particular event.


Timeline - Editor
Display Times In: ● Local Time Zone ○ GMT / UTC
View Mode: Counts Details List
Scale: ● Logarithmic ○ Linear
Add Event
Snapshot Report
Refresh View
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
Number of Events (Logarith...
January
February
March
April
August
September
October
November
December
Drag the mouse to select a time interval to zoom into.
Right-click for more actions.
Start: Jan 1, 2018 12:00:00 AM
Zoom in/out to
End: Jan 1, 2019 12:00:00 AM
02:27 AM
05-Apr-23

2018-01-01 00:00:00 to 2019-01-01 00:00:00 257 Results

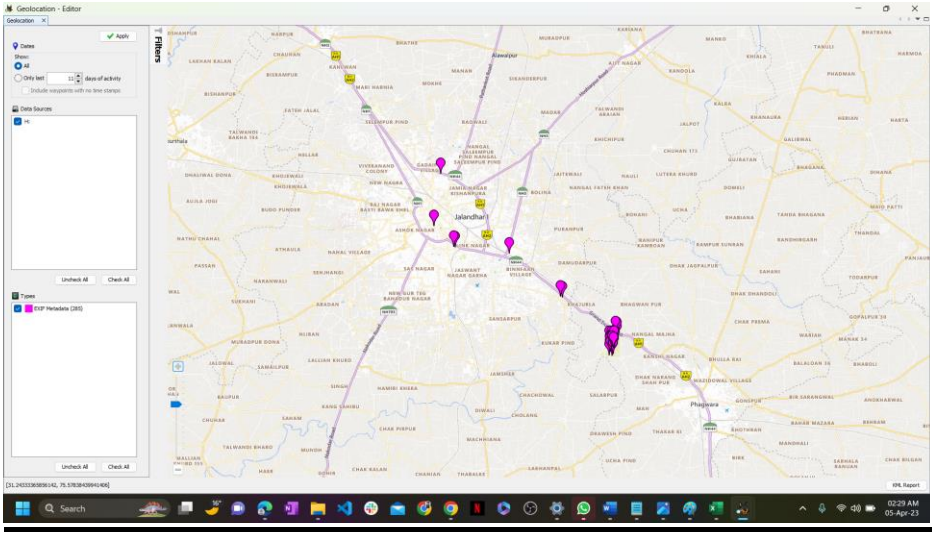
Table Thumbnail Summary

Save Table as CSV

Icon	Date/Time	Description	Event Type
	2018-04-15 10:18:28	/Systems/_r2nv2.vbs	File Modified
	2018-04-15 10:18:28	/_r2nv2.vbs	File Modified
	2018-04-15 10:18:28	/_r2nv2.vbs	File Modified
	2018-04-23 16:45:48	/$OrphanFiles/_PL-20~1.HTM	File Modified
	2018-04-23 16:45:48	/$OrphanFiles/_ICENS~1.HTM	File Modified
	2018-04-23 16:45:48	/$OrphanFiles/_PL-20~1.HTM	File Modified
	2018-04-23 16:45:48	/$OrphanFiles/_ICENS~1.HTM	File Modified
	2018-04-23 16:45:48	/$OrphanFiles/_PL-20~1.HTM	File Modified
	2018-04-23 16:45:48	/$OrphanFiles/_ICENS~1.HTM	File Modified
	2018-04-28 20:52:58	/_ootmgr	File Modified
	2018-04-28 20:52:58	/_ootmgr.efi	File Modified
	2018-04-28 20:52:58	/Systems/bootmgr	File Modified
	2018-04-28 20:52:58	/Systems/bootmgr.efi	File Modified
	2018-04-28 20:52:58	/Systems/boot/BCD	File Modified
	2018-04-28 20:52:58	/Systems/boot/boot.sdi	File Modified
	2018-04-28 20:52:58	/Systems/boot/memtest.exe	File Modified
	2018-04-28 20:52:58	/Systems/boot/bg-bg/bootmgr.exe.mui	File Modified
	2018-04-28 20:52:58	/Systems/boot/cs-cz/bootmgr.exe.mui	File Modified
	2018-04-28 20:52:58	/Systems/boot/cs-cz/memtest.exe.mui	File Modified

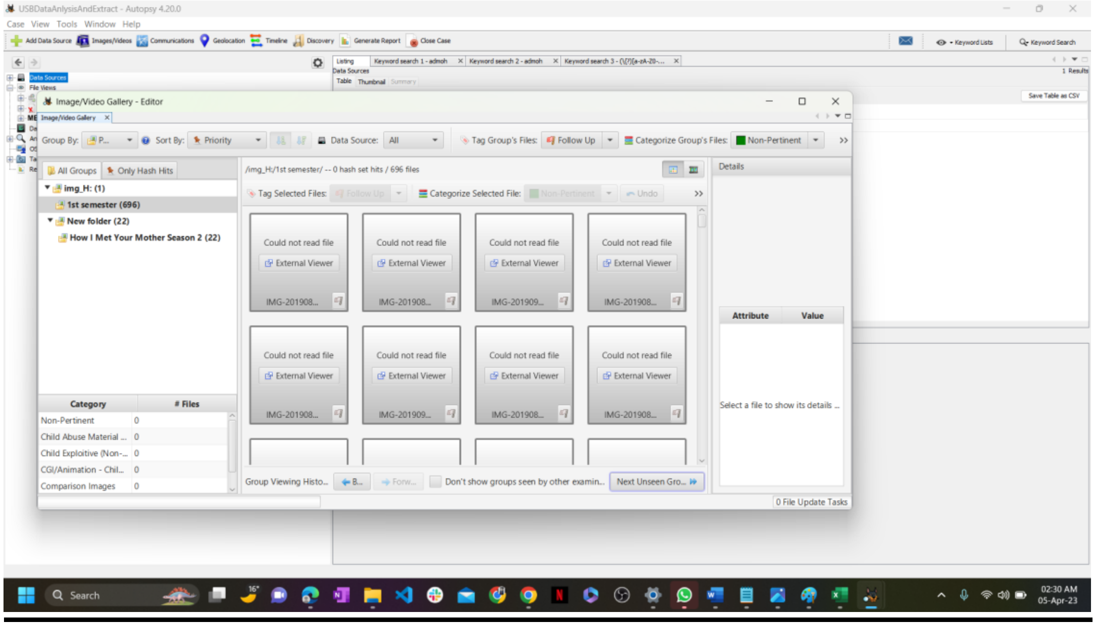
Drag the mouse to select a time interval to zoom into.

- ✓ Geolocation Viewer: In this window, artifacts with longitude and latitude attributes are displayed as waypoints on a map. However, if the data source does not contain any artifacts with such attributes, no waypoints will be displayed on the map.



- ✓ Images/Videos Viewer: This tool provides a Gallery View feature that allows users to view images and videos contained in the data source. In Gallery View, the information is presented in the form of attribute-value pairs, providing users with easy access to relevant metadata about each item.

- ✓



Category	# Files
Non-Pertinent	0
Child Abuse Material ...	0
Child Exploitive (Non-...	0
CGI/Animation - Chil...	0
Comparison Images	0

4. BIBILIOGRAPHY

i. google.com

ii. wikipedia.org

iii. autopsy.com

iv. geeksforgeeks.org

GitHub Link -> MyGitHubRepolink