INT 301

CA-3

OPEN-SOURCE TECHNOLOGIES

Detailed Information on

Disk Forensics

Name : Dipraj Daripa

Reg No. : 11911828

Program : B.Tech CSE

Semester : 8Th sem

School : Computer Science and Engineering

Faculty :

Date of submission : 6^{h} 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 :
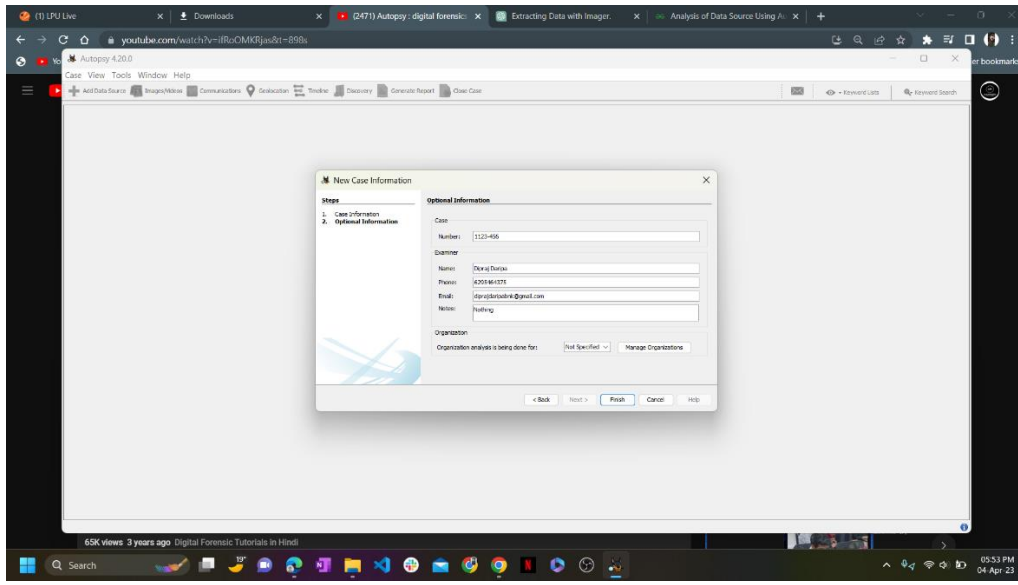Open Autopsy and create a new case.
You can Open a recent case or open any case.
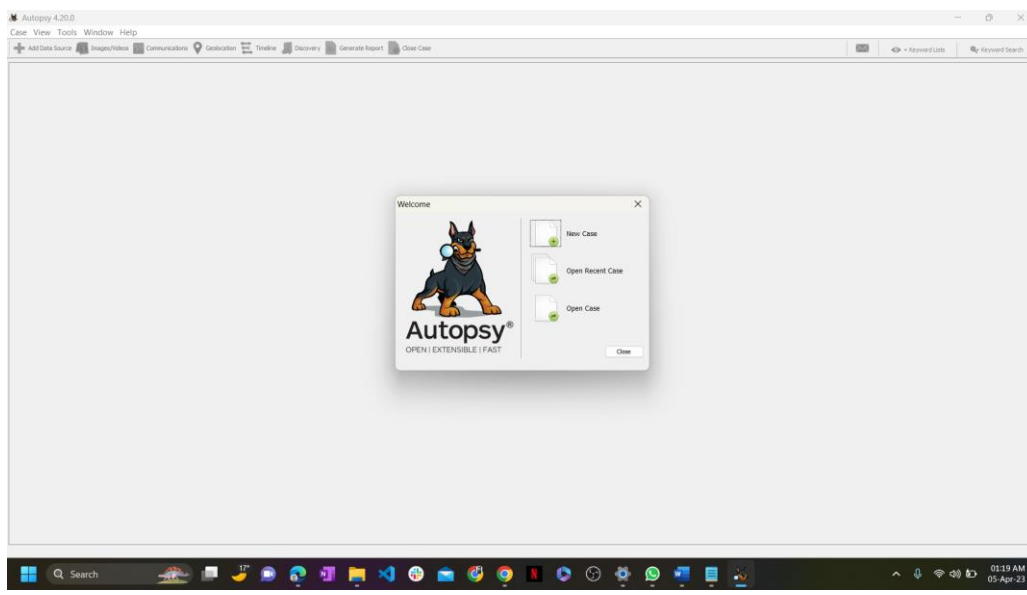
3.2 Optional System Information:
First you need to create a case Number for this.
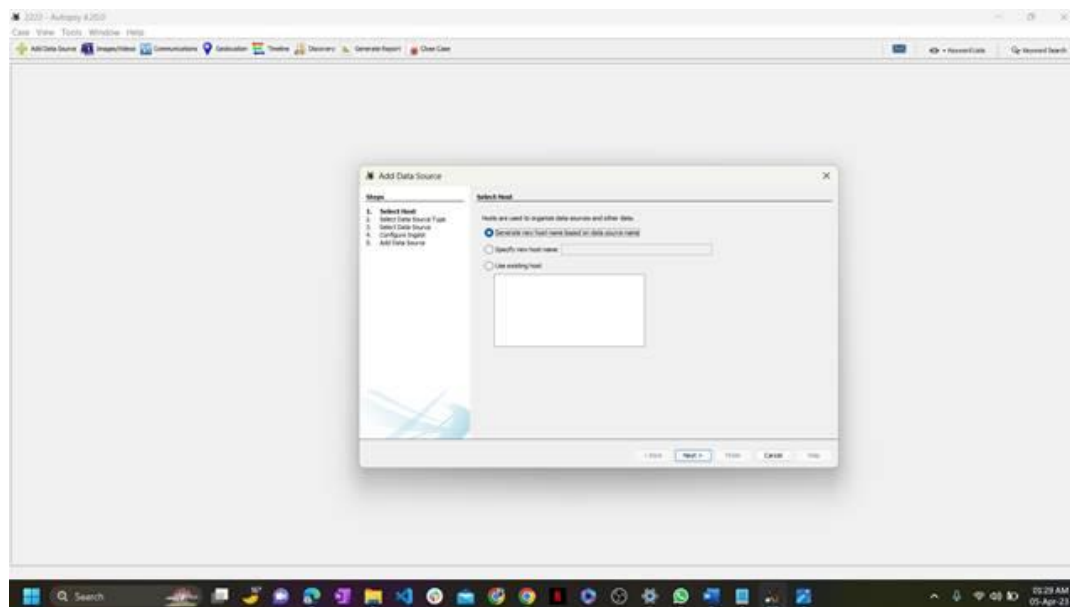Then Put the detail of the exminner.

3.3 Add Data Source:

Select the appropriate data source .

Step 1)

Select the 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.
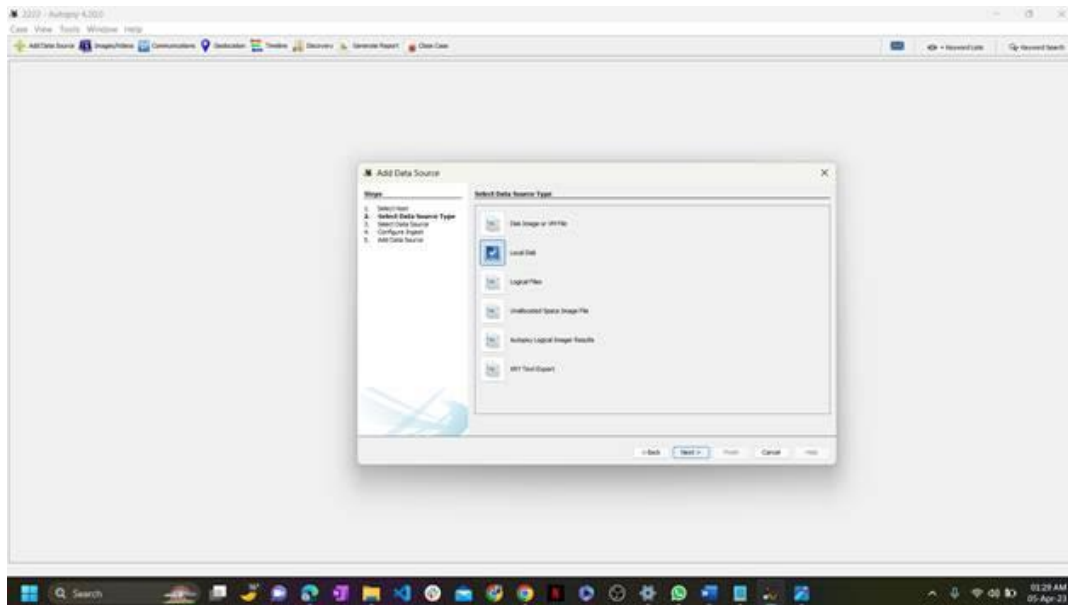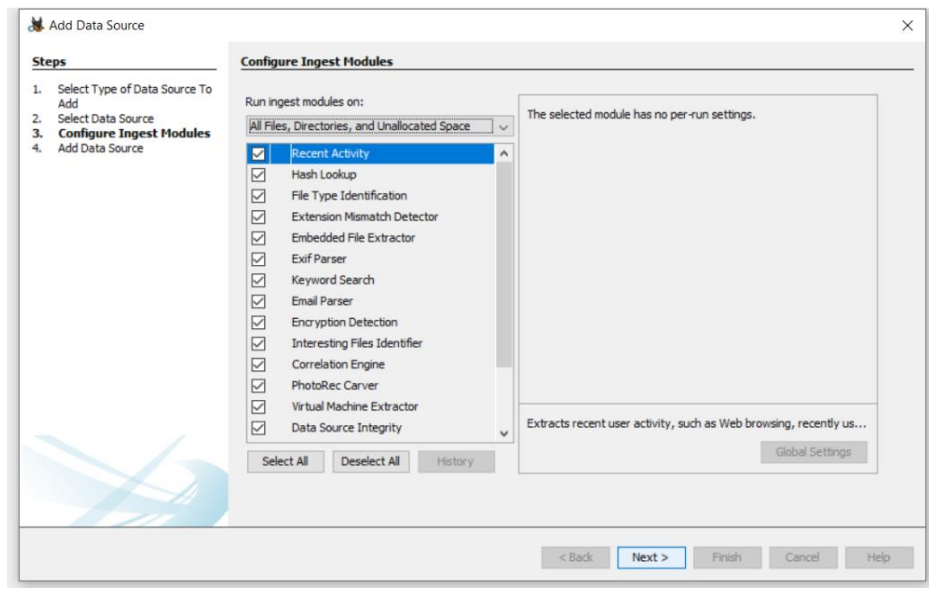

Step 3)

Select the data Source

Which data Source You want to analysis.
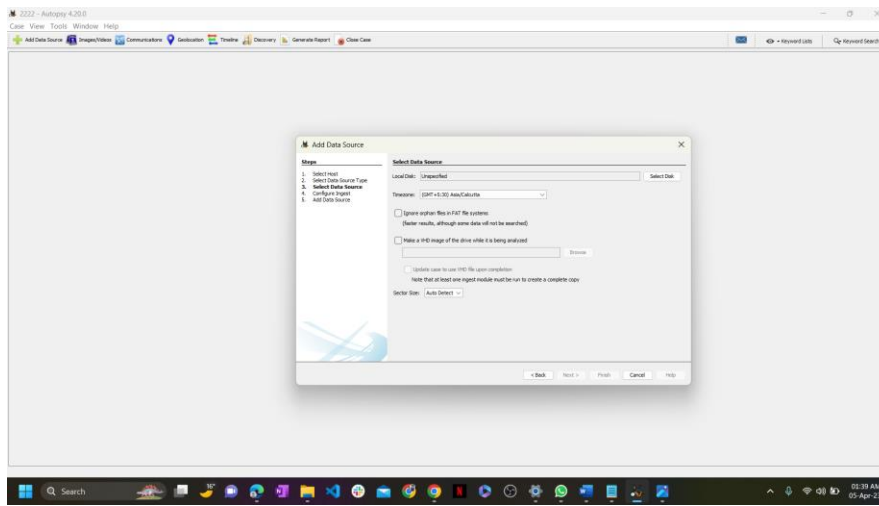
Step 4)

Configure ingest modules.

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.
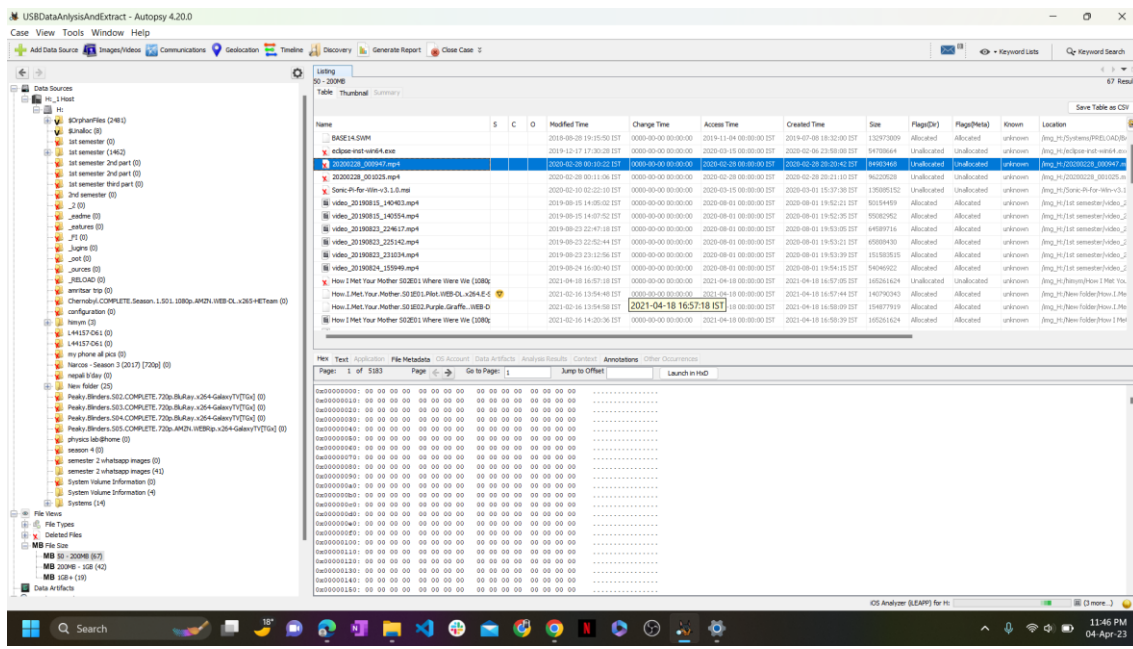- Android Analyzer: Analyzes SQLite and other files from an Android device.

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.

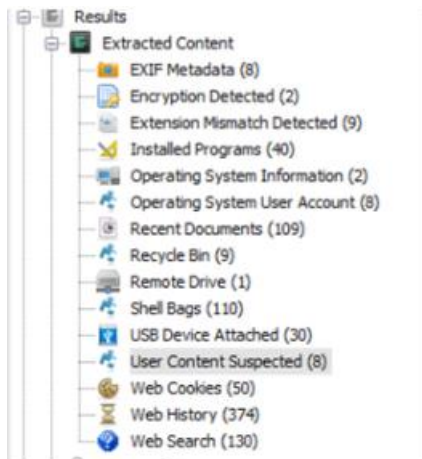## 3.4   Exploring the Data Source:

- 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:

Meta data:

- **Extracted Deleted File Data**: 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.

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

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

- **Result**

o Encryption Detection: Identifies files that are password-protected or encrypted.

o Extension Mismatch Detection: Identifies files whose extensions do not match their MIME types, which may indicate suspicious activity.

o Installed Programs: Displays information about the software used on the system, extracted from the Software Registry hive.

o Operating System Information: Provides details about the operating system, gathered from the Windows Registry hive and the Software Registry hive.

o Recent Documents: Lists all documents accessed around the time the disk image was captured.

o Recycle Bin: Displays files that were temporarily stored on the system before being permanently deleted.

o Remote Drives: Shows information about all remote drives accessed using the system.

o Web Cookies: Reveals cookies that store user information from websites, providing insights into the user's online activities.

o Web History: Displays details about the user's browser history.

o EXIF Metadata: Contains all .jpg images with associated EXIF metadata that can be analyzed further.

o 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.

- **Reports:**

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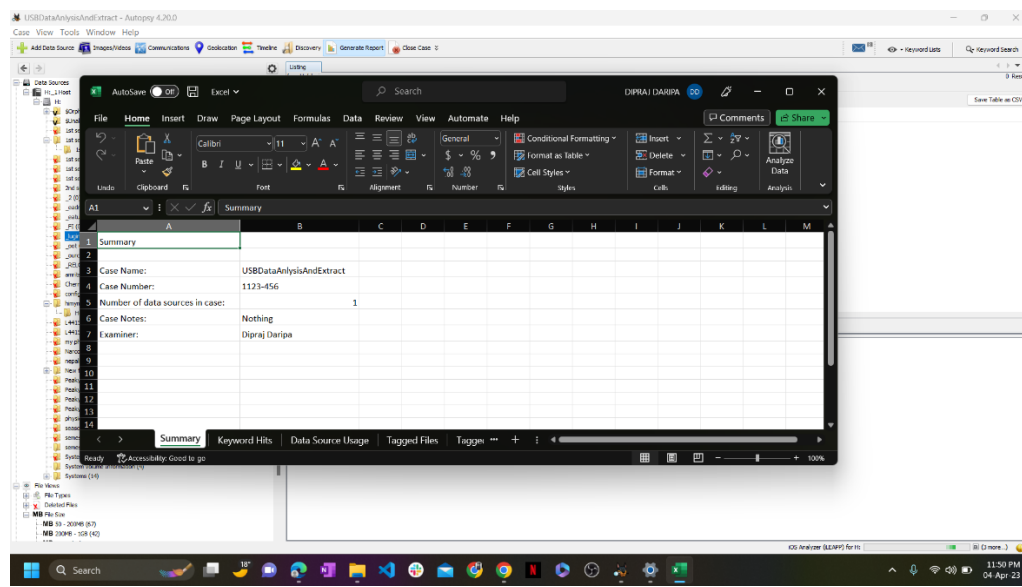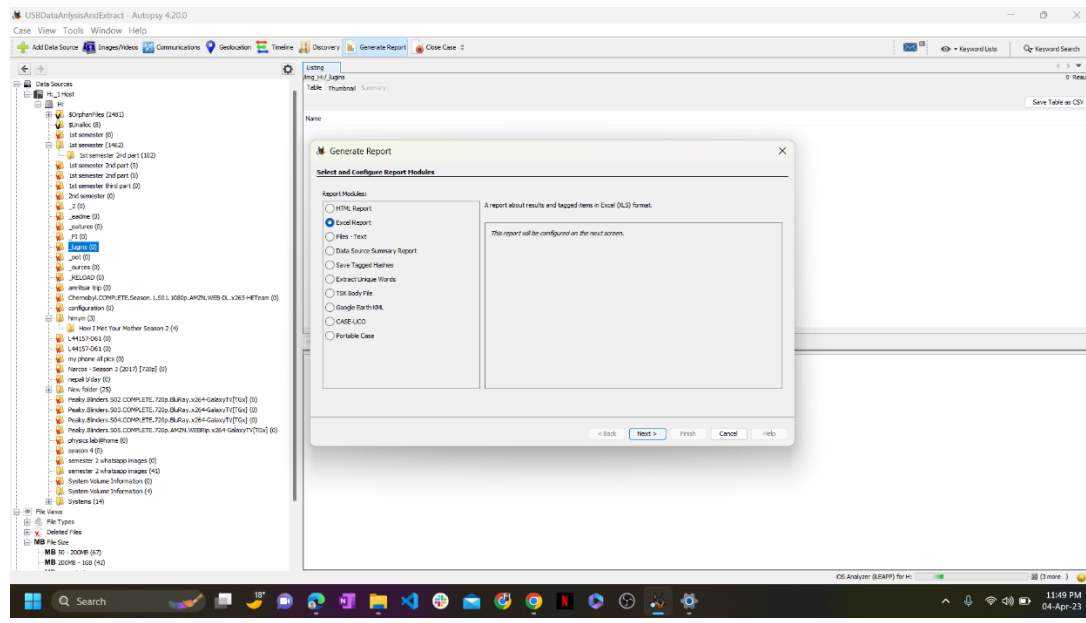

- **Additional Information :**

✓ 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.
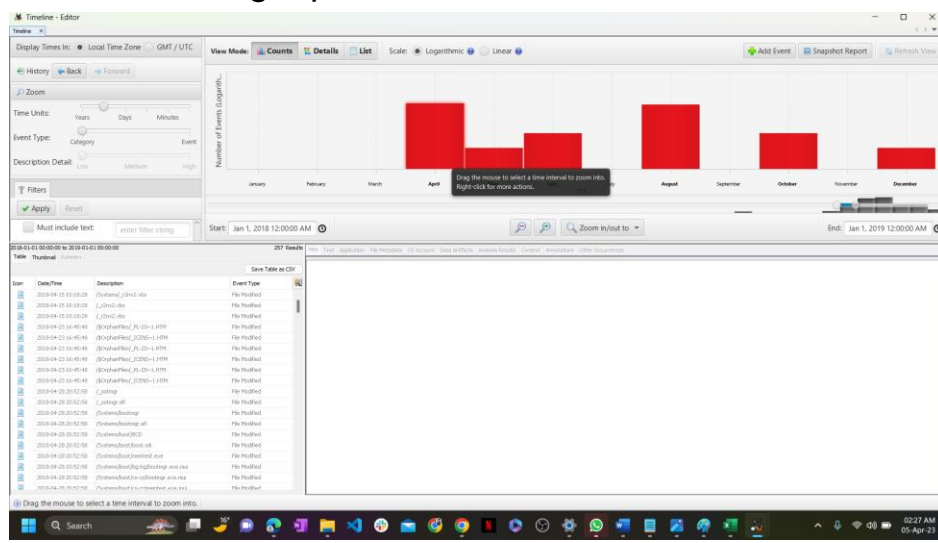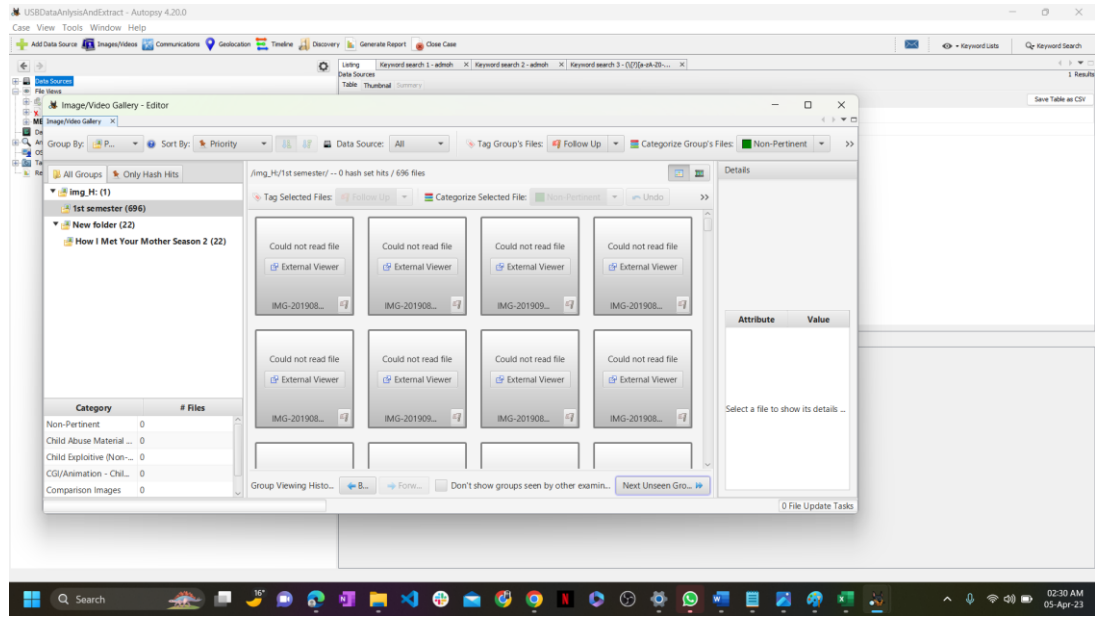

✓ Geolocation Viewer: In this window, artifacts with longitude and latitude attributes are displayed as waypoints on a map. However, if the data source does not contain any artifacts with such attributes, no waypoints will be displayed on the map.
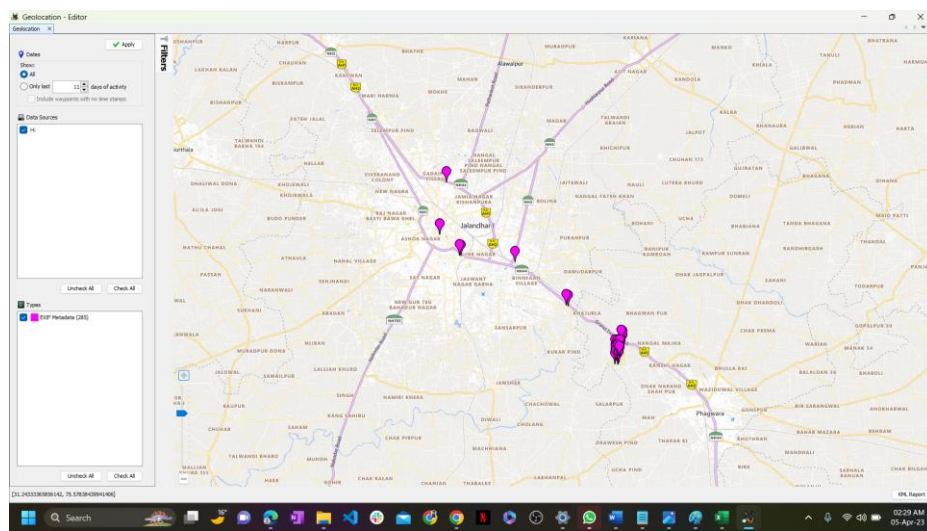
✓ Images/Videos Viewer: This tool provides a Gallery View feature that allows users to view images and videos contained in the data source. In Gallery View, the information is presented in the form of attribute-value pairs, providing users with easy access to relevant metadata about each item.

✓

4. BIBILIOGRAPHY

i.   google.com
ii. wikipedia.org
iii. autopsy.com
iv. geeksforgeeks.org