Digital Forensic Project at Luke Tech Limited, Canada

Assignment 1: Evidence Analysis

1.Describe the steps involved in analyzing digital evidence during a forensic investigation.

1. **Identification**: The first thing is to identify the devices containing the data that will be used for the investigation e.g laptop, desktop, mobile phone, tablet
   These devices are seized and kept in a secured place so as to prevent anyone from tampering with it.
2. **Preservation**: After the devices have been seized and isolated the next thing is to extract and preserve the data found from the devices found which should be isolated, secured and not to be tampered with.
3. **Analysis**: After extracting the relevant data from the devices to be used as digital evidence the next step is to examine and bring out the clues or points that will ebe used in the investigation,
4. **Documentation**: The next is to document the findings conducted from the analysis of data used in the investigation. The documentation will show how the various activities carried out by the investigator on the evidence.
5. **Presentation**: Once the investigation is complete, the findings will be presented to the court if the case is genuine or not.

2.What techniques can be used to identify and authenticate digital evidence?

Cryptographic Hashing Algorithm is the technique used to ensure that the digital evidence has not been altered or modified just to ensure data integrity.

3.Explain the importance of maintaining the integrity of digital evidence during the analysis process

Integrity of digital evidence means the data collected on the digital device be have not been tampered with/modified/altered so that the evidence can be admissible in the court of law.

4.How would you approach the analysis of file systems and deleted files to uncover relevant information?

- **Reverse Steganography**: a technique used to extract hidden data by examining the underlying hash or string of characters representing an image or other data item
- **File or Data Carving**: identifying and recovering deleted files by searching for the fragments that deleted files may leave
- **Keyword Searches**: using keywords to identify and analyze information relevant to the investigation, including deleted data

.

5.Discuss the significance of examining volatile memory in a digital forensic investigation

It can reveal information about active malware, hidden processes, encrypted data in memory, or remnants of deleted files, offering a wealth of evidence that can be crucial to an investigation.

6. How can digital artefacts such as emails, chat logs, and browser history be recovered and analyzed?

Artefacts like emails, chat logs and browser history can be recovered and analyzed using autopsy forensic tool.
It depends on the digital devices that's being used as evidence in the investigation. For example if it is through a suspect data (Hard disk drive for example) after recovering all the data from the device. There is a section called artefacts that contains all this information's which can be viewed.

7. What is metadata, and why is it important in digital forensic analysis?

   Metadata is used to describe various hidden information created along with documents, photographs and computer smartphones or tablets.

   It allows forensic data analyst to make accurate timelines and resolve civil and criminal disputes provide additional information, authenticate and preserve integrity of the evidence

Assignment 2: Reporting Evidence

1. What are the key elements that should be included in a digital forensic report?

   The key elements are: Title, Table of Contents, Overview/Case/Case Summary, Evidence, Objectives, Steps taken during an investigation (forensic Analysis), Tools Used, Appendices, Relevant findings, Exhibit

2. How would you structure a report to present the findings of a digital forensic investigation?

   The first thing I will do before presenting my findings is to document the report, After that I will write a report to present my findings. The report will contain the title of the investigation, table of contents will cover the body of the report like chapters and its contents, page numbers etc, An executive summary summarizing the case, forensic analysis and other elements that should be in the report. The report will be used in the court of law to prove or deny a case.

3. Discuss the importance of clear and concise language in a forensic report

   It ensures effective communication, reduces ambiguity and helps convey the message without any confusion.

4. Explain the role of visual aids, such as diagrams or screenshots, in supporting the findings in a report.

Visual aids allows the audience to understand things easily without wasting much time and effort.

5. How should you handle sensitive or confidential information in a forensic report?
   Sensitive or Confidential Information can be handled in the following ways

   - Get informed consent: Whenever possible, investigators should obtain informed consent from individuals before collecting or analyzing their personal information.
   - Use secure methods for collecting and storing data: Data should be collected and stored using secure methods, such as encryption and password protection.
   - Limit access to sensitive information: Only authorized personnel should have access to sensitive information.
   - Be mindful of data disposal: When data is no longer needed, it should be disposed of securely to prevent unauthorized access.

6. What are the potential challenges in preparing a report for non-technical stakeholders?

   The challenges are finding it difficult to understand the forensics terminology, not familiar with how to use the forensics tools either hardware/software, Report might be difficult for them to comprehend.

7. Discuss ethical considerations and best practices when reporting digital forensic findings

   - Protection of Right and Privacy

   Digital Forensics code of ethics is essential to make sure that the privacy and rights of an individual keeps safe during the process of investigation.

   - Ensuring Legal Compliance

   Performing Digital Forensics under a court's jurisdiction is essential. Ethics in digital forensics is important to make sure that all the investigation is taking place under the premise of the court of law or under the legal and regulatory requirements.

   - Building Trust and Authenticity

   Digital Forensics ethics are essential to build trust and credibility between the forensics investigators and the client. It ensures that the investigation takes place with no bias or modification. It is completely fair and pure from the point of extracting trust.

   - Compliance

Investigators must comply with all legal and ethical requirements related to digital forensics. They must also follow their organizations or client's policies and procedures.

- Objectivity

Digital forensic investigators must be impartial and objective in their investigations. You must avoid any bias, or conflict of interest that could influence your judgement.

- Confidentiality

Every piece of information found during the investigation is kept confidential in accordance with digital forensics ethics. Unless required by law, an authorized client, or an organization, no information will be divulged.

- Competence

Researchers should have the necessary knowledge, skills and training to do their job competently. They must constantly update their skills and knowledge to keep up with advances in technology and maintain digital forensics ethics.

- Respect

Investigators should treat all parties involved in an investigation with respect and professionalism. You must respect the privacy and human rights of individuals and not discriminate based on race, gender, religion or any other factor.

These principle ethics in digital forensics helps to ensure that the investigations are conducted ethically and professionally with proper protection of privacy, integrity, without any biases and maintain the credibility of the investigation process.

8. Provide an example of a well-written conclusion section in a digital forensic report.

After examining the device (Hard Disk Drive), It was discovered that Microsoft edge browser was accessed with the username: achebody@gmail.com at 9:05am on 15/09/2024 and data artefacts containing the chat histories, web histories, hacking applications and other software's for gaining access into the company's website were deleted and cleared from the browser history.

Assignment 3: Data Acquisition and Recovery

1. Explain the difference between physical and logical data acquisition in digital forensics

   Logical acquisition involves collecting files that are specifically related to the case under investigation. This technique is typically used when an entire drive or network is too large to be copied while physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory chip)". direct communication with a device's internal data storage to collect the stored data. It is a type of data collection that includes system files, application data, and other information, that is not accessible to the user via the GUI of the device.

2. What are the primary methods and tools used for data acquisition from different types of devices?

   The Primary Methods are Invasive and Noninvasive Methods.

   The tools used for data acquisition from different types of devices are: Manual Extraction, Logical Analysis, Hex Dump/JTAG, Chip-Off, Micro Read

3. Discuss the challenges and considerations when acquiring data from mobile devices

- Differences in hardware:

Mobile devices come in all shapes and sizes, with different types of hardware. This can make it difficult to develop mobile forensics tools that work on all devices.

- Password security and encryption:

Many mobile devices are password-protected and encrypted, making data recovery and mobile forensics difficult.

- Mobile operating systems**:**

There are many different mobile operating systems, each with its own file system and data storage methods. This can make data acquisition and interpretation difficult.

- Accidental device reset:

One of the most common problems mobile forensics experts face is when a user accidentally resets their device. This can delete all the data on the device, making it difficult to recover.

- Lack of tools and equipment:

Mobile forensics is still a relatively new field, and relatively few tools exist. This makes it difficult to perform mobile forensics efficiently.

- Anti-forensic techniques:

As mobile forensics becomes more popular, criminals are also becoming more aware of it and are using anti-forensic techniques to prevent their data from being recovered.

- Mobile platform security features:

Many mobile devices have built-in security features that can make data recovery difficult. For example, Apple's iPhone has a "Secure Enclave" feature that encrypts all the data on the device.

- Preventing data modification:

One of the goals of mobile forensics is to preserve the data on a mobile device so it can be used as evidence in court. However, this can be difficult if the data is constantly modified. Many mobile devices automatically delete old data to make room for new data. This can make it difficult to recover deleted data.

- Dynamic nature of evidence:

Mobile devices are constantly changing, making it difficult to keep track of all the data on a device. A user might install a new app or delete an old one, which can change the data on the device. This makes it difficult to know what data is relevant and what isn't.

- Device alteration:

Mobile devices can be easily altered. For example, a user might root their device, which modify's the default data on the device and make it difficult to recover.

- Communication shielding:

This is when a user uses a mobile device to communicate with someone they don't want to be tracked. For example, they might use a burner phone or an encrypted messaging app. This can make it difficult to recover the data from the mobile device.

- Malicious programs:

These programs are designed to prevent mobile forensics experts from accessing data on a mobile device. For example, a user might install a program that encrypts all the data on their device.

- Legal issues:

Mobile forensics can be used to recover a lot of sensitive data which can be used in a court case. However, many laws govern how this data can be used. For instance, there are laws that protect a user's privacy.

4. What techniques can be employed to recover deleted files and folders from a storage device

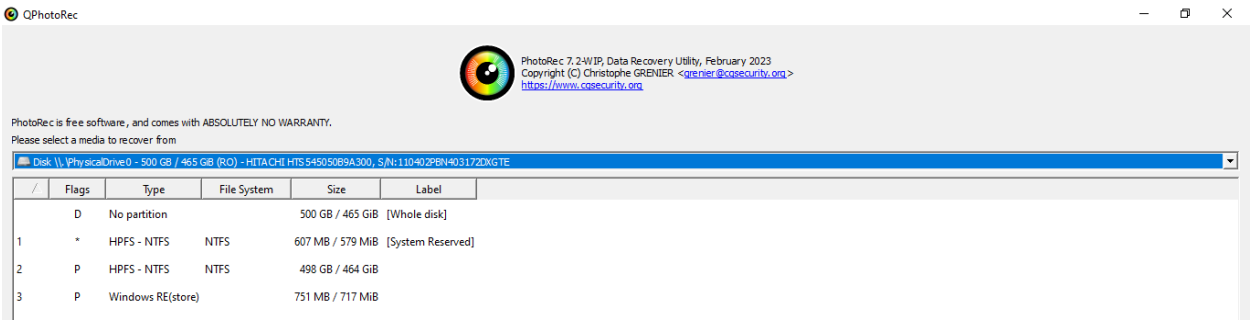
Deleted Files and Folders from a storage folder can be recovered using data recovery tools like photorec and Autopsy

5. Describe the process and limitations of using PhotoRec for data recovery.

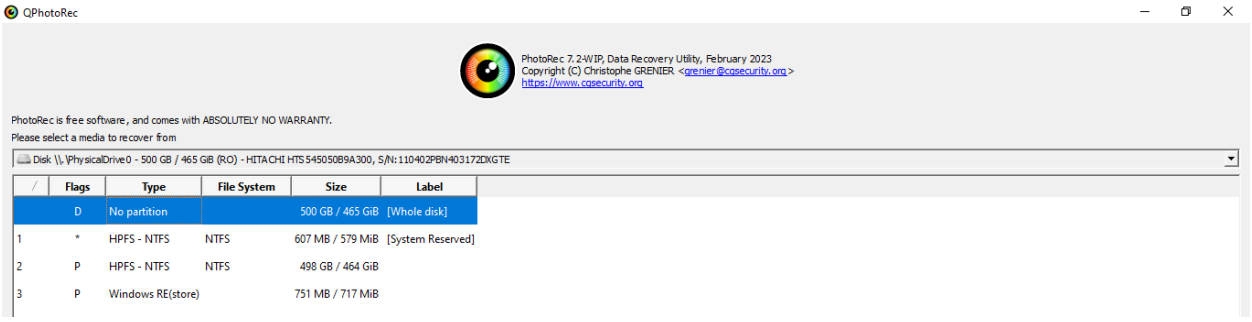
   The process of using PhotoRec for data recovery are using window OS

   - Download and Install the PhotoRec on your computer

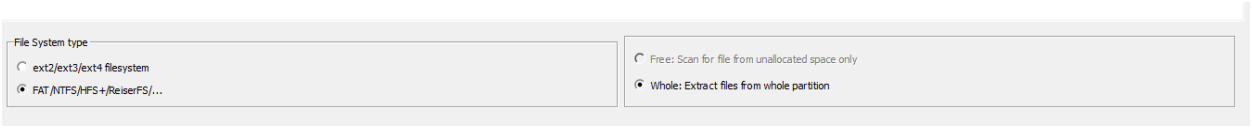
   - Launch the software on the computer and choose the storage you want to recover the lost data which could be internal or external drive: USB drive, Hard disk, Memory card, Select the appropriate option and proceed



- Choose the file system type

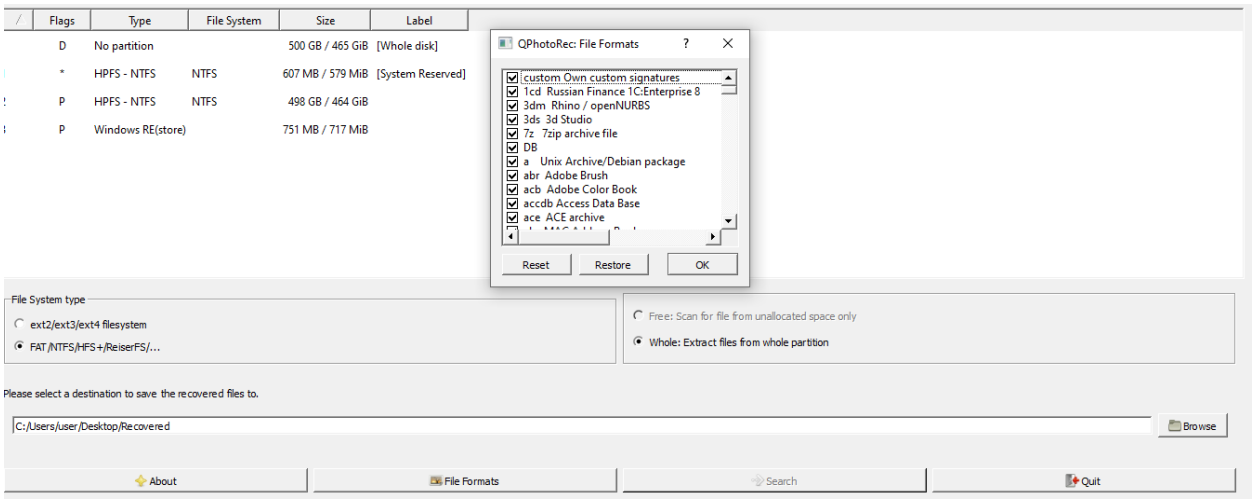


- Choose the Partition and File type

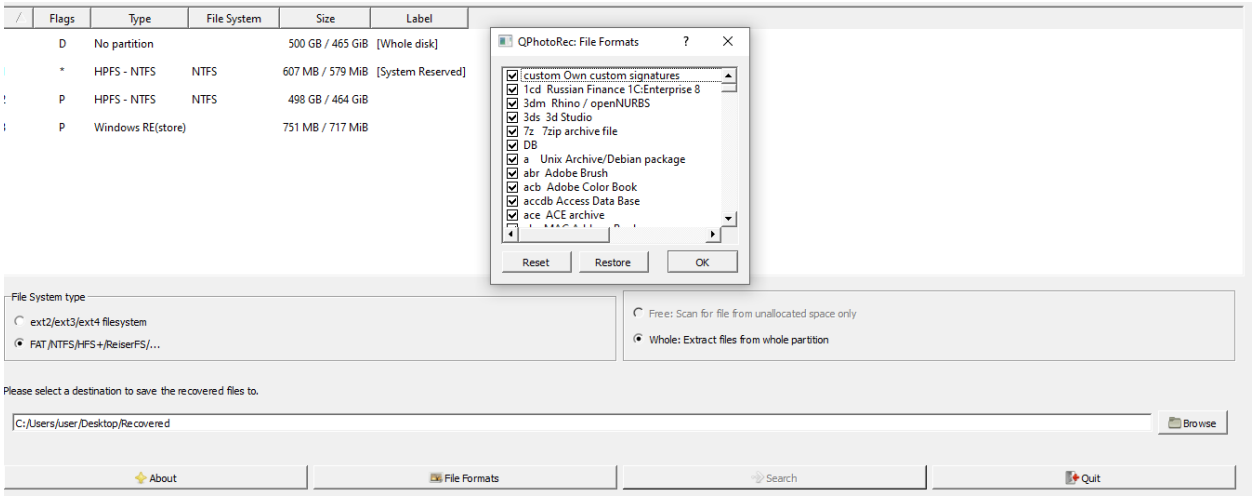


- Select the destination where the recovered data will be saved

- Select file formats like pdf, doc, png etc



- Click on Search button to start the recovery process



The limitations of using PhotoRec are:

- Poor Customer support
- Obsolete graphical interface with an elementary command-line aesthetic.

6. Explain the concept of carving and its relevance in digital forensic investigations.

Carving is the act of recovering a file from unstructured digital forensic images. The term unstructured indicates that the original digital image does not contain useful file system information which may be used to assist in this recovery.

which is a general term for extracting structured data out of raw data, based on format specific characteristics present in the structured data

Its relevance in digital forensic investigations recovering files and fragments of files when directory entries are corrupt or missing

7. Discuss the capabilities and features of the Autopsy digital forensics tool.

    - The capabilities of autopsy are that it has been able to meet up with the demand of modern investigative process as the technology is evolving.

    - It is versatile ranging from extracting hidden information's, web artefacts, managing cases and even support law enforcement agency in sourcing for digital evidence with its different Features.

    - It is Reliable and it is open source free and accessible to wide range of users.

    Features of Autopsy are:

- Multi-User Cases: Collaborate with fellow examiners on large cases.

- Timeline Analysis: Displays system events in a graphical interface to help identify activity.

- Keyword Search: Text extraction and index searched modules enable you to find files that mention specific terms and find regular expression patterns.

- Web Artifacts: Extracts web activity from common browsers to help identify user activity.

- Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices.

- LNK File Analysis: Identifies short cuts and accessed documents

- Email Analysis: Parses MBOX format messages, such as Thunderbird.

- EXIF: Extracts geo location and camera information from JPEG files.

- File Type Sorting: Group files by their type to find all images or documents.

- Media Playback: View videos and images in the application and not require an external viewer.

- Thumbnail viewer: Displays thumbnail of images to help quick view pictures.

- Robust File System Analysis: Support for common file systems, including NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.

- Hash Set Filtering: Filter out known good files using NSRL and flag known bad files using custom hashsets in HashKeeper, md5sum, and EnCase formats.

- Tags: Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.

- Unicode Strings Extraction: Extracts strings from unallocated space and unknown file types in many languages (Arabic, Chinese, Japanese, etc.).

- File Type Detection based on signatures and extension mismatch detection.

- Interesting Files Module will flag files and folders based on name and path.

- Android Support: Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more.

- Input Formats

  Autopsy analyzes disk images, local drives, or a folder of local files. Disk images can be in either raw/dd or E01 format. E01 support is provided by libewf.

  - Reporting

  Autopsy has an extensible reporting infrastructure that allows additional types of reports for investigations to be created. By default, an HTML, XLS, and Body file report are available. Each are configurable depending on what information an investigator would like included in their report:

- HTML and Excel: The HTML and Excel reports are intended to be fully packaged and shareable reports. They can include references to tagged files along with comments and notes inserted by the investigator as well as other automated searches that Autopsy performs during ingest. These include bookmarks, web history, recent documents, keyword hits, hashset hits, installed programs, devices attached, cookies, downloads, and search queries.

- Body File: Primarily for use in timeline analysis, this file will include MAC times for every file in an XML format for import by external tools, such as mactime in The Sleuth Kit.

An investigator can generate more than one report at a time and either edit one of the existing or create a new reporting module to customize the behavior for their specific needs.

8. How would you handle encrypted data during the data acquisition and recovery process

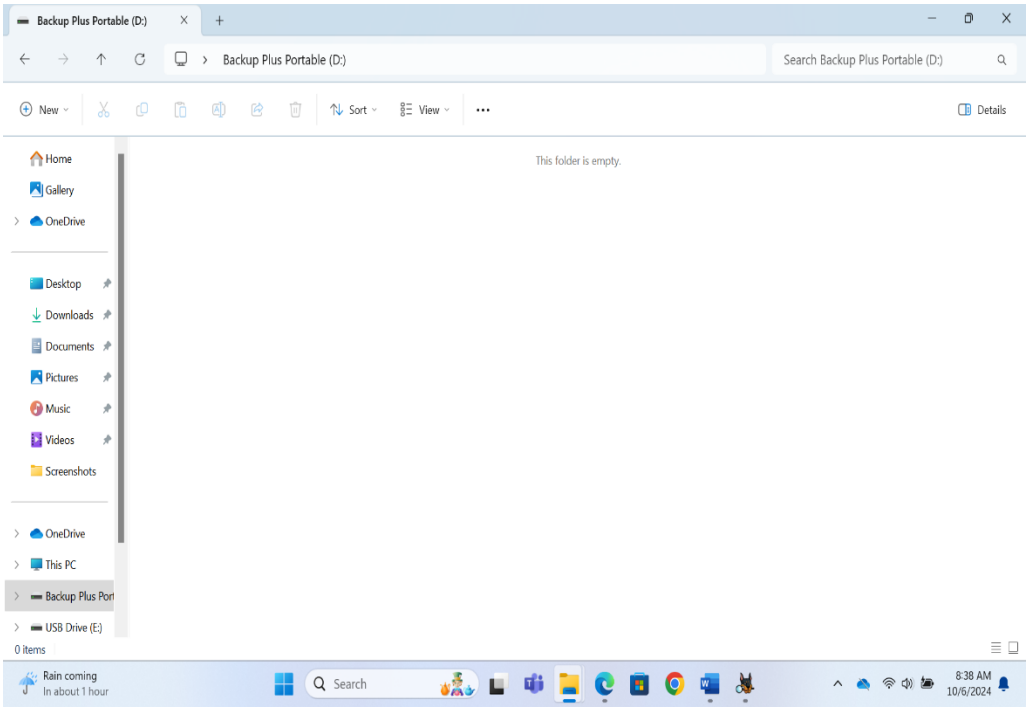
Encrypted data are sensitive data or information's that have been protected from an unauthorized person. In a situation whereby I come across an encrypted data during data acquisition recovery process and the encrypted data is the evidence we are looking for in the suspect data/suspect device during digital investigation. I will decrypt the device using BitLocker drive encryption on my laptop so as to have access to the data stored on the device.

Practical Assignment

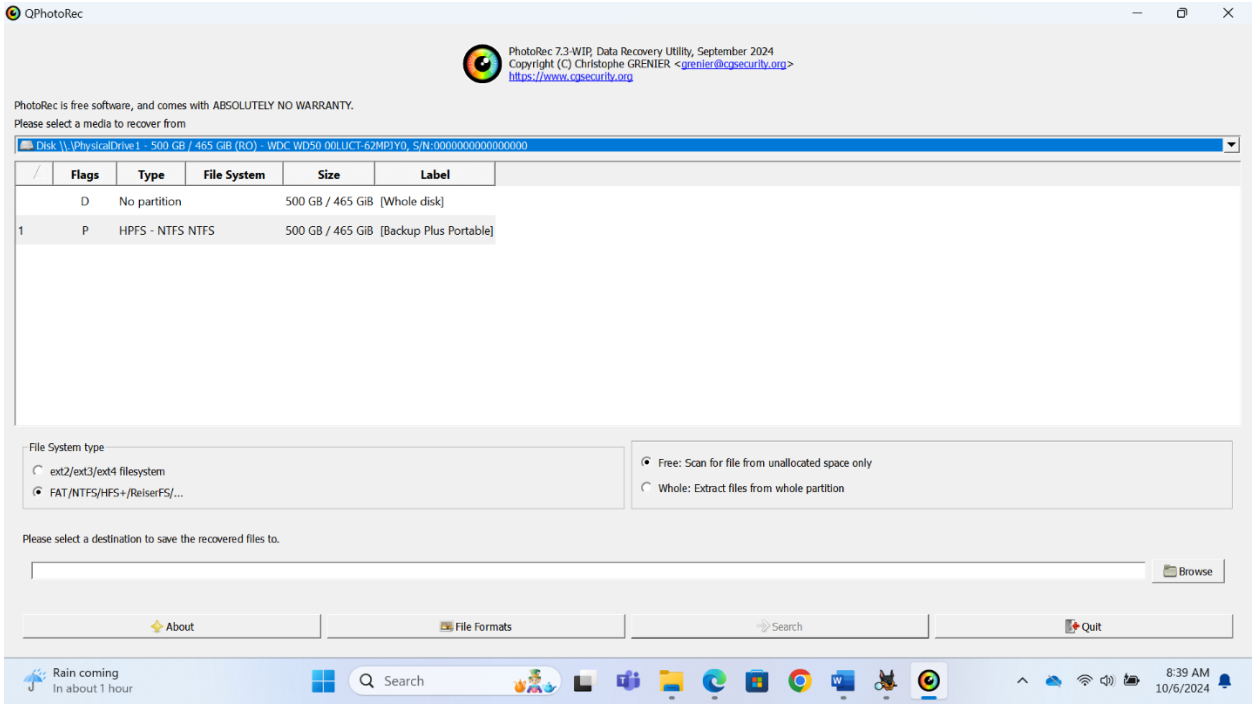
Forensic Analysis on a USB Drive D: using PhotoRec

- Task: Recover deleted files and any other intriguing elements you may come across using Photorec

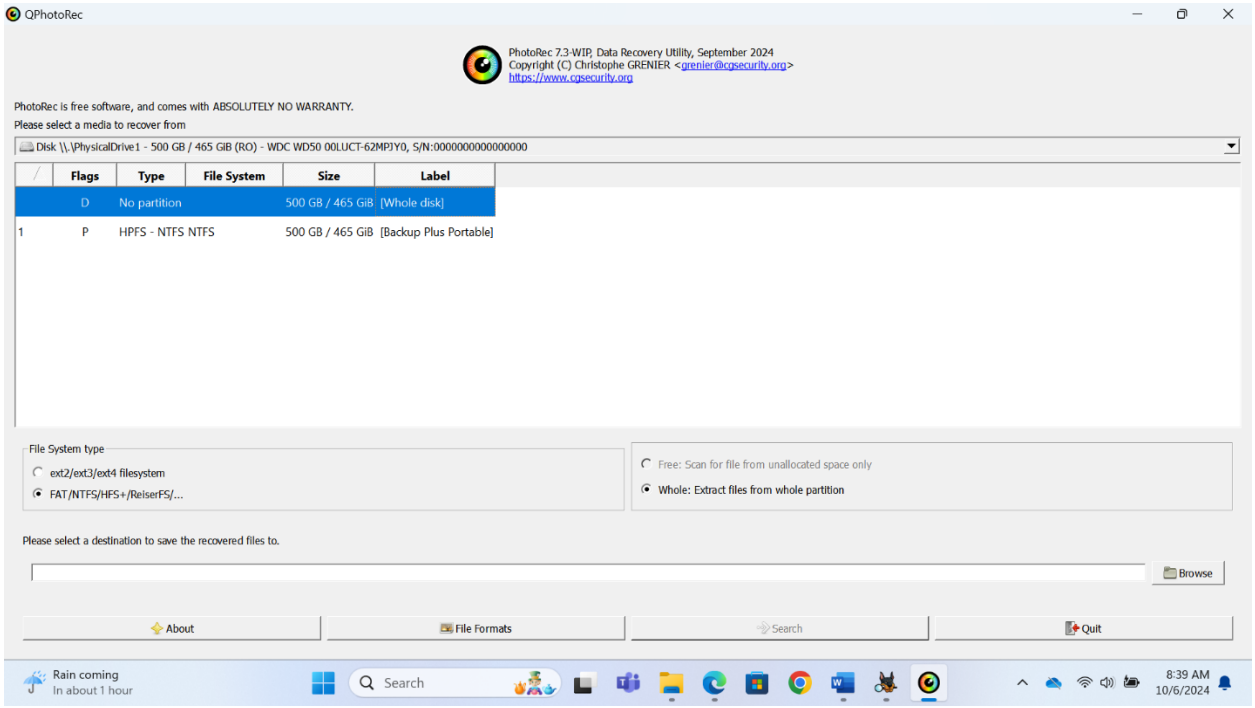
- I launched my PhotoRec Software after deleting the files on my USB Drive (D:)



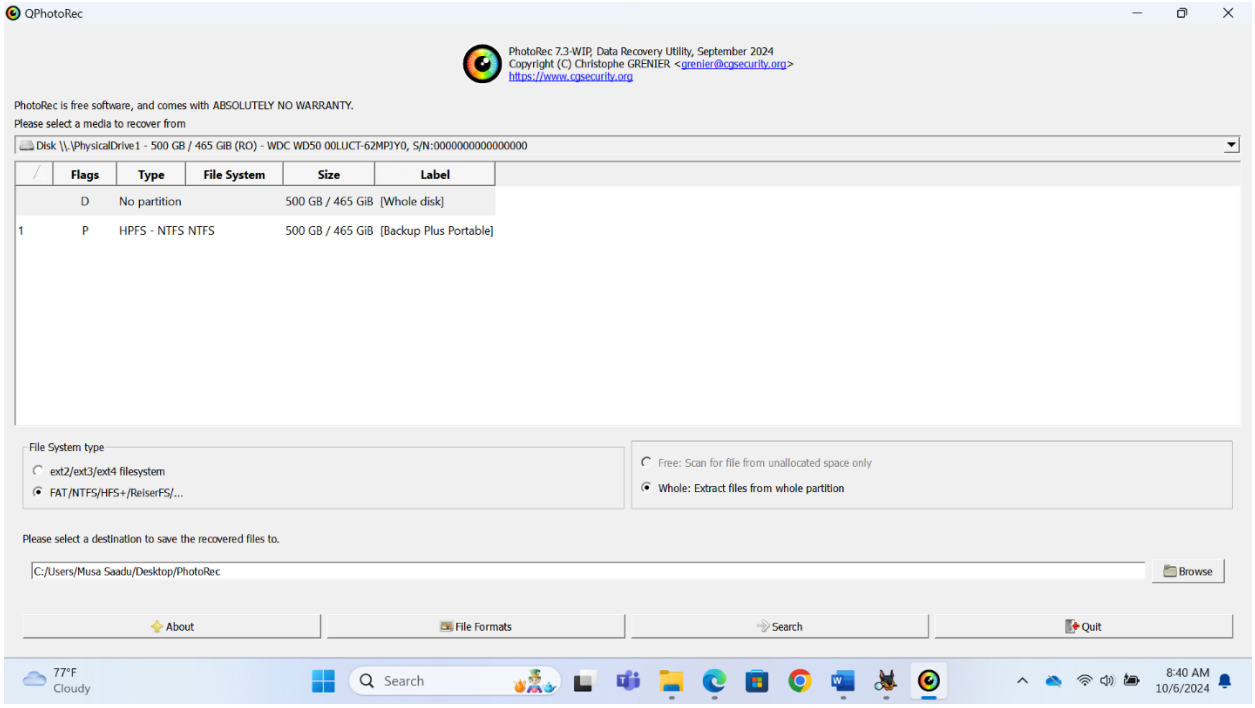
- I select the media I want to recover the lost data from which is the external drive: USB drive D:



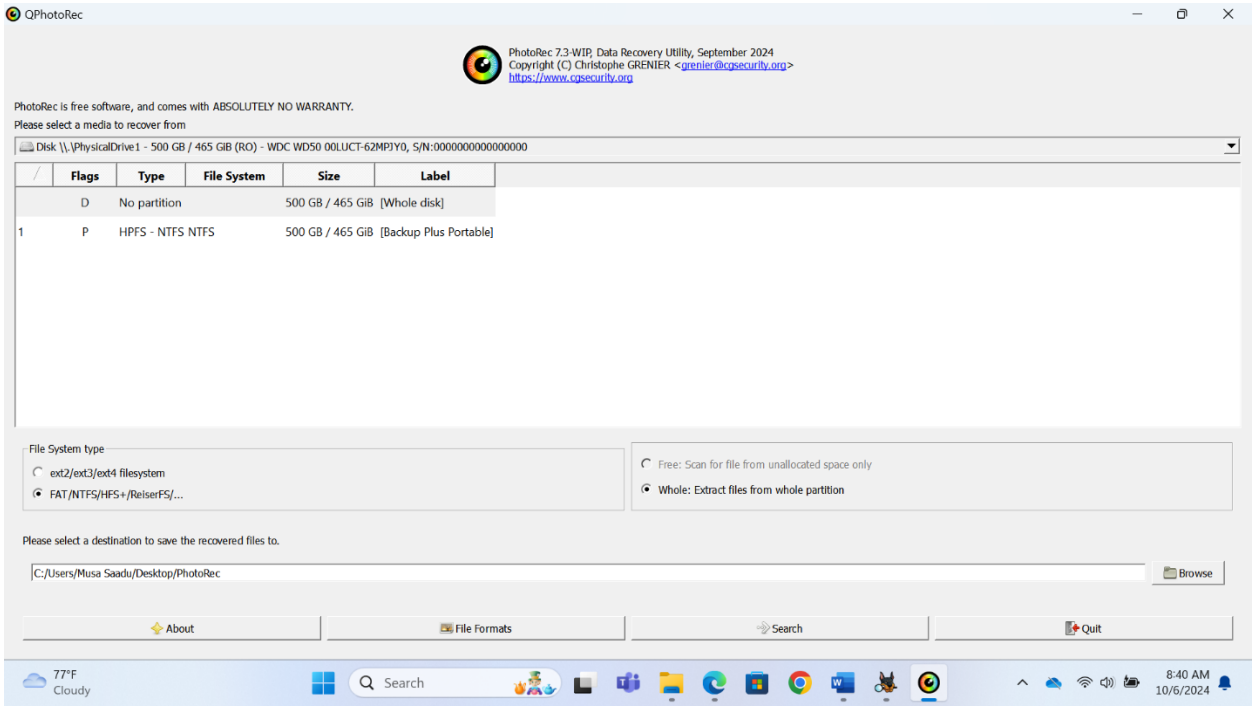
- I chose the file system type which is No Partition



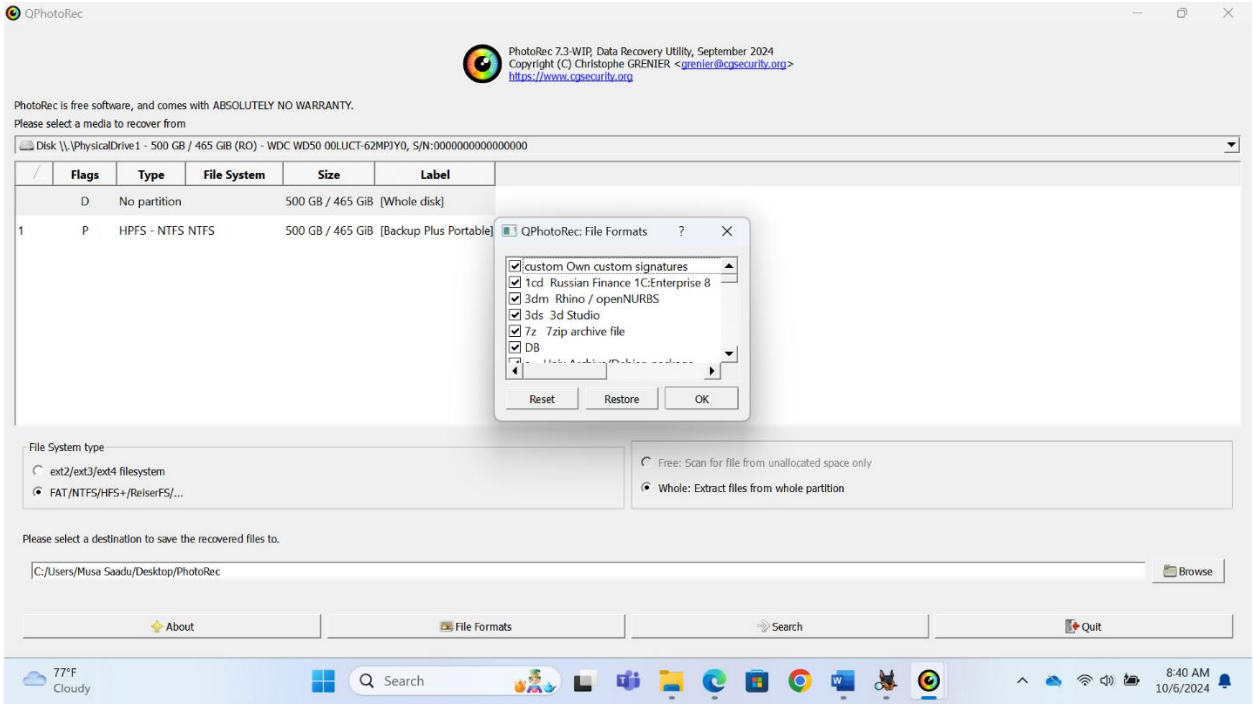
- I select the File system FAT/NFTS/HFS+ and whole: extract file from whole partition



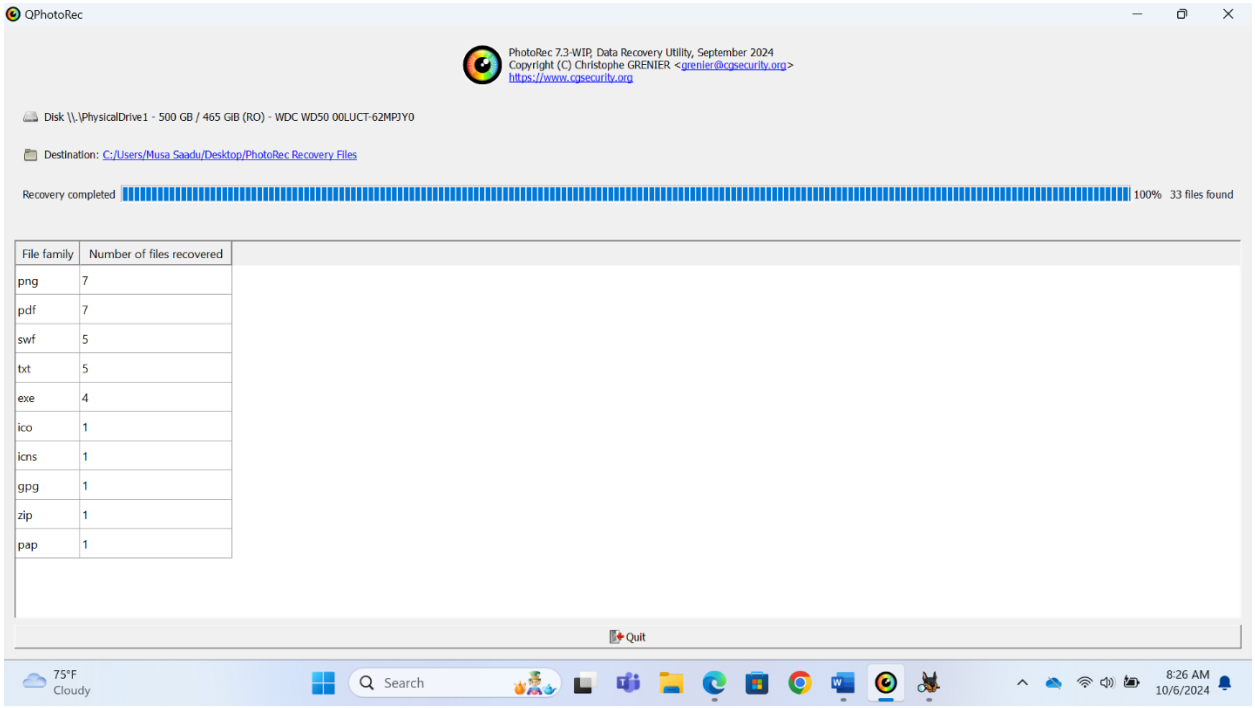
- I browsed for the destination to save the recover files to



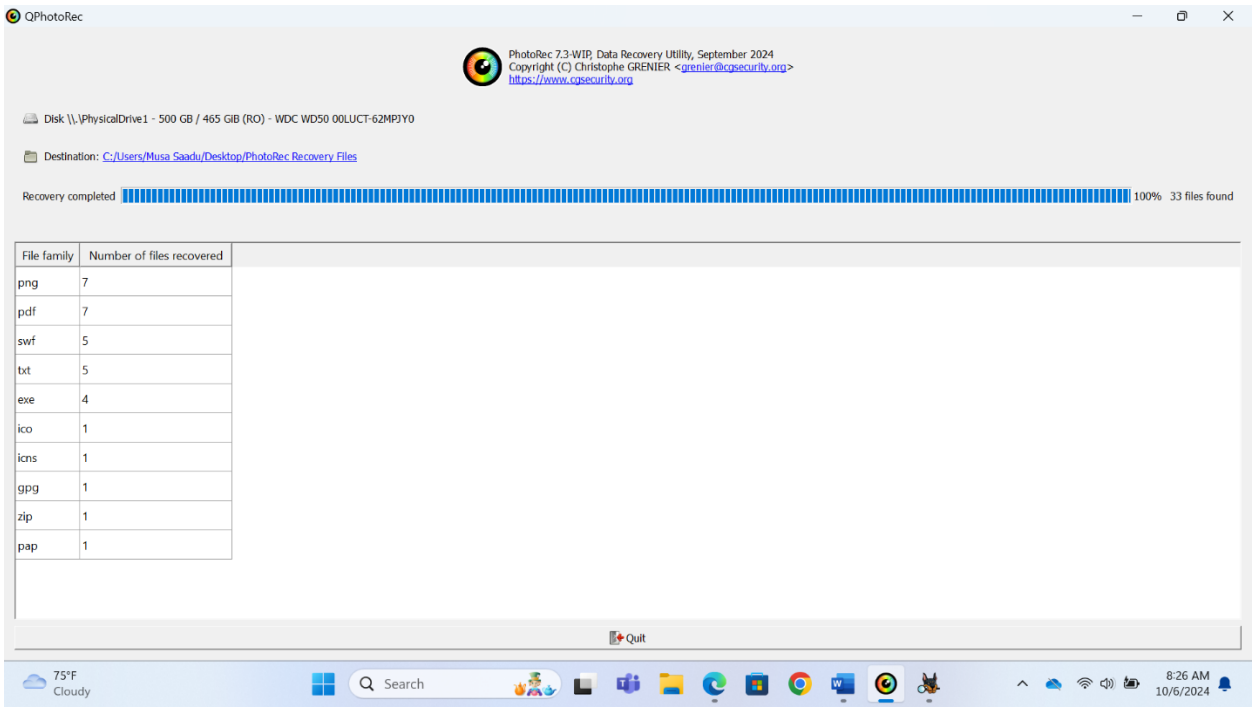
- I select the file formats like pdf, png etc



- I clicked on the Search Button for the recovery to start



- Recovered Files for the USB Dive D:

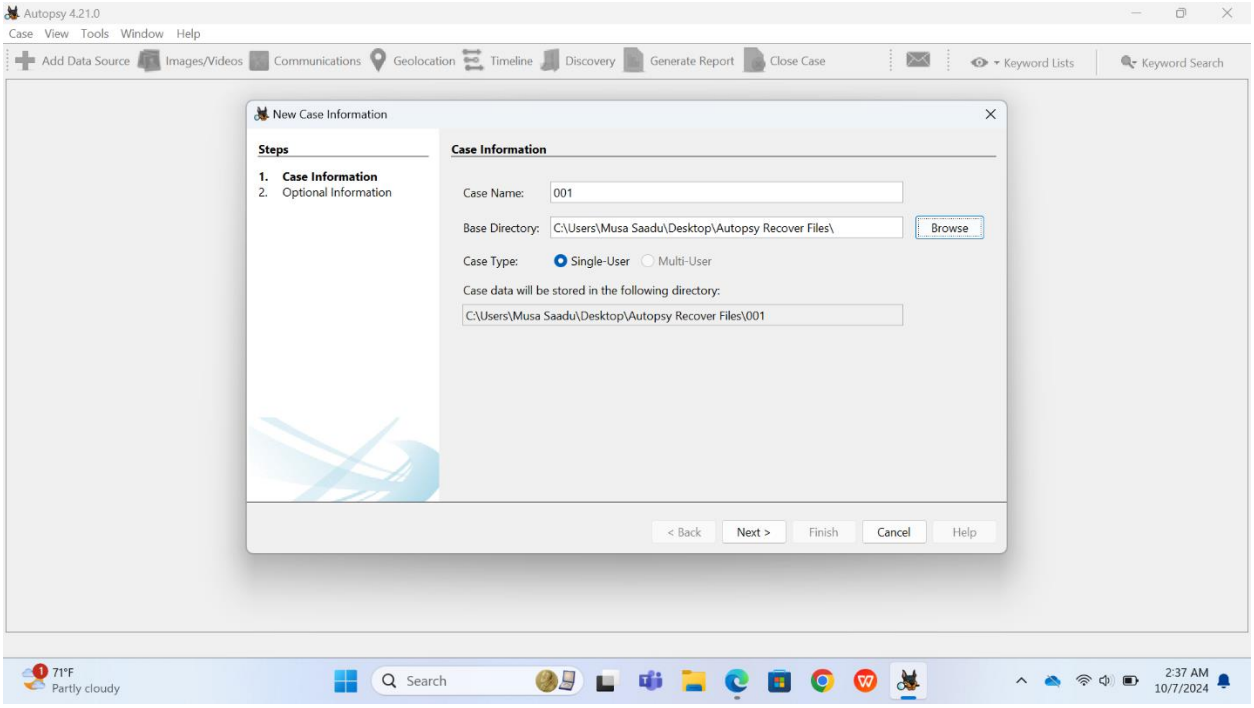


Forensic Analysis on a USB Drive D: using Autopsy

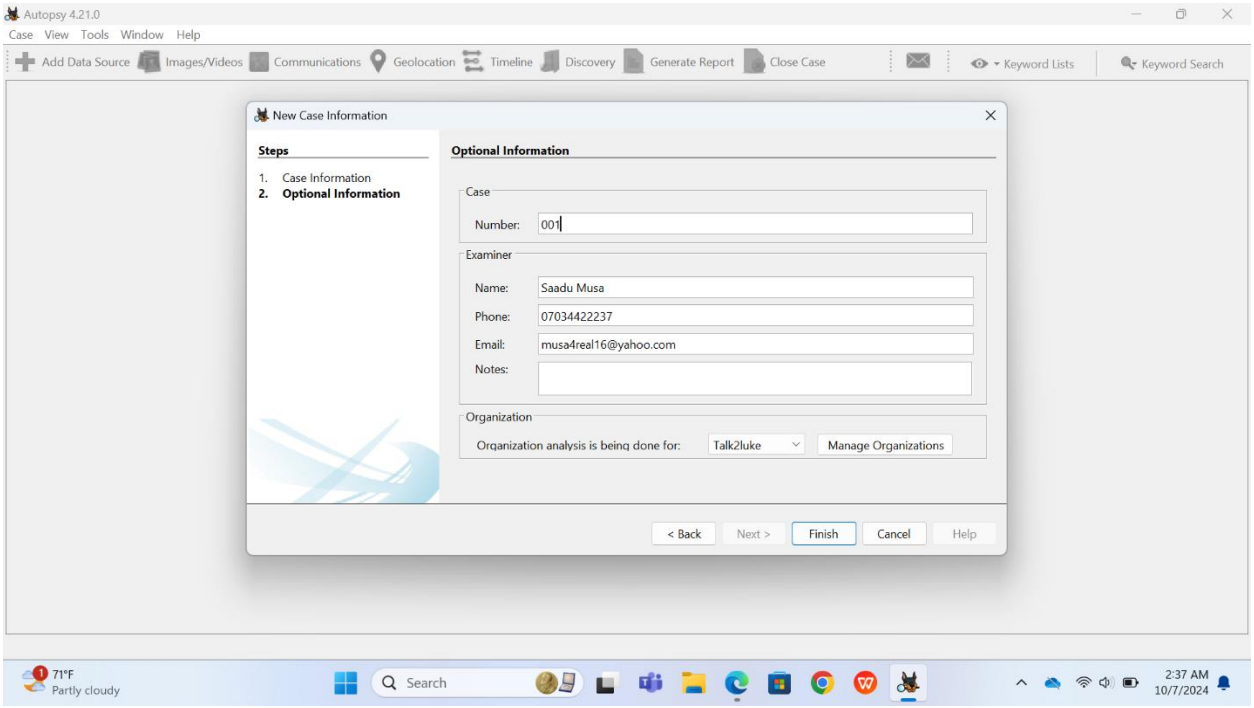
- Task: Recover deleted files and any other intriguing elements you may come across using Autopsy

- I launched my Autopsy Software after deleting the files on my USB Drive (D:) and select New case

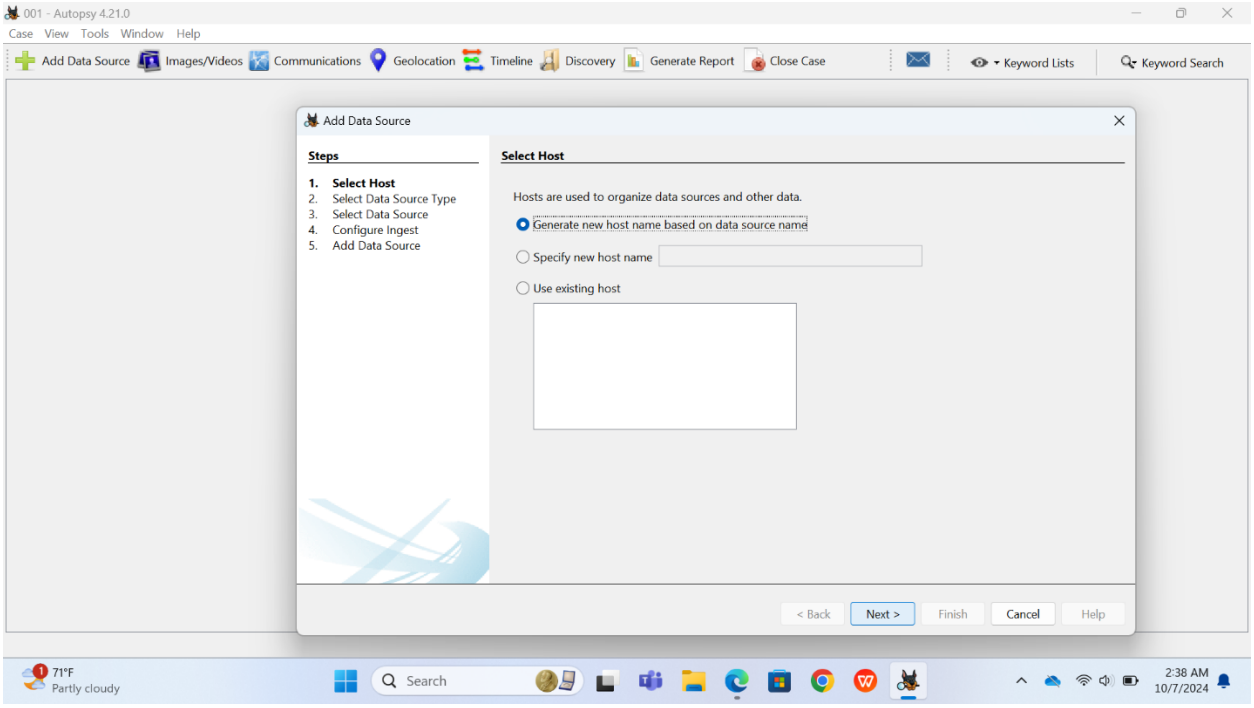
- I filled the case information by entering case name, browsed base directory and case type



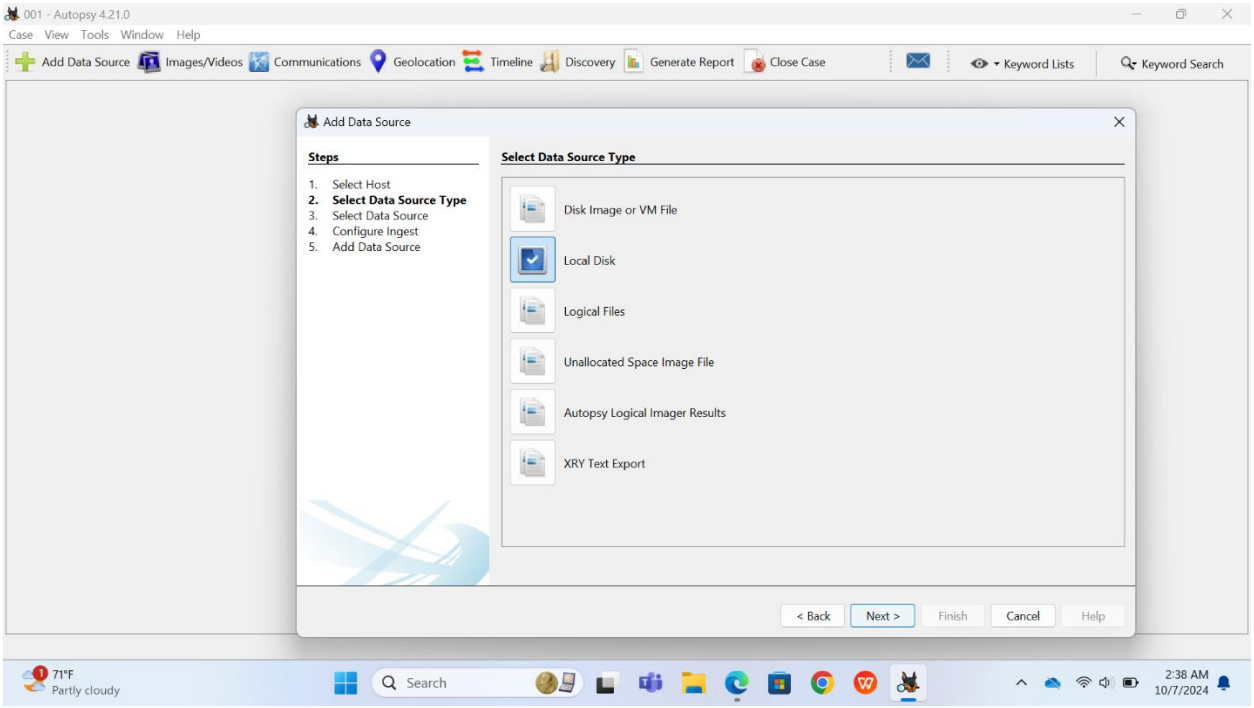
- I filled case number and the examiner details



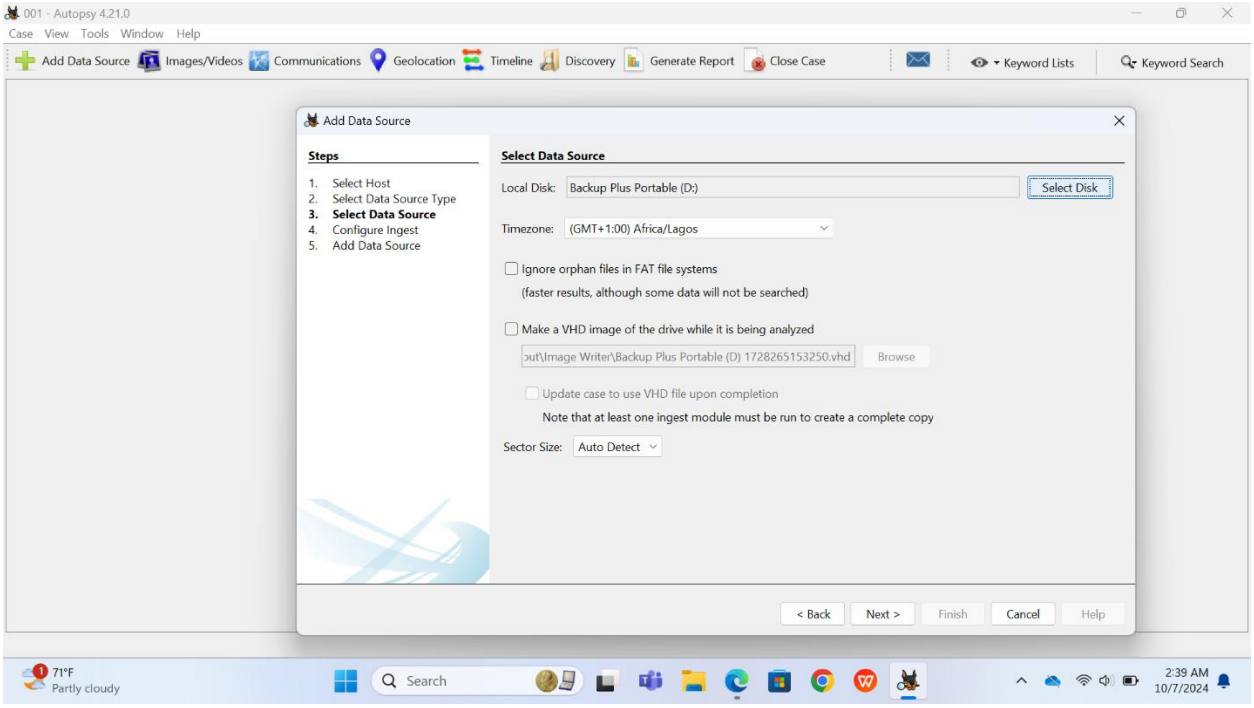
- I selected the Host : Generate new host name based on data source name



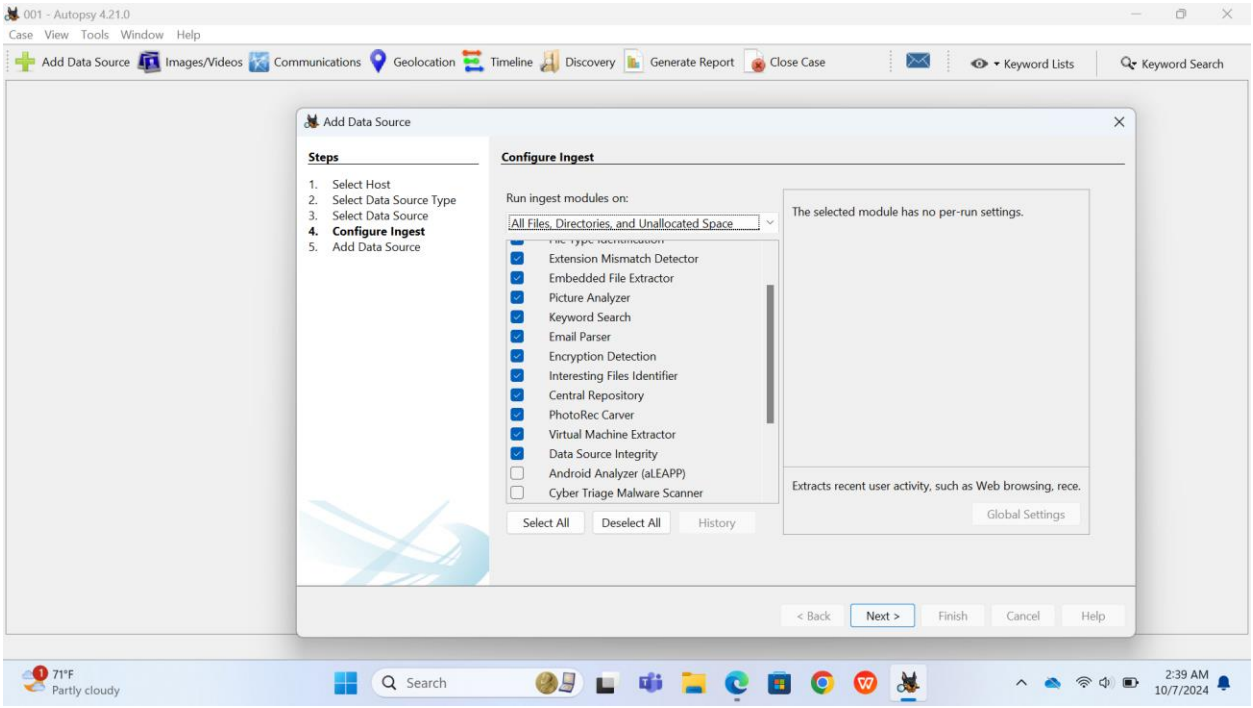
- I selected the Data Source Type : Local Disk



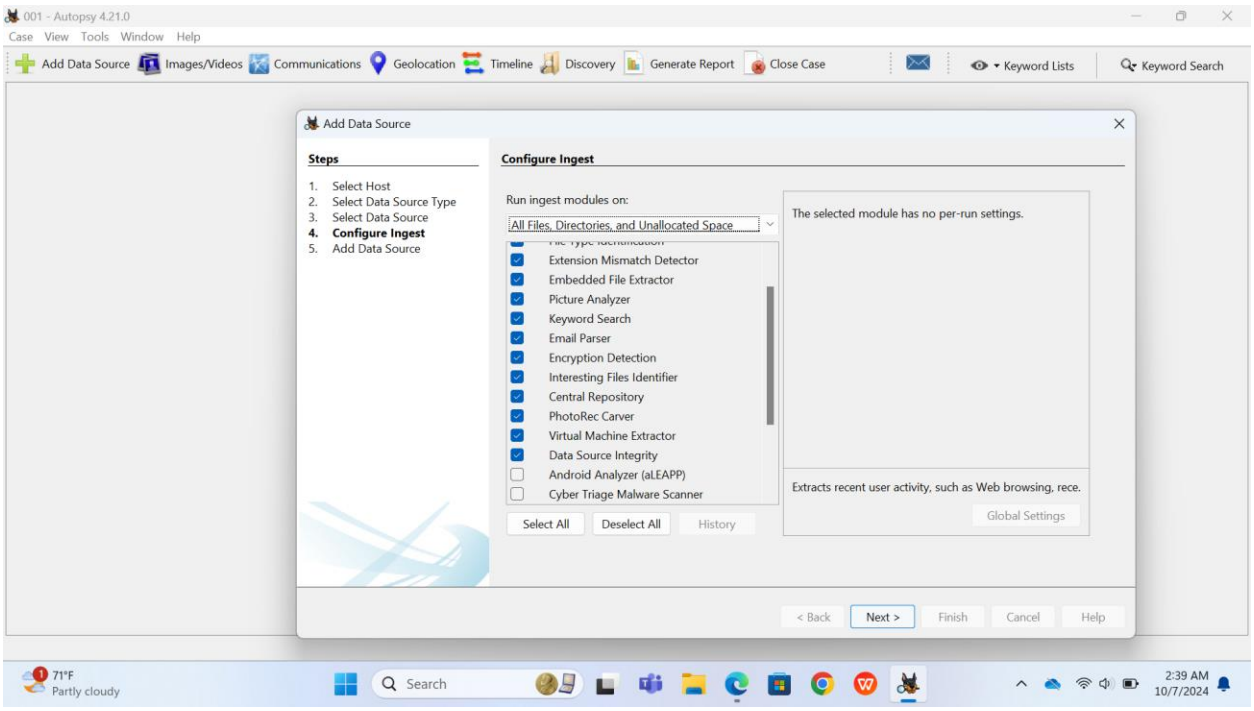
- I selected the Data Source



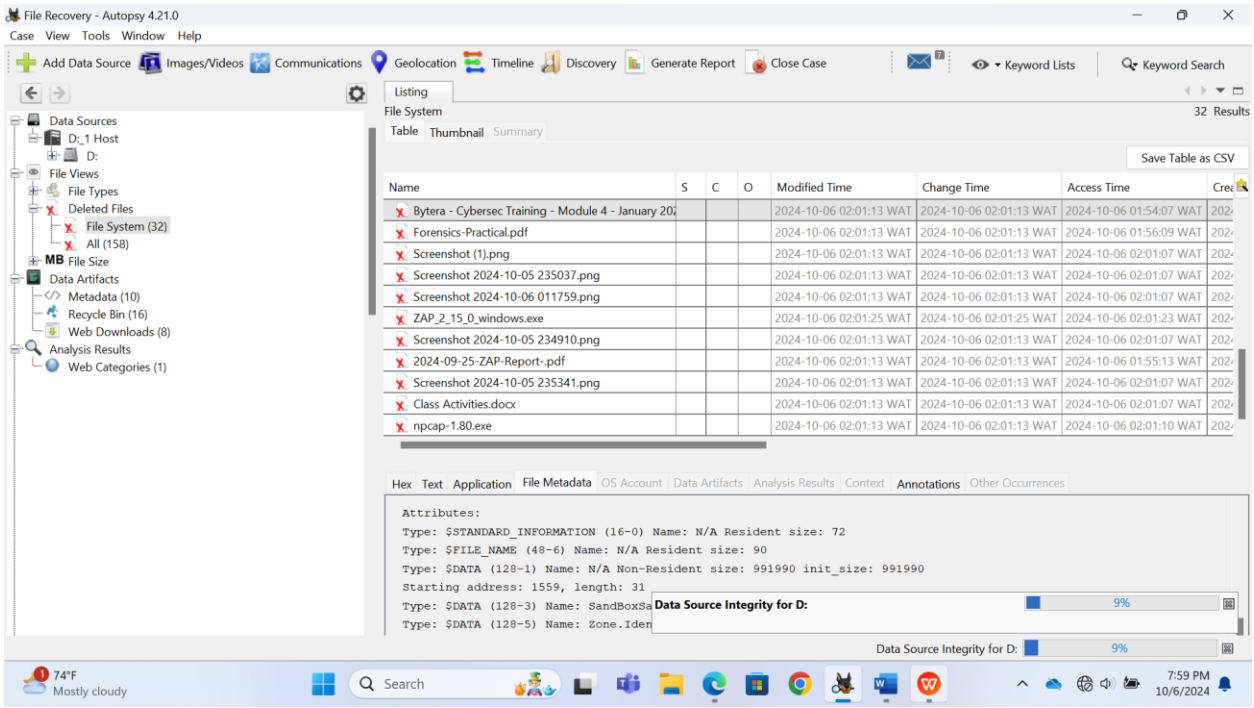
- Configure Ingest: I selected the appropriate modules for my device for scanning

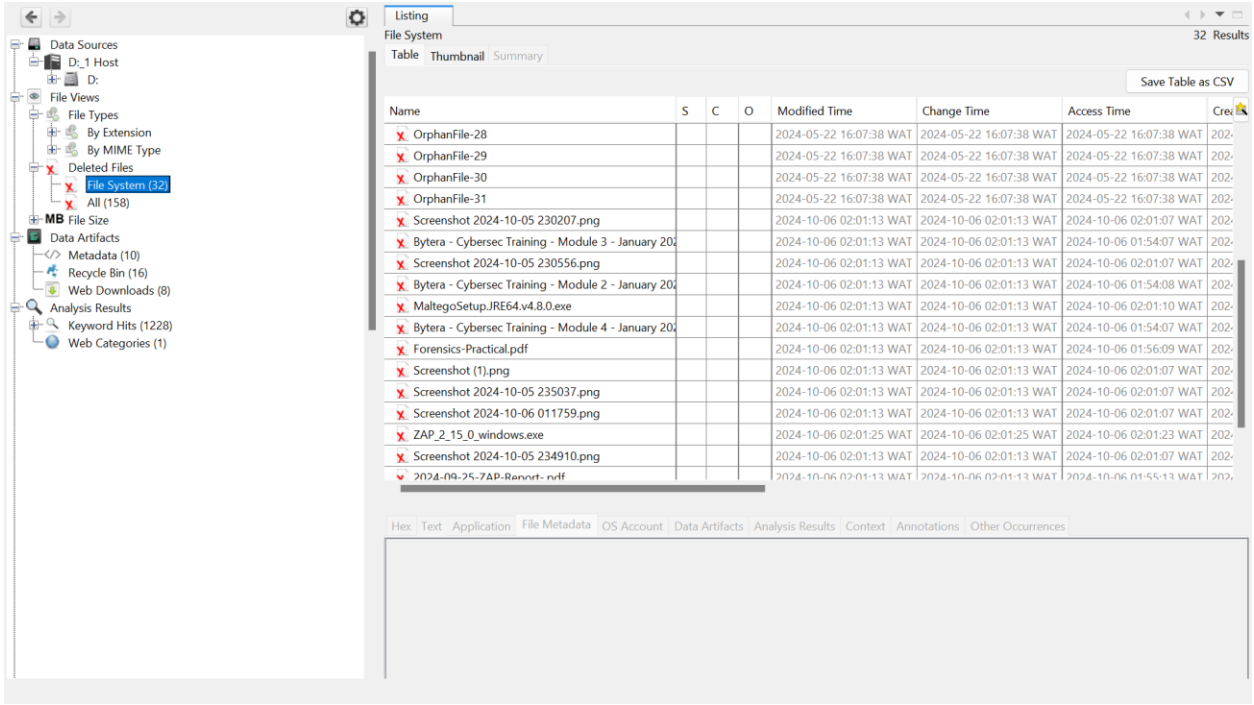


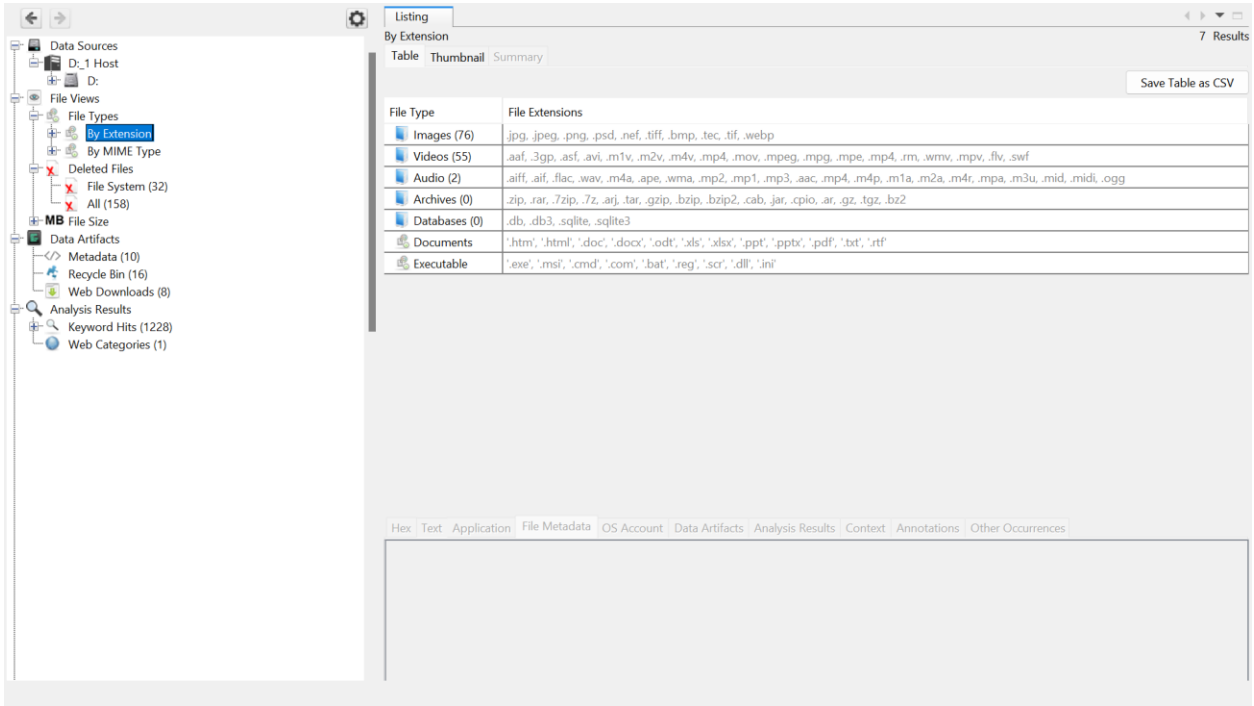
- Lastly I added the Data \source for the analysis to begin

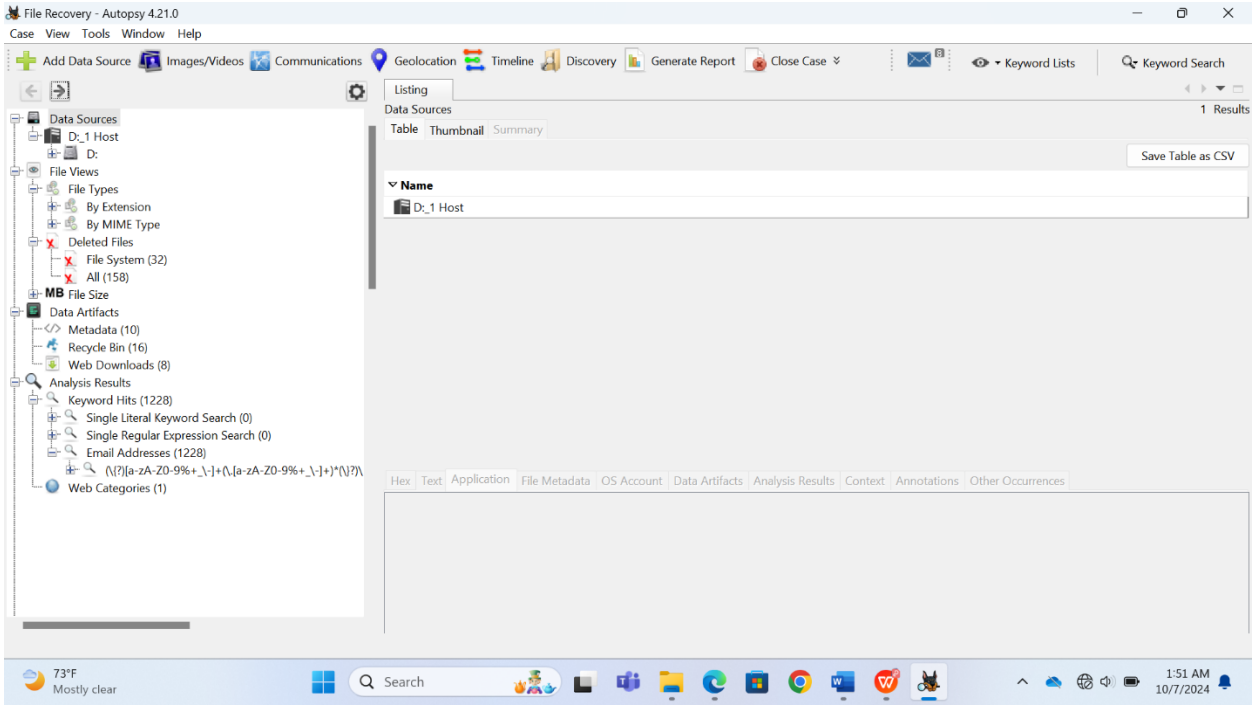


Screenshots of all discoveries for autopsy




Data Sources
D:_1 Host
D:
File Views
File Types
By Extension
By MIME Type
Deleted Files
File System (32)
All (158)
File Size
Data Artifacts
Metadata (10)
Recycle Bin (16)
Web Downloads (8)
Analysis Results
Keyword Hits (1228)
Web Categories (1)
Listing
File System
32 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
OrphanFile-28
OrphanFile-29
OrphanFile-30
OrphanFile-31
Screenshot 2024-10-05 230207.png
Bytera - Cybersec Training - Module 3 - January 202
Screenshot 2024-10-05 230556.png
Bytera - Cybersec Training - Module 2 - January 202
MaltegoSetup.JRE64.v4.8.0.exe
Bytera - Cybersec Training - Module 4 - January 202
Forensics-Practical.pdf
Screenshot (1).png
Screenshot 2024-10-05 235037.png
Screenshot 2024-10-06 011759.png
ZAP_2_15_0_windows.exe
Screenshot 2024-10-05 234910.png
2024-09-25-ZAP-Report-.pdf
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


Data Sources
D:_1 Host
D:
File Views
File Types
By Extension
By MIME Type
Deleted Files
File System (32)
All (158)
File Size
Data Artifacts
Metadata (10)
Recycle Bin (16)
Web Downloads (8)
Analysis Results
Keyword Hits (1228)
Web Categories (1)
Listing
By Extension
7 Results
Table
Thumbnail
Summary
Save Table as CSV
File Type
File Extensions
Images (76)
.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
Videos (55)
.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
Audio (2)
.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg
Archives (0)
.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
Databases (0)
.db, .db3, .sqlite, .sqlite3
Documents
'.htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.pptx', '.pdf', '.txt', '.rtf'
Executable
'.exe', '.msi', '.cmd', '.com', '.bat', '.reg', '.scr', '.dll', '.ini'
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences



Generate a comprehensive report detailing your conclusions regarding the USB/memory card.

- Autopsy Forensic Report for case File Recovery

Refrences

- Writing DFIR Reports: A Primer - Forensic Focus
- Digital Forensics: Autopsy's Magic in Recovering Deleted Data | by Aastha Thakker | Medium
- Digital-Forensics-Report/Forensic Examination Report.pdf at master · arvindpj007/Digital-Forensics-Report · GitHub

- importnace of volatile memory in digital forensic - Search (bing.com)
- Importance of RAM Dump in Digital Forensics | LevelBlue (att.com)
- Autopsy Mobile Forensics (Android) - YouTube
- Autopsy Forensic Tool Review (How to Use Autopsy to Recover Deleted Files) (imyfone.com)
- PhotoRec Step By Step - CGSecurity