



**Forensic analysis using
Open source technology.**

By Nikhil Yadav

11907684

Rollno.49 INT301 CA3

Index

1. Introduction

1.1 Objective of the project	5
1.2 Description of the project	5
1.3 Scope of the project	5

2. System Description

2.1 Target system description	6
2.2 Assumptions and Dependencies (If applicable)	6-7

3. Analysis Report

3.1 Final result of the Microsoft edge	7-10
3.2 Final result of the Firefox	10-11
3.3 Final result of the Google	11-13

4. Reference/ Bibliography

Chapter 1

Introduction

What is disk forensics?

Disk forensics, also known as computer forensics or digital forensics, is the practice of collecting, analyzing, and preserving digital evidence from computer storage devices, such as hard drives, solid-state drives, flash drives, and memory cards. The goal of disk forensics is to identify, preserve, and analyze data in a way that maintains its integrity and authenticity, and to use the information obtained to support legal or investigative purposes.

Why is disk forensics important?

Disk forensics is important because it enables investigators to recover and analyze data that may be crucial to solving crimes or resolving disputes. In many cases, digital evidence can provide more comprehensive and accurate information than traditional forms of evidence, such as witness testimony or physical artifacts.

Types of disk forensics

There are several types of disk forensic analysis, including:

- **Live analysis:** This involves analyzing data on a computer while it is still running, which can be useful in situations where investigators need to quickly gather information without disrupting the normal functioning of the system.
- **Post-mortem analysis:** This involves analyzing data on a computer that has been shut down or seized, and can provide a more thorough and detailed examination of the system.
- **Network forensics:** This involves analyzing data from network traffic to identify evidence of criminal activity, such as hacking or data theft.
- **Memory forensics:** This involves analyzing data from a computer's RAM (random access memory), which can provide valuable information about running processes, open files, and other system activity.
- **Mobile device forensics:** This involves analyzing data from smartphones, tablets, and other mobile devices, which can contain valuable evidence in cases involving cybercrime, fraud, or other digital

offenses.

Disk Forensics

Disk forensics is a vital component of digital forensics that focuses on the investigation of data stored on physical storage media, such as hard drives and solid-state drives. Disk forensics involves examining the contents of the disk to identify evidence of digital activity.

When a crime is suspected, a forensic examiner may seize the suspect's computer or storage devices and conduct an analysis of the data stored on the disk. Disk forensics can help investigators identify the source of digital evidence and reconstruct events that took place on the disk.

To conduct a disk forensic examination, the examiner must use specialized tools and techniques to identify, preserve, and analyze data on the disk. This may involve making a bit-by-bit copy of the disk to preserve the original evidence, searching for hidden or deleted files, and analyzing the file system to determine how data was stored and accessed.

Disk forensics is often used in criminal investigations, such as cases involving fraud, cybercrime, and intellectual property theft. It can also be used in civil litigation to gather evidence in cases involving electronic discovery, trade secret theft, and breach of contract.

To be an expert in disk forensics, one must have in-depth knowledge of computer hardware, operating systems, file systems, and data recovery techniques. The examiner must also be proficient in the use of specialized tools and software to analyze disk images and recover deleted or hidden data.

1.1 Objective of the project

The objective of this project is to use open-source software to generate a report that can extract deleted data from a hard disk drive. Specifically, the software tool that will be used in this project is Autopsy, which is a powerful digital forensic investigation tool that can analyze disk images and recover data from them.

1.2 Description of the project

The project involves using Autopsy to generate a report that can extract deleted data from a hard disk drive. Autopsy is a free and open-source digital forensics tool that is widely used by law enforcement agencies, government organizations, and digital forensics professionals to analyze and recover data from digital devices.

To use Autopsy for this project, we will need to obtain a disk image of the hard drive that contains the deleted data. This can be done using a disk imaging tool such as dd or FTK Imager. Once we have the disk image, we can load it into Autopsy and run a search for deleted files.

Autopsy has a built-in search functionality that can identify deleted files based on various criteria such as file type, file size, and file name. Once the deleted files have been identified, we can generate a report that lists the recovered files along with their metadata such as the date and time they were deleted, the file path, and the file size.

The report generated by Autopsy can be exported in various formats such as HTML, PDF, or CSV. This report can then be used by digital forensics investigators to analyze the recovered data and determine whether any malicious activity occurred on the hard drive.

1.3 Scope of the project

The scope of this project is limited to using Autopsy to generate a report that can extract deleted data from a hard disk drive. The project does not involve analyzing the recovered data or determining the cause of the data loss. The project also assumes that a disk image of the hard drive is available for analysis. If a disk image is not available, the project may require additional steps to create one.

Chapter 2

System Description

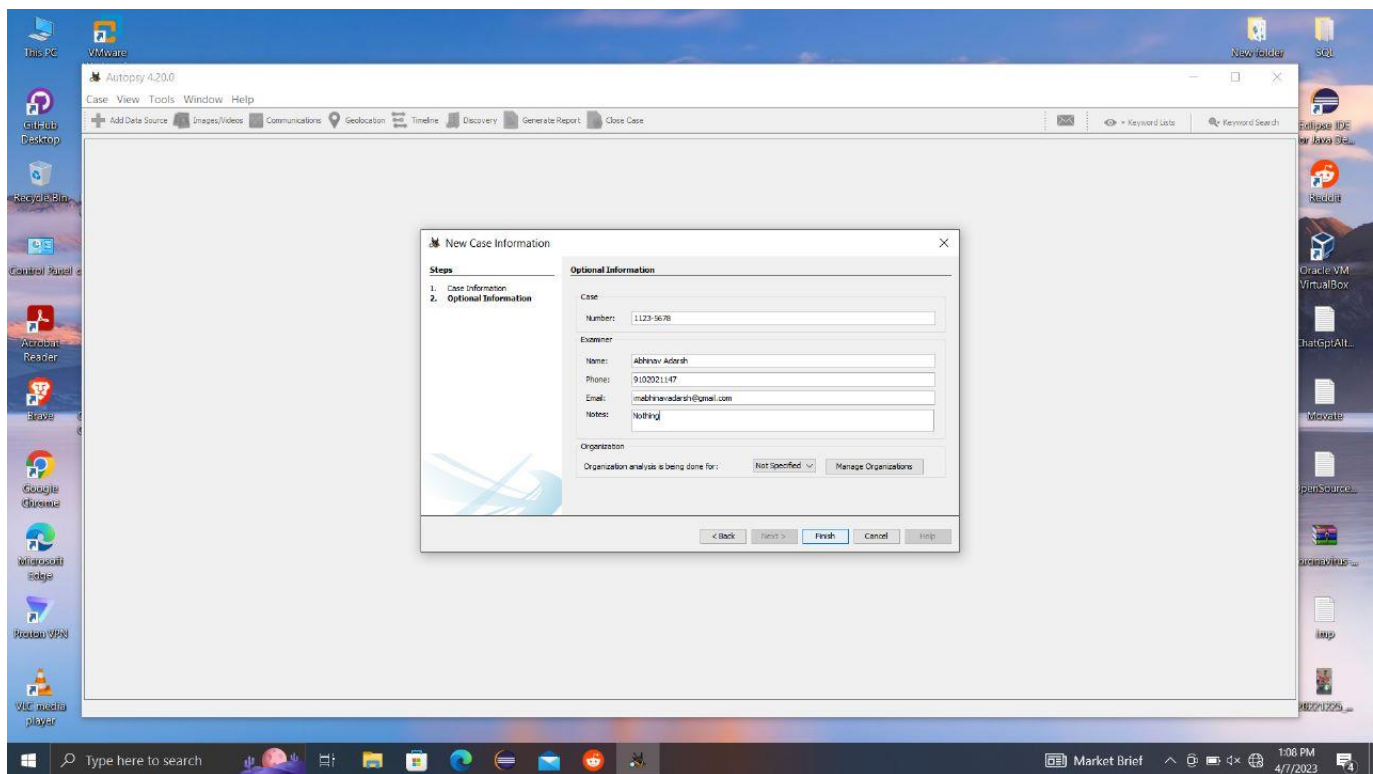
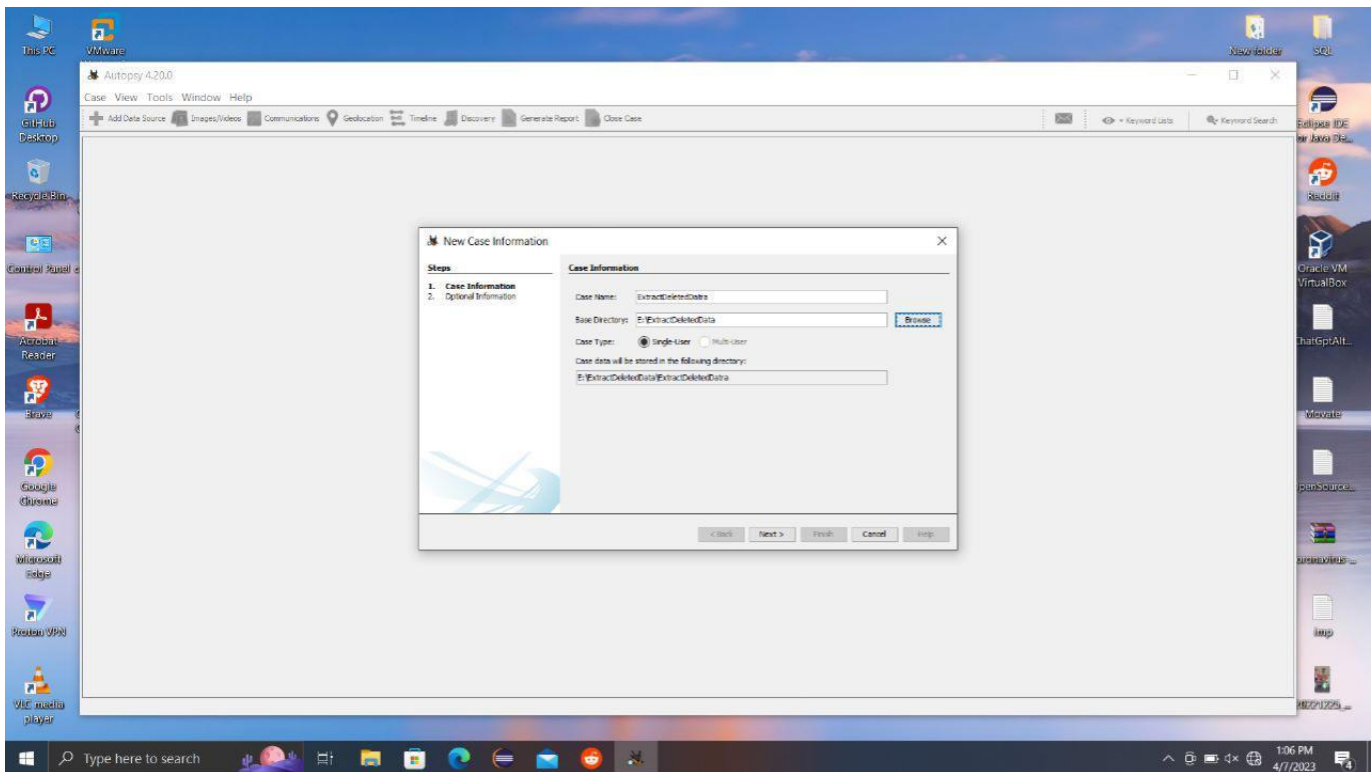
1.4 Target system description

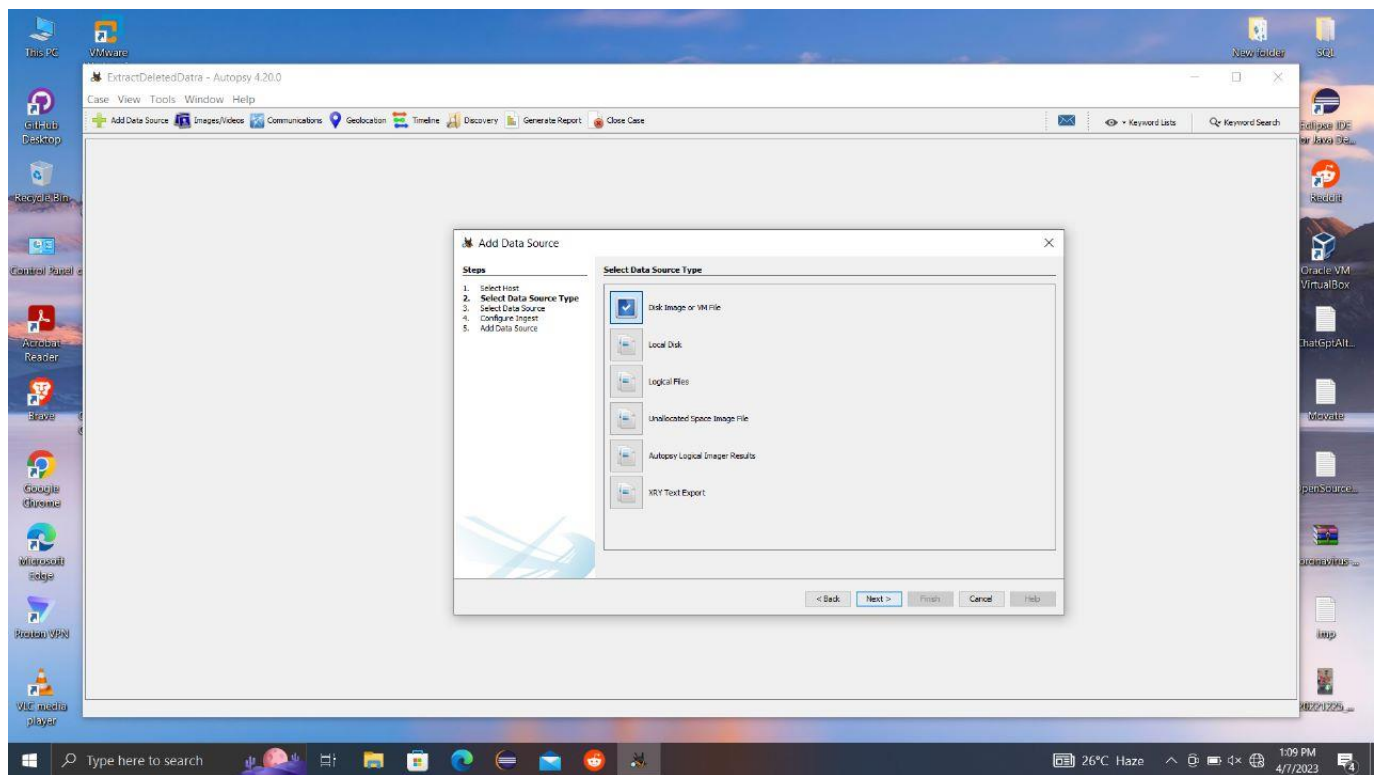
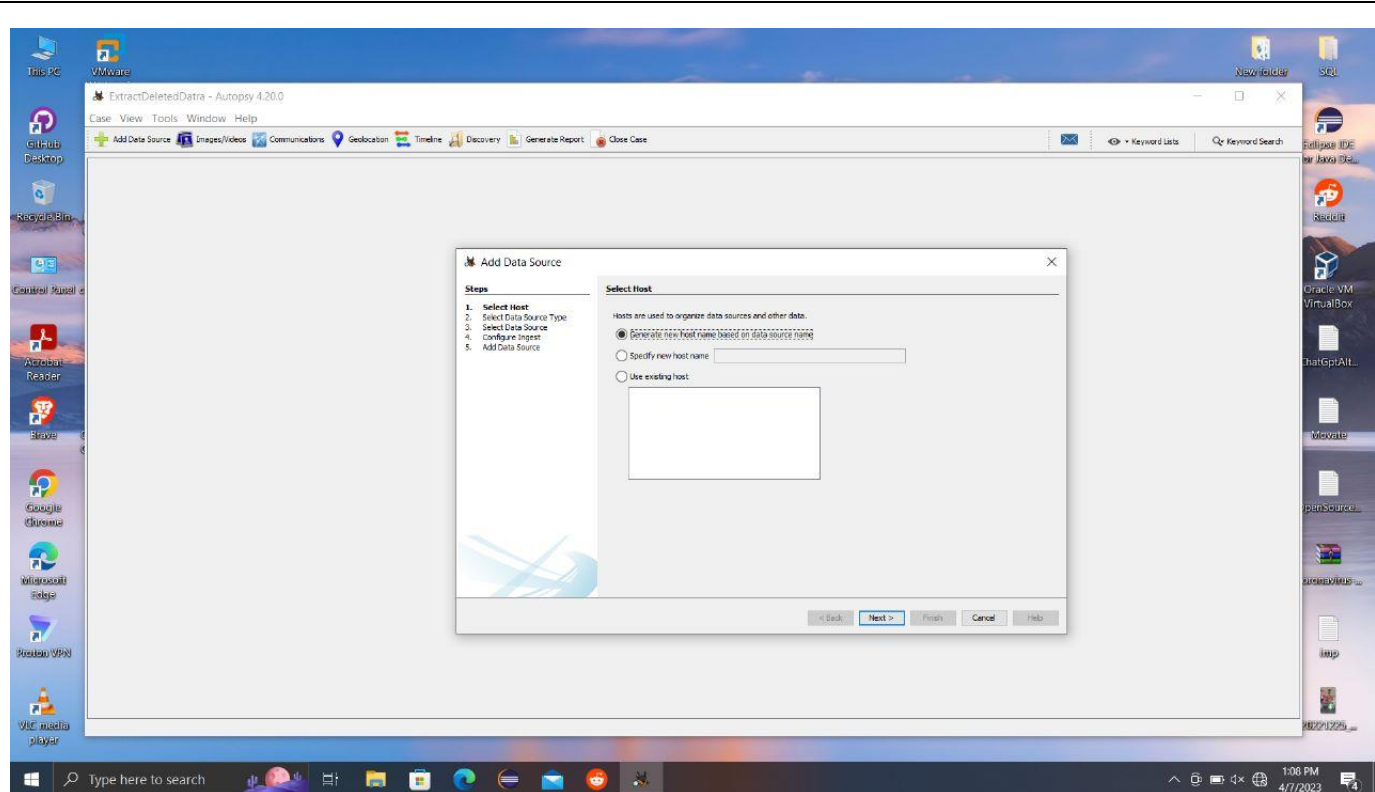
- A digital forensics system capable of extracting deleted data from a hard disk drive.
- The system will use open-source software Autopsy to generate a report that can identify and recover deleted files from a disk image of the hard drive.
- The system should have the processing power and memory to run Autopsy.
- A write-blocker device or hardware write-blocking capability is required to ensure that the data on the storage devices is not altered during the extraction process.
- The system should understand the file system on the storage device and how the data is organized, such as NTFS, FAT32, or ext4.
- A secure location to store the extracted data, such as an encrypted hard drive or other secure storage device, is necessary.
- The system should have the necessary permissions or legal authority to extract and analyze the data on the storage devices.
- Proper documentation of the extraction process and any findings is important to ensure that the extracted data can be used as evidence in legal proceedings if necessary.

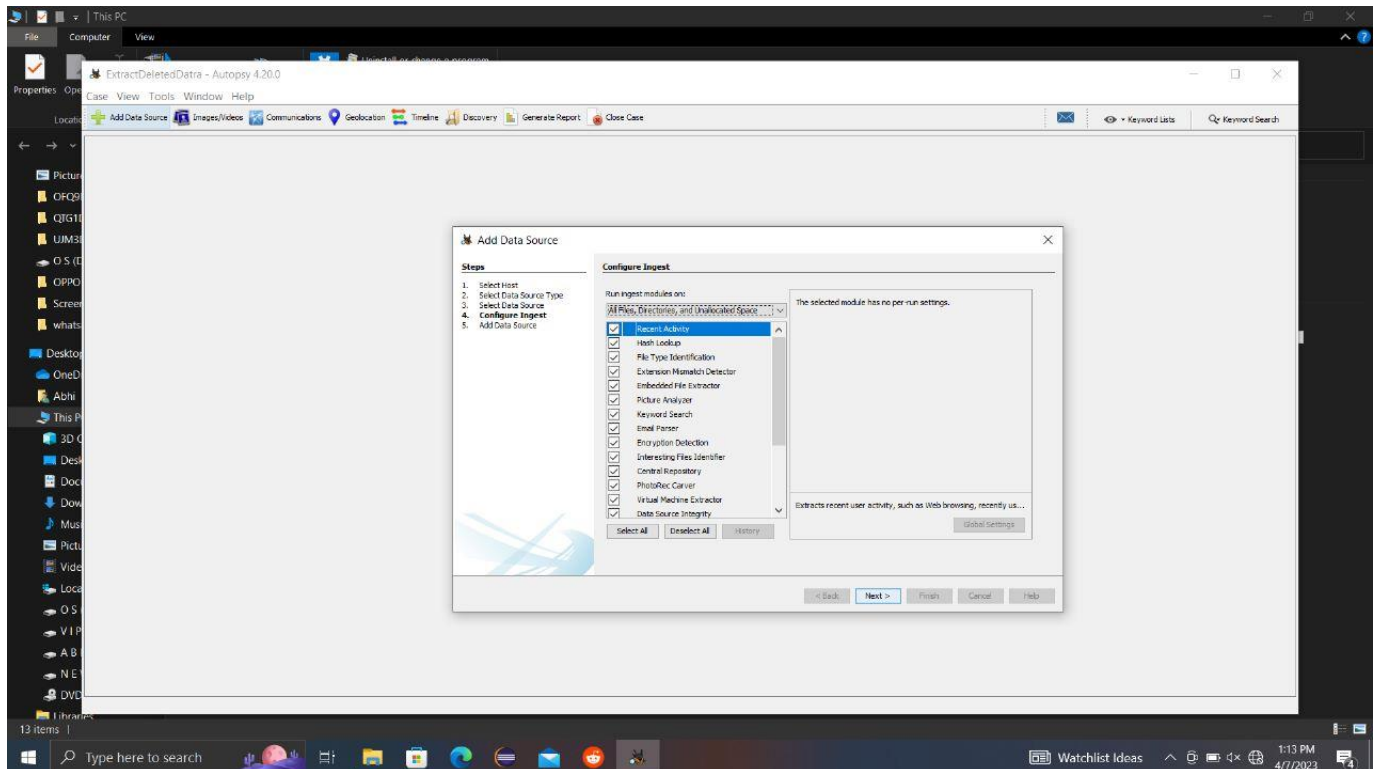
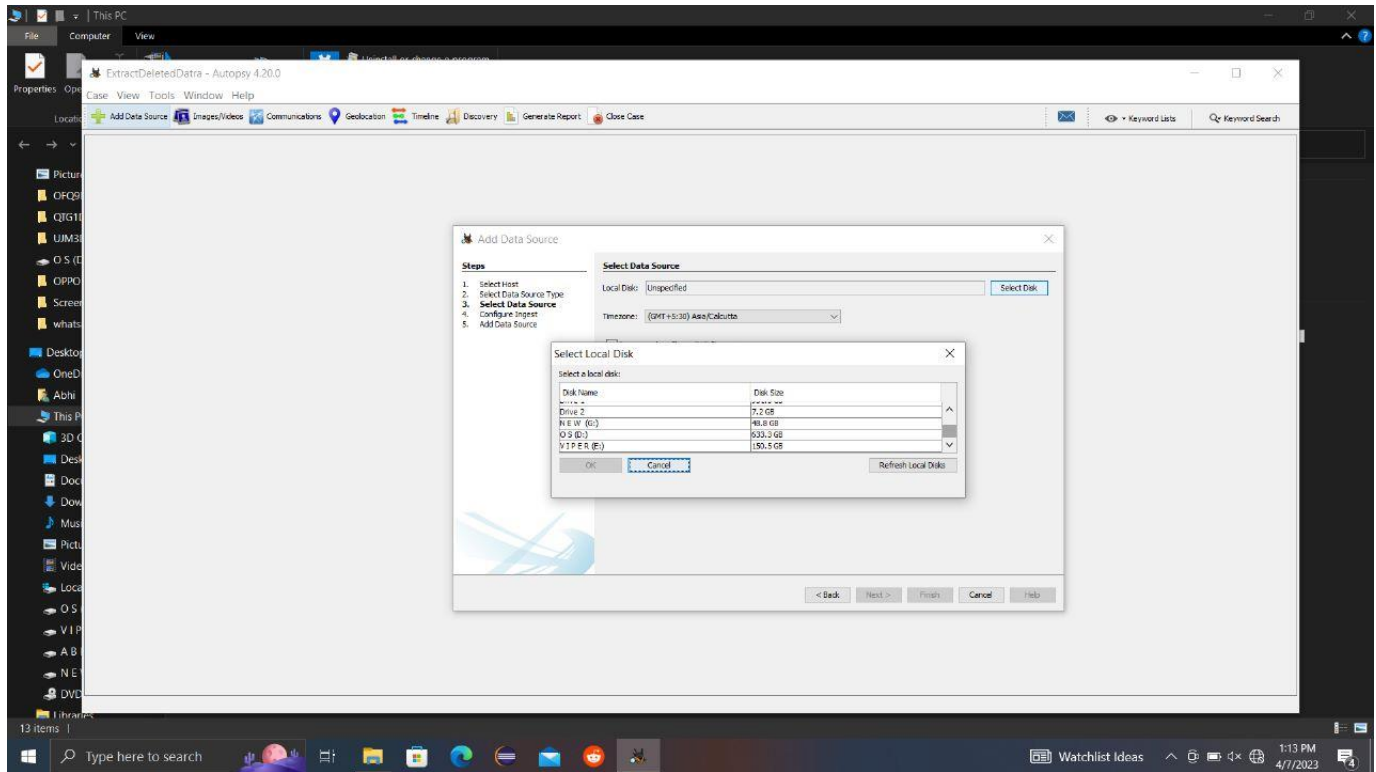
1.5 Assumptions and Dependencies (If applicable)

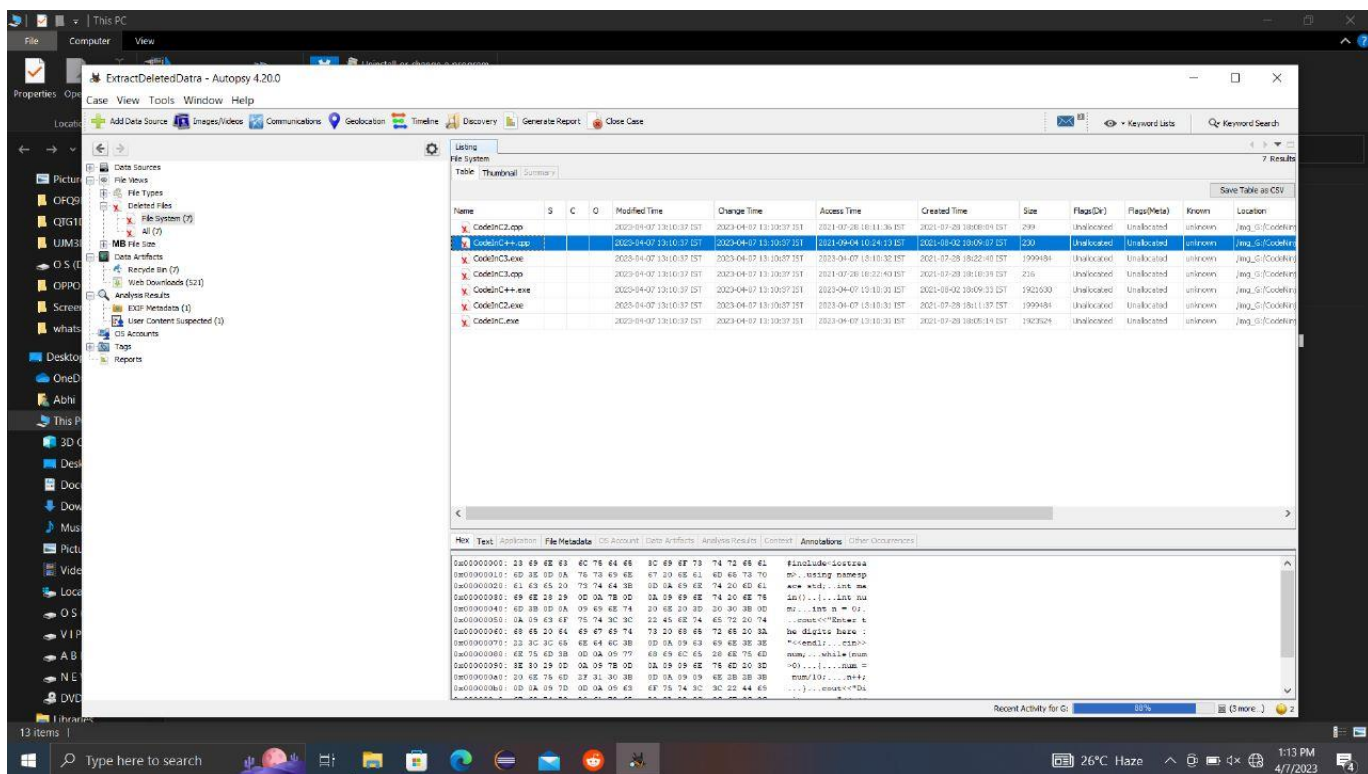
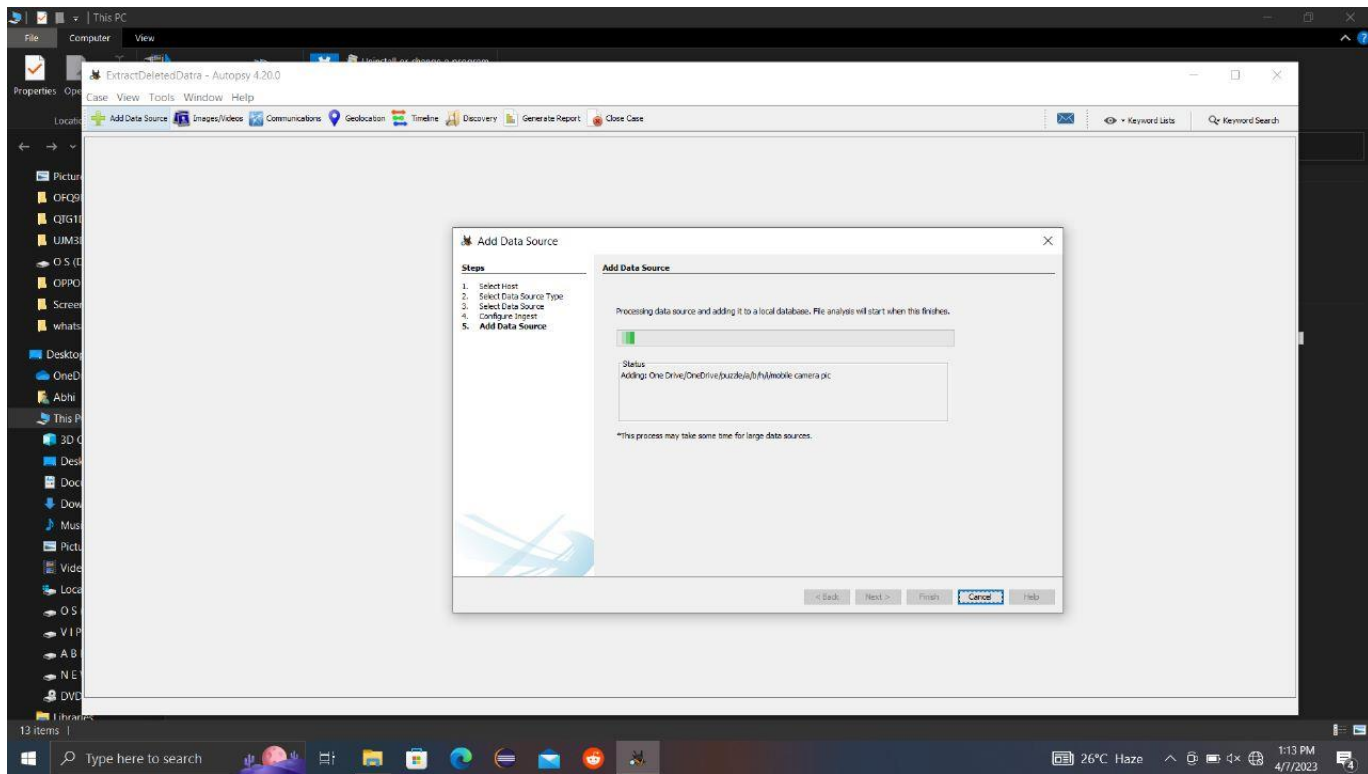
- The hard disk drive is available for analysis and has not been physically damaged.
- Autopsy is installed and properly configured on the digital forensics system.
- The storage device is accessible to the digital forensics system.
- The file system of the storage device is supported by Autopsy.
- The extracted data may need to be further analyzed or processed using other software.

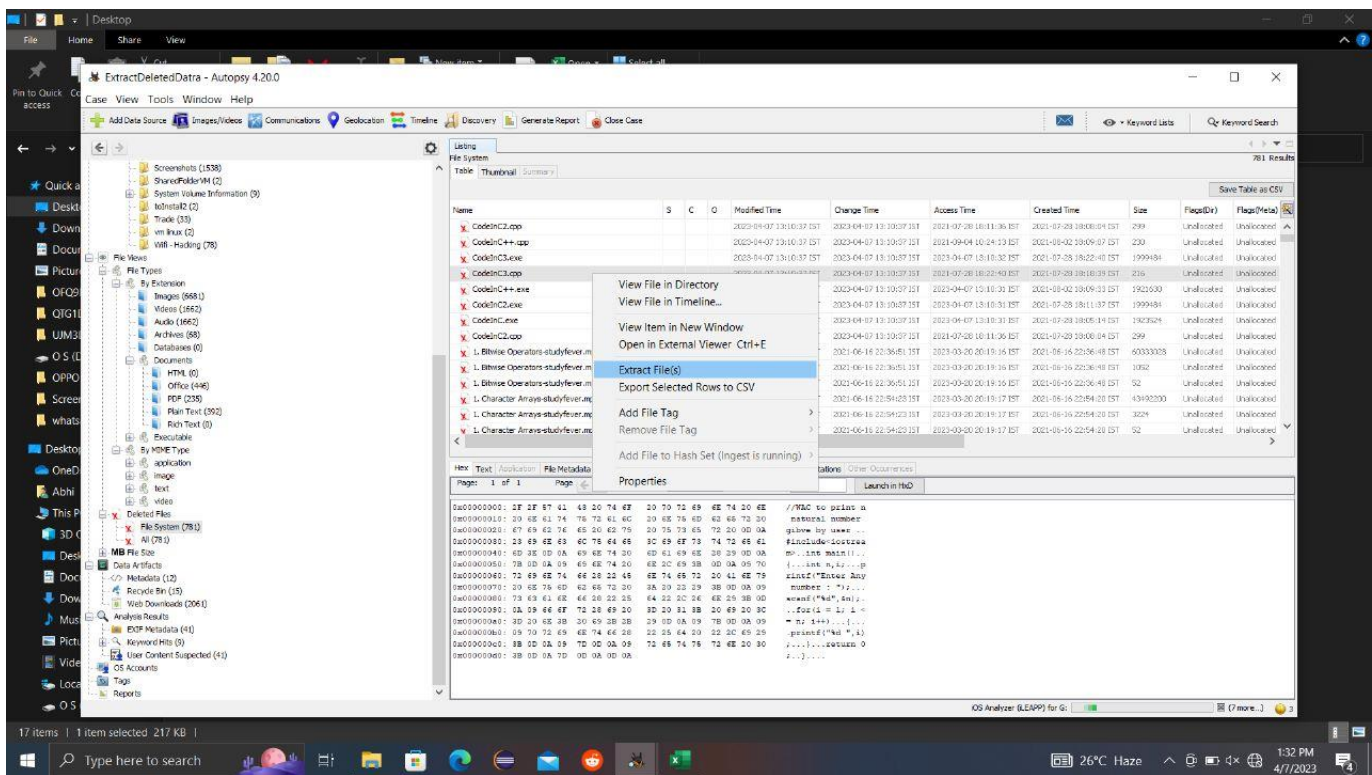
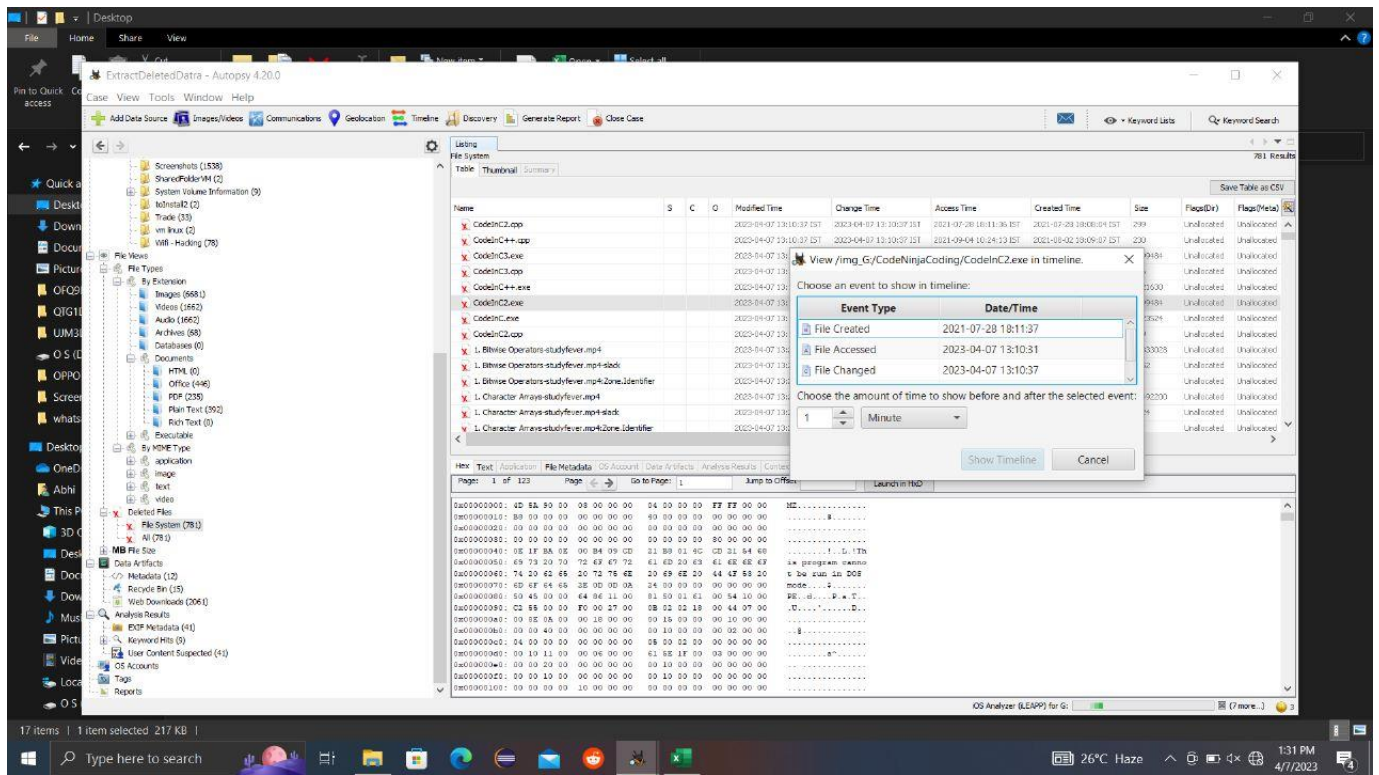
2. Analysis Screenshot

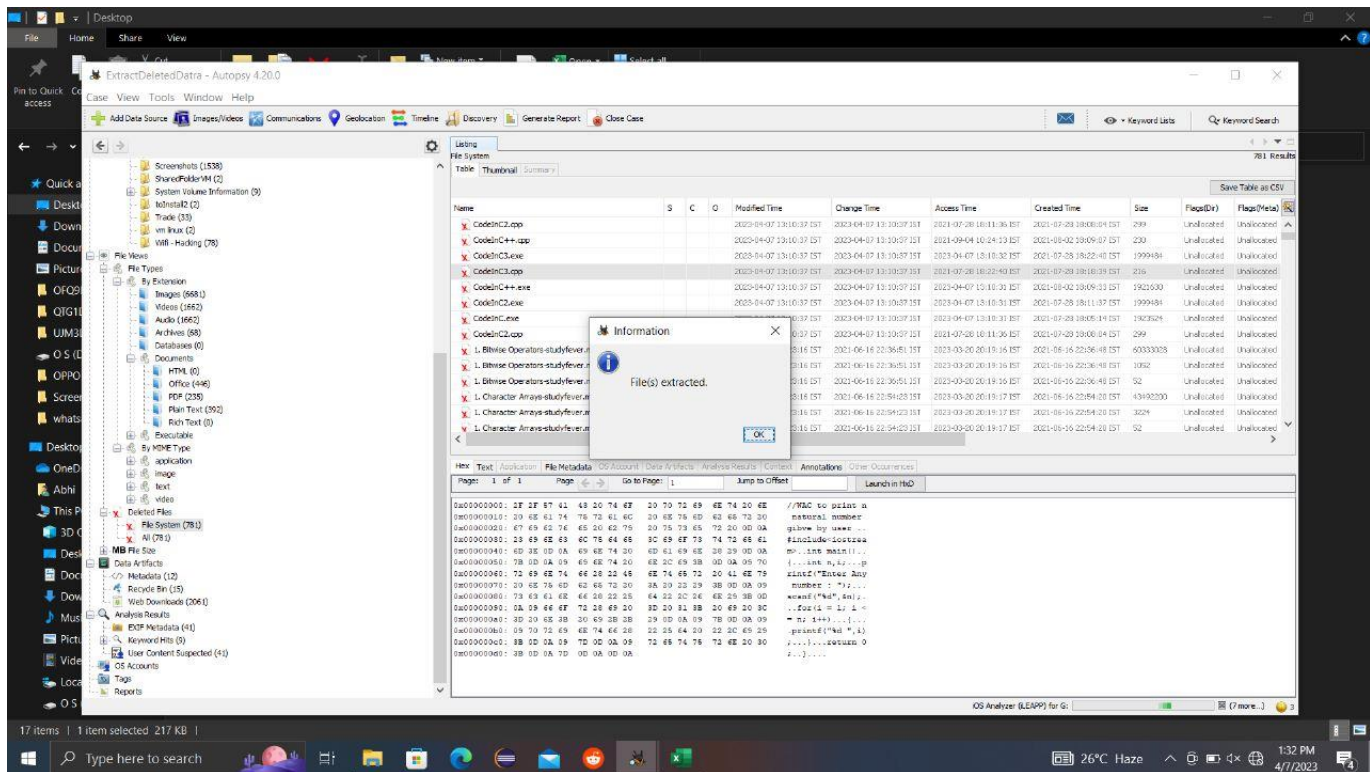












3. Reference/ Bibliography

1. Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.
2. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press.
3. Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to Computer Forensics and Investigations. Cengage Learning.
4. Quick, D., Chakraborty, S., & Martini, B. (2019). Digital Forensics Basics: A Practical Guide Using Windows OS. Apress.
5. Autopsy User Documentation: <https://sleuthkit.org/autopsy/docs/user-docs/3.1/>

