Academic Task-3

“Use any open-source tool to recover deleted files.”

Submitted by

Deeksha Khosla

Registration Number : 12001009

Section : KE015

Course Code : INT 301

Course Title : Open-Source Technologies

Under the Guidance of

Dr. Manjot Kaur

School of Computer Science and Technology

CHAPTER-01

INTRODUCTION

Digital forensics has become increasingly important in the modern world, as technology has advanced and the use of electronic devices has become more widespread. This field encompasses a range of techniques and methods that are used to collect and analyze electronic data in order to investigate and prosecute crimes, as well as prevent security breaches. The ability to extract data from storage media is a key component of digital forensics, and it requires the use of specialized software tools.

In this particular project, we will be focusing on the use of an open source software called Autopsy to extract data from disk drives and other storage media. Autopsy is a powerful tool that is widely used in the field of digital forensics, and it offers a range of features that make it an excellent choice for this task. Our aim is to demonstrate the effectiveness of Autopsy in facilitating forensic analysis of computer systems, and to provide a practical example of how this software can be used to extract valuable data from storage media.

By the end of this project, we hope to have gained a deeper understanding of digital forensics and the role that software tools such as Autopsy play in this field. We also hope to have provided a useful resource for anyone who is interested in learning more about how to extract and analyze electronic data from storage media.

1.1. Objective of the project

The primary goal of this project is to provide a practical demonstration of how Autopsy can be used as apowerful and effective tool for digital forensics.

1. Understanding the basic principles of digital forensics and the importance of extracting data from storage media.
2. Learning how to use Autopsy to extract data from various types of storage media, including hard drives, USB drives, and memory cards.
3. Identifying and interpreting different types of file systems, partition types, and disk layouts, and understanding how this information can be used to extract data.
4. Analyzing and interpreting data that has been extracted using Autopsy, and identifying key pieces of information that can be used to investigate crimes or prevent security breaches.
5. Understanding the limitations of Autopsy and other digital forensics tools, and learning how to overcome common challenges and obstacles.
6. Documenting the entire process of using Autopsy to extract data from storage media, and providing a step-by-step guide that can be used as a reference for others who are interested in learning more about this process.

Ultimately, the aim of this project is to demonstrate the potential of Autopsy as a powerful and flexible tool for digital forensics, and to provide a practical example of how this tool can be used to extract valuable data from storage media. By the end of this project, we will have gained a deeper understanding of digital forensics.

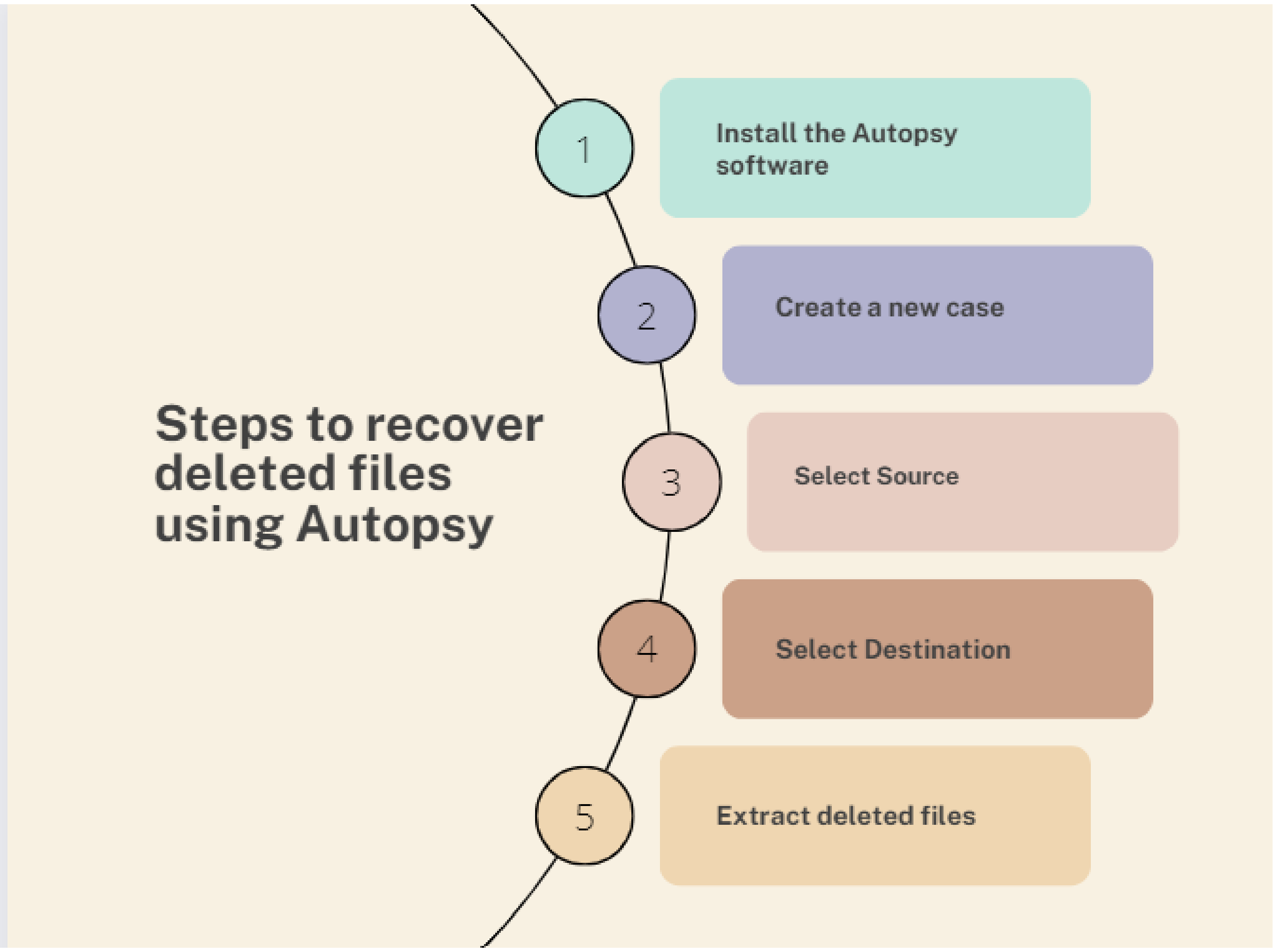


Fig1: Flowchart of the process

1.2. Description of the project

The project will begin with the installation and configuration of Autopsy on a computer system. This will involve downloading and installing the software, as well as configuring it to work with the storage media that will be analyzed. Once Autopsy has been set up, the project team will select a set of storage media, such as hard drives, USB drives, or memory cards, to be analyzed. The storage media may be acquired through a variety of means, such as through law enforcement or other sources.

The next stage of the project will involve using Autopsy to extract data from the selected storage media. This will involve running scans and searches using Autopsy's built-in tools, which include file analysis, keyword search, timeline analysis, and hash analysis. The extracted data will be stored in a secure location, and analyzed using a range of techniques to identify patterns, anomalies, and other important information.

Once the data has been extracted and analyzed, the findings will be documented in a report. This report will include a detailed description of the methods used to extract and analyze the data, as well as a summary of the key findings. The report will also provide recommendations for further investigation or action based on the findings of the analysis.

By the end of the project, the team will have gained a deep understanding of the capabilities of Autopsy as a tool for digital forensics, as well as a solid understanding of the principles and techniques of digital forensics more broadly. The project will provide valuable insights into the use of Autopsy for extracting and analyzing data from storage media, and will provide a practical example of how this tool can be used toinvestigate crimes or prevent security breaches.

1.3. Scope of the project

The scope of this project involves using an open source software tool to extract data from disk drives and other storage media, in order to facilitate the forensic analysis of computer systems. The project will involve selecting a suitable open source software tool, such as Autopsy, The Sleuth Kit, or TestDisk, and using it to extract data from a set of storage media. In this particular project we are using **AUTOPSY.**

The data extracted from the storage media will be analysed using the built-in tools of the selected software tool, such as file analysis, keyword search, timeline analysis, and hash analysis. The findings of the analysis will be documented in a report, which will highlight the key findings and provide recommendations for further investigation or action.

The project will require the installation and configuration of the selected software tool, as well as the acquisition of storage media for analysis. The project team will need to follow best practices and adhere to relevant ethical and legal standards throughout the project, such as obtaining consent from individuals whose data is being analysed and ensuring that the data is stored securely.

The scope of the project will also include gaining a deep understanding of the capabilities of the selected software tool for digital forensics, as well as a solid understanding of the principles and techniques of digital forensics more broadly.

CHAPTER-02

SYSTEM DESCRIPTION

2.1. Target System Description

The target system for this project is a device running a regular Windows 10 operating system. The device has an 8GB RAM and 1TB of HDD and 256 GB of SSD for the framework to work efficiently. The device is running on a regular device and not using any virtual machine to work.

2.2. Assumptions and Dependencies

It is assumed that the target device is not compromised and has no malware or virus present. Dependencies for this project include the open source software which is known as Autopsy digitalforensic tool.

2.3. Data set used in support of your project (if any then paste the link)

NOT APPLICABLE

2.4. Methodology

The methodology for this project involves the

following steps:

Step 1: Installation of the software.

Step 2: Analyze and setup the software

Step 3: scanning for the forensic findings and extraction for any deleted files

Step 4: Identifying the file and recovery of the target

CHAPTER-03

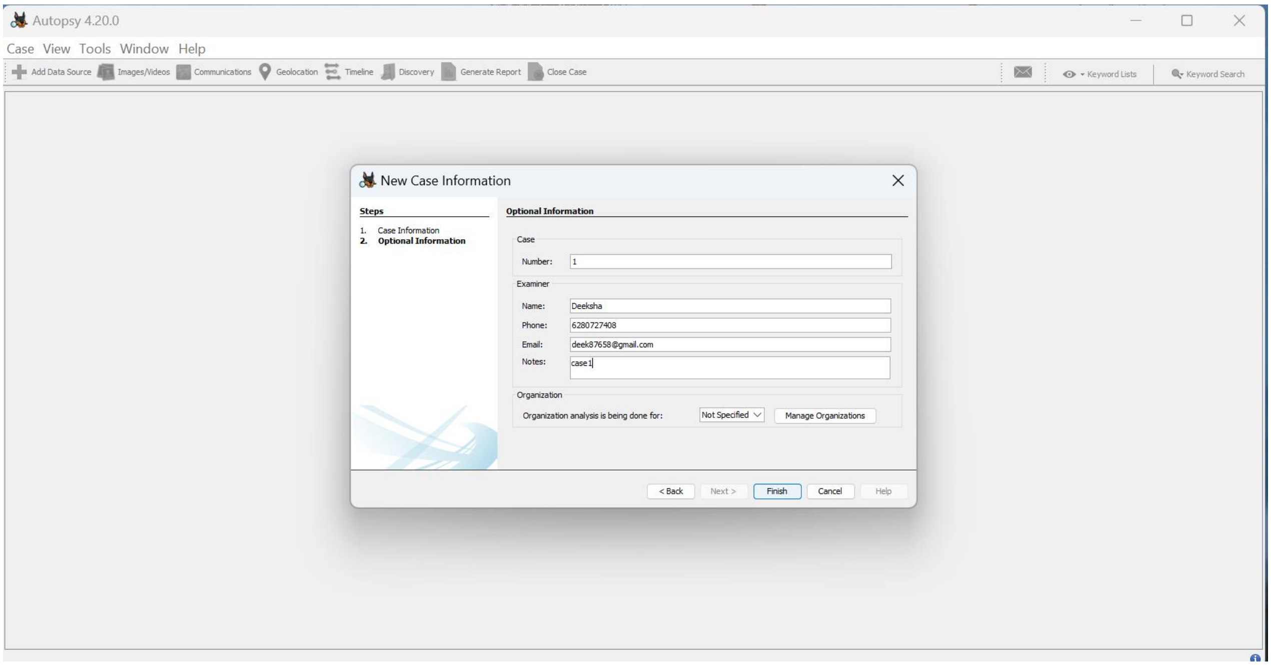
ANALYSIS REPORT

3.1. System Snapshots and Full Analysis Report

Step 1: Download and Install Autopsy, Anyone can download it from the official Autopsy website https://www.autopsy.com/download/ and then follow the instructions to install

Step 2: After the full installation process is done then it’s time select the first case,

After making the first case we need to give information of the investigator so that the software can keep the record of the case.



New Case Information

Steps

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

Optional Information

Case

Number: 1

Examiner

Name: Deeksha

Phone: 6280727408

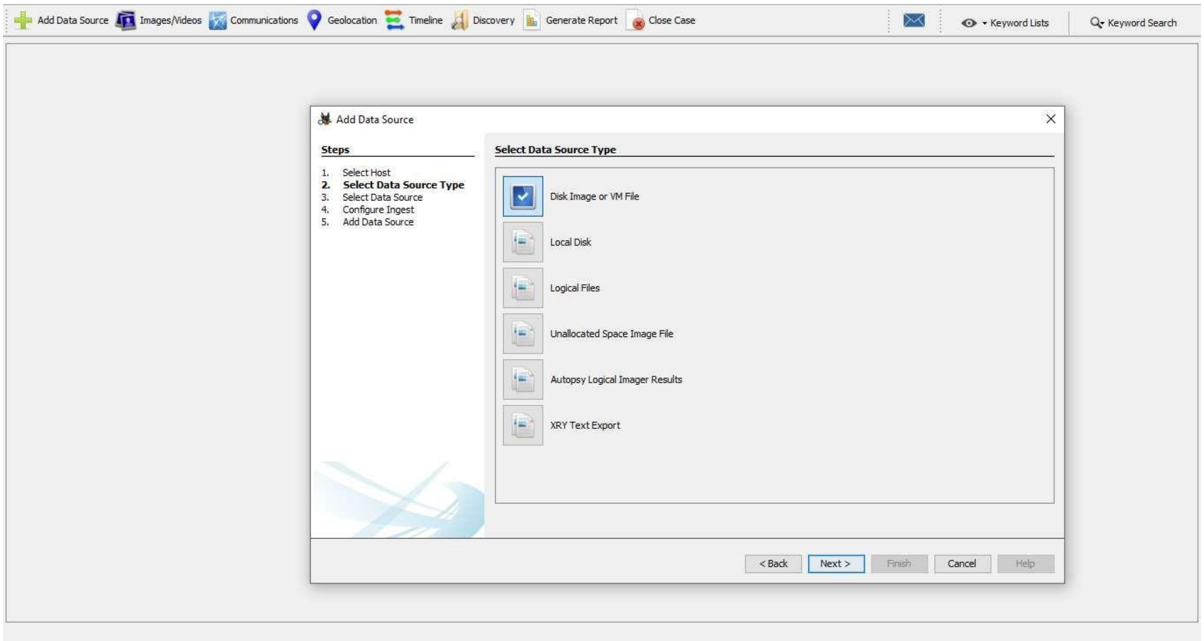
Email: deek87658@gmail.com

Notes: case1

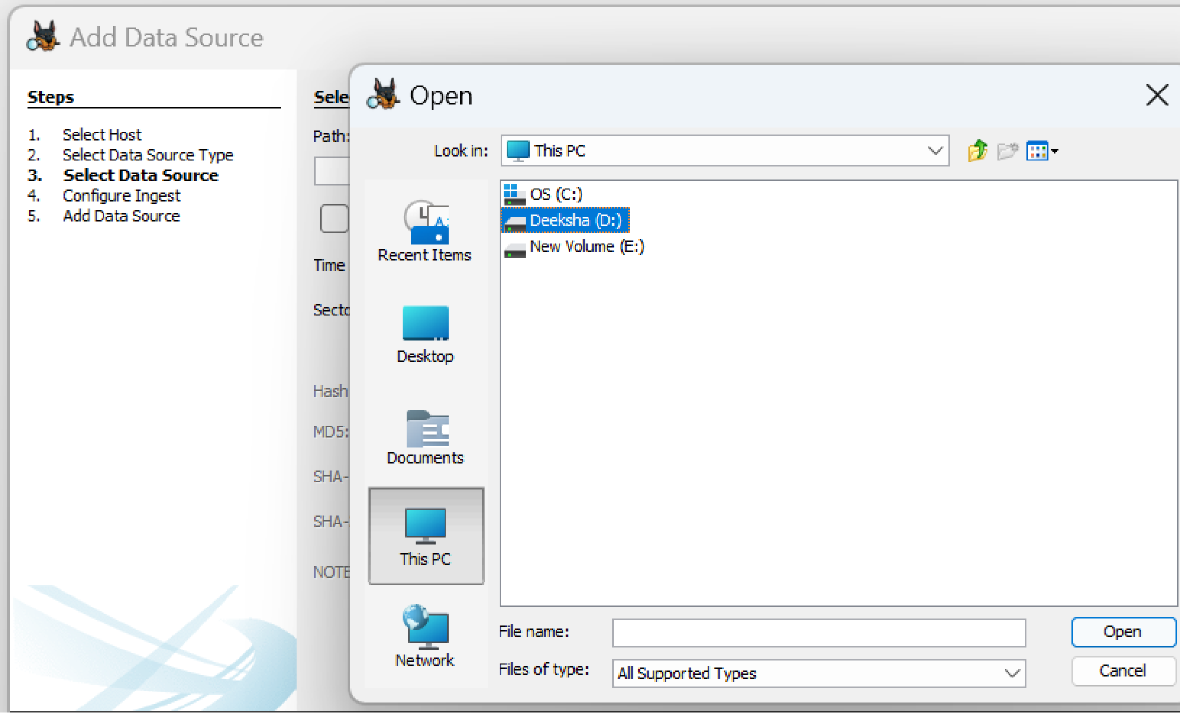
Organization

Organization analysis is being done for: Not Specified

Step 3: after giving the information we need to select the Data storage type, which is in this case in the local disk.



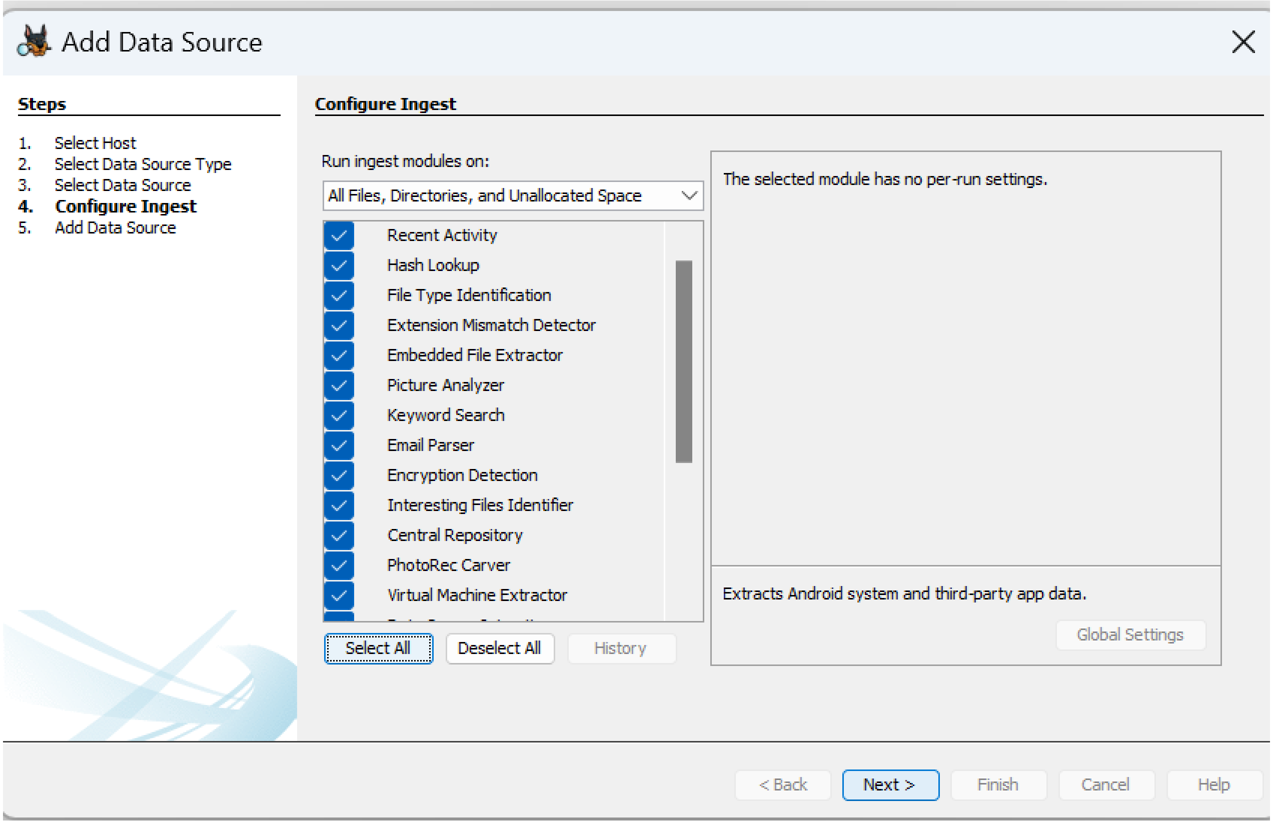
Step 4: in this step we need to select the exact drive from where we believe our targeted file isdeleted and one we selected that drive we are ready for the next steps.



Look in: This PC

Files of type: All Supported Types

Step 5: after all things are set, we have to select the file type, as the recovery process is very complex it is better to remove all the extra task that may cause the system to take more and unnecessary time, power and load.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

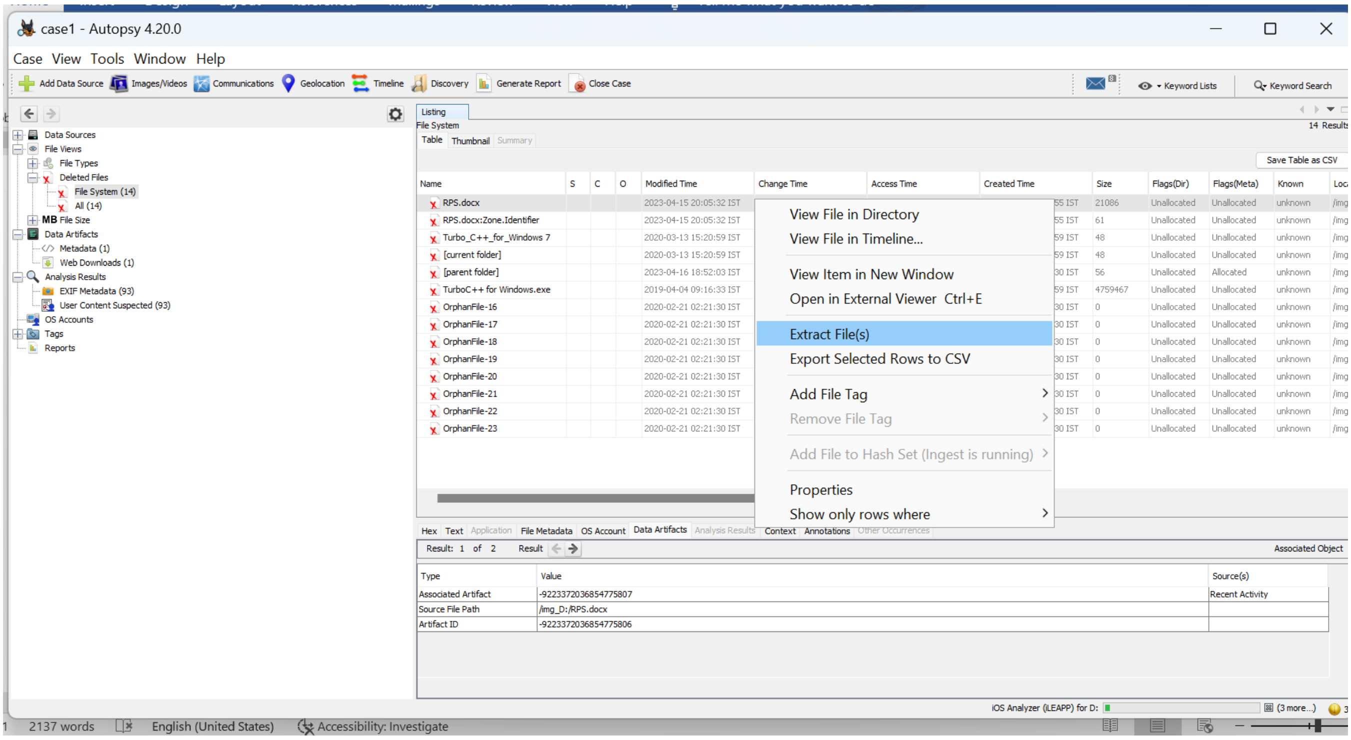
All Files, Directories, and Unallocated Space

☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Picture Analyzer
☑ Keyword Search
☑ Email Parser
☑ Encryption Detection
☑ Interesting Files Identifier
☑ Central Repository
☑ PhotoRec Carver
☑ Virtual Machine Extractor

The selected module has no per-run settings.

Extracts Android system and third-party app data.

Step 6: Here the software is started its analysis and finding all the deleted file that may be foundin the targeted drive.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Loc
RPS.docx				2023-04-15 20:05:32 IST			55 IST	21086	Unallocated	Unallocated	unknown	/img
RPS.docx:Zone.Identifier				2023-04-15 20:05:32 IST			55 IST	61	Unallocated	Unallocated	unknown	/img
Turbo_C++_for_Windows 7				2020-03-13 15:20:59 IST			59 IST	48	Unallocated	Unallocated	unknown	/img
[current folder]				2020-03-13 15:20:59 IST			59 IST	48	Unallocated	Unallocated	unknown	/img
[parent folder]				2023-04-16 18:52:03 IST			30 IST	56	Unallocated	Allocated	unknown	/img
TurboC++ for Windows.exe				2019-04-04 09:16:33 IST			59 IST	4759467	Unallocated	Unallocated	unknown	/img
OrphanFile-16				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img
OrphanFile-17				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img
OrphanFile-18				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img
OrphanFile-19				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img
OrphanFile-20				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img
OrphanFile-21				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img
OrphanFile-22				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img
OrphanFile-23				2020-02-21 02:21:30 IST			30 IST	0	Unallocated	Unallocated	unknown	/img

Type	Value	Source(s)
Associated Artifact	-9223372036854775807	Recent Activity
Source File Path	/img_D:/RPS.docx	
Artifact ID	-9223372036854775806	

Step 7: After a long process the software is found all the deleted files including our demonstrated file which we suppose to recover from the system “RPS.docx” after this we need to click on the extract file button and the software will recover the file on the target location for us.

Conclusion

In conclusion, the use of open source software tools such as Autopsy for digital forensics is becoming increasingly important in modern-day law enforcement and cybersecurity. This project has demonstrated the utility of Autopsy in extracting data from disk drives and other storage media, and in facilitating forensic analysis of computer systems.

By successfully recovering a deleted file from the drive with the help of Autopsy, the project has shown the potential of open source software tools for providing valuable evidence in investigations and legal cases. The project also highlights the importance of following best practices and adhering to relevant ethical and legal standards in digital forensics.

Furthermore, the project has provided valuable insights into the capabilities of Autopsy and other open source software tools for digital forensics, and has demonstrated the importance of acquiring a solid understanding of the principles and techniques of digital forensics when using these tools.

Overall, the project has been successful in achieving its objective of demonstrating the use of Autopsy as an open source software tool for extracting data from disk drives and other storage media, and has provided a practical example of how these tools can be used to investigate crimes or prevent security breaches.

CHAPTER-04

REFERENCE/ BIBLIOGRAPHY

[1] Autopsy Official Website: https://www.autopsy.com/download/

[2] "Digital Forensics with Linux" by Cory Altheide and Harlan Carvey

[3] "File System Forensic Analysis" by Brian Carrier

[4] "Handbook of Digital Forensics and Investigation" edited by Eoghan Casey

[5] "Practical Forensic Imaging: Securing Digital Evidence with Linux Tools" by Bruce Nikkel

[6] "Linux Forensics" by Philip Polstra

[7] "Mastering Digital Forensics with PowerShell" by Alissa Torres and Mike Pilkington

[8] Carvey, H., & Altheide, C. (2011). Digital forensics with Linux. Prentice Hall Press.

[9] Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

[10] Casey, E. (Ed.). (2011). Handbook of digital forensics and investigation. Academic Press.

[11] Nikkel, B. (2014). Practical forensic imaging: Securing digital evidence with Linux tools. No Starch Press.

[12] Polstra, P. (2015). Linux forensics. No Starch Press.

[13] Torres, A., & Pilkington, M. (2019). Mastering digital forensics with PowerShell. Packt Publishing.

[14] Appel, A., & Vigna, G. (2012). An investigation of file carving signatures for forensic multimedia analysis. In Proceedings of the 12th Annual Conference on Digital Forensics, Security and Law (pp. 1-12).

[15] Chua, T., & Huang, K. (2013). Carving out deleted files in file allocation table systems. Digital Investigation, 10(1), 57-68.

[16] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64-S73.

[17] Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. In Proceedings of the 2003 ACM Workshop on Computer Security (pp. 41-52).

[18] Quick, D. (2005). File system analysis using The Sleuth Kit. Digital Investigation, 2(1), 7-12.

[19] Sammes, J., & Jenkinson, A. (2007). Forensic computing: A practitioner's guide. Springer Science & Business Media.