CA – 3

(Task Based)

Name – Kamal Kant
Registration No. – 11915735
Roll No. – 30
Section – KE015
Course Code – INT 301
Assigned Question – Q15

Submitted to – Dr. Manjot Kaur

1. Introduction

Fig 1.1. Email Forensics

Email Forensics: Emails play a very important role in business communications and have emerged as one of the most important applications on internet. They are a convenient mode for sending messages as well as documents, not only from computers but also from other electronic gadgets such as mobile phones and tablets.

In digital forensics, emails are considered as crucial evidence and Email Header Analysis has become important to collect evidence during forensic process.

Fig 1.2. Disk Forensics

Disk Forensics: Disk forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc...

1.1 Objectives of the project

The primary objective of email forensics is to focuses on the forensic analysis of email to collect digital evidence for cybersecurity attacks and cyber incidents. It comprises an in-depth forensic investigation of various email aspects such as Message-IDs, transmission routes, attached files and documents, IP addresses of servers and computers, etc. The analysis of emails and the content within to determine the legitimacy, source, date, time, the actual sender, and recipients in a forensically sound manner. The aim of this is to provide admissible digital evidence for use in civil or criminal courts.

The primary objective of disk forensics is to extract the forensic information from the digital drive such as hard disk drive, USB devices, floppy, CD, DVD and Flash Drives. The process of Disk Forensics are Identify digital evidence, Seize & Acquire the evidence, Authenticate the evidence, Preserve the evidence, Analyse the evidence, Report the findings and Documenting. Analysis is the process of collecting digital evidence from the content of the storage media depending upon the nature of the case being examined. This involves searching for keywords, picture analysis, timeline analysis, registry analysis, mailbox analysis, database analysis, cookies, temporary and Internet history files analysis, recovery of deleted items and analysis, data carving and analysis, format recovery and analysis, partition recovery and analysis, etc.

1.2 Description of the project

Emails play a very important role in business communications and have emerged as one of the most important applications on internet. They are a convenient mode for sending messages as well as documents, not only from computers but also from other electronic gadgets such as mobile phones and tablets.

The negative side of emails is that criminals may leak important information about their company. Hence, the role of emails in digital forensics has been increased in recent years. In digital forensics, emails are considered as crucial evidences and Email Header Analysis has become important to collect evidence during forensic process.

An investigator has the following goals while performing email forensics −

- To identify the main criminal
- To collect necessary evidences
- To presenting the findings
- To build the case

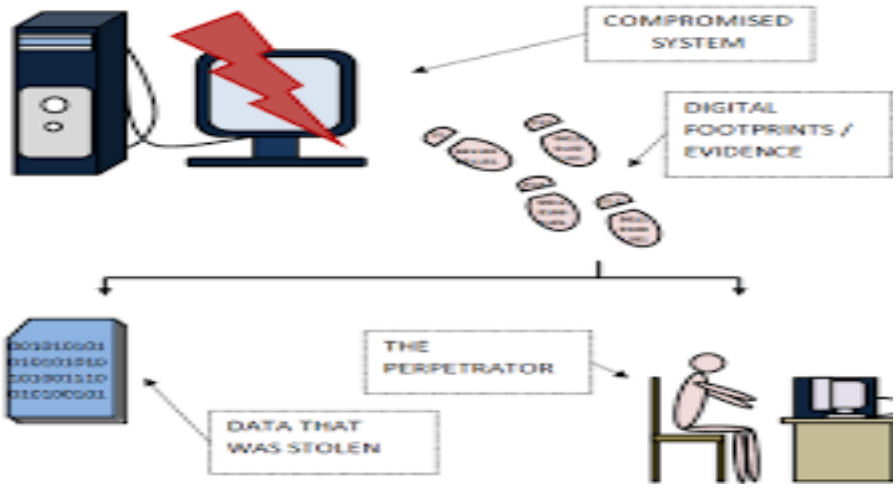


Fig 1.3. Stealing of Data

Disk forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc.. The process of Disk Forensics are

1. Identify digital evidence
2. Seize & Acquire the evidence
3. Authenticate the evidence
4. Preserve the evidence
5. Analyse the evidence
6. Report the findings
7. Documenting

First step in Disk Forensics is identification of storage devices at the scene of crime like hard disks with IDE/SATA/SCSI interfaces, CD, DVD, Floppy disk, Mobiles, PDAs, flash cards, SIM, USB/ Fire wire disks, Magnetic Tapes, Zip drives, Jazz drives etc. These are some of the sources of digital evidence.

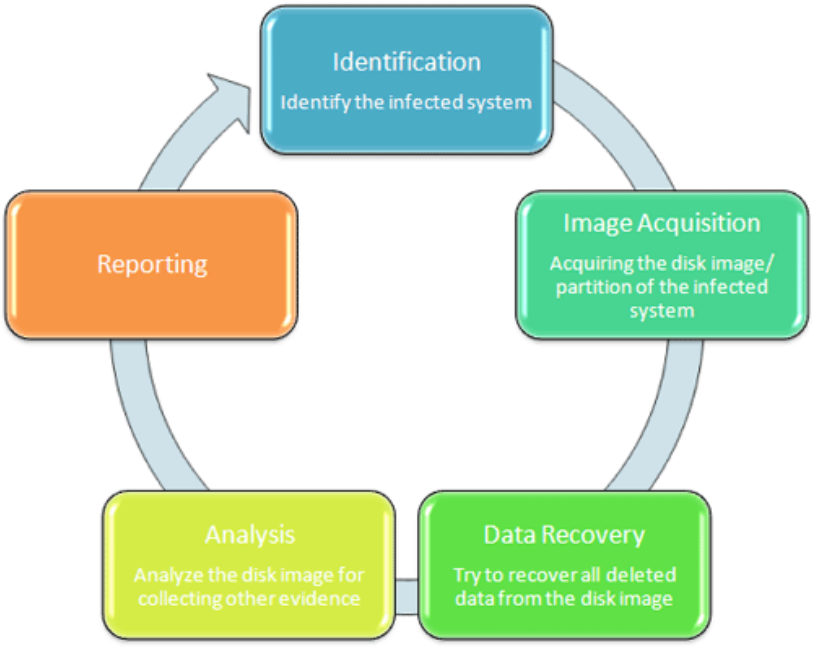


Fig 1.4. Process of Disk Forensics

1.3 Scope of the project

Email forensics is a branch of digital forensics that deals with the investigation of email-related crimes or incidents. It involves the recovery, preservation, analysis, and presentation of electronic evidence obtained from email systems, email messages, and related metadata. The scope of email forensics includes:

Email system analysis: Investigating the email server, logs, and other system files to determine how the email was sent, received, and stored.

Email content analysis: Examining the email message, attachments, and related metadata to determine the authenticity, integrity, and source of the email.

Email header analysis: Analyzing the email header information to trace the email's path and identify any anomalies or inconsistencies.

Email recovery and analysis: Recovering deleted or damaged email messages and analyzing them for relevant evidence.

Email tracing and tracking: Tracing the source and destination of the email, identifying the email sender, and tracking the email's path through various email servers and networks.

Email authentication and verification: Verifying the authenticity of the email message and attachments and determining if the email has been altered or tampered with.

Overall, the scope of email forensics is quite broad and covers a wide range of activities aimed at investigating and analyzing email-related incidents to support legal or criminal investigations.

Disk forensics, also known as computer or digital forensics, is a branch of digital forensics that deals with the investigation of computer storage devices such as hard drives, solid-state drives (SSDs), USB drives, memory cards, and other storage media. The scope of disk forensics includes:

Disk imaging: Creating a bit-by-bit copy of the storage device, including all data, metadata, and system files.

Data recovery: Recovering deleted, hidden, or encrypted files, and analyzing the recovered data for evidence.

File system analysis: Examining the file system and metadata to identify file creation and modification dates, file types, and file attributes.

Disk partition analysis: Analyzing the partition table to identify the location and size of partitions, and to recover lost or damaged partitions.

Registry analysis: Examining the Windows registry to recover deleted or modified registry keys and values.

Network analysis: Analyzing network traffic, logs, and other data to identify communication patterns and connections.

Malware analysis: Identifying and analyzing malware, including viruses, Trojans, and rootkits.

Data carving: Recovering fragmented or damaged files from disk sectors and unallocated space.

Timeline analysis: Creating a timeline of system events, including file creation, modification, and deletion, system shutdowns and reboots, and network connections.

Overall, the scope of disk forensics is quite broad and covers a wide range of activities aimed at investigating and analyzing computer storage devices to support legal or criminal investigations. Disk forensics is an important tool for law enforcement, corporations, and individuals to investigate computer-related crimes, intellectual property theft, and other digital security incidents.

2. System Description

2.1 Target System description

PhotoRec is a free and open-source file recovery software that is designed to recover lost files including photos, videos, and documents from a wide range of storage devices such as hard drives, USB drives, memory cards, and CD/DVDs. PhotoRec was originally designed to recover digital images, but it can recover many other types of files as well. PhotoRec is a command-line tool that works by analyzing the data stored on the storage device to find and recover deleted or damaged files. It uses file headers and data patterns to identify and recover lost files. PhotoRec is a powerful tool that can recover files from damaged or reformatted disks, and it supports a wide range of file systems, including FAT, NTFS, and EXT.One advantage of using PhotoRec is that it is free and open source, which means that it is widely available and can be used by anyone. It also supports a wide range of platforms including Windows, macOS, and Linux, making it a versatile tool for data recovery. However, since PhotoRec is a command-line tool, it may be less user-friendly than some other data recovery software.

grep is a command-line tool used in Unix-based operating systems to search for specific strings or patterns of characters within a file or multiple files. The name "grep" stands for "global regular expression print". grep is a versatile tool that allows you to search for a wide range of patterns, including simple strings, regular expressions, and patterns that span multiple lines. It can search for patterns in a single file, or it can search for patterns across multiple files and directories. grep is a powerful tool that can be used to quickly search for and find specific strings or patterns of characters within one or more files. Its versatility and ability to work with regular expressions make it a popular tool among developers, system administrators, and other users of Unix-based systems.

2.2 Assumptions and dependencies

As a data recovery tool Photorec relies on several assumptions and dependencies to function effectively. Some of these include:

File system support: PhotoRec assumes that the file system of the storage device being analyzed is supported by the software. While PhotoRec supports a wide range of file systems, there may be some unsupported file systems that it cannot analyze.

File fragmentation: PhotoRec assumes that files are not fragmented across multiple sectors. If a file is fragmented, PhotoRec may not be able to recover the entire file.

Physical damage: PhotoRec assumes that the storage device being analyzed is physically intact and not damaged. If the device is physically damaged, PhotoRec may not be able to recover any data.

File formats: PhotoRec assumes that it can identify the file format of the recovered data. If a file format is not recognized, PhotoRec may not be able to recover the file.

System resources: PhotoRec requires a sufficient amount of system resources to perform data recovery. If the system does not have enough resources, PhotoRec may run slowly or not work properly.

Root privileges: PhotoRec requires root privileges to access and analyze certain parts of the storage device. If the user does not have root privileges, some features of PhotoRec may not be available.

User knowledge: PhotoRec assumes that the user has some knowledge of how to use a command-line interface and how to interpret the output of the software. If the user does not have this knowledge, they may have difficulty using PhotoRec effectively.

As a search tool grep relies on several assumptions and dependencies to function effectively. Some of these include:

File formats: grep assumes that the files being searched are in plain text format. It may not work properly on binary files or other non-text formats.

Regular expressions: grep relies on regular expressions to match patterns within files. Users must have a basic understanding of regular expressions to use grep effectively.

Command-line interface: grep is a command-line tool, which means that users must be comfortable working with the command line interface and understand basic Unix commands.

Operating system: grep is designed to work on Unix-based operating systems, such as Linux and macOS. While it is available on Windows through third-party tools like Cygwin or Git Bash, its behavior and features may differ from those on Unix-based systems.

Permissions: grep may not be able to search files if the user does not have permission to access them. Users must have appropriate permissions to search files and directories.

Output formatting: grep outputs the matching lines of a file by default, but users may need to use additional command-line options to customize the output format.

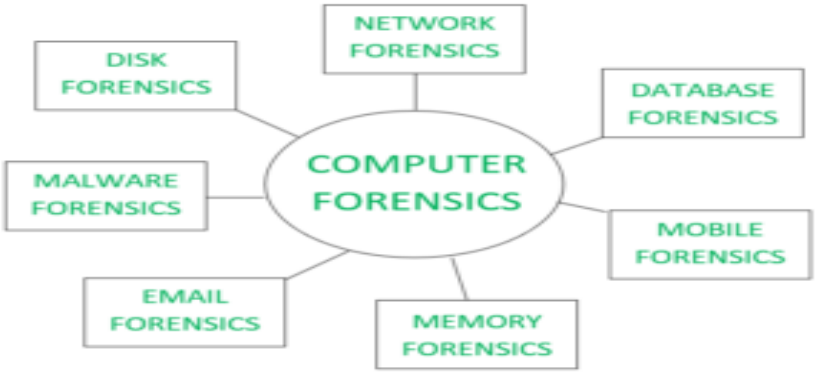


Fig 2.1 Different Types of Computer Forensics

2.3 Advantages of Photorec

Photorec is a powerful and versatile tool fordata recovery, and provides several advantages for users, including:

File Recovery: One of the main advantages of PhotoRec is its ability to recover a wide variety of file types, including photos, videos, documents, and more. It can recover files from a variety of storage devices, including hard drives, USB drives, memory cards, and CD/DVDs.

Cross-Platform Compatibility: PhotoRec is a cross-platform tool, which means that it can be used on a variety of operating systems including Windows, macOS, and Linux. This makes it a versatile option for data recovery, as users can easily switch between different operating systems without having to learn new tools.

Free and Open Source: PhotoRec is a free and open-source tool, which means that it is available to anyone and can be used without any licensing fees. This makes it an accessible option for users who need to recover lost data but cannot afford to purchase commercial software.

Powerful Algorithms: PhotoRec uses powerful algorithms to recover lost files, including file headers and data patterns to identify and recover files that have been deleted or damaged.

Disk Imaging: PhotoRec can create an image of a damaged or failing disk, which can be used to recover data even if the original disk is not accessible. This can be a lifesaver in situations where data loss is caused by physical damage to the storage device.

2.4 Disadvantages of Photorec

While PhotoRec is a powerful tool for data recovery, there are some potential disadvantages to consider when using it:

Command-line interface: PhotoRec uses a command-line interface, which may be less user-friendly than some other data recovery software with a graphical user interface (GUI). Users may need to be familiar with the command-line interface and understand basic Unix commands to use PhotoRec effectively.

Limited file preview: Unlike some other data recovery software, PhotoRec does not provide a file preview option, which means that users cannot view recovered files before saving them. This can make it difficult to determine if the recovered files are what the user is looking for, and may result in the recovery of unnecessary files.

File recovery quality: While PhotoRec is effective at recovering lost files, there is no guarantee that all files will be recovered, and some files may be corrupted or unrecoverable.

Fragmented files: If the storage device being recovered contains fragmented files, PhotoRec may not be able to recover the entire file, resulting in a partial or incomplete file recovery.

Limited file system support: While PhotoRec supports a wide range of file systems, there are some file systems that are not supported, such as Apple's APFS file system.

No file organization: When recovering files with PhotoRec, the recovered files are not organized in their original file structure, making it difficult to locate specific files.

2.5 Advantages of grep

grep is a powerful and versatile tool for searching for patterns in text files and provides several advantages for users, including:

Fast search: grep can search large amounts of text files quickly and efficiently, making it a useful tool for searching through log files or other large text files.

Versatility: grep is a versatile tool that allows users to search for a wide range of patterns using regular expressions, making it a powerful tool for developers, system administrators, and other users of Unix-based systems.

Customizable output: grep allows users to customize the output format to display additional information such as line numbers or context lines.

Multiple file search: grep can search for patterns across multiple files and directories, making it a useful tool for batch processing.

Unix integration: grep is integrated with the Unix command line interface, which means that it can be easily combined with other Unix commands to perform complex operations.

Availability: grep is a standard Unix command and is available on almost all Unix-based operating systems, making it an accessible tool for users of these systems.

2.6 Disadvantages of grep

While grep is a powerful and versatile tool for searching files, it does have some potential disadvantages:

Limited context: By default, grep only shows the lines of a file that match the search pattern, without providing additional context. This can make it difficult to understand the meaning of the matched lines, especially if the pattern is very general or if the file is large.

Regular expression complexity: grep uses regular expressions to match patterns, which can be very powerful but also very complex. Users need to have a good understanding of regular expressions to use grep effectively, and complex patterns can be difficult to create and debug.

Overwhelming output: When searching for patterns in multiple files, grep can produce a large amount of output, which can be overwhelming and difficult to parse. Users need to use additional options or pipe the output to other tools to refine and organize the results.

No GUI: grep is a command-line tool, which can be a disadvantage for users who prefer graphical user interfaces or who are not comfortable working with the command line.

Limited file formats: grep is designed to search plain text files and may not work properly on binary files or other non-text formats.

2.7 Functional Dependencies of Photorec

File recovery: PhotoRec's primary function is to recover lost or deleted files from various types of storage devices, including hard drives, USB drives, memory cards, and CD/DVDs.

File system support: PhotoRec supports a wide range of file systems, including FAT, NTFS, and EXT. This means that it can recover files from devices formatted with these file systems.

File type support: PhotoRec can recover a wide range of file types, including photos, videos, documents, and archives. It can recover files in various formats such as JPEG, PNG, PDF, and ZIP.

Cross-platform compatibility: PhotoRec is available for multiple platforms including Windows, macOS, and Linux. This means that it can be used on different operating systems without requiring any platform-specific modifications.

Free and open source: PhotoRec is free and open-source software, which means that it is available for anyone to use and can be modified to suit specific needs.

Command-line interface: PhotoRec is a command-line tool that requires users to interact with it through a terminal window. This makes it more suitable for users who are comfortable with the command line interface.

2.8 Functional Dependencies of “grep”

Searching: The primary function of grep is to search for specific strings or patterns of characters within files or directories.

Regular expressions: grep relies on regular expressions to define patterns and search for matches within files.

Pattern matching: grep can match patterns within a single line of a file or across multiple lines, depending on the search options used.

Filtering: grep can be used to filter files based on whether they contain a specific pattern or not, using options like -l or -L.

Output formatting: grep can output the matching lines of a file or the names of the files that contain a pattern, depending on the options used.

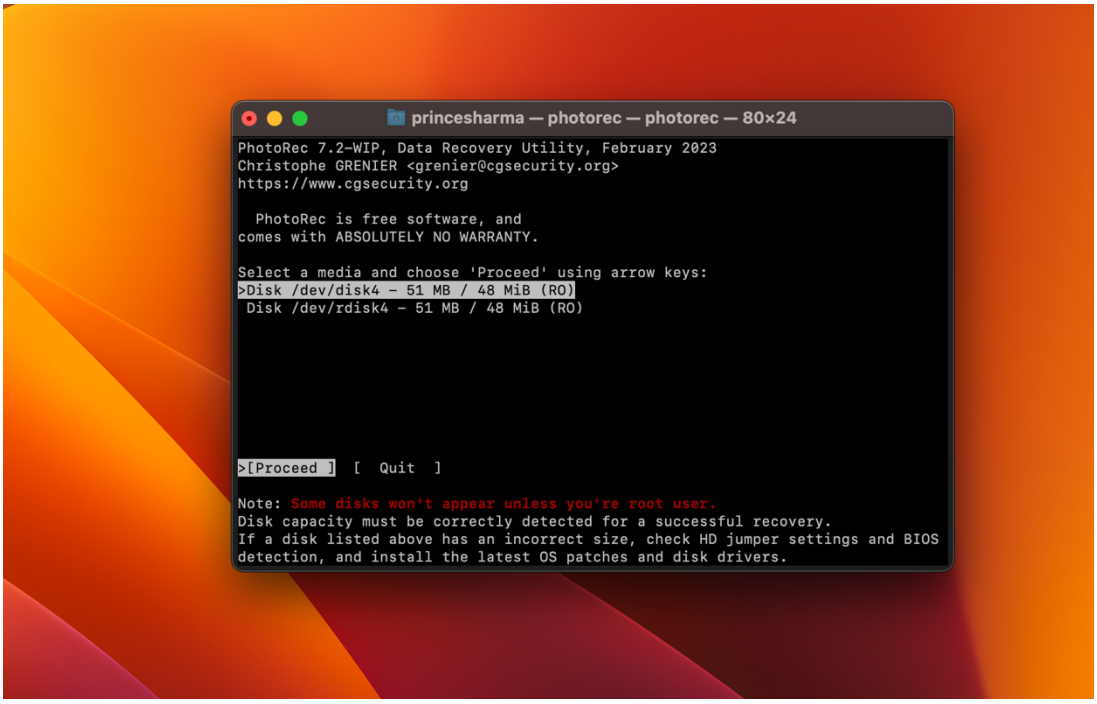
Recursive search: grep can recursively search through directories and subdirectories to find files that match a pattern.

Case sensitivity: grep can be used with case-sensitive or case-insensitive search options, depending on the search requirements.

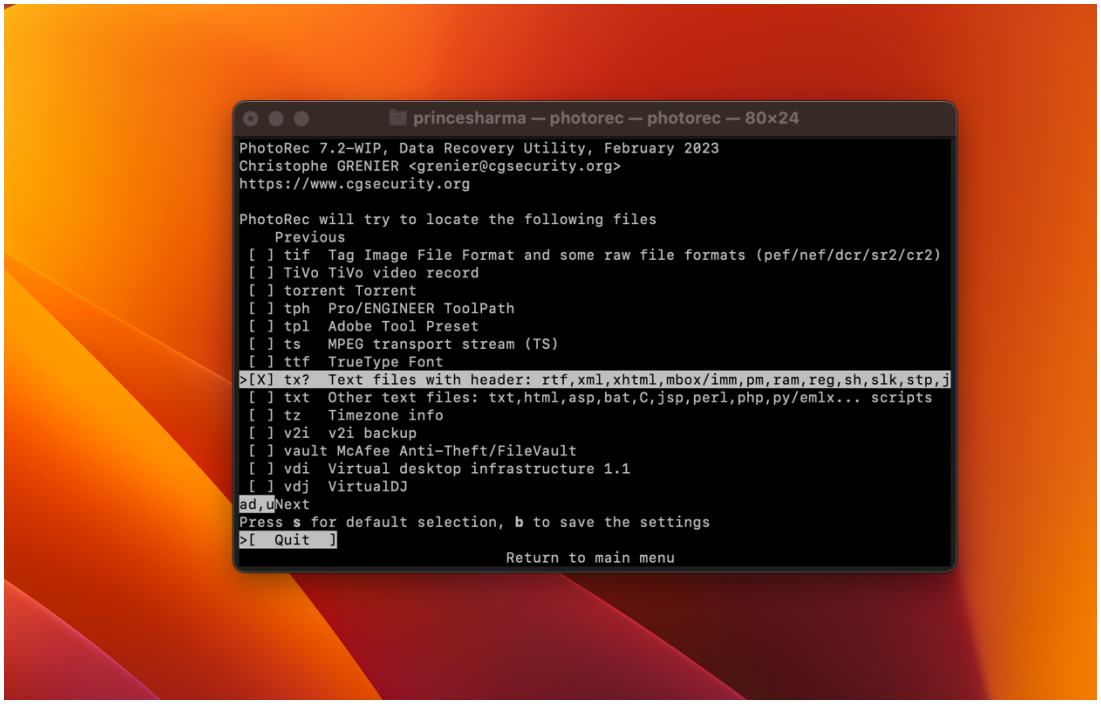
3. Analysis Report

3.1 Implementation of Email Recovery

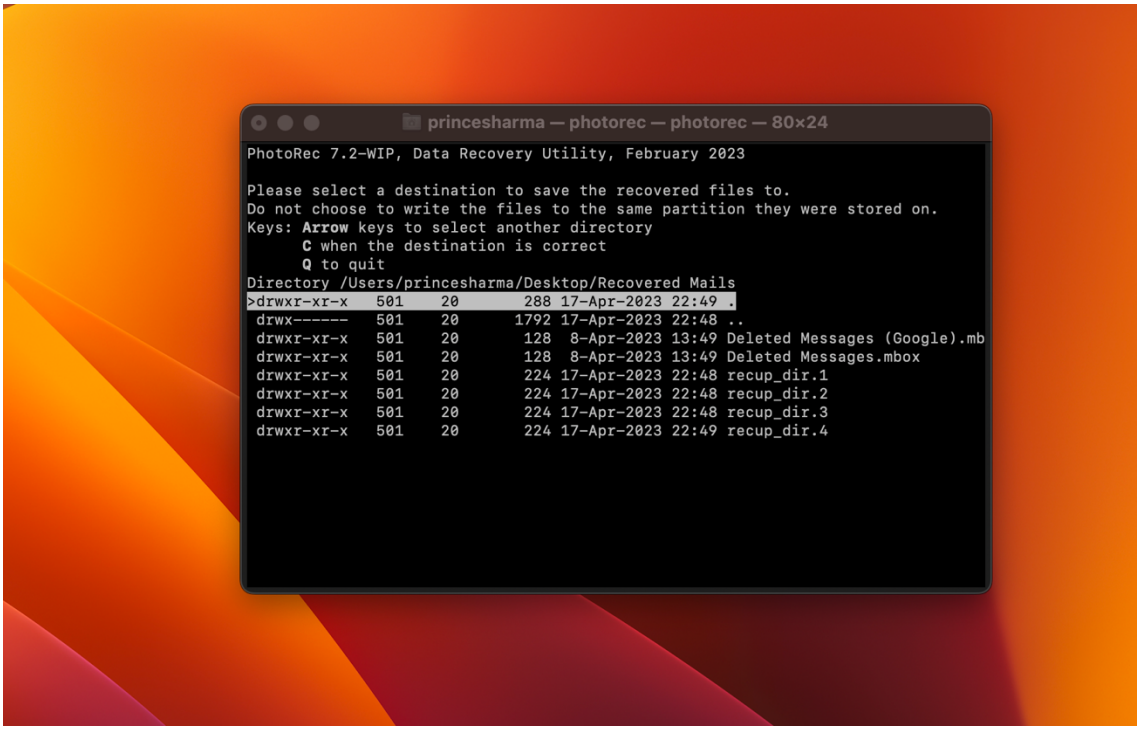
1. Select the disk from which you want to recover data.



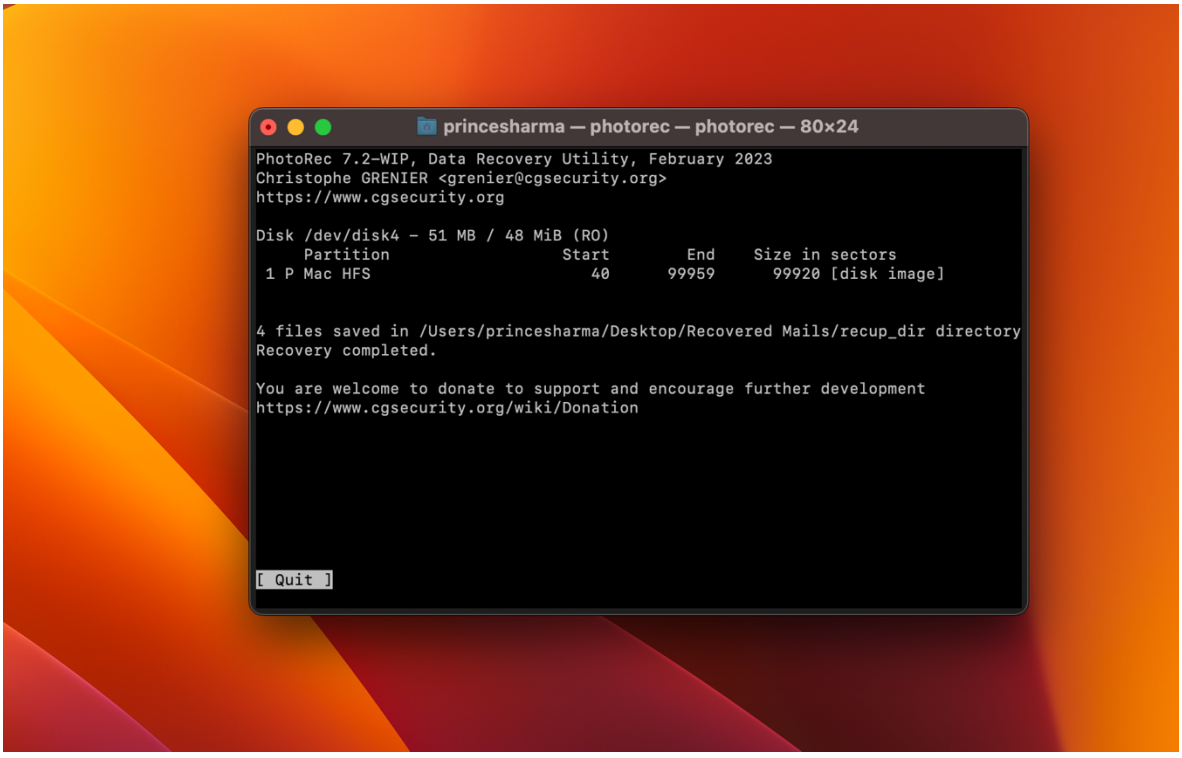
2. Select the type of file you want to recover.



3. Select the Destination path and press c

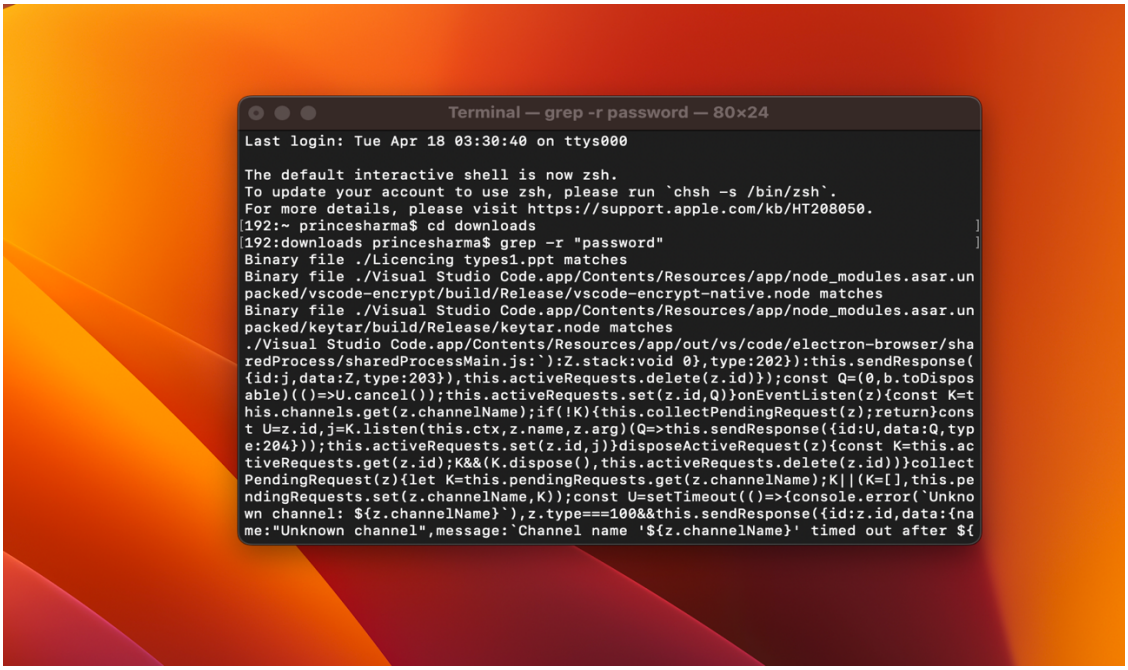


4. The files are recovered.

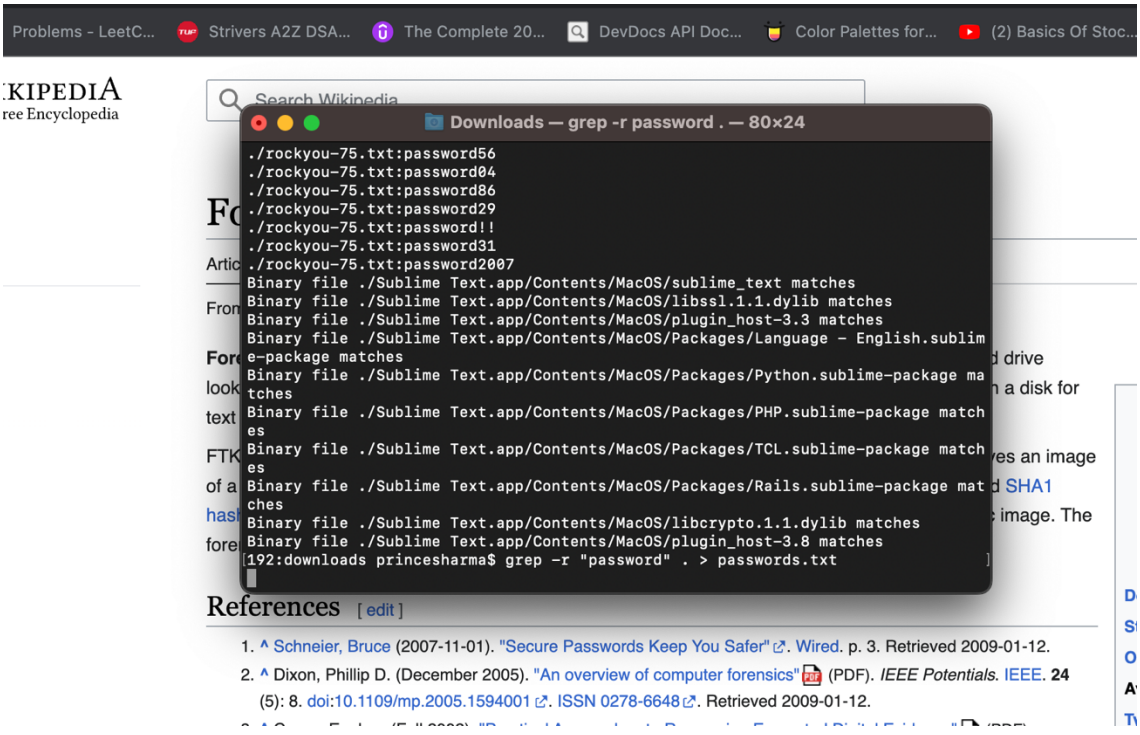


3.1 Implementation of disk scanning

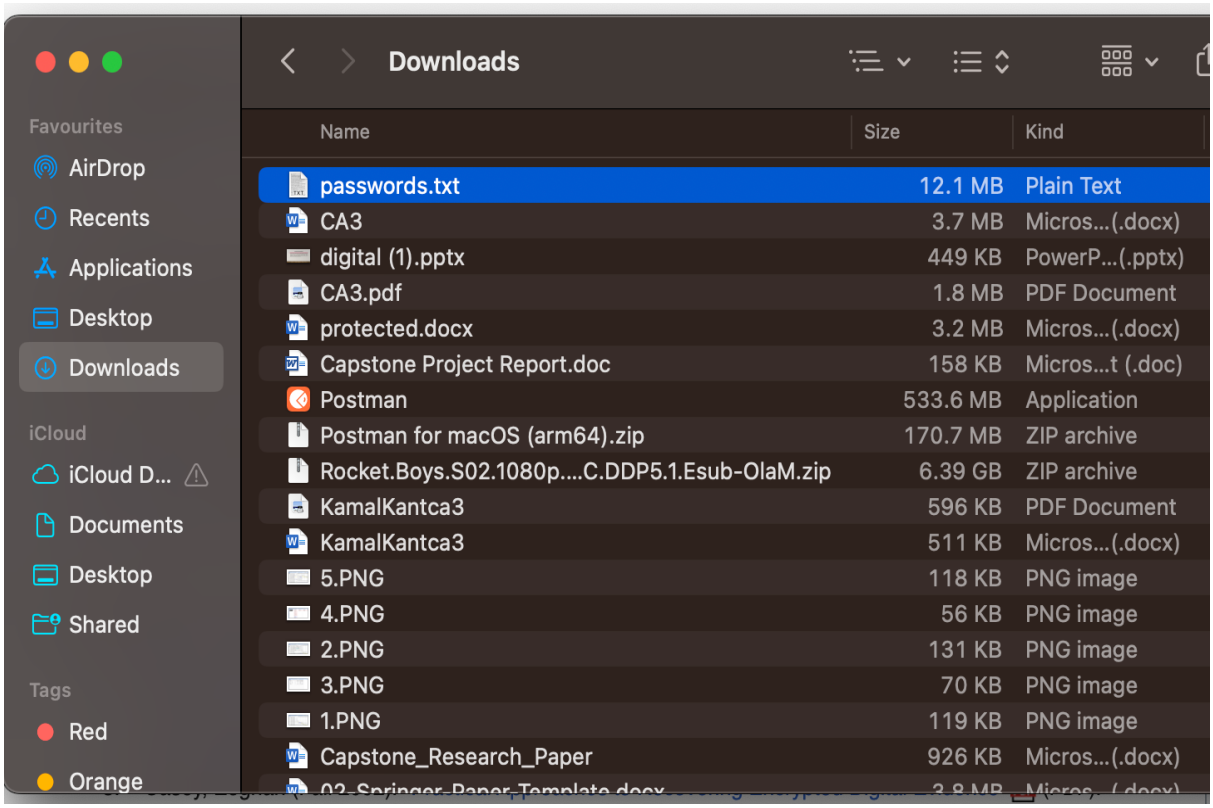
1. Go to the destination where you want to scan for text strings and use command “ grep -r “password” to scan disk for “password” string.



2. To save the output of the grep command to a txt file, use the following command: grep -r "password" . > passwords.txt. This will save the output to a file called "passwords.txt" in the current directory.



3. The required file which can be used as password dictionary



Reference/Bibliography

1. Garfinkel, S.L.: Digital Forensics Research: The Next 10 Years. Digital Investigation 7(suppl.), 64-73.
2. https://www.tutorialspoint.com/python_digital_forensics/python_digital_forensics_investigation_using_emails.htm
3. Digital Forensics Research Workshop. "A road map for digital forensics research, technical report", DFRWS, November 2001, pp. 15-20.
4. https://en.wikipedia.org/wiki/Forensic_Toolkit
5. Sommer P. "Intrusion detection systems as evidence". http://www.raidsymposium.org/raid98/Prog-RAID98/Full- Papers/Sommer-text.pdf, 200204-05.
6. https://en.wikipedia.org/wiki/EnCase
7. Research paper by Vamshee Krishna Devendran on “A Comparative Study of Email Forensics”

Gitub link - https://github.com/KamalKant786/open-source-project