LOVELY PROFESSIONAL UNIVERSITY

INT301 - OPEN-SOURCE TECHNOLOGIES

Academic Task-3

Submitted by

Pallab Gogoi

Reg. no : 11909573

Roll no: 22

Index

Chapter 1

1.Introduction:

What is computer forensics:

Computer forensics is a branch of digital forensics that involves the analysis, review, and preservation of electronic data stored on computers and other digital devices. This research area deals with the identification and recovery of digital evidence that can be used in legal proceedings such as criminal and civil cases. Computer forensics uses specialized tools and techniques to collect and analyse data from various sources such as hard drives, USB drives, smartphones, and other digital devices.

Types of computer forensics:

Database forensics:
Database forensics is a branch of digital forensic science that deals with analysis and recovery of data from compromised database.

Email forensics:

Email forensics is a branch of digital forensic science that deals with analysis of email messages to gather digital evidence.

Malware forensics:

Malware analysis is the process of analysing and dissecting malicious software, also known as malware, to identify its behaviour, purpose, and potential impact on a system.

Memory forensics:

It is a branch of digital forensics which deals with the analysis of RAM and cache.

Mobile forensics:

It is the examination of mobile devices to retrieve and analyse the information they contain, including contacts, incoming and outgoing text messages, pictures, and video files.

Network forensics:

Network forensics is a subfield of digital forensics that involves the investigation, analysis, and reconstruction of network activity to gather digital evidence for investigative purposes.

1.Objective of the project:

To use any open-source software to find and repair partly erased or damaged multimedia files from system from last 3 months.

1.1 Description of the project:

In this project an open-source software called PhotoRec which is used to recover, repair partly erased or damaged multimedia files. PhotoRec is created and maintained by CGSecurity, and they are available for a wide range of operating systems, including Windows, macOS, and Linux. PhotoRec is primarily designed for file recovery. It can recover lost or damaged files from a wide range of storage media, including hard drives, memory cards, USB drives, and more. It supports a wide range of file formats, including documents, photos, videos, and music files, among others. PhotoRec can even recover files from damaged or formatted partitions, as well as from disks with damaged or missing file systems. PhotoRec works by scanning the disk or media for file signatures, and then reconstructing the files based on the signatures.

1.2 Scope of the project:

The scope of the project is to use an open-source data recovery application to perform forensics on a particular drive and repair, recover data from it. Recovering lost data falls under the umbrella of forensics data collection. Forensics data collection process is mainly used by law-enforcement officials to gather evidence. Although such open-source applications can be used by general population to recover data that they lost accidently. The most important part of the data recovery process is carefully monitoring each stage to ensure the integrity of evidence is preserved and no tampering has occurred.

In this project demonstration document steps and process of data recovery using open-source application PhotoRec is explained. Photorec is a versatile data recovery software that can recover a wide range of lost files, including images such as JPEG, PNG, GIF, BMP, audio files like MP3 and WAV, video files such as MP4, AVI, MPEG, documents such as PDF, DOC, XLS, and archive formats like ZIP. It is a free and open-source software that is designed to recover data from various storage devices, including hard drives, memory cards, and USB drives. Photorec is a powerful tool that can help users recover their lost files quickly and efficiently.

Chapter 2

2. System Description

2.1 Target system description:

Processor: Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz 2.50 GHz

Installed RAM: 16 GB

Operating system: Microsoft Windows 11

System type: 64-bit operating system, x64-based processor

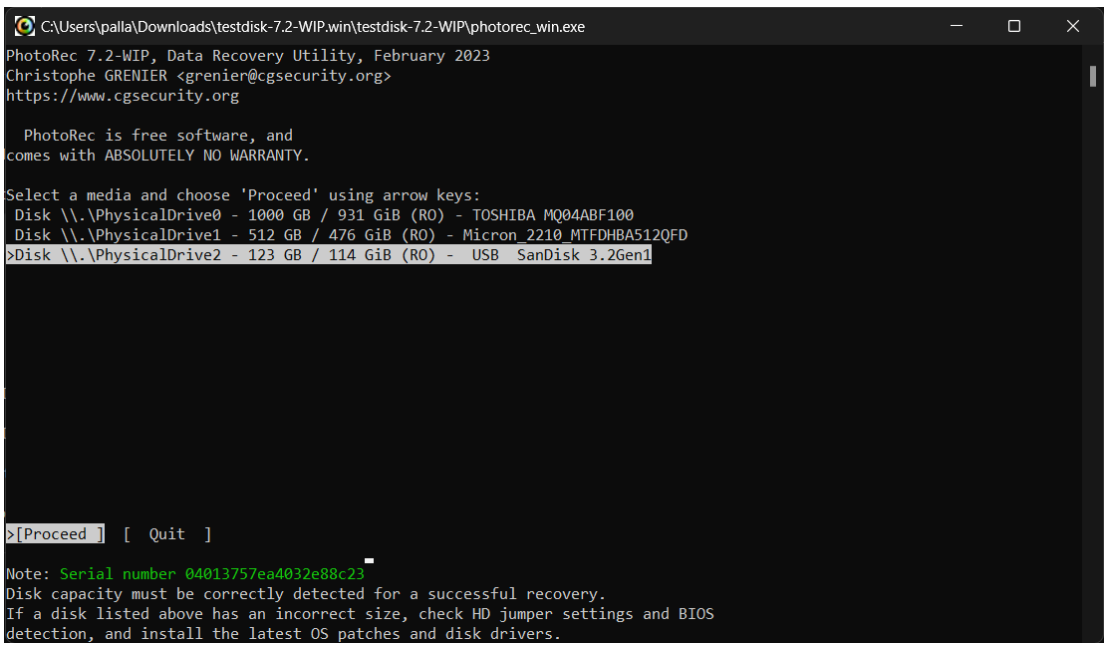
2.2 Assumptions and dependencies: A partition of a disk drive which was previously filled with image, video and text files for the test purpose was formatted and the analysis was done on that partition.

Chapter 3

3.Analysis report: This part contains the step-by-step process of using PhotoRec to analyse and recover lost data.

3.1 System snapshots and full analysis report:

Step 1: Download the application, locate, and execute the photorec_win.exe program. Details: Once the application is opened with proper permissions, it will open an interface where all connected disk drives are shown. Using the arrow keys select the desired disk drive and press ENTER key to proceed further.

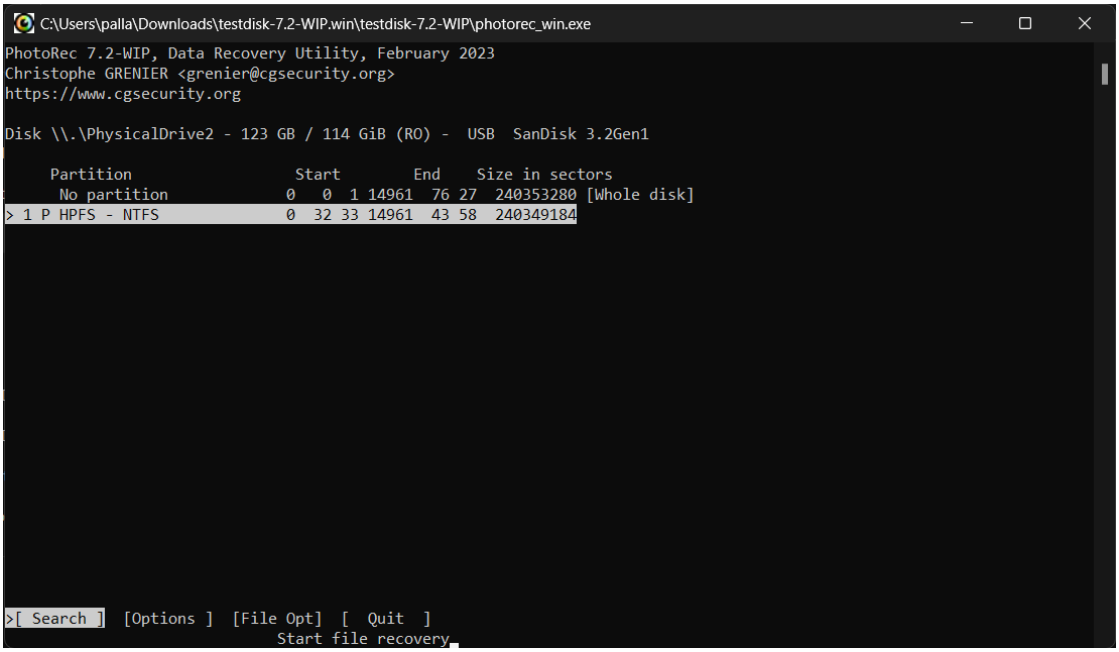


Snapshot 1: Selection of target disk drive

Step 2: Next step is to select the target partition from the disk drive. Using the arrow keys select the target partition and press ENTER key to proceed further.

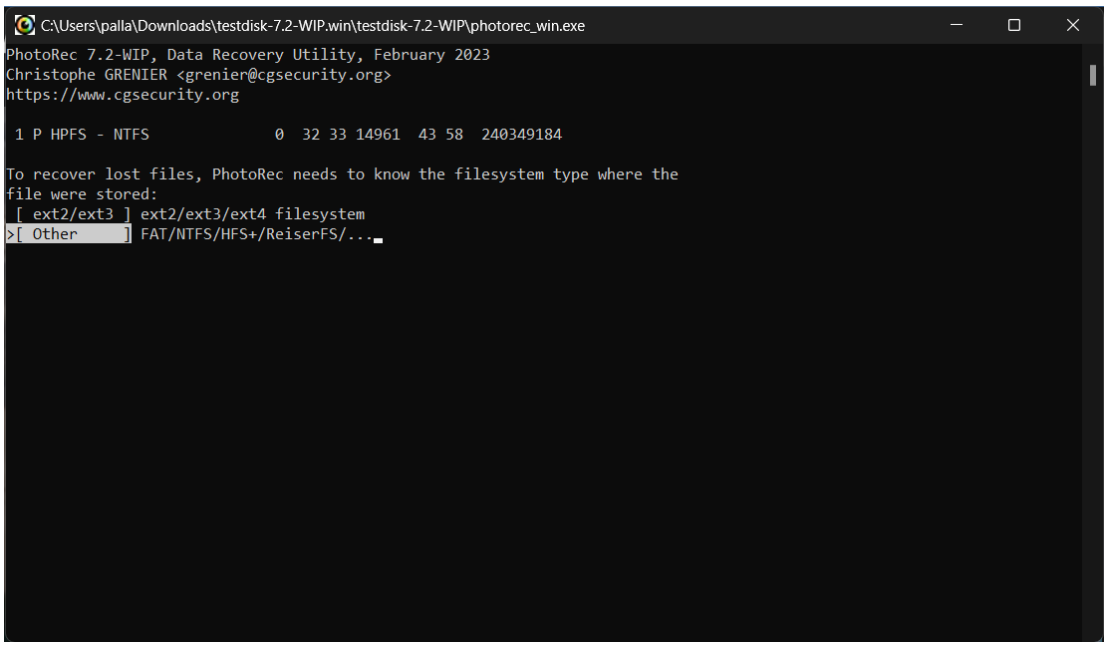
In this menu left and right arrow keys can be used to set more advanced file options.

For this example, the options are kept as default.



Snapshot 2: Partition is selected using up and down arrow keys.

Step 3: In this step filesystem type is selected where the files were stored. For Linux it is ext2/ext3/ext4 filesystem. For windows it is FAT/NTFS/HFs+/ReiserFS/… .Using the up and down arrow keys select the filesystem type and press ENTER to continue further.

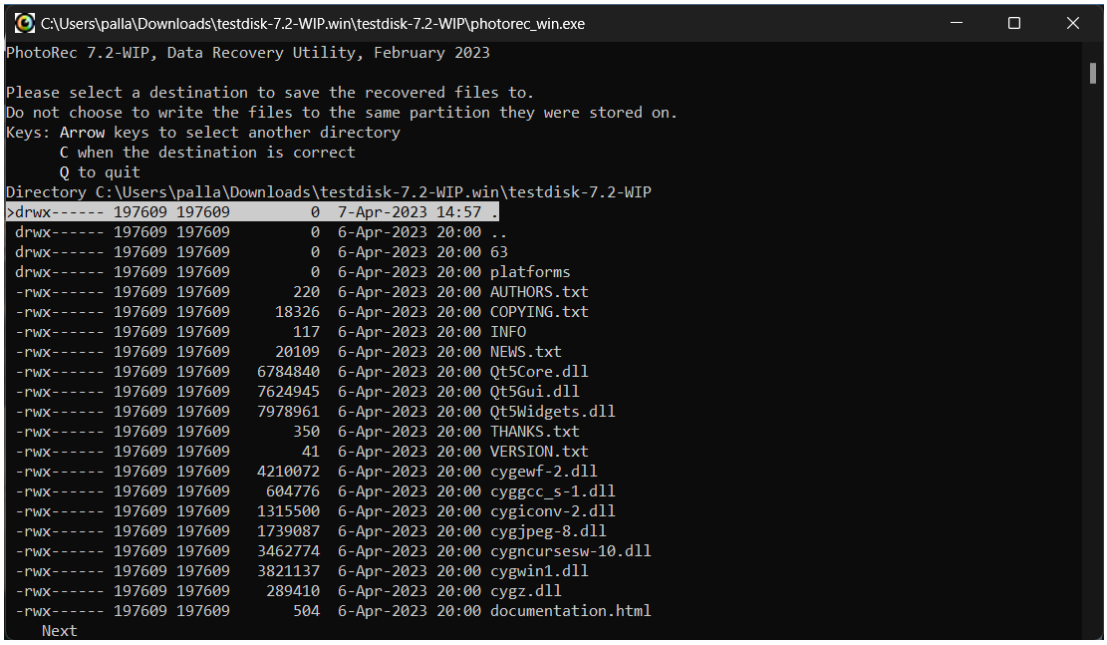


Snapshot 3: Selection of filesystem type.

Step 4: In this step destination to store the recovered files are set.

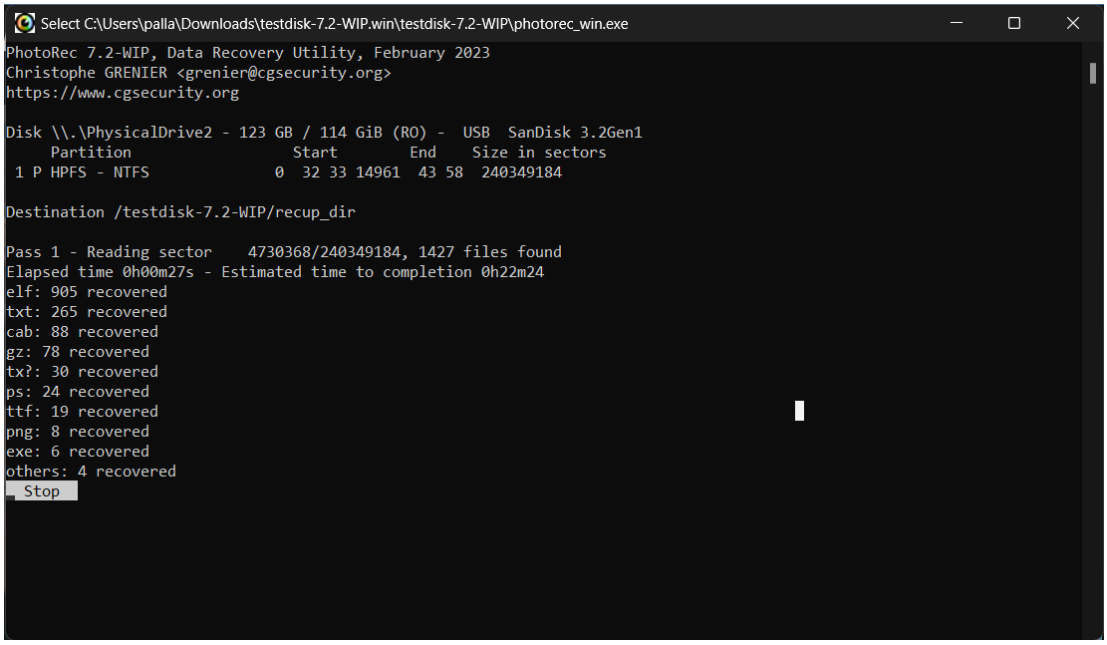
Up and down arrow keys are used to select desired destination and press “C” to select and confirm destination.

NOTE: Do not choose the partition on which you are working on as destination.



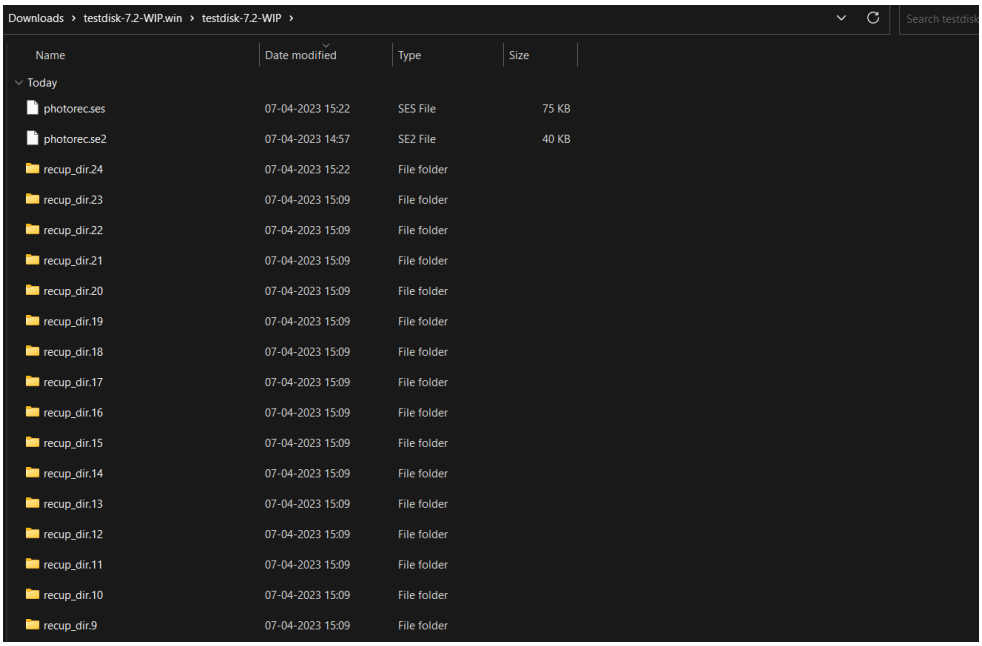
Snapshot 4: Destination for recovered files is selected.

Step 5: After the destination is selected the process of recovering files is automatically started. Depending upon the size of the partition and the target machine specification time to complete the recovery process varies.



Snapshot 5: Recovering files in progress.

Results: After the process is completed, we can go to the previously selected destination folder to see the recovered files. Recovered files are stored according to their file type inside a new directory named as “recup_dir.xx” ,here xx is digits in increasing order.



Snapshot 6: Recovered files.

4. Reference/ Bibliography

[1] https://www.cgsecurity.org/wiki/TestDisk
[2] https://www.techtarget.com/searchsecurity/definition/computer-forensics
[3] https://www.geeksforgeeks.org/introduction-of-computer-forensics/

5.Github Link: https://github.com/pallab-gogoi/INT301CA3