Report of Project

Sidra | 11905480 | 46

Lovely Professional University

INT301: Open Source Technologies

Dr. Manjot Kaur

https://github.com/Sidrasimrose/CA3

08/04/2023

INDEX

CHAPTER 1

1.Introduction

Computer Forensics

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Computer forensics -- which is sometimes referred to as computer forensic science -- essentially is data recovery with legal compliance guidelines to make the information admissible in legal proceedings.

In the civil and criminal justice system, computer forensics helps ensure the integrity of digital evidence presented in court cases. As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence -- and the forensic process used to collect, preserve and investigate it -- has become more important in solving crimes and other legal issues.

- Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- Database Forensics: It deals with the study and examination of databases and their related metadata.
- Malware Forensics: It deals with the identification of suspicious code and studying viruses, worms, etc.
- Email Forensics: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.

- Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- Mobile Phone Forensics: It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.

Advantages of computer forensics:

- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

Disadvantages of computer Forensics:

- Before the digital evidence is accepted into court it must be proved that it is not tampered with.
- Producing and keeping electronic records safe is expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.
- If the tool used for digital forensics is not according to specified standards, then in a court of law, the evidence can be disapproved by justice.
- A lack of technical knowledge by the investigating officer might not offer the desired result.

This project of recovering partly erased damaged files from last 3 months comes under memory forensics.

Memory Forensics: It is the art of analyzing a computer's memory dump for the purpose of investigating an incident or collecting evidence. This can be useful for a variety of purposes, such as determining the root cause of a system crash, identifying malware infections, or recovering lost or deleted data.

1.1 Objective of the project

The objective of this project is to use open source software to find and repair partly erased or damaged multimedia files from a system within the last 3 months.

1.2 Description of the project

Multimedia files, such as photos, videos, and audio recordings, are important assets for many users. Unfortunately, these files can become corrupted, damaged, or accidentally deleted. The purpose of this project is to use open source software to recover and repair multimedia files that have been partially erased or damaged on a system within the last 3 months.

1.3 Scope of the project

The scope of this project is to recover and repair multimedia files that have been partially erased or damaged within the last 3 months. The project will focus on open source software (EaseUS) that is freely available and can be run on a typical desktop computer.

CHAPTER 2

1. System Description

2.1 Target system description

The target system for this project is a typical desktop computer running a modern operating system, such as Windows, macOS, or Linux. The computer should have a standard set of multimedia files, including photos, videos, and audio recordings, that have been partially erased or damaged within the last 3 months.

2.2 Assumptions and Dependencies

The project assumes that the target system has not been subject to any major hardware failures or other catastrophic events that would prevent the recovery of multimedia files. The project also assumes that the open source software used is compatible with the target system and can be installed and run without issue.

2.3 Functional/Non-Functional Dependencies

The project depends on the functionality of open source software tools to recover and repair multimedia files. Non-functional dependencies may include the availability of hardware resources, such as storage space and processing power, to run the open source software.

2.4 Data set used in support of project

The project will use a sample set of multimedia files, including photos, videos, and audio recordings, that have been partially erased or damaged within the last 3 months. The files will be sourced from a test system and will not include any sensitive or private information. No data set is required for this project.

2.5 Software description

EaseUS Data Recovery Wizard is not just another data recovery software, but also a user-friendly app, with a Windows Explorer type interface, and a three-step easy file recovery process. It works on internal and external hard drives, USB flash drives, memory cards and various types

of partitions. EaseUS can easily do Format Recovery, Partition Recovery and recover deleted files emptied from Recycle Bin or recover lost data due to software crash, virus infection, unexpected shutdown or any other unknown reasons from FAT/NTFS file system under Windows 2000/XP/2003/Vista/2008/Windows 7.

Features of the software

- Recover deleted or lost files emptied from the Recycle Bin.
- File recovery with original file name and storage path after accidental format, even if you have reinstalled Windows.
- Disk recovery after a hard disk crash, partitioning error, partition loss.
- Get data back from RAW hard drives.
- Recover office document, photo, image, video, music, email, etc.
- Powerful search file function after scanning.
- Create a disk image of the current status of your hard drive.
- Continue previous recovery without rescan.
- Recover from hard drive, USB drive, memory card, memory stick, camera card, Zip drive, floppy disk or other storage media.
- Support FAT12, FAT16, FAT32, NTFS/NTFS5 and EXT2/EXT3 file systems.
- Support Windows 2000/XP/2003/Vista/2008/Windows 7 Operating Systems.
- Support MBR disk, dynamic disk and GPT disk.
- Powerful recovery algorithm.
- High quality of file recovery.

CHAPTER 3

3. **Analysis Report**

3.1 System snapshots and full analysis report

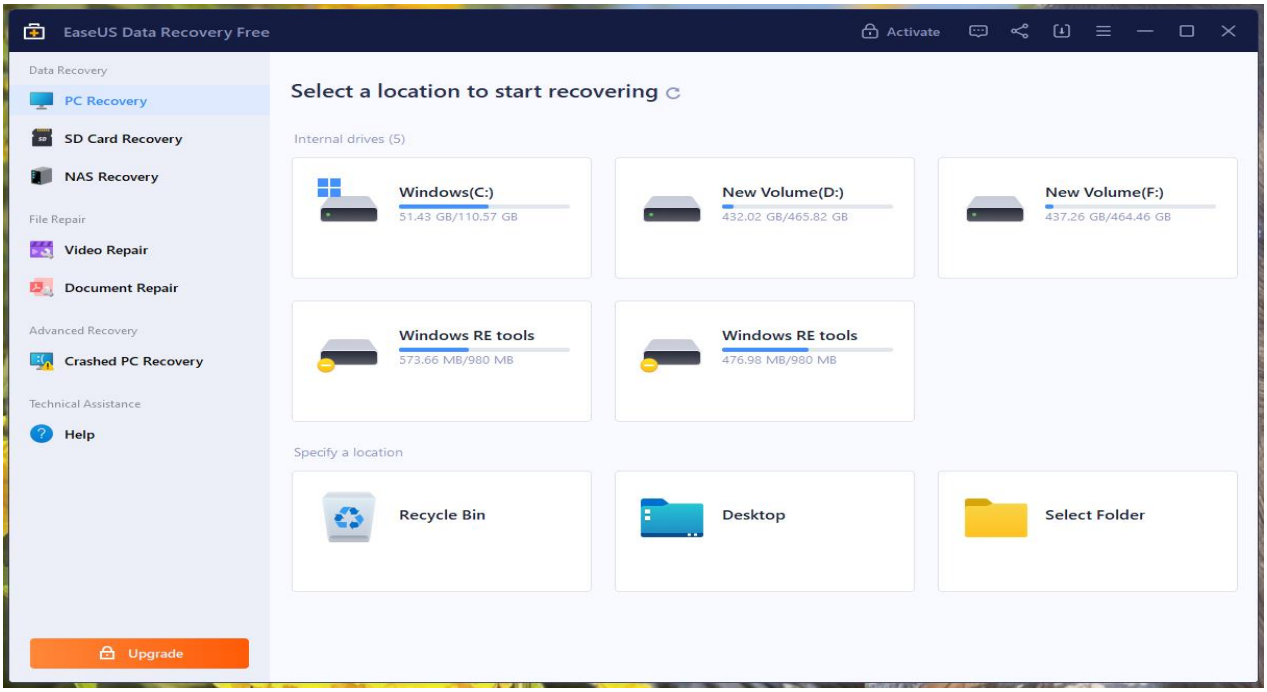

Fig 1. Home page

Once the software is installed, we can go ahead and select one of the drives shown in the interface. The demonstration uses ‘New Volume(D:)’ to run a full scan.

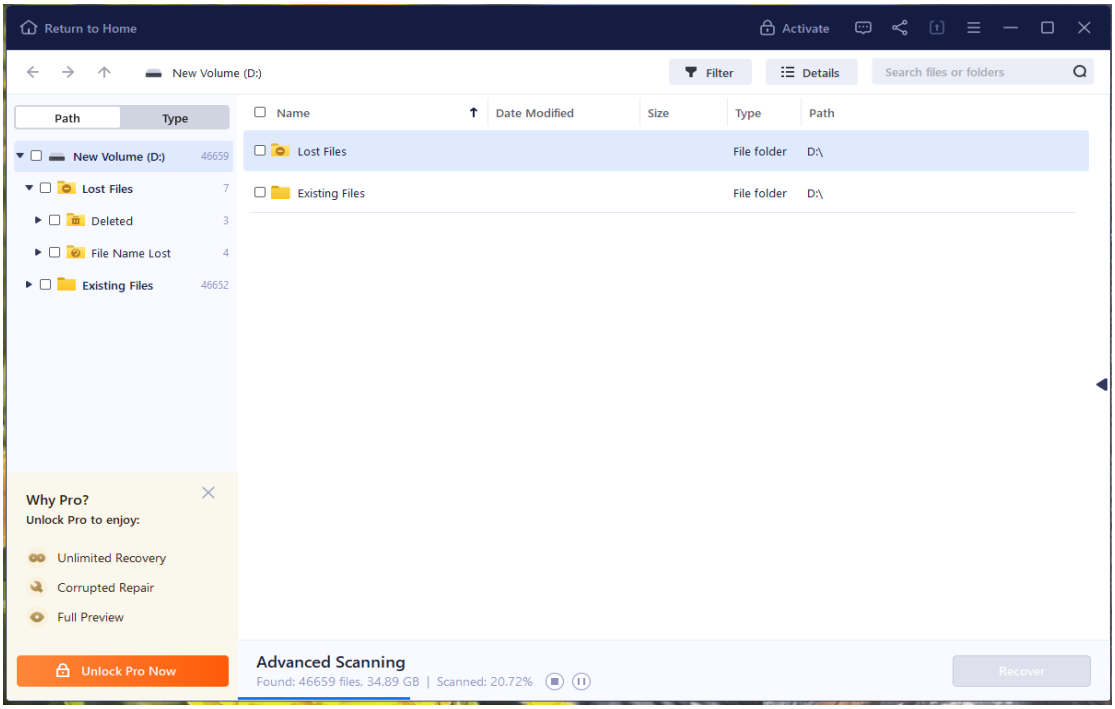

Fig. 2 Choose lost/Existing Files

In this image the software asks of you want to recover data from lost files or existing files.

.

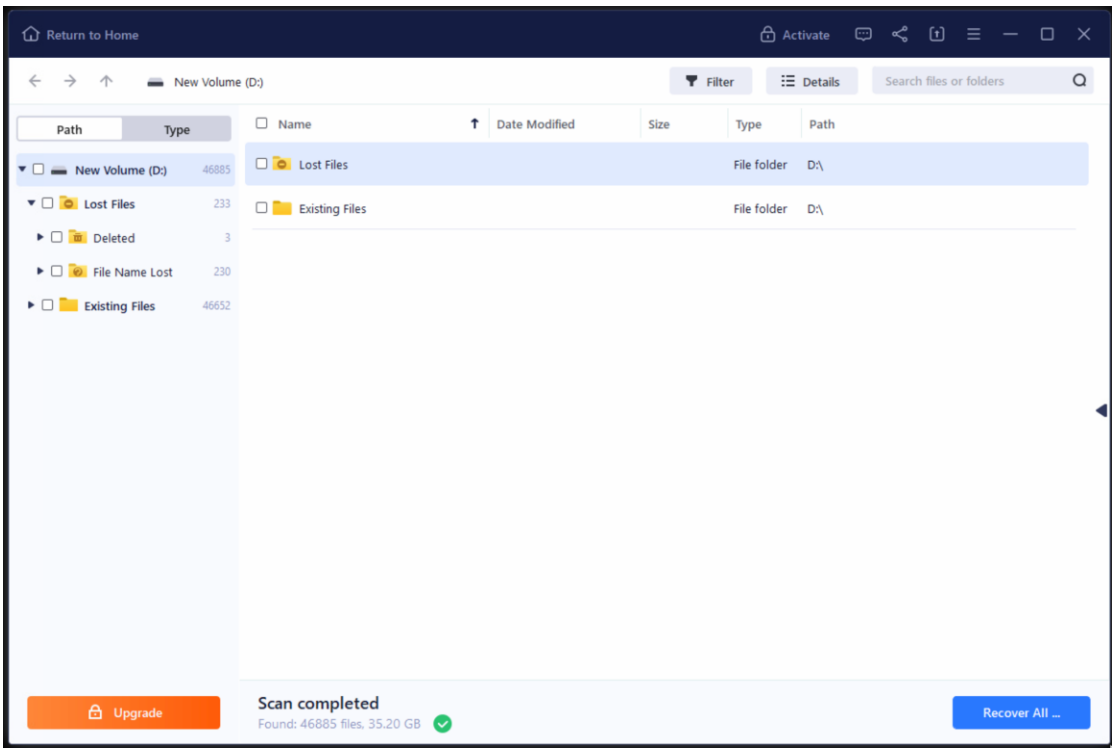

Fig. 3 Scan approved

In the above image we have selected the folders which we want to recover and then the software scans our drive. It gives us an analysis of our drive, saying 46885 files found.

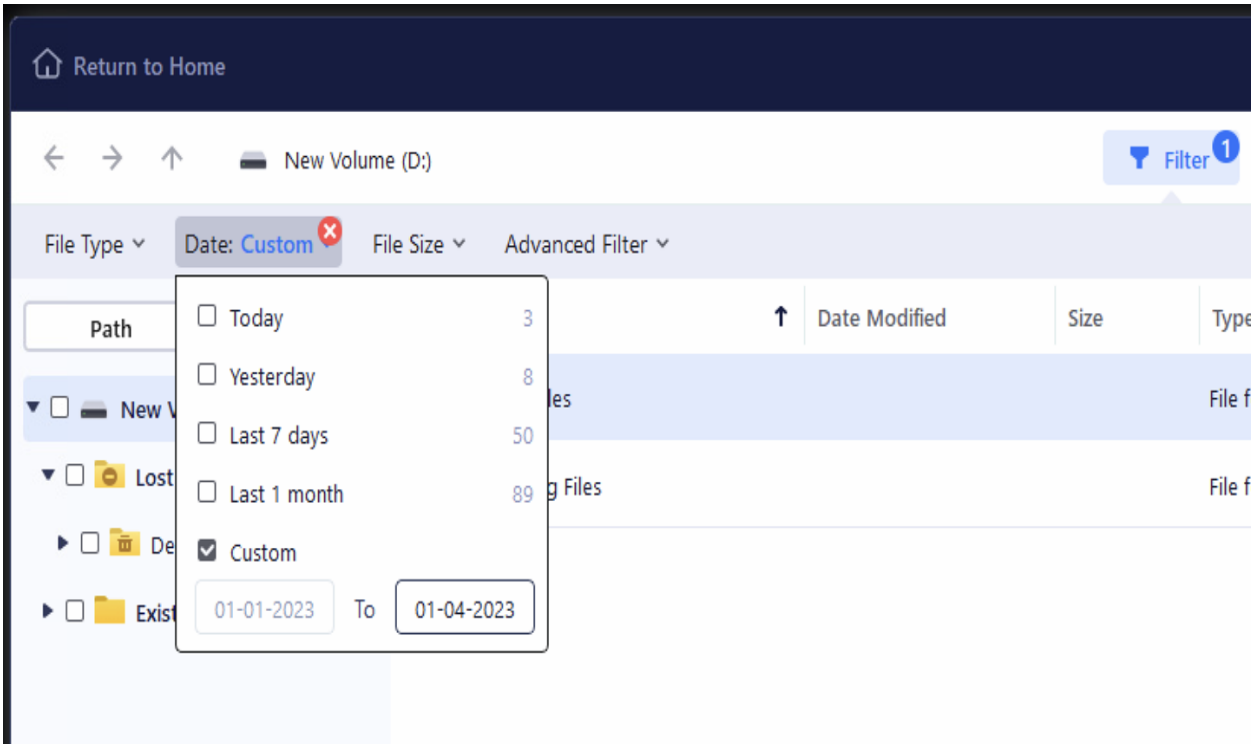

Fig. 4 Apply Filter

Once the scan is fully completed, we can go ahead and apply the necessary filters, like setting the Date to display files. As we have to recover multimedia files from last three months so we have set up the dates accordingly from 01-01-2023 to 01-04-2023.

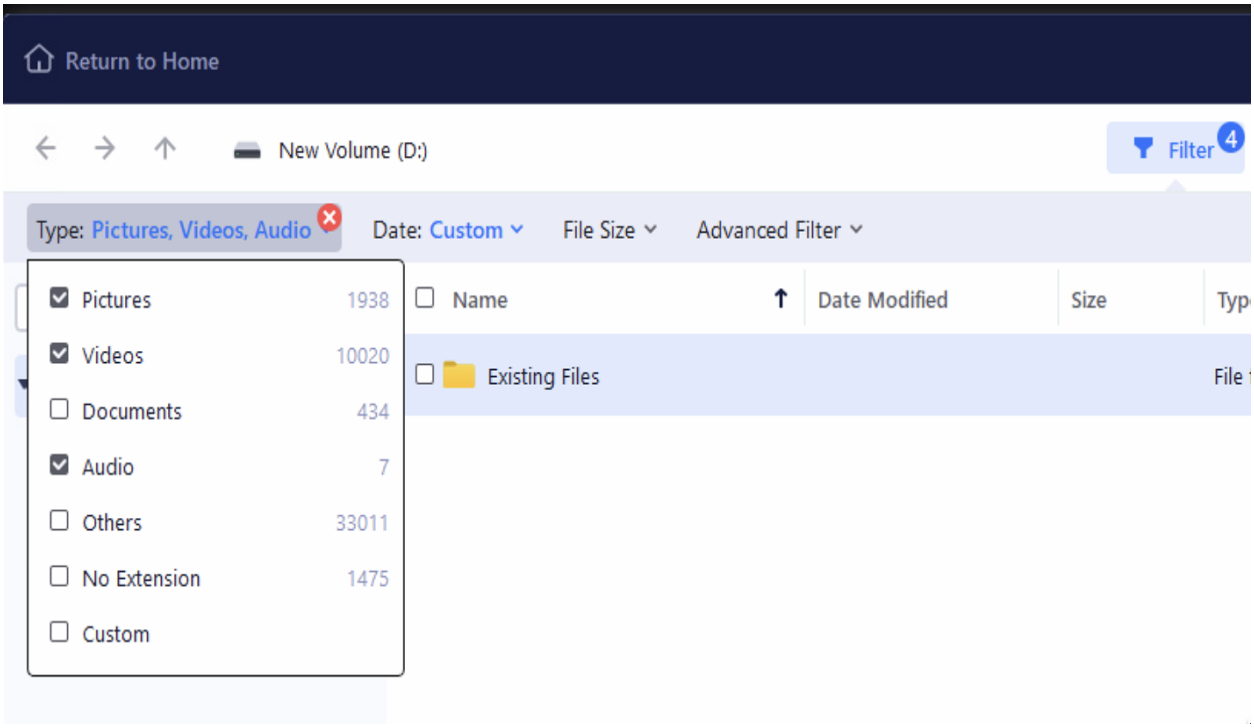

Fig.6 Select Multimedia files

As we have to recover partly damaged or erased multimedia files so we have go ahead with applying more filters. Here the file type is set to pictures, videos and audio.

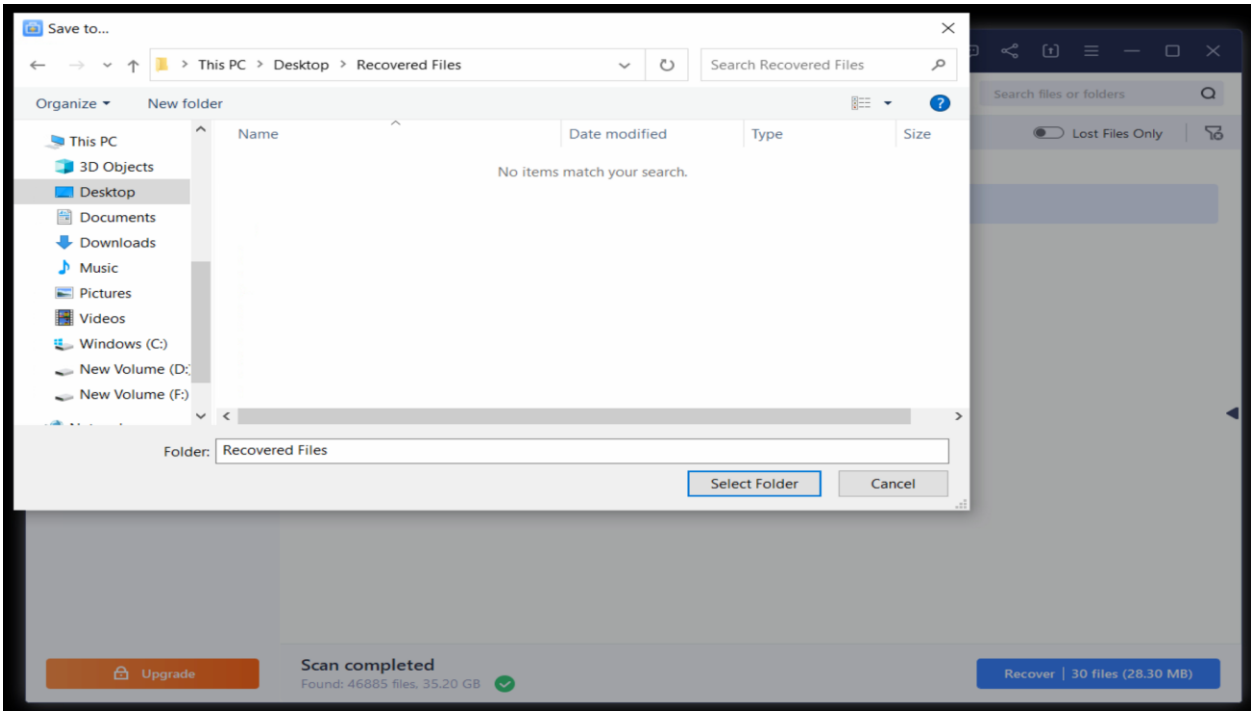

Fig. 7 Create folder for recovered files

We can set the path of recovered files according to our will. So here I have a created a folder named Recovered files on the desktop .

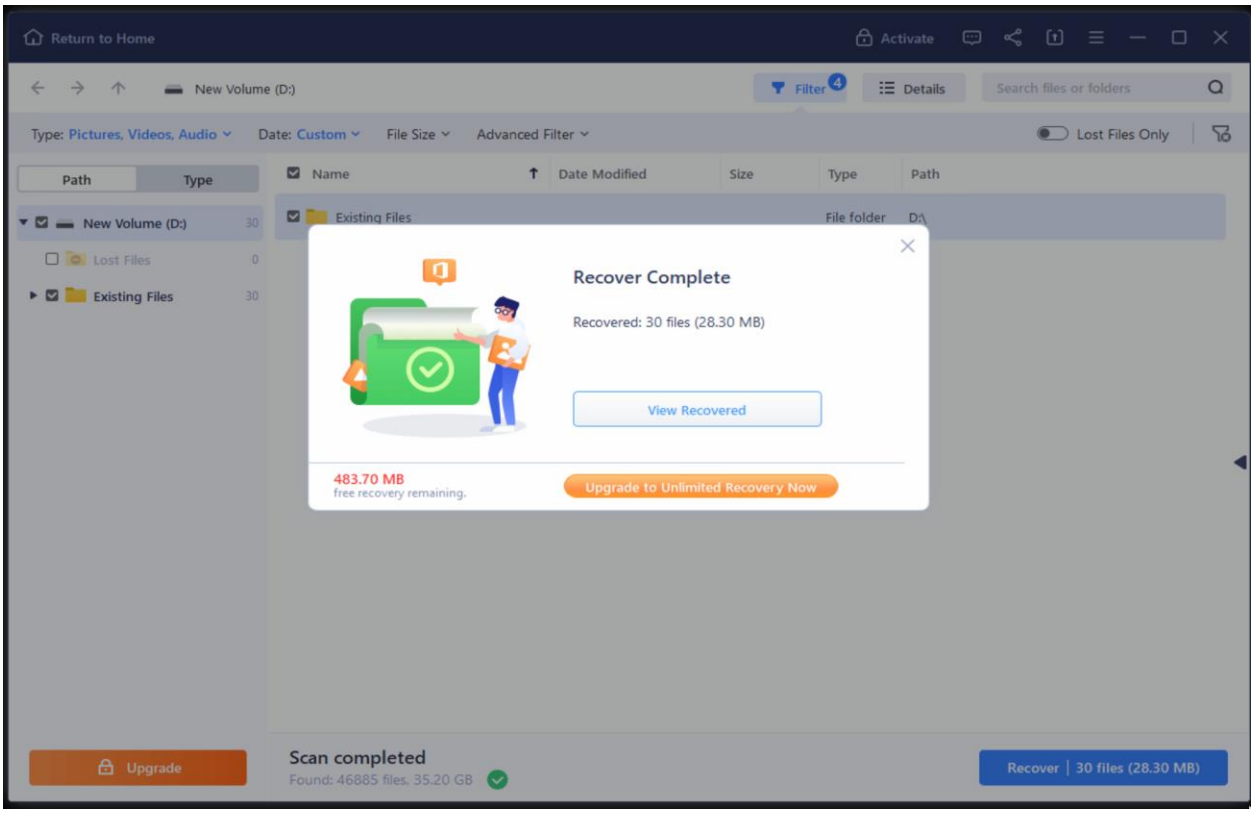

Fig. 8 Successful completion

The above image shows that we have successfully recovered partly erased or damaged multimedia files from last three months.

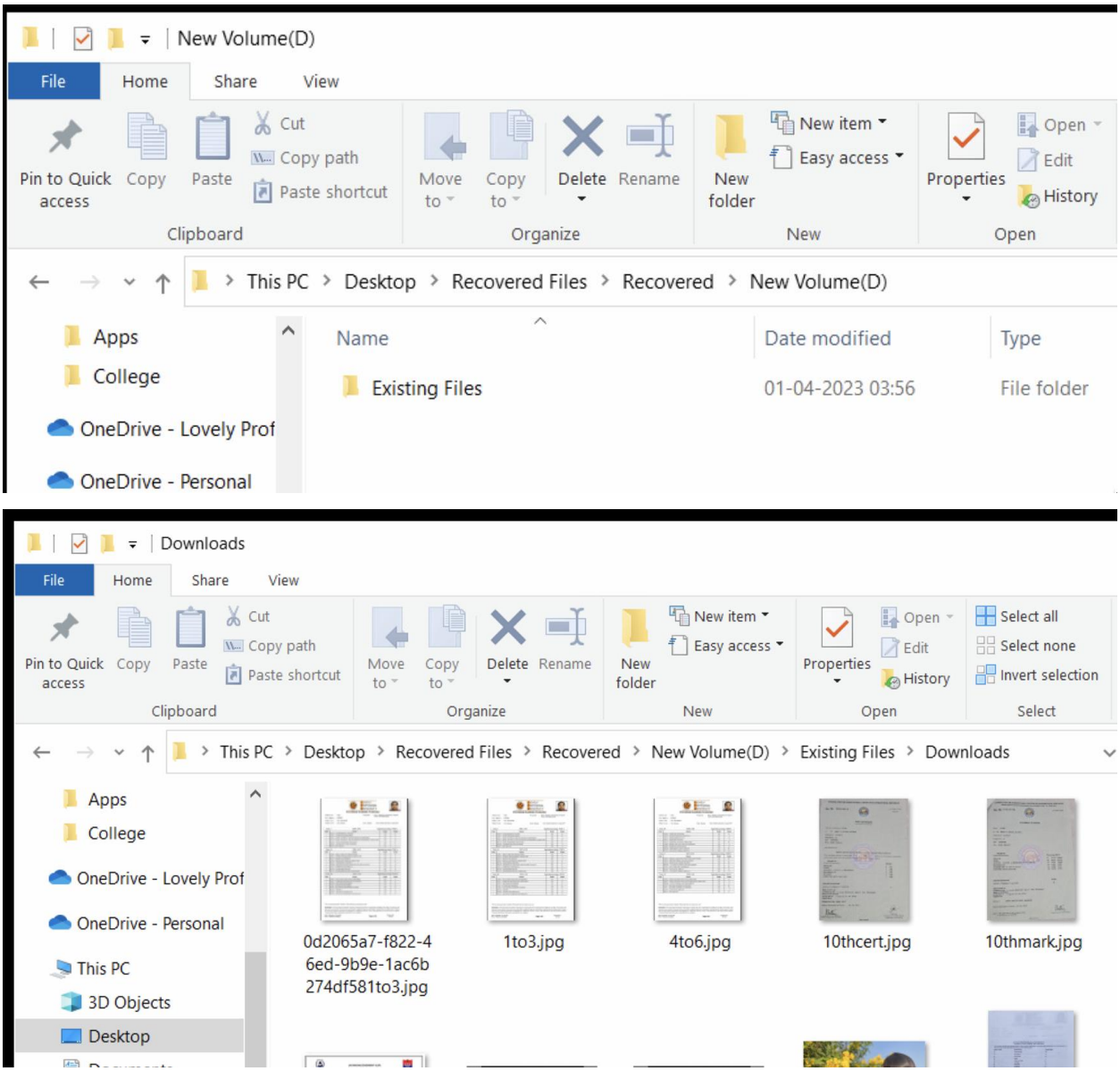

Fig. 9 Verify recovered files

Once the recovery process is completed, a new folder will be created with all the recovered files at the destination folder we chose earlier. And we can verify that all the partly/fully erased or damaged multimedia files in the last 3 months have been recovered.

Reference/ Bibliography

1] https://www.techtarget.com/searchsecurity/definition/computer-forensics

2] https://www.geeksforgeeks.org/introduction-of-computer-forensics/

3] https://medium.com/@cloud_tips/memory-forensics-tools-123e32387adb

4] https://www.easeus.com/partner/data-recovery/data-recovery-software-open-source.htm