MIT World Peace University

Digital Forensics and Investigation
Third Year B. Tech, Semester 5

To demonstrate Computer forencsic application programs for recovering deleted files and or deleted partitions.

Lab Assignment 3

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

September 24, 2023

Contents

1 Aim

Explore various computer forensic application programs for recovering deleted files and or deleted partitions and demonstrate any one such tool.

2 Objectives

1. Understand the concept of computer forensics and its importance in recovering deleted files and partitions.
2. Select one computer forensic application program and demonstrate its usage for recovering deleted files and/or partitions.
3. To understand the working of the tool.
4. To understand the importance of the tool.

3 Theory

3.1 Introduction to Digital Data Recovery

Digital data recovery is a critical process in the field of information technology. It involves the retrieval of lost, deleted, or corrupted data from digital storage devices. These devices can range from hard drives and solid-state drives (SSDs) to memory cards, USB drives, and even network-attached storage (NAS) systems. Data recovery plays a vital role in safeguarding valuable information and ensuring data integrity.

3.2 Need for Data Recovery Tools

3.2.1 Causes of Data Loss

Data loss can occur due to various reasons, including:

- Accidental Deletion: Users unintentionally delete important files or folders.
- Hardware Failure: Storage devices may experience physical or logical failures.
- Software Errors: Operating system crashes or software glitches can lead to data loss.
- Viruses and Malware: Malicious software can corrupt or delete files.

3.2.2 Minimizing Downtime

The need for data recovery tools is evident in their ability to minimize downtime in both personal and professional settings. Organizations rely on these tools to recover critical business data, while individuals use them to retrieve cherished photos, documents, and more.

3.3 Types of Data Recovery Tools

Data recovery tools can be categorized into two main types:

3.3.1 Software-Based Tools

Software-based data recovery tools are applications that run on a computer's operating system. They employ various algorithms and techniques to recover lost data. Some notable software-based tools include:

- **Recuva:** A user-friendly tool for recovering deleted files.
- **TestDisk:** A powerful open-source tool for partition recovery.
- **PhotoRec:** A tool specialized in recovering media files from various storage devices.

3.3.2 Hardware-Based Tools

Hardware-based data recovery tools are specialized devices used primarily for physical data recovery. These tools are employed when a storage device has suffered severe damage or has become inaccessible through normal software-based methods.

3.4 Historical Perspective

3.4.1 Early Data Recovery Tools

In the early days of computing, data recovery tools were rudimentary and could often recover only specific file types. These tools were limited in their capabilities and relied on basic file recovery methods.

3.4.2 Modern Data Recovery Tools

With advancements in technology, modern data recovery tools have evolved significantly. They now employ advanced techniques such as file carving, which allows them to recover a wide range of data formats by identifying file signatures and assembling fragmented files.

3.5 Common Data Recovery Processes

The data recovery process typically involves the following steps:

3.5.1 Scanning and Detection

Data recovery tools initiate a thorough scan of the storage device to identify lost or damaged files. During this phase, the tool identifies file headers and footers, as well as file signatures, to determine the file types present on the device.

3.5.2 File Reconstruction

In cases where files are fragmented or partially overwritten, data recovery tools attempt to reconstruct these files by piecing together available fragments. Advanced tools employ algorithms to determine file boundaries and recover the maximum amount of data.

3.5.3 Data Extraction

Once the lost data is identified and reconstructed, it is extracted from the damaged storage device. It is crucial to save the recovered data to a separate, secure location to prevent further data loss.

3.6 Challenges in Data Recovery

3.6.1 Fragmentation

One of the primary challenges in data recovery is dealing with fragmented data. Files can be scattered across a storage device, requiring sophisticated algorithms to reassemble them correctly.

3.6.2 Encryption

The prevalence of data encryption poses a significant challenge to data recovery efforts. Encrypted data requires decryption keys for successful recovery, and without these keys, recovery may be impossible.

3.6.3 Physical Damage

In cases of severe hardware failure, such as a malfunctioning read/write head on a hard drive, physical repairs may be necessary. However, physical repairs are complex and not always successful, making them a last resort in data recovery.

3.7 Forensic Perspective on Data Recovery

From a forensic standpoint, digital data recovery takes on a crucial role in investigations and legal proceedings. Forensic experts often find themselves needing to recover deleted files for various reasons:

3.7.1 Importance of Recovering Deleted Files in Forensic Investigations

- *Digital Evidence* Deleted files can contain critical digital evidence in criminal investigations. This evidence may include incriminating documents, communications, or digital footprints left by suspects.
- *Case Reconstruction* Recovering deleted files aids in reconstructing the sequence of events or actions that occurred on a digital device. This reconstruction can be pivotal in understanding the timeline and context of a crime.
- *Alibi Verification* Deleted files may also serve to corroborate or refute alibis provided by suspects or witnesses. Their recovery can help establish the credibility of statements made during an investigation.

3.7.2 Challenges in Forensic Data Recovery

Forensic experts encounter unique challenges in the process of recovering deleted files:

- *Anti-Forensic Measures* Perpetrators often employ anti-forensic techniques to hinder data recovery efforts, including secure file deletion, encryption, and data obfuscation.
- *Chain of Custody* Maintaining a proper chain of custody for recovered data is critical in forensic investigations to ensure its admissibility as evidence in court.
- *Data Tampering* Recovered data must be handled with care to prevent any unintentional tampering or alteration that could compromise its integrity in legal proceedings.

3.8 Legal and Ethical Considerations in Forensic Data Recovery

Forensic experts are bound by strict legal and ethical standards when recovering deleted files:

- *Search Warrants* The acquisition of digital evidence, including recovered deleted files, often requires proper search warrants and legal authorization.
- *Data Privacy* Respect for individuals' data privacy rights is paramount, and forensic experts must ensure that their actions are in compliance with relevant laws and regulations.
- *Expert Testimony* Forensic experts may be called upon to provide expert testimony in court regarding the methods used in data recovery and the authenticity of the recovered files.

4 Deleted File Recovery Procedure

Using testdisk to recover deleted files and partitions.

Files to be recovered

Partition Before Deletion

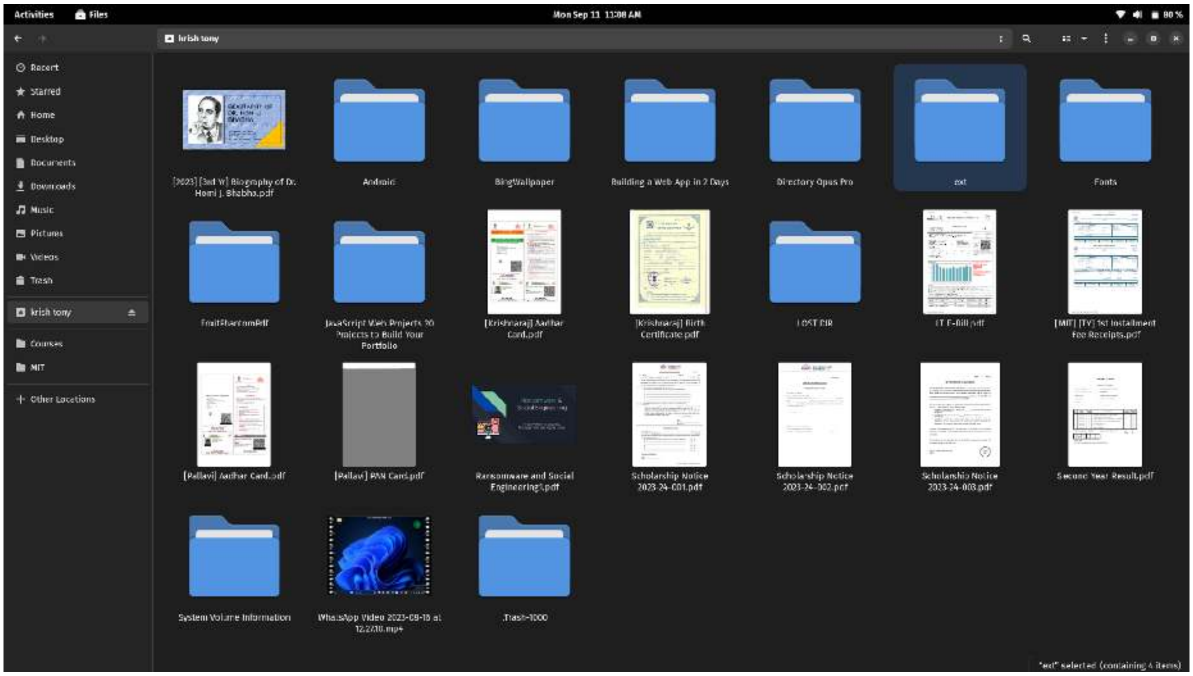
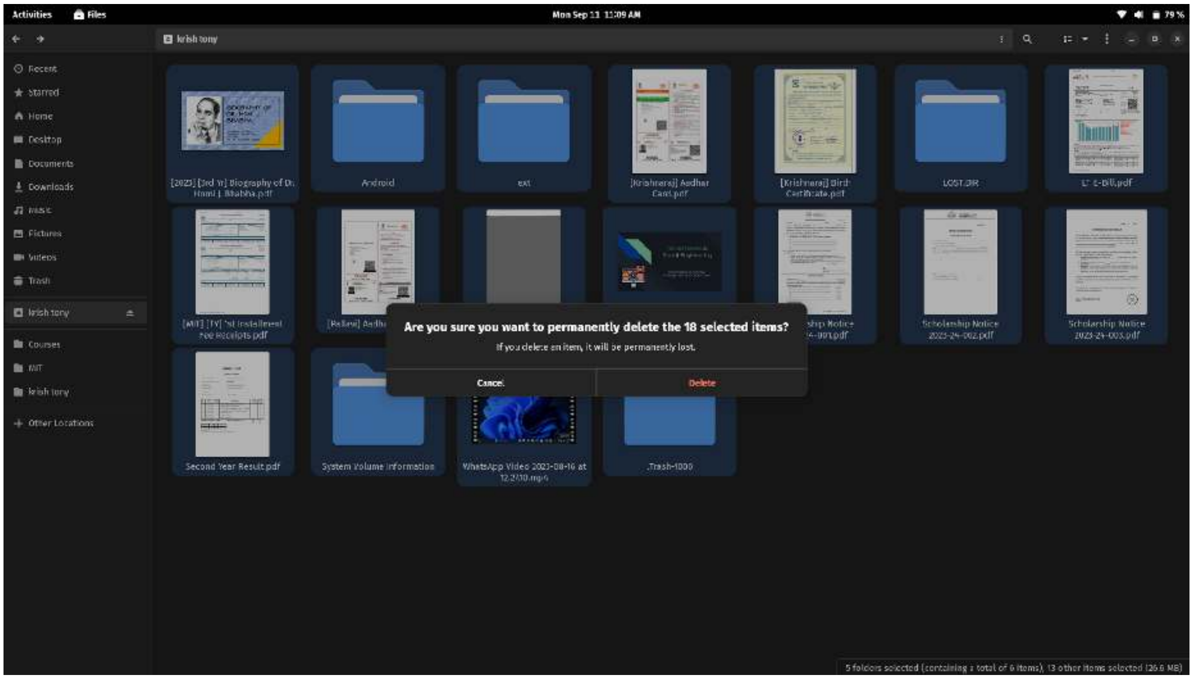

Activities
Files
Mon Sep 11 11:08 AM
80 %
krish tony
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
krish tony
Courses
MIT
Other Locations
[2023] [3rd Yr] Biography of Dr. Homi J. Bhabha.pdf
Android
BingWallpaper
Building a Web App in 2 Days
Directory Opus Pro
ext
Fonts
FruitPhantomPdf
JavaScript Web Projects 20 Projects to Build Your Portfolio
[Krishnaraj] Aadhar Card.pdf
[Krishnaraj] Birth Certificate.pdf
LOST DIR
IT E-Bill.pdf
[MIT] [TY] 1st Installment Fee Receipts.pdf
[Pallavi] Aadhar Card.pdf
[Pallavi] PAN Card.pdf
Ransomware and Social Engineering1.pdf
Scholarship Notice 2023-24-001.pdf
Scholarship Notice 2023-24-002.pdf
Scholarship Notice 2023-24-003.pdf
Second Year Result.pdf
System Volume Information
WhatsApp Video 2023-09-18 at 12.27.18.mp4
.Trash-1000
"ext" selected (containing 4 items)

Figure 1: Partition Before Deletion

Deleting Files


Activities
Files
Mon Sep 11 11:09 AM
79 %
krish tony
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
krish tony
Courses
MIT
krish tony
Other Locations
[2023] [3rd Yr] Biography of Dr. Homi J. Bhabha.pdf
Android
ext
[Krishnaraj] Aadhar Card.pdf
[Krishnaraj] Birth Certificate.pdf
LOST.DIR
E-Bill.pdf
[MIT] [TY] 1st Installment Fee Receipts.pdf
[Balaji] Aadha
ship Notice -001.pdf
Scholarship Notice 2023-24-002.pdf
Scholarship Notice 2023-24-003.pdf
Second Year Result.pdf
System Volume Information
WhatsApp Video 2023-08-16 at 12.27.10.mp4
.Trash-1000
Cancel
Delete

Are you sure you want to permanently delete the 18 selected items?

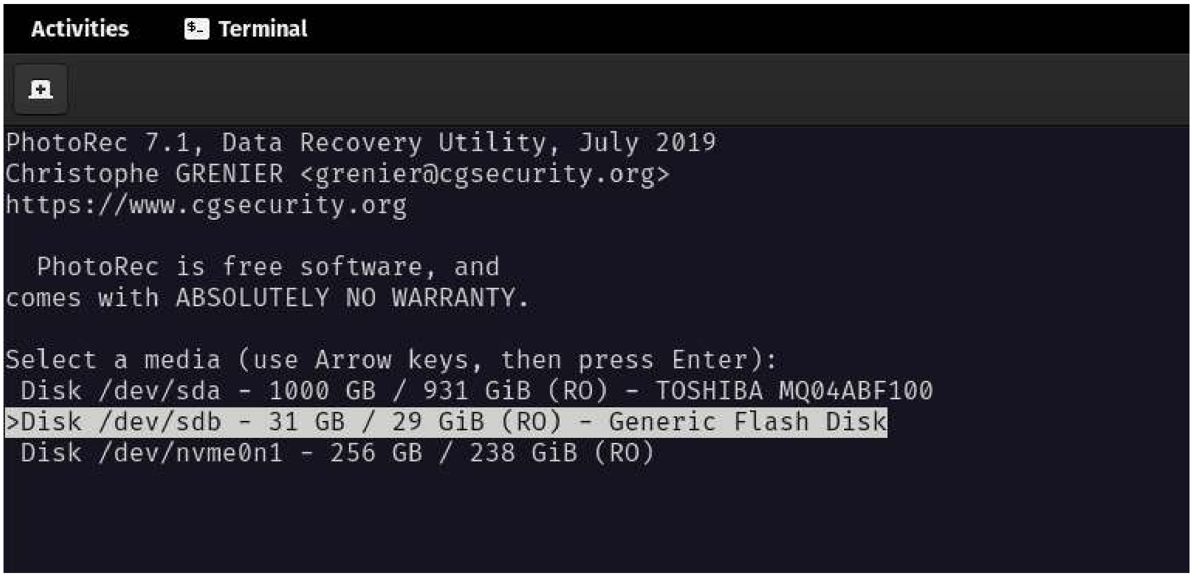
If you delete an item, it will be permanently lost.

5 folders selected (containing a total of 6 items), 13 other items selected (26.6 MB)

Figure 2: Deleting Files

Steps

Selecting the disk



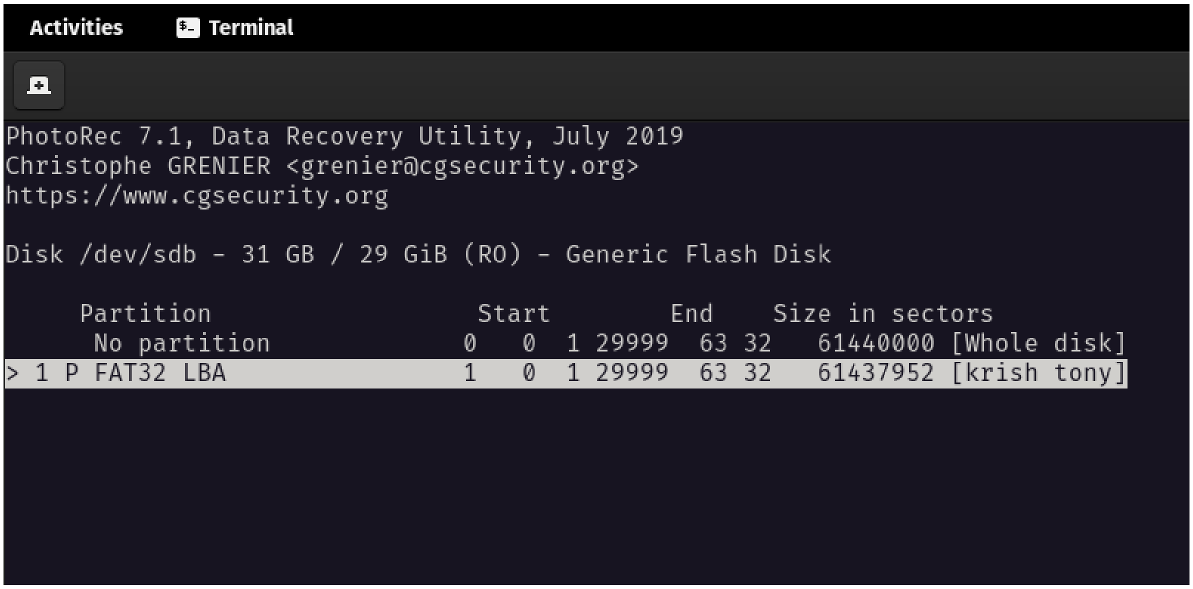
```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

  PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
 Disk /dev/sda - 1000 GB / 931 GiB (RO) - TOSHIBA MQ04ABF100
>Disk /dev/sdb - 31 GB / 29 GiB (RO) - Generic Flash Disk
 Disk /dev/nvme0n1 - 256 GB / 238 GiB (RO)
```

Figure 3: Selecting the disk

Selecting the partition table type



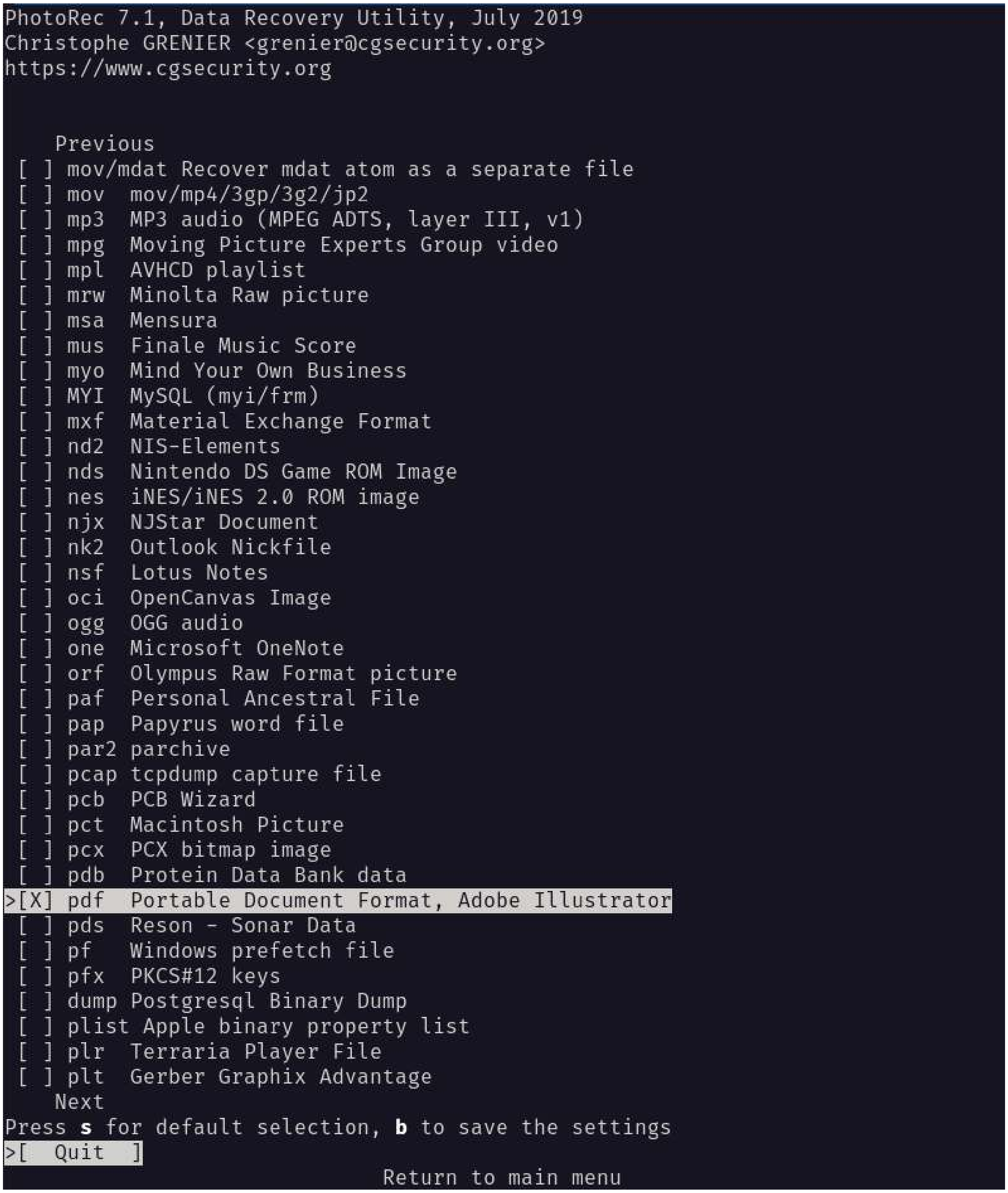
```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 31 GB / 29 GiB (RO) - Generic Flash Disk

     Partition                  Start        End    Size in sectors
      No partition             0   0  1 29999  63 32   61440000 [Whole disk]
> 1 P FAT32 LBA                1   0  1 29999  63 32   61437952 [krish tony]
```

Figure 4: Selecting the partition table type

Selecting the type of files needs to be recover

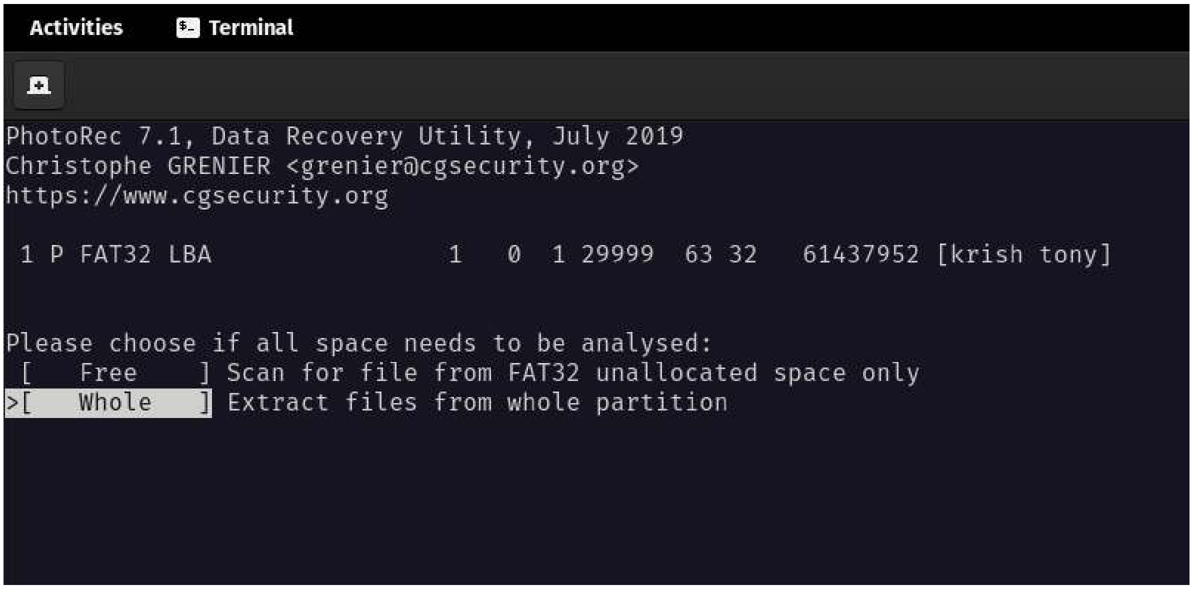


```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


    Previous
 [ ] mov/mdat Recover mdat atom as a separate file
 [ ] mov  mov/mp4/3gp/3g2/jp2
 [ ] mp3  MP3 audio (MPEG ADTS, layer III, v1)
 [ ] mpg  Moving Picture Experts Group video
 [ ] mpl  AVHCD playlist
 [ ] mrw  Minolta Raw picture
 [ ] msa  Mensura
 [ ] mus  Finale Music Score
 [ ] myo  Mind Your Own Business
 [ ] MYI  MySQL (myi/frm)
 [ ] mxf  Material Exchange Format
 [ ] nd2  NIS-Elements
 [ ] nds  Nintendo DS Game ROM Image
 [ ] nes  iNES/iNES 2.0 ROM image
 [ ] njx  NJStar Document
 [ ] nk2  Outlook Nickfile
 [ ] nsf  Lotus Notes
 [ ] oci  OpenCanvas Image
 [ ] ogg  OGG audio
 [ ] one  Microsoft OneNote
 [ ] orf  Olympus Raw Format picture
 [ ] paf  Personal Ancestral File
 [ ] pap  Papyrus word file
 [ ] par2 parchive
 [ ] pcap tcpdump capture file
 [ ] pcb  PCB Wizard
 [ ] pct  Macintosh Picture
 [ ] pcx  PCX bitmap image
 [ ] pdb  Protein Data Bank data
>[X] pdf  Portable Document Format, Adobe Illustrator
 [ ] pds  Reson - Sonar Data
 [ ] pf   Windows prefetch file
 [ ] pfx  PKCS#12 keys
 [ ] dump Postgresql Binary Dump
 [ ] plist Apple binary property list
 [ ] plr  Terraria Player File
 [ ] plt  Gerber Graphix Advantage
    Next
Press s for default selection, b to save the settings
>[  Quit  ]
                              Return to main menu
```

Figure 5: Selecting the type of files needs to be recover

Select if All space needs to be searched or just the free space



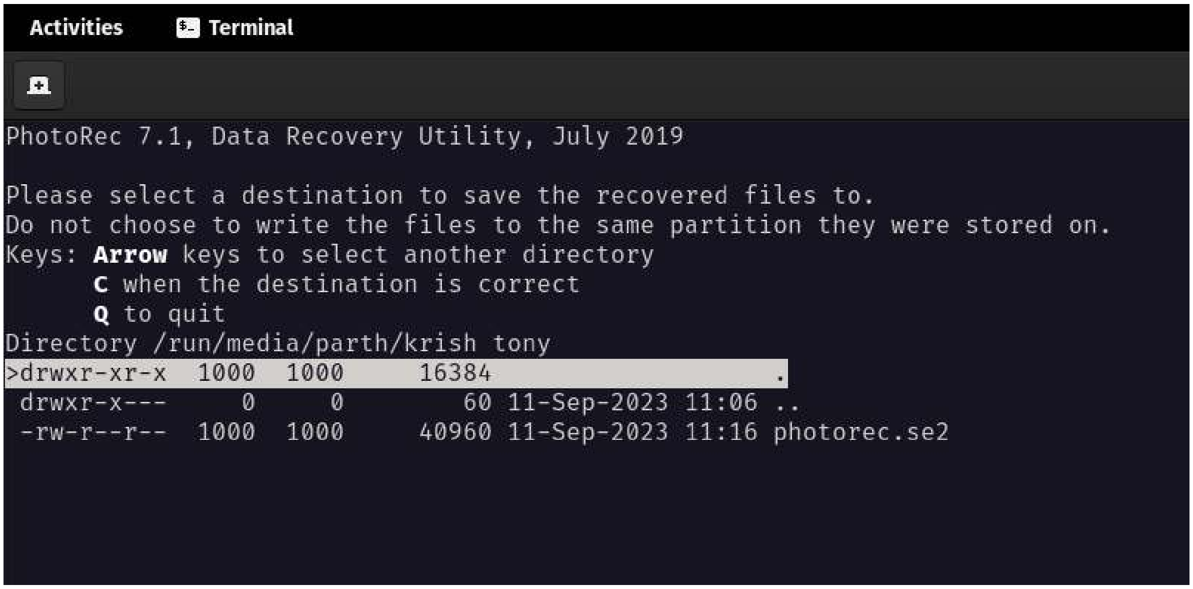
```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

 1 P FAT32 LBA              1   0  1 29999  63 32   61437952 [krish tony]


Please choose if all space needs to be analysed:
 [   Free    ] Scan for file from FAT32 unallocated space only
>[   Whole   ] Extract files from whole partition
```

Figure 6: Select if All space needs to be searched or just the free space

Selecting the Location to store the recovered files

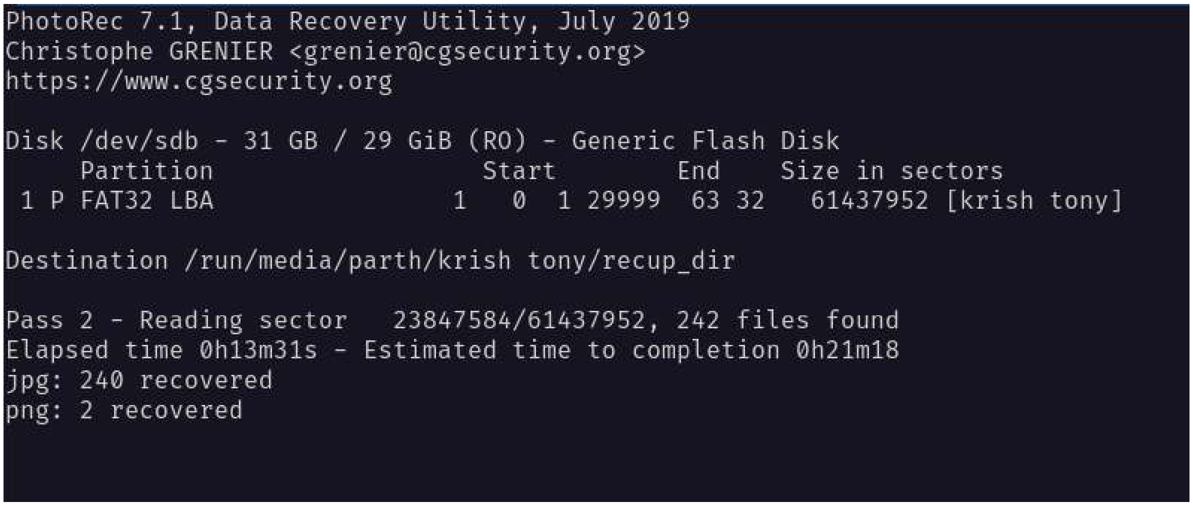


```
PhotoRec 7.1, Data Recovery Utility, July 2019

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /run/media/parth/krish tony
>drwxr-xr-x  1000  1000     16384                     .
 drwxr-x---     0     0        60 11-Sep-2023 11:06 ..
 -rw-r--r--  1000  1000     40960 11-Sep-2023 11:16 photorec.se2
```

Figure 7: Selecting the Location to store the recovered files

Recovering the files



```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 31 GB / 29 GiB (RO) - Generic Flash Disk
     Partition                  Start        End    Size in sectors
 1 P FAT32 LBA                1   0  1 29999  63 32   61437952 [krish tony]

Destination /run/media/parth/krish tony/recup_dir

Pass 2 - Reading sector   23847584/61437952, 242 files found
Elapsed time 0h13m31s - Estimated time to completion 0h21m18
jpg: 240 recovered
png: 2 recovered
```

Figure 8: Recovering the files

Recovered Files are Stored In the Recup_dir.1

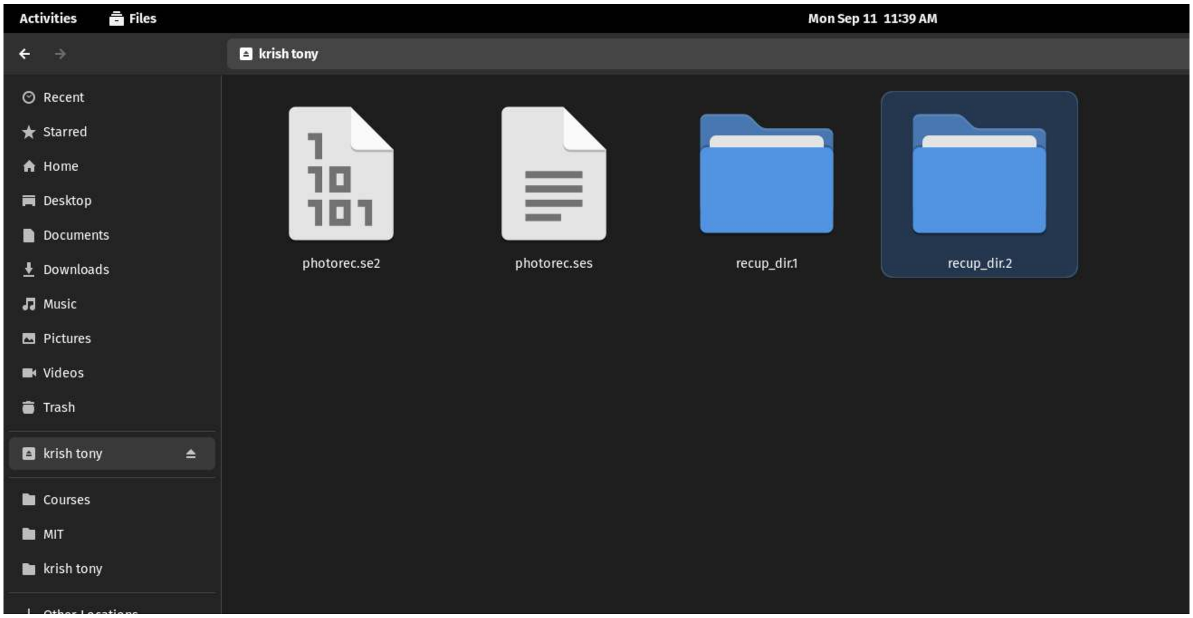


Figure 9: Recovered Files are Stored In the Recup_dir.1

Recovered Files

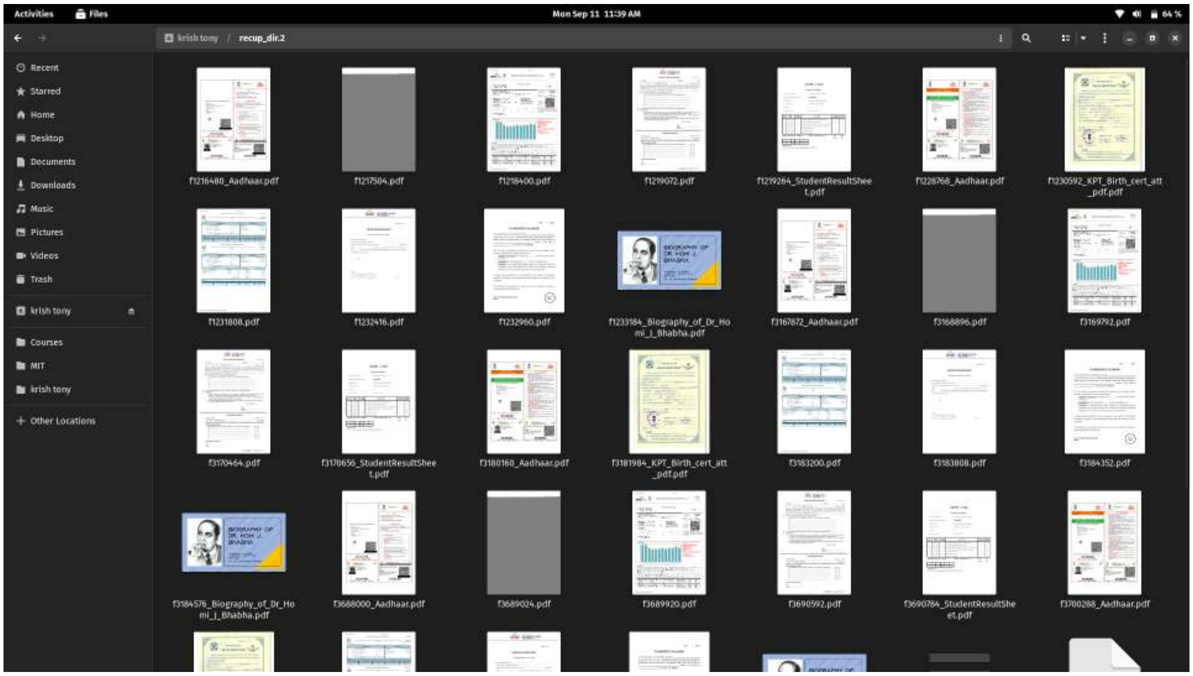


Figure 10: Recovered Files

5 Platform

Operating System: Arch Linux x86-64
IDEs or Text Editors Used: Visual Studio Code
Compilers or Interpreters: None.

6 Conclusion

In forensic investigations, the recovery of deleted files is not only valuable but often essential for uncovering the truth and building a strong case.

Forensic experts face distinct challenges in this process, including countering anti-forensic measures, maintaining chain of custody, and upholding legal and ethical standards. Nevertheless, their expertise in digital data recovery is pivotal in delivering justice and ensuring the integrity of the legal system.

We have successfully explored and Studied various computer forensic application programs for recovering deleted files and or deleted partitions and demonstrated any one such tool.

References

[1] Open Source Data Recovery Software List
Software Suggest

[2] TestDisk Page
Test Disk Data Recovery Software

[3] TestDisk Docs
Documentation for Test Disk Data Recovery Software