School of Computer Engineering and Technology
Academic Year: 2023-2024 Sem V

Digital Forensics and Investigation

Lab Assignment : 03

Title: Recovering Permanently Deleted Files From Windows/Kali Linux

Prepared By
Saurabh Jitendra Jadhav
Roll No:-PA12
Batch A1

August 27,2023

1. Aim:

To study and understand the tools used for Recovering Permanently Deleted files From Windows/Kali Linux.

2. Objective:

1. To Understand Data Recovery Tools.
2. To Analyze File Recovery Processes.

3. Introduction:

In the world of digital investigation, recovering permanently deleted files is a crucial task. When we normally delete files, like using the "Delete" key, they go to a special folder (Recycle Bin or Trash) and can be brought back easily. But sometimes, files are deleted in a way that skips this step, and they seem gone forever. This practical aims to recover these hard-to-find files from both Windows and Kali Linux systems.

4. Theory:

A)File Deletion in File Systems:

When a file is deleted from a storage device, the operating system marks the space occupied by the file as available for reuse, but the actual file content remains intact until it is overwritten by new data. This provides an opportunity for recovery.

B)Windows File Recovery:

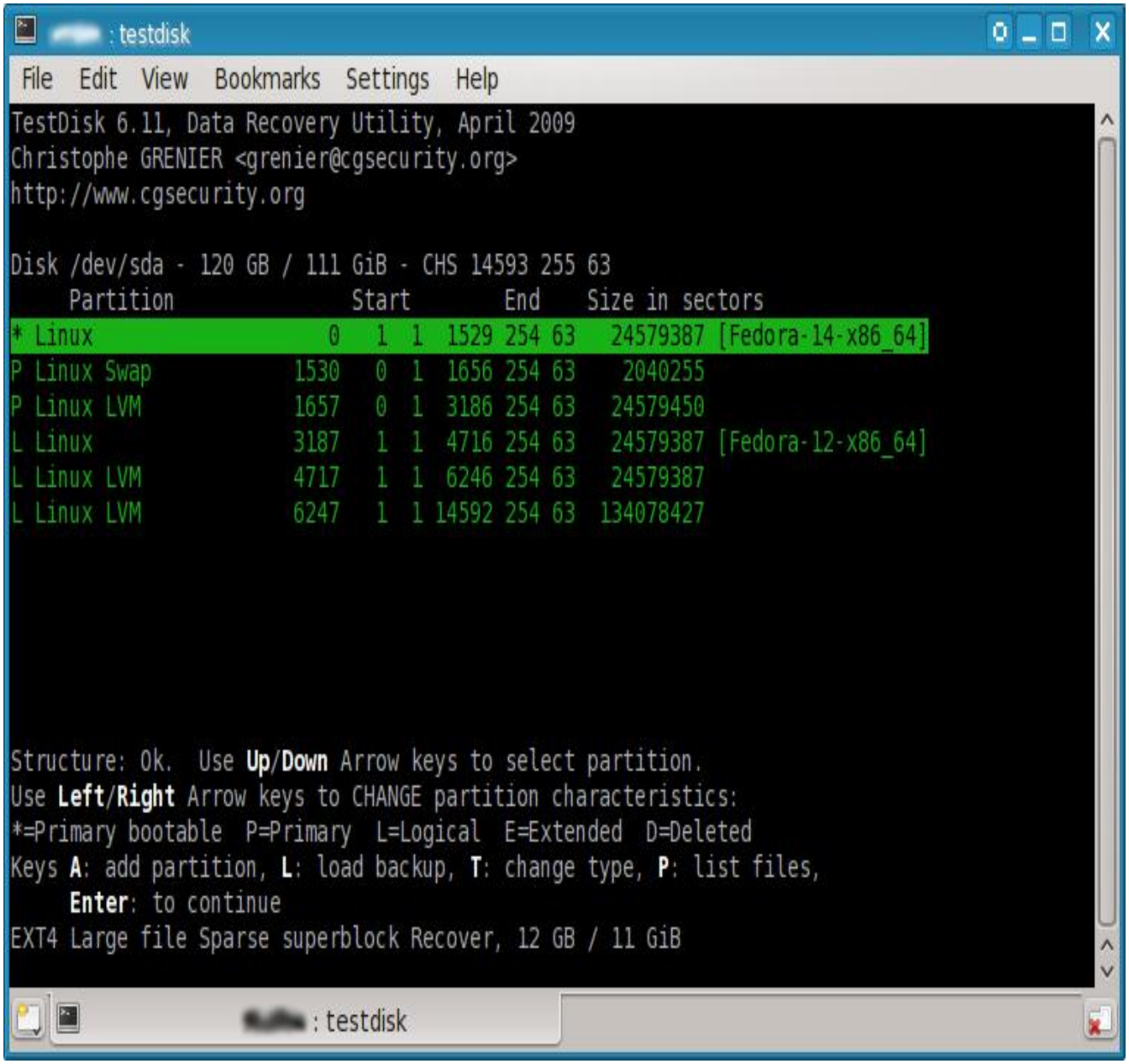
In the Windows environment, the File Allocation Table (FAT) or Master File Table (MFT) keeps track of file locations. Data recovery tools scan these tables to identify and recover deleted files. Tools like Recuva or TestDisk perform file signature-based searches to locate file headers and footers, enabling recovery even without intact file system structures.

C) Kali Linux File Recovery:

Kali Linux, as a forensic and penetration testing platform, offers tools like PhotoRec and Scalpel. **PhotoRec** uses file signature analysis to recover a wide range of file types, even if file system structures are damaged or missing. **Scalpe**l focuses on carving out specific file types based on predefined headers and footers.

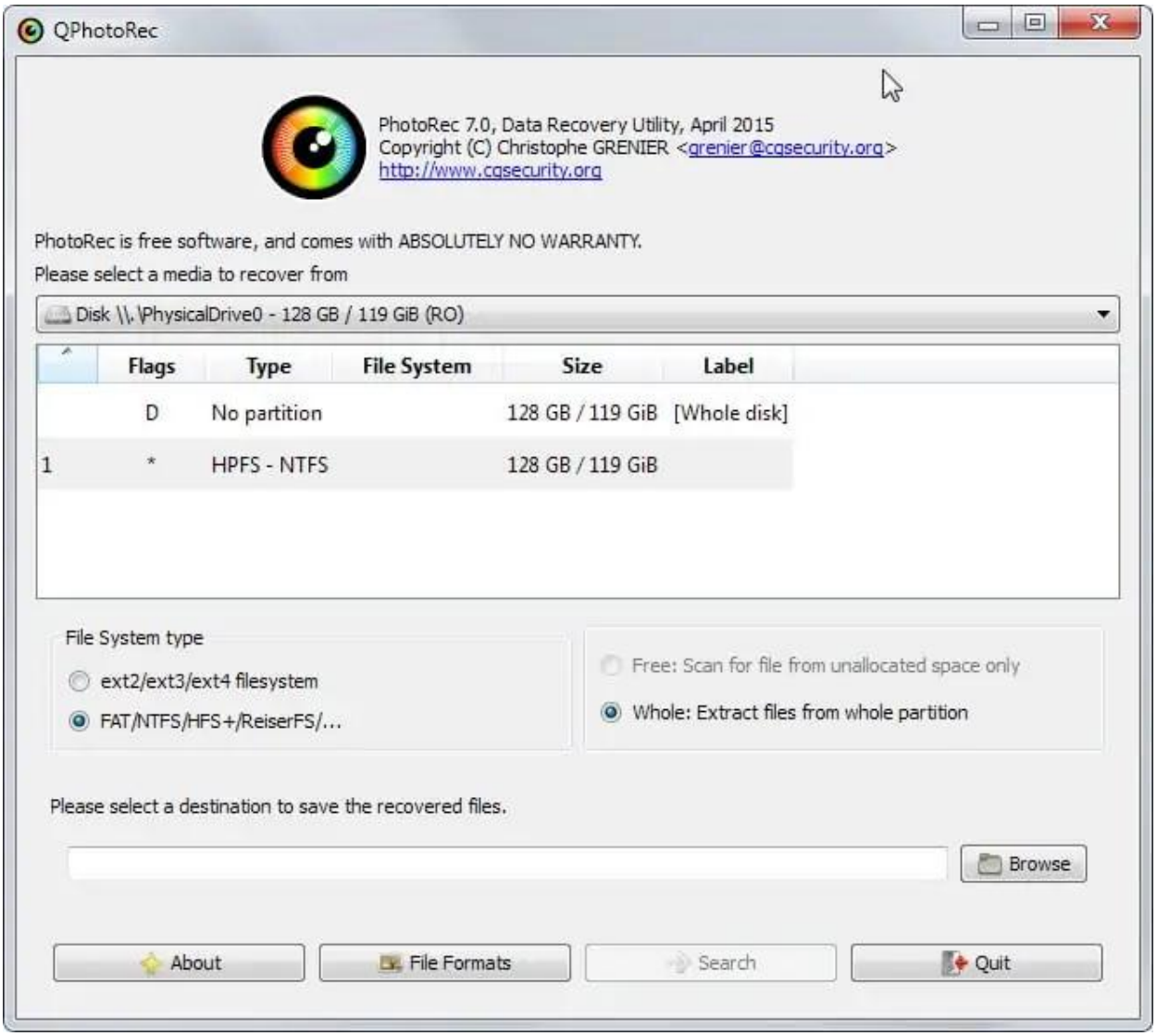
Tools Used For Date Recovering Files

1 TestDisk: A powerful tool for recovering lost partitions and making non-booting disks bootable again. It can also help in recovering deleted files from various file systems.



TestDisk Interlace

2 PhotoRec: Developed by the same team as TestDisk, PhotoRec is designed specifically for file recovery. It works on a wide range of file types and can recover data even from damaged or formatted partitions.



Photorec Interface

3 Autopsy: An open-source digital forensics platform that includes several tools for disk imaging, file recovery, and analysis. Autopsy offers a user-friendly interface and integrates with The Sleuth Kit for advanced analysis.

Autopsy Interface

4 Scalpel: A file carving tool that allows for precise extraction of specific file types from disk images. It's useful for recovering files based on predefined headers and footers.

Installation Step:

$ sudo apt-get install scalpel

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  scalpel
0 upgraded, 1 newly installed, 0 to remove and 390 not upgraded.
Need to get 0 B/33.9 kB of archives.
After this operation, 118 kB of additional disk space will be used.
Selecting previously unselected package scalpel.
(Reading database ... 151082 files and directories currently installed.)
Unpacking scalpel (from .../scalpel_1.60-1build1_i386.deb) ...
Processing triggers for man-db ...
Setting up scalpel (1.60-1build1) ...
tecmint@tecmint-Latitude-D630:~$
```

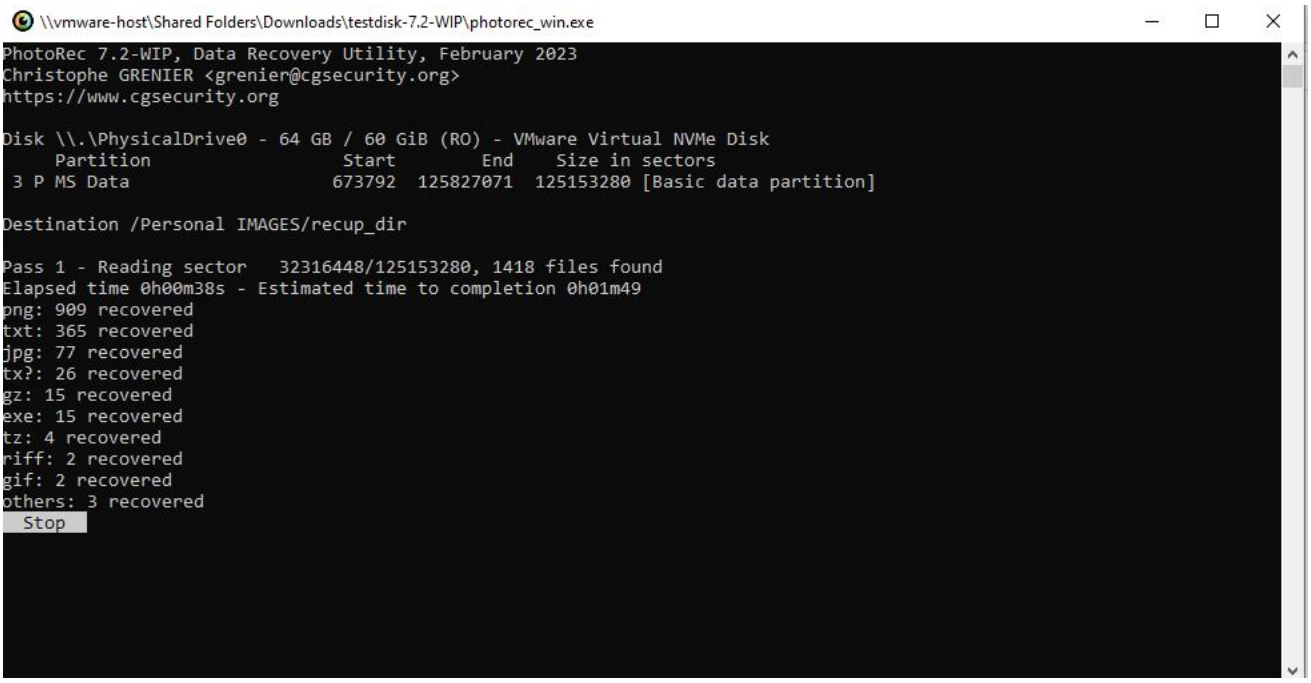
Installation Steps

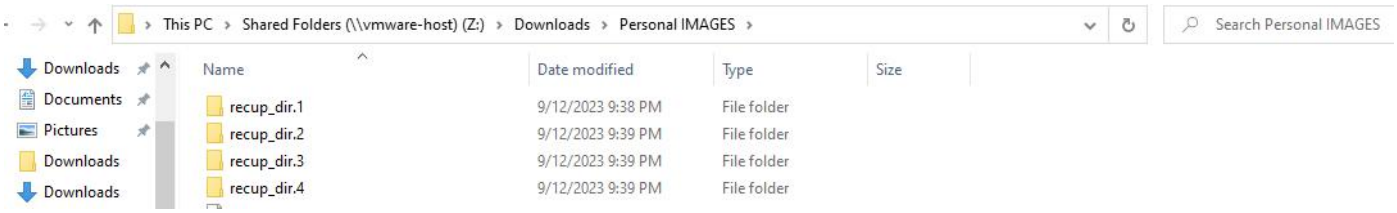
```
/etc/scalpel/scalpel.conf - Mousepad
File  Edit  Search  View  Document  Help
Warning, you are using the root account, you may harm your system.
#       art     y       150000  \x4a\x47\x04\x0e        \xcf\xc7\xcb
#       art     y       150000  \x4a\x47\x03\x0e        \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
        gif     y       5000000         \x47\x49\x46\x38\x37\x61        \x00\x3b
        gif     y       5000000         \x47\x49\x46\x38\x39\x61        \x00\x3b
        jpg     y       5242880         \xff\xd8\xff???Exif             \xff\xd9        REVERSE
        jpg     y       5242880         \xff\xd8\xff???JFIF             \xff\xd9        REVERSE

#
# PNG
#       png     y       20000000        \x50\x4e\x47?   \xff\xfc\xfd\xfe
#
#
# BMP   (used by MSWindows, use only if you have reason to think there are
#       BMP files worth digging for. This often kicks back a lot of false
#       positives
#
#       bmp     y       100000  BM??\x00\x00\x00
#
# TIFF
```

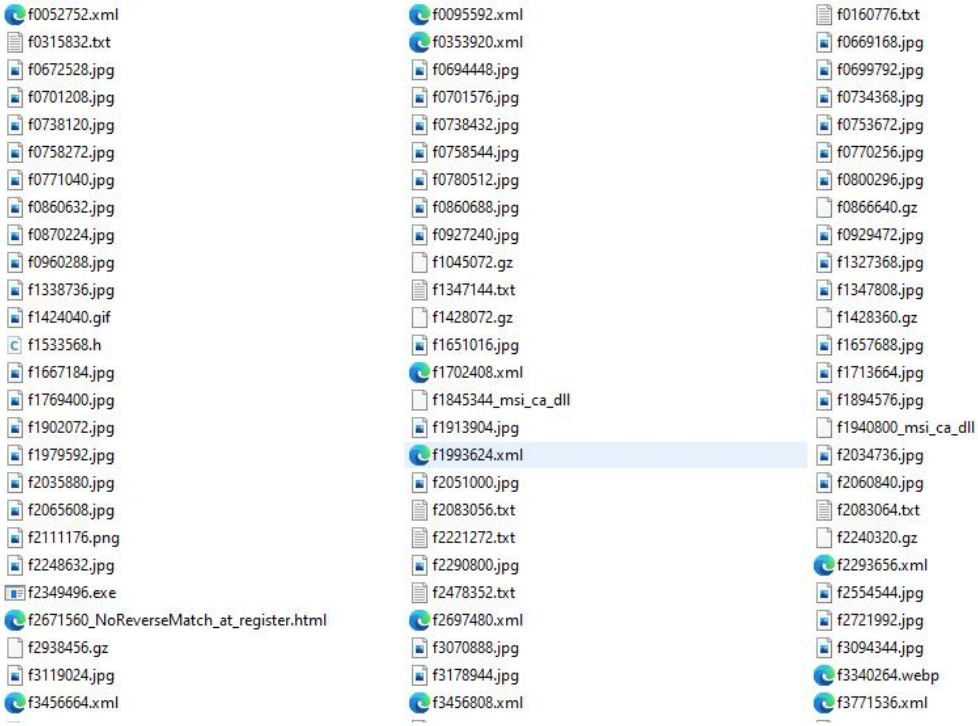
Scalpel Interface:- .conf file editing to mentioned which file type you want to recover

Implementation: Photorec Tool





Recoverd files were Saved in recup_dir



Conclusion:

Thus, we have studied and understood the tools used for Digital Forensics and Investigation for Recovering permanently deleted files from Windows and kali linux.We have also found out the tools used for Data Recovery and studied some of the tools used for it.