



Dr. Vishwanath Karad

**MIT WORLD PEACE
UNIVERSITY** | PUNE

TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

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:

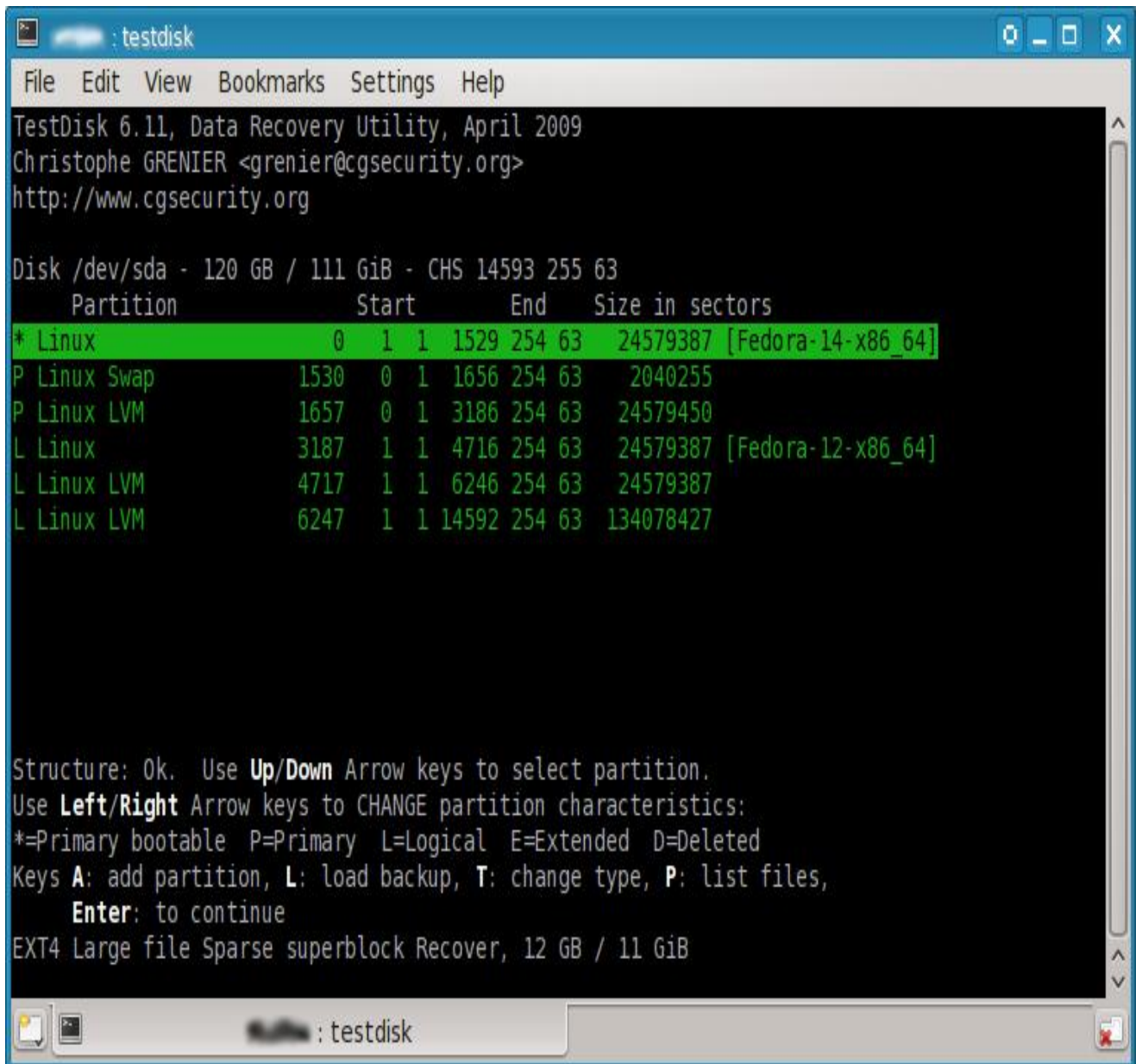
In the Windows environment, the File Allocation Table (FAT) or Master File Table (MFT) keeps track of file locations. Data recovery tools scan these tables to identify and recover deleted files. Tools like Recuva or TestDisk perform file signature-based searches to locate file headers and footers, enabling 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. **Scalpel** focuses on carving out specific file types based on predefined headers and footers.

Tools Used For Data 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.



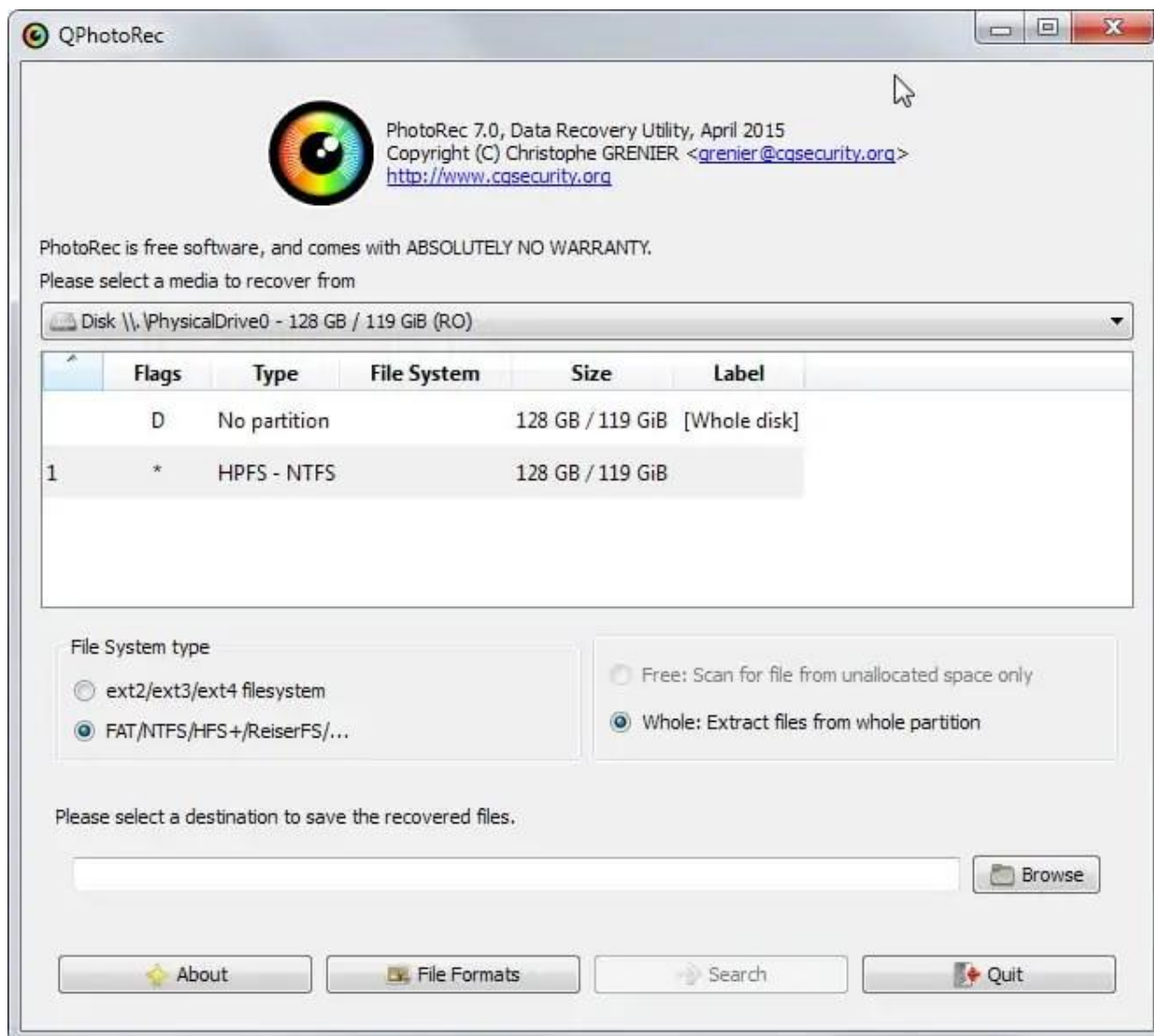
```
testdisk
File Edit View Bookmarks Settings Help
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 120 GB / 111 GiB - CHS 14593 255 63
Partition      Start      End  Size in sectors
* Linux         0  1  1  1529 254 63  24579387 [Fedora-14-x86_64]
P Linux Swap    1530  0  1  1656 254 63  2040255
P Linux LVM     1657  0  1  3186 254 63  24579450
L Linux        3187  1  1  4716 254 63  24579387 [Fedora-12-x86_64]
L Linux LVM     4717  1  1  6246 254 63  24579387
L Linux LVM     6247  1  1 14592 254 63 134078427

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
      Enter: to continue
EXT4 Large file Sparse superblock Recover, 12 GB / 11 GiB
```

TestDisk Interface

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

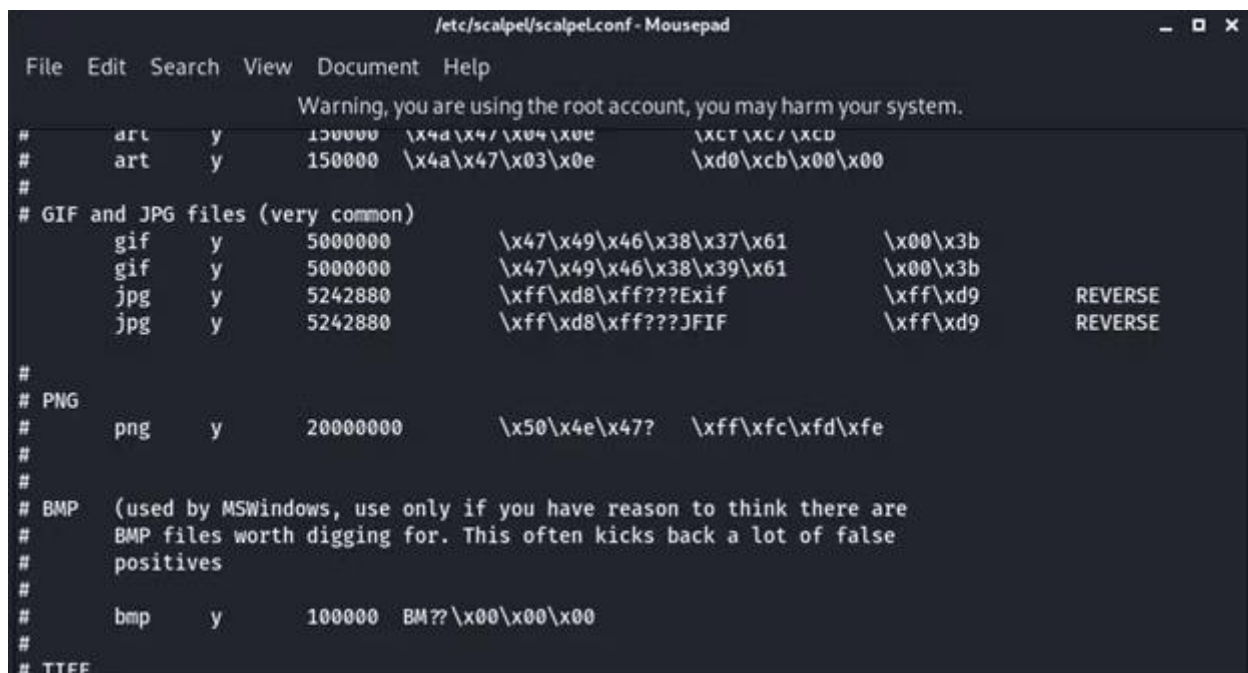
4 Scalpel: A file carving tool that allows for precise extraction of specific file types from disk images. It's useful for recovering files based on predefined headers and footers.

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      1500000  \x4d\x47\x03\x0e  \xct\xcc\xcd
#      art      y      1500000  \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
#
# TTF

```

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

Implementation: Photorec Tool

```

\\vmware-host\Shared Folders\Downloads\testdisk-7.2-WIP\photorec_win.exe
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 64 GB / 60 GiB (R0) - VMware Virtual NVMe Disk
Partition      Start      End      Size in sectors
3 P MS Data    673792    125827071 125153280 [Basic data partition]

Destination /Personal IMAGES/recup_dir

Pass 1 - Reading sector 32316448/125153280, 1418 files found
Elapsed time 0h00m38s - Estimated time to completion 0h01m49
png: 909 recovered
txt: 365 recovered
jpg: 77 recovered
tx?: 26 recovered
gz: 15 recovered
exe: 15 recovered
tz: 4 recovered
riff: 2 recovered
gif: 2 recovered
others: 3 recovered
Stop

```

File Explorer view showing the directory structure:

This PC > Shared Folders (\\vmware-host) (Z:) > Downloads > Personal IMAGES

Name	Date modified	Type	Size
recup_dir.1	9/12/2023 9:38 PM	File folder	
recup_dir.2	9/12/2023 9:39 PM	File folder	
recup_dir.3	9/12/2023 9:39 PM	File folder	
recup_dir.4	9/12/2023 9:39 PM	File folder	

Recoverd files were Saved in recup_dir

f0052752.xml	f0095592.xml	f0160776.txt
f0315832.txt	f0353920.xml	f0669168.jpg
f0672528.jpg	f0694448.jpg	f0699792.jpg
f0701208.jpg	f0701576.jpg	f0734368.jpg
f0738120.jpg	f0738432.jpg	f0753672.jpg
f0758272.jpg	f0758544.jpg	f0770256.jpg
f0771040.jpg	f0780512.jpg	f0800296.jpg
f0860632.jpg	f0860688.jpg	f0866640.gz
f0870224.jpg	f0927240.jpg	f0929472.jpg
f0960288.jpg	f1045072.gz	f1327368.jpg
f1338736.jpg	f1347144.txt	f1347808.jpg
f1424040.gif	f1428072.gz	f1428360.gz
f1533568.h	f1651016.jpg	f1657688.jpg
f1667184.jpg	f1702408.xml	f1713664.jpg
f1769400.jpg	f1845344_msi_ca_dll	f1894576.jpg
f1902072.jpg	f1913904.jpg	f1940800_msi_ca_dll
f1979592.jpg	f1993624.xml	f2034736.jpg
f2035880.jpg	f2051000.jpg	f2060840.jpg
f2065608.jpg	f2083056.txt	f2083064.txt
f2111176.png	f2221272.txt	f2240320.gz
f2248632.jpg	f2290800.jpg	f2293656.xml
f2349496.exe	f2478352.txt	f2554544.jpg
f2671560_NoReverseMatch_at_register.html	f2697480.xml	f2721992.jpg
f2938456.gz	f3070888.jpg	f3094344.jpg
f3119024.jpg	f3178944.jpg	f3340264.webp
f3456664.xml	f3456808.xml	f3771536.xml

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.