Forensic File Recovery and Imaging Using Scalpel on Kali Linux

This project demonstrates the process of using **Scalpel**, a file carving tool, to recover a deleted file from a disk and create a forensic image of the recovered data. We focus on recovering a specific file (`Readme.md`) that was deleted and documenting the steps for forensically sound data recovery.

Project Overview

The goal of this project is to:

1. Recover a deleted file (`Readme.md`) using **Scalpel**.
2. Create a forensic disk image containing the recovered files.
3. Generate a hash of the forensic image to ensure data integrity.

This document explains the step-by-step process, tools used, and reasoning behind each step in the recovery process.

Tools Used

- **Kali Linux**: A Linux distribution designed for digital forensics and penetration testing.
- **Scalpel**: A file carving tool that recovers deleted files based on file headers and footers.
- **dd**: A utility to create a forensic disk image.
- **md5sum/sha256sum**: Tools to generate a hash of the forensic image to verify its integrity.

Process Breakdown

1. Setup the Environment

Step: Install Scalpel

To begin, we need to ensure that **Scalpel** is installed on the system.

> sudo apt update >sudo apt install scalpel

I think that Scalpel is already preinstalled, but make sure by reinstalling it again.

Reason:

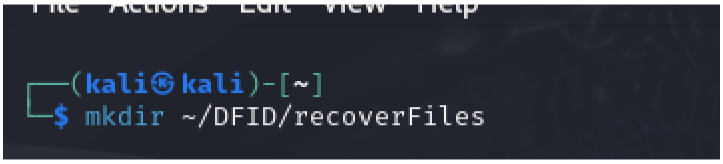
Scalpel is the primary tool used to recover deleted files. It works by scanning the disk or partition for specific file types based on headers/footers or other identifiable patterns.

I created a Directory which I called DFID (Digital Forensics Incident Response) as I am currently learning it. Hence the name, I had a Readme.md file from my previous project so I thought why not copy it and paste it on the Directory that I created, I deleted the file from the DFID as a way of “losing the file” so that I could retrieve it. You can do the same so that you can see if you can retrieve the file as well.

2. Create a Directory for Recovered Files

Step: Create a directory to store the recovered files.

mkdir ~/DFID/recoverFiles

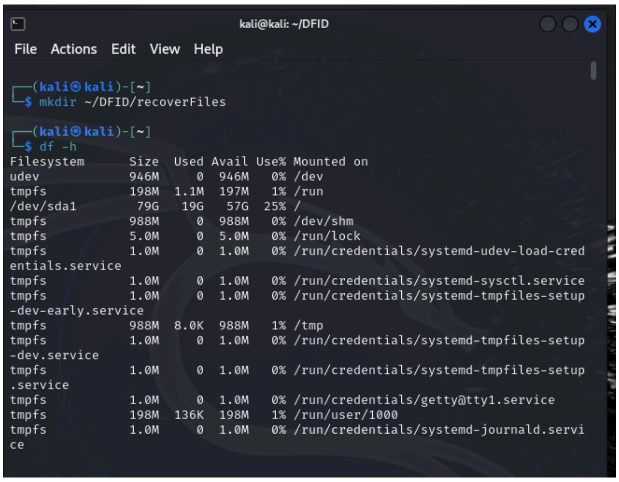


```
┌──(kali㉿kali)-[~]
└─$ mkdir ~/DFID/recoverFiles
```

We need a location where Scalpel will store the files it recovers during the carving process. This keeps the recovered data organized and isolated from the rest of the system.

3. Identify the Partition

Step: Identify the partition where the deleted file was located.



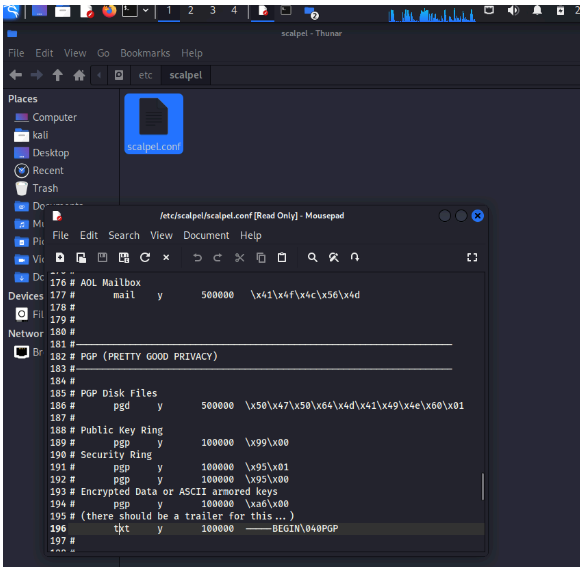
```
┌──(kali㉿kali)-[~]
└─$ mkdir ~/DFID/recoverFiles

┌──(kali㉿kali)-[~]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            946M     0  946M   0% /dev
tmpfs           198M  1.1M  197M   1% /run
/dev/sda1        79G   19G   57G  25% /
tmpfs           988M     0  988M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-udev-load-cred
entials.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup
-dev-early.service
tmpfs           988M  8.0K  988M   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup
-dev.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup
.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           198M  136K  198M   1% /run/user/1000
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.servi
ce
```

df -h / lsblk

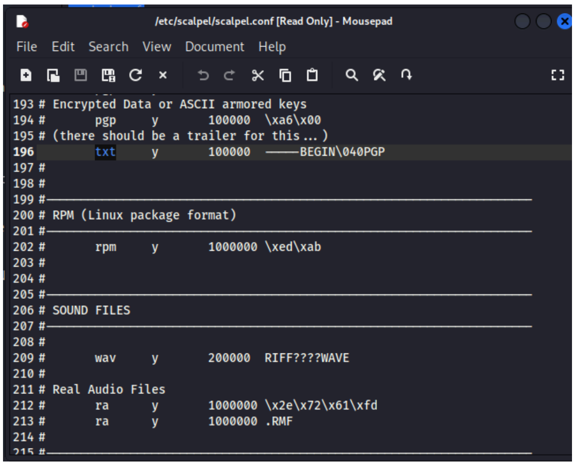
We need to specify which partition or storage device held the deleted file so that Scalpel knows where to scan for the data. As you can see in my case it was inside the /dev/sda1. Make sure you locate it. You can go to the folders on Kali, file system and look for a folder called dev and look at what folders or files are in there.

4. Configure Scalpel for File Recovery

Step: Edit Scalpel's configuration file (`scalpel.conf`).


scalpel - Thunar
File Edit View Go Bookmarks Help
etc
scalpel
Places
Computer
kali
Desktop
Recent
Trash
Devices
Network
scalpel.conf
/etc/scalpel/scalpel.conf [Read Only] - Mousepad
File Edit Search View Document Help

```
# AOL Mailbox
#       mail    y       500000   \x41\x4f\x4c\x56\x4d
#
#
#
#---------------------------------------------------------------------
# PGP (PRETTY GOOD PRIVACY)
#---------------------------------------------------------------------
#
# PGP Disk Files
#       pgd     y       500000  \x50\x47\x50\x64\x4d\x41\x49\x4e\x60\x01
#
# Public Key Ring
#       pgp     y       100000  \x99\x00
# Security Ring
#       pgp     y       100000  \x95\x01
#       pgp     y       100000  \x95\x00
# Encrypted Data or ASCII armored keys
#       pgp     y       100000  \xa6\x00
# (there should be a trailer for this ... )
        txt     y       100000  -----BEGIN\040PGP
#
```


/etc/scalpel/scalpel.conf [Read Only] - Mousepad
File Edit Search View Document Help

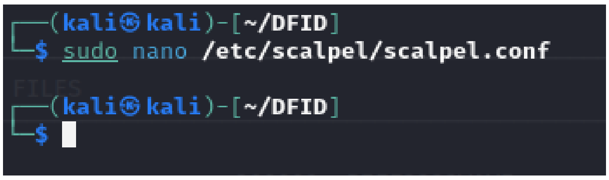
```
# Encrypted Data or ASCII armored keys
#       pgp     y       100000  \xa6\x00
# (there should be a trailer for this ... )
        txt     y       100000  -----BEGIN\040PGP
#
#
#---------------------------------------------------------------------
# RPM (Linux package format)
#---------------------------------------------------------------------
#       rpm     y       1000000 \xed\xab
#
#
#---------------------------------------------------------------------
# SOUND FILES
#---------------------------------------------------------------------
#
#       wav     y       200000  RIFF????WAVE
#
# Real Audio Files
#       ra      y       1000000 \x2e\x72\x61\xfd
#       ra      y       1000000 .RMF
#
#---------------------------------------------------------------------
```

sudo nano /etc/scalpel/scalpel.conf

- You can also find it inside where all your folders are in Kali, on the Devices > File system then look for a folder scalpel when you get in you will find a .txt right-click and open with a pad. Uncomment or add the following line to recover text-based files (like `Readme.md`)

  txt y 5000000 \x20\x20\x00\x00\x00\x00\x00\x00 \x20\x20\x20\x20

  Save and exit. Scalpel works by searching for specific file types based on the patterns defined in its configuration file. Since `Readme.md` is a text-based file, we modify the configuration to include text files in the recovery process.



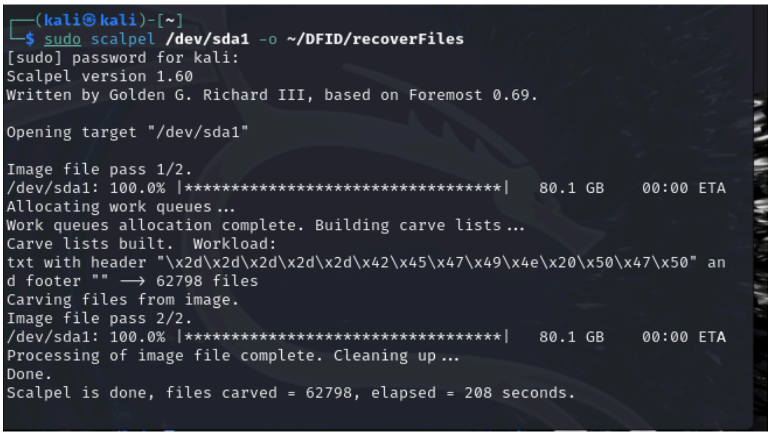
```
┌──(kali㉿kali)-[~/DFID]
└─$ sudo nano /etc/scalpel/scalpel.conf

┌──(kali㉿kali)-[~/DFID]
└─$ 
```

5. Run Scalpel to Recover the Deleted File

Step: Run Scalpel on the identified partition.

sudo scalpel /dev/sda1 -o ~/DFID/recoverFiles

We use this command to run Scalpel on the specified partition (`/dev/sda1` in this case) and output any recovered files to the `~/DFID/recoverFiles` directory. Scalpel will analyze the entire partition to locate any files that match the specified criteria (text files in this case).



```
┌──(kali㉿kali)-[~]
└─$ sudo scalpel /dev/sda1 -o ~/DFID/recoverFiles
[sudo] password for kali:
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/dev/sda1"

Image file pass 1/2.
/dev/sda1: 100.0% |**********************************|   80.1 GB    00:00 ETA
Allocating work queues ...
Work queues allocation complete. Building carve lists ...
Carve lists built.  Workload:
txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" an
d footer "" ⟶ 62798 files
Carving files from image.
Image file pass 2/2.
/dev/sda1: 100.0% |**********************************|   80.1 GB    00:00 ETA
Processing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 62798, elapsed = 208 seconds.
```

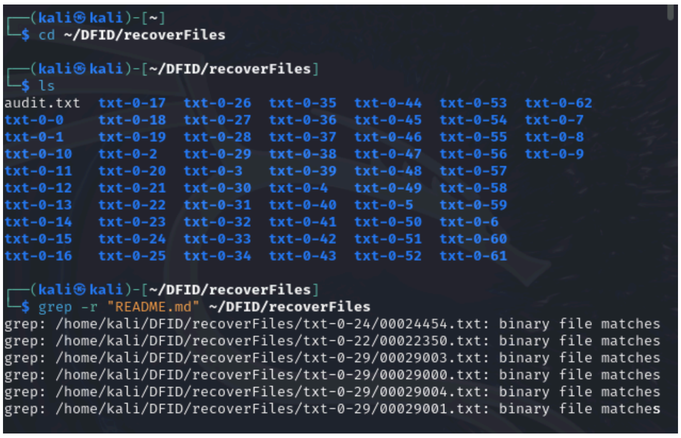
It will take some time so be patient, I hope you have your music playing as you do this. Walk around, drink some water, and look at the beautiful sunrise, lol I am doing this project early morning so I got to enjoy the sunrise. Let's get back to work.

6. Verify the Recovered Files

Step: After Scalpel completes the recovery process, verify that the deleted `Readme.md` file has been recovered.

cd ~/DFID/recoverFiles / grep -r "Readme" ~/DFID/recoverFiles

Mine came as audits.txt.This step allows us to confirm that Scalpel successfully recovered the deleted Readme.md file. We use grep to search through the recovered files for any instances of the term "Readme."

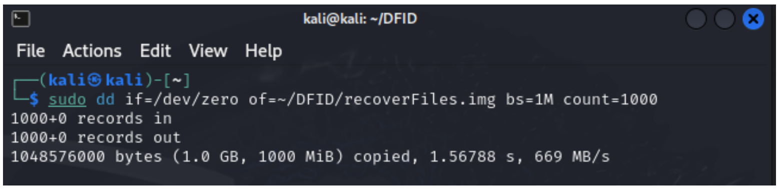


```
┌──(kali㉿kali)-[~]
└─$ cd ~/DFID/recoverFiles

┌──(kali㉿kali)-[~/DFID/recoverFiles]
└─$ ls
audit.txt  txt-0-17  txt-0-26  txt-0-35  txt-0-44  txt-0-53  txt-0-62
txt-0-0    txt-0-18  txt-0-27  txt-0-36  txt-0-45  txt-0-54  txt-0-7
txt-0-1    txt-0-19  txt-0-28  txt-0-37  txt-0-46  txt-0-55  txt-0-8
txt-0-10   txt-0-2   txt-0-29  txt-0-38  txt-0-47  txt-0-56  txt-0-9
txt-0-11   txt-0-20  txt-0-3   txt-0-39  txt-0-48  txt-0-57
txt-0-12   txt-0-21  txt-0-30  txt-0-4   txt-0-49  txt-0-58
txt-0-13   txt-0-22  txt-0-31  txt-0-40  txt-0-5   txt-0-59
txt-0-14   txt-0-23  txt-0-32  txt-0-41  txt-0-50  txt-0-6
txt-0-15   txt-0-24  txt-0-33  txt-0-42  txt-0-51  txt-0-60
txt-0-16   txt-0-25  txt-0-34  txt-0-43  txt-0-52  txt-0-61

┌──(kali㉿kali)-[~/DFID/recoverFiles]
└─$ grep -r "README.md" ~/DFID/recoverFiles
grep: /home/kali/DFID/recoverFiles/txt-0-24/00024454.txt: binary file matches
grep: /home/kali/DFID/recoverFiles/txt-0-22/00022350.txt: binary file matches
grep: /home/kali/DFID/recoverFiles/txt-0-29/00029003.txt: binary file matches
grep: /home/kali/DFID/recoverFiles/txt-0-29/00029000.txt: binary file matches
grep: /home/kali/DFID/recoverFiles/txt-0-29/00029004.txt: binary file matches
grep: /home/kali/DFID/recoverFiles/txt-0-29/00029001.txt: binary file matches
```

7. Create a Forensic Image of the Recovered Files

Step: Use the dd command to create a forensic image of the recovered files.

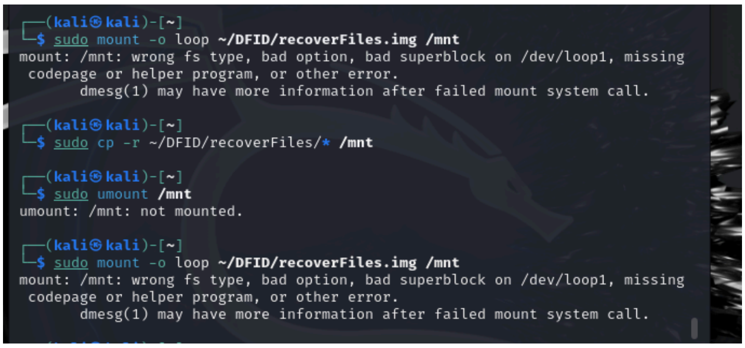
sudo dd if=/dev/zero of=~/DFID/recoverFiles.img bs=1M count=1000
Mount the newly created image: sudo mount -o loop ~/DFID/recovered_files.img /mnt



```
┌──(kali㉿kali)-[~]
└─$ sudo dd if=/dev/zero of=~/DFID/recoverFiles.img bs=1M count=1000
1000+0 records in
1000+0 records out
1048576000 bytes (1.0 GB, 1000 MiB) copied, 1.56788 s, 669 MB/s
```

Copy the recovered files into the image: sudo cp -r ~/DFID/recovered_files/* /mnt

sudo umount /mnt



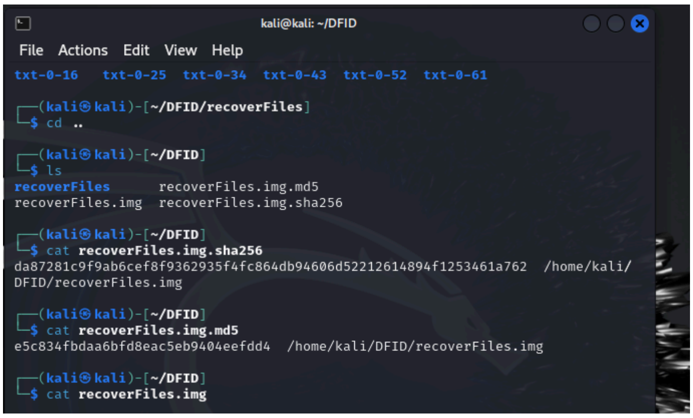
```
┌──(kali㉿kali)-[~]
└─$ sudo mount -o loop ~/DFID/recoverFiles.img /mnt
mount: /mnt: wrong fs type, bad option, bad superblock on /dev/loop1, missing
 codepage or helper program, or other error.
       dmesg(1) may have more information after failed mount system call.

┌──(kali㉿kali)-[~]
└─$ sudo cp -r ~/DFID/recoverFiles/* /mnt

┌──(kali㉿kali)-[~]
└─$ sudo umount /mnt
umount: /mnt: not mounted.

┌──(kali㉿kali)-[~]
└─$ sudo mount -o loop ~/DFID/recoverFiles.img /mnt
mount: /mnt: wrong fs type, bad option, bad superblock on /dev/loop1, missing
 codepage or helper program, or other error.
       dmesg(1) may have more information after failed mount system call.
```

The dd command is commonly used in digital forensics to create a bit-for-bit copy (disk image) of the recovered files. This ensures that the recovered data is preserved in a forensically sound manner. By copying the files into a forensic image, we protect the integrity of the recovered data for further analysis.

8. Generate a Hash for the Forensic Image

Step: Generate a hash of the forensic image to ensure integrity.

- **For MD5 hash**: md5sum ~/DFID/recoverFiles.img > ~/DFID/recoverFiles.img.md5
- **For SHA-256 hash**:sha256sum ~/DFID/recoverFiles.img > ~/DFID/recoverFiles.img.sha256



```
txt-0-16   txt-0-25  txt-0-34  txt-0-43  txt-0-52  txt-0-61

┌──(kali㉿kali)-[~/DFID/recoverFiles]
└─$ cd ..

┌──(kali㉿kali)-[~/DFID]
└─$ ls
recoverFiles       recoverFiles.img.md5
recoverFiles.img  recoverFiles.img.sha256

┌──(kali㉿kali)-[~/DFID]
└─$ cat recoverFiles.img.sha256
da87281c9f9ab6cef8f9362935f4fc864db94606d52212614894f1253461a762  /home/kali/
DFID/recoverFiles.img

┌──(kali㉿kali)-[~/DFID]
└─$ cat recoverFiles.img.md5
e5c834fbdaa6bfd8eac5eb9404eefdd4  /home/kali/DFID/recoverFiles.img

┌──(kali㉿kali)-[~/DFID]
└─$ cat recoverFiles.img
```

Generating a hash of the forensic image allows us to verify that the image has not been altered or tampered with in the future. Hashes are critical in forensic investigations to confirm the authenticity and integrity of evidence. **I hope you find this guide helpful, wait for more as more is coming. XOXO Gamu**