Experiment No.7
To perform data carving using open source tools
Date of Performance:
Date of Submission:

Aim: To perform data carving using open source tools

Objective: To make use of the scalpel tool to recover from a disk image

Theory:

Data carving, also known as file carving, is the forensic technique of reassembling files from raw data fragments when no filesystem metadata is available. It is a common procedure when performing data recovery, after a storage device failure, for instance. In Digital Forensics, carving is a helpful technique in finding hidden or deleted files from digital media. A file can be hidden in areas like lost clusters, unallocated clusters and slack space of the disk or digital media. To use this method of extraction, a file should have a standard file signature called a file header (start of the file). A search is performed to locate the file header and continued until the file footer (end of the file) is reached. The data between these two points will be extracted and analyzed to validate the file. The extraction algorithm uses different methods of carving depending on the file formats.

Scalpel

scalpel is a fast file carver that reads a database of header and footer definitions and extracts matching files from a set of image files or raw device files.

scalpel is filesystem-independent and will carve files from FAT16, FAT32, exFAT, NTFS, Ext2, Ext3, Ext4, JFS, XFS, ReiserFS, raw partitions, etc.

scalpel is a complete rewrite of the Foremost 0.69 file carver and is useful for both digital forensics investigations and file recovery.

Scalpel is also included in the Autopsy tool. On Kali Linux, scalpel is available as a command based tool.

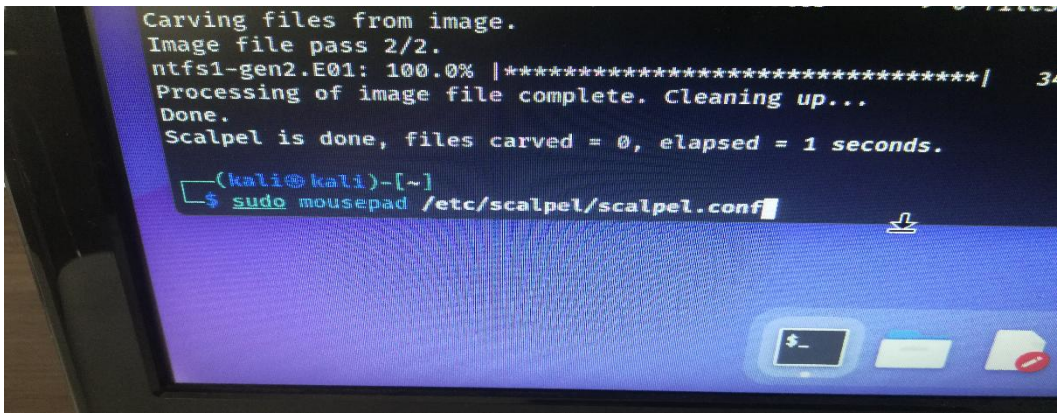


Fig.1 Edit Scalpel.conf file

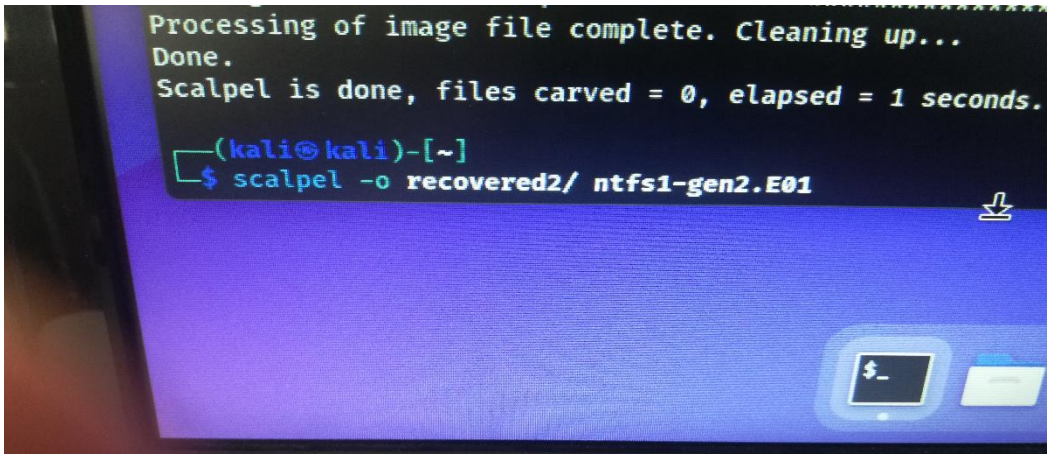


Fig. 2 Command to Carve out file

The above images shows the view of the scalpel tool on the Kali Linux platform.

Process:

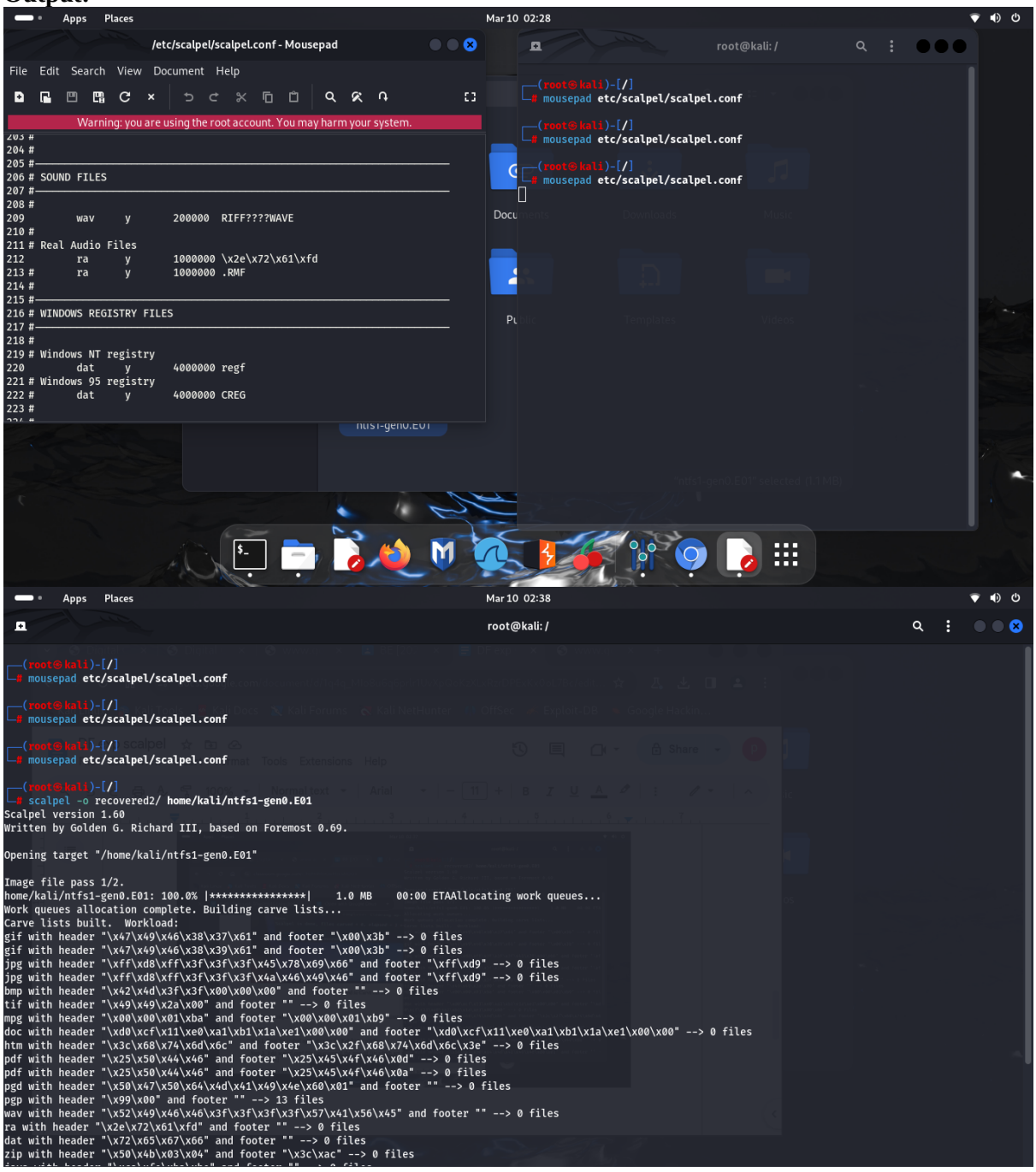
Step 1. Open the scalpel application on the Kali Linux platform

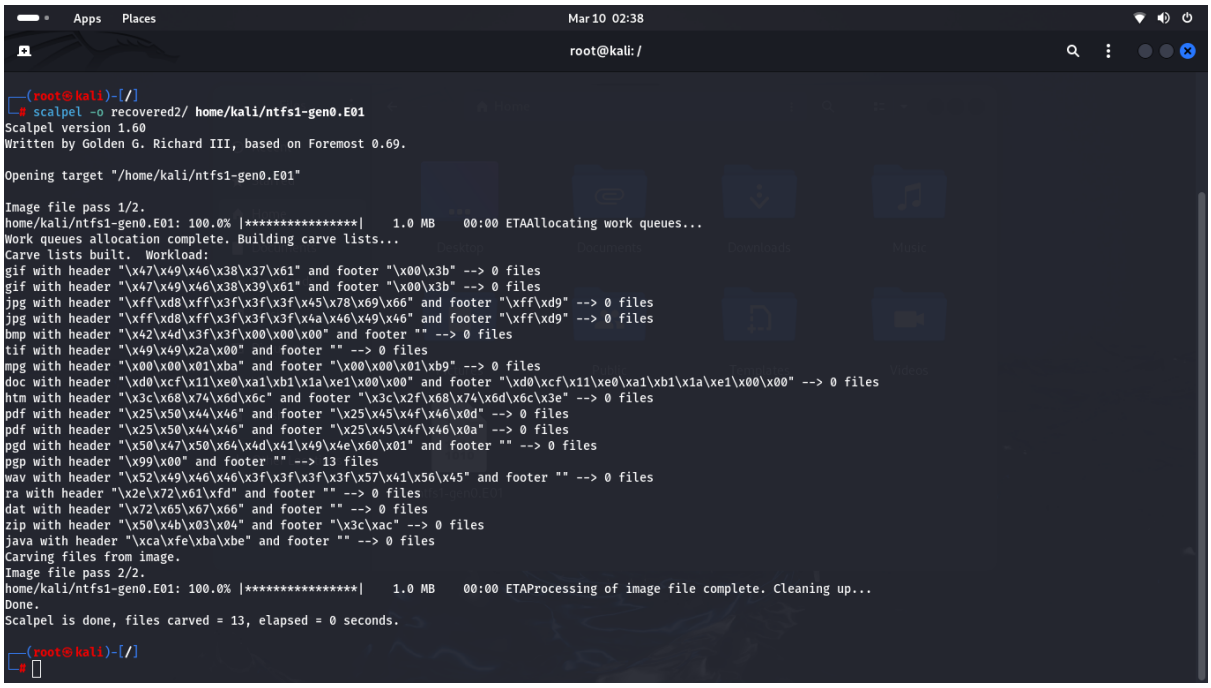
Step 2. Edit scalpel.conf file [un-comment the type of file which are needed to be carved out – Refer Fig.1]

Step 3. Create/download mirror image of the hard disk which is to analyzed by scalpel

Step 4. Carve out the files from the mirror image of the hard disk [Refer fig.2]

Output:


Apps Places
Mar 10 02:28
/etc/scalpel/scalpel.conf - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
root@kali: /
(root㉿kali)-[/]
mousepad etc/scalpel/scalpel.conf
Apps Places
Mar 10 02:38
root@kali: /
(root㉿kali)-[/]
scalpel -o recovered2/ home/kali/ntfs1-gen0.E01
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Opening target "/home/kali/ntfs1-gen0.E01"
Image file pass 1/2.
home/kali/ntfs1-gen0.E01: 100.0% |****************| 1.0 MB 00:00 ETAAllocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built. Workload:
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" --> 0 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 0 files
tif with header "\x49\x49\x2a\x00" and footer "" --> 0 files
mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 0 files
htm with header "\x3c\x68\x74\x6d\x6c" and footer "\x3c\x2f\x68\x74\x6d\x6c\x3e" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files
pgd with header "\x50\x47\x50\x64\x4d\x41\x49\x4e\x60\x01" and footer "" --> 0 files
pgp with header "\x99\x00" and footer "" --> 13 files
wav with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x57\x41\x56\x45" and footer "" --> 0 files
ra with header "\x2e\x72\x61\xfd" and footer "" --> 0 files
dat with header "\x72\x65\x67\x66" and footer "" --> 0 files
zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 0 files



Conclusion:

Scalpel is a powerful file carving tool in digital forensics that helps recover deleted or fragmented files from disk images, providing crucial evidence that might otherwise be lost. It supports various file formats and is essential for reconstructing files from raw data. In a digital forensics investigation, Scalpel plays a key role in recovering hidden or deleted evidence, aiding in case resolution.