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.

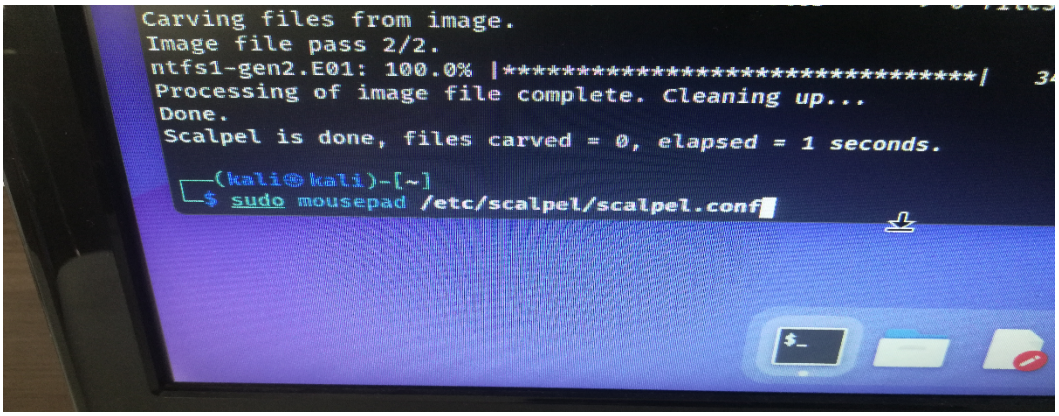


Fig.1 Edit Scalpel.conf file

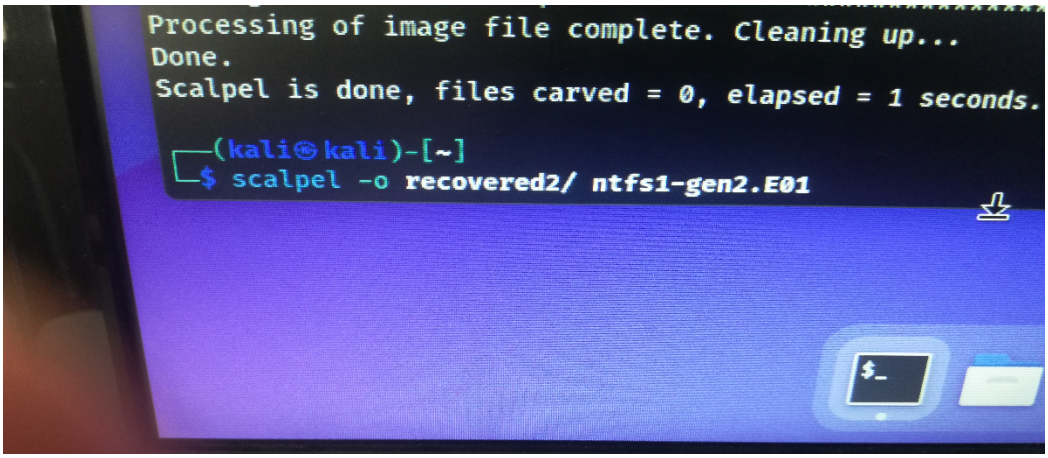


Fig. 2 Command to Carve out file

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

Process:

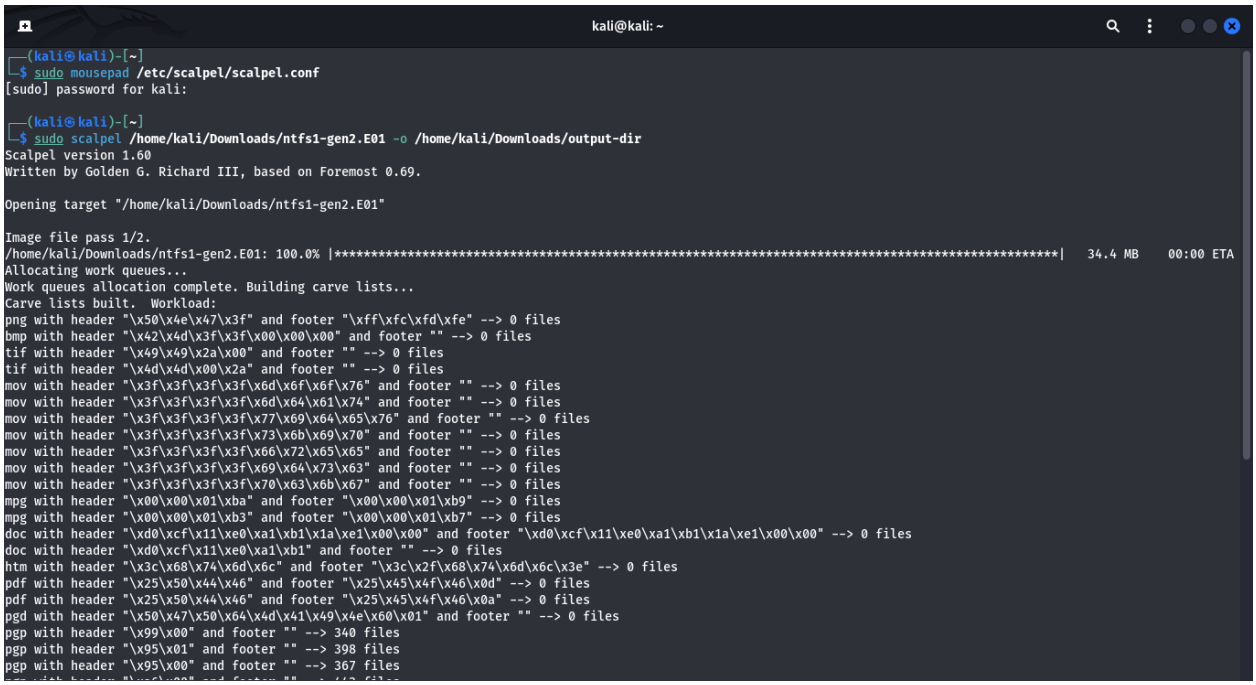
Step 1. Open the scalpel application on the Kali Linux platform

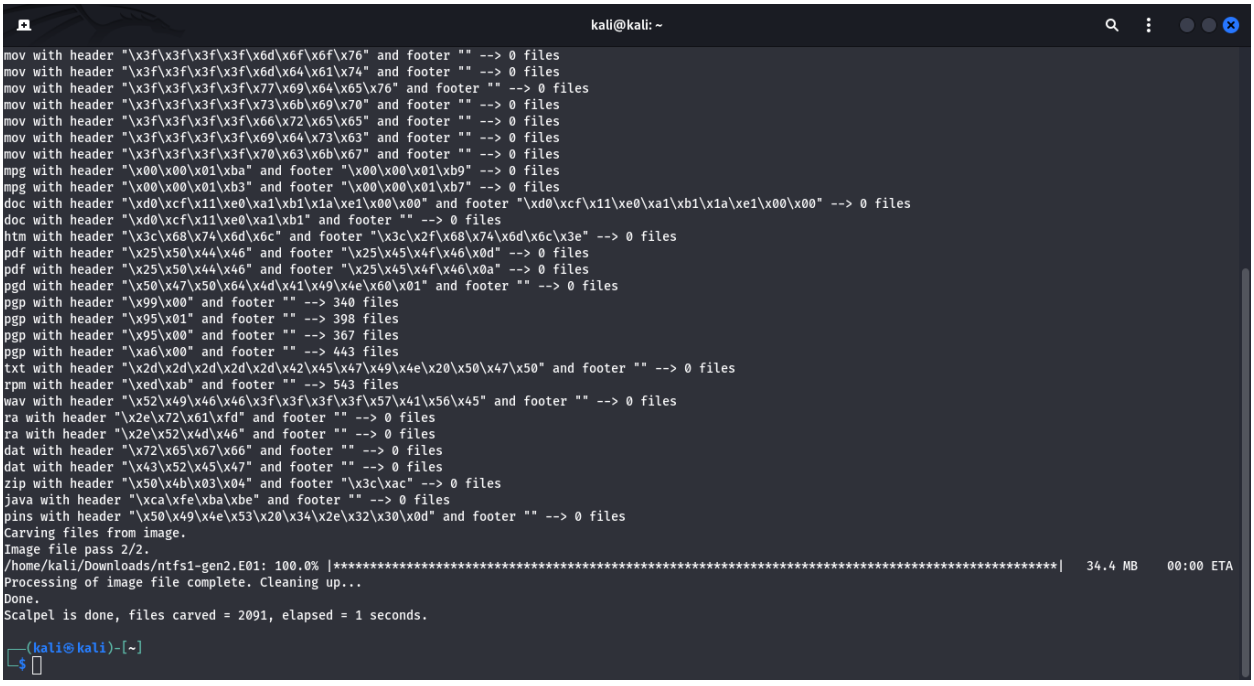
Step 2. Edit scalpel.conf file [un-comment the type of file which are needed to be carved out – Refer Fig.1]

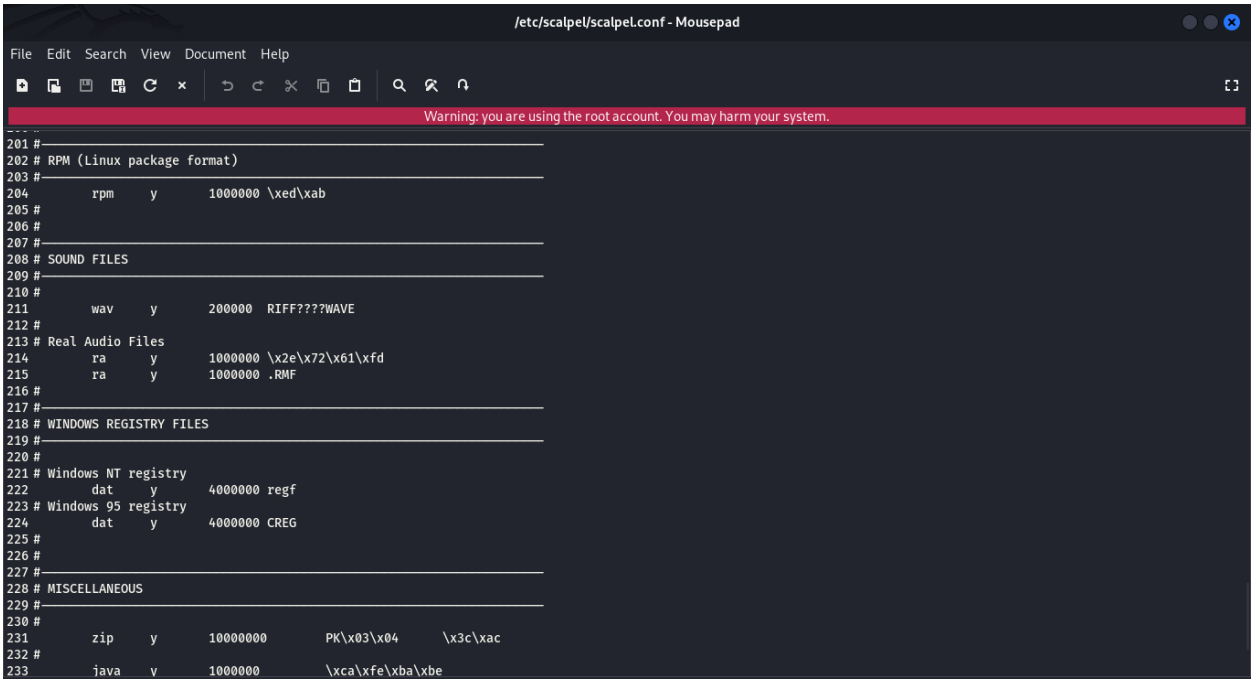
Step 3. Create/download mirror image of the hard disk which is to analyzed by scalpel

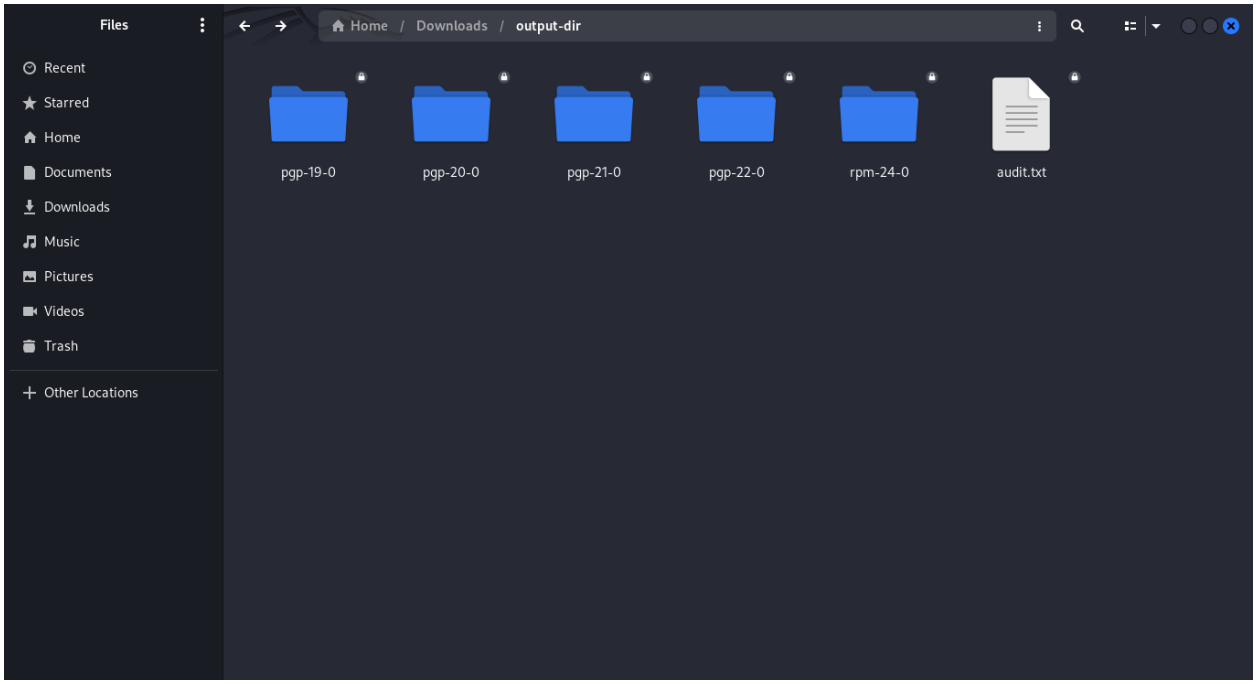
Step 4. Carve out the files from the mirror image of the hard disk [Refer fig.2]

Output:


kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ sudo mousepad /etc/scalpel/scalpel.conf
[sudo] password for kali:
┌──(kali㉿kali)-[~]
└─$ sudo scalpel /home/kali/Downloads/ntfs1-gen2.E01 -o /home/kali/Downloads/output-dir
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Opening target "/home/kali/Downloads/ntfs1-gen2.E01"
Image file pass 1/2.
/home/kali/Downloads/ntfs1-gen2.E01: 100.0% |********| 34.4 MB 00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built. Workload:
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 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
tif with header "\x4d\x4d\x00\x2a" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x6f\x6f\x76" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x64\x61\x74" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x77\x69\x64\x65\x76" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x73\x6b\x69\x70" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x66\x72\x65\x65" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x69\x64\x73\x63" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x70\x63\x6b\x67" and footer "" --> 0 files
mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 0 files
mpg with header "\x00\x00\x01\xb3" and footer "\x00\x00\x01\xb7" --> 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
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 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 "" --> 340 files
pgp with header "\x95\x01" and footer "" --> 398 files
pgp with header "\x95\x00" and footer "" --> 367 files


kali@kali: ~
mov with header "\x3f\x3f\x3f\x3f\x6d\x6f\x6f\x76" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x6d\x64\x61\x74" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x77\x69\x64\x65\x76" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x73\x6b\x69\x70" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x66\x72\x65\x65" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x69\x64\x73\x63" and footer "" --> 0 files
mov with header "\x3f\x3f\x3f\x3f\x70\x63\x6b\x67" and footer "" --> 0 files
mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 0 files
mpg with header "\x00\x00\x01\xb3" and footer "\x00\x00\x01\xb7" --> 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
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 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 "" --> 340 files
pgp with header "\x95\x01" and footer "" --> 398 files
pgp with header "\x95\x00" and footer "" --> 367 files
pgp with header "\xa6\x00" and footer "" --> 443 files
txt with header "\x2d\x2d\x2d\x2d\x2d\x42\x45\x47\x49\x4e\x20\x50\x47\x50" and footer "" --> 0 files
rpm with header "\xed\xab" and footer "" --> 543 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
ra with header "\x2e\x52\x4d\x46" and footer "" --> 0 files
dat with header "\x72\x65\x67\x66" and footer "" --> 0 files
dat with header "\x43\x52\x45\x47" and footer "" --> 0 files
zip with header "\x50\x4b\x03\x04" and footer "\x3c\xac" --> 0 files
java with header "\xca\xfe\xba\xbe" and footer "" --> 0 files
pins with header "\x50\x49\x4e\x53\x20\x34\x2e\x32\x30\x0d" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
/home/kali/Downloads/ntfs1-gen2.E01: 100.0% |********| 34.4 MB 00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 2091, elapsed = 1 seconds.
┌──(kali㉿kali)-[~]
└─$


/etc/scalpel/scalpel.conf - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
201 #----------
202 # RPM (Linux package format)
203 #----------
204 rpm y 1000000 \xed\xab
205 #
206 #
207 #----------
208 # SOUND FILES
209 #----------
210 #
211 wav y 200000 RIFF????WAVE
212 #
213 # Real Audio Files
214 ra y 1000000 \x2e\x72\x61\xfd
215 ra y 1000000 .RMF
216 #
217 #----------
218 # WINDOWS REGISTRY FILES
219 #----------
220 #
221 # Windows NT registry
222 dat y 4000000 regf
223 # Windows 95 registry
224 dat y 4000000 CREG
225 #
226 #
227 #----------
228 # MISCELLANEOUS
229 #----------
230 #
231 zip y 10000000 PK\x03\x04 \x3c\xac
232 #
233 java y 1000000 \xca\xfe\xba\xbe


Files
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
Home / Downloads / output-dir
pgp-19-0
pgp-20-0
pgp-21-0
pgp-22-0
rpm-24-0
audit.txt

Conclusion:

Scalpel plays a significant role in digital forensics investigations by enabling the recovery of deleted or hidden files from raw disk images, even when filesystem metadata is missing or corrupted. Its ability to carve out files based on headers and footers makes it a powerful tool for extracting evidence such as documents, images, and media files from unallocated space, slack space, or formatted partitions. This capability is especially valuable in cases where suspects attempt to destroy or hide digital evidence, thus making Scalpel an essential utility for forensic analysts during evidence recovery and analysis.