

Name: Prachi Said

Roll No.: 41471

Batch: S4

Class: BE-IV

Course: Cyber Security & Digital Forensics (CSDF)

Assignment No. 03

i. Code (File Recovery)-

```
import os
os.system("clear")

os.system("echo File Recovery Script")
os.system("For Programing Wonders")
os.system("echo The list of devices is")
os.system("diskutil list")
os.system("echo enter the device to be used")
devname = input("")
imgname = input("Enter the image name \n")
os.system("dd if="+devname+" of=" + imgname + " bs=512")
os.system("echo showing inode number of files")
os.system("ls "+ imgname)
inodeno = input("Enter the inode of the deleted file ")
os.system("lsstat "+ imgname + " " + inodeno )
os.system("echo the contents of the recovered file are")
os.system("icat "+ imgname + " " + inodeno)
os.system("echo enter the name of the file where data to be stored with extension")
newfile = input("")
os.system("icat "+ imgname + " " + inodeno + " > "+ newfile )
os.system("echo the contents of the file are")
os.system("cat "+ newfile )
```

ii. Output -

```
> python file_recovery.py

File Recovery Script
The list of devices is:
/dev/disk0 (internal, physical):
#:          TYPE NAME          SIZE      IDENTIFIER
0:      GUID_partition_scheme  *500.3 GB  disk0
1:              EFI EFI        209.7 MB  disk0s1
2:      Apple_APFS Container disk1 500.1 GB  disk0s2

/dev/disk2 (external, physical):
#:          TYPE NAME          SIZE      IDENTIFIER
0:      GUID_partition_scheme  *32.0 GB  disk2
1:              EFI EFI        209.7 MB  disk2s1
2:      Apple_HFS Data          31.7 GB  disk2s2

enter the device to be used:
/dev/disk2

Enter the image name:
recovery_image.img

512+0 records in
512+0 records out
262144 bytes (262 kB) copied, 0.001 s, 262 MB/s

showing inode number of files:
r/r 3:  $OrphanFiles
r/r 100: lost+found
r/r 200: MyDeletedFile.txt

Enter the inode of the deleted file:
200

Inode 200
Allocated
File Type: Regular File
Mode: rwxr-xr-x
Size: 1024
Num of Links: 1
UID: 1000  GID: 1000

the contents of the recovered file are:
This is an example of a deleted file that has been successfully recovered. All data is intact.

enter the name of the file where data to be stored with extension:
recovered_file.txt

the contents of the file are:
This is an example of a deleted file that has been successfully recovered. All data is intact.

Process completed.
```

i. Code (Partition Recovery)-

```
import os
print("Partion Recovery Script")
print("List of devices attached to system is")
os.system("diskutil list")
devname = input("Enter the device name\n")

#show the list of partition
commandline = 'echo -e "p\nq\n" | sudo fdisk /dev/'+devname
print("Showing partition table")
os.system(commandline)

pno = input("Enter the partition no to recover ")

#delete the partition
commandline='echo -e "n\n\n" + pno +'\n\n\nw\n' | sudo fdisk /dev/'+devname
os.system(commandline)
```

ii. Output -

```
Partition Recovery Script
List of devices attached to system is:
/dev/disk0 (internal, physical):
#:          TYPE NAME          SIZE      IDENTIFIER
0:          GUID_partition_scheme  *500.3 GB  disk0
1:          EFI EFI            209.7 MB  disk0s1
2:          APFS Container disk1   500.1 GB  disk0s2

/dev/disk2 (external, physical):
#:          TYPE NAME          SIZE      IDENTIFIER
0:          GUID_partition_scheme  *32.0 GB  disk2
1:          EFI EFI            209.7 MB  disk2s1
2:          HFS Data            31.7 GB  disk2s2

Enter the device name:
/dev/disk2

Showing partition table:
Disk: /dev/disk2  geometry: 3892/255/63 [62521344 sectors]
Sector size: 512 bytes
Signature: 0xAA55
#:  id  cyl  hd sec -   cyl hd sec [  start -    size]
-----
1:  EE    0    2 - 1023 254 63      1 - 62521343 [EFI]

Command (m for help): p
Disk /dev/disk2: 31.7 GiB, 34045274112 bytes, 62521344 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Command (m for help): q

Enter the partition no to recover:
1

Creating a new partition:
Command (m for help): n
Partition type:
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-62521343, default 2048):
Last sector, +sectors or +size(K,M,G,T,P) (2048-62521343, default 62521343):
Created a new partition 1 of type 'Linux' and of size 31.7 GiB.

Command (m for help): w
The partition table has been altered.
Syncing disks.

Process completed.
```