

LAB-05 Reviewing-Unallocated-Space-Extracting-Data-with-Tools-Digital-Investigation-Processes

AIM:

To review unallocated space in a disk image, extract data using forensic tools, and understand the digital investigation process.

DESIGN STEPS:

Step 1:

Use tools like Autopsy or Sleuth Kit (blkls, icat) to identify and analyze unallocated space.

Step 2:

Extract data from unallocated space and examine for hidden or deleted content.

Step 3:

Document and interpret findings as part of the digital investigation process.

PROGRAM:

Data Extraction and Investigation Tool Usage

Command 1

```
lsblk
```



Command 2

```
sudo dd if=/dev/sda of=/home/kali/disk.img bs=512
```



Command 3

```
mmls ~/disk.img
```



Command 4

```
sudo ls -lh disk.img
```



Command 5

```
strings disk.img | less
```



OUTPUT:

Command 1

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ lsblk  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  
sda 8:0 0 80.1G 0 disk  
└─sda1 8:1 0 80.1G 0 part /  
sr0 11:0 1 1024M 0 rom  
  
(kali@kali)-[~]  
$
```

Command 2

```
(kali@kali)-[~]  
$ sudo dd if=/dev/sda of=/home/kali/disk.img bs=1M count=10  
10+0 records in  
10+0 records out  
10485760 bytes (10 MB, 10 MiB) copied, 0.0218616 s, 480 MB/s  
  
(kali@kali)-[~]  
$
```

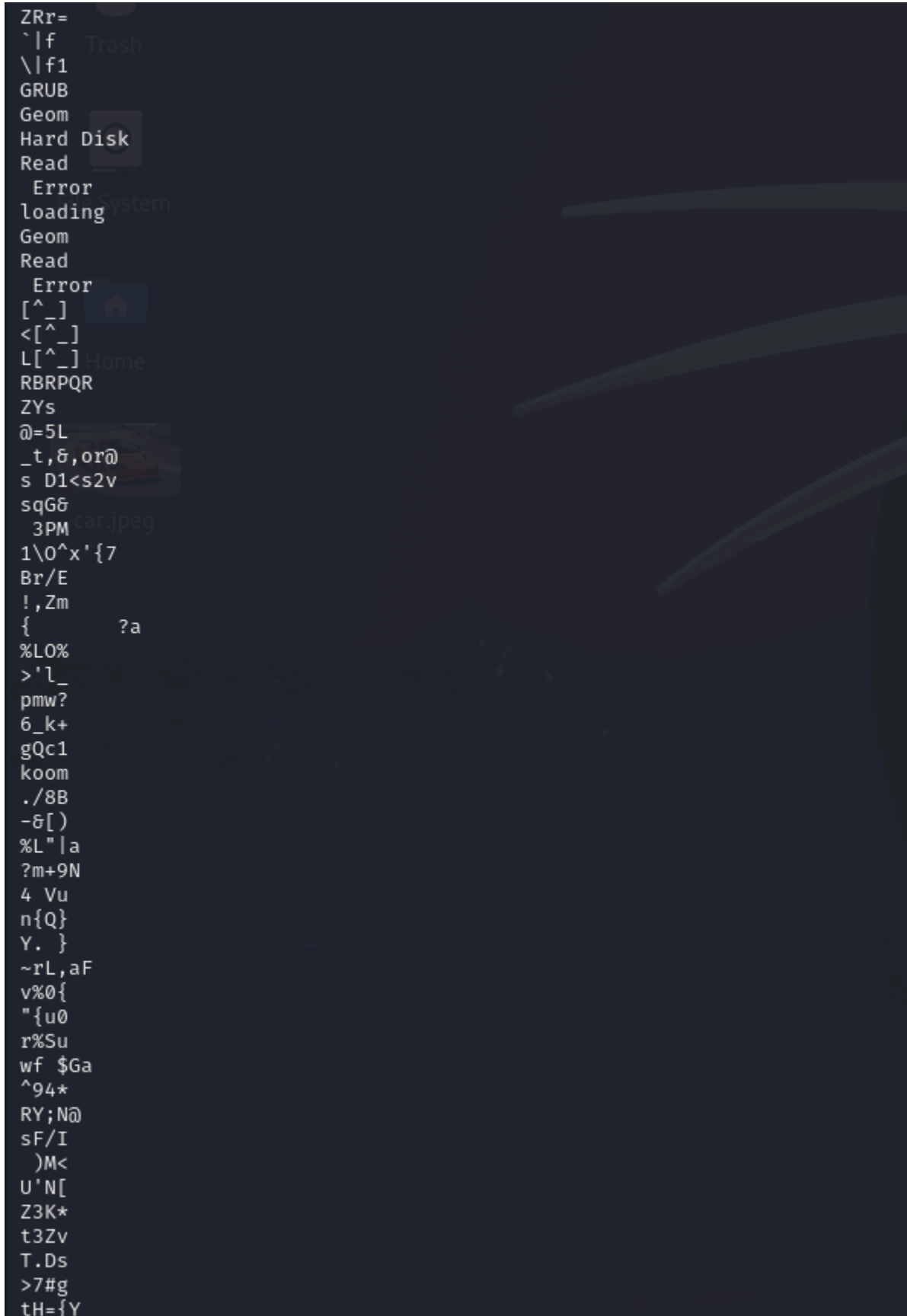
Command 3

```
(kali@kali)-[~]  
$ mmls ~/disk.img  
DOS Partition Table  
Offset Sector: 0  
Units are in 512-byte sectors  
  
Slot Start End Length Description  
000: Meta 0000000000 0000000000 0000000001 Primary Table (#0)  
001: 0000000000 0000002047 0000002048 Unallocated  
002: 000:000 0000002048 0167968749 0167966702 Linux (0x83)
```

Command 4

```
(kali㉿kali)-[~]  
$ sudo ls -lh disk.img  
-rw-r--r-- 1 root root 10M Apr 22 19:28 disk.img  
  
(kali㉿kali)-[~]  
$
```

Command 5



RESULT:

The unallocated space was successfully analyzed, data was extracted, and the digital investigation process was followed effectively.