Analysis-of-the-Disk-Structure-using-Sleuth-Kit

AIM:

To analyze the disk structure of a given disk image using Sleuth Kit tools in Kali Linux.

DESIGN STEPS:

Step 1:

Obtain or create a disk image file (e.g., disk.dd) to analyze. Open the terminal in Kali Linux.

Step 2:

Use Sleuth Kit tools like mmls, fsstat, and fls to examine the partition layout, file system details, and file listing.

Step 3:

Interpret the output of the tools to understand the disk structure, including partitions, sectors, and files.

PROGRAM:

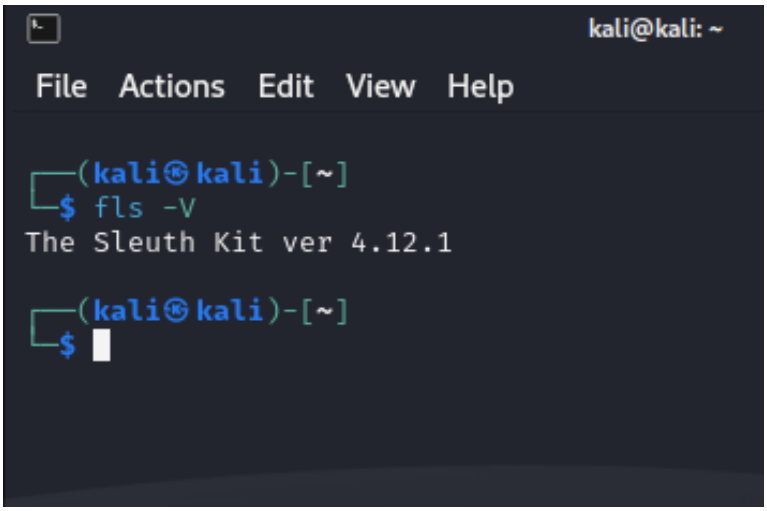
Sleuth Kit Disk Analysis Commands

✅ Option 1: Create a Sample Disk Image (for Testing)

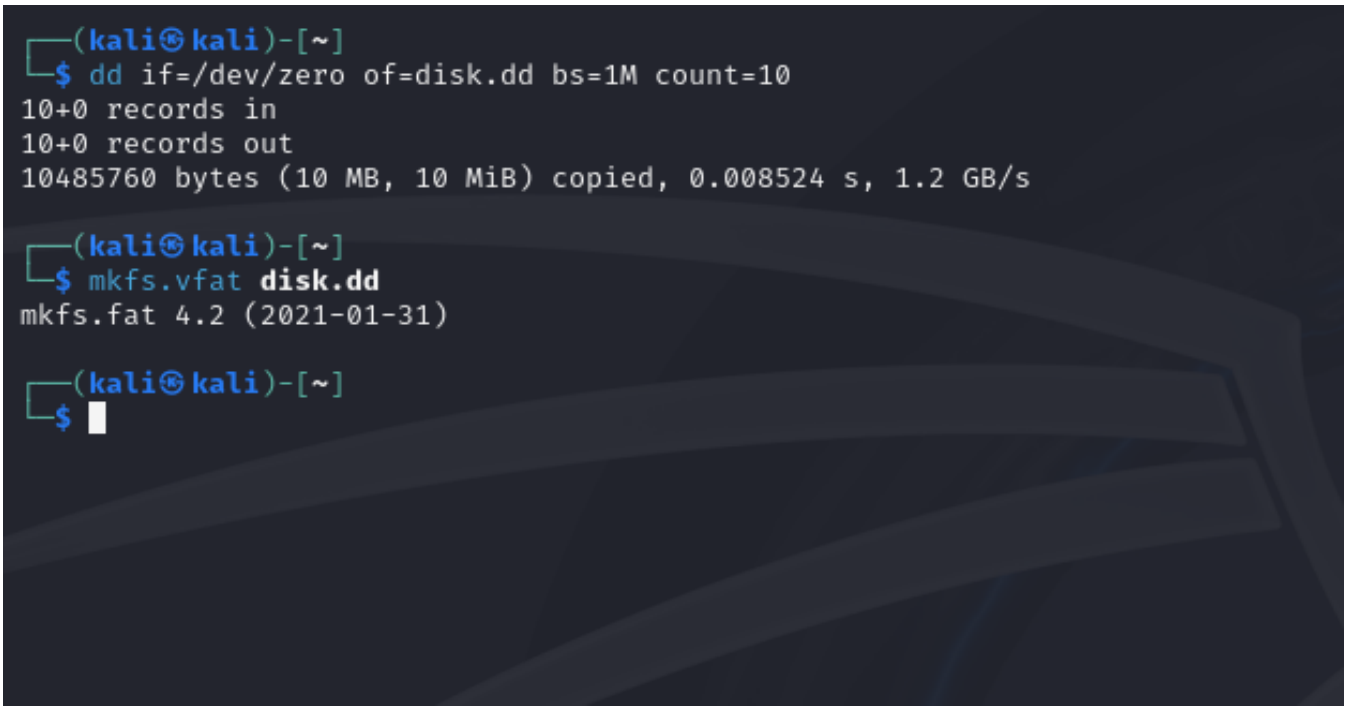
Let's create a 10MB blank disk image and simulate file system activity:

```
cd ~/Downloads

# Step 1: Create an empty disk image
dd if=/dev/zero of=file.dd bs=1M count=10

# Step 2: Format it with a file system (like FAT32)
mkfs.vfat file.dd
```

OUTPUT:



Create Disk



mmls

```
mmls disk.dd
```

fls

```
fls -f fat -o 0 disk.dd
```

```
┌──(kali㉿kali)-[~]
└─$ mmls disk.dd

┌──(kali㉿kali)-[~]
└─$ fls -f fat -o 0 disk.dd
v/v 326979:     $MBR
v/v 326980:     $FAT1
v/v 326981:     $FAT2
V/V 326982:     $OrphanFiles

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ sudo mkdir /mnt/dd_mount
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo mount -o loop disk.dd /mnt/dd_mount

┌──(kali㉿kali)-[~]
└─$ sudo cp /home/kali/Desktop/car.jpeg /mnt/dd_mount

┌──(kali㉿kali)-[~]
└─$ sudo touch /mnt/dd_mount/afshan.txt

┌──(kali㉿kali)-[~]
└─$ sudo mkdir /mnt/dd_mount/DFDI_EX2
```

```
┌──(kali㉿kali)-[~]
└─$ fls -f fat -o 0 disk.dd
r/r 4:  car.jpeg
r/r 6:  afshan.txt
d/d 7:  DFDI_EX2
v/v 326979:     $MBR
v/v 326980:     $FAT1
v/v 326981:     $FAT2
V/V 326982:     $OrphanFiles

┌──(kali㉿kali)-[~]
└─$
```

RESULT:

The analysis was performed successfully using Sleuth Kit, and the disk structure was understood in detail.