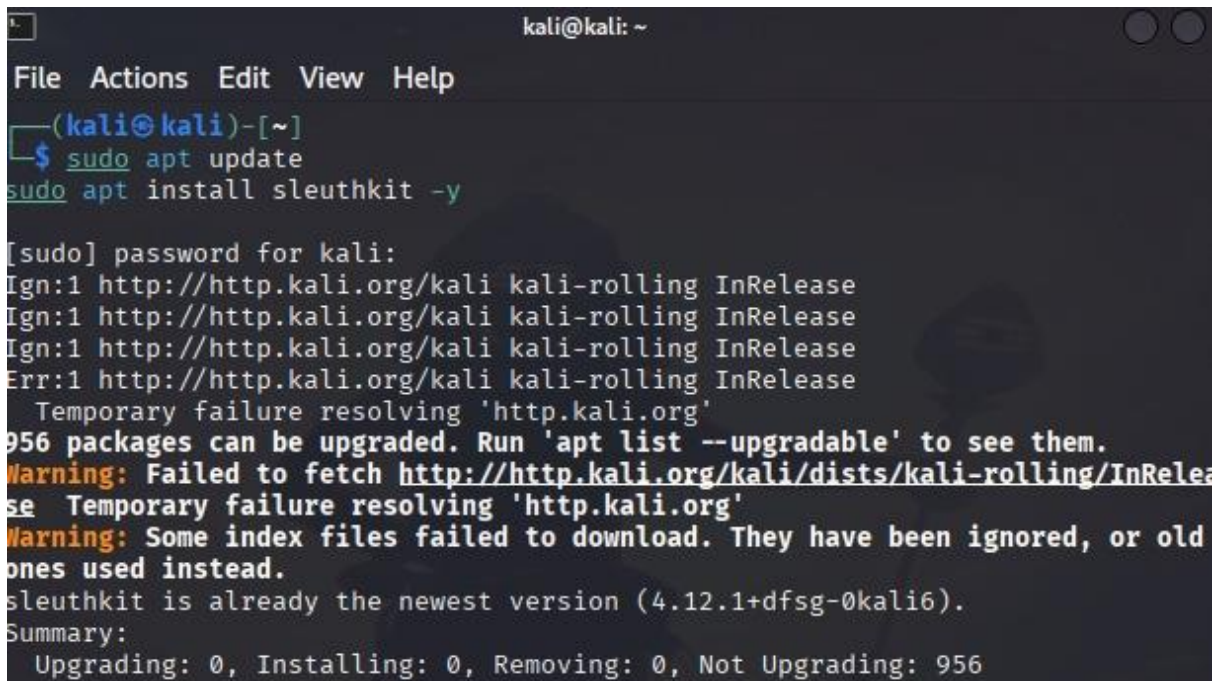


Experiment No. 6 — Use Sleuth Kit to Analyze Digital Evidence

Aim

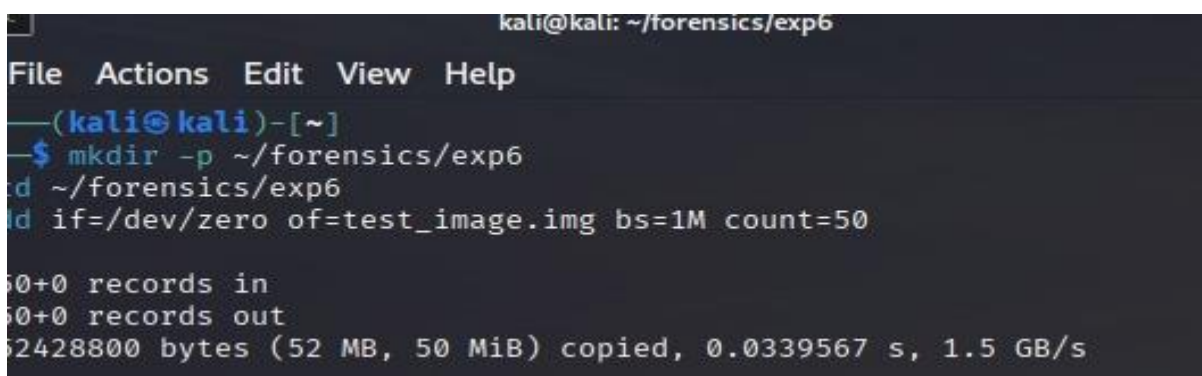
To use **The Sleuth Kit (TSK)** command-line tools to analyze a disk image and recover digital evidence.

Step 1 — install sleuth kit in linux terminal



```
kali@kali: ~  
File Actions Edit View Help  
—(kali@kali)-[~]  
$ sudo apt update  
sudo apt install sleuthkit -y  
[sudo] password for kali:  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Err:1 http://http.kali.org/kali kali-rolling InRelease  
Temporary failure resolving 'http.kali.org'  
956 packages can be upgraded. Run 'apt list --upgradable' to see them.  
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  
Temporary failure resolving 'http.kali.org'  
Warning: Some index files failed to download. They have been ignored, or old  
ones used instead.  
sleuthkit is already the newest version (4.12.1+dfsg-0kali6).  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 956
```

Step 2 — Create a Dummy Disk Image:



```
kali@kali: ~/forensics/exp6  
File Actions Edit View Help  
—(kali@kali)-[~]  
$ mkdir -p ~/forensics/exp6  
cd ~/forensics/exp6  
dd if=/dev/zero of=test_image.img bs=1M count=50  
50+0 records in  
50+0 records out  
52428800 bytes (52 MB, 50 MiB) copied, 0.0339567 s, 1.5 GB/s
```

Step 3 — Format the Image with a Filesystem

```
(kali㉿kali)-[~/forensics/exp6]
$ mkfs.ext4 test_image.img

mke2fs 1.47.2 (1-Jan-2025)
Discarding device blocks: done
Creating filesystem with 51200 1k blocks and 12824 inodes
Filesystem UUID: 1b2d5ff4-8d0a-44cc-bf54-5e64fd799622
Superblock backups stored on blocks:
    8193, 24577, 40961

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
```

Step 4 — Mount and Add Sample Files

```
(kali㉿kali)-[~/forensics/exp6]
$ sudo mkdir -p /mnt/testmount
sudo mount -o loop test_image.img /mnt/testmount

sudo touch /mnt/testmount/file1.txt
echo "This is digital evidence file." | sudo tee /mnt/testmount/file1.txt
sudo mkdir /mnt/testmount/docs
echo "Confidential report inside docs folder." | sudo tee /mnt/testmount/docs
/report.txt
sudo umount /mnt/testmount

[sudo] password for kali:
\\This is digital evidence file.
Confidential report inside docs folder.
```

Step 5 — Identify File System Information & List Files and Directories

```
(kali㉿kali)-[~/forensics/exp6]
└─$ fsstat test_image.img > filesystem_info.txt
cat filesystem_info.txt | head -n 10

FILE SYSTEM INFORMATION
-----
File System Type: Ext4
Volume Name:
Volume ID: 229679fd645e54bfcc440a8df45f2d1b

Last Written at: 2025-10-21 11:33:28 (EDT)
Last Checked at: 2025-10-21 11:33:11 (EDT)

Last Mounted at: 2025-10-21 11:33:28 (EDT)

(kali㉿kali)-[~/forensics/exp6]
└─$ fls -r test_image.img > file_list.txt
cat file_list.txt

d/d 11: lost+found
r/r 13: file1.txt
d/d 1833: docs
+ r/r 14: report.txt
V/V 12825: $OrphanFiles
```

Step 6 — View Metadata of a File

```
(kali㉿kali)-[~/forensics/exp6]
└─$ istat test_image.img 12 > metadata_info.txt
cat metadata_info.txt

inode: 12
Allocated
Group: 0
Generation Id: 0
uid / gid: 0 / 0
mode: rrw-----
Flags: Extents,
size: 32768
num of links: 1

Inode Times:
Accessed:      2025-10-21 11:33:11.000000000 (EDT)
File Modified: 2025-10-21 11:33:11.000000000 (EDT)
Inode Modified: 2025-10-21 11:33:11.000000000 (EDT)
File Created:  2025-10-21 11:33:11.000000000 (EDT)

Direct Blocks:
3493 3494 3495 3496 3497 3498 3499 3500
3501 3502 3503 3504 3505 3506 3507 3508
3509 3510 3511 3512 3513 3514 3515 3516
3517 3518 3519 3520 3521 3522 3523 3524
```

Step 7 — Recover a File from the Image

```
(kali@kali)-[~/forensics/exp6]
$ icat test_image.img 14 > report_recovered.txt
cat report_recovered.txt

Confidential report inside docs folder.
```

Step 8 — Create a Timeline & Report Generation

```
(kali@kali)-[~/forensics/exp6]
$ fls -m / -r test_image.img > body.txt
mactime -b body.txt > timeline.txt
cat timeline.txt | head -n 10

Old package separator "" deprecated at /usr/bin/mactime line 154.
Old package separator "" deprecated at /usr/bin/mactime line 167.
Tue Oct 21 2025 11:33:11      12288 macb d/drwx----- 0      0      11
  /lost+found
Tue Oct 21 2025 11:33:28      31 macb r/rrw-r--r-- 0      0      13
  /file1.txt
      40 macb r/rrw-r--r-- 0      0      14
  /docs/report.txt
      1024 macb d/drwxr-xr-x 0      0      1833
  /docs

(kali@kali)-[~/forensics/exp6]
$ tar -czvf sleuthkit_results.tar.gz filesystem_info.txt file_list.txt meta
data_info.txt timeline.txt

filesystem_info.txt
file_list.txt
metadata_info.txt
timeline.txt
```

Result

Successfully analyzed a disk image using **The Sleuth Kit** tools and extracted file metadata, recovered deleted files, and created a forensic timeline.

