Ex No . 06- 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.

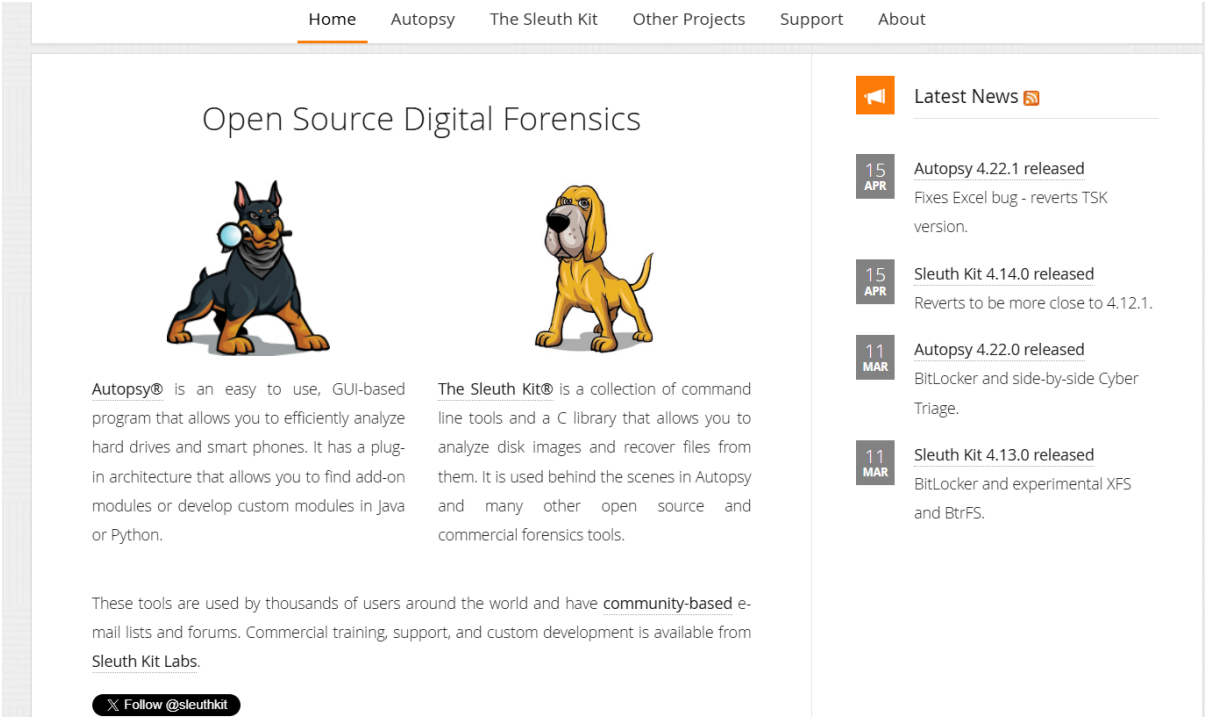
PROCEDURE:

Sleuth Kit is used to analyze disk images and recover digital evidence. It allows examination of file systems, listing of files and partitions, recovery of deleted files, and extraction of metadata. Optimal time line analysis help track file activity, and all findinds can be complicated into a report for secure storage.

Step 1: Install Sleuth Kit

Download Sleuth Kit:

Visit the official Sleuth Kit website or Google Drive link



Download the latest version for Window

Install Sleuth Kit:

Run the installer and follow the instructions to install Sleuth Kit on your Windows mach

Step 2: Acquire the Disk Image

Before analysis, you need a disk image of the evidence. This can be an image of a hard drive, memory card, or any other storage device

Create Disk Image:

Use a tool like FTK Imager or dd to create a bit-by-bit copy of the storage devic

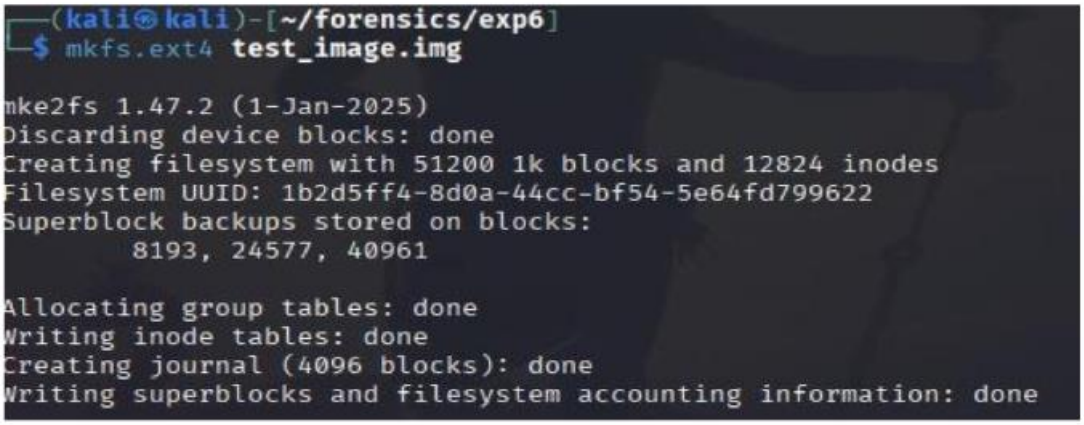
Ensure the image is in a format supported by Sleuth Kit, such as .dd, .raw, .img, or .E01

Download the required files from Google Drive:

4Dell Latitude CPi.E01

4Dell Latitude CPi.E02

-



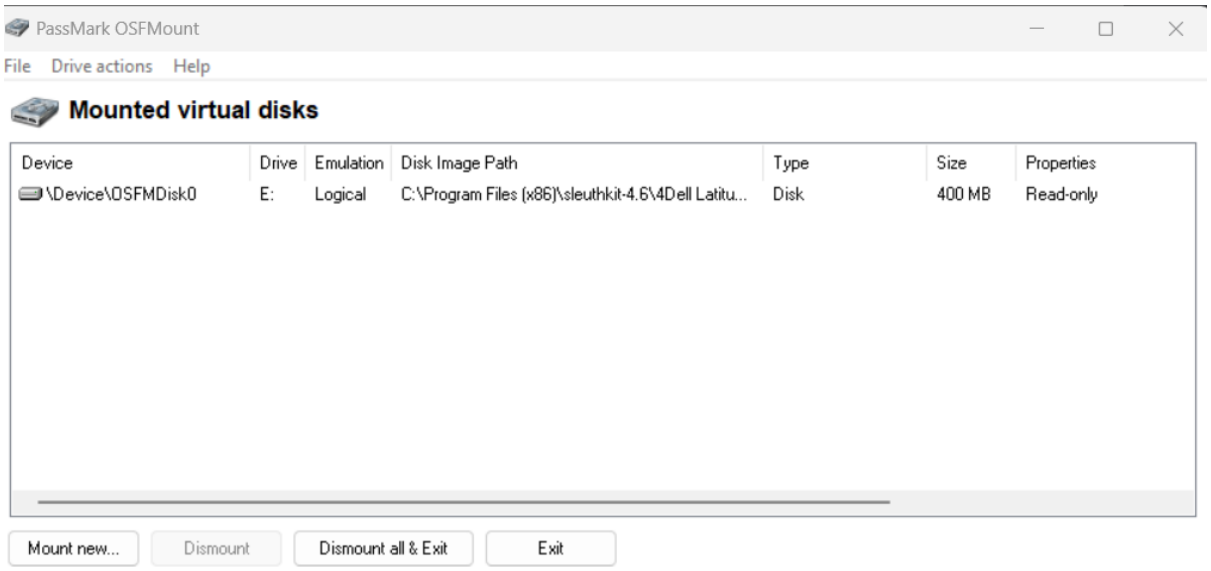
Step 3: Mount the Disk Image (Optional)

Mounting the disk image makes it easier to analyze the file system

Mount the Image:

Use a tool like OSFMount to mount the image as a virtual drive on your Windows system

This step is optional but helps with navigating the file system easily



Step 4: Analyze the File System

Use Sleuth Kit tools to analyze the file system and locate evidence.

Navigate to the Sleuth Kit Directory:

Open Command Prompt and navigate to the directory where Sleuth Kit is installed

Identify File System Type with fsstat:

bash

fsstat "4Dell Latitude CPi.E01" > filesystem_info.txt

This command outputs information about the file system, which is crucial for understanding the structure of the disk.

```
C:\Users\sesi varma>fsstat
Missing image name
usage: fsstat [-tvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o imgof
fset] image
        -t: display type only
        -i imgtype: The format of the image file (use '-i list' for supporte
d types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: File system type (use '-f list' for supported types)
        -o imgoffset: The offset of the file system in the image (in sectors
)
        -P pooltype: Pool container type (use '-P list' for supported types)
        -B pool_volume_block: Starting block (for pool volumes only)
        -v: verbose output to stderr
        -V: Print version
        -k password: Decryption password for encrypted volumes

C:\Users\sesi varma>-
```

List Partitions with mmls:

bash

mmls "4Dell Latitude CPi.E01" > partitions.txt

This command lists the partitions within the image file.

Analyze File System with fls:

bash

fls -r "4Dell Latitude CPi.E01" > file_list.txt

This command recursively lists files and directories in the file system, showing their metadata.

Recover Deleted Files with icat:

bash

icat "4Dell Latitude CPi.E01" [inode number] > [output file]

Replace [inode number] with the inode of the file you want to recover, which you can find from the fls output.

```
C:\Users\sesi varma>icat [hard disk][inode number]
Invalid inode address: number]
usage: icat [-hrRsvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o imgo
ffset] image [images] inum[-typ[-id]]
        -h: Do not display holes in sparse files
        -r: Recover deleted file
        -R: Recover deleted file and suppress recovery errors
        -s: Display slack space at end of file
        -i imgtype: The format of the image file (use '-i list' for supporte
d types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: File system type (use '-f list' for supported types)
        -o imgoffset: The offset of the file system in the image (in sectors
)
        -P pooltype: Pool container type (use '-P list' for supported types)
        -B pool_volume_block: Starting block (for pool volumes only)
        -S snap_id: Snapshot ID (for APFS only)
        -v: verbose to stderr
        -V: Print version
        -k password: Decryption password for encrypted volumes
```

Step 5: Analyze Metadata

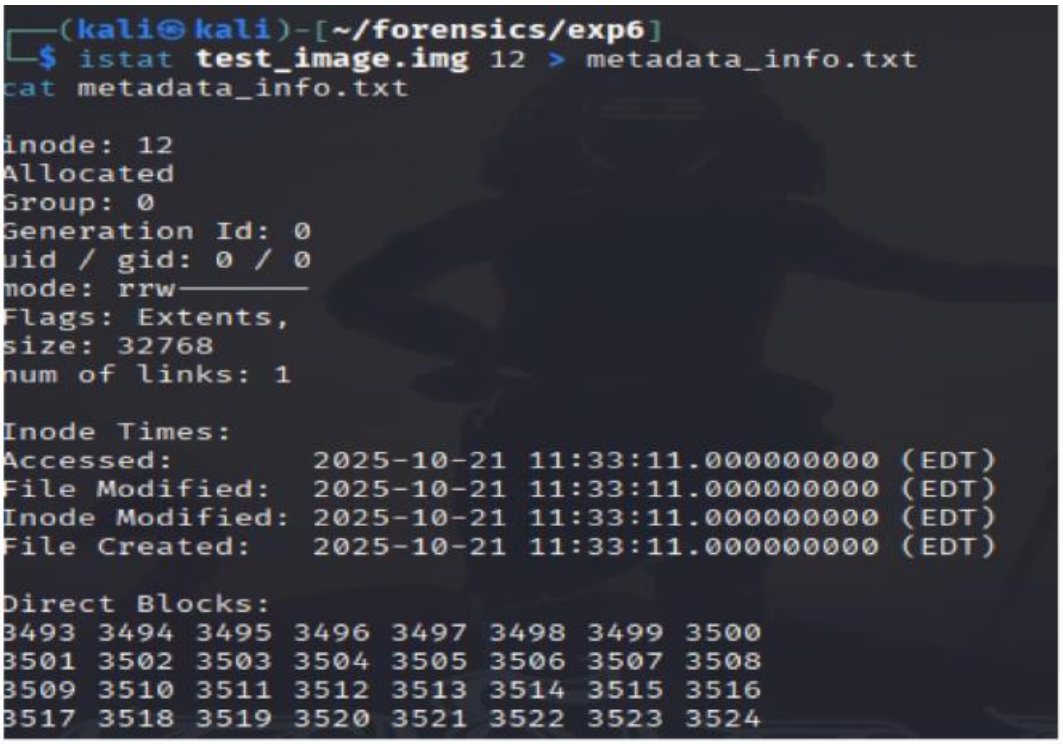
Extract metadata from files to understand more about the file's history.

View Metadata with istat:

bash

istat "4Dell Latitude CPi.E01" [inode number] > metadata_info.txt

This provides detailed information about a file, including timestamps, size, and allocation status.



Step 6: Timeline Analysis (Optional)

Creating a timeline of file activity can be crucial in an investigation.

Create Timeline with mactime:

Generate a body file using fls:

bash

fls -m / -r "4Dell Latitude CPi.E01" > body.txt

Then create the timeline:

```
C:\Users\sesi varma>fls -r[hard disk]
Invalid argument: disk]
usage: fls [-adDFlhpruvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-m
dir/] [-o imgoffset] [-z ZONE] [-s seconds] image [images] [inode]
        If [inode] is not given, the root directory is used
        -a: Display "." and ".." entries
        -d: Display deleted entries only
        -D: Display only directories
        -F: Display only files
        -l: Display long version (like ls -l)
        -i imgtype: Format of image file (use '-i list' for supported types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: File system type (use '-f list' for supported types)
        -m: Display output in mactime input format with
              dir/ as the actual mount point of the image
        -h: Include MD5 checksum hash in mactime output
        -o imgoffset: Offset into image file (in sectors)
        -P pooltype: Pool container type (use '-P list' for supported types)
        -B pool_volume_block: Starting block (for pool volumes only)
        -S snap_id: Snapshot ID (for APFS only)
        -p: Display full path for each file
        -r: Recurse on directory entries
        -u: Display undeleted entries only
        -v: verbose output to stderr
        -V: Print version
        -z: Time zone of original machine (i.e. EST5EDT or GMT) (only useful
 with -l)
        -s seconds: Time skew of original machine (in seconds) (only useful
with -l & -m)
        -k password: Decryption password for encrypted volumes
```

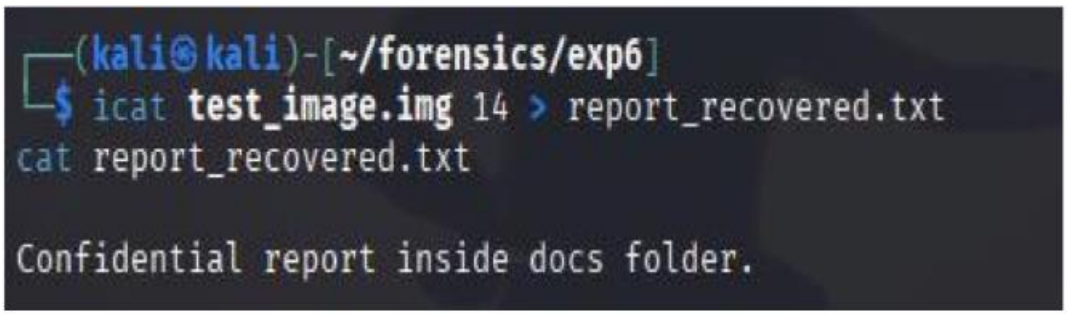
bash

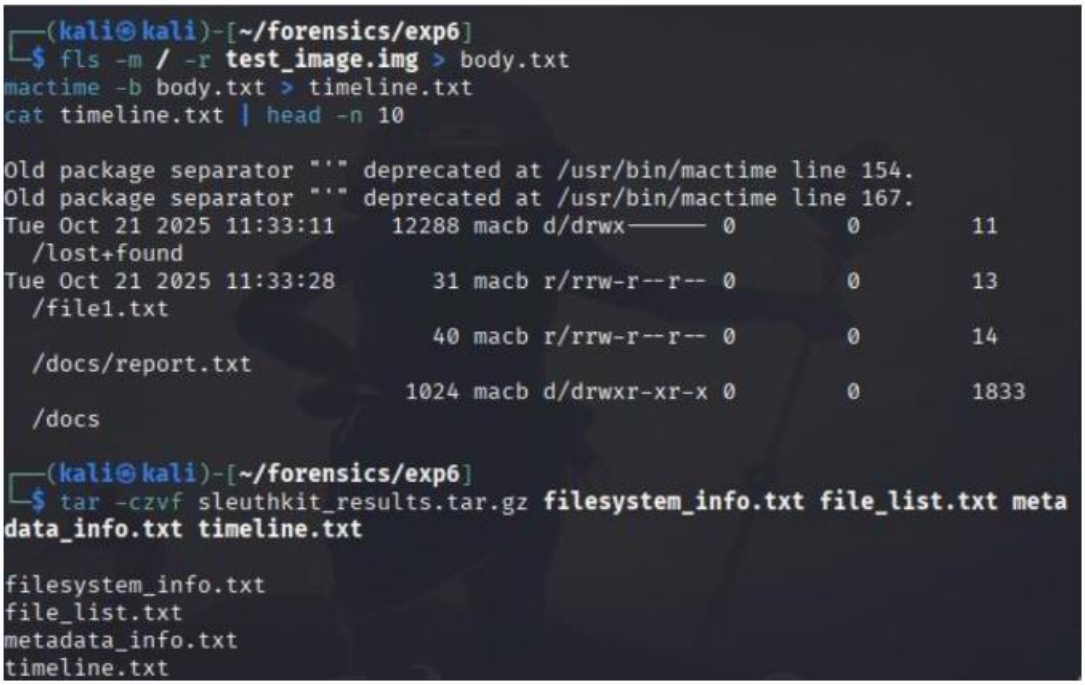
mactime -b body.txt > timeline.txt

The timeline includes MAC (Modified, Accessed, Changed) times of files.

Result:

By following these steps, you can use Sleuth Kit on a Windows machine to effectively analyze digital evidence and extract crucial information for your investigation.




┌──(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