Ex. No 6: Use Sleuth Kit to Analyze Digital Evidence

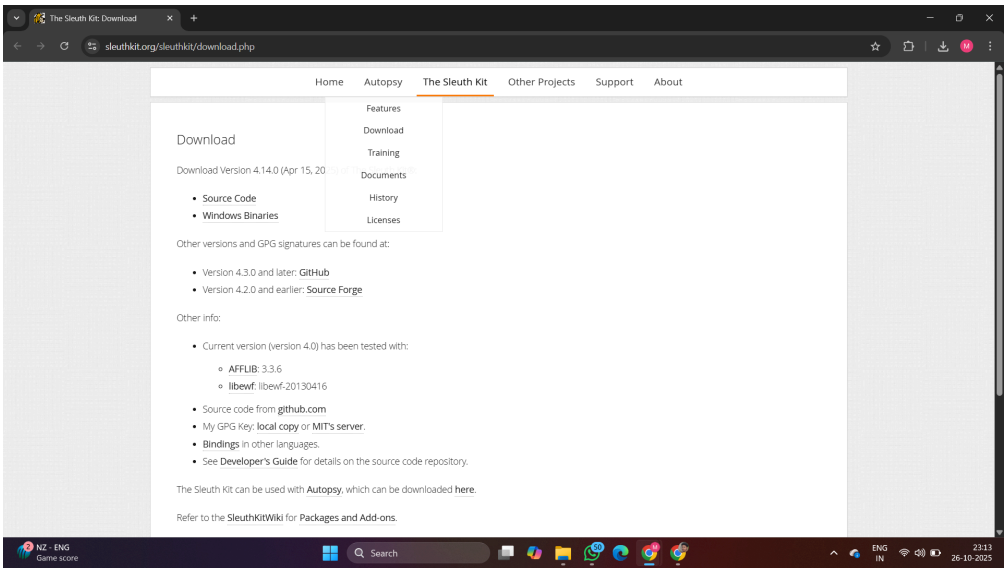
Aim

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

Steps

Step 1: Installation

- Download and install **The Sleuth Kit (TSK)** for Windows from its official website.
- Follow on-screen installation instructions.



Step 2: Acquire the Disk Image

- Create or obtain a forensic disk image using tools like **FTK Imager** or **dd**.
- Supported formats: `.dd` , `.raw` , `.img` , `.E01`
- Example evidence files:
  - `4Dell Latitude CPi.E01`
  - `4Dell Latitude CPi.E02`

Step 3: (Optional) Mount the Disk Image

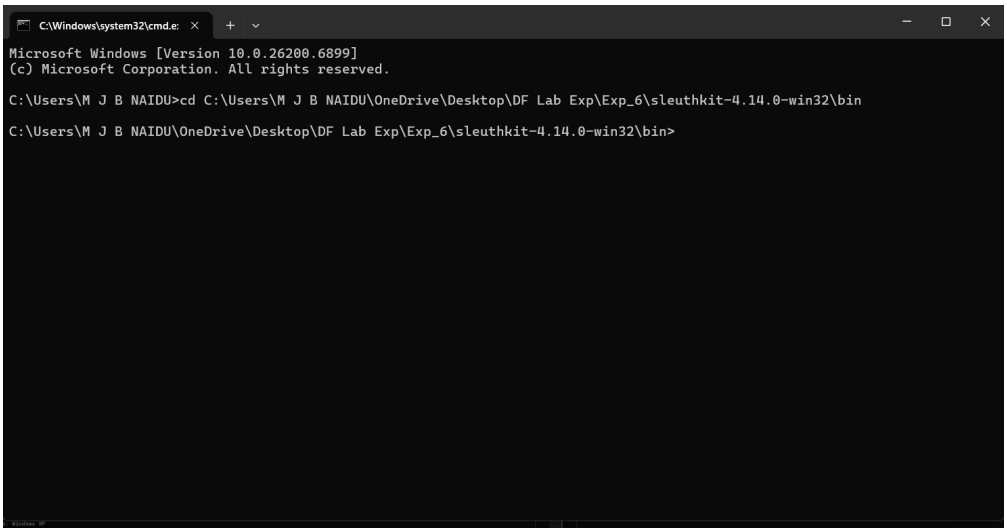
- Use **OSFMount** to mount the `.E01` or `.dd` image as a virtual drive.
- This helps in manually browsing the contents if needed.

Step 4: Analyze the File System

Navigate to Sleuth Kit:

Run:

```
cd C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-
```

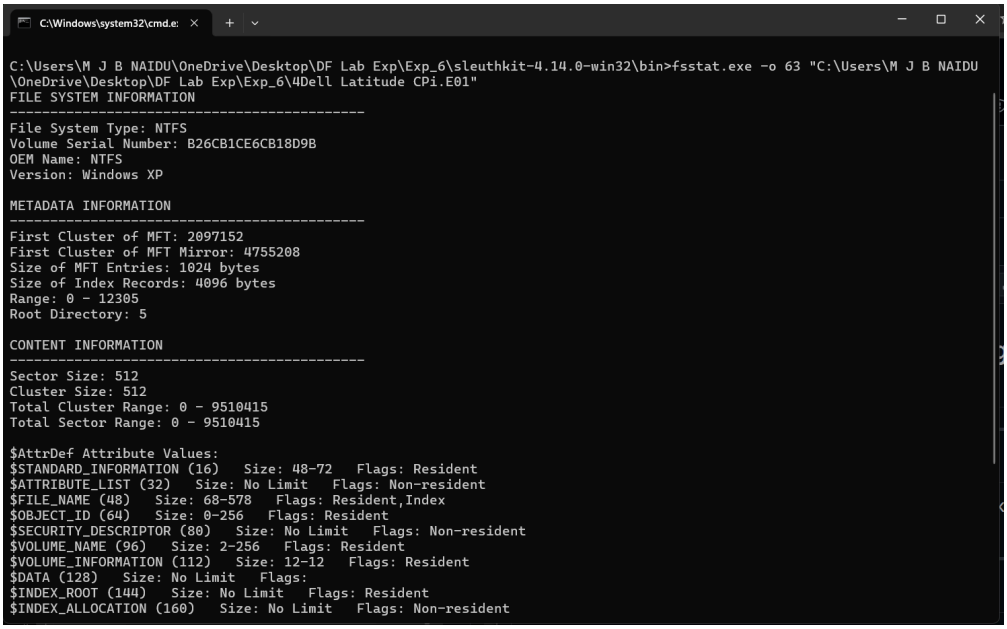


Identify File System Type:

Run:

```
fsstat.exe -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4D
```

This command gives details about the file system type, layout, and structure.

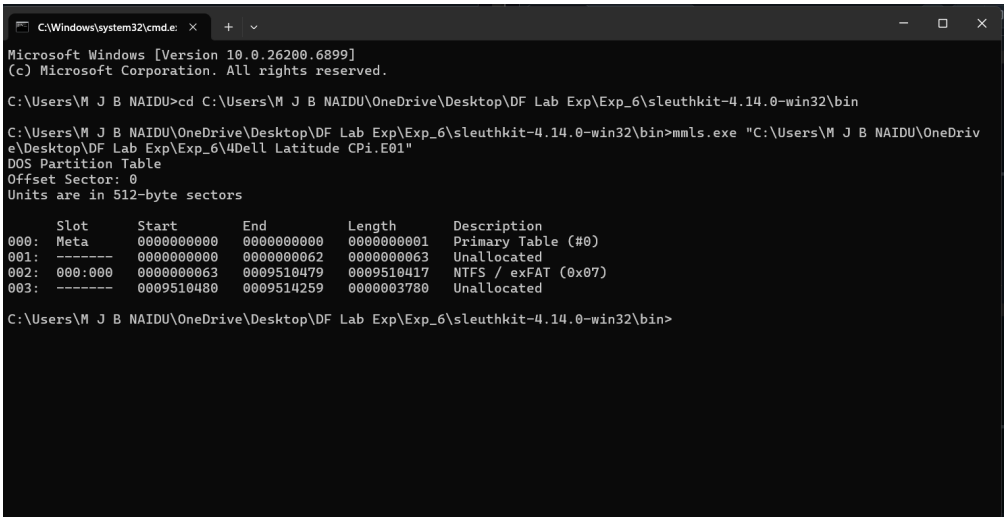


List Partitions:

Run:

```
mmls.exe "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4Dell Lati
```

This lists all partitions present in the disk image.

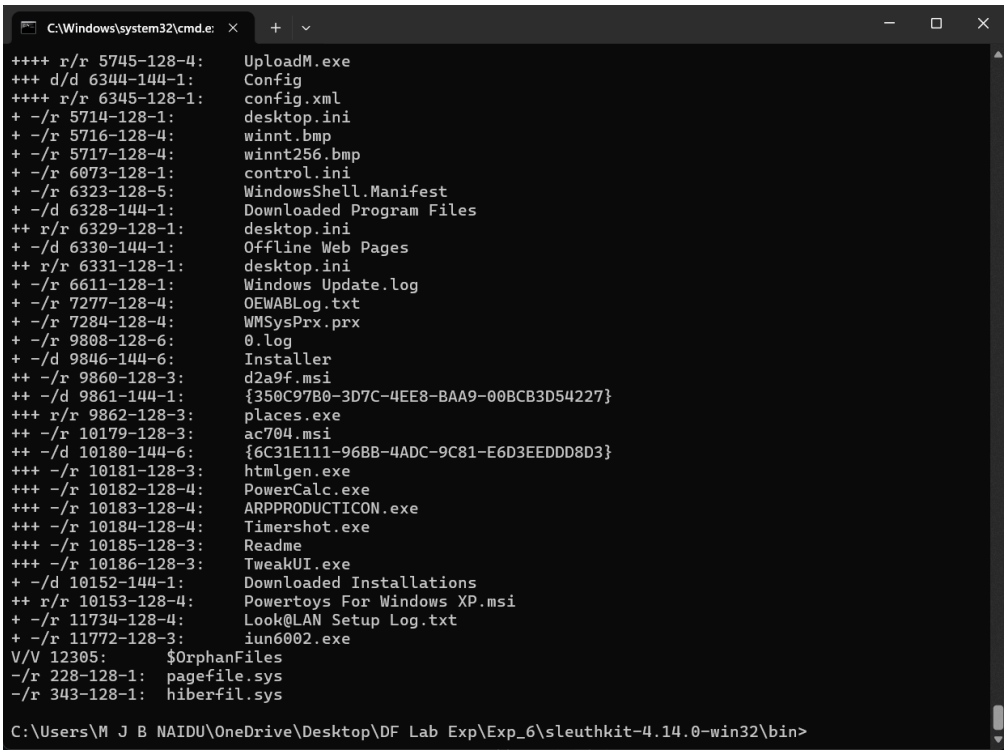


List Files and Directories

Run:

```
fls.exe -r -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4D
```

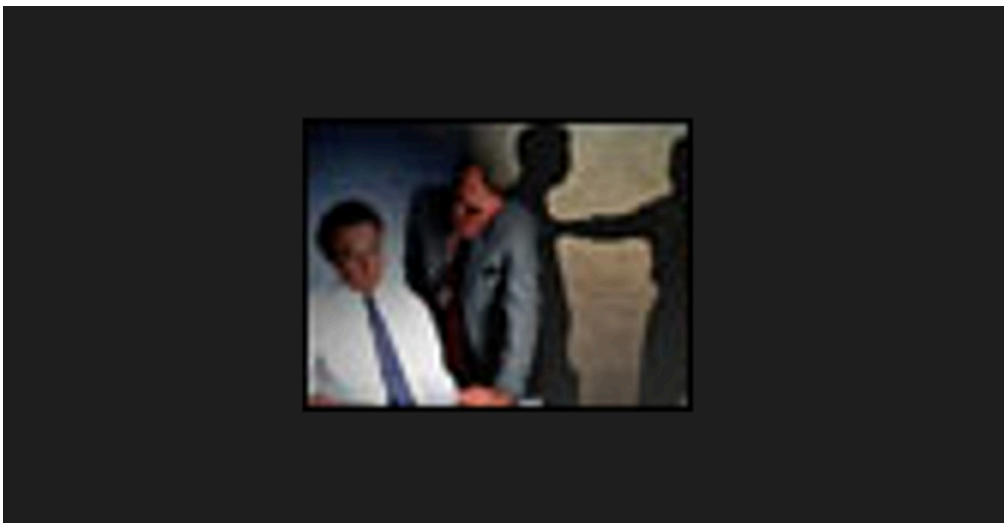
This recursively lists all files and directories, including deleted ones.



Recover Deleted Files

Run:

```
icat.exe -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4Del
```



Step 5: Analyze Metadata

Use the `istat` command to extract metadata of a specific file:

```
istat.exe -o 63  "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4D
```

This provides information such as:

- File creation, modification, and access timestamps
- File size and allocation status

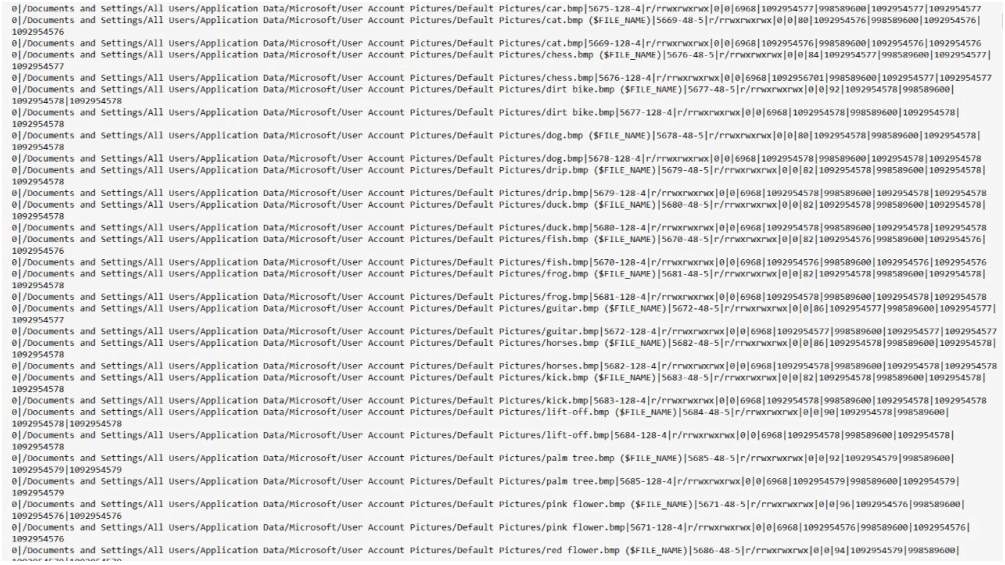
```
MFT Entry Header Values:
Entry: 11366        Sequence: 1
$LogFile Sequence Number: 31327279
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 295  (S-1-5-21-2000478354-688789844-1708537768-1003)
Created:        2004-08-21 00:35:21.487568000 (India Standard Time)
File Modified:  2004-08-21 00:35:21.487568000 (India Standard Time)
MFT Modified:   2004-08-21 00:35:21.487568000 (India Standard Time)
Accessed:       2004-08-21 00:35:21.487568000 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Archive
Name: TZ_CAR~1.JPG
Parent MFT Entry: 8375  Sequence: 3
Allocated Size: 0       Actual Size: 0
Created:        2004-08-21 00:35:21.487568000 (India Standard Time)
File Modified:  2004-08-21 00:35:21.487568000 (India Standard Time)
MFT Modified:   2004-08-21 00:35:21.487568000 (India Standard Time)
Accessed:       2004-08-21 00:35:21.487568000 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Archive
Name: tz_career_boss[1].jpg
Parent MFT Entry: 8375  Sequence: 3
Allocated Size: 0       Actual Size: 0
Created:        2004-08-21 00:35:21.487568000 (India Standard Time)
File Modified:  2004-08-21 00:35:21.487568000 (India Standard Time)
MFT Modified:   2004-08-21 00:35:21.487568000 (India Standard Time)
Accessed:       2004-08-21 00:35:21.487568000 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 90
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 108
Type: $DATA (128-4)   Name: N/A   Non-Resident   size: 1644  init_size: 1644
3514379 3514380 3514381 3514382
```

Step 6: Timeline Analysis (Optional)

Generate a chronological timeline of file system activity.

1. Create a **body file**:

```
fls.exe -m / -r -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp
```



2. Generate the **timeline**:

```
mactime -b body.txt > timeline.txt
```

This file lists the **MAC (Modified, Accessed, Changed)** timestamps of all files.

Step 7: Reporting

1. Collect all analysis outputs:
    - `filesystem_info.txt`
    - `partitions.txt`
    - `file_list.txt`
    - `metadata_info.txt`
    - `timeline.txt` (if created)
2. Review and summarize findings such as:
    - File system type and structure
    - Deleted or recovered files
    - File metadata insights
    - Activity timeline (if available)

Step 8: Finalize and Store Evidence

- Archive all reports and analysis files securely.
- Maintain the **chain of custody** to ensure evidence integrity.
- Store archives in a **secure and access-controlled** environment.

Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

Successfully analyzed the given disk image using **The Sleuth Kit (TSK)**.
Extracted file system information, recovered deleted files, analyzed metadata, and generated a forensic timeline report.