

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.

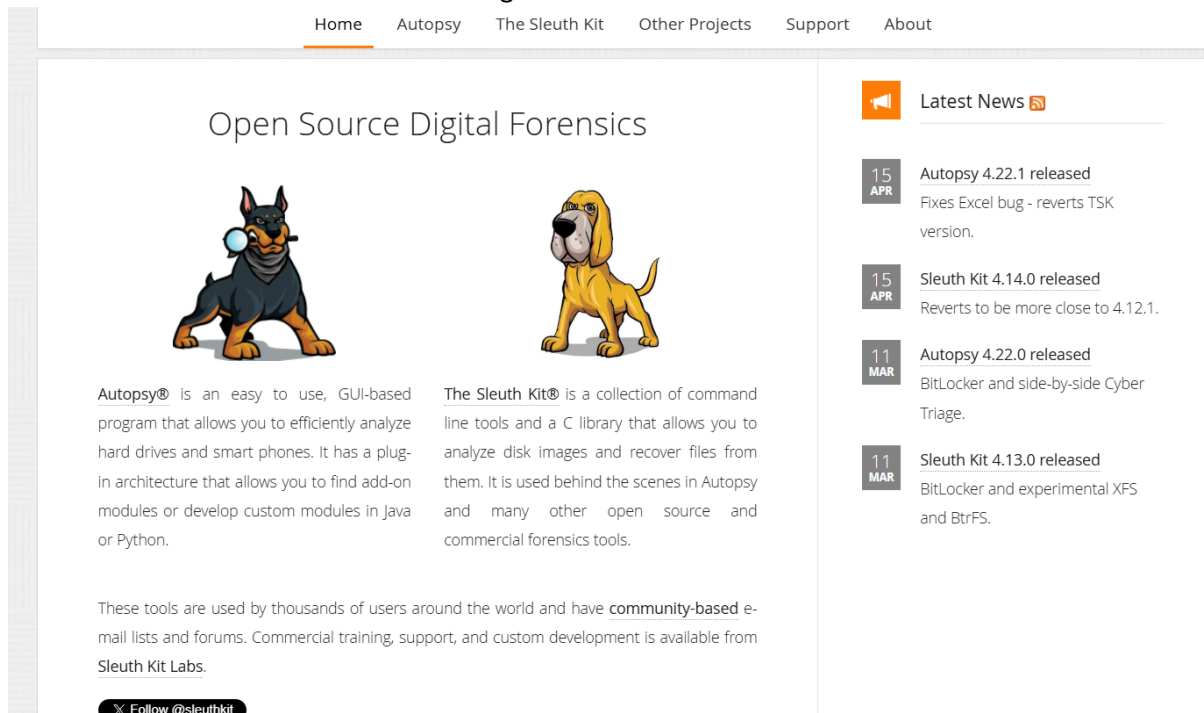
PROCEDURE:

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 findings 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




The screenshot shows the official Sleuth Kit website. The header includes navigation links: Home, Autopsy, The Sleuth Kit, Other Projects, Support, and About. The main content area is titled "Open Source Digital Forensics" and features two cartoon dogs: a black and tan Doberman Pinscher on the left and a yellow Labrador Retriever on the right. Below the Doberman is a description of Autopsy®, a GUI-based program for analyzing hard drives and smart phones. Below the Labrador is a description of The Sleuth Kit®, a collection of command line tools and a C library for analyzing disk images and recovering files. A sidebar on the right titled "Latest News" lists recent releases: Autopsy 4.22.1, Sleuth Kit 4.14.0, Autopsy 4.22.0, and Sleuth Kit 4.13.0. At the bottom left, there is a social media link to follow @sleuthkit on Twitter.

Home Autopsy The Sleuth Kit Other Projects Support About

Open Source Digital Forensics



Autopsy® is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.



The Sleuth Kit® is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

These tools are used by thousands of users around the world and have **community-based** e-mail lists and forums. Commercial training, support, and custom development is available from Sleuth Kit Labs.

Follow @sleuthkit

Latest News

- 15 APR** Autopsy 4.22.1 released
Fixes Excel bug - reverts TSK version.
- 15 APR** Sleuth Kit 4.14.0 released
Reverts to be more close to 4.12.1.
- 11 MAR** Autopsy 4.22.0 released
BitLocker and side-by-side Cyber Triage.
- 11 MAR** Sleuth Kit 4.13.0 released
BitLocker and experimental XFS and Btrfs.

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

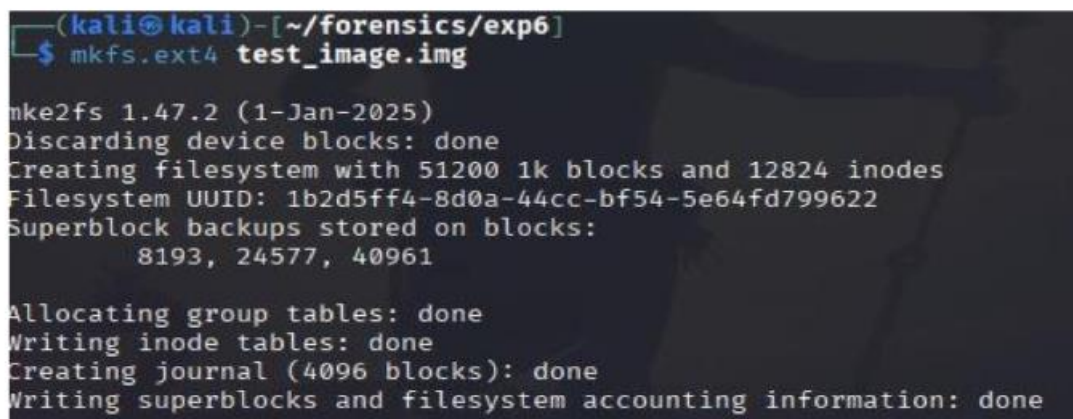
Ensure the image is in a format supported by Sleuth Kit, such as .dd, .raw, .img, or .E01

Download the required files from Google Drive:

4Dell Latitude CPi.E01

4Dell Latitude CPi.E02

-



```
(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
```

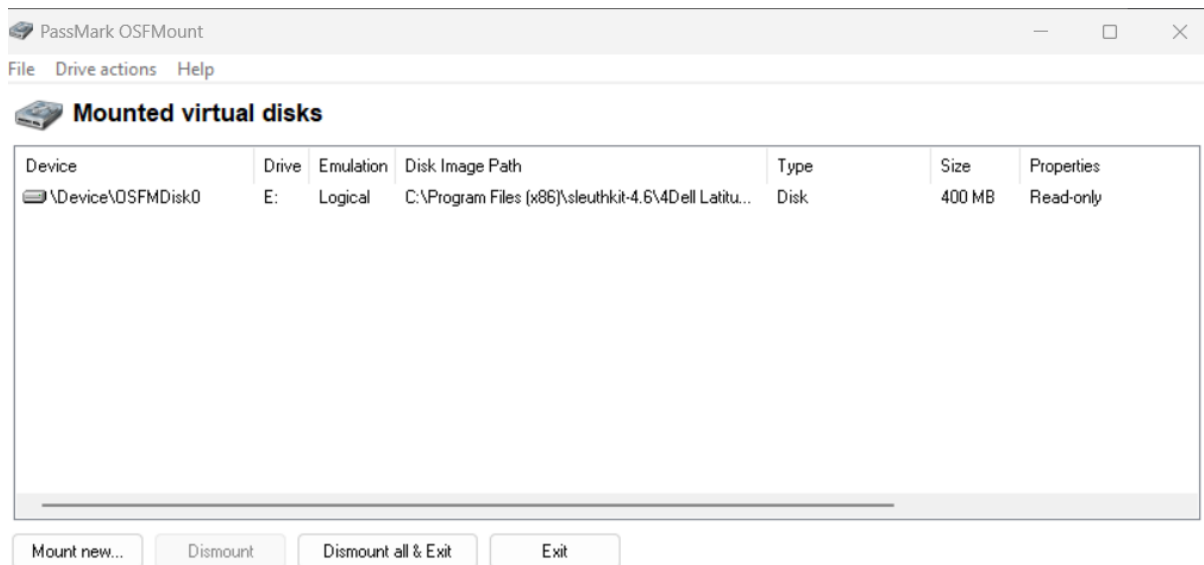
Step 3: Mount the Disk Image (Optional)

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 imgoff
fset] image
    -t: display type only
    -i imgtype: The format of the 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)
    -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 imgoffset] 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 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)
    -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.

```
(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 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]
└─$ icat test_image.img 14 > report_recovered.txt
cat report_recovered.txt

Confidential report inside docs folder.

```

```
(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
```