Ex No - 06 Use Sleuth Kit to analyze digital evidence

AIM:

To use the Sleuth Kit (TSK) tool to analyze digital evidence and extract useful forensic information such as file details, deleted files, and metadata from a disk image.

DESCRIPTION:

The Sleuth Kit (TSK) is a collection of command-line tools used for performing digital forensic analysis on disk images and file systems. It helps investigators examine file systems to recover deleted files, analyze partition layout s, and view metadata.

Each Sleuth Kit tool focuses on a specific type of analysis:

- mmls – lists partition layout of the disk image
- fsstat – displays file system details
- fls – lists files and directories in a file system
- icat – extracts file content using inode numbers
- istat – shows detailed metadata information for a file

Sleuth Kit tools are often used in conjunction with the Autopsy GUI, providing a complete forensic investigation suite.

PROCEDURE:

```
binaya@LAPTOP-F1KG4QN9:~$ mmls disk.dd
Error stat(ing) image file (raw_open: image "disk.dd" - No such file or directory)
binaya@LAPTOP-F1KG4QN9:~$ # make a 100MB empty file (raw image)
dd if=/dev/zero of=testdisk.dd bs=1M count=100 status=progress

# format it as ext4
mkfs.ext4 -F testdisk.dd
# -F forces mkfs on a regular file
100+0 records in
100+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 0.11926 s, 879 MB/s
mke2fs 1.47.0 (5-Feb-2023)
Discarding device blocks: done
Creating filesystem with 25600 4k blocks and 25600 inodes

Allocating group tables: done
Writing inode tables: done
Creating journal (1024 blocks): done
Writing superblocks and filesystem accounting information: done
```

```
binaya@LAPTOP-F1KG4QN9:~$ sudo apt update
sudo apt install sleuthkit
[sudo] password for binaya:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1260 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1541 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [208 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.5 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [8984 B]
Get:10 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [292 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [904 kB]
Get:12 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [15.4 kB]
Get:14 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1496 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [202 kB]
Get:16 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.2 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [19.3 kB]
Get:18 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [301 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [2069 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [468 kB]
Get:21 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:22 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [500 B]
Get:23 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [27.4 kB]
Get:24 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [377 kB]
Get:25 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [5708 B]
Get:26 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:27 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [31.3 kB]
Get:28 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [384 B]
Get:29 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [2170 kB]
Get:30 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [489 kB]
Get:31 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:32 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [516 B]
Get:33 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [30.3 kB]
Get:34 http://archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [5564 B]
Get:35 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:36 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [484 B]
Get:37 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Packages [40.4 kB]
Get:38 http://archive.ubuntu.com/ubuntu noble-backports/main Translation-en [9208 B]
Get:39 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7140 B]
Get:40 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [368 B]
```

```
binaya@LAPTOP-F1KG4QN9:~$ # attach file to a loop device
sudo losetup --find --show testdisk.dd
# note the output, e.g. /dev/loop0

# create a mount point and mount
sudo mkdir -p /mnt/testdisk
sudo mount -o loop /dev/loop0 /mnt/testdisk

# create some files
sudo bash -c 'echo "secret1" > /mnt/testdisk/file1.txt'
sudo bash -c 'echo "public info" > /mnt/testdisk/file2.txt'
sudo bash -c 'printf "private data\n" > /mnt/testdisk/confidential.txt'

# create a nested folder and add files
sudo mkdir -p /mnt/testdisk/docs
sudo bash -c 'echo "doc A" > /mnt/testdisk/docs/docA.txt'
sudo bash -c 'echo "doc B" > /mnt/testdisk/docs/docB.txt'

# remove (delete) one file to simulate deleted evidence
sudo rm /mnt/testdisk/confidential.txt
sudo rm /mnt/testdisk/docs/docB.txt

# sync and unmount
sync
sudo umount /mnt/testdisk

# detach loop device
sudo losetup -d /dev/loop0
/dev/loop0
```

```
binaya@LAPTOP-F1KG4QN9:~$ # show filesystem statistics (offset 0)
fsstat -o 0 testdisk.dd

# list root directory entries (non-recursive)
fls -o 0 testdisk.dd

# list recursively (adds inode numbers and deleted flags)
fls -r -o 0 testdisk.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext4
Volume Name:
Volume ID: f7db8674f1b26abd4445f2bdbb61b25b

Last Written at: 2025-10-27 05:28:38 (UTC)
Last Checked at: 2025-10-27 05:28:19 (UTC)

Last Mounted at: 2025-10-27 05:28:38 (UTC)
Unmounted properly
Last mounted on: /mnt/testdisk

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Extents, 64bit, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size

Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 25601
Root Directory: 2
Free Inodes: 25585
Inode Size: 256

CONTENT INFORMATION
--------------------------------------------
Block Groups Per Flex Group: 16
Block Range: 0 - 25599
Block Size: 4096
Free Blocks: 22950

BLOCK GROUP INFORMATION
--------------------------------------------
Number of Block Groups: 1
Inodes per group: 25600
Blocks per group: 32768

Group: 0:
  Block Group Flags: [INODE_ZEROED]
  Inode Range: 1 - 25600
  Block Range: 0 - 25599
```

OUTPUT:

```
binaya@LAPTOP-F1KG4QN9:~$ fsstat
Missing image name
usage: fsstat [-tvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o imgoffset] 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
```

```
binaya@LAPTOP-F1KG4QN9:~$ fls
Missing image name
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
```

```
binaya@LAPTOP-F1KG4QN9:~$ icat
Missing image name and/or address
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
```

RESULT:

Thus, the Sleuth Kit tool was successfully used to analyze digital evidence.
The experiment extracted and viewed the file system structure, file metadata, and recovered deleted files from the given disk image.