

The Sleuth Kit (TSK)

Abrar

October 09, 2024

The Sleuth Kit (TSK) is a collection of command-line tools used for digital forensics to analyze disk images and recover files and data from various file systems. It supports file systems like FAT, NTFS, EXT, HFS+, UFS, and more.

Key TSK Tools and Usage

1. mmls (Media Management List):

- **Purpose:** Lists the partition layout of a disk or disk image.
- **Usage:** `mmls <disk-image>`
- **Example:** `mmls disk.img`
- Outputs start/end sectors, partition types, and sizes.

2. fls (File List):

- **Purpose:** Lists files and directories in a file system, including deleted files.
- **Usage:** `fls [options] <image> [inode]`
- **Example:** `fls -r disk.img`
- **Options:**
 - **-r:** Recursively lists directories and files.Lists all files and directories, along with inode numbers.

3. icat (Inode Cat):

- **Purpose:** Extracts file content using its inode number.
- **Usage:** `icat <image> -o <offset> <inode>`
- **Example:** `icat disk.img -o 360448 2371`
- **Options:**
 - **-o:** Offset of the partition (where the file system starts).

4. **istat (Inode Stat):**

- **Purpose:** Displays detailed information about a specific inode, including file metadata.
- **Usage:** `istat <image> <inode>`
- **Example:** `istat disk.img 2371`
- Outputs file metadata for the inode 2371 (file size, permissions, timestamps, etc.).

5. **fsstat (File System Stat):**

- **Purpose:** Displays details about the file system (e.g., type, layout, metadata locations).
- **Usage:** `fsstat <image>`
- **Example:** `fsstat disk.img`
- Displays information like block sizes, superblock info, and file system layout.

6. **tsk_recover (File Recovery):**

- **Purpose:** Recovers all files from a partition, including deleted files.
- **Usage:** `tsk_recover <image> <output-directory>`
- **Example:** `tsk_recover disk.img /output/recovered_files/`
- Recovers files from `disk.img` to the specified directory.

7. **blkls (Block List):**

- **Purpose:** Extracts all unallocated (deleted) blocks from a file system.
- **Usage:** `blkls <image>`
- **Example:** `blkls disk.img`
- Extracts unallocated blocks from the disk image.