**Ex. No:6 Use Sleuth Kit to analyze digital evidence**

**Description**

The Sleuth Kit (TSK) is a collection of command-line tools that allow you to analyze disk images and recover digital evidence. Here's a step-by-step guide to using Sleuth Kit on a Windows machine to analyze digital evidence:

**Step 1: Install Sleuth Kit**

1. **Download Sleuth Kit**:
   * Visit the official [Sleuth Kit website](https://www.sleuthkit.org/) or <https://drive.google.com/drive/u/1/folders/1ilSFY7Tqn2L7AjQGhq8yJ8kixc_xTU-v>
   * and download the latest version for Windows.
2. **Install Sleuth Kit**:
   * Run the installer and follow the instructions to install Sleuth Kit on your Windows machine.

**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.

1. **Create Disk Image**:
   * Use a tool like FTK Imager or dd to create a bit-by-bit copy of the storage device. Ensure the image is in a format supported by Sleuth Kit, such as .dd, .raw, .img, or .E01.
   * Download the below files from the google drive
     1. 4Dell Latitude CPi.E01
     2. 4Dell Latitude CPi.E02

**Step 3: Mount the Disk Image (Optional)**

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

1. **Mount the Image**:
   * You can 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.

1. **Navigate to the Sleuth Kit Directory**:
   * Open the Command Prompt and navigate to the directory where Sleuth Kit is installed.
2. **Identify File System Type with fsstat**:
   * Run the command:

arduino

fsstat [image file] > filesystem\_info.txt

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

1. **List Partitions with mmls**:
   * Run the command:

arduino

mmls [image file] > partitions.txt

* + This command lists the partitions within the image file.

1. **Analyze File System with fls**:
   * Run the command:

arduino

fls -r [image file] > file\_list.txt

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

1. **Recover Deleted Files with icat**:
   * To extract a specific file, use icat:

css

icat [image file] [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.

**Step 5: Analyze Metadata**

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

1. **View Metadata with istat**:
   * Run the command:

css

istat [image file] [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.

1. **Create Timeline with mactime**:
   * Generate a body file using fls:

css

fls -m / -r [image file] > body.txt

* + Then create the timeline:

css

mactime -b body.txt > timeline.txt

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

**Step 7: Generate a Report**

Document your findings by compiling all the data into a comprehensive report.

1. **Compile the Data**:
   * Gather all the output files (e.g., filesystem\_info.txt, partitions.txt, file\_list.txt, metadata\_info.txt, timeline.txt).
2. **Analyze and Document**:
   * Review the findings, highlight important evidence, and write a report summarizing the investigation's results.

**Step 8: Finalize and Store Evidence**

Ensure that all evidence and reports are securely stored.

1. **Archive Evidence**:
   * Use a secure method to archive the disk image and analysis results, ensuring integrity and confidentiality.
2. **Store Securely**:
   * Store the archived data in a secure location, following the chain of custody procedures.

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.