Assignment 2:

Command-Line Forensic Investigation using The Sleuth Kit

Technical Requirements

Software Environment

- Linux distribution (Ubuntu 20.04+ recommended or Kali Linux) / Virtual Machine
- The Sleuth Kit (TSK) version 4.12 or higher

Evidence Files

- `cfreds_2015_data_leakage_rm#2.7z`
- Case documentation from NIST CFReDS project

Assignment Phases

TASK1: Sleuth Kit Environment Setup and Image Analysis

Objectives

- Install and configure The Sleuth Kit on Linux system
- Verify evidence integrity using TSK image tools
- Understand TSK tool categorization and command hierarchy

Key Tasks

1. **TSK Installation**

```
sudo apt-get update
sudo apt-get install sleuthkit


To Verify installation:
```

```
Mmls -V (capital alphabet)
V- returns the version
```

2. **Evidence Verification**

```
img_stat cfreds_2015_data_leakage_rm#2.dd
img_cat cfreds_2015_data_leakage_rm#2.dd | sha1sum
```

TASK 2: Volume and Partition Analysis

Objectives

- Analyze disk partitioning scheme using media management tools
- Understand partition layouts and identify unallocated space
- Calculate proper sector offsets for file system analysis

Commands

```
# Analyze partition structure (Analyze any partition structures like DOS,GPT,MAC)
mmls cfreds_2015_data_leakage_rm#2.dd

# Get detailed partition information (what type of partitioning scheme or volume system is used on a disk image.)
mmstat cfreds_2015_data_leakage_rm#2.dd

# Extract specific partition for analysis
mmcat cfreds_2015_data_leakage_rm#2.dd 2 > partition2.dd

# Analyze DOS partition table specifically
mmls -t dos cfreds_2015_data_leakage_rm#2.dd
```

TASK 3: File System Structure Analysis

Objectives

- Analyze FAT32 file system structure using `fsstat`

- Extract file system metadata and statistical information

Commands

```
# Basic file system analysis
fsstat -o 128 cfreds_2015_data_leakage_rm#2.dd

# Extract specific FAT32 information
fsstat -f fat32 -o 128 cfreds_2015_data_leakage_rm#2.dd | grep -E 'File
System|Cluster|Total Range|FAT [0-9]'


# Save complete analysis for documentation
fsstat -o 128 cfreds_2015_data_leakage_rm#2.dd > filesystem_analysis.txt
(the file “filesystem_analysis.txt” can be opened using the command open [File_name])
```

TASK 4: File and Directory Enumeration

Objectives

- Master file listing capabilities using `fls` command
- Identify deleted files and directories in the file system
- Construct comprehensive directory trees and file hierarchies

Comprehensive File Analysis

```
# List root directory contents
fls -o 128 cfreds_2015_data_leakage_rm#2.dd

# Recursive listing of entire file system
fls -o 128 -r cfreds_2015_data_leakage_rm#2.dd > complete_file_list.txt

# Identify deleted files (marked with *)
fls -o 128 -r cfreds_2015_data_leakage_rm#2.dd | grep '\*' > deleted_files.txt
```