CH. DEVI LAL STATE INSTITUTE
of Engineering & Technology
PANNIWALA MOTA, SIRSA

Laboratory Manual

of

Digital Forensic

(PE/CSE/89-P)

Prepared By:

Dr. Manju Devi

Assistant Professor

(Computer Science & Engg. Deptt.)

DIGITAL FORENSICS LAB MANUAL

Course Information

Course Code: : PE/CSE/89-P Course Credits: 1 Type: Professional Elective Lab. Course Contact Hours: 2 hours/week Mode: Lab practice	**Course Assessment Methods (internal: 50; external: 50)** The internal and external assessment is based on the level of participation in lab. sessions and the timely submission of lab experiments/assignments, the quality of solutions designed for the assignments, the performance in VIVA- VOCE, the quality of lab. file and ethical practices followed. The internal examination is conducted by the course coordinator. The external examination is conducted by external examiner appointed by the Controller of Examination in association with the internal examiner appointed by the Chairperson of the Department.

Pre-requisites

Basic knowledge of computer systems and operating systems like Windows, Linux, MacOS.

Course Objective

To provide practical exposure to digital forensic tools and techniques for investigating digital evidence.

Course Outcomes

CO1: Apply digital forensic tools for file system analysis.

CO2: Analyze ethical practices in investigations.

CO3: Evaluate tools for imaging and wiping drives.

CO4: Develop solutions for disk imaging problems.

CO5: Create structured lab records.

CO6: Demonstrate independent learning and problem solving.

List of Experiment

1. Extracting Recently Opened Files from Windows Registry
2. Extracting Auto-Run Programs from Windows Registry
3. Wiping a USB Drive Using dd Command in Linux
4. Imaging a Hard Drive Using FTK Imager
5. Recovering Deleted Files Using System Restore
6. Extracting and Analyzing System Restore Files
7. Timeline Analysis Using Autopsy
8. File System Analysis of Deleted and Hidden Files
9. Android Data Extraction Using CAINE
10. Network Traffic Analysis Using Wireshark

PRACTICAL 1

Title: Extracting Recently Opened Files from Windows Registry

Aim: To extract and analyze recently opened files from Windows Registry.

Tools Required: Windows OS, Registry Editor / Command Prompt

Procedure:

- Open Run → type regedit

- Navigate to RecentDocs path

- View recently opened files

Result: Recently accessed files extracted successfully.

PRACTICAL 2

Title: Extracting Auto-Run Programs from Windows Registry

Aim: To identify startup programs.

Tools Required: Windows OS

Procedure:

- Navigate to Run registry keys

- View auto-start programs

Result: Auto-run programs identified.

PRACTICAL 3

Title: Wiping a USB Drive Using dd Command

Aim: To securely wipe a USB drive.

Tools Required: Linux OS

Procedure:

- Use lsblk

- Unmount drive

- Run dd command

Result: USB wiped successfully.

PRACTICAL 4

Title: Imaging a Hard Drive Using FTK Imager

Aim: To create forensic image.

Tools Required: FTK Imager

Procedure:

- Create disk image

- Verify hash

Result: Image created successfully.

PRACTICAL 5

Title: Recovering Deleted Files Using System Restore

Aim: To recover deleted files.

Procedure:

- Use rstrui

- Select restore point

Result: Files recovered.

PRACTICAL 6

Title: Extracting and Analyzing System Restore Files

Aim: Analyze restore data.

Procedure:

- Access System Volume Information

- Use FTK Imager

Result: Files analyzed.

PRACTICAL 7

Title: Timeline Analysis Using Autopsy

Aim: Analyze activity timeline.

Procedure:

- Create case

- Add data

- View timeline

Result: Timeline generated.

PRACTICAL 8

Title: File System Analysis

Aim: Identify deleted/hidden files.

Procedure:

- Load image

- Analyze files

Result: Files recovered.

PRACTICAL 9

Title: Android Data Extraction Using CAINE

Aim: Extract Android data.

Procedure:

- Connect device

- Run adb commands

Result: Data extracted.

PRACTICAL 10

Title: Network Traffic Analysis Using Wireshark

Aim: Analyze network traffic.

Procedure:

- Capture packets

- Apply filters

Result: Traffic analyzed.