III Year II Semester CYBER CRIMES & DIGITAL FORENSICS LAB

Course Objectives:

- Investigate cybercrime and collect evidences
- Able to use knowledge of forensic tools and software
- To understand the preservation of digital evidence.
- To learn about stenography Perceptual models

Course Outcomes Table

Course Outcome (CO)	Description	Knowledge Level (K)
CO1	Identify the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrongdoing.	**K3**
CO2	Construct the file system storage mechanisms of two common desktop operating systems and forensics tools used in data analysis.	**K6**
CO3	List and implement all running processes, network connections from a memory image, and determine whether a firewall is set by analyzing a memory image.	**K4**
CO4	Define and perform live incident response on a system, view all browser history, and list all established network connections in a computer (Triage Incident Response).	**K1**

Experiment- 1

Evidence Collection

a) Linux: Capturing RAM dump using fmem https://github.com/NateBrune/fmem

- dcfldd if=/dev/fmem of=memory.dump hash=sha256 sha256log=memory.dump.sha256 bs=1MB count=1000

b) Linux: Capturing Disk using dfldd https://www.obsidianforensics.com/blog/imaging-using-dcfldd

- dcfldd if=/dev/sdb1 of=/media/disk/test_image.dd hash=md5, sha1hashlog=/media/disk/hashlog.txt

c) Windows: Capture RAM dump of a windows system a. Hint: FTK Imager or RAMCapture
d) Windows: Capture Disk Image of a windows system Hint: FTK Imager

Experiment- 2

Disk Analysis

i) List all files in a directory from a disk image

  a. FTK Imager

ii) Export a particular file from a disk image

  a. FTK Imager

iii) Recover a deleted file from a disk image

  a. FTK Imager

Experiment- 3

Memory Analysis

1. List all running processes from a memory image
2. List all network connections from a memory image
3. Find out whether a firewall is set by analyzing a memory image Hint: volatility

Experiment- 4

Live Incident Response

1. Perform live incident response on a system
2. View all browser history in a computer
3. List out all established network connections in a computer Hint: Triage Incident Response

Exercise- 5 Implement E-Mail Tracking and Email Investigation

Exercise- 6 Implement video Analytics for a live video

Exercise- 7 Analysis on different Malware Working

Exercise- 8 Work on Mail Bombs &SMS bombs

Exercise- 9 Implement a case on windows and Linux forensics

Exercise- 10 Implement a case on network Forensic

Exercise- 11 Work on different types of vulnerabilities

Exercise- 12 Implement a case on Mobile Forensics

Exercise- 13 Develop a Evidence and Preparation and Documentation