Suggested Teaching Guideline for

Cyber Forensics PG-DITISS September 2022

Duration: 20 Classroom hrs + 24 Lab hrs (Total: 44 hrs)

Objective: To introduce the student to Cyber Forensics and cyber laws.
Evaluation method: Theory exam – 40% weightage
Lab exam – 40% weightage
Internal Assessment – 20% weightage

List of Books / Other training material

Reference: Guide to Computer Forensics and Investigations
Computer Forensics and Investigations/nelson

Note: Conduct lab sessions based on case studied. Faculty can ask to students to get some case studies and choose among that for explanation.

Session 1:
Introduction

- Overview - Computer Forensics
- Difference – Computer Crime & Un-authorized activities
- Cyber Laws
- Process of Computer Forensics (six)
- Need for forensics investigator

Session 2:

- Computer Forensics Involves
    - Preservation
    - Identification
    - Extraction
    - Documentation
    - Interpretation
- Goals of Forensics Analysis
- Types of Cyber Forensics Techniques
- Cyber forensics Procedures
- Preparation
    - What to do before the incident
    - Incident response plan
    - Incident response team
- Detecting Incidents
- Chain of custody

Session 3:

- Evidence Checkout Log
- Handling Evidence
- First Response
- Formulate/Execute Response Strategy
- Forensic duplication
- Authenticate the Evidence
- Investigation
- Common Mistakes
- Detection

Lab:

- Demo and lab sessions on Evidence Checkout Log, Investigation and Detection.

Session 4:

- The Initial Assessment
- Incident Notification Checklist
- Hexadecimal notation
- Practical Bits
- Slight diversion
- What is use of Hexadecimal

Session 5:

- Encoding And Encryption
- The Hex Editor
- Files
- Hashing
- Hashing DLs
- MD5 Hash collisions
- Hash Collisions
- Bit Rot

Lab:

- Demo and lab sessions on Encoding and Ecryption.

Session 6:

- Standard Operating Procedures
- Processing Crime and Incident Scenes – Working with Windows & DOS Systems Current

Session 7:

- Forensics Implications
- Accreditation Standards
- Performing a Cyber Forensics Investigation
- Privacy and Cyber Forensics

Session 8:

- Computer Forensics Tools:
  - Sysinternals Suite
  - FTK Forensics Tool kit
  - FTK Imager
  - OSF
  - Hex

Lab:

- Demo and lab sessions on Cyber Check Suit

Session 9:

- Concept of collecting and analyzing artefacts from systems that are in the active state

Lab:

- Demo and lab sessions on Live system forensics

Session 10:

- Concept of collection and analysis of artefacts from Linux systems
- An introduction to Mobile forensics, IOT forensics and Cloud forensics

Lab:

- Demo and lab sessions on Linux Forensics