

# DIGITAL FORENSICS

|                                   |                                         |                                                          |                         |
|-----------------------------------|-----------------------------------------|----------------------------------------------------------|-------------------------|
| <b>Subject Code:</b><br>CS35326CS | <b>Subject Type:</b> DE<br>(Elective-4) | <b>Evaluation Scheme:</b><br>MSE (30), TA (20), ESE (50) | <b>L-T-P:</b> 3-0-0 (3) |
|-----------------------------------|-----------------------------------------|----------------------------------------------------------|-------------------------|

**Pre-Requisites:** Computer Networks, Operating System and Programming

**Course Objective:** To explore the depths of various digital incident domains, gain practical skills in detecting cyberattacks and incidents using commercial, open-source, and freeware tools, and develop case-oriented procedures for emerging scenarios.

**Course Outcomes:** At the end of the course, the student will be able to

| CO   | Course Outcomes                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| CO-1 | Understand the significance of digital evidences and basic digital forensics procedures for conducting the examination on different digital devices. |
| CO-2 | Understand digital forensics and incident response, data acquisition and validation, and demonstrate e-discovery tools.                              |
| CO-3 | Understand how to extract & examine logs or artifacts from electronic evidences.                                                                     |
| CO-4 | Understand investigation procedure of volatile and non-volatile memories, operating systems, file systems, and networks.                             |
| CO-5 | Devise methodologies and techniques for forensic investigation of modern digital devices.                                                            |

## Syllabus:

### Unit-1: Introduction to Digital Forensics

Introduction to Digital Forensics, Stages of Forensic: acquisition or imaging, analysis and reporting standards, Chain of custody, Domains of Digital Forensics, Forensic Imaging, IT Act 2000, IT Act Amendments, DPDP Act, Privacy Preserving Forensics, Data De-Duplication, Types of Electronic Evidences and their Artifacts.

### Unit-2: Volatile and Non-Volatile Memory Forensics

Volatile and Non-Volatile Memory Forensics, Tools and Techniques for Memory Forensics, File System Forensics Analysis: NTFS, Ext 2/3/4, FAT, APFS etc., Forensic Study of File System Metadata and Other Attributes, Secure Deletion, Slack Space, Data Recovery.

### Unit-3: Computer Forensics

Computer Forensics: Windows Forensics, Data Carving Techniques, Anti and Anti-Anti Forensics, Event Reconstruction Methods and Tools, Time Stomping, Database Forensics, Network Forensics, Approximate Matching.

### Unit-4: Emerging Technologies in Digital Forensics

Email Forensics, Mobile Forensics Tools & Techniques, DRONE Forensics, IoT Forensics, Cloud Forensics, Cryptocurrency Forensics, Role of AI in Digital Forensics, AI Forensics, Emerging Technologies in Digital Forensics.

## Learning Resources:

### Text Books:

1. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2017.
2. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, III Edition, 2016.
3. Angus McKenzie Marshall, Digital Forensics: Digital Evidence in Criminal Investigations, Wiley-Blackwell, 2018.
4. Carrier, Brian. File System Forensic Analysis. Addison-Wesley Professional, 2005.
5. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning.
6. Handbook on Securing Cyber-Physical Critical Infrastructure, Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann (Elsevier), 2012.
7. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006.
8. Warren G. Kruse II and Jay G. Heiser, Computer Forensics: Incident Response Essentials, Addison Wesley, 2002.