



# MARRI LAXMAN REDDY INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(AN AUTONOMOUS INSTITUTION)

(Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad)

Accredited by NAAC with 'A' Grade & Recognized Under Section 2(f) & 12(B) of the UGC act, 1956

## COURSE CONTENT

DIGITAL FORENSICS								
III Semester: CSE								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P		C	CIA	SEE
2535819	Foundation	3	0	0	3	40	60	100
		Contact Classes: 45			Tutorial Classes: Nil			Practical Classes: Nil
						Total Classes: 45		
Prerequisites: Cybercrime and Information Warfare, Computer Networks.								

### Course Overview:

The Digital Forensics course provides students with the knowledge and practical skills required to investigate digital crimes, collect and preserve digital evidence, analyze computer systems and network traffic, and support legal proceedings. The emphasis is on understanding forensic methodologies, legal and ethical considerations, and using forensic tools to extract and interpret evidence from digital devices and environments.

### Course Objectives:

1. To understand the fundamentals of digital forensics and cybercrime investigation.
2. To learn techniques for collection, preservation, and analysis of digital evidence.
3. To study forensic tools and procedures for computer, network, and mobile investigations.
4. To analyze legal, ethical, and procedural aspects of digital forensic investigations.
5. To develop skills in cybercrime detection, evidence management, and forensic reporting.

### Course Outcomes: After Completion of the Course, Students should be able to

1. Apply the principles of forensic science, computer forensics, and digital forensics to cybercrimes using a holistic investigative approach.
2. Demonstrate procedures for cyber-crime scene analysis, including search, seizure, and handling of electronic evidence in compliance with legal requirements.
3. Analyze evidence management and presentation techniques and law enforcement procedures for effective investigation.
4. Examine methodologies for conducting computer and network forensic investigations using forensic workstations, open-source tools, and case study evaluation.
5. Evaluate mobile forensic techniques, legal aspects of digital forensics and recent trends to recommend responsible and lawful practices in investigations.

**UNIT - I: Digital Forensics Science:** Forensics science, computer forensics, and digital forensics.

**Computer Crime:** Criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, holistic approach to cyber-forensics.

### UNIT - II

#### Cyber Crime Scene Analysis:

Discuss the various court orders etc., methods to search and seizure electronic evidence,

retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

### **UNIT - III**

#### **Evidence Management & Presentation:**

Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, explain what the normal case would look like, define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

### **UNIT - IV**

**Computer Forensics:** Prepare a case, begin an investigation, understand computer forensics workstations and software, conduct an investigation, complete a case, Critique a case, **Network Forensics:** open-source security tools for network forensic analysis, requirements for preservation of network data.

### **UNIT - V**

**Mobile Forensics:** mobile forensics techniques, mobile forensics tools.

**Legal Aspects of Digital Forensics:** IT Act 2000, amendment of IT Act 2008.

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

### **TEXT BOOKS:**

1. John Sammons, The Basics of Digital Forensics, Elsevier.
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications.

### **REFERENCE BOOKS:**

1. William Oettinger, Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing; 1st edition (30 April 2020), ISBN.
2. Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge.

### **ELECTRONIC RESOURCES:**

1. <https://www.coursera.org/learn/digital-forensics-essentials-dfe>
2. <https://academy.cyber5w.com/courses/C5W-100>
3. <https://alison.com/course/introduction-to-digital-forensics>
4. <https://alison.com/course/digital-forensics-examiner>

### **MATERIALS ONLINE:**

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)