



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		
2235831	Foundation	L	T	P	C	CIA	SEE	Total
		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 fundamental concepts, principles, and importance of digital forensics in cybercrime investigation.
2. To study forensic investigation procedures, evidence collection, preservation, and analysis techniques for digital systems.
3. To learn methods for investigating computer systems, networks, emails, web activities, and mobile devices.
4. To analyze legal and ethical aspects related to digital evidence, cyber laws, and forensic procedures.
5. To develop the ability to use digital forensic tools and techniques for detecting, investigating, and preventing cybercrimes.

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

1. Differentiate various types of cybercrimes in relevant to the forensic science, computer forensics, and digital forensics.
2. Analyze cyber criminalistic processes and adopt a holistic approach to investigate digital crimes, including criminal behavior and cyber-attack patterns.
3. Apply evidence collection, management, and presentation techniques in compliance with legal standards, including court orders, probable cause, and IT Act provisions.
4. Design computer and network forensic investigations using forensic workstations, software tools, and open-source network analysis tools to preserve digital evidence.
5. Demonstrate mobile forensics techniques, tools, and emerging trends, and implement search and seizure procedures for electronic evidence on mobile devices.

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)