INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

CYBER CRIME INVESTIGATION & DIGITAL FORENSICS								
VII Semester: CSE (CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACCD20	Core	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: There are no prerequisites to take this course								

I. COURSE OVERVIEW:
Cyber Crime Investigation & Digital Forensics focuses on understanding cyber threats, investigating digital crimes, and applying forensic techniques to extract, analyze, and preserve digital evidence. The course covers legal frameworks, forensic tools, and methodologies used in cyber investigations, ensuring compliance with industry best practices.

II. COURSE OBJECTIVES:
The students will try to learn:

I	The understanding of fundamental concepts of cybercrime and digital forensics.
II	The study of investigation techniques and forensic analysis methodologies.
III	The usage of forensic tools for evidence collection and preservation.
VI	The awareness of legal and ethical considerations in cybercrime investigations

III. COURSE OUTCOMES:
After successful completion of the course, students should be able to:

CO1	Understand cybercrime classifications and digital forensics fundamentals.
CO2	Apply forensic techniques for data recovery and evidence analysis.
CO3	Utilize forensic tools for investigating cyber incidents.
CO4	Interpret legal and regulatory aspects of digital forensics
CO5	Develop incident response strategies and forensic reports.
CO6	Implement best practices for securing digital evidence and maintaining chain of custody.

IV. COURSE CONTENT:

MODULE -I: INTRODUCTION TO CYBERCRIME AND DIGITAL FORENSICS (10)

Cybercrime types and classifications, Cyber laws and legal frameworks, Role of digital forensics in cybercrime investigation, Digital evidence and chain of custody, Computer forensics process and methodologies, Incident response and forensic readiness, Case studies on cybercrime investigations, Ethical hacking and penetration testing fundamentals, Emerging cyber threats and attack vectors.

MODULE –II: DIGITAL EVIDENCE COLLECTION AND ANALYSIS (10)

Identification and acquisition of digital evidence, Data carving and recovery techniques, File system forensics: FAT, NTFS, EXT, Memory forensics and volatile data collection, Network forensics and traffic analysis, Cloud forensics and remote investigations, Mobile device forensics and data extraction, Email forensics and fraud investigation, Case study: Digital evidence handling procedures

MODULE-III: COMPUTER AND MOBILE FORENSICS (09)

Hard disk imaging and forensic duplication, Windows, Linux, and Mac OS forensics, Malware analysis and reverse engineering, Mobile OS forensics: Android and iOS, SIM card and call log analysis, Mobile application security and forensics, Cloud-based mobile forensics, Social media and encrypted messaging investigations, Practical case study on computer and mobile forensic

MODULE-IV: NETWORK AND MALWARE FORENSICS (10)

Network packet capture and analysis, Intrusion detection and prevention techniques, Advanced persistent threats (APT) detection, Web and email server forensics, Malware detection and sandboxing techniques, Log analysis and correlation techniques, Deep web and dark web investigations, Digital evidence admissibility in court, Case study: Investigating real-world cyber incidents

MODULE-V: ADVANCED FORENSIC TECHNIQUES AND FUTURE TRENDS (09)

AI and machine learning in digital forensics, Blockchain forensics and cryptocurrency investigations, IoT forensics and smart device investigations, Big data analytics in forensic investigations, Digital rights management and anti-forensics techniques, Cyber threat intelligence and risk assessment, Virtual reality (VR) and augmented reality (AR) forensics, Ethical, legal, and policy issues in digital forensics, Future trends in cybercrime investigation

V. TEXTBOOKS:

1. Bill Nelson, "Computer Forensics and Cyber Crime Investigation," Cengage Learning, 3rd Edition, 2018.
2. Harlan Carvey, "Windows Forensics Analysis," Syngress, 4th Edition, 2018.
3. Cory Altheide, Harlan Carvey, "Digital Forensics with Open Source Tools," Syngress, 1st Edition, 2011.

VI. REFERENCE BOOKS:

1. Chris Sanders, "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems," No Starch Press, 3rd Edition, 2017.
2. Eoghan Casey, "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet," Academic Press, 3rd Edition, 2011.
3. Davide Balzarotti, "Practical Malware Analysis," No Starch Press, 1st Edition, 2012.

VII. ELECTRONIC RESOURCES:

1. https://www.nist.gov
2. https://www.sans.org/digital-forensics
3. https://nij.ojp.gov
4. https://www.coursera.org,
5. https://www.udemy.com, https://www.edx.org

VIII. MATERIAL ONLINE:

1. Course template
2. Tech-talk topics
3. Assignments
4. Definition and terminology

5. Tutorial question bank
6. Model question paper – I
7. Model question paper – II
8. Lecture notes
9. Early lecture readiness videos (ELRV)
10. Power point presentations