INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

CYBER CRIME AND DIGITAL FORENSICS								
VII Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
ACSD49	**Elective**	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		3	-	-	3	40	60	100
Contact Classes:48	**Total Tutorials: Nil**	**Total Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: Network Security								

I.COURSE OVERVIEW:

Cyber forensics, also known as digital forensics, involves the collection, analysis, and preservation of digital evidence to investigate cybercrimes. This course provides an in-depth understanding of forensic methodologies, tools, and legal aspects related to digital investigations.

II.COURSE OBJECTIVES:

The students will try to learn:

I. A brief explanation of the objective is to provide digital evidences which are obtained from digital media.

II. In order to understand the objectives of computer forensics, first of all, people have to recognize the different roles computer plays in a certain crime.

III. According to a snippet from the United States Security Service, the functions computer has in different kinds of crimes.

III.COURSE OUTCOMES:

After successful completion of the course, students will be able to:

CO1 Understand the principles and procedures of cyber forensics and digital evidence handling.

CO2 Identify and analyze various types of cybercrimes and forensic techniques.

CO3 Apply forensic tools and methods to acquire and examine digital evidence.

CO4 Demonstrate knowledge of legal, ethical, and professional issues in cyber forensics.

CO5 Perform forensic investigations on computer systems, networks, and mobile devices.

CO6 Prepare forensic reports and present findings in accordance with legal standards.

IV.COURSE CONTENT:

MODULE-I:

Introduction of Cybercrime: Types, The Internet spawn's crime, Worms versus viruses, Computers' roles in crimes, Introduction to digital forensics, Introduction to Incident - Incident Response Methodology — Steps - Activities in Initial Response, Phase after detection of an incident

MODULE-II:

Initial Response and forensic duplication, Initial Response & Volatile Data Collection from Windows system -Initial Response & Volatile Data Collection from Unix system — Forensic Duplication: Forensic duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic. Duplicate/Qualified Forensic Duplicate of a Hard Drive

MODULE-III:

Forensics analysis and validation: Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, performing remote acquisitions

Network Forensics: Network forensics overview, performing live acquisitions, developing standard procedures for network forensics, using network tools, examining the honeynet project.

MODULE-IV:

Current Forensic tools: evaluating computer forensic tool needs, computer forensics software tools, computer forensics hardware tools, validating and testing forensics software E-Mail Investigations: Exploring the role of e-mail in investigation, exploring the roles of the client and server in e-mail, investigating e-mail crimes and violations, understanding e-mail servers, using specialized e-mail forensic tools. Cell phone and mobile device forensics: Understanding mobile device forensics, understanding acquisition procedures for cell phones and mobile devices.

MODULE-V:

Working with Windows and DOS Systems: understanding file systems, exploring Microsoft File Structures, Examining NTFS disks, Understanding whole disk encryption, windows registry, Microsoft startup tasks, MS-DOS startup tasks, virtual machines.

V. TEXT BOOKS:

1. Kevin Mandia, Chris Prosise, "*Incident Response and computer forensics*", Tata McGraw Hill, 2006.
2. John R. Vacca*, "Computer Forensics, Computer Crime Investigation"*, Firewall Media, New Delhi,2005
3. Nelson, Phillips Enfinger, "*Computer Forensics and Investigations*", CENGAGE Learning,2007.

VI. REFERENCE BOOKS:

1. Real Digital Forensics by Keith J. Jones, Richard Bejtiich, Curtis W. Rose, Addison- Wesley Pearson Education
2. Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brian Jenkinson, Springer International

VII. WEB REFERENCES:

1. https://slideplayer.com/slide/5158896/
2. www.scs.carleton.ca/~c_shu/Courses/comp4900d/notes/PPT/lect1_intro.ppt.

VIII. MATERIALS ONLINE:

1. Course outline description
2. Tutorial question bank
3. Definition and terminology
4. Open ended experiments
5. Tech-talk topics
6. Assignments
7. Model question paper - I
8. Model question paper - II
9. Lecture notes
10. Early learning readiness videos (ELRV)
11. Power point presentations