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

COURSE CONTENT

DIGITAL FORENSICS

VII Semester: CSE(CS)

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
ACCC11	Core	3	1	0	4	30	70	100
Contact Classes: 45	Tutorial Classes: 15	Practical Classes: Nil				Total Classes: 60		

Prerequisite: There are no prerequisites to take this course

I. COURSE OVERVIEW:

This course provides learners with a baseline understanding of common cyber security threats, Vulnerabilities and risks. An overview of how basic cyber attacks are constructed and applied to real systems is also included. Examples include simple Unix kernel hacks, Internet worms, and Trojan horses in software utilities. Network attacks such as distributed denial of service (DDOS) and botnet-attacks are also described and illustrated using real time examples from the past couple of decades.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The various types of cyber-attacks and cyber-crimes.
II. The threats and risks within context of the cyber security.
III. The overview of the cyber laws and concepts of cyber forensics.
IV. The defensive techniques against these attacks.

III. COURSE SYLLABUS

MODULE-I: INTRODUCTION TO DIGITAL FORENSICS (09)

Introduction: Computer Forensics Fundamentals – Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues. Types of Computer Forensics Technology – Types of Computer Forensics Systems – Vendor and Computer Forensics Services.

MODULE-II: DATA ACQUISITION AND INCIDENT RESPONSE (09)

Computer forensics evidence and capture: Data Recovery – Evidence Collection and Data Seizur E-Duplication and Preservation of Digital Evidence-Computer Image Verification and Authentication, conducting and investigations.

MODULE-III: MEMORY FORENSICS (09)

Computer forensic analysis: Discover of Electronic Evidence-Identification of Data – Reconstructing Past Events – Fighting against Macro Threats.

Information Warfare Arsenal – Tactics of the Military – Tactics of Terrorist and Rogues – Tactics of Private Companies.

MODULE-IV: INFORMATION WARFARE (09)

Information warfare: Arsenal – Surveillance Tools – Hackers and Theft of Components – Contemporary Computer Crime-Identity Theft and Identity Fraud – Organized Crime &Terrorism – Avenues Prosecution and Government Efforts – Applying the First Amendment to Computer Related Crime-The Fourth Amendment and other Legal Issues.

MODULE-V: DIGITAL FORENSIC CASES (09)

Computer forensic cases: Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence –Processing Evidence and Report Preparation – Future Issues.

IV. TEXT BOOKS:

1. John R. Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Cengage Learning, 2nd Edition, 2005. (CHAPTERS 1 – 18).
2. Marjie T Britz, “Computer Forensics and Cyber Crime: An Introduction”, Pearson Education, 2nd Edition, 2008. (CHAPTERS 3 – 13).
3. Warren G. Kruse II and Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002.

V. REFERENCE BOOKS:

1. MariE-Helen Maras, “Computer Forensics: Cybercriminals, Laws, and Evidence”, Jones & Bartlett Learning; 2nd Edition, 2014.
2. Chad Steel, “Windows Forensics”, Wiley, 1st Edition, 2006.
3. Majid Yar, “Cybercrime and Society”, SAGE Publications Ltd, Hardcover, 2nd Edition, 2013.
4. Robert M Slade, “Software Forensics: Collecting Evidence from the Scene of a Digital Crime”, Tata McGraw Hill, Paperback, 1st Edition, 2004.