COURSE CONTENT

CYBER CRIME AND COMPUTER FORENSICS

OE – I: VI Semester: ECE / EEE
OE –II: VII Semester: AERO / MECH / CIVIL

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
AITC19	Elective	3	-	-	3	30	70	100
Contact Classes: 45	Tutorial Classes: Nil	Practical Classes: Nil				Total Classes: 45		

I. COURSE OVERVIEW:

This course is designed to introduce the participant to the cybercrime prevention, detection and incident management processes, policies, procedures and cybercrime governance activities. The course is focus on cybercrime management standards, guidelines and procedures as well as the implementation and governance of these activities. In addition, it also provides the students an understanding of the new and advanced digital investigation techniques for machines, systems and networks since new technologies are opening today the door to new criminal approaches.

II.COURSE OBJECTIVES:

The students will try to learn:

I. The fundamental concepts of computer forensics and different types of forensics systems.
II. The methodologies to analyze and validate the forensics data.
III. The different tools and tactics that is associated with cyber forensics.

III. SYLLABUS:

MODULE – I: INTRODUCTION (09)

Introduction: Computer forensics fundamentals, types of computer forensics technology, types of computer forensics systems, vendor and computer forensics services.

MODULE – II: COMPUTER FORENSICS EVIDENCE AND CAPTURE (09)

Data recovery, evidence collection and data seizure, duplication and preservation of digital evidence, computer image verification and authentication.

MODULE – III: COMPUTER FORENSIC ANALYSIS (09)

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)

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: COMPUTER FORENSIC CASES (09)

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. (UNIT I – IV)
2. Marjie T Britz, "Computer Forensics and Cyber Crime: An Introduction", Pearson Education, 2nd Edition, 2008. (UNIT IV – V)

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.