		CATEGORY	L	T	P	CREDIT
22-382-0321	**CYBER FORENSICS**	**ELECTIVE**	3	1	0	4

Prerequisite: Nil

Course Outcomes: After the completion of the course the student will be able to

CO1	Explain systematic approach to computer investigations.	(Cognitive level: Understand)
CO2	Apply forensic procedure to collect and recoverdigital evidence using tools.	(Cognitive level : Apply)
CO3	Judge the validity of digital evidence beforepresenting using cryptographic hashes.	(Cognitive level : Analyze)
CO4	Create forensic duplicates for investigation using tools and commands for capturing digital evidence .	(Cognitive level : Create)
CO5	Describe steps to follow for network , email and mobile forensics.	(Cognitive level : Understand)

Mapping of Course Outcomes with Programme Outcomes - Low=1, Medium=2, High=3

	PO 1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO10**	**PO11**	**PO12**
CO1	**2**	**2**				2	2			2		
CO2	**2**	**2**	**2**	1	2	2	2			2		
CO3	**2**	**2**				2	2			2		
CO4	**2**	**2**	**2**	1	2	2	2			2		
CO5	**2**	**2**				2	2			2		

22-382-0321 CYBER FORENSICS

UNIT I (8 Hours)

Computer Forensics Fundamentals: Computer Crime, challenges with computer crime, different types of computer crime-Identity Theft, Identity fraud, Email and internet Fraud, Theft of financial data , Corporate Data Theft, Cyber extortion-Ransomware attack, Phishing, Hacking, Spoofing, Harassment, Intellectual property Theft , Ethical Hacking, Windows Hacking . Computer Forensics Fundamentals- Type of Computer Forensics Technology, Computer forensics specialist approaches - Scientific method in forensic analysis, Computer Forensics Services.

UNIT II (10 Hours)

Computer Forensics Evidence and Capture , Data Recovery-Evidence collection - archiving , artifacts , systematic collections steps, controlling contamination , reconstructing the attacks . Data Seizure - Duplication and preservation of Digital Evidence, Computer image verification and Authentication-Cryptographic Hashes. Data Acquisition. Investigating Cybercrime, Duties Support Functions and Competencies.

UNIT III (10 Hours)

Types of Evidence: The Rules of Evidence, Volatile Evidence, order of volatility- Why Collect Evidence in the first place, Collection Options Obstacles. Computer forensics and network forensics, systematic procedure for network forensics analysis. Incident - Incident Response Methodology - Steps, Activities in Initial Response Phase after detection of an incident, Creating response toolkit.

UNIT IV (9 Hours)

Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system, Forensic Duplication, Qualified Duplication, Forensic Duplicates as Admissible Evidence, Forensic Duplication using Linux commands, Creating windows Forensic Duplicate using tool, Forensic Duplicate of a Hard Disc.

UNIT V (8 Hours)

Collecting Network-Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud. Hackers Tools. Cellphone and mobile device forensics. Forensics hardware and software, Information Security Investigations, Corporate Cyber Forensics, Investigating large scale Data breach cases, Analyzing Malicious software.

Text Books/References

1. John R. Vacca, Computer Forensics: Computer Crime Scene Investigation Laxmi Publications, 2015 reprint.
2. Dr.Darren R Hayes, A Practical guide to Computer Forensics investigation, Pearson 2015.
3. Aaron Philipp, David Cowen, Chris Davis , Computer Forensics Secrets & Solutions , McGraw-Hill Osborne Media, 2006
4. Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group–2008.
5. Bill Nelson,Amelia Philips and Christopher Steuart, "Guide to computer forensics and investigations", Cengage Learning; 4th edition, 2009.
6. Dejey ,Murugan ," Cyber Forensics", OXFORD,2018.