GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

WEF Academic Year	: 2021-22
Semester	: 2
Category of the Course	: Program Core Course-III
Course Name & Code	: Digital Forensics and Investigations (4725901)

Prerequisite:

- Digital electronics fundamentals, Computer hardware and software knowledge, Internetworking concepts, Cyber laws, policies and compliances, Cyber evidence act.

Rationale:

- Digital forensic is needed when cybercrime is reported. It is a process to identify the true reasons behind cybercrime by systematic and scientifically investigation of various collected digital pieces of evidence.
- Digital forensics refers to the process of collection, acquisition, preservation, analysis, and presentation of electronic evidence (a.k.a., digital evidence) for intelligence purposes and/or use in investigations and prosecutions of various forms of crime, including cybercrime.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
L	T	PR	C	Theory		Practical		
				ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr No	Course Content	No of Hours	%
1	**UNIT-I: Digital Forensics and Its Environment** Concepts in Digital Evidence, Nature and Special Properties of Digital Evidence, Objective of the Digital Forensics, The key technical Concepts, Forensic readiness, Computer Forensic Flaws and Risks, Computer Forensic-Rules, Procedures and Legal Issues	06	10
2	**UNIT-II: Computer System Forensic and its Investigation Process** Understanding of Systems, Disks and Media, Understanding Data Acquisition and Duplication, Principles of Data Acquisition, types, tools	08	20

	and validation methods. Operating System Forensics, Documentation Process		
3	**UNIT-III: Network Forensics** Network Attacks, Network Forensic, Analysis of network traffic techniques and Investigating Traffics Logs, Investigation of Web attacks, Web attack detection tools, Router Forensics, Documentation Process	08	20
4	**UNIT-IV: Investigation E-mail Crimes** Email system basics, Email Crimes, Steps to Investigate Email, Email Forensic Tools.	06	10
5	**UNIT-V: Investigating Wireless Attacks** Basics of Wireless, Access Controls, Wireless Penetration Testing	06	15
6	**UNIT-VI: Mobile Devices/PDA Forensics** Cellular Networks, Components of PDA, PDA Forensics, Investigation Methodology and Tips, Mobile Forensics tools	06	15
7	**UNIT-VII: Current Trends in the Digital Forensics**	02	10

Textbooks/Reference Books:

1. The Basics of Digital Forensic – The primer for Getting Started in Digital Forensics by John Sammons, Elsevier – Syngress publication
2. Practical Digital Forensic by Richard Boddington – PACKT Publication – Open-source Community
3. Network Forensics – Tracking hackers through Cyberspace by Sherri Davidoff and Jonathan Ham, Pearson Publication
4. The official CHFI Study Guide for Computer Hacking Forensics Investigators published by Syngress Publishing Inc. Elsevier.

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Understand the nature and special properties of the digital evidence, Digital Forensics rules, Procedures and Legal Issues	UN
02	Acquire Digital evidence to do Computer System Forensics along with documentation procedure	AP

03	Acquire Digital evidence to do Network Forensics along with documentation procedure	AP
04	Investigate Email and Wireless Attacks	AN
05	Critiquing various Computer Systems, Network Systems, Email and Wireless System Forensic Tools	EL

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM platform
- Recently Published papers/articles in reputed journals