GUJARAT TECHNOLOGICAL UNIVERSITY

BACHELOR OF ENGINEERING SYLLABUS

BRANCH: Artificial Intelligence and Data Science

SUBJECT CODE: 3174303

Academic Year	2023-24
Semester	7th Semester
Category of the Course	Professional Elective -IV
Course Name & Code	Cyber Forensics

Prerequisite:

Basic understanding of Operating System , Networking devices.

Rationale:

Cyber forensic is required to curb the cyber crime . It is a process to identify the true reasons behind cybercrime by systematic and scientifically investigation of various collected digital pieces of evidence.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	00	03	70	30	00	00	100

Course Content:

Sr No	Couser Content	No of Hours	Mapped Course Outcome
1	Unit-I: Introduction: Definition of Computer Forensics, Introduction to Different Types of cyber crime ,Overview of IT Act 2000,Evolution of computer forensics, Stages of computer forensics process, uses of computer forensics, objectives of computer forensics and Role of forensics investigator.	6	CO1
2	Unit-II: Introduction to Computer Crime Investigation Intial Decision-Making Process, Assess the situation , Understanding of Systems, Disks and Media, Understanding Data, Principles of Data Acquisition and Duplication, types, Tools to acquire the data, Analyze the data , Chain of custody and Report the Investigation.	6	CO2

	.		
3	UNIT-III: Evidence Handling What is Digital Evidence?, Locard's Principle, Best Evidence Rule, Stages in Digital Evidence Investigation Process, The Challenges of Evidence Handling, Importance of Certificate 65B in the court, Overview of Evidence-Handling Procedures.	6	CO3
4	Unit-IV Cyber Crime Scene Analysis: Discuss various court orders in which digital evidences has impact of the court decision,Methods to Search and Seizure Electronic Evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation	6	CO4
5	Unit-V Network Forensics and Mobile Forensics Network components and their forensics importance, CERT-in incident report ing form, Forensics information from network, Log Analysis, Network Forensics Tools, Introduction to mobile forensics, challenges in mobile forensics, Evidences in mobile device, mobile forensic process, mobile forensics acquisition tools.	8	CO5
6	Unit-VI Website Attack Investingation and Email Forensics Web attacks, Types of Web Attacks, Web Attackc Forensics, Web Application Forensics Tools, Website Log Analysis process, Types of Email Services, Email Header, Email Attacks and Crimes, Privacy in Emails, Email Forensics and Email Forensics Tools.	6	CO1
7	Unit-VII Recent trends in Cyber Forensics.	2	

Reference Book:

1. The Basics of Digital**BookForensic:** – 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.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level*
1	To understand the nature of the cyber crime , IT ACT and computer forensics.	UN
2	To apply different techniques to find out the evidences in the electronic gadets.	AP
3	To analyze different methods for the cyber crime scene investigation.	AN
4	To analyze different types of network and website incidents to be report in CERT-in incident form.	AN
5	To evaluate the forensics tool and latest technology to overcum the challenges in digital forensics.	EL

Suggested Course Practical List:

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

List of Laboratory/Learning Resouces Required:

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