GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering
Level: UG
Subject Code : 3174809
Subject Name : Cybercrime Investigation and Digital Evidence Handling

w. e. f. Academic Year:	A.Y. 2025-26
Semester:	VII
Category of the Course:	OPEC-2

Prerequisite:	Understanding of digital logic, operating system concepts, Computer hardware knowledge
Rationale:	This course aims to equip students with foundational and practical knowledge in digital investigation techniques used in cybercrime cases. It emphasizes evidence acquisition, forensic processes, technical analysis, and legal considerations relevant across all engineering domains.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
1	Explain the principles of forensic science and digital investigation.	U
2	Examine digital attack patterns and infer the motives behind cybercrimes	An
3	Interpret the cyber pieces of evidence, Digital forensic process model and Assess digital evidence within the context of legal frameworks and forensic methodology.	E
4	Utilize digital tools to conduct investigations and identify relevant artifacts.	Ap
5	Evaluate digital crime scenes and the evidence gathered from digital environments.	An

**Revised Bloom's Taxonomy (RBT)*

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering
Level: UG
Subject Code : 3174809
Subject Name : Cybercrime Investigation and Digital Evidence Handling

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
2	0	2	3	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hours
1.	**Introduction to Digital Investigations: Overview of forensic science, digital evidence principles, forensic models, and Locard's exchange principle.**	**03**
2.	**Technical Foundations: Essentials of computer systems, file and memory structures, and data storage formats.**	**06**
3	**Digital Investigation Workflow**: Cybercrime scene protocols, evidence documentation, forensic imaging, live and offline forensic methods, hashing, and report writing.	**06**
4	**Operating System Artifacts**: Recovery of deleted data, analyzing hibernation and registry files, metadata inspection, system restore elements.	**06**
5.	**Legal Frameworks in Digital Forensics**: Regulations and laws influencing digital investigations, with focus on electronic discovery procedures.	**03**
6.	**Forensic Toolkits and Assurance:** Selection, validation, and operation of both software and hardware-based forensic tools.	**03**
7.	**Case Analysis and Online Evidence**: Investigation through browser activity, email headers, and social platforms	**03**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
–	**30**	**30**	**15**	**10**	**15**

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

Books:

- *The Basics of Digital Forensics* – John Sammons
- *Cybersecurity: Understanding Cybercrimes, Computer Forensics, and Legal Perspectives* – Nina Godbole & Sunit Belapure
- *Practical Digital Forensics* – Richard Boddington

Web Resources:

- Coursera Digital Forensics Courses
- Information Security Awareness – MeitY

Recommended Tools/Platforms for Practical Use:

- **Autopsy** – Forensic browser for digital analysis
- **FTK Imager** – Disk imaging and data preview
- **Volatility Framework** – Memory forensics
- **ExifTool** – Metadata extraction
- **NetworkMiner** – Passive network sniffing and packet analysis
- **X-Ways Forensics** – Disk cloning and analysis

- **Bulk Extractor** – Scan disk images for email addresses, credit card numbers
- **RedLine** – Memory and file analysis
- **The Sleuth Kit (TSK)** – File system forensic analysis
- **HashMyFiles** – File hash verification

****