GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code: 3170725
Semester –VII
Subject Name: Digital Forensics

Type of course: Open Elective

Prerequisite: Understanding of digital logic, operating system concepts, Computer hardware knowledge

Rationale: With the rapid growth of internet users over the globe, the rate of cybercrime is also increasing. Nowadays, Internet applications become an essential part of every discipline with their variety of domain-specific applications. The basic objectives to offer this course as an open elective category to aware engineering graduates of every discipline to understand cybercrimes and their Operandi to analyze the attack.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE (E)	PA (M)	ESE (V)	PA (I)	
2	0	2	3	70	30	30	20	150

Content:

Sr. No.	Content	Total Hrs
1	**Introduction:** Understanding of forensic science, digital forensic, The digital forensic process, Locard's exchange principle, Scientific models.	3
2	**Understanding of the technical concepts:** Basic computer organization, File system, Memory organization concept, Data storage concepts	6
3	**Digital Forensics Process Model:** Introduction to cybercrime scene, Documenting the scene and evidence, maintaining the chain of custody, forensic cloning of evidence, Live and dead system forensic, Hashing concepts to maintain the integrity of evidence, Report drafting.	6
4	**Computer Operating system Artifacts:** Finding deleted data, hibernating files, examining window registry, recycle bin operation, understanding of metadata, Restore points and shadow copies	6
5	**Legal aspects of digital forensics:** Understanding of legal aspects and their impact on digital forensics, Electronics discovery	3
6	**Understanding of digital Forensic tools** Quality assurance, Tool validation, Tool selection, Hardware and Software tools	3
6	**Case Study:** Understanding of Internet resources, Web browser, Email header forensic, social networking sites	3

Suggested Specification table with Marks (Theory):

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
14	**21**	**21**	**14**	**0**	**0**

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Reference Books:

1. The basics of digital Forensics (Latest Edition) – The primer for getting started in digital forensics by John Sammons – Elsevier Syngress Imprint
2. Cybersecurity – Understanding of cybercrimes, computer forensics and Legal perspectives by Nina Godbole and Sunit Belapure – Wiley India Publication
3. Practical Digital Forensics – Richard Boddington [PACKT] Publication, Open source community

Course Outcomes:

After completion of the course, students will able to

Sr. No.	CO statement	Marks
CO-1	Describe Forensic science and Digital Forensic concepts	14
CO-2	Determine various digital forensic Operandi and motive behind cyber attacks	07
CO-3	Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective.	14
CO-4	Demonstrate various forensic tools to investigate the cybercrime and to identify the digital pieces of evidence	21
CO-5	Analyze the digital evidence used to commit cyber offences.	14

List of Experiments: Practical work will be based on the above syllabus with a minimum of 10 experiments to be performed. It is suggested that the following tools/e-resources can explore during the practical sessions

- Wireshark
- COFEE Tool
- Magnet RAM Capture
- RAM Capture
- NFI Defragger
- Toolsley
- Volatility

List of e-Learning Resources:

1. https://nptel.ac.in/
2. https://www.coursera.org/
3. Ministry of Electronics and Information Technology (MeitY) – Govt of India – Information Security Project - https://www.infosecawareness.in/