# GUJARAT TECHNOLOGICAL UNIVERSITY

**Program Name: Master of Engineering**

**Level: PG**

**Branch: Cyber Security**

**Subject Code : ME02059011**

**Subject Name : Digital Forensics and Investigations Process**

| | |
|---|---|
| w. e. f. Academic Year: | 2024-25 |
| Semester: | 2 |
| Category of the Course: | PCC |

| | |
|---|---|
| **Prerequisite:** | Digital electronics fundamentals, Computer hardware and software knowledge, Internetworking concepts, Cyber laws, policies and compliances, Cyber evidence act**.** |
| **Rationale:** | • Digital forensics is needed when cybercrime is reported. It is a process to identify the true reasons behind cybercrime by systematic and scientific investigation of various collected digital pieces of evidence.<br>• 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 Outcome:**

After Completion of the Course, Student will able to:

| No | Course Outcomes | RBT Level |
|---|---|---|
| 01 | Understand the terminologies of forensic science as per the digital era. | UN |
| 02 | Apply the legal aspects of Digital Forensics with new law introduced in INDIA. | AN |
| 03 | Discover the evidence with respect to different branches of Digital Forensics. | AP |
| 04 | Analyze the cyber crime investigation methodology in controlled environment. | AP |
| 05 | Critique various cyber crime scene on various computing platforms. | EL |

**Revised Bloom's Taxonomy (RBT)*

**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) | |
| 03 | 00 | 02 | 04 | 70 | 30 | 20 | 30 | 150 |

# GUJARAT TECHNOLOGICAL UNIVERSITY

**Program Name: Master of Engineering**

**Level: PG**

**Branch: Cyber Security**

**Subject Code : ME02059011**

**Subject Name : Digital Forensics and Investigations Process**

**Course Content:**

| Unit No. | Content | No. of Hours | % of Weightage |
|---|---|---|---|
| 1. | **UNIT-I: Digital Forensics and Its Environment** Objective of the Digital Forensics, Concepts in Digital Evidence, Nature and Special Properties of Digital Evidence, Forensic readiness, Computer Forensic Flaws and Risks, Computer Forensic-Rules, Procedures and Legal Issues, Anti-Forensics Techniques. | 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 and validation methods. Operating System Forensics, Documentation Process. Bharatiya Sakshya Adhiniyam,2023, IT Act 2000. | 08 | 20 |
| 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 | 07 | 15 |
| 7 | **UNIT-VII: Current Trends in the Digital Forensics** Cyber insurance cover and compliance, AI tools for digital evidence etc. | 04 | 10 |
| | **TOTAL** | **45** | **100** |

**Suggested Specification Table with Marks (Theory):**

| Distribution of Theory Marks (in %) | | | | | |
|---|---|---|---|---|---|
| **R Level** | **U Level** | **A Level** | **N Level** | **E Level** | **C Level** |
| **10** | **20** | **20** | **20** | **20** | **10** |

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

**References/Suggested Learning Resources:**

**(a) 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.

**(b) Open source software and website:**

1. Course-related online MOOC on SWAYAM NPTEL/Coursera Platform.
2. Recently published papers/articles of reputed journals/conferences.s

**Suggested Course Practical List:**

- List of Laboratory/Learning Resources Required: The practical work will be carried out based on the content covered during the academic sessions.

**List of Laboratory/Learning Resources Required:** SANS, NIST, DFIR websites etc.

**Suggested Project List:** Creation of local network and its security projects.

* * * * * * *