GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Information Technology

Subject Code: DI04016021

Subject Name: Cyber Security and Digital Forensics

w. e. f. Academic Year:	2025-26
Semester:	4th
Category of the Course:	PCC

Prerequisite:	Students should have a basic understanding of computers and operating systems, Students should be familiar with computers, operating systems, and basic networking concepts. Basic programming skills and an understanding of system security and cryptography will help in learning cyber security and digital forensics.
Rationale:	Cyber Security and Digital Forensics are two essential disciplines in the field of information technology. Cyber Security and Digital Forensics are essential to address the critical shortage of professionals in these fields. This curriculum equips students with the knowledge and skills needed to protect sensitive data, understand the legal and ethical aspects of digital investigations, and pursue diverse career opportunities in information security and digital forensics. Furthermore, it contributes to national security by preparing professionals to defend critical digital infrastructure and fosters adaptability to emerging threats and technologies in the ever-evolving digital landscape. This curriculum ensures that graduates are not only technically proficient but also ethically responsible professionals who can play a crucial role in protecting digital assets, solving digital crimes, and contributing to the broader field of information technology and security

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	Acquire knowledge of Cyber Security concepts including Vulnerabilities, Threats and Proxy Server.	Understand
02	Explain the different types of network and system security techniques and threats.	Understand
03	Understand the different types cybercrimes and Analyze cybercrime.	Apply
04	Implement ethical hacking methodologies using Kali Linux, including vulnerability analysis.	Apply
05	Understand and Explain use of digital forensics methodologies for Cyber Crime investigation.	Understand

**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(M)	PA(I)	ESE (V)	
3	0	2	4	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hrs	% of Weightage
1.	**Fundamental of Cyber Security** 1.1. The CIA Triad 1.2. Authentication, Authorization, and Accounting (AAA) 1.3. Vulnerabilities, Threats, and Risks 1.4. Types Of Proxy Server & Need of Private Proxy 1.5. Seven Layers of Cyber Security • Functions • Security Controls / Examples	5	14
2.	**Network and System Security** 2.1.Threats and Countermeasures Concepts (Definition Only) Malware: i. Viruses, Worms, Trojan Horses, Ransomware System and Program Vulnerabilities: ii. Buffer Overflows, Privilege Escalation 2.2.Security purpose Role of OSI Model Layers • Functions • Protocols • Security Attacks/Threats 2.3.Overview & Types of Operational Technology attacks 2.4.Overview & Types of IoT Attacks	8	18
3.	**Cyber Crime** 3.1 What is Cybercrime and Classification of Cyber Criminals 3.2 Classification of cyber-crimes 3.2.1. Crimes Against Organization • Email Bombing • Logic Bomb • Web Jacking • Data diddling	10	25

	• Denial of Service/ Distributed Denial of Service 3.2.2. Crimes Against Individuals • Cyber bullying • Cyber stalking • Cyber defamation • Phishing • Cyber fraud and Cyber theft • Spyware • Email spoofing • Man in the middle attack 3.2.3. Society • Cyber pornography • Cyber terrorism • cyber spying • Social Engineering Attack • Online gambling 3.2.4. Property • Credit Card Fraud • Software Piracy • Copyright infringement • Trademarks violations 3.3 Challenges & Prevention of Cyber Crime 3.4 Cyber Law (Introduction Only) The Information Technology ACT, 2008 OFFENCES (Section 65 Section 66 Section 67)		
4.	**Ethical Hacking** 4.1. Concept of Hacking and Types of Hackers 4.2. Basics of Ethical Hacking (Vulnerability, Exploit, 0-Day) 4.3. Five Steps of Hacking • Information Gathering, • Scanning, • Gaining Access, • Maintaining Access, • Covering Tracks 4.4. Use of Penetration Testing and Security Tools in Kali Linux (Introduction Only) 4.5. Vulnerability Scanning/ Vulnerability Based Hacking • Foot printing • Scanning • Password Cracking • Brute Force Attacks • Injection Attacks • Phishing Attacks	12	25

	• Block chain Attacks 4.6. Port Scanning 4.7. Remote Administration Tool (RAT) and Protect System from RAT 4.8. What is Sniffing and Mechanism of Sniffing 4.9. Session Hijacking		
5.	**DIGITAL FORENSICS** 5.1. Introduction to Digital Forensics 5.2. Locard's Principle of Exchange in Digital Forensics 5.3. Branches of Digital Forensics (Concept with Example Only) • Disk / Memory Forensics • Network Forensics • Database Forensics • Software forensics • Email Forensics • Malware Forensics • Mobile Forensics 5.4. Phases of digital/computer forensics investigation • Identification • Preservation • Analysis • Documentation • Presentation 5.5. Methods to Preserve a Digital Evidence • Drive Imaging • Hash Values • Chain of Custody 5.6. Critical Steps in Preserving Digital Evidence 5.7. Types of Devices Examined in Digital Forensics Investigations (Concept with Example Only) • Computers and Laptops • Smart Devices • Device Memory • Network Devices and Servers • CCTV • Drones	10	18
	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
30	40	30	-	-	-

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

References/Suggested Learning Resources:

(b) Books:

Sr NO	Title	Author(s) / Editor(s)	Publisher	ISBN / Notes
1	Cybercrime and Digital Forensics: An Introduction (3rd Edition)	Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar	Routledge, UK / London (Routledge is UK/US)	ISBN-13: 978-0367360078
2	Digital Forensics	André Årnes (editor)	Wiley (Wiley-VCH)	ISBN-13: 978-1-119-26238-1
3	Guide to Computer Forensics and Investigations (7th Edition)	Bill Nelson, Amelia Phillips, Christopher Steuart	Cengage Learning (Boston / India / US)	ISBN-13: 978-0357672884
4	Handbook of Digital Forensics and Investigation	Eoghan Casey (editor)	Academic Press / Elsevier	ISBN-13: 978-0123742674
5	A Practical Guide to Digital Forensics Investigations	(various, lab / skills focus)	Pearson / uCertify labs	ISBN-13: 978-0-13-688939-7
6	Digital Forensics Explained (2nd Edition)	Greg Gogolin (editor)	CRC Press / Routledge	ISBN-13: 978-0367503437

(b) Open Source Digital Forensics & Cyber Crime Tools & Resources.

Tool Name	Category / Primary Function	Website / Project Page
The Sleuth Kit (TSK) & Autopsy	End-to-End Forensic Platform, Disk/File System Analysis	https://www.sleuthkit.org/ / https://www.autopsy.com/
Volatility Framework	Memory Forensics (RAM Analysis)	https://www.volatilityfoundation.org/
Wireshark	Network Protocol Analyzer (Network Forensics)	https://www.wireshark.org/
ExifTool	Metadata Forensics (Read/Write/Edit metadata in files)	https://exiftool.org/
Digital Forensics Framework (DFF)	Digital Forensics and Investigation Framework	https://www.digital-forensic.org/
SIFT Workstation	Linux distribution and collection of open-source forensic tools (SANS Investigative Forensic Toolkit)	https://www.sans.org/tools/sift-workstation/
Caine (Computer	Ubuntu-based Live Linux	https://www.caine-live.net/

Aided Investigative Environment)	Distribution for Digital Forensics	
PALADIN	Ubuntu-based Live Linux Distribution for Forensic Imaging and Analysis	https://sumuri.com/product/paladin-pro/ (Note: While PALADIN is a distro, it includes many open-source tools.)
Xplico	Network Forensic Analysis Tool (NFAT) to reconstruct applications' content from network traffic	http://www.xplico.org/
plaso (log2timeline)	Tool to extract timestamps from various files and aggregate them for timeline analysis	https://github.com/log2timeline/plaso
Guymager	Open-source disk imaging tool for Linux	GitHub/Project Pages (Search "Guymager forensics")
Nmap (Network Mapper)	Network discovery and security auditing	https://nmap.org/
Ghidra	Software Reverse Engineering (SRE) Framework (developed by the NSA)	https://ghidra-sre.org/
MISP (Malware Information Sharing Platform)	Threat Intelligence Platform for sharing and analyzing threat indicators	https://www.misp-project.org/

Suggested Course Practical List:

The following practical outcomes (PrOs) are the subcomponents of the COs. These PrOs need to be attained to achieve the COs.

Sr. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
1	Prepare detailed case study analysis report on the Browsers and networks for accessing the Dark Web, its relationship to the broader internet, and its role as an enabler for malicious activities.	1	2
2	Demonstrate intrusion detection system (ids) using any Open Source tool.	1	2
3	Prepare detailed case study analysis report and interpret the email header to trace the source of the email, identify security risks, and verify authenticity using email header analyzer tools.	2	2
4	Prepare a Python module to analyze the strength of a given password.	2	2
5	Prepare detailed case study analysis report on data hiding and invisible signature using Open Source Steganography tool.	2	2

6	Write the python code to Create malicious script for generating multiple folders for ethical hacking.	3	2
7	Prepare detailed study report on Open-source intelligence (OSINT) framework and perform Information gathering using Username, Email address, Domain name and IP address.	3	2
8	Prepare detailed case study analysis report on recent types of cybercrimes.	3	2
9	Prepare a Python module to extract and display hidden EXIF metadata from images.	4	2
10	Perform basic commands in Kali Linux and Port scanning using NMAP.	4	4
11	Perform web Artifact analysis using Autopsy. (https://www.sleuthkit.org/autopsy/)	5	4
12	Identification and Analysis of Software Vulnerabilities using CVE and MITRE Database Detection & Threat Mapping using the MITRE ATT&CK® Framework.	5	4
	Total		**30**

Note :- More Practical Exercises can be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.

List of Laboratory/Learning Resources Required:

Sr. No.	Laboratory/Learning Resources/Equipment Name with Broad Specifications	PrO. No.
1	Computer system with operating system: Windows 7 or higher Ver., macOS, and Kali Linux, with 4GB or higher RAM, Python versions: 2.7.X, 3.6.X	All
2	Python IDEs and Code Editors, Goolge Colab Platform, Open Source: Anaconda Navigator, Autopsy, Openstego, FTK Imager, Wireshark, Nmap,OpenSSL, and any basic forensic software	

Suggested Activities for Students:

Other than the classroom and laboratory learning, following are the suggested student related co-curricular activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

Case Studies & Reports

- Analyze real-world cyber incidents or breaches.
- Prepare short reports or presentations summarizing the causes, impact, and lessons learned.

Hands-On Lab Exercises

- Practice encryption and decryption of sample text or files.
- Explore basic network scanning and security checks in a controlled environment.
- Simulate malware detection and learn safe ways to handle suspicious files.

Interactive Quizzes & Discussions

- Weekly quizzes on key concepts like network security, ethical hacking, or cybercrime types.
- Group discussions on emerging threats and preventive measures.

Tools Familiarization

- Introduce students to free tools like Wireshark, Nmap, OpenSSL, Autopsy, and basic forensic software.
- Learn basic reporting using logs or captured data.

Mini Projects & Demonstrations

- Simulate a safe cyber-attack and show how to detect and prevent it.
- Conduct a mock forensic investigation and document findings.

Awareness Activities

- Create posters, videos, or presentations on safe internet practices.
- Organize or attend workshops and training sessions on topics like cyber security, ethical hacking, penetration testing.
- Awareness campaigns for social engineering, phishing, and password hygiene.

* * * * * * *