GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATIONS

Programme	Master of Computer Applications	Branch/Spec.	Computer Engineering
Semester	III	Version	1.0.0.0
Effective from Academic Year	2026-27	Effective for the Batch admitted in	July 2025
Course Code	P13A5DFC	Course Name	Digital Forensics and Cyber Security Tools

Teaching Scheme						Examination Scheme (Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	2	0	2	0	2	Theory	40	60	100
Hours	2	0	4	0	4	Practical	20	30	50

Objective:

To introduce students to advanced cyber security tools and technologies used in modern security operations and digital investigations.

Pre-requisites:

Basic knowledge of computer networks and cyber security concepts.

Course Outcomes:

On successful completion of the course, the students will be able to:

CO1	Explain cyber security tools, cyber law concepts, and IT Act provisions
CO2	Describe digital forensic processes and information hiding techniques
CO3	Apply steganography tools, forensic tools, and security monitoring techniques
CO4	Analyze logs, security incidents, and threat intelligence data

Theory Syllabus

Unit	Content	Hrs.
1	**Cyber Law in India – IT Act 2000** Introduction to Cyber Law, Need for cyber regulations, Information Technology Act 2000 overview, Amendments (IT Amendment Act 2008) Key Sections: Section 43 (Damage to computer system),Section 65 (Tampering with source code) ,Section 66 (Computer-related offences),Section 66C (Identity theft),Section 66D (Cheating by impersonation),Section 66F (Cyber terrorism),Section 67 (Obscene content),Digital signatures and electronic governance,Cyber crime investigation agencies in India, Legal and ethical issues in penetration testing, Cyber Law Case Studies	8
2	**Digital Forensics Fundamentals** Core Concepts: Introduction, Branches, and Locard's Principle of Exchange. Investigation Process: Evidence collection (Live vs. Dead), Write Blockers, and Chain of Custody. Forensic Analysis: Disk and Memory basics, File Systems, Windows Registry, and Log Analysis. Recovery & Tools: Data Recovery, Data Carving, and role and usage of Cyber Forensic Tools.	7
3	**Introduction Steganography and Information Hiding** Fundamentals: Concept of Information Hiding; Comparative analysis of Steganography, Cryptography, and Watermarking. Techniques & Media: Classification of Steganography (Text, Image, Audio, Video); Spatial domain (LSB method) vs. Transform domain techniques. Security & Application: Introduction to Steganalysis; Misuse of steganography in cybercrime; Applications, Case studies, and Tools.	8

4	**Security Operations and Incident Response** Incident Response Fundamentals: The Incident Response (IR) lifecycle; Industry frameworks (NIST/SANS), Security Monitoring: Importance of log monitoring, log sources, and introduction to SIEM concepts, Malware Investigation: Basics of malware types, introduction to investigation tools, and Static vs. Dynamic analysis techniques, Network Forensics: Introduction to Wireshark, packet capture fundamentals, utilizing filters, and analyzing traffic patterns, Case Studies, Application: Analysis of real-world security breach case studies.	7
Practical Content		
Practical, assignments and tutorials are based on above syllabus.		
Text Books		
1	Digital Forensics Basics- A Practical guide using Windows OS by Nihad A. Hassan	
2	Computer Incident Response and Forensics Team Management by Leighton R. Johnson III	
3	Information Hiding: Techniques for Steganography and Digital Watermarking, by Stefan Katzenbeisser and Fabien A.P. Petitcolas, Artech House	
4	Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems Chris Sanders, No Starch Press	
Reference Books		
1	Cyber Security Fundamentals William Stallings — Cryptography and Network Security: Principles and Practice	
2	Bill Nelson, Amelia Phillips & Christopher Steuart — Guide to Computer Forensics and Investigations	
3	Steganography in Digital Media: Principles, Algorithms, and Applications by Jessica Fridrich,Cambridge University Press	
4	Cyber Law & IT Act (India Specific) Pavan Duggal - Cyber Law in India	
5	Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks, by Lisa Bock, Packt Publishing	
ICT/MOOCs Reference		
1	Google Cybersecurity Professional Certificate https://www.coursera.org/professional-certificates/google-cybersecurity/?utm_source=chatgpt.com	
2	Cisco Networking Academy: Learn Cybersecurity, Python & More https://www.netacad.com/catalogs/learn	

Mapping of CO with PO and PSO:								
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	1	2	1	1	3	2
CO2	2	3	2	2	1	1	3	2
CO3	2	2	3	3	2	1	2	2
CO4	3	3	2	3	2	1	2	3