Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Faculty of Computer Applications

Programme	B.Sc. IT Honours (Cyber Security)	**Branch**	Computer Applications
Semester	V	**Version**	1.0.0.0
Effective from Academic Year	2026-27	**Effective for the batch Admitted in**	June 2024
Subject code	U65B5DF	**Subject Name**	DIGITAL FORENSIC

Teaching scheme						**Examination scheme (Marks)**			
(Per week)	**Lecture (DT)**		**Practical (Lab.)**		**Total**		**CCE**	**SEE**	**Total**
	L	TU	P	TW					
Credit	4	-	-	-	4	Theory	50	50	100
Hours	4	-	-	-	4				

Objective:

To emphasize the fundamental and importance of digital forensic and incident response. The students will learn different techniques and procedure that enable them to conduct digital investigation systematically.

Pre-requisites:

Fundamental knowledge of cyber security, cyber-attacks and cyber law

Learning Outcome:

Name of CO	Description
CO1	Understand the fundamental concepts and their role in cyber security and incident response.
CO2	Describe and apply the digital forensic investigation process
CO3	Identify various forensic tools such as FTK, Autopsy, EnCase, Sleuth Kit, and Wireshark
CO4	Able to understand the techniques of network evidence.
CO5	Interpret the legal aspects, laws, and regulations relevant to digital forensic investigations

Mapping of CO and PO:

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	0	0	2	3	2	0	2	2	1	0
CO2	3	3	2	2	3	2	1	1	2	2	0	2
CO3	2	2	1	1	3	1	1	0	1	1	1	0
CO4	2	3	2	2	3	1	1	0	1	1	0	1
CO5	2	1	1	0	1	3	2	0	2	3	0	0

Content:

Unit	Content	Hrs.
1	**Introduction to Digital Forensics** • Definition and Scope of Digital Forensics • Need for and Importance of Cyber Security • Categories of Computer Crimes and Incidents • Incident Response: Incident response process, the role of digital forensic, incident response framework	12
2	**Digital Forensics Process:** • Chain of Custody and Forensic Process Overview • Digital Evidence: Types, Characteristics, and Legal Considerations • Challenges in Digital Forensics • Steps in Digital Forensic Investigation: Identification, Preservation, Collection, Examination, Analysis, Reporting.	12
3	**Introduction to Popular Forensic Tools:** • FTK, Autopsy, EnCase, Sleuth Kit, X-Ways and Wireshark	12

4	**Network Evidence Collection:** • Preparation, Network diagram, configuration: Logs and log management, • network device evidence, Security information and event management system • Security onion, packet Capture, Evidence collection.	12
5	**Introduction Laws and regulations:** • Rules of evidence in Digital Forensic **Introduction to Mobile Forensics:** • Android and iOS File System Structure • Mobile Data Extraction Techniques	12

Practical Content:	
-	
Reference Books:	
1	Digital Forensics and Incident Response - An intelligent way to respond to attacks 1st edition by Gerard Johansen Published by Packt Publishing Ltd.
2	Real Digital Forensics 1st edition by Keith J. Jones, Richard Bejtiich, Curtis W. Rose, Published by Addison Wesley Pearson Education
3	Computer Evidence Collection & Presentation 1st edition by Christopher L.T. Brown Published by Firewall Media
Web Reference:	
1	https://www.cybrary.it/course/computer-hacking-forensics/
2	https://www.cs.nmt.edu/df/lectures.html
MOOC Certification	
1	https://www.coursera.org/learn/digital-forensics – Coursera (by RIT)
Question Paper Scheme:	
	End Semester Examination Duration: (2 Hours Theory Examination) **Note for Examiner: -** Q-1 Any Five out of Seven (25 Marks) Q-2 Any Two out of Three (06 Marks) Q-3 Mandatory question (05 Marks) Q-4 Any Two out of Three (08 Marks) Q-5 Any Two out of Three(06 Marks) *The question paper must comprehensively address all Course Outcomes (COs), align with Bloom's Taxonomy levels, and ensure complete syllabus coverage.