Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Faculty of Computer Applications

Programme	BCA Honors (Cyber Security)	**Branch**	Computer Applications
Semester	II	**Version**	1.0.0.0
Effective from Academic Year	2026-2027	**Effective for the batch Admitted in**	June 2026
Subject Code	U102E7BCF	**Subject Name**	BASICS OF COMPUTER FORENSICS

Teaching scheme						**Examination scheme (Marks)**			
(Per week)	**Lecture (DT)**		**Practical (Lab.)**		**Total**		**CE**	**SEE**	**Total**
	L	TU	P	TW					
Credit	2		-	-	2	Theory	25	25	50
Hours	2		-	-	2	Practical	-	-	-

Objective:

The objective of this course is to introduce students to the fundamentals of computer forensics, digital evidence, cyber-crimes, and forensic investigation procedures. The course aims to develop basic skills required to identify, collect, analyze, and report digital evidence while understanding the legal and ethical aspects of computer forensics.

Pre-requisites:

Students need to know about A fundamental understanding of computers, operating systems, and networks is required, but no prior knowledge of computer forensics is necessary.

Course Outcomes :

Name of CO	Description
CO1	Explain the concepts, scope, and importance of computer forensics and its role in investigating cyber-crimes.
CO2	Identify different types of cyber-crimes and digital evidence and explain relevant legal, ethical, and procedural requirements.
CO3	Apply standard forensic investigation processes to collect, preserve, and analyze digital evidence in a systematic manner.
CO4	Analyze file systems, storage media, operating systems, and basic network data for forensic purposes.
CO5	Use basic forensic tools to prepare professional forensic reports and understand emerging areas such as mobile and cloud forensics.

Mapping of CO and PO

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

Content:

Unit		Hrs

1	**Introduction to Computer Forensics** ● Definition, scope, and objectives of computer forensics ● History and evolution of digital forensics ● Types of cyber crimes ● Role and responsibilities of a forensic investigator ● Challenges and limitations in computer forensics	06
2	**Cyber Crime, Legal & Ethical Aspects** ● Overview of cyber-crimes (hacking, fraud, identity theft, etc.) ● Information Technology Act (India) and cyber laws ● Digital evidence and legal admissibility ● Chain of custody ● Ethical issues in computer forensics	06
3	**Cyber Crime, Legal & Ethical Aspects** ● Overview of cyber-crimes (hacking, fraud, identity theft, etc.) ● Information Technology Act (India) and cyber laws ● Digital evidence and legal admissibility ● Chain of custody ● Ethical issues in computer forensics	06
4	**System, Storage & Network Forensics** ● File system basics (FAT, NTFS) ● Hard disk structure and partitions ● Storage media (HDD, SSD, USB, memory cards) ● Deleted file recovery concepts ● Operating system forensics (Windows, Linux, Mac – overview) ● Network and Internet forensics ● Email and web browser forensics	06
5	**Advanced Forensics, Tools & Reporting** ● Mobile forensics (introduction) ● Cloud forensics (overview and challenges) ● Overview of forensic tools (FTK, EnCase, Autopsy, etc.) ● Open-source vs commercial forensic tools ● Forensic report writing ● Role of forensic expert in court ● Case studies and future trends	06
Practical Content:		
Not Applicable		
Text Books:		

1	Digital Evidence and Computer Crime: Forensic Science by Eoghan Casey, Academic Press Publisher.
Reference Books:	
1	Nelson, B., Phillips, A., & Steuart, C., Guide to Computer Forensics and Investigations, Cengage Learning.
2	Nina Godbole & Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India.
3	Albert J. Marcella Jr. & Doug Menendez, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, CRC Press.
4	Nihad A. Hassan, Digital Forensics Basics: A Practical Guide Using Windows OS, Springer.
Web References / MOOC / Certification Course	
1	https://www1.mooc-list.com/course/computer-and-hacking-forensics-cybrary
2	https://alison.com/course/digital-forensics-examiner
3	https://alison.com/course/introduction-to-digital-forensics
4	https://www.mygreatlearning.com/academy/learn-for-free/courses/cyber-forensics
5	https://www.getyoureducation.net/course/digital-forensics
6	https://www1.mooc-list.com/course/digital-forensics-essentials-dfe-coursera
7	https://www.coursera.org/learn/digital-forensics-concepts
Question Paper Scheme:	
	End Semester Examination Duration: (1 Hour Theory Examination) **Note for Examiner:** - Q-1 Any Five out of Seven (05 Marks) Q-2 Any Two out of Three (05 Marks) Q-3 Mandatory question (05 Marks) Q-4 Any Two out of Three (05 Marks) Q-5 Any Two out of Three (05 Marks) *The question paper must comprehensively address all Course Outcomes (COs), align Taxonomy levels, and ensure complete syllabus coverage.*