GANPAT UNIVERSITY									
FACULTY OF ENGINEERING AND TECHNOLOGY									
Programme	Bachelor of Technology					Branch/Spec.	Computer Science & Engineering (CS)		
Semester	VII					Version	1.0.0.1		
Effective from Academic Year			2022-23			Effective for the batch Admitted in			June 2019
Subject code	2CSE707		Subject Name			CYBER FORENSICS			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	1	0	4	Theory	40	60	100
Hours	3	0	2	0	5	Practical	30	20	50

Pre-requisites:

Computer Networks, Ethical Hacking, basic knowledge on Windows, Mac and Linux OS

Objectives of the Course:

After successful completion of the course students should be able to

- Understand the fundamental of Cyber Forensics
- Analyze and validate the forensics data
- Work with different tools and techniques associated with Cyber Forensics
- Understand the document prepared for the Forensics investigation

Theory syllabus

Unit	Content	Hrs
1	**Cyber Forensics** Cybercrime, Basics of cyber forensics, cyber forensics investigation processes, digital evidence, challenges in cyber forensics, skills required for cyber forensics expert	**4**
2	**OS Forensics** Digital Evidence in Windows, File system, Timeline analysis, challenges Digital Evidence on Macintosh, Digital Evidence on UNIX	**8**
3	**Network Forensics** Forensics Footprints, Seizure of Networking Devices, Network Forensics Artifacts, ICMP Attack	**7**
4.	**Mobile Forensics** Acquisition Protocol, Android Operating System, Manual Extraction, Physical Acquisition, Challenges in Mobile Forensics	**7**
5.	**Cloud Forensics and Web Attack Forensics and Email Forensics** Introduction, Artifacts in Cloud Forensics, Challenges, Forensics as a service. Intrusion forensics, database forensics, Preventive Forensics	**8**
6.	**Solid State Device (SSD) Forensics** SSD Components, SSD concept, Forensics Analysis of an SSD	**4**
7.	**Report Writing for High-Tech Investigation** Understanding and importance of Reports, Guidelines	**4**

Practical content:

Study of different tools used for forensic investigation and perform different operations like recover the lost files, extract the information of the attacker, etc.

Text Books:

1.	Practical Cyber Forensics: An incident- Based Approach to Forensic Investigations, by Niranjan Reddy
2.	Digital evidence and computer crime: Forensic science, computers and the internet by Casey, E, Academic Press
Reference Books:	
1.	CyberForensics - Understanding Information Security Investigation by Jennifer Bayuk
2.	Handbook of Digital Forensics and Investigation By Eoghan Casey 1st Edition
3.	Casey, E. Handbook of digital forensics and investigation. Academic Press
4.	Cyber Forensics from Data to Digital Evidence by Albert J. Marcella, Jr.,PHD, CISA, CISM Frederic Guillossou, CISSP, CCE
5.	Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to computer forensics and investigations. Cengage Learning.
Course Outcomes:	
COs	Description
CO1	Understand the fundamental of Cyber Forensics
CO2	Analyze and validate the forensics data
CO3	Work with different tools and techniques associated with Cyber Forensics
CO4	Understand the document prepared for the Forensics investigation

Mapping of CO and PO:

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