Course Syllabus
Gyanmanjari Institute of Technology
Semester-5 (B.Tech.)

Subject: Computer Forensics-BETCE14405

Type of course: Professional Core and Professional Elective Courses

Prerequisite: Fundamental knowledge of computing systems, cybersecurity, networking and basic programming for forensic investigation and analysis.

Rationale:

In the era of increasing digital threats, the need for skilled professionals in computer forensics has become essential to safeguard information and combat cybercrime. This comprehensive course is designed to immerse students in the critical areas of digital investigation, empowering them to navigate the complex landscape of modern cybersecurity with confidence. By focusing on core areas such as digital evidence collection, network and memory forensics, and legal protocols; learners will develop a holistic understanding of the forensics process—from securing and analyzing evidence to ensuring adherence to legal standards and ethical considerations. Through hands-on activities, students will also explore cutting-edge technologies like artificial intelligence in network forensics, equipping them with the practical skills and theoretical knowledge needed to address the evolving challenges in the field of digital investigations.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
				Theory Marks		Practical Marks		CA	
CI	T	P	C	ESE	MSE	V	P	ALA	
4	0	2	5	60	30	10	20	30	150

Legends: CI-ClassRoom Instructions; T – Tutorial; P - Practical; C – Credit; ESE - End Semester Examination; MSE- Mid Semester Examination; V – Viva; CA - Continuous Assessment; ALA- Active Learning Activities.

Course Content:

Sr. No	Course content	Hrs.	% Weightage
1	**Introduction:** Forensic Science, Computer Forensics Fundamentals – Types of Computer Forensics Technology. **Basics of Computer:** Computer organization, Components of computer- input and output devices, CPU, Memory hierarchy, Types of memory, Storage devices.	08	15%
2	**Cybercrime and Digital Forensics: Evidence Collection, Analysis, and Legal Procedures:** Definition and types of cybercrimes, electronic evidence and handling, Internet crimes, Cryptography, Analysis of cyber-criminalistics area, Digital Forensics, Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and unretrieved communications, Evidence Management & Presentation, Preservation of Digital Evidence.	14	20%
3	**Computer Forensics:** Introduction of Computer Forensics, prepare a case, begin an investigation, understand computer forensics workstations and software, Developing Forensic Capabilities – Conduct an investigation, complete a case, critique a case, Searching and Seizing Computer Related Evidence, Windows Systems-FAT12, FAT16, FAT32 and NTFS.	14	20%
4	**Network Forensics:** Overview of Network Forensics, Open-source security tools for network forensic analysis, requirements for preservation of network data, Wireless Network Forensics.	08	15%
5	**Memory and Mobile Forensics:** **Memory Forensics:** History of Memory Forensics, x86/x64 architecture, Volatility Framework & plugins Memory acquisition, File Formats – PE/ELF/Mach-O, Related tools – Bulk Extractor and YARA, Introduction to Anti-forensics, tools and techniques. **Mobile Forensics:** Mobile forensics techniques, Mobile forensics tools.	08	15%

6	**Cyber Ethics and Legal Aspects:** Overview of IT Act, 2000, Amendments and Limitations of IT Act, The Importance of Cyber Law, Significance of cyber-Ethics, Cyberbullying and Online Harassment, General Data Protection Regulation (GDPR), The Impact of Digital Forensics in Law Enforcement, Introduction to Artificial Intelligence Ethics and Block chain Ethics.	08	15%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Identifying Essential Court Documents for a Legally Sound Criminal Investigation:** In this activity each student individually is recognizing the specific court documents required in a criminal investigation is essential for developing a thorough and legally sound approach to gathering evidence and supporting the investigative process. The findings must be compiled into a PDF report and uploaded to the GMIU Web Portal.	10
2	**Mastering Digital Evidence Handling: Essential Steps for Integrity and Legal Compliance in Investigations:** In this activity each student individually prepares a document covering the steps to identify, collect, handle, and preserve digital evidence. These are essential skills for safeguarding evidence integrity and adhering to legal requirements in digital investigations. The findings should be documented in a PDF report and uploaded to the GMIU Web Portal.	10
3	**AI in Network Forensics:** In this activity each student individually is examine the role of Artificial Intelligence in Network Forensics through the analysis of real-world cases, identifying how AI technologies can improve the efficiency and accuracy of the investigative process. Refer to relevant research papers to support your understanding. The findings must be compiled into a PDF report and uploaded to the GMIU Web Portal.	10
	Total	30

Suggested Specification table with Marks (Theory):60

Distribution of Theory Marks (Revised Bloom's Taxonomy)						
Level	**Remembrance (R)**	**Understanding (U)**	**Application (A)**	**Analyze (N)**	**Evaluate (E)**	**Create (C)**
Weightage %	35%	30%	15%	10%	10%	-

Course Outcome:

After learning the course, the students should be able to:	
CO1	Understand the fundamentals of forensic science and its role in investigations.
CO2	Define cybercrimes and classify their various types in the digital landscape.
CO3	Analyze forensic workstations, tools, and software for evidence collection.
CO4	Analyze forensic techniques for investigating wireless networks and related threats.
CO5	Explore significance of memory forensics, cyber laws, IT Act 2000 and ethical considerations in digital forensics.

List of Practical:

Sr. No	Description	Unit No	Hrs.
1	To study detail working of boot process the operating system (Windows, Linux).	1	4
2	Implementing Steganography for hiding and retrieving data in an image.	2	4
3	Analysis of Internet Crimes and Cyberbullying Case Study.	2	2
4	Examine SQL injection attack.	2	2
5	To track the details of the computer in past using Last Activity view tool.	3	4
6	Recovering Deleted Files and Partitions.	3	2
7	To track the details of the computer in past using Last Activity view tool.	3	2
8	Analysis of TCP protocol using Wireshark.	4	4

9	Analyze network traffic to identify suspicious activity using open-source tools. Capture and analyze packets to detect malicious behavior.	4	4
10	Explore the Nmap tool and list how it can be used for network defense.	4	2
11	Investigating Wireless Attacks.	4	2
12	Explore Mobile Forensics.	5	2
		Total	30

Instructional Method:

The course delivery method will depend upon the requirement of content and the needs of students. The teacher, in addition to conventional teaching methods by black board, may also use any tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

Practical examination will be conducted at the end of semester for evaluation of performance of students in the laboratory.

Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Reference Books:

[1] Computer Forensics: Cybercriminals, Laws, and Evidence, Marjie T. Britz, Pearson.
[2] Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Cengage Learning.
[3] Incident Response & Computer Forensics, Jason T. Luttgens, Matthew Pepe, Kevin Mandia, McGraw Hill.
[4] Digital Forensics with Open-Source Tools, Cory Altheide, Harlan Carvey, Elsevier.
[5] The IT Act, 2000 with Rules, Regulations, and Amendments, P. M. Bakshi, Universal Law Publishing.