Subject: Computer Forensics – MSCFS12511

Type of course: Minor

Prerequisite: Basic awareness of laws and ethical standards related to data privacy, evidence handling, and cybercrime investigations.

Rationale: The Computer Forensics syllabus prepares students to investigate digital crimes by teaching essential skills in data analysis, evidence handling, and legal considerations. A strong foundation in computer science, networking, and cybersecurity ensures students can effectively apply forensic techniques to uncover and preserve digital evidence, supporting legal proceedings and ethical standards in cybercrime investigations.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
CI	T	P	C	Theory Marks		Practical Marks		CA	
				ESE	MSE	V	P	ALA	
3	0	0	3	60	30	10	00	50	150

Legends: CI-Class Room 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:

Unit No.	Course content	Hrs	% Weight age
1	**Cyber Crime and computer crime :** Introduction to Digital Forensics, Definition and types of cybercrimes, electronic evidence and handling, electronic media, collection, searching and storage of electronic media, introduction to internet crimes, hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes and modules.	10	25

2	**Basics of Computer** Computer organisation, components of computer- input and output devices, CPU, Memory hierarchy, types of memory, storage devices, system softwares, application softwares, basics of computer languages.	10	25
3	**Computer Forensics** Definition and Cardinal Rules, Data Acquisition and Authentication Process, Windows Systems-FAT12, FAT16, FAT32 and NTFS, UNIX file Systems, mac file systems, computer artifacts, Internet Artifacts, OS Artifacts and their forensic applications.	10	25
4.	**Forensic Tools and Processing of Electronic Evidence** Introduction to Forensic Tools, Usage of Slack space, tools for Disk Imaging, Data Recovery, Vulnerability Assessment Tools, Encase and FTK tools, Anti Forensics and probable counters, retrieving information, process of computer forensics and digital investigations, processing of digital evidence, digital images, damaged SIM and data recovery, multimedia evidence, retrieving deleted data: desktops, laptops and mobiles, retrieving data from slack space, renamed file, ghosting, compressed files.	15	25

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1.	**Electronic Evidence Handling Exercise** Faculty will provide students with a hypothetical crime scene involving digital devices. They must outline the steps involved in handling, collecting, and storing electronic evidence in accordance with best practices and will upload it on GMIU web Portal.	10
2.	**Memory Hierarchy Comparison** Ask students to create a table or chart comparing different types of memory (e.g., registers, cache, RAM, hard disk) in terms of speed, cost, and capacity and upload it on GMIU web Portal.	10
3.	**Data Authentication Exercise** Faculty will provide students with a set of digital data (e.g., images, documents) and ask them to outline the steps involved in data acquisition and authentication and upload it on GMIU web Portal.	10
4.	**Forensic Application Mapping** Students will work in groups to map out forensic applications and tools used to analyze specific artifacts on different operating systems. Each group will focus on one OS and demonstrate how its artifacts (e.g., registry in	10

GYANMANJARI INNOVATIVE UNIVERSITY
GMIU
BHAVNAGAR

	Windows, system logs in UNIX) are analyzed using specific forensic tools and upload it on GMIU web Portal.	
5.	**Mobile Data Recovery Exercise** Faculty will provide students with a case involving a damaged SIM card or mobile device, and ask them to outline the steps and tools needed to recover data and upload the same it on GMIU web Portal.	10
	Total	**50**

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)
Weight age	30%	30%	30%	10%	0	0

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcome:

After learning the course the students should be able to:	
CO1	Analyze the techniques used in hacking, cracking, and fraud in cyberspace, including preventive measures.
CO2	Describe the different types of memory (e.g., RAM, cache, hard disk) and their roles in computing performance.
CO3	Identify and explain the characteristics of various file systems (FAT12, FAT16, FAT32, NTFS, UNIX, macOS) and their role in digital evidence collection.
CO4	Demonstrate the complete process of digital forensics, including the handling of electronic evidence, data recovery, and proper documentation for legal proceedings.

GYANMANJARI INNOVATIVE UNIVERSITY • BHAVNAGAR •

Instructional Method:

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

From the content 10% topics are suggested for flipped mode instruction.

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

The internal evaluation will be done on the basis of Active Learning Assignment

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

Reference Books:

[1] Digital Evidence and Computer Crime by Eoghan Casey.
[2] Practical Guide to Computer Forensics Investigations by Cheryi A. O'Connor.
[3] Computer Forensics: Investigating Networked Computers by Mark S. Pollitt & Peter Stephenson.
[4] Handbook of Digital Forensics and Investigation by Eoghan Casey.

G...ANJARI INNOVATIVE UNIVERSIT
• BH...