दिव्यम् ददामि ते चक्षुः
GMIU
Gyanmanjari
Innovative University

Course Syllabus
Gyanmanjari Science College
Semester-5 (B.Sc)

Subject: Cyber Forensics - BSCFS15310

Type of course: Minor

Prerequisite: Basic understanding of computer, its applications and online crimes

Rationale: This course covers computer forensics, its fundamentals and investigation of digital crimes. Students will be able to identify data, learn about digital evidences and their retrieval and understand the cyber tools and its application.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
CI	T	P	C	ESE		CCE			
				Theory	Practical	MSE	LWA/V	ALA	
4	0	0	4	100	00	30	00	70	200

Legends: CI-Class Room Instructions; T – Tutorial; P - Practical; C – Credit; SEE - Semester End Evaluation; MSE- Mid Semester Examination; LWA - Lab Work Assessment; V – Viva voce; CCE-Continuous and Comprehensive Evaluation; ALA- Active Learning Activities.

4 Credits * 25 Marks = 75 Marks (each credit carries 25 Marks) Theory
SEE 100 Marks will be converted in to 50 Marks
CCE 100 Marks will be converted in to 50 Marks

Course Content:

Unit No	Course Content	Hrs	% Weightage
1	**Computer Forensics**: Introduction, use in law enforcement, computer forensics assistance to human resource, computer forensics services, benefits of professional forensic methodology, steps taken by computer forensics specialists, types of computer forensics technology, CFX- 2000, types of	15	25%

GYANMANJARI INNOVATIVE UNIVERSITY • BHAVNAGAR • GMIU

	law enforcement computer forensics technology, business computer forensics technology, computer forensics evidence and capture.		
2	**Evidence collection and data seizure**: evidence collection, collection options, obstacles, types of evidences, volatile evidence, general procedure, collection and archiving, methods of collections, artifacts, collection steps, controlling contamination, chain of custody, duplication and preservation of digital evidence, computer image verification and authentication	15	25%
3	**Computer forensic analysis**: discover of electronic evidence, identification of data, reconstruction of past events, fighting against macro threats, information warfare arsenal, tactics of military, tactics of terrorist and rogues, tactics of private companies.	15	25%
4	**Information warfare**: Arsenal, Surveillance Tools, Hackers and Theft of Components, Contemporary Computer Crime, Identity Theft and Identity Fraud, Organized Crime &Terrorism, Avenues Prosecution and Government Efforts – Applying the First Amendment to Computer Related Crime, The Fourth Amendment and other Legal Issues.	15	25%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Trace the Trail** Provide students with a simulated forensic report containing logs, timestamps, and file metadata. Their task is to analyze the clues and reconstruct the sequence of events in a cybercrimeand they will upload it on GMIU web Portal.	10
2	**Digital Breadcrumbs** Give students a series of events (e.g., web history, login attempts, file access) scrambled out of order. They must arrange the events chronologically and determine a possible motive or suspect and will upload the same on GMIU web Portal.	10
3	**Who Dunnit? Cyber Edition** Provide students with clues such as email headers, timestamps, and usernames. They piece together the story and determine which suspect is behind the cybercrime and upload it on GMIU web Portal.	10

4	**Code breaker Chronicles** Present students with an encrypted message or hash and have them manually work through cipher puzzles or hashing algorithms to decode or verify its contents and upload it on GMIU web Portal.	10
5	**Cyber crime case study analysis** Students will be provided with famous cyber crime cases, they have to discuss forensic challenges and suggest the solutions and submit the report of case on GMIU web portal.	10
6	**Steganography detection challenge** Students will be provided with hidden messages or images inside files using steganography tools (example: openstego, steg hide), they have to analyze suspicious files and extract hidden data and upload the retrieved data image on GMIU web portal.	10
7	**Attendance**	10
Total		70

Suggested Specification table with Marks (Theory):75

Distribution of Theory Marks **(Revised Bloom's Taxonomy)**						
Level	Remembrance (R)	Understanding (U)	Application (A)	Analyze (N)	Evaluate (E)	Create (C)
Weightage	20%	40%	30%	10	00	00

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.

GYANMANJARI INNOVATIVE UNIVERSITY BHAVNAGAR GMIU

Course Outcome:

After learning the course the students should be able to:	
CO1	Analyze the nature, retrieval, and preservation of digital evidence.
CO2	Examine the classification, characteristics, and evolution of computer crimes.
CO3	Assess government efforts and avenues for prosecuting information warfare crimes.
CO4	Investigate network intrusions, traffic, and web attacks using forensic techniques.

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] MariE-Helen Maras, "Computer Forensics: Cybercriminals, Laws, and Evidence", Jones & Bartlett Learning; 2nd Edition, 2014.

[2] CyberForensics - Understanding Information Security Investigation by Jennifer Bayuk

[3] Handbook of Digital Forensics and Investigation By Eoghan Casey 1st Edition

[4] Cyber Forensics from Data to Digital Evidence by Albert J. Marcella, Jr.,PHD, CISA, CISM Frederic Guillossou, CISSP, CCE

GYANMANJARI INNOVATIVE UNIVERSITY BHAVNAGAR