

Branch Name:	IMCA
Program Code:	CS301
Course Title:	Cyber Forensics
Course Code:	1CS3010806T
Pre-requisite Course:	Basic knowledge of Computer Networks, Operating Systems (Windows/Linux), and Information Security concepts including cyber threats, system architecture, and data handling.

Course Objective:

1. Understand the principles, goals, and methodologies of digital forensics.
2. Master the process of computer forensics investigation, including data acquisition, analysis, and reporting.
3. Develop expertise in Windows forensics, including file system analysis and event log examination.
4. Explore network forensics techniques, including data collection, analysis, and intrusion detection.
5. Apply legal and ethical principles in digital forensics investigations, including compliance with IT laws and regulations.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
4	-	-	4	60	40	-	-	100

Course Contents:

Unit No	Topic	Total Hours	Weight age (%)
1	Introduction to Cyber Forensics • Introduction to forensic • Types of Forensic • Computer/ Digital forensic concept & goal • Computer forensic process • Benefits of computer forensics • Objectives of computer forensics • Role of Forensic Investigator • Forensic Readiness • Basics principles of forensic • Computer Forensics Investigation Process: • Introduction to Computer Crime Investigation • Assess the situation and acquire the data • Analyze the data • Report the investigation • Chain of custody	12	25
2	Digital Evidence and First Responder Procedure • What is Digital Evidence?	12	25

	• First Responder Toolkit • Digital Evidence Collection & Preservation • Computer Image Verification and Authentication • Collection Issues facing computer forensics. • Types of Investigation • Techniques of Digital Forensics • CRPC & IT Act Introduction, Laws & Sections are applicable in the Forensic Process • Role of Forensic Investigator, Duties of Forensic Investigator		
3	Windows Forensics • Introduction to Windows Forensics • Need for Windows forensics • Major forensic areas in Windows • Volatile & Non-Volatile Information. • Windows File System, Types of File System • Data Recovery • Retrieving deleted files and retrieving cache files • Retrieving files in unallocated space • Slack space, swap space • file carving • Event Logs	12	25
4	Network Forensics • Introduction to Network Forensic Process • Network Data collection methods • Network Components and their Forensic Importance • Host, Node, Router, Switch, Hub, NIC, DNS, IP Address • Forensic Tools (Wireshark, Nmap, SPLUNK, CAINE, EnCase, Snort) • Logs and Event Analysis: • Windows Registry – Windows event log file – Windows password storage. • Wireless Attack Forensics: • Introduction – Web Attack Forensics – Web Application Forensic Tools	12	25

Text Books:

1. Digital Forensics and Incident Response: Fundamentals and Practices by Gerard Johansen
2. Practical Incident Response: An Introduction to Enterprise Incident Response, Second Edition by Phil Beyer and Chris Childers
3. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters

Reference Books:

1. Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8, Fourth Edition by Harlan Carvey
2. Incident Response & Computer Forensics, Third Edition by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia

List of Open Source Software/learning website:

- <https://tryhackme.com>
- <https://hackthebox.com>
- <https://letsdefend.io>
- <https://github.com/>

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Explain the principles, types, investigation process, and forensic readiness in digital forensics.	3 Apply
CLO2	Apply techniques for identification, collection, preservation, and authentication of digital evidence while maintaining chain of custody and legal compliance.	4 Analyze
CLO3	Analyze Windows systems through file system examination, event log analysis, and data recovery techniques.	4 Analyze
CLO4	Investigate network-based incidents using forensic tools, packet analysis, and log analysis techniques.	5 Evaluate
CLO5	Evaluate digital forensic tools, techniques, and legal frameworks to ensure accurate investigation and compliance with cyber laws (IT Act, CRPC).	6 Create
CLO6	Design and produce comprehensive forensic investigation reports by integrating evidence analysis, incident response, and professional documentation practices.	3 Apply

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CLO1	H	M	-	-	M	-	-	L	-	-	-	M	M	M
CLO2	H	M	M	-	H	-	-	-	-	-	-	M	H	M
CLO3	M	H	H	M	H	-	-	-	-	-	-	M	H	H
CLO4	M	H	H	M	H	-	-	-	-	-	-	M	H	H
CLO5	M	H	H	H	H	-	-	-	-	-	-	M	H	H
CLO6	M	M	H	H	H	-	-	M	M	L	L	H	M	H

H:High, M:Medium, L:Low