

Branch Name:	Bachelor of Computer Application (BCA)
Program Code:	CS101
Course Title:	Digital Forensic
Course Code:	18-CAE405-4C
Pre-requisite Course:	Basic knowledge of Operating System, Computer Networks, and Cyber Security

Course Objective (CO):

This course is intended to make the students:

- Understand digital forensics concepts and cybercrime investigation techniques
- Learn evidence acquisition, preservation, and analysis procedures
- Develop hands-on skills using open-source forensic tools
- Analyze cyber incidents including mobile and network environments
- Prepare professional forensic reports and understand legal frameworks

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	
2	-	4	4	25	25	25	25	100

Course Contents:

Sr. No	Topics	Total Hours	Weightage (%)
1.	Introduction to Digital Forensic Definition, Need, Scope - Types of Cyber Crimes (Phishing, Identity Theft, Malware) - Digital Evidence Types (Volatile & Non-Volatile) - Forensic Readiness & Challenges	10	20
2.	Forensic Investigation Process & Legal Framework Investigation Phases: Identification, Collection, Preservation, Analysis - Chain of Custody - Documentation & Reporting Standards - Overview of IT Act 2000 (India) & Cyber Laws	8	20
3.	Computer Forensics: File Systems (FAT, NTFS basics) - Disk Imaging & Cloning - Data Recovery Techniques - Registry & Log Analysis - Introduction to Memory Forensics	10	20
4.	Network, Email & Mobile Forensics: Network Traffic Analysis (Basics) - Email Header Investigation - Mobile Data Analysis (Call logs, Media, Apps) - Social Media Forensics (Basic)	10	20
5.	Forensic Tools, Case Study & Report Writing :- Autopsy, FTK Imager (Free), Wireshark - Introduction to Volatility (Demo) - Simple Cyber Crime Case Analysis - Forensic Report Preparation	8	20

Course Learning Outcomes (CLO):

At the end of this course, the student would be able

CLO1: Understand the fundamentals of digital forensics and cybercrime

CLO2: Apply forensic investigation methods and legal procedures

CLO3: Use open-source forensic tools for data analysis

CLO4: Analyze cyber incidents and prepare professional reports

List Text Book:

1. "Cyber Security and Cyber Laws" – Dr. Kumar K.
2. "Information Security and Cyber Laws" – Dr. Surya Prakash Tripathi
3. "Fundamentals of Cyber Security" – Dr. Pankaj Agarwal

List of Reference Book:

1. "Cyber Forensics" – Dr. M. Rezaul Karim
2. "Digital Evidence and Computer Crime" – Eoghan Casey (International but standard)
3. "Guide to Computer Forensics and Investigations" – Bill Nelson

E-Resource / Web Links:

NPTEL Cyber Security Course <https://nptel.ac.in>

Digital Forensics Full Course <https://www.youtube.com/watch?v=3b6n3lsJ0t4>

Wireshark Beginner Tutorial <https://www.youtube.com/watch?v=TkCSr30UojM>

Autopsy Tool Hands-on <https://www.youtube.com/watch?v=ZK8bqC3lYw8>

Cyber Crime Investigation Basics <https://www.youtube.com/watch?v=8z5p8sR4z3Q>

List of Experiments:**Basic Level(Foundation)**

1. Study and documentation of real cybercrime cases (India-based)
2. Identification of digital evidence from sample files
3. File metadata analysis using free tools
4. Understanding file systems (FAT/NTFS) using demo tools

Intermediate Level (Hands-on)

5. Disk imaging using **FTK Imager (Free version)**
6. Recover deleted files using **Autopsy Tool**
7. Log file analysis (Windows/Linux logs)
8. Email header analysis (trace sender IP)

Applied Level (Skill Development)

9. Network packet capture and analysis using **Wireshark**
10. Basic mobile data investigation (images, logs, app data)
11. Password analysis using **John the Ripper (Demo)**
12. Memory analysis demo using **Volatility**

Case-Based Learning (Very Important)

13. Mini case: "Unauthorized Access in College Lab"
14. Mini case: "Phishing Email Investigation"
15. Prepare full forensic report (structured format)

Suggested Open-Source Tools

- **Autopsy** (Best for beginners)
- **FTK Imager (Free)**
- **Wireshark**
- **Volatility (Intro level)**
- **John the Ripper (Demo use)**



In Effect from Academic Year 2023-24

H: High, M: Medium, L: Low