

Branch Name:	Bachelor of Computer Application (BCA)
Program Code:	CS101
Course Title:	Penetrating and Autopsy (Crime Investigation)
Course Code:	17-CAE402-4C
Pre-requisite Course:	Students should have basic knowledge of Computer Networks (TCP/IP, OSI model), Operating Systems (Windows/Linux), Web Technologies. Understanding of programming concepts (C/Python/Java) and introductory information security concepts is recommended. Awareness of cyber ethics and legal responsibilities is also desirable.

Course Objective (CO):

This course is intended to make the students:

- To introduce students to the fundamentals of cyber penetration testing and digital crime investigation.
- To develop practical skills in ethical hacking and vulnerability assessment.
- To understand digital autopsy (computer forensics) techniques used in cybercrime investigation.
- To familiarize students with legal, ethical and procedural aspects of cybercrime investigation in India.
- To analyze real-world cybercrime case studies and apply investigation techniques..

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.	Fundamentals of Cyber Crime & Ethical Penetration Testing: Introduction to Cyber Crime - Types of Cyber Crimes (Phishing, Malware, Ransom ware, Identity Theft) - Basics of Ethical Hacking - Penetration Testing Concepts - Phases of Penetration Testing - Tools Overview (Kali Linux, Nmap, Wireshark – Conceptual understanding) -Legal Framework: IT Act 2000 (India)	10	20
2.	UNIT II: Network & System Penetration Techniques: Foot printing and Reconnaissance - Scanning Techniques - Vulnerability Assessment - Password Cracking Concepts - Social Engineering Attacks - Web Application Vulnerabilities (SQL Injection, XSS – Conceptual) - Defensive Mechanisms (Firewall, IDS, IPS) (Practical Component: Basic lab-based vulnerability scanning simulation)	10	20
3.	Digital Autopsy & Computer Forensics: Introduction to Digital Forensics - Digital Evidence Types - Chain of Custody - Disk Imaging & Data Recovery Concepts - File System Analysis - Log File Investigation - Email and Mobile Forensics Basics - Forensic Tools Overview (FTK, Autopsy Tool – Conceptual) (Practical Component: Forensic image analysis using open-source tools)	10	20
4.	Legal, Ethical & Documentation Aspects: Cyber Laws in India - Indian Evidence Act (Digital Evidence) - Documentation and Reporting Standards - Incident Response Procedures - Ethics in Cyber Investigation - Role of Cyber Cell & CERT-In - Courtroom Presentation of Digital Evidence (Practical Component: Mock investigation report writing)	09	20
5.	Case Study Based (Applied Investigation): Phishing Attack Investigation - Ransom ware Incident Analysis - Insider Data Theft - Social Media Crime Investigation - Banking Fraud (Digital Transaction)	09	20

Course Learning Outcomes (CLO):

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

- CLO1: Explain cyber crime concepts and penetration testing methodology.
- CLO2: Perform basic vulnerability assessment and scanning techniques.
- CLO3: Apply digital forensic methods to analyze cyber evidence.
- CLO4: Interpret Indian cyber laws and ethical practices.
- CLO5: Analyze real-world cybercrime cases and prepare investigation reports.

List of Text Book:

1. Nina Godbole & Sunit Belapure – Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (Wiley India)
2. Harish Chander – Cyber Laws and IT Protection (PHI Learning)
3. Atul Kahate – Cryptography and Network Security (McGraw Hill India)
4. Dr. Surya Prakash Tripathi – Cyber Crime and Digital Forensics (Indian Edition)

List of Reference Book:

1. Vivek Sood – Cyber Law Simplified (McGraw Hill India)
2. Kamath Nandan – Handbook of Digital Forensics and Investigation
3. Nilakshi Jain – Information Security and Cyber Laws

E-Resource / Web Links:

- <https://www.cert-in.org.in>
- <https://cybercrime.gov.in>
- <https://owasp.org>
- <https://nptel.ac.in>
- <https://www.coursera.org> (Cyber Security Courses)
- Ministry of Electronics & IT – <https://www.meity.gov.in>

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)		
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO2	PSO 3
CLO1				H	H		M						L		
CLO2	H			H	H		M			M	M		M	L	M
CLO3				M	H								M		
CLO4	H				H								M		
CLO5				H	H	H	M	M	M		H		M	M	H
CLO6				H	H	H	M	M	M		H		M	M	H

H: High, M: Medium, L: Low

Practical List (Open-Source Platforms Only)

1. Installation of Kali Linux in VirtualBox Environment.
2. Basic Linux Commands and User Management.
3. Network Discovery and Port Scanning using Nmap.
4. Packet Capturing and Analysis using Wireshark.
5. Vulnerability Scanning using OpenVAS.
6. Web Application Testing using DVWA.
7. Password Hash Analysis using John the Ripper.
8. Social Engineering Awareness Simulation using GoPhish.
9. Disk Imaging using dd Command / FTK Imager (Free Version).
10. Digital Forensic Analysis using Autopsy Tool.
11. System Log File Analysis in Linux Environment.
12. Email Header Analysis for Investigation.
13. Browser History and Cache Forensic Analysis.
14. Case Study Based Digital Crime Investigation and Forensic Report Preparation.

Recommended Open-Source Platforms Summary

Category	Tools
OS	Kali Linux
Virtualization	VirtualBox
Scanning	Nmap
Packet Analysis	Wireshark
Vulnerability Scan	OpenVAS
Web Testing	DVWA
Password Testing	John the Ripper
Forensics	Autopsy
Log Analysis	ELK Stack
Disk Imaging	dd