Learning Outcomes-based Curriculum Framework

For

Diploma in Digital Forensics and Investigation
(1 Year/2 Semester Program)

Department of Computer Science & Engineering
Faculty of Engineering and Technology
Chaudhary Devi Lal University
Sirsa-125055
2025

Programme Educational Objectives (PEOs)

PEO 1: Core Competence

Graduates will acquire a strong foundational understanding of digital forensics principles, cybercrime investigation techniques, and relevant legal frameworks to competently address challenges in digital evidence acquisition, analysis, and preservation.

PEO 2: Professional Practice

Graduates will demonstrate proficiency in using forensic tools, software, and investigative methodologies in real-world scenarios, enabling them to work effectively in multidisciplinary teams across law enforcement agencies, private cybersecurity firms, and corporate environments.

PEO 3: Lifelong Learning and Adaptability

Graduates will engage in continuous learning and stay updated with emerging technologies, evolving cyber threats, and regulatory developments to remain relevant and effective in the ever-changing landscape of digital forensics and cybersecurity.

PEO 4: Ethics and Responsibility

Graduates will uphold the highest standards of professional ethics, data privacy, and legal compliance, demonstrating integrity and accountability in handling sensitive information and digital evidence during investigations.

Program Outcomes (POs): Upon successful completion of the Diploma in Digital Forensics and Investigation, the graduate will be able to:

PO1: Basic Knowledge: Apply knowledge of computing, networking, and digital systems to understand and analyse cyber incidents and digital evidence.

PO2: Technical Proficiency: Demonstrate competency in using forensic tools, scripting, and investigative software to acquire, preserve, examine, and interpret digital data from a variety of platforms.

PO3: Problem Analysis: Identify, analyse, and solve technical problems related to cybercrimes, security breaches, and data integrity using appropriate forensic and investigative techniques.

PO4: Legal and Regulatory Awareness: Understand and apply relevant legal provisions, cyber laws, and digital evidence admissibility standards in national and international contexts.

PO5: Communication: Communicate forensic findings effectively through clear documentation, technical reporting, and presentation, both orally and in writing.

PO6: Ethics and Professionalism: Apply ethical principles, maintain confidentiality, and demonstrate responsibility and integrity while dealing with sensitive digital evidence and victim information.

PO7: Lifelong Learning:Recognise the need for and engage in independent learning to keep pace with rapid technological changes in digital forensics, cybersecurity, and investigation practices.

PO8: Investigation and Critical Thinking: Design, conduct, and report structured forensic investigations using methodical, logical, and evidence-based approaches.

Table 1: Semester-wise course codes, course titles, workload and credits

Course Code	Course Title	Workload		Credit	Max. Marks
		L	P		
Semester – 1					
DDFI-11	IT Hardware and Network Infrastructure	3	2	4	100
DDFI-12	Principles of Information and Cyber Security	3	2	4	100
DDFI-13	Python Programming for Security	3	2	4	100
DDFI-14	Operating System Security	3	2	4	100
	Total	12	8	16	400
Semester – 2					
DDFI-21	Cyber Laws and Privacy Framework in India	4	-	4	100
DDFI-22	Fundamentals of Digital Forensics	4	-	4	100
DDFI-23	Digital Forensics and Investigation Lab	-	8	4	100
DDFI-24	Project Work	-	-	4	100
	Total	8	8	16	400

Semester I

DDFI-11: IT Hardware and Network Infrastructure							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Understand the architecture of computers and components.
Learn fundamentals of network infrastructure and configuration.
Gain hands-on experience with networking devices.
Understand LAN, WAN, and internet technologies.

Course Outcomes:

CO1: Identify and describe computer hardware components.
CO2: Demonstrate understanding of networking concepts and protocols.
CO3: Configure basic LAN and wireless setups.
CO4: Work with networking devices like routers and switches.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	2	1	1	0	0	0
CO2	3	3	2	2	1	0	0	0
CO3	2	3	3	2	2	1	0	0
CO4	3	3	3	2	1	1	1	1

Detailed Syllabus:

Unit 1: Introduction to IT Hardware

Basic Computer Components: CPU, Memory (RAM, ROM), Storage Devices (HDD, SSD), Motherboard, Input/Output Devices.

Peripheral Devices and their security considerations.
Introduction to different types of servers (web, database, file) and their components.

Unit 2: Network Fundamentals

Introduction to Computer Networks: LAN, WAN, MAN.
Network Topologies: Bus, Star, Ring, Mesh.
OSI Model and TCP/IP Model: Layers, protocols at each layer (HTTP, HTTPS, FTP, DNS, DHCP, SMTP, POP3, IMAP).
IP Addressing: IPv4, IPv6, Subnetting.
Concept of Ports.

Unit 3: Network Devices and Infrastructure

Network Devices: Hubs, Switches, Routers, Modems, Firewalls, Access Points.
Network Cabling: UTP, STP, Fiber Optic.
Wireless Networking: Wi-Fi standards.
Network Services: DNS, DHCP, VPN, NAT.

Unit 4: Virtualization and Cloud Basics

Introduction to Virtualization: Virtual Machines, Hypervisors (Type 1, Type 2).
Benefits of virtualization in cybersecurity.
Basic concepts of Cloud Computing: IaaS, PaaS, SaaS.
Public, Private, Hybrid Clouds.

Suggested Readings:

1. Andrew S. Tanenbaum, "Computer Networks"
2. Behrouz A. Forouzan, "Data Communications and Networking"
3. Scott Mueller, "Upgrading and Repairing PCs"
4. "CompTIA A+ Core 1 and Core 2 Exam Cram" by David L. Prowse
5. "CompTIA Network+ N10-008 Cert Guide" by Anthony Sequeira
6. "Computer Networking: A Top-Down Approach" by James Kurose and Keith Ross

List of Lab Exercises (only indicative)

Lab 1-2: IT Hardware Familiarization and Assembly: Identify computer components, basic assembly/disassembly of a PC, connecting peripherals.

Lab 3-4: Network Cable Crimping and Configuration: Crimping UTP cables (straight-through, crossover), configuring basic network settings (IP address, subnet mask, gateway).

Lab 5-6: Network Device Configuration: Basic configuration of a router/switch (password, IP address, basic routing/VLANs).

Lab 7-8: Windows Security Hardening: User account management, Firewall configuration, Local Security Policy settings, Event Viewer analysis.

Lab 9-10: Linux Security Hardening: User and group management, File permissions (chmod, chown), SSH hardening, UFW firewall configuration.

Lab 11-12: Basic Network Scanning and Analysis: Using ping, ipconfig/ifconfig, netstat, tracert/traceroute to understand network connectivity.

DDFI-12: Principles of Information and Cyber Security							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Understand core principles of information security.Identify various cyber threats and attack vectors.Explore security models, cryptography, and authentication.Learn incident response and risk management.

Course Outcomes:

CO1: Explain core principles of information security.
CO2: Identify cyber threats and their impacts.
CO3: Understand authentication and encryption mechanisms.
CO4: Develop basic response strategies to security incidents.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	2	1	0	0	0	0
CO2	3	3	2	2	1	1	0	0
CO3	3	3	3	2	2	1	0	0
CO4	2	3	3	2	2	2	1	1

Detailed Syllabus:

Unit 1: Information Security Principles

Confidentiality, Integrity, Availability (CIA Triad).
Authentication, Authorization, Accounting (AAA).
Non-repudiation.
Risk Management: Identification, Assessment, Mitigation.
Security Policies, Standards, Guidelines, Procedures.
Physical Security.

Unit 2: Introduction to Cyber Security

Definition and Scope of Cybersecurity.
Key components of a robust cybersecurity framework.
Roles and responsibilities in cybersecurity.
Cybersecurity vs. Information Security.
Common Security Breaches and their impact.

Unit 3: Cyber Threats and Attacks

Types of Cyber Threats: Malware (Viruses, Worms, Trojans, Ransomware, Spyware, Adware), Phishing, Spear Phishing, Whaling.
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
Man-in-the-Middle (MITM) attacks.
SQL Injection, Cross-Site Scripting (XSS).
Social Engineering techniques.
Advanced Persistent Threats (APTs).

Unit 4: Basic Cyber Security Countermeasures

Antivirus and Anti-malware software.
Firewalls (Hardware and Software).
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
Strong Passwords and Multi-Factor Authentication (MFA).
Data Backup and Recovery.
Security Awareness Training.

Suggested Readings:

1. William Stallings, "Cryptography and Network Security"
2. Nina Godbole and Sunit Belapure, "Cyber Security"
3. Charles P. Pfleeger, "Security in Computing"
4. "CompTIA Security+ SY0-601 Cert Guide" by David L. Prowse (for foundational security concepts)
5. "Hacking: The Art of Exploitation" by Jon Erickson (for deeper understanding of exploitation, more advanced)
6. "The Official (ISC)2 CISSP CBK Reference" (for broader information security concepts, advanced)
7. "Cyber Security: A Practitioner's Guide to Cyber Risks and Threats" by Paul Dorey, Jeremy Hintz, David Livingston

List of Lab Exercises (indicative list):

Lab 1: The CIA Triad and Access Control: Use a virtual machine to set up user permissions on a shared folder to enforce confidentiality, integrity, and availability.

Lab 2: Risk Assessment and Mitigation: Conduct a basic risk assessment for a hypothetical scenario, identify threats and vulnerabilities, and propose mitigation strategies.

Lab 3: Security Policy Analysis: Analyze a real-world security policy, identify its key

components, and create a checklist for new employees based on the policy.

Lab 4: Malware Analysis (Safe Environment): Use a sandboxing tool in a controlled virtual environment to analyze the behavior of pre-approved, non-destructive malware samples.

Lab 5: Phishing Simulation (Controlled Environment): Use a local web server to demonstrate the mechanics of a phishing attack by creating a fake login page and discussing how to identify it.

Lab 6: SQL Injection Attack Simulation: Use a vulnerable web application to demonstrate how to perform a SQL injection attack and discuss its prevention.

Lab 7: Firewall Configuration and Rules: Configure a software firewall on a virtual machine to block specific ports and IP addresses, and verify the rules using a network scanning tool.

Lab 8: Multi-Factor Authentication (MFA) Implementation: Set up and demonstrate multi-factor authentication on a service to understand its security benefits.

Lab 9: Data Backup and Recovery Simulation: Perform a data backup of important files on a virtual machine, simulate data loss, and restore the files from the backup.

DDFI-13: Python Programming for Security							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Learn basic Python programming constructs.Understand scripting for automation in security. Utilize libraries for network and security tasks.

Course Outcomes:

CO1: Write Python scripts using control structures.
CO2: Develop file-handling and pattern-matching scripts.
CO3: Create network-based scripts for packet analysis.
CO4: Automate basic security tasks using Python.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	1	1	0	0	0	0
CO2	3	3	2	1	1	0	0	0
CO3	3	3	3	2	2	1	0	0
CO4	2	3	3	2	3	1	1	0

Detailed Syllabus:

Unit I: Python Basics for Security

Introduction to Python: Data types, control structures, functions, modules
Working with files and directories
Exception handling and logging
Introduction to Python Virtual Environments
Installing packages via pip (e.g., requests, scapy, nmap)

Unit II: Networking and Reconnaissance Automation

Using Python for socket programming
Port scanning using Python and Nmap module
Banner grabbing and service enumeration
DNS queries and WHOIS lookups
HTTP request automation using requests, urllib

Unit III: Cryptography and Hashing

Understanding hashing algorithms: MD5, SHA1, SHA256
Implementing symmetric encryption using PyCryptodome
Password hashing and verification
Using Python for file integrity monitoring
Basic steganography and data encoding/decoding

Unit IV: Forensics and Malware Analysis with Python

Log file parsing and regex filtering
File metadata and timestamps extraction
Using pefile, yara, and pyshark for malware analysis
Memory and process inspection (using psutil)
Writing basic scripts for browser artifact extraction
Report generation and JSON/CSV parsing

Suggested Tools and Libraries:

Python 3.x, pip, venv, Scapy, PyCryptodome, Nmap, YARA, PEfile, psutil, requests, pyshark, BeautifulSoup, os, shutil

Suggested Readings and Resources:

1. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers – TJ O'Connor
2. Black Hat Python – Justin Seitz
3. Python for Offensive PenTest – Hussam Khrais

List of Lab Exercises (only indicative)

Lab 1-2: Python Basics: Hands-on exercises on variables, data types, control flow, functions.

Lab 3-4: File Handling and String Manipulation: Reading/writing files, parsing text, regular expressions for log parsing.

Lab 5-6: Network Programming with Sockets: Developing a simple TCP/UDP client and server.

Lab 7-8: Simple Port Scanner and Banner Grabbing: Implementing a basic port scanner and extracting service banners.

Lab 9-10: Password Generator and Hashing Utility: Creating scripts to generate strong

passwords and compute hash values (MD5, SHA256).

Lab 11-12: Basic System Automation Scripts: Scripts to check system info, manage processes, or perform simple file operations.

DDFI-14: Operating System Security							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	03	03	Lecture	50	25 (15 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance
Practical	01	02	Practical	25	-	3 Hours	TEE (Expt, Lab Record, Viva)

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of FIVE short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of TEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

Understand OS architecture and components.
Study security features in Windows, Linux, iOS, and Android.
Learn system hardening and access control techniques.

Course Outcomes:

CO1: Understand core OS concepts and security roles.
CO2: Apply access control in Windows and Linux.
CO3: Configure security settings on mobile platforms.
CO4: Implement system hardening techniques.

CO-PO Matrix:

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	1	1	0	0	0	0
CO2	3	3	2	2	1	1	1	0
CO3	3	3	2	2	2	1	1	0
CO4	2	3	3	2	2	1	1	1

Detailed Syllabus:

Unit 1: Introduction to OS Security

Goals of OS Security: Confidentiality, Integrity, Availability.
User and Group Management.
File System Permissions.
Authentication and Authorization Mechanisms.
Security patches and updates.

Unit 2: Windows Operating System Security

User Account Control.
Windows Firewall configuration.
Group Policy Management Editor (gpedit.msc) for security settings.
Registry Editor for security configurations.
Windows Security Baselines and templates.
Disk Encryption (BitLocker).
Windows Event Viewer for security auditing.
Introduction to PowerShell for security tasks.

Unit 3: Linux Operating System Security

Linux File System Permissions (chmod, chown).
User and Group management in Linux.
Sudoers file configuration.
SSH Hardening.
Firewall (UFW, Iptables) configuration.
SELinux and AppArmor (basic concepts).
Log file analysis in Linux.
Introduction to shell scripting for security automation.

Unit 4: Mobile OS Security (iOS and Android)

Basic security features of iOS: App Store security, Face ID/Touch ID.
Basic security features of Android: Permissions model, Google Play Protect, Device encryption.
Common mobile attack vectors and mitigation strategies (e.g., malicious apps, insecure Wi-Fi).

Suggested Readings:

1. William Stallings, "Operating Systems: Internals and Design Principles"
2. Brian Ward, "How Linux Works"
3. Andrew S. Tanenbaum, "Modern Operating Systems"
4. "Practical Linux Forensics A Guide for Digital Investigators" by Bruce Nikkel (relevant for Linux hardening)
5. "Windows Internals" (series of books by Mark Russinovich, highly technical but good for deeper understanding)
6. Official Microsoft and Linux Foundation documentation/guides on security.

List of Lab Exercises (indicative only):

Lab 1: User, Group, and File System Management: Create user accounts and groups on both a Windows and a Linux virtual machine. Assign users to groups and then use file system permissions (NTFS permissions on Windows, `chmod`/`chown` on Linux) to enforce different

levels of access to specific files and folders.

Lab 2: Authentication and Patch Management: Configure strong password policies and account lockout policies on a Windows VM. In a separate exercise, demonstrate the process of checking for and applying security updates on both a Windows and a Linux VM, explaining the importance of a regular patching cycle.

Lab 3: Windows Firewall and User Account Control: On a Windows virtual machine, configure the Windows Firewall to block a specific application from accessing the internet and to block all incoming traffic on a particular port. Also, change the User Account Control (UAC) settings and observe the difference in user prompts when attempting to install software.

Lab 4: Group Policy and Security Baselines: Use the Group Policy Management Editor (`gpedit.msc`) on a Windows VM to enforce a complex password policy and disable USB storage access. Introduce the concept of a security baseline and demonstrate how to apply a pre-configured security template.

Lab 5: Disk Encryption and Event Logging: Enable BitLocker on a partition of a Windows virtual machine and demonstrate the encryption/decryption process. In a separate exercise, use the Windows Event Viewer to filter for and analyze security-related events, such as failed logon attempts.

Lab 6: Linux Permissions and Sudoers File: On a Linux virtual machine, use `chmod` and `chown` to modify file permissions and ownership. Then, edit the `/etc/sudoers` file to grant a standard user account specific administrative privileges for a single command, without giving them full `sudo` access.

Lab 7: SSH Hardening and Firewall Configuration: Configure SSH on a Linux VM to disable root login, change the default port, and use key-based authentication instead of passwords. Use a Linux firewall (e.g., UFW or Iptables) to block all incoming traffic except for the newly configured SSH port.

Lab 8: Log Analysis and Shell Scripting: Analyze log files in `/var/log` to identify failed login attempts or other suspicious activity. Write a basic shell script that automates a simple security task, such as checking for the existence of a specific user or a suspicious file.

Lab 9: Mobile OS Security Features: Using an Android emulator (e.g., Android Studio) and a demonstration with a physical iOS device, explore and configure the built-in security features. This includes demonstrating the permissions model for a newly installed app on Android and setting up biometric authentication (Face ID/Touch ID) and device encryption on iOS.

Lab 10: Mobile Security Threats: Simulate a common mobile threat by downloading a pre-approved, benign application from an untrusted source on an Android emulator. Analyze the app's requested permissions and discuss the potential risks of such a download. Discuss mitigation strategies, such as the importance of using official app stores and being wary of insecure Wi-Fi.

Semester II

DDFI-21: Cyber Laws and Privacy Framework in India							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Theory	04	04	Lecture	70	30 (20 / 5 / 5)	3 Hours	TEE/MTE/ Assignment/ Attendance

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of SEVEN short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of FOURTEEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives:

To understand the evolution of cyber laws in India.
To examine various provisions of the Information Technology Act.
To explore the interface of privacy, surveillance, and digital rights.
To analyze the BNS (Bharatiya Nyaya Sanhita) and BNSS (Bharatiya Nagarik Suraksha Sanhita) in cybersecurity contexts.

Course Outcomes:

CO1: Explain the key provisions of the Information Technology Act, 2000, and its role in regulating cyber activities.
CO2: Describe the legal framework for data privacy in India, particularly the Digital Personal Data Protection Act, 2023.
CO3: Analyze the relevance of Bharatiya Nyaya Sanhita (BNS) and Bharatiya Nagarik Suraksha Sanhita (BNSS) to cybercrime investigation and prosecution.
CO4: Understand ethical considerations and intellectual property rights in the context of cybersecurity.

CO-PO Matrix:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	2	-	-	-	3	-	-	-
CO2	2	-	-	-	3	-	-	-
CO3	2	-	-	-	3	-	-	-
CO4	1	-	-	1	3	-	-	-

Detailed Syllabus:

Unit 1: Introduction to Cyber Law in India

Need and Importance of Cyber Laws.
Information Technology Act, 2000 (IT Act): Overview, Amendments.
Digital Signatures and Electronic Governance.
Cyber Crimes: Definitions and Penalties under IT Act. (Sections related to cyber fraud, hacking, data theft, publishing obscene content).
Jurisdiction in Cyber Space.

Unit 2: Privacy Laws in India

Right to Privacy as a Fundamental Right (Puttaswamy Judgement).
Digital Personal Data Protection Act, 2023 (DPDPA): Key provisions, obligations of Data Fiduciaries, rights of Data Principals, Data Protection Board of India.
Sensitive Personal Data or Information (SPDI) Rules.
Data Localization concepts.
Consent and Notice requirements under DPDPA.

Unit 3: BNS and BNSS - Cybersecurity Aspects

Overview of BNS (replacing IPC) and BNSS (replacing CrPC).
Provisions in BNS related to cyber offenses (e.g., electronic evidence, digital evidence tampering, specific cybercrime definitions if explicitly covered).
Provisions in BNSS related to investigation, evidence collection, and trial procedures for cybercrimes (e.g., audio-video recording of search, forensic investigations).
Interplay between IT Act, DPDPA, BNS, and BNSS in addressing cybercrime.

Unit 4: Intellectual Property and Ethical Considerations

Copyright, Trademark, Patent in Digital Domain.
Cyber Squatting, Domain Name Disputes.
Ethics in Cybersecurity: Professional codes of conduct, responsible disclosure, ethical hacking guidelines.
Case studies of major cybercrime incidents and their legal implications.

Suggested Readings:

1. Vakul Sharma, "Information Technology Law and Practice"
2. Talat Fatima, "Cyber Crimes"
3. Pavan Duggal, "Cyber Law: The Indian Perspective"
4. "Information Technology Act, 2000" (Bare Act and commentaries)
5. "Digital Personal Data Protection Act, 2023" (Bare Act and analysis)
6. "Bharatiya Nyaya Sanhita (BNS)" and "Bharatiya Nagarik Suraksha Sanhita (BNSS)" (Relevant sections pertaining to cybercrime)
7. "Cyber Law and Cyber Crimes" by Prof. S.R. Bhansali

DDFI-202: Fundamentals of Digital Forensics								
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks			Exam Duration	Assessment Methods
				External	Internal			
Theory	04	04	Lecture	70	30		3 Hours	TEE/MTE/ Assignment/ Attendance
					20	5 5		

Instructions to paper setter for term-end theory examination: There shall be NINE questions in total. Question number one will be compulsory and will consist of SEVEN short/objective-type questions from the complete syllabus. In addition, there shall be EIGHT questions (two questions from each unit). The student will attempt one question from each unit in addition to the compulsory question. All questions will be of FOURTEEN marks each.

The paper setter will set the paper in both English and Hindi/ mixed mode languages. Accordingly, students can also write the answers the same way.

Course Objectives: To provide students with a foundational understanding of digital forensics, incident response principles, and the handling of digital evidence across various computing environments.

Course Outcomes (COs):

CO1: Explain the fundamental concepts of digital forensics and the incident response life cycle.
CO2: Describe the principles of digital evidence and the importance of chain of custody and forensic soundness.
CO3: Differentiate between various file systems and data storage mechanisms relevant to forensics.
CO4: Apply hashing techniques for verifying data integrity and understand basic data acquisition methods.
CO5: Identify common forensic artifacts from Windows, Linux operating systems, and web browsers.

CO-PO Matrix:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	1	-	1	2	-	-	2
CO2	3	-	-	-	3	-	-	-
CO3	2	2	-	-	-	-	-	-
CO4	2	1	1	1	-	-	-	1
CO5	2	2	-	1	-	-	1	2

Detailed Syllabus:

Unit 1: Introductory topics

Overview of digital forensics: Definition and importance of digital forensics, goals of digital forensics (identification, preservation, analysis, presentation), types of digital forensics (computer, network, mobile, cloud, etc.)

The NIST Digital Forensics Process Model.

Introduction to incident response:Definition and importance of incident response, the incident response life cycle (preparation, identification, containment, eradication, recovery, post-incident analysis), relationship between digital forensics and incident response, roles and responsibilities in an incident response team.

Digital evidence principles:Definition of digital evidence and its characteristics (volatile, fragile, easily altered), admissibility of digital evidence in court (relevance, authenticity, reliability, completeness), chain of custody: importance and documentation, forensic soundness: ensuring integrity of evidence.

Unit 2: File Systems and Data Storage Principles

Introduction to data storage:Types of storage media (HDD, SSD, USB drives, Optical Media, Memory Cards), data organization on storage devices (sectors, clusters, blocks)

Common file systems:FAT (FAT12, FAT16, FAT32): structure, allocation tables, directory entries. NTFS: master file table (MFT), metadata, alternate data streams (ADS). Ext2/Ext3/Ext4 (Linux): iNodes, block groups, directory entries. HFS+ (macOS - conceptual overview)

Data acquisition and preservation:Forensic imaging: bit-stream imaging vs. logical imaging. write blockers (hardware and software). hashing: MD5, SHA-1, SHA-256 for integrity verification. tools for imaging and hashing (e.g., dd, dcfldd, FTK Imager – conceptual introduction)

Unit 3: File Integrity, Hashing, and Evidence Handling

File integrity verification:Purpose of hashing in forensics, understanding cryptographic hashes (one-way, collision resistance), calculating and verifying hashes (practical use cases)

Digital evidence handling best practices:Preparation for incident response and forensics investigations, first responder procedures at the scene, collection of volatile data (ram, , network connections, running processes), collection of non-volatile data (disk images), packaging, transporting, and storing digital evidence

Data recovery fundamentals: Understanding file deletion (logical vs. physical deletion), data carving: recovering deleted files based on file headers/footers, introduction to steganography and cryptography in forensics context (conceptual),

Unit 4: Introduction to OS and Network Forensics

Operating system forensics:Windows forensics: registry analysis, event logs, prefetch files, recycle bin, link files. Linux forensics: log files (syslog, auth.log), bash history, /proc file system, common attack artifacts.

Browser forensics:Internet history, cache, cookies, downloads. browser specific artifacts (e.g., SQLITE databases for Chrome/Firefox). recovering web activity from various browsers.

Network forensics: Introduction to network traffic analysis. packet capturing and protocol analysis (conceptual, Wireshark mention). identifying common network attack indicators from logs.

Suggested Readings:

1. "Guide to Computer Forensics and Investigations" by Bill Nelson, Amelia Phillips, Frank Enfinger, and Christopher Steuart (Latest Edition)
2. "Digital Forensics and Incident Response: A Practical Guide to Forensic Investigations and Incident Response" by Gerard Johansen
3. FTK Documentation and User Guides (AccessData website)
4. Autopsy User Guide and Documentation (sleuthkit.org)
5. "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig (for malware aspects)
6. "The Official (ISC)2 CISSP CBK Reference" (for broader security principles)
7. NIST Special Publications (SP 800-61 Rev. 2: Computer Security Incident Handling Guide, SP 800-86: Guide to Integrating Forensic Techniques into Incident Response)
8. SANS Institute Forensics Blog and Resources
9. "File System Forensic Analysis" by Brian Carrier (more advanced for file system details)
10. Official documentation for relevant OS (Windows, Linux, iOS, Android)
11. "Mobile Forensics – Advanced Investigative Techniques" by Matthew S. Shannon, George J. Mohay, Richard J. W. Smith (more advanced, conceptual reference)

DDFI-23: Digital Forensics and Investigation Lab							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Practical	04	08	Lab-based	100	-	3 Hours	TEE (Expt, Lab record, Viva)

Course Objectives:

1. To provide extensive hands-on experience in setting up forensic environments and performing forensically sound data acquisition.
2. To equip students with practical skills in analyzing various file systems, operating system artifacts, and recovering hidden/deleted data.
3. To enable students to conduct specialized forensic investigations across web browsers, mobile devices, email, and network traffic.
4. To introduce the challenges and methodologies of cloud forensics and train students in producing comprehensive forensic reports for complex digital crime scenarios.

Course Outcomes (COs):

CO1: Set up and configure a forensic workstation, perform forensically sound data acquisition of digital media, and verify its integrity using hashing tools.
CO2: Analyze common file systems (FAT, NTFS, Ext) to identify hidden data and recover deleted files, and extract/interpret critical forensic artifacts from Windows and Linux operating systems.
CO3: Conduct specialized forensic analysis for web browsers, mobile devices, email communications, and network traffic, extracting and interpreting relevant digital evidence.
CO4: Understand cloud data sources and analyze cloud service logs, and integrate findings from multiple forensic sources to investigate complex digital crime scenarios and prepare professional forensic reports.

CO-PO Matrix:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	3	2	-	3	3	2	2	2
CO2	3	3	1	3	3	2	2	2
CO3	3	3	1	3	3	2	2	2
CO4	3	3	2	3	3	3	3	3

List of Lab Experiments/Problems: (indicative list only)

Problem 1: Forensic Workstation Setup and Basic Hashing. Challenge: Configure a virtual forensic workstation by installing essential tools (Autopsy, FTK Imager Lite, hashing utilities,

Wireshark, etc.). Demonstrate proper network isolation for lab work and practice calculating and verifying cryptographic hashes for various files to ensure data integrity.

Problem 2: Digital Evidence Acquisition & Integrity Verification. Challenge: Perform a forensically sound bit-stream acquisition of a target digital media (e.g., a virtual USB drive or small hard disk image). Calculate and compare hashes of both the source and the acquired image to verify data integrity and document the entire chain of custody for the acquisition process.

Problem 3: File System Analysis & Data Carving. Challenge: Load provided disk images (containing FAT32, NTFS, and Ext file systems) into Autopsy and use The Sleuth Kit (TSK) command-line tools to explore their structures. Identify and successfully recover deleted files from unallocated space using data carving techniques, and investigate Alternate Data Streams (ADS) on NTFS partitions.

Problem 4: Windows Operating System Artifact Analysis. Challenge: Given a Windows OS disk image, utilize Autopsy to extract and analyze key forensic artifacts. Your analysis should include interpreting Registry Hives (e.g., user activity, system configurations), examining Event Logs for suspicious activities, and recovering/interpreting Prefetch files, JumpLists, and Recycle Bin contents to reconstruct user and program execution activity.

Problem 5: Linux Operating System Artifact Analysis. Challenge: Given a Linux OS disk image, use Autopsy or command-line TSK tools to extract and analyze common forensic artifacts. Focus on examining system log files (syslog, auth.log), analyzing bash history, and identifying critical system files and configurations that might indicate compromise.

Problem 6: In-depth Analysis with Autopsy & Timeline Creation. Challenge: Conduct a comprehensive digital forensic investigation of a complex simulated case involving a disk image with various artifacts. Utilize advanced Autopsy features (e.g., keyword searching with regular expressions, file type identification, hash set analysis, email parsing) and generate a detailed timeline of events by correlating artifacts from the file system, logs, and web history to reconstruct the incident's narrative.

Problem 7: Browser Forensics Deep Dive. Challenge: Analyze forensic images containing web browser artifacts from multiple popular browsers (Chrome, Firefox, Edge). Extract and interpret Browse history, downloads, cookies, cache, form data, and autofill data to identify user activity, visited websites, and potential evidence of illicit online behavior.

Problem 8: Mobile Forensics (Practical & Simulated). Challenge: Perform a simulated or logical acquisition of an Android emulator (using ADB) or an iOS backup. Analyze the extracted mobile data, including SMS, call logs, contacts, photos, videos, and application-specific data (e.g., WhatsApp, social media app data), to uncover relevant forensic evidence. Use appropriate open-source mobile forensics tools.

Problem 9: Email Forensics (Practical). Challenge: Analyze provided email archives (PST/OST/EML/MBOX files) to extract and interpret email headers for sender tracing, mail server routes, and identification of spoofing. Additionally, recover deleted emails and identify indicators of phishing attempts, malicious attachments (without execution), or suspicious communication patterns.

Problem 10: Network Forensics & Log Analysis. Challenge: Analyze captured network traffic (PCAP files) using Wireshark to identify suspicious network connections, data exfiltration attempts, and reconstruct network conversations. Correlate these network events with relevant

system and server logs (e.g., firewall logs, web server logs) to build a clearer picture of attack patterns.

Problem 11: Cloud Forensics (Conceptual & API/Log Analysis). Challenge: Understand the various data sources and unique challenges of cloud forensics across different service models (IaaS, PaaS, SaaS). Analyze mock cloud logs (e.g., AWS CloudTrail, Azure Activity Logs) to identify suspicious API calls, resource modifications, or unauthorized access attempts in a cloud environment.

Problem 12: Comprehensive Case Study & Forensic Reporting. Challenge: Investigate a complex mock digital crime scenario by integrating all previously learned skills. You will receive multiple digital artifacts (e.g., disk images, mobile backups, email archives, network captures). Conduct a full investigation from identification to detailed analysis, documenting every step, and finally prepare a comprehensive, professional forensic report suitable for presentation to a simulated court or client.

DDFI-24: Project Work							
Course Type	Course Credit	Contact Hours/ Week	Delivery Mode	Maximum Marks		Exam Duration	Assessment Methods
				External	Internal		
Project Work	04	-	-	100	-	-	TEE (presentation / viva voce)

List of Project Topics (indicative only):

Category 1: Case Study & Incident Response Simulation: These projects involve simulating a digital crime and conducting a full forensic investigation.

1. Ransomware Incident Investigation and Recovery:

   Description: Simulate a ransomware attack on a small virtual machine (e.g., by executing harmless ransomware samples from a controlled environment or using a simulated ransomware script). Conduct a forensic analysis to identify the initial infection vector, trace the ransomware's activity, identify encrypted files, and demonstrate recovery techniques (e.g., using shadow copies, file recovery tools on unallocated space, or anti-ransomware decryption tools if applicable for specific strains).

   Focus: Malware forensics, file system analysis, timeline reconstruction, incident response steps.

2. Insider Threat Investigation (Data Exfiltration):

   Description: Design a scenario where a simulated "insider" attempts to exfiltrate sensitive data from a corporate network/system. Investigate common vectors like USB drives, cloud storage synchronization, email attachments, or network shares. Your project involves collecting evidence from various artifacts (e.g., USB device connection logs, browser history, email logs, file access timestamps) to identify the culprit and the leaked data.

   Focus: OS artifact analysis (Windows/Linux), network forensics (if exfiltration via network), data recovery, timeline analysis.

3. Compromised Web Server Investigation:

   Description: Simulate a web server defacement or data breach (e.g., SQL injection leading to data dump, web shell upload). Your task is to analyze web server logs (Apache/IIS), database logs, and file system changes to pinpoint the vulnerability exploited, the attacker's actions, and potentially recover lost data.

   Focus: Log analysis, web forensics, file system integrity, vulnerability identification.

4. Phishing Attack Investigation:

   Description: Analyze a collection of suspicious emails (PST/EML files) from a simulated phishing incident. Extract email headers, identify malicious links/attachments, trace the origin of the emails, and determine potential victims. The project can also include a simulated phishing attempt (in a controlled environment) to capture and analyze the artifacts.

Focus: Email forensics, header analysis, open-source intelligence (OSINT) for link/domain analysis.

Category 2: Tool Development & Enhancement (using Python/Scripting): These projects involve developing small utilities or enhancing existing open-source tools to assist in forensic tasks.

1. Automated Log File Analyzer (Python-based):

Description: Develop a Python script that can parse common log files (e.g., Windows Event Logs exported to CSV/XML, Apache access logs, Linux auth.log). The script should identify and flag suspicious patterns, authentication failures, or specific events based on user-defined rules.

Focus: Python programming, regular expressions, log parsing, basic anomaly detection.

2. Mobile Device Data Extractor/Analyzer (for specific artifacts):

Description: Focus on a specific mobile artifact (e.g., SMS messages, call logs, WhatsApp chat database) from a logical acquisition of an Android emulator. Develop a Python script to parse and present this data in a readable, forensically sound format.

Focus: Python programming, SQLite database interaction, mobile OS data structures.

3. File Carving Utility for Specific File Types:

Description: Develop a basic Python script that can carve (recover) specific file types (e.g., JPG, PDF, DOCX) from raw disk images or unallocated space by identifying file headers and footers. Compare its effectiveness with existing tools.

Focus: Python programming, file formats, binary data analysis.

4. Digital Evidence Hashing and Verification Tool:

Description: Create a Python-based utility that can calculate MD5, SHA1, and SHA256 hashes of files or directories. The tool should also be able to verify the integrity of a file/image by comparing its current hash with a previously recorded hash value. Include a simple GUI if possible.

Focus: Python programming, cryptographic hashing, GUI development (optional).

Category 3: Comparative Analysis & Research: These projects involve evaluating and comparing different forensic techniques or tools.

1. Comparative Analysis of Disk Imaging Tools:

Description: Compare the features, performance (speed, image size), and integrity verification capabilities of multiple open-source and/or trial versions of commercial disk imaging tools (e.g., FTK Imager, dd, dcfldd, Guymager). Document the process and present a detailed report on their strengths and weaknesses.

Focus: Tool evaluation, methodology, critical analysis.

2. Effectiveness of Data Wiping Techniques:

Description: Investigate various data wiping techniques (e.g., single pass zero, DoD 5220.22-M, Gutmann method). Apply these techniques to a test drive and then attempt to recover data using forensic tools to assess the effectiveness of each method.

Focus: Data recovery, anti-forensics, practical experimentation.

3. Forensic Analysis of Encrypted vs. Non-Encrypted Drives:

Description: Prepare a drive with various types of data, then encrypt a portion/whole of it using common encryption methods (e.g., BitLocker, VeraCrypt). Attempt to perform forensic analysis on both the unencrypted and encrypted sections, documenting the challenges and possibilities of data recovery and analysis on encrypted media.

Focus: Encryption technologies, challenges in forensics, data recovery.

Category 4: Emerging Areas in Forensics: These projects touch upon newer and evolving domains within digital forensics.

1. Basic IoT Device Forensics (e.g., Smart Bulb/Speaker Logs):

Description: If accessible and safe, identify a simple IoT device (e.g., a smart bulb, an old router) and attempt to extract logs or configuration data from it. Analyze this data for user activity or network connections. If direct access is not possible, focus on analyzing network traffic generated by the IoT device.

Focus: IoT ecosystem understanding, network traffic analysis, device-specific data extraction challenges.

2. Social Media Artifact Analysis:

Description: Focus on collecting and analyzing publicly available data from a specific social media platform (e.g., Twitter using APIs, or manually scraped public profiles) related to a simulated event. Identify techniques for extracting user posts, connections, and timelines that could be forensically relevant. (Emphasize ethical data collection and privacy).

Focus: OSINT, data scraping (ethical), social media data structures.

3. Introduction to Blockchain Forensics (Conceptual/Tool-based):

Description: Investigate how blockchain transactions (e.g., Bitcoin) can be traced for forensic purposes. Use open-source blockchain explorers to trace specific transactions and analyze patterns, understanding how cryptocurrency movements can be mapped.

Focus: Blockchain technology, cryptocurrency tracing, open-source blockchain tools.

Important Considerations for Diploma Projects:

Scope: Projects should be manageable within the diploma timeframe (typically 1 semester or 1 academic year).

Ethical Hacking vs. Forensics: Ensure projects strictly adhere to ethical guidelines. All data used should be consent-based, simulated, or publicly available. No real-world unauthorized access or investigation should be performed.

Documentation: A comprehensive project report is crucial, detailing:

1. Problem Statement and Objectives
2. Background and Literature Review
3. Methodology (Tools used, steps taken, ethical considerations)
4. Findings and Analysis (with screenshots and relevant data)
5. Conclusions and Future Work
6. References