Telangana Council of Higher Education (TGCHE)
Govt. of Telangana

Common Syllabus for All Universities in Telangana

Syllabus of

B.Sc. (Hons.)
Digital Forensics
and
Cyber Security

Duration: 4 years

B.Sc. (Hons.)
Digital Forensics and Cyber Security

Programme	B.Sc. (Honours) Digital Forensics and Cyber Security
Duration	4 years (3 Years / 6 Semesters, with recommended Sem VII-VIII internship/research extension)
Core paper code pattern	C-101 to C-108 across Semesters I-IV
Elective paper code pattern	E-109 A/B, E-110 A/B, E-111 A/B and E-112 A/B across Semesters V-VI
Design rule	Every semester contains at least one Chemistry, one Digital Forensics paper and one Cyber Security / DFIR paper

B.Sc. (Hons.)
Digital Forensics and Cyber Security
Credit Grid

Courses	Paper / Stream	Papers	Total Credits	I	II	III	IV	V	VI
Core Courses - DSC	Major-1	6	30	5	5	5	5	5	5
	Major-2	6	30	5	5	5	5	5	5
	Minor-1	4	20	5	5	5	5	-	-
MIL/AEC (First Language)	English	4	16	4	4	4	4	-	-
Second Language	Hindi/Telugu/Urdu/Others	4	16	4	4	4	4	-	-
GE/Multi-disciplinary Course	MDC1	1	4	-	-	-	-	4	-
SEC Skill Enhancement Courses	SEC1, SEC2	2	4	-	-	-	-	2	2
	SEC3, SEC4	2	4	-	-	-	-	2	2
Value Added Course (VAC)	VAC1, VAC2	2	4	-	-	-	-	1+1*	1+1*
Internship	Internship/ Project	1	4	-	-	-	-	-	4
Total credits each semester		32	132	23	23	23	23	20	20
Total Credits till Sem VI				**132**					
Credits for Internship during Sem VII & VIII		Sem VII	14	Project Work					
		Sem VIII	14	Project Work					
Total Credits				**160**					

Note:

1. Under the proposed CBCS structure for Undergraduate Programmes (2026-27), students will pursue two Majors and one Minor, collectively referred to as Discipline Specific Core (DSC). Both Major and Minor courses will remain integrated up to the fourth semester, after which students will have the option to drop one Minor Course in both the fifth and sixth semesters. The syllabus and credits for Major and Minor courses will remain consistent up to the fourth semester, whereas the Major continues through the fifth and sixth semesters.
2. * represents - Community Outreach / Summer Internship/ Apprenticeship/ etc., as per UGC guidelines

Paper Code Map

Semester	DF Code	Digital Forensics / Investigation Paper	Track	Credits	CS Code	Cyber Security / DFIR Paper	Track	Credits
Semester I	C-101	Introduction to Digital Forensics, Evidence Handling & Cyber Forensics	Digital Forensics	5	C-102	Computer Fundamentals & Cyber Security Fundamentals	Cyber Security	5
Semester II	C-103	Cyber Crime Investigation & Database Evidence	Digital Forensics / Legal	5	C-104	Network Fundamentals & Secure Communications	Cyber Security	5
Semester III	C-105	Digital Crime Scene Management, Acquisition & Imaging	Digital Forensics	5	C-106	Security Governance, Risk, Asset Security & Indian Cyber Law	Cyber Security / GRC	5
Semester IV	C-107	Operating System Forensics: Windows, Linux & Android Artifacts	Digital Forensics	5	C-108	Security Architecture, IAM, Applied Cryptography & Secure SDLC	Cyber Security	5
Semester V	E-109 A/B	IoT Device Forensics OR Network Forensics & Packet Analysis	Digital Forensics Elective	5	E-110 A/B	Multimedia/Deepfake Forensics OR AI Security & AI Forensics	Cyber Security / Hybrid Elective	5
Semester VI	E-111 A/B	Python for Forensic Automation OR Blockchain & Cryptocurrency Forensics	Digital Forensics Elective	5	E-112 A/B	OSINT, Threat Intelligence & Dark Web Investigation OR Live Data Collection, IR & Threat Hunting	Cyber Security / DFIR Elective	5

Semester-Wise Curriculum at a Glance

Sem	Digital Forensics Coverage	Cyber Security / DFIR Coverage	Core Technical Practices
I	C-101: Digital-forensics foundations, evidence handling and cyber forensics	C-102: computer fundamentals, CIA triad, cyber security basics and cyber hygiene	Evidence handling, hashing, VM lab, OS artefact identification
II	C-103: cybercrime investigation and database evidence	C-104: network fundamentals and secure communications	SQL/log extraction, email headers, Wireshark, secure network configuration
III	C-105: digital crime-scene management, acquisition and imaging	C-106: governance, risk, asset security and Indian cyber law	Imaging, chain of custody, risk register, compliance checklist
IV	C-107: operating-system forensics across Windows, Linux and Android	C-108: architecture, IAM, cryptography and secure SDLC	Registry/log analysis, threat modeling, PKI/TLS, OWASP testing
V	E-109 A/B: IoT device forensics OR network forensics	E-110 A/B: multimedia/deep fake forensics OR AI security and AI forensics	IoT/PCAP analysis, deepfake/media validation, AI threat modeling
VI	E-111 A/B: Python automation OR blockchain/cryptocurrency forensics	E-112 A/B: OSINT/threat intelligence/dark web OR live data collection, IR and threat hunting	Python parsers, blockchain tracing, OSINT, SIEM, live response, IR report

B.Sc. (Hons.) Digital Forensics and Cyber Security

Programme Outcomes (POs)

PO1: Apply foundational and applied knowledge of cyber security, digital forensics, network security, incident response and cyber law to investigate and mitigate cyber threats.

PO2: Analyze cyber incidents, evaluate digital evidence and develop effective technical and investigative solutions for security challenges.

PO3: Demonstrate proficiency in forensic tools, scripting, network analysis, operating systems and cyber security technologies.

PO4: Apply emerging technologies, tools and methodologies in cyber security and digital forensics for academic and professional practice.

PO5: Apply ethical practices, legal standards and professional responsibilities while handling digital evidence and conducting cyber investigations.

PO6: Prepare technical reports, forensic documentation and incident reports effectively.

PO7: Work collaboratively in multidisciplinary teams and demonstrate leadership in security and investigation activities.

PO8: Adapt to evolving cyber threats, technologies and forensic methodologies through lifelong learning.

Programme Specific Outcomes (PSOs)

PSO1: Acquire, preserve, analyze and report digital evidence from computers, mobile devices, networks and IoT environments using standard forensic procedures.

PSO2: Implement cyber security controls, conduct threat hunting, incident response and vulnerability assessment using industry-standard tools.

PSO3: Develop automation scripts, perform OSINT and threat intelligence analysis and apply AI-assisted techniques in cyber investigations.

PSO4: Apply cyber laws, governance frameworks, compliance standards and ethical principles relevant to cyber security and digital forensics.

B.Sc. (Hons.) Digital Forensics and Cyber Security
SEMESTER I

Paper C-101: Introduction to Digital Forensics, Evidence Handling & Cyber Forensics

Course Objectives (COBs):

COB1: To introduce the fundamentals of digital forensics, cybercrime and electronic evidence.
COB2: To develop knowledge of digital evidence acquisition, preservation and integrity maintenance procedures.
COB3: To familiarize students with forensic tools and techniques used in digital investigations and analysis.
COB4: To provide understanding of cybercrime investigation procedures, legal aspects and professional ethics in digital forensics.

Course Outcomes (COs):

CO1: Understand fundamentals of digital forensics, cybercrime and digital evidence.
CO2: Apply evidence acquisition, preservation and integrity verification techniques.
CO3: Use forensic tools and techniques for digital evidence analysis and reporting.
CO4: Demonstrate knowledge of cybercrime investigation, legal procedures and professional ethics.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	2	1	2	1	1	2	3	1	1	2
CO2	3	3	3	1	2	2	1	2	3	2	1	2
CO3	3	3	3	2	2	2	1	2	3	2	2	2
CO4	3	3	2	2	3	3	2	2	2	2	1	3

Theory **Credits: 4**

UNIT I: Fundamentals of Digital and Cyber Forensics

Introduction to Forensic Science: Definition and scope of Forensic Science - Branches of Forensic Science - Role of Forensic Science investigations

Basics of Digital Forensics: Definition and importance of digital forensics – Evolution of cyber forensics – Scope and applications of digital forensics

Cybercrime and Digital Evidence: Types of Cybercrimes – Characteristics of digital evidence – Probative value of electronic evidence

Digital Forensic Investigation: Role of forensic investigator – Stages of digital investigation – Challenges in cyber forensic investigations

Legal and Ethical Aspects: Admissibility of digital evidence – Ethical responsibilities of investigators – Emerging trends in cyber forensics

UNIT II: Digital Evidence, Acquisition and Preservation

Types of Digital Evidence: Volatile evidence – Non-volatile evidence – Sources of digital evidence

Digital Data and Artefacts: File systems and storage media – Metadata and timestamps – Network artefacts and logs

Evidence Collection Procedures: Identification of evidences – Seizure of digital evidences – Packaging and transportation of evidence

Preservation of Digital Evidence: Chain of custody procedures - Write-blocking techniques - Evidence preservation methods

Integrity Verification: Concepts of hashing - SHA and MD5 algorithms - Verification of forensic integrity

Unit III: Digital Forensic Tools and Techniques

Forensic Imaging Techniques: Disk acquisition methods - Live and dead acquisition - Bit-stream imaging

Forensic Software Tools: Introduction to FTK Imager - Introduction to Autopsy - Features of forensic analysis tools

Data Recovery and Analysis: Deleted file recovery - Password recovery techniques - Analysis of storage devices

Internet and Communication Analysis: Browser history examination - Email forensic analysis - Log file analysis

Documentation and Reporting: Maintenance of case diary - Documentation standards - Preparation of forensic reports

Unit IV: Cybercrime Investigation and Professional Practices

Cybercrime Investigation Process: Complaint registration - Search and seizure procedures - Digital evidence examination

Analysis and Interpretation: Evidence interpretation methods - Correlation of digital artefacts - Preparation of expert opinion

Courtroom Presentation: Presentation of forensic findings - Expert witness testimony - Courtroom procedures for digital evidence

Professional Conduct and Safety: Professional ethics in investigations - Confidentiality and privacy - Investigator safety precautions

Cyber Laws and Future Trends: National cyber laws - International cyber regulations - Future challenges in cyber forensics

Practicals **Credits: 1**

1. Preparation of mock seizure memo for digital evidence collection.
2. Demonstration of evidence bagging, labelling and sealing procedures for electronic devices.
3. Maintenance of chain-of-custody forms for seized digital evidence.

4. Examination of file metadata and timestamps from digital files.
5. Collection and analysis of browser history, cookies and cache data.
6. Demonstration of SHA-256 and MD5 hash generation for integrity verification.
7. Creation of forensic disk image using FTK Imager.
8. Preparation of digital forensic case diary and investigation notes.

References:

1. Thomas J. Holt, Adam M Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics An Introduction, 3rd Edition, Routledge, 2022
2. Eoghan Casey, Digital Evidence and Computer Crime Forensic Science, Computers and the Internet, 3rd Edition, Academic Press, 2011
3. Bill Nelson, Amelia Phillips, Chris Steuart, Guide to Computer Forensics and Investigations, 6th Edition, Cengage, 2018

Paper C-102: Computer Fundamentals & Cyber Security Fundamentals

Course Objectives (COBs):

COB1: To introduce the fundamentals of computer systems, architecture and operating systems relevant to cyber security and digital forensics.

COB2: To develop understanding of system artefacts, storage structures and operating system environments including Windows, Linux and Android.

COB3: To provide knowledge of cyber security principles, threats, vulnerabilities, malware and security controls.

COB4: To familiarize students with endpoint security practices, cyber security frameworks and professional responsibilities in cyber security environments.

Course Outcomes (COs):

CO1: Understand computer architecture, operating systems and system artefacts relevant to cyber security and digital forensics.

CO2: Identify and analyze system artefacts, logs and user activity traces in Windows, Linux and Android environments.

CO3: Apply cyber security principles to identify threats, vulnerabilities, malware and appropriate security controls.

CO4: Demonstrate knowledge of endpoint security, cyber security frameworks, secure practices and professional responsibilities.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	3	1	1	1	1	2	2	3	1	1
CO2	3	3	3	2	2	2	1	2	3	2	1	1
CO3	3	3	3	2	2	2	1	2	2	3	1	2
CO4	3	2	2	2	3	3	2	3	1	3	1	3

Theory **Credits: 4**

Unit I: Computer Fundamentals and Architecture

Basics of Computer Systems: Definition and characteristics of computers - Generations of computers - Types of computer systems

Computer Architecture: Central Processing Unit (CPU) - Memory units: RAM and ROM - Input and output devices

Storage and Peripheral Devices: Primary and secondary storage - Storage media and devices - Peripheral device interfaces

Firmware and Virtualization: BIOS and UEFI firmware - Concept of virtualization - Virtual machines and hypervisors

Computer Performance and Maintenance: System performance factors - Hardware troubleshooting basics - Preventive maintenance practices

Unit II: Operating Systems and System Artefacts

Introduction to Operating Systems: Functions of operating systems - Types of operating systems - User interface and command-line interface

Windows Operating System: Windows file system basics - Registry structure and functions - Windows event logs and artefacts

Linux Operating System: Linux file system hierarchy - Linux user and permission management - Linux log files and system artefacts

Android Operating System: Android architecture overview - Android file structure - Android application and user artefacts

System Artefacts and Data Identification: Temporary files and cache data - User activity traces - Identification of system artefacts

Unit III: Cyber Security Fundamentals

Principles of Information Security: Confidentiality, Integrity and Availability (CIA Triad) - Authentication, Authorization and Accounting (AAA) - Information security objectives

Threats and Threat Actors: Types of cyber threats - Threat actors and motivations - Social engineering attacks

Vulnerabilities and Exploits: System vulnerabilities - Exploit concepts and attack vectors - Vulnerability assessment basics

Malware and Cyber Attacks: Types of malware - Malware propagation techniques - Indicators of compromise

Security Controls and Risk Reduction: Administrative controls - Technical and physical controls - Security awareness and cyber hygiene

Unit IV: Endpoint Security and Cyber Security Frameworks

Endpoint Security: Endpoint protection concepts - Anti-malware and antivirus tools - Secure endpoint configuration

Patch Management and Backup: Importance of software updates - Patch management process - Data backup and recovery methods

Secure Configuration Practices: Password management - Multi-factor authentication - Secure browsing and email practices

Introduction to NIST CSF 2.0: Overview of NIST Cybersecurity Framework - Core functions of NIST CSF 2.0 - Framework implementation basics

Security Policies and Professional Practices: Organizational security policies - Incident reporting procedures - Ethical and professional responsibilities

Practicals **Credits: 1**

1. Installation and configuration of virtual machines using virtualization software.
2. Basic system information gathering using command-line tools.
3. Identification of vulnerabilities using basic vulnerability scanning tools.
4. Demonstration of malware detection using antivirus software.

5. Performing software updates and patch management exercises.
6. Configuration of password security and multi-factor authentication.
7. Backup and restoration of files and system data.
8. Case study analysis on cyber hygiene and incident response procedures.

References:

1. Neeharika Adabala: Fundamentals of computers by V. Rajaraman, 6th edition, PHI Learning, 2014.
2. William Stallings: Computer organization & architecture, 11th edition, Pearson, 2022.
3. Cory Altheide, Harlan Carvey: Digital Forensics with Open Source Tools, 1st edition, Syngress, 2011.
4. Christopher Grow, Philip A. Craig, Jr., Donald Short: Cybersecurity Essentials, by Charles J. Brooks, 1st Edition, John Wiley & Sons, Inc., 2018

B.Sc. (Hons.) Digital Forensics and Cyber Security
SEMESTER II

Paper C-103: Cyber Crime Investigation & Database Evidence

Course Objectives (COBs):

COB1: To introduce the fundamentals, types and impact of cybercrimes and digital offences.
COB2: To develop understanding of cybercrime complaint handling, first response procedures and evidence preservation techniques.
COB3: To provide knowledge of database fundamentals, SQL operations and database logs relevant to cybercrime investigations.
COB4: To familiarize students with database evidence analysis, cybercrime case studies and preparation of investigation reports.

Course Outcomes (COs):

CO1: Understand cybercrime concepts, digital offences and challenges in cybercrime investigations.
CO2: Apply cybercrime complaint handling, evidence identification and chain-of-custody procedures.
CO3: Use database concepts, SQL queries and audit logs for digital investigations.
CO4: Analyze database evidence, communication records and cybercrime case studies for forensic reporting.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	2	1	2	1	1	2	2	2	1	2
CO2	3	3	3	1	3	2	1	2	3	2	1	2
CO3	3	3	3	2	2	2	1	2	2	2	2	1
CO4	3	3	2	2	3	3	2	2	3	2	2	3

Theory Syllabus **Credits: 4**

Unit I: Introduction to Cybercrime and Digital Offences

Fundamentals of Cybercrime: Definition and scope of cybercrime - Evolution of cyber offences - Impact of cybercrime on society

Types of Cybercrimes: Phishing and online fraud - Identity theft and impersonation - Cyber stalking and online harassment

Financial and Organized Cybercrimes: Ransomware attacks - Online extortion techniques - Banking and financial cyber frauds

Online Abuse and Emerging Threats: Social media crimes - Child exploitation and online abuse - Dark web and anonymous crimes

Investigation Challenges in Cybercrime: Jurisdictional issues - Challenges in evidence collection - Emerging trends in cybercrime

Unit II: Cybercrime Complaint Handling and First Response

Complaint Intake Procedures: Cybercrime complaint registration - FIR and incident documentation - Preliminary verification procedures

Role of First Responders: Duties of first responders - Securing the crime scene - Initial evidence preservation steps

Evidence Identification and Triage: Identification of digital evidence - Evidence prioritization and triage - Volatile and non-volatile evidence handling

Documentation and Chain of Custody: Preparation of seizure memos - Chain of custody procedures - Documentation standards in investigations

Coordination in Cybercrime Response: Interaction with law enforcement agencies - Coordination with CERT organizations - Reporting and escalation mechanisms

Unit III: Database Fundamentals and SQL for Investigations

Basics of Databases: Definition and types of databases - Relational database model - Database management systems (DBMS)

Database Structures and Components: Tables, rows and columns - Primary and foreign keys - Relationships among tables

SQL Fundamentals: Data definition and manipulation commands - SELECT, INSERT, UPDATE and DELETE queries - Filtering and sorting data using SQL

Transactions and Audit Trails: Database transactions - Audit trails and logging mechanisms - Database security and access control

Database Logs and Evidentiary Value: Types of database logs - Timestamp records and synchronization - Importance of database logs in investigations

Unit IV: Database Evidence and Cybercrime Case Analysis

Database Evidence Collection: Identification of database evidence - Extraction of evidentiary records - Preservation of database integrity

User Activity and Log Analysis: User activity tracking - Application log analysis - Correlation of timestamps and events

Data Recovery and Examination: Basics of deleted data recovery - Recovery of **database records - Verification of recovered evidence**

Email and Structured Data Analysis: Email header examination - Structured log analysis - Correlation of communication records

Cybercrime Case Studies and Reporting: Analysis of cybercrime case studies - Preparation of evidence matrix - Drafting of cybercrime investigation reports

Practicals **Credits: 1**

1. Preparation of cybercrime complaint and FIR documentation.
2. Mock cybercrime scene handling and first responder exercise.
3. Demonstration of chain-of-custody documentation for digital evidence.
4. Identification and classification of database records relevant to investigations.
5. Creation of simple relational database tables using SQL.
6. Email header analysis and tracing exercises.
7. Demonstration of basic deleted data recovery techniques.
8. Preparation of cybercrime investigation case diary and report.

References:

1. Sunit Belapure, Nina Godbole: Cyber Security Kindle Edition, Wiley, 2011
2. Bill Nelson, Amelia, Phillips, Christopher Steuart: Guide to Computer Forensics and Investigations, 7th edition, Cengage Learning, 2024
3. Abraham Silberschatz, Henry F. Korth and S. Sudarshan: Database System Concepts, 7th edition, McGraw-Hill, 2020
4. Pete Finnigan: Oracle Incident Response and Forensics, Preparing for and Responding to Data Breaches, Apress, 2017

Paper C-104: Network Fundamentals & Secure Communications

Course Objectives (COBs):

COB1: To introduce the fundamentals of computer networks, communication protocols and network architectures.

COB2: To develop understanding of network infrastructure components, enterprise networking and wireless communication technologies.

COB3: To provide knowledge of network security mechanisms, secure protocols and access control techniques.

COB4: To familiarize students with network monitoring, packet analysis and secure communication practices in modern networks.

Course Outcomes (COs):

CO1: Understand computer networking concepts, protocols, addressing and communication models.

CO2: Apply routing, switching, VLANs and wireless networking concepts in enterprise networks.

CO3: Demonstrate knowledge of network security controls, secure protocols and access control mechanisms.

CO4: Analyze network traffic, packet captures and attack patterns using network monitoring techniques.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	3	1	1	1	1	2	2	3	1	1
CO2	3	3	3	2	2	2	1	2	2	3	1	1
CO3	3	3	3	2	3	2	1	2	2	3	1	2
CO4	3	3	3	2	2	3	1	2	3	3	2	1

Theory **Credits: 4**

Unit I: Fundamentals of Computer Networks

Introduction to Networking: Definition and scope of computer networks - Types of computer networks - Network topologies and architectures

OSI and TCP/IP Models: Layers of the OSI model - TCP/IP protocol suite - Comparison of OSI and TCP/IP models

IP Addressing and Network Configuration: IPv4 addressing and subnetting - IPv6 addressing concepts - Static and dynamic IP configuration

Core Network Protocols: DNS and DHCP protocols - ARP and ICMP protocols - TCP and UDP communication protocols

Data Transmission and Communication: Packet switching concepts - Data encapsulation and decapsulation - Network communication workflow

Unit II: Network Infrastructure and Enterprise Networking

Routing Fundamentals: Functions of routers - Static and dynamic routing - Routing protocols overview

Switching Technologies: Functions of switches - MAC addressing and switching - Broadcast and collision domains

Network Address Translation and VLANs: Concepts of NAT - Types of NAT - VLAN configuration and applications

Wireless Networking Basics: Wireless communication standards - Wi-Fi security mechanisms - Wireless network components

Enterprise Network Design: Enterprise network architecture - Network scalability and redundancy - Basics of network documentation

Unit III: Network Security and Secure Protocols

Fundamentals of Network Security: Principles of secure communication - Threats to network security - Security objectives in networks

Firewalls and Intrusion Detection: Types of firewalls - Intrusion Detection Systems (IDS) - Intrusion Prevention Systems (IPS)

Secure Remote Communication: Virtual Private Networks (VPNs) - Secure tunneling concepts - Remote access security

Network Access Control and Segmentation: Network Access Control (NAC) - Network segmentation techniques - Access control mechanisms

Secure Network Protocols: HTTPS and TLS protocols - Secure Shell (SSH) basics - Secure communication practices

Unit IV: Network Monitoring, Traffic Analysis and Secure Communication

Packet Capture and Analysis: Concepts of packet capture - Packet analysis techniques - Introduction to Wireshark

Network Monitoring and Telemetry: NetFlow fundamentals - DNS telemetry concepts - Monitoring network traffic patterns

Introductory Attack Traffic Analysis: Types of network attacks - Identification of suspicious traffic - Indicators of compromise in networks

CIA Triad in Network Security: Confidentiality in communication networks - Integrity protection mechanisms - Availability and redundancy measures

Secure Communication Practices: Secure network design principles - Best practices for communication security - Emerging trends in secure networking

Practicals **Credits: 1**

1. Demonstration of OSI and TCP/IP protocol communication using network simulators.
2. IPv4 and IPv6.addressing and sub netting exercises.
3. Packet capture and protocol identification using Wireshark.
4. Configuration of basic routing and switching functions.
5. Wireless network setup and security configuration.

6. Firewall rule configuration and traffic filtering demonstration.
7. Introduction to IDS/IPS rule configuration in a lab environment.
8. Demonstration of VPN setup for secure communication.

References:

1. James F. Kurose, Keith W. Ross: Computer Networking, A Top-down Approach, 8th edition, Pearson, 2022
2. Behrouz A. Forouzan: Data Communications and Networking Global, 5th Edition, McGraw-Hill Education, 2012
3. William Stallings: Network security essentials applications and standards, 3rd edition, Prentice Hall, 2007
4. William Stallings: Cryptography and Network Security, Principles and Practice 7th edition, Pearson, 2016
5. Chris Sanders: Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, 3rd Edition, No Starch Press, 2017
6. Richard Bejtlich: The Practice of Network Security Monitoring - Understanding Incident Detection and Response, No Starch Press, 2013

B.Sc. (Hons.) Digital Forensics and Cyber Security
SEMESTER III

Paper C-105: Digital Crime Scene Management, Acquisition & Imaging

Course Objectives (COBs):

COB1: To introduce the concepts and procedures involved in digital crime-scene management and evidence handling.
COB2: To develop understanding of forensic data acquisition methods, volatile data collection and evidence preservation techniques.
COB3: To provide knowledge of disk imaging, forensic integrity verification and timeline reconstruction methods.
COB4: To familiarize students with forensic standards, documentation practices, reporting procedures and legal considerations in digital investigations.

Course Outcomes (COs):

CO1: Understand digital crime-scene management procedures, evidence identification and preservation techniques.
CO2: Apply live and dead acquisition methods for collection of volatile and non-volatile digital evidence.
CO3: Use forensic imaging, hashing and timeline reconstruction techniques for digital investigations.
CO4: Demonstrate knowledge of forensic standards, documentation, reporting and legal procedures in digital forensics.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	2	1	2	2	1	2	3	1	1	2
CO2	3	3	3	2	2	2	1	2	3	2	1	2
CO3	3	3	3	2	2	2	1	2	3	2	2	2
CO4	3	2	2	2	3	3	2	2	2	1	1	3

Theory **Credits: 4**

Unit I: Digital Crime Scene Management

Fundamentals of Digital Crime Scenes: Definition and scope of digital crime scenes - Types of digital crime scenes - Role of digital forensic investigators
Crime Scene Planning and Preparation: Crime-scene planning procedures - Risk assessment and investigator safety - Selection of tools and equipment
Search and Identification of Evidence: Identification of evidence sources - Search techniques for digital devices - Prioritization of digital evidence

Seizure and Documentation Procedures: Seizure of digital devices - Evidence labeling and packaging - Preparation of seizure memos

Evidence Handling and Preservation: Chain of custody procedures - Transportation and storage of evidence - Preservation of evidence integrity

Unit II: Data Acquisition and Volatile Evidence Collection

Fundamentals of Data Acquisition: Definition and objectives of acquisition - Types of acquisition methods - Importance of forensic soundness

Live and Dead Acquisition: Live acquisition techniques - Dead acquisition methods - Comparison of live and dead acquisition

Volatile Data Collection: Types of volatile data - Memory and running process acquisition - Network connection and session capture

Shutdown and System Handling Decision: Safe shutdown procedures - Risks associated with shutdown - Decision-making during acquisition

Acquisition Documentation: Recording acquisition details - Documentation standards - Verification of acquisition process

Unit III: Disk Imaging and Timeline Reconstruction

Disk Imaging Fundamentals: Concepts of forensic imaging - Bit-stream image acquisition - Image formats and storage

Hashing and Integrity Verification: Purpose of hash functions - MD5 and SHA hash algorithms - Verification of forensic images

File Systems and Artefacts: Basics of file systems - File-system artefacts and metadata - Deleted file and partition artefacts

Timeline Reconstruction: Importance of timeline analysis - File metadata examination - Event and log correlation

Forensic Analysis Techniques: Preliminary forensic examination - Artefact interpretation - Reporting of findings

Unit IV: Forensic Standards, Documentation and Reporting

Digital Forensic Process Models: Investigation process models - Phases of forensic examination - Best practices in digital investigations

International Standards in Digital Forensics: Overview of ISO/IEC 27037 - ISO/IEC 27041 and 27042 guidelines - ISO/IEC 27043 incident investigation principles

Documentation and Photography: Preparation of evidence registers - Photograph logs and scene documentation - Case diary maintenance

Report Writing and Evidence Storage: Drafting forensic reports - Evidence storage procedures - Long-term preservation of evidence

Professional and Legal Considerations: Ethical responsibilities of investigators - Legal admissibility of evidence - Courtroom presentation of forensic findings

Ramesh

Practicals **Credits: 1**

1. Mock crime-scene tabletop exercise for digital investigations.
2. Demonstration of live and dead acquisition procedures.
3. Collection of volatile memory and running process information.
4. Creation of forensic disk images using open-source tools.
5. Verification of forensic image integrity using MD5 and SHA hashes.
6. Examination of basic file-system artefacts and metadata.
7. Timeline creation using file metadata and log sources.
8. Correlation of system logs and event timestamps.

References:

1. Bill Nelson, Amelia, Phillips, Christopher Steuart,: Guide to Computer Forensics and Investigations, 7th edition, Cengage Learning, 2024
2. Eoghan Casey: Digital Evidence and Computer Crime, 3rd edition, Academic Press, 2011
3. Jason T. Luttgens, Matthew Pepe and Kevin Mandia: Incident Response & Computer Forensics, 3rd Edition, McGraw Hill Education, 2014
4. Brian Carrier: File System Forensic Analysis, 1st Edition, Addison-Wesley, 2005

Paper C-106: Security Governance, Risk, Asset Security & Indian Cyber Law

Course Objectives (COBs):

COB1: To introduce the principles of security governance, risk management and professional ethics in cyber security.

COB2: To develop understanding of security frameworks, standards and organizational security controls.

COB3: To provide knowledge of asset security, privacy protection, data lifecycle management and third-party risk management.

COB4: To familiarize students with Indian cyber laws, regulatory compliance and professional responsibilities in cyber security practices.

Course Outcomes (COs):

CO1: Understand security governance, risk management principles and professional ethics in cyber security.

CO2: Apply security frameworks, standards and controls for organizational information security management.

CO3: Demonstrate knowledge of asset security, privacy protection, data lifecycle and third-party risk management.

CO4: Analyze Indian cyber laws, regulatory frameworks and professional compliance requirements in cyber security.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	2	2	3	2	1	2	1	2	1	3
CO2	3	3	3	2	2	2	1	2	1	3	1	3
CO3	3	3	2	2	3	2	1	2	2	2	1	3
CO4	3	2	1	2	3	3	2	2	1	2	1	3

Theory **Credits: 4**

Unit I: Security Governance and Risk Management

Fundamentals of Security Governance: Principles of security governance - Information security objectives - Roles and responsibilities in governance

Security Policies and Compliance: Types of security policies - Standards, procedures and guidelines - Regulatory compliance requirements

Risk Management Concepts: Definition and types of risk - Risk assessment methodologies - Risk analysis and evaluation

Ethics and Professional Responsibility: Ethical principles in Cybersecurity - Professional codes of conduct - Responsibilities of security professionals

Governance Frameworks and CISSP Domains: Overview of CISSP Domain 1 - Overview of CISSP Domain 2 - Governance and asset security integration

Unit II: Security Frameworks, Standards and Controls

NIST Cybersecurity Framework: Overview of NIST CSF 2.0 - Core functions of NIST CSF - Application of CSF in organizations

NIST Risk Management Framework: RMF process steps - Categorization and control selection - Continuous monitoring concepts

ISO/IEC 27001:2022: Information Security Management System (ISMS) - Clauses and controls overview - Risk-based implementation approach

ISO/IEC 27002:2022: Security control categories - Organizational and technical controls - Best practices for implementation

CIS Controls v8.1: Overview of CIS Controls - Critical security safeguards - Mapping controls to organizational security

Unit III: Asset Security, Privacy and Third-Party Risk

Asset Security Fundamentals: Definition and types of information assets - Asset ownership and accountability - Asset inventory management

Asset Classification and Data Lifecycle: Data classification methods - Data lifecycle stages - Data retention and disposal policies

Data Protection and DLP: Data Loss Prevention (DLP) concepts - Data handling and protection measures - Encryption and access control practices

Privacy and Personal Data Protection: Privacy principles and requirements - Handling of personal data - Organizational privacy responsibilities

Third-Party and Vendor Risk: Third-party risk assessment - Vendor management practices - Supply chain security considerations

Unit IV: Indian Cyber Laws and Professional Practices

Introduction to Information Technology Laws in India: Information Technology Act 2000 - IT Rules 2021 - CERT-In Directions 2022

Introduction to Digital Personal Data Protection Framework: DPDP Act 2023 overview - DPDP Rules 2025 - Rights and obligations under DPDP

Introduction to Criminal and Evidentiary Laws: Bharatiya Nyaya Sanhita (BNS) 2023 - Bharatiya Nagarik Suraksha Sanhita (BNSS) 2023 - Bharatiya Sakshya Adhiniyam (BSA) 2023

Intellectual Property Rights and Cyber Psychology: Intellectual Property Rights (IPR) in cyberspace - Cyber psychology and cyber behaviour - Online ethics and digital conduct

Professional Responsibility and Legal Compliance: Responsibilities of Cybersecurity professionals - Incident reporting and compliance obligations - Legal and ethical challenges in Cybersecurity

Practicals **Credits: 1**

1. Preparation of organizational security policy documents.
2. Risk identification and risk assessment exercises.
3. Development of data retention and disposal schedules.
4. Demonstration of Data Loss Prevention (DLP) concepts using case studies.

5. Preparation of ISO/IEC 27001 compliance documentation.
6. Drafting of privacy and data protection compliance checklists.
7. Preparation of CERT-In and DPDP-aware compliance checklist.
8. Analysis of Cyber law cases involving BNS, BNSS, and BSA provisions.

References:

1. Mike Chapple, James Michael Stewart: CISSP Official Study Guide John Wiley & Sons, 2012
2. Thomas R. Peltier: Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management, CRC Press, 2016
3. Michael E. Whitman and Herbert J. Mattord: Principles of Information Security, Cengage Learning India Pvt. Ltd., 2023
4. Pavan Duggal: Cyber Law and Cyber Security in India, Universal LexisNexis, 2024
5. Dr. Legha Mamta Ranjitsingh: The Evolution of Cyber Law: A Critical Analysis of Jurisprudence, Regulation, and Digital Rights, Crown Publishing, 2025

B.Sc. (Hons.) Digital Forensics and Cyber Security
SEMESTER IV

Paper C-107: Operating System Forensics: Windows, Linux & Android Artefacts

Course Objectives (COBs):

COB1: To introduce the forensic analysis of Windows, Linux and Android operating systems and their artefacts.
COB2: To develop understanding of operating system logs, user activity traces and application artefacts for forensic investigations.
COB3: To provide knowledge of Android acquisition methods, SQLite databases and mobile forensic artefact analysis.
COB4: To familiarize students with timeline reconstruction, anti-forensics detection, deleted-file recovery and forensic reporting procedures.

Course Outcomes (COs):

CO1: Understand Windows, Linux and Android operating system artefacts relevant to digital forensic investigations.
CO2: Analyze operating system logs, user activity traces and application artefacts for evidence identification.
CO3: Apply acquisition, database analysis, timeline reconstruction and deleted-file recovery techniques in forensic investigations.
CO4: Demonstrate knowledge of anti-forensics detection, forensic documentation and reporting of operating system artefacts.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	3	1	1	1	1	2	3	2	1	1
CO2	3	3	3	2	2	2	1	2	3	2	1	1
CO3	3	3	3	2	2	2	1	2	3	2	2	2
CO4	3	2	2	2	3	3	2	2	2	1	1	3

Theory **Credits: 4**

Unit I: Windows Forensic Artefacts

Fundamentals of Windows Forensics: Windows operating system architecture - User and system artefacts - Importance of Windows forensic analysis
Windows Registry Analysis: Structure of registry hives - User and system registry keys - Forensic significance of registry data
Windows Event and Activity Logs: Windows event logs - System and security logs - Log analysis techniques

User Activity Artefact: Prefetch files and shortcuts - Jump lists and recent files - Recycle bin artefacts

Browser and Internet Artefacts: Browser history and cache - Cookies and download records - Analysis of internet activity traces

Unit II: Linux Forensic Artefacts

Fundamentals of Linux Forensics: Linux operating system structure - Linux file system hierarchy - User and system artefacts in Linux

Linux User Activity Artefacts: Shell history files - User account information - Command execution traces

Linux Log Analysis: Authentication logs - Systemd journal logs - Syslog and kernel logs

Scheduled Tasks and Package Logs: Cron jobs and scheduled tasks - Package installation logs - Software update records

Linux File Permissions and Security: File permission structures - Ownership and access controls - Detection of suspicious activities

Unit III: Android Forensic Artefacts

Fundamentals of Android Forensics: Android operating system architecture - Android file system layout - User and application artefacts

Android Data Acquisition: Logical acquisition methods - Introduction to ADB - Device communication and debugging

Android Application Artefacts: App data storage locations - Shared preferences and cache files - Analysis of user-generated data

SQLite Databases and Logs: SQLite database structure - Extraction of database records - Android system and application logs

Android Security and Privacy Artefacts: Permissions and access records - Deleted data traces - Indicators of tampering or misuse

Unit IV: Timeline Analysis, Anti-Forensics and Reporting

Timeline Analysis Techniques: Concepts of timeline reconstruction - Correlation of timestamps - Event sequencing methods

User Attribution and Behaviour Analysis: Identification of user actions - User account correlation - Analysis of login and activity records

Anti-Forensics Techniques: Types of anti-forensics methods - Detection of artefact manipulation - Indicators of evidence tampering

Deleted File Recovery Basics: File deletion concepts - Recovery of deleted artefacts - Verification of recovered evidence

Forensic Documentation and Reporting: Documentation of forensic findings - Preparation of forensic reports - Presentation of OS artefact evidence

Practicals **Credits: 1**

1. Examination of Windows registry hives.
2. Analysis of Windows event logs, recycle bin, browser history and security logs.
3. Linux shell history and command-history analysis.
4. Demonstration of Linux files permission and ownership analysis.
5. Examination of Android application artefacts and cache files.
6. Extraction and analysis of SQLite database records from Android devices.
7. Demonstration of deleted-file recovery techniques.
8. Preparation of forensic reports based on OS artefact findings.

References:

1. Harlan Carvey: Windows Forensic Analysis Toolkit Advanced Analysis Techniques for Windows 8 Syngress Media Inc., 2014
2. Bill Nelson, Amelia, Phillips: Guide to Computer Forensics and Investigations, 7th edition, Cengage Learning, 2024
3. Eoghan Casey: Digital Evidence and Computer Crime, 3rd edition, Academic Press, 2011
4. Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters: The Art of Memory Forensics - Detecting Malware and Threats in Windows, Linux, and Mac Memory, 1st Edition, Wiley, 2014
5. Bruce Nikkel: Practical Linux Forensics - A Guide for Digital Investigators, Starch Press, 2021
6. Andrew Hoog: Android Forensics: Investigation, Analysis and Mobile Security for Google Android, Syngress, 2011
7. Brian Carrier: File System Forensic Analysis, 1st Edition, Addison-Wesley, 2005

Paper C-108: Security Architecture, IAM, Applied Cryptography & Secure SDLC

Course Objectives (COBs):

COB1: To introduce the principles of security architecture, trusted design and secure system development.

COB2: To develop understanding of Identity and Access Management (IAM), authentication mechanisms and access control models.

COB3: To provide knowledge of applied cryptography, PKI, digital signatures and secure communication protocols.

COB4: To familiarize students with secure SDLC practices, OWASP security principles, threat modeling and cloud security concepts.

Course Outcomes (COs):

CO1: Understand security architecture principles, trusted design concepts and secure infrastructure components.

CO2: Apply IAM concepts, authentication mechanisms and access control techniques for secure systems.

CO3: Demonstrate knowledge of cryptographic techniques, PKI, digital signatures and secure communication protocols.

CO4: Analyze secure SDLC practices, threat models, OWASP principles and cloud security configurations.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PSO1	PSO2	PSO3	PSO4
CO1	3	2	3	2	2	1	1	2	1	3	1	2
CO2	3	3	3	2	2	2	1	2	1	3	1	2
CO3	3	3	3	2	2	2	1	2	2	3	2	2
CO4	3	3	3	3	2	2	1	3	1	3	2	2

Theory **Credits: 4**

Unit I: Security Architecture and Trusted Design

Fundamentals of Security Architecture: Principles of security architecture - Security models and frameworks - Objectives of secure system design

CISSP Security Architecture Concepts: Overview of CISSP Domain 3 - Trusted computing principles - Security architecture components

Secure System Design: Secure design principles - Defense in depth strategy - Security by design concepts

Trusted Platforms and Infrastructure: Trusted Platform Module (TPM) basics - Secure boot mechanisms - Hardware and firmware security

Security Architecture Evaluation: Security assessment techniques - Architecture review methodologies - Security baseline establishment

Unit II: Identity and Access Management (IAM)

Fundamentals of IAM: Identity and access management concepts - Authentication and authorization mechanisms - Accountability and auditing principles

Least Privilege and Zero Trust: Principle of least privilege - Zero Trust architecture concepts - Micro-segmentation and access control

Multi-Factor Authentication Technologies: Multi-factor authentication (MFA) - FIDO2 and passkey authentication - Biometric and token-based authentication

Identity Federation and Access Protocols: OAuth framework basics - OpenID Connect (OIDC) concepts - Single sign-on (SSO) mechanisms

Privileged Access Management: Privileged account management (PAM) - Monitoring privileged activities - Risks associated with privileged access

Unit III: Applied Cryptography and Secure Communication

Fundamentals of Cryptography: Objectives of cryptography - Cryptographic terminology - Applications of cryptography in Cybersecurity

Hashing and Symmetric Encryption: Hash functions and integrity verification - Symmetric encryption algorithms - Key management principles

Asymmetric Encryption and PKI: Public key cryptography concepts - Public Key Infrastructure (PKI) - Key exchange mechanisms

Digital Signatures and Certificates: Digital signature generation and verification - Digital certificates and certificate authorities - Certificate lifecycle management

Secure Communication Protocols: TLS and HTTPS protocols - Secure communication channels - Cryptographic protection in networks

Unit IV: Secure SDLC, OWASP and Cloud Security

Secure Software Development Lifecycle: Phases of secure SDLC - Security integration in development - Secure coding practices

Threat Modeling and Risk Identification: Threat modeling concepts - STRIDE and PASTA methodologies - Identification of software threats

OWASP Security Principles: OWASP Top 10 overview - Web application security principles - API and mobile security considerations

Security Testing and Code Review: Static Application Security Testing (SAST) - Dynamic Application Security Testing (DAST) - Secure configuration review methods

Cloud Security and Logging Architecture: Fundamentals of cloud security - Logging and monitoring architecture - Secure configuration baselines for cloud systems

Practicals **Credits: 1**

1. Preparation of security architecture diagrams for secure systems.
2. Demonstration of least privilege and role-based access control implementation.
3. Configuration of multi-factor authentication mechanisms.
4. Demonstration of privileged access management concepts.
5. Generation and verification of cryptographic hash values.

6. Demonstration of symmetric and asymmetric encryption techniques.
7. Creation and verification of digital certificates.
8. Generation and verification of digital signatures.

References:

1. Mike Chapple, James Michael Stewart, Darril Gibson, David Seidl: ISC2 CISSP Certified Information Systems Security Professional Official Study Guide and Practice Tests Bundle, John Wiley & Sons, Incorporated, 2024
2. Ertem Osmanoglu: Identity and Access Management Business Performance Through Connected Intelligence, Syngress, 2013
3. Evan Gilman, Doug Barth: Zero Trust Networks - Building Secure Systems in Untrusted Networks, O'Reilly Media, 2017
4. William Stallings: Cryptography and Network Security: Principles and Practice, 8th Edition, Pearson, 2022
5. Bruce Schneier: Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition, Wiley, 2015.