PROGRAM CURRICULUM

(Applicable for the batches admitted from A.Y 2025-26)

M.Sc. (Cyber Security & Digital Forensics)

for
Two Year Post Graduation Degree Program

ADITYA
UNIVERSITY

Aditya Nagar, ADB Road, Surampalem - 533 437

ADITYA UNIVERSITY

Vision

- To be a globally recognized university through excellence in Education, Innovation and Sustainable growth.

Mission

Deliver collaborative education to prepare students for global challenges through

- Transformative learning
- Vibrant research ecosystem
- Sustainable and inclusive community

DEPARTMENT OF FORENSIC SCIENCE

Vision

- To be a leading center of forensic science education and research, advancing justice through scientific excellence, innovation, and interdisciplinary collaboration.

Mission

M1: Transformative, hands-on forensic education fostering critical thinking, ethics and rigor.

M2: Interdisciplinary research ecosystem supporting justice and global challenges.

M3: Sustainable and inclusive community of globally competent professionals.

PROGRAMME EDUCATIONAL OBJECTIVES (PEO)

Postgraduates of the Program will

PEO1: Career Success and Leadership

Graduates will establish successful careers and demonstrate professional competence and leadership in their respective domains of forensic science, cyber security, digital forensics, and related fields.

PEO2: Higher Studies, Research, and Entrepreneurship

Graduates will pursue higher studies, research opportunities, or entrepreneurial pathways to contribute to advancements in their chosen discipline and allied areas.

PEO3: Lifelong Learning and Ethical Responsibility

Graduates will engage in lifelong learning, adapt to emerging global challenges, and uphold ethical responsibility in their professional and personal endeavors.

PROGRAMME SPECIFIC OUTCOMES (PSO)

After successful completion of the program, the graduates will be able to

PSO1: Scientific and Technical Skills

Apply knowledge from physical, biological, computational, and digital sciences to examine forensic or digital evidence. Use appropriate laboratory and digital tools and follow proper investigative protocols.

PSO2: Ethics and Professional Practice

Conduct forensic or digital investigations with integrity. Follow ethical standards and legal rules and ensure accurate handling and documentation of evidence for judicial or professional use.

PROGRAMME OUTCOMES (PO)

After successful completion of the program, the graduates will be able to

PO1: Integrated Forensic and Digital Competence

Apply foundational and advanced concepts from life sciences, physical sciences, computer sciences, and legal studies to investigate, analyze, and interpret physical, biological, and digital evidence in crime investigations.

PO2: Evidence Collection and Scene Management

Demonstrate proficiency in identifying, securing, documenting, and managing both physical and digital crime scenes, ensuring the integrity, continuity, and admissibility of collected evidence.

PO3: Analytical and Instrumental Proficiency

Operate laboratory instruments and digital forensic tools to accurately examine, process, and interpret chemical, biological, physical, and electronic evidence using validated analytical techniques.

PO4: Multidisciplinary and Technological Insight

Integrate knowledge from forensic pathology, toxicology, cyber forensics, network security, psychology, and data analytics to address complex challenges in modern forensic investigations.

PO5: Legal Awareness and Ethical Responsibility

Exhibit awareness of national laws, cyber regulations, and ethical standards governing forensic practice, maintaining integrity, confidentiality, impartiality, and adherence to justice in all professional actions.

PO6: Technical Documentation and Forensic Reporting

Develop competence in preparing comprehensive laboratory records, forensic reports, and digital documentation that meet scientific and legal standards, ensuring clarity, accuracy, and traceability.

PO7: Courtroom and Professional Communication Skills

Demonstrate the ability to present technical findings effectively in judicial proceedings and communicate professionally with law enforcement, legal experts, and multidisciplinary teams.

PO8: Evidence-Based and Critical Decision-Making

Employ scientific reasoning, statistical analysis, and critical thinking to evaluate data, validate findings, and make informed decisions in forensic and digital investigations.

PO9: Innovation, Research, and Lifelong Learning

Engage in research, innovation, and continuous learning to stay updated with evolving forensic methodologies, analytical technologies, cybersecurity threats, and global standards.

PO10: Collaboration, Leadership, and Professionalism

Work effectively as part of multidisciplinary forensic and investigative teams, demonstrating leadership, accountability, adaptability, and professionalism in diverse work environments.

PO11: Societal Impact and Public Awareness

Communicate forensic and cybersecurity knowledge responsibly to promote public awareness, contribute to crime prevention, and support the ethical use of science and technology in justice delivery.

Department of Forensic Science

M.Sc. (Cyber Security & Digital Forensics) Program Curriculum – 2025 - 26

(Applicable for the students submitted from the A.Y. 2025-26)

PG Programs Offered

- M.Sc. in Cyber Security & Digital Forensics
- M.Sc. in Forensic Science

Credit Division Category-wise

Sr. No.	Broad Category of Course	Credits
1	Major Core Courses (MCC)	68
2	Skill Enhancement Courses (SEC)	10
3	Summer Internship (SI)	2
3	Internships (INT)	8
4	Minor Project (MNP)	4
5	Major Project (MJP)	8
Total Credits to be earned for M.Sc. Degree		**100**

Major Core Courses (MCC)

Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS14	I	Principles of Cyber Security	FC	3		1	4	50	50	100	-
2512FS18		Zero Trust Architecture	FC	3		1	4	50	50	100	PCS
2512FS19		Advanced Digital Forensics	IC	2		2	4	50	50	100	-
2512FS24		Security Information and Event Management	IC	2		2	4	50	50	100	PCS
2512FS01		Advanced Multimedia Forensics	AC	2		2	4	50	50	100	ADF
2512FS03		Cyberlaw & Incident Response Management	AC	3		1	4	50	50	100	-
2512FS10	II	Advance Linux	FC	3		1	4	50	50	100	-
2512FS20		Cryptographic Backdoors	IC	3		1	5	50	50	100	-
2512FS23		Quantum Computing in Steganography	IC	3		2	5	50	50	100	-
2512FS09		Network Forensics	AC	3		2	5	50	50	100	ADF
2512FS06		Memory Forensics	AC	3		2	5	50	50	100	ADF
2512FS12	III	Ethical Hacking and Cyber Risk Assessment	FC	2		2	4	50	50	100	-
2512FS21		Digital Frauds	IC	2		2	4	50	50	100	-
2512FS22		Governance, Risk and Compliance	IC	3		1	4	50	50	100	-
2512FS02		Business Continuity Plan	AC	3		1	4	50	50	100	-
2512FS08		Mobile and IOT Forensics	AC	2		2	4	50	50	100	ADF
Total				39		**25**	**68**				

Skill Enhancement Courses (SEC)

Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS13	I	IT Skills	FC			2	2	50	50	100	-
2512FS11	II	Courtroom Testimony	FC	2			2	50	50	100	-
2512FS15	III	Research Methodology & Scientific Writing	FC	4			4	50	50	100	-
2512FS16	IV	Student Activity Based Learning	FC				2	100	-	100	-
Total				**6**		**2**	**10**				

Minor Project (MNP)

Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS07	III	Minor Project	AC			4	4	100	-	100	-
Total						**4**	**4**				

Summer Internships (SI)

Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS25	III	Summer Internship	AC			2	2	100	-	100	-
Total						**2**	**2**				

Internships (INT)

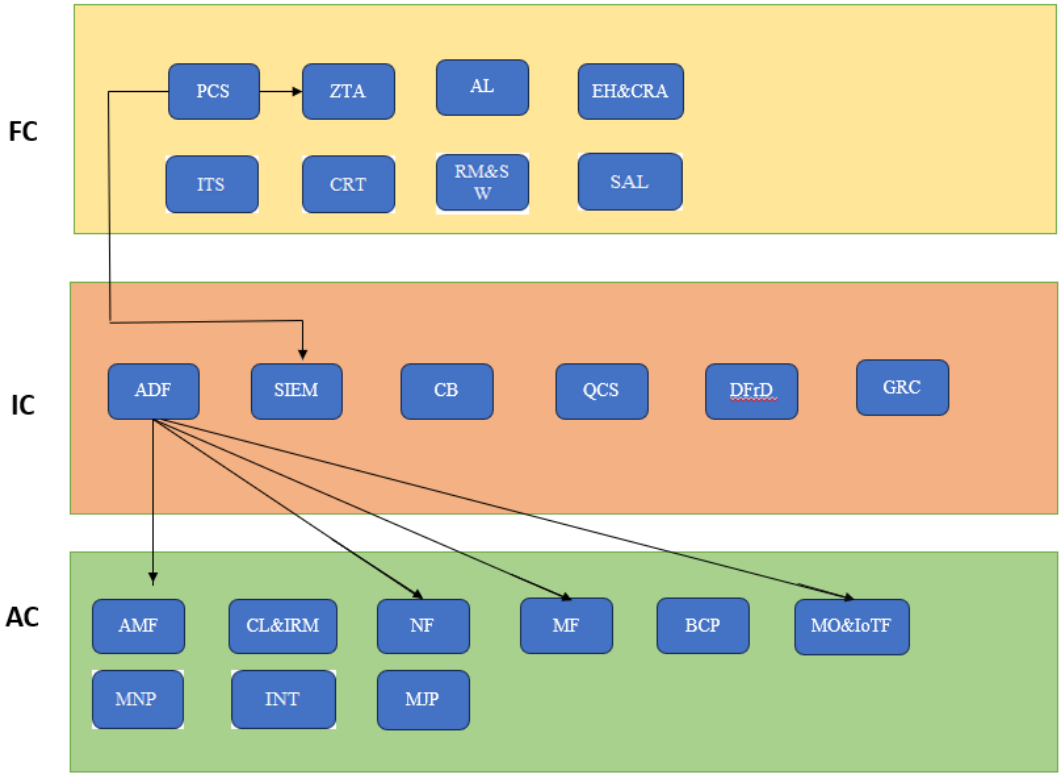
Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS04	IV	Internship	AC			8	8	100	-	100	-
Total						**8**	**8**				

Major Project (MJP)

Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS05	IV	Major	AC			8	8	50	50	100	-

		Project									
Total						**8**	**8**				

2025-26 M.Sc. (CS & DF) CURRICULUM PREREQUISITE FLOW CHART



PCS	Principles of Cyber Security	ADF	Advanced Digital Forensics	AMF	Advanced Multimedia Forensics
ZTA	Zero Trust Architecture	SIEM	Security Information and Event Management	CL&IRM	Cyberlaw & Incident Response Management
AL	Advance Linux	CB	Cryptographic Backdoors	NF	Network Forensics
EH&CRA	Ethical Hacking and Cyber Risk Assessment	QCS	Quantum Computing in Steganography	MF	Memory Forensics
		DFrd	Digital Frauds	BCP	Business Continuity Plan
		GRC	Governance, Risk and Compliance	MO&IOTF	Mobile and IOT Forensics
ITS	IT Skills	-	-	MNP	Minor Project
CRT	Courtroom Testimony	-	-	INT	Internship
RM&SW	Research Methodology & Scientific Writing	-	-	MJP	Major Project
SABL	Student Activity Based Learning	-	-	SI	Summer Internship

Semester-wise Curriculum

I SEMESTER

Course code	Course Title	Course		Credits				Total Hours
		Category	Level	L	T	P	Total	
2512FS14	Principles of Cyber Security	MCC	FC	3		1	4	5
2512FS18	Zero Trust Architecture	MCC	FC	3		1	4	5
2512FS19	Advanced Digital Forensics	MCC	IC	2		2	4	6
2512FS24	Security Information and Event Management	MCC	IC	2		2	4	6
2512FS01	Advanced Multimedia Forensics	MCC	AC	2		2	4	6
2512FS03	Cyberlaw & Incident Response Management	MCC	AC	3		1	4	5
2512FS13	IT Skills	SEC	FC			2	2	4
	Total			**15**		**11**	**26**	**37**

II SEMESTER

Course code	Course Title	Course		Credits				Total Hours
		Category	Level	L	T	P	Total	
2512FS10	Advance Linux	MCC	FC	3		1	4	5
2512FS20	Cryptographic Backdoors	MCC	IC	3		2	5	7
2512FS23	Quantum Computing in Steganography	MCC	IC	3		2	5	7
2512FS09	Network Forensics	MCC	AC	3		2	5	7
2512FS06	Memory Forensics	MCC	AC	3		2	5	7
2512FS11	Courtroom Testimony	SEC	FC	2			2	2
	Total			**14**		**12**	**26**	**38**

III SEMESTER

Course code	Course Title	Course		Credits				Total Hours
		Category	Level	L	T	P	Total	
2512FS12	Ethical Hacking and Cyber Risk Assessment	MCC	FC	2		2	4	6
2512FS21	Digital Frauds	MCC	IC	2		2	4	6
2512FS22	Governance, Risk and Compliance	MCC	IC	3		1	4	5
2512FS02	Business Continuity Plan	MCC	AC	3		1	4	5
2512FS08	Mobile and IOT Forensics	MCC	AC	2		2	4	6
2512FS07	Minor Project 1	MNP	AC			4	4	8
2512FS15	Research Methodology & Scientific Writing	SEC	FC	4			4	4
2512FS25	Summer Internship	SI	AC			2	2	20
	Total			**16**		**14**	**30**	**60**

IV SEMESTER

Course code	Course Title	Course		Credits				Total Hours
		Category	Level	L	T	P	Total	
2512FS04	Internship	INT	AC			8	8	18
2512FS05	Major Project	MJP	AC			8	8	18
2512FS16	Student Activity Based Learning	SEC	500				2	-
	Total					**16**		**36**

Total Credits: 100

Major Core Courses (MCC)

Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS14	I	Principles of Cyber Security	FC	3		1	4	50	50	100	-
2512FS18		Zero Trust Architecture	FC	3		1	4	50	50	100	PCS
2512FS19		Advanced Digital Forensics	IC	2		2	4	50	50	100	-
2512FS24		Security Information and Event Management	IC	2		2	4	50	50	100	PCS
2512FS01		Advanced Multimedia Forensics	AC	2		2	4	50	50	100	ADF
2512FS03		Cyberlaw & Incident Response Management	AC	3		1	4	50	50	100	-
2512FS10	II	Advance Linux	FC	3		1	4	50	50	100	-
2512FS20		Cryptographic Backdoors	IC	3		2	5	50	50	100	-
2512FS23		Quantum Computing in Steganography	IC	2		2	5	50	50	100	-
2512FS09		Network Forensics	AC	2		2	5	50	50	100	ADF
2512FS06		Memory Forensics	AC	2		2	5	50	50	100	ADF
2512FS12	III	Ethical Hacking and Cyber Risk Assessment	FC	2		2	4	50	50	100	-
2512FS21		Digital Frauds	IC	2		2	4	50	50	100	-
2512FS22		Governance, Risk and Compliance	IC	3		1	4	50	50	100	-
2512FS02		Business Continuity Plan	AC	3		1	4	50	50	100	-
2512FS08		Mobile and IOT Forensics	AC	2		2	4	50	50	100	ADF
Total				39		**29**	**68**				

Principles of Cyber Security

	L	T	P	C
Course Code: 2512FS14	3	0	1	4

Semester I

Course Outcomes:

At the end of the Course, Student will be able to:

CO1: Understanding core cybersecurity principles, including, confidentiality, integrity, and availability (CIA Triad).

CO2: Analyze various cyber threats, vulnerabilities, and risk management techniques.
CO3: Evaluate cryptographic techniques and security models for securing digital assets.
CO4: Examine network security measures, access control mechanisms, and security protocols.
CO5: Implement cybersecurity best practices in compliance with legal and ethical considerations.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	1	3	3	1	-	2	2	1	3
CO2	2	3	2	3	2	2	1	3	2	2	2
CO3	3	2	3	3	3	2	1	2	2	1	2
CO4	3	3	3	3	2	3	1	3	2	2	2
CO5	2	2	2	3	2	2	3	2	2	3	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	1
CO4	3	1
CO5	2	3

UNIT – I: Fundamentals of Cyber Security

Overview of Cyber Security: Definition, Scope, and Importance; Cyber Threats and Attack Vectors: Malware, Phishing, Ransomware, Insider Threats; Security Concepts: Confidentiality, Integrity, Availability (CIA Triad); Cybersecurity Frameworks: NIST; Cyber Risk Management & Security Policies;

Practice – Cryptography Implementation

UNIT – II: Risk Management and Security Policies

Risk Analysis and Management: Identifying threats, vulnerabilities, and mitigation strategies. Security Policies and Standards: Role of security policies in organizations, security auditing, compliance requirements. Incident Response & Disaster Recovery: Incident handling steps, digital forensics basics, and recovery planning. Security Awareness & Training: Role of employees in cybersecurity.

Practice – Firewall & IDS Configuration

UNIT – III: Cryptography and Data Security

Cryptographic Concepts: Symmetric vs asymmetric encryption, key management, cryptographic attacks. Public Key Infrastructure (PKI): Digital signatures, certificates, and trusted authorities. Hashing & MD5, SHA-256. Types of data: Data in Motion, Data at Rest & Data in use.

Practice – Phishing Attack Analysis

UNIT – IV: Network and System Security

Network Security Fundamentals: Firewalls, IDS/IPS, VPNs, secure network protocols. Endpoint Security, Access Control Models: Role-based access control (RBAC), discretionary (DAC) vs mandatory access control (MAC). Authentication and Authorization: Multi-factor authentication (MFA). Wireless Security: Wi-Fi security standards.

Practice – Network Packet Analysis – Use Wireshark

UNIT – V: Cybersecurity Governance, Compliance, and Ethics

Cyber Laws and Regulations: GDPR, HIPAA, PCI DSS, Indian IT Act 2000 & amendments. Cybersecurity Governance: Security policies, organizational structure, security frameworks. Cyber Ethics and Professional Responsibility: Ethical challenges, privacy concerns, responsible disclosure.

Practice- Create strong password policies and test password cracking.

Textbooks:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson.
2. Charles P. Pfleeger, Security in Computing, Prentice Hall.

Reference Books:

1. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley.
2. Niels Ferguson, Cryptography Engineering: Design Principles and Practical Applications, Wiley.

Web Links:

1. https://www.nist.gov/cyberframework
2. https://owasp.org/
3. https://www.cisecurity.org/
4. https://www.sans.org/
5. https://attack.mitre.org/

Zero Trust Architecture

L	T	P	C
3	0	1	4

Course Code: 2512FS18

Semester I

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the core principles and need for Zero Trust Architecture (ZTA) in modern cybersecurity.
CO2: Analyze identity-based security models, least privilege access, and micro-segmentation strategies.
CO3: Implement security controls using Zero Trust frameworks and technologies.
CO4: Evaluate ZTA deployment challenges and integration with cloud, IoT, and enterprise networks.
CO5: Examine compliance requirements, risk management, and security best practices in Zero Trust environments.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	3	3	1	-	2	2	1	3
CO2	3	3	2	3	3	2	1	3	2	2	2
CO3	3	3	3	3	2	2	1	3	3	3	2
CO4	3	2	3	3	2	2	1	3	3	2	2
CO5	2	3	2	2	3	3	3	2	3	3	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	1
CO4	3	1
CO5	2	3

Unit-Wise Syllabus:

UNIT – I: Fundamentals of Zero Trust Security

Introduction to Zero Trust: Definition, Evolution, and Importance. Traditional Security vs. Zero Trust: Perimeter-based security limitations. Zero Trust Core Principles: Never trust, always verify; Least privilege access; Assume breach. Components of Zero Trust Architecture: Identity, network, endpoints, applications, and data. NIST Zero Trust Model: Overview and implementation guidelines.

Practice- Zero Trust Network Setup – Configure and implement network segmentation

UNIT – II: Identity and Access Management in Zero Trust

Identity as the New Perimeter: The role of identity in ZTA. Multi-Factor Authentication (MFA): Types, benefits, and implementation. Identity Federation and Single Sign-On (SSO). Role-Based Access Control (RBAC) vs Attribute-Based Access Control (ABAC). Privileged Access Management (PAM): Securing admin accounts and credentials.

Practice- Identity & Access Management (IAM) in ZTA – Set up MFA.

UNIT – III: Network Security and Micro-Segmentation

Network Segmentation and Micro-Segmentation: Concepts and benefits. Software-Defined Perimeter (SDP): Implementation and security controls. Secure Access Service Edge (SASE): Integration with Zero Trust. Network Access Control (NAC): Ensuring only authorized devices connect.

Practice- Cloud Security with Zero Trust

UNIT – IV: Zero Trust Implementation and Technologies

Zero Trust in Cloud Security: Implementing ZTA in AWS, Azure, and Google cloud. Endpoint Security in ZTA: Endpoint Detection and Response (EDR), XDR solutions. Data-Centric Security: Data encryption, tokenization, and access controls. Continuous security monitoring in CI/CD pipelines.

Practice- Security Monitoring with Zero Trust Analytics

UNIT – V: Compliance, Challenges, and Future of ZTA

Regulatory Compliance in ZTA: GDPR, NIST, ISO 27001, PCI DSS. Zero Trust Adoption Challenges: Organizational, technical, and cultural barriers. Zero Trust Case Studies: Real-world implementations and success stories. Future Trends in Zero Trust:

Practice- Monitor user and device activity logs to simulate trust evaluation.

Textbooks:

1. John Kindervag, Zero Trust Networks: Building Secure Systems in Untrusted Networks, O'Reilly.
2. Jason Garbis & Jerry W. Chapman, Zero Trust Security: An Enterprise Guide, Packt Publishing.

Reference Books:

1. Chase Cunningham, Cyber Warfare – Truth, Tactics, and Strategies, O'Reilly.
2. Neil Rerup, Zero Trust: The Big Picture, Kindle Edition.

Web Links:

1. https://csrc.nist.gov/publications/detail/sp/800-207/final
2. https://www.microsoft.com/en-us/security/business/zero-trust
3. https://attack.mitre.org/
4. https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf
5. https://cloud.google.com/beyondcorp

Advanced Digital Forensics

L	T	P	C
2	0	2	4

Course Code: 2512FS19

Semester I

Course Outcomes:

At the end of the course, students will be able to:

CO1: Analyze and extract forensic evidence from Windows, Linux, and macOS systems.
CO2: Apply cryptographic techniques for forensic encryption/decryption processes.
CO3: Perform memory forensic investigations using advanced tools and frameworks.
CO4: Conduct virtual machine forensic analysis including snapshot and image inspection.
CO5: Investigate cloud-based platforms for evidence gathering and analysis in distributed environments.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	3	3	3	2	2	2	3	2	2	2
CO2	3	2	3	3	3	2	1	2	3	2	2
CO3	3	3	3	3	3	3	1	3	3	2	2
CO4	3	3	3	3	3	2	1	2	3	2	2
CO5	3	3	2	2	3	3	2	3	3	3	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	1
CO3	3	1
CO4	3	1
CO5	3	2

Unit-Wise Syllabus:

UNIT – I: Windows Forensics

Data Collection: Volatile & Non- volatile data. Registry Analysis, Browser Usage, Hibernate File Analysis, Crash Dump Analysis, File System Analysis, File Metadata and Timestamp Analysis, Event Viewer Log Analysis, MFT analysis, Timeline Creation, Evidence Collection in Linux and Mac Operating system.

Practice- Perform snapshot analysis and artifact recovery in a virtual machine.

UNIT – II: Cryptography

Cryptographic System: Definition and Classification, Secret Key, Cryptography, Cryptanalysis and Attacks, Encryption and their types, Encryption algorithms, brute force attack, Decryption and their types, HDD and Artifacts Encryption and Decryption Techniques. **Practice-** Data Acquisition: - acquisition using: - FTK Imager.

UNIT – III: Memory Forensics

Introduction to Memory Forensics, x86/x64 architecture, Data structures, Volatility Framework & plugins Memory acquisition, Recovering attacker activity from memory, Introduction to Anti-forensics, tools and techniques.

Practice- Recovery of data using bulk extractor.

UNIT – IV: Virtual Machine Forensics

Hypervisors: Types, Files and Formats. Virtual Machines: Descriptions, Use and implementation in Forensic Analysis, Use of VMware to establish working version of suspect's machine, Networking and virtual networks within Virtual Machine, Forensic Analysis of a Virtual Machine (Imaging of a VM, Identification and Extraction of supporting VM files in the host system, VM Snapshots, Mounting Image, Searching for evidence)

Practice- Creating a backup using icloud.

UNIT – V: Cloud Forensics

Cloud storage architecture, forensic challenges, Dropbox & Google Drive forensics, cloud artifact analysis, data remnants on endpoints, cloud evidence preservation and analysis frameworks.

Practice-Forensics Case Study: Solve the Case study (image file) provided in the lab.

Textbooks:

1. Window Forensic Analysis (DVD Toolkit) by Harlan Carver.
2. File System Forensic Analysis by Brain Carrier.

Reference Books:

1. **Harlan Carvey** – Windows Forensic Analysis Toolkit
2. **Jason Luttgens et al.** – Incident Response & Computer Forensics

Web Links:

1. https://www.volatilityfoundation.org
2. https://digital-forensics.sans.org
3. https://www.autopsy.com
4. https://www.magnetforensics.com
5. https://cyber.gc.ca/en

Security Information and Event Management

L	T	P	C
2	0	2	4

Course Code: 2512FS24

Semester I

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the role of Security Information and Event Management (SIEM) in cybersecurity operations.
CO2: Learn event correlation techniques and log analysis for real-time threat detection.
CO3: Implement SIEM solutions for security monitoring, incident response, and compliance.
CO4: Analyze various security events and alerts to mitigate cyber threats.
CO5: Gain hands-on experience with SIEM tools to detect and respond to security incidents.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	3	3	2	-	2	2	1	3
CO2	3	3	3	3	2	2	1	3	3	2	2
CO3	3	3	3	3	3	3	2	3	3	2	3
CO4	3	3	3	3	2	2	1	3	3	3	2
CO5	3	3	3	3	3	3	2	3	3	3	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	1
CO3	3	3
CO4	3	2
CO5	3	1

Unit-Wise Syllabus:

UNIT – I: Introduction to SIEM and Log Management

Overview of SIEM: Need for SIEM in cybersecurity, benefits, and components. Log Sources and Log Management: System logs, network logs, application logs, audit logs. Log Collection and Normalization: Structured vs. unstructured logs. Event Correlation and Threat Hunting: How SIEM detects security incidents. Challenges in SIEM Implementation: Scalability, false positives.

Practice- SIEM Rule Creation – Developing correlation rules for detecting threats.

UNIT – II: SIEM Architecture and Deployment

SIEM Architecture: Data ingestion, event processing, correlation engine, dashboards. SIEM Deployment Models: On-premises vs. cloud-based SIEM solutions. Security Log Storage and Retention Policies:
Practice- Real-Time Security Monitoring.

UNIT – III: Event Correlation and Threat Detection

Correlation Rules and Use Cases: Identifying suspicious patterns and attack indicators. Anomaly Detection: Statistical analysis, baselining, and machine learning in SIEM. Reducing false positives. Security Monitoring in Real-Time: Detecting malware, insider threats and APTs.

Practice- Incident Investigation & Response.

UNIT – IV: Incident Response and Forensics with SIEM
SIEM in Incident Response: Workflow, investigation, and remediation. Case Studies on Cyber Attacks: Analysis of SIEM-detected incidents. Security Automation and Orchestration (SOAR): Automating incident response. Forensic Analysis with SIEM: Using logs and events for digital forensic investigations.

Practice- Create a dashboard showing system and user activities.

UNIT – V: Advanced SIEM Features and Future Trends

User and Entity Behavior Analytics (UEBA): AI-based anomaly detection in SIEM. Threat Hunting with SIEM: Proactive threat detection techniques. SIEM in Cloud and Hybrid Environments: Challenges and best practices. Integration with Endpoint Detection & Response (EDR) and XDR. Future Trends: AI-driven SIEM, predictive analytics, zero-trust security integration.

Practice-Simulate a brute-force login attempt and detect it via log analysis.

Textbooks:

1. Rafeeq Ur Rehman, SIEM Implementation, McGraw-Hill.
2. Gary C. Kessler, SIEM Security Logging and Event Management, CRC Press.

Reference Books:

1. Michael G. Solomon, Security Operations and SIEM, Sybex.
2. Eric Conrad, The CISSP Guide to Security Operations, McGraw-Hill

Web Links:

1. https://www.ibm.com/docs/en/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_pdfs.html
2. https://docs.securityonion.net/
3. https://www.ibm.com/think/topics/security-operations-center
4. ELK Stack Security Monitoring
5. https://www.splunk.com/en_us/data-insider/what-is-siem.html

Advanced Multimedia Forensics

L	T	P	C
2	0	2	4

Course Code: 2512FS01

Semester I

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the fundamentals of multimedia content and file formats.
CO2: Learn techniques for detecting image, video, and audio tampering.
CO3: Analyze digital media for forensic evidence.
CO4: Apply tools and methods for content authentication.
CO5: Prepare forensic reports from multimedia investigations.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	-	-	3	-	-	-	-	-	-	-
CO2	3	3	3	3	-	-	-	3	-	-	-
CO3	3	3	3	3	-	3	-	3	-	-	-
CO4	3	3	3	3	-	3	-	3	-	-	-
CO5	3	3	3	-	3	3	3	-	-	-	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	2	1
CO2	3	2
CO3	3	2
CO4	3	2
CO5	2	3

Unit-Wise Syllabus:

UNIT – I: Introduction to Multimedia Forensics

Definition, scope, and importance of multimedia forensics. Types of digital media – images, audio, video. Sources of digital evidence. File formats and metadata basics. Challenges in multimedia evidence handling.

Practice- Analyze image metadata.

UNIT – II: Image Forensics

Image structure and compression (JPEG, PNG, TIFF). Metadata analysis (EXIF). Forgery detection: copy-move, splicing, resampling. Lighting and shadow analysis. Image enhancement and tamper localization.

Practice- Detect, copy-move forgeries in images.

UNIT – III: Video Forensics

Video formats and compression (MP4, AVI, MKV). Frame-level analysis, frame duplication detection. Keyframe and GOP analysis. Deepfake and synthetic video detection. Source camera identification.

Practice- Perform deep fake video detection.

UNIT – IV: Audio Forensics

Audio formats and properties (WAV, MP3). Audio editing detection, speech enhancement. Noise profiling, speaker identification. Authenticity checks and tampering analysis. Forensic audio tools overview.

Practice- Analyze audio tampering.

UNIT – V: Applications, and Reporting

Legal admissibility of multimedia evidence. Case studies. Writing professional forensic reports for multimedia evidence.

Practice-Create a multimedia forensic report from a sample investigation.

Textbooks:

1. Hany Farid – Photo Forensics
2. Nasir Memon – Multimedia Security: Steganography and Digital Watermarking

Reference Books:

1. Jessica Fridrich – Digital Image Forensic Analysis
2. Niels Provos & Peter Honeyman – Detecting Steganographic Content

Web Links:

1. https://www.forensically.net
2. https://www.deepware.ai
3. https://www.exiftool.org
4. https://www.coursera.org/learn/multimedia-forensics
5. https://www.ampedsoftware.com

Cyberlaw & Incident Response Management

L	T	P	C
3	0	1	4

Course Code: 2512FS03

Semester I

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the legal framework for cyberspace and digital evidence.
CO2: Analyze laws governing cybercrime and data protection.
CO3: Learn best practices for managing and responding to cybersecurity incidents.
CO4: Develop skills for documenting and reporting security incidents legally.
CO5: Prepare for compliance with national and international cybersecurity laws.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	-	-	-	3	-	-	-	-	-	3
CO2	-	-	-	1	3	-	-	1	-	-	3
CO3	-	-	-	3	3	-	-	3	-	-	-
CO4	-	3	-	-	-	3	3	-	-	-	-
CO5	-	-	-	3	3	-	-	-	-	-	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	2	3
CO2	2	3
CO3	2	2
CO4	1	3
CO5	2	3

Unit-Wise Syllabus:

UNIT – I: Introduction to Cyberlaw and Digital Evidence

Fundamentals of cyberlaw, legal challenges in cyberspace. Overview of digital evidence: types, handling, admissibility. Electronic records and digital signatures. Basics of IT compliance.

Practice- Draft a cyber incident response policy for an organization.

UNIT – II: Cybercrime and Legal Provisions

Classification of cybercrimes: financial fraud, hacking, identity theft, cyberstalking. Indian legal provisions: Overview of the IT Act, IPC sections related to cybercrime. GDPR and HIPAA.

Practice- Analyze a cybercrime case using applicable sections of the IT Act.

UNIT – III: Incident Response Fundamentals

Incident lifecycle: preparation, identification, containment, eradication, recovery, and lessons learned. Roles and responsibilities of incident response teams (IRT). IR policy and planning, communication strategies.

Practice- Simulate an incident handling process using a case scenario.

UNIT – IV: Investigation and Legal Procedures

Chain of custody, forensic documentation, logging and monitoring. Role of law enforcement. Reporting structure and formats. Collaboration with CERT-In and international agencies. Legal considerations during evidence handling.

Practice- Document and preserve digital evidence in a mock investigation.

UNIT – V: Compliance and Case Studies

Cybersecurity standards (ISO/IEC 27001, NIST). Industry-specific compliance: BFSI, healthcare, government. Real-world incident response case studies. Understanding penalties, liability, and digital rights.

Practice- Create a compliance checklist for data protection regulations (e.g., GDPR).

Textbooks:

1. Karnika Seth – Computers, Internet and New Technology Laws
2. Vivek Sood – Cyber Laws in India

Reference Books:

1. Thomas J. Holt – Cybercrime and Digital Forensics
2. Brian Carrier – File System Forensic Analysis

Web Links:

1. https://www.cert-in.org.in
2. https://www.meity.gov.in
3. https://www.sans.org/digital-forensics-incident-response/
4. https://www.nist.gov/cyberframework
5. https://www.cybercrime.gov.in

Advanced Linux

L	T	P	C
3	0	1	4

Course Code: 2512FS10

Semester II

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand advanced Linux architecture, kernel internals, and system boot process.
CO2: Administer, secure, and optimize Linux-based systems for multi-user environments.
CO3: Develop and troubleshoot shell scripts and automation tools for system administration.
CO4: Monitor, manage, and analyze Linux logs, permissions, and user roles for forensic readiness.
CO5: Explore Linux-based tools used in cybersecurity, penetration testing, and digital forensics.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	3	2	2-	1	2	3	2	1
CO2	3	3	3	3	3	2	2	3	3	3	3
CO3	2	2	3	3	2	3	1	3	3	2	1
CO4	3	3	3	3	3	3	2	3	2	2	2
CO5	3	2	3	3	3	2	2	3	3	2	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	2
CO3	3	1
CO4	3	2
CO5	3	2

Unit-Wise Syllabus:

UNIT – I: Advanced Linux Architecture & Kernel Internals

Overview of Linux architecture and distributions, Kernel types and compilation, The boot process: BIOS/UEFI, GRUB, systemd; Init systems: SysVinit vs systemd, Runlevels and targets
Linux Kernel modules: inserting, removing, listing; Process Management: ps, top, nice, kill, signals.

Practice- Kernel module installation and system boot configuration

UNIT – II: File Systems, Disk Management & Permissions

Advanced file system structure (EXT4, XFS), Mounting, unmounting, LVM: logical volume management; Disk partitioning, File permissions and ACLs, Special permissions: SUID, SGID, Sticky bit, File integrity and hashing (md5, sha256).

Practice- File system creation, LVM configuration, and permission auditing

UNIT – III: Networking, Security & User Management

Network configuration (CLI & GUI tools), TCP/IP, hostname resolution, DNS, DHCP, Network troubleshooting tools: netstat, ping, traceroute, iftop. User & group management. Firewall configuration: iptables, firewalld.

Practice- Network troubleshooting and firewall setup using iptables.

UNIT – IV: Shell Scripting & Automation

Bash shell scripting: variables, conditionals, loops. Functions, arrays, and string manipulation. Regular expressions and text processing (grep, awk, sed).

Practice- Bash script to automate backup and logging tasks

UNIT – V: System Monitoring, Logging & Forensics Tools

System logs: /var/log, journalctl, rsyslog. Log rotation and management. Performance monitoring: htop, iotop, vmstat, dstat. Linux system hardening techniques. Introduction to Linux forensics tools: Sleuth Kit, Autopsy. Packet sniffing with tcpdump.

Practice- Log analysis and detection of suspicious activities on a Linux system

Textbooks:

1. Mark G. Sobell – A Practical Guide to Linux Commands, Editors, and Shell Programming
2. Richard Blum – Linux Command Line and Shell Scripting Bible

Reference Books:

1. Brian Ward – How Linux Works: What Every Superuser Should Know
2. Paul Cobbaut – Linux Fundamentals

Web Links:

1. https://www.kernel.org/
2. https://linux.die.net/
3. https://tldp.org/
4. https://wiki.archlinux.org/
5. https://linuxsecurity.expert/

Cryptographic Backdoors

L	T	P	C
3	0	2	5

Course Code: 2512FS20

Semester II

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the concepts of cryptographic backdoors, including their architecture and history.
CO2: Identify and analyze intentional and unintentional backdoors in cryptographic algorithms and implementations.
CO3: Evaluate the ethical, legal, and political implications of backdoors in cryptographic systems.
CO4: Detect and prevent cryptographic backdoors using reverse engineering and formal verification techniques.
CO5: Investigate real-world cases of cryptographic backdoors in protocols, hardware, and software.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	1	2	2	1	2	1	2	2	1	1
CO2	3	2	3	3	2	2	1	3	2	2	2
CO3	2	1	1	2	3	2	3	2	2	1	3
CO4	3	3	3	3	2	2	1	3	2	2	2
CO5	3	2	3	3	2	2	2	3	3	2	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	2
CO3	2	3
CO4	3	2
CO5	3	2

Unit-Wise Syllabus:

UNIT – I: Introduction to Cryptographic Backdoors

Definition and scope of cryptographic backdoors, History and evolution of backdoors in cryptography, Classification: hardware, software, protocol-level, Intentional vs. unintentional backdoors, Threat modeling and attack surfaces, Governmental access mechanisms and national security concerns

Practice- Analyze a cryptographic PRNG implementation for bias or flaws.

UNIT – II: Backdoors in Cryptographic Algorithms

Design vulnerabilities in cryptographic primitives. Case studies: weak key generation, and pseudo-random number generators (PRNGs). Mathematical trapdoors in elliptic curve cryptography (ECC). Influence of NSA and standards organizations (e.g., NIST).

Practice- Perform entropy analysis and randomness testing on PRNG outputs.

UNIT – III: Implementation and Hardware Backdoors

Software-level cryptographic backdoors: libraries and compilers. Side-channel attacks. Hardware Trojan horses in cryptographic chips. Firmware backdoors and BIOS-level manipulations. Backdoored random number generators in embedded systems.

Practice- Compare secure vs. insecure encryption implementations.

UNIT – IV: Detection, Mitigation & Verification

Techniques for identifying backdoors: reverse engineering, fuzzing, and symbolic execution. Cryptanalysis and differential testing. Formal verification of cryptographic algorithms. Open-source cryptographic validation tools. Strategies for secure algorithm design and implementation.

Practice- Observe how weak or tampered encryption can lead to unauthorized access.

UNIT – V: Legal, Ethical & Case Studies

Legal framework surrounding cryptographic regulation. The debate over lawful intercept vs. user privacy. Ethical implications for cybersecurity professionals. Real-world case studies.

Practice- Analyze open-source crypto tools for potential flaws or backdoors.

Textbooks:

1. Bruce Schneier – Applied Cryptography
2. Christof Paar, Jan Pelzl – Understanding Cryptography

Reference Books:

1. Jean-Philippe Aumasson – Serious Cryptography
2. Niels Ferguson – Practical Cryptography

Web Links:

1. https://eprint.iacr.org/
2. https://verifpal.com/
3. https://www.schneier.com/
4. https://project-everest.github.io/

Quantum Computing in Steganography

L	T	P	C
2	0	2	4

Course Code: 2512FS23

Semester II

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the foundational principles of quantum mechanics relevant to quantum steganography.
CO2: Differentiate between classical and quantum steganographic techniques.
CO3: Apply quantum communication protocols for secure data hiding and covert communication.
CO4: Analyze the security and limitations of quantum steganographic systems.
CO5: Explore real-world applications and research challenges in quantum-based covert communication.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	1	2	3	1	2	1	2	3	1	1
CO2	2	1	2	3	1	2	1	2	2	1	1
CO3	3	2	3	3	2	2	1	3	3	2	2
CO4	3	2	3	3	2	2	1	3	2	2	2
CO5	3	1	2	3	2	2	1	2	3	2	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	1
CO3	3	2
CO4	3	2
CO5	3	1

Unit-Wise Syllabus:

UNIT – I: Introduction to Quantum Computing & Steganography

Basics of quantum mechanics: qubits, superposition, entanglement, and measurement. Classical vs. quantum communication. Introduction to steganography: definitions, history, importance in cybersecurity.

Practice- Implement a walk-based protocol for message hiding.

UNIT – II: Quantum Communication Foundations

Quantum information theory basics. Quantum entanglement and its role in secure communication.

Practice- Visualize quantum entanglement using quantum circuit simulations.

UNIT – III: Quantum Steganographic Protocols
Principles and models of steganography. Quantum steganography using entangled states. Quantum steganography via quantum dense coding.

Practice- Encode classical data into quantum bits (simulated).

UNIT – IV: Security, Detection & Countermeasures
Security analysis: quantum vs. classical security. Eavesdropping detection. Various forms of Steganalysis.
Practice- Explore security properties of quantum steganography via theoretical design.

UNIT – V: Applications and Research Frontiers
Quantum internet communication. Quantum steganography in future directions.
Practice- Research and present a simulation model of quantum steganography.

Textbooks:

1. Michael A. Nielsen & Isaac L. Chuang – Quantum Computation and Quantum Information
2. Mark M. Wilde – Quantum Information Theory

Reference Books:

1. William Stallings – Cryptography and Network Security
2. Shafi Goldwasser – Foundations of Cryptography

Web Links:

1. https://quantum-computing.ibm.com/
2. https://qiskit.org/
3. https://arxiv.org/
4. https://www.quantiki.org/
5. https://quantum.country/

Network Forensics

L	T	P	C
2	0	2	4

Course Code: 2512FS09

Semester II

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand core principles and components of network forensics.
CO2: Capture, analyze, and interpret network traffic for forensic purposes.
CO3: Use forensic tools to detect and trace network-based attacks.
CO4: Learn methods for evidence collection and preservation over networks.
CO5: Apply legal and ethical principles in network forensic investigations.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	1	2	3	2	1	1	2	2	1	1
CO2	3	3	3	3	2	2	2	3	2	2	2
CO3	3	3	3	3	2	2	2	3	2	3	2
CO4	3	3	3	3	3	3	2	3	2	2	2
CO5	1	1	1	1	3	2	3	2	2	2	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	1
CO3	3	2
CO4	3	3
CO5	2	3

Unit-Wise Syllabus:

UNIT – I: Introduction to Network Forensics

Overview of networks and its role in Digital Forensics. Key terminologies: packets, sessions, protocols. Differences between network forensics and traffic analysis.

Practice- Capture and analyze packets.

UNIT – II: Network Protocols and Log Analysis

Basics of TCP/IP, DNS, DHCP, HTTP, and SMTP protocols. Identifying abnormal behavior and traffic anomalies. Analyzing logs from firewalls, routers, IDS/IPS. Case studies of log-based investigations.

Practice- Investigate a simulated DDoS attack and trace the source.

UNIT – III: Packet Capture and Analysis Tools

Packet capturing tools: Wireshark, tcpdump, Network miner. Deep packet inspection and protocol analysis. Session reconstruction and filtering techniques. Identifying suspicious packets and payload analysis.

Practice- Analyze firewall and IDS logs to detect intrusion patterns.

UNIT – IV: Intrusion Detection and Attack Tracing

Types of network attacks: DDoS, port scanning, spoofing, ARP poisoning, MITM. Role of IDS/IPS in forensics. Signature vs. anomaly-based detection. Tracing attack sources and attribution.

Practice- Reconstruct HTTP sessions from packet captures.

UNIT – V: Evidence Handling and Reporting

Evidence acquisition: Chain of custody, integrity, and preservation. Writing forensic reports. Presenting findings in court. Network forensics in the cloud and wireless environments. Challenges and best practices.

Practice- Create a forensic report based on a simulated network breach.

Textbooks:

1. Nikhil Kumar – Network Forensics
2. Jason Luttgens – Network Forensics: Tracking Hackers through Cyberspace

Reference Books:

1. Eric Cole – Network Security Bible
2. Michael Collins – Network Security Through Data Analysis

Web Links:

1. https://www.wireshark.org
2. https://www.sans.org
3. https://packetlife.net
4. https://www.malware-traffic-analysis.net
5. https://www.varonis.com/blog/network-forensics

Memory Forensics

L	T	P	C
2	0	2	4

Course Code: 2512FS06

Semester II

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the principles and importance of volatile memory analysis.
CO2: Learn the architecture and structure of memory in modern systems.
CO3: Use forensic tools for memory acquisition and investigation.
CO4: Detect malware, rootkits, and hidden activities from memory dumps.
CO5: Correlate memory evidence with incident response and investigation.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	1	2	3	2	1	1	2	2	1	1
CO2	3	1	2	3	1	1	1	2	2	1	1
CO3	3	3	3	3	2	2	1	3	2	2	2
CO4	3	3	3	3	3	2	1	3	2	2	2
CO5	3	3	2	3	3	2	2	3	2	2	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	1
CO3	3	2
CO4	3	2
CO5	3	3

Unit-Wise Syllabus:

UNIT – I: Introduction to Memory Forensics

Importance of volatile data, memory components, types of memory (RAM, cache), memory vs. disk forensics, basic memory acquisition methods, live vs. dead acquisition, legal considerations.

Practice- Capture memory using DumpIt and FTK Imager.

UNIT – II: Memory Acquisition

Memory acquisition methods and tools (FTK Imager, DumpIt, LiME), live acquisition techniques, imaging volatile memory safely, maintaining integrity through hashing (MD5, SHA1), chain of custody, challenges in capturing memory from various operating systems.

Practice- Analyze Windows registry.

UNIT – III: Volatility Framework and Plugins

Introduction to Volatility, installation and usage. Plugins for process analysis, DLLs, handles, network connections, services, clipboard, and command history. Practical investigations using Volatility.
Practice- Recover command history and clipboard activity from memory.

UNIT – IV: Malware and Attack Detection

Indicators of compromise in memory, rootkits, keyloggers, and hidden processes. Analyzing PE headers, Timelining user and attacker activity.

Practice- Identify malware behavior and injected code in RAM.

UNIT – V: Advanced Memory Forensics and Tools

Shellbags, ShimCache, Registry analysis, Memory compression, Virtual memory analysis. Advanced tools: Rekall, Redline, Bulk Extractor. Report generation and forensic documentation.

Practice- Detect credential dumping from memory.

Textbooks:

1. Michael Hale Ligh – The Art of Memory Forensics
2. Sherri Davidoff – Network Forensics (select chapters)

Reference Books:

1. Chris Pogue – Unix and Linux Forensic Analysis Toolkit
2. Eoghan Casey – Digital Evidence and Computer Crime

Web Links:

1. https://volatilityfoundation.org
2. https://rekall-forensic.readthedocs.io
3. https://github.com/volatilityfoundation
4. https://www.memoryanalysis.net
5. https://digital-forensics.sans.org

Ethical Hacking and Cyber Risk Assessment

L	T	P	C
2	0	2	4

Course Code: 2512FS12

Semester III

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand key terms and concepts in web fundamentals
CO2: Understand the underlying principles in how a windows server hardening is done.
CO3: Ability to understand the RFI and LFI (remote file inclusion; local file inclusion) vulnerability.
CO4: Ability to identify, analyze and remediate Advanced session analysis, hijacking, and fixation techniques by learning and implementing real-world scenarios.
CO5: Understand key terms and concepts of Static and Dynamic Analysis for Mobile Applications.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	1	2	3	1	1	1	2	2	1	1
CO2	3	2	3	3	2	2	1	3	2	2	2
CO3	3	2	3	3	2	2	1	3	2	2	1
CO4	3	3	3	3	2	2	2	3	2	2	2
CO5	3	2	2	3	2	2	1	3	2	2	1

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	1

Unit-Wise Syllabus:

UNIT – I: Introduction to Ethical Hacking & Risk Assessments

Definition and Goals of Ethical Hacking, Importance of Ethical Hacking in Cyber Security, Types of Hackers (White Hat, Black Hat, Grey Hat, etc.), Phases of Ethical Hacking, Reconnaissance/Information Gathering **(**Passive and active reconnaissance) Scanning (Port Scanning, Vulnerability Scanning, and Network Scanning) Gaining Access (Exploiting Vulnerabilities) Maintaining Access (Installing Backdoors, Trojans, Rootkits)

Practice- Configure Burp Suite and perform the operations - Intruder, Spider, Repeater and Sequencer.

UNIT – II: Footprinting and Scanning

Mapping a Network: Why Map a (Remote) Network, Ping Sweeping: Fping, Nmap Ping Scan, OS Fingerprinting: Fingerprinting with Nmap Port Scanning, Three Way Handshake, Scan Types, TCP Connect Scan with Nmap, TCP SYN Scan with Nmap, Version Detection with Nmap, Specifying the Targets: By DNS Name, With an IP Addresses List, Choosing the Ports to Scan, Nmap Examples, Port Scanning, Service Detection, Vulnerabilities Database Lookup.

Practice- Perform a vulnerability scan and generate a pentest report.

UNIT – III: Web Application Pen Testing

Brute-force, Dictionary-based Enumeration. Cross Site Scripting, XSS Actors, Vulnerable Web Applications, Users, Attackers, Finding an XSS, Reflected XSS Attacks, Reflected XSS Filters, Understanding of various injection techniques.

Practice- Identify vulnerability in a website/app and generate a mitigation report.

UNIT – IV: Advanced Exploitation Techniques

Password Attacks: Brute Force Attacks, Dictionary Attack, Rainbow Tables. Cross-Site Request Forgery (CSRF), File Inclusion Attacks, Insecure CAPTCHA Analysis, and Web-Based Attack Vectors.

Practice- Perform defense mechanism of XSS

UNIT – V: Static and Dynamic Analysis

Static and Dynamic Analysis Techniques, Focusing on Architecture, Design, Threat Modeling, Data Storage, Privacy, Cryptography, Authentication, and Session Management. Identification and Mitigation of Vulnerabilities such as Insecure Direct Object References, Information Leakage, Improper Error Handling, Request Forgery, and Remote Code Execution, Secure Coding Principles.

Practice- Scan a local server and prepare the gap report.

Textbooks:

1. Learning Nessus for Penetration Testing, by Himanshu Kumar.
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.

Reference Books:

1. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (by Dafydd Stuttard, Marcus Pinto).
2. Metasploit - The Penetration Tester's Guide Paperback – Import, 15 Jul 2011 by David Ken.

Web Links:

1. https://purplesec.us/learn/vulnerability-assessment-vs-penetration-testing/
2. https://spp.org/documents/22755/vul_assess_video.pdf
3. https://www.nitttrchd.ac.in/imee/Labmanuals/Vulnerability%20Assessment.pdf
4. http://www.pentest-standard.org/
5. https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Assessment_Cheat_Sheet.html

Digital Frauds

L	T	P	C
2	0	2	4

Course Code: 2512FS21

Semester III

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand various types of digital frauds and their evolving techniques.
CO2: Analyze fraud schemes in sectors like banking, e-commerce, social media, and telecom.
CO3: Apply digital forensic methodologies to investigate and mitigate digital frauds.
CO4: Understand the legal and regulatory frameworks related to cyber frauds.
CO5: Implement preventive and detective measures using real-time fraud detection tools.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	3	2	1	1	2	2	1	2
CO2	3	3	3	3	2	2	2	3	2	2	2
CO3	3	3	3	3	3	3	2	3	2	2	2
CO4	2	1	1	2	3	2	3	2	2	1	3
CO5	3	3	3	3	3	2	2	3	3	2	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	3	3
CO4	2	3
CO5	3	2

Unit-Wise Syllabus:

UNIT – I: Introduction to Digital Frauds

Definition and classification of digital frauds. Evolution of cyber frauds in the digital economy. Fraud triangle: Opportunity, Motivation, Rationalization. Overview of key fraud sectors: banking, insurance, healthcare, education, and e-commerce. Economic and reputational impact of digital fraud.

Practice- Identify and trace the source using headers and IP tracking of a simulated phishing attack.

UNIT – II: Common Types of Digital Frauds

Email and phishing frauds. Identity theft and synthetic identity fraud. Credit card and banking frauds (SIM swap, UPI frauds, ATM skimming). Online marketplace and auction frauds. Telecom and mobile-based frauds. Ransomware and extortion schemes.

Practice- Use Wireshark to detect suspicious data transfers from a network

UNIT – III: Digital Forensics in Fraud Investigation

Forensic approach to detecting digital fraud. Evidence collection, chain of custody, and analysis. Investigation of fraudulent emails, call logs, device images, and logs. Metadata analysis, log correlation, IP tracing. Case studies.

Practice- Create an awareness report on current fraud trends and mitigation.

UNIT – IV: Tools & Techniques for Fraud Detection

Introduction to fraud detection systems (FDS). Real-time monitoring tools for banking and e-commerce. Machine Learning and AI in fraud detection. Data analytics and visualization tools for fraud correlation. Fraud detection rules, red flags, and behavioral anomalies.

Practice- Trace a fraudulent transaction scenario using open-source blockchain explorers.

UNIT – V: Legal Framework & Cyber Ethics

Indian legal provisions: IPC, IT Act 2000 (Amendment 2008), RBI guidelines. Role of CERT-IN, RBI Ombudsman, Cyber Police. Case filing, reporting portals (cybercrime.gov.in), and grievance redressal. International regulations: GDPR, PCI-DSS recommendations on fraud. Ethical aspects in fraud investigations, privacy, and user data protection.

Practice- Analyze an e-commerce website and identify IOC's.

Textbooks:

1. Joseph T. Wells – Principles of Fraud Examination
2. Sudeep Das – Digital Fraud: Prevent, Detect, and Investigate

Reference Books:

1. Satish Jain – Cyber Security and Cyber Laws
2. Manan Thakkar – Digital Forensics and Cyber Crime with Kali Linux

Web Links:

1. https://cybercrime.gov.in/
2. https://www.cert-in.org.in/
3. https://www.fraud-magazine.com/
4. https://rbi.org.in/
5. https://www.finra.org/

Governance, Risk and Compliance

L	T	P	C
3	0	1	4

Course Code: 2512FS22

Semester III

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the principles and frameworks of IT and cybersecurity governance.
CO2: Identify, assess, and mitigate organizational and IT-related risks.
CO3: Evaluate compliance requirements with regulatory standards and industry frameworks.
CO4: Develop and implement GRC strategies aligned with business goals.
CO5: Apply tools and techniques for monitoring, auditing, and improving GRC processes.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	1	2	3	2	2	1	3	3	2	1
CO2	3	3	3	3	2	2	1	3	3	3	1
CO3	2	1	1	2	3	3	3	2	2	2	3
CO4	3	2	2	3	2	3	2	3	3	3	1
CO5	3	3	3	3	3	3	2	3	3	3	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	2
CO2	3	2
CO3	2	3
CO4	3	2
CO5	3	2

Unit-Wise Syllabus:

UNIT – I: Introduction to GRC

Definition and importance of GRC in cybersecurity. Components and integration of Governance, Risk, and Compliance. GRC drivers: Legal, regulatory, and business. Organizational structure, roles, and responsibilities in GRC. Global GRC trends and digital transformation impacts.

Practice- Conduct a sample risk assessment for a critical application

UNIT – II: IT and Cybersecurity Governance

IT governance frameworks: COBIT, ITIL, ISO/IEC 38500. Cybersecurity governance: Principles, policies, procedures. Aligning cybersecurity with enterprise objectives. Roles of CISO, CIO, and board in governance. Measuring governance effectiveness using KPIs and metrics.

Practice- Create a governance policy template for an IT department

UNIT – III: Risk Management

Types of risks: Strategic, operational, technical, compliance, reputational. Risk management process: Identification, analysis, evaluation, treatment, monitoring. Qualitative and quantitative risk assessments. Risk mitigation and risk appetite.

Practice- Analyze a real-world GRC failure (case study presentation)

UNIT – IV: Regulatory and Legal Compliance
Compliance standards: GDPR, HIPAA, SOX, PCI-DSS, HI TRUST, ISO 27001, NIST. Auditing and reporting for compliance. Data protection, privacy policies, breach notification rules. Role of automation in compliance management.
Practice- Identify non-compliance issues in a provided case scenario.

UNIT – V: GRC Tools and Case Studies

Introduction to GRC platforms: RSA Archer, MetricStream, ServiceNow GRC. Implementation of the lifecycle of GRC tools. Integrating GRC with enterprise risk management and security operations. Case studies on GRC failure and success in organizations. Developing a GRC strategy roadmap.

Practice- Prepare a compliance checklist and audit report.

Textbooks:

1. Gerardus Blokdyk – Governance, Risk and Compliance: Complete Self-Assessment Guide
2. Anthony Tarantino – Governance, Risk, and Compliance Handbook

Reference Books:

1. Mark Bragg – IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT
2. David Kim & Michael Solomon – Fundamentals of Information Systems Security

Web Links:

1. https://www.isaca.org/
2. https://www.nist.gov/cyberframework
3. https://gdpr.eu/
4. https://www.metricstream.com/
5. https://www.iso.org/isoiec-27001-information-security.html

Business Continuity Plan

L	T	P	C
3	0	1	4

Course Code: 2512FS02

Semester III

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the fundamentals and life cycle of business continuity planning.
CO2: Assess organizational risks and perform Business Impact Analysis (BIA).
CO3: Design, document, and implement effective BCP strategies.
CO4: Apply recovery planning techniques for IT, operations, and critical services.
CO5: Evaluate BCP effectiveness through simulation, testing, and continuous improvement.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	3	2	2	1	3	3	2	1
CO2	3	3	3	3	2	2	1	3	3	2	2
CO3	3	2	2	3	2	3	2	3	3	3	2
CO4	3	3	3	3	3	3	2	3	3	3	2
CO5	3	2	2	3	3	3	2	3	3	3	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	2
CO3	3	2
CO4	3	2
CO5	3	2

Unit-Wise Syllabus:

UNIT – I: Introduction to Business Continuity

Definition, importance, and scope of Business Continuity. Relationship between BCP, Disaster Recovery (DR), Crisis Management, and Risk Management. Regulatory requirements. Phases of Business Continuity Life Cycle. Governance structure and roles in BCP.

Practice- Prepare a Business Impact Analysis report for a sample organization.

UNIT – II: Risk Assessment and Business Impact Analysis (BIA)

Risk identification and classification. Threat modeling (natural, technical, human-induced threats). BIA process: Identifying critical functions, RTO, RPO, MTPD. Asset classification and prioritization. Interdependencies between functions and services.

Practice- Develop a complete BCP document with communication flow and recovery strategies

UNIT – III: Strategy Development and Planning

Business Continuity Strategies: Alternate site, backup services, cloud redundancy. Incident Response and Communication Plans. Recovery strategies for IT systems, applications, data, and personnel. Supply chain and vendor risk considerations. Legal and compliance aspects in continuity planning.

Practice- Identify critical assets and draft a risk mitigation matrix.

UNIT – IV: BCP Implementation and Testing

BCP Employee training and awareness programs. Coordination with emergency response and civil defense agencies.

Practice- Design a communication plan during an incident.

UNIT – V: Monitoring, Review & Improvement

Performance metrics and KPIs for BCP. Audit and assessment of continuity capabilities. Incident analysis and root cause identification. Continuous improvement and lifecycle refresh. Case studies: Business continuity failures and best practices

Practice- Test a mock BCP activation scenario and evaluate response.

Textbooks:

1. Andrew Hiles – Business Continuity Management: Global Best Practices
2. Michael Wallace – Business Continuity and Disaster Recovery Planning for IT Professionals

Reference Books:

1. NIST SP 800-34 – Contingency Planning Guide for Federal Information Systems
2. ISO/IEC 22301 – Societal Security – Business Continuity Management Systems

Web Links:

1. https://www.fema.gov/emergency-managers/risk-management/business-continuity
2. https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
3. https://www.iso.org/standard/75106.html
4. https://www.ready.gov/business
5. https://www.thebci.org/

Mobile and IOT Forensics

L	T	P	C
2	0	2	4

Course Code: 2512FS08

Semester III

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the forensic process for mobile and IoT devices.
CO2: Explore data acquisition techniques across platforms (Android, iOS, IoT).
CO3: Analyze artifacts from mobile apps, messaging, calls, GPS, and IoT logs.
CO4: Evaluate tools used for forensic investigation of smart and embedded devices.
CO5: Study challenges, legal issues, and standard procedures in mobile/IoT forensics.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	2	2	3	2	2	1	3	3	2	1
CO2	3	3	3	3	2	3	1	3	2	2	2
CO3	3	3	3	3	2	3	1	3	3	2	2
CO4	3	3	3	3	2	3	1	3	3	3	2
CO5	2	1	1	2	3	2	2	2	2	2	3

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	3	1
CO3	3	2
CO4	3	2
CO5	2	3

Unit-Wise Syllabus:

UNIT – I: Introduction to Mobile and IoT Forensics

Overview of mobile and IoT forensics, significance in modern investigations, challenges, mobile OS architecture (Android & iOS), IoT device ecosystem, legal aspects, and forensic standards.

Practice- Analyze mobile app artifacts.

UNIT – II: Mobile Device Forensics: Data Acquisition

Types of data: device, app, cloud-based; Acquisition methods: logical, physical, file system, and manual.

Practice- Perform logical and physical acquisition of an Android device.

UNIT – III: Mobile Device Forensics: Data Analysis

Recovery and analysis of contacts, messages, call logs, app data, GPS/location data, browser history, photo/video metadata, deleted data recovery, malware detection in mobile OS.

Practice- Extract and analyze GPS data and messaging logs.

UNIT – IV: IoT Device Forensics

IoT device types: wearables, smart home, healthcare, surveillance, automotive. Acquisition techniques, Case studies.

Practice- Investigate IoT device logs and firmware using network traffic analysis.

UNIT – V: Challenges, Legal Frameworks, and Reporting

Limitations of mobile/IoT forensics: encryption, obfuscation, cloud dependency. Privacy considerations. Reporting structure and admissibility in court. Global standards and legal references.

Practice- Simulate forensic acquisition from a smart home hub or wearable device.

Textbooks:

1. Andrew Hoog – Mobile Forensics: Advanced Investigative Strategies
2. Satish Bommisetty – Learning iOS Forensics

Reference Books:

1. Sean Morrissey – Android Forensics

2. Heather Mahalik – Mobile Device Forensics Cookbook

Web Links:

1. https://www.magnetforensics.com
2. https://www.cellebrite.com
3. https://www.mobileforensicscentral.com
4. https://www.iotforensic.org
5. https://www.forensicfocus.com

Skill Enhancement Courses (SEC)

Course Code	Sem	Course Name	Level	L	T	P	C	CIE	SEE	Total	Pre-requisite
2512FS13	I	IT Skills	FC			2	2	50	50	100	-
2512FS11	II	Courtroom Testimony	FC	2			2	50	50	100	-
2512FS15	III	Research Methodology & Scientific Writing	FC	4			4	50	50	100	-
2512FS16	IV	Student Activity Based Learning	FC				2	100	-	100	-
Total				**6**		**2**	**10**				

IT Skills

(Common to M.Sc. Forensic Science & M.Sc. Cyber Security & Digital Forensics)

Course Code: 2512FS13

L	T	P	C
0	0	2	2

Semester I

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the role of computing and information technology in the digital world.
CO2: Identify, describe, and apply emerging technologies in teaching and learning environments.
CO3: Effectively apply written, oral, and interpersonal communication skills and use information technology.
CO4: Analyze organizational context, strategy, operations, processes, and performance.
CO5: Understand the importance of keeping safe online.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	3	1	1	2	1	1	1	2	2	1	1
CO2	2	1	1	2	1	2	1	2	3	1	1
CO3	1	1	1	1	2	3	3	2	3	3	2
CO4	2	2	1	3	1	2	1	3	3	3	1
CO5	3	2	3	2	3	1	1	2	2	1	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	3	1
CO2	2	1
CO3	2	2
CO4	2	1
CO5	3	3

Unit-Wise Syllabus:

UNIT - I: Advanced Computer & Office Automation

Computer Fundamentals: In-depth study of CPU architecture, memory management, and system performance optimization. Advanced Operating Systems: Multi-user OS, virtualization,

file system management, and cloud computing integration. Office Automation: AI-driven automation, workflow optimization, and integration with cloud services (Google Drive, OneDrive). Cybersecurity in Office Systems: Data encryption, access control, and secure document handling.

Practice- Document Formatting & Structuring in Microsoft Word

UNIT II: Microsoft Word - Advanced Document Processing

Advanced Formatting & Structuring: Custom templates, multi-section formatting, indexing, and citations. Collaboration & Review: Track changes, comments, version history, and co-authoring in cloud environments. Macros & Automation: Automating repetitive tasks with macros and scripting for efficiency. Security & Legal Considerations: Document encryption, digital signatures, and access control.

Practice- Data Analysis & Visualization in Microsoft Excel

UNIT III: Microsoft Excel - Data Analytics & Automation

Data Analysis & Visualization: Advanced PivotTables, Power Query, and Power BI integration. Complex Formulas & Functions: Nested formulas, array formulas, and statistical functions. Automation & Scripting: VBA for automation, creating custom macros, and automating repetitive tasks. Big Data & Database Connectivity: Importing/exporting data from SQL, Access, and online sources.

Practice- Professional Presentation Design in Microsoft PowerPoint

UNIT IV: Microsoft PowerPoint - Professional Presentation & Multimedia Integration

Advanced Slide Design: Custom themes, dynamic transitions, and interactive elements. Multimedia & Interactivity: Embedding videos, hyperlinks, live polls, and audience engagement tools. AI-Enhanced Presentations: Smart suggestions, real-time transcription, and speech-to-text integration. Cloud & Collaboration: Co-authoring, real-time editing, and remote presentation delivery.

Practice- Email & Calendar Management in Microsoft Outlook

UNIT V: Microsoft Outlook & Professional Communication

Email Automation & Management: Rules, filters, scheduled emails, and AI-based categorization. Task & Calendar Optimization: Recurring tasks, shared calendars, and integration with project management tools. CRM & Contact Management: Advanced contact

grouping, mailing lists, and business communication strategies. Data Security & Compliance: Email encryption, phishing protection, and legal compliance for professional use.

Practice- Office Automation Integration & Workflow Optimization

Textbooks:

1. Digital Logic and Computer Design – M. Morris Mano
2. Digital Fundamentals – Thomas L. Floyd

Reference Books:

1. Digital Logic Design and Computer Organization – Nikrouz Faroughi
2. Fundamentals of Digital Logic with VHDL Design – Stephen Brown & Zvonko Vranesic.

Web Links:

1. https://www.coursera.org/browse/information-technology
2. https://www.globalknowledge.com/us-en/training/course-catalog/
3. https://alison.com/courses/it
4. https://www.cbtnuggets.com/it-training
5. https://skillsbuild.org/learners

Courtroom Testimony

(Common to M.Sc. Forensic Science & M.Sc. Cyber Security & Digital Forensics)

Course Code: 2512FS11

L	T	P	C
2	0	0	2

Semester II

Course Outcomes:

At the end of the course, students will be able to:

CO1: Compare/contrast evidence admissibility standards in federal and state courts.
CO2: Relate scientific evidence to other components of the criminal justice system.
CO3: Use key court rulings to discuss admissibility and presentation of scientific evidence.
CO4: Apply concepts and principles of scientific evidence admissibility to real world cases & explain the role expert testimony plays in criminal and civil cases.
CO5: Demonstrate the process of expert testimony, including qualification, direct- and cross-examination Discuss ethical considerations for expert witnesses.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11
CO1	2	2	3	2	3	2	2	2	1	2	1
CO2	2	2	3	2	3	1	2	2	1	2	1
CO3	3	2	3	2	3	2	3	2	1	2	1
CO4	3	2	3	2	3	2	3	2	1	3	1
CO5	3	2	2	2	3	2	3	1	1	3	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	PSO1	PSO2
CO1	2	3
CO2	2	3
CO3	2	3
CO4	2	3
CO5	1	3

Unit-Wise Syllabus:

UNIT - I: Fundamentals of Expert Witness Testimony

Role and responsibilities of an expert witness, Legal framework: Rules of evidence and admissibility (Frye, Daubert standards), Voir dire: Qualification and disqualification of experts, Ethical considerations and professional conduct in testimony, Case studies on expert witness credibility.

UNIT - II: Preparation of Expert Witness Documents

Drafting an expert witness Curriculum Vitae (CV), Creating and structuring expert reports, Developing testimony question lists (voir dire, direct, and cross-examination, Handling conflicting evidence and maintaining objectivity, Practical exercise: Writing a CV and testimony question list.

UNIT - III: Courtroom Procedures and Mock Testimony

Structure of courtroom proceedings and legal terminology, Roles of the judge, jury, attorneys, and expert witnesses, Direct and cross-examination techniques, Handling aggressive questioning and maintaining composure, Practical exercise: Conducting a mock testimony session

UNIT - IV: Virtual and Simulated Trial Practice

Virtual court procedures and online legal platforms, Differences between virtual and in-person testimony, Conducting a mock trial: Opening statements, expert qualification, and testimony
Evaluating testimonies: Peer review techniques and self-assessment, Practical exercise: Participating in a virtual mock trial

UNIT -V: Post-Testimony Analysis and Professional Development

Reviewing courtroom performance and feedback analysis, Writing a reflection paper on courtroom experiences, Identifying strengths and areas for improvement, Continuous learning: Attending legal workshops and expert witness training
Practical exercise: Writing a reflection paper on the mock trial experience

Textbooks:

1. Faigman, D. L., Kaye, D. H., Saks, M. J., & Sanders, J. (2018). Modern Scientific Evidence: The Law and Science of Expert Testimony.
2. Risinger, D. M. (2019). The New Wigmore: A Treatise on Evidence – Expert Evidence.

Reference Books:

1. Saks, M. J., & Faigman, D. L. (2022). Expert Evidence and Scientific Proof in the Courtroom.
2. Schumann, A. D. (2017). Testifying in Court: A Guide for Expert Witnesses

Web Links:

1. National Institute of Justice (NIJ): www.nij.gov
2. Federal Judicial Center: www.fjc.gov
3. American Academy of Forensic Sciences (AAFS): www.aafs.org
4. Daubert Tracker (Legal Expert Testimony Database): www.dauberttracker.com
5. Expert Witness Training Online: www.seak.com

Research Methodology & Scientific Writing

(Common to M.Sc. Forensic Science & M.Sc. Cyber Security & Digital Forensics)

Course Code: 2512FS15

Semester III	L	T	P	C
	4	0	0	4

Course Outcomes:

At the end of the course, students will be able to:

CO1: Understand the fundamental principles of research methodology, including the meaning, objectives, and types of research.

CO2: Learn the process of identifying a research problem, formulating hypotheses, and designing research studies.

CO3: Explore various research methods, experimental designs, and data collection techniques used in scientific investigations.

CO4: Apply statistical and sampling techniques for effective data analysis and interpretation in research.

CO5: Develop scientific writing skills for preparing research reports, abstracts, and proposals for academic and professional use.

Mapping of Course Outcomes with Program Outcomes:

CO/PO	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**
CO1	3	3	2	3	2	2	1	3	3	2	1
CO2	3	3	2	3	2	2	1	3	3	2	1
CO3	3	3	2	3	2	2	1	3	3	2	1
CO4	3	3	3	3	2	2	1	3	3	2	1
CO5	3	2	2	3	2	3	3	3	3	3	2

Mapping of Course Outcomes With Program Specific Outcomes:

CO/PSO	**PSO1**	**PSO2**
CO1	3	2
CO2	3	2
CO3	3	1
CO4	3	1
CO5	3	3

Unit-Wise Syllabus:

Unit-I: Introduction to Research Methodology

Introduction to Research, Meaning of Research, Definition, Characteristics and Functions, Objectives, Classification and Kinds of Research, Research Problem, Introduction to Research Problems, Selecting and Defining the Research Problem, Sources of Research Problems, Criteria for Selection the Problem, Delimiting a Problem, Assumptions about a Problem, Evaluating the Problem.

Unit -II: Hypothesis Formulation & Research Design

Meaning and Definitions of Hypothesis, Assumptions, Postulates, Functions, Importance, Kinds, Characteristics of a Good Hypothesis, Variables in a Hypothesis, Sources of Hypothesis, Testing of Hypothesis, Research Plan and Design, Meaning and Definition of Research Design, Types and Characteristics of Research Design, Sampling, Meaning and Definition of Sampling, Functions of Population and Sampling, Types of Sampling Designs, Characteristics of a Good Sample, Application of Sampling Technique in Various Types of Research.

Unit- III: Types of Research & Experimental Design

Survey Research, Historical Research, Philosophical Research, Experimental Research, Case Study Research, Genetic Research, Need and Purpose of Experimental Design, Importance, Characteristics of Good Experimental Design, Basic Principles of Experimental Design, and Types of Basic Experimental Design.

Unit -IV: Research Tools & Data Collection

Questionnaire, Schedule, Rating Scale, Tests, Achievement Tests, Aptitude Tests, Psychological Tests, Meaning and Importance of Data Collection, Nature of Data, Qualitative vs. Quantitative Data, Constants, Variables, Variates, Characteristics of Quantitative Data, Types of Data, Primary Data, Secondary Data, Methods of Data Collection, Interviews, Observations, Surveys, Experiments, Organization and Classification of Data.

Unit-V: Scientific Writing & Research Report Preparation

Research Report Writing, Need, Importance, Format, Preliminary Section, Main Section, Reference Section, Mechanics of Report Writing, Scientific Writing, Writing Research Abstracts, Writing Research Papers, Purpose, Structure, Submission Process, Research Proposal Writing, Need, Structure, Writing for Dissertations, Ph.D., and Preparing Proposals for Research Funding.

Textbooks

1. Kothari, C. R. (2004). Research methodology: Methods and techniques (2nd ed.). New Age International.

2. Creswell, J. W. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage publications.

References

1. Babbie, E. (2020). The practice of social research (15th ed.). Cengage Learning.
2. Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

Web Links

1. https://www.scribbr.com/methodology/
2. https://www.researchgate.net/publication/Research_Methodology
3. https://www.sagepub.com/en-us/nam/research-methods
4. https://www.sciencedirect.com/topics/social-sciences/research-methodology
5. https://www.elsevier.com/authors/tools-and-resources/researcher-academy