Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

M.Sc. Cyber Forensics - II SEMESTER
Batch 2025 - 2027

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
MSCFN201		Forensic Data Base Analysis	60	20	20	30	20	3	0	2	4

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P – Practical; C - Credit; Th. - Theory
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Learning Objectives:

The student should develop skills and understanding in:

1. The design methodology for databases and verifying their structural correctness
2. Implementing databases and application software primarily in the relational model
3. Using querying languages, primarily SQL, and other database supporting software
4. Applying the theory behind various database models and query languages
5. Implementing security and integrity policies relating to databases
6. The basic principles behind data warehousing and preparation for data analytics
7. Working in group settings to design and implement database projects

Learning outcomes:

1. Basic data structures and their uses (lists, arrays)
2. The basic concepts of object-oriented programming (classes, inheritance)
3. The design, implementation, and testing of medium-sized problem solutions in software
4. contexts in which databases are used
5. basic familiarity with a Unix environment.

Unit –I Fundamentals of Databases

What is a Database, DBMS - Purpose of DB and Users of DB, Components of DB, Concepts of RDBMS, Basic SET Concepts (SET, Subset), Set of Ordered Tuples - Relations as a DB (Concepts of PK, FK, Surrogate Keys, Composite Keys, Candidate Keys), Relational DB Operators (Cartesian Product, Union, Intersect, Difference), Relational DB Normal Forms (1NF, 2NF, 3NF) - E-R Model.

Unit –II Database Security Lifecycle

Concept of DB Security Lifecycle, Creating Data Risk Assessment, Analyzing data threats, risks & vulnerabilities, need for database security architecture, implementing feedback mechanisms, Adjusting policies & practices based on feedback mechanisms using different security models.

Unit –III Database Security

Models-Access Matrix Models, Objects & Subjects, Types of Objects & Subjects, Access Modes (Static & Dynamic), Access Levels, Issues in Database Security, Database Access Controls, Security Logs and Audit Trails, Encryption, SQL Data Control Language, Security in Oracle, Statistical Database Security, SQL Injection, Database Security and Internet.

Unit-IV Password Management

Authentication and Password Security: choosing an appropriate authentication option, understanding system administration privileges, choosing strong passwords, implementing account lockout after failed login attempts, creating and enforcing password profiles, using passwords for all database components, understanding and securing authentication back doors

Unit-V Virtual Private Databases

Introduction to VPDs, How VPDs work, VPD Components, how to use VPD, Example, Security Measures, Direct Attacks Against Computer, Need for VPDs, Implementing VPDs

Suggested Reading

1. Fundamentals of Database System" by ElmasriRamez and NavatheShamkant
2. Database Management Systems" by SEEMA KEDAR
3. Database Management Systems" by Panneerselvam R
4. Database Management Systems" by G K Gupta
5. Database Security" by Alfred Basta and Melissa Zgola
6. Information Warfare and Security (ACM Press)" by Dorothy E Denning

LIST OF EXPERIMENTS:

1. Design a Database and create required tables. For e.g. Bank, College Database
2. Apply the constraints like Primary Key , Foreign key, NOT NULL to the tables.
3. Write a sql statement for implementing ALTER, UPDATE and DELETE
4. Write the queries to implement the joins
5. Write the query for implementing the following functions: MAX(),MIN(),AVG(),COUNT()
6. Write the query to implement the concept of Integrity constrains
7. Write the query to create the views 8) Perform the queries for triggers .
8. Perform the following operation for demonstrating the insertion , updation and deletion usingthe referential integrity constraints
9. Write the query for creating the users and their role.

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

M.Sc. Cyber Forensics - II SEMESTER
Batch 2025 - 2027

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
MSCFN202		Computer Network and Forensics	60	20	20	30	20	3	0	2	4

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P – Practical; C - Credit; Th. - Theory
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Course Objectives: The student will have ability:
1. To understand the different aspects of Network Security.
2. To learn about different Cryptography Encryption and Decryption Technique.

Course Outcomes: Upon completion of the subject, students will be able to:
1. Understand Need of Security in and Type of threats.
2. Understand Security mechanism and basic and Advance Ciphers.
3. Understand Advance encryption Techniques.
4. Understand the Key exchange protocols used in Public Key Cryptography.
5. Understand the Authentication and Steganography concept.

Unit-1

Introduction to Network, Internet, IP address, Private and Public IP address, Classes of IP address, Subnetting IP address, TCP 3 Three-Way Handshake, OSI model, TCP/IP model, MAC address, Cookies, Cache, LAN, WAN, Standards and Protocols, Advance network configuration and troubleshooting

Unit -2

Introduction to Switched Networks, Basic Switching Concepts and Configuration Routing Dynamically, VLANs, Routing Concepts, Inter-VLAN Routing, Static Routing, Routing Dynamically, Single-Area OSPF, Access Control Lists, DHCP, Network Address Translation for IPv4

Unit-3

Introduction to Scaling Networks, LAN Redundancy, Link Aggregation, Wireless LANs, Adjust and Troubleshoot Single-Area OSPF, Multiarea OSPF, EIGRP, EIGRP Advanced Configurations and Troubleshooting, IOS Images and Licensing

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

M.Sc. Cyber Forensics - II SEMESTER
Batch 2025 - 2027

Unit-4

Connecting Networks, Hierarchical Network Design, connecting to the WAN, Point-to-Point Connections, Frame Relay, Network Address Translation for IPv4, Broadband Solutions, Securing Site-to-Site Connectivity, Monitoring the Network, Troubleshooting the Network

Unit-5

Introduction to Network Forensics, Common Protocols, SSL, TLS, Network Devices, Log Manipulation, Browsers as Digital Evidence, Capturing Traffic Flow with Common Tools, Wireshark GUI and CLI, Filters of Wireshark, File Extraction with Network Miner, TCP Dump, CAP Files Manipulation, Packet Structure and Analysis, Internet Traffic analysis, basics of e-mail, different protocols of e-mail, e-mail analysis, Introduction to IDS, IPS, SIEM, SOC, endpoint security, honeypot, introduction to IoT devices and forensics

Practical's

1. Study of different types of Network cables and Practically implement the cross-wired cable and straight-through cable using a crimping tool.
2. Connect the computers in the Local Area Network.
3. Performing an Initial Switch and Router Configuration.
4. Implementing an IP Addressing Scheme, Interpreting Ping and Traceroute Output.
5. a. Configuring Ethernet and Serial Interfaces.
   b. Configuring a Default Route.
   c. Configuring Static and Default Routes.
6. Configuring RIP.
7. Configuring EIGRP and OSPF.
8. Configuring iBGP.
9. Study TCPDump and Wireshark.
10. Pcap Analysis Case Studies.

Reference Books:

1. Anton Chauvakin, Kevin Schmidt, Christ Phillips, Logging and Log Management: TheAuthorative Guide to understanding the Concepts Surrounding Logging and log Management,Syngress, 2012
2. R. David, Miller, Shon Harris, Alan Harper, Stephen VanDyke, and Chris Blask, SecurityInformation and Event Management (SIEM) Implementation, Network Pro Library, 2010
3. Tyler Wrightson, Wireless Network Security A Beginners Guide, 2012
4. Network Forensics: Tracking Hackers through Cyberspace 1st Edition, by Sherri Davidoff,Jonathan Ham , Pearson
5. Network Forensics by Ric Messier, Wiley
6. Wireshark 101: Essential Skills for Network Analysis by Laura Chappell, LauraChappellUniversity

Chairperson	Chairperson	Controller of Examinations	Registrar
Board of Studies – Forensic Science Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Faculty of Studies - Science Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore	Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

M.Sc. Cyber Forensics - II SEMESTER
Batch 2025 - 2027

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
MSCFN203		Cyber Security Management and Incident Response	60	20	20	30	20	3	0	2	4

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P – Practical; C - Credit; Th. - Theory
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Learning objective: The student will have ability:

1. Plan and prepare for all stages of an investigation - detection, initial response and management interaction.
2. Investigate web server attacks, DNS attacks and router attacks and alsocanlearn the importance of evidence handling and storage.
3. Monitor network traffic and detect illicit servers and covert channels

Learning Outcome

1. Obtain basic knowledge on dealing with system security related incidents.
2. Increase knowledge on potential defenses and counter measures against common threat vectors/vulnerabilities.
3. Gain experience using tools and common processes in performing analysis of compromised systems and dynamic malware analysis.
4. Obtain current knowledge of events and tools/support kits in the subject area.

Unit-1 Introduction to Incident Response

What Is a Computer Security Incident, What Are the Goals of Incident Response, Who Is Involved in the Incident Response Process, Incident Response Methodology, Pre-Incident Preparation, Detection of Incidents, Initial Response, Investigate the Incident.
Cyber Security Management and Incident Response

Unit II - Initial Response and Forensic Duplication

Initial Response & Volatile Data Collection from Windows system - Initial Response &Volatile Data Collection from Unix system - Forensic Duplication: Forensic Duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive

Unit III - Storage and Evidence Handling

File Systems: FAT, NTFS - Forensic Analysis of File Systems - Storage Fundamentals: Storage Layer, Hard Drives Evidence Handling: Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure

Unit IV - Network Forensics

Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud

Unit V - Systems Investigation and Ethical Issues

Data Analysis Techniques - Investigating Live Systems (Windows &Unix) - Investigating Hacker Tools - Ethical Issues – Cybercrime

References

1. Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”, TataMcGrawHill,2006.
2. Peter Stephenson, "Investigating Computer Crime: A Handbook for Corporate Investigations", Sept 1999
3. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools andTechnology", Academic Press, 1st Edition, 2001
4. Skoudis. E., Perlman. R. Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall Professional Technical Reference. 2001.
5. Norbert Zaenglein, "Disk Detective: Secret You Must Know to Recover Information from a Computer", Paladin Press, 2000
6. Bill Nelson, Amelia Philips and Christopher Steuart, “Guide to computer forensics and investigations”, course technology,4thedition, ISBN: 1-435-4 9883-6
7. Chris Prosise & Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill Publication
8. Electronic Crime Scene Investigation A guide for First Responders, US Dept. Justice.

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

M.Sc. Cyber Forensics - II SEMESTER
Batch 2025 - 2027

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
MSCFN2041	Elective	Forensic Accounting	60	20	20	0	0	4	0	0	4

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P – Practical; C - Credit; Th. - Theory
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Learning objective: The student will have the ability:

1. **To understand the basics of forensic accounting and their concepts**
2. Risk-based audit planning and audit project management techniques
3. Fundamentals of business processes
4. Frauds in Insurance

Learning Outcome: Upon completion of the subject, students will be able to:

1. **To understand basics of forensic accounting its concepts**
2. Risk-based audit planning and audit project management techniques
3. Fundamentals of business processes
4. Frauds in Insurance

Unit-1

Forensic Accounting – Introduction, Principles of accounting – Basic concepts of forensic accounting, Understanding Frauds – Fraud examination methodology – Introduction to Financial Statements, Financial Statement Frauds, IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards. Risk assessment concepts and tools & techniques used in planning, examination, reporting and follow-up

Unit-2

Fundamentals of business processes: Purchasing, Payroll, Accounts payable, accounts receivable, Role of IS in these processes. Control Principles related to controls in information systems

Unit-3

Risk-based audit planning and audit project management techniques, including follow-up. Applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits. Evidence Collection Techniques: Observation, Inquiry, Inspection, Interview, Data Analysis, Forensic Investigation Techniques, Computer-assisted audit

techniques [CAATs] used to gather, protect and preserve audit evidence

Unit-4

Frauds in Insurance, Frauds in Health Care, Frauds in Banking, Frauds in Tax, Frauds in StockMarket / Securities, Consumer Frauds, Frauds in Public Sector, Frauds in Contract andprocurement, case study of various frauds

Unit-5

Sampling methodologies and substantive/data analytical procedures. Reporting andCommunication techniques: Facilitation, Negotiation, Conflict Resolution, Audit reportstructure, issue writing, management summary, result verification. Audit Quality assurance (QA)systems and frameworks. Various types of audits: Internal, External, Financial, and methods forassessing and placing reliance on the work of other auditors and control entities, Frauds onintellectual property rights and implications, money laundering

Suggested Readings

1. Fraud auditing and forensic accounting, Jack Bologna, Wiley Publication
2. Forensic Accounting for Dummies by FrimetteKass-Shraibman and Vijay S. Sampath, Wiley Publication
3. Essentials of Forensic Accounting (AIPCA), Wiley , ISBN: 9781526505866
4. A Guide To Forensic Accounting Investigation, Thomas W. Golden, Steven L. Skalak, And Mona M. Clayton (Willey)
5. Forensic Accounting and Fraud Investigation by Stephen Pedneault, Frank Rudewicz, Michael Sheetz and Howard Silverstone (CPE Edition)
6. The Forensic Accountant's HandBook, Compiled by Chetan Dalal, Mahesh Bhatki, JatinJhaveri, Rajan Gupte and Govindsingh Purohit
7. Information Technology Security and Risk Management by Jill Slay and Andy Koronios (Willey)

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

M.Sc. Cyber Forensics - II SEMESTER
Batch 2024 - 2026

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			END SEM University Exam	Two Term Exam	Teachers Assessment*	END SEM University Exam	Teachers Assessment*				
MSCFN2042	Elective	Data Privacy	60	20	20	0	0	4	0	0	4

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P – Practical; C - Credit; Th. - Theory
*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Learning objective: The student will have ability:

1. Data Privacy Management and Data Privacy Management controls
2. Privacy Program Governance and Compliance and Legal Framework
3. Privacy in Cloud Computing and IOTPrivacy in Cloud

Learning Outcome: Upon completion of the subject, students will be able to:

1. Data Protection & Privacy Terminologies
2. Data protection principles and Safeguards Data protection principles

Unit 1: Introduction to Privacy

Data Protection & Privacy Terminologies - Data Protection Principles and Approaches to Privacy - Code for protection of Personal Information - Information Life Cycle -Data Security Threats and Mitigation - Data Storage Security Issues in Cloud Computing

Unit 2: Data Protection Principles

Data protection principles and Safeguards Data protection principles - Subject access request Damage or distress - Preventing direct marketing Automated decision taking - Correcting inaccurate personal data - Compensation, Exemptions& Complaints - Big data - CCTV & Data sharing - Online & apps Privacy by design - Guidance Note on Protecting the confidentiality of Personal Data –Safeguarding Personal Information - Using Personal Information on Websites and with Other Internet-related Technologies- Privacy considerations for sensitive online information, including policies and notices, access, security, authentication, identification, and data collection. –Data Privacy in online data collection, email, searches, online marketing and advertising, social media, online assurance, cloud computing and mobile devices.

Unit 3: Data Privacy Management

Data Privacy Management controls & Plan - Data Privacy Management Reference Model – ISTPA - Data Protection in the context of Police and Criminal Justice - Cross Border data transfer - Do not Track Privacy Policy - Developing Privacy Management Tools -Information security practices for data privacy - Developing a privacy management plan -Rights of the Data Subject - Documenting the privacy baseline of the organization –Dataprocessors and third-party vendor assessments - Physical assessments; mergers, acquisitionsand divestures - Privacy threshold analysis; privacy impact assessments - Privacy Monitoringand Incident Management (MIM) - Auditing your privacy program; creating awareness of the organization's privacy program; Compliance monitoring; handling informationrequests; andhandling privacy incidents.

Unit 4: Privacy and Legal Framework

Privacy Program Governance and Compliance and Legal Framework Privacy Organization and Relationship (POR) - Privacy Policy and Processes (PPP) - Regulatory Compliance Intelligence (RCI) - Privacy legislations - applicability andinterpretation - Privacy Awareness and Training (PAT) – Legal Framework for Dataprotection, Security and Privacy Norms

Unit 5: Privacy in Cloud Computing

Privacy in cloud computing and IOTPrivacy in Cloud _ Introduction to Privacy in cloud computing - Cloud computing paradigmand privacy - Challenges to privacy in cloud computing - Privacy in IoT - IoT Governance -IoT Security & Privacy Issues - IoT Privacy challenges - IoT Privacy solutions.

Suggested Readings

1. Data Privacy (English, Hardcover, Venkataraman anNataraja) ISBN: 9781498721042, 9781498721042
2. Data Privacy: A runbook for engineers by Nishant Bhajaria ISBN-13:978-1617298998
3. Cyber Privacy: Who Has Your Data and Why You Should Care Hardcover – November 3, 2020by April Falcon Doss

Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Forensic Science

M.Sc. Cyber Forensics - II SEMESTER
Batch 2024 - 2026

COURSE CODE	CATEGORY	COURSE NAME	TEACHING & EVALUATION SCHEME								
			THEORY			PRACTICAL		L	T	P	CREDITS
			SEM Universit	Term	Teachers Assessme	SEM Universit	Teachers Assessme				
MSCFN205		Project-1	0	0	0	60	40	0	0	6	3

Legends: L - Lecture; T - Tutorial/Teacher Guided Student Activity; P – Practical; C - Credit; Th. - Theory

*Teacher Assessment shall be based following components: Quiz/Assignment/ Project/Participation in Class, given that no component shall exceed more than 10 marks

Every student will carry out project under supervision of supervisor (s) Internal/External. The topic shall be approved by a committee constituted by the head of the concerned Institute. Every student shall present two seminar talks, the first at the beginning of the project (Phase-1) to present the scope of the work and to finalize the topic, and towards the end of the seminar, presenting the work carried out by him/her in the semester.