Department of Cyber Forensics

Course Outcome

B.Sc. (Forensic Science) Semester I
Paper VI: Basics of Digital and Cyber Forensics

Objectives: This course covers

- Basics of Computer Science
- Data Representation and
- Basics of Operating System

Outcomes: After Completion of the course, students will know about.

- Evolution of Computers
- Components of Computer
- Types of Memory
- External Storage Devices
- Types of Software's
- Types of various number systems
- Interconversion between various number systems
- Logic Gates and their combinations
- Functions, features and types of Operating System

B.Sc. (Forensic Science) Semester II
Paper VI: Basics of Digital and Cyber Forensics

Objectives: This course covers

- Concept of Computer Networks
- File Systems
- Internet
- Cyber Crimes
- Digital Evidence

Outcomes: After Completion of the course, students will know about.

- Characteristics and structure of file systems – FAT12, FAT16, FAT32, NTFS, Ext2, Ext3 & HFS.
- Difference between various file systems
- Concept of Computer Networks
- Network Topologies
- Types of Computer Networks
- Networking Devices
- ISO OSI reference model
- TCP/IP model
- World Wide Web and concepts
- Electronic communication
- Network security
- Concept of cyber crime and types of cyber crimes
- Digital evidence and physical evidence
- Nature of digital evidence
- Precautions while dealing with digital evidence

B.Sc. (Forensic Science) Semester III
Paper VI: Advanced Digital and Cyber Forensics

Objectives: This course covers

- Cyber forensic investigation process
- Roles of cyber forensic expert
- Need of investigating cyber crimes
- Incident response process
- Cyber forensic tools and utilities

Outcomes: After Completion of the course, students will know about.

- Various steps involved in cyber forensic investigation process
- Qualities and skills required for cyber forensic expert
- Establishing a Basis or justification to investigate various cybercrimes.
- Incident response methodology
- Formation of Computer Security Incident Response Team
- Understand functionalities and uses of various cyber forensic tools and utilities

B.Sc. (Forensic Science) Semester IV
Paper VI: Advanced Digital and Cyber Forensics

Objectives: This course covers

- To learn Evidence collection and analysis process
- To understand internal architecture of the File system
- To learn various concealment techniques
- To understand the concept of biometrics

Outcomes: After Completion of the course, students will know about.

- The process of collecting volatile and non-volatile evidences by using various tools
- Various windows and Linux File System internal.
- Cryptography, steganography methods and tools
- Basic concepts, uses and types of Biometrics

B.Sc. (Forensic Science) Semester V
Paper VI: Applied Digital and Cyber Forensics

Objectives: This course covers

- Data and Evidence Recovery
- Cyber Forensic Investigation
- Security Issues

Outcomes: After Completion of the course, students will know about.

- Mobile Forensics
- Evidence Recovery tools and process from computer , internet , cell phone, etc.
- Chain of Custody
- Security technologies
- Digital signature
- Email investigation and recovery

- Password cracking
- Types of cyber attack and its preventive measures
- Ethics of computer security

B.Sc. (Forensic Science) Semester VI
Paper VI: Applied Digital and Cyber Forensics

Objectives: This course covers

- Electronic World
- Forensic Auditing
- Information Technology Act

Outcomes: After Completion of the course, students will know about.

- E-Governance, E-Commerce, E-Business, E-Banking
- Online Transaction
- EDI software
- Process of Forensic Auditing
- Investigation of Fraud, Fighting Fraud, Fraud Prevention, Fraud Detection, Recognizing the Symptoms of Fraud;
- IT Act 2000 and amendments
- Emerging trends in Information Technology law.

Department of Cyber Forensics

Course Outcome

M.Sc. (Forensic Science) Semester I

MFS-106: Paper VI Digital and CyberForensics

Objectives: This course covers

- Information Technology Act 2000 and Amendment Act 2008 along with cybercrimes mentioned in Acts, internet & web technologies,
- Information Security and Program Security
- Database Security and Network Security

Outcomes: After Completion of the course, students will know about.

- Indian Information Technology Act, 2000 and its Amendment Act, 2008
- Various internet and Web technologies such as HTML, PHP. MYSQL. CSS, etc.
- Investigation of Cybercrimes
- Security mechanisms such as encryption, decryption, and computer Security Concepts.
- Need of information system security and various concepts to protect information system.
- Program security, malicious code, and control against program threats.
- Basics of Database Management System and Structured Query Language.
- Database Security Concepts.
- Need of network security. Threats and countermeasures in network security.
- Intrusion Detection System: - its types and need.

M.Sc. (Forensic Science) Semester II

MFS-206: Paper XIVDigital and CyberForensics

Objectives: This course covers

- Cybercrime Investigation of different operating systems.
- Study of Open source tools for digital forensics and Registry Forensic
- Introduction to Biometrics

Outcomes: After Completion of the course, students will know about.

- Investigation procedure of Windows and Linus Systems.
- Use of open source tools for digital forensics.
- Structure of Windows Registry.
- Need and procedure of windows registry analysis.
- Concepts of Biometrics system.
- Various biometric traits.
- Concepts of Image Processing.

M.Sc. (Forensic Science) Semester III

MFS-302: Paper XVIII (Special I) Operating SystemandWeb Security

Objectives: This course covers

- Introduction to Operating System
- Functions of Operating System
- client server application and webapplications designing challenges.
- Secure Website Design.

Outcomes: After Completion of the course, students will know about.

- Basics and types of operating systems.

- Functions of operating system.
- Networking & network security concepts of operating systems
- Understanding vulnerabilities in traditional client server application and webapplications.
- Various attacks on Web Application and Client Server Applications
- Architecture and Design Issues for Web Applications
- Secure website designing techniques.

MFS-303: Paper XIX(Special II) Advanced ComputerNetwork and NetworkSecurity

Objectives: This course covers

- Study of Circuit Switched Networks
- Study of Advanced Networking Concepts
- Importance of network Security & Authentication
- Study of Network Architecture & Security

Outcomes: After Completion of the course, students will know about.

- Basics of circuit switched networks
- Network Models and various Protocols
- Need of network security and various attacks on networks.
- Authentication mechanism for network security.
- Internet and E-commerce security issues
- encapsulation of network services,
- allocation oftraffic control functions.
- Internal boundary systems
- Network hardening techniques.
- Management Issues of Wireless and Mobile Devices
- Mobile communication technologies.

M.Sc. (Forensic Science) Semester IV
Specialization IV: Cyber Security and Cyber Forensic
MFS-402 Paper XXI(Special Paper I) Mobile andCyber Forensics

Objectives: This course covers

- Learning Mobile Forensics
- Study of Live Forensics and Memory Image Forensics
- Study of Image Forensics
- Study of Network and Anti- computer Forensics

Outcomes: After Completion of the course, students will know about.

- Need of mobile device forensics
- Professional applications for mobile forensics
- Procedure for mobile forensics investigation
- Data acquisitions types
- Commercial and open source tools for mobile forensics
- The concept of Live forensics
- Advantages of live forensics over dead forensics
- Volatility framework and its plugins for live forensics

- Image forgery and its types
- Detection of forged images
- Network forensics procedures.
- Types of Anti-computer forensics
- Effectiveness of anti-forensics

MFS-403 Paper XXII(Special Paper II)Ethical Hacking andRecovery Forensic

Objectives: This course covers

- Hacking
- System Hacking and prevention
- Recovery Forensic
- Study of Win Hex Tools

Outcomes: After Completion of the course, students will know about.

- Basics of Ethical Hacking
- UnderstandingMalicious and hostile code
- Authentication and Authorization
- Computer security and analyse security breachingattacks, Risk analysis, risk assessment
- Concepts of DoS Attack, Session Hijacking, Web Server Hacking, Web Application Hacking, SQL Injection and Social Engineering and its prevention.
- Data Recovery from external storage devices.
- Study of Winhex forensic applications.

MFS-404 PaperXXIII(Special Paper III)Digital Imageprocessing

Objectives: This course covers

- Digital Image Processing
- Pattern Recognition
- Steganography & Steganalysis
- Watermarking

Outcomes: After Completion of the course, students will know about.

- Fundamental Steps in Image Processing
- Image quality enhancement
- Image compression methods
- Introduction to pattern recognition
- Bayesian decision theory
- Information hiding using Steganography, watermarking.
- Importance of steganography and watermarking
- Steganographic methods
- Steganalysis algorithms
- Models of watermarking
- Watermark security

MFS-405 PaperXXIV (Special Paper IV)Biometrics

Objectives: This course covers

- Unimodal and Multimodal Biometrics
- Automated Fingerprint, Face, speaker Recognition techniques.

Outcomes: After Completion of the course, students will know about.

- Introduction to biometrics
- Biometric technologies
- Multi-Modal Biometric Systems
- Concepts of fingerprint recognition
- Practical applications of fingerprint recognition
- Types of scanners for fingerprint recognition
- Basics of speaker recognition.
- Algorithms for training, recognition and adaptation to speakerand transmission channel
- analysis and decision techniques for speaker recognition
- Introduction to Face Recognition
- Working of Face recognition
- Verification vs. Identification using Face recognition
- Facial Recognition Technologies, Facial RecognitionApplications.