

M.Sc. (Digital Forensic and Information Security)

Programme Outcomes (POs)

- PO1:** Demonstrate the fundamental knowledge & basic principles in respective field of sciences.
- PO2:** Design and conduct experiments and simulations, as well as critically analyzing the results and interpret them.
- PO3:** Develop a research culture and implementation of the policies to tackle the burning issues at global level and enhance the scientific temper.
- PO4:** Inculcate logical thinking to address a problem and become result oriented with a positive attitude.
- PO5:** Analyze, and apply appropriate tools & techniques for decision making and problem solving.
- PO6:** Develop personal strengths like emphasizing perseverance, building negotiation skills and communication skills as a team member or team leader.
- PO7:** Understand professional and ethical responsibility while carrying out research and design activities.
- PO8:** Recognize the need for, and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change.

Programme Specific Outcomes (PSOs)

- PSO 01:** Recognize diverse aspects of Forensic science, like crime scene management, cyber and digital forensics, questioned document examination, Forensic Chemical, biological & physical sciences evidence collection, preservation and evaluation.
- PSO 02:** Interpret the functioning of the justice system, police organizations, forensic scientists, techniques involved in collection, preservation and evaluation of evidences; various aspects of the allied sciences that assist in forensic investigation protocols, and the step by step development of the investigative procedures.
- PSO 03:** Appraise the concepts learned in the classroom and make conclusions based on scientific thinking, ability to identify and differentiate between methods/protocols, instrumentation and evaluative procedures required in the investigative process that is required for crime solving and also document the same as per norms.
- PSO 04:** Work collaboratively in the laboratory to acquire and analyze data and to solve problems scientifically and systematically. Develop professional and ethical responsibility.

Course Outcomes (COs)

2022-2023 Batch

Semester	Course Code	Course Name	Course Outcomes (COs)
I	22MSDFIS1H01	Introduction to Forensic Science	<p>CO1: Recall history and development of Forensic Science</p> <p>CO2:List organizational setup of Forensic Science Lab</p> <p>CO3:Describe various national and international agencies related to Forensics and their role</p> <p>CO4: Discuss various disciplines of Forensic Science</p> <p>CO5: Explain Criminal Justice System and its role</p>
	22MSDFIS1H03	Cyber crime and Cyber law	<p>CO1: Recall the concept and elements of crime.</p> <p>CO2: Classify the different modes and methods of cybercrimes</p> <p>CO3: Illustrate the different preventive measures against cyber crimes</p> <p>CO3: Illustrate the different preventive measures against cyber crimes</p> <p>CO4: Interpret diverse legal provisions pertaining to cyber and its correlation with substantive laws</p> <p>CO5: Assess the functioning of national and international conventions and provisions in relation to cyber space</p>

	<p>22MSDFIS1S01</p>	<p>Multimedia Forensics</p>	<p>CO1: Describe the basic concepts of Audio and video analysis including the elements of video, image and audio</p> <p>CO2: Describe noise, its characteristics, human vocal tract structures</p> <p>CO3: Demonstrate Image enhancement and restoration, audio enhancement, Facial image restoration.</p> <p>CO4: Examine audio and video evidence found at crime scene, audio recording for speaker recognition.</p> <p>CO5: Prove the integrity of image evidence, authenticity of audio and video evidence.</p>
	<p>22MSDFIS1S02</p>	<p>Criminal Justice system and criminal law</p>	<p>CO1: Outline the fundamentals of Criminal Justice System along with the basic terminologies in Criminal Justice System</p> <p>CO2: Interpret the structure, role, duties and functioning of the Judiciary in addition with the reforms and the provisions in Penal, Procedural and Evidentiary laws to keep students aware of the statutes.</p> <p>CO3: Dissect the nature of cyber offenses under Information Technology Act, 2000 along with the importance of digital evidence</p> <p>CO4: Assess the structural reforms within the Criminal Justice System and its implications.</p>
	<p>22MSDFIS1H01L</p>	<p>Introduction to Forensic Science Lab</p>	<p>CO1: Define and distinguish between different types of crime scenes, specifically focusing on the unique characteristics and challenges of indoor and outdoor crime scenes.</p>

			<p>CO2:Demonstrate collection, packaging, sealing, and labeling of various physical and biological evidence</p> <p>CO3: Examine competency in the use of various methods for developing latent fingerprints, such as dusting, fuming, and chemical development, and be able to select the most effective technique based on the circumstances.</p> <p>CO4:Analyze and compare bullets and cartridge casings to determine if they were fired from the same firearm.</p> <p>CO5:Appraise the ability to use various methods and technologies to identify counterfeit currency, such as watermarks, security threads, color-shifting ink, and microprinting.</p>
	<p>22MSDFIS1S01L</p>	<p>Multimedia Forensics Lab</p>	<p>CO1: Describe the measures taken for recording of speech sample and identify its segregation and transcription techniques</p> <p>CO2: Employ various enhancement and spectrographic techniques on the speech sample and interpret the results</p> <p>CO3: Differentiate all the modes of disguise in an audio recording or a speech sample.</p> <p>CO4: Assess the CCTV footage and the extracted audio from the video</p>

<p align="center">II</p>	<p>22MSDFIS2H02</p>	<p>Mobile and Network Forensics</p>	<p>CO1: Identify various basic concepts of mobile forensics like SIM and its structure, operating systems like android, blackberry etc</p> <p>CO2: Distinguish and discriminate between GSM and CDMA, types of networks.</p> <p>CO3: Interpret various features of different operating systems, networks and firewalls</p> <p>CO4: Examination of different types of networks for any intrusion.</p> <p>CO5: Illustrate various features supporting intrusion and crime committed.</p>
	<p>22MSDFIS2H03</p>	<p>Email and Cloud Forensics</p>	<p>CO1: Describe the working of email and various parts involved.</p> <p>CO2: Discuss the Functioning of the cloud architecture and their types.</p> <p>CO3: Illustrate the concept of cloud forensic and the importance of cloud investigation.</p> <p>.CO4: Articulate the different features that can be used as digital evidence.</p>
	<p>22MSDFIS2H04</p>	<p>Incident Handling and Response</p>	<p>CO1: Understand the fundamental concepts of Information Security, including the types of Information Security Governance, Risk & Compliance (GRC), and their scope and objectives.</p>

			<p>CO2:Analyze and apply various IT Governance Metrics & Frameworks such as BASEL, OECD, ITIL, ISO/IEC 27001, and COBIT to effectively manage Information Security.</p> <p>CO3: Identify and evaluate Threat Surfaces and implement preventive measures, Incident Response strategies, and Post-Incident Compliance Reporting procedures</p> <p>CO4: Utilize tools and techniques to recognize and mitigate vulnerabilities such as Backdoors, Denial of Service (DOS) attacks, Network Spoofing, Tampering, and Exploits in both Windows and Linux systems.</p> <p>CO5: Demonstrate knowledge and proficiency in legal aspects related to Information Security, including Chain of Custody, Log Aggregators, and Compliance with regulations such as HIPAA, SOC, GDPR, and Process-Breach Management.</p>
	<p>22MSDFIS2S01</p>	<p>Fraud Examination</p>	<p>CO1: Define the types of fraud and the impact of fraud on organizations and society.</p> <p>CO2: Outline an understanding of the common fraud schemes, the methods used by fraudsters, and the red flags that signal fraudulent activity.</p> <p>CO3: Employ design and implement effective fraud prevention and detection programs, including internal controls, monitoring systems, and audits.</p>

			<p>CO4: Examine the legal aspects of fraud examination, including laws, regulations, and ethical considerations.</p> <p>CO5: Appraise skills in conducting fraud investigations, including interviewing techniques, document analysis, and evidence collection.</p>
	22MSDFIS2S02	Crime Mapping	<p>CO1: Recall the principles, methods, and techniques used in crime mapping, including data collection, data analysis, visualization, and interpretation.</p> <p>CO2: Outline large amounts of data, identify patterns and trends, and draw conclusions.</p> <p>CO3:Employ spatial data and mapping tools to enhance students' spatial awareness and their ability to analyze spatial relationships.</p> <p>CO4: Examine wide range of applications in law enforcement, public safety, and criminal justice</p> <p>CO5: Appraise hands-on experience using mapping software, collecting and analyzing data, and creating visualizations.</p>
	22MSDFIS2H01L	Fundamentals of Information security Lab	<p>CO1:Describe Threat Surfaces and implement preventive measures, Incident Response strategies, and Post-Incident Compliance Reporting procedures</p>

			<p>CO2: Explain the fundamental concepts of Information Security, including the types of Information Security Governance, Risk & Compliance (GRC), and their scope and objectives.</p> <p>CO3: Apply various IT Governance Metrics & Frameworks such as BASEL, OECD, ITIL, ISO/IEC 27001, and COBIT to effectively manage Information Security.</p> <p>CO4: Distinguish and utilize tools and techniques to recognize and mitigate vulnerabilities such as Backdoors, Denial of Service (DOS) attacks, Network Spoofing, Tampering, and Exploits in both Windows and Linux systems.</p> <p>CO5: Summarize knowledge and proficiency in legal aspects related to Information Security, including Chain of Custody, Log Aggregators, and Compliance with regulations such as HIPAA, SOC, GDPR, and Process-Breach Management.</p>
	<p>22MSDFIS2H02L</p>	<p>Mobile and Network Forensics Lab</p>	<p>CO1: Understand the structure of SIM modules</p> <p>CO2: Apply different tools like Wireshark, MobileEdit for acquisition and network monitoring.</p> <p>CO3: Analyze the importance and application of different network commands.</p> <p>CO4: Critically evaluate firewall logs.</p> <p>CO5: Create a report after the completion of analysis.</p>

	22MSDFIS2H03L	Email and Cloud Forensics Lab	<p>CO1: Demonstrate the email data recovery from internet cache using different email platforms</p> <p>CO2: Describe email header extraction & its investigation.</p> <p>CO3: Define the Virtual Machine creation in Operating System</p> <p>CO4: Articulate the technique of imaging and Analysis in VMware.</p>
--	----------------------	-------------------------------	---