

FACULTY OF COMPUTER APPLICATIONS

Programme	Master of Computer Applications					Branch/Spec.	Computer Application		
Semester	II					Version	1.0.0.0		
Effective from Academic Year				2026-27		Effective for the batch Admitted in		July 2026	
Subject Code	P12E6DFI		Subject Name			Digital Forensics & Incident Response			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	2	0	2	0	4	Theory	40	60	100
Hours	2	0	4	0	6	Practical	20	30	50
Objective:									
To provide knowledge of digital evidence, forensic investigation, evidence preservation and acquisition and enable students to perform incident response, and prepare legally and technically defensible reports.									
Pre-requisites:									
Require the basic knowledge of Students should have basic knowledge of operating systems, computer networks, file systems, storage devices, Linux/Windows environments, and cybersecurity fundamentals. Familiarity with system logs, networking, virtualization, and basic system administration is desirable.									
Course Outcomes:									
Name of CO		Description							
CO1		Explain legal, ethical, procedural, and evidentiary requirements of digital-forensic investigation, including chain of custody.							
CO2		Perform forensically sound acquisition, imaging, preservation, hashing, and handling of digital evidence.							
CO3		Analyze disk, file-system, memory, network, malware, mobile, cloud, email, and application artifacts using appropriate forensic techniques.							
CO4		Apply incident-response frameworks to investigate security incidents and prepare structured forensic investigation reports.							
Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	
CO1	2	3	1	2	1	-	3	2	
CO2	2	3	3	3	1	1	3	2	
CO3	3	3	3	3	2	1	3	3	
CO4	3	3	3	3	2	1	3	3	

Content:		
Unit	SECTION – I	Hrs
1	Foundations of Digital Forensics, Cyber Law and Evidence Management Introduction to digital forensics, history, scope and applications, forensic science principles applied to digital evidence, Locard's Principle of Exchange, cybercrime investigation, legal and ethical considerations, Information Technology Act 2000 and amendments, Indian Evidence Act Section 65B and admissibility considerations, search and seizure procedures, types of digital evidence, order of volatility, live and dead evidence, forensic investigation process including identification, preservation, collection, examination, analysis and presentation, chain of custody, evidence documentation, evidence bags, hashing using MD5 and SHA-256, write blockers, forensic imaging principles, ISO/IEC 27037, NIST SP 800-86, forensic laboratory setup, forensic readiness, first-responder procedures and preservation of evidence.	08
2	Disk, File-System and Host Forensics Storage-media fundamentals, HDD and SSD architecture, MBR and GPT partitioning, FAT32, NTFS, ext4 and APFS, forensic acquisition, bit-stream imaging, write blocking, raw/dd, E01 and AFF image formats, FTK Imager, dd and Guymager, NTFS forensic artifacts including MFT, \$LogFile, USN Journal, alternate data streams and MACB timestamps, deleted-file recovery, unallocated-space analysis, file carving, Scalpel, Foremost and PhotoRec, Windows Registry forensics, Registry hives, recent documents, USB history, Run keys and Shellbags, Linux and macOS forensic artifacts, syslog, auth.log, application logs and host-based event reconstruction	07
SECTION – II		
3	Memory, Network, Malware, Mobile and Cloud Forensics Volatile-memory forensics, RAM acquisition, WinPMem, DumpIt and LiME concepts, memory analysis using Volatility, process and DLL analysis, handles and network connections, network-forensics fundamentals, packet capture, NetFlow, full-packet versus metadata capture, Wireshark and Zeek, C2 traffic, DNS tunneling and data-exfiltration patterns, Windows Event Logs, SIEM-based log correlation, forensic timeline construction, malware-forensics fundamentals, static analysis using hashing, strings and PE headers, basic dynamic analysis in sandbox environments, Android and iOS file-system overview, logical, physical and file-system acquisition concepts, mobile artifacts including calls, messages, application data and geolocation, cloud-forensics challenges including multi-tenancy and jurisdiction, AWS CloudTrail and Azure Activity Log as evidence sources, email-header analysis, messaging-application artifacts and metadata extraction.	08
4	Anti-Forensics, Timeline Analysis and Incident Response Anti-forensic techniques including data wiping, timestomping, steganography and encryption,	07

	detection approaches, timeline analysis, super-timeline construction using Plaso/log2timeline concepts, incident-response fundamentals, NIST SP 800-61, SANS PICERL model, preparation, identification, containment, eradication, recovery and lessons learned, SOC workflows, incident detection and triage, alert prioritization, ransomware, data breach, insider threat and business-email-compromise response, recovery planning, post-incident review, root-cause analysis, Indicators of Compromise (IOC), Indicators of Attack (IOA), threat-intelligence integration, MITRE ATT&CK mapping, forensic report writing, expert testimony fundamentals, ransomware and data-breach case studies, and complete incident-response investigation.	
Practical Content:		
List of programs specified by the subject teacher based on above mentioned topics		
Text/Reference Books:		
1	Nihad A. Hassan, Digital Forensics Basics: A Practical Guide Using Windows OS, Apress.	
2	Leighton R. Johnson III, Computer Incident Response and Forensics Team Management, Syngress.	
3	Brian Carrier, File System Forensic Analysis, Addison-Wesley.	
Web References / MOOC / Certification Course		
1		
2		
3		
Question Paper Scheme:		
	University Examination Duration: 3 Hours Note for Examiner: - (I) Questions 1 and 4 are compulsory with no options. (II) Internal options should be given in questions 2, 3, 5 and 6. SECTION – I Q.1 –8 Marks Q.2 –11 Marks Q.3 –11 Marks SECTION - II Q.4 –8 Marks Q.5 –11 Marks Q.6 –11 Marks	