MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING
(A Unit of Rajalaxmi Education Trust®, Mangalore)
Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE, New Delhi
Accredited by NAAC with A+ Grade & ISO 9001:2015 Certified Institution

Model Question Paper

Third Semester MCA Degree Examination

Digital Forensics

Time: 3 Hours **Max. Marks: 100**

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M: Marks, L: RBT (Revised Bloom's Taxonomy) level, C: Course outcomes.

		Module -1	M	L	C
Q1	a.	You are a digital forensic investigator tasked with preparing a case involving corporate fraud. Construct a plan detailing how you would prepare for the investigation while ensuring adherence to professional conduct.	10	L3	CO1
	b.	A private healthcare organization has reported that sensitive patient data has been leaked to an external source. As a digital forensic investigator, you are tasked with conducting an investigation to determine how the breach occurred, identify the perpetrator, and assess the extent of the damage. Identify and apply the steps required to conduct the investigation in this scenario, ensuring all evidence is preserved and the organization's operations are minimally disrupted.	10	L3	CO1
		OR			
Q2	a.	A multinational financial services company has reported unauthorized access to its email server. The breach involved several confidential communications being forwarded to an unknown external email address. The company suspects insider involvement and requests a detailed forensic investigation to identify the method of access, the perpetrator, and the extent of the data compromise. Design a digital forensics investigation plan for this case, outlining the steps, tools, and methodologies you would use to uncover the truth while maintaining evidence integrity.	10	L3	CO1
	b.	A technology startup suspects that a former employee deliberately formatted their company-issued laptop's hard disk to destroy evidence of intellectual property theft before leaving the organization. The startup has handed over the laptop for forensic analysis. Construct a plan detailing how you would use data recovery tools and workstations to recover the formatted data, identify potential evidence, and ensure the recovered information's integrity for use in legal proceedings.	10	L3	CO1
		Module- 2			
Q3	a.	A financial institution has reported unusual activity involving the unauthorized transfer of sensitive financial records. They suspect an insider is responsible and have provided a RAID storage device from the suspected employee's workstation for analysis. Choose the best acquisition method to handle the RAID device, ensuring all data is preserved without altering its integrity, and justify your choice of tools and techniques in this situation.	10	L3	CO2
	b.	A global e-commerce company has reported unauthorized access to its customer database hosted on a remote cloud server. As a digital forensic investigator, you are tasked with acquiring and validating the digital evidence from the remote server to identify the breach's origin and assess the extent of the compromise. Apply the steps required to validate the digital evidence acquisition process, ensuring that the integrity of the evidence is maintained and that it is admissible in legal proceedings.	10	L3	CO2
		OR			

Q4	a.	A multinational corporation suspects that a coordinated cyberattack has compromised its internal network, with sensitive files distributed across multiple devices, including servers, employee workstations, and cloud storage systems. As a digital forensic investigator, how would you apply forensic tools to systematically gather and preserve data from these devices, ensuring the integrity of the evidence and maintaining a detailed chain of custody for legal admissibility.	10	L3	CO2
	b.	A retail company's payment processing system has been compromised by malware, potentially leading to the exfiltration of sensitive customer payment data. As a digital forensic investigator, construct a detailed model outlining the method to perform data acquisition on the compromised system. Include the steps, tools, and techniques required to ensure the integrity of the evidence, minimize system disruption, and avoid further compromise during the process.	10	L3	CO2
Module - 3					
Q5	a.	During a corporate cybersecurity breach involving unauthorized access to sensitive financial data, identify and apply the methods to collect digital evidence while ensuring compliance with private-sector regulations and privacy laws.	10	L3	CO3
	b.	A mid-sized company has fallen victim to a ransomware attack that has locked critical business files. Construct the process of securing and documenting the digital crime scene, detailing the steps required to preserve evidence while minimizing disruption to the company's operations.	10	L3	CO3
OR					
Q6	a.	A forensic team has seized a suspect's laptop in connection with intellectual property theft. Apply hashing techniques to verify the integrity of the evidence collected, and provide examples of hashing algorithms and their application in this context.	10	L3	CO3
	b.	In a cyberstalking case, law enforcement requests your expertise to plan a search and seizure operation at the suspect's residence. Develop a detailed plan for the operation, ensuring the proper handling and documentation of digital evidence in line with legal and ethical requirements.	10	L3	CO3
Module - 4					
Q7	a.	A suspect is accused of leaking sensitive information through email. Select the tools you would use to investigate the email and justify your choice based on their effectiveness in handling email-related digital forensics.	10	L3	CO4
	b.	A social media influencer reports receiving cyber harassment through anonymous messages. Apply digital forensic methods to analyze the suspect's social media accounts and identify potential evidence.	10	L3	CO4
OR					
Q8	a.	Encrypted files are discovered on a suspect's laptop during an investigation. Construct the process of testing and validating forensic software tools to decrypt and analyze the files while maintaining the integrity of the evidence.	10	L3	CO4
	b.	A server is suspected of unauthorized cryptocurrency mining within a company's network. Evaluate the use of hardware forensic tools to analyze the server, ensuring that relevant evidence is collected and preserved for further investigation.	10	L3	CO4
Module - 5					
Q9	a.	You are tasked with analyzing the logs from a virtual machine suspected of being used for illegal activities. Utilize the principles of virtual machine forensics to investigate the case, ensuring evidence integrity and detailed reporting.	10	L3	CO5
	b.	A suspect has allegedly used steganography to hide sensitive data within image files. Construct a detailed approach to validate and analyze the hidden information, specifying the tools and techniques required to uncover the concealed data.	10	L3	CO5
OR					

Q10	a.	A compromised web server has been identified in a large e-commerce platform, and live acquisition of data is required without affecting its operations. Construct a method to perform the live acquisition while minimizing disruption and ensuring the integrity of the collected data.	10	L3	CO5
	b.	A corporate intranet was breached, and unauthorized access to sensitive documents occurred. Apply network forensic techniques to investigate the case, focusing on identifying the attacker and the methods used in this intrusion.	10	L3	CO5

*****