24MCPE652

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 appointed as a digital forensic consultant for a manufacturing firm facing allegations of internal data manipulation. Apply a pre-investigation strategy covering authorization, scope definition, risk assessment, and professional ethics.	10	L3	CO1
	b.	A university reports unauthorized access to its examination database resulting in altered student grades. As a forensic investigator, apply the digital investigation process to identify the breach source while ensuring academic operations are not disrupted.	10	L3	CO1
		OR			
Q2	a.	A telecom company suspects misuse of official credentials to access confidential call records. Design a digital forensic investigation plan, specifying evidence sources, tools, and documentation methods to ensure evidence integrity.	10	L3	CO1
	b.	A corporate laptop suspected of data destruction using secure wipe utilities is submitted for analysis. Construct a recovery and examination plan to identify residual evidence and validate findings for court presentation.	10	L3	CO1
		Module- 2			
Q3	a.	An IT firm provides a NAS device suspected of storing illegally accessed client data. Choose and justify an appropriate acquisition method, ensuring data completeness and forensic soundness.	10	L3	CO2
	b.	A government portal hosted on a remote server experienced unauthorized logins. Apply evidence acquisition and validation steps suitable for remote systems while maintaining admissibility.	10	L3	CO2
		OR			
Q4	a.	A cyberattack affects multiple endpoints including desktops, mobile devices, and cloud backups. Apply forensic data collection techniques across heterogeneous systems while maintaining a chain of custody.	10	L3	CO2
	b.	A compromised ATM system is suspected of malware-based skimming. Construct a forensic acquisition model minimizing service downtime and preventing further contamination.	10	L3	CO2
		Module - 3			
Q5	a.	A private organization is under investigation for violating data protection regulations after a breach. Identify and apply evidence collection methods compliant with legal and privacy frameworks.	10	L3	CO3
	b.	An organization hit by a ransomware incident seeks forensic assistance. Construct a procedure to secure and document the digital crime scene without disrupting business continuity.	10	L3	CO3
		OR			

Q6	a.	Digital evidence seized from a suspect’s external drive must be verified. Apply hashing techniques and explain how hash values ensure evidence integrity.	10	L3	CO3
	b.	Law enforcement plans a raid in a cyber fraud case involving multiple digital devices. Develop a legally compliant search and seizure plan ensuring proper documentation and handling of evidence.	10	L3	CO3
Module - 4					
Q7	a.	An organization suspects sensitive data leakage via corporate email accounts. Select suitable email forensic tools and justify their effectiveness in evidence extraction.	10	L3	CO4
	b.	A public figure receives threatening messages through social networking platforms. Apply social media forensic techniques to identify digital traces and potential suspects.	10	L3	CO4
OR					
Q8	a.	Password-protected archives are recovered during a forensic examination. Construct a tool validation and analysis process to access the data while preserving integrity.	10	L3	CO4
	b.	A data center server is suspected of running unauthorized cryptocurrency mining software. Build the hardware forensic approaches to collect volatile and non-volatile evidences.	10	L3	CO4
Module - 5					
Q9	a.	A cloud-based virtual machine is suspected of hosting illegal activities. Utilize virtual machine forensic principles to analyze logs and snapshots with proper reporting.	10	L3	CO5
	b.	An image repository is suspected of containing hidden confidential information. Construct a forensic approach to detect and extract steganographic content.	10	L3	CO5
OR					
Q10	a.	A live database server must be examined after a security breach. Develop a live acquisition methodology ensuring minimal service interruption and data integrity.	10	L3	CO5
	b.	A corporate LAN intrusion resulted in unauthorized file transfers. Apply network forensic techniques to trace attacker behavior and intrusion methods.	10	L3	CO5

*****