23ICOE321

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

Sixth Semester BE Degree Examination

Digital Forensics

Time: 3 Hours (180 Minutes) **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.	Trace the historical evolution of cyber forensics and explain the need for digital forensics in modern investigations.	10	L2	CO1
	b.	Explain the Digital Forensics Life Cycle with a neat diagram.	10	L2	CO1
		OR			
Q2	a.	Define digital evidence and explain its characteristics and types.	10	L2	CO1
	b.	Discuss the chain of custody and explain its importance in legal proceedings.	10	L2	CO1
		Module- 2			
Q3	a.	Explain the steps involved in preparing a computer investigation for a corporate environment.	10	L2	CO2
	b.	Describe the systematic approach to a digital investigation including assessing and planning the case.	10	L2	CO2
		OR			
Q4	a.	Describe the technical procedures required to investigate an internet abuse case within an organization's private network.	10	L2	CO2
	b.	Discuss the role of interviews and interrogations in high-tech crime investigations.	10	L2	CO2
		Module - 3			
Q5	a.	Explain various storage formats of digital evidence: Raw, Proprietary, and Advanced Forensic Format.	10	L2	CO3
	b.	Describe the role of forensic acquisition tools in digital investigations. Explain the working of any two commonly used acquisition tools.	10	L2	CO3
		OR			
Q6	a.	Explain the process of bit-stream image acquisition and its importance.	10	L2	CO3
	b.	Describe the procedure for performing RAID data acquisitions. What challenges are faced during RAID acquisitions and how are they addressed?	10	L2	CO3
		Module - 4			
Q7	a.	Explain the rules of evidence and their relevance in digital forensics.	10	L2	CO4
	b.	Describe the steps involved in processing a computer crime scene.	10	L2	CO4
		OR			
Q8	a.	Explain the procedures for seizing and storing digital evidence at an incident scene.	10	L2	CO4
	b.	Discuss the role of digital hashing in validating and preserving digital evidence.	10	L2	CO4
		Module - 5			
Q9	a.	Explain mobile phone forensics and Smartphone forensics, highlighting major challenges.	10	L2	CO5

	b.	Discuss the challenges involved in the forensic analysis of digital images and still cameras. Explain how metadata is useful in such investigations.	10	L2	CO5
OR					
Q10	a.	Explain the techno-legal challenges associated with evidence from handheld devices.	10	L2	CO5
	b.	Explain the role of computer forensics in litigation. How does digital evidence from hand-held devices support legal proceedings?	10	L2	CO5

-*****-