Q. Code:430363

Reg. No.

M.E / M.TECH. DEGREE EXAMINATIONS, MAY 2024

Second Semester

CF22202 – DIGITAL FORENSICS AND DIGITAL INVESTIGATIONS

(Information Technology)

(Regulation 2022)

TIME: 3 HOURS **MAX. MARKS: 100**

COURSE OUTCOMES	STATEMENT	RBT LEVEL
CO 1	Relate the fundamentals of computer forensics, laws, report writing and tools in digital investigations	**4**
CO 2	Assess the investigative smart practices and applicability of concerned laws & investigative tools	**4**
CO 3	Inspect the acquired data, recover the deleted data and manage a case.	**3**
CO 4	Select the correct method to handle the digital evidence and acquire appropriate certification to build the career in digital forensics.	**3**
CO 5	Create a method for gathering, assessing and applying new and existing legislation specific to the practice of digital forensics.	**3**

PART- A (20 x 2 = 40 Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	How the evidence exchange helps the investigators establish connections between victims, offenders, and crime scenes?	**1**	**4**
2.	Why is authentication and maintaining a chain of custody crucial in digital forensics processes?	**1**	**4**
3.	Differentiate computer forensics, network, mobile, and malware forensics.	**1**	**4**
4.	Distinguish individual and class characteristics of digital evidence.	**1**	**4**
5.	Analyze the techniques involved in scaffolding for performing digital investigations.	**2**	**4**
6.	What is forensic examination? Examine the different levels of forensic examination in digital investigations.	**2**	**4**
7.	How evidence integrity is maintained while dealing with digital evidences?	**2**	**4**
8.	Identify the different representations of data used in digital investigations.	**2**	**4**
9.	Classify the role of computers in violent crime investigation.	**3**	**3**
10.	State the challenges of Intrusion Investigation.	**3**	**2**
11.	Interpret the need of reconstruction in the process of digital investigation.	**3**	**2**

12.	Illustrate the formation and evaluation of hypothesis in digital investigations.	**3**	**2**
13.	List any three forensics tools for used for automatic recovery of data in windows system.	**4**	**2**
14.	Identify the three levels of forensic examination in applying Forensic Science to Computers.	**4**	**3**
15.	Draw the conceptual representation of a directory and innode where the file types include regular, directory, symbolic link and socket.	**4**	**3**
16.	Recall the file systems used in different operating systems.	**4**	**2**
17.	Differentiate Internet legitimate users and criminal users.	**5**	**2**
18.	How the online databases are used as an investigation tool?	**5**	**2**
19.	Comment on the challenges of investigation in a Linux system.	**5**	**2**
20.	Mention the role and functionality of a sniffer tool.	**5**	**2**

PART- B (5 x 10 = 50 Marks)

			Marks	**CO**	**RBT LEVEL**
21. (a)		A digital investigator may be facing different challenges while doing investigations. Examine the methodologies to deal with all the challenges effectively.	**(10)**	**1**	**4**
		(OR)			
(b)		Infer how the language of computer crime investigation is involved in addressing criminal activities.	**(10)**	**1**	**4**
22. (a)		Examine the usage of different process models employed within the field of digital forensics.	**(10)**	**2**	**4**
		(OR)			
(b)		Inspect the terminologies and the principles in handling a digital crime scene. Explain with a real-time case study.	**(10)**	**2**	**4**
23. (a)		What are the strategies for effectively employing digital evidence in the investigation and substantiation of an alibi?	**(10)**	**3**	**3**
		(OR)			
(b)	**(i)**	Write the goals and analysis strategies that can be applied in malicious computer program investigation.	**(5)**	**3**	**3**
	(ii)	How the cyberstalkers operate? Identify the investigation steps in cyberstalking.	**(5)**	**3**	**3**
24. (a)		Explain the various techniques applied by digital investigators in dealing with password protection and encryption.	**(10)**	**4**	**3**
		(OR)			
(b)		Develop the process of dealing with digital evidence in UNIX system using various processing tools.	**(10)**	**4**	**3**

25. (a)	Why is it crucial to maintain online anonymity and implement self-protection measures in forensic science?	**(10)**	**5**	**3**
	(OR)			
(b)	Compile the various concepts of TCP/IP based digital investigation.	**(10)**	**5**	**3**

PART- C (1 x 10 = 10 Marks)

(Q.No.26 is compulsory)

		Marks	CO	RBT LEVEL
26.	How the Equivocal Forensic Analysis was employed in a Corporate Data Breach Investigation for identifying the perpetrators and adopting mitigation steps to prevent future threats?	**(10)**	**2**	**4**

****