Q. Code: 807475

Reg. No. | | | | | | | | | | | | | |

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

Seventh Semester

IT18701 – CYBER FORENSICS

(Information Technology)

(Regulation 2018 / Regulation 2018A)

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.	**1**
CO 2	Assess the investigative smart practices and applicability of concerned laws & investigative tools.	**2**
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.	**4**
CO 5	Create a method for gathering, assessing and applying new and existing legislation specific to the practice of digital forensics.	**5**

PART- A (10 x 2 = 20 Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	Explain the scope of Cyber Forensics.	**1**	**1**
2.	Differentiate disk image from disk clone.	**1**	**2**
3.	Explain the importance of Chain of Custody form.	**2**	**1**
4.	Describe Why are bit lockers so significant to the investigator?	**2**	**2**
5.	List down the areas that concern the legal aspects of investigation.	**3**	**1**
6.	Distinguish between no-knock and after hours warrants.	**3**	**2**
7.	Describe the need for duplication of digital evidence.	**4**	**3**
8.	Justify the statement “Hash generation in live forensics is not advisable”.	**4**	**3**
9.	Examine why the write protect interfaces are so significant to the investigator?	**5**	**4**

10.	Compare community cloud and hybrid cloud.	**5**	**2**	

PART- B (5 x 14 = 70 Marks)

		Marks	CO	RBT LEVEL
11. (a)	Compute the RAM, Drive and File Slack for the following: Cluster with 1000 sectors each of size 4096 bytes, File of size: 0.5Mb is Stored.	**(14)**	**1**	**3**
	(OR)			
(b)	Illustrate the investigative approach: A law enforcement agency, Cybercrime Unit, was tasked with investigating a cybercrime involving the unauthorized access and manipulation of financial records stored on various devices with different file systems. The investigation required forensic analysis of multiple file systems to uncover evidence of illegal activities and identify the perpetrators.	**(14)**	**1**	**3**
12. (a)	Discuss the investigation process flow for the case study: A multinational corporation, XYZ Inc., experienced a cyber extortion attempt wherein hackers gained unauthorized access to the company's sensitive data and threatened to release it publicly unless a substantial ransom was paid. Faced with the looming threat of reputational damage and financial loss, XYZ Inc. enlisted the assistance of law enforcement agencies specializing in cybercrime investigations.	**(14)**	**2**	**3**
	(OR)			
(b)	Discuss the importance of Network Time Protocol in the investigation of the case study: A financial institution experienced a data breach resulting in the unauthorized access and manipulation of sensitive financial records. Forensic investigators were tasked with identifying the perpetrators and determining the extent of the breach.	**(14)**	**2**	**3**
13. (a)	Illustrate the plain view doctrine, and why does it have such a significant impact on digital forensics? What are three approaches to ascertaining	**(14)**	**3**	**4**

whether the doctrine applies to a specific case?

(OR)

(b)	Explain in detail about various legislated laws that are used for ensuring the privacy of an individual.	**(14)**	**3**	**4**

14. (a)	Justify the reason behind the denial: A man was brought to court after employees at a computer repair shop discovered child pornography on his computer. He tried to get the evidence disqualified as the result of an illegal search, but the judge denied his motion.	**(14)**	**4**	**4**

(OR)

(b)	Explain the document analysis procedure for the case study: A financial institution, Alpha Bank, detected irregularities in loan applications and suspected fraudulent activities perpetrated by a group of individuals within the organization. Forensic investigators were tasked with conducting digital document analysis to uncover evidence of fraud, identify the perpetrators, and assist in legal proceedings.	**(14)**	**4**	**4**

15. (a)	Illustrate the investigation procedure for the case study: A multinational corporation, Global Tech Inc., experienced a significant data breach resulting in the unauthorized access and exfiltration of sensitive customer information stored in the cloud. Forensic investigators were tasked with conducting a cloud forensics investigation to identify the perpetrators, determine the extent of the breach, and mitigate further risks to data security.	**(14)**	**5**	**3**

(OR)

(b)	Illustrate the investigation procedure for the case study: A multinational technology corporation, TechSolutions Inc., suspected that confidential intellectual property (IP) and trade secrets were being leaked to competitors through unauthorized mobile device usage by employees. Forensic investigators were tasked with conducting a mobile forensics investigation to identify the source of the data leak, gather evidence, and prevent further disclosure of sensitive information.	**(14)**	**5**	**3**

PART- C (1 x 10 = 10 Marks)

(Q.No.16 is compulsory)

		Marks	CO	RBT LEVEL
16.	Summarize the investigation procedure for the case study: A software development company, InnovateTech Inc., suspected that a former employee had stolen proprietary source code and confidential business plans via email before leaving the company to join a competitor. To protect its intellectual property (IP) and pursue legal action against the perpetrator, InnovateTech engaged forensic investigators to conduct an email forensics investigation.	**(10)**	**3**	**5**

****