Reg. No.												

Question Paper Code	11908

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL/MAY 2023

Sixth Semester

Information Technology

20ITEL603 - CYBER SECURITY AND FORENSICS

(Regulations 2020)

Duration: 3 Hours | Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks, K-Level, CO
1.	Define cyberspace.	2,K1,CO1
2.	Mention the various ways to protect from cyber attack.	2,K1,CO1
3.	What is the need for cyber law?	2,K1,CO2
4.	What is GDPR?	2,K1,CO2
5.	List the elements in the evidence custody form.	2,K1,CO3
6.	Mention some digital forensics tools that can perform remote acquisition.	2,K1,CO3
7.	What is innocent information? Give example.	2,K1,CO5
8.	How are digital incidents secured?	2,K1,CO5
9.	Define network forensics.	2,K1,CO6
10.	What is the order of volatility?	2,K1,CO6

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	(i) Discuss the Fundamentals of Cyber Security in detail. (ii) Write short notes on the four Layers of Cyberspace.	06,K2,CO1 07,K1,CO1
		OR	
	b)	Justify the statement – "Security considerations are essential for managing the web asset".	13,K3,CO1
12.	a)	Discuss some of the common flaws that disrupt the success of encryption.	13,K2,CO2
		OR	
	b)	Explain the measures to be implemented for mitigating cyber attack.	13,K2,CO2
13.	a)	Explain the procedures for corporate high tech investigations.	13,K2,CO3
		OR	
	b)	How will you determine the best acquisition method? What is the contingency planning for image acquisition?	13,K3,CO3

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

14. a) Discuss about collecting evidence in private-sector incident scenes. *13,K2,CO5*

OR

b) Detail the steps for preparing the investigation team. *13,K2,CO5*

15. a) Explain the acquisition procedures for mobile devices. *13,K2,CO6*

OR

b) Illustrate the procedures used in network forensics. *13,K2,CO6*

PART - C (1 × 15 = 15 Marks)

16. a) What is an Intrusion Detection System? Explain the types with suitable example. *15,K2,CO4*

OR

b) Discuss about Threat Management in detail with suitable examples. *15,K2,C*