17-04-23

Reg. No.												

Question Paper Code	11766

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

Eighth Semester

Computer Science and Engineering

CS8074 - CYBER FORENSICS

(Regulations 2017)

Duration: 3 Hours | Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks, K-Level,CO
1.	Write any four examples of computer crime.	*2,K1, CO1*
2.	Define Data acquisition.	*2,K1, CO1*
3.	Describe extraction in computing the investigation.	*2,K2, CO2*
4.	List the general tasks investigators perform while working with Digital Evidence.	*2,K2, CO2*
5.	Give some legal and illegal purposes for using steganography.	*2,K1, CO3*
6.	Define any three standard procedures used in Network Forensics.	*2,K1, CO3*
7.	List the uses of hiding file extension from web pages.	*2,K2, CO4*
8.	Define Sniffing.	*2,K1, CO4*
9.	Define Session Hijacking.	*2,K1, CO5*
10.	Justify why many programs are vulnerable to SQL injection and buffer overflow attacks.	*2,K2, CO5*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	Explain different types of CF techniques available with examples.	*13,K2,CO1*
		OR	
	b)	Explain the following in brief (i) Forensic duplication and investigation. (ii) Understanding Computer Investigation.	*13,K2,CO1*
12.	a)	With an example case study how evidences can be collected in windows environment.	*13,K3,CO2*
		OR	
	b)	List and explain different computer forensics tools involved in evidence collection.	*13,K3,CO2*

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

13. a) Sam send a death threat mail to john .After sending the email, Sam deleted the email. Investigation people recovered the Sam email from recycle bin. John has reported an email message with a word document attachment from the suspect. In this scenario explain how the investigation people locate the evidence of the email and attachment. *13,K3,CO3*

OR

b) Generalize the roles of the following term in investigations *13,K3,CO3*
(i) Network Forensics.
(ii) Cell Phone Device Forensics.

14. a) Define footprinting and explain the following terminologies *13,K3,CO4*
(i) Open source or passive information gathering and Anonymous footprinting.
(ii) Organizational or private footprinting and Active information gathering.

OR

b) (i) Apply Ethical Hacking to stop crime and why it is necessary. *13,K3,CO4*
(ii) Explain the Scope and limitation of Ethical Hacking.

15. a) Explain the following in brief *13,K2,CO5*
(i) Denial of Service.
(ii) SQL injection.

OR

b) Discus the scenario where session hijacking can be done. What are the steps to hijack a session? What are the dangers posed by hijacking a session? *13,K4,CO5*

PART - C (1 × 15 = 15 Marks)

16. a) In December 2015, two California residents attacked a holiday party for the San Bernardino county Department of Public Health, killing 14 people and injuring 22 others. Soon after the attack, the two perpetrators were killed in a shoot-out with police officers. Before they were killed, both perpetrators destroyed their personal phones. Police were able to recover only the work-issued Phone of one of the shooters. The attacker's work phone was protected by a four-digit pin number and was set to erase all data on the phone after ten incorrect password-entry attempts. Explain how to extract data from mobile devices. *15,K3,CO6*

OR

b) Discus the following case study. *15,K3,CO6*
Create an environment where Man-in-the-middle and man-in-the browser attacks can be used. How can brute force be used for session hijacking?