

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code: 2058101

B.E. / B.Tech. DEGREE EXAMINATIONS, NOV / DEC 2024

Eighth Semester

Information Technology

CS8074 – CYBER FORENSICS

(Regulation 2017)

Time: Three Hours

Maximum: 100 Marks

Answer ALL questions

PART – A

(10 x 2 = 20 Marks)

1. What is meant by Identity theft & Identity Fraud?
2. Define RAID Data Acquisition.
3. Define the term “Digital Evidence”.
4. Express the term ‘Computer Forensics Tool Testing’?
5. Give some legal and illegal purposes for using steganography.
6. What are SIMCon’s features?
7. What DNS footprinting?
8. How can we defend against password cracking?
9. Differentiate ‘LAND attack’ and ‘SMURF attack’.
10. Which form of encryption does WPA use?

PART – B

(5 x 13 = 65 Marks)

11. (a) Summarize in detail about Incident Response Methodology and the six steps associated with it. (13)

(OR)

- (b) Write short notes on:
(i) Forensic duplication (7)
(ii) Forensic investigation (6)

12. (a) Discuss the validation and testing of forensic software. How Validation and Discrimination differ from each other. (13)

(OR)

- (b) Examine the processes involved in preparing for a search and the seizing procedure for Digital Evidence. (13)

13. (a) Describe the process of investigating email crimes and violation. (13)

(OR)

- (b) Give a brief description of the following data-hiding techniques: (5 + 4 + 4)
(i) Hiding Partitions
(ii) Bit-Shifting
(iii) Marking Bad Clusters

14. (a) What are the different attack vectors through which the attacker can attack information system? Explain. (13)

(OR)

- (b) Explain different types of spyware, Email and Internet spyware. (13)

15. (a) Describe in detail about the Steps in Performing Session Hijacking. (13)

(OR)

- (b) Write an overview of WEP, WPA Authentication Mechanisms, and Cracking Techniques. (13)

PART – C

(1 x 15 = 15 Marks)

16. (a) Write in detail about SQL injection. (15)

(OR)

- (b) Describe about Social Engineering with neat explanation. (15)