

Reg. No. :

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

Question Paper Code: 49024

B.E. / B.Tech. DEGREE EXAMINATION, AUGUST 2021

Elective

Computer Science and Engineering

14UCS914 – CYBER FORENSICS

(Regulation 2014)

Duration: 1:45 hour

Maximum: 50 Marks

PART A - (10 x 2 = 20 Marks)

(Answer any ten of the following questions)

1. Mention the two main transformation types that form the basis of IPsec.
2. List the algorithms used in PGP 5.X
3. Who can use Computer Forensic Evidence?
4. Define Recovery Certificate.
5. What is meant by Data Hiding?
6. Distinguish between HMAC and MAC.
7. List the algorithms used in PGP 5.X
8. How will you specify the rules for computer Forensics in investigation ?
9. Point out the tools used in validation and discrimination in Forensics.
10. Define Network Forensics.
11. Explain IPsec Protocol Documents.
12. List out the data fields contained in ASCII Armor Format.
13. Who can use Computer Forensic Evidence?
14. Define Recovery Certificate.
15. What is meant by Data Hiding?

PART – B (3 x 10= 30 Marks)

(Answer any three of the following questions)

11. Discuss about Key Management Protocol for IPsec. (8)
12. Briefly explain the types of Firewalls with a neat diagram and examples. (8)
13. Explain in detail about Incident Response Methodology and the six steps associated with it. (8)
14. Describe about the following mechanisms:
 - (i) Understanding File Systems. (8)
15. Describe in detail about using specialized E-mail Forensics Tools. (8)