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

Question Paper Code : X 20375

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2020
Seventh/Eighth Semester
Computer Science and Engineering
CS 6004 – CYBER FORENSICS
(Common to Information Technology)
(Regulations 2013)

Time : Three Hours | Maximum : 100 Marks

Answer ALL questions

PART – A **(10×2=20 Marks)**

1. Write the importance of SSL protocol.
2. Draw the ESP packet format.
3. List out the advantages of firewalls.
4. Need for SET business requirements.
5. Write the role of a computer in a crime.
6. "Stealing your mail, including your bank and credit card statements, preapproved credit offers, telephone calling cards and tax information" – Is your personal identify theft ? Justify.
7. Write any two types of field kit to be used in crime scene.
8. Name any four software forensic tools.
9. Write the validation process of forensics data.
10. What are the methods used to validate the forensics data ?

PART – B **(5×13=65 Marks)**

11. a) Explain the basic components of the IPsec security architecture. **(13)**

(OR)

b) i) Write short notes on Key Management Protocol for IPsec. **(7)**

ii) How the Pseudo Random Number Generator (PRNG) works ? **(6)**

12. a) i) Discuss the process of assess "Digital Envelope" in S/MIME. **(7)**

ii) What is Secure Electronic Transaction (SET) ? Outline the SET system participants. **(6)**

(OR)

b) Explain the different types of firewalls with a neat diagram. **(13)**

13. a) Discuss various types of Computer forensics techniques. **(13)**

(OR)

b) Write the preparation steps to acquire digital evidence, processing crime scene. **(13)**

14. a) Describe the processing crime and incident scenes. **(13)**

(OR)

b) Examine the MS-DOS Startup Tasks and about other Disk Operating Systems in detail. **(13)**

15. a) E-Mail Investigations ? Explain. **(13)**

(OR)

b) i) Write the various data hiding techniques. **(5)**

ii) Describe the cell phone and mobile devices forensics. **(8)**

PART – C **(1×15=15 Marks)**

16. a) Explain the system that enforces an access control policy between two networks and also blocks traffic and permits traffic.

(OR)

b) Larry deposits a stolen third-party check into his account. No problems are detected during cheque clearance, and two days later cleared funds are available in Larry's account. Subsequently an ATM camera records Larry making a cash withdrawal. The bank's forensics system analyzes the video image and a match is found against the latest police records of Larry, wanted in connection with illegal drug activities. How would your forensic system continue to handle this analysis ?

———————