Reg. No. : ☐☐☐☐☐☐☐☐☐☐☐☐☐

Question Paper Code : 70362

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2021.

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. List the Payload Types for ISAKMP.

2. List out the data fields contained in ASCII Armor Format.

3. Suppose the string of octets [0008 02fe] forms an MPI. The length of the MPI in bits [00000000 00001001] or 9 (= 23 + 20) in octets. Identify the actual integer value of the MPI.

4. List the types and importance of firewalls.

5. What is identity fraud?

6. Define forensic duplication.

7. When you delete a image/audio/video, do you really delete it? Is it possible to revert the deleted data?

8. What is a virtual machine?

9. What is a MVNO?

10. What is the purpose of PUK?

PART B — (5 × 13 = 65 marks)

11. (a) Outline the steps in the Hashed Message Authentication Code algorithm with an example. (13)

Or

(b) Outline the overall operation of the SSL record protocol with a diagram. (13)

12. (a) Discuss in detail about PGP.

Or

(b) Give a detailed description about the role of firewalls.

13. (a) Discuss in detail the systematic approach in computer investigations and conducting an Investigation in Computer Organizations. (13)

Or

(b) Discuss the investigation of Employee termination case, Internet abuse investigation, Attorney Client Privilege investigation in corporate high tech investigation.

14. (a) Outline the seizing procedure for the Digital Evidence at the Crime Scene.

Or

(b) Illustrate with an example to examine the NTFS disk.

15. (a) Explain the process of investigating e-mail crimes and violation. (13)

Or

(b) Appraise the acquisition procedures for cell phones and mobile devices. (13)

PART C — (1 × 15 = 15 marks)

16. (a) Draw a framework for protecting credit card transactions over the Internet and outline their functions. (15)

Or

(b) Prepare a plan for conducting a computer investigation. (15)

———————