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

Question Paper Code : 20342

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2018.

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. Define Certificate.
4. Define SOCKS.
5. Show the hierarchy of Contemporary Cybercriminals.
6. Outline the tasks of a Computer Forensics Examination Protocol.
7. State the motivations for computer intrusion or theft of information in contemporary society.
8. Distinguish between Validation and discrimination.
9. Show various Steganalysis attack methods.
10. Define order of volatility (OOV).

PART B — (5 × 13 = 65 marks)

11. (a) Explain in detail about functionalities of IP Authentication Header.

Or

(b) Explain how series of message is exchanged between client and server by SSL Handshake Protocol.

12. (a) Explain in detail about the basic terminologies required to design and configure a firewall.

Or

(b) Explain in detail about MIME.

13. (a) Determine the Physical Requirements for a Computer Forensics Lab.

Or

(b) Demonstrate the use of computer forensic hardware and software tools used to solve the different types of forensics.

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

Or

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

15. (a) Explain all the data hiding techniques and how to apply the data hiding techniques in various applications.

Or

(b) List out the steps involved in examining in Microsoft e-mail server logs and explain it in detail.

PART C — (1 × 15 = 15 marks)

16. (a) You're using Disk Manager to view primary and extended partitions on a suspect's drive. The program reports the extended partitions total size as larger than the sum of the sizes of logical partitions in this extended partition. Justify the following terms when

(i) The disk is corrupted.

(ii) There's a hidden partition.

(iii) Nothing; this is what you'd expect to see.

(iv) The drive is formatted incorrectly.

(v) Password is unknown.

Or

(b) Interpret and validate the results of a forensics analysis, you should do which of the following.

(i) Calculate the hash value with two different tools.

(ii) Use a different tool to compare the results of evidence you find.

(iii) Repeat the steps used to obtain the digital evidence, using the same tool, and recalculate.

(iv) The hash value to verify the results.

(v) Do both (i) and (ii).

(vi) Do both (ii) and (iii).

(vii) Do both (i) and (iii).

———————