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

Question Paper Code : 52841

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2019.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6004 — CYBER FORENSICS

(Common to Information Technology)

(Regulation 2013)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Draw the ESP packet format.
2. Define HMAC algorithm.
3. Write the role of firewalls.
4. What are the business requirements for SET?
5. Is your personal information used against you, to do crime? Justify.
6. List the benefits of computer forensics methodology.
7. List out any two forensics tool for evidence collection.
8. How to identify the cyber crime?
9. Write any one the network forensics scenario.
10. How to perform the remote acquisition process?

PART B — (5 × 13 = 65 marks)

11. (a) Discuss the basic components of the IPsec security architecture.

Or

(b) Explain the overall operation of the SSL record protocol.

12. (a) Describe in detail about different types of firewalls.

Or

(b) (i) How the dual signature and signature verification is done? Explain. (7)

(ii) Explain the PGP (Pretty Good Privacy) message format. (6)

13. (a) (i) Discuss the problems associated with computer crime. (7)

(ii) Write about traditional computer crime. (6)

Or

(b) (i) Explain the forensic duplication and investigation process in detail. (7)

(ii) Discuss the Identity theft and Identity fraud. (6)

14. (a) Consider the situations, Employer files have been deleted, disks have been reformatted, or other steps have been taken to conceal or destroy the evidence. How to recover the evidence using any forensics tool to safe guard the employee?

Or

(b) How to process the cyber crime and incident scenes? Explain it.

15. (a) Write short notes on :

(i) Email Investigations. (7)

(ii) Data Hiding techniques. (6)

Or

(b) A man has been arrested by the Crime Branch of Mumbai Police for allegedly sending threatening text messages to Bollywood actress. The accused sent four messages to the actress, threatening to kill her children if she did not pay him, say sources. How to do mobile device forensics on this case?

PART C — (1 × 15 = 15 marks)

16. (a) Consider the encoding process from 8-bit Input groups to the output character string in the radix-64 alphabet.

(i) Input raw text: 0x 15 d0 2f 9e b7 4c

(ii) Input raw text: 0x 15 d0 2f 9e b7.

Or

(b) A patient with a heart ailment was transported to a hospital where an angiogram was performed. The patient later had a stint inserted into an artery, along with a second angiogram, but died shortly thereafter. A third angiogram was performed immediately after the patient's death. Images of the angiogram procedures were purportedly stored on computer hard drives. The day following the patient's death, hospital staff were able to locate images for the first and third angiograms but could not find any images of the second procedure. The hospital and doctor were sued for medical malpractice and wrongful death. The plaintiffs also claimed the defendants had deliberately deleted the images of the second angiogram that allegedly proved the wrongful death claim. A CES team (CFST) was engaged by the doctor's insurance company to locate images of the second angiogram on the computer hard drive. Explain the possible actions that the CFST took to locate the images.