Reg. No. : □□□□□□□□□□□□

Question Paper Code : 91376

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2019
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. Differentiate MAC and HMAC.
2. Draw the header format of IP authentication protocol.
3. List out the limitations of firewalls.
4. Write the advantages of E-commerce transactions.
5. Can your personal information be used against you to do crime ? Justify.
6. How can Hidden Data in Forensics Technology be found ?
7. Classify the software forensic tools.
8. How to process the threatening SMS related crimes ?
9. Write the validation process of forensics data.
10. Name any three mobile device forensics tools.

PART – B (5×13=65 Marks)

11. a) Draw the diagram for Server and Client communication in SSL handshaking protocol and discuss it.

(OR)

b) i) Discuss about key management protocol used with IPSec. (7)

ii) Elaborate on the key Generation using Pseudo Random function to expand secrets into blocks of data in TLS with an example. (6)

12. a) i) What is meant by Digital Envelope ? Explain its significance in E-mail security. (7)

ii) Describe the secure payment processing in SET. (6)

(OR)

b) Write the role of firewall and explain the types of firewalls with neat diagrams.

13. a) i) Explain in detail about identity Theft and identity Fraud and mention the points of differences between them. (7)

ii) Discuss the investigation of Employee case, internet abuse investigation, Attorney Client Privilege investigation in corporate high tech investigation. (6)

(OR)

b) Discuss the various types of computer forensics techniques.

14. a) i) Illustrate how will the processing of an incident or a crime scene takes place in cyber forensics. (7)

ii) How to collect the document evidence in Lab ? Explain. (6)

(OR)

b) Examine the evidences that can be collected in MS-DOS and Windows Operating Systems in detail.

15. a) Illustrate the investigations that can be carried out on threatening messages, prize won messages and offer orders forwarded through E-mails.

(OR)

b) Discuss the various data hiding techniques with examples.

PART – C (1×15=15 Marks)

16. a) A parent was concerned that her son was accessing unwanted websites from his computer. Each time the computer was checked by a technician, no evidence was found. How would a computer forensics service go about investigating this incident ?

(OR)

b) A public institution was the victim of a hacker. The subject got into the network and placed several large media files on several computers and changed the desktop configurations. Management decided against calling law enforcement initially (because of media attention) and instructed the IT department to get a cyber forensics system to privately investigate. How did the cyber forensics system go about conducting the investigation ?