Reg. No. : □□□□□□□□□□□□

Question Paper Code : 40884

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2018

25/04/18

AN

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. Bring out any two difference between Http and Https protocol.

2. Define SSL session and SSL connection.

3. How PGP provides confidentiality ?

4. What is a proxy server ?

5. Define identity fraud.

6. What is e-mail abuse ?

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 steganography ?

10. Give examples for e-mail forensics tools.

PART – B (5×16=80 Marks)

11. a) i) Outline the basic components of the IPSec security architecture. (4)

ii) Explain the OAKLEY key determination protocol. (12)

(OR)

b) Explain with a diagram the overall operation of the Secure Sockets Layer (SSL) record protocol. (16)

12. a) What is a firewall ? Explain with a diagram a screened host firewall which uses a single-homed bastion host, a screened host firewall which uses a dual-homed bastion host and a screened subnet firewall. (16)

(OR)

b) What is Secure Electronic Transaction (SET) ? Explain the business requirements for SET and outline the SET system participants. (16)

13. a) Outline the problems and challenges forensic examiners face when preparing and processing investigations, including the ideas and questions they must consider. (16)

(OR)

b) Explain the process of acquiring data with a Linux Boot CD. (16)

14. a) Outline the process of preparing to acquire digital evidence, processing an incident or crime scene and processing data centers with RAID systems. (16)

(OR)

b) Explain the following : NTFS data streams, NTFS compressed files and NTFS encrypting file system. (16)

15. a) Explain the process of investigating e-mail crimes and violation. (16)

(OR)

b) Appraise the acquisition procedures for cell phones and mobile devices. (16)
