CSE 424 A (R-15)

Total No. of Questions :09] [Total No. of Pages : 02

IV/IV B.Tech. DEGREE EXAMINATIONS, NOV/DEC- 2019

Second Semester

COMPUTER SCIENCE ENGINEERING

COMPUTER FORENSICS

Time: Three Hours **Maximum marks:60**

Answer Question No.1 Compulsory **12X1=12 M**

Answer ONE Question from each Unit **4X12=48 M**

1. Briefly explain following
   a) What are the challenges in evidence handling?
   b) List some tools to recover deleted files.
   c) What is the use of cache files?
   d) What are the types of networks available?
   e) Define Web.
   f) Define Registry
   g) Give the types of evidence
   h) State the motivations for computer intrusion or theft of information in contemporary society
   i) Mention some problems with Computer Forensic Evidence.
   j) Expand FIRE
   k) Tools used on network forensics.
   l) Expand GUI

UNIT-I

2. a) What is computer forensics? Explain the use of computer forensics in law enforcement?
   b) Describe the role of evidence in computer forensics.

P.T.O

(OR)

3. a) Describe the role of windows registry in collecting forensic evidence.

   b) What is a file system? Give comparison of various file systems used for storage.'

UNIT-II

4. a) Briefly explain the process of collecting the volatile data in Windows system.

   b) Explain the factors that affect backup in data recovery.

(OR)

5. What are the steps involved in computer evidence processing? Explain.

UNIT-III

6. a) What are the steps in a computer forensic investigation? Who does it?

   b) Describe procedures for acquiring data from cell phones and mobile devices.

(OR)

7. a) Which tool do you prefer, Encase or FTK, and why?

   b) State and explain different mobile forensics equipment.

UNIT-IV

8. Give an overview of investigative procedure for extraction, preservation and disposition of legal evidence in a court of law.

(OR)

9. a) Illustrate various methods in dealing with hostilc codes.

   b) How law enforcement is done in computer forensics? Explain.

CSE 424 A (R-15)

Total No. of Questions :09] [Total No. of Pages : 02

IV/IV B.Tech. (Regular) DEGREE EXAMINATIONS, APRIL- 2019

Second Semester

COMPUTER SCIENCE ENGINEERING

COMPUTER FORENSICS

Time: Three Hours **Maximum marks:60**

Answer Question No.1 Compulsory **12X1=12 M**

Answer ONE Question from each Unit **4X12=48 M**

1. Briefly explain following
   a) Define meta data
   b) What is chain of custody?
   c) Laws related to computer forensics
   d) List the challenges involved in evidence handling
   e) What is live acquisition
   f) Encryption Vs decryption
   g) Mention some problems with Computer Forensic Evidence
   h) What is the need of data recovery in computer forensics?
   i) What is the use of file system?
   j) What methods are available for recovering passwords?
   k) What types of devices can forensic evidence be found on?
   l) Give the importance of disk imaging.

UNIT-I

2. a) What is cyber crime? Compare traditional criminal activity with cyber crime.
   b) How the understanding of File Systems plays a crucial role in cyber forensics.

(OR)

3. Illustrate how will the processing of an incident or a crime scene takes place in cyber forensics. **P.T.O**

UNIT-II

4. a) How steganography is used to protect copyrighted material?

   b) What is evidence? Give different categories of evidence.

(OR)

5. Describe about how the whole disk encryption is performed in Cyber forensics.

UNIT-III

6. a) What are the main concerns in the search and scizure procedures for cell phones and mobile devices? Give reasons for those concerns.

   b) Give the features of Sleuth Kit Forensic browser.

(OR)

7. a) Explain the attacks on network and its prevention.

   b) How will you collect network based evidence? Discuss various means of analyzing it.

UNIT-IV

8. a) Describe various threats to software. Explain with an example each.

   b) What is criminal justice? How does it work?

(OR)

9. a) Focus on the privacy issues to be considered in computer crime.

   b) Discuss various mechanisms to handle buffer overflow problem.