[6263]-86

B.E. (Computer Engineering)
CYBER SECURITY AND DIGITAL FORENSICS
(2019 Pattern) (Semester - VII) (410244 C) (Elective - III)

Time : 2½ Hours]

[Max. Marks : 70

Instructions to the candidates:

1) Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8.
2) Neat diagrams must be drawn wherever necessary.
3) Figures to the right side indicate full marks.
4) Assume suitable data if necessary.

Q1) a) What are the typical services offered by computer forensics professionals? (explain any two) **[9]**

b) What specific technologies are utilized in the field of business computer forensics? (Describe any two) **[9]**

OR

Q2) a) How does computer forensics technology vary cross different sectors like miltary law enforcement & business? **[9]**

b) What are the key components of a data recovery solutions in computer forensics? Explain in detail. **[9]**

Q3) a) What are various options available for collecting digital evidences? Explain in detail? **[8]**

b) Explain the essential steps in processing digital evidence from the crime scene? **[9]**

OR

Q4) a) What is the volatile evidence in the context of computer forensics, and why is it important to collect in quickly? **[8]**

b) What are the hypical steps involve in the collection of digital evidence? **[9]**

Q5) a) What are some common data hiding techniques? Explain any one in detail? **[8]**

b) What is the honey net project, and how does it contribute to network forensics? **[9]**

OR

P.T.O.

Q6) a) What precautions should investigators take to prevent data alteration or loss during the seicure process? Explain any one in detail? **[8]**

b) What are the challenges and best practices associated with performing remove acqisitions? **[9]**

Q7) a) Whar are the common examples of email crime & violations that may necessitate investigation? Explain any one in detail? **[9]**

b) Explain any software tool using in computer forensics investigation and its respective purpose? **[9]**

OR

Q8) Write short note (any two) **[18]**

a) Computer forensics hardware tools

b) Validating & testing forensics software

c) e-mail investigation

◀▶ ◀▮ ▮▶