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

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 indicate full marks.
  4)   Assume suitable data, if necessary.

Q1) a) What are the typical steps followed by computer forensics specialists in an investigation? Explain any 2 in detail.   **[8]**

   b) In what ways can business benefit from computer forensics technology explain in details?   **[9]**

<div align="center">OR</div>

Q2) a) Explain in details different computer forensics services.   **[9]**

   b) Why is data backup & recovery important in computer forensics?   **[8]**

Q3) a) What are the typical steps involved in the collection of digital evidence?**[9]**

   b) What are the different approaches for validating forensic data?   **[9]**

<div align="center">OR</div>

Q4) a) Why collect evidence? collection options in digital evidence. explain in details?   **[9]**

   b) Discuss the various legal aspects of collecting and storing digital evidence.   **[9]**

Q5) a) What are same common network tools, used in network forensics.   **[9]**

   b) Describe the process of seizing digital evidence at a crime or incident scene?   **[8]**

<div align="center">OR</div>

Q6) a) What is the honeynet project, how does it contribute to network forensics? **[9]**

b) Give in detail the different techniques to hide data in digital forensics? **[8]**

Q7) a) Write short note on. **[9]**

    i) Tools for email forensics

    ii) Computer forensics hardware tools

b) Explain the process for validating and testing forensics software. **[9]**

<center>OR</center>

Q8) a) What is function email server show does it store of mange e-mail data? **[9]**

b) Write short note on. **[9]**

    i) Computer forensics software tools

    ii) E-mail Investigations

<center>■■■■</center>