

[6584]-96

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 whenever necessary.
- 3) Figures to the right indicate full marks.
- 4) Assume suitable data, if necessary.

- Q1) a) What are the various steps taken by computer forensics specialists. [8]
- ✓ b) Describe in brief the significance of data recovery and backup. Explain various data recovery solutions. [9]

OR

- Q2) a) Explain in brief computer forensic services. Write the applications of Digital forensics in health care. [8]
- b) What is role of digital forensics in law enforcement? [9]

- Q3) a) Discuss the various legal aspects of collecting and storing digital evidence. [9]
- b) Enlist and explain different computer evidence processing steps. [9]

OR

- Q4) a) What are various methods of collecting digital evidence and explain any four digital evidence collection steps. [9]
- ✓ b) What is chain custody? Discuss methods to control the contamination of digital evidence? [9]

- Q5) a) Describe different approaches for validating forensics data. [9]
- ✓ b) Explain the approaches for seizing digital evidence at the crime scene. [8]

OR

P.T.O.

SPPU-BE-COMP-CONTENT – KSKA Git

- Q6) a) Describe the steps of identifying digital evidence in computer forensics. [9]
b) Explain process of developing standard procedures for network forensics using network forensics tools. [8]

- Q7) a) Write short notes on : [9]

- i) Computer forensics tools testing and validation.
ii) E-mail crimes

- b) State the features of any five Computer forensic hardware tools. [9]

OR

- Q8) a) What is the volatile evidence. [9]

- b) Write short notes : [9]

- i) Role of client and server in email.
ii) Specialized email crimes & investigations tools.

