B.E. (Information Technology) Seventh Semester (C.B.S.)
Elective - II : Digital Forensics for Information Technology

P. Pages : 2

Time : Three Hours

Max. Marks : 80

1080

_____

Notes : 1. All questions carry marks as indicated.
2. Solve Question 1 OR Questions No. 2.
3. Solve Question 3 OR Questions No. 4.
4. Solve Question 5 OR Questions No. 6.
5. Solve Question 7 OR Questions No. 8.
6. Solve Question 9 OR Questions No. 10.
7. Solve Question 11 OR Questions No. 12.
8. Due credit will be given to neatness and adequate dimensions.

1. a) What is digital Forensics? Explain the use of digital Forensics in law enforcement. **7**

   b) Explain the following business computer forensics technology. **7**

      i) Creating trackable electronic documents.

      ii) Forensic services available.

   OR

2. a) Explain the benefits of professional forensics methodology in detail. **7**

   b) Define cyber crime? What are the various types of cyber crimes. Also explain its classification. **7**

3. a) Explain controlling contamination. The chain of custody? **6**

   b) What is data backup and recovery. Explain the role of backup in data recovery. **7**

   OR

4. a) What are the steps involved in computer evidence processing? Explain. **7**

   b) Explain the process of validating the forensic data? **6**

5. a) How are evidences collected? What are different evidence processing steps. **7**

   b) What is duplication of digital evidence? Explain its purpose? **6**

   OR

6. a) How do you evaluate computer forensic tools? **7**

   b) Enumerate the basic steps for computer forensic investigations. **6**

7.	a)	Enumerate different steps of live acquisitions explain in brief.	7
	b)	How do we seize digital evidence at the scene.	6

OR

8.	a)	How do you secure a computer incident or crime scene?	7
	b)	Explain evidence retention and media storage needs?	6
9.	a)	Explain the process of investigating E-mail crimes and violations?	7
	b)	Explain the SIM card and SIM file structure?	6

OR

10.	a)	What is role of e-mail in forensic investigations?	7
	b)	What is i-node? What information is contained in i-node?	6
11.	a)	Write short notes on **any two.**	7

    i)   RAID server disks.

    ii)   NTFS system files.

    iii) Windows Registry.

	b)	What are three rules for forensic hashes? How can we obtain digital hash.	7

OR

12.	a)	What happens when a file is deleted from windows explorer and from the command prompt? Explain.	7
	b)	Explain the functions of following registry.	7

    a)   HKEYS

    b)   HKEY_CLASS_ROOT

    c)   HKEY_LOCAL_MACHINE

****