B.E. (Information Technology) Semester Seventh (C.B.S.)

Elective - II : Digital Forensics for Information Technology

P. Pages : 2 **KNT/KW/16/7508**

Time : Three Hours * 0 8 8 1 * Max. Marks : 80

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.
9. Illustrate your answers whenever necessary with the help of neat sketches.

1. a) What is digital forensics? How it differs from normal forensic science? Explain brief history of digital forensics. **7**

b) What it is necessary to maintain professional conduct during computer investigation? How can this be maintained. **7**

OR

2. a) Explain the procedure of digital forensics with the help of neat sketch. **7**

b) Explain the term cyber crime.What actors are involved in it? What are different kinds of cyber crimes? **7**

3. a) Explain the meaning of Digital evidence. Explain some important provisions of law dealing with digital evidence. **7**

b) List standard system analysis steps to be applied when preparing a case. **6**

OR

4. a) How data collection is done? Explain different data collection methods. **6**

b) Explain how evidence is collected in private sector incidents. **7**

5. a) Write short notes on: **6**
i) Network forensics.

ii) Internet abuse.

b) What is data acquisition? What are its types? What are its goals? Explain. **7**

OR

6. a) Explain why investigation plan may require refining and modification? Elaborate further with example. **7**

b) What are different evidence processing steps? Explain. **6**

7. a) Enumerate steps for storing digital evidence. **6**

b) What is digital hash? How it is obtained. Explain different kinds of hashes. **7**

OR

8. a) How do you prepare yourself for search? What do you do for securing a computer incident or crime scene? **7**

b) Explain general steps for live acquisition. **6**

9. a) How to investigate email crimes & violations? Explain in detail. **7**

b) Explain the following terms: **any three**. **6**

i) CDMA ii) EDGE
iii) OFDM iv) ITU

OR

10. a) Describe the procedure for acquiring data from cell phones and mobile devices. **7**

b) Explain SIM file structure in detail. **6**

11. a) Explain NTFS in detail. What are the metadata records in master file table of NTFS? **7**

b) What happens when a file is deleted from windows explorer and form the command prompt? Explain can it be recovered even after the dist. get formatted? **7**

OR

12. Write short notes on **any three.** **14**

1) Android forensics 2) Windows registry
3) Disk encryption tools 4) Forensic hashes

****