CBCS SCHEME

USN | | | | | | | | | | |

18SFC21

Second Semester M.Tech. Degree Examination, June/July 2019
Preserving Recovering Digital Evidence

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. What is Digital Evidence? Explain the different categories of computer system and different challenging aspects of digital evidence. **(10 Marks)**

b. Explain the role of digital evidence during investigation process. **(10 Marks)**

OR

2 a. Explain investigative methodology with neat diagram. **(10 Marks)**

b. Explain different steps involved in investigative reconstruction. **(10 Marks)**

Module-2

3 a. During the forensic examination of the windows system, explain the different ways of internet traces that can be recovered. **(10 Marks)**

b. During the forensic examination of the unix system, explain the different ways of internet traces that can be recovered. **(10 Marks)**

OR

4 a. Explain data recovery in window system. **(08 Marks)**

b. Explain file system of unix system. Describe the traces on the file system which are helpful in digital evidence examination using unix system. **(12 Marks)**

Module-3

5 a. List the steps involved in applying forensic science to networks. Explain ay 4 in detail. **(10 Marks)**

b. With neat diagram explain documentation, collection and preservation on physical and data link layer. **(10 Marks)**

OR

6 a. Explain how TCP/IP related data evidences are useful in digital investigation. **(12 Marks)**

b. List the internet services at the application layer and explain briefly their role in criminal investigation. **(08 Marks)**

Module-4

7 a. Explain different steps used in investigating cyber stalking. **(10 Marks)**

b. What is Alibi? Explain investigating an alibi, time as alibi and location as an alibi. **(10 Marks)**

OR

8 a. With neat diagram explain possible sources of evidence in sex offense investigation and steps involved in investigative reconstruction. **(10 Marks)**

b. How computer intrusions are investigated with respect to processes as a source of evidence in windows and unix system? **(10 Marks)**

Module-5

9 a. Explain the overview of identification and seizure process. (10 Marks)
b. What are the digital evidence examination guidelines to be followed during processing of windows GUI? (10 Marks)

OR

10 a. List the steps to be taken in preservation of digital evidence. (10 Marks)
b. What are the digital evidence examination guidelines to be followed during processing of dos/windows command line? (10 Marks)

* * * * *