CBCS Scheme

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

16/17SFC21

Second Semester M.Tech. Degree Examination, June/July 2018
Preserving and Recovering Digital Evidence

Time: 3 hrs. Max. Marks: 80

Note: *Answer 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. **(08 Marks)**

b. Explain with example cybertrail. Explain the challenging aspects of the cybertrail. **(08 Marks)**

OR

2 a. Explain the role of digital evidence during investigation process. **(08 Marks)**

b. Explain language of computer crime investigation in detail. **(08 Marks)**

Module-2

3 a. What is investigative reconstruction process? What are its uses? Explain equivocal forensic analysis in detail. **(08 Marks)**

b. Explain technology and law with respect to US(United States) perspective. **(08 Marks)**

OR

4 a. What is investigation intrusions? Explain processes as a source of evidence for Windows and Unix. **(08 Marks)**

b. Explain the different steps involved in investigative reconstruction. **(08 Marks)**

Module-3

5 a. Explain the different steps used in investigating cyberstalking. **(08 Marks)**

b. What is an Alibi? Explain investigating an Alibi, Time as Alibi and location as Alibi? **(08 Marks)**

OR

6 a. Explain an overview of identification and seizure process. **(08 Marks)**

b. Explain preservation with sample preservation forms. **(08 Marks)**

Module-4

7 a. Explain how computer intruders operate. **(08 Marks)**

b. Explain how cyberstalkers operate. **(08 Marks)**

OR

8 a. Briefly discuss about the private, public and e-mail encryption with example. **(08 Marks)**

b. What are the different stages/sessions of applying forensic science? Explain any four sessions. **(08 Marks)**

Module-5

9 a. During the forensic examination of Windows system, what are the different ways of internet traces can be recovered. **(08 Marks)**

b. List the TCP/IP related digital evidence. Explain any three in detail. **(08 Marks)**

OR

10 a. Explain collection and examination of handled devices. **(08 Marks)**

b. Explain TCP/IP related digital evidence in transport layer. **(08 Marks)**

* * * * *