M.Tech 3rd Semester Forensics and Information Security Examination, December–2017

PRESERVING AND RECOVERING DIGITAL EVIDENCE

Paper-MTCF-301

Time allowed : 3 hours] *[Maximum marks : 100*

Note : ***Question No. 1 is compulsory.*** *Attempt* ***five*** *questions in total selecting* ***one*** *question from each section.*

1. (a) Define the term 'modus operandi'.
   (b) What is a computer virus ?
   (c) What do you mean by investigative reconstruction?
   (d) How registry files are helpful in digital investigation ?
   (e) What do you mean by time as alibi ?
   (f) What is internet trace file ?
   (g) Define the term 'IRC'.
   (h) What do you mean by password protection and encryption ? 2½×8=20

Section–A

2. Explain the following : 20
   (a) Direct vs circumstantial evidences.
   (b) Role of computers in crime investigation.
   (c) Threshold assessments.

3. What do you mean by digital investigation ? Explain one digital investigation process model. 20

Section–B

4. Write notes on : 20
   (a) Data recovery in unix
   (b) Role of log files in digital investigation
   (c) Data hiding

5. (a) Explain how file system can be used for forensic examination. 10
   (b) Explain data recovery process in Mac OS. 10

Section–C

6. Write notes on : 20
   (a) TCP/IP related digital evidence
   (b) E-mail forgery and tracking
   (c) Legitimate vs criminal use of internet services

7. (a) What is filtering and data reduction ? 10
   (b) Explain the use of internet as investigation tool. 10