

(3 Hours)

Total Marks: 80

N.B.: (1) Question No.1 is compulsory.

(2) Attempt any three questions from the remaining five questions.

(3) Make suitable assumptions wherever necessary but justify your assumptions.

1. (a) What is Cybercrime? What are the different roles of computer with respect to cybercrime. 05
(b) Explain the term Chain of Custody. 05
(c) What is CSIRT? 05
(d) What all volatile information which you will be collecting before switching off computer system. Also explain its role in digital forensic investigation. 05
2. (a) Explain various forensic duplication tools used for analysis. 10
(b) Explain Incident Response Methodology in detail. 10
3. (a) Explain procedure for recording cryptographic checksum of digital files and advantages of it. 10
(b) Explain guidelines for incident report writing. Give one report writing example. 10
4. (a) Explain how intruders make use of social engineering & reverse social engineering to achieve their motive. 10
(b) List down various Digital forensic tools and explain one tool with case study example. 10
5. (a) Explain the difference between FAT file system and NTFS file system structure 10
(b) Explain the attacks on Network and its prevention. 10
6. Write a short note on 20
 - (1) Intrusion detection
 - (2) Can-SPAM and CFAA