C1001

Total Pages : 4 Roll No. ....

MIT (CS)-202/PGDCS-06

Digital Forensic

(MSCCS-18/PGDCS-17)

2nd Semester Examination, 2022 (June)

Time : 2 Hours] **Max. Marks : 80**

Note : This paper is of Eighty (80) marks divided into two (02) Sections A and B. Attempt the questions contained in these sections according to the detailed instructions given therein.

SECTION–A

(Long Answer Type Questions)

Note : Section 'A' contains Five (05) long answer type questions of Twenty (20) marks each. Learners are required to answer any Two (02) questions only.

(2×20=40)

1. Answer the following : (5 marks each)

(a) What are the four stages of computer forensic process?

(b) What are the objectives of computer forensics?

(c) What is the role of a forensics investigator?

(d) What is continuity of evidence?

2. Answer the following:

(a) State Locard's Principle. (4)

(b) What is best evidence rule? Under what circumstances the duplicate copy of the digital evidence is admissible for lawful purposes? (8)

(c) What are the essential characteristics of digital evidence? (8)

3. Answer the following :

(a) What do you mean by "shadow copy" of the World Wide Web and 'cloaked' URL? Where does it take place? Describe in detail. (10)

(b) How is privacy a big issue in emailing? (5)

(c) What are the various types of email services? (5)

4. Answer the following :

(a) What are the different steps involved in the assessment of the situation? (7)

(b) What are the important guidelines for forming an investigating team? (7)

(c) How the authenticity of the digital evidence can be proved? (6)

5. Answer the following :

(a) State major features of wireshark tool. (6)

(b) What is promiscuous mode in networking? (5)

(c) Describe any 3 web application forensic tools. (9)

SECTION–B

(Short Answer Type Questions)

Note : Section 'B' contains Eight (08) short answer type questions of Ten (10) marks each. Learners are required to answer any Four (04) questions only. (4×10=40)

1. Answer the following :

(a) What is network sniffing? List some popular tools used for packet sniffing. (5)

(b) List all the important sections that should be included in the investigation report. (5)

2. Answer the following : (5 marks each)

(a) What is a file system? Why it is used?

(b) What are different types of File Systems? Explain in detail.

3. Answer the following : (5 marks each)

(a) What do you understand by network tapping and port mirroring?

(b) How are the network logs captured and analyzed? Explain.

4. Answer the following:

(a) Why the testimonies of the experts are becoming increasingly important these days? (5)

(b) Describe the various steps of report preparation in detail. (5)

5. Answer the following :

(a) List all the important sections that should be included in the investigation report. (5)

(b) What are the different techniques of digital forensics? (5)

6. Answer the following :

(a) Explain the working of HDD

(b) What is cyclic redundancy check (CRC)? (5)

7. Explain various types of mobile communications and relate this to forensic investigation.

8. State the usage and forensic importance of PsLoggedon, Netsessions, logonsessions tools.