A–1280

Total Pages : 4 **Roll No. .....**

MIT (CS)-202

(MCA/MSCCS)

Digital Forensics

Examination February, 2026

Time : 2:00 Hrs. Max. Marks : 70

Note* :–** This paper is of Seventy (70) marks divided into Two (02) Sections 'A' and 'B'. Attempt the questions contained in these Sections according to the detailed instructions given therein. ***Candidates should limit their answers to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

Section–A

(Long Answer Type Questions) (2×19=38)

***Note* :–** Section 'A' contains Five (05) Long-answer type questions of Nineteen (19) marks each. Learners are required to answer any *two* (02) questions only.

1. (a) What are various steps involved in forensic readiness planning ? 7

(b) State the usage and forensic importance of PsLoggedon, Netsessions, logonsessions tools. 12

2. (a) State Locard's Principle. 3

(b) What is a slack space, swap space and file carving ? 6

(c) What is the role of intrusion detection and prevention systems (IDS/IPS) in web attack investigations ? 10

3. (a) What is first responder's toolkit ? What are the steps for preparing first responder's toolkit ? 8

(b) What are the different techniques of digital forensics ? 11

4. (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) Explain the difference between FAT32, NTFS, and exFAT file systems. 5

(c) What is incident response ? Explain goals of incident response. 4

5. (a) List and explain major cyber laws in India (e.g., IT Act, 2000 and its amendments). 11

(b) Describe the importance of server logs and web traffic analysis in web attack investigations. 5

(c) Explain the term evidence ? Also explain its types. 3

Section–B

(Short Answer Type Questions) (4×8=32)

***Note* :–** Section 'B' contains Eight (08) Short-answer type questions of Eight (08) marks each. Learners are required to answer any *four* (04) questions only.

1. What is network sniffing ? List some popular tools used for packet sniffing.

2. Give the details of file systems that different Operating System supports.

3. What do you understand be network tapping and port mirroring ?

4. Describe any three web application forensic tools.

5. What are the major sources of evidences in a mobile device ? Explain.

6. Describe the various steps of report preparation in detail.

7. How is registry information important in windows forensics ?

8. State major features of wireshark tool.

****