A–818

Total Pages : 3 **Roll No. .....**

MIT (CS)-202

(MCA/MSCCS)

(Digital Forensics)

3rd/2nd Semester Examination, 2024 (June)

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 the major sources of evidences in a mobile device ? Explain. 10

   (b) What are various steps involved in forensic readiness planning ? 9

2. (a) What are the components of a computer investigation toolkit ? 9

   (b) Explain the digital evidence investigation process in detail. 10

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

   (b) Define the terms the following :

      (i) Slack space

      (ii) Lost cluster

      (iii) Bad sector 6

   (c) State the usage and forensic importance of PsLoggedon, Netsessions, logonsessions tools. 10

4. (a) Describe the disk and file structure in a windows system. 10

   (b) State and explain various network components and their forensic importance. 8

5. (a) Describe web application forensic tools. 12

(b) What is first responder's toolkit ? What are the steps for preparing first responder's toolkit. 7

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. State major features of wireshark tool.
2. What do you mean by "shadow copy" of the World Wide Web and 'cloaked' URL ? Where does it take place ?
3. List and describe email attacks.
4. What is the role of a forensics investigator ?
5. What are the objectives of computer forensics ?
6. Why initial decision-making process is important ?
7. What is a file, system ? Why it is used ?
8. What is incident response ? Explain goal of incident response.

****