P-853

Total Pages : 3   Roll No. ....

MIT(CS)-202

Digital Forensics

(MCA/MSCCS/PGDCS)

3rd /2nd Semester Examination, 2023 (June)

Time : 2 Hours]   **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 answer to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

SECTION–A
(Long Answer Type Questions)

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.

(2×19=38)

1. Answer the following :

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

(b) Explain incident investigation methodology in details.

2. Answer the following :

(a) What is incident? Explain incident response methodology in detail.

(b) Explain volatile data collection procedure for windows system.

3. Answer the following :

(a) Explain importance of forensic duplication and its methods also list some duplication tools.

(b) Explain procedure to investigating routers.

4. Answer the following :

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

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

5. Write note on :

(i) Network file system.

(ii) Storage layer of file system.

SECTION–B
(Short Answer Type Questions)

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. (4×8=32)

1. State Locard's Principle.

2. Describe the disk and file structure in a windows system.

3. What is first responded's toolkit? What are the steps for preparing first responder's toolkit.

4. What do you understand by network tapping and port mirroring?

5. What is evidence? Explain the various types of digital evidence.

6. Explain data acquisition process in detail.

7. What are the different obstacles in evidence collections?

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