K–982

Total Page No. : 3] **[Roll No. .....**

MIT(CS)–202

MCA/MSCCS IIIrd/IInd Semester Examination Dec., 2023

DIGITAL FORENSICS

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 there in. ***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 different phases of investigation process? Explain with the help of a diagram. 8

(b) What is digital evidence ? What is its role in the investigation process ? Give examples of some common digital evidences. 8

(c) What is forensics readiness plan ? 3

2. (a) What do you mean by Application Forensics Readiness ? 7

(b) Explain various interfaces of HDD in detail. 6

(c) Give the details of file systems that different Operating System supports. 6

3. (a) How the deleted and lost files are recovered in a windows system ? 6

(b) What are the *five* types of password cracking methods ? 7

(c) What types of attacks are possible on wireless networks ? 6

4. (a) Describe the major amendments in the INDIAN IT Act (2008). Describe some offences and the corresponding penalties. 14

(b) Explain various types of mobile communications and relate this to forensic investigation. 5

5. (a) Describe the mobile forensic process. 10

(b) Describe the major types of web attacks in brief. 9

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 volatile data ? What is order of volatility of digital evidences ? Explain.
2. What are the four stages of computer forensic process ?
3. How are the network logs captured and analyzed ? Explain.
4. Explain the main features of ERD Commander.
5. How is registry information important in windows forensics ?
6. What are IDS and IDPS ?
7. What is network sniffing ? List some popular tools used for packet sniffing.
8. How do you detect wireless attacks ?

****