S-752

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

MIT(CS)-202

Digital Forenscis

(MCA/MSCCS/PGDCS)

3RD /2ND Semester, Examination 2022(Dec.)

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.

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 x 19 = 38]

P.T.O.

Q.1. Answer the following:

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

(b) What are the uses of computer forensics?

(c) Discuss various steps involved in forensic readlines planning?

Q.2. Answer the following:

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

(b) What are the different phases of investigation process? Explain with the help of a diagram.

Q.3. Answer the following:

(a) What is possible investigation phase carried out in data collection and analysis?

(b) How you will trace the crime which has been happened through email using tool?

Q.4. Answer the following:

(a) What are steps involved in computer evidence handling? Explain in detail?

(b) Explain procedure for recording cryptographic checksum of digital files and advantages of it.

Q.5. Write note on:

(a) NTFS disk

(b) Laws related to computer forensic

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 x 8 = 32]

Q.1. What is best evidence rule? Under what circumstances the duplicate copy of the digital evidence is admissible for lawful purposes?

Q.2. What are the various technical, legal and administrative issued faced by computer forensics?

Q.3. What is volatile data? What is order of volatility of digital evidences? Explain.

P.T.O.

Q.4. How are the network logs captured and analyzed? Explain.

Q.5. What is incident response? Explain goals of incident response.

Q.6. What is DOS attack? How to achieve recovery from DOS attack?

Q.7. Explain the Steps taken by Computer Forensics Specialist. Write three types of Computer Forensics Technologies also.

Q.8. Explain the term evidence? Explain types of evidences.

****