Total No. of Printed Pages : 6 Roll No.................

MIT (CS)-202/PGDCS-06

DIGITAL FORENSIC

Master of Science (Cyber Security)/P.G. Diploma in Cyber Security (MSCCS-18/PGDCS-17)

2nd Semester, Examination-2020

Time Allowed : 2 Hours Maximum Marks : 80

Note : This paper is of Eighty (80) marks divided into Two (02) sections A and B. Attempt the question 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 Twenty (20) marks each. Learners are required to answer any two (02) questions only. (2×20=40)

1. Answer the following : (4 marks each)

   (a) What is forensics readiness plan?

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

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

   (d) What is continuity of evidence?

   (e) What are the benefits of forensic readiness?

2. Answer the following : (4 marks each)

   (a) State Locard's Principle.

   (b) What are the essential characteristics of digital evidence?

   (c) What is chain of evidence and chain of custody? Explain.

(d) Explain the working of Hard Disk Drive.

(e) What is cyclic redundancy check (CRC)?

3. Answer the following :

(a) State and explain various network components and their forensic importance. 6

(b) How are the network logs captured and analyzed? Explain. 7

(c) What do you mean by Application Forensics Readiness ? 7

4. Answer the following :

(a) Describe the structure of SMTP messaging with a neat diagram. 6

(b) Which headers in SMTP useful in tracing a message sender identity? 7

(c) Write the steps involved in mobile acquisition. 7

5. Answer the following :

(a) What do you mean by net neutrality and open internet? 6

(b) Describe the various steps of report preparation in detail. 7

(c) What is volatile data? What is order of volatility of digital evidences? Explain. 7

Section-B

(Short answer type questions)

Note: Section-B Contains Eight (08) short answer type questions of Ten (10) marks each. Learners are required to answer any four (04) questions only. (4×10=40)

1. Explain the data acquisition process in detail.

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

3. Answer the following :

   (a) Describe the disk and file structure in a windows system. 5

   (b) How is registry information important in windows forensics? 5

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

5. How text messages be analyzed in forensics?

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

7. What are the important guidelines for forming an investigating team? Why initial decision-making process is important?

8. Define the terms :

(a) Slack space 3

(b) Lost cluster 4

(c) Bad sector. 4

****