Total pages : 04 Roll No. ....

MIT (CS)-202/PGDCS-06

Digital Forensic

(MSCCS-18/PGDCS-17)

Examination 2021 (Winter)

Time : 2 Hours **Max. Marks:80**

Note : This paper is of eighty (80) 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 Twenty (20) marks each. Learners are required to answer any two (02) questions only.

(2 x 20=40)

Q.1 Answer the following :

a. What is forensics readiness plan.(7 marks)

b. What are the benefits of forensic readiness? (4 marks)

c. What are various steps involved in forensic readiness planning? (6 marks)

d. What are the uses of computer forensics? (3 marks)

P.T.O.

Q.2 Answer the following :

a. Explain the digital evidence investigation process in detail. (7 marks)

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

c. What is volatile data? What is order of volatility of digital evidences? Explain. (6 marks)

Q.3 Answer the following :

a. Describe the major types of web attacks in brief. (10 marks)

b. Describe the Major tasks an investigator needs to do while performing web application forensics? (10 marks)

Q.4 Answer the following :

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

b. What is journaling? (4 marks)

c. What is booting? Explain the booting process of Window 7 in detail. (10 marks)

Q.5 Answer the following :

a. What are IDS and IDPS? (5 marks)

b. Describe the structure of SMTP messaging with a neat diagram. (8 marks)

c. How text messages be analyzed in forensics? (7 marks)

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 x 10=40)

Q.1 Answer the following :

a. What is computer forensics? Define. (3 marks)

b. What are the different phases of investigation process? Explain with the help of a diagram. (7 marks)

Q.2 What is digital evidence? What is its role in the investigation process? Give examples of some common digital evidences.

Q.3 What are the various technical, legal and administrative issues faced by computer forensics?

P.T.O.

Q.4 Answer the following : (5 marks each)

a. What is Hard Disk Drive? What are its main characteristics?

b. Explain various interfaces of HDD in detail.

Q.5 Answer the following :

a. What is a slack space, swap space and file carving? (6 marks)

b. How is registry information important in windows forensics? (4 marks)

Q.6 Answer the following :

a. What are the major sources of evidences in a mobile device? Explain. (5 marks)

b. Write the steps involved in mobile acquisition. (5 marks)

Q.7 Answer the following :

a. Describe the majore amedments in the INDIAN IT ACT (2008). Describe some offences and the corresponding penalties. (7 marks)

b. What do you mean by net neutrality and open internet? (3 marks)

Q.8 State the usage and forensic importance of Ps Loggedon, Netsessions, logonsessions tools.

****