Total No. of Pages : 06 Roll No. .....

PGDCS-06
Digital Forensic
PG Diploma in Cyber Security
(PGDCS-17)
2nd Semester
Examination, 2019

Time : **3** *Hours* *[Maximum 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 Fifteen (15) marks each. Learners are required to answer any three (03) questions only. **(3×15=45)**

1. Answer the following : (5 marks each)

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

   (b) What are the components of a computer

investigation toolkit ?

(c) What is best evidence rule? Under what circumstances the duplicate copy of the digital evidence is admissible for lawful purposes?

2. Answer the following :

   (a) List few examples of open source wireless Intrusion Detection Systems that are available for usage. (7 marks)

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

3. Answer the following :

   (a) What do you mean by Application Forensics Readiness? (4 marks)

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

   (c) Commission of cybercrime may be divided into how many groups? Describe them. (5 marks)

4. Answer the following :

   (a) What are the major sources of evidences in a mobile device? (4 marks)

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

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

5. Answer the following :

   (a) What do you mean by net neutrality and open Internet? (5 marks)

   (b) How is privacy a big issue in emailing. (5 marks)

   (c) State Locard's principle. (2 marks)

   (d) What is continuity of evidence ? (3 marks)

Section–B

(Short-Answer-Type Questions)

Note : Section 'B' contains Eight (08) short-answer-type questions of Seven (07) marks each. Learners are required to answer any Five (05)

questions only. **(5×7=35)**

1. Answer the following :

   (a) What are the four stages of computer forensic process? (3 marks)

   (b) What is forensics readiness plan? What are various steps involved in forensic readiness planning? (4 marks)

2. Answer the following :

   (a) Explain the data acquisition process in detail. (3 marks)

   (b) List all the important sections that should be included in the investigation report. (4 marks)

3. Answer the following :

   (a) What is volatile data? What is order of volatility of digital evidences? Explain. (3 marks)

   (b) What is first responder's toolkit? What are the steps for preparing first responder's toolkit. (4 marks)

4. Answer the following :

   (a) What is cyclic redundancy check (CRC)? (3 marks)

(b) What is booting? Explain the booting process of Window 7 in detail. (4 marks)

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

6. What are different types of File Systems? Explain in detail.

7. Answer the following :

   (a) What is a slack space, swap space and file carving? (3 marks)

   (b) Describe the disk and file structure in a windows system. (4 marks)

8. Answer the following :

   (a) Describe Windows Event Log File Format. (2 marks)

   (b) What are IDS and IDPS? (2 marks)

   (c) What do you understand be network tapping and port mirroring? (3 marks)