No. of Printed Pages : 5 **MSEI–027**

MASTER OF SCIENCE (INFORMATION SECURITY)/ P. G. DIPLOMA IN INFORMATION SECURITY (MSCIS/PGDIS)

Term-End Examination

December, 2023

MSEI-027 : DIGITAL FORENSICS

Time : 2 Hours *Maximum Marks : 50*

Note* : *Section–A : *Answer all the objective type questions.*

Section–B : *Answer all the very short answer type questions.*

Section–C : *Answer any* **two** *questions out of three short answer type questions.*

Section–D : *Answer any* **two** *questions out of three long answer type questions.*

Section—A

Note : *Attempt all the following questions.*

1. Which method uses stochastic properties of the computer system to investigate activities lacking digital artifacts ? 1

   (a) Steganography

   (b) Stochastic forensics

   (c) Both (a) and (b)

   (d) None of the above

2. How many C's are there in computer forensics ? 1

   (a) 1

   (b) 2

   (c) 3

   (d) 4

3. Which is not a type of data that is used in storage or mobile devices ? 1

   (a) Conceptual data

   (b) Address data

   (c) Logical data

   (d) Physical data

4. Data that is often used in Court or Judicial proceedings is : 1

   (a) Logical data

   (b) Physical data

   (c) Conceptual data

   (d) None of the above

5. In visual validation, the cell device's .... is used to validate the recovered files from a forensic tool. 1

   (a) GUI

   (b) CUI

   (c) Encase

   (d) Mobile screen

6. Digital evidence is only useful in a Court of law. 1

   (a) True

   (b) False

7. One of the most common approaches to validating forensic software is to : 1

   (a) Examine the source code

   (b) Ask others if the software is reliable

   (c) Compare results of multiple tools for discrepancies

   (d) None of the above

8. Examples of data that should be immediately preserved include : 1

   (a) USB drives

   (b) Digital picture frames

   (c) USB bracelets

   (d) System and network information

9. A forensic analysis conducted on a forensic duplicate of the system in question is referred to as : 1

   (a) Virtual analysis

   (b) Post-mortem analysis

   (c) Clone analysis

   (d) None of the above

10. Which of the following is a wireless protocol ? 1

    (a) 802.11b

    (b) 802.11x

    (c) HyperLANZ

    (d) All of the above

Section—B

Note : *Attempt all the questions.*

11. What is mobile forensic ? 2

12. Define phishing. 2

13. What is IP spoofing ? 2

14. What is digital evidence ? 2

15. What are forensic duplication tool requirements ? 2

Section—C

Note : *Attempt any* ***two*** *out of three short answer type questions.*

16. Why do we need computer forensic tools ? 5

17. Explain the evolution of computer forensic tool. 5

18. Explain the history of digital forensic fields. 5

Section—D

Note : *Attempt any* ***two*** *out of three long type questions.*

19. Explain in detail the task of hardware forensic tool. 10

20. Explain the line data collection process in detail. 10

21. What is intrusion detection ? Explain the attacks on network and the prevention from attacks in detail. 10