No. of Printed Pages : 4

MSEI-027

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

Term-End Examination

June, 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** out of three long answer type questions.*

Section—A

***Note* :** Attempt all the following questions. 1 each

1. Computer forensics is also known as ..... .
   (a) Digital forensic science
   (b) Computer crime
   (c) Computer forensic science
   (d) None of the above

2. Which of the following techniques are used during computer forensic investigations ?
   (a) Cross-drive analysis
   (b) Line analysis
   (c) Deleted files
   (d) All of the above

3. CDRs in mobile forensic stands for ..... .
   (a) Call details records
   (b) Compact disk rewritable
   (c) Compact disk readers
   (d) Call data records

4. In mobile forensic, visual validation means ..... .
   (a) The examiner checks for physical damage signs and validate it with a recovered evidence report by the collected officer.
   (b) The examiner uses the GUI of the mobile device to confirm the findings from the forensic tool.
   (c) Both (a) and (b)
   (d) None of the above

5. You are supposed to maintain three types of records. Which answer is not a record ?
   (a) Chain of custody
   (b) Documentation of the crime scene
   (c) Searching the crime scene
   (d) Document your actions

6. What is the full form of SOP in cell device forensic ?
   (a) Standard Operating Procedure
   (b) Standard of Preservation
   (c) Safety Operational Procedure
   (d) Set Operational Procedure

7. Video Surveillance can be a form of digital evidence.
   (a) True
   (b) False

8. Forensic examination is the process of extracting, viewing and analyzing information from the evidence collected.
   (a) True
   (b) False

9. It is unwise to rely on a recovered IP address because :
   (a) An IP address may change many times during a session
   (b) Offenders can change their IP address
   (c) IP addresses only exist in system memory
   (d) None of the above

10. Which of the following are layer 7 protocols ?
   (a) Ethernet
   (b) HTTP
   (c) TCP
   (d) All of the above

Section—B

Note : Attempt all the following questions. 2 each

11. What is digital forensic ?
12. Define the cyber stalking.
13. Discuss moneylaundering.
14. How many types of computer forensic tools are there ?
15. What are the challenges in evidence handling ?

Section—C

Note : Attempt any ***two*** out of three short answer type questions. 5 each

16. Discuss DNS spoofing in detail.
17. Discuss the different types of banking financial crimes.
18. Explain the various types of evidence and rules of evidence.

Section—D

Note : Attempt any ***two*** out of three long answer type questions. 10 each

19. Explain the computer frauds in India in detail.
20. Explain the incidence response methodology in detail.
21. What is forensic duplication ? Why is it needed ? How do you create forensic duplication of hard drive ?