No. of Printed Pages : 5 **MSEI-027**

P. G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 2020

MSEI-027 : DIGITAL FORENSICS

Time : 2 Hours *Maximum Marks : 50*

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

Section B : *Answer all the very short answer 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

(Objective Type Questions)

Note : *Attempt all questions.*

1. The first step in a digital forensic process is 1

2. When performing a forensic analysis, what device is used to prevent the system from recording data on an evidence disk ? 1

   (a) Write-Blocker

   (b) Protocol analyzer

   (c) Firewall

   (d) Disk Editor

3. .... is a collection of infected computers or bots that been taken by hackers and are used to perform malicious tasks or functions. 1

4. .... is a digital object that contains reliable information that supports or refutes a hypothesis. 1

5. .... is a programming instructions that are complied into the executable files that are sold by software development companies. 1

6. GSM stands for 1

7. .... is the international or uniternational use of a portable USB mass storage device to illicitly download confidential data from a network endpoint. 1

8. Whenever a system is compromised, there is almost always something left behind by the attacker be it code fragments, trojan programmes, running processes, or sniffer log files. These are known as 1

9. .... is "an information resource whose value lies in unauthorized or illicit use of that resource". 1

10. TFTP stands for 1

Section—B

(Very Short Answer Questions)

***Note :** Attempt all questions.*

11. Explain the advantages of wireless devices. 2

12. Explain the purpose of SHA algorithm. 2

13. Explain the purpose of CAPTCHA. 2

14. Which IT Amendment Act, 2008 Section is applicable for Data theft from Removable Drives ? Suggestions to prevent data theft. 2

15. What is 802.11 Standard ? 2

Section—C

(Short Answer Type Questions)

***Note :** Attempt any two questions.*

16. Explain the different parameters of Log File Analysis. 5

17. Explain the wireless point security standards. 5

18. Explain the purpose of CDR Analysis while investigations. 5

Section—D

(Long Answer Type Questions)

***Note :** Attempt any two questions.*

19. Explain the modes of operation in wireless communications and different categories of WLAN. 10

20. How to implement the file attributes analysis ? What is the process to reconstruct deleted files ? 10

21. What is the difference between dead acquisition, live acquisition and error handling ? 10

1380