No. of Printed Pages : **4**

MSEI-027

00022

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

December, 2016

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note : *(i)* ***Section A*** *- Answer* ***all*** *the objective type questions.*

(ii) ***Section B*** *- Answer* ***all*** *the very short answer type questions.*

(iii) ***Section C*** *- Answer* ***any two*** *out of* ***three*** *short answer type questions.*

(iv) ***Section D*** *- Answer* ***any two*** *out of* ***three*** *long answer type questions.*

SECTION - A

(Attempt **all** the questions.)

1. PDA stands for : **1**

(a) Personal Digital Assistant

(b) Personal Digital Admin.

(c) Personal Digital Admission

(d) None of these

2. A Multi-Media Card (MMC) is a solid state disk card with _____ number of pins connector. **1**

3. Class 1 Bluetooth devices have the range of _____ metres. **1**

4. GPRS stands for : 1

(a) General Packet Radio Server

(b) General Packet Radio Service

(c) General Package Radio Server

(d) None of these

5. _____ is the collection of infected computers or bots that have been taken over by hackers. 1

6. EDGE stands for Enhanced Data Rate for GSM Evolution. 1

(a) True (b) False

7. The full form of FIFO is _____. 1

8. _____ is the full form of BIOS. 1

9. "SSIDS" stands for _____. 1

10. "TFTP" stands for _____. 1

SECTION - B

(5 very short answer type questions)

(Attempt all the questions)

11. What is volatile evidence ? 2

12. Write a short note on freezing the scene. 2

13. What is honey potting ? 2

14. Give any two differences between E-mail Spamming and E-mail Bombing. 2

15. Which one is more ideal-dead analysis or live analysis and why ? 2

SECTION - C

(Attempt **2** out of **3** short answer type questions)

16. What are the legal issues involved in seizure of the computer equipment ? Explain the principal of Computer - Based Evidence. 5

17. Explain the major characteristics of financial crimes. 5

18. Explain any two tools used in "Forensics Examination of Mobile Devices". 5

SECTION - D

(Attempt **2** out of **3** long questions)

19. What is Digitized document forensic ? In computer investigation how the printout can be investigated and how the investigator come to know about the printer and from which the print had been taken. 10

20. What are the items that need to be considered for conducting an effective investigation for cyber crime ? 10

21. Write a short note on the following : 10

(a) SNMP

(b) Root - kits

(c) Data theft

(d) Cloning in forensic analysis