No. of Printed Pages : 4

MSEI-027

00801

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June, 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. FTC stands for _____. **1**

(a) Federal Trade Commission

(b) Federal Trade Commissioner

(c) Federal Trade Command

(d) None of these

2. RSA is _____ key cryptosystem. **1**

3. DDOS stands for _____. **1**

4. A _____ attacker entices computer to log into a computer, which is set up as an AP (Access Point). 1

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

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

7. _____ is a computer program that can copy itself and infect a computer. 1

8. An _____ is a form of internet text messaging or synchronous conferencing. 1

9. WAP stands for Wired Application Protocol : 1

   (a) True

   (b) False

10. "PGP" stands for _____. 1

SECTION - B

Very short type of questions.

(Attempt **all** the questions.)

11. What is Spoofing ? 2

12. What is 'Identity theft' ? Define types of data theft. 2

13. What is exculpatory evidence ? 2

14. Differentiate "copy of the drive" and "imaging of the drive". 2

15. What are three major phases of Digital Forensics ? 2

SECTION - C

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

16. What is Money laundering ? 5

17. Explain the advantages and disadvantages of software based firewall and hardware based firewall. 5

18. What are some initial assessment you should make for a computing investigation ? 5

SECTION - D

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

19. Explain "Log File Analysis". What is "File Carving" in Data recovery ? What is salvaging of data ? **10**

20. What is Intrusion Detection System ? How does it different from firewall ? Define IPS. **10**

21. Write a short note on the following : **10**

(a) Cyber bullying

(b) SIM Card Acquisition

(c) Cyber Terrorism

(d) Admissible Evidence

(e) Logic Bomb