

**P.G. DIPLOMA IN INFORMATION SECURITY
(PGDIS)**

Term-End Examination

01272

December, 2012

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 questions.

SECTION - A

(Attempt all the questions)

1. WPA stands for _____. 1
- (a) Wi-Fi Protected Access
 - (b) Wi-Fi Protected Antenna
 - (c) Wi-Fi Protected Area
 - (d) Wi-Fi Protected Architecture
2. http stands for "hyper text technical protocol". 1
- (a) True
 - (b) False

3. _____ Stands for TCP. 1
4. DDoS Stands for _____. 1
5. The simulation is clearly related to a _____ attack as it targets the organization's equipment. 1
6. Area of investigation also need service of _____ to collect, analysis, and present computer based information so that it is suitable for use as evidence in court of lab. 1
7. GSM Stands for _____. 1
8. A _____ attacker entices computer to log into a computer, which is set up as a AP (Access Point). 1
9. In an _____, connections are made spontaneously such that a connection is made from the transmitting device to the receiver. 1
10. SSID Stands for _____. 1

SECTION - B

(5 very short answer type questions)

(Attempt all the questions)

11. Give any two difference between E-Mail Spaming and E-Mail Bombing. 2

OR

Define Data theft.

12. What is Electronic tempering ? 2

13. Define Identity theft. Define types of data theft. 2

14. Define Active and Passive Reconnaissance in Hacking. 2

15. Explain the use of IEEE 802.16. 2

SECTION - C

(Attempt 2 out of 3 short answer type questions)

16. Explain the advantages and disadvantages of software based firewall and hardware based firewall. 5
17. Define file Carving and Radius Server with examples. 5
18. Name two types of wireless securities. Explain the term logs and logging in collecting and Archiving. 5

SECTION - D

(Attempt 2 out of 3 long questions)

19. What is a log file analysis ? What is data theft ? 10
Define Ad-hoc network.
20. What is Intrusion Detection System ? How does 10
it different from firewall ? Define IPS.
21. Write a short note on the following : 5x2=10
- (a) Firewall
 - (b) Routers
 - (c) Logic bomb
 - (d) SNMP
 - (e) 802.11b, 802.11g wifi 2.
-