

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

Term-End Examination

December, 2017

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours

Maximum Marks : 50

- Note :**
- (i) **Section 'A'** - Answer all the objective questions.
 - (ii) **Section 'B'** - Answer all the very short answer questions.
 - (iii) **Section 'C'** - Answer any two questions 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. SHA stands for _____ 1
2. IMEI stands for _____ 1
3. PUK stands for _____ 1
4. GPRS stands for _____ 1
5. UDP Protocol also use 3 ways Handshake for connection establishment. (True/False) 1
6. What is the latest file system used in LINUX 64 bit OS ? 1

7. MAC address defined in NIC Chipset. (True/False) 1
8. _____ Command, commonly use in Linux to create hard disk image. 1
9. ICMP Protocol use behind _____ Command. 1
10. _____ bits size for IPV6 Protocol. 1

SECTION - B

(5 Very short answer questions)

(Attempt all questions)

11. Define Cyber Bullying and Cyber Terrorism. 2
12. Define Botnets and E-mail Spams. 2
13. Define Boot Loaders with examples. 2
14. Explain the image file format. Explain embedded image. 2
15. Explain Ad hoc mode of operation. 2

SECTION - C

(Attempt 2 out of 3 short answer type questions)

16. What are the Artifacts of Cyber forensics ? What are the Artifacts collection steps generally used ? 5
17. What is the difference between Logical Data Acquisition and Physical Data Acquisition ? 5
18. What is the process of LOG File Analysis ? How to Reconstruct Deleted Files ? 5

SECTION - D

(Attempt 2 out of 3 long answer type questions)

19. What is the difference between WiFi 802.11b, 802.11g and 802.11n series ? 10
 20. Explain any 5 Email and IRC related Crimes. 10
 21. What do you mean by steganography ? Explain in detail. What are Symmetric and Asymmetric types ? 10
-