

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

**Term-End Examination**

**December, 2021**

**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** questions out of three long answer type questions.*

---

---

**SECTION A**

*Attempt **all** the questions.*

1. PUK stands for \_\_\_\_\_ . 1
2. USB drive uses \_\_\_\_\_ memory. 1
3. \_\_\_\_\_ is a computer program that can copy itself and infect a computer. 1

4. The full form of FIFO is \_\_\_\_\_ . 1
5. TCP/IP Protocol is used behind ping command. 1  
(a) True  
(b) False
6. UDP Protocol uses 3-way handshake for connection establishment. 1  
(a) True  
(b) False
7. A \_\_\_\_\_ attacker entices computers to log into a computer, which is set up as an AP (Access Point). 1
8. TFTP stands for \_\_\_\_\_ . 1
9. IMAP stands for \_\_\_\_\_ . 1
10. IMEI stands for \_\_\_\_\_ . 1

## SECTION B

*Attempt **all** the questions.*

- |  |   |
|--|---|
| 11. Explain Cloud Forensic.                    | 2 |
| 12. Define Exculpatory Evidence.               | 2 |
| 13. What do you mean by 'freezing the scene' ? | 2 |
| 14. Explain Seizure.                           | 2 |
| 15. Explain Boot Loaders.                      | 2 |

## SECTION C

*Attempt **two** out of three short answer type questions.*

- |   |   |
|---|---|
| 16. Describe any digital forensic investigation model.            | 5 |
| 17. Describe software-based firewall and hardware-based firewall. | 5 |
| 18. What are the major characteristics of financial crimes ?      | 5 |

## SECTION D

Attempt **two** out of three long answer type questions.

- 19.** Explain in detail any four E-mail and IRC related crimes. 10
- 21.** Describe the classification of CFCC (Cyber Fraud and Cyber Crime). What are the pre-search preparations required for a forensic investigation case ? 10
- 22.** What is “Log File Analysis” ? What is “File Carving” in data recovery ? What is Salvaging of data ? 10
-