

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

Term-End Examination,

December 2019

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

Section - A

Attempt all the questions.

1. Ubuntu is also _____. 1
2. WAP stands for Wired Application protocol 1
 - a) True
 - b) False
3. EDGE stands for enhanced Data Rate for GSM Environment. 1
 - a) True
 - b) False

(2)

4. HTTP stands for "Hyper Text Technical Protocol" 1
a) True
b) False
5. TCP/IP protocol used behind ping command 1
a) True
b) False
6. "TFTP" stands for _____. 1
7. DDOS stands for _____. 1
8. "SSIDs" stands for _____. 1
9. PDA stands for _____. 1
10. The name of Website containing periodic posts _____. 1

Section - B

(Five very short answer type questions)

Attempt all questions.

11. What is CDR? How it helps for Investigation? 2
12. Explain the difference between "Line acquisition" and "Post mortem acquisition". 2
13. What is CoC (Chain of Custody)? 2
14. What are the different formats for digital evidence? 2
15. Explain Salvaging of data. 2

(3)

Section - C

(Attempt **two** out of **three** short answer type questions)

16. What are the legal issues involved in seizure of the computer equipment? 5
17. What is IMEI? Why it is used in Mobile phone devices? How it is helpful in forensic investigation? 5
18. Explain any two tools used in "Forensic examination of Mobile devices". 5

Section - D

(Attempt **two** out of **three** long answer type questions)

19. What is the general process for conducting a digital investigation? 10
20. What are the counterfeit documents? What are the steps involved in detection of counterfeit document? Give a brief note on the duties performed by the examiner. 10
21. Write short notes on the following: 5×2=10
- a) Harassment
 - b) Admissible evidence
 - c) SIM card acquisition
 - d) Cyber bullying
 - e) Human trafficking

