No. of Printed Pages : 4

MSEI-027

01312

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

December, 2018

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. _____ is the full form of BIOS. 1

2. Computer forensics involves all of the following started activities except : 1
   (a) manipulation of computer data.
   (b) extraction of computer data.
   (c) interpretation of computer data.
   (d) preservation of computer data.

3. A drive is prepared in three processes. This processes include all of the following except : 1
   (a) high-level formatting
   (b) low-level formatting
   (c) formatting
   (d) partitioning

4. All of the following are examples of real security and privacy risks except : 1

(a) hackers (b) spam
(c) viruses (d) identity theft

5. Which of the following is NOT one of the four major data processing functions of a computer ? 1

(a) gathering data
(b) processing data into information
(c) analyzing the data or information
(d) storing the data or information

6. Computer gather data, which means that they allow users to _____ data. 1

7. As a good forensic practice, why would it be a good idea to wipe a forensic drive before using it ? 1

(a) Chain of custody
(b) No need to wipe
(c) Different file and Operating systems
(d) Cross-contamination

8. Which duplication method produces an exact replica of the original drive ? 1

(a) Bit-Stream Copy (b) Image Copy
(c) Mirror Copy (d) Drive Image

9. The binary language consists of two digits : _____ and _____. 1

10. Output devices store instructions or data that the CPU processes. 1

(a) True (b) False

SECTION - B

(5 very short answer type questions)

(Attempt **all** questions)

11. Once you format your hard drive, does it erase everything or can information still be retrieved. 2

12. Explain the difference between "live acquistion"and "post mortem acquisition". 2

13. What is CoC (Chain of Custody) and why is it important for evidence integrity ? 2

14. What are the different formats for digital evidence ? 2

15. What are the components of disk drives ? 2

SECTION - C

(Attempt 2 out of 3 Short answer type questions)

16. How can deleted data be retrieved from a PC ? How it is possible to know what Internet sites have been visited ? 5

17. State and explain the general tasks that the investigators perform when working with digital evidence. 5

18. Describe procedures for acquiring data from cell phones and mobile devices. 5

SECTION - D

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

19. What are the items that need to be considered for conducting an effective investigation for Cyber Crime ? **10**

20. What is Intrusion Detection System ? How it is different from fire wall ? **10**

21. Write Short note on the following : **2.5x4=10**
    (a) Logic Bomb
    (b) Admissible Evidence
    (c) Roof-kits
    (d) Hacking