No. of Printed Pages : 4 MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

01423

Term-End Examination

June, 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. What is the most significant legal issue in computer forensic ? 1
   - (a) Preserving Evidence
   - (b) Seizing Evidence
   - (c) Admissibility of Evidence
   - (d) Discovery of Evidence

2. When a file is deleted ? 1
   - (a) The file remains intact.
   - (b) The FAT entry for the file is zeroed out so it shows that the area is available for use by a new file.
   - (c) The first character of the directory entry file name is changed to a special character.
   - (d) All of the above.

3. Which of the following is not a property of computer evidence ? 1

(a) Authentic and Accurate

(b) Complete and convincing

(c) Duplicated and preserved

(d) Conform and Human Readable

4. __________ is the science of hiding messages in messages. 1

(a) Scanning

(b) Spoofing

(c) Steganography

(d) None

5. When shutting down a computer, what information typically lost ? 1

(a) Data in RAM memory

(b) Running Processes

(c) Current network connections

(d) All of the above

6. USB drives use __________. 1

(a) RAM memory

(b) Cache memory

(c) Flash memory

(d) None of the above

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 system

(d) Cross-contamination

8. Which of the following is an example of input device ? 1

(a) Scanner
(b) Speaker
(c) CD
(d) Printer

9. The operating system is the most common type of __________ software. 1

(a) Communication
(b) Application
(c) System
(d) Word-processing software

10. __________ are computers that excel at executing many different computer programs at the same time. 1

SECTION - B

(5 Very short answer type questions)
(Attempt **all** questions)

11. What are the techniques for obtaining and exploiting personal information for identity theft ? 2

12. What are the three major phases of Digital forensic ? 2

13. Differentiate "copy of the drive" and "imaging of the drive". 2

14. Define Active and Passive Reconnaissance in Hacking. 2

15. Define windows registry. Why it is important in forensic ? 2

SECTION - C

(Attempt **2** out of **3** short answer type questions)

16. What are some initial assessment you should make for a computing investigation ? **5**

17. How forensic analysis is done on windows and mobile devices ? **5**

18. What is data acquisition and duplication ? Give a brief description of data acquisition tools. **5**

SECTION - D

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

19. Explain the classification of CFCC (Cyber Fraud and Cyber Crime). What are the pre-search preparation required for the forensic investigation case ? **10**

20. What are the counterfeit documents ? What are steps involved in detectional counterfeit documents ? Give a brief note on the duties performed by the examiner. Also discuss the elements of a forensic report. **10**

21. Write short notes on the following : (**any four**)

(a) Cyber terrorism **2.5x4=10**

(b) Forensic Auditing

(c) Logic bomb

(d) Cyber bullying

(e) Identity theft