No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

00702

Term-End Examination

December, 2015

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 questions.*

(iv) ***Section 'D'***- *Answer* ***any two*** *out of* ***three*** *long questions.*

SECTION - A

(Attempt **all** the questions)

1. In General, _____ involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve data. **1**

2. In microsoft file structure, sectors are rounded together to form _____. **1**

3. The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity. **1**

4. _____ field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death. 1

5. In a computer forensic investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court ? 1

   (a) Rules of evidence.

   (b) Law of probability.

   (c) Chain of custody.

   (d) Policy of separation.

6. When examining a file with a Hex Editor, what space does the file header occupy ? 1

   (a) The last several bytes of the file.

   (b) The first several bytes of the file.

   (c) None, file header are contained in the FAT.

   (d) One byte at the beginning of the file.

7. What does the acronym POST mean as it relates to a Pc ? 1

   (a) Primary Operations Short Test.

   (b) Power On Self Test.

   (c) Pre Operational Situation Test.

   (d) Primary Operating System Test.

8. To preserve digital evidence, an investigator should _____. 1

(a) Make two copies of each evidence item using a single imaging tool.

(b) Make a single copy of each evidence item using an approved imaging tool.

(c) Make two copies of each evidence item using different imaging tools.

(d) Only store the original evidence item.

9. http stands for "hyper text transfer protocol". 1

(a) True (b) False

10. DDoS stands for _____. 1

SECTION - B

(5 very short answer questions)

(Attempt **all** questions)

11. What is cloning in forensic analysis ? 2

12. What is admissible evidence ? 2

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

14. What is Logic Bomb ? 2

15. What is cloud forensic ? 2

SECTION - C

(Attempt **2** out of **3** short answer type questions) **5**

16. Explain the principles of Computer - Based Evidence.

17. What are legal issues involved in seizure of the computer equipment ? **5**

18. Explain any digital forensic investigation model. **5**

SECTION - D

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

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

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

21. Write a short note on the following : **5x2=10**

(a) Firewall.

(b) Hacking.

(c) Electronic tempering.

(d) Logic bomb.

(e) IEEE 802.16.