No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

00951

Term-End Examination

June, 2015

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 questions.*

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

SECTION - A

(Attempt **all** the questions)

1. Which Intrusion Detection System (IDS) usually provide the most false alarm due to unpredictable behaviors of users and networks ? 1

   (a) Network based IDS system (NIDS)
   (b) Host based IDS system (HIDS)
   (c) Anomaly Detection
   (d) Signature recognition

2. _____ refers to the unauthorized entry into a computer system. 1

3. _____ is the science of acquiring, preserving, retrieving and presenting data that has been processed electronically and stored on computer media. 1

4. The first step in a digital Forensics process is _____. 1

5. GSM stands for _____. 1

6. Ubuntu is a(n) _____. 1

7. _____ is the use of the internet or the other electronic means to stalk or harass an individual, a group of individual, or an organization. 1

8. The name of website containing periodic posts_____. 1

9. When examining hard disk without a write-blocker, you should not start windows because windows will write data to the : 1
   (a) Recycle Bin
   (b) Case files
   (c) BIOS
   (d) MSDOS. sys

10. When performing a forensic analysis, what device is used to prevent the system from recording data on an evidence disk ? 1
   (a) Write-blocker
   (b) Protocal Analyzer
   (c) Firewall
   (d) Disk Editor

SECTION - B

(5 very short answer questions)
(Attempt **all** questions)

11. What is electronic tempering ? **2**

12. Define Active and Passive Reconnaissance in Hacking. **2**

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

14. What is firewall ? **2**

15. What is cloud forensic ? **2**

SECTION - C

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

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

17. Explain Daubert Guideline. Why these guidelines helpful in the digital forensic investigation. **5**

18. What is IMEI ? Why it is used in mobile phone devices ? How it is helpful in forensic investigation ? **5**

SECTION - D

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

19. Discuss the levels of analysis for data acquisition from mobiles phones. **10**

20. How digital evidence is processed ? What are the steps involved in Evidence Acquisition ? Explain with the help of hypothetical case. **10**

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

(a) Hacking

(b) Cloning in forensic analysis

(c) Digital Evidence

(d) Admissible Evidence

(e) Logic Bomb