No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

01254

June, 2019

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note :

*Section A – Answer **all** the objective type questions.*

*Section B – Answer **all** the very short answer type questions.*

*Section C – Answer any **two** questions out of three short answer type questions.*

*Section D – Answer any **two** questions out of three long answer type questions.*

SECTION A

*Attempt **all** the questions.*

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

2. The first step in a digital forensic process is _____. *1*

3. The name of website containing periodic posts is _____. *1*

4. _____ is the collection of infected computers or bots that have been taken over by hackers. *1*

5. A _____ attacker entices computer to log into a computer, which is set up as an AP (Access Point). *1*

6. SSID stands for _____. *1*

7. SNMP stands for _____. *1*

8. IMAP stands for _____. *1*

9. In Microsoft file structure, sectors are rounded together to form _____. *1*

10. _____ is the full form of BIOS. *1*

SECTION B

*Answer all **five** very short answer type questions.*

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

12. What is File carving and Bluesnarfing ? *2*

13. What is the difference between "copy of the drive" and "imaging of the drive" ? *2*

14. What is electronic tampering ? *2*

15. Define Windows Registry. Why is it important for forensics ? *2*

SECTION C

*Answer any **two** questions out of three short answer type questions.*

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

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

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

SECTION D

*Answer any **two** questions out of three long answer type questions.*

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

20. What is the difference between WiFi and WiMax ? Specify their standards, technical characteristics and security policies. *10*

21. What are the issues involved with detection of cyber-crimes in India ? *10*