No. of Printed Pages : 4

MSEI-027

P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

00904

December, 2014

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 following questions. *10×1=10*

1. _____ is one where the suspect operating system is still running and being used to copy data. *1*

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

3. An _____ is a form of Internet text messaging or synchronous conferencing. *1*

4. _____ is "an information resource whose value lies in unauthorized or illicit use of that resource". *1*

5. The _____ is an online publication devoted to discussions of the theory and practice of handling digital evidence. *1*

6. Whenever a system is compromised, there is almost always something left behind by the attacker be it code fragments, trojaned programs, running processes, or sniffer log files. These are known as _____ . *1*

7. The _____ is a non-profit organisation that is dedicated to educating law enforcement professionals in the area of computer forensics. *1*

8. _____ is the intentional or unintentional use of a portable USB mass storage device to illicitly download confidential data from a network endpoint. *1*

9. A _____ is a process where we develop and test hypotheses that answer questions about digital events. *1*

10. The field of _____ involves identifying, extracting, documenting and preserving information that is stored or transmitted in electronic or magnetic form. *1*

SECTION B

Answer all 5 very short answer type questions. *5×2=10*

11. Define types of data theft. *2*

12. Why is spam so prevalent on the Internet ? *2*

13. Which one is more ideal – dead analysis or live analysis and why ? *2*

14. What is volatile evidence ? *2*

15. What are the three major phases of Digital forensics ? *2*

SECTION C

Answer any 2 questions out of 3 short answer type questions. *2×5=10*

16. Write short notes on the following : $2\frac{1}{2} \times 2 = 5$

(a) Cyber bullying

(b) Data theft

17. Explain the major characteristics of white collar economic crimes. *5*

18. Explain the background of botnets. *5*

SECTION D

Answer any 2 questions out of 3 long answer type questions. *2×10=20*

19. Cyber crime is a rapidly growing field and problem area for law enforcing agencies. Do you agree ? Explain in detail. *10*

20. What are the items that need to be considered for conducting an effective investigation for cyber crime ? *10*

21. Explain the five rules of collecting electronic evidence in detail. *10*