P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

00982

Term-End Examination

June, 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 out of three long questions.*

SECTION - A
(Attempt all the questions)

1.   A _____ occurs when the data from a suspect system is being copied without the assistance of the suspect operating system.   **1**

2.   The full form of FIFO is _____ .   **1**

3.   _____ is a collection of infected computers or bots that have been taken over by hackers and are used to perform malicious tasks or functions.   **1**

4.   Regular auditing and accounting of your system is useful not only for detecting intruders but also as a form of _____ .   **1**

5. _____ is a windows - based acquisition and   1
   analysis tool that comes in both local and
   network - based versions.

6. _____ is any evidence presented by a person   1
   who was not a direct witness.

7. The _____ was established in 1995 to provide   1
   a forum for law enforcement agencies across the
   world to exchange information about computer
   forensics issues.

8. _____ is a digital object that contains reliable   1
   information that supports or refutes a hypothesis.

9. _____ is the use of electronic messaging   1
   systems to send unsolicited bulk messages
   indiscriminately.

10. _____ is the programming instructions that   1
   are compiled into the executable files that are sold
   by software development companies.

SECTION - B
(5 very short answer type questions)
(Attempt **all** the questions)

11. What is electronic tempering ?   2

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

13. Explain the types of Spam.   2

14. What is exculpatory evidence ?   2

15. What are the two basic forms of collection ?   2

SECTION - C

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

16. Write short notes on :   2.5x2=5
    (a) Cyber terrorism
    (b) Identity theft

17. Explain the major characteristics of financial   5
    crimes.

18. Electronic crime is difficult to investigate and   5
    prosecute. Elaborate this statement.

SECTION - D

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

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

20. You are working as a investigator for looking over   **10**
    the intellectual properties policies of the company
    "XYZ Ltd" and to check for the violations, if any.
    How you will plan your investigation and what
    are the main questions which you will ask the
    company and its employees ?

21. Forensic analysis of digital evidence depends on   **10**
    the case context and largely relies on the
    knowledge, experience, expertise, thoroughness
    and in some cases the curiosity of the practioner
    performing the work. Do you agree ? Explain
    the underlying process of forensic analysis in
    detail.

_____