Seat No: _____ **Enrollment No: _____**

PARUL UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

B.Tech. Summer 2018 - 19 Examination

Semester: 8 **Date: 1/05/2019**
Subject Code: 03105481 **Time: 10:30am to 1:00pm**
Subject Name: Cyber Forensics **Total Marks: 60**

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Make suitable assumptions wherever necessary.
4. Start new question on new page.

Q.1 **Objective Type Questions** – (Fill in the blanks, one word answer, MCQ-not more than Five in case of MCQ) (All are compulsory) (Each of one mark) **(15)**

1._____ is a fairly easy task in computer forensics analysis.
2. Validate your tools and verify your evidence with _____ to ensure integrity.
3.Email messages are distributed from one central server to many connected client computers, a configuration called _____
4. On older Macintosh OSs, all information about the volume is stored in the _____.

5. Linux is unique in that it uses _____, that contains descriptive information about each file and directory.

6._____ is the art of hiding information inside image files.

7. Data _____ involves changing or manipulating a file to conceal information.
8._____ are handy when you need to image the drive of a computer far away from your location or when you don't want a suspect to be aware of an ongoing investigation.
9._____ is an independent malicious program that needs not any host program.
10. _____ is a code injection attack that allows the attacker to execute malicious JavaScript in another user's browser.
11. _____ can help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program.

a) Broadcast Forensics b) Computer Forensics
c) Network Forensics d) Traffic Forensics

12. You begin any computer forensics case by creating an_____

a) Investigation plan b) Evidence custody form
c) Risk Assessment Report d) Investigation Report

13. _____ are devices and/or software placed on a network to monitor traffic

a) Packet Sniffers b) Hubs
c) Bridges d) Honeypots

14.Marking bad clusters data hiding techniques are called is more common with _____ file systems.

a) NTFS b) HFS
c) FAT d) Ext2fs

15.The files that provide helpful information to an email investigation are log files and _____ files.

a) batch b) scripts
c) configuration d) .rts

Q.2 Answer the following questions. (Attempt any three) **(15)**

A) What is an incident? Explain Incident response methodology in detail with diagrammatic representation.
B) Describe about the file system structure of various computer systems.
C) Write about window registry in detail.
D)What are the tools used for analyzing a computer if any challenge has raised?

Q.3 A) What are the various techniques used for hiding of data in system investigation? Explain the methods involved in these processes. **(07)**

B) How can you differentiate with forensics investigation of network with that of mobile devices. **(08)**

OR

B) Explain the role of Email in investigation for evidences. **(08)**

Q.4 A) what is ethical hacking? Describe the various steps used by an ethical hacker to understand the loopholes of the system. **(07)**

OR

A) Explain about hijacking of session and various techniques for hacking web servers. **(07)**

B) Write in detail about SQL injection with quoting examples from real life experiences. **(08)**