Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – III • EXAMINATION – WINTER • 2013

Subject code: 735101 **Date: 28-11-2013**

Subject Name: Cyber Forensics

Time: 10.30 am – 01.00 pm **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q. No. 1

a. Explain Antiforensics, with appropriate example. [7 Marks]
b. Draw & explain Flow chart for Digital crime investigations under ITAA 2008. [7 Marks]

Q. No. 2

a. Simulate Phishing attack and investigate the phishing case. [7 Marks]
b. Discuss Email based crime investigation scenario.
Hint: Take any Email based crime; simulate the crime, how it is done and what are the investigation steps need to perform to detect the crime. [7 Marks]

Q. No. 3

a. Write & explain Classification of Cyber Forensics. [7 Marks]
b. Explain the Steps should be followed in Crime Scene Investigation. [7 Marks]

Q. No. 4

a. Write a technical note on Forensic Duplication. [7 Marks]
b. Write the difference between Mobile Phone's Logical Acquisition & Physical Acquisition. [7 Marks]

Q. No. 5

a. Explain briefly on Network drive imaging & Logical File collection. [7 Marks]
b. Differentiate with appropriate example - Forensics of Cloud and Forensics using Cloud. [7 Marks]

Q. No. 6

a. Write & explain about Digital Forensics Investigation Methods. [7 Marks]
b. What is Malware? Write types of malware. How antivirus identifies the malware? [7 Marks]

Q. No. 7

a. What do you mean by Steganography? Explain about Steganography detection. [7 Marks]
b. Explain the basics steps should have to follow for the Digital Forensics process. [7 Marks]

Q. No. 8

a. What do you mean by Spoofing? How to investigate IP & MAC spoofing attack. [7 Marks]
b. What do you mean by data confidentiality? Explain the advantages. [7 Marks]

****