Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – III • EXAMINATION – WINTER 2012

Subject code: 735101 Date: 30-12-2012

Subject Name: Cyber Forensics

Time: 10.30 am – 01.00 pm Total Marks: 70

Instructions:

1. **Attempt question 1, which is compulsory and answer any four from the rest questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right hand indicate the marks.**

Q. No. 1

a. What do you mean by Computer Forensics? How does it differentiate from Digital Forensics? [7 Marks]

b. Explain the forensic investigation process in detail. [7 Marks]

Q. No. 2

a. What is a Cyber Crime? How is it different from unauthorized activities? Explain both the concepts with two examples. [8 Marks]

b. Explain Incident Response. Discuss why IR is important. [6 Marks]

Q. No. 3

a. What do you mean by evidence control? Why evidence control is important in a Forensic Investigation? Discuss some process that can ensure evidence control. [8 Marks]

b. List three open source forensic tools and their features/capabilities (purpose). [6 Marks]

Q. No. 4

a. What is crime scene response? Explain the same with some examples [6 Marks]

b. Explain the four types of evidence with examples. [8 Marks]

Q. No. 5

a. Explain some of the important points need to be considered when you are setting up a Forensic Laboratory. [8 Marks]

b. Compare the advantages and disadvantages of FAT / FAT32 with NTFS from a forensic stand–point. [7 Marks]

Q. No. 6

a. Explain file signature in detail. What is the importance of file signature in digital forensics? Give some examples. [8 Marks]

b. What is a host–based integrity checker? Explain its working. [6 Marks]

Q. No. 7

a. What is ADS? Explain its working. How can we detect ADS? [8 Marks]

b. Explain in detail about Post Mortem Analysis. [6 Marks]

Q. No. 8

a. What is a block device file? Explain in detail. [7 Marks]

b. What is a portable forensic lab? What are the requirements for setting up a portable forensic lab? [7 Marks]

****