Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – III • EXAMINATION – WINTER • 2014

Subject code: 2735101 Date: 27-11-2014

Subject Name: Cyber Forensics

Time: 02:30 pm - 05:00 pm Total Marks: 70

Instructions:

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

Q.1	**(a)**	What Is Computer Forensics? How does it differentiate from Digital Forensics?	**07**
	(b)	What is a Cyber Crime? How is it different from unauthorized activities? Explain both the concepts with two examples	**07**
Q.2	**(a)**	Explain Log analysis in details. Discuss few log files which are related to forensics.	**07**
	(b)	What is windows registry? Explain it's structure in detail. Discuss in detail how windows registry is related to forensics	**07**
		OR	
	(b)	What is Memory Analysis? What are the information that can be gathered as part of Memory Analysis.	**07**
Q.3	**(a)**	What is hard disk forensics? Explain the internals of a hard disk in detail.	**07**
	(b)	Differentiate between Allocated Space, Unallocated Space, Slack space and Un-used space	**07**
		OR	
Q.3	**(a)**	What is an MBR? Explain the internal structure of MBR in detail.	**07**
	(b)	What is Anti-Digital forensics? Explain some of the ADF concepts	**07**
Q.4	**(a)**	Explain some of the points to be considered when setting up a Forensic Laboratory.	**07**
	(b)	What is a portable forensic lab? What are the requirements for setting up a portable forensic lab?	**07**
		OR	
Q.4	**(a)**	Explain the different types of digital data.	**07**
	(b)	Differences between Live Analysis and Post Mortem Analysis.	**07**
Q.5	**(a)**	Explain the advantage and disadvantages of using open source and commercial forensic tools.	**07**
	(b)	Differentiate with appropriate example - Forensics of Cloud and Forensics using Cloud	**07**
		OR	
Q.5	**(a)**	Explain NTFS and MFT in detail?	**07**
	(b)	Compare the advantages and disadvantages of FAT / FAT32 with NTFS from a forensic stand-point.	**07**

****