Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– III • EXAMINATION – SUMMER 2015

Subject Code: 732303 **Date: 02/05/2015**

Subject Name: Software Forensics

Time: 2:30 pm to 5:00 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)**	Define Digital forensic, Software forensic and Network forensic. List and explain software forensic technologies and practices.	**7**
	(b)	Explain detection and anti-detection techniques for computer virus and malware.	**7**
Q.2	**(a)**	How the programming process and tools used to develop the program are used as software forensic tools?	**7**
	(b)	Define Blackhats. Explain different types of Blackhats and their characteristics.	**7**
		OR	
	(b)	Define Blackhats and explain various Blackhat products.	**7**
Q.3	**(a)**	List and explain types of evidences. Explain rules of evidences.	**7**
	(b)	If you are asked to carry out software forensics based on programming style, which features would you look for? Explain in detail.	**7**
		OR	
Q.3	**(a)**	Discuss the issues related to laws and ethics related to software forensics.	**7**
	(b)	Explain the significance of ñfunctionò as an indicator of cultural style of programming.	**7**
Q.4	**(a)**	What is ñcusumò? Explain its significance with respect to software forensics.	**7**
	(b)	Explain the requirement and process of Decompilation of software code.	**7**
		OR	
Q.4	**(a)**	Write short note on stylistic analysis and linguistic forensic.	**7**
	(b)	Compare content and non content analysis.	**7**
Q.5	**(a)**	Write a note on Plagiarism detection vs Authorship analysis	**7**
	(b)	Briefly discuss the tools like DEBUG and BinText for software code analysis.	**7**
		OR	
Q.5	**(a)**	If you are given to do authorship analysis, how would you do it? What problems would you face while carrying out authorship analysis? Do u think it is reliable?	**7**
	(b)	What is plagiarism? Which tools would you use to determine plagiarism? Explain in detail.	**7**