Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME – SEMESTER III (NEW) – EXAMINATION – WINTER-2016

Subject Code: 3735101 **Date:25/10/2016**

Subject Name: Cyber forensics

Time:02:30 pm to 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)**		**07**
		(i) Describe the steps involved in cyber forensics.	**03**
		(ii) "Encoding is not encrypting" Justify.	**04**
	(b)		**07**
		(i) In a common criminal computer forensic case, which types of investigative team members can be found?	**03**
		(ii) A Word document is prepared and saved on laptop with the filename Sand.doc. The process of saving a file on hard disk involves which three basic events? Which steps are involved in deleting this file? If investigation is needed for Sand.doc, can it be retrieved?	**04**
Q.2	**(a)**	Explain Forensic Acquisition Utilities.	**07**
	(b)	Write the goals of forensics analysis.	**07**
		OR	
	(b)	Which steps need to be taken to learn about the case?	**07**
Q.3	**(a)**	Why it is important to document everything in case of cyber forensic?	**07**
	(b)		**07**
		(i) What is a forensic image of computer?	
		(ii) What is forensic copy of a hard drive?	
		OR	
Q.3	**(a)**	Explain any one concealment technique.	**07**
	(b)		**07**
		(i) How does computer forensics differ from data recovery?	
		(ii) What type of data is focused in cyber forensic investigation?	
Q.4	**(a)**	Write about Forensic Implications.	**07**
	(b)	How to combine Cyber Forensics and the Investigating Criminal Behaviour. Explain with example.	**07**
		OR	
Q.4	**(a)**	Write cyber forensic principles.	**07**
	(b)	What is computer security incident? It includes which events?	**07**
Q.5	**(a)**	Write the laws outlined for cyber forensic.	**07**
	(b)	What is computer crime? What is invasion of privacy in cyber forensics?	**07**
		OR	
Q.5	**(a)**	Which common mistakes are made in evidence collection?	**07**
	(b)	Explain incident response methodology.	**07**

****