Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER– IV (NEW) EXAMINATION – SUMMER 2017

Subject Code: 2745603 **Date:03/05/2017**

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)**	Explain best practices in handling digital evidence. Explain "Rule of Evidence".	**07**
	(b)	Explain in brief- Source of Digital Evidences.	**07**
Q.2	**(a)**	Explain how an E-mail can be traced for forensics purpose. Outline various steps involved.	**07**
	(b)	Explain Privacy challenges in cyber forensic with suitable example.	**07**
		OR	
	(b)	What is Memory Analysis? What is the information that can be gathered as part of Memory Analysis?	**07**
Q.3	**(a)**	Explain the key steps to be performed in solving a computer forensics case.	**07**
	(b)	What are the typical elements of a digital forensics investigation report? Explain its importance.	**07**
		OR	
Q.3	**(a)**	Explain "Chain of Custody" in computer/digital forensics.	**07**
	(b)	Write a note on "Forensic Duplication".	**07**
Q.4	**(a)**	Explain briefly on Network drive imaging & Logical File collection.	**07**
	(b)	Explain Cyber Crimes and Information Technology Act.	**07**
		OR	
Q.4	**(a)**	Write the difference between Mobile Phone's Logical Acquisition & Physical Acquisition.	**07**
	(b)	Explain the advantages and disadvantages of using open source and commercial forensic tools.	**07**
Q.5	**(a)**	Write a note on "Requirement (necessity, constraint, condition and pre-requisite) for building a forensic laboratory".	**07**
	(b)	Explain procedure for gathering evidences from live systems. What care should be taken at the time of evidence gathering from live system?	**07**
		OR	
Q.5	**(a)**	Explain hashing and encryption from a digital forensic point of view.	**07**
	(b)	Explain tools and techniques used to commit cyber crimes.	**07**

****