Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – WINTER 2022

Subject Code:3170725 Date:07-01-2023

Subject Name:Digital forensics

Time:10:30 AM TO 01:00 PM Total Marks:70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	What is your understanding of the term "chain of custody" in the context of digital forensics?	**03**
	(b)	What is digital forensics explain the process of digital forensics?	**04**
	(c)	Define: hibernating files, examining window registry, recycle bin operation Operation.	**07**
Q.2	**(a)**	Explain forensic science.	**03**
	(b)	Describe forensic cloning of evidence.	**04**
	(c)	What is locard's exchange principle and how does it apply to digital forensics?	**07**
		OR	
	(c)	Explain order of volatility in brief.	**07**
Q.3	**(a)**	What types of tools can be selected for use in mobile device investigations?	**03**
	(b)	Why it is important in the forensic investigation to work on duplicate image?	**04**
	(c)	Describe techniques to remove metadata.	**07**
		OR	
Q.3	**(a)**	What is hashing explain hashing concepts to maintain the integrity of evidence?	**03**
	(b)	Write a note on Electronics discovery.	**04**
	(c)	Discuss e-mail header forensic in brief.	**07**
Q.4	**(a)**	What are the legal provisions against cyber crime?	**03**
	(b)	Explain tool validation in context of quality assurance.	**04**
	(c)	Explain Hashing concepts to maintain the integrity of evidence.	**07**
		OR	
Q.4	**(a)**	What are three types of tools used by digital forensic examiners?	**03**
	(b)	What relevance does metadata have to the evidence collected?	**04**
	(c)	Define and differentiate Live and dead system forensic.	**07**
Q.5	**(a)**	How to restore your deleted or modified folders or files from Shadow Copies.	**03**
	(b)	What is the most important legal features about digital evidence?	**04**
	(c)	What is an example of a network forensic technique?	**07**
		OR	
Q.5	**(a)**	What information analyst could get from email header?	**03**
	(b)	Discuss techniques of hibernating files.	**04**
	(c)	Documenting the scene and evidence, maintaining the chain of custody.	**07**

****