TE Sem-VI EXTC C-scheme May 2026
Date: 20/05/2026

Time: 3 hrs. Maximum Marks = 80

NB:

1. **Question No. 1 is compulsory and solve any THREE questions from remaining questions**
2. **Assume suitable data if necessary**
3. **Draw clean and neat diagrams**

			Marks
Q1.		Attempt any four	
	a.	Differentiate between White Hat, Black Hat, and Grey Hat hackers.	5
	b.	What is a "Computer Security Incident" and what are the goals of incident response?	5
	c.	List and explain the different forensic image formats used in digital investigations.	5
	d.	What is "Volatile Data" and why is its collection critical in a live investigation?	5
	e.	Explain the concept of "Culpability" with reference to Intent, Knowledge, and Negligence.	5
Q2.	a.	What is Social Engineering? Explain different social engineering techniques and discuss why it is often considered the most difficult hacking technique to prevent.	10
	b.	Explain violent and non-violent cybercrimes. How does the computer's role vary in these scenarios?	10
Q3.	a.	Explain any three types of digital forensics. What are the primary objectives of conducting a forensic investigation?	10
	b	Differentiate between computer viruses, worms, Trojan horses, and trap doors. Explain how each can be used to facilitate a cybercrime.	10
Q4.	a.	Explain the necessity of forensic duplication. Describe the different forensic duplication techniques and image formats used to ensure evidence integrity.	10
	b.	Explain the steps involved in collecting and preserving digital evidence from a crime scene. Why is a "Chain of Custody" essential during this process?	10
Q5.	a.	Explain the process of email tracing to identify a sender. What information can be gathered from an email header and how can it be used as evidence?	10
	b.	What is a response tool kit? Explain how to create a response tool kit for Unix?	10
Q6.	a.	Explain the core requirements and legal implications of the CAN-SPAM Act for commercial email senders. How does this act assist in digital forensic investigations?	10
	b.	List the complexities of evidence handling in a network environment. Explain the steps involved in a forensic investigation of routers.	10

****