1/1

TE Sem VI | Branch - IT | NOV-2025 | Q.P code - 95950
Date - 11.12.2025

(3 Hours) Total Marks: 80

N.B.: (1) Question No.1 is compulsory.
(2) Attempt any three questions from the remaining five questions.
(3) Make suitable assumptions wherever necessary but justify your assumptions.

1.	(a) Define phishing attack and explain how attackers execute it.	05
	(b) What is digital evidence? Discuss the admissibility criteria in court.	05
	(c) Explain the role of Chain of Custody in digital investigation	05
	(d) Differentiate between Vulnerability Assessment and Penetration Testing.	05
2.	(a) Explain the Ethical Hacking lifecycle with a neat diagram.	10
	(b) Describe the Incident Response Phases as per NIST framework.	10
3.	(a) Discuss Computer Forensics Investigation Process in detail.	10
	(b) Explain how digital evidence is collected and preserved from Windows and Linux systems	10
4.	(a) What is Network Forensics? Explain the tools used for analyzing network traffic.	10
	(b) Describe E-mail Forensics. Explain steps to track header information and trace sender identity..	10
5.	(a) Explain various Mobile Forensic acquisition techniques (Logical, Physical, Cloud-based).	10
	(b) Elaborate common types of cybercrimes with suitable real-world examples.	10
6.	Write a short note on (Any Two)	20

(1) CSIRT Roles and Responsibilities.
(2) Anti-Forensic Techniques.
(3) Denial of Service (DoS) Attack
(4) Report Writing Guidelines in Forensic Investigation
