

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY GURAJADA VIZIANAGARAM
IV B. Tech I Semester Regular/Supplementary Examinations OCT/NOV 2025
CYBER SECURITY & FORENSICS

(CSE, IT)

Time: 3 hours

Max. Marks: 70

Answer any **FIVE** Questions. **ONE** Question from **Each unit**

All Questions Carry Equal Marks

UNIT-I

1. a) What are botnets and attack vectors? Explain how they are used in large-scale cyberattacks. [7M]
b) Discuss the origin of cybercrime and how it differs from traditional crime. [7M]
(OR)
2. a) Describe the role and motivations of cybercriminals. What categories can they be classified into? [7M]
b) Explain the different classifications of cybercrimes with suitable examples. [7M]

UNIT-II

3. a) Differentiate between brute-force, dictionary, and rainbow table attacks, and mention the countermeasures for each. [7M]
b) Explain how steganography is used for concealing information and how forensic experts can detect hidden data. [7M]
(OR)
4. a) Discuss how DoS and DDoS attacks differ in terms of scale and execution. Analyze their impact on network availability. [7M]
b) Compare viruses, worms, and Trojan horses in terms of infection mechanism, propagation method, and damage potential. Give one real-world example of each. [7M]

UNIT-III

5. a) What are encryption and decryption methods? Explain how they affect cybercrime investigations and the techniques investigators use to access encrypted data. [7M]
b) Discuss the tools and methods used for recovering deleted evidence and explain how the recovered data can support the investigation. [7M]
(OR)
6. a) In what ways does eDiscovery help in the identification, preservation, and presentation of electronic evidence during legal proceedings? [7M]
b) Outline common password-cracking approaches and the investigative tools used to unlock restricted files and accounts. [7M]

UNIT-IV

7. a) How does computer forensics differ from general IT security and incident response? [7M]
b) Discuss challenges and forensic techniques specific to Windows system forensics versus Linux system forensics. [7M]

(OR)

8. a) Compare computer forensics software tools and hardware tools. Give examples of each and explain the scenarios where a hardware solution is preferred over software. [7M]
- b) Describe the role of audio-video analysis in investigations. What techniques are used to authenticate, enhance, and extract evidential content from multimedia files? [7M]

UNIT-V

9. a) Examine the major challenges faced by Indian law enforcement agencies in handling cybercrimes. How do these challenges affect the overall cybercrime scenario in India? [7M]
- b) Explain the concept of a digital signature. How does the Indian IT Act ensure its authenticity, integrity, and legal validity? [7M]

(OR)

10. a) How the Indian cyber legal framework balances between privacy, freedom of expression, and cybersecurity enforcement? [7M]
- b) Discuss the relationship between Cyberlaw, technology, and students in the Indian context. [7M]
