JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATIONS- 2026

B.Tech-VI Semester (CSE)

COURSE CODE (CREDITS): 25B1WCI645 (3) MAX MARKS: 25

COURSE NAME: Digital Forensics

COURSE INSTRUCTOR: NTS* MAX. TIME: 1 Hour 30 Min

Note: *(a) All questions are compulsory.*

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

(c) Use of calculator is not allowed

Q.No	**Question**	**CO**	**Marks**
Q1	Explain the concept of Pre-Incident Preparation, Incident Detection, and Characterization in computer security incidents. How do these stages help in minimizing the impact of cyber attacks?	3	5
Q2	A company detects unusual outbound traffic from a server suspected of malware infection. Apply the Incident Response Process (Initial Response, Investigation, Remediation, Reporting) to handle this situation. Clearly outline steps to be followed.	3	5
Q3	Discuss the concept of Forensic Duplication and compare Traditional Duplication and Live System Duplication	4	5
Q4	A financial institution faced a ransomware attack where critical systems were encrypted. Investigators found that the attack spread due to delayed detection and lack of preparedness. Analyze the case and answer: (a) Identify failures in Pre-Incident Preparation and Detection (b) Suggest an improved Incident Response Strategy (c) What investigative information should be tracked?	3	5
Q5	During a forensic investigation, a suspect's system image revealed deleted files, file slack space data, and traces of browser activity. (a) Explain how Hashing ensures integrity of evidence (b) Describe how tools like The Sleuth Kit / Foremost can be used for data recovery (c) Analyze the importance of file system analysis and data carving in this case.	4	5