JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS- 2026

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS):25B1WCI645 (3) MAX MARKS: 35

COURSE NAME: Digital Forensics

COURSE INSTRUCTOR: NTS* MAX. TIME: 2 Hours

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 major differences between cybercrime investigation and ethical hacking. Discuss the role of reconnaissance and scanning tools during forensic investigations with suitable examples.	CO1	5
Q2	Describe the Incident Response Methodology used in digital forensic investigations. Explain the importance of live data collection on Windows or UNIX systems during an active security incident.	CO3	5
Q3	(a) Explain the concept of forensic duplication and compare traditional duplication with live system duplication. (b) Discuss the significance of forensic image formats and forensic containers in maintaining evidence authenticity.	CO4	3+4=7
Q4	(a) Explain how network traffic analysis helps in identifying network intrusions. (b) Discuss the role of Intrusion Detection Systems (IDS) in digital forensics and differentiate between Host-based IDS and Network-based IDS.	CO5	4+4=8
Q5	**Case Study:** A multinational organization suspects that an internal employee installed malware on a company workstation and transferred confidential files through suspicious network activity. During the investigation, the forensic team discovered deleted files, abnormal router logs, and traces of unauthorized remote access. As a digital forensic investigator, answer the following: (a) Explain the steps involved in performing forensic imaging and preserving digital evidence integrity using hashing techniques.	CO4, CO5, CO6	2+2+2+2+2 =10

	(b) Describe how deleted files can be recovered using file carving techniques and forensic tools. (c) Explain how router logs and network traffic can be analyzed to identify unauthorized access. (d) Prepare the outline of a forensic investigation report mentioning major sections and their purpose. (e) Compare the features and applications of any two forensic tools such as Autopsy, Sleuth Kit, or SFIT in the context of the above investigation. Mention which tool would be more suitable for malware and deleted file analysis.		