JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1EXAMINATION- 2025

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI631 (2) MAX. MARKS: 15

COURSE NAME: DIGITAL FORENSICS

COURSE INSTRUCTORS: AAYUSH SHARMA MAX. TIME: 1 Hour

Note:(a)All questions are compulsory.

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

Q.No	Question	CO	Marks
Q1	Rahul, a final-year computer science student, skipped most of his cybersecurity classes to focus on freelance hacking gigs. He created fake degree certificates using a compromised college portal and sold them to lazy peers. When the college discovered the fraud, they called in a digital forensics team. Answer the following: 1. The forensic team suspects Rahul used reconnaissance tools to find the portal's vulnerabilities. Name two tools he might have used, and explain how they helped him identify weaknesses. 2. Rahul claims he "never studied forensics" and didn't know deleting files was illegal. Argue why his ignorance violates digital forensic rules. 3. Rahul's lack of education led to sloppy mistakes (e.g., using his personal email for scams). How would proper knowledge of phases of ethical hacking have helped him avoid detection?	[CO 2]	3
Q2	To skip exams, a group of students hacked the college's cafeteria Wi-Fi to send fake "exam canceled" emails to the entire batch. They used a Raspberry Pi for packet sniffing but forgot to clear logs. The dean demands accountability. Answer the following: 1. The students used open-source tools they "learned from YouTube." Contrast their approach with structured ethical hacking steps. 2. Classify this attack under categories of cybercrime.	[CO 1]	3
Q3	Kavya, a struggling final-year student, after experiencing multiple rejections from multiple placement drives is now facing financial issues at home in desperation stole code from a peer's project to launch her startup. The peer discovered the theft via GitHub logs and filed a complaint. Investigators found the original code on Kavya's hard drive and testimonies from her team. Answer the following: 1. What kind of evidence is the **GitHub commit history** and **team's statements**, Compare their roles in proving theft. 2. If Kavya argues that the code on her hard drive was accidentally copied, how could forensic evidence refute or support this claim?	[CO 2]	3

Q4	Aditi, a college intern at a digital forensics firm with a PPO of 24 LPA, was tasked with collecting evidence from a student's laptop suspected of hosting pirated exam papers. In her rush to impress her boss, she skipped documenting her steps, copied files directly to her personal USB drive, and left the laptop unattended in university library for 30 minutes. Later, the defense attorney argued the evidence was tampered with, and the case dismissed. Aditi lost her internship and is now working as a frontend developer in a startup with 5 LPA package. Answer the following: 1. Identify three critical mistakes Aditi made in handling the evidence. 2. Propose a step-by-step process Aditi should have followed including tools (e.g., write-blockers, hash generators) and documentation practices. 3. Aditi thought, "Documentation is just paperwork!" refute this statement.	[CO 1] [CO 2]	3
Q5	Explain **any three** of the five cardinal rules of digital forensics.	[CO 2]	3