JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2025

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI631 (2) MAX. MARKS: 35

COURSE NAME: DIGITAL FORENSICS

COURSE INSTRUCTORS: AAYUSH SHARMA 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

Q.No	Question	CO	Marks
Q1	**Scenario:** An investigator has SSH access to a compromised Linux box. The initial directory listing reveals a hidden folder named .secret containing a file bandit24. Inside, clues hint that the next password is stored in a file buried somewhere under /var/log, with one change: filenames have had all vowels (a,e,i,o,u) stripped. **Task:** (a) Write a single find command (with any necessary flags) that locates the file containing the next password. (b) Pipe its contents to grep to extract only the line matching the regex **^password: [[:alnum:]]{32}$.**	[CO4]	[3X2]
Q2	**Scenario:** Your lab is ISO 17025 certified. You must produce the final investigative report for a case. **Task:** Write a concise outline (using bullet-level headings) covering at minimum: 1. Title page elements 2. Executive summary length guideline (in words) 3. Methodology section subsections (list at least 4) 4. Chain of custody appendix references (naming convention) 5. Conclusion and recommendations formatting rules	[CO6]	[5X2]
Q3	**Answer the following:** 1. Explain the structural differences between MBR and GPT, including their partition limits and integrity mechanisms. 2. Using TestDisk, provide the two-step command sequence to scan for lost partitions on a raw image (disk.dd) and then write the recovered GPT table back to the media. 3. A RAID 5 array has lost one disk. Describe how you would reconstruct the logical volume for analysis, naming a free tool or method.	[CO4] [CO5]	[3X3]
Q4	A) You are shown this PHP snippet used to fetch user profiles: **<?php** **$id = $_GET['id'];** **$query = "SELECT name, email FROM users WHERE id = $id";** **$res = mysqli_query($conn, $query);** **// ...** **?>**	[CO3]	[2X5]

Tasks :-

1. Identify the vulnerability in one sentence.
2. Craft a malicious URL payload that retrieves all rows via a Boolean-based injection.

B) Consider this snippet rendering a welcome message:

```
<?php
  $user = $_GET['user'];
?>
<html>
  <body>
    <h1>Welcome, <?= $user ?></h1>
  </body>
</html>
```

Tasks :-

1. Show an example GET request that triggers a reflected XSS alert popup.
2. Explain (in one line) why this payload succeeds.