# JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

## TEST -2 EXAMINATION- APRIL-2023

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

COURSE NAME: Digital Forensics

COURSE INSTRUCTORS: Dr. Nancy Singla MAX. TIME: 1 Hour 30 Minutes

***Note:*** *All questions are compulsory. Marks are indicated against each question in square brackets.*

1. Your organization receives a call from a federal law enforcement agency, informing you that they have information indicating a data breach occurred involving your environment. The agency provides a number of specific details, including the date and time when sensitive data was transferred out of your network, the IP address of the destination, and the nature of the content. [3+2] (CO3)
   (a) Does this information match the characteristics of a good lead? Explain why or why not.
   (b) How can you turn this information into an actionable lead?

2. What is the purpose of footprinting in a hacking attempt? Explain how it is performed? [5] (CO1)

3. (a) What are the three high level areas that are focused during pre-incident preparation? [3+2] (CO3)
   (b) During the Incident Response; when does the remediation process start, and why?

4. What is live data acquisition? Explain in which scenarios "live acquisition" is necessary. [5] (CO4)

5. (a) If you have connected hard drive as an evidence to a system for imaging, do you need to use a write blocker? Explain why or why not? [2+3] (CO4)
   (b) Identity the following:
      i. Tool used to recover partition in the case of disk corruption
      ii. RAID level where blocks are mirrored across pair of drives
      iii. Metadata units on UNIX derived file systems