JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2023

B.Tech-VI Semester (CSE/IT)

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

COURSE NAME: DIGITAL FORENSICS

COURSE INSTRUCTORS: DR. NANCY SINGLA MAX. TIME: 2 Hours

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

1. Digital forensics is a constantly evolving scientific field with many sub-disciplines. Explain the different types of digital forensics. [5] (CO2)

2. Investigators respond to a homicide on a street corner. The victim was shot once in the chest, and there are no witnesses. The victim was identified and a search was conducted on his residence in an attempt to determine a suspect or motive. A computer was found at his residence. The computer was already turned on and was running Windows XP. The investigators follow the traditional method of computer evidence collection by shutting down the system and collecting the computer. The computer was booked into evidence for review by a computer forensics examiner. [2+3] (CO2)

   Considering the above scenario, answer the following:
   (a) Do you think the investigator followed the right investigation practice by shutting down the computer system?
   (b) Explain what evidences could be collected on-scene from the computer system. Also, mention the tool used for the collection and analysis of the evidence.

3. In malware analysis, what is the difference between the static and dynamic analysis and what are the main tools used in each one of these analysis techniques? [5] (CO4)

4. Consider a scenario, where an attacker has gained access to a router on a network and has performed routing table poisoning attack. [5+5] (CO5)
   (a) How could a routing table in a router be poisoned by an attacker? What could be the intentions of an attacker while performing router poisoning on a network?
   (b) Considering yourself as a network forensic investigator, what steps would you take to investigate this attack?

5. Is it possible to recover deleted files from a hard drive? If yes, then how? [5] (CO6)

6. What is the purpose of the Intrusion Detection Systems (IDS)? Explain the different types of detection methods used by the IDS. [5] (CO5)