POORNIMA UNIVERSITY, JAIPUR

Write Roll No Below:

____

END SEMESTER EXAMINATION, 2023-2024 EVEN SEMESTER

MCA (Cyber Security) I () - II (Main/Back) End Semester Examination,

23MCYCCA2102: Cyber Forensic

Time: 3 Hours **Total Marks:** 60 **Min. Passing Marks:** 21/24/27 **Question Paper ID:** 001106

Instructions: Attempt all five questions. There is an internal choice either (a or b) in Q1 to Q5. Marks of each question or its parts are indicated against each question/part. Draw neat sketches wherever necessary to illustrate the answer. Assume missing data suitably (if any) and clearly indicate the same in the answer.

Bloom Level(BL): 1-Remembering, 2-Understanding, 3-Applying, 4-Analysing, 5-Evaluating, 6-Creating

Use of following supporting material is permitted during examination for this subject: Nil

---

Q1. **(a)** (i) discuss the potential impact of cybercrimes on individuals and organizations. **[Marks 6]**
(ii) Highlight the key phases and techniques involved in a typical computer investigation. **[Marks 6]**

Marks 12 **BL** 1 **CO** 1

(OR)

(b) (i) What specific tasks can non-technical staff perform as first responders, and how do their actions contribute to the overall success of the forensic process? **[Marks6]**
(ii) How does the first responder procedure differ for each group, and why is it important for a coordinated response in handling cyber incidents? **[Marks 6]**

Q2. **(a)** (i) Explain the differences between magnetic, non-magnetic, and optical storage mediums. **[Marks 6]**
(ii) Describe the functioning of essential components in storage devices, such as platters, head assembly, and spindle motor. **[Marks 6]**

Marks 12 **BL** 1 **CO** 2

(OR)

(b) (i) Discuss the process of data acquisition in the context of computer forensics. **[Marks 6]**
(ii) Explain different type of memory allocation methods in details **[Marks 6]**

Q3. **(a)** (i) How would you initiate the process of evidence collection in a Windows environment when investigating a suspected security incident? **[Marks 6]**
(ii) Describe the significance of Windows event logs in forensic investigations, and provide examples of specific events that could be indicative of malicious activity. **[Marks6]**

Marks 12 **BL** 1 **CO** 3

(OR)

(b) (i) Explain the importance of memory forensics in a Windows investigation. What kind of information can be extracted from volatile memory, and how can it aid in understanding an incident? **[Marks 6]**
(ii) Explain window forensics in detail. **[Marks 6]**

Q4. **(a)** **Scenario:** An organization has noticed multiple user accounts being compromised, and the attackers seem to be using dictionary attacks.
(i) As a cybersecurity analyst, how would you investigate and respond to this situation? **[Marks 6]**
(ii) What measures would you implement to prevent future occurrences of dictionary attacks? **[Marks 6]**

Marks 12 **BL** 1 **CO** 4

(OR)

(b) **Scenario:** An organization has noticed multiple user accounts being compromised, and the attackers seem to be using dictionary attacks.
(i) What indicators might suggest that a dictionary attack is underway, and how would you distinguish it from other types of password attacks? **[Marks 6]**
(ii) How dictionary attack works explain with example. **[Marks 6]**

Q5. **(a)** (i) How does a company typically establish an evidence handling procedure to mitigate risks associated with corporate espionage? Discuss key steps involved in this process.**[Marks 6**]
(ii) What is the significance of maintaining a proper chain of custody in cases related to corporate espionage? Describe the potential consequences of mishandling or breaking this chain.**[Marks 6]**

Marks 12 **BL** 1 **CO** 5

(OR)

(b) What are the main features introduced in the Indian IT Act of 2008 (Amendment) that specifically address issues related to corporate espionage? How do these amendments enhance cybersecurity measures for businesses operating in India? **[Marks 12]**

*****End of Question Paper*****