Student ID: 231285

Air University

Mid Semester Examinations: Fall 2025

Subjective Part

(To be solved on Answer Books only)

Subject: Digital Forensics
Class: BSCYS-F-23
Section(s): A + B
Course Code: CY-334

Time Allowed: 120 Minutes
Max Marks: 50
FM's Name: Hassan Iftikhar
FM's Signature:

INSTRUCTIONS

- Attempt responses on the answer book only.
- Nothing is to be written on the question paper.
- Rough work or writing on question paper will be considered as use of unfair means.
- Tables / calculators are allowed / not allowed.

Q 1	CLO 01	Domain: Understanding	Marks 24

You are part of digital forensics team investigating corporate incident:

1. What immediate steps would you take before initiating the acquisition to ensure evidence is preserved and properly documented? (8 Marks)

2. Explain how you would decide between performing a live acquisition or powering down for dead imaging, and justify your choice technically and legally? (8 Marks)

3. Explain how you would approach the acquisition, what tools you might use, and how you would maintain the integrity of the data? (8 Marks)

Q2	CLO 02	Domain: Analysis	Marks 17

As digital forensic manager you receive multiple evidence hard drives from a corporate fraud investigation. A senior executive insists on accessing a copy of the evidence immediately for "internal review." Moreover they are requesting for immediate submission of forensic analysis report.

1. How would you handle this request while maintaining chain of custody, confidentiality, and compliance with forensic procedures? (9 Marks)

2. What will be your strategy to submit the forensic reports while maintaining the integrity and quality of forensic analysis? (8 Marks)

Q3 CLO 03 Domain: File Structure Marks 9

Explain the following:

1. What is the purpose of the Master Boot Record (MBR) in digital forensics analysis? (3 Mark)

2. Differentiate between logical acquisition and physical acquisition of a disk. (3 Marks)

3. What information can a forensic analyst obtain from file system metadata? (3 Marks)