Student ID ____________

Air University
Final Semester Examinations: 2026

Subjective Part
(To be solved on Answer Books only)

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

Time Allowed: 120 Minutes
Max Marks: 100
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 40

You are a member of a digital forensics team investigating a corporate security incident. You are assigned to examine a Windows system:

1. Identify and explain the relevant Windows Registry keys you would examine to confirm unauthorized USB and remote software activity. Justify the forensic significance of each key. Which tools will be used to investigate the artifacts ? (10 Marks)

2. Define the Windows Registry and explain its importance in this digital forensic investigations. Also, describe the five main Windows Registry root keys (20 Marks)

3. Explain Windows forensics in detail and identify various Windows system files and artifacts that may be useful during the investigation? (10 Marks)

Q2 CLO 02 Domain: Analysis Marks 35

You are investigating an incident and suspect the use of anti-forensic techniques affecting various evidence items:

1. Explain in detail the different types of anti-forensic techniques and discuss their possible implementation on digital evidence items. (15 Marks)

2. Explain how evidence timeline reconstruction can be affected by timestomping and log manipulation.? (10 Marks)

3. Explain the challenges anti-forensic techniques pose during evidence acquisition and preservation? (10 Marks)

Q3 CLO 03 Domain: File Structure Marks 25

A corporate employee is suspected of leaking confidential documents and also accused of harassment using an android smartphone. The device is seized while powered on.

1. Explain what immediate steps should be taken to preserve data on the device? (10 Marks)
2. Which forensic tools will be used to perform the acquisition of the smart phone and discuss the acquisition type that will be initiated to image the evidence? (08 Marks)
3. Which Android artifacts would you examine to identify file transfer activity? (07 Marks)