

Dr. Babasaheb Ambedkar Open University
Term End Examination January – 2026

Course	: MCA	Date	: 26/02/2026
Subject Code	: MCA-E4305	Time	: 03:00pm to 05:15pm
Subject Name	: Digital Records and Cyber Forensics	Duration	: 02.15 Hours
		Max. Marks	: 70

Section A

Answer the following (Attempt any three) (30)

1. Define digital records and explain their characteristics, types, advantages, and disadvantages with suitable examples.
2. Explain the nature of digital evidence and describe the processes involved in acquisition, preservation, analysis, and presentation of digital evidence.
3. Explain Windows forensic analysis with reference to registry analysis, event logs, and file system artifacts.
4. Explain mobile network investigations and discuss the techniques used for collection and analysis of mobile digital evidence.
5. Explain the cybercrime investigation process with reference to ACPO guidelines and digital evidence handling procedures.

Section B

Answer the following (Attempt any four) (20)

1. Describe the basic steps involved in the computer forensics investigation process.
2. Write a short note on the challenges involved in electronic discovery.
3. Write a note on data hiding and evidence destruction techniques.
4. Explain the scope of computer forensics in modern cybercrime investigations.
5. Explain the importance of validation and testing of digital forensic tools.
6. Explain the functions of cyber forensic laboratories

Section C

Part – A (Multiple Choice Questions) (10)

- 1 Computer forensics primarily deals with:
A Network optimization B Data encryption
C Software development D Collection and analysis of digital evidence
- 2 Which of the following is a key ethical responsibility of a digital forensic expert?
A Speeding up investigations B Not altering original evidence
C Sharing findings publicly D Bypassing legal procedures
- 3 Which step comes first in crime scene investigation?
A Interviewing suspects B Evidence analysis
C Securing the crime scene D Report writing
- 4 Which is a major challenge in e-Discovery?
A Large volume of electronic data B Limited storage
C Hardware failure D Power issues
- 5 Which process converts evidence into a court-presentable form?
A Acquisition B Preservation
C Analysis D Identification

- 6 Anti-forensics techniques are used to:
A Secure systems B Hide or destroy digital evidence
C Improve investigation speed D Encrypt backups
- 7 Network forensics mainly focuses on:
A File systems B Operating systems
C Mobile devices D Network traffic analysis
- 8 Computer forensics is useful in:
A Criminal, civil, and corporate cases B Only criminal cases
C Only civil cases D Academic research only
- 9 Windows Registry is mainly used to store:
A Multimedia files B System configuration information
C Network packets D Email data
- 10 CERT-In in India mainly deals with:
A Cyber education B Cyber laws
C Cyber security incidents and response D Digital payments

Part – B (Do as Directed)

(10)

State whether the following statements are true or false

- 1 Computer forensics includes the recovery of deleted or destroyed digital data.
- 2 Lack of trained personnel is a major challenge for cyber forensic laboratories.
- 3 Indian Evidence Act does not recognize digital evidence.
- 4 Confiscated digital devices should be accessed immediately at the crime scene.
- 5 Government initiatives help strengthen cybercrime investigation infrastructure.
- 6 Validation of forensic tools helps ensure court acceptance of findings.
- 7 Windows event logs help investigators identify system activities.
- 8 Digital evidence is irrelevant in civil litigation cases.
- 9 Network forensics focuses only on offline data analysis.
- 10 Data wiping strengthens digital evidence authenticity.
