

5E1847	Roll No. _____	Total No. of Pages : 2
	5E1847	
B.Tech. V-Sem. (Main & Back) Examination, November/December - 2025 Computer Sc. and Engg. (Cyber Security) 5CCS5-12 Digital Forensics and Incident Response		

Time : 3 Hours

Maximum Marks : 70

Instructions to Candidates:

Attempt all Ten questions from Part A, Five questions out of seven questions from Part B and Three questions out of five questions from Part C.

Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.

Use of following supporting material is permitted during examination.

(Mentioned in form No. 205).

PART - A

(Answer should be given up to 25 words only)

All questions are compulsory.

(10×2=20)

1. What are the benefits of computer forensics in courts?
2. Define digital forensics.
3. Why is preservation of evidence important?
4. What is meant by legal concerns in computer forensics?
5. Mention types of removable media used in mobile device forensics.
6. Define evidence admissibility in court.
7. What is the role of expert witness testimony in digital forensics?
8. Mention any two techniques of acquiring live volatile data.
9. What is purpose of performing searches in forensic analysis?
10. What is metadata extraction in digital forensics?

PART - B

(Analytical / Problem Solving Questions)

Attempt any Five questions.

(5×4=20)

- ✓1. Explain the concept of chain of custody. Also mention an example.
2. Differentiate between traditional and digital forensics.
3. Discuss challenges and privacy issues that are faced in forensic investigation process.
- ✓4. Mention steps involved in duplication and preservation of evidence.
- ✓5. What is the process of acquiring live volatile data during forensic investigation?
- ✓6. Explain various types of mobile device evidence sources.
- ✓7. Discuss how email and messenger analysis help in forensic investigations.

PART - C

(Descriptive / Analytical / Problem Solving / Design Questions)

Attempt any Three questions.

(3×10=30)

- ✓1. Explain the complete process of acquisition and duplication of digital evidence, including data analysis and hidden file detection.
 - ✓2. Explain role of court testimony, expert witnesses, and evidence admissibility in mobile device forensics.
 3. Discuss in detail volatile and non-volatile evidence. How does order of volatility affect forensic investigations?
 4. What are legal concerns, privacy issues and law enforcement methodologies involved in digital forensics?
 - ✓5. Explain various sources of digital evidence in mobile devices and challenges in handling them.
-