

[Time:2.30 Hrs]

[Marks:75]

Please check whether you have got the right question paper.

- N.B:**
- 1. All question are compulsory.**
 - 2. Figures to the right indicate full marks.**

- Q.1 Attempt any Three of the following: 15**
- Why is IM data significant in forensic investigations?
 - What role does digital evidence play in cybercrime cases?
 - What is steganography and how is it detected?
 - Describe the importance of forensic imaging in law enforcement cases.
 - How does WPA2 encryption protect data?
 - Mention two roles performed by a forensic analyst.
- Q.2 Attempt any Three of the following: 15**
- Discuss different types of data backup methods and their advantages.
 - Give examples of volatile and non-volatile evidence.
 - List the steps involved in collecting digital evidence.
 - Describe the methods used by forensic experts to recover hidden data.
 - What are the basic rules of digital evidence admissibility?
 - What is the role of forensic imaging in data recovery?
- Q.3 Attempt any Three of the following: 15**
- What are the primary sources of network-based evidence?
 - What is physical interception in network forensics?
 - How does a NIDS collect evidence?
 - What is active acquisition in network forensics?
 - Differentiate between signature-based and anomaly-based detection.
 - What is the purpose of packet sniffers?
- Q.4 Attempt any Three of the following: 15**
- What is a UFED device and what is its use?
 - Why should web proxy logs be examined during a forensic investigation?
 - How are mobile phones used in modern digital crimes?
 - Discuss the role of log correlation in network forensics.
 - What is a web proxy?
 - Compare the forensic relevance of routers and firewalls during an investigation.
- Q.5 Attempt any Three of the following: 15**
- Analyze a case study and highlight the forensic techniques used.
 - How can forensic experts detect identity theft?
 - Why is file conversion important in digital investigations?
 - Define flow analysis in network monitoring.
 - Which layer of the OSI model is IEEE 802.11 a part of?
 - What is network architecture in the context of forensic analysis?

*****END*****