

(3 Hours)

Marks : 80

- Note: 1) Question number 1 is compulsory.  
2) Attempt any THREE from remaining questions.

- Q.1**
- a. What is Evidence? Explain the various types of digital evidence. **5**
  - b. How are ethical hackers different than malicious hackers? **5**
  - c. Explain importance of forensic duplication and its method. Also list some duplication tools. **5**
  - d. List and explain the various types of cybercrime **5**
- Q.2**
- a. List and Explain the different types of Evidence in digital forensics. **10**
  - b. What is an Intrusion Detection System? Explain different types of Intrusion Detection system. **10**
- Q.3**
- a. Explain volatile data collection procedure for windows system. **10**
  - b. What is Incident Response? Explain Incident Response Methodology in detail. **10**
- Q.4**
- a. What are the steps involved in computer evidence handling? Explain in detail. **10**
  - b. Explain RAID technique in detail **10**
- Q.5**
- a. Explain guidelines for incident report writing. Give one report writing example. **10**
  - b. List various Digital forensic tools and explain any one tool with case study. **10**
- Q.6**
- a. Explain procedure to investigating routers **5**
  - b. Explain the attacks on Network and its prevention. **5**
  - c. What is Cyber-crime? What are the different roles of computer with respect to cybercrime **5**
  - d. Explain importance of Hashing in Forensics analysis. **5**