Unit I

1. Define Computer Forensics. Explain the application areas of computer forensics in detail.
2. Explain the Types of military forensics technology in detail
3. Explain the Steps taken by computer forensics specialists
4. Explain the Forensic process improvement in detail.
5. Explain the types of Business Computer Forensic Technology
6. Explain the types of Law Enforcement Computer Forensic Technology.
7. When the cybercrime will be occurred? Explain in detail.

Unit II

1. What are the tips to be followed while collecting digital evidence?
2. List and explain the rules and types of evidence.
3. Illustrate Data recovery solution in detail
4. Explain the computer evidence processing steps.
5. What are the methods of Evidence collection? Explain in detail
6. How to preserve the digital crime scene? Explain
7. What are the legal aspects to be considered while collecting and preserving the evidence?
8. Describe the Artifacts and collection steps while collecting the evidence.

Unit III

1. What is meant by Corporate Information? Explain in detail.
2. Illustrate “Reconstructing the past events”
3. Explain the following:

   a)Useable file formats b)Unusable file formats c)Converting Files
4. Describe “Destruction of Email”.
5. List and explain the International Principles against Damaging of Computer Evidence.
6. Explain in detail about the tools needed for intrusion response to the destruction of data.

Unit IV

1. Explain E-bombs in detail.
2. Illustrate Email wiretaps, spy dust balls, Tracking Tots and mechanical dragonflies.
3. Explain the six technologies involved in PLS Architecture.
4. Describe Cyber footprint and criminal tracking.
5. Illustrate Implications of cookies and integrated platforms with examples.

Unit V

1. Illustrate advance encryption with examples.
2. Explain advance hacking in detail.
3. How a Hacker Works?
4. Describe Advanced Tracker Hackers.
5. Explain “The problem of present” and “Outlook for the Future”.