

Computer Forensics in Today's World

- Forensics Science
- Computer Forensics
 1. Security Incident Report
 2. Aspects of Organizational Security
 3. Evolution of Computer Forensics
 4. Objective of Computer Forensics
 5. Need for Compute Forensics
- Forensics Readiness
 1. Benefits of Forensics Readiness
 2. Goals of Forensics Readiness
 3. Forensics Readiness Planning
- Cyber Crime
 1. Computer Facilitated Crimes
 2. Modes of Attacks
 3. Examples of Cyber Crime
 4. Types of Computer Crimes
 5. Cyber Criminals
 6. Organized Cyber Crime: Organizational Chart
 7. How Serious are Different Types of Incidents?
 8. Disruptive Incidents to the Business
 9. Cost Expenditure Responding to the Security Incident
- Cyber Crime Investigation
 1. Key Steps in Forensics Investigation
 2. Rules of Forensics Investigation
 3. Need for Forensics Investigator
 4. Role of Forensics Investigator
 5. Accessing Computer Forensics Resources
 6. Role of Digital Evidence
- Corporate Investigations
 1. Understanding Corporate Investigations
 2. Approach to Forensics Investigation: A Case Study
 3. Instructions for the Forensic Investigator to Approach the Crime Scene
 4. Why and When Do You Use Computer Forensics?
 5. Enterprise Theory of Investigation (ETI)
 6. Legal Issues
 7. Reporting the Results

- Reporting a Cyber Crime
 1. Why you Should Report Cybercrime?
 2. Reporting Computer-Related Crimes
 3. Person Assigned to Report the Crime
 4. When and How to Report an Incident?
 5. Who to Contact at the Law Enforcement?
 6. Federal Local Agents Contact
 7. More Contacts
 8. CIO Cyberthreat Report Form