Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks.

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. CHFI investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information known as computer data recovery.

**Course Duration:** 120 Hours

**Pre-Requisite:** Basic Knowledge of Internet

**Free:** Online exam practice with CHFI lab environment, past 10 years exams and online practical lab access

**DLP Kit Includes:** Online Training and Tutor, Audio and Video Tutorials, Books, E-Books, Certification, Examination Fee, Registration Fee, Query Session, Audio and Video Conferencing, Online Exam and Fee

**Course Module.**

**Module 01: Computer Forensics in Today’s World**

1. Forensic Science
2. Computer Forensics
   2.1. Security Incident Report
   2.2. Aspects of Organizational Security
   2.3. Evolution of Computer Forensics
   2.4. Objectives of Computer Forensics
   2.5. Need for Computer Forensics
   2.6. Benefits of Forensic Readiness
   2.7. Goals of Forensic Readiness
   2.8. Forensic Readiness Planning
3. Cyber Crime
   3.1. Cybercrime
   3.2. Computer Facilitated Crimes
   3.3. Modes of Attacks
   3.4. Examples of Cyber Crime
   3.5. Types of Computer Crimes
   3.6. How Serious were Different Types of Incident?
   3.7. Disruptive Incidents to the Business
   3.8. Time Spent Responding to the Security Incident
   3.9. Cost Expenditure Responding to the Security Incident
4. Cyber Crime Investigation
   4.1. Cyber Crime Investigation
   4.2. Key Steps in Forensic Investigation
   4.3. Rules of Forensics Investigation
   4.4. Need for Forensic Investigator
   4.5. Role of Forensics Investigator
   4.6. Accessing Computer Forensics Resources
   4.7. Role of Digital Evidence
   4.8. Understanding Corporate Investigations
   4.9. Approach to Forensic Investigation: A Case Study
   4.10. When an Advocate Contacts the Forensic Investigator, He Specifies How to Approach the Crime Scene
   4.11. Where and When do you Use Computer Forensics
5. Enterprise Theory of Investigation (ETI)
6. Legal Issues
7. Reporting the Results

**Module 02: Computer Forensics Investigation Process**

1. Investigating Computer Crime
   1.1. Before the Investigation
1.2. Build a Forensics Workstation
1.3. Building Investigating Team
1.4. People Involved in Performing Computer Forensics
1.5. Review Policies and Laws
1.6. Forensics Laws
1.7. Notify Decision Makers and Acquire Authorization
1.8. Risk Assessment
1.9. Build a Computer Investigation Toolkit

2. Computer Forensic Investigation Methodology
2.1. Steps to Prepare for a Computer Forensic Investigation
2.2. Obtain Search Warrant
2.2.1. Example of Search Warrant
2.2.2. Searches Without a Warrant
2.3. Evaluate and Secure the Scene
2.3.1. Forensic Photography
2.3.2. Gather the Preliminary Information at Scene
2.3.3. First Responder
2.4. Collect the Evidence
2.4.1. Collect Physical Evidence
2.4.1.1. Evidence Collection Form
2.4.2. Collect Electronic Evidence
2.4.3. Guidelines in Acquiring Evidences
2.5. Secure the Evidence
2.5.1. Evidence Management
2.5.2. Chain of Custody
2.6. Acquire the Data
2.6.1. Duplicate the Data (Imaging)
2.6.2. Verify Image Integrity
2.6.3. Recover Lost or Deleted Data

2.7. Analyze the Data

2.7.1. Data Analysis

2.7.2. Data Analysis Tools

2.8. Assess Evidence and Case

2.8.1. Evidence Assessment

2.8.2. Case Assessment

2.8.3. Processing Location Assessment

2.8.4. Best Practices

2.9. Prepare the Final Report

2.9.1. Documentation in Each Phase

2.9.2. Gather and Organize Information

2.9.3. Writing the Investigation Report

2.9.4. Sample Report

2.10. Testify in the Court as an Expert Witness

2.10.1. Expert Witness

2.10.2. Testifying in the Court Room

2.10.3. Closing the Case

2.10.4. Maintaining Professional Conduct

2.10.5. Investigating a Company Policy Violation

2.10.6. Computer Forensics Service Providers

Module 03: Searching and Seizing of Computers

1. Searching and Seizing Computers without a Warrant

1.1. Searching and Seizing Computers without a Warrant

1.2. § A: Fourth Amendment’s “Reasonable Expectation of Privacy” in Cases Involving Computers: General Principles

1.3. § A.1: Reasonable Expectation of Privacy in Computers as Storage Devices

1.4. § A.3: Reasonable Expectation of Privacy and Third-Party Possession

1.5. § A.4: Private Searches
1.6. § A.5 Use of Technology to Obtain Information
1.7. § B: Exceptions to the Warrant Requirement in Cases Involving Computers
1.8. § B.1: Consent
1.9. § B.1.a: Scope of Consent
1.10. § B.1.b: Third-Party Consent
1.11. § B.1.c: Implied Consent
1.12. § B.2: Exigent Circumstances
1.13. § B.3: Plain View
1.14. § B.4: Search Incident to a Lawful Arrest
1.15. § B.5: Inventory Searches
1.16. § B.6: Border Searches
1.17. § B.7: International Issues
1.18. § C: Special Case: Workplace Searches
1.19. § C.1: Private Sector Workplace Searches
1.20. § C.2: Public-Sector Workplace Searches
2. Searching and Seizing Computers with a Warrant
2.1. Searching and Seizing Computers with a Warrant
2.2. A: Successful Search with a Warrant
2.3. A.1: Basic Strategies for Executing Computer Searches
2.4. § A.1.a: When Hardware Is Itself Contraband, Evidence, or an Instrumentality or Fruit of Crime
2.5. § A.1.b: When Hardware is Merely a Storage Device for Evidence of Crime
2.6. § A.2: The Privacy Protection Act
2.7. § A.2.a: The Terms of the Privacy Protection Act
2.8. § A.2.b: Application of the PPA to Computer Searches and Seizures
2.9. § A.3: Civil Liability Under the Electronic Communications Privacy Act (ECPA)
2.10. § A.4: Considering the Need for Multiple Warrants in Network Searches
2.11. § A.5: No-Knock Warrants
2.12. § A.6: Sneak-and-Peek Warrants
2.13. § A.7: Privileged Documents

2.14. § B: Drafting the Warrant and Affidavit

2.15. § B.1: Accurately and Particularly Describe the Property to be Seized in the Warrant and/or Attachments to the Warrant

2.16. § B.1.a: Defending Computer Search Warrants Against Challenges Based on the Description of the “Things to be Seized”

2.17. § B.2: Establish Probable Cause in the Affidavit

2.18. § B.3: In the Affidavit Supporting the Warrant, Include an Explanation of the Search Strategy as Well as the Practical & Legal Considerations That Will Govern the Execution of the Search

2.19. § C: Post-Seizure Issues

2.20. § C.1: Searching Computers Already in Law Enforcement Custody

2.21. § C.2: The Permissible Time Period for Examining Seized Computers

2.22. § C.3: Rule 41(e) Motions for Return of Property

3. The Electronic Communications Privacy Act

3.1. § The Electronic Communications Privacy Act

3.2. § A. Providers of Electronic Communication Service vs. Remote Computing Service

3.3. § B. Classifying Types of Information Held by Service Providers

3.4. § C. Compelled Disclosure Under ECPA

3.5. § D. Voluntary Disclosure

3.6. § E. Working with Network Providers

4. Electronic Surveillance in Communications Networks

4.1. Electronic Surveillance in Communications Networks

4.2. § A. Content vs. Addressing Information

4.3. § B. The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127


4.5. § C.1: Exceptions to Title III

4.6. § D. Remedies For Violations of Title III and the Pen/Trap Statute

5. Evidence

5.1. Evidence
Module 04: Digital Evidence

1. Digital Data
   1.1. Definition of Digital Evidence
   1.2. Increasing Awareness of Digital Evidence
   1.3. Challenging Aspects of Digital Evidence
   1.4. The Role of Digital Evidence
   1.5. Characteristics of Digital Evidence
   1.6. Fragility of Digital Evidence
   1.7. Anti-Digital Forensics (ADF)
   1.8. Types of Digital Data
   1.9. Rules of Evidence
   1.10. Best Evidence Rule
   1.11. Federal Rules of Evidence
   1.12. International Organization on Computer Evidence (IOCE)
   1.14. IOCE International Principles for Digital Evidences
   1.15. SWGDE Standards for the Exchange of Digital Evidence

2. Electronic Devices: Types and Collecting Potential Evidence
   2.1. Electronic Devices: Types and Collecting Potential Evidence

3. Evidence Assessment
   3.1. Digital Evidence Examination Process
   3.2. Evidence Assessment
   3.3. Prepare for Evidence Acquisition

4. Evidence Acquisition
4.1. Preparation for Searches
4.2. Seizing the Evidences
4.3. Imaging
4.4. Bit-stream Copies
4.5. Write Protection
4.6. Evidence Acquisition
4.7. Acquiring Evidence from Storage Devices
4.8. Collecting the Evidence
4.9. Collecting the Evidence from RAM
4.10. Collecting Evidence from Stand-Alone Network Computer
4.11. Chain of Custody
4.12. Chain of Evidence Form
5. Evidence Preservation
5.1. Preserving Digital Evidence: Checklist
5.2. Preserving Floppy and Other Removable Media
5.3. Handling Digital Evidence
5.4. Store and Archive
5.5. Digital Evidence Findings
6. Evidence Examination and Analysis
6.1. Evidence Examination
6.2. Physical Extraction
6.3. Logical Extraction
6.4. Analyze Host Data
6.5. Analyze Storage Media
6.6. Analyze Network Data
6.7. Analysis of Extracted Data
6.8. Timeframe Analysis
6.9. Data Hiding Analysis
6.10. Application and File Analysis

6.11. Ownership and Possession

7. Evidence Documentation and Reporting

7.1. Documenting the Evidence

7.2. Evidence Examiner Report

7.3. Final Report of Findings

7.4. Computer Evidence Worksheet

7.5. Hard Drive Evidence Worksheet

7.6. Removable Media Worksheet

8. Electronic Crime and Digital Evidence Consideration by Crime Category

Module 05: First Responder Procedures

1. Electronic Evidence

2. First Responder

3. Role of First Responder

4. Electronic Devices: Types and Collecting Potential Evidence

5. First Responder Toolkit

5.1. First Responder Toolkit

5.2. Creating a First Responder Toolkit

5.3. Evidence Collecting Tools and Equipment

6. First Response Basics

6.1. First Responder Rule

6.2. Incident Response: Different Situations

6.3. First Response for System Administrators

6.4. First Response by Non-Laboratory Staff

6.5. First Response by Laboratory Forensic Staff

7. Securing and Evaluating Electronic Crime Scene

7.1. Securing and Evaluating Electronic Crime Scene: A Check-list

7.2. Warrant for Search & Seizure
7.3. Planning the Search & Seizure
7.4. Initial Search of the Scene
7.5. Health and Safety Issues
8. Conducting Preliminary Interviews
8.1. Questions to ask When Client Calls the Forensic Investigator
8.2. Consent
8.3. Sample of Consent Search Form
8.4. Witness Signatures
8.5. Conducting Preliminary Interviews
8.6. Conducting Initial Interviews
8.7. Witness Statement Checklist
9. Documenting Electronic Crime Scene
9.1. Documenting Electronic Crime Scene
9.2. Photographing the Scene
9.3. Sketching the Scene
10. Collecting and Preserving Electronic Evidence
10.1. Collecting and Preserving Electronic Evidence
10.2. Order of Volatility
10.3. Dealing with Powered OFF Computers at Seizure Time
10.4. Dealing with Powered ON Computers at Seizure Time
10.5. Dealing with Networked Computer
10.6. Dealing with Open Files and Startup Files
10.7. Operating System Shutdown Procedure
10.8. Computers and Servers
10.9. Preserving Electronic Evidence
10.10. Seizing Portable Computers
10.11. Switched ON Portables
11. Packaging and Transporting Electronic Evidence
11.1. Evidence Bag Contents List
11.2. Packaging Electronic Evidence
11.3. Exhibit Numbering
11.4. Transporting Electronic Evidence
11.5. Handling and Transportation to the Forensics Laboratory
11.6. Storing Electronic Evidence
11.7. Chain of Custody

12. Reporting the Crime Scene

13. Note Taking Checklist

14. First Responder Common Mistakes

Module 06: Incident Handling

1. What is an Incident?
2. Security Incidents
3. Category of Incidents
3.1. Category of Incidents: Low Level
3.2. Category of Incidents: Mid Level
3.3. Category of Incidents: High Level
4. Issues in Present Security Scenario
5. How to identify an Incident?
6. How to prevent an Incident?

7. Defining the Relationship between Incident Response, Incident Handling, and Incident Management

8. Incident Management
8.1. Incident Management
8.2. Threat Analysis and Assessment
8.3. Vulnerability Analysis
8.4. Estimating Cost of an Incident
8.5. Change Control

9. Incident Reporting
9.1. Incident Reporting
9.2. Computer Incident Reporting
9.3. Whom to Report an Incident?
9.4. Report a Privacy or Security Violation
9.5. Preliminary Information Security Incident Reporting Form
9.6. Why don’t Organizations Report Computer Crimes?

10. Incident Response
10.1. Respond to a Security Incident
10.2. Security Incident Response (Detailed Form)
10.3. Incident response policies
10.4. Incident Response Checklist
10.5. Response Handling Roles
10.6. Incident Response: Roles and Responsibilities
10.6.1. SSM
10.6.2. ISSM
10.6.3. ISSO

10.8. Budget/Resource Allocation

11. Incident Handling
11.1. Handling Incidents
11.2. Procedure for Handling Incident
11.3. Preparation
11.4. Identification
11.5. Containment
11.6. Eradication
11.7. Recovery
11.8. Follow-up
11.9. Post-Incident Activity
11.10.  Education, Training, and Awareness
11.11.  Post Incident Report
11.12.  Procedural and Technical Countermeasures
11.13.  Vulnerability Resources

12.  CSIRT
12.1.  What is CSIRT?
12.2.  CSIRT: Goals and Strategy
12.3.  CSIRT Vision
12.4.  Motivation behind CSIRTs
12.5.  Why does an Organization need an Incident Response Team?
12.6.  Who works in a CSIRT?
12.7.  Staffing your Computer Security Incident Response Team: What are the Basic Skills Needed?
12.8.  Team Models
12.8.1.  Delegation of Authority
12.9.  CSIRT Services can be Grouped into Three Categories:
12.10.  CSIRT Case Classification
12.11.  Types of Incidents and Level of Support
12.12.  Service Description Attributes
12.13.  Incident Specific Procedures-I (Virus and Worm Incidents)
12.15.  Incident Specific Procedures-III (Social Incidents, Physical Incidents)
12.17.  US-CERT Incident Reporting System
12.18.  CSIRT Incident Report Form
12.19.  CERT(R) Coordination Center: Incident Reporting Form
12.20.  Example of CSIRT
12.21.1.  Step 1: Obtain Management Support and Buy-in
12.21.2. Step 2: Determine the CSIRT Development Strategic Plan

12.21.3. Step 3: Gather Relevant Information

12.21.4. Step 4: Design your CSIRT Vision

12.21.5. Step 5: Communicate the CSIRT Vision

12.21.6. Step 6: Begin CSIRT Implementation

12.21.7. Step 7: Announce the CSIRT

12.22. Limits to Effectiveness in CSIRTs

12.23. Working Smarter by Investing in Automated Response Capability

13. World CERTs

13.1. World CERTs

13.2. Australia CERT (AUSCERT)

13.3. Hong Kong CERT (HKCERT/CC)

13.4. Indonesian CSIRT (ID-CERT)

13.5. Japan CERT-CC (JPCERT/CC)

13.6. Singapore CERT (SingCERT)

13.7. Taiwan CERT (TWCERT)

13.8. China CERT (CNCERT/CC)

13.9. CERT-CC

13.10. US-CERT

13.11. Canadian Cert

13.12. Forum of Incident Response and Security Teams

13.13. CAIS

13.14. NIC BR Security Office Brazilian CERT

13.15. EuroCERT

13.16. FUNET CERT

13.17. DFN-CERT

13.18. JANET-CERT


13.21. IRTs Around the World

Module 07: Computer Forensics Lab

1. Setting a Computer Forensics Lab
   1.1. Computer Forensics Lab
   1.2. Planning for a Forensics Lab
   1.3. Budget Allocation for a Forensics Lab
   1.4. Physical Location Needs of a Forensic Lab
   1.5. Structural Design Considerations
   1.6. Environmental Conditions
   1.7. Electrical Needs
   1.8. Communication Needs
   1.9. Work Area of a Computer Forensics Lab
   1.10. Ambience of a Forensic Lab
   1.11. Ambience of a Forensic Lab: Ergonomics
   1.12. Physical Security Recommendations
   1.13. Fire-Suppression Systems
   1.14. Evidence Locker Recommendations
   1.15. Computer Forensics Investigator
   1.16. Law Enforcement Officer
   1.17. Forensic Lab Licensing Requisite
   1.18. Features of the Laboratory Imaging System
   1.19. Technical Specification of the Laboratory-based Imaging System
   1.20. Forensics Lab
   1.21. Auditing a Computer Forensics Lab
   1.22. Recommendations to Avoid Eyestrain
   1.23. Computer Forensic Labs, Inc
   1.24. Procedures at Computer Forensic Labs (CFL), Inc
1.25. Data Destruction Industry Standards

1.26. Case Study: San Diego Regional Computer Forensics Laboratory (RCFL)

2. Hardware Requirements

2.1. Equipment Required in a Forensics Lab

2.2. Forensic Workstations

2.3. Basic Workstation Requirements in a Forensic Lab

2.4. Stocking the Hardware Peripherals

2.4.1. Paraben Forensics Hardware

2.4.1.1. Handheld First Responder Kit

2.4.1.2. Wireless StrongHold Bag

2.4.1.3. Remote Charger

2.4.1.4. Device Seizure Toolbox

2.4.1.5. Wireless StrongHold Tent

2.4.1.6. Passport StrongHold Bag

2.4.1.7. Project-a-Phone

2.4.1.8. SATA Adaptor Male/ Data cable for Nokia 7110/6210/6310/i

2.4.1.9. Lockdown

2.4.1.10. SIM Card Reader/ Sony Client N & S Series Serial Data Cable

2.4.1.11. CSI Stick

2.4.1.12. Portable USB Serial DB9 Adapter

2.5. Portable Forensic Systems and Towers

2.5.1. Forensic Air-Lite VI MKII laptop

2.5.2. Portable Forensic Systems and Towers: Original Forensic Tower II

2.5.3. Portable Forensic Systems and Towers: Portable Forensic Workhorse V

2.5.4. Portable Forensic Workhorse V: Tableau 335 Forensic Drive Bay Controller

2.5.5. Portable Forensic Systems and Towers: Forensic Air-Lite IV MK II

2.5.6. Portable Forensic Systems and Towers: Forensic Tower II

2.6. Forensic Write Protection Devices and Kits: Ultimate Forensic Write Protection Kit
2.7. Tableau T3u Forensic SATA Bridge Write Protection Kit

2.8. Tableau T8 Forensic USB Bridge Kit/Addonics Mini DigiDrive READ ONLY 12-in-1 Flash Media Reader

2.9. Tableau TACC 1441 Hardware Accleerator

2.10. Multiple TACC1441 Units

2.11. Digital Intelligence Forensic Hardware

2.11.1. FRED SR (Dual Xeon)

2.11.2. FRED-L

2.11.3. Forensic Recovery of Evidence Data Center (FREDC)

2.11.4. Rack-A-TACC

2.11.5. FREDDIE

2.11.6. UltraKit

2.11.7. UltraBay

2.11.8. UltraBlock

2.11.9. Micro Forensic Recovery of Evidence Device (µFRED)

2.12. Wiebetimech

2.12.1. Forensics DriveDock

2.12.2. Forensics UltraDock v4

2.12.3. Drive eRazer

2.12.4. v4 Combo Adapters

2.12.5. ProSATA SS8

2.12.6. HotPlug

2.13. CelleBrite UFED System

2.14. DeepSpar:


2.14.2. 3D Data Recovery

2.14.3. Phase 1 Tool: PC-3000 Drive Restoration system:

2.14.4. Phase 2 Tool: DeepSpar Disk Imager

2.14.5. Phase 3 Tool: PC-3000 Data Extractor
2.15. InfinaDyne Forensic Products
2.15.1. Robotic Loader Extension for CD/DVD Inspector
2.15.2. Rimage Evidence Disc System
2.16. CD DVD Forensic Disc Analyzer with Robotic Disc Loader
2.17. Image MASSter
2.17.1. RoadMASSter- 3
2.17.2. Image MASSter –Solo-3 Forensic
2.17.3. Image MASSter –WipeMASSter
2.17.4. Image MASSter –DriveLock
2.17.5. Image MASSter: Serial-ATA DriveLock Kit USB/1394B
2.17.6. Image MASSter: DriveLock Firewire/USB
2.17.7. Image MASSter: DriveLock IDE
2.17.8. Image MASSter: DriveLock In Bay
2.18. Logicube:
2.18.1. Forensic MD5
2.18.2. Forensic Talon *
2.18.3. RAID I/O Adapter ™
2.18.4. GPStamp™
2.18.5. Portable Forensic Lab™
2.18.6. CellDEK *
2.18.7. Omniport
2.18.8. Desktop write PROtecs
2.18.9. USB adapters
2.18.10. Adapters
2.18.11. Cables
2.19. Power Supplies and Switches
2.20. DIBS Mobile Forensic Workstation
2.21. DIBS Advanced Forensic Workstation
2.22. DIBS® RAID: Rapid Action Imaging Device

2.23. Forensic Archive and Restore Robotic Devices: Forensic Archive and Restore (FAR Pro)

3. Software Requirements

3.1. Basic Software Requirements in a Forensic Lab

3.2. Maintain Operating System and Application Inventories

3.3. Paraben Forensics Software: Device Seizure

3.4. Paraben Hard Drive Forensics: P2 Commander

3.5. Crucial Vision

3.6. Paraben Hard Drive Forensics: P2 eXplorer

3.7. InfinaDyne Forensic Products

3.7.1. CD/DVD Inspector

3.7.2. AccuBurn-R for CD/DVD Inspector

3.7.3. Flash Retriever Forensic Edition

3.7.4. ThumbsDisplay

3.8. TEEL Technologies SIM Tools

3.8.1. SIMIS

3.8.2. SIMulate

3.8.3. SIMgen

3.9. LiveDiscover™ Forensic Edition

3.10. Tools: LiveWire Investigator

Module 08: Understanding Hard Disks and File Systems

1. Hard Disk

1.1. Disk Drive Overview

1.2. Physical Structure of Hard Disk

1.3. Logical Structure of Hard Disk

1.4. Types of Hard Disk Interfaces

1.4.1. Types of Hard Disk Interfaces: SCSI

1.4.2. Types of Hard Disk Interfaces: IDE/EIDE
1.4.3. Types of Hard Disk Interfaces: USB
1.4.4. Types of Hard Disk Interfaces: ATA
1.4.5. Types of Hard Disk Interfaces: Fibre Channel
1.5. Disk Platter
1.6. Tracks
1.7. Tracks Numbering
1.8. Sector
1.9. Sector Addressing
1.10. Cluster
1.10.1. Cluster Size
1.10.2. Slack Space
1.10.3. Lost Clusters
1.10.4. Bad Sector
1.10.5. Disk Capacity Calculation
1.10.6. Measuring the Performance of Hard Disk
2. Disk Partitions
2.1. Disk Partitions
2.2. Master Boot Record
3. Boot Process
3.1. Windows XP System Files
3.3. http://www.bootdisk.com
4. File Systems
4.1. Understanding File Systems
4.2. Types of File Systems
4.3. List of Disk File Systems
4.4. List of Network File Systems
4.5. List of Special Purpose File Systems
4.6. Popular Linux File Systems
4.7. Sun Solaris 10 File System: ZFS
4.8. Mac OS X File System
4.9. Windows File Systems
4.10. CD-ROM / DVD File System
4.11. Comparison of File Systems
5. FAT32
5.1. FAT
5.2. FAT Structure
5.3. FAT32
6. NTFS
6.1. NTFS
6.2. NTFS Architecture
6.3. NTFS System Files
6.4. NTFS Partition Boot Sector
6.5. NTFS Master File Table (MFT)
6.6. NTFS Metadata File Table (MFT)
6.7. Cluster Sizes of NTFS Volume
6.8. NTFS Files and Data Storage
6.9. NTFS Attributes
6.10. NTFS Data Stream
6.11. NTFS Compressed Files
6.12. NTFS Encrypted File Systems (EFS)
6.13. EFS File Structure
6.14. EFS Recovery Key Agent
6.15. EFS Key
6.16. Deleting NTFS Files
6.17. Registry Data
6.18. Examining Registry Data
6.19. FAT vs. NTFS
7. Ext3
7.1. Ext2
7.2. Ext3
8. HFS and CDFS
8.1. HFS
8.2. CDFS
9. RAID Storage System
9.1. RAID Storage System
9.2. RAID Levels
9.3. Recover Data from Unallocated Space using File Carving Process
10. Hard Disk Evidence Collector Tools
10.1. Evidor
10.2. WinHex
10.3. Logicube: Echo PLUS
10.4. Logicube: Sonix
10.5. Logicube: OmniClone Xi
10.6. Logicube: OmniWipe
10.7. Logicube: CloneCard Pro
10.8. ImageMASSter: ImageMASSter 40008i
10.9. eDR Solutions: Hard Disk Crusher

Module 09: Digital Media Devices
1. Digital Storage Devices
1.1. Digital Storage Devices
1.2. Magnetic Tape
1.3. Floppy Disk
1.4. Compact Disk
1.5. CD-ROM
1.6. DVD
1.7. DVD-R, DVD+R, and DVD+R(W)
1.8. DVD-RW, DVD+RW
1.9. DVD+R DL/ DVD-R DL/ DVD-RAM
1.10. Blu-Ray
1.11. Network Attached Storage (NAS)
1.12. iPod
1.13. Zune
1.14. Flash Memory Cards
1.15. Secure Digital (SD) Memory Card
1.16. Secure Digital High Capacity (SDHC) Card
1.17. Secure Digital Input Output (SDIO) Card
1.18. Compact Flash (CF) Memory Card
1.19. Memory Stick (MS) Memory Card
1.20. Multi Media Memory Card (MMC)
1.21. xD-Picture Card (xD)
1.22. SmartMedia Memory (SM) Card
1.23. Solid state drives
1.24. Tape Libraries and Autoloaders
1.25. Barracuda Hard Drives
1.26. Hybrid Hard Drive
1.27. Holographic Data Storage
1.28. ExpressCard
1.29. USB Flash Drives
1.30. USB Flash in a Pen
1.31. E-ball Futuristic Computer

2. Different Models of Digital Devices
2.1. Different Types of Pocket Hard Drives

2.2. Different Types of Network-Attached Storage Devices

2.3. Different Types of Digital Camera Devices

2.4. Different Types of Mini Digital Cameras

2.5. Different Types of Digital Video Cameras

2.6. Different Types of Mobile Devices

2.7. Mobile Devices in the Future

2.8. Different Types of Digital Audio Players

2.9. Different Types of Digital Video Players

2.10. Different Types of Laptop computers

2.11. Solar Powered Concept for Laptop Gadget

2.12. Different Types of Bluetooth Devices

2.13. Different Types of USB Drives

Module 10: CD/DVD Forensics

1. Compact Disk

2. Types of CDs

3. Digital Versatile Disk (DVD)

4. DVD-R and DVD+R

5. DVD-RW and DVD+RW

6. DVD+R DL, DVD-R DL, DVD-RAM

7. HD-DVD (High Definition DVD)

8. HD-DVD

9. Blu-Ray

10. SID Code

11. How Criminal uses CD/DVD for Crime

12. Pre-Requisite for CD/DVD Forensics

13. Steps for CD Forensics

13.1. Collect the CD/DVD Evidences
13.2. Precautions while Collecting the Evidences
13.3. Document the Scene
13.4. Preserve the Evidences
13.5. Create Image of CD/DVD
13.6. Recover Data from Damaged or Corrupted CDs/DVDs
13.7. Data Analysis
14. Identify Pirated CD/DVDs
15. Original and Pirated CD/DVDs
16. CD/DVD Imaging Tools
16.1. UltraISO
16.2. MagicISO
16.3. Cdmage
16.4. Alcohol
16.5. Nero
17. CD/DVD Data Recovery Tools
17.1. CDRoller
17.2. Badcopy Pro
17.3. Multi Data Rescue
17.4. InDisk Recovery
17.5. Stellar Phoenix -CD Data Recovery Software
17.6. CD Recovery Toolbox
17.7. IsoBuster
17.8. CD/DVD Inspector
17.9. Acodisc CD & DVD Data Recovery Services

Module 11: Windows Linux Macintosh Boot Process
1. Terminologies
2. Boot Loader
3. Boot Sector
4. Anatomy of MBR

5. Windows Boot Sequence

6. Linux Boot Sequence

7. Macintosh Boot Sequence

8. Windows XP Boot Process

8.1. Windows XP Boot Process

9. Linux Boot Process

9.1. Common Startup Files in UNIX

9.2. List of Important Directories in UNIX

10. Linux Boot Process Steps

10.1. Step 1: The Boot Manager

10.1.1. GRUB: Boot Loader

10.2. Step 2: init

10.2.1. Step 2.1: /etc/inittab

10.2.2. Run Levels

10.2.3. The Run Level Scripts

10.2.4. How Processes in Runlevels Start

10.2.5. The Run Level Actions

10.3. Step 3: Services

10.4. Step 4: More inittab

10.4.1. Operating Modes

11. Macintosh Boot Process

11.1. Mac OS X

11.2. Mac OS X Hidden Files

11.3. Booting Mac OS X

11.4. Mac OS X Boot Options

11.5. The Mac OS X Boot Process

Module 12: Windows Forensics I
1. Volatile Information
2. Non-volatile Information
3. Collecting Volatile Information
   3.1. System Time
   3.2. Logged-on-Users
   3.3. Open Files
   3.4. Net file Command
   3.5. Psfile Tool
   3.6. Openfiles Command
   3.7. NetBIOS Name Table Cache
   3.8. Network Connections
   3.9. Netstat with the --ano Switch
4. Netstat with the --r Switch
   4.1. Process Information
   4.2. Tlist Tool
   4.3. Tasklist Command
   4.4. Pslist Tool
   4.5. Listdlls Tool
   4.6. Handle Tool
   4.7. Process-to-Port Mapping
   4.8. Netstat Command
   4.9. Fport Tool
   4.10. Openports Tool
   4.11. Network Status
   4.12. Ipconfig Command
   4.13. Promiscdetect Tool
   4.14. Promqry Tool
   4.15. Other Important Information
5. Collecting Nonvolatile Information
   5.1. Collecting Nonvolatile Information
   5.2. Examining File Systems
   5.3. Registry Settings
   5.4. Microsoft Security ID
   5.5. Event Logs
   5.6. Index.dat File
   5.7. Devices and Other Information
   5.8. Slack Space
   5.9. Virtual Memory
   5.10. Tool: DriveSpy
   5.11. Swap File
   5.12. Windows Search Index
   5.13. Tool: Search Index Examiner
   5.14. Collecting Hidden Partition Information
   5.15. Hidden ADS Streams
   5.16. Investigating ADS Streams

6. Windows Memory Analysis
   6.1. Windows Memory Analysis
   6.2. Importance of Memory Dump
   6.3. EProcess Structure
   6.4. Process Creation Mechanism
   6.5. Parsing Memory Contents
   6.6. Parsing Process Memory
   6.7. Extracting the Process Image
   6.8. Collecting Process Memory

7. Windows Registry Analysis
   7.1. Inside the Registry
8.5. Forensic Tool: Cache Monitor
8.6. Tool - IE History Viewer
8.7. IE Cookie Analysis
8.8. Investigating Internet Traces
8.9. Tool – IECookiesView
8.10. Tool- IE Sniffer
9. MD5 Calculation
9.1. MD5 Calculation
9.2. MD5 Algorithm
9.3. MD5 Pseudocode
9.4. MD5 Generator: Chaos MD5
9.5. Secure Hash Signature Generator
9.6. MD5 Generator: Mat-MD5
9.7. MD5 Checksum Verifier 2.1
10. Windows File Analysis
10.1. Recycle Bin
10.2. System Restore Points
10.3. Prefetch Files
10.4. Shortcut Files
10.5. Searching with Event Viewer
10.6. Word Documents
10.7. PDF Documents
10.8. Image Files
10.9. File Signature Analysis
10.10. NTFS Alternate Data Streams
10.11. Executable File Analysis
10.12. Documentation Before Analysis
10.13. Static Analysis Process
10.14. Search Strings  
10.15. PE Header Analysis  
10.16. Import Table Analysis  
10.17. Export Table Analysis  
10.18. Dynamic Analysis Process  
10.19. Creating Test Environment  
10.20. Collecting Information Using Tools  
10.21. Dynamic Analysis Steps  

11. Metadata Investigation  
11.1. Metadata  
11.2. Types of Metadata  
11.3. Metadata in Different File System  
11.4. Viewing Metadata  
11.5. MetaViewer  
11.6. Metadata Analyzer  
11.7. iScrub  

Module 13: Windows Forensics II  
1. Text Based Log  
1.1. Understanding Events  
1.2. Event Record Structure  
1.3. Vista Event Logs  
1.4. IIS Logs  
1.5. Parsing IIS Logs  
1.6. Parsing FTP Logs  
1.7. Parsing DHCP Server Logs  
1.8. Parsing Windows Firewall Logs  
1.9. Using the Microsoft Log Parser  
2. Other Audit Events
2.1. Evaluating Account Management Events
2.2. Examining Audit Policy Change Events
2.3. Examining System Log Entries
2.4. Examining Application Log Entries

3. Forensic Analysis of Event Logs
3.1. Using EnCase to Examine Windows Event Log Files
3.2. Windows Event Log Files Internals
3.3. Window Password Issues
3.4. Understanding Windows Password Storage
3.5. Cracking Windows Passwords Stored on Running Systems
3.7. Sniffing and Cracking Windows Authentication Exchanges
3.8. Cracking Offline Passwords

4. Forensics Tools
4.1. Helix
4.2. Tools Present in Helix CD for Windows Forensics
4.3. Helix Tool: SecReport
4.4. Helix Tool: Windows Forensic Toolchest (WFT)
4.5. Built-in Tool: Sigverif
4.6. Word Extractor
4.7. Registry Viewer Tool: RegScanner
4.8. Pmdump
4.9. System Scanner
4.10. Integrated Windows Forensics Software: X-Ways Forensics
4.11. Tool - Traces Viewer
4.12. Traces Viewer: Images
4.13. Traces Viewer: Pages
4.14. Traces Viewer: Other
Module 14: Linux Forensics

1. Introduction to Linux

1.1. Introduction of Linux OS
1.2. Linux Boot Sequence
1.3. File System in Linux
1.4. File System Description
1.5. Linux Forensics

1.6. Use of Linux as a Forensics Tool
1.7. Advantages of Linux in Forensics
1.8. Disadvantages of Linux in Forensics
1.9. Precautions During Investigation
1.10. Recognizing Partitions in Linux
1.11. Mount Command
1.12. dd command options
1.13. Floppy Disk Analysis
1.14. Hard Disk Analysis

2. Data Collection

2.1. Forensic Toolkit Preparation
2.2. Data Collection using the Toolkit
2.3. Keyword Searching
2.4. Linux Crash Utility
2.5. Linux Crash Utility: Commands

2.5.1. Crash> ps
2.5.2. crash> ps -t
2.5.3.  crash> ps -a
2.5.4.  crash> foreach files
2.5.5.  crash> foreach net
3.  Case Examples
3.1.  Case Example I
3.1.1.  Step-by-Step Approach to Case
3.1.2.  Challenges In Disk Forensics With Linux
3.2.  Case Example II
3.2.1.  Jason Smith Case
3.2.2.  Step-by-Step Approach to Case
4.  Linux Forensics Tools
4.1.  Popular Linux Forensics Tools
4.1.1.  The Sleuth Kit
4.1.2.  Tools in “The Sleuth Kit”
4.2.  Autopsy
4.2.1.  The Evidence Analysis Techniques in Autopsy
4.2.1.1.  File Listing
4.2.1.2.  File Content
4.2.1.3.  Hash Databases
4.2.1.4.  File Type Sorting
4.2.1.5.  Timeline of File Activity
4.2.1.6.  Keyword Search
4.2.1.7.  Meta Data Analysis
4.2.1.8.  Data Unit Analysis
4.2.1.9.  Image Details
5.  SMART for Linux
5.1.  Features of SMART for Linux
6.  Penguin Sleuth
6.1. Tools Included in Penguin Sleuth Kit

7. THE FARMAER’S BOOT CD
7.1. Delve

8. Forensix

9. Maresware

10. Major Programs Present in Maresware

11. Captain Nemo

12. The Coroner’s Toolkit (TCT)

13. Tool: FLAG

14. Tool: Md5deep

15. Tool: TestDisk

16. Tool: Vinetto

Module 15: Mac Forensics

1. Mac OS and File Systems
1.1. Mac OS X

1.2. Partitioning Schemes
1.2.1. Apple Partition Map (APM)
1.2.2. Apple Partition Map Entry Record
1.2.3. GUID Partition Table

1.3. Mac OS X File System
1.3.1. HFS+ File System

1.4. Mac OS X Directory Structure

1.5. Mac Security Architecture Overview

2. Mac Forensics: Collecting Evidence
2.1. Pre-requisites for Mac Forensics

2.2. Obtaining System Date and Time

2.3. Single User Mode

2.4. Determining and Resetting Open Firmware Password
2.5. Checking Plist Files
2.6. Collect User Home Directory Information
2.7. Forensics Information in User Library Folder
2.8. Collect User Accounts Information
2.9. User IDs
2.10. Gather user information from plist files
2.11. Use Spotlight for Keyword Search
2.12. Collecting Information Regarding Parental Controls for Local Account
2.13. File Vault and Mac OS X Security
2.15. POSIX Permissions
2.15.1. Viewing POSIX Permissions
2.16. Viewing ACL Permissions
2.17. Mac OS X Log Files
2.18. Locating iChat Configuration File
2.19. Viewing iChat Logs
2.20. Gathering Safari Information
2.21. Checking Wi-Fi Support
2.22. Checking Bluetooth Support
2.23. Vulnerable Features of Mac
3. Mac Forensics: Imaging
3.1. Imaging a Target Macintosh
3.1.1. Target Disk Mode
3.1.2. LiveCD Method
3.1.3. Drive Removal
3.2. Acquiring the Encrypted User Home Directory
3.3. .Mac and Related Evidence
3.4. Quick View Plus
3.5. Cover Flow

4. Mac Forensics: Tools
   4.1. gpart
   4.2. MadLockPick
   4.3. File Juicer
   4.4. MacAnalysis
   4.5. MacQuisition
   4.6. FTK Imager
   4.7. dd_rescue
   4.8. md5deep
   4.9. Foremost
   4.10. Mac forensic lab
   4.11. LinkMASSter

Module 16: Data Acquisition and Duplication

1. Data Acquisition
   1.1. Data Acquisition
   1.2. Types of data acquisition systems
   1.3. Determining the Best Acquisition Methods
   1.4. Data Recovery Contingencies
   1.5. Data Acquisition Mistakes

2. Data Duplication
   2.1. Issues with Data Duplication
   2.2. Data Duplication in Mobile Multi-database System
   2.3. Data Duplication System Used in USB Devices
   2.4. Data Backup

3. Data Acquisition Tools and Commands
   3.1. MS-DOS Data Acquisition Tool: DriveSpy
       3.1.1. Using Windows Data Acquisition Tools
3.1.2. FTK Imager

3.2. Acquiring Data on Linux
3.2.1. dd command
3.2.2. Extracting the MBR
3.2.3. Netcat Command
3.2.4. dd command (Windows XP Version)
3.2.5. Mount Image Pro
3.2.6. Snapshot Tool

3.3. Snapback DatArrest
3.3.1. Data Acquisition Toolbox
3.3.2. Data Acquisition Tool: SafeBack

3.4. Hardware Tool: Image MASSter Solo-3 Forensic
3.4.1. Image MASSter --RoadMASSter- 3
3.4.2. Image MASSter --WipeMASSter
3.4.3. Image MASSter --DriveLock

3.5. Hardware Tool: LinkMASSter-2
3.6. Hardware Tool: RoadMASSter-2

3.7. Logicube: ECHOPLUS & Sonix
3.8. Logicube: OmniClone Xi series
3.9. Logicube: OmniPORT
3.10. Logicube: OmniWipe & Clone Card Pro
3.11. Logicube: Forensic MD5
3.12. Logicube: Forensic Talon
3.13. Logicube: RAID I/O Adapter
3.14. Logicube: GPStamp
3.15. Logicube: Portable Forensic Lab
3.16. Logicube: CellDEK
3.17. Logicube: Desktop write PROtects
Module 17: Recovering Deleted Files and Deleted Partitions

1. Recovering Deleted Files

1.1. Deleting Files

1.2. What happens when a File is deleted in Windows?

1.3. Recycle Bin in Windows

1.3.1. Storage Locations of Recycle Bin in FAT and NTFS System

1.3.2. How The Recycle Bin Works

1.4. Damaged or Deleted INFO File
1.5. Damaged Files in Recycled Folder
1.6. Damaged Recycle Folder
1.7. How to Undelete a File
1.8. Data Recovery in Linux
1.9. Tools to Recover Deleted Files
1.9.1. Tool: Search and Recover
1.9.2. Tool: Zero Assumption Digital Image Recovery
1.9.3. Tool: e2Undel
1.9.4. Tool: R-linux
1.9.5. Tool: O&O Unerase
1.9.6. Tool: Restorer 2000
1.9.7. Tool: Badcopy Pro
1.9.8. Tool: File Scavenger
1.9.9. Tool: Mycroft V3
1.9.10. Tool: PC ParaChute
1.9.11. Tool: Stellar Phoenix
1.9.12. Tool: Filesaver
1.9.13. Tool: Virtual Lab
1.9.14. Tool: Drive and Data Recovery
1.9.15. Tool: Active@ UNERASER - DATA Recovery
1.9.16. Tool: Restoration
1.9.17. Tool: PC Inspector File Recovery
1.9.18. Tool: PC Inspector Smart Recovery
1.9.19. Tool: Fundelete
1.9.20. Tool: RecoverPlus Pro
1.9.21. Tool: OfficeFIX
1.9.22. Tool: Recover My Files
1.9.23. Tool: Zero Assumption Recovery
1.9.24. Tool: SuperFile Recover
1.9.25. Tool: IsoBuster
1.9.26. Tool: CDRoller
1.9.27. Tool: DiskInternals Uneraser
1.9.28. Tool: DiskInternal Flash Recovery
1.9.29. Tool: DiskInternals NTFS Recovery
1.9.30. Recover lost/deleted/corrupted files on CDs and DVDs
1.9.31. Tool: Undelete
1.9.32. Tool: Active@ UNDELETE
1.9.33. Data Recovery Tool: CD Data Rescue
1.9.34. Tool: File Recover
1.9.35. Tool: WinUndelete
1.9.36. Tool: R-Undelete
1.9.37. Tool: Image Recall
1.9.38. Tool: eIMAGE Recovery
1.9.39. Tool: Recover4all Professional
1.9.40. Tool: eData Unerase
1.9.41. Tool: Easy-Undelete
1.9.42. InDisc Recovery
1.9.43. TOKIWA DataRecovery
1.9.44. Data Recovery Wizard Professional
1.9.45. CD Recovery Toolbox
1.9.46. Smart Protector-Internet Eraser
1.9.47. Active@ File Recovery
1.9.48. SoftPerfect File Recovery
1.9.49. Partition Recovery
1.9.50. FinalRecovery
1.9.51. Mutilate File Wiper
1.9.52. Repair My Excel
1.9.53. Repair Microsoft Word Files
1.9.54. Zip Repair
1.9.55. Canon RAW File Recovery Software

2. Recovering Deleted Partitions
2.1. Deletion of Partition
2.2. Deletion of Partition using Windows
2.3. Deletion of Partition using Command Line
2.4. Recovery of Deleted Partition
2.5. Recovering Deleted Partition Tools
2.5.1. GetDataBack
2.5.2. DiskInternals Partition Recovery
2.5.3. Active@ Partition Recovery
2.5.4. Handy Recovery
2.5.5. Acronis Recovery Expert
2.5.6. Active@ Disk Image
2.5.7. TestDisk
2.5.8. Recover It All!
2.5.9. Scaven
2.5.10. Partition Table Doctor
2.5.11. NTFS Deleted Partition Recovery
2.5.12. Flash Retriever Forensic
2.5.13. ThumbsDisplay

Module 18: Forensics Investigations Using AccessData FTK
1. Forensic Toolkit (FTK®)
2. Features of FKT
3. Installation of FTK
3.1. Software Requirement
3.2. Installing FTK
3.3. FTK Installation
3.4. Codemeter Stick Installation
3.5. Oracle Installation
3.6. Single Computer Installation
3.7. Choosing An Evidence Server
3.8. Installing the KFF Library
3.9. Installing on Separate Computers
4. Starting with FTK
4.1. Starting FTK
4.2. Setting Up The Application Administrator
4.3. Case Manager Window
4.4. Toolbar Components
4.5. Properties Pane
4.6. Hex Interpreter Pane
4.7. Web Tab
4.8. Filtered Tab
4.9. Text Tab
4.10. Hex Tab
4.11. Explore Tab
4.12. Quickpicks Filter
4.13. Data Processing Status Dialog
4.14. Overview Tab
4.15. Email Tab
4.16. Graphics Tab
4.17. Thumbnails Pane
4.18. Bookmarks Tab
4.19. Live Search Tab
4.20. Index Search Tab
4.21. Creating Tabs
4.22. Launching FKT

5. Working with FTK
5.1. Creating A Case
5.2. Evidence Processing Options
5.3. Selecting Data Carving Options
5.4. Selecting Evidence Discovery Options
5.5. Selecting Evidence Refinement (Advanced) Options
5.6. Selecting Index Refinement (Advanced) Options
5.7. Refining an Index by File Date/Size
5.8. Adding Evidence
5.9. Backing Up the Case
5.10. Restoring a Case
5.11. Deleting a Case

6. Working with Cases
6.1. Opening an Existing Case
6.2. Adding Evidence
6.3. Selecting a Language
6.4. Additional Analysis
6.5. Properties Tab
6.6. The Hex Interpreter Tab
6.7. Using The Bookmark Information Pane
6.8. Creating a Bookmark
6.9. Bookmarking Selected Text
6.10. Adding Evidence to an Existing Bookmark
6.11. Moving A Bookmark
6.12. Removing A Bookmark
6.13. Deleting Files From A Bookmark

6.14. Verifying Drive Image Integrity

6.15. Copying Information From FTK

6.16. Exporting File List Info

6.17. Exporting the Word List

6.18. Creating a Fuzzy Hash Library

6.19. Selecting Fuzzy Hash Options During Initial Processing

6.20. Additional Analysis Fuzzy Hashing

6.21. Comparing Files Using Fuzzy Hashing

6.22. Viewing Fuzzy Hash Results

7. Searching a Case

7.1. Conducting A Live Search

7.2. Customizing The Live Search Tab

7.3. Documenting Search Results

7.4. Using Copy Special to Document Search Results

7.5. Bookmarking Search Results

8. Data Carving

8.1. Data carving

8.2. Data Carving Files In An Existing Case

9. Using Filters

9.1. Creating A Filter

9.2. Refining A Filter

9.3. Deleting A Filter

10. Decrypting Encrypted Files

10.1. Decrypting Files And Folders

10.2. Viewing Decrypted Files

10.3. Decrypting Domain Account EFS Files

10.4. Decrypting Credant Files
10.5. Decrypting Safeguard Utimaco Files

11. Working with Reports

12. Creating A Report
12.1. Saving Settings
12.2. Entering Basic Case Information
12.3. Including Bookmarks
12.4. Including Graphics
12.5. Selecting a File Path List
12.6. Selecting a File Properties List
12.7. Registry Selections
12.8. Selecting the Report Location
12.9. HTML Case Report
12.10. PDF Report

13. Customizing the Interface
13.1. Creating Custom Tabs
13.2. Customizing File List Columns
13.3. Creating and Modifying Column Settings

Module 19: Forensics Investigations Using EnCase

1. Evidence File
2. Verifying Evidence Files
3. Evidence File Format
4. Verifying File Integrity
5. Hashing
6. Acquiring Image
7. Configuring EnCase
8. View Menu
9. Device Tab
10. Viewing Files and Folders
11. Bottom Pane
12. Viewers in Bottom Pane
13. Status Bar
14. Searching
15. Keywords
16. Adding Keywords
17. Grouping
18. Add multiple Keywords
19. Starting the Search
20. Search Hits Tab
21. Search Hits
22. Bookmarks
23. Creating Bookmarks
24. Adding Bookmarks
25. Bookmarking Selected Data
26. Recovering Deleted Files/folders in FAT Partition
27. Viewing Recovered Files
28. Recovering Folders in NTFS
29. Master Boot Record (MBR)
30. Bookmark Data
31. NTFS Starting Point
32. Viewing Disk Geometry
33. Recovering Deleted Partitions
34. Hash Values
35. Creating Hash Sets
36. MD5 Hash
37. Creating Hash
38. Viewers
Module 20: Steganography

1. Steganography
2. Model of Stegosystem
3. Application of Steganography
4. Classification of Steganography
   4.1. Technical Steganography
   4.2. Linguistic Steganography
5. Digital Steganography Techniques
   5.1. Injection
   5.2. Least Significant Bit (LSB)
   5.3. Transform Domain Techniques
   5.4. Spread Spectrum Techniques
   5.5. Perceptual Masking
6. Cover Generation Technique
7. Statistical Method Technique
8. Distortion Technique
9. Different Forms of Steganography
   9.1. Text File Steganography
   9.2. Image File Steganography
      9.2.1. Steganography Technique in Image File
      9.2.2. Least Significant Bit Insertion in Image Files
      9.2.3. Process of Hiding Information in Image Files
9.2.4. Masking and Filtering in Image Files
9.2.5. Algorithms and Transformation
9.3. Audio File Steganography
9.3.1. Low-bit Encoding in Audio Files
9.3.2. Phase Coding
9.3.3. Spread Spectrum
9.3.4. Echo Data Hiding
9.4. Video File Steganography
10. Steganographic File System
11. Issues in Information Hiding
11.1. Levels of Visibility
11.2. Robustness vs. Payload
11.3. File Format Dependence
12. Cryptography
13. Model of Crypto System
14. Steganography vs. Cryptography
15. Public Key Infrastructure (PKI)
16. Key Management Protocols
17. Watermarking
17.1. What is Watermarking?
17.2. Case Study
17.3. Steganography vs. Watermarking
17.4. Types of Watermarks
17.4.1. Visible Watermarks
17.4.2. Invisible Watermarks
17.5. Working of Different Watermarks
17.6. Attacks on Watermarking
17.7. Application of Watermarking
17.8. Currency Watermarking

17.9. Digimarc's Digital Watermarking

17.10. Watermarking – Mosaic Attack

17.10.1. Mosaic Attack – Javascript code

17.10.2. 2Mosaic – Watermark breaking Tool

18. Steganography Detection

18.1. How to Detect Steganography?

18.2. Detecting Steganography

18.3. Detecting Text, Image, Audio and Video Steganography

18.4. Counterfeit Detection

19. Steganalysis

19.1. Steganalysis Methods/Attacks on Steganography

19.1.1. Attack Types

19.1.2. Stego Only Attack

19.1.3. Known Cover Attack

19.1.4. Known Message Attack

19.1.5. Known Stego Attack

19.1.6. Chosen Stego Attack

19.1.7. Disabling or Active Attack

19.1.8. Chosen Message Attack

19.1.9. Disabling or Active Attacks

19.1.10. Blur

19.1.11. Noise

19.1.12. Noise Reduction

19.1.13. Sharpen


19.1.15. Resample

19.1.16. Soften
20. Introduction to Stego-Forensics
21. Steganography in the Future
22. Hiding Information in DNA
23. Unethical Use of Steganography
24. TEMPEST
25. Emissions Security (EMSEC)
26. Van Eck phreaking
27. Legal Use of Steganography
28. Steganography Tools
28.1. S-Tools
28.2. Steghide
28.3. Mp3Stego
28.4. Invisible Secrets 4
28.5. Stegdetect
28.6. Steg Suite
28.7. Stego Watch
28.8. Snow
28.9. Fort Knox
28.10. Image Hide
28.11. Blindside
28.12. Camera/Shy
28.13. Gifshuffle
28.14. Data Stash
28.15. JPHIDE and JPSEEK
28.16. wbStego
28.17. OutGuess
28.18. Masker
28.19. Cloak
28.20. StegaNote
28.21. Stegomagic
28.22. Hermetic Stego
28.23. StegSpy
28.24. Stealth
28.25. WNSTORM
28.26. Xidie
28.27. CryptArkan
28.28. Info Stego
28.29. Scramdisk
28.30. Jpegx
28.31. CryptoBola
28.32. ByteShelter I
28.33. Camuflage
28.34. Stego Analyst
28.35. Steganos
28.36. Pretty Good Envelop
28.37. Hydan
28.38. EzStego
28.39. Steganosaurus
28.40. appendX
28.41. Stego Break
28.42. Stego Hunter
28.43. StegParty
28.44. InPlainView
28.45. Z-File
28.46. MandelSteg and GIFExtract

Module 21: Image Files Forensics
1. Common Terminologies
2. Introduction to Image Files
   2.1. Understanding Vector Images
   2.2. Understanding Raster Images
   2.3. Metafile Graphics
3. Image File Formats
   3.1. Understanding Image File Formats
      3.1.1. GIF (Graphics Interchange Format)
      3.1.2. JPEG (Joint Photographic Experts Group)
      3.1.3. JPEG File Structure
      3.1.4. JPEG 2000
      3.1.5. BMP (Bitmap) File
      3.1.6. BMP File Structure
      3.1.7. PNG (Portable Network Graphics)
      3.1.8. Tagged Image File Format (TIFF)
      3.1.9. TIFF File Structure
      3.1.10. ZIP (Zone Information Protocol)
3.2. Best Practices for Forensic Image Analysis
4. Use MATLAB for Forensic Image Processing
   4.1. Advantages of MATLAB
5. Data Compression
   5.1. How File Compression Works?
   5.2. Understanding Data Compression
   5.3. Huffman Coding Algorithm
   5.4. Lempel-Ziv Coding Algorithm
   5.5. Lossy Compression
   5.6. Vector Quantization
6. Locating and Recovering Image Files
6.1. Locating and Recovering Image Files
6.2. Analyzing Image File Headers
6.3. Repairing Damaged Headers
6.4. Reconstructing File Fragments
6.5. Identifying Unknown File Formats
6.6. Identifying Image File Fragments
   6.6.2. Picture Viewer: Ifran View
   6.6.3. Picture Viewer: ACDsee
   6.6.4. Picture Viewer: Thumbsplus
   6.6.5. Picture Viewer: AD
   6.6.6. Picture Viewer: Max
   6.6.7. FastStone Image Viewer
   6.6.8. XnView
   6.6.9. Faces – Sketch Software
7. Digital Camera Data Discovery Software: FILE HOUND
9. Steganography in Image Files
10. Steganalysis Tool
   10.1. Hex Workshop
   10.2. S-tools
   10.3. Stegdetect
11. Image File Forensic Tools
   11.1. GFE Stealth (Graphics File Extractor)
   11.2. ILook v8
   11.3. P2 eXplorer
   11.4. VisionStage
   11.5. Digital Pictures Recovery
12. Identifying Copyright Issues on Graphics

13. Case Study

Module 22: Audio file forensics

1. Audio Forensics

2. Why audio forensics

3. Use of voice as a tool

4. Fast Fourier Transform (FFT)

5. Methodologies of Audio Forensics

6. Voice Identification

7. Audibility Analysis

8. Audio Enhancement

9. Authenticity Analysis

10. Sound Identification

11. Event Sequence Analysis

12. Dialogue decoding

13. Remnant Signal Analysis

14. Integrity Verification of the Audio

15. Audio Forensics Process

15.1. Evidence handling

15.2. Preparation of Exemplars

15.3. Preparation of Copies

15.4. Preliminary Examination

15.5. Analog to Digital Conversion

15.5.1. Audio File Formats

15.6. Preparation of Spectrograms

15.7. Spectrographic Analysis

16. Sound Spectrograph

17. Sound Recordings As Evidence In Court Proceedings
18. Audio File Manipulation

19. Tools

19.1. DCLive Forensics

19.2. Zoom H2 Portable Digital Recorder

19.3. CEDAR for Windows

19.3.1. Console

19.3.2. Declick

19.3.3. Decrackle

19.3.4. DEHIS2

19.3.5. NR-3 v2

19.3.6. Phase Corrector

19.3.7. EQ and dynamics

19.3.8. Spectral analyzer

19.4. Audio File Forensic Tools

19.4.1. DCVST

19.4.2. Advanced audio corrector

19.4.3. Acoustica

19.4.4. Smaart

19.4.5. DNS1500 Dialogue Noise Suppressor

19.4.6. DNS2000 Dialogue Noise Suppressor

19.4.7. DNS 3000 Dialogue Noise Suppressor

19.4.8. M-Audio MicroTrack 2496 Portable Digital Recorder

19.4.9. Cardinal

19.4.10. JBR 4 Channel Microcassette Playback/Transcriber Unit

19.4.11. JBR Universal DVD/CD Player/Transcriber Unit

Module 23: Video File Forensics

1. Video File Forensics

2. Crimes involving Video Files
3. Need of Video File Forensics
4. Video File Formats
5. Pre-Requisite for Video Forensics
6. Selecting Video Forensics Tools
7. Precaution During Video File Forensics
8. Preparing for Video Forensics
9. Video Forensic Methodology
9.1. Frame Averaging
9.2. Video De-Multiplexing
9.3. De-multiplexing Tool: Video Active
9.4. dPlex Pro: De-multiplexing Tool
9.5. Video Stabilizing
9.6. Motion Deblurring
9.7. Magnifying and Color Correcting Video
9.8. Spotlighting the Particular Region
9.9. Audio Analysis
9.10. Performing Video Steganalysis
10. StegSecret
11. UQLIPS: Near Duplicate Video Clip Detection System
12. Analysis of Output
13. Video Forensics Tools
13.1. dTective
13.2. VideoFOCUS
13.3. Sarensix Video Forensic Services
13.4. Audio Video Forensic Lab (AVFL)
13.5. VideoDetective
13.6. Jam
13.7. Ikena Reveal
Module 24: Application Password Crackers

1. Password - Terminology

2. What is a Password Cracker?

3. How Does a Password Cracker Work?

4. Various Password Cracking Methods

4.1. Brute Force Attack

4.1.1. Brute Force Attack Time Estimator

4.2. Dictionary Attack

4.3. Syllable Attack/Rule-based Attack/Hybrid Attack

4.4. Password Guessing

4.5. Rainbow Attack

4.5.1. Time Needed to Crack Passwords

5. Classification of Cracking Software

5.1. System Level Password Cracking

5.2. CMOS Level Password Cracking

5.3. Tool: Cmospwd

5.4. ERD Commander

5.5. Active Password Changer

5.6. Application Software Password Cracker

5.7. Distributed Network Attack

5.8. Passware Kit

5.9. Accent Keyword Extractor

5.10. Advanced Zip Password Recovery

6. Default Password Database


6.3. http://www.cirt.net/cgi-bin/passwd.pl

7. Pdf Password Crackers
8. Password Cracking Tools
8.1. Cain & Abel
8.2. LCP
8.3. SID&User
8.4. Ophcrack 2
8.5. John the Ripper
8.6. Netscapass
8.7. Access PassView
8.8. RockXP
8.9. Magical Jelly Bean Keyfinder
8.10. PstPassword
8.11. Protected Storage PassView
8.12. Network Password Recovery
8.13. Mail PassView
8.14. Asterisk Key
8.15. Messenger Key
8.16. MessenPass
8.17. Password Spectator
8.18. SniffPass
8.19. Asterisk Logger
8.20. Dialupass
8.21. Mail Password Recovery
8.22. Database Password Sleuth
8.23. CHAOS Generator
8.24. PicoZip Recovery
8.25. Crack
8.26. Brutus
Module 25: Log Capturing and Event Correlation

1. Computer Security Logs
   1.1. Computer Security Logs
   1.2. Operating System Logs
   1.3. Application Logs
   1.4. Software Security Logs
   1.5. Router Log Files
   1.6. Honeypot Logs
   1.7. Linux Process Accounting
   1.8. Logon Event in Window
   1.9. Windows Log File
   1.10. Configuring Windows Logging
   1.11. Analyzing Window Log
   1.12. Setting up Remote Logging in Windows
   1.13. Windows Log File: System Logs
   1.15. Log on Events That Appear in the Security Event Log
   1.16. IIS Logs
   1.17. Maintaining Credible IIS Log Files
   1.18. Log File Accuracy
   1.19. Log Everything
   1.20. Keeping Time
   1.21. UTC Time
   1.22. View the DHCP Logs
   1.23. DHCP Logs
1. ODBC Logging

2. Logs and Legal Issues
   2.1. Legality of Using Logs
   2.2. Records of Regularly Conducted Activity as Evidence
   2.3. Laws and Regulations

3. Log Management
   3.1. Log Management
   3.2. Functions of Log Management
   3.3. Challenges in Log Management

4. Centralized Logging and Syslogs
   4.1. Central Logging Design
   4.2. Steps to Implement Central Logging
   4.3. Syslog
   4.4. Syslog in Unix-like Systems
   4.5. Steps to Set Up Syslog Server for Unix Systems
   4.6. Centralized Syslog Server
   4.7. IIS Centralized Binary Logging
   4.8. Extended Logging in IIS Server

5. Time Synchronization
   5.1. Why Synchronize Computer Times?
   5.2. What is NTP Protocol?
   5.3. NTP Stratum Levels
   5.4. NIST Time Servers
   5.5. Configuring the Windows Time Service

6. Event Correlation
   6.1. Event Correlation
   6.2. Types of Event Correlation
   6.3. Prerequisites for Event Correlation
6.4. Event Correlation Approaches

7. Log Capturing and Analysis Tools

7.1. Syslog-ng Logging System

7.2. WinSyslog Syslog Server

7.3. Kiwi Syslog Server

7.4. Tenable Security Center

7.5. IISLoger: Development tool

7.6. Socklog: IDS Log Analysis Tool

7.7. Microsoft Log Parser: Forensic Analysis Tool

7.8. Firewall Analyzer: Log Analysis Tool

7.9. Adaptive Security Analyzer (ASA) Pro

7.10. GFI EventsManager

7.11. How does GFI EventsManager work?

7.12. Activeworx Security Center

7.13. Ntsyslog


7.15. EventLog Analyzer

7.16. FLAG – Forensic and Log Analysis GUI

7.17. Simple Event Correlator (SEC)

Module 26: Network Forensics and Investigating Logs

1. Introduction to Network Forensics

2. Intrusion Process

3. Network Vulnerabilities

4. Network Attacks

5. Looking for Evidence

6. Investigating Logs

6.1. Postmortem and Real-Time Analysis

6.2. Handling Logs as Evidence
6.3. Log File Authenticity
6.4. Use Signatures, Encryption and Checksums
6.5. Work with Copies
6.6. Ensure System Integrity
6.7. Access Control
6.8. Chain of Custody
6.9. Condensing Log File
7. Log Injection Attacks
7.1. New Line Injection Attack
7.2. New Line Injection Attack Countermeasure
7.3. Separator Injection Attack
7.4. Defending Separator Injection Attack
7.5. Time Stamp Injection Attack
7.6. Defending Time Stamp Injection Attack
7.7. Word Wrap Abuse Attack
7.8. Defending Word Wrap Abuse Attack
7.9. HTML Injection Attack
7.10. Defending HTML Injection Attack
7.11. Terminal Injection Attack
7.12. Defending Terminal Injection Attack
8. Other Kinds of Log File Attacks

Module 27: Investigating Network Traffic
1. Network Addressing Schemes
2. OSI Reference Model
3. Overview of Network Protocols
4. TCP/IP Protocol
5. Overview of Physical and Data-link Layer of the OSI Model
6. Overview of Network and Transport Layer of the OSI Model
7. Types of Network Attacks
8. Why to Investigate Network Traffic?
9. Evidence Gathering Via Sniffing
10. Acquiring Traffic using DNS Poisoning Techniques
11. Intranet DNS Spoofing (Local Network)
12. Internet DNS Spoofing (Remote Network)
13. Internet DNS Spoofing
14. Proxy Server DNS Poisoning
15. DNS Cache Poisoning
16. Evidence Gathering From ARP Table
17. Evidence Gathering at the Data-link Layer: DHCP Database
18. Gathering Evidence by IDS
19. Traffic Capturing and Analysis Tools
19.1. Tool: Tcpdump
19.2. Tool: Windump
19.3. Tool: NetIntercept
19.4. Tool: Wireshark
19.5. CommView
19.6. Softperfect Network Sniffer
19.7. HTTP Sniffer
19.8. EtherDetect Packet Sniffer
19.9. OmniPeek
19.10. Iris Network Traffic Analyzer
19.11. SmartSniff
19.12. NetSetMan Tool
19.13. Distinct Network Monitor
19.15. Ntop
19.16. Etherape
19.17. Colasoft Capsa Network Analyzer
19.18. Colasoft EtherLook
19.19. AnalogX Packetmon
19.20. BillSniff
19.21. IE HTTP Analyzer
19.22. EtherDetect Packet Sniffer
19.23. EtherScan Analyzer
19.24. Sniphere
19.25. IP Sniffer
19.26. AW Ports Traffic Analyzer
19.27. Ipgrab
19.28. Nagios
19.29. Give Me Too
19.30. Sniff - O – Matic
19.31. EtherSnoop
19.32. GPRS Network Sniffer: Nokia LiG
19.33. Siemens Monitoring Center
19.34. NetWitness
19.35. Netresident Tool
19.36. nGenius InfiniStream
19.37. eTrust Network Forensics
19.38. ProDiscover Investigator
19.39. P2 Enterprise Shuttle (P2EES)
19.40. Show Traffic
19.41. Network Probe
19.42. Snort Intrusion Detection System
19.43. Snort IDS Placement
Module 28: Router Forensics

1. What is a Router?
2. Functions of a Router
3. A Router in an OSI Model
4. Routing Table and its Components
5. Router Architecture
6. Routing Information Protocol
7. Implications of a Router Attack
8. Routers Vulnerabilities
9. Types of Router Attacks
  9.1. Router Attack Topology
  9.2. Denial of Service (DoS) Attacks
  9.3. Packet “Mistreating” Attacks
  9.4. Routing Table Poisoning
  9.5. Hit-and-Run and Persistent Attacks
10. Router Forensics vs. Traditional Forensics
11. Steps for Investigating Router Attacks
  11.1. Seize the Router and Maintain Chain of Custody
12. Sample Chain Of Custody (COC) Form
13. Guidelines for the Router Forensic
14. Incident Response
15. Recording your Session
16. Accessing the Router
17. Volatile Evidence
18. Obtaining Configuration of Router
19. Volatile Evidence Gathering
20. Direct Access: Using show commands
22. Compare the Configuration of Router
23. Examine the Router Table
24. Examine the Access Control List
25. Router Logs
26. Example of Router Logs
27. NETGEAR Router Logs
28. Link Logger
29. Sawmill: Linksys Router Log Analyzer
30. Logging
31. Handling a Direct Compromise Incident
32. Other Incidents
33. Real Time Forensics
34. Router Audit Tool (RAT)
35. Generate the Report

Module 29: Investigating Wireless Attacks
1. Wireless Networking Technologies
2. Wireless Networks
3. Wireless Attacks
4. Passive Attack
5. Threats from Electronic Emanations
6. Active Attacks on Wireless Networks
7. Denial-of-Service Attacks
8. Man-in-the-Middle Attack (MITM)
9. Hijacking and Modifying a Wireless Network
10. Association of Wireless AP and Device
11. Network Forensics in a Wireless Environment
12. Steps for Investigation
13. Key Points to Remember
14. Points You Should not Overlook while Investigating the Wireless Network
15. Obtain a Search Warrant
16. Document the Scene and Maintain Chain Of Custody
17. Identify Wireless Devices
18. Wireless Components
19. Search for Additional Devices
20. Detect Wireless Connections
21. Detect Wireless Enabled Computers
22. Manual Detection of Wireless APs
23. Active Wireless Scanning Technique
24. Passive Wireless Scanning Technique
25. Detect WAPs using the Nessus Vulnerability Scanner
26. Capture Wireless Traffic
27. Tool: Wireshark
27.1. Feature of Wireshark
28. Tool: tcpdump
28.1. tcpdump Commands
29. ClassicStumbler
30. Wireless Network Monitoring Tools
30.1. MacStumbler
30.2. iStumbler
30.3. AirPort Signal
30.4. AirFart
30.5. Kismet
31. Determine Wireless Field Strength: Field Strength Meters (FSM)
32. Prepare Wireless Zones & Hotspots Maps
33. Methods to Access a Wireless Access Point
34. Direct-connect to the Wireless Access Point
35. Nmap
35.1. Scanning Wireless Access Points using Nmap
36. Rogue Access Point
36.1. Tools to Detect Rogue Access Points: Netstumbler
36.2. Tools to Detect Rogue Access Points: MiniStumbler
37. “Sniffing” Traffic Between the Access Point and Associated Devices
38. Scanning using Airodump
39. MAC Address Information
40. Airodump: Points to Note
41. Forcing Associated Devices to Reconnect
42. Check for MAC Filtering
43. Changing the MAC Address
44. Wireless Data Acquisition and Analysis
45. Report Generation

Module 30: Investigating Web Attacks
1. Indications of a Web Attack
2. Types of Web Attacks
3. Cross-Site Scripting (XSS)
4. Investigating Cross-Site Scripting (XSS)
5. Cross-Site Request Forgery (CSRF)
6. Anatomy of CSRF Attack
7. Pen-Testing CSRF Validation Fields
8. SQL Injection Attacks
9. Investigating SQL Injection Attacks
11. Code Injection Attack
12. Investigating Code Injection Attack
13. Parameter Tampering
14. Cookie Poisoning
15. Investigating Cookie Poisoning Attack
16. Buffer Overflow/Cookie Snooping
17. Detecting Buffer Overflow
18. DMZ Protocol Attack/ Zero Day Attack
19. Authentication Hijacking
20. Investigating Authentication Hijacking
21. Log Tampering
22. Directory Traversal
23. Cryptographic Interception
24. URL Interpretation and Impersonation Attack
25. Overview of Web Logs
26. Investigating Web Attack
27. Example of FTP Compromise
28. Investigating FTP Logs
29. Investigating FTP Servers
30. Investigating IIS Logs
31. Investigating Apache Logs
32. Investigating Web Attacks in Windows-based Servers
33. Web Page Defacement
34. Defacement Using DNS Compromise
35. Investigating DNS Poisoning
36. Intrusion Detection
37. Security Strategies to Web Applications
38. Investigating Static and Dynamic IP Address
39. Checklist for Web Security
42. Dotdefender
43. AccessDiver
44. Log Analyzer: Server Log Analysis
45. Web Attack Investigation Tools
45.1. Analog
45.2. Deep Log Analyzer
45.3. AWStats
45.4. WebLog Expert
45.5. AlterWind Log Analyzer
45.6. Webalizer
45.7. eWebLog Analyzer
45.8. N-Stealth
45.9. Acunetix
45.10. Falcove
45.11. AppScan
45.12. Watchfire AppScan
45.13. Emsa Web Monitor
45.14. WebWatchBot
45.15. Paros
45.16. HP WebInspect
45.17. KeepNI
45.18. Wikto
45.19. Mapper
45.20. N-Stalker
45.21. Scrawlr
45.22. Exploit-Me

46. Tools for Locating IP Address

46.1. Hide Real IP
46.2. Whatismyip
46.3. IP Detective Suite
46.4. Enterprise IP - Address Manager
46.5. Whois Lookup
46.6. SmartWhois
46.7. ActiveWhois
46.8. LanWhois

47. Nslookup
48. Traceroute

49. Tools for Locating IP Address

49.1. NeoTrace (Now McAfee Visual Trace)
49.2. Whois
49.3. CountryWhois
49.4. IP2Country
49.5. CallerIP
49.6. Whois.net
49.7. Pandora FMS

50. CounterStorm-1: Defense Against Known, Zero Day, and Targeted Attacks

Module 31: Investigating DoS Attacks

1. DoS Attack
2. Indications of a DoS/DDoS Attack
3. Types of DoS Attacks
4. Ping of Death Attack
5. Teardrop Attack
6. SYN Flooding
7. Land
8. Smurf
9. Fraggle and Snork Attack
10. WINDOWS OUT-OF-BAND (OOB) Attack and Buffer Overflow
11. Nuke Attacks and Reflected Attack
12. DDoS Attack
13. Working of DDoS Attacks
14. Classification of DDoS Attack
15. DDoS Attack Taxonomy
16. DoS Attack Modes
17. Techniques to Detect DoS Attack
18. Techniques to Detect DoS Attack: Activity Profiling
19. Techniques to Detect DoS Attack: Sequential Change-Point Detection
20. Techniques to Detect DoS Attack: Wavelet-based Signal Analysis
21. Monitoring CPU Utilization to Detect DoS Attacks
22. Detecting DoS Attacks Using Cisco NetFlow
23. Detecting DoS Attacks Using Network Intrusion Detection System (NIDS)
24. Investigating DoS Attack
25. ICMP Traceback
26. Hop-by Hop IP Traceback
27. Limitations of Hop-by Hop IP Traceback
28. Backscatter Traceback
29. How the Backscatter Traceback Works
30. IP Traceback with IPSec
31. CenterTrack Method
32. Packet Marking
33. Probabilistic Packet Marking (PPM)
34. Check Domain Name System (DNS) Logs
35. Tracing with "log-input"
36. Control Channel Detection
37. Correlation and Integration
38. Path Identification (Pi) Method
39. Packet Traffic Monitoring Tools
40. Tools for Locating IP Address
41. Challenges in Investigating DoS Attack
42. Network Monitoring Tools
42.1. Nmap
42.2. Friendly Pinger
42.3. IPHost Network Monitor
42.4. Tail4Win
42.5. Status2k
42.6. DoSHTTP
42.7. Admin’s Server Monitor

Module 32: Investigating virus, Trojan, spyware and Rootkit Attacks
1. Statistics of the Malicious and Potentially Unwanted Programs
2. Viruses and Worms
2.1. Virus Top 20 for January 2008
2.2. Viruses
2.3. Worms
2.4. How to Know a Virus Infected a System
2.5. Characteristics of a Virus
2.6. Working of a Virus
2.6.1. Working of a Virus: Infection Phase
2.6.2. Working of a Virus: Attack Phase
2.7. Symptoms of a Virus-Like Attack
2.8. Indications of a Virus Attack
2.9.    Modes of Virus Infection
2.10.   Stages of Virus Life
2.11.   Virus Classification
2.12.   How Does a Virus Infect?
2.13.   Storage Patterns of a Virus
2.14.   Virus Detection
2.15.   Virus Detection Methods
2.16.   Virus Incident Response
2.17.   Investigating Viruses
3.      Trojans and Spyware
3.1.    Trojans and Spyware
3.2.    Working of Trojans
3.3.    How Spyware Affects a System
3.4.    What Spyware Does to the System
3.5.    What Do Trojan Creators Look For?
3.6.    Different Ways a Trojan Can Get into a System
3.7.    Identification of a Trojan Attack
3.8.    Remote Access Trojans (RAT)
3.9.    Ports Used by Trojans
4.      Antivirus Tools
4.1.    AVG Antivirus
4.2.    Norton Antivirus
4.3.    McAfee
4.4.    Kaspersky Anti-Virus
4.5.    BitDefender
4.6.    SocketShield
4.7.    CA Anti-Virus
4.8.    F-Secure Anti-Virus
4.9. F-Prot Antivirus
4.10. Panda Antivirus Platinum
4.11. avast! Virus Cleaner
4.12. Norman Virus Control
4.13. ClamWin
5. Anti Trojan Tools
5.1. TrojanHunter
5.2. Comodo BOClean
5.3. Trojan Remover: XoftspySE
5.4. Trojan Remover: Spyware Doctor
5.5. SPYWAREfighter
5.6. Evading Anti-Virus Techniques
5.7. Sample Code for Trojan Client/Server
6. Evading Anti-Trojan/Anti-Virus Using Stealth Tools
7. Backdoor Countermeasures
8. Tool: Tripwire
9. System File Verification
10. MD5sum.exe
11. Tool: Microsoft Windows Defender
12. Rootkit
12.1. Introduction of Rootkit
12.2. Attacks Approach
12.3. Types of Rootkits
12.4. Rootkit Detection
13. Windows Rootkit
13.1. Fu Rootkit
13.2. Vanquish
13.3. AFX Rootkit
Module 33: Investigating Internet Crimes

1. Internet Crimes
2. Internet Forensics
3. Why Internet Forensics
4. Goals of Investigation
5. Investigating Internet Crime Steps
6. Obtain a Search Warrant
7. Interview the Victim
8. Prepare Bit-Stream Copies
9. Check the Logs
10. Identify the Source of the Attack
11. IP Address
12. Internet Assigned Numbers Authority
13. Regional Internet Registry (RIR)
14. Internet Service Provider
15. Trace the IP Address of the Attacker Computer
16. Domain Name System (DNS)
17. DNS Record Manipulation
18. DNS Lookup
18.1. nslookup
19. Analyze the Whois Information
19.1. Whois
19.2. Example Whois Record
20. Whois Tools and Utilities
20.1. Samspade
20.2. SamSpade Report
20.3. IP Address Locator
20.4. www.centralops.net: Tracing Geographical Location of a URL
20.5. DNS Lookup Result: centralops.net
20.6. Traceroute
21. Collect the Evidence
22. Examining Information in Cookies
23. Viewing Cookies in Firefox
23.1. Tool: Cookie Viewer
24. Switch URL Redirection
25. Sample Javascript for Page-based Redirection
26. Embedded JavaScript
27. Downloading a Single Page or an Entire Web Site
27.1. Tool: My Offline Browser
28. Recovering Information from Web Pages
28.2. Take Me Back Results
Module 34: Tracking Emails and Investigating Email Crimes

1. Email System
2. E-mail Client
3. E-mail Server
4. SMTP Server
5. POP3 and IMAP Server
6. Importance of Electronic Records Management
7. E-mail Crime
8. Spamming
9. Mail Bombing/Mail Storm
10. Crime via Chat Rooms
11. Identity Fraud/Chain Letter
12. Phishing
13. Email Spoofing
14. Investigating E-mail Crime and Violation
15. Obtain a Search Warrant and Seize the Computer and Email Account
16. Obtain a Bit-by-Bit Image of Email Information
17. Email Message
18. Viewing Header in Microsoft Outlook
19. Viewing Header in AOL
20. Viewing Headers in Hotmail
21. Viewing Header in Gmail
22. Viewing Header in Yahoo Mail
23. Examining an Email Header
24. Analysis of Email Header at Timmy
25. Received: Headers
26. Forging Headers
27. List of Common Headers
28. Examining Additional Files (.pst or .ost files)
   28.1. Pst File Location
29. Microsoft Outlook Mail
30. Examine the Originating IP Address
31. http://centralops.net/co/
32. Exchange Message Tracking Center
33. MailDetective Tool
34. Examine Phishing
35. Forensic ToolKit (FTK)
36. E-Mail Examiner by Paraben
37. Network E-Mail Examiner by Paraben
38. Recover My Email for Outlook
39. Diskinternals – Outlook Recovery
40. Tracing Back
41. Tracing Back Web Based E-mail
42. Abuse.Net
43. Network Abuse Clearing House
44. Tool: LoPe
45. Tool: FINALEMAIL
46. Handling Spam
47. Tool: eMailTrackerPro
48. Email Trace
49. Tool: ID Protect
50. Email Investigation Tool
50.1. R-Mail
50.2. Email Detective
50.3. SPAM Punisher
50.4. SpamArrest
51. U.S. Laws Against Email Crime: CAN-SPAM Act
52. U.S.C. § 2252A
54. Email Crime Law in Washington: RCW 19.190.020

Module 35: PDA Forensics
1. Personal Digital Assistant (PDA)
2. Information Stored in PDA
3. PDA Components
4. PDA Characteristics
5. Generic PDA Hardware Diagram
6. Palm OS
7. Architecture of Palm OS Devices
8. Pocket PC
9. Architecture for Windows Mobile
10. Linux-based PDAs
11. Architecture of the Linux OS for PDAs
12. PDA Generic States
13. PDA Security Issues
14. ActiveSync and HotSync Features
15. ActiveSync Attacks
16. HotSync Attacks
17. PDA Forensics
17.1. PDA Forensics steps
17.2. Points to Remember while Conducting Investigation
17.3. Securing and Evaluating the Scene
17.4. Seize the Evidences
17.5. Identify the Evidence
17.6. Preserve the Evidence
17.7. Acquire the Information
17.8. Data Acquisition Techniques
17.9. Examination and Analysis the Information
17.10. Document Everything
17.11. Make the Report
18. PDA Forensic Tool
18.1. PDA Secure
18.2. Device Seizure
18.3. DS Lite
18.4. EnCase
18.5. SIM Card Seizure
18.6. Palm dd (pdd)
18.7. Duplicate Disk
18.8. Pocket PC Forensic Software
18.9. Mobile Phone Inspector
Module 36: Blackberry Forensics

1. Blackberry
2. BlackBerry Operating System
3. How BlackBerry Works
4. BlackBerry Serial Protocol
5. BlackBerry Serial Protocol: Packet Structure
6. Blackberry Attack
7. Blackberry Attack Toolkit
8. BlackBerry Attachment Service Vulnerability
9. TeamOn Import Object ActiveX Control vulnerability
10. Denial of Service in BlackBerry Browser
11. BlackBerry Security
12. BlackBerry Wireless Security
13. BlackBerry Security for Wireless Data
14. Prerequisites for BlackBerry Forensics
15. Steps for BlackBerry Forensics
16. Collect the Evidence
17. Document the Scene and Preserve the Evidence
18. Radio Control
19. Imaging and Profiling in BlackBerry
20. Acquire the Information
21. Hidden Data in BlackBerry
22. Acquire Logs Information from BlackBerry
23. Program Loader
24. Review of Information
25. Best Practices for Protecting Stored Data
Module 37: iPod and iPhone Forensics

1. iPod
2. iPhone Overview
3. What a Criminal Can do With iPod
4. What a Criminal Can do With iPhone
5. iPhone OS Overview
6. iPhone Disk Partitions
7. Apple HFS+ and FAT32
8. Application Formats
9. iPod and iPhone Forensics
10. Evidence Stored on iPod and iPhone
11. Forensic Prerequisites
12. Collecting iPod/iPhone Connected with Mac
13. Collecting iPod/iPhone Connected with Windows
14. Disable Automatic Syncing
15. Write Blocking
16. Write Blocking in Different OS
17. Image the Evidence
18. View the iPod System Partition
19. View the Data Partition
20. Break Passcode to Access the Locked iPhone
21. Acquire DeviceInfo File
22. Acquire SysInfo File
23. Recover IPSW File
24. Check the Internet Connection Status
25. View Firmware Version
26. Recover Network Information
27. Recovering Data from SIM Card
28. Acquire the User Account Information
29. View the Calendar and Contact Entries
30. Recovering Photos
31. Recovering Address Book Entries
32. Recovering Calendar Events
33. Recovering Call Logs
34. Recovering Map Tile Images
35. Recovering Cookies
36. Recovering Cached and Deleted Email
37. Recover Deleted Files
38. Forensic Information from the Windows Registry
39. Forensic Information from the Windows: setupapi.log
40. Recovering SMS Messages
41. Other Files Which are Downloaded to the Computer During iTunes Sync Process
42. Analyze the Information
43. Timeline Generation
44. Timeline Generation: File Status After Initialization the iPod with iTunes and Before Closing iTunes
45. Timeline Generation: File Status After Connecting iPod to the Computer for Second Time, Copying Music, and Closing iTunes
46. Time Issues
47. Jailbreaking in iPod Touch and iPhone
47.1. Jailbreaking
47.2. AppSnapp
47.3. iFuntastic
47.4. Pwnage: Tool to Unlock iPod Touch
47.5. Erica Utilities for iPod Touch

48. Tools

48.1. EnCase
48.2. DiskInternals Music Recovery
48.3. Recover My iPod: Tool
48.4. iPod Data Recovery Software
48.5. iPod Copy Manager
48.6. Stellar Phoenix iPod Recovery
48.7. Aceso
48.8. Cellebrite UME 36 Pro
48.9. Walf
48.10. Device Seizure
48.11. PhoneView
48.12. iPhone Drive
48.13. Tansee iPhone Transfer SMS
48.14. SIM Analyzer
48.15. SIMCon – SIM Card Recovery
48.16. SIM Card Data Recovery Software

Module 38: Cell Phone Forensics

1. Mobile Phone

2. Hardware Characteristics of Mobile Devices

3. Software Characteristics of Mobile Devices

4. Components of Cellular Network

5. Cellular Network

6. Different Cellular Networks

7. Different OS in Mobile Phone
8. What a Criminal Can do with Mobiles
9. Mobile Forensics
10. Forensics Information in Mobile Phones
11. Subscriber Identity Module (SIM)
12. SIM File System
13. Integrated Circuit Card Identification (ICCID)
14. International Mobile Equipment Identifier (IMEI)
15. Electronic Serial Number (ESN)
16. Precaution to be Taken before Investigation
17. Points to Remember while Collecting the Evidence
18. Acquire the Information
19. Acquire Data from SIM Cards
20. Acquire Data from Unobstructed Mobile Devices
21. Acquire the Data from Obstructed Mobile Devices
22. Memory Considerations in Mobiles
23. Acquire Data from Memory Cards
24. Memory Cards
25. Acquire Data from Synched Devices
26. Gather Data from Network Operator
27. Check Call Data Records (CDR’s)
28. Analyze the Information
29. Cell Phone Forensic Tools
29.1. SIM Analyzer
29.2. SIMCon
29.3. SIM Card Data Recovery
29.4. Memory Card Data Recovery
29.5. Device Seizure
29.6. SIM Card Seizure
29.7. Cell Phone Analyzer
29.8. Oxygen Forensic Suite
29.9. BitPim
29.10. MOBIedit! Forensic
29.11. PhoneBase
29.12. Secure View
29.13. XACT

Forensic Card Reader (FCR)
29.15. ForensicSIM Toolkit
29.16. SIMIS 3G
29.17. UME-36Pro - Universal Memory Exchanger
29.18. Cellebrite UFED System - Universal Forensic Extraction Device
29.19. ZRT
29.20. Neutrino
29.21. ICD 5005
29.22. ICD 1300

30. Challenges for Forensic Efforts

Module 39: USB Forensics
1. Universal Serial Bus (USB)
2. USB Flash Drive
3. Screenshot: USB Flash Drive
4. Misuse of USB
5. USB Forensics
6. USB Forensic Investigation
7. Secure and Evaluate the Scene
8. Document the Scene and Devices
9. Image the Computer and USB Device
10. Acquire the Data
11. Check Open USB Ports
12. Examine Registry of Computer: USBTOR
13. Examine Registry of Computer: DeviceClasses
14. Examine Registry of Computer: MountedDevice
15. Generate Reports
16. USB Forensic Tools
16.1. Bad Copy Pro
16.2. Data Doctor Recovery
16.3. USB Image Tool
16.4. USBDeview

Module 40: Printer Forensics
1. Introduction to Printer Forensics
2. Different Printing Modes
3. Methods of Image Creation
4. Printers with Toner Levels
5. Parts of a Printer
6. Printer Identification Strategy
7. Printer Identification
8. Printer Forensics Process
9. Pre-Processing
10. Printer Profile
11. Forensics
12. Ballistics
13. A Clustering Result of a Printed Page
14. Digital Image Analysis
15. Printout Bins
16. Document Examination
Module 41: Investigating Corporate Espionage

1. Investigating Corporate Espionage: Case Study
2. Introduction to Corporate Espionage
3. Motives Behind Spying
4. Information that Corporate Spies Seek
5. Corporate Espionage: Insider/Outsider Threat
6. Threat of Corporate Espionage due to Aggregation of Information
7. Techniques of Spying
8. Defense Against Corporate Spying
9. Controlled Access
10. Background Investigation of the Personnel
11. Basic Security Measures to Protect Against Corporate Spying
12. Steps to Prevent Corporate Espionage
13. Key Findings from U.S Secret Service and CERT Coordination Center/SEI study on Insider Threat
14. Netspionage
15. Investigating Corporate Espionage Cases
16. Employee Monitoring: Activity Monitor
17. Spector CNE Employee Monitoring Software
18. Track4Win
19. Spy Tool
19.1. SpyBuddy
19.2. NetVizor
19.3. Privatefirewall w/Pest Patrol
20. Anti Spy Tool
20.1. Internet Spy Filter
20.2. Spybot S&D
20.3. SpyCop
20.4. Spyware Terminator
20.5. XoftSpySE
21. Spy Sweeper
22. Counter Spy
23. SUPERAntiSpyware Professional
24. IMonitorPCPro - Employee Monitoring Software
25. Case Study: HP Chief Accused of Corporate Spying
26. Case Study: India’s Growing Corporate Spy Threat
27. Guidelines while Writing Employee Monitoring Policies

Module 42: Investigating Computer Data Breaches

1. How Data Breaches Occur
1.1. Using The External Memory Devices
1.2. Using The Internet
1.3. Using Mobiles And iPods
1.4. Using Malware
1.5. Others Techniques
2. Investigating Local Machine
2.1. Check The Registry Editor
2.2. Check For CD/DVD Burning Software
2.3. Check For Browsing History
2.4. Check The Downloads
2.5. Check The Mail History
2.6. Check For Suspicious Software
3. Investigating Network
3.1. Check The Firewall
3.2. Check The Mail Server
3.3. Check The Printers
4. Countermeasures

Module 43: Investigating Trademark and Copyright Infringement
1. Trademark Infringement
1.1. Trademarks
1.2. Trademark Eligibility and Benefits of Registering It
1.3. Service Marks and Trade Dress
1.4. Trademark Infringement
1.5. Monitoring Trademark Infringements
1.6. Key Considerations before Investigating Trademark Infringements
1.7. Steps for Investigating Trademark Infringements
2. Copyright Infringement
2.1. Copyright
2.2. Investigating Copyright Status
2.3. How Long Does a Copyright Last?
2.4. U.S Copyright Office
2.5. How is Copyrights Enforced?
2.6. Copyright Infringement: Plagiarism

2.7. Types of plagiarism

2.8. Steps for Plagiarism Prevention

2.9. Plagiarism Detection Factors

3. Plagiarism Detection Tools

3.1. Turnitin

3.2. CopyCatch

3.3. Copy Protection System (COPS)

3.4. SCAM (Stanford Copy Analysis Mechanism)

3.5. CHECK

3.6. Jplag

3.7. VAST

3.8. SIM

3.9. Urkund

3.10. WC()pfind

3.11. GPSP

3.12. PLAGUE

3.13. SPaT

3.14. Sherlock

3.15. PRAISE

3.16. SafeAssignment

3.17. EVE2

3.18. iThenticate

3.19. Dupli Checker


4. Patent Infringement

4.1. Patent
4.2. Patent Infringement
4.3. Types of Patent Infringement
4.4. Patent Search
4.6. How ip.com Works
4.7. Domain Name Infringement
4.8. How to Check for Domain Name Infringement?

5. Intellectual Property
5.1. Intellectual Property
5.2. Investigating Intellectual Property Theft
5.3. Steps for Investigating Intellectual Property Theft

6. Digital Rights Management
6.1. Digital Rights Management (DRM)

7. Windows Media Digital Rights Management

8. Media-DRM Packager

9. Haihaisoft Media DRM Packager

10. DRM Software for Copy Protection

11. IntelliProtector

12. Trademarks and Copyright Laws
12.1. US Laws for Trademarks and Copyright
12.2. Indian Laws for Trademarks and Copyright
12.3. Japanese Laws for Trademarks and Copyright
12.4. Australia Laws For Trademarks and Copyright
12.5. UK Laws for Trademarks and Copyright
12.6. China Laws for Trademarks and Copyright
12.7. Canada Laws for Trademarks and Copyright
12.8. South African Laws for Trademarks and Copyright
12.9. South Korean Laws for Trademarks and Copyright
Module 44: Investigating Sexual Harassment Incidents

1. Sexual Harassment - Introduction
2. Types of Sexual Harassment
3. Consequences of Sexual Harassment
4. Sexual Harassment Statistics
5. Do's and Don'ts if You Are Being Sexually Harassed
6. Stalking
7. Stalking Behaviors
8. Stalking Effects
9. Guidelines for Stalking Victims
10. Responsibilities of Supervisors
11. Responsibilities of Employees
12. Complaint Procedures
12.1. Informal procedures
12.2. Formal procedures
13. Investigation Process
13.1. Investigation Process
13.2. Sexual Harassment Investigations
13.3. Sexual Harassment Policy
13.4. Preventive Steps
14. Laws on Sexual Harassment
14.1. U.S Laws on Sexual Harassment
14.2. The Laws on Sexual Harassment: Title VII of the 1964 Civil Rights Act
14.3. The Laws on Sexual Harassment: The Civil Rights Act of 1991
14.4. The Laws on Sexual Harassment: Equal Protection Clause of the 14th Amendment
14.5. The Laws on Sexual Harassment: Common Law Torts
14.6. The Laws on Sexual Harassment: State and Municipal Laws
14.7. Australian Laws on Sexual Harassment
14.8. The Laws on Sexual Harassment: Sex Discrimination Act 1984
14.11. The Laws on Sexual Harassment: Workplace Relations Act 1996
14.13. German Law: Protection of Employees Act
14.15. Law of the People's Republic of China on the Protection of Rights and Interests of Women
14.16. Penal Code, Section 509. in Malaysia

15. Sample Complaint Form

16. Laws Against Stalking

Module 45: Investigating Child Pornography Cases
1. Introduction to Child Pornography
2. People’s Motive Behind Child Pornography
3. People Involved in Child Pornography
4. Role of Internet in Promoting Child Pornography
5. Effects of Child Pornography on Children
6. Measures to Prevent Dissemination of Child Pornography
7. Challenges in Controlling Child Pornography
8. Precautions before Investigating Child Pornography Cases
9. Steps for Investigating Child Pornography
9.1. Step 1: Search and Seize all Computer and Media Devices
9.2. Step 2: Check Authenticated Login Sessions
9.3. Step 3: Search Hard Disk for Pornographic Material
9.4. Step 4: Recover Deleted Files and Folders
9.5. Step 5: Check Metadata of Files and Folders Related with Pornography
9.6. Step 6: Check and Recover the Browser Information
9.6.1. Browsing History, Save Form, and Search History
9.6.2. Download History
9.6.3. Cache
9.6.4. Cookies
9.6.5. Saved Passwords
9.6.6. Authenticated Sessions
9.7. Step 7: Check ISP Logs
10. Sources of Digital Evidence
11. Citizens’ Responsibility on pornography
12. Guidelines to Avoid Child Pornography on the Web
13. Guidelines for Parents to Protect Children from Pornography
14. Tools to Protect Children from Pornography
14.1. Reveal
14.2. iProtectYou
14.3. WUPC Web Control for Parents 4
14.4. BrowseControl
14.5. ChatGuard
14.6. Child Exploitation Tracking System (CETS)
15. Reports on Child Pornography
16. Laws Against Child Pornography
16.1. U.S. Laws against Child Pornography
16.2. Australia Laws against Child Pornography
16.3. Austria Laws against Child Pornography
16.4. Belgium Laws against Child Pornography
16.5. Cyprus Laws against Child Pornography
16.6. Japan Laws against Child Pornography
16.7. South African Laws against Child Pornography
16.8. UK laws against Child Pornography
16.10. England and Wales Laws
16.11. Scotland laws
16.13. Children’s Internet Protection Act (CIPA)
17. Anti-Child-Pornography Organizations
17.1. Innocent Images National Initiative
17.2. Internet Crimes against Children (ICAC)
17.3. Antichildporn.org
17.4. How to Report to Antichildporn.org about Child Pornography Cases
17.5. Child Exploitation and Online Protection (CEOP) Centre
17.6. ThinkUKnow
17.7. Virtual Global Taskforce (VGT)
17.8. Internet Watch Foundation (IWF)
17.9. International Centre for Missing & Exploited Children (ICMEC)
17.10. National Center for Missing & Exploited Children (NCMEC)
17.11. Child Victim Identification Program (CVIP)
17.12. Financial Coalition against Child Pornography (FCACP)
17.13. Perverted Justice
17.15. Canadian Centre for Child Protection
17.17. Association of Sites Advocating Child Protection (ASACP)
17.18. Web Sites against Child Porn (WSACP)
17.20. Child Focus
17.21. StopChildPorno.be
Module 46: Investigating Identity Theft Cases

1. Identity Theft
   1.1. Identity Theft
   1.2. Identifying Information
   1.3. Identity Theft Statistics for 2007
   1.4. Identity Theft Complaints By Age of The Consumer
   1.5. Example of Identity Theft
   1.6. Who Commits Identity Theft
   1.7. How Criminals Get Information
   1.8. How Personal Information Was Stolen: Statistics
   1.9. Techniques Used By Criminals
   1.10. How Does A Criminal Use Information
   1.11. FTC Consumer Sentinel
   1.12. Identity Theft Movies

2. Investigating Identity Theft
   2.1. Investigating Identity Theft
   2.2. Interview The Victim
   2.3. Get The Credit Reports
   2.4. Sample Credit Report
   2.5. Collect Information About Online Activities of Victim
   2.6. Collect Information About The Websites Where Victim Has Disclosed Personal Information
     2.6.1. http://www.whois.net/
     2.6.2. http://centralops.net/co/
     2.6.3. http://www.archive.org/
   2.7. Search The FTC Consumer Sentinel
   2.8. Collect Information From Point Of Sale
   2.9. Collect Information From Courier Services
   2.10. Get Call Records From Service Providers If Stolen Identity Is Used To Obtain Phone Service
2.11. Search The Suspect’s Address
2.12. Obtain Search And Seize Warrant
2.13. Seize The Computer And Mobile Devices From Suspects
2.14. Collect The Browser Information From Suspects Computer

3. Identity Theft Laws
3.2. United States Federal Laws
3.3. Australia
3.4. Canada
3.5. Hong Kong
3.6. United Kingdom

4. Protection From Identity Theft
4.1. Protection From ID Theft
4.2. What Should Victims Do?
4.3. Resources for Victims

Module 47: Investigating Defamation over Websites and Blog Postings
1. What is a Blog
2. Types of Blogs
3. Blogging
4. Who is Blogging?
5. Blogosphere Growth
6. Defamation over Websites and Blog Postings
7. Steps for Investigating Defamation Over Websites and Blog Postings
8. Search the Content of Blog in Google
9. Check the URL of the Blog/Webpage
10. Check the Copyright and Privacy Policy
11. Check the Profile of Author of the Blog/Web Post
12. Intelius Search (www.intelius.com)
13. Yahoo! People Search
14. Satellite Picture of a Residence
15. Best PeopleSearch (http://www.bestpeoplesearch.com/)
16. People-Search-America.com
17. Check the Comments for the Blog
18. Search in www.archive.org
19. Search Results
20. Check in Whois Database
21. Whois Database Result
22. Search the Email Address and Telephone Number
23. Visit 411 and Search for Telephone Numbers
24. Search for UK Telephone Numbers at BT
25. Check the Physical Location

Module 48: Investigating Social Networking Websites for Evidences
1. Introduction: Social Networking
2. What Is a Social Networking Site
3. MySpace
4. Facebook
5. Orkut
6. Crime Using Social Networking Website
7. Use of Social Networking Websites in Investigations
8. Investigation Process
9. Search for Convict Account on Website
10. Mirror the web pages in the CD-ROM
11. Investigation in MySpace
12. Investigation in Facebook
13. Investigation in Orkut
14. Investigating Profile
15. Investigating Scrapbook
16. Investigating Photos and Video
17. Investigating Testimonials
18. Investigating View Events
19. Investigating Friendlist
20. Investigating Communities
21. Report Generation

Module 49: Investigation Search Keywords
1. Keyword Search
2. Developing a Keyword Search List
3. Index-Based Keyword Searching
4. Bitwise Searching
5. Keyword Search Techniques
6. Choice of Searching Methodology
7. Issues with Keyword Searching
8. Odyssey Keyword Search

Module 50: Investigative Reports
1. Computer Forensic Report
2. Computer Forensic Report Template
3. Report Specifications
4. Report Classification
5. Layout of an Investigative Report
6. Guidelines for Writing a Report
7. Use of Supporting Material
8. Importance of Consistency
9. Salient Features of a Good Report
10. Important Aspects of a Good Report
11. Investigative Report Format
12. Attachments and Appendices
13. Include Metadata
14. Signature Analysis
15. Sample Forensic Report
16. Investigation Procedures
17. Collecting Physical and Demonstrative Evidence
18. Collecting Testimonial Evidence
19. Dos and Don'ts of Forensic Computer Investigations
20. Case Report Writing and Documentation
21. Create a Report to Attach to the Media Analysis Worksheet
22. Best Practices for Investigators
23. Writing Report Using FTK

Module 51: Becoming an Expert Witness
1. What is an Expert Witness
2. Role of an Expert Witness
3. What Makes a Good Expert Witness?
4. Types of Expert Witnesses
4.1. Computer Forensics Experts
4.2. Role of Computer Forensics Expert
4.3. Medical & Psychological Experts
4.4. Civil Litigation Experts
4.5. Construction & Architecture Experts
4.6. Criminal Litigation Experts
5. Scope of Expert Witness Testimony
6. Technical Testimony vs. Expert Testimony
7. Preparing for Testimony
8. Evidence Preparation and Documentation
9. Evidence Processing Steps
10. Checklists for Processing Evidence
11. Examining Computer Evidence
12. Prepare the Report
13. Evidence Presentation
14. Rules Pertaining to an Expert Witness’ Qualification
15. Daubert Standard
16. Frye Standard
17. Importance of Resume
18. Testifying in the Court
19. The Order of Trial Proceedings
20. General Ethics while Testifying
21. Importance of Graphics in a Testimony
22. Helping your Attorney
23. Avoiding Testimony Issues
24. Testifying during Direct Examination
25. Testifying during Cross Examination
26. Deposing
27. Recognizing Deposing Problems
28. Guidelines to Testify at a Deposing
29. Dealing with Media
30. Finding an Computer Forensic Expert

Module 52: How to Become a Digital Detective
1. Digital Detective
2. Roles and Responsibilities of Digital Detectives
3. Traits of a Digital Detective
4. Technical Skills
5. Qualification of Digital Detectives
6. Wider Competencies
Module 53: Computer Forensics for Lawyers

1. Computer Forensics for Lawyers
2. Initial Information to be Known by Lawyers When an Incident Occurs
3. Presenting the Case
4. What Lawyers Should Know
5. Functions of Lawyers
6. When Do Lawyers Really Need to Hire a Forensic Expert?
7. Identify the Right Forensic Expert
8. Industry Associations Providing Expert Forensic Investigators
9. Check for Legitimacy
10. What Lawyers Should Know in the Forensic Process
11. What Makes Evidence Inadmissible in the Court
12. Computer Forensics Cases
13. What Lawyers Should Expect from Forensic Examiner

Module 54: Law and Computer Forensics

1. Computer Forensics Laws
2. Role of Law Enforcement Agencies in Forensics Investigation
3. Guidelines for Law Enforcement Agencies
4. Law Enforcement Policies
5. Internet Laws and Statutes
7. Intellectual Property Rights
8. Cyber Stalking
10. The USA Patriot Act of 2001
11. Federal Information Security Management Act
12. Gramm-Leach Bliley Act
13. CAN-SPAM Act
14. Personal Information Protection and Electronic Documents Act
15. Data Protection Act 1998
17. Cyber Terrorism Preparedness Act of 2002
18. Laws Related to Information Assurance and Security
19. Federal Records Act
20. Federal Managers Financial Integrity Act of 1982
21. Federal Property and Administration Service Act
22. Government Paperwork Elimination Act
23. Paperwork Reduction Act
24. Computer Fraud and Abuse Act
25. Freedom of Information Act
27. Implications of Public Law 107-347 Regarding Certification and Accreditation
28. Information Privacy Act 2000
28.1. National Archives and Records Act
31. Austrian Laws
32. Belgium Laws
33. Brazilian Laws
34. Canadian Laws
35. Denmark Laws
36. European Laws
37. France Laws
38. German Laws
39. Greece Laws
40. Hongkong Laws
41. Indian Laws
42. Italian Laws
43. Japanese Laws
44. Latvian Laws
45. Malaysian Laws
46. Malta laws
47. Netherlands Laws
48. Norwegian Laws
50. Singapore Laws: Computer Misuse Act
52. United States Laws
53. Internet Crime Schemes and Prevention Tips
54. Internet Crime Schemes
55. Internet Crime Prevention Tips
56. Reporting a Cybercrime
57. Why You Should Report Cybercrime
58. Reporting Computer-related Crimes
58.1. Person Assigned to Report the Crime
58.2. When and How to Report an Incident?
58.3. Who to Contact at the Law Enforcement?
58.4. Federal Local Agents Contact
58.4.1. More Contacts
59. CIO Cyberthreat Report Form
60. Crime Investigating Organizations
61. Crime Investigating Organizations
62. Interpol - Information Technology Crime Center
63. www.interpol.int
64. Federal Bureau of Investigation
65. How the FBI Investigates Computer Crime
66. Federal Statutes Investigated by the FBI
67. Contact FBI Form
68. National White Collar Crime Center (NW3C)
69. Internet Crime Complaint Center (IC3)
70. Department of Homeland Security
71. National Infrastructure Protection Center
72. The G8 Countries: Principles to Combat High-tech Crime
74. Crime Legislation of EU
75. Law Enforcement Interfaces (EnRoute)

Module 55: Computer Forensics and Legal Compliance

1. Legal Compliance
   1.1. Regulatory Compliance and Computer Forensics
   1.2. Legal and Liability Issues
   1.3. Information Security Compliance Assessment

2. Legal Compliance Program
   2.1. Principles of Legal Compliance Program
   2.2. Elements of an Effective Compliance Program
   2.3. Role of Senior Management in Compliance Program
   2.4. Importance of Compliance and Ethics Programs
   2.5. Benefits of Compliance Program
   2.7. Compliance Program Checklist
2.8. Compliance with Consent Decrees

2.9. Memoranda of Understanding/Agreement (MOU/MOA)

2.10. Enterprise Compliance and Risk Analysis

2.11. Creating Effective Compliance Training Program

2.12. Responsibilities of Senior Systems Managers

2.13. Legal Compliance to Prevent Fraud, Waste, and Abuse

3. Terms Related to Legal Compliance

3.1. Copyright Protection

3.2. Copyright Licensing

3.3. Criminal Prosecution

3.4. Due Diligence

3.5. Evidence Collection and Preservation

3.6. Importance of Evidence Collection

3.7. Importance of Evidence Preservation

Module 56: Security Policies

1. Access Control Policy


3. Audit Trails and Logging Policies

4. Documentation Policy

5. Evidence Collection and Preservation Policies

6. Information Security Policy


8. Personnel Security Policies & Guidance

Module 57: Risk Assessment

1. Risk

2. Security Planning

3. Risk Management

3.1. Importance of Risk Management
4. Principle of Risk Management

5. IT Security Risk Management

6. Risk Analysis

7. Conduct Business Impact Analysis (BIA)

8. Roles and Responsibilities of all the Players in the Risk Analysis Process

9. Risk Analysis and/or Vulnerability Assessment Components

10. Risk Policy

11. Risk Assessment

11.1. Importance of Risk Assessment

12. Approval to Operate (ATO) and Interim Approval to Operate (IATO)

12.1. Importance of Risk Assessment to Obtain an IATO and ATO

13. Risk Assessment Methodology

14. Information Sources for Risk Assessments

15. Risk Assessment Process

15.1. Develop Policy and Procedures for Conducting a Risk Assessment

15.2. Write Risk Assessment Reports

15.3. Coordinate Resources to Perform a Risk Assessment

15.4. Risk Assessment Plan

16. Analyze Threats and Vulnerabilities of an Information System

17. Residual Risk

17.1. Explain Residual Risk

18. Residual Risk Policy


19. Cost/benefit Analysis

19.1. Cost/Benefit Analysis for Information Assurance

20. Importance of Cost/Benefit Analysis for Information Assurance

21. Cost/benefit Analysis Procedure

22. Risk Acceptance
22.1. Risk Acceptance Process
23. Management’s Risk Acceptance Posture
24. Risk Assessment and Countermeasures
25. Risk Analysts
26. Risk Mitigation
27. Risk and Certification/Accredition of Information Systems
27.1. Role of Systems Certifiers and Accreditors in Risk Mitigation
28. Role of Documentation in Reducing Risk

Module 58: Evaluation and Certification of Information Systems
1. Accreditation
   1.1. Importance of Accreditation
   1.2. Types of Accreditation
   1.3. Site Accreditation
   1.4. Significance of NSTISSP
2. Approval to Operate (ATO)
3. Interim Approval to Operate (IATO)
   3.1.1. Contents of SSAA
   3.2. Justification for Waiver
4. Cost-Benefit Analysis
5. Information Classification
6. Importance of Information Classification
7. Investigative Authorities
8. Key Management Infrastructure
9. Information Marking
10. Certification Test & Evaluation (CT&E)
11. Certification Tools
12. Product Assurance
12.1. Protection Profiles
12.2. Security Targets
13. Contracting For Security Services
14. Disposition of Classified Material
15. Optical Remanence
16. Magnetic Remanence
17. Facilities Planning
17.1. Importance of Facilities Planning
18. System Disposition/Reutilization
20. System Security Architecture
21. C&A Process for Information System
22. C&A Life Cycle
22.1. Responsibilities Associated with Accreditation
22.2. Roles Associated with Certification
23. Information Ownership

Module 59: Ethics in Computer Forensics
1. Introduction to Computer Forensic Ethics
2. Procedure to Implement Ethics
3. Importance of Computer Ethics
4. Challenges in Teaching Computer Forensics Ethics
5. Ethical Predicaments
6. The Ethical Requirements During Investigation
7. Ethics in Preparation of Forensic Equipments
8. Ethics of Computer Forensic Investigator
9. Maintaining Professional Conduct
10. Ethics in Logical Security
11. Ethics in Obtaining the Evidence
12. Ethics while Preserving the Evidence

13. Ethics in Documenting Evidence

14. Ethics in Bringing Evidence to Courtroom

Module 60: Computer Forensic Tools

1. Software Forensic Tools

1.1. Visual TimeAnalyzer

1.2. X-Ways Forensics

1.3. Evidor

1.4. Slack Space & Data Recovery Tools:

1.5. Ontrack

1.6. Data Recovery Tools:

1.6.1. Device Seizure 1.0

1.6.2. Data Recovery Tools: Forensic Sorter v2.0.1

1.6.3. Data Recovery Tools: Directory Snoop

1.7. Permanent Deletion of Files:

1.7.1. PDWipe

1.7.2. Permanent Deletion of Files: Darik's Boot and Nuke (DBAN)

1.8. File Integrity Checker:

1.8.1. FileMon

1.8.2. File Date Time Extractor (FDTE)

1.8.3. Decode - Forensic Date/Time Decoder

1.9. Disk Imaging Tools: Snapback Datarrest

1.10. Partition Managers: Partimage

1.11. Linux/Unix Tools: Ltools and Mtools

1.12. Password Recovery Tool:

1.12.1. @Stake

1.12.2. Password Recovery Tool: Decryption Collection Enterprise

1.12.3. Password Recovery Tool: AIM Password Decoder
1.12.4. Password Recovery Tool: MS Access Database Password Decoder

1.13. Internet History Viewer:

1.13.1. CookieView - Cookie Decoder

1.13.1.1. Internet History Viewer: Cookie Viewer

1.13.1.2. Internet History Viewer: Cache View

1.13.1.3. Internet History Viewer: FavURLView - Favourite Viewer

1.13.1.4. Internet History Viewer: NetAnalysis

1.14. Multipurpose Tools:

1.14.1. Maresware


1.15. Toolkits:

1.15.1. NTI Tools

1.15.2. Toolkits: R-Tools-I

1.15.3. Toolkits: R-Tools-II

1.15.4. Toolkits: Datalifter

1.15.5. Toolkits: Accessdata

1.15.6. FTK – Forensic Toolkit

1.15.7. Toolkit: Fastbloc

1.15.8. Toolkit: Encase

1.16. Email Recovery Tool:

1.16.1. E-mail Examiner

1.16.2. Network E-mail Examiner

1.17. Case Agent Companion

1.18. Chat Examiner

1.19. Forensic Replicator

1.20. Registry Analyzer
1.21.  ASR Data’s SMART
1.22.  Oxygen Phone Manager
1.23.  SIM Card Seizure
1.24.  Text Searcher
1.25.  Autoruns
1.26.  Autostart Viewer
1.27.  Belkasoft RemovEx
1.28.  HashDig
1.29.  Inforenz Forager
1.30.  KaZ Alyser
1.31.  DiamondCS OpenPorts
1.32.  Pasco
1.33.  Patchit
1.34.  PE Explorer
1.35.  Port Explorer
1.36.  PowerGREP
1.37.  Process Explorer
1.38.  PyFLAG
1.39.  Registry Analyzing Tool: Regmon
1.40.  Reverse Engineering Compiler
1.41.  SafeBack
1.42.  TapeCat
1.43.  Vision

2.  Hardware Computer Forensic Tools
2.1.  Hard Disk Write Protection Tools
2.1.1.  PDBlock
2.1.2.  Nowrite & Firewire Drivedock
2.1.3.  LockDown
2.1.4. Write Protect Card Reader
2.1.5. Drive Lock IDE
2.1.6. Serial-ATA DriveLock Kit
2.1.7. Wipe MASSter
2.1.8. ImageMASSter Solo-3 IT
2.1.9. ImageMASSter 4002i
2.1.10. ImageMasster 3002SCSI
2.1.11. Image MASSter 3004SATA

Module 61: Windows Based Command Line Tools
1. 3Scan
2. AGREP
3. Aircrack
4. ARPFlash
5. ASPNetUserPass
6. AtNow
7. BBIE
8. BFI
9. Renamer
10. BootPart
11. BuiltIn Account Manager
12. bzip2
13. WhoAml
14. Command Line SFV Checker 0.1
15. MaxDIR 2.29
16. Run! 2.6.7
17. Network Ping
18. WinTraceRoute
19. 4NT 8.02
Module 62: Windows Based GUI Tools

1. Process Viewer Tool
   1.1. CurrProcess
   1.2. Process Explorer
   1.3. ProcessMate
   1.4. ServiWin

2. Registry Tool
   2.1. Autoruns
   2.2. Autostart Viewer
   2.3. ERUNT
   2.4. Hijackthis
   2.5. Loadorder
   2.6. Regbrws
   2.7. Regedit PE
   2.8. Regscanner

3. Desktop Utility Tool
   3.1. BossKey
   3.2. Count Characters
   3.3. HoverSnap
   3.4. Lens
   3.5. Pixie
   3.6. PureText
   3.7. ShoWin
   3.8. Sizer
   3.9. SysExporter

4. Office Application Tool:
   4.1. ASCII Values
   4.2. Atlantis Nova
4.3. Character Grid
4.4. DateStat
4.5. DBF Explorer
4.6. DHB Workshop
4.7. firstobject XML Editor
4.8. Foxit PDF Reader
4.9. Irfan View
4.10. MetaPad
4.11. PrintServer
5. Remote Control Tool
5.1. Gencontrol
5.2. IVT
5.3. Putty
5.4. VNC Viewer
6. Network Tools
6.1. Adapterwatch
6.2. Commtest
6.3. CurrPorts
6.4. Hey Joe!
6.5. IP2
6.6. IP Netinfo
6.7. Ldp
6.8. Necrosoft Dig
6.9. Net Send (NT Toolkit)
6.10. POP3 Preview
6.11. Popcorn
6.12. Quick Mailer
6.13. TCPView
6.14. Trout
6.15. WinArpSpoof

7. Network Scanner Tool
7.1. Attack Tool Kit (ATK)
7.2. DDos Ping
7.3. DNSWalker
7.4. DSScan
7.5. GetAcct
7.6. JJIEnc
7.7. MyDoomScanner
7.8. Netstumbler
7.9. RPCScan
7.10. RPCScan2
7.11. ShareEnum
7.12. Shed
7.13. SNScan
7.14. SuperScan4

8. Network Sniffer Tool
8.1. Analyzer
8.2. IPSniffer
8.3. NGSSniff
8.4. Show Traffic
8.5. SmartSniff
8.6. Sniphere

9. Hard Disk Tool
9.1. 48-bit LBA Technology
9.2. Darik’s Boot and Nuke
9.3. DirectDisk
9.4. Disk Checker
9.5. Disk Investigator
9.6. DiskMon
9.7. DiskPatch
9.8. DiskPie Pro
9.9. Emsa Disk Check
9.10. Hard Disk Indicator, HDSpeed
9.11. HD Tach
9.12. HD Tune
9.13. HDClone
9.14. HDINFO Tool
9.15. Maxtor MaxBlast
9.16. Maxtor Powermax
9.17. MBRtool
9.18. MBRWork
9.19. Sectedit
9.20. Sector Inspector
9.21. Western Digital Diagnostic
10. Hardware Info Tools
10.1. Bart’s Stuff Test
10.2. Central Brain Identifier
10.3. Data LifeGuard Diagnostics for Windows
10.4. Drive View
10.5. DTemp
10.6. HD Tune
10.7. HD_Speed
10.8. Monitor Test
10.9. Nero CD/DVD Speed
10.10. Nero Drive Speed
10.11. Nero Info Tool
10.12. ReSysInfo
10.13. SIW
10.14. WinAudit

11. File Management Tool
11.1. 1-4a Rename
11.2. A43
11.3. CD2ISO
11.4. Delold
11.5. Disktools Imagemaker
11.6. Drvcloner XP, Cdmanipulator
11.7. Drvimager XP
11.8. Dscrypt
11.9. Express Burn
11.10. Ntouch, Rawwrite for Windows
11.11. Pablo Commander
11.12. Pagedefrag
11.13. Replace in Files, Splitter Light
11.14. UUD32 Windows
11.15. Wintidy

12. File Recovery Tool
12.1. Handy Recovery
12.2. PC Inspector
12.3. Restoration
12.4. R-Linux
12.5. Smart Recovery
12.6. Zip File Recovery
13. File Transfer Tool
13.1. Babyftp Server
13.2. Babypop3 Server
13.3. Babyweb Server
13.4. Dropupload, File Gateway
13.5. Dropupload, File Gateway
13.6. Freeway FTP
13.7. HFS HTTP File Server
13.8. Nullsoft Copy, Smbdownloader
13.9. Simple Socket File Transfer
13.10. Synchronize It! V1.69
13.11. TFTPD32
13.12. Wackget, Thirdddir
13.13. Unstoppable Copier
13.14. Winscp

14. File Analysis Tool
14.1. AccessEnum
14.2. BinText
14.3. CDMage
14.4. DBF Viewer Plus
14.5. DefragNT
14.6. Dependency Walker
14.7. Disk Investigator
14.8. DiskView
14.9. DupeLocator
14.10. E-Grabber
14.11. ExamDiff
14.12. Explore2FS
14.13. File Analyzer
14.15. Folders Report
14.16. Gemulator Explorer
14.17. HashCalc
14.18. Lister
14.19. MDB View
14.20. Media Checker
14.21. PEiD
14.22. Resource Hacker
14.23. Space Monger
14.24. Tiny Hexer
14.25. Virtual Floppy Driver
14.26. Win Interrogate
14.27. xTeq X-Find
15. Password Tool
15.1. CISCO PIX Firewall Password Calculator
15.2. Encode Unix Password
15.3. Password Assistant (NTToolkit)
15.4. Password Generator
16. Password Cracking Tool
16.1. Access PassView
16.2. Chat Recovery
16.3. Asterisk Logger
16.4. Basic Authentication
16.5. Brutus
16.6. DeBat!
16.7. Dialupass
16.8. Enterprise Manager PassView
16.9. GetKey
16.10. GetPass
16.11. Keyfinder
16.12. Lepton’s crack
16.13. Mail PassView
16.14. Messenger Key
16.15. MessenPass
16.16. Netscapass
16.17. Outlooker
16.18. PCAnywhere PassView
16.19. Protected Storage PassView
16.20. RockXP
16.21. Share Password Checker
16.22. X-Pass
17. Other GUI Tools:
17.1. AtomicTime, FavouritesView
17.2. IECookiesView
17.3. IEHistoryView
17.4. MozillaCookiesViewer
17.5. MyUninstaller
17.6. Neutron
17.7. NewSID
17.8. ShortCutsMan
17.9. Timer, Stinger
17.10. WinUpdatesList
17.11. DB2 MAESTRO 8.4
17.12. ORACLE MAESTRO 8.3
17.13. SQL MAESTRO FOR MYSQL 8.3
17.14. EMS SQL MANAGER 2007 FOR ORACLE 1.1
17.15. EMS SQL MANAGER 2005 FOR POSTGRESQL 3.7
17.16. EMS SQL MANAGER 2008 FOR SQL SERVER 3.0
17.17. EMS SQL MANAGER 2007 FOR POSTGRESQL 4.3
17.18. EMS SQL MANAGER 2008 FOR INTERBASE/FIREBIRD 5.0
17.19. EMS SQL MANAGER FOR DBISAM 1.6
17.20. MS SQL Maestro 8.1
17.21. SQLite Maestro 8.5
17.22. SQLite Data Wizard 8.4
17.23. SQLite Code Factory 7.5
17.24. SQLite PHP Generator 8.1
17.25. Hash 1.04
17.26. Navicat MySQL Manager for Linux 8.0.22

Module 63: Forensics Frameworks

1. FORZA Framework
   1.1. What is Forensics Framework?
   1.2. Fundamental Principle in Digital Forensics Investigation Procedures
   1.3. FORZA Framework
   1.4. Roles and Responsibilities of Participants in Digital Forensics Investigation Procedures
   1.5. Process Flow in FORZA Framework
   1.6. High-level View of FORZA Framework
   1.7. FORZA Framework Layers
   1.8. Contextual Investigation Layer
   1.9. Contextual Layer
   1.10. Legal Advisory Layer
   1.11. Conceptual Security Layer
   1.12. Technical Presentation Layer
1.13. Data Acquisition Layer
1.14. Data Analysis Layer
1.15. Legal Presentation Layer

2. An Event-Based Digital Forensic Investigation Framework
2.1. Event-based Framework
2.2. Digital Analysis Types
2.3. Digital Investigation Process Model
2.4. Digital Crime Scene Investigation Phases

3. Enhanced Digital Investigation Process Model
3.1. Enhanced Digital Investigation Process Model
3.2. Physical Crime Scene Investigation
3.3. Digital Crime Scene Investigation
3.4. Phases of Enhanced Digital Investigation Process Model

4. Extended Model of Cybercrime Investigations
4.1. Extended Model of Cybercrime Investigations
4.2. Activities in Cybercrime Investigations

5. Computer Forensics Field Triage Process Model
5.1. Computer Forensics Field Triage Process Model
5.2. Computer Forensics Field Triage Process Model Phases

6.1. Objectives-based Framework
6.2. Proposed Digital Investigation Process
6.3. Objectives-Based Framework Phases

Module 64: Forensics Investigation Templates
1. Case Feedback Form
2. Seizure Record
3. List of Evidence Gathered Form
4. Evidence Preservation Checklist
5. BIOS Configuration
6. System Configuration
7. Application Summary
8. Monitor Investigation Checklist
9. Hard Disk Investigation Checklist
10. Floppy Investigation Checklist
11. CD Investigation Checklist
12. Zip Drive Investigation Checklist
13. Flash Drives Investigation Checklist
14. Tape Investigation Checklist
15. Handheld Device Investigation Checklist: Blackberry
16. Handheld Device Investigation Checklist: iPod
17. Handheld Device Investigation Checklist: Mobile Phone
18. Handheld Device Investigation Checklist: PDA
19. Fax Investigation Checklist
20. Hub Investigation Checklist
21. Switch Investigation Checklist
22. Router Investigation Checklist
23. Physical Security Checklist
24. Identity Theft Checklist

Module 65: Computer Forensics Consulting Companies

1. Burgess Forensics
2. Center for Computer Forensics (CCF)
3. Navigant Consulting
4. ACR Data Recovery
5. Computer Forensic Services
6. Cyber Evidence Inc.
7. Data Recon
8. ADR (American Data Recovery) Computer Forensics
10. CIA Solutions
11. Federal Bureau of Investigation (FBI)
12. Interpol
13. National Center for Missing and Exploited Children (NCMEC)
14. Logicube
15. Logicube: Screenshot
16. LJ Forensics
17. Intelligent Computer Solutions (ICS)
18. Intelligent Computer Solutions (ICS): Screenshot
19. Cy4or
20. Forensicon
21. Global Digital Forensics
22. Integrity Security & Investigation Services, Inc. (ISIS)
23. Trial Solutions
24. Digital Detective
25. Florida Department of Law Enforcement
26. Northern California Computer Crimes Task Force (NC3TF)
27. Child Exploitation and Online Protection Centre (CEOP)
28. eFrauda
29. International Association of Computer Investigative Specialists (IACIS)
30. 7Safe
31. Adroit Infotech Consultancy Service
32. Digital Medix
33. Hill Schwartz Spilker Keller LLC (HSSK)
34. IRIS Data Services
35. Computer Forensic Labs, Inc.
For more information or query please feel free to contact us:

**Byte Code Cyber Securities**

**Address:** 72-B, 3rd Floor,
Vikas Marg, Laxmi Nagar,
New Delhi: 110092
Near Nirman Vihar Metro Station, Opposite Pillar No.50

**Telephone:** +91-64601115, +91-9210001115
**Website:** www.bytec0de.com
**Email:** info@bytec0de.com