CHFIv8 course outline:
Module 01: Computer Forensics in Today's World

1. Forensics Science
2. Computer Forensics
   1. Security Incident Report
   2. Aspects of Organizational Security
   3. Evolution of Computer Forensics
   4. Objective of Computer Forensics
   5. Need for Computer Forensics
3. Forensics Readiness
   1. Benefits of Forensics Readiness
   2. Goals of Forensics Readiness
   3. Forensics Readiness Planning
4. Cyber Crime
   1. Computer Facilitated Crimes
   2. Modes of Attacks
   3. Examples of Cyber Crime
   4. Types of Computer Crimes
   5. Cyber Criminals
   6. Organized Cyber Crime: Organizational Chart
   7. How Serious are Different Types of Incidents?
   8. Disruptive Incidents to the Business
   9. Cost Expenditure Responding to the Security Incident
5. Cyber Crime Investigation
   1. Key Steps in Forensics Investigation
   2. Rules of Forensics Investigation
   3. Need for Forensics Investigator
   4. Role of Forensics Investigator
   5. Accessing Computer Forensics Resources
   6. Role of Digital Evidence
6. Corporate Investigations
   1. Understanding Corporate Investigations
   2. Approach to Forensics Investigation: A Case Study
   3. Instructions for the Forensic Investigator to Approach the Crime Scene
   4. Why and When Do You Use Computer Forensics?
   5. Enterprise Theory of Investigation (ETI)
   6. Legal Issues
   7. Reporting the Results
7. Reporting a Cyber Crime
   1. Why you Should Report Cybercrime?
   2. Reporting Computer-Related Crimes
   3. Person Assigned to Report the Crime
   4. When and How to Report an Incident?
   5. Who to Contact at the Law Enforcement?
   6. Federal Local Agents Contact
Module 02: Computer Forensics Investigation Process

1. Investigating Computer Crime
   1. Before the Investigation
   2. Build a Forensics Workstation
   3. Building the Investigation Team
   4. People Involved in Computer Forensics
   5. Review Policies and Laws
   6. Forensics Laws
   7. Notify Decision Makers and Acquire Authorization
   8. Risk Assessment
   9. Build a Computer Investigation Toolkit

2. Steps to Prepare for a Computer Forensics Investigation

3. Computer Forensics Investigation Methodology
   1. Obtain Search Warrant
      1. Example of Search Warrant
      2. Searches Without a Warrant
   2. Evaluate and Secure the Scene
      1. Forensics Photography
      2. Gather the Preliminary Information at the Scene
      3. First Responder
   3. Collect the Evidence
      1. Collect Physical Evidence
         1. Evidence Collection Form
      2. Collect Electronic Evidence
      3. Guidelines for Acquiring Evidence
   4. Secure the Evidence
      1. Evidence Management
      2. Chain of Custody
         1. Chain of Custody Form
   5. Acquire the Data
      1. Duplicate the Data (Imaging)
      2. Verify Image Integrity
         1. MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
      3. Recover Lost or Deleted Data
         1. Data Recovery Software
   6. Analyze the Data
      1. Data Analysis
      2. Data Analysis Tools
   7. Assess Evidence and Case
      1. Evidence Assessment
Module 03: Searching and Seizing Computers

1. Searching and Seizing Computers without a Warrant
   1. Searching and Seizing Computers without a Warrant
   2. § A: Fourth Amendment’s “Reasonable Expectation of Privacy” in Cases Involving Computers: General Principles
   3. § A.1: Reasonable Expectation of Privacy in Computers as Storage Devices
   4. § A.3: Reasonable Expectation of Privacy and Third-Party Possession
   5. § A.4: Private Searches
   6. § A.5 Use of Technology to Obtain Information
   7. § B: Exceptions to the Warrant Requirement in Cases Involving Computers
   8. § B.1: Consent
   9. § B.1.a: Scope of Consent
   10. § B.1.b: Third-Party Consent
   11. § B.1.c: Implied Consent
   12. § B.2: Exigent Circumstances
   13. § B.3: Plain View
   14. § B.4: Search Incident to a Lawful Arrest
   15. § B.5: Inventory Searches
   16. § B.6: Border Searches
   17. § B.7: International Issues
   18. § C: Special Case: Workplace Searches
   19. § C.1: Private Sector Workplace Searches
   20. § C.2: Public-Sector Workplace Searches

2. Searching and Seizing Computers with a Warrant
   1. Searching and Seizing Computers with a Warrant
   2. A: Successful Search with a Warrant
   3. A.1: Basic Strategies for Executing Computer Searches
   4. § A.1.a: When Hardware is itself Contraband, Evidence, or an Instrumentality or
Module 04: Digital Evidence
1. Digital Data
   1. Definition of Digital Evidence
   2. Increasing Awareness of Digital Evidence
   3. Challenging Aspects of Digital Evidence
   4. The Role of Digital Evidence
   5. Characteristics of Digital Evidence
   6. Fragility of Digital Evidence
   7. Anti-Digital Forensics (ADF)

2. Types of Digital Data
   1. Types of Digital Data

3. Rules of Evidence
   1. Rules of Evidence
   2. Best Evidence Rule
   3. Federal Rules of Evidence
   4. International Organization on Computer Evidence (IOCE)
   5. IOCE International Principles for Digital Evidence
   6. Scientific Working Group on Digital Evidence (SWGDE)
   7. SWGDE Standards for the Exchange of Digital Evidence

4. Electronic Devices: Types and Collecting Potential Evidence
   1. Electronic Devices: Types and Collecting Potential Evidence

5. Digital Evidence Examination Process
   1. Evidence Assessment
      1. Evidence Assessment
      2. Prepare for Evidence Acquisition
   2. Evidence Acquisition
      1. Preparation for Searches
      2. Seizing the Evidence
      3. Imaging
      4. Bit-Stream Copies
      5. Write Protection
      6. Evidence Acquisition
      7. Evidence Acquisition from Crime Location
      8. Acquiring Evidence from Storage Devices
      9. Collecting Evidence
     10. Collecting Evidence from RAM
     11. Collecting Evidence from a Standalone Network Computer
     12. Chain of Custody
     13. Chain of Evidence Form
   3. Evidence Preservation
      1. Preserving Digital Evidence: Checklist
      2. Preserving Removable Media
      3. Handling Digital Evidence
      4. Store and Archive
      5. Digital Evidence Findings
   4. Evidence Examination and Analysis
1. Evidence Examination
2. Physical Extraction
3. Logical Extraction
4. Analyze Host Data
5. Analyze Storage Media
6. Analyze Network Data
7. Analysis of Extracted Data
8. Timeframe Analysis
9. Data Hiding Analysis
10. Application and File Analysis
11. Ownership and Possession

5. Evidence Documentation and Reporting
   1. Documenting the Evidence
   2. Evidence Examiner Report
   3. Final Report of Findings
   4. Computer Evidence Worksheet
   5. Hard Drive Evidence Worksheet
   6. Removable Media Worksheet

   1. Electronic Crime and Digital Evidence Consideration by Crime Category

---

**Module 05: First Responder Procedures**

1. Electronic Evidence
2. First Responder
3. Roles of First Responder
4. Electronic Devices: Types and Collecting Potential Evidence
5. First Responder Toolkit
   1. First Responder Toolkit
   2. Creating a First Responder Toolkit
   3. Evidence Collecting Tools and Equipment
6. First Response Basics
   1. First Response Rule
   2. Incident Response: Different Situations
   3. First Response for System Administrators
   4. First Response by Non-Laboratory Staff
   5. First Response by Laboratory Forensics Staff
7. Securing and Evaluating Electronic Crime Scene
   2. Securing the Crime Scene
   3. Warrant for Search and Seizure
   4. Planning the Search and Seizure
   5. Initial Search of the Scene
   6. Health and Safety Issues
8. Conducting Preliminary Interviews
1. Questions to Ask When Client Calls the Forensic Investigator
2. Consent
3. Sample of Consent Search Form
4. Witness Signatures
5. Conducting Preliminary Interviews
6. Conducting Initial Interviews
7. Witness Statement Checklist

9. Documenting Electronic Crime Scene
   1. Documenting Electronic Crime Scene
   2. Photographing the Scene
   3. Sketching the Scene
   4. Video Shooting the Crime Scene

10. Collecting and Preserving Electronic Evidence
    1. Collecting and Preserving Electronic Evidence
    2. Order of Volatility
    3. Dealing with Powered On Computers
    4. Dealing with Powered Off Computers
    5. Dealing with Networked Computer
    6. Dealing with Open Files and Startup Files
    7. Operating System Shutdown Procedure
    8. Computers and Servers
    9. Preserving Electronic Evidence
    10. Seizing Portable Computers
    11. Switched On Portables
    12. Collecting and Preserving Electronic Evidence

11. Packaging and Transporting Electronic Evidence
    1. Evidence Bag Contents List
    2. Packaging Electronic Evidence
    3. Exhibit Numbering
    4. Transporting Electronic Evidence
    5. Handling and Transportation to the Forensics Laboratory
    6. Storing Electronic Evidence
    7. Chain of Custody
    8. Simple Format of the Chain of Custody Document
    9. Chain of Custody Forms
    10. Chain of Custody on Property Evidence Envelope/Bag and Sign-out Sheet

12. Reporting the Crime Scene
    1. Reporting the Crime Scene

13. Note Taking Checklist
14. First Responder Common Mistakes

---

Module 06: Computer Forensics Lab

1. Setting a Computer Forensics Lab
   1. Computer Forensics Lab
2. Planning for a Forensics Lab
3. Budget Allocation for a Forensics Lab
4. Physical Location Needs of a Forensics Lab
5. Structural Design Considerations
6. Environmental Conditions
7. Electrical Needs
8. Communication Needs
9. Work Area of a Computer Forensics Lab
10. Ambience of a Forensics Lab
11. Ambience of a Forensics Lab: Ergonomics
12. Physical Security Recommendations
13. Fire-Suppression Systems
14. Evidence Locker Recommendations
15. Computer Forensic Investigator
16. Law Enforcement Officer
17. Lab Director
18. Forensics Lab Licensing Requisite
19. Features of the Laboratory Imaging System
20. Technical Specification of the Laboratory-Based Imaging System
21. Forensics Lab
22. Auditing a Computer Forensics Lab
23. Recommendations to Avoid Eyestrain

2. Investigative Services in Computer Forensics
   1. Computer Forensics Investigative Services
   2. Computer Forensic Investigative Service Sample
   3. Computer Forensics Services: PenrodEllis Forensic Data Discovery
   4. Data Destruction Industry Standards
   5. Computer Forensics Services

3. Computer Forensics Hardware
   1. Equipment Required in a Forensics Lab
   2. Forensic Workstations
   3. Basic Workstation Requirements in a Forensics Lab
   4. Stocking the Hardware Peripherals
   5. Paraben Forensics Hardware
      1. Handheld First Responder Kit
      2. Wireless StrongHold Bag
      3. Wireless StrongHold Box
      4. Passport StrongHold Bag
      5. Device Seizure Toolbox
      6. Project-a-Phone
      7. Lockdown
      8. iRecovery Stick
      9. Data Recovery Stick
     10. Chat Stick
     11. USB Serial DB9 Adapter
     12. Mobile Field Kit
7. Portable Forensic Systems and Towers: Original Forensic Tower II and F
8. Portable Forensic Workhorse V: Tableau 335 Forensic Drive Bay Controller
11. Portable Forensic Systems and Towers: Forensic Tower IV Dual Xeon
13. Forensic Write Protection Devices and Kits: Ultimate Forensic Write Protection Kit II-ES
14. Tableau T3u Forensic SATA Bridge Write Protection Kit
15. Tableau T8 Forensic USB Bridge Kit/Addonics Mini DigiDrive READ ONLY 12-in-1 Flash Media Reader
16. Tableau TACC 1441 Hardware Accelerator
   1. Multiple TACC1441 Units
17. Tableau TD1 Forensic Duplicator
18. Power Supplies and Switches
19. Digital Intelligence Forensic Hardware
   1. FRED SR (Dual Xeon)
   2. FRED-L
   3. FRED SC
   4. Forensic Recovery of Evidence Data Center (FREDC)
   5. Rack-A-TACC
   6. FREDDIE
   7. UltraKit
   8. UltraBay II
   9. UltraBlock SCSI
   10. Micro Forensic Recovery of Evidence Device (μFRED)
   11. HardCopy 3P
20. Wiebetech
   1. Forensics DriveDock v4
   2. Forensics UltraDock v4
   3. Drive eRazer
   4. v4 Combo Adapters
   5. ProSATA SS8
   6. HotPlug
21. CelleBrite
   1. UFED System
   2. UFED Physical Pro
   3. UFED Ruggedized
22. DeepSpar
   1. Disk Imager Forensic Edition
   2. 3D Data Recovery
   3. Phase 1 Tool: PC-3000 Drive Restoration System
   4. Phase 2 Tool: DeepSpar Disk Imager
   5. Phase 3 Tool: PC-3000 Data Extractor
23. InfinaDyne Forensic Products
1. Robotic Loader Extension for CD/DVD Inspector
2. Robotic System Status Light

24. Image MASSter
   1. Solo-4 (Super Kit)
   2. RoadMASSter- 3
   3. WipeMASSter
   4. WipePRO
   5. Rapid Image 7020CS IT

25. Logicube
   1. Forensic MD5
   2. Forensic Talon®
   3. Portable Forensic Lab™
   4. CellIDEK®
   5. Forensic Quest-2®
   6. NETConnect™
   7. RAID I/O Adapter™
   8. GPStamp™
   9. OmniPort
   10. Desktop WritePROtects
   11. USB Adapter
   12. CloneCard Pro
   13. EchoPlus
   14. OmniClone IDE Laptop Adapters
   15. Cables

26. VoomTech
   1. HardCopy 3P
   2. SHADOW 2

4. Computer Forensics Software
   1. Basic Software Requirements in a Forensic Lab
   2. Maintain Operating System and Application Inventories
   3. Imaging Software
      1. R-drive Image
      2. P2 eXplorer Pro
      3. AccuBurn-R for CD/DVD Inspector
      4. Flash Retriever Forensic Edition
   4. File Conversion Software
      1. FileMerlin
      2. SnowBatch®
      3. Zamzar
   5. File Viewer Software
      1. File Viewer
      2. Quick View Plus 11 Standard Edition
   6. Analysis Software
      1. P2 Commander
      2. DriveSpy
      3. SIM Card Seizure
4. CD/DVD Inspector
5. Video Indexer (Vindex™)
7. Monitoring Software
   1. Device Seizure
   2. Deployable P2 Commander (DP2C)
   3. ThumbsDisplay
   4. Email Detective
8. Computer Forensics Software
   1. DataLifter
   2. X-Ways Forensics
   3. LiveWire Investigator

Module 07: Understanding Hard Disks and File Systems

1. Hard Disk Drive Overview
   1. Disk Drive Overview
   2. Hard Disk Drive
   3. Solid-State Drive (SSD)
   4. Physical Structure of a Hard Disk
   5. Logical Structure of Hard Disk
   6. Types of Hard Disk Interfaces
   7. Hard Disk Interfaces
      1. ATA
      2. SCSI
      3. IDE/EIDE
      4. USB
      5. Fibre Channel
8. Disk Platter
9. Tracks
   1. Track Numbering
10. Sector
    1. Advanced Format: Sectors
    2. Sector Addressing
11. Cluster
    1. Cluster Size
    2. Changing the Cluster Size
    3. Slack Space
    4. Lost Clusters
12. Bad Sector
13. Hard Disk Data Addressing
14. Disk Capacity Calculation
15. Measuring the Performance of the Hard Disk

2. Disk Partitions and Boot Process
   1. Disk Partitions
   2. Master Boot Record
1. Structure of a Master Boot Record
3. What is the Booting Process?
4. Essential Windows System Files
5. Windows Boot Process
6. Macintosh Boot Process

3. Understanding File Systems
1. Understanding File Systems
2. Types of File Systems
3. List of Disk File Systems
4. List of Network File Systems
5. List of Special Purpose File Systems
6. List of Shared Disk File Systems
7. Popular Windows File Systems

1. File Allocation Table (FAT)
   1. FAT File System Layout
   2. FAT Partition Boot Sector
   3. FAT Structure
   4. FAT Folder Structure
   5. Directory Entries and Cluster Chains
   6. Filenames on FAT Volumes
   7. Examining FAT
   8. FAT32

2. New Technology File System (NTFS)
   1. NTFS Architecture
   2. NTFS System Files
   3. NTFS Partition Boot Sector
   4. Cluster Sizes of NTFS Volume
   5. NTFS Master File Table (MFT)
      1. Metadata Files Stored in the MFT
   6. NTFS Files and Data Storage
   7. NTFS Attributes
   8. NTFS Data Stream
   9. NTFS Compressed Files
      1. Setting the Compression State of a Volume

10. Encrypting File Systems (EFS)
    1. Components of EFS
    2. Operation of Encrypting File System
    3. EFS Attribute
    4. Encrypting a File
    5. EFS Recovery Key Agent
    6. Tool: Advanced EFS Data Recovery
    7. Tool: EFS Key

11. Sparse Files
12. Deleting NTFS Files

3. Registry Data
4. Examining Registry Data
5. FAT vs. NTFS
8. Popular Linux File Systems
   1. Linux File System Architecture
   2. Ext2
   3. Ext3
9. Mac OS X File System
   1. HFS vs. HFS Plus
   2. HFS
   3. HFS Plus
      1. HFS Plus Volumes
      2. HFS Plus Journal
10. Sun Solaris 10 File System: ZFS
11. CD-ROM / DVD File System
12. CDFS
4. RAID Storage System
   1. RAID Levels
   2. Different RAID Levels
   3. Comparing RAID Levels
   4. Recover Data from Unallocated Space Using File Carving Process
5. File System Analysis Using The Sleuth Kit (TSK)
   1. The Sleuth Kit (TSK)
      1. The Sleuth Kit (TSK): fsstat
      2. The Sleuth Kit (TSK): istat
      3. The Sleuth Kit (TSK): fls and img_stat

Module 08: Windows Forensics

1. Collecting Volatile Information
   1. Volatile Information
      1. System Time
         1. Logged-on Users
         2. Psloggedon
         3. Net Sessions Command
         4. Logonsessions Tool
      2. Open Files
         1. Net File Command
         2. PsFile Command
         3. OpenFiles Command
      3. Network Information
      4. Network Connections
      5. Process Information
      6. Process-to-Port Mapping
      7. Process Memory
      8. Network Status
9. Other Important Information

2. Collecting Non-volatile Information
   1. Non-volatile Information
      1. Examine File Systems
      2. Registry Settings
      3. Microsoft Security ID
      4. Event Logs
      5. Index.dat File
      6. Devices and Other Information
      7. Slack Space
      8. Virtual Memory
      9. Swap File
      10. Windows Search Index
      11. Collecting Hidden Partition Information
      12. Hidden ADS Streams
         1. Investigating ADS Streams: StreamArmor
      13. Other Non-Volatile Information

3. Windows Memory Analysis
   1. Memory Dump
   2. EProcess Structure
   3. Process Creation Mechanism
   4. Parsing Memory Contents
   5. Parsing Process Memory
   6. Extracting the Process Image
   7. Collecting Process Memory

4. Windows Registry Analysis
   1. Inside the Registry
   2. Registry Structure within a Hive File
   3. The Registry as a Log File
   4. Registry Analysis
   5. System Information
   6. TimeZone Information
   7. Shares
   8. Audit Policy
   9. Wireless SSIDs
   10. Autostart Locations
   11. System Boot
   12. User Login
   13. User Activity
   14. Enumerating Autostart Registry Locations
   15. USB Removable Storage Devices
   16. Mounted Devices
   17. Finding Users
   18. Tracking User Activity
   19. The UserAssist Keys
   20. MRU Lists
21. Search Assistant
22. Connecting to Other Systems
23. Analyzing Restore Point Registry Settings
24. Determining the Startup Locations

5. Cache, Cookie, and History Analysis
   1. Cache, Cookie, and History Analysis in IE
   2. Cache, Cookie, and History Analysis in Firefox
   3. Cache, Cookie, and History Analysis in Chrome
   4. Analysis Tools
      1. IE Cookies View
      2. IE Cache View
      3. IE History Viewer
      4. MozillaCookiesView
      5. MozillaCacheView
      6. MozillaHistoryView
      7. ChromeCookiesView
      8. ChromeCacheView
      9. ChromeHistoryView

6. MD5 Calculation
   1. Message Digest Function: MD5
   2. Why MD5 Calculation?
   3. MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
   4. MD5 Checksum Verifier
   5. ChaosMD5

7. Windows File Analysis
   1. Recycle Bin
   2. System Restore Points (Rp.log Files)
   3. System Restore Points (Change.log.x Files)
   4. Prefetch Files
   5. Shortcut Files
   6. Word Documents
   7. PDF Documents
   8. Image Files
   9. File Signature Analysis
   10. NTFS Alternate Data Streams
   11. Executable File Analysis
   12. Documentation Before Analysis
   13. Static Analysis Process
   14. Search Strings
   15. PE Header Analysis
   16. Import Table Analysis
   17. Export Table Analysis
   18. Dynamic Analysis Process
   19. Creating Test Environment
   20. Collecting Information Using Tools
8. Metadata Investigation
   1. Metadata
   2. Types of Metadata
   3. Metadata in Different File Systems
   4. Metadata in PDF Files
   5. Metadata in Word Documents
   6. Tool: Metadata Analyzer

9. Text Based Logs
   1. Understanding Events
   2. Event Logon Types
   3. Event Record Structure
   4. Vista Event Logs
   5. IIS Logs
      1. Parsing IIS Logs
   6. Parsing FTP Logs
      1. FTP sc-status Codes
   7. Parsing DHCP Server Logs
   8. Parsing Windows Firewall Logs
   9. Using the Microsoft Log Parser

10. Other Audit Events
    1. Evaluating Account Management Events
    2. Examining Audit Policy Change Events
    3. Examining System Log Entries
    4. Examining Application Log Entries

11. Forensic Analysis of Event Logs
    1. Searching with Event Viewer
    2. Using EnCase to Examine Windows Event Log Files
    3. Windows Event Log Files Internals

12. Windows Password Issues
    1. Understanding Windows Password Storage
    2. Cracking Windows Passwords Stored on Running Systems
    3. Exploring Windows Authentication Mechanisms
       1. LanMan Authentication Process
       2. NTLM Authentication Process
       3. Kerberos Authentication Process
    4. Sniffing and Cracking Windows Authentication Exchanges
    5. Cracking Offline Passwords

13. Forensic Tools
    1. Windows Forensics Tool: OS Forensics
    2. Windows Forensics Tool: Helix3 Pro
    3. Integrated Windows Forensics Software: X-Ways Forensics
    4. X-Ways Trace
    5. Windows Forensic Toolchest (WFT)
    7. Computer Online Forensic Evidence Extractor (COFEE)
    8. System Explorer
9. Tool: System Scanner
10. SecretExplorer
11. Registry Viewer Tool: Registry Viewer
12. Registry Viewer Tool: RegScanner
13. Registry Viewer Tool: Alien Registry Viewer
14. MultiMon
15. CurrProcess
16. Process Explorer
17. Security Task Manager
18. PrcView
19. ProcHeapViewer
20. Memory Viewer
21. Tool: PMDump
22. Word Extractor
23. Belkasoft Evidence Center
24. Belkasoft Browser Analyzer
25. Metadata Assistant
26. HstEx
27. XpoLog Center Suite
28. LogViewer Pro
29. Event Log Explorer
30. LogMeister
31. ProDiscover Forensics
32. PyFlag
33. LiveWire Investigator
34. ThumbsDisplay
35. DriveLook

Module 09: Data Acquisition and Duplication

1. Data Acquisition and Duplication Concepts
   1. Data Acquisition
   2. Forensic and Procedural Principles
   3. Types of Data Acquisition Systems
   4. Data Acquisition Formats
   5. Bit Stream vs. Backups
   6. Why to Create a Duplicate Image?
   7. Issues with Data Duplication
   8. Data Acquisition Methods
   9. Determining the Best Acquisition Method
10. Contingency Planning for Image Acquisitions
11. Data Acquisition Mistakes

2. Data Acquisition Types
   1. Rules of Thumb
   2. Static Data Acquisition
1. Collecting Static Data
2. Static Data Collection Process
3. Live Data Acquisition
   1. Why Volatile Data is Important?
   2. Volatile Data
   3. Order of Volatility
   4. Common Mistakes in Volatile Data Collection
   5. Volatile Data Collection Methodology
   6. Basic Steps in Collecting Volatile Data
   7. Types of Volatile Information
3. Disk Acquisition Tool Requirements
   1. Disk Imaging Tool Requirements
   2. Disk Imaging Tool Requirements: Mandatory
   3. Disk Imaging Tool Requirements: Optional
4. Validation Methods
   1. Validating Data Acquisitions
   2. Linux Validation Methods
   3. Windows Validation Methods
5. RAID Data Acquisition
   1. Understanding RAID Disks
   2. Acquiring RAID Disks
   3. Remote Data Acquisition
6. Acquisition Best Practices
   1. Acquisition Best Practices
7. Data Acquisition Software Tools
   1. Acquiring Data on Windows
   2. Acquiring Data on Linux
   3. dd Command
   4. dcfldd Command
   5. Extracting the MBR
   6. Netcat Command
   7. EnCase Forensic
   8. Analysis Software: DriveSpy
   9. ProDiscover Forensics
   10. AccessData FTK Imager
   11. Mount Image Pro
   12. Data Acquisition Toolbox
   13. SafeBack
   14. iLookPI
   15. RAID Recovery for Windows
   16. R-Tools R-Studio
   17. F-Response
   18. PyFlag
   19. LiveWire Investigator
   20. ThumbsDisplay
   21. DataLifter
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>X-Ways Forensics</td>
</tr>
<tr>
<td>23.</td>
<td>R-drive Image</td>
</tr>
<tr>
<td>24.</td>
<td>DriveLook</td>
</tr>
<tr>
<td>25.</td>
<td>DiskExplorer</td>
</tr>
<tr>
<td>26.</td>
<td>P2 eXplorer Pro</td>
</tr>
<tr>
<td>27.</td>
<td>Flash Retriever Forensic Edition</td>
</tr>
<tr>
<td>8.</td>
<td>Data Acquisition Hardware Tools</td>
</tr>
<tr>
<td>1.</td>
<td>US-LATT</td>
</tr>
<tr>
<td>2.</td>
<td>Image MASSter: Solo-4 (Super Kit)</td>
</tr>
<tr>
<td>3.</td>
<td>Image MASSter: RoadMASSter-3</td>
</tr>
<tr>
<td>4.</td>
<td>Tableau TD1 Forensic Duplicator</td>
</tr>
<tr>
<td>5.</td>
<td>Logicube: Forensic MD5</td>
</tr>
<tr>
<td>6.</td>
<td>Logicube: Portable Forensic Lab™</td>
</tr>
<tr>
<td>7.</td>
<td>Logicube: Forensic Talon®</td>
</tr>
<tr>
<td>8.</td>
<td>Logicube: RAID I/O Adapter™</td>
</tr>
<tr>
<td>10.</td>
<td>Logicube: USB Adapter</td>
</tr>
<tr>
<td>11.</td>
<td>Disk Jockey PRO</td>
</tr>
<tr>
<td>12.</td>
<td>Logicube: Forensic Quest-2®</td>
</tr>
<tr>
<td>13.</td>
<td>Logicube: CloneCard Pro</td>
</tr>
<tr>
<td>14.</td>
<td>Logicube: EchoPlus</td>
</tr>
<tr>
<td>15.</td>
<td>Paraben Forensics Hardware: Chat Stick</td>
</tr>
<tr>
<td>16.</td>
<td>Image MASSter: Rapid Image 7020CS IT</td>
</tr>
<tr>
<td>17.</td>
<td>Digital Intelligence Forensic Hardware: UltraKit</td>
</tr>
<tr>
<td>18.</td>
<td>Digital Intelligence Forensic Hardware: UltraBay II</td>
</tr>
<tr>
<td>19.</td>
<td>Digital Intelligence Forensic Hardware: UltraBlock SCSI</td>
</tr>
<tr>
<td>20.</td>
<td>Digital Intelligence Forensic Hardware: HardCopy 3P</td>
</tr>
<tr>
<td>21.</td>
<td>Wiebetech: Forensics DriveDock v4</td>
</tr>
<tr>
<td>22.</td>
<td>Wiebetech: Forensics UltraDock v4</td>
</tr>
<tr>
<td>23.</td>
<td>Image MASSter: WipeMASSter</td>
</tr>
<tr>
<td>24.</td>
<td>Image MASSter: WipePRO</td>
</tr>
<tr>
<td>26.</td>
<td>Forensic Tower IV Dual Xeon</td>
</tr>
<tr>
<td>27.</td>
<td>Digital Intelligence Forensic Hardware: FREDDIE</td>
</tr>
<tr>
<td>28.</td>
<td>DeepSpar: 3D Data Recovery</td>
</tr>
<tr>
<td>1.</td>
<td>Phase 1 Tool: PC-3000 Drive Restoration System</td>
</tr>
<tr>
<td>2.</td>
<td>Phase 2 Tool: DeepSpar Disk Imager</td>
</tr>
<tr>
<td>3.</td>
<td>Phase 3 Tool: PC-3000 Data Extractor</td>
</tr>
<tr>
<td>29.</td>
<td>Logicube</td>
</tr>
<tr>
<td>1.</td>
<td>Cables</td>
</tr>
<tr>
<td>2.</td>
<td>Adapters</td>
</tr>
<tr>
<td>3.</td>
<td>GPStamp™</td>
</tr>
<tr>
<td>4.</td>
<td>OmniPort</td>
</tr>
<tr>
<td>5.</td>
<td>CellIDEK®</td>
</tr>
<tr>
<td>30.</td>
<td>Paraben Forensics Hardware</td>
</tr>
<tr>
<td>1.</td>
<td>Project-a-Phone</td>
</tr>
</tbody>
</table>
Module 10: Recovering Deleted Files and Deleted Partitions

1. Recovering the Deleted Files
   1. Deleting Files
   2. What Happens When a File is Deleted in Windows?
   3. Recycle Bin in Windows
      1. Storage Locations of Recycle Bin in FAT and NTFS System
      2. How the Recycle Bin Works
      3. Damaged or Deleted INFO File
      4. Damaged Files in Recycled Folder
      5. Damaged Recycle Folder
   4. File Recovery in MAC OS X
   5. File Recovery in Linux

2. File Recovery Tools for Windows
   1. Recover My Files
   2. EASEUS Data Recovery Wizard
   3. PC INSPECTOR File Recovery
   4. Recuva
   5. DiskDigger
   6. Handy Recovery
   7. Quick Recovery
   8. Stellar Phoenix Windows Data Recovery

9. Tools to Recover Deleted Files
   1. Total Recall
   2. Advanced Disk Recovery
   3. Windows Data Recovery Software
   4. R-Studio
   5. PC Tools File Recover
   6. Data Rescue PC
   7. Smart Undelete
   8. FileRestore Professional
   9. Deleted File Recovery Software
   10. DDR Professional Recovery Software
   11. Data Recovery Pro
   12. GetDataBack
   13. UndeletePlus
   14. Search and Recover
   15. File Scavenger
   16. FileSaver
17. Virtual Lab
18. Active@ UNDELETE
19. Win Undelete
20. R-Undelete
21. Recover4all Professional
22. eData Unerase
23. Active@ File Recovery
24. FinalRecovery

3. File Recovery Tools for MAC
   1. MAC File Recovery
   2. MAC Data Recovery
   3. Boomerang Data Recovery Software
   4. VirtualLab
   5. File Recovery Tools for MAC OS X
      1. DiskWarrior
      2. AppleXsoft File Recovery for MAC
      3. Disk Doctors MAC Data Recovery
      4. R-Studio for MAC
      5. Data Rescue
      6. Stellar Phoenix MAC Data Recovery
      7. FileSalvage
      8. TechTool Pro

4. File Recovery Tools for Linux
   1. R-Studio for Linux
   2. Quick Recovery for Linux
   3. Kernal for Linux Data Recovery
   4. TestDisk for Linux

5. Recovering the Deleted Partitions
   1. Disk Partition
   2. Deletion of Partition
   3. Recovery of the Deleted Partition

6. Partition Recovery Tools
   1. Active@ Partition Recovery for Windows
   2. Acronis Recovery Expert
   3. DiskInternals Partition Recovery
   4. NTFS Partition Data Recovery
   5. GetDataBack
   6. EASEUS Partition Recovery
   7. Advanced Disk Recovery
   8. Power Data Recovery
   9. Remo Recover (MAC) - Pro
10. MAC Data Recovery Software
11. Quick Recovery for Linux
12. Stellar Phoenix Linux Data Recovery Software
13. Tools to Recover Deleted Partitions
   1. Handy Recovery
2. TestDisk for Windows  
3. Stellar Phoenix Windows Data Recovery  
4. ARAX Disk Doctor  
5. Power Data Recovery  
6. Quick Recovery for MAC  
7. Partition Find & Mount  
8. Advance Data Recovery Software Tools  
9. TestDisk for MAC  
11. Disk Drill  
12. Stellar Phoenix MAC Data Recovery  
13. ZAR Windows Data Recovery  
15. Quick Recovery for FAT & NTFS  
16. TestDisk for Linux

Module 11: Forensics Investigation using AccessData FTK

1. Overview and Installation of FTK  
   1. Overview of Forensic Toolkit (FTK)  
   2. Features of FTK  
   3. Software Requirement  
   4. Configuration Option  
   5. Database Installation  
   6. FTK Application Installation  
2. FTK Case Manager User Interface  
   1. Case Manager Window  
      1. Case Manager Database Menu  
         1. Setting Up Additional Users and Assigning Roles  
      2. Case Manager Case Menu  
         1. Assigning Users Shared Label Visibility  
      3. Case Manager Tools Menu  
         1. Recovering Processing Jobs  
         2. Restoring an Image to a Disk  
      4. Case Manager Manage Menu  
         1. Managing Carvers  
         2. Managing Custom Identifiers  
3. FTK Examiner User Interface  
   1. FTK Examiner User Interface  
      1. Menu Bar: File Menu  
         1. Exporting Files  
         2. Exporting Case Data to a Custom Content Image  
         3. Exporting the Word List  
      2. Menu Bar: Edit Menu  
      3. Menu Bar: View Menu
4. Menu Bar: Evidence Menu
5. Menu Bar: Tools Menu
   1. Verifying Drive Image Integrity
   2. Mounting an Image to a Drive
6. File List View
   1. Using Labels
   2. Creating and Applying a Label

4. Starting with FTK
   1. Creating a case
   2. Selecting Detailed Options: Evidence Processing
   3. Selecting Detailed Options: Fuzzy Hashing
   4. Selecting Detailed Options: Data Carving
   5. Selecting Detailed Options: Custom File Identification
   7. Selecting Detailed Options: Index Refinement (Advanced)

5. FTK Interface Tabs
   1. FTK Interface Tabs
      1. Explore Tab
      2. Overview Tab
      3. Email Tab
      4. Graphics Tab
      5. Bookmarks Tab
      6. Live Search Tabs
      7. Volatile Tab

6. Adding and Processing Static, Live, and Remote Evidence
   1. Adding Evidence to a Case
   2. Evidence Groups
   3. Acquiring Local Live Evidence
   4. FTK Role Requirements For Remote Acquisition
   5. Types of Remote Information
   6. Acquiring Data Remotely Using Remote Device Management System (RDMS)
   7. Imaging Drives
   8. Mounting and Unmounting a Device

7. Using and Managing Filters
   1. Accessing Filter Tools
   2. Using Filters
   3. Customizing Filters
   4. Using Predefined Filters

8. Using Index Search and Live Search
   1. Conducting an Index Search
      1. Selecting Index Search Options
      2. Viewing Index Search Results
      3. Documenting Search Results
   2. Conducting a Live Search: Live Text Search
   3. Conducting a Live Search: Live Hex Search
   4. Conducting a Live Search: Live Pattern Search
9. Decrypting EFS and other Encrypted Files
   1. Decrypting EFS Files and Folders
   2. Decrypting MS Office Files
   3. Viewing Decrypted Files
   4. Decrypting Domain Account EFS Files from Live Evidence
   5. Decrypting Credant Files
   6. Decrypting Safeboot Files

10. Working with Reports
    1. Creating a Report
    2. Entering Case Information
    3. Managing Bookmarks in a Report
    5. Selecting a File Path List
    6. Adding a File Properties List
    7. Making Registry Selections
    8. Selecting the Report Output Options
    9. Customizing the Formatting of Reports
    10. Viewing and Distributing a Report

---

**Module 12: Forensics Investigation Using EnCase**

1. Overview of EnCase Forensic
   1. Overview of EnCase Forensic
   2. EnCase Forensic Features
   3. EnCase Forensic Platform
   4. EnCase Forensic Modules

2. Installing EnCase Forensic
   1. Minimum Requirements
   2. Installing the Examiner
   3. Installed Files
   4. Installing the EnCase Modules
   5. Configuring EnCase
      1. Configuring EnCase: Case Options Tab
      2. Configuring EnCase: Global Tab
      3. Configuring EnCase: Debug Tab
      4. Configuring EnCase: Colors Tab and Fonts Tab
      5. Configuring EnCase: EnScript Tab and Storage Paths Tab
   6. Sharing Configuration (INI) Files

3. EnCase Interface
   1. Main EnCase Window
      1. System Menu Bar
      2. Toolbar
      3. Panes Overview
         1. Tree Pane
         2. Table Pane
3. Table Pane: Table Tab
4. Table Pane: Report Tab
5. Table Pane: Gallery Tab
6. Table Pane: Timeline Tab
7. Table Pane: Disk Tab and Code Tab

4. View Pane
5. Filter Pane
   1. Filter Pane Tabs
   2. Creating a Filter
   3. Creating Conditions

6. Status Bar

4. Case Management
   1. Overview of Case Structure
   2. Case Management
   3. Indexing a Case
   4. Case Backup
   5. Options Dialog Box
   6. Logon Wizard
   7. New Case Wizard
   8. Setting Time Zones for Case Files
   9. Setting Time Zone Options for Evidence Files

5. Working with Evidence
   1. Types of Entries
   2. Adding a Device
      1. Adding a Device using Tableau Write Blocker
   3. Performing a Typical Acquisition
   4. Acquiring a Device
   5. Canceling an Acquisition
   6. Acquiring a Handsprings PDA
   7. Delayed Loading of Internet Artifacts
   8. Hashing the Subject Drive
   9. Logical Evidence File (LEF)
   10. Creating a Logical Evidence File
   11. Recovering Folders on FAT Volumes
   12. Restoring a Physical Drive

6. Source Processor
   1. Source Processor
   2. Starting to Work with Source Processor
   3. Setting Case Options
   4. Collection Jobs
      1. Creating a Collection Job
      2. Copying a Collection Job
      3. Running a Collection Job
   5. Analysis Jobs
      1. Creating an Analysis Job
      2. Running an Analysis Job
6. Creating a Report
7. Analyzing and Searching Files
   1. Viewing the File Signature Directory
   2. Performing a Signature Analysis
   3. Hash Analysis
   4. Hashing a New Case
   5. Creating a Hash Set
   6. Keyword Searches
   7. Creating Global Keywords
   8. Adding Keywords
   9. Importing and Exporting Keywords
   10. Searching Entries for Email and Internet Artifacts
   11. Viewing Search Hits
   12. Generating an Index
   13. Tag Records
8. Viewing File Content
   1. Viewing Files
   2. Copying and Unerasing Files
   3. Adding a File Viewer
   4. Viewing File Content Using View Pane
   5. Viewing Compound Files
   6. Viewing Base64 and UUE Encoded Files
9. Bookmarking Items
   1. Bookmarks Overview
   2. Creating a Highlighted Data Bookmark
   3. Creating a Note Bookmark
   4. Creating a Folder Information/Structure Bookmark
   5. Creating a Notable File Bookmark
   6. Creating a File Group Bookmark
   7. Creating a Log Record Bookmark
   8. Creating a Snapshot Bookmark
   9. Organizing Bookmarks
   10. Copying/Moving a Table Entry into a Folder
   11. Viewing a Bookmark on the Table Report Tab
   12. Excluding Bookmarks
   13. Copying Selected Items from One Folder to Another
10. Reporting
   1. Reporting
   2. Report User Interface
   3. Creating a Report Using the Report Tab
   4. Report Single/Multiple Files
   5. Viewing a Bookmark Report
   6. Viewing an Email Report
   7. Viewing a Webmail Report
   8. Viewing a Search Hits Report
   9. Creating a Quick Entry Report
Module 13: Steganography and Image File Forensics

1. Steganography
   1. What is Steganography?
   2. How Steganography Works
   3. Legal Use of Steganography
   4. Unethical Use of Steganography
2. Steganography Techniques
   1. Steganography Techniques
   2. Application of Steganography
   3. Classification of Steganography
   4. Technical Steganography
   5. Linguistic Steganography
   6. Types of Steganography
      1. Image Steganography
         1. Least Significant Bit Insertion
         2. Masking and Filtering
         3. Algorithms and Transformation
         4. Image Steganography: Hermetic Stego
         5. Steganography Tool: S-Tools
         6. Image Steganography Tools
            1. ImageHide
            2. QuickStego
            3. Gifshuffle
            4. OutGuess
            5. Contraband
            6. Camera/Shy
            7. JPHIDE and JPSEEK
            8. StegaNote
      2. Audio Steganography
         1. Audio Steganography Methods
         2. Audio Steganography: Mp3stegz
         3. Audio Steganography Tools
            1. MAXA Security Tools
            2. Stealth Files
            3. Audiostegano
            4. BitCrypt
            5. MP3Stego
            6. Steghide
            7. Hide4PGP
            8. CHAOS Universal
      3. Video Steganography
1. Video Steganography: MSU StegoVideo
2. Video Steganography Tools
   1. Masker
   2. Max File Encryption
   3. Xiao Steganography
   4. RT Steganography
   5. Our Secret
   6. BDV DataHider
   7. CHAOS Universal
   8. OmniHide PRO
3. Document Steganography: wbStego
   1. Byte Shelter I
   2. Document Steganography Tools
      1. Merge Streams
      2. Office XML
      3. CryptArkan
      4. Data Stash
      5. FoxHole
      6. Xidie Security Suite
      7. StegParty
      8. Hydan
   1. Byte Shelter I
   2. Document Steganography Tools
      1. Merge Streams
      2. Office XML
      3. CryptArkan
      4. Data Stash
      5. FoxHole
      6. Xidie Security Suite
      7. StegParty
      8. Hydan
5. Whitespace Steganography Tool: SNOW
6. Folder Steganography: Invisible Secrets 4
   1. Folder Steganography Tools
      1. StegoStick
      2. QuickCrypto
      3. Max Folder Secure
      4. WinMend Folder Hidden
      5. PSM Encryptor
      6. XPTools
      7. Universal Shield
      8. Hide My Files
7. Spam/Email Steganography: Spam Mimic
8. Issues in Information Hiding
3. Steganalysis
   1. Steganalysis
   2. How to Detect Steganography
   3. Detecting Text, Image, Audio, and Video Steganography
   4. Steganalysis Methods/Attacks on Steganography
   5. Disabling or Active Attacks
   6. Steganography Detection Tool: Stegdetect
   7. Steganography Detection Tools
      1. Xstegsecret
      2. Stego Watch
      3. StegAlyzerAS
4. StegAlyzerRTS
5. StegSpy
6. Gargoyle Investigator™ Forensic Pro
7. StegAlyzerSS
8. StegMark

4. Image Files
   1. Image Files
   2. Common Terminologies
   3. Understanding Vector Images
   4. Understanding Raster Images
   5. Metafile Graphics
   6. Understanding Image File Formats
   7. GIF (Graphics Interchange Format)
   8. JPEG (Joint Photographic Experts Group)
      1. JPEG File Structure
      2. JPEG 2000
   9. BMP (Bitmap) File
      1. BMP File Structure
   10. PNG (Portable Network Graphics)
       1. PNG File Structure
   11. TIFF (Tagged Image File Format)
       1. TIFF File Structure

5. Data Compression
   1. Understanding Data Compression
   2. How Does File Compression Work?
   3. Lossless Compression
   4. Huffman Coding Algorithm
   5. Lempel-Ziv Coding Algorithm
   6. Lossy Compression
   7. Vector Quantization

6. Locating and Recovering Image Files
   1. Best Practices for Forensic Image Analysis
   2. Forensic Image Processing Using MATLAB
   3. Locating and Recovering Image Files
   4. Analyzing Image File Headers
   5. Repairing Damaged Headers
   6. Reconstructing File Fragments
   7. Identifying Unknown File Formats
   8. Identifying Image File Fragments
   9. Identifying Copyright Issues on Graphics
   10. Picture Viewer: IrfanView
   11. Picture Viewer: ACDSee Photo Manager
   12. Picture Viewer: Thumbsplus
   13. Picture Viewer: AD Picture Viewer Lite
   14. Picture Viewer Max
   15. Picture Viewer: FastStone Image Viewer
Module 14: Application Password Crackers

1. Password Cracking Concepts
   1. Password - Terminology
   2. Password Types
   3. Password Cracker
   4. How Does a Password Cracker Work?
   5. How Hash Passwords are Stored in Windows SAM

2. Types of Password Attacks
   1. Password Cracking Techniques
   2. Types of Password Attacks
   3. Passive Online Attacks: Wire Sniffing
   4. Password Sniffing
   5. Passive Online Attack: Man-in-the-Middle and Replay Attack
   6. Active Online Attack: Password Guessing
   7. Active Online Attack: Trojan/Spyware/keylogger
   8. Active Online Attack: Hash Injection Attack
   9. Rainbow Attacks: Pre-Computed Hash
   10. Distributed Network Attack
       1. Elcomsoft Distributed Password Recovery

3. Non-Electronic Attacks
   11. Manual Password Cracking (Guessing)

4. Systems Software vs. Applications Software
   12. Automatic Password Cracking Algorithm
   13. Time Needed to Crack Passwords
5. System Software Password Cracking
   1. Bypassing BIOS Passwords
      1. Using Manufacturer’s Backdoor Password to Access the BIOS
      2. Using Password Cracking Software
         1. CmosPwd
      3. Resetting the CMOS using the Jumpers or Solder Beads
      4. Removing CMOS Battery
      5. Overloading the Keyboard Buffer and Using a Professional Service
   2. Tool to Reset Admin Password: Active@ Password Changer
   3. Tool to Reset Admin Password: Windows Key

6. Application Software Password Cracking
   1. Passware Kit Forensic
   2. Accent Keyword Extractor
   3. Distributed Network Attack
   4. Password Recovery Bundle
   5. Advanced Office Password Recovery
   6. Office Password Recovery
   7. Office Password Recovery Toolbox
   8. Office Multi-document Password Cracker
   9. Word Password Recovery Master
   10. Accent WORD Password Recovery
   11. Word Password
   12. PowerPoint Password Recovery
   13. PowerPoint Password
   14. PowerPoint Key
   15. Stellar Phoenix Powerpoint Password Recovery
   16. Excel Password Recovery Master
   17. Accent EXCEL Password Recovery
   18. Excel Password
   19. Advanced PDF Password Recovery
   20. PDF Password Cracker
   21. PDF Password Cracker Pro
   22. Atomic PDF Password Recovery
   23. PDF Password
   24. Recover PDF Password
   25. Appnimi PDF Password Recovery
   26. Advanced Archive Password Recovery
   27. KRyLack Archive Password Recovery
   28. Zip Password
   29. Atomic ZIP Password Recovery
   30. RAR Password Unlocker
   31. Default Passwords
   33. http://www.cirt.net/passwords
   34. http://default-password.info
   35. http://www.defaultpassword.us

7. Password Cracking Tools
   1. L0phtCrack
   2. OphCrack
   3. Cain & Abel
   4. RainbowCrack
   5. Windows Password Unlocker
   6. Windows Password Breaker
   7. SAMInside
   8. PWdump7 and Fgdump
   9. PCLoginNow
  10. KerbCrack
  11. Recover Keys
  12. Windows Password Cracker
  13. Proactive System Password Recovery
  14. Password Unlocker Bundle
  15. Windows Password Reset Professional
  16. Windows Password Reset Standard
  17. Krbpwguess
  18. Password Kit
  19. WinPassword
  20. Passware Kit Enterprise
  21. Rockxp
  22. PasswordsPro
  23. LSASecretsView
  24. LCP
  25. MessenPass
  26. Mail PassView
  27. Messenger Key
  28. Dialupass
  29. Protected Storage PassView
  30. Network Password Recovery
  31. Asterisk Key
  32. IE PassView

Module 15: Log Capturing and Event Correlation

1. Computer Security Logs
   1. Computer Security Logs
   2. Operating System Logs
   3. Application Logs
   4. Security Software Logs
   5. Router Log Files
   6. Honeypot Logs
7. Linux Process Accounting
8. Logon Event in Windows
9. Windows Log File
   1. Configuring Windows Logging
   2. Analyzing Windows Logs
   3. Windows Log File: System Logs
   4. Windows Log File: Application Logs
   5. Logon Events that appear in the Security Event Log
10. IIS Logs
    1. IIS Log File Format
    2. Maintaining Credible IIS Log Files
11. Log File Accuracy
12. Log Everything
13. Keeping Time
14. UTC Time
15. View the DHCP Logs
    1. Sample DHCP Audit Log File
16. ODBC Logging
2. Logs and Legal Issues
   1. Legality of Using Logs
   2. Records of Regularly Conducted Activity as Evidence
   3. Laws and Regulations
3. Log Management
   1. Log Management
      1. Functions of Log Management
      2. Challenges in Log Management
      3. Meeting the Challenges in Log Management
4. Centralized Logging and Syslogs
   1. Centralized Logging
      1. Centralized Logging Architecture
      2. Steps to Implement Central Logging
   2. Syslog
      1. Syslog in Unix-Like Systems
      2. Steps to Set Up a Syslog Server for Unix Systems
      3. Advantages of Centralized Syslog Server
   3. IIS Centralized Binary Logging
5. Time Synchronization
   1. Why Synchronize Computer Times?
   2. What is NTP?
      1. NTP Stratum Levels
   3. NIST Time Servers
   4. Configuring Time Server in Windows Server
6. Event Correlation
   1. Event Correlation
      1. Types of Event Correlation
      2. Prerequisites for Event Correlation
3. Event Correlation Approaches

7. Log Capturing and Analysis Tools
   1. GFI EventsManager
   2. Activeworx Security Center
   3. EventLog Analyzer
   4. Syslog-\textregistered\ ng OSE
   5. Kiwi Syslog Server
   6. WinSyslog
   7. Firewall Analyzer: Log Analysis Tool
   8. Activeworx Log Center
   9. EventReporter
   10. Kiwi Log Viewer
   11. Event Log Explorer
   12. WebLog Expert
   13. XpoLog Center Suite
   14. ELM Event Log Monitor
   15. EventSentry
   16. LogMeister
   17. LogViewer Pro
   18. WinAgents EventLog Translation Service
   19. EventTracker Enterprise
   20. Corner Bowl Log Manager
   22. FLAG - Forensic and Log Analysis GUI
   23. Simple Event Correlator (SEC)

---

Module 16: Network Forensics, Investigating Logs and Investigating Network Traffic

1. Network Forensics
   1. Network Forensics
   2. Network Forensics Analysis Mechanism
   3. Network Addressing Schemes
   4. Overview of Network Protocols
   5. Overview of Physical and Data-Link Layer of the OSI Model
   6. Overview of Network and Transport Layer of the OSI Model
   7. OSI Reference Model
   8. TCP/ IP Protocol
   9. Intrusion Detection Systems (IDS) and Their Placement
      1. How IDS Works
      2. Types of Intrusion Detection Systems
      3. General Indications of Intrusions
   10. Firewall
   11. Honeypot

2. Network Attacks
   1. Network Vulnerabilities
2. Types of Network Attacks
   1. IP Address Spoofing
   2. Man-in-the-Middle Attack
   3. Packet Sniffing
      1. How a Sniffer Works
   4. Enumeration
   5. Denial of Service Attack
   6. Session Sniffing
   7. Buffer Overflow
   8. Trojan Horse
3. Log Injection Attacks
   1. New Line Injection Attack
      1. New Line Injection Attack Countermeasure
   2. Separator Injection Attack
      1. Defending Separator Injection Attacks
   3. Timestamp Injection Attack
      1. Defending Timestamp Injection Attacks
   4. Word Wrap Abuse Attack
      1. Defending Word Wrap Abuse Attacks
   5. HTML Injection Attack
      1. Defending HTML Injection Attacks
   6. Terminal Injection Attack
      1. Defending Terminal Injection Attacks
4. Investigating and Analyzing Logs
   1. Postmortem and Real-Time Analysis
   2. Where to Look for Evidence
   3. Log Capturing Tool: ManageEngine EventLog Analyzer
   4. Log Capturing Tool: ManageEngine Firewall Analyzer
   5. Log Capturing Tool: GFI EventsManager
   6. Log Capturing Tool: Kiwi Syslog Server
   7. Handling Logs as Evidence
   8. Log File Authenticity
   9. Use Signatures, Encryption, and Checksums
   10. Work with Copies
   11. Ensure System’s Integrity
   12. Access Control
   13. Chain of Custody
   14. Condensing Log File
5. Investigating Network Traffic
   1. Why Investigate Network Traffic?
   2. Evidence Gathering via Sniffing
   3. Capturing Live Data Packets Using Wireshark
      1. Display Filters in Wireshark
      2. Additional Wireshark Filters
   4. Acquiring Traffic Using DNS Poisoning Techniques
      1. Intranet DNS Spoofing (Local Network)
2. Intranet DNS Spoofing (Remote Network)
3. Proxy Server DNS Poisoning
4. DNS Cache Poisoning
5. Evidence Gathering from ARP Table
6. Evidence Gathering at the Data-Link Layer: DHCP Database
7. Gathering Evidence by IDS

6. Traffic Capturing and Analysis Tools
   1. NetworkMiner
   2. Tcpdump/Windump
   3. Intrusion Detection Tool: Snort
      1. How Snort Works
   4. IDS Policy Manager
   5. MaaTec Network Analyzer
   6. Iris Network Traffic Analyzer
   7. NetWitness Investigator
   8. Colasoft Capsa Network Analyzer
   9. Sniff - O - Matic
   10. NetResident
   11. Network Probe
   12. NetFlow Analyzer
   13. OmniPeek Network Analyzer
   14. Firewall Evasion Tool: Traffic IQ Professional
   15. NetworkView
   16. CommView
   17. Observer
   18. SoftPerfect Network Protocol Analyzer
   19. EffeTech HTTP Sniffer
   20. Big-Mother
   21. EtherDetect Packet Sniffer
   22. Ntop
   23. EtherApe
   24. AnalogX Packetmon
   25. IEInspector HTTP Analyzer
   26. SmartSniff
   27. Distinct Network Monitor
   28. Give Me Too
   29. EtherSnoop
   30. Show Traffic
   31. Argus

7. Documenting the Evidence Gathered on a Network

Module 17: Investigating Wireless Attacks

1. Wireless Technologies
   1. Wireless Networks
2. Wireless Terminologies
3. Wireless Components
4. Types of Wireless Networks
5. Wireless Standards
6. MAC Filtering
7. Service Set Identifier (SSID)
8. Types of Wireless Encryption: WEP
9. Types of Wireless Encryption: WPA
10. Types of Wireless Encryption: WPA2
11. WEP vs. WPA vs. WPA2

2. Wireless Attacks
   1. Wi-Fi Chalking
      1. Wi-Fi Chalking Symbols
   2. Access Control Attacks
   3. Integrity Attacks
   4. Confidentiality Attacks
   5. Availability Attacks
   6. Authentication Attacks

3. Investigating Wireless Attacks
   1. Key Points to Remember
   2. Steps for Investigation
      1. Obtain a Search Warrant
      2. Identify Wireless Devices at Crime Scene
         1. Search for Additional Devices
         2. Detect Rogue Access Point
      3. Document the Scene and Maintain a Chain of Custody
      4. Detect the Wireless Connections
         1. Methodologies to Detect Wireless Connections
         2. Wi-Fi Discovery Tool: inSSIDer
         3. GPS Mapping
            1. GPS Mapping Tool: WIGLE
            2. GPS Mapping Tool: Skyhook
         4. How to Discover Wi-Fi Networks Using Wardriving
      5. Check for MAC Filtering
      6. Changing the MAC Address
      7. Detect WAPs using the Nessus Vulnerability Scanner
      8. Capturing Wireless Traffic
         1. Sniffing Tool: Wireshark
         2. Follow TCP Stream in Wireshark
         3. Display Filters in Wireshark
         4. Additional Wireshark Filters
      5. Determine Wireless Field Strength
         1. Determine Wireless Field Strength: FSM
         2. Determine Wireless Field Strength: ZAP Checker Products
         3. What is Spectrum Analysis?
      6. Map Wireless Zones & Hotspots
7. Connect to Wireless Network
   1. Connect to the Wireless Access Point
   2. Access Point Data Acquisition and Analysis: Attached Devices
   3. Access Point Data Acquisition and Analysis: LAN TCP/IP Setup
   4. Access Point Data Acquisition and Analysis
      1. Firewall Analyzer
      2. Firewall Log Analyzer
8. Wireless Devices Data Acquisition and Analysis
9. Report Generation

4. Features of a Good Wireless Forensics Tool
5. Wireless Forensics Tools
   1. Wi-Fi Discovery Tools
      1. NetStumbler
      2. NetSurveyor
      3. Vistumbler
      4. WirelessMon
      5. Kismet
      6. AirPort Signal
      7. WiFi Hopper
      8. Wavestumbler
      9. iStumbler
     10. WiFinder
     11. Meraki WiFi Stumbler
     12. Wellenreiter
     13. AirCheck Wi-Fi Tester
     14. AirRadar 2
   2. Wi-Fi Packet Sniffers
      1. OmniPeek
      2. CommView for Wi-Fi
      3. Wi-Fi USB Dongle: AirPcap
      4. tcpdump
      5. KisMAC
   3. Acquiring Traffic Using DNS Poisoning Techniques
      1. Intranet DNS Spoofing (Local Network)
      2. Intranet DNS Spoofing (Remote Network)
      3. Proxy Server DNS Poisoning
      4. DNS Cache Poisoning
   4. Evidence Gathering from ARP Table
   5. Evidence Gathering at the Data-ink Layer: DHCP Database
   6. Gathering Evidence by IDS

6. Traffic Capturing and Analysis Tools
   1. NetworkMiner
   2. Tcpdump/Windump
   3. Intrusion Detection Tool: Snort
      1. How Snort Works
   4. IDS Policy Manager
5. MaaTec Network Analyzer
6. Iris Network Traffic Analyzer
7. NetWitness Investigator
8. Colasoft Capsa Network Analyzer
9. Sniff - O - Matic
10. NetResident
11. Network Probe
12. NetFlow Analyzer
13. OmniPeek Network Analyzer
14. Firewall Evasion Tool: Traffic IQ Professional
15. NetworkView
16. CommView
17. Observer
18. SoftPerfect Network Protocol Analyzer
19. EffeTech HTTP Sniffer o Big-Mother o EtherDetect Packet Sniffer
   1. Cascade Pilot Personal Edition
   2. OptiView® XG Network Analysis Tablet
   3. Network Packet Analyzer
   4. Network Observer
   5. Ufasoft Snif
   6. CommView for WiFi
   7. Network Assistant
20. Wi-Fi Raw Packet Capturing Tools
   1. WirelessNetView
   2. Pirni Sniffer
   3. Tcpdump
   4. Airview
21. Wi-Fi Spectrum Analyzing Tools
   1. Cisco Spectrum Expert
   2. AirMedic
   3. BumbleBee
   4. Wi-Spy

Module 18: Investigating Web Attacks

1. Introduction to Web Applications and WebServers
   1. Introduction to Web Applications
   2. Web Application Components
   3. How Web Applications Work
   4. Web Application Architecture
   5. Open Source Webserver Architecture
   6. Indications of a Web Attack
   7. Web Attack Vectors
   8. Why Web Servers are Compromised
   9. Impact of Webserver Attacks
10. Website Defacement
11. Case Study

2. Web Logs
   1. Overview of Web Logs
   2. Application Logs
   3. Internet Information Services (IIS) Logs
      1. IIS Webserver Architecture
      2. IIS Log File Format
   4. Apache Webserver Logs
   5. DHCP Server Logs

3. Web Attacks
   1. Web Attacks - 1
   2. Web Attacks - 2
      1. Unvalidated Input
      2. Parameter/Form Tampering
      3. Directory Traversal
      4. Security Misconfiguration
      5. Injection Flaws
      6. SQL Injection Attacks
      7. Command Injection Attacks
         1. Command Injection Example
      8. File Injection Attack
   9. What is LDAP Injection?
      1. How LDAP Injection Works
   10. Hidden Field Manipulation Attack
   11. Cross-Site Scripting (XSS) Attacks
      1. How XSS Attacks Work
   12. Cross-Site Request Forgery (CSRF) Attack
      1. How CSRF Attacks Work
   13. Web Application Denial-of-Service (DoS) Attack
      1. Denial of Service (DoS) Examples
   14. Buffer Overflow Attacks
   15. Cookie/Session Poisoning
      1. How Cookie Poisoning Works
   16. Session Fixation Attack
   17. Insufficient Transport Layer Protection
   18. Improper Error Handling
   19. Insecure Cryptographic Storage
   20. Broken Authentication and Session Management
   21. Unvalidated Redirects and Forwards
   22. DMZ Protocol Attack/ Zero Day Attack
   23. Log Tampering
   24. URL Interpretation and Impersonation Attack
   25. Web Services Attack
   26. Web Services Footprinting Attack
   27. Web Services XML Poisoning
28. Webserver Misconfiguration
29. HTTP Response Splitting Attack
30. Web Cache Poisoning Attack
31. HTTP Response Hijacking
32. SSH Bruteforce Attack
33. Man-in-the-Middle Attack
34. Defacement Using DNS Compromise

4. Web Attack Investigation
   1. Investigating Web Attacks
   2. Investigating Web Attacks in Windows-Based Servers
   3. Investigating IIS Logs
   4. Investigating Apache Logs
   5. Example of FTP Compromise
   6. Investigating FTP Servers
   7. Investigating Static and Dynamic IP Addresses
   8. Sample DHCP Audit Log File
   9. Investigating Cross-Site Scripting (XSS)
   10. Investigating SQL Injection Attacks
   11. Pen-Testing CSRF Validation Fields
   12. Investigating Code Injection Attack
   13. Investigating Cookie Poisoning Attack
   14. Detecting Buffer Overflow
   15. Investigating Authentication Hijacking
   16. Web Page Defacement
   17. Investigating DNS Poisoning
   18. Intrusion Detection
   19. Security Strategies to Web Applications
   20. Checklist for Web Security

5. Web Attack Detection Tools
   1. Web Application Security Tools
      1. Acunetix Web Vulnerability Scanner
      2. Falcove Web Vulnerability Scanner
      3. Netsparker
      4. N-Stalker Web Application Security Scanner
      5. Sandcat
      6. Wikto
      7. WebWatchBot
      8. OWASP ZAP
      9. SecuBat Vulnerability Scanner
     10. Websecureify
     11. HackAlert
     12. WebCruiser
   2. Web Application Firewalls
      1. dotDefender
      2. IBM AppScan
      3. ServerDefender VP
3. Web Log Viewers
   1. Deep Log Analyzer
   2. WebLog Expert
   3. AlterWind Log Analyzer
   4. Webalizer
   5. eWebLog Analyzer
   6. Apache Logs Viewer (ALV)
4. Web Attack Investigation Tools
   1. AWStats
   2. Paros Proxy
   3. Scrawlr
6. Tools for Locating IP Address
   1. Whois Lookup
   2. SmartWhois
   3. ActiveWhois
   4. LanWhois
   5. CountryWhois
   6. CallerIP
   7. Hide Real IP
   8. IP - Address Manager
   9. Pandora FMS

Module 19: Tracking Emails and Investigating Email Crimes

1. Email System Basics
   1. Email Terminology
   2. Email System
   3. Email Clients
   4. Email Server
   5. SMTP Server
   6. POP3 and IMAP Servers
   7. Email Message
   8. Importance of Electronic Records Management
2. Email Crimes
   1. Email Crime
   2. Email Spamming
   3. Mail Bombing/Mail Storm
   4. Phishing
   5. Email Spoofing
   6. Crime via Chat Room
   7. Identity Fraud/Chain Letter
3. Email Headers
   1. Examples of Email Headers
   2. List of Common Headers
4. Steps to Investigate
1. Why to Investigate Emails
2. Investigating Email Crime and Violation
   1. Obtain a Search Warrant and Seize the Computer and Email Account
   2. Obtain a Bit-by-Bit Image of Email Information
   3. Examine Email Headers
      1. Viewing Email Headers in Microsoft Outlook
      2. Viewing Email Headers in AOL
      3. Viewing Email Headers in Hotmail
      4. Viewing Email Headers in Gmail
      5. Viewing Headers in Yahoo Mail
      6. Forging Headers
   4. Analyzing Email Headers
      1. Email Header Fields
      2. Received: Headers
      3. Microsoft Outlook Mail
      4. Examining Additional Files (.pst or .ost files)
      5. Checking the Email Validity
      6. Examine the Originating IP Address
   5. Trace Email Origin
      1. Tracing Back
      2. Tracing Back Web-based Email
   6. Acquire Email Archives
      1. Email Archives
      2. Content of Email Archives
      3. Local Archive
      4. Server Storage Archive
      5. Forensic Acquisition of Email Archive
   7. Recover Deleted Emails
      1. Deleted Email Recovery
5. Email Forensics Tools
   1. Stellar Phoenix Deleted Email Recovery
   2. Recover My Email
   3. Outlook Express Recovery
   4. Zmeil
   5. Quick Recovery for MS Outlook
   6. Email Detective
   7. Email Trace - Email Tracking
   8. R-Mail
   9. FINALeMAIL
   10. eMailTrackerPro
   11. Forensic Tool Kit (FTK)
   12. Paraben’s email Examiner
   13. Network Email Examiner by Paraben
   14. DiskInternal’s Outlook Express Repair
   15. Abuse.Net
   16. MailDetective Tool
6. Laws and Acts against Email Crimes
   1. U.S. Laws Against Email Crime: CAN-SPAM Act
   2. 18 U.S.C. § 2252A
   3. 18 U.S.C. § 2252B
   4. Email Crime Law in Washington: RCW 19.190.020

Module 20: Mobile Forensics

1. Mobile Phone
   1. Mobile Phone
   2. Different Mobile Devices
   3. Hardware Characteristics of Mobile Devices
   4. Software Characteristics of Mobile Devices
   5. Components of Cellular Network
   6. Cellular Network
   7. Different Cellular Networks

2. Mobile Operating Systems
   1. Mobile Operating Systems
   2. Types of Mobile Operating Systems
   3. WebOS
      1. WebOS System Architecture
   4. Symbian OS
      1. Symbian OS Architecture
   5. Android OS
      1. Android OS Architecture
   6. RIM BlackBerry OS
   7. Windows Phone 7
      1. Windows Phone 7 Architecture
   8. Apple iOS

3. Mobile Forensics
   1. What a Criminal can do with Mobiles Phones?
   2. Mobile Forensics
   3. Mobile Forensics Challenges
   4. Forensics Information in Mobile Phones
   5. Memory Considerations in Mobiles
   6. Subscriber Identity Module (SIM)
   7. SIM File System
   8. Integrated Circuit Card Identification (ICCID)
   9. International Mobile Equipment Identifier (IMEI)
   10. Electronic Serial Number (ESN)
   11. Precautions to be Taken Before Investigation

4. Mobile Forensic Process
   1. Mobile Forensic Process
      1. Collect the Evidence
         1. Collecting the Evidence
2. Points to Remember while Collecting the Evidence
3. Collecting iPod/iPhone Connected with Computer

2. Document the Scene and Preserve the Evidence
3. Imaging and Profiling
4. Acquire the Information
   1. Device Identification
   2. Acquire Data from SIM Cards
   3. Acquire Data from Unobstructed Mobile Devices
   4. Acquire the Data from Obstructed Mobile Devices
   5. Acquire Data from Memory Cards
   6. Acquire Data from Synched Devices
   7. Gather Data from Network Operator
   8. Check Call Data Records (CDRs)
   9. Gather Data from SQLite Record
   10. Analyze the Information

5. Generate Report

5. Mobile Forensics Software Tools
   1. Oxygen Forensic Suite 2011
   2. MOBILedit! Forensic
   3. BitPim
   4. SIM Analyzer
   5. SIMCon
   6. SIM Card Data Recovery
   7. Memory Card Data Recovery
   8. Device Seizure
   9. SIM Card Seizure
   10. ART (Automatic Reporting Tool)
   11. iPod Data Recovery Software
   12. Recover My iPod
   13. PhoneView
   14. Elcomsoft Blackberry Backup Explorer
   15. Oxygen Phone Manager II
   16. Sanmaxi SIM Recoverer
   17. USIMdetective
   18. CardRecovery
   19. Stellar Phoenix iPod Recovery Software
   20. iCare Data Recovery Software
   21. Cell Phone Analyzer
   22. iXAM
   23. BlackBerry Database Viewer Plus
   24. BlackBerry Signing Authority Tool

6. Mobile Forensics Hardware Tools
   1. Secure View Kit
   2. Deployable Device Seizure (DDS)
   3. Paraben's Mobile Field Kit
   4. PhoneBase
Module 21: Investigative Reports

1. Computer Forensics Report
   1. Computer Forensics Report
   2. Salient Features of a Good Report
   3. Aspects of a Good Report

2. Computer Forensics Report Template
   1. Computer Forensics Report Template
   2. Simple Format of the Chain of Custody Document
   3. Chain of Custody Forms
   4. Evidence Collection Form
   5. Computer Evidence Worksheet
   6. Hard Drive Evidence Worksheet
   7. Removable Media Worksheet

3. Investigative Report Writing
   1. Report Classification
   2. Layout of an Investigative Report
      1. Layout of an Investigative Report: Numbering
   3. Report Specifications
   4. Guidelines for Writing a Report
   5. Use of Supporting Material
   6. Importance of Consistency
   7. Investigative Report Format
   8. Attachments and Appendices
   9. Include Metadata

10. Signature Analysis
11. Investigation Procedures
12. Collecting Physical and Demonstrative Evidence
13. Collecting Testimonial Evidence
14. Do’s and Don'ts of Forensics Computer Investigations
15. Case Report Writing and Documentation
16. Create a Report to Attach to the Media Analysis Worksheet
17. Best Practices for Investigators

4. Sample Forensics Report
   1. Sample Forensics Report
Module 22: Becoming an Expert Witness

1. Expert Witness
   1. What is an Expert Witness?
   2. Role of an Expert Witness
   3. What Makes a Good Expert Witness?
2. Types of Expert Witnesses
   1. Types of Expert Witnesses
   2. Computer Forensics Experts
      1. Role of Computer Forensics Expert
   3. Medical & Psychological Experts
   4. Civil Litigation Experts
   5. Construction & Architecture Experts
   6. Criminal Litigation Experts
3. Scope of Expert Witness Testimony
   1. Scope of Expert Witness Testimony
   2. Technical Witness vs. Expert Witness
   3. Preparing for Testimony
4. Evidence Processing
   1. Evidence Preparation and Documentation
   2. Evidence ProcessingSteps
   3. Checklists for Processing Evidence
   4. Examining Computer Evidence
   5. Prepare the Report
   6. Evidence Presentation
5. Rules for Expert Witness
   1. Rules Pertaining to an Expert Witness’s Qualification
   2. Daubert Standard
   3. Frye Standard
   4. Importance of Resume
   5. Testifying in the Court
   6. The Order of Trial Proceedings
6. General Ethics While Testifying
   1. General Ethics While Testifying
   2. Importance of Graphics in a Testimony
   3. Helping your Attorney
   4. Avoiding Testimony Issues
   5. Testifying during Direct Examination
   6. Testifying during Cross-Examination
   7. Deposition
   8. Recognizing Deposition Problems
9. Guidelines to Testify at a Deposition
10. Dealing with Media
11. Finding a Computer Forensic Expert