

# **EC-Council Computer Hacking Forensic Investigator Version 4**

- **Course Number:** CHFIv4
- **Course Length:** 5 Days

## **Course Overview**

This instructor-led course will give students the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute the associated crimes. Many of today's top tools of the information forensic trade will be taught during this course including software, hardware, and highly specialized techniques.

## **Prerequisites**

It is strongly recommended that students attend the CEH class before enrolling in this program.

## **Audience**

This course is of significant benefit to Police and other Law Enforcement Personnel, Defense and Military personnel, anyone working in Government Agencies, e-Business Security Professionals, Systems Administrators, Legal Professionals, Banking, Insurance and other professionals, and IT managers.

## **Certification Exam**

This course prepares students for the EC-Council Computer Hacking Forensic Investigator exam CHFI 312-49.

# Course Outline

## **Course Introduction**

6m

Course Introduction

## **Module 01 - Computer Forensics in Today's World**

42m

Computer Forensics in Today's World

Scenario

Demo - Introduction to IAAC Website

Forensic Science

Computer Forensics

Security Incident Report

Demo - Security Research Studies

Aspects of Organizational Security

Evolution of Computer Forensics

Objectives of Computer Forensics

Need for Computer Forensics

Benefits of Forensic Readiness

Goals of Forensic Readiness

Forensic Readiness Planning

Cyber Crime

Computer Facilitated Crimes

Modes of Attack

Examples of Cyber Crime

Types of Computer Crimes

How Serious Were Different Types of Incidents

Time Spent Responding to the Security Incident

Cyber Crime Investigation

Key Steps in Forensic Investigation

Demo - Crime Scene Processing

Rules of Forensic Investigation

Need for Forensic Investigation

Role of Forensics Investigation

Accessing Computer Forensic Resources

Role of Digital Evidence

Understanding Corporate Investigations

Approach to Forensic Investigation: A Case Study

When an Advocate Contacts the Forensic Investigator, He Specifies How to Approach the Crime Scene

Where and When Do You Use Computer Forensics

Enterprise Theory of Investigation (ETI)

Demo - FBI ETI Model

Legal Issues

Reporting the Results

Module 01 - Review

## **Module 02 - Computer Forensics Investigation Process**

1hr 20m

Computer Forensics Investigation Process

Investigating Computer Crime

Before the Investigation

Build a Forensics Workstation  
Building Investigation Team  
People Involved in Computer Forensics  
Review Policies and Laws  
Demo - CyberCrime.gov Website Review  
Demo - Extra Cyber Crime Resources  
Forensics Laws  
Notify Decision Makers and Acquire Authorization  
Demo - Legal Resources  
Risk Assessment  
Build a Computer Investigation Toolkit  
Demo - Forensics Toolkit of Documentation  
Computer Forensics Investigation Methodology  
Demo - DOJ Forensics Flow Chart  
Steps to Prepare for a Computer Forensic Investigation  
Obtain a Search Warrant  
Searches Without a Warrant  
Evaluate and Secure the Scene  
Forensic Photography  
Gather the Preliminary Information at Scene  
First Responder  
Demo - First Responder Guides  
Collect the Evidence  
Collect Physical Evidence  
Evidence Collection Form  
Collect Electronic Evidence  
Guidelines in Acquiring Evidence  
Secure the Evidence  
Evidence Management  
Chain of Custody  
Chain of Custody Form  
Demo - Chain of Custody  
Original Evidence  
Duplicate the Data (Imaging)  
Verify Image Integrity  
Recover Lost or Deleted Data  
Analyze the Data  
Data Analysis  
Data Analysis Tools  
Assess Evidence and Case  
Evidence Assessment  
Case Assessment  
Processing Location Assessment  
Best Practices  
Prepare the Final Report  
Documentation in Each Phase  
Gather and Organize Information  
Writing the Investigation Report  
Demo - Forensics Report Example  
Testify in Court as an Expert Witness

Demo - Extra Reading "A Hypothesis-Based Approach to Digital Forensic Investigations"  
Expert Witness  
Testifying in the Court Room  
Closing the Case  
Maintaining Professional Conduct  
Investigating a Company Policy Violation  
Computer Forensics Service Providers  
Module 02 - Review

## **Module 03 - Searching and Seizing Computers**

52m

Searching and Seizing Computers

News Overview

Searching and Seizing Computers without a Warrant

Demo - DOJ Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

A: Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers: General Principles

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

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

A.4: Private Searches

A.5 Use of Technology to Obtain Information

B: Exceptions to the Warrant Requirement in Cases Involving Computers

B.1: Consent

B.1.a: Scope of Consent

B.1.b: Third-Party Consent

B.1.c: Implied Consent

B.3: Plain View

B.5: Inventory Searches

B.6: Border Searches

B.7: International Issues

C: Special Case: Workplace Searches

C.2: Public-Sector Workplace Searches

Searching and Seizing Computers with a Warrant

Successful Search With A Warrant

A.1: Basic Strategies for Executing Computer Searches

A.1.a: When Hardware Is Itself Contraband, Evidence, or an Instrumentality or Fruit of Crime

A.1.b: When Hardware is Merely a Storage Device for Evidence of Crime

A.2: The Privacy Protection Act

A.2.a: The Terms of the Privacy Protection Act

A.3: Civil Liability Under the Electronic Communications Privacy Act (ECPA)

A.7: Privileged Documents

B: Drafting the Warrant and Affidavit

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

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

B.2: Establish Probable Cause in the Affidavit

B.3: In the Affidavit Supporting the Warrant, Include an Explanation of the Search Strategy

C: Post-Seizure Issues

C.1: Searching Computers Already in Law Enforcement Custody

C.2: The Permissible Time Period For Examining Seized Computers

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

Demo - Legal Extra Reading

The Electronic Communications Privacy Act

B. Classifying Types of Information Held by Service Providers

E. Working with Network Providers

Electronic Surveillance in Communications Networks

A. Content vs. Addressing Information

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

EVIDENCE

A. Authentication

B. Hearsay

C. Other Issues

Module 03 - Review

## **Module 04 - Digital Evidence**

2hr 11m

Digital Evidence

Definition of Digital Evidence

Increasing Awareness of Digital Evidence

Challenging Aspects of Digital Evidence

The Role of Digital Evidence

Characteristics of Digital Evidence

Fragility of Digital Evidence

Types of Digital Data

Demo - Binary and Hex Basics

Rules of Evidence

Best Evidence Rule

Demo - Best Evidence

Federal Rules of Evidence

International Organization on Computer Evidence (IOCE)

IOCE International Principles for Digital Evidence

Scientific Working Group on Digital Evidence (SWGDE)

SWGDE Standards for the Exchange of Digital Evidence

Electronic Devices: Types and Collecting Potential Evidence

Evidence Assessment

Prepare for Evidence Acquisition

Preparation for Searches

Seizing the Evidence

Imaging

Bit-Stream Copies

Demo - Extra Bit-Stream Example Cases

Write Protection

Demo - Hardware Write Blocker Example

Evidence Acquisition

Evidence Acquisition from Crime Location

Acquiring Evidence from Storage Devices

Collecting the Evidence

Collecting Evidence from RAM

Demo - Freezing RAM to Extract Encryption Keys

Collecting Evidence from Stand-alone Network Computer

Chain of Custody

Preserving Digital Evidence: Checklist

Preserving Floppy and Other Removable Media

Handling Digital Evidence

Store and Archive  
Digital Evidence Findings  
Evidence Examination and Analysis  
Evidence Examination  
Physical Extraction  
Logical Extraction  
Analyze Host Data  
Analyze Storage Media  
Analyze Network Data  
Analysis of Extracted Data  
Timeframe Analysis  
Data Hiding Analysis  
Application and File Analysis  
Ownership and Possession  
Documenting the Evidence  
Evidence Examiner Report  
Final Report of Findings  
Demo - Evidence Worksheet  
Electronic Crime and Digital Evidence Consideration by Crime Category  
Module 04 - Review

## **Module 05 - First Responder Procedures**

49m

First Responder Procedures  
Electronic Evidence  
First Responder Overview  
Great PDF Guide  
Demo - First Responders Guide  
Demo - PDA and Mobile Take Note  
Roles of First Responder  
First Responder Toolkit  
Creating a First Responder Toolkit  
Evidence Collecting Tools and Equipment  
First Response Rule  
Incident Response: Different Situations  
First Response for System Administrators  
First Response by Non-Laboratory Staff  
First Response by Laboratory Forensic Staff  
Securing and Evaluating Electronic Crime Scene: A Check-list  
Planning the Search and Seizure  
Initial Search of the Scene  
Health and Safety Issues  
Consent  
Witness Signatures  
Conducting Preliminary Interviews  
Conducting Initial Interviews  
Documenting Electronic Incident Scene  
Collecting and Preserving Electronic Evidence  
Order of Volatility  
Dealing with Powered OFF Computers at Seizure Time  
Dealing with Powered ON Computers

Demo - Power State and Review  
Dealing with Networked Computer  
Operating System Shutdown Procedure  
Seizing Portable Computers  
Switched ON Portables  
Evidence Bag Contents List  
Packaging Electronic Evidence  
Exhibit Numbering  
Transporting Electronic Evidence  
Handling and Transportation to the Forensics Laboratory  
Chain of Custody  
Demo - Documentation  
Module 05 - Review

## **Module 06 - Incident Handling**

1hr 20m

Incident Handling  
What is an Incident  
Security Incidents  
Category of Incidents  
Category of Incidents: Low Level  
Category of Incidents: Mid Level  
Category of Incidents: High Level  
Issues in Present Security Scenario  
How to Identify an Incident  
How to Prevent an Incident  
Defining the Relationship between Incident Response, Incident Handling, and Incident Management  
Incident Management  
Threat Analysis and Assessment  
Vulnerability Analysis  
Estimating Cost of an Incident  
Change Control  
Incident Reporting  
Demo - Incident Handling Report Form  
Whom to Report an Incident  
Report a Privacy or Security Violation  
Demo - Preliminary Info Sec Incident Reporting  
Why Don't Organizations Report Computer Crimes  
Responding to a Security Incident  
Demo - Incident Response Documentation  
Incident Response Policy  
Roles and Responsibilities of SSM, ISSM, and ISSO  
Contingency/Continuity of Operations Planning  
Handling Incidents  
Procedure for Handling Incident  
1. Preparation  
2. Identification  
3. Containment  
4. Eradication  
5. Recovery  
6. Follow-up

Post-Incident Activity  
Education, Training, and Awareness  
Demo - User Awareness Training  
Procedural and Technical Countermeasures  
Vulnerability Resources  
What is CSIRT  
CSIRT: Goals and Strategy  
Motivation Behind CSIRTs  
Global Incident Response Teams  
Staffing your Computer Security Incident Response Team: What are the Basic Skills Needed  
Team Models  
Delegation of Authority  
CSIRT Services Can Be Grouped into Three Categories  
CSIRT Case Classification  
Types of Incidents and Level of Support  
Service Description Attributes  
Incident Specific Procedures-I (Virus and Worm Incidents)  
Incident Specific Procedures-II (Hacker Incidents)  
Incident Specific Procedures-III (Social Incidents, Physical Incidents)  
How CSIRT Handles Case: Steps  
Best Practices for Creating a CSIRT  
Limits to Effectiveness in CSIRTs  
Module 06 - Review

## **Module 07 - Computer Forensics Lab**

2hr 9m

Computer Forensics Lab  
Demo - Modules Resources  
Planning for a Forensics Lab  
Budget Allocation for a Forensics Lab  
Physical Location Needs of a Forensic Lab  
Structural Design Considerations  
Environmental Conditions  
Electrical Needs  
Communication Needs  
Work Area of a Computer Forensic Lab  
Ambience of a Forensic Lab  
Ambience of a Forensic Lab: Ergonomics  
Physical Security Recommendations  
Fire-Suppression Systems  
Demo - FSSA Website  
Evidence Locker Recommendations  
Demo - Storage Lockers  
Computer Forensic Investigator  
Demo - Forensics Certification Exams and Bodies  
Forensic Lab Licensing Requisite  
Demo - Forensics Legal Requirements Resource  
Features of the Laboratory Imaging System  
Demo - Eraser  
Technical Specification of the Laboratory-based Imaging System  
Forensics Lab

Auditing a Computer Forensic Lab  
Recommendations to Avoid Eyestrain  
Computer Forensic Labs, Inc.  
Data Destruction Industry Standards  
Demo - Data Destruction with Eraser Free Tool  
Demo - DBan Secure Erase  
Example Hardware Essential in a Forensics Lab  
Forensic Workstations  
Basic Workstation Requirements in a Forensic Lab  
Stocking the Hardware Peripherals  
Demo - Paraben Forensics Webstore Products  
Demo - Image Master Product Line Store  
Demo - Logicube.com Website  
Requirements for a Forensics Lab  
Basic Software Requirements in a Forensic Lab  
Maintain Operating System and Application Inventories  
Demo - A Forensics Software Requirements Intro  
Demo - CAINE Computer Aided Investigative Environment Live CD  
Demo - Opening a WinXP VirtualMachine Using Vmware Workstation  
Demo - 7 Zip Compression  
Demo - Unzipping a file with either Zip Genius or 7 Zip  
Demo - Nlite Custom Windows Install Deploy  
Demo - BackTrack 101  
Demo - Live Forensics  
Module 07 – Review

## **Module 08 - Understanding Hard Disks and File Systems**

3hr 6m

Understanding Hard Disks and File Systems  
Disk Drive Overview - I  
Disk Drive Overview - II  
Physical Structure of Hard Disk  
Logical Structure of Hard Disk  
Types of Hard Disk Interfaces  
Types of Hard Disk Interfaces: SCSI  
Types of Hard Disk Interfaces: IDE/EIDE  
FireWire vs. USB  
Types of Hard Disk Interfaces: ATA  
Types of Hard Disk Interfaces: Fibre Channel  
Disk Platter  
Tracks  
Track Numbering  
Sector  
Sector Addressing  
Cluster  
Cluster Size  
Slack Space  
Lost Clusters  
Bad Sector  
Disk Capacity Calculation  
Measuring the Performance of Hard Disk

Disk Partitions  
Master Boot Record  
Windows XP System Files  
Windows Boot Process (XP/2003)  
Demo - Boot Process  
Bootdisk.com  
File Systems  
Understanding File Systems  
Types of File Systems  
List of Disk File Systems  
List of Network File Systems  
List of Special Purpose File Systems  
Popular Linux File Systems  
Sun Solaris 10 File System: ZFS  
Mac OS X File System  
Windows File Systems  
CD-ROM / DVD File System  
Comparison of File Systems  
FAT32  
FAT  
FAT Structure  
FAT32 cont.  
NTFS  
NTFS Architecture  
NTFS System Files  
NTFS Partition Boot Sector  
NTFS Master File Table (MFT)  
NTFS Metadata File Table (MFT)  
Cluster Sizes of NTFS Volume  
NTFS Files and Data Storage  
NTFS Attributes-I  
NTFS Attributes-II  
NTFS Data Stream-I  
NTFS Data Stream-II  
Demo - Alternate Data Streams  
Demo - LADS  
NTFS Compressed Files  
NTFS Encrypted File Systems (EFS)  
EFS File Structure  
EFS Recovery Key Agent-I  
EFS Recovery Key Agent -II  
EFS Key  
Deleting NTFS Files  
Registry Data-I  
Registry Data-II  
Registry Data-III  
Examining Registry Data  
FAT vs. NTFS  
Demo - FAT vs NTFS  
Ext2

Ext3  
HFS  
CDFS  
RAID Storage System  
RAID Levels  
Demo - RAID  
Recover Data from Unallocated Space Using File Carving Process  
Evidor  
WinHex  
Logicube Tools  
Logicube: CloneCard Pro  
ImageMASSTER: ImageMASSTER 4008i  
eDR Solutions: Hard Disk Crusher  
Demo - Mac Match  
Module 08 - Review

## **Module 09 - Digital Media Devices**

35m

Digital Media Devices  
Magnetic Tape  
Floppy Disk  
Compact Disk  
CD-ROM  
DVD  
DVD-R, DVD+R, and DVD+R(W)  
DVD-RW, DVD+RW  
DVD Differences  
DVD+R DL/ DVD-R DL/ DVD-RAM  
Blu-Ray  
Network Attached Storage (NAS)  
iPod  
Zune  
Flash Memory Cards  
Secure Digital (SD) Memory Card  
Secure Digital High Capacity (SDHC) Card  
Secure Digital Input Output (SDIO) Card  
Secure Digital Input Output (SDIO)  
Compact Flash (CF) Memory Card  
Memory Stick (MS) Memory Card  
Multi Media Memory Card (MMC)  
xD-Picture Card (xD)  
SmartMedia Memory (SM) Card  
Solid-State Drive (SSD)  
Tape Libraries and Autoloaders  
WD VelociRaptor  
Hybrid Hard Drive  
Holographic Data Storage  
ExpressCard  
USB Flash Drives  
Demo - USB Deview  
NOR / NAND Flash

E-ball Futuristic Computer  
Different Models of Digital Devices  
Different Types of Pocket Hard Drives  
Different Types of Network-Attached Storage Devices  
Different Types of Digital Camera Devices  
Different Types of Digital Video Cameras  
Different Types of Mobile Devices  
Mobile Devices in the Future  
Module 09 - Review

### **Module 10 - CD/DVD Forensics**

15m

CD/DVD Forensics  
SID Code  
Pre-Requisite for CD/DVD Forensics  
Steps for CD Forensics  
Collect the CD/DVD Evidence  
Precautions while Collecting the Evidence  
Document the Scene  
Preserve the Evidence  
Create an Image of a CD/DVD  
Recover Data from Damaged or Corrupted CDs/DVDs  
Data Analysis  
Identify Pirated CD/DVDs  
Original and Pirated CD/DVDs  
CD/DVD Imaging Tools  
CD/DVD Data Recovery Tools  
CD & DVD Data Recovery Services  
Module 10 - Review

### **Module 11 - Windows Linux Macintosh Boot Process**

53m

Windows Linux Macintosh Boot Process  
Terminologies  
Boot Loader  
Boot Sector  
Anatomy of MBR  
Windows Boot Sequence  
Linux Boot Sequence  
Macintosh Boot Sequence  
Windows XP Boot Process  
Windows Vista Boot Sequence  
Vista Boot Process  
Linux Boot Process  
Common Startup Files in UNIX  
List of Important Directories in UNIX  
Linux Boot Process cont.  
Linux Boot Process Steps  
Step 1: The Boot Manager  
GRUB: Boot Loader  
Step 2: init  
Step 2.1: /etc/inittab

Runlevels  
The Run Level Scripts  
How Processes in Run Level Starts  
Run Level Actions  
Step 3: Services  
Step 4: More inittab  
Operating Modes  
Macintosh Boot Process  
Mac OS X  
Mac OS X Hidden Files  
Booting Mac OS X (Supported on Non-Intel Macs)  
Screenshot  
Mac OS X Boot Options  
The Mac OS X Boot Process  
Module 11 - Review

## **Module 12 - Windows Forensics I**

3hr 48m

Windows Forensics I  
Volatile Information  
Demo - Volatile Information  
Non-Volatile Information  
Module Overview  
System Time  
Demo - System Time  
Demo - Uptime  
Logged-On-Users  
Open Files  
Demo - Open Files  
Net File Command  
Psfile Tool  
Openfiles Command  
NetBIOS Name Table Cache  
Network Connections  
Netstat with -ano Switch: Screenshot  
Netstat with the -r Switch: Screenshot  
Demo - Networking Command Line Tools  
Process Information  
Tlist Tool  
Tasklist Command  
Tasklist with the /v Switch: Screenshot  
Pslist Tool  
Listdlls Tool  
Handle Tool  
Demo - Process Explorer  
Process-to-Port Mapping  
Netstat Command  
Fport Tool  
Openports Tool  
Network Status  
Ipconfig Command

Demo - TCP View  
Demo - IP2  
Promiscdetect Tool  
Promqry Tool  
Other Important Information  
Demo - System Information  
Collecting Nonvolatile Information  
Examining File Systems  
Registry Settings  
Microsoft Security ID  
Event Logs  
Index.dat File  
Vista Index.dat Location  
Demo - Index.dat File  
Text View of an Index.dat File  
Devices and Other Information  
Demo - PS Tools  
Demo - Agile  
DevCon Screenshot  
Slack Space  
Slack Space Information Collection  
Virtual Memory  
Tool: DriveSpy  
Swap File  
Windows Search Index  
Tool: Search Index Examiner  
Collecting Hidden Partition Information  
Hidden ADS Streams  
Windows Memory Analysis  
Importance of Memory Dump  
EProcess Structure  
Process Creation Mechanism  
Parsing Memory Contents  
Demo - Parsing Memory Contents  
Collecting Process Memory  
Windows Registry Analysis  
Registry Contents  
Demo - Windows Registry Editors Overview  
Registry Structure within a Hive File  
Registry Analysis  
System Information  
Time Zone Information  
Shares  
Audit Policy  
Demo - Win Audit  
Demo - Audit Policy  
Wireless SSIDs  
Autostart Locations  
Demo - System Config Utility  
System Boot

User Login  
User Activity  
Enumerating Autostart Registry Locations  
USB Removable Storage Devices  
Mounted Devices  
Finding Users  
Tracking User Activity  
The UserAssist Keys  
MRU Lists  
Search Assistant  
Connecting to Other Systems  
Analyzing Restore Point Registry Settings  
Demo - Using System Restore  
Determining the Startup Locations  
Demo - Finding Auto Run Using Regedt32  
Cache, Cookie and History Analysis  
Cache, Cookie and History Analysis in IE  
Demo - IE Analysis  
Cache, Cookie and History Analysis in Firefox/Netscape  
Browsing Analysis Tool: Pasco  
Tool - IE Cache View  
Forensic Tool: Cache Monitor  
IE Cookie Analysis  
Tool - IECookiesView  
Tool - IE Sniffer  
MD5 Calculation  
MD5 Algorithm  
MD5 Pseudocode  
MD5 Generator: Chaos MD5  
Demo - Hashing  
Secure Hash Signature Generator  
Windows File Analysis  
Recycle Bin  
System Restore Points  
Prefetch Files  
Shortcut Files  
Searching with Event Viewer  
Word Documents  
PDF Documents  
Image Files  
File Signature Analysis  
NTFS Alternate Data Streams  
Executable File Analysis  
Documentation Before Analysis  
Static Analysis Process  
Search Strings  
PE Header Analysis  
Import Table Analysis  
Export Table Analysis  
Dynamic Analysis Process

Creating Test Environment  
Collecting Information Using Tools  
Dynamic Analysis Steps  
Metadata Investigation  
Metadata  
Types of Metadata  
Metadata in Different File Systems  
Viewing Metadata  
Demo - ReSysInfo  
Demo - Anti-Forensics  
Module 12 - Review

## **Module 13 - Windows Forensics II**

48m

Windows Forensics II  
Understanding Events  
Event Record Structure  
Vista Event Logs  
Demo - Windows Server Event Viewer  
IIS Logs  
Parsing IIS Logs  
Parsing FTP Logs  
Parsing DHCP Server Logs  
Parsing Windows Firewall Logs  
Using the Microsoft Log Parser  
Evaluating Account Management Events  
Examining Audit Policy Change Events  
Examining System Log Entries  
Examining Application Log Entries  
Using EnCase to Examine Windows Event Log Files  
Windows Event Log Files Internals  
Window Password Issues  
Understanding Windows Password Storage  
Cracking Windows Passwords Stored on Running Systems  
Exploring Windows Authentication Mechanisms  
Sniffing and Cracking Windows Authentication Exchanges  
Cracking Offline Passwords  
Module 13 - Review

## **Module 14 - Linux Forensics**

1hr 6m

Linux Forensics  
Introduction of Linux OS  
Linux Boot Sequence  
File System Description  
Common Directories / Contents  
Linux Forensics  
Use of Linux as a Forensics Tool  
Advantages of Linux in Forensics  
Disadvantages of Linux in Forensics  
Precautions During Investigation  
Recognizing Partitions in Linux

Mount Command  
Demo - Linux Drive Mounting  
Floppy Disk Analysis  
Hard Disk Analysis  
Linux Crash Utility  
Crash Commands  
Case Examples  
Case Example I  
Step-by-Step Approach to Case  
Challenges in Disk Forensics with Linux  
Case Example II  
Step-by-Step Approach to Case  
Linux Forensics Tools  
Popular Linux Forensics Tools  
The Sleuth Kit  
Tools in “The Sleuth Kit”  
The Evidence Analysis Techniques in Autopsy  
SMART for Linux  
Features of SMART for Linux  
SMART: Screenshots 1  
SMART: Screenshots 2  
Penguin Sleuth  
The Farmer’s Boot CD  
Demo - Helix  
Forensix  
Tool: Maresware  
Module 14 - Review

## **Module 15 - Mac Forensics**

1hr

Mac Forensics  
Mac OS X  
Partitioning Schemes  
Apple Partition Map(APM)  
Apple Partition Map Entry Record  
GUID Partition Table  
Mac OS X File System  
HFS+ File System  
Mac OS X Directory Structure  
Mac Security Architecture Overview  
Screenshot: Mac Security Architecture  
Pre-requisites for Mac Forensics  
Obtaining System Date and Time  
Single User Mode  
Determining and Resetting Open Firmware Password  
Checking Plist Files  
Gathering Network Setting Information from Plist Files  
Collect User Home Directory Information  
Forensic Information in User Library Folder  
Collect User Accounts Information  
User IDs

Gathering User Information from Plist files  
Use Spotlight for Keyword Search  
Cracking File Vault  
POSIX Permissions  
Viewing POSIX Permissions  
Viewing ACL Permissions  
Mac OS X Log Files  
Locating iChat Configuration File  
Checking Instant Messaging Configuration Plist Files  
Viewing iChat Logs  
Gathering Safari Information  
Checking Wi-Fi Support  
Checking Bluetooth Support  
Gathering Information from Printer Spool (CUPS)  
Vulnerable Features of Mac  
Imaging a Target Macintosh  
Target Disk Mode  
LiveCD Method  
Drive Removal  
Acquiring the Encrypted User Home Directory  
.Mac and Related Evidence  
Quick View Plus  
Cover Flow  
Module 15 – Review

## **Module 16 - Data Acquisition and Duplication**

1hr 16m

Data Acquisition and Duplication  
Data Acquisition  
Data Acquisition Terminology  
Types of Data Acquisition Systems  
Determining the Best Acquisition Methods  
Data Recovery Contingencies  
Data Acquisition Mistakes  
Data Duplication  
Issues with Data Duplication  
Data Duplication in Mobile Multi-Database System  
Data Duplication System Used in USB Devices  
Data Backup  
Data Acquisition Tools and Commands  
MS-DOS Data Acquisition Tool: DriveSpy  
Using Windows Data Acquisition Tools  
FTK Imager  
Acquiring Data on Linux  
Demo - Using DD  
Demo - Netcat  
Demo - Mount Image Pro  
Demo - Snapshot  
Data Acquisition Toolbox  
Data Acquisition Tool: SafeBack  
Demo - Data Acquisition

Demo - Data Acquisition II  
Hardware Tool: Image MASSter Solo-3 Forensic  
Image MASSter Solo-3 Forensic  
Image MASSter: RoadMASSter -3  
Image MASSter: Wipe MASSter  
Image MASSter: DriveLock  
Logicube: Echo PLUS & Sonix  
Logicube: OmniPORT  
Logicube: Forensic MD5  
Logicube: RAID I/O Adapter  
Logicube: GPStamp  
Logicube: CellDEK  
Data Duplication Tools  
Data Duplication Tool: R-drive Image  
Data Duplication Tool: DriveLook  
Data Duplication Tool: DiskExplorer  
Demo - File Recovery  
Hardware Tool: ImageMASSter 6007SAS  
Hardware Tool: Disk Jockey IT  
SCSIPAK  
IBM DFSMSdss  
DeepSpar: Disk Imager Forensic Edition  
DeepSpar: 3D Data Recovery  
Phase 1 Tool: PC-3000 Drive Restoration System  
Phase 2 Tool: DeepSpar Disk Imager  
Phase 3 Tool: PC-3000 Data Extractor  
MacQuisition  
MacQuisition: Screenshot  
Module 16 – Review

## **Module 17 – Recovering Deleted Files and Partitions**

43m

Recovering Deleted Files and Partitions  
Recovering Deleted Files  
Deleting Files  
What Happens When a File is Deleted in Windows  
Recycle Bin in Windows  
Storage Locations of Recycle Bin in FAT and NTFS System  
How the Recycle Bin Works  
Damaged or Deleted INFO File  
Damaged Files in Recycled Folder  
Damaged Recycle Folder  
How to Undelete a File  
Data Recovery in Linux  
Tools to Recover Deleted Files  
Tool: Search and Recover  
Tool: Zero Assumption Digital Image Recovery  
More Tools to Recover Deleted Files  
Tool: Mycroft V3  
Tool: PC ParaChute  
Other Tools to Recover Deleted Files

Tool: Image Recall  
Tool: eIMAGE Recovery  
Demo - Handy Recovery  
Demo - Recovering Files and Partitions  
Tools to Recover Deleted Files  
Recovering Deleted Partitions  
Deletion of Partition  
Deletion of Partition using Windows  
Deletion of Partition using Command Line  
Recovery of Deleted Partition  
Recovering Deleted Partition Tools  
Tool: TestDisk  
ThumbsDisplay  
Demo - HD Tune  
Module 17 - Review

## **Module 18 - Forensic Investigation Using AccessData FTK**

1hr 20m

Forensic Investigation Using AccessData FTK  
Forensic Toolkit (FTK)  
Features of FTK  
Installation of FTK  
Demo - Installing FTK V1.7  
Software Requirement  
Installing FTK  
FTK Installation  
Codemeter Stick Installation  
Oracle Installation  
Single Computer Installation  
Choosing An Evidence Server  
Installing the KFF Library  
Installing on Separate Computers  
Demo - KFF Install v1.7  
Setting Up The Application Administrator  
Case Manager Window  
Toolbar Components  
Properties Pane  
Hex Interpreter Pane  
Web Tab  
Filtered Tab  
Text Tab  
Hex Tab  
Explore Tab  
Quickpicks Filter  
Data Processing Status Dialog  
Email Tab  
Graphics Tab  
Thumbnails Pane  
Bookmarks Tab  
Live Search Tab  
Index Search Tab

Creating Tabs  
Launching FTK  
Working with FTK  
Creating A Case  
Demo - Creating a New Case with FTK v1.7  
Demo - FTK  
Evidence Processing Options  
Selecting Data Carving Options  
Selecting Evidence Discovery Options  
Selecting Evidence Refinement (Advanced) Options  
Selecting Index Refinement (Advanced) Options  
Refining an Index by File Date/Size  
Adding Evidence  
Backing Up the Case  
Restoring a Case  
Deleting a Case  
Working with Cases  
Opening an Existing Case  
Adding Evidence  
Selecting a Language  
Additional Analysis  
Properties Tab  
The Hex Interpreter Tab  
Using The Bookmark Information Pane  
Creating a Bookmark  
Bookmarking Selected Text  
Adding Evidence to an Existing Bookmark  
Moving A Bookmark  
Removing A Bookmark  
Deleting Files From A Bookmark  
Verifying Drive Image Integrity  
Copying Information From FTK  
Exporting File List Info  
Exporting the Word List  
Creating a Fuzzy Hash Library  
Selecting Fuzzy Hash Options During Initial Processing  
Additional Analysis Fuzzy Hashing  
Comparing Files Using Fuzzy Hashing  
Viewing Fuzzy Hash Results  
Demo - Opening a Case Run Data Carving and Bookmark Evidence  
Searching A Case  
Conducting A Live Search  
Customizing The Live Search Tab  
Documenting Search Results  
Using Copy Special to Document Search Results  
Bookmarking Search Results  
Data Carving  
Using Filters  
Creating A Filter  
Refining A Filter

Decrypting Encrypted Files  
Decrypting Files And Folders  
Decrypting Domain Account EFS Files  
Decrypting Safeguard Utimaco Files  
Working with Reports  
Creating A Report  
Saving Settings  
Including Bookmarks  
Including Graphics  
Selecting a File Path List  
Selecting a File Properties List  
Registry Selections  
Selecting the Report Location  
PDF Report  
Customizing the Interface  
Module 18 - Review

## **Module 19 - Forensics Investigations Using EnCase**

23m

Forensics Investigations Using EnCase  
Evidence File  
Verifying Evidence Files  
Evidence File Format  
Verifying File Integrity  
Hashing  
Acquiring Image  
Configuring EnCase  
EnCase Options Screen  
EnCase Screens  
View Menu  
Device Tab  
Viewing Files and Folders  
Bottom Pane  
Viewers in View Pane  
Status Bar  
Searching  
Keywords  
Keywords: Screenshot  
Adding Keywords  
Grouping  
Add Multiple Keywords  
Starting the Search  
Search Hits Tab  
Search Hits  
Bookmarks  
Creating Bookmarks  
Adding Bookmarks  
Bookmarking Selected Data  
Recovering Deleted Files/folders in FAT Partition  
Viewing Recovered Files  
Recovering Folders in NTFS

Master Boot Record  
Bookmark Data  
NTFS Starting Point  
Viewing Disk Geometry  
Recovering Deleted Partitions  
Hash Values  
Creating Hash Sets  
MD5 Hash  
Creating Hash  
Viewers  
Signature Analysis  
Viewing the Results  
Copy/UnErase Files or Folders  
E-mail Recovery  
Reporting  
Final Report  
Demo - Encase  
Module 19 - Review

## **Module 20 – Steganography**

1hr 30m

Steganography  
Model of Stegosystem  
Steganography Concepts  
Application of Steganography  
Classification of Steganography  
Technical Steganography  
Linguistic Steganography  
Digital Steganography Techniques  
Injection  
Least Significant Bit (LSB)  
Transform Domain Techniques  
Spread Spectrum Techniques  
Perceptual Masking  
Cover Generation Technique  
Statistical Method Technique  
Distortion Technique  
Different Forms of Steganography  
Text File Steganography  
Image File Steganography  
Steganography Technique in Image File  
Least Significant Bit Insertion in Image Files  
Demo - Imagehide Steg Tool  
Masking and Filtering in Image Files  
Algorithms and Transformation  
Audio File Steganography  
Low-Bit Encoding in Audio Files  
Phase Coding  
Spread Spectrum  
Echo Data Hiding  
Video File Steganography

Steganographic File System  
Issues in Information Hiding  
Demo - Stegoarchive.com Website Software  
Cryptography  
Model of Cryptosystem  
Steganography vs. Cryptography  
Public Key Infrastructure (PKI)  
Key Management Protocols  
Watermarking  
What is Watermarking?  
Case Study  
Steganography vs. Watermarking  
Types of Watermarks  
Attacks on Watermarking  
Application of Watermarking  
Currency Watermarking  
Digimarc's Digital Watermarking  
Watermarking – Mosaic Attack  
Mosaic Attack – Javascript Code  
Steganography Detection  
How to Detect Steganography  
Detecting Steganography  
Detecting Text, Image, Audio and Video Steganography  
Counterfeit Detection  
Steganalysis  
Steganalysis Methods/Attacks on Steganography  
Disabling or Active Attacks  
Introduction to Stego-Forensics  
Steganography in the Future  
Hiding Information in DNA  
Unethical Use of Steganography  
TEMPEST  
Emission Security or Emanations Security (EMSEC)  
Van Eck Phreaking  
Legal Use of Steganography  
Steganography Tools  
Steganography Tool: S- Tools  
Demo - S-Tools  
Steganography Tool: Steghide  
Tool: Mp3Stego  
Tool: Invisible Secrets 4  
Tool: Stegdetect  
Stego Suite – Steg Detection Tool  
Tool: Snow  
Steganography Tools cont.  
Demo - Stegonagraphy  
Module 20 - Review

## **Module 21 - Image File Forensics**

47m

Image File Forensics  
Common Terminologies  
Introduction to Image Files  
Understanding Vector Images  
Understanding Raster Images  
Metafile Graphics  
Image File Formats  
Understanding Image File Formats  
GIF (Graphics Interchange Format)  
JPEG (Joint Photographic Experts Group)  
JPEG File Structure  
JPEG 2000  
BMP (Bitmap) File  
PNG (Portable Network Graphics)  
Tagged Image File Format (TIFF)  
TIFF File Structure  
ZIP (Zone Information Protocol)  
Best Practices for Forensic Image Analysis  
Use MATLAB for Forensic Image Processing  
Advantages of MATLAB  
How File Compression Works?  
Understanding Data Compression  
Huffman Coding Algorithm  
Lempel-Ziv Coding Algorithm  
Lossy Compression  
Vector Quantization  
Locating and Recovering Image Files  
Analyzing Image File Headers  
Repairing Damaged Headers  
Reconstructing File Fragments  
Identifying Unknown File Formats  
Identifying Image File Fragments  
Image File Forensic Tools  
Demo - Image Forensics  
GFE Stealth - Forensics Graphics File Extractor Tool  
Identifying Copyright Issues on Graphics  
Module 21 - Review

## **Module 22 - Audio File Forensics**

27m

Audio File Forensics  
Audio Forensics  
Why Audio Forensics?  
Use of Voice as a Tool  
Fast Fourier Transform (FFT)  
FFT Analysis: Screenshot 1  
FFT Analysis: Screenshot 2  
Methodologies of Audio Forensics  
Voice Identification  
Audibility Analysis

Audio Enhancement  
Audio Enhancement: Screenshots  
Authenticity Analysis  
Sound Identification  
Event Sequence Analysis  
Dialogue Decoding  
Remnant Signal Analysis  
Integrity Verification of the Audio  
Audio Forensics Process  
Audio Forensics Process: Evidence Handling  
Audio Forensics Process: Preparation of Exemplars  
Audio Forensics Process: Preparation of Copies  
Audio Forensics Process: Preliminary Examination  
Audio Forensics Process: Analog to Digital Conversion  
Audio Forensics Process: Preparation of Spectrograms  
Audio Forensics Process: Spectrographic Analysis  
Sound Spectrograph  
Sound Recordings As Evidence In Court Proceedings  
Audio File Manipulation  
Tools  
DCLive Forensics  
Zoom H2 Portable Digital Recorder  
CEDAR for Windows  
Audio File Forensic Tools  
Module 22 - Review

## **Module 24 - Application Password Crackers**

43m

Application Password Crackers  
Password - Terminology  
What is a Password Cracker?  
How Does a Password Cracker Work?  
Password Cracking Methods  
Various Password Cracking Methods  
Brute Force Attack  
Brute Force Attack Time Estimator  
Dictionary Attack  
Syllable Attack/ Rule-based Attack/ Hybrid Attack  
Password Guessing  
Rainbow Attack  
Time Needed to Crack Passwords  
Classification of Cracking Software  
Demo - Password Cracking  
System Password Cracking  
System Level Password Cracking  
CMOS Level Password Cracking  
Tool: CmosPwd  
ERD Commander  
Active Password Changer  
Application Password Cracking  
Application Software Password Cracker

Demo - Application Password Cracking  
Distributed Network Attack  
Default Password Database  
Password Cracking Tools  
Password Recommendations for Improving Password Security  
Standard Password Advice  
Demo - Password Assistant  
Module 24 - Review

## **Module 26 - Network Forensics and Investigating Logs**

44m

Network Forensics and Investigating Logs  
Network Forensics  
The Intrusion Process  
Network Vulnerabilities  
Network Attacks  
Where to Look for Evidence  
Investigating Logs  
Postmortem and Real-Time Analysis  
Handling Logs as Evidence  
Log File Authenticity  
Use Signatures, Encryption, and Checksums  
Work with Copies  
Ensure System Integrity  
Access Control  
Chain of Custody  
Condensing Log File  
Log Injection Attacks  
New Line Injection Attack  
New Line Injection Attack Countermeasure  
Separator Injection Attack  
Defending Separator Injection Attack  
Timestamp Injection Attack  
Defending Timestamp Injection Attack  
Word Wrap Abuse Attack  
Defending Word Wrap Abuse Attack  
Other Kinds of Log File Attacks  
Module 26 - Review

## **Module 27 - Investigating Network Traffic**

1hr 34m

Investigating Network Traffic  
Network Addressing Schemes  
OSI Reference Model  
TCP/ IP Protocol  
Overview of Network Protocols  
Overview of Physical and Data-Link Layer of the OSI Model  
Overview of Network and Transport Layer of the OSI Model  
Types of Network Attacks  
Why Investigate Network Traffic  
Evidence Gathering Via Sniffing  
Demo - Investigating Network Traffic

Acquiring Traffic Using DNS Poisoning Techniques  
Intranet DNS Spoofing (Local Network)  
Demo - DNS Spoofing (Local Network)  
Internet DNS Spoofing (Remote Network)  
Internet DNS Spoofing  
Proxy Server DNS Poisoning  
DNS Cache Poisoning  
Demo - DNS Analysis  
Evidence Gathering From ARP Table  
Evidence Gathering at the Data-link Layer: DHCP Database  
Screenshot: DHCP Log  
Gathering Evidence by IDS  
Traffic Capturing and Analysis Tools  
Tool: Tcpcmdump  
Screenshot: Tcpcmdump  
Tool: Windump  
Tool: NetIntercept  
Tool: Wireshark  
Demo - Wireshark  
Snort Intrusion Detection System  
Snort IDS Placement  
IDS Policy Manager  
Documenting the Evidence Gathered on a Network  
Evidence Reconstruction for Investigation  
Module 27 – Review

## **Module 28 - Router Forensics**

1hr 23m

Router Forensics  
Router  
Functions of a Router  
A Router in an OSI Model  
Routing Table and its Components  
Router Architecture  
Routing Information Protocol  
Implications of a Router Attack  
Routers Vulnerabilities  
Types of Router Attacks  
Router Attack Topology  
Denial of Service (DoS) Attacks  
Packet “Mistreating” Attacks  
Routing Table Poisoning  
Hit-and-Run and Persistent Attacks  
Router Forensics vs. Traditional Forensics  
Steps for Investigating Router Attacks  
Seize the Router and Maintain Chain of Custody  
Guidelines for the Router Forensic  
Incident Response  
Recording Session  
Accessing the Router  
Volatile Evidence

Obtaining Configuration of Router  
Volatile Evidence Gathering  
Direct Access: Using Show Commands  
Indirect Access: Using Scanning Tool  
Compare the Configuration of Router  
Examine the Router Table  
Examine the Access Control List  
Router Logs  
Demo - Router Forensics  
Link Logger  
Link Logger: Screenshot  
Logging  
Handling a Direct Compromise Incident  
Other Incidents  
Real Time Forensics  
Router Audit Tool (RAT)  
Generate the Report  
Module 28 - Review

## **Module 29 - Investigating Wireless Attacks**

35m

Investigating Wireless Attacks  
Wireless Networking Technologies  
Wireless Networks  
Wireless Attacks  
Passive Attack  
Threats from Electronic Emanations  
Active Attacks on Wireless Networks  
Denial-of-Service Attacks  
Man-in-the-Middle Attack (MITM)  
Hijacking and Modifying a Wireless Network  
Network Forensics in a Wireless Environment  
Steps for Investigation  
Key Points to Remember  
Points You Should Not Overlook While Investigating the Wireless Network  
Obtain a Search Warrant  
Document the Scene and Maintain Chain Of Custody  
Identify Wireless Devices  
Wireless Components  
Search for Additional Devices  
Detect Wireless Connections  
Detect Wireless Enabled Computers  
Manual Detection of Wireless APs  
Active Wireless Scanning Technique  
Passive Wireless Scanning Technique  
Capture Wireless Traffic  
Tool: Wireshark  
Determine Wireless Field Strength: Field Strength Meters (FSM)  
Prepare Wireless Zones & Hotspots Maps  
Methods to Access a Wireless Access Point  
Direct-connect to the Wireless Access Point

Default Credentials List  
Direct-connect to the Wireless Access Point  
Rogue Access Point  
Tools to Detect Rogue Access Points: Netstumbler  
“Sniffing” Traffic Between the Access Point and Associated Devices  
MAC Address Information  
Check for MAC Filtering  
Changing the MAC Address  
Report Generation  
Module 29 - Review

## **Module 30 - Investigating Web Attacks**

1hr 17m

Investigating Web Attacks  
Scenario  
Indications of a Web Attack  
Types of Web Attacks  
Cross-Site Scripting (XSS)  
Cross-Site Request Forgery (CSRF)  
Anatomy of CSRF Attack  
Pen-Testing CSRF Validation Fields  
SQL Injection Attacks  
Investigating SQL Injection Attacks  
Code Injection Attack  
Investigating Code Injection Attack  
Parameter Tampering  
Cookie Poisoning  
Investigating a Cookie Poisoning Attack  
Buffer Overflow/Cookie Snooping  
Detecting Buffer Overflow  
DMZ Protocol Attack / Zero Day Attack  
Authentication Hijacking  
Investigating Authentication Hijacking  
Log Tampering  
Directory Traversal  
Cryptographic Interception  
URL Interpretation and Impersonation Attack  
Overview of Web Logs  
Investigating Web Attack  
Investigating FTP Servers  
Investigating IIS Logs  
Investigating Apache Logs  
Investigating Web Attacks in Windows Based Servers  
Web Page Defacement  
Defacement Using DNS Compromise  
Investigating DNS Poisoning  
Intrusion Detection  
Security Strategies for Web Applications  
Investigating Static and Dynamic IP Address  
Checklist for Web Security  
Log Analyzer: Server Log Analysis

Web Attack Investigation Tools  
Demo - Locating IP Addresses  
Module 30 - Review

## **Module 31 - Investigating DoS Attacks**

45m

Investigating DoS Attacks  
DoS Attack  
Indications of a DoS/DDoS Attack  
Types of DoS Attacks  
Ping of Death Attack  
Teardrop Attack  
SYN Flooding  
Demo - SYN Flooding  
Land  
Smurf  
Fraggle and Snork Attack  
Windows Out-Of-Band (OOB) Attack and Buffer Overflow  
Nuke Attacks and Reflected Attack  
Demo - Investigation DoS Attacks  
DDoS Attack  
Working of DDoS Attacks  
Classification of DDoS Attack  
DDoS Attack Taxonomy  
DoS Attack Modes  
Techniques to Detect DoS Attack  
Demo - Smart Sniff  
Techniques to Detect DoS Attack: Activity Profiling  
Techniques to Detect DoS Attack: Sequential Change-Point Detection  
Techniques to Detect DoS Attack: Wavelet-based Signal Analysis  
Monitoring CPU Utilization to Detect DoS Attacks  
Detecting DoS Attacks using Cisco NetFlow  
Detecting DoS Attacks using Network Intrusion Detection System (NIDS)  
Investigating DoS Attack  
Demo - 3D Trace Route  
ICMP Traceback  
Hop by Hop IP Traceback  
Challenges in Investigating DoS Attack  
Module 31 - Review

## **Module 33 - Investigating Internet Crimes**

1hr 20m

Investigating Internet Crimes  
Internet Crimes  
Internet Forensics  
Why Internet Forensics?  
Goals of Investigation  
Steps to Investigate Internet Crimes  
Obtain a Search Warrant  
Interview the Victim  
Prepare Bit-Stream Copies  
Check the Logs

Identify the Source of the Attack  
IP Address  
Internet Assigned Numbers Authority  
Regional Internet Registry (RIR)  
Internet Service Provider  
Trace the IP Address of the Attacker Computer  
Domain Name System (DNS)  
DNS Record Manipulation  
DNS Lookup  
Nslookup  
Analyze the Whois Information  
Whois  
Whois Tools and Utilities  
Samspace  
IP Address Locator  
Tracing Geographical Location of a URL  
Demo – Investigating Internet Crimes  
Traceroute  
Collect the Evidence  
Examining Information in Cookies  
Viewing Cookies in Firefox  
Tool: Cookie Viewer  
Switch URL Redirection  
Embedded JavaScript  
Downloading a Single Page or an Entire Web Site  
Tool: My Offline Browser  
Tool: WayBack Machine  
Trace the Email  
Email Headers Forging  
Viewing Header Information  
Tracing Back Spam Mail  
VisualRoute  
Demo - Visual Route  
Report Generation  
Module 33 - Review

## **Module 34 - Tracking Emails and Investigating Email Crimes**

57m

Tracking Emails and Investigating Email Crimes  
Email System  
Email Client  
Email Server  
SMTP Server  
POP3 and IMAP Servers  
Importance of Electronic Records Management  
Email Crime  
Spamming  
Mail Bombing/Mail Storm  
Crime via Chat Rooms  
Identity Fraud/Chain Letter  
Phishing

Email Spoofing  
Investigating Email Crime and Violations  
Obtain a Search Warrant and Seize the Computer and Email Account  
Obtain a Bit-by-Bit Image of Email Information  
Email Message  
Viewing Header in Microsoft Outlook  
Microsoft Outlook Header  
Viewing Header in AOL  
Example: Rudy Sends an E-Mail to Timmy  
Analysis of Email Header to Timmy  
Received: Headers  
Forging Headers  
List of Common Headers  
Examining Additional Files (.pst or .ost files)  
Pst File Location  
Microsoft Outlook Mail  
Examine the Originating IP Address  
<http://centralops.net/co/>  
Exchange Message Tracking Center  
MailDetective Tool  
Examine Phishing  
Forensic Tool Kit (FTK)  
Recover My Email for Outlook  
Tracing Back  
Tracing Back Web Based Email  
Demo - Email Trace  
Abuse.Net  
Tool: LoPe  
Tool:eMailTrackerPro  
Module 34 - Review

## **Module 35 - PDA Forensics**

31m

PDA Forensics  
Personal Digital Assistant (PDA)  
Information Stored in PDAs  
PDA Components  
Obama's new BlackBerry  
Secure Baby...  
PDA Characteristics  
Generic PDA Hardware Diagram  
Palm OS  
Architecture of Palm OS Devices  
Pocket PC  
Architecture for Windows Mobile  
Linux-based PDAs  
Architecture of the Linux OS for PDAs  
PDA Generic States  
PDA Security Issues  
ActiveSync and HotSync Features  
ActiveSync Attacks

HotSync Attack  
PDA Forensics  
PDA Forensic Steps  
Points to Remember while Conducting Investigation  
Acquire the Information  
Data Acquisition Techniques  
PDA Forensics Tools  
PDA Secure  
PDA Secure: Screenshot  
Device Seizure  
DS Lite  
PDA Security Countermeasures  
Module 35 - Review

### **Module 36 - BlackBerry Forensics**

23m

BlackBerry Forensics  
BlackBerry  
How BlackBerry Works  
BlackBerry Serial Protocol  
Blackjacking Attack  
BlackBerry Attack Toolkit  
BlackBerry Attachment Service Vulnerability  
TeamOn Import Object ActiveX Control Vulnerability  
Denial of Service in BlackBerry Browser  
BlackBerry Security  
BlackBerry Wireless Security  
BlackBerry Security for Wireless Data  
Prerequisites for Blackberry Forensics  
Steps for BlackBerry Forensics  
Imaging and Profiling in BlackBerry  
Acquire the Information  
Hidden Data in BlackBerry  
Acquire Logs Information from BlackBerry  
Program Loader  
Review of Information  
Simulator: Screenshot  
BlackBerry Signing Authority Tool  
Forensics Tool: RIM BlackBerry Physical Plug-in  
ABC Amber BlackBerry Converter  
Pocket PC  
BlackBerry Database Viewer Plus  
Module 36 - Review

### **Module 37 - iPod and iPhone Forensics**

31m

iPod and iPhone Forensics  
News: Students Charged: iPod used as Criminal Tool  
iPod  
iPhone Overview  
What a Criminal Can Do with an iPod  
What a Criminal Can Do with an iPhone

iPhone OS Overview  
iPhone Disk Partitions  
Apple HFS+ and FAT32  
Application Formats  
iPod and iPhone Forensics cont.  
Evidence Stored on iPod and iPhone  
Forensic Prerequisites  
Collecting iPod/iPhone Connected with Mac  
Collecting iPod/iPhone Connected with Windows  
Disable Automatic Syncing  
Write Blocking  
Write Blocking in Different OS  
Image the Evidence  
View the iPod System Partition  
View the Data Partition  
Break Passcode to Access the Locked iPhone  
Acquire DeviceInfo File  
Acquire SysInfo File  
SysInfo File  
Recover IPSW File  
Check the Internet Connection Status  
View Firmware Version  
Recover Network Information  
Recovering Data from SIM Card  
Acquire the User Account Information  
View the Calendar and Contact Entries  
Recovering Photos  
Recovering Address Book Entries  
Recovering Calendar Events  
Recovering Call Logs  
Recovering Map Tile Images  
Recovering Cookies  
Recovering Cached and Deleted Email  
Recover Deleted Files  
Forensic Information from the Windows Registry  
Forensic Information from the Windows: setupapi.log  
Recovering SMS Messages  
Timeline Generation  
Time Issues  
Module 37 - Review

## **Module 38 - Cell Phone Forensics**

22m

Cell Phone Forensics  
Mobile Phone  
Hardware Characteristics of Mobile Devices  
Software Characteristics of Mobile Devices  
Components of Cellular Network  
Cellular Network  
Different Cellular Networks  
Different OS in Mobile Phone

What a Criminal Can do with Mobiles  
Mobile Forensics  
Forensics Information in Mobile Phones  
Subscriber Identity Module (SIM)  
Integrated Circuit Card Identification (ICCID)  
International Mobile Equipment Identifier (IMEI)  
Electronic Serial Number (ESN)  
Precautions to be Taken Before Investigation  
Points to Remember While Collecting the Evidence  
Acquire the Information  
Acquire Data from SIM Cards  
Acquire Data from Unobstructed Mobile Devices  
Acquire the Data from Obstructed Mobile Devices  
Memory Considerations in Mobiles  
Acquire Data from Memory Cards  
Memory Cards  
Acquire Data from Synched Devices  
Gather Data from Network Operator  
Check Call Data Records (CDR's)  
Challenges for Forensic Efforts  
Module 38 - Review

### **Module 41 - Investigating Corporate Espionage**

45m

Investigating Corporate Espionage  
Introduction to Corporate Espionage  
Motives Behind Spying  
Information that Corporate Spies Seek  
Corporate Espionage: Insider/Outsider Threat  
Threat of Corporate Espionage Due to Aggregation of Information  
Techniques of Spying  
Defense Against Corporate Spying  
Controlled Access  
Background Investigation of the Personnel  
Basic Security Measures to Protect Against Corporate Spying  
Steps to Prevent Corporate Espionage  
Investigating Corporate Espionage Cases  
Employee Monitoring: Activity Monitor  
Spector CNE Employee Monitoring Software  
Tool: Privatefirewall with Pest Patrol  
Anti Spy Tools  
Demo - Spy Sweeper  
Demo - Hijack This  
Guidelines While Writing Employee Monitoring Policies  
Module 41 - Review

### **Module 43 - Investigate Trademark and Copyright Infringement**

25m

Investigate Trademark and Copyright Infringement  
Trademark Infringement  
Trademarks  
Trademark Eligibility and Benefits of Registering It

Service Marks and Trade Dress  
Trademark Infringement  
Monitoring Trademark Infringements  
Key Considerations Before Investigating Trademark Infringements  
Steps for Investigating Trademark Infringements  
Copyright Infringement  
Copyright  
Investigating Copyright Status  
How Long Does a Copyright Last?  
U.S. Copyright Office  
How Are Copyrights Enforced ?  
Copyright Infringement: Plagiarism  
Types of Plagiarism  
Steps for Plagiarism Prevention  
Plagiarism Detection Factors  
Plagiarism Detection Tools  
Patent Infringement  
Patent  
Patent Infringement (Cont.)  
Types of Patent Infringement  
Patent Search  
<http://www.ip.com>  
How ip.com Works  
Domain Name Infringement  
How to Check for Domain Name Infringement  
Intellectual Property  
Investigating Intellectual Property Theft  
Steps for Investigating Intellectual Property Theft  
Digital Rights Management  
Windows Media Digital Rights Management  
Media-DRM Packager  
Trademarks and Copyright Laws  
U.S. Laws for Trademarks and Copyright  
Module 43 - Review

## **Module 44 - Investigating Sexual Harassment Incidents**

27m

Investigating Sexual Harassment Incidents  
Sexual Harassment  
Types of Sexual Harassment  
Consequences of Sexual Harassment  
What You Should Do if You are Being Sexually Harassed  
Stalking  
Stalking Behaviors  
Responsibilities of Supervisors  
Responsibilities of Employees  
Complaint Procedures  
Investigation Process  
Sexual Harassment Investigations  
Sexual Harassment Policy  
Preventive Steps

U.S. Laws on Sexual Harassment  
Australian Laws on Sexual Harassment  
Indian Law: Sexual Harassment of Women in the Workplace  
Module 44 - Review

### **Module 45 - Investigating Child Pornography Cases**

45m

Investigating Child Pornography Cases  
Introduction to Child Pornography  
People's Motive Behind Child Pornography  
People Involved in Child Pornography  
Role of Internet in Child Pornography  
Measures to Prevent Dissemination of Child Pornography  
Challenges in Controlling Child Pornography  
Precautions before Investigating Child Pornography Cases  
Steps for Investigating Child Pornography  
Step 1: Search and Seize all Computers and Media Devices  
Step 2: Check Authenticated Login Sessions  
Step 3: Search Hard Disk for Pornographic Material  
Step 4: Recover Deleted Files and Folders  
Step 5: Check Metadata of Files and Folders Related with Pornography  
Step 6: Check and Recover the Browser Information  
Browsing History, Save Form, and Search History  
Download History  
Cache  
Cookies  
Saved Passwords  
Authenticated Sessions  
Step 7: Check ISP Logs  
Sources of Digital Evidence  
Guidelines to Avoid Child Pornography on Web  
Guidelines for Parents to Reduce the Risk of Child being Porned  
Reveal  
ChatGuard  
U.S. Laws against Child Pornography  
U.K. Laws against Child Pornography  
Children's Internet Protection Act (CIPA)  
Perverted Justice  
Module 45 - Review

### **Module 50 - Investigative Reports**

24m

Investigative Reports  
Computer Forensic Report  
Computer Forensics Report Template  
Report Specifications  
Report Classification  
Layout of an Investigative Report  
Layout of an Investigative Report: Numbering  
Guidelines for Writing a Report  
Use of Supporting Material  
Importance of Consistency

Salient Features of a Good Report  
Important Aspects of a Good Report  
Investigative Report Format  
Attachments and Appendices  
Include Metadata  
Investigation Procedures  
Collecting Physical and Demonstrative Evidence  
Collecting Testimonial Evidence  
The Do and Do Not's of Forensic Computer Investigations  
Case Report Writing and Documentation  
Create a Report to Attach to the Media Analysis Worksheet  
Best Practices for Investigators  
Module 50 - Review

### **Module 51 - Becoming an Expert Witness**

47m

Becoming an Expert Witness  
What is an Expert Witness  
Role of an Expert Witness  
What Makes a Good Expert Witness?  
Types of Expert Witnesses  
Computer Forensics Experts  
Role of Computer Forensics Expert  
Technical Witness vs. Expert Witness  
Preparing for Testimony  
Evidence Preparation and Documentation  
Evidence Processing Steps  
Examining Computer Evidence  
Prepare the Report  
Evidence Presentation  
Rules Pertaining to an Expert Witness' Qualification  
Importance of a Resume  
Testifying in the Court  
The Order of Trial Proceedings  
General Ethics While Testifying  
Importance of Graphics in a Testimony  
Helping Your Attorney  
Avoiding Testimony Issues  
Testifying During Direct Examination  
Testifying During Cross-Examination  
Deposing  
Dealing with Media  
Module 51 - Review  
Course Closure

**Total Duration: 38h 23m**