



**EC-Council**

# **Computer Hacking Forensic Investigator**

## **Course Description**

The CHFI course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be taught during this course, including software, hardware and specialized techniques. The need for businesses to become more efficient and integrated with one another, as well as the home user, has given way to a new type of criminal, the "cyber-criminal." It is no longer a matter of "will your organization be comprised (hacked)?" but, rather, "when?" Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.

## **Who Should Attend**

Police and other law enforcement personnel, Defense and Military personnel, e-Business Security professionals, Systems administrators, Legal professionals, Banking, Insurance and other professionals, Government agencies, IT managers

## **Prerequisites**

It is strongly recommended that you attend the CEH class before enrolling into CHFI program.

## **Duration:**

5 days (9:00 – 5:00)

## **Certification**

The CHF1 312-49 exam will be conducted on the last day of training. Students need to pass the online Prometric exam to receive the CHF1 certification.

## **Course Outline v3**

### Module 01: Computer Forensics in Today's World

- § Ways of Forensic Data Collection
- § Objectives of Computer Forensics
- § Benefits of Forensic Readiness
- § Categories of Forensics Data
- § Computer Facilitated Crimes
  - o Type of Computer Crimes
  - o Examples of Evidence
- § Stages of Forensic Investigation in Tracking Cyber Criminals
- § Key Steps in Forensics Investigations
- § Need for Forensic Investigator
- § When An Advocate Contacts The Forensic Investigator, He Specifies How To Approach
- § Enterprise Theory of Investigation (ETI)
- § Where and when do you use Computer Forensics
- § Legal Issues
- § Reporting the Results

## Module 02: Law and Computer Forensics

- § Privacy Issues Involved in Investigations
- § Fourth Amendment Definition
- § Interpol- Information Technology Crime Center
- § Internet Laws and Statutes
- § Intellectual Property Rights
- § Cyber Stalking
- § Crime Investigating Organizations
- § The G8 Countries: Principles to Combat High-tech Crime
- o The G8 Countries: Action Plan to Combat High-Tech Crime (International Aspects of Computer Crime)
- § United Kingdom: Police and Justice Act 2006
- § Australia: The Cybercrime Act 2001
- § Belgium
- § European Laws
- § Austrian Laws
- § Brazilian Laws
- § Belgium Laws
- § Canadian Laws
- § France Laws
- § Indian Laws
- § German Laws

- § Italian Laws
- § Greece Laws
- § Denmark Laws
- § Norwegian Laws
- § Netherlands Laws
- § Internet Crime Schemes
- o Why You Should Report Cybercrime
- o Reporting Computer-related Crimes
- o Person Assigned to Report the Crime
- o When and How to Report an Incident?
- o Who to Contact at the Law Enforcement?
- o Federal Local Agents Contact
- o More Contacts
- o Cyberthreat Report Form

#### Module 03: Computer Investigation Process

- § Securing the Computer Evidence
- § Preparation for Searches
- § Chain-of Evidence Form
- § Accessing the Policy Violation Case: Example
- § 10 Steps to Prepare for a Computer Forensic Investigation
- § Investigation Process

- o Policy and Procedure Development
- o Evidence Assessment
  - Case Assessment
  - Processing Location Assessment
  - Legal Considerations
  - Evidence Assessment
- o Evidence Acquisition
  - Write Protection
  - Acquire the Subject Evidence
- o Evidence Examination
  - Physical Extraction
  - Logical Extraction
  - Analysis of Extracted Data
  - Timeframe Analysis
  - Data Hiding Analysis
  - Application and File Analysis
  - Ownership and Possession
- o Documenting and Reporting
  - What Should be in the Final Report?
- § Maintaining Professional Conduct

Module 04: First Responder Procedure

- § Electronic Evidence
- § The Forensic Process
- § Types of Electronic Devices
  - o Electronic Devices: Types and Collecting Potential Evidence
- § Evidence Collecting Tools and Equipment
- § First Response Rule
- § Incident Response: Different Situations
  - o First Response for System Administrators
  - o First Response by Non-Laboratory Staff
  - o First Response by Laboratory Forensic Staff
- § Securing and Evaluating Electronic Crime Scene
- § Ask These Questions When A Client Calls A Forensic Investigator
- § Health and Safety Issues
- § Consent
- § Planning the Search and Seizure
  - o Initial Search of the Scene
  - o Witness Signatures
  - o Conducting Preliminary Interviews
    - Initial Interviews
  - o Documenting Electronic Crime Scene
  - o Photographing the Scene

- o Sketching the Scene
- o Collecting and Preserving Electronic Evidence
  - Evidence Bag Contents List
  - Order of Volatility
  - Dealing with Powered OFF Computers at Seizure Time
  - Dealing with a Powered ON PC
  - Computers and Servers
  - Collecting and Preserving Electronic Evidence
  - Seizing Portable Computers
  - Switched ON Portables
  - Packaging Electronic Evidence
  - Exhibit Numbering
- o Transporting Electronic Evidence
- o Handling and Transportation to the Forensic Laboratory
- § 'Chain of Custody'
- § Findings of Forensic Examination by Crime Category

#### Module 05 : CSIRT

- § How to Prevent an Incident?
- § Defining the Relationship between Incident Response, Incident Handling, and Incident Management
- § Incident Response Checklist
- § Incident Management

- § Why don't Organizations Report Computer Crimes?
- § Estimating Cost of an Incident
- § Vulnerability Resources
- § Category of Incidents
  - o Category of Incidents: Low Level
  - o Category of Incidents: Mid Level
  - o Category of Incidents: High Level
- § CSIRT: Goals and Strategy
  - o Motivation behind CSIRTs
  - o Why an Organization needs an Incident Response Team?
  - o Who works in a CSIRT?
  - o Staffing your Computer Security Incident Response Team: What are the Basic Skills Needed?
  - o Team Models
  - o CSIRT Services can be Grouped into Three Categories:
  - o CSIRT Case Classification
  - o Types of Incidents and Level of Support
  - o Service Description Attributes
  - o Incident Specific Procedures
  - o How CSIRT handles Case: Steps
  - o US-CERT Incident Reporting System
  - CSIRT Incident Report Form

- CERT(R) Coordination Center: Incident Reporting Form
- o Limits to Effectiveness in CSIRTs
- o Working Smarter by Investing in Automated Response Capability
- § World CERTs <http://www.trusted-introducer.nl/teams/country.html>
- § <http://www.first.org/about/organization/teams/>
- § IRTs Around the World

#### Module 06: Computer Forensic Lab

- § Ambience of a Forensics Lab: Ergonomics
- § Forensic Laboratory Requirements
- o Paraben Forensics Hardware: Handheld First Responder Kit
- o Paraben Forensics Hardware: Wireless StrongHold Bag
- o Paraben Forensics Hardware: Remote Charger
- o Paraben Forensics Hardware: Device Seizure Toolbox
- o Paraben Forensics Hardware: Wireless StrongHold Tent
- o Paraben Forensics Hardware: Passport StrongHold Bag
- o Paraben Forensics Hardware: Project-a-Phone
- o Paraben Forensics Hardware: SATA Adaptor Male/ Data cable for Nokia 7110/6210/6310/i
- o Paraben Forensics Hardware: Lockdown
- o Paraben Forensics Hardware: SIM Card Reader/ Sony Clie N & S Series Serial Data Cable
- o Paraben Forensics Hardware: USB Serial DB9 Adapter

- § Portable Forensic Systems and Towers: Forensic Air-Lite VI MKII laptop
- o Portable Forensic Systems and Towers: Original Forensic Tower II
- o Portable Forensic Systems and Towers: Portable Forensic Workhorse V
- o Portable Forensic Workhorse V: Tableau 335 Forensic Drive Bay Controller
- o Portable Forensic Systems and Towers: Forensic Air-Lite IV MK II
- o Portable Forensic Systems and Towers: Forensic Tower II
- § Forensic Write Protection Devices and Kits: Ultimate Forensic Write Protection Kit
- o Tableau T3u Forensic SATA Bridge Write Protection Kit
- o Tableau T8 Forensic USB Bridge Kit/Addonics Mini DigiDrive READ ONLY 12-in-1 Flash Media Reader
- § Power Supplies and Switches
- § DIBS® Mobile Forensic Workstation
- o DIBS® Advanced Forensic Workstation
- o DIBS® RAID: Rapid Action Imaging Device
- § Forensic Archive and Restore Robotic Devices: Forensic Archive and Restore (FAR Pro)
- § Forensic Workstations
- § Tools: LiveWire Investigator
- § Features of the Laboratory Imaging System
- o Technical Specification of the Laboratory-based Imaging System
- § Computer Forensic Labs, Inc
- o Procedures at Computer Forensic Labs (CFL), Inc

§ Data Destruction Industry Standards

Module 07: Understanding File Systems and Hard Disks

§ Types of Hard Disk Interfaces

- o Types of Hard Disk Interfaces: SCSI
- o Types of Hard Disk Interfaces: IDE/EIDE
- o Types of Hard Disk Interfaces: USB
- o Types of Hard Disk Interfaces: ATA
- o Types of Hard Disk Interfaces: Fibre Channel
- o Disk Capacity Calculation
- o Evidor: The Evidence Collector
- o WinHex

§ EFS Key

§ FAT vs. NTFS

§ Windows Boot Process (XP/2003)

§ <http://www.bootdisk.com>

Module 08: Understanding Digital Media Devices

§ Digital Storage Devices

§ Magnetic Tape

§ Floppy Disk

§ Compact Disk

§ CD-ROM

- § DVD
  - o DVD-R, DVD+R, and DVD+R(W)
  - o DVD-RW, DVD+RW
  - o DVD+R DL/ DVD-R DL/ DVD-RAM
  - o HD-DVD (High Definition DVD)
  - o HD-DVD
- § Blu-Ray
- § CD Vs DVD Vs Blu-Ray
- § HD-DVD vs. Blu-Ray
- § iPod
- § Zune
- § Flash Memory Cards
  - o Secure Digital (SD) Memory Card
  - o Compact Flash (CF) Memory Card
  - o Memory Stick (MS) Memory Card
  - o Multi Media Memory Card (MMC)
  - o xD-Picture Card (xD)
  - o SmartMedia Memory (SM) Card
- § USB Flash Drives
  - o USB Flash in a Pen

- § Terminologies
- § Boot Loader
- § Boot Sector
- § Anatomy of MBR
- § Basic System Boot Process
- § MS-DOS Boot Process
- § Windows XP Boot Process
- § Common Startup Files in UNIX
- § List of Important Directories in UNIX
- § Linux Boot Process
- § Macintosh Forensic Software by BlackBag
  - o Directory Scan
  - o FileSpy
  - o HeaderBuilder
- § Carbon Copy Cloner (CCC)
- § MacDrive6

#### Module 10: Windows Forensics

- § Windows Forensics Tool: Helix
  - o Tools Present in Helix CD for Windows Forensics
  - o Helix Tool: SecReport
  - o Helix Tool: Windows Forensic Toolchest (WFT)

- § MD5 Generator: Chaos MD5
  - o Secure Hash Signature Generator
  - o MD5 Generator: Mat-MD5
  - o MD5 Checksum Verifier 2.1
- § Registry Viewer Tool: RegScanner
- § Virtual Memory
- § System Scanner
- § Integrated Windows Forensics Software: X-Ways Forensics
- § Tool: Traces Viewer
- § Investigating ADS Streams

#### Module 11: Linux Forensics

- § File System Description
- § Mount Command
- § Popular Linux Forensics Tools
  - o The Sleuth Kit
    - Tools Present in "The Sleuth Kit"
  - o Autopsy
    - The Evidence Analysis Techniques in Autopsy
  - o SMART for Linux
  - o Penguin Sleuth
    - Tools Included in Penguin Sleuth Kit

- o Forensix
- o Maresware
- Major Programs Present in Maresware
- o Captain Nemo
- o THE FARMER'S BOOT CD

#### Module 12: Data Acquisition and Duplication

- § Mount Image Pro
- § Snapshot Tool
- § Snapback DatArrest
- § Hardware Tool: Image MASter Solo-3 Forensic
- o Hardware Tool: LinkMASter-2 Forensic
- o Hardware Tool: RoadMASter-2
- § Save-N-Sync
- § Hardware Tool: ImageMASter 6007SAS
- § Hardware Tool: Disk Jockey IT
- § SCSIPAK
- § IBM DFSMSdss
- § Tape Duplication System: QuickCopy

#### Module 13: Computer Forensic Tools

##### **Part I- Software Forensics Tools**

- § Visual TimeAnalyzer

- § X-Ways Forensics
- § Evidor
- § Data Recovery Tools: Device Seizure 1.0
  - o Data Recovery Tools: Forensic Sorter v2.0.1
  - o Data Recovery Tools: Directory Snoop
- § Permanent Deletion of Files: Darik's Boot and Nuke (DBAN)
- § File Integrity Checker: FileMon
  - o File Integrity Checker: File Date Time Extractor (FDTE)
  - o File Integrity Checker: Decode - Forensic Date/Time Decoder
- § Partition Managers: Partimage
- § Linux/Unix Tools: Ltools and Mtools
- § Password Recovery Tool: Decryption Collection Enterprise v2.5
  - o Password Recovery Tool: AIM Password Decoder
  - o Password Recovery Tool: MS Access Database Password Decoder
- § Internet History Viewer: CookieView - Cookie Decoder
  - o Internet History Viewer: Cookie Viewer
  - o Internet History Viewer: Cache View
  - o Internet History Viewer: FavURLView - Favourite Viewer
  - o Internet History Viewer: NetAnalysis
- § FTK- Forensic Toolkit
- § Email Recovery Tool: E-mail Examiner

- o Email Recovery Tool: Network E-mail Examiner
  - § Case Agent Companion
  - § Chat Examiner
  - § Forensic Replicator
  - § Registry Analyzer
  - § SIM Card Seizure
  - § Text Searcher
  - § Autoruns
  - § Autostart Viewer
  - § Belkasoft RemovEx
  - § HashDig
  - § Inforenz Forager
  - § KaZAlyser
  - § DiamondCS OpenPorts
  - § Pasco
  - § Patchit
  - § PE Explorer
  - § Port Explorer
  - § PowerGREP
  - § Process Explorer
  - § PyFLAG

- § Registry Analyzing Tool: Regmon
- § Reverse Engineering Compiler
- § SafeBack
- § TapeCat
- § Vision

## Part II- Hardware Forensics Tools

- § List of Hardware Computer Forensic Tools
  - o Hard Disk Write Protection Tools: Nowrite & Firewire Drivedock
  - o LockDown
  - o Write Protect Card Reader
  - o Drive Lock IDE
  - o Serial-ATA DriveLock Kit
  - o Wipe MASster
  - o ImageMASster Solo-3 IT
  - o ImageMASster 4002i
  - o ImageMasster 3002SCSI
  - o Image MASster 3004SATA

## Module 14: Forensics Investigations Using Encase

- § Evidence File
  - o Evidence File Format
- § Verifying File Integrity

- § Hashing
- § Acquiring Image
- § Configuring Encase
  - o Encase Options Screen
  - o Encase Screens
  - o View Menu
  - o Device Tab
  - o Viewing Files and Folders
  - o Bottom Pane
- § Viewers in Bottom Pane
  - o Status Bar
  - o Status Bar
- § Searching
- § Keywords
  - o Adding Keywords
  - o Grouping
  - o Add multiple Keywords
- § Starting the Search
  - o Search Hits Tab
  - o Search Hits
- § Bookmarks

- o Creating Bookmarks
- o Adding Bookmarks
- o Bookmarking Selected Data
- § Recovering Deleted Files/folders in FAT Partition
- o Viewing Recovered Files
- o Recovering Folders in NTFS
- § Master Boot Record
- § NTFS Starting Point
- § Viewing Disk Geometry
- § Recovering Deleted Partitions
- § Hash Values
- o Creating Hash Sets
- o MD5 Hash
- o Creating Hash
- § Viewers
- § Signature Analysis
- § Viewing the Results
- § Copying Files Folders
- § E-mail Recovery
- § Reporting
- § Encase Boot Disks

§ IE Cache Images

Module 15: Recovering Deleted Files and Deleted partitions

Part I: Recovering Deleted Files

§ Deleting Files

§ What happens when a File is Deleted 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

§ Tools to Recover Deleted Files

- o Tool: Search and Recover
- o Tool: Zero Assumption Digital Image Recovery
- o Tool: PC Inspector Smart Recovery
- o Tool: Fundelete
- o Tool: RecoverPlus Pro
- o Tool: OfficeFIX
- o Tool: Recover My Files
- o Tool: Zero Assumption Recovery
- o Tool: SuperFile Recover
- o Tool: IsoBuster

- o Tool: CDRoller
- o Tool: DiskInternals Uneraser
- o Tool: DiskInternal Flash Recovery
- o Tool: DiskInternals NTFS Recovery
- o Recover Lost/Deleted/Corrupted files on CDs and DVDs
- o Tool: Undelete
- o Tool: Active@ UNDELETE
- o Data Recovery Tool: CD Data Rescue
- o Tool: File Recover
- o Tool: WinUndelete
- o Tool: R-Undelete
- o Tool: Image Recall
- o Tool: eIMAGE Recovery
- o Tool: File Scavenger
- o Tool: Recover4all Professional
- o Tool: eData Unerase
- o Tool: Easy-Undelete
- o Tool: InDisk Recovery
- o Tool: Repair My Excel
- o Tool: Repair Microsoft Word Files
- o Tool: Zip Repair

- o Tool: Canon RAW File Recovery Software

## Part II: Recovering Deleted Partitions

- § Deletion of Partition
- § Deletion of Partition using Windows
- § Deletion of Partition using Command Line
- § Recovery of Deleted Partition
- § Deleted Partition Recovery Tools
- o Tool: GetDataBack
- o Tool: DiskInternals Partition Recovery
- o Tool: Active@ Partition Recovery
- o Tool: Handy Recovery
- o Tool: Acronis Recovery Expert
- o Tool: Active Disk Image
- o Tool: TestDisk
- o Tool: Recover It All!
- o Tool: Scaven
- o Tool: Partition Table Doctor
- o Tool: NTFS Deleted Partition Recovery

## Module 16: Image Files Forensics

- § Common Terminologies
- § Understanding Image File Formats

- o GIF (Graphics Interchange Format)
- o JPEG (Joint Photographic Experts Group)
- o JPEG 2000
- o BMP (Bitmap) File
- o PNG (Portable Network Graphics)
- o Tagged Image File Format (TIFF)
- o ZIP (Zone Information Protocol)
- § How File Compression Works
- § Huffman Coding Algorithm
- § Lempel-Ziv Coding Algorithm
- § Vector Quantization
- § <http://www.filext.com>
- § Picture Viewer: AD
- § Picture Viewer: Max
- § FastStone Image Viewer
- § XnView
- § Faces – Sketch Software
- § Steganalysis
- o Steganalysis Tool: Stegdetect
- § Image File Forensic Tool: GFE Stealth (Graphics File Extractor)
- o Tool: ILook v8

- o Tool: P2 eXplorer

## Module 17: Steganography

- § Classification of Steganography
- § Steganography vs. Cryptography
- § Model of Stegosystem
- § Model of Cryptosystem
- Introduction to Stego-Forensics
- o Important Terms in Stego-Forensics
- Steganography vs. Watermarking
- o Attacks on Watermarking
- o Application of Watermarking
- o Digimarc's Digital Watermarking
- o Watermarking – Mosaic Attack
- Mosaic Attack – Javascript code
- 2Mosaic – Watermark breaking Tool
- Steganalysis
- o Steganalysis Methods/Attacks on Steganography
- TEMPSET
- Van Eck phreaking
- Printer Forensics
- o Is Your Printer Spying On You?

- o DocuColor Tracking Dot Decoding
- § Steganography Tools
  - o Tool: Steganos
  - o Steganography Tool: Pretty Good Envelop
  - o Tool: Gifshuffle
  - o Refugee
  - o Tool: JPHIDE and JPSEEK
  - o Tool: wbStego
  - o Tool: OutGuess
  - o Tool: Invisible Secrets 4
  - o Tool: Masker
  - o Tool: Hydan
  - o Tool: Cloak
  - o Tool: StegaNote
  - o Tool: Stegomagic
  - o Hermetic Stego
- § Application of Steganography
- § How to Detect Steganography?
  - o Stego Suite – Steg Detection Tool
  - o StegSpy

Module: 18: Application Password Crackers

- § Brute Force Attack
- § Dictionary Attack
- § Syllable Attack/Rule-based Attack/Hybrid Attack
- § Password Guessing
- § Rainbow Attack
- § CMOS Level Password Cracking
  - o Tool CmosPwd
  - o ERD Commander
  - o Active Password Changer
- § <http://www.virus.org/index.php?>
- § Pdf Password Crackers
- § Password Cracking Tools
  - o Tool: Cain & Abel
  - o Tool: LCP
  - o Tool: SID&User
  - o Tool: Ophcrack 2
  - o Tool: John the Ripper
  - o Tool: DJohn
  - o Tool: Crack
  - o Tool: Brutus
  - o Tool: Access PassView

- o Tool: RockXP
- o Tool: Magical Jelly Bean Keyfinder
- o Tool: PstPassword
- o Tool: Protected Storage PassView
- o Tool: Network Password Recovery
- o Tool: Mail PassView
- o Tool: Asterisk Key
- o Tool: Messenger Key
- o Tool: MessenPass
- o Tool: Password Spectator Pro
- o Tool: SniffPass
- o Tool: Asterisk Logger
- o Tool: Dialupass
- o Tool: Mail Password Recovery
- o Tool: Database Password Sleuth
- o Tool: CHAOS Generator
- o Tool: PicoZip Recovery
- o Tool: Netscapass
- § Common Recommendations for Improving Password Security
- § Standard Password Advice

- § Introduction to Network Forensics
  - o The Hacking Process
  - o The Intrusion Process
- § Looking for Evidence
- § Log Files as Evidence
- § Records of Regularly Conducted Activity
- § Legality of Using Logs
- § Maintaining Credible IIS Log Files
- § Log File Accuracy
- § Log Everything
- § Keeping Time
  - o UTC Time
- § Use Multiple Logs as Evidence
- § Avoid Missing Logs
- § Log File Authenticity
- § Work with Copies
- § Access Control
- § Chain of Custody
- § Importance of Audit Logs
  - o Central Logging Design
  - o Steps to Implement Central Logging

- o Centralized Syslog Server
- o Syslog-ng: Security Tool
- o IIS Centralized Binary Logging
- o ODBC Logging
- o IISLogger: Development tool
- o Socklog: IDS Log Analysis Tool
- o KiwiSysLog Tool
- o Microsoft Log Parser: Forensic Analysis Tool
- o Firewall Analyzer: Log Analysis Tool
- o Adaptive Security Analyzer (ASA) Pro: Log Analysis Tool
- o GFI EventsManager
- How does GFI EventsManager work?
- o Activeworx Security Center
- o EventLog Analyzer
- § Why Synchronize Computer Times?
- § What is NTP Protocol?
- o NTP Stratum Levels
- § NIST Time Servers
- § Configuring the Windows Time Service

## Module 20: Investigating Network Traffic

- § Network Addressing Schemes

- § Tool: Tcpcmdump
- § CommView
- § Softperfect Network Sniffer
- § HTTP Sniffer
- § EtherDetect Packet Sniffer
- § OmniPeek
- § Iris Network Traffic Analyzer
- § SmartSniff
- § NetSetMan Tool
- § Evidence Gathering at the Data-link Layer: DHCP database
- § DHCP Log
- § Siemens Monitoring Center
- § Netresident Tool
- § eTrust Network Forensics
- § IDS Policy Manager <http://www.activeworx.org>

#### Module 21: Investigating Wireless Attacks

- § Association of Wireless AP and Device
- § Search Warrant for Wireless Networks
- § Key Points to Remember
- § Points You Should Not Overlook while Testing the Wireless Network
- § Methods to Access a Wireless Access Point

- o Direct-connect To the Wireless Access Point
- Nmap
- Scanning Wireless Access Points using Nmap
- Rogue Access Point
- o “Sniffing” Traffic Between the Access Point and Associated Devices
- Scanning using Airodump
- MAC Address Information
- Airodump: Points to Note
- § Searching for Additional Devices
- § Forcing Associated Devices to Reconnect
- § Check for MAC Filtering
- o Changing the MAC Address
- § Passive Attack
- § Active Attacks on Wireless Networks
- § Investigating Wireless Attacks

## Module 22: Investigating Web Attacks

- § Types of Web Attacks
- o Cross-Site Scripting (XSS)
- Investigating Cross-Site Scripting (XSS)
- o Cross-Site Request Forgery (CSRF)
- Anatomy of CSRF Attack

- Pen-testing CSRF Validation Fields
- o Code Injection Attack
- Investigating Code Injection Attack
- o Command Injection Attack
- o Parameter Tampering
- o Cookie Poisoning
- Investigating Cookie Poisoning Attack
- o Buffer Overflow/Cookie Snooping
- Investigating Buffer Overflow
- o DMZ Protocol Attack, Zero Day Attack
- § Example of FTP Compromise
- § Acunetix Web Vulnerability Scanner
- o Tools for Locating IP Address: Hide Real IP
- o Tools for Locating IP Address: [www.whatismyip.com](http://www.whatismyip.com)
- o Tools for Locating IP Address: IP Detective Suite
- o Tools for Locating IP Address: Enterprise IP – Address Manager
- § Intrusion Detection
- § CounterStorm-1: Defense against Known, Zero Day and Targeted Attacks

#### Module 23: Router Forensics

- § Routing Information Protocol
- § Hacking Routers

- § Router Attack Topology
- § Recording your Session
- § Router Logs
- § NETGEAR Router Logs
- § Link Logger
- § Sawmill: Linksys Router Log Analyzer
- § Real Time Forensics
- § Router Audit Tool (RAT)

#### Module 24: Investigating DoS Attacks

- § DoS Attacks
- § Types of DoS Attacks
  - o Types of DoS Attacks: Ping of Death Attack
  - o Types of DoS Attacks: Teardrop Attack
  - o Types of DoS Attacks: SYN Flooding
  - o Types of DoS Attacks: Land
  - o Types of DoS Attacks: Smurf
  - o Types of DoS Attacks: Fraggle
  - o Types of DoS Attacks: Snork
  - o Types of DoS Attacks: WINDOWS OUT-OF-BAND (OOB) Attack
- § DDoS Attack
  - o Working of DDoS Attacks (FIG)

- o Classification of DDoS Attack
- § DoS Attack Modes
- § Indications of a DoS/DDoS Attack
- § Techniques to Detect DoS Attack
- o Techniques to Detect DoS Attack: Activity Profiling
- o Sequential Change-Point Detection
- o Wavelet-based Signal Analysis
- § Challenges in the Detection of DoS Attack

#### Module 25: Investigating Internet Crimes

- § Internet Crimes
- § Internet Forensics
- o Why Internet Forensics
- § IP Address
- § Domain Name System (DNS)
- o DNS Record Manipulation
- o DNS Lookup
- § Email Headers
- o Email Headers Forging
- o Tracing Back Spam Mails
- § Switch URL Redirection
- o Sample Javascript for Page-based Redirection

- o Embedded JavaScript
- § Recovering Information from Web Pages
- o Downloading a Single Page or an Entire Web Site
- § Tool: Grab-a-Site
- § Tool: SurfOffline 1.4
- § Tool: My Offline Browser 1.0 [www.newprosoft.com](http://www.newprosoft.com)
- § Tool: WayBack Machine
- § HTTP Headers
- o Viewing Header Information
- § Examining Information in Cookies
- o Viewing Cookies in Firefox
- § Tracing Geographical Location of a URL: [www.centralops.net](http://www.centralops.net)
- o DNS Lookup Result: [centralops.net](http://centralops.net)
- o DNS Lookup Result: [centralops.net](http://centralops.net)
- § NetScanTools Pro
- § Tool: Privoxy <http://www.privoxy.org>

#### Module 26: Tracking E-mails and Investigating E-mail Crimes

- § Client and Server in E-mail
- § E-mail Client
- § E-mail Server
- § Real E-mail System

- § Received: Headers
- § Forging Headers
- § List of Common Headers
- § Exchange Message Tracking Center
- § MailDetective Tool
  - o Forensic ToolKit (FTK)
  - o Tool: E-Mail Detective
  - o Recover My Email for Outlook
  - o Diskinternals – Outlook Recovery
  - o Tool: SpamArrest
  - o Tool: ID Protect - [www.enom.com](http://www.enom.com)
- § U.S. Laws Against Email Crime: CAN-SPAM Act
- § U.S.C. § 2252A
- § U.S.C. § 2252B
- § Email crime law in Washington: RCW 19.190.020

#### Module 27: Investigating Corporate Espionage

- § Introduction to Corporate Espionage
- § Motives behind Corporate Espionage
- § Information that Corporate Spies Seek
- § Corporate Espionage: Insider/Outsider Threat
- § Techniques of Spying

- § Defense Against Corporate Spying
- § Netspionage
- § Investigating Corporate Espionage Cases
- § Employee Monitoring: Activity Monitor
- § Spy Tool: SpyBuddy

## Module 28: Investigating Trademark and Copyright Infringement

- § Characteristics of Trademarks
- § Copyright
- § Copyright Infringement: Plagiarism
  - o Plagiarism Detection Factors
  - o Plagiarism Detection Tool: Copy Protection System (COPS)
  - o Plagiarism Detection Tool: SCAM (Stanford Copy Analysis Mechanism)
  - o Plagiarism Detection Tool: CHECK
  - o Plagiarism Detection Tool: Jplag
  - o Plagiarism Detection Tool: VAST
  - o Plagiarism Detection Tool: SIM
  - o Plagiarism Detection Tool: PLAGUE
  - o Plagiarism Detection Tool: YAP
  - o Plagiarism Detection Tool: SPLaT
  - o Plagiarism Detection Tool: Sherlock
  - o Plagiarism Detection Tool: Urkund

- o Plagiarism Detection Tool: PRAISE
- o Plagiarism Detection Tool: FreestylerIII
- o Plagiarism Detection Tool: SafeAssignment
- § <http://www.ip.com>
- o How it works?
- § Investigating Intellectual Property
- § US Laws for Trademarks and Copyright
- § Indian Laws for Trademarks and Copyright
- § Japanese Laws for Trademarks and Copyright
- § Australia Laws For Trademarks and Copyright
- § UK Laws for Trademarks and Copyright

#### Module 29: Investigating sexually harassment incidents

- § Sexual Harassment - Introduction
- § Types of Sexual Harassment
- § Consequences of Sexual Harassment
- § Responsibilities of Supervisors
- § Responsibilities of Employees
- § Complaint Procedures
- § Investigation Process
- § Sexual Harassment Investigations
- § Sexual Harassment Policy

- § Preventive Steps
- § U.S Laws on Sexual Harassment
- § The Laws on Sexual Harassment: Title VII of the 1964 Civil Rights Act
- § The Laws on Sexual Harassment: The Civil Rights Act of 1991
- § The Laws on Sexual Harassment: Equal Protection Clause of the 14th Amendment
- § The Laws on Sexual Harassment: Common Law Torts
- § The Laws on Sexual Harassment: State and Municipal Laws

### Module 30: Investigating Child Pornography

- § Introduction to Child Pornography
- § People's Motive Behind Child Pornography
- § People Involved in Child Pornography
- § Role of Internet in Promoting Child Pornography
- § Effects of Child Pornography on Children
- § Measures to Prevent Dissemination of Child Pornography
- § Challenges in Controlling Child Pornography
- § Guidelines for Investigating Child Pornography Cases
- § Sources of Digital Evidence
- § Antichildporn.org
  - o How to Report Antichildporn.org about Child Pornography Cases
  - o Report Format of Antichildporn.org
- § Tools to Protect Children from Pornography: Reveal

- o Tool: iProtectYou
- o Child Exploitation Tracking System (CETS)
  - § <http://www.projectsafechildhood.gov/>
  - § Innocent Images National Initiative
  - § Internet Crimes Against Children (ICAC)
  - § Reports on Child Pornography
  - § U.S. Laws against Child Pornography
  - § Australia Laws against Child Pornography
  - § Austria Laws against Child Pornography
  - § Belgium Laws against Child Pornography
  - § Cyprus Laws against Child Pornography
  - § Japan Laws against Child Pornography

#### Module 31: PDA Forensics

- § Features
- § PDA Forensics Steps
  - o Investigative Methods
  - § Tool:
    - o PDA Secure – Forensic Tool
    - o EnCase – Forensic Tool

#### Module 32: iPod Forensics

- § iPod

- o iPod Features
- o iPod as Operating System
  - § Apple HFS+ and FAT32
  - § Application Formats
  - § Misuse of iPod
  - § iPod Investigation
- o Mac Connected iPods
- o Windows Connected iPods
- o Storage
- o Lab Analysis
- o Remove Device From Packaging
  - § Testing Mac Version
  - § Full System Restore as Described in the Users' Manual
  - § Testing Windows Version
  - § User Account
  - § Calendar and Contact Entries
  - § Macintosh Version
  - § EnCase
  - § Deleted Files
  - § Windows Version
  - § Registry Key Containing the iPod's USB/Firewire Serial Number

- § Tool:
- o DiskInternals Music Recovery
- o Recover My iPod: Tool

### Module 33: Blackberry Forensics

- § Blackberry: Introduction
- § BlackBerry Functions
- § BlackBerry as Operating System
- § How BlackBerry (RIM) Works
- § BlackBerry Serial Protocol
- § BlackBerry Security
- § BlackBerry Wireless Security
- o BlackBerry Security for Wireless Data
- o Security for Stored Data
- § Forensics
- § Acquisition
- § Collecting Evidence from Blackberry
- o Collecting Evidence from Blackberry: Gathering Logs
- o Collecting Evidence from Blackberry: Imaging and Profiling
- § Review of Evidence
- § Simulator – Screenshot
- § Blackberry Attacks

- § Protecting Stored Data
- § Data Hiding in BlackBerry
- § BlackBerry Signing Authority Tool

#### Module 34: Investigative Reports

- § Understanding the Importance of Reports
- § Investigating Report Requirements
- § Sample Forensic Report
  - o Sample Report
- § Guidelines for Writing Reports
- § Important Aspects of a Good Report
- § Dos and Don'ts of Forensic Computer Investigations
- § Case Report Writing and Documentation
- § Create a Report to Attach to the Media Analysis Worksheet
- § Investigative Procedures
  - o Collecting Physical and Demonstrative Evidence
  - o Collecting Testimonial Evidence
- § Best Practices for Investigators

#### Module 35: Becoming an Expert Witness

- § What is Expert Witness
- § Types of Expert Witnesses
  - o Computer Forensics Experts

- o Medical & Psychological Experts
- o Civil Litigation Experts
- o Construction & Architecture Experts
- o Criminal Litigation Experts
- § Scope of Expert Witness Testimony
- § Checklists for Processing Evidence
- § Examining Computer Evidence
- o Recognizing Deposing Problems
- § Dealing with Media

© 2002 EC-Council. All rights reserved.

This document is for informational purposes only. EC-Council MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. EC-Council logo is registered trademarks or trademarks of EC-Council in the United States and/or other countries.