

Certification

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

Course Outline v3.0

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
- Type of Computer Crimes
- 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
- 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
- Why You Should Report Cybercrime
- Reporting Computer-related Crimes
- Person Assigned to Report the Crime
- When and How to Report an Incident?
- Who to Contact at the Law Enforcement?
- Federal Local Agents Contact
- More Contacts
- 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
- Policy and Procedure Development
- Evidence Assessment
- Case Assessment
- Processing Location Assessment
- Legal Considerations
- Evidence Assessment
- Evidence Acquisition
- Write Protection
- Acquire the Subject Evidence
- Evidence Examination
- Physical Extraction
- Logical Extraction
- Analysis of Extracted Data
- Timeframe Analysis
- Data Hiding Analysis
- Application and File Analysis
- Ownership and Possession
- 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
- Electronic Devices: Types and Collecting Potential Evidence
- 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
- Ask These Questions When A Client Calls A Forensic Investigator
- Health and Safety Issues
- Consent
- Planning the Search and Seizure
- Initial Search of the Scene
- Witness Signatures
- Conducting Preliminary Interviews
- Initial Interviews
- Documenting Electronic Crime Scene
- Photographing the Scene
- Sketching the Scene
- 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
- Transporting Electronic Evidence
- 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
- Category of Incidents: Low Level
- Category of Incidents: Mid Level
- Category of Incidents: High Level
- CSIRT: Goals and Strategy
- Motivation behind CSIRTs
- Why an Organization needs an Incident Response Team?

- Who works in a CSIRT?
- Staffing your Computer Security Incident Response Team: What are the Basic Skills Needed?
- Team Models
- CSIRT Services can be Grouped into Three Categories:
- CSIRT Case Classification
- Types of Incidents and Level of Support
- Service Description Attributes
- Incident Specific Procedures
- How CSIRT handles Case: Steps
- US-CERT Incident Reporting System
- CSIRT Incident Report Form
- CERT(R) Coordination Center: Incident Reporting Form
- Limits to Effectiveness in CSIRTs
- 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
- Paraben Forensics Hardware: Handheld First Responder Kit
- Paraben Forensics Hardware: Wireless StrongHold Bag
- Paraben Forensics Hardware: Remote Charger
- Paraben Forensics Hardware: Device Seizure Toolbox
- Paraben Forensics Hardware: Wireless StrongHold Tent
- Paraben Forensics Hardware: Passport StrongHold Bag
- Paraben Forensics Hardware: Project-a-Phone

- Paraben Forensics Hardware: SATA Adaptor Male/ Data cable for Nokia 7110/6210/6310/i
- Paraben Forensics Hardware: Lockdown
- Paraben Forensics Hardware: SIM Card Reader/ Sony Clie N & S Series Serial Data Cable
- Paraben Forensics Hardware: USB Serial DB9 Adapter
- Portable Forensic Systems and Towers: Forensic Air-Lite VI MKII laptop
- Portable Forensic Systems and Towers: Original Forensic Tower II
- Portable Forensic Systems and Towers: Portable Forensic Workhorse V
- Portable Forensic Workhorse V: Tableau 335 Forensic Drive Bay Controller
- Portable Forensic Systems and Towers: Forensic Air-Lite IV MK II
- Portable Forensic Systems and Towers: Forensic Tower II
- Forensic Write Protection Devices and Kits: Ultimate Forensic Write Protection Kit
- Tableau T3u Forensic SATA Bridge Write Protection Kit
- 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
- DIBS® Advanced Forensic Workstation
- 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
- Technical Specification of the Laboratory-based Imaging System
- Computer Forensic Labs, Inc
- Procedures at Computer Forensic Labs (CFL), Inc
- Data Destruction Industry Standards

Module 07: Understanding File Systems and Hard Disks

- Types of Hard Disk Interfaces
 - Types of Hard Disk Interfaces: SCSI
 - Types of Hard Disk Interfaces: IDE/EIDE
 - Types of Hard Disk Interfaces: USB
 - Types of Hard Disk Interfaces: ATA
 - Types of Hard Disk Interfaces: Fibre Channel
 - Disk Capacity Calculation
 - Evidor: The Evidence Collector
 - 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
 - DVD-R, DVD+R, and DVD+R(W)
 - DVD-RW, DVD+RW
 - DVD+R DL/ DVD-R DL/ DVD-RAM
 - HD-DVD (High Definition DVD)
 - HD-DVD
 - Blu-Ray
 - CD Vs DVD Vs Blu-Ray

- HD-DVD vs. Blu-Ray
- iPod
- Zune
- Flash Memory Cards
 - Secure Digital (SD) Memory Card
 - Compact Flash (CF) Memory Card
 - Memory Stick (MS) Memory Card
 - Multi Media Memory Card (MMC)
 - xD-Picture Card (xD)
 - SmartMedia Memory (SM) Card
- USB Flash Drives
 - USB Flash in a Pen

Module 09: Windows, Linux and Macintosh Boot Processes

- 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
 - Directory Scan
 - FileSpy
 - HeaderBuilder

- Carbon Copy Cloner (CCC)
- MacDrive6

Module 10: Windows Forensics

- Windows Forensics Tool: Helix
 - Tools Present in Helix CD for Windows Forensics
 - Helix Tool: SecReport
 - Helix Tool: Windows Forensic Toolchest (WFT)
- MD5 Generator: Chaos MD5
 - Secure Hash Signature Generator
 - MD5 Generator: Mat-MD5
 - 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
 - The Sleuth Kit
 - Tools Present in "The Sleuth Kit"
 - Autopsy
 - The Evidence Analysis Techniques in Autopsy
- SMART for Linux
- Penguin Sleuth

- Tools Included in Penguin Sleuth Kit
 - Forensix
 - Maresware
- Major Programs Present in Maresware
 - Captain Nemo
 - 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
- Hardware Tool: LinkMASter-2 Forensic
- 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
- Data Recovery Tools: Forensic Sorter v2.0.1
- Data Recovery Tools: Directory Snoop

- Permanent Deletion of Files: Darik's Boot and Nuke (DBAN)
- File Integrity Checker: FileMon
- File Integrity Checker: File Date Time Extractor (FDTE)
- 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
- Password Recovery Tool: AIM Password Decoder
- Password Recovery Tool: MS Access Database Password Decoder
- Internet History Viewer: CookieView - Cookie Decoder
- Internet History Viewer: Cookie Viewer
- Internet History Viewer: Cache View
- Internet History Viewer: FavURLView - Favourite Viewer
- Internet History Viewer: NetAnalysis
- FTK- Forensic Toolkit
- Email Recovery Tool: E-mail Examiner
- 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
 - Hard Disk Write Protection Tools: Nowrite & Firewire Drivedock
 - LockDown
 - Write Protect Card Reader
 - Drive Lock IDE
 - Serial-ATA DriveLock Kit
 - Wipe MASSter
 - ImageMASSter Solo-3 IT
 - ImageMASSter 4002i
 - ImageMasster 3002SCSI
 - Image MASSter 3004SATA

Module 14: Forensics Investigations Using Encase

- Evidence File
 - 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 Bottom Pane
 - Status Bar
 - Status Bar
- Searching
 - Keywords
 - 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
- NTFS Starting Point
- Viewing Disk Geometry
- Recovering Deleted Partitions
- Hash Values
- Creating Hash Sets
- MD5 Hash
- 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
 - Tool: Search and Recover
 - Tool: Zero Assumption Digital Image Recovery
 - Tool: PC Inspector Smart Recovery
 - Tool: Fundelete
 - Tool: RecoverPlus Pro
 - Tool: OfficeFIX
 - Tool: Recover My Files
 - Tool: Zero Assumption Recovery
 - Tool: SuperFile Recover
 - Tool: IsoBuster
 - Tool: CDRoller
 - Tool: DiskInternals Uneraser
 - Tool: DiskInternal Flash Recovery
 - Tool: DiskInternals NTFS Recovery
 - Recover Lost/Deleted/Corrupted files on CDs and DVDs
 - Tool: Undelete
 - Tool: Active@ UNDELETE
 - Data Recovery Tool: CD Data Rescue
 - Tool: File Recover
 - Tool: WinUndelete
 - Tool: R-Undelete
 - Tool: Image Recall
 - Tool: eIMAGE Recovery
 - Tool: File Scavenger
 - Tool: Recover4all Professional

- Tool: eData Unerase
- Tool: Easy-Undelete
- Tool: InDisk Recovery
- Tool: Repair My Excel
- Tool: Repair Microsoft Word Files
- Tool: Zip Repair
- 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
- Tool: GetDataBack
- Tool: DiskInternals Partition Recovery
- Tool: Active@ Partition Recovery
- Tool: Handy Recovery
- Tool: Acronis Recovery Expert
- Tool: Active Disk Image
- Tool: TestDisk
- Tool: Recover It All!
- Tool: Scaven
- Tool: Partition Table Doctor
- Tool: NTFS Deleted Partition Recovery

Module 16: Image Files Forensics

- Common Terminologies
- Understanding Image File Formats

- GIF (Graphics Interchange Format)
- JPEG (Joint Photographic Experts Group)
- JPEG 2000
- BMP (Bitmap) File
- PNG (Portable Network Graphics)
- Tagged Image File Format (TIFF)
- 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
- Steganalysis Tool: Stegdetect
 - Image File Forensic Tool: GFE Stealth (Graphics File Extractor)
- Tool: ILook v8
- Tool: P2 eXplorer

Module 17: Steganography

- Classification of Steganography
- Steganography vs. Cryptography
- Model of Stegosystem
- Model of Cryptosystem

- Introduction to Stego-Forensics
 - Important Terms in Stego-Forensics
- Steganography vs. Watermarking
 - Attacks on Watermarking
 - Application of Watermarking
 - Digimarc's Digital Watermarking
 - Watermarking – Mosaic Attack
- Mosaic Attack – Javascript code
- 2Mosaic – Watermark breaking Tool
- Steganalysis
 - Steganalysis Methods/Attacks on Steganography
- TEMPSET
- Van Eck phreaking
- Printer Forensics
 - Is Your Printer Spying On You?
 - DocuColor Tracking Dot Decoding
- Steganography Tools
 - Tool: Steganos
 - Steganography Tool: Pretty Good Envelop
 - Tool: Gifshuffle
 - Refugee
 - Tool: JPHIDE and JPSEEK
 - Tool: wbStego
 - Tool: OutGuess
 - Tool: Invisible Secrets 4
 - Tool: Masker
 - Tool: Hydan

- Tool: Cloak
- Tool: StegaNote
- Tool: Stegomagic
- Hermetic Stego
 - Application of Steganography
 - How to Detect Steganography?
- Stego Suite – Steg Detection Tool
- 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
- Tool CmosPwd
- ERD Commander
- Active Password Changer
 - <http://www.virus.org/index.php?>
 - Pdf Password Crackers
 - Password Cracking Tools
- Tool: Cain & Abel
- Tool: LCP
- Tool: SID&User
- Tool: Ophcrack 2
- Tool: John the Ripper
- Tool: DJohn

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

Module 19: Network Forensics and Investigating Logs

- Introduction to Network Forensics
- The Hacking Process
- 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
 - 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
 - Central Logging Design
 - Steps to Implement Central Logging
 - Centralized Syslog Server
 - Syslog-ng: Security Tool
 - IIS Centralized Binary Logging
 - ODBC Logging
 - IISLogger: Development tool
 - Socklog: IDS Log Analysis Tool
 - KiwiSysLog Tool
 - Microsoft Log Parser: Forensic Analysis Tool
 - Firewall Analyzer: Log Analysis Tool

- Adaptive Security Analyzer (ASA) Pro: Log Analysis Tool
- GFI EventsManager
- How does GFI EventsManager work?
- Activeworx Security Center
- EventLog Analyzer
- Why Synchronize Computer Times?
- What is NTP Protocol?
- NTP Stratum Levels
- NIST Time Servers
- Configuring the Windows Time Service

Module 20: Investigating Network Traffic

- Network Addressing Schemes
- Tool: Tcpdump
- 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
- Direct-connect To the Wireless Access Point
- Nmap
- Scanning Wireless Access Points using Nmap
- Rogue Access Point
- “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
- Changing the MAC Address
- Passive Attack
- Active Attacks on Wireless Networks
- Investigating Wireless Attacks

Module 22: Investigating Web Attacks

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

- Pen-testing CSRF Validation Fields
- Code Injection Attack
- Investigating Code Injection Attack
- Command Injection Attack
- Parameter Tampering
- Cookie Poisoning
- Investigating Cookie Poisoning Attack
- Buffer Overflow/Cookie Snooping
- Investigating Buffer Overflow
- DMZ Protocol Attack, Zero Day Attack
- Example of FTP Compromise
- Acunetix Web Vulnerability Scanner
- Tools for Locating IP Address: Hide Real IP
- Tools for Locating IP Address: www.whatismyip.com
- Tools for Locating IP Address: IP Detective Suite
- 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
 - Types of DoS Attacks: Ping of Death Attack
 - Types of DoS Attacks: Teardrop Attack
 - Types of DoS Attacks: SYN Flooding
 - Types of DoS Attacks: Land
 - Types of DoS Attacks: Smurf
 - Types of DoS Attacks: Fraggle
 - Types of DoS Attacks: Snork
 - Types of DoS Attacks: WINDOWS OUT-OF-BAND (OOB) Attack
- DDoS Attack
 - Working of DDoS Attacks (FIG)
 - Classification of DDoS Attack
- DoS Attack Modes
- Indications of a DoS/DDoS Attack
- Techniques to Detect DoS Attack
 - Techniques to Detect DoS Attack: Activity Profiling
 - Sequential Change-Point Detection
 - Wavelet-based Signal Analysis
- Challenges in the Detection of DoS Attack

Module 25: Investigating Internet Crimes

- Internet Crimes
- Internet Forensics
 - Why Internet Forensics

- IP Address
- Domain Name System (DNS)
 - DNS Record Manipulation
 - DNS Lookup
- Email Headers
 - Email Headers Forging
 - Tracing Back Spam Mails
- Switch URL Redirection
 - Sample Javascript for Page-based Redirection
 - Embedded JavaScript
- Recovering Information from Web Pages
 - 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
- Tool: WayBack Machine
- HTTP Headers
 - Viewing Header Information
- Examining Information in Cookies
 - Viewing Cookies in Firefox
- Tracing Geographical Location of a URL: www.centralops.net
 - DNS Lookup Result: [centralops.net](http://www.centralops.net)
 - DNS Lookup Result: [centralops.net](http://www.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
- Forensic ToolKit (FTK)
- Tool: E-Mail Detective
- Recover My Email for Outlook
- Diskinternals – Outlook Recovery
- Tool: SpamArrest
- Tool: ID Protect - 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
 - Plagiarism Detection Factors
 - Plagiarism Detection Tool: Copy Protection System (COPS)
 - Plagiarism Detection Tool: SCAM (Stanford Copy Analysis Mechanism)
 - Plagiarism Detection Tool: CHECK
 - Plagiarism Detection Tool: Jplag
 - Plagiarism Detection Tool: VAST
 - Plagiarism Detection Tool: SIM
 - Plagiarism Detection Tool: PLAGUE
 - Plagiarism Detection Tool: YAP
 - Plagiarism Detection Tool: SPiAT
 - Plagiarism Detection Tool: Sherlock
 - Plagiarism Detection Tool: Urkund
 - Plagiarism Detection Tool: PRAISE
 - Plagiarism Detection Tool: FreestylerIII
 - Plagiarism Detection Tool: SafeAssignment
- <http://www.ip.com>
 - 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
 - How to Report Antichildporn.org about Child Pornography Cases
 - Report Format of Antichildporn.org
- Tools to Protect Children from Pornography: Reveal
 - Tool: iProtectYou
 - Child Exploitation Tracking System (CETS)
 - <http://www.projectsafefchildhood.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
 - Investigative Methods
- Tool:
 - PDA Secure – Forensic Tool
 - EnCase – Forensic Tool

Module 32: iPod Forensics

- iPod

- iPod Features
- iPod as Operating System
 - Apple HFS+ and FAT32
 - Application Formats
 - Misuse of iPod
 - iPod Investigation
- Mac Connected iPods
- Windows Connected iPods
- Storage
- Lab Analysis
- 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:
- DiskInternals Music Recovery
- 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
- BlackBerry Security for Wireless Data
- Security for Stored Data
- Forensics
- Acquisition
- Collecting Evidence from Blackberry
- Collecting Evidence from Blackberry: Gathering Logs
- 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
- 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
- Collecting Physical and Demonstrative Evidence
- Collecting Testimonial Evidence
- Best Practices for Investigators

Module 35: Becoming an Expert Witness

- What is Expert Witness
- Types of Expert Witnesses
- Computer Forensics Experts
- Medical & Psychological Experts
- Civil Litigation Experts
- Construction & Architecture Experts
- Criminal Litigation Experts
- Scope of Expert Witness Testimony
- Checklists for Processing Evidence
- Examining Computer Evidence
- Recognizing Deposing Problems
- Dealing with Media