# Computer Hacking Forensic Investigator

## Training Program

### Course Description

Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud.

The CHFI course will give participants the necessary skills to identify an intruder's footprints and 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.

The CHFI is a very advanced security-training program. Proper preparation is required before conducting the CHFI class.

### 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)**

### Exam Title

Computer Hacking Forensic Investigator v4

## 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.

## Exam Availability Locations

- Prometric Prime
- Prometric APTC
- VUE

## Exam Code

The exam code varies when taken at different testing centers.

- Prometric Prime: 312-49
- Prometric APTC: EC0-349
- VUE: 312-49

## Number of questions

50

## Duration

2 hours

## Passing score

70%

# Course Outline CHFI v4

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

- Forensic Science
- Computer Forensics
  - Security Incident Report
  - 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
  - Cybercrime
  - Computer Facilitated Crimes
  - Modes of Attacks
  - Examples of Cyber Crime
  - Types of Computer Crimes
  - How Serious were Different Types of Incident?
  - Disruptive Incidents to the Business
  - Time Spent Responding to the Security Incident
  - Cost Expenditure Responding to the Security Incident
- Cyber Crime Investigation
  - Cyber Crime Investigation
  - Key Steps in Forensic Investigation
  - Rules of Forensics Investigation
  - Need for Forensic Investigator
  - Role of Forensics Investigator
  - Accessing Computer Forensics 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)

- Legal Issues
- Reporting the Results

**Module 02: Computer Forensics Investigation Process**

- Investigating Computer Crime
  - Before the Investigation
  - Build a Forensics Workstation
  - Building Investigating Team
  - People Involved in Performing Computer Forensics
  - Review Policies and Laws
  - Forensics Laws
  - Notify Decision Makers and Acquire Authorization
  - Risk Assessment
  - Build a Computer Investigation Toolkit
- Computer Forensic Investigation Methodology
  - Steps to Prepare for a Computer Forensic Investigation
  - Obtain Search Warrant
    - Example of Search Warrant
    - Searches Without a Warrant
  - Evaluate and Secure the Scene
    - Forensic Photography
    - Gather the Preliminary Information at Scene
    - First Responder
  - Collect the Evidence
    - Collect Physical Evidence
      - Evidence Collection Form
    - Collect Electronic Evidence
    - Guidelines in Acquiring Evidences
  - Secure the Evidence
    - Evidence Management
    - Chain of Custody
  - Acquire the Data
    - 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
  - Sample Report
- Testify in the Court as an Expert Witness
  - Expert Witness
  - Testifying in the Court Room
  - Closing the Case
  - Maintaining Professional Conduct
  - Investigating a Company Policy Violation
  - Computer Forensics Service Providers

**Module 03: Searching and Seizing of Computers**

- Searching and Seizing Computers without a Warrant
  - Searching and Seizing Computers without a Warrant
  - § 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.2: Exigent Circumstances
  - § B.3: Plain View
  - § B.4: Search Incident to a Lawful Arrest

- § B.5: Inventory Searches
- § B.6: Border Searches
- § B.7: International Issues
- § C: Special Case: Workplace Searches
- § C.1: Private Sector Workplace Searches
- § C.2: Public-Sector Workplace Searches

- Searching and Seizing Computers with a Warrant
  - Searching and Seizing Computers with a Warrant
  - A: 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.2.b: Application of the PPA to Computer Searches and Seizures
  - § A.3: Civil Liability Under the Electronic Communications Privacy Act (ECPA)
  - § A.4: Considering the Need for Multiple Warrants in Network Searches
  - § A.5: No-Knock Warrants
  - § A.6: Sneak-and-Peek Warrants
  - § 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 as Well as the Practical & Legal Considerations That Will Govern the Execution of the Search
  - § 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
- The Electronic Communications Privacy Act
  - § The Electronic Communications Privacy Act
  - § A. Providers of Electronic Communication Service vs. Remote Computing Service
  - § B. Classifying Types of Information Held by Service Providers
  - § C. Compelled Disclosure Under ECPA
  - § D. Voluntary Disclosure

- § E. Working with Network Providers
- Electronic Surveillance in Communications Networks
  - Electronic Surveillance in Communications Networks
  - § A. Content vs. Addressing Information
  - B. The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127
  - C. The Wiretap Statute ("Title III"), 18 U.S.C. §§ 2510-2522
  - § C.1: Exceptions to Title III
  - § D. Remedies For Violations of Title III and the Pen/Trap Statute
- Evidence
  - Evidence
  - § A. Authentication
  - § B. Hearsay
  - § C. Other Issues
  - End Note

**Module 04: Digital Evidence**

- Digital Data
  - 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
  - Anti-Digital Forensics (ADF)
  - Types of Digital Data
  - Rules of Evidence
  - Best Evidence Rule
  - Federal Rules of Evidence
  - International Organization on Computer Evidence (IOCE)
  - http://www.ioce.org/
  - IOCE International Principles for Digital Evidences
  - SWGDE Standards for the Exchange of Digital Evidence
- Electronic Devices: Types and Collecting Potential Evidence
  - Electronic Devices: Types and Collecting Potential Evidence
- Evidence Assessment
  - Digital Evidence Examination Process
  - Evidence Assessment

- Prepare for Evidence Acquisition

- Evidence Acquisition
  - Preparation for Searches
  - Seizing the Evidences
  - Imaging
  - Bit-stream Copies
  - Write Protection
  - Evidence Acquisition
  - Acquiring Evidence from Storage Devices
  - Collecting the Evidence
  - Collecting the Evidence from RAM
  - Collecting Evidence from Stand-Alone Network Computer
  - Chain of Custody
  - Chain of Evidence Form
- Evidence Preservation
  - 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
- Evidence Documentation and Reporting
  - Documenting the Evidence
  - Evidence Examiner Report
  - Final Report of Findings
  - Computer Evidence Worksheet

- Hard Drive Evidence Worksheet
- Removable Media Worksheet

- Electronic Crime and Digital Evidence Consideration by Crime Category

**Module 05: First Responder Procedures**

- Electronic Evidence
- First Responder
- Role of First Responder
- Electronic Devices: Types and Collecting Potential Evidence
- First Responder Toolkit
  - First Responder Toolkit
  - Creating a First Responder Toolkit
  - Evidence Collecting Tools and Equipment
- First Response Basics
  - First Responder 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
  - Securing and Evaluating Electronic Crime Scene: A Check-list
  - Warrant for Search & Seizure
  - Planning the Search & Seizure
  - Initial Search of the Scene
  - Health and Safety Issues
- Conducting Preliminary Interviews
  - Questions to ask When Client Calls the Forensic Investigator
  - Consent
  - Sample of Consent Search Form
  - Witness Signatures
  - Conducting Preliminary Interviews
  - Conducting Initial Interviews
  - Witness Statement Checklist
- Documenting Electronic Crime Scene
  - Documenting Electronic Crime Scene
  - Photographing the Scene

- Sketching the Scene
- Collecting and Preserving Electronic Evidence
  - Collecting and Preserving Electronic Evidence
  - Order of Volatility
  - Dealing with Powered OFF Computers at Seizure Time
  - Dealing with Powered ON Computers at Seizure Time
  - Dealing with Networked Computer
  - Dealing with Open Files and Startup Files
  - Operating System Shutdown Procedure
  - Computers and Servers
  - Preserving Electronic Evidence
  - Seizing Portable Computers
  - Switched ON Portables
- Packaging and Transporting Electronic Evidence
  - Evidence Bag Contents List
  - Packaging Electronic Evidence
  - Exhibit Numbering
  - Transporting Electronic Evidence
  - Handling and Transportation to the Forensics Laboratory
  - Storing Electronic Evidence
  - Chain of Custody
- Reporting the Crime Scene
- Note Taking Checklist
- First Responder Common Mistakes

**Module 06: 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

- Incident Management
- Threat Analysis and Assessment
- Vulnerability Analysis
- Estimating Cost of an Incident
- Change Control

- Incident Reporting
  - Incident Reporting
  - Computer Incident Reporting
  - Whom to Report an Incident?
  - Report a Privacy or Security Violation
  - Preliminary Information Security Incident Reporting Form
  - Why don't Organizations Report Computer Crimes?
- Incident Response
  - Respond to a Security Incident
  - Security Incident Response (Detailed Form)
  - Incident response policies
  - Incident Response Checklist
  - Response Handling Roles
  - Incident Response: Roles and Responsibilities
    - SSM
    - ISSM
    - ISSO
  - Contingency/Continuity of Operations Planning
  - Budget/Resource Allocation
- Incident Handling
  - Handling Incidents
  - Procedure for Handling Incident
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Follow-up
  - Post-Incident Activity
  - Education, Training, and Awareness
  - Post Incident Report
  - Procedural and Technical Countermeasures

- Vulnerability Resources

- CSIRT
  - What is CSIRT?
  - CSIRT: Goals and Strategy
  - CSIRT Vision
  - Motivation behind CSIRTs
  - Why does an Organization need an Incident Response Team?
  - Who works in a CSIRT?
  - 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
  - US-CERT Incident Reporting System
  - CSIRT Incident Report Form
  - CERT(R) Coordination Center: Incident Reporting Form
  - Example of CSIRT
  - Best Practices for Creating a CSIRT
    - Step 1: Obtain Management Support and Buy-in
    - Step 2: Determine the CSIRT Development Strategic Plan
    - Step 3: Gather Relevant Information
    - Step 4: Design your CSIRT Vision
    - Step 5: Communicate the CSIRT Vision
    - Step 6: Begin CSIRT Implementation
    - Step 7: Announce the CSIRT
  - Limits to Effectiveness in CSIRTs
  - Working Smarter by Investing in Automated Response Capability

- World CERTs
  - World CERTs
  - Australia CERT (AUSCERT)
  - Hong Kong CERT (HKCERT/CC)

- Indonesian CSIRT (ID-CERT)
- Japan CERT-CC (JPCERT/CC)
- Singapore CERT (SingCERT)
- Taiwan CERT (TWCERT)
- China CERT (CNCERT/CC)
- CERT-CC
- US-CERT
- Canadian Cert
- Forum of Incident Response and Security Teams
- CAIS
- NIC BR Security Office Brazilian CERT
- EuroCERT
- FUNET CERT
- DFN-CERT
- JANET-CERT
- http://www.first.org/about/organization/teams/
- http://www.apcert.org/about/structure/members.html
- IRTs Around the World

**Module 07: Computer Forensics Lab**

- Setting a Computer Forensics Lab
  - Computer Forensics Lab
  - 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 Forensics Lab
  - Ambience of a Forensic Lab
  - Ambience of a Forensic Lab: Ergonomics
  - Physical Security Recommendations
  - Fire-Suppression Systems
  - Evidence Locker Recommendations
  - Computer Forensics Investigator
  - Law Enforcement Officer

- Forensic Lab Licensing Requisite
- Features of the Laboratory Imaging System
- Technical Specification of the Laboratory-based Imaging System
- Forensics Lab
- Auditing a Computer Forensics Lab
- Recommendations to Avoid Eyestrain
- Computer Forensic Labs, Inc
- Procedures at Computer Forensic Labs (CFL), Inc
- Data Destruction Industry Standards
- Case Study: San Diego Regional Computer Forensics Laboratory (RCFL)

- Hardware Requirements
  - Equipment Required in a Forensics Lab
  - Forensic Workstations
  - Basic Workstation Requirements in a Forensic Lab
  - Stocking the Hardware Peripherals
    - Paraben Forensics Hardware
      - Handheld First Responder Kit
      - Wireless StrongHold Bag
      - Remote Charger
      - Device Seizure Toolbox
      - Wireless StrongHold Tent
      - Passport StrongHold Bag
      - Project-a-Phone
      - SATA Adaptor Male/ Data cable for Nokia 7110/6210/6310/i
      - Lockdown
      - SIM Card Reader/ Sony Client N & S Series Serial Data Cable
      - CSI Stick
      - Portable 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
- Tableau TACC 1441 Hardware Accleerator
- Multiple TACC1441 Units
- Digital Intelligence Forensic Hardware
  - FRED SR (Dual Xeon)
  - FRED-L
  - Forensic Recovery of Evidence Data Center (FREDC)
  - Rack-A-TACC
  - FREDDIE
  - UltraKit
  - UltraBay
  - UltraBlock
  - Micro Forensic Recovery of Evidence Device (µFRED)
- Wiebetech
  - Forensics DriveDock
  - Forensics UltraDock v4
  - Drive eRazer
  - v4 Combo Adapters
  - ProSATA SS8
  - HotPlug
- CelleBrite UFED System
- DeepSpar:
  - Disk Imager Forensic Edition
  - 3D Data Recovery
  - Phase 1 Tool: PC-3000 Drive Restoration system:
  - Phase 2 Tool: DeepSpar Disk Imager
  - Phase 3 Tool: PC-3000 Data Extractor
- InfinaDyne Forensic Products
  - Robotic Loader Extension for CD/DVD Inspector
  - Rimage Evidence Disc System
- CD DVD Forensic Disc Analyzer with Robotic Disc Loader
- Image MASSter
  - RoadMASSter- 3
  - Image MASSter --Solo-3 Forensic
  - Image MASSter –WipeMASSter

- Image MASSter –DriveLock
- Image MASSter: Serial-ATA DriveLock Kit USB/1394B
- Image MASSter: DriveLock Firewire/USB
- Image MASSter: DriveLock IDE
- Image MASSter: DriveLock In Bay

o Logicube:

- Forensic MD5
- Forensic Talon ®
- RAID I/O Adapter ™
- GPStamp™
- Portable Forensic Lab™
- CellDEK ®
- Omniport
- Desktop write PROtects
- USB adapters
- Adapters
- Cables

o Power Supplies and Switches
o DIBS Mobile Forensic Workstation
o DIBS Advanced Forensic Workstation
o DIBS® RAID: Rapid Action Imaging Device
o Forensic Archive and Restore Robotic Devices: Forensic Archive and Restore (FAR Pro)

▪ Software Requirements

o Basic Software Requirements in a Forensic Lab
o Maintain Operating System and Application Inventories
o Paraben Forensics Software: Device Seizure
o Paraben Hard Drive Forensics: P2 Commander
o Crucial Vision
o Paraben Hard Drive Forensics: P2 eXplorer
o InfinaDyne Forensic Products

- CD/DVD Inspector
- AccuBurn-R for CD/DVD Inspector
- Flash Retriever Forensic Edition
- ThumbsDisplay

o TEEL Technologies SIM Tools

- SIMIS

- SIMulate
- SIMgen

- LiveDiscover™ Forensic Edition
- Tools: LiveWire Investigator

**Module 08: Understanding Hard Disks and File Systems**

- Hard Disk
  - Disk Drive Overview
  - 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
    - Types of Hard Disk Interfaces: USB
    - Types of Hard Disk Interfaces: ATA
    - Types of Hard Disk Interfaces: Fibre Channel
  - Disk Platter
  - Tracks
  - Tracks Numbering
  - Sector
  - Sector Addressing
  - Cluster
    - Cluster Size
    - Slack Space
    - Lost Clusters
    - Bad Sector
    - Disk Capacity Calculation
    - Measuring the Performance of Hard Disk
- Disk Partitions
  - Disk Partitions
  - Master Boot Record
- Boot Process
  - Windows XP System Files
  - Windows Boot Process (XP/2003)
  - http://www.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
- NTFS
  - 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
  - NTFS Data Stream
  - NTFS Compressed Files
  - NTFS Encrypted File Systems (EFS)
  - EFS File Structure
  - EFS Recovery Key Agent
  - EFS Key
  - Deleting NTFS Files
  - Registry Data
  - Examining Registry Data
  - FAT vs. NTFS
- Ext3
  - Ext2
  - Ext3

- HFS and CDFS
  - HFS
  - CDFS
- RAID Storage System
  - RAID Storage System
  - RAID Levels
  - Recover Data from Unallocated Space using File Carving Process
- Hard Disk Evidence Collector Tools
  - Evidor
  - WinHex
  - Logicube: Echo PLUS
  - Logicube: Sonix
  - Logicube: OmniClone Xi
  - Logicube: OmniWipe
  - Logicube: CloneCard Pro
  - ImageMASSter: ImageMASSter 40008i
  - eDR Solutions: Hard Disk Crusher

**Module 09: Digital Media Devices**

- Digital Storage 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
  - 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

- 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 drives
- Tape Libraries and Autoloaders
- Barracuda Hard Drives
- Hybrid Hard Drive
- Holographic Data Storage
- ExpressCard
- USB Flash Drives
- USB Flash in a Pen
- 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 Mini Digital Cameras
  - Different Types of Digital Video Cameras
  - Different Types of Mobile Devices
  - Mobile Devices in the Future
  - Different Types of Digital Audio Players
  - Different Types of Digital Video Players
  - Different Types of Laptop computers
  - Solar Powered Concept for Laptop Gadget
  - Different Types of Bluetooth Devices
  - Different Types of USB Drives

**Module 10: CD/DVD Forensics**

- Compact Disk
- Types of CDs
- Digital Versatile Disk (DVD)
- DVD-R and DVD+R
- DVD-RW and DVD+RW
- DVD+R DL, DVD-R DL, DVD-RAM
- HD-DVD (High Definition DVD)

- HD-DVD
- Blu-Ray
- SID Code
- How Criminal uses CD/DVD for Crime
- Pre-Requisite for CD/DVD Forensics
- Steps for CD Forensics
  - Collect the CD/DVD Evidences
  - Precautions while Collecting the Evidences
  - Document the Scene
  - Preserve the Evidences
  - Create Image of 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
  - UltraISO
  - MagicISO
  - Cdmage
  - Alcohol
  - Nero
- CD/DVD Data Recovery Tools
  - CDRoller
  - Badcopy Pro
  - Multi Data Rescue
  - InDisk Recovery
  - Stellar Phoenix -CD Data Recovery Software
  - CD Recovery Toolbox
  - IsoBuster
  - CD/DVD Inspector
  - Acodisc CD & DVD Data Recovery Services

### Module 11: 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 XP Boot Process
- Linux Boot Process
  - Common Startup Files in UNIX
  - List of Important Directories in UNIX
- Linux Boot Process Steps
  - Step 1: The Boot Manager
    - GRUB: Boot Loader
  - Step 2: init
    - Step 2.1: /etc/inittab
    - Run Levels
    - The Run Level Scripts
    - How Processes in Runlevels Start
    - The 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
  - Mac OS X Boot Options
  - The Mac OS X Boot Process

**Module 12: Windows Forensics I**

- Volatile Information
- Non-volatile Information
- Collecting Volatile Information
  - System Time
  - Logged-on-Users
  - Open Files
  - Net file Command
  - Psfile Tool
  - Openfiles Command

- NetBIOS Name Table Cache
- Network Connections
- Netstat with the –ano Switch

- Netstat with the –r Switch
  - Process Information
  - Tlist Tool
  - Tasklist Command
  - Pslist Tool
  - Listdlls Tool
  - Handle Tool
  - Process-to-Port Mapping
  - Netstat Command
  - Fport Tool
  - Openports Tool
  - Network Status
  - Ipconfig Command
  - Promiscdetect Tool
  - Promqry Tool
  - Other Important Information
- Collecting Nonvolatile Information
  - Collecting Nonvolatile Information
  - Examining File Systems
  - Registry Settings
  - Microsoft Security ID
  - Event Logs
  - Index.dat File
  - Devices and Other Information
  - Slack Space
  - Virtual Memory
  - Tool: DriveSpy
  - Swap File
  - Windows Search Index
  - Tool: Search Index Examiner
  - Collecting Hidden Partition Information
  - Hidden ADS Streams
  - Investigating ADS Streams
- Windows Memory Analysis

- Windows Memory Analysis
- Importance of Memory Dump
- EProcess Structure
- Process Creation Mechanism
- Parsing Memory Contents
- Parsing Process Memory
- Extracting the Process Image
- Collecting Process Memory

- Windows Registry Analysis
  - Inside the Registry
  - Registry Contents
  - Registry Structure within a Hive File
  - Registry Analysis
  - System Information
  - Time Zone Information
  - Shares
  - Audit Policy
  - Wireless SSIDs
  - Autostart Locations
  - 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
  - Determining the Startup Locations
- Cache, Cookie and History Analysis
  - Cache, Cookie and History Analysis in IE
  - Cache, Cookie and History Analysis in Firefox/Netscape
  - Browsing Analysis Tool: Pasco

- IE Cache View
- Forensic Tool: Cache Monitor
- Tool - IE History Viewer
- IE Cookie Analysis
- Investigating Internet Traces
- Tool – IECookiesView
- Tool- IE Sniffer

- MD5 Calculation
  - MD5 Calculation
  - MD5 Algorithm
  - MD5 Pseudocode
  - MD5 Generator: Chaos MD5
  - Secure Hash Signature Generator
  - MD5 Generator: Mat-MD5
  - MD5 Checksum Verifier 2.1
- 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 System
  - Viewing Metadata
  - MetaViewer
  - Metadata Analyzer
  - iScrub

**Module 13: Windows Forensics II**

- Text Based Log
  - Understanding Events
  - Event Record Structure
  - Vista Event Logs
  - IIS Logs
  - Parsing IIS Logs
  - Parsing FTP Logs
  - Parsing DHCP Server Logs
  - Parsing Windows Firewall Logs
  - Using the Microsoft Log Parser
- Other Audit Events
  - Evaluating Account Management Events
  - Examining Audit Policy Change Events
  - Examining System Log Entries
  - Examining Application Log Entries
- Forensic Analysis of Event Logs
  - 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
- Forensics Tools
  - Helix
  - Tools Present in Helix CD for Windows Forensics

- Helix Tool: SecReport
- Helix Tool: Windows Forensic Toolchest (WFT)
- Built-in Tool: Sigverif
- Word Extractor
- Registry Viewer Tool: RegScanner
- Pmdump
- System Scanner
- Integrated Windows Forensics Software: X-Ways Forensics
- Tool - Traces Viewer
- Traces Viewer: Images
- Traces Viewer: Pages
- Traces Viewer: Other
- Traces Viewer: Cookies
- CD-ROM Bootable Windows XP
- Ultimate Boot CD-ROM
- List of Tools in UB CD-ROM

**Module 14: Linux Forensics**

- Introduction to Linux
  - Introduction of Linux OS
  - Linux Boot Sequence
  - File System in Linux
  - File System Description
  - 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
  - dd command options
  - Floppy Disk Analysis
  - Hard Disk Analysis
- Data Collection
  - Forensic Toolkit Preparation
  - Data Collection using the Toolkit
  - Keyword Searching

- Linux Crash Utility
- Linux Crash Utility: Commands
  - Crash> ps
  - crash> ps -t
  - crash> ps –a
  - crash> foreach files
  - crash> foreach net

- Case Examples
  - Case Example I
    - Step-by-Step Approach to Case
    - Challenges In Disk Forensics With Linux
  - Case Example II
    - Jason Smith Case
    - Step-by-Step Approach to Case
- Linux Forensics Tools
  - Popular Linux Forensics Tools
    - The Sleuth Kit
    - Tools in “The Sleuth Kit”
  - Autopsy
    - The Evidence Analysis Techniques in Autopsy
      - File Listing
      - File Content
      - Hash Databases
      - File Type Sorting
      - Timeline of File Activity
      - Keyword Search
      - Meta Data Analysis
      - Data Unit Analysis
      - Image Details
- SMART for Linux
  - Features of SMART for Linux
- Penguin Sleuth
  - Tools Included in Penguin Sleuth Kit
- THE FARMAER’S BOOT CD
  - Delve
- Forensix
- Maresware

- Major Programs Present in Maresware
- Captain Nemo
- The Coroner's Toolkit (TCT)
- Tool: FLAG
- Tool: Md5deep
- Tool: TestDisk
- Tool: Vinetto

**Module 15: Mac Forensics**

- Mac OS and File Systems
  - 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
- Mac Forensics: Collecting Evidence
  - Pre-requisites for Mac Forensics
  - Obtaining System Date and Time
  - Single User Mode
  - Determining and Resetting Open Firmware Password
  - Checking Plist Files
  - Collect User Home Directory Information
  - Forensics Information in User Library Folder
  - Collect User Accounts Information
  - User IDs
  - Gather user information from pllist files
  - Use Spotlight for Keyword Search
  - Collecting Information Regarding Parental Controls for Local Account
  - File Vault and Mac OS X Security
  - Cracking File Vault
  - POSIX Permissions
    - Viewing POSIX Permissions
  - Viewing ACL Permissions

- Mac OS X Log Files
- Locating iChat Configuration File
- Viewing iChat Logs
- Gathering Safari Information
- Checking Wi-Fi Support
- Checking Bluetooth Support
- Vulnerable Features of Mac

- Mac Forensics: Imaging
  - 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
- Mac Forensics: Tools
  - gpart
  - MadLockPick
  - File Juicer
  - MacAnalysis
  - MacQuisition
  - FTK Imager
  - dd_rescue
  - md5deep
  - Foremost
  - Mac forensic lab
  - LinkMASSter

**Module 16: Data Acquisition and Duplication**

- Data Acquisition
  - Data Acquisition
  - 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
    - dd command
    - Extracting the MBR
    - Netcat Command
    - dd command(Windows XP Version)
    - Mount Image Pro
    - Snapshot Tool
  - Snapback DatArrest
    - Data Acquisition Toolbox
    - Data Acquisition Tool: SafeBack
  - Hardware Tool: Image MASSter Solo-3 Forensic
    - Image MASSter --RoadMASSter- 3
    - Image MASSter --WipeMASSter
    - Image MASSter –DriveLock
  - Hardware Tool: LinkMASSter-2
  - Hardware Tool: RoadMASSter-2
  - Logicube: ECHOPLUS & Sonix
  - Logicube: OmniClone Xi series
  - Logicube: OmniPORT
  - Logicube: OmniWipe & Clone Card Pro
  - Logicube: Forensic MD5
  - Logicube: Forensic Talon
  - Logicube: RAID I/O Adapter
  - Logicube: GPStamp
  - Logicube: Portable Forensic Lab
  - Logicube: CellDEK
  - Logicube: Desktop write PROtects
  - Logicube: USB adapter
  - Logicube: Adapters

- Logicube: Cables

- Data Duplication Tools
  - Data Duplication Tool: R-drive Image
  - Data Duplication Tool: DriveLook
  - Data Duplication Tool: DiskExplorer
  - Save-N-Sync
  - Hardware Tool: ImageMASSter 6007SAS
    - Hardware Tool: Disk Jockey IT
  - SCSIPAK
  - IBM DFSMSdss
  - Tape Duplication System: QuickCopy
  - 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
  - Athena Archiver

**Module 17: Recovering Deleted Files and Deleted 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
    - Tool: e2Undel
    - Tool: R-linux
    - Tool: O&O Unerase

- Tool: Restorer 2000
- Tool: Badcopy Pro
- Tool: File Scavenger
- Tool: Mycroft V3
- Tool: PC ParaChute
- Tool: Stellar Phoenix
- Tool: Filesaver
- Tool: Virtual Lab
- Tool: Drive and Data Recovery
- Tool: Active@ UNERASER - DATA Recovery
- Tool: Restoration
- Tool: PC Inspector File 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: Recover4all Professional
- Tool: eData Unerase

- Tool: Easy-Undelete
- InDisc Recovery
- TOKIWA DataRecovery
- Data Recovery Wizard Professional
- CD Recovery Toolbox
- Smart Protector-Internet Eraser
- Active@ File Recovery
- SoftPerfect File Recovery
- Partition Recovery
- FinalRecovery
- Mutilate File Wiper
- Repair My Excel
- Repair Microsoft Word Files
- Zip Repair
- Canon RAW File Recovery Software

▪ Recovering Deleted Partitions
  - o Deletion of Partition
  - o Deletion of Partition using Windows
  - o Deletion of Partition using Command Line
  - o Recovery of Deleted Partition
  - o Recovering Deleted Partition Tools
    - GetDataBack
    - DiskInternals Partition Recovery
    - Active@ Partition Recovery
    - Handy Recovery
    - Acronis Recovery Expert
    - Active@ Disk Image
    - TestDisk
    - Recover It All!
    - Scaven
    - Partition Table Doctor
    - NTFS Deleted Partition Recovery
    - Flash Retriever Forensic
    - ThumbsDisplay

- Forensic Toolkit (FTK®)
- Features of FKT
- Installation of FTK
  - 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
- Starting with FTK
  - Starting FTK
  - 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
  - Overview Tab
  - Email Tab
  - Graphics Tab
  - Thumbnails Pane
  - Bookmarks Tab
  - Live Search Tab
  - Index Search Tab
  - Creating Tabs
  - Launching FKT
- Working with FTK
  - Creating A Case

- 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
- 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
  - Data carving
  - Data Carving Files In An Existing Case
- Using Filters
  - Creating A Filter
  - Refining A Filter
  - Deleting A Filter
- Decrypting Encrypted Files
  - Decrypting Files And Folders
  - Viewing Decrypted Files
  - Decrypting Domain Account EFS Files
  - Decrypting Credant Files
  - Decrypting Safeguard Utimaco Files
- Working with Reports
- Creating A Report
  - Saving Settings
  - Entering Basic Case Information
  - Including Bookmarks
  - Including Graphics
  - Selecting a File Path List
  - Selecting a File Properties List
  - Registry Selections
  - Selecting the Report Location
  - HTML Case Report
  - PDF Report
- Customizing the Interface
  - Creating Custom Tabs
  - Customizing File List Columns
  - Creating and Modifying Column Settings

**Module 19: Forensics Investigations Using Encase**

- Evidence File
- Verifying Evidence Files
- Evidence File Format
- Verifying File Integrity

- Hashing
- Acquiring Image
- Configuring EnCase
- View Menu
- Device Tab
- Viewing Files and Folders
- Bottom Pane
- Viewers in Bottom Pane
- 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 (MBR)
- 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 and Folders

- Email Recovery
- Reporting
- IE Cache Images

**Module 20: Steganography**

- Steganography
- Model of Stegosystem
- 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
    - Process of Hiding Information in Image Files
    - 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

- Levels of Visibility
- Robustness vs. Payload
- File Format Dependence

- Cryptography
- Model of Crypto System
- Steganography vs. Cryptography
- Public Key Infrastructure (PKI)
- Key Management Protocols
- Watermarking
  - What is Watermarking?
  - Case Study
  - Steganography vs. Watermarking
  - Types of Watermarks
    - Visible Watermarks
    - Invisible Watermarks
  - Working of Different Watermarks
  - Attacks on Watermarking
  - Application of Watermarking
  - Currency Watermarking
  - Digimarc's Digital Watermarking
  - Watermarking – Mosaic Attack
    - Mosaic Attack – Javascript code
    - 2Mosaic – Watermark breaking Tool
- Steganography Detection
  - How to Detect Steganography?
  - Detecting Steganography
  - Detecting Text, Image, Audio and Video Steganography
  - Counterfeit Detection
- Steganalysis
  - Steganalysis Methods/Attacks on Steganography
    - Attack Types
    - Stego Only Attack
    - Known Cover Attack
    - Known Message Attack
    - Known Stego Attack
    - Chosen Stego Attack
    - Disabling or Active Attack

- Chosen Message Attack
- Disabling or Active Attacks
- Blur
- Noise
- Noise Reduction
- Sharpen
- Rotate
- Resample
- Soften

- Introduction to Stego-Forensics
- Steganography in the Future
- Hiding Information in DNA
- Unethical Use of Steganography
- TEMPEST
- Emissions Security (EMSEC)
- Van Eck phreaking
- Legal Use of Steganography
- Steganography Tools
  - S- Tools
  - Steghide
  - Mp3Stego
  - Invisible Secrets 4
  - Stegdetect
  - Steg Suite
  - Stego Watch
  - Snow
  - Fort Knox
  - Image Hide
  - Blindside
  - Camera/Shy
  - Gifshuffle
  - Data Stash
  - JPHIDE and JPSEEK
  - wbStego
  - OutGuess
  - Masker
  - Cloak

- StegaNote
- Stegomagic
- Hermetic Stego
- StegSpy
- Stealth
- WNSTORM
- Xidie
- CryptArkan
- Info Stego
- Scramdisk
- Jpegx
- CryptoBola
- ByteShelter I
- Camuflage
- Stego Analyst
- Steganos
- Pretty Good Envelop
- Hydan
- EzStego
- Steganosaurus
- appendX
- Stego Break
- Stego Hunter
- StegParty
- InPlainView
- Z-File
- MandelSteg and GIFExtract

**Module 21: Image Files 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
- BMP File Structure
- PNG (Portable Network Graphics)
- Tagged Image File Format (TIFF)
- TIFF File Structure
- ZIP (Zone Information Protocol)

o Best Practices for Forensic Image Analysis

- Use MATLAB for Forensic Image Processing
  - o Advantages of MATLAB
- Data Compression
  - o How File Compression Works?
  - o Understanding Data Compression
  - o Huffman Coding Algorithm
  - o Lempel-Ziv Coding Algorithm
  - o Lossy Compression
  - o Vector Quantization
- Locating and Recovering Image Files
  - o Locating and Recovering Image Files
  - o Analyzing Image File Headers
  - o Repairing Damaged Headers
  - o Reconstructing File Fragments
  - o Identifying Unknown File Formats
  - o Identifying Image File Fragments
    - http://www.filext.com
    - Picture Viewer: Ifran View
    - Picture Viewer: ACDsee
    - Picture Viewer: Thumbsplus
    - Picture Viewer: AD
    - Picture Viewer: Max
    - FastStone Image Viewer
    - XnView
    - Faces – Sketch Software
- Digital Camera Data Discovery Software: FILE HOUND

- http://vectormagic.com/
- Steganography in Image Files
- Steganalysis Tool
  - Hex Workshop
  - S-tools
  - Stegdetect
- Image File Forensic Tools
  - GFE Stealth (Graphics File Extractor)
  - ILook v8
  - P2 eXplorer
  - VisionStage
  - Digital Pictures Recovery
- Identifying Copyright Issues on Graphics
- Case Study

**Module 22: Audio file forensics**

- Audio Forensics
- Why audio forensics
- Use of voice as a tool
- Fast Fourier Transform (FFT)
- Methodologies of Audio Forensics
- Voice Identification
- Audibility Analysis
- Audio Enhancement
- Authenticity Analysis
- Sound Identification
- Event Sequence Analysis
- Dialogue decoding
- Remnant Signal Analysis
- Integrity Verification of the Audio
- Audio Forensics Process
  - Evidence handling
  - Preparation of Exemplars
  - Preparation of Copies
  - Preliminary Examination
  - Analog to Digital Conversion
    - Audio File Formats

- Preparation of Spectrograms
- 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
    - Console
    - Declick
    - Decrackle
    - DEHISS2
    - NR-3 v2
    - Phase Corrector
    - EQ and dynamics
    - Spectral analyzer
  - Audio File Forensic Tools
    - DCVST
    - Advanced audio corrector
    - Acoustica
    - Smaart
    - DNS1500 Dialogue Noise Suppressor
    - DNS2000 Dialogue Noise Suppressor
    - DNS 3000Dialogue Noise Suppressor
    - M-Audio MicroTrack 2496 Portable Digital Recorder
    - Cardinal
    - JBR 4 Channel Microcassette Playback/Transcriber Unit
    - JBR Universal DVD/CD Player/Transcriber Unit

**Module 23: Video File Forensics**

- Video File Forensics
- Crimes involving Video Files
- Need of Video File Forensics
- Video File Formats
- Pre-Requisite for Video Forensics

- Selecting Video Forensics Tools
- Precaution During Video File Forensics
- Preparing for Video Forensics
- Video Forensic Methodology
  - Frame Averaging
  - Video De-Multiplexing
  - De-multiplexing Tool: Video Active
  - dPlex Pro: De-multiplexing Tool
  - Video Stabilizing
  - Motion Deblurring
  - Magnifying and Color Correcting Video
  - Spotlighting the Particular Region
  - Audio Analysis
  - Performing Video Steganalysis
- StegSecret
- UQLIPS: Near Duplicate Video Clip Detection System
- Analysis of Output
- Video Forensics Tools
  - dTective
  - VideoFOCUS
  - Sarensix Video Forensic Services
  - Audio Video Forensic Lab (AVFL)
  - VideoDetective
  - Jam
  - Ikena Reveal

**Module 24: Application Password Crackers**

- Password - Terminology
- What is a Password Cracker?
- How Does a Password Cracker Work?
- 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
    - System Level Password Cracking
    - CMOS Level Password Cracking
        - Tool: Cmospwd
        - ERD Commander
        - Active Password Changer
    - Application Software Password Cracker
    - Distributed Network Attack
    - Passware Kit
    - Accent Keyword Extractor
    - Advanced Zip Password Recovery
- Default Password Database
    - http://phenoelit.darklab.org/
    - http://www.defaultpassword.com/
    - http://www.cirt.net/cgi-bin/passwd.pl
    - http://www.virus.org/index.php?
- Pdf Password Crackers
- Password Cracking Tools
    - Cain & Abel
    - LCP
    - SID&User
    - Ophcrack 2
    - John the Ripper
    - Netscapass
    - Access PassView
    - RockXP
    - Magical Jelly Bean Keyfinder
    - PstPassword
    - Protected Storage PassView
    - Network Password Recovery
    - Mail PassView
    - Asterisk Key
    - Messenger Key
    - MessenPass
    - Password Spectator
    - SniffPass

- Asterisk Logger
- Dialupass
- Mail Password Recovery
- Database Password Sleuth
- CHAOS Generator
- PicoZip Recovery
- Crack
- Brutus
- Distributed John

- Common Recommendations for Improving Password Security
- Standard Password Advice

**Module 25: Log Capturing and Event Correlation**

- Computer Security Logs
  - Computer Security Logs
  - Operating System Logs
  - Application Logs
  - Software Security Logs
  - Router Log Files
  - Honeypot Logs
  - Linux Process Accounting
  - Logon Event in Window
  - Windows Log File
  - Configuring Windows Logging
  - Analyzing Window Log
  - Setting up Remote Logging in Windows
  - Windows Log File: System Logs
  - Windows Log File: Application Logs
  - Log on Events That Appear in the Security Event Log
  - IIS Logs
  - Maintaining Credible IIS Log Files
  - Log File Accuracy
  - Log Everything
  - Keeping Time
  - UTC Time
  - View the DHCP Logs
  - DHCP Logs

- ODBC Logging

- Logs and Legal Issues
  - Legality of Using Logs
  - Records of Regularly Conducted Activity as Evidence
  - Laws and Regulations
- Log Management
  - Log Management
  - Functions of Log Management
  - Challenges in Log Management
- Centralized Logging and Syslogs
  - Central Logging Design
  - Steps to Implement Central Logging
  - Syslog
  - Syslog in Unix-like Systems
  - Steps to Set Up Syslog Server for Unix Systems
  - Centralized Syslog Server
  - IIS Centralized Binary Logging
  - Extended Logging in IIS Server
- Time Synchronization
  - Why Synchronize Computer Times?
  - What is NTP Protocol?
  - NTP Stratum Levels
  - NIST Time Servers
  - Configuring the Windows Time Service
- Event Correlation
  - Event Correlation
  - Types of Event Correlation
  - Prerequisites for Event Correlation
  - Event Correlation Approaches
- Log Capturing and Analysis Tools
  - Syslog-ng Logging System
  - WinSyslog Syslog Server
  - Kiwi Syslog Server
  - Tenable Security Center
  - IISLoger: Development tool
  - Socklog: IDS Log Analysis Tool
  - Microsoft Log Parser: Forensic Analysis Tool

- Firewall Analyzer: Log Analysis Tool
- Adaptive Security Analyzer (ASA) Pro
- GFI EventsManager
- How does GFI EventsManager work?
- Activeworx Security Center
- Ntsyslog
- EventReporter
- EventLog Analyzer
- FLAG – Forensic and Log Analysis GUI
- Simple Event Correlator (SEC)

**Module 26: Network Forensics and Investigating Logs**

- Introduction to Network Forensics
- Intrusion Process
- Network Vulnerabilities
- Network Attacks
- Looking 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
  - Time Stamp Injection Attack
  - Defending Time Stamp Injection Attack
  - Word Wrap Abuse Attack
  - Defending Word Wrap Abuse Attack
  - HTML Injection Attack

- Defending HTML Injection Attack
- Terminal Injection Attack
- Defending Terminal Injection Attack

- Other Kinds of Log File Attacks

**Module 27: Investigating Network Traffic**

- Network Addressing Schemes
- OSI Reference Model
- Overview of Network Protocols
- TCP/ IP Protocol
- 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 to Investigate Network Traffic?
- Evidence Gathering Via Sniffing
- Acquiring Traffic using DNS Poisoning Techniques
- Intranet DNS Spoofing (Local Network)
- Internet DNS Spoofing (Remote Network)
- Internet DNS Spoofing
- Proxy Server DNS Poisoning
- DNS Cache Poisoning
- Evidence Gathering From ARP Table
- Evidence Gathering at the Data-link Layer: DHCP Database
- Gathering Evidence by IDS
- Traffic Capturing and Analysis Tools
  - Tool: Tcpdump
  - Tool: Windump
  - Tool: NetIntercept
  - Tool: Wireshark
  - CommView
  - Softperfect Network Sniffer
  - HTTP Sniffer
  - EtherDetect Packet Sniffer
  - OmniPeek
  - Iris Network Traffic Analyzer
  - SmartSniff
  - NetSetMan Tool

- Distinct Network Monitor
- Maa Tec Network Analyzer
- Ntop
- Etherape
- Colasoft Capsa Network Analyzer
- Colasoft EtherLook
- AnalogX Packetmon
- BillSniff
- IE HTTP Analyzer
- EtherDetect Packet Sniffer
- EtherScan Analyzer
- Sniphere
- IP Sniffer
- AW Ports Traffic Analyzer
- Ipgrab
- Nagios
- Give Me Too
- Sniff - O – Matic
- EtherSnoop
- GPRS Network Sniffer: Nokia LIG
- Siemens Monitoring Center
- NetWitness
- Netresident Tool
- nGenius InfiniStream
- eTrust Network Forensics
- ProDiscover Investigator
- P2 Enterprise Shuttle (P2EES)
- Show Traffic
- Network Probe
- Snort Intrusion Detection System
- Snort IDS Placement
- IDS Policy Manager

- Documenting the Evidence Gathered on a Network
- Evidence Reconstruction for Investigation

**Module 28: Router Forensics**

- What is a 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
- Sample Chain Of Custody (COC) Form
- Guidelines for the Router Forensic
- Incident Response
- Recording your 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
- Example of Router Logs
- NETGEAR Router Logs
- Link Logger
- Sawmill: Linksys Router Log Analyzer
- Logging
- Handling a Direct Compromise Incident
- Other Incidents

- Real Time Forensics
- Router Audit Tool (RAT)
- Generate the Report

**Module 29: 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
- Association of Wireless AP and Device
- 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
- Detect WAPs using the Nessus Vulnerability Scanner
- Capture Wireless Traffic
- Tool: Wireshark
  - Feature of Wireshark
- Tool: tcpdump
  - tcpdump Commands
- ClassicStumbler
- Wireless Network Monitoring Tools

- MacStumbler
- iStumbler
- AirPort Signal
- AirFart
- Kismet

- 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
- Nmap
  - Scanning Wireless Access Points using Nmap
- Rogue Access Point
  - Tools to Detect Rogue Access Points: Netstumbler
  - Tools to Detect Rogue Access Points: MiniStumbler
- 2. “Sniffing” Traffic Between the Access Point and Associated Devices
- Scanning using Airodump
- MAC Address Information
- Airodump: Points to Note
- Forcing Associated Devices to Reconnect
- Check for MAC Filtering
- Changing the MAC Address
- Wireless Data Acquisition and Analysis
- Report Generation

**Module 30: Investigating Web Attacks**

- Indications of a Web Attack
- 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
- SQL Injection Attacks
- Investigating SQL Injection Attacks
- News: SQL Injection Attacks Against Databases Rise Sharply
- Code Injection Attack
- Investigating Code Injection Attack

- Parameter Tampering
- Cookie Poisoning
- Investigating 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
- Example of FTP Compromise
- Investigating FTP Logs
- 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 to Web Applications
- Investigating Static and Dynamic IP Address
- Checklist for Web Security
- Statistics 2005-2007
- Statistics 2000-2007
- Dotdefender
- AccessDiver
- Log Analyzer: Server Log Analysis
- Web Attack Investigation Tools
  - Analog
  - Deep Log Analyzer
  - AWStats
  - WebLog Expert

- AlterWind Log Analyzer
- Webalizer
- eWebLog Analyzer
- N-Stealth
- Acunetix
- Falcove
- AppScan
- Watchfire AppScan
- Emsa Web Monitor
- WebWatchBot
- Paros
- HP WebInspect
- KeepNI
- Wikto
- Mapper
- N-Stalker
- Scrawlr
- Exploit-Me

- Tools for Locating IP Address
  - Hide Real IP
  - Whatismyip
  - IP Detective Suite
  - Enterprise IP - Address Manager
  - Whois Lookup
  - SmartWhois
  - ActiveWhois
  - LanWhois
- Nslookup
- Traceroute
- Tools for Locating IP Address
  - NeoTrace (Now McAfee Visual Trace)
  - Whois
  - CountryWhois
  - IP2Country
  - CallerIP
  - Whois.net
  - Pandora FMS

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

**Module 31: Investigating DoS Attacks**

- DoS Attack
- Indications of a DoS/DDoS Attack
- Types of DoS Attacks
- Ping of Death Attack
- Teardrop Attack
- SYN Flooding
- Land
- Smurf
- Fraggle and Snork Attack
- WINDOWS OUT-OF-BAND (OOB) Attack and Buffer Overflow
- Nuke Attacks and Reflected Attack
- DDoS Attack
- Working of DDoS Attacks
- Classification of DDoS Attack
- DDoS Attack Taxonomy
- DoS Attack Modes
- Techniques to Detect DoS Attack
- 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
- ICMP Traceback
- Hop-by Hop IP Traceback
- Limitations of Hop-by Hop IP Traceback
- Backscatter Traceback
- How the Backscatter Traceback Works
- IP Traceback with IPSec
- CenterTrack Method
- Packet Marking
- Probabilistic Packet Marking (PPM)
- Check Domain Name System (DNS) Logs

- Tracing with "log-input"
- Control Channel Detection
- Correlation and Integration
- Path Identification (Pi) Method
- Packet Traffic Monitoring Tools
- Tools for Locating IP Address
- Challenges in Investigating DoS Attack
- Network Monitoring Tools
  - Nmap
  - Friendly Pinger
  - IPHost Network Monitor
  - Tail4Win
  - Status2k
  - DoSHTTP
  - Admin's Server Monitor

**Module 32: Investigating virus, Trojan, spyware and Rootkit Attacks**

- Statistics of the Malicious and Potentially Unwanted Programs
- Viruses and Worms
  - Virus Top 20 for January 2008
  - Viruses
  - Worms
  - How to Know a Virus Infected a System
  - Characteristics of a Virus
  - Working of a Virus
    - Working of a Virus: Infection Phase
    - Working of a Virus: Attack Phase
  - Symptoms of a Virus-Like Attack
  - Indications of a Virus Attack
  - Modes of Virus Infection
  - Stages of Virus Life
  - Virus Classification
  - How Does a Virus Infect?
  - Storage Patterns of a Virus
  - Virus Detection
  - Virus Detection Methods
  - Virus Incident Response

- Investigating Viruses
- Trojans and Spyware
  - Trojans and Spyware
  - Working of Trojans
  - How Spyware Affects a System
  - What Spyware Does to the System
  - What Do Trojan Creators Look For?
  - Different Ways a Trojan Can Get into a System
  - Identification of a Trojan Attack
  - Remote Access Trojans (RAT)
  - Ports Used by Trojans
- Anti virus Tools
  - AVG Antivirus
  - Norton Antivirus
  - McAfee
  - Kaspersky Anti-Virus
  - BitDefender
  - SocketShield
  - CA Anti-Virus
  - F-Secure Anti-Virus
  - F-Prot Antivirus
  - Panda Antivirus Platinum
  - avast! Virus Cleaner
  - Norman Virus Control
  - ClamWin
- Anti Trojan Tools
  - TrojanHunter
  - Comodo BOClean
  - Trojan Remover: XoftspySE
  - Trojan Remover: Spyware Doctor
  - SPYWAREfighter
  - Evading Anti-Virus Techniques
  - Sample Code for Trojan Client/Server
- Evading Anti-Trojan/Anti-Virus Using Stealth Tools
- Backdoor Countermeasures
- Tool: Tripwire
- System File Verification

- MD5sum.exe
- Tool: Microsoft Windows Defender
- Rootkit
  - Introduction of Rootkit
  - Attacks Approach
  - Types of Rootkits
  - Rootkit Detection
- Windows Rootkit
  - Fu Rootkit
  - Vanquish
  - AFX Rootkit
- Linux Rootkit
  - Knark
  - Adore
  - Ramen
  - Beastkit
- Rootkit Detection Tools
  - UnHackMe
  - UnHackMe Procedure
  - F-Secure BlackLight
  - RootkitRevealer
  - Microsoft Windows Malicious Software Removal Tool
  - Rkhunter
  - chkrootkit
  - IceSword

**Module 33: Investigating Internet Crimes**

- Internet Crimes
- Internet Forensics
- Why Internet Forensics
- Goals of Investigation
- Investigating Internet Crime Steps
- 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
  - Example Whois Record
- Whois Tools and Utilities
  - Samspade
  - SamSpade Report
  - IP Address Locator
  - www.centralops.net: Tracing Geographical Location of a URL
  - DNS Lookup Result: centralops.net
  - Traceroute
- Collect the Evidence
- Examining Information in Cookies
- Viewing Cookies in Firefox
  - Tool: Cookie Viewer
- Switch URL Redirection
- Sample Javascript for Page-based Redirection
- Embedded JavaScript
- Downloading a Single Page or an Entire Web Site
  - Tool: My Offline Browser
- Recovering Information from Web Pages
  - Tool: WayBack Machine
  - *Take Me Back* Results
- Investigation Tool
  - Grab-a-Site
  - SurfOffline
  - Trace the Email
  - https://www.abika.com/forms/Verifyemailaddress.asp

- HTTP Headers
- Email Headers Forging
- Viewing Header Information
- Tracing Back Spam Mails
  - VisualRoute
  - NeoTrace (Now McAfee Visual Trace)
  - NetScanTools Pro
- Report Generation

**Module 34: Tracking Emails and Investigating Email crimes**

- Email System
- E-mail Client
- E-mail Server
- SMTP Server
- POP3 and IMAP Server
- Importance of Electronic Records Management
- E-mail Crime
- Spamming
- Mail Bombing/Mail Storm
- Crime via Chat Rooms
- Identity Fraud/Chain Letter
- Phishing
- Email Spoofing
- Investigating E-mail Crime and Violation
- 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
- Viewing Header in AOL
- Viewing Headers in Hotmail
- Viewing Header in Gmail
- Viewing Header in Yahoo Mail
- Examining an Email Header
- Analysis of Email Header at 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 ToolKit (FTK)
- E-Mail Examiner by Paraben
- Network E-Mail Examiner by Paraben
- Recover My Email for Outlook
- Diskinternals – Outlook Recovery
- Tracing Back
- Tracing Back Web Based E-mail
- Abuse.Net
- Network Abuse Clearing House
- Tool: LoPe
- Tool:FINALeMAIL
- Handling Spam
- Tool: eMailTrackerPro
- Email Trace
- Tool: ID Protect
- Email Investigation Tool
  - R-Mail
  - Email Detective
  - SPAM Punisher
  - SpamArrest
- 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 35: PDA Forensics**

- Personal Digital Assistant (PDA)
- Information Stored in PDA
- PDA Components

- 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 Attacks
- PDA Fornnsics
  - PDA Forensics steps
  - Points to Remember while Conducting Investigation
  - Securing and Evaluating the Scene
  - Seize the Evidences
  - Identify the Evidence
  - Preserve the Evidence
  - Acquire the Information
  - Data Acquisition Techniques
  - Examination and Analysis the Information
  - Document Everything
  - Make the Report
- PDA Forensic Tool
  - PDA Secure
  - Device Seizure
  - DS Lite
  - EnCase
  - SIM Card Seizure
  - Palm dd (pdd)
  - Duplicate Disk
  - Pocket PC Forensic Software
  - Mobile Phone Inspector
  - Memory Card Data Recovery Software
- PDA Security Countermeasures

## Module 36: Blackberry Forensics

- Blackberry
- BlackBerry Operating System
- How BlackBerry Works
- BlackBerry Serial Protocol
- BlackBerry Serial Protocol: Packet Structure
- Blackberry 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
- Collect the Evidence
- Document the Scene and Preserve the Evidence
- Radio Control
- Imaging and Profiling in BlackBerry
- Acquire the Information
- Hidden Data in BlackBerry
- Acquire Logs Information from BlackBerry
- Program Loader
- Review of Information
- Best Practices for Protecting Stored Data
- BlackBerry Signing Authority Tool
- Forensics Tool: RIM BlackBerry Physical Plug-in
- ABC Amber BlackBerry Converter
- Packet PC
- ABC Amber vCard Converter
- BlackBerry Database Viewer Plus

## Module 37: iPod and iPhone Forensics

- iPod
- iPhone Overview

- What a Criminal Can do With iPod
- What a Criminal Can do With iPhone
- iPhone OS Overview
- iPhone Disk Partitions
- Apple HFS+ and FAT32
- Application Formats
- iPod and iPhone Forensics
- 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
- 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
- Other Files Which are Downloaded to the Computer During iTunes Sync Process
- Analyze the Information
- Timeline Generation
- Timeline Generation: File Status After Initialization the iPod with iTunes and Before Closing iTunes
- Timeline Generation: File Status After Connecting iPod to the Computer for Second Time, Copying Music, and Closing iTunes
- Time Issues
- Jailbreaking in iPod Touch and iPhone
  - Jailbreaking
  - AppSnapp
  - iFuntastic
  - Pwnage: Tool to Unlock iPod Touch
  - Erica Utilities for iPod Touch
- Tools
  - EnCase
  - DiskInternals Music Recovery
  - Recover My iPod: Tool
  - iPod Data Recovery Software
  - iPod Copy Manager
  - Stellar Phoenix iPod Recovery
  - Aceso
  - Cellebrite UME 36 Pro
  - Walf
  - Device Seizure
  - PhoneView
  - iPhone Drive
  - Tansee iPhone Transfer SMS
  - SIM Analyzer
  - SIMCon – SIM Card Recovery
  - SIM Card Data Recovery Software

### Module 38: 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)
- SIM File System
- Integrated Circuit Card Identification (ICCID)
- International Mobile Equipment Identifier (IMEI)
- Electronic Serial Number (ESN)
- Precaution 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)
- Analyze the Information
- Cell Phone Forensic Tools
  - SIM Analyzer
  - SIMCon
  - SIM Card Data Recovery
  - Memory Card Data Recovery
  - Device Seizure
  - SIM Card Seizure
  - Cell Phone Analyzer
  - Oxygen Forensic Suite
  - BitPim
  - MOBILedit! Forensic
  - PhoneBase
  - Secure View

- XACT
- CellDEK
  Forensic Card Reader (FCR)
- ForensicSIM Toolkit
- SIMIS 3G
- UME-36Pro - Universal Memory Exchanger
- Cellebrite UFED System - Universal Forensic Extraction Device
- ZRT
- Neutrino
- ICD 5005
- ICD 1300

- Challenges for Forensic Efforts

**Module 39: USB Forensics**

- Universal Serial Bus (USB)
- USB Flash Drive
- Screenshot: USB Flash Drive
- Misuse of USB
- USB Forensics
- USB Forensic Investigation
- Secure and Evaluate the Scene
- Document the Scene and Devices
- Image the Computer and USB Device
- Acquire the Data
- Check Open USB Ports
- Examine Registry of Computer: USBTOR
- Examine Registry of Computer: DeviceClasses
- Examine Registry of Computer: MountedDevice
- Generate Reports
- USB Forensic Tools
  - Bad Copy Pro
  - Data Doctor Recovery
  - USB Image Tool
  - USBDeview

**Module 40: Printer Forensics**

- Introduction to Printer Forensics
- Different Printing Modes

- Methods of Image Creation
- Printers with Toner Levels
- Parts of a Printer
- Printer Identification Strategy
  - Printer Identification
- Printer Forensics Process
  - Pre-Processing
  - Printer Profile
  - Forensics
  - Ballistics
- A Clustering Result of a Printed Page
- Digital Image Analysis
- Printout Bins
- Document Examination
  - Services of Document Examiner
  - Tamper-proofing of Electronic and Printed Text Documents
- Phidelity
- Zebra Printer Labels to Fight against Crime
- Cryptoglyph Digital Security Solution
- Case Study
- Is Your Printer Spying On You?
- DocuColor Tracking Dot Decoding
- Tools
  - Print Spooler Software
  - Investigating Print Spooler
  - iDetector
  - Print Inspector
  - EpsonNet Job Tracker

**Module 41: Investigating Corporate Espionage**

- Investigating Corporate Espionage: Case Study
- 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
- Key Findings from U.S Secret Service and CERT Coordination Center/SEI study on Insider Threat
- Netspionage
- Investigating Corporate Espionage Cases
- Employee Monitoring: Activity Monitor
- Spector CNE Employee Monitoring Software
- Track4Win
- Spy Tool
  - SpyBuddy
  - NetVizor
  - Privatefirewall w/Pest Patrol
- Anti Spy Tool
  - Internet Spy Filter
  - Spybot S&D
  - SpyCop
  - Spyware Terminator
  - XoftSpySE
- Spy Sweeper
- Counter Spy
- SUPERAntiSpyware Professional
- IMonitorPCPro - Employee Monitoring Software
- Case Study: HP Chief Accused of Corporate Spying
- Case Study: India's Growing Corporate Spy Threat
- Guidelines while Writing Employee Monitoring Policies

**Module 42: Investigating Computer Data Breaches**

- How Data Breaches Occur
  - Using The External Memory Devices
  - Using The Internet
  - Using Mobiles And iPods
  - Using Malware
  - Others Techniques
- Investigating Local Machine

- Check The Registry Editor
- Check For CD/DVD Burning Software
- Check For Browsing History
- Check The Downloads
- Check The Mail History
- Check For Suspicious Software

- Investigating Network
  - Check The Firewall
  - Check The Mail Server
  - Check The Printers
- Countermeasures

**Module 43: Investigating 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 is Copyrights Enforced?
  - Copyright Infringement: Plagiarism
  - Types of plagiarism
  - Steps for Plagiarism Prevention
  - Plagiarism Detection Factors
- Plagiarism Detection Tools
  - Turnitin
  - CopyCatch
  - Copy Protection System (COPS)
  - SCAM (Stanford Copy Analysis Mechanism)
  - CHECK

- Jplag
- VAST
- SIM
- Urkund
- WCopyfind
- GPSP
- PLAGUE
- SPlaT
- Sherlock
- PRAISE
- SafeAssignment
- EVE2
- iThenticate
- Dupli Checker
- http://www.plagiarismdetect.com/
- http://www.plagiarism.org.uk/

- Patent Infringement
  - Patent
  - Patent Infringement
  - 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
  - Intellectual Property
  - Investigating Intellectual Property Theft
  - Steps for Investigating Intellectual Property Theft
- Digital Rights Management
  - Digital Rights Management (DRM)
- Windows Media Digital Rights Management
- Media-DRM Packager
- Haihaisoft Media DRM Packager
- DRM Software for Copy Protection
- IntelliProtector
- Trademarks and Copyright Laws

- 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
- China Laws for Trademarks and Copyrigh
- Canada Laws for Trademarks and Copyright
- South African Laws for Trademarks and Copyright
- South Korean Laws for Trademarks and Copyright
- Belgium Laws for Trademarks and Copyright
- Hong Kong Laws for Intellectual Property

**Module 44: Investigating Sexual Harassment Incidents**

- Sexual Harassment - Introduction
- Types of Sexual Harassment
- Consequences of Sexual Harassment
- Sexual Harassment Statistics
- Do's and Don'ts if You Are Being Sexually Harassed
- Stalking
- Stalking Behaviors
- Stalking Effects
- Guidelines for Stalking Victims
- Responsibilities of Supervisors
- Responsibilities of Employees
- Complaint Procedures
  - Informal procedures
  - Formal procedures
- Investigation Process
  - Investigation Process
  - Sexual Harassment Investigations
  - Sexual Harassment Policy
  - Preventive Steps
- Laws on Sexual Harassment
  - 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
- Australian Laws on Sexual Harassment
- The Laws on Sexual Harassment: Sex Discrimination Act 1984
- The Laws on Sexual Harassment: Equal Opportunity for Women in the Workplace Act 1999
- The Laws on Sexual Harassment: Anti-Discrimination Act 1991
- The Laws on Sexual Harassment: Workplace Relations Act 1996
- Indian Law: Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Bill, 2006
- German Law: Protection of Employees Act
- UK Law: The Employment Equality (Sex Discrimination) Regulations 2005
- Law of the People's Republic of China on the Protection of Rights and Interests of Women
- Penal Code, Section 509. in Malaysia

- Sample Complaint Form
- Laws Against Stalking

**Module 45: Investigating Child Pornography Cases**

- 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
- Precautions before Investigating Child Pornography Cases
- Steps for Investigating Child Pornography
  - Step 1: Search and Seize all Computer 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
- Citizens' Responsibility on pornography
- Guidelines to Avoid Child Pornography on the Web
- Guidelines for Parents to Protect Children from Pornography
- Tools to Protect Children from Pornography
    - Reveal
    - iProtectYou
    - WUPC Web Control for Parents 4
    - BrowseControl
    - ChatGuard
    - Child Exploitation Tracking System (CETS)
- Reports on Child Pornography
- Laws Against 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
    - South African Laws against Child Pornography
    - UK laws against Child Pornography
    - State Laws: Michigan Laws against Child Pornography
    - England and Wales Laws
    - Scotland laws
    - Philippines laws ( Republic Acts)
    - Children's Internet Protection Act (CIPA)
- Anti-Child-Pornography Organizations
    - Innocent Images National Initiative
    - Internet Crimes against Children (ICAC)
    - Antichildporn.org
    - How to Report to Antichildporn.org about Child Pornography Cases
    - Child Exploitation and Online Protection (CEOP) Centre
    - ThinkUKnow
    - Virtual Global Taskforce (VGT)
    - Internet Watch Foundation (IWF)

- International Centre for Missing & Exploited Children (ICMEC)
- National Center for Missing & Exploited Children (NCMEC)
- Child Victim Identification Program (CVIP)
- Financial Coalition against Child Pornography (FCACP)
- Perverted Justice
- National Society for the Prevention of Cruelty to Children (NSPCC)
- Canadian Centre for Child Protection
- http://cybertip.ca/
- Association of Sites Advocating Child Protection (ASACP)
- Web Sites against Child Porn (WSACP)
- http://www.reportchildporn.com/
- Child Focus
- StopChildPorno.be

**Module 46: Investigating Identity Theft Cases**

- Identity Theft
  - Identity Theft
  - Identifying Information
  - Identity Theft Statistics for 2007
  - Identity Theft Complaints By Age of The Consumer
  - Example of Identity Theft
  - Who Commits Identity Theft
  - How Criminals Get Information
  - How Personal Information Was Stolen: Statistics
  - Techniques Used By Criminals
  - How Does A Criminal Use Information
  - FTC Consumer Sentinel
  - Identity Theft Movies
- Investigating Identity Theft
  - Investigating Identity Theft
  - Interview The Victim
  - Get The Credit Reports
  - Sample Credit Report
  - Collect Information About Online Activities of Victim
  - Collect Information About The Websites Where Victim Has Disclosed Personal Information
    - http://www.whois.net/
    - http://centralops.net/co/

        - http://www.archive.org/
    - Search The FTC Consumer Sentinel
    - Collect Information From Point Of Sale
    - Collect Information From Courier Services
    - Get Call Records From Service Providers If Stolen Identity Is Used To Obtain Phone Service
    - Search The Suspect's Address
    - Obtain Search And Seize Warrant
    - Seize The Computer And Mobile Devices From Suspects
    - Collect The Browser Information From Suspects Computer
- Identity Theft Laws
    - United States: Federal Identity Theft and Assumption Deterrence Act of 1998
    - Unites States Federal Laws
    - Australia
    - Canada
    - Hong Kong
    - United Kingdom
- Protection From Identity Theft
    - Protection From ID Theft
    - What Should Victims Do?
    - Resources for Victims

**Module 47: Investigating Defamation over Websites and Blog Postings**

- What is a Blog
- Types of Blogs
- Blogging
- Who is Blogging?
- Blogosphere Growth
- Defamation over Websites and Blog Postings
- Steps for Investigating Defamation Over Websites and Blog Postings
- Search the Content of Blog in Google
- Check the URL of the Blog/Webpage
- Check the Copyright and Privacy Policy
- Check the Profile of Author of the Blog/Web Post
- Intelius Search (www.intelius.com)
- Yahoo! People Search
- Satellite Picture of a Residence
- Best PeopleSearch (http://www.bestpeoplesearch.com/)

- People-Search-America.com
- Check the Comments for the Blog
- Search in www.archive.org
- Search Results
- Check in Whois Database
- Whois Database Result
- Search the Email Address and Telephone Number
- Visit 411 and Search for Telephone Numbers
- Search for UK Telephone Numbers at BT
- Check the Physical Location

**Module 48: Investigating Social Networking Websites for Evidences**

- Introduction: Social Networking
- What Is a Social Networking Site
- MySpace
- Facebook
- Orkut
- Crime Using Social Networking Website
- Use of Social Networking Websites in Investigations
- Investigation Process
- Search for Convict Account on Website
- Mirror the web pages in the CD-ROM
- Investigation in MySpace
- Investigation in Facebook
- Investigation in Orkut
- Investigating Profile
- Investigating Scrapbook
- Investigating Photos and Video
- Investigating Testimonials
- Investigating View Events
- Investigating Friendlist
- Investigating Communities
- Report Generation

**Module 49: Investigation Search Keywords**

- Keyword Search
- Developing a Keyword Search List

- Index-Based Keyword Searching
- Bitwise Searching
- Keyword Search Techniques
- Choice of Searching Methodology
- Issues with Keyword Searching
- Odyssey Keyword Search

**Module 50: Investigative Reports**

- Computer Forensic Report
- Computer Forensic Rreport Template
- Report Specifications
- Report Classification
- Layout of an Investigative Report
- 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
- Signature Analysis
- Sample Forensic Report
- Investigation Procedures
- Collecting Physical and Demonstrative Evidence
- Collecting Testimonial Evidence
- Dos and Don'ts of Forensic Computer Investigations
- Case Report Writing and Documentation
- Create a Report to Attach to the Media Analysis Worksheet
- Best Practices for Investigators
- Writing Report Using FTK

**Module 51: 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
  - Medical & Psychological Experts
  - Civil Litigation Experts
  - Construction & Architecture Experts
  - Criminal Litigation Experts
- Scope of Expert Witness Testimony
- Technical Testimony vs. Expert Testimony
- Preparing for Testimony
- Evidence Preparation and Documentation
- Evidence Processing Steps
- Checklists for Processing Evidence
- Examining Computer Evidence
- Prepare the Report
- Evidence Presentation
- Rules Pertaining to an Expert Witness' Qualification
- Daubert Standard
- Frye Standard
- Importance of 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
- Recognizing Deposing Problems
- Guidelines to Testify at a Deposing
- Dealing with Media
- Finding an Computer Forensic Expert

**Module 52: How to Become a Digital Detective**

- Digital Detective
- Roles and Responsibilities of Digital Detectives

- Traits of a Digital Detective
- Technical Skills
- Qualification of Digital Detectives
- Wider Competencies
- Computer Forensics Training and Certification
- Join Online Forums
- Knowledge About Law

**Module 53: Computer Forensics for Lawyers**

- Computer Forensics for Lawyers
- Initial Information to be Known by Lawyers When an Incident Occurs
- Presenting the Case
- What Lawyers Should Know
- Functions of Lawyers
- When Do Lawyers Really Need to Hire a Forensic Expert?
- Identify the Right Forensic Expert
- Industry Associations Providing Expert Forensic Investigators
- Check for Legitimacy
- What Lawyers Should Know in the Forensic Process
- What Makes Evidence Inadmissible in the Court
- Computer Forensics Cases
- What Lawyers Should Expect from Forensic Examiner

**Module 54: Law and Computer Forensics**

- Computer Forensics Laws
- Role of Law Enforcement Agencies in Forensics Investigation
- Guidelines for Law Enforcement Agencies
- Law Enforcement Policies
- Internet Laws and Statutes
  - Federal Laws (Computer Crime)
  - Intellectual Property Rights
  - Cyber Stalking
- Information Security Acts
  - The USA Patriot Act of 2001
  - Federal Information Security Management Act
  - Gramm-Leach Bliley Act
  - CAN-SPAM Act

- Personal Information Protection and Electronic Documents Act
- Data Protection Act 1998
- Criminal Damage Act 1991
- Cyber Terrorism Preparedness Act of 2002

- Laws Related to Information Assurance and Security
  - Federal Records Act
  - Federal Managers Financial Integrity Act of 1982
  - Federal Property and Administration Service Act
  - Government Paperwork Elimination Act
  - Paperwork Reduction Act
  - Computer Fraud and Abuse Act
  - Freedom of Information Act
  - E-Government Act 0f 2002 /Public Law 107-347
  - Implications of Public Law 107-347 Regarding Certification and Accreditation
  - Information Privacy Act 2000
  - National Archives and Records Act
- Computer Crime Acts
  - Australia: The Cybercrime Act 2001
  - Austrian Laws
  - Belgium Laws
  - Brazilian Laws
  - Canadian Laws
  - Denmark Laws
  - European Laws
  - France Laws
  - German Laws
  - Greece Laws
  - Hongkong Laws
  - Indian Laws
  - Italian Laws
  - Japanese Laws
  - Latvian Laws
  - Malaysian Laws
  - Malta laws
  - Netherlands Laws
  - Norwegian Laws
  - Philippines Laws: Electronic Commerce Act of 2000

- Singapore Laws: Computer Misuse Act
- United Kingdom: Police and Justice Act 2006
- United States Laws

- Internet Crime Schemes and Prevention Tips
  - Internet Crime Schemes
  - Internet Crime Prevention Tips
- Reporting a Cybercrime
  - 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
  - CIO Cyberthreat Report Form
- Crime Investigating Organizations
  - Crime Investigating Organizations
  - Interpol - Information Technology Crime Center
  - *www.interpol.int*
  - Federal Bureau of Investigation
  - How the FBI Investigates Computer Crime
  - Federal Statutes Investigated by the FBI
  - Contact FBI Form
  - National White Collar Crime Center (NW3C)
  - Internet Crime Complaint Center (IC3)
  - Department of Homeland Security
  - National Infrastructure Protection Center
  - The G8 Countries: Principles to Combat High-tech Crime
  - The G8 Countries: Action Plan to Combat High-Tech Crime (International Aspects of Computer Crime)
  - Crime Legislation of EU
  - Law Enforcement Interfaces (EnRoute)

**Module 55: Computer Forensics and Legal Compliance**

- Legal Compliance
  - Regulatory Compliance and Computer Forensics
  - Legal and Liability Issues

- Information Security Compliance Assessment
- Legal Compliance Program
  - Principles of Legal Compliance Program
  - Elements of an Effective Compliance Program
  - Role of Senior Management in Compliance Program
  - Importance of Compliance and Ethics Programs
  - Benefits of Compliance Program
  - Best Practices for Successful Implementation of a Compliance Program
  - Compliance Program Checklist
  - Compliance with Consent Decrees
  - Memoranda of Understanding/ Agreement (MOU/MOA)
  - Enterprise Compliance and Risk Analysis
  - Creating Effective Compliance Training Program
  - Responsibilities of Senior Systems Managers
  - Legal Compliance to Prevent Fraud, Waste, and Abuse
- Terms Related to Legal Compliance
  - Copyright Protection
  - Copyright Licensing
  - Criminal Prosecution
  - Due Diligence
  - Evidence Collection and Preservation
  - Importance of Evidence Collection
  - Importance of Evidence Preservation

**Module 56: Security Policies**

- Access Control Policy
- Administrative Security Policies and Procedures
- Audit Trails and Logging Policies
- Documentation Policy
- Evidence Collection and Preservation Policies
- Information Security Policy
- National Information Assurance (IA) Certification & Accreditation (C&A) Process Policy
- Personnel Security Policies & Guidance

**Module 57: Risk Assessment**

- Risk
- Security Planning

- Risk Management
  - Importance of Risk Management
- Principle of Risk Management
- IT Security Risk Management
- Risk Analysis
- Conduct Business Impact Analysis (BIA)
- Roles and Responsibilities of all the Players in the Risk Analysis Process
- Risk Analysis and/or Vulnerability Assessment Components
- Risk Policy
- Risk Assessment
  - Importance of Risk Assessment
- Approval to Operate (ATO) and Interim Approval to Operate (IATO)
  - Importance of Risk Assessment to Obtain an IATO and ATO
- Risk Assessment Methodology
- Information Sources for Risk Assessments
- Risk Assessment Process
  - Develop Policy and Procedures for Conducting a Risk Assessment
  - Write Risk Assessment Reports
  - Coordinate Resources to Perform a Risk Assessment
  - Risk Assessment Plan
- Analyze Threats and Vulnerabilities of an Information System
- Residual Risk
  - Explain Residual Risk
- Residual Risk Policy
  - Residual Risk Standard: ISO/IEC 27005:2008
- Cost/benefit Analysis
  - Cost/Benefit Analysis for Information Assurance
- Importance of Cost/Benefit Analysis for Information Assurance
- Cost/benefit Analysis Procedure
- Risk Acceptance
  - Risk Acceptance Process
- Management's Risk Acceptance Posture
- Risk Assessment and Countermeasures
- Risk Analysts
- Risk Mitigation
- Risk and Certification/Accredition of Information Systems
  - Role of Systems Certifiers and Accreditors in Risk Mitigation

- Role of Documentation in Reducing Risk

**Module 58: Evaluation and Certification of Information Systems**

- Accreditation
  - Importance of Accreditation
  - Types of Accreditation
  - Site Accreditation
  - Significance of NSTISSP
- Approval to Operate (ATO)
- Interim Approval to Operate (IATO)
  - Systems Security Authorization Agreement (SSAA)
    - Contents of SSAA
  - Justification for Waiver
- Cost-Benefit Analysis
- Information Classification
- Importance of Information Classification
- Investigative Authorities
- Key Management Infrastructure
- Information Marking
- Certification Test & Evaluation (CT&E)
- Certification Tools
- Product Assurance
  - Protection Profiles
  - Security Targets
- Contracting For Security Services
- Disposition of Classified Material
- Optical Remanence
- Magnetic Remanence
- Facilities Planning
  - Importance of Facilities Planning
- System Disposition/Reutilization
- Life Cycle System Security Planning
- System Security Architecture
- C&A Process for Information System
- C&A Life Cycle
  - Responsibilities Associated with Accreditation
  - Roles Associated with Certification

- Information Ownership

**Module 59: Ethics in Computer Forensics**

- Introduction to Computer Forensic Ethics
- Procedure to Implement Ethics
- Importance of Computer Ethics
- Challenges in Teaching Computer Forensics Ethics
- Ethical Predicaments
- The Ethical Requirements During Investigation
- Ethics in Preparation of Forensic Equipments
- Ethics of Computer Forensic Investigator
- Maintaining Professional Conduct
- Ethics in Logical Security
- Ethics in Obtaining the Evidence
- Ethics while Preserving the Evidence
- Ethics in Documenting Evidence
- Ethics in Bringing Evidence to Courtroom

**Module 60: Computer Forensic Tools**

- Software Forensic Tools
  - Visual TimeAnalyzer
  - X-Ways Forensics
  - Evidor
  - Slack Space & Data Recovery Tools:
  - Ontrack
  - Data Recovery Tools:
    - Device Seizure 1.0
    - Data Recovery Tools: Forensic Sorter v2.0.1
    - Data Recovery Tools: Directory Snoop
  - Permanent Deletion of Files:
    - PDWipe
    - Permanent Deletion of Files: Darik's Boot and Nuke (DBAN)
  - File Integrity Checker:
    - FileMon
    - File Date Time Extractor (FDTE)
    - Decode - Forensic Date/Time Decoder
  - Disk Imaging Tools: Snapback Datarrest

- Partition Managers: Partimage
- Linux/Unix Tools: Ltools and Mtools
- Password Recovery Tool:
  - @Stake
  - Password Recovery Tool: Decryption Collection Enterprise
  - 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
- Multipurpose Tools:
  - Maresware
  - Multipurpose Tools: LC Technologies Software
  - Multipurpose Tools: Winhex Specialist Edition
  - Multipurpose Tools: Prodiscover DFT
- Toolkits:
  - NTI Tools
  - Toolkits: R-Tools-I
  - Toolkits: R-Tools-II
  - Toolkits: Datalifter
  - Toolkits: Accessdata
  - FTK – Forensic Toolkit
  - Toolkit: Fastbloc
  - Toolkit: Encase
- Email Recovery Tool:
  - E-mail Examiner
  - Network E-mail Examiner
- Case Agent Companion
- Chat Examiner
- Forensic Replicator
- Registry Analyzer
- ASR Data's SMART
- Oxygen Phone Manager

- 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

- Hardware Computer Forensic Tools
  - Hard Disk Write Protection Tools
    - PDBlock
    - 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 61: Windows Based Command Line Tools

- 3Scan

    - AGREP
    - Aircrack
    - ARPFlash
    - ASPNetUserPass
    - AtNow
    - BBIE
    - BFI
    - Renamer
    - BootPart
    - BuiltIn Account Manager
    - bzip2
- WhoAmI
- Command Line SFV Checker 0.1
- MaxDIR 2.29
- Run! 2.6.7
- Network Ping
- WinTraceRoute
- 4NT 8.02
- Nbtstat
- Netsh
- Taskkill
- Tasklist
- WMIC
    - NetStat Agent
    - Ping 1.2
    - DNS lookup 1.1
    - Findstr
    - mtsend.py
    - wmctrl 1.07
    - stsadm
    - listadmin (2.40-1)
    - Copyprofile
    - NBLookup.exe
    - Whoiscl
    - AccExp
    - c2pas32
    - fscript 2.0

- GConf
- FMPP
- XQilla
- Mosek
- ToggIT Command Line Helper 1.0
- Bayden SlickRun 2.1
- cb 1.0.0.1
- Blat
- ffmpeg

**Module 62: Windows Based GUI Tools**

- Process Viewer Tool
  - CurrProcess
  - Process Explorer
  - ProcessMate
  - ServiWin
- Registry Tool
  - Autoruns
  - Autostart Viewer
  - ERUNT
  - Hijackthis
  - Loadorder
  - Regbrws
  - Regedit PE
  - Regscanner
- Desktop Utility Tool
  - BossKey
  - Count Characters
  - HoverSnap
  - Lens
  - Pixie
  - PureText
  - ShoWin
  - Sizer
  - SysExporter
- Office Application Tool:
  - ASCII Values
  - Atlantis Nova

- Character Grid
- DateStat
- DBF Explorer
- DHB Workshop
- firstobject XML Editor
- Foxit PDF Reader
- Irfan View
- MetaPad
- PrintServer

- Remote Control Tool
  - Gencontrol
  - IVT
  - Putty
  - VNC Viewer
- Network Tools
  - Adapterwatch
  - Commtest
  - CurrPorts
  - Hey Joe!
  - IP2
  - IP Netinfo
  - Ldp
  - Necrosoft Dig
  - Net Send (NT Toolkit)
  - POP3 Preview
  - Popcorn
  - Quick Mailer
  - TCPView
  - Trout
  - WinArpSpoof
- Network Scanner Tool
  - Attack Tool Kit(ATK)
  - DDos Ping
  - DNSWalker
  - DSScan
  - GetAcct
  - JJJExec

- MyDoomScanner
- Netstumbler
- RPCScan
- RPCScan2
- ShareEnum
- Shed
- SNScan
- SuperScan4

- Network Sniffer Tool
  - Analyzer
  - IPSniffer
  - NGSSniff
  - Show Traffic
  - SmartSniff
  - Sniphere
- Hard Disk Tool
  - 48-bit LBA Technology
  - Darik's Boot and Nuke
  - DirectDisk
  - Disk Checker
  - Disk Investigator
  - DiskMon
  - DiskPatch
  - DiskPie Pro
  - Emsa Disk Check
  - Hard Disk Indicator, HDSpeed
  - HD Tach
  - HD Tune
  - HDClone
  - HDINFO Tool
  - Maxtor MaxBlast
  - Maxtor Powermax
  - MBRtool
  - MBRWork
  - Sectedit
  - Sector Inspector
  - Western Digital Diagnostic

- Hardware Info Tools
  - Bart's Stuff Test
  - Central Brain Identifier
  - Data LifeGuard Diagnostics for Windows
  - Drive View
  - DTemp
  - HD Tune
  - HD_Speed
  - Monitor Test
  - Nero CD/DVD Speed
  - Nero Drive Speed
  - Nero Info Tool
  - ReSysInfo
  - SIW
  - WinAudit
- File Management Tool
  - 1-4a Rename
  - A43
  - CD2ISO
  - Delold
  - Disktools Imagemaker
  - Drvcloner XP, Cdmanipulator
  - Drvimager XP
  - Dscrypt
  - Express Burn
  - Ntouch, Rawwrite for Windows
  - Pablo Commander
  - Pagedefrag
  - Replace in Files, Splitter Light
  - UUD32 Windows
  - Wintidy
- File Recovery Tool
  - Handy Recovery
  - PC Inspector
  - Restoration
  - R-Linux
  - Smart Recovery

- Zip File Recovery
- File Transfer Tool
  - Babyftp Server
  - Babypop3 Server
  - Babyweb Server
  - Dropupload, File Gateway
  - Dropupload, File Gateway
  - Freeway FTP
  - HFS HTTP File Server
  - Nullsoft Copy, Smbdownloader
  - Simple Socket File Transfer
  - Synchronize It! V1.69
  - TFTPD32
  - Wackget, Thirddir
  - Unstoppable Copier
  - Winscp
- File Analysis Tool
  - AccessEnum
  - BinText
  - CDMage
  - DBF Viewer Plus
  - DefragNT
  - Dependency Walker
  - Disk Investigator
  - DiskView
  - DupeLocator
  - E-Grabber
  - ExamDiff
  - Explore2FS
  - File Analyzer
  - File List Generator
  - Folders Report
  - Gemulator Explorer
  - HashCalc
  - Lister
  - MDB View
  - Media Checker

- PEiD
- Resource Hacker
- Space Monger
- Tiny Hexer
- Virtual Floppy Driver
- Win Interrogate
- xTeq X-Find

- Password Tool
  - CISCO PIX Firewall Password Calculator
  - Encode Unix Password
  - Password Assistant (NTToolkit)
  - Password Generator
- Password Cracking Tool
  - Access PassView
  - Chat Recovery
  - Asterisk Logger
  - Basic Authentication
  - Brutus
  - DeBat!
  - Dialupass
  - Enterprise Manager PassView
  - GetKey
  - GetPass
  - Keyfinder
  - Lepton's crack
  - Mail PassView
  - Messenger Key
  - MessenPass
  - Netscapass
  - Outlooker
  - PCAnywhere PassView
  - Protected Storage PassView
  - RockXP
  - Share Password Checker
  - X-Pass
- Other GUI Tools:
  - AtomicTime, FavouritesView

- IECookiesView
- IEHistoryView
- MozillaCookiesViewer
- MyUninstaller
- Neutron
- NewSID
- ShortCutsMan
- Timer, Stinger
- WinUpdatesList
- DB2 MAESTRO 8.4
- ORACLE MAESTRO 8.3
- SQL MAESTRO FOR MYSQL 8.3
- EMS SQL MANAGER 2007 FOR ORACLE 1.1
- EMS SQL MANAGER 2005 FOR POSTGRESQL 3.7
- EMS SQL MANAGER 2008 FOR SQL SERVER 3.0
- EMS SQL MANAGER 2007 FOR POSTGRESQL 4.3
- EMS SQL MANAGER 2008 FOR INTERBASE/FIREBIRD 5.0
- EMS SQL MANAGER FOR DBISAM 1.6
- MS SQL Maestro 8.1
- SQLite Maestro 8.5
- SQLite Data Wizard 8.4
- SQLite Code Factory 7.5
- SQLite PHP Generator 8.1
- Hash 1.04
- Navicat MySQL Manager for Linux 8.0.22

**Module 63: Forensics Frameworks**

- FORZA Framework
  - What is Forensics Framework?
  - Fundamental Principle in Digital Forensics Investigation Procedures
  - FORZA Framework
  - Roles and Responsibilities of Participants in Digital Forensics Investigation Procedures
  - Process Flow in FORZA Framework
  - High-level View of FORZA Framework
  - FORZA Framework Layers
  - Contextual Investigation Layer
  - Contextual Layer

- Legal Advisory Layer
- Conceptual Security Layer
- Technical Presentation Layer
- Data Acquisition Layer
- Data Analysis Layer
- Legal Presentation Layer

- An Event-Based Digital Forensic Investigation Framework
  - Event-based Framework
  - Digital Analysis Types
  - Digital Investigation Process Model
  - Digital Crime Scene Investigation Phases
- Enhanced Digital Investigation Process Model
  - Enhanced Digital Investigation Process Model
  - Physical Crime Scene Investigation
  - Digital Crime Scene Investigation
  - Phases of Enhanced Digital Investigation Process Model
- Extended Model of Cybercrime Investigations
  - Extended Model of Cybercrime Investigations
  - Activities in Cybercrime Investigations
- Computer Forensics Field Triage Process Model
  - Computer Forensics Field Triage Process Model
  - Computer Forensics Field Triage Process Model Phases
- Objectives-Based Framework for the Digital Investigations Process
  - Objectives-based Framework
  - Proposed Digital Investigation Process
  - Objectives-Based Framework Phases

**Module 64: Forensics Investigation Templates**

- Case Feedback Form
- Seizure Record
- List of Evidence Gathered Form
- Evidence Preservation Checklist
- BIOS Configuration
- System Configuration
- Application Summary
- Monitor Investigation Checklist
- Hard Disk Investigation Checklist

- Floppy Investigation Checklist
- CD Investigation Checklist
- Zip Drive Investigation Checklist
- Flash Drives Investigation Checklist
- Tape Investigation Checklist
- Handheld Device Investigation Checklist: Blackberry
- Handheld Device Investigation Checklist: iPod
- Handheld Device Investigation Checklist: Mobile Phone
- Handheld Device Investigation Checklist: PDA
- Fax Investigation Checklist
- Hub Investigation Checklist
- Switch Investigation Checklist
- Router Investigation Checklist
- Physical Security Checklist
- Identity Theft Checklist

**Module 65: Computer Forensics Consulting Companies**

- Burgess Forensics
- Center for Computer Forensics (CCF)
- Navigant Consulting
- ACR Data Recovery
- Computer Forensic Services
- Cyber Evidence Inc.
- Data Recon
- ADR (American Data Recovery) Computer Forensics
- Berryhill Computer Forensics, Inc.
- CIA Solutions
- Federal Bureau of Investigation (FBI)
- Interpol
- National Center for Missing and Exploited Children (NCMEC)
- Logicube
- Logicube: Screenshot
- LJ Forensics
- Intelligent Computer Solutions (ICS)
- Intelligent Computer Solutions (ICS): Screenshot
- Cy4or
- Forensicon

- Global Digital Forensics
- Integrity Security & Investigation Services, Inc. (ISIS)
- Trial Solutions
- Digital Detective
- Florida Department of Law Enforcement
- Northern California Computer Crimes Task Force (NC3TF)
- Child Exploitation and Online Protection Centre (CEOP)
- eFrauda
- International Association of Computer Investigative Specialists (IACIS)
- 7Safe
- Adroit Infotech Consultancy Service
- Digital Medix
- Hill Schwartz Spilker Keller LLC (HSSK)
- IRIS Data Services
- Computer Forensic Labs, Inc.

# Classroom Lecture Hours

| | |
|---|---|
| 30 Minutes | Module 01: Computer Forensics in Today's World |
| 30 Minutes | Module 02: Computer Forensics Investigation Process |
| 30 Minutes | Module 04: Digital Evidence |
| 30 Minutes | Module 05: First Responder Procedures |
| 30 Minutes | Module 06: Incident Handling |
| 1 Hour | Module 07: Computer Forensics Lab |
| 1 Hour 30 Minutes | Module 08: Understanding Hard Disks and File Systems |
| 30 Minutes | Module 09: Digital Media Devices |
| 1 Hour | Module 11: Windows Linux Macintosh Boot Process |
| 2 Hour | Module 12: Windows Forensics I |
| 1 Hour 30 Minutes | Module 13: Windows Forensics II |
| 1 Hour | Module 14: Linux Forensics |
| 1 Hour | Module 15: Mac Forensics |
| 1 Hour | Module 16: Data Acquisition and Duplication |
| 1 Hour | Module 17: Recovering Deleted Files and Deleted Partitions |
| 1 Hour | Module 18: Forensics Investigations Using AccessData FTK |
| 1 Hour | Module 19: Forensics Investigations Using Encase |
| 1 Hour | Module 20: Steganography |
| 30 Minutes | Module 21: Image Files Forensics |
| 30 Minutes | Module 24: Application Password Crackers |
| 1 Hour 30 Minutes | Module 25: Log Capturing and Event Correlation |
| 1 Hour | Module 26: Network Forensics and Investigating Logs |
| 30 Minutes | Module 27: Investigating Network Traffic |
| 1 Hour | Module 28: Router Forensics |
| 1 Hour | Module 29: Investigating Wireless Attacks |
| 1 Hour | Module 30: Investigating Web Attacks |
| 1 Hour | Module 31: Investigating DoS Attacks |
| 1 Hour | Module 33: Investigating Internet Crimes |
| 1 Hour | Module 34: Tracking Emails and Investigating Email crimes |
| 30 Minutes | Module 35: PDA Forensics |
| 30 Minutes | Module 36: Blackberry Forensics |
| 1 Hour | Module 37: iPpod and iPhone Forensics |
| 30 Minutes | Module 38: Cellphone Forensics |

| | |
|---|---|
| 30 Minutes | Module 41: Investigating Corporate Espionage |
| 30 Minutes | Module 43: Investigating Trademark and Copyright Infringement |
| 30 Minutes | Module 44: Investigating Sexual Harassment Incidents |
| 30 Minutes | Module 45: Investigating Child Pornography Cases |
| 30 Minutes | Module 50: Investigative Reports |
| 30 Minutes | Module 51: Becoming an Expert Witness |

# CHFI v4 Labs

## Module 01: Computer Forensics in Today's World (Lab time: 30 minutes)

**Lab 01 - 01:** Go through Computer Forensics whitepaper

**Lab 01 - 02:** Read 'An Introduction to Forensic Readiness Planning' whitepaper

**Lab 01 - 03:** Understand what computer forensics is

**Lab 01 - 04:** Understand Legal Methods of Using Computer Forensics Techniques for Computer Crime Analysis and Investigation

**Lab 01 - 05:** Read 'Information Technology Crimes' whitepaper

## Module 02: Computer Forensics Investigation Process (Lab time: 30 minutes)

**Lab 02 - 01:** Go through 'First Responders Guide to Computer Forensics' whitepaper

**Lab 02 - 02:** Understand Computer Forensics

**Lab 02 - 03:** Read 'Introduction to the Incident Response Process' whitepaper

**Lab 02 - 04:** Go through 'Computer Forensics - an approach to evidence in cyberspace' whitepaper

## Module 03: Searching and seizing of Computers (Self Do Labs)

**Lab 03 - 01:** Understand how to search and seize computers and data

**Lab 03 - 02:** Go through 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' whitepaper

## Module 04: Digital Evidence (Lab time: 30 minutes)

**Lab 04 - 01:** Read 'Forensic Examination of Digital Evidence A Guide for Law Enforcement' whitepaper

**Lab 04 - 02:** Go through 'Computer Forensics' whitepaper

**Lab 04 - 03:** Understand the Good Practice Guide for Computer Based Electronic Evidence

**Lab 04 - 04:** Go through 'Law Enforcement and Digital Evidence' whitepaper

**Lab 04 - 05:** Read 'Legal view of digital evidence' whitepaper

## Module 05: First Responder Procedures (Lab time: 30 minutes)

**Lab 05 - 01:** Go through 'Electronic Crime Scene Investigation A Guide for First Responders' whitepaper

**Lab 05 - 02:** Understand 'how to Collect Evidence from a Running Computer' whitepaper

**Lab 05 - 03:** Read 'An Introduction to Computer Forensics' whitepaper

**Lab 05 - 04:** Go through 'Best Practices for Seizing Electronic Evidence' whitepaper

**Lab 05 - 05:** Read 'First Responders Guide to Computer Forensics' whitepaper

## Module 06: Incident Handling (Lab time: 30 minutes)

**Lab 06 - 01:** Go through 'CSIRT Management' whitepaper

**Lab 06 - 02:** Read 'Handbook for Computer Security Incident Response Teams (CSIRTs)' whitepaper

**Lab 06 - 03:** Go through 'A Step-by-Step Approach on how to setup a CSIRT' whitepaper

**Lab 06 - 04:** Understand how to Respond to a Customer's security incidents

**Lab 06 - 05:** Go through 'CSIRT Services' whitepaper

## Module 07: Computer Forensics Lab (Lab time: 15 minutes)

**Lab 07 - 01:** Go through 'Equipping a Forensic Lab' whitepaper

**Lab 07 - 02:** Understanding the World of Forensics

**Lab 07 - 03:** Read 'Computer Forensics' whitepaper

## Module 08: Understanding Hard Disks and File Systems (Lab time: 45 minutes)

**Lab 08 - 01:** Use WinHex which is a universal hexadecimal editor, for data recovery, and low-level data processing.

**Lab 08 - 02:** Understand NTFS and FAT32 File Systems

**Lab 08 - 03:** Understand how to Analyze the hidden data in NTFS file system

**Lab 08 - 04:** Go through 'Linux File Systems' whitepaper

**Lab 08 - 05:** Understanding Disk Geometries

**Lab 08 - 06:** Understanding RAID Levels

## Module 09: Digital Media Devices (Lab time: 15 minutes)

**Lab 09 - 01:** Read 'DVDs' whitepaper

**Lab 09 - 02:** Understand the Performance of SDHC Flash Memory Card

**Lab 09 - 03:** Go through 'Drop Proofing a Hard Disk Drive' whitepaper

## Module 10: CD & DVD Forensics (Self Do Labs)

**Lab 10 - 01:** Go through 'CD- and DVD-Technology' whitepaper

**Lab 10 - 02:** Understand the CD and DVD Formats

**Lab 10 - 03:** Read 'Corrupted DVD's-An emerging forensic problem which may constitute untrustworthy evidence' whitepaper

**Lab 10-04:** Understand the Making Sense of DVD Formats "Plus" and "Dash (Minus)"

## Module 11: Windows, Linux, Macintosh Boot Process (Lab time: 30 minutes)

**Lab 11 - 01:** Understand how to Manage the Boot Process

**Lab 11 - 02:** Go through 'XP_Chapter4' whitepaper

**Lab 11 - 03:** Understand the Linux Boot Process

**Lab 11 - 04:** Read 'BootX' whitepaper

## Module 12: Windows Forensics I (Lab time: 1 Hr)

**Lab 12 - 01:** Use “Cache monitor” to monitor the cache of the IE

**Lab 12 - 02:** Use “Dependency Walker” to list the imported and exported functions of a portable executable file

**Lab 12 - 03:** Use “Metadata Analyzer” to analyze the metadata hidden in the word documents

**Lab 12 - 04:** Use “Metaviewer” to view the metadata hidden in the word documents

**Lab 12 - 05:** Use “Openports” to get open port information, type of the connection, process ID and process name, local and remote port numbers, remote connection IP and state

**Lab 12 - 06:** Use “Pmdump” to dump the memory contents of a running process to a file

**Lab 12 - 07:** Use “Promqry” to detect network interfaces that are running in promiscuous mode

**Lab 12 - 08:** use “Pslist” to detect network interfaces that are running in promiscuous mode

**Lab 12 - 09:** Use “Psloggedon” to detect network interfaces that are running in promiscuous mode

**Lab 12 - 10:** Use “Tlist” to determine the Process ID

**Lab 12 - 11:** Use “IE Cache View” to read the Internet Explorer cache

## Module 13: Windows Forensics II (Lab time: 1 Hr)

**Lab 13 - 01:** Go through ‘forensic-analysis-Windows-registry’ whitepaper

**Lab 13 - 02:** Read the ‘registry_examination’ whitepaper

**Lab 13 - 03:** Go through ‘Forensic analysis of the Windows registry in memory’ whitepaper

**Lab 13 - 04:** Understand how to Preserve Live Digital Evidence on Windows

**Lab 13 - 05:** Run and explore various features of Helix

**Lab 13 - 06:** Use “OLLYDBG” for binary code analysis

**Lab 13 - 07:** Use “RegScanner” to scan the Registry and find the desired Registry values

**Lab 13 - 08:** Use “Scaner” to fetch specific information about the processes

**Lab 13 - 09:** Use “GetDataBack for NTFS” to recover lost or damaged data from NTFS drives

## Module 14: Linux Forensics (Lab time: 30 minutes)

**Lab 14 - 01:** Understand the Beginners Guide to Linux Forensics

**Lab 14 - 02:** Go through ‘Digital Forensics using Linux and Open Source Tools’ whitepaper

**Lab 14 - 03:** Read ‘Forensics with Linux’ whitepaper

**Lab 14 - 04:** Go through ‘Using Linux for Incident Response & Data Forensics’ whitepaper

**Lab 14 - 05:** Read ‘unix_linux_forensics’ whitepaper

## Module 15: Mac Forensics (Lab time: 30 minutes)

**Lab 15 - 01:** Go through ‘macforensics’ whitepaper

**Lab 15 - 02:** Read the ‘Mac Forensics1’ whitepaper

**Lab 15 - 03:** Understand MacForensicsCraiger

**Lab 15 - 04:** Go through ‘mac security issues-rsc’ whitepaper

## Module 16: Data Acquisition and Duplication (Lab time: 30 minutes)

**Lab 16 - 01:** Use "Mount Image Pro" to mount the image of the drives and acquire the required data from the image

**Lab 16 - 02:** Understand the DAQbasics

**Lab 16 - 03:** Go through 'imbalance-kolcz' whitepaper

**Lab 16 - 04:** Read 'Aspects of data acquisition' whitepaper

## Module 17: Recovering Deleted Files and Deleted Partitions (Lab time: 1 Hr)

**Lab 17 - 01:** Use "BadCopy Pro" to recover and rescue corrupted or lost data from damaged, unreadable, formatted or defective disks

**Lab 17 - 02:** Use "DiskInternals Uneraser" to recover any deleted file, including documents, photos, mp3 and zip files, or even folders and damaged disks

**Lab 17 - 03:** Use "IsoBuster" to rescue lost files from a bad or trashed CD or DVD or a Blu-Ray disc

**Lab 17 - 04:** Use "ThumbsDisplay" for examining and reporting the contents of Thumbs.db files used by Windows

**Lab 17 - 05:** Use "O&O UnErase tool" for the restoration of deleted data

**Lab 17 - 06:** Use "PC Inspector File Recovery tool" to reconstruct the damage files that might be deleted due to abnormal system shutdown, through computer virus, and so on

**Lab 17 - 07:** Use "PC Inspector Smart Recovery tool" to recover accidentally deleted or formatted pictures, videos or sound files from the selected media

**Lab 17 - 08:** Use **"**Recover My Files" tool to recover deleted files and formatted or corrupt drives

**Lab 17 - 09:** Use the tool "Restoration" to restore the files that are deleted from the recycle bin or deleted while holding down the Shift key.

**Lab 17 - 10:** Use "Restorer2000" for data recovery and disk restoration functionality

**Lab 17 - 11:** Use "R-Undelete" to undelete files on a valid logical disk visible by the host OS when files were: removed without Recycle Bin; removed by virus attack or power failure

**Lab 17 - 12:** Use "Search and Recover" tool to recover deleted files

**Lab 17 - 13:** Use **"**Zero Assumption Recovery" for data recovery

**Lab 17 - 14:** Use "ReviveR" to recover deleted files even if the files were deleted from the recycle bin

**Lab 17 - 15:** Use "Active @ UNERASER" to recover deleted files and folders on FAT12, FAT16, FAT32 and NTFS file systems

**Lab 17 - 16:** Understand how-to-recover-deleted-files

**Lab 17 - 17:** Read the "An Integrated Approach to Recovering Deleted Files from NAND Flash Data" whitepaper

## Module 18: Forensics Investigations Using AccessData FTK (Lab time: 30 minutes)

**Lab 18 - 01:** Understand the AccessData Forensic Toolkit

**Lab 18 - 02:** Go through 'FORENSIC TOOLKIT® 2.1.0' whitepaper

**Lab 18 - 03:** Read 'Test Results for Digital Data Acquisition Tool FTK Imager 2.5.3.14' whitepaper

## Module 19: Forensics Investigations Using Encase (Lab time: 30 minutes)

**Lab 19 - 01:** Go through 'NIST Computer Security Incident Handling Guide' whitepaper

**Lab 19 - 02:** Read the 'Test Environment and Procedures for Testing EnCase 3.20' whitepaper

## Module 20: Steganography (Lab time: 1 Hr)

**Lab 20 - 01:** Use "StegoMagic" to hide any file or message in TEXT, WAV, BMP 24 bit and BMP 256 Color files

**Lab 20 - 02**: Use "StegSpy" to identify the hidden message in a file

**Lab 20 - 03**: Use "wbStego tool" to hide any file in certain carrier file using Steganography

**Lab 20 - 04**: Use "Steganos Security Suite" to protect the sensitive data

**Lab 20 - 05**: Use "Fort Knox" tool for hiding, securing files and folders, password protection lock and logon password masking

**Lab 20 -06**: Use "StegaNote" to protect the sensitive data by hiding the information in images

**Lab 20 - 07**: Use "JPHS" program to hide a file in a jpeg visual image

**Lab 20 - 08**: Use "ImageHide" to hides loads of text in images

**Lab 20 - 09**: Use "S-Tools" to hide multiple applications in a single object

**Lab 20 - 10**: Use "Invisible Secret" encrypts and hides data and files for secure transfer across the net.

**Lab 20 - 11**: Use "Blindside" tool to hide files of any file type within a Windows bitmap image

**Lab 20 - 12**: Use "Hermetic Stego" to hide a message file in a single BMP image or in a set of BMP images

**Lab 20 - 13**: Use "Masker" tool to encrypt the files and hide files and folders in a carrier file

**Lab 20 - 14**: Use "Steghide" tool to hide data in various kinds of image and audio-files

**Lab 20 - 15**: Use "2mosaic" tool to break a watermark

**Lab 20 - 16**: Use "jpegx" tool to encrypt and hide messages in jpeg files

**Lab 20 - 17:** Use "Camera/Shy" tool to encrypt text with a click of the mouse and bury the text in an image

**Lab 20 - 18**: Use CryptoBola tool to determine which parts (bits) of the JPEG-encoded data play the least significant role in the reproduction of the image

**Lab 20 - 19**: Use "Mp3stego" tool to hide information in MP3 files during the compression process

**Lab 20 - 20**: Use "gifshuffle" tool to conceal messages in GIF images by shuffling the colormap

**Lab 20 - 21:** Use "wnstorm" tool to encrypt files

**Lab 20 - 22:** Use "Steganos" to create several profiles for different users with steganos password manager

**Lab 20 - 23:** Go through 'An Encrypto- Stego Technique Based Secure Data Transmission System' whitepaper

**Lab 20 - 24:** Understand An Evaluation of Image Based Steganography Methods

**Lab 20 - 25:** Read 'Steganography and Digital Watermarking' whitepaper

## Module 21: Image Files Forensics (Lab time: 45 minutes)

**Lab 21 - 01:** Use "AD Picture Viewer" to view, print, organize and catalogue image collections

**Lab 21 - 02:** Use "FastStone Image Viewer" for image viewing, management, comparison, red-eye removal, emailing, resizing, cropping, color adjustments.

**Lab 21 - 03:** Use "Hex Workshop" to advance binary editing

**Lab 21 - 04**: Use "XnView" to view and convert graphic files

**Lab 21 - 05:** Use "Picture Viewer Max" locate, view, edit, print, organize, and send/receive picture/image files over the Internet.

**Lab 21 - 06:** Use "PhotoZoom" to create image enlargements of unequalled quality up to 1 million by 1 million pixels

**Lab 21 - 07:** Read 'A forensic image processing environment for investigation of surveillance video' whitepaper

**Lab 21 - 08:** Go through 'Forensic Image Analysis of Familiar-based iPAQ' whitepaper

**Lab 21 - 09:** Read 'Recovering Image Files' whitepaper

## Module 22: Audio File Forensics (Self Do Labs)

**Lab 22 - 01:** Understand Open-Standard File Format

**Lab 22 - 02:** Go through 'Audio forensics' whitepaper

**Lab 22 - 03:** Go through 'Digital Audio forensics' whitepaper

**Lab 22 - 04:** Understand DigitalAudio_Background

## Module 23: Video File Forensics (Self Do Labs)

**Lab 23 - 01:** Go through 'dTective' whitepaper

**Lab 23 - 02:** Understand Forensic Enhancement Software

**Lab 23 - 03:** Read the 'Forensic Tape Services' whitepaper

**Lab 23 - 04:** Understand Forensic Video Decisions

## Module 24: Application Password Crackers (Lab time: 45 minutes)

**Lab 24 - 01**: Use "PicoZip Recovery Tool" to recover lost or forgotten passwords from password protected Zip files

**Lab 24 - 02:** Use "SID & User" to get the SID of a given account name

**Lab 24 - 03:** Use "Asterisk Logger" to reveal the password inside the password-box, and add a record to passwords list in the main window

**Lab 24 - 04:** Use "Asterisk Key" to reveal the passwords hidden under the asterisks

**Lab 24 - 05:** Use "BRUTUS" to crack online password for Windows, HTTP, POP3, FTP, SMB, Telnet etc.

**Lab 24 - 06:** Use "Cain & Abel" to recover passwords for Microsoft Operating Systems

**Lab 24 - 07:** Use "CHAOS generator" to generate passwords of any length and character content

**Lab 24 - 08:** Use "LCP" for auditing and recovering passwords in Windows NT/2000/XP/2003

**Lab 24 - 09:** Use "Ophcrack" to crack Windows Password passwords on Rainbow Tables

**Lab 24 - 10:** Use "RockXP" to retrieve password

**Lab 24 - 11:** Read the 'Cracking –sql-passwords' whitepaper

**Lab 24 - 12:** Go through 'Advances in password cracking' whitepaper

**Lab 24 - 13:** Read the 'Password Cracking and Sniffing' whitepaper

**Lab 24 - 14:** Understand Password Cracking in the Field

## Module 25: Log Capturing and Event Correlation (Lab time: 45 minutes)

**Lab 25 - 01:** Use "Firewall Analyzer" for log analysis of Firewall, Proxy server, IDS/IPS, and VPN devices

**Lab 25 - 02:** Read 'VeriSign Log Management Service' whitepaper

**Lab 25 - 03:** Understand Benefits of Centralized Log file Correlation

**Lab 25 - 04:** Read the 'Log_Consolidation_and_Event_Management' whitepaper

## Module 26: Network Forensics and Investigating Logs (Lab time: 30 minutes)

**Lab 26 - 01:** Understand logging

**Lab 26 - 02:** Go through 'Policies to Enhance Computer and Network' whitepaper

**Lab 26 - 03:** Read 'Breaching Trust' whitepaper

## Module 27: Investigating Network Traffic (Lab time: 45 minutes)

**Lab 27 - 01:** Use "AnalogX PacketMon" to capture IP packets that pass through the network interface

**Lab 27 - 02:** Use "BillSniff" for detailed information about current traffic, as well as overall protocol statistics and more

**Lab 27 - 03:** Use "Colasoft MAC Scanner" for scanning MAC addresses and IP address in LAN

**Lab 27 - 04:** Use "CommView" for network monitoring and the analyzing

**Lab 27 - 05:** Use "EffeTech HTTP Sniffer" for network analyzing

**Lab 27 - 06:** Use "EtherDetect Packet Sniffer" for network analyzing

**Lab 27 - 07:** Use "Etherscan Analyzer" for network sniffing

**Lab 27 - 08:** Use "IP Sniffer" to built around a packet sniffer

**Lab 27 - 09:** Use "NetResident" for network content monitoring

**Lab 27 - 10:** Use "NetWitness" for threat analysis

**Lab 27 - 11:** Use "Sniphere" for network sniffing

**Lab 27 - 12:** Go through 'Investigating Multi-Fractality of Network Traffic' whitepaper

**Lab 27 - 13:** Read the 'Chasing Errors through the Network Stack' whitepaper

**Lab 27 - 14:** Understand IP Network Traffic an Investigation

## Module 28: Router Forensics (Lab time: 30 minutes)

**Lab 28 - 01:** Read 'Effective Data Investigation on Cisco Routers' whitepaper

**Lab 28 - 02:** Go through 'A Scalable Method for Router Attack Detection and Location in Link State Routing' whitepaper

**Lab 28 - 03:** Read 'Internet Infrastructure Security' whitepaper

**Lab 28 - 04:** Understand routingprotocols

## Module 29: Investigating Wireless Attacks (Lab time: 30 minutes)

**Lab 29 - 01:** Go through 'An Investigation of Unauthorised Use of Wireless Networks' whitepaper

**Lab 29 - 02:** Read 'Using Nessus to Detect Wireless Access Points' whitepaper

**Lab 29 - 03:** Read the 'Wireless Networking for International Safeguard-INMM' whitepaper

**Lab 29 - 04:** Read 'wp_wireless-intrusion-detection' whitepaper

## Module 30: Investigating Web Attacks (Lab time: 45 minutes)

**Lab 30 - 01:** Use "Acunetix Web Scanner" to encrypt and hide the data and files for secure transfer across the net

**Lab 30 - 02:** Use "Emsa Web Monitor" for web monitoring

**Lab 30 - 03:** Use "Whois" to determine the registrant or assignee of Internet resources, such as a domain name, an IP address, or an autonomous system number

**Lab 30 - 04:** Go through 'A new taxonomy of web attacks suitable for efficient encoding' whitepaper

**Lab 30 - 05:** Understand Techniques for Large-Scale Automatic Detection of Web Site Defacements

**Lab 30 - 06:** Read the 'Top Ten Web Attacks' whitepaper

**Lab 30 - 07:** Go through 'Web application attacks Learning Guide' whitepaper

## Module 31: Investigating DoS Attacks (Lab time: 45 minutes)

**Lab 31 - 01:** Use "3d Traceroute" to visually monitor the Internet connectivity

**Lab 31 - 02:** Use "SmartSniff" to capture TCP/IP packet

**Lab 31 - 03:** Understand A Novel Packet Marketing Method in DDoS Attack Detection

**Lab 31 - 04:** Go through 'Deciphering Detection Techniques Part III Denial of Service Detection' whitepaper

**Lab 31 - 05:** Understand Distributed Denial of Service Attack Tools

**Lab 31 - 06:** Understanding the Various Types of Denial of Service Attack

## Module 32: Investigating Virus, Trojan, Spyware and Rootkit Attacks (Self Do Labs)

**Lab 32 - 01:** Use "TrojanHunter" to searchr and remove Trojans from system

**Lab 32 - 02:** Go through 'Detecting And Recovering From A Virus Incident' whitepaper

**Lab 32 - 03:** Read the 'Combating the Spyware menace Solutions for the Enterprise' whitepaper

**Lab 32 - 04:** Go through 'Tracking and Tracing Cyber Attacks' whitepaper

## Module 33: Investigating Internet Crimes (Lab time: 45 minutes)

**Lab 33 - 01:** Use "VisualRoute" to analyze Internet connection performance and diagnoses connectivity problems

**Lab 33 - 02:** Go through 'CYBER CRIMES' whitepaper

**Lab 33 - 03:** Understand how to Collect Evidence from Running Computer

**Lab 33 - 04:** Understand Cybercrime Investigation and Prosecution the Role of Penal and Procedural Law

**Lab 33 - 05:** Read 'Investigations Involving the Internet and Computer Networks' whitepaper

## Module 34: Tracking Emails and Investigating Email crimes (Lab time: 15 minutes)

**Lab 34 - 01:** Go through 'Experimental System for Malicious Email Tracking' whitepaper

**Lab 34 - 02:** Understand how to investigate email

**Lab 34 - 03:** Read 'Investigating Email with attachments' whitepaper

## Module 35: PDA Forensics (Lab time: 30 minutes)

**Lab 35 - 01:** Read 'Efficient Forensic Tools for Handheld Devices' whitepaper

**Lab 35 - 02:** Go through 'Guidelines on PDA Forensics sp800-72' whitepaper

**Lab 35 - 03:** Understand iPod Forensics

**Lab 35 - 04:** Read 'nist_pda_forensics' whitepaper

**Lab 35 - 05:** Read 'Forensic Image Analysis of Familiar-based iPAQ' whitepaper

## Module 36: Blackberry Forensics (Lab time: 15 minutes)

**Lab 36 - 01:** Read 'Forensic Examination of a RIM' whitepaper

**Lab 36 - 02:** Understand the relevance of RIM forensics

**Lab 36 - 03:** Read 'MOBILE DEVICE FORENSICS' whitepaper

## Module 37: Ipod and iPhone Forensics (Lab time: 15 minutes)

**Lab 37 - 01:** Read 'ipod forensics - forensically sound examination of an apple ipod' whitepaper

**Lab 37 - 02:** Go through 'The Security Newsletter' whitepaper

**Lab 37 - 03:** Understand iPhone processing

## Module 38: Cellphone Forensics (Lab time: 15 minutes)

**Lab 38 - 01:** Read 'Cell Phone Forensics' whitepaper

**Lab 38 - 02:** Go through 'Guidelines on Cell Phone Forensics' whitepaper

**Lab 38 - 03:** Read 'Overcoming Impediments to Cell Phone Forensics' whitepaper

## Module 39: USB Forensics (Self Do Labs)

**Lab 39 - 01:** Use "USBDeview" to list all USB devices that are currently connected to computer

**Lab 39 - 02:** Read 'Forensic Write Protection Guide' whitepaper

**Lab 39 - 03:** Go through 'Analysis of USB Flash Drives in a VirtualEnvironment' whitepaper

## Module 40: Printer Forensics (Self Do Labs)

**Lab 40 - 01:** Use Print Inspector to manage the print jobs queued to any shared printer

**Lab 40 - 02:** Read 'A survey of forensic characterization methods for physical devices' whitepaper

**Lab 40 - 03:** Go through 'Printer Profiling for Forensics and Ballistics' whitepaper

## Module 41: Investigating Corporate Espionage (Lab time: 30 minutes)

**Lab 41 - 01:** Use "Activity Monitor" to track network activity

**Lab 41 - 02:** Use "Spy Sweeper" to block and remove spyware

**Lab 41 - 03:** Use "Spyware Terminator" to remove or quarantine spyware, adware, Trojans, keyloggers, home page hijackers, and other malware threats

**Lab 41 - 04:** Read 'Coporate_Espionage' whitepaper

## Module 42: Investigating Computer Data Breaches (Self Do Labs)

**Lab 42 - 01:** Read 'Data Breach' whitepaper

**Lab 42 - 02:** Go through 'Application Auditing Guidelines for investigating internal data breaches' whitepaper

**Lab 42 - 03:** Understand breach-procedures

## Module 43: Investigating Trademark and Copyright Infringement (Lab time: 15 minutes)

**Lab 43 - 01:** Read 'basics-of-copyright-infringement' whitepaper

**Lab 43 - 02:** Go through 'online_filesharing' whitepaper

**Lab 43 - 03:** Read 'Copyright_Infringement_Litigation' whitepaper

## Module 44: Investigating Sexual Harassment Incidents (Lab time: 15 minutes)

**Lab 44 - 01:** Read 'JBB Sexual Harassment' whitepaper

**Lab 44 - 02:** Go through 'sexual_harassment' whitepaper

**Lab 44 - 03:** Read 'GuidelinesforSexualHarassment' whitepaper

## Module 45: Investigating Child Pornography Cases (Lab time: 15 minutes)

**Lab 45 - 01:** Read 'Pornography' whitepaper

**Lab 45 - 02:** Understand probable cause and issues in child pornography cases

**Lab 45 - 03:** Read 'Child Pornography Patters From NIBRS' whitepaper

## Module 46: Investigating Identity Theft Cases (Self Do Labs)

**Lab 46 - 01:** Read 'Online ID theft techniques, investigation' whitepaper

**Lab 46 - 02:** Read 'Internet Identity Theft' whitepaper

**Lab 46 - 03:** Read 'Phishing-dhs-report' whitepaper

## Module 47: Investigating Defamation over Websites and Blog Postings (Self Do Labs)

**Lab 47 - 01:** Read 'European Blog Influencer Barometer with Ipsos MORI' whitepaper

**Lab 47 - 02:** Read 'Boudreau Speaking on Blogging' whitepaper

**Lab 47 - 03:** Understand what is the Blogosphere?

**Lab 47 - 04:** Read 'To Blog or Not To Blog' whitepaper

**Lab 47 - 05:** Read 'Five Golden Rules for Blogger Relations' whitepaper

## Module 48: Investigating Social Networking Websites for Evidence (Self Do Labs)

**Lab 48 - 01:** Read 'Identity Theft' whitepaper

**Lab 48 - 02:** Read 'Lessons from Facebook' whitepaper

**Lab 48 - 03:** Read 'social_networking_the_basics' whitepaper

**Lab 48 - 04:** Go through 'The Business Impacts of Social Networking' whitepaper

**Lab 48 - 05:** Understand what a community is

## Module 49: Investigation Search Keywords (Self Do Labs)

**Lab 49 - 01:** Go through 'TheArtOfKeywordSearching' whitepaper

**Lab 49 - 02:** Read the 'High Speed Bitwise Search for Digital Forensic System' whitepaper

**Lab 49 - 03:** Go through 'Case-Relevance Information Investigation Binding Computer Intelligence to the Current Computer Forensic Framework' whitepaper

## Module 50: Investigative Reports (Lab time: 15 minutes)

**Lab 50 - 01:** Read 'Scientific Working Group on Digital Evidence' whitepaper

**Lab 50 - 02:** Read 'databreachreport' whitepaper

**Lab 50 - 03:** Read 'Forensic report' whitepaper

## Module 51: Becoming an Expert Witness (Lab time: 15 minutes)

**Lab 51 - 01:** Go through 'Expert Witness_module' whitepaper

**Lab 51 - 02:** Read 'EXPERTWITNESS' whitepaper

**Lab 51 - 03:** Read 'Court Critique of Expert Witness Testimony' whitepaper

## Module 52: How to Become a Digital Detective (Self Do Labs)

**Lab 52 - 01:** Go through 'Digital Detective Has Crime Lab In Case' whitepaper

**Lab 52 - 02:** Read 'Digital detective – Bluetooth' whitepaper

## Module 53: Computer Forensics for Lawyers (Self Do Labs)

**Lab 53 - 01:** Go through 'computer forensics for attorneys' whitepaper

**Lab 53 - 02:** Read 'computer_forensics_what_attorneys_should_know' whitepaper

**Lab 53 - 03:** Read 'ForensicLifeCycleWhitePaper' whitepaper

## Module 54: Law and Computer Forensics (Self Do Labs)

**Lab 54 - 01:** Go through 'Computer Forensics' whitepaper

**Lab 54 - 02:** Read 'Computer Forensics For Law Enforcement' whitepaper

## Module 55: Computer Forensics and Legal Compliance (Self Do Labs)

**Lab 55 - 01:** Go through 'Compliance and Computer Forensics' whitepaper

**Lab 55 - 02:** Read 'Creating an effective compliance and ethics program to prevent and detect employee misconduct' whitepaper

**Lab 55 - 03:** Read 'Information Security Compliance' whitepaper

**Lab 55 - 04:** Read 'Pedagogic Overview of Compliance Training' whitepaper

## Module 56: Security Policies (Self Do Labs)

**Lab 56 - 01:** Go through 'info_security_policy' whitepaper

**Lab 56 - 02:** Read 'Information Security' whitepaper

**Lab 56 - 03:** Read 'secpolicy' whitepaper

**Lab 56 - 04:** Go through 'security-policy' whitepaper

**Lab 56 - 05:** Read 'wcsu_security_policy_1007' whitepaper

## Module 57: Risk Assessment (Self Do Labs)

**Lab 57 - 01:** Go through 'Information Security Risk Assessment' whitepaper

**Lab 57 - 02:** Read 'Risk Assessment and Risk Management Methods' whitepaper

**Lab 57 - 03:** Read 'Five steps to risk assessment' whitepaper

**Lab 57 - 04:** Go through 'Risk Management Guide for Information Technology Systems sp800-30' whitepaper

**Lab 57 - 05:** Read 'General Security Risk Assessment Guideline' whitepaper

## Module 58: Evaluation and Certification of Information System (Self Do Labs)

**Lab 58 - 01:** Go through 'Information System Certification and Accreditation Process' whitepaper

**Lab 58 - 02:** Understand information systems audit

**Lab 58 - 03:** Read 'Making the Evaluation of Information Systems Insightful' whitepaper

**Lab 58 - 04:** Go through 'Management Planning Guide for Information Systems Security Auditing' whitepaper

**Lab 58 - 05:** Read 'Methodological Recommendations for Information Systems Audit' whitepaper

## Module 59: Ethics in Computer Forensics (Self Do Labs)

**Lab 59 - 01:** Go through the topic Ethics in 'computer foransics' whitepaper

**Lab 59 - 02:** Understand the goals of ethics education in Information Assurance

**Lab 59 - 03:** Read 'Computer Forensics An Essential Ingredient for Cyber Security' whitepaper

## Module 60: Computer Forensic Tools (Self Do Labs)

**Lab 60 - 01:** Use "Belkasoft RemovEx" Pro to disable Internet Explorer and Windows Explorer plugins

**Lab 60 - 02**: Use "Cookie Viewer" to discover the information that web sites store on computer

**Lab 60 – 03:** Use The 'Decode - Forensic Date/Time Decoder' utility to decode the various date/time values found embedded within binary and other file types

**Lab 60 - 04**: Use "NetAnalysis" to automatically rebuild HTML web pages from an extracted cache, automatically adding the correct location of the graphics

**Lab 60 - 05**: Use "Port Explorer" to view all the open network ports/sockets on the system

**Lab 60 - 06**: Use R-Undelete to recover deleted file from for FAT and NTFS file systems

**Lab 60 – 07:** Use R-Wipe & Clean to wipe useless files and keep computer privacy

**Lab 60 – 08:** Use Intelli-SMART for storage fault tolerance

**Lab 60 – 09:** Use "Photorecovery" to recover images, movies, and sound files from all types of digital media

**Lab 60 - 10**: Use Process Explorer tool to get information about DLL processes

**Lab 60 – 11:** Use PowerGREP to search through large numbers of files on PC or network, including text and binary files, compressed archives, MS Word documents, Excel spreadsheets and PDF files

**Lab 60 – 12:** Use "PE Explorer" tool for inspecting the inner workings of user software, third party application and libraries for which user do not have source code

**Lab 60 - 13**: Use "R-Studio" to undelete and data recovery software recovering from FAT12/16/32, NTFS, NTFS5, HFS/HFS+ (Macintosh), Little and Big Endian variants of UFS1/UFS2

**Lab 60 - 14**: Use E-mail Examiner to recover active and deleted mail messages

**Lab 60 - 15**: Use Visual TimeAnalyzer to tracks all computer usage and presents detailed, richly illustrated reports

**Lab 60 - 16**: Use Directory Snoop to snoop FAT and NTFS formatted disk drives to see the data hidden in the cracks and recover deleted files

**Lab 60 - 17**: Use ScanDiskRescuePRO to recover images, documents, mail, video, and music

**Lab 60 - 18**: Use R-Word tool designed reconstruct damaged Microsoft Word documents

**Lab 60 - 19**: Use "FileRecovery Pro" to scan and find lost partitions, boot sectors and other file system components

**Lab 60 - 20**: Use "Datalifter" to recover lost images from erased or corrupted media cards

**Lab 60 - 21**: Use "Autoruns" to get the programs configured to run during system boot-up or login, and the entries in the order Windows processes them

## Module 61: Windows Based Command Line Tools (Self Do Labs)

**Lab 61 - 01:** Use LADS (List Alternate Data Streams) to list the name and size of every alternate data stream (ADS)

**Lab 61 - 02:** Use MACMatch to search for files by their last write, last access or creation time without changing any of these times

**Lab 61 - 03:** Use "Setowner" for setting the owner of a file or series of files in a directory

**Lab 61 - 04:** Use "Uptime" to measure the time of a computer system

**Lab 61 - 05:** Use "AccExp" to expire user accounts

**Lab 61 - 06**: Use "Auth" to test authentication of a user id

**Lab 61 – 07:** Use "Find NBT" to scan a subnet looking for Windows PCs

**Lab 61 - 08:** Use "FindPDC" to find the PDC of a domain

**Lab 61 – 09:** Use "GetUserInfo" to retrieve info about user accounts from Windows machines

**Lab 61 - 10:** Use "LG" to manage built-in, local groups, and domain local groups

**Lab 61 – 11:** Use "Mirror" to mirror two directories with sub-structures

**Lab 61 - 12:** Use "NBTScan" to scan NETBIOS devices on a local or remote TCP/IP network

**Lab 61 - 13:** Use "ntfsinfo" to check the information regarding NTFS drives

**Lab 61 – 14:** Use "pwdump2" to check the pid of lsass automatically

**Lab 61 - 15:** Use "Windump" to view all the adapters from the network card

**Lab 61 - 16:** Use "WINEXIT" to logoff, shut down, poweroff, force, or reboot the system

## Module 62: Windows Based GUI Tools (Self Do Labs)

**Lab 62 - 01:** Use "HijackThis" to generate an in depth report of registry and file settings from a computer

**Lab 62 – 02**: Use "Handy Recovery" to recover files accidentally lost on MS Windows

**Lab 62 – 03:** Use "HD Tune" to check the health of your hard drive

**Lab 62 - 04**: Use "HD Tach" for random access read/write storage devices such as hard drives, removable drives (ZIP/JAZZ), flash devices, and RAID arrays

**Lab 62 – 05:** Use "IP2" to reveal your current Internet IP address, even if you are behind a router

**Lab 62 – 06:** Use the "Password Assistant" software tool to implement meaningful passwords for a secure password login

**Lab 62 – 07:** Use "Unstoppable Copier" for recovering files from scratched CD's or defective floppy/hard disks

**Lab 62 – 08:** Use WinArpSpoofer to manipulate the ARP table of another computer on a LAN

**Lab 62 – 09:** Use WinAudit to perform a detailed audit of the hardware and software configuration of your computer

**Lab 62 - 10**: Use "Disk Checker" for getting information on defective sectors numbers as well as the file name they belong to

**Lab 62 - 11**: Use "Process Explorer" to get the information about the processes that have been opened or loaded

**Lab 62- 12:** Use Data Life Guard Diagnostics for Windows to perform drive identification, diagnostics, and repairs on a WD FireWire, EIDE, or USB drive

**Lab 62 – 13:** Use ReSysInfo to view the information of BIOS information, CMOS, desktop, DirectX, drives, environment, fonts, keyboard, locale, machine & APM, main board, MCI, memory, mouse, multimedia, network, OpenGL, passwords, ports, printers & fax, processes, processor, video system

**Lab 62 - 14**: Use SNScan to detect the devices that are potentially vulnerable to SNMP related security threats

**Lab 62 - 15**: Use "Accessenum" to check who has what access to directories, files and Registry keys on your system

**Lab 62 - 16**: Use "BabyFTP Server" for anonymous access

**Lab 62 - 17**: Use "CommTest" to meet your various video tasks

**Lab 62 - 18**: Use “TCP View” for detailed listings of all TCP and UDP endpoints on your system

**Lab 62 - 19**: Use “Trout” for visual traceroute

## Module 63: Forensics Frameworks (Self Do Labs)

**Lab 63 - 01:** Go through ‘Framework for a Digital Forensic Investigation’ whitepaper

**Lab 63 - 02:** Read ‘PyFlag – An advanced network forensic framework’ whitepaper

# Module Briefing

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

**Module Brief:**

Computer forensic investigation determines the value of evidence at the crime scene and the related evidence that is held. The functions of forensic scientists include proper analysis of the physical evidence, providing expert testimony in court, and furnishing training in proper recognition, collection and preservation of physical evidence

The field of computer investigations and forensics is still in its developing stages. It plays a major role in tracking the cyber criminals. This module will introduce you to computer forensics in today's world. It discusses about various crimes prevailing, need for computer forensics, forensic readiness planning, Enterprise Theory of Investigation (ETI), and some of the most important problems and concerns that are faced by forensic investigators today.

### Module 02: Computer Forensics Investigation Process

**Module Brief:**

Securing the computer evidence is the process by which all information held on a computer is retrieved in order to aid an investigation. Investigation process helps you to perform appropriate analysis of the incident or crime took place.

This module describes the different stages involved in performing the investigation process. It deals with how to prepare for the investigation, how to collect, analyze, manage the case, how the investigation is done, the role of an expert witness, and how the reports should be presented in the courtroom. It provides a list of service providers for computer forensics.

### Module 03: Searching and Seizing of Computers

**Module Brief:**

Investigator need to search and seize the computer after the occurrence of the incident for gathering the evidence. It helps the investigator solve the case easily.

After the completion of this module, an investigator gets familiar with the searching and seizing of computers with and without warrant, post seizure issues, the electronics communications privacy act, electronic surveillance in communications networks, evidence, and authentication.

### Module 04: Digital Evidence

**Module Brief:**

Digital Evidence is the delicate information, which needs to be collected and preserved carefully. Now-a-days, the use of digital devices has increased drastically and thus the use of such digital devices in crime is more than the previous. Hence, the investigator needs to deal with the evidence collection and preservation of the evidence from the digital device.

This module will introduce you how to find the digital evidence from the computer system or any electronic devices that contain digital data in a forensically sound manner. It discusses the federal rules and international principles of computer evidence, and thus explains in detail about the digital evidence examination process.

### Module 05: First Responder Procedure

**Module Brief:**

First responder refers to the person who first arrives at the crime scene and accesses the victim's system once the incident has been reported. He/she may be a network/system administrator, law enforcement officer, or investigation officer.

The role of a system administrator is important in ensuring all aspects of network security and maintenance. He/she also plays a vital role in the incident of a computer used in a security incident or illegal act. Under no circumstances should anyone, except the forensic analysts, make any attempts to restore or recover the information from any computer system or device that holds electronic information. This module describes the first responder procedure which deals with the role of the first responder, collecting and preserving electronic evidence from the target computer system when an incident is reported.

### Module 06: Incident Handling

**Module Brief:**

Until a few years ago, the need for an incident response team within every organization was never given a serious thought. Since there is a lack of trained professionals who can respond to incidents and minimize the effects, organizations are opting for in-house incident response teams.

After completing this module, one can gain in-depth understanding the incident, types of incidents, incident reporting, incident response, incident handling, basic procedures in handling incidents, various CSIRTs present in the world, and more.

### Module 07: Computer Forensics Lab

**Module Brief:**

A Computer Forensics Lab is a designated location for conducting computer based investigation on collected evidences. It is totally an efficient computer forensics platform which is able to investigate any cyber crime events. In computer forensics lab, investigator analyzes media, audio, intrusion, and any type of cyber crime events obtained from the crime scene.

This module describes the requirements of a forensic investigation, such as the lab and the office. The lab is an important part of any forensic investigation. It lists out various complex and minute details, such as determining the physical layout of the lab, environmental conditions, and the lighting. It also highlights the importance of acquiring certification for an investigator. It showcases the need for a forensic workstation and the benchmark to select the best possible forensic workstation. It lists out the duties of the lab manager and staff, so that they help in smooth running of an investigation rather than being a hurdle.

### Module 08: Understanding File Systems and Hard Disks

**Module Brief:**

Hard disk is an important source of the information, by the point of view of the investigator. Thus, an investigator should know the structure and behavior of the hard disk. The data to be collected as the evidence from the hard disk has to be located and protected from perishing. Hence, all the necessary information about the hard disk should be known to the investigator. Also, the file system is important as the data storage and distribution in the hard disk is dependent on the file system used.

On completion of this module, investigator gets familiar with disk drive, types of hard disk interfaces, and understanding of file systems, disk partitions, and various hard disk evidence collector tools

### Module 09: Digital Media Devices

**Module Brief:**

Digital Evidence is delicate information which needs to be collected and preserved carefully. Now-a-days the use of digital devices is increased drastically and thus the use of such digital devices in crime is more than the previous. Hence, investigator needs to deal with the evidence collection and preservation of the evidences from the digital device.

This module will introduce you how to find the digital evidence from the computer system or any electronic devices that contains digital data in forensically sound manner. This module discusses about digital media devices such as: tapes, floppy disks, CDs, DVDs, iPods, flash memory cards, and USB flash drives.

### Module 10: CD & DVD Forensics

**Module Brief:**

A Compact Disc (CD) is a polycarbonate plastic or optical disk with one or more metal layers for storing digital data. It is a standard medium for distributing large quantities of information in a dependable package where a DVD, also called a “Digital Versatile Disc” or “Digital Video Disc”, is used for storing the digital data. It is capable of storing two hours of data, which is more when compared to that of a CD.

This module will familiarize you with compact disk, DVD, how criminal uses CDs and DVDs for crime, how to perform CD forensics, and various tools for performing CD/DVD imaging and data recovery.

### Module 11: Windows, Linux and Macintosh Boot Processes

**Module Brief:**

Booting is the process of loading an operating system into the computer's main memory or random access memory (RAM). Once the operating system is loaded, the computer is ready for users to run applications. This module describes the terminologies and basic booting process in Windows XP, Linux, and Mac OS X operating systems. It also emphasizes the various step by step booting processes for Windows Linux and Mac OS X.

### Module 12: Windows Forensics I

**Module Brief:**

When a Windows based system is investigated for gathering evidence and relevant facts, it involves several steps for collecting volatile data. Volatile data contains the current information about the machines, registers, caches, etc. This module familiarizes with the process of forensic investigation in Windows based environment. It also highlights the various tools that help in the investigation process to solve Windows crimes.

### Module 13: Windows Forensics II

**Module Brief:**

Windows operating system maintains the logs of the activities done by the user and also the changes taking place on the system. These logs are important by the point of view of the investigation as it shows the things which happened on the system and changes taken place. These logs are stored on specific location in the system, investigator should have knowledge of the system as it will help to extract the logs and use it as evidence.

This module explains about the text based logs and forensic analysis of the event based logs. It also covers the password issues encountered during the investigation.

**Module 14: Linux Forensics**

**Module Brief:**

Linux is an important and widely used Operating system. Many users opt for the Linux as it is free and is open source. Forensic investigator should know how to investigate the Linux system and where to search for the evidences. A detailed and good knowledge about the Linux system will help the investigator in the investigation process.

This module familiarizes with the Linux forensic investigation process. It discusses the analysis techniques such as Floppy Disk Analysis and Hard Disk Analysis. It also emphasizes several popular Linux tool kits that provide GUI as well for convenience and their search techniques.

**Module 15: Mac Forensics**

**Module Brief:**

Now-a-days Mac OS getting more and more popular among the user, and thus the use of the Mac system in crime is also increased. Thus it is important for the forensic investigator to have knowledge of the Mac system to investigate the cases which involves the Mac system.

This module gives the overall idea about the Mac OS and File System, Partitioning Schemes, Mac OS X Directory Structure, Pre-requisites for Mac Forensics, POSIX Permissions, Mac OS X Log Files, and Vulnerable Features of Mac. It also covers the imaging process involved in the Mac forensics and the tools which are useful for the investigation.

**Module 16: Data Acquisition and Duplication**

**Module Brief:**

Data acquisition is an important step in the investigation process. The data collected from the victim's system is presented as the evidence. So the data should be kept with the investigator and produced in the court while the trial is going on. Sometimes instead of data acquisition, duplication of the data is the best way to collect the data. Duplicated data can also be presented at the court.

This module deals with data acquisition and data duplication process which are the important aspects of the forensic investigation. It also highlights the popular tools required during the data acquisition and data duplication process.

**Module 17: Recovering Deleted Files and Deleted partitions**

**Module Brief:**

During the investigation of the computer system, investigator may come across a situation where the evidences of the crime are deleted from the system. In this case investigator should know how to recover the deleted files, which can be used as evidence. Deleted files and deleted partitions can be a good source of evidences which are useful to provide an important clue in the investigation.

This module covers the various methods in which a forensic investigator can recover the deleted files. It deals primarily with understanding the basic concept of recovering deleted files. The module also highlights the various data recovery tools and the salient features of these tools.

**Module 18: Forensics Investigations Using AccessData FTK**

**Module Brief:**

Encase is broadly used tool in the forensics. It helps in gathering and examining the evidences for the forensic investigation process. This module familiarizes with the topics such as, Forensic Toolkit(FTK), installation of FTK, starting with FTK, working with FTK, working with Cases, searching a Case, data

carving, using filters, decrypting encrypted files, working with reports, and customizing the interface. This module mainly highlights the working procedure and salient features of FTK.

### Module 19: Forensics Investigations Using Encase

**Module Brief:**

Encase is widely known and used tool in the forensics. It helps to collect and verify the evidences for the investigation process. This module covers the Evidence files, Verifying file integrity, Configuring Encase, Searching, and Bookmarks.

This module describes the complete process of forensic investigation using EnCase.

### Module 20: Steganography

**Module Brief:**

Steganography, the art of hidden writing, has been in use for centuries. It involves embedding a hidden message in some transport or carrier medium, and has been used by mathematicians, military personnel, and scientists. They all engage themselves in changing the common language and transferring it through secret and hidden communication.

The objective of this module is to make you familiar with the concept of steganography. This module covers the various methods in which steganography can be applied either legally or illegally. It discusses the early history and evolution of steganography, and highlights the various steganography tools that are used and the salient features of these tools as well.

### Module 21: Image Files Forensics

**Module Brief:**

In the investigation process the image files have important role. Image files can be presented as evidence in the court. It is important to recover the image files from the attacked computer and preserve it. Image files are very delicate and can be corrupted if it is not handled properly.

This module covers the various methods in which a forensic investigator can go about recovering image files. This module mainly deals with understanding the basic concept of recovering image files. This module also highlights the various image recovery, steganalysis, and viewing tools that are used in this process.

### Module 22: Audio File Forensics

**Module Brief:**

Audio forensics is the term that symbolizes the investigation of the audio files that are considered as evidence. It not only involves the collection of audio evidence, but also provides various methodologies in order to preserve, analyze, and enhance the original samples.

This module describes in detail about audio forensics, need for audio forensics, methodologies, audio forensic process, and the tools used for investigation.

### Module 23: Video File Forensics

**Module Brief:**

In most of the investigation cases, investigators get the evidence video which is blurred or underexposed. The role of the video forensics investigator is to make that video comprehensible. Investigators use special

techniques and tools to process the video and find out the details of the people and other investigative information.

This module familiarizes with the concept of video forensics which means taking recorded video and enhancing it to a point where detailed faces of people and other investigative information can be seen.

This module deals with the topics such as, video file forensics, need of video file forensics, video file formats, devices used for video forensics, video file forensics steps, etc.

### Module 24: Application Password Crackers

**Module Brief:**

A password cracker is an application program that is used to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a human cracker to obtain unauthorized access to resources.

This module deals with password crackers and tools used in the password recovery. It throws light on delicate concepts, such as ways to bypass BIOS passwords, remove CMOS batteries, and Windows XP/2000/NT keys. It also enumerates the BIOS password crackers and explains the passware kit. It also highlights topics such as the default password database and distributed network attacks.

### Module 25: Log Capturing and Event Correlation

**Module Brief:**

Computer security logs contain information about the events occurring within systems and networks. They contain various log entries and each entry contains information about a particular event that has occurred. This module familiarizes with computer security logs, logs and legal issues, and log management. It also discusses about the various log capturing and analysis tools and their salient features.

### Module 26: Network Forensics and Investigating Logs

**Module Brief:**

Attacks on corporate, government, academic, and other critical infrastructure networks are increasing in number, sophistication, and severity. Network forensics involves the investigation of all those components of the network where data resides or flow. Examination of each component of a network topology can give important information about an attack on network and its perpetrator.

This module explains how hardware such as Routers, switches, hubs etc and software as firewalls; traffic analyzers etc provide important information. This module will familiarizes with the topics such as, network forensics, network attacks, where to look for evidence, investigating logs, etc.

### Module 27: Investigating Network Traffic

**Module Brief:**

The module gives a brief overview of the network protocols and the four layers of the OSI model. Evidence gathering methodologies at the physical, data link, network, and transport protocol are explained. Evidence gathering method on a network has also been discussed. It also discusses the topics such as, 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 to investigate network traffic, and evidence gathering via sniffing.

### Module 28: Router Forensics

Router forensics does not differ much from traditional forensics except in some particular steps taken during investigations. During router investigations, the system needs to be online, whereas in traditional forensic investigations, the system needs to be powered off for conducting investigations. The reason behind this is that the router needs to be online so that the forensic investigator can have exact knowledge of what type of traffic is carried through the router.

This module describes the main concept of investigating routers to point out countermeasures that could possibly avoid future attacks. It covers the topics such as Routers, Router Logs, and Types of router attacks, Hacking Routers, and Router attack topology. It also emphasizes the router analyzer tools and salient features of these tools.

### Module 29: Investigating Wireless Attacks

**Module Brief:**

With the increase in the use of wireless network and wireless devices, there is an increase in the number of security issues. Wireless attacks became easy for attackers who are familiar with passive attack techniques resulting in loss of time and money of the company/organization.

This module familiarizes you with the types of wireless attacks and thus helping you in investigating those attacks. It covers the topics such as analyzing DHCP log files for issued MAC addresses, firewall logs for intrusions, and network logs for intrusion activities during investigating wireless networks. It also highlights the various scanning tools that are used.

### Module 30: Investigating Web Attacks

**Module Brief:**

Internet is a network that connects systems globally with the help of web pages. Web attacks are the attacks where these web pages are attacked to perform malfunctioning, thus leaving the users, lose their credentials.

This module covers the topics that give a clear understanding of web attacks investigation process such as indication of web attacks, types of web attacks, and how to deal with these attacks. It also highlights the tools that are helpful during the web attacks investigation process and salient features of these tools. The focus of this module is how to investigate web attacks and how to prevent systems from different types of web attacks.

### Module 31: Investigating DOS Attacks

**Module Brief:**

“DoS attack is type of network attack intended to make a computer resource inaccessible to its legitimate and authorized users by flooding the network by bogus traffic or disrupting connections.” This module describes denial-of-service attacks and how attackers explicitly attempt to prevent legitimate users of a service from using it. The attacker may target a particular server application (HTTP, FTP, ICMP, TCP etc) or the network as a whole. This module also familiarizes with the topics such as, indications of a DoS/DDoS attack, types of DoS attack, DDoS attack, working of DDoS attack, classification of DDoS attack, and detecting DoS attacks using Cisco NetFlow.

### Module 32: Investigating Virus, Trojan, Spyware and Rootkit Attacks

**Module Brief:**

This module familiarizes with the software programs such as viruses, which are meant to infect computer from one to another and interrupt in computer operations. This module helps in understanding the

characteristics and symptoms of virus or worm attack on the system and how to prevent for this using various virus detection methods. This module also highlights the various anti-virus and anti-Trojan tools and their salient features.

### Module 33: Investigating Internet Crimes

**Module Brief:**

Internet crimes are crimes committed over the Internet or by using the Internet. The executor or perpetrator commits criminal acts and carries out wrongful activities on the web in a variety of ways. Internet Forensics, which is the application of scientific and legally sound methods for the investigation of Internet crimes, whose focus ranges from an individual system to the Internet.

Forensics experts use a combination of advanced computing techniques and human intuition to uncover clues about people and computers involved in Internet crime. In Internet forensics, it is usually the case that forensics experts go through the same level of education and training as the hacker; but the difference is one of the morals, not skill. This module familiarizes with the topics such as Internet crimes, Internet forensics, and various Internet crime detection methods. It also highlights the Internet information gathering tools and features of these tools.

### Module 34: Tracking E-mails and Investigating E-mail Crimes

**Module Brief:**

Electronic communication is known for its global connectivity but cyber criminals exploit this unique feature. This module is intended to make you familiar with a subject that is currently a prime concern: email crime. The focus of this module is how to investigate email crime and what are the countermeasures to prevent it.

This module familiarizes you with Email System, Email Client, Email Server, Real Email System, Email Crime, Spamming, and Identity Fraud/Chain Letter.

### Module 35: PDA Forensics

**Module Brief:**

Personal Digital Assistants (PDA) is a lightweight and small mobile handheld device. Computer forensic investigators handling a PDA would need a basic understanding of the features of various types of PDA available in the market. They must take care in examining the PDA because any wrong step would lead to the loss of valuable and case-related information.

This module describes the basic understanding of PDA, its security issues, and various PDA forensics steps taken while PDA forensic investigation. It also highlights the forensic tools and their features that are helpful during investigation.

### Module 36: Blackberry Forensics

**Module Brief:**

Blackberry is a personal wireless handheld device that supports e-mail, mobile phone capabilities, text messaging, web browsing, and other wireless information services. This module familiarizes with topics such as Blackberry, Blackberry functions, and its security. It mainly focuses on ways of Collecting Evidence from Blackberry and how Blackberry investigation is carried. It also highlights the Signing Authority Tool which protects the data and intellectual property of the applications.

### Module 37: iPod and iPhone Forensics

**Module Brief:**

Like any other digital storage device, the iPod/ iPhone may hold incriminating evidence. In its native format, the iPod/ iPhone may contain calendar entries related to a crime or other event of interest. Additionally, contact information stored on the device may be relevant to an investigation. The iPod/ iPhone is also capable of creating voice recordings. As such, recordings of meetings may be recovered. Coupled with photographs or other substantiation the iPod/ iPhone could be a rich source of evidence to the investigator. With its large hard drive, the iPod/ iPhone is the ideal storage location for music that violates Copyright, and with the newer devices pornographic pictures.

This module discusses how iPod/ iPhone act as excellent alternate data storage option, its features, how to conduct forensic analysis on the data hidden within the device, how iPod/ iPhone forensic investigation is carried out, and how to avoid the misuse of iPod/ iPhone.

### Module 38: Cellphone Forensics

**Module Brief:**

The mobile phone or cellular phone is a short-range, electronic device used for mobile voice or data communication over a network of specialized base stations that are offered by various network providers. It is a personal device for an individual who uses it for his/her personal and professional purposes.

This module describes the cellphone features, necessity, its security issues, mobile forensics for recovering the digital evidence present in the device. It also highlights the tools and their features that help the investigator in solving the case.

### Module 39: USB Forensics

**Module Brief:**

Universal Serial Bus (USB) is the serial bus standard to interface device to a host computer. It is a plug-and-play interface between a computer and add-on devices such as audio players, joy sticks, scanners, printers, etc.,

This module familiarizes you with the USB, USB flash drive, and forensic investigation process for the USB. It provides the security issues against USB, how the attacker misuses the USB and also highlights about the forensic tools and their features hence solving the case easily.

### Module 40: Printer Forensics

**Module Brief:**

Printer is a computer peripheral that reproduces text, images, or any information on the paper or any other printable surface.

This module deals with the investigation of the printed documents. It briefly describes about printer forensics, different printing methods that are used for printing purpose, how the printing process is performed, how a particular printer can be identified from printed document, how the documents are examined, and different techniques and tools to identify and investigate on a printer.

### Module 41: Investigating Corporate Espionage

**Module Brief:**

Information gathered through espionage is generally confidential information that the source does not want to divulge or make public. Information can make or mar the success story of an organization in today's business world. There has been a buzz for a while about competitors stealing trade secrets and

other information to enhance their competitive edge. Companies all over the world are losing billions of dollars due to trade secret thefts. Losses due to corporate espionage are far more devastating than other technical and non-technical losses.

The Module "Investigating Corporate Espionage" will discuss various aspects of corporate espionage, spying detailed study about insider/outsider threat, netspionage, and strategies to prevent and investigate such cases.

### Module 42: Investigating Computer Data Breaches

**Module Brief:**

Data can be stolen using external memory devices that are available with a capacity of 64 MB to 250 GB. These external hard disks can be used to copy the complete hard disk data.

This module helps in understanding the cryptography and steganography technique used to send data avoiding data breaches. It mainly focuses on how to investigate and countermeasure data breaches.

### Module 43: Investigating Trademark and Copyright Infringement

**Module Brief:**

According to **www.legal-definitions.com** "*An infringement is the unauthorized use of another's right or privilege, usually an intellectual property right, such as a patent, copyright, or trademark*". A party that owns the rights to a particular trademark can sue other parties for trademark infringement based on the standard "*likelihood of confusion*".

This module discusses how trademark infringement, copyright infringement, and intellectual property theft can be investigated. It covers topics such as Trademark characteristics, Copyright Infringement, patent infringement, domain infringement, and different country laws for Trademarks and Copyright. DRM and also highlights several Plagiarism Detection Tools as well.

### Module 44: Investigating Sexual Harassment Incidents

**Module Brief:**

Sexual harassment is an unwelcomed sexual advancement prevailing in various places either verbally or physically. It is a kind of sexual behavior that is offensive to the victim and may cause harm to the victim physically, psychologically, and materially because such behavior is against the consent of the victim.

This module focuses on the topics such as sexual harassment, stalking, their types, responsibilities of supervisors and employees against harassment, investigating process, the laws against sexual harassment and stalking, and preventive measures to overcome these problems.

### Module 45: Investigating Child Pornography

**Module Brief:**

Child pornography is the serious crime prevailing on the Internet. It is the harassing act against the children where the adults are using them for their gratification. There is an increase in number of children who are accessing the Internet all over the world. Rapidly expanding computer technology and the Internet has given access to the production and distribution of the child pornography.

This module describes child pornography affects children physically, socially, and psychologically. It mainly focuses on how to prevent dissemination of child pornography, steps for investigating child pornography cases and laws against child pornography. It highlights the Internet filtering and monitoring guidelines and tools to protect children from accessing pornography. It also briefly describes the anti-child porn organizations

### Module 46: Investigating Identity Theft Cases

**Module Brief:**

Identity theft is the theft or unauthorized use of others' personal identifying information for fraudulent or unlawful activities.

This module familiarizes with the topics such as, identity theft, who commits identity theft, how criminals get information, techniques used by criminals, how a criminal uses information, investigating identity theft, identity theft laws, and protection from identity theft.

### Module 47: Investigating Defamation over Websites and Blog Posting

**Module Brief:**

Defamation is a false and unprivileged statement of fact that is harmful to someone reputation. It is published with fault meaning as a result of negligence or malice. It frames the negative image of any individual, business, product, group, government or nation.

This module familiarizes with defamation over websites and blog postings. It highlights the steps for investigating defamation over websites and blog postings.

### Module 48: Investigating Social Networking Websites for Evidence

**Module Brief:**

The social networking sites are the most rapidly growing phenomena on the Internet. This module helps in understanding the social networking sites that provide a good medium to place personal profiles, share their ideas, build the contacts, and provides a medium to build a network for the business. This module mainly focuses on the social networking websites that are increasingly used in legal and criminal investigations.

### Module 49: Investigating Search Keywords

**Module Brief:**

Keywords are also known as Seed Information as they are the starting point of the investigation. Keyword searching for terms relating to a case can be an important source for experts charged with uncovering digital clues in a forensic investigation. This module describes how experts frequently conduct keyword searches of active files, deleted files, unallocated space, cookies, logs, Temporary Internet Files, etc. to search for evidence. This module mainly highlights the keyword search techniques and various issues related to keyword search.

### Module 50: Investigative Reports

**Module Brief:**

This module will familiarize you with computer forensic report which provides detailed information on complete forensics investigation process. It can be prepared by the computer forensic investigator. This module explains how computer forensic investigator collects the complete information involved in the case, investigates them, and prepares the final report. It can be used to communicate the results of the forensic investigation. It can be used not only to present the facts but also to communicate expert opinion.

This module also highlights the topics such as, need of an investigative report, report specifications, report classification, layout of an investigative report, and guidelines for writing a report, best practices for investigators, writing report using FTK, etc.

### Module 51: Becoming an Expert Witness

**Module Brief:**

Expert witness is a person who is well skilled and has knowledge above an average person in particular areas such as forensics, medicine, allied health, aviation, and other fields required to facilitate in proving or disproving a case. This module discusses about expert witness, types of expert witnesses, and scope of expert witness testimony. It also deals with examining computer evidence and recognizing the deposing problems.

### Module 52: How to Become a Digital Detective

**Module Brief:**

Digital detective is an agency or person specialized in computer forensics and network security. Digital Detectives are trained experts to detect and investigate crimes ranging from crimes against children to file system recovery on computers that have been damaged or hacked. This module familiarizes with the topics such as, roles and responsibilities of digital detectives, traits of a digital detective, technical skills of digital detective, qualification of digital detectives, and wider competencies of a digital detective.

### Module 53: Computer Forensics for Lawyers

**Module Brief:**

The need for knowledge about electronic data with the experience grounded exclusively on paper discovery makes it hard for lawyers to meet the challenge of digital data discovery. The critical errors can be avoided in the first place if the lawyers gain a fundamental understanding of how a computer stores data and the file management system. This module mainly deals with what lawyers should know in the forensic process and the cases related computer forensics.

### Module 54: Law and Computer Forensics

**Module Brief:**

The objective of this module is to make you aware of the laws and acts that are related to cyber crime investigation. It introduces you to the Acts relating to cyber crime. The module concludes with a note on how to investigate a cyber crime.

### Module 55: Computer Forensics and Legal Compliance

**Module Brief:**

Private and confidential information used and shared without authorization, increases the possibility of identity theft and other unauthorized uses. This module describes about the regulatory compliance that refers to systems or departments at corporations and public agencies to ensure that personnel are aware of, and take steps to comply with relevant laws and regulations. It mainly highlights the principles of legal compliance, elements of an effective compliance program and compliance program structure.

### Module 56: Security Policies

**Module Brief:**

This Module familiarizes with access control policy, administrative security policies & procedures. This module also highlights the topics such as, audit trails and logging policies, documentation policy, evidence collection preservation policies, information security policy, National Information Assurance (IA) Certification and Accreditation ( C&A) Process Policy, etc.

**Module 57: Risk Assessment**

**Module Brief:**

Risk is a measure of possible inability to achieve a goal, objective, or target within a defined security, cost, plan, and technical limitations. It is a possibility of loss resulting from a hazard, security incident, or event. It adversely affects the organization's operations and revenues.

This module describes how organizations have to handle the possibility of risks and their consequences. In order to do so, they develop varied practices that suit the requirements of those organizations. This module helps in understanding the security planning that helps in managing and reducing the probability of risk.

**Module 58: Evaluation and Certification of Information Security**

**Module Brief:**

Accreditation is a process of obtaining certification to meet the minimum requirements needed by an accrediting agency. This process certifies the competency, authority, and credibility of an organization.

This module helps in understanding the concept of evaluation of certification of information security. It mainly focuses on the topic accreditation certificates that are issued by the certification specialists after testing every standard in laboratories in compliance with the established standards such as physical standards, chemical standards, forensic standards, quality standards, and security standards. This module also familiarizes with the topics such as, type Accreditation, Approval to Operate(ATO), System Security Authorization Agreement (SSAA), cost-benefit analysis, and Certification Test & Evaluation (CT&E).

**Module 59: Ethics in Computer Forensics**

**Module Brief:**

Ethics form a major part in the society and the computer world. Ethics refers to the behavior of a person in relation to a subject. It tells about the norms that distinguish between the acceptable and unacceptable behavior. Organizations implement policies to provide guidelines for ethics. This module helps in understanding the procedure to implement ethics and challenges in teaching computer forensics ethics.

**Module 60: Computer Forensic Tools**

**Module Brief:**

Cyber crime forensic investigation requires forensics hardware and software tools to collect the evidences in forensically sound manner. The objective of this module is to make you aware of the various computer forensic tools used in cyber crime investigation. This module provides information on computer forensics software and hardware tools that are important in forensic investigation.

**Module 61: Windows Based Command Line Tools**

**Module Brief:**

This module familiarizes with various Windows based command line tools and their salient features.

**Module 62: Windows Based GUI Tools**

**Module Brief:**

This module familiarizes with various Windows based graphical user interface tools and their salient features.

### Module 63: Forensics Frameworks

**Module Brief:**

This module familiarizes with various forensics frameworks based on fundamental principles in digital forensics investigation procedures.

### Module 64: Forensics Investigation Templates

**Module Brief:**

This module provides various forensics investigation templates that you can use during your forensic investigation assignments.

### Module 65: Computer Forensics Consulting Companies

**Module Brief:**

Burgess Forensics provides Computer Forensics, Electronic Discovery Services, as well as Expert Witness Testimony. This module familiarizes with a list of computer forensics consulting companies that provides services like, recovering files from damaged operating systems or hardware making forensic images or copies of originals, either at our offices or on site.

# CHFIv4 Course Objectives

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

- Discusses different aspects of organizational security
- Defines and discusses various terminologies related to computer forensics, forensic science, and cyber crimes
- Discusses the objectives and need for computer forensics
- Explains goals and benefits of Forensic Readiness and discusses Forensic Readiness Planning in detail
- Discusses various computer facilitated crimes, modes of attacks, types of computer crimes, and provide relevant examples of cyber crime
- Explains the key steps and rules in forensic investigation
- Discusses the need and role of the computer investigator
- Describes the role of digital evidence in forensic investigations and how to access computer forensics resources
- Explains different approaches to forensic investigation, where and when do you use computer forensics, and Enterprise Theory of Investigation (ETI)
- Discusses various legal issues and reports related to computer forensic investigations

### Module 02: Computer Forensics Investigation Process

- Provides an overview of computer crime investigation process
- Explains how to build a forensic workstation, investigating team, and computer investigation toolkit
- Describes computer forensic investigation methodology
- Discusses about how to notify decision makers and acquire authorization for computer forensic investigation
- Details the steps to prepare for a computer forensic investigation
- Describes the importance of forensic photography, and first responders in forensic investigation process
- Discusses how to collect and secure the evidence in a forensically sound manner
- Explains the techniques to acquire and analyze the data
- Describes evidence and case assessment
- Discusses how to prepare the final investigation report, and testify in the court as a expert witness

### Module 03: Searching and seizing of Computers

- Explains the legal issues involved in searching and seizing computers with and without a warrant
- Describes private searches, inventory searches, border searches, and workplace searches
- Discusses on searching and seizing computers with a warrant, successful search with a warrant, The Privacy Protection Act, Sneak-and-Peek Warrants, and Post-Seizure Issues

- Describes about The Electronic Communications Privacy Act, voluntary disclosure, electronic surveillance in communications networks, and other issues

**Module 04: Digital Evidence**

- Defines the digital data and various types of digital data
- Explains the measures to increase awareness of digital evidence
- Discusses digital evidence, evidence assessment, evidence preservation, and Chain-of-Custody
- Discusses challenging aspects of the digital evidence, and role and characteristics of the digital evidence
- Introduces with the federal rules of evidence
- Provides a checklist for handling and preserving digital evidence
- Explains techniques for evidence examination and analysis
- Provides an overview on evidence documentation and reporting, computer evidence worksheet, and electronic crime and digital evidence consideration by crime category

**Module 05: First Responder Procedures**

- Discusses the roles and responsibilities of first responder for securing and evaluating electronic crime scene
- Describes first responder tool kit and how to create it
- Explains how to conduct preliminary interviews
- Discusses how to document electronic crime scene
- Provides an overview on how to collect and store the electronic evidence
- Discusses electronic evidence packaging, evidence bag contents
- Explains how to transport electronic evidence
- Prepares report on crime scene
- Provides checklist for first responder

**Module 06: Incident Handling**

- Defines the attacks, threats such as environmental/natural threats, Human Threats on information system
- Provides an overview of security incident, incident response, incident handling, and incident management
- Discusses various categories of incidents
- Describes incident management, threat analysis and assessment, vulnerability analysis
- Explains how to report computer incidents
- Discusses the objectives of security incident response
- Provides checklist for incident response policy
- Describes the roles and responsibilities of the Senior System Manager (SSM), Information System Security Manager (ISSM), Information System Security Officer (ISSO), and Incident Response Procedure

- Explains the Contingency/Continuity of Operations Planning
- Describes how to allocate budget/resource for handling the incident
- Lists the procedures for incident handling
- Discusses post-incident activity and report, procedural and technical countermeasures, and vulnerability resources
- Describes the goals, strategies, and vision of Computer Security Incident Response Team (CSIRT)List the steps for creating CSIRT and worldwide CERT Coordination Centers

**Module 07: Computer Forensics Lab**

- Discusses about budget allocation, physical location needs, procedures, for setting up a computer forensics lab
- Describes the hardware requirements for computer forensics lab such as forensic workstations, paraben forensics hardware i.e., handheld first responder kit, wireless stronghold bag, remote charger, portable forensic systems and towers, forensic write protection devices and kits, digital intelligence forensic hardware, wiebetech etc
- Discusses various forensic tools such as CelleBrite UFED System, DeepSpar, InfinaDyne Forensic Products, Image MASSter, Logicube, and DIBS Mobile Forensic Workstation
- Describes the software requirements for computer forensics lab such as paraben forensics software: device seizure, P2 commander, InfinaDyne forensic products: CD/DVD inspector, TEEL Technologies SIM Tools, and LiveDiscover™ forensic edition

**Module 08: Understanding Hard Disks and File Systems**

- Discusses about physical and logical structure of hard disk, types of hard disk interfaces, disk platters, tracks, sectors, and cluster
- Provides an overview of file system such as boot process, FAT32, NTFS, NTFS Encrypted File Systems (EFS), HFS, and CDFS
- Explains how to delete NTFS files
- Discusses various hard disk evidence collection tools

**Module 09: Digital Media Devices**

- Defines magnetic tape, floppy disk, compact disk, CD-ROM, and DVD
- Explains various flash memory cards such as Secure Digital (SD) memory card, Compact Flash (CF) memory card, Multi Media Memory Card (MMC), barracuda hard drives, and E-ball futuristic computer
- Discuses various digital devices models such as pocket hard drives, digital camera devices, digital video cameras, digital audio players, laptop computers, and Bluetooth and USB devices

**Module 10: CD/DVD Forensics**

- Defines compact disk and discusses its types
- Discusses about Digital Versatile Disk (DVD) and its various types
- Explains the steps in CD forensics and data analysis
- Discusses various CD/DVD imaging and data recovery tools

**Module 11: Windows, Linux, Macintosh Boot Process**

- Defines boot loader and boot sector
- Describes the anatomy of MBR
- Provides an overview of Macintosh boot sequence, Windows XP boot process, and Linux boot process
- Explains the startup files in UNIX
- Lists and discusses each steps in Windows, Linux and Macintosh boot process

**Module 12: Windows Forensics I**

- Describes volatile information such as system time, logged-on-users, open files, net file command, network connections, process information, process-to-port mapping, netstat command, and network status
- Discusses various volatile information collection tools
- Describes different techniques for collecting nonvolatile information such as registry settings and event logs
- Explains various processes involved in forensic investigation of a Windows system such as memory analysis, registry analysis, IE cache analysis, cookie analysis, MD5 calculation, Windows file analysis, and metadata investigation
- Discusses various tools and algorithms related to Windows forensics

**Module 13: Windows Forensics II**

- Provides an overview of IIS, FTP, DHCP, and firewall logs
- Discusses the importance of audit events and event logs in Windows forensics
- Explains the static and dynamic event log analysis
- Discusses different Windows password issues such as password cracking
- Discusses various forensics tools such as Helix, SecReport, Pslist etc

**Module 14: Linux Forensics**

- Describes about Linux OS, Linux boot sequence, file system in Linux, file system description, and Linux forensics
- Discusses the advantages and disadvantages of Linux forensics
- Describes Linux partitions
- Explain the purpose of Mount command
- Discusses about floppy and hard disk analysis, and forensics toolkit preparation
- Explains how to collect data using toolkit
- Provides an overview of keyword searching, Linux crash utility, and its commands
- Discusses various Linux forensics tools such as Autopsy, The Sleuth Kit, FLAG, Md5deep etc.

**Module 15: Mac Forensics**

- Describes about Mac OS and its File Systems
- Discusses about partitioning schemes, Mac OS X file system, Mac OS X directory structure, and Mac security architecture overview
- Explains how to gather evidence in Mac forensics
- Provides an overview of user home directory, POSIX permissions, viewing iChat logs, checking Wi-Fi support, checking Wi-Fi support, and obtaining system date and time
- Discusses various Mac forensics tools such as dd_rescue, gpart, File Juicer, FTK Imager etc.

**Module 16: Data Acquisition and Duplication**

- Defines data acquisition and its types
- Discusses with data duplication, its Issues, and backups
- Explains how to acquire data on Linux, MacQuisition, and Athena archiver
- Discusses various data acquisition and duplications tools such as DriveSpy, SafeBack, Image MASSter, RoadMASSter-2, Logicube, DeepSpar etc.

**Module 17: Recovering Deleted Files and Deleted Partitions**

- Discusses how to recover deleted files
- Explains how to Identify creation date, last accessed date of the file, and deleted sub-directories
- Discusses various deleted file recovery tools such as search and recover, O&O unerase, File Scavenger, DiskInternal flash recovery, and TOKIWA data recovery
- Explains the deletion of partitions using Windows interface and command line interface
- Discusses various deleted partition recovery tools such as GetDataBack, Active@ Partition Recovery, Scaven etc.

**Module 18: Forensics Investigations Using AccessData FTK**

- Introduces to Forensic Toolkit (FTK®) and its various features
- Explains FTK installation steps
- Provides step-by-step illustration of FTK working
- Explains how to search, create, open and work with cases
- Discusses different methods for decrypting and viewing encrypted files and folders
- Describes how to create, refine and delete filters
- Describes different steps for creating reports using FTK
- Discusses FTK interface customization

**Module 19: Forensics Investigations Using Encase**

- Discusses Encase, its uses, and functionality
- Describes evidence file format
- Explains how to verify file integrity

- Discusses hashing, configuring EnCase
- Explains how to view files and folders
- Describes how to search and add keywords

**Module 20: Steganography**

- Defines Steganography and its types
- Lists the application of Steganography
- Discusses various digital steganography techniques such as injection, transform domain techniques, perceptual masking, and distortion technique, different forms of steganography like text file steganography, image file steganography, audio file steganography, and video file steganography
- Describes about Steganographic File System, Cryptography and its Model
- Differentiates steganography vs. cryptography
- Explains Public Key Infrastructure (PKI)
- Discusses watermarking and its types
- Explains the steganalysis and its attacks, Stego-Forensics, Emissions Security (EMSEC), and TEMPEST
- Discusses various steganography tools such as Fort Knox, S- Tools, Steganos, wbStego, JPHIDE and JPSEEK, Stegomagic, Stegdetect, Scramdisk, MandelSteg and GIFExtract etc.

**Module 21: Image Files Forensics**

- Discusses about Image Files, Various Image File Formats, and Best Practices for Forensic Image Analysis
- Explains the use MATLAB for forensic image processing
- Discusses the algorithm for data compression
- Explains how to locate and recover image files
- Describes how to identify image file fragments, and steganography in image files
- Discusses various image file forensics tools

**Module 22: Audio file forensics**

- Defines the audio forensics and its requirements
- Discusses various audio forensics tools such as advanced audio corrector, SmaartLive 5.x, RoboNanny v1.00, PBXpress, Sigview audio analyzer etc.
- Describes suppression of noise and voice identification techniques
- Explains audio forensics methodology
- Discusses various audio file formats
- Lists the guidelines for the forensic audio recorders

**Module 23: Video File Forensics**

- Defines video file forensics and its requirements

- Discusses various video file formats
- Describes the methodology of video forensics
- Discusses various video forensics tools such as VideoDetective, Ikena Reveal, VideoFOCUS etc.

**Module 24: Application Password Crackers**

- Explains the functionality of password crackers
- Lists various methods in password cracking
- Describes the classification of cracking software, default password database, and PDF password crackers
- Discusses various password cracking tools such as Cain & Abel, Ophcrack 2, John the Ripper, Access Passview, Mail Passview etc.

**Module 25: Log Capturing and Event Correlation**

- Defines logs and its types
- Explains how to capture and protect log
- Discusses about centralized logging infrastructure, syslog, and log management infrastructure
- Describes log analysis and event correlation and even logging
- Discusses various log management tools such as Log Management Software, NitroSecurity NitroView LogCaster, Kiwi Syslog Daemon, Syslog Watcher etc.

**Module 26: Network Forensics and Investigating Logs**

- Introduces network forensics concepts
- Discusses about End-to-end Forensic Investigation, Log Files, NetFlow logs, Postmortem and Real-Time Analysis, Logging Polices, and Records of Regularly Conducted Activity
- Explains the Router Log Files, Honeypot Logs, Text Based Logs, Microsoft Log Parser, Log File Accuracy, Use Signatures, Encryption and Checksums, and Access Control
- Describes the Importance of Audit Logs, Central Logging Design, Steps to Implement Central Logging, Logon Events That Appear in the Security Event Log, ODBC Logging, Centralized Logging Server, and Distributed System Logging
- Provides overview of Activeworx Security Center, Configuring Windows Logging, Setting up Remote Logging in Windows, Condensing Log File, Log File Review, and Configuring the Windows Time Service
- Discusses various network forensics and log capturing tools

**Module 27: Investigating Network Traffic**

- Discusses connected organizations, connectivity involved in communications, and importance of the connectivity
- Explains network addressing schemes, OSI reference model, and TCP/ IP protocol
- Covers types of network attacks, evidence gathering via sniffing, and Internet DNS spoofing
- Describes proxy server DNS poisoning
- Discusses various network traffic tools

**Module 28: Router Forensics**

- Introduces router concepts
- Discusses router in an OSI model, router architecture, and routing information protocol
- Describes routers vulnerabilities, and types of router attacks
- Covers Steps for Investigating Router Attacks
- List the guidelines for the router forensic, and accessing the router
- Describes how to gather volatile evidence
- Explains direct access and indirect access
- Discusses various router forensics tools

**Module 29: Investigating Wireless Attacks**

- Discusses wireless technology, electronic emanations, and threats from electronic emanations
- Explains importance of wireless technology, risks associated with portable wireless systems, importance of vulnerabilities associated with connected systems wireless technology
- Describes various wireless networking technologies such as wireless networks, wireless attacks, passive attack, denial-of-service attacks, and man-in-the-middle attack
- Discusses Network Forensics in a Wireless Environment
- Covers the steps for investigation of wireless attacks
- Describes wireless components, detecting wireless connections, and detecting wireless enabled computers
- Discusses active wireless scanning, passive wireless scanning techniques
- how to capture wireless traffic
- Discusses various wireless tools
- Covers wireless data acquisition and analysis

**Module 30: Investigating Web Attacks**

- Explains types of Web Attacks like Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF)
- Discusses anatomy of CSRF Attack, SQL injection attacks, how to investigate SQL injection attacks
- Describes Cookie Poisoning, how to investigate Cookie Poisoning attack, Buffer Overflow, and authentication hijacking
- Explains Log tampering, Directory Traversal, Cryptographic Interception, URL Interpretation and Impersonation Attack
- Discusses how to investigate web attack, FTP Logs , FTP Servers, IIS Logs, Apache Logs , and Web Page Defacement
- Discusses Defacement Using DNS Compromise, how to investigate DNS Poisoning , intrusion detection, and checklist for web security
- Explains the use of various tools

**Module 31: Investigating DoS Attacks**

- Discusses DoS attack, indications of a DoS/DDoS attack, and types of DoS Attacks
- Explains Nuke attacks and Reflected attack
- Discusses the working of DDoS attacks, and DDoS attack taxonomy
- Describes techniques to detect DoS attack such as Activity Profiling, Sequential Change-Point Detection, Wavelet-based Signal Analysis, and CPU utilization monitoring
- Explains methods to detect DoS attacks using Cisco NetFlow, and Network Intrusion Detection System (NIDS)
- Explains ICMP Traceback, Hop-by Hop IP Traceback, Backscatter Traceback, IP Traceback with IPSec
- Explains Packet Marking, Control Channel Detection, Correlation and Integration, and challenges in investigating DoS attack
- Describes the use of various tools

**Module 32: Investigating Virus, Trojan, Spyware and Rootkit Attacks**

- Explains techniques to detect viruses, Trojans, and spyware
- Describes types of viruses, Trojans, and Spyware programs
- Discusses source of the malware attacks, methods of attack, and means of the attack
- Explains the malware mitigation techniques
- Discusses various issues involved with the investigation of malware attacks

**Module 33: Investigating Internet Crimes**

- Discusses Internet crimes, Internet forensics, and goals of the investigation over Internet
- Explains how to investigate Internet crime, obtain a search warrant, and interview the victim
- Describes how to identify the source of the online attack
- Explains the Regional Internet Registry (RIR), Domain Name System (DNS), DNS record manipulation, and DNS lookup
- Discusses how to collect the evidence, examine information in cookies, and view cookies in Firefox
- Explains email headers, email headers forging, and HTTP headers
- Discusses various techniques to view header information, and tracing back spam mails
- Describes the use of various tools that can help in investigating Internet crimes

**Module 34: Tracking Emails and Investigating Email Crimes**

- Explains electronic records management, importance of electronic records management, electronic-mail security, and electronic-mail security
- Discusses non-repudiation, and importance and role of non-repudiation in information security
- Discusses Public Key Infrastructure (PKI), and its importance in email communication

- Describes various email crimes such as identity fraud/chain letter and explains various issues associated with investigation of email crimes
- Explains different elements of email headers, and how to view header in Microsoft Outlook, AOL, and Hotmail
- Discusses web browser forensic, and local forensic in context of email investigation
- Explains how to track an email message
- Describes email exploits such as Phishing
- Discusses different techniques for obscuring webmail headers
- Demonstrates various email investigation tools

**Module 35: PDA Forensics**

- Describes Personal Digital Assistant (PDA), PDA Components, and information stored in PDA
- Discusses PDA Security Issues, PDA Attacks
- Explains PDA Forensics steps, points to remember while conducting investigation, and PDA Seizure
- Describes SIM card seizure and PDA security countermeasures
- Explains the use of various tools

**Module 36: Blackberry Forensics**

- Describes Blackberry, BlackBerry functions, and BlackBerry as Operating System
- Explains how BlackBerry (RIM) works and BlackBerry serial protocol
- Discusses Blackberry attack such as Blackjacking, and attachment service vulnerability
- Discusses BlackBerry security, BlackBerry wireless security, and BlackBerry security for wireless data
- Explains Acquisition, collecting evidence from Blackberry, gathering logs, and imaging and profiling
- Describes review of evidence, protecting stored data, and data hiding in BlackBerry

**Module 37: iPod and iPhone Forensics**

- Describes iPod, iPod Features, Apple HFS+, and and FAT32
- Explains misuse of iPod and iPod attack like Jailbreaking
- Describes iPod Forensics, documenting the device in the scene, acquisition and preservation, write blocking and write prevention, imaging and verification, and analysis
- Discusses Mac connected iPods, Windows connected iPods, and Lab Analysis
- Describes testing Mac version, Windows version, Macintosh version, and Windows version
- Explains Forensic Information in the iPod such as DeviceInfo File, SysInfo File, Data Partition, and iPod System Partition
- Discusses IPSW files, evidence stored on iPhone, and forensic prerequisites

- Describes how to recover keyboard cache, recover deleted images, recover contacts, recover call history, recover browser cache, recover deleted voicemail, recover SMS messages and other communication, and recover cached and deleted email
- Explains how to recovering corrupt iPhone system files by decrypting the IPSW files

**Module 38: Cell Phone Forensics**

- Explains hardware characteristics of mobile devices, software characteristics of mobile devices, and components of the cellular network
- Describes different cellular networks, different OS in mobile phone, and Forensics information in mobile phones
- Discusses Subscriber Identity Module (SIM), SIM file system, Integrated Circuit Card Identification (ICCID), International Mobile Equipment Identifier (IMEI), and Electronic Serial Number (ESN)
- Explains Precaution to be taken before investigation, points to remember while collecting the evidence, acquiring data from SIM cards, acquiring the data from obstructed mobile devices, and acquiring data from synched devices
- Describes SIM card data recovery software, memory card data recovery, SIM card seizure, and challenges for forensic efforts
- Discusses use of various tools

**Module 39: USB Forensics**

- Explains Universal Serial Bus (USB), USB flash drive , misuse of USB, and USB Forensics
- Discusses USB Forensic Investigation, and how to secure and evaluate the scene
- Describes documenting the scene and devices, imaging the computer and USB device, and acquiring the data
- Explains how to check Open USB ports by checking Registry of computer
- Discusses use of various tools

**Module 40: Printer Forensics**

- Explains printer forensics, different printing modes, methods of image creation, and printer identification strategy
- Describes printer forensics process, a clustering result of a printed page, and digital image analysis
- Explains Printout Bins and document examination
- Discusses use of various tools

**Module 41: Investigating Corporate Espionage**

- Explains access authorization and importance of access authorization
- Describes various auditable events
- Discusses various issues involved with background investigation of employees
- Discusses accountability for classified/sensitive data, importance of accountability for sensitive data, classification and declassification of information

- Describes access controls, importance of manual/automated access controls, access privileges, importance of access privileges,
- Discusses different access control principles such as discretionary access control and mandatory access controls
- Explains separation of duties, need to ensure separation of duties, importance of the Need to Ensure Separation of duties, Need-To-Know controls, importance of Need to Know controls
- Discusses the vulnerabilities associated with aggregation, disclosure of classified/sensitive information, and liabilities associated with disclosure of classified/sensitive information
- Explains use of various tools

**Module 42: Investigating Computer Data Breaches**

- Explains how data breaches occur
- Discusses how to investigating local machine for a data breach incident
- Describes how to investigating network for a data breach incident
- Explains countermeasures for data breaches

**Module 43: Investigating Trademark and Copyright Infringement**

- Explains trademarks, characteristics of trademarks, and eligibility and benefits of registering trademarks
- Discusses service marks and trade dress
- Explains the trademark and copyright infringement
- Explains the issues involved in investigating copyright status and copyrights enforcement
- Describes On-Line Copyright Infringement Liability Limitation Act, and Copyright infringement
- Explains types of plagiarism, guidelines for plagiarism prevention, and plagiarism detection factors
- Explains various plagiarism detection tools
- Describes patent, patent infringement, patent search, 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, and UK Laws for Trademarks and Copyright

**Module 44: Investigating Sexual Harassment Incidents**

- Explains sexual harassment, types of sexual harassment, and consequences of sexual harassment
- Describes responsibilities of supervisors, responsibilities of employees, and investigation process
- Explains sexual harassment investigations, sexual harassment policy, and preventive steps
- Describes U.S Laws on Sexual Harassment, The Laws on Sexual Harassment: Title VII of the 1964 Civil Rights Act, The Civil Rights Act of 1991, Equal Protection Clause of the 14th Amendment, Common Law Torts, and State and Municipal Laws

**Module 45: Investigating Child Pornography Cases**

- Explains child pornography, people's motive behind child pornography, people involved in child pornography, and role of Internet in promoting child pornography
- Discusses effects of child pornography on children, measures to prevent dissemination of child pornography, and challenges in controlling child pornography
- Describes how to Avoid Porn on Web,
- Discusses current methods of detecting child sexual abuse, and guidelines for investigating child pornography cases
- Explains guidelines for risk reduction to parents, how to report Antichildporn.org about child pornography cases
- Highlights U.S. Laws against Child Pornography, Australia Laws against Child Pornography, and Canadian laws against Child Pornography
- Explains use of various tools

**Module 46: Investigating Identity Theft Cases**

- Explains identity theft, and identifying information
- Describes how to identity theft complaints by age of the consumer, example of identity theft, who commits identity theft
- Discusses how criminals get information, and steal personal information
- Explains how does a criminal use information and how to investigate identity theft
- Discusses about interviewing the victim, collecting information about online activities of the victim, and obtaining search and seizing warrant
- Describes seizing of the computer and mobile devices from suspects and collecting information from point of sale
- Discusses United States: Federal Identity Theft and Assumption Deterrence Act of 1998, Unites States Federal Laws
- Explains protection from ID theft, and what should victims do?

**Module 47: Investigating Defamation over Websites and Blog Postings**

- Explains what is a blog, types of blogs, and who is blogging
- Discusses blogosphere growth, defamation over websites, and blog postings
- Describes steps for investigating defamation over websites and blog postings such as searching the content of blog in Google, checking in "Whois" database, checking the physical location, searching the source of blog, checking the copyright and privacy policy, and visit 411 and search for telephone numbers

**Module 48: Investigating Social Networking Websites for Evidence**

- Explains social networking, and what is a social networking site
- Discusses MySpace, Facebook, Orkut investigation process
- Describes how to Investigate MySpace, Facebook, and Orkut
- Discusses investigating profile , investigating scrapbook, investigating photos and video, and investigating communities

**Module 49: Investigation Search Keywords**

- Discusses Keyword Search
- Explains developing a keyword search list, index-based keyword searching, and bitwise searching
- Describes keyword search techniques, choice of searching methodology, issues with keyword searching, and Odyssey keyword search

**Module 50: Investigative Reports**

- Explains importance of reports and need of an investigative report
- Discusses report requirements, report specification, and report classification
- Describes the importance of report attachments and appendices
- Explains the layout of an investigative report
- Discusses how to report computer and Internet-related crimes
- Provides computer forensic report templates, and guidelines for writing reports
- Describes the importance of consistency, and important aspects of a good report

**Module 51: Becoming an Expert Witness**

- Explains what is expert witness, who is an expert witness, and role of an expert witness
- Discusses expert witness ethics, types of expert witnesses,
- Describes how to hire a computer forensics expert, civil litigation expert
- Describes scope of expert witness testimony, preparing for testimony, and evidence preparation and documentation
- Explains evidence processing steps and checklists for processing evidence
- Describes evidence presentation, importance of graphics in a testimony, recognizing deposing problems, and guidelines to testify at a deposing

**Module 52: How to Become a Digital Detective**

- Explains roles and responsibilities of a digital detective
- Provides a basic eligibility criteria for a digital detective

**Module 53: Computer Forensics for Lawyers**

- Explains common mistakes
- Discusses metadata, deleted data, and presenting the case
- Explains cases in which computer evidence was sought
- Provides real time case studies
- Describes industry associations which provides expert forensic investigators, how to identify the right forensic expert, and cross-examination of the computer forensic expert

**Module 54: Law and Computer Forensics**

- Explains the computer forensics laws, law enforcement interfaces/policies, and Internet laws and statutes
- Discusses on various information security acts such as USA Patriot Act of 2001, Federal Information Security Management Act, Gramm-Leach Bliley Act, CAN-SPAM Act, Personal Information Protection and Electronic Documents Act, Data Protection Act 1998, Criminal Damage Act 1991, and Cyber Terrorism Preparedness Act of 2002
- Describes the importance of laws related to Information Assurance and Security such as Federal Records Act, Federal Managers Financial Integrity Act of 1982, Federal Property and Administration Service Act, Government Paperwork Elimination Act, Paperwork Reduction Act, Computer Fraud and Abuse Act, Freedom of Information Act, E-Government Act 0f 2002 /Public Law 107-347, Implications of Public Law 107-347 Regarding Certification and Accreditation, Information Privacy Act 2000, and National Archives and Records Act
- Provides an overview of computer crime acts related to different countries around the globe
- Lists the Internet crime schemes and prevention tips
- Explains how to report a cybercrime
- Introduces with crime investigating organizations such as FBI, National White Collar Crime Center (NW3C), and Internet Crime Complaint Center (IC3) etc.

**Module 55: Computer Forensics and Legal Compliance**

- Discusses on compliance and computer forensics, the importance of legal and liability issues, information security compliance assessment, elements of an effective compliance program, and compliance program structure
- Describes the responsibilities of senior systems managers, principle of legal compliance, and creating effective compliance training program
- Explain the importance of copyright protection, copyright licensing, criminal prosecution, due diligence, and evidence collection and preservation
- Provides an overview of Memoranda of Understanding/Agreement (MOU/MOA) and legal compliance to prevent fraud, waste, and abuse

**Module 56: Security Policies**

- Explains the importance of access control policies, administrative security policies and procedures, documentation policies, evidence collection and preservation policies, and information security policy
- Discusses about audit trails and logging policies, personnel security policies & guidance, National Information Assurance (IA) Certification & Accreditation (C&A) Process policy, and biometric policies

**Module 57: Risk Assessment**

- Defines Risk and its Principles and Risk Assessment
- Explains the Importance of Risk Assessment to Support Granting an ATO, Risk Assessment to Support Granting an IATO, and Residual Risk
- Discusses the importance of risk analysts, risk mitigation, and role of documentation in reducing risk

### Module 58: Evaluation and Certification of Information Systems

- Explains accreditation, importance of accreditation, certification process, types of accreditation, and significance of NSTISSP
- Discusses Approval to Operate (ATO), purpose and contents of ATO, Interim Approval to Operate (IATO), purpose and contents of IATO,
- Explain recertification, and importance of the recertification process
- Describes Systems Security Authorization Agreement (SSAA), Contents of SSAA, and Purpose of SSAA
- Explains cost/benefit analysis of information assurance, information classification, investigative authorities, key management infrastructure, and information marking
- Discusses Certification Test & Evaluation (CT&E), certification tools, significance/results of certification tools, contracting for security services, types of contracts for security services, and threats from contracting for security services
- Explains various issues involved in disposition of classified material
- Explains importance of remanence, facilities planning, and system disposition/reutilization
- Describes life cycle system security planning, importance of life cycle system security planning, system security architecture , Certification and Accreditation (C&A), responsibilities associated with accreditation, and roles associated with certification
- Explains information ownership, and how to establish information ownership
- Discusses roles and responsibilities of system certifiers and accreditors in certification of information systems

### Module 59: Ethics in Computer Forensics

- Explains Computer Forensic Ethics, procedure to implement ethics, and importance of computer ethics
- Discusses challenges in teaching computer forensics ethics, ethical predicaments, and the ethical requirements during an investigation
- Describes ethics in preparation of forensic equipments, ethics of computer forensic investigator, and maintaining professional conduct
- Explains ethics in logical security, ethics in obtaining the evidence, ethics while preserving the evidence, and ethics in documenting evidence

### Module 60: Computer Forensic Tools

- Lists the uses of Computer Forensics Tools such as Software Forensic Tools, Data Recovery Tools, Permanent Deletion of Files, File Integrity Checker, Password Recovery Tool, Internet History Viewer, Toolkits, and Hardware Computer Forensic Tools

### Module 61: Windows Based Command Line Tools

- Demonstrates the use of Windows based command line tools such as Aircrack, BootPart, WhoAmI, Nbtstat, Tasklist, DNS lookup, Copyprofile, AccExp, GConf, Mosek, Bayden SlickRun 2.1, ffmpeg etc.

### Module 62: Windows Based GUI Tools

- Lists and demonstrates the use of Windows based GUI Tools such as Process Viewer Tools, Registry Tools, Desktop Utility Tools, Office Application Tools, Remote Control Tools, Network Tools, Network Scanner Tools, Network Sniffer Tools, Hard Disk Tool, File Management Tools, and File Recovery Tools

### Module 63: Forensics Frameworks

- Explains various forensics frameworks i.e. the FORZA, event-based digital forensic investigation framework, and objectives-based framework
- Discusses about enhanced digital investigation process model and computer forensics field triage process model

### Module 64: Forensics Investigation Templates

- Provides templates and checklists for collecting and preserving digital evidence

### Module 65: Computer Forensics Consulting Companies

- Provides a list of major computer forensics consulting companies