Course 832 – Computer Hacking Forensic Investigator

Duration: 5 days

You Will Learn How To

- Understand how perimeter defenses work
- Scan and attack you own networks, without actually harming them
- Understand steps taken by intruders to escalate their privileges in your system
- Detect intrusion, create policies, social engineering, DDoS attacks, buffer overflows, and even virus creation

Course Benefits

This CHFI training course will give you the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be taught during this course, including software, hardware and specialized techniques.

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 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.

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

Course Content

Computer Forensics in Today's World

- Forensics Science
- Computer Forensics
- Forensics Readiness
- Cyber Crime
- Cyber Crime Investigation
- Corporate Investigations
- Reporting a Cyber Crime

Computer Forensics Investigation Process

- Investigating Computer Crime
- Steps to Prepare for a Computer Forensics Investigation
- Computer Forensics Investigation Methodology

Searching and Seizing Computers

- Searching and Seizing Computers without a Warrant
- Searching and Seizing Computers with a Warrant
- The Electronic Communications Privacy Act
- Electronic Surveillance in Communications Networks
- Evidence

Digital Evidence

- Digital Data
- Types of Digital Data
- Rules of Evidence
- Electronic Devices: Types and Collecting Potential Evidence
- Digital Evidence Examination Process
- Electronic Crime and Digital Evidence Consideration by Crime Category

First Responder Procedures

- Electronic Evidence
- First Responder
- Roles of First Responder
- Electronic Devices: Types and Collecting Potential Evidence
- First Responder Toolkit
- First Response Basics
- Securing and Evaluating Electronic Crime Scene
- Conducting Preliminary Interviews
- Documenting Electronic Crime Scene
- Collecting and Preserving Electronic Evidence
- Packaging and Transporting Electronic Evidence
- Reporting the Crime Scene
- Note Taking Checklist
- First Responder Common Mistakes

Computer Forensics Lab

- Setting a Computer Forensics Lab
- Investigative Services in Computer Forensics
- Computer Forensics Hardware
- Computer Forensics Software
- Securing Laptop Computers

Understanding Hard Disks and File Systems

- Hard Disk Drive Overview
- Disk Partitions and Boot Process
- Understanding File Systems
- RAID Storage System
- File System Analysis Using The Sleuth Kit (TSK)

Windows Forensics

- Collecting Volatile Information
- Collecting Non-volatile Information
- Windows Memory Analysis
- Windows Registry Analysis
- Cache, Cookie, and History Analysis
- MD5 Calculation
- Windows File Analysis
- Metadata Investigation

- Text Based Logs
- Other Audit Events
- Forensic Analysis of Event Logs
- Windows Password Issues
- Forensic Tools

Data Acquisition and Duplication

- Data Acquisition and Duplication Concepts
- Data Acquisition Types
- Disk Acquisition Tool Requirements
- Validation Methods
- RAID Data Acquisition
- Acquisition Best Practices
- Data Acquisition Software Tools
- Data Acquisition Hardware Tools

Recovering Deleted Files and Deleted Partitions

- Recovering the Deleted Files
- File Recovery Tools for Windows
- File Recovery Tools for MAC
- File Recovery Tools for Linux
- Recovering the Deleted Partitions
- Partition Recovery Tools

Forensics Investigation using AccessData FTK

- Overview and Installation of FTK
- FTK Case Manager User Interface
- FTK Examiner User Interface
- Starting with FTK
- FTK Interface Tabs
- Adding and Processing Static, Live, and Remote Evidence
- Using and Managing Filters
- Using Index Search and Live Search
- Decrypting EFS and other Encrypted Files
- Working with Reports

Forensics Investigation Using EnCase

- Overview of EnCase Forensic
- Installing EnCase Forensic
- EnCase Interface
- Case Management
- Working with Evidence
- Source Processor
- Analyzing and Searching Files
- Viewing File Content
- Bookmarking Items
- Reporting

Steganography and Image File Forensics Steganography

- Steganography Techniques
- Steganalysis
- Image Files
- Data Compression
- Locating and Recovering Image Files
- Image File Forensics Tools

Application Password Crackers

- Password Cracking Concepts
- Types of Password Attacks
- Classification of Cracking Software
- Systems Software vs. Applications Software
- System Software Password Cracking
- Application Software Password Cracking
- Password Cracking Tools

Log Capturing and Event Correlation

- Computer Security Logs
- Logs and Legal Issues
- Log Management
- Centralized Logging and Syslogs
- Time Synchronization
- Event Correlation
- Log Capturing and Analysis Tools

Network Forensics, Investigating Logs and Investigating Network Traffic

- Network Forensics
- Network Attacks
- Log Injection Attacks
- Investigating and Analyzing Logs
- Investigating Network Traffic
- Traffic Capturing and Analysis Tools
- Documenting the Evidence Gathered on a Network

Investigating Wireless Attacks

- Wireless Technologies
- Wireless Attacks
- Investigating Wireless Attacks
- Features of a Good Wireless Forensics Tool
- Wireless Forensics Tools
- Traffic Capturing and Analysis Tools
- Wi-Fi Raw Packet Capturing Tools
- Wi-Fi Spectrum Analyzing Tools

Investigating Web Attacks

- Introduction to Web Applications and Webservers
- Web Logs
- Web Attacks
- Web Attack Investigation
- Web Attack Detection Tools
- Tools for Locating IP Address

Tracking Emails and Investigating Email Crimes

- Email System Basics
- Email Crimes
- Email Headers
- Steps to Investigate
- Email Forensics Tools
- Laws and Acts against Email Crimes

Mobile Forensics

- Mobile Phone
- Mobile Operating Systems
- Mobile Forensics
- Mobile Forensic Process
- Mobile Forensics Software Tools
- Mobile Forensics Hardware Tools

Investigative Reports

- Computer Forensics Report
- Computer Forensics Report Template
- Investigative Report Writing
- Sample Forensics Report
- Report Writing Using Tools

Becoming an Expert Witness

- Expert Witness
- Types of Expert Witnesses
- Scope of Expert Witness Testimony
- Evidence Processing
- Rules for Expert Witness
- General Ethics While Testifying

About ActiveLearning, Inc.

ActiveLearning is the Philippines' leading provider of Information Technology and Project Management education, where thousands of students take courses from Application Development to Project Management to Network Security, and much more. Our courses are taught by expert instructors, and learning is enhanced through a blend of in-depth lectures, workshops, and hands-on exercises.