

CHFI - COMPUTER HACKING FORENSIC INVESTIGATOR

Course Code: 3401

Gain knowledge and experience with essential security systems through the exploration of common ethical hacking topics at Global Knowledge. [Learn more here.](#)

EC-Council released the most advanced computer forensic investigation program in the world. This course covers major forensic investigation scenarios that enable you to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation.

Battles between corporations, governments, and countries are no longer fought using physical force. Cyber war has begun and the consequences can be seen in everyday life. With the onset of sophisticated cyber attacks, the need for advanced cybersecurity and investigation training is critical. If you or your organization requires the knowledge or skills to identify, track, and prosecute cyber criminals, then this is the course for you. You will learn how to excel in digital evidence acquisition, handling, and forensically sound analysis. These skills will lead to successful prosecutions in various types of security incidents such as data breaches, corporate espionage, insider threats, and other intricate cases involving computer systems.

This course includes an exam voucher.

What You'll Learn

- The computer forensic investigation process and the various legal issues involved
- Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner
- Types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- Roles of the first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, and reporting the crime scene

- Setting up a computer forensics lab and the tools involved in it
- Various file systems and how to boot a disk
- Gathering volatile and non-volatile information from Windows
- Data acquisition and duplication rules
- Validation methods and tools required
- Recovering deleted files and deleted partitions in Windows, Mac OS X, and Linux
- Forensic investigation using AccessData FTK and EnCase
- Steganography and its techniques
- Steganalysis and image file forensics
- Password cracking concepts, tools, and types of password attacks
- Investigating password protected files
- Types of log capturing, log management, time synchronization, and log capturing tools
- Investigating logs, network traffic, wireless attacks, and web attacks
- Tracking emails and investigate email crimes
- Mobile forensics and mobile forensics software and hardware tools
- Writing investigative reports
- Dark Web Forensics and IOT Forensics

Who Needs to Attend

IT professionals involved with information system security, computer forensics, and incident response

Prerequisites

It is strongly recommended that you attend Certified Ethical Hacker v9 before enrolling into CHFI program.

CHFI - COMPUTER HACKING FORENSIC INVESTIGATOR

Course Code: 3401

CLASSROOM LIVE

\$4,805 CAD

5 Day

Classroom Live Outline

1. Computer Forensics in Today's World
2. Computer Forensics Investigation Process
3. Understanding Hard Disks and File Systems
4. Data Acquisition and Duplication
5. Defeating Anti-forensics Techniques
6. Windows Forensics
7. Linux and Mac Forensics
8. Network Forensics
9. Malware Forensics
10. Investigating Web Attacks
11. Dark Web Forensics
12. Cloud Forensics
13. Email and Social Media Forensics
14. Mobile Forensics
15. IoT Forensics

Classroom Live Labs

Lab 1: Computer Forensics in Today's World

Lab 2: Learning about Computer Crime Policies, Programs, and Computer Forensics Laws

Lab 3: Reporting a Cybercrime to the FBI

Lab 4: Case Study: Child Pornography

Lab 5: Additional Reading Material

Lab 6: Computer Forensics Investigation Process

Lab 7: Recovering Data Using the Recover My Files Tool

Lab 8: Performing Hash, Checksum, or HMAC Calculations Using the HashCalc Tool

Lab 9: Generating MD5 Hashes Using MD5 Calculator

Lab 10: Additional Reading Material

Lab 11: Searching and Seizing Computers with a Search Warrant

Lab 12: Understanding an Application for a Search Warrant (Exhibit A)

Lab 13: Additional Reading Material

Lab 14: Studying the Digital Evidence Examination Process - Case Study 1

Lab 15: Studying Digital Evidence Examination Process - Case Study 2

Lab 16: Additional Reading Material

Lab 17: Studying First Responder Procedures

Lab 18: Understanding the First Responder Toolkit

Lab 19: Additional Reading Material

Lab 20: Computer Forensics Lab

Lab 21: Gathering Evidence Using the Various Tools of DataLifter

Lab 22: Viewing Files of Various Formats Using the File Viewer Tool

Lab 23: Handling Evidence Data Using the P2 Commander Tool

Lab 24: Creating a Disk Image File of a Hard Disk Partition Using the R-Drive Image Tool

Lab 25: Additional Reading Material

Lab 26: Understanding Hard Disks and File Systems

Lab 27: Recovering Deleted Files from Hard Disks Using WinHex

Lab 28: Analyzing File System Types Using The Sleuth Kit (TSK)

Lab 29: Case Study: Corporate Espionage

Lab 30: Additional Reading Material

Lab 31: Performing Windows Forensics

Lab 32: Discovering and Extracting Hidden Forensic Material on Computers Using OSForensics

Lab 33: Extracting Information about Loaded Processes Using Process Explorer

Lab 34: Investigating Metadata Using Metadata Analyzer

Lab 35: Viewing, Monitoring, and Analyzing Events Using the Event Log Explorer Tool

Lab 36: Performing a Computer Forensic Investigation Using the Helix Tool

Lab 37: Case Study: Terrorist Attack

Lab 38: Case Study: Brutal Murder

Lab 39: Forensics Challenge: Banking Troubles

Lab 40: Additional Reading Material

Lab 41: Data Acquisition and Duplication

Lab 42: Investigating NTFS Drive Using DiskExplorer for NTFS

Lab 43: Viewing Content of Forensic Image Using AccessData FTK Imager Tool

Lab 44: Searching Text Strings in the Hard Disk Partition Image Using DriveLook

Lab 45: Forensics Challenge: Forensic Analysis of a Compromised Server

Lab 46: Additional Reading Material

Lab 47: Recovering Deleted Files and Deleted Partitions

Lab 48: File Recovery Using EASEUS Data Recovery Wizard

Lab 49: File Recovery Using Quick Recovery Tool

Lab 50: Partition Recovery Using MiniTool Power Data Recovery Tool

Lab 51: Case Study: Employee Sabotage

Lab 52: Case Study: Virus Attack

Lab 53: Additional Reading Material

Lab 54: Forensics Investigation

Lab 55: Investigating a Case Using AccessData FTK

Lab 56: Case Study: Business Rivalry

Lab 57: Case Study: Sabotage

Lab 58: Forensics Investigation Using EnCase

Lab 59: Case Study: Disaster Recovery Investigation

Lab 60: Performing a Steganalysis and Forensics of an Image File

Lab 61: Analyzing Images for Hidden Messages Using Stegdetect

Lab 62: Analyzing Image File Headers Using Hex Workshop

Lab 63: Identifying Image File Format Using IrfanView

Lab 64: Recovering Photo Evidence from a Raw File Using Adroit Photo Forensics

2011

Lab 65: Case Study: Steganography

Lab 66: Forensics Challenge: Malware Reverse Engineering

Lab 67: Additional Reading Material

Lab 68: Application Password Crackers

Lab 69: Cracking Password Using the Password Recovery Bundle Tool

Lab 70: Cracking Password Using the Advanced Office Password Recovery Tool

Lab 71: Password Cracking Using the Advanced PDF Password Recovery Tool

Lab 72: Cracking Password Using KRYLack Archive Password Recovery Tool

Lab 73: Password Cracking Using the Windows Password Breaker Tool

Lab 74: Case Study: Encrypted Documents

Lab 75: Additional Reading Material

Lab 76: Capturing and Analyzing Log Files

Lab 77: Capturing and Analyzing the Logs of a Computer using GFI EventsManager Tool

Lab 78: Investigating System Log Data Using XpoLog Center Suite Tool

Lab 79: Viewing Event Logs Using Kiwi Syslog Server Tool

Lab 80: Forensics Challenge: Log Mysteries

Lab 81: Additional Reading Material

Lab 82: Network Forensics

Lab 83: Capturing and Analyzing Live Data Packets Using Wireshark Tool

Lab 84: Analyzing a Network Using the Colasoft Capsa Network Analyzer Tool

Lab 85: Monitoring the Network and Capturing Live Traffic Using NetWitness Investigator Tool

Lab 86: Forensics Challenge: Pcap Attack Trace

Lab 87: Additional Reading Material

Lab 88: Investigating Wireless Attacks

Lab 89: Cracking a WEP Network with Aircrack-ng for Windows

Lab 90: Sniffing the Network Using the OmniPeek Network Analyzer

Lab 91: Forensics Challenge: VoIP

Lab 92: Additional Reading Material

Lab 93: Investigating Web Attacks

Lab 94: Finding Web Security Vulnerabilities Using N-Stalker Web Application Security Scanner

Lab 95: Analyzing Domain and IP Address Queries Using SmartWhois Tool

Lab 96: Case Study: Trademark Infringement

Lab 97: Forensics Challenge: Browsers Under Attack

Lab 98: Additional Reading Material

Lab 99: Investigating Email Crimes

Lab 100: Recovering Deleted Emails Using the Recover My Email Utility

Lab 101: Investigating Email Crimes Using Paraben's Email Examiner Tool

Lab 102: Tracing an Email Using the eMailTrackerPro Tool

Lab 103: Case Study: Racial Discrimination

Lab 104: Forensics Challenge: Analyzing Malicious Portable Destructive Files

Lab 105: Additional Reading Material

Lab 106: Mobile Forensics

Lab 107: Investigating Mobile Information Using Oxygen Forensic Suite 2011

Lab 108: Case Study: iPod - A Handy Tool for Crime

Lab 109: Additional Reading Material

Lab 110: Investigative Reports

Lab 111: Creating an Investigative Report Using ProDiscover Tool

Lab 112: Case Study: Pornography

Lab 113: Additional Reading Material

Lab 114: Studying about Computerlegalexperts.com

Lab 115: Finding a Computer Forensics Expert

Lab 116: Understand to Becoming an Expert Witness

Lab 117: Case Study: Expert WitnessExpert Witness

Lab 118: Additional Reading Material

Lab 119: Analyzing Al-Qaida Hard Disk Using Various Forensics Tools

CHFI - COMPUTER HACKING FORENSIC INVESTIGATOR

Course Code: 3401

VIRTUAL CLASSROOM LIVE

\$4,805 CAD

5 Day

Virtual Classroom Live Outline

1. Computer Forensics in Today's World
2. Computer Forensics Investigation Process
3. Understanding Hard Disks and File Systems
4. Data Acquisition and Duplication
5. Defeating Anti-forensics Techniques
6. Windows Forensics
7. Linux and Mac Forensics
8. Network Forensics
9. Malware Forensics
10. Investigating Web Attacks
11. Dark Web Forensics
12. Cloud Forensics
13. Email and Social Media Forensics
14. Mobile Forensics
15. IoT Forensics

Virtual Classroom Live Labs

Lab 1: Computer Forensics in Today's World

Lab 2: Learning about Computer Crime Policies, Programs, and Computer Forensics Laws

Lab 3: Reporting a Cybercrime to the FBI

Lab 4: Case Study: Child Pornography

Lab 5: Additional Reading Material

Lab 6: Computer Forensics Investigation Process

Lab 7: Recovering Data Using the Recover My Files Tool

Lab 8: Performing Hash, Checksum, or HMAC Calculations Using the HashCalc Tool

Lab 9: Generating MD5 Hashes Using MD5 Calculator

Lab 10: Additional Reading Material

Lab 11: Searching and Seizing Computers with a Search Warrant

Lab 12: Understanding an Application for a Search Warrant (Exhibit A)

Lab 13: Additional Reading Material

Lab 14: Studying the Digital Evidence Examination Process - Case Study 1

Lab 15: Studying Digital Evidence Examination Process - Case Study 2

Lab 16: Additional Reading Material

Lab 17: Studying First Responder Procedures

Lab 18: Understanding the First Responder Toolkit

Lab 19: Additional Reading Material

Lab 20: Computer Forensics Lab

Lab 21: Gathering Evidence Using the Various Tools of DataLifter

Lab 22: Viewing Files of Various Formats Using the File Viewer Tool

Lab 23: Handling Evidence Data Using the P2 Commander Tool

Lab 24: Creating a Disk Image File of a Hard Disk Partition Using the R-Drive Image Tool

Lab 25: Additional Reading Material

Lab 26: Understanding Hard Disks and File Systems

Lab 27: Recovering Deleted Files from Hard Disks Using WinHex

Lab 28: Analyzing File System Types Using The Sleuth Kit (TSK)

Lab 29: Case Study: Corporate Espionage

Lab 30: Additional Reading Material

Lab 31: Performing Windows Forensics

Lab 32: Discovering and Extracting Hidden Forensic Material on Computers Using OSForensics

Lab 33: Extracting Information about Loaded Processes Using Process Explorer

Lab 34: Investigating Metadata Using Metadata Analyzer

Lab 35: Viewing, Monitoring, and Analyzing Events Using the Event Log Explorer Tool

Lab 36: Performing a Computer Forensic Investigation Using the Helix Tool

Lab 37: Case Study: Terrorist Attack

Lab 38: Case Study: Brutal Murder

Lab 39: Forensics Challenge: Banking Troubles

Lab 40: Additional Reading Material

Lab 41: Data Acquisition and Duplication

Lab 42: Investigating NTFS Drive Using DiskExplorer for NTFS

Lab 43: Viewing Content of Forensic Image Using AccessData FTK Imager Tool

Lab 44: Searching Text Strings in the Hard Disk Partition Image Using DriveLook

Lab 45: Forensics Challenge: Forensic Analysis of a Compromised Server

Lab 46: Additional Reading Material

Lab 47: Recovering Deleted Files and Deleted Partitions

Lab 48: File Recovery Using EASEUS Data Recovery Wizard

Lab 49: File Recovery Using Quick Recovery Tool

Lab 50: Partition Recovery Using MiniTool Power Data Recovery Tool

Lab 51: Case Study: Employee Sabotage

Lab 52: Case Study: Virus Attack

Lab 53: Additional Reading Material

Lab 54: Forensics Investigation

Lab 55: Investigating a Case Using AccessData FTK

Lab 56: Case Study: Business Rivalry

Lab 57: Case Study: Sabotage

Lab 58: Forensics Investigation Using EnCase

Lab 59: Case Study: Disaster Recovery Investigation

Lab 60: Performing a Steganalysis and Forensics of an Image File

Lab 61: Analyzing Images for Hidden Messages Using Stegdetect

Lab 62: Analyzing Image File Headers Using Hex Workshop

Lab 63: Identifying Image File Format Using IrfanView

Lab 64: Recovering Photo Evidence from a Raw File Using Adroit Photo Forensics

2011

Lab 65: Case Study: Steganography

Lab 66: Forensics Challenge: Malware Reverse Engineering

Lab 67: Additional Reading Material

Lab 68: Application Password Crackers

Lab 69: Cracking Password Using the Password Recovery Bundle Tool

Lab 70: Cracking Password Using the Advanced Office Password Recovery Tool

Lab 71: Password Cracking Using the Advanced PDF Password Recovery Tool

Lab 72: Cracking Password Using KRYLack Archive Password Recovery Tool

Lab 73: Password Cracking Using the Windows Password Breaker Tool

Lab 74: Case Study: Encrypted Documents

Lab 75: Additional Reading Material

Lab 76: Capturing and Analyzing Log Files

Lab 77: Capturing and Analyzing the Logs of a Computer using GFI EventsManager Tool

Lab 78: Investigating System Log Data Using XpoLog Center Suite Tool

Lab 79: Viewing Event Logs Using Kiwi Syslog Server Tool

Lab 80: Forensics Challenge: Log Mysteries

Lab 81: Additional Reading Material

Lab 82: Network Forensics

Lab 83: Capturing and Analyzing Live Data Packets Using Wireshark Tool

Lab 84: Analyzing a Network Using the Colasoft Capsa Network Analyzer Tool

Lab 85: Monitoring the Network and Capturing Live Traffic Using NetWitness Investigator Tool

Lab 86: Forensics Challenge: Pcap Attack Trace

Lab 87: Additional Reading Material

Lab 88: Investigating Wireless Attacks

Lab 89: Cracking a WEP Network with Aircrack-ng for Windows

Lab 90: Sniffing the Network Using the OmniPeek Network Analyzer

Lab 91: Forensics Challenge: VoIP

Lab 92: Additional Reading Material

Lab 93: Investigating Web Attacks

Lab 94: Finding Web Security Vulnerabilities Using N-Stalker Web Application Security Scanner

Lab 95: Analyzing Domain and IP Address Queries Using SmartWhois Tool

Lab 96: Case Study: Trademark Infringement

Lab 97: Forensics Challenge: Browsers Under Attack

Lab 98: Additional Reading Material

Lab 99: Investigating Email Crimes

Lab 100: Recovering Deleted Emails Using the Recover My Email Utility

Lab 101: Investigating Email Crimes Using Paraben's Email Examiner Tool

Lab 102: Tracing an Email Using the eMailTrackerPro Tool

Lab 103: Case Study: Racial Discrimination

Lab 104: Forensics Challenge: Analyzing Malicious Portable Destructive Files

Lab 105: Additional Reading Material

Lab 106: Mobile Forensics

Lab 107: Investigating Mobile Information Using Oxygen Forensic Suite 2011

Lab 108: Case Study: iPod - A Handy Tool for Crime

Lab 109: Additional Reading Material

Lab 110: Investigative Reports

Lab 111: Creating an Investigative Report Using ProDiscover Tool

Lab 112: Case Study: Pornography

Lab 113: Additional Reading Material

Lab 114: Studying about Computerlegalexperts.com

Lab 115: Finding a Computer Forensics Expert

Lab 116: Understand to Becoming an Expert Witness

Lab 117: Case Study: Expert WitnessExpert Witness

Lab 118: Additional Reading Material

Lab 119: Analyzing Al-Qaida Hard Disk Using Various Forensics Tools

Jul 14 - 18, 2025 | 8:30 AM - 4:30 PM EDT

Sep 15 - 19, 2025 | 8:30 AM - 4:30 PM EDT

Nov 3 - 7, 2025 | 8:30 AM - 4:30 PM EST



CHFI - COMPUTER HACKING FORENSIC INVESTIGATOR

Course Code: 3401

PRIVATE GROUP TRAINING

5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/9/2025 11:57:42 PM

Copyright © 2025 Global Knowledge Training LLC. All Rights Reserved.