



[View Full Course Details including Latest Schedule Online](#)

EC-COUNCIL

CHFI Certification Training

Course Overview

Our 5-day, instructor-led CHFI (Computer Hacking Forensic Investigator) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online is geared toward IT security professionals in police and law enforcement, military and government, banking, network, and e-business. It will teach you how to:

- Detect different types of attacks
- Differentiate between various types of digital evidence
- Gather evidence to prosecute cyber criminals
- Secure a network & prevent an intrusion
- Recover lost & deleted files
- Track & investigate emails, logs, network traffic, wireless attacks & web attacks

This course will fully prepare you for the CHFI Certification exam.

You should be familiar with Windows-based computer systems before taking this course.

Course Outline

Computer Forensics in Today's World

- Understanding computer forensics
- Why and when do you use computer forensics?
- Cyber crime (types of computer crimes)
- Case study
- Challenges cyber crimes present for investigators
- Cyber crime investigation
- Rules of forensics investigation
- Understanding digital evidence
- Types of digital evidence
- Characteristics of digital evidence
- Role of digital evidence
- Sources of potential evidence



- Rules of evidence
- Forensics readiness
- Computer forensics as part of an incident response plan
- Need for forensic investigator
- Roles and responsibilities of forensics investigator
- What makes a good computer forensics investigator?
- Investigative challenges
- Legal and privacy issues
- Code of ethics
- Accessing computer forensics resources

Computer Forensics Investigation Process

- Importance of computer forensics process
- Phases involved in the computer forensics investigation process
- Pre-investigation phase
- Investigation phase
- Post-investigation phase

Understanding Hard Disks and File Systems

- Hard disk drive overview
- Disk partitions and boot process
- Understanding file systems
- RAID storage system
- File system analysis

Data Acquisition and Duplication

- Data acquisition and duplication concepts
- Static acquisition
- Validate data acquisitions
- Acquisition best practices

Defeating Anti-Forensics Techniques

- What is anti-forensics?
- Anti-forensics techniques



Operating System Forensics (Windows, Mac, Linux)

- Introduction to OS forensics
- Windows forensics
- Linux forensics
- MAC forensics

Network Forensics

- Introduction to network forensics
- Fundamental logging concepts
- Event correlation concepts
- Network forensic readiness
- Network forensics steps
- Network traffic investigation
- Documenting the evidence
- Evidence reconstruction

Investigating Web Attacks

- Introduction to web application forensics
- Web attack investigation
- Investigating web server logs
- Web attack detection tools
- Tools for locating IP Address
- WHOIS lookup tools

Database Forensics

- Database forensics and its importance
- MSSQL forensics
- MySQL forensics

Cloud Forensics

- Introduction to cloud computing
- Cloud forensics



Malware Forensics

- Introduction to malware
- Introduction to malware forensics

Investigating Email Crimes

- Email system
- Email crimes (email spamming, mail bombing/mail storm, phishing, email spoofing, crime via chat room, identity fraud/chain letter)
- Email message
- Steps to investigate email crimes and violation
- Email forensics tools
- Laws and acts against email crimes

Mobile Phone Forensics

- Mobile device forensics

Forensics Report Writing and Persuasion

- Writing investigation reports
- Expert witness testimony

Exam Information

CHFI Certification Training Course Details:

- Number of Questions: 150
- Passing Score: 70%
- Duration: 4 hours
- Format: multiple choice
- Delivery: Prometric/Pearson VUE
- Code: 312-49



PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

CHFI Certification Exam Objectives:

The CHFI certification exam tests candidates on these twenty-two domains:

- Computer Forensics in Today's World
- Computer Forensics Investigation Process Searching and Seizing Computers
- Digital Evidence
- First Responder Procedures
- Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation with AccessData FTK
- Forensics Investigation with EnCase
- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing and Event Correlation
- Network Forensics, Investigating Logs and Network Traffic
- Investigation Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigation Email Crimes
- Mobile Forensics
- Investigative REports
- Becoming and Expert Witness

Phoenix TS is an authorized testing center for Prometric and Pearson VUE exams. Register for exams by calling us at **(240) 667-7757** or visiting the Pearson VUE and Prometric websites.

Starting at **\$2,695**

ATTENTION

For GSA pricing or Contractor quotes call

[240.667.7757](tel:240.667.7757)

GSA



Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Included in this CHFI Certification Training course

- 5-Day Training with a CHFI Certified Instructor
- Official EC-Council CHFI courseware
- Pre and Post Assessments
- 30+ CHFI Labs
- CHFI Exam Voucher
- CHFI Testing on the Last Day of Class
- Onsite Exam Scheduling and Testing Center
- Certificate of Completion for up to 40 CEUs/CPEs to be used toward renewing relevant certifications
- EC-Council Training Center of the Year
- EC-Council Authorized Training Course
- CHFI Course Retake Guarantee
- Meets 8570.01-M training requirements for CSSP Analyst, CSSP Infrastructure Support, CSSP Auditor
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*



PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

- Freshly baked cookies every afternoon*

**denotes this benefit is only available at participating locations*