Cyber Gate ACADEMY

EC-CHFI

CERTIFIED HACKING FORENSIC INVESTIGATION COURSE

Course Overview

The CHFI course will give participants 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 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 cyber-criminal, then this is the course for you.

Course Duration

5 Days (40 Hours).

Target Audience

In addition, this course and subsequent certification (CFR-410) meet all requirements for personnel requiring DoD directive 8570.01-M position certification baselines:

- CSSP Analyst
- CSSP Infrastructure Support
- CSSP Incident Responder
- CSSP Auditor

Learning Objectives

The CHFI V10 course aims to equip learners with the knowledge and skills required to perform effective computer forensic investigations. Students will learn how to gather necessary evidence to prosecute cyber criminals. The course’s objectives include understanding how to work in an investigative process, tracing and recovering deleted files, cracking passwords, and learning how to develop a systematic approach in computer forensic evidence analysis. Furthermore, learners will understand the principal concepts of cybercrimes and the laws involved. It also covers strategies to maintain data confidentiality, integrity, and availability by providing hands-on experience using various forensic investigation techniques and standard tools.

Course Content

Module 01: Computer Forensics in Today's World.
Module 02: Law and Computer Forensics.
Module 03: Computer Investigation Process.
Module 04: First Responder Procedure.
Module 05: CSIRT.
Module 06: Computer Forensic Lab.
Module 07: Understanding File Systems and Hard Disks.
Module 08: Understanding Digital Media Devices.
Module 09: Windows, Linux and Macintosh Boot Processes.
Module 10: Windows Forensics.
Module 11: Linux Forensics.
Module 12: Data Acquisition and Duplication.
Module 13: Computer Forensic Tools.
Module 14: Forensics Investigations Using Encase.
Module 15: Recovering Deleted Files and Deleted partitions.
Module 16: Image Files Forensics.
Module 17: Steganography.
Module: 18: Application Password Crackers.
Module 19: Network Forensics and Investigating Logs.
Module 20: Investigating Network Traffic.
Module 21: Investigating Wireless Attacks.
Module 22: Investigating Web Attacks.
Module 23: Router Forensics.
Module 24: Investigating DoS Attacks.
Module 25: Investigating Internet Crimes.
Module 26: Tracking E-mails and Investigating E-mail Crimes.
Module 27: Investigating Corporate Espionage.
Module 28: Investigating Trademark and Copyright Infringement.
Module 29: Investigating sexually harassment incidents.
Module 30: Investigating Child Pornography.
Module 31: PDA Forensics.
Module 32: iPod Forensics.
Module 33: Blackberry Forensi.
Module 34: Investigative Reports.
Module 35: Becoming an Expert Witness.

Prerequisites

Attendees should meet the following prerequisites:

It is strongly recommended that you attend the CEH class before enrolling into CHFI program. Recommended prerequisites:

- CEH - EC-Council Certified Ethical Hacker (CEH) + Exam voucher

Course Agenda

Day 1	Module 01: Computer Forensics in Today's World Module 02: Law and Computer Forensics Module 03: Computer Investigation Process Module 04: First Responder Procedure Module 05: CSIRT Module 06: Computer Forensic Lab Module 07: Understanding File Systems and Hard Disks
Day 2	Module 08: Understanding Digital Media Devices Module 09: Windows, Linux and Macintosh Boot Processes Module 10: Windows Forensics Module 11: Linux Forensics Module 12: Data Acquisition and Duplication Module 13: Computer Forensic Tools Module 14: Forensics Investigations Using Encase
Day 3	Module 15: Recovering Deleted Files and Deleted partitions Module 16: Image Files Forensics Module 17: Steganography Module: 18: Application Password Crackers Module 19: Network Forensics and Investigating Logs Module 20: Investigating Network Traffic Module 21: Investigating Wireless Attacks
Day 4	Module 22: Investigating Web Attacks Module 23: Router Forensics Module 24: Investigating DoS Attacks Module 25: Investigating Internet Crimes Module 26: Tracking E-mails and Investigating E-mail Crimes Module 27: Investigating Corporate Espionage Module 28: Investigating Trademark and Copyright Infringement
Day 5	Module 29: Investigating sexually harassment incidents Module 30: Investigating Child Pornography Module 31: PDA Forensics Module 32: iPod Forensics Module 33: Blackberry Forensi Module 34: Investigative Reports Module 35: Becoming an Expert Witness

Technical Requirement

1. Laptop with minimum 8GB Ram.
2. Connected Monitor for iLabs.
3. Hi speed Internet Connection as All the labs it will be accessed through EC-Council Cloud.

Exam Voucher Validity

It will be valid for 12month starting from the last day of the course.

Certification Expiry

It will be valid for 3 years.

YOUR
TRUSTED
DEFENDERS

ADDRESS

CyberGate Academy
ADPOLY, MBZ City

WEB

academy@cybergate.tech
training@cybergate.tech