EC-Council

CHFI™ v8

Computer Hacking Forensic INVESTIGATOR

Computer Hacking Forensic Investigator

"Be the leader. Deserve a place in the CHFI certified elite class. Earn cutting edge skills in computer forensics"

"If you desire to acquire the knowledge or skill set to identify, track and bring the cyber criminals to justice, then this course is the right choice for you"

"CHFI, the most sought-after information security certification in the field of Computer Forensic Investigation. Designed to reinforce the skills of the new generation of cyber sleuths."

EC-Council

Computer Hacking Forensic Investigator

Course Description:

EC-Council releases the most advanced Computer Forensic Investigation program in the world. CHFIv8 presents a detailed methodological approach to computer forensics and evidence analysis. It is a comprehensive course covering major forensic investigation scenarios that enable students 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 every day life. With the onset of sophisticated cyber-attacks, the need for advanced cyber security and investigation training is a mandate in the present day. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cybercriminals, then this is the course for you. This course helps students to excel in digital evidence acquisition,handling and analysis in a forensically sound manner. Acceptable in a court of law, 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.

Target Audience:

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

Prerequisites

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

Duration

5 days (9:00 – 5:00)

Certification

The CHFI 312-49 exam will be conducted on the last day of training (optional). Students need to pass the online Prometric exam to receive the CHFI certification.

Exam Details

1. Number of Questions: 150
2. Passing Score: 70%
3. Test Duration: 4 Hours
4. Test Format: Multiple Choice
5. Test Delivery: Prometric Prime / Prometric APTC / VUE

Exam Code

The exam code varies when taken at different testing centers.

1. Prometric Prime: 312-49
2. Prometric APTC: EC0-349
3. VUE: 312-49

Key features of CHFI v8

Updated Content

CHFIv8 contains updated information including concepts, methodologies and tools.

Organized Content

The well-organized content enhances the learning experience and ensures better understanding of key concepts and investigation methodologies.

Methodological Approach

CHFIv8 presents step-by-step procedures,best practices and guidelines to carry out forensic investigation.

Illustration Rich

Concepts are well-illustrated to create self-explanatory slides which makes it classroom and instructor friendly.

New Investigation Techniques

CHFIv8 provides in-depth knowledge of new techniques and tools used in forensic investigation to meet the toughest challenges in fighting cybercrime.

Investigation Tools

CHFIv8 showcases hundreds of investigation tools including EnCase, Access Data FTK, and ProDiscover.

Sample Evidence Files

CHFIv8 DVD contains a huge cache of evidence files for analysis including RAW, .dd images, video and audio files, MS Office files, systems files etc.

Visual Content Technology

Use of rich Visual Content Technology to present concepts and forensic investigation techniques.

Lab Setup

Lab setup manual provides detailed procedures to setup a lab environment complete with network environment, evidence files and other prerequisite tools.

DVD-ROM Content

CHFIv8 also provides a DVD-ROM with a repository of the around 8 GB of the latest investigation and security tools.

Version Comparison

Computer Hacking Forensic Investigator courseware has undergone tremendous improvements compared to its previous versions. We have invested 4 times the effort in fundamental research and development since its last release, and have given CHFIv8 a complete makeover. The new version is a breakaway from earlier releases with more emphasis given on techniques and methodologies, which helps in the development of an advanced forensic analysis skill set. 'A picture is worth a thousand words' and we at EC-Council have enforced the saying by using addvance Visual Content technology (VCT) to explain various forensic investigation concepts. The comprehensive instructor slides and student manual in CHFIv8 empowers the instructors with flawless flow and outstanding diagrammatic representation of the investigation techniques, which makes it easier to teach and enables students to understand the concepts.

> "The CHFI Certification is an incredible asset to my company which has now a better understanding of Security issues, especially concerning vulnerability."
>
> - Frank Chow, CHFI, Automated Systems (HK) Ltd, China.

i Labs

The iLabs is a subscription based service that allows students to log on to a virtualized remote machine running Windows 2008 Server to perform various exercises featured in the CHFIv8 Lab Guide. All you need is a web browser to connect and start experimenting. The virtual machine setup reduces the time and effort spent by instructors and partners prior to the classroom engagement. It is a hassle free service available 24/7 x number of days subscribed.

Benefits

- Enables students to practice various investigation techniques in a real time and simulated environment
- The course tools and programs are preloaded on the iLabs machine thereby saving productive time and effort

What will you learn?

Students going through CHFI training will 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
- Different types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- Roles of 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
- How to set 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
- How to recover deleted files and deleted partitions in Windows, Mac OS X, and Linux
- The process involved in forensic investigation using AccessData FTK and EnCase
- Steganography and its techniques, Steganalysis, and image file forensics
- Password Cracking Concepts, tools, types of password attacks and how to investigate password protected files
- Different types of log capturing, log management, time synchronization, and log capturing tools
- How to investigate logs, network traffic, wireless attacks, and web attacks
- How to track e-mails and investigate e-mail crimes
- Mobile forensics and mobile forensics software and hardware tools
- How to write investigative reports

> "The course material is up to date and very complete. It really takes you on a trip through the Security field. Each chapter has lab exercises and this makes you understand the stuff in the book much better. If you are working or want to work in the Information Security field this training is highly recommended."
>
> - Martin de Kok, Sr Security Officer, Netherlands.

Course Outline Version 8

CHFIv8 curriculum consists of 22 instructor-led training modules.

1. Computer Forensics in Today's World
2. Computer Forensics Investigation Process
3. Searching and Seizing Computers
4. Digital Evidence
5. First Responder Procedures
6. Computer Forensics Lab
7. Understanding Hard Disks and File Systems
8. Windows Forensics
9. Data Acquisition and Duplication
10. Recovering Deleted Files and Deleted Partitions
11. Forensics Investigation Using AccessData FTK
12. Forensics Investigation Using EnCase
13. Steganography and Image File Forensics
14. Application Password Crackers
15. Log Capturing and Event Correlation
16. Network Forensics, Investigating Logs and Investigating Network Traffic
17. Investigating Wireless Attacks
18. Investigating Web Attacks
19. Tracking Emails and Investigating Email Crimes
20. Mobile Forensics
21. Investigative Reports
22. Becoming an Expert Witness

"CHFI is a certification that gives a complete overview of the process that a forensic investigator must follow when investigating a cybercrime. It includes not only the right treatment of the digital evidence in order to be accepted in the Courts but also useful tools and techniques that can be applied to investigate an incident."

- Virginia Aguilar, CHFI, KPMG, Madrid.

EC-Council

EC-Council

6330 Riverside Plaza Ln NW
Suite 210
Albuquerque, NM 87120

Tel: +1.505.341.3228
Fax: +1.505.341.0050

http://www.eccouncil.org
E-mail: info@eccouncil.org