EC-Council CHFI

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to keep the learning engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by working forensic examiners

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- Introductory to intermediate experience in computer forensics
- A working understanding of operating systems, file systems and networking
- Our CEH camp is strongly recommended first — EC-Council recommends the same

TARGET AUDIENCE

- Digital forensic analysts and examiners
- Incident responders who must preserve evidence, not just contain a breach
- Security consultants and ethical hackers adding the forensics discipline
- Law enforcement officers and legal staff investigating digital crime

EXAM

312-49 — EC-Council CHFI, version 11

150 multiple-choice questions, scenario-based. Four hours.

There is no single pass mark. EC-Council sets a cut score per exam form, between 60% and 85%, to keep difficulty consistent across forms.

CHFI is **ANSI accredited** and is approved by the US Department of Defense under **directive 8140** for cyber forensics work roles.

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **EC-Council CHFI** certification. As with all our EC-Council training experiences, the exam is delivered in the classroom.

CHFI is the forensics credential for people who have to answer what happened, when, and who did it — and then prove it. It runs the whole investigation: acquiring and duplicating evidence without altering it, defeating anti-forensics, and analyzing what is left across Windows, Linux, macOS, networks, malware, web attacks, the dark web, cloud, email, social media, mobile and IoT.

The work is done on evidence rather than on slides. Students run major forensic investigation scenarios with the standard tools, which is the only way the discipline transfers. It maps to exam **312-49**, and the **exam voucher is available** at $1,199 USD.

COURSE OBJECTIVES

Primary course objectives:

- Run an investigation process that holds up: scope, authority, documentation, chain of custody
- Understand hard disks and file systems, and what actually survives on them
- Acquire and duplicate evidence without altering the original
- Recognize and defeat anti-forensics — wiping, hiding, timestamps, encryption
- Investigate Windows systems and the artifacts they leave behind
- Investigate Linux and macOS on their own terms, not by Windows habits
- Perform network forensics: capture, logs, and reconstructing what crossed the wire
- Analyze malware behavior and its traces on a compromised host
- Investigate web attacks and the server-side evidence they leave
- Work dark web and cloud forensics, where the evidence is not on a machine you own
- Investigate email and social media, including headers, accounts and attribution
- Perform mobile and IoT forensics across the major platforms and devices
- Present findings so they survive scrutiny by a court or a board

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

EC-Council CHFI

WHAT YOU WILL BE ABLE TO DO

- Acquire evidence forensically, and keep a chain of custody that holds
- Recover what an adversary tried to destroy or hide
- Follow an incident across hosts, networks, cloud and mobile devices
- Write findings that survive scrutiny by a court or a board

EXCLUSIVE LEARNING PACKAGE

- Forensic acquisition and imaging toolkit
- Disk, memory and mobile evidence image library
- Anti-forensics detection workshop pack
- CHFI video course
- CHFI reading plan and review guide
- CHFI certification practice exam

COURSE MODULES

01 Computer Forensics in Today's World
- Topic A: The forensics landscape and what drives an investigation
- Topic B: Legal, regulatory and ethical boundaries

02 Computer Forensics Investigation Process
- Topic A: Pre-investigation: authority, scope and readiness
- Topic B: Investigation phase and chain of custody
- Topic C: Post-investigation: reporting and testimony

03 Understanding Hard Disks and File Systems
- Topic A: Disk architecture and storage media
- Topic B: Windows, Linux and macOS file systems
- Topic C: What survives deletion, and where

04 Data Acquisition and Duplication
- Topic A: Live and static acquisition
- Topic B: Forensic duplication and write blocking
- Topic C: Validating an image and proving it unaltered

05 Defeating Anti-forensics Techniques
- Topic A: Wiping, hiding and obfuscation
- Topic B: Timestamp manipulation and trail obscuring
- Topic C: Encryption, and what can still be recovered

06 Windows Forensics
- Topic A: Volatile and non-volatile data collection
- Topic B: Registry, event log and file system artifacts
- Topic C: Browser, application and user activity

07 Linux and Mac Forensics
- Topic A: Linux artifacts, logs and file system evidence
- Topic B: macOS artifacts and property lists
- Topic C: Memory forensics on both

08 Network Forensics
- Topic A: Capture, and the traffic worth keeping
- Topic B: Log correlation across devices
- Topic C: Reconstructing an intrusion from the wire

09 Malware Forensics
- Topic A: Static and dynamic analysis
- Topic B: Behavior, persistence and traces on the host
- Topic C: Attribution, and its limits

10 Investigating Web Attacks
- Topic A: Web server and application logs
- Topic B: Common attack signatures in evidence
- Topic C: Reconstructing the attacker's path

11 Dark Web Forensics
- Topic A: How the dark web works, and what it leaves behind
- Topic B: Tor browser artifacts and investigation

12 Cloud Forensics
- Topic A: Investigating evidence you do not physically hold
- Topic B: Provider cooperation, jurisdiction and legal process
- Topic C: Container and serverless considerations

13 Email and Social Media Forensics
- Topic A: Headers, routing and message reconstruction
- Topic B: Account and platform evidence
- Topic C: Attribution and identity

14 Mobile Forensics
- Topic A: Mobile architecture and acquisition methods
- Topic B: Android and iOS artifacts
- Topic C: Application, location and messaging data

15 IoT Forensics
- Topic A: IoT architecture, protocols and attack surface
- Topic B: Acquiring evidence from embedded devices