

312-49: Computer Hacking Forensic Investigator (CHFI)

Investigate cyber incidents with forensically sound methods — and prepare for the CHFI 312-49 exam with practical case work.

DURATION

5 days · 40 hours

LEVEL

Advanced

CURRICULUM

14 modules · 9 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

When a breach, fraud or insider incident happens, organisations need to know exactly what occurred, and they need evidence that will stand up to scrutiny from management, regulators or a court. Digital forensic investigators provide that. This five-day course is exam-aligned preparation for the CHFI 312-49 exam, built around a realistic investigation that runs through the week.

Day one establishes the foundations: the forensic investigation process, legal considerations, first response, evidence handling and chain of custody, and how hard disks and file systems store data. Day two covers data acquisition and duplication, anti-forensics techniques and how to defeat them, and Windows forensics, including the registry, event logs, memory and user activity artefacts. Day three moves to Linux and macOS forensics and network forensics, using logs and packet captures to reconstruct events.

Day four covers web attack investigation, the dark web, email crimes and malware forensics, including static and dynamic analysis basics. Day five addresses cloud, mobile and IoT forensics, then brings the week together with writing a forensic report and an exam-readiness session.

This is independent, exam-aligned training; it does not use EC-Council courseware and Ace Skills Consulting does not claim to be an EC-Council Accredited Training Centre. Exam eligibility and registration are handled through EC-Council's official channels, so confirm the current version and requirements with EC-Council before booking.

Highlights

- 40 hours of live, investigation-focused training
- Evidence acquisition and chain of custody in practice
- Windows, Linux, network, cloud and mobile forensics
- Malware and email investigation labs
- Practice questions mapped to the exam areas

What's included

- Week-long investigation case with real artefacts
- Disk imaging and verification labs
- Memory and registry analysis
- Network, email and malware investigation exercises
- Forensic report writing workshop
- Practice questions with explanations
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Incident responders and SOC analysts
- Digital forensics and e-discovery professionals
- Law enforcement and fraud investigation staff
- IT security professionals handling internal investigations

Prerequisites

- Strong understanding of operating systems and networking
- Security fundamentals at Security+ or CEH level
- Comfort with command-line tools

Detailed curriculum — 5 days, 40 hours, 14 modules, 9 hands-on labs

Day 1 Investigation Process & Storage Fundamentals

8 hours

1.1 Forensic investigation process

- Phases of an investigation
- First response and scene handling
- Legal considerations and admissibility
- Chain of custody

1.2 Hard disks and file systems

- Disk structures and partitions
- Boot processes
- NTFS, FAT and ext file systems
- Deleted file recovery concepts

LAB Examine file system structures and recover deleted files · 50 min

1.3 Building the case

- Case briefing and scoping
- Documentation standards

Day 2 Acquisition, Anti-Forensics & Windows Forensics

8 hours

2.1 Data acquisition and duplication

- Live versus dead acquisition
- Hash verification
- Write blockers and imaging formats
- Memory acquisition

LAB Create and verify a forensic disk image · 45 min

2.2 Anti-forensics

- Data hiding and steganography
- Detecting anti-forensics
- Wiping and timestamp manipulation

2.3 Windows forensics

- Registry analysis
- User activity artefacts
- Event logs
- Memory analysis

LAB Build a timeline of user activity from Windows artefacts · 60 min

Day 3 Linux, macOS & Network Forensics

8 hours

3.1 Linux and macOS forensics

- Linux log and shell history analysis
- macOS file system and artefacts
- Linux memory forensics

LAB Investigate a compromised Linux server · 50 min

3.2 Network forensics

- Log correlation
- Investigating network attacks
- Packet capture analysis
- Wireless investigation basics

LAB Reconstruct an intrusion from packet captures and logs · 55 min

Day 4 Web, Email & Malware Forensics

8 hours

4.1 Web attacks and the dark web

- Web server log analysis
- Dark web investigation concepts
- Investigating web application attacks

LAB Trace a web attack through server logs · 40 min

4.2 Email investigation

- Email architecture and headers
- Email evidence collection
- Phishing and spoofing investigation

4.3 Malware forensics

- Static analysis basics
- Indicators of compromise
- Dynamic analysis in a sandbox
- Fileless malware investigation

LAB Analyse a malware sample in a sandbox · 50 min

Day 5 Cloud, Mobile & IoT Forensics, Reporting & Exam Readiness

8 hours

5.1 Cloud forensics

- Challenges of cloud investigations
- Container forensics
- Collecting evidence from AWS and Azure logs

5.2 Mobile and IoT forensics

- Android and iOS acquisition approaches
- IoT device investigation
- Mobile artefacts

LAB Review artefacts from a mobile device image · 35 min

5.3 Reporting and exam readiness

- Writing a forensic report
- Practice questions and review
- Presenting findings and expert testimony basics

LAB Write the final report for the week's case · 40 min

Skills and tools

Skills you will build

Digital forensics

Chain of custody

Disk imaging

File system analysis

Windows forensics

Memory forensics

Linux forensics

Network forensics

Email investigation

Malware analysis

Cloud forensics

Mobile forensics

Forensic reporting

Tools used in class

Autopsy

FTK Imager

Volatility

Wireshark

Registry Explorer

Sleuth Kit

CyberChef

REMnux

Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	Computer Hacking Forensic Investigator (CHFI)
Exam code	312-49
Format	Multiple choice
Official page	https://www.eccouncil.org/

Exam skill areas covered

Exam covers the fundamentals and the investigation process

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

How do I register for the CHFI exam?

Registration and eligibility are handled through EC-Council's official channels. We explain the process, but vouchers and eligibility decisions come from EC-Council.

Is this official EC-Council training?

No. This is independent, exam-aligned preparation using our own material and case studies.

Do I need CEH before CHFI?

It is not required, but CEH-level understanding of attacks makes investigations much easier to follow.

Which tools will I use?

Mainly free and open-source forensic tools such as Autopsy, Volatility and Wireshark, so you can continue practising afterwards.

Can you run this for an investigations team?

Yes. Private batches can focus on the evidence sources most relevant to your organisation.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/312-49-computer-hacking-forensic-investigator-chfi · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

CEH, CHFI and CND are trademarks of the International Council of E-Commerce Consultants (EC-Council). All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed

by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website.
Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.