

EC-COUNCIL

CHFI — Computer Hacking Forensic Investigator Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

40 HOURS

5 DAYS

At a glance

COURSE	CHFI — Computer Hacking Forensic Investigator
TRACK	EC-Council
DOMAIN	Cyber Security
LEVEL	Intermediate
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Fifteen modules, mapped one-for-one to the official CHFI v11 blueprint and taught in the same order, so nothing on the exam is left uncovered.

CHFI is not an attack course. It is about what happens after the attack — recovering evidence from disks, memory, networks, phones and cloud accounts in a way that survives scrutiny. The discipline is procedural before it is technical: an artefact you cannot account for is an artefact you cannot use. Every module below is taught with that constraint in front of it.

Artificial intelligence appears in v11 as a working tool rather than the organising idea. It shows up where it genuinely earns its place — triage of large data sets, automation and orchestration of repetitive acquisition work — and we treat it the same way: useful for volume, never a substitute for the investigator's own verification.

Half the classroom time is hands-on, working cases end to end against disk images, memory captures and traffic we have prepared, so you are reconstructing an incident rather than answering a quiz about one.

Module 01 — Computer Forensics in Today's World

What the discipline is, what it is for, and the rules that make evidence admissible rather than merely interesting.

- Forensic science fundamentals and the types of cybercrime you will be asked to investigate
- The forensic readiness of an organisation, and what to put in place before an incident
- Roles and responsibilities of the forensic investigator within an incident
- Legal compliance, jurisdiction, and the standards that govern digital evidence
- Where artificial intelligence assists forensic work, and where its output must be verified
- Forensics automation and orchestration, and what it can safely take off your hands
- Evidence admissibility, chain of custody and the consequences of breaking it
- Reporting obligations and the investigator as an expert witness

Module 02 — Computer Forensics Investigation Process

The full lifecycle of a case, from the first phone call to testimony.

- The pre-investigation phase: building a lab, tooling, and authorisation to act
- Search and seizure, warrants, and lawful acquisition of devices
- First responder procedure and documenting the scene before touching it
- Evidence collection, packaging, transport and secure storage
- Data acquisition, verification and hashing as an integrity control
- Evidence examination, analysis and correlation across sources
- Case documentation, note-taking discipline and the forensic report
- Testifying to your findings and defending your methodology under challenge

Module 03 — Understanding Hard Disks and File Systems

You cannot recover what you do not understand at the structural level.

- Physical and logical disk structures, sectors, clusters and slack space
- Partitioning schemes and the boot process on Windows and on Linux
- FAT, exFAT and NTFS internals, including the master file table

- Linux file systems — ext2, ext3, ext4 — and macOS APFS and HFS+
- RAID configurations and reconstructing arrays for analysis
- File carving from unallocated space when metadata is gone
- Hex-level examination, file signatures and identifying disguised files
- Solid-state storage, wear levelling, TRIM and their effect on recoverability

Module 04 — Data Acquisition and Duplication

Getting a copy that will stand up, without altering the original.

- Static and live acquisition, and choosing between them under pressure
- Logical, sparse and bit-stream imaging, and what each one preserves
- Write blockers, hardware and software, and verifying they worked
- Volatile memory capture and the order of volatility
- Imaging formats, compression and segmenting large evidence sets
- Hash verification before, during and after duplication
- Acquiring from encrypted volumes, RAID sets and virtual machines
- Validation, contingency planning and what to do when acquisition fails

Module 05 — Defeating Anti-Forensics Techniques

Suspects hide their tracks. This module is about noticing that they tried.

- Anti-forensic categories and the goals behind each one
- Data deletion, wiping and secure-erase, and what survives them
- Recovering deleted files, partitions and reformatted volumes
- Password protection, encryption and lawful approaches to locked data
- Steganography, alternate data streams and other hiding techniques
- Artefact wiping, trail obfuscation and timestamp manipulation
- Detecting file extension and metadata tampering
- Countering anti-forensics and documenting the attempt as evidence in itself

Module 06 — Windows Forensics

The operating system you will encounter most, and the artefacts it leaves behind.

- Collecting volatile and non-volatile data from a live Windows host
- Windows memory analysis: processes, network connections and injected code
- Registry structure and the forensic value of specific hives and keys
- Windows event logs, ShimCache, Amcache and program execution artefacts
- File system artefacts: prefetch, jump lists, LNK files and recycle bin
- Browser, cache and user activity reconstruction
- Windows timeline analysis and building a defensible sequence of events
- Correlating artefacts to distinguish user action from automated behaviour

Module 07 — Linux and Mac Forensics

Two platforms with different conventions, both common in real cases.

- Linux volatile and non-volatile data collection

- Linux log architecture, syslog, journald and shell history artefacts
- Linux memory analysis and identifying malicious processes
- macOS file system layout, APFS structures and system artefacts
- macOS logs, property lists and user activity traces
- Mail, browser and application data on both platforms
- Mounting and examining images from Unix-family systems safely
- Timeline reconstruction across mixed-platform environments

Module 08 — Network Forensics

Evidence that exists only while it is in motion, and the logs that outlive it.

- Network forensics fundamentals and the sources worth collecting
- Log correlation across firewalls, routers, proxies and endpoints
- Centralised logging, SIEM and the evidential value of aggregated logs
- Packet capture, indexing and analysis of recorded traffic
- Detecting and reconstructing network-based attacks from traffic
- Wireless network forensics and attacks specific to it
- Identifying encrypted and tunnelled traffic, and what can still be inferred
- Documenting network findings so they hold up alongside host evidence

Module 09 — Malware Forensics

Establishing what a sample does, safely, and what it did on this machine.

- Malware classification, propagation and entry points
- Building and using an isolated analysis environment
- Static analysis: file structure, strings, imports and packing
- Dynamic analysis: behaviour, process, registry, file and network activity
- Memory-resident and fileless malware, and finding them after the fact
- Extracting indicators of compromise from an analysed sample
- Attributing on-disk artefacts to a specific malware family
- Reporting malware findings for both technical and legal audiences

Module 10 — Investigating Web Attacks

Reading a compromise backwards from the web server that took the hit.

- Web application architecture and where evidence accumulates
- Indicators that a web application or server was attacked
- Apache, IIS and application log analysis
- Investigating injection, cross-site scripting and file upload attacks
- Detecting web shells, backdoors and unauthorised code changes
- Investigating denial-of-service and brute-force activity
- Reconstructing the attacker's session and the data they reached
- Preserving web evidence when the server must stay in production

Module 11 – Dark Web Forensics

Investigating activity that is deliberately structured to resist investigation.

- Dark web concepts, onion routing and how anonymity is achieved
- The Tor browser, its architecture and its forensic footprint
- Tor artefacts on a suspect machine, in memory and on disk
- Identifying dark web marketplace and communication activity
- Cryptocurrency transactions as an investigative thread
- Legal and ethical limits when investigating anonymised services
- Correlating dark web indicators with conventional host evidence
- Documenting findings where attribution is inherently partial

Module 12 – Cloud Forensics

Someone else holds the evidence, and you have to ask for it correctly.

- Cloud service and deployment models, and what each means for an investigation
- The shared responsibility model applied to evidence access
- Jurisdiction, data residency and cross-border legal process
- Acquiring evidence from major cloud providers through supported mechanisms
- Cloud logging sources: control plane, audit, storage and identity logs
- Container and virtual machine forensics in cloud environments
- Investigating account compromise and cloud misconfiguration incidents
- Cloud forensic challenges: volatility, multi-tenancy and limited access

Module 13 – Email and Social Media Forensics

Messages, accounts and the metadata that tells you more than the text does.

- Email system architecture, protocols and where copies exist
- Email header analysis and tracing a message to its origin
- Investigating phishing, spoofing, spam and business email compromise
- Recovering email from client stores, servers and archives
- Social media as an evidence source, and lawful acquisition from platforms
- Account takeover, impersonation and harassment investigations
- Authenticating message and account evidence against challenge
- Preservation requests, legal process and working with service providers

Module 14 – Mobile Forensics

The device that goes everywhere the suspect goes.

- Mobile hardware and operating system architecture on Android and iOS
- Mobile storage layouts and where user data actually sits
- Handling a seized device: isolation, power state and avoiding remote wipe
- Logical, file system and physical acquisition methods
- Locked devices, encryption and the limits of lawful access
- Analysing call, message, location, application and cloud-sync data
- SIM card examination and carrier-held records

- Reporting mobile findings and explaining acquisition limits honestly

Module 15 – IoT Forensics

Small devices, awkward storage, and evidence nobody expected to need.

- IoT architecture, components and communication protocols
- IoT threats and the incidents that generate forensic demand
- Identifying evidence sources across device, gateway, network and cloud
- Acquiring data from embedded storage and constrained devices
- Firmware extraction and analysis
- Analysing IoT protocol traffic for evidence of interference
- Correlating device evidence with companion applications and cloud accounts
- Practical limits of IoT forensics and how to state them in a report

Who should take this

Incident responders and SOC analysts who need to work a case beyond containment, digital forensics practitioners formalising what they already do, system and network administrators drawn into investigations, and legal, audit and compliance staff who must commission forensic work and assess what comes back.

You will need working knowledge of operating systems, file systems and networking, and to be comfortable on a command line. Prior forensic experience is not required.

The exam

- Computer Hacking Forensic Investigator, exam code 312-49 — 150 multiple-choice questions, four hours

EC-Council sets the passing mark per exam form rather than at a single fixed figure, so the cut score varies between forms within the range they publish. The exam voucher is purchased separately from the certification body; we arrange it on your behalf and send you the code, and you book your own exam date.

How we deliver it

Five days, classroom or online live, or at your office for a private group. Half the time is hands-on, working prepared cases end to end. Small cohorts, so everyone gets lab time rather than watching someone else have it.

Mapped to the official CHFI v11 blueprint. Taught from Hacky Security's own curriculum and lab estate by instructors who also work our security operations centre.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/chfi/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.