# CHFI - Computer Hacking Forensic Investigator

InfoSec Training Online with EC-Council iClass. Online, Live, Instructor Led

Exam Details:

Questions: 50

Time: 120 Minutes

Passing Score: 70%

Format: Multiple choice

Cost: $150.00

Other Requirements: Must sign an Ethics Agreement.

Renewal: None.

Editors' Quick Thoughts

This cert may not be as hot as CEH, but it is definitely covering a hot area of security - forensics. Think of this as CSI for computers. There's defintiely a need for vendor-neutral certifications in forensics. This is one of them. CCE is probably it's biggest competitor. SANS is also in this space. But the big boy on the block is a vendor-specific credential, EnCase. As the federal government and the court system move into a future where eDiscovery is already the law for pretty much every type of case, the need for forensics professioanls is without a doubt growing. One word of caution (and this is less about CHFI and more about forensics in general)is that this is an exciting field technically, but sometimes the evidence you must see is disturbing.

From the Horse's Mouth (EC-Council's Web Site Content):

Computer hacking forensic investigation  is the  process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. CHFI investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information.

Securing and analyzing electronic evidence is a central theme in an ever-increasing number of conflict situations and criminal cases. Electronic evidence is critical in the following situations:

- Disloyal employees
- Computer break-ins
- Possession of pornography
- Breach of contract
- Industrial espionage
- E-mail Fraud

- Bankruptcy
- Disputed dismissals
- Web page defacements
- Theft of company documents

Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud.

The CHFI course will provide participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law.

The CHFI course will benefit:

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance and other professional
- Government agencie
- IT managers

More from EC-Council.

EH-Net Resources

-

Book Recommendations

-

Related Forums

-

Related News Feed