INVESTIGATE

C|HFI

COMPUTER HACKING FORENSIC INVESTIGATOR

EC-Council

CORE/SPECIALIST

RSA

COURSE OVERVIEW

CHFIv9 covers a detailed methodological approach to computer forensics and evidence analysis. It provides the necessary skillset for identification of intruder's footprints and gathering necessary evidence for its prosecution. All major tools and theories used by cyber forensics industry are covered in the curriculum.

The certification can fortify the applied knowledge level of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, computer and network security professionals, and anyone who is concerned about the integrity of the network and digital investigations.

WHAT I WILL LEARN

- Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling.
- Perform anti-forensic methods detection.
- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred.
- Extract and analyze of logs from various devices like proxy, firewall, IPS, IDS, Desktop, laptop, servers, SIM tool, router, firewall, switches AD server, DHCP logs, Access Control Logs & conclude as part of investigation process.
- Identify & check the possible source/incident origin.
- Recover deleted files and partitions in Windows, Mac OS X, and Linux.
- Conduct reverse engineering for known and suspected malware files.
- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents.

COURSE OUTLINE

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Operating System Forensics
- Defeating Anti-Forensics Techniques
- Data Acquisition and Duplication
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Investigative Reports

EXAM INFORMATION

EXAM TITLE: CHFI ECO 312-49

NUMBER OF QUESTIONS: 150

DURATION: 4 hours

TEST FORMAT: Multiple Choice

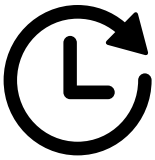
TEST DELIVERY: ECC EXAM PORTAL

PASSING SCORE

In order to maintain the high integrity of our certifications exams, EC-Council Exams are provided in multiple forms (I.e. different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has "real world" applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall "Cut Score" for each exam form. To ensure each form has equal assessment standards, cut scores are set on a "per exam form" basis. Depending on which exam form is challenged, cut scores can range from 60% to 78%.

TARGET AUDIENCE

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



COURSE DURATION
4 hours

RSA

Contact us at:
RSAU@rsa.com