EC-Council Certified Hacking Forensic Investigator

Course code: CHFI

The CHFI Certified Hacking Forensic Investigator is a unique training where students can learn with the newest techniques and tools in the discipline of computer forensics from a vendor-neutral perspective. The C|HFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personal, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure. Computer forensics training teaches that computer forensics investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. 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. Computer forensic 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.Students who attend this training will get a voucher for the globaly recognized CHFI 312-49 Exam.

Who is the course for

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

What we teach you

- The process of investigating cyber-crime, laws involved, and the details in obtaining a search warrant.
- Different types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- Roles of first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting the crime scene
- How to recover deleted files and deleted partitions in Windows, Mac OS X, and Linux
- The process involved in forensic investigation using Access Data FTK and Encase Steganography and its techniques, Steganalysis, and image file forensics
- Password Cracking Concepts, tools, types of password attacks and how to investigate password protected file breach
- Different types of log capturing techniques, log management, time synchronization, log capturing tools
- How to investigate logs, network traffic, wireless attacks, and web attacks
- How to track e-mails and investigate e-mail crimes and many more

Required skills

All attendants should have a solid understanding of all hacking techniques covered in the GOC3 an CEHv8 training.

Course outline

- Forensic investigation process
- Collecting the digital evidence of cyber crime
- Proper incident response handling
- Setting a Computer Forensics Lab
- Understanding Hard Disks and File Systems
- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Forensics Investigation using AccessData FTK
- Forensics Investigation Using EnCase
- Steganography and Image File Forensics
- Application Password Crackers

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Log Capturing and Event Correlation
- Network Forensics, Investigating Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics
- Investigative Reports
- Becoming an Expert Witness

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk