EC-COUNCIL COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)

5 Days

Overview

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

Students attending this course will take exam **ECO-349** to achieve their CHFI certification.

Prerequisites

A foundational knowledge of computers Operating Systems and Networking protocols.

Course Overview

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 professionals
- Government agencies
- IT managers

Course Outline:

Computer Forensics and Investigations as a Profession

Understanding Computer Investigations

Working with Windows and DOS Systems

Macintosh and Linux Boot Processes and Disk Structures

The Investigator's Office and Laboratory

Current Computer Forensics Tools

Digital Evidence Controls

Processing Crime and Incident Scenes

Data Acquisition

Computer Forensic Analysis

E-mail Investigations

Recovering Image Files

Writing Investigation Reports

Becoming an Expert Witness

Computer Security Incident Response Team

Logfile Analysis

Recovering Deleted Files

Application Password Crackers

Investigating E-Mail Crimes

Investigating Web Attacks

Investigating Network Traffic

Investigating Router Attacks

The Computer Forensics Process

Data Duplication

Windows Forensics

Linux Forensics

Investigating PDA

Enforcement Law and Prosecution

Investigating Trademark and Copyright Infringement