Computer Hacking Forensic Investigator (CHFI)

Duration 5 Days

COURSE DESCRIPTION

CHFI v10 includes all the essentials of digital forensics analysis and evaluation required for today's digital world. From identifying the footprints of a breach to collecting evidence for a prosecution, CHFI v10 walks students through every step of the process with experiential learning. This course has been tested and approved by veterans and top practitioners of the cyber forensics industry.

CHFI v10 is engineered by industry practitioners for both professionals and aspiring professionals alike from careers including forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.

WHO SHOULD ATTEND

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

- 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

PREREQUISITES

- IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, and incident response.
- Knowledge of Threat Vectors.

CERTIFICATION

The CHFI certification is awarded after successfully passing the exam EC0 312-49. CHFI EC0 312-49 exams are available at ECC exam center around the world.

- **Number of Questions:** 150
- **Passing Score:** 70%
- **Test Duration:** 4 hours
- **Test Format:** Multiple choice

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th   **Call us today 0-2634-7993-4**

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

OUTLINE

- **Module 01**: Computer Forensics in Today's World
- **Module 02**: Computer Forensics Investigation Process
- **Module 03**: Understanding Hard Disks and File Systems
- **Module 04**: Data Acquisition and Duplication
- **Module 05**: Defeating Anti-Forensics Techniques
- **Module 06**: Windows Forensics
- **Module 07**: Linux and Mac Forensics
- **Module 08**: Network Forensics
- **Module 09**: Investigating Web Attacks
- **Module 10**: Dark Web Forensics
- **Module 11**: Database Forensics
- **Module 12**: Cloud Forensics
- **Module 13**: Investigating Email Crimes
- **Module 14**: Malware Forensics
- **Module 15**: Mobile Forensics
- **Module 16**: IoT Forensics