

Every crime leaves a trail of evidence



**SECURING
NETWORKS WITH
FORENSIC
SCIENCE**

Computer Hacking Forensic Investigator v9

INTRODUCING CHFI V9: WORLD'S MOST COMPREHENSIVE COMPUTER FORENSIC CERTIFICATION PROGRAM

Digital technologies are changing the face of business. As organizations rapidly embracing digital technologies such as cloud, mobile, big data and IOT, the context of digital forensics is more relevant than before. The growing number of cybercrimes has changed the role of forensics from DNA to Digital.

According to the market research report published by IndustryARC, by 2020, the digital forensics market will reach 4.8 billion USD. IndustryARC also predicts that the maximum use of digital forensics is from the federal sector and this will grow from \$1,097.2 million in 2015 to \$2,060.5 million by 2020. The major drivers for this are increasing threats from cybercrime and terrorist attacks. Foote Partners, which tracks information technology (IT) jobs across all skill levels, projects the global demand for cyber security talent to rise to six million by 2019, with an expected shortfall of 1.5 million professionals.

Over the last many years, EC-Council's CHFI certification has gained massive traction and recognition amongst Fortune 500 enterprises globally. It has immensely benefited professionals from law enforcement, criminal investigation, defense, and security field. CHFI v9, the latest version of the program has been designed for professionals handling digital evidence while investigating cybercrimes. It is developed by an experienced panel of subject matter experts and industry specialists, and also has set global standards for computer forensics best practices. In addition, it also aims at elevating the knowledge, understanding, and skill levels of in cyber security and forensics practitioners.

ABOUT CHFI v9

CHFI v9 covers detailed methodological approach to computer forensic 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 forensic 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.

CHFI provides necessary skills to perform effective digital forensic investigation



It is a comprehensive course covering major forensic investigation scenarios that enables students to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carryout computer forensic investigation leading to prosecution of perpetrators



CHFI presents a methodological approach to computer forensic including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence

COURSEWARE DETAILS



COURSE DETAILS

Course Title: Computer Hacking Forensic Investigator (CHFI) v9

Duration: 40 hours (5 days, 9:00AM – 5:00PM)

Class Format:

- Instructor-led classroom – Authorized Training Center (ATC)
- Live online training – iClass



EXAM DETAILS

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: MCQ
- Test Delivery: ECC exam portal



PREREQUISITES

- IT/forensics professionals with basic knowledge on IT/cyber security, computer forensics, and incident response
- Prior completion of CEH training would be an advantage



WHO SHOULD ATTEND

- | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">• Anyone interested in cyber forensics/investigations• Attorneys, legal consultants, and lawyers• Law enforcement officers• Police officers• Federal/ government agents• Defense and military• Detectives/ investigators | <ul style="list-style-type: none">• Incident response team members• Information security managers• Network defenders• IT professionals, IT directors/ managers• System/network engineers• Security analyst/ architect/ auditors/ consultants |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



WHAT'S NEW IN CHFI V9

- 14 comprehensive modules and 39 labs
- More than 40 percent of new labs
- More than 400 new/updated tools
- Classroom friendly curriculum with diagrammatic representation of concepts and examples
- New and rich presentation style with eye catching graphics
- Coverage of latest operating systems
- Updated patch management and testing environment
- Well tested, result oriented, descriptive and analytical lab manual to evaluate the presented concepts

COURSE OUTLINE

CHFI v9 curriculum is a comprehensive course with 14 training modules covering major forensic investigation scenarios



Module 1. Computer forensics in today's world



Module 2. Computer forensics investigation process



Module 3. Understanding hard disks and file systems



Module 4. Data acquisition and duplication



Module 5. Defeating anti-forensics techniques



Module 6. Operating system forensics



Module 7. Network forensics



Module 8. Investigating web attacks



Module 9. Database forensics



Module 10. Cloud forensics



Module 11. Malware forensics



Module 12. Investigating email crimes



Module 13. Mobile forensics



Module 14. Forensics report writing and presentation



WHY CHFI

- The CHFI v9 program has been redesigned and updated after thorough investigation including current market requirements, job tasks analysis, and recent industry focus on forensic skills
- It is designed and developed by experienced subject matter experts and digital forensics practitioners
- CHFI is a complete vendor neutral course covering all major forensics investigations technologies and solutions
- CHFI has detailed labs for hands-on learning experience. On an average, approximately 50% of training time is dedicated to labs
- It covers all the relevant knowledge-bases and skills to meets with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- The student kit contains large number of white papers for additional reading
- The program presents a repeatable forensics investigation methodology required from a versatile digital forensic professional which increases employability
- The student kit contains several forensics investigation templates for evidence collection, chain-of-custody, final investigation reports, etc.
- The program comes with cloud-based virtual labs enabling students to practice various investigation techniques in a real-time and simulated environment

ENDORSEMENTS AND TESTIMONIALS



IDENTITY



PRIVACY



ENDORSEMENTS



NSA and CNSS: Compliant with 4012 (Senior System Managers) training standards for information security professionals in the federal government by the United States National Security Agency (NSA) and the Committee on National Security Systems (CNSS)



NICE: Accepted into National Infocomm Competency Framework (NICE) infocomm professionals competency requirement list



DVA: The Department of Veterans Affairs (DVA) has included CHFI under its GI Bill for the reimbursement of test fees for veterans and other eligible persons in accordance with the provisions of PL 106-419



KOMLEK and CPS: The Malaysian Military Cyber Security Warfare Department (KOMLEK) has stipulated their military professionals to be CHFI Certified as part of their Cyber Warfare Training Program (CPS)



TESTIMONIALS

"It is my pleasure to take the time to praise the EC-Council for having such a magnificent class, specifically THE Computer Hacking Forensic Investigator course. The course had an abundance of information, utilities, programs, and hands on experience. I am a consultant at Dell and we do have a lot of technical training, but I must comment that this one is one of the best trainings I have seen in several years. I will definitely recommend this course to all my colleagues."

– *Hector Alvarez, CHFI, Enterprise & Storage Consultant, Dell Corporation, Austin, Texas*

"All the treatment has been excellent, the material and the content of the course overcomes my expectations. Thanks to the instructor and to Idera for their professionalism."

– *Sergio Lopez Martin, CHFI, Security Sales, IBM, Spain*

"CHFI is a certification that gives a complete overview of the process that a forensic investigator must follow when is investigating a cybercrime. It includes not only the right treatment of the digital evidence in order to be accepted in the Courts but also useful tools and techniques that can be applied to investigate an incident."

– *Virginia Aguilar, CHFI, KPMG, Madrid*

"The Computer Hacking Forensic Investigator (CHFI) certification has been instrumental in assuring both my company and our clients that my skillset is among the elite in the cyber security and response profession. The CHFI allows my company to readily identify to our DoD clients that our team is trained to perform the rigorous functions required of cyber threat response team. Our company can now better brand our capability to investigate cyber security incidents, perform computer/malware forensic analysis, identify active threats, and report our findings."

– *Brad W. Beatty, Cyber Security Analyst, Booz Allen Hamilton, USA*



About EC-Council

EC-Council (International Council of E-Commerce Consultants) is one of the world's largest certification bodies for information security professionals. EC-Council is a member-based organization that certifies individuals in various information security and ebusiness skills. It has been certified by American National Standards Institute to meet its ANSI 17024 standard. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI) and EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT) programs, and as well as many other programs. These programs are offered in over 140 countries and have trained over 150,000 and certified more than 60,000 security professionals through a training network of over 500 training partners globally.

Individuals who have achieved EC-Council certifications include those from some of the finest organizations around the world such as the US Army, the FBI, Microsoft, IBM and the United Nations.