Microtek LEARNING

EC-Council

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: Please refer https://cert.eccouncil.org/faq.html
- Test Duration: 4 hours
- Test Format: MCQ
- Test Delivery: ECC exam portal

PREREQUISITES

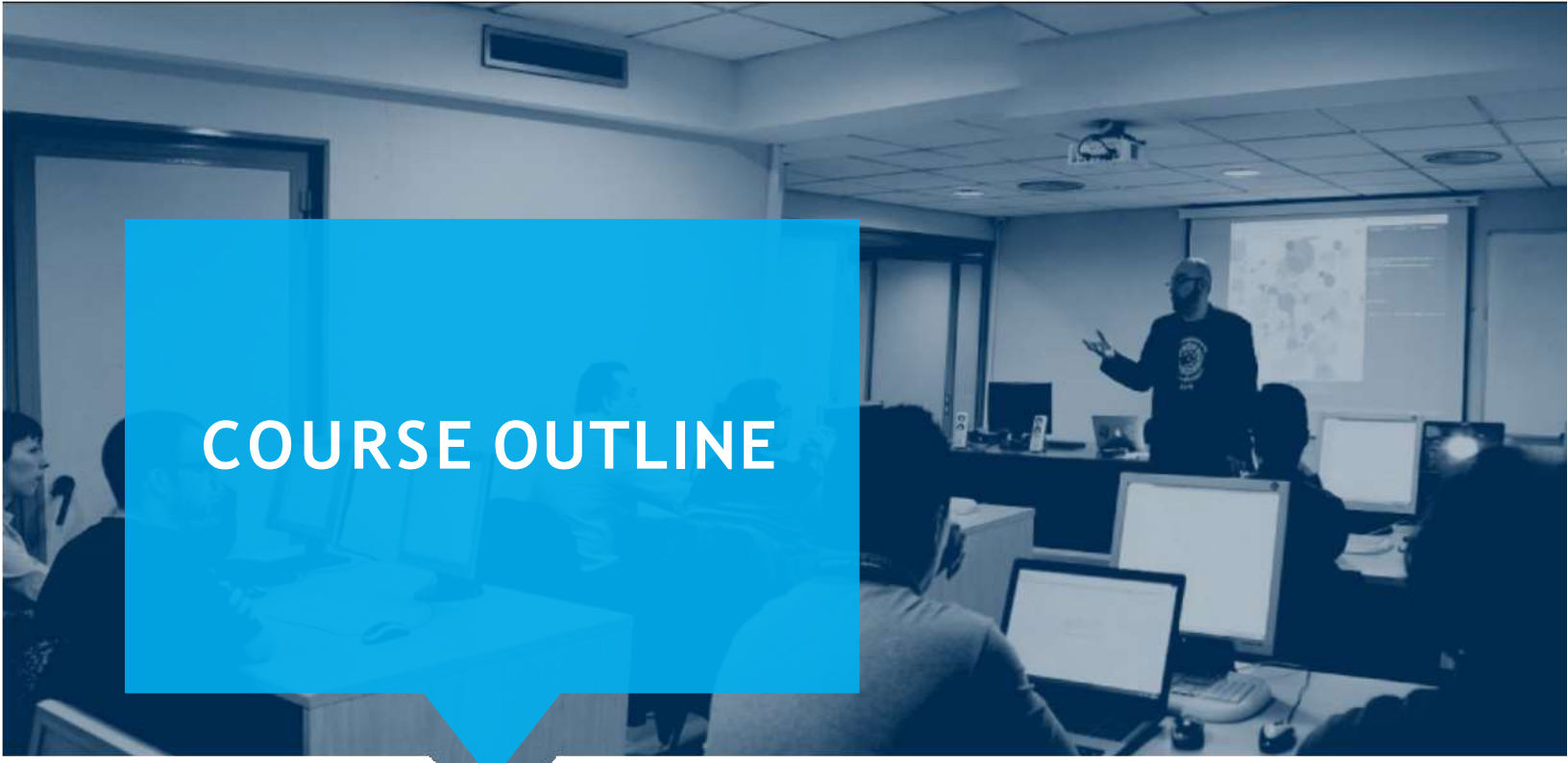
- IT/forensics professionals with basic knowledge on IT/cybersecurity, computer forensics, and incident response
- Prior completion of CEH training would be an advantage

WHO SHOULD ATTEND

- Anyone interested in cyber forensics/investigations
- Attorneys, legal consultants, and lawyers
- Law enforcement officers
- Police officers
- Federal/ government agents
- Defense and military
- Detectives/ investigators
- 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?

- We are one of the few organizations that specialize in information security (IS) to achieve ANSI 17024 accreditation for its Computer Hacking Forensic Investigator certification
- 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 40% 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

Microtek
LEARNING

For any query [Contact Us - MicrotekLearning]