GIT
Creating IT Professional

CHFI™ v10

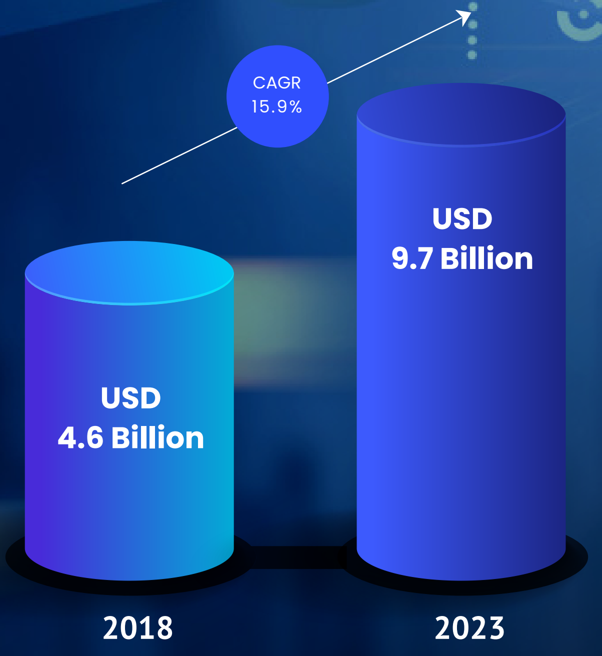
Computer Hacking Forensic INVESTIGATOR

When Hackers Are **SMART,** Investigators Need To Be **SMARTER.**

Lead The Digital Forensics Movement By Becoming A **Computer Hacking Forensic Investigator** With **EC-Council.**

www.gitinfo.com

training@gitinfo.com



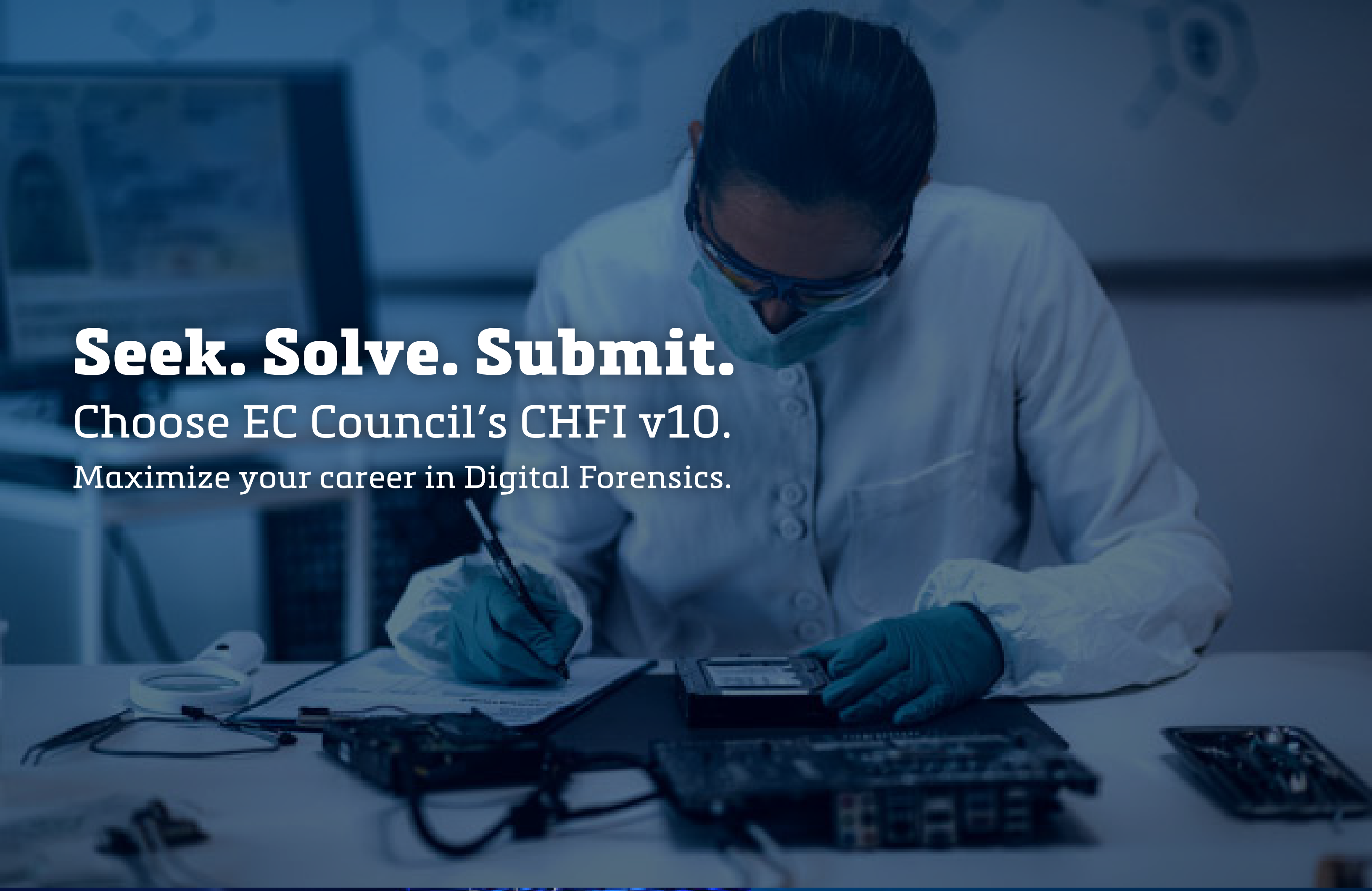
Digital Forensic Market Growth

Every crime leaves a digital footprint, and we have the skills to track those footprints. Every crime leaves a digital trail and with EC Council's CHFI v10, you will learn to unravel these pieces of evidence, decode them and report them. From decoding a hack to taking legal action against the perpetrators, you will be an active respondent in times of cyber-breaches.

With organizations rapidly adopting new digital technologies and cyberattacks being a prime risk factor*, it is no surprise that computer forensics is the need of the hour. The estimated growth of the worldwide forensics market is projected at USD 9.7 billion by 2023*.

[1]: World Economic Forum Report 2021

[2]: https://www.marketsandmarkets.com/Market-Reports/digital-forensics-market-230663168.html



Seek. Solve. Submit.

Choose EC Council's CHFI v10.

Maximize your career in Digital Forensics.

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.

With our years of expertise and experience, comes CHFI v10.

ANSI 17024 accredited Certification Program | Mapped to the NICE 2.0 framework | Recognized by the DoD under Directive 8570

- Includes critical modules in Dark Web Forensics and IoT Forensics
- More than 50% of new and advanced forensic labs
- Extensive coverage of Malware Forensics (latest malware samples such as Emotet and EternalBlue)
- Latest forensic tools including Splunk, DNSQuerySniffer, etc.
- Significant coverage of forensic methodologies for public cloud infrastructure, including Amazon AWS and Microsoft Azure
- In-depth focus on Volatile and Non-volatile data acquisition and examination process (RAM Forensics, Tor Forensics, etc.)
- More than 50GB of crafted evidence files for investigation purposes
- New techniques such as Defeating Anti-forensic technique, Windows ShellBags including analyzing LNK files and Jump Lists
- Massive updates on all modules in CHFI
- Accepted and trusted by cybersecurity practitioners across the Fortune 500 globally

Valued by Leading Organizations Across the World

CISCO
J.P.Morgan
AT&T
IBM
HCL
KPMG
pwc
GE
BOEING
NTT DATA
tcs TATA CONSULTANCY SERVICES
PayPal
Reliance
PEPSICO
paloalto NETWORKS
accenture
FUJITSU
SGX
Atos
Deloitte.
genpact
HUAWEI
SAUDI ARABIAN AIRLINES
أرامكو السعودية saudi aramco
HSBC
Marriott INTERNATIONAL
QATAR AIRWAYS القطرية
salesforce
gsk
EY
DELL
Microsoft
AIRBUS
L&T Infotech
Capgemini

Industries that prefer CHFI professionals

- e-Businesses
- Legal Firms
- Banking and Finance
- Law Enforcement
- Government Agencies
- Information Technology
- Defense and Security
- Digital Forensics Service Providers

Why CHFI v10?

- EC-Council is one of the few ANSI 17024 accredited institutions globally that specializes in Information Security. The Computer Hacking Forensic Investigator (CHFI) credential is an ANSI 17024 accredited certification.
- The CHFI v10 program has been redesigned and updated after a thorough investigation into current market requirements, job tasks analysis, and the recent industry focus on forensic skills.
- It is designed and developed by experienced subject matter experts and digital forensics practitioners.
  - CHFI v10 program includes extensive coverage of Malware Forensics processes, along with new modules such as Dark Web Forensics and IoT Forensics.
  - It also covers detailed forensic methodologies for public cloud infrastructure, including Amazon AWS and Azure.
  - The program is developed with an in-depth focus on Volatile data acquisition and examination processes (RAM Forensics, Tor Forensics, etc.).
- CHFI v10 is a complete vendor-neutral course covering all major forensics investigation technologies and solutions.
- CHFI has detailed labs for a hands-on learning experience. On average, 50% of training time is dedicated to labs, loaded on EC-Council's CyberQ (Cyber Ranges).
- It covers all the relevant knowledge bases and skills to meet regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- It comes with an extensive number of white papers for additional reading.
- The program presents a repeatable forensics investigation methodology from a versatile digital forensic professional, increasing employability.
- The courseware is packed with forensics investigation templates for evidence collection, the chain of custody, final investigation reports, etc.
- The program comes with cloud-based virtual labs, loaded on advanced Cyber Ranges, enabling students to practice various investigation techniques in real-time and realistically simulated environments.

Course 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

Training @ EC Council with CHFI v10

iLearn (Self-Study)

This solution is an asynchronous, self-study environment that delivers EC-Council's sought-after CHFI digital forensics training courses in a streaming video format.

iWeek (Live Online)

This solution is a live, online, instructor-led training course, allowing students to attend the CHFI digital forensics training course from anywhere with an internet connection.

Master Class

This solution offers the opportunity to learn Certified Hacking Forensic Investigator from world-class instructors in collaboration with top digital forensics professionals.

Training Partner (Instructor led training)

CHFI v10 is available globally through EC-Council's Authorized Training Partners. Conveniently located in your area, this offers you the benefit of learning from experienced certified EC-Council instructors along with your peers to gain real-world skills.

Academia

This solution offers CHFI v10 through EC-Council Academia Partner institutions and is for students enrolled in applicable college or university degree programs.

CHFI Exam Details

Number of Questions: **150**

Test Duration: **4 hours**

Test Format: **Multiple choice**

Test Delivery: **EC-Council Exam Portal**

Recommended Prerequisites

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

CHFI v10 – Recommended by the very best.

Recommendations / Accreditations / Mapping

The National Initiative for Cybersecurity Education (NICE)

American National Standards Institute (ANSI)

Committee on National Security Systems (CNSS)

United States Department of Defense (DoD)

National Infocomm Competency Framework (NICF)

MSC

KOMLEK

American Council on Education (ACE)

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 definitively 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 Itera for their professionalism.

- Sergio Lopez Martin, CHFI, Security Sales, IBM, Spain

> CHFI is a certification that gives an 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's sole purpose is to build and refine the cybersecurity profession, globally. We help individuals, organizations, educators, and governments address global workforce problems through the development and curation of world-class cybersecurity education programs and their corresponding certifications and provide cybersecurity services to some of the largest businesses globally.

Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, Intelligence Community, NATO, and over 2000 of the best Universities, Colleges, and Training Companies, our programs have proliferated through over 140 Countries and have set the bar in cybersecurity education.

Best known for the Certified Ethical Hacker program, we are dedicated to equipping over 230,000 information age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer.

We are an ANSI 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570, in the UK by the GCHQ, CREST, and a variety of other authoritative bodies that influence the entire profession. Founded in 2001, EC-Council employs over 400 people worldwide with 10 global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL.

Learn more at **www.eccouncil.org**