CHFI
Computer Hacking Forensic INVESTIGATOR

EC-Council
Building A Culture Of Security

COMPUTER HACKING FORENSIC INVESTIGATOR V11

Build Ultimate Investigative Skills And Organizational Forensic Readiness With Advanced Strategies

Master Skills of Forensic Investigation

❯Decode ❯Compile ❯Defend ❯Legal Action

Digital Forensics—The Need of the Hour Amidst Escalating Threats

In 2022, phishing topped the cybercrimes reported to the U.S. Internet Crime Complaint Center, affecting about 300,497 individuals, with nearly 58,859 personal data breaches reported. [1]

As per the 2022 Internet Crime Report, investment fraud led to the highest financial losses for individuals in the U.S., totaling over $3.3 billion. Business email compromise (BEC) followed with reported losses of around $2.7 billion, while victims of tech support fraud reported losses of $806 million. [2]

The global average cost of a data breach in 2023 was $4.45 million, a 15% increase over three years, as per the Cost of Data Breach Report 2023. [3]

Why is Digital Forensics Crucial For Organizations And Professionals?

No cybersecurity team is complete without digital forensics. Digital forensics and investigations are critical to successfully handling a cyber incident when it occurs.

A breach can be brutal; investing in building an expert in-house forensics team with C|HFI training is a strategic move for enterprises looking to safeguard their stakeholder's interests as well as theirs. The C|HFI empowers the existing team by applying the latest investigation practices.

The C|HFI Boosts Investigative Forensics Skills and Builds Organization Forensic Readiness

- Successful Security Operations With Proof
- Minimized Cost Of Cyber Investigations
- Faster Detection And Mitigation Of Attack Vectors
- Regulatory Compliance and Reduced Regulatory Costs
- Reduced Insurance Premiums

Demand for Digital Forensics Professionals

The U.S. Bureau of Labor Statistics projects that the employment of forensic science technicians is projected to grow 13% from 2022 to 2032, much faster than the average for all occupations.

What is the Computer Hacking Forensic Investigator (C|HFI) Program?

EC-Council's C|HFI program prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. This includes establishing the forensics process, lab and evidence handling procedures, as well as the investigation procedures required to validate/triage incidents and point the incident response teams in the right direction. Forensic readiness is crucial as it can differentiate between a minor incident and a major cyber-attack that brings a company to its knees.

This intense hands-on digital forensics program immerses students in over 68 forensic labs, enabling them to work on crafted evidence files and utilize the tools employed by the world's top digital forensics professionals. Students will go beyond traditional hardware and memory forensics and learn current topics such as cloud forensics, mobile and IoT, investigating web application attacks, and malware forensics. The C|HFI presents a methodological approach to computer forensics, including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence.

Students learn how to acquire and manage evidence through various operating environments, as well as the chain of custody and legal procedures required to preserve evidence and ensure it is admissible in court. This knowledge will help them prosecute cybercriminals and limit liability for target organizations.

The program provides credible professional knowledge with a globally recognized certification required for successful digital forensics and DFIR careers, thus increasing your employability.

C|HFI Course Modules:

01 Computer Forensics in Today's World

02 Computer Forensics Investigation Process

03 Understanding Hard Disks and File Systems

04 Data Acquisition and Duplication

05 Defeating Anti-Forensics Techniques

06 Windows Forensics

07 Linux and Mac Forensics

08 Network Forensics

09 Malware Forensics

10 Investigating Web Attacks

11 Dark Web Forensics

12 Cloud Forensics

13 Email and Social Media Forensics

14 Mobile Forensics

15 IoT Forensics

What Will You Learn?

01 Computer forensics fundamentals, different types of cybercrimes and their investigation procedures, and regulations and standards that influence computer forensics investigation

02 Various phases involved in the computer forensics investigation process

03 Different types of disk drives and their characteristics, booting process and file systems in Windows, Linux, and Mac operating systems, file system examination tools, RAID and NAS/SAN storage systems, various encoding standards, and file format analysis

04 Data acquisition fundamentals and methodology, eDiscovery, and how to prepare image files for forensics examination

05 Various anti-forensics techniques used by attackers, different ways to detect them and related tools, and countermeasures

06 Volatile and non-volatile data acquisition in Windows-based operating systems, Windows memory and registry analysis, electron application analysis, web browser forensics, and examination of Windows files, ShellBags, LNK files, jump lists, and Windows event logs

07 Volatile and non-volatile data acquisition and memory forensics in Linux and Mac operating systems

08 Network forensics fundamentals, event correlation concepts, Indicators of Compromise (IOCs) and ways to identify them from network logs, techniques and tools related to network traffic investigation, incident detection and examination, and wireless attack detection and investigation

09 Malware forensics concepts, static and dynamic malware analysis, system and network behavior analysis, and ransomware analysis

10 Web application forensics and challenges, web application threats and attacks, web application logs (IIS logs, Apache web server logs, etc.), and how to detect and investigate various web application attacks

11 Tor browser working methodology and steps involved in the Tor browser forensics process

12 Cloud computing concepts, cloud forensics and challenges, fundamentals of AWS, Microsoft Azure, and Google Cloud and their investigation processes

13 Components in email communication, steps involved in email crime investigation, and social media forensics

14 Architectural layers and boot processes of Android and iOS devices, mobile forensics process, various cellular networks, SIM file system, and logical and physical acquisition of Android and iOS devices

15 Different types of IoT threats, security problems, vulnerabilities and attack surfaces areas, and IoT forensics processes and challenges

Key Features and Critical Components of the C|HFI Program

Master a methodological forensics framework approach

for performing digital forensics investigation

- Documenting the Crime Scene
- Search and Seizure
- Evidence Preservation
- Data Acquisition
- Data Acquisition
- Data Examination
- Reporting

15 modules
covering core domains of digital forensics

2100+
pages of the comprehensive student manual

1550+
pages of lab manual covering detailed lab scenarios and instructions

68
hands-on labs

600+
digital forensics tools

100%
compliance with **NICE Special Publication 800-181** cybersecurity workforce framework

70+ GB
of crafted evidence files for investigation purposes

40%
of training time dedicated to labs

Approved by the
US Department of Defense (DoD)
under Directive 8570/8140

Accredited by the
ANAB ISO/IEC 17024
National Accreditation Board

Covers relevant knowledge bases and skills to meet regulatory compliance standards such as **ISO 27001, PCI DSS, SOX, HIPPA,** etc.

Key Benefits of the C|HFI Program

1 Master a methodological forensics framework approach for performing digital forensics investigation:

1. Documenting the Crime Scene 2. Search and Seizure

3. Evidence Preservation 4. Data Acquisition 5. Data Examination 6. Reporting

The C|HFI training program teaches evidence collection, analysis, and preservation of digital evidence. Learners are guided through a step-by-step process that adheres to industry best practices. This structured methodology enhances the efficiency and effectiveness of digital investigations and ensures the integrity and admissibility of the collected evidence.

2 Build skills for investigating diverse types of digital forensic investigations:

Students in this training program delve into the intricacies of digital evidence examination, analysis, and preservation across various contexts. The curriculum emphasizes hands-on experience, allowing learners to navigate real-world situations commonly encountered in computer forensics. C|HFI training empowers individuals to become adept and capable of addressing the evolving challenges of the cybersecurity landscape.

3 70+ GB of crafted evidence files for investigation purposes:

The C|HFI training goes above and beyond by providing participants with an invaluable resource – more than 70 GB of meticulously crafted evidence files tailored for investigation purposes. This extensive collection serves as a practical and hands-on supplement to the theoretical aspects of the training. Learners can immerse themselves in a diverse range of simulated scenarios, each designed to replicate real-world digital forensics challenges.

4 Gain in-depth knowledge in volatile and non-volatile data acquisition and examination of Mac operating systems and also RAM forensics, Tor forensics, etc.:

Including volatile and non-volatile data acquisition and examining the Mac Operating System in the C|HFI course is paramount. It enhances the comprehensiveness of the training, preparing individuals to navigate the complexities of Mac-based digital forensics scenarios with precision and expertise, thereby expanding their capabilities in the evolving landscape of computer forensics.

5 Become proficient in malware forensics process and malware analysis, including the latest analysis: BlackCat (ALPHV):

This focused training ensures that students develop expertise in unraveling the complexities of malware, including the latest variants like BlackCat. By delving into the intricacies of malware forensics, learners are equipped with the skills to detect, analyze, and respond to evolving cyber threats, enhancing their proficiency in safeguarding digital environments against malicious activities.

6 Learn social media forensics and wireless network forensics:

By focusing on social media forensics, the course enhances professionals' capabilities to uncover relevant information, detect cyber threats, and conduct thorough digital investigations in the context of social media interactions. This specialized training ensures that participants gain expertise in analyzing wireless network traffic, identifying security vulnerabilities, and conducting forensic examinations in wireless environments.

7 Learn electron application and web browser forensics:

By focusing on electron application forensics, the course prepares professionals to navigate the complexities of these modern applications, enhancing their ability to uncover digital evidence, analyze potential security risks, and contribute effectively to digital forensic investigations in the evolving realm of software development.

By focusing on web browser forensics, the course equips professionals with the knowledge to trace online behaviors, detect potential threats, and conduct thorough digital investigations, contributing to a comprehensive skill set in computer forensics.

8 Gain in-depth skills in mobile forensics analysis:

With the ubiquity of mobile devices, understanding the nuances of forensic investigation specific to smartphones is crucial. This specialized training ensures that participants acquire the skills to extract and analyze digital evidence from mobile devices comprehensively.

9 Learn how to perform digital forensics investigation through Python scripting:

The C|HFI training ensures that participants understand the theoretical aspects of digital forensics and gain practical skills in automating and enhancing investigative processes using Python scripts. By incorporating this focus, the course equips professionals to streamline tasks, analyze data more effectively, and adapt to the evolving demands of digital investigations, highlighting the significance of coding skills in computer forensics.

10 Master a unique skill set with C|HFI - the first certification to offer dark web & IoT forensics:

In dark web forensics, C|HFI students will learn to acquire the suspect machine's memory dumps and local storage image files, examine memory dumps and local storage image files for illegal activities taking place using emails, and retrieve accessed emails and email attachments.
In IoT forensics, students will learn to perform logical and physical acquisition on Android wear and retrieve potential evidence. Perform client-based and cloud-based analysis on Amazon Alexa devices to discover artifacts stored on the device.

11 Become skilled in forensic methodologies for cloud infrastructure (AWS, Azure and GCP):

The C|HFI training ensures that participants gain proficiency in navigating the complexities of major cloud platforms (AWS, Azure, and GCP), allowing them to conduct thorough digital forensic examinations in cloud-based scenarios. The inclusion of cloud-specific methodologies broadens the skill set of digital forensic professionals.

12 Learn techniques such as defeating anti-forensic techniques, Windows ShellBags, etc.:

In learning techniques such as defeating anti-forensic methods, Windows ShellBags, analyzing LNK files, and jump lists, you acquire advanced skills in digital forensics. This includes understanding methods to counter attempt, conceal, or manipulate digital evidence, exploring the intricacies of Windows file system artifacts like ShellBags and LNK files, and utilizing jump lists for detailed timeline analysis, enhancing your proficiency in forensic investigations.

13 Learn the latest digital forensics tools/platforms and frameworks:

The C|HFI course includes a library of tools, platforms, and frameworks across different operating platforms required by security professionals/computer forensic analysts to perform an effective organizational digital forensics investigation. This gives students a wider range of options than any other program on the market.

14 40% of training time is dedicated to lab training that simulates real-life networks and platforms:

The theory-to-practice ratio in the C|HFI program is 60:40, providing students with real-time experience and hands-on practice with the latest digital forensic tools, techniques, methodologies, scripts, and frameworks. The C|HFI is integrated with labs to emphasize the learning objectives. The lab environment simulates a real-time situation for computer forensic analysts, and this experience can help in effectively identifying and mitigating various business risks by successfully carrying out a computer forensic investigation, leading to the prosecution of perpetrators.

15 The C|HFI is designed by SMEs and digital forensics practitioners worldwide after a rigorous JTA of the job roles involved in the field of digital forensics, increasing your employability:

The C|HFI was developed by top-notch digital forensics practitioners and experts in the domain through rigorous industry-wide JTA. It was developed after intensive analysis of all possible combinations of Task, Knowledge, Skill, and Ability (TKSA) from relevant job postings of various multinational companies. This comprehensive mapping/analysis synchronizes the C|HFI program to industry-wide computer forensic analyst job requirement criteria, thus increasing your employability.

Training and Exam Details

Training Details:

iLearn (Self-Study)

This solution is an asynchronous, self-study environment in a video streaming format.

Week (Live Online)

This solution is a live, online, instructor-led training format.

Training Partner (In Person)

This solution offers "in-person" training so that you can benefit from collaborating with your peers and gaining real-world led by expert, certified instructors.

Exam Title:

Computer Hacking Forensic Investigator

Exam Code:	Number of Questions:	Duration:	Availability:
312-49	150	4 hours	ECC EXAM Portal

Who Can Apply?

Recommended Prerequisites for the C|HFI:
IT/Forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, incident response, and threat vectors.

Salaries

As per the Salary Survey 75 Report, EC-Council's C|HFI is the only Digital Forensics certification with a six-digit salary of up to **$117,950.**

Recognition/Endorsement/Mapping

U.S. Department of Defense

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17024
PERSONNEL CERTIFICATION BODY

NICE

Why Do Top DFIR & Digital Forensics Professionals Across the Globe Prefer the the C|HFI Program?

The **C|HFI** certification gives a comprehensive overview of the process that a forensic investigator must follow when investigating a cybercrime. It includes the right treatment of the digital evidence to be accepted in the courts and useful tools and techniques that can be applied to investigate an incident.

Virginia Aguilar,
Google, EX-KPMG
Madrid

Grace Pittmon

Navitus Health Solutions

IT Security Manager

The C|HFI provides a very streamlined and step-by-step forensics methodology from a very agnostic perspective. Yet, it still covers some key environments and platforms in detail, such as cloud environments, mobile devices, databases, and network devices. The program is very detailed in its coverage and explanation of the forensics tool. But at the same time, it's also very simplified, so anyone new to forensics can benefit from it. Also, the lab format was easy to comprehend and follow for those new to cybersecurity. The C|HFI program is very organized in its approach and presentation, making it easier for me to retain information long after completing the course. For those looking to advance their careers in cybersecurity, it's a good set of skills to showcase the value you will provide to an employer regardless of the career path you're pursuing. Whether you're interested in the strategic side of the house, meaning executive roles, or whether you want to move to or advance in the tactical or operational side of cybersecurity, C|HFI can be the best one for you!

Brad W. Beatty

Cyber Security Analyst

Booz Allen Hamilton

USA

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

Organizations That Employ C|HFI Certified Members

Sources:

1. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
3. https://www.ibm.com/reports/data-breach

About EC-Council

EC-Council invented the Certified Ethical Hacker (C|EH) Program. Founded in 2001 in response to 9/11, the EC-Council's mission is to provide the training and certifications that apprentice and experienced cybersecurity professionals need to keep corporations, government agencies, and others who employ them safe from cyber-attacks.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different training programs, certifications, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified over 350,000 professionals across the globe. EC-Council is the gold standard in cybersecurity education and certification, trusted by seven of the Fortune 10, half of the Fortune 100, and various agencies, public and private, across 140 nations.

A truly global organization with a driving belief in bringing diversity, equity, and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the US, the UK, India, Malaysia, Singapore, and Indonesia.

For more details, visit: www.eccouncil.org

EC-Council

Building A Culture Of Security