



ERIC REED

CYBERSECURITY TRAINING

PASS ON THE FIRST ATTEMPT!™



COMPANY OVERVIEW

For over 25 years, Eric Reed Cybersecurity Training has been a trusted leader in cybersecurity education, equipping more than 60,000 professionals with the skills needed to defend against emerging cyber threats. Our mission is to empower individuals and organizations with comprehensive, hands-on training that translates directly to real-world success. Recognized with multiple industry awards—including an unprecedented 10-time EC Council Instructor of the Year and 7-time Circle of Excellence honoree—we combine innovative delivery methods with a passion for excellence to ensure our students achieve certification success on the first attempt



EC-COUNCIL C|HFI V11

The Computer Hacking Forensic Investigator (C|HFI) certification focuses on digital forensic investigation, helping professionals detect, analyze, and report cybercrimes.



ONLINE LIVE LEARNING



ON-DEMAND LIVE LEARNING

ONLINE LIVE & ON-DEMAND LIVE

All the benefits of live, instructor-led training with the convenience of on-demand.

- **Online Live:** Attend our scheduled sessions in real time (Monday–Friday). Get immediate interaction with the instructor and fellow students.
- **On-Demand Live:** Access recordings of the most recent live sessions on your own schedule, while still having direct instructor support.
- **Flexible Scheduling:** Choose a structured approach—one-week bootcamp (M–F), two nights a week for five weeks, or every Saturday for five weeks. Need more wiggle room? Adjust any schedule to fit your lifestyle!



COURSE OBJECTIVES

- Conduct forensic investigations on compromised systems.
- Recover, analyze, and preserve digital evidence.
- Apply forensic techniques to detect unauthorized access.
- Use forensic tools to analyze network traffic and logs.
- Ensure legal compliance and evidence documentation.



SALARY RANGE

C|HFI → \$95,000 - \$140,000

These figures are approximate and depend on location, experience, and job role. Higher salaries are usually seen in major tech hubs and with significant experience.



JOB ROLES

- **Forensic Analyst**
- **Incident Responder**



"It's was a great class that covered all aspects of security. Most importantly, I appreciate the fact that you are giving up your own time to assist us and maintain a sharedrive with the latest security tools and informative papers even after the class is over. I was able to pass the test after one week of attending the training."

-Shadi Ehalabi

Contact Us

- 📞 (707) 722-7333
- ✉ info@ericreedlive.com
- 📍 1401 61st St S
Gulfport, FL 33707



WWW.LINKEDIN.COM/IN/ERICREEDLIVE/



EC-COUNCIL C|HFI OVERVIEW

1 - Computer Forensics in Today's World

- Understand the Fundamentals of Computer Forensics
- Understand Cybercrimes and their Investigation Procedures
- Understand Digital Evidence
- Understand Forensic Readiness, Incident Response and the Role of SOC (Security Operations Center) in Computer Forensics
- Identify the Roles and Responsibilities of a Forensic Investigator
- Understand the Challenges Faced in Investigating Cybercrimes
- Understand Legal Compliance in Computer Forensics



2 - Computer Forensics Investigation Process

- Understand the Forensic Investigation Process and its Importance
- Understand the Pre-investigation Phase
- Understand First Response
- Understand the Investigation Phase
- Understand the Post-investigation Phase



3 - Understanding Hard Disks and File Systems

- Describe Different Types of Disk Drives and their Characteristics
- Explain the Logical Structure of a Disk
- Understand Booting Process of Windows, Linux and Mac Operating Systems
- Understand Various File Systems of Windows, Linux and Mac Operating Systems
- Examine File System Using Autopsy and The Sleuth Kit Tools
- Understand Storage Systems
- Understand Encoding Standards and Hex Editors
- Analyze Popular File Formats Using Hex Editor



4 - Data Acquisition and Duplication

- Understand Data Acquisition Fundamentals
- Understand Data Acquisition Methodology
- Prepare an Image File for Examination



5 - Defeating Anti-forensics Techniques

Understand Anti-forensics Techniques

Discuss Data Deletion and Recycle Bin Forensics

Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions

Explore Password Cracking/Bypassing Techniques

Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch

Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption

Detect Program Packers and Footprint Minimizing Techniques

Understand Anti-forensics Countermeasures



6 - Windows Forensics

Collect Volatile and Non-volatile Information

Perform Windows Memory and Registry Analysis

Examine the Cache, Cookie and History Recorded in Web Browsers

Examine Windows Files and Metadata

Understand ShellBags, LNK Files, and Jump Lists

Understand Text-based Logs and Windows Event Logs

7 - Linux and Mac Forensics

Understand Volatile and Non-volatile Data in Linux

Analyze Filesystem Images Using The Sleuth Kit

Demonstrate Memory Forensics Using Volatility & PhotoRec

Understand Mac Forensics



8 - Network Forensics

Understand Network Forensics

Explain Logging Fundamentals and Network Forensic Readiness

Summarize Event Correlation Concepts

Identify Indicators of Compromise (IoCs) from Network Logs

Investigate Network Traffic

Perform Incident Detection and Examination with SIEM Tools

Monitor and Detect Wireless Network Attacks



9 - Malware Forensics

Define Malware and Identify the Common Techniques Attackers Use to Spread Malware
Understand Malware Forensics Fundamentals and Recognize Types of Malware Analysis
Understand and Perform Static Analysis of Malware
Analyze Suspicious Word and PDF Documents
Understand Dynamic Malware Analysis Fundamentals and Approaches
Analyze Malware Behavior on System Properties in Real-time
Analyze Malware Behavior on Network in Real-time
Describe Fileless Malware Attacks and How they Happen
Perform Fileless Malware Analysis - Emotet



10 - Investigating Web Attacks

Understand Web Application Forensics
Understand Internet Information Services (IIS) Logs
Understand Apache Web Server Logs
Understand the Functionality of Intrusion Detection System (IDS)
Understand the Functionality of Web Application Firewall (WAF)
Investigate Web Attacks on Windows-based Servers
Detect and Investigate Various Attacks on Web Applications



11 - Dark Web Forensics

Understand the Dark Web
Determine How to Identify the Traces of Tor Browser during Investigation
Perform Tor Browser Forensics



12 - Cloud Forensics

Understand the Basic Cloud Computing Concepts
Understand Cloud Forensics
Understand the Fundamentals of Amazon Web Services (AWS)
Determine How to Investigate Security Incidents in AWS
Understand the Fundamentals of Microsoft Azure
Determine How to Investigate Security Incidents in Azure
Understand Forensic Methodologies for Containers and Microservices



13 - Investigating Email Crimes

Understand Email Basics
Understand Email Crime Investigation and its Steps
U.S. Laws Against Email Crime



14 - Mobile Forensics

- Understand the Importance of Mobile Device Forensics
- Illustrate Architectural Layers and Boot Processes of Android and iOS Devices
- Explain the Steps Involved in Mobile Forensics Process
- Investigate Cellular Network Data
- Understand SIM File System and its Data Acquisition Method
- Illustrate Phone Locks and Discuss Rooting of Android and Jailbreaking of iOS Devices
- Perform Logical Acquisition on Android and iOS Devices
- Perform Physical Acquisition on Android and iOS Devices
- Discuss Mobile Forensics Challenges and Prepare Investigation Report



15 - IoT Forensics

- Understand IoT and IoT Security Problems
- Recognize Different Types of IoT Threats
- Understand IoT Forensics
- Perform Forensics on IoT Devices