Training: EC-Council
# CHFI - Computer Hacking Forensic Investigator

EC-Council Building A Culture Of Security

## TRAINING GOALS:

C|HFI Computer Hacking Forensic INVESTIGATOR

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. Establishing the forensics process, lab, evidence handling procedures, and investigation techniques are 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, working on crafted evidence files utilizing the tools of the world's top digital forensics professionals. Students will go beyond traditional hardware and memory forensics, covering current topics in cloud forensics, mobile and IoT, and 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 various forensic investigation techniques and standard forensic tools. As they learn how to acquire and manage evidence through various operating environments, students also learn the chain of custody and legal procedures required to preserve evidence and ensure it is admissible in court, enabling the eventual prosecution of cyber criminals and containing liability on the victim organization.

The program provides credible professional knowledge with globally recognized certification required



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

for a successful digital forensics and DFIR career, thus increasing your employability.

What will you learn?

- Computer forensics fundamentals, different types of cybercrimes and their investigation procedures, and regulations and standards that influence computer forensics investigation
- Various phases involved in the computer forensics investigation process
- 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
- Data acquisition fundamentals and methodology, eDiscovery, and how to prepare image files for forensics examination
- Various anti-forensics techniques used by attackers, different ways to detect them and related tools, and countermeasures
- 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, and Jump Lists, and Windows event logs
- Volatile and non-volatile data acquisition and memory forensics in Linux and Mac operating systems
- 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
- Malware forensics concepts, static and dynamic malware analysis, system and network behavior analysis, and ransomware analysis
- 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
- Tor browser working methodology and steps involved in the Tor browser forensics process
- Cloud computing concepts, cloud forensics, and challenges, fundamentals of AWS, Microsoft Azure, and Google Cloud and their investigation processes
- Components in email communication, steps involved in email crime investigation, and social media forensics
- 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
- Different types of IoT threats, security problems, vulnerabilities and attack surfaces areas, and IoT forensics process and challenges

Who CHFI is for:



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Cybersecurity Professionals (Forensic Analysts & Incident Responders)
- Law Enforcement Personnel & Private Investigators
- IT Managers & System Administrators
- Legal Professionals & Compliance Officers
- Military & Government Intelligence Officers

*Each participant in an authorized training CHFI - Computer Hacking Forensic Investigator held in Compendium CE will receive a free CHFI certification exam voucher.*

## CONSPECT:

- Module 1 - Computer Forensics in Today’s World
  - Understand the Fundamentals of Computer Forensics
    - Understanding Computer Forensics
    - Scope of Computer Forensics
  - Understand Cybercrimes and their Investigation Procedures
    - Types of Cybercrimes
    - Impact of Cybercrimes at the Organizational Level
    - Cyber Attribution
    - Cybercrime Investigation
  - Understand Digital Evidence and eDiscovery
    - Introduction to Digital Evidence
    - Types of Digital Evidence
    - Roles of Digital Evidence
    - Sources of Potential Evidence
    - Rules of Evidence
    - Best Evidence Rule
    - Federal Rules of Evidence (United States)
    - The Association of Chief Police Officers (ACPO) (inherited into NPCC) Principles of Digital Evidence
    - Computer Forensics vs. eDiscovery
    - Legal and IT Team Considerations for eDiscovery
    - Best Practices for Handling Digital Evidence



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Understand Forensic Readiness
  - Forensic Readiness
  - Forensic Readiness and Business Continuity
  - Forensics Readiness Planning
  - Forensic Readiness Procedures
- Understand the Role of Various Processes and Technologies in Computer Forensics
  - Computer Forensics as a part of Incident Response Plan
  - Role of Computer Forensics in SOC Operations
  - Role of Threat Intelligence in Computer Forensics
  - Role of Artificial Intelligence in Computer Forensics
  - Forensics Automation and Orchestration
- Identify the Roles and Responsibilities of a Forensic Investigator
  - Need for a Forensic Investigator
  - Roles and Responsibilities of a Forensics Investigator
  - What Makes a Good Computer Forensics Investigator?
  - Code of Ethics
  - Managing Clients or Employers during Investigations
  - Accessing Computer Forensics Resources
- Understand the Challenges Faced in Investigating Cybercrimes
  - Challenges Cybercrimes Pose to Investigators
  - Other Factors that Influence Forensic Investigations
  - Computer Forensics: Legal Issues
  - Computer Forensics: Privacy Issues
- Understand Various Standards and Best Practices Related to Computer Forensics
  - ISO Standards
  - ENFSI Best Practices for Forensic Examination of Digital Technology
- Understand Laws and Legal Compliance in Computer Forensics
  - Role of Local/International Agencies during Cybercrime Investigation
  - Computer Forensics and Legal Compliance
  - Other Laws Relevant to Computer Forensics

- Module 2 - Computer Forensics Investigation Process
  - Understand the Forensic Investigation Process and its Importance
    - Importance of Computer Forensic Investigation Process
    - Phases Involved in the Computer Forensics Investigation Process
  - Understand First Response
    - First Response



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- First Responder
- Roles of First Responder
- First Response Basics
- First Response: Different Situations
- First Responder Common Mistakes
- Health and Safety Issues

- Understand the Pre-investigation Phase
  - Setting Up a Computer Forensics Lab
  - Building the Investigation Team
  - Understanding Hardware and Software Requirements of Forensics Lab
  - Validating Laboratory Software and Hardware
  - Ensuring Quality Assurance
  - Building Security Content, Scripts, Tools, or Methods to Enhance Forensic Processes
- Understand the Investigation Phase
  - Documenting the Electronic Crime Scene
  - Search and Seizure
  - Evidence Preservation
  - Data Acquisition
  - Data Analysis
  - Case Analysis
- Understand the Post-investigation Phase
  - Reporting
  - Testifying as an Expert Witness

- Module 3 - Understanding Hard Disks and File Systems
  - Describe Different Types of Disk Drives and their Characteristics
    - Understanding Hard Disk Drive
    - Understanding Solid-State Drive (SSD)
    - Disk Interfaces
  - Explain the Logical Structure of a Disk
    - Logical Structure of Disks
  - Understand the Booting Process of Windows, Linux, and macOS Operating Systems
    - What is the Booting Process?
    - Essential Windows System Files and Components
    - Windows Boot Process: BIOS-MBR Method
    - Windows Boot Process: UEFI-GPT
    - macOS Boot Process



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Linux Boot Process
- Windows File Systems
- Linux File Systems
- macOS File Systems

- Understand File System Analysis
  - File System Analysis Using Autopsy
  - File System Analysis Using The Sleuth Kit (TSK)
  - File System Timeline Creation and Analysis Using The Sleuth Kit (TSK)
  - NTFS Timestamp Rules in Windows and Linux
- Understand Storage Systems
  - RAID Storage System
  - Network-Attached Storage (NAS)
  - Storage Area Network (SAN)
  - Differences between NAS and SAN
- Understand Encoding Standards and Hex Editors
  - Character Encoding Standards
  - OFFSET
  - Understanding Hex Editors
  - Understanding Hexadecimal Notation
- Analyze Popular File Formats Using Hex Editor
  - Image File Analysis: JPEG
  - Image File Analysis: BMP
  - Hex View of Popular Image File Formats
  - PDF File Analysis
  - Word File Analysis
  - PowerPoint File Analysis
  - Excel File Analysis
  - Hex View of Other Popular File Formats
  - Hex View of Popular Video File Formats
  - Hex View of Popular Audio File Formats

- Module 4 - Data Acquisition and Duplication
  - Understand Data Acquisition Fundamentals
    - Understanding Data Acquisition
    - Live Acquisition
    - Order of Volatility
    - Dead Acquisition



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Rules of Thumb for Data Acquisition
- Types of Data Acquisition
- Determine Data Acquisition Format

- Understand eDiscovery
  - eDiscovery
  - Electronic Discovery Reference Model (EDRM) Cycle
  - Monitor and Maintain Accurate Metrics and Detailed Tracking Information Related to eDiscovery
  - eDiscovery Collection Methodologies
  - Best Practices for eDiscovery
  - eDiscovery Tools
- Understand Data Acquisition Methodology
  - Data Acquisition Methodology
  - Step 1: Determine the Best Data Acquisition Method
  - Step 2: Select Data Acquisition Tool
  - Step 3: Sanitize Target Media
  - Step 4: Acquire Volatile Data
  - Step 5: Enable Write Protection on the Evidence Media
  - Step 6: Acquire Non-volatile Data
  - Step 7: Plan for Contingency
  - Step 8: Validate Data Acquisition Using
  - Data Acquisition Guidelines and Best Practices
- Prepare an Image File for Examination
  - Preparing an Image for Examination
  - Scenario 1: Examining Images on Linux Forensic Workstation
  - Scenario 2: Examining Images on Windows Forensic Workstation
  - Scenario 3: Examining Images on Mac Forensic Workstation
  - Digital Forensic Imaging Tools

- Module 5 - Defeating Anti-forensics Techniques
  - Understand Anti-forensics Techniques
    - What is Anti-forensics?
    - Challenges to Forensics from Anti-forensics
  - Discuss Data Deletion and Recycle Bin Forensics
    - Anti-forensics Technique: Data/File Deletion
    - What Happens When a File is Deleted in Windows?
    - Recycle Bin in Windows



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions
  - File Carving
  - Recovering Deleted Partitions
- Explore Password Cracking/Bypassing Techniques
  - Anti-forensics Technique: Password Protection
  - Tools to Extract the Password Hashes
  - Password Cracking Tools
  - Bypassing Passwords on Powered-off Computer
  - Tool to Reset Admin and Local User Password: PassFab 4WinKey
  - Bypassing Windows User Password by Booting Live USB
  - Application Password Cracking Tools
- Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch
  - Anti-forensics Technique: Steganography
  - Defeating Anti-forensics Technique: Detecting Data Hiding in File System Structures
  - Anti-forensics Technique: Alternate Data Streams
  - Anti-forensics Technique: Trail Obfuscation
  - Defeating Anti-forensics Technique: Detecting File Extension Mismatch Using Autopsy
- Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption
  - Anti-forensics Technique: Artifact Wiping
  - Anti-forensics Technique: Overwriting Data/Metadata
  - Anti-forensics Technique: Encryption
- Detect Program Packers and Footprint Minimizing Techniques
  - Anti-forensics Technique: Program Packers
  - Anti-forensics Techniques that Minimize Footprint
  - Anti-forensics Countermeasures

- Module 6 - Windows Forensics
  - Understand Windows Forensics
    - Introduction to Windows Forensics
    - Windows Forensics Methodology
  - Collect Volatile Information
    - Collecting Volatile Information
  - Collect Non-volatile Information
    - Collecting Non-volatile Information



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Perform Windows Memory Analysis
  - Windows Memory Analysis
  - Windows Crash Dump
  - Collecting Process Memory
  - Memory Forensics
- Perform Windows Registry Analysis
  - Windows Registry Analysis
  - Windows Registry Analysis Using Magnet AXIOM
- Perform Electron Application Analysis
  - Electron Application Forensics
  - Extracting Data from Microsoft Teams
  - Extracting Data from WhatsApp
  - Extracting Data from Skype
- Perform Web Browser Forensics
  - Web Browser Forensics
  - Cache, Cookie, and History Analysis: Mozilla Firefox
  - Cache, Cookie, and History Analysis: Google Chrome
  - Cache, Cookie, and History Analysis: Microsoft Edge
  - Recovering Private Browsing Data and Browser Artifacts
  - Carving SQLite Database Files Using FTK® Imager
- Examine Windows Files and Metadata
  - Windows File Analysis
  - Metadata Investigation
- Understand ShellBags, LNK Files, and Jump Lists
  - Windows ShellBags
  - Analyzing LNK Files
  - Analyzing Jump Lists
- Understand Text-based Logs and Windows Event Logs
  - Understanding Events
  - Types of Logon Events
  - Event Log File Format
  - Organization of Event Records
  - ELF_LOGFILE_HEADER Structure
  - EventLogRecord Structure
  - Windows 11 Event Logs
  - Evaluating Account Management Events



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Event Logs
- Windows Forensics Tools
- Hashing it Out in PowerShell: Using Get-FileHash

- Module 7 - Linux and Mac Forensics
  - Collect Volatile Information in Linux
    - Introduction to Linux Forensics
    - Collecting Volatile Information
  - Collect Non-volatile Information in Linux
    - Collecting Non-volatile Information
  - Understand Linux Memory Forensics
    - Linux Memory Forensics
  - Understand Mac Forensics
    - Introduction to Mac Forensics
    - Mac Forensics Data
    - Mac Log Files
    - Mac Directories
  - Collect Volatile Information in Mac
    - Collecting Volatile Information
  - Collect Non-volatile Information in Mac
    - Collecting Non-volatile Information
  - Understand Mac Memory Forensics and Mac Forensics Tools
    - Mac Memory Forensics
    - APFS Analysis
    - Parsing Metadata on Spotlight
    - Mac Forensics Tools
- Module 8 - Network Forensics
  - Understand Network Forensics
    - Introduction to Network Forensics
    - Postmortem and Real-Time Analysis
    - Network Attacks
    - Indicators of Compromise (IoCs)
    - Where to Look for Evidence
    - Types of Network-based Evidence
  - Summarize Event Correlation Concepts
    - Event Correlation
    - Types of Event Correlation



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

- Prerequisites of Event Correlation
- Event Correlation Approaches

- Identify Indicators of Compromise (IoCs) from Network Logs
  - Log Files as Evidence
  - Analyzing Firewall Logs
  - Analyzing IDS Logs
  - Analyzing Honeypot Logs
  - Analyzing Router Logs
  - Analyzing DHCP Logs
  - Analyzing Cisco Switch Logs
  - Analyzing VPN Logs
  - Analyzing SSH Logs
  - Analyzing DNS Server Logs
  - Network Log Analysis Tools
- Investigate Network Traffic
  - Why Investigate Network Traffic?
  - Gathering Evidence via Sniffers
  - Sniffing Tools
  - Analyze Traffic for TCP SYN Flood DoS Attack
  - Analyze Traffic for SYN-FIN Flood DoS Attack
  - Analyze Traffic for ICMP Flood Attack
  - Analyze Traffic for UDP Flood Attack
  - Analyze Traffic for HTTP Flood Attack
  - Analyze Traffic for FTP Password Cracking Attempts
  - Analyze Traffic for SMB Password Cracking Attempts
  - Analyze Traffic for Sniffing Attempts
  - Analyze Traffic for SMTP HELO Flood Attack
  - Analyze Traffic to Detect Malware Activity
  - Analyze Network Traffic through NetFlow
  - Network Forensic Analysis Using Dshell
  - Tools for Investigating Network Traffic
- Perform Incident Detection and Examination Using SIEM Tools
  - Centralized Logging Using SIEM Solutions
  - SIEM Solutions
  - Examine Brute-force Attack
  - Examine DoS Attack



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Examine Malware Activity
- Examine Data Exfiltration Attempts over FTP
- Examine Network Scanning Attempts
- Examine Ransomware Attack
- Detect Rogue DNS Server (DNS Hijacking/DNS Spoofing)

- Understand Wireless Network Forensics
  - Introduction to Wireless Network Forensics
  - Wireless Network Forensics Challenges and Risks
  - Types of Wireless Evidence
  - Wireless Network Forensics Process
- Detect and Investigate Wireless Network Attacks
  - Detect Rogue Access Points
  - Detect Access Point MAC Address Spoofing Attempts
  - Detect Misconfigured Access Points
  - Detect Wi-Fi Jamming Attempts Using Wireshark
  - Analyze Wireless Packet Captures
  - Analyze Wi-Fi Spectrum
  - Analyze the Wireless Network Report
  - Tools for Investigating Wireless Network Traffic

- Module 9 - Malware Forensics
  - Understand Malware Concepts
    - Introduction to Malware
    - Different Ways for Malware to Enter a System
    - Common Techniques Attackers Use to Distribute Malware across Web
    - Components of Malware
  - Understand Malware Forensics
    - Introduction to Malware Forensics
    - Why Analyze Malware?
    - Malware Analysis Challenges
    - Malware Forensic Artifacts
    - Indicators of Malware
    - Prominence of Setting Up a Controlled Malware Analysis Lab
    - Preparing Testbed for Malware Analysis
    - Malware Analysis Tools
    - Documentation Before Analysis
    - Types of Malware Analysis



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Perform Static Malware Analysis
  - Static Malware Analysis: File Fingerprinting
  - Static Malware Analysis: Local and Online Malware Scanning
  - Static Malware Analysis: Performing Strings Search
  - Static Malware Analysis: Identifying Packing/Obfuscation Methods
  - Static Malware Analysis: Finding the Portable Executables (PE) Information
  - Static Malware Analysis: Identifying File Dependencies
  - Static Malware Analysis: Malware Disassembly
  - Static Malware Analysis: Analyzing ELF Executable Files
  - Static Malware Analysis: Analyzing Mach-O Executable Files
- Analyzing Suspicious Documents
  - Analyzing Suspicious MS Office Document
  - Analyzing Suspicious MS Excel Document
  - Analyzing Suspicious PDF Document
- Perform System Behavior Analysis
  - System Behavior Analysis: Monitoring Registry Artifacts
  - System Behavior Analysis: Monitoring Processes
  - System Behavior Analysis: Monitoring Windows Services
  - System Behavior Analysis: Monitoring Startup Programs
  - System Behavior Analysis: Monitoring Windows Event Logs
  - System Behavior Analysis: Monitoring API Calls
  - System Behavior Analysis: Monitoring Device Drivers
  - System Behavior Analysis: Monitoring Installation
  - System Behavior Analysis: Monitoring System Calls
  - System Behavior Analysis: Monitoring Scheduled Tasks
  - System Behavior Analysis: Monitoring Files and Folders
- Perform Network Behavior Analysis
  - Network Behavior Analysis: Monitoring Network Activities
  - Network Behavior Analysis: Monitoring Port
  - Network Behavior Analysis: Monitoring DNS
  - Network Behavior Analysis: Monitoring Browser Activity
- Perform Ransomware Analysis
  - Ransomware Analysis - BlackCat (ALPHV)

- Module 10 - Investigating Web Attacks
  - Understand Web Application Forensics
    - Introduction to Web Application Forensics



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Challenges in Web Application Forensics
- Indicators of a Web Attack
- OWASP Top 10 Application Security Risks - 2021
- Web Application Threats
- Web Attack Investigation Methodology

- Understand Internet Information Services (IIS) Logs
  - IIS Web Server Architecture
  - IIS Logs
  - Analyzing IIS Logs
  - Analyzing IIS HTTP Logs Using HttpLogBrowser
  - IIS Log Analysis Tools
- Understand Apache Web Server Logs
  - Apache Web Server Architecture
  - Apache Web Server Logs
  - Apache Access Logs
  - Apache Error Logs
  - Analyzing Apache Web Server Logs Using Python
  - Apache Log Analysis Tools
- Detect and Investigate Various Attacks on Web Applications
  - Investigating Cross-Site Scripting (XSS) Attack
  - Investigating SQL Injection Attack
  - Investigating Path/Directory Traversal Attack
  - Investigating Command Injection Attack
  - Investigating XML External Entity (XXE) Attack
  - Investigating Brute-force Attack

- Module 11 - Dark Web Forensics
  - Understand the Dark Web and Dark Web Forensics
    - Understanding the Dark Web
    - Tor Relays
    - Working of the Tor Browser
    - Tor Bridge Node
    - Dark Web Forensics
    - Dark Web Forensics Challenges
  - Determine How to Identify the Traces of Tor Browser during Investigation
    - Identifying Tor Browser Artifacts: Command Prompt
    - Identifying Tor Browser Artifacts: Windows Registry



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Identifying Tor Browser Artifacts: Prefetch Files
- Identifying Tor Browser Artifacts: places.sqlite File

- Perform Tor Browser Forensics
  - Tor Browser Forensics: Memory Acquisition
  - Collecting Memory Dumps
  - Memory Dump Analysis: Bulk Extractor
  - Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Open)
  - Forensic Analysis of Storage to Acquire Email Attachments (Tor Browser Open)
  - Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Closed)
  - Forensic Analysis of Storage to Acquire Email Attachments (Tor Browser Closed)
  - Forensic Analysis: Tor Browser Uninstalled

- Module 12 - Cloud Forensics
  - Understand Cloud Computing Concepts
    - Introduction to Cloud Computing
    - Types of Cloud Computing Services
    - Separation of Responsibilities in Cloud
    - OWASP Top 10 Cloud Security Risks
    - Cloud Computing Threats
    - Cloud Computing Attacks
  - Understand Cloud Forensics
    - Introduction to Cloud Forensics
    - Uses of Cloud Forensics
    - Cyber Crime on Cloud Environment
    - Cloud Forensics: Stakeholders and their Roles
    - Cloud Forensics Challenges
  - Understand Amazon Web Services (AWS) Fundamentals
    - Introduction to Amazon Web Services
    - Shared Responsibility Model for AWS
    - Data Storage in AWS
    - Logs in AWS
  - Perform AWS Forensics
    - Forensic Acquisition of Amazon EC2 Instance: Methodology
    - Collecting Information Using AWS-CLI
    - Investigating CloudWatch Logs
    - Investigating S3 Server Access Logs



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Investigating AWS CloudTrail for IAM-based Incidents
- Investigating Amazon VPC Flow Logs Using AWS Management Console
- Analyzing AWS Security Incidents Using GuardDuty

- Understand Microsoft Azure Fundamentals
  - Introduction to Microsoft Azure
  - Division of Responsibilities in Azure
  - Data Storage in Azure
  - Logs in Azure
- Perform Microsoft Azure Forensics
  - Forensic Acquisition of VMs in Azure: Methodology
  - Analyzing Azure Monitor Logs
  - Collecting and Analyzing Logs In Azure AD
  - Investigating Security Incidents using Microsoft Azure Sentinel
- Understand Google Cloud Fundamentals
  - Introduction to Google Cloud
  - Shared Responsibilities in Google Cloud
  - Data Storage in Google Cloud
  - Logs in Google Cloud
- Perform Google Cloud Forensics
  - Forensic Acquisition of Persistent Disk Volumes in GCP: Methodology
  - Analyzing Google Workspace Logs
  - Analyzing Log Data using Google Cloud Log Analytics
  - Analyzing Google Cloud VPC Flow Logs
  - Investigating Google Cloud Security Incidents
  - Investigating Google Cloud Container Security Incidents
  - Investigating Google Cloud VM-based Security Incidents

- Module 13 - Email and Social Media Forensics
  - Understand Email Basics
    - Introduction to an Email System
    - Components Involved in Email Communication
    - How Email Communication Works?
    - Understanding the Parts of an Email Message
  - Explain Email Crime Investigation and its Steps
    - Introduction to Email Crime Investigation
    - Steps to Investigate Email Crimes
  - Understand U.S. Laws Against Email Crime



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- S. Laws Against Email Crime: CAN-SPAM Act
- Explain Social Media Forensics
  - Introduction to Social Media Forensics
  - Social Media Crimes
  - Social Media Forensics Challenges
  - Manually Collecting Data from Social Media Platforms
  - Collecting Evidence from Social Media Platforms Using WebPreserver
  - Extracting Footages from Social Media Platforms
  - Tracking Social Media User Activities Using Social Searcher
  - Constructing and Analyzing Social Network Graphs
  - Social Media Forensics Tools

- Module 14: Mobile Forensics
  - Understand Mobile Device Forensics
    - Mobile Device Forensics
    - OWASP Top 10 Mobile Risks - 2016
    - Mobile Attacks
    - Mobile Hardware and Forensics
    - Mobile OS and Forensics
    - Mobile Forensics Challenges
  - Understand Android and iOS Architecture, Boot Process, and File Systems
    - Mobile Device Architecture
    - Android OS Architecture
    - Android Boot Process
    - iOS Architecture
    - iOS Boot Process
    - Android File System
    - iOS File System
  - Understand Mobile Forensics Process
    - Mobile Forensics Process
    - Android Forensics Process
    - iOS Forensics Process
  - Investigate Cellular Network Data
    - Components of Cellular Network
    - Different Cellular Networks
    - Cell Site Analysis: Analyzing Service Provider Data
    - CDR Contents



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Perform File System Acquisition
  - Subscriber Identity Module (SIM)
- Understand Phone Locks, Rooting, and Jailbreaking of Mobile Devices
  - Phone Locking on Android
  - Phone Locking on iOS
  - Rooting of Android Devices
  - Jailbreaking of iOS Devices
- Perform Logical Acquisition on Mobile Devices
  - Logical Acquisition
  - Extracting Data from Android Devices Using Magnet ACQUIRE
  - Cloud Data Acquisition on Android and iOS Devices
  - Cloud Data Acquisition: Using Commercial Tools
- Perform Physical Acquisition on Mobile Devices
  - Physical Acquisition
  - SQLite Database Extraction
  - JTAG Forensics
  - Chip-off Forensics
  - Flasher Boxes
- Perform Android and iOS Forensic Analysis
  - Static Analysis and Dynamic Analysis of Android Package Kit (APK)
  - Android Logs
  - Examining Android Logs Using Logcat
  - Android Log Analysis Tools
  - Collecting WhatsApp Artifacts from Android Devices
  - Analyzing Android Chrome Artifacts
  - Android Forensic Analysis: Using Commercial Tools
  - Extracting iOS Signal Data Using Belkasoft Evidence Center
  - Analyzing iOS Safari Artifacts
  - Decrypting and Analyzing iOS Keychains
  - iOS Forensic Analysis: Using Commercial Tools

- Module 15: IoT Forensics
  - Understand IoT Concepts
    - What is the IoT?
    - IoT Architecture
    - IoT Security Problems
    - OWASP Top 10 IoT Threats



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- OWASP IoT Attack Surface Areas
- IoT Attacks

- Perform Forensics on IoT Devices
  - Introduction to IoT Forensics
  - IoT Forensics Process
  - IoT Forensics Challenges
  - Wearable IoT Device: Smartwatch
  - IoT Device Forensics: Smart Speaker—Amazon Echo
  - Hardware Level Analysis: JTAG and Chip-off Forensics
  - Extracting and Analyzing Data from Drone/UAVs
  - IoT Forensics Tools

## REQUIREMENTS:

IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, incident response, and threat vectors.

## Difficulty level

## CERTIFICATE:

The participants will obtain certificates signed by EC-Council (course completion). This course will help prepare you also for the CHFI certification exam.

CHFI v11 exam details:

- Exam Code : 312-49
- Number of Questions : 150
- Duration : 4 hours
- Availability: ECC Exam Portal
- Passing Score: 60-85%
- Test Format : Multiple Choice Question (MCQs)

*Each participant in an authorized training CHFI - Computer Hacking Forensic Investigator held in Compendium CE will receive a free CHFI certification exam voucher.*



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

## TRAINER:

Certified EC-Council Instructor (CEI)

## ADDITIONAL INFORMATION:

The training materials include official EC-Council electronic courseware, 180-day access to iLabs, and an exam voucher.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007