CYBER SECURITY

EC-Council Computer Hacking Forensic Investigator

INCLUSIONS	LENGTH	PRICE (Incl. GST)	VERSION
Exam voucher	**5 days**	**$5170**	**10**

EC-COUNCIL AT LUMIFY WORK

The International Council of E-Commerce Consultants (EC-Council) is a member-based organisation that certifies individuals in various e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Security Analyst (ECSA) and Licensed Penetration Tester (LPT) certifications and cyber security courses. Lumify Work is the partner of choice for EC-Council in Australia.

WHY STUDY THIS COURSE

Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks.

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 defence forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.

Exam vouchers
Note that exams are not taken while sitting an EC-Council course. You will be provided with an exam voucher. Candidates are required to book their exam after completion of the course, and are welcome to book a spot at their local Lumify Work campus. Your voucher will come with an expiry date. Please refer to the Lumify Work booking terms and conditions regarding exam voucher validity.

Please note: There are strict conditions applied to attendance at this course. Prior to the course, or on the first day, students are required to sign an agreement form. Further details and a copy of the form will be provided in your pre-course information or with your courseware in MyDDLS.

WHAT YOU'LL LEARN

- Forensic Science

https://www.lumifywork.com/en-au/courses/eccouncil-computer-hacking-forensic-investigator/

CYBER SECURITY

EC-Council Computer Hacking Forensic Investigator

- Regulations, Policies and Ethics
- Digital Evidence
- Procedures and Methodology
- Digital Forensics
- Tools/Systems/Programs

My instructor was great being able to put scenarios into real world instances that related to my specific situation.

I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.

I learnt a lot and felt it was important that my goals by attending this course were met.

Great job Lumify Work team.

AMANDA NICOL
IT SUPPORT SERVICES MANAGER - HEALTH WORLD LIMITED

https://www.lumifywork.com/en-au/courses/eccouncil-computer-hacking-forensic-investigator/

CYBER SECURITY

EC-Council Computer Hacking Forensic Investigator

Lumify Work Customised Training

We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.

For more information, please contact us on 1 800 853 276.

COURSE SUBJECTS

Module 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
- Identify the Roles and Responsibilities of a Forensic Investigator
- Understand the Challenges Faced in Investigating Cybercrimes
- Understand Legal Compliance in Computer Forensics

Module 2: Computer Forensics Investigation Process

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

Module 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

https://www.lumifywork.com/en-au/courses/eccouncil-computer-hacking-forensic-investigator/

EC-Council Computer Hacking Forensic Investigator

- Understand Encoding Standards and Hex Editors
- Analyse Popular File Formats Using Hex Editor

Module 4: Data Acquisition and Duplication

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

Module 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 Minimising Techniques
- Understand Anti-Forensics Countermeasures

Module 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 Text-based Logs and Windows Event Logs

https://www.lumifywork.com/en-au/courses/eccouncil-computer-hacking-forensic-investigator/

CYBER SECURITY

EC-Council Computer Hacking Forensic Investigator

Module 7: Linux and Mac Forensics

- Understand Volatile and Non-volatile Data in Linux
- Analyse Filesystem Images Using The Sleuth Kit
- Demonstrate Memory Forensics Using Volatility & PhotoRec
- Understand Mac Forensics

Module 8: Network Forensics

- Understand Network Forensics
- Explain Logging Fundamentals and Network Forensic Readiness
- Summarise 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

Module 9: 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)
- Analysing ModSecurity Audit Logs
- Investigate Web Attacks on Windows-based Servers
- Detect and Investigate Various Attacks on Web Applications

Module 10: Dark Web Forensics

https://www.lumifywork.com/en-au/courses/eccouncil-computer-hacking-forensic-investigator/

EC-Council Computer Hacking Forensic Investigator

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

Module 11: Database Forensics

- Understand Database Forensics and its Importance
- Determine Data Storage and Database Evidence Repositories in MSSQL Server
- Collect Evidence Files on MSSQL Server
- Perform MSSQL Forensics
- Understand Internal Architecture of MySQL® and Structure of Data Directory
- Understand Information Schema and List MySQL Utilities for Performing Forensic Analysis
- Perform MySQL Forensics on WordPress Web Application Database

Module 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

Module 13: Investigating Email Crimes

LUMIFY work

Call 1800 853 276 and speak to a Lumify Work Consultant today!

training@lumifywork.com
facebook.com/LumifyWorkAU
twitter.com/LumifyWorkAU
lumifywork.com
linkedin.com/company/lumify-work
youtube.com/@lumifywork

EC-Council Computer Hacking Forensic Investigator

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

Module 14: Malware Forensics

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

Module 15: 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

https://www.lumifywork.com/en-au/courses/eccouncil-computer-hacking-forensic-investigator/

EC-Council Computer Hacking Forensic Investigator

- Perform Logical Acquisition on Android and iOS Devices
- Perform Physical Acquisition on Android and iOS Devices
- Discuss Mobile Forensics Challenges and Prepare Investigation Report

Module 16: IoT Forensics

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

LUMIFY work

Call 1800 853 276 and speak to a Lumify Work Consultant today!

training@lumifywork.com
facebook.com/LumifyWorkAU
twitter.com/LumifyWorkAU
lumifywork.com
linkedin.com/company/lumify-work
youtube.com/@lumifywork

CYBER SECURITY

EC-Council Computer Hacking Forensic Investigator

WHO IS THE COURSE FOR?

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

Target Audience:

- Police and other law enforcement personnel
- Defence and Security personnel
- e-Business Security professionals
- Legal professionals
- Banking, Insurance, and other professionals
- Government agencies
- IT managers
- Digital Forensics Service Providers

We can also deliver and customise this training course for larger groups – saving your organisation time, money and resources. For more information, please contact us on 1800 U LEARN (1800 853 276)

PREREQUISITES

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

The supply of this course by Lumify Work is governed by the booking terms and conditions. Please read the terms and conditions carefully before enrolling in this course, as enrolment in the course is conditional on acceptance of these terms and conditions.

https://www.lumifywork.com/en-au/courses/eccouncil-computer-hacking-forensic-investigator/