Computer Hacking Forensics Investigator (CHFI) (Voucher Included) - Online

Online Computer Hacking Forensics Investigator Training

Digital forensics has a key place on every cybersecurity team. Without it, most organization's security posture and maturity will fail to see its full potential. In this 100% online course, you will gain a critical skill set for the identification of an intruder's footprints and gathering necessary evidence for prosecution.

Upon successful completion, you will be prepared to take and pass the EC-Council's Computer Hacking Forensic Investigator (CHFI) Certification exam, a credential that validates your understanding of digital forensic tools and how they're used in the cybersecurity industry.

Job Outlook for Computer Hacking Forensics Investigator Professionals

The US Bureau of Labor Statistics forecasts 31% growth in demand for information security analysts between now and 2029, much faster than the average for all occupations. The BLS notes that this growth is driven largely by the increasing number of cyberattacks.

BLS data indicates that information security analysts earn $99,730 per year, on average.

All Courses Held Online
For Information Visit:
lcc.edu/jtc/career-training

EC-COUNCIL

Computer Hacking Forensics Investigator (CHFI) (Voucher Included) - Online

Course Objectives

- Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling.
- Understand how to perform anti-forensic methods detection and post-intrusion analysis of electronic and digital media to determine who, where, what, when, and how the intrusion occurred.
- Gain the ability to extract and analyze logs from various devices like proxy, firewall, servers, and more.
- Learn the skills to identify the possible source or incident origin.

Curriculum

I. Computer Forensics in Today's World
II. Computer Forensics Investigation Process
III. Understanding Hard Disks and File Systems
IV. Data Acquisition and Duplication
V. Defeating Anti-Forensics Techniques
VI. Operating System Forensics
VII. Network Forensics
VIII. Investigating Web Attacks
IX. Database Forensics
X. Cloud Forensics
XI. Malware Forensics
XII. Investigating Email Crimes
XIII. Mobile Forensics
XIV. Forensics Report Writing and Presentation

LANSING COMMUNITY COLLEGE | **COMMUNITY EDUCATION & WORKFORCE DEVELOPMENT**

All Courses Held Online

For Information Visit:

lcc.edu/jtc/career-training

EC-COUNCIL

COURSE FREQUENTLY ASKED QUESTIONS

ALL COURSES HELD ONLINE
FOR INFORMATION VISIT:

lcc.edu/jtc/career-training

WHAT DO COMPUTER HACKING FORENSIC INVESTIGATORS DO?
COMPUTER HACKING FORENSIC INVESTIGATION IS THE PROCESS OF DETECTING HACKING ATTACKS AND PROPERLY OBTAINING EVIDENCE TO REPORT THE CRIME AND CONDUCT AUDITS TO PREVENT FUTURE ATTACKS. THEIR RESPONSIBILITIES ARE CONTINUALLY EXPANDING AS THE NUMBER OF CYBERATTACKS INCREASES.

WHAT JOB TITLES ARE ASSOCIATED WITH COMPUTER HACKING FORESNSIC INVESTIGATORS?
COMPUTER HACKING FORENSIC INVESTIGATORS ARE OFTEN REFERRED TO AS "INFORMATION SECURITY ANALYSTS." THEY MAY ALSO HOLD FORMAL TITLES SUCH AS:

- CYBER SECURITY ANALYST
- CYBER SECURITY ENGINEER
- COMPUTER FORENSICS INVESTIGATOR
- COMPUTER FORENSICS TECHNICIAN
- FORENSIC COMPUTER ANALYST
- INFORMATION SECURITY MANAGER
- SECURITY ENGINEER
- SECURITY ANALYST

IS CERTIFICATION IMPORTANT FOR COMPUTER HACKING FORENSIC INVESTIGATORS?
DIGITAL FORENSICS IS VITAL TO CYBERSECURITY. A CERTIFICATION SUCH AS THE EC-COUNCIL'S COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI) CERTIFICATION EXAM WILL VALIDATE YOUR UNDERSTANDING OF DIGITAL FORENSIC TOOLS AND HOW THEY'RE USED IN THE CYBERSECURITY INDUSTRY.

CAN FORESNSIC INVESTIGATORS WORK REMOTELY?
THESE INVESTIGATORS POSSESS VALUABLE, PORTABLE SKILL, AND AS A RESULT, MANY WORK REMOTELY AS EMPLOYEES.

ARE THERE ANY PREREQUISITES OR REQUIREMENTS?
PRIOR TO ENROLLING IN THIS COURSE, YOU SHOULD HAVE A WORKING KNOWLEDGE OF INFORMATION TECHNOLOGY, CYBERSECURITY, COMPUTER FORENSICS AND INCIDENT RESPONSE.

EC-COUNCIL