PECB Where Excellence Meets Recognition



PECB Certified
Digital Forensics Examiner (CDFE)

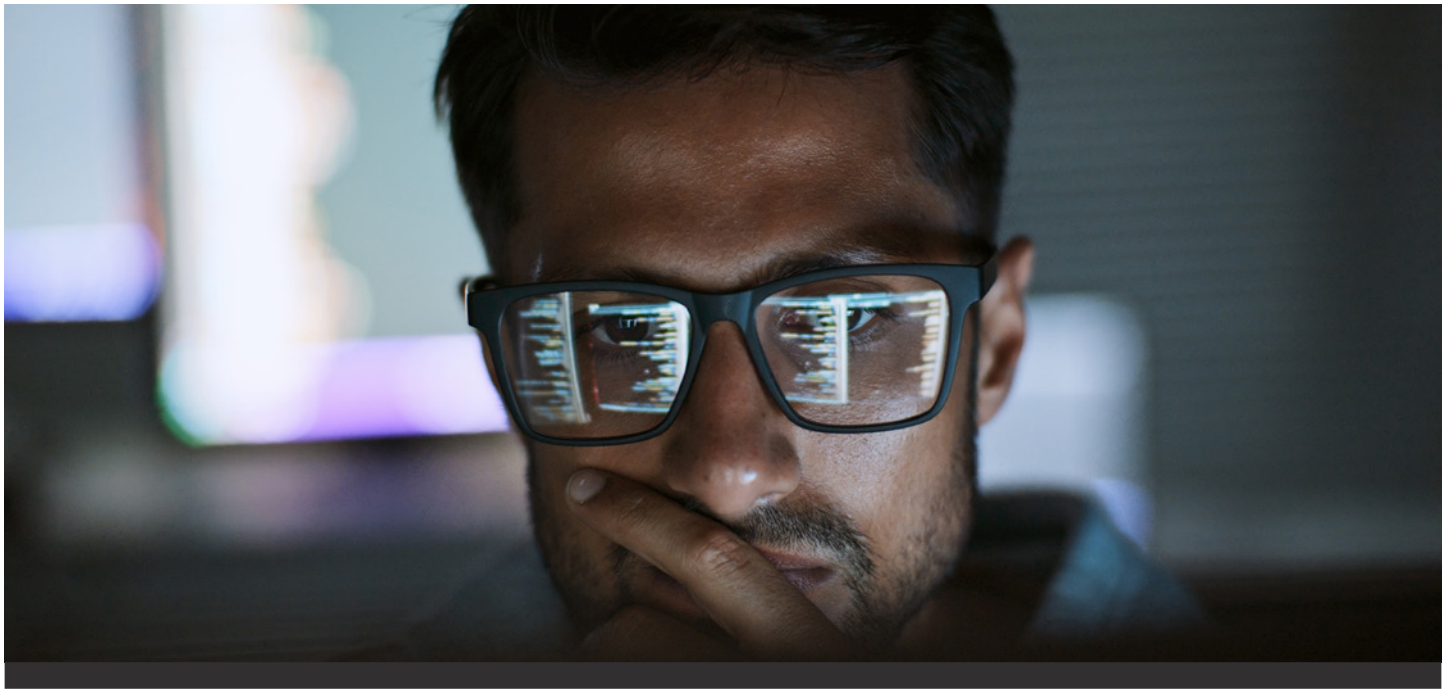
Gain expertise in uncovering, analyzing, and preserving digital evidence for legal investigations.

Why should you attend?

The Certified Digital Forensics Examiner (CDFE) training provides the expertise to conduct digital forensic investigations and obtain legally admissible digital evidence. This course provides a comprehensive understanding of forensic analysis techniques across various platforms, including Windows, macOS, Linux, and mobile devices.

Throughout the course, you will learn about the latest tools and methods for acquiring, analyzing, and preserving digital evidence, all while adhering to best practices in the industry. You will also explore core areas such as file system forensics, memory forensics, network analysis, and advanced malware analysis. By mastering the critical components of digital forensics, you will be well-prepared to handle complex investigations and secure evidence from a range of devices and systems.

Upon successful completion of the training, you will be eligible to sit for the PECB Certified Digital Forensics Examiner (CDFE) exam. Earning this credential will demonstrate your capability to lead advanced investigations, perform in-depth analysis, and ensure the integrity of digital evidence across diverse environments.



Who should attend?

This training course is intended for:

- Digital forensics analysts and investigators
- IT security professionals and incident responders
- Legal professionals involved in cybercrime cases
- Corporate security officers and compliance managers
- Professionals seeking to advance their knowledge in digital forensics
- Information security tea m members
- Cybersecurity professionals and cyber intelligence analysts

Course agenda

Duration: 5 days

Day 1 | Foundations of digital forensics

- Training course objectives and structure
- Introduction to digital forensics
- Digital forensics tools and techniques
- Network analysis with Wireshark
- Basics of malware analysis

Day 2 | File system analysis and reverse engineering

- File system forensics
- Memory forensics
- Reverse engineering in Windows (PE files)
- Reverse engineering in Linux (ELF files)
- x86 architecture fundamentals

Day 3 | Malware analysis and threat hunting

- Advanced malware analysis techniques
- Introduction to Zeek for network analysis
- Ghidra for malware analysis
- Yara rule development for threat hunting

Day 4 | Advanced forensic analysis and incident response

- Dark web forensics
- Interactive behavior analysis
- Memory and file system techniques
- Advanced scripting and automation with Zeek
- Patch analysis and modifications with Ghidra
- Closing of the training course

Day 5 | Certification Exam



Learning objectives

By the end of this training course, participants will be able to:

- Demonstrate an in-depth understanding of digital forensic principles, legal considerations, and investigative procedures applicable to cybercrime and incident response
- Effectively collect, preserve, and analyze digital evidence from various sources, ensuring adherence to chain-of-custody and evidentiary standards
- Utilize industry-standard forensic tools and methodologies to examine file systems, recover deleted data, and detect evidence of tampering or malicious activity
- Produce comprehensive forensic reports and communicate findings clearly, supporting both technical and legal audiences in investigations and potential litigation

Examination

Duration: 3 hours

The "PECB Certified Digital Forensics Examiner" exam fully meets the PECB Examination and Certification Program (ECP) requirements. It covers the following competency domains:

Domain 1 | Network traffic and protocol analysis

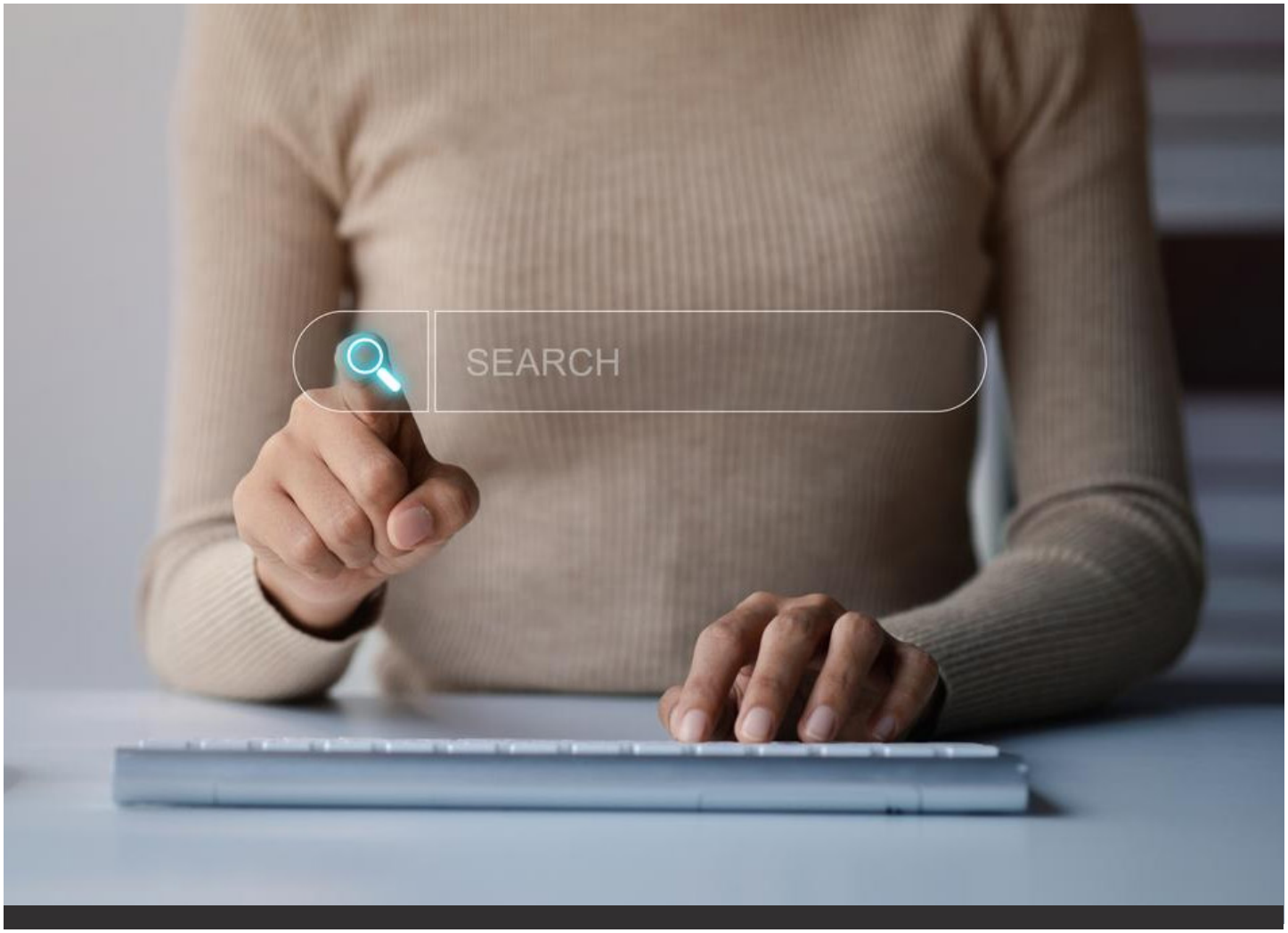
Domain 2 | Memory acquisition and forensics

Domain 3 | File-system and disk forensics

Domain 4 | Malware analysis and reverse engineering

Domain 5 | Threat hunting, automation, and correlation

For specific information about exam type, languages available, and other details, please visit the List of PECB Exams and the Examination Rules and Policies.



Certification

After passing the exam, you can apply for one of the credentials in the table below. You will receive a certificate once you fulfill all the requirements of the selected credential.

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Provisional Digital Forensics Examiner	PECB Certified Digital Forensics Examiner exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Digital Forensics Examiner (CDFE)	PECB Certified Digital Forensics Examiner exam or equivalent	Five years: two years of work experience in computer forensics	300 hours	Signing the PECB Code of Ethics

For more information about the PECB certification process, please refer to Certification Rules and Policies.

General information

- Certificate and examination fees are included in the price of the training course.
- Participants will receive more than 300 pages of comprehensive training materials, including practical labs.
- Participants who have attended the training course will receive an attestation of course completion worth 31 CPD (Continuing Professional Development) credits.
- Candidates who have completed the training course with one of our partners and failed the first exam attempt are eligible to retake the exam for free within a 12-month period from the date the coupon code is received because the fee paid for the training course includes a first exam attempt and one retake. Otherwise, retake fees apply.