INTI.Q SOLUTIONS

PECB

PECB Certified
Lead Forensics Examiner

Master the Computer Forensics processes

Why should you attend?

Lead Computer Forensics Examiner training enables you to acquire the necessary expertise to perform Computer Forensics processes in order to obtain complete and reliable digital evidence. During this training course, you will also gain a thorough understanding of Computer Forensics fundamentals, based on the best practices used to perform forensics evidence recovery and analytical techniques. This training course is focused on core skills required to collect and analyze data from Windows, Mac OS X, and Linux operating systems, and also from mobile devices.

After mastering all the necessary concepts of Computer Forensics processes, you can sit for the exam and apply for a "PECB Certified Lead Computer Forensics Examiner" credential. By holding a PECB Lead Computer Forensics Examiner Certificate, you will be able to prove that you have the expertise to lead advanced forensic investigations and conduct forensics analysis, reporting, and evidence acquisition.

Who should attend?

- Computer Forensics specialists
- Computer Forensics consultants
- Cybersecurity professionals
- Cyber intelligence analysts
- Electronic data analysts
- Specialists in computer evidence recovery
- Professionals working or interested in law enforcement
- Professionals seeking to advance their knowledge in Computer Forensics analysis
- Information Security team members
- Information technology expert advisors
- Individuals responsible for examining media to extract and disclose data
- IT Specialists

Course agenda

Duration: 5 days

Day 1 | Incident Response and Computer Forensic Concepts

- Course objectives and structure
- Standard and regulatory framework
- Historical aspects of Digital Forensic
- Basic concepts and definitions in ISO 27037
- Overview of ISO 27037 standard
- Roles and responsibility of CLFE
- Computer Forensic Laboratory

Day 2 | Prepare and Lead a Computer Forensic Investigation

- Technical fundamentals
- File System Forensic
- Common File Systems
- Common Operating Systems
- Forensic Acquisition

Day 3 | Digital Artifacts Analysis and Management

- Digital artifacts: Identify, acquire, analyze and communicate
- Using open source forensic acquisition and analysis tools
- ISO/IEC 27037:2012
- Advanced Keywords searching with Regular Expression

Day 4 | Case Presentation & Trial Simulation

- Decision-making of collection or acquisition of potential digital evidence
- Other Essential Digital Forensic Topics
- CLFE Professional Ethics
- Presenting Digital Forensic Findings
- Competence and evaluation of examiners
- Closing the training

Day 5 | Certification Exam

Learning objectives

- Understand the roles and responsibilities of the Lead Computer Forensics examiner during digital forensic investigation
- Understand the purpose of electronic media examination and its correlation with common standards and methodologies
- Comprehend the correct sequence of steps of a computer incident investigation and digital forensic operation
- Understand the common commercial and open source tools that may be used during incident investigation and digital forensic operations
- Acquire the necessary competencies to plan and execute a computer forensics operation and also implement and maintain a safety network to protect evidence

Examination

Duration: 3 hours

The "PECB Certified Lead Computer Forensics Examiner" exam fully meets the requirements of the PECB Examination and Certification Programme (ECP). The exam covers the following competency domains:

Domain 1 | Fundamental principles and concepts of Computer Forensics

Domain 2 | Best practices on Computer Forensics

Domain 3 | Digital forensics laboratory requirements

Domain 4 | Operating system and file system structures

Domain 5 | Mobile devices

Domain 6 | Computer crime investigation and forensics examination

Domain 7 | Maintaining chain of evidence

For more information about exam details, please visit Examination Rules and Policies.

Certification

After successfully completing the exam, you can apply for the credentials shown on the table below.
You will receive a certificate once you comply with all the requirements related to the selected credential.

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

The requirements for PECB Computer Forensics Examiner Certifications are:

Credential	Exam	Professional experience	CFMS project experience	Other requirements
PECB Certified Provisional Forensics Examiner	PECB Certified Lead Forensics Examiner Exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Forensics Examiner	PECB Certified Lead Forensics Examiner Exam or equivalent	**Two years:** One year of field experience in computer forensics	Forensics activities totaling 200 hours	Signing the PECB Code of Ethics
PECB Certified Lead Forensics Examiner	PECB Certified Lead Forensics Examiner Exam or equivalent	**Five years:** Two years of field experience in computer forensics	Forensics activities totaling 300 hours	Signing the PECB Code of Ethics

General information

- Certification and examination fees are included in the price of the training course
- Training material containing over 450 pages of information and practical examples will be distributed
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued
- In case of exam failure, you can retake the exam within 12 months for free