When Recognition Matters

# PECB CERTIFIED LEAD FORENSICS EXAMINER

## MASTERING THE IMPLEMENTATION AND MANAGEMENT OF COMPUTER FORENSICS PROCESSES

## SUMMARY

This five-day intensive course enables the participants to develop the necessary expertise in mastering the computer forensics processes as specified in CLFE certification. Participants will gain a thorough understanding of fundamental computer forensics, based on the best practices used to implement the forensics evidence recovery and analytical processes. The CLFE certification focuses on core skills required to collect and analyze data from Windows, Mac OS X, Linux computer systems, as well as from mobile devices.

## WHO SHOULD ATTEND?

- Computer Forensic specialists
- Electronic data analysts
- Specialists in computer search and evidence recovery
- Professionals working or interested in law enforcement
- Professionals willing to advance their knowledge in computer forensic analysis
- Members of an information security team
- Expert advisors in information technology
- Individuals responsible for examining media to extract and disclose data

## COURSE AGENDA

DURATION: 5 DAYS

DAY 1

### Introduction to scientific principles of Computer Forensics operations

- Scientific principles of computer forensics
- Introduction to computer forensics process approach
- The analysis and implementation of the fundamental operations
- Preparation and execution of forensics procedures and operations

DAY 2

### The computer and operating structure

- Identification and selection of the characteristics of the computer structure
- Identification of peripherals and other components
- Understanding the operating systems
- Extraction and analysis of the file structure

DAY 3

### Forensics of networks and mobile devices

- Understanding the network, cloud and virtual environments
- Generic methods for data examination in a virtual environment
- Examination of a cell phone or tablet
- Enumeration of cell phones and tablets needed for forensics examination
- Storage of information in mobile devices

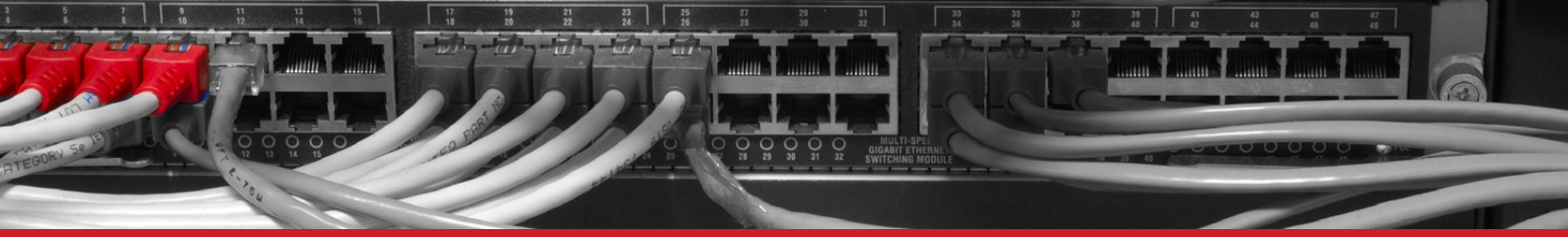
DAY 4

### Computer Forensics tools and methodologies

- Enumeration and examination of the computer hardware and software
- Determination and testing of corrective measures
- Analysis and selection of the best procedures for computer forensics operation
- Discovery, documentation and return of the evidence on-site
- Analyzing and applying the contextual parameters

DAY 5

### Certification Exam



## LEARNING OBJECTIVES

- To ensure that the CLFE can protect him or herself against injury, threat to credibility and protect the integrity of the examined media throughout the computer forensics operation
- To ensure that the CLFE can conduct a complete computer forensics operation and determine the course of action to be followed in order to achieve the goal of the operation
- To ensure that the CLFE can safely handle computers, extract and install peripherals and components, relate the presence of certain ports to the actual or eventual presence of a media containing information to be examined
- To ensure that the CLFE has a clear knowledge where the information can be found on an electronic media or bit-stream image of a media, it would be operating the systems or user information, actual deleted or hidden information
- To ensure that the CLFE can conduct a forensically sound examination, extraction and preservation of evidence located on a network, in the cloud or in a virtual environment
- To ensure that the CLFE can conduct a basic, yet forensically sound examination of a cell phone or tablet
- To ensure that the CLFE can use efficiently the tools (software, hardware and supplies) of the field examination kit for a better goal achievement of the computer forensics operation
- To ensure that the CLFE can justify the way an artifact was acquired or left behind in an ordered, standard and forensically sound manner

## EXAMINATION

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

1 **Domain 1: Scientific Principles of computer forensics**

Main Objective: To ensure that the CLFE can protect himself against injury, threat to credibility and protect the integrity of the examined media throughout the computer forensics operation

2 **Domain 2: Computer forensics operations fundamentals**

Main Objective: To ensure that the CLFE can conduct a complete computer forensics operation and determine the course of action to be followed to achieve the goal of the operation

3 **Domain 3: Forensics: computer hardware structure**

Main Objective: To ensure that the CLFE can safely handle computers, extract and install peripherals and components, relate the presence of certain ports to the actual or eventual presence of a media containing information to be examined

4 **Domain 4: Forensics: operating systems and file structure**

Main Objective: To ensure that the CLFE have a clear knowledge where information can be found on an electronic media or bit-stream image of a media, would it be operating system's or user information or actual, deleted or hidden information

5 **Domain 5: Forensics of network, cloud and virtual environments**

Main Objective: To ensure that the CLFE can conduct a forensically sound examination, extraction and preservation of evidence located on a network, in the cloud or in a virtual environment

6 **Domain 6: Forensics of cell phones and tablets**

Main Objective: To ensure that the CLFE can conduct a basic but forensically sound examination of a cell phone or a tablet

7 **Domain 7: Computer Forensics operation tools and software**

Main Objective: To ensure that the CLFE can conduct a basic but forensically sound examination of a cell phone or a tablet

8 **Domain 8: Forensics: examination, acquisition and preservation of electronic evidence**

Main Objective: To ensure that the CLFE can justify the way an artifact was acquired or left behind in an ordered, standard and forensically sound manner

- The "PECB Certified Lead Forensics Examiner" exam is available in different languages, such as English, French, Spanish and Portuguese
- Duration: 3 hours
- For more information about the exam, please visit: www.pecb.com

## CERTIFICATION

- A certificate of "PECB Certified Lead Forensics Examiner" will be issued to those participants who successfully pass the exam and comply with all the other requirements related to this credential:

| Credential | Exam | Professional Experience | Education | Other Requirements |
|---|---|---|---|---|
| **PECB Certified Lead Forensics Examiner** | PECB Certified Lead Forensics Examiner Exam | **Two years** One year of field experience in Computer Forensics | At least Secondary School | Signing the PECB code of ethics |

## GENERAL INFORMATION

- Certification fees are included in the exam price
- Participant manual contains over 450 pages of information and practical examples
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued to the participants
- In case of failure of the exam, participants are allowed to retake it for free under certain conditions