PECB

When Recognition Matters

WHITEPAPER

CLFE

CERTIFIED LEAD FORENSIC EXAMINER

CONTENT

PRINCIPAL AUTHORS
Eric LACHAPELLE, PECB
Mustafë BISLIMI , PECB
Bardha AJVAZI, PECB

INTRODUCTION

Computer forensics is the use of analytical and investigative methods to identify, collect, examine and preserve evidence that is magnetically stored or encoded in PC's, hard disks, flash drives, PDA's, mobile phones, etc. Computer forensics can be used as evidence for computer crimes or any other crime, in addition to finding out exactly what happened on a computing device and who is responsible for the occurrence.

The goal is to perform a structured investigation while maintaining a documented chain of evidence that can undergo the legal analysis of a court of law, for either a criminal or civil proceeding.

Gaining skills and knowledge to practice computer forensics will help ensure the overall integrity and survival of a network infrastructure.

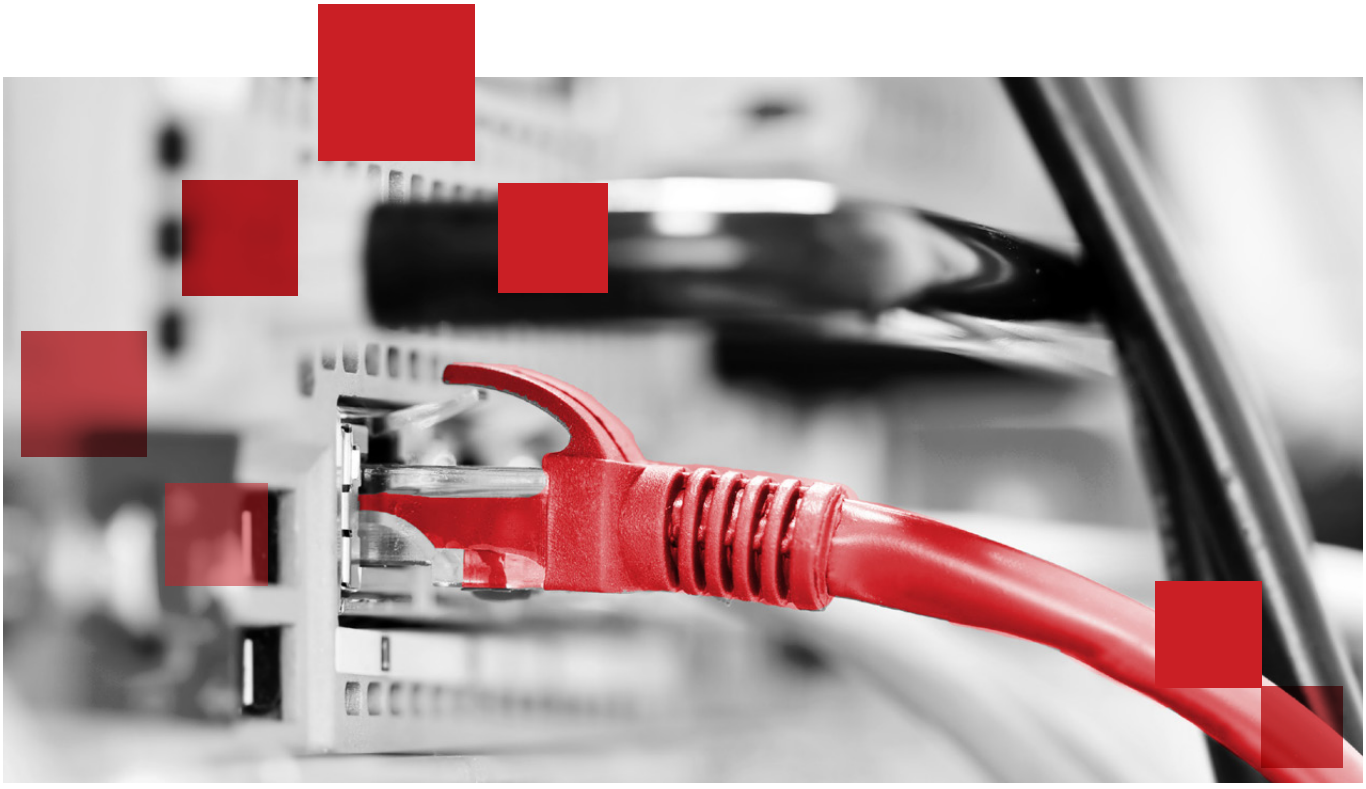
The key elements of computer forensics are:

- The use of scientific methods,
- Collection and preservation,
- Validation,
- Identification,
- Analysis and interpretation, and
- Documentation and presentation.

Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification.

Forensic investigators typically follow the following set of procedures:

- After making sure the device cannot be accidentally contaminated, investigators make a digital copy of the device's storage media.
- It is then locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.



An overview of CFLE

In the early 1980s personal computers became more accessible to consumers, leading to an increase in computer criminal activity.

The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court.

The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.
The scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events.

Recently, commercial organizations have vastly benefited from computer forensics in a variety of cases such as:

- Intellectual property theft,
- Industrial espionage,
- Employment disputes,
- Fraud investigations,
- Forgeries,
- Bankruptcy investigations,
- Inappropriate email and internet use in the work place,
- Regulatory compliance etc.

The role of computer forensics will play an even more critical role in society as computer technology emerges. It is an extremely hot topic and is used widely among all industries. Corporations and government agencies hire computer forensics specialists, whenever they need a computer-related crime investigated.

The science of computer forensics has a limitless future as long as technology advances, the field will continue to expand. Any methodology, process or procedural breakdown in the application of forensics can jeopardize the company's case.

So, what is Computer Forensics?

The U.S. Department of Justice defines computer forensics as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events."

Computer forensics typically are performed to determine what activity took place, on a particular device by a user, or to restore previously deleted or corrupted data.

The CLFE certification focuses on core skills required to collect and analyze data from Windows, Mac OS X, Linux computer systems as well as mobile devices.

Did you know that…?

- Forensic analysis can reveal what web sites have been visited and what files have been downloaded?
- Forensic analysis can reveal what documents have been sent to the printer even if it was a document printed directly from a floppy disk?
- Forensic analysis can reveal when files were last accessed or when files were deleted?
- Forensic analysis can reveal attempts to fabricate or hide evidence?
- Forensic analysis can reveal deleted e-mail even if a web based e-mail server was used like Yahoo, MSN, or Hotmail.

Key domains of a CLFE

- Domain 1: Scientific principles of computer forensics
- Domain 2: Computer forensics operations fundamentals
- Domain 3: Forensics: computer hardware structure
- Domain 4: Forensics: operating systems and file structure
- Domain 5: Forensics of network, cloud and virtual environments
- Domain 6: Forensics of cell phones and tablets
- Domain 7: Computer forensics operation tools and software
- Domain 8: Forensics: examination, acquisition and preservation of electronic evidence

ll Scientific principles of computer forensics

To ensure that the CLFE can protect him/herself against injury, threat to credibility and protect the integrity of the examined media throughout the computer forensics operation.

ll Computer forensics operations fundamentals

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.

ll Forensics: computer hardware structure

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

ll Forensics: operating systems and file structure

To ensure that the CLFE understands how to find information on an electronic media or bit-stream image of a media. In addition, the CLFE should be aware of the type of information found, if it is from an operating system, if it is user information or actual, deleted or hidden information.

ll Forensics of network, cloud and virtual environments

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.

ll Forensics of cell phones and tablets

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

ll Computer forensics operation tools and software

To ensure that the CLFE can efficiently use the tools (software, hardware and supplies) of the field examination-kit to better achieve the goal of the computer forensics operation.

ll Forensics: examination, acquisition and preservation of electronic evidence

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

Electronic evidence is information and data of investigative value that is stored on a computer or is transmitted through it.

How does a CLFE approach the investigation?

The following model presents the common actions that a CLFE takes to complete their investigation:

Stage 1: Investigation preparation

- Identify the purpose of the investigation
- Identify the resources required

Stage 2: Evidence acquisition

- Identify and preserve digital evidence

Stage 3: Analysis of evidence

- Identify tools and techniques to use
- Process data
- Interpret analysis results

Stage 4: Results dissemination

- Report and present findings

What are the Business Benefits of Computer Forensics?

Some of the benefits of incorporating data analysis in a business can include:

- Capability to reduce or eliminate sampling risk,
- Assessment of relevant types of data from different systems or sources to show a more complete picture,
- Capability to easily trend relevant data over periods of time,
- Fast identification and extraction of certain risk criteria from the entire data population for further analysis,
- Testing for effectiveness of the control environment and policies in place by identifying attributes that violate rules, and
- Finding trends of which company personnel, consultants and forensic accountants were unaware of.

Today, with the sophistication of powerful software and the technological ability to extract large amounts of data, 100% of the information may be analyzed.

What are the challenges that a CLFE can come across?

New technologies and enhancements in procedures are allowing engineers and developers to create more stable and strong hardware, software and tools for the specialist to use in computer-related criminal investigations.

With new and complex advancements, difficult challenges arise. Some of the challenges that the field of computer forensics may face are:

- The advancement of encryption,
- The broad system of networking,
- Legal obstacles, and
- The substantial growth of storage media.

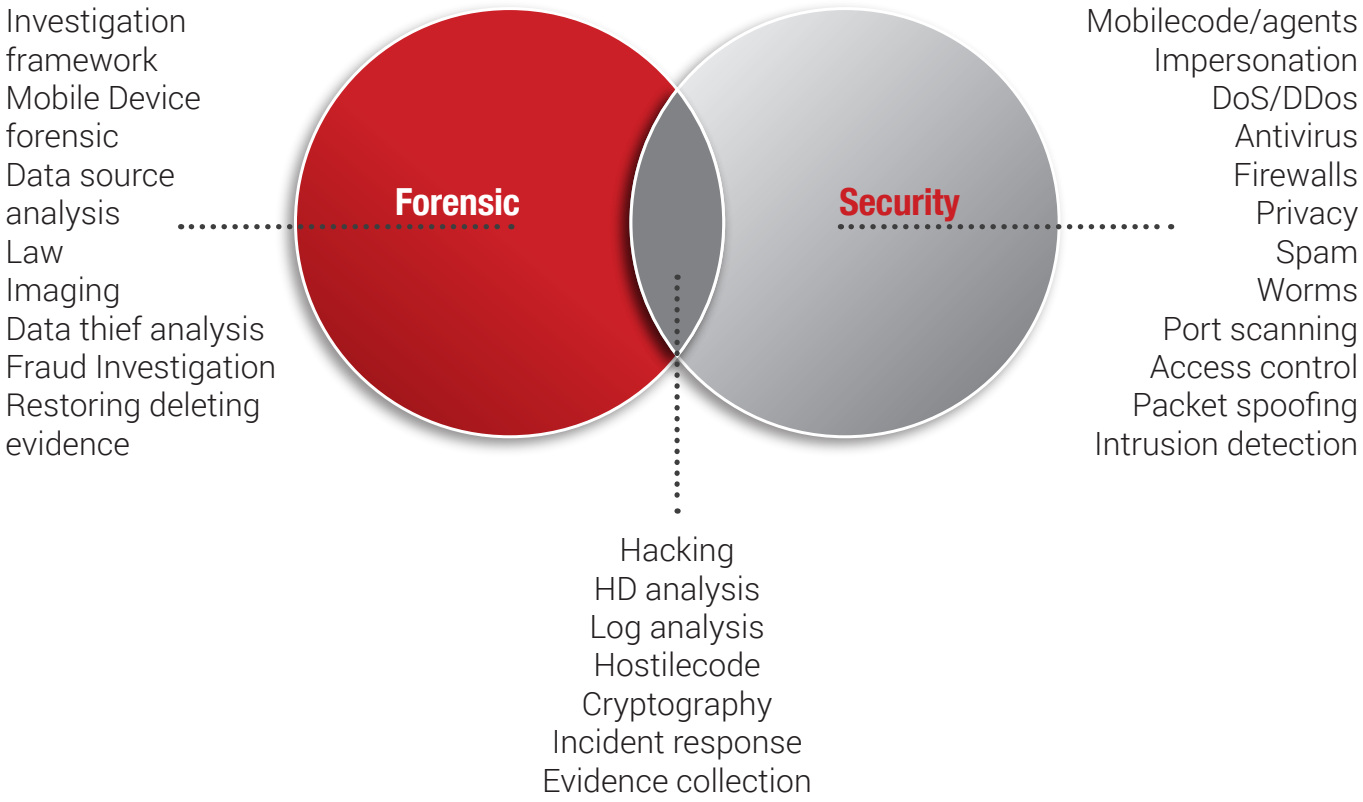
There are several basic rules that specialists tend to follow:

- Ensure that no forensics evidence is damaged, destroyed or otherwise compromised by the procedures used during the investigation,
- Never work on the original evidence,
- Establish and maintain a continuing chain of custody, and
- Document everything.

The ever-changing nature of technology contributes to the problems encountered by experts when collecting and preparing digital evidence for courtroom presentation.

Link of CLFE with other IT Security Standards

Recent years have seen considerable development in computer forensic and network security.
This has resulted in an ever increasing range of new protocols, new encryption algorithms, new methods of authentication, smarter firewalls and intrusion detection techniques, and new anti-malware products. To a significant degree, the sciences of security and forensics have both seen rapid but separate developments. Considering the similarities between these two important fields, they often connect and work together.



What are the application requirements for the CLFE Certification?

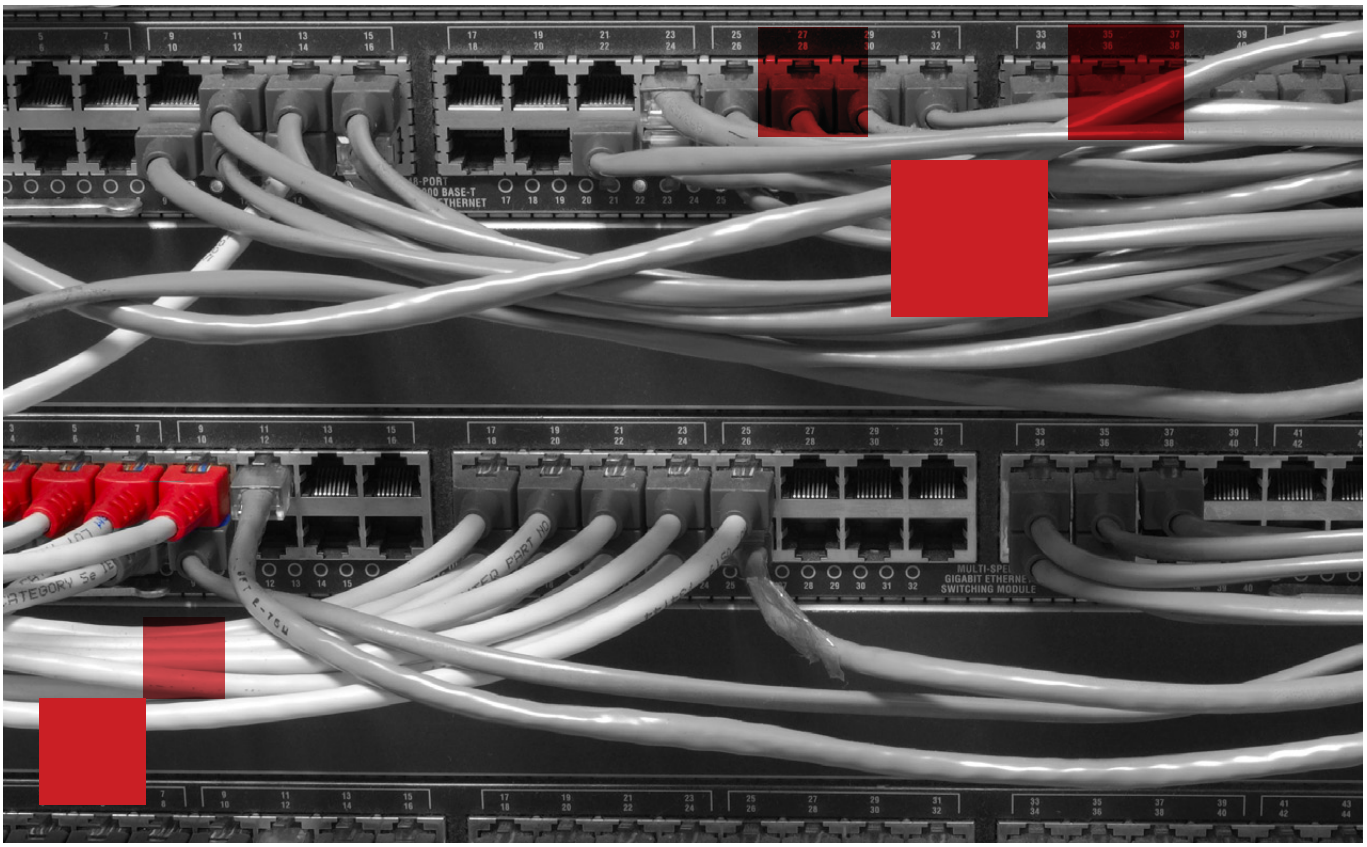
The table below briefly describes the requirements that an individual must meet in order to apply for the CLFE Certification offered by PECB.

Certification	Education	Exam	Professional experience	Other requirements
Certified Lead Forensics Examiner	At least secondary school	CLFE Exam	Two years One year of field experience in computer forensics	Signing the PECB code of ethics

Steps for obtaining a PECB Certification

To ensure that individuals achieve planned and desired CLFE results, the following steps will serve as guidance on how to become PECB Certified on Certified Lead Forensic Examiner - CLFE.

1. Participate in the training course,
2. Register for the certification exam,
3. Sit for the certification exam,
4. Apply for the certification scheme upon successful completion, and
5. Obtain the certification.



PECB

+1-844-426-7322

customer@pecb.com

Customer Service