

Hands-on course , 5  
day(s)  
Ref : CLF

### Participants

Computer Forensic specialists, Professionals working or interested in law enforcement, Members of an information security team, Expert advisors in information technology.

### Pre-requisites

Good knowledge in computer and information security.

### Next sessions

## CLFE, Certified Lead Forensics Examiner, certification

*This five-day intensive course enables the participants to develop the expertise in mastering the computer forensics processes. 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.*

### OBJECTIVES

- To ensure that the CLFE can protect him or herself against injury, threat to credibility
- To ensure that the CLFE can conduct a complete computer forensics operation
- To ensure that the CLFE has knowledge where the information can be found on an electronic or bit-stream image of a media
- To ensure that the CLFE can justify the way an artifact was acquired or left behind in a forensically sound manner

#### 1) Introduction to scientific principles of Computer Forensics operations

#### 2) The computer and operating structure

#### 3) Forensics of networks and mobile devices

#### 4) Computer Forensics tools and methodologies

#### 5) 3 hours certification Exam

### Certification

*A certificate of " Certified Lead Forensic Examiner" is awarded to participants who have passed the examination and meeting all other requirements for certification.*

### 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.

### 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.

### 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.

### 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.

### 5) 3 hours certification Exam

- 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 of network, cloud and virtual environments.