Course : Forensics iOS

Practical course - 3d - 21h00 - Ref. FOE
Price : 2100 € E.T.

This training course will give you the knowledge you need to carry out forensic analysis on iOS.

Teaching objectives

At the end of the training, the participant will be able to:

- Identify the traces left when a computer system is breached
- Investigate Apple systems
- Properly collect the evidence needed for legal proceedings
- Know different investigation techniques

Intended audience
System and network engineers/administrators, security managers.

Prerequisites
Good knowledge of IT security, networks/systems, and iOS systems.

Practical details
Hands-on work
Training alternates theory and practice. Everything we learn is put into practice.

Course schedule

1 **Forensic analysis of a mobile system**

- Computer forensics.
- Types of computer crime on mobile systems.
- Role of the computer surveyor.

PARTICIPANTS
System and network engineers/administrators, security managers.

PREREQUISITES
Good knowledge of IT security, networks/systems, and iOS systems.

TRAINER QUALIFICATIONS
The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS
The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Modern cybercrime

- Types of crime.
- Security incident management framework, CERT.
- Setting up labs: tools needed for iOS investigation.
- Analyze and understand attacks on mobile systems.
- Protection tools, French legislation.

Hands-on work
Network analysis of DDOS attacks, infections and BotNet traffic.

3 Digital proof

- Definition, role, types and filing rules.
- Evaluate and secure the electronic elements of a crime scene.
- Collect and preserve the integrity of electronic evidence.

Hands-on work
Duplicate data bit by bit, check integrity, recover files and analyze digital data.

4 Mobile systems forensic basics

- Understand the architecture of mobile systems and SIM cards.
- Forensic techniques for mobile systems.
- Forensic processes for mobile systems.

Hands-on work
Analyse des applications et malwares sous mobile. Etude de la distribution forensic Santoku.

5 The basics of forensic analysis of iOS systems

- Architecture and security of iOS systems.
- Hardware structure and models of Apple systems: mobiles, watches, iPad.
- File system for Apple systems.

Hands-on work
Setting up an iOS forensic investigation lab.

6 Data extraction and analysis techniques for iOS systems

- Techniques for data capture, analysis and encrypted or unencrypted backups.
- Collection of volatile and non-volatile data.
- iOS data analysis and recovery.
- Bypassing iOS system access security techniques.
- Data collection from a captured image and an iCloud system.
- Use of mobile investigation tools such as Elcomsoft iOS or Oxygen Forensic Detective, NowSecureCE.
- Data extraction techniques from third-party software.

Hands-on work
Investigate a captured image of an iOS system: jailbreak iOS systems, bypass encryption, collect and analyze RAM data, extract application data.

(7) **Forensic investigation reports**

- Understand the importance of investigative reports.
- Writing methodologies and templates for iOS forensics reports.

Dates and locations

REMOTE CLASS
2026 : 13 Apr., 3 June, 19 Oct., 7 Dec.

PARIS LA DÉFENSE
2026 : 27 May, 12 Oct., 30 Nov.