Publication date : 07/01/2024

Course : Forensics Android

Practical course - 3d - 21h00 - Ref. FOL
Price : 2470 CHF E.T.

This training course will give you the knowledge you need to carry out investigations on different Android systems and correctly collect the evidence required for legal proceedings.

Teaching objectives

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

- Acquire the skills needed to perform forensic analysis on Android
- Collect and preserve the integrity of electronic evidence
- Analyze intrusion a posteriori

Intended audience

Systems and network engineers/administrators, security managers.

Prerequisites

Good knowledge of IT security, networks/systems and Android 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

Systems and network engineers/administrators, security managers.

PREREQUISITES

Good knowledge of IT security, networks/systems and Android 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 to investigate Android.
- Analyze and understand attacks on mobile systems.
- Protection tools, French legislation.

Hands-on work
Network analysis of DDOS attacks, infections and BotNet traffic to C2.

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 evidence.

Hands-on work
Bit-by-bit duplication, integrity, file recovery and data analysis.

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
Analysis of mobile applications and malware. Forensic investigation with Santoku distribution.

5 The basics of forensic analysis of Android systems

- Study of Android model architectures.
- Study of software components: Kernel, Android Runtime, Libraries.
- Study of Android system security.

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

6 Data extraction and analysis techniques for Android systems

- Data extraction and acquisition techniques.
- Collection of volatile and non-volatile data.
- Android data analysis and recovery systems.
- Analysis and reverse engineering of Android applications.
- Bypass locking techniques.
- Obtain root access rights.
- Data extraction techniques from third-party software.

Hands-on work
Global investigation of a captured Android system image: Bypass encryption. Collecting and analyzing RAM. Root Android and extract data from third-party applications.

7 Forensic investigation reports

- Understand the importance of reports.
- Copywriting methodologies and templates.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

Dates and locations

REMOTE CLASS
2026 : 23 Mar., 20 May, 12 Oct., 23 Nov.