Publication date : 05/13/2024

Course : Forensics Windows

Practical course - 5d - 35h00 - Ref. FOH
Price : 3660 CHF E.T.

After a computer attack, forensic investigation is used to collect and analyze evidence for legal proceedings. The main objective is therefore to recover and analyze data proving a digital crime.

Teaching objectives

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

- Managing a digital investigation on a Windows computer
- Analyze intrusion a posteriori
- Collect and preserve the integrity of electronic evidence

Intended audience

People wishing to get started in computer forensics. Windows system administrators. Computer law experts.

Prerequisites

A solid grounding in information systems security.

Practical details

Hands-on work

Training alternates theory and practice. Everything we learn is put into practice.

Course schedule

1 Inforensics presentation

- Scope of investigation.
- Toolkit, methodology "First Responder" and Post-mortem analysis.
- Hard disks, introduction to file systems and time stamps.
- Data acquisition (persistent and volatile) and encrypted media management.
- Search for deleted data.
- Backups, Volume Shadow Copies and flash storage hazards.
- Windows registers and register structures.
- Analysis of logs, events / antivirus / other software.

PARTICIPANTS

People wishing to get started in computer forensics. Windows system administrators. Computer law experts.

PREREQUISITES

A solid grounding in information systems security.

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 Investigation scenario

- Download/access confidential content.
- Program execution, file and folder manipulation traces.
- Deleted files, unallocated space and carving.
- Geolocation and photographs (Exifs data).
- SMTP logs: server-side acquisition, mail client analysis.
- WiFi access points and USB devices.
- HTML5, emails and users abused by malware.
- Exfiltration of information.

3 Interaction on the Internet

- Office 365.
- Sharepoint.
- Traces on Windows ADs.
- Presentation of the main artifacts.
- Basics of RAM analysis.
- Use of Internet browsers.
- Chrome / IE / Edge / Firefox.

4 Linux forensics

- The basics of inforensics on a Linux workstation.
- The basics of inforensics on a Linux server: Web server logs & file system correlations.
- Creation and analysis of a file system timeline.

5 Overview

- Creation and analysis of a timeline enriched with artifacts.
- Example of tools for querying large volumes of data.

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 : 16 Mar., 15 June, 28 Sep., 7 Dec.