Cyberdefense

Training Catalogue 2025
Knowledge is power

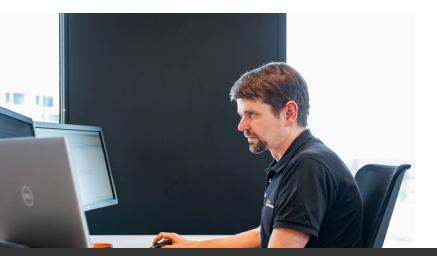## IR 3.02 | Incident Response & Forensic Analysis (Level 2)

Overview

This intensive hand-om one-day course expands on the content of IR3.01 and introduces all the basic concepts you need to understand incident response and forensic analysis in a Windows environment. It covers advanced disk acquisition scenarios and will enable you to delve into the heart of the NTFS file system. You will also learn how to perform direct acquisitions of the operating system to extract valuable information from its many artefacts.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins

Skills you'll learn

- **IR 3.01**
- **Level 3**
- **1 day**
- **French or English**

Course Modules

- **Introduction**
  - Objectives
  - Quick reminder of the IR3.01 takeaways
- **Advanced disk acquisition scenarios**
  - Encrypted media
  - BitLocker case
  - A few words on flash memories
  - SSD vs HDD
  - SSD acquisition
- **NTFS artifacts**
  - Overview of the MFT and MBR
  - The MFT metadata from a DFIR perpective
    - $MFT metadata ($SI, $FN, $DATA, $I30)
    - Transaction log ($LogFile)
    - Change log ($UsnJrnl)
  - Metadata parsing and limitations
- **Windows artifacts**
  - Registry artifacts
  - File-based artifacts
  - Event logs
- **Live acquisition**
- **Lab - Further investigate the Active Directory compromise**
  - Understanding live acquisition principles
  - Analyzing the output of a live acquisition
  - Parsing the acquired event logs
  - File-based artifacts analysis
  - Network and files deletion artifacts
- **Small game to remember the most important points of the day with fun**

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01