### Forensic Introduction



David Cruciani

david.cruciani@circl.lu

2024-2025

### Overview

- 1. Introduction (Course 1)
- 2. Understand disk (Course 1)
- 3. Imaging / Cloning and Mounting (Course 1)
- 4. File system analysis (Course 2)
- 5. NTFS (Course 2)
- 6. File System Time Line (Course 2)
- 7. Carving and String Search (Course 2)
- 8. Windows Registry (Course 2)
- 9. Windows Event Logs (Course 2)
- 10. Other Windows Artifacts (Course 2)
- 11. Introduction to Flowintel (Course 3)
- 12. The Exercise (Course 3)

## 11. Introduction to Flowintel

### 11.1 Flowintel?

- Case management
- Designed to be as simple as possible with essential options
- Primarily for security analysts, but not exclusively
- Accessible to anyone, including non-technical users
- Some features, like MISP integration, may not be useful for everyone

# 11.2 Live demo

# 12. The Exercise

### 12.1 Informations

- By group (2, max 3)
- Create a case in flowintel
  - Prepare each step of the investigation
    - Create tasks for acquisition also
    - For each task that need a tool, specify it
  - Distribute tasks and make assignment
  - Use this as a follow up of the investigation
  - Use notes in task to write down what you are doing
- Now make the analyze of circl\_dfir/Last\_exercise

### 12.2 The disk

- EWF disk image
- sudo apt install libewf-dev ewf-tools
- ewfexport disk-jean.E01
  - o enter
  - o out.raw
  - o enter
  - o enter
  - o enter

## Contact and Reference

- david.cruciani@circl.lu
- https://github.com/DavidCruciani
- info@circl.lu