CCF Lab 2 - Forensic file system analysis

In this lab, you will learn how to investigate a forensic analysis of a compromised file system. This is one of the basic and at the same time relevant and actual areas in forensic science.

Task 1 - Download the evidence file

You are offered to investigate the image of compromised system.

> If your st student number is odd, then you are investigating case1, if your st is even, then you are working with case2.

Download the core image: Case1

Download the core image: Case2

Case1&2 contains a large number of classic artifacts based on Windows OS.

Task 2 - Black box Forensics analysis

Use any forensics tools that you want. Different forensics tools can help you to analyze:

- Figure out the platform, system and file system type
- Perform a malware search
- Create and analyze a timeline
- Find artifacts in Windows components:
  - Windows Registry
  - Logs
  - Personal data of users
  - Network
  - Mail
  - Browser
  - Messengers
  - Windows libraries and configuration files
  - Other assets found in the compromised system

Task 3 - Create a Forensics Report

Prepare a forensic report on the results of the investigation on behalf of the investigator. This should include a timestamp, evidence/artifact, proof (specify your action, tool, screenshot - *if possible*). Try to follow to the the generally accepted standards for the preparation of a report on forensics. Example. However, it is not strict and mandatory to observe exactly such formatting.