How to analyze malware?

➡ Understand what a program does by looking at system calls, library calls, IO operations and so on

Two complementary approaches:

1. **Static Analysis**
   Analyze binary code and infer its behavior (control flow and data flow approaches)

2. **Dynamic Analysis**
   Run program in a sandbox and observe its behavior

How to automate malware analysis?

➡ Anti-malware tools combine static and dynamic analysis but use different approaches to make a decision

- **Signatures**
  Detect based on signatures database (known patterns)
  See *Yara* rules: https://yara.readthedocs.io/en/latest/

- **Machine learning**
  Detection based on similarities with a collection of known malware