# Memory

## Principle

- Additional information about execution etc.
- Can catch malware that only runs in memory

## Challenges

- Integrity

## Methods

- Kernel Level Application
  - e.g. LiME (Linux Memory Extractor) as Kernel Module
- Hardware bus based / dma
- Cold boot
  - Theoretical method to use remanence
- Hibernation files
- Virtualization

## Tools

https://forensics.wiki/windows_memory_analysis/

### Creation

- FTK Imager
- WindowsPmem Win
- LiME

### Analysis

- Volatility 3 — active, Python3-based memory analysis framework.
- Redline (FireEye) — free analyzer + triage with GUI, timeline and IOC features.
- MemProcFS — mounts a physical memory image as a virtual read-only filesystem.