

# Tools

## SIEM

- [Kibana](#)
- [Splunk](#)

## Network

[Wireshark](#)

## IR

- [X-ways](#)
- [Axiom](#)
- [F-Response](#)
- [Arsenal Image Mounter](#)
- [Magnet RAM Capture](#)
- [Exiftool](#)
- [SQLite Database Browser](#)
- [OST/PST Viewer](#)
- [Registry Viewer](#)
- [Regripper](#)
- [Ghidra](#)

## Memory

- [Volatility](#)

## Forensics