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

- evtwalk
  - Parse Windows Event Logs
- yaru
  - Yet another registry utility
- usp
  - USB parser
- dissect
  - Analysis of file systems and images
- timelines] * tools like [[plaso, log2timeline, timesketch

Data Collection

- CyLR
  - Collect artefacts on Win, Linux and MacOS
- UAC
  - Unix Artefacts Collector
- ntfswalk
  - ntfswalk, gena (gui)
- Scripts

Memory

- Volatility

Forensics