

Tools

SIEM

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

Network

- [Wireshark](#)

IR

- [Velociraptor](#)
 - remote artefact collection and administration
- [iris](#)
 - Collaborative Incident Response Platform
- [x_ways](#)
- [axiom](#)
- [f_Response](#)
- [arsenal_image_mounter](#)
- [magnet_ram_capture](#)
- [exiftool](#)
- [sqlite_database_browser](#)
- [ost_pst_viewer](#)
- [registry_viewer](#)
- [regripper](#)
- [ghidra](#)

Commandline

- [evtwalk](#)
 - Parse Windows Event Logs
- [dissect](#)
 - Analysis of file systems and images
- [timelines](#) * tools like [[plaso](#), [log2timeline](#), [timesketch](#)]
- [hayabusa](#)
 - Parses windows event logs or sysmon/linux

Windows GUI

- [MemProcFS](#)
- [Wireshark](#)
- [networkminer](#)
- [snort](#)
- [zeek](#)
- [yaru](#)
 - TZworks, yet another registry utility
- [usp](#)
 - TZWorks, USB parser
- [sysinternals](#)
 - tcpview, resmon,

Malware Analysis

- <https://threatfox.abuse.ch>
- <https://bazaar.abuse.ch>
- <https://thalosintelligence.com>
- <https://www.virustotal.com>

Data Collection

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

Active Directory

* [ping_castle](#)

Memory

- [Volatility](#)

Triage

- [//github.com/orlikoski/CyLR](https://github.com/orlikoski/CyLR)

Disks

- [dd](#), ddc3dd, ddrescue
- [ewfquire](#)
- [guymager](#)
- [FTK Imager](#)

```
sudo ewfquire -c empty-block /dev/sda
```

Forensics