GUI Based Tool

CLI Based Tool

List of Tools used for Memory Forensics

Windows Acquisition Tools:

- Belkasoft Live RAM Capture — https://belkasoft.com/ram-capturer
- Magnet RAM Capture — https://www.magnetforensics.com/resources/magnet-ram-capture/
- Rekall Winpmem — https://rekall.readthedocs.io/en/gh-pages/Tools/pmem.html
- MoonSols Dumpit — https://github.com/topics/dumpit
- AccessData FTK Imager — https://www.exterro.com/ftk-imager

MacOS Acquisition Tools:

- AVML — https://github.com/microsoft/avml

Linux Acquisition Tools:

- OSXPmem — https://github.com/Velocidex/c-aff4

Memory Analysis Tools:

Analysis Tools

- Volatility 2 — https://github.com/volatilityfoundation/volatility
- Volatility 3 — https://github.com/volatilityfoundation/volatility3
- MemProcFS — https://github.com/ufrisk/MemProcFS
- Orochi — https://github.com/LDO-CERT/orochi
- Volatility Workbench — https://www.osforensics.com/tools/volatility-workbench.html
- VolUtility — https://github.com/kevthehermit/VolUtility

The course is on 50% Sale now!
Grab the deal before it's too late

Scan to know more