

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>

Linux Acquisition Tools:



AVML

<https://github.com/microsoft/avml>



OSXPmem

<https://github.com/Velocidex/c-aff4>

Memory 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>





Memory Forensics Master Class for IRs



- 66 Total Lessons
- 30+ Demo and Lab Lessons
- 1 Infected Windows 10 Memory Image
- 1 Windows 10 Memory Image
- 1 WCRY Infected Memory Image
- 1 Cider Infected Memory Image
- 1 Windows 11 Memory Image
- 1 Linux Memory Image
- 1 MacOS Memory Image
- OpenSource Tool bundles (setup files) used in the class
- Oracle VM for Linux Forensics Workstation
- Oracle VM for OIB Forensics Suite
- Course Assessment with Hands-on Lab
- Life time access to the Course
- Downloadable Presentation Deck
- Course Completion Certificate

Memory Forensics Masterclass for Incident...

66 Lessons • 8 Trials

₹2,000 ~~₹4,500~~

56% OFF

💧 💧 The course is on 50% Sale now!

Grab the deal before it's too late 🏃 🏃

Scan to know more

