A GUI tool for Volatility Memory Forensics

Volatility is a command line memory analysis and forensics tool for extracting artifacts from memory dumps. Volatility Workbench is free, open source and runs in Windows. It provides a number of advantages over the command line version including,

- No need of remembering command line parameters.
- Storage of the operating system profile, KDBG address and process list with the memory dump, in a .CFG file. When a memory image is re-loaded, this saves a lot of time and avoids the frustration of not knowing the correct profile to select.
- Simpler copy & paste.
- Simpler printing of paper copies (via right click).
- Simpler saving of the dumped information to a file on disk.
- A drop down list of available commands and a short description of what the command does.
- Time stamping of the commands executed.
- Auto-loading the first dump file found in the current folder.
- Support for analysing Mac and Linux memory dumps.

Get started by **downloading the tool**

[source: https://www.osforensics.com/tools/volatility-workbench.html]