Live Forensics

Digital Forensics

Live or Memory Forensics

- Live, or memory-based, forensics is forensic activity performed on a running system
- The prevalence of encryption can mean that files are only readable while the system is running
- The use of network data sources can mean that only the running system has access to the data you want to capture
- Some data is only stored in memory, and never saved to files on the storage devices, so it must be captured from memory while the system is live
- Both ephemeral and persistent data are present in memory, and may be the only way to correlate the two (e.g. keys with data, logins with passwords, user accounts with actions)

Memory Capture

- Memory capture involves using a program which has administrator access to read RAM and can access all of memory
- Most forensic software suites include programs for this
- There are many standalone tools, both free and commercial to capture memory dumps
- Live memory is in constant flux, capture tools are affected by this
- Hibernation files can be used to get a frozen image of memory at the time of hibernation
- VMs that have been suspended have a memory image file that can be used for live forensics
- Cold boot techniques are interesting, but seldom practical

Windows Memory Capture

- https://belkasoft.com/ram-capturer is an example of a full-featured RAM capture tool
- Magnet RAM Capture is another good commercial tool which is free to use
- Dumpit is also popular, and does a symbol capture - recently became part of Comae Stardust threat hunter software but remains free to download and use
- They run in kernel mode which means they bypass most tools a user may have installed to prevent memory snooping
- They can run from a USB stick or other removable media so you can capture a live image of a running system before shutting it down to image any storage devices - this is always the preferred method
- Redline provides an interesting way to build custom data collectors for live analysis
- winpmem is a command-line tool for Windows memory capture
- The live image may provide you with the necessary passwords and encryption keys to later access encrypted files and online accounts

MacOSX Memory Capture

- MacOS presents unique obstacles to the forensic investigator, due to Apple's focus on protecting the privacy of their users
- In particular, current versions even prevent root from doing "root stuff" as freely as it could in the past (see SIP) but memory capture can still be done with advance planning
- The Rekall toolset was able to provide the necessary capabilities to analyze MacOS live systems and many vendors provide MacOS versions of their tools, but it has been discontinued and will only be useful on old Macs
- The GRR project may be a solution for MacOS, but is a very different approach requiring proactive installation of agents around the network
- Some forensic analysis software suites from the big commercial software vendors can provide limited analysis of MaOS memory images

Linux Memory Capture

- LiME (Linux Memory Extractor) is a kernel-based tool you can add to a Linux system that provides a memory capture mechanism
- LiME supports capturing to a local file, as well as to a TCP port, so that you can do remote captures
- It can run as an agent, so that you can do multiple captures over time if the situation calls for that

Memory Dump Analysis

- The open source tool Volatility is available for all major operating systems and provides a comprehensive toolset for analysis of memory dumps
- Forensics software suites can include varying levels of support for memory image analysis
- Memory dumps can contain information and data far beyond what a forensic investigation is looking for, and the analysis tools are used for many purposes, not just forensics
- As a result, the tools often provide many features and capabilities
- The Belkasoft Evidence Center tool can do advanced analysis of memory dumps to find various user-specific data items such as credentials, chat transcripts, social media history, etc.
- Magnet Forensics, Redline Forensics, and Comae are examples of other major players in this software market

Volatility

- Volatility is a command line tool, Redline provides a gui if you want to be empowered and limited by one, their Memoryze tool is also interesting (Redline's tools are for Windows)
- Volatility does not capture memory, use another tool such as RamCapturer for that - analysis can be done on any platform and does not need to be the same platform the image was captured on
- Volatility 2 has been out for a long time and is useful for older operating system releases, Volatility 3 is greatly improved and useful for newer operating system releases
- The commands available in Volatility to analyze your capture are different between the 2 verions
- volatility -f memdumpfile.mem imageinfo will help you to identify the OS profile when using Volatility 2 (called a SymbolSpace in Vol3) to use for analysis, can take a loooong time to run
- volatility -f memdumpfile.mem --profile=profilename -h will show you a list of volatility commands you can try on your memory image (N/A for Vol3)

Useful Plugins

- Commands to examine running processes, some or all may be present for the system you are investigating
  - pslist, psscan, pstree, psxview
  - procdump, memdump, privs
- cmdscan, consoles, cmdline can be used to examine open cmd windows
- netscan, svscan, iehistory can be used to examine networking
- hivelist, hivescan, hivedump, hashdump, userassist, shellbags, and shimcache can be used to explore registry and windows explorer activity and content
- modscan can be used to examine loaded kernel modules and drivers
- timeliner can build a list showing when things were loaded into memory

Getting started using Volatility

- https://www.youtube.com/watch?v=1PAGcPJFwbE&list=PLIv3b9B16Zaf-uDIgouB0DMiPNYU_sJFN - playlist of videos demonstrating volatility, with Windows, MacOSX, and both Kali and SIFT Linux systems
- See https://www.sans.org/ for a cheat sheet of memory forensics commands and artifacts that can be valuable when running volatility

Further Study

- The field of memory forensics is large and growing
- It is a hot topic in the anti-malware industry, anti-malware programs use the same OS hooks and tricks as malware - APT malware is often only visible in memory, not in persistent storage
- The Art of Memory Forensics is a good book with various resource files to take your knowledge of this area to the next level - their labs, quizzes, sample memory dumps, and answer keys are all free to download
- Memory analysis can be scripted and this allows us to automate the tasks to reduce time needed and reduce situations where a human investigator may miss evidence

Memory Forensics Lab

- Capture RAM from a VM using a capture tool
- Install volatility ram capture analyzer
- Run several high level commands from volatility to get an overview of what was running and what it was talking to