Lab Assignment 7

# Task – Working with Memory

In this assignment, you will be introduced to the basics of memory analysis. This lab may require access to the Cone Forensics Lab. Items in **RED/BOLD** are deliverable.

If we have not already covered the definitions for certain terms, or you are unfamiliar with them, I have included some below.

**Memory Acquisition**: Memory captured from a live OS with a tool such as FTK Imager or copied from a Virtual Machine (VMware .vmem file) .

**Host/Guest:** The host OS is the operating system running directly on the local hardware. The guest is an operating system that is “hosted” on the host OS and run insides a window operated by the hypervisor (Virtualization software).

**Volatility**: A python based framework for memory analysis. In this lab it is recommended to use the 64 bit exe version rather than py scripts.

**VMEM**: VMware stores device ram in a separate file while the VM is active. This file is removed after shutdown. As with a host OS, the RAM can be captured live using a tool like FTK Imager from within the OS, however the RAM from the current state can simply be copied out from the host without ever entering the guest OS.

In FTK Imager, these items can be seen outlined in red in the graphic below:

1. From a workstation: access the server’s shared directory and copy the file Joshua1.vmem to a folder on your desktop. If the file is already there, remove it and make a fresh copy. Hash the original file and the copy. You may wish to add both the original and the copy into FTK Imager to run these concurrently. Alternatively, you may use a command line alternative such as Powershell (Get-FileHash <filepath> -Algorithm MD5)



1. Create a TXT file in the same folder. This file should be named Lab7\_[name], where [name] is your first and last name.
2. Open FTK and create a new case. Select processing options and add Joshua1.vmem.
3. While this is completing, download the latest release of Volatility.
   1. Currently <http://downloads.volatilityfoundation.org/releases/2.6/volatility_2.6_win64_standalone.zip>
   2. There may be a newer release, check “Releases” on the menu at the top of the page.
   3. Unpack the zip and open the command prompt, then change directories to the location of your volatility exe.
4. Volatility is a powerful memory analysis tool, but as it is command line based we will have to use correctly formatted syntax – to cut down on errors the commands are supplied. The first command will deal with determining the type of OS that was running on the evidence memory capture (assuming we were not told or did not make note of it at the time of capture).
5. Run the following commands against the Joshua memory capture:
   1. **Find the profiles with imageinfo**

***volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem imageinfo***

* + 1. **What are the first and last suggested profiles?**
    2. **How many processors were running on this machine?**
  1. **Be certain of the correct profile, using kernel debugger scan option.**

***volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile=Win7SP1x64\_23418 kdbgscan***

**In this case, using the incorrect profile Win2008R2SP0 will yield similar results. However an inexact match would not process correctly and we’d see no processes.**

**How many processes are listed under PsActiveProcessHead?**

* 1. **Find an active user program with pslist.**

***volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile=Win7SP1x64\_23418 pslist***

* + 1. **Which one of the following were running: calc, notepad, paint?**
  1. **Find an unique user with access to that process with getsids. This output will be significant so redirect the output to a text file.**

***volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile=Win7SP1x64\_23418 getsids > sids.txt.***

* + 1. **Open the file. Apart from standard system or windows accounts, was any uniquely named user account associated with notepad?**
  1. **Using symbolic links, we can determine disks present on the system. This output will be significant so redirect the output to a text file.**

***volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile= Win7SP1x64\_23418 symlinkscan > symlink.txt***

* + 1. **Open the file. Search for a link to determine which disk is associated with the “C:” drive. Also, what volumes are located on the parent disk of “C:”?**
  1. **Identify registry information.**

**Windows information *volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile= Win7SP1x64\_23418 printkey -K “Software\Microsoft\Windows NT\CurrentVersion”***

**Get the hives *volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile= Win7SP1x64\_23418 hivelist***

* + 1. **What is the offset (virtual) for the System hive? You will need this for the next question.**
  1. **See how you traverse the in-memory registry, *volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile=Win7SP1x64 printkey -o [hive offset]***

**Because the USB key we want is normally under CurrentControlSet, but that key is a link to another key, listing *volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile=Win7SP1x64 printkey -o [hive offset] -K "CurrentControlSet "* will show the path to which key we want. In this case, the ControlSet001.**

***volatility\_2.6\_win64\_standalone.exe -f joshua1.vmem --profile=Win7SP1x64 printkey -o [hive offset]-K "ControlSet001\Enum\USB"***

* 1. **The previous command shows a list of Vendor ID’s. You can add them to the -K statement in double quotes to continue down the tree.** 
     1. **What is the VID for the Bluetooth Device?**

1. Once this is complete, have a look at the FTK tab “Volatile” and identify what items you might find useful for further exploring in Volatility. Hash the memory file and determine if you have caused any changes. Use the answers in you TXT and your screen captures to write **a SANS style forensics report**.
2. Once you have completed your report and provided to Renee` via canvas for grading, please remove the memory capture from the local machine. You may delete your lab files folder as well if you have a copy to provide to Renee`.