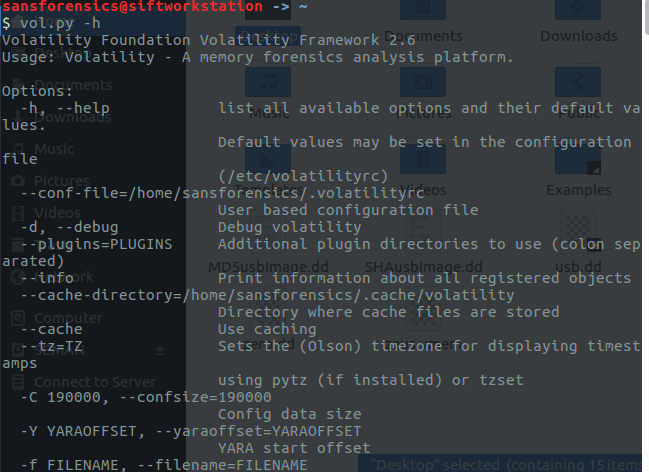
Lab 3: Marco Seman and Jason Lu

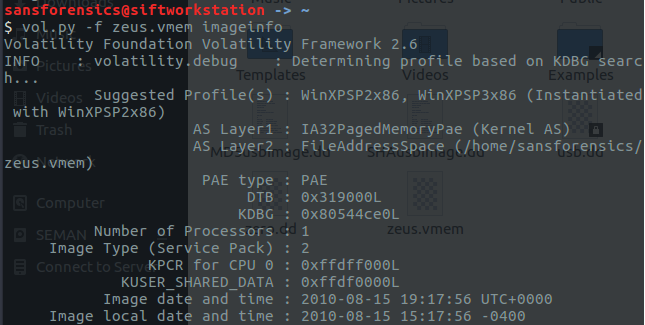
ACTIVITY #1:

Run vol.py –h to see volatility’s options and plugins.

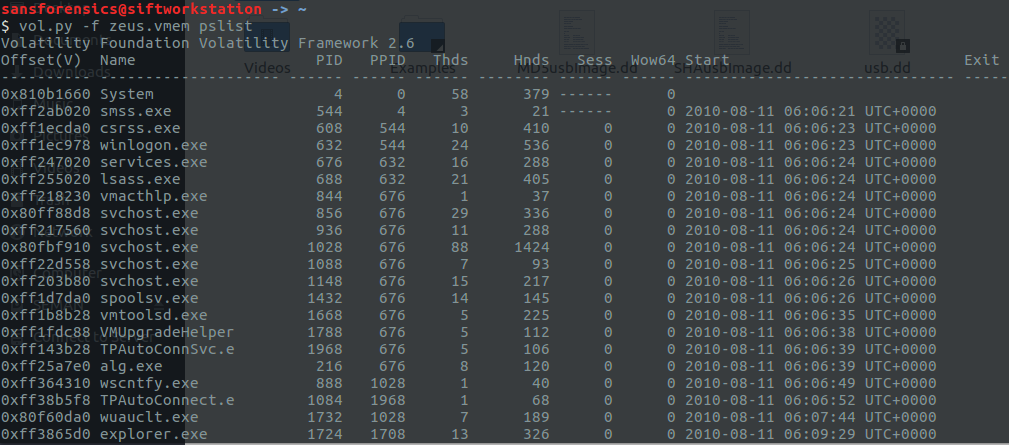


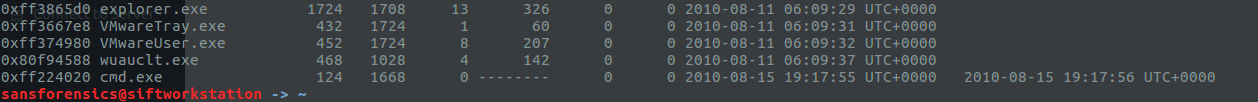
Practice these basic plugins to understand how you can use the result for your investigation. For example, vol.py –f zeus.vmem imageinfo

Imageinfo:Shows basic system information such as type of OS

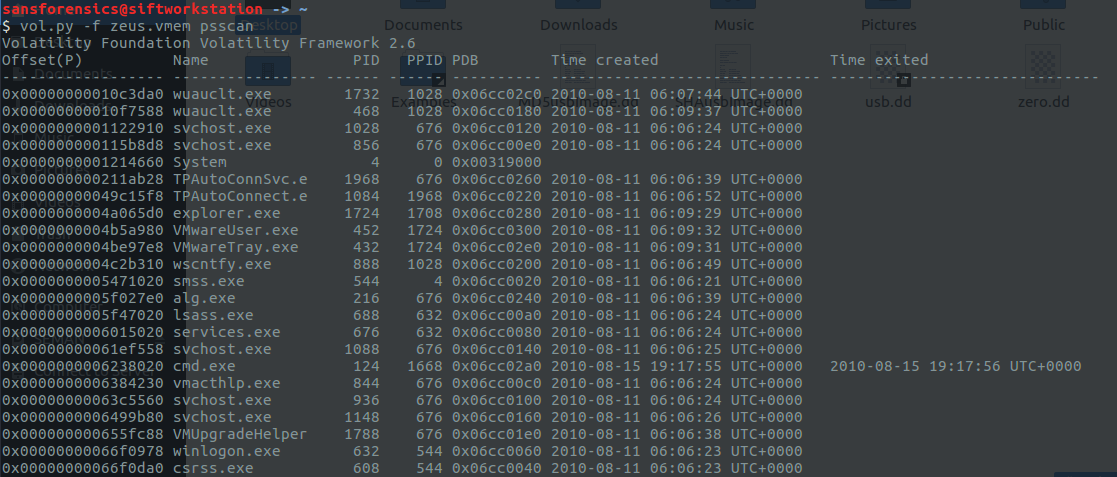


Pslist: Lists the processes of a system

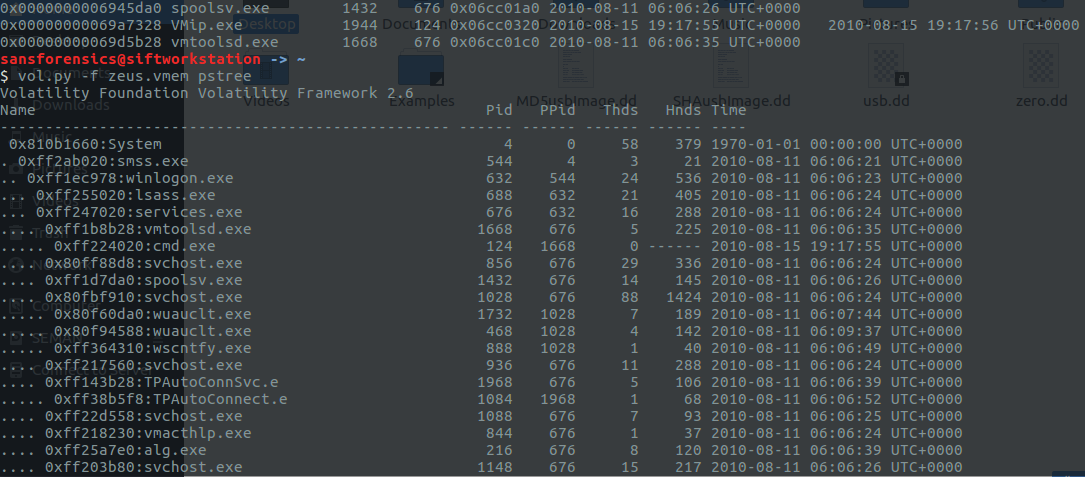




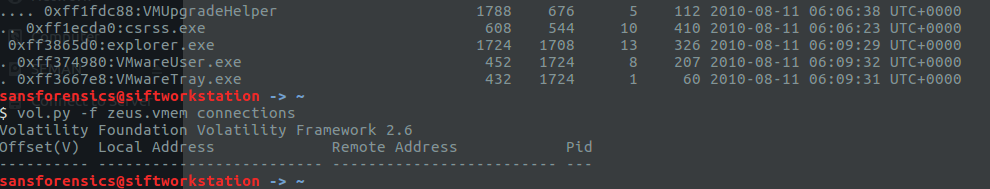
Psscan: Finds processes that previously terminated (inactive) and processes that have been hidden or unlinked by a rootkit



Pstree: Displays the process listing in tree form

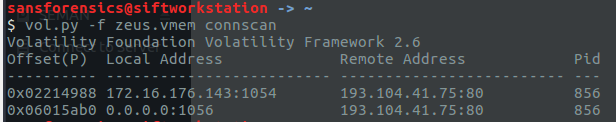


Connections: Shows the TCP connections that were active at the time of the memory acquisition



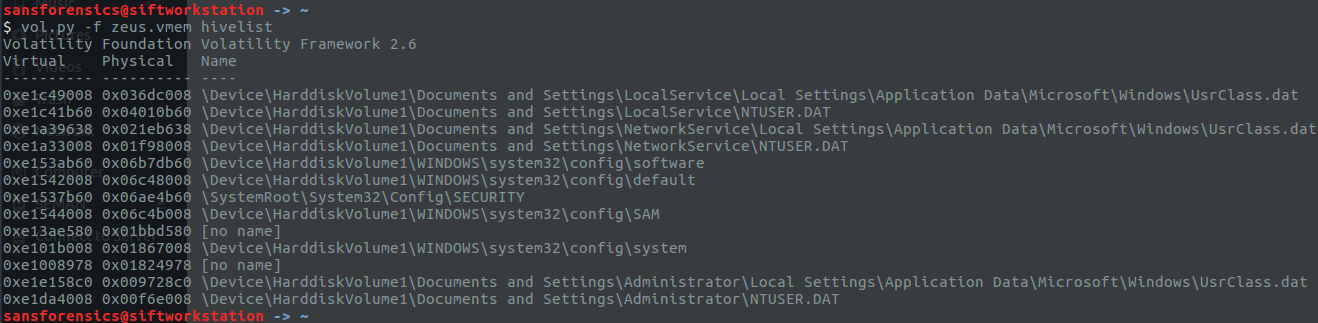
Connscan: Extracts TCP connections that were active at the time of the memory acquisition

and previous connections that have since been terminated.

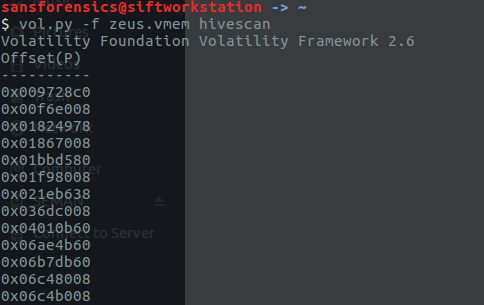


Hivelist: Locates the virtual addresses of registry hives in memory and the full paths to the

corresponding hive on disk

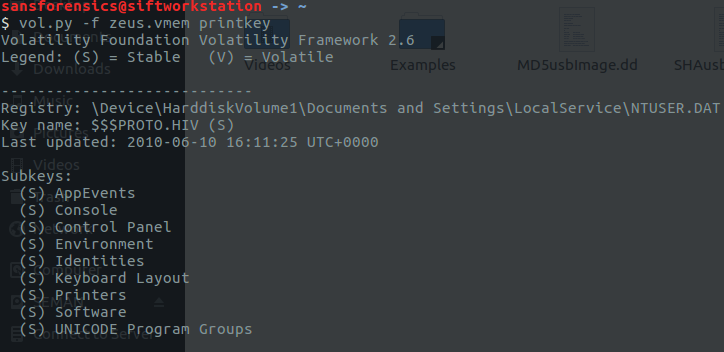


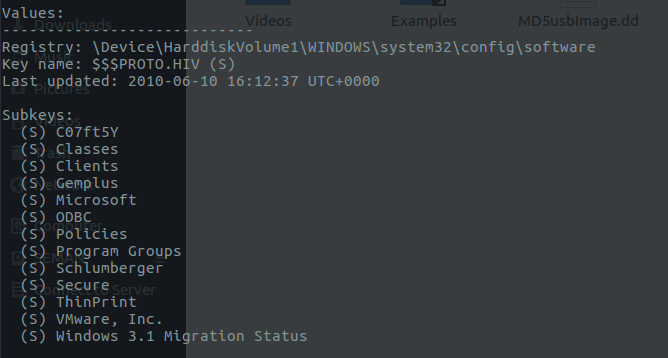
hivescan: Displays the physical addresses of registry hives in memory

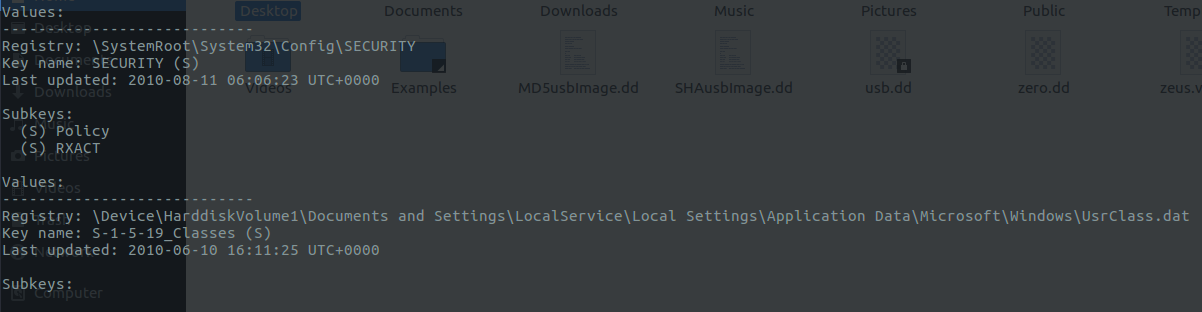


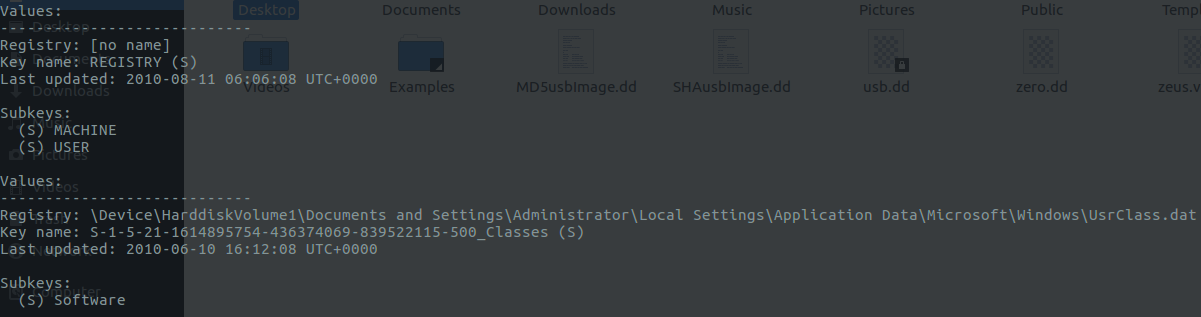
printkey: Displays the subkeys, values, data, and data types contained within a specified

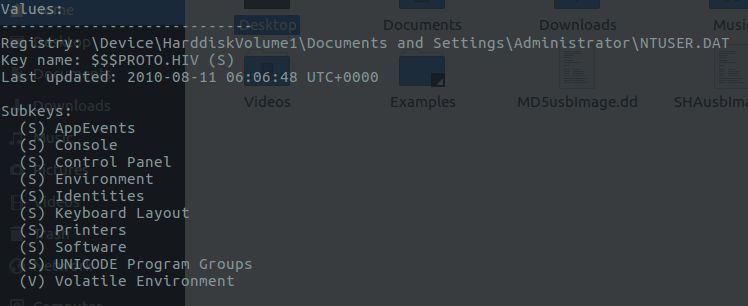
registry key

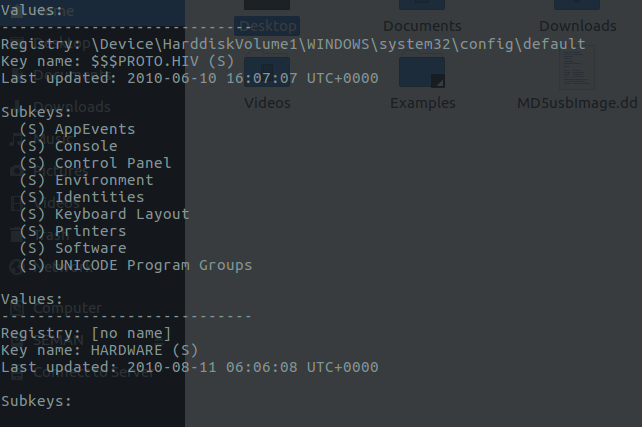


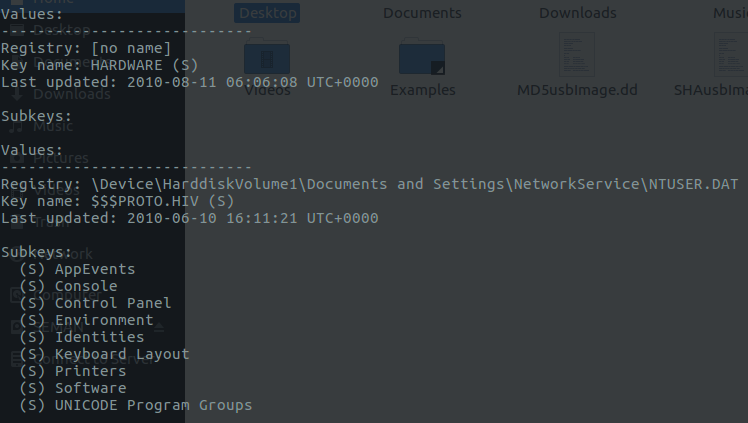


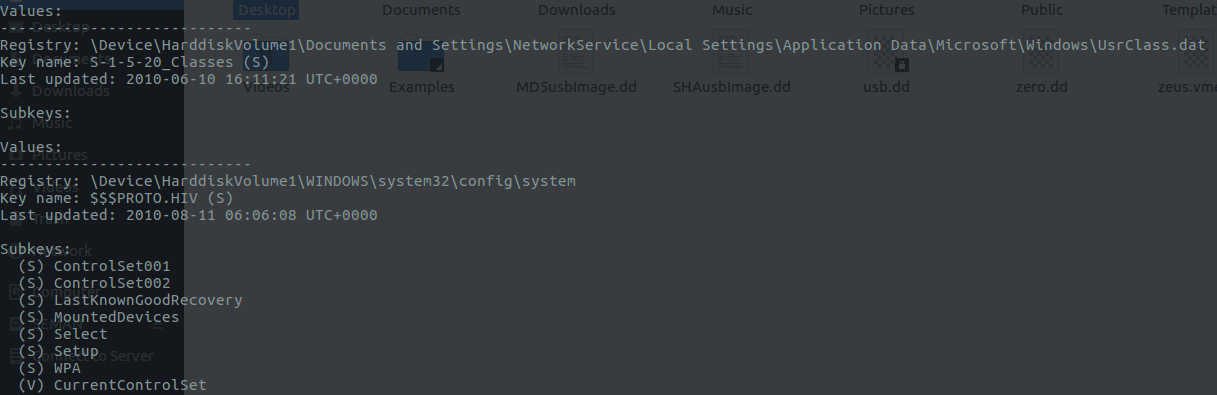


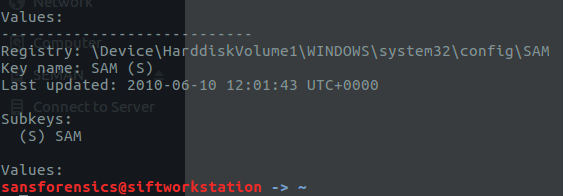












For our third lab, we learned how to run and view a malware called Zeus which is a forensics analyst tool used to extract information from RAM. In our first lesson, we learned how to view the information of the systems such as number of processors(1), and type of image (service pack) 2. For plist, psscan, and pstree, we learned what the OS is processing along with their ID and time it started/created. For the connscan, we learned how to extract TCP connections from the time the memory was running along with the previous connections that were running. For the hivelist and hive scan we learned how to view the memories registry key along with the full path the full locations on the disk. The printkey function was the most interesting command where it revealed the information within a registry key which included subkey, values, data types, and data.