**CIS-387: Digital Forensics (4 credits)**

**With Dr. Jinhua Guo**

**Lab 3**

**Demetrius Johnson**

**October 05, 2022**

# ACTIVITY 1: PRACTICING VOLITILITY (vol.py program)

## 1) Run vol.py -h to see volatility’s options

Text

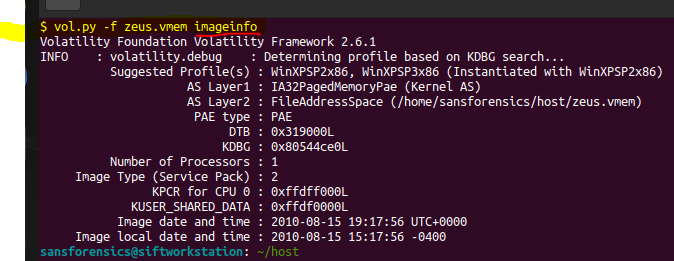
Description automatically generated

* Above, showing some of the options of vol.py command line program.

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

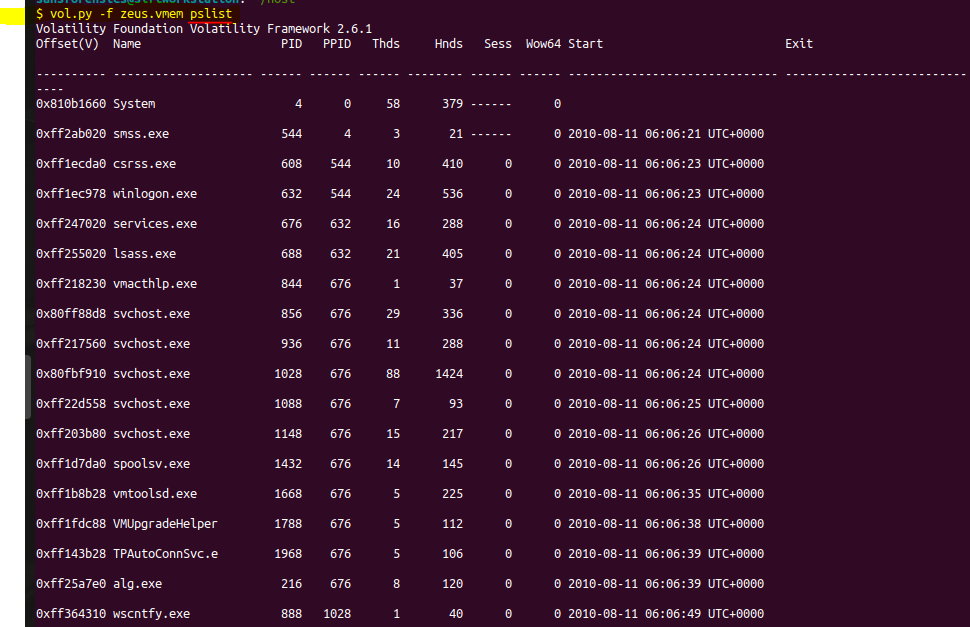
### **imageinfo**

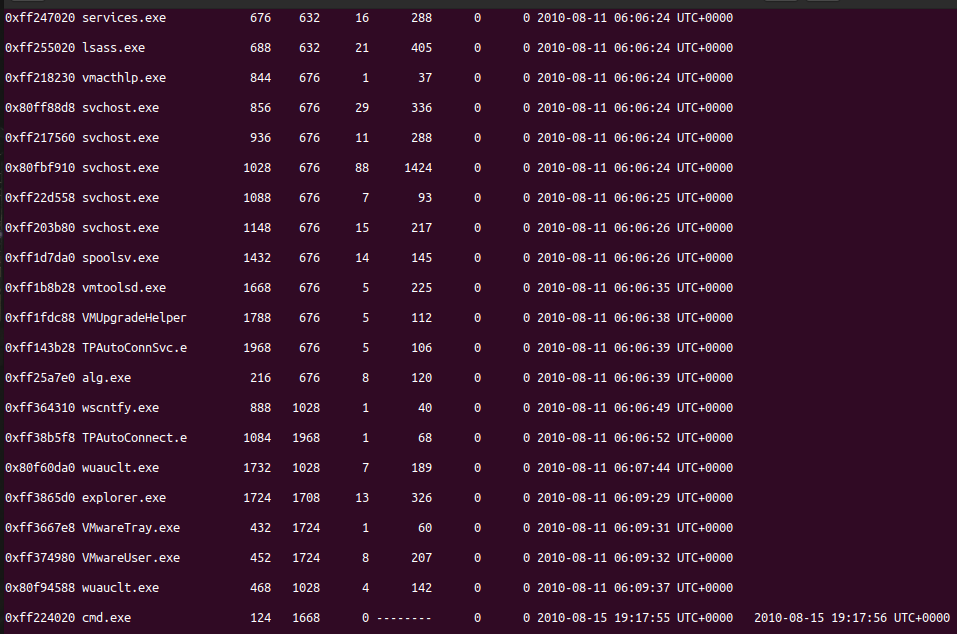
Shows basic system information such as type of OS.



### **pslist**

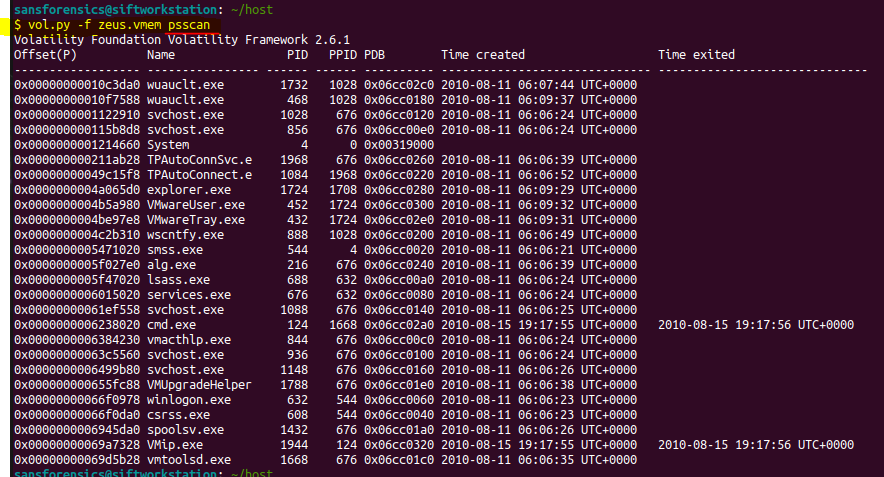
Lists the processes of a system.





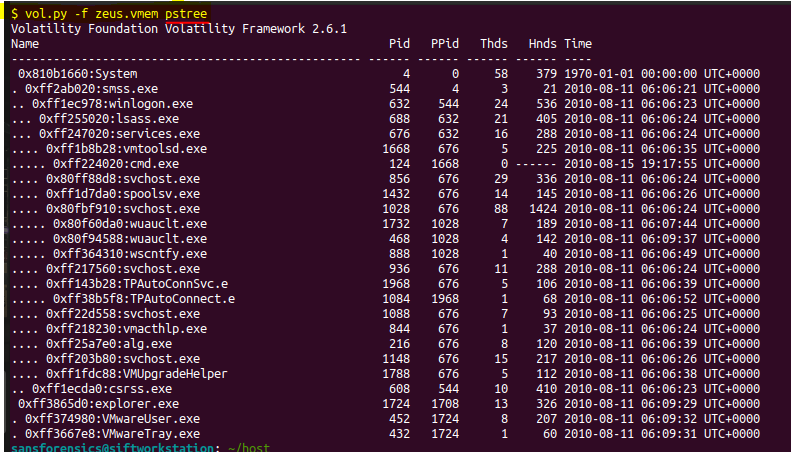
### **psscan**

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



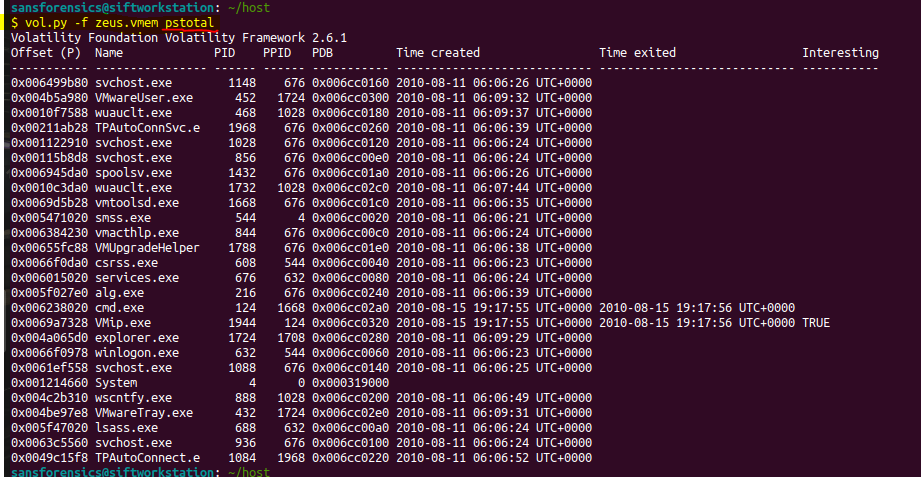
### **pstree**

Displays the process listing in tree form connections Shows the TCP connections that were active at the time of the memory acquisition.



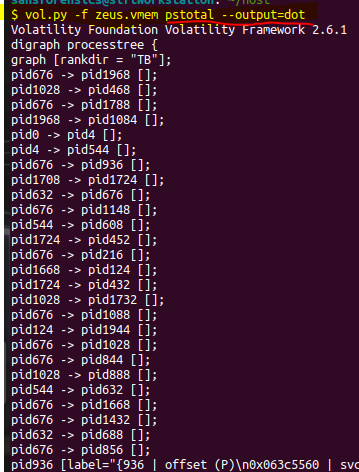
### pstotal (I did this optional command so that I can analyze easier)

Outputs a combination of pslist, psscan, and pstree.



### pstotal --output=dot (I did this optional command so that I can analyze easier)

Outputs a combination of pslist, psscan, and pstree in a graphical way.



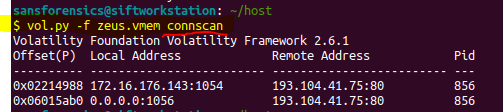






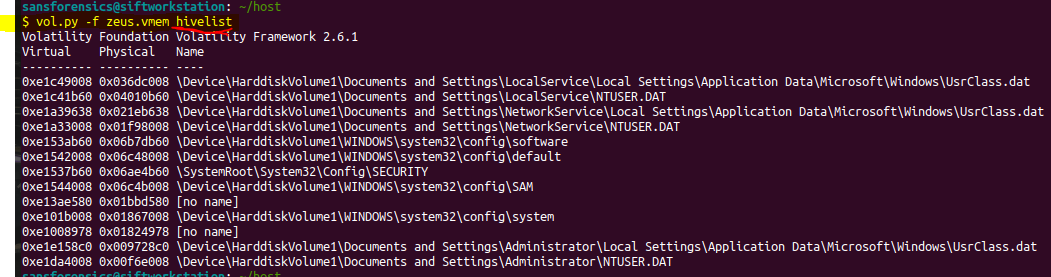
### **connscan**

Extracts TCP connections that were active at the time of the memory acquisition and previous connections that have since been terminated.



### **hivelist**

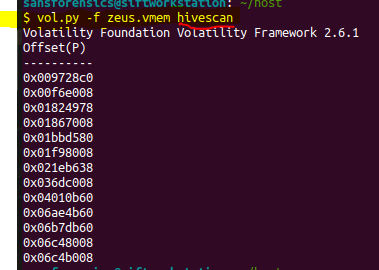
Locates the virtual addresses of registry hives in memory and the full paths to the corresponding hive on disk.



* I notice that above there are two registry hives in memory that have no name/path.

### **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 example:

**vol.py -f zeus.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\winlogon"**

Text

Description automatically generated

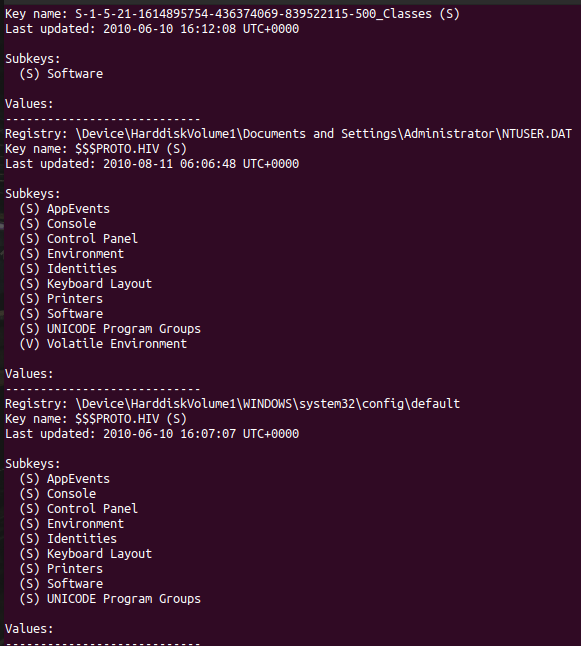
#### now I will run printkey for all registry locations on the zues.vmem image file:

Text

Description automatically generated

Text

Description automatically generated



Text

Description automatically generated

Text

Description automatically generated

# Summary/Reflection

The system is possibly compromised because of the svchost.exe. I found that it has multiple processes running, but it is a part of services.exe as a parent process – so perhaps this is normal. I also found that svchost.exe has a TCP connection on port 80 (HTTP), which is typically a protocol used by web browser applications, which svchost.exe is not a web browser application. Lastly, I notice that one of the svchost.exe processes has 1400+ handles, meaning that it is using 1400+ system resources (files, libraries, other binaries and streams…etc.), meaning that it could be a process that is spying, and sending and receiving data about other processes on the machine.