Volatility Exercises

Sample memory images:
https://umd.box.com/s/8owf6xk9a9ma51hqcvwnn4s8hqz9ppff

https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples’

Volatility is installed as part of SIFT and you can run with “vol.py”

You can also clone it with git: git clone https://github.com/volatilityfoundation/volatility.git

Standalone executables are also available to download from
http://www.volatilityfoundation.org/26

Command reference guide: run “vol.py –info” or see:
https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

Typical command arguments:

```
vol.py –f <filename> --profile <Profile> <pluginname> <pluginoptions>
```

<filename> = file location of the memory dump
<Profile> = a profile of an Operating System’s memory to extract information against (ex: “Win7SP0x64”)
<pluginname> = plugin to extract some sort of data from (ex: pslist to list processes)
<pluginoptins> = optional features of that plugin (ex: save results to a file/directory)

For the most part the order of the command arguments have no specific order so you can move them around. You can also specify custom plugins in a different directory with “—plugins=/path/to/plugins” or “—plugins=C:\location\of\zipefile.zip”

Examples:

```
vol.py -f memdump.mem imageinfo
```

```
vol.py –f memdump.mem --profile=Win7SP0x64 dumpfiles --dump-dir=/tmp/dump -S /tmp/dump/results.txt
```

```
vol.py -f memdump.mem --profile=Win7SP0x64 iehistory
```

```
vol.py -f memdump.mem --profile=Win7SP0x64 hashdump
```

```
vol.py -f memdump.mem --profile=Win7SP0x64 lsadump
```