We will go over this topic in the next class video lecture so don't worry if it seems overwhelming at the moment. (This is for video lectures 3 & 4)

You have been given a memory dump (hw2.mem) from a system that is suspected to have malware on it.  The memory dump is available here: https://umd.box.com/s/p6uhyf9j2sycod5z5by2yqufp3ifm2vs[(Links to an external site.)](https://umd.box.com/s/kbl5vfxptkivayfnjvmlyh94js0c1z89)

1. What was going on at the time the memory dump was taken? (What programs appeared to be running at the time the image was taken and what do you suspect about what what happening.)

2. Can you extract the malware for further analysis?  What command(s) did you run? What commands did you try that were not successful and what did those commands output?

3. What’s the malware file name?

4. What’s is the MD5 hash for it (It’s not real malware, I promise.)

Try various Volatility plugins, [https://github.com/volatilityfoundation/volatility/wiki/Command-Reference (Links to an external site.)](https://github.com/volatilityfoundation/volatility/wiki/Command-Reference) may be of help but are not required.

**\*5.**: Write a short description of what plugins you used and what you found interesting from a forensic analysis perspective(including the answers to the 4 questions above).

\*\*The plugin cheatsheet on the sift desktop can be very helpful