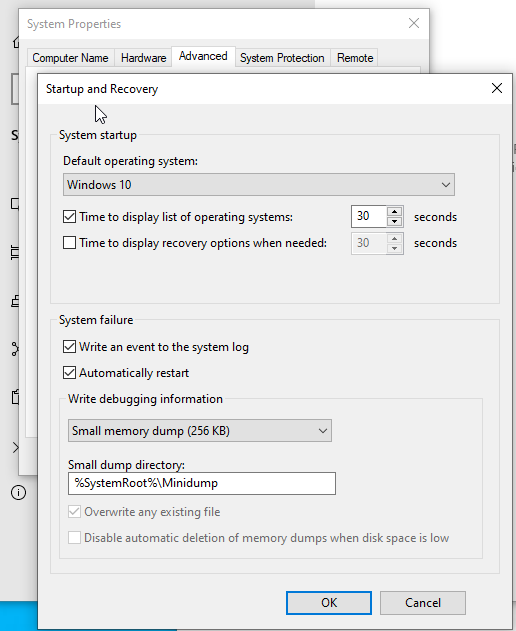
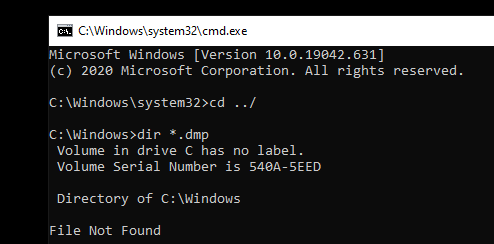
Windows Forensics

PART 1: Windows Crash Dump

Task 1:

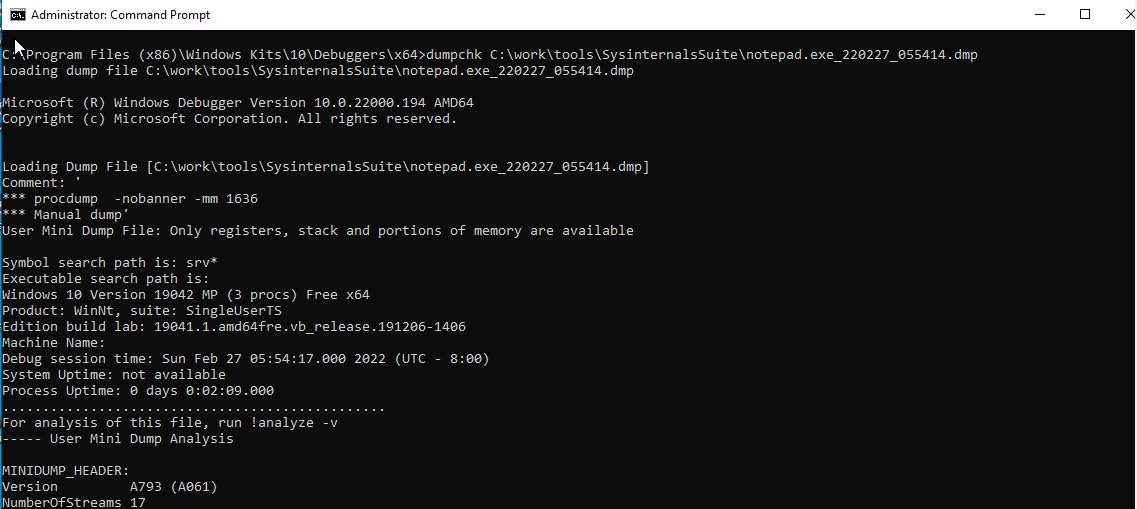
This step teaches us to create memory dump whenever window crashes so we can later investigate about the memory location, program status and other stuff.





Task 2:

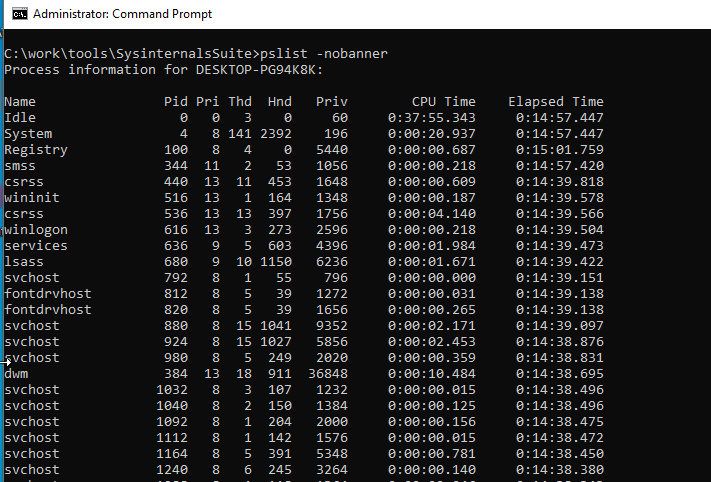
**Dumpchk** is a tool that is used to analyze the crash dump files.

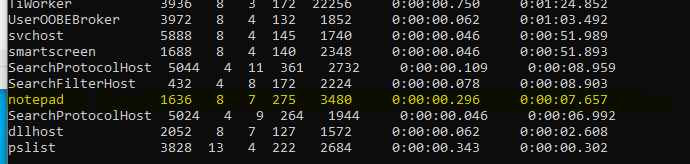


PART 2: Collecting Process Information

Task 1:

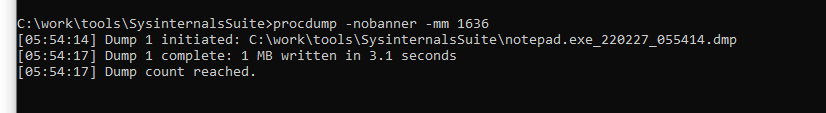
**Pslist** is a tool that is used to display information about CPU usage and the processes running on the computer





Here using **pslist** we found the **PID** of the notepad application which is **1636.**

Task 2:



***prodump*** *is a tool used to dump the memory of a particular process. We use this command “****procdump*** *-****nobanner*** *-****mm******1636****”*

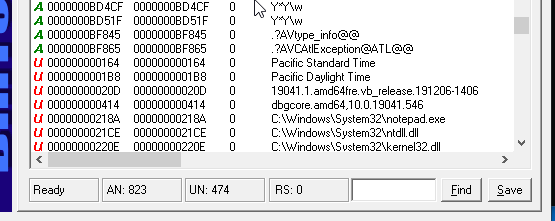
*🡪* ***procdump*** *dumps the memory*

*🡪* ***-nobanner*** *removes the banner*

*🡪* ***-mm*** *mini dump*

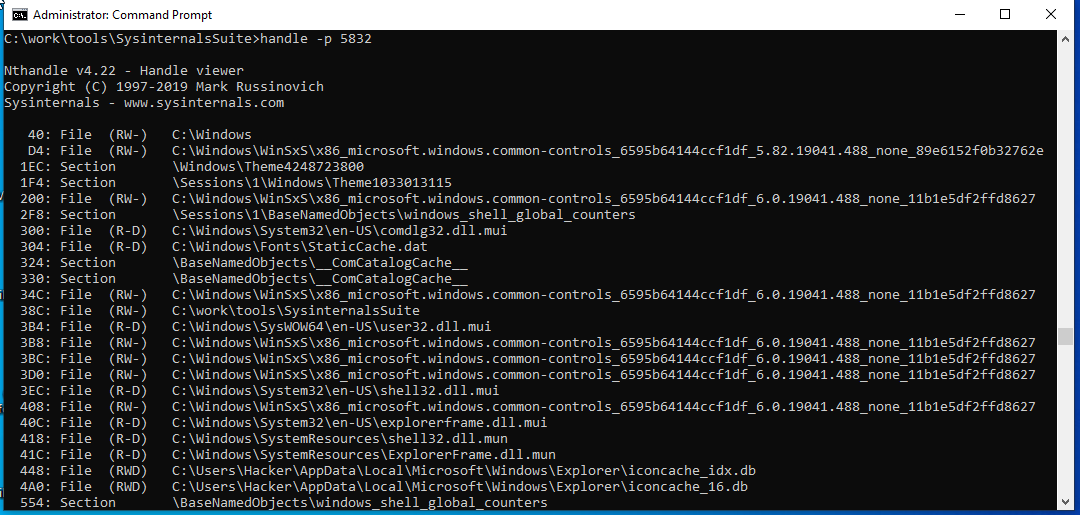
*🡪* ***1636*** *is a* ***PID (****process id)*

Task 3:



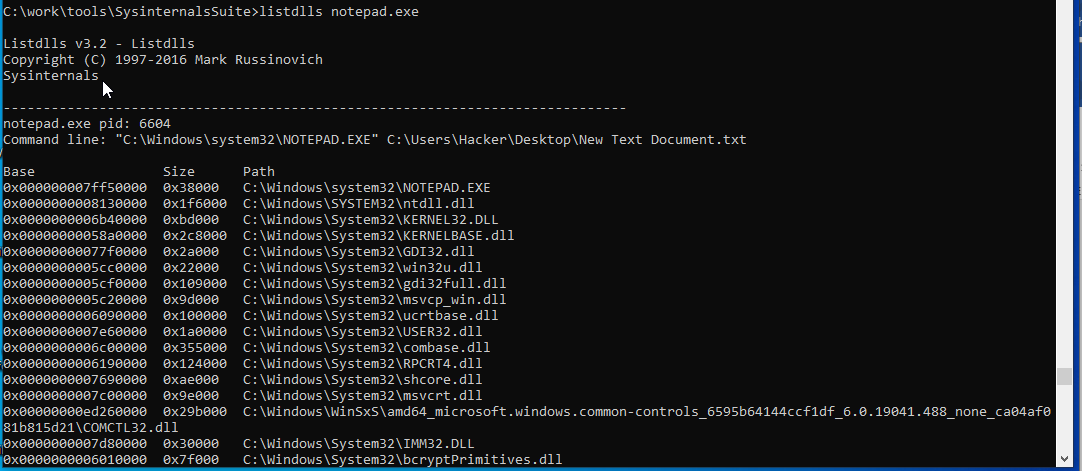
*This is* ***Bintext*** *application that reads the memory dump file that we create.*

Task 4:



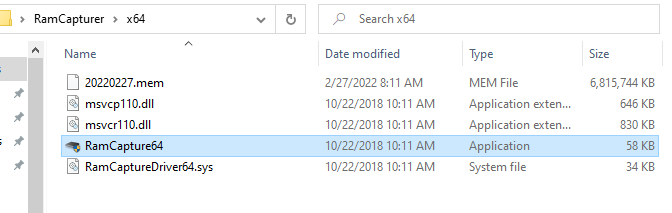
***Handlers*** *are used just like pointers and gives us dump of the open files for all the processes.*

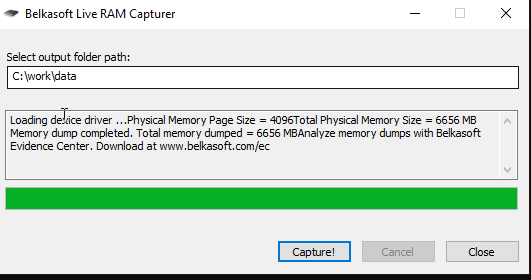
Task 5:

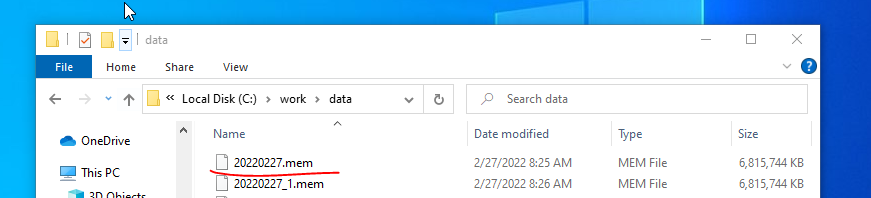


***listdll*** *is another windows utility that list all the dynamic link library that are loaded into the processes.*

PART 3: Ram Acquisition







***Ram******acquisition*** *is the process of creating an active image of the content running on the RAM and storing it into a file such as “****.mem****”*

SUMMARY

This whole lab was divided into three parts. First part taught us about the windows crash dump, it showed us how to create memory dump if our system crashes accidently. It also taught us about the tool named dumpchk that reads the memory dump file created above. Second part taught us how to use the tools pslist, procdump, Bintext, handle and listdll and retrieve the information about the memory dump or processes. Third part taught us about the ram acquisition that can be done using a software called Belkasoft. This creates a copy of content stored in the RAM so it can be investigated later.