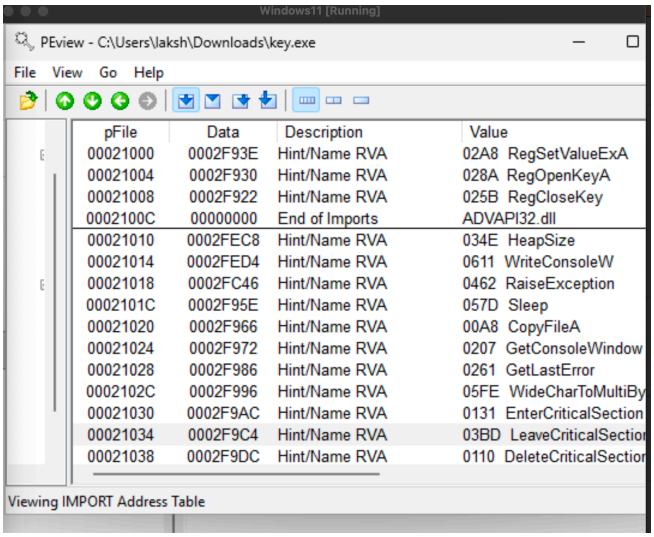
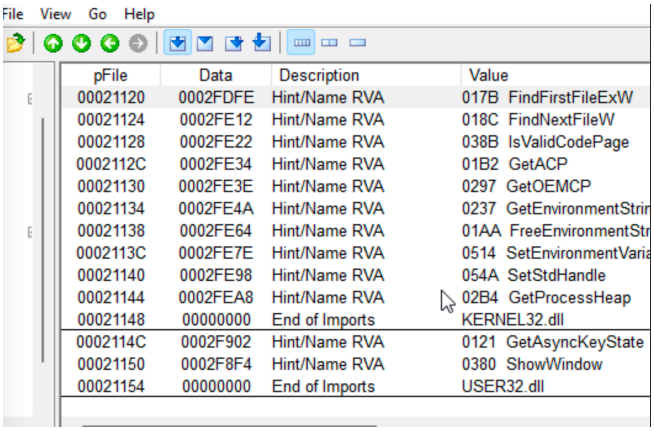
Week-9 IOT Exercise-1
Lakshminath Reddy Alamuru
SUID: 367982169

Downloading the virtual box with windows 11 which is taking time. As I have linux machine virtual box.

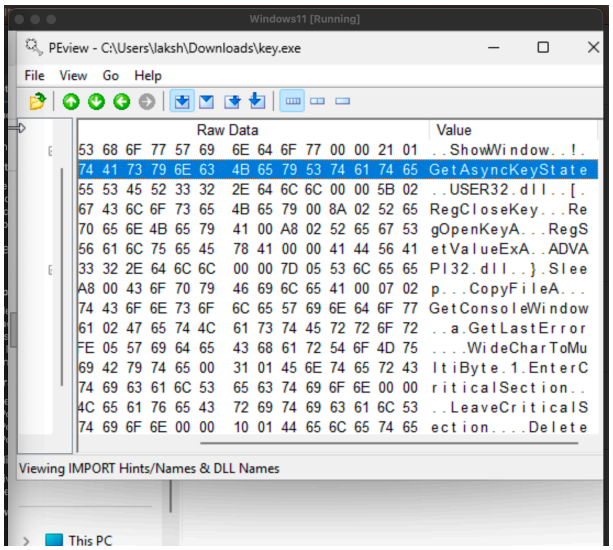
Task-1

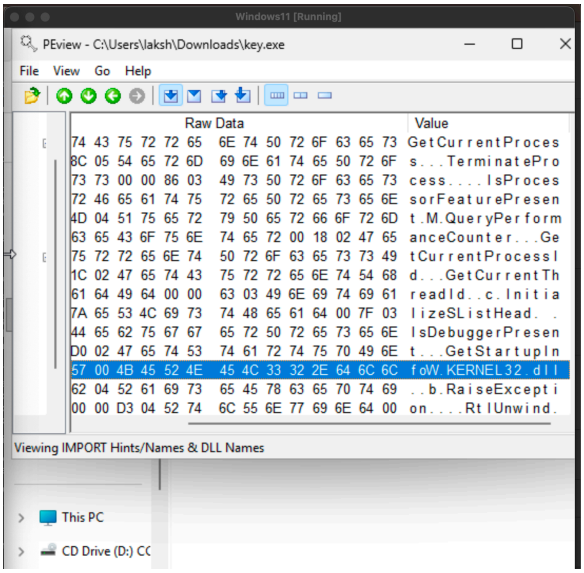
Downloaded the key.7z file and extracted the file with passwords malware.
Then opened the file from PEview and provided the screenshots after navigating to import address table in rdata section

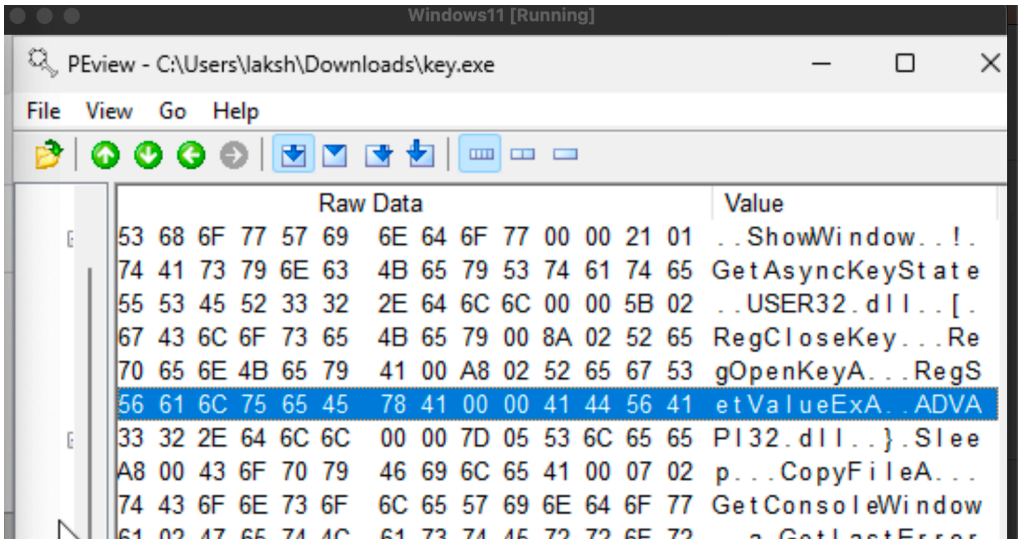




User32.dll, give the hints of getasynckeysstate, showwindow.







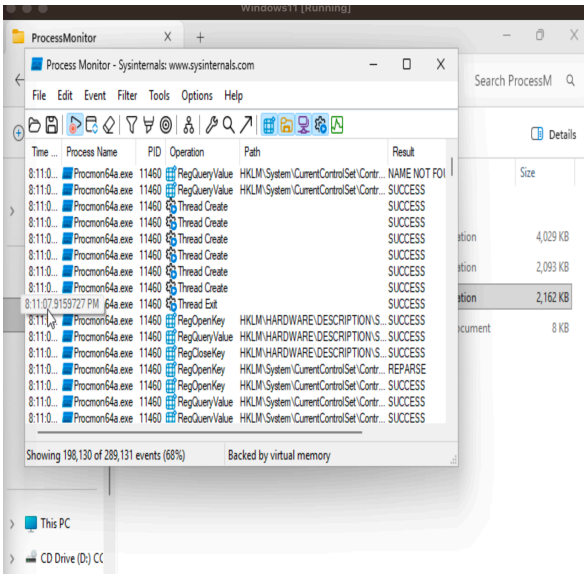
User32.dll is windows UI/input API

GetAsyncKeyState often signals key polling (possible keylogger/hotkey/anti-analysis) when called repeatedly in tight loops and followed by writes or network send.
ShowWindow manipulates window visibility (e.g., SW_HIDE)

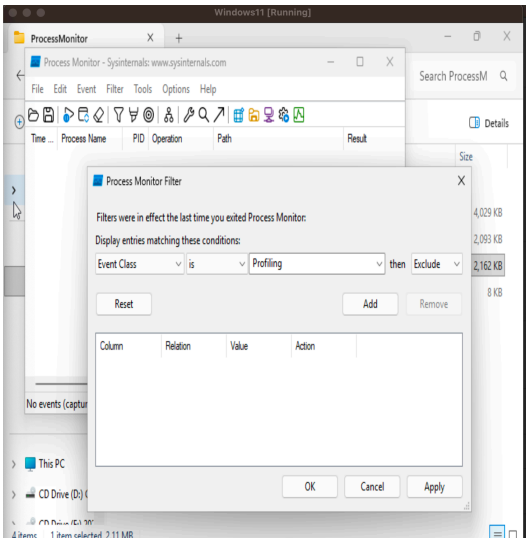
ADVAPI32.dll gives regopenkey, regclosekey
Kernel.dll gives getprocessheap , setstdhandle which is more about the kernel related hints that can provide.

Task-2

I have downloaded the application for process monitor.



I have removed all the processes, and showed the screenshot below



Learnings:

Got the greater understanding on the PEview, process monitor application. Which gave me the better understanding on the dynamic malware analysis.