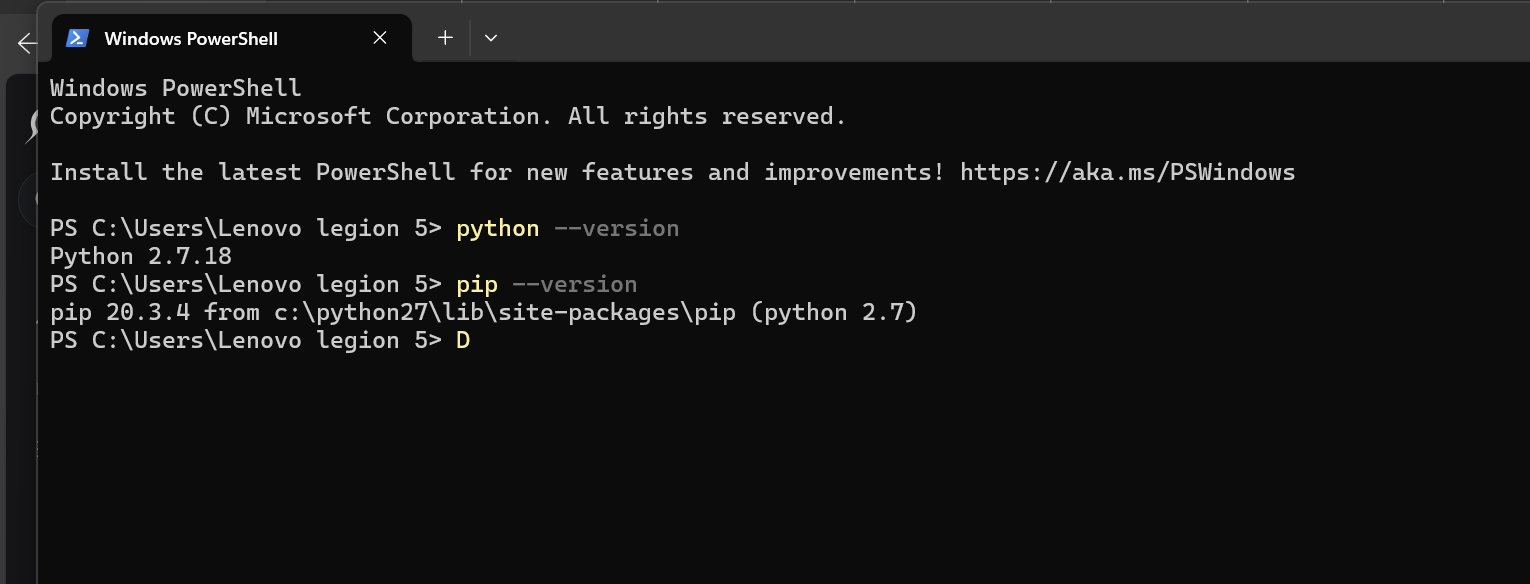
**NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302**

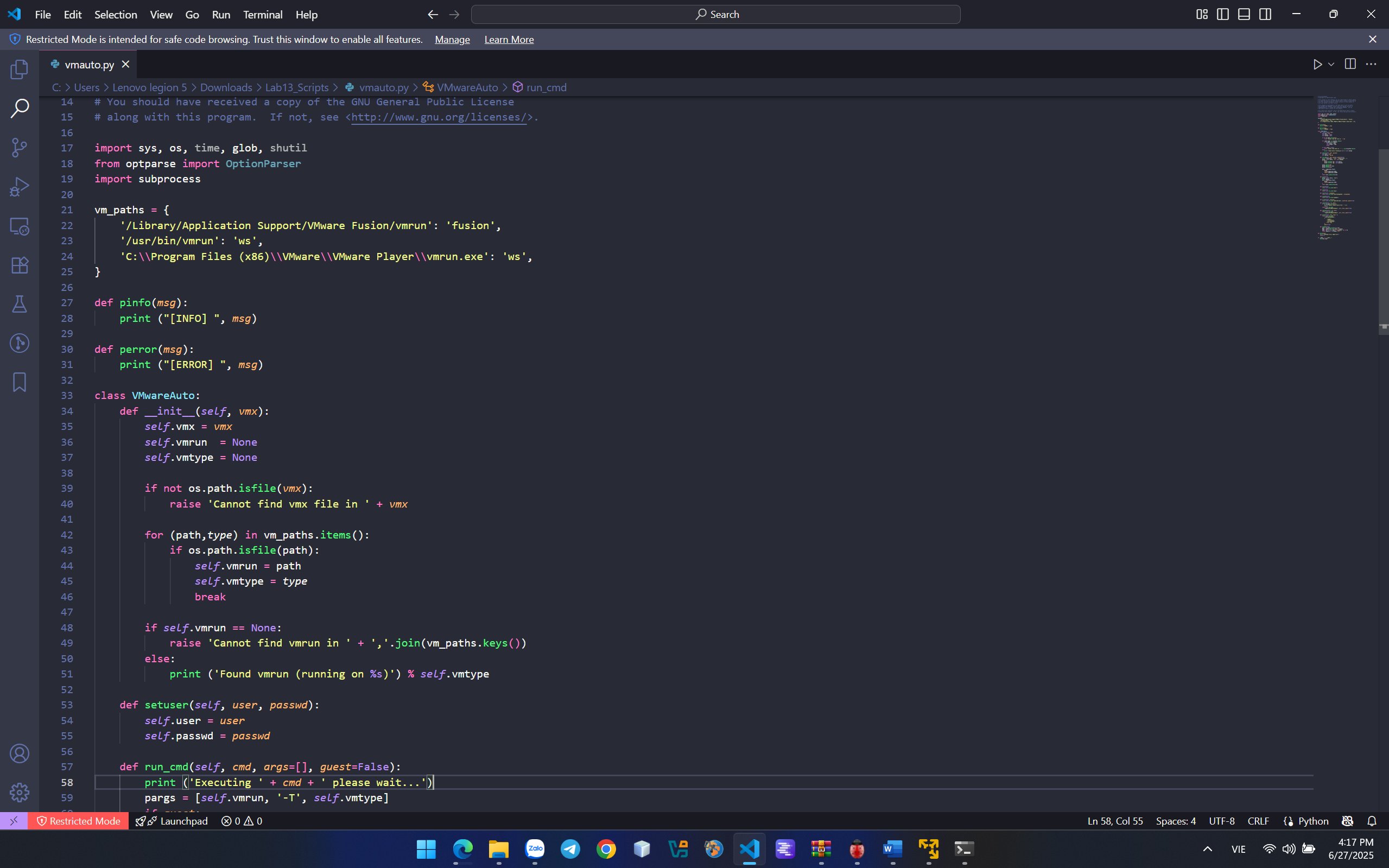
**LAB 13:**

Automated Malware Analysis VMWARE Steps:

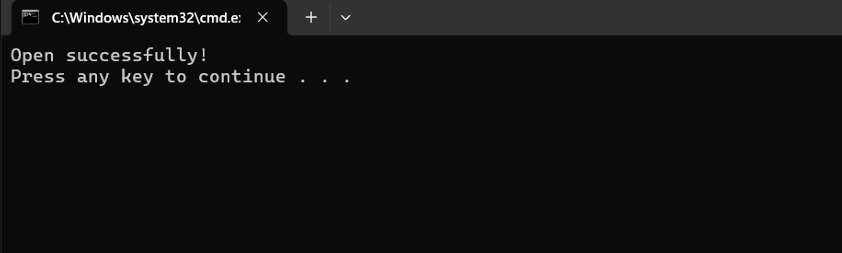
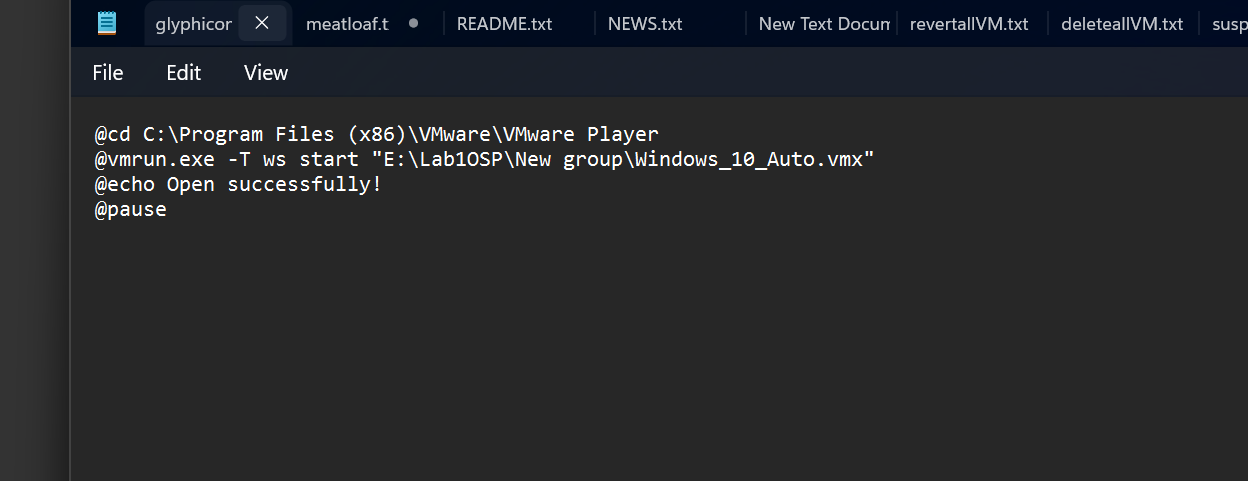
Setting python and pip:

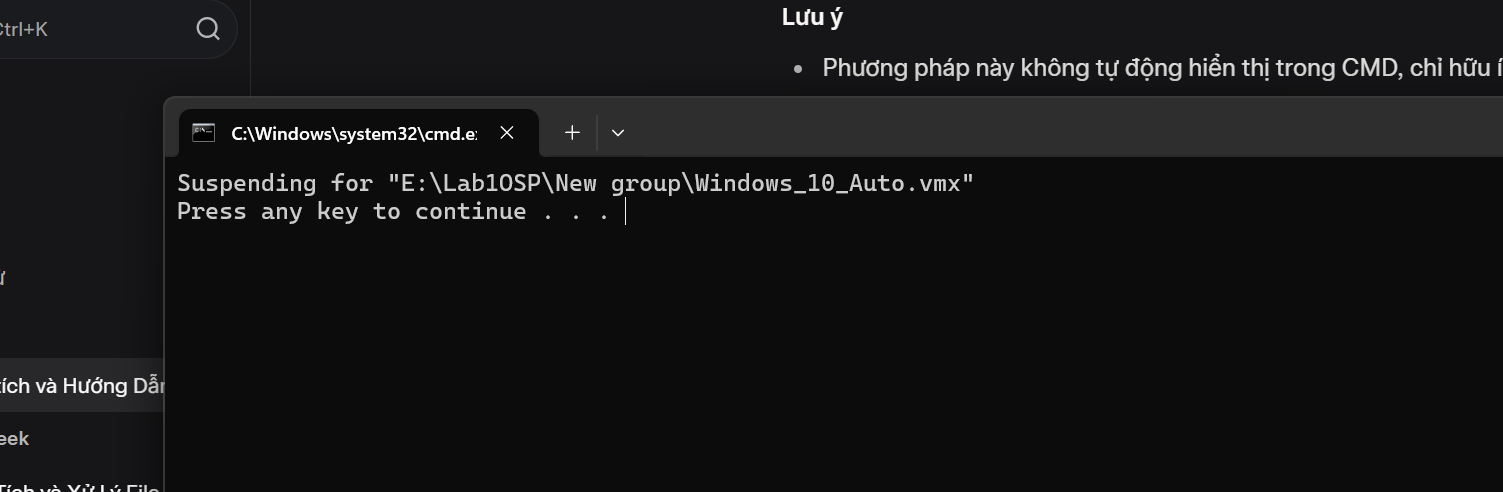
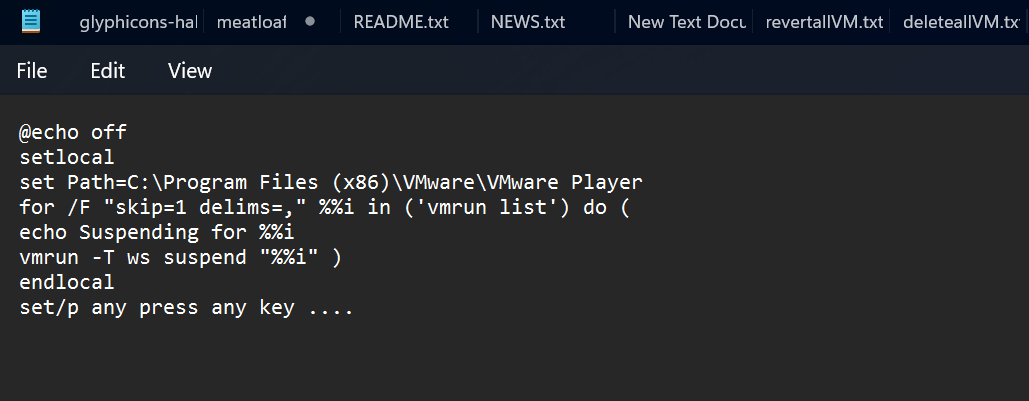


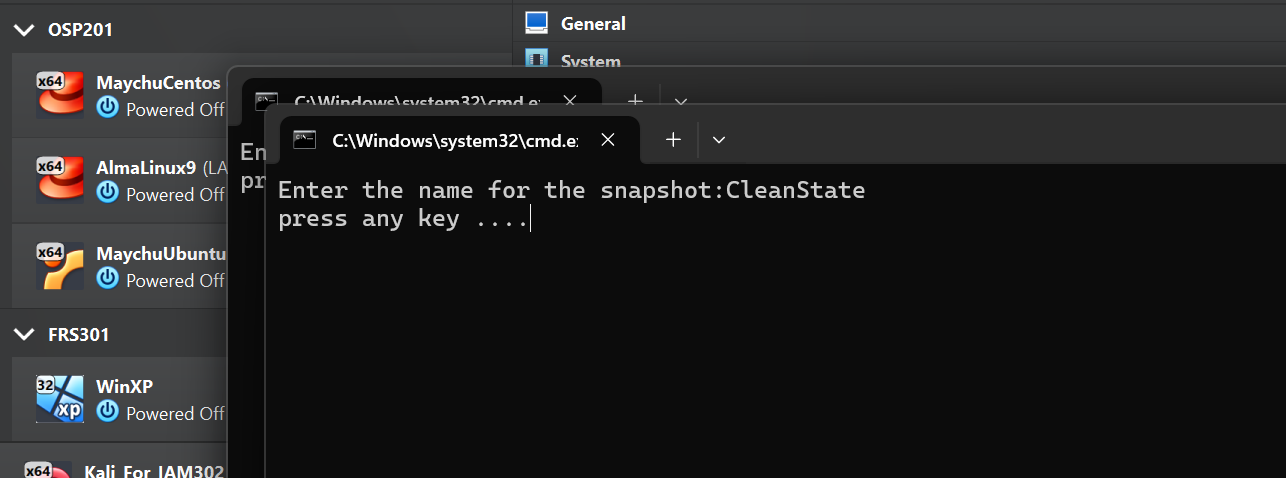
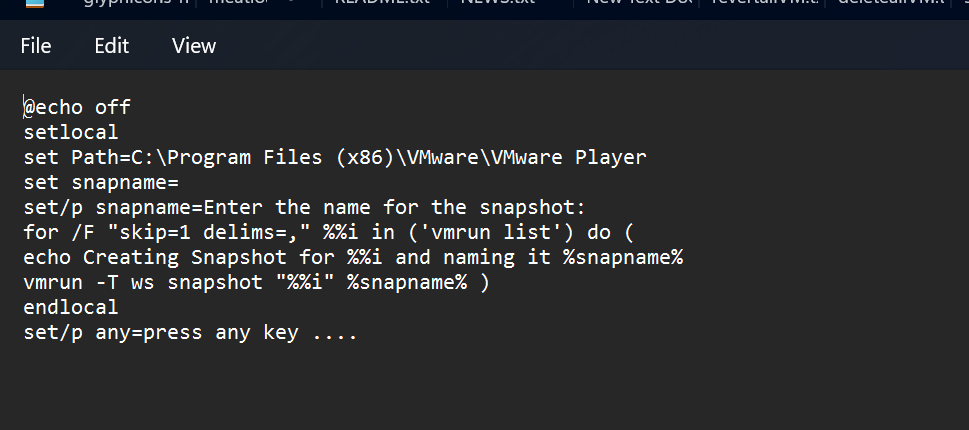
Content of vmauto.py

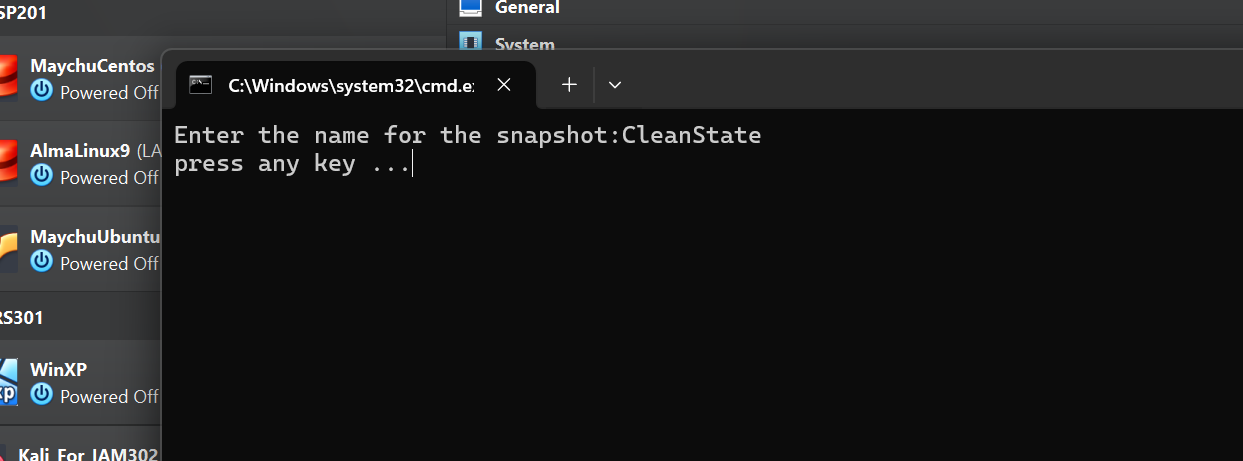
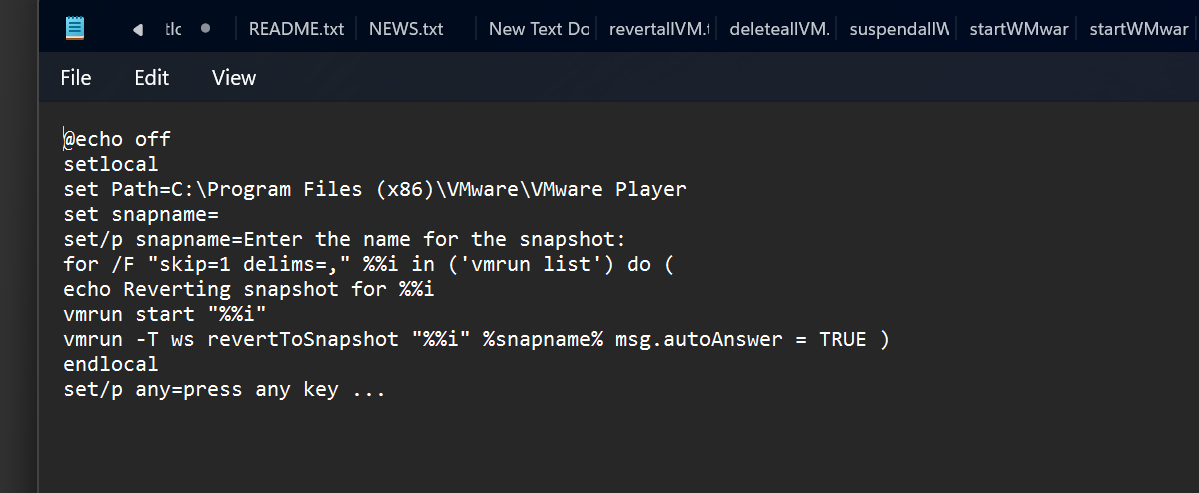


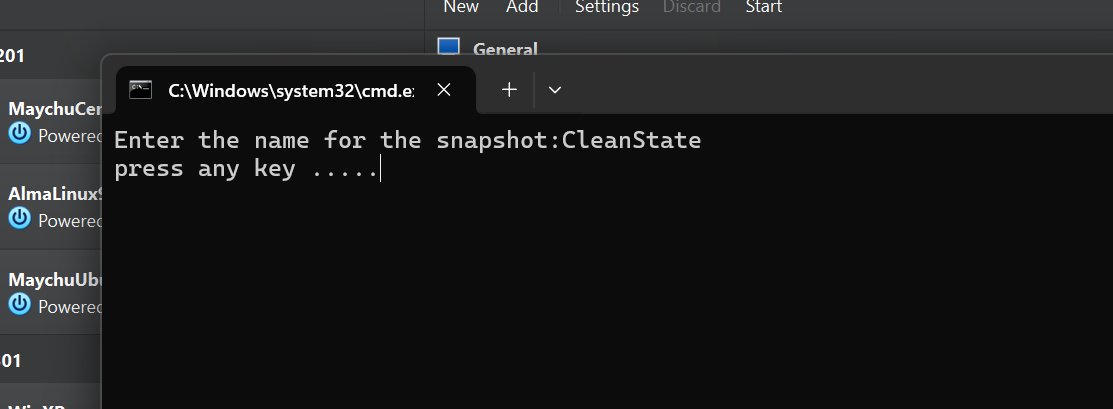
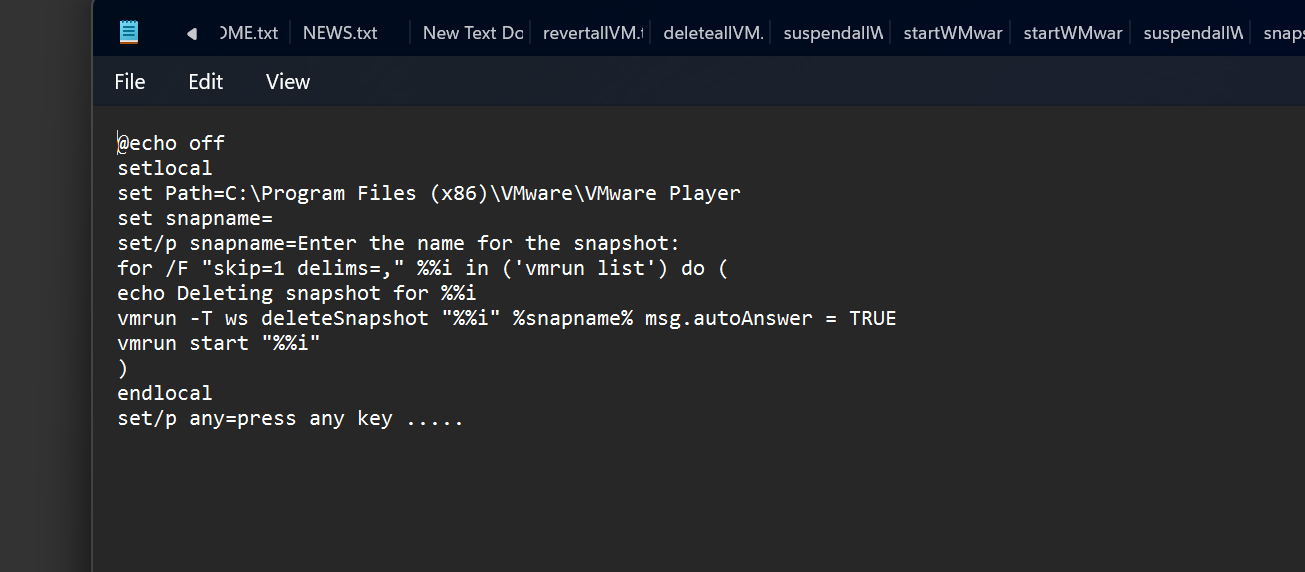
Create script to turn on Windows 10 virtual machine in Vmware.



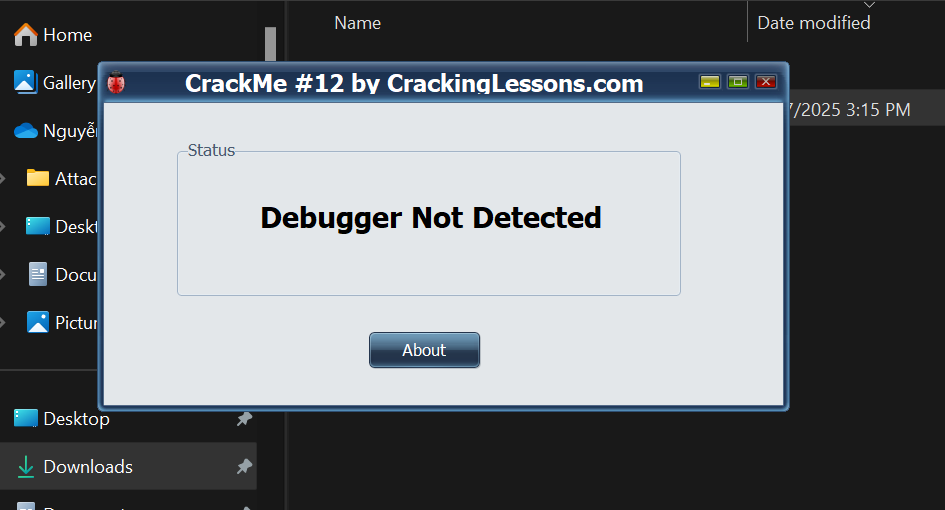
Create a script to suspend all virtual machines running on VMware. 

Create a script to create snapshots for virtual machines running on VMware. 

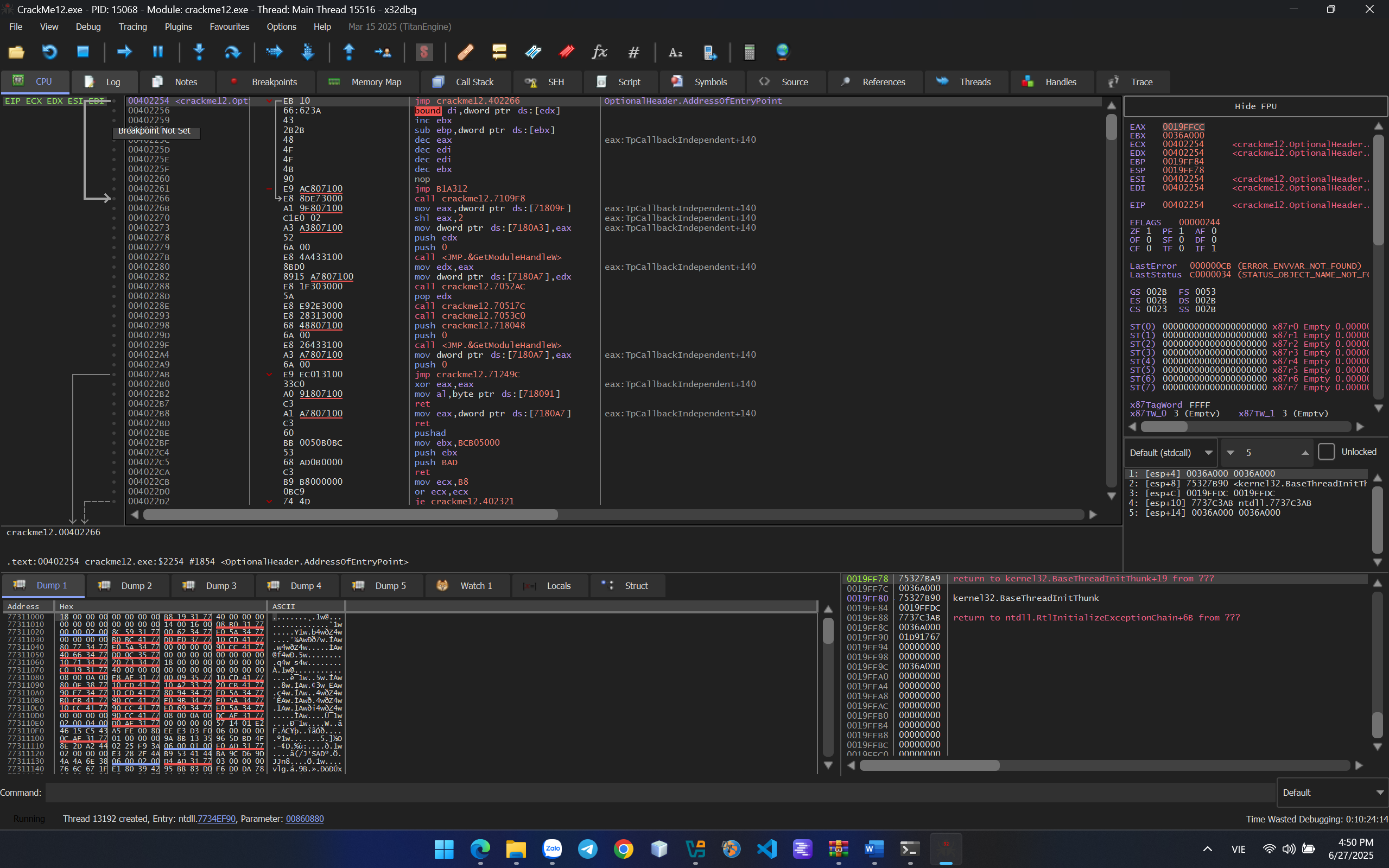
Create a script to revert all snapshots for virtual machines running on VMware. 

Create a script to delete newly created snapshot files from the above script

**CrackMe #12**

This CrackMe has Anti-Debugging features. If you open it with a debugger and then run, it will detect the debugger and exit. Your task is to bypass the anti-debugging feature, so that the program will continue to run and show the window below:

Open in x32dbg and press F9 to run, but nothing appeared. May be this program has anti debugger so it didn’t run in x32dbg tools.

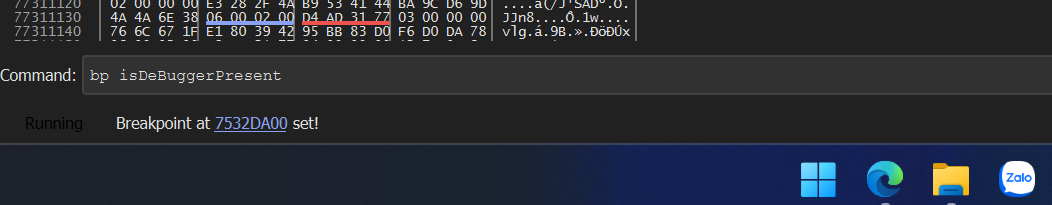


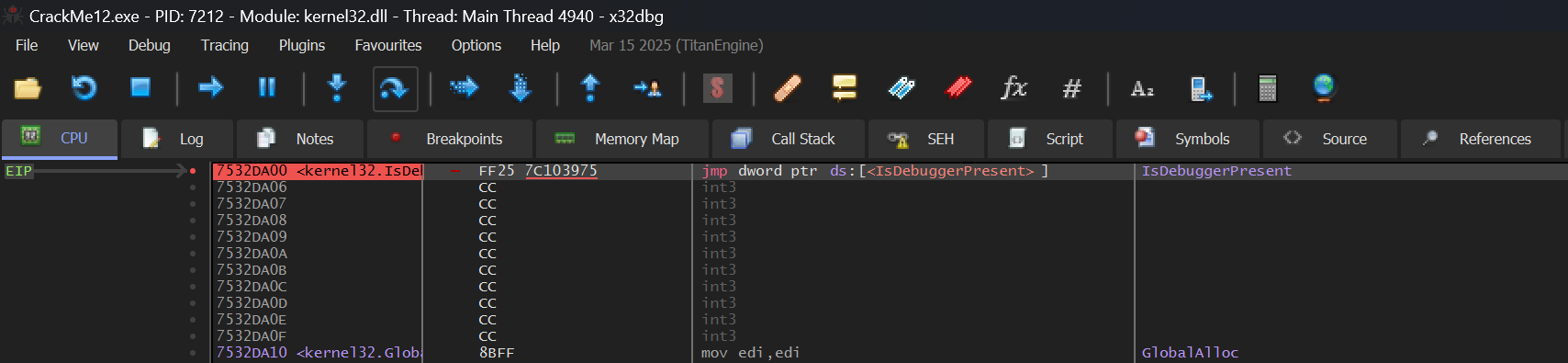
To avoid anti-debugging, people came up with anti-anti-debugging, and there are 2 commonly used methods for it to work: setting breakpoints on anti-debugging APIs or use anti-anti-debugging plugins.

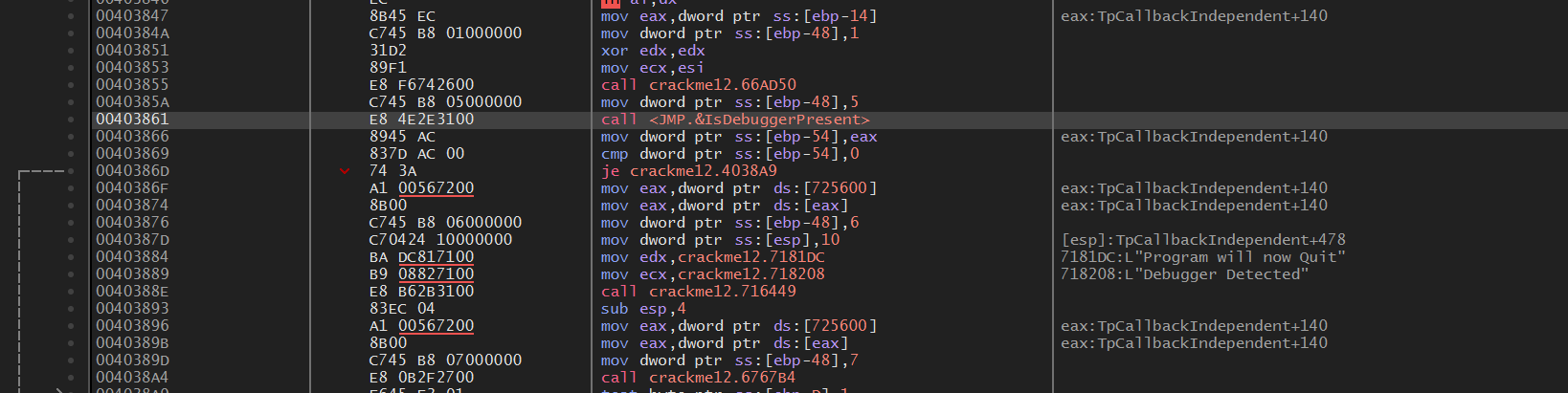
I will follow the way setting breakpoint API anti-debugging

Set a breakpoint on the isDebuggerPresent() function to prevent the program from terminating immediately when clicking run.

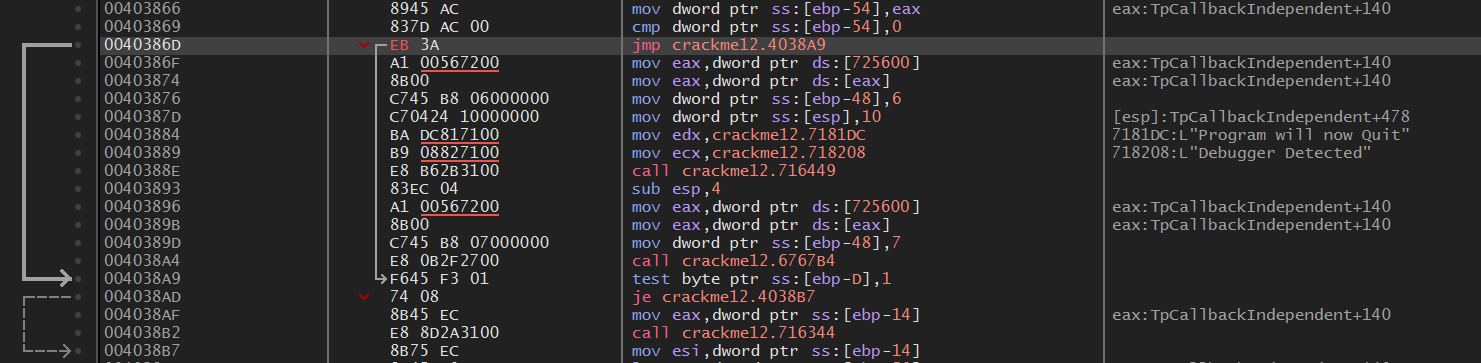
*Note: The isDebuggerPresent() function is the most commonly used API to check whether a program is running with a debugger or not.*

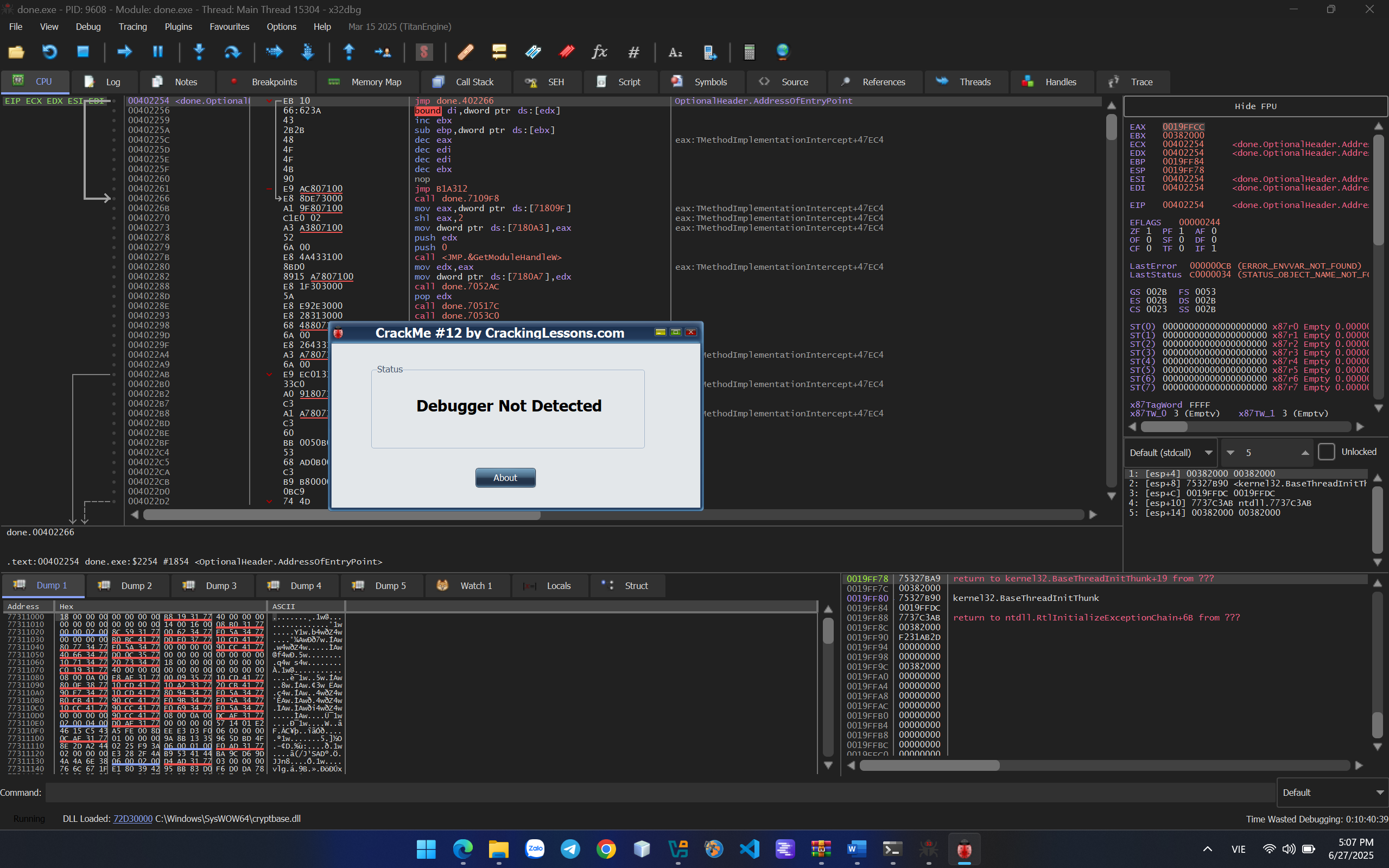


Click run to see where that function is located.

Click "run to user code" to view the overall code. 

It appears to check what value the function returns, then stores it from eax, compares it with 0, and if it's not equal to 0, the je instruction won't be executed and will display the quit program window.

Change je to jmp to always jump and prevent the quit window from appearing. After making the modification, click run again and the program has reappeared, successfully cracking the anti-debugger. 

Debugging successfully!

DONE!!!