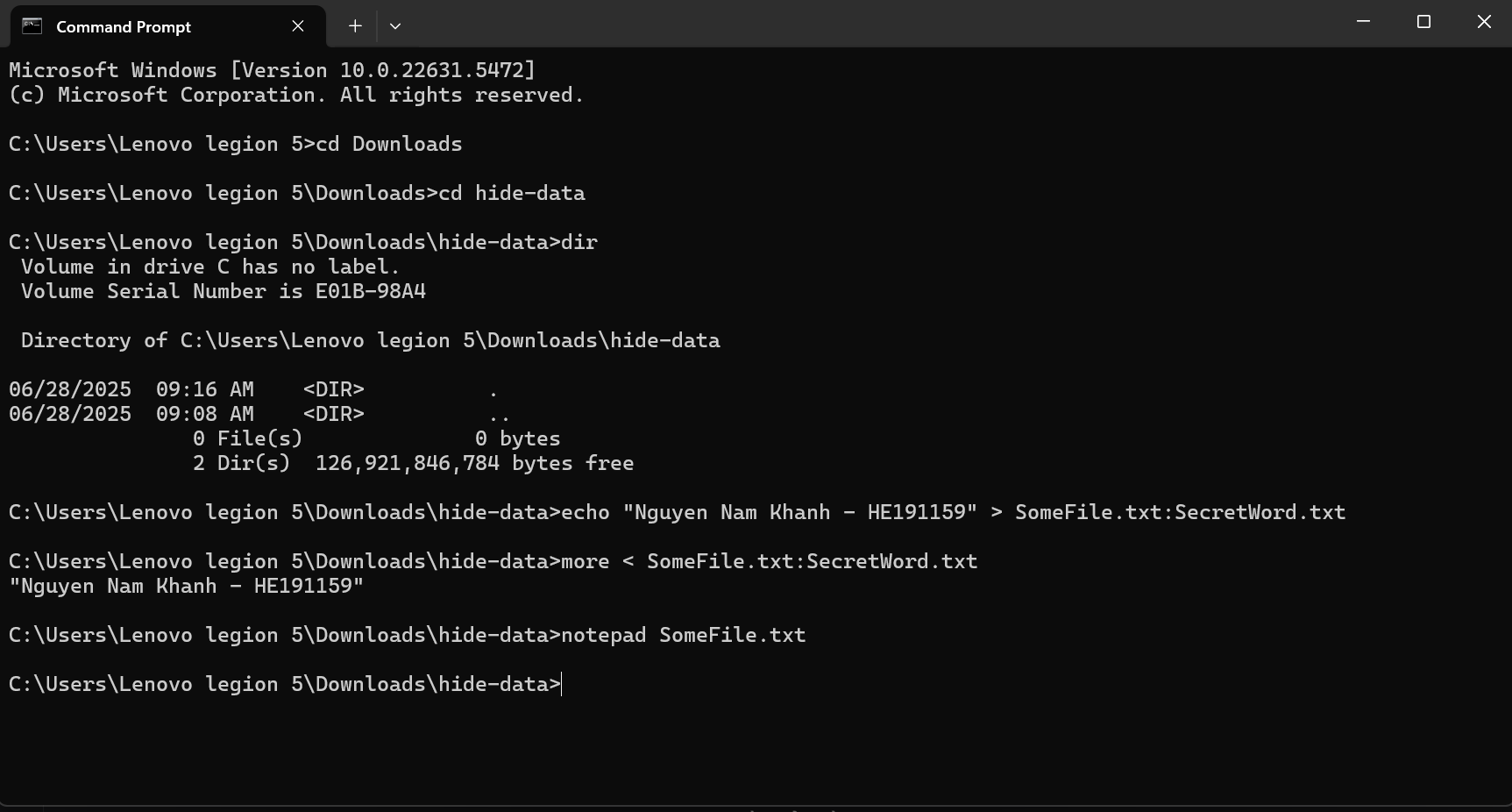
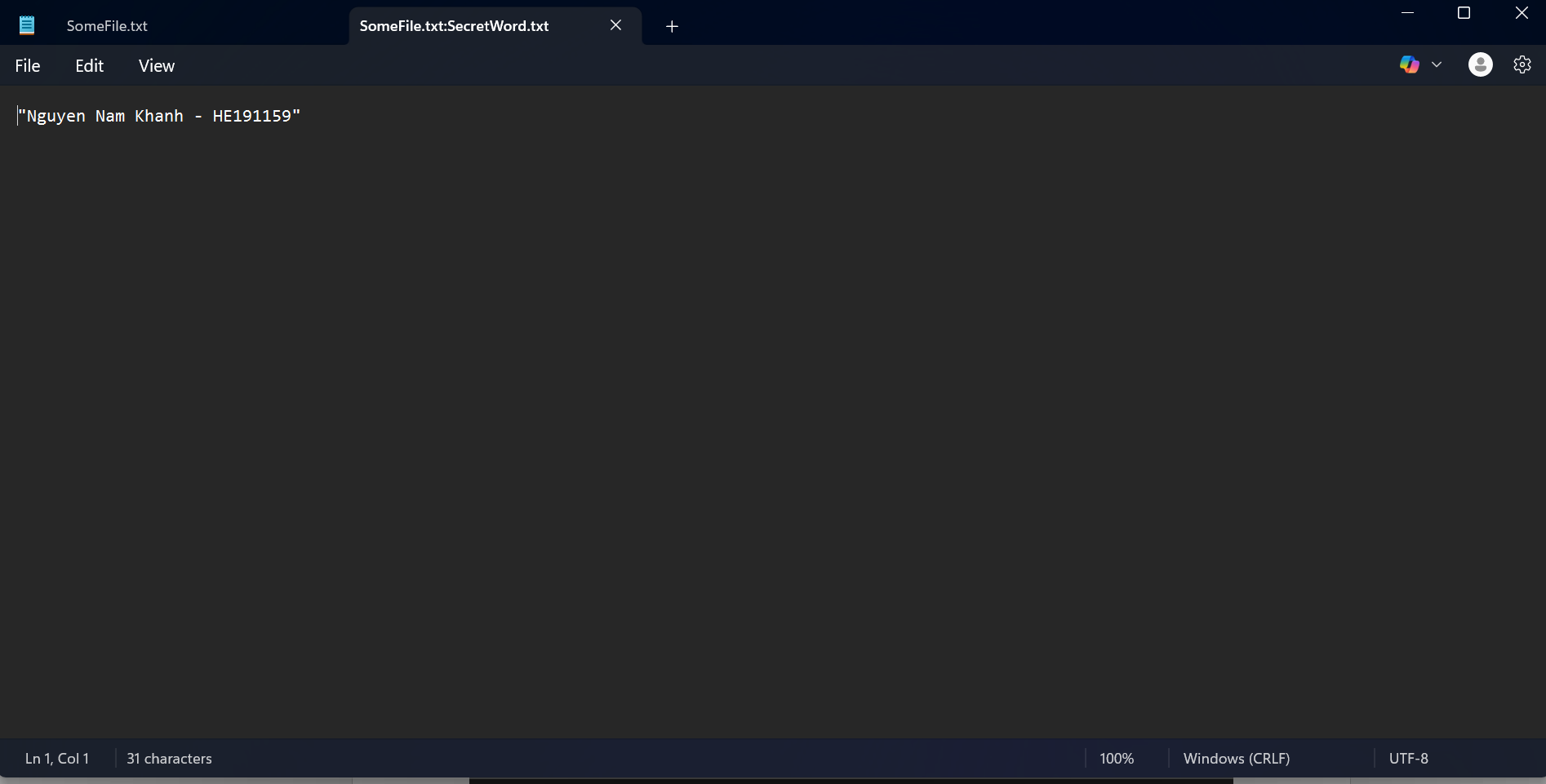
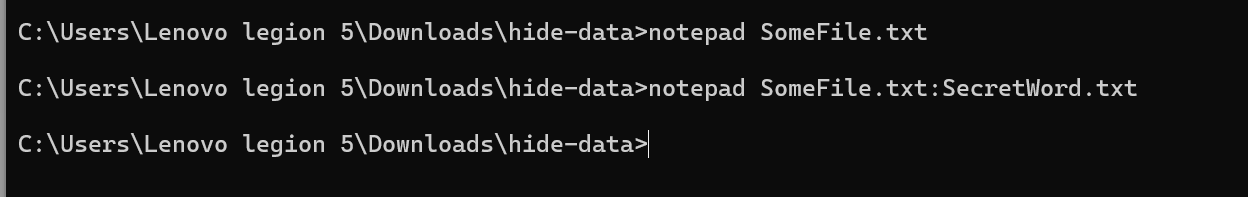
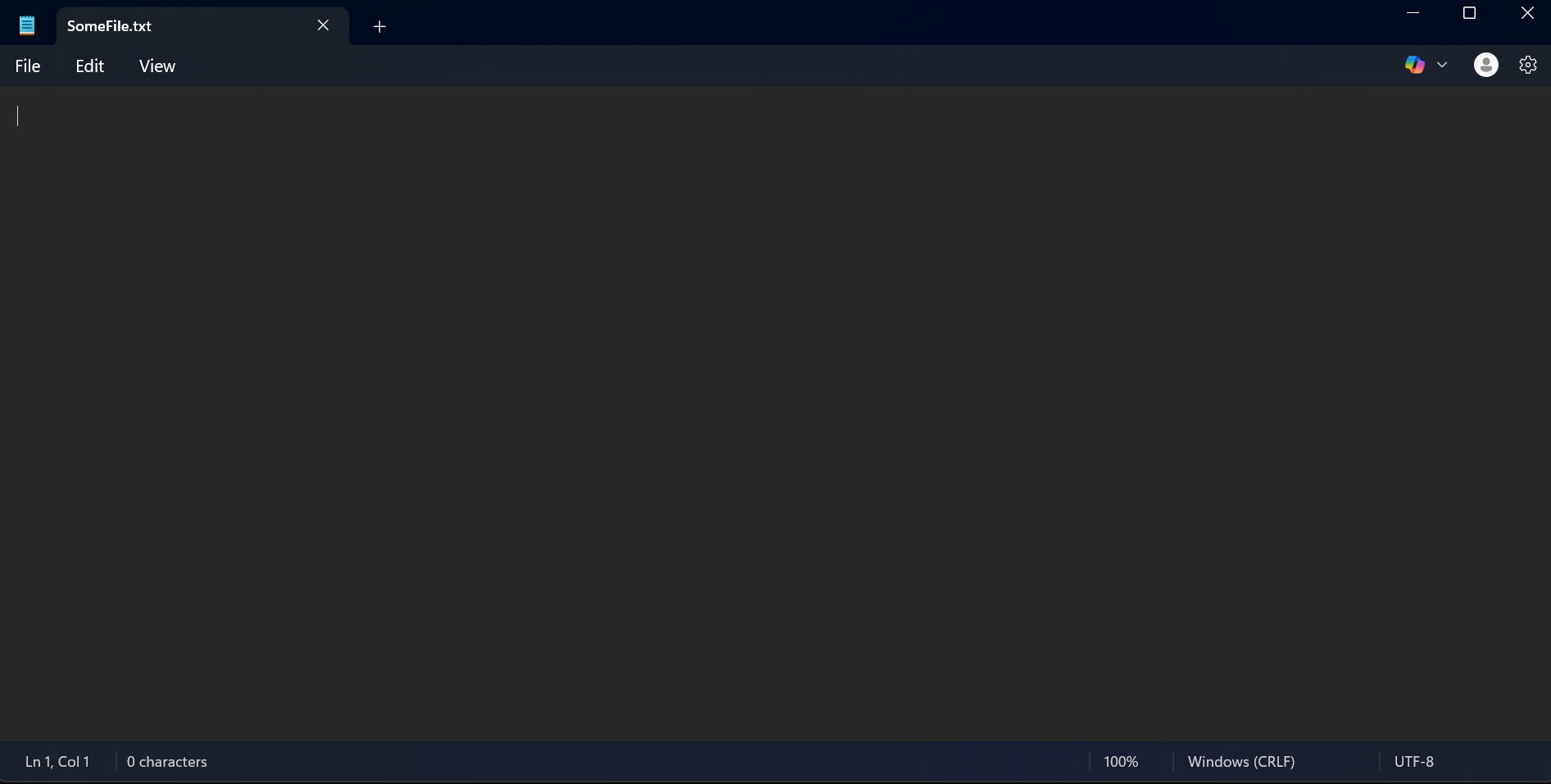
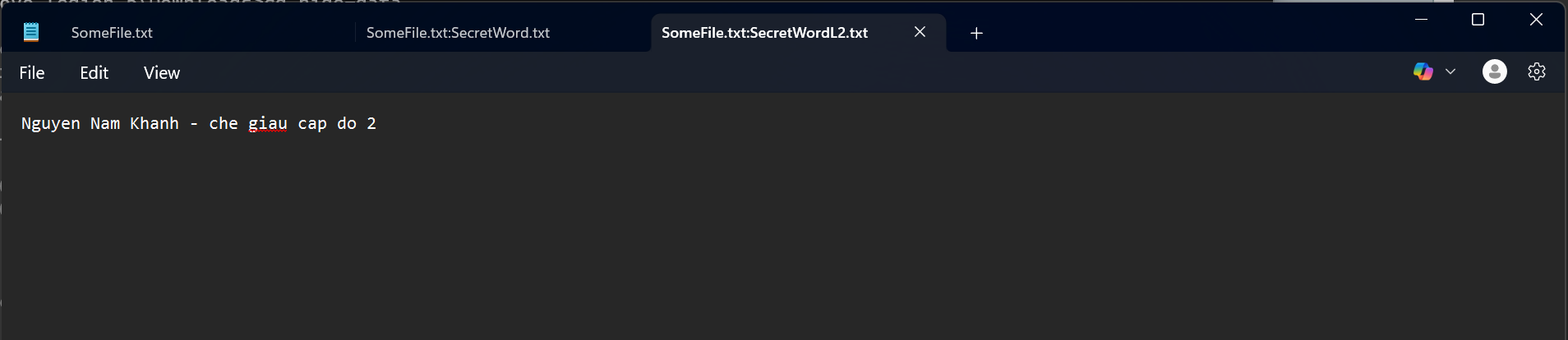
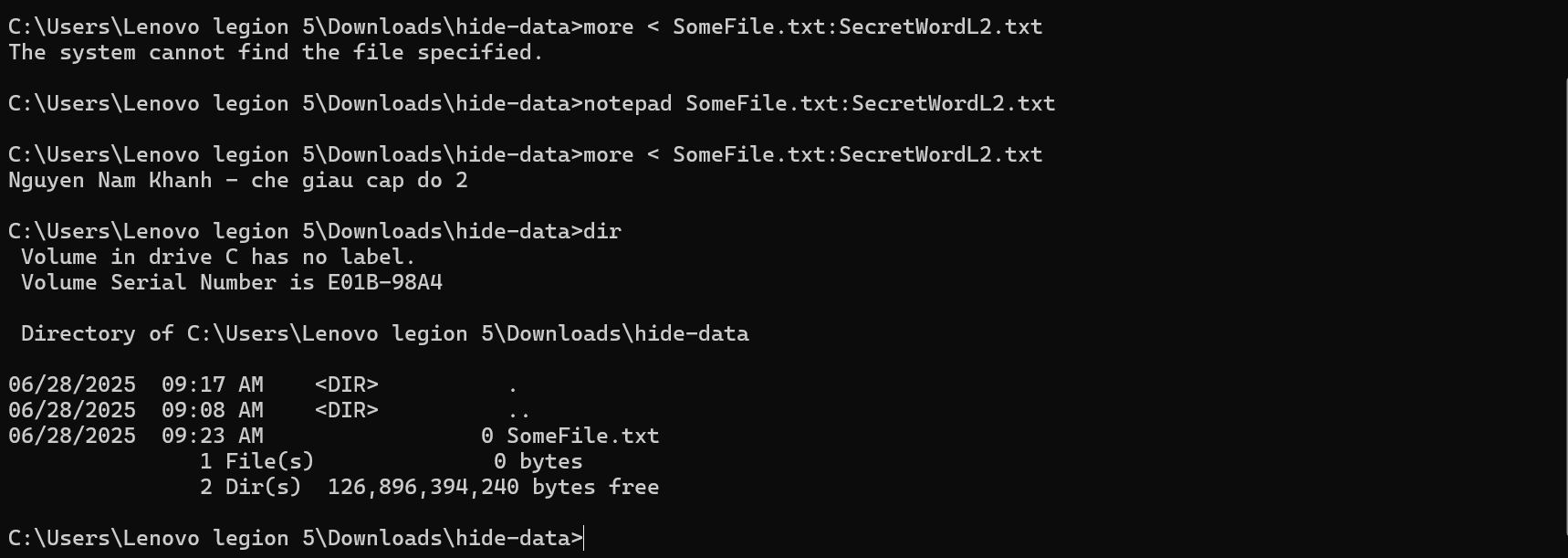
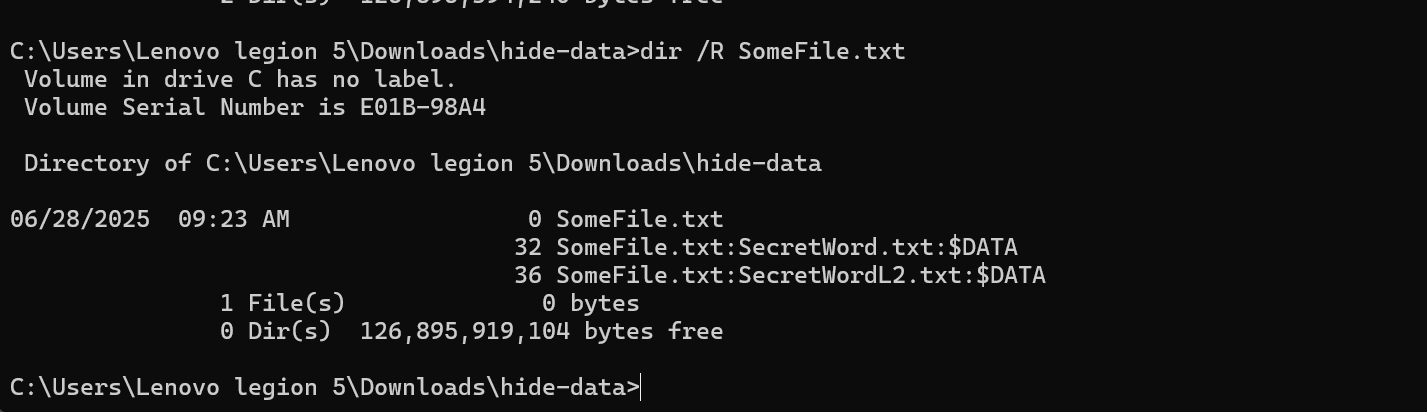
**NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302**

**Lab 14: Using TSK for Network and Host**

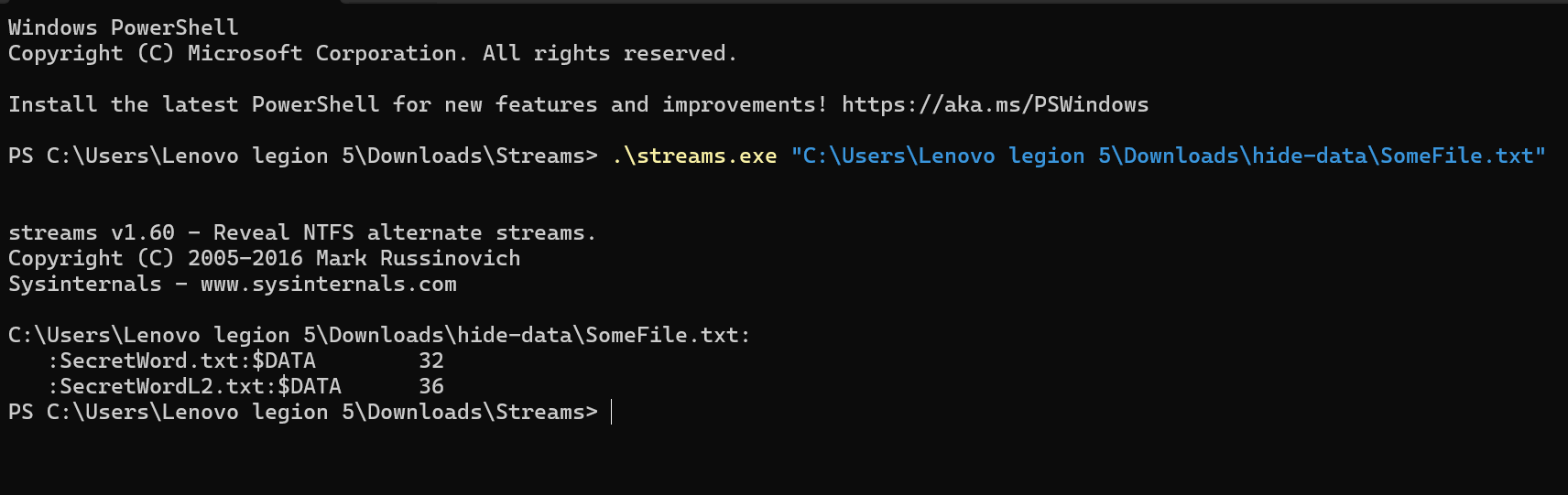
“Hide” data LEVEL 1



“Hide” data LEVEL 2

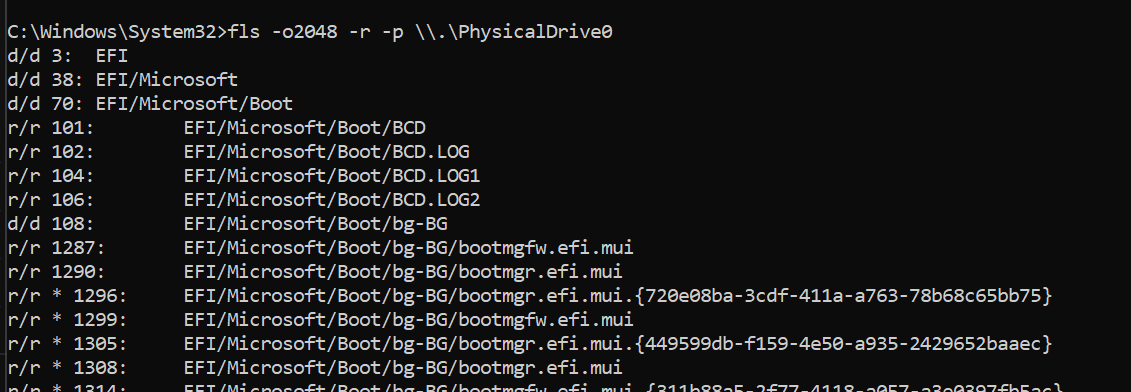
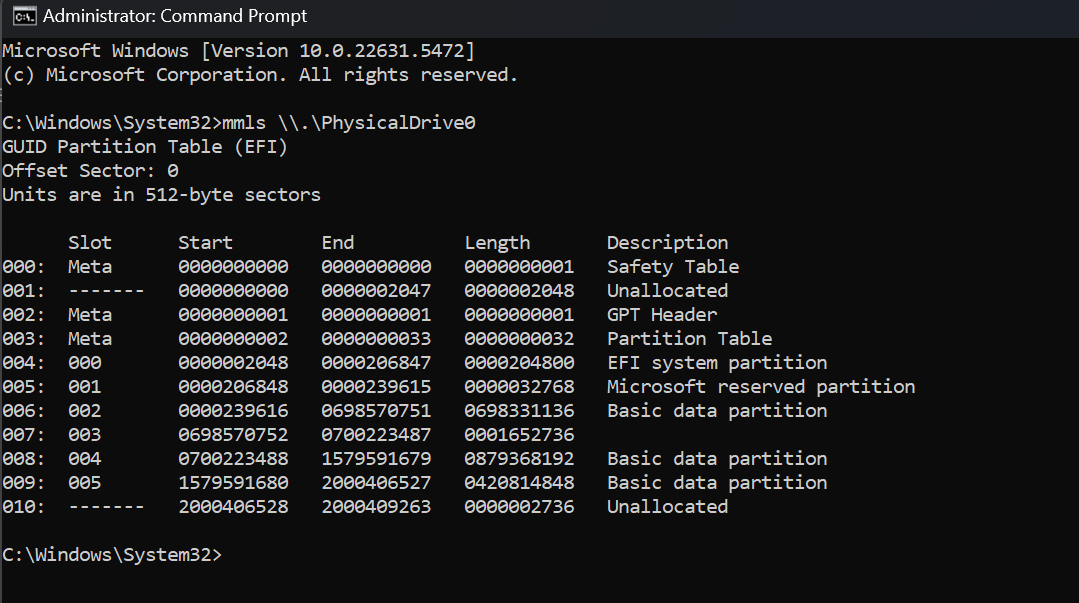
Detect “Hide” data

Some tools for detect ADS: TSK or autopsy, lads.exe1, lns.exe2, sfind.exe3, streams.exe4

I use streams.exe

Analyzing the Master File Table (MFT) for ADS Info

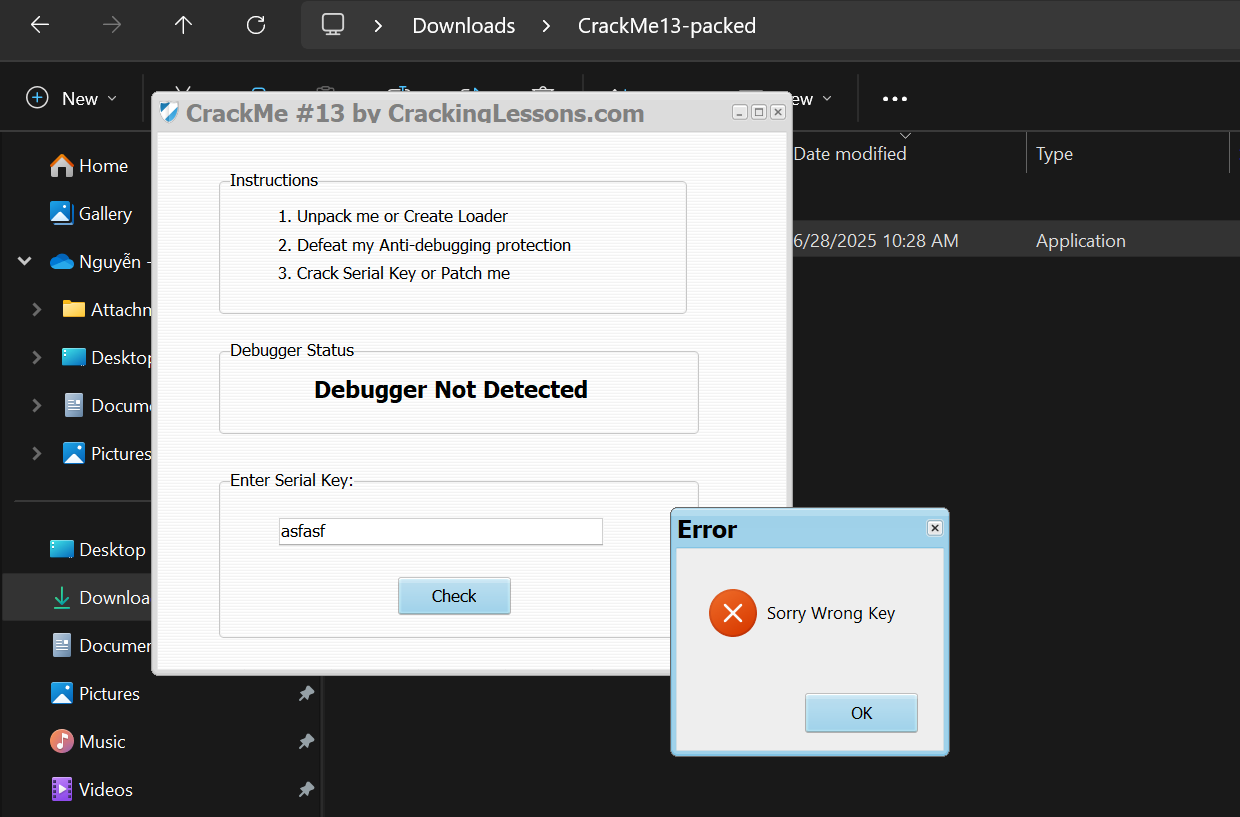
mmls \\.\PhysicalDrive0

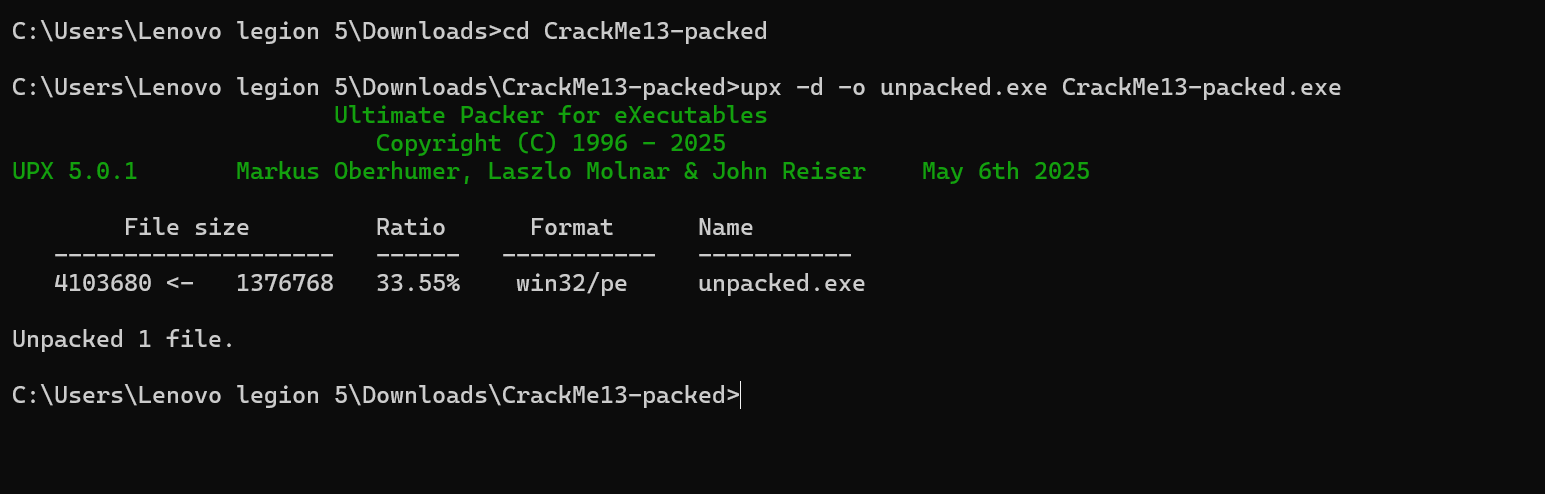


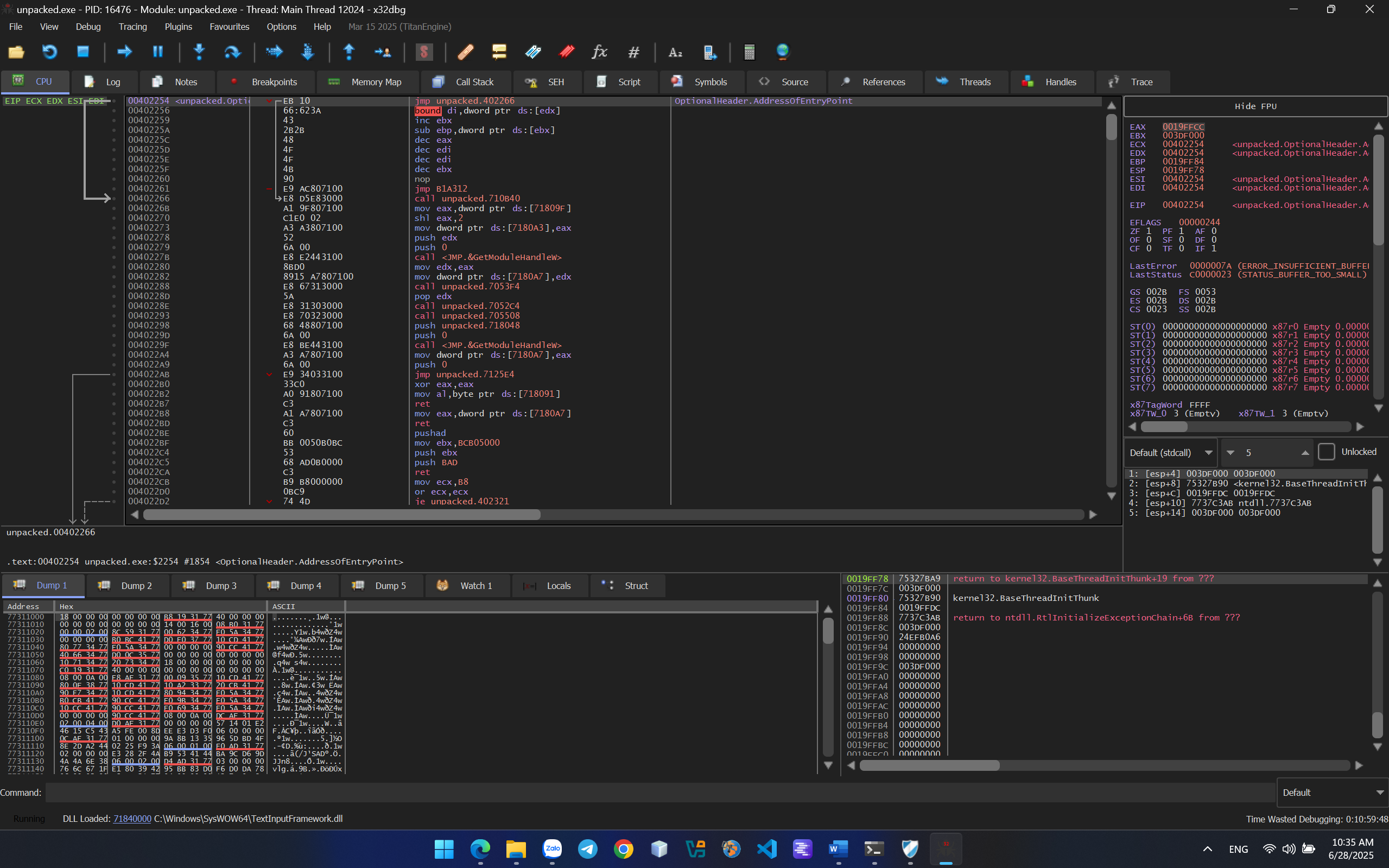
**CRACK ME 13:**

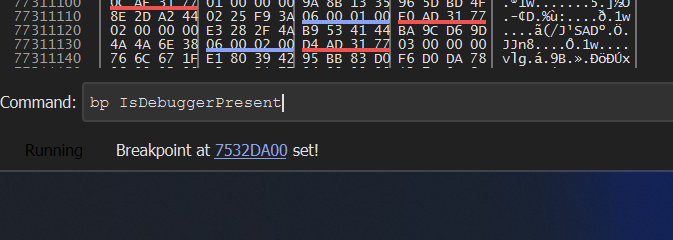
This CrackMe combines three features:

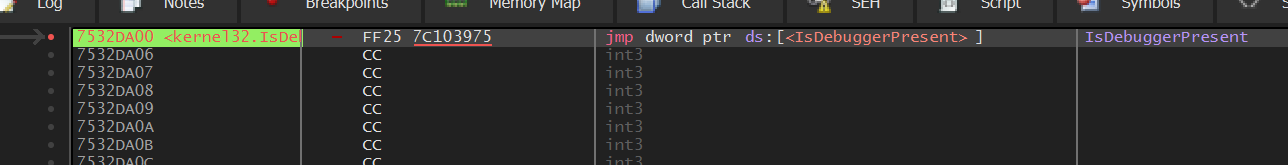
1. Packing
2. Anti-Debugging
3. Software Serial Key Requirement



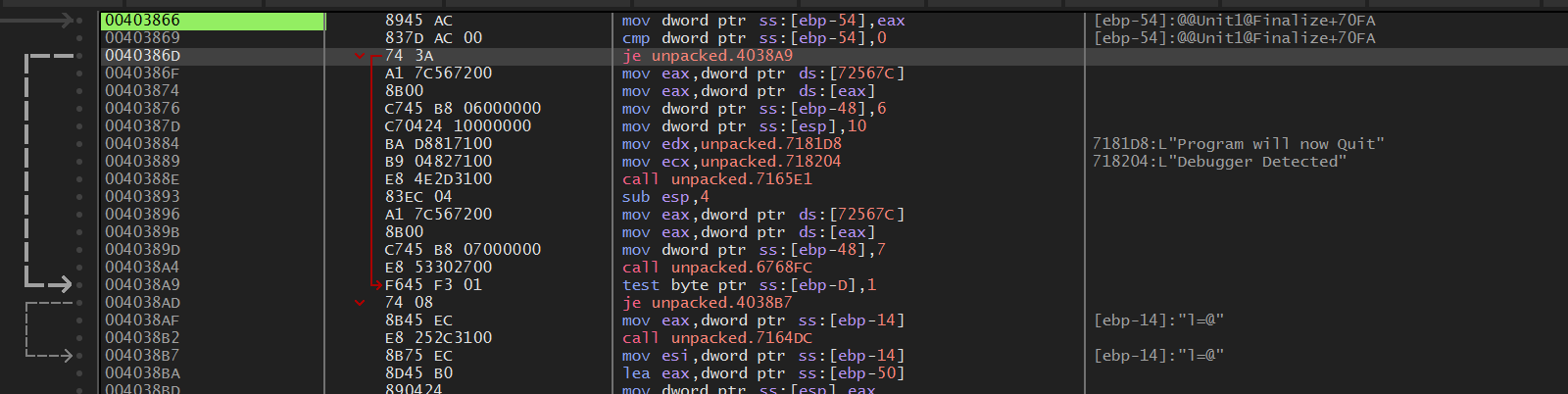
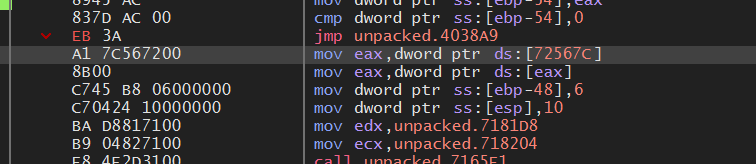
First we use UPX tools to unpacked this file .exe, since it’s packed by these tool: 

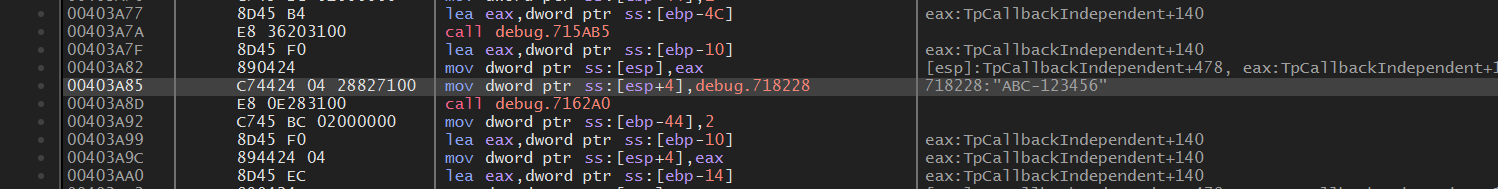
Next, move to solce the anti-debugging requirement, like the crackme 12 challenge, when throw this file to x32dbg, we can run to debug, because this file has been anti-debugged. 

We do as done in crackme 12, put a breakpoint at IsDebuggerPresent function 

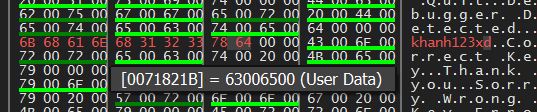
After that, run to breakpoint: 

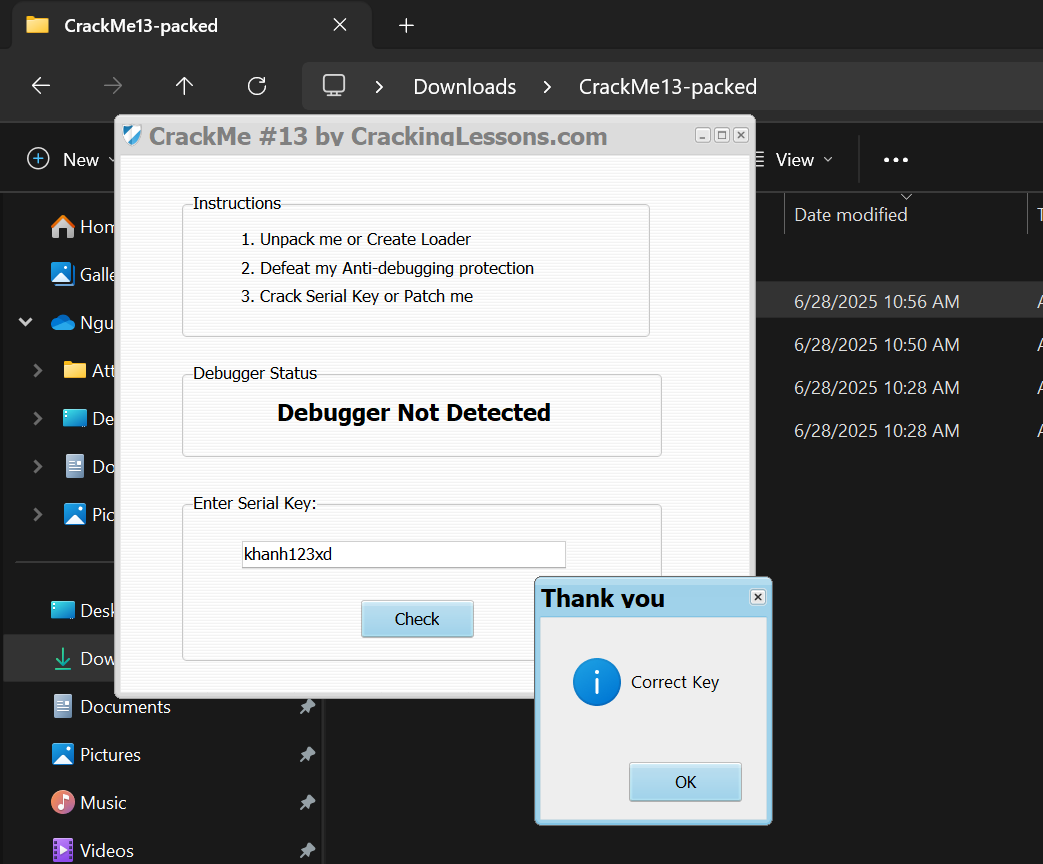
Press run to user code to see the detail:

 Similar to the previous exercise, when running to that breakpoint, we can see it checks whether the IsDebuggerPresent function returns 0 or 1. If it returns 0, the je instruction is executed and the program doesn't quit. However, since we're cracking it, we don't check the condition but change je to jmp directly to bypass the quit notification entirely. 

When anti anti-debugging successfully, we can find the serial key easily in address 00403A85: 

Follow in dump in 718228 and change the value in dump:



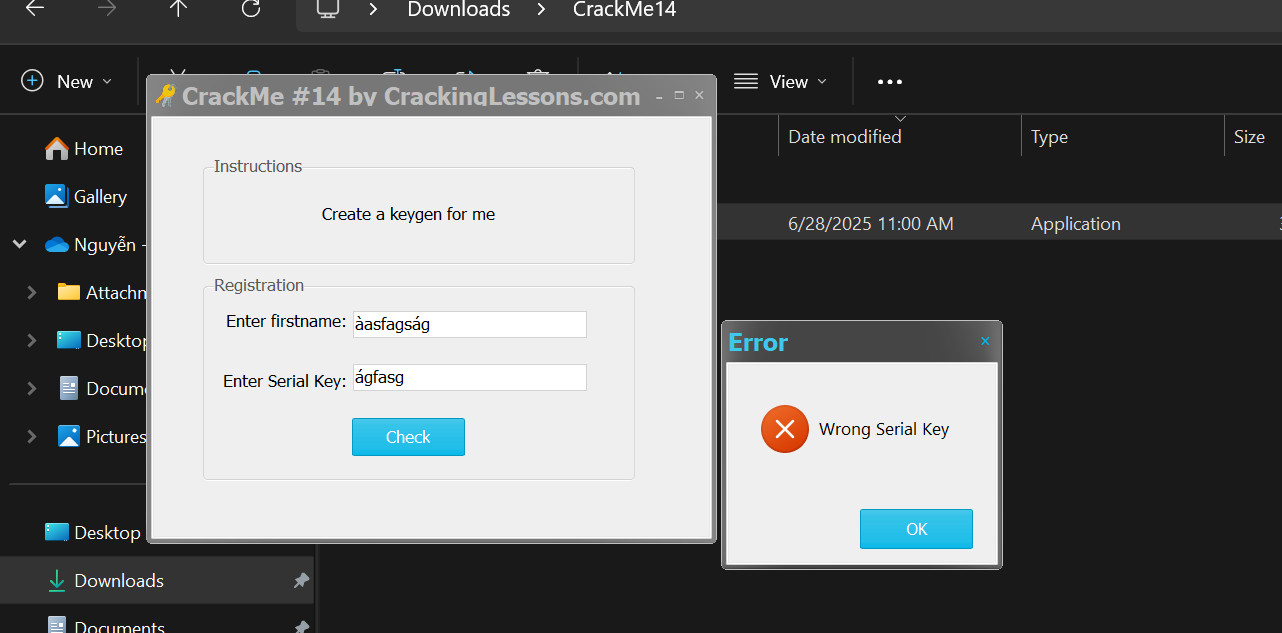
I change ABC-123456 to khanh123xd 

DONE!!!

**CRACK ME 14:**

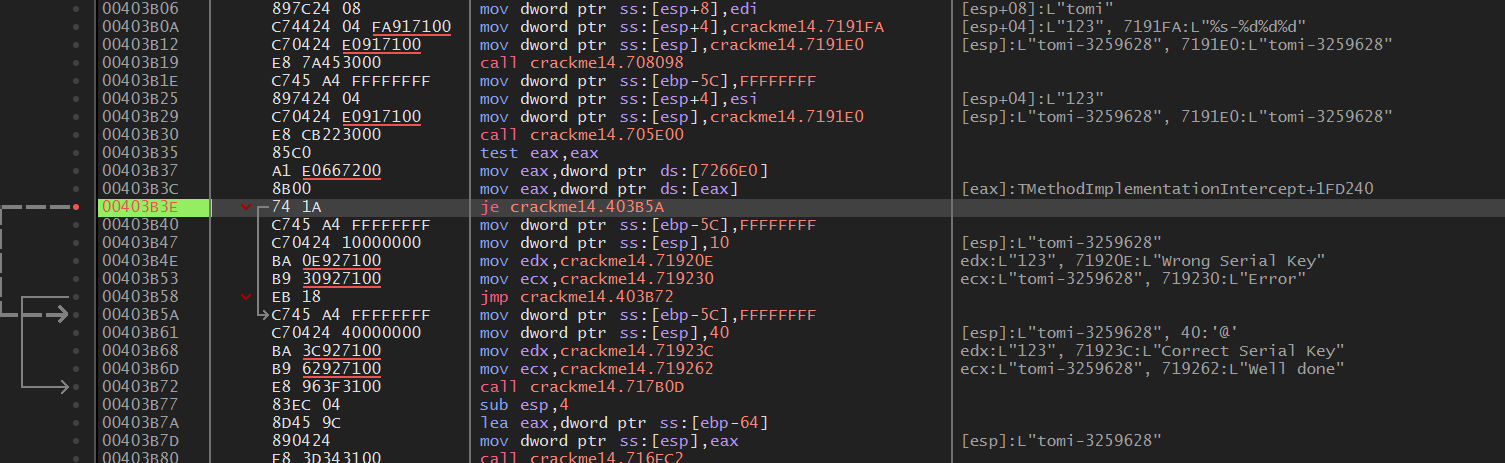
This CrackMe asks for your firstname and then generates a Serial Key based on your firstname.

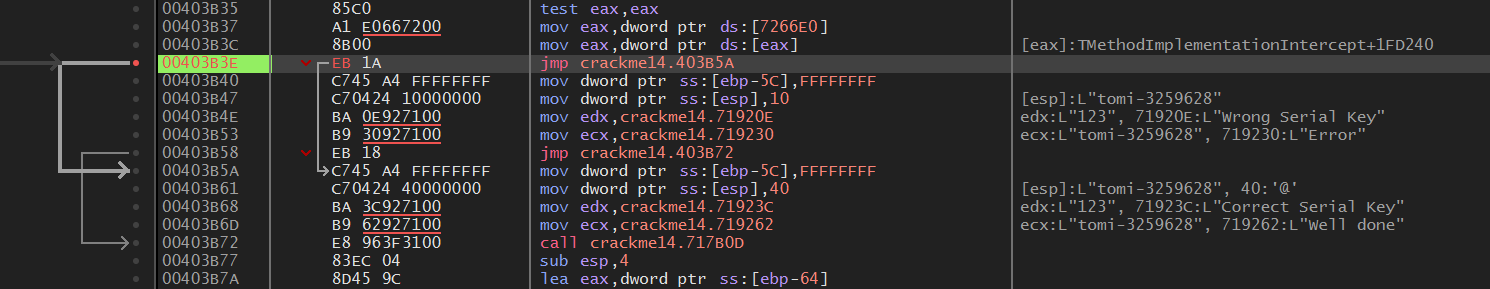
1. Create a Keygen that will be able to generate any Serial Key based on your firstname.
2. To solve this challenge, you may create a self-keygen or, write a separate keygen.



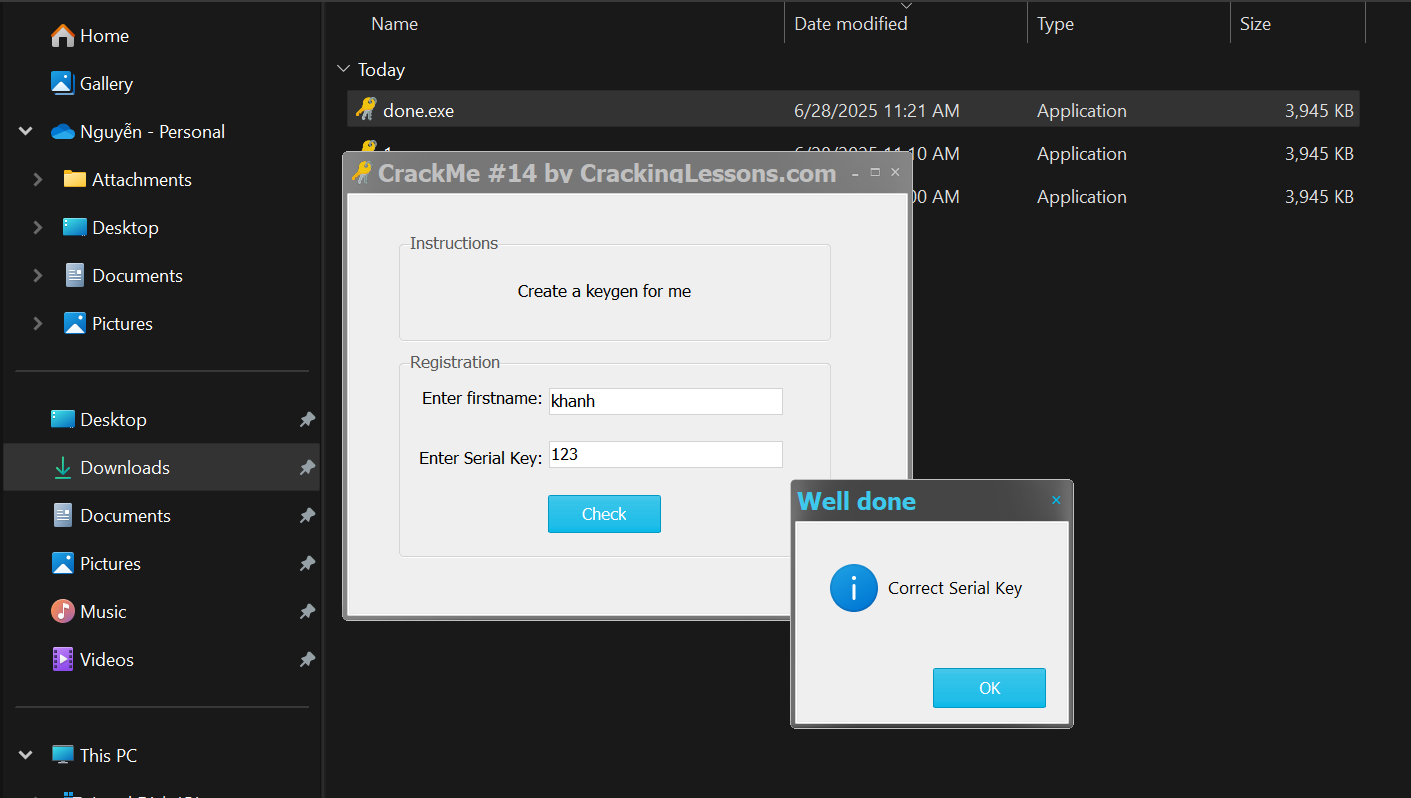
This challenge is done when i create my own key successfully by combining name and serial key. This key will display in the box when you check.

First find the code report the error “Wrong Serial Key”



As you see, in address 00403B3E, this JE command will jump to the correct status if the code above Test eax, eax is set ZF flag when eax is 0. But follow the result, we know that, this JE command is not executed so i change to the JMP command: 

Pacth file and check:

DONE!!!