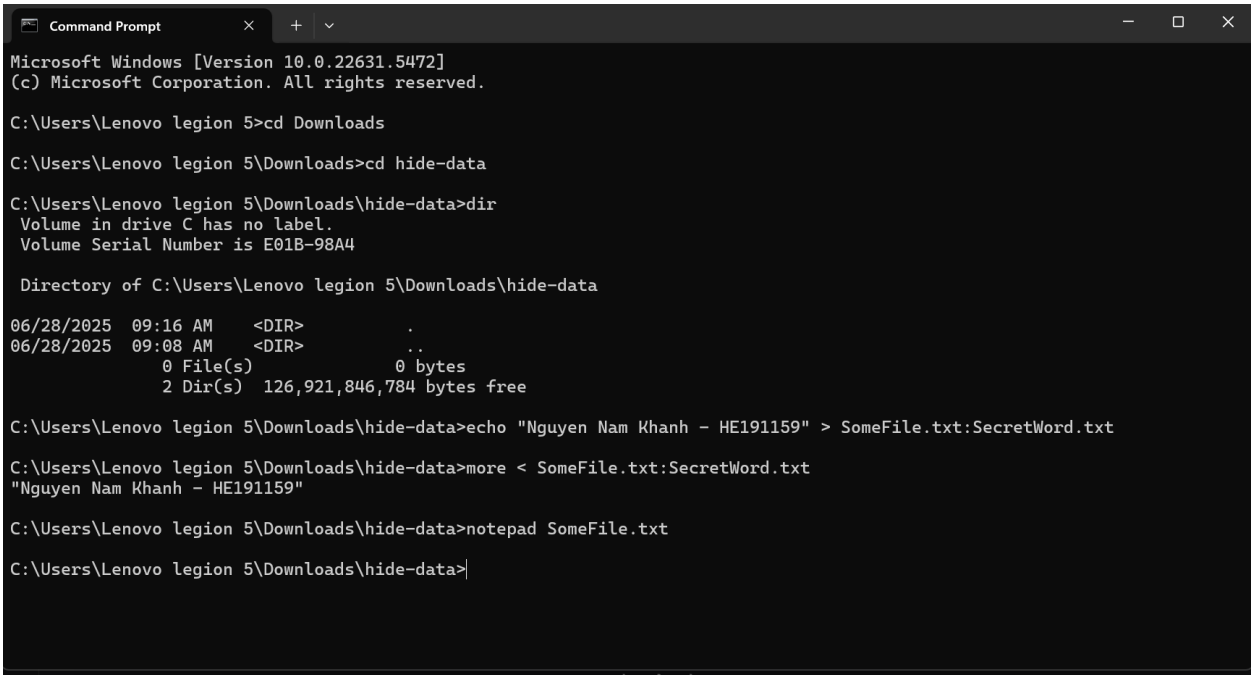
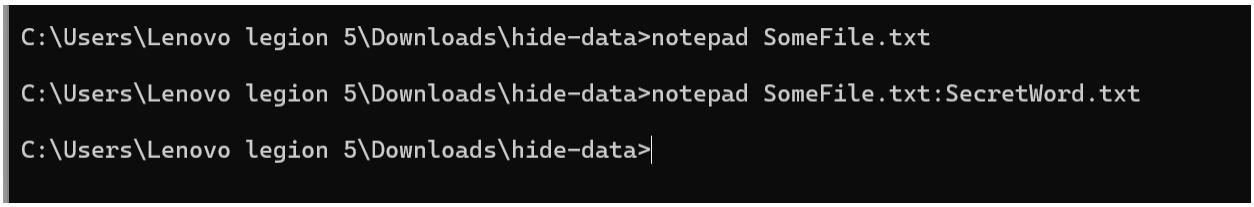
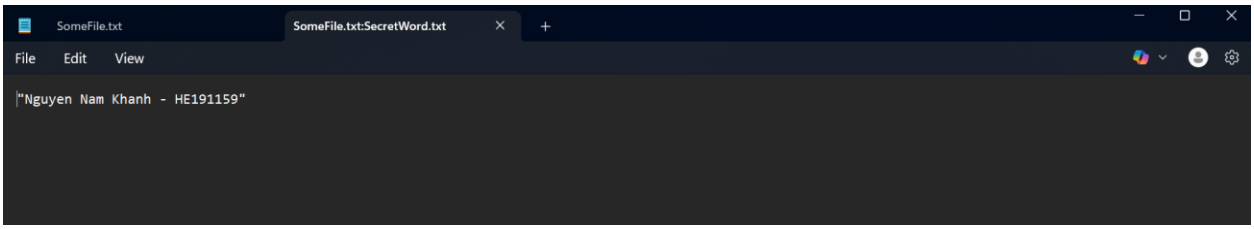
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

Lab 14: Using TSK for Network and Host

“Hide” data LEVEL 1

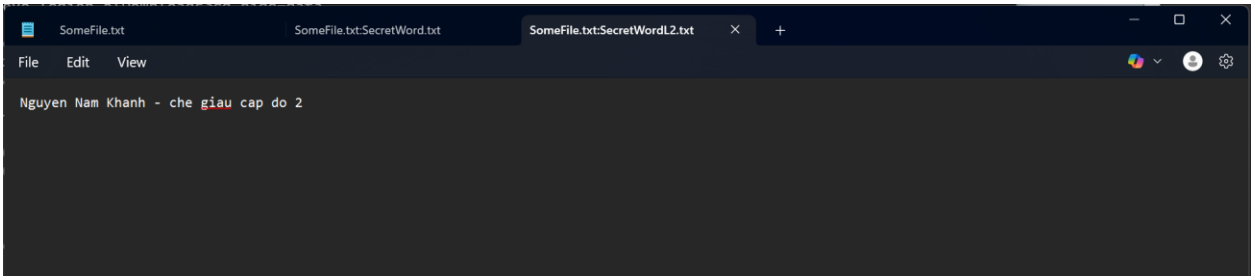






“Hide” data LEVEL 2

```
C:\Users\Lenovo legion 5\Downloads\hide-data>more < SomeFile.txt:SecretWordL2.txt
The system cannot find the file specified.

C:\Users\Lenovo legion 5\Downloads\hide-data>notepad SomeFile.txt:SecretWordL2.txt

C:\Users\Lenovo legion 5\Downloads\hide-data>more < SomeFile.txt:SecretWordL2.txt
Nguyen Nam Khanh - che giau cap do 2

C:\Users\Lenovo legion 5\Downloads\hide-data>dir
 Volume in drive C has no label.
 Volume Serial Number is E01B-98A4

 Directory of C:\Users\Lenovo legion 5\Downloads\hide-data

06/28/2025  09:17 AM    <DIR>          .
06/28/2025  09:08 AM    <DIR>          ..
06/28/2025  09:23 AM                 0 SomeFile.txt
               1 File(s)              0 bytes
               2 Dir(s)  126,896,394,240 bytes free

C:\Users\Lenovo legion 5\Downloads\hide-data>
```



Detect “Hide” data

```
C:\Users\Lenovo legion 5\Downloads\hide-data>dir /R SomeFile.txt
 Volume in drive C has no label.
 Volume Serial Number is E01B-98A4

 Directory of C:\Users\Lenovo legion 5\Downloads\hide-data

06/28/2025  09:23 AM                 0 SomeFile.txt
                                    32 SomeFile.txt:SecretWord.txt:$DATA
                                    36 SomeFile.txt:SecretWordL2.txt:$DATA
               1 File(s)              0 bytes
               0 Dir(s)  126,895,919,104 bytes free

C:\Users\Lenovo legion 5\Downloads\hide-data>
```

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

I use streams.exe

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Lenovo legion 5\Downloads\Streams> .\streams.exe "C:\Users\Lenovo legion 5\Downloads\hide-data\SomeFile.txt"


streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Lenovo legion 5\Downloads\hide-data\SomeFile.txt:
   :SecretWord.txt:$DATA        32
   :SecretWordL2.txt:$DATA      36
PS C:\Users\Lenovo legion 5\Downloads\Streams>
```

Analyzing the Master File Table (MFT) for ADS Info

mmls \\.\PhysicalDrive0

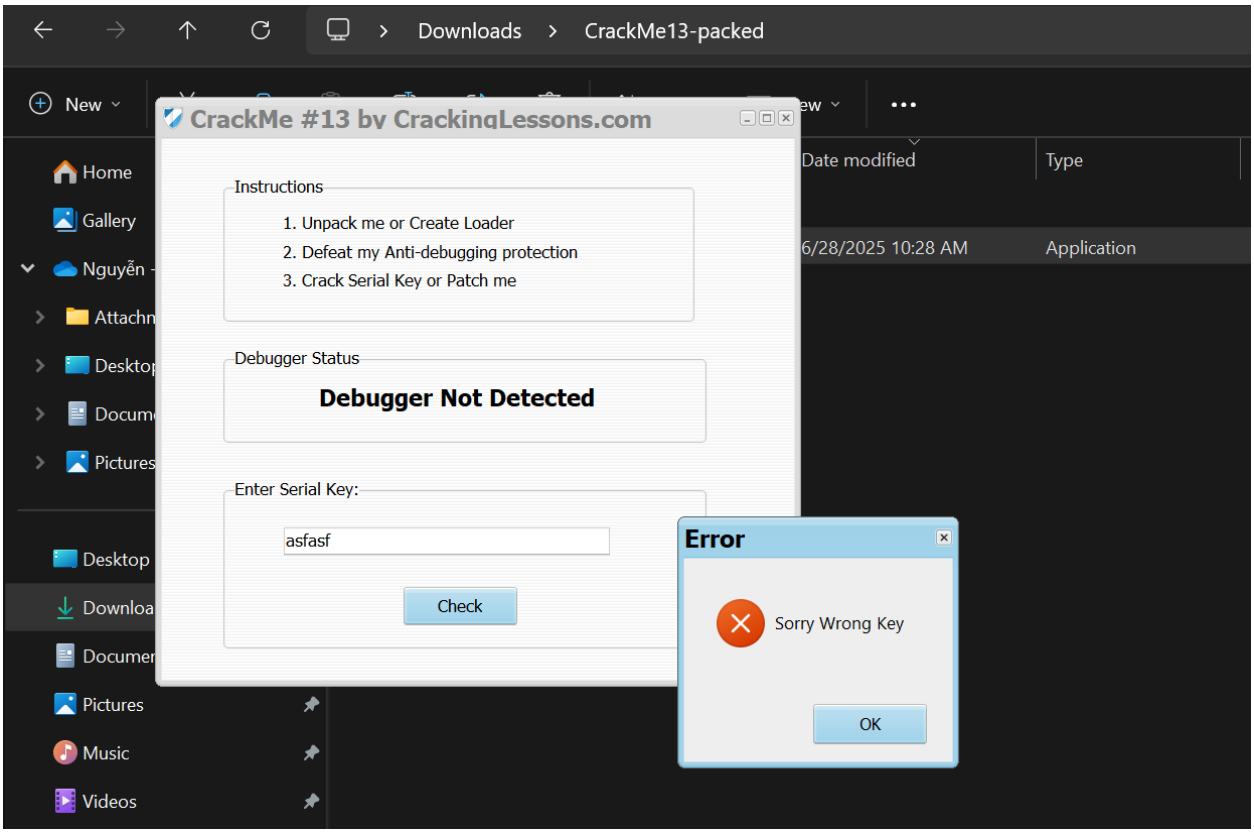
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.5472]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>mmls \\.\PhysicalDrive0
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
004:  000       0000002048   0000206847   0000204800   EFI system partition
005:  001       0000206848   0000239615   0000032768   Microsoft reserved partition
006:  002       0000239616   0698570751   0698331136   Basic data partition
007:  003       0698570752   0700223487   0001652736
008:  004       0700223488   1579591679   0879368192   Basic data partition
009:  005       1579591680   2000406527   0420814848   Basic data partition
010:  -------   2000406528   2000409263   0000002736   Unallocated
```

```
C:\Windows\System32>fls -o2048 -r -p \\.\PhysicalDrive0
d/d 3:  EFI
d/d 38: EFI/Microsoft
d/d 70: EFI/Microsoft/Boot
r/r 101:        EFI/Microsoft/Boot/BCD
r/r 102:        EFI/Microsoft/Boot/BCD.LOG
r/r 104:        EFI/Microsoft/Boot/BCD.LOG1
r/r 106:        EFI/Microsoft/Boot/BCD.LOG2
d/d 108:        EFI/Microsoft/Boot/bg-BG
r/r 1287:       EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
r/r 1290:       EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui
r/r * 1296:     EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui.{720e08ba-3cdf-411a-a763-78b68c65bb75}
r/r * 1299:     EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui
r/r * 1305:     EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui.{449599db-f159-4e50-a935-2429652baaec}
r/r * 1308:     EFI/Microsoft/Boot/bg-BG/bootmgr.efi.mui
r/r * 1314:     EFI/Microsoft/Boot/bg-BG/bootmgfw.efi.mui.{311b88e5-2f77-4118-a057-a3e0897fb5ac}
```

CRACK ME 13:

This CrackMe combines three features:

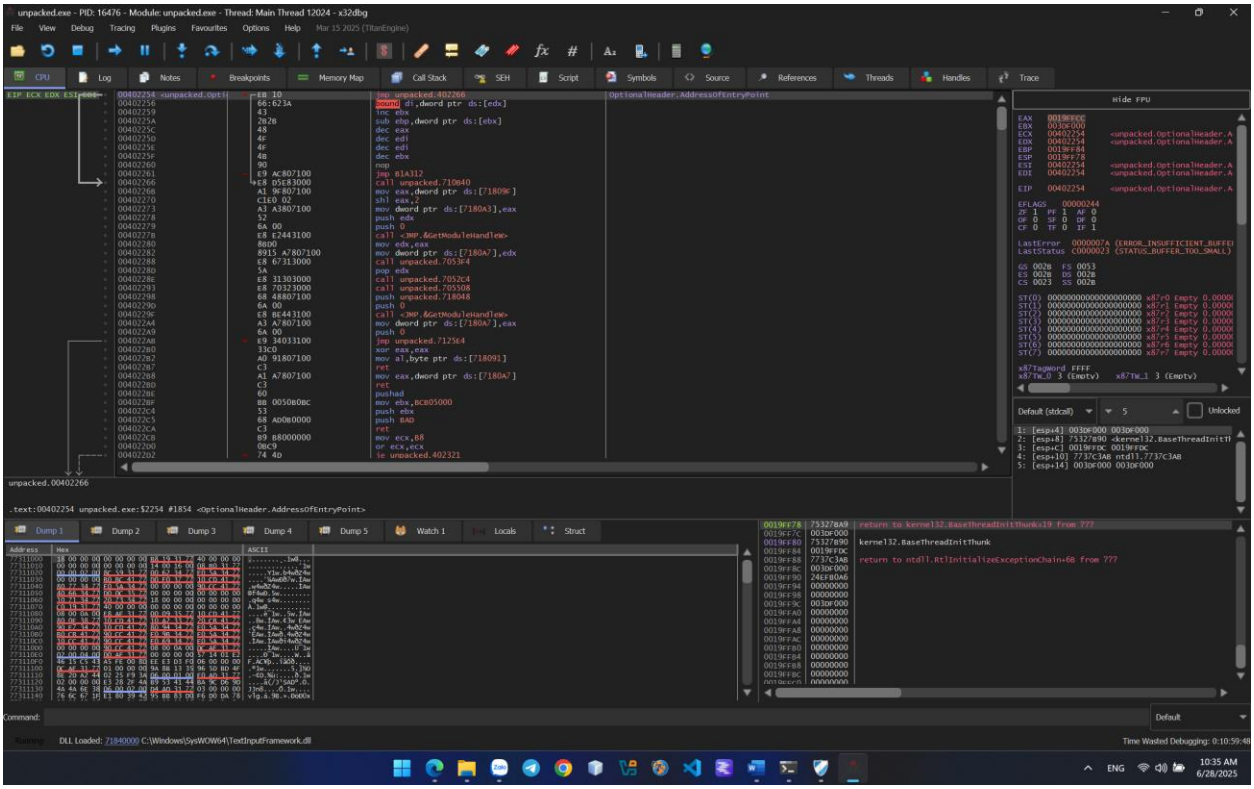
1. Packing
2. Anti-Debugging
3. Software Serial Key Requirement



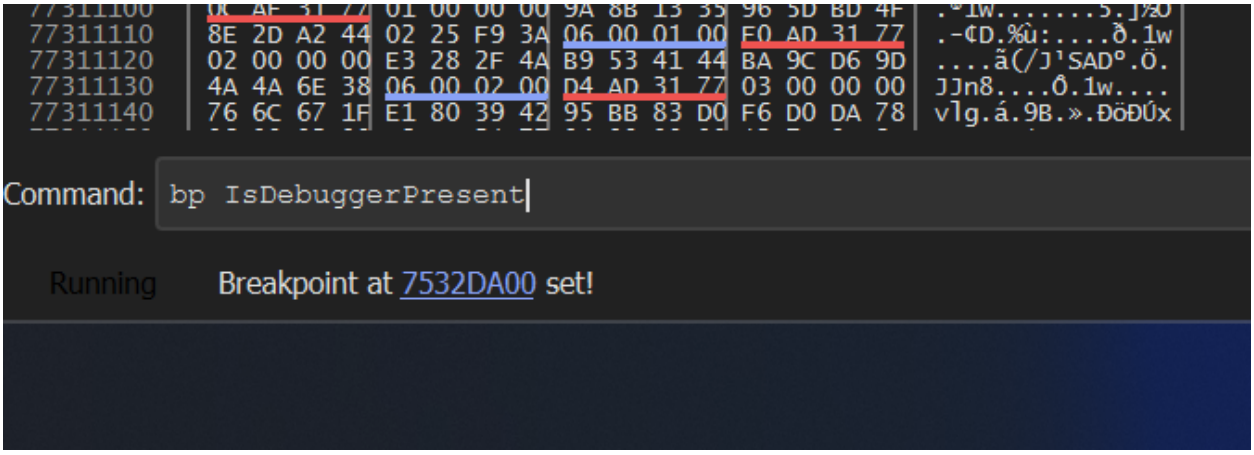
First we use UPX tools to unpacked this file .exe, since it's packed by these tool:

```
C:\Users\Lenovo legion 5\Downloads>cd CrackMe13-packed

C:\Users\Lenovo legion 5\Downloads\CrackMe13-packed>upx -d -o unpacked.exe CrackMe13-packed.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2025
UPX 5.0.1       Markus Oberhumer, Laszlo Molnar & John Reiser    May 6th 2025

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   4103680 <-   1376768   33.55%    win32/pe     unpacked.exe

Unpacked 1 file.

C:\Users\Lenovo legion 5\Downloads\CrackMe13-packed>
```

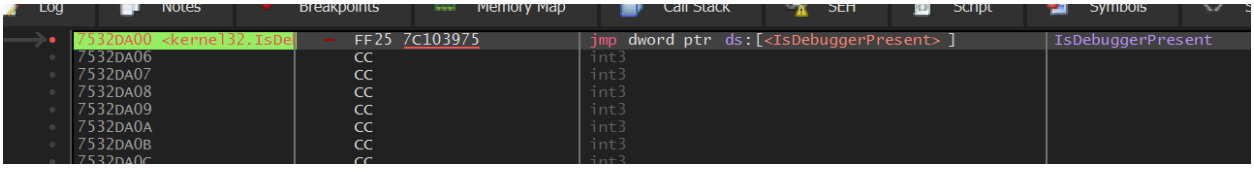
Next, move to solce the anti-debugging requirement, like the crackme 12 challenge, when throw this file to x32dbg, we can run to debug, because this file has been anti-debugged.



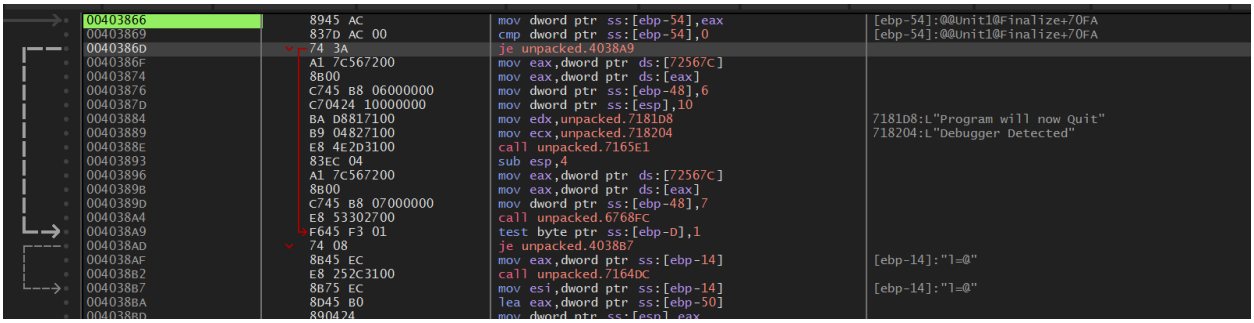
We do as done in crackme 12, put a breakpoint at IsDebuggerPresent function



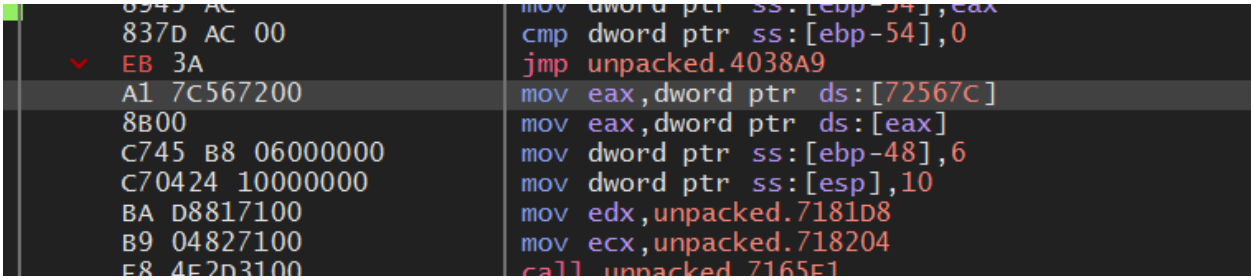
After that, run to breakpoint:



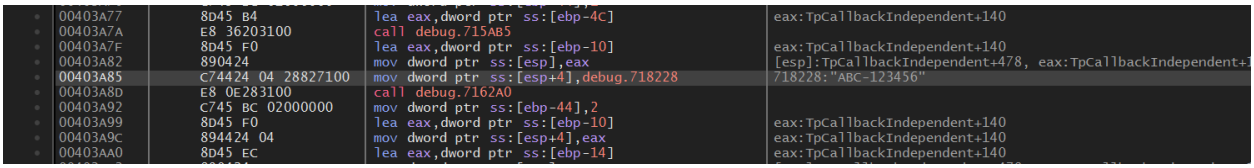
Press run to user code to see the detail:



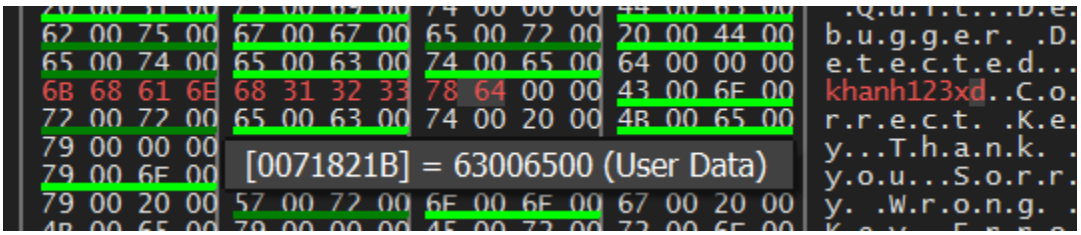
Similar to the previous exercise, when running to that breakpoint, we can see it checks whether the IsDebuggerPresent function returns 0 or 1. If it returns 0, the je instruction is executed and the program doesn't quit. However, since we're cracking it, we don't check the condition but change je to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



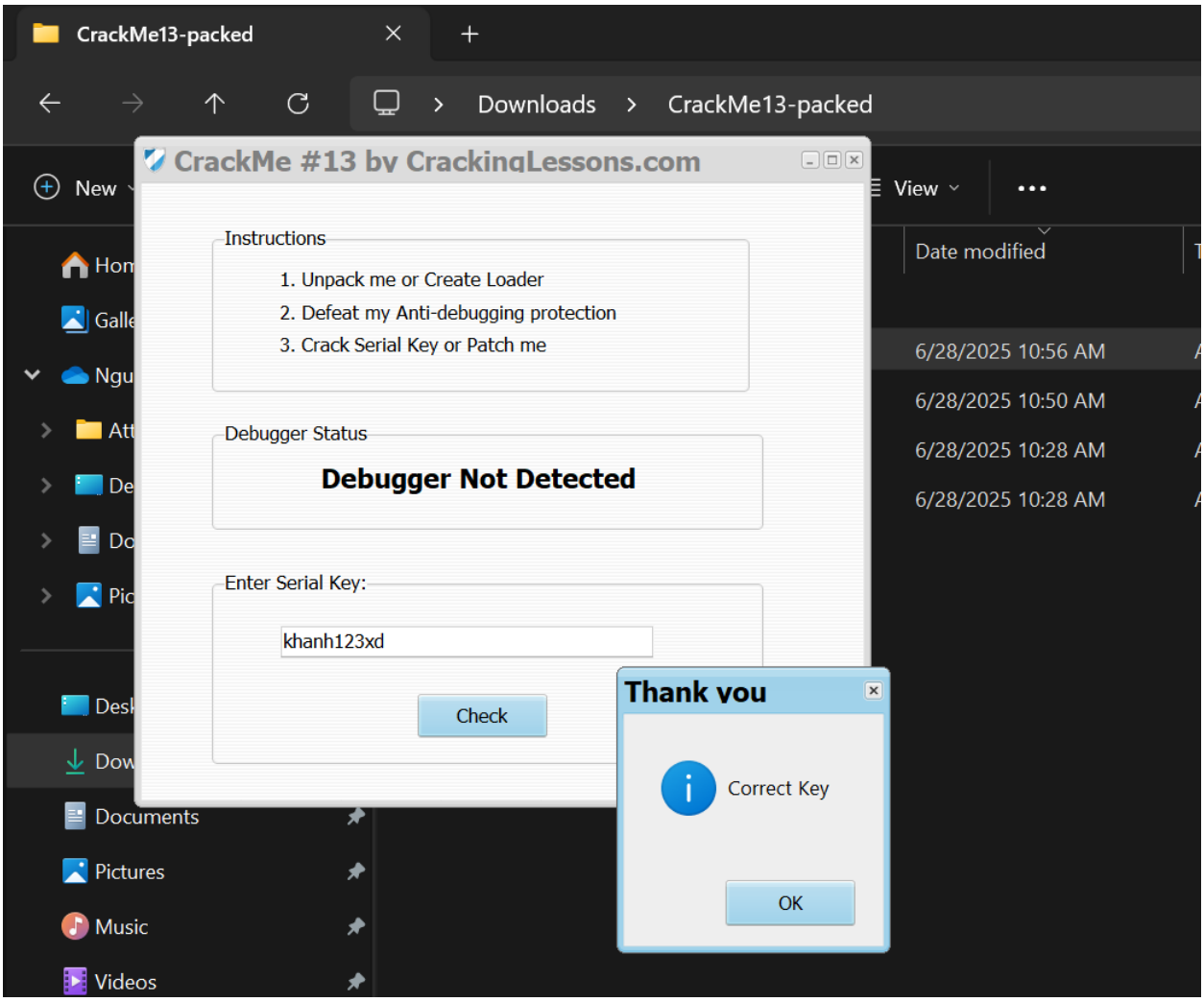
When anti anti-debugging successfully, we can find the serial key easily in address 00403A85:



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



I change ABC-123456 to khanh123xd

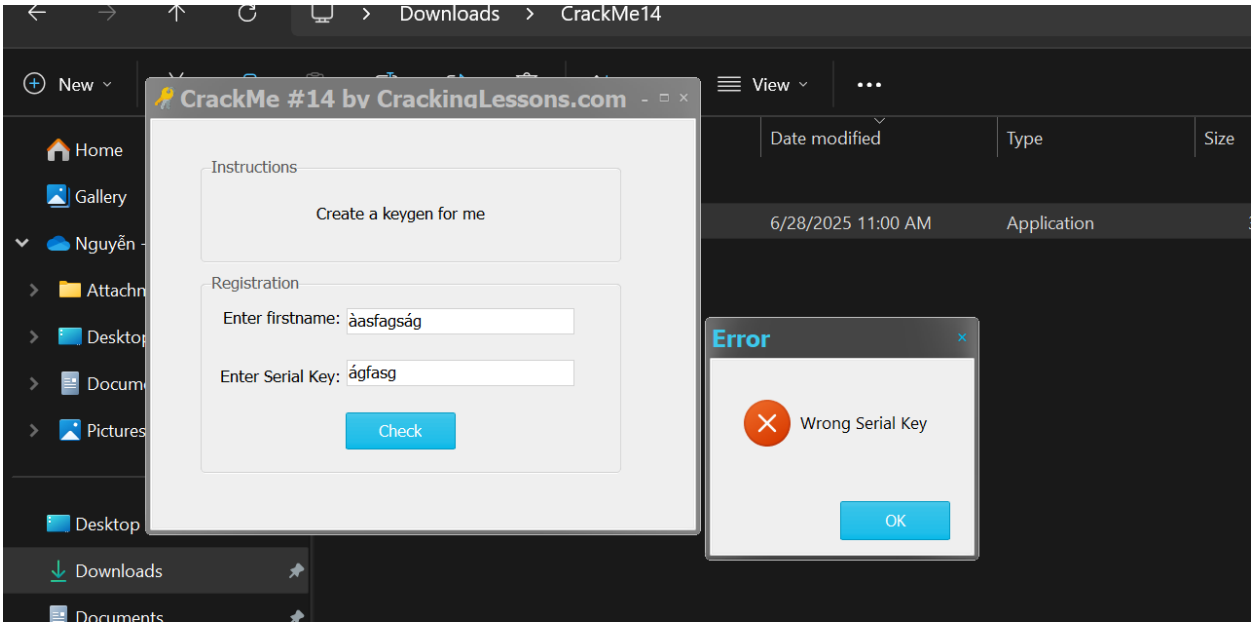


DONE!!!

CRACK ME 14:

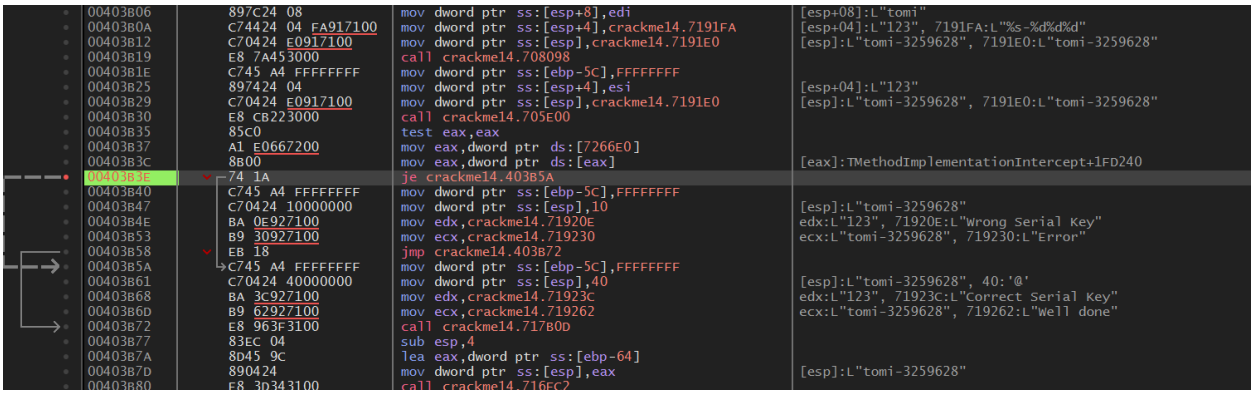
This CrackMe asks for your firstname and then generates a Serial Key based on your firstname.

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.



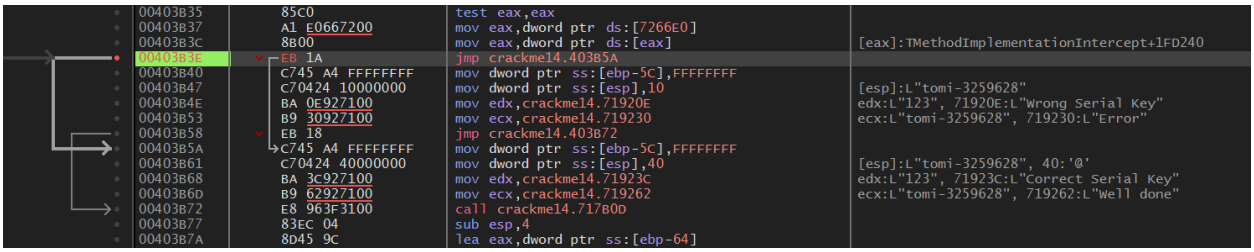
This challenge is done when i create my own key successfully by combining name and serial key. This key will display in the box when you check.

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

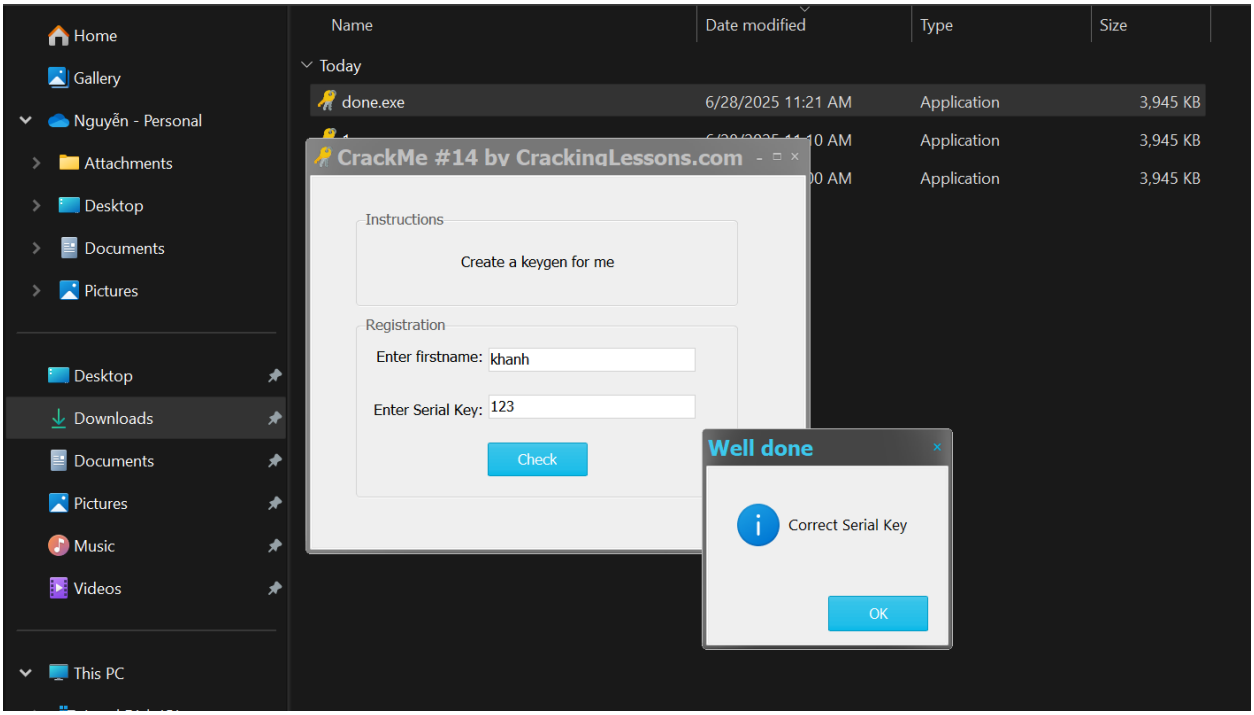


As you see, in address 00403B3E, this JE command will jump to the correct status if the code above Test eax, eax is set ZF flag when eax is 0. But follow the result, we know that,

this JE command is not executed so i change to the JMP command:



Pacth file and check:



DONE!!!