

Lab 14: Using TSK for Network and Host

“Hide” data LEVEL 1

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

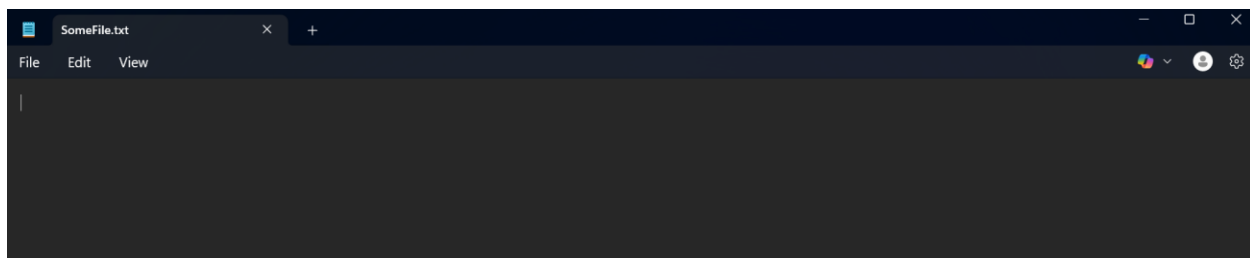
C:\Users\Lenovo legion 5>cd Downloads
C:\Users\Lenovo legion 5\Downloads>cd hide-data
C:\Users\Lenovo legion 5\Downloads\hide-data>dir
Volume in drive C has no label.
Volume Serial Number is E01B-98A4

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

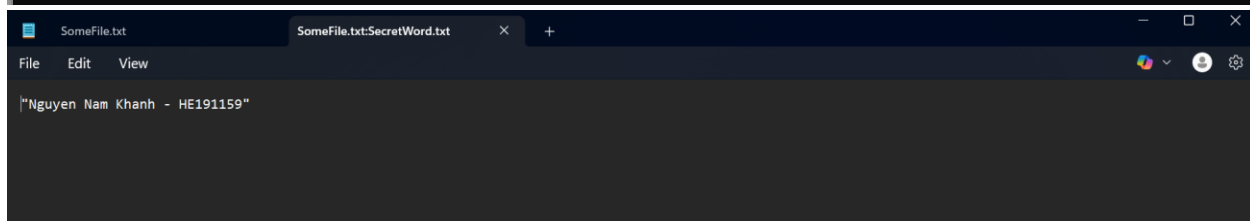
06/28/2025  09:16 AM    <DIR>          .
06/28/2025  09:08 AM    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s) 126,921,846,784 bytes free

C:\Users\Lenovo legion 5\Downloads\hide-data>echo "Nguyen Nam Khanh - HE191159" > SomeFile.txt:SecretWord.txt
C:\Users\Lenovo legion 5\Downloads\hide-data>more < SomeFile.txt:SecretWord.txt
"Nguyen Nam Khanh - HE191159"

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



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



“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

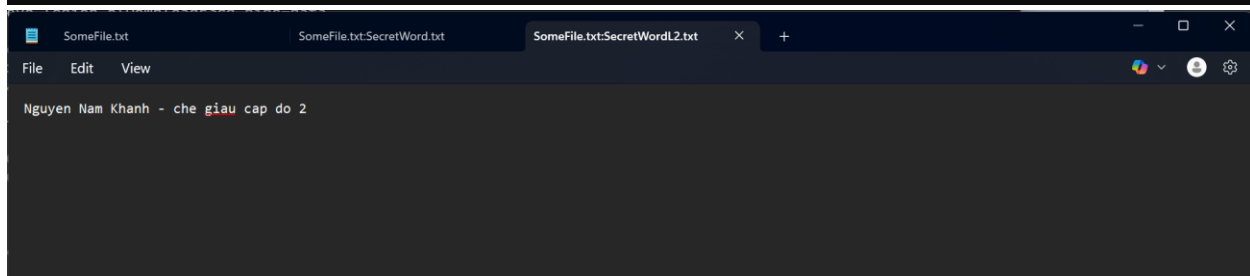
C:\Users\Lenovo legion 5\Downloads\hide-data>more < SomeFile.txt:SecretWordL2.txt
Nguyen Nam Khanh - che giau cap do 2

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

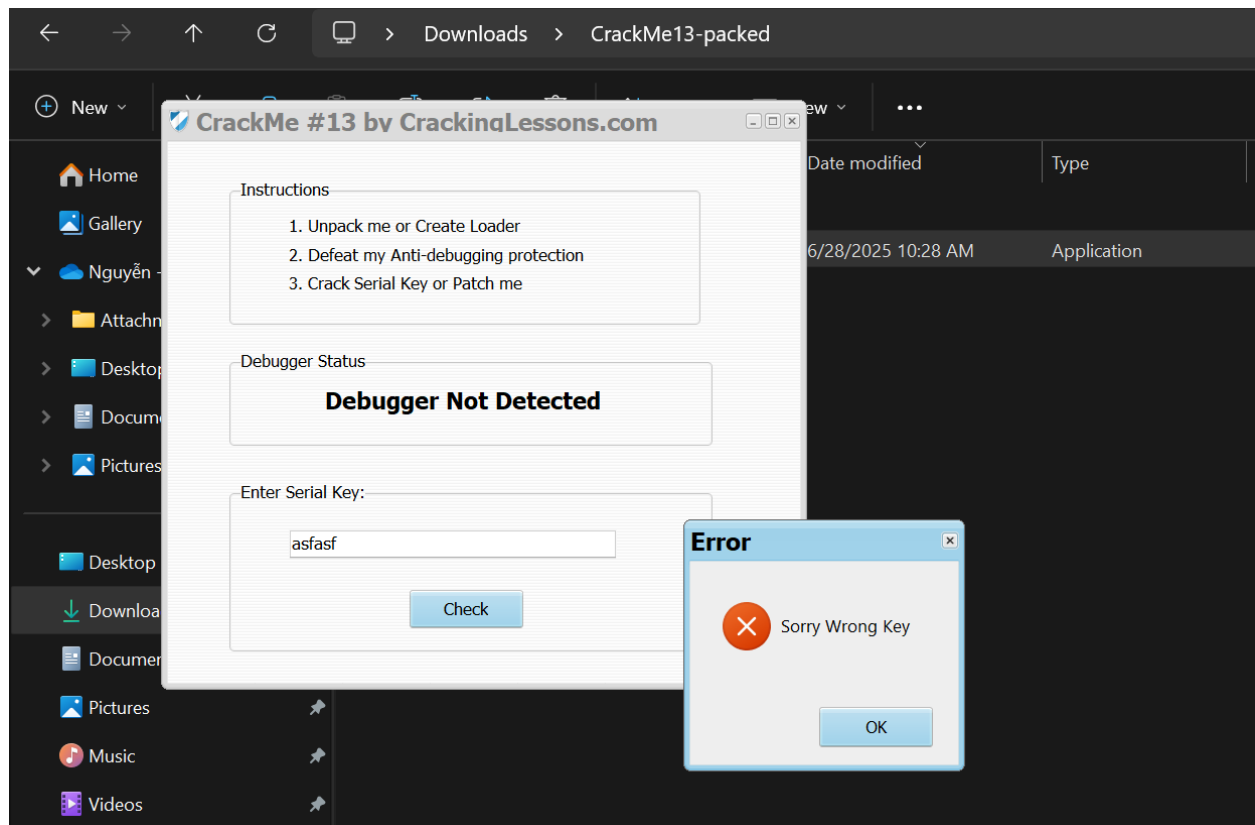
    Slot      Start      End      Length    Description
000: Meta     0000000000  0000000000  0000000001  Safety Table
001: -----  0000000000  0000002047  0000002048  Unallocated
002: Meta     0000000001  0000000001  0000000001  GPT Header
003: Meta     0000000002  0000000033  0000000032  Partition Table
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.{311b88a5-2f77-4118-a057-a3e0307fb5ac}
```

CRACK ME 13:

This CrackMe combines three features:

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



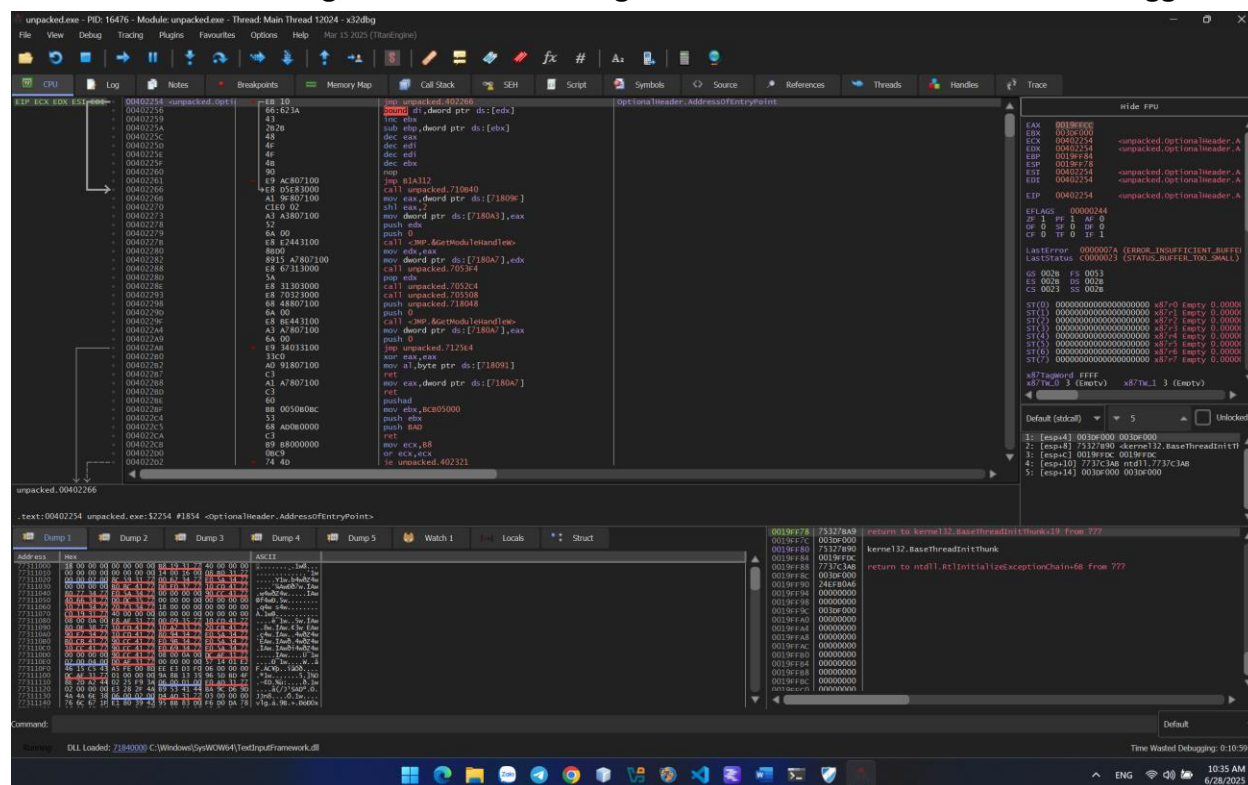
First we use UPX tools to unpacked this file .exe, since it's packed by these tool:

```
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

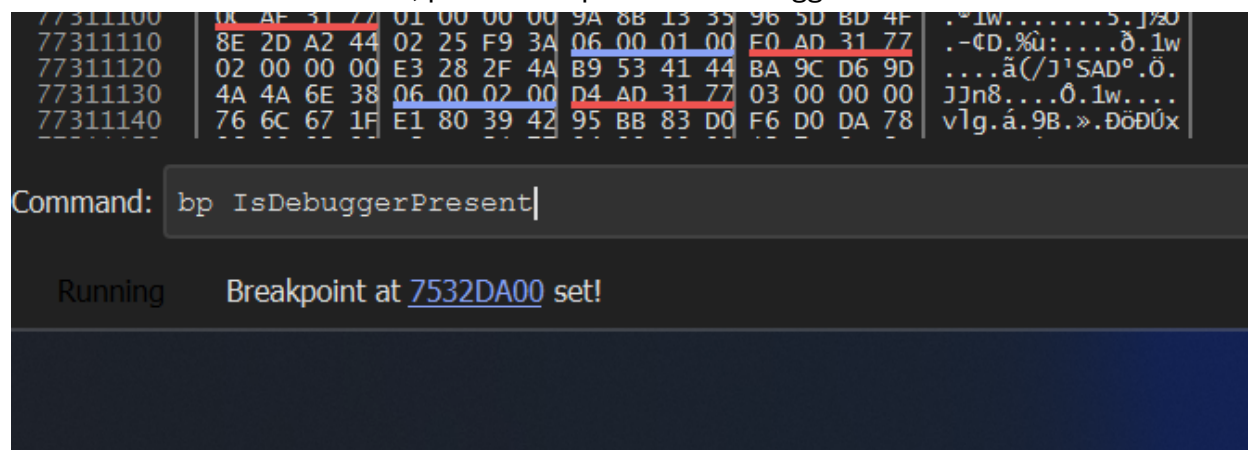
   File size   Ratio   Format   Name
-----
4103680 <- 1376768 33.55%  win32/pe  unpacked.exe

Unpacked 1 file.
C:\Users\Lenovo legion 5\Downloads\CrackMe13-packed>|
```

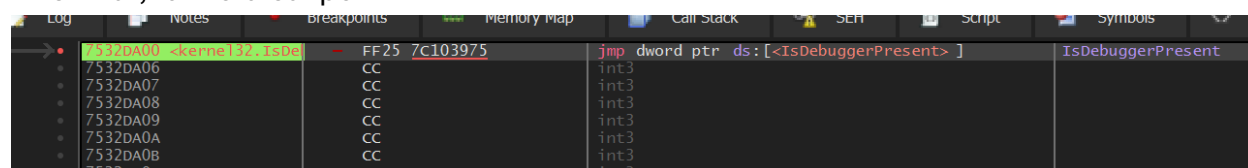
Next, move to solve the anti-debugging requirement, like the crackme 12 challenge, when throw this file to x32dbg, we can run to debug, because this file has been anti-debugged.



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:

00403866	8945 AC	mov dword ptr ss:[ebp-54],eax	[ebp-54]:00Unit10Finalize+70FA
00403869	837D AC 00	cmp dword ptr ss:[ebp-54],0	[ebp-54]:00Unit10Finalize+70FA
0040386D	74 3A	je unpacked.4038A9	
0040386F	A1 7C567200	mov eax,dword ptr ds:[72567C]	
00403874	8B00	mov eax,dword ptr ds:[eax]	
00403876	C745 B8 06000000	mov dword ptr ss:[ebp-48],6	
0040387D	C70424 10000000	mov dword ptr ss:[esp],10	
00403884	BA D8817100	mov edx,unpacked.7181D8	7181D8:"Program will now Quit"
00403889	B9 04827100	mov ecx,unpacked.718204	718204:"Debugger Detected"
0040388E	E8 4E2D3100	call unpacked.7165E1	
00403893	83EC 04	sub esp,4	
00403896	A1 7C567200	mov eax,dword ptr ds:[72567C]	
0040389B	8B00	mov eax,dword ptr ds:[eax]	
0040389D	C745 B8 07000000	mov dword ptr ss:[ebp-48],7	
004038A4	E8 53302700	call unpacked.6768FC	
004038A9	F645 F3 01	test byte ptr ss:[ebp-D],1	
004038AD	74 08	je unpacked.4038B7	
004038AF	8B45 EC	mov eax,dword ptr ss:[ebp-14]	[ebp-14]:"l=0"
004038B2	E8 252C3100	call unpacked.7164DC	
004038B7	8B75 EC	mov esi,dword ptr ss:[ebp-14]	[ebp-14]:"l=0"
004038BA	8D45 B0	lea eax,dword ptr ss:[ebp-50]	
004038BD	8D45 B0	mov dword ptr ss:[esp],eax	

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.

8945 AC	mov dword ptr ss:[ebp-54],eax	
837D AC 00	cmp dword ptr ss:[ebp-54],0	
EB 3A	jmp unpacked.4038A9	
A1 7C567200	mov eax,dword ptr ds:[72567C]	
8B00	mov eax,dword ptr ds:[eax]	
C745 B8 06000000	mov dword ptr ss:[ebp-48],6	
C70424 10000000	mov dword ptr ss:[esp],10	
BA D8817100	mov edx,unpacked.7181D8	
B9 04827100	mov ecx,unpacked.718204	
E8 4E2D3100	call unpacked.7165E1	

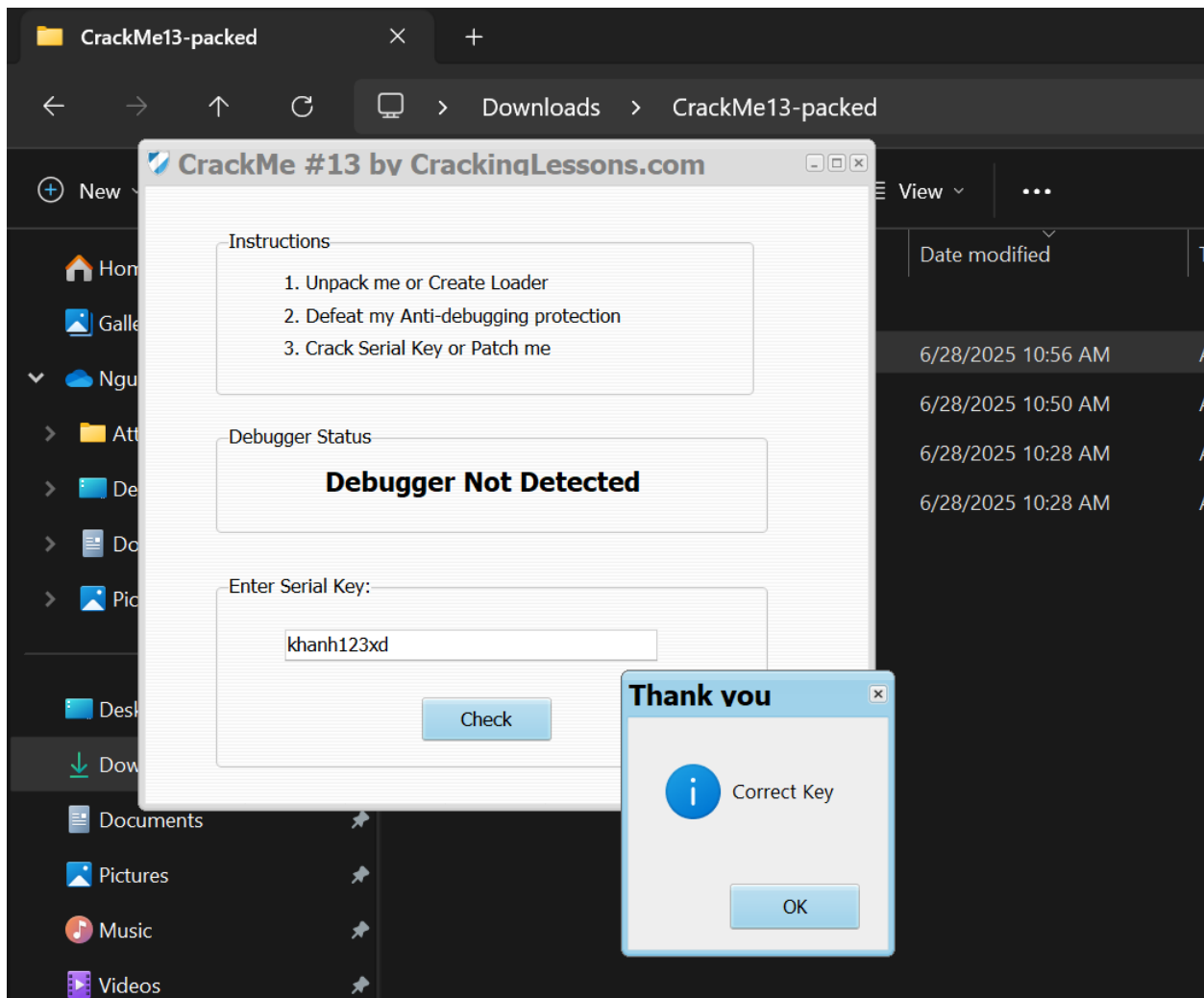
When anti anti-debugging successfully, we can find the serial key easily in address 00403A85:

00403A77	8D45 B4	lea eax,dword ptr ss:[ebp-4C]	eax:TpCallbackIndependent+140
00403A7A	E8 36203100	call debug.715AB5	
00403A7F	8D45 F0	lea eax,dword ptr ss:[ebp-10]	eax:TpCallbackIndependent+140
00403A82	890424	mov dword ptr ss:[esp],eax	[esp]:TpCallbackIndependent+478, eax:TpCallbackIndependent+140
00403A85	C74424 04 28827100	mov dword ptr ss:[esp+4],debug.718228	718228:"ABC-123456"
00403A8D	E8 0E283100	call debug.7162A0	
00403A92	C745 BC 02000000	mov dword ptr ss:[ebp-44],2	
00403A99	8D45 F0	lea eax,dword ptr ss:[ebp-10]	eax:TpCallbackIndependent+140
00403A9C	894424 04	mov dword ptr ss:[esp+4],eax	eax:TpCallbackIndependent+140
00403AA0	8D45 EC	lea eax,dword ptr ss:[ebp-14]	eax:TpCallbackIndependent+140

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

20 00 71 00	71 00 67 00	74 00 00 00	44 00 01 00	.Q.u.i.t...D.e
62 00 75 00	67 00 67 00	65 00 72 00	20 00 44 00	b.u.g.g.e.r. .D.
65 00 74 00	65 00 63 00	74 00 65 00	64 00 00 00	e.t.e.c.t.e.d..
6B 68 61 6E	68 31 32 33	78 64 00 00	43 00 6E 00	khanh123xd..C.o
72 00 72 00	65 00 63 00	74 00 20 00	48 00 65 00	r.r.e.c.t. .K.e
79 00 00 00				y...T.h.a.n.k. .
79 00 6F 00	[0071821B] = 63006500 (User Data)			y.o.u...S.o.r.r.
79 00 20 00	57 00 72 00	6E 00 6E 00	67 00 20 00	y. .W.r.o.n.g. .
48 00 65 00	79 00 00 00	45 00 72 00	72 00 65 00	K.e.y...F.e.r.r.

I change ABC-123456 to khanh123xd

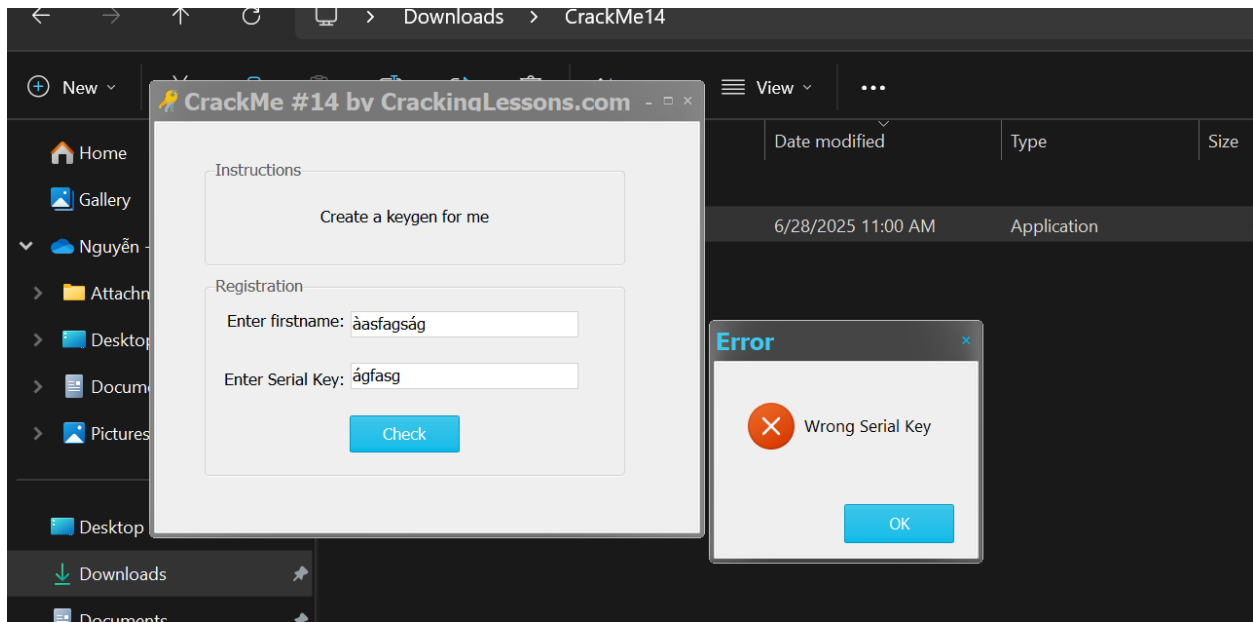


DONE!!!

CRACK ME 14:

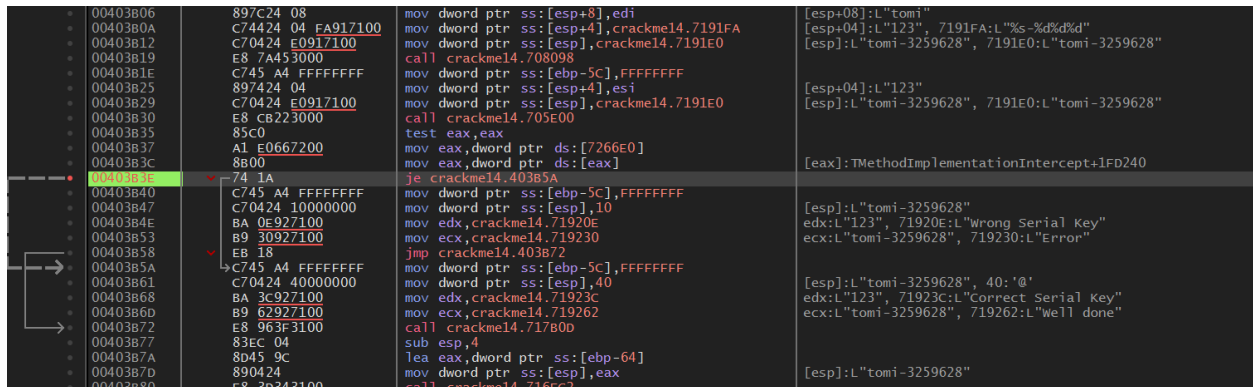
This CrackMe asks for your firstname and then generates a Serial Key based on your firstname.

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”

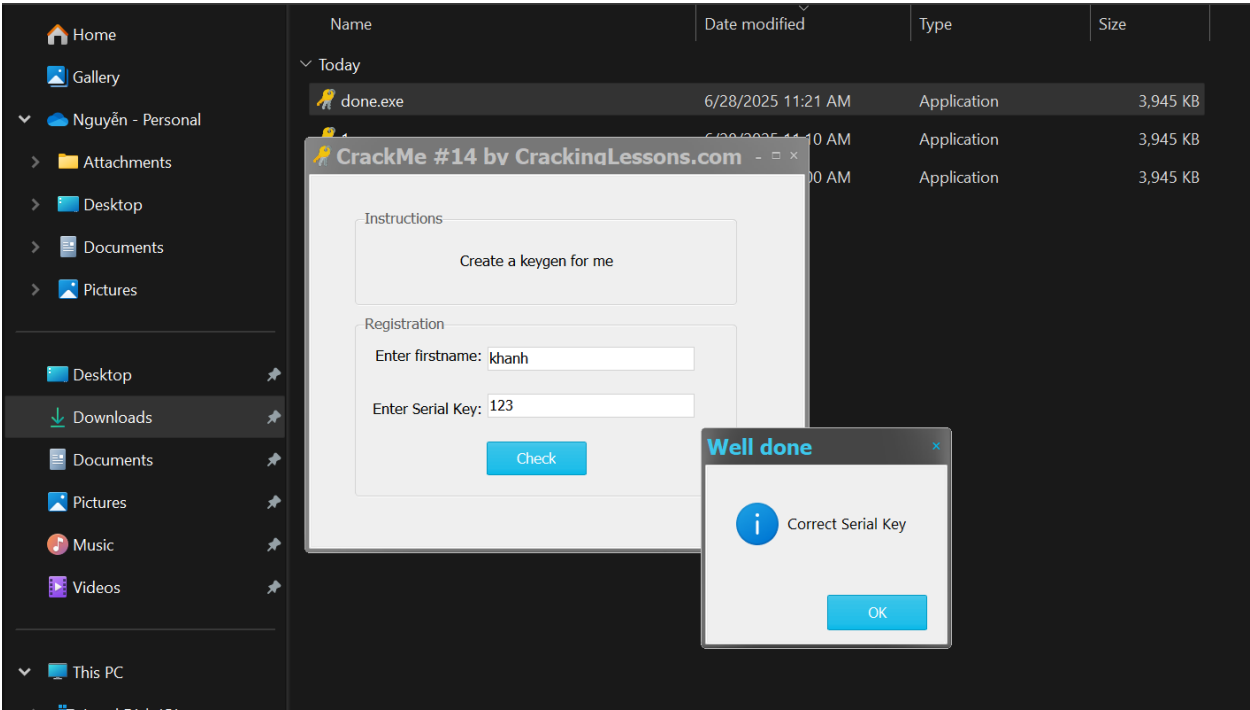


As you see, in address 00403B3E, this JE command will jump to the correct status if the code above Test eax, eax is set ZF flag when eax is 0. But follow the result, we know that,

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

00403B35	85C0	test eax, eax	
00403B37	A1 E0667200	mov eax, dword ptr ds:[7266E0]	
00403B3C	8B00	mov eax, dword ptr ds:[eax]	[eax]:TMethodImplementationIntercept+1FD240
00403B3E	EB 1A	jmp crackme14.403B5A	
00403B40	C745 A4 FFFFFFFF	mov dword ptr ss:[ebp-5C], FFFFFFFF	[esp]:L"tomi-3259628"
00403B47	C70424 10000000	mov dword ptr ss:[esp], 10	edx:L"123", 71920E:L"Wrong Serial Key"
00403B4E	BA 0E927100	mov edx, crackme14.71920E	ecx:L"tomi-3259628", 719230:L"Error"
00403B53	B9 30927100	mov ecx, crackme14.719230	
00403B58	EB 18	jmp crackme14.403B72	
00403B5A	C745 A4 FFFFFFFF	mov dword ptr ss:[ebp-5C], FFFFFFFF	
00403B61	C70424 40000000	mov dword ptr ss:[esp], 40	[esp]:L"tomi-3259628", 40:'@'
00403B68	BA 3C927100	mov edx, crackme14.71923C	edx:L"123", 71923C:L"Correct Serial Key"
00403B6D	B9 62927100	mov ecx, crackme14.719262	ecx:L"tomi-3259628", 719262:L"Well done"
00403B72	E8 963F3100	call crackme14.717B0D	
00403B77	83EC 04	sub esp, 4	
00403B7A	8D45 9C	lea eax, dword ptr ss:[ebp-64]	

Pachh file and check:



DONE!!!