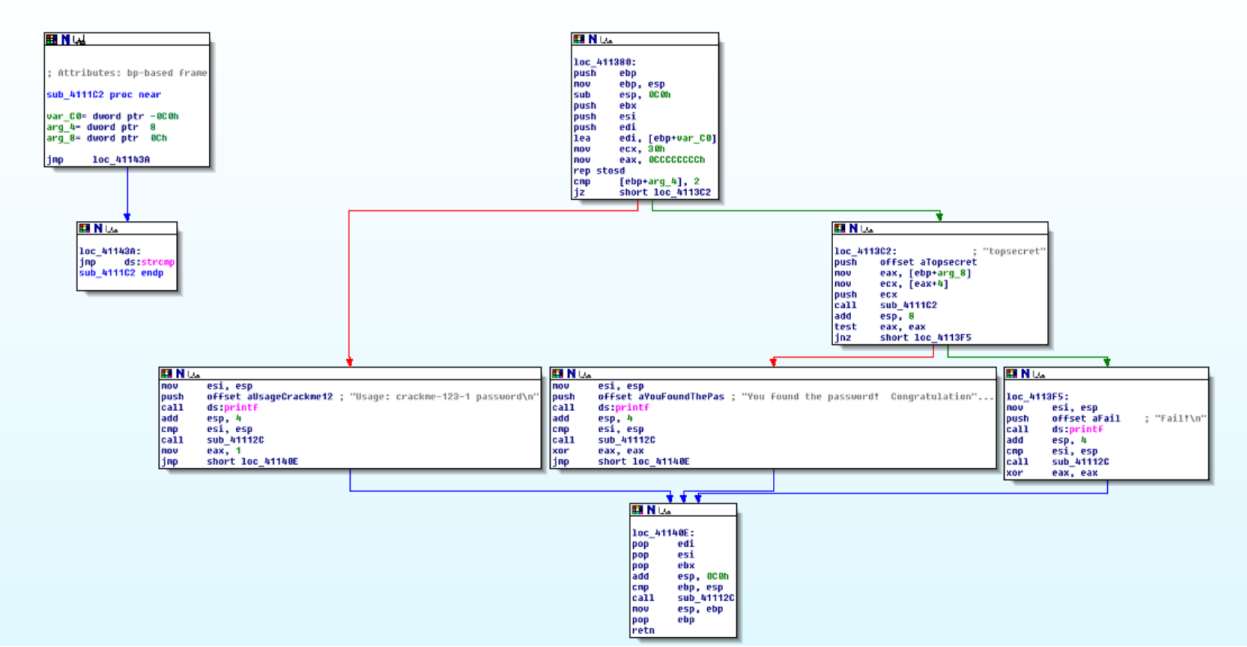
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

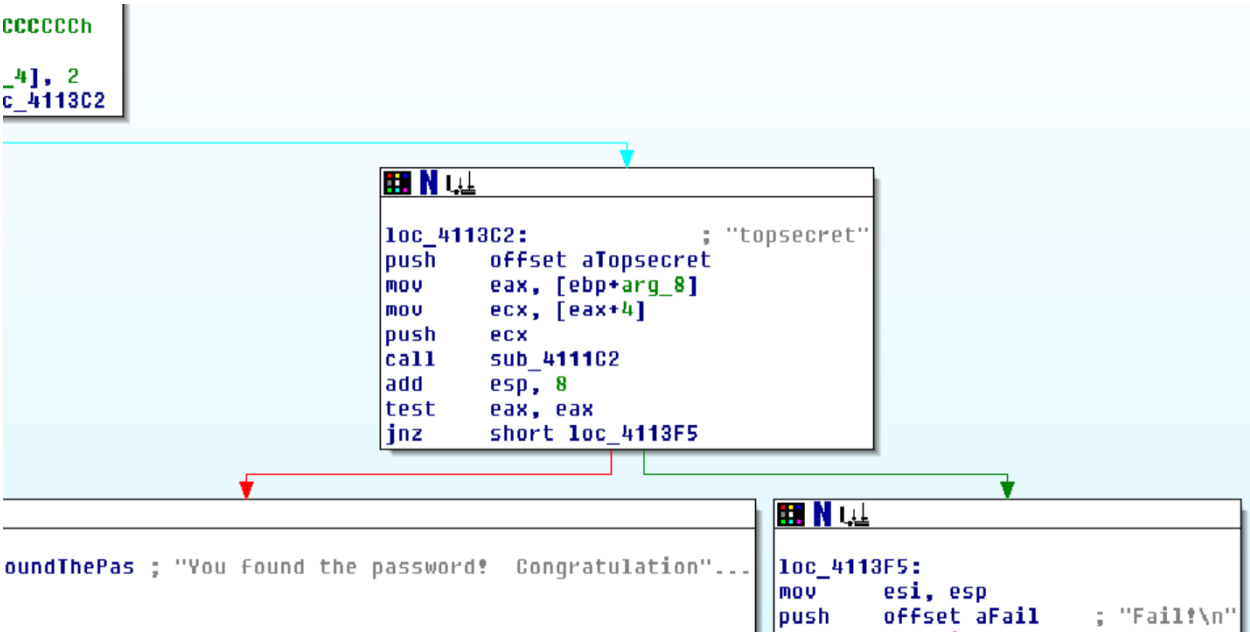
LAB 15: Reverse Engineering with IDA Pro Freeware

Viewing Disassembled Code

Crackme-121-1.exe:



Drag the "View-A" screen to show module "B", as shown below:

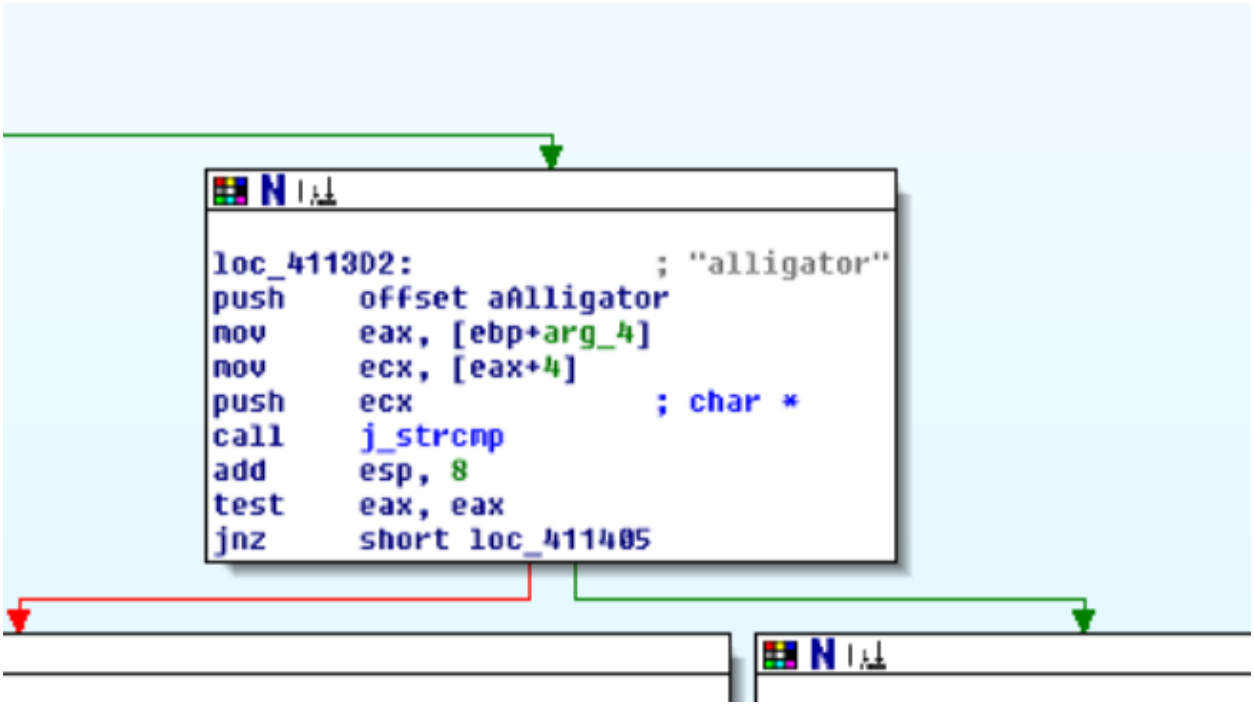


Running the Executable

```
C:\Users\Lenovo legion 5\Downloads\test>crackme-121-1.exe
Usage: crackme-123-1 password

C:\Users\Lenovo legion 5\Downloads\test>crackme-121-1.exe wrongpassword
Fail!

C:\Users\Lenovo legion 5\Downloads\test>crackme-121-1.exe topsecret
You found the password!  Congratulations!

C:\Users\Lenovo legion 5\Downloads\test>
```

Crackme-121-2.exe:

Load the executable in IDA Pro and Find the module containing the password, and save a screen capture of it:



Run the program at a command prompt and save an image of it congratulating you for finding the password:

```
C:\Users\Lenovo legion 5\Downloads\test>crackme-121-2.exe alligator
You found the password!  Congratulations!

C:\Users\Lenovo legion 5\Downloads\test>
```

Crackme-121-3.exe:

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

Load the executable in IDA Pro and Find the modules containing the passwords, and save a screen capture of them:

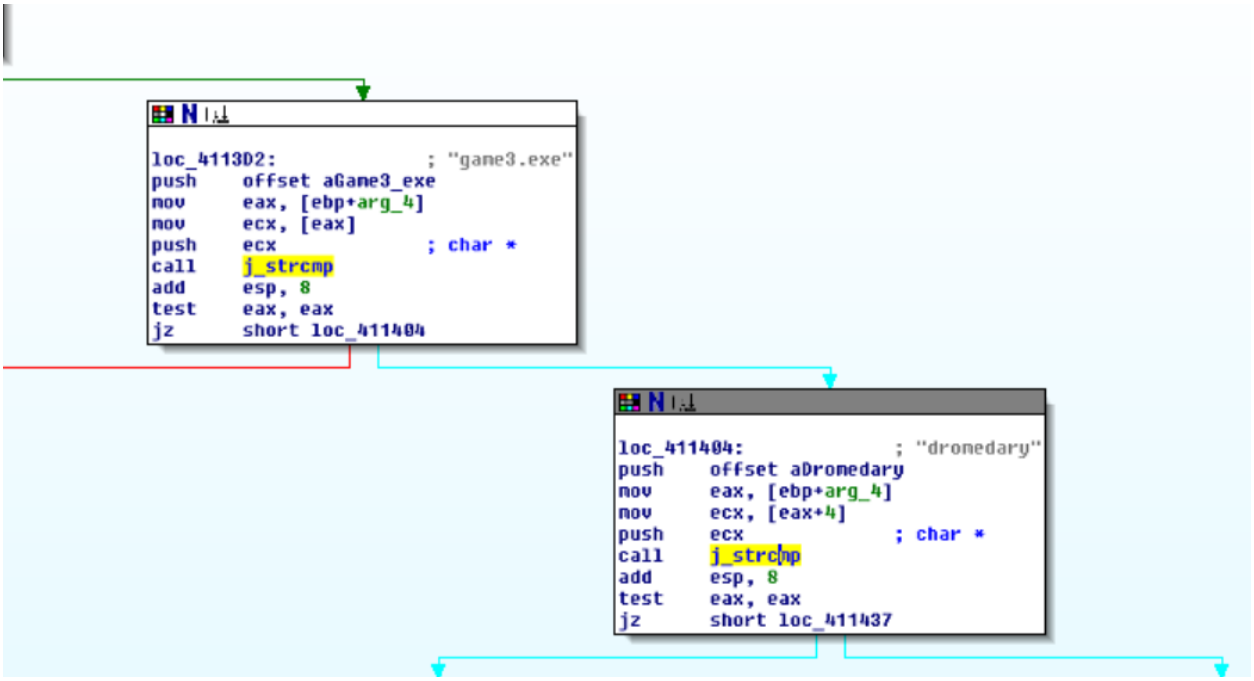
Run the program at a command prompt and save an image of it congratulating you for finding the passwords:

```
C:\Users\Lenovo legion 5\Downloads\test>crackme-121-3.exe sufferring succotash
Fail!  First word was wrong!

C:\Users\Lenovo legion 5\Downloads\test>crackme-121-3.exe suffering succotash
Congratulations!  You found the passwords!

C:\Users\Lenovo legion 5\Downloads\test>
```

Crackme-121-4.exe:

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

Load the executable in IDA Pro and Find the modules that perform string comparisons (strcmp) and try to guess what they are referring to:



Run the program at a command prompt and save an image of it congratulating you for solving the puzzle:

```
C:\Users\Lenovo legion 5\Downloads\test>game3.exe dromedary
Congratulations!  You solved the crackme puzzle!

C:\Users\Lenovo legion 5\Downloads\test>
```

Note: because crackme-121-4.exe is not match the note of "use age" so I change file name to game3.exe and receive the successful result above.

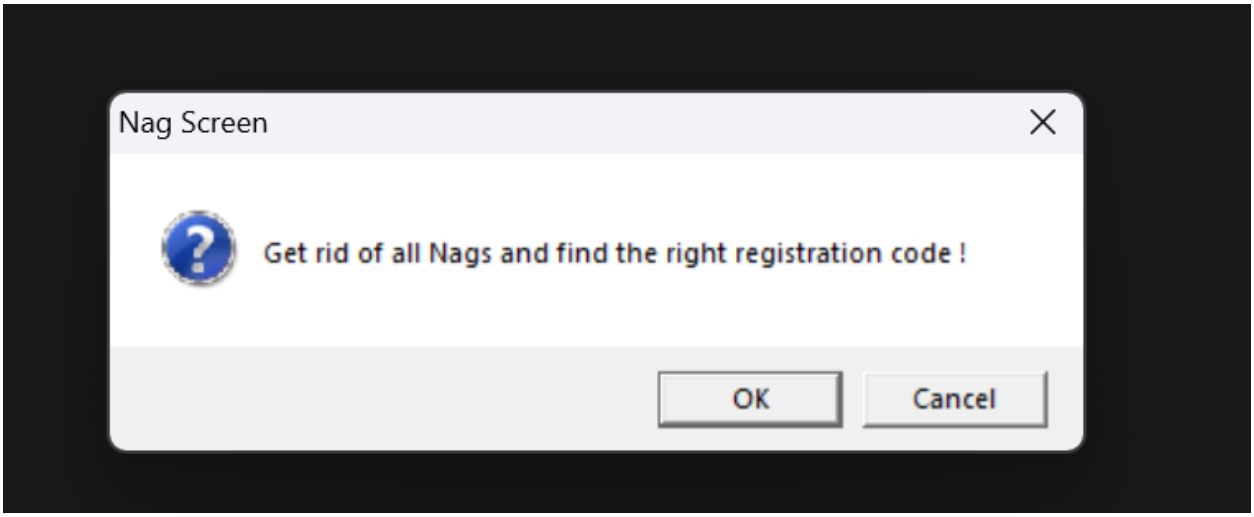
```
C:\Users\Lenovo legion 5\Downloads\test>crackme-121-4.exe
Usage: game3.exe password

C:\Users\Lenovo legion 5\Downloads\test>
```

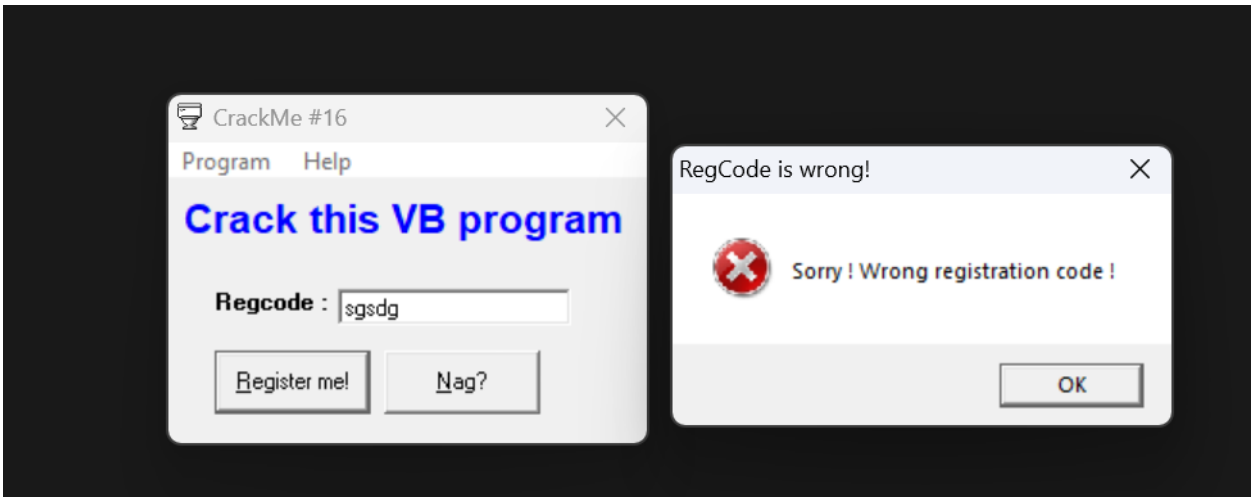
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

CRACKME 16

This crackme is created with Visual Basic 5/6 which is prior to the .NET framework. Some programs out there are still written in it. So here's your opportunity to crack such a program. It is a mod of one of Lena's VB programs. Note that this crackme is compiled to native format. The p-code format will be covered in another crackme.

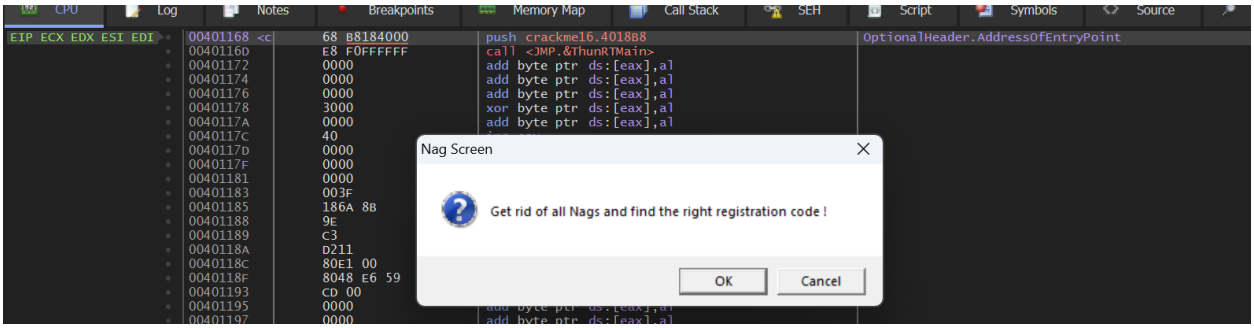
1. Get rid of the Nag screen which pops-up before the above window shows.
2. Crack the Regcode.



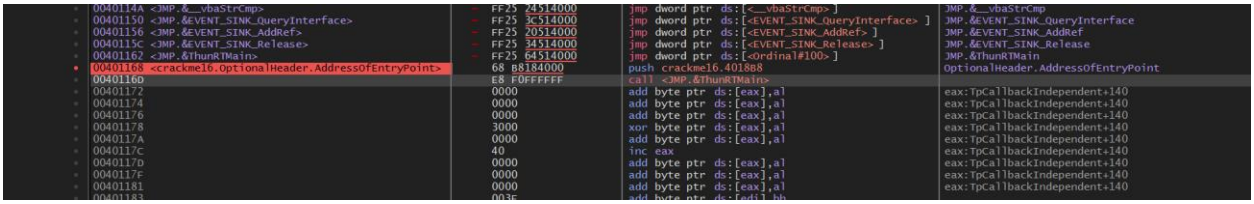


NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

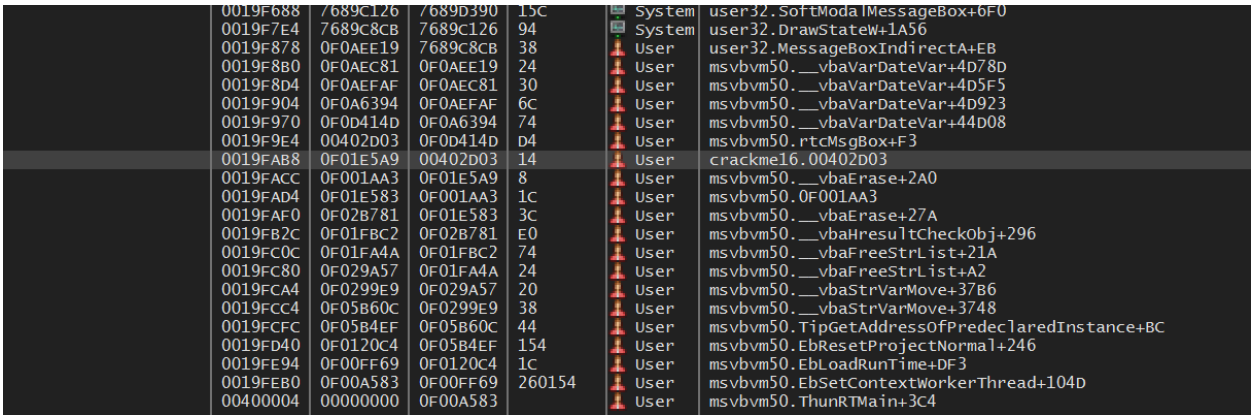
First, push the code to x32dbg and run to view the code call the Nag



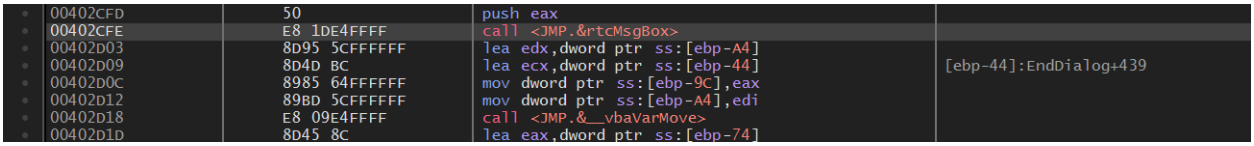
Notice the Call <JMP.&ThuRTMain>, that line of code call stack to display the NAG screen, because when we run to display NAG, CPU reaches to this code.

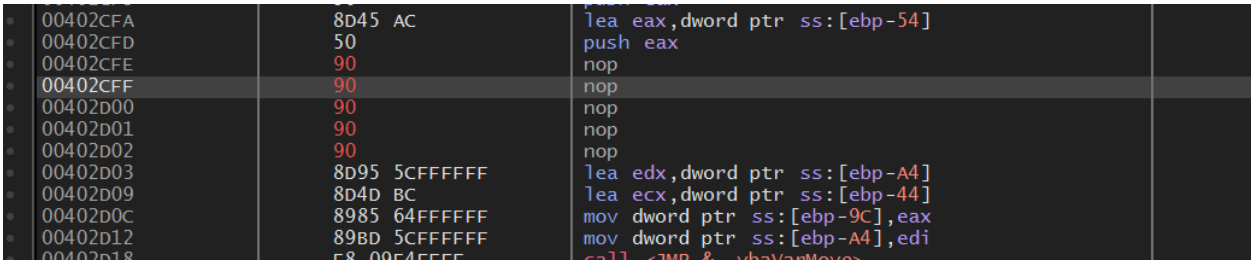


View call stack to see the code call the NAG screen, crackme16.00402D03 is the stack part call the NAG screen:

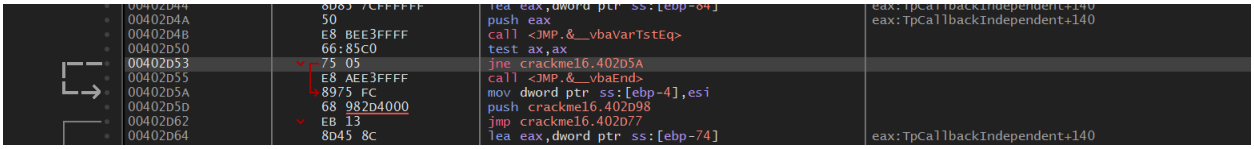


Click to this code to view detaily, address 00402CFE executes to display NAG screen so I fill with nop in this line.





Patch and run again to check, we have problem that the program quit immediately so i we continute to trace below this code to see what happen:



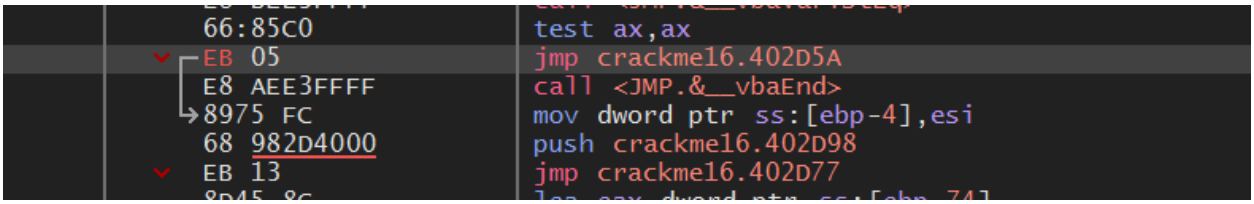
Below the previous NOP, we catch this part of code:

Test ax, ax

Jne crackme16.402D5A => this code not execute because, the previous test is equal.

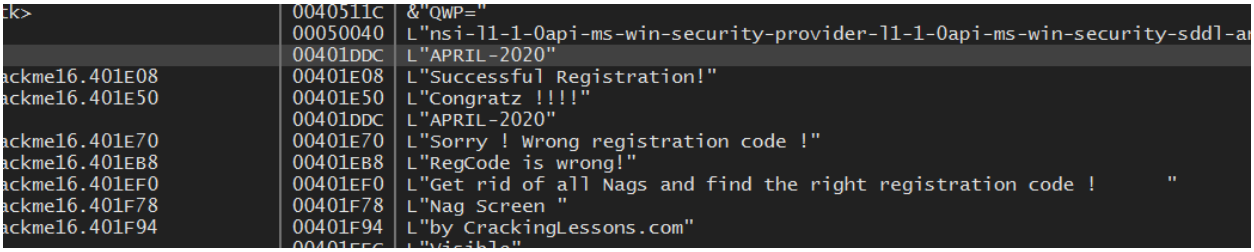
Call <JMP.&__vbaEnd> => this cause program closed immediately.

So I change to JNE to JMP to pass the Call below.

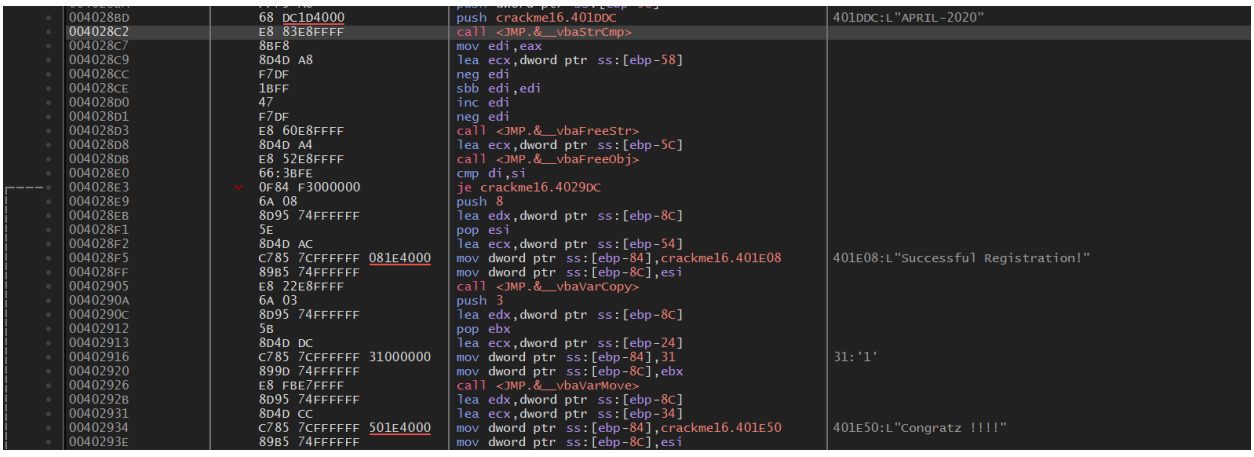


This is done of removing NAG.

To crack regcode, we find to string references to see the the hint:



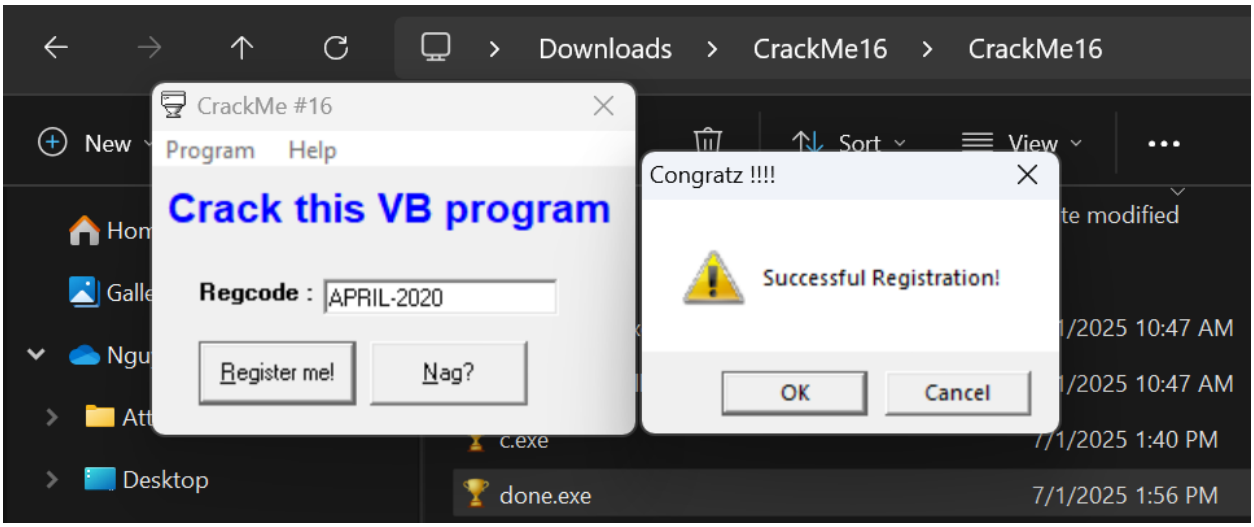
We found that string “APRIL-2020”, but let inspect to the code to view detaily:



NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

Below the code of string APRIL-2020, program call the vbaStrCmp, that is the logic comparing our input with regcode (possibly APRIL-2020).

We try to patch the code and run to check:



DONE!!!