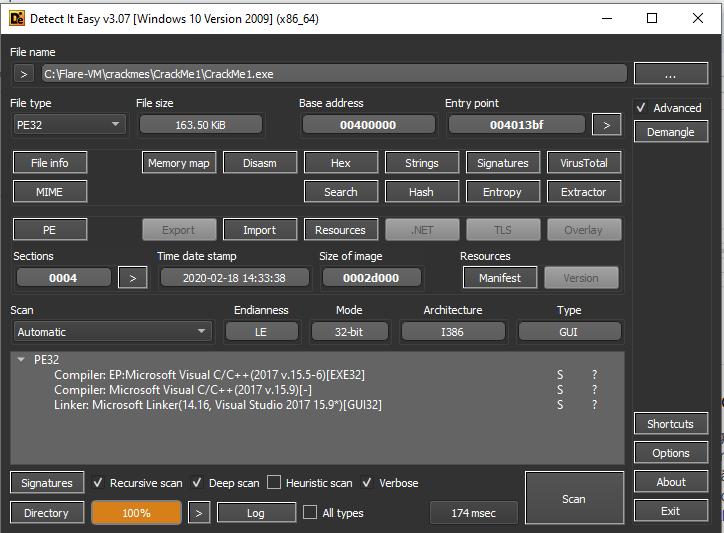
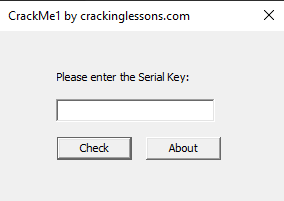
Open crackme1 with DIE:



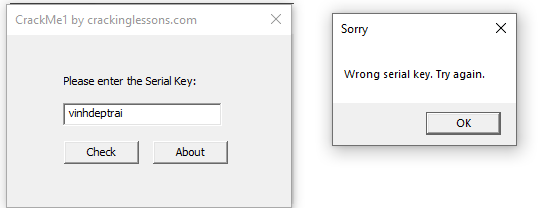
PE32 bit file -> using x32dbg

Run crackme1 first:



It requires enter a serial key to check

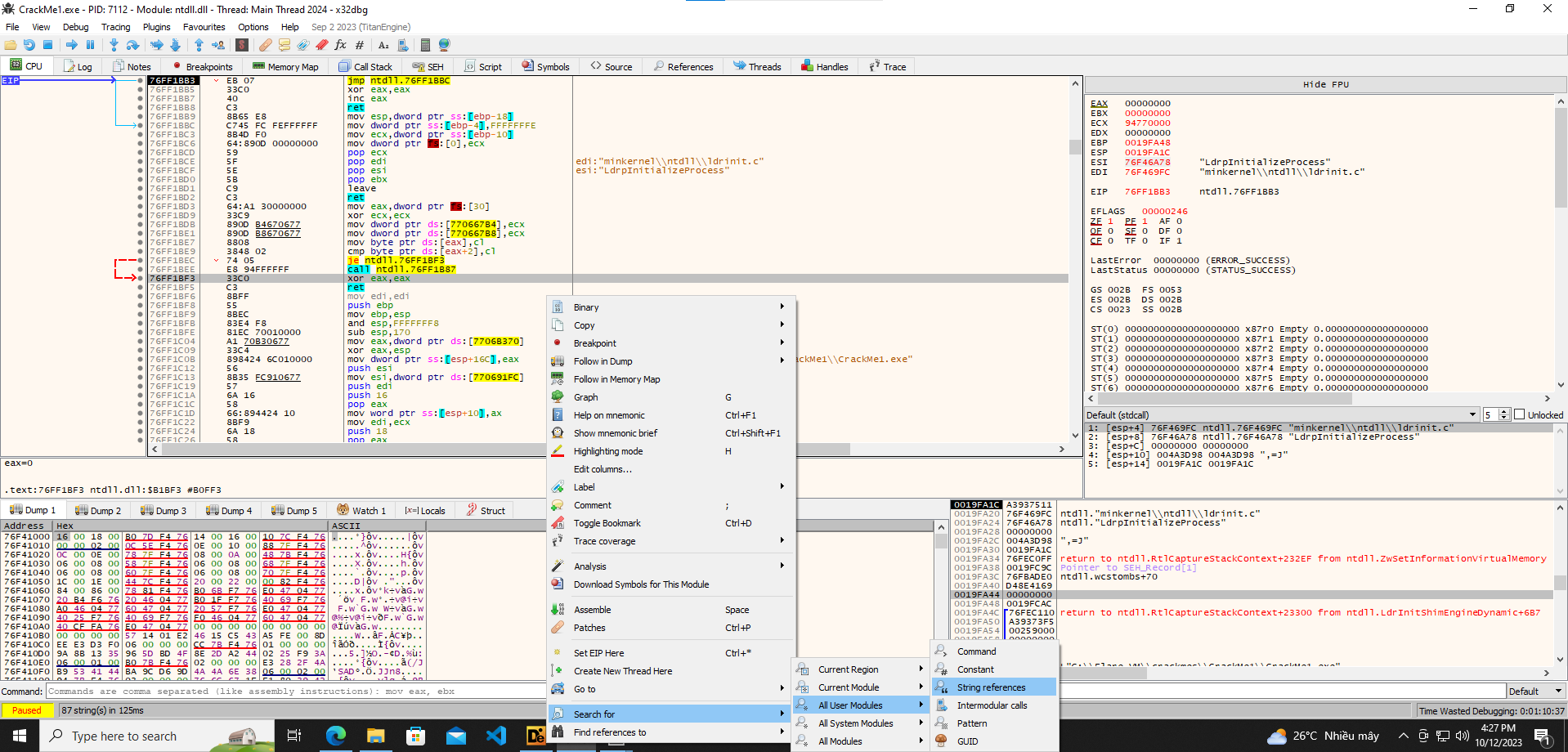
Test with some random key:

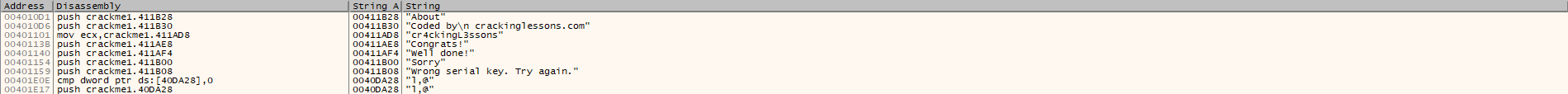


It checks key and pops up a window to tell wrong or correct key

Throw it into x32dbg

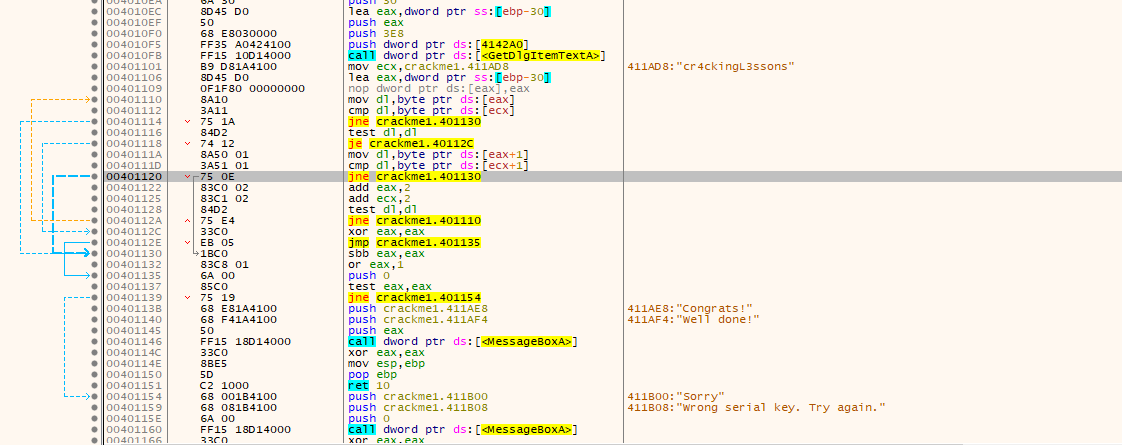
Using search for task of x32dbg, select find all strings references

we get:

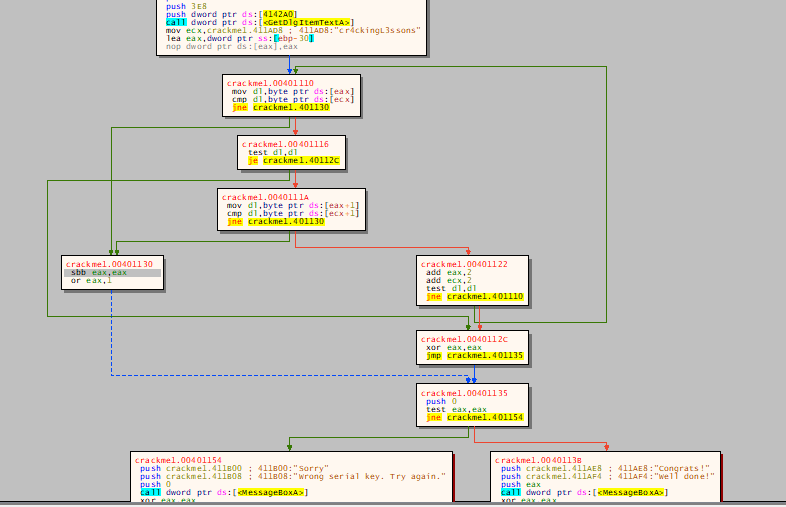


Found some strings we met before when run program and some related strings like “Well Done!”

double click to string to go to where the program use these strings



press G to show logical graph of this code



first it call GetDlgItemTextA: this is an API to get input from a box which is our input serial key

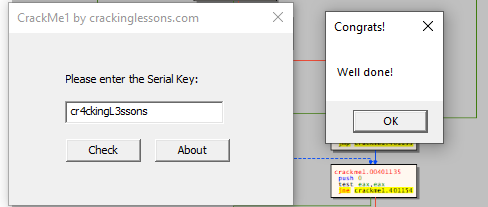
the address of input key is stored in eax

new it loads a string “cr4ckingL3ssons” into a register ecx

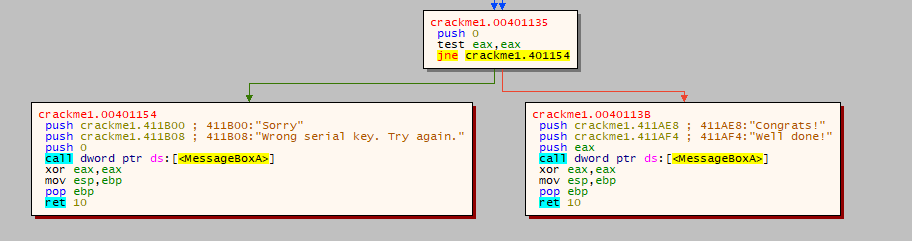
next it compares byte by byte of two strings, if they are the same, Congrats and Well done ! will be shown otherwhile Sorry Wrong serial key. Try again will

===> **can conclude that the correct serial key is: cr4ckingL3ssons**

Check:



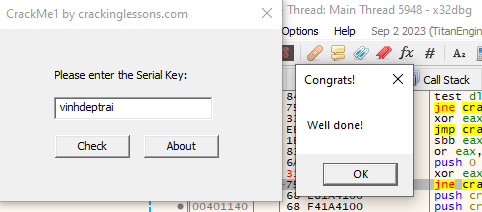
To make the crackme always show Well done tag



it takes a test eax, check whether eax = 0 or not, if it equal zero, Well done will be shown

so we can path test eax, eax to xor eax, eax which always make zero flag set, so we can always jump to Well done!

Check:



Now it seems very good :))