Bs”d

WHITE UP

**Objective**:

To answer the following questions:

1. In what function the first printed string is referenced?
2. What is the secret message?
3. Write a python/c/cpp simulator of the main functionality of the program.

**Topics Covered:**

X32dbg

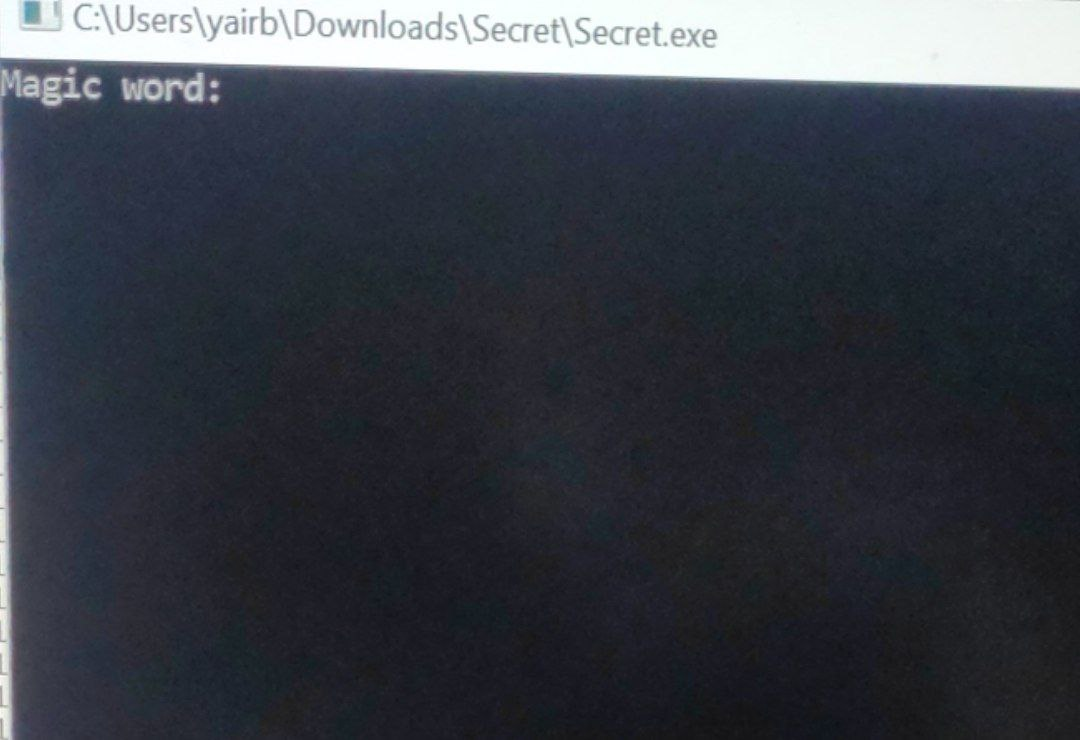
Reversing

Dynamic analyzing

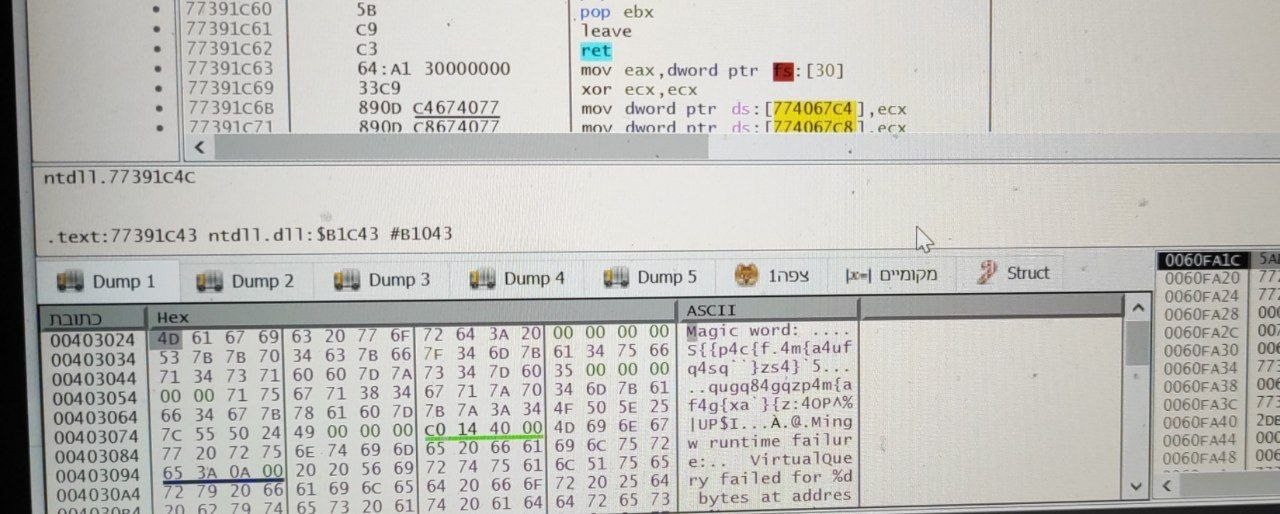
**Procedure:**

Here are the ideas on how to solve this challenge :D. Let’s perform dynamic analysis on the exe file by using x32dbg in windows machine (my favorite debugging tools).

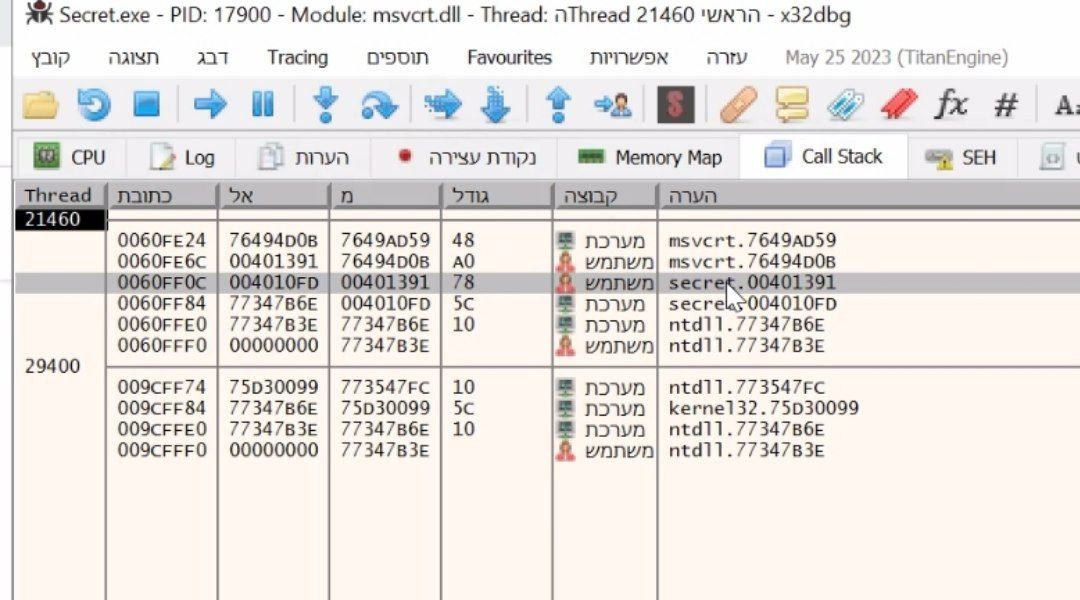
My first step was to run the file to find a string output that will help me to find the main func.



After I found it out, I opened x32dbg memory map >> find pattern >> and searched for “Magic”.

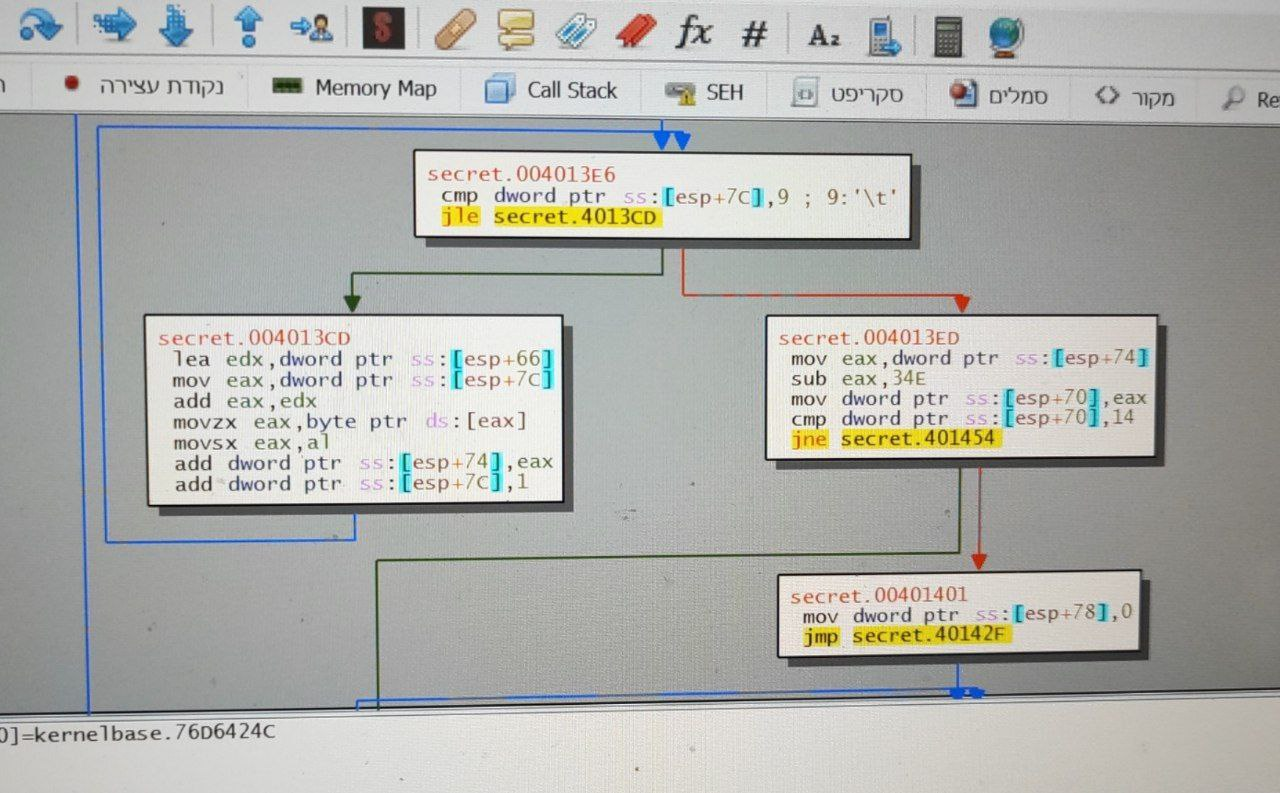


I found the string in the file. After that I set a breaking point on the first byte to find the function that the string is referenced in. after I ran the program I got to this window:

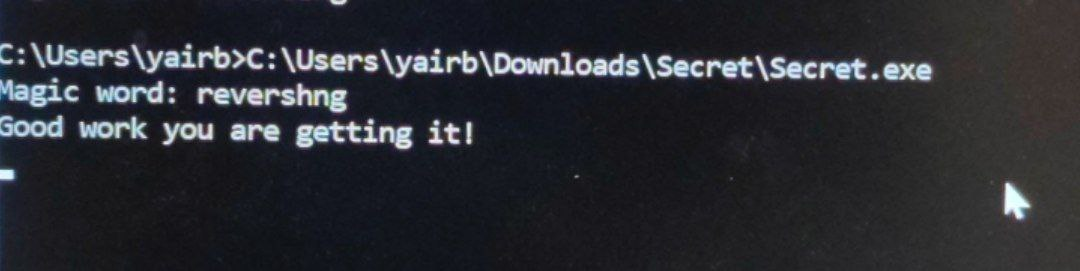


**I searched the user addresses that find the main function – and found out it was the third address.**

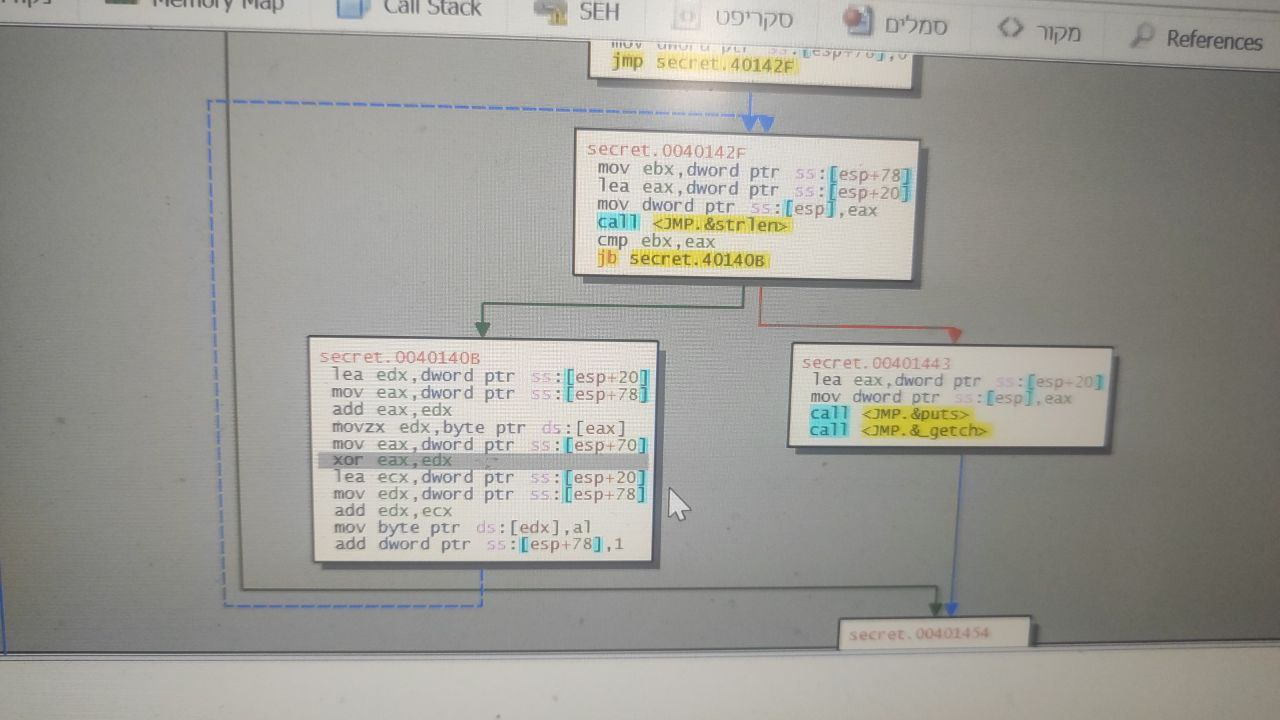
After I found the right function, I zoomed out to graphic mode and started to debag the code to find out the secret message and what he is doing. I started to look into the code and understood there is a loop that sums up all of the ascii value of the input – except for the first one and till the ninth



. After the loop is done we are subtracting 0x34E from the sum variable and compering it to 0x14. So, I checked out for words with 34e+14 sum value in ascii and for my surprise “revershng” is one of them. I entered revershng as the Magic word and revealed the secret message.



After I looked into the function that prints the message(in the picture below), I understood that the message is encrypted by xor 0x14 operation. I debagged the loop and found that the encrypted message was "S{{p4c{f4m{a4ufq4sq}zs4}`5".



After I knew exactly what SECRET is doing, I coded the same in cpp.

That’s all for the write up, I hope you guys did enjoy my second ever write up on reverse engineering challenge. Cheers! I’m also hope that i can continue to publish some write up for the interesting challenges in the future**.**

נ.ב. הצילום מסך במחשב משום מה לא עבד חלק מהזמן אז יש תמונות מהטלפון - סורי על האיכות.