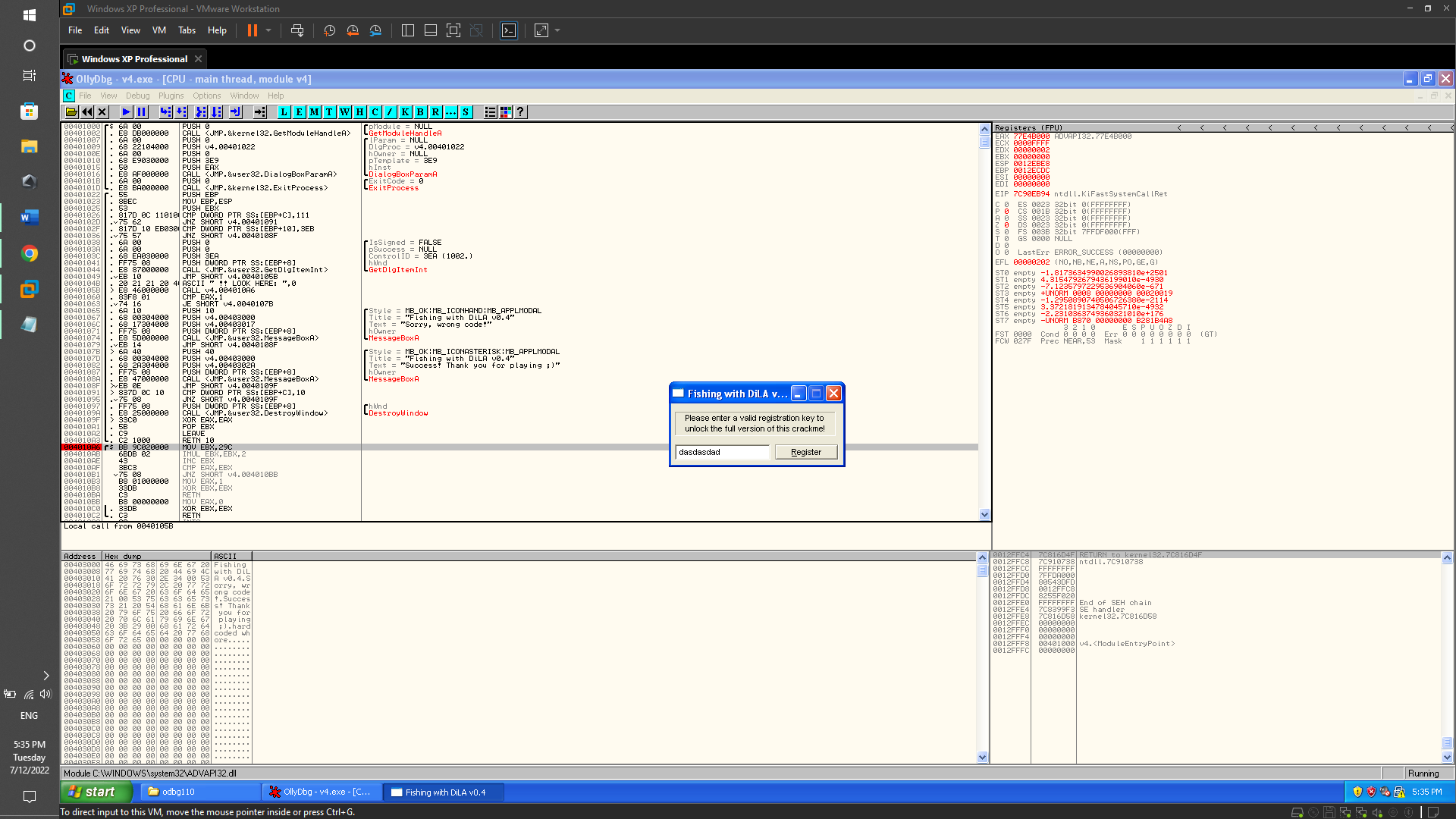
LAB 12

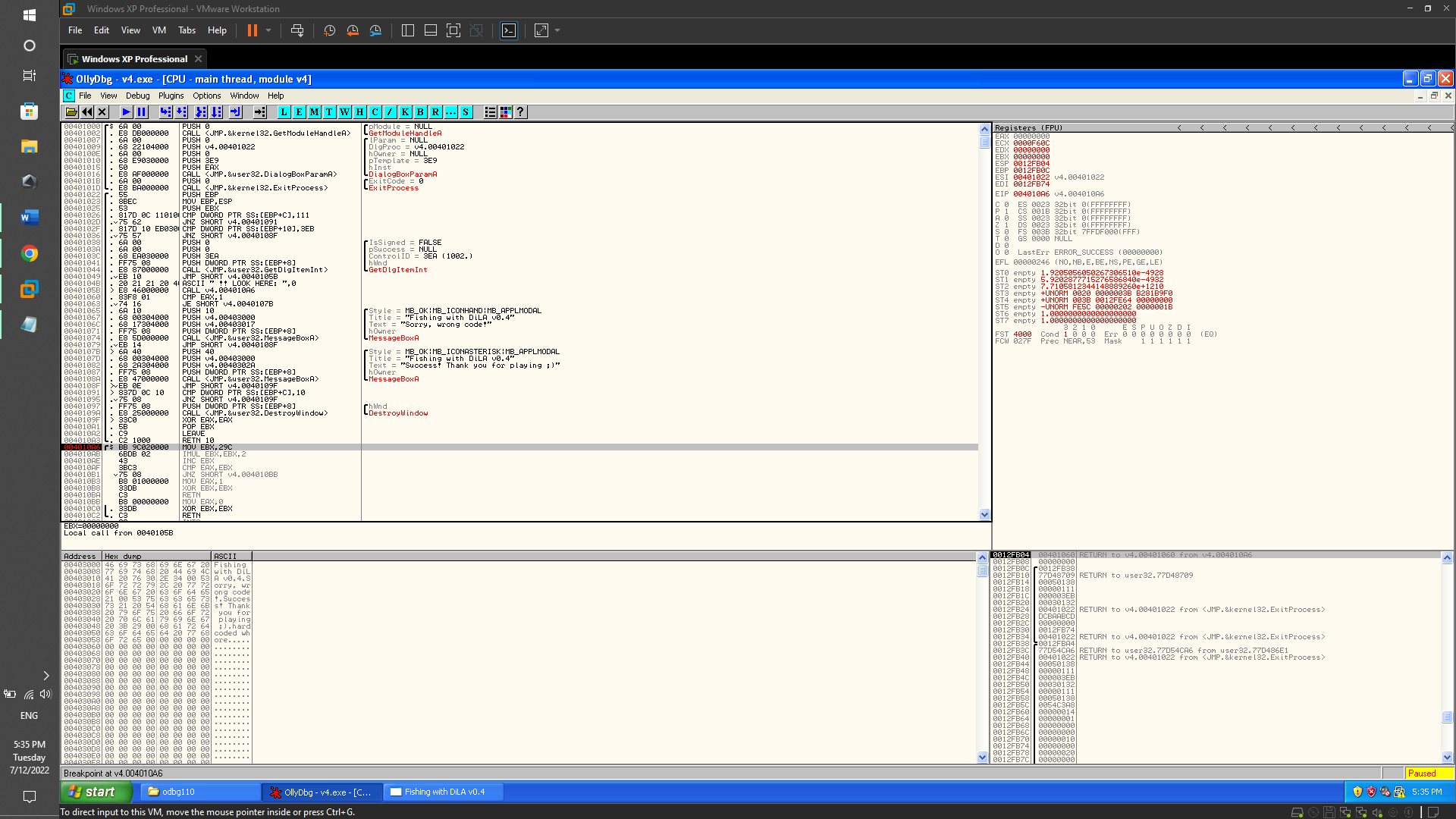
Nguyễn Thanh Hoài Lộc – SE151250

Part 1:

F9 để chạy thử chương trình.



Nhập ngẫu nhiên password và ta thấy chương trình được thực thi.

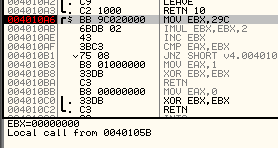


0040105B |> E8 46000000 CALL v4.004010A6 <- move to the EBX the value 0x539 (1337)

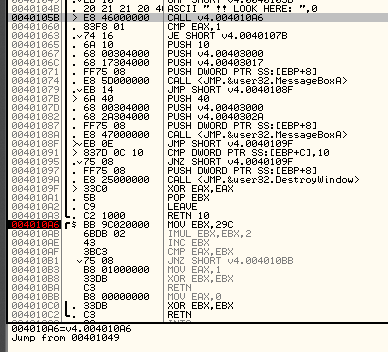
00401060 |. 83F8 01 CMP EAX,1 <- if the (serial = 0x539)

00401063 |. 74 16 JE SHORT v4.0040107B <- else

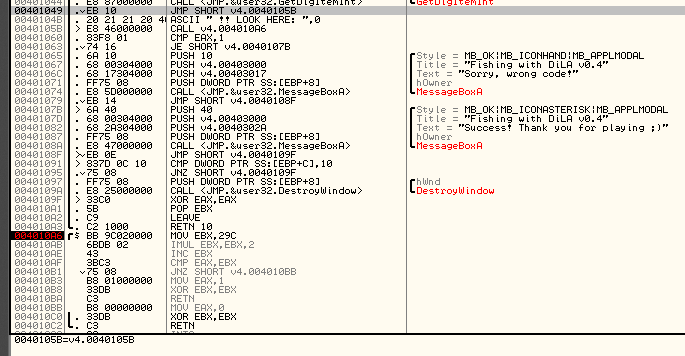
Call from 0040105B



Jump from 00401049



0040105B=v4.0040105B



004010A6 /$ BB 9C020000 MOV EBX,29C <- move to the EBX the value 0x29C (EBX = 0x29C)

004010AB |. 6BDB 02 IMUL EBX,EBX,2 <- multiply the EBX by 2 (EBX = EBX \* 2)

004010AE |. 43 INC EBX <- incrementate the EBX register by 1 (EBX = EBX + 1)

004010AF |. 3BC3 CMP EAX,EBX <- if the (serial = 0x539), show the goodboy message

004010B1 |. 75 08 JNZ SHORT v4.004010BB <- else show the badboy message

004010B3 |. B8 01000000 MOV EAX,1

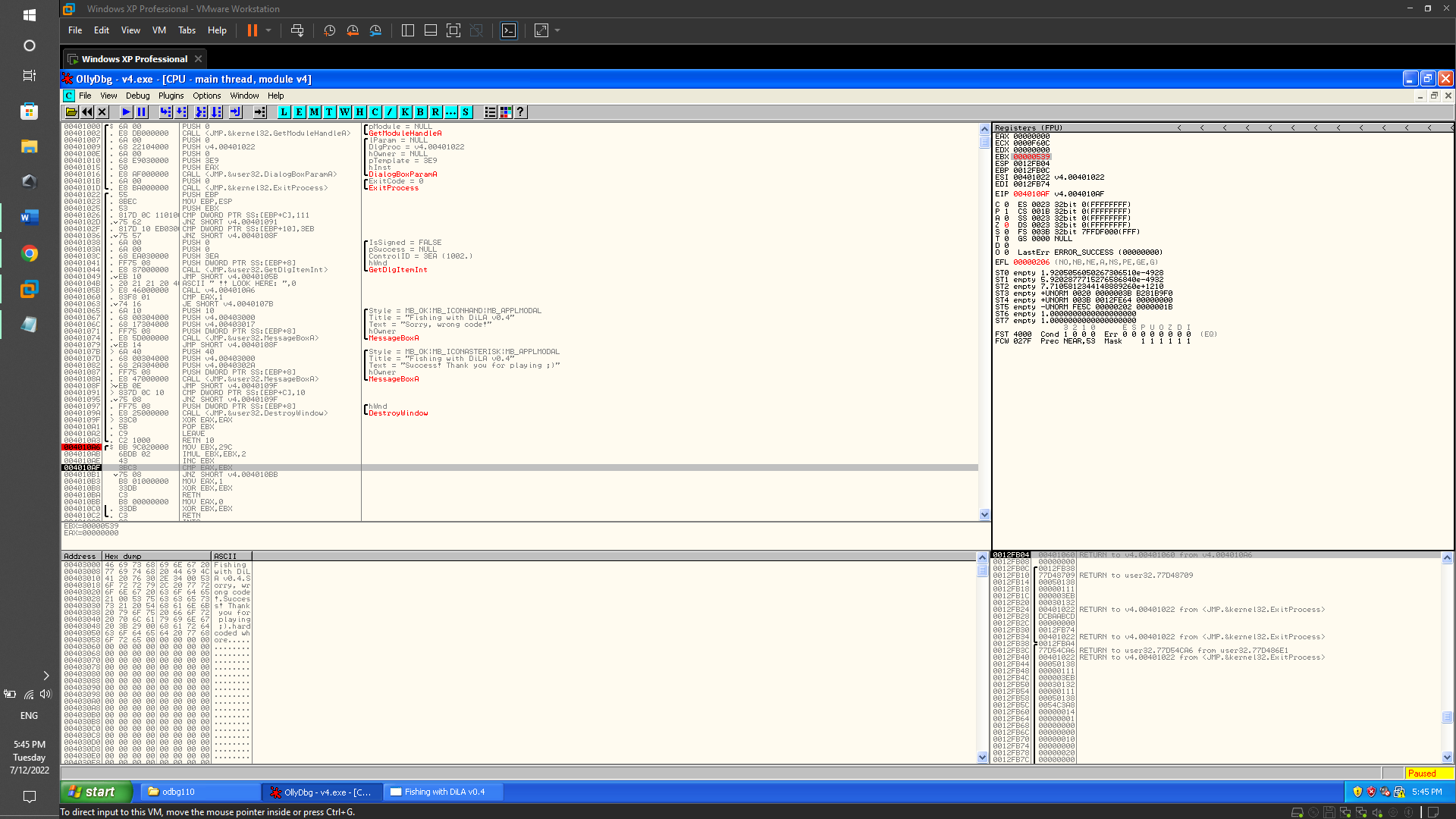
004010B8 |. 33DB XOR EBX,EBX

004010BA |. C3 RETN

004010BB |> B8 00000000 MOV EAX,0

004010C0 |. 33DB XOR EBX,EBX

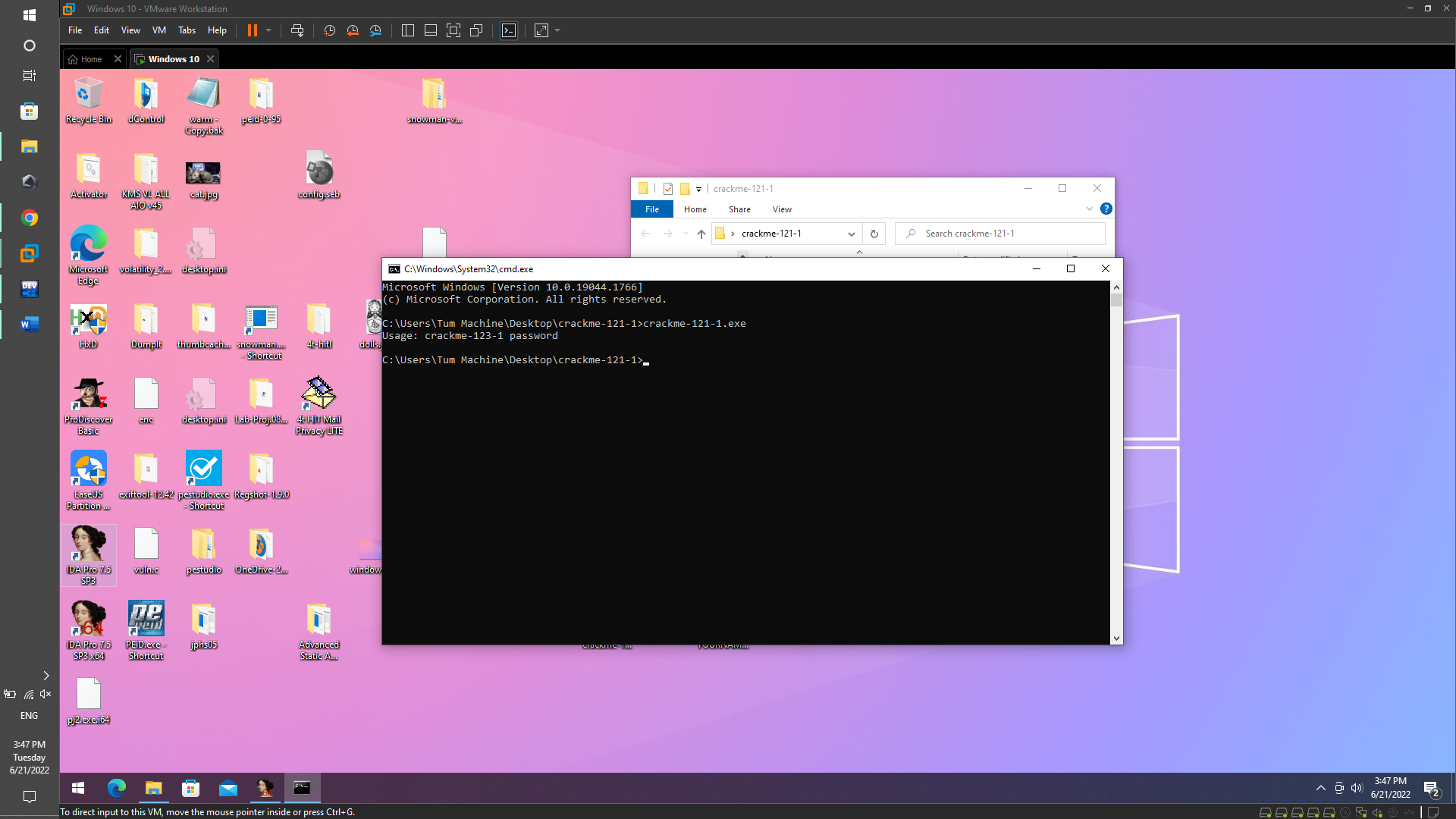
004010C2 \. C3 RETN



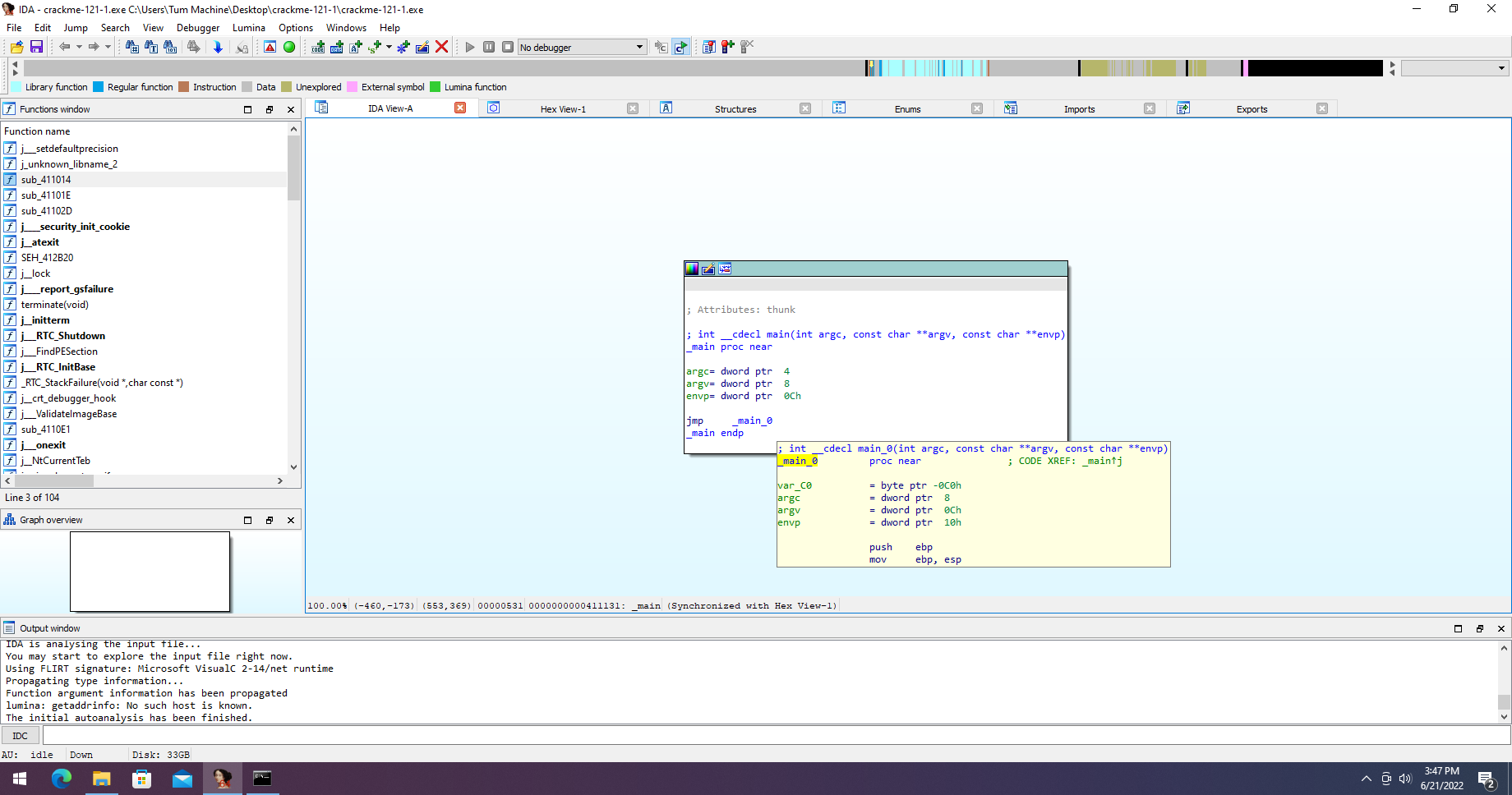
Hex 539 -> password DEC 1337

Part 2:

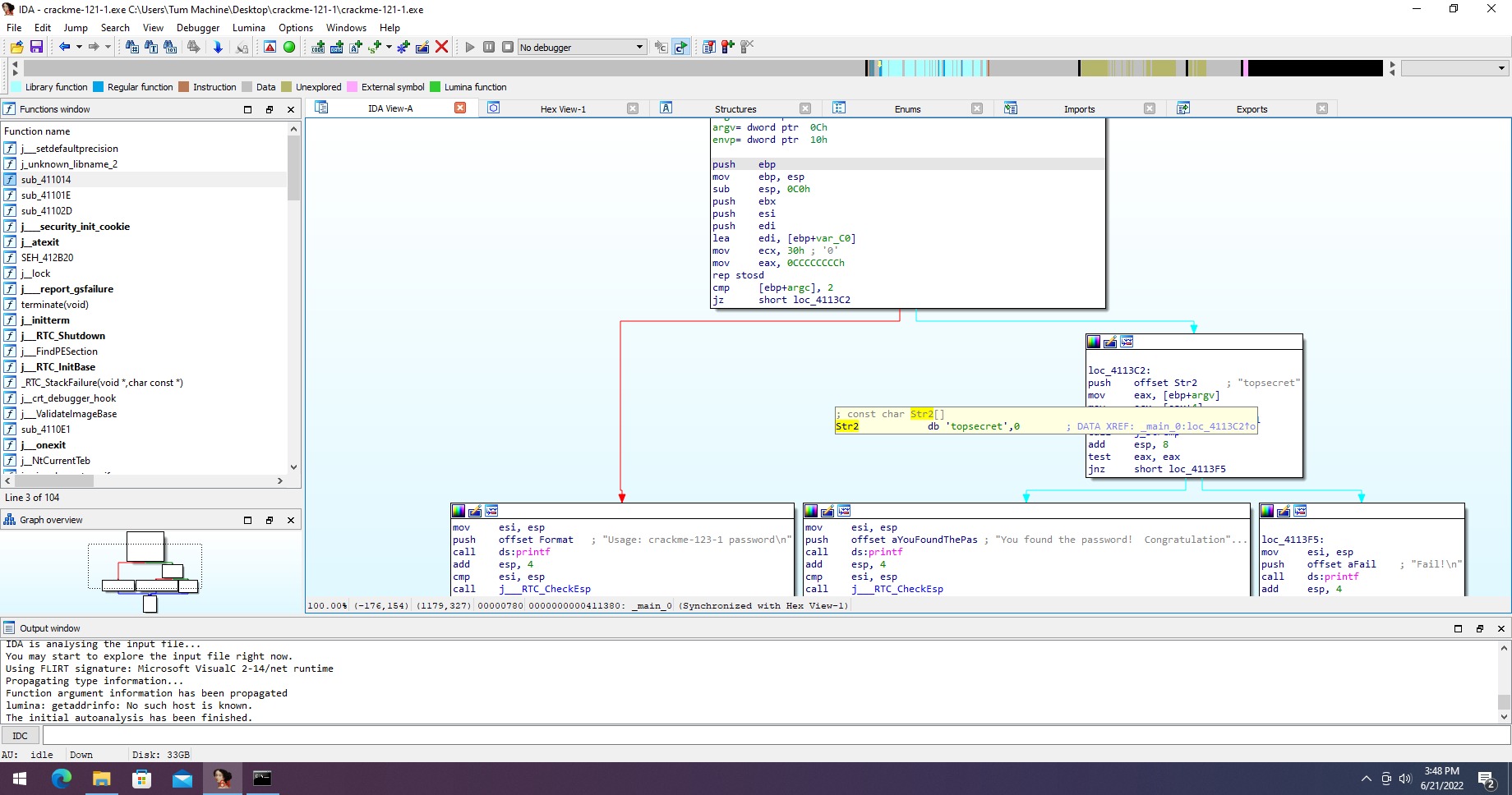
* Try program crackme-121-1.exe with cmd. We get the requirement to have a password after the .exe file

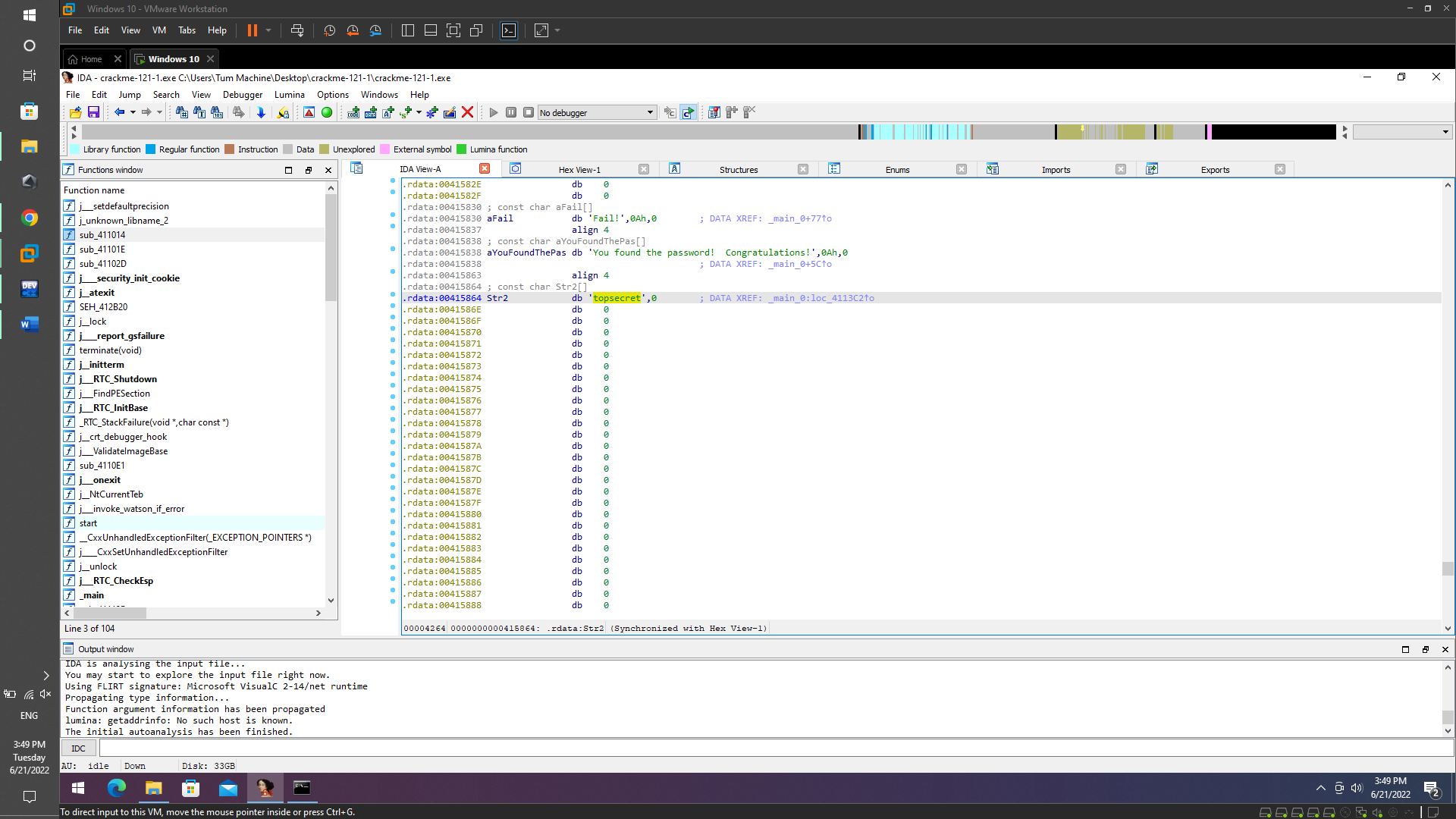


* Run IDA Pro to analyze the crackme-121-1.exe file. We see that the main function is very simple, but there is a jmp instruction to the main\_0 . function



* Moving to the topsecret command, we get the password itself





* Try again run file crackme-121-1.exe with password followed by "crackme-121-1.exe topsecret". and get successful results

