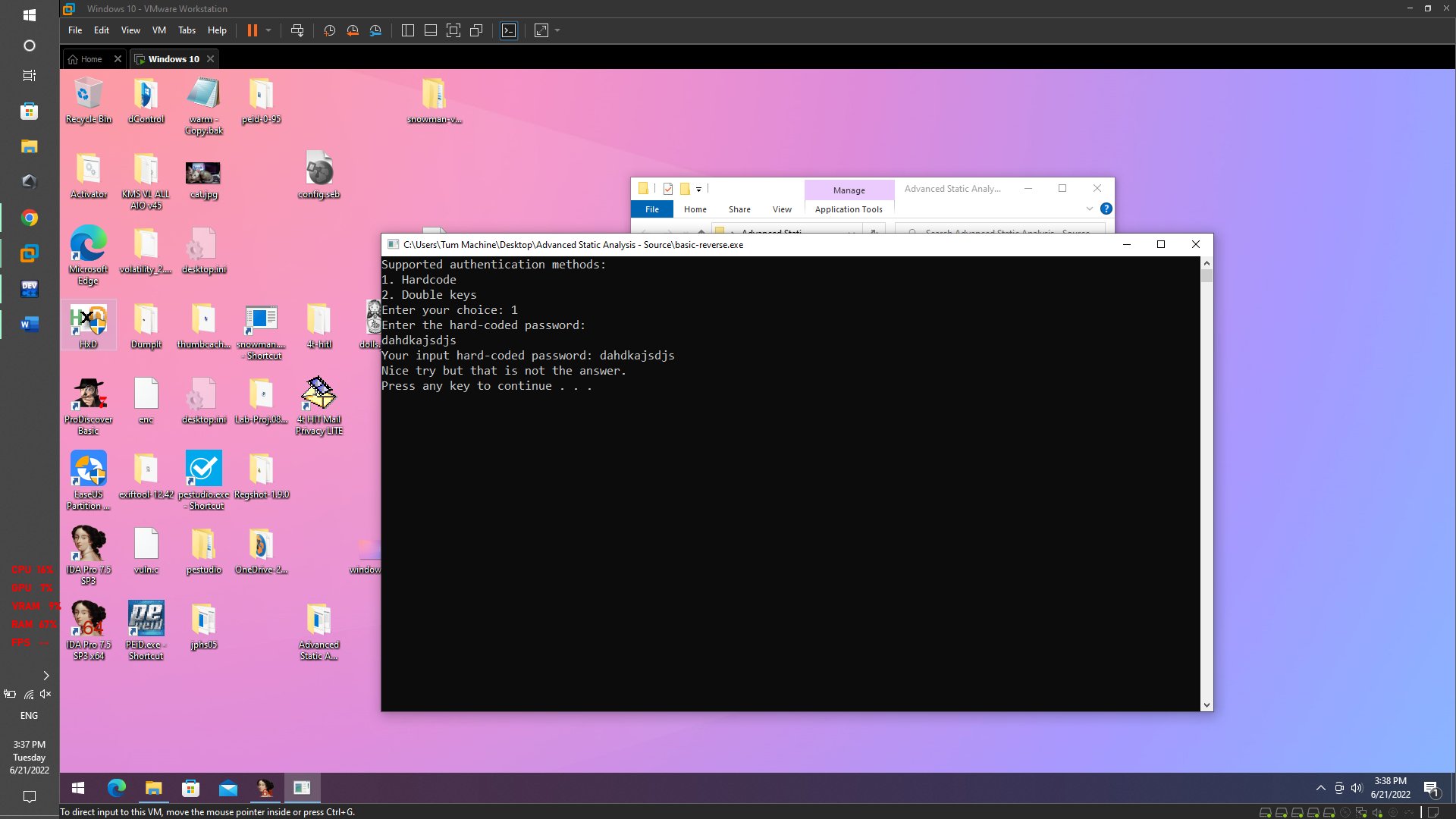
LAB 7

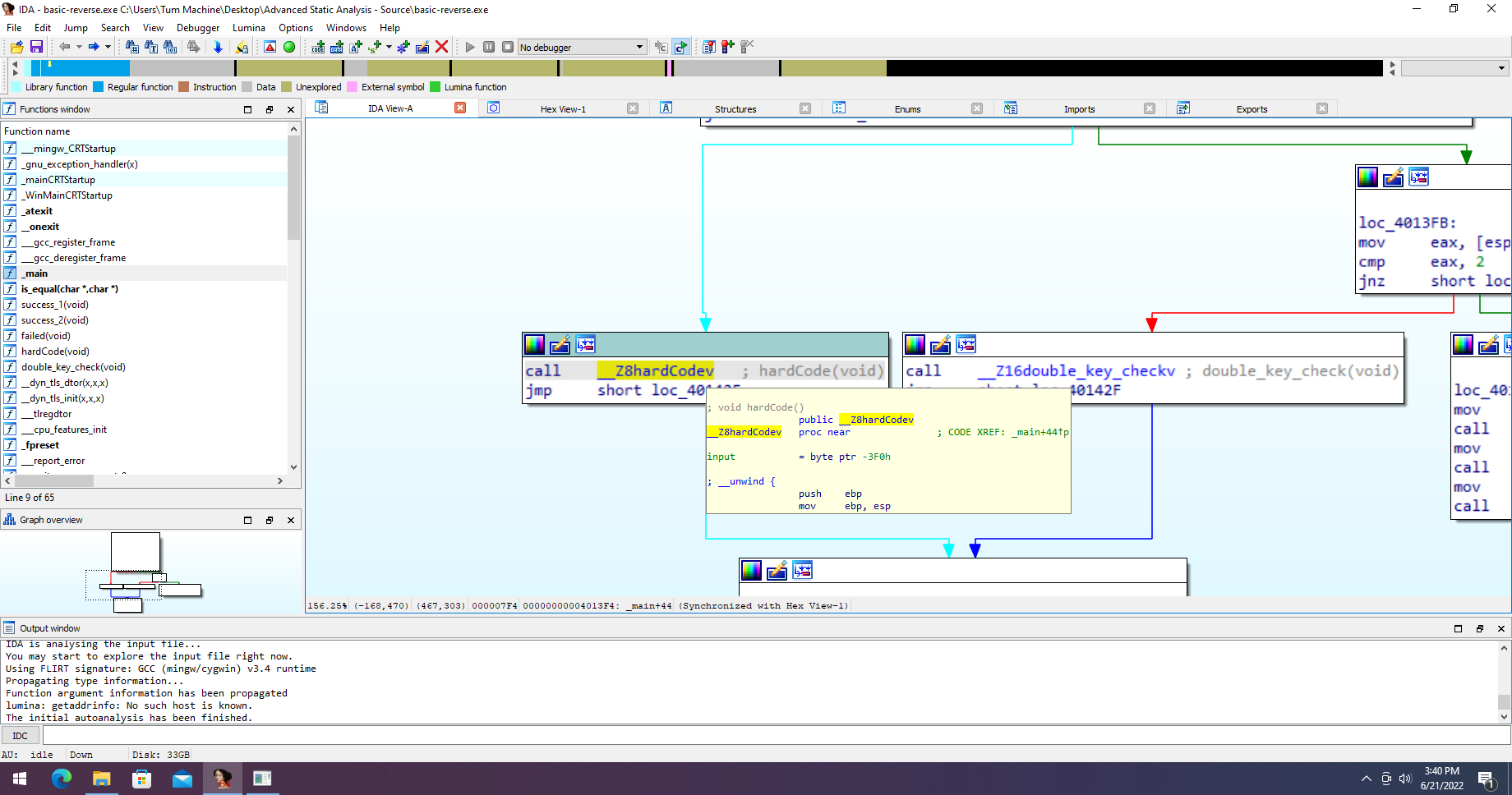
Nguyễn Thanh Hoài Lộc – SE151250

Part 1:

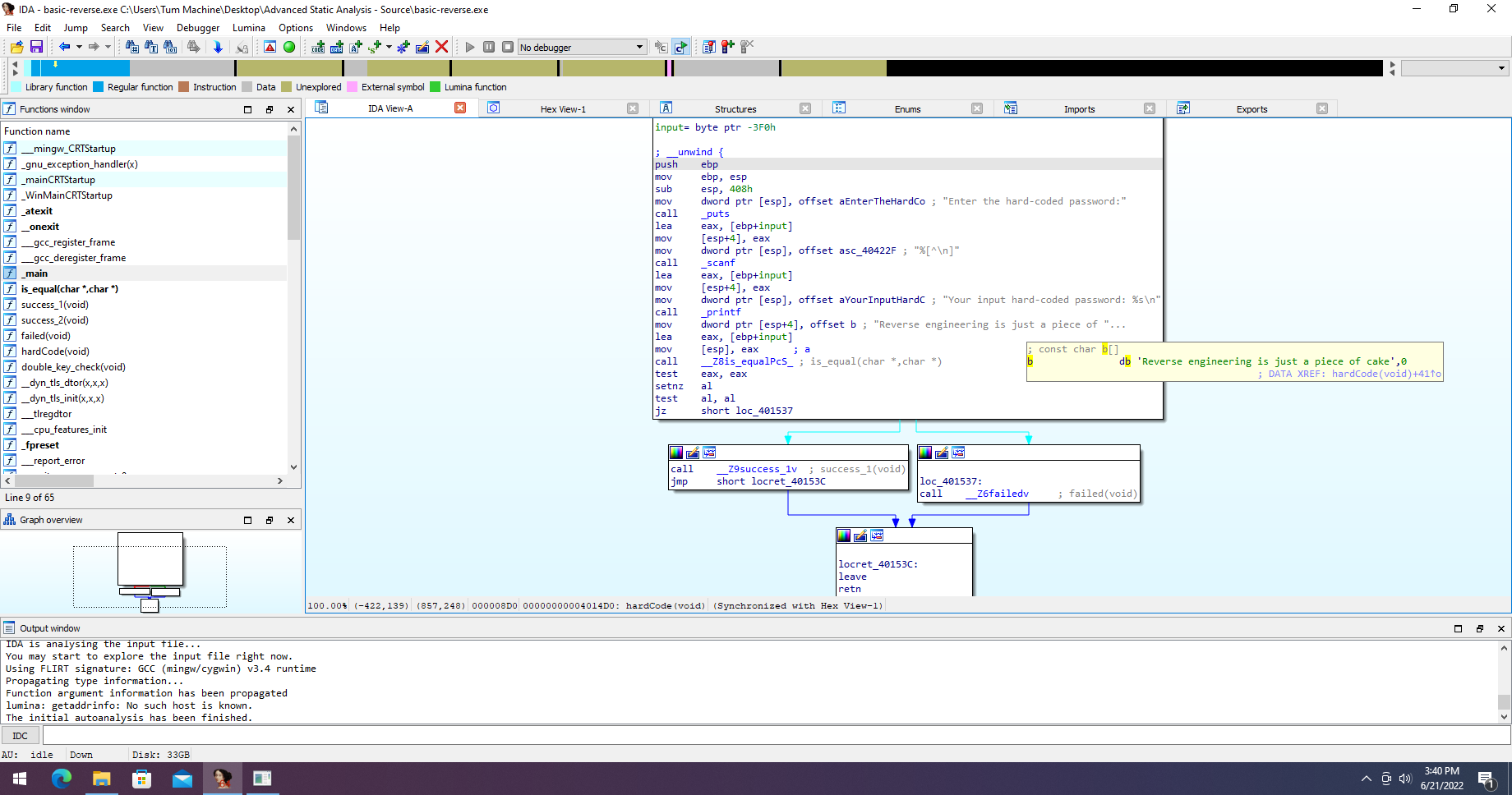
* Run the file basic-reverse.exe with cmd. Select the hardcode then randomly enter the password. We get "...is not the answer"



* Use the IDA pro tool to open the source code to find the password. choose to call "\_Z8hardCodev"

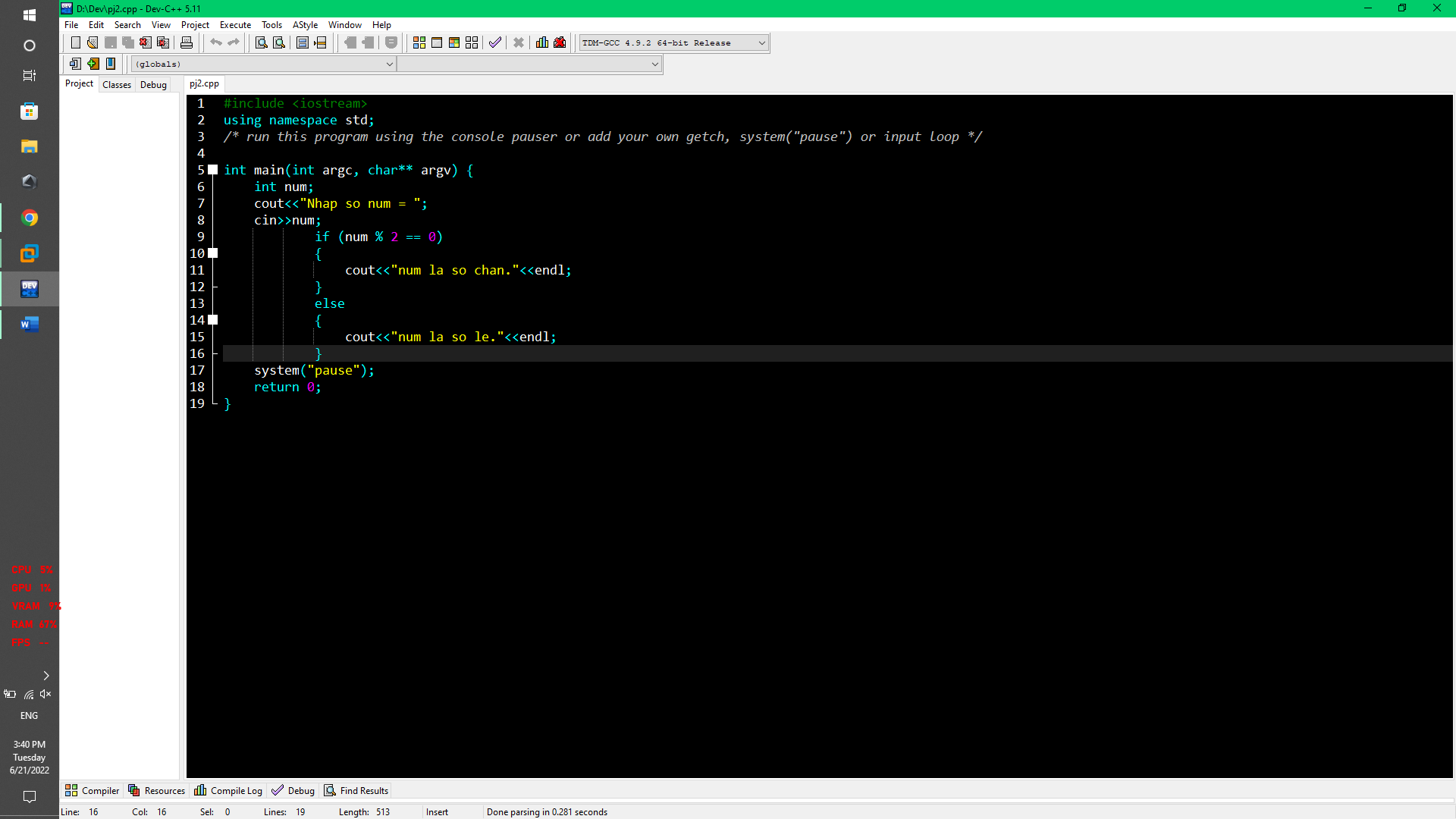


* Obtained the password is: "Reverse engineering is just a piece of cake"

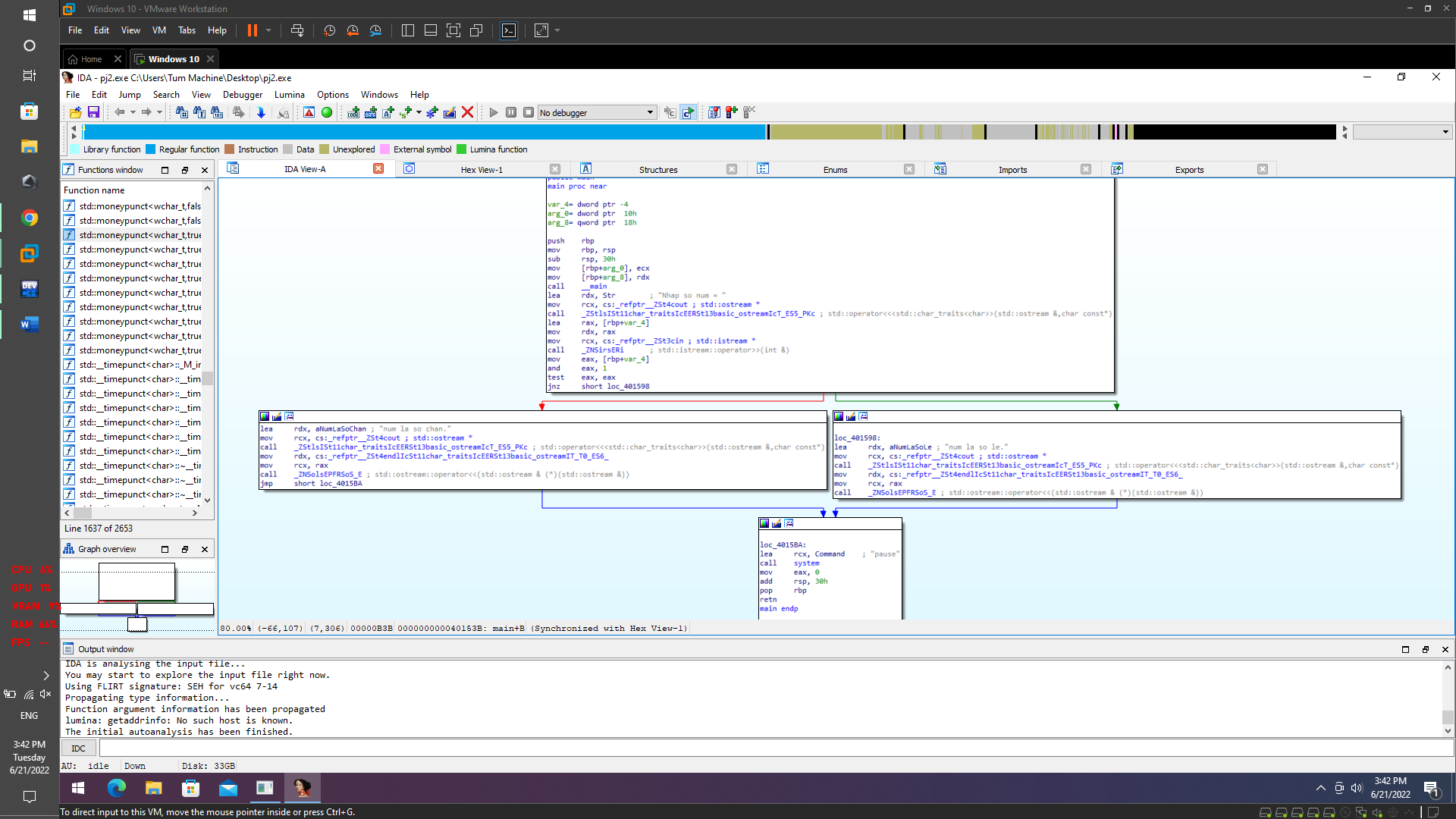


Part 2:

* Create a C++ program. run file a and get 1 .exe file

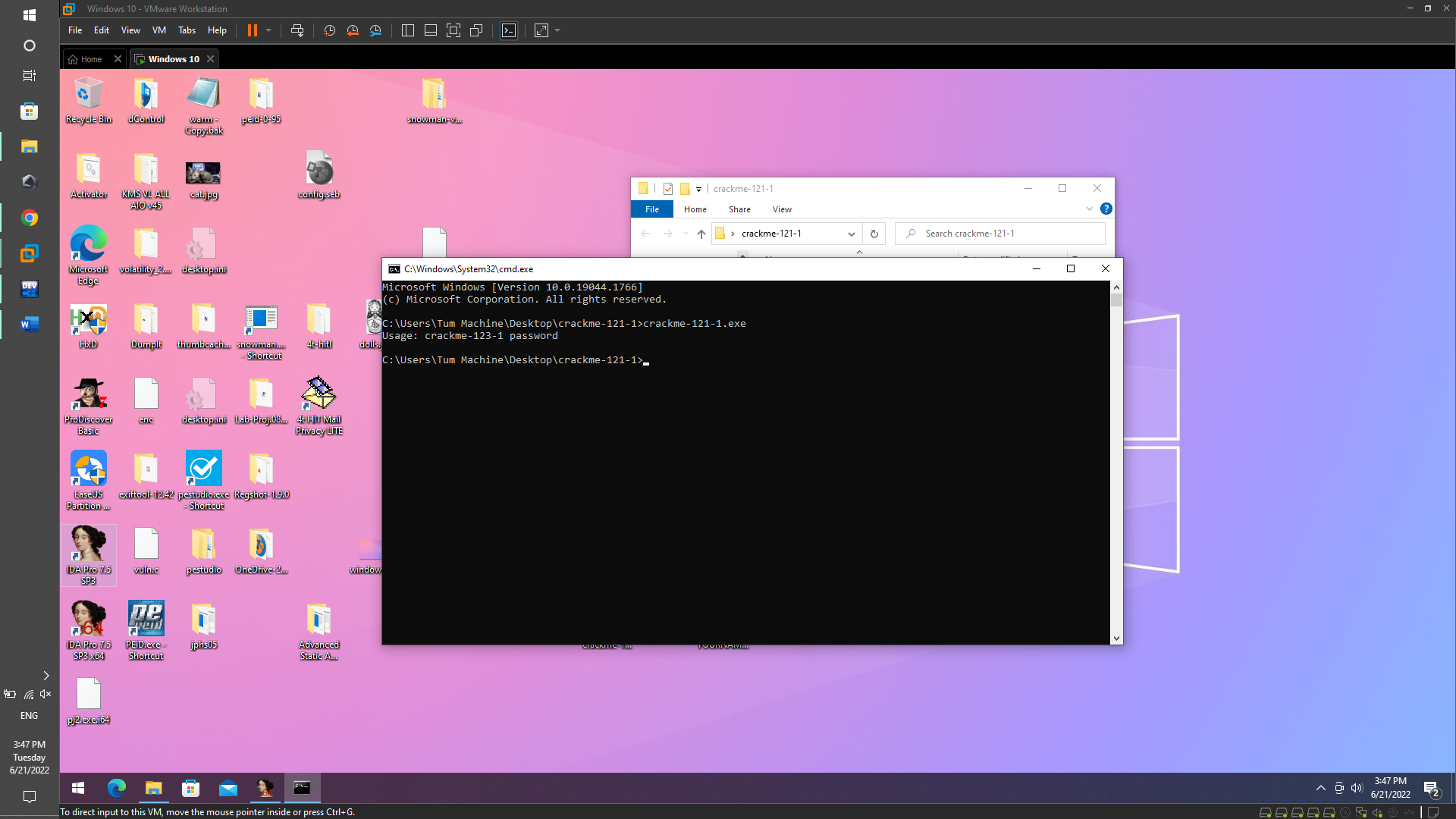


* Using IDA Pro to analyze the self-created .exe file from C++, we get two if else branches as shown

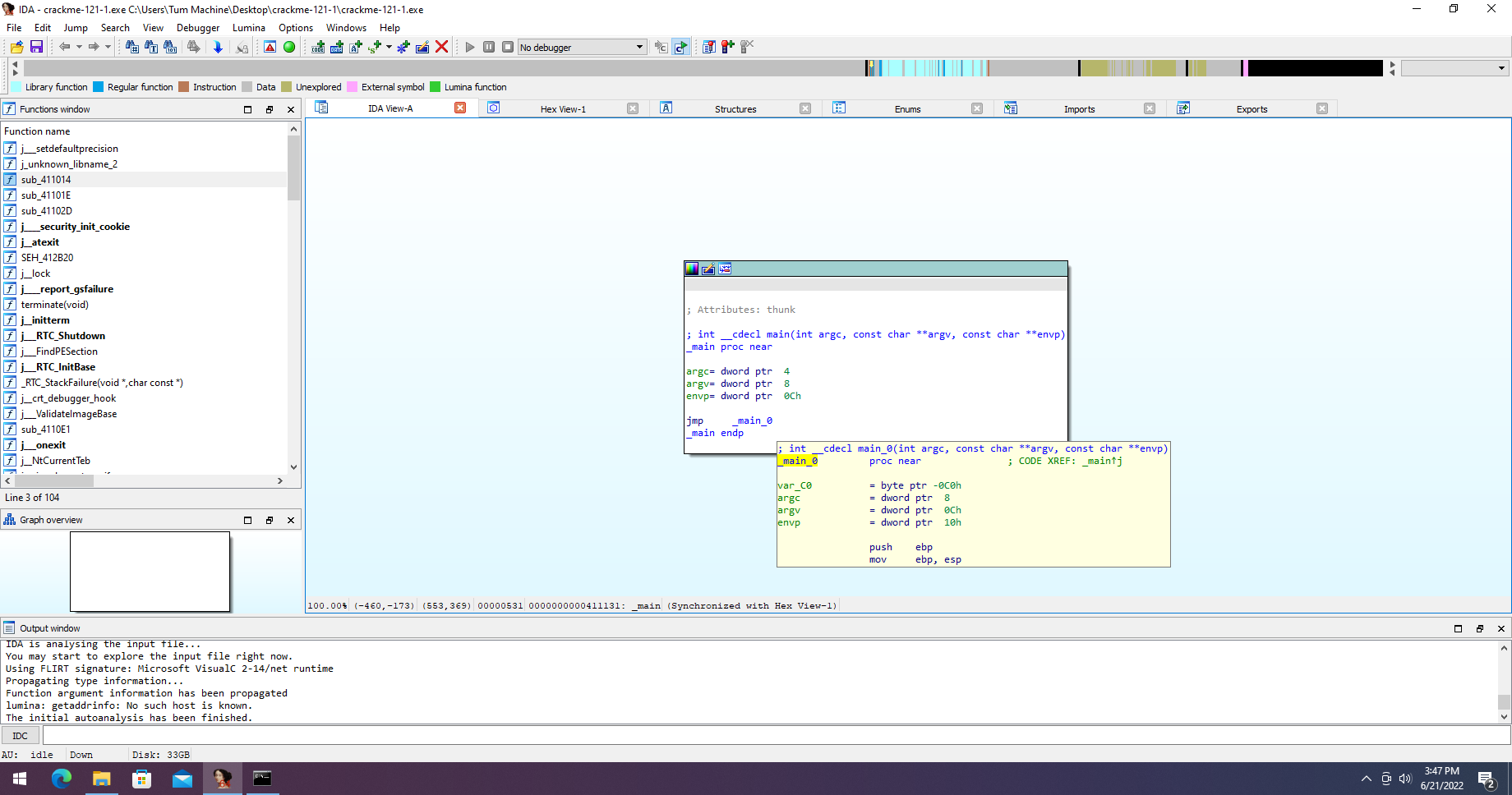


Part 3:

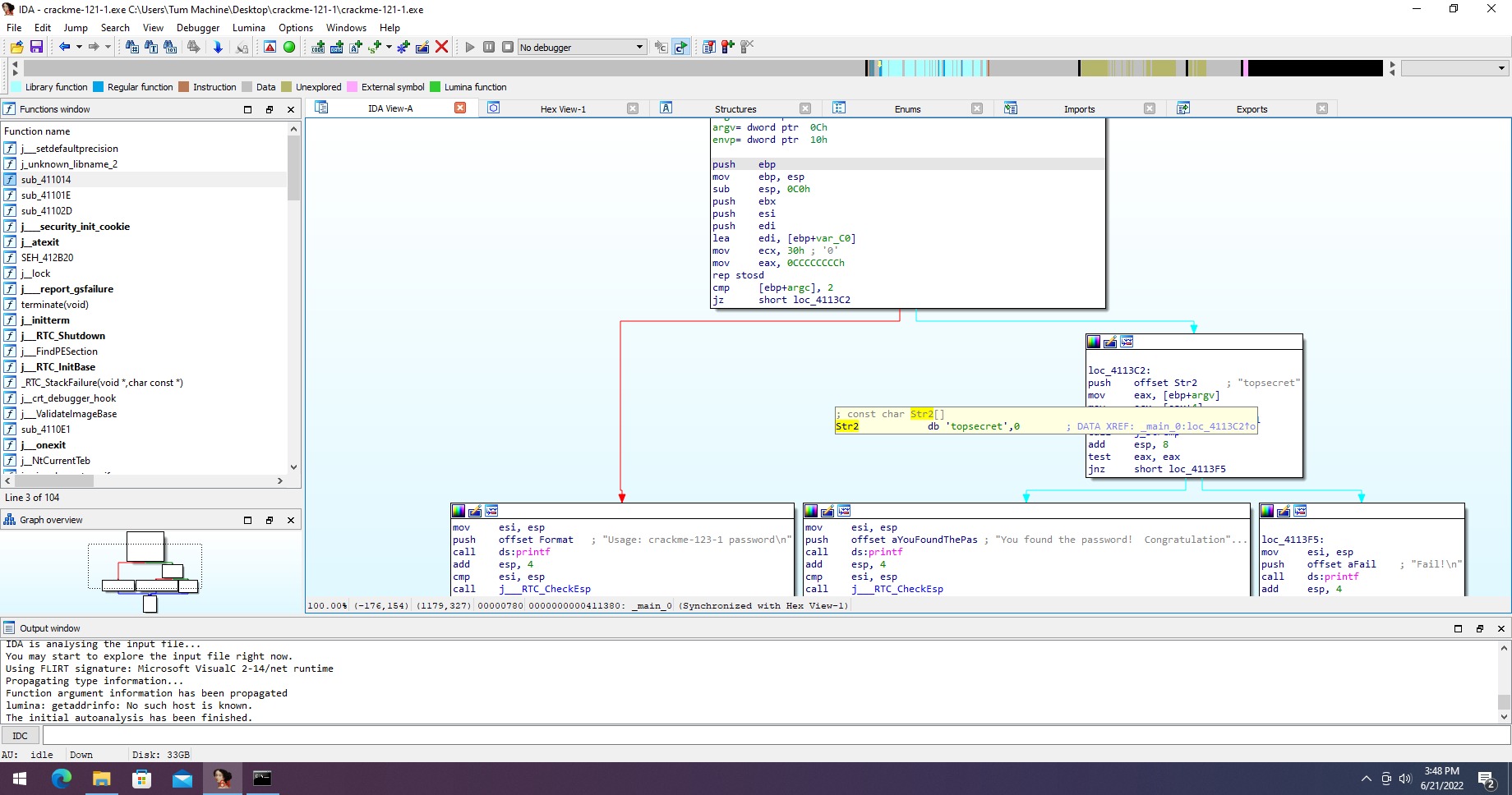
* Try program crackme-121-1.exe with cmd. We get the requirement to have a password after the .exe file

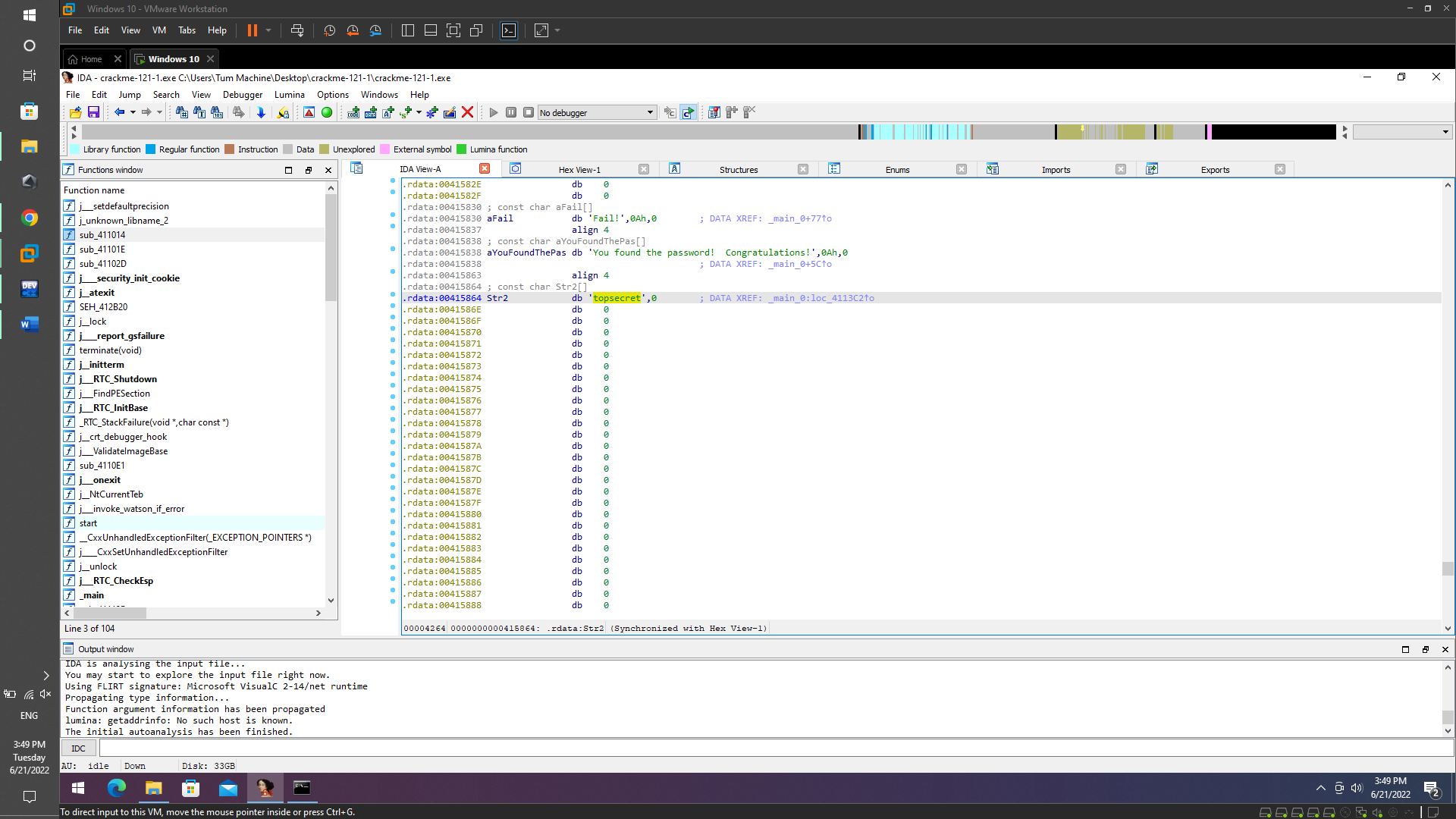


* Run IDA Pro to analyze the crackme-121-1.exe file. We see that the main function is very simple, but there is a jmp instruction to the main\_0 . function



* 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

