Malware Analysis

Reverse Engineering

Created By: - Rohan Goswami

AIM:
Consider yourself as a MA team member in the MMC company, they have given you a task to bypass the license key for Some executable files. You have to do reverse engineering on the given executable files and bypass the license key or try to get unauthorized access.

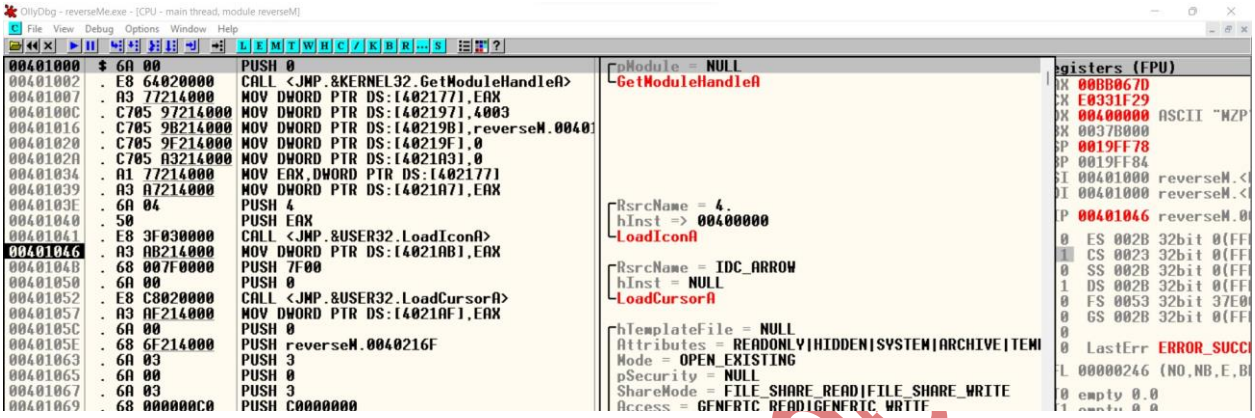
Exe File 1: ReverseMe.exe

So first of all We use Ollydbg, which is a debugging tool used for binary analysis.

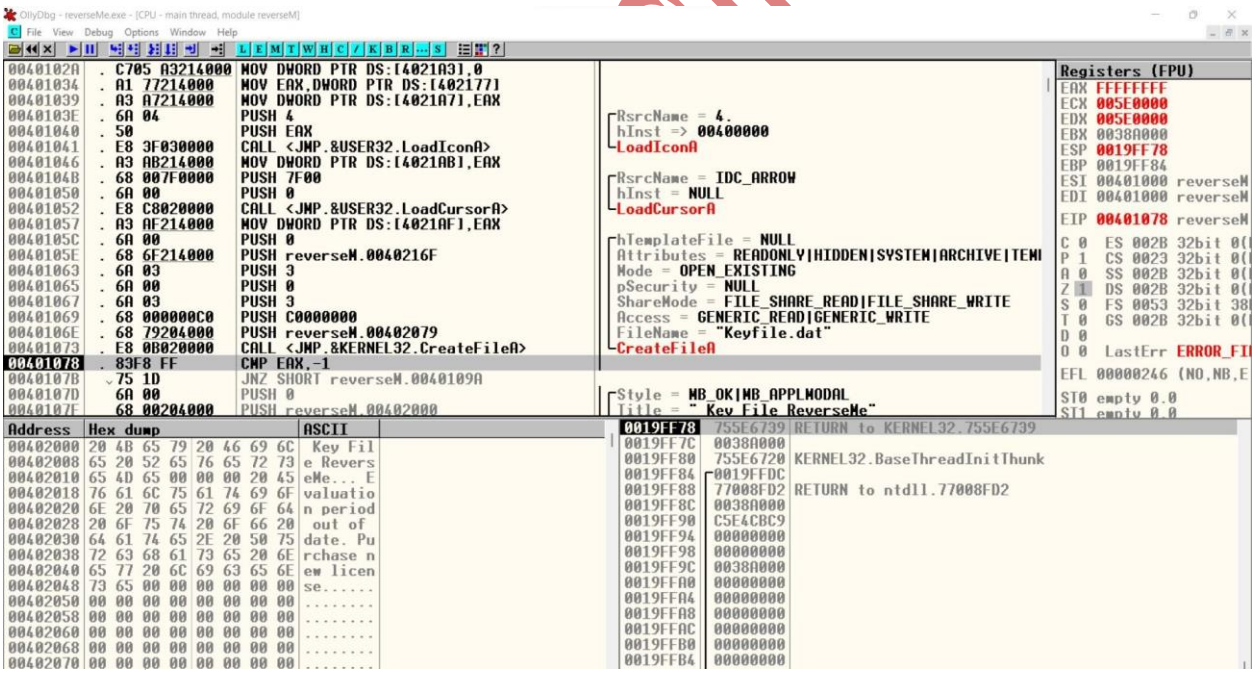
So it converts binary language into assembly language.
We basically take things apart, figuring it out how it works and keeping it together.

So when we open ReverseMe.exe in ollydbg the first thing we see is an assembly language instructions given to execute the exe file now we have to analyze how it works and crack it.

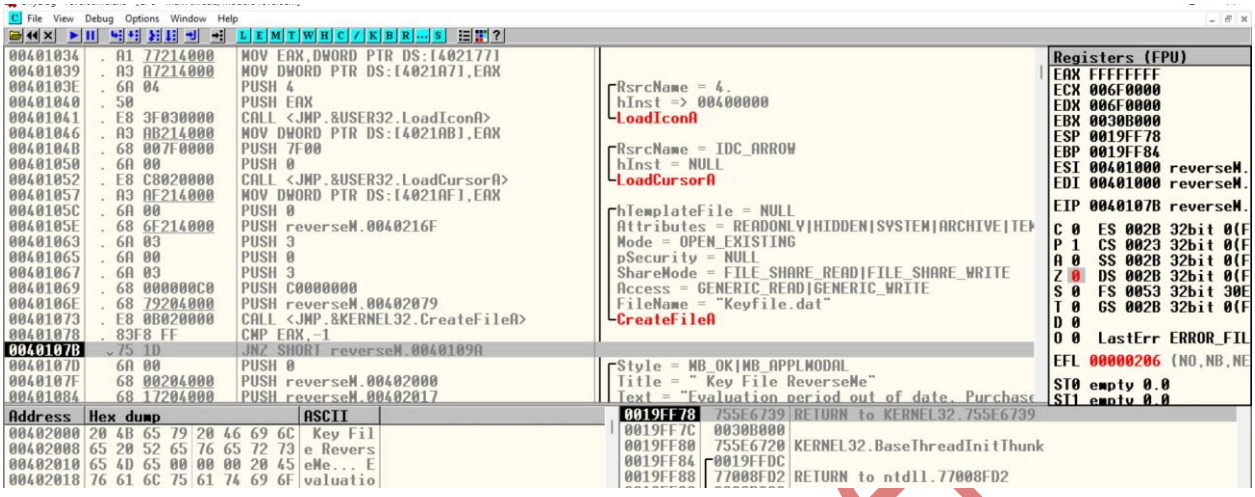
So it calls GetModuleHandleA.



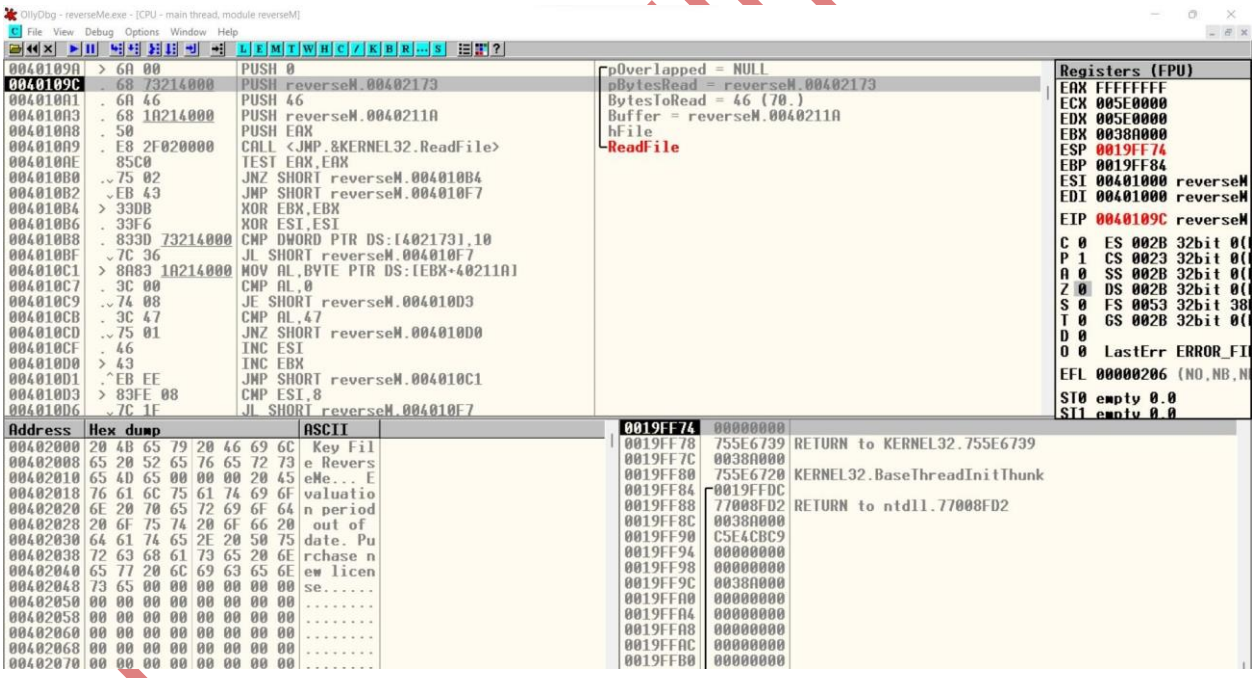
Now you can see it creates a file named Keyfile.dat.



Now if in JNZ we set Z = 0, then it will go to a specific address, it will only go to specific location if Z = 0 so the problem was that if we set Z = 1, it will execute code until it exit's the process.

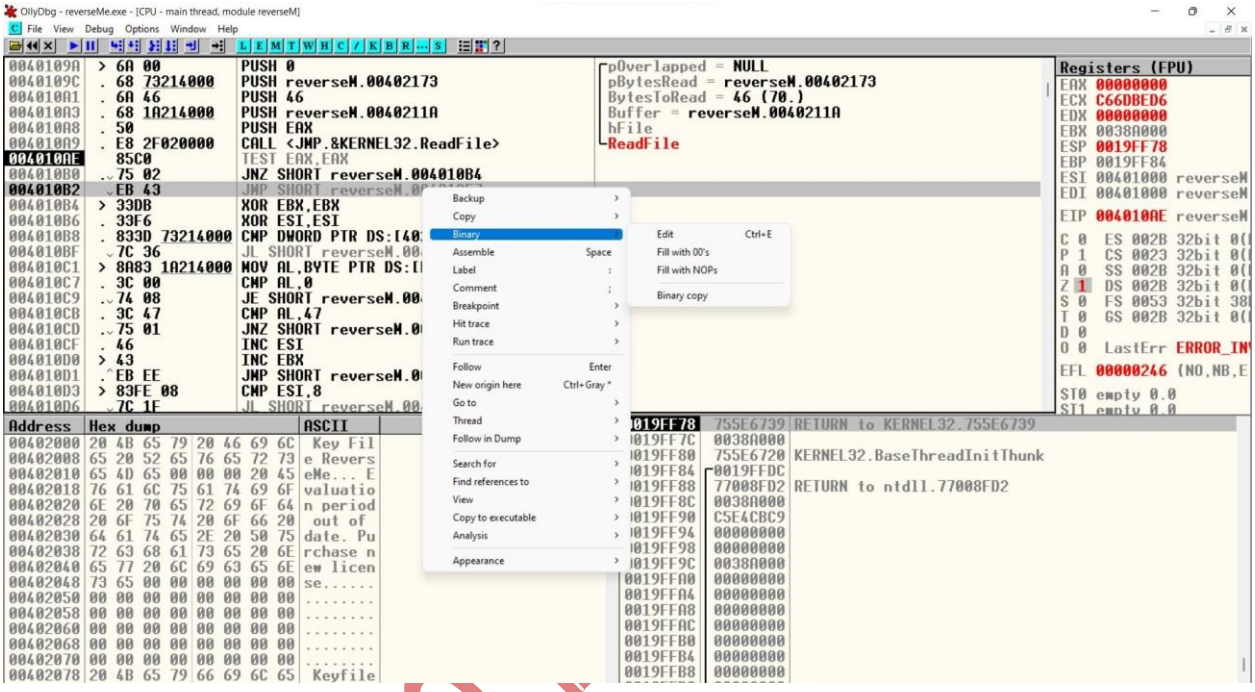


Now it reads the file and tests the extended accumulator.

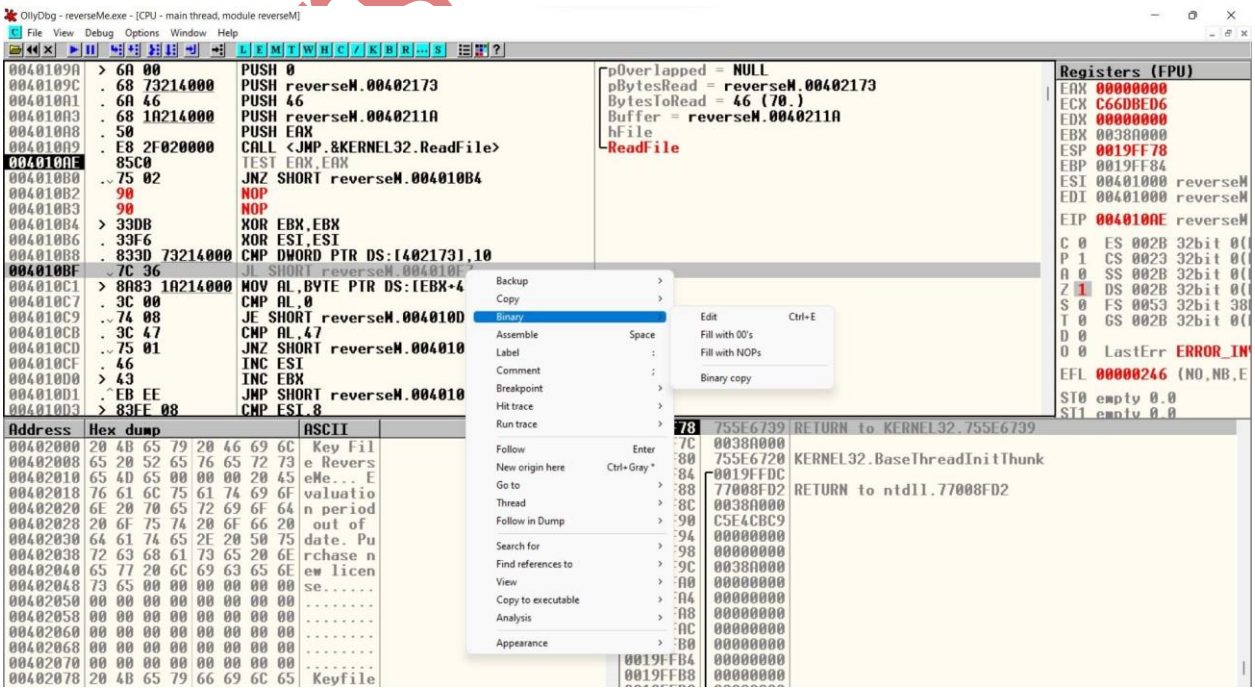


Here as you can see after the TEST is done it goes to address so if it goes
to this address as 004010F7 then i think it will give us as the key file is not valid.

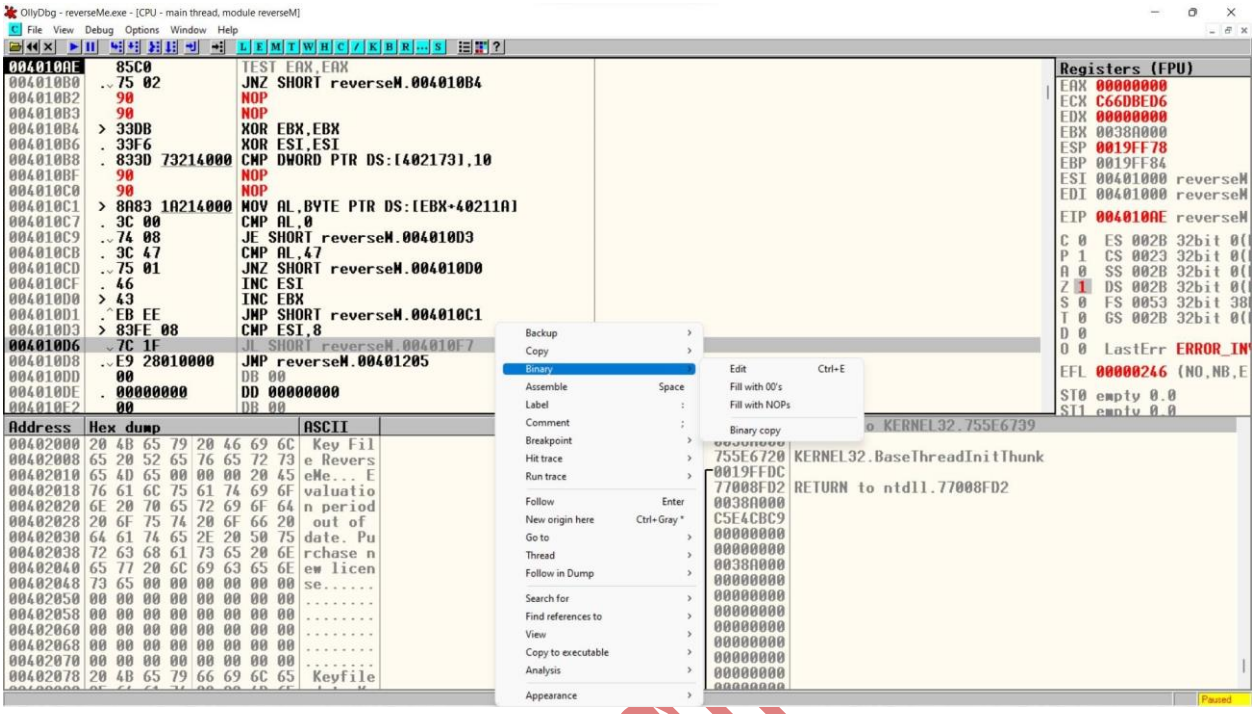
So what we have to do is whenever 004010F7 is inputted we just have to fill it as NOP.

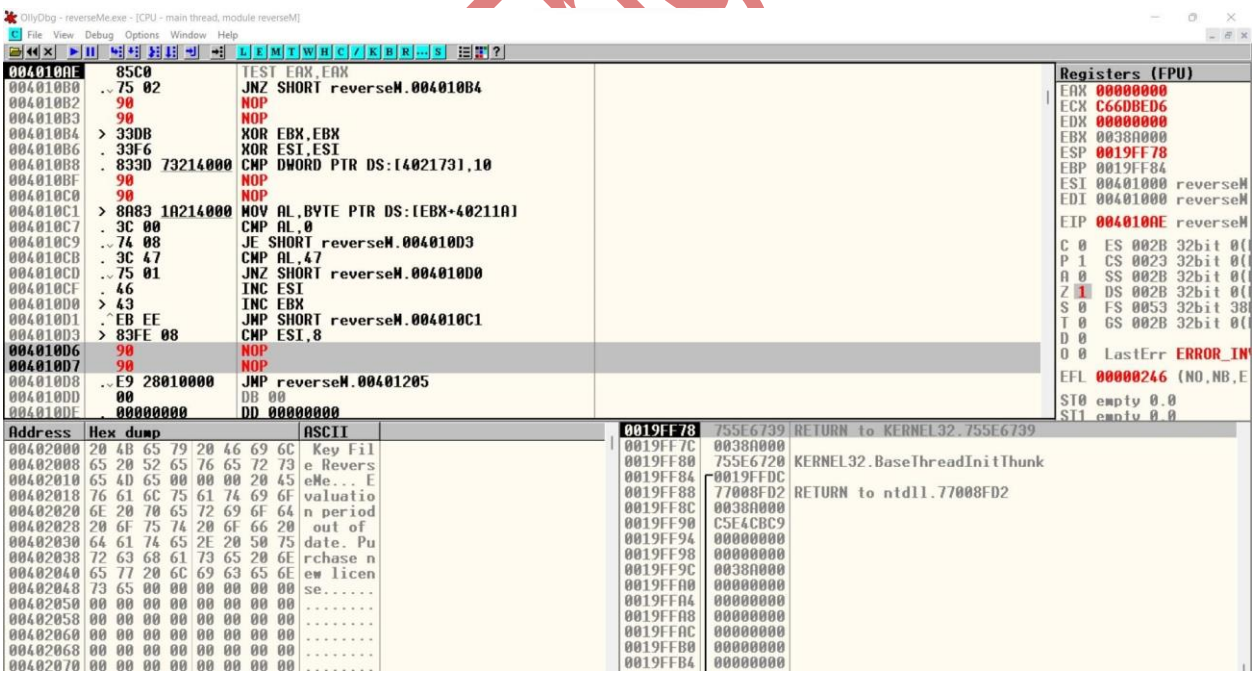


After that in 10BF it gives 004010F7 address we also have to fill with NOP.



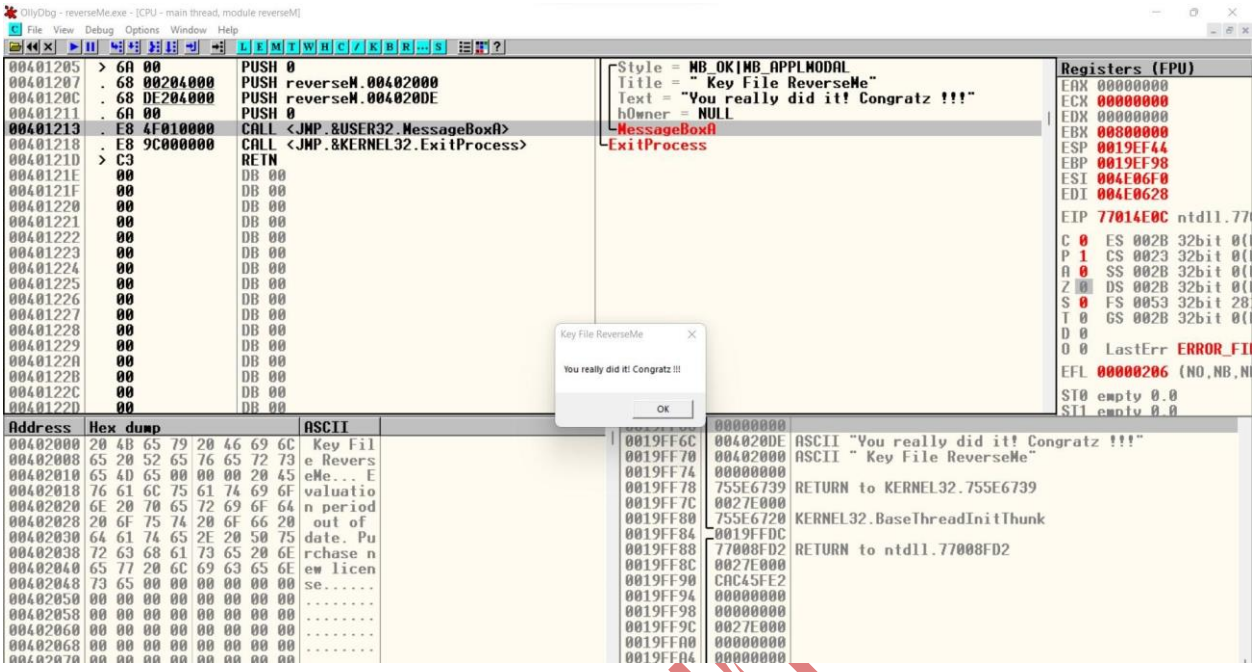
After that in 10D6 it gives 004010F7 addresses we also have to fill with NOP.





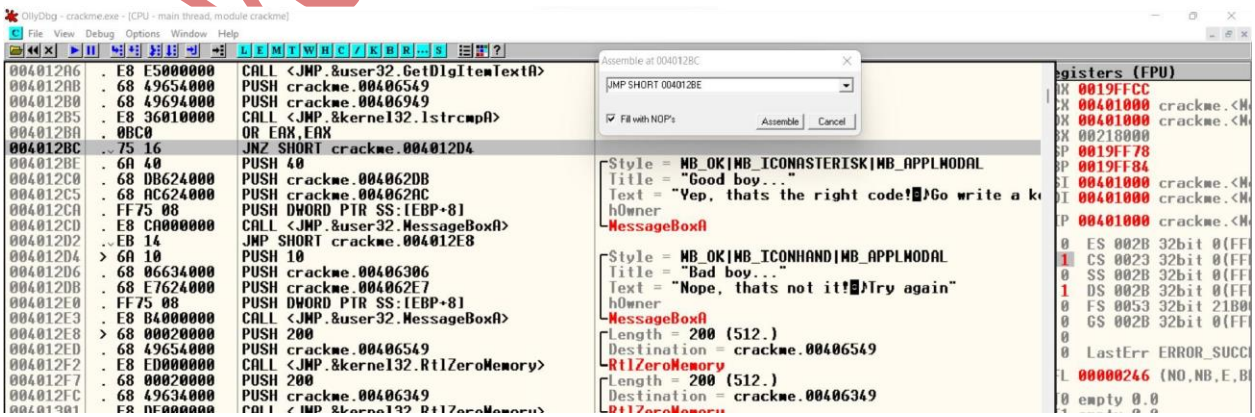
After that we executed it.

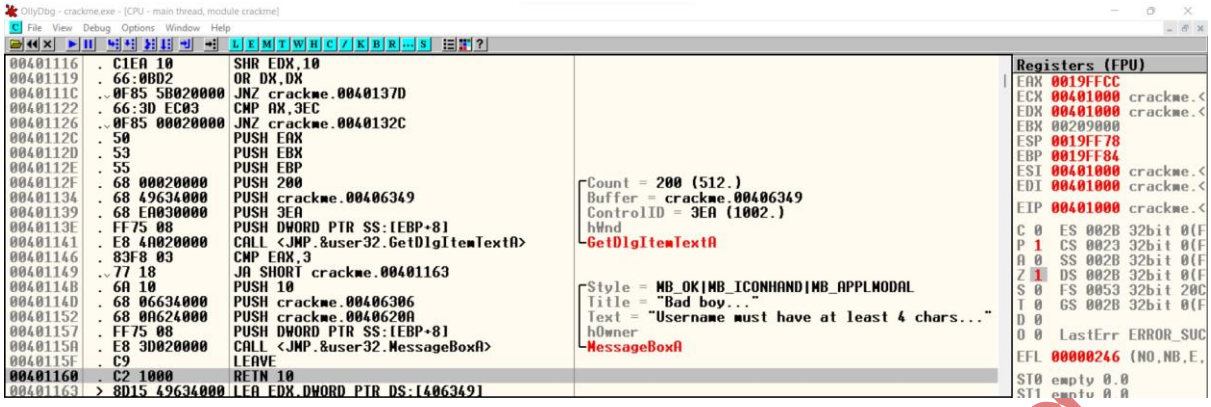
You can see it goes to 00401205 and when it goes to MessageBoxA a message box will appear and it will give us you really did it.



Exe File 2: Crackme.exe

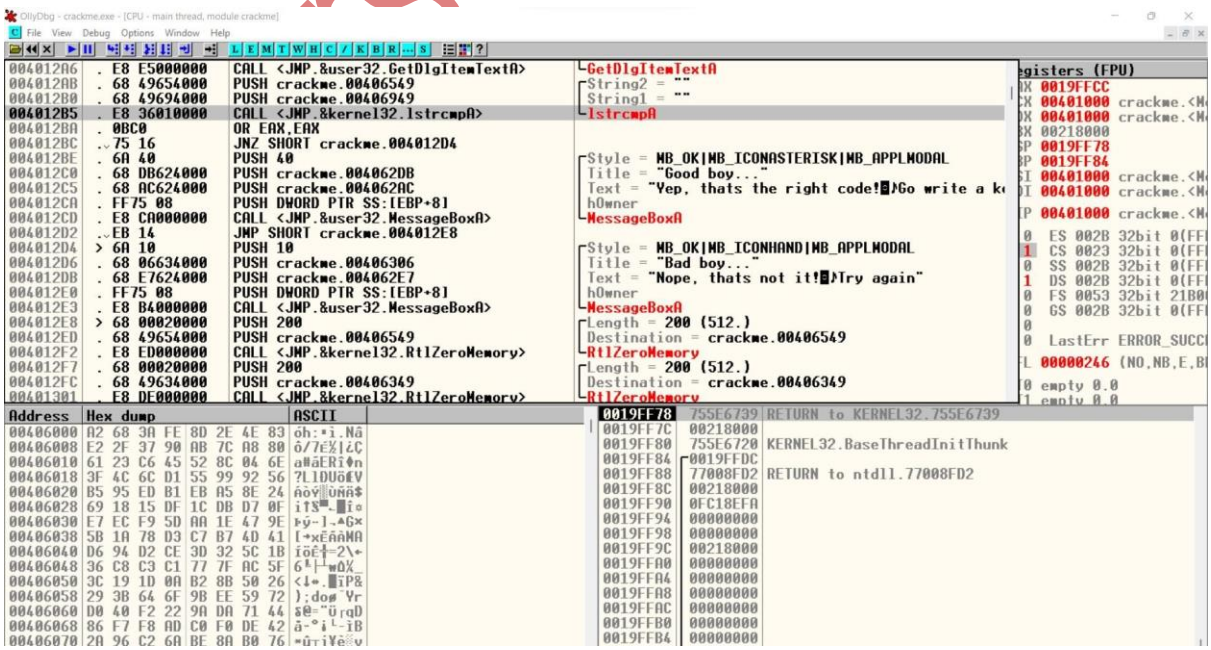
So what happens here when you execute the code, it will give us a dialogue box about giving username and reg code, so when we write 2 characters then will say minimum 4 characters required.





Now here in you can see that it compares the
Mem 00406549 = Mem 00406949 so what is going on is its jumps to 12D4 location which will give us output as a try again.

So what we will do is to modify the address and give it to a specific address which will give us successful output.



So when we execute the code again it will give us a dialogue box and when we write the username and Reg code it will give us a message box as that's the right code.