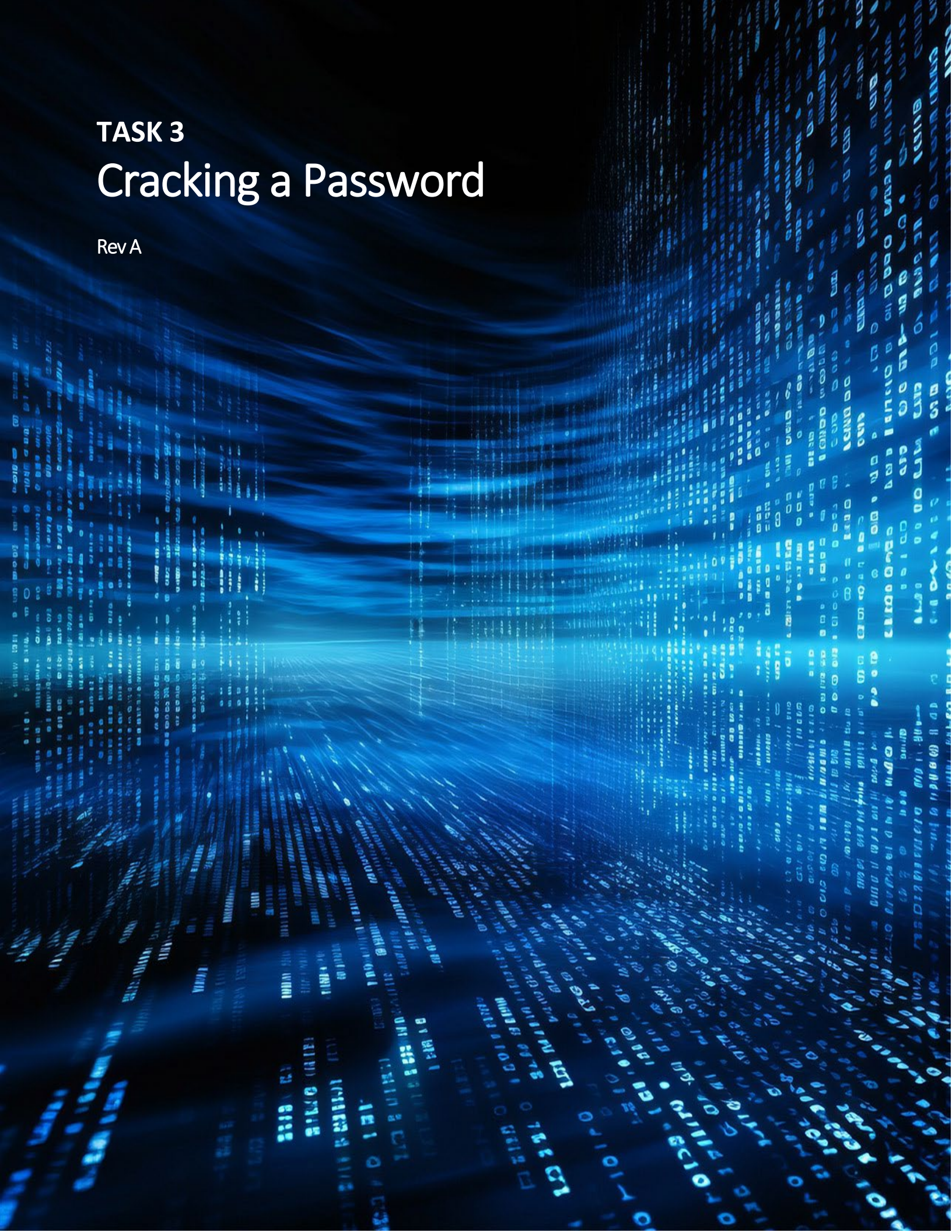


TASK 3

Cracking a Password

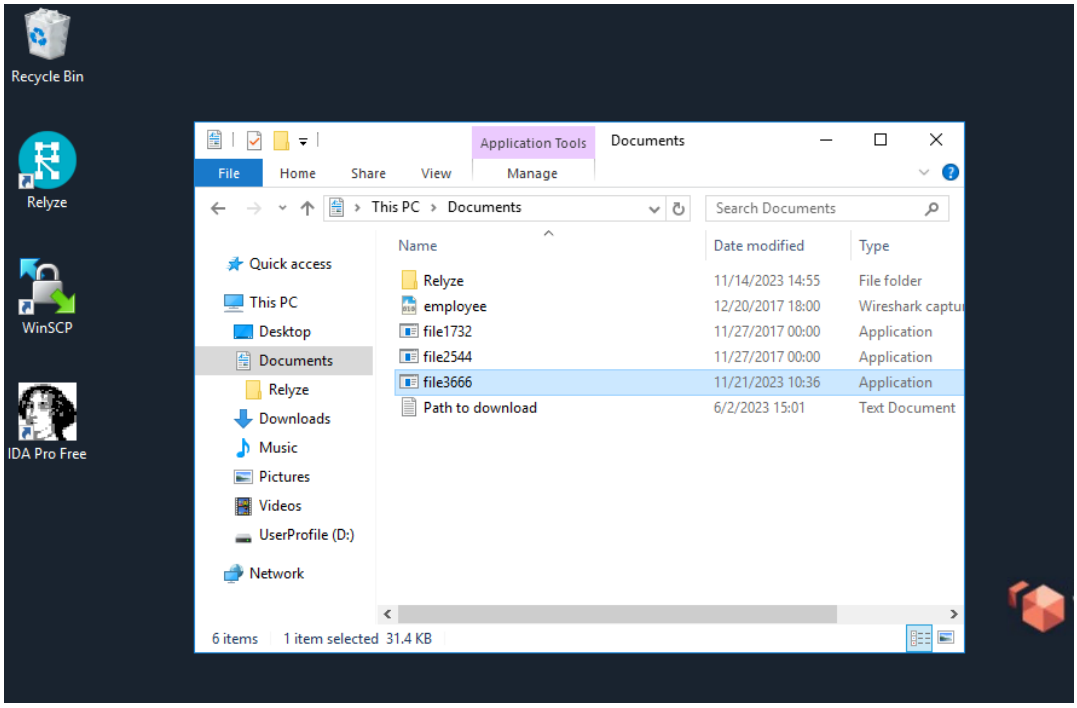
Rev A

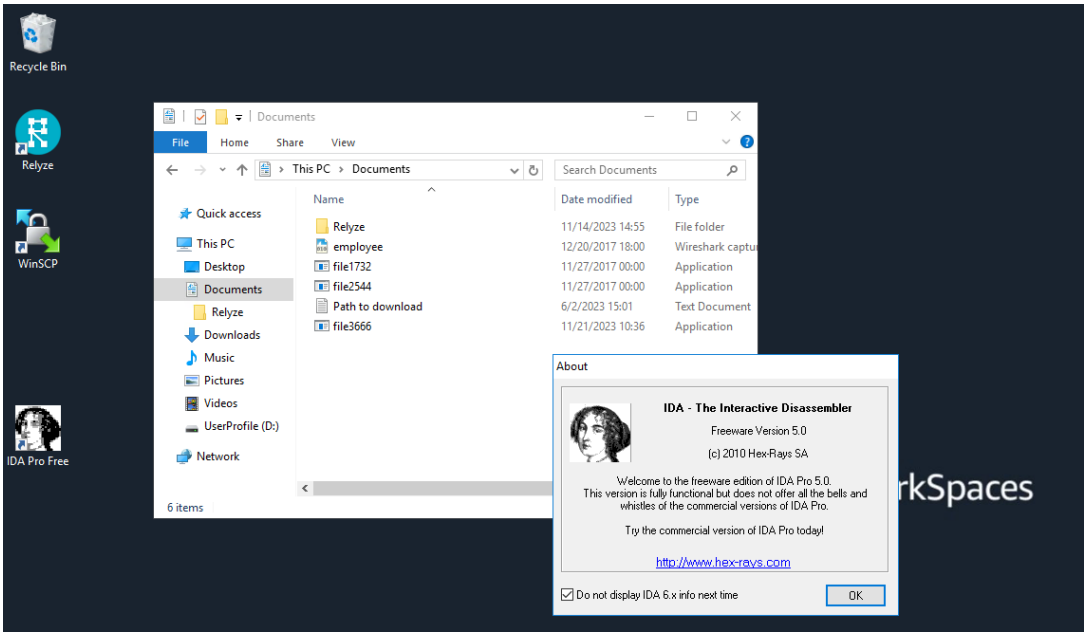
Cracking a Password

Cracking a Password

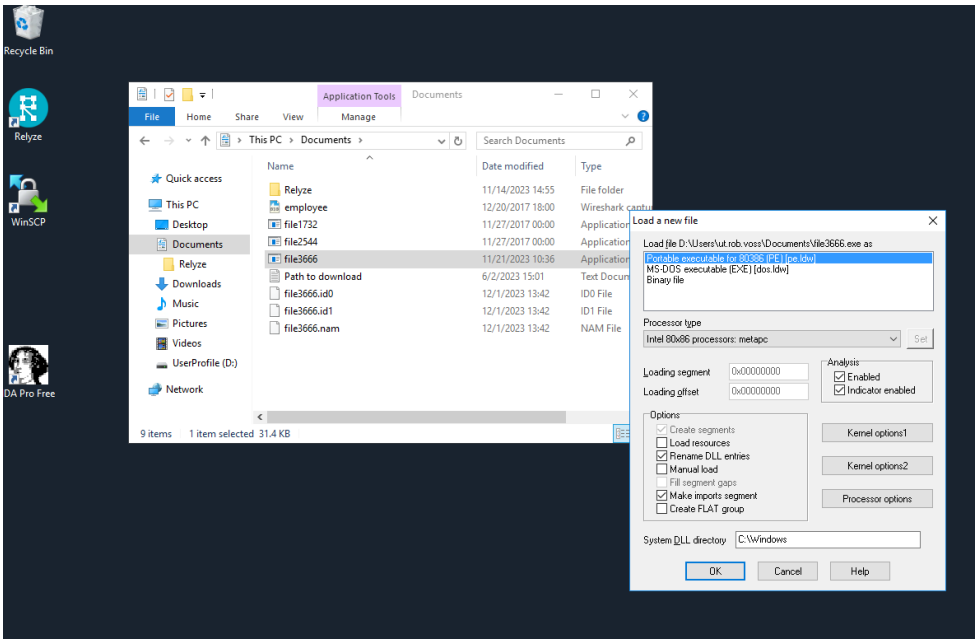
1 Opening a File in IDA Pro

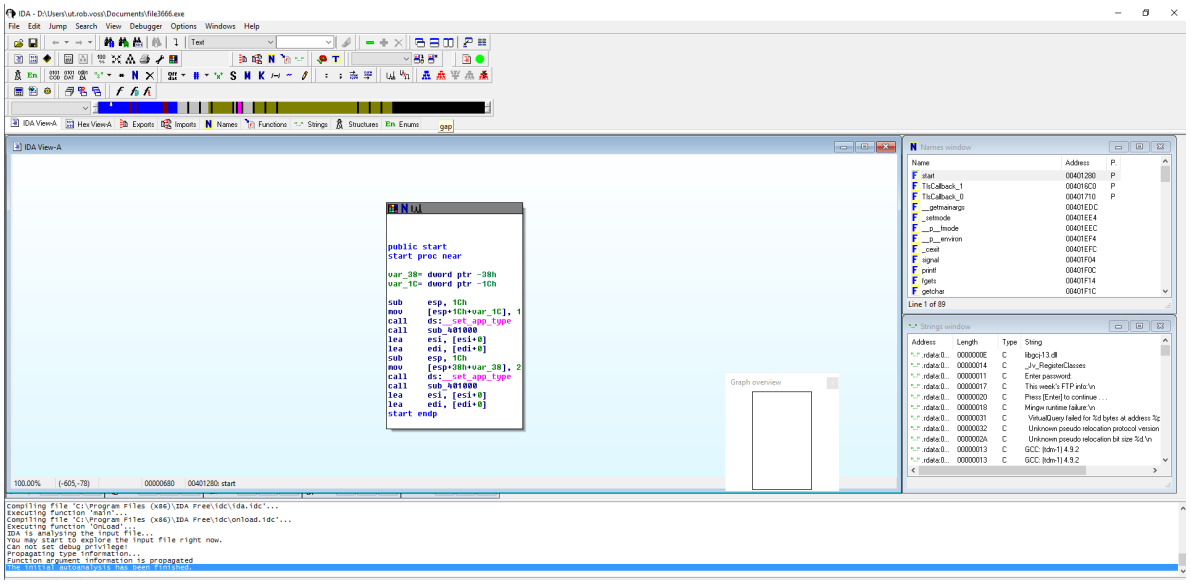
Open file 3666 in IDA Pro
Select file and drag and drop on top of IDA Pro
Click ok





Cracking a Password

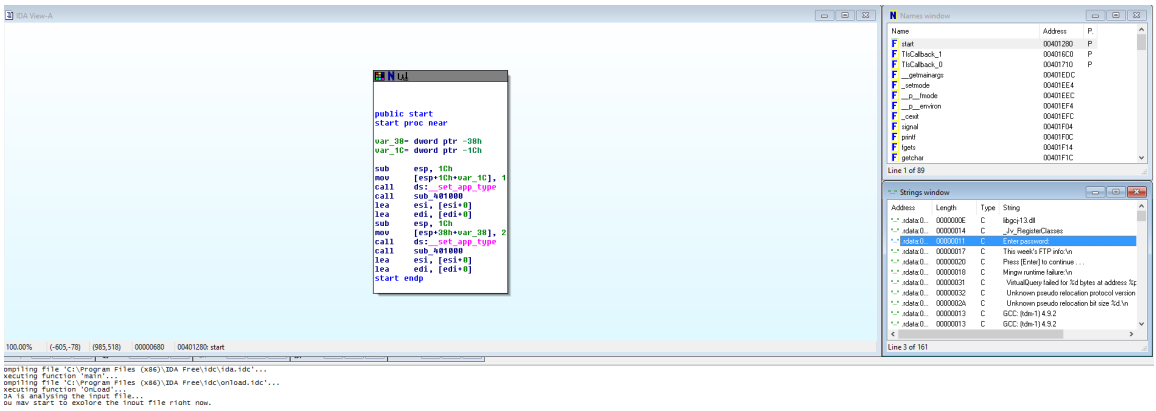




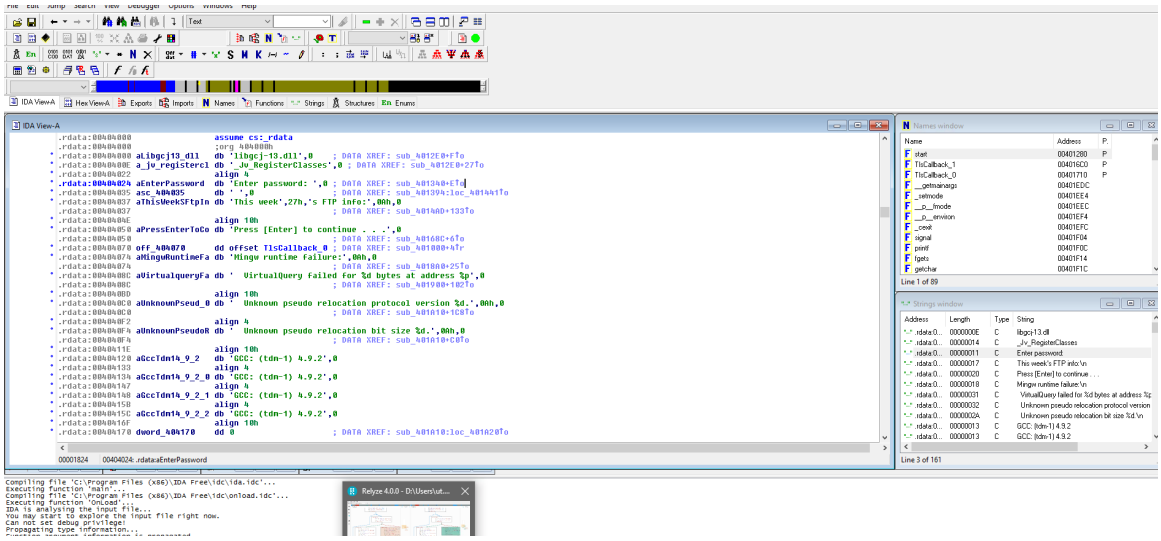
Cracking a Password

2 Renaming Subroutines

Starting from the Strings window, locate the subroutine that asks for a password.
(This is where the flow of control for this program starts.)

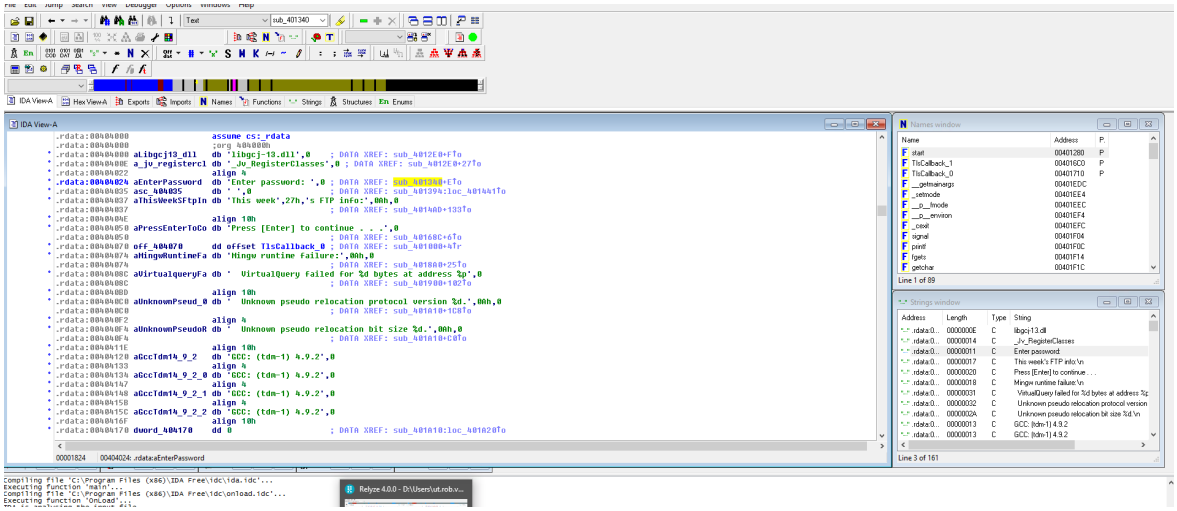


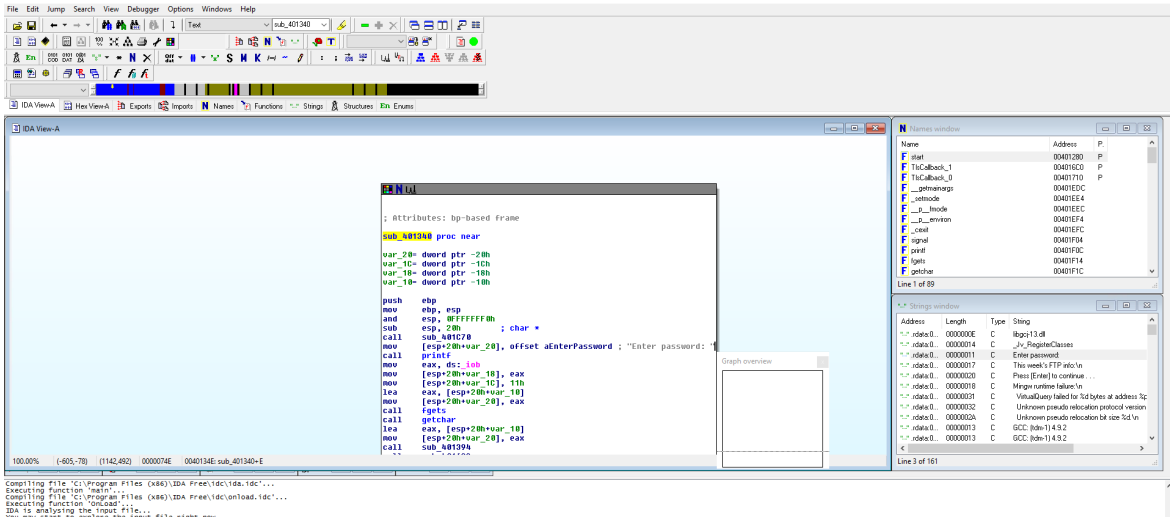
Double click on sub routine to have it load into the View a window



Cracking a Password

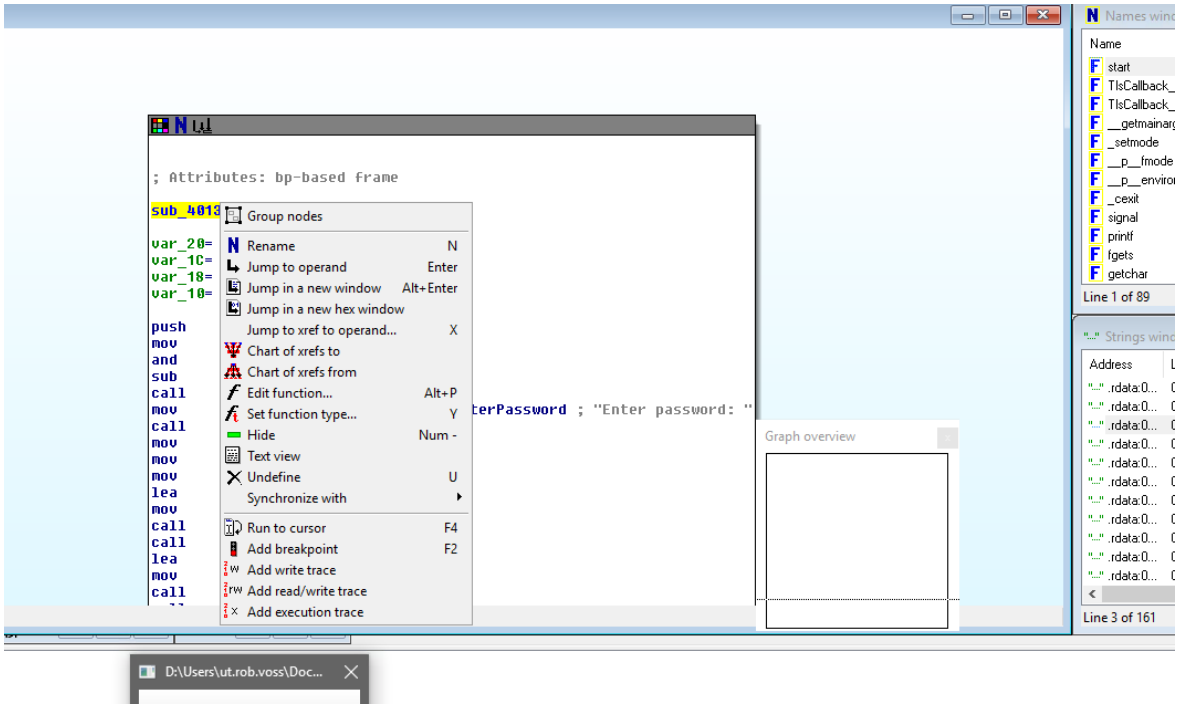
Find the sub routine and double click on it…

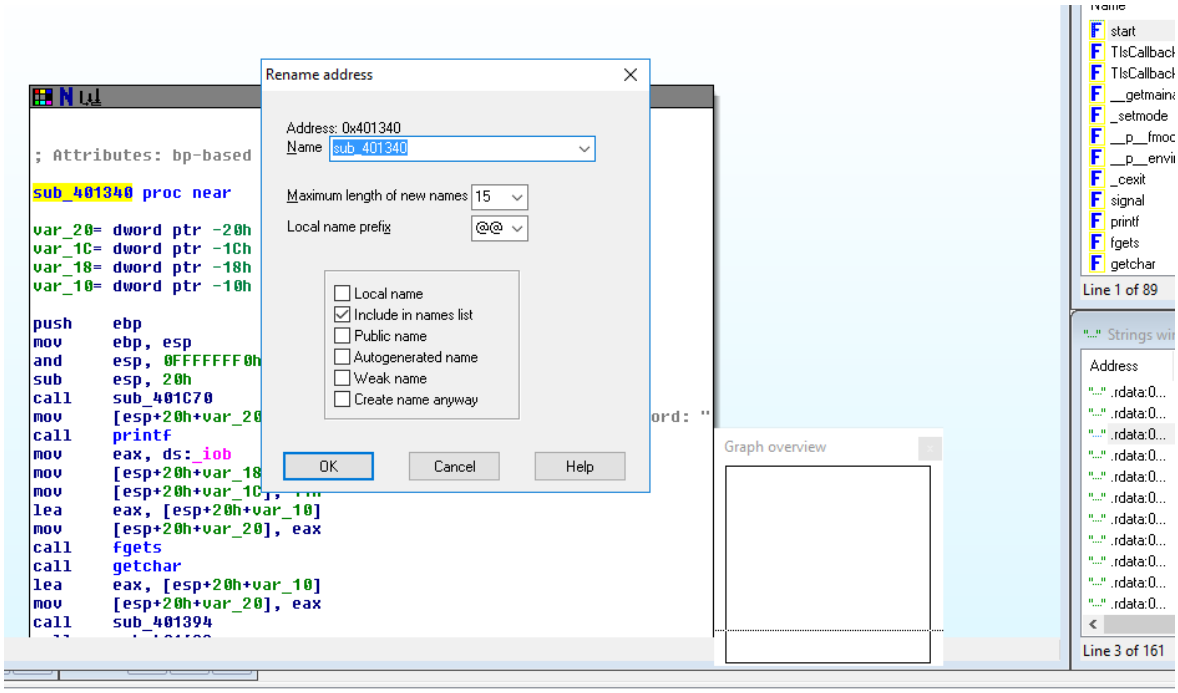




Cracking a Password

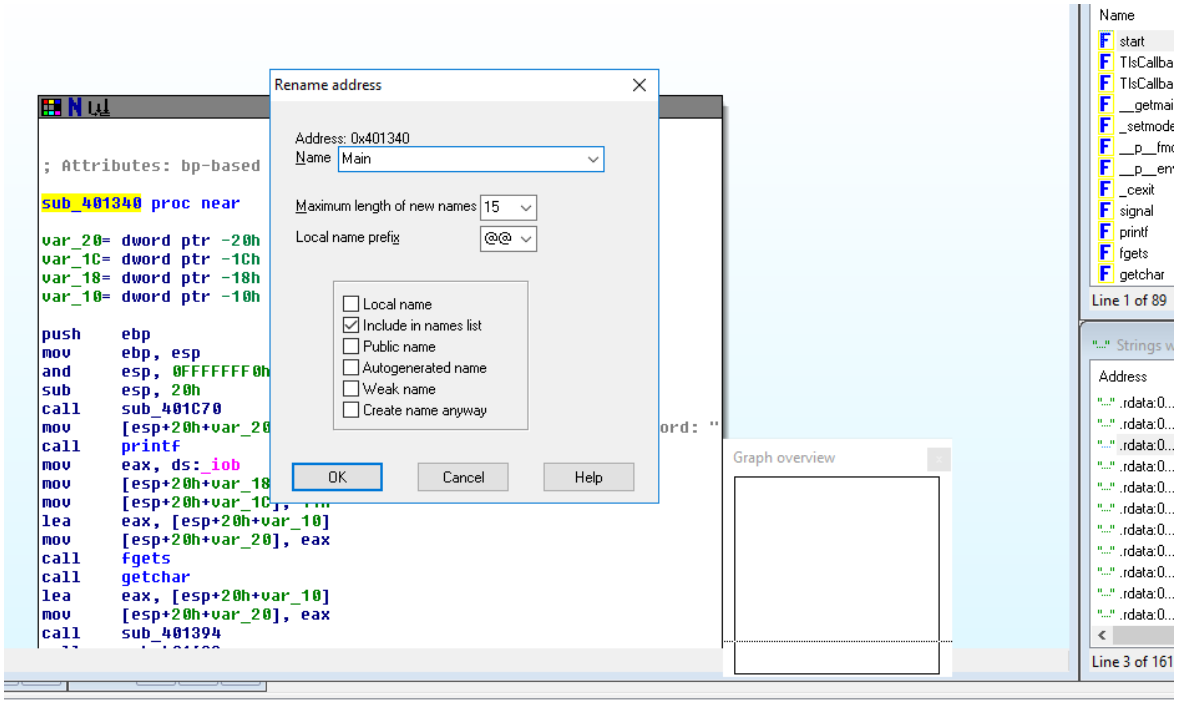
Right click on the sub routine name and select rename…



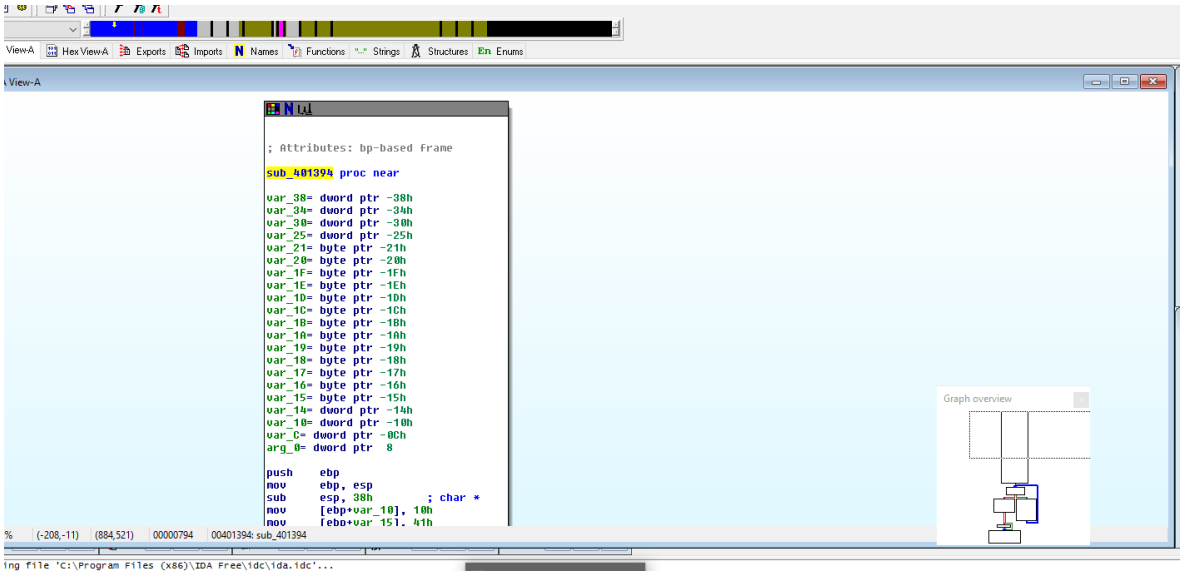


Cracking a Password

Reanme this sub routine ***Main***

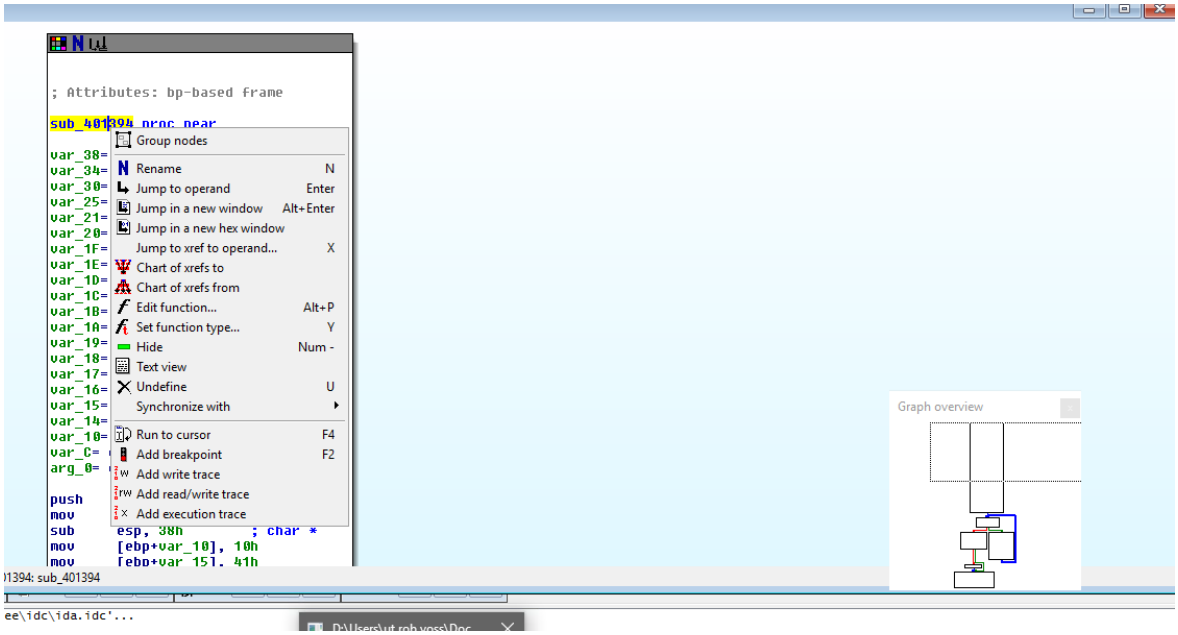


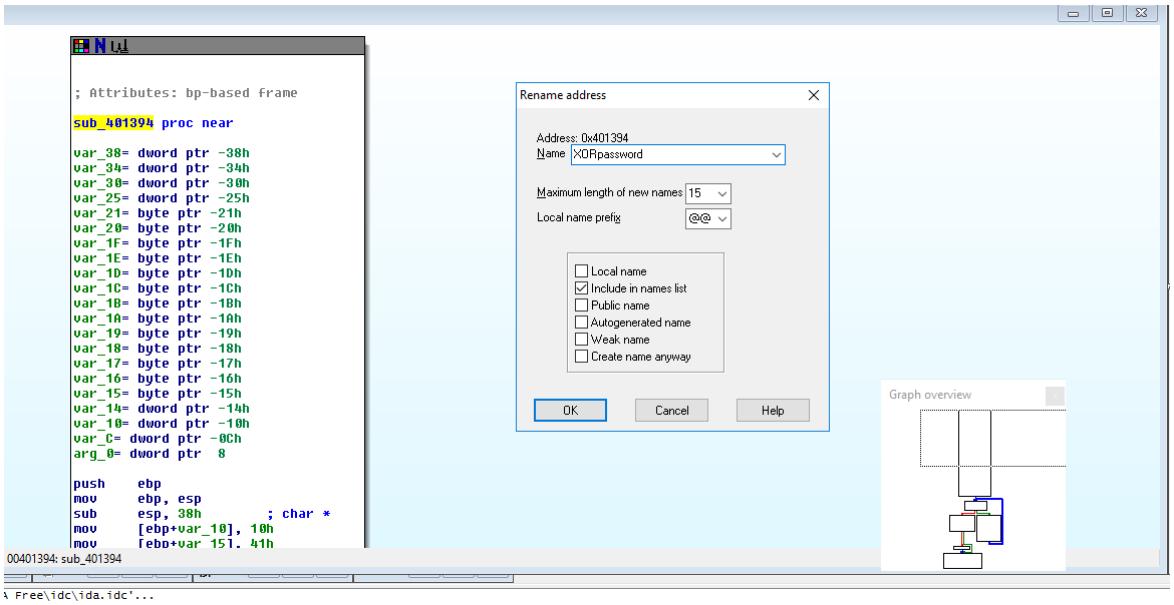
Select first call sub routine sub_401394



Cracking a Password

Rename it the XORpassword

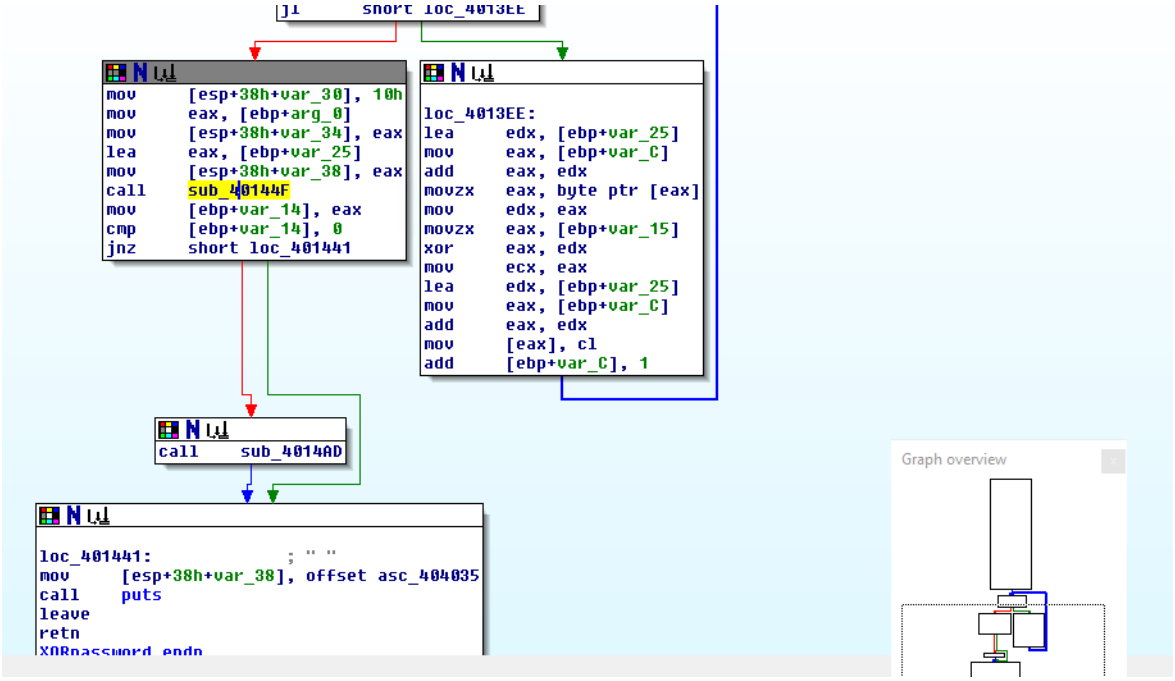


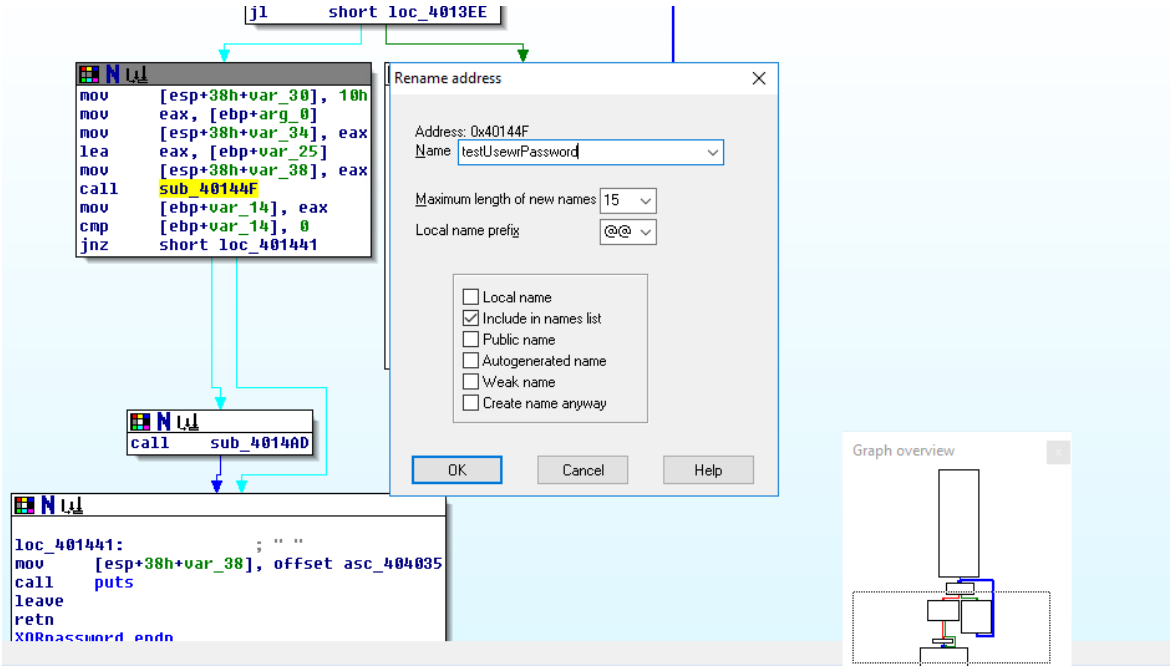


Cracking a Password

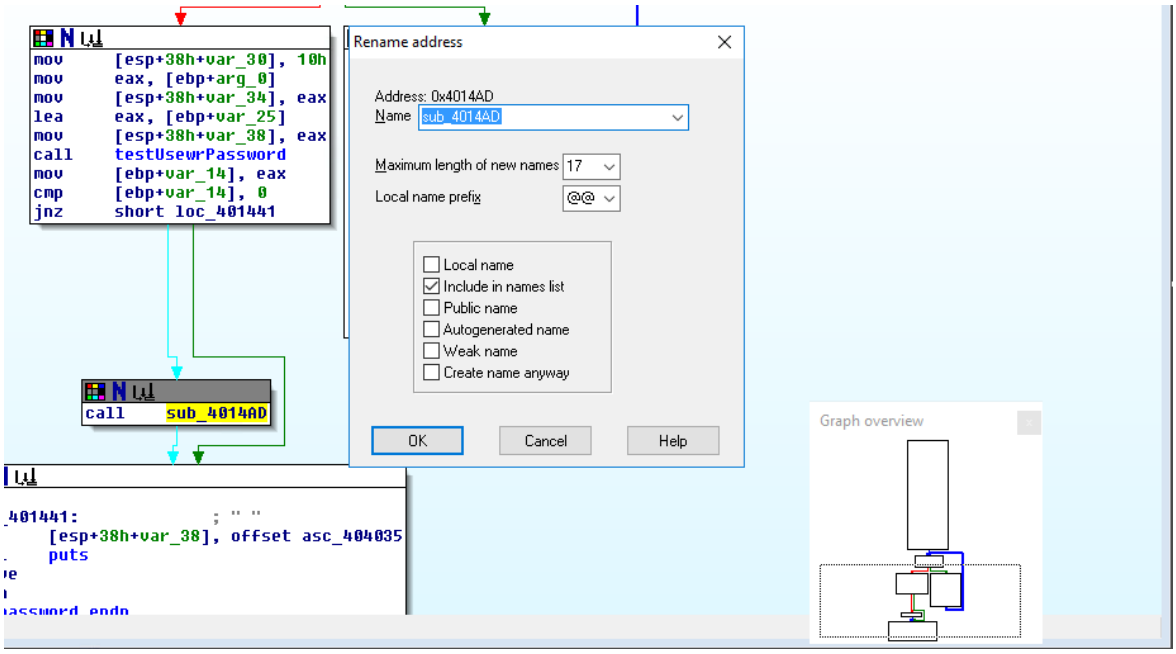
Scroll down and locate

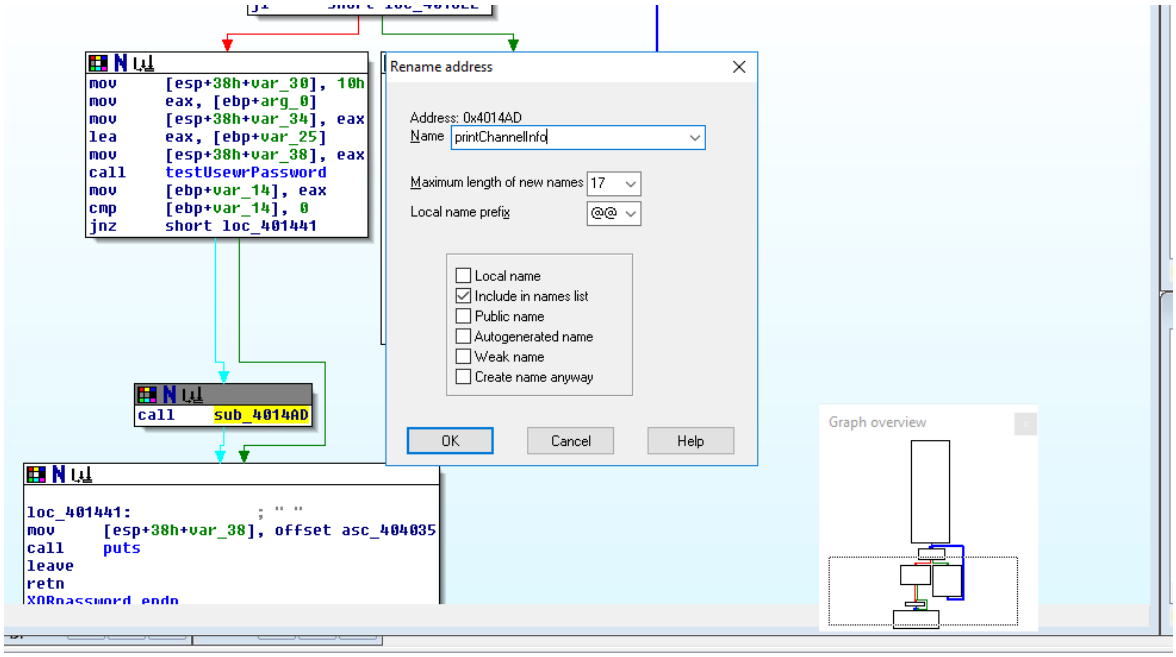
1) Password comparison sub routine
2) Print routine





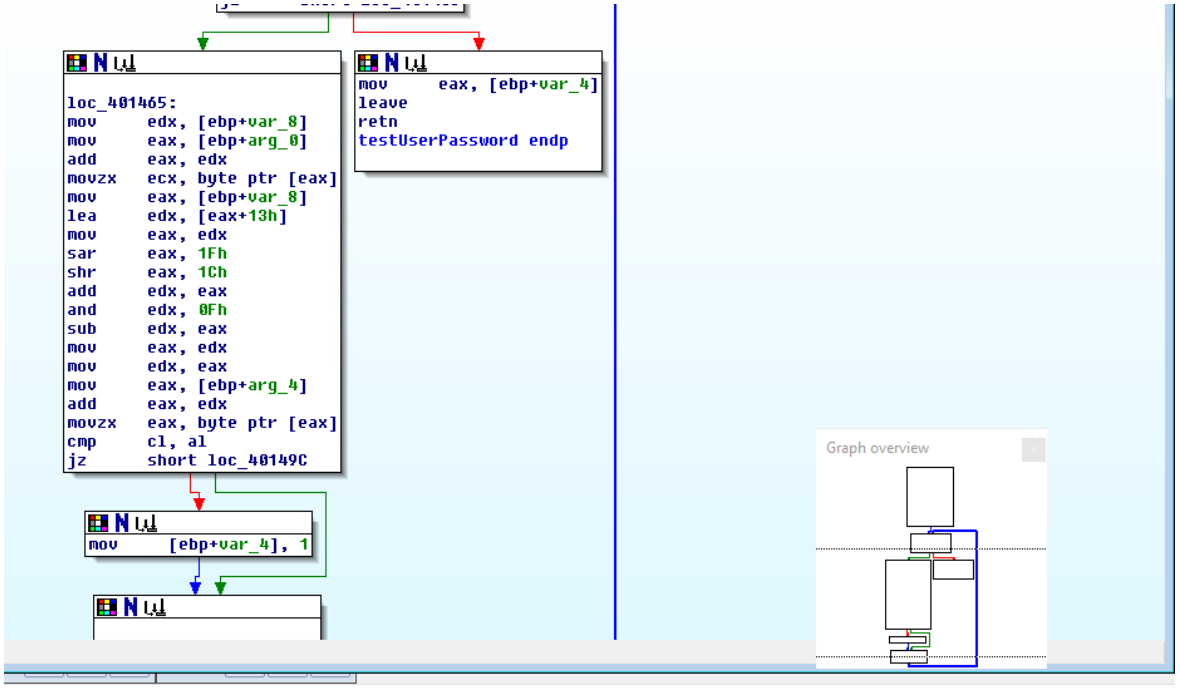
Cracking a Password



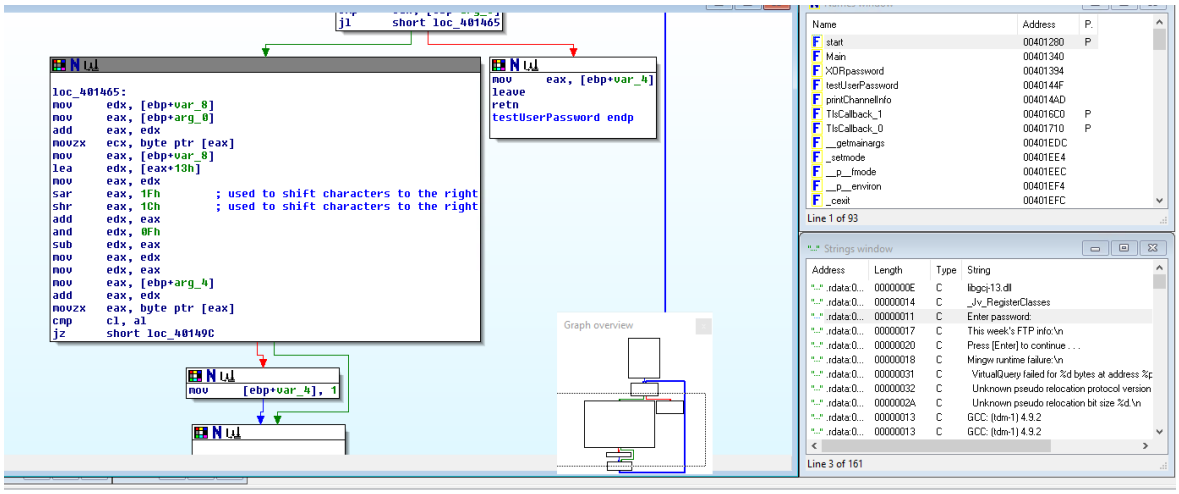


Cracking a Password

Return to and open testUserPassword
Investigate this sub routine

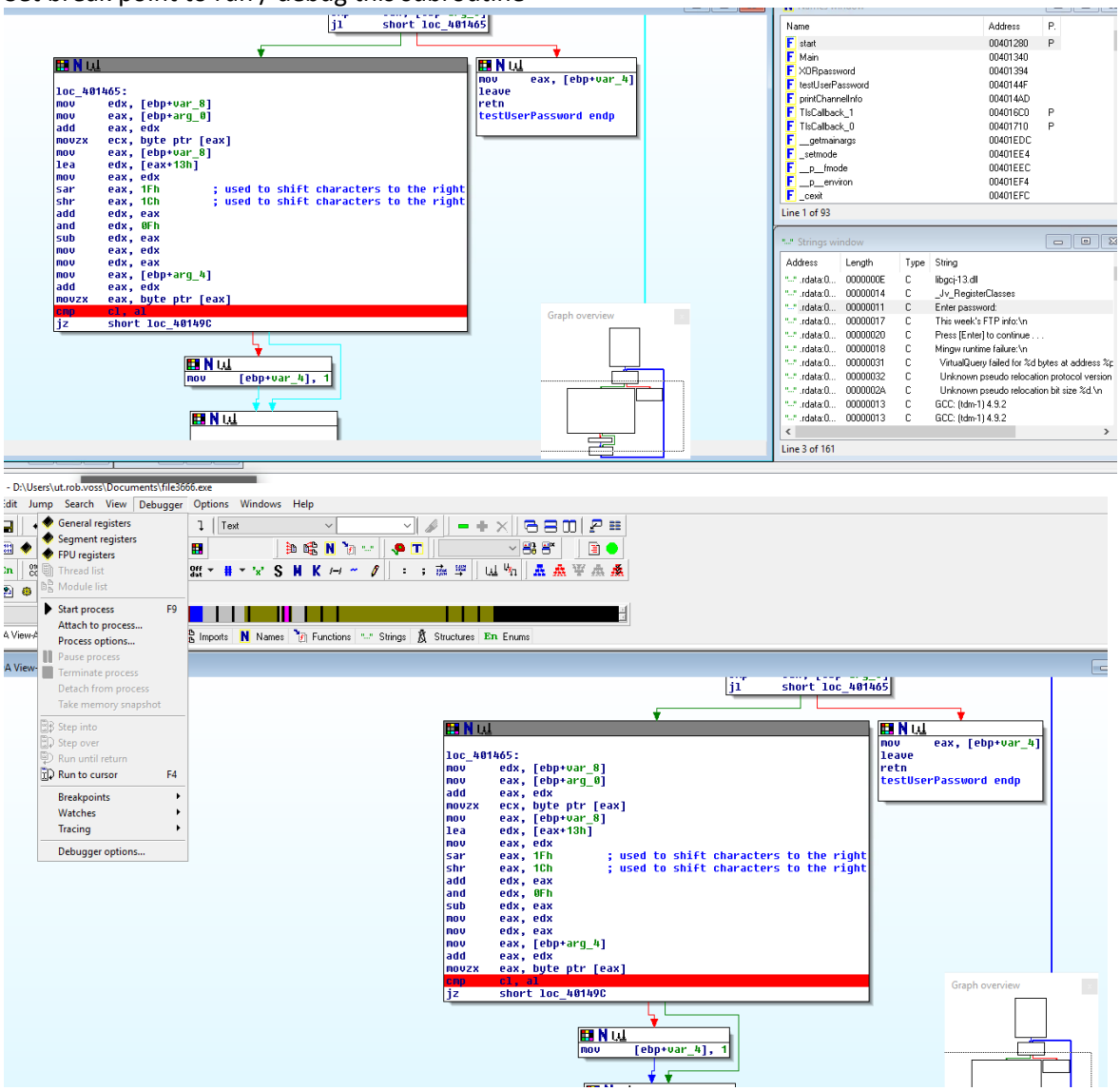


SAR and SHR are two new concepts…
They are both used to shift characters to the right…(SAL SHL will shift to the left)
Add a comment here
: used to shift characters to the right



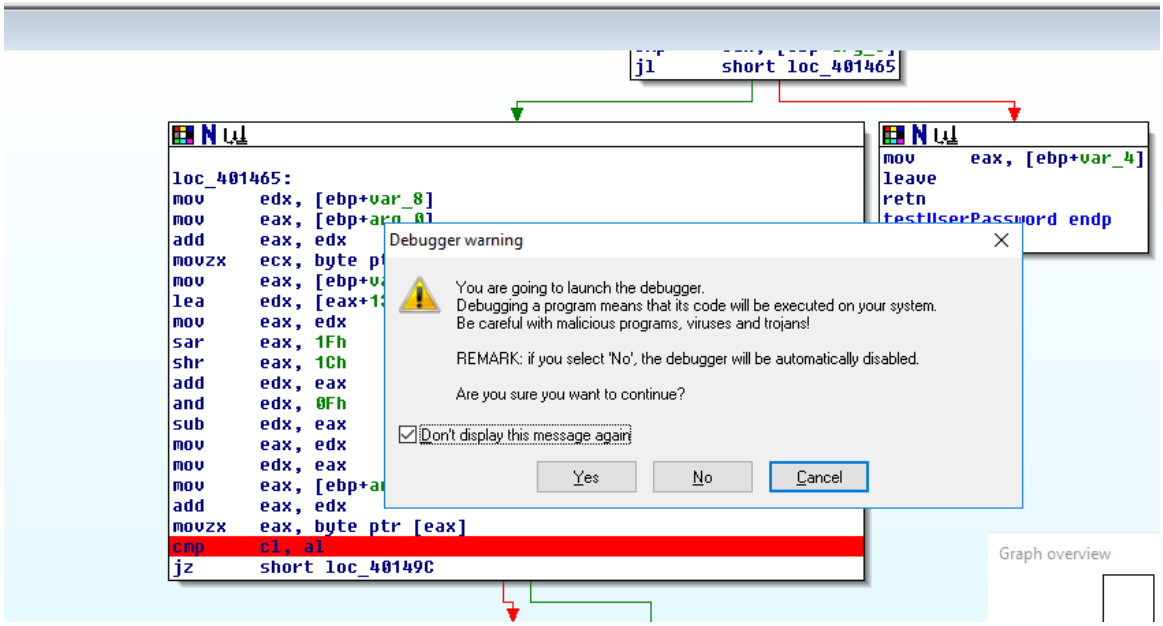
Cracking a Password

Set break point to run / debug this subroutine

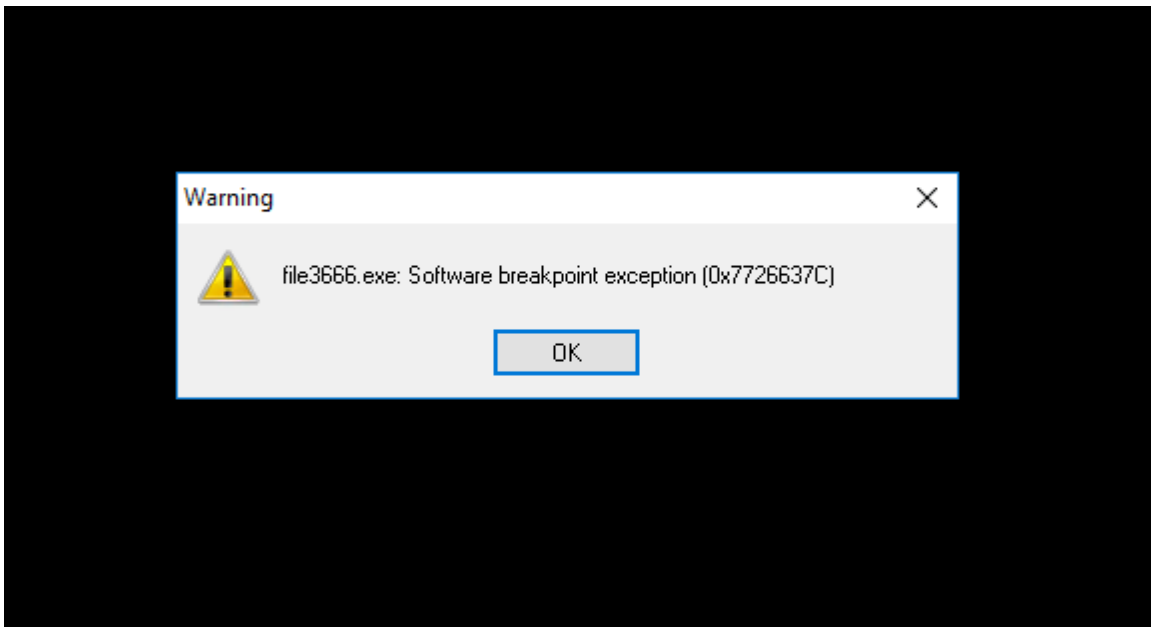


Start Process or F9

Cracking a Password

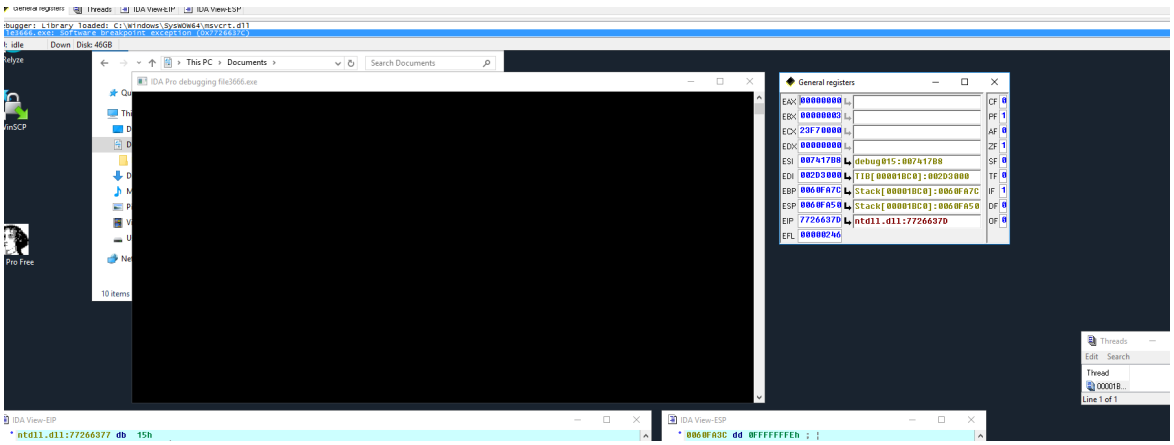


Knowing that this file is safe you can select don't display and hit yes



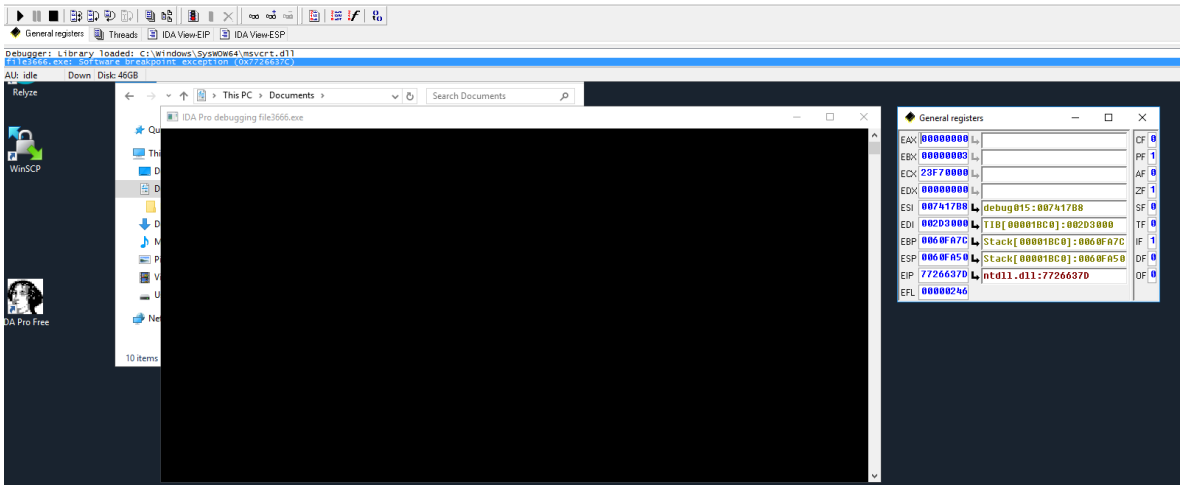
Hit OK

Cracking a Password



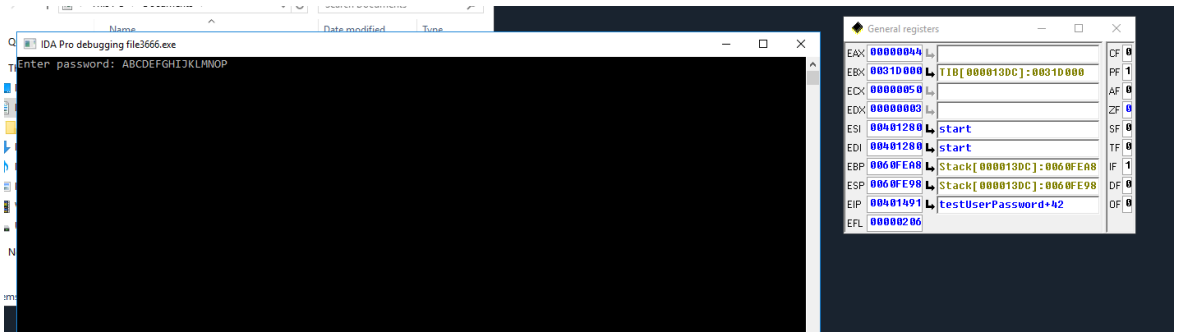
Start Process

Hit the right arrow button on the upper left task bar



Cracking a Password

Enter a password for testing…in this case something that will be easily identifiable in hex ABCDEFGHIJKLMNOP



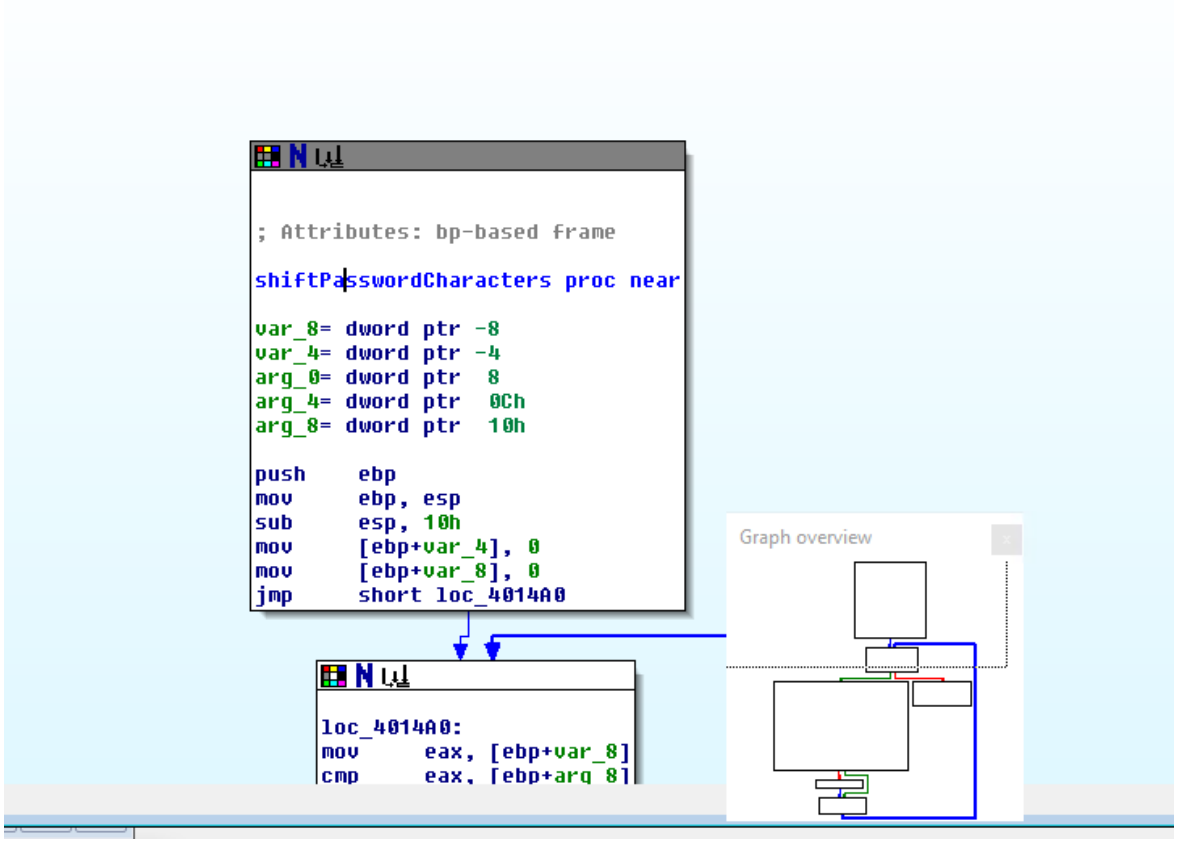
Cycling through the routine you can see that the registers are at different hex and will cycle up by one each time…

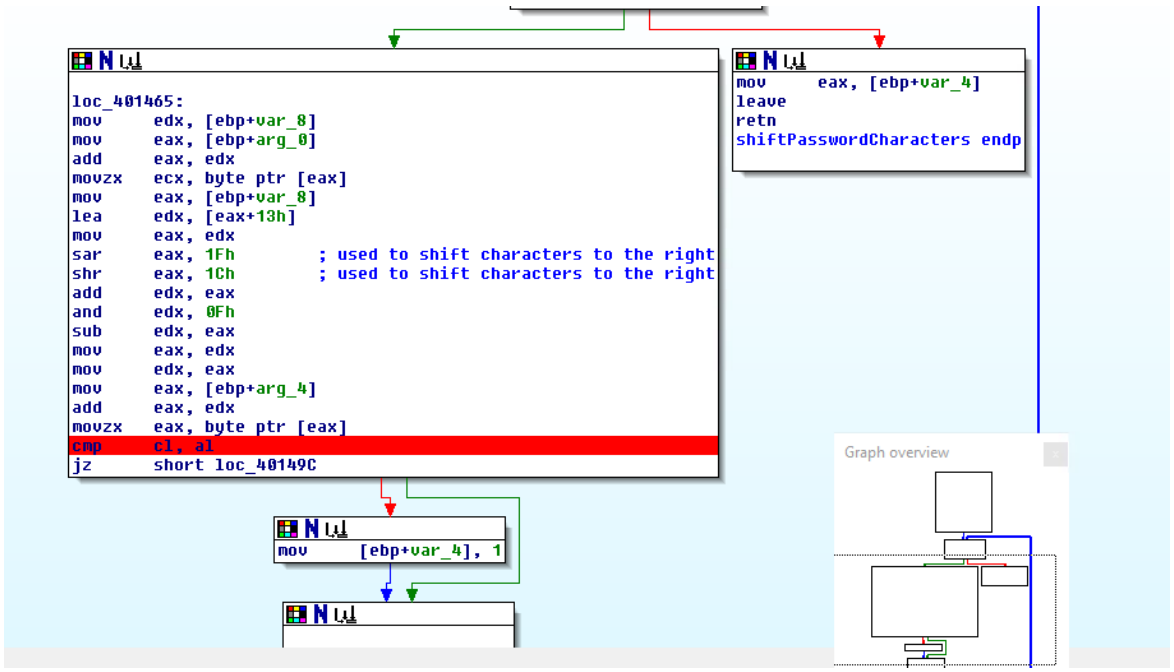
Through multiple processes it has become apparent that the password is similar to the original password PasswordStillSux…but this sun routine adds another element to it by shifting the characters 3 times to the right…as seen in register EDX…

Knowing this you can do two things now…
Rename the sub routine shiftPasswordCharacters

And you now know the password is SuxPasswordStill
When you push to the right on PasswordStillSux the last letter jumps to become the first letter…if you do 3 shifts the password now becomes SuxPasswordStill…

Cracking a Password





Cracking a Password

Run the password