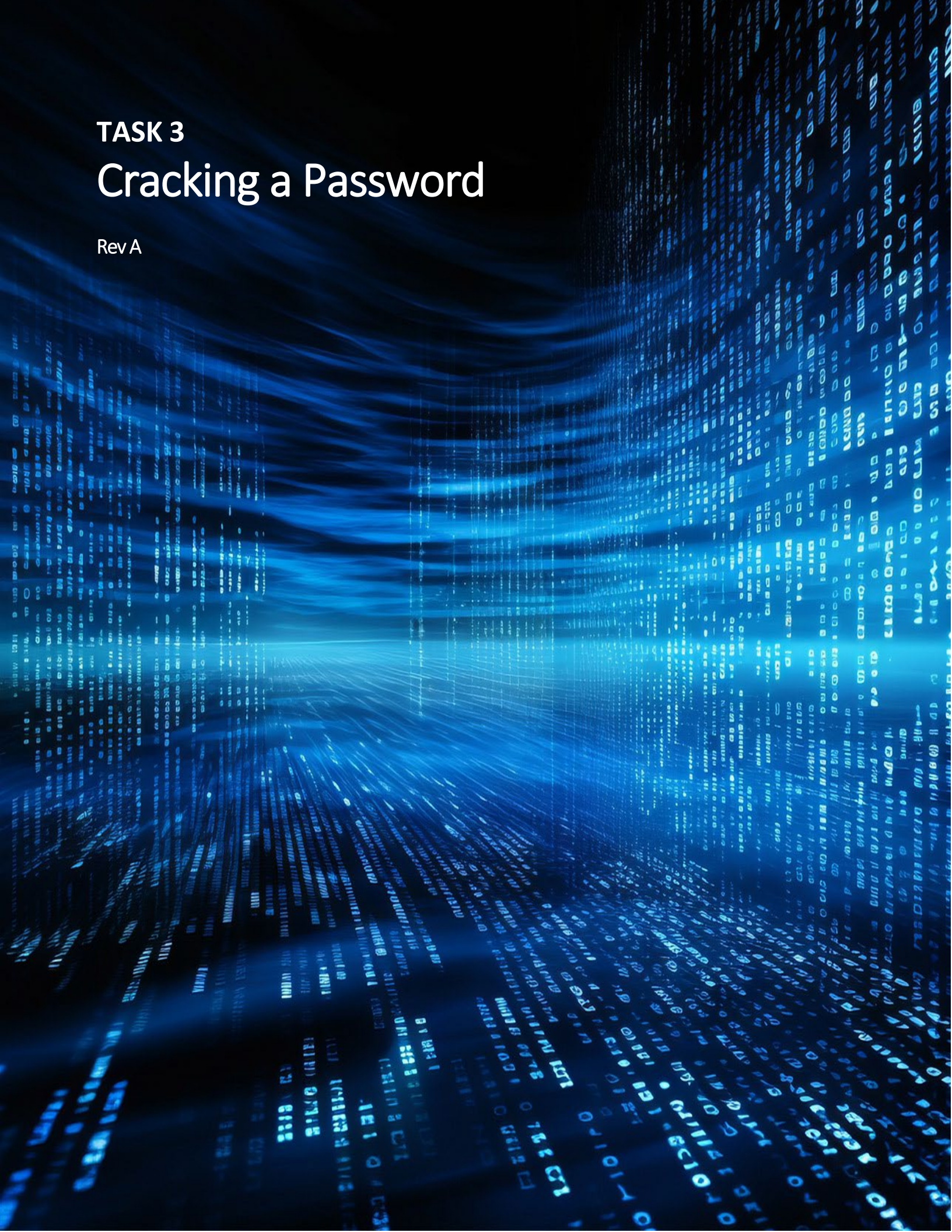


TASK 3

Cracking a Password

Rev A



Cracking a Password

1	Comparing Binaries Using Relyze	Error! Bookmark not defined.
2	Crack and Decrypt the Password.....	Error! Bookmark not defined.
3	Converting From HEX to ASCII	Error! Bookmark not defined.
4	Run the Program.....	Error! Bookmark not defined.
5	Connect to the IRC Channel.....	Error! Bookmark not defined.
5.1	Open PuTTY.....	Error! Bookmark not defined.
5.1.1	Input Host Name.....	Error! Bookmark not defined.
5.1.2	Input Username.....	Error! Bookmark not defined.
5.1.3	Input Password	Error! Bookmark not defined.
5.2	Input irssi.....	Error! Bookmark not defined.
5.2.1	Set Nickname	Error! Bookmark not defined.
5.2.2	Request Network List.....	Error! Bookmark not defined.
5.2.3	Connect to network (somber)	Error! Bookmark not defined.
5.2.4	Join #nymeria.....	Error! Bookmark not defined.
5.3	Observe conversation	Error! Bookmark not defined.
5.3.1	Identify Other Players	Error! Bookmark not defined.
5.3.2	See Who the Players Are	Error! Bookmark not defined.

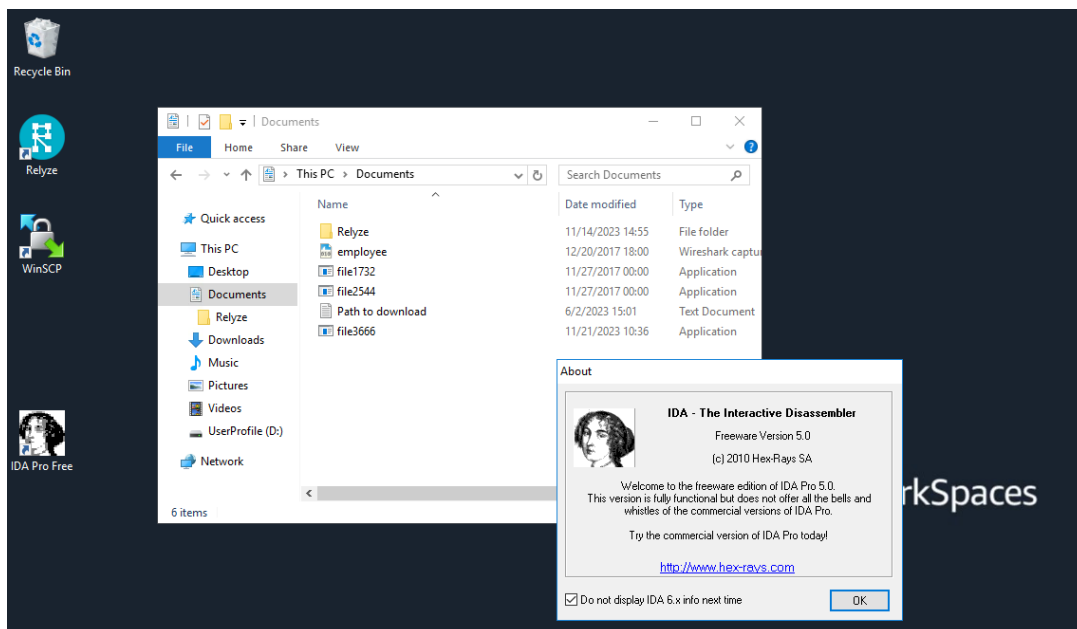
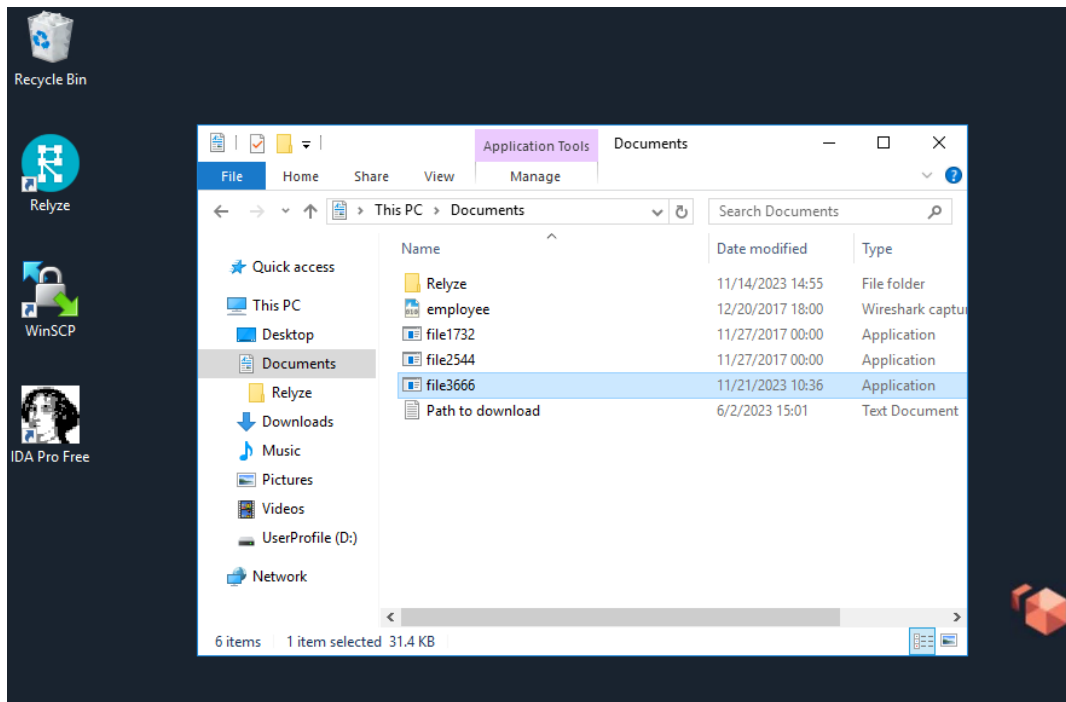
Cracking a Password

1 Opening a File in IDA Pro

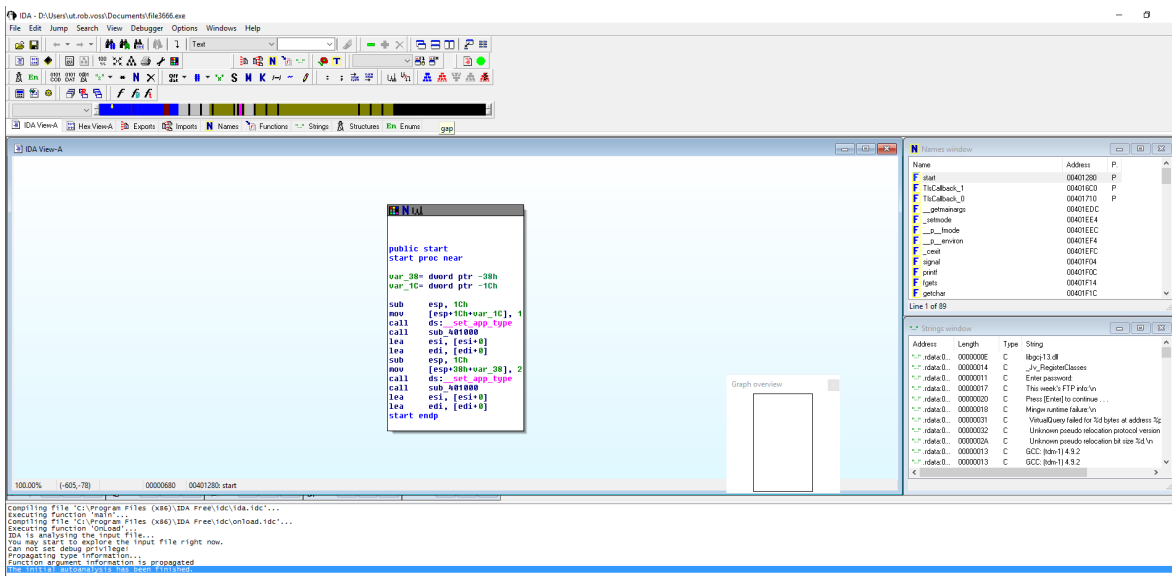
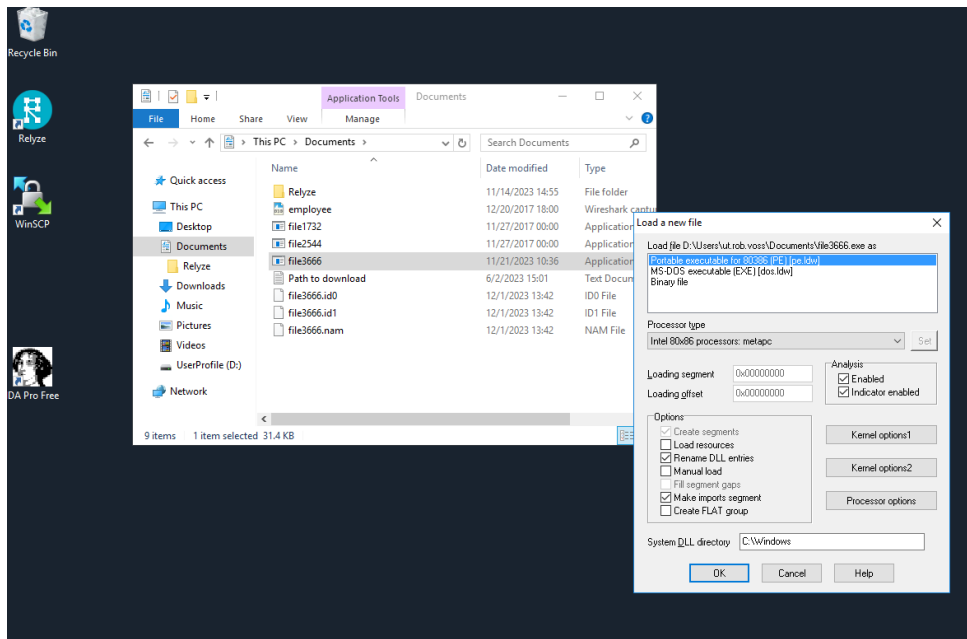
Open file 3666 in IDA Pro

Select file and drag and drop on top of IDA Pro

Click ok



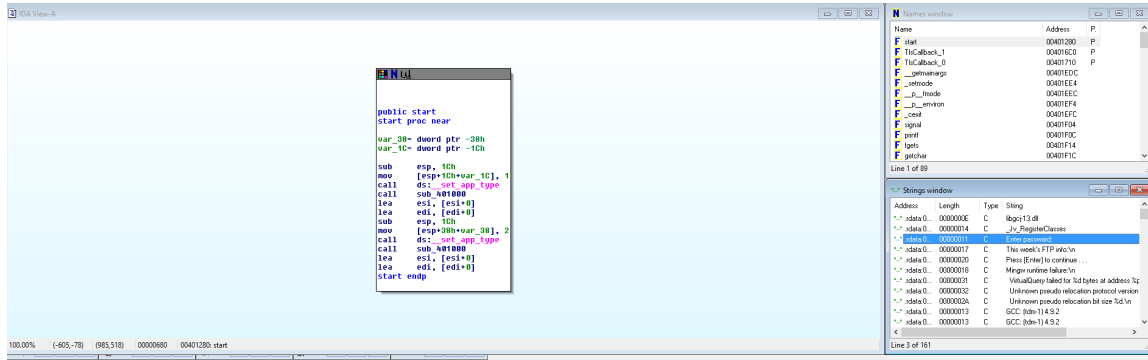
Cracking a Password



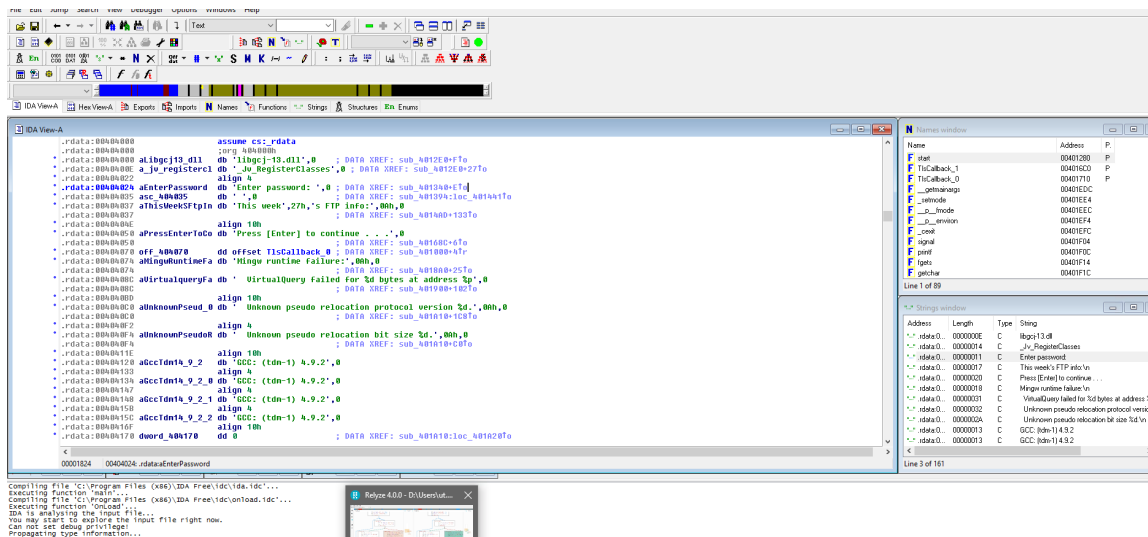
Cracking a Password

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.)

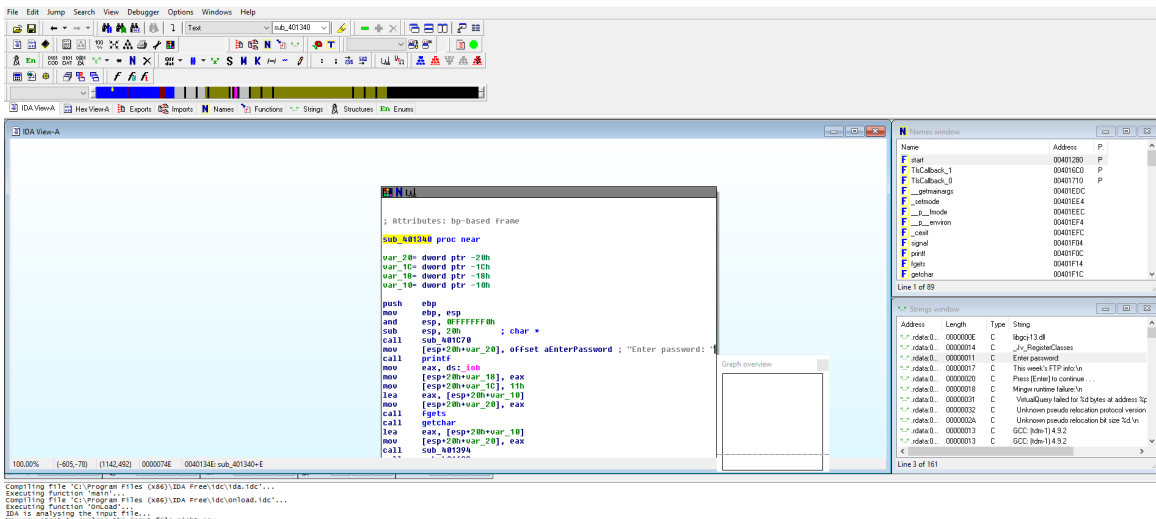
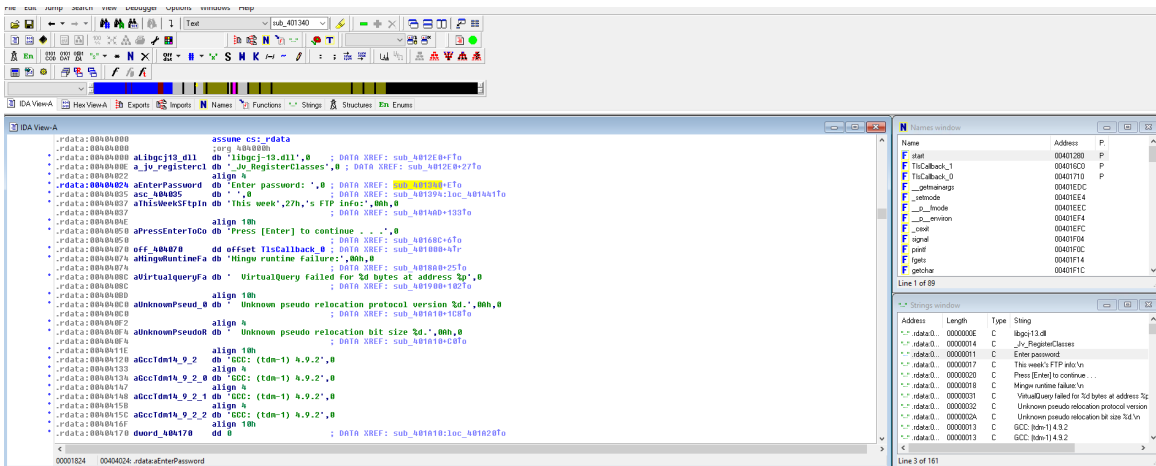


Double click on sub routine to have it load into the View a window



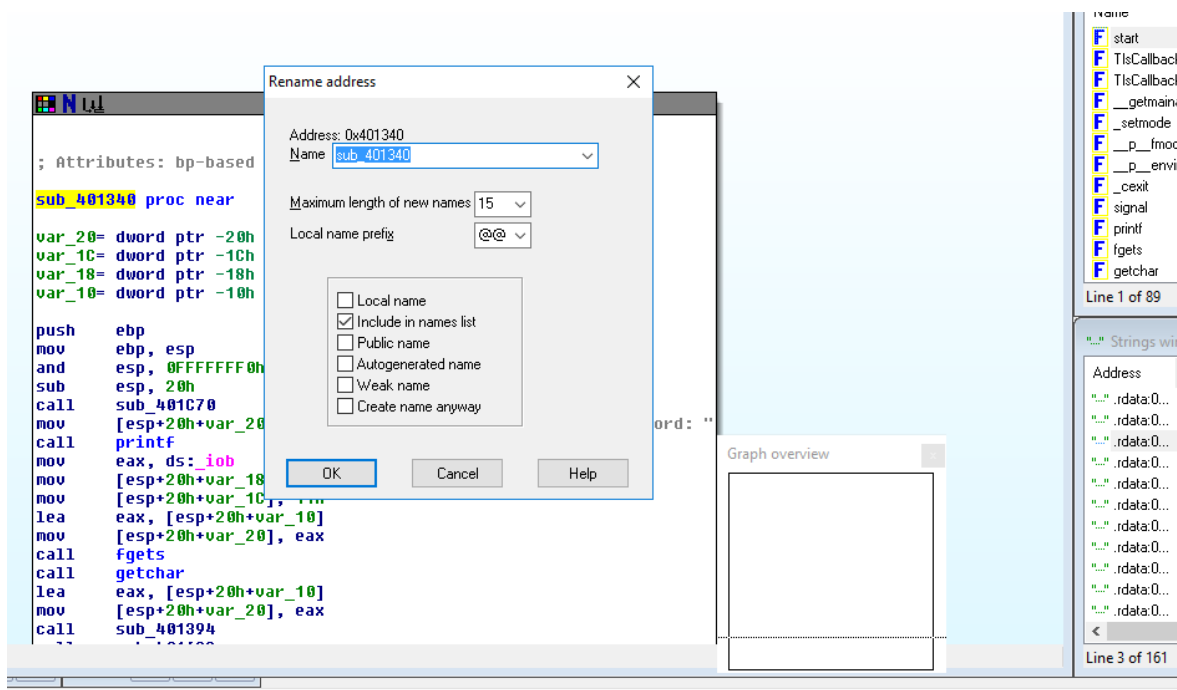
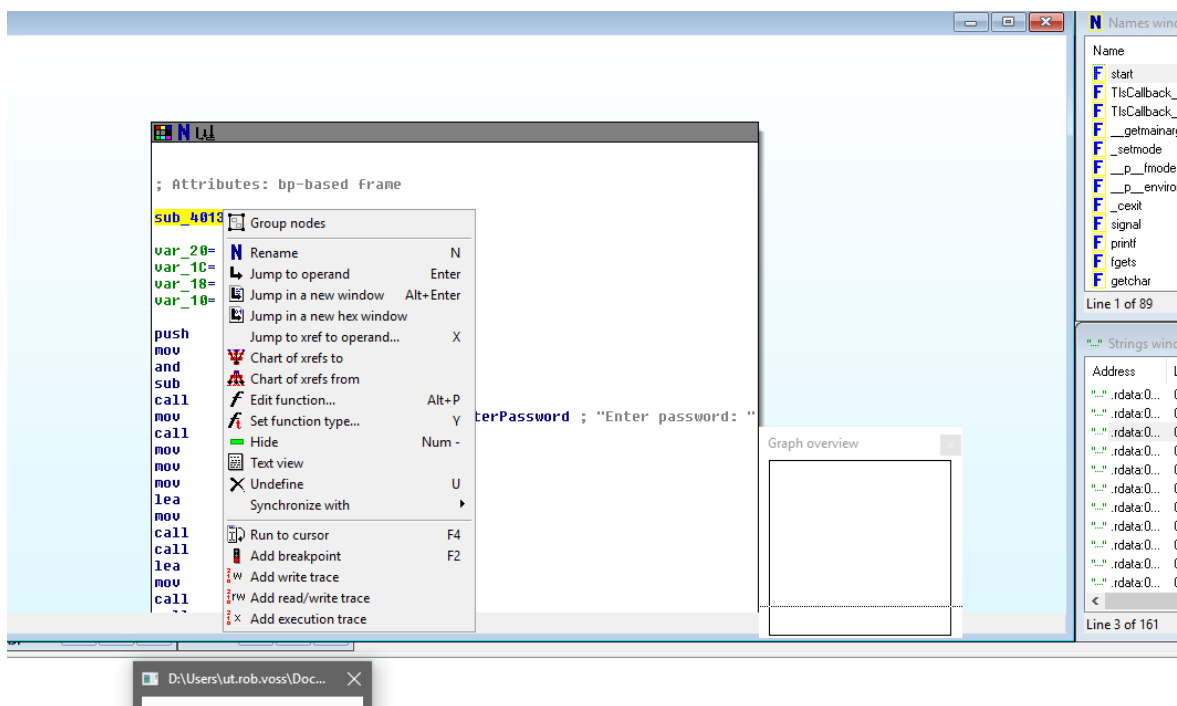
Cracking a Password

Find the sub routine and double click on it...



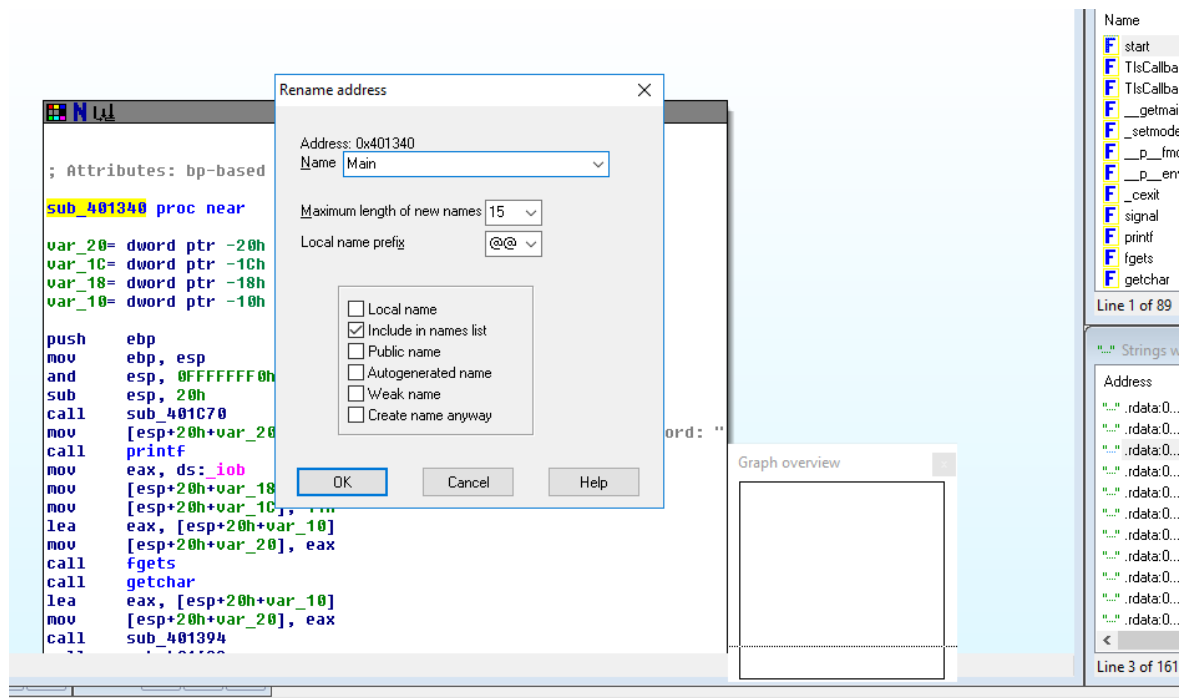
Cracking a Password

Right click on the sub routine name and select rename...

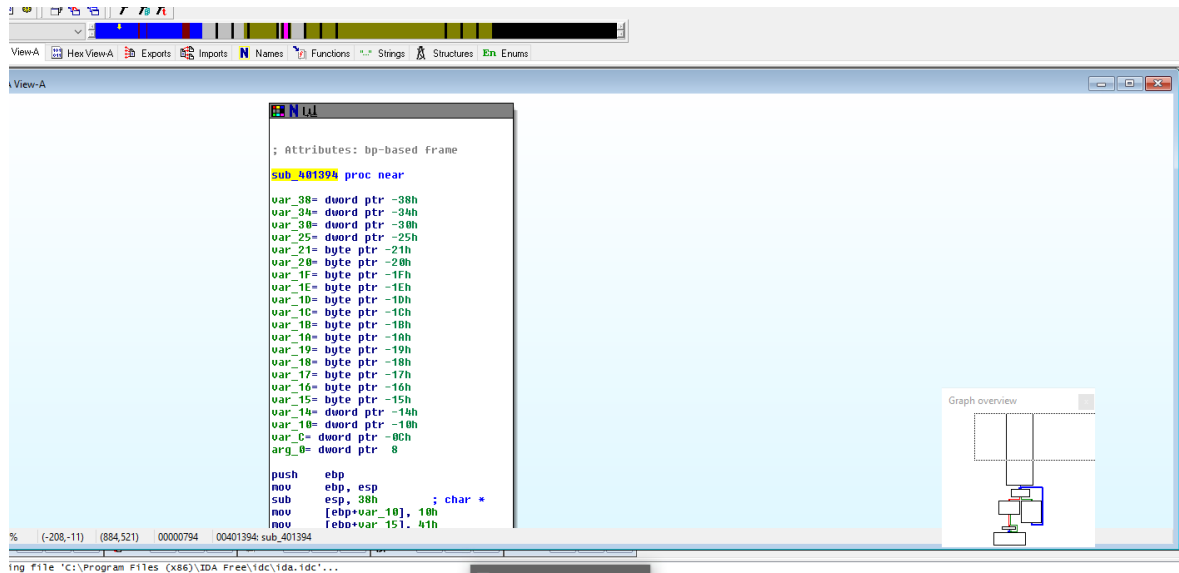


Cracking a Password

Reaname this sub routine **Main**

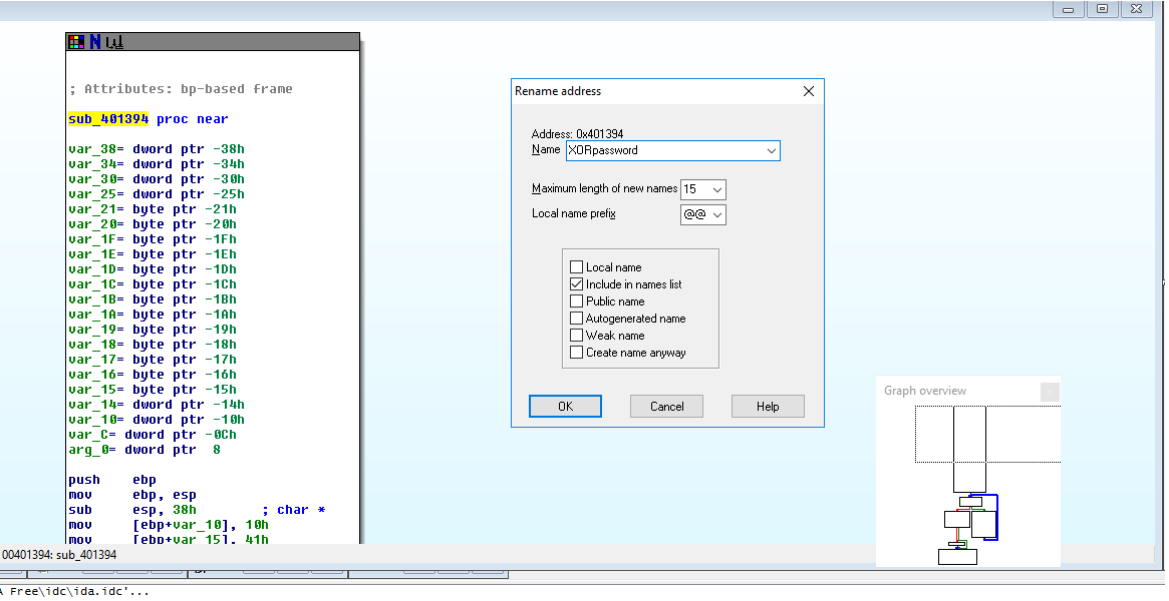
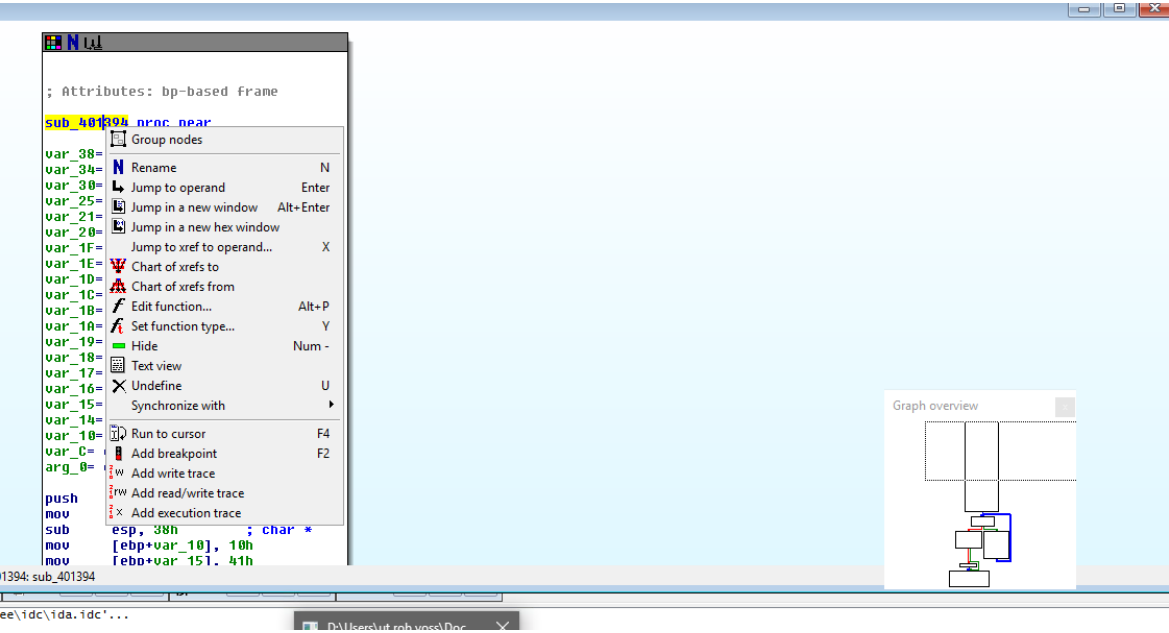


Select first call sub routine sub_401394



Cracking a Password

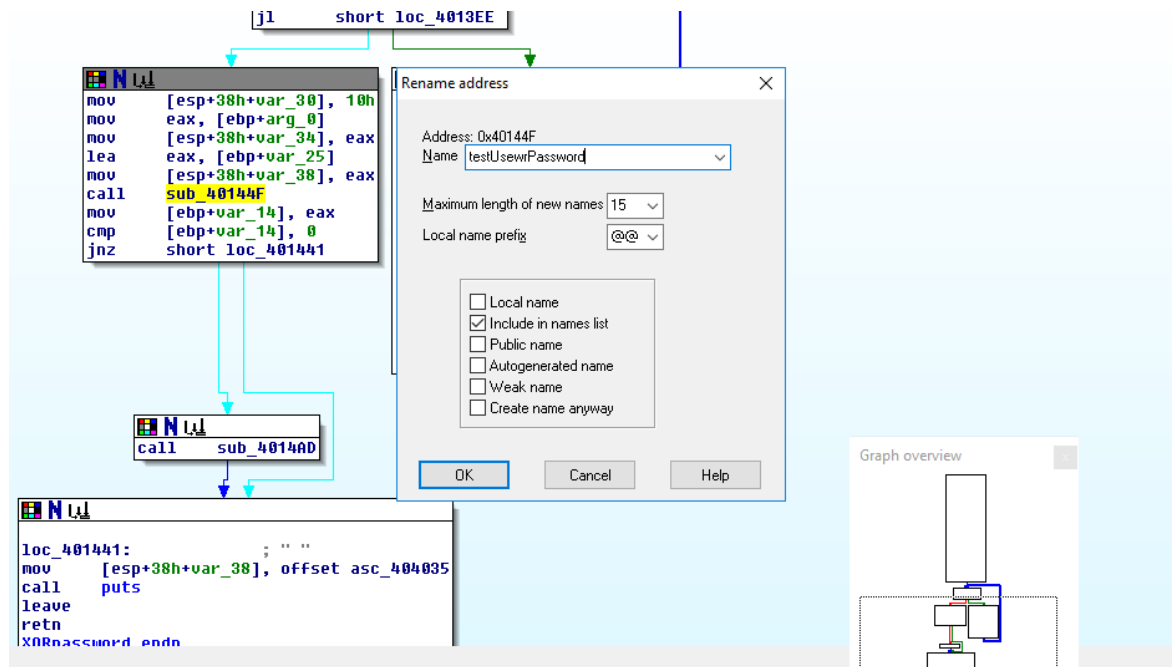
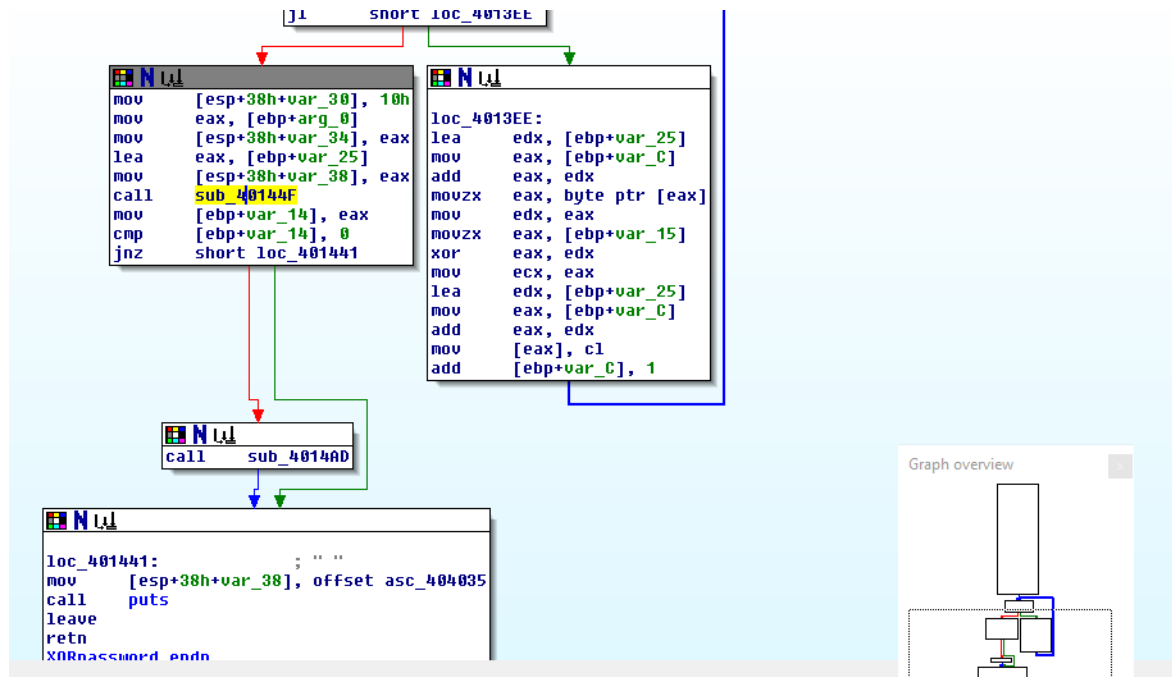
Rename it the XORpassword



Cracking a Password

Scroll down and locate

- 1) Password comparison sub routine
- 2) Print routine



Cracking a Password

The screenshot displays a debugger window with assembly code and a 'Rename address' dialog box. The assembly code is as follows:

```
mov [esp+38h+var_30], 10h
mov eax, [ebp+arg_0]
mov [esp+38h+var_34], eax
lea eax, [ebp+var_25]
mov [esp+38h+var_38], eax
call testUserPassword
mov [ebp+var_14], eax
cmp [ebp+var_14], 0
jnz short loc_401441

loc_401441:
mov [esp+38h+var_38], offset asc_404035
puts
password endn
```

The 'Rename address' dialog box is open, showing the address 0x4014AD and the name 'sub_4014AD'. The dialog box has the following options:

- Maximum length of new names: 17
- Local name prefix: @@
- ☐ Local name
- ☒ Include in names list
- ☐ Public name
- ☐ Autogenerated name
- ☐ Weak name
- ☐ Create name anyway

The 'Graph overview' window shows a control flow graph with a single block.

The second screenshot shows the same assembly code, but the 'Rename address' dialog box is now showing the name 'printChannelInfo' instead of 'sub_4014AD'. The assembly code is as follows:

```
mov [esp+38h+var_30], 10h
mov eax, [ebp+arg_0]
mov [esp+38h+var_34], eax
lea eax, [ebp+var_25]
mov [esp+38h+var_38], eax
call testUserPassword
mov [ebp+var_14], eax
cmp [ebp+var_14], 0
jnz short loc_401441

loc_401441:
mov [esp+38h+var_38], offset asc_404035
call puts
leave
retn
XORpassword endn
```

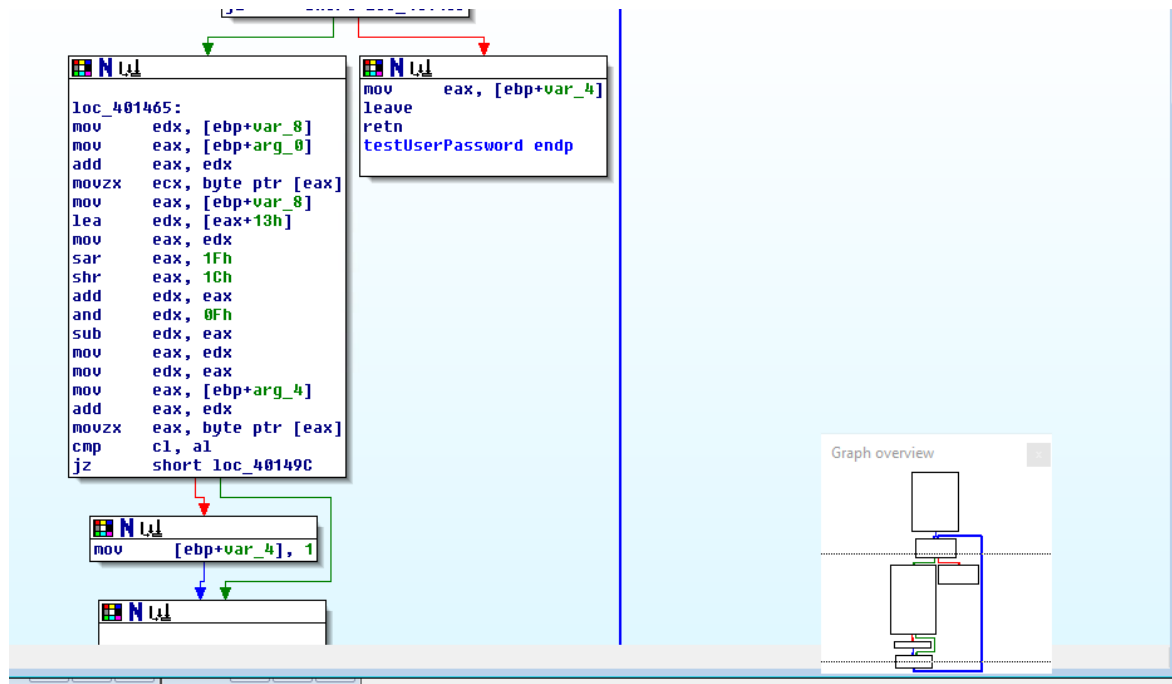
The 'Rename address' dialog box is open, showing the address 0x4014AD and the name 'printChannelInfo'. The dialog box has the following options:

- Maximum length of new names: 17
- Local name prefix: @@
- ☐ Local name
- ☒ Include in names list
- ☐ Public name
- ☐ Autogenerated name
- ☐ Weak name
- ☐ Create name anyway

The 'Graph overview' window shows a control flow graph with a single block.

Cracking a Password

Return to and open testUserPassword
Investigate this sub routine

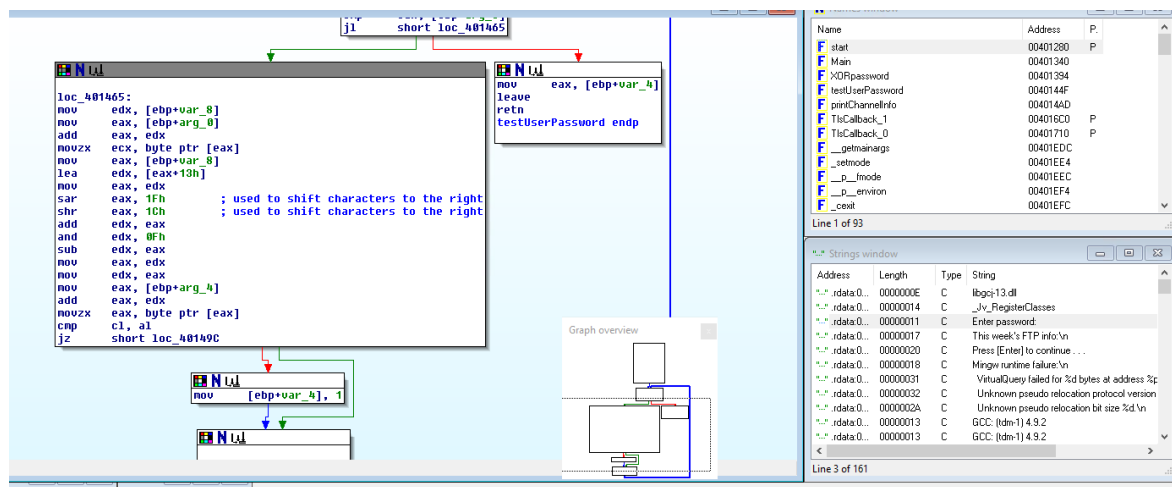


SAR and SHR are two new concepts...

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

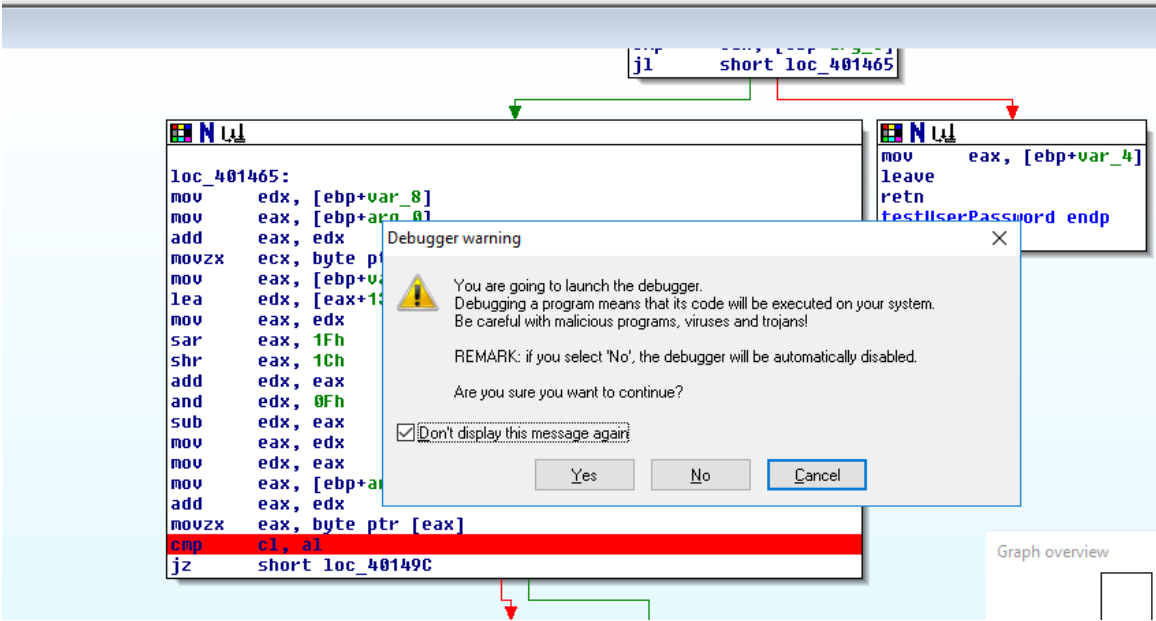
Set break point to run / debug this subroutine

The screenshot displays a debugger interface with the following components:

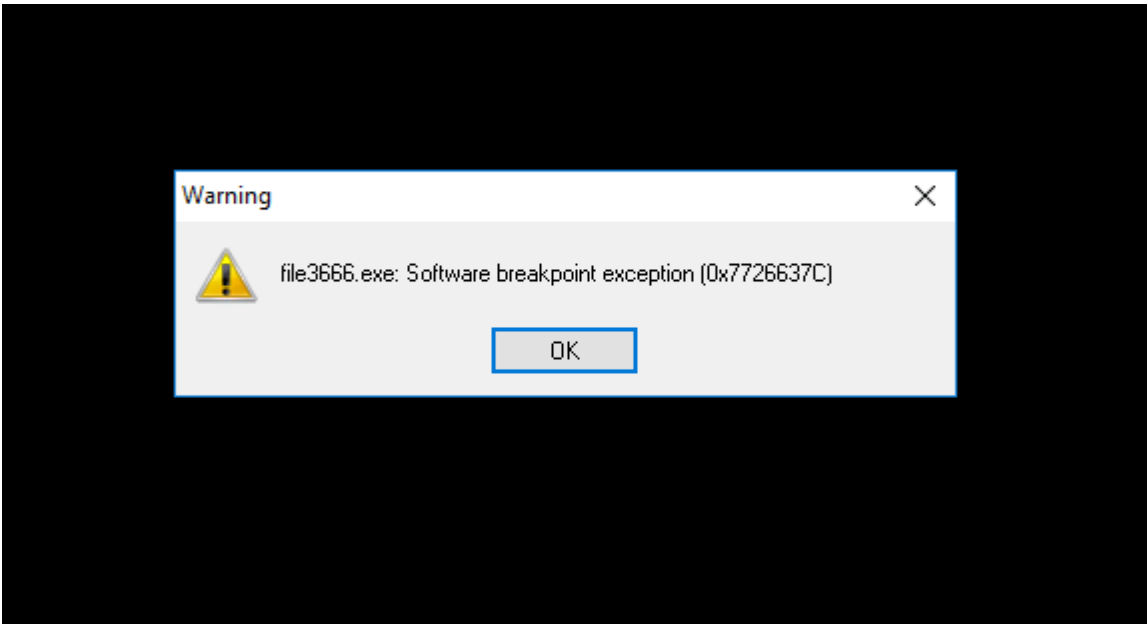
- Assembly Window:** Shows the assembly code for the subroutine `loc_401465`. The code includes instructions for moving registers, adding arguments, and performing conditional jumps. A red line highlights the instruction `movzx eax, byte ptr [eax]` at address `loc_40149C`.
- String window:** Lists strings found in the program, including "ibgc-13.dll", "Jv_RegisterClasses", "Enter password", and various error messages.
- Debugger Controls:** A sidebar on the left contains buttons for "Start process", "Attach to process...", "Process options...", "Pause process", "Terminate process", "Detach from process", "Take memory snapshot", "Step into", "Step over", "Run until return", "Run to cursor", "Breakpoints", "Watches", "Tracing", and "Debugger options...".
- Graph overview:** A small window showing a control flow graph of the assembly code.

Start Process or F9

Cracking a Password

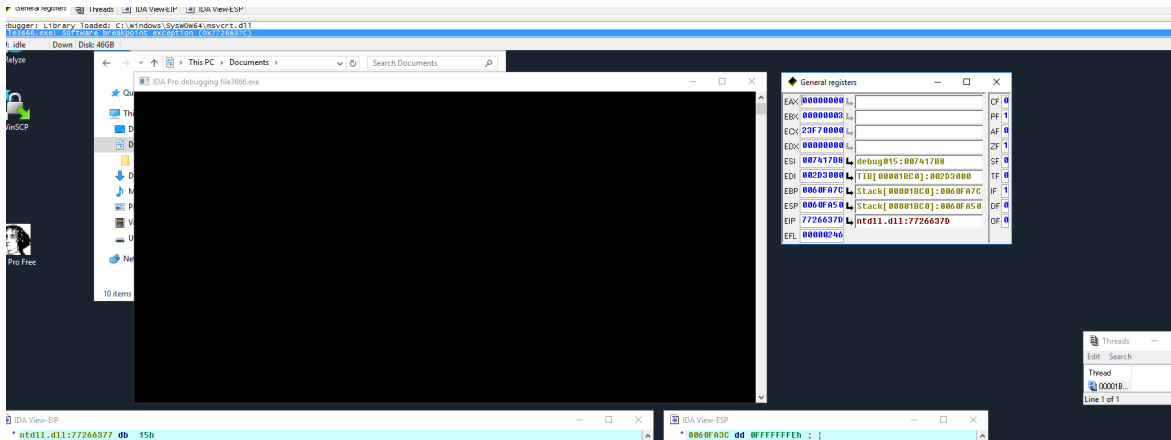


Knowing that this file is safe you can select don't display and hit yes



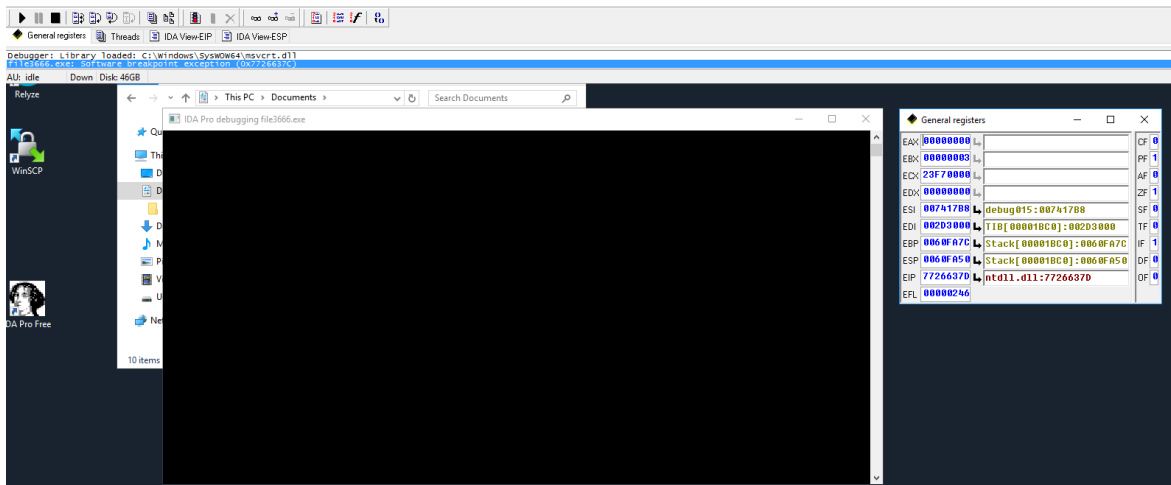
Hit OK

Cracking a Password



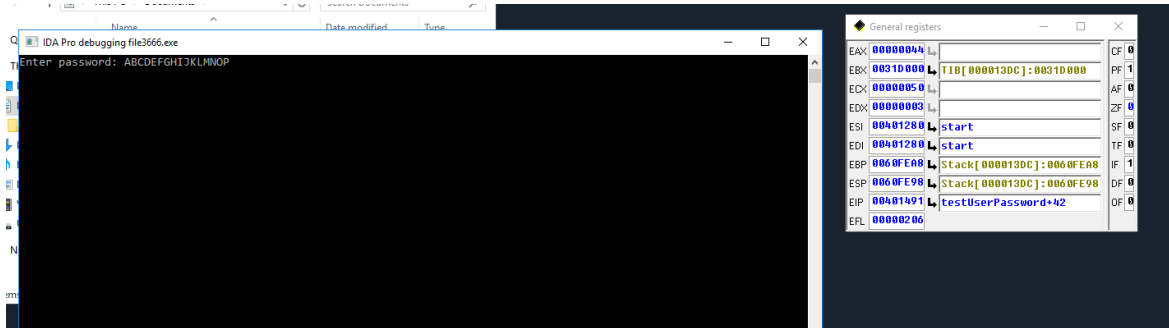
Start Process

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
ABCDEF GHIJ KLMNOP



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...

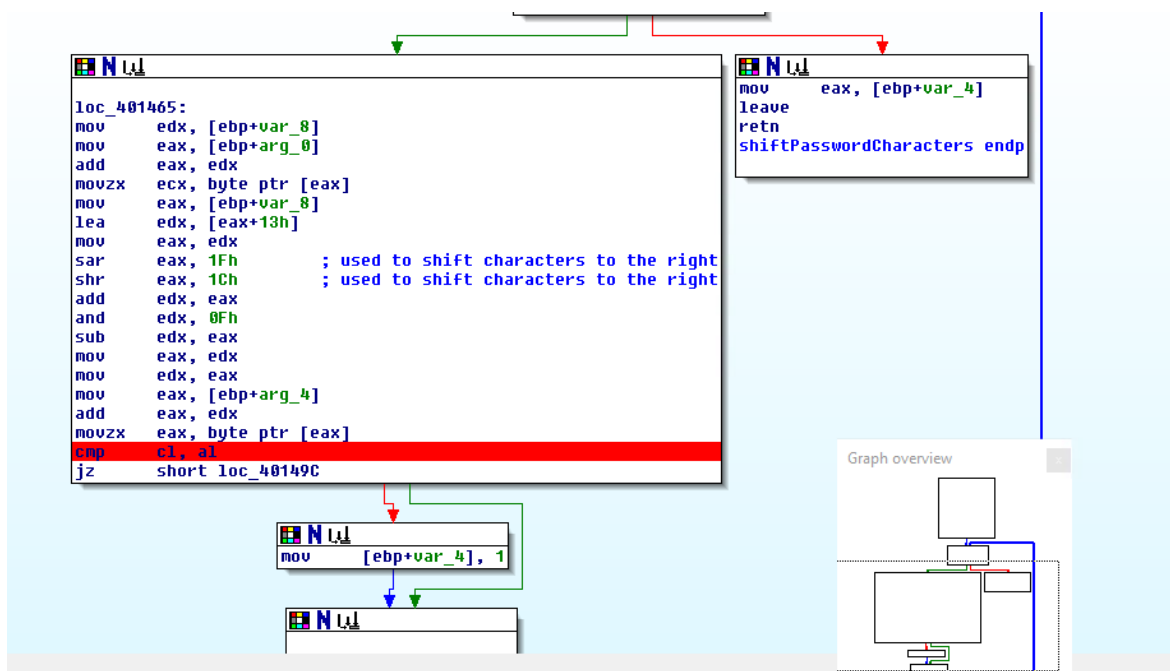
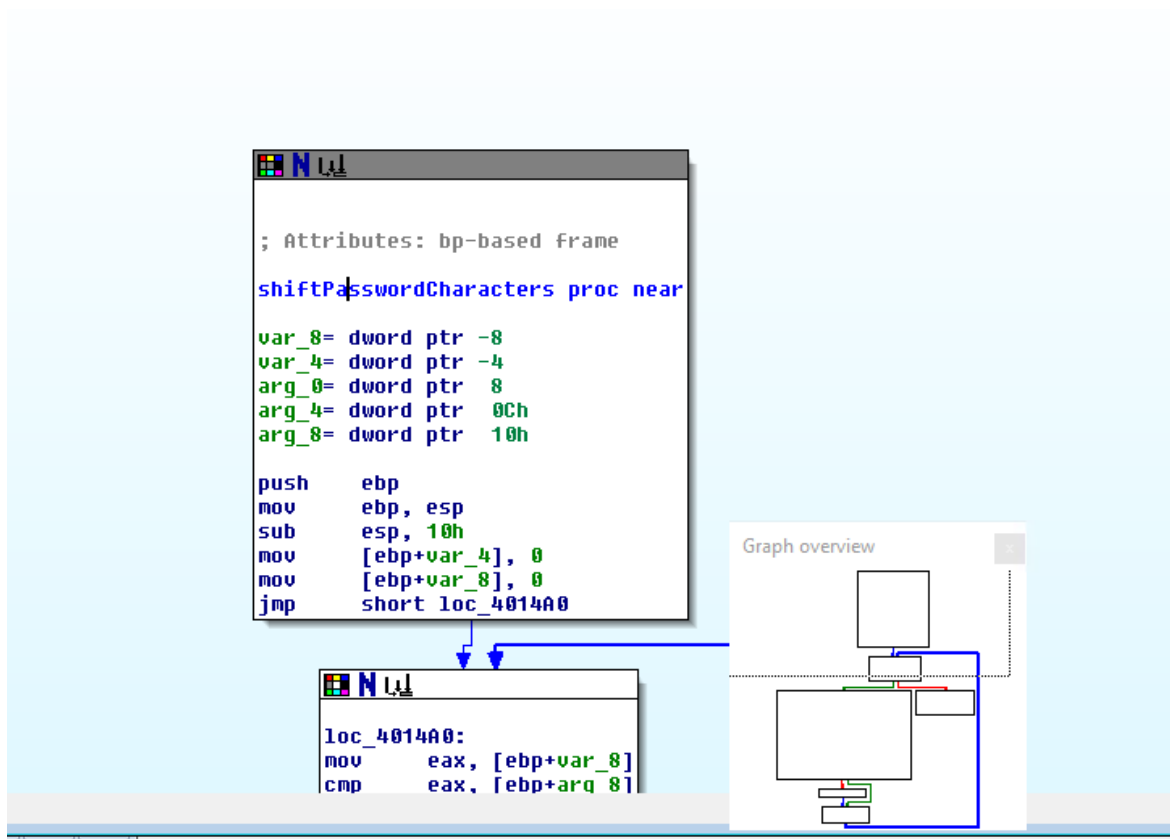
Knowing this you can do two things now...

Rename the sub routine shiftPasswordCharacters

And you now know the password is SuxPasswordStill

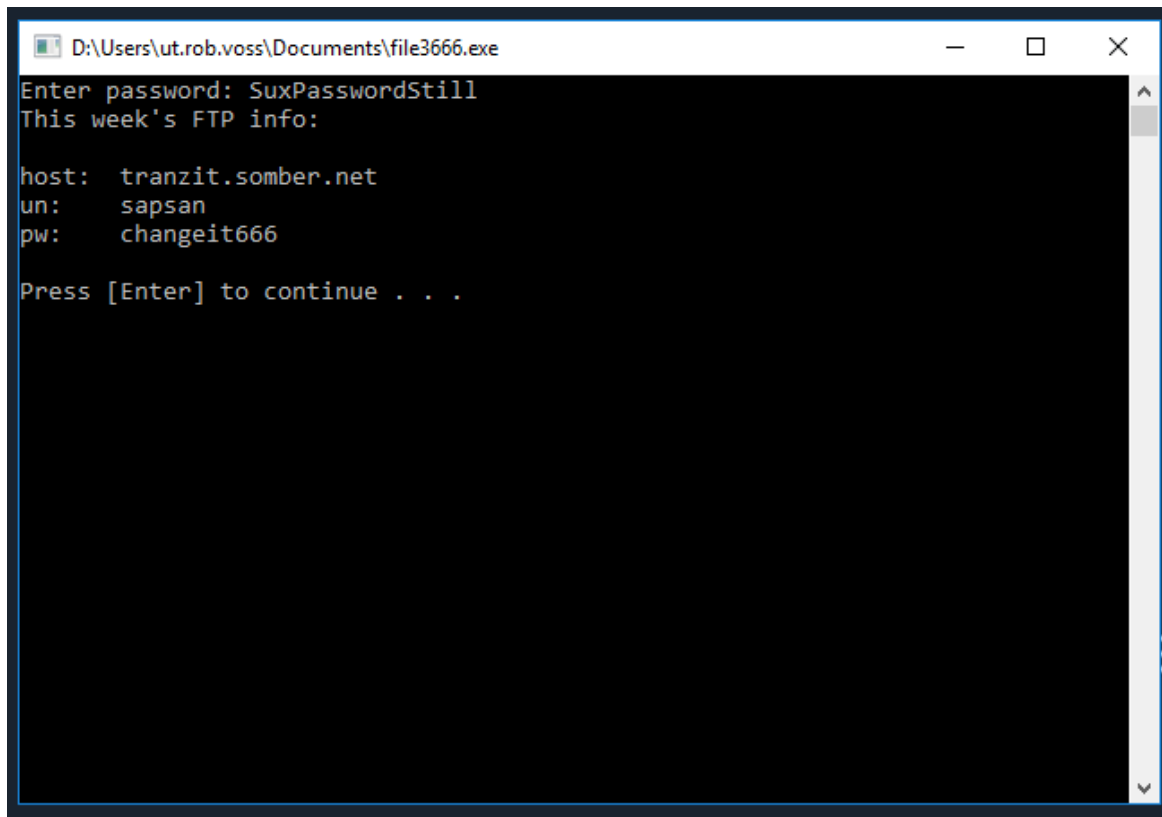
When you push to the right on PasswordStillSux the last letter jumps to become the first letter...if you do 3 shifts the password now becomes SuxPasswordStill...

Cracking a Password



Cracking a Password

Run the password



```
D:\Users\ut.rob.voss\Documents\file3666.exe
Enter password: SuxPasswordStill
This week's FTP info:

host: transit.somber.net
un:  sapsan
pw:  changeit666

Press [Enter] to continue . . .
```