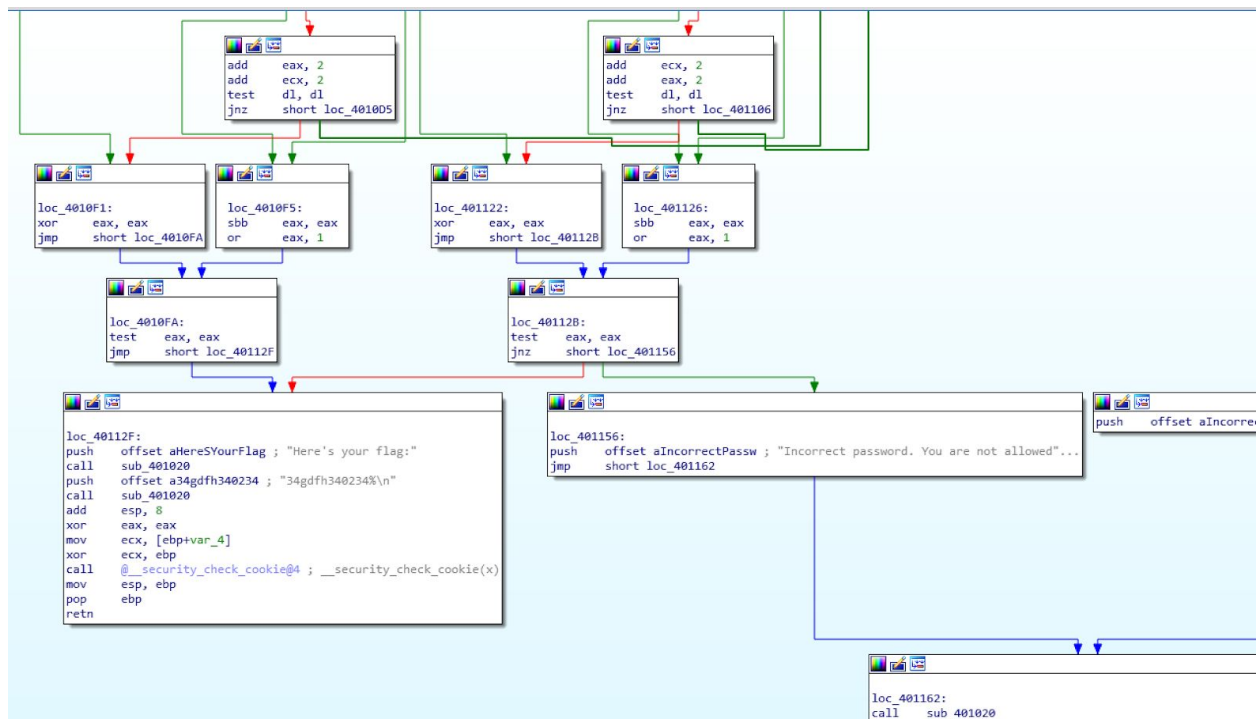


Project 2 Report

Part 1

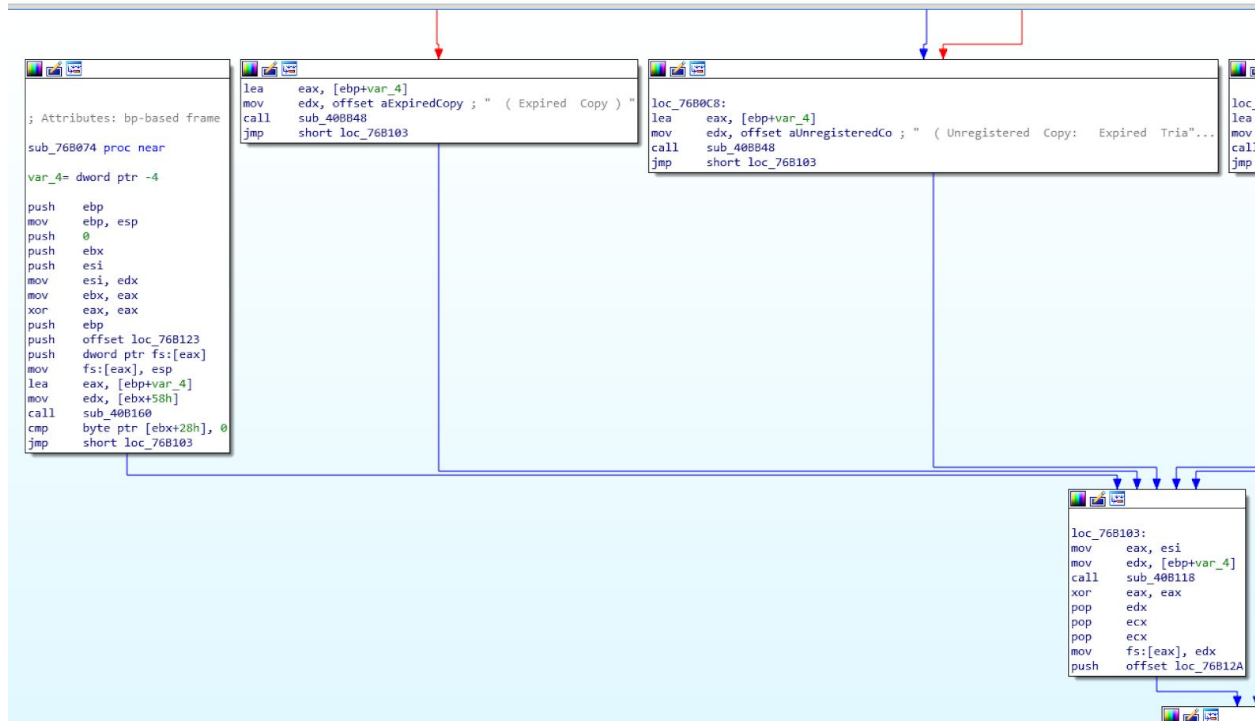
For part 1, the main objective was to print out the flag despite entering the incorrect credentials. By searching through the assembly searching for keywords, such as flag and password, we found the location that outputs the flag. We then use the graph overview to find the location that checks for credentials, loc_4010FA. There is a jump if zero call in 4010FA that points to outputting "Incorrect password...". This jz call was changed to a jmp and the location was changed to bypass the incorrect credentials to directly point to the flag at loc_40112F.



```
C:\Users\aaahun\Desktop\cs165project2>authenticate_yourself.exe
Please enter your username and password to be authenticated:
Username: asfi
Password: afsijiafs
Here's your flag:34gdfh340234
C:\Users\aaahun\Desktop\cs165project2>
```

Part 2

For part 2, it was pretty much the same process as part 1 to get rid of the banner. Scan through the code looking for keywords in the comments such as “unregistered copy” or “expired copy”. Use the graph overview to find where these locations are being called from. Change the `jmp` at the bottom of the subroutine to a `jmp` that points past the banner locations to `loc_76B103`.



WinEdt 9.0

