David Huang

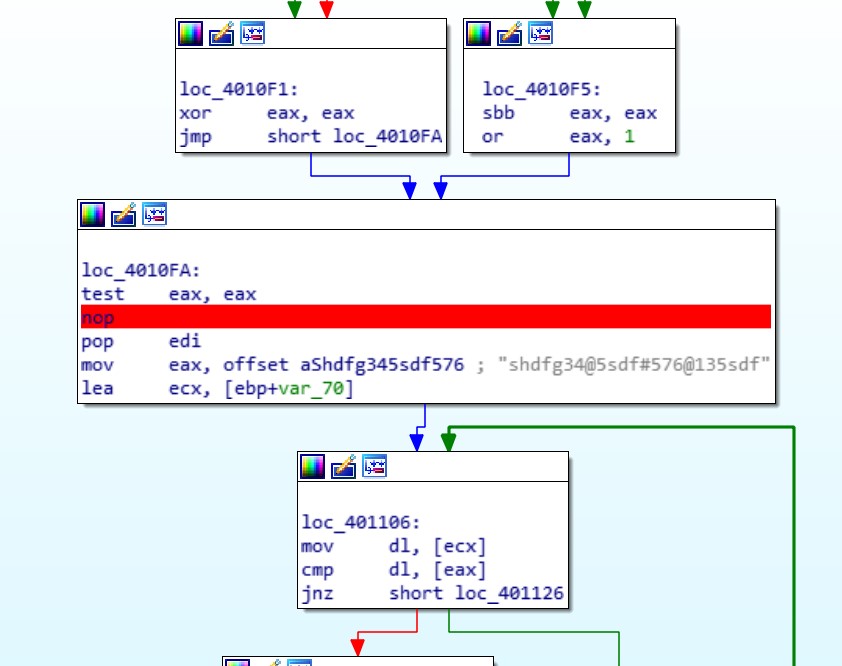
dhuan008@ucr.edu

**Part 1:**

Here's your flag:**34gdfh340234**

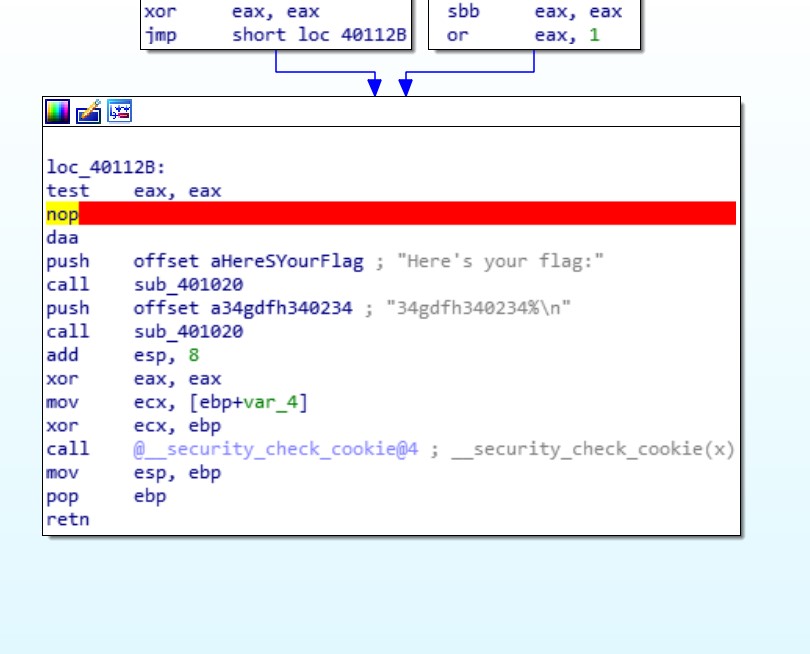
Changed the JNZ (opcode 75) to NOP (opcode 90). Highlighted in red. No instruction to goto incorrect username, so as long as there isn't a overflow or something we will always get the flag.. I did the same thing for password check.

|  |  |  |
| --- | --- | --- |
| Address | Original bytes | Patched bytes |
| 00000000004010FC | 75 | 90 |



Password - Same logic as above.

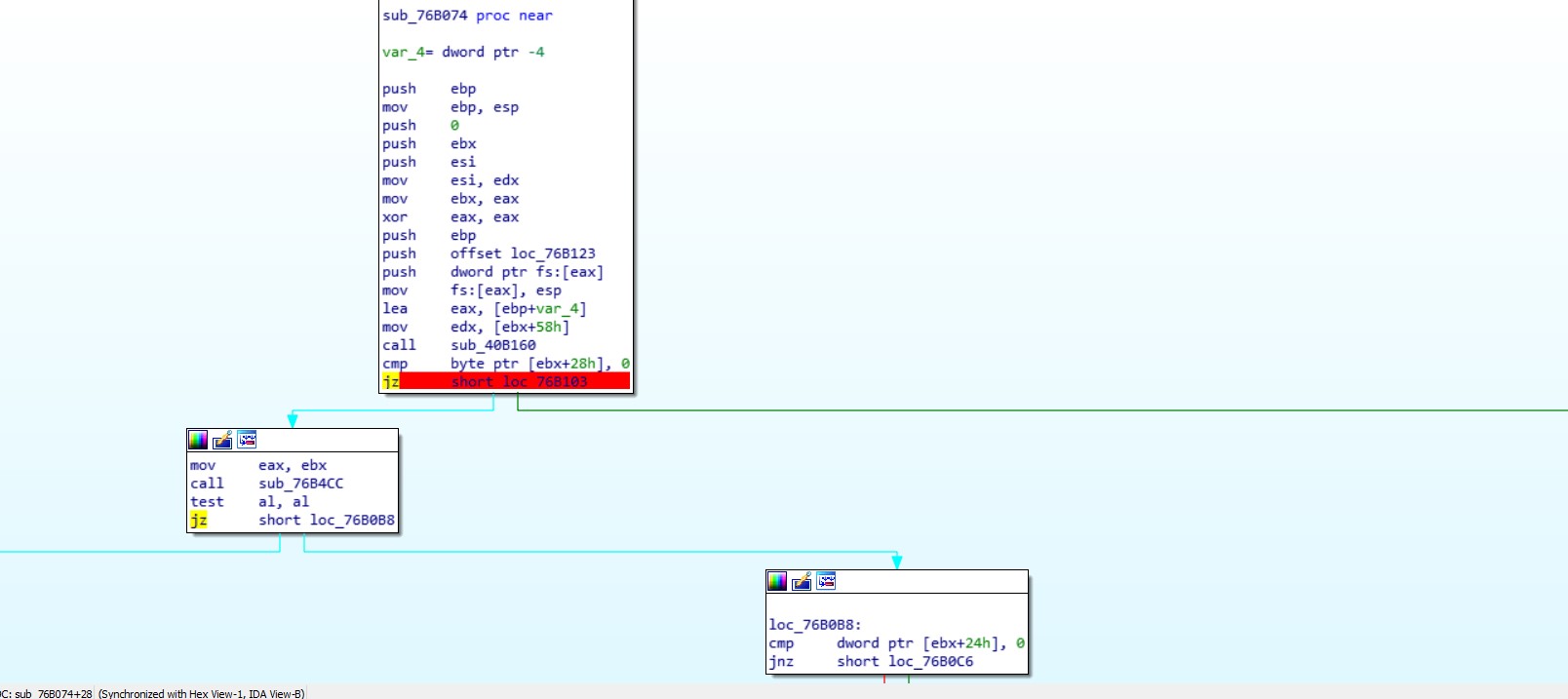
|  |  |  |
| --- | --- | --- |
| Address | Original bytes | Patched bytes |
| 000000000040112D | 75 | 90 |

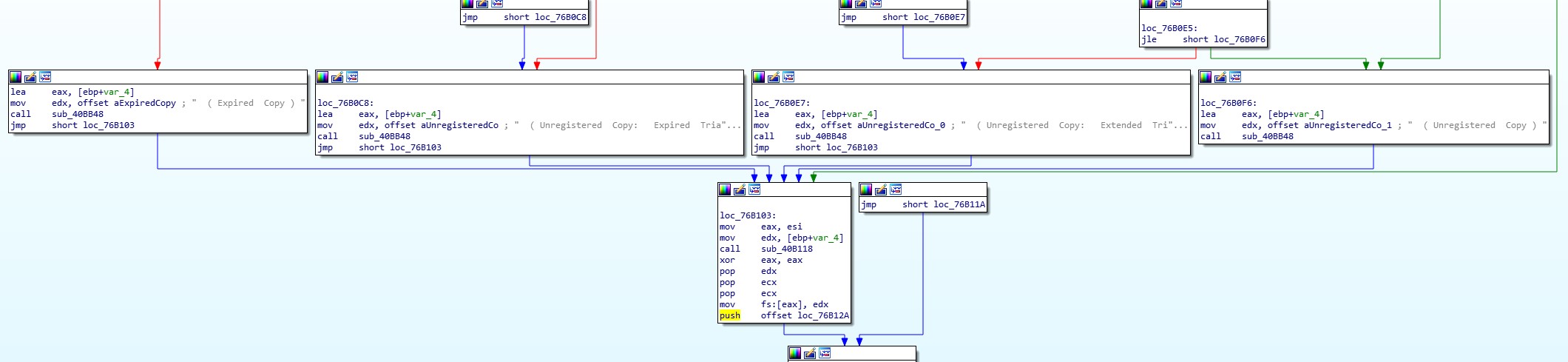


**Part 2.**

I was actually searching for the trial period is over string when i found the location of the banner modification code which contains all of the Unregistered copy and Expired copy modifications. So i changed the code to bypass all of them. Technically i did it by reversing the comparison so since its a unregistered copy it wont show as unregistered. Jnz to jz.

|  |  |  |
| --- | --- | --- |
| Address | Original bytes | Patched bytes |
| 000000000076B074 | 75 | 74 |





Afterwards I tried to remove the call to the trial popup but it seemed to always come back despite my changes, and the requirements stated that it was either the banner or the the reminder pop-up.