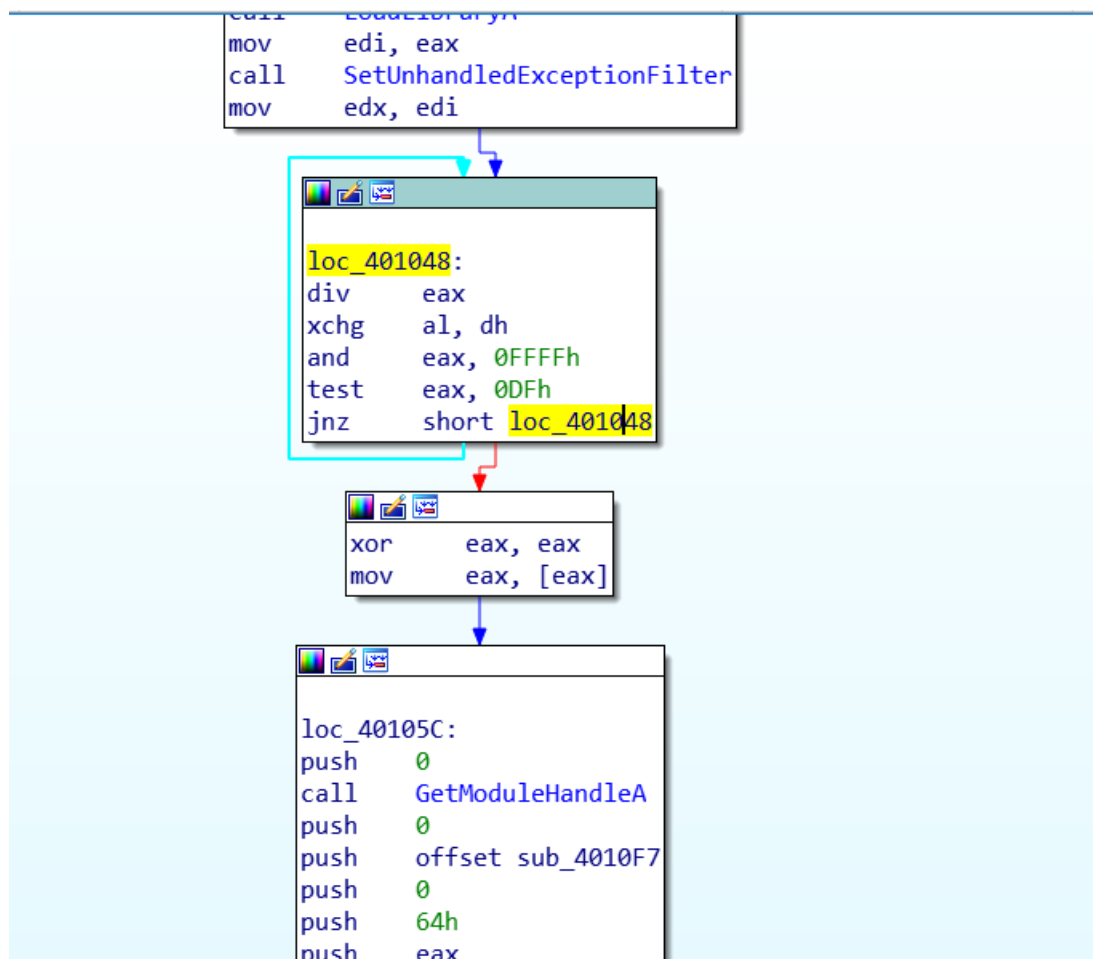


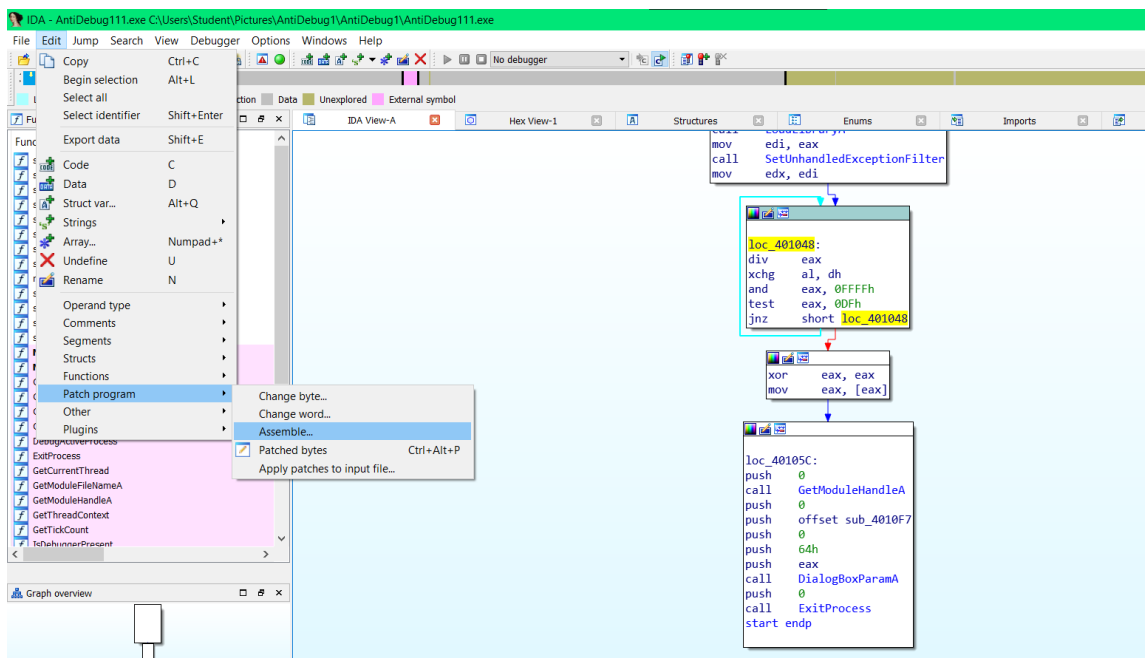
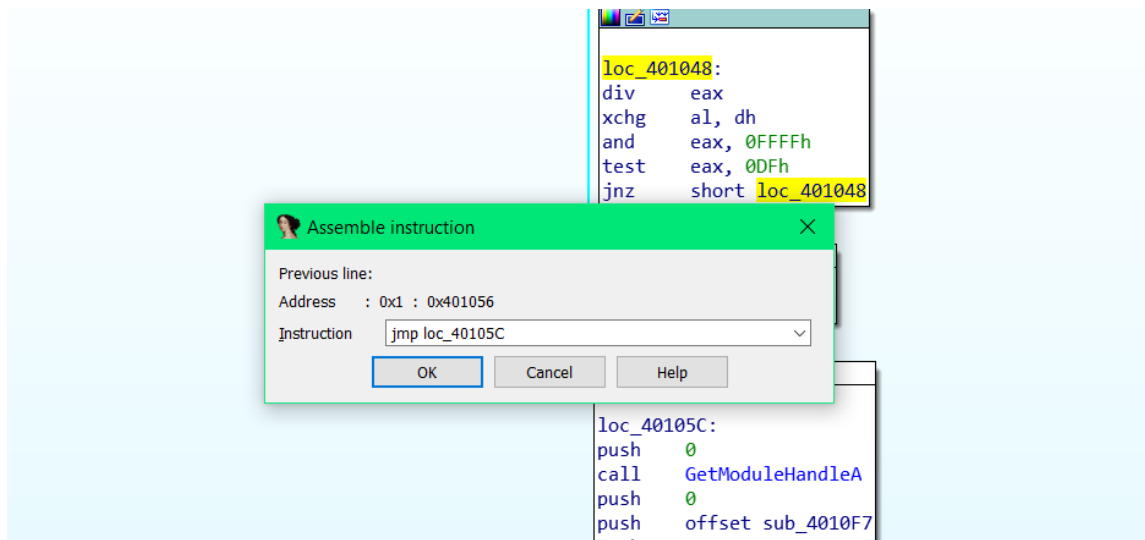
Lỗi 1: Trong hàm loc_401048 dưới hàm test thì phải nhảy đến được hàm loc_40105C, nhưng ở đây k nhảy đi được:v



Sửa:

tại dòng **jnz** **short loc_401048** sẽ sửa thành **jmp loc_40105C**

Vào Edit -> patch program -> assembly -> enter



Lỗi 2:

vào sub_4010F7

```
loc_40105C:  
push 0  
call GetModuleHandleA  
push 0  
push offset sub_4010F7  
push 0
```

sửa đoạn **jnz short loc_401256** thành **jmp loc_40122D**

```
call lstrlenA  
mov dword_40370C, eax  
mov dword_403714, 0  
push 0 ; ReturnLength  
push 4 ; ProcessInformationLength  
push offset dword_403714 ; ProcessInformation  
push 7 ; ProcessInformationClass  
push 0FFFFFFFh ; ProcessHandle  
call NtQueryInformationProcess  
test eax, eax  
jnz short loc_401256  
  
push dword_403720  
call SendDlgItemMessageA  
push 0  
push 0  
push 402h  
push 3EFh  
push dword_403720  
call SendDlgItemMessageA  
call sub_4014F3  
xor [eax], al  
; END OF FUNCTION CH
```

```
loc_40122D:  
lea esi, dword_4010A4  
mov al, 4Fh  
add al, byte ptr dword_403714  
mov ecx, 0Ah
```

5,1616) (387,117) 000005BD 004011BD: sub_4010F7+C6 (Synchronized with EIP)

Array... Numpad+*

✖ Undefined U

🏷️ Rename N

Operand type

Comments

Segments

Structs

Functions

Patch program

Other

Plugins

Change byte...

Change word...

Assemble...

Patched bytes Ctrl+Alt+P

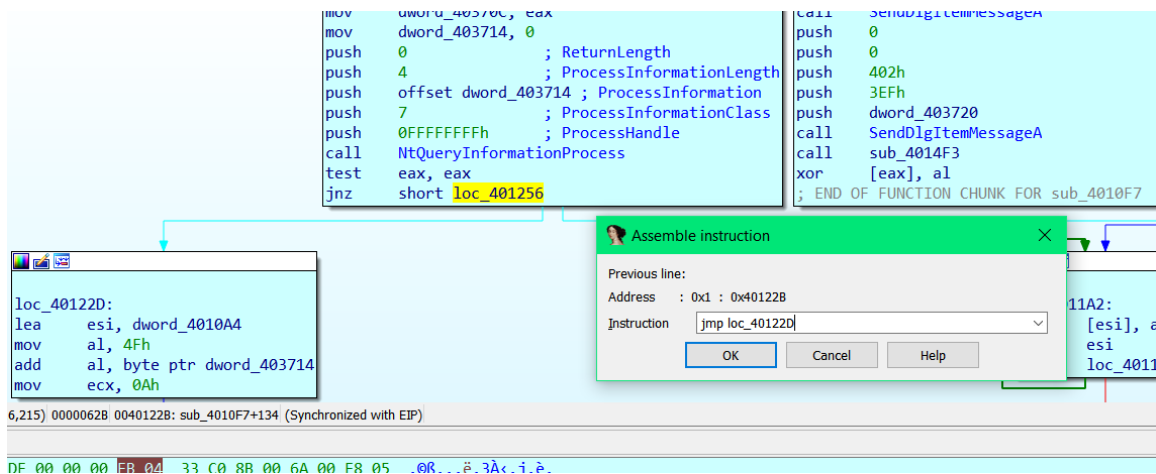
Apply patches to input file...

```
push offset dword_403714 ; ProcessInformation  
push 7 ; ProcessInformationClass  
push 0FFFFFFFh ; ProcessHandle  
call NtQueryInformationProcess  
test eax, eax  
jnz short loc_401256  
  
mov ecx, 0Ah
```

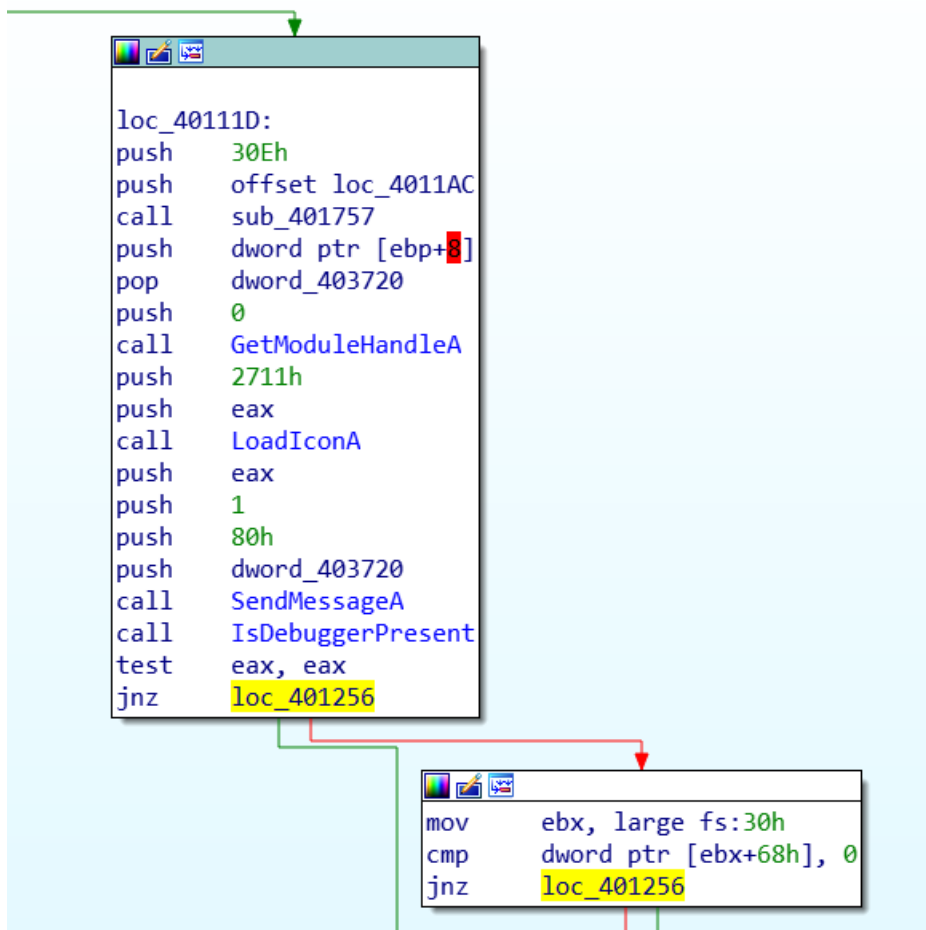
0.00% (-25,1616) (48,5) 0000062B 0040122B: sub_4010F7+C6 (Synchronized with EIP)

Hex View-1

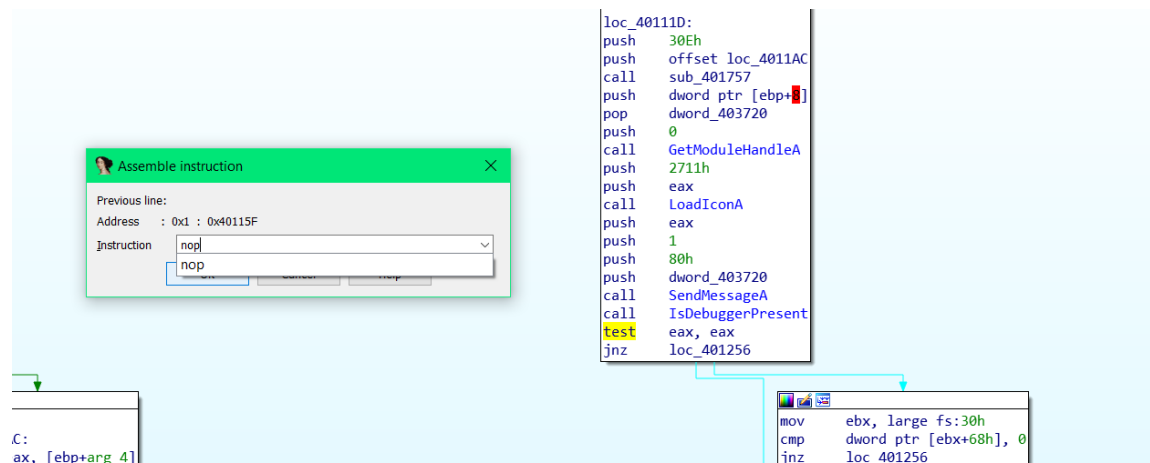
```
1401050 00 A9 DF 00 00 00 EB 04 33 C0 8B 00 6A 00 E8 05 .0B...ë.3Ä<.j.è.  
1401060 08 00 00 6A 00 68 F7 10 40 00 6A 00 6A 6A 50 F8 i h @ i idPa
```



Lỗi 3:



tại dòng cuối cùng hàm loc_40111D, nó nhảy luôn xuống loc_401256 là exit process nên ta sẽ nop lệnh này đi.



Sau khi sửa xong thì lưu thành file exe để chạy được như sau:

Edit->Patch program->Apply patches to input file

