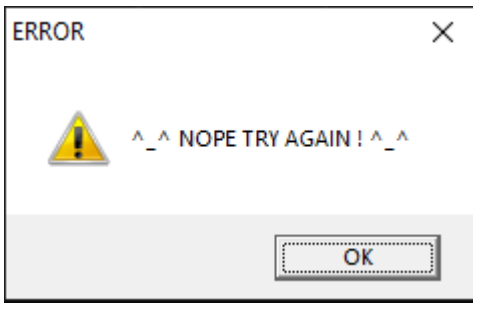
ESREV III WriteUp

Etudiant	Date	Sujet
34zY	13/02/2023	ESREV 3

Reconnaissance

Fichier executable windows :

Lancement du programme :

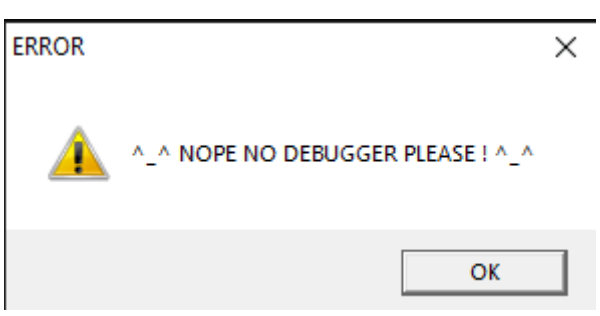


On obtient ce message d'erreur : "^_^ NOPE TRY AGAIN ! ^_^".

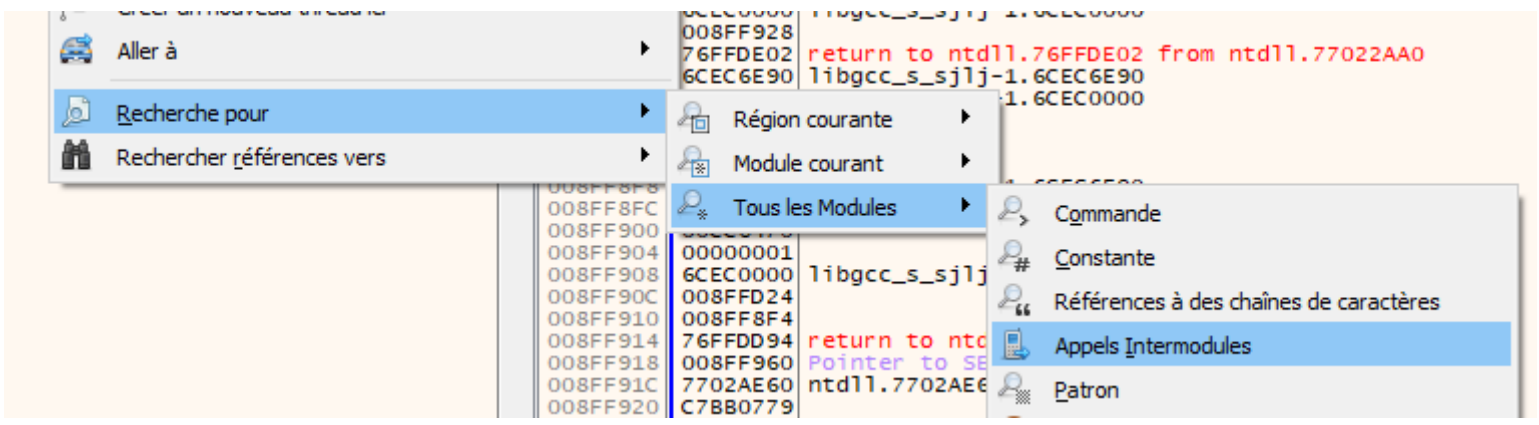
Exploitation

Désactiver le système Anti-Debug

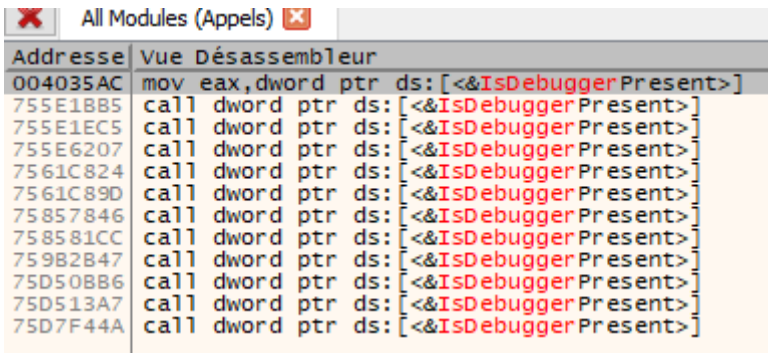
Le Debugging n'est pas autorisé sur le programme :



Chercher la protection anti-debug :

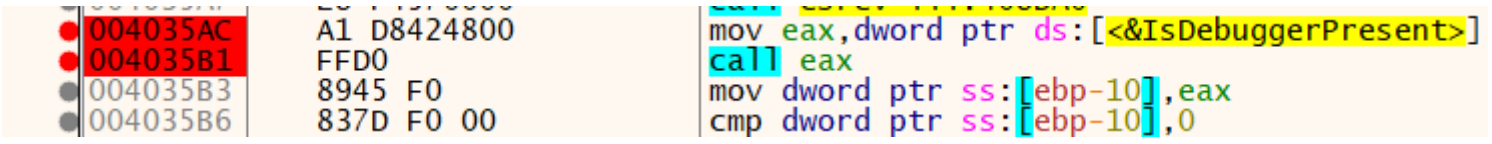


Taper "IsDebuggerPresent":



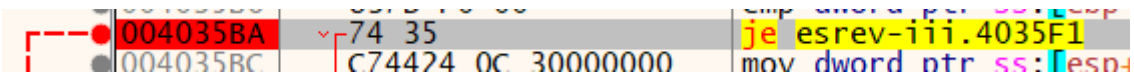
On obtient plusieurs instruction relié à cette appel à la librairie kernel32.

On repère l'instruction dans le désassembleur et on place des breakpoint dessus :

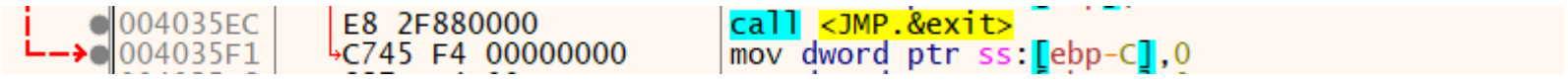


On voit que le registre eax est comparé à 0. Donc la sortie de la fonction IsDebuggerPresent est comparé à 0.

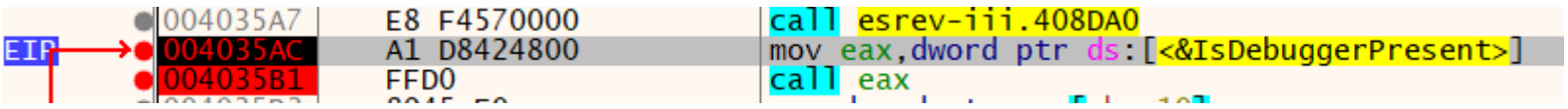
Si la sortie est égale à 0 on saute vers le début du programme :



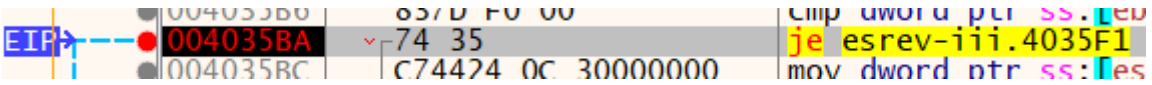
Sinon on se retrouvera à executer l'instruction call qui pointe sur l'adresse JMP.&exit qui correspond à la sortie du programme.



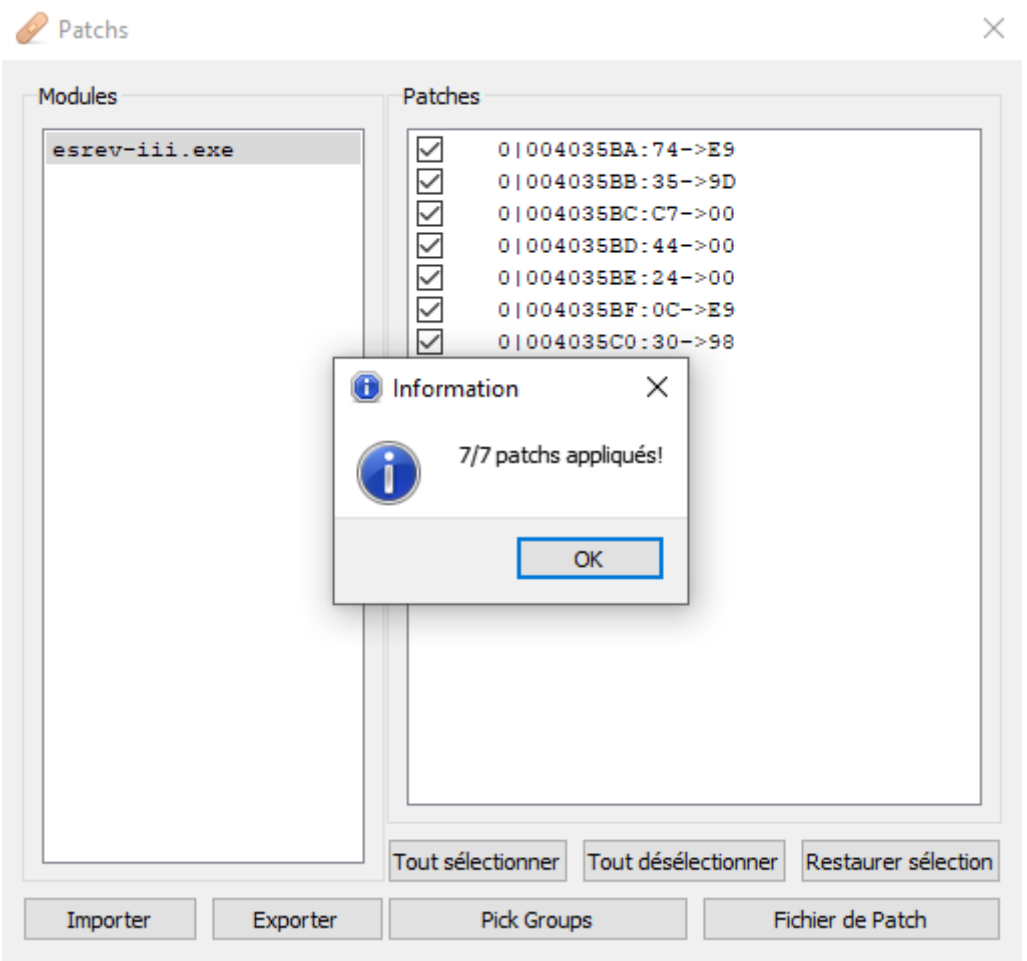
Dès que le programme démarre on fait avancer le programme jusqu'à que l'EIP pointe sur les breakpoints de l'Anti-Debug :



On voit que EAX est égale à 1 ici, donc on remplace ce EAX à 0 pour passer cette instruction JE :

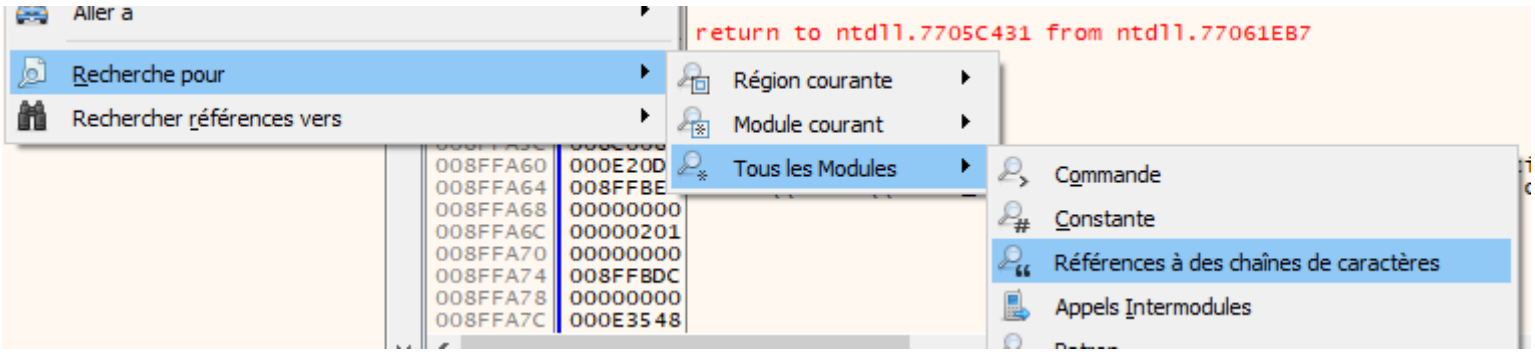


remplacer la comparaison avec une instruction JMP vers le début du programme en 0x0040365C, et générer un patch.

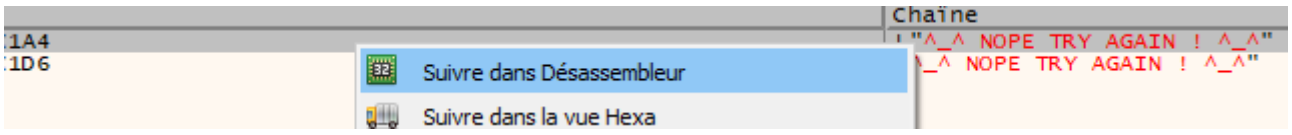


Extraction du flag

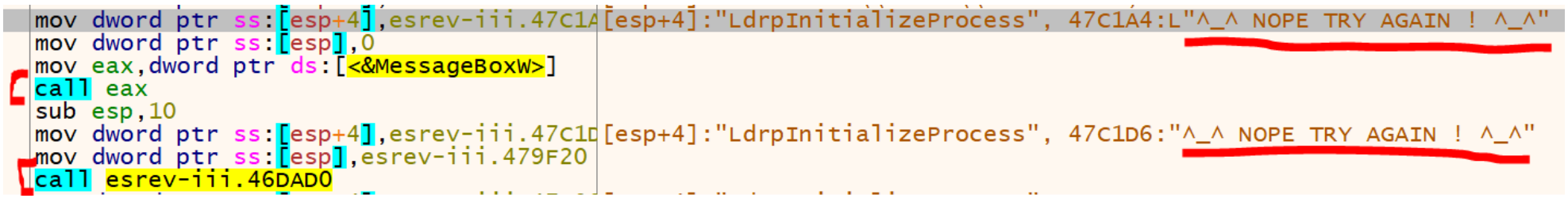
Ouvrir l'executable dans lequel on a patch l'anti-debugger dans un debugger et chercher pour ces lignes de charactères qui correspondes au message d'erreur :



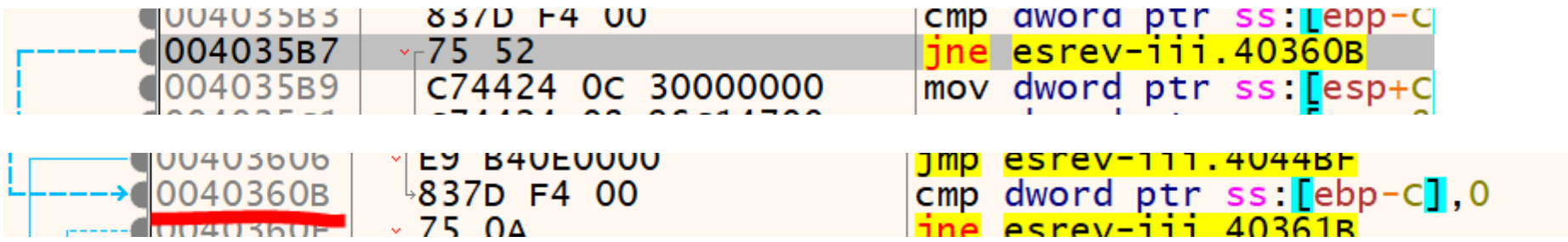
Suivre les résultats dans le désassembleur :



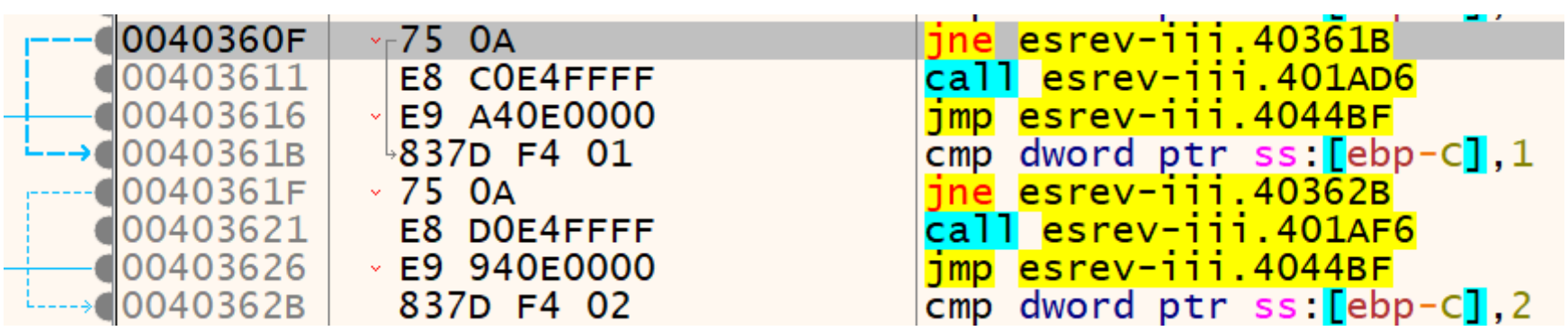
On peut voir les deux calls qui correspondent à l'affichage de message d'erreur dans la MessageBox Windows et le message d'erreur dans la sortie de la ligne de commande :



Avant les messages d'erreur nous avons une vérification avec JNE, si ce n'est pas égale donc on saute vers la fonction visée :

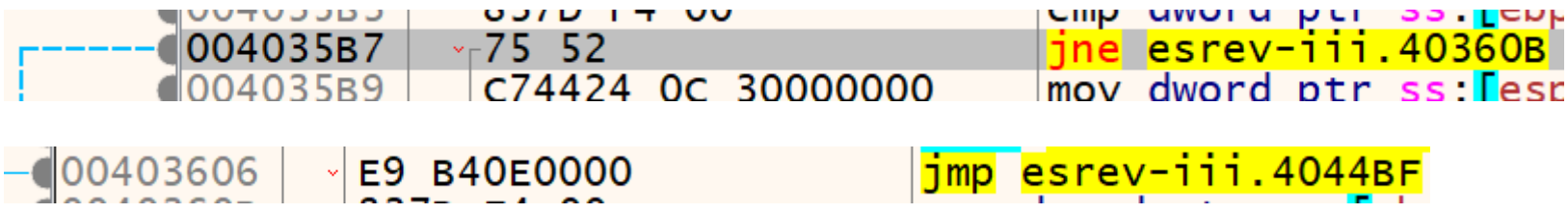


La fonction saute vers une comparaison et ainsi de suite :

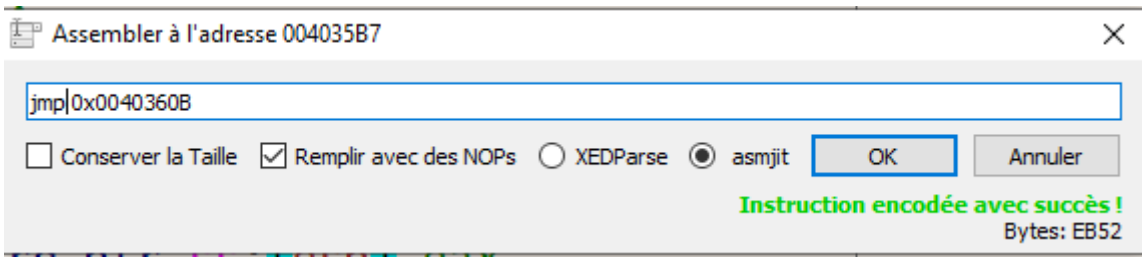


Si ce n'est pas égale on saute vers l'autre comparaison.

Donc cette instruction JNE doit être executé pour éviter les messages d'erreurs et ce JMP qui ramène vers la fin du programme :



On remplace JNE par un JMP comme ça le programme saute vers l'adresse où il y a la première comparaison dans tout les cas :



Le programme des centaines de comparaisons jusqu'à arriver à une instruction qui déplace des chaines de charactère vers l'esp :

```
004044C5    75 5D                jne esrev-iii-removed-debug.404524
mov dword ptr ss:[esp],esrev-iii-removed-debug.47C24 47C24D:"Not yet!"
call <JMP.&puts>
```

Si ce n'est pas égale l'instruction nous redirige vers une l'adresse qui print "Not yet!" et ensuite il ferme le programme.

On remplace cette instruction JNE par des nops :

```
004044C5    90                   nop
004044C6    90                   nop
```

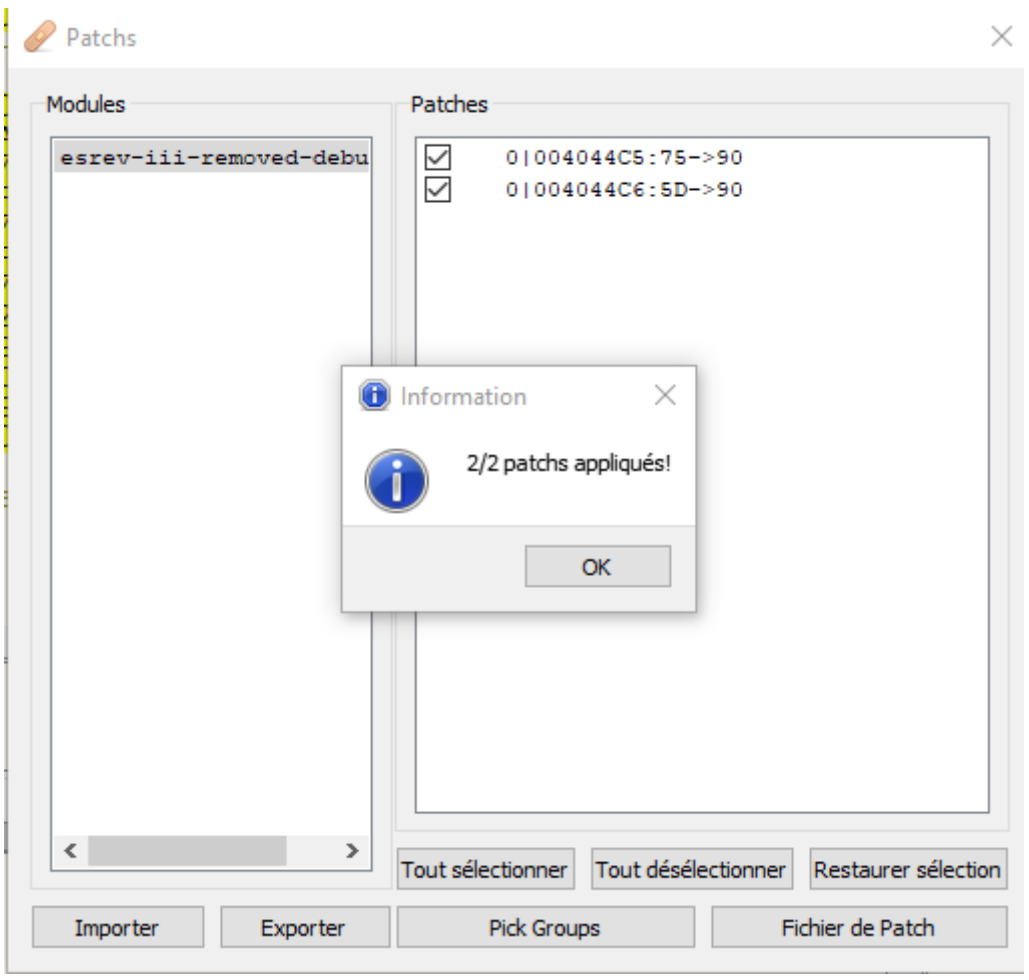
Pour passer l'eip vers l'adresse qui stock un "You" en chaine de charactère :

```
47C247:"Y o u"
```

Ensuite plusieurs instruction qui pointe vers des addresses de fonctions sont appelé sur une même ligné :

```
004044E6    E8 55960600          call esrev-iii-removed-debug.46DB40
004044EB    E8 9AD2FFFF          call esrev-iii-removed-debug.40178A
004044F0    E8 E2D2FFFF          call esrev-iii-removed-debug.4017D7
004044F5    E8 25D3FFFF          call esrev-iii-removed-debug.40181F
004044FA    E8 68D3FFFF          call esrev-iii-removed-debug.401867
004044FF    E8 ABD3FFFF          call esrev-iii-removed-debug.4018AF
00404504    E8 EED3FFFF          call esrev-iii-removed-debug.4018F7
00404509    E8 84D4FFFF          call esrev-iii-removed-debug.401992
0040450E    E8 CBD4FFFF          call esrev-iii-removed-debug.4019DE
00404513    E8 14D5FFFF          call esrev-iii-removed-debug.401A2C
00404518    E8 61D5FFFF          call esrev-iii-removed-debug.401A7E
0040451D    E8 0ED2FFFF          call esrev-iii-removed-debug.401730
```

On verra quelle est le resultat de l'execution de ces fonctions en patchant le fichier :



Crack / Flag

Lancer le programme cracké :

```
C:\                                                    >ESREV-III-removed-debug-cracked.exe
Y o u s a w _ m y f L 4 G 221
```

Flag : Yousaw_myfL4G221