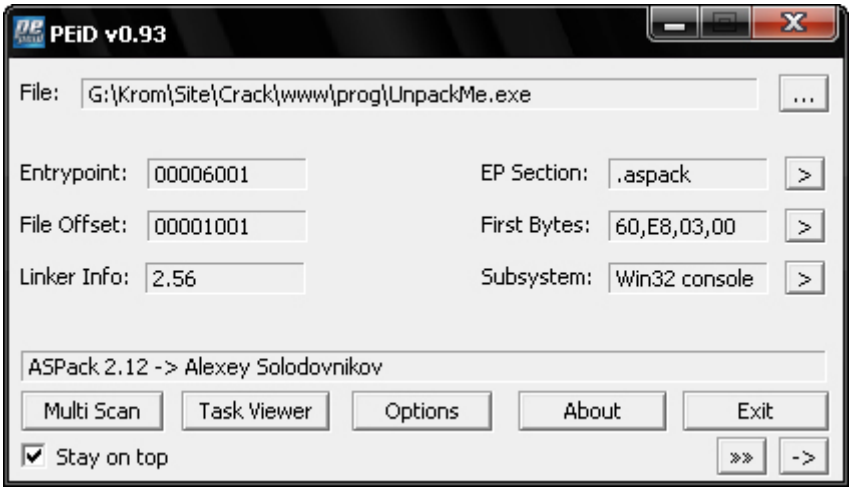
Cours N° 9

Dans ce cours, nous allons voir la protection ASPack 2.12 sur un UnpackMe, il est téléchargeable ICI

- **http://www.KromCrack.com/prog/UnpackMe.exe**

Je ne vais pas ici refaire la théorie sur le packer, mais juste vous expliquer comment Unpacker la protection ASPack 2.12
Un des premiers reflexes à avoir est de l'analyser avec PEiD, qui nous dit ceci :

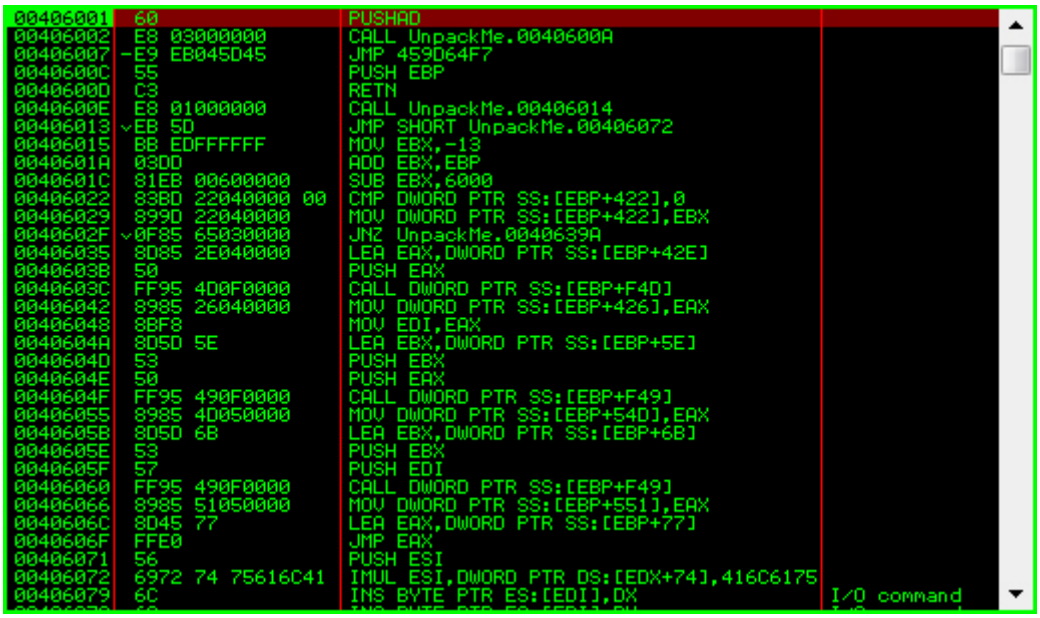


Quand on essaie de l'ouvrir avec OllyDBG, un message d'erreur apparaît nous disant que l'EP est placé en dehors du code.
Nous voyons aussi qu'il ne trouve aucune références dans :

- ->> Search for ->> All Referenced text strings.

Donc la même si vous ne l'aviez pas analysé avec PEiD, aucun doute qu'il est bien packé.

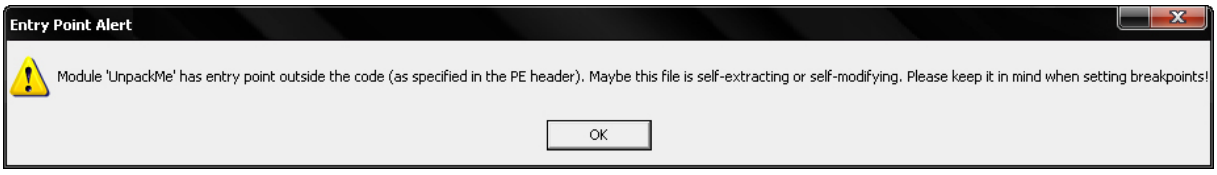
On voit aussi que le code Désassemblé est illisible et qui Commence par un PUSHAD.



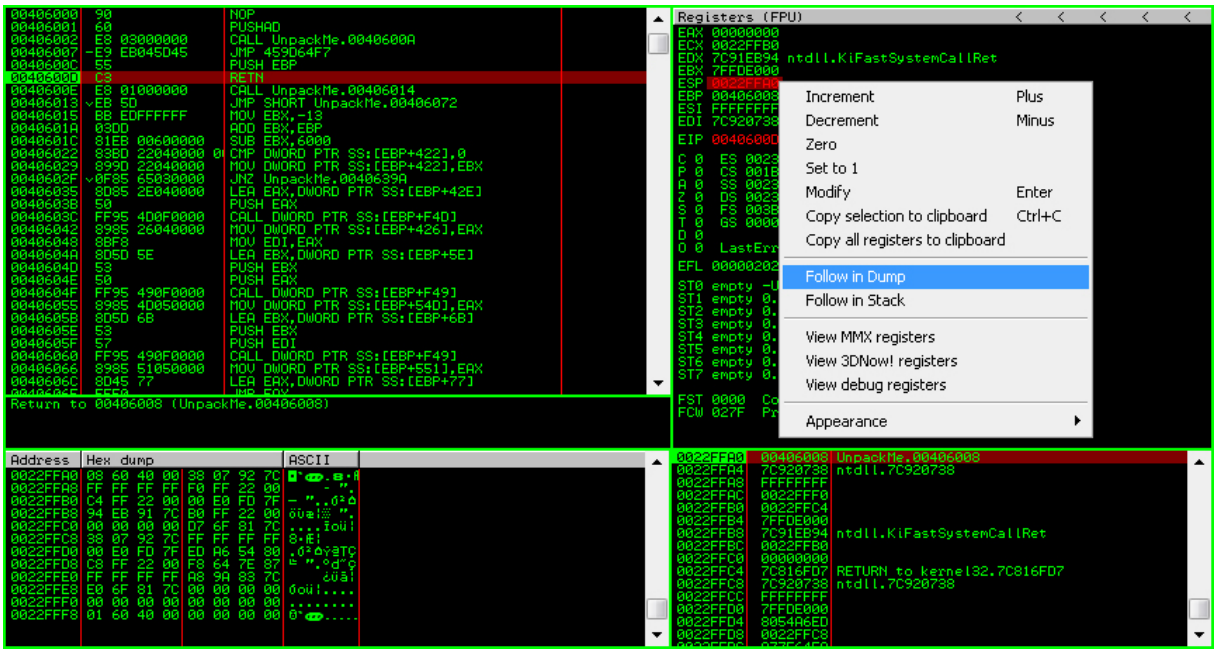
Quand il est ouvert dans OllyDBG le programme commence au PUSHAD en 00406001. Pourquoi j'ai mis 6001 en rouge ?
Parce que c'est l'actuel EP (Entry Point) et non l'OEP (Original Entry Point).

Alors commençons !

Quand vous l'ouvrer avec OllyDBG, un message d'erreur vient vous dire que l'EP se situe en dehors du Code. Cliquez sur "Ok" et continuons :



Vous commencez au PUSHAD à la ligne 00406001.
Faites une série de F7 (Et surtout pas F8) jusqu'à arriver au RETN en 0040600D (5x F7 en tout).
Arrivé là, faites un Clic droit sur le contenu du registre ESP, puis ->> Follow in Dump.

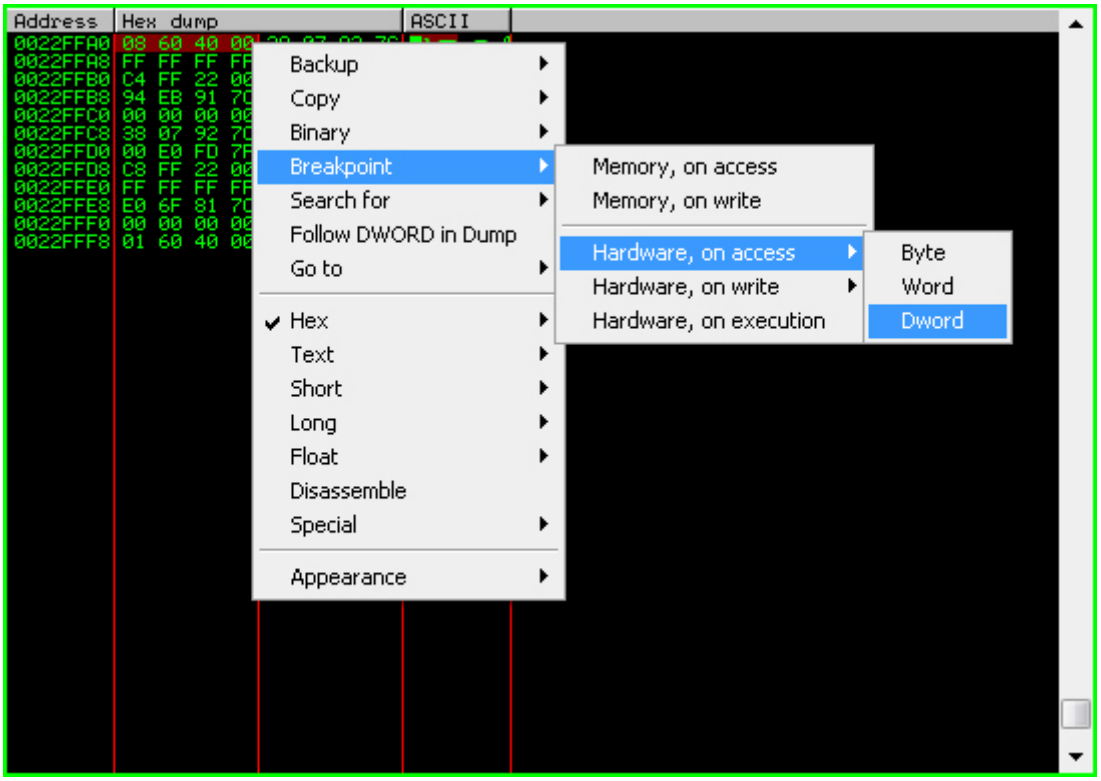


Arrivé dans le Dump à l'adresse 0022FFA0 (Contenu du registre ESP), sélectionnez les 4 premiers nombres Hexadécimaux, puis Clic droit ->> Breakpoint ->> Hardware, on Access ->> Dword.

Il faut sélectionner les 4 premiers car l'on veut savoir a quel moment le registre ESP va être consulté et comme c'est un registre de 32 Bits, il faut mettre un Breakpoint sur l'ensemble du registre.

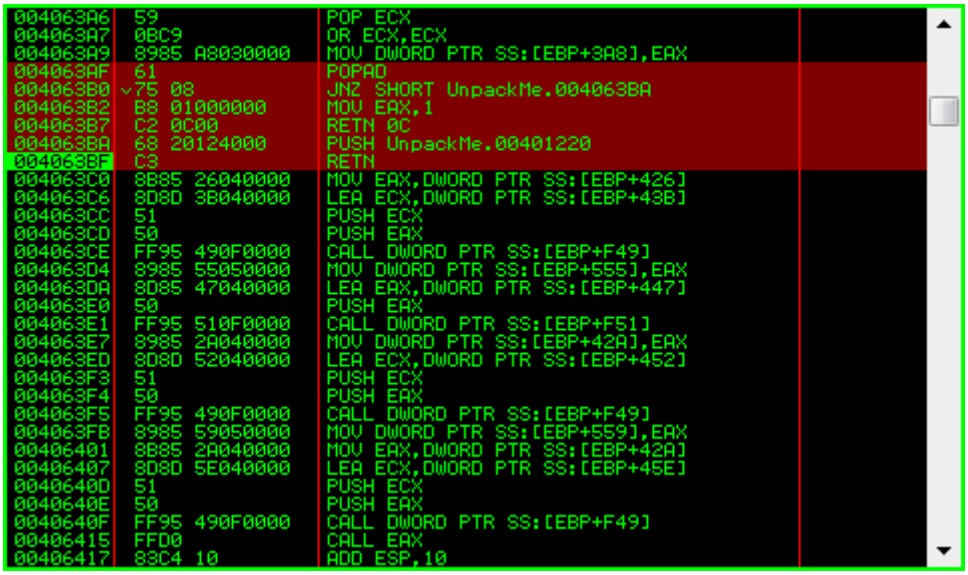
Petite parenthèse :

- Byte == 8 Bits
- Word == 16 Bits
- Dword == 32 Bits



Une fois le Breakpoint en place, lancez-le avec F9. Vous allez Breaker en 004063B0, une ligne après le POPAD.

Continuez F8 jusqu'à arriver au RETN à l'adresse 004063BF. Là on se trouve à la dernière ligne du Packer, faites un F8 de plus et vous arriverez en 00401220.

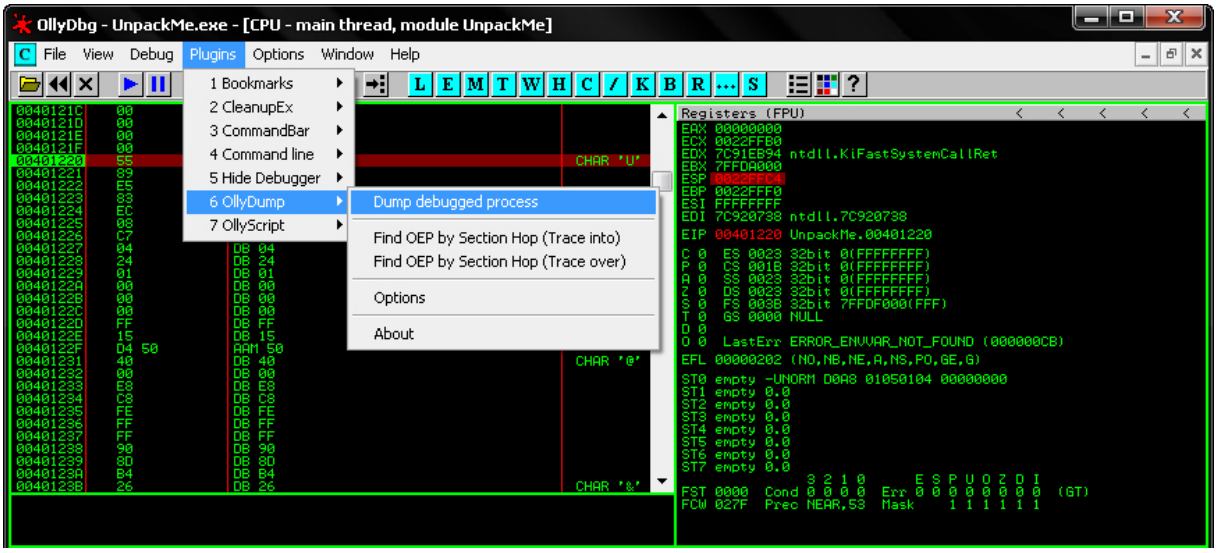


L'OEP se situe donc en 00401220. Maintenant cela change un peu par rapport au Cours N° 8. Pour faire le Dump on ne va se servir de ProcDump, Mais d'un Plugin d'OllyDBG appelé "OllyDump" téléchargeable ICI ou dans la rubrique "Download" :

- **http://www.KromCrack.com/prog/OllyDump.dll**

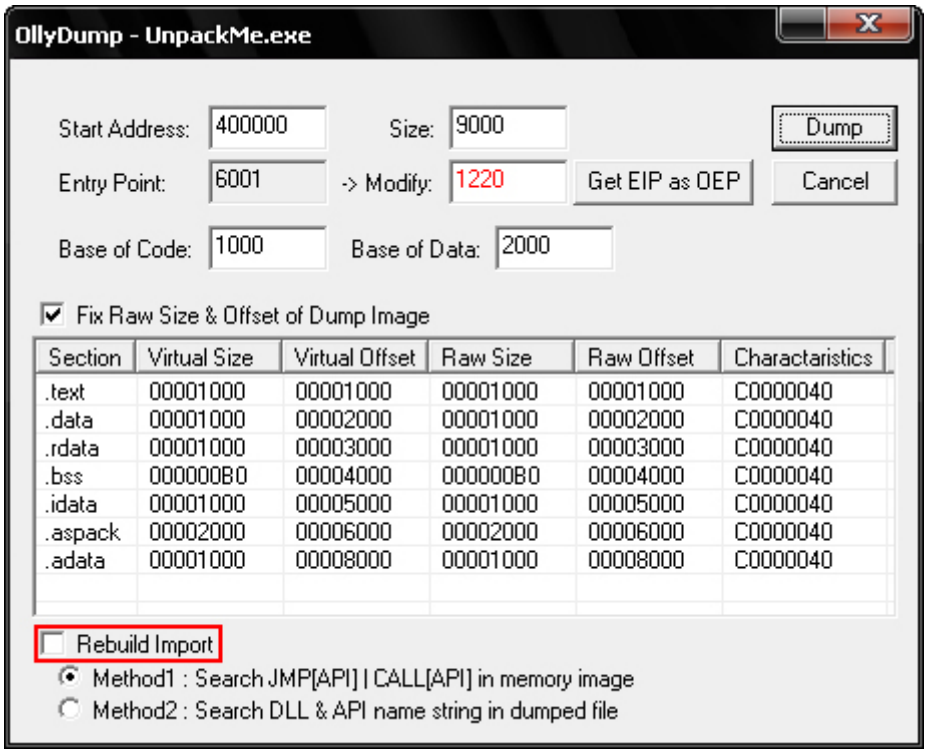
Pour l'installer, vous devez la placer dans le même répertoire qu'OllyDBG. une fois arrivé à la ligne 00401220 (qui est l'OEP) faites :

- Plugins ->> OllyDump ->> Dump debugged process.



Une nouvelle fenêtre s'ouvre et nous voyons l'EP : 6001 et l'OEP : 1220

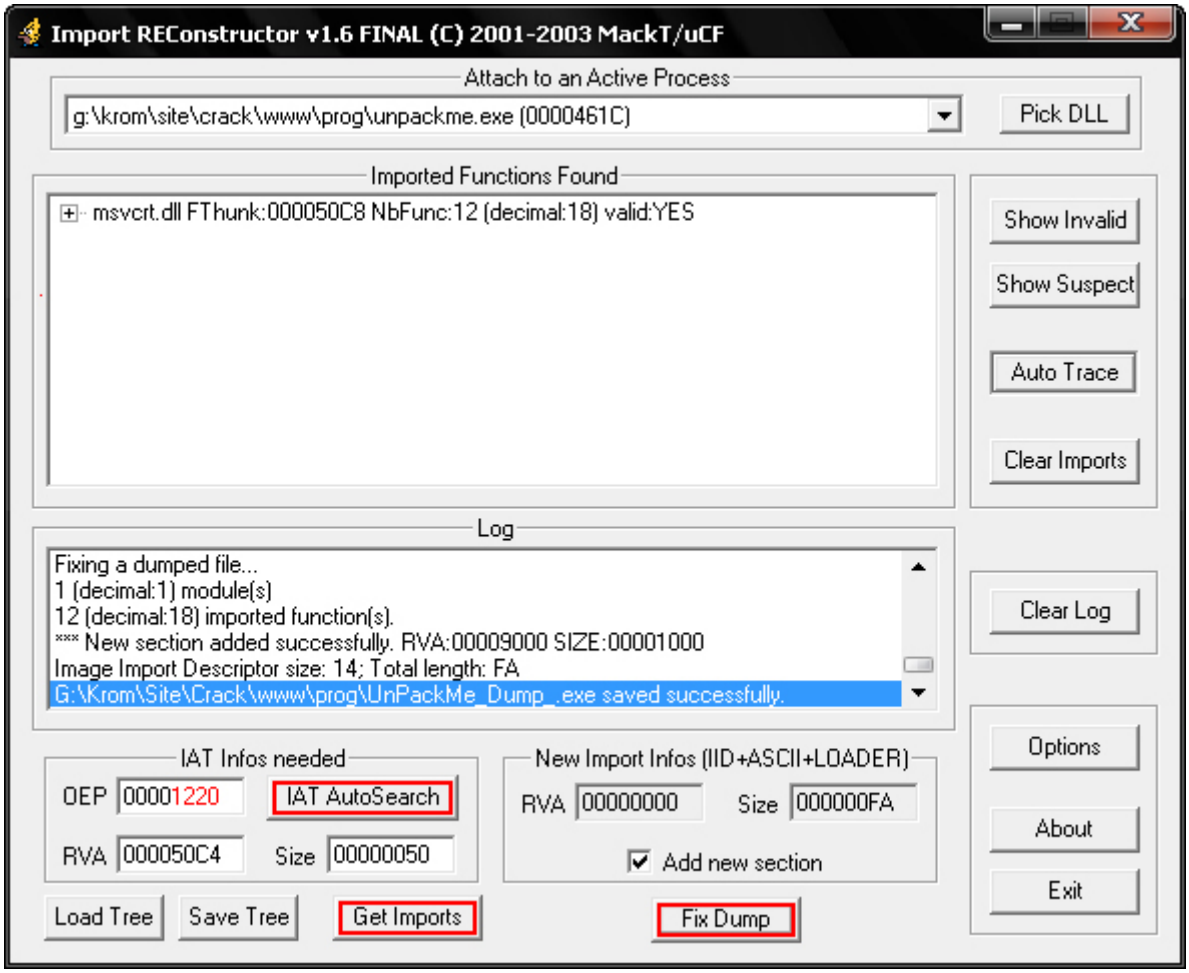
Décochez la case "Rebuild Import", puis Cliquez sur "Dump", et sauvez-le sous "UnpackMe_Dump.exe"



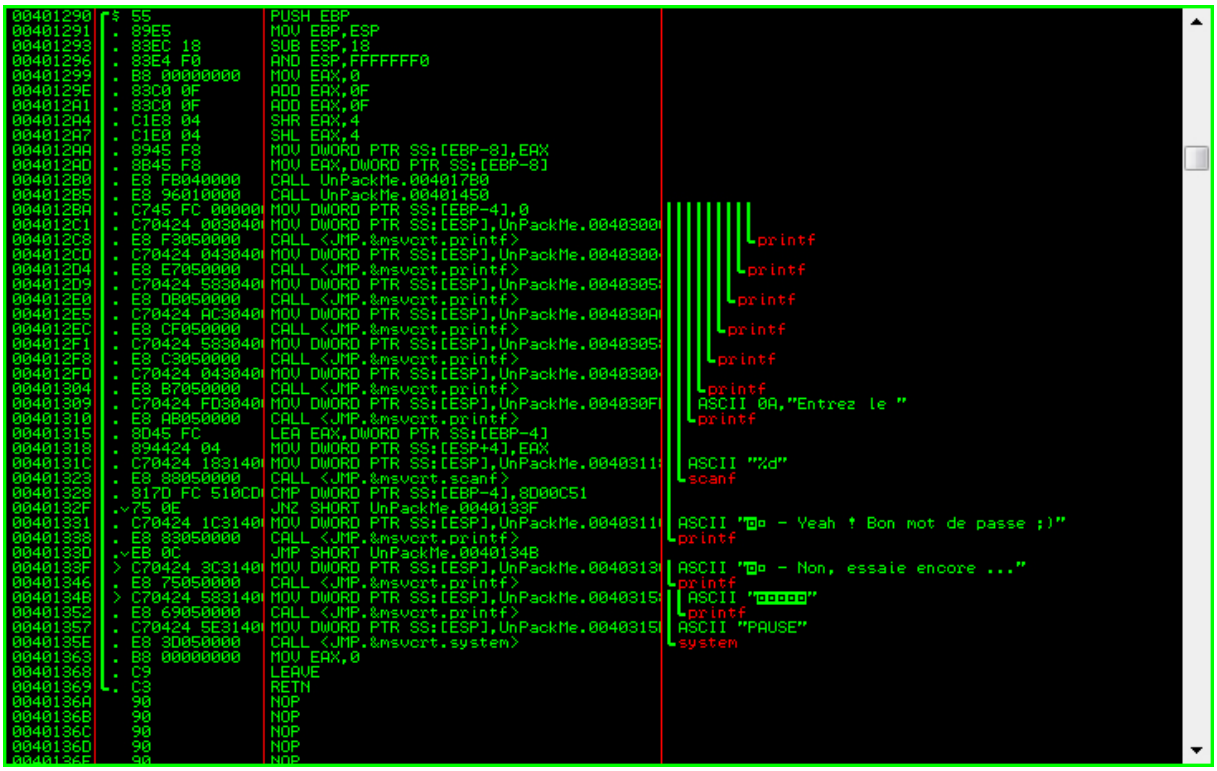
Si vous essayez de l'ouvrir, Windows va vous renvoyer une erreur 0xc0000005 car vous n'avez pas encore reconstituer l'IAT

On va donc la reconstituer avec ImportRec 1.6.

- Il faut lancer le programme Packé - UnpackMe.exe
- Ensuite sélectionnez-le dans "Attach to an Active Process"
- Modifiez l'OEP en y mettant 1220.
- Cliquez sur "IAT AutoSearch"
- Cliquez ensuite sur "GetImports"
- Puis "Fix Dump" et sélectionnez notre fichier Dumper "UnpackMe_Dump.exe"
- Le fichier Unpacker est enregistré sous "UnpackMe_Dump_.exe"



Et une fois l'UnpackMe Unpacké, vous voyez maintenant un code beaucoup plus clair et plus lisible ;)



J'espère que ce cours a été clair ;)

Si vous avez rencontré une erreur ou que quelque chose ne marche pas, vous pouvez m'envoyer un mail à **Admin@KromCrack.com** ou en parler sur le forum :

- **http://www.KromCrack.com/forum/**