- Thxer.com -

Les Articles |\|on-Geek By Thxer

For Commu N-PN

IDA L'usine a Gaz

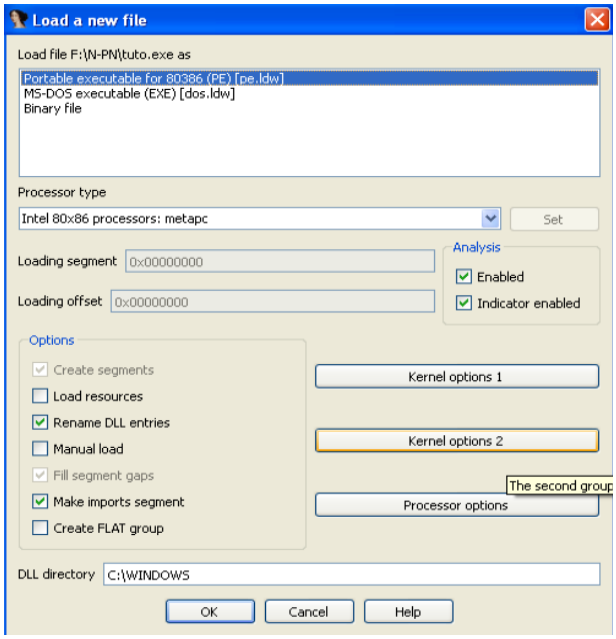
Intro

Il est 1:00 du mat', et suite à une suggestion de petit « tuto » sur ida je me tords dans mon lit, pleins d'idées ... ou plutôt ce tuto me prends la tête alors je m'y attelle.

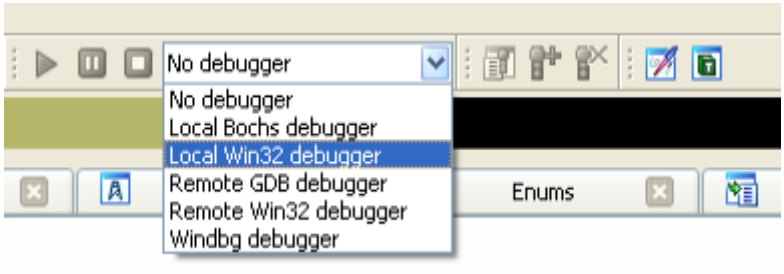
Alors IDA, certains disent « C'est une usine à gaz », et ben ... oui carrément, personnellement je pense que c'est la hotte du père noël !
Je vous propose donc une petite visite guidée. (nocturne :( )

Mettre en place le debugger

IDA c'est bien mais lorsqu'on ouvre notre premier PE, on ne peut pas le debug dessuite. Il faut choisir le bon debugger.



Ici On desass le .exe



Comme c'est un PE on choisit « Local Win32 debugger »

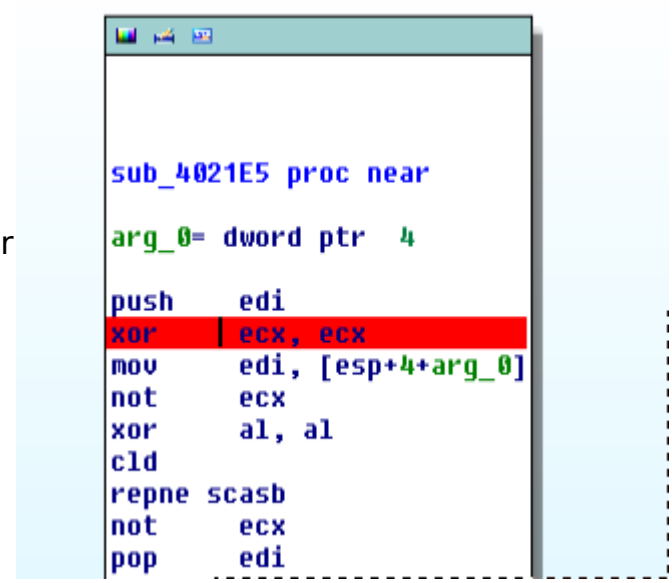
Yeah ! C'est vert on peut Debug !!!

Oui mais on peut aussi poser des Breakpoints (bp) car avant c'était pas possible.
Du coup pour poser un bp = F2.

La suite c'est comme pour OLLY :

F9 = Run , F8=Fonction suivante, F7= Pas à Pas (ça donne des crampes)

Là =>
J'ai posé un super bp au pif sur un xor

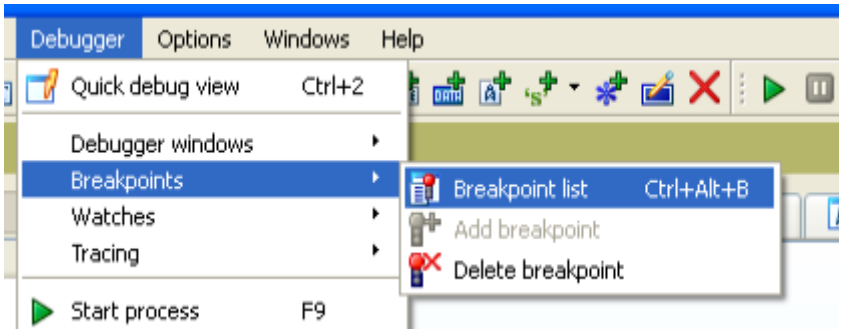


Bref quand c'est rouge y'a un bp.
(F2 pour enlever)

Vous voulez lister les Bp ?

Voilà

=>

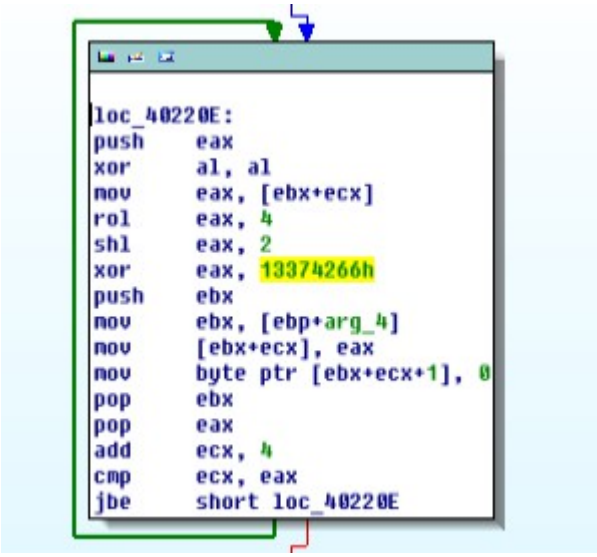


Bon okey, jusque là ça reste ... basique

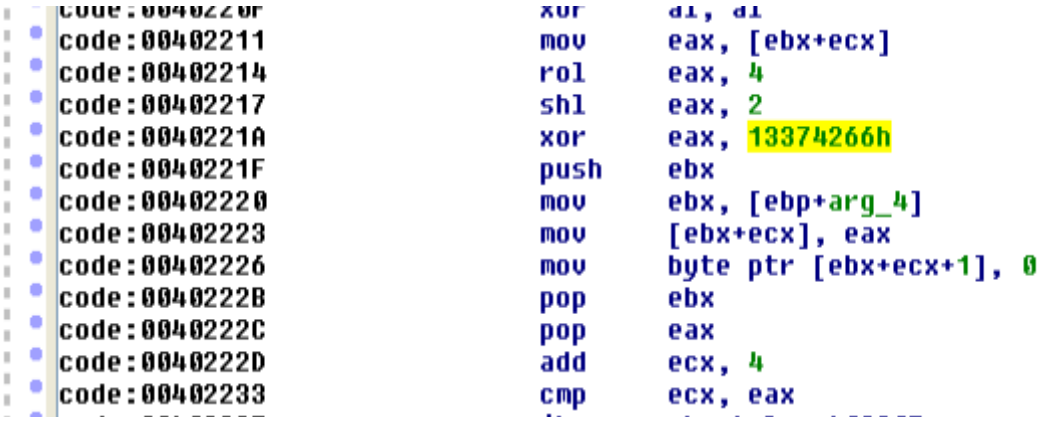
La Graph View !

C'est une des nombreuses qualités d'ida, le mode « graph »
En général vous êtes sur cette vue de base.
Mais le Hic c'est que quand vous voulez vous balader dans le code bah ... vous savez plus comment revenir le (-) de OLLY ne marche pas.
Il suffit d'utiliser la touche « espace » pour basculer entre les vues.

Vue « Graph »



Vue « Inside »



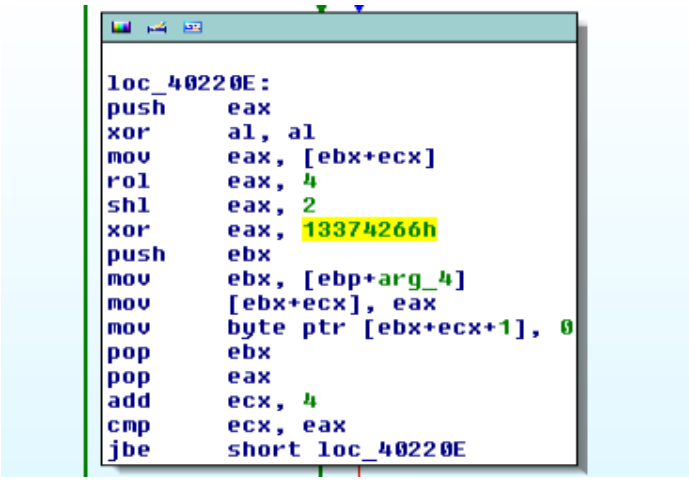
Pour rentrer dans un call il suffit de cliquer deux fois dessus.

On commence à toucher des choses cool non ?

Le Pseudo-Code

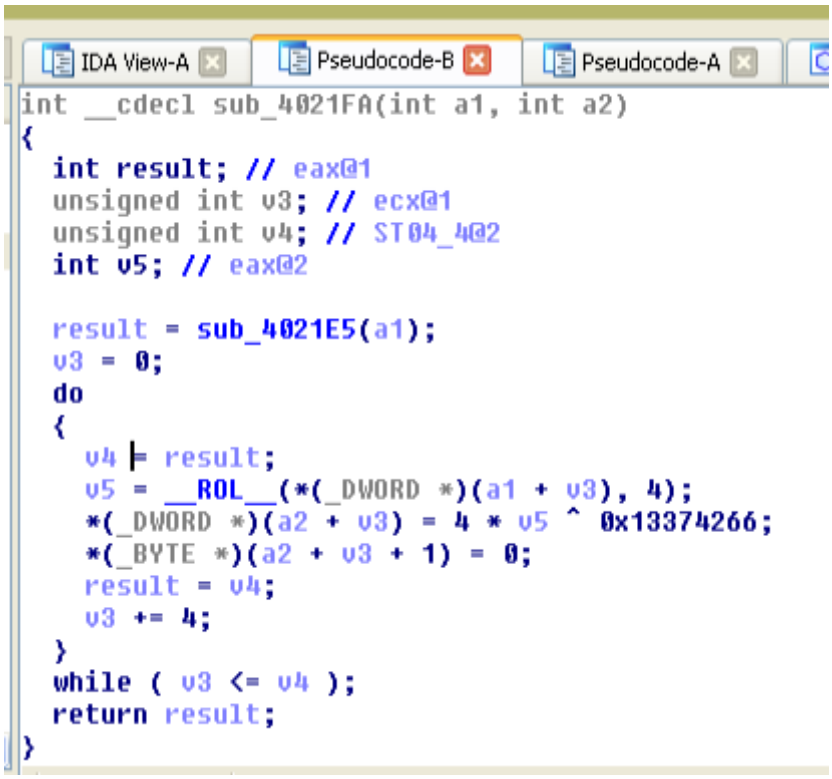
Parfois on se mélange un peu dans l'asm, et un pseudo code-c nous aidera à comprendre la mécanique interne, du coup IDA le fait pour nous.

Allez dans votre fonction.



```
loc_40220E:
push    eax
xor     al, al
mov     eax, [ebx+ecx]
rol     eax, 4
shl     eax, 2
xor     eax, 13374266h
push    ebx
mov     ebx, [ebp+arg_4]
mov     [ebx+ecx], eax
mov     byte ptr [ebx+ecx+1], 0
pop     ebx
pop     eax
add     ecx, 4
cmp     ecx, eax
jbe     short loc_40220E
```

Puis faire F5 :



IDA View-A | Pseudocode-B | Pseudocode-A

```
int __cdecl sub_4021FA(int a1, int a2)
{
  int result; // eax@1
  unsigned int v3; // ecx@1
  unsigned int v4; // ST04_4@2
  int v5; // eax@2

  result = sub_4021E5(a1);
  v3 = 0;
  do
  {
    v4 = result;
    v5 = __ROL__(*(_DWORD *)(a1 + v3), 4);
    *(_DWORD *)(a2 + v3) = 4 * v5 ^ 0x13374266;
    *(_BYTE *)(a2 + v3 + 1) = 0;
    result = v4;
    v3 += 4;
  }
  while ( v3 <= v4 );
  return result;
}
```

Magique non ? Pour revenir ? => Cliquez sur IDA View-A

Je sais pas vous ... mais perso je ne veux pas m'arrêter là.

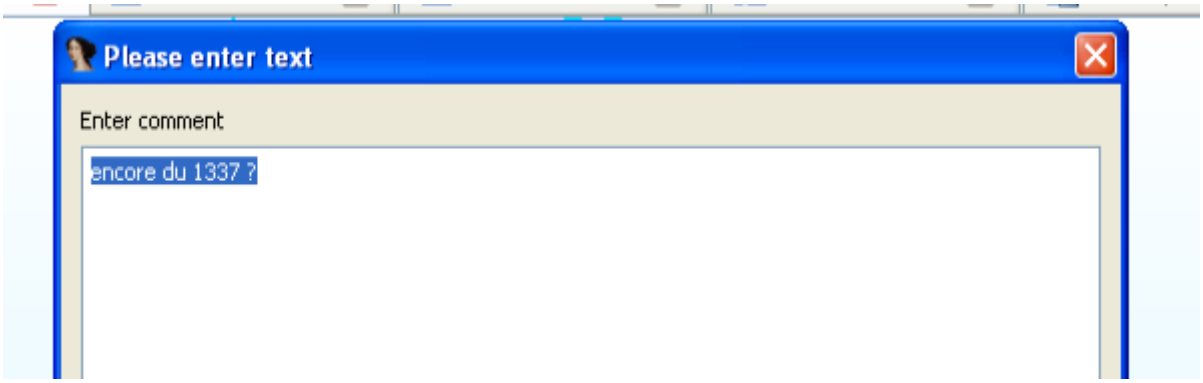
Le Renommage Ou Façonner son code !

Quand on dessas prendre des notes c'est bien, mais commenter et s'approprier le code c'est encore mieux !
IDA propose de pouvoir tout renommer, les variables, les fonctions etc ... mais elle permet aussi de commenter le code !

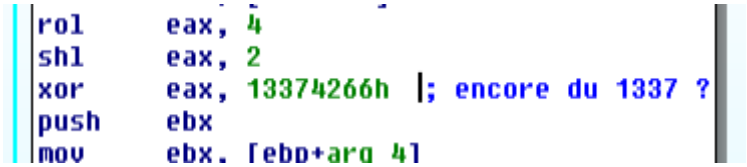
Let's run !

Commenter le code

Les commentaire en asm c'est « : », du coup taper « : » sur votre ligne, une fenêtre s'ouvre commentez !



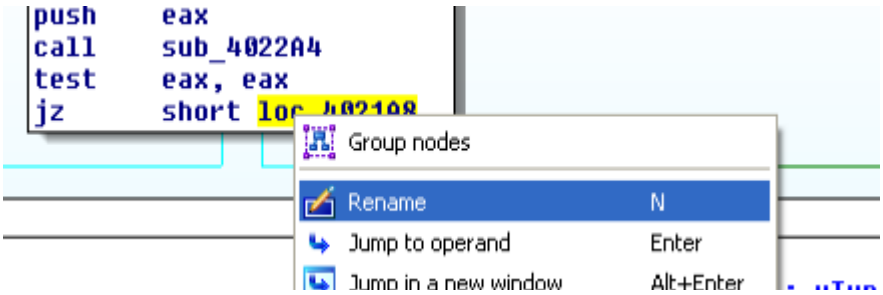
Donne =>

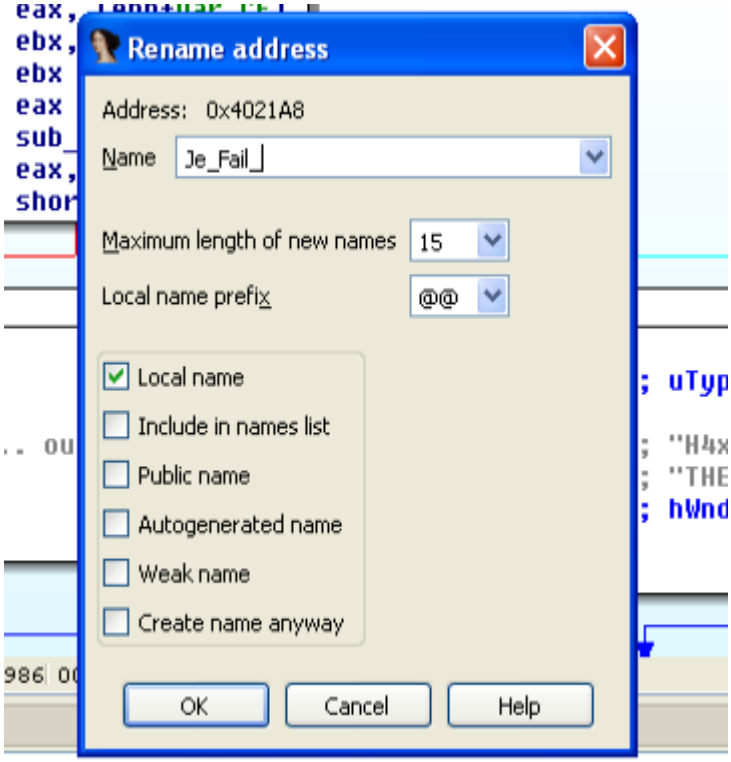


Renommer le reste

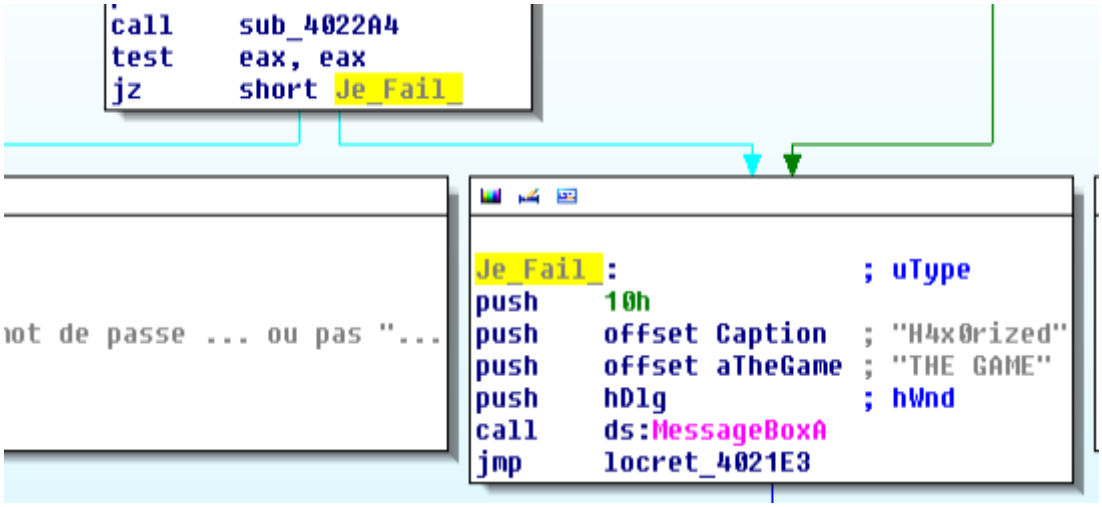
Vous venez de trouver ce que fait une fonction ou autre ? Oubliez le papier IDA est là !

Clic droit =>



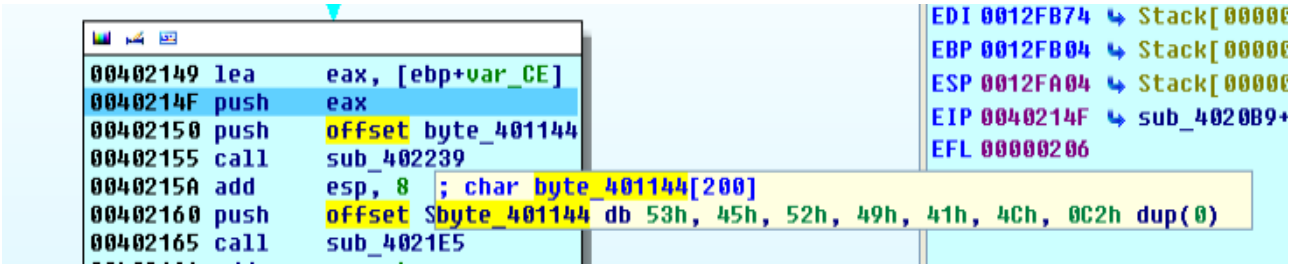


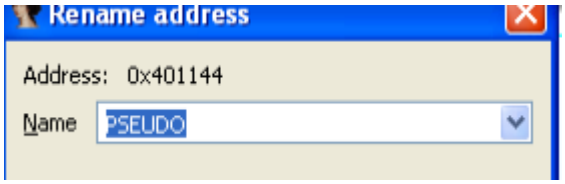
Donne :

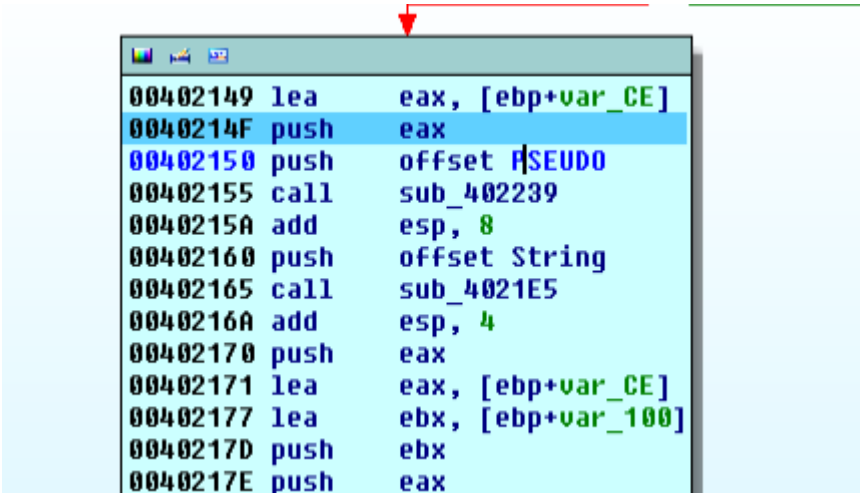


<u>Autre exemple :</u>

Ici je sais qu'a cet offset j'ai le PSEUDO autant le dire non ?

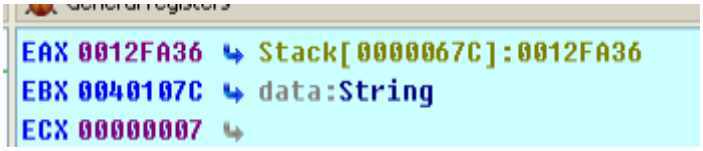




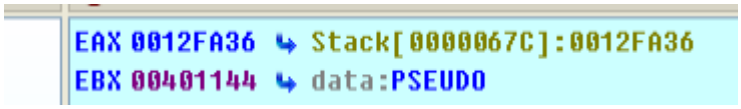


Pas mal non ?
Ce qui donne dans les registres :

Avant



Après

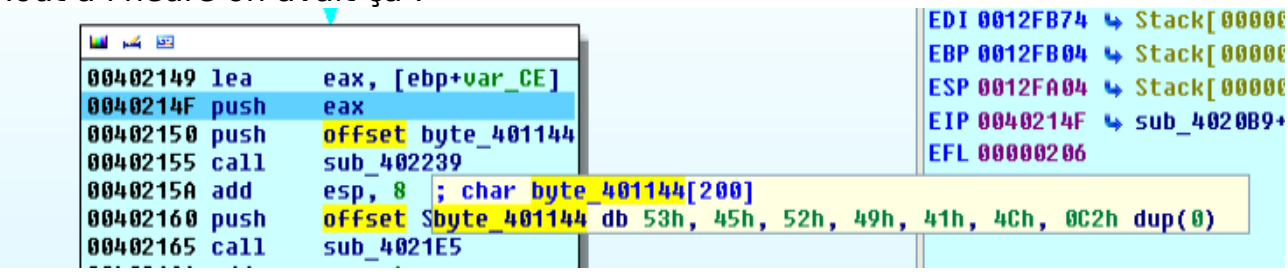


Héhé ! Je vous laisse imaginer la suite ...

Encore plus ? Ok .. je vous livre mes découvertes :) .

Afficher les Strings

Tout à l'heure on avait ça :



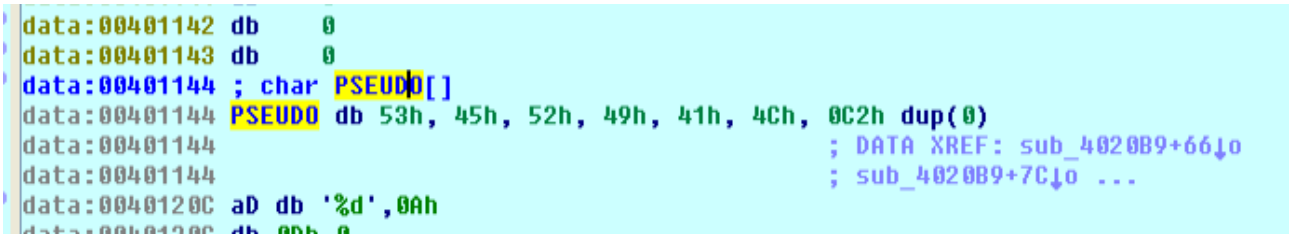
On ne parle pas tous (encore) l'hexa couramment.

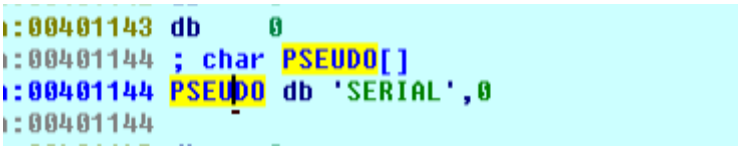
```
echo -e "\x53\x45\x52\x49\x41\x4c"
SERIAL
```

Donc on voit bien qu'en allant vite tout à l'heure j'ai renommer l'offset du serial en pseudo … passons : p .

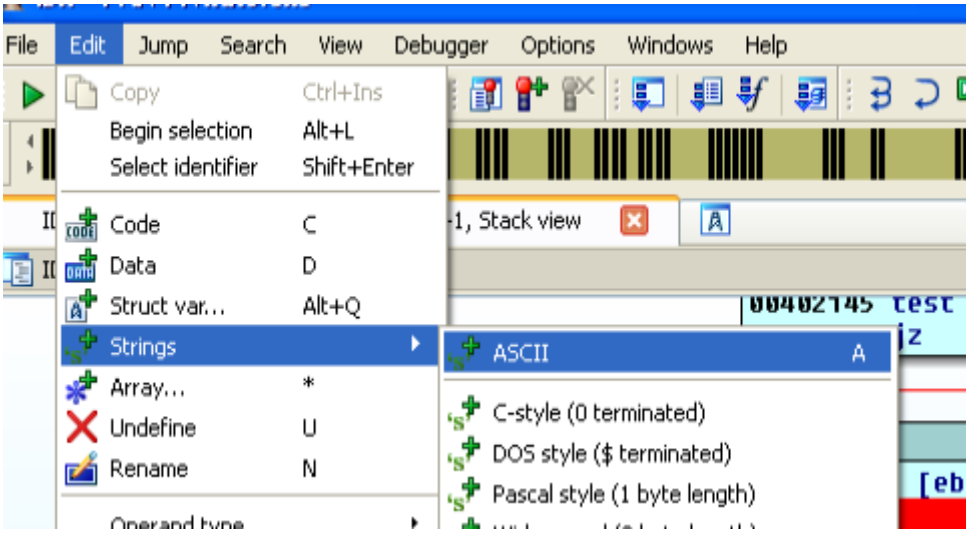
Donc c'est assez lourd de devoir « convertir » en string à chaque fois.

Donc on va sur notre bidule et on appuie sur « a »



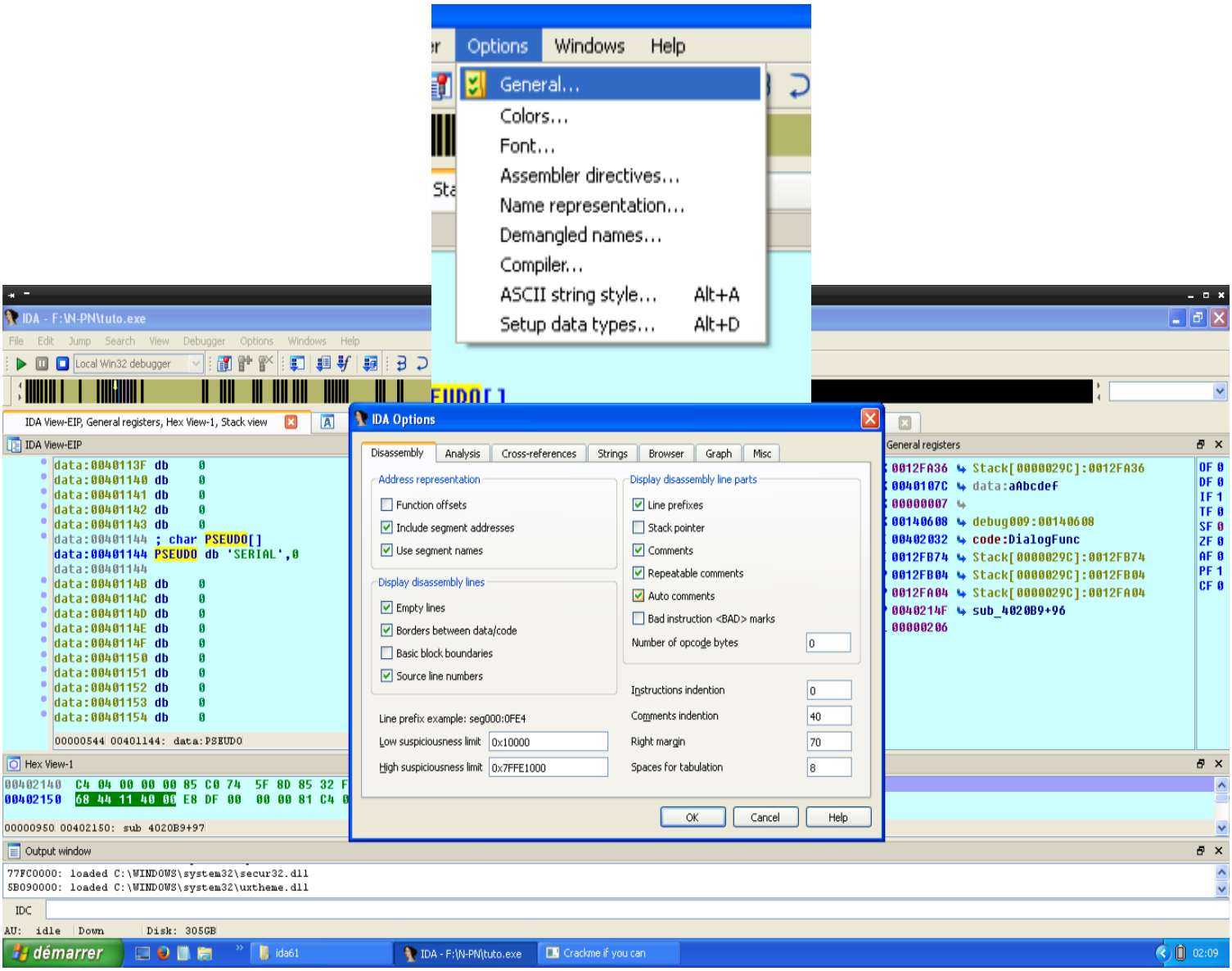


On peut aussi :



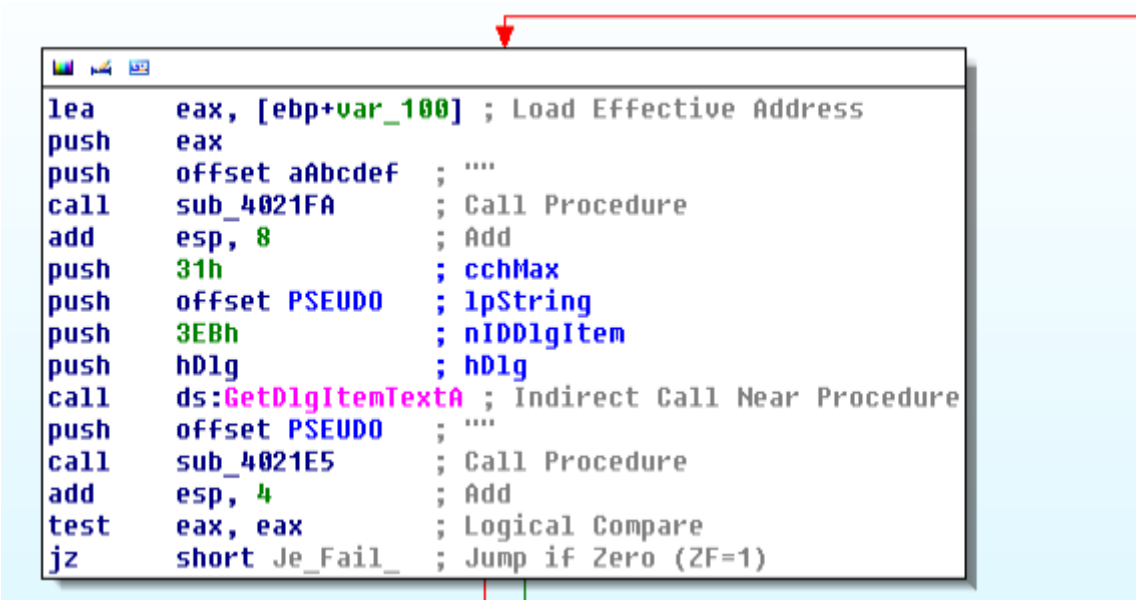
Une aide bienvenue !

Encore autre chose, parfois on se confond dans les JMP , JZ , JBE , XOR , ROL alors IDA nous traduit .. si si je vous jure !



Cochez « Auto-Comments »

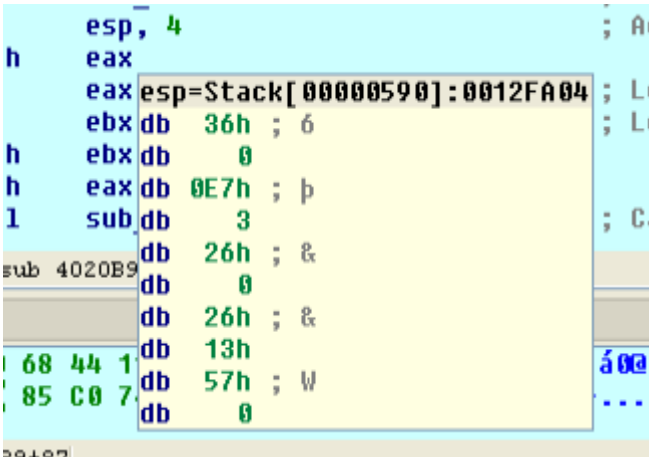
J'admets le résultat est un peu lourd, mais bon ça peut aider sur un trou de mémoire .



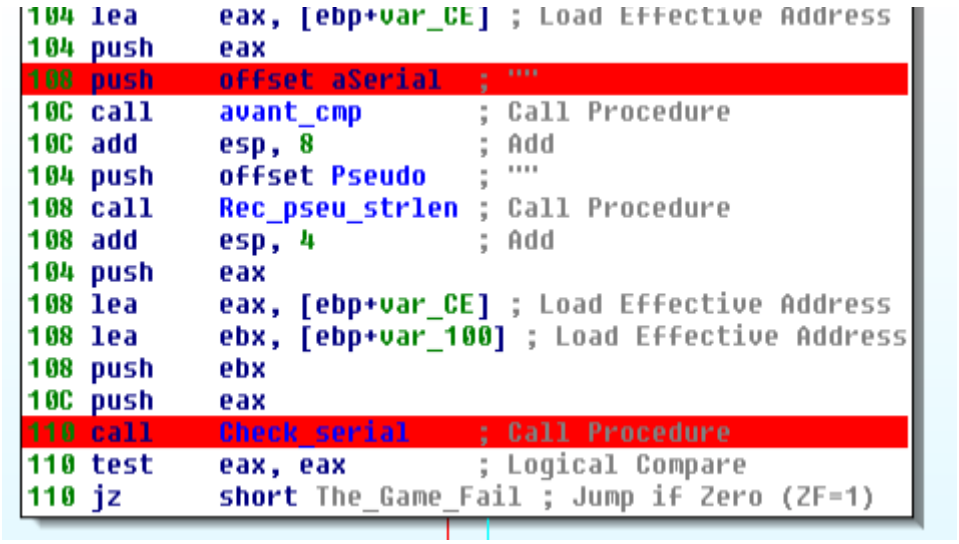
IDA Ne Perd pas le Nord (lui)

Envie de savoir en plein debug ce que vaut un registre , ou ce que va donner le résultat de quelque chose ? Laissez votre souris dessus !

Esp ?

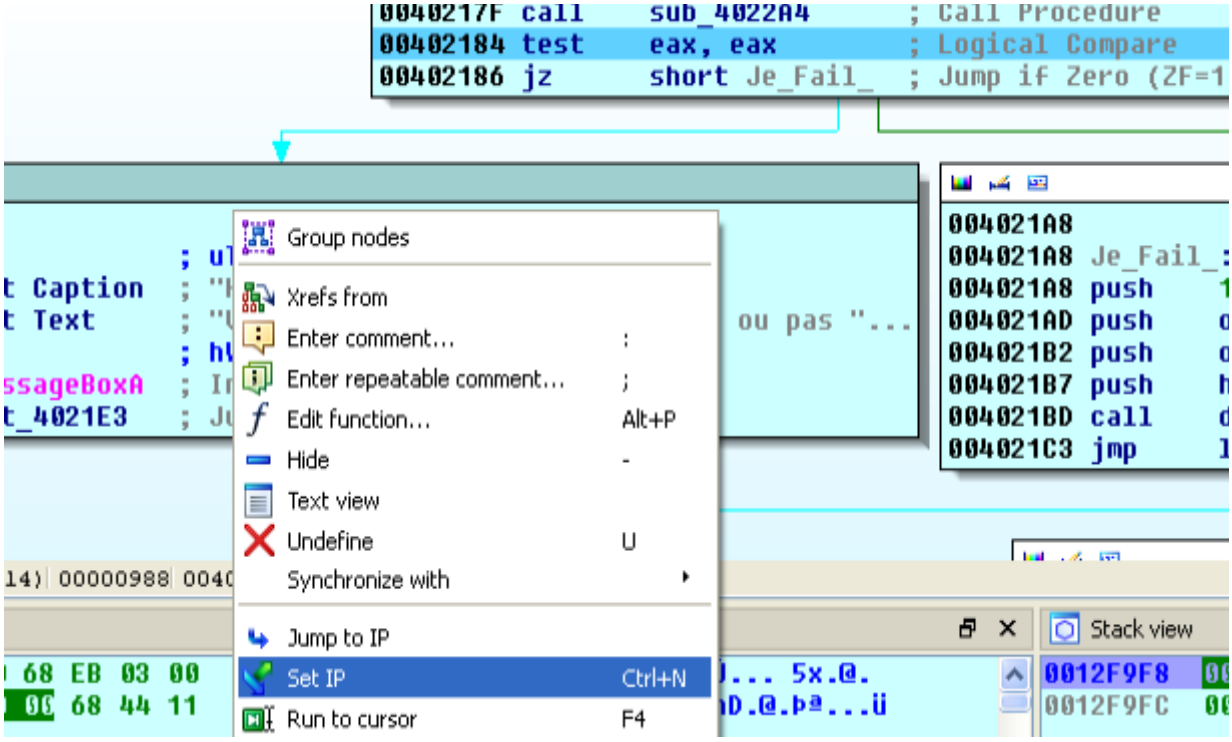


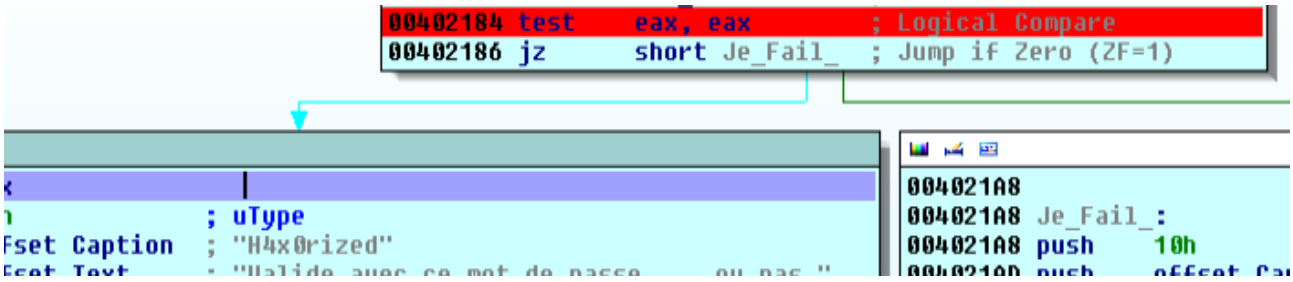
Voilà une petite idée quand on bosse sur un truc :



L'édition Hexa et le Jump To

Vous voulez tester un nop ou autre sans toucher à l'hexa ? Faite clic droit « Set IP ».



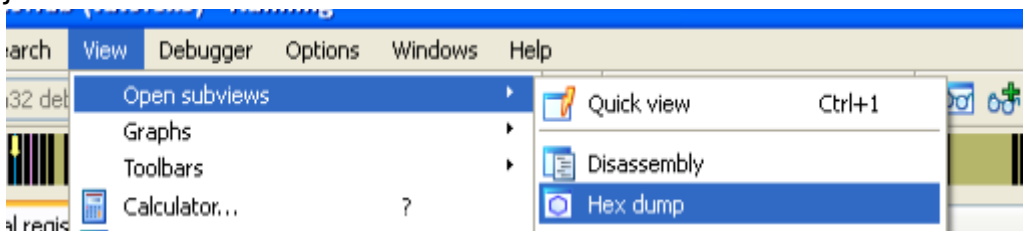


On jump plus à fail.

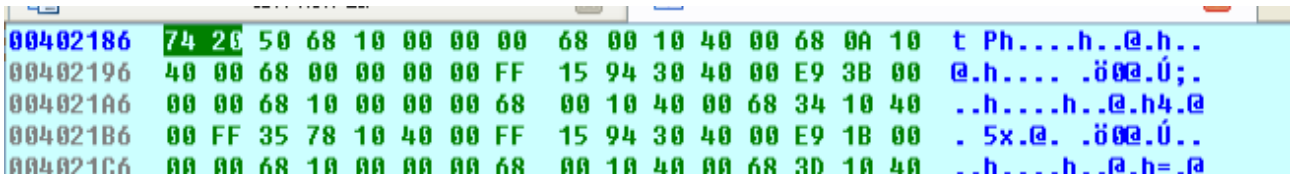
Éditer l'Hexa

On met en jaune (1 clic)

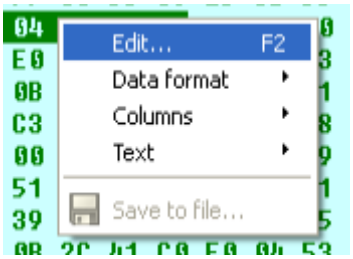
Si jamais on ouvre la « Hex view »



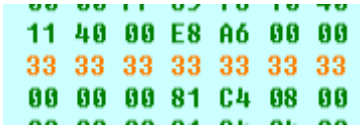
« Notre Jump est déjà sélectionne »



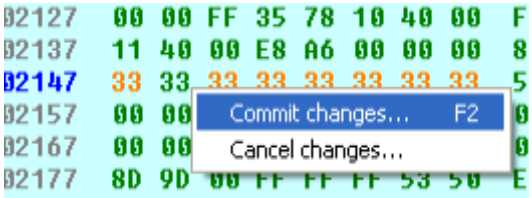
On clic droit « edit » :



On met ce que l'on souhaite :



On enregistre :



--
Alors Heureux ? Il y'a encore beaucoup de choses mais c'est déjà pas mal.
A une prochaine !

Thxer ;)