cela donne vous pouvez regarder dans la fenêtre en bas à l'adresse 402160 (+ESI mais comme celui-ci a varié de 0 à 6 les résultats commencent en 402160+0 donc bien 402160 et finissent en 402166) ce que cela donne (ici "yvw•••"). Nous verrons par la suite à quoi cela sert.

On continue notre pas à pas (pour éviter de faire en pas à pas les 6 boucles de la routine vous pouvez poser un BP juste à la sortie de la routine en 00401139 et appuyez sur Run pour s'y rendre immédiatement). Par la suite on trouve un INC EBX (pour passer au caractère suivant, donc caractère suivant le deuxième 01h) et une mise à 0 de ESI. Et ensuite encore une routine qui est strictement identique à la deuxième rencontrée à une différence près : CMP ESI,1B2 et non 1D5. Il faut donc que la somme des caractères après le deuxième 01h soit égale à 1B2h. On a 4 caractères après le deuxième séparateur. On fait donc 1B2/4 = 6C et il reste 2. Donc on aura trois fois 6C et une fois 6C +2 soit 6E : 4E|4E|4E|4E|4E|4F|01|37|38|39|41|42|43|01|6C|6C|6C|6E. On fait donc les modifications dans l'éditeur hexa (pensez à réinitialiser OllyDbg et noter à quelle ligne on est). On teste en lançant le .exe. Et là : BINGO ! Ça marche ! Mais il y a un petit détail qui ne va pas ! Notre nom ne ressemble à rien ! :-(On va donc voir comment il trouve le nom. On va donc breaker là où en était (00401155) et continuer à analyser le code. Une fois le programme breaké, on va regarder un peu en dessous pour avoir une vue globale de la suite. Et on remarque :

```
004011F4 > \68 60214000 PUSH due-cm2.00402160 ; /Text = "yvw..."
004011F9 . 6A 01 PUSH 1 ; |ControlID = 1
004011FB . FF75 08 PUSH DWORD PTR SS:[EBP+8] ; |hWnd
004011FE . E8 5E010000 CALL <JMP.&USER32.SetDlgItemTextA> ; \SetDlgItemTextA
```

Le texte qu'il va afficher : yvw... ressemble étrangement à ce qu'on avait aperçu en 402160, là où on avait le résultat du XOR. Cette routine servait donc à trouver le nom. Maintenant il n'y a plus qu'à calculer pour arriver à afficher notre nom. On va essayer d'afficher "Deamon" (le nom fera forcément 6 caractères donc 6 lettres au maximum). On va donc décomposer mon nom "Deamon" en valeur hexa (pour cela soit vous prenez une table ascii qui est disponible dans HexDecCharEditor (l'icône du carré jaune :-)) ou soit vous tapez dans la partie ascii de l'éditeur et sa correspondance en hexa s'affiche).

D|e|a|m|o|n donne donc 44|65|61|6D|6F|6E. Mais pour trouver les lettres le crackme calcule en faisant un XOR entre les caractères après le premier 01h et ceux avant. On a : 4E|4E|4E|4E|4E|4F|01|X1|X2|X3|X4|X5|X6|01|6C|6C|6C|6E. Pour avoir 44 en pour la première lettre ("D") il faut que 4E XOR X1 = 44 (la variable X1 correspondant au nombre recherché pour la première lettre, X2 pour la seconde...) donc X1 = 4E XOR 44 = 0A. Faites le calcul du XOR avec la calculatrice de windows. Donc voici ce que ça donne :

X1 = 4E XOR 44 = 0A
X2 = 4E XOR 65 = 2B
X3 = 4E XOR 61 = 2F
X4 = 4E XOR 6D = 23
X5 = 4E XOR 6F = 21
X6 = 4F XOR 6E = 21

Ce qui nous donne : 4E|4E|4E|4E|4E|4F|01|0A|2B|2F|23|21|21|01|6C|6C|6C|6E

Si votre nom est plus court ou plus long vous pouvez déplacer les séparateurs et