Cours N° 2

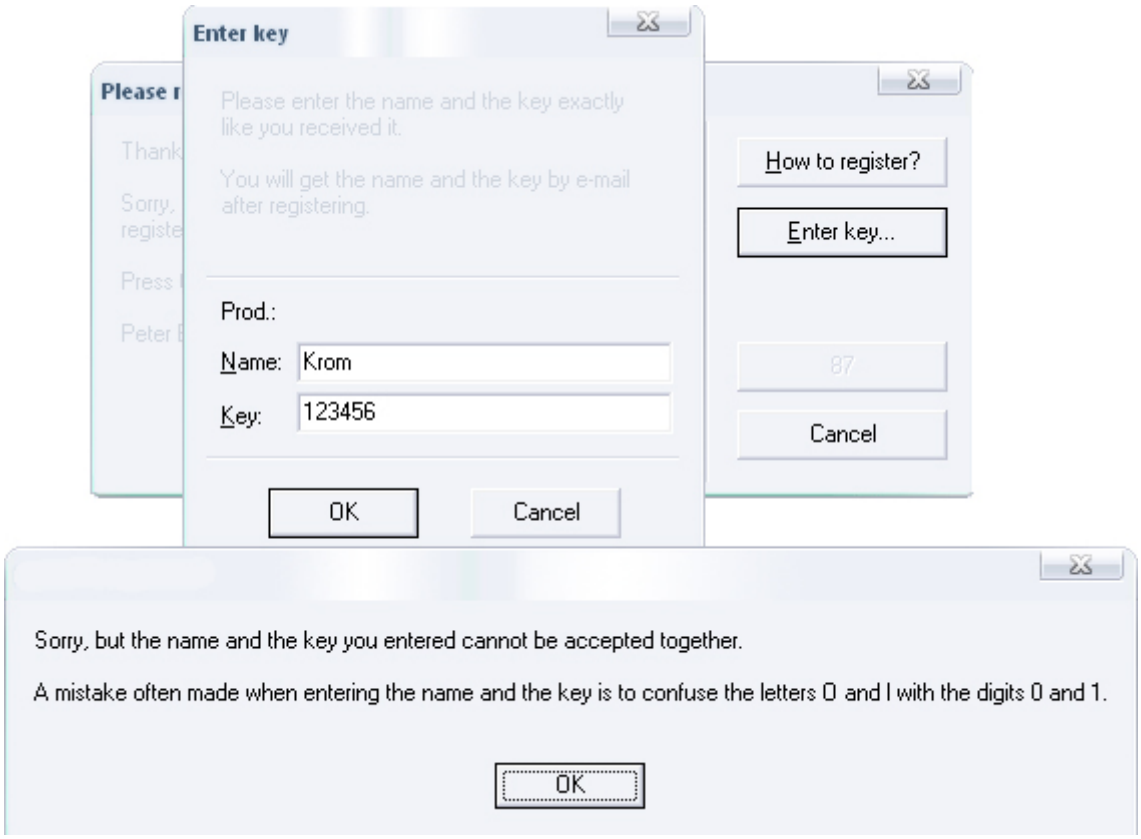
Pour ce premier vrais cours, l'objectif sera de modifier le programme pour qu'il nous enregistre avec n'importe quel code.

Il est téléchargeable ici :

- http://www.KromCrack.com/prog/HexaCours2.exe

(Password : KrommorK)

Quand on le lance, une fenêtre d'enregistrement s'affiche et nous demande de nous enregistrer et quand on clique sur "Enter Key..." et que l'on rentre un nom d'enregistrement et un code quelconque, ce message d'erreur apparait :



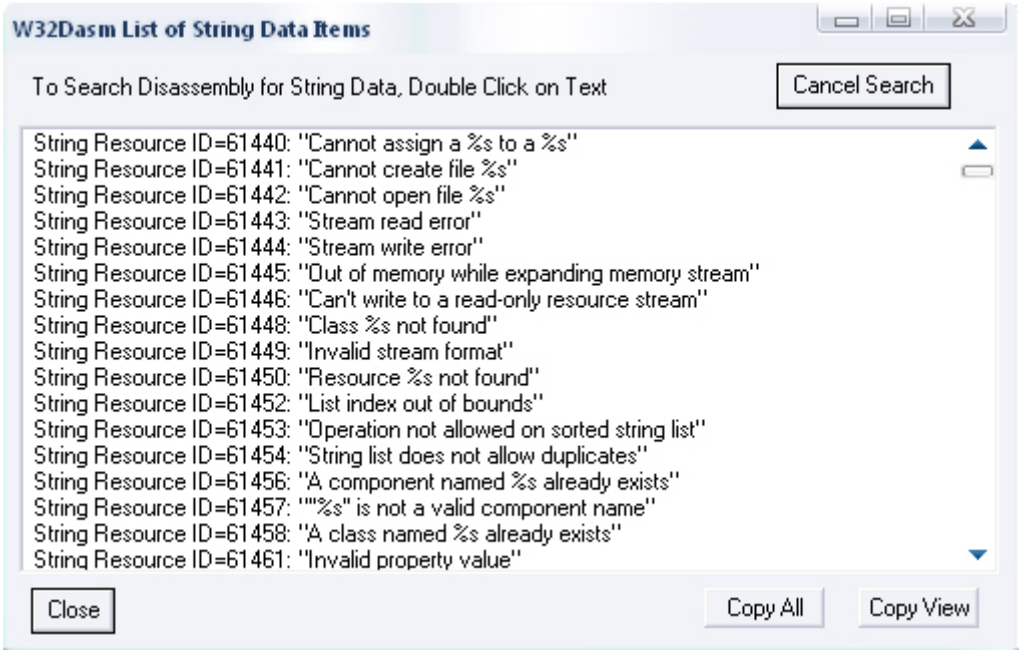
Ce que l'on va faire, c'est modifier le programme pour qu'il nous enregistre en entrant des informations bidon (ex : Krom / 123456).

Commençons par le débugger avec WinDasm 8.93 Téléchargeable ici :

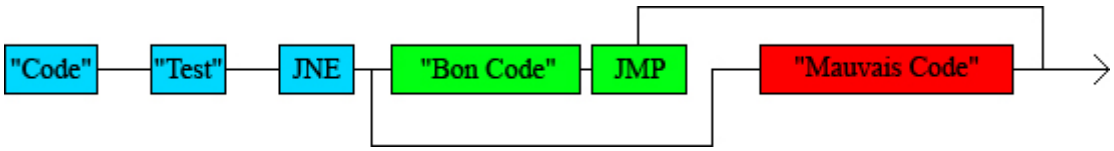
- http://www.KromCrack.com/prog/WinDasm.exe

(Password : KrommorK).

Lancez WinDasm et aller dans Disassembler -> Open File To Disassemble... -> et choisissez Hexa.exe. Faites CTRL + S pour aller au début du code (CTRL + START) puis aller voir les Strings Data Références. Ces lignes de codes représentent les messages des fenêtres du programme. Cliquez sur l'icone en dessous de HexData et Refs  . Vous avez alors cette fenêtre qui s'affiche :



Le but de ce cours est de Cracker ce programme pour qu'il nous enregistre avec n'importe quelle nom et avec n'importe quel code, donc ce que l'on va faire c'est "Casser" la vérification du code pour que celui-ci soit "Toujours bon". Le message d'erreur qui a apparu quand nous avons essayé de nous enregistrer n'est que le mauvais résultat de la vérification du code.

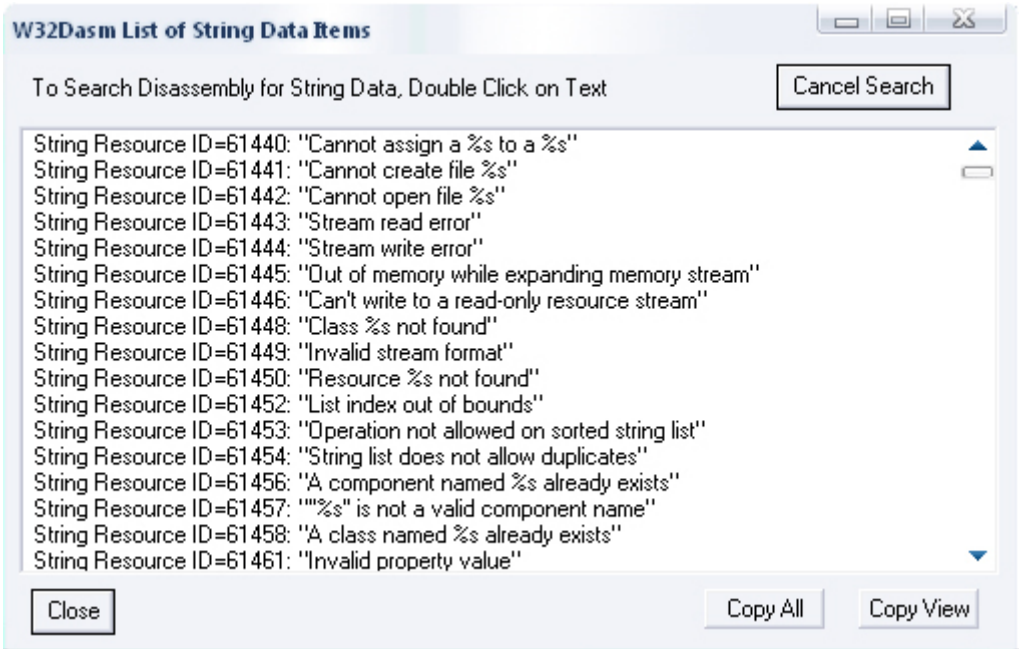


Dans ce schéma, on voit qu'une fois le code entré, il est vérifié par ce que l'on appelle "Une routine de calcule". Apres cette vérification, on arrive a un JNE (Jump if not égual to Zéro ou en français : Saute si ce n'est pas égual à 0, sous entendu saute si la vérification du code donne autre chose que 0 donc autre chose que le bon code) qui saute vers le message d'erreur que nous avons eu avant :

-> "Sorry, but the name and the key you entered cannot be accepted together..."

Ce qu'il faudra faire c'est modifier le programme pour que le TEST indique au JNE que le code est "bon" ce qui aura pour but d'enregistrer le programme. Il faut donc remonter avant ce message d'erreur pour modifier "la routine de calcul ou d'enregistrement".

Après cette petite parenthèse sur le calcul du sérial, cliquez sur Strings Data Références ->  , et une fenêtre s'affiche :



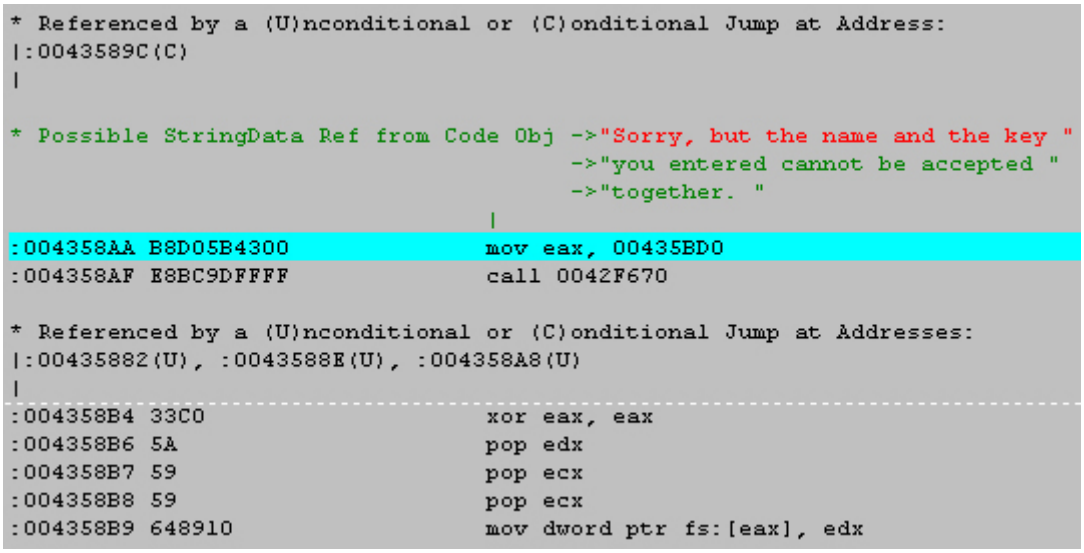
Pour retrouver la phrase contenue dans le message d'erreur sans y passer des heures, cliquez sur "Copy All" puis Démarrer -> Exécuter... -> notepad.exe Collez ensuite dans le bloc-notes.
Recherchez ensuite :

"Sorry, but"

Et vous trouverez :

"Sorry, but the name and the key "

Vous avez vu que ce message était vers la fin. Retournez maintenant dans WinDasm et double cliquez sur cette ligne, vous arriverez ici :



Regardez cette phrase un peu plus haut :

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
| : 0043589C (C)

Cette ligne de code veut simplement dire que nous sommes arrivés ici :

004358AA |> B8 D05B4300 MOV EAX,HexDecCh.00435BD0

Par un saut depuis la ligne :

0043589C |. 75 0C JNE SHORT HexDecCh.004358AA

Pour aller à cette ligne faites SHIFT + F12 -> 0043589C

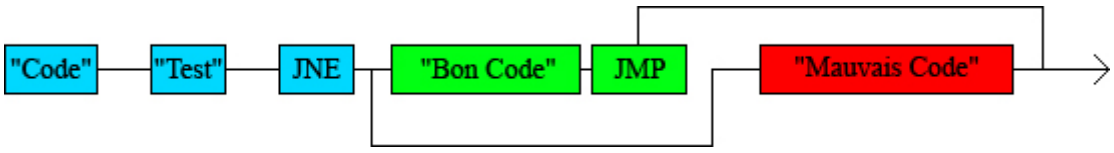
```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0043585C(C)
|
:00435890 E89F23FDFF              call 00407C34
:00435895 83BBD801000007          cmp dword ptr [ebx+000001D8], 00000007
:0043589C 750C                    jne 004358AA
```

Arrivés là, rien d'intéressant alors remontons de la même manière encore un peu plus :
SHIFT + F12 -> 0043585C

Et là, on arrive à un endroit intéressant:

```
:00435855 E8EEC2FFFF               call 00431B48
:0043585A 84C0                     test al, al
:0043585C 7432                     je 00435890
```

Eh oui, un CALL suivi d'un TEST et d'un JE (Jump if Egal to 0) ou JNE (Jump if Not Egal to 0) est presque toujours la routine de vérification du code. Alors voici comment ça se passe : On entre un code, il est mis dans le CALL, puis le TEST vérifie si le code est différent du bon ou pas et dit au JE ou JNE de sauter vers le bon ou le mauvais message d'enregistrement. (La méthode de vérification du code à été expliqué plus en détail un peu plus haut)



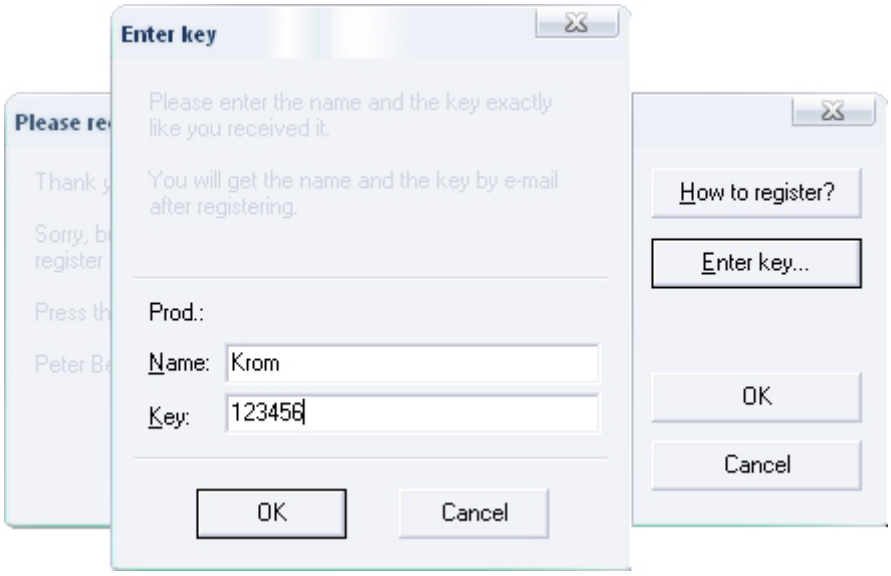
On va donc voir ce qui ce passe dans le CALL et donc voir comment le code est contrôlé :

-> Faites CTRL + L puis LOAD et 2 nouvelles fenêtres vont s'ouvrir:

Puis SHIFT + F12 et notez l'adresse du CALL (00435855)

-> Une fois que vous êtes sur la ligne pressez la touche F2 ce qui aura pour but de mettre un BreakPoint (Un point d'Arrêt). Ce BreakPoint va arrêter le programme dès qu'il arrivera sur cette ligne et donc il va s'arrêter avant la vérification du code.
-> Ensuite pressez la touche F9, cette touche va lancer le programme.

Le programme s'ouvre et la vous et cliquez sur "Enter Key..."
Puis entrer votre nom et un serial bidon (ex : Krom / 123456). Puis OK
Et la vous aller entendre entendez un "Bing" , cela veut dire que le programme a "Breaker" sur l'adresse 00435855



Après avoir fait ok le programme ne nous dit pas -> "Sorry, but the name and the key you entered cannot be accepted together..." car nous avons stoppé le programme avant qu'il fasse sa vérification.
Retournons alors dans WinDasm où on va entrer dans le CALL avec F7 et exécuter lignes par lignes avec F8 jusqu'a arriver ici :

00431D73 . C2 0400 RETN 4

Ce "ret 004" est l'instruction qui délimite la fin du CALL
Remontons un peu pour voir où le code est mis comme "faux" dans le registre. (On peut voir clairement quelles lignes ne sont pas exécuté -> elles ne sont pas en rouge).

On voit ici que c'est à cause du JNE et du JL (qui ont sauté par-dessus les lignes) que les lignes plus bas n'ont pas été exécutées.

00431BDE . 0F85 33010000 JNE HexDecCh.00431D17

00431BEF . 0F8C 22010000 JL HexDecCh.00431D17

```
:00431BB8 E84F3DFDFF              call 0040590C
:00431BBD 8B55E4                  mov edx, dword ptr [ebp-1C]
:00431BC0 8D4508                  lea eax, dword ptr [ebp+08]
:00431BC3 E8EC18FDFF              call 004034B4
:00431BC8 8B55F8                  mov edx, dword ptr [ebp-08]
:00431BCB 8BC3                    mov eax, ebx
:00431BCD E886FEFFFF              call 00431A58
:00431BD2 8BF0                    mov esi, eax
:00431BD4 8B4508                  mov eax, dword ptr [ebp+08]
:00431BD7 E8EC3EFDFF              call 00405AC8
:00431BDC 3BF0                    cmp esi, eax
:00431BDE 0F8533010000            jne 00431D17
:00431BE4 8B45F8                  mov eax, dword ptr [ebp-08]
:00431BE7 E8A819FDFF              call 00403594
:00431BEC 83F80A                  cmp eax, 0000000A
:00431BEF 0F8C22010000            jl 00431D17
:00431BF5 B201                    mov dl, 01
:00431BF7 B8E8F74200              mov eax, 0042F7E8
:00431BFC E89BDCFFFF              call 0042F89C
:00431C01 8945E8                  mov dword ptr [ebp-18], eax
:00431C04 33C0                    xor eax, eax
:00431C06 55                      push ebp
:00431C07 68101D4300              push 00431D10
:00431C0C 64FF30                  push dword ptr fs:[eax]
:00431C0F 648920                  mov dword ptr fs:[eax], esp
:00431C12 BA02000080              mov edx, 80000002
:00431C17 8B45E8                  mov eax, dword ptr [ebp-18]
:00431C1A E80DDDFFFF              call 0042F92C
:00431C1F 8D55E4                  lea edx, dword ptr [ebp-1C]
:00431C22 B8801D4300              mov eax, 00431D80
:00431C27 E8C0E3FFFF              call 0042FFEC
:00431C2C 8D45E4                  lea eax, dword ptr [ebp-1C]
:00431C2F 8B55FC                  mov edx, dword ptr [ebp-04]
:00431C32 E86519FDFF              call 0040359C
:00431C37 8B55E4                  mov edx, dword ptr [ebp-1C]
:00431C3A B101                    mov cl, 01
:00431C3C 8B45E8                  mov eax, dword ptr [ebp-18]
:00431C3F E84CDDFFFF              call 0042F990
:00431C44 84C0                    test al, al
:00431C46 0F84AE000000            je 00431CFA
:00431C4C 8D55E4                  lea edx, dword ptr [ebp-1C]
:00431C4F B8A01D4300              mov eax, 00431DA0
:00431C54 E893E3FFFF              call 0042FFEC
```

Nous voyons que si on annule les sauts les lignes plus bas vont s'exécuter ce qui aura pour but d'enregistrer le programme.

00431BDE . 0F85 33010000 JNE HexDecCh.00431D17

00431BEF . 0F8C 22010000 JL HexDecCh.00431D17

Pour les annuler, il faut les remplacer par:

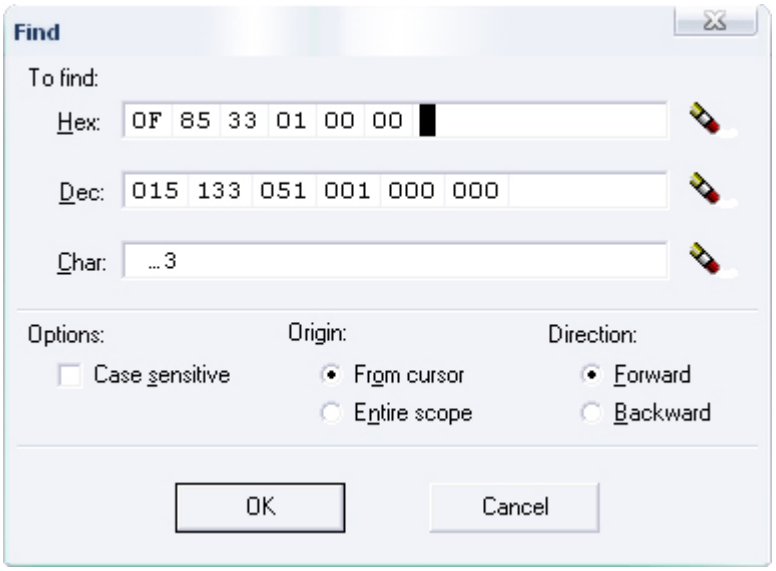
00431BDE . 9090 90909090 nop nop nop nop nop nop

00431BEF . 9090 90909090 nop nop nop nop nop nop

"nop" C'est l'instruction qui vent dire "No OPeration" -> "ne rien faire"
Pour modifiez ces lignes, vous pouvez utilisez un autre Editeur Hexadécimal ou Hexa.exe mais bon il vous faudra attendre un moment mais bon , on a le temps ;)
Donc, une fois Hexa.exe lancé, faites CTRL + F (Pour rechercher). et rechercher :

0F8533010000

Pourquoi ça ? Parce que 0F8533010000 ce n'est que l'instruction jne 00431D17 traduit en Hexadécimal.



Vous arrivez donc là:

FF	FF	8B	F0	8B	45	08	E8	EC	3E	FD	FF	3B	F0	0F	85
33	01	00	00	8B	45	F8	E8	A8	19	FD	FF	83	F8	0A	0F
8C	22	01	00	00	B2	01	B8	E8	F7	42	00	E8	9B	DC	FF

Mettez ensuite votre curseur sur le "0F" et notez 90 jusqu'a 00.

Attention toutefois à bien vérifier s'il n'y a qu'une seul occurrence, pour vérifier cela, tapez F3.
F3 a pour but d'aller a l'occurrence suivant donc si le programme émet un son et qu'il ne va pas plus loin ça veut dire que c'est bon, sinon il faudra regarder ce qu'il y a avant et après ce que l'on cherche

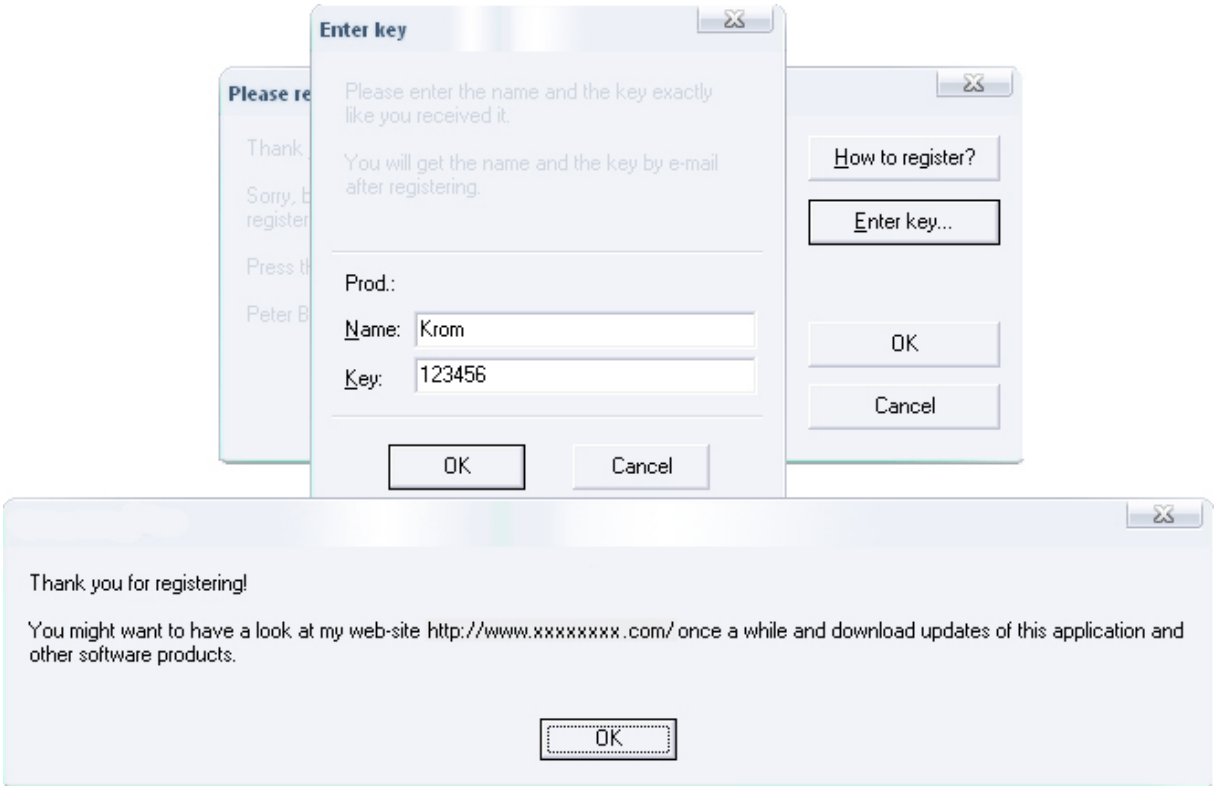
le premier étant Cracker passons au 2 ème saut en

00431BEF . 0F8C 22010000 JL HexDecCh.00431D17

Comme avant, CTRL + F et recherchez 0F8C22010000

33	01	00	00	8B	45	F8	E8	A8	19	FD	FF	83	F8	0A	0F
8C	22	01	00	00	B2	01	B8	E8	F7	42	00	E8	9B	DC	FF
FF	89	45	E8	33	C0	55	68	10	1D	43	00	64	FF	30	64

Même modification qu'avant :
Mettez ensuite votre curseur sur le "0F" et notez 90 jusqu'a 00. Après ces 2 modifications, cliquez sur File -> Save as... et enregistrer le en tant que "Hexa Cracked.exe".
Fermez ensuite l'éditeur Hexadécimal et lancez Hexa Cracked.exe. Et là, quand on clique sur "Enter Key..." et que l'on entre un enregistrement bidon (ex : Krom / 123456) Ca marche !! On est maintenant enregistré !



Et dans Help -> Infos... on peut voir :

Registered by: Krom

Ce programme est maintenant totalement Cracké ;)

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/**