Source :
flashtro.com
Traducteur : Gi@nts

Tutorials	**AmigaCracking : ROBOCOP**
Protection	**Single Track Protection - CopyLock**
(source) Original Author	**Scenex**
Submitted by (on flashtro.com)	**scenex Date: 2004-07-28 10:52**
Version FR	**22/02/2015 Gi@nts**

ROBOCOP
* CRACK TUTORIAL *

Materiels nécéssaire :

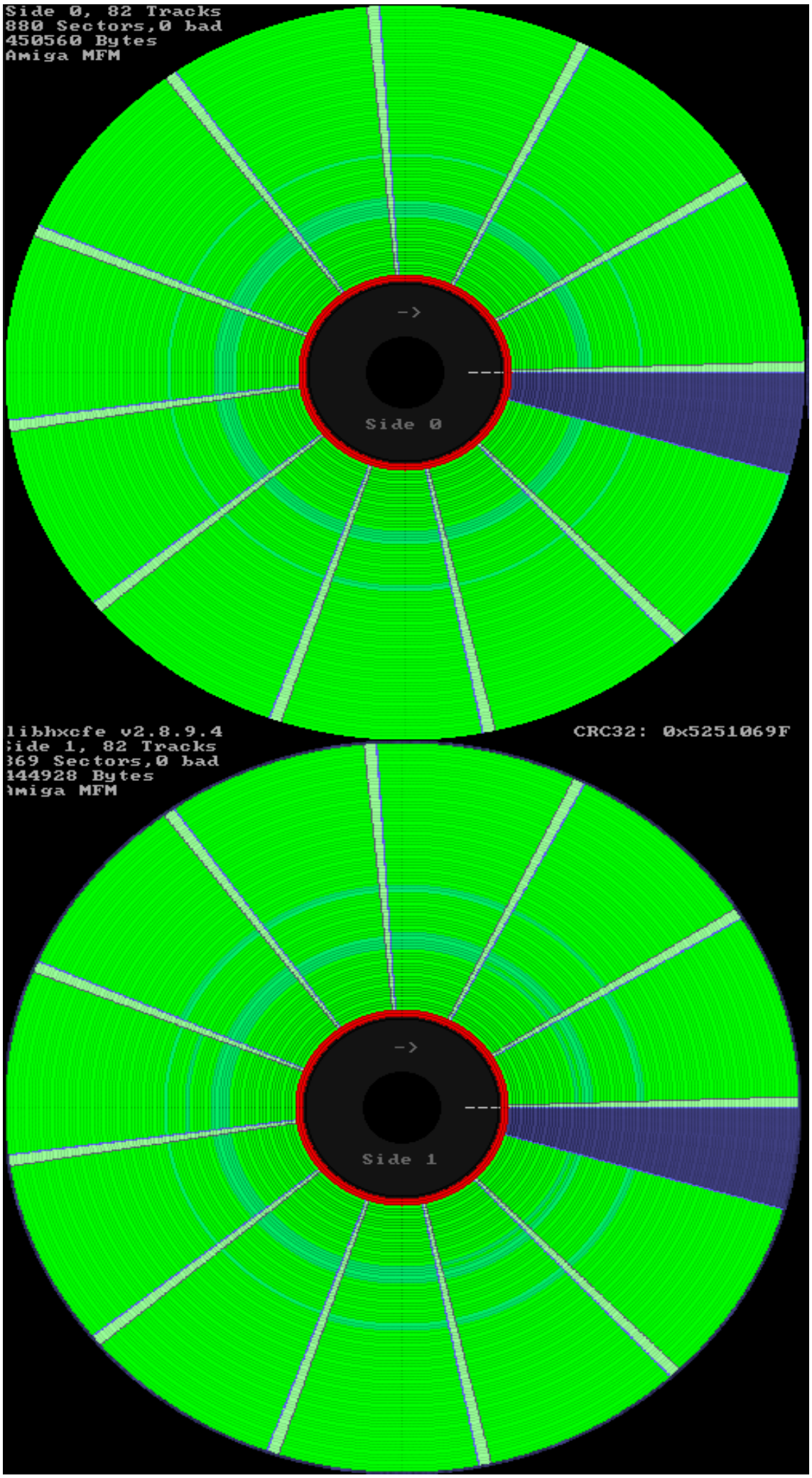
1) Un AmigA avec 512K (ou plus) ou l'émulateur WINUAE
2) Une Carte ACTION REPLAY MKIII (ou ça ROM Image)
3) Le jeu Original ROBOCOP ou son image CAPS (SPS 1620)
4) le logiciel Xcopy Pro en disquette ou image disk.

General Info:

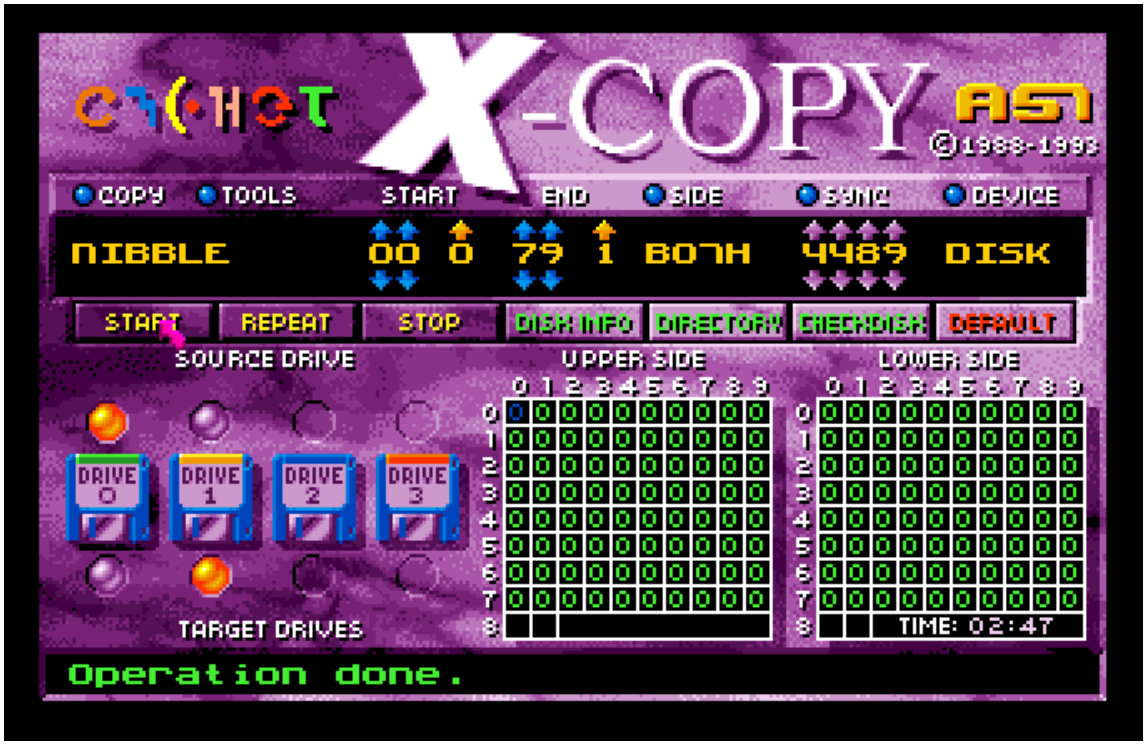
Ce tutoriel Français est basé sur le tutoriel original de Scenex.
Ce document n'est pas une traduction mot par mot de celui-ci mais plus une nouvelle version.
Suivit pas à pas avec des nouvelles informations.

Bon tuto.

Gi@nts


Side 0, 82 Tracks
880 Sectors,0 bad
450560 Bytes
Amiga MFM
->
Side 0
libhxcfe v2.8.9.4
ide 1, 82 Tracks
69 Sectors,0 bad
144928 Bytes
miga MFM
CRC32: 0x5251069F
->
Side 1

Comme dans Tous bon hack qui se respecte, on va commencer par essayer de copier le disk original.
Démarrer votre logiciel de copie préféré, à savoir **Xcopy Pro**
Choisissez le mode **NIBBLE, insérez** une disquette **vierge** en **DF1** et la disquette du **jeu original** en **DF0**
Lancer la copie



Malgré une copie qui semble n'avoir posée aucun problème particulier, le jeu ne fonctionnera pas.
Mais gardons quand même sous le coude ce ***backup.***

Insérez la disquette original du jeux dans le lecteur de l'Amiga, nous allons charger le **bootblock** en mémoire et regarder ça de plus prêt :

#RT alias Read Track, permet le chargement de la track 0 à 1 (1er piste de la face 0)
#D, alias Désassemble

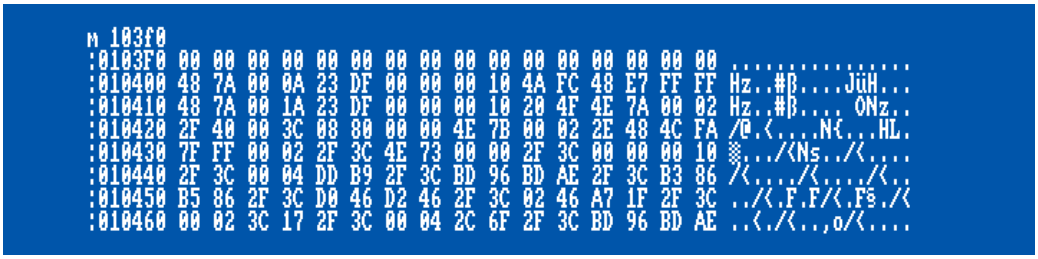
Tapez : rt 0 1 10000 puis **d 10000**

Il semblerait qu'on ait notre petite routine de déplacement de donnée ici :

01002C MOVE.L A3,28(A1) <== Adresse de destination en **A3**
010030 MOVE.L #1200,24(A1) <== Nbr de donnée a copier : **$1200**
010038 MOVE.L #400.2C(A1) <== Adresse source de lecture : **$400**

Cela va donc copier **$1200** de donnée à partir de **$400** vers l'adresse contenue dans **A3**

Voyons voir de plus prêt ce qui se trouve en ce moment à cette adresse**.**
#M alias memory read, permet de voir les données en mémoire.
Taper n 103F0



On remarquera notre jolie saut à l'adresse **$1005C** une fois les données déplacées.
On va modifier notre petit **'bootblock'** pour éviter ce **JMP** histoire d'en savoir plus.

Taper :

#BRA, Instruction du 68000 qui permet de se brancher à l'adresse indiqué, ici une boucle sur nous même.
#BOOTCHK, permet de calculer le checksum d'un bootblock en mémoire
#WT, alias Write Track, permet d'écrire une zone mémoire sur la disquette à l'adresse indiqué en cylindre.

 # On modifie le code à partir de 1005C
A 1005C

#On change le RTS par un BRA sur soit même, la fameuse boucle infini.
BRA 1005C [**ENTRER**] puis [**ESCAPE**]

#On calcul le nouveau checksum de ce bootblock
BOOTCHK 10000

#On sauve le tout sur disquette
Insérez la disquette de **backup** préalablement crée et taper :
WT 0 1 10000

```
d 1005c
~01005C JMP     (A3)
a 1005c
^01005C BRA 1005C
^01005E
bootchk 10000
Old checksum was F2B031EB, now is set to E08531EB
wt 0 1 10000
Disk ok
```

Effectuer un **reboot** de votre Amiga tout en laissant la disquette de backup dans celui-ci.

Après un court chargement (celui du **bootblock**), l'Amiga semble ne plus rien faire.
Il est entré dans notre boucle sans fin.

Entrer dans votre **AR**
Taper : D

~0015B4 BRA 000015B4

On est bien dans notre boucle sans fin, impeccable.
On va voir si maintenant on arrive à trouver notre petite signature de **'copylock'** en mémoire.
Taper F 48 7A

```
d
~0015B4 BRA     000015B4

f 48 7a
Search from: 000000 to: C80000
0059E8  0059F8  _
```

Bingo, trouver !

On jette un petit coup d'œil en mémoire à l'adresse indiquer :
Taper n 59E8

```
n 59e8
.0059E8 Hz..#ß....JüH...Hz..#ß.... ONz../@.(....N(...HL.▒.../(Ns../(....
.005A28 /(..../(..../(..../(.F.F/(.Fs./(..(./(..,o/(....#....$.|§.\....$
.005A68 r.q./.m.../4m..T/.Ä)aM.T.@Yi.y.@...z..'..\...6.@.wö=....|...\./.
.005AA8 |.aM...8k9/......N.....QAV.*.v.(@r.W@x|...6ü.M..ö."üdÖ........äd
.005AE8 f.t...q..u.I..1...9C..(..*&|U...[.LKädl.1.9.Y...u..EW.o..B.),..E
.005B28 s.#...s....e..)..F..q."W....üZ..ß../'1f.Oi.R.$S.sJ..;M(.4.......
```

Au passage, on en profite pour regarder la tête du registre **A3**
Taper R

```
r
D0=00000000 0000001F 00000001 00000000  00000000 00000000 FFFFFFFF 0000004B
A0=00C0152A 00C014E2 00C014E2 000059E8  00001558 00FC0818 00C00276 00C80000
PC = 000015B4 USP = 00C014B2 SR = 0014 T=0 S=0 I=000 X=1 N=0 Z=1 V=0 C=0
```

On notera que l'adresse indiqué dans **A3** est exactement celle trouvé dans notre commande de recherche de **'copylock'**
Ceux d'entre vous qui ont déjà réalisé d'autres tuto copylock auront remarqué que l'adresse **59E8** est récurrente (voir crack-tuto d'Arkanoid – revenge Of Doh)

Maintenant on va tous simplement continuer l'exécution du **bootblock**
Cela passe bien sur par la suppression de notre modification.

Taper A 15B4 puis **JMP (A3)** [ENTRER] puis [ESCAPE]

```
a 15b4
^0015B4 JMP (A3)
^0015B6
x_
```

Et avant de retourner à l'exécution de notre code, on **remplace** la **disquette de backup** par la **disquette original** de notre **jeu** dans le lecteur Amiga, puis :

#X permet le retour au code Amiga en court.
Taper X

Laisser le jeu accéder à 1 ou 2 pistes (**pas plus)** et **entrer** dans votre **AR**
On va aller voir si le code à changer.
Taper n 59E8

Sur l'image ci dessous on peu voir la zone mémoire **AVANT** le **JMP(A3)** et **APRES** le **JMP(A3)**

```
n 59e8
.0059E8 Hz..#ß....JüH...Hz..#ß.... QNz../@.(....N(...HL.▒.../(Ns../(....
.005A28 /(..../(..../(..../(.F.F/(.Fß./(..(./(..,o/(....#....$.lß.\....$
.005A68 r.q./.m.../4m..I/.A)aM.T.@Yi.y.@...z..'..\...6.@.wö=....|...\./.
.005AA8 |.aM...8k9/......N.....QAV.*.v.(@r.W@x|...6ü.M..ö."üdÖ........äd
.005AE8 f.t...q..u.I..i...9C..(..*&|U...[.LKädl.i.9.Y...u..EW.o..B.),..E
.005B28 s.#...s....e..)..F..q."W....üz..ß../'1f.Oi.R.SS.sJ..;M(.4.......

n 59e8
.0059E8 A...!...N@.|..3ü▒..ß..Q....A..ß..0(..0ü..Q...3ü. .ß..A..BC... (
.005A28 ...-. Q..üN.p.2(..4(..6(..A.....C...a...f.N.....H.▒üNV.ü8..D..=D
.005A68 .ü=A..=B..=C..-H.ä-I..äX.@..R@=@..p.6.g...ÖA.|..n.........ü...n
.005AA8 ....g..A=A..HA=A..a..T0...r..@.n..o.2...=A..a..vf!......f.a...a.
.005AE8 .Ff(0....n..g.=@..0..........äBn..0....n..'./.a...a... .g r.2...
.005B28 .n....g..I.ü...n...n../A.(N^J.Lß?.Nux.Bn.üBn..Bn..4...a...f...p.
```

A l'évidence, il y a eu du changement, le '**copylock**' a sûrement décodé les données.
Voyons voir jusqu'où vont ces données.

Taper n 59E8 et **descendez** jusqu'à atteindre ce qui vous semble la fin des données chargée en mémoire
En l'occurrence : **$6262**

```
:006178 4C DF 00 0C 4E 75 48 E7 20 00 74 55 08 39 00 04 Lß..NuH. .tU.9..
:006188 00 BF E0 01 67 10 70 03 72 FF 61 00 00 20 51 CA ....g.p.r.a.. Q.
:006198 FF EC 70 1E 60 10 30 2E FF DC D0 40 41 FA 00 B4 ..p.`.0..ü.@A...
:0061A8 42 70 00 00 70 00 4C DF 00 04 4E 75 2F 00 61 00 Bp..p.Lß..Nu/.a.
:0061B8 00 32 4A 01 6B 04 08 80 00 01 08 80 00 00 13 C0 .2J.k...........
:0061C8 00 BF D1 00 08 C0 00 00 13 C0 00 BF D1 00 20 1F ..............
:0061D8 61 00 00 44 4E 75 61 00 00 0A 13 C0 00 BF D1 00 a..DNua.........
:0061E8 4E 75 48 A7 60 00 30 2E FF DC 14 39 00 BF D1 00 NuHß`.0..ü.9....
:0061F8 00 02 00 7F 06 00 00 03 01 82 04 00 00 03 D0 40 ...▒...........@
:006208 32 3B 00 50 08 01 00 00 67 04 08 82 00 02 10 02 2;.P....g.......
:006218 4C 9F 00 06 4E 75 61 00 00 20 08 39 00 00 00 BF L...Nua.. .9....
:006228 EE 01 66 F6 53 80 66 EE 4E 75 08 39 00 00 00 BF ..föS.f.Nu.9....
:006238 EE 01 66 1C 53 80 67 18 13 FC 00 08 00 BF EE 01 ..f.S.g..ü......
:006248 13 FC 00 CC 00 BF E4 01 13 FC 00 02 00 BF E5 01 .ü....ä..ü......
:006258 4E 75 FF FF FF FF FF FF FF 00 00 00 00 00 00 00 Nu..............
```

Dans un premier temps on va sauver tout ca sur une disquette vierge.
Insérez donc une nouvelle disquette formatée

Taper :

SM track, 59E8 6262

Soit exactement : **$6262** – **$59E8** = **$87A** de données

Avant le moindre accès disque, **Entrez** dans votre **AR**
Taper :
LM track, 10000

Remplace maintenant la **disquette de SAUVEGARDE** par la **disquette original** dans le lecteur Amiga
Taper :

RT 0 2 30000

#On transfère nos datas décryptée vers la zone tampon en question (30000+400)
TRANS 10000 1087A 30400

Remplace la **disquette du jeu original** par la **disquette de BACKUP** dans le lecteur Amiga, puis :

Taper :
#Et on sauve le tout sur disquette,
WT 0 2 30000

Maintenant je le jeu devrais être fonctionnel et surtout copiable simplement avec xcopy
Redémarrer votre Amiga et apprécier le jeu !