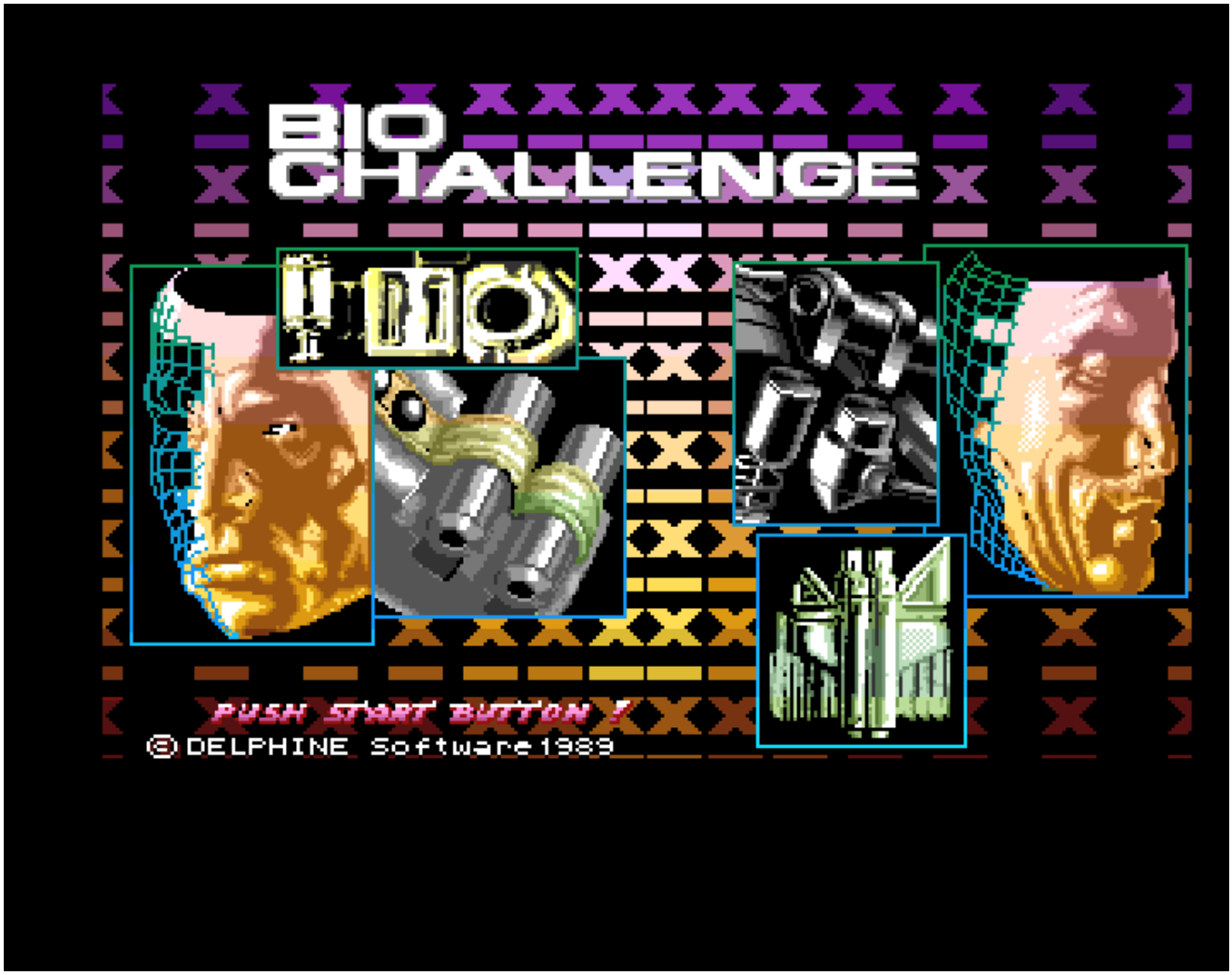


Tutoriel	**AmigaCracking : Bio Challenge**
Protection	**Bootlock**
Auteur Original	**Rob**
Soumit par (sur flashtro.com)	**Rob [2004-07-25]**
Version	**18/02/2017 Gi@nts**
Vérification/Correction	**V2**

BIO CHALLENGE
* CRACK TUTORIEL *

Table des matières

Matériels nécessaire

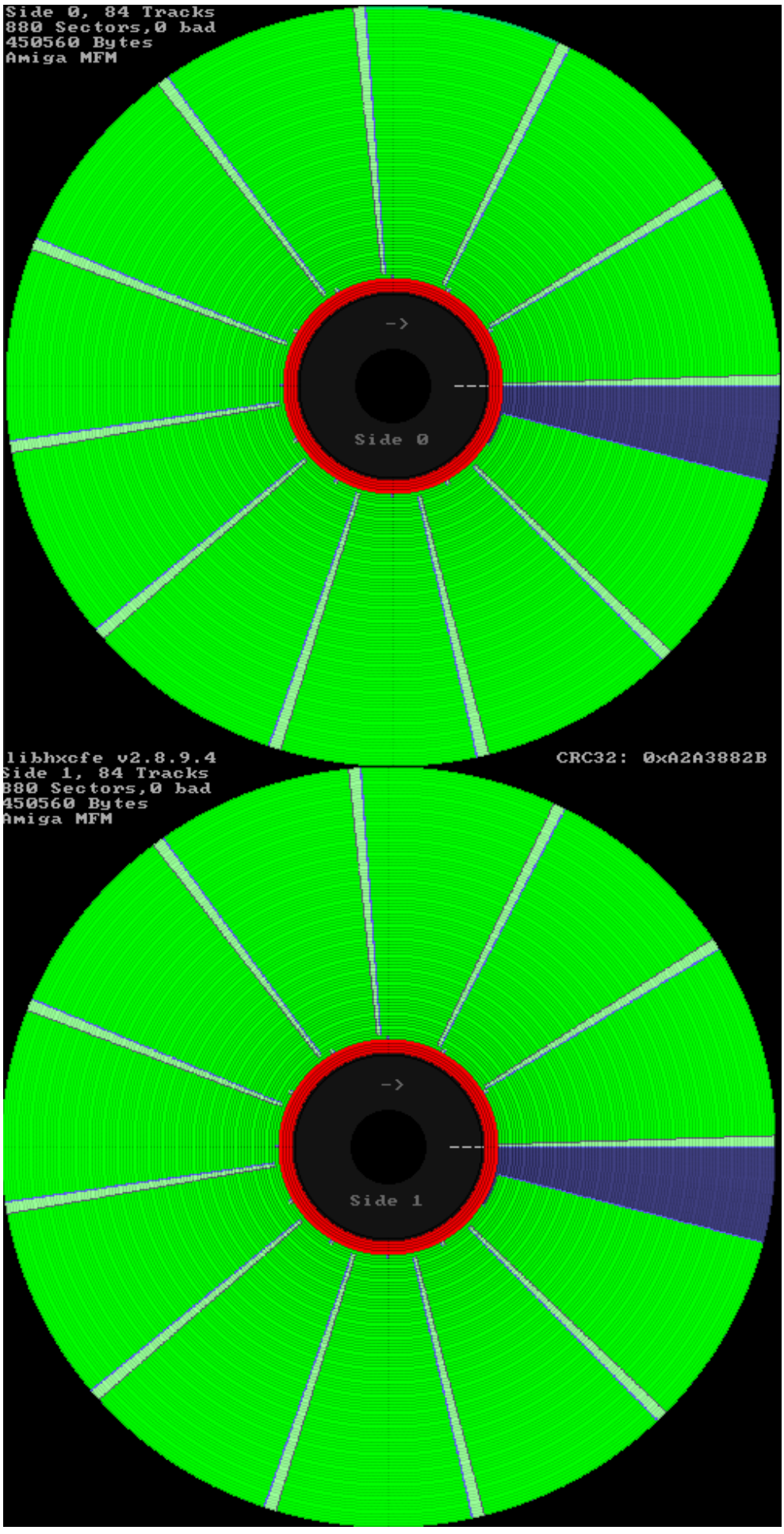
1) Un AMiGA avec 512K ou l'émulateur WINUAE
2) Une Carte ACTION REPLAY MKIII (ou ça ROM Image)
3) Une version de Xcopy Pro (image ou disquette)
4) Le jeu Original BIO CHALLENGE ou son image CAPS (SPS 1734)

General Info

Ce tutoriel Français est basé sur le tutorial original de Rob.
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.

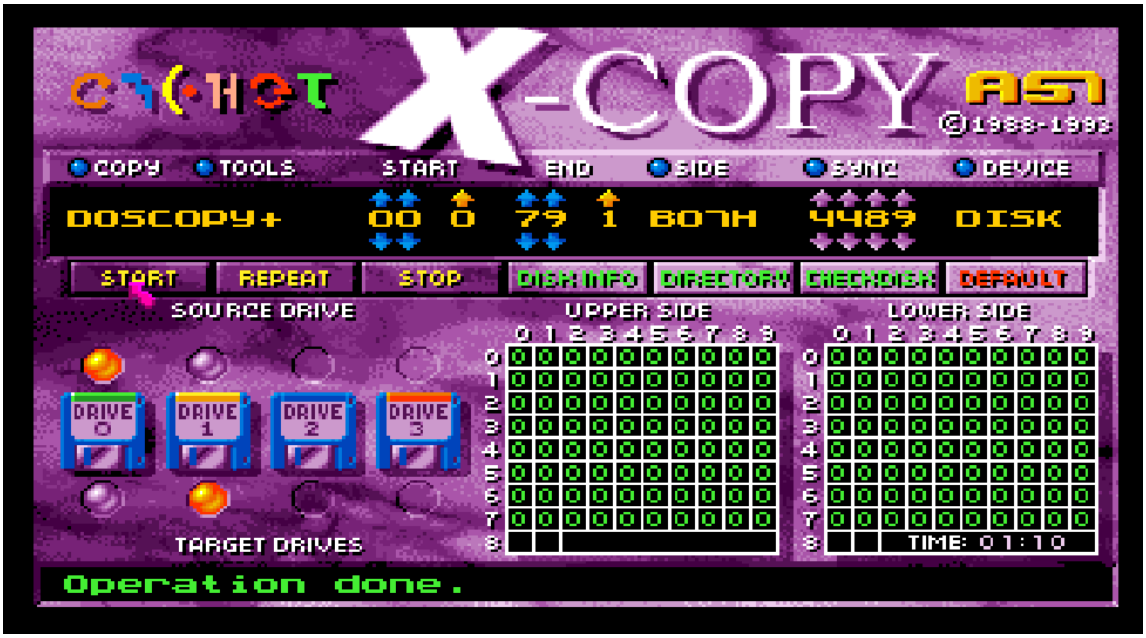
Bon tuto.

Gi@nts


Side 0, 84 Tracks
880 Sectors,0 bad
450560 Bytes
Amiga MFM
->
Side 0
libhxcfe v2.8.9.4
Side 1, 84 Tracks
880 Sectors,0 bad
450560 Bytes
Amiga MFM
CRC32: 0xA2A3882B
->
Side 1

Au travail

Comme dans Tous bon hack qui se respecte, on va commencer par essayer de copier le disk original.
À l'aide de X-Copy Pro, effectuer une copie de la disquette originale en mode **DOSCOPY+**



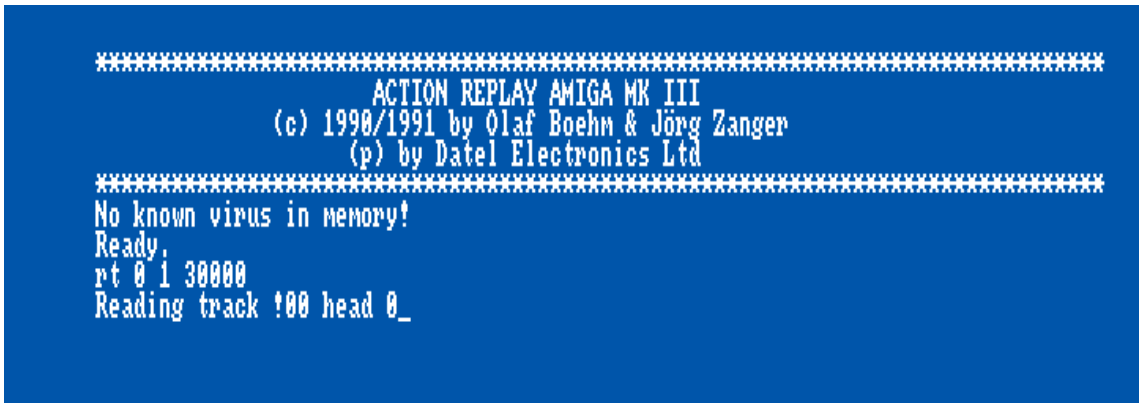
A première vue, pas de système de protection spécifique...

Rebooter votre amiga avec cette copie insérée dans le lecteur DF0 et booter dessus.
Assez rapidement, l'Amiga Crash.

Commençons donc par charger la première piste dans la mémoire pour voir ce qui se passe.

#RT alias Read Track, permet le chargement de la track 0 à 1 (1ère piste de la face 0)
#M, alias Visualisation mémoire HEXA/ASCII

Entrer dans votre AR et tapez le texte suivant : `rt 0 1 30000`

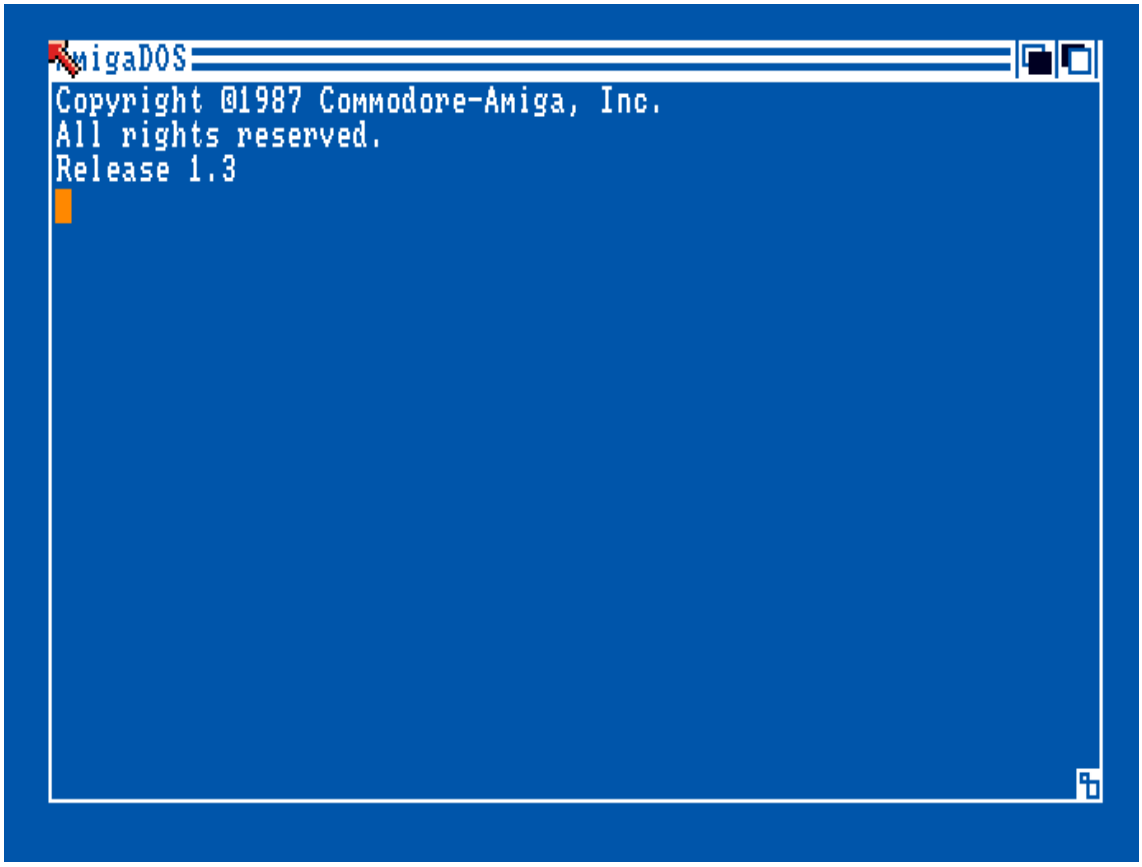


Taper : `m 30000`

```
m 30000
:030000 44 4F 53 00 4C CA C7 2D 00 00 03 70 48 E7 C0 E0 DOS.L..-...pH...
:030010 2C 78 00 04 4E AE FF 7C 41 FA FF E6 2F 48 00 08 ,x..N..|A.../H..
:030020 2F 7C 00 06 00 00 00 10 22 6F 00 0C 20 2F 00 10 /|......"o.. /..
:030030 23 40 00 28 23 7C 00 00 12 00 00 24 23 7C 00 00 #@.(#|.....$#|..
:030040 04 00 00 2C 33 7C 00 02 00 1C 2C 78 00 04 4E AE ...,3|....,x..N.
:030050 FE 38 22 6F 00 0C 10 29 00 1F 66 D0 4C DF 03 03 .8"o...)..f.LB..
:030060 4E 75 50 72 6F 74 65 63 74 69 6F 6E 20 28 43 29 NuProtection (C)
:030070 43 6F 70 79 72 69 67 68 74 20 31 39 38 39 20 52 Copyright 1989 R
:030080 6F 62 20 4E 6F 72 74 68 65 6E 20 43 6F 6D 70 75 ob Northen Compu
:030090 74 69 6E 67 2E 20 41 6C 6C 20 52 69 67 68 74 73 ting. All Rights
:0300A0 20 52 65 73 65 72 76 65 64 2E 00 00 00 00 00 00  Reserved.......
:0300B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
:0300C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
-
```

Comme le montre clairement l'image ci-dessus, la 1er piste est standard avec un *header* '**DOS**'
On peut aussi voire assez clairement des informations ascii qui nous laissent penser qu'il s'agit d'une protection **RNC copylock**

Réinsérer la disquette **originale** du **jeu** et **booter** dessus.
Après quelques instants on peut voir un **CLI** ainsi que le workbench apparaître suivi du chargement du jeu.
Nous allons nous servir de cette '*petite faille*' *'boot cli'* pour passer la protection très simplement.



Réi**nsérez** votre **copie** préalablement effectuée dans le lecteur de l'amiga, **entrer** dans votre **AR**
#INSTALL, alias BOOTBLOCK INSTALL, permet d'installer un secteur de boot sur l'unité indiquée, 0=DF0, 1=DF1
et **Tapez :** `INSTALL 0`

```
******************************************************************************
                    ACTION REPLAY AMIGA MK III
              (c) 1990/1991 by Olaf Boehm & Jörg Zanger
                    (p) by Datel Electronics Ltd
******************************************************************************
No known virus in memory!
Ready.
install 0
Ready to install disk in drive df0:? (y/n)
y
Disk ok
```

Rebooter votre Amiga, **tester** le jeu.