

Les Protections sur Atari ST/AMIGA

Vous savez tout comme moi que nos chères disquettes adorées ST/Amiga ont été dotées par les programmeurs voir les **dupliqueurs** de formats empêchant la copie de ces dernières. Nous allons voir en détail de quelle manière elles se présentent.

Premier détail technique, il faut savoir que l'Amiga dispose d'un contrôleur de disquette complètement programmable. On peut en effet lui faire lire les format **AmigaDOS** classiques en 880ko par disquettes, mais aussi les formats Atari ST, PC 720ko, Macintosh GCR (Group Code recorded : enregistrement des données groupées). Pour ce dernier il n'existe qu' 1 ou 2 jeux qui exploitent ce format très spécial.

On va aller progressivement dans la force des protections avec exemple à l'appui.

DLFRSILVER

SOMMAIRE:

I) INTRODUCTION

II) LES PROTECTIONS OFF-DISK ou PAR MANUEL/CODES

III) LES PROTECTIONS SOFTWARE

A) LE SYSTEME COPYLOCKS

- A.1) *LE SYSTEME COPYLOCK DIT « INTERNE »*
- A.2) *LE SYSTEME COPYLOCK DIT « EXTERNE »*
- A.3) *LE SYSTEME RNPDOS*

B) LE SYSTEME SPEEDLOCK

C) LE SYSTEME PROTEC

D) LE SYSTEME STARTER/PISTE LONGUE

E) LE SYSTEME LONGTRACK D'UBI SOFT

F) LE SYSTEME MFM

- F.1) *MFM DISK STANDARD*
- F.2) *MFM DISK ETENDUES AVEC DEPASSEMENT DE CAPACITE*
- F.3) *MFM CUSTOM*
 - F.3.1) *AVEC SUPER DEPASSEMENT DE CAPACITE CHEZ PSYGNOSIS SUR AMIGA*
 - F.3.2) *PAR READTRACK SUR ATARI ST MADE IN LANKHOR*
- F.4) *MFM HYBRIDES*

G) LE SYSTEME DUAL FORMAT

H) LE SYSTEME « FLAKEY BITS »

I) LE SYSTEME CUSTOM MULTIPLE

IV) LES PROTECTIONS HARDWARE ou DONGLE

V) CONCLUSION

VI) GLOSSAIRE

LES PROTECTIONS OFF-DISK OU PAR MANUEL/CODES

Les protections Off-disk ou manuel/codes sont en générale appliquées sur les jeux d'aventure, car ceux-ci sont installables la plupart du temps sur disque dur, et sont bien souvent en format **AmigaDOS** standard 880ko.

Cela concerne des jeux comme **Explora I**, **Secret of Monkey Island I et II**, **Indiana Jones and the Fate of Atlantis**, la série des **Elvira** d' Horrorsoft. Tout ceux-là sont installables et n'ont aucune protection disque.

Cependant il faut noter que certains jeux cumulent les protections. Si on prend les jeux Silmarils, ceux-ci dans leur versions européenne disposent d'une protection Off-disk qui non seulement s'active 1 voir 2 fois en cours de jeu, ce qui fait que les pirates en ont loupés au déplombage plus d'une, mais aussi d'une protection disk nommée "Protection par piste longue" appelée LONGTRACK. Celle-ci sera détaillée plus bas dans la partie dédiée aux protections disks.

Les protections par codes concernent des jeux comme ceux de Coktel Vision, qui étaient fournis avec des grilles codées. Comme pour la protection par manuel, au bout de plusieurs essais ratés, le jeu plante ou bien certains registres processeurs sont vidés ou bien le programme pointe vers un endroit qui n'engendre aucun traitement (espace mémoire vide de toute données), et donc le programme reste inerte.

LES PROTECTIONS SOFTWARE

A) LE SYSTEME COPYLOCKS

Vous connaissez tous des jeux sur ST ou bien Amiga qui n'ont pas l'air comme ça, le jeu s'amorce gentiment, le lecteur de disquette ne fait pas un bruit de dingue, l'ordinateur marque une pause, puis continue de charger le jeu. Elle a été créée en 1987 sur Atari ST, et apposée dans le jeu **R-type** d'Activision.

C'est la plus connue des protections disponible sur le marché à l'époque. Elle est elle-même subdivisée en plusieurs versions que je vais vous détailler. Elle a été créée par un anglais nommé Rob Northen. La protection porte l'acronyme de RNC Copylock © Rob Northen Computing 19XX que l'on retrouve dans la majorité des jeux qu'elle protège.



Rob Northen, créateur du Copylock

C'est le cerveau qui a créé cette protection et qui l'a mise en service sur 500 jeux Amiga et ST. La protection n'est pas copiable avec un Amiga ou un ST standard, fait appel à un mot de synchro non standard. ex sur Amiga le mot utilisé pour lire une piste DOS standard est \$4489. Sur une piste copylock, il est de \$8912 XXXX XXXX. Cette valeur a changée suivant les versions. Quand la piste copylock est testée, elle renvoie une clé numéro de série codée sur 32 bits, qui est après injectée dans les registres du 68000 pour être incluse dans le programme, pour soit activer une fonction, détruire des portions de programme en mémoire, voir décrypter une partie de programme dans un jeu, ou bien même décrypter un bootblock.

A l'époque il utilisait une machine de duplication « TRACE » tournant sous Unix qui pouvait écrire les format de protection copylock tel qu'il les avait écrit via un script.

A.1) LE SYSTEME COPYLOCK DIT « INTERNE »

*** La première version se présente comme ceci :

La piste 0 est anormale. Toutes les pistes de 1 à 79 sont dites **AmigaDOS** standard ou bien Atari ST DOS standard. Un des secteurs est d'une taille plus faible que les autres, et non recopiable. La routine de test vérifie que le temps d'accès est de X msec. Si le chiffre est X+ 5 msec, alors c'est une copie.

Ceci est le type n°1 des copylocks, le plus facile à exterminer.

En interne le copylock Amiga se présente de la manière suivante :

Le programme est systématiquement basculé en mode superviseur, ce qui veut dire qu'on prend le contrôle intégral du hardware de la machine, et que les instructions dites 'ILLEGAL' du 68000 sont utilisables. Le copylock est une routine rajoutée dans un programme, bien souvent encryptée, et en son milieu on trouve l'instruction privilégiée 'ILLEGAL' d'où le besoin que le programme soit mis en mode superviseur.

Son implémentation la plus basique, ultra facile à virer a été implementée sur les jeux suivants : **Stormlord**, **Astaroth**, **Robocop** pour ne citer que ceux-là.

Le **bootsecteur/loader** de ces jeux était en fait encrypté et caché par le système copylock.

L'opération est simple, à l'aide d'un original, et d'une cartouche telle qu'une action replay 3, on laisse le programme décrypter le vrai bootsecteur, qui lui-même est copié en mémoire et copié en \$400 dans la RAM chip de l'Amiga là où on est censé le trouver normalement à la place de celui du copylock. On a juste à recopier le bootsecteur sur la copie au bon endroit et le tour est joué. Si la protection échoue, le bootblock n'est pas décrypté et l'Amiga reste bloquer ou bien fait un reset après le test de la piste.



Screen tiré de X-copy qui montre les pistes de Stormlord

*** Par la suite, le copylock a évolué, car cette première version a été vaincue par le premier venu en 2 minutes chrono.

Rick Dangerous me vient à l'esprit, il date de 1989 et utilise toujours un copylock en piste 0. Cette fois-ci, le numéro de série de la piste copylock sert à décrypter le programme principal. Si on utilise une copie, le programme n'est pas décrypté et boom, plantage de la machine et reset.

C'est cette version de copylock qui sera la plus répandue de toute. Les jeux qui l'ont utilisée sont nombreux, citons par exemple : **Powerdrift**, **Badlands**, **Licence to kill**, etc....

*** La troisième version commence à devenir plus méchante. On a toujours notre piste 0 plombée comme à l'accoutumée, mais cette fois-ci on a pas 1 routine copylock d'incorporée au programme, mais au moins 3 si ce n'est plus. Un jeu comme **Frenetic** de Core Design en a 3 ou 4 qui font une vérification disk et qui en plus décryptent le programme.

Sleepwalker d' Ocean est l'exemple même d'un jeu protégé par copylock mal déplombé, le numéro de série d'une des versions craquées disponibles à l'époque avaient été mal câblé dans le programme. Résultat, une routine bien planquée faisait disparaître le tonneau dans les égouts du niveau 1 vous bloquant ainsi de manière impossible à contourner.

Des jeux comme **Hook** d' Ocean, **Darkman** sont littéralement criblés par la protection copylock. Les routines copylock sont ici encryptées, exécutent du code en mémoire, remplacent des instructions dans le jeu, et sont en plus protégées par checksum !!! (**Hook** n'a d'ailleurs jamais été craqué proprement jusqu'à il y a peu). on peut trouver facilement plus de 20 checksums qui le protègent, en mémoire et sur disk de toute modifications.

Mais le best of the best, c'est le jeu **Parasol Stars** d' Ocean. Vous connaissez ce jeu qui est une adaptation directe de la version PC-Engine, il tient sur une seule disquette et pourtant, la protection mise sur ce jeu est un poème à lui tout seul. imaginez un peu : Le jeu est au format DOS. doté d'une piste 0 protégée par copylock.

ont tous des images de 128x64 pixels, et les données sont protégées par des copylocks, dotés de 3 routines copylocks vérifiées un nombre incalculable de fois lors du déroulement du jeu, mais surtout il est truffé de checksums ! Il y en a 20 en tout, et le jeu est intégralement encrypté, et les fichiers du jeu sont codés et engoncés dans une surcouche codée en langage objet !

Résultat, pour un jeu qui faisait une fois la programmation terminée 300ko, on se retrouve avec un jeu qui fait une fois la protection appliquée 650ko. La protection fait donc à elle toute seule 350 ko ! Jamais on a vu telle chose sur un jeu et pourtant il y en a d'autres qui sont aussi très bien pourvu, j'en parlerais plus loin. La version Atari ST c'est même tarif même punition.

A.2) LE SYSTEME COPYLOCK DIT « EXTERNE »

Là ça commence à devenir intéressant, ici la protection est beaucoup plus complexe à contourner. Fini le système de pistes DOS là on est face à un système de pistes protégées MFM + des routines copylocks dans le programme qui testent la piste 0. Les pistes 1 à 79 voir 1 à 81 sont protégées par un mot de synchronisation différent ce qui rend les pistes incopiables. De plus, le format MFM débouche ici sur une surcapacité du stockage des données.

Quelques exemples : **R-type** Amiga, **Rainbow Islands**, **New Zealand Story** sur Atari ST



Voici le tableau des pistes sous X-copy. La piste 0 contient le copylock et les piste 1 à 79 contiennent la protection MFM RNC Standard. Les 5 rouges correspondent à une protection MFM Standard.

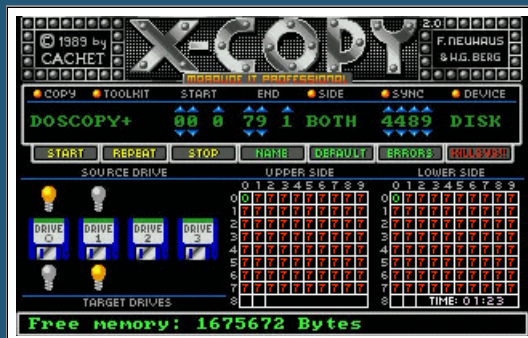
Pour sortir le programme de sa coque, il faut ripper, en utilisant le loader ou les loaders du jeu, toutes les données du disque, récupérer le numéro de série de la piste copylockée, le « cabler » dans les données rippées, et créer un chargeur de pistes hardware, connu sous le nom de trackloader.

Ce système marche de la façon suivante : Les pistes font \$1600 de données chacune, il faut en charger tant de kilo-octets à tel endroit en mémoire. Les pistes RNC external étendues font \$1800 au lieu des \$1600 que l'on a sur une disquette au format AmigaDOS. \$1600 de données par coté soit \$3200 de données pour une piste sur une disquette double face.

A.3) LE SYSTEME RNPDOS

On touche au fin du fin, le top du top. Mais ça ne s'appelle plus copylock, mais Rob Northen ProtectedDOS. Le système RNPDOS utilise un dépassement de capacité des disquettes, on passe de 880ko par disk à 970ko, mais la vraie particularité est le fonctionnement et le décodage des pistes.

Les jeux qui utilisent ce système sont **Alien breed - Tower Assault** de Team 17, **Superfrog**, **Body Blows** de team 17, **Primal Rage** de Warner interactive, **Mortal Kombat I et II** d'Acclaim, mais aussi **Jurassic Park** d'Ocean. Cette protection n'existe pas sur Atari ST.



Voici le tableau X-copy de **Superfrog**. Chaque piste est encryptée et verrouillée par un numéro de série qui marche sur le principe du copylock classique.

Non seulement une copie ne marchera pas, mais en plus les données ne peuvent pas être décodées et elles restent verrouillées.

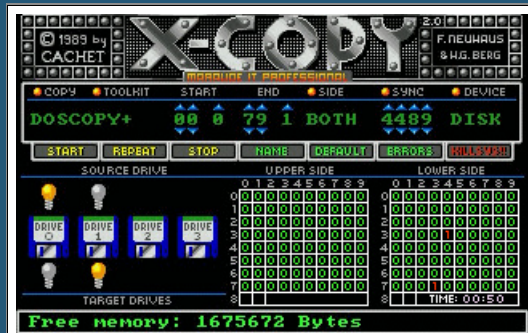
Superfrog tient dans sa version craquée sur 4 disquettes au lieu de 3 à cause du dépassement de taille. Et les fichiers de ce jeu sont compressés avec un outil fourni par Rob, le compresseur RNC propack, qui permet un taux de compression phénoménal. **Alien breed - Tower Assault** tient sur 3 disquettes, mais si on rippe tous les fichiers stockés sur les

pistes une fois décodées, (car le jeu est installable sur disque dur) et qu'on les décompresse avec l'utilitaire track2file, le jeu fait 19 mo !! c'est tout bonnement énorme.

Quand à **Jurassic Park**, aucune des version pirates n'est craquée correctement, ni même fonctionnelle. Le jeu est protégée par RNPDOS + criblé de checksum en mémoire (50 au moins) + dépassement de capacité disk + routine copylock reliée au ennemis (ex : certains dinos sont invincibles dans le crack de Paradox, c'est un effet secondaire d'une protection qui a mal été craqué) ainsi que le système de mot de passe, qui est complètement inopérant sur la version craquée.

B) LE SYSTEME SPEEDLOCK

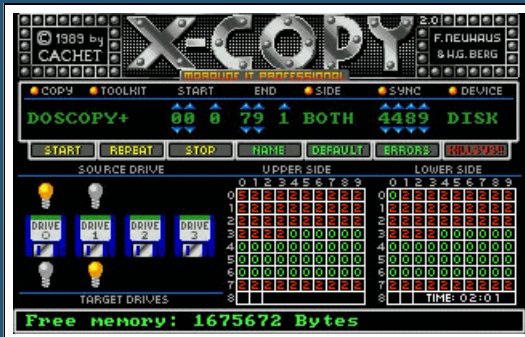
Le système speedlock est excessivement bizarre, car utilisée sur peu de jeu. Les quatre que je connais sont **Voodoo Nightmare**, **Dragon's Breath** de Palace Software et **ATF 2** de Digital integration ainsi que **Treasure Trap** d' Electronic zoo.



Voodoo Nightmare est en pistes DOS, mais bizarrement il y a 2 pistes protégées contre la copie en plein milieu de la disquette, et pas sur la même piste par face. Regardez le screenshot ci-contre pour vous faire une idée.

Cette protection marche par détection de la densité des données sur les pistes protégées (marchent au timing lors de la lecture). D'où le nom speedlock, qui veut dire blocage par la vitesse.

L'encryptage tient ici une place de choix.

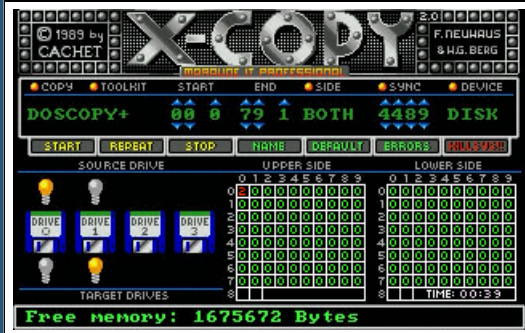


ATF 2 lui est protégé par speedlock, mais utilise des pistes protégées MFM, et un dépassement de capacité. Une fois le jeu installé sous whdload, l'image décodée de la disquette fait 982ko soit 102ko de données supplémentaires.

Comme on le voit, c'est un speedlock exotique avec des pistes MFM et des pistes DOS standard.

Le speedlock de **Treasure Trap** lui ressemble à un copylock dans son fonctionnement. Si le test de la protection échoue, le chargement est bloqué.

C) LE SYSTEME PROTEC



On trouve ce système de protection sur les jeux **Gemini Wings**, **Sorcery +** de Virgin Mastertronic.

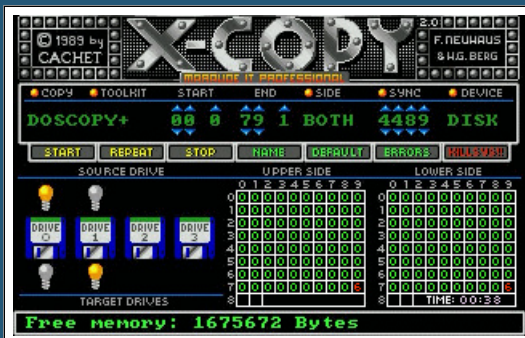
Celle de **Gemini Wings** ci-dessous :

Elle est appliquée sur ces jeux qui sont en fichiers et pas en chargement de pistes. Elle est logée dans le programme principal et teste simplement la valeur hexa retournée par le test de la piste protégée, (qui est la piste 0) dans le registre de donnée D0 du 68000.

La encore, une protection très facile à contourner, plus simple que le copylock de base.

D) LE SYSTEME STARTER/PISTE LONGUE

C'est la protection disk utilisée sur les jeux **Silmarils**, **Targhan**, la série des **Ishar I, II, III**, **Transarctica**, **Storm master**, **le Fetiche Maya**, **Colorado**, etc.... Mais également les jeux Loriciel comme **Tennis Cup**, **ADS**, **Panza kick boxing**, etc.... Cette protection aurait été conçu chez Loriciel par ailleurs. (Titus est aussi un grand consommateur de ce type de protection. Les jeux **Moktar**, **Prehistorik**, **Crazy Cars 3**, **Super Cauldron** utilisent des pistes longues en guise de protection.)



Voici la typo sous X-copy d'une jeu protégé par STARTER. C'est une protection par piste longue qu'on appelle « longtrack ». Elle consiste en une piste dotée d'une foule de secteur d'une taille plus petite que la normale, mais la piste en elle-même fait une taille super longue, \$19 E0 au lieu des \$1600 sur une piste normale. C'est la piste 79 qui est ici utilisée pour cette protection.

La lecture de la piste renvoie une clé sous la forme d'un nombre hexadécimal qui est mis d'abord dans le registre de donnée D6 et qui est ensuite copié dans D0 une fois celui-ci mis à 0. Si le mauvais nombre est remonté dans le cas d'une copie, le jeu plante.

Et voici la routine de protection telle qu'elle se présente sur les versions Amiga des jeux **Silmarils** :

Ici comme vous le voyez, la ligne assembleur C0A2AE exécute la routine de protection, envoie la tête de lecture sur la piste 79, procède au calcul qui va bien, renvoie le nombre hexadécimal 152B dans le registre d6. Cette clé varie suivant les jeux.

```

=====
^C0A2AE MOVEA.L #BFD100,A5
^C0A2B4 MOVE.L A0,00C0AE26
^C0A2BA BSR 00C0A2D8
^C0A2BE BSR 00C0A33E
^C0A2C2 BSR 00C0A374
^C0A2C6 BSR 00C0A3F4
^C0A2CA BSR 00C0A462
^C0A2CE BSR 00C0A4B4
^C0A2D2 CLR.L D0
^C0A2D4 MOVE.W D6,D0
^C0A2D6 RTS
=====

```

```

r
D0=00000000 00000000 0000FFFF 0000FFFF 00000001 0000048F 0000152B 00C05184
A0=0001F6CA 00C17FDC 00C04DB8 00C077D4 00C0AE0A 00BFD100 00DFF000 00C00000
PC = 00C0A2D4 USP = 00C1855C SR = 0004 T=0 S=0 I=000 X=0 N=0 Z=1 V=0 C=0

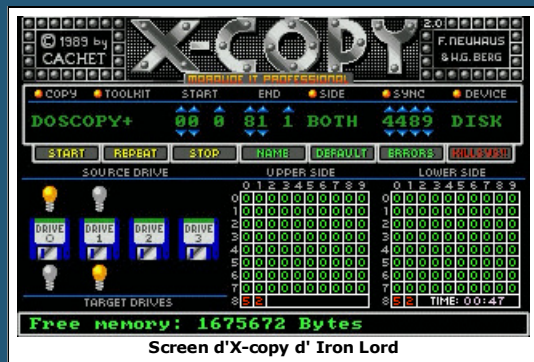
```

Vous voyez ici le tableau d'état des registres du 68000 de l'Amiga, La ligne assembleur C0A2D2 demande le vidage du registre D0, et la ligne C0A2D4 demande la copie du WORD (mot) stocké en D6 dans D0. Sur cet exemple la bonne clé c'est 152B pour **Ishar 3 ECS** de la compilation **Ishar Trilogy**. Sur une copie, le registre D6 passe une mauvaise valeur de D6 vers D0. Le programme plante après l'introduction.

Même si la routine varie un peu suivant les jeux, ce système est récurrent. D'ailleurs **Ishar 3 ECS** ne marche pas sur A1200 à cause de la protection. Une fois celle-ci oblitérée, le jeu passe sans souci.

Pour cabler le bon nombre, on efface les lignes C0a2ba à C0a2ce et on mets MOVE.W #152B, D6 et après move.W D6,D0 . On modifie et on sauvegarde le programme « start ». On relance le jeu et celui n'essaie même pas d'aller en piste 79, il charge directement le menu principal.

E) LE SYSTEME LONGTRACK D'UBI SOFT



Ubi Soft a utilisé cette protection sur **Iron Lord** et **Final command**, ainsi que **Zombi**.

C'est une protection par piste longue placée en pistes 80 à 82. Les données sur ces pistes sont agencées de façon particulières, qui font qu'elles ne sont pas copiables.

Là encore, seul un système de copie hardware peut copier ce type de protection.

F) LE SYSTEME MFM

F.1) MFM DISK STANDARD

Des jeux comme **Twinworld** de Blue Byte, **Smash TV** d' Ocean, utilisent une protection MFM classique (forme d'encodage dont les infos de décodage sont dans le trackloader, toutes les pistes sont encodées en MFM) sans fioriture ni bizarreries.

Un simple changement de mot de synchro caractérise le format utilisé pour ces jeux là.

F.2) MFM DISK ETENDUES AVEC DEPASSEMENT DE CAPACITE

C'est pareil que par protection MFM standard, sauf qu'ici on a droit à une méchante surcapacité en plus sur disk.

Turrican I, II, III, BC Kid, Snow Bros, Dragon's Lair I, II, III, Space Ace 1 et 2, Wrath of the Demon, Awesome de Psygnosis pour ne citer qu'eux font partie de cette catégorie.

Turrican Amiga ne peut pas être copié pour 2 raisons, la première c'est que le jeu fait décodé 1,1 mo tassé sur une seule disquette et utilise en plus 5 routines copylock engoncées dans les fichiers de jeu. Le format créé par Factor 5 permet de mettre presque 350ko kilo de données de plus sur une disquette classique. **Turrican 2 et 3** sont abonnés au même principe ainsi que **BC Kid**. Tout ces jeux tiennent obligatoirement sur 2 disquettes si on les passe sur des disquettes standardisées.

Les jeux Ready Soft sont quand à eux une exception. Randy Linden le programmeur en chef sur ces jeux a créé un format MFM surpuissant puisque chaque disquette Amiga de ces jeux contient autant de données (notez que ce sont des disquettes double densités) que des disquettes PC HD 1,44mo. On a en moyenne 1,2 mo de données sur chaque disquette de **Dragon's Lair** soit une taille de piste énorme \$1950 de données en lieu et place des \$1600 alloués normalement à un format de piste DOS. Ça explique pourquoi ce jeu qui prend 6 disquettes en original en fait 3 de plus dans sa version craquée. Toutes pleines à rabord en plus. **Wrath of the Demon** lui a 1mo de données décodées par disquettes.

Pour recopier ces jeux protégés, il faudrait utiliser des lecteur Haute densité et des disquettes HD pour stocker toutes les données sans problème. Et utiliser un dispositif de copie matériel... Sans quoi la copie est impossible.

Awsome de Psygnosis dispose d'une intro qui fait 960ko, ce qui fait qu'elle tient aussi sur 2 disquettes si on la met sur des disquettes classiques.

F.3) MFM CUSTOM

F.3.1) AVEC SUPER DEPASSEMENT DE CAPACITE CHEZ PSYGNOSIS SUR AMIGA

Ici on tape dans l'irréel. Peu de personnes connaissent la spécificité de cette protection créée par Psygnosis. On l'appelle le format MFM Psygnosis 1.5. Pourquoi ? hé bien voilà cette protection n'est absolument pas copiable car elle permet une telle augmentation de la taille des données stockée que ça en est ahurissant. Chaque disquette contient au moins 1,2 mo de données décodées soit 2,5 mo de données MFM brutes. Il y a 4 jeux concernés : **Nitro, the Killing Game Show, Obitus, Armour Geddon**.

Le pire, c'est que le bootsecteur lui-même est encrypté, et utilise une routine qui ne permet pas de voir les octets décodés.

Le stockage est 30% plus important qu'une disquette protégée par système MFM classique. A ce jour **Obitus** n'a jamais été craqué correctement, la version crackée a été bâclée. Quand on cherche à copier **Obitus** dans X-copy, on voit des 7 rouges qui sont le signe de piste longues.

F.3.2) PAR READTRACK SUR ATARI ST MADE IN LANKHOR

Pourquoi **Maupiti Island** sur ST n'a t'il jamais été craqué proprement ? Parce que le jeu contient des routines de contrôle checksum en mémoire, et aussi un système très particulier pour la lecture des pistes. En effet, quand l'Amiga fait très bien du readtrack, l'Atari st en temps normal ne sait pas faire ça. Tout du moins pour faire de la lecture de données. Les gars de chez Lankhor ont réussi à détourner les routines système pour faire faire du readtrack à l'Atari. Les pirates en ont bavé pour remettre les données sur des pistes standard, hélas les copies craquées disponible ne sont pas propres, le jeu n'aura jamais été craqué correctement.

F.4) MFM HYBRIDES

Voici la partie exotique de notre dossier héhé :D, je vais faire allusion aux jeux éducatifs de Coktel vision nommés ADI.

Qui n'a jamais utilisé pour ses enfants cette suite applicative éducative ?

Hé bien voilà une grosse particularité de l'Amiga, tandis que la disquette de lancement ADI est au format Amiga DOS, le programme principal est doté de routines spéciales permettant le décodage des disquettes application fournies qui elles sont au format MFM Atari ST/PC 720ko.

Ces pistes font une taille de \$1400 de données au lieu des \$1600 que l'on a normalement.

Ces disquettes sont lisibles sur ST et PC et donc copiable sur ces machines, mais sur Amiga, elles sont considérées comme protégées et donc pas copiable. L'Amiga sait néanmoins les lire et les décoder.

La bonne solution pour faire des copies de sauvegarde, c'est de se servir d'un PC ou ST pour créer des backup et les charger ensuite sur son Amiga.

Parmi les jeux connus protégés par pistes Atari ST sur Amiga il y a la plupart des jeux de Dinamic (**Satan, Astro Marine Corps, Narco police**) certains jeux de chez Thalion (**Wings of Death, Prehistoric Tale** par ex), **Ninja Remix** d' Eclipse, **Plan 9 from Outer space, James Pond** de Millenium, **Karaté Kid, Fire and Brimstone, Goldrunner, Starglider**, etc.....

Il y en a de sources sûres à ce jour 80 jeux référencés. Ils ne sont d'ailleurs toujours pas préservés par SPS, mais devraient bientôt sortir au format IPF.

G) LES PROTECTIONS DITES DUAL FORMAT

Ceci est une invention d'un des meilleurs de chez Thalion, j'ai nommé notre cher Jochen Hippel.

C'est lui qui a créé le système dual format. En fait, ce système a été utilisé sur les jeux **Lethal Xcess** de Thalion, **Monster Business**.

Le jeu se lance indifféremment que l'on insère les disquettes sur un ST ou un Amiga.

La piste de démarrage est spéciale, elle contient sur une face le bootsecteur Atari, et sur l'autre le bootsecteur Amiga. Suivant la machine sur laquelle on insère la disquette, hop le boot correspondant à la machine est chargé et décode par la suite les pistes protégées MFM de 1 à 79.

J'en profite également pour dire que la plupart des protections disque sur Atari ST des jeux Thalion ont été créées sur Amiga, d'après des informations que l'on a eu par les gens de Thalion eux-mêmes.... Si c'est pas amusant ;)

H) LES PROTECTIONS DITES PAR « FLAKEY BITS »

Ce type de protection est assez particulière. En fait, sur une disquette, on peut formater ou non les pistes que l'on veut. Certaines sont non formatées, et donc contiennent ce que l'on appelle du « bruit » . Ce n'est pas du vide, mais plutôt un état aléatoire permanent des bits 0 ou 1.

Je m'explique, sur un jeu original doté de cette protection, quand le jeu ordonne la lecture d'une piste dotée de « flakey bits », la lecture renvoie soit 0 soit 1 en résultat, tandis qu'une copie de cette disquette renverra de façon permanente 0 ou bien 1.

Ça donne ceci :

01010101010101010 (original)
00000000000000000 (copie cas 1)
11111111111111111 (copie cas 2).

Cette protection ne peut être recopiée même avec un hardware de type cyclone. Elle ne se copie qu'industriellement via une **machine traceuse** (duplicateur).

Les jeux **Super Hang-On, Fatal Heritage**, utilisent cette protection.

I) LES PROTECTIONS CUSTOM MULTIPLE

L'exemple absolu, c'est le jeu **Double Dragon 2** converti par Richard Aplin.

Voici la liste détaillée des systèmes de protection mis en place

Par Richard Aplin le programmeur :

- 66 x fichiers du jeu encryptés
- 66 x routines de vérification de la protection encryptée dans chaque fichier
- 4 x loaders (encryptés/non-encryptés) dans le fichier principal
- 13 x Routines d'accès au loader (activées par des erreurs d'adresses!)
- 3 x Checksums (test et dépôt de données sur la pile)
- 1 x loader dans le jeu qui décrypte quand il est appelé, puis se ré-encrypte lui-même après coup!
- 1 x système de fichier MFM avec des blocs de données de \$1800 bizarre
- 1 x piste de protection testée plus de fois que Ben Johnson
- 1 x bootsecteur encrypté
- 235 x erreurs d'adresses,
- 16 x erreur d'adresse dans la copperlist

Comme on peut le voir, la protection est extrêmement lourde, et le crack existant de ce jeu ne peut pas tourner sur autre chose qu'un Amiga 500 de base justement à cause d'elle. La protection regroupe une piste de protection longue + un format MFM lourd + encryption à tout les étages + 1 **bootsecteur** encrypté.

LES PROTECTIONS HARDWARE ou DONGLE

Peu de jeux utilisent ce type de protection, car elles reviennent cher au coût final d'achat du jeu.

Je parle bien sûr de **Robocop 3**, **B.A.T 1** sur Atari ST, **B.A.T 2** sur Amiga/ST, **Dames Grand-Maitre** de Cobra Soft, **Dyna Blaster** d'Ubi Soft, **Jeanne d'arc** sur Atari ST.

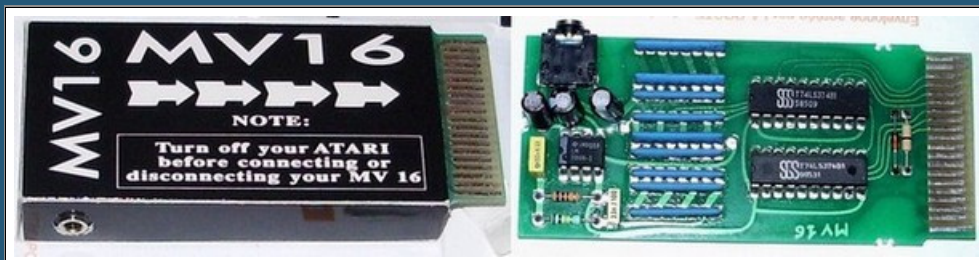
Robocop 3 utilise un dongle s'insérant sur le port joystick. La routine de détection est paraît-il facile à trouver d'après ce qu'en dit Galahad du groupe FAIRLIGHT. Il a été déjoué au moment même de sa sortie, ça a été donc inutile ici d'implémenter ce système.

Photo du dongle :



B.A.T 1 sur Atari ST utilise une cartouche que j'appelle « dérivative » c'est-à-dire que le son est rerouté vers la carte en étant censé l'améliorer (dans la pratique, l'amélioration est imperceptible). La carte MV16 est une arnaque absolue, le son grésille toujours autant, et empêche une émulation convenable sur un émulateur. D'ailleurs la version Amiga n'en a pas et utilise à la place une protection MFM standard avec dépassement de capacité. Le disk 1 du jeu contient 1,1 mo de données décodées au lieu de 880ko en DOS standard.

Photo de la carte MV16 :



B.A.T 2 utilise aussi un dongle à brancher sur le port modem sur ST et sur port série sur Amiga. Le jeu est protégé sur disk sur ST et en pistes DOS normales sur Amiga. A noter que **B.A.T 2** en français n'avait jamais été craqué du moins dans sa version française, jusqu'à ce que je patche la disquette 1 et que je retire le check du dongle (qui soit dit en passant consiste à NOPPER une simple instruction, et cela marche sur la VF, la version allemande et anglaise).

Photo du dongle :



Dyna Blaster sur ST, Amiga et PC se joue à 4 joueurs, les joueurs 3 et 4 sur port classique, et les joueurs 1 et 2 sur le dongle branché sur le port parallèle. Si le jeu ne détecte pas le dongle pour le joueur 1 et 2, on ne peut pas jouer.

Photo du dongle :

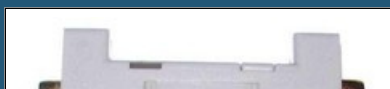




Photo du dongle de Dames Grand-Maitre :



Jeanne d'Arc sur Atari ST utilise aussi un dongle, qui fait planter le jeu si il est absent.

CONCLUSION

Maintenant que ce dossier est terminé, il y a sûrement des questions qui vous traversent l'esprit, telle que quelle aurait pu être la protection la plus efficace, voir leur niveau d'efficacité ?

Je suis d'avis sur une chose, la meilleure protection est celle qui est la plus compatible avec les différents modèles d'une même machine, qui rend la copie très difficile, avec ses talons d'Achille camouflés par de l'encryptage, et, de manière plus vicieuse qu'elle entraîne des modifications une fois activée dans le code du jeu, qu'elle soit protégée même une fois chargée en mémoire par des routines de contrôle de sommes (checksums), ainsi qu'un dépassement systématique de capacité de stockage.

Ce qui me dérange le plus, c'est le fait que les protections de manière générale sont codées de façon « dégueulasse », non respectueuses des règles constructeur. Et je ne parle pas de ces protections activées à grand coup de « division par 0 » qui comme vous le savez est quelque chose d'interdit pour un ordinateur, sauf que l'Amiga, le ST par exemple une fois passé en mode superviseur peut se permettre d'utiliser ce type d'instruction privilégiée. Un autre aspect de protection efficace, consiste à programmer son déclenchement en code C. Le code C est une horreur à craquer pour un pirate, plus que tout le reste. Les protections de **Croisière pour un Cadavre**, **Flashback**, bref, la plupart des jeux codés en langage C sont bien plus dur à craquer qu'un jeu programmé en assembleur, beaucoup plus facile d'accès. Aujourd'hui les protections que l'on connaît sur PC ne sont que les pâles copies des protections d'hier. Aussi stupides, programmées de manière tout aussi « sâles ». La protection Securom que l'on a aujourd'hui fonctionne de la même manière que le système copylock de l'Amiga/ST, Safedisc lui est une aussi pâle copie des protections qui vérifient des secteurs defectueux ou erronés situés sur des pistes non formatées. La protection Starforce 3 est un exemple de la protection qui va trop loin. Je la compare volontiers à la protection de **Double Dragon 2** sur Amiga. Et je t'encrypte à tout berzingue, et que je mets une piste protégée contre la copie, et que je t'enterre au plus profond du code, pour finalement rendre le programme instable.

Au fond rien n'a vraiment changé. Le dépassement de capacité n'aura duré que le temps de quelques jeux comme **Sanitarium** ou **Final Fantasy 8**. On a lâché les disquettes pour le CDrom / DVDrom en gardant les mêmes recettes.

Les protections au final ne font qu'exciter les hackers de tout bord, et agacer prodigieusement les utilisateurs finaux. Mais les éditeurs disent qu'ils ne peuvent pas se permettre de louper les ventes d'un jeu en n'en mettant aucune. Reste que les protections que nous connaissons sur Amiga et ST sont de sacrés morceaux d'ingéniosité pour pouvoir contrer le piratage.

DLFRSILVER

AMIGADOS : *Amiga Disk Operating System*. C' est le système d'exploitation (SE) de l'Amiga comme le fut le MS-DOS sur PC.

BOOTSECTEUR : Premier secteur d'un disque sur lequel se trouve le bootstrap, petit programme exécutable permettant de lancer le programme principal.

CHECKSUM : Somme de tous les bits d'une ligne, d'un message, d'un fichier ... dans le but de détecter une erreur.

DUPLICATEUR PROFESSIONNEL : Machine aussi appelé "TRACER" permettant de dupliquer fidèlement un logiciel à partir d'un master, y compris la protection. Il y avait essentiellement 2 types de duplicateurs qui tournaient sous UNIX.

- Le 1006 : où l'on pouvait connecter 6 chargeurs
 - Le 1020 : où l'on pouvait connecter 20 chargeurs
- Chaque chargeurs pouvait contenir 100 disquettes 3.5" ou 5.25"

PROPACK : Système de compression de données utilisé dans la plupart des jeux.

TRACK LOADER : Routine de chargement de piste. C'est par définition plus rapide pour charger les données qu'un chargement par fichier. Cette routine peut décoder si on le prévoit comme tel des pistes MFM protégées. Elle permet un chargement en volume de donnée en aveugle. Une fois les données mise dans le buffer de décodage MFM, les données décodées sont disponibles, ensuite il suffit de les positionner correctement en RAM et de les exécuter.



Duplicateur professionnel appelé aussi "TRACER"