La Protection des disquettes selon Daniel Duffau (3ème partie)

Utilisation du debugger d'Euphoric pour récupérer l'oeil de Zoltec

Par André C.

Ecran-menu de la disquette CEO-soft 2

Ecran-titre du jeu de Daniel Duffau

Récupération de l'œil de Zoltec

Je passe maintenant au 3e programme proposé sur la disquette CEO-soft 2, parce que j'ai une copie "en clair" de ce jeu, paru sur la disquette trimestrielle de mars 1998. Cela devrait me faciliter la tâche et me permettre d'améliorer mon expérience de la récupération des programmes protégés en utilisant le Dump d'Euphoric. Cette première version, dont le copyright indique 1985, est composée de deux fichiers Basic :

- Un "lanceur" ŒIL.COM qui occupe 15 secteurs de #0501 à #1243.

- Le jeu proprement dit ŒIL.JEU qui occupe 142 secteurs de #0501 à #990B.

Sous Euphoric, je repars de la disquette CEO-soft 2 et choisis l'option 3 (voir écran ci-dessus à gauche).

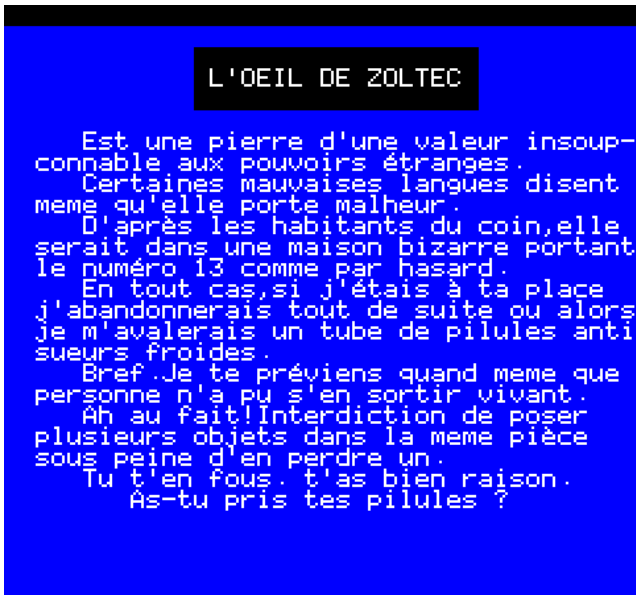
Première surprise le copyright est de 1988, donc c'est une version très postérieure à celle de 1985, probablement encore spécialement adaptée pour la disquette CEO-soft 2 (voir écran ci-dessus à droite).

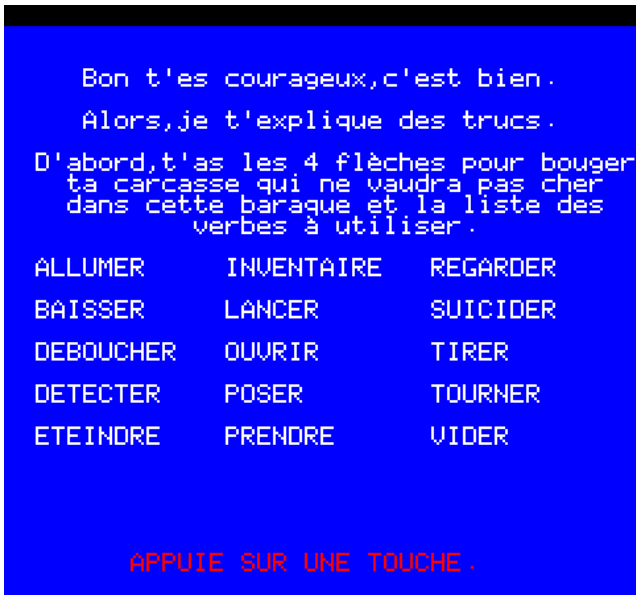
A l'issue des deux écrans d'instructions, je presse F9 (le Dump d'Euphoric) juste avant de répondre à "Appuie sur une touche" (voir les deux écrans, page suivante en haut).

Je passe à l'examen du fichier "Dump". Il y a bien un programme Basic de #0501 à #12AE, donc légèrement plus long que pour l'autre version... Ce programme est suivi par des divagations (un peu n'importe quoi). Je copie les #3502 octets du programme et ajoute par devant un entête K7 adapté. Je sauve le fichier TAP et le teste. Apparemment tout semble OK. Le programme reste en attente de la touche qui va déclencher le chargement de la 2e partie.

Je recommence avec CEO-soft 2, option 3, touche après "Appuie sur une touche", attend patiemment que la 2e partie soit chargée, transcodée, mise en place et enfin appuie sur F9.

Je passe à l'examen du fichier "Dump". Il y a bien un programme Basic à partir de #0501, mais curieusement il y a encore quelque chose après le triple #00. La fin apparente du programme (#8FF3) tombe avant celle de l'autre version (#900B). Je sauve la zone de #0501 à #8FF3 (adresse du triple #00).





Les deux écrans d'instructions avant le début du jeu…

Je refais le manège habituel et récupère ce 2e Basic sur ma disquette de travail et je teste.

Ça commence mal : dès l'appui sur une touche (on est alors à la fin de la 1ère partie et la touche doit lancer la 2e partie), le jeu plante avec un "BREAK ON BYTE #0025 IN 760". Et... la ligne 760 se termine par un CALL#1393. Or ça ne correspond à rien dans le 1er Basic. Je soupçonne l'existence d'un fichier "composite" (Basic+LM) (voir Ceo-Mag n°291, pages 10-12). Et effectivement, dans le 1er fichier "Dump", il y a du code en #1393 (alors que la 1ère partie était censée se terminer en #12AE). Je jette un coup d'œil sur le code en #1393. Zut ! c'est encore bien compliqué !

le programme en place à partir de #0501 et lancer l'exécution. Ma disquette de travail n'a pas ces données et plouf ça plante !

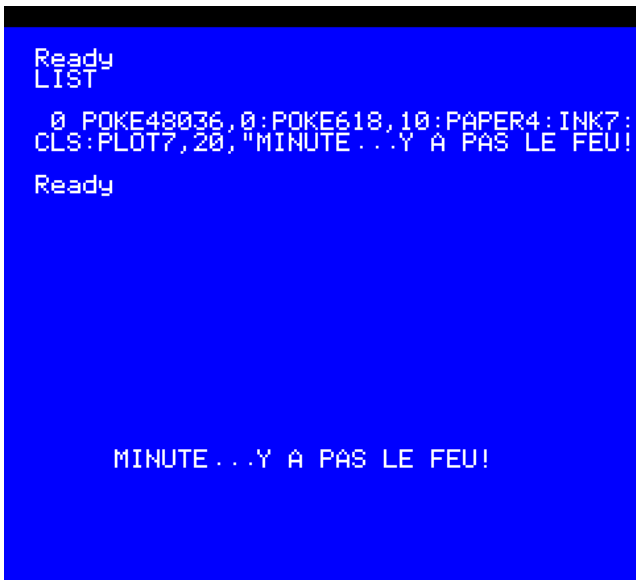
Je ne vois que 2 solutions:
- Décoder le système, mais ça débouche sur des complications importantes.
- Remplacer le CALL#1393 par un bête !LOAD"ŒIL.JEU" comme sur la disquette trimestrielle de mars 1989 (version de 1985 non protégée).

Je fais la modification et teste. Cette fois le 2e programme Basic se lance, affiche le message pour patienter pendant le chargement: "MINUTE… Y A PAS LE FEU !" et bing, il s'arrête net !

Je fais un LIST pour comprendre et je constate que le programme se réduit à une seule ligne:

Il y a des bouts de code mêlés à des octets incohérents (en apparence)... Au diable les varices, oups… l'avarice, je sauve large, très large et refais le manège habituel. Ce coup là, ce n'est pas mieux, j'obtiens une erreur de lecture très instructive: "TRACK: 20 SECTOR : 08 READ FAULT 10 ? DISK I/O ERROR IN 7603" ! Le CALL#1393 a commandé une lecture, mais le disque ne correspond pas ! Évidemment ma disquette de travail n'a rien à voir avec la disquette CEO-soft 2.

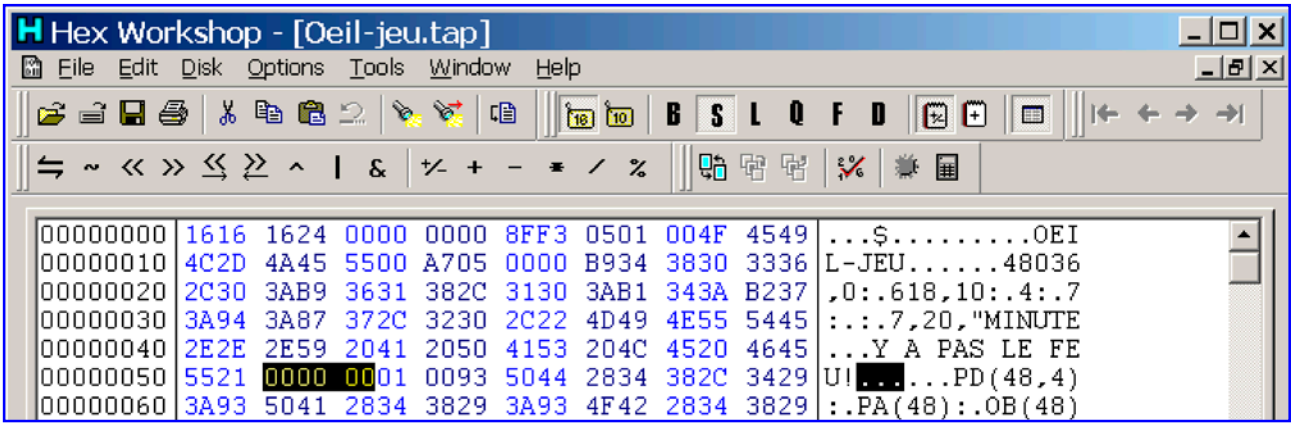
Réfléchissons un peu. Dans le cas de la disquette CEO-soft 2, après avoir exécuté le 1er Basic, il faut non pas charger le 2e, mais lire des données sur la disquette, effectuer un transcodage, mettre



Le jeu s'arrête immédiatement après "Minute…"

0 POKE48036,0:POKE618,10:PAPER4:INK7:CLS:PLOT7,20,"MINUTE...Y A PAS LE FEU!

Grrr... Encore le même coup du triple #00 intempestif ! Décidément, je serais toujours un grand naïf. J'aurais bien dû m'y attendre et examiner le "Dump" d'un peu plus près... Avec Mluch, j'avais attribué mes ennuis à un accident et pas à une protection et j'étais toujours dans l'idée que le triple #00 marque la fin réelle du programme. Me faire prendre deux fois au même piège, quel c.. !



Début du fichier "OEIL-JEU.TAP: on voit un triple " #00 juste à la fin de la 1ère ligne Basic !

Je reprends le "Dump" de ŒIL.JEU avec mon éditeur hexadécimal et rechercher les triples #00 :

Le premier est en #053D. C'est celui qui est situé après "Y A PAS LE FEU".

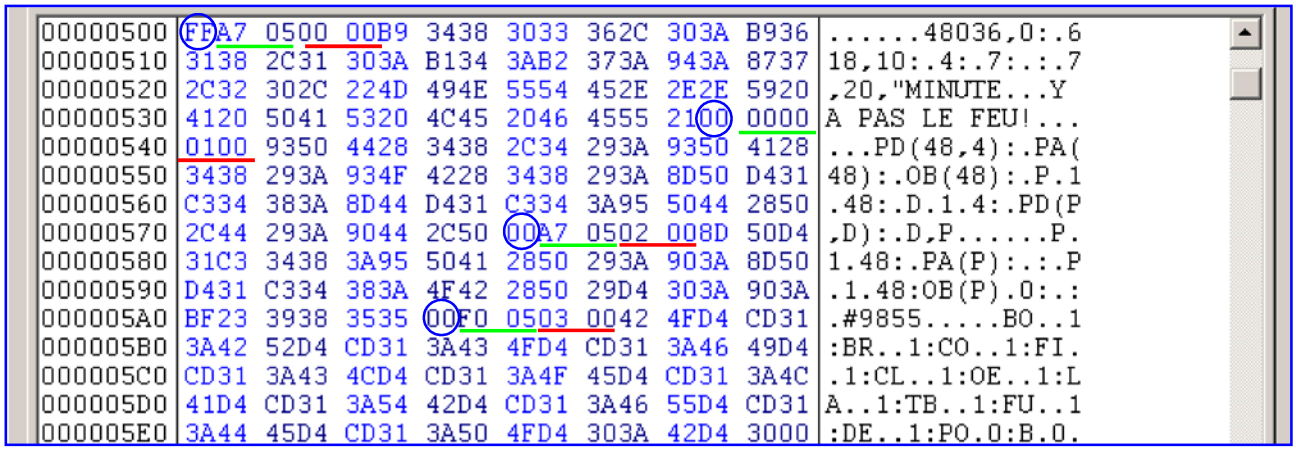
Le second est en #8FF0. Ce doit être le "vrai".

Les suivants sont en #8FF8, #8FFF, etc. mais sont situés dans une zone de données sans signification évidente (sauf si on est en présence d'un fichier composite, voir Ceo-Mag n°291, pages 10-12).

Le fichier OEIL.JEU, qui allait de #0501 à #8FF3 (octet suivant le triple #00), est donc à priori correct. J'en corrige l'offset en remplaçant l'entête par #501 octets #FF) et sauve sous le nom OEIL-JEU.BIN.

A partir de #501, je recherche les liens des lignes. En fait, je recherche les #00, qui marquent la fin de la ligne précédente (figure ci-dessus).

Dans cette figure les #00 cerclés en bleu sont les



Etat du programme Basic "OEIL-JEU.TAP" avant correction de plusieurs liens de lignes

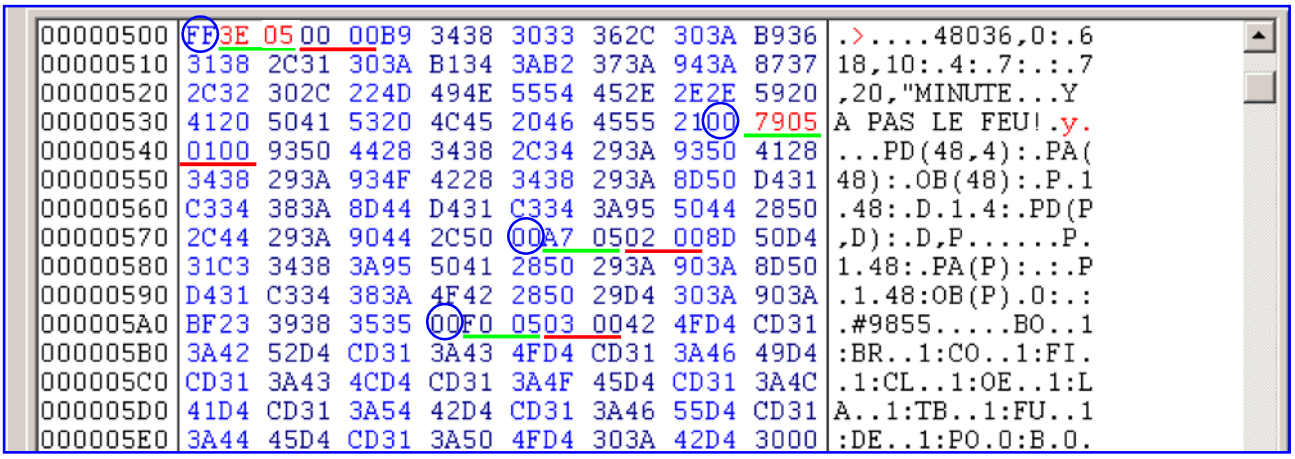
marques de fin des lignes Basic. Il est suivit d'un nombre sur deux octets souligné en vert qui est le lien (adresse du lien de la ligne suivante). Puis vient un autre nombre sur deux octets souligné en rouge qui est le n° de ligne. Enfin suit le code Basic, puis le #00 de fin de ligne etc.

En #0501 se trouve le premier lien #05A7, suivit du n° de ligne 0 (#0000). Ce lien est faux, il faudra y mettre #053E. Notez qu'en #0500 on devrait avoir #00, le #FF provient de mon ajustement d'offset.

- En #053D, fin de la ligne n°0 suivie du lien #0000. Ce lien est faux, il faudra y mettre #0579.
- En #0578, fin de la ligne n°1 suivie du lien #05A7 et du n° de ligne 2. Ce lien est correct.
- En #05AC, fin de la ligne n°2 suivie du lien #05F0 et du n° de ligne 3. Ce lien est correct.
- En #05EF, fin de la ligne n°3 suivie du lien #062F et du n° de ligne 4. Ce lien est correct.

Tous les liens semblent donc corrects à partir du #05EF du début de la ligne n°3. Les corrections faites, je remplace les #501 octets #FF par l'entête d'origine, que j'avais mis de côté. Je recharge OEIL-JEU.TAP dans ma disquette de travail et teste.

Patatras, j'obtiens un "BREAK ON BYTE #9855 IN 2". Un LIST 2 et je vois tout de suite que c'est à cause du CALL#9855. Ce CALL, qui repose sur du langage machine situé après le programme Basic (fichier "composite"), n'était pas nécessaire dans la version initiale de 1885 (disquette trimestrielle de mars 1998). C'est encore de la protection, comme dans le cas de MLUCH.



```
00000500 FF3E 0500 00B9 3438 3033 362C 303A B936 .>....48036,0:.6
00000510 3138 2C31 303A B134 3AB2 373A 943A 8737 18,10:.4:.7:.:.7
00000520 2C32 302C 224D 494E 5554 452E 2E2E 5920 ,20,"MINUTE...Y
00000530 4120 5041 5320 4C45 2046 4555 2100 7905 A PAS LE FEU!.y.
00000540 0100 9350 4428 3438 2C34 293A 9350 4128 ...PD(48,4):.PA(
00000550 3438 293A 934F 4228 3438 293A 8D50 D431 48):.OB(48):.P.1
00000560 C334 383A 8D44 D431 C334 3A95 5044 2850 .48:.D.1.4:.PD(P
00000570 2C44 293A 9044 2C50 00A7 0502 008D 50D4 ,D):.D,P......P.
00000580 31C3 3438 3A95 5041 2850 293A 903A 8D50 1.48:.PA(P):.:.P
00000590 D431 C334 383A 4F42 2850 29D4 303A 903A .1.48:OB(P).0:.:
000005A0 BF23 3938 3535 00F0 0503 0042 4FD4 CD31 .#9855.....BO..1
000005B0 3A42 52D4 CD31 3A43 4FD4 CD31 3A46 49D4 :BR..1:CO..1:FI.
000005C0 CD31 3A43 4CD4 CD31 3A4F 45D4 CD31 3A4C .1:CL..1:OE..1:L
000005D0 41D4 CD31 3A54 42D4 CD31 3A46 55D4 CD31 A..1:TB..1:FU..1
000005E0 3A44 45D4 CD31 3A50 4FD4 303A 42D4 3000 :DE..1:PO.0:B.0.
```

Etat du programme Basic "OEIL-JEU.TAP" après correction de deux liens de lignes

Voici la liste des différences entre la version de 1985 et celle de 1988 (disquette CEO-soft 2). Les n° entre crochets sont les n° de ligne de la version 1985, puis de la version 1988 :

- 1e ligne [800-> inexistante]
- 2e ligne [900->0] ajout d'un " à la fin de la chaîne de caractères
- 3e ligne [1550->1 inchangée]
- 4e ligne [1560->2] ajout d'un CALL#9855 en fin de ligne
- 5e ligne [1600->3 inchangée]
- 6e ligne [1610->4 inchangée] etc. jusqu'à la ligne 6050
- Xe ligne [6050->6050] RUN1550 remplacé par GOTO3

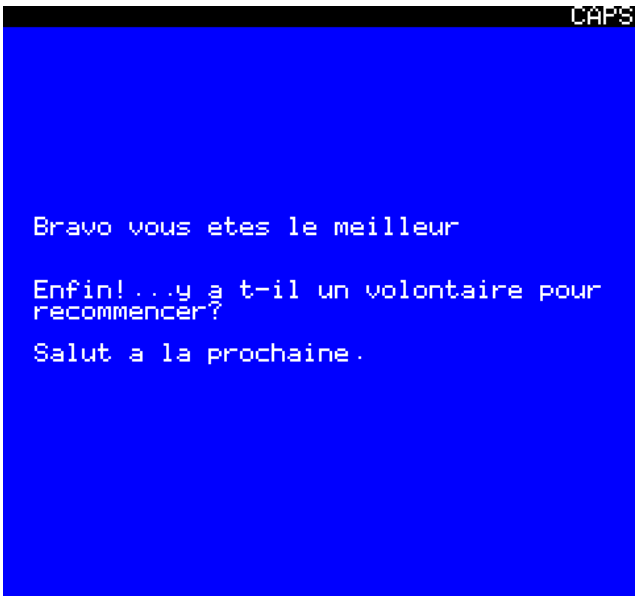
En résumé, il suffit de supprimer le CALL#9855 de la ligne 2. Ce que je fais en éditant le fichier OEIL.JEU de la disquette et en resauvant avec SAVEO"CEO.JEU",AUTO

Je teste et... ça marche au poil ! Pour être vraiment sûr, j'applique la solution du jeu, fournie par Dominique P. dans le Ceo-Mag n°194, pages 27-29, et je parviens sans encombre à sortir de la maison maudite avec l'œil de Zoltec (écran final ci-dessous).

Bilan des différentes versions de "L'œil de Zoltec" en ma possession :

1. "L'œil de Zoltec" de la disquette trimestrielle de mars 1998. Cette version est copyrightée "1985" et fonctionne parfaitement. Ses protections sont puériles.
2. "L'œil de Zoltec" de CEO-soft 2. Cette version est semblable à la version précédente, mais visiblement postérieure. Elle est copyrightée "1988". Ses protections sont sévères. La copie que j'ai extraite de la disquette CEO-soft 2 est au plus proche de la version "plombée" et fonctionne parfaitement.

Nous verrons ce que ça donne pour le dernier jeu dans le prochain article. à suivre…



Les écrans de début du jeu… et de fin, avec (très) brèves félicitations pour avoir gagné !