La Protection des disquettes selon Daniel Duffau (4ème partie)

Utilisation du debugger d'Euphoric pour récupérer Yahtzee

Par André C.

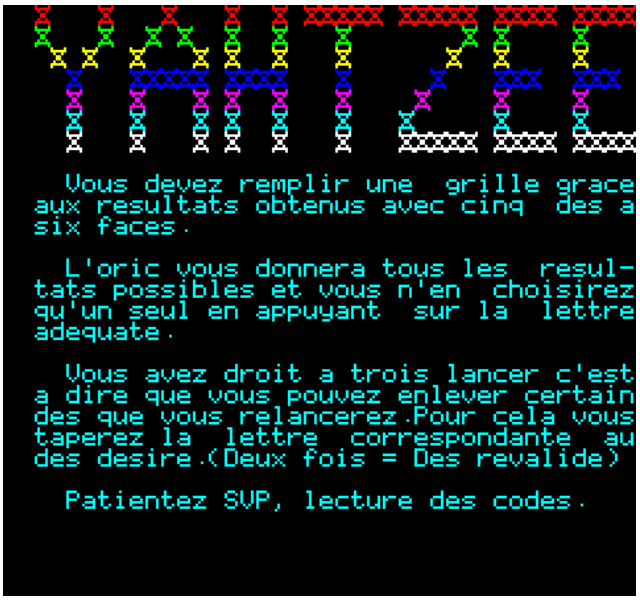
Ecran-menu de la disquette CEO-soft 2

Récupération de "Yahtzee" de Thomas Gempp

Cette fois, ça risque d'être plus difficile, car j'y vais à l'aveugle. Je n'ai absolument aucune indication sur ce programme. Va falloir avoir de la chance ou se creuser la cervelle sérieusement...

Je lance la disquette CEO-soft 2 dans Euphoric. Au menu, je choisis l'option 2. Le 1er écran affiche "Un jeu de Thomas GEMPP (02/86)". Puis vient un écran-titre en deux parties, qui donnent quelques explications (voir ci-dessous).

A l'apparition du message "APPUYEZ SUR UNE TOUCHE POUR JOUER", j'appuie sur la touche F9 d'Euphoric. Avec un éditeur hexadécimal, j'examine le fichier Dump obtenu. Je trouve un programme Basic en #0501. Les données se poursuivent jusqu'en #3E4B, mais la fin ne semble pas



Les deux premiers écrans (titre & instructions) de Yahtzee

avoir de sens.

Je recherche les triples #00. Il fallait s'y attendre, le 1er est situé en #0506 et le 2ème en #3DCF.

Je copie, dans un fichier vierge, le bloc allant de #0501 à #3DD2 (c'est l'octet qui suit le triple #00) soit #38D2 octets. Je sauve sous le nom "YAHTZEE.BIN" et, comme pour les autres jeux, j'ajoute par devant #0501 fois l'octet #FF, afin de rétablir l'offset normal de la mémoire de l'Oric.

J'examine la chaîne des liens de lignes et en corrige deux liens qui étaient erronés (c'est devenu la routine maintenant).

Reportez-vous à la figure "Etat du programme Basic "YAHTZEE" avant correction de plusieurs liens de lignes" de la page suivante.

```
00000500 FF44 0700 00A1 0000 0072 00B1 303A B236 .D.......r..0:.6
00000510 3AB9 3631 382C 3130 3A94 3A9E 2335 4646 :.618,10:.:.#5FF
00000520 453A 9A3A 9353 3128 332C 3138 292C 5332 E:.:.S1(3,18),S2
00000530 2833 2C31 3829 006A 0573 005A 24D4 2222 (3,18).j.s.Z$.""
00000540 3A8D 51D4 31C3 3338 3A5A 24D4 5A24 CC22 :.Q.1.38:Z$.Z$."
00000550 2022 3AB9 2342 4238 31CC 512C 3332 3A90  ":.#BB81.Q,32:.
00000560 3AB9 2342 4238 312C 3000 8205 7400 99E7 :.#BB81,0...t...
00000570 2823 4646 4643 29D4 2346 3432 44C9 3131 (#FFFC).#F42D.11
00000580 3900 BA05 7500 8A23 3237 382C 2342 4343 9...u..#278,#BCC
```

Etat du programme Basic "YAHTZEE" avant correction de plusieurs liens de lignes

Dans cette figure les #00 cerclés en bleu sont les 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 #0744, suivit du n° de ligne 0 (#0000). Ce lien est faux, il faudra y mettre #0507, adresse du lien suivant.

Notez qu'en #0500 on devrait avoir #00, le #FF provient de mon ajustement d'offset.

En #0507, le lien est nul (#0000) et forme avec le #00 de fin de la 1ère ligne, un triple #00 de fin de Basic. Ce lien est évidemment faux, il faut le remplacer par #0537, adresse du lien suivant.

En #0537, le lien est correct (#056A est bien l'adresse du lien suivant). Les liens suivants sont tous corrects.
Voir la figure ci dessous après correction.

```
00000500 FF07 0500 00A1 0037 0572 00B1 303A B236 .......7.r..0:.6
00000510 3AB9 3631 382C 3130 3A94 3A9E 2335 4646 :.618,10:.:.#5FF
00000520 453A 9A3A 9353 3128 332C 3138 292C 5332 E:.:.S1(3,18),S2
00000530 2833 2C31 3829 006A 0573 005A 24D4 2222 (3,18).j.s.Z$.""
00000540 3A8D 51D4 31C3 3338 3A5A 24D4 5A24 CC22 :.Q.1.38:Z$.Z$."
00000550 2022 3AB9 2342 4238 31CC 512C 3332 3A90  ":.#BB81.Q,32:.
00000560 3AB9 2342 4238 312C 3000 8205 7400 99E7 :.#BB81,0...t...
00000570 2823 4646 4643 29D4 2346 3432 44C9 3131 (#FFFC).#F42D.11
00000580 3900 BA05 7500 8A23 3237 382C 2342 4343 9...u..#278,#BCC
```

Etat du programme Basic "YAHTZEE" après correction de plusieurs liens de lignes

Je remplace les #0501 octets #FF par un entête adapté et sauve sous le nom "YAHTZEE.TAP". Ce TAP est transféré sur disquette selon la procédure maintenant habituelle (la parution de cette série d'article s'échelonnant sur plusieurs mois, le lecteur qui aurait besoin de précisions est invité à se reporter notamment à la 2ème partie, concernant MLUCH).

Le test du fichier "YAHTZEE.COM" se révèle sans problème (à part la difficulté du jeu). Le listing de ce programme est conforme à ce qui était observé sur le fichier Dump. La dernière ligne listée est bien la suivante :

```
541 DATA 0,0,0,0
```

J'examine les CALL présents dans ce listing :

- Ligne 125 : CALL#B400
- Ligne 149 : CALL Z1, CALL#9C44, CALL Z2
- Ligne 181 : CALL#98AC
- Ligne 206 : CALL#98AC
- Ligne 207 : CALL Z1, CALL#9BF0
- Ligne 208 : CALL Z2

- Ligne 211 : CALL Z1, CALL Z2
- Ligne 212 : CALL Z2
- Ligne 213 : CALL Z2, CALL#FAFA, CALL#FB14
- Ligne 242 : CALL Z2
- Ligne 337 : CALL X1

On trouve facilement que Z1 est initialisé à :

- #F9AA en Rom 1.1 ou
- #F960 en Rom 1.0 (initialisation du VIA 6522)

Idem pour Z2 :

- #E940 en Rom 1.1 ou
- #E807 en Rom 1.0 (VIA et autoriser les IRQ)

D'autres adresses en Rom sont également utilisées :

- #FAFA (ZAP) et
- #FB14 (son du clavier)

Tandis que X1 prend tour à tour les valeurs #9865, #9870, #987B, #9886 et #9891, d'autre appels en Ram sont également effectués: #98AC, #9BF0, #9C44 et #B400. Thomas a clairement fait appel à des routines en langage machine pour accélérer le jeu. Il importe donc que ces routines soit bien présentes. J'examine donc les commandes READ pour voir si c'est le programme Basic qui les met en place.

- Ligne 125 : Mise en place du code de #B400 à #B422.
- Ligne 239 à 243 : Mise en place du code de #9800 à #9C72 (DATA lignes 341 à 455), puis du code de #9D00 à #9FB7 (DATA lignes 459 à 529).
- Ligne 247 et 248 : Redéfinition de caractères (DATA lignes 533 à 541).

Conclusion : Les CALL appellent soit des sous-programmes en langage machine, mis en place par le programme lui-même, soit des sous-programmes en Rom (avec distinction Oric-1/Atmos). Aucun CALL ne cible la zone de #3DD3 à #97FF, qui ne contient donc que des "résidus" de transcodage et mise en place. On

trouve également des "résidus" de #A000 à #B3FF (Yahtzee n'utilise pas d'écran Hires), de #B423 à #B454 et de #BFE0 à #BFFF.

Au total, la version "déplombée" est très raisonnablement conforme à l'original, car seul le programme Basic a été conservé et ne présente pas de problème.

Maintenant cette version est plus aisée à manipuler (un seul fichier Basic) et se charge beaucoup plus rapidement (il n'y a plus ni le scrolling, ni le menu CEO-soft 2, ni le transcodage et la mise en place du programme qui étaient tous très lent. Avis donc à ceux qui voudraient tenter leur chance (et leur stratégie) à YAHTZEE !

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