La protection de Tetrix

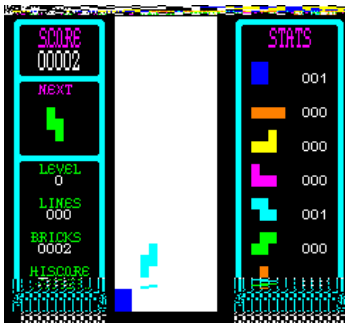
par André Chéramy

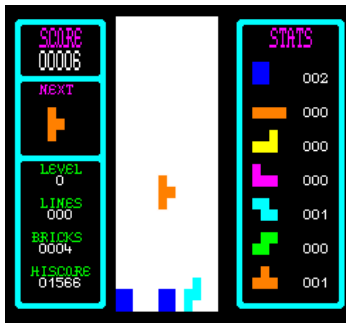
Vous avez suivi dans le Ceo-Mag les aventures de Steve Marshall aux prises avec des problèmes de fiabilité (avec son matériel réel) sans savoir si cela vient des disquettes HD utilisées, de son lecteur 3.5" (lui aussi HD) ou peut-être de Sedoric 3.0.

Après avoir examiné les fichiers dsk correspondants, j'ai pu constater que dans son système les écritures se produisent parfois mal à propos, écrasant d'autres données, voire le système Sedoric lui-même. Mais les causes de ce dysfonctionnement ne sont pas claires.

Récemment il m'a envoyé l'image d'une disquette Sedoric 3.0 avec le programme Tetrix d'André Widhani, (c) Mirage Software, (fig. 1 & 2). Il s'agit d'un programme en langage machine localisé de #9000 à #AE61 avec adresse d'exécution en #A000 et checksum #386E.

Selon Steve certains programmes, mis au point sous Sedoric 1.x ne fonctionneraient peut-être pas correctement avec Sedoric 3.0. Par exemple, après copie sur disquette Sedoric 3.0, Tetrix présentait un dysfonctionnement rédhibitoire : l'écran était pollué par des caractères semi-graphiques, (fig. 3), alors que son original fonctionnait correctement sous Sedoric 1.007 (fig. 4, obtenue ultérieurement).





J'ai donc examiné la disquette et j'ai constaté que tout était normal, sauf que le programme Tetrix exhibait un affichage pollué. Mais Tetrix n'a pas mieux marché lorsque je l'ai copié sur une disquette Sedoric 1.x ou 2.x. Je lui ai donc demandé de m'envoyer une image de l'original afin de voir comment ça marche, quand ça marche et de poursuivre la recherche du problème.

La disquette originale Bkarcade.dsk que j'ai reçue contenait de nombreux programmes (voir menu et directory fig. 5 et 6). J'ai rapidement constaté que la taille totale des fichiers ne correspondait pas au nombre de secteurs libres. Il manquait 64 secteurs ! De plus, la disquette avait un lourd passé : de nombreux fichiers avaient l'objet de suppressions et de réécriture. En examinant le contenu des secteurs j'ai découvert les restes d'anciens programmes et un entrelacement de secteurs appartenant à différents fichiers. Je rappelle que lorsqu'on supprime un fichier, l'entrée correspondante est effacée du directory et les secteurs correspondants sont marqués «libres» dans la bitmap, mais les datas eux-mêmes restent intacts, tant qu'ils ne sont pas écrasés par l'écriture d'un nouveau fichier.

Bref, je me suis demandé si Tetrix ne faisait pas l'objet d'une protection (à cause des 64 secteurs manquants, qui pouvaient représenter un fichier caché, c'est à dire effacé manuellement du directory, mais toujours présent dans la bitmap et les secteurs). En raison de la complexité de la disquette, j'ai perdu pas mal de temps à vérifier l'intégrité du système et à chercher les 64 secteurs fantômes. Je vous donne tout de suite ma conclusion : la disquette «originale» avait beaucoup «vécu» et les secteurs manquants résultaient tout simplement de «read/write errors», comme cela arrive si souvent avec le matériel Oric.

Reste que Tetrix fonctionnait correctement sur cette disquette «originale» v1.007 fatiguée et que ce programme était pollué après copie sur n'importe quelle autre disquette Sedoric (y compris v1.007 fraîchement formatée).

Par hasard, j'ai effectué un BACKUP sous Euphoric (plutôt que de faire une copie du fichier dsk sous Windows comme je fais habituellement) et surprise, la copie marchait correctement. Ceci m'a permis d'éliminer une protection intervenant sur les gaps, comme celle de XL-DOS, découverte par Fabrice Francès (voir Ceo-Mag n°102 page 22). En effet, ce genre de protection est redoutable et très difficile à mettre en évidence, à moins de désassembler le programme.

J'ai alors eu l'idée farfelue de sauver Tetrix avec CSAVE en utilisant une v 3.0 de Sedoric (seule compatible). Cela implique de copier Tetrix sur une disquette 3.0 et de travailler sur une version de Tetrix qui ne marche pas ! Enfin, j'ai vérifié la checksum du «tap» obtenu : #386E comme sur la disquette originale Bkarcade.dsk. NB : Comme déjà indiqué, Tetrix est localisé de #9000 à #AE61 avec adresse d'exécution en #A000.

Reboutant avec diverses disquettes fraîchement formatées sous différentes versions de Sedoric je tentais les commandes suivantes : CLOAD «TETRIX» : CALL #A000 et à chaque fois le programme était pollué.

Eclair de génie (les chevilles !), j'ai ajouté la disquette originale Bkarcade.dsk en B et j'ai rebouté avec une version 3.0 en A. Puis j'ai tapé : CLOAD «TETRIX» : B- : CALL #A000 et victoire, Tetrix marchait correctement. Ceci m'apportait donc deux informations : d'abord Tetrix peut marcher sous Sedoric 3.0 et ensuite lors de l'exécution, Tetrix va lire une clef sur la disquette originale, une clef qui est absente de toutes les autres copies sauf celles effectuées avec BACKUP.

Donc cette clef se trouve dans un secteur transmis ni par INIT (donc pas situé dans les secteurs du DOS), ni par COPY «*.*» (donc pas situé dans les fichiers présents dans le directory). Mais ce secteur est copié par BACKUP. La clef se trouve donc dans les données d'un des 1360 secteurs de la disquette. Simple ! Il suffit d'écraser un à un ces 1360 secteurs pour voir à quel moment on perd la clef ! Un peu lourd ! Autre possibilité, prendre le problème à l'envers : copier progressivement les pistes de Bkarcade.dsk sur une disquette vierge et voir à quel moment le programme est débloqué. Puis connaissant la piste, rechercher le secteur.

J'utilise pour ce genre de travail un utilitaire génial : COPFORM v2.2 (voir Ceo-Mag n°56 pages 5 et 6). Il permet, entre autres choses, de copier une ou plusieurs pistes à partir d'un numéro de piste donné. Dans un premier temps, j'ai copié le minimum : les 6 premières pistes de la disquette (de n°#00 à #05), la piste de bitmap et directory (n°#14) et les 3 pistes où se trouvait Tetrix (n°# 23 à #25), copie effectuée en 3 passes.

Puis j'ai bouté avec ma copie toute fraîche (quoique un peu problématique cette disquette «partielle», s'il fallait en faire autre chose...). Victoire ! Tetrix marche sans être pollué. Donc la clef se trouve dans les secteurs copiés. Evidemment, j'avais copié un peu large : la fin de la piste n°#05 contenait le début d'un programme TET.COM, de même le début de la piste n°#23 et la fin de la n°#25 contenait des secteurs appartenant aux fichiers TILESWOP.COM, LOWSCORES.COM et VIDFLIP1.BIN. Mais la clef ne pouvait s'y trouver, puisqu'elle n'est pas transmise par la commande COPY «*.*» qui copie ces fichiers.

Comme j'avais déjà vérifié que les secteurs du DOS étaient normaux (voir plus haut), il ne restait donc que la piste n°#14. Dans cette piste, les secteurs n°#05, #06, #08, #09, #0B, #0C, #E, #F et #11 contenaient des données n'appartenant à aucun fichier du directory et pouvant représenter d'anciennes données, correspondant à des fichiers effacés. Ça se présente mal, s'il faut vérifier tout ça !

Comment savoir simplement où se trouve la clef ? Plutôt que de copier des #00 dans les secteurs à tester avec NIBBLE sous Euphoric, j'ai décidé d'effectuer cette opération avec HexWorkshop v3.11, un éditeur hexadécimal sous Windows. J'ouvre l'image de ma disquette «partielle» et j'examine la piste n°#14. Pour en trouver le premier secteur, il faut chercher la suite hexadécimale «14000101» (pour piste #14, face #00, secteur #01 et format de données #01=256 octets), les 256 octets commencent juste après la suite hexadécimale «A1A1A1FB» qui suit. Les secteurs n°#01 (système) et n°#02 (bitmap) se révélèrent normaux à première vue. Mais le secteur n°#03 m'a sauté aux yeux : il contenait des données or j'étais en train d'examiner une copie de Bkarcade.dsk (Sedoric v1.007) et ce secteur ne devrait donc contenir que des #00. En effet dans la version 1.x, ce secteur bien que réservé (marqué occupé) ne sert pas et contient toujours des zéros. Ici, il contenait les octets suivants : 65666A6767C9BAC96566646967B6C7C46566646966C3AEB etc. Soit en Ascii : efjgg...efdig...efdif...efddf...efc^c...efcj]...efcde...efcc]...eff]c...etc.

Sûr de tenir ma clef, j'ai repris une version «polluée», j'y ai copié les 256 octets du secteur 3 de la piste #14 de la disquette Bkarcade.dsk avec HexWorkshop et j'ai rebouté : Victoire ! Tetrix n'est plus pollué !

Donc, contrairement à ce que j'ai écrit plus haut, Tetrix n'est pas vraiment compatible avec les versions de Sedoric autres que 1.x. En effet, les versions 2.x et 3.0 utilisent le secteur 3 de la piste #14 pour le 2e secteur de bitmap, qui permet d'exploiter les disquettes 80 pistes. Il y aura donc inévitablement un conflit entre la clef et le 2e secteur de bitmap. Néanmoins, si l'on s'abstient de toute opération impliquant la bitmap, ça devrait marcher quand même. On a alors une sorte de protection vraiment «crados» ! Testons...

J'ai alors formaté deux disquettes «minimales» en 22 pistes de 16 secteurs mono face avec les versions 1.007 et 3.0 de Sedoric, j'y ai copié Tetrix (avec la commande COPY) et enfin j'ai ajouté la clef avec HexWorkshop comme indiqué ci-dessus (écrasant par là même le 2e secteur de bitmap de la disquette 3.0). Comme je m'y attendais, Tetrix marche impeccablement dans les deux cas. CQFD !