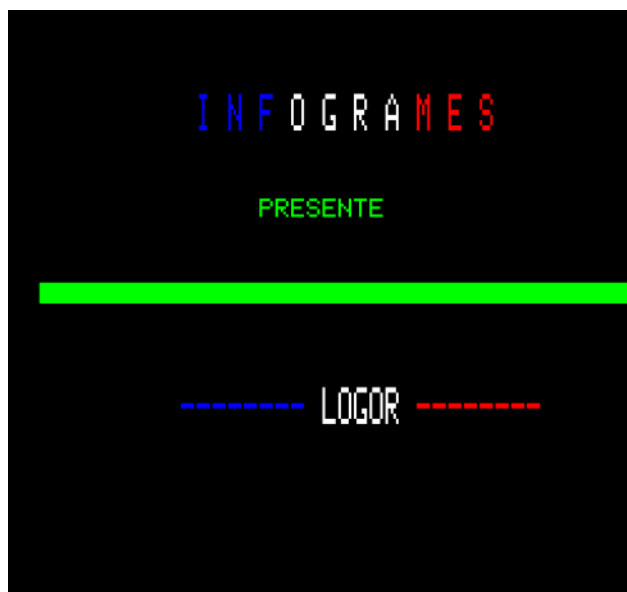


# Récupérez les écrans des logiciels protégés

## 1 - Méthode

par André C.



### Constatation

Les cassettes et les disquettes 3" vieillissent mal, de même que leurs lecteurs respectifs. Le transfert des logiciels Oric sur des supports modernes est donc crucial. C'est grâce à ces transferts et à divers émulateurs que nous pouvons profiter, encore aujourd'hui, des programmes achetés dans les années 80. Simon G., Dominique P., Fabrice F. et bien d'autres ont réussi à transférer au format .tap la plupart des logiciels du commerce, notamment ceux qui comptent parmi les mieux protégés. La complexité des moyens de protection mis en œuvre est parfois surprenante au vu de leur valeur économique somme toute limitée.

### Un florilège de protections

Les passionnés de casse-têtes pourront découvrir ou relire les nombreux articles pas-

sionnants parus dans le CEO-mag à ce sujet. Pas loin d'une centaine d'articles ont été publiés qui décortiquent les divers procédés de



protection rencontrés. Parmi les plus spectaculaires, citons C-SAFE, utilisé pour Titan, Logor et Talisman de chez Infogrames et pour Vortex de chez Loriciels (voir articles "C-SAFE et .TAP" par Simon G. et Dominique P., CEO-mag n°261, pages 14 et 15, ainsi

que "Cassettes, un florilège de formats exotiques (2)" par Dominique P., CEO-mag 262, pages 18 et 19.

Mais il existe tout une panoplie d'autres systèmes de protection et de formats exotiques...

### Bilan des transferts au format .tap ou .dsk

Un très grand nombre de logiciels sont maintenant disponibles dans ces formats. Pour lever les protections, il a parfois été nécessaire de modifier un minimum d'octets, mais toujours avec le souci de coller au plus près à l'original.

Les procédures utilisées pour contourner certaines protections sont si complexes, qu'il est souvent beaucoup plus simple de lire les cassettes audio, d'enregistrer la "musique" au format classique .wav. Le fichier obtenu peut alors être placé sur une bande magnétique ou un CD et réinjecté dans un Oric réel ou être rechargé dans un émulateur. Mais bien sûr ce fichier .wav inclut toujours la protection. Le logiciel est utilisable, mais on ne peut pas "regarder dedans".

Au moins 25 fichiers au format .wav sont aujourd'hui disponibles sur oric.org et concernent évidemment les logiciels les plus récents.

### Ecrans versus recopie d'écrans

Certes, les émulateurs permettent d'effectuer des recopies d'écrans, mais les fichiers obtenus sont aux formats .BMP, .GIF, etc. Il serait intéressant de récupérer les écrans TEXT ou HIRES aux formats Oric .SCR et .HRS sur un support .tap ou .dsk. Dans le même genre d'idée, ce serait chouette de récupérer les caractères redéfinis, les musiques, etc. Or, comme écrit plus haut, on ne peut pas "regarder dedans". Mais est-ce bien sûr?

### Exploration de la Ram

Non seulement c'est tout à fait possible, mais en plus c'est très simple. En effet, les émulateurs permettent d'effectuer un dump de la mémoire. Ainsi avec Euphoric, un simple appui sur la touche F9 sauve un fichier DUMP de 64 Ko correspondant à l'intégralité de la mémoire de l'Oric émulé. Il ne reste plus qu'à explorer ce fichier DUMP à l'aide d'un

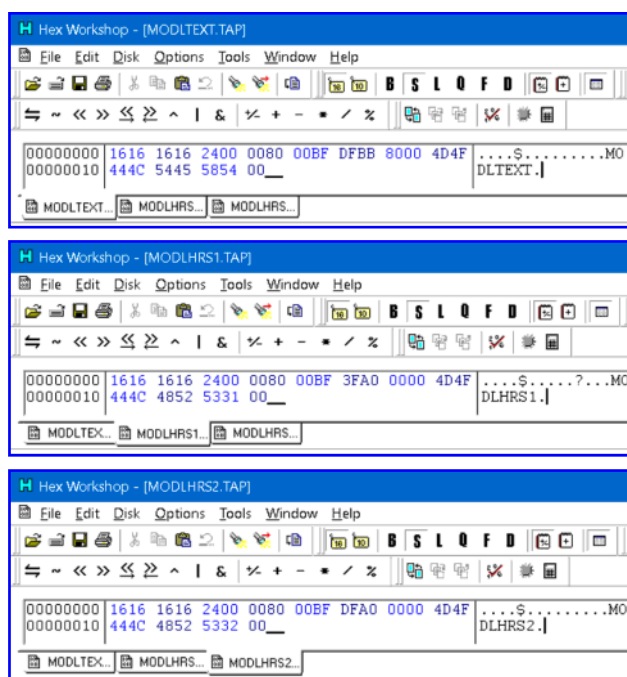
éditeur hexadécimal et d'en extraire les parties intéressantes par exemple les écrans.

### Les divers types d'écrans

Trois types d'écrans peuvent être récupérés :

- 1) Ecrans basse résolution (TEXT, LORES0 et LORES1) situés de #BB80 à #BFDF en Ram (soit #0460 octets ou 1120 en décimal ce qui correspond bien à 28 lignes de 40 caractères).
- 2) Ecrans haute résolution seuls (sans les 3 lignes de texte) situés de #A000 à #BF3F (soit #1F40 octets ou 8000 en décimal pour 200 lignes de 40 tirets de 6 pixels).
- 3) Ecrans haute résolution avec les 3 lignes de texte en dessous, situés de #A000 à #BFDF (soit #1FE0 octets ou 8160 en décimal. On remarquera une petite curiosité : la Ram comporte 4 lignes de texte sous l'écran Hires (d'où les 160 octets supplémentaires) mais la première des quatre n'est pas affichée et les 40 octets correspondants restent donc inutilisés!

Puisqu'on connaît les adresses de début et de fin de ces écrans, rien ne sera plus facile que de les récupérer (puisque'ils ont la même adresse en Ram et dans le fichier DUMP) et de les copier derrière un en-tête cassette. Les en-têtes cassettes ont été décrits dans le CEO-mag n°153 page 17. Mais il est plus simple (et plus sûr) de sauver un écran bidon et d'en



récupérer l'en-tête, plutôt que de construire celui-ci octet par octet.

### Fabriquez les en-têtes appropriés

Pour ces 3 types de d'écran, il vous faudra faire 3 modèles d'en-tête avec le petit programme SAUVENT.COM suivant (voir le fichier .zip joint à cet article) :

```
100 HIRES
110 CSAVE"MODLHRS1",A#A000,E#BF3F
120 CSAVE"MODLHRS2",A#A000,E#BFDF
130 TEXT
140 CSAVE"MODLTEXT",A#BB80,E#BFDF
150 PING
```

Pour avoir les 3 en-têtes, récupérez les octets du début du fichier .tap, allant du #16 initial au #00 (inclus) situé juste après le nom du fichier. Dans les conditions décrites, les 3 en-têtes auront au final une longueur de 23 octets (ou 22 si le début du fichier ne comporte que 3 fois l'octet #16 au lieu de 4, selon la version d'émulateur utilisé). A l'issue de ce petit travail, vous disposerez donc de 3 modèles d'en-tête que vous garderez précieusement. Les fichiers .tap correspondant à ces 3 en-têtes sont dans le zip joint à cet article.

### Récupérez les DUMPs

La procédure de récupération des écrans est maintenant simple :

- 1) Lancez Euphoric en mode Atmos, pressez F1, validez "Hardware tape" et indiquez le nom du fichier .wav à traiter, (par ex. LOGOR.WAV qui n'existe pas en version .tap). Pressez F1 pour revenir à l'Atmos.
- 2) Tapez CLOAD"" et chargez le fichier .wav. Tiens cela n'a pas changé : C'est toujours très long ! Sauf que 2 appuis sur la touche F4 et ça charge 4 fois plus vite ! Retour à la vitesse normale par un appui sur la touche F5.
- 3) Le programme se lance. Guettez le moment où s'affiche l'écran que vous désirez sauvegarder et pressez la touche F9 (dump mémoire) puis sur F11 (débugueur). En mode débogueur l'exécution se fige, ce qui vous laisse le temps de renommer le fichier DUMP obtenu (par ex DUMP01 etc.),

sinon il sera écrasé au prochain appui sur la touche F9. Nouvel appui sur la touche F11 pour sortir du débogueur. Guettez le prochain écran intéressant (s'il y en a), F9 puis F11, etc.

- 4) Notez qu'il est possible de recharger un des états ainsi sauvé pour reprendre l'exécution du programme là où elle en était, en relançant Euphoric avec "Euphoric -a -r" (attention le nom du fichier utilisé par Euphoric sera DUMP tout court).

Petite difficulté dans mon système : Euphoric sauvegarde le fichier DUMP dans le répertoire "Tapes", mais si on relance avec "Euphoric -a -r", Euphoric cherche DUMP dans le répertoire "Euphoric". Mais c'est sans doute un problème de configuration.

### Et enfin, récupérez les écrans

Vous vous trouvez maintenant en possession d'un ou plusieurs fichiers DUMPxx. Il faut en extraire la zone écran qui vous intéresse et lui coller un en-tête ad hoc par devant. Prenons par exemple le format Hires long (avec les 3 lignes de texte en dessous) situé en Ram de #A000 à #BFDF.

Dans votre éditeur hexadécimal :

- 1) Ouvrez le modèle d'en-tête correspondant, soit MODLHRS2. CTRL+A puis CTRL+C pour copier les 23 octets du fichier.
- 2) Ouvrez un nouveau document. CTRL+V pour y coller l'en-tête. Editez les 8 caractères "MODLHRS2" pour renommer votre fichier .tap
- 3) Ouvrez le fichier DUMPxx à traiter. Sélectionnez les #1FE0 octets correspondant à l'écran Hires. Par exemple *Goto #A000* puis *Select bloc #1FE0*, puis CTRL+C.
- 4) Allez dans le nouveau document, à la fin de l'en-tête, CTRL+V, pour y coller l'écran.
- 5) Sauvegardez votre écran au format .tap par exemple sous le nom ECRANxx.tap. C'est fait.

A suivre...