

Le Journal du Soft

LA ROM SUCEUSE

Par André Chéramy et Claude Sittler

Le mois dernier, nous avons décrit la ROM déplombeuse, dont le grand mérite est de bloquer totalement l'exécution automatique des programmes et de préserver le contenu de la RAM. La commande OLD n'est intéressante que si l'on doit travailler sans Microdisc, donc sans Sedoric. La ROM déplombeuse permet donc de faire face dans la plupart des cas de récupération de programme K7 en vue de leur adaptation pour fonctionner sur disquette. En effet il ne suffit pas de faire un SAVE pour régler le problème, mais au moins on peut étudier le programme sauvé et le modifier de manière idoine. Attendez-vous quand même à avoir plus à faire qu'à convertir les CLOAD en LOAD...

POURQUOI FAUT-IL ALLER PLUS LOIN ?

Il y a des cas où il est impossible de charger les différents fichiers qui constituent un programme sur K7, parce que justement la protection consiste à tromper la commande CLOAD. Par exemple, l'un des morceaux chargés, devra être exécuté pour mettre en place et lancer une routine spéciale, qui doit s'occuper de charger la suite... Inutile de vous dire que si les concepteurs se sont donné ce mal, c'est parce que la suite en question n'est pas conforme au standard de CLOAD. L'entête par exemple pourra être abracadabrante et CLOAD enverra le fichier dans un endroit critique ce qui entraînera le plantage de la machine ! Mais dans ce domaine, tout est possible et ce n'est pas encore demain que nous aurons fait le tour de la question des protections.

LES SOLUTIONS POSSIBLES

Il n'est pas bien difficile de dupliquer la K7. La solution qui consiste à connecter deux magnétophones ne donne pas de bons résultats. Jadis une bidouille avait été proposée sous forme d'un petit circuit électronique à intercaler entre les deux magnétophones. Grosso modo, ce circuit était une copie de l'interface K7 de l'Oric. Il savait donc lire un signal Oric et aussi re-émettre un signal Oric. Aujourd'hui, il est tout simplement possible d'effectuer une copie viable avec sa chaîne hi-fi. Il faut seulement veiller à utiliser un pré-réglage qui effectue la copie sans introduire de modifications et à utiliser la vitesse normale, pour obtenir le maximum de fidélité. Et ça marche au poil !

Il est aussi possible de faire un fichier WAV en enregistrant la « musique » de la K7 et après conversion de générer un fichier utilisable par Euphoric. Si cela vous branche, suivez les pas de Grégory Guazzelli (Ceo-Mag n°123).

Mais notre propos n'est pas de dupliquer des K7. Nous cherchons à transférer les K7 originales sur disquette. C'est dans ce contexte que notre ROM suceuse représente peut-être l'arme absolue. Encore qu'elle ne règle toujours pas le problème de l'adaptation.

QUE FAIT LA ROM SUCEUSE ?

Outre qu'elle possède toutes les propriétés de la ROM déplombeuse, puisque nous sommes partis de celle-ci, elle offre une commande supplémentaire : SUCE.

Cette nouvelle commande lit un à un les octets qui arrivent sur le port K7 (il faut donc mettre en lecture le magnétophone, sans compter sur le relais de télécommande), sans chercher à comprendre

de quoi il s'agit : Amorce, entête, type de programme, AUTO ou non, elle s'en moque, ce n'est pas son problème.

Au fur et à mesure, elle stocke ces octets en RAM, à partir de #0505. Elle avale tant que le magnéto-
phone tourne et que la bande « chante ». Enfin, faites quand même attention, la place disponible en
mémoire (environ 45000 octets) sera remplie au bout d'environ 5 minutes en mode FAST, si vous ne
voulez pas écraser le premier jeu de caractères...

Mais ce n'est pas grave, il y a sûrement une petite pose sur la bande et même si ce n'est pas le cas il
suffit de reculer la bande d'un tour et de recommencer l'opération. Le procédé est aveugle et il suffira
de recoller les morceaux.

La commande SUCE est très primitive, c'est pour ça qu'elle marche ! Il faudra seulement lui dire
d'arrêter à la fin avec un gentil reset, en pressant soit le bouton sous l'Atmos (reset à chaud), soit le
bouton du Microdisc (reset à froid). Même dans ce dernier cas, la ROM suceuse fera en sorte que la
mémoire ne soit pas ré-initialisée.

DETAIL DES MODIFICATIONS APPORTEES

Cette ROM sera distribuée également avec la disquette trimestrielle de décembre 2001, mais vous
pouvez aussi la fabriquer vous-même en suivant la procédure que nous avons déjà décrite à mainte
reprise dans notre série d'articles du « Journal du Soft ». En partant de la ROM V1.1 dernière mou-
ture, dont la checksum est #1A25, ou de la ROM déplombeuse, dont la checksum est #26E3, la
checksum du fichier produit SUCE.ROM devra être #239F. En voici le détail en suivant l'ordre crois-
sant des adresses :

De #C0ED à #C0F0, le nom de la commande EDIT (soit #45, #44, #49 et #D4, le code ASCII du
dernier caractère étant augmenté de #80, ici « T » = #54 + #80 = #D4) a été remplacé par celui de la
commande SUCE (#53, #55, #43, #C5). Remarquez que la longueur est identique. La commande
EDIT n'est jamais utilisée. On peut faire LIST n°_de_ligne, qui revient au même. L'adresse d'exé-
cution de la nouvelle commande SUCE est la même que celle de la commande EDIT. La routine corres-
pondant à EDIT a donc été remplacée par le code de la commande SUCE.

De #C693 à #C6B2, la routine de EDIT à été remplacée par la routine SUCE suivante :

C692-	20 6A E7	JSR \$E76A	Configure le VIA pour travail K7
C695-	A9 05	LDA #\$05	Ecrit l'adresse #0505 en #00-#01
C697-	85 00	STA \$00	Ce sera l'adresse où copier en RAM
C699-	85 01	STA \$01	
C69B-	A0 00	LDY #\$00	Initialise l'index à zéro
C69D-	20 C9 E6	JSR \$E6C9	Lire un octet sur le port K7
C6A0-	91 00	STA (\$00),Y	Le stocker en RAM à partir de #0505
C6A2-	18	CLC	
C6A3-	A5 00	LDA \$00	Incrémenter
C6A5-	69 01	ADC #\$01	le pointeur
C6A7-	85 00	STA \$00	en #00 (octet de poids faible)
C6A9-	A5 01	LDA \$01	Reporter l'éventuelle retenue
C6AB-	69 00	ADC #\$00	en #01 (octet de poids fort)
C6AD-	85 01	STA \$01	NB toujours = ou > à #05
C6AF-	D0 EC	BNE \$C69D	Boucle forcée lecture octet suivant
C6B1-	EA	NOP	jusqu'à bouton reset pressé
C6B2-	EA	NOP	Neutralise le reste de EDIT

De #ED9B à #EDBB, le message de Copyright :

« ORIC DEPLOMBEUSE V1.1 © 1986 MARGARINE » a été modifié en :
« ORIC ROM SUCEUSE V1.1 © 2001 MARGARINE ».

En #F915 et #F91A, les couleurs de INK (#07 blanche) et PAPER (#14 bleue) ont été changées en #04 (encre bleue) et #13 (papier jaune).

TEST DE LA ROM SUCEUSE

Pour commencer, faites simple. Sauvez un petit programme BASIC en AUTO, par exemple celui en deux lignes indiqué ci-dessus, avec un CSAVE « ABC »,AUTO

Le mois dernier, vous avez déjà vu ce qui se passe avec un Atmos normal et avec un Atmos équipé de la ROM déplombeuse lorsqu'on utilise les commandes CLOAD, LIST, NEW et OLD et RUN ou lorsqu'on l'on effectue un reset à froid (bouton poussoir du Microdisc ou CALL#F88F) ou à chaud (bouton sous l'Atmos ou CALL#F8B2). Pour ces diverses manœuvres, la ROM suceuse se comporte de la même manière que la ROM déplombeuse.

Mais, là où il y a du nouveau, c'est que la commande EDIT est refusée (File not found error). Normal, nous l'avons éliminée.

Lancer la commande SUCE et mettez votre magnétophone en lecture. A part la « musique » caractéristique du magnétophone, il semble ne rien se passer. Dès la fin de la « musique », faites un reset Microdisc ou Atmos (le résultat sera le même). Un LIST ne donnera rien et pour cause ! Est-il bien utile de tenter un OLD ?

Avant toute chose, sauvez votre chantier avec un SAVE « RAM »,A#505,EDEEK(#00), on ne sait jamais, l'analyse peut durer un peu... Chargez ensuite un petit moniteur, de préférence celui dont vous avez l'habitude, pourvu qu'il se charge assez haut en mémoire. Examinez la mémoire à partir de #500. Vous allez trouver votre petit programme BASIC, précédé de la bande amorcée et de l'entête : Tout a été avalé et stocké.

Repérez et notez les adresses de début et de fin du programme proprement dit et faites un SAVE « ABC »,A#deb,E#fin. Un STATUS « ABC »,A#501 remettra les adresses en ordre. Rechargez le programme et faites un OLD suivi d'un SAVE « ABC.BAS »,AUTO permettra de récupérer le programme dans sa forme BASIC opérationnelle. Et voilà c'est fait !

Ce ne sera pas plus difficile pour récupérer n'importe quel programme, pourvu qu'il ne fasse pas l'objet d'une protection sauvage. Notez que même dans ce cas, il vous sera toujours possible de récupérer proprement la chose pour l'utiliser comme fichier .TAP sous Euphoric.

EXEMPLE DE DUMP

Pour vous aidez, voici un petit exemple de programme BASIC, le même que le mois dernier :

```
10 PRINT « LIGNE 1 »
20 PRINT « LIGNE 2 »
```

Voilà ce que ça donne en RAM, après chargement avec la commande SUCE :

ADRESSE	VALEUR
505	16 16 16 16 16 16 16 16 16 16 16
510	16 16 16 16 16 16 16 16 16 16 16 16 16 16 16
520	16 16 16 16 16 16 16 16 16 16 16 16 16 16 16
etc.	
600	16 16 16 16 16 16 16 16 24 00 00 00 00 05 21 05
610	01 00 41 42 43 00 10 05 0A 00 BA 22 4C 49 47 4E
620	45 20 31 22 00 1F 05 14 00 BA 22 4C 49 47 4E 45
630	20 32 22 00 00 00 1E

RAPPEL DE LA STRUCTURE D'UN FICHIER K7

Il y a bien longtemps que vous n'avez pas regardé à quoi ressemble un fichier K7 et vous êtes perplexe devant le contenu de votre RAM ?

Vous trouverez ci-dessous les offsets (numéros d'ordre depuis le début) sur une K7 de type Euphoric (amorce réduite à 3 octets #16 au lieu de 259), les adresses et valeurs des octets copiés en page 2 lors d'un CLOAD, les adresses et valeurs des octets copiés en RAM lors d'un CLOAD, les adresses (à titre indicatif seulement) et valeurs des octets chargés en RAM avec la commande SUCE et la signification de ces octets. Toutes les valeurs sont en hexadécimal (sauf la traduction des n° de ligne).

Remarques :

*La longueur de l'entête K7 est variable et dépend de la longueur du nom du fichier, laquelle peut être nulle. Les offsets et adresses indiqués à la suite ne sont donc valables que pour l'exemple donné.

**Le nom de fichier est stocké en page deux de #293 à #2A3. Il peut avoir de zéro à 16 caractères et comporte toujours en plus un zéro final de fin de nom. Remarquez enfin, que l'entête K7 en page 2 et sur la bande sont dans l'ordre inverse. Ce n'est pas grave, mais les adresses de début et fin de fichier sont dans l'ordre habituel LLHH (octet de poids faible, puis de poids fort) en page2 et dans l'ordre HHLL sur la bande ! Fabrice Broche s'est d'ailleurs mélangé les crayons dans « L'Oric à nu » en inversant aussi les octets « type de fichier » et « status », ce qui n'a rien à voir.

OFFSET K7	ADRESSE PAGE 2	ADRESSE CLOAD	ADRESSE SUCE	OCTET(S)	SIGNIFICATION
00-02	-	-	505-607	16	Bande amorce (259 ou 2 fois #16)
03	-	-	608	24	Drapeau début de l'entête
04-05	2AF-2B0	-	609-60A	00 00	Drapeaux sans grand intérêt
06	2AE	-	60B	00 ou 80 ou 40	Drapeau BASIC Drapeau LM ou Bloc mémoire Drapeau Tableau
07	2AD	-	60C	00 non nul	Status STOP Status AUTO
08-09	2AB-2AC	-	60D-60E	521	Adresse fin programme
0A-0B	2A9-2AA	-	60F-610	501	Adresse début programme
0C	2A8	-	611	00	Drapeau fin entête K7
0D-0F	293-295**	-	612-614	414243	Nom de fichier, ici « ABC »*
10	296	-	615	00	Drapeau fin de nom, début data
11-12	-	501-502	616-617	10 05	Lien = adr ligne suiv. ici #0510
13-14	-	503-504	618-619	0A 00	n° de ligne, ici #000A soit 10
15	-	505	61A	BA	Code de la commande PRINT
16-1E	-	506-50E	61B-623	22 4C 49 47 4E 45 20 31 22	Texte «LIGNE1 »
1F	-	50F	624	00	Drapeau de fin de la 1ere ligne
20-21	-	510-511	625-626	1F 05	Lien = adr ligne suiv. ici #0515
22-23	-	512-513	627-628	14 00	n° de ligne, ici #0014 soit 20
24	-	514	629	BA	Code de la commande PRINT
25-2D	-	515-51D	62A-632	22 4C 49 47 4E 45 20 32 22	Texte «LIGNE 2»
2E	-	51E	633	00	Drapeau de fin de la 2eme ligne
2F-30	-	51F-520	634-635	00 00	Lien nul = fin programme BASIC
31	-	521	636	1E	Non significatif mais sauvé

La valeur de cet octet est sans intérêt, Mais c'est sur lui que pointe #9C - #9D qui indique le début des variables. De manière illogique, cet octet est sauvegardé avec le programme BASIC ! En pratique la fin du programme BASIC est donc marquée par la présence de trois #00 consécutifs.

A suivre...