REINVENTING OLDSCHOOL SECURITY

1991—2011 : LE TEMPS PASSE, LES TECHNIQUES RESTENT...

BRUNO @ KEROUANTON . NET

NUIT DU HACK 2011

18 JUIN 2011 – DISNEYLAND PARIS

JURACKERFEST.CH

➔ 26-27 AOÛT 2011 À DELÉMONT (CH)

THE SWISS JURA HACKERSPACE FESTIVAL

Concours de piratage
CHF 1500.- de prix à gagner

Vous aimez les démoparties ? Moi aussi !

Infos et inscriptions sur le site

+ twitter : @jurackerfest


éé.net

REINVENTING OLDSCHOOL SECURITY

1991—2011 : LE TEMPS PASSE, LES TECHNIQUES RESTENT...

BRUNO @ KERQUANTON . NET

NUIT DU HACK 2011

18 JUIN 2011 – DISNEYLAND PARIS

Petite incursion dans un monde fabuleux !

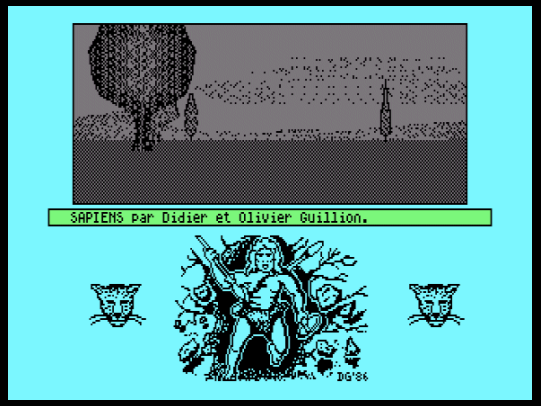
LA SÉCURITÉ DES SI NE DATE PAS D'HIER !

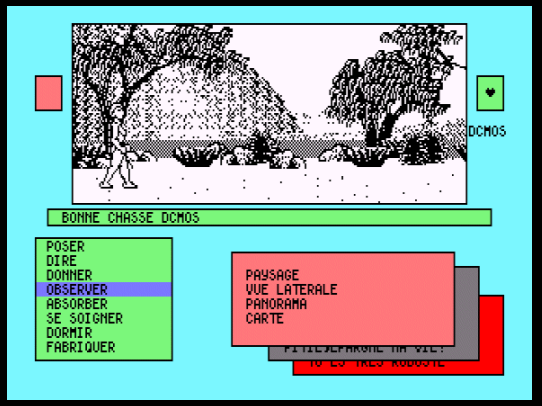
TOUT A COMMENCÉ (POUR MOI) AVEC CECI…

- Un Thomson MO5

(C'était en 1987)

- Le jeu «Sapiens» sur K7





Le jeu démarrait «tout seul»

Le son au démarrage était «bizarre»

ON ÉCOUTE ?

Le son au chargement d'un jeu «normal» :

Le son au chargement du jeu «Sapiens» :

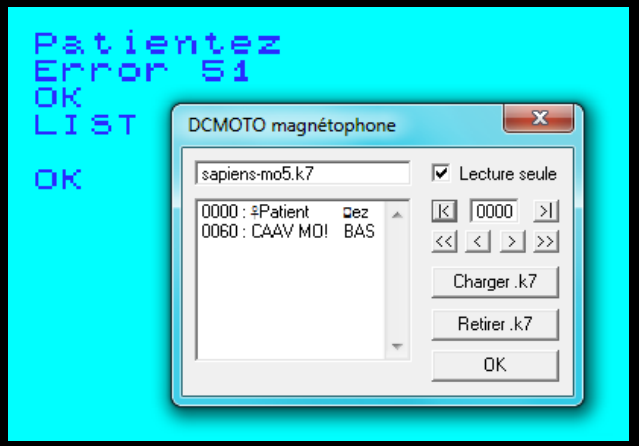
Et ce que ça donne «en vrai» !

Remerciements et amitiés à Didier et Olivier Guillion, les auteurs de ce jeu, avec qui je suis toujours en relation ! - www.myriad-online.com

UN DES PREMIERS «BUFFER OVERFLOW» !

… ou presque !

Le loader se chargeait sur la zone RAM réservée au retour de la routine de chargement.



Résultat

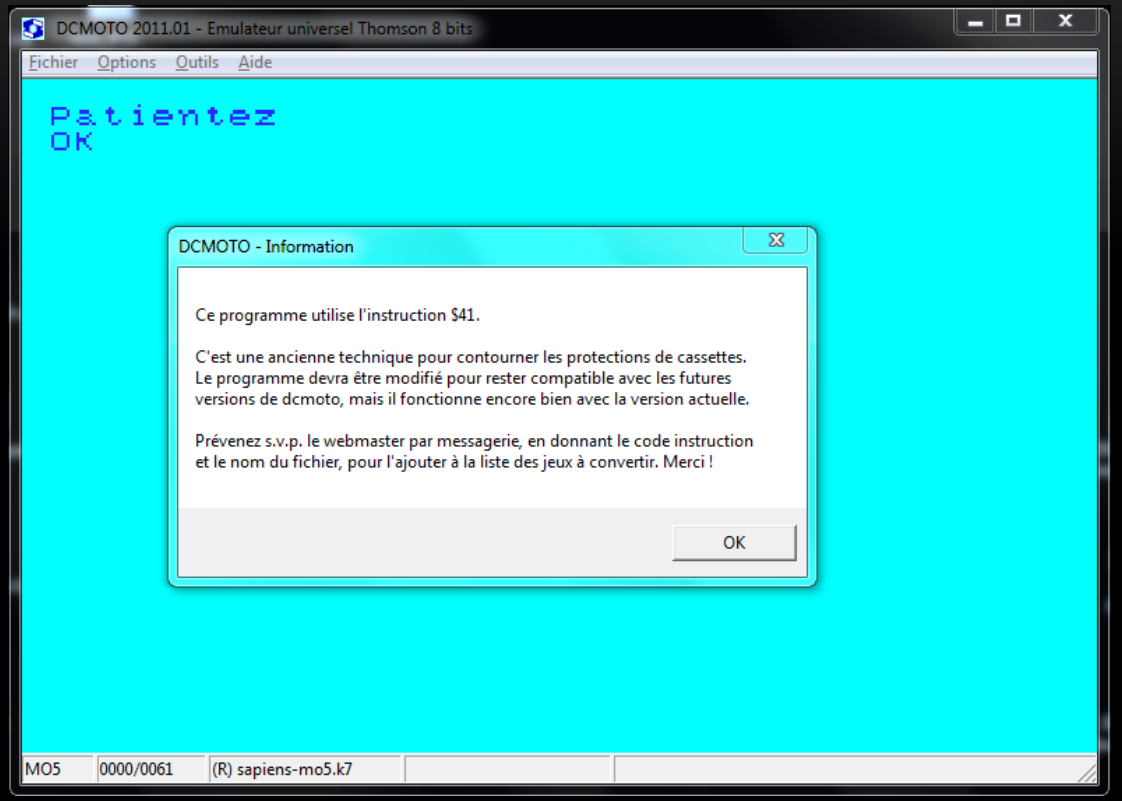
➔ Ecrasement du pointeur retour

➔ Buffer overflow et prise de contrôle du MO5 par le loader…

LA ROUTINE DE CHARGEMENT…

- **Fast-Loader**
- ➔ Routine propriétaire

- **Instructions $41 et $42**
- ➔ Opcodes illégaux



L'art de sécuriser un système !

C'ÉTAIT ASSEZ MYSTÉRIEUX… ET PASSIONNANT

- Ca donnait envie de chercher, de comprendre.

erratum apple

Il manquait dans le listing de Fast Boot Maker du numéro 79 une routine en langage machine. La voici, bien entendu accompagnée de son indispensable Hex-Check. Sauvegardez-la en faisant "BSAVE RWTS.A$ 300.LS 94".

```
0300- 4C 59 FF 4C 06 03 20 E3  0300-  ($60)
0308- 03 85 06 84 05 A5 00 A0  0308-  ($04)
0310- 04 91 05 A5 01 C9 10 90  0310-  ($7D)
0318- 04 A9 00 85 01 A0 05 91  0318-  ($1D)
0320- 05 A9 00 A0 08 91 05 A5  0320-  ($35)
0328- 03 C8 91 05 A5 02 C9 03  0328-  ($32)
0330- 90 04 A9 00 85 02 A0 0C  0330-  ($16)
0338- 91 05 A9 00 A0 03 91 05  0338-  ($0A)
0340- 48 A9 21 85 24 A9 17 85  0340-  ($5A)
0348- 25 20 22 FC AD EC B7 20  0348-  ($0D)
0350- DA FD 20 F4 FB A0 ED B7  0350-  ($FF)
0358- 20 DA FD 18 A0 F4 B7 A9  0358-  ($98)
0360- B0 80 F7 07 20 E4 FB 4E  0360-  ($9A)
0368- 20 E3 03 20 D9 03 B0 1B  0368-  ($91)
0370- A9 00 85 48 E6 01 A5 01  0370-  ($27)
0378- C9 10 D0 06 A9 00 85 01  0378-  ($22)
0380- E6 00 E6 03 A5 03 C5 04  0380-  ($64)
0388- 90 07 60 20 3A FF 4C 66  0388-  ($38)
03A0- 00 1B 00 1C 1D 1E FF FF  0390-  ($9C)
```

Et à ce moment là, il y avait HEBDOGICIEL LE 1er HEBDOMADAIRE QUI CRACHE DANS LA SOUPE INFORMATIQUE

IL FALLAIT APPRENDRE SUR LE TAS

FAST BOOT MAKER

Vous vous êtes souvent plaint de la lenteur du système d'exploitation. Voici un programme qui vous permet d'accélérer considérablement la vitesse de chargement.

Frédéric MUTTER

Mode d'emploi :

Tapez les listings 1, 2, et 3 en les sauvegardant respectivement sous les noms FASTBOOT MAKER, BOOT 0 et BOOT 1. Les listings 2 et 3 sont accompagnés de leur vérificateur (HEX-CHECK). Pour faire démarrer le programme, taper RUN FASTBOOT MAKER.

Option 1 : Crée une disquette FASTBOOT en demandant un fichier contenant une image de présentation pour le lancement. Il peut y être inscrit par exemple 'Tapez sur la barre d'espace pour continuer', ou A Aventure P Pac-man, etc...

Option 2 : Met sur la disquette FASTBOOT les fichiers binaires (uniquement). Il faut pour cela donner l'adresse de départ en decimal. Cette adresse est trouvée de la façon suivante : BLOAD nom du programme et PRINT PEEK (43634)+ PEEK(43635)* 256.

Option 3 : Effectue le catalogue de la disquette FASTBOOT, et permet de reprendre ses fichiers sous DOS 3.3 normal. Le catalogue est présenté de la façon suivante :

Numéro du programme Touche correspondante Longueur Piste et Secteur

Pour reprendre les fichiers, taper le numéro correspondant et le programme demandera alors sous quel nom vous désirez le sauvegarder.

Option 4 : Fait le catalogue d'une disquette normale sous DOS 3.3

Option 5 : Quitte le programme.

LISTING 1

```
5  REM FASTBOOT MAKER V3.1(C)198
   5  PAR MUTTER FREDERIC
20  TEXT : HOME : INVERSE : PRINT
   "FASTBOOT MAKER PAR MUTTER "
   (C)85-PARIS-$": NORMAL : POKE
   40286,102: POKE 40287,213: ONERR
    GOTO 430
30 D$ =  CHR$ (13) + CHR$ (4): IF
    PEEK (768) <  > 76 OR  PEEK
   (771) <  > 76 THEN  PRINT D$
   ;"BLOAD RWTS"
40  VTAB 7: PRINT "1)Creation d'
   une disquette.....FAST BOOT"

50  PRINT : PRINT "2)Mettre un f
   ichier binaire en.FAST BOOT"

60  PRINT : PRINT "3)Catalogue d
   e la disquette....FAST BOOT"

   00":X =  PEEK (43617): IF  PEEK
   (43616) = 0 THEN X = X - 1
310  VTAB 10: INPUT "adresse de
    depart (dec):";A
320  PRINT : INPUT "Piste:";B: INPUT
   "Secteur:";C: IF B < 3 OR C <
   0 OR C > 17 GOTO 320
330  PRINT : PRINT "touche pour
   le charger:";: GET F$: PRINT
   F$: PRINT "classement (1 a 1
   0):";: GET G: PRINT G
340  VTAB 17: HTAB 12: PRINT "C'
   est bon ?";: GET X$: IF X$ =
   "O" THEN 360
350  RUN
360  HOME : VTAB 12: PRINT "Mett
   ez votre disquette dans le l
   ecteur  et defoncez une touc
   he";: GET C$
370 TR = B:ST = C:DR = 2:PI = 22
   :P2 = X + 23: GOSUB 460
380 TR = 0:ST = P:DR = 1:PI = 49
   :P2 = 50: GOSUB 460
390  POKE 12543 + G,X + 1: POKE
   12575 + G,B: POKE 12607 + G,
   gramme:";N$: PRINT : PRINT "
   Inserer votre disquette DOS
   3.3";: GET R$: PRINT D$;"BSA
   VE";N$;",A5632,L";P: HOME : VTAB
   11: INVERSE
530  PRINT "ATTENTION PROGRAMME
   SAUVE EN A$1600": POKE 49168
   ,0: PRINT : PRINT "FAITES:":
    NORMAL : PRINT : PRINT "$BL
   OAD ";N$;" ,A";B(A): PRINT "
   $BSAVE ";N$;" ,A";B(A);",L";
   P: PRINT : PRINT "MDI,JE FAT
   IGUE ALORS ((THE END))": VTAB
   14: END
```

LISTING 2

Hex-Check

```
0800- 01 E8 48 A9 62 20 80 08   (0EF)
0808- AF B4 85 27 B0 BC C0 10   (0FC)
0810- F8 49 D5 D0 F7 B0 BC C0   (0E1)
0818- 10 FB C9 AA D0 F3 B0 BC   (19A)
0820- C0 10 FB C9 A5 D0 EA A9   (0DC)
0828- 00 A0 56 84 3C BC BC C0   (08E)
0830- 10 FB 59 D6 02 A4 3C 88   (07A)
0838- 99 00 03 D0 EE 84 3C BC   (0A0)
```

```
0990- 02 01 EC 00 00 03 E0 02   (032)
0998- 00 03 EE 01 00 03 EF 03   (033)
09A0- 00 03 F2 00 02 03 F3 02   (021)
09A8- 02 03 F4 01 02 03 F5 03   (033)
09B0- 02 03 F6 00 01 03 F7 02   (003)
09B8- 01 03 F9 01 01 03 FA 03   (011)
09C0- 01 03 FB 00 03 03 FC 02   (027)
09C8- 03 03 FD 01 03 03 FE 03   (011)
09D0- 03 03 FF A0 51 BA 20 98   (022)
09D8- B7 A5 01 38 E0 49 BA 85   (080)
09E0- 01 AC 49 BA 98 18 65 01   (0B6)
09E8- 8E 29 BA 90 29 BA C8 CC   (037)
09F0- AA BA 90 F1 90 EE A6 28   (033)
09F8- A9 60 85 02 C6 02 F0 25   (05F)
0A00- 10 FB C9 AA D0 F2 A0 53   (029)
0A08- A0 EC C0 10 F8 C9 96 D0   (0E5)
0A10- E7 A9 10 85 27 A0 EC C0   (0A0)
0A18- 10 FB 24 85 26 A0 EC C0   (0E3)
0A20- 10 FB 25 26 99 2C 05 45   (018)
0A28- 27 88 10 E7 A0 00 B7 A0   (03A)
0A30- EC C0 10 FB C9 DE D0 AE   (04E)
0A38- DA A0 EC C0 10 FB C9 AA   (0E3)
0A40- 00 A4 1B 40 FF FF FF DF   (02C)
0A48- AA D5 AA D5 AA D5 FF FF   (07F)
0A50- FF FF FF 00 00 00 00 00   (0FF)
0A58- 00 00 00 00 00 00 00 00   (000)
0A60- 00 00 00 00 00 00 00 00   (000)
0A68- 00 00 24 98 99 98 8C 9C   (09D)
0A70- 18 14 18 A0 A1 A2 A3 A4   (0B8)
0A78- A5 1C 20 AB A9 AA 24 28   (03C)
0A80- 2C 30 34 B0 B1 38 3C 40   (04D)
0A88- 44 48 4C B8 B9 54 58 5C   (0FB)
```

IL FALLAIT APPRENDRE SUR LE TAS

FAST BOOT MAKER

Vous vous êtes souvent plaint de la lenteur du système d'exploitation. Voici un programme qui vous permet d'accélérer considérablement la vitesse de chargement.

Frédéric MUTTER

Mode d'emploi :

Tapez les listings 1, 2, et 3 en les sauvegardant respectivement sous les noms FASTBOOT MAKER, BOOT 0 et BOOT 1. Les listings 2 et 3 sont accompagnés de leur vérificateur (HEX-CHECK). Pour faire démarrer le programme, taper RUN FASTBOOT MAKER.

Option 1 : Crée une disquette FASTBOOT en demandant un fichier contenant une image de présentation pour le lancement. Il peut y être inscrit par exemple 'Tapez sur la barre d'espace pour continuer', ou A Aventure P Pac-man, etc...

Option 2 : Met sur la disquette FASTBOOT les fichiers binaires (uniquement). Il faut pour cela donner l'adresse de départ en decimal. Cette adresse est trouvée de la façon suivante : BLOAD nom du programme et PRINT PEEK (43634)+ PEEK(43635)* 256.

Option 3 : Effectue le catalogue de la disquette FASTBOOT, et permet de reprendre ses fichiers sous DOS 3.3 normal. Le catalogue est présenté de la façon suivante :

Numéro du programme Touche correspondante Longueur Piste et Secteur

Pour reprendre les fichiers, taper le numéro correspondant et le programme demandera alors sous quel nom vous désirez le sauvegarder.

Option 4 : Fait le catalogue d'une disquette normale sous DOS 3.3

Option 5 : Quitte le programme.

LISTING 1

```
5  REM FASTBOOT MAKER V3.1(C)198
   5  PAR MUTTER FREDERIC
20  TEXT : HOME : INVERSE : PRINT
   "FASTBOOT MAKER PAR MUTTER "
   (C)85-PARIS-$": NORMAL : POKE
   40286,102: POKE 40287,213: ONERR
    GOTO 430
30 D$ =  CHR$ (13) +  CHR$ (4): IF
    PEEK (768) <  > 76 OR  PEEK
   (771) <  > 76 THEN  PRINT D$
   ;"BLOAD RWTS"
40  VTAB 7: PRINT "1)Creation d'
   une disquette.....FAST BOOT"

50  PRINT : PRINT "2)Mettre un f
   ichier binaire en.FAST BOOT"

60  PRINT : PRINT "3)Catalogue d
   e la disquette....FAST BOOT"

   00":X =  PEEK (43617): IF  PEEK
   (43616) = 0 THEN X = X - 1
310  VTAB 10: INPUT "adresse de
    depart (dec):";A
320  PRINT : INPUT "Piste:";B: INPUT
   "Secteur:";C: IF B < 3 OR C <
   0 OR C > 17 GOTO 320
330  PRINT : PRINT "touche pour
   le charger:";: GET F$: PRINT
   F$: PRINT "classement (1 a 1
   0):";: GET G: PRINT G
340  VTAB 17: HTAB 12: PRINT "C'
   est bon ?";: GET X$: IF X$ =
   "O" THEN 360
350  RUN
360  HOME : VTAB 12: PRINT "Mett
   ez votre disquette dans le l
   ecteur  et defoncez une touc
   he";: GET C$
370 TR = B:ST = C:DR = 2:P1 = 22
   :P2 = X + 23: GOSUB 460
380 TR = 0:ST = 9:DR = 1:P1 = 49
   :P2 = 50: GOSUB 460
390  POKE 12543 + G,X + 1: POKE
   12575 + G,B: POKE 12607 + G,
   gramme:";N$: PRINT : PRINT "
   Inserer votre disquette DOS
   3.3";: GET R$: PRINT D$;"BSA
   VE";N$;",A$632,L";P: HOME : VTAB
   11: INVERSE
530  PRINT "ATTENTION PROGRAMME
   SAUVE EN A$1600": POKE 49168
   ,0: PRINT : PRINT "FAITES:":
    NORMAL : PRINT : PRINT "BL
   OAD ";N$;",A";B(A): PRINT "
   $BSAVE ";N$;",A";B(A);",L";
   P: PRINT : PRINT "MDI,JE FAT
   IGUE ALORS ((THE END))": VTAB
   14: END
```

LISTING 2

Hex-Check

```
0800- 01 E8 48 A9 62 20 8D D8   (0EF)
0808- AF B4 85 27 80 BC C0 10   (0FC)
0810- F8 49 D5 D0 F7 BD BC C0   (0E1)
0818- 10 FB C9 AA D0 F3 B0 BC   (19A)
0820- C0 10 FB C9 A5 D0 EA A9   (0DC)
0828- 00 A0 56 84 3C BC BC C0   (08E)
0830- 10 FB 59 D6 02 A4 3C 88   (07A)
0838- 99 00 03 D0 EE 84 3C BC   (0A0)
```

```
0990- 02 01 EC 00 00 03 E0 02   (032)
0998- 00 03 EE 01 00 03 EF 03   (033)
09A0- 00 03 F2 00 02 03 F3 02   (021)
09A8- 02 03 F4 01 02 03 F5 03   (033)
09B0- 02 03 F6 00 01 03 F7 02   (000)
09B8- 01 03 F9 01 01 03 FA 03   (011)
09C0- 01 03 FB 00 03 03 FC 02   (027)
09C8- 03 03 FD 01 03 03 FE 03   (011)
09D0- 03 03 FF A0 51 BA 20 98   (022)
09D8- B7 A5 01 38 E0 4F BA 85   (080)
09E0- 01 AC 4F BA 98 18 65 01   (0B6)
09E8- EE 2F BA F0 3F BA C8 CC   (037)
09F0- AA BA F0 F1 90 EE A6 28   (033)
09F8- AF A0 05 02 C6 02 F0 25   (05F)
0A00- 10 FB C9 AA D0 F2 A0 53   (029)
0A08- A0 EC C0 10 F8 C9 96 D0   (0E5)
0A10- E7 A9 10 85 27 A0 EC C0   (040)
0A18- 10 FB 24 85 26 A0 EC C0   (0E3)
0A20- 10 FB 25 26 99 2C 05 45   (018)
0A28- 27 88 10 E7 A0 00 B7 A0   (03A)
0A30- EC C0 10 FB C9 DE D0 AE   (04E)
0A38- DA A0 EC C0 10 FB C9 AA   (0E3)
0A40- 00 A4 1B 40 FF FF FF DF   (02C)
0A48- AA D5 AA D5 AA D5 FF FF   (07F)
0A50- FF FF FF 00 00 00 00 00   (0FF)
0A58- 00 00 00 00 00 00 00 00   (000)
0A60- 00 00 00 00 00 00 00 00   (000)
0A68- 00 00 24 98 99 98 8C 9C   (0D0)
0A70- 18 14 18 A0 A1 A2 A3 A4   (080)
0A78- A5 1C 20 AB A9 AA 24 28   (03C)
0A80- 2C 30 34 B0 B1 38 3C 40   (04D)
0A88- 44 48 4C B8 B9 74 78 7C   (0F8)
```

IL FALLAIT APPRENDRE SUR LE TAS

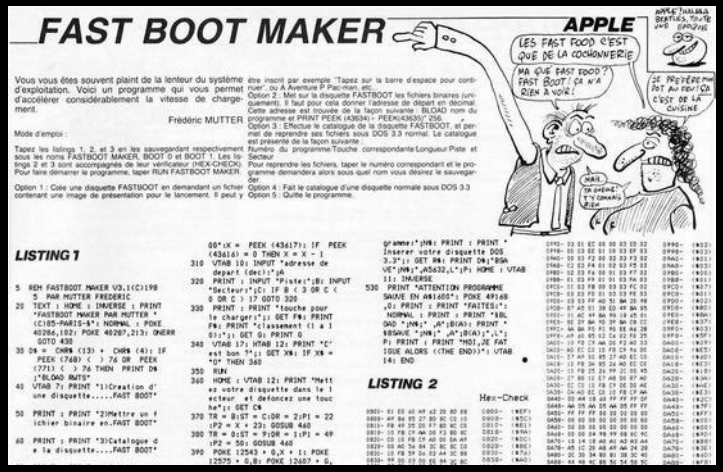
Et maîtriser (dans l'ordre)

- PEEK et POKE
- L'hexadécimal
- Le langage machine

… et enfin seulement,

- L'assembleur !

```
390  POKE 12543 + G,X + 1: POKE
     12575 + G,B: POKE 12607 + G,
     C: POKE 12671 + G,A / 256: POKE
     12639 + G,A - 256 *  PEEK (1
     2671 + G): POKE 12735 + G,A /
     256: POKE 12703 + G,A - 256 *
      PEEK (12735 + G): POKE 1276
     7 + G, ASC (F$) + 128
400 TR = 0:ST = 9:DR = 2:P1 = 49
     :P2 = 50: GOSUB 460
410 A =  INT (X / 16):C = C + X -
     A * 16: HOME : VTAB 12: PRINT
     "Le prochain programme doit
     etre mis sur": HTAB 8: PRINT
     "la piste:";A + B;" / secteu
     r:";C + 1: GET A$: RUN
420  HOME : VTAB 12: PRINT "Inse
     rez votre disquette dans le
     lecteur";: GET A$: PRINT D$;
     "CATALOG": PRINT "une touche
      pour revenir au menu:";: GET
     A$: RUN
```



FAST BOOT MAKER

APPLE

Vous vous êtes souvent plaint de la lenteur du système d'exploitation. Voici un programme qui vous permet d'accélérer considérablement la vitesse de chargement.

Frédéric MUTTER

Mode d'emploi :

Tapez les listings 1, 2, et 3 en les sauvegardant respectivement sous les noms FASTBOOT MAKER, BOOT 0 et BOOT 1. Les listings 2 et 3 sont accompagnés de leur vérificateur (HEX-CHECK). Pour faire démarrer le programme, taper RUN FASTBOOT MAKER.

Option 1 : Crée une disquette FASTBOOT en demandant un fichier contenant une image de présentation pour le lancement. Il peut y être inscrit par exemple : 'Tapez sur la barre d'espace pour continuer' ou 'A Aventure P Pac-man, etc.

Option 2 : Met sur la disquette FASTBOOT les fichiers binaires (uniquement). Il faut pour cela donner l'adresse de départ en décimal. Cette adresse est trouvée de la façon suivante : BLOAD nom du programme et PRINT PEEK (43634) + PEEK(43635)*256.

Option 3 : Effectue le catalogue de la disquette FASTBOOT, et permet de reprendre ses fichiers sous DOS 3.3 normal. Le catalogue est présenté de la façon suivante :
Numéro du programme/Touche correspondante/Longueur/Piste et Secteur
Pour reprendre les fichiers, taper le numéro correspondant et le programme demandera alors sous quel nom vous désirez le sauvegarder.

Option 4 : Fait le catalogue d'une disquette normale sous DOS 3.3

Option 5 : Quitte le programme.

LES FAST FOOD C'EST QUE DE LA COCHONNERIE

MA QUE FAST FOOD? FAST BOOT! ÇA N'A RIEN À VOIR!

JE PRÉFÈRE MANGER AU FOU! ÇA C'EST DE LA CUISINE

HAIE TA GUEULE T'Y CONNAIS RIEN

LISTING 1

```
5  REM FASTBOOT MAKER V3.1(C)198
   5  PAR MUTTER FREDERIC
20 TEXT : HOME : INVERSE : PRINT
   "FASTBOOT MAKER PAR MUTTER "
   (C)85-PARIS-5": NORMAL : POKE
   40286,102: POKE 40287,213: ONERR
    GOTO 430
30 D$ = CHR$ (13) + CHR$ (4): IF
    PEEK (768) <  > 76 OR  PEEK
   (771) <  > 76 THEN  PRINT D$
   ;"BLOAD RWTS"
40 VTAB 7: PRINT "1)Creation d'
   une disquette....FAST BOOT"

50 PRINT : PRINT "2)Mettre un f
   ichier binaire en.FAST BOOT"

60 PRINT : PRINT "3)Catalogue d
   e la disquette....FAST BOOT"

80 X = PEEK (43617): IF  PEEK
   (43616) = 0 THEN X = X - 1
310 VTAB 10: INPUT "adresse de
    depart (dec):";A
320 PRINT : INPUT "Piste:";B: INPUT
    "Secteur:";C: IF B < 3 OR C <
    0 OR C > 17 GOTO 320
330 PRINT : PRINT "touche pour
   le charger";: GET P$: PRINT
   P$: PRINT "(t)assement (1 a 1
   0):";: GET G: PRINT G
340 VTAB 17: HTAB 12: PRINT "C'
    est bon ?";: GET XN: IF XN =
   "O" THEN 360
350 RUN
360 HOME : VTAB 12: PRINT "Mett
   ez votre disquette dans le l
   ecteur  et dénoncez une touc
   he";: GET C$
370 TR = 0:ST = C:DR = 2:P1 = 22
    :P2 = X + 23: GOSUB 460
380 TR = 0:ST = 9:DR = 1:P1 = 49
    :P2 = 50: GOSUB 460
390  POKE 12543 + G,X + 1: POKE
   12575 + G,B: POKE 12607 + G,
```

```
   gramme":HN: PRINT : PRINT "
   Inserer votre disquette DOS
   3.3";: GET R$: PRINT D$;"BSA
   VE";HN;",A$632,L*1P: HOME : VTAB
    11: INVERSE
530  PRINT "ATTENTION PROGRAMME
   SAUVE EN A$1605": POKE 49168
   ,0: PRINT : PRINT "FAITES";:
    NORMAL : PRINT : PRINT "UBL
   OAD ";HN;" ,A";B(A): PRINT "
   $BSAVE ";HN;" ,A";B(A);",L";
   P: PRINT : PRINT "MOI,JE FAT
   IGUE ALORS ((THE END))": VTAB
    14: END
```

LISTING 2

Hex-Check

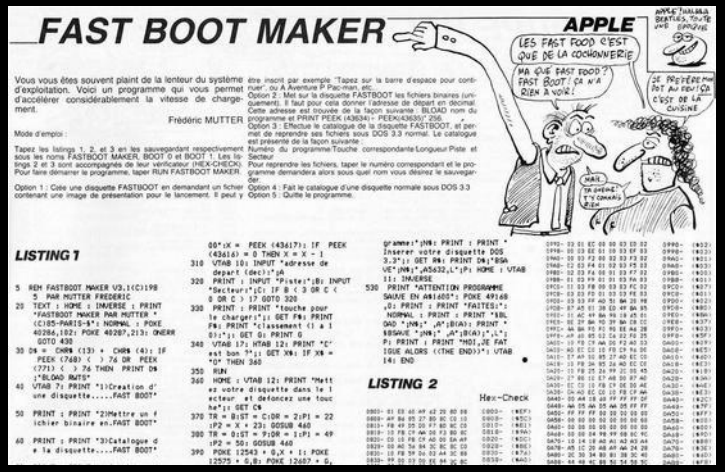
IL FALLAIT APPRENDRE SUR LE TAS

Et maîtriser (dans l'ordre)

- PEEK et POKE
- L'hexadécimal
- Le langage machine

… et enfin seulement,

- L'assembleur !



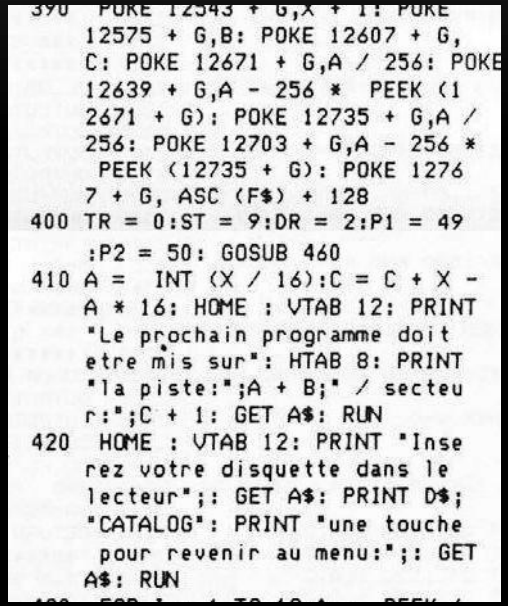
FAST BOOT MAKER

APPLE

LISTING 1

LISTING 2

Hex-Check



```
390  POKE 12543 + G,X + 1: POKE
     12575 + G,B: POKE 12607 + G,
     C: POKE 12671 + G,A / 256: POKE
     12639 + G,A - 256 *  PEEK (1
     2671 + G): POKE 12735 + G,A /
     256: POKE 12703 + G,A - 256 *
      PEEK (12735 + G): POKE 1276
     7 + G, ASC (F$) + 128
400 TR = 0:ST = 9:DR = 2:P1 = 49
     :P2 = 50: GOSUB 460
410 A =  INT (X / 16):C = C + X -
     A * 16: HOME : VTAB 12: PRINT
     "Le prochain programme doit
     etre mis sur": HTAB 8: PRINT
     "la piste:";A + B;" / secteu
     r:";C + 1: GET A$: RUN
420  HOME : VTAB 12: PRINT "Inse
     rez votre disquette dans le
     lecteur";: GET A$: PRINT D$;
     "CATALOG": PRINT "une touche
      pour revenir au menu:";: GET
     A$: RUN
```

LISTING 2

Hex-Check

```
0800- 01 E0 60 A9 62 20 8D 08    0800-  ($EF)
0808- A9 B6 85 27 BD 8C C0 10    0808-  ($5C)
0810- FB 49 D5 D0 F7 BD 8C C0    0810-  ($B1)
0818- 10 FB C9 AA D0 F3 BD 8C    0818-  ($9A)
0820- C0 10 FB C9 AD D0 EA A9    0820-  ($DC)
0828- 00 A0 56 84 3C BC 8C C0    0828-  ($BE)
0830- 10 FB 59 D6 02 A4 3C 88    0830-  ($76)
0838- 99 00 03 D0 EE 84 3C BC    0838-  ($A0)
0840- 8C C0 10 FB 59 D6 02 A4    0840-  ($8E)
0848- 3C 91 26 C8 D0 EF BC 8C    0848-  ($4C)
0850- C0 10 FB 59 D6 02 D0 41    0850-  ($37)
0858- A0 00 A2 56 CA 30 FB B1    0858-  ($E4)
0860- 26 5E 00 03 2A 5E 00 03    0860-  ($0C)
0868- 2A 91 26 C8 D0 EE E6 27    0868-  ($AA)
0870- A2 60 CE EE 08 D0 95 20    0870-  ($8F)
0878- 58 FC A0 27 B9 A4 08 49    0878-  ($7F)
0880- FF 99 00 04 88 10 F5 4C    0880-  ($43)
0888- 00 B6 4C A9 FA 8D F4 03    0888-  ($D3)
0890- AD 51 C0 A9 00 8D F2 03    0890-  ($E9)
0898- A9 C6 8D F3 03 60 F9 F9    0898-  ($72)
08A0- F9 F9 F9 F9 F9 FE EC EB    08A0-  ($00)
08A8- FD F0 F0 EB DF F2 FE F4    08A8-  ($31)
08B0- FA ED DF EF FE ED DF F2    08B0-  ($19)
08B8- EA EB EB FA ED DF F9 ED    08B8-  ($36)
08C0- FA FB FA ED F6 FC DF D7    08C0-  ($14)
08C8- FC D6 C7 CA ED F0 F2 DF    08C8-  ($17)
08D0- EC F3 F0 EB DF E9 F6 DF    08D0-  ($1B)
08D8- D3 DF F9 FD F0 F0 EB DF    08D8-  ($3C)
08E0- FD E6 DF EB ED F0 F3 F3    08E0-  ($32)
08E8- DF D9 DF FC F0 D1 06 FE    08E8-  ($FC)
08F0- A5 25 C9 18 D0 ED A9 04    08F0-  ($C1)
08F8- 85 25 A9 00 85 FE A0 00    08F8-  ($D2)
```

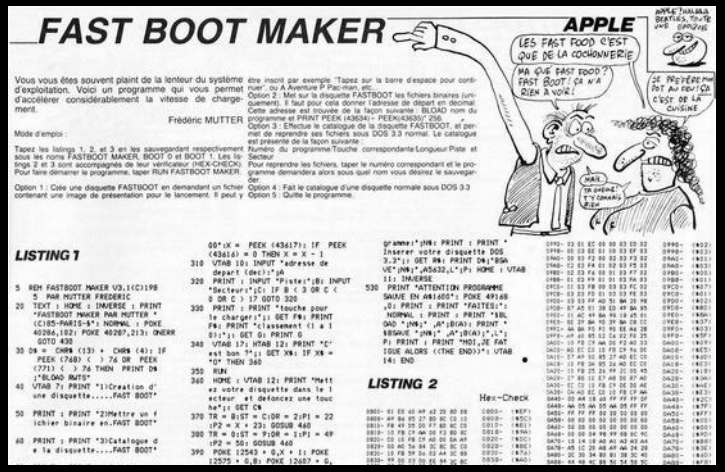
IL FALLAIT APPRENDRE SUR LE TAS

Et maîtriser (dans l'ordre)

- PEEK et POKE
- L'hexadécimal
- Le langage machine

… et enfin seulement,

- L'assembleur !

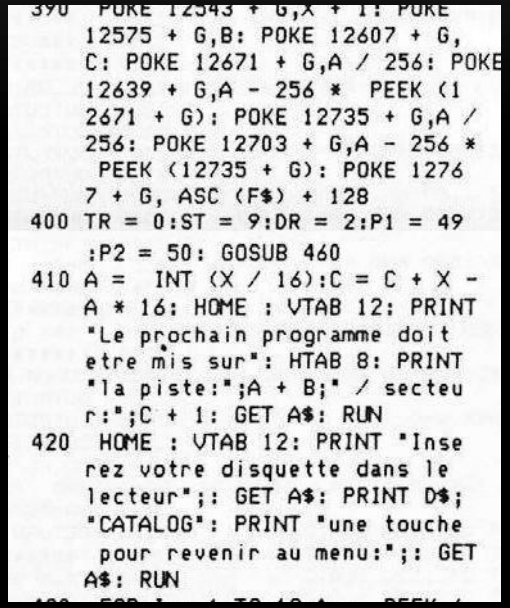

FAST BOOT MAKER

APPLE

LISTING 1

LISTING 2

Hex-Check


```
390  POKE 12543 + G,X + 1: POKE
     12575 + G,B: POKE 12607 + G,
     C: POKE 12671 + G,A / 256: POKE
     12639 + G,A - 256 *  PEEK (1
     2671 + G): POKE 12735 + G,A /
     256: POKE 12703 + G,A - 256 *
      PEEK (12735 + G): POKE 1276
     7 + G, ASC (F$) + 128
400 TR = 0:ST = 9:DR = 2:P1 = 49
     :P2 = 50: GOSUB 460
410 A =  INT (X / 16):C = C + X -
     A * 16: HOME : VTAB 12: PRINT
     "Le prochain programme doit
     etre mis sur": HTAB 8: PRINT
     "la piste:";A + B;" / secteu
     r:";C + 1: GET A$: RUN
420  HOME : VTAB 12: PRINT "Inse
     rez votre disquette dans le
     lecteur";: GET A$: PRINT D$;
     "CATALOG": PRINT "une touche
      pour revenir au menu:";: GET
     A$: RUN
```

Ca formait l'esprit !!!


LISTING 2

Hex-Check

0800-	01	E0	60	A9	62	20	8D	08	0800-	($EF)
0808-	A9	B6	85	27	BD	8C	C0	10	0808-	($5C)
0810-	FB	49	D5	D0	F7	BD	8C	C0	0810-	($B1)
0818-	10	FB	C9	AA	D0	F3	BD	8C	0818-	($9A)
0820-	C0	10	FB	C9	AD	D0	EA	A9	0820-	($DC)
0828-	00	A0	56	84	3C	BC	8C	C0	0828-	($BE)
0830-	10	FB	59	D6	02	A4	3C	88	0830-	($76)
0838-	99	00	03	D0	EE	84	3C	BC	0838-	($A0)
0840-	8C	C0	10	FB	59	D6	02	A4	0840-	($8E)
0848-	3C	91	26	C8	D0	EF	BC	8C	0848-	($4C)
0850-	C0	10	FB	59	D6	02	D0	41	0850-	($37)
0858-	A0	00	A2	56	CA	30	FB	B1	0858-	($E4)
0860-	26	5E	00	03	2A	5E	00	03	0860-	($0C)
0868-	2A	91	26	C8	D0	EE	E6	27	0868-	($AA)
0870-	A2	60	CE	EE	08	D0	95	20	0870-	($8F)
0878-	58	FC	A0	27	B9	A4	08	49	0878-	($7F)
0880-	FF	99	00	04	88	10	F5	4C	0880-	($43)
0888-	00	B6	4C	A9	FA	8D	F4	03	0888-	($D3)
0890-	AD	51	C0	A9	00	8D	F2	03	0890-	($E9)
0898-	A9	C6	8D	F3	03	60	F9	F9	0898-	($72)
08A0-	F9	F9	F9	F9	F9	FE	EC	EB	08A0-	($00)
08A8-	FD	F0	F0	EB	DF	F2	FE	F4	08A8-	($31)
08B0-	FA	ED	DF	EF	FE	ED	DF	F2	08B0-	($19)
08B8-	EA	EB	EB	FA	ED	DF	F9	ED	08B8-	($36)
08C0-	FA	FB	FA	ED	F6	FC	DF	D7	08C0-	($14)
08C8-	FC	D6	C7	CA	ED	F0	F2	DF	08C8-	($17)
08D0-	EC	F3	F0	EB	DF	E9	F6	DF	08D0-	($1B)
08D8-	D3	DF	F9	FD	F0	F0	EB	DF	08D8-	($3C)
08E0-	FD	E6	DF	EB	ED	F0	F3	F3	08E0-	($32)
08E8-	DF	D9	DF	FC	F0	D1	06	FE	08E8-	($FC)
08F0-	A5	25	C9	18	D0	ED	A9	04	08F0-	($C1)
08F8-	85	25	A9	00	85	FE	A0	00	08F8-	($D2)

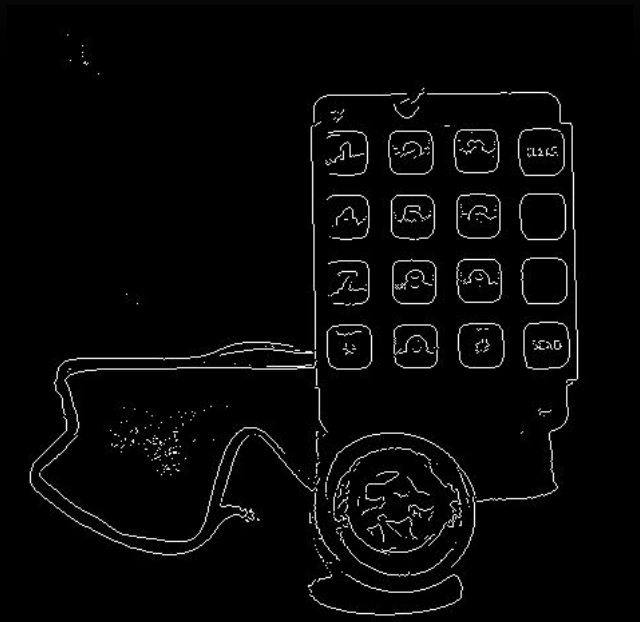
Un nouveau phénomène arrivait…

ET PENDANT CE TEMPS

LES PIRATES DÉBARQUAIENT AUX USA

Les Phreakers

Steve Wozniak… et sa BlueBox



```
----------------------------------------
****************************************
----------------------------------------
  - WHAT CAN I DO WITH A BLUEBOX ? -
----------------------------------------
WELL, YOU CAN DIAL NEARLY ALL NUMBER'S
WORLDWIDE! - YOU CAN GET UN-LISTED
NUMBER'S FROM ANY COUNTRY AND YOU CAN
DIAL WITH OPERATOR STATUS (REAL FUNNY)

YOU'LL KNOW: HOW TO DO THAT ?
REALLY SIMPLE, I'LL TRY TO EXPLAIN
YOU, HOW TO DO THAT!?!

IF YOU PLAN, TO USE US-OPERATOR'S !
PLEASE, READ THE OTHER NICE FILE'S
AVAILABLE AROUND THE GLOBE! IN ALL
GOOD P/H/A-BOARD'S...
ABOUT: HOW TO USE US-OPERATOR'S!

        - SEIZING A THRUNK -
(WRITTEN FOR PHREAKS FROM GERMNAY)
----------------------------------
FOR CALLING VIA:       FREQUENCIES:
----------------------------------
ALGERIA                      2000 Hz
ARGENTINA                    3825 Hz
AUSTRALIA                600& 750 Hz
                        (SEPERATE)
AUSTRIA                      2280 Hz
BAHAMAS                      2600 Hz
BANGLADESH                   3825 Hz
BRAZIL                       3825 Hz
BURUNDI                      3825 Hz
CAMEROON                     3825 Hz
CANADA                       2600 Hz
CHILE                        3825 Hz
CUBA                    2100/3825 Hz
CYPRUS                       3825 Hz
CZECHOSLOVAKIA               2280 Hz
DENMARK                 3000/3825 Hz
DOMINICAN REP.               2600 Hz
FIJI                         3825 Hz
FRANCE                  2280/3850 Hz
GHANA                        3825 Hz
HUNGARY                 2280/3825 Hz
INDIA                        2400 Hz
IRAQ                         3825 Hz
(ONLY, WHEN YOU FIND A NUMBER AFTER
 THE GULF-WAR IN 1991 - HAHA!)
IRELAND                 2040/2400 Hz
                    COMPOUND 2280 Hz
ISRAEL                       3850 Hz
ITALY                   2040/2400 Hz
                  COMPOUND & SEPERATE
JAMAICA                      2600 Hz
JORDAN                       3825 Hz
KENIA                   2040/2400 Hz
KOREA                        3825 Hz
LIBERIA                      3825 Hz
LUXEMBOURG                   3825 Hz
MADAGASCAR                   2280 Hz
MOROCCO                      2280 Hz
MOZAMBIQUE                   2400 Hz
```

C'ÉTAIT LE DÉBUT DE LA SSI… D'UNE CERTAINE MANIÈRE !


HEBDOGICIEL

N° 107

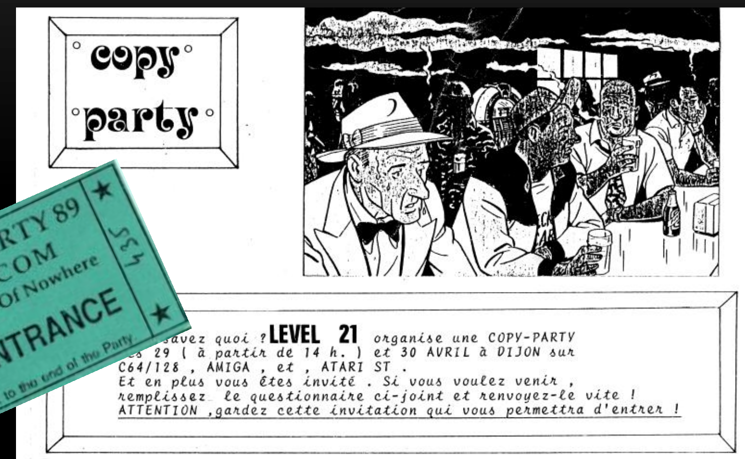
le premier journal d'informatique pirates je vous aime.

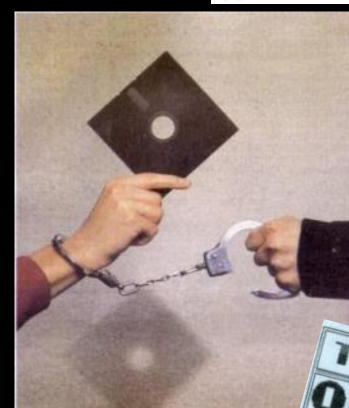
10 F

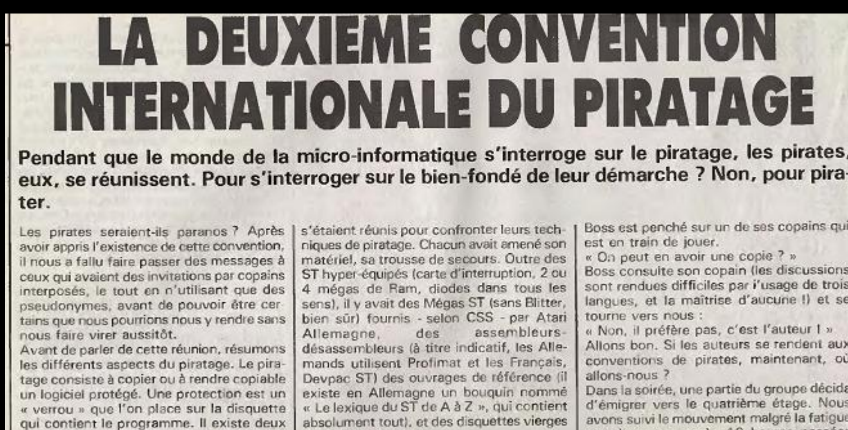
CENTRE MONDIAL DE PIRATAGE

Le Centre Mondial d'Informatique sis à Paris a deux avantages : on y manipule gratuitement toutes sortes d'ordinateurs et on y pirate à tout va. Avec votre argent, espèce de contribuable.

CULTURE MONDIALE






LA DEUXIEME CONVENTION INTERNATIONALE DU PIRATAGE

Pendant que le monde de la micro-informatique s'interroge sur le piratage, les pirates, eux, se réunissent. Pour s'interroger sur le bien-fondé de leur démarche ? Non, pour pirater.

Les pirates seraient-ils paranos ? Après avoir appris l'existence de cette convention, il nous a fallu faire passer des messages à ceux qui avaient des invitations par copains interposés, le tout en n'utilisant que des pseudonymes, avant de pouvoir être certains que nous pourrions nous y rendre sans nous faire virer aussitôt.
Avant de parler de cette réunion, résumons les différents aspects du piratage. Le piratage consiste à copier ou à rendre copiable un logiciel protégé. Une protection est un « verrou » que l'on place sur la disquette qui contient le programme. Il existe deux façons de passer outre cette protection :

s'étaient réunis pour confronter leurs techniques de piratage. Chacun avait amené son matériel, sa trousse de secours. Outre des ST hyper-équipés (carte d'interruption, 2 ou 4 mégas de Ram, diodes dans tous les sens), il y avait des Mégas ST (sans Blitter, bien sûr) fournis - selon CSS - par Atari Allemagne, des assembleurs-désassembleurs (à titre indicatif, les Allemands utilisent Profimat et les Français, Devpac ST) des ouvrages de référence (il existe en Allemagne un bouquin nommé « Le lexique du ST de A à Z », qui contient absolument tout), et des disquettes vierges par boîtes de cent.

Boss est penché sur un de ses copains qui est en train de jouer.
« On peut en avoir une copie ? »
Boss consulte son copain (les discussions sont rendues difficiles par l'usage de trois langues, et la maîtrise d'aucune !) et se tourne vers nous :
« Non, il préfère pas, c'est l'auteur ! »
Allons bon. Si les auteurs se rendent aux conventions de pirates, maintenant, où allons-nous ?
Dans la soirée, une partie du groupe décida d'émigrer vers le quatrième étage. Nous avons suivi le mouvement malgré la fatigue grandissante - après 10 heures passées

C'ÉTAIT DÉJÀ LE TEMPS DES RÉSEAUX SOCIAUX !

MINITEL
Rendez-vous des pirates branchés

Ne partez pas, le minitel ne veut pas forcément dire de l'argent foutu en l'air et je vais vous démontrer pourquoi :

Tarif du Télétel 2 - 3614 -

TARIFS	Rouge	Blanc	Bleu	Bleu Nuit
Coût Horaire	22,20	15,60	11,40	7,80

Et pour accompagner ce tarif, je vous conseille de vous brancher sur R-Tel en 3614 (code : 135060318*RTEL).

Vous pourrez y rencontrer tous les pirates de votre ordinateur adoré (Transcom, Babygang, Poltergeist, Squadron, Alcatraz, Megaforce, Wild Copper, Les Nuls, Replicants...).

Au lieu de téléphoner en province, créer une BAL (Boîte à lettre) sur ce

HACKERS Voice

"Le Journal qui Dérange"

Février 1989 — © Stinger/ TRANSCOM — Numéro 4

VIVE LE MINITEL !

Je vous entends déja dire, il n'y a aucun rapport entre le minitel et un skieur, et bien si, car c'est l'époque du ski et en plus je parle du minitel dans ce numéro (quelle coïncidence). Sinon pour le résumé de la copy-party de Venlo, il faut se reporter au CCCP 2, car c'est très détaillé et l'article a été fait par Just-Ice/Ikari. Au fait, j'ai supprimé le concours car cela n'amène pas plus d'articles apparement et puis par pitié, faut pas attendre de recevoir HVoice direct chez soi sans avoir envoyer de timbres. Alors faites un bon geste, envoyez moi vos timbres et des articles par la même occasion, car n'oubliez pas, c'est vous qui faites le journal (enfin presque héhé). Ensuite, j'envisage d'organiser the 3rd Devil's Party en octobre et cette fois-ci, il y aura un Amiga 500 à gagner et pleins d'autres prix. Vous aurez plus de précisions vers le mois de septembre. Enfin en attendant, appréciez ce numéro, ainsi que les prochains qui paraîtront qu'en j'aurais assez d'articles (désolé pour la présentation, faute de place). BYE

STINGER / TRANSCOM

FRENCH CHARTS

1st TRANSCOM

10 th POLTERGEIST
11th SQUADRON
12th YANKEES
13th BABYGANG
14th LEVEL 21

Belle remontée de Squadron et très belle chute de Babygang. Yankees gagne une petite place, Poltergeist et Level 21 restent à leurs anciennes places. Mais attention Poltergeist, ressaisisez-vous !!!

JE VEUX VOTRE FRIC !!!

Hein, quoi ??? Ha c'est à moa ! Bon, bon, bon, vous connaissez l'histoire de la petite fille qui... Ha bon d'accord. Alors là j'ai deux problèmes. D'abord, il faut que j(c'arrive à truander ceux qui me connaissent, mais en plus il faut aussi que j'arnaque les autres. Ca va donner ! Bon, si vous voulez savoir qui je suis, vous regardez en bas à droite de ce texte. Maintenant, pourquoi je suis là et pourquoi je vous emmerde avec mes...???

Si vous le savez pas encore mais vous devriez le savoir, je suis graphiste sur 64 mais aussi sur Amiga. Alors si vous faites partie d'un groupe (style : les jolis et joyeux crackers de France) et que vous voulez faire une démo, alors là je dis STOP. Adressez-vous à un profesionnel (et que c'est vrai, et même que je viens de finir Iron Lord 64, ha que alors !!!). Bon je vous préfère pas dire le prix, parce que sinon vous dijoncteriez. **Enfin, bref, moi Leto II, déclare vendre des dessins pour qui voudra bien m'en acheter** !!!

Maintenant c'est officiel, alors, si vous en voulez un, contactez illico le rédacteur en chef de cette feuille de chou, pardon, je voulais dire de ce superbe et merveilleux ouvrage, merveilleusement imprimé et dont les qualités vous laisseront pantois (NDLR : Je préfère !!!).

Ceci dit, je m'arrête la sinon Stinger va me passer un savon (vous l'aviez compris, c'est lui qu'il faut contacter).

LETO II / CFR

TOUT LE MONDE COPY

Depuis que Stinger et moi avons organisé les 2 premières copy-partys en France digne de ce nom, tous les groupes français veulent à leur tour s'y mettre.

Il y en a de prévu pour les 6 mois à venir. Yankees en fait 2 d'un coup une à Cergy-Pontoise, l'autre à Joeuf en Lorraine. Poltergeist prendrait le relais à St-Etienne, et cela se termine pour l'instant par celle de Level 21 (mais celle-ci est la suite logique de Paris), à moins que OCB entretemps en face une également. Si cela continue, il n'y aura plus assez de vacances scolaires pour assisté à tous ces rendez-vous.

Espérons que les autres groupes comme Babygang, Squadron résisteront à la tentation pour cette première partie de l'année. Pour le moment celle de Paris a semble t'il été la plus réussite. N'étant pas allé à Genève, je m'en remet à ceux qui ont assisté à celle de Paris et de Genève, ils jugeront.

Et évitez de faire une copy-party Amiga vu les problèmes des pirates face à l'APP.

Bon je vous quitte pour cet article en espérant quand même que vous alliez à tous ces rendez-vous, si vous le pouvez.

COBRA / LEVEL 21

News of OCB - Steph/OCB

Nous recherchons un programmeur et un graphiste 64 et nous vous informons qu'un nouveau membre est dans OCB (Ken) et il fait des musiques sur 64, donc attendez-vous à des super démos et intros avec ses musiques. Ensuite nous avons sortis un fanzine "AAARGH Two, the revenge"90 % comique et comprenant des plans, notices de jeux, etc... le tout sur ce bon vieux C64. Pour recevoir un exemplaire, écrivez moi. Et pour finir en beauté, un petit truc de JM/OCB pour Typhoon version TCOM, car ces fumistes n'ont meme pas fait le level-trainer ! (NDLR : OCB n'avait qu'à le cracker !) Enfin heureusement qu'on est là. Bon après avoir chargé le 1er programme faites un Poke2394,0:RUN, il décompacte puis le curseur revient, faites POKE $1094,N° level (1 ≤N° level ≤7) suivi d'un SYS $0c00, et après le 1er Level, vous commencez au level de votre choix. Ben, c'est tout pour aujoud'hui et n'hésitez pas à me contacter.

Une cinquantaine de personnes a la nuit de l'informatique

Récemment, le club informatique de la Cahute a organisé la 2e édition de la nuit de l'informatique. Le local de la Cahute était tout juste suffisant pour accueillir la cinquantaine de mordus qui n'ont pas hésité à passer la nuit pour satisfaire leur passion.

Certains s'étaient déplacés d'Angers, du Mans et même de Paris. On y trouvait différents types de personnalités, des graphistes chargés d'élaborer les images, des programmeurs pour la mise en mouvement mais aussi nombreux curieux. Notons que la plupart s'étaient déplacés avec leur matériel, preuve de leur motivation.

Des participants des 24 heures de l'informatique à la Cahute.

LA NUIT DU HACK. . . IL Y A 20 ANS !

M.C.S.
Demo Party
1991

The M.C.S. Demo Party is coming soon, and you're invited !

It will begin the 16th of february 1991 at 8 PM and will finish the the 17th.

The costs for the two days are 50 FF (food and drink included).

If you come by train : Once arrived in Nantes please call us, and we'll come at the train station to drive you to the place.

If you come by car, once in Nantes, take the direction of "Thouaré" (south-east), and when you'll be there, look for some panels "Le club des jeunes" (young's club). It's clearly indicated. If you want, you can ask people for "La Cahute", since it's the same place.
IF YOU ARE LOST, OR IF YOU WANT TO PHONE US :
GADGET : 40-63-10-81 (ask Bruno)
AXEL FOLLET : 40-48-10-73 (ask Guillaume)
"LA CAHUTE" : 40-72-62-44 (ask Jérome)

There will be many ST's but also some Amigas, a TT (8Mb and 40Mb HD) , an Archimedes (2Mb), PC (386 33Mhz VGA 19'screen), Lynx, Game Boy, and many peripherals for Atari.
If you've got 44Mb cartridges, you can bring them since we've got a 44Mb hard disk. Also there will be 40/80 tracks 5'1/4 disk drive, so you can bring 5'1/4 disks too !

IMPORTANT : This Demo Party has to be a meeting for demo makers and not a copyparty.

GADGET from M.C.S.
M.C.S. is a member of THE ALLIANCE

members of the M.C.S. are:

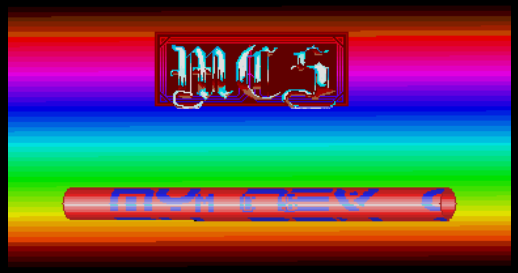
Shark (code/cracking)
Madrom (code/cracking)
Gadget (code/relations/videotex)
Axel follet (swapping/news/hacking/code)
Naish and... Bugs bunny (swapper/graphist)

BYTEBOAT
PARTY

LES 10 ET 11 AVRIL 1993
A NANTES
INVITATION

ON APPRENAIT À PROGRAMMER DES **DEMOS**

(En assembleur, bien évidemment…)



LA SCÈNE DEMOMAKER : HISTORIQUE

A été créée peu après l'apparition des groupes de pirates

1. Nécessité de «marquer» les logiciels distribués

   Programmation d'intros ➔ Animations audiovisuelles

2. Dissociation du jeu et de l'intro

3. Groupement des intros
   ➔ la démo était née

ET LA SÉCURITÉ, LÀ DEDANS ?

Les démos sont très complexes techniquement

- «Pushing the envelope»
  ➔ Invention de méthodes pas prévues par les constructeurs (overscan…)

- Volonté de protéger le code et les routines de la démo
  ➔ Intégration de protections logicielles dans les démos (anti débogage…)

- Gestion des données optimisée
  ➔ Routines disque propriétaire (DMA, formatage spécial, chargement rapide…)
  ➔ Packers (Décompression temps-réel, chiffrement et obfuscation…)

- Programmation «exotique» optimisée
  ➔Code autogénéré, code automodifié…

A. De la sécurité sur MO5 et sur K7

LES PROTECTIONS MO5

PROTECTIONS MO5 ET K7 (1/2)

- **Protection K7 anticopieur**
  Checksum de fin de bloc non standard, algorithme de vérification modifié pour l'accepter.
- **Protection pour programmes en BASIC**
  lignes de plus de 255 octets… l'éditeur ne peut pas les afficher.
- **Protection anti désassemblage**
  Instructions illégales (300 opcodes valides, le reste étant non documenté / invalide)
- **Masquage des routines assembleur**
  Stockage en mémoire vidéo (192 octets dispo)
  Si couleur du texte = couleur du fond (8Ko dispo)

- **Anti fouineurs de mémoire**
  Interdire la commande Basic PEEK() en détournant les vecteurs d'accès au BASIC

Crédit : Daniel Coulon - http://regards.sur.sciences.free.fr/histoire/ordis/protection_cassettes/protection_des_jeux_sur_cassette.htm

PROTECTIONS MO5 ET K7 (2/2)

- **Rootkit sur K7 (!)**
  Bloc de fin de fichier (&FF00) de plus de 2 octets, avec 254 octets de code auto-chargé.
- **Chiffrement du stream K7**
  Avec un simple XOR le plus souvent, routine de décodage protégée par opcodes invalides.
- **Protection anti-chargement K7**
  Blocs K7 non standard, et loader spécifique chargé au début.

- **Rendre le programme invisible sur la K7**
  Modifier la fréquence d'enregistrement des bits (!), plus courts qu'en MFM
  Le lecteur de K7 ne peut les lire sans une routine spéciale.

  0=___/
  1=_/_/

- **Empêcher le chargement (et densifier le stockage)**
  Raccourcir l'intervalle de silence entre les blocs (275 octets) pour «saturer» le CPU.

Crédit : Daniel Coulon - http://regards.sur.sciences.free.fr/histoire/ordis/protection_cassettes/protection_des_jeux_sur_cassette.htm

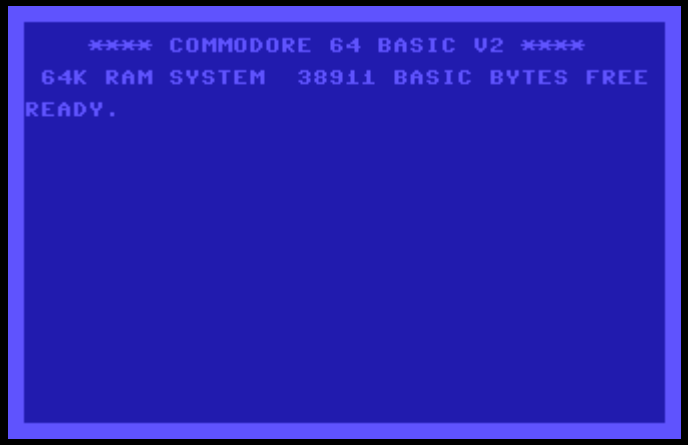
B. De la sécurité sur COMMODORE 64

LES PROTECTIONS C64

LE COMMODORE 64

- 30 millions d'unités vendues
  Processeur : MOS 6510 (8 bits)
  RAM : 64 Ko
  ROM : 20 Ko (8+8+4)
  Vitesse : 1 MHz

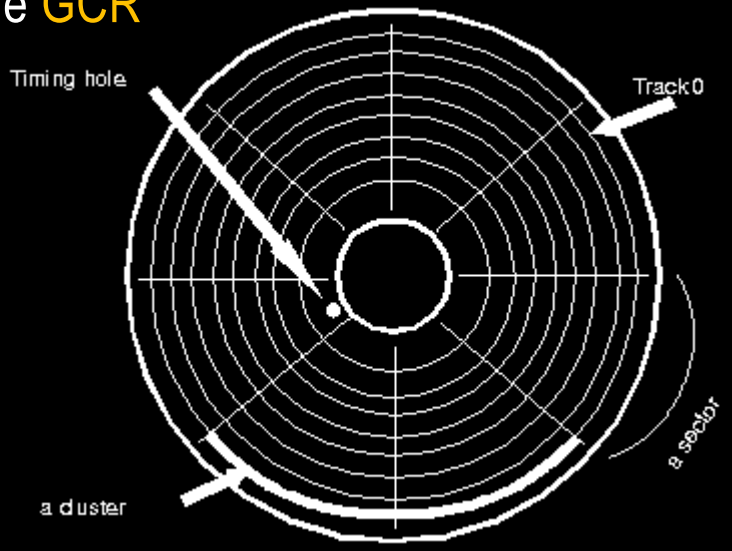
- Très bon processeur son.
  Processeur vidéo correct.
- Matériel robuste et performant (pour l'époque)
- Excellent pour programmer (en assembleur)



Scene demomaker toujours très active en 2011 !

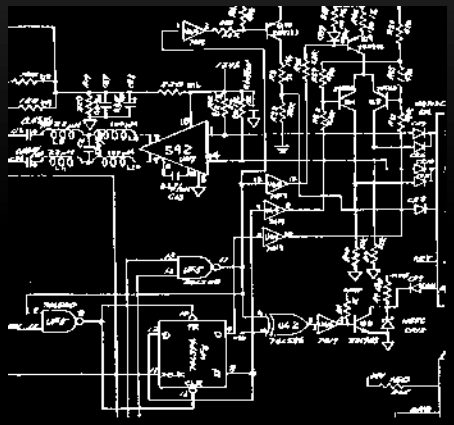
LES DISQUETTES C64

- 170Ko par face, 35 pistes officielles
- Pas de capteur optique de synchro
- Encodage GCR



Piste	Secteurs 256 octets	bits/s
1 - 17	21	307 692
18 - 24	19	285 714
25 - 30	18	266 667
31 – 35	17	250 000
36 – 42	17	250 000 (non standard)

LE LECTEUR DE DISQUETTES 1541



- Processeur : MOS 6502 (8 bits)
  RAM : 2 Ko
  ROM : 16 Ko
  Vitesse : 1 MHz

- Liaison série avec le C64 (très lente)
  Firmware initial : 300 octets/sec
  Firmware custom : >4Ko/sec

- Un vrai C64 en miniature !

De la RAM, une CPU… Ca vous donne des idées ?

LES PROTECTIONS DISQUETTE C64

Charger une routine loader dans le C1541 pour gérer :

- Erreurs physiques (volontaires) sur le disque
- Erreurs de synchronisation (absence de trou)
- Variation de la vitesse du lecteur
- Changer l'encodage GCR (secteurs/piste)
- Ecriture entre les pistes
- Pistes «doubles» («fat tracks»)
- etc.

LES ASTUCES SUR C64

- Découverte d'opcodes non documentés
  (faire du fuzzing*, ce n'est pas nouveau !)*

- Utilisation d'espaces RAM non documentés
  (Les rootkits*, ce n'est pas nouveau !)*

- Utilisation du processeur du lecteur C1541 pour faire des calculs
  *(*CUDA *ce n'est pas nouveau !)*

- Détournement des vecteurs d'interruption logicielles (IRQ)
  (Les hooks *système, ce n'est pas nouveau !)*

- Utilisation du mode trace, etc.

C. De la sécurité sur Atari ST

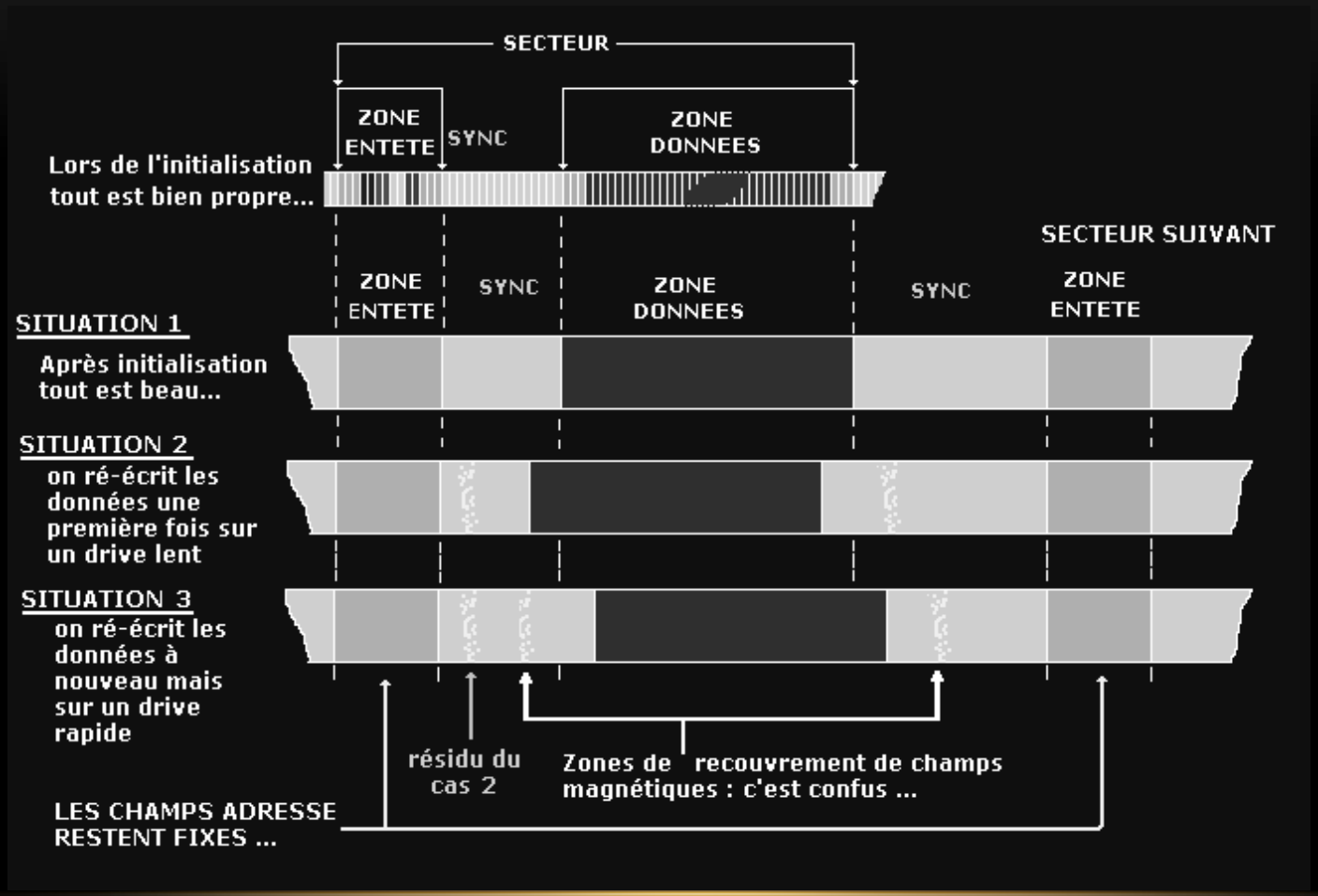
LES PROTECTIONS ATARI ST

L'ATARI ST

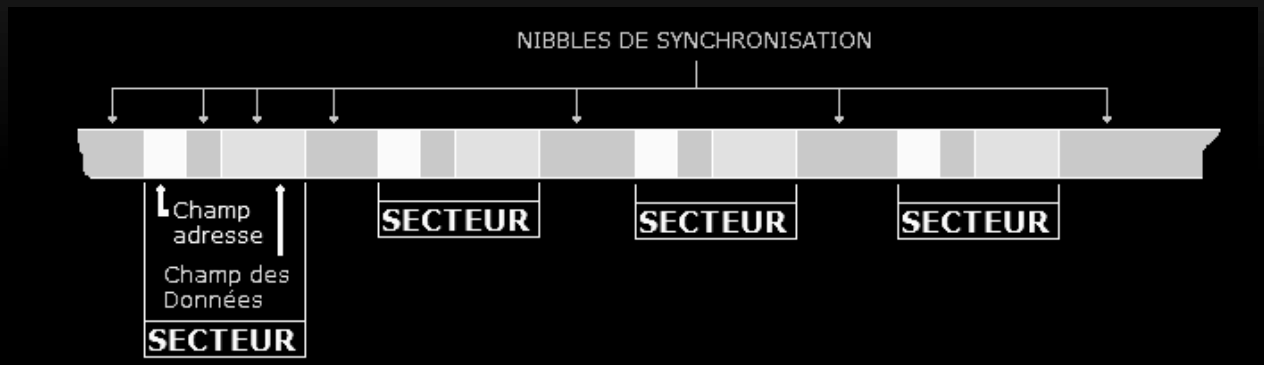
Processeur(s)	: MC 68000 (16 bits)
Contrôleurs mémoire	: Glue, MMU, DMA
Gestionnaire d'interruptions	: MFP 68901
Contrôleur disquettes	: WD 1772
Chipset vidéo	: Shifter
Chipset son	: YM-2149
Chipset MIDI + clavier	: ACIA 6850
Contrôleur clavier	: HD6301V1P
RAM	: 512 / 1024 Ko
Vitesse	: 8MHz

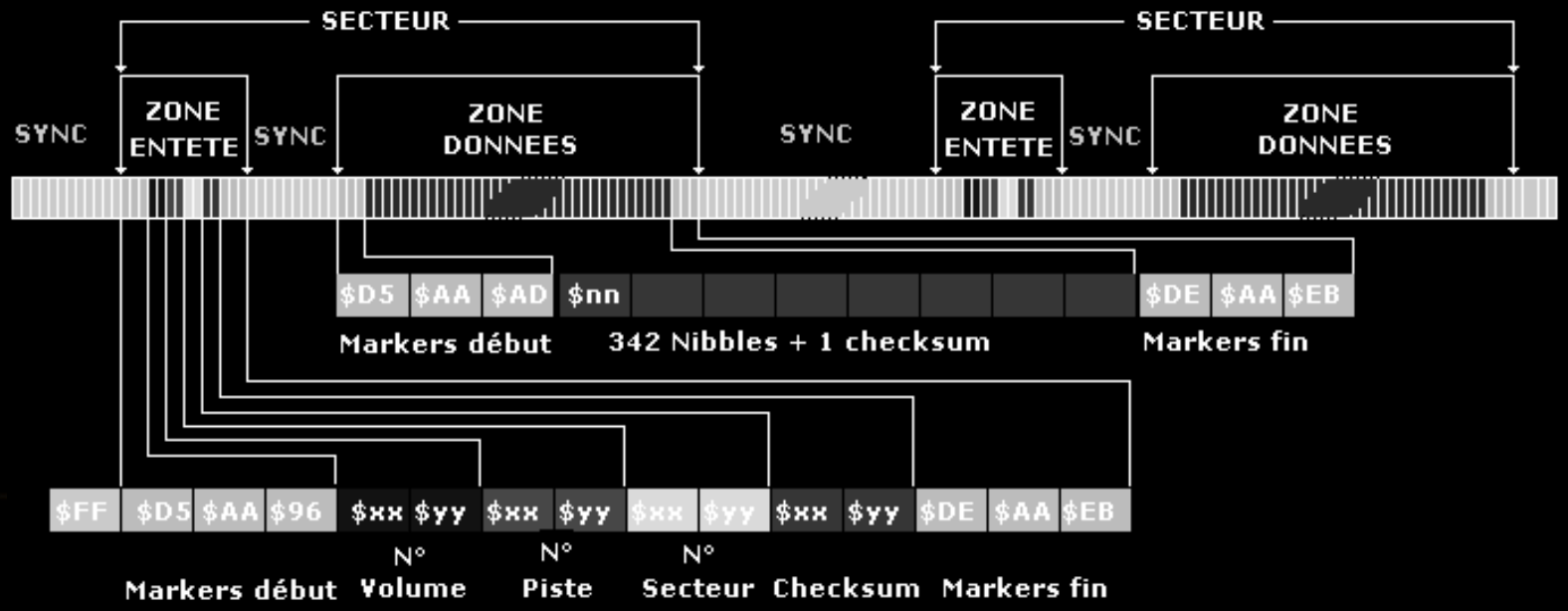
Bien plus performant, très agréable à programmer (en assembleur 68000 !)

PROTECTIONS DISQUETTE (1/4)



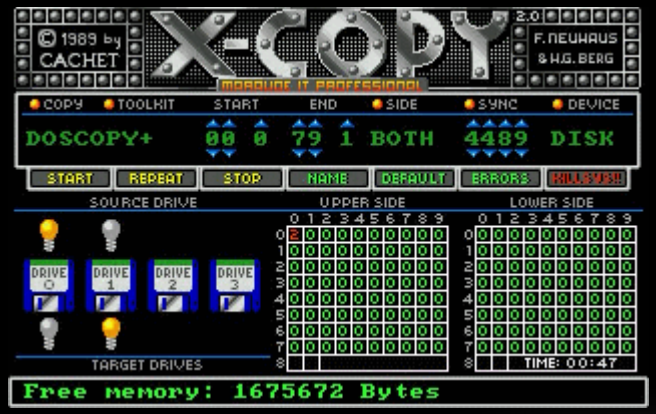
PROTECTIONS DISQUETTE (2/4)





PROTECTIONS DISQUETTE (3/4)

- Ecrire plus de secteurs ou pistes que prévu (jusqu'à 11 secteurs, 41 pistes)
- Ecrire entre les pistes (c'est moi !)
- Laisser des pistes non formatées



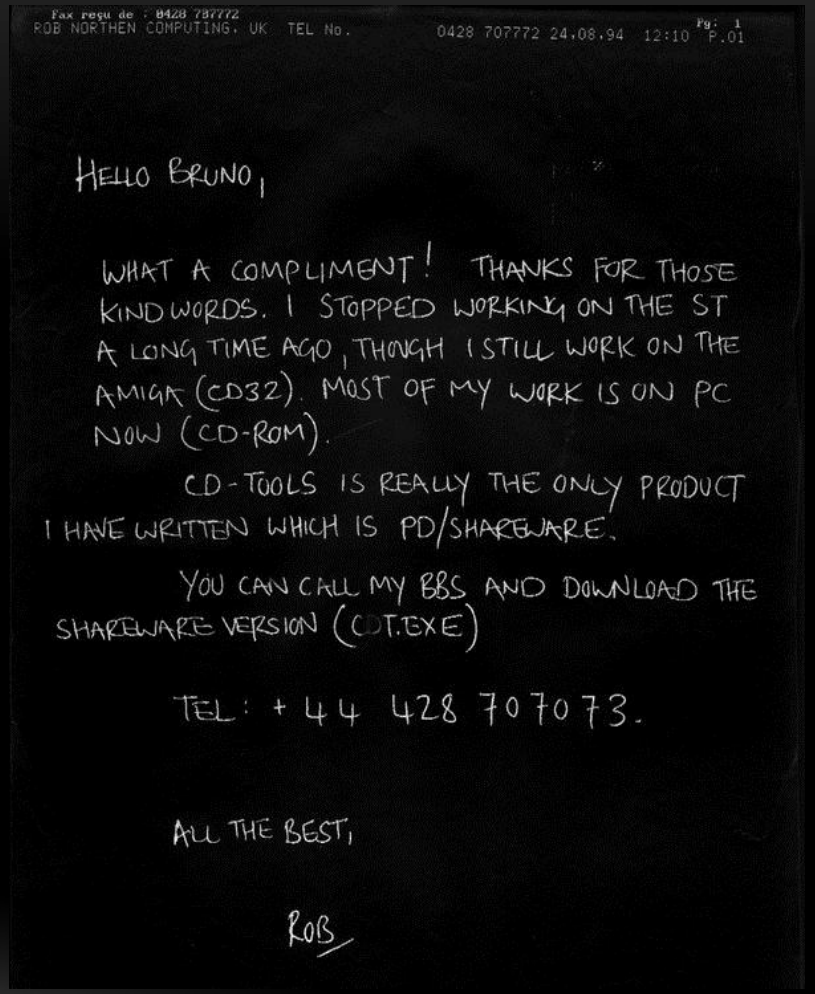

```
BSR       160(PC)             seekToPreviousTrack
TST.L     D6
BNE.S     14(PC)              L0006
TST.L     D2
BPL.S     10(PC)              L0006
ADDQ.B    #1,D2
ANDI.B    #1,D2
DBF       D7,-38(PC)          L0004
BSR       94(PC)              eraseBuffer
MOVE.W    (A7)+,$43E.L
MOVE.W    D2,D1               ;d1.w = drive no. key disk was found in
MOVE.L    D6,D0               ;d0.l = serial no. 0=key disk not found
MOVEM.L   (A7)+,A0-A3/D2-D7
BRA       1376(PC)            L002D


SUBQ.L    #4,A7
MOVE.W    #5,D0               ;Sector 5 in Track 0 (normal sector)
BSR       172(PC)             fdcMeasureSectorTiming
MOVE.L    D0,(A7)
MOVE.W    #6,D0               ;Sector 6 in Track 0 (slower sector, ~3%)
BSR       162(PC)             fdcMeasureSectorTiming
MOVE.L    (A7),D1
SUB.L     D1,D0               ;delta between 5 and 6
BMI.S     44(PC)              L000A
MULU      #100,D0
DIVU      D1,D0               ;convert delta into percent
CMP.B     #1,D0               ;1 percent or less is not good enough!
BLT.S     32(PC)              L000A

MOVEQ     #0,D0
MOVEQ     #3,D1
MOVEA.L   A3,A0
SUB.L     (A0)+,D0            ;checksum over first 16 bytes of sector 6 = "Rob Northen
DBF       D1,-4(PC)           L0008
CMP.L     #$B34C4FDC,D0       ;has to be a specific value!
BNE.S     12(PC)              L000A
MOVE.L    D0,D6
MOVEQ     #1,D1
ADD.L     (A0)+,D6            ;secret ID over the next 8 bytes
```

TECHNIQUE «WEAK BITS»

- Exemple : Dungeon Master
- Lecture des bits sur la disquette..
  Certains sont écrits avec un taux
  de magnétisation faible, la tête de lecture
  peut soit lire un 0, soit un 1…
- Le programme effectue des statistiques
- si les valeurs lues sont toujours les mêmes,
  c'est que c'est une copie !

LES PROTECTIONS «ROB NORTEN»

- «Copylock» : parmi les meilleures sur ST
  - Détournement du vecteur d'interruption Trace
  - Code automodifié, obfusqué et protégé
  - Format de disquette propriétaire
  - Taille d'un secteur différent
  - Chiffrement du bootsecteur
  - Et plein d'autres choses !



Fax reçu de : 0428 787772
ROB NORTHEN COMPUTING, UK TEL No. 0428 707772 24.08.94 12:10 Pg: 1 P.01

HELLO BRUNO,

WHAT A COMPLIMENT! THANKS FOR THOSE KIND WORDS. I STOPPED WORKING ON THE ST A LONG TIME AGO, THOUGH I STILL WORK ON THE AMIGA (CD32). MOST OF MY WORK IS ON PC NOW (CD-ROM).

CD-TOOLS IS REALLY THE ONLY PRODUCT I HAVE WRITTEN WHICH IS PD/SHAREWARE.

YOU CAN CALL MY BBS AND DOWNLOAD THE SHAREWARE VERSION (CDT.EXE)

TEL: +44 428 707073.

ALL THE BEST,

ROB

PROTECTIONS PROGRAMME

Code autogénéré

- Routine initiale qui génère le reste du code, et l'exécute ensuite.
  Permet de gagner en place disque
  Permet de gagner du temps en exécution (déroulement des boucles «gcc -funroll»)

Code automodifié

- Boucle qui s'exécute et qui change ses propres instructions avant bouclage
  Permet de gagner en place disque et RAM
  Optimisation, obfuscation,…

➔ Protections anti-désassemblage (le code doit être éxécuté pour être désassemblé !)

Les virus polymorphiques, ça vous dit quelque chose ?

DÉTOURNEMENT D'INTERRUPTIONS

- Routine de décodage lancée en synchro avec les VBL (Balayage écran)
  ➔ Code se plante si la synchro est perdue (débogage, mode trace…)

- Technique de «freeze» de programme protégé
  Souder un interrupteur sur la patte NMI du 68000, pour interrompre le programme, puis exécuter une routine de débogage située en mémoire vidéo !

UNE ROUTINE DANS LE CLAVIER !

- Routine de protection installée dans le processeur gérant le clavier (6301, 8 bits)
  - ➔ Code assembleur différent du 68000
  - ➔ Difficile d'imaginer qu'une routine de checksum se trouve à cet endroit !

C'était un truc à moi…


```
"anda $%04x",        HD6301_DISASM_MEMORY16},
"bita $%04x",        HD6301_DISASM_MEMORY16},
"ldaa $%04x",        HD6301_DISASM_MEMORY16},
"staa $%04x",        HD6301_DISASM_MEMORY16},
"eora $%04x",        HD6301_DISASM_MEMORY16},
"adca $%04x",        HD6301_DISASM_MEMORY16},
"oraa $%04x",        HD6301_DISASM_MEMORY16},
"adda $%04x",        HD6301_DISASM_MEMORY16},
"cpx  $%04x",        HD6301_DISASM_MEMORY16},
"jsr  $%04x",        HD6301_DISASM_MEMORY16},
"lds  $%04x",        HD6301_DISASM_MEMORY16},
"sts  $%04x",        HD6301_DISASM_MEMORY16},
```

Et pour finir en musique et en beauté

EXEMPLE AVEC UNE VRAIE DÉMO

OVERSCAN
(FULLSCREEN)

Résolution de 416*277 pixels
au lieu de 320*200 ?

Désynchronisation du balayage écran !

- D'abord la bordure basse
  Passage à 60Hz à la 199 ligne.

- Puis la bordure haute
  60Hz 13 ou 29 lignes «avant» le haut.
  Vérification grâce au Timer B (HBL)

- Puis la bordure droite, et enfin gauche…
  Passage à 70 Hz (attention danger !) durant quelques cycles.

Très technique, très précis … Nécessite une parfaite connaissance des cycles d'horloge et ASM 68000 !

THE UNION DEMO

Disquette protégée 14 secteurs

```
FE8C 91C8 D1FC 0000 04EA  ...p`.þŒ‘ÈÑü...ê
4520 554E 494F 4E2D 4445   .NÐTHE UNION-DE
544C 4F41 4445 5220 4259  MO-BOOTLOADER BY
414D 5046 274D 4158 2120   MAD'MAMPF'MAX!
4354 4F52 5320 544F 2047   14 SECTORS TO G
4F55 2041 5245 2052 4541  O... YOU ARE REA
4B4C 4F50 5054 2049 4620  LLY BEKLOPPT IF
414E 5420 544F 2043 5241   YOU WANT TO CRA
2E2E 2E00 91FC 0000 01F8  CK IT.....‘ü...ø
700B 0A98 444F 4F46 51C8  N Aúÿ€p..˜DOOFQÈ
```

Copieur intégré

MERCI POUR VOTRE ATTENTION !

BONNE CHANCE POUR LA NUIT DU HACK !!!!!

BONUS : QUELQUES LIENS

• Thomson MO5	Emulateur et logiciels Demoscene	http://dcmoto.free.fr http://pulsdemos.com
• Commodore 64	Emulateurs Demoscene	http://viceteam.org http://csdb.c64.org
• Atari ST	Emulateurs Demoscene	http://leonard.oxg.free.fr/ http://pacidemo.planet-d.net
• Demoscene	Intros et demos	http://scene.org http://pouet.net
•	Demoparties	http://demoparty.net