Sauvetage iMac

iMac A1225

Ordi donné à Elouan, fév. 2025

Serial no. : VM920XLU250
Model no. : A1225
EMC no. : 2134
IC : 4324A-BRCM1022

Supprimer le mot de passe du BIOS

«the user cannot reset a forgotten EFI password, only a certified Apple technician has the ability to do that. Since Iran is not an Apple supported location at this time, you do not have any options but to travel to a country that is supported. Or you could try contacting Apple via the ExpressLane and see if they can offer help»

https://support.apple.com/en-us/102384

En somme, ce n'est pas réalisable MAIS il semble que certaines personnes aient réussi en utilisant un raspberry pi comme programmeur SPI et en reprogrammant la puce EFI :

- https://gist.github.com/willzhang05/e5b5563cdc65514dfb7ca131e03ca4b2
- https://web.archive.org/web/20221226062036/https://www.ghostlyhaks.com/blog/blog/hacking/18-how-to-bypass-apple-efi-firmware-lock
- https://web.archive.org/web/20181006134342/https://rossmanngroup.com/boards/forum/board-repair-troubleshooting/2455-how-to-read-write-erase-apple-efi-spi-rom-with-raspberry-pi

En gros :

- démonter, cf. tuto ifixit
- identifier la puce EFI
- reprogrammer

On peut trouver des pinces pour programmer ce genre de puces sur ebay pour pas chère, ou des versions de qualité chez Pomona (distribué par digikey, farnell, etc.)

- https://www.pomonaelectronics.com/products/test-clips/ic-test-clips
- https://www.ebay.fr/itm/285795230884 clip de test SOIC8 SOP8 pour programmation
- https://www.ebay.fr/itm/335418447704 clip de test SOIC16 SOP16 pour programmation

Il faut rajouter des ventouses pour enlever l'écran de l'imac

- https://www.ebay.fr/itm/155330567520 screen suction cup

Pour d'autres modèles de Mac, il existe aussi un logiciel payant : https://checkm8.info/mac-efi-unlock-software

Reprogrammer la puce EFI d'un mac A1225

Elouan / Emoc, juillet 2025

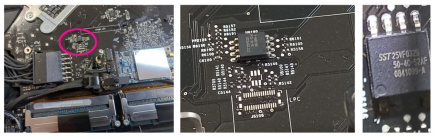
1. Démonter l'ordi pour accéder à la carte mère

Nécessaire : assortiment de tournevis, 2 ventouses de démontage

Pour cela, on suit le tuto tuto ifixit

2. Localiser et identifier la puce ROM EFI

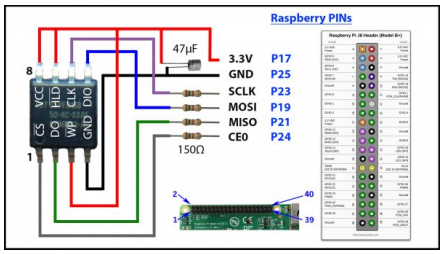
Une fois démonté, il faut chercher la puce EFI sur la carte mère, on la trouve au dessus des barrettes de RAM.
L'inscription permet de l'identifier, il s'agit d'une puce SST25VF032B de Microchip (32 Mbit SPI Serial Flash), datasheet : SST25VF032B



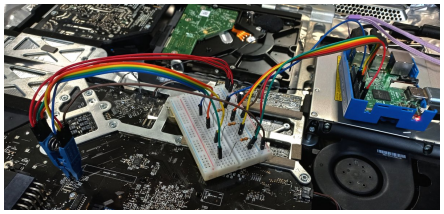
3. montage et installation

Nécessaire

Préparer le montage pour relier le raspberry pi, en suivant ce schéma (source : rossman-group). Vérifier dans la datasheet de la puce mémoire que le brochage correspond bien! Et aussi qu'elle est dans la base de flashrom (https://github.com/flashrom/flashrom/blob/main/flashchips/sst.c)



Ce qui donne



4. préparation du raspberry pi

Commencer en activant le SPI sur le Raspberry Pi :

```
sudo raspi-config               # pour activer le SPI
```

Dans interface options, activer le SPI

Puis, dans un terminal :

```
sudo apt install flashrom       # installation du logiciel
sudo modprobe spi_bcm2835       # charger le module SPI
ls /dev/                        # vérifier qu'on y trouve spidev0.0
```

Tout est en place pour lire le contenu de la puce mémoire! On utilise flashrom pour copier le contenu de la puce dans un fichier (read1.bin, etc.)

```
flashrom -r read1.bin -c "SST25VF032B" -V -p linux_spi:dev=/dev/spidev0.0
flashrom -r read2.bin -c "SST25VF032B" -V -p linux_spi:dev=/dev/spidev0.0
flashrom -r read3.bin -c "SST25VF032B" -V -p linux_spi:dev=/dev/spidev0.0
```

On lit plusieurs fois le contenu afin d'être sûr que tout s'est bien passé, ensuite on compare les sommes de contrôle md5 pour vérifier que les fichiers sont bien identiques. Les 3 commandes suivantes devraient renvoyer le même résultat.

```
md5sum read1.bin
md5sum read2.bin
md5sum read3.bin
```

X. à suivre

Édition du fichier avec un éditeur hexadécimal comme imhex ou wxHexEditor (on a essayé hexedit et hexcurse mais il n'y a pas de fonction de recherche)

```
sudo apt install wxhexeditor
```

(suite le 15 juillet 2025)

https://gist.github.com/willzhang05/e5b5563cdc65514dfb7ca131e03ca4b2

Autres ressources

- https://philsrandomblathering.quora.com/Adventures-in-BIOS-Password-Recoveryv
- https://tomvanveen.eu/flashing-bios-chip-raspberry-pi/
- https://darksideofapple.wordpress.com/2015/01/04/3-methods-for-bypassing-apple-efi-firmware-password-icloud-lock/
- https://repair.wiki/w/A1278_MacBook_Pro_EFI_Password
- Sur Flashrom
    - https://www.flashrom.org/user_docs/raspberry_pi.html
    - https://www.flashrom.org/supported_hw/supported_flashchips.html
    - https://manpages.debian.org/jessie/flashrom/flashrom.8
- Recherche avec imhex : https://docs.werwolv.net/imhex/views/find

iMac A1125

tentative 9 juin 2020

E. a récupéré un vieil iMac dans une poubelle. Problème, il y a des mots de passe ...

On commence par identifier la machine, ce n'est pas très compliqué, c'est écrit dessus!

```
iMac 24''/3.06/2x2GB,1TB/SD/MSE/KB-FRA
Model no A1125
IC : 4324A-BRCM1022
```

L'année aussi est inscrite : 2008, on peut déduire le système minimum : MacOSX 10.5 Leopard ou 10.6 Snow leopard grâce à cette page : MacOS

Sur MacOS, il existe différentes combinaisons de touche, au démarrage, pour démarrer la machine dans une configuration particulière. On va utiliser ⌘+R pour démarrer en *recovery mode*

Depuis cet écran, on peut lancer un terminal, pour connaître la version de MacOS

```
sw_vers -productVersion
```

Il s'agit de MacOS 10.9.3 (= Mavericks, de 2013)

A partir de cet écran on peut aussi retirer un mot de passe d'accès (menus du haut)
Il est aussi possible d'accéder au menu des utilitaires MacOS, pour réinstaller MacOS, ou agir sur le disque dur.

Ça serait une possibilité de réinstaller l'OS mais il semblerait qu'il y ait 5.29 GB de données à télécharger, soit quelques heures et donc pas possible de le faire cette après-midi...

On va tenter autre chose : démarrer en single user mode et enlever les mot de passe utilisateur (source)
Mais ça ne marche pas, snif...

Donc tentage de réinstallation avec connexion gros débit, ultérieurement programmé

(à suivre)

→ nouveau mot de passe : motdepasse (peut etre M majuscule)

E. récupère l'iMac, pas d'info sur la suite