Formation CNEJITA
2 Février 2016

Outils et techniques d'investigation:

« Quand les solutions forensiques ne savent plus faire »

Modèle économique

Qualité de l'expertise → **Viabilité du modèle économique**

- **Equipement (logiciel, matériel et pièces détachées)**
- **Temps de veille et de formation**
- **Temps de mise en état**
- **Temps d'extraction et la comparaison entre les différents modes**
- **Interprétation du résultat**
- **Rédaction du rapport**

Temps moyen pour un smartphone → **12 heures**

Introduction

Parfois les solutions forensiques ne permettent pas d'accéder aux contenus des téléphones ou de contourner leur dispositif de sécurité.

Les trois principales solutions du marché:

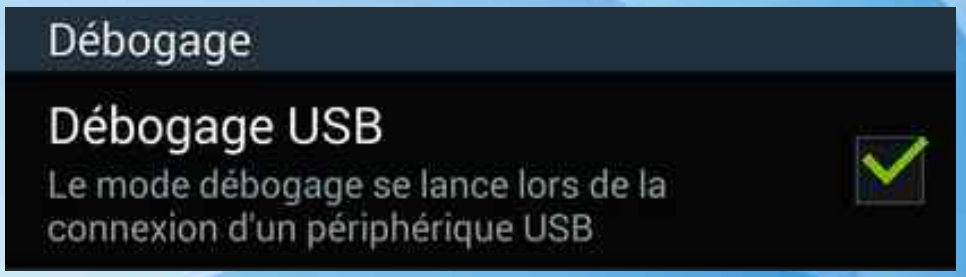
CELLEBRITE

OXYGEN

XRY

IPHONE 4S/ DEBOGAGE USB

A partir de l'IPHONE (4S ou IOs > 5.1) ou bien encore quand le débogage USB n'est pas activé sur les smartphones ANDROID, il nous est impossible de contourner le dispositif de sécurité.



PETITS TELEPHONES/ BLACKBERRY

De même, on rencontre le problème avec les « petits » téléphones ou bien avec les BLACKBERRY. Il paraît délicat de contourner le dispositif de sécurité.

Attention: Le câble USB peut ne pas offrir un canal data.

WINDOWS PHONE

Généralement, les outils classiques ne permettent d'accéder qu'à la partition MEDIAS

.

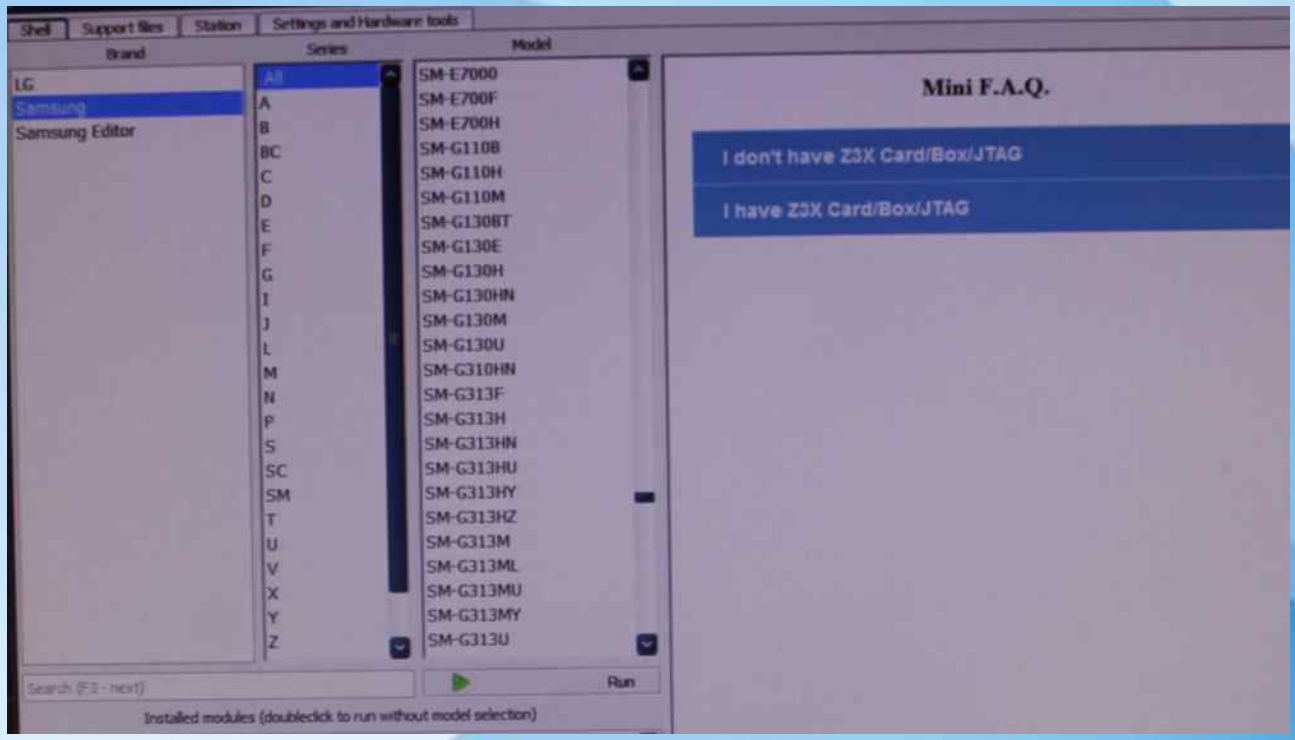
Pas de répertoire téléphonique, pas de SMS, pas de mail, applications, ….

FLASHBOX

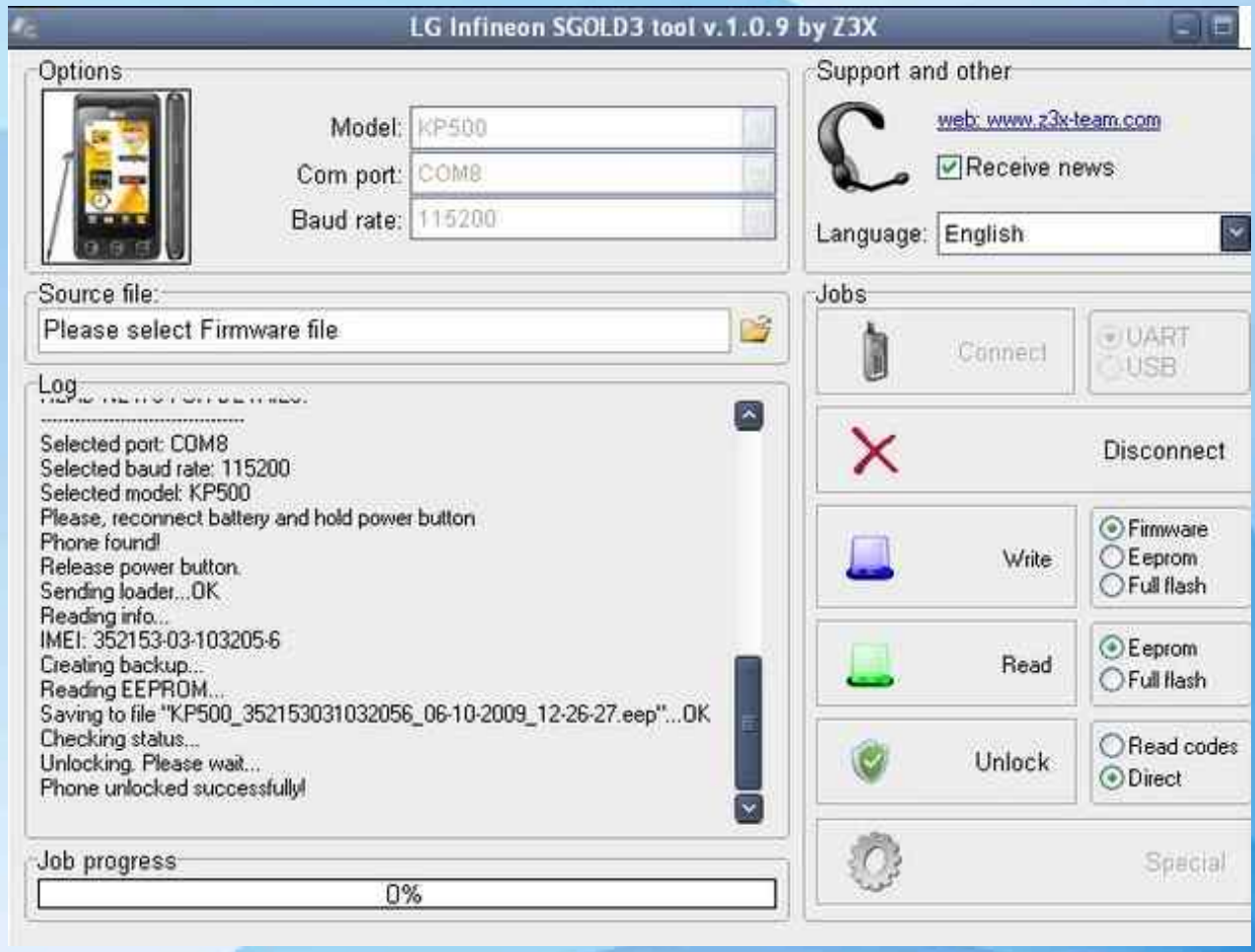
La Z3X BOX permet particulièrement de révéler les mots de passe des petits téléphones et le cas échéant extraire le contenu de la mémoire en fichier binaire.

La FLASHBOX

La Z3X BOX offre une bibliothèque (Z3X Shell) de téléphones pris en charge qu'il convient de mettre à jour régulièrement.



Attention: Le modèle exact doit être sélectionné.



Attention: Les boutons sont contextuels. Donc, chaque modèle offre des possibilités qui peuvent différer d'un autre.

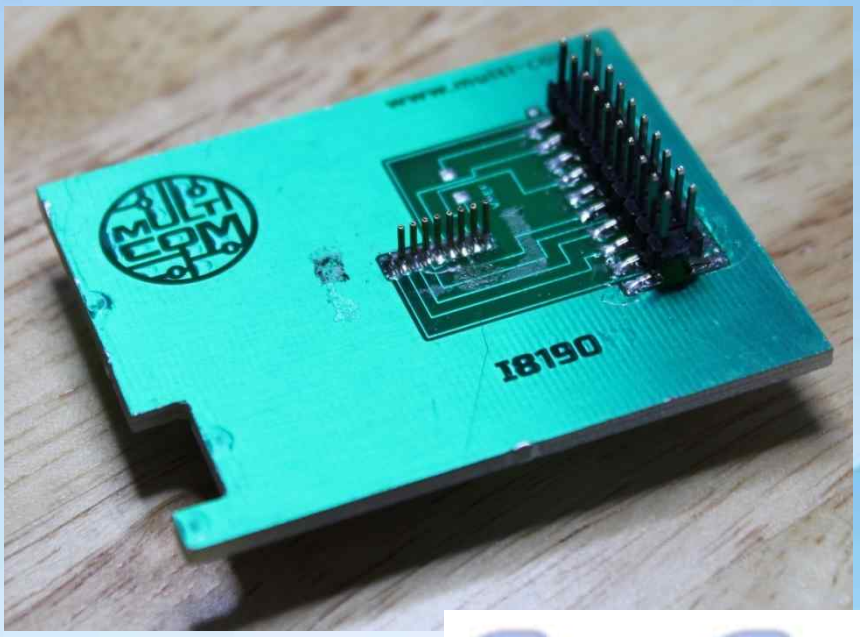
JTAG: RIFF BOX

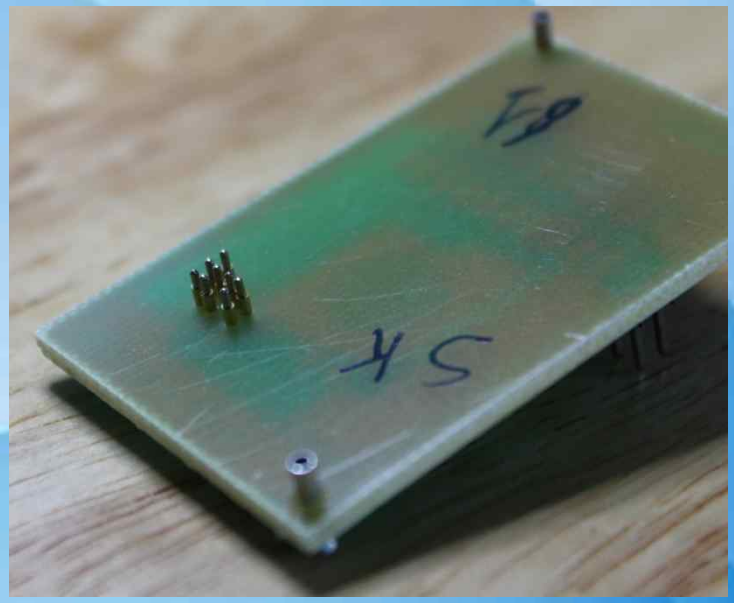
Un principe similaire à la Z3X BOX mais offre beaucoup plus de possibilités mais avec beaucoup plus de contraintes, particulièrement pour les Windows Phone.

Permet de réaliser un DUMP de la mémoire:
- USB .
- Soudage.
- Circuits imprimés.

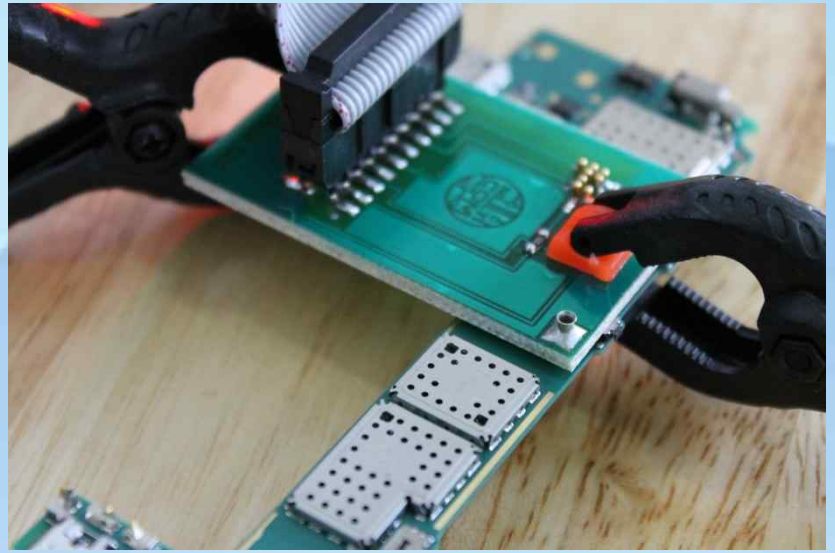
METHODE DE FONCTIONNEMENT DE LA RIFF BOX

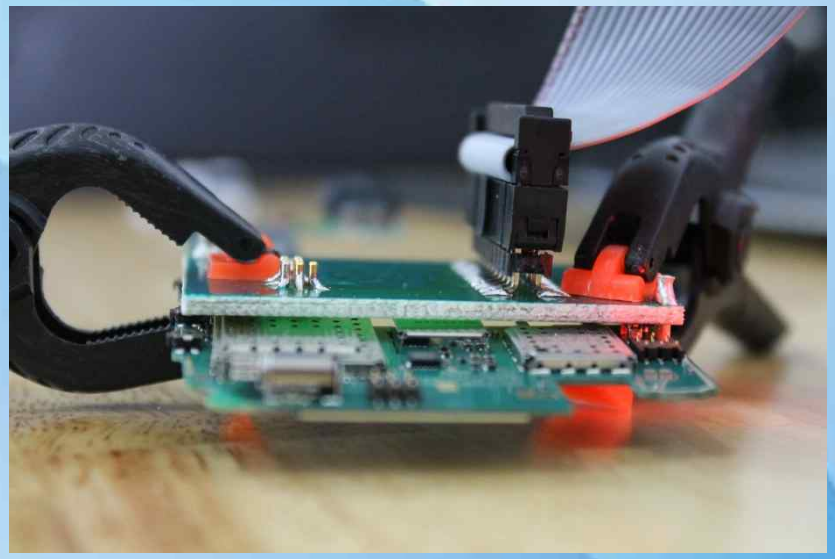
Sur un système de circuit électronique imprimé:

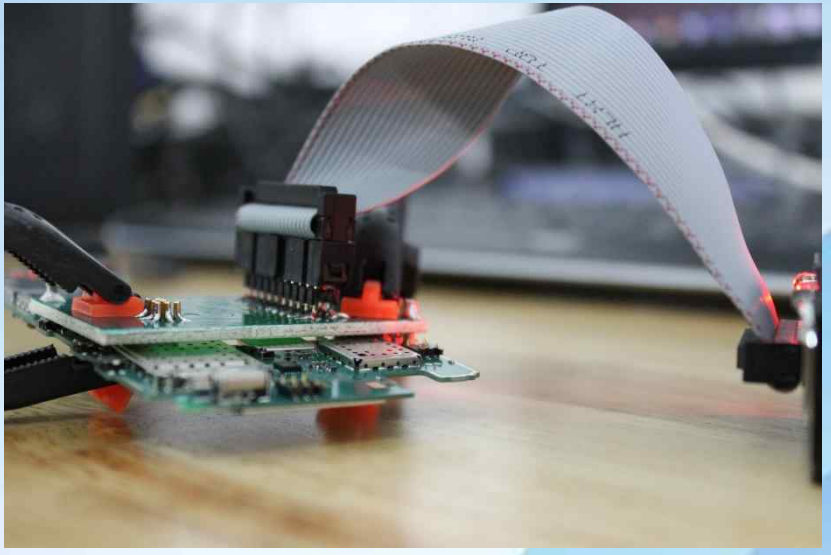


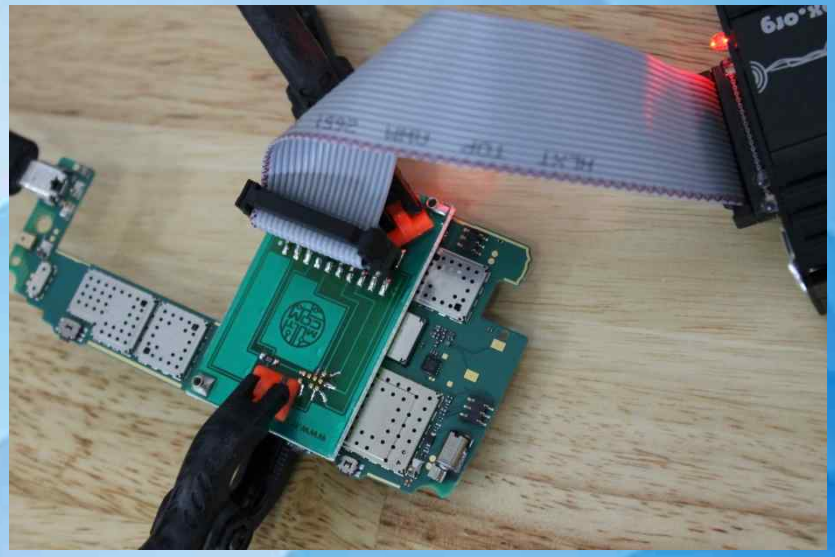


PRINCIPE DE LA RIFF BOX

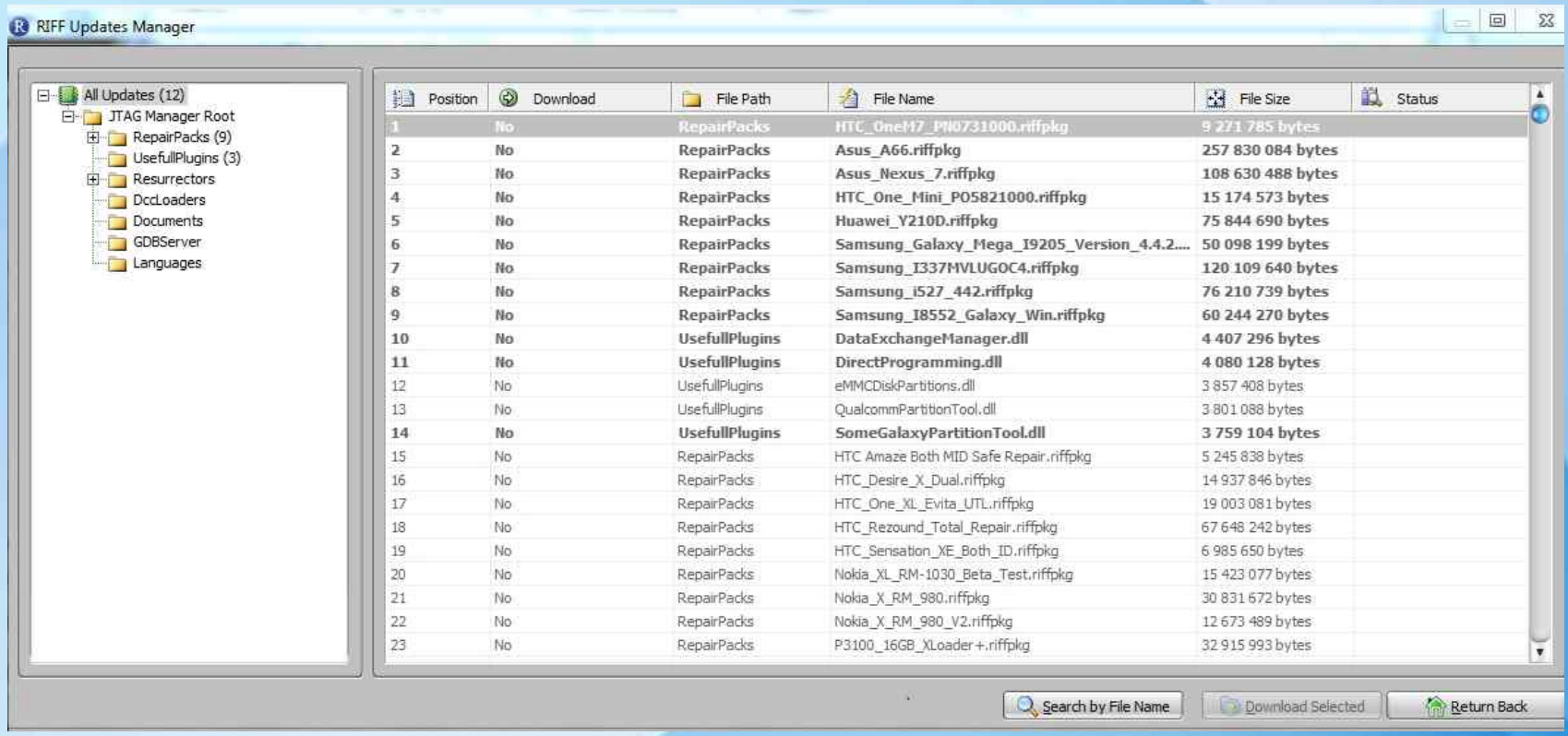








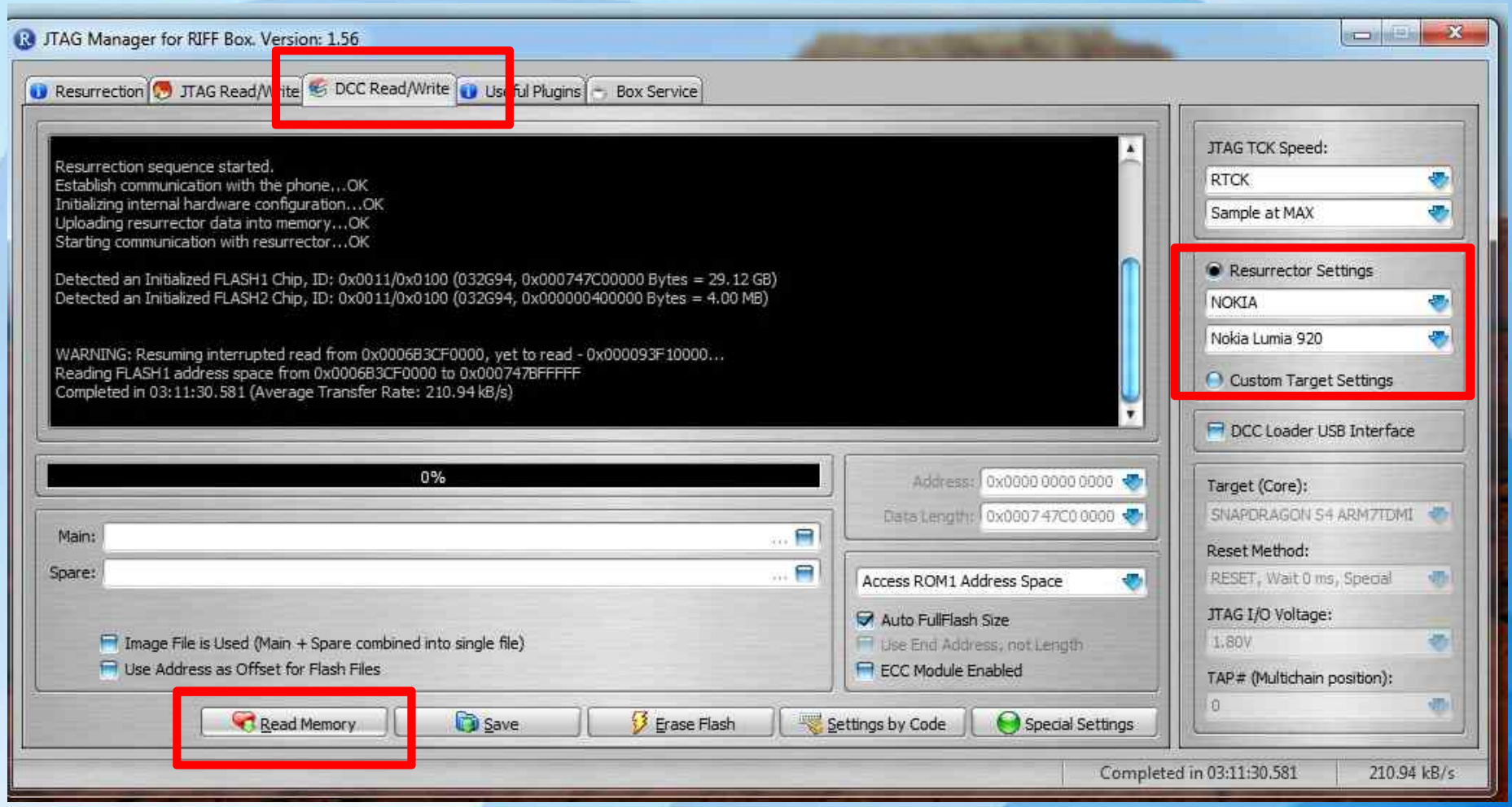
Bibliothèque RIFF BOX



Attention: Le modèle exact doit être sélectionné.

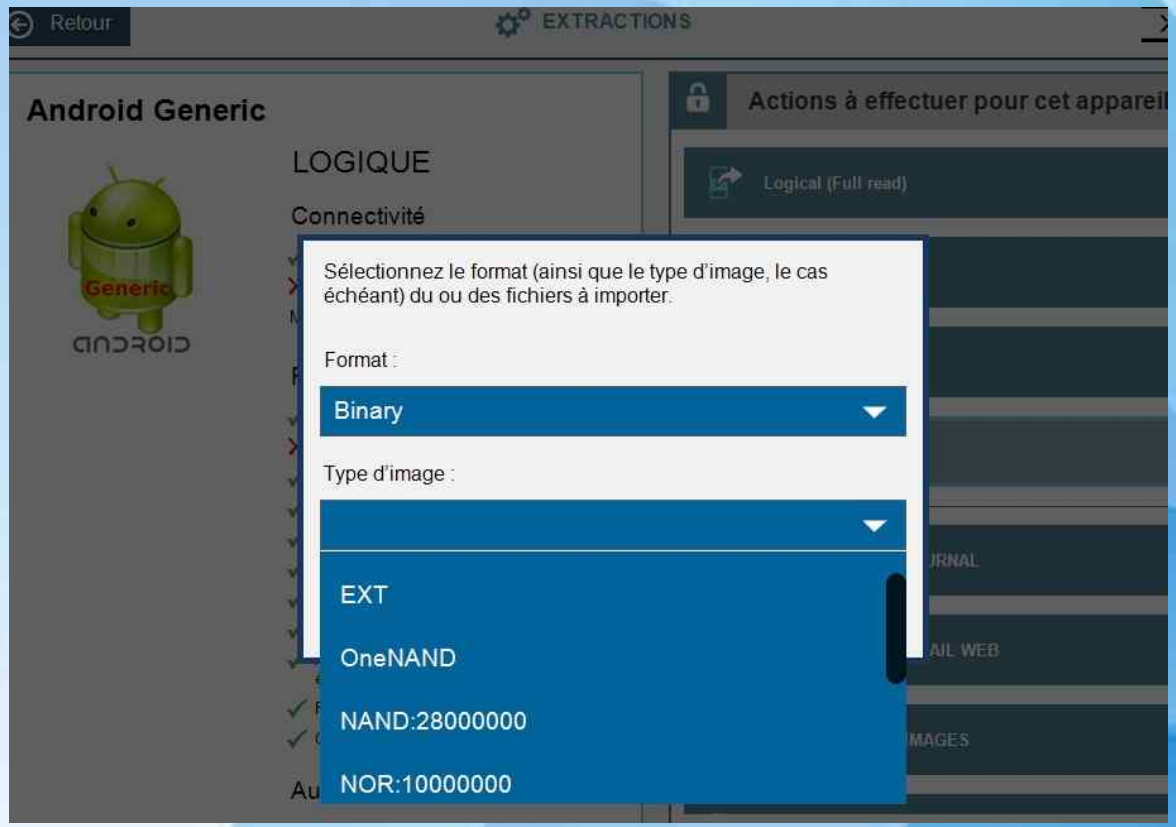
LIMITES DE FONCTIONNEMENT DU LOGICIEL

Il arrive parfois d'accéder uniquement à une partition notamment avec 512Mo.



EXPLOITATION

Intégration et décodage du fichier binaire



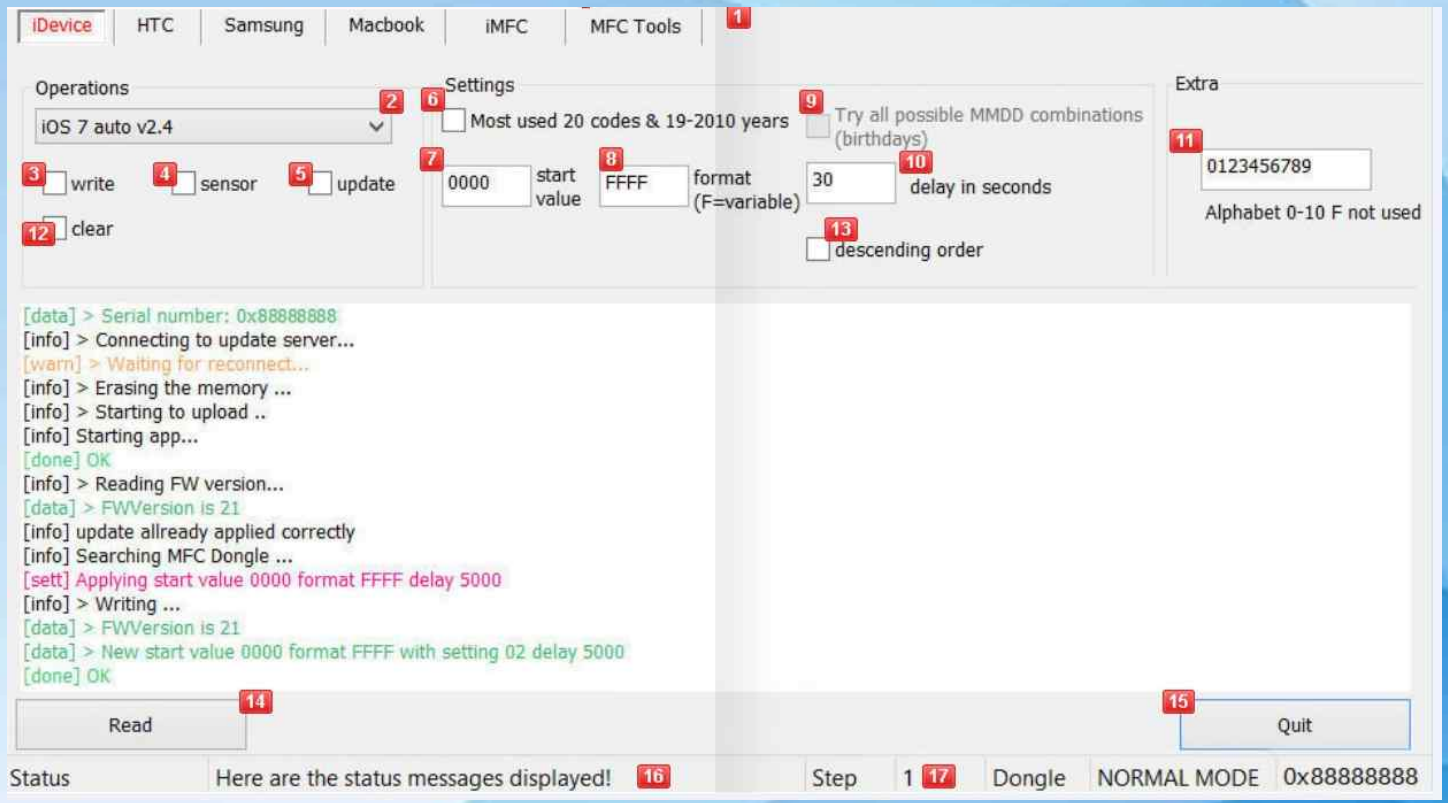
MFC DONGLE

Généralement utilisé sur les IPHONE, mais aussi pour les SAMSUNG et les HTC.

Dépend de l'état de la dalle tactile.
Processus long avec risque de blocable définitif du support, peut être même un Wipe.

METHODES DE FONCTIONNEMENT DU MFC

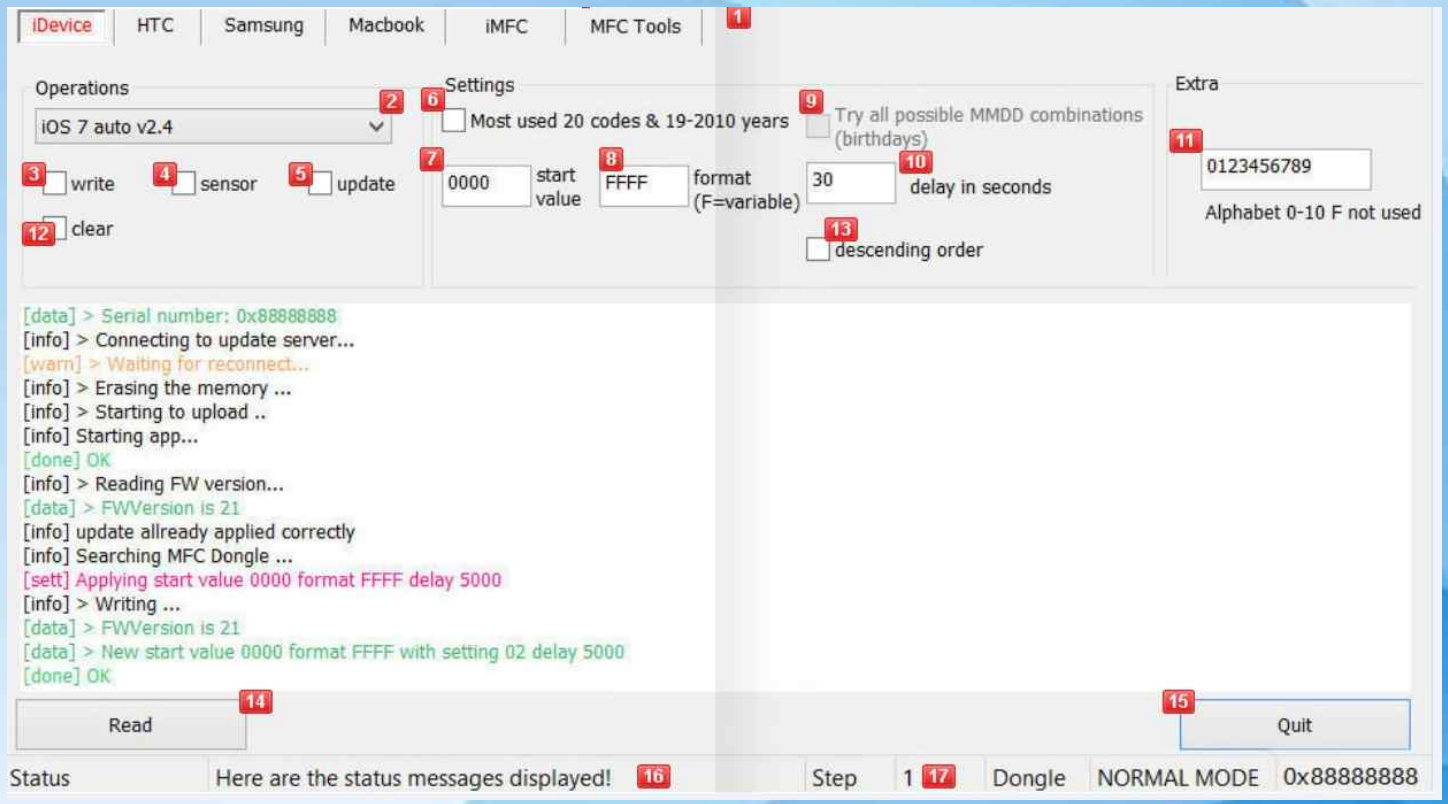
Paramétrer la clé du dispositif.



IMFC: permet de déceler plus de détails issus du support.

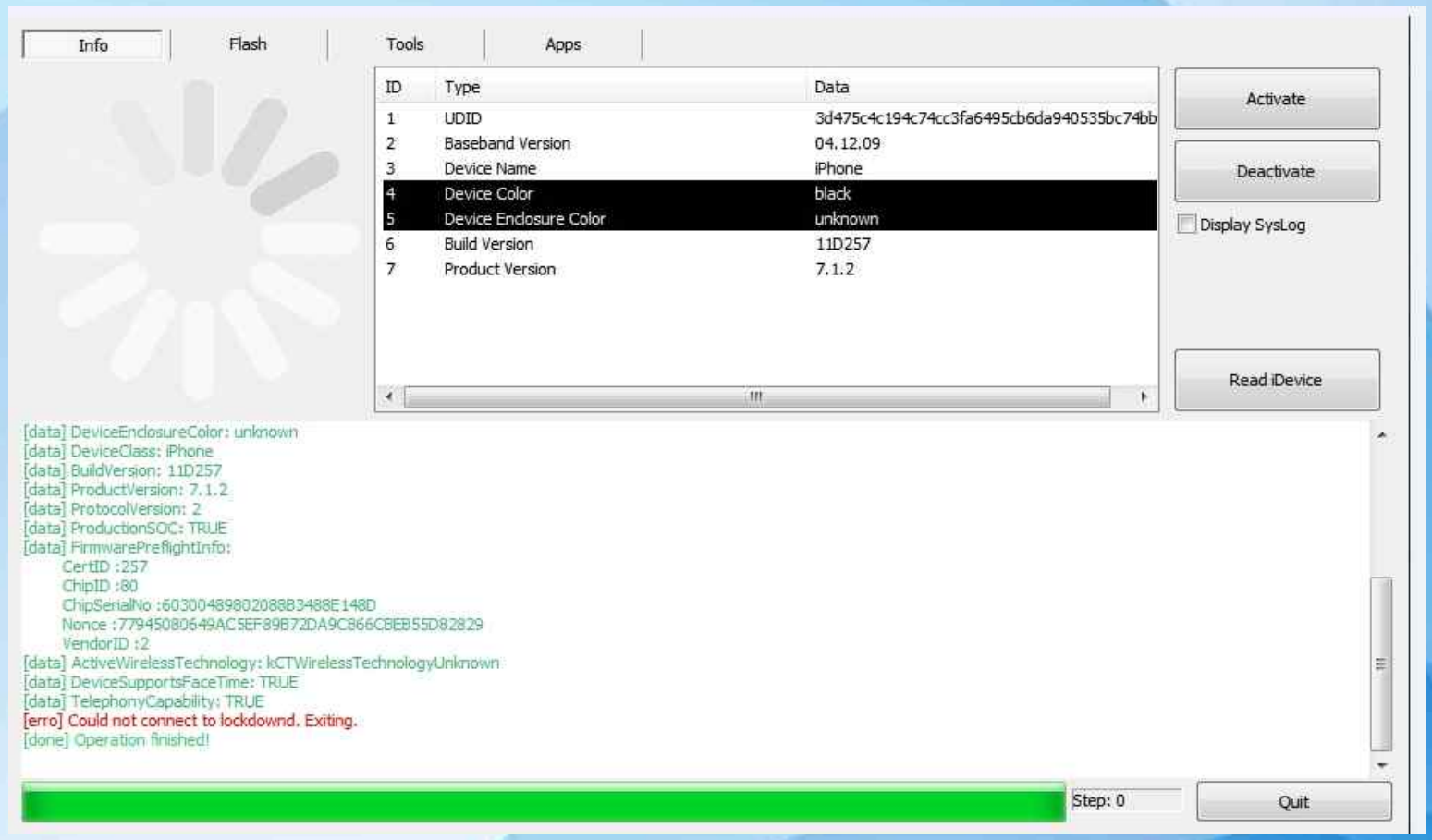
CONSULTER EN LIGNE LE MANUEL DU MFC

Paramétrer la clé du dispositif.



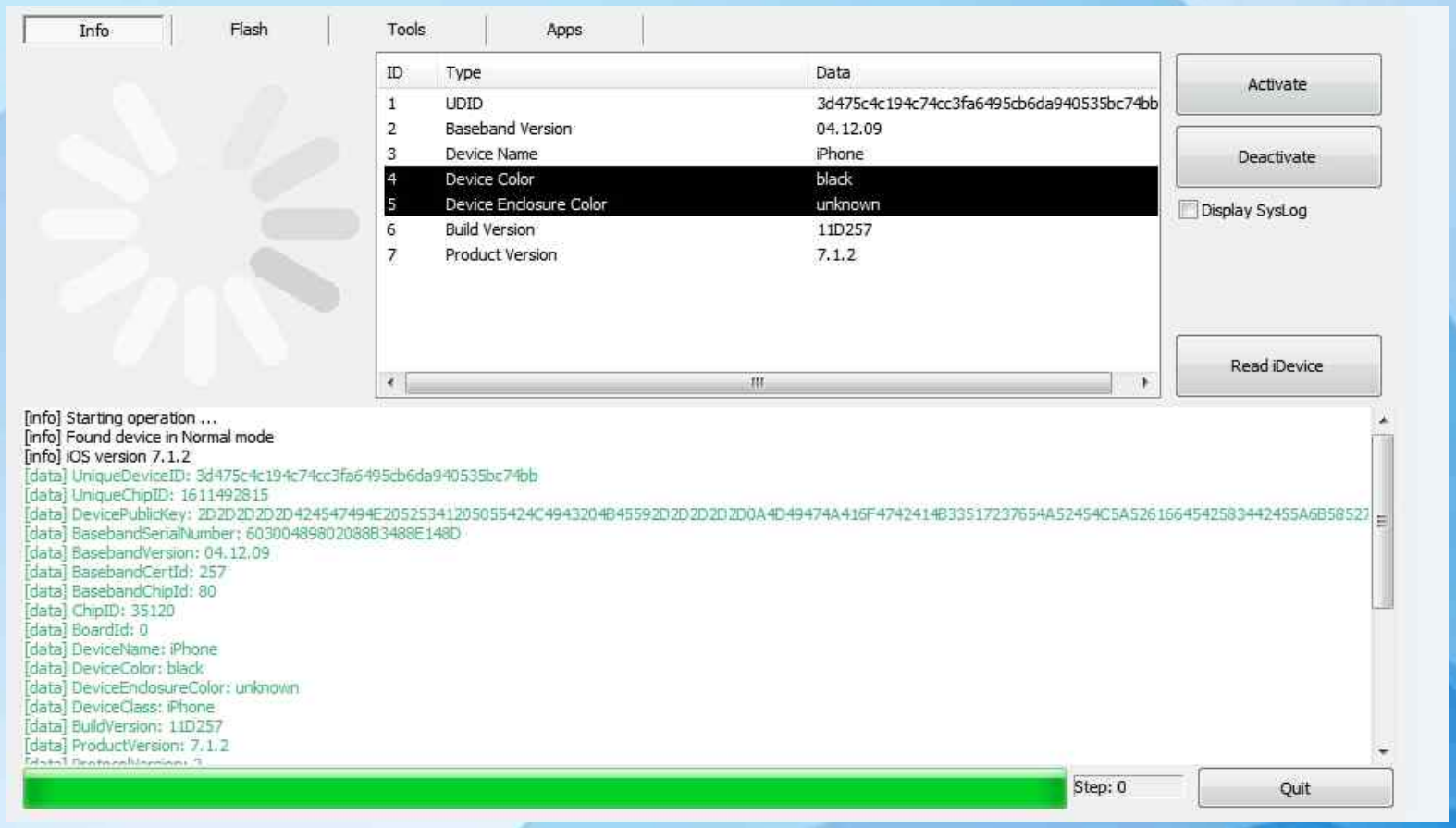
IMFC: permet de déceler plus de détails issus du support.

IMFC

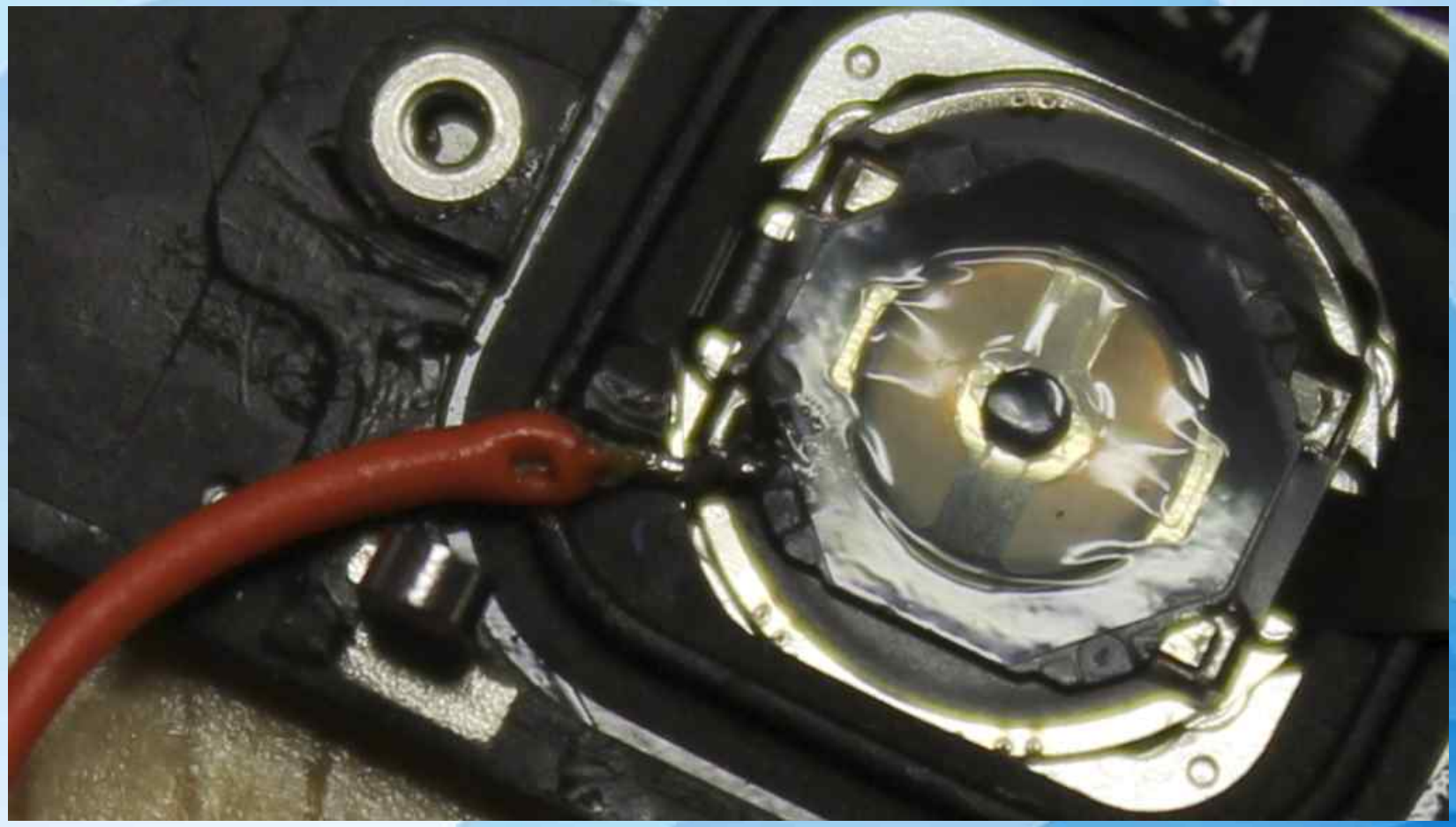


IMFC: permet de déceler plus de détails issus du support.

IMFC


Info
Flash
Tools
Apps
ID
Type
Data
1
UDID
3d475c4c194c74cc3fa6495cb6da940535bc74bb
2
Baseband Version
04.12.09
3
Device Name
iPhone
4
Device Color
black
5
Device Enclosure Color
unknown
6
Build Version
11D257
7
Product Version
7.1.2
Activate
Deactivate
Display SysLog
Read iDevice
[info] Starting operation ...
[info] Found device in Normal mode
[info] iOS version 7.1.2
[data] UniqueDeviceID: 3d475c4c194c74cc3fa6495cb6da940535bc74bb
[data] UniqueChipID: 1611492815
[data] DevicePublicKey: 2D2D2D2D2D424547494E20525341205055424C4943204B45592D2D2D2D2D0A4D49474A416F4742414B3351723765 4A52454C5A52616645425834424455A6B58527
[data] BasebandSerialNumber: 603004898020 88B3488E148D
[data] BasebandVersion: 04.12.09
[data] BasebandCertId: 257
[data] BasebandChipId: 80
[data] ChipID: 35120
[data] BoardId: 0
[data] DeviceName: iPhone
[data] DeviceColor: black
[data] DeviceEnclosureColor: unknown
[data] DeviceClass: iPhone
[data] BuildVersion: 11D257
[data] ProductVersion: 7.1.2
Step: 0
Quit

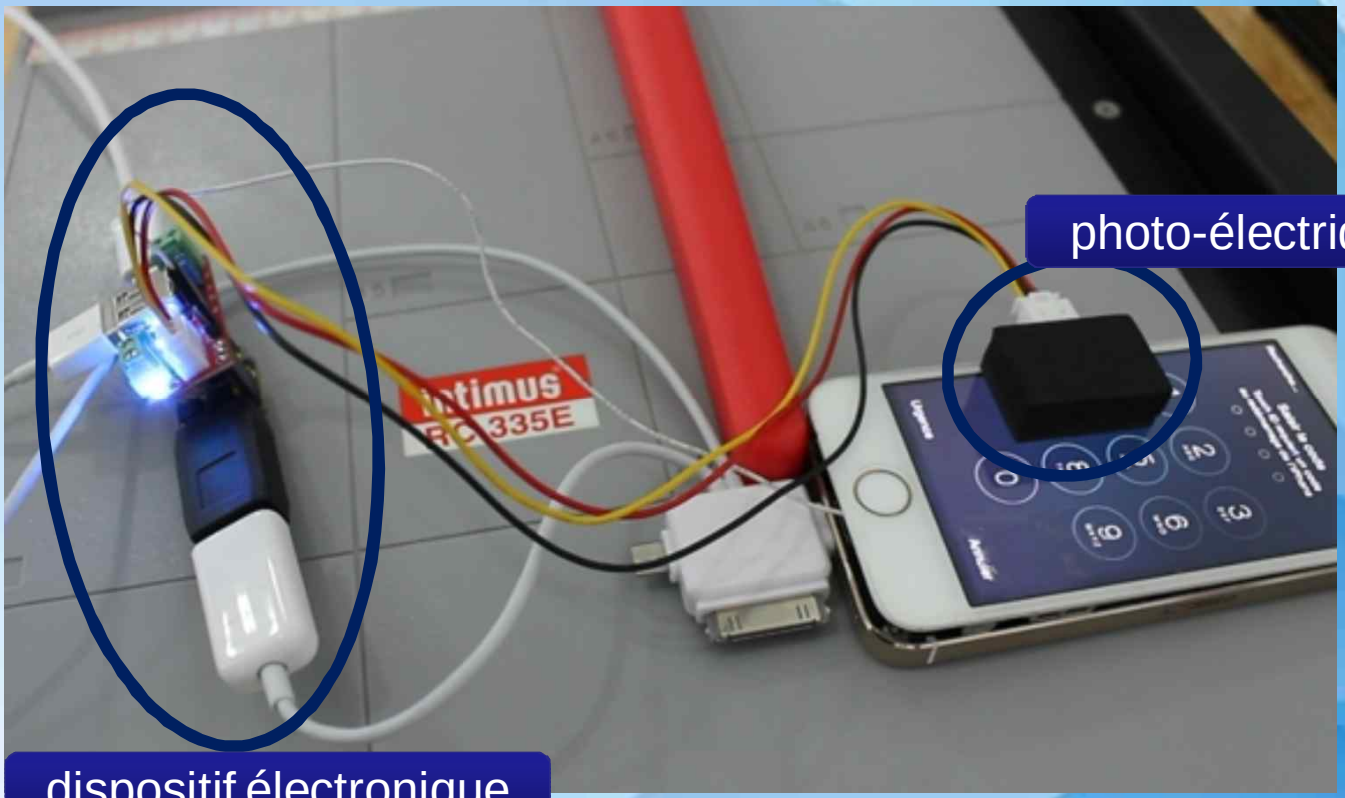
DIFFICULTE: Soudure



MFC DONGLE, C’EST QUOI ?

C’est une cellule photo-électrique avec un dispositif électronique qui se met sur le téléphone.

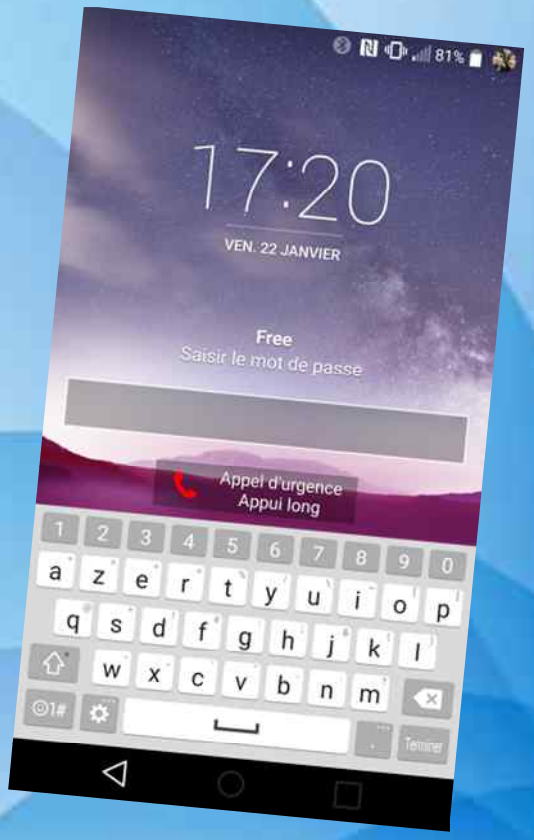
+ VIDEO



LES LIMTES DE MFC DONGLE

Malgré les possibilités qu'offrent l'outil, MFC DONGLE a ses limites :

- Le code numérique qui est par exemple à 6 digits ou alphanumérique
- Susceptible d'effacer la mémoire du téléphone
- Taux de réussite de l'ordre de 50%



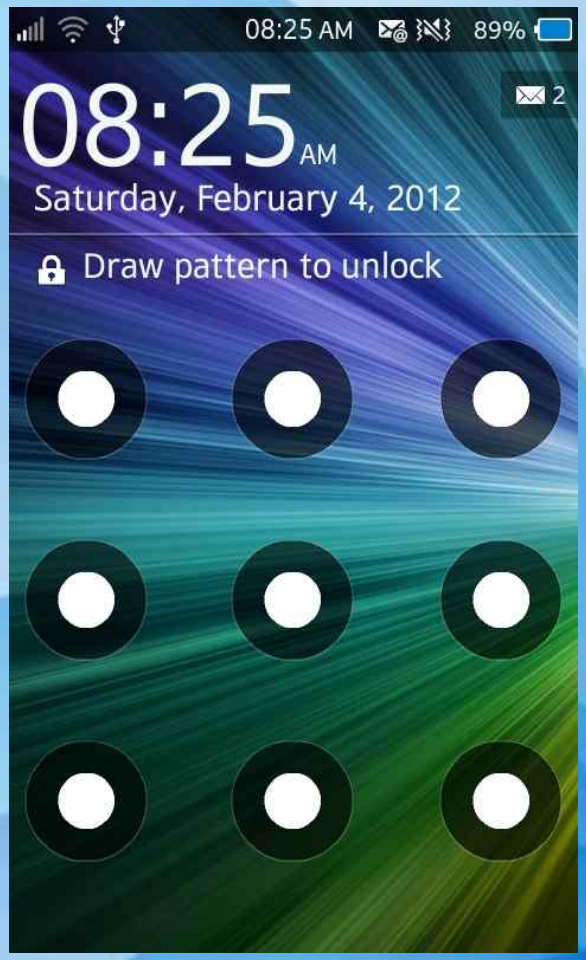
Méthode: FLASH RECOVERY

La méthode « Flash Recovery » consiste à modifier une partition du téléphone pour pouvoir neutraliser le dispositif de sécurité.

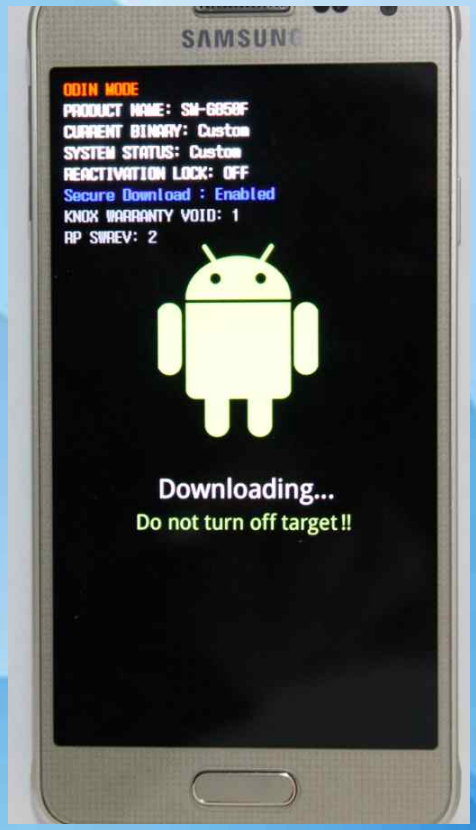
Pour le modifier, il convient de vérifier l'existence d'un binaire (éprouvé).

Ce n'est pas une manipulation anodine et cette méthode est susceptible d'effacer définitivement les données contenues dans le téléphone.

Il existe un site de référence:
http://forum.xda-developers.com/



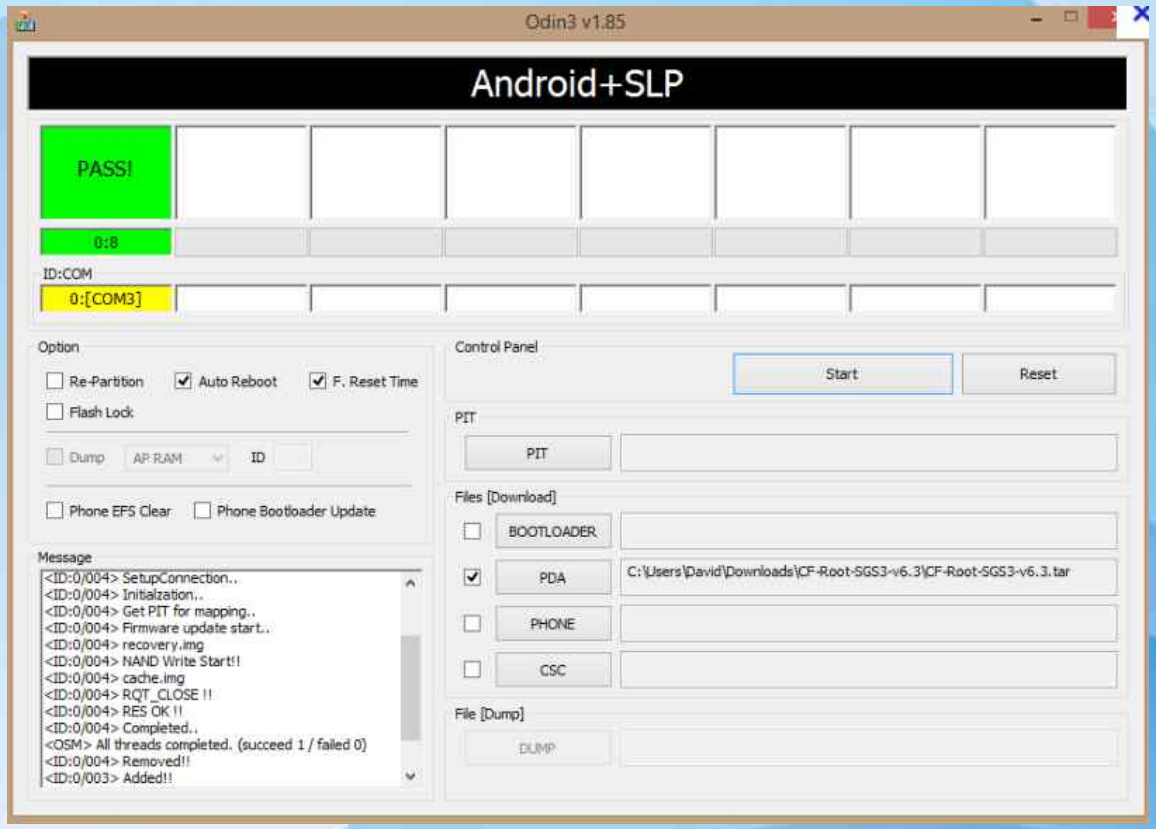
FLASH RECOVERY



Downloading

Bien lire les commentaires postés dans le forum.
Plusieurs teams de développement (fastboot, flashtools, …).

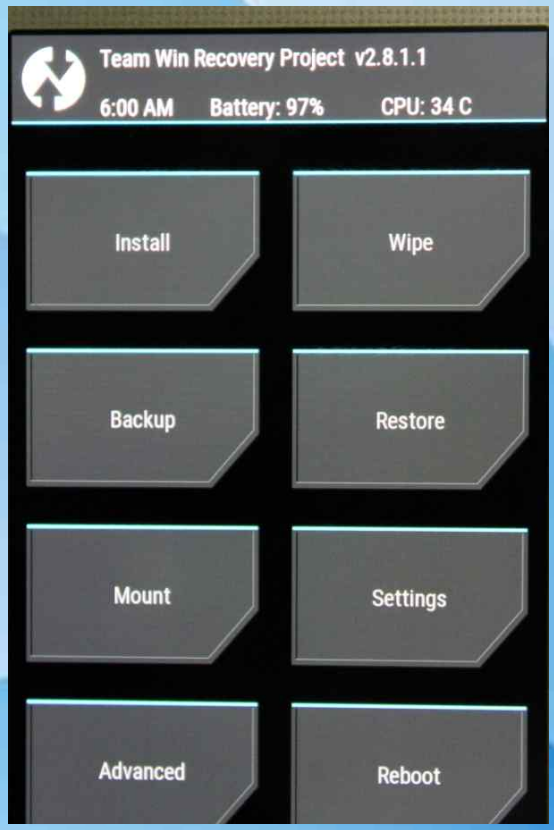
FLASH RECOVERY



Chaque modèle de téléphone possède sa combinaison de touches.

FLASH RECOVERY

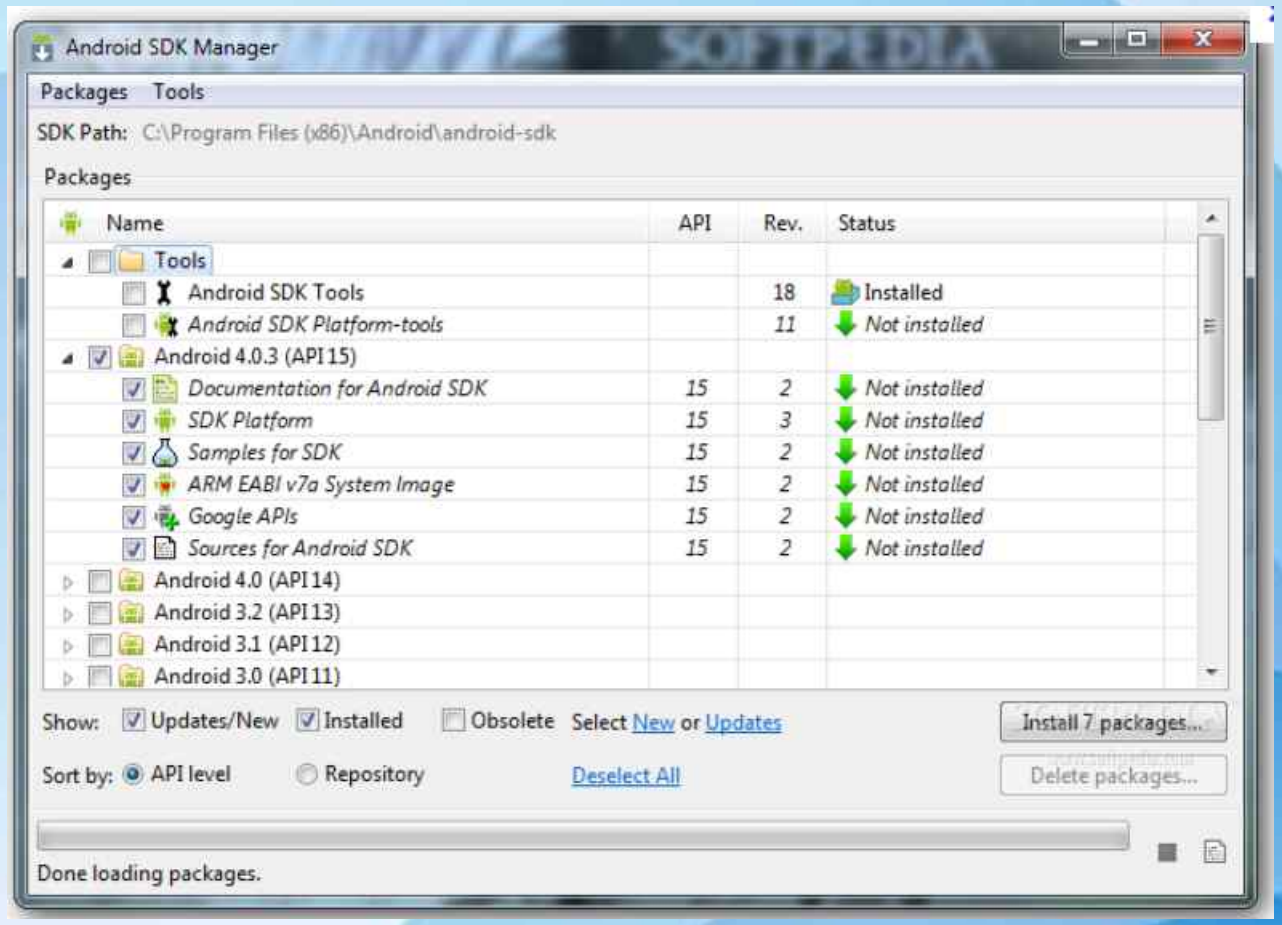
Recovery - avant



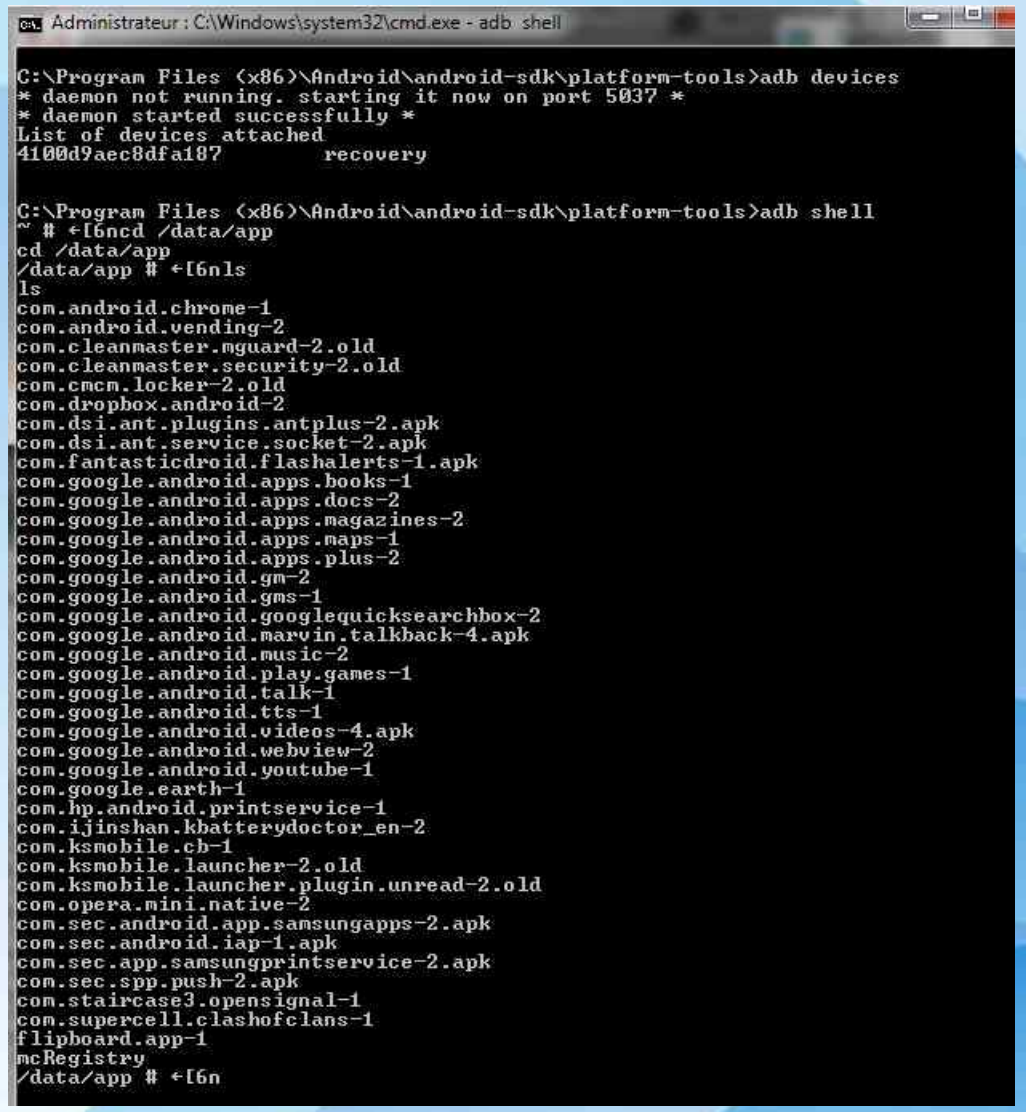
Recovery - après

Monter la partition système en restant en mode recovery.

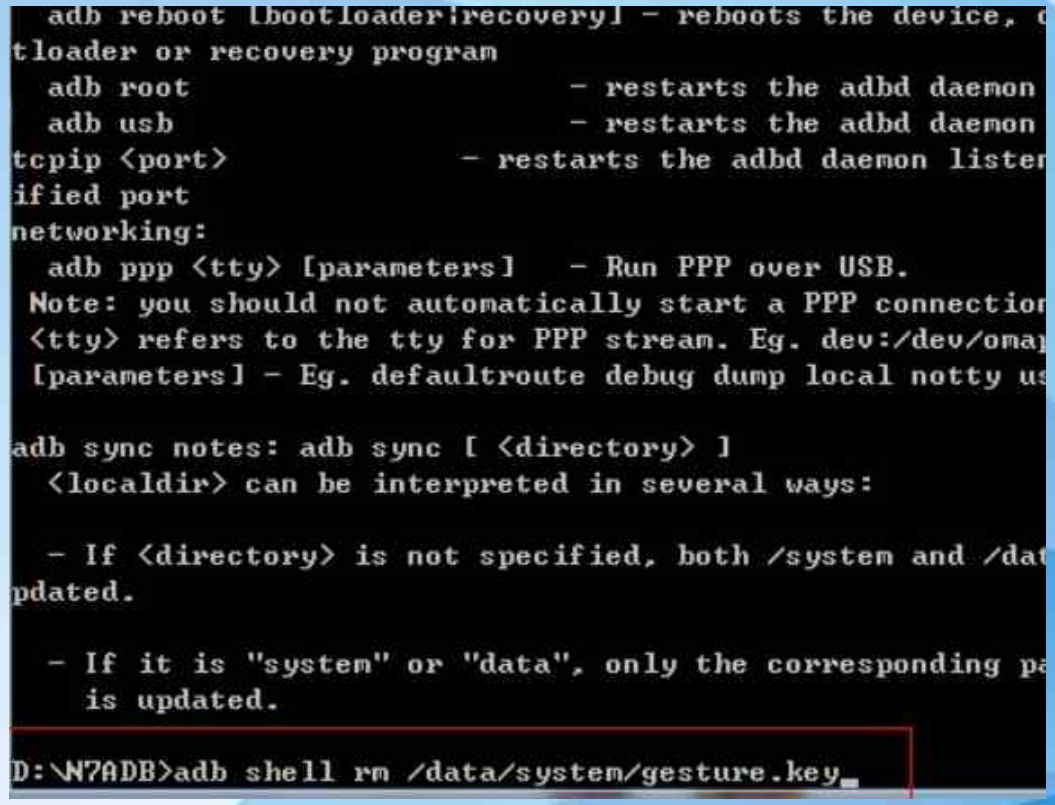
Installation du pack ANDROID SDK



Lancement de la console ADB

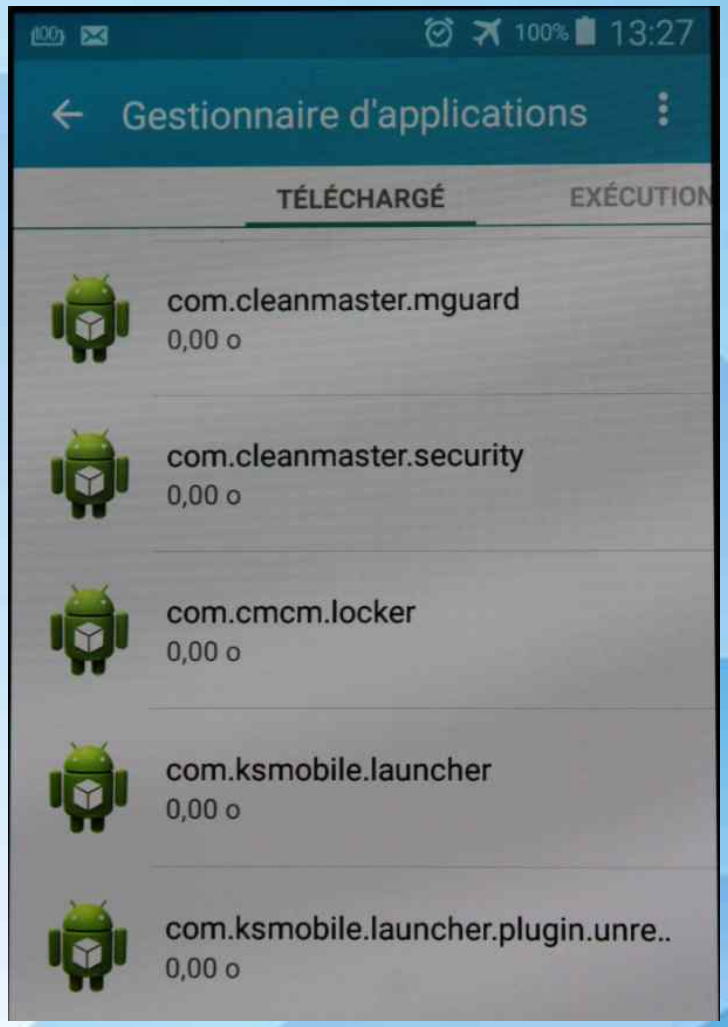


Console ADB: Neutralisation des fichiers de sécurité

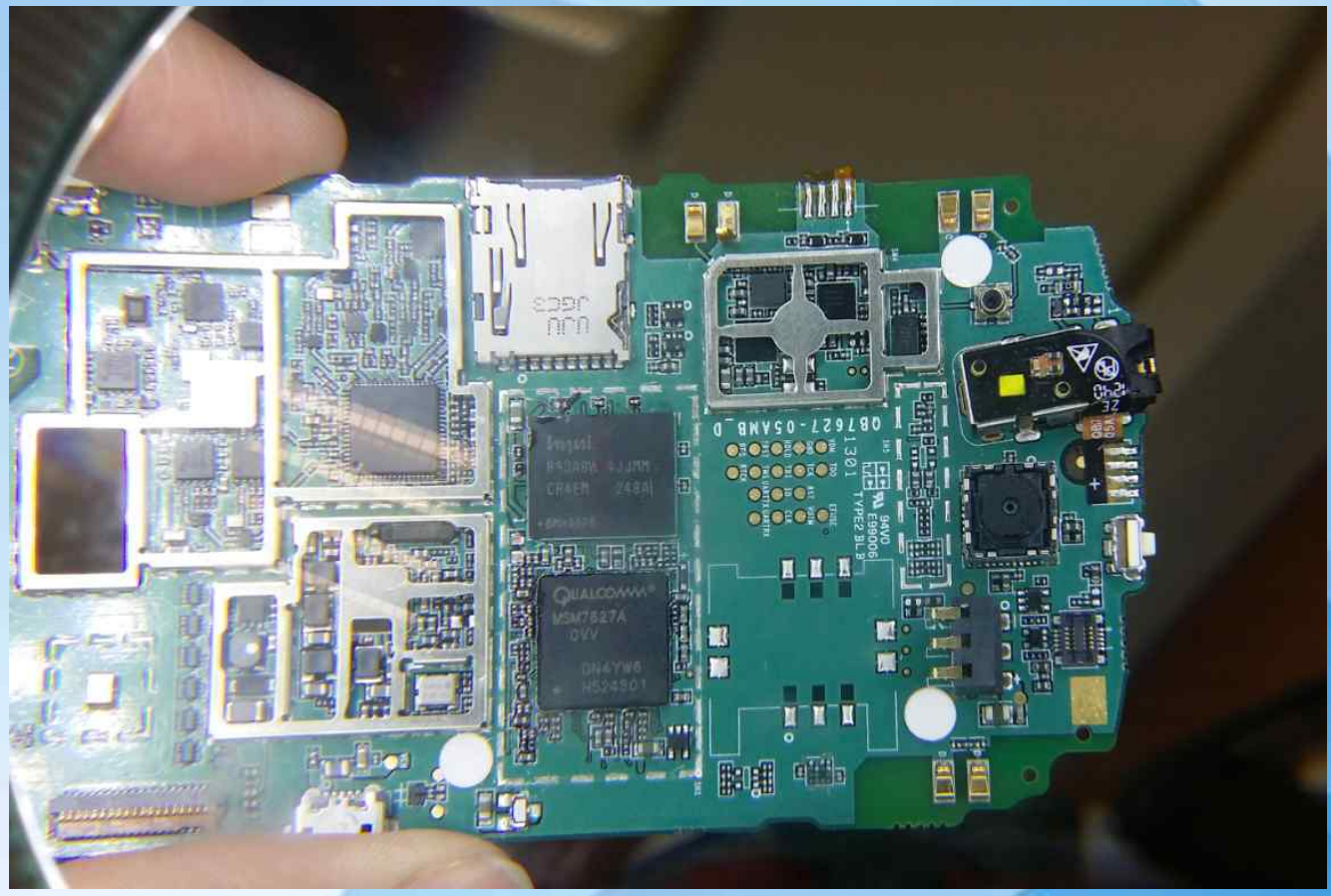


Confrontation à des problèmes de droit.

Côté application



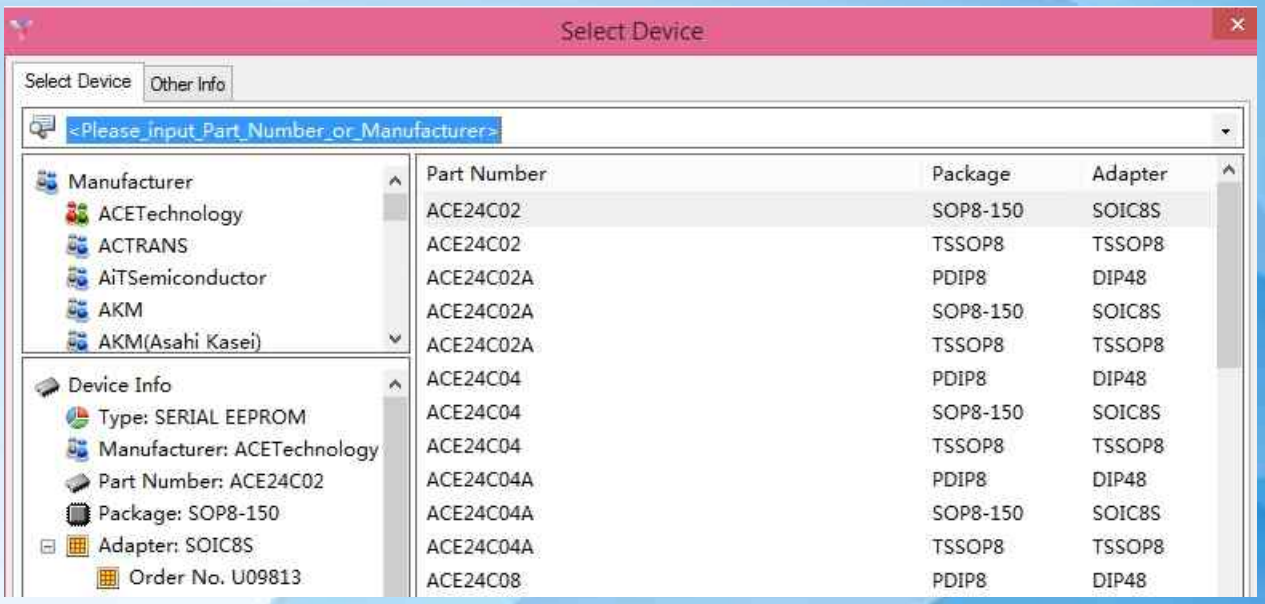
CHIP OFF ou la manipulation de la dernière chance



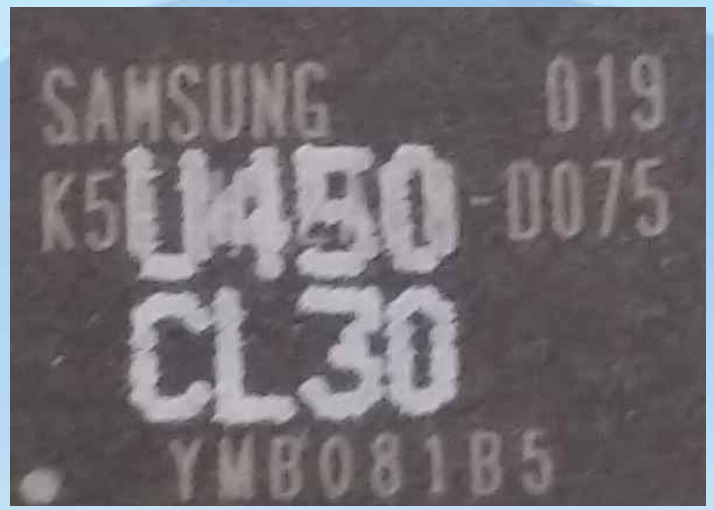
L’appareil de référence

L’appareil de référence

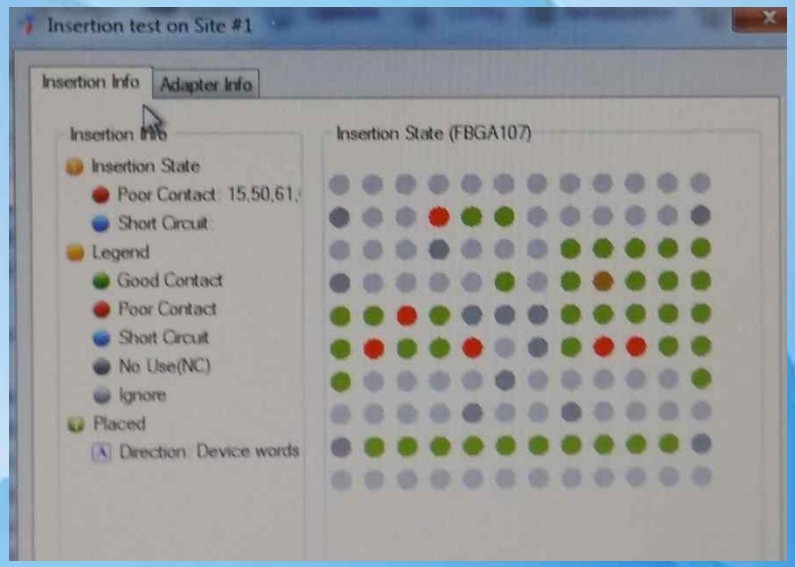
Procédure en pratique



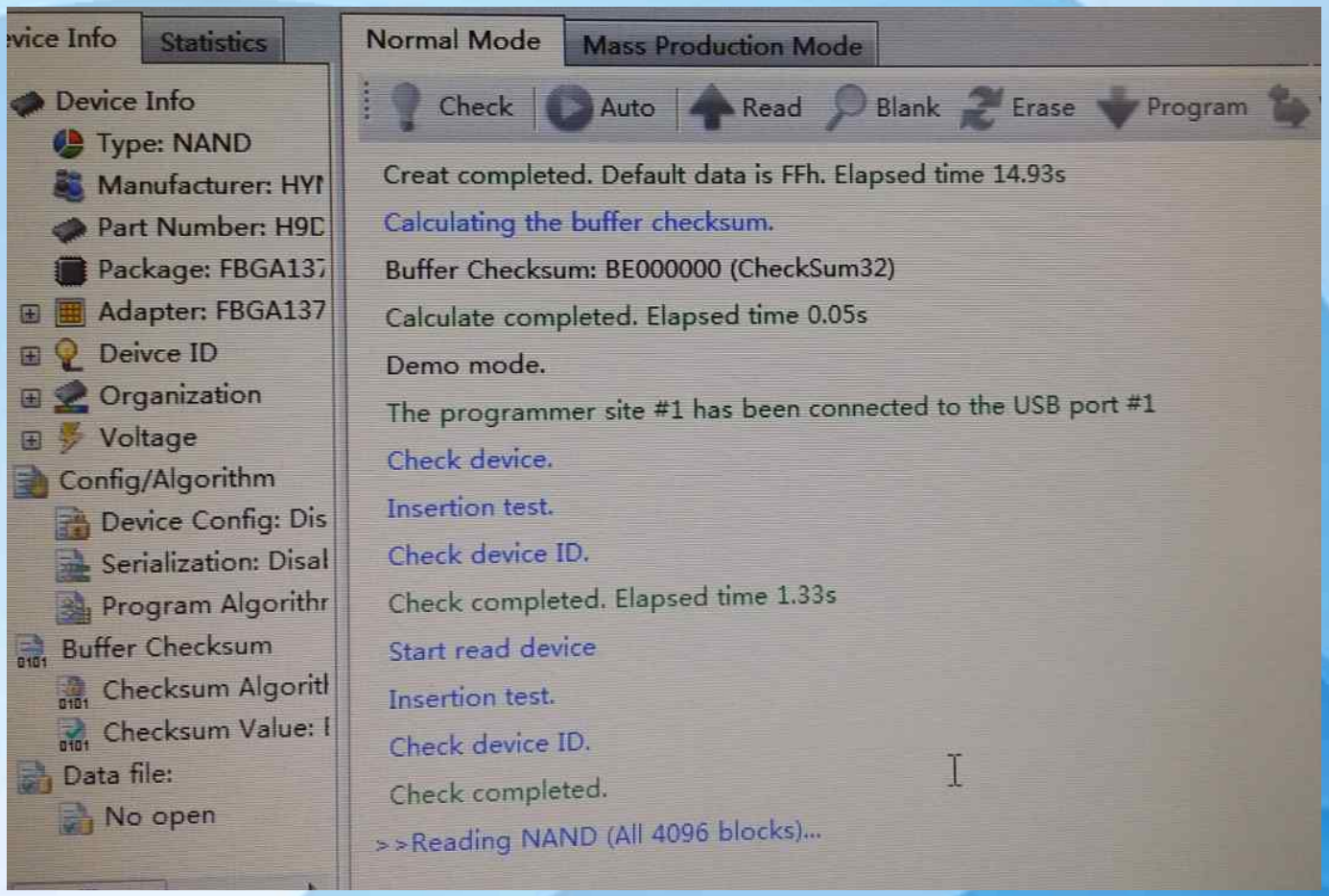
Procédure technique



Procédure technique

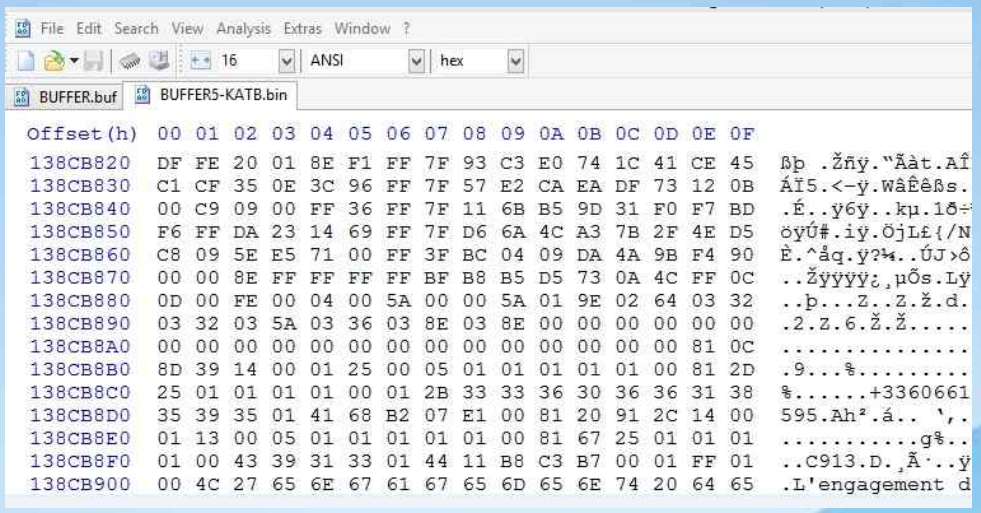


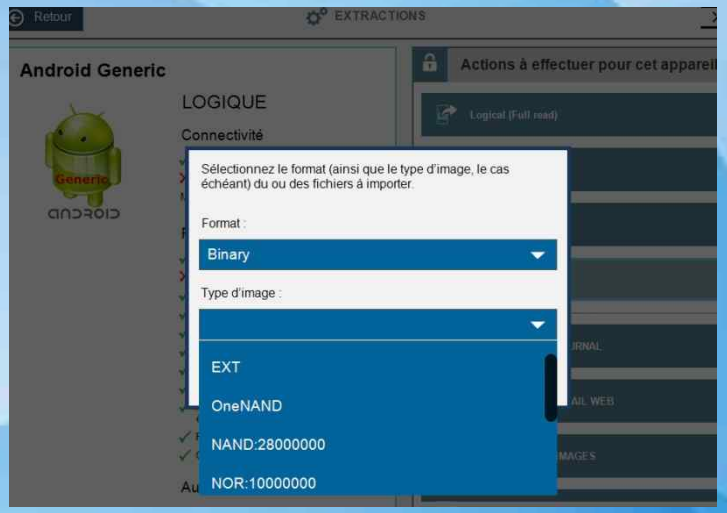
Procédure technique



Extraction des informations.

A l'aspirateur ou au ramasse-miettes….





Fin ou presque ….

Merci pour votre attention