



# 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.

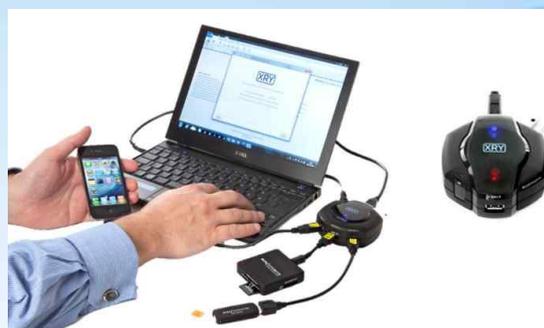
Les trois principales solutions du marché:



**CELLEBRITE**



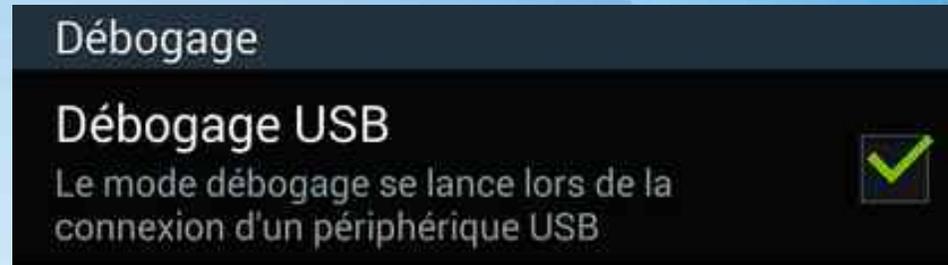
**OXYGEN**



**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, ....**

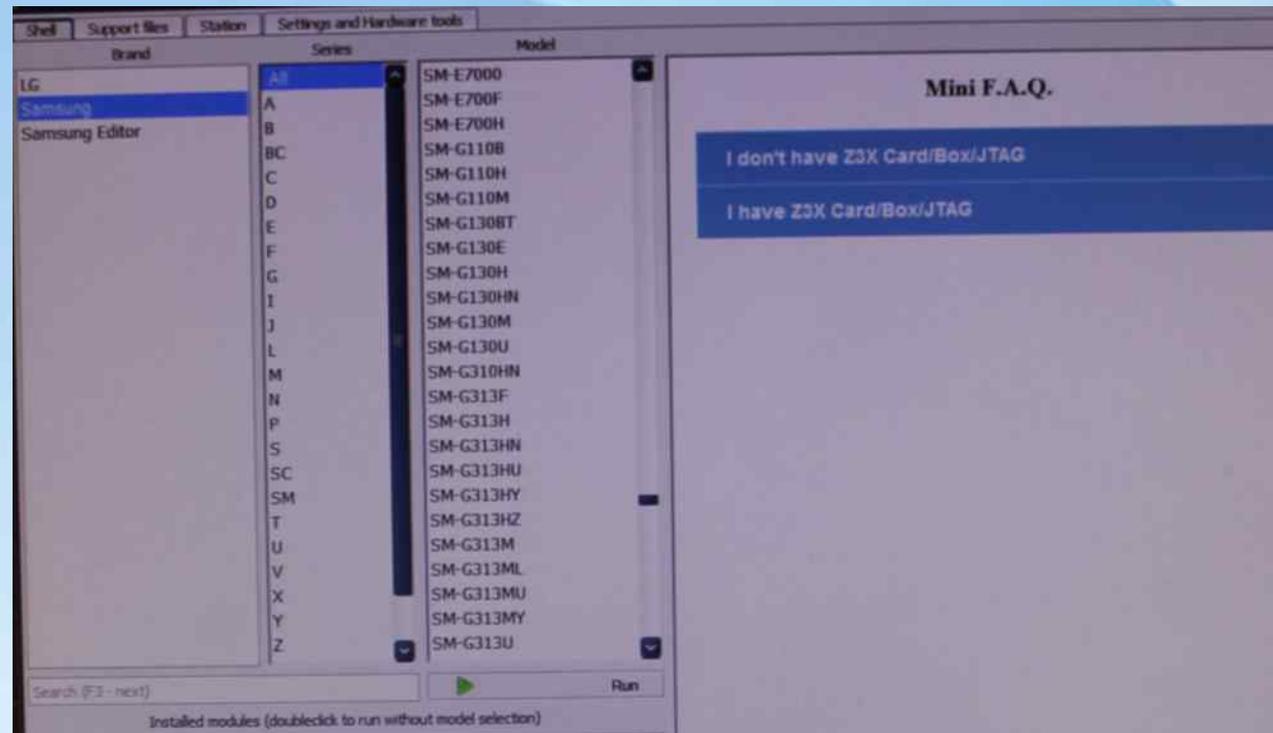
# FLASHBOX

**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.**



LG Infineon SGOLD3 tool v.1.0.9 by Z3X

**Options**

Model: KP500  
Com port: COM8  
Baud rate: 115200

**Support and other**

web: [www.z3x-team.com](http://www.z3x-team.com)  
 Receive news  
Language: English

**Source file:**  
Please select Firmware file

**Log**

Selected port: COM8  
Selected baud rate: 115200  
Selected model: KP500  
Please, reconnect battery and hold power button  
Phone found!  
Release power button.  
Sending loader...OK  
Reading info...  
IMEI: 352153-03-103205-6  
Creating backup...  
Reading EEPROM...  
Saving to file "KP500\_352153031032056\_06-10-2009\_12-26-27.eep"...OK  
Checking status...  
Unlocking. Please wait...  
Phone unlocked successfully!

**Jobs**

Connect | UART | USB

Disconnect

Write |  Firmware |  Eeprom |  Full flash

Read |  Eeprom |  Full flash

Unlock |  Read codes |  Direct

Special

**Job progress**  
0%

**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.**

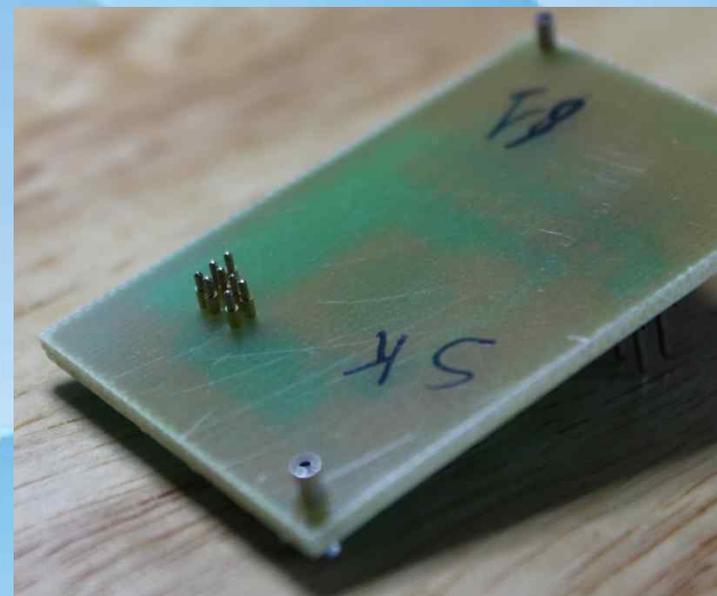
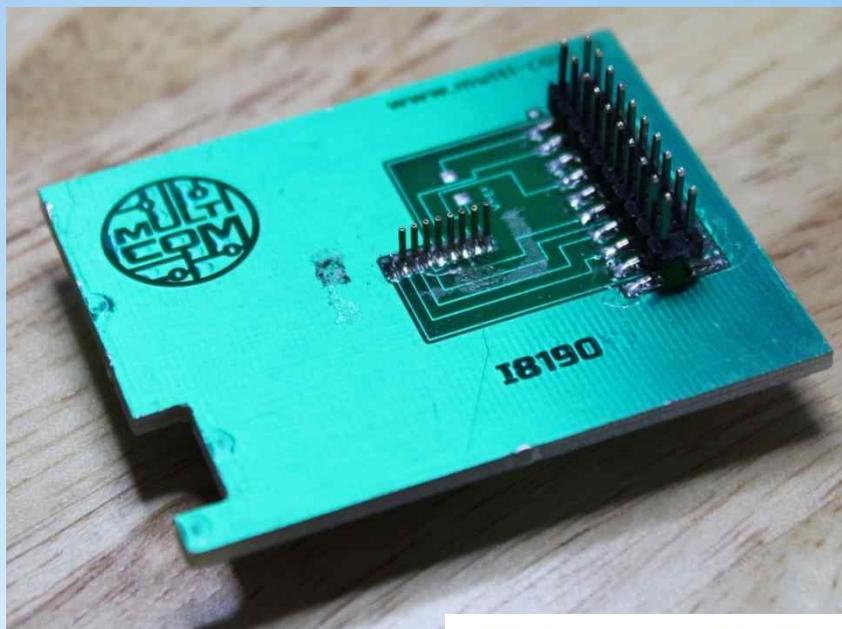


Permet de réaliser un DUMP de la mémoire:

- USB .
- Soudage.
- Circuits imprimés.

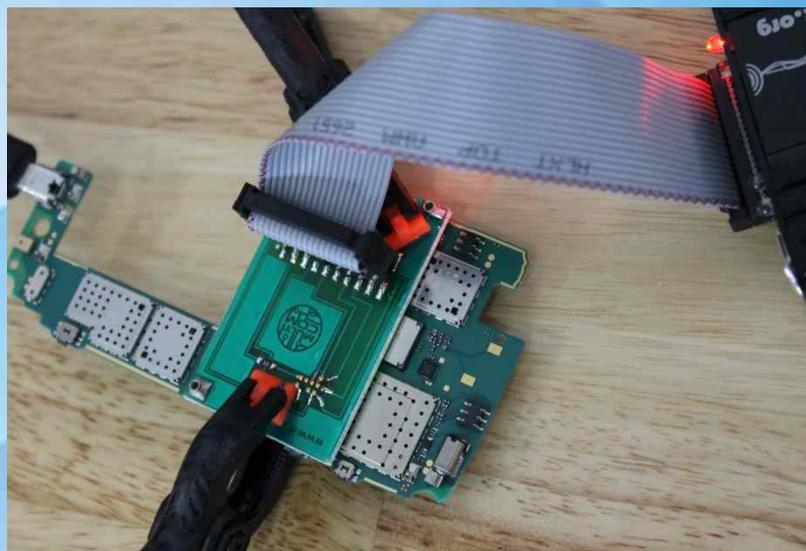
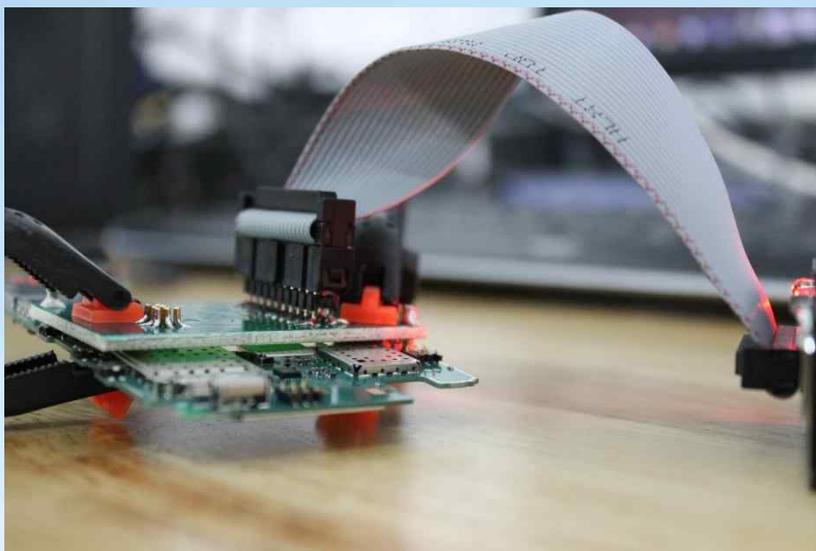
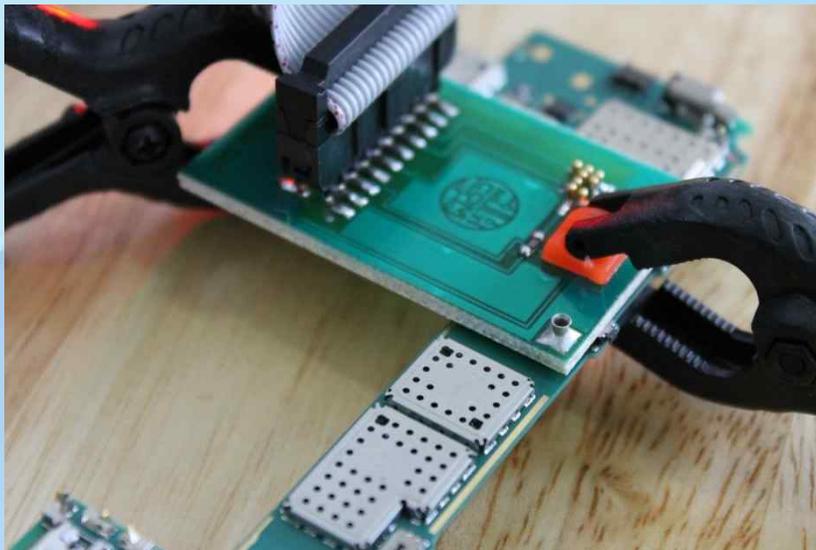
# METHODE DE FONCTIONNEMENT DE LA RIFF BOX

Sur un système de circuit électronique imprimé:

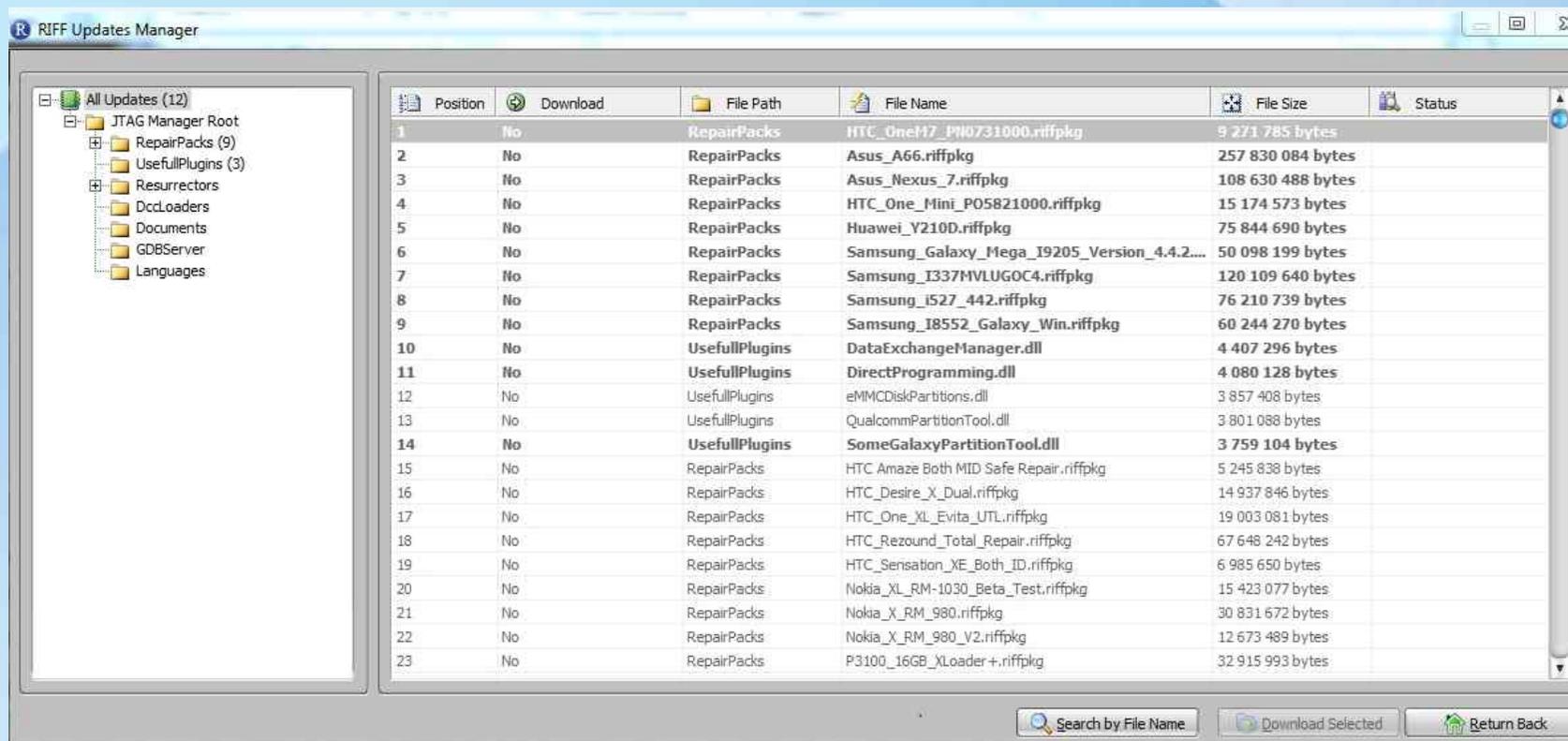


FoneFunShop®

## PRINCIPE DE LA RIFF BOX



# Bibliothèque RIFF BOX



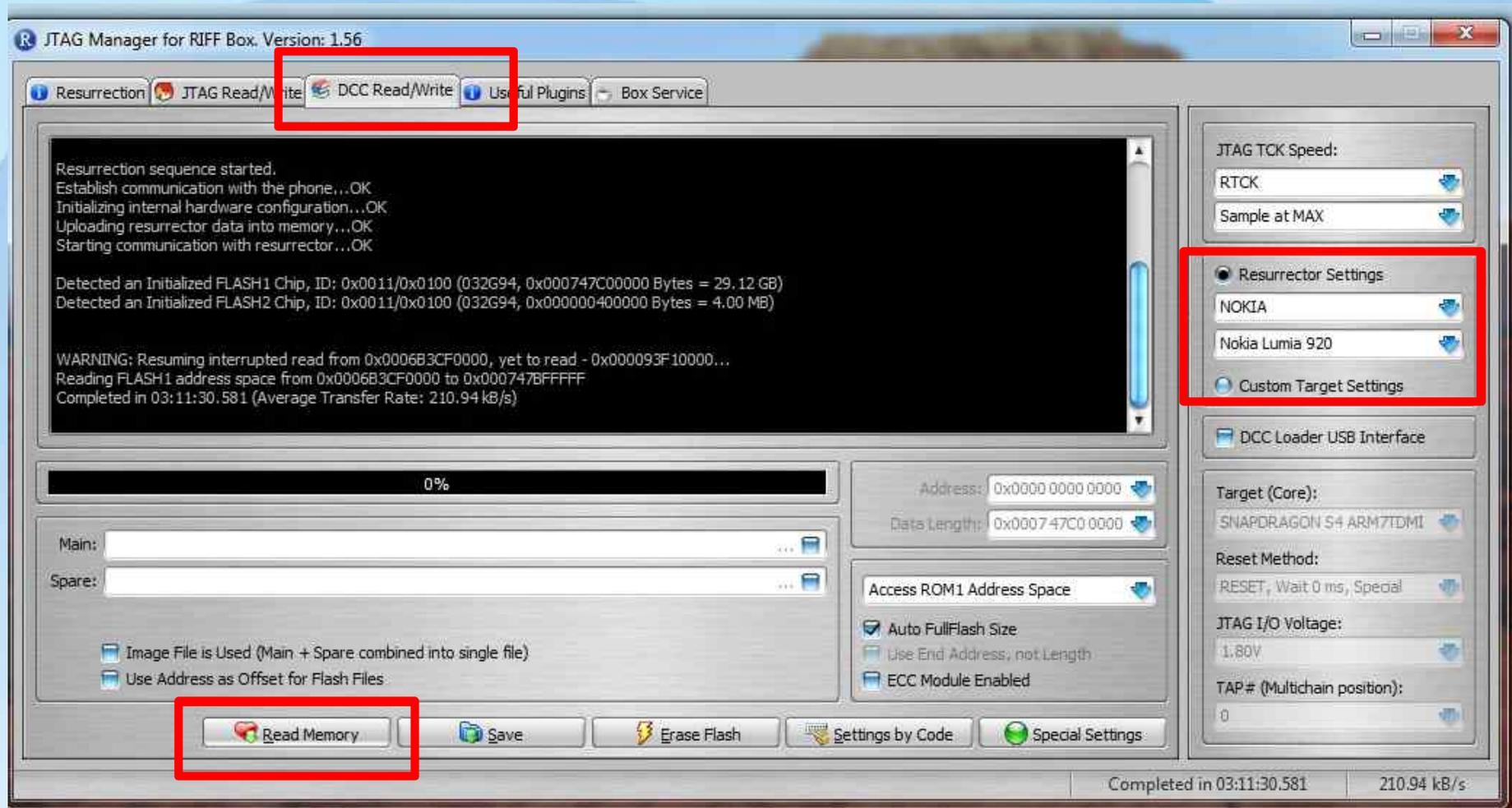
The screenshot shows the RIFF Updates Manager application window. On the left is a tree view of the update structure, and on the right is a table listing individual updates with columns for Position, Download status, File Path, File Name, File Size, and Status.

Position	Download	File Path	File Name	File Size	Status
1	No	RepairPacks	HTC_OneM7_PN0731000.rifpkg	9 271 785 bytes	
2	No	RepairPacks	Asus_A66.rifpkg	257 830 084 bytes	
3	No	RepairPacks	Asus_Nexus_7.rifpkg	108 630 488 bytes	
4	No	RepairPacks	HTC_One_Mini_P05821000.rifpkg	15 174 573 bytes	
5	No	RepairPacks	Huawei_Y210D.rifpkg	75 844 690 bytes	
6	No	RepairPacks	Samsung_Galaxy_Mega_I9205_Version_4.4.2...	50 098 199 bytes	
7	No	RepairPacks	Samsung_I337MVLUGOC4.rifpkg	120 109 640 bytes	
8	No	RepairPacks	Samsung_I527_442.rifpkg	76 210 739 bytes	
9	No	RepairPacks	Samsung_I8552_Galaxy_Win.rifpkg	60 244 270 bytes	
10	No	UsefullPlugins	DataExchangeManager.dll	4 407 296 bytes	
11	No	UsefullPlugins	DirectProgramming.dll	4 080 128 bytes	
12	No	UsefullPlugins	eMMCDiskPartitions.dll	3 857 408 bytes	
13	No	UsefullPlugins	QualcommPartitionTool.dll	3 801 088 bytes	
14	No	UsefullPlugins	SomeGalaxyPartitionTool.dll	3 759 104 bytes	
15	No	RepairPacks	HTC_Amaze_Both_MID_Safe_Repair.rifpkg	5 245 838 bytes	
16	No	RepairPacks	HTC_Desire_X_Dual.rifpkg	14 937 846 bytes	
17	No	RepairPacks	HTC_One_XL_Evita_UTL.rifpkg	19 003 081 bytes	
18	No	RepairPacks	HTC_Rezound_Total_Repair.rifpkg	67 648 242 bytes	
19	No	RepairPacks	HTC_Sensation_XE_Both_ID.rifpkg	6 985 650 bytes	
20	No	RepairPacks	Nokia_XL_RM-1030_Beta_Test.rifpkg	15 423 077 bytes	
21	No	RepairPacks	Nokia_X_RM_980.rifpkg	30 831 672 bytes	
22	No	RepairPacks	Nokia_X_RM_980_V2.rifpkg	12 673 489 bytes	
23	No	RepairPacks	P3100_16GB_XLoader+.rifpkg	32 915 993 bytes	

**Attention: Le modèle exact doit être sélectionné.**

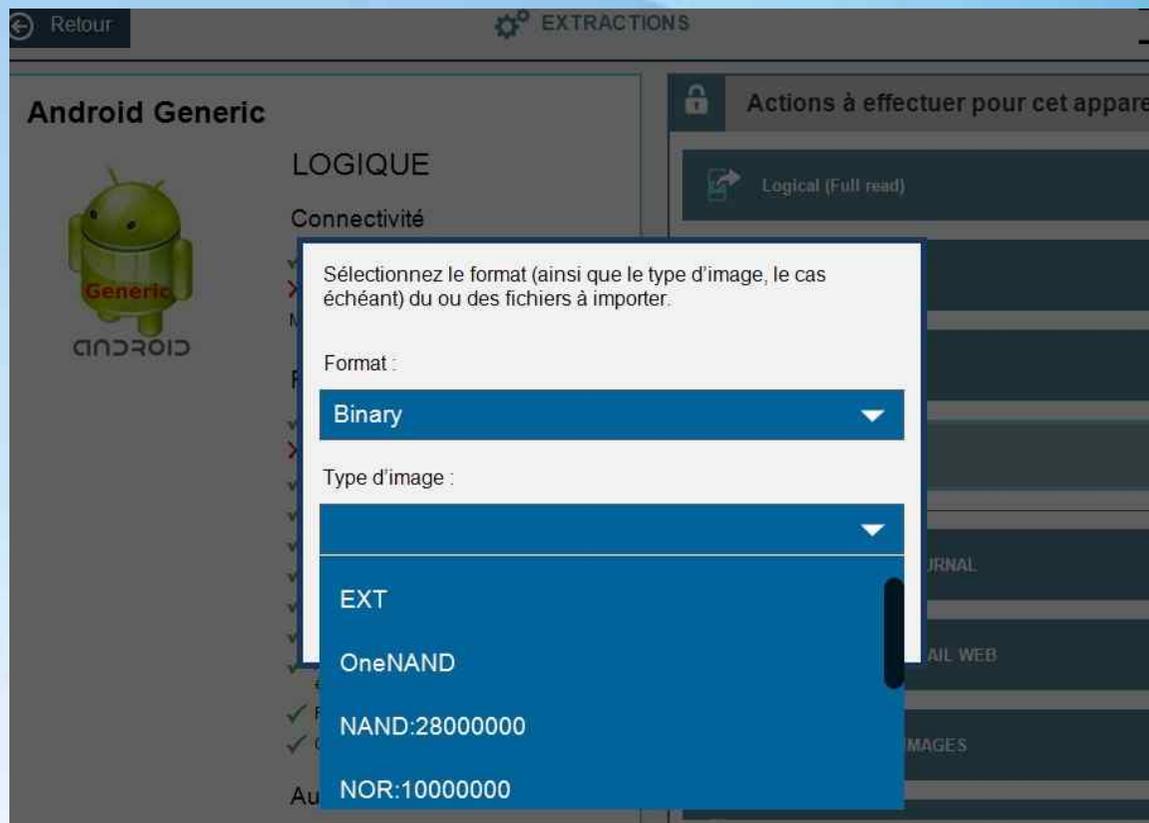
# LIMITES DE FONCTIONNEMENT DU LOGICIEL

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 blocage définitif du support, peut être même un Wipe.**

# METHODES DE FONCTIONNEMENT DU MFC

Paramétrer la clé du dispositif.

The screenshot displays the IMFC software interface with the following components:

- Device Selection:** iDevice, HTC, Samsung, Macbook, IMFC, MFC Tools (1)
- Operations:** iOS 7 auto v2.4 (2), write (3), sensor (4), update (5), clear (12)
- Settings:** Most used 20 codes & 19-2010 years (6), start value (7) 0000, format (8) FFFF (F=variable), Try all possible MMDD combinations (birthdays) (9), delay in seconds (10) 30, descending order (13)
- Extra:** 0123456789 (11), Alphabet 0-10 F not used
- Terminal Log:**

```
[data] > Serial number: 0x88888888  
[info] > Connecting to update server...  
[warn] > Waiting for reconnect...  
[info] > Erasing the memory ...  
[info] > Starting to upload ..  
[info] Starting app...  
[done] OK  
[info] > Reading FW version...  
[data] > FWVersion is 21  
[info] update already applied correctly  
[info] Searching MFC Dongle ...  
[sett] Applying start value 0000 format FFFF delay 5000  
[info] > Writing ...  
[data] > FWVersion is 21  
[data] > New start value 0000 format FFFF with setting 02 delay 5000  
[done] OK
```
- Buttons:** Read (14), Quit (15)
- Status Bar:** Status Here are the status messages displayed! (16), Step 1 (17), Dongle NORMAL MODE, 0x88888888

**IMFC: permet de décèler plus de détails issus du support.**

# CONSULTER EN LIGNE LE MANUEL DU MFC

Paramétrer la clé du dispositif.

The screenshot displays the IMFC software interface with the following components:

- Navigation:** Tabs for iDevice, HTC, Samsung, Macbook, IMFC, and MFC Tools. A red '1' is placed above the IMFC tab.
- Operations:** A dropdown menu set to 'iOS 7 auto v2.4'. A red '2' is placed next to it. Below are checkboxes for 'write' (red '3'), 'sensor' (red '4'), 'update' (red '5'), and 'clear' (red '12').
- Settings:** A section with a red '6' above it. It includes a checkbox for 'Most used 20 codes & 19-2010 years' (red '6'), a text input for 'start value' (red '7') containing '0000', a text input for 'format (F=variable)' (red '8') containing 'FFFF', a text input for 'delay in seconds' (red '10') containing '30', a checkbox for 'Try all possible MMDD combinations (birthdays)' (red '9'), and a checkbox for 'descending order' (red '13').
- Extra:** A text input for a key (red '11') containing '0123456789' and the text 'Alphabet 0-10 F not used'.
- Terminal Log:** A central area showing system messages such as '[data] > Serial number: 0x88888888', '[info] > Connecting to update server...', '[warn] > Waiting for reconnect...', '[info] > Erasing the memory ...', '[info] > Starting to upload ..', '[info] Starting app...', '[done] OK', '[info] > Reading FW version...', '[data] > FWVersion is 21', '[info] update already applied correctly', '[info] Searching MFC Dongle ...', '[sett] Applying start value 0000 format FFFF delay 5000', '[info] > Writing ...', '[data] > FWVersion is 21', and '[data] > New start value 0000 format FFFF with setting 02 delay 5000'. A red '14' is placed above the bottom of this area.
- Buttons:** 'Read' (red '14') and 'Quit' (red '15') buttons.
- Status Bar:** At the bottom, it shows 'Status Here are the status messages displayed!' (red '16'), 'Step 1' (red '17'), 'Dongle NORMAL MODE', and '0x88888888'.

**IMFC: permet de décèler plus de détails issus du support.**

# IMFC

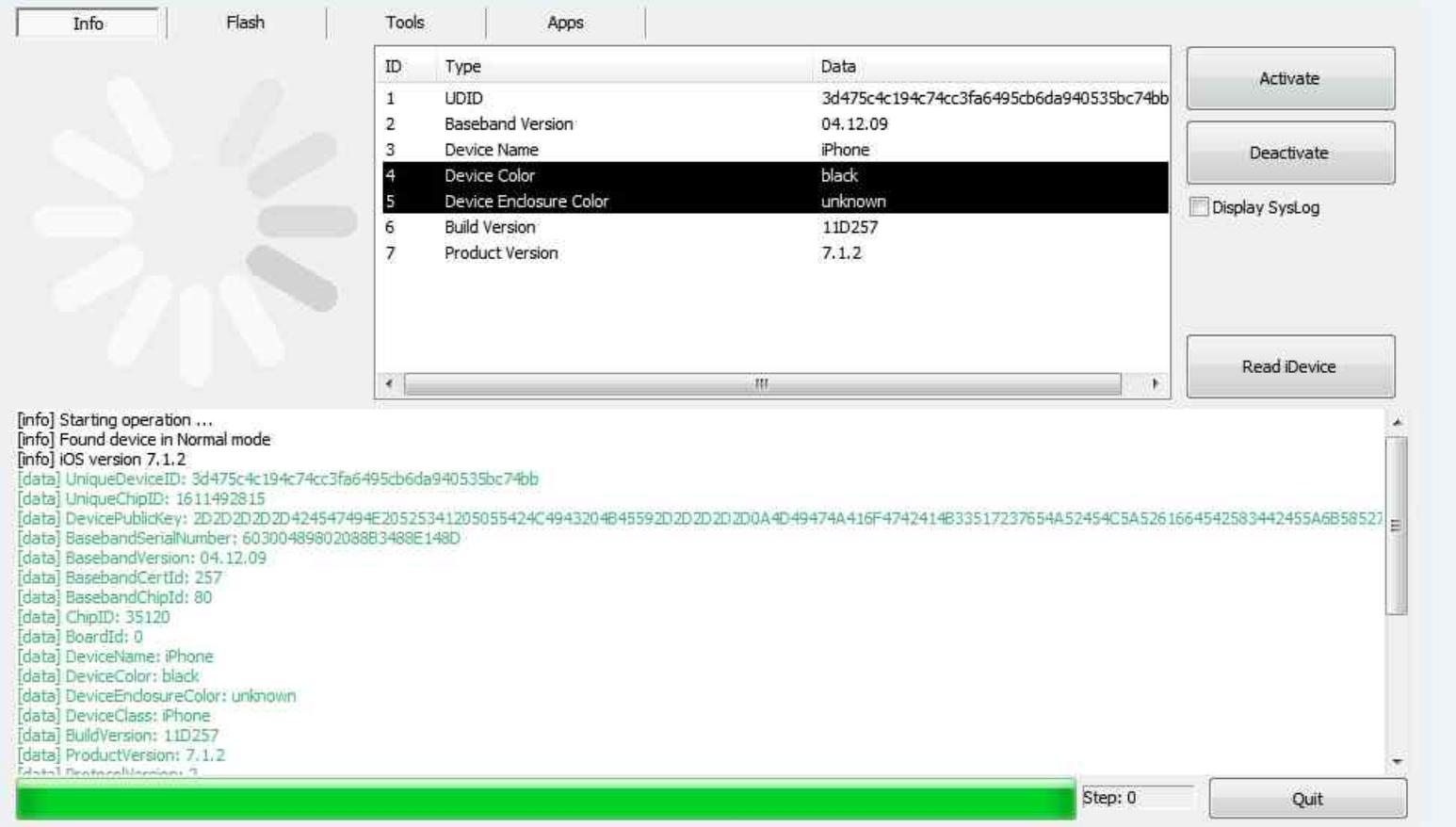
The screenshot displays the IMFC application interface. It features a top navigation bar with tabs for 'Info', 'Flash', 'Tools', and 'Apps'. The 'Info' tab is active, showing a table of device information. To the right of the table are buttons for 'Activate', 'Deactivate', 'Display SysLog' (with a checkbox), and 'Read iDevice'. Below the table is a large text area containing a log of system data and error messages. At the bottom, there is a green progress bar, a 'Step: 0' indicator, and a 'Quit' button.

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

```
[data] DeviceEnclosureColor: unknown
[data] DeviceClass: iPhone
[data] BuildVersion: 11D257
[data] ProductVersion: 7.1.2
[data] ProtocolVersion: 2
[data] ProductionSOC: TRUE
[data] FirmwarePreflightInfo:
  CertID :257
  ChipID :80
  ChipSerialNo :6030048980208883488E148D
  Nonce :77945080649AC5EF89B72DA9C866CBEB55D82829
  VendorID :2
[data] ActiveWirelessTechnology: kCTWirelessTechnologyUnknown
[data] DeviceSupportsFaceTime: TRUE
[data] TelephonyCapability: TRUE
[erro] Could not connect to lockdown. Exiting.
[done] Operation finished!
```

**IMFC: permet de décèler plus de détails issus du support.**

# IMFC



The screenshot displays the IMFC software interface. The 'Info' tab is selected, showing a table of device information. The table has three columns: ID, Type, and Data. The data is as follows:

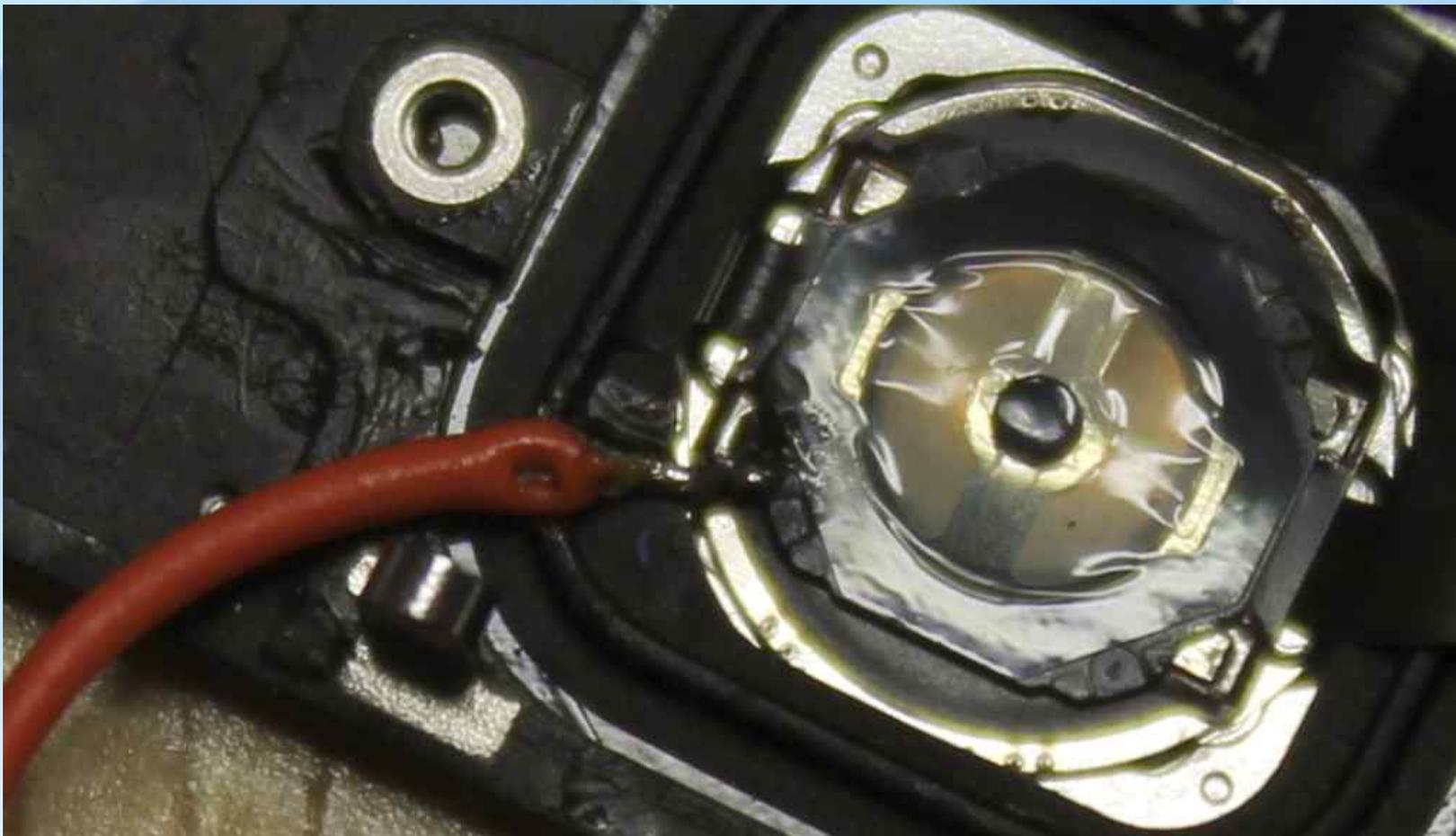
ID	Type	Data
1	UDID	3d475c4c194c74cc3fa6495cb6da940535bc74bb
2	Baseband Version	04.12.09
3	Device Name	iPhone
4	Device Color	black
5	Device Endosure Color	unknown
6	Build Version	11D257
7	Product Version	7.1.2

Below the table, there is a log window showing the following information:

```
[info] Starting operation ...  
[info] Found device in Normal mode  
[info] iOS version 7.1.2  
[data] UniqueDeviceID: 3d475c4c194c74cc3fa6495cb6da940535bc74bb  
[data] UniqueChipID: 1611492815  
[data] DevicePublicKey: 2D2D2D2D2D424547494E20525341205055424C4943204B45592D2D2D2D2D0A4D49474A416F4742414B33517237654A52454C5A5261664542583442455A6B58527  
[data] BasebandSerialNumber: 6030048980208883488E148D  
[data] BasebandVersion: 04.12.09  
[data] BasebandCertId: 257  
[data] BasebandChipId: 80  
[data] ChipID: 35120  
[data] BoardId: 0  
[data] DeviceName: iPhone  
[data] DeviceColor: black  
[data] DeviceEndosureColor: unknown  
[data] DeviceClass: iPhone  
[data] BuildVersion: 11D257  
[data] ProductVersion: 7.1.2  
[data] ProtocolVersion: 3
```

At the bottom of the interface, there is a green progress bar, a 'Step: 0' indicator, and a 'Quit' button.

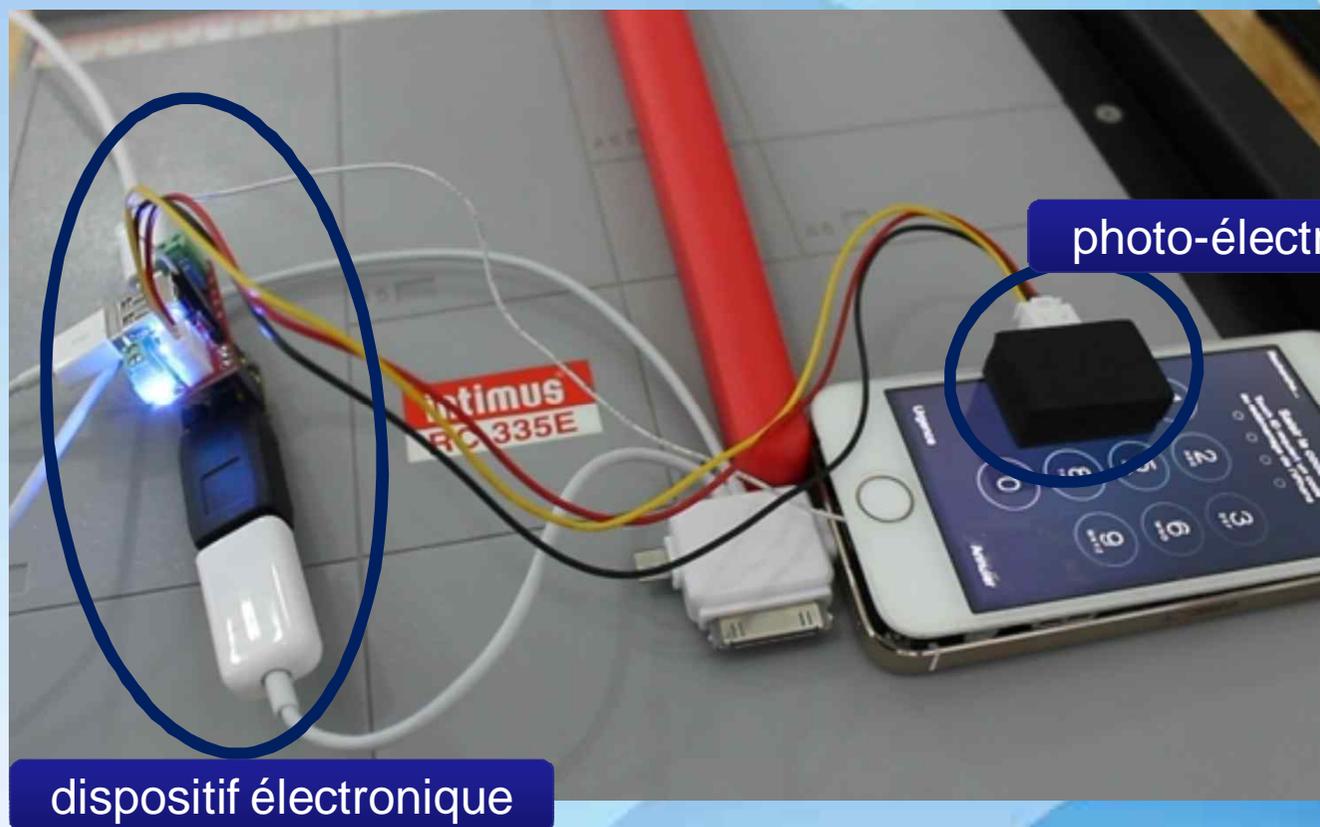
## **DIFFICULTE: Soudure**



# 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%**



**50%**



# Méthode: FLASH RECOVERY

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

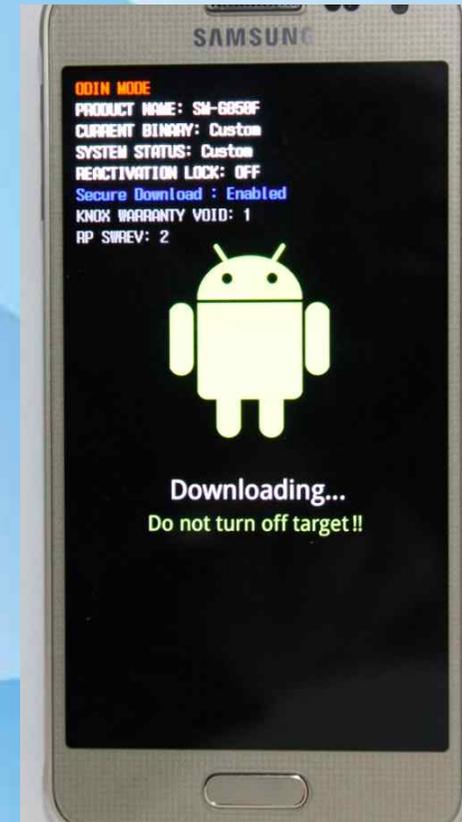
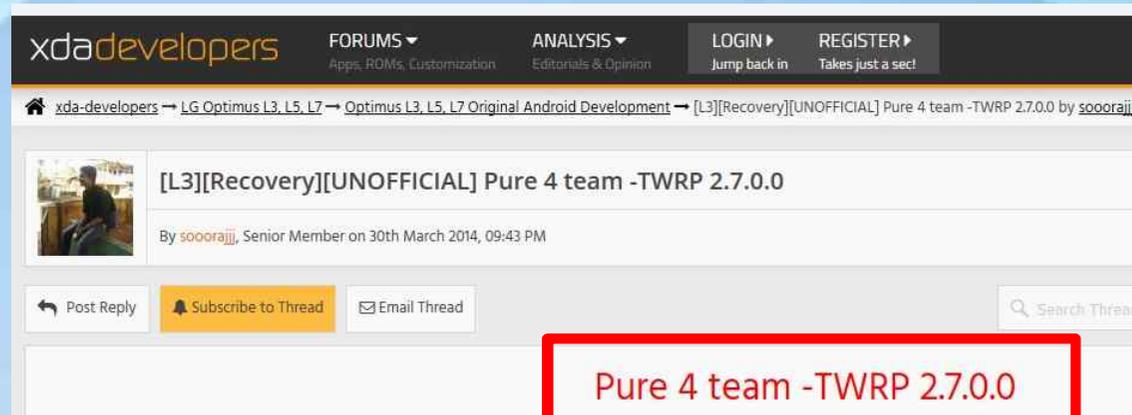
Pour le modifier, il convient de vérifier l'existence d'un binaire (éprouvé).

**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/>*



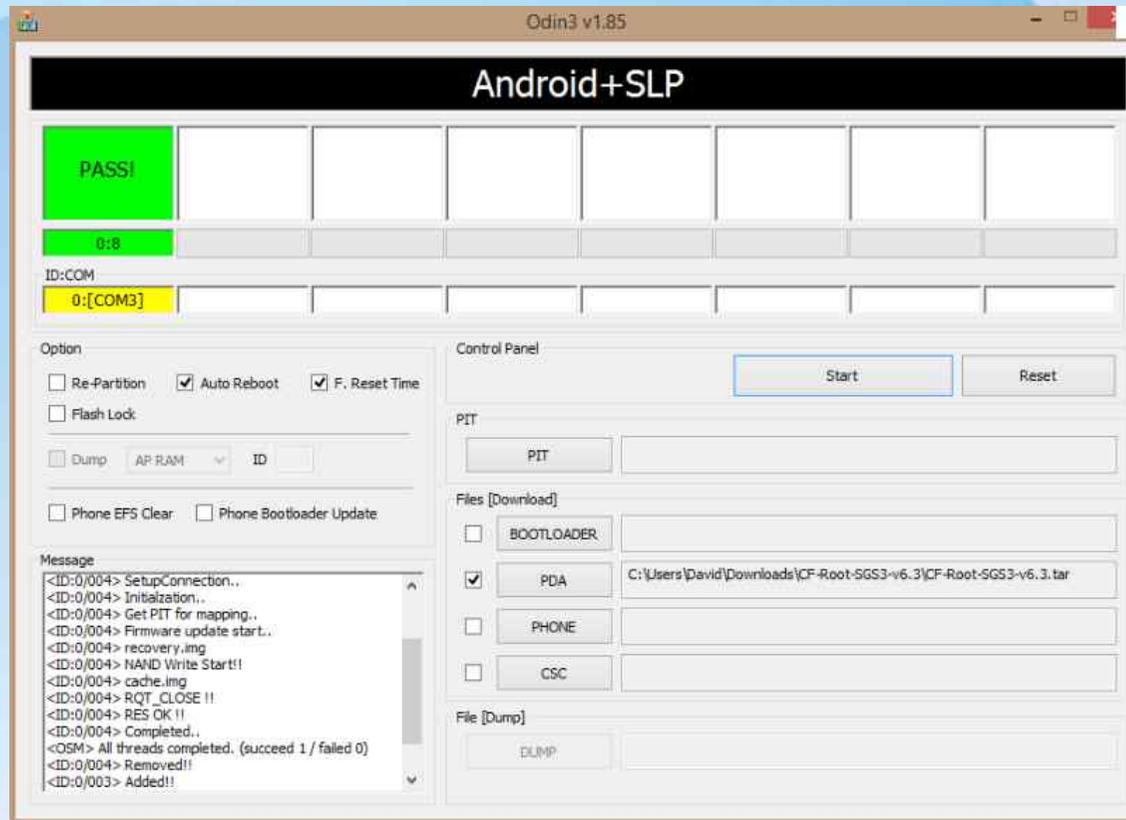
# FLASH RECOVERY



**Downloading**

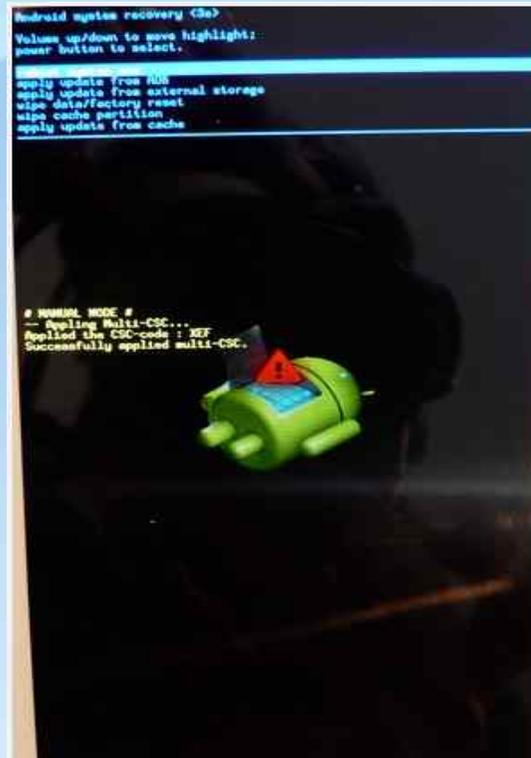
**Bien lire les commentaires postés dans le forum.  
Plusieurs teams de développement (fastboot, flashtools, ...).**

# FLASH RECOVERY



**Chaque modèle de téléphone possède sa combinaison de touches.**

# FLASH RECOVERY



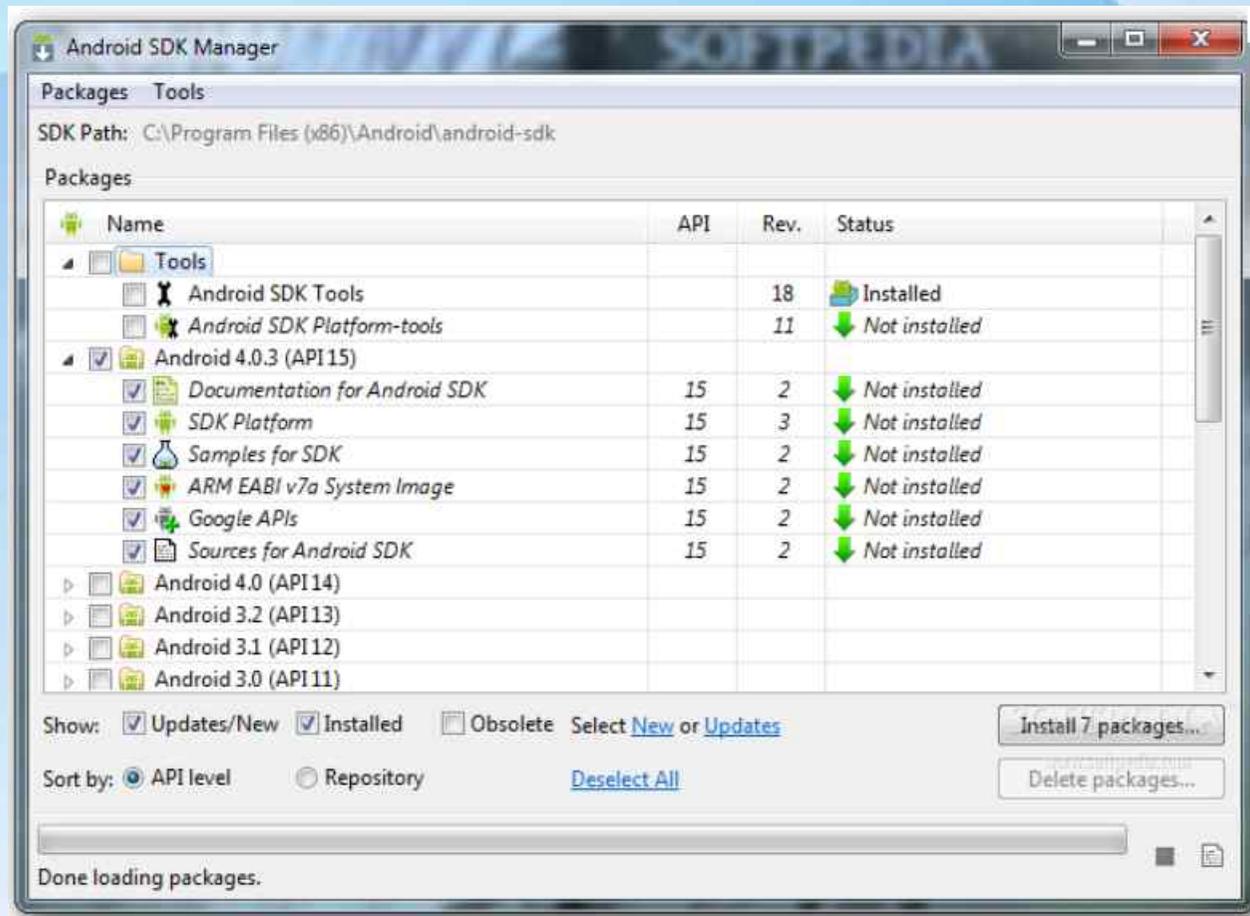
Recovery - avant



Recovery - après

**Monter la partition système en restant en mode recovery.**

# Installation du pack ANDROID SDK



# Lancement de la console ADB

```
Administrateur : C:\Windows\system32\cmd.exe - adb shell

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached
4100d9aec8dfa187    recovery

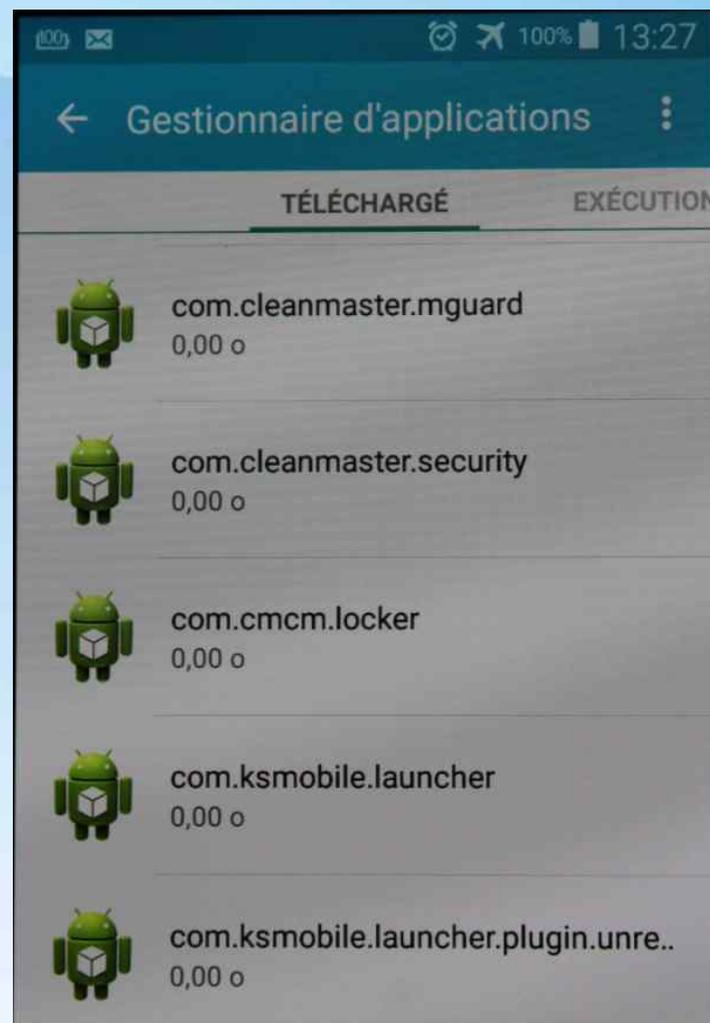
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb shell
~ # ↵[6ncd /data/app
cd /data/app
/data/app # ↵[6nls
ls
com.android.chrome-1
com.android.vending-2
com.cleanmaster.mguard-2.old
com.cleanmaster.security-2.old
com.cmcm.locker-2.old
com.droptbox.android-2
com.dsi.ant.plugins.antplus-2.apk
com.dsi.ant.service.socket-2.apk
com.fantasticdroid.flashalerts-1.apk
com.google.android.apps.books-1
com.google.android.apps.docs-2
com.google.android.apps.magazines-2
com.google.android.apps.maps-1
com.google.android.apps.plus-2
com.google.android.gm-2
com.google.android.gms-1
com.google.android.googlequicksearchbox-2
com.google.android.marvin.talkback-4.apk
com.google.android.music-2
com.google.android.play.games-1
com.google.android.talk-1
com.google.android.tts-1
com.google.android.videos-4.apk
com.google.android.webview-2
com.google.android.youtube-1
com.google.earth-1
com.hp.android.printservice-1
com.ijinshan.kbatterydoctor_en-2
com.ksmobile.ch-1
com.ksmobile.launcher-2.old
com.ksmobile.launcher.plugin.unread-2.old
com.opera.mini.native-2
com.sec.android.app.samsungapps-2.apk
com.sec.android.iap-1.apk
com.sec.app.samsungprintservice-2.apk
com.sec.spp.push-2.apk
com.staircase3.opensignal-1
com.supercell.clashofclans-1
flipboard.app-1
mcRegistry
/data/app # ↵[6n
```

## Console ADB: Neutralisation des fichiers de sécurité

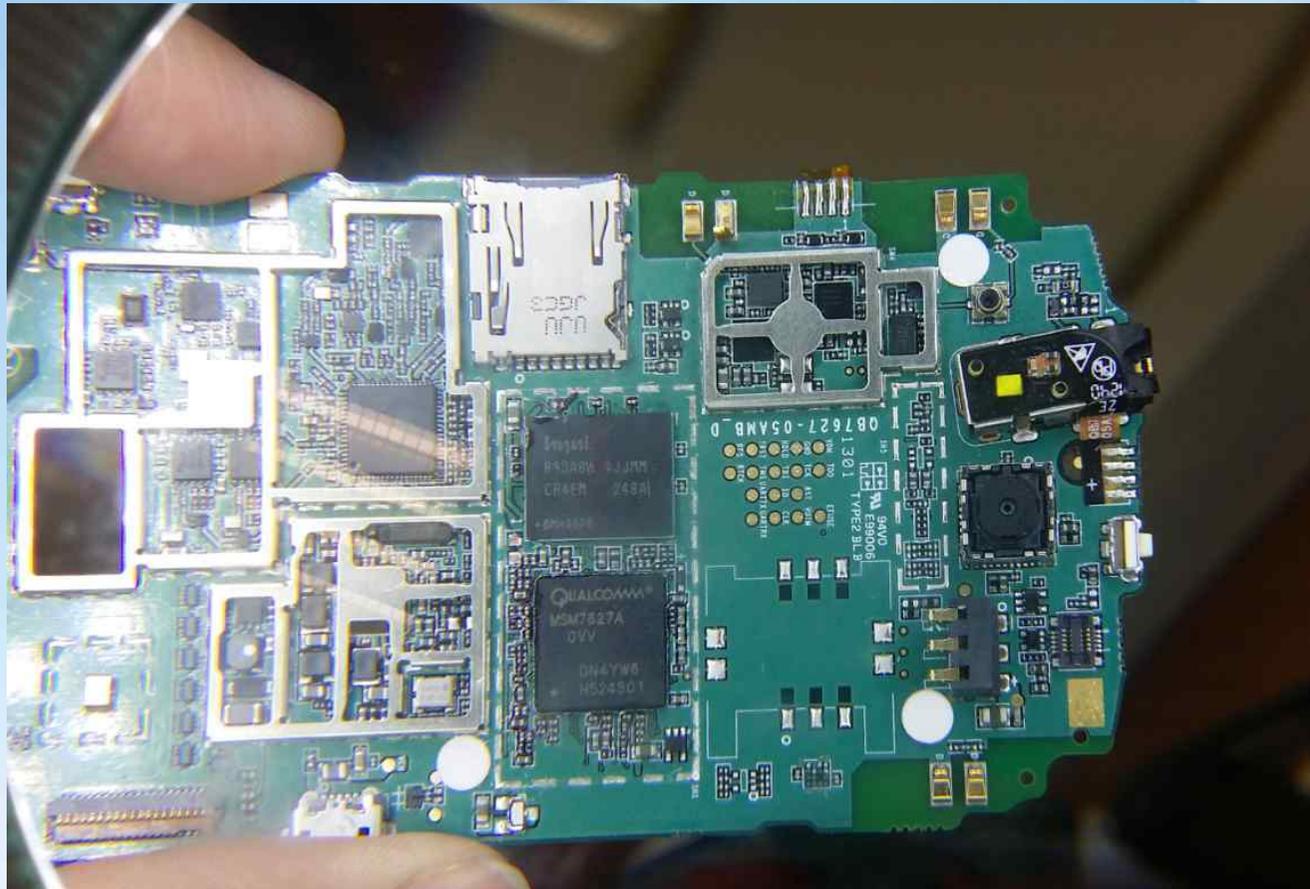
```
adb reboot [bootloader|recovery] - reboots the device, t
tloader or recovery program
adb root - restarts the adbd daemon
adb usb - restarts the adbd daemon
tcpip <port> - restarts the adbd daemon lister
ified port
networking:
adb ppp <tty> [parameters] - Run PPP over USB.
Note: you should not automatically start a PPP connection
<tty> refers to the tty for PPP stream. Eg. dev:/dev/omap
[parameters] - Eg. defaultroute debug dump local notty us
adb sync notes: adb sync [ <directory> ]
<localdir> can be interpreted in several ways:
- If <directory> is not specified, both /system and /dat
updated.
- If it is "system" or "data", only the corresponding pa
is updated.
D:\N7ADB>adb shell rm /data/system/gesture.key_
```

**Confrontation à des problèmes de droit.**

# Côté application



## CHIP OFF ou la manipulation de la dernière chance



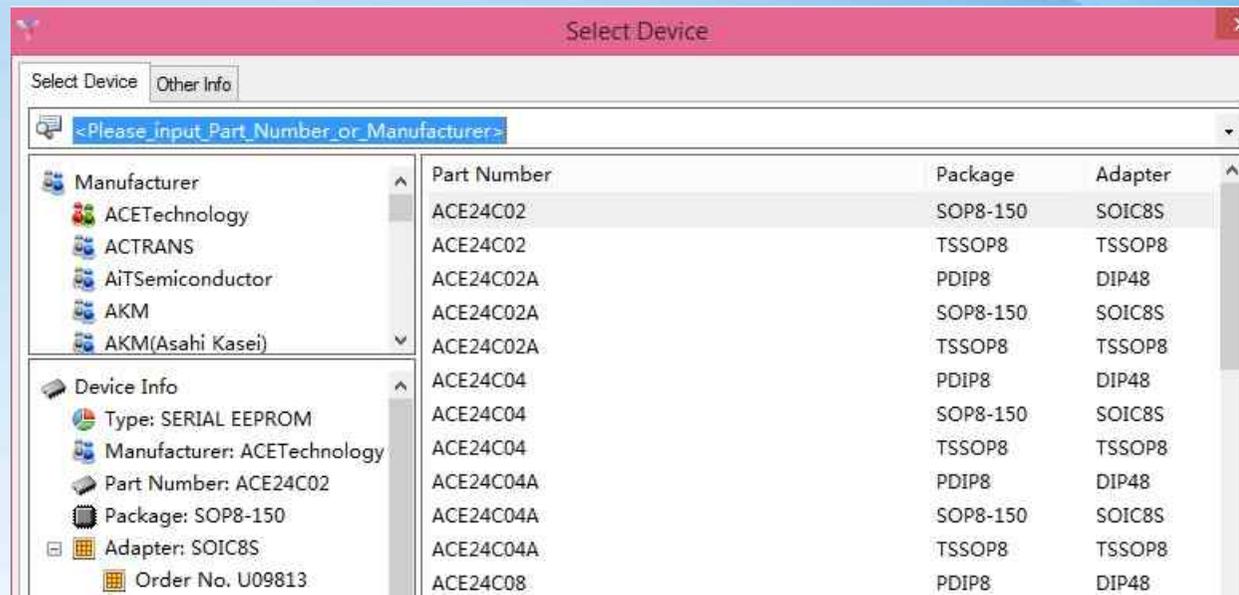
## L'appareil de référence



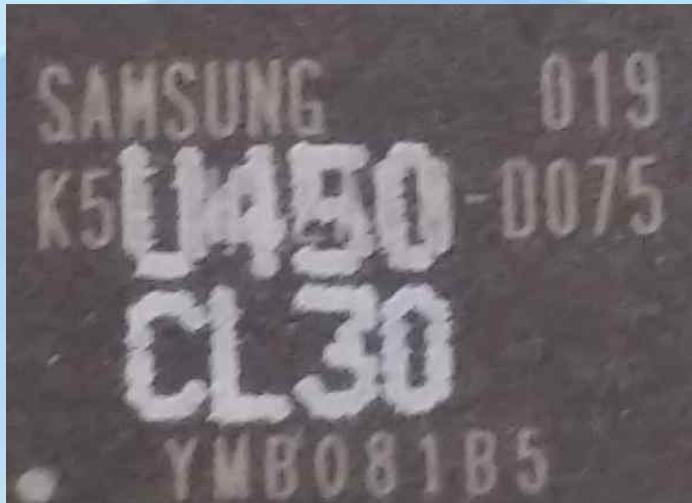
## L'appareil de référence



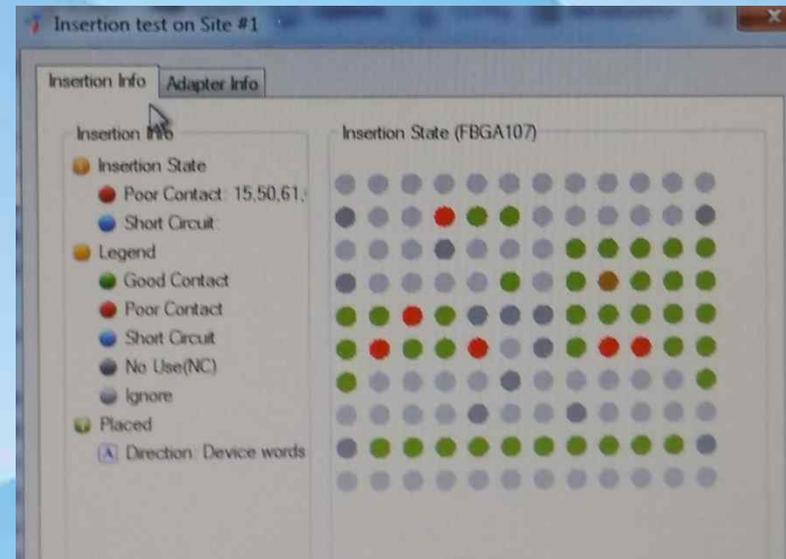
# Procédure en pratique



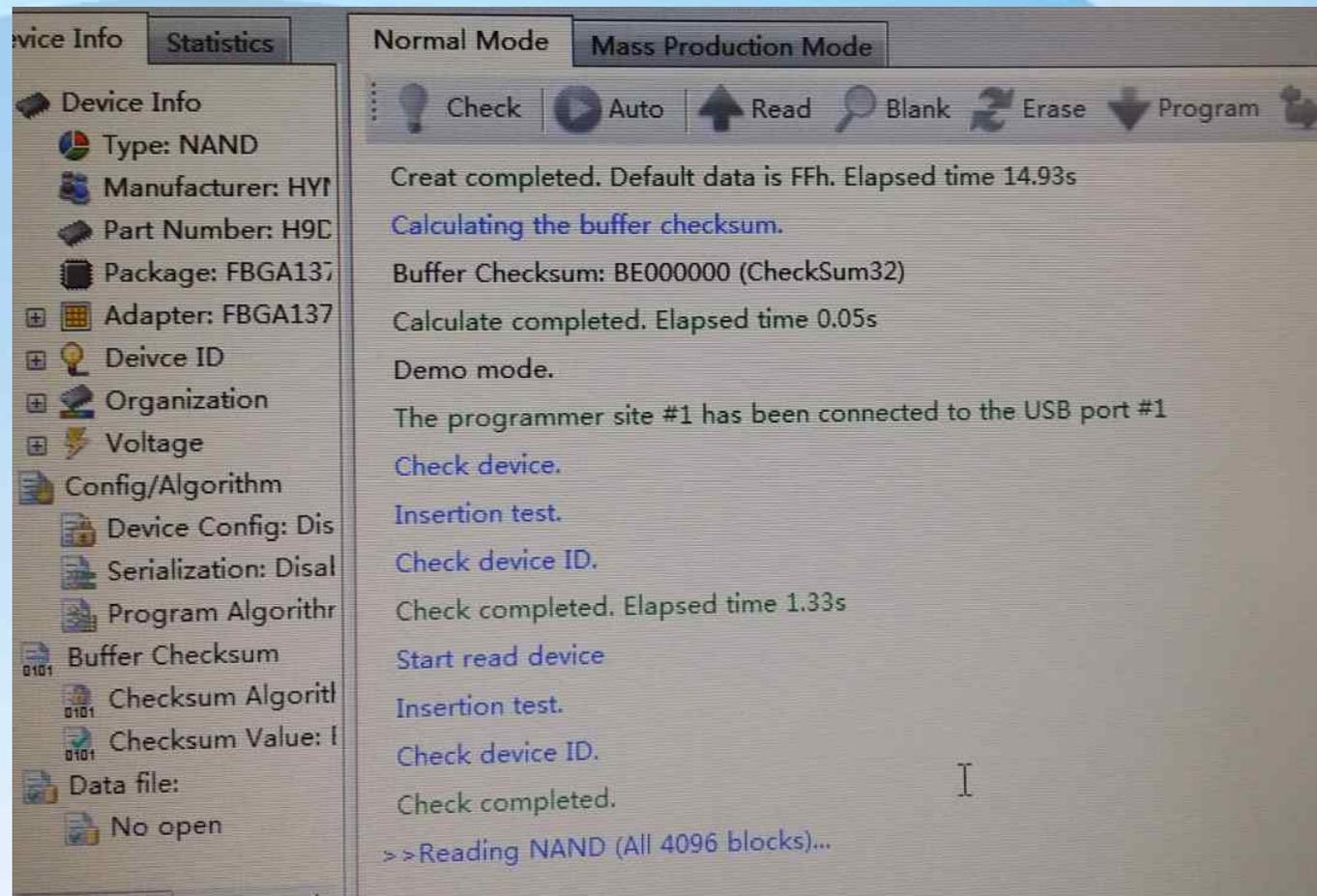
## Procédure technique



# Procédure technique

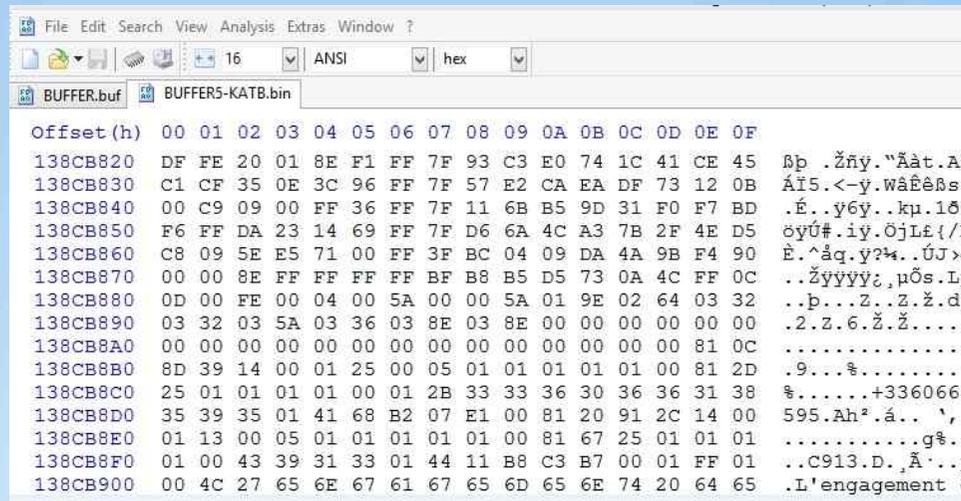


# Procédure technique



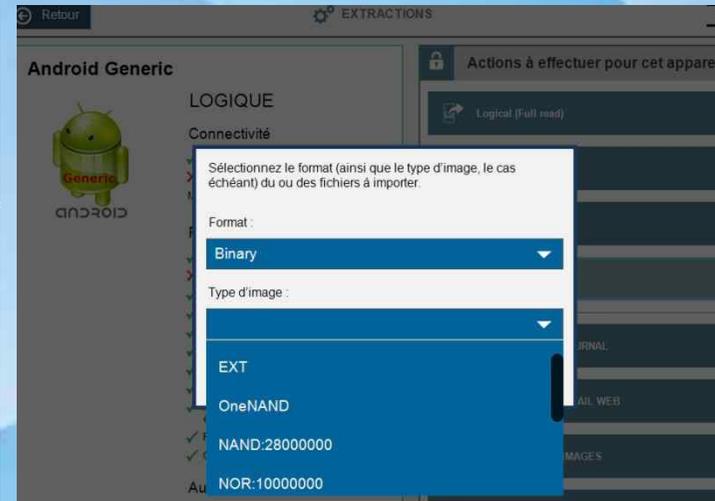
# Extraction des informations.

A l'aspirateur ou au ramasse-miettes....



A screenshot of a hex editor window. The menu bar includes File, Edit, Search, View, Analysis, Extras, and Window. The toolbar shows a page size of 16 and encoding options for ANSI and hex. Two files are open: BUFFER.buf and BUFFERS-KATB.bin. The main area displays a memory dump with columns for Offset (h) and hex data. The hex data is shown in pairs of columns, with corresponding ASCII characters to the right.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F		
138CB820	DF	FE	20	01	8E	F1	FF	7F	93	C3	E0	74	1C	41	CE	45	8p .žňý."Äät.Aİ	
138CB830	C1	CF	35	0E	3C	96	FF	7F	57	E2	CA	EA	DF	73	12	0B	Äİ5.<-ÿ.WäÊßs.	
138CB840	00	C9	09	00	FF	36	FF	7F	11	6B	B5	9D	31	F0	F7	BD	.É..ÿ6ÿ..kp.1ð	
138CB850	F6	FF	DA	23	14	69	FF	7F	D6	6A	4C	A3	7B	2F	4E	D5	öÿŰ#.iÿ.ÖjLÉ{/N	
138CB860	C8	09	5E	E5	71	00	FF	3F	BC	04	09	DA	4A	9B	F4	90	È.^âq.ÿ?*...ŰJ>ð	
138CB870	00	00	8E	FF	FF	FF	FF	BF	B8	B5	D5	73	0A	4C	FF	0C	..žÿÿÿÿÿç,µŌs.Lÿ	
138CB880	0D	00	FE	00	04	00	5A	00	00	5A	01	9E	02	64	03	32	..p...z..z.ž.d.	
138CB890	03	32	03	5A	03	36	03	8E	03	8E	00	00	00	00	00	00	.2.z.6.ž.ž.....	
138CB8A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	81	0C	.....
138CB8B0	8D	39	14	00	01	25	00	05	01	01	01	01	01	00	81	2D	.9...%.....	
138CB8C0	25	01	01	01	01	00	01	2B	33	33	36	30	36	36	31	38	%.....+3360661	
138CB8D0	35	39	35	01	41	68	B2	07	E1	00	81	20	91	2C	14	00	595.Ah².á.. \,	
138CB8E0	01	13	00	05	01	01	01	01	01	01	00	81	67	25	01	01	.....g%..	
138CB8F0	01	00	43	39	31	33	01	44	11	B8	C3	B7	00	01	FF	01	..C913.D.Ā...ÿ	
138CB900	00	4C	27	65	6E	67	61	67	65	6D	65	6E	74	20	64	65	.L'engagement d	



A screenshot of the EXTRACTIONS application interface. The window title is 'EXTRACTIONS'. On the left, there is a section for 'Android Generic' with an Android logo. The main area is titled 'LOGIQUE' and 'Connectivité'. A dialog box is open, prompting the user to 'Sélectionnez le format (ainsi que le type d'image, le cas échéant) du ou des fichiers à importer.' The dialog has two dropdown menus: 'Format' (set to 'Binary') and 'Type d'image' (set to 'EXT'). Below these are several image format options: 'OneNAND', 'NAND:28000000', and 'NOR:10000000'. On the right side of the application, there is a section 'Actions à effectuer pour cet appareil' with a 'Logical (Full read)' button.

# Fin ou presque ....



## Merci pour votre attention