TUTORIEL POUR MANIPULATION DE ROMS
SIATRONICS.COM
Août 2008

Ce tutoriel servait à l'origine aux utilisateurs de téléphones HTC désirant manipuler la ROM de leurs téléphones. Il n'a ici que vocation d'enseignement, le téléphone HTC étant pris à titre d'exemple. SIATRONICS ne saurait être responsable des conséquences et dommages éventuels découlant de l'utilisation de ce tutoriel ou des logiciels fournis pour la manipulation des ROMs.

1- Dumper votre ROM

Voici comment réaliser une sauvegarde complète de votre rom.

1 désactiver la sécurité :
1.1 installer un éditeur de registre sur le PDA
1.2 Modifier la ligne de registre : HKLM\Security\Policies\Policies valuename '00001001' dword:2, modifier et mettre dword:1
1.3 soft reset

2 télécharger et dézipper :itsutilsbin-20070705.zip que vous trouverez dans le pack ROMs. Dézippez de préférence dans mes documents (ca sera plus simple pour le chemin d'accès)

3 autoriser la connexion du téléphone :
3.1 connecter le téléphone au PC via USB
3.2 Lancer pdocread.exe (la fenêtre s'ouvre et se ferme) il se peut qu'un message apparaisse sur le téléphone, clicker oui.

4 Accès à l'outil sous Dos :
4.1 allez sous DOS (executer/cmd)
4.2 positionnez vous sur le répertoire ou vous avez dézipper itsutilsbin (cd espace le nom du repertoire pour rentrer dans un répertoire, cd.. pour remonter d'un niveau)

5 Détail de la rom :
Tapez : « pdocread.exe –l »

Vous devez voir apparaitre un détail comme ça :

```
F:\Documents de D@vid>pdocread.exe -l
210.38M (0xd260000) FLASHDR
|            3.12M (0x31f000) Part00
|            3.50M (0x380000) Part01
|           70.50M (0x4680000) Part02
|          133.25M (0x8540000) Part03
  1.89G (0x79280000) DSK1:
|            1.89G (0x79120e00) Part00
 20.00k (0x5000) BTD1:
|           19.00k (0x4c00) PART00
STRG handles:
handle e5cf4c92 19.00k (0x4c00)
handle e5c264fa  1.89G (0x79120e00)
handle 2747ec1a133.25M (0x8540000)
handle 4748c0e6 70.50M (0x4680000)
handle 874b0fda  3.50M (0x380000)
handle 874b0eee  3.12M (0x31f000)
disk e5cf4c92
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
disk e5c264fa
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
disk 2747ec1a
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
disk 4748c0e6
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
disk 874b0fda
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
disk 874b0eee
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Il s’agit du détail des partitions de la rom dont voici le détail (enfin ce que j'ai trouvé):
Part01 = XIP
part02 = IMGFS (image de la rom)
part03 = zone de stockage
Les parties les plus importantes sont la 1 et la 2, ce n’est pas grave si vous n’arriver pas à copier la 3.

6 copie des partitions :
Pour extraire chacune des partitions copier/coller une à une les lignes suivantes et faite entrer :
“pdocread -w -d FLASHDR -b 0x800 -p Part00 0 0x31f000 Part00.raw”
“pdocread -w -d FLASHDR -b 0x800 -p Part01 0 0x380000 Part01.raw”
“pdocread -w -d FLASHDR -b 0x800 -p Part02 0 0x4560000 Part02.raw”
“pdocread -w -d FLASHDR -b 0x800 -p Part03 0 0x8660000 Part03.raw”

voici ce que ça donne à l’écran :

```
F:\Documents de D@vid>pdocread -w -d FLASHDR -b 0x800 -p Part00 0 0x31f000 Part0
0.raw
CopyTFFSToFile(0x0, 0x31f000, Part00.raw)

F:\Documents de D@vid>pdocread -w -d FLASHDR -b 0x800 -p Part01 0 0x380000 Part0
1.raw
CopyTFFSToFile(0x0, 0x380000, Part01.raw)

F:\Documents de D@vid>pdocread -w -d FLASHDR -b 0x800 -p Part02 0 0x4560000 Part
02.raw
CopyTFFSToFile(0x0, 0x4560000, Part02.raw)

F:\Documents de D@vid>pdocread -w -d FLASHDR -b 0x800 -p Part03 0 0x8660000 Part
03.raw
CopyTFFSToFile(0x0, 0x8660000, Part03.raw)
```

Le temps de création est plus long pour les parts 2 et 3 donc ne vous inquiétez pas
Chez moi la taille des parts =
Part00 = 3 196 ko
Part01 = 3 584 ko
part02 = 71 040 ko
part03 = 136 448 ko

7 les fichiers de sauvegarde :
Les fichiers sont extraits là où vous avez dézippé itsutilsbin. Mettez les de côté car ce sont ces fichiers qui permettrons de reconstruire votre rom.

2- Reconstruire une Rom

Voici un tuto vous permettant de reconstruire une rom à partir de vos fichiers .raw du dump. Attention le tuto ci dessous permet de reconstruire une sauvegarde de l'OS mais pas de la radio, du SPL et du splash screen.

1 le dump :

Pour reconstruire une ROM, vous devez déjà avoir fait une sauvegarde de votre rom, c'est ce qu'on appelle le dump.

2 Installation de la rom kitchen :

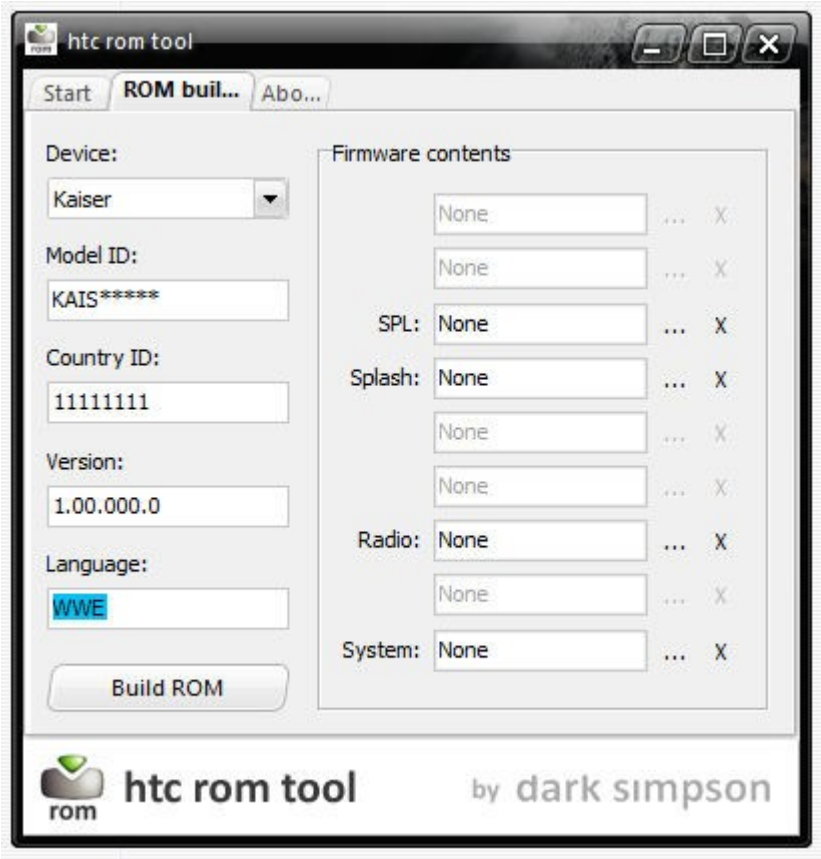
La rom kitchen va vous permettre de « cuisiner » votre propre rom ou de reconstruire une rom à partir de fichier sauvegardé lors du dump
Vous trouverez les différentes versions de la rom kitchen pour téléphone dans le pack ROMs (Pour le tuto nous utilisons la v0.3 beta et je vous invite à lire le fichier readme qui l'accompagne).

3 préparation des fichiers :
3.1 Placez vos fichiers de sauvegarde **part1** et **part 2** dans le dossier « **BaseRom** » de votre kitchen
3.2 placer le fichier **RUU_signed.nbh** de n'importe quelle rom RUU que vous trouverez . Par exemple, prenez la version française qui est ici :
http://www.megaupload.com/?d=7RGEFS5B

4 création de la rom :
4.1 désactivez votre antivirus (sinon vous aurez des conflits avec certains scripts)
4.1 lancez « begin.cmd » choissisez 2 et passez les étapes une à une
Vous allez automatiquement passer les commandes (les fichiers .cmd) de la kitchen de 1 à 7 :
1a.ExtractNBHContent.cmd
1b.ExtractNBHContent.cmd
2a.ExtractDumpIMGFS.cmd
2b.ExtractDumpIMGFS.cmd
3a.ExtractDumpXIP.cmd
3b.ExtractDumpXIP.cmd
4.CopyROMXIP.cmd
5.PKGTool.cmd
6.MoveOEMSYS.cmd
7.DeleteBoot.cmd
Voici une partie de ce qui va défiler :

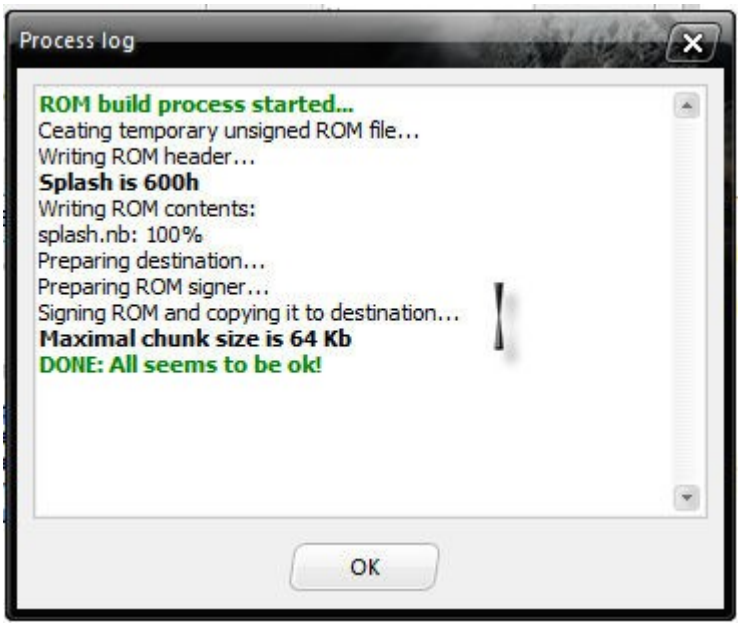
```
802442a0 - 80245000 L00000d60 NUL
80245000 - 80258754 L00013754 o32 region_0 rva=00001000 vsize=00013754 real=03e3
5000 psize=00013754 f=60000020 for FLASHDRV.DLL
80258754 - 80259000 L000008ac NUL
80259000 - 80259720 L00000720 o32 region_2 rva=0001d000 vsize=00000720 real=03e5
1000 psize=00000720 f=40000040 for FLASHDRV.DLL
80259720 - 8025a000 L000008e0 NUL
8025a000 - 8025a170 L00000170 o32 region_4 rva=0001f000 vsize=00000170 real=03e5
3000 psize=00000170 f=40000040 for FLASHDRV.DLL
8025a170 - 8025b000 L00000e90 NUL
8025b000 - 8025d896 L00002896 o32 region_0 rva=00001000 vsize=00002896 real=03e2
e000 psize=00002898 f=60000020 for htcfsfilter.DLL
8025d896 - 8025e000 L0000076a NUL
8025e000 - 8025e2d0 L000002d0 o32 region_2 rva=00005000 vsize=000002d0 real=03e3
2000 psize=000002d0 f=40000040 for htcfsfilter.DLL
8025e2d0 - 8025f000 L00000d30 NUL
8025f000 - 8025f174 L00000174 o32 region_3 rva=00006000 vsize=00000174 real=03e3
3000 psize=00000174 f=40000040 for htcfsfilter.DLL
8025f174 - 80260000 L00000e8c NUL
80260000 - 8026091a L0000091a o32 region_0 rva=00001000 vsize=0000091a real=03e2
9000 psize=0000091c f=60000020 for MMMAP.dll
8026091a - 80261000 L000006e6 NUL
80261000 - 80261048 L00000048 o32 region_2 rva=00003000 vsize=00000048 real=03e2
b000 psize=00000048 f=40000040 for MMMAP.dll
80261048 - 80262000 L00000fb8 NUL
80262000 - 80262168 L00000168 o32 region_3 rva=00004000 vsize=00000168 real=03e2
c000 psize=00000168 f=40000040 for MMMAP.dll
80262168 - 80263000 L00000e98 NUL
80263000 - 80265a97 L00002a97 o32 region_0 rva=00001000 vsize=00002a97 real=03e2
0000 psize=00002a98 f=60000020 for wce_rex.DLL
80265a97 - 80266000 L00000569 NUL
80266000 - 80266210 L00000210 o32 region_2 rva=00006000 vsize=00000210 real=03e2
5000 psize=00000210 f=40000040 for wce_rex.DLL
80266210 - 80267000 L00000df0 NUL
80267000 - 8026716c L0000016c o32 region_4 rva=00008000 vsize=0000016c real=03e2
7000 psize=0000016c f=40000040 for wce_rex.DLL
8026716c - 8026816c L00001000 o32 region_1 rva=0006a000 vsize=00001351 real=01ff
a000 psize=00001000 f=c0000040 for crypt32.dll
8026816c - 8026936c L00001200 o32 region_1 rva=0003a000 vsize=00006f64 real=0004
a000 psize=00001200 f=c8000040 for filesys.exe
8026936c - 802abfd6 L00042c6a filedata wince.nls
802abfd8 - 802dbfd8 L00030000 filedata bmui.nb0
802dbfd8 - 802e5fd8 L0000a000 filedata boot.hv
802e5fd8 - 802ecfd8 L00007000 filedata mxip_lang.vol
802ecfd8 - 802f2bec L00005c14 filedata boot.rgu
802f2bec - 802f6591 L000039a5 filedata sysroots.p7b
802f6594 - 802f7734 L000011a0 filedata 3174b293-abb8-d934-b13c-77f0d46081c2.dsm
802f7734 - 802f7734 L00000000 rom_00 end
802f7734 - 80380000 unknown
3174b293-abb8-d934-b13c-77f0d46081c2.dsm
3346da5d-3675-4a67-925e-75f623184bda.dsm
723fb954-d931-4348-b672-82a188e587b5.dsm
723fb954-d931-4348-b672-82a188e587b5.rgu
81959fbc-573f-2628-ebbf-1a0979b4934f.dsm
bmui.nb0
boot.hv
boot.rgu
d92a4f0a-378a-4482-8fd3-bd127a05e4de.dsm
mxip_lang.vol
sysroots.p7b
wince.nls
       12 fichier(s) copié(s).
Appuyez sur une touche pour continuer...
```

4.2 une fois la fenêtre fermée lancez **8.BuildOS.cmd** qui va créer le fichier **os-new.nb** qui est votre nouvelle rom au format nb.
4.3 lancez **9.CreateROMTéléphone.bat**
4.4 lancez **HTC rom tool** et dans la ligne <u>système</u> allez chercher le fichier **OS-new.NB** que vous venez de créer



4.3 lancer la création (**built rom**) en lui donnant le nom **RUU_signed.nbh**

NB : l'outil HTC rom tool sert aussi bien à modifier l'os, le spl, le splash que la radio… à vous de choisir



5 création du pack d'installation :

5.1 dans un même dossier coller le fichier **RUU_signed.nbh** précédemment créé et le ficher **TéléphoneCustomRUU.exe** qui se trouve dans tools et qui est le lanceur du fichier RUU.

5.2 zipper le dossier et donnez-lui un nom parlant que vous ne confondrez pas avec

une autre rom

Bravo vous avez réussi à créer une sauvegarde et un pack d'installation de votre rom

3- Découpage d'une ROM

Ce tuto permet d'extraire les différents éléments (OS, SPL, radio) d'une ROM (officielle ou non), afin de créer un pack d'installation d'un ou plusieurs éléments en particulier provenant de cette ROM. Cela permet de mixer les éléments de différentes ROM (l'OS d'une ROM, le SPL d'une autre par exemple…) Cette méthode ne fonctionne pas uniquement qu'avec le téléphone.

1 Pré-requis :
Avoir une ROM complète :
- ROM WWE = dossier contenant (RUU_signed.nbh + TéléphoneCustomRUU.exe)
- ROM officielle = renommer le .exe en .rar pour obtenir le fichier RUU-signed.nbh

2 Outils :
téléchargez NBHextract.exe que vous trouverez ici : http://forum.xda-developers.com/showthread.php?t=289830

3 créer un nouveau répertoire vide et mettez y :
- NBHextract.exe
- Le fichier RUU_signed.nbh de votre ROM

4 Extraction :
4.1 Allez sous DOS (executer/cmd)
4.2 allez dans le répertoire où vous avez placé vos 2 fichiers précédents

4.3 Tapez la commande nbhextract.exe RUU_signed.nbh
Voici à quoi ca doit ressembler :

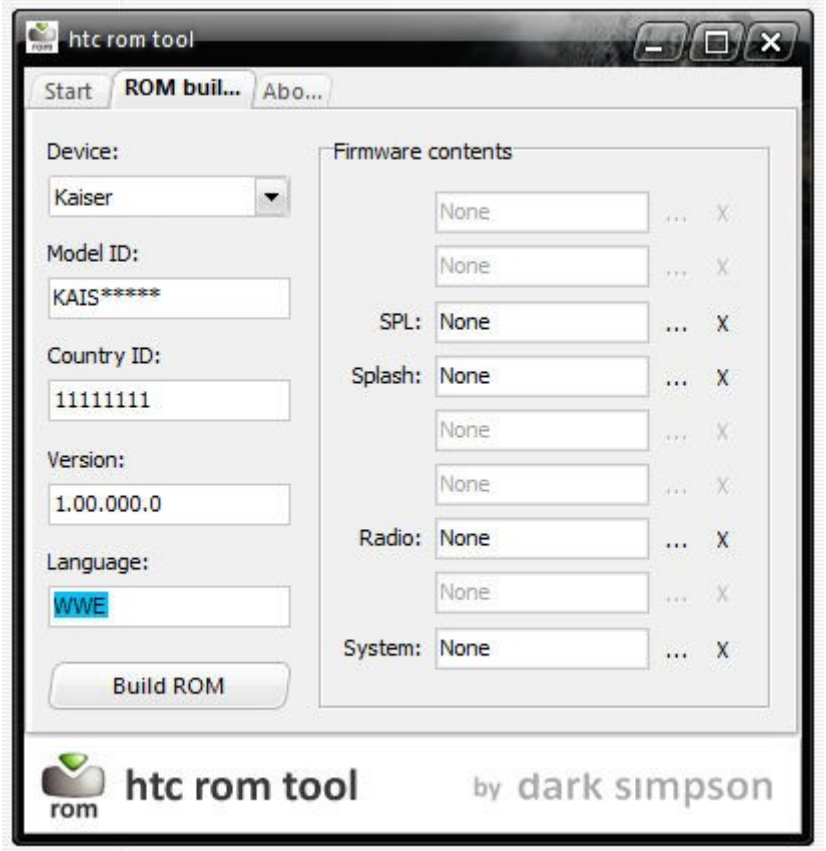
```
F:\Documents de D@vid\test SPL>nbhextract.exe RUU_signed.nbh
=== NBHextract v1.0
=== Extract contents from HTC NBH files
=== (c)2007 xda-developers.com
=== by: pof & TheBlasphemer based on itsme perl scripts

Device:   KAIS*****
CID:      11111111
Version:  1.00.000.0
Language: WWE
Extracting: 00_OS.nb

F:\Documents de D@vid\test SPL>
```

4.3 Vos fichiers ont été extraits dans votre dossier avec les 2 autres fichiers et ils se nomment :
00_Unknown.nb
01_SPL.nb
02_MainSplash.nb
02_MainSplash.bmp

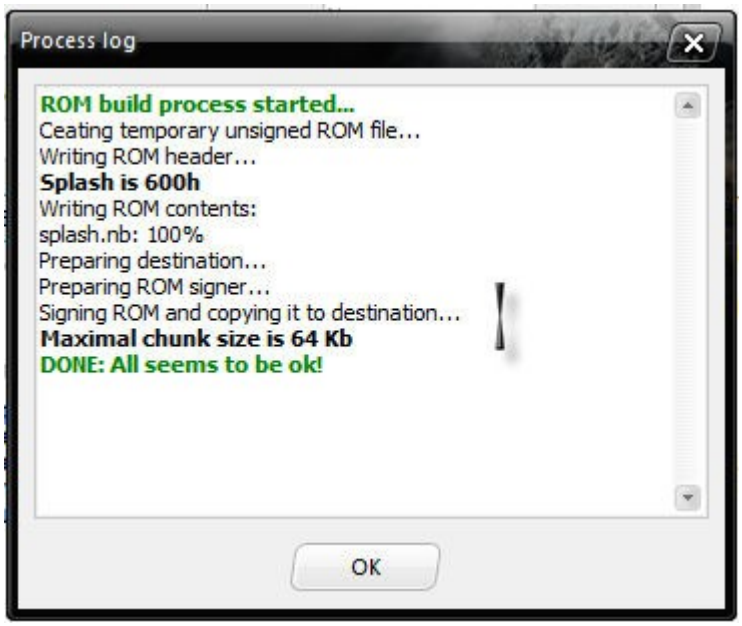
03_OS.nb

NB : A noter que pour le moment je n'ai pas trouvé une ROM custom Téléphone contenant autre chose que l'OS… cette liste de fichier a été extraite par Thuffir sur une ROM officielle HTC (en .exe)

5 Reconstruction d'un kit de flashage avec 1 ou plusieurs éléments (OS, SPL ou autre) :
Exemple avec le SPL :
5.1 lancez HTC rom tool et dans la ligne SPL allez chercher le fichier SPL.NB que vous venez d'extraire



5.2 lancer la création (built rom) en lui donnant le nom RUU_signed.nbh



6 Création du pack d'installation :
6.1 dans un même dossier coller le fichier RUU_signed.nbh précédemment créé et le ficher TéléphoneCustomRUU.exe qui se trouve dans tools et qui est le lanceur du fichier RUU.
6.2 zipper le dossier et donnez-lui un nom parlant que vous ne confondrez pas avec une autre rom

Bravo vous avez réussi à créer un pack d'installation avec uniquement un élément provenant d'une ROM custom (méthode identique avec les autres fichiers

voir 2 fichiers simultanément).

4-Construire une ROM custom

Voici les grandes lignes de la construction d'une ROM custom.

A) Préparation

1 Installation de la rom kitchen :

La rom kitchen va vous permettre de « cuisiner » votre propre rom ou de reconstruire une rom à partir de fichier sauvegardé lors du dump

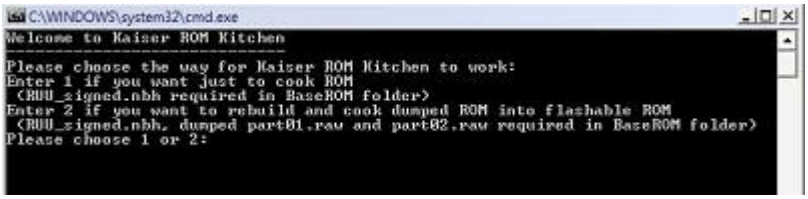
Elle est disponible dans le pack ROMs.

2 préparations des fichiers :

Dans le dossier « **BASE ROM** » placer le **fichier RUU_signed.nbh** de la ROM que vous souhaitez utiliser comme base. Vous pouvez prendre la version française HTC qui est ici : http://www.megaupload.com/?d=7RGEFS5B

3 Décomposition de votre ROM RUU :

3.1 désactivez votre antivirus (sinon vous aurez des conflits avec certains scripts)
3.2 lancez « **begin.cmd** » choissisez 1 et passez les étapes une à une en lisant les instructions à l'écran



3.3 Une fois le découpage terminé vous allez trouver dans votre kitchen les dossiers :
- Temp (contient les fichiers temporaires pour vos travaux)
- SYS (contient les logs du constructeur ici HTC)
- OEM (contient les logs des opérateurs téléphonique, si vous avez pris une rom HTC officielle ce dossier sera vide)
- ROM (contient l'OS de base)

<u>B) Customisation de la ROM</u>

Pour customiser une rom, vous avez 3 grandes possibilités :
- l'ajout de cab qui s'installerons au 1er démarrage du téléphone et qui seront désinstallables par la suite (autant prendre une rom officielle de base et installer les cabs 1 par 1 selon votre envie, ca évite de flasher),
- l'intégration pure et simple du log dans la rom (le log fera partie intégrante de la rom, c'est plus propre comme dans la rom de Thuffir),
- la modification de registre pour modifier les paramètres du système, du hardware ou des soft

4 Pour ajouter un cab dans une ROM :

4.1 Il faut placer les cabs directement dans OEM\OperatorPKG_PT
4.2 Ajouter la liste des cabs dans un fichier « **config_PT.txt** » du genre « CAB: \Windows\WiFicountrycode.CAB »

5 Pour intégrer un log directement dans la rom :

5.1 Créer un répertoire dans OEM avec le nom du log à installer (évitez les caractères spéciaux du genre les accents)
5.2 Copier le contenu du cab du log désiré dans ce dossier (utilisez un extracteur de

cab)
5.3 Créer le fichier **.dsm** (à l'aide du bloc note) en lui donnant un nom codé trouvé sur ce site (http://www.famkruithof.net/uuid/uuidgen) (sélectionner 4 : random).

The following version 1 UUID / GUID is generated for your use:

286636a8-9ec0-11dc-8314-0800200c9a66

This UUID is generated according to RFC 4122, using the timestap / nodeid version (version 1), where the nodeid comes from network equipment I own. (Like a UUID generated using the `uuidgen -t` command.)

Create multiple UUIDs at once: 1 (at most 500 at once)
Generate an UUID / GUID of another type: Version 1: Time/Node based
Get

This type of UUID is generated using the current time, a clock id which changes in case the current time is found to be older than the latest known time a UUID is generated and an IEE 802 hardware address which should be unique.Still the following disclaimer applies:
Disclaimer:
The provided UUID (GUID) is provided AS IS without warranty of any kind, not even the warranty that the generated UUID is actually unique. The entire risk of using this UUID is upto you. If you cannot agree to those terms do not use the generated UUID.
Please do not use UUID from a cached paged.

More information about UUIDs.

Extract the time from a version 1 UUID.

Contact information on the homepage of this host.
An agent adding logging to your java programs at runtime
The uptime of this host.

5.4 Créer le fichier **.rgu** (à l'aide du bloc note) en lui donnant le même nom codé et y insérer les lignes de registre nécessaires au programme que vous aurez extrait du cab (attention le fichier doit être en unicode)

```
REGEDIT4


[HKEY_CLASSES_ROOT\.ZIP]
@="ZIPArchive"

[HKEY_CLASSES_ROOT\ZIPArchive]
@="ZIP Archive"

[HKEY_CLASSES_ROOT\ZIPArchive\Shell\Open\Command]
@="\"%InstallDir%\\cecmd.exe\" \"%1\""

[HKEY_CLASSES_ROOT\ZIPArchive\DefaultIcon]
@="%InstallDir%\\cecmd.exe,-102"

[HKEY_CLASSES_ROOT\.TCFOLDER]
@="tcfolder"

[HKEY_CLASSES_ROOT\tcfolder]
@="Total Commander Folder"

[HKEY_CLASSES_ROOT\tcfolder\DefaultIcon]
@="%InstallDir%\\cecmd.exe,-105"

[HKEY_CURRENT_USER\Software\Ghisler\CECmd\Configuration]
"LANGUAGE"="%InstallDir%\\Français.lng"

|
```

5.5 Créer un fichier **initflashfiles.txt** dans lequel vous mettrez les chemins ou seront

installé les différents fichiers de votre application. (Exemple :
Directory("\Windows\\Menu Démarrer\Programmes\"):-
File("Totalcmd.lnk","\Windows\Totalcmd.lnk")

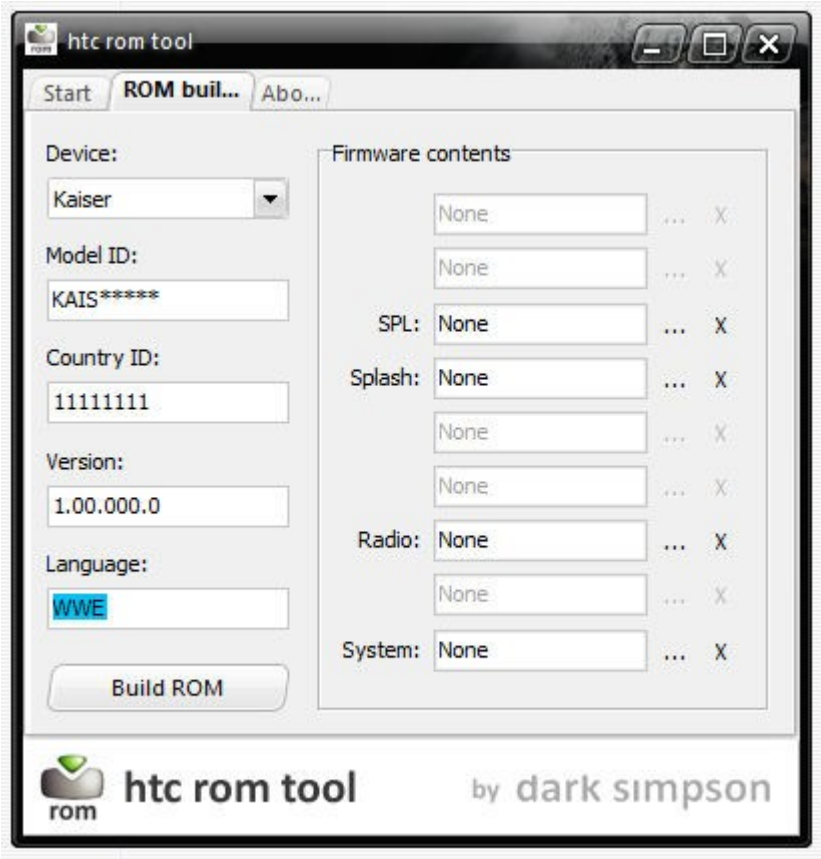
NB : vous trouverez des packs OEM prêt à être copié/collé ici :
http://www.megaupload.com/es/?d=8QVXWZQF

6 Pour modifier le registre :

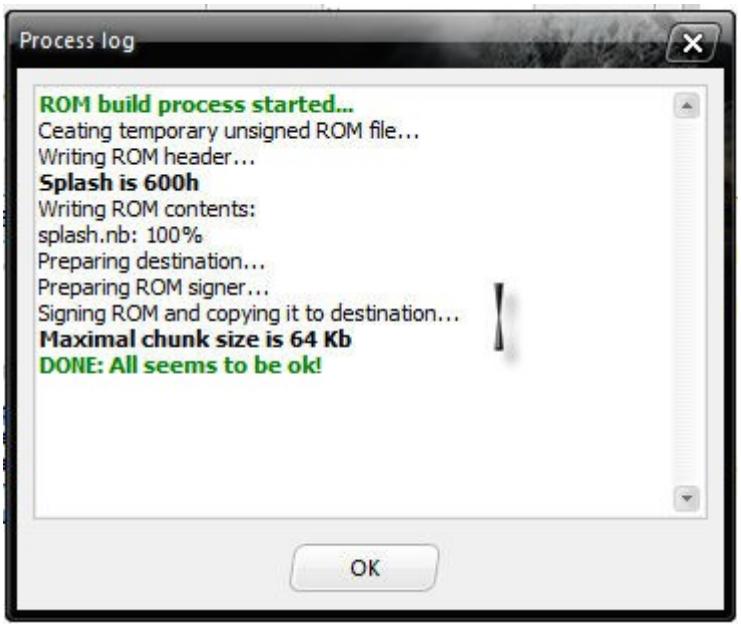
Toutes les lignes de registres se trouvent dans les packs OEM dans les fichiers **.Rgu**. Il vous suffit de modifier directement les valeurs dans ces fichiers ou bien de créer de nouvelles lignes de registre. Attention de ne pas oublier de laisser 2 lignes blanches à la fin du fichier.

7 Assemblage de votre ROM :

7.1 Lancer **8.BuildOS.cmd** qui va créer le fichier **os-new.nb** qui est votre nouvelle rom au format nb.
7.2 lancer **9.CreateROMTéléphone.bat**
7.3 lancez **HTC rom tool** et dans la ligne système allez chercher le fichier **OS-new.NB** que vous venez de créer



7.4 lancer la création (built rom) en lui donnant le nom **RUU_signed.nbh**



NB : l'outil HTC rom tool sert aussi bien à modifier l'os, le spl, le splash que la radio… à vous de choisir

8 Création du pack d'installation :

8.1 dans un même dossier coller le fichier **RUU_signed.nbh** précédemment créé et le ficher **TéléphoneCustomRUU.exe** qui se trouve dans tools et qui est le lanceur du fichier RUU.

8.2 zipper le dossier et donnez-lui un nom parlant que vous ne confondrez pas avec une autre rom

Bravo vous avez réussi à créer votre ROM custom !

Rappel : avant l'installation d'une ROM custom vous devez impérativement flasher le hard SPL grâce à l'utilitaire fourni dans le pack ROMs.