Replicant - Issue #2024

Issue # 2025 (New): Enable to recreate the EFS partition completely from scratch

Find offset and encoding of IMEI in the EFS for libsamsung-ipc

04/20/2020 10:22 PM - Denis 'GNUtoo' Carikli

Status:	New	**Start date:**	04/21/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Telephony and mobile data	**Estimated time:**	0.00 hour
Target version:	Any version	**Spent time:**	0.00 hour
Resolution:		**Grant:**	
Device:	Galaxy Nexus (I9250), Galaxy Note (N7000), Galaxy Note 2 (N7100), Galaxy Note 8.0 (N51xx), Galaxy S (I9000), Galaxy S 2 (I9100), Galaxy S 3 (I9300), Galaxy Tab 2 10.1 (P51xx), Galaxy Tab 2 7.0 (P31xx), Nexus S (I902x)		

Description

History

#1 - 04/20/2020 10:27 PM - Denis 'GNUtoo' Carikli

Libsamsung-ipc already has a tool to compute the checksum of the EFS nv_data.bin files, so we can change their content.

The idea would be to write a tool to restore the EFS.

As the EFS is usually printed under the battery, users would lookup the EFS there and would give that to the tool.

Some XDA threads have probably the information for various devices.

It would be interesting to have information for any of the devices that are or could be supported by libsamsung-ipc, so if anyone has links to that it would be nice to post it here.

#2 - 04/20/2020 10:31 PM - Denis 'GNUtoo' Carikli

- Parent task set to #1869

This would be useful to be able to reconstruct EFS from scratch.

#3 - 04/20/2020 10:34 PM - Denis 'GNUtoo' Carikli

- Parent task changed from #1869 to #2025

#4 - 04/20/2020 10:34 PM - Denis 'GNUtoo' Carikli

- Device Galaxy Nexus (I9250), Galaxy Note (N7000), Galaxy Note 2 (N7100), Galaxy Note 8.0 (N51xx), Galaxy S (I9000), Galaxy S 2 (I9100), Galaxy S 3 (I9300), Galaxy Tab 2 10.1 (P51xx), Galaxy Tab 2 7.0 (P31xx) added

#5 - 07/08/2020 12:41 PM - Denis 'GNUtoo' Carikli

We now have a tool from Paulk for the XMM616:

- https://git.replicant.us/contrib/GNUtoo/hardware_replicant_libsamsung-ipc/log/?h=patches-todo/modem-tools
- https://git.replicant.us/contrib/GNUtoo/hardware_replicant_libsamsung-ipc/tree/tools/rfs-imei.c?h=patches-todo/modem-tools

However the only device with an XMM616 I have is the Galaxy S, and it's EFS is completely gone. Because of that I wasn't able to manage to verify that the original tool or my modifications are supposed to work.

Also once the nv_data.bin has been rebuilt from LineageOS, I still wasn't able to change the IMEI:

- Some fields weren't set, I could clearly see things like 'REV__' and 'Not Active'
- The IMEI is 004999010640000 which is the default IMEI
- The IMEI field was reset to 0xFFFFFFFF in the first RFS messages right after restarting the Replicant RIL
- After changing the IMEI, I also tried changing 'Not Active' and many other fields, adjusted the checksum, and here again the IMEI fields was

overwritten with 0xFFFFFFFF.
- I tried setting the IMEI to 004999010640000 with the tool, and here again the field was changed to 0xFFFFFFFF again, probably even after trying to change some fields like 'Not Active' too.

edit1: add more background.