Reached milestones and ongoing development on Replicant

Replicant

Paul Kocialkowski
paulk@replicant.us

Sunday February 1st, 2015

Replicant

"Replicant is a fully free Android distribution running on several devices, a free software mobile operating system putting the emphasis on freedom and privacy/security"

- Pragmatic way for **software freedom** on **mobile devices**
- Started in mid-2010: **Openmoko FreeRunner** and **HTC Dream**
- **Fully free** version of Android
- **Ethical** project that **respects** users
- Functional and **usable** daily
- **Privacy** enhancements (…)

Replicant development

Technical grounds:

- **AOSP** base at first
- **CyanogenMod** for more devices

Implications of a fully free system:

- **Remove** or **replace** proprietary parts:
  executables, libraries, firmwares
- Get rid of **malicious features**
  tracking, statistics, etc

Additional work:

- **Adapt** the system for the lack of proprietary components:
  graphics acceleration, firmwares loading
- "**Branding**", look and feel
- Maintenance, **security** updates

Replacing non-free software

Have as many features available as possible!

Reverse engineering:

- Long list of **proprietary** parts:
  graphics, audio, camera, sensors, RIL, hardware video decoding, etc
- **Documentation** is seldom available:
  [Chip maker] is not in a position to provide details of the formula we addressed with [OEM] phone team.
- **Reverse engineering**:
  logs, tracing, strings, decompiling, kernel driver, maths, frustration
- **Understanding** what's going on
- Writing **free software replacements**

Hard tasks that Repicant doesn't deal with:

- Graphics acceleration, firmwares, modem system

Replacing non-free software

Free software replacements written for Replicant:

- **RIL**: Samsung-RIL, libsamsung-ipc: **30000** lines, **9** devices
- **Camera**: **5500-10000** lines, **2** devices
- **Audio**: **4500** lines, **3** devices
- **Sensors**: **3000-4000** lines, **8** devices

Cooperation with other **communities**:

- **SHR/FSO** for libsamsung-ipc
- **CyanogenMod/Teamhacksung** for camera, audio
- Integration of work from Replicant (e.g. CyanogenMod)
- Technical advantages

Replicant advancement timeline

December 2010	January 2011	April 2011	Summer 2011
Replicant 2.2			
HTC Dream	Nexus One	SDK	libsamsung-ipc

November 2011	January 2012	April 2012	September 2012
Replicant 2.3			
Nexus S (I902x)	Samsung-RIL	Galaxy S (I9000)	GTA04

November 2012	January 2013	April 2013	July 2013
Replicant 4.0			
Galaxy Nexus (I9025) Galaxy S 2 (I9100)	SDK	Galaxy Tab 2 10.1 (P51xx) Galaxy Tab 2 7.0 (P31xx)	Galaxy S 3 (I9300)

October 2013	January 2014	June 2014
Replicant 4.0	Replicant 4.2	
Galaxy Note (N7000)	Galaxy Note 2 (N7100), SDK	GTA04

Challenges in new devices

Samsung devices:

- RIL: **Samsung-RIL**, **libsamsung-ipc**, device-specific transport

Nexus S (I902x) , Galaxy S (I9000):

- Camera: preview, EGL
- Sensors: accelerometers, magnetic field sensors

Galaxy S 2 (I9100), Galaxy Note (N7000):

- Audio: Yamahell, **Yamaha-MC1N2-Audio**, **TinyALSA-Audio**
- Camera: **Exynos Camera**

Galaxy S 3 (I9300), Galaxy Note 2 (N7100):

- Camera: **Exynos Camera** rewrite, S5C73M3 interleaved format
- Sensors

Replicant status

Current status of Replicant:

- Lead by **one** developer, on **spare** time
- Very few **external** contributions
- Latest version: **Replicant 4.2**
- Supports up to **12** different devices
  mostly Samsung Galaxy and Nexus devices
- Funded thanks to **donations**

Taking a step back

Taking a step back

Bad modem isolation

⚠

Taking a step back

Proprietary and signed bootloaders

What do we do now?

Possible directions for Replicant:

Idea #1:

- Catch up with **mainstream** Android devices
- **Latest** Android versions
- Free system, **proprietary bootloaders**
- Avoid known bad **modem isolation**

Idea #2:

- Focus on better devices that **allow** free bootloaders
- Good or allegedly good **modem isolation**
- Take freedom to the **next step**!

Why not make a fully free system out of [**Tizen|Firefox OS|**...]?

Openmoko Neo FreeRunner (GTA02)

First “historical" example of a good device:

Back in 2008, the Openmoko Neo Freerunner (GTA02):

- Free **PCB design**
- **Isolated** modem
- No loaded proprietary **firmwares**
- Free **bootloader**
- Fully free GNU/Linux **systems**

Currently:

- Old device (400Mhz CPU, 128Mb RAM)
- **Openmoko** retired
- **Community** retired
- A few **systems** are still alive

Goldelico GTA04

In 2011-2012, **Golden Delicious** started the **GTA04**:

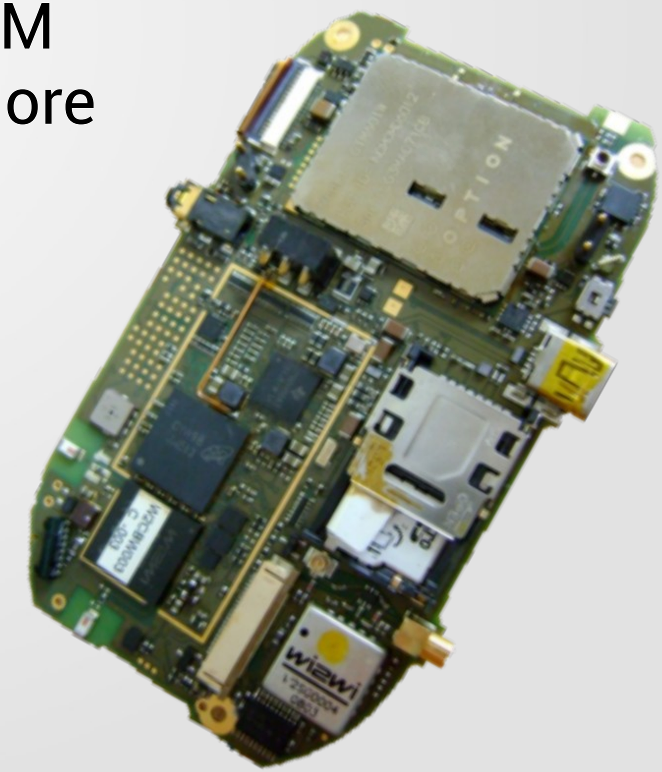
- **Motherboard replacement** for the Openmoko FreeRunner (GTA02)
- Complete units, other form factors (**Letux**)

Reasonably efficient hardware:

- OMAP3 (**DM3730**), 800Mhz-1Ghz, 512Mib RAM
- Modem, GPS, sensors, Wi-Fi, bluetooth and more

Goldelico GTA04:

- Free **bootloader**
- Supposedly good **modem isolation**
- Friendly **manufacturer**
- Ships with **Debian**
- Documented **PCB design**
- Documented chips **protocols**



Goldelico GTA04

Early Replicant support:

- Started in **mid-2012** (Replicant 2.3)
- **Broken** kernel, no suspend/resume, missing Android features
- Most hardware features **missing**
- Not **usable**

GTA04 and **Android** kernels don't mix:

- Merge GTA04 support on **Android kernels**
  "Lost IRQs", missing features, broken PM
- Merge Android support on **GTA04 kernels**
  merge issues, runtime issues

Frustration: no Replicant on the GTA04 for a year or so

Goldelico GTA04

A new hope:

- **Linux 3.12** kernel from **Goldelico**, with reasonable support
  ***Android** features merged but still **PM** issues*
- **Replicant 4.2** support from Goldelico
- Cooperation on the **kernel**, different **userspaces**
- **Features**: GPS, audio, lights, vibrator, *Wi-Fi*

Goldelico Replicant 4.2:

- **Single partition** approach, multi-boot
- Other **form factors**
- WIP **Hayes-RIL**, **Sensors**
- Non-free **Wi-Fi firmware**

Upstream Replicant 4.2:

- **Android partitions** scheme
- CWM **recovery**
- **Encryption**

OpenPhoenux and the future

OpenPhoenux community:

- Dedicated to **free software**
- Aims to respect **privacy**

Syndicates such projects:

- **GTA04** and derivatives
- **Neo900**

Plans for the future on Replicant:

- Features support:
  Hayes-RIL, sensors, bluetooth, etc
- Fully operational kernel
- Multi-devices support, single image

More information:

- http://www.openphoenux.org/
- http://www.gta04.org/
- http://www.neo900.org/

Pre-order your GTA04A5 or Neo900!

LG Optimus Black (P970)

“A hacker's journey: freeing a phone from the ground up"

- Mainstream device by **LG**, released in 2011
- **OMAP 3630** platform
- Technical documentation leaked online
  EN_LG-P970_SVC_ENG_110415.pdf
- **U-Boot** and **X-Loader** source code released by LG
- **OMAP GP** (General Purpose) device!

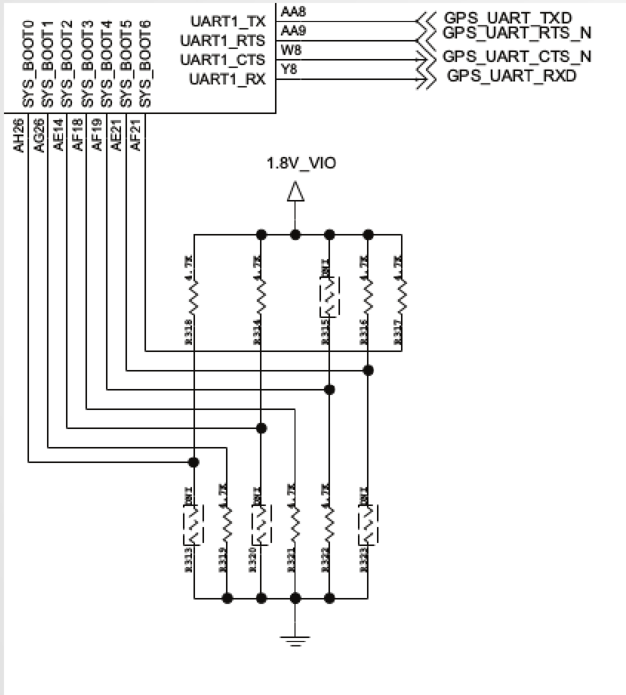
```
$ devmem 0x480022f0 16
0x0325
```

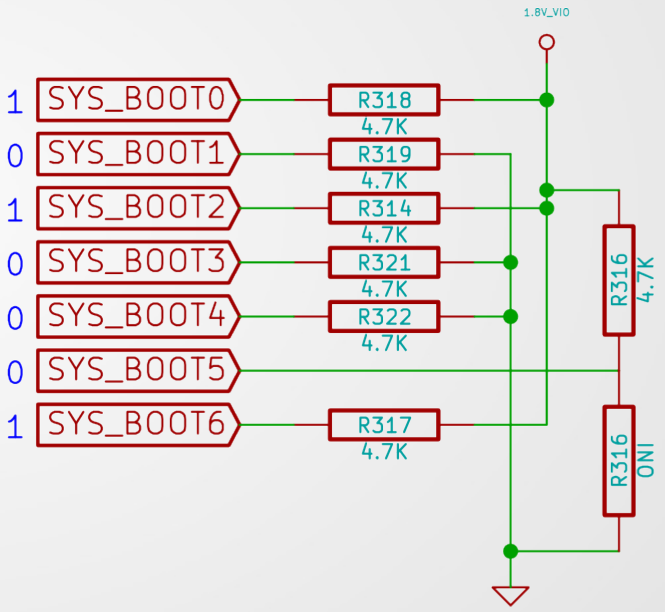
- No **signature** checks
- Free **bootloaders** possible!

LG Optimus Black (P970): Boot

Running code on the device:

- SYS_BOOT5=0 (boot priority: MMC2 > USB)
- One resistor away…





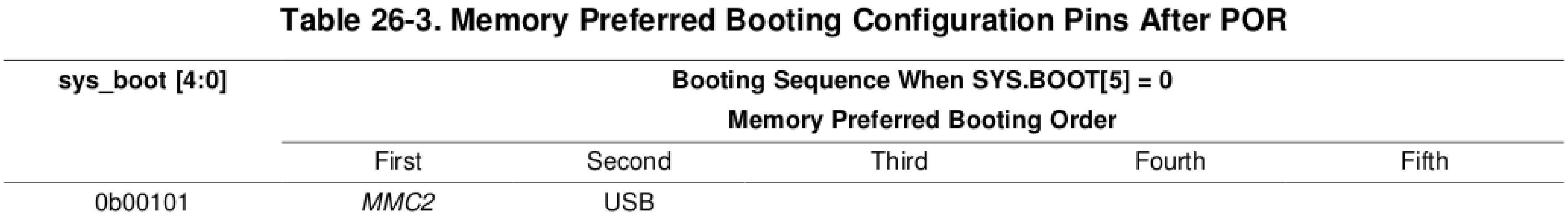


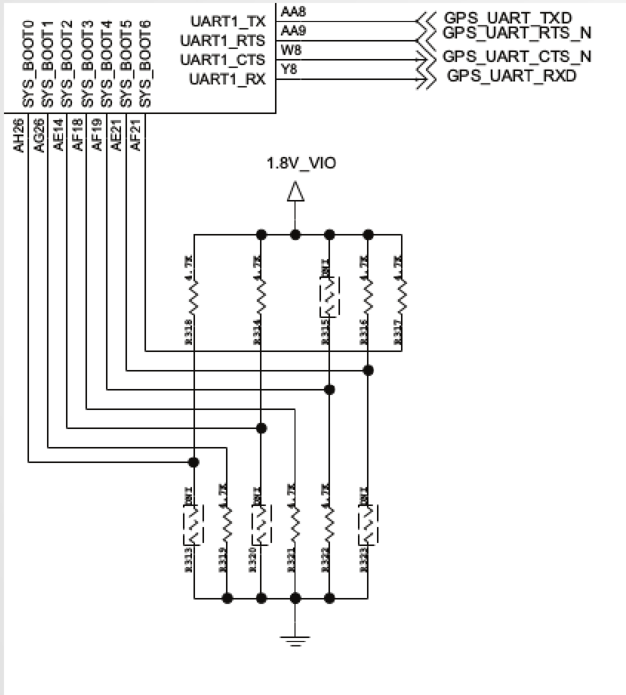
Table 26-3. Memory Preferred Booting Configuration Pins After POR

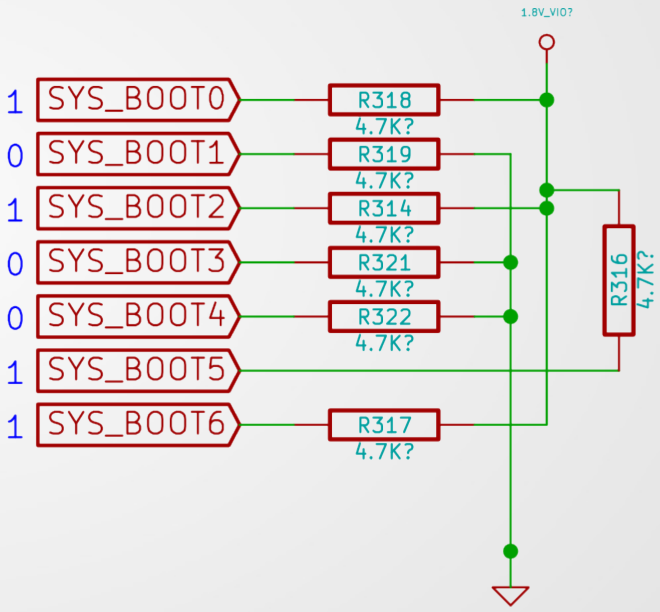
sys_boot [4:0]	Booting Sequence When SYS.BOOT[5] = 0				
	Memory Preferred Booting Order				
	First	Second	Third	Fourth	Fifth
0b00101	*MMC2*	USB			

LG Optimus Black (P970): Boot

Running code on the device:

- SYS_BOOT5=1 (boot priority: USB > MMC2)
- Let's remove R323!





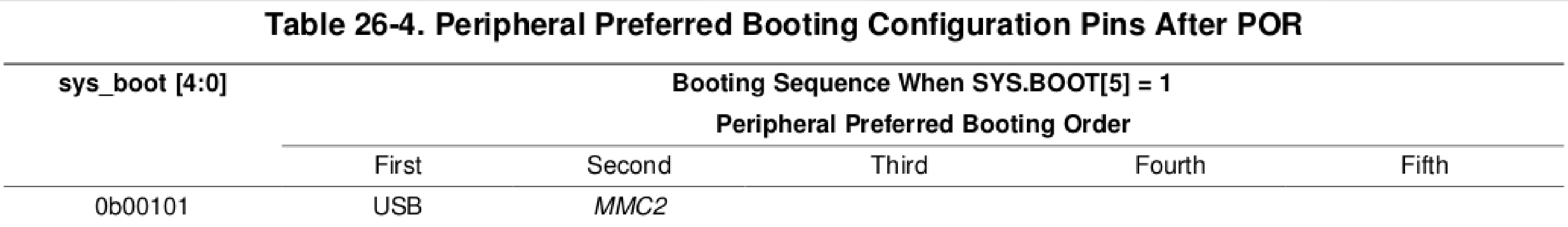
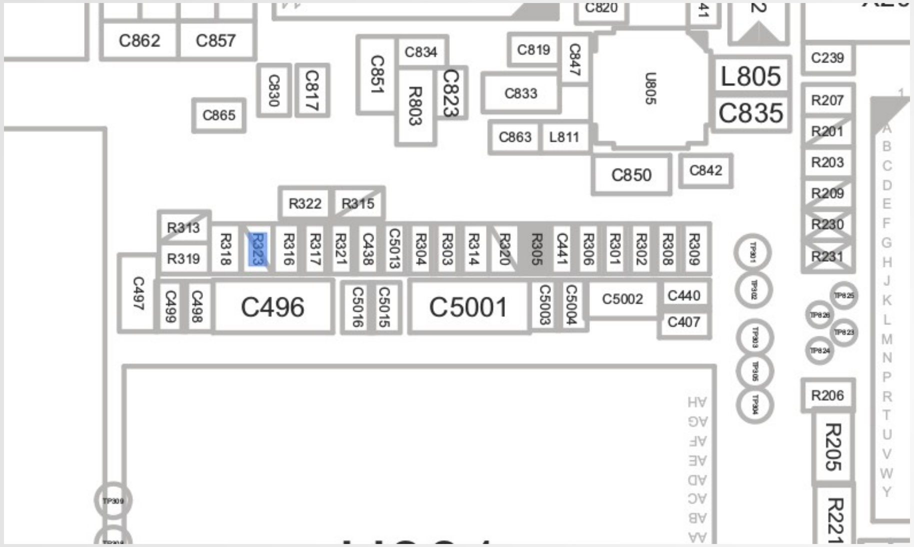


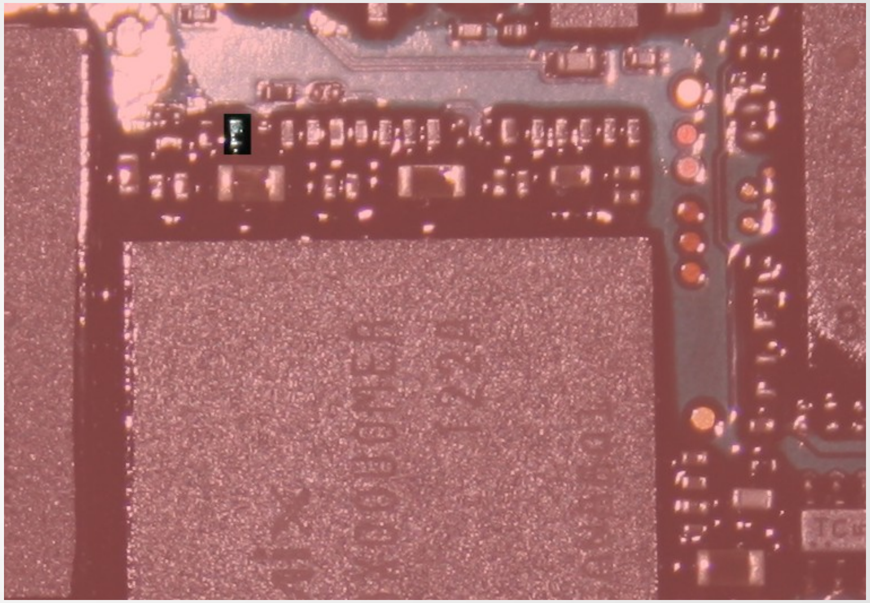
Table 26-4. Peripheral Preferred Booting Configuration Pins After POR

sys_boot [4:0]	Booting Sequence When SYS.BOOT[5] = 1 Peripheral Preferred Booting Order				
	First	Second	Third	Fourth	Fifth
0b00101	USB	*MMC2*			

LG Optimus Black (P970): USB boot

Tiny tiny resistor...





Plug USB in and... tada (bootrom show up)!

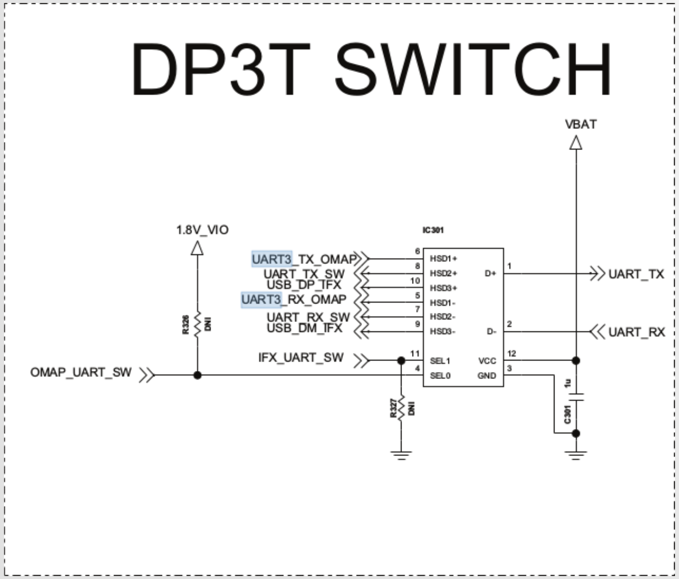
```
usb 3-1: new high-speed USB device number 15 using xhci_hcd
usb 3-1: unable to get BOS descriptor
usb 3-1: New USB device found, idVendor=0451, idProduct=d00e
usb 3-1: New USB device strings: Mfr=33, Product=37, SerialNumber=0
usb 3-1: Product: OMAP3630
usb 3-1: Manufacturer: Texas Instruments
```

LG Optimus Black (P970): UART

Now what?

- Code loading works with omap-u-boot-utils' pusb
- But we're blind!

Time to get some serial output (UART3):



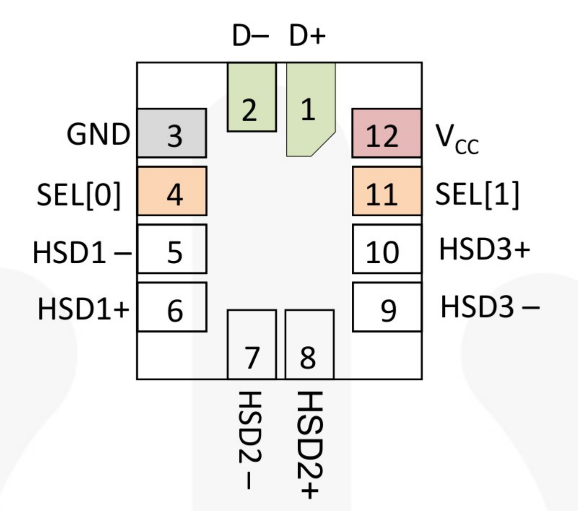
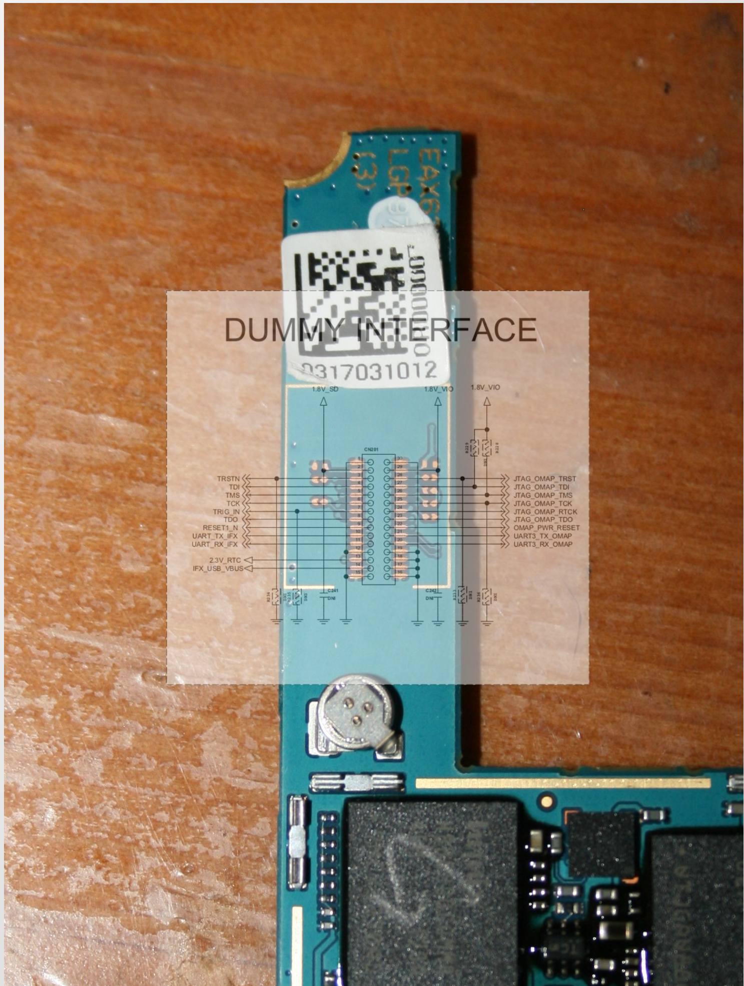


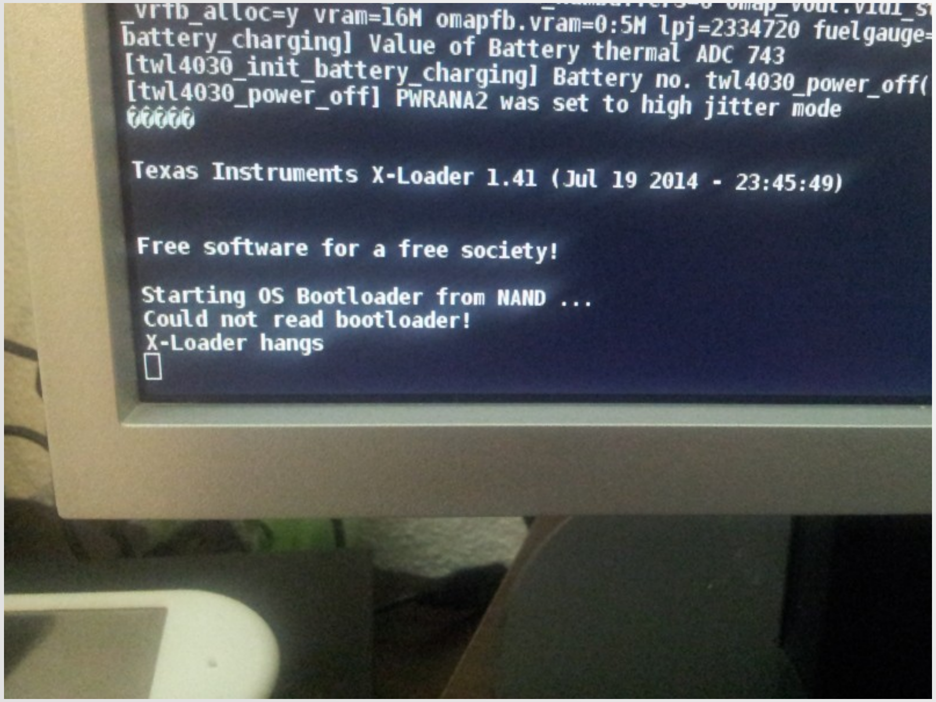
Figure 2. Pin Assignments (Top Through View)



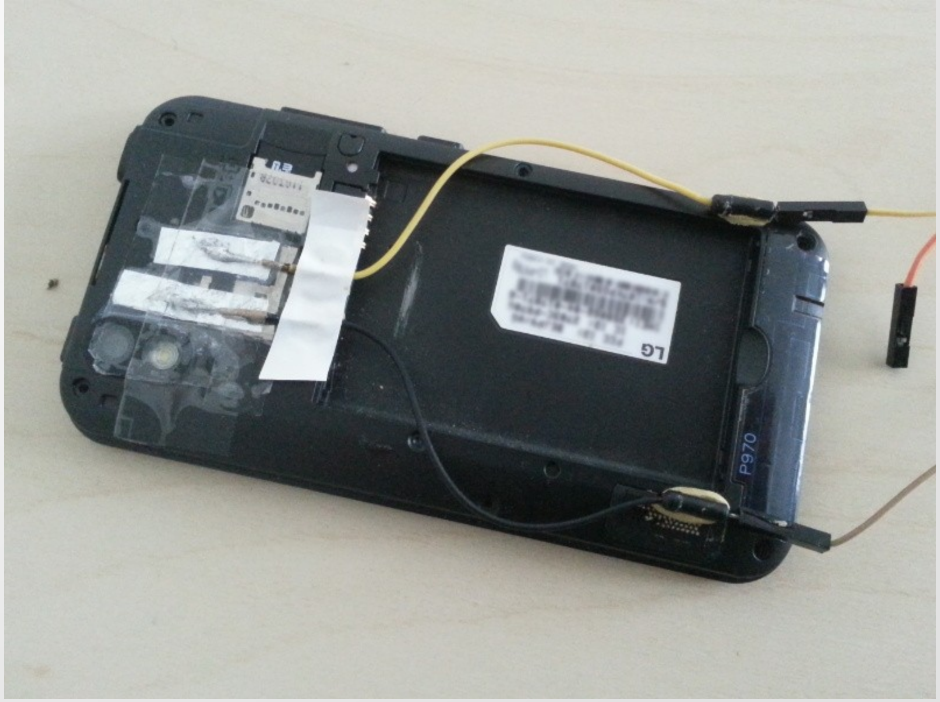
LG Optimus Black (P970): UART

Now what?

- Code loading works with omap-u-boot-utils' pusb
- Seeing the light!



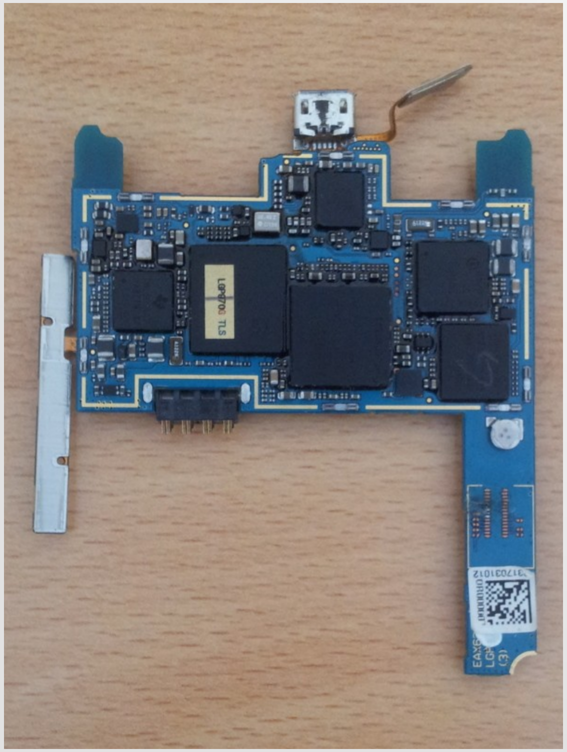
```
_vrfb_alloc=y vram=16M omapfb.vram=0:5M lpj=2334720 fuelgauge=
battery_charging] Value of Battery thermal ADC 743
[twl4030_init_battery_charging] Battery no. twl4030_power_off(
[twl4030_power_off] PWRANA2 was set to high jitter mode
�����

Texas Instruments X-Loader 1.41 (Jul 19 2014 - 23:45:49)


Free software for a free society!

Starting OS Bootloader from NAND ...
Could not read bootloader!
X-Loader hangs
```

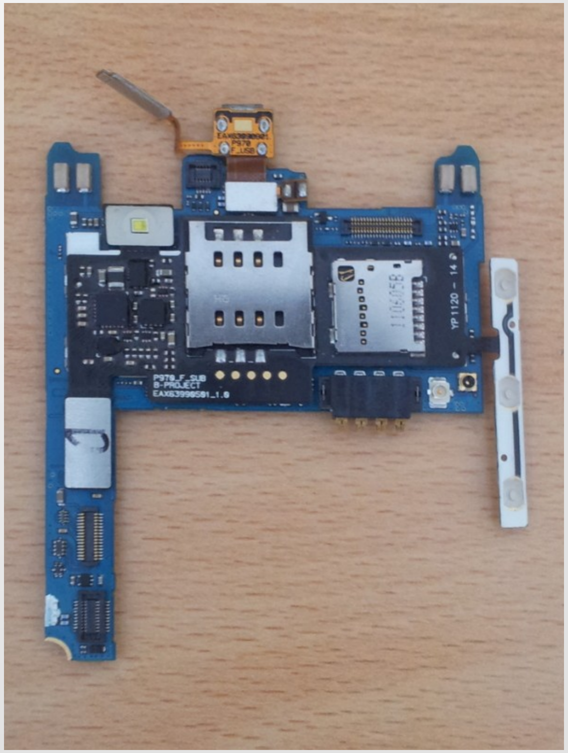


LG Optimus Black (P970): Bootloaders

Starting the actual work:

- Released version of LG's **X-Loader**
- *Upstream* **X-Loader**
- U-Boot from external sdcard (MMC1)
- I2C3 problem:





LG Optimus Black (P970): U-Boot

Adding proper support:

- **Upstream** U-Boot
- U-Boot **SPL** instead of **X-Loader**
- **Reference** (legacy) code from LG

Current status:

- A few independent **patches** accepted
- Personal tree with **WIP code**
  git://git.code.paulk.fr/u-boot-sniper.git
- **Basic** support, **muxing**, external **sdcard** (MMC1)
- **USB** support (**fastboot**)
- Booting **CWM recovery** (with issues)

LG Optimus Black (P970): Future

U-Boot planned features:

- **LCD video** support
- **Keys** detection (run-time **boot selection**)
- **USB** connector **UART**
- Proper **kernel** boot
- **Upstream** support

Plans for the future:

- **Replicant** support
  Hayes-RIL, sensors, ...
- Replicant wiki **documentation**
- **Upstream** kernel support

Missing features with free software: GPS, DSP, Wi-Fi/bluetooth

Allwinner (sunxi) tablets

Allwinner (sunxi) platforms:

- Linux-sunxi community: http://www.linux-sunxi.org/
- Free **bootloaders** (upstream **U-Boot**, **U-Boot SPL**)
- **Fully-featured** legacy kernel (**sunxi-3.4**)
- Cheap **Chinese** tablets (often Wi-Fi-only)

Replicant support (planned):

- **Build** system
- Support for various **devices** and **platforms** (sun4i, sun5i, sun7i)
- **Single image** for all platforms and devices
  sunxid, sunxi.prop, sunxi modules, Hayes-RIL device, configuration
- **Installation** script, **CWM recovery**

Allwinner (sunxi) tablets

Initial support for a handful of devices:

- Support depends on **kernel drivers** and **userspace modules**
- Linux-sunxi **documentation**
- **Kernel drivers**, script.fex
- **Userspaces modules**, sunxi.prop

Add support for your **own** device!

```
CWM-based Recovery v6.0.3.6
Warning: No file_contexts
```

Other areas of (future) work

Other interesting devices:

- Amazon Kindle Fire (first generation): OMAP 4430 GP
- More to discover!

Replicant wiki:

- Samsung Galaxy Back-door
- Devices evaluation
- Privacy/security on devices, modem isolation
- Signed/proprietary bootloaders
- List of OMAP GP/HS devices, boot order
- Technical information (UART)

Replicant

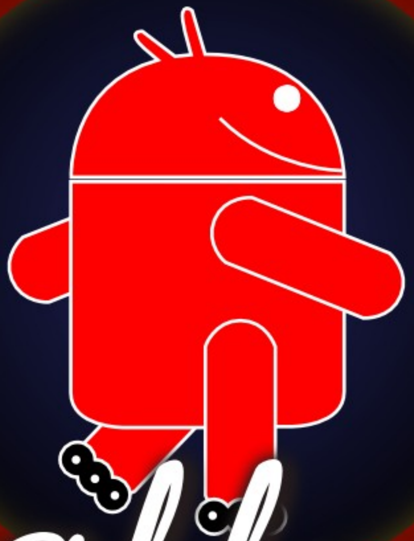
Learn more about Replicant:

- Website: http://www.replicant.us/
- Blog: http://blog.replicant.us/
- Wiki/tracker: http://redmine.replicant.us/

Join the community:

- Forums
- Mailing list
- IRC channel: #replicant at freenode
- Get in touch and get involved!

Say hi (and verify our GPG release key)!



That's all Folks!