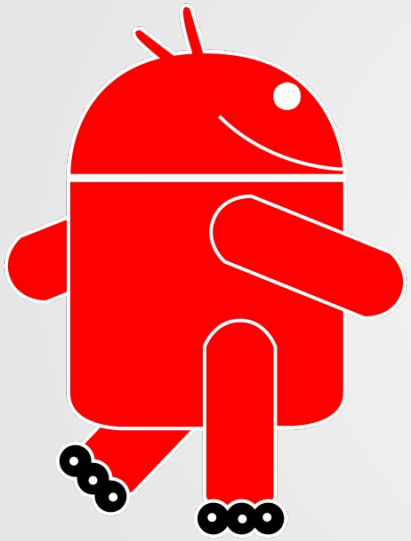
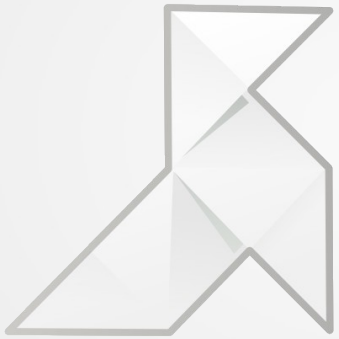
Liberating mobile devices from the ground up



Replicant



Embedded Freedom

Paul Kocialkowski
paulk@replicant.us

Wednesday July 8th, 2015

16es Rencontres Mondiales du Logiciel Libre
du 4 au 10 juillet 2015

RMLL
BEAUVAIS 2015
Destination libre

Supported devices

Supported devices

Bad modem isolation

Supported devices

Proprietary and signed bootloaders

Current situation

Overview of the current situation:

- ✗ No free hardware
- ✗ Non-free firmwares in integrated circuits
- ✗ Non-free modem systems
- ✗ Proprietary bootroms
- ✔ Modem isolation (hard to figure out reliably)
- ✔ Free and unsigned bootloaders
- ✔ Mostly-free systems
- ✔ Free applications

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

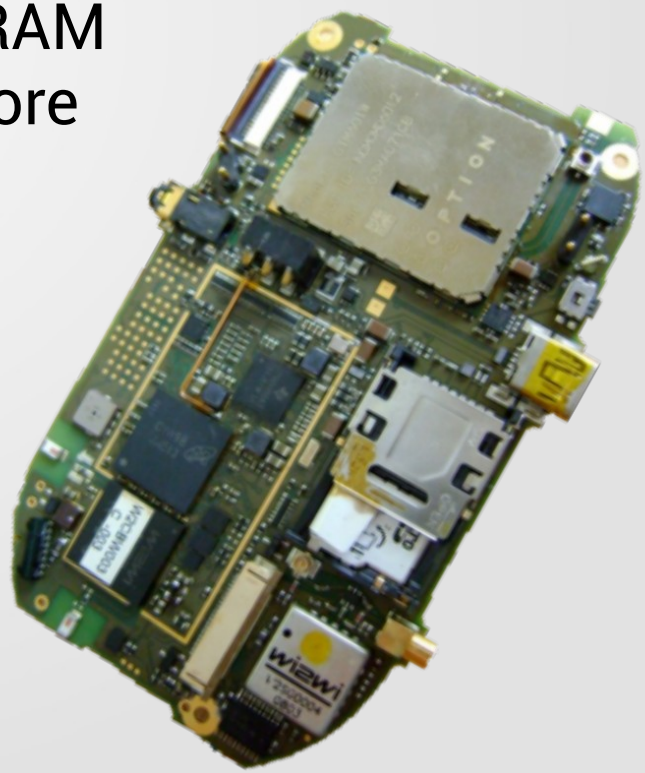
Goldelico GTA04

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**), 800 MHz-1 GHz, 512 MiB 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**

Goldelico GTA04

Work for the **future**, missing **features** :

- Proper **PM** to last at least a full day
- **Hayes-RIL** rewrite
- Telephony **audio** routing integration
- **Sensors** integration
- **Bluetooth** support (bluedroid)
- **Multi-device** support (single image)

Long term goals:

- Somewhat accelerated **graphics**
- **Video** decoding

Bottlenecks:

- **GPU** graphics acceleration, 3D
- **DSP** video decoding
- **Wi-Fi** firmware

OpenPhoenux community

OpenPhoenux community:
- Dedicated to **free software**
- Aims to respect **privacy**

Syndicates such projects:
- **GTA04** and derivatives
- **Neo900**

Join the community!
http://www.openphoenux.org/

openphoenux

N900

Nokia **N900** (2009):

- **OMAP3** SoC, 256 MiB RAM
- **Debian**-based Maemo system
- Various **non-free** software, fimwares
- **Non-free** and **signed** first-stage **bootloader**

Nowadays:

- **Community** around Maemo still **alive**
- Need for more powerful hardware
- Software **compatibility** (non-free…)
- N900 widely spread

In the meantime:

- Nokia **N9**, **N950**

Neo900

The **Neo900** project was born!

- Motherboard **replacement**
- **Openmoko** veteran **Joerg** as EE and community
- Early prototyping by **Golden Delicious** (2013)
- Fundraising, prototyping, sourcing

Hardware similar to the GTA04:

- OMAP3 (**DM3730**), 1 GHz, 1 GiB RAM
- Modem (LTE), GPS, sensors, Wi-Fi, bluetooth, NFC and more

Privacy-related aspects:

- **Sensors** for **suspicious** power use
- Switches for **reliably** turning off
- Modem **isolation** (apart GPS)

Neo900

Software aspects:

- **Free** and **non-signed bootloaders** (OMAP GP)
- Very similar to the **GTA04**
- Same bottlenecks

Replicant support:

- **GTA04** multi-device support
- Minor diff
- No device yet

> *"Neo900 will support all operating systems available for GTA04 (QtMoko, SHR, Debian, Replicant, ...) and should serve as a great platform for porting systems like Maemo, Ubuntu or Firefox OS - or even for writing your own one!"*

OpenPhoenux

GTA04

- Pre-order now!
- http://www.gta04.org/

openphoenux

Neo900

- Pre-order now!
- http://www.neo900.org

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!

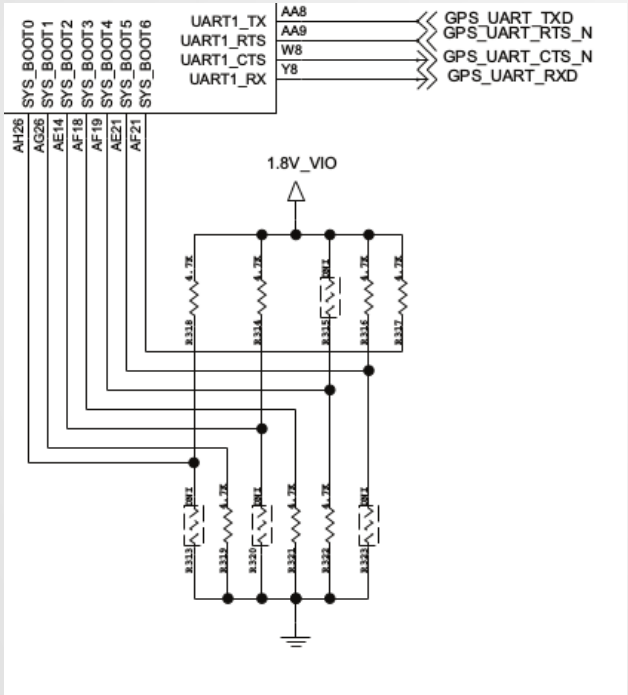
```
$ devmem 0x480022f0 16
0x0325
```

- 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…



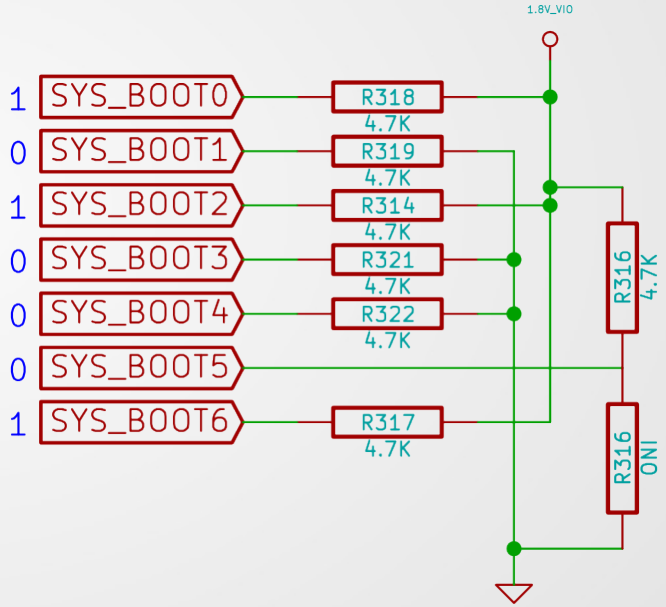


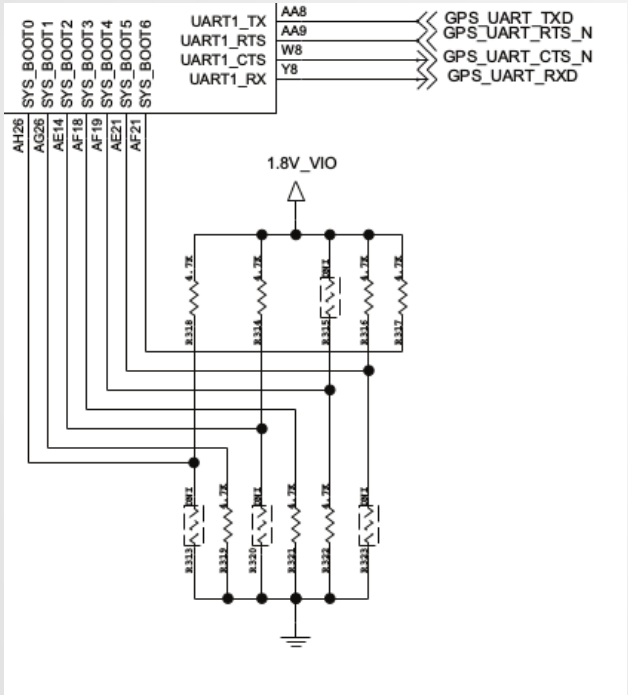
Table 26-3. Memory Preferred Booting Configuration Pins After POR

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!



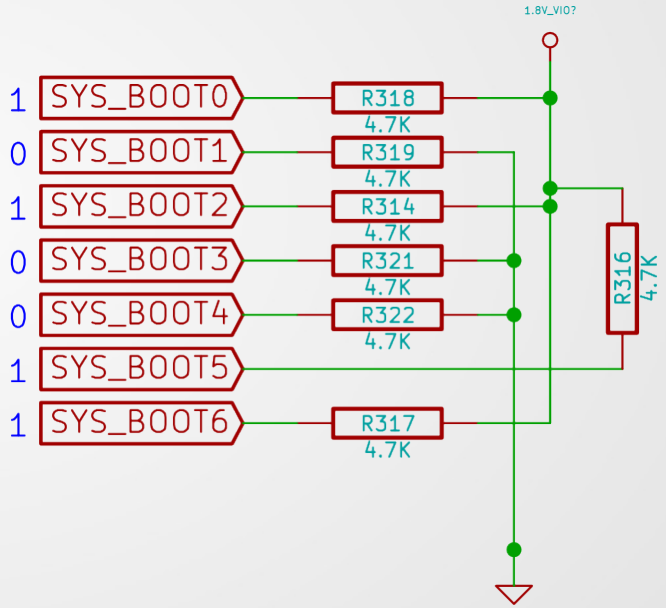
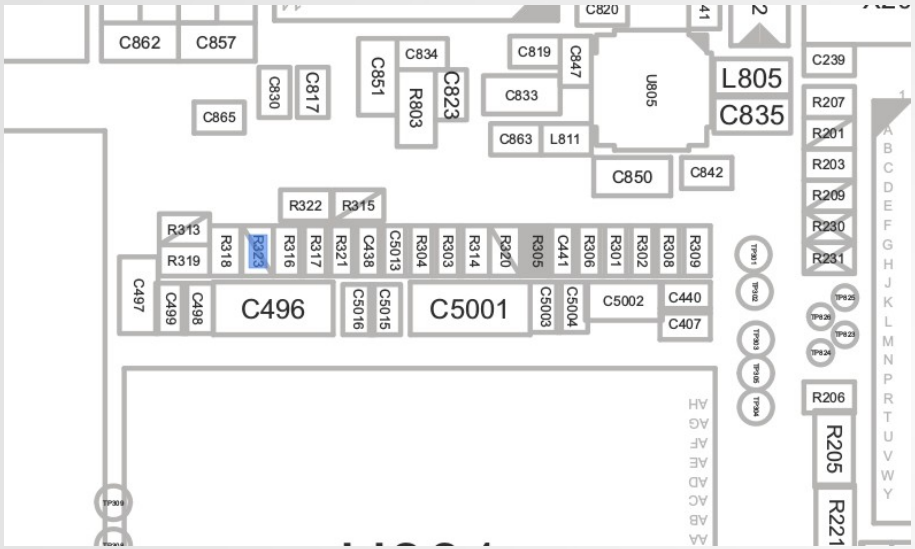


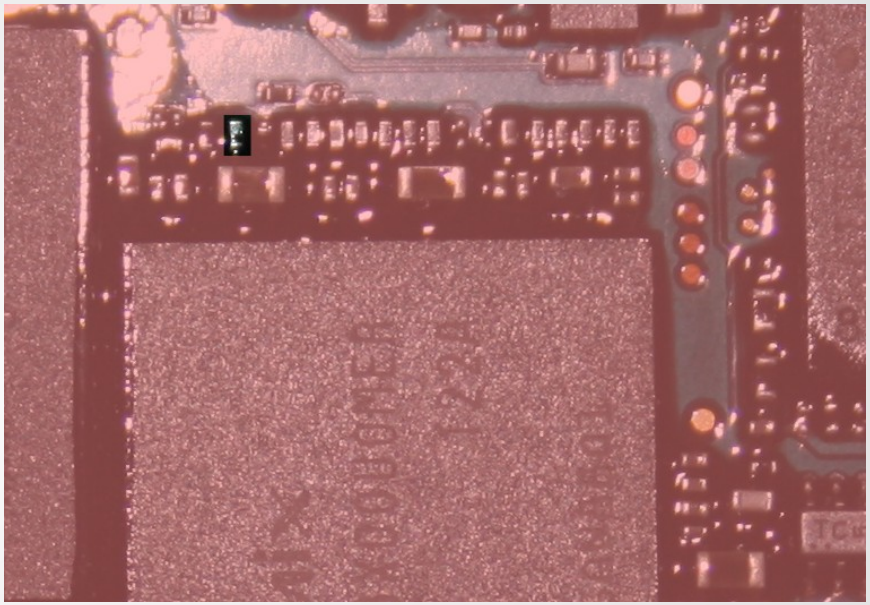
Table 26-4. Peripheral Preferred Booting Configuration Pins After POR

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)!

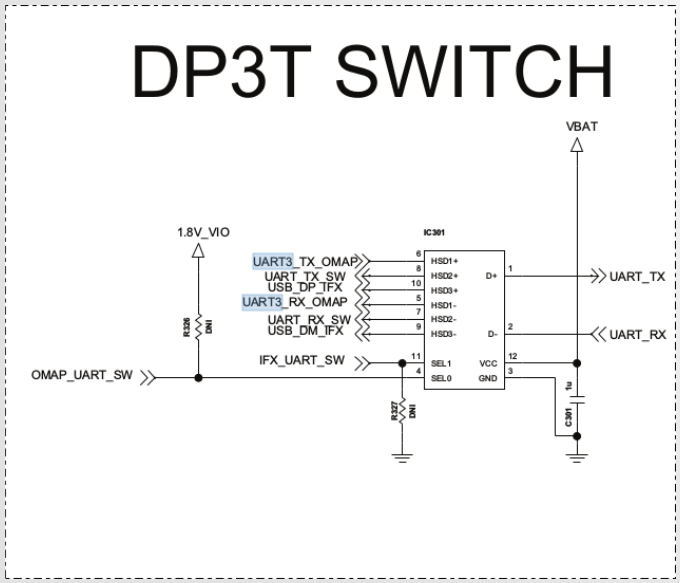
```
usb 3-1: new high-speed USB device number 15 using xhci_hcd
usb 3-1: unable to get BOS descriptor
usb 3-1: New USB device found, idVendor=0451, idProduct=d00e
usb 3-1: New USB device strings: Mfr=33, Product=37, SerialNumber=0
usb 3-1: Product: OMAP3630
usb 3-1: Manufacturer: Texas Instruments
```

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):



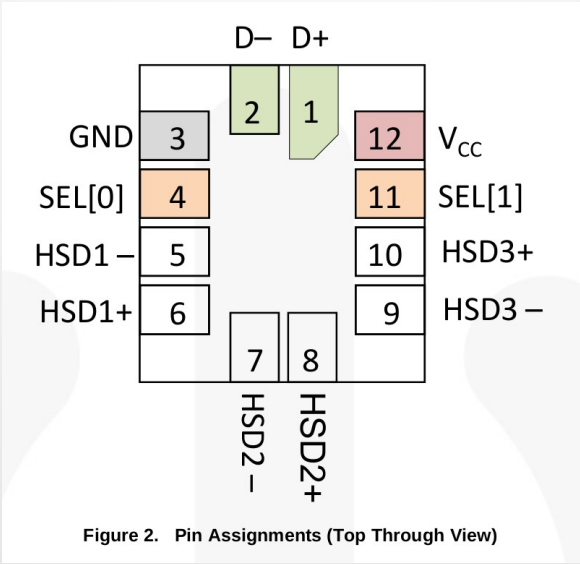
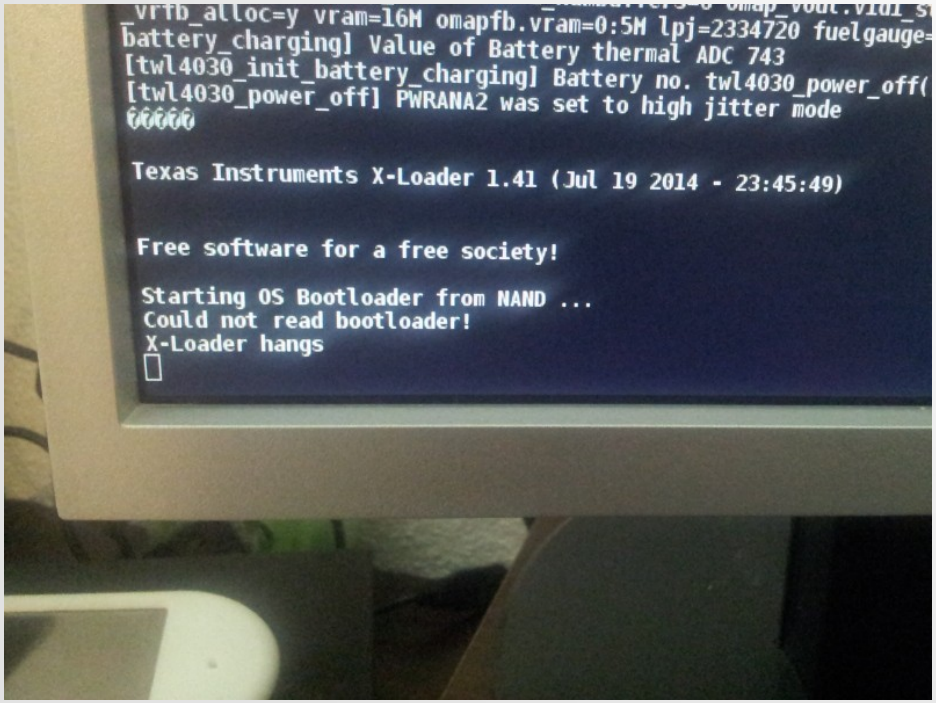


Figure 2. Pin Assignments (Top Through View)

LG Optimus Black (P970): UART

Now what?

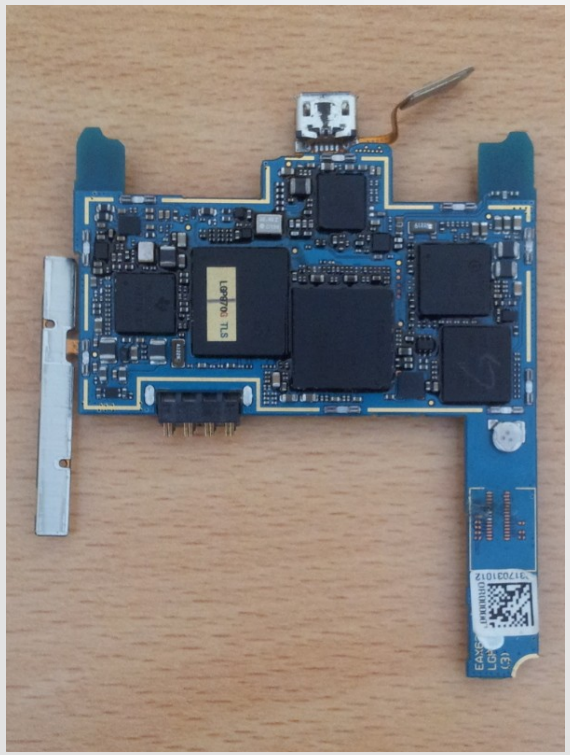
- Code loading works with omap-u-boot-utils' pusb
- Seeing the light!

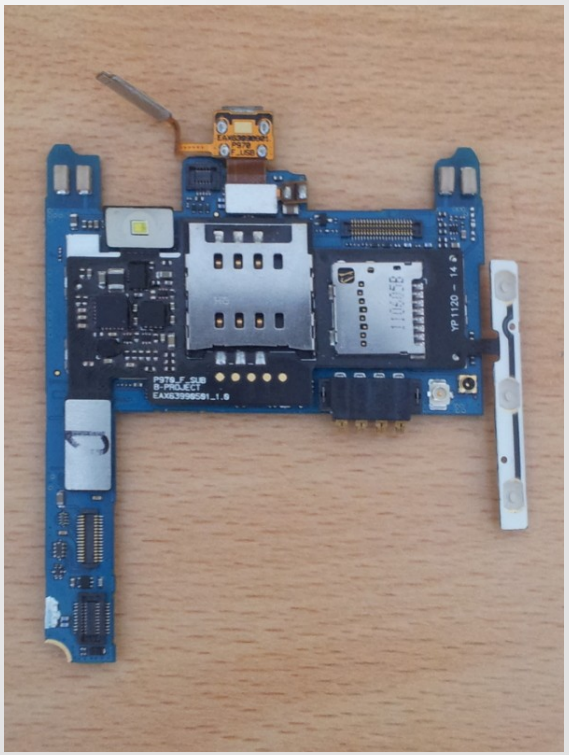


LG Optimus Black (P970): Bootloaders

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:
- Various **patches** for the OMAP3 accepted upstream
- **Aging** code base and **new** U-Boot **APIs**
- About **fully-featured** dirty code:
  git://git.code.paulk.fr/u-boot.git
- Booting **CWM recovery**, **CyanogenMod**
- Cool features (fastboot, sdcard booting)

Upstreaming:
- Sane minimalistic base, nearly ready for initial submission

LG Optimus Black (P970): Future

Replicant support:
- will be started soon!
- **Hayes-RIL**, **sensors**

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

Documentation about the device:
- Replicant **wiki**
- **Resistor** removal
- **UART** (soldering and connector)
- **U-Boot** installation
- **Modem** isolation

Modem isolation looks **good** (dedicated RAM/storage)!

Allwinner (sunxi) tablets

Allwinner (sunxi) **platforms**:

- Linux-sunxi community:
  http://www.linux-sunxi.org/
- Cheap **Chinese** tablets (often Wi-Fi-only)

Allwinner **free software** support:

- Leaked and released SDKs
- Old kernels & U-Boot
- boot0 (& boot1) bootloaders

Allwinner and the free software **community**:
https://github.com/allwinner-zh

- Some documentation (incomplete)
- Kernel for recent platforms (sun8i*)
- U-Boot and boot0 source code
- Many license violations!

Allwinner (sunxi) tablets

Linux-sunxi community free software support:

- Linux-sunxi 3.4 kernel
- ***fully-featured*** *for sun4i/sun5i, mostly for sun7i*
- Free **accelerated video** decoding
- Free **accelerated 2D graphics** (G2D)
- Limare support (Mali GPU)

Upstream effort:

- **Upstream** Linux (missing features, more platforms)
  Free electrons and C.H.I.P.
- **Upstream** U-Boot, U-Boot SPL
  fully-featured, and more!

Allwinner (sunxi) tablets

Replicant support (planned):

- Upstream **U-Boot**
- **Linux-sunxi** kernel and **SDK** kernel
- **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**

Replicant

Allwinner (sunxi) tablets

Initial support for a handful of devices:

- A10: iNet 3F (ZaTab), iNet 3W
- A13: Ampe A76, TZX-Q8-713B7
- A20: Ainol AW1, Yones Toptech BD1078, A20-OlinuXino-LIME2, Cubieboard2

Adding support for a new device:

- **U-Boot** support (DRAM init)
- Kernel **drivers** (SDK, etc)
- **script.fex**
- Userspace **modules**, sunxi.prop

Add support for your **own** device!

More work for the future :

Other interesting devices:
- Amazon Kindle Fire (first generation): OMAP4 GP
- Acer generation 10 tablets: OMAP4 GP
- More to discover!

More interesting **platforms**:
- Nvidia Tegra non-ODM (Tegra K1, X1)
- Freescale i.MX (i.MX6)

More platforms to **evaluate**:
- Rockchip

Replicant wiki:
- List of OMAP GP/HS devices, boot order
  Motorola phones, Moto 360

Replicant

Learn more about Replicant:

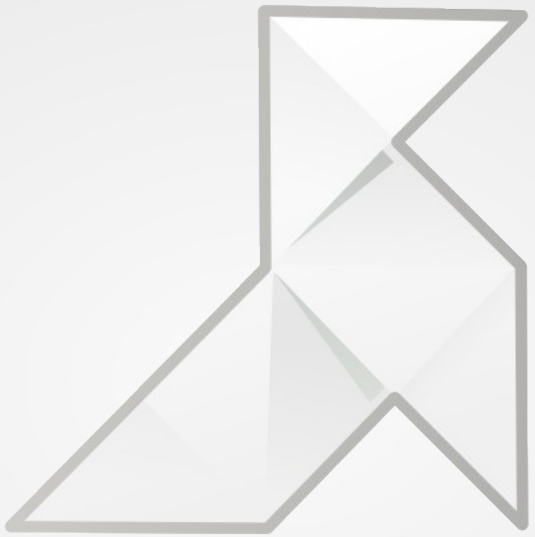
- Website: http://www.replicant.us/
- Blog: http://blog.replicant.us/
- Wiki/tracker: http://redmine.replicant.us/

Join the community:

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

The project needs you!

- Replicant deserves more than one developer
- Donations are welcome (devices are expensive)



Embedded
Freedom


That's all Folks!

Text, images:

- © 2013-2015 Paul Kocialkowski
  Creative Commons BY-SA 3.0 license

Other images:

- **Replicant robot**, © Mirella Vedovetto, Paul Kocialkowski,
  Creative Commons BY-SA 3.0 licence
- **Cocotte en papier**, © Coyau,
  Creative Commons BY-SA 3.0 licence
- **Openmoko Neo FreeRunner**, © FIC/OpenMoko,
  Creative Commons BY-SA 3.0 licence
- **OpenPhoenux logo**, © Philip Horger
  Creative Commons BY-SA 3.0 license
- **GTA04 board,** © Golden Delicious
  Creative Commons BY-SA 3.0 license
- **LG Optimus Black schematics,** © LG Electronics