Free Mobile

...when Android is not enough.

Sebastian Krzyszkowiak
dos

http://dosowisko.net/

P.I.W.O. X
Poznań, 17.05.2014

http://neo900.org/piwo/

Agenda

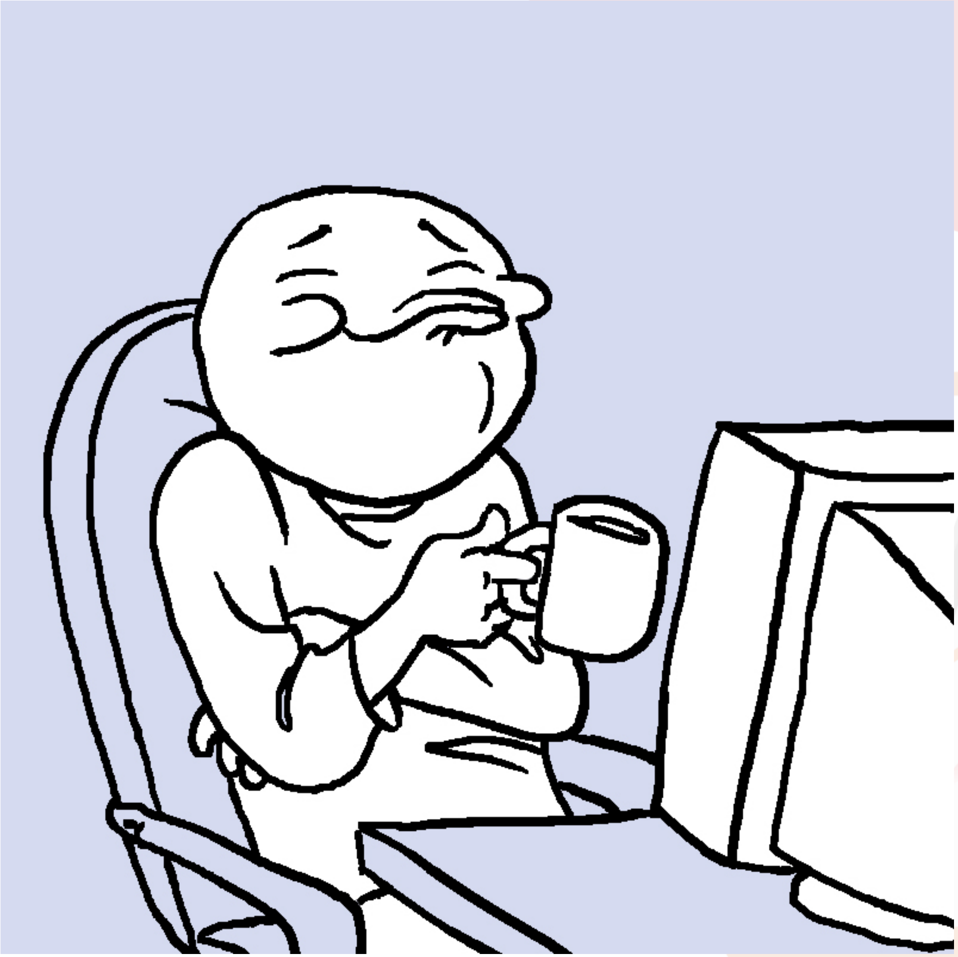
- Hardware
  - The history of Openmoko
  - Raise of the *Phoenux*
  - Neo900
- Privacy and GSM (and what **Neo900** can offer there)
- Software
  - *Community-based* mobile operating systems
  - freesmartphone.org middleware
  - Demo + live coding!

When Android is not enough?

- Completely custom userspace
- Long term support? You'd wish.
- Sure, it's open... **but**
  - Is your Android device open as well?
  - Can you influence its development?
  - Can you use it with FLOSS only?
    - There is Replicant. But... is it compatible with your phone?
  - Can you **replace it**? No, I don't mean „modding”.

Alternatives?

- iOS



Alternatives?

- Windows Phone

Alternatives?

- Firefox OS
- Ubuntu Touch
- Tizen
- Sailfish OS

Not really.

- Repeating Android mistakes with undocumented, closed and locked-down hardware
- Limited paradigms
- Customer friendly
  - Yes, sometimes it can be a flaw.
- **Not completely FLOSS!**

Hardware

The Hardware Problem

- I'm the admin of my PC.
  Why can't I be the admin of my phone as well?
- We don't use App Stores on Pcs.
  Why should we need them on phones?
- We can choose from hundreds of systems to install on PC.
  Why can't we do that on mobiles as well?

The Hardware Problem

Does a cellphone really differ so much from your average laptop?

It doesn't.

It's just smaller and more integrated.

The Hardware Problem

- Lack of documentation
- Closed components
- Porting – the neverending story
- Upstream? In your dreams.
- When you have to break into your own device in order to use it as you wish, **something is completely wrong!**

The Wise Quote Time

„The reasonable man adapts himself to the world; the unreasonable one persists in trying to adapt the world to himself. Therefore all progress depends on the unreasonable man.”

George Bernard Shaw

The Wise Quote Time

„Think different"

Apple Inc

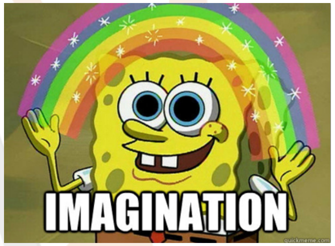
:)

The solution

- Stop adapting to the world
  - Porting is futile

The solution

- Stop adapting to the world
  - Porting is futile
- Start adapting the world!
  - Make hardware dedicated to hacking



Openmoko

- Started by Sean Moss-Pultz
- Funded by Taiwanese company *First International Computer, Inc* (FIC)

Neo1973 GTA01

- Released July 9, 2007
- Samsung s3c2410 @ 266 MHz
- 128 MB RAM
- 64 MB NAND flash
- 480x640 screen, 282 dpi „retina” :P
- TI Calypso 2.5G modem
- Targeted to developers

Neo1973 GTA01

- Lack of WiFi
- GPS needed proprietary driver

Neo Freerunner GTA02

- Released July 3, 2008
- Samsung s3c2442 @ 400 MHz
- SMedia Glamo 3362
- 256 MB NAND flash
- Unbrickable bootloader
- WiFi, u-blox GPS
- Powered USB host mode
- Around 15 000 units sold

Neo Freerunner GTA02

- Glamo graphics accelerator turned out to be a *de*cceletator
- Famous hw problems (GSM buzz, deep sleep), but fixable with some soldering

GTA03 / 3D7K

Speculated specs:

- Cinterion MC75i 2.75G modem
- Cameras
- Samsung s3c6410 @ 533MHz / 667MHz / 800MHz with integrated 3D accelerator
- Unique, transparent case made by famous designer
- **Cancelled in 2009**.

The fall.

- Openmoko Inc. going out of mobile phone business
- Moving to WikiReader instead

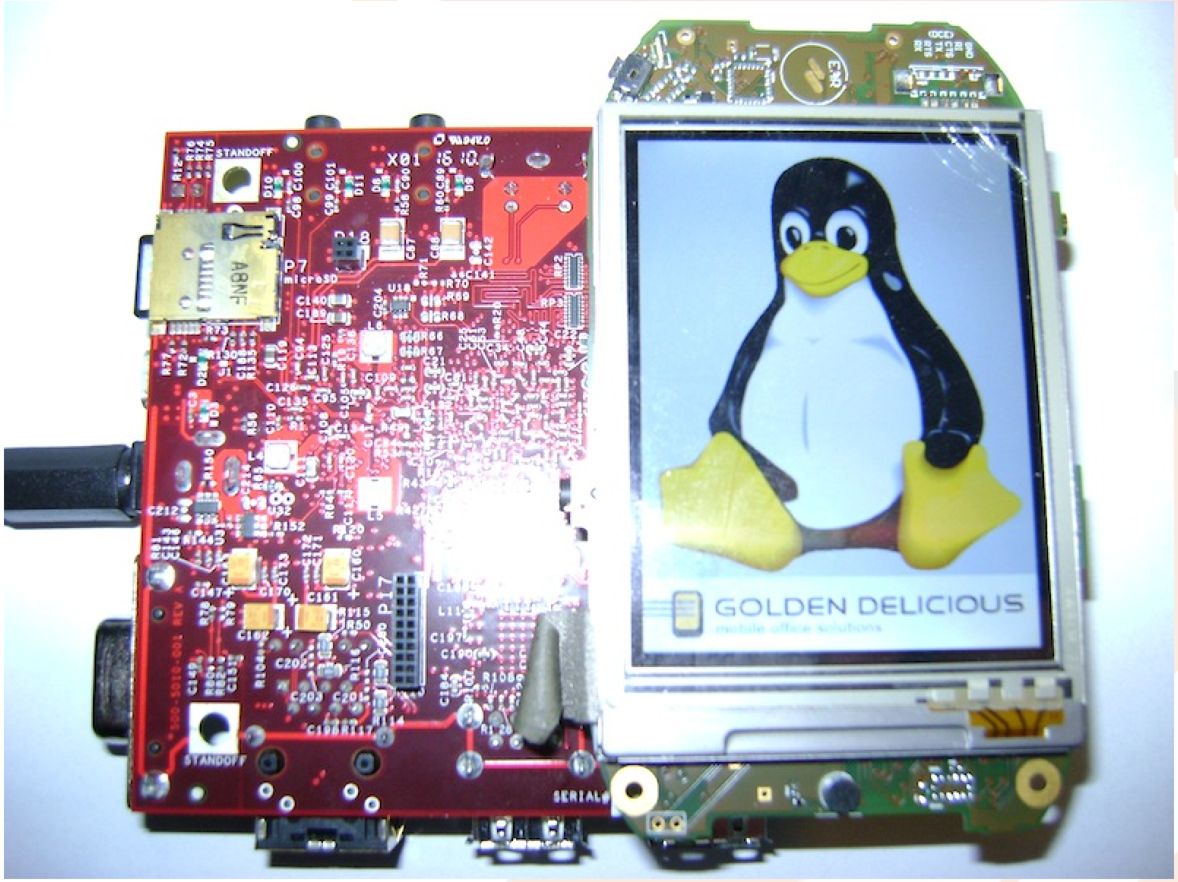
The rise.

- Fortunately, there's an amazing community!
  - Some software support for Neo Freerunner still exists!
  - New hardware initiatives appear.

OpenPhoenux

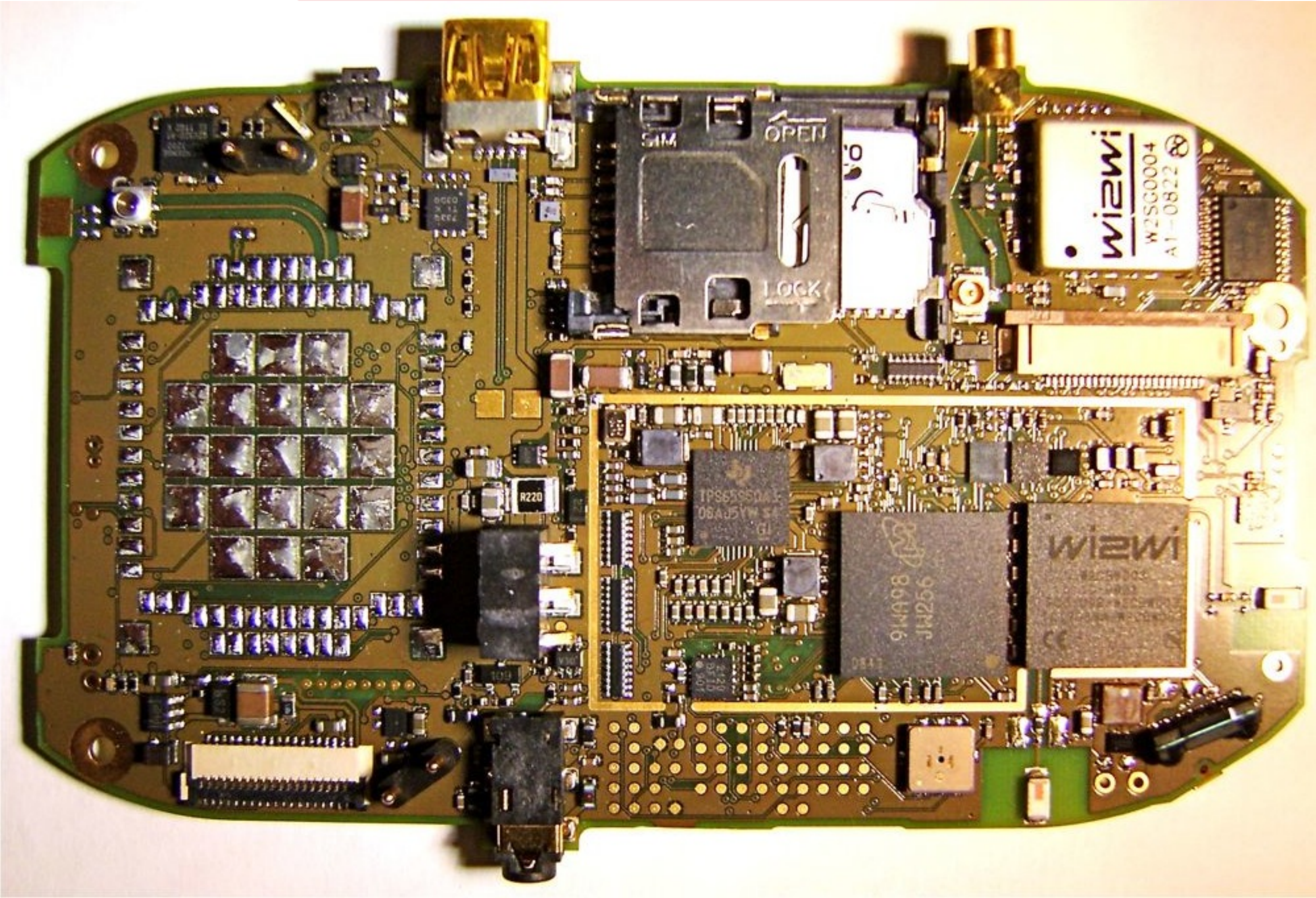
Openmoko Beagle Hybrid

- Project started in 2010 by Dr. H. Nikolaus Schaller
  Golden Delicious Computers GmbH&Co. KG



GTA04

- Beagle Hybrid integrated into single board



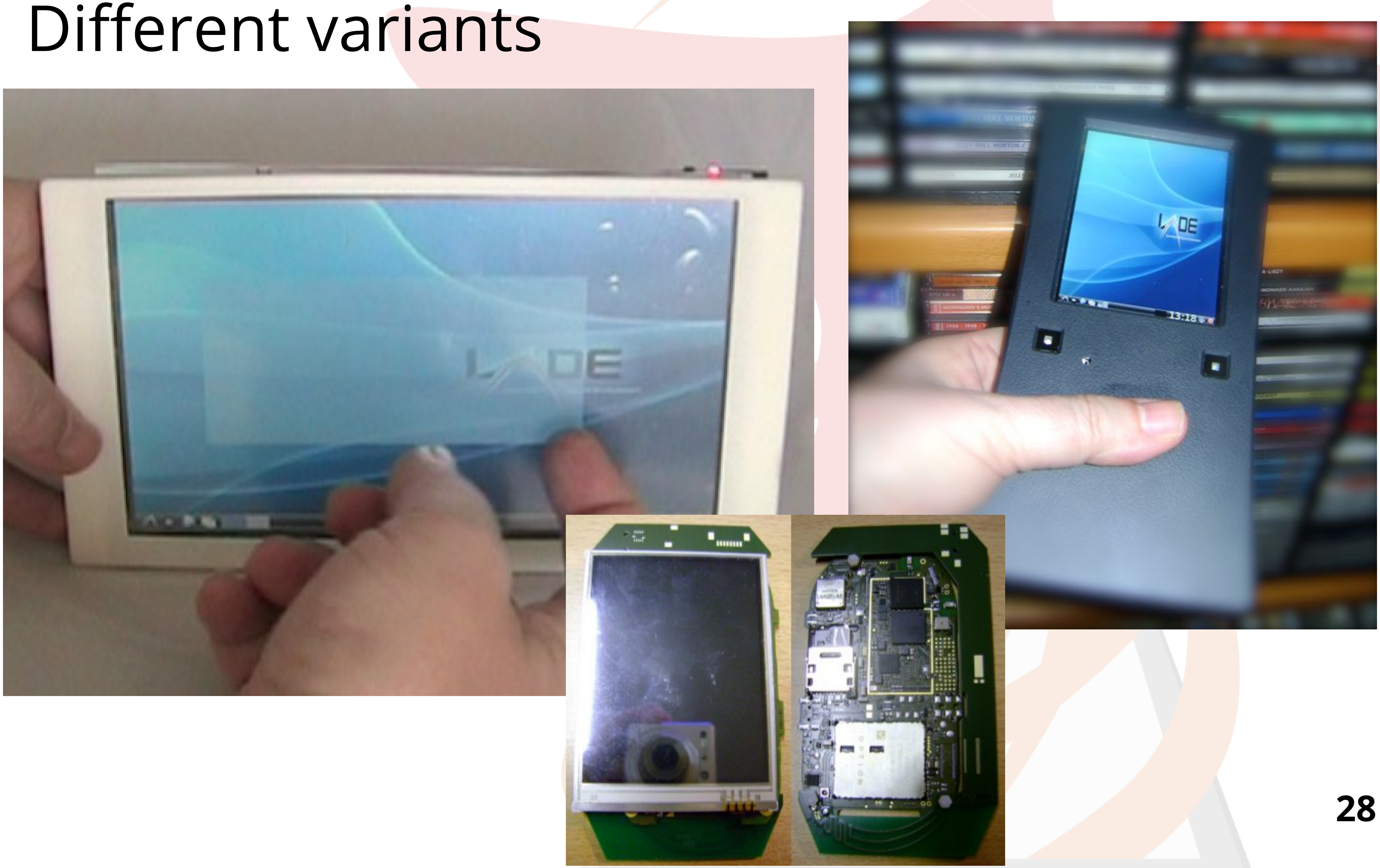
More photos: http://download.goldelico.com/gta04/images/

GTA04

- TI OMAP3 DM3730 @ 800 MHz / 1000 MHz
- PowerVR 3D accelerator
- 512 MB RAM
- 512 MB / 1 GB NAND flash
- Option GTM601 3.75G modem
- http://projects.goldelico.com/p/gta04-main/page/FeatureList/
- **Fits into GTA01/02 case**

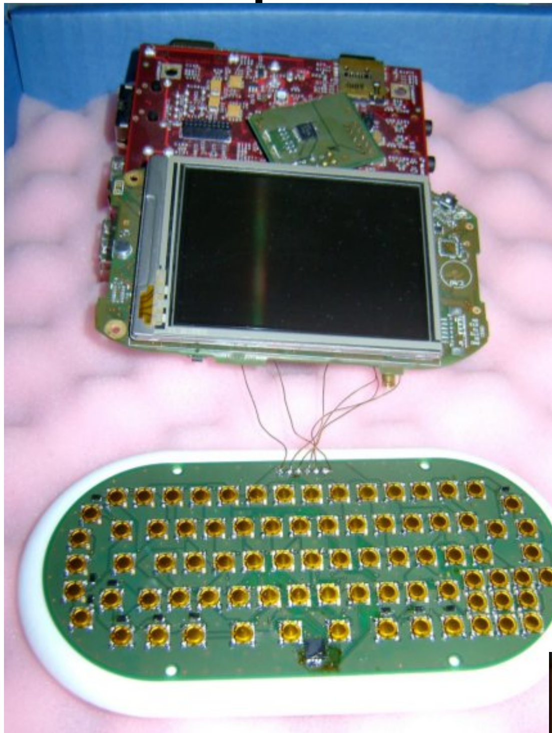
GTA04

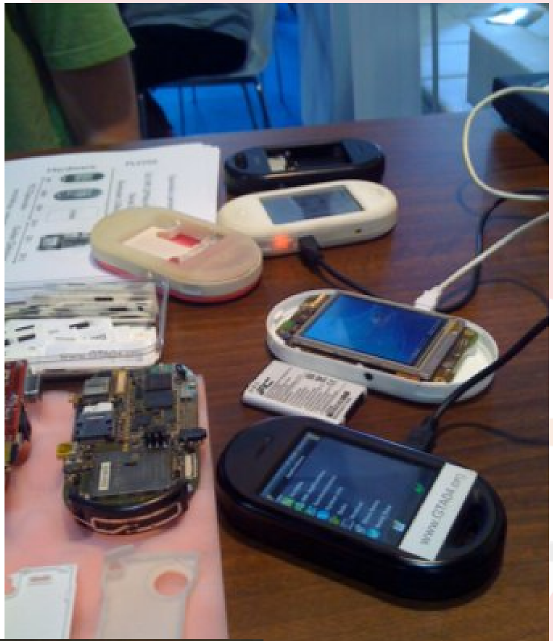
- Different variants



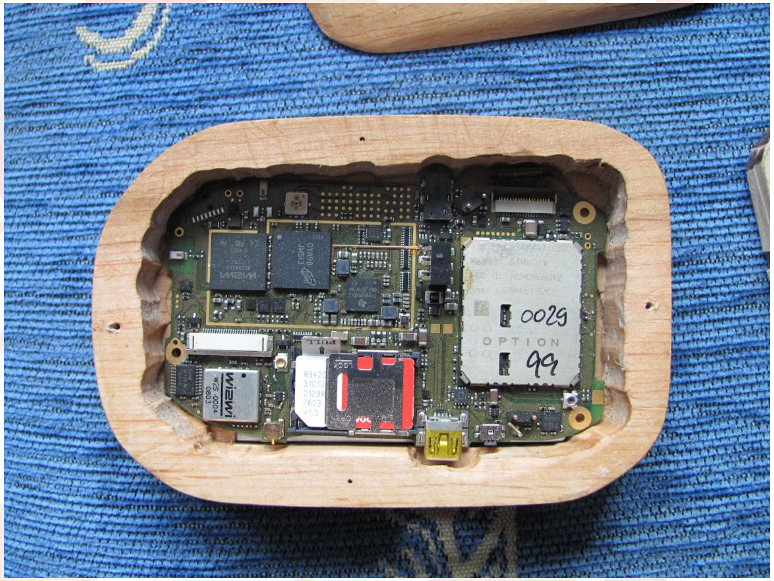
GTA04

- Experiments with cases and hw keyboard



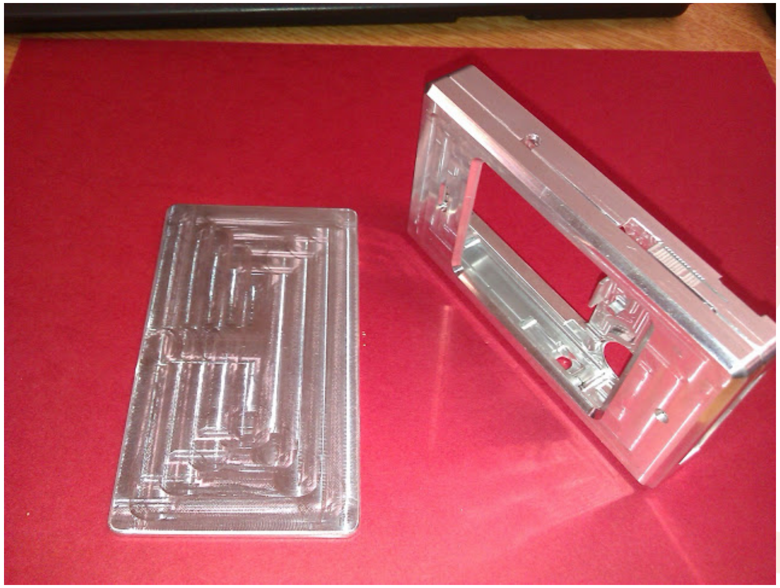


GTA04



https://plus.google.com/photos/114961040002008630266/albums/5668207533167351537?banner=pwa

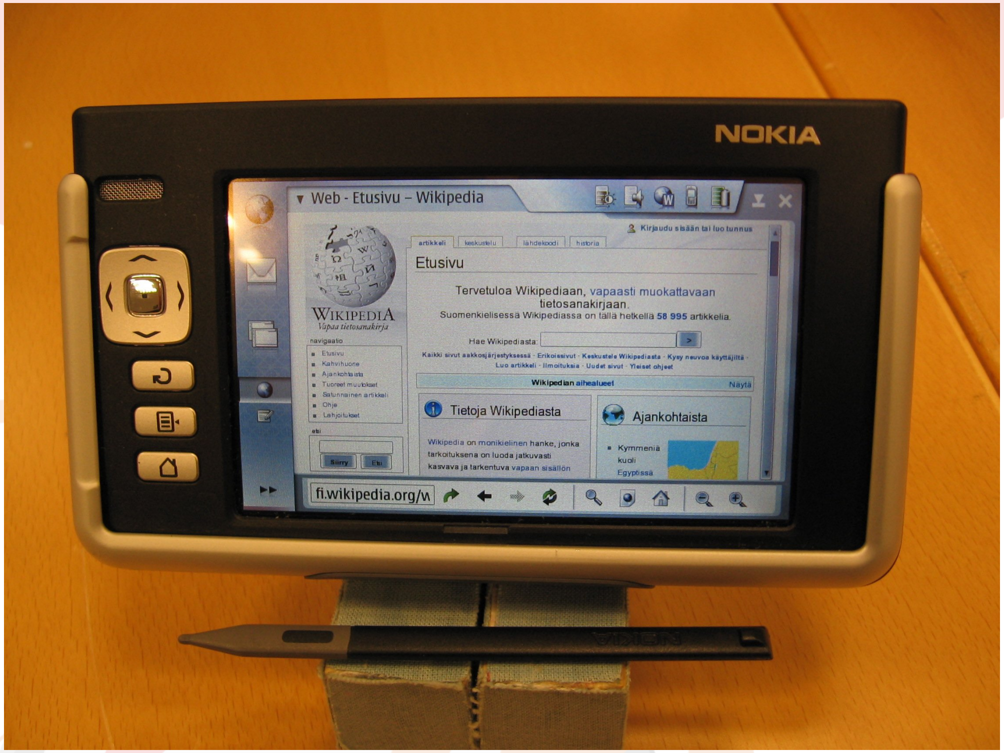
GTA04



1:23
APPS
WIDGETS
Apollo
Browser
Calculator
Calendar
Camera
Clock
Downloads
DSP Manager
Email
F-Droid
File Manager
Gallery
Messaging
Movie Studio
People
Phone
Search
Settings
Sound Recor
Speech Reco
Terminal Em
Voice Dialer

Nokia Internet Tablets

- Running on Maemo
- Nokia 770
- Nokia N800
- Nokia N810
- …


NOKIA
Web - Etusivu – Wikipedia
Etusivu
Tervetuloa Wikipediaan, vapaasti muokattavaan tietosanakirjaan.
Tietoja Wikipediasta
Ajankohtaista
fi.wikipedia.org/w

Nokia N900

- First Maemo based phone
- Released November 11, 2009
- Hacker friendly, with fully free kernel and no restrictions in bootloader
- Still active Maemo 5 community

Neo900

Neo900

Finally **the first true successor** to the N900.
Following the FOSS spirit of **Openmoko**.

Merge of GTA04 and Nokia N900

http://neo900.org/

Neo900

- Announced August 25, 2013
- Team members:
  - Jörg Reisenweber
  - Nikolaus Shaller
  - Sebastian Krzyszkowiak

Neo900

- TI OMAP3 DM3730 @ 1 GHz
- 1 GB RAM
- 1 GB NAND + 32/64 GB eMMC
- Cinterion PHS8/PLS8 modem (LTE)
- GPS/GLONASS
- Battery hot-swap support
- Modem sandbox and monitoring solution
- http://neo900.org/specs

Neo900

- Unexpectedly good reaction!
- Oct 30, 2013 – fundraiser started
- Nov 04, 2013 – 25k EUR reached
- Dec 02, 2013 – 200 devices reached
- Now at 366 devices / 76k EUR

Neo900

- Right now donations are temporarily suspended due to reorganisation.
- The raised amount may change due to having to pay it back :(
- New way to collect the money starting soon
- Stay informed: http://neo900.org/subscribe

Privacy

Open baseband?

- Unfortunately, it's not going to happen for both economical and legal reasons.
- Basebands are cryptographically locked and any change in their firmware results in revokation of their certification, rendering them illegal to use in public networks.

OsmocomBB

- Open baseband firmware
- Runs on *TI Calypso* (the same as in GTA01/02)
- **Illegal** to use as a phone outside the lab
- http://bb.osmocom.org

Open baseband?

- However, open baseband **does not** fix the privacy problems.

The threats

- Tracking
  - Trilateration based (IPL, OTDOA, E-OTD, U-TDOA)
  - GPS-assisted (RRLP)
- Eavesdropping
- Data leakage
- Security bugs in firmware
- Direct access to main RAM

Not solvable

- Eavesdropping of calls
- Eavesdropping of Internet connection
- Trilateration while connected to the network

It can (and **does**) happen *outside* of the device or is *necessary* for it to function. Aside from **encryption**, there's nothing we can do against it.

Neo900 concept

- **Counter-surveillance** rather than audit and trust
- Everything not 100% in control is **considered rogue**
- Rogue stuff is **sandboxed** and constantly **monitored**

Neo900 design

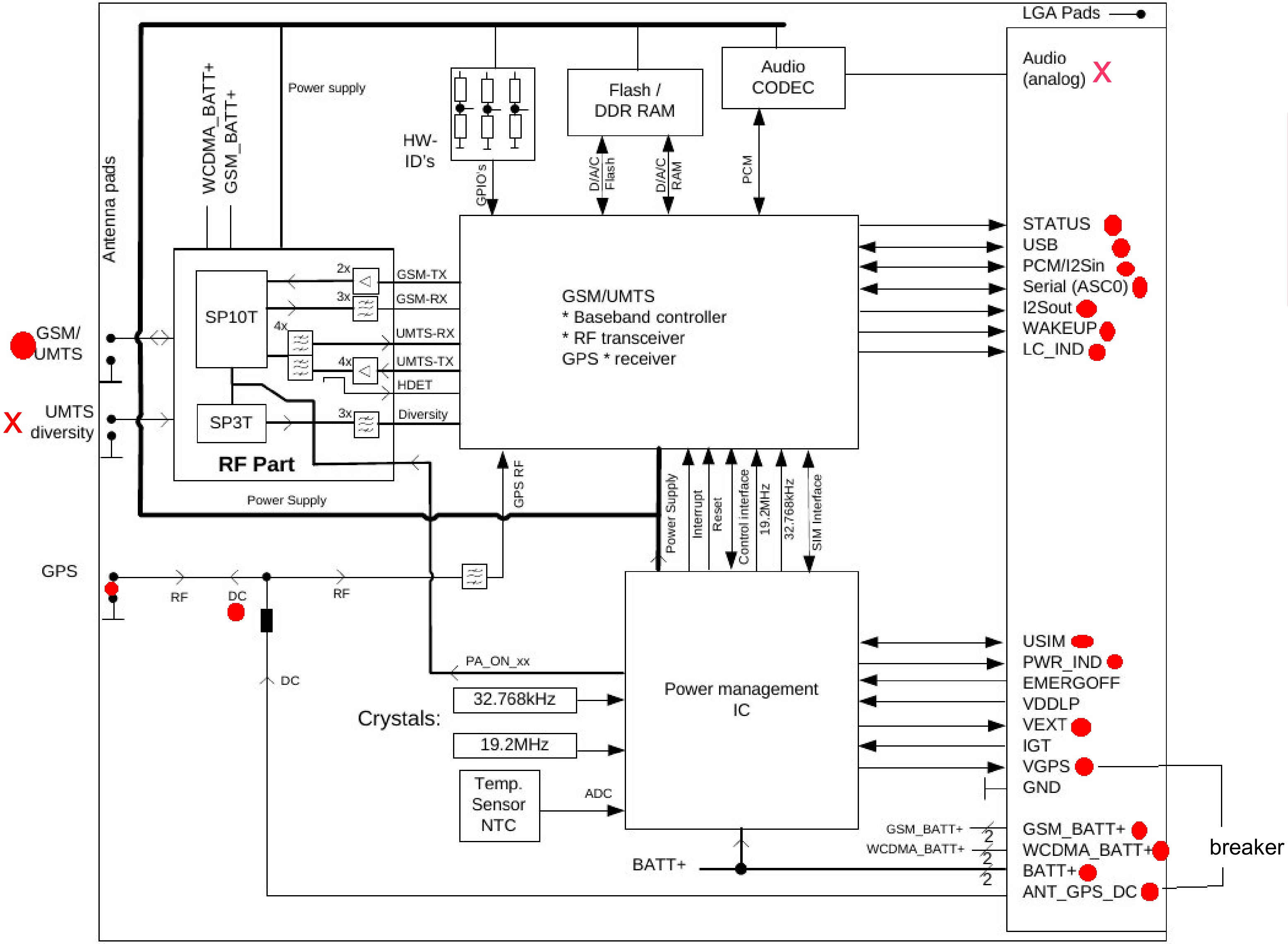


Figure 2: PHS8-P/PHS8-K block diagram

Neo900 design

- If the modem is compromised, the main system **remains safe** use the encryption, Luke
- If the modem is supposed to be off, but it isn't – **we know that** and can react accordingly
- If the GPS is in use when not requested – **we know that** but the antenna will be disabled :)
- If the modem tries to record audio when not requested – **we know that** but it won't be able to do it :)

Neo900 design

- When modem act badly, user is notified and automatic hard reset via emergency_off line is applied.

Neo900 concept

- This way, when something fishy is going on, software kicks off an alarm to make user do **efficient measures** to stop the threat:
  - Removing the battery
  - Destroying the device
  - Hiding it under the seat in bus and leaving
- With basic solutions like external power switch, user is not aware that his device has been tampered with.

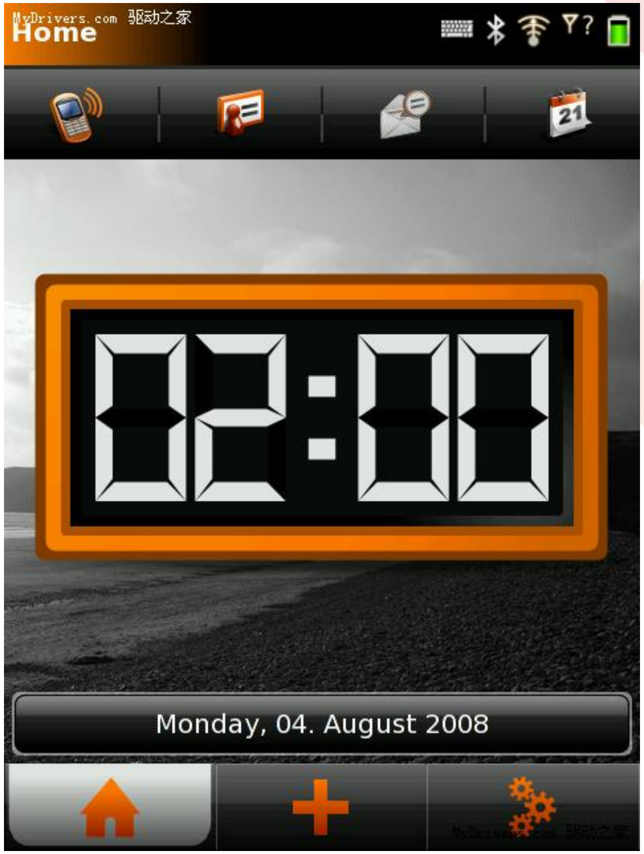
Neo900 design

- Our monitoring approach can also reveal some „rogue” activities from outside – like packet-storms on airports.

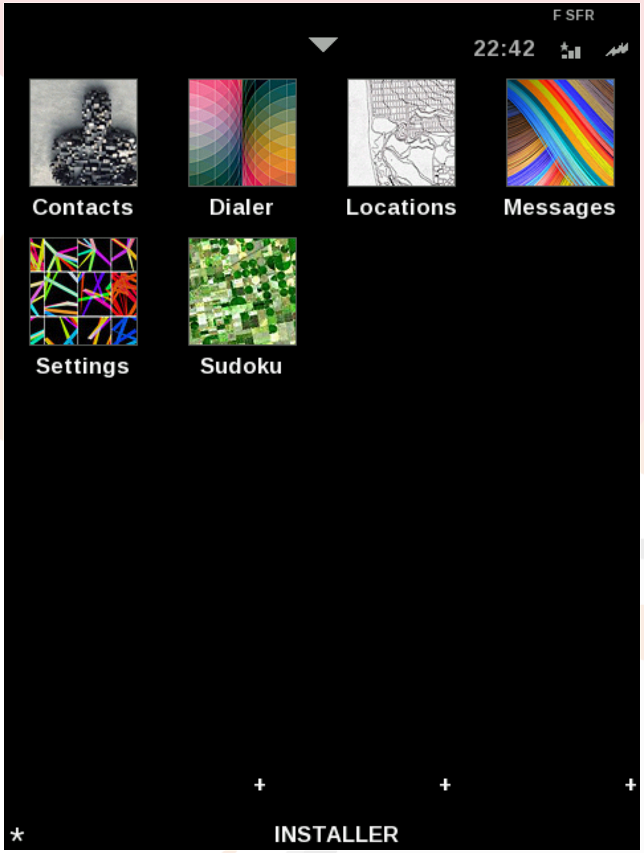
  https://www.schneier.com/blog/archives/2014/04/gogo_wireless_a.html#c5459667

Software

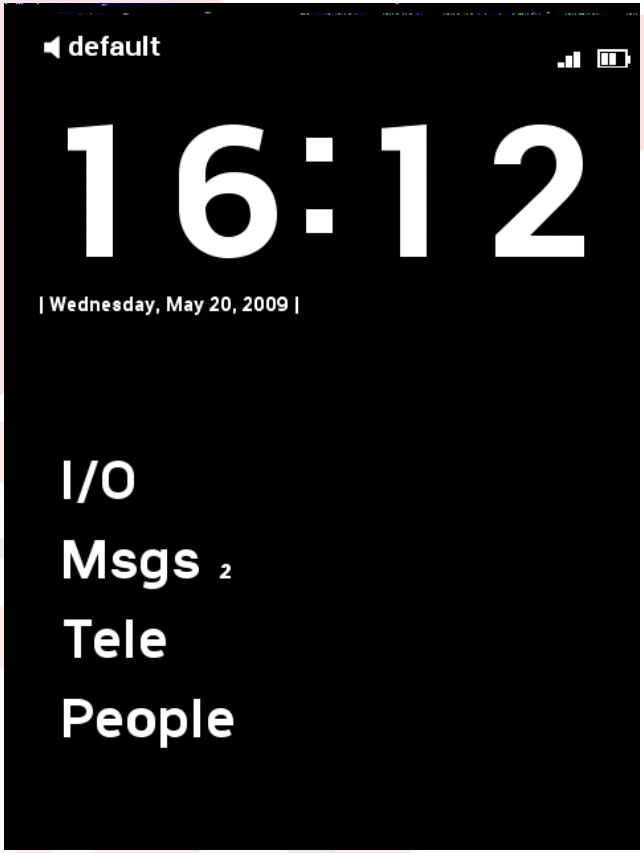
Openmoko



Om2007.2



Om2008

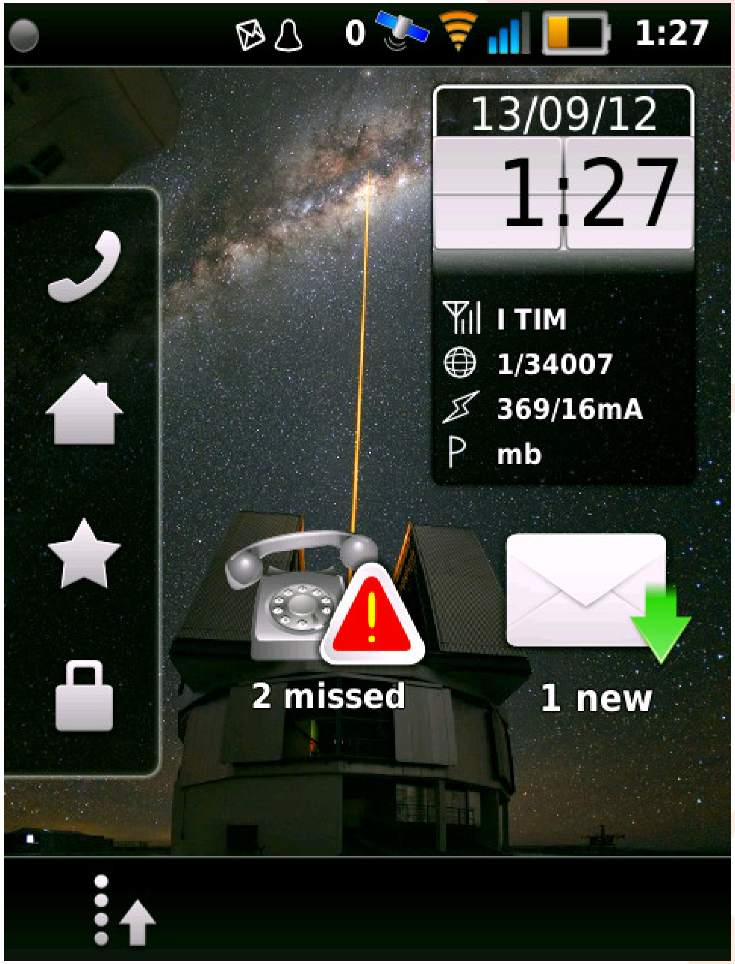


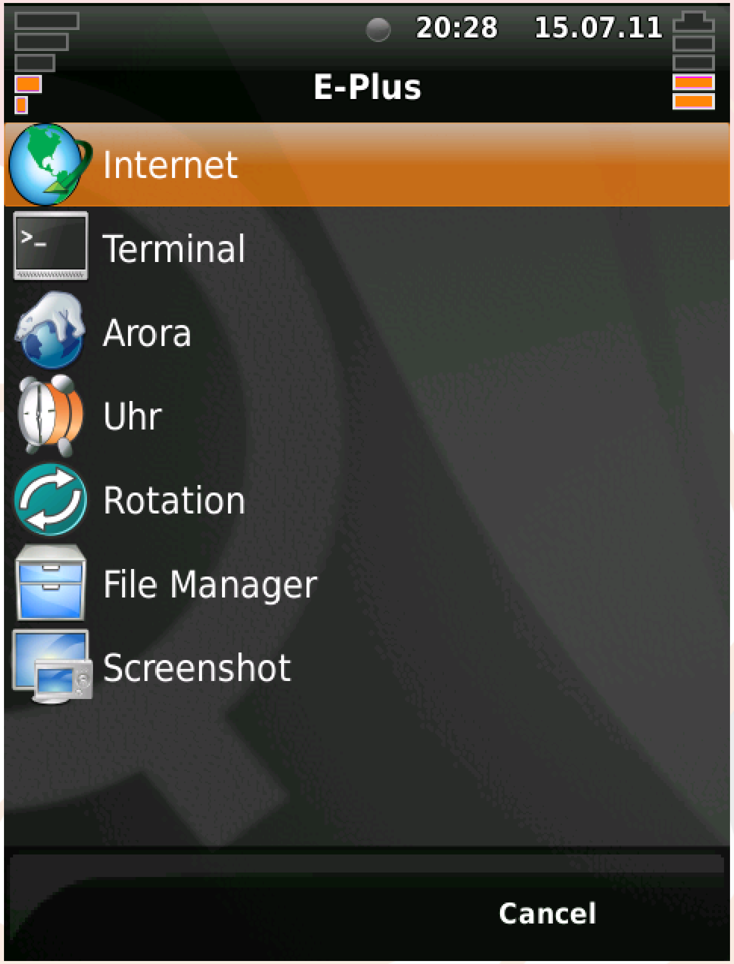
Om2009

QtMoko

http://qtmoko.sourceforge.net/

- Fork of Qtopia / Qt Extended

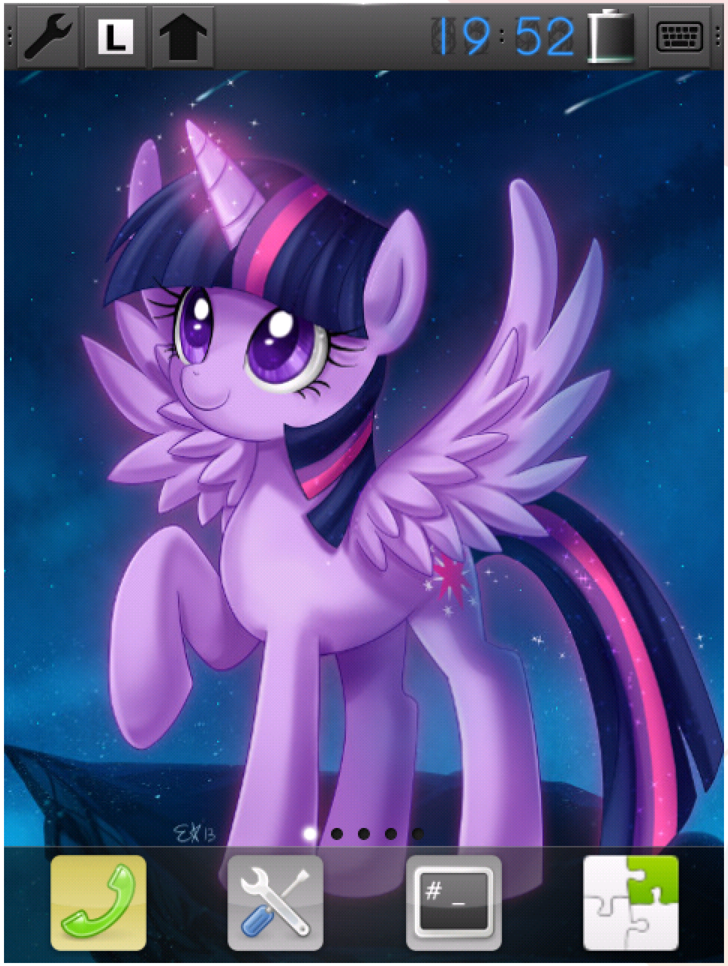


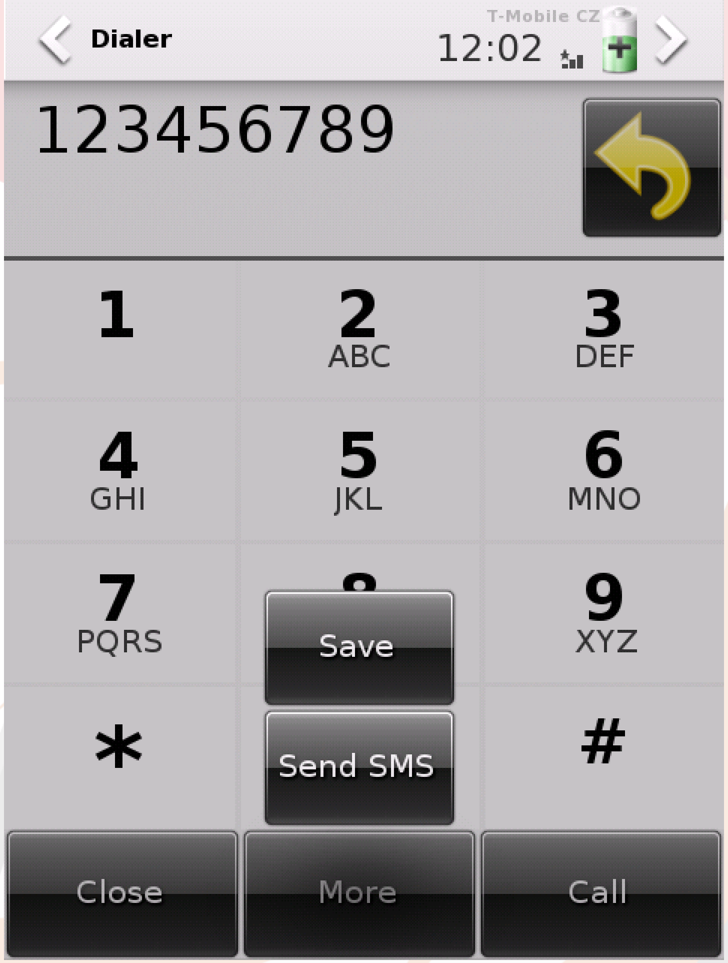


SHR

http://shr-project.org/

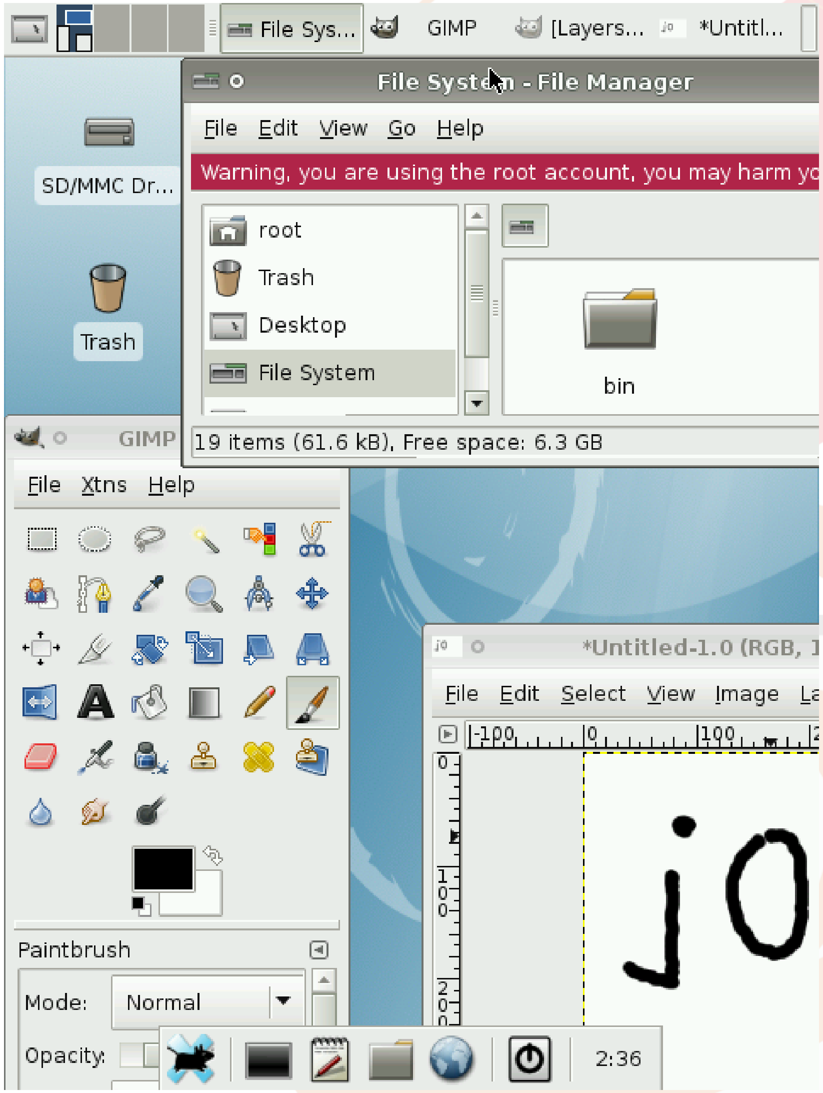
- Based on e17 and FSO




Dialer

123456789

Debian

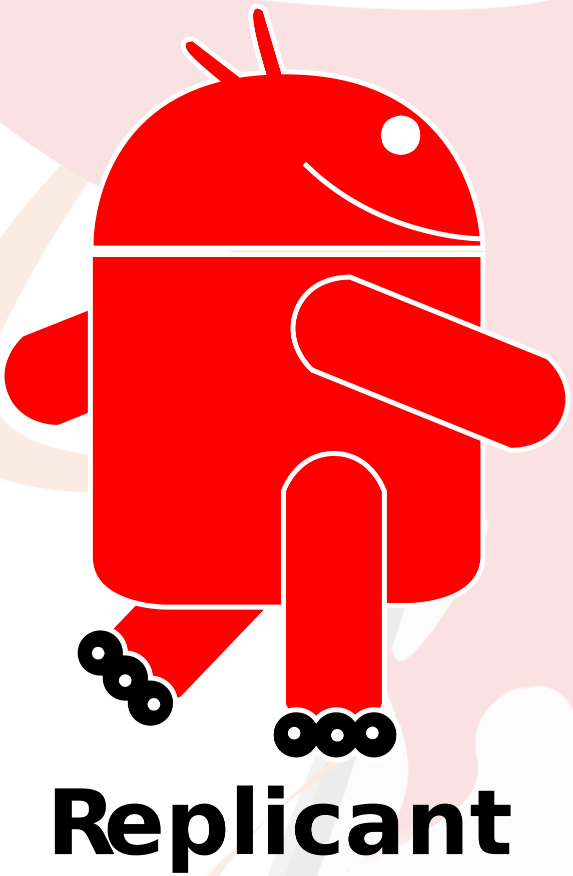


Warning, you are using the root account, you may harm yo

19 items (61.6 kB), Free space: 6.3 GB

Mode: Normal

Replicant



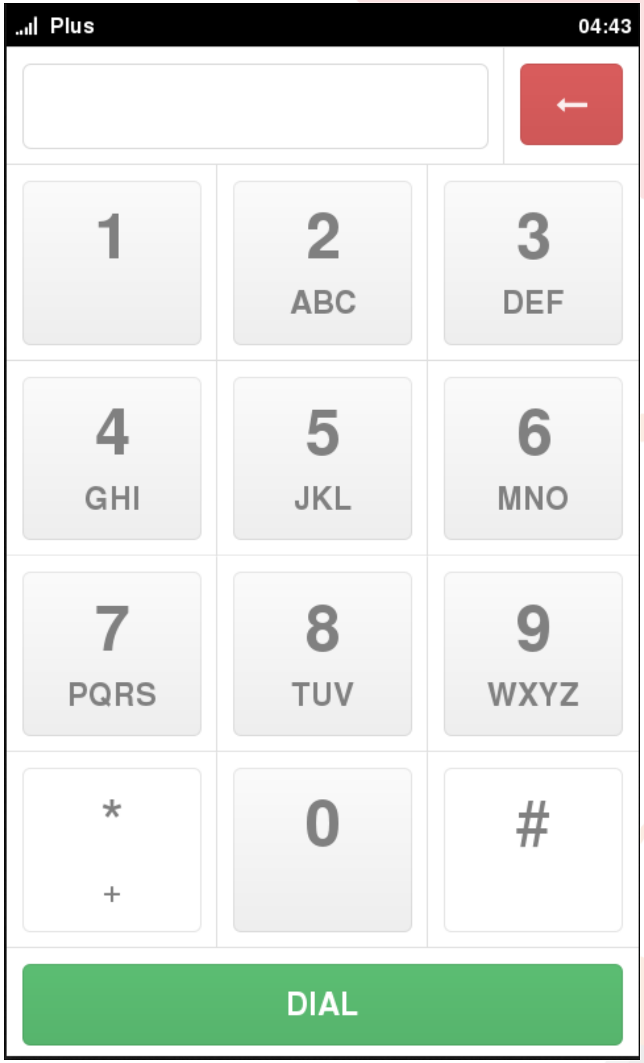
http://replicant.us/

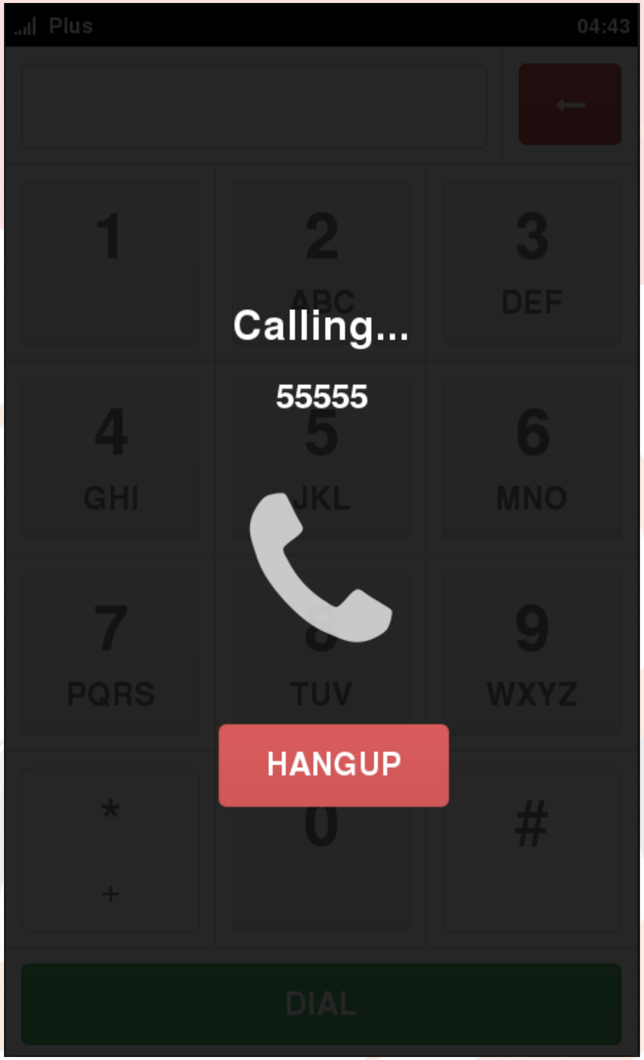
„Freemantle”

- Maemo 5 „Fremantle”
- Proprietary components being successively replaced with FLOSS equivalents by community
- CSSU – community updates
- http://maemo.org/

jasi

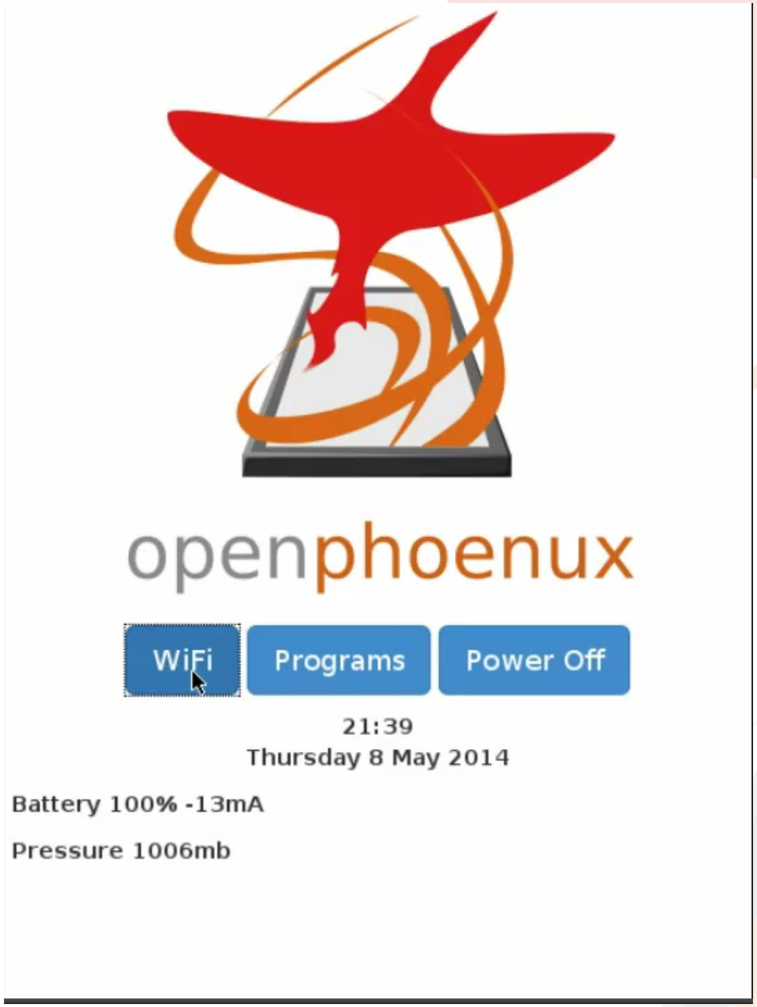
- https://www.youtube.com/watch?v=jKyK-h4i_wM





Neil's Experimental Userspace

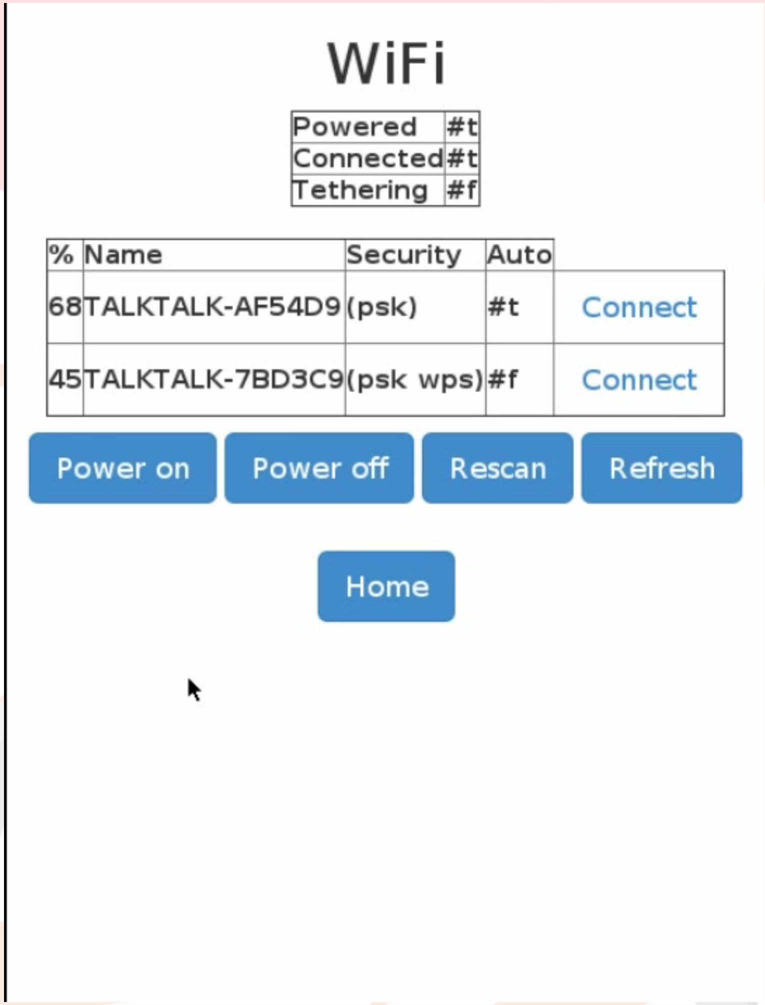
- By Neil Jerram



21:39
Thursday 8 May 2014

Battery 100% -13mA

Pressure 1006mb



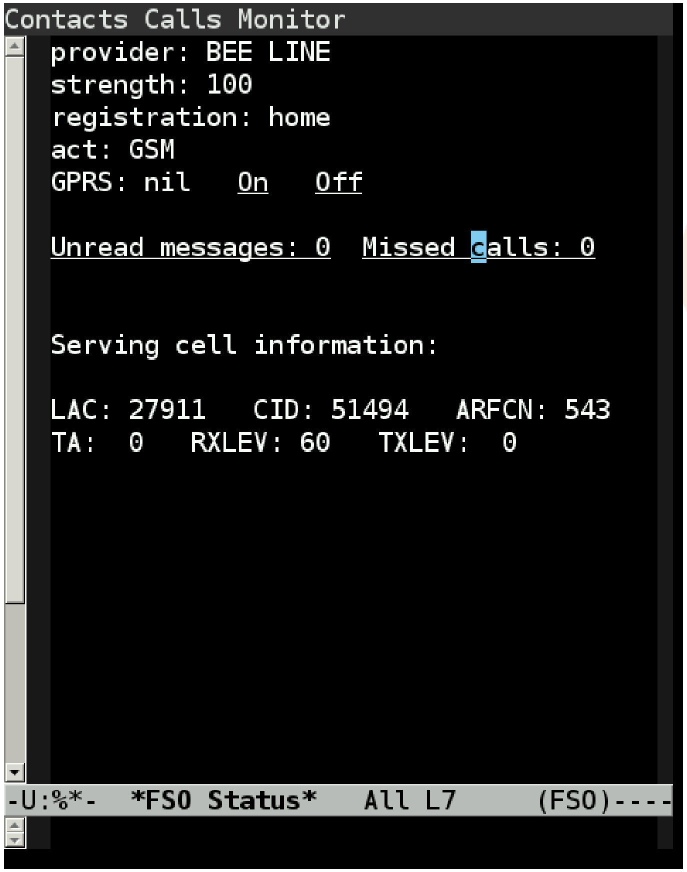
WiFi

Powered	#t
Connected	#t
Tethering	#f

%	Name	Security	Auto	
68	TALKTALK-AF54D9	(psk)	#t	Connect
45	TALKTALK-7BD3C9	(psk wps)	#f	Connect

fso-el

- By Paul Fertser



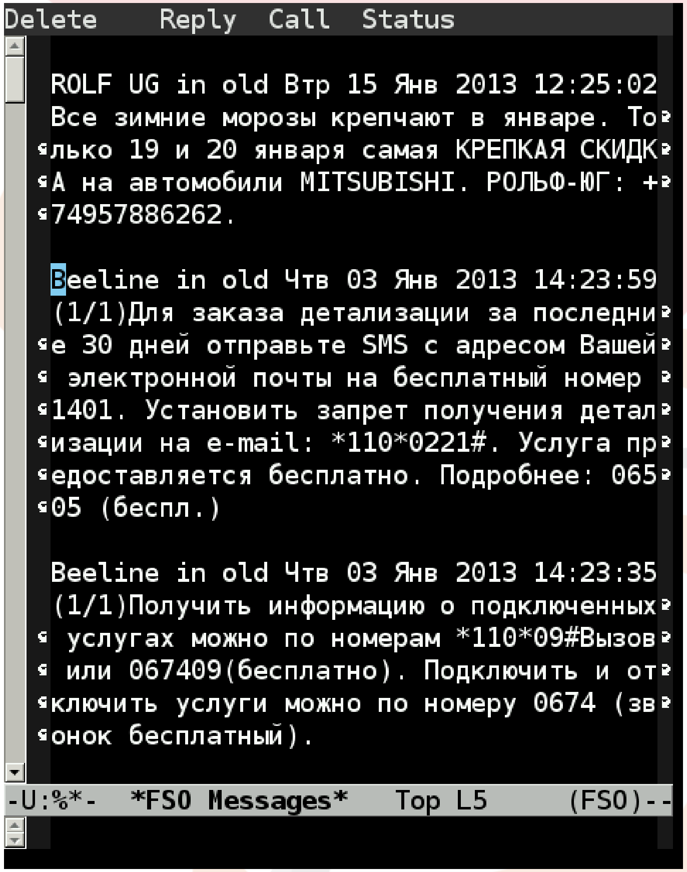
```
Contacts Calls Monitor
provider: BEE LINE
strength: 100
registration: home
act: GSM
GPRS: nil   On   Off

Unread messages: 0  Missed calls: 0


Serving cell information:

LAC: 27911   CID: 51494   ARFCN: 543
TA:  0   RXLEV: 60   TXLEV:  0
```

```
-U:%*-   *FSO Status*   All L7      (FSO)----
```



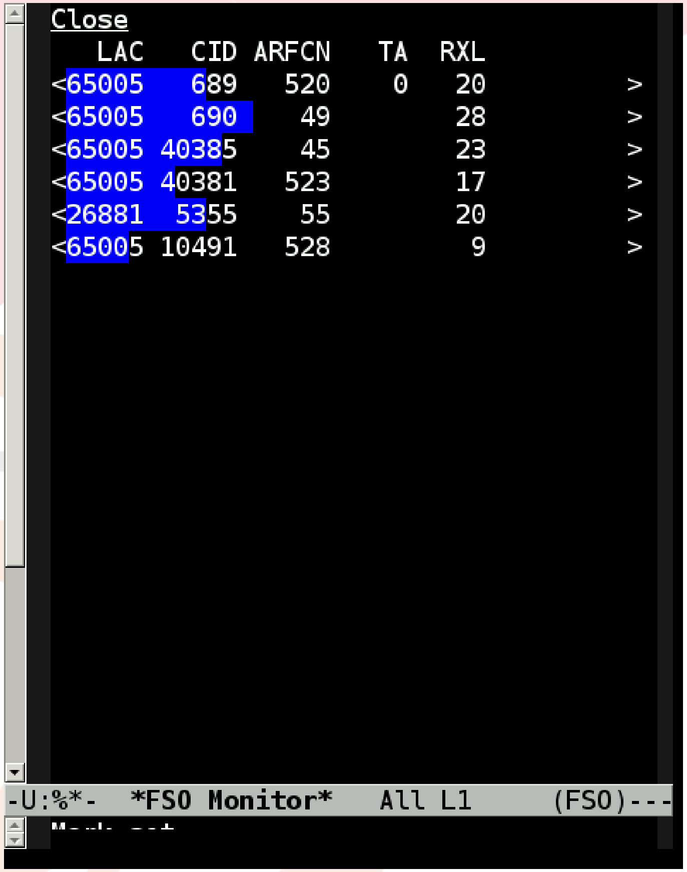
```
Delete     Reply  Call  Status

 ROLF UG in old Втр 15 Янв 2013 12:25:02
 Все зимние морозы крепчают в январе. То
лько 19 и 20 января самая КРЕПКАЯ СКИДК
А на автомобили MITSUBISHI. РОЛЬФ-ЮГ: +
74957886262.

 Beeline in old Чтв 03 Янв 2013 14:23:59
 (1/1)Для заказа детализации за последни
е 30 дней отправьте SMS с адресом Вашей
 электронной почты на бесплатный номер 
1401. Установить запрет получения детал
изации на e-mail: *110*0221#. Услуга пр
едоставляется бесплатно. Подробнее: 065
05 (беспл.)

 Beeline in old Чтв 03 Янв 2013 14:23:35
 (1/1)Получить информацию о подключенных
 услугах можно по номерам *110*09#Вызов
 или 067409(бесплатно). Подключить и от
ключить услуги можно по номеру 0674 (зв
онок бесплатный).
```

```
-U:%*-   *FSO Messages*   Top L5      (FSO)--
```



```
Close
   LAC    CID ARFCN    TA  RXL
<65005    689   520     0   20          >
<65005    690    49         28          >
<65005 40385    45          23          >
<65005 40381   523          17          >
<26881   5355    55         20          >
<65005 10491   528           9          >
```

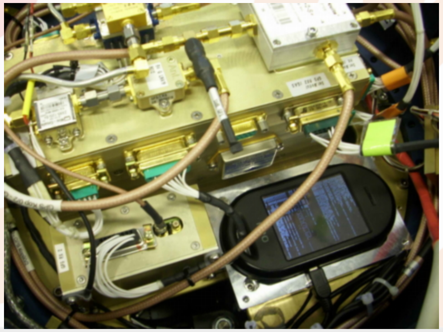
```
-U:%*-   *FSO Monitor*   All L1      (FSO)---
```

Miscellaneous

- OpenWRT
- FreeBSD
- Arch
- Gentoo
- QuantumSTEP
- Inferno
- ...and more!

Interesting projects

- ReMoko https://code.google.com/p/remoko/
- Accelges https://code.google.com/p/accelges/
- Freerunner Navigation Board http://wiki.openmoko.org/wiki/Freerunner_Navigation_Board_v3
- Freerunner in space



Demo!

freesmartphone.org

- A set of D-Bus APIs to get the most out of your smartphone
- Full-fledged GSM middleware (fsogsmd)
- Resource handling daemon (fsousaged)
- Power management etc. (fsodeviced)
- ...and more!
- http://docs.freesmartphone.org/

freesmartphone.org

- Easy to use in your application, using any D-Bus enabled language
- Let's try it!

Questions?

Thank you!

http://neo900.org/piwo/