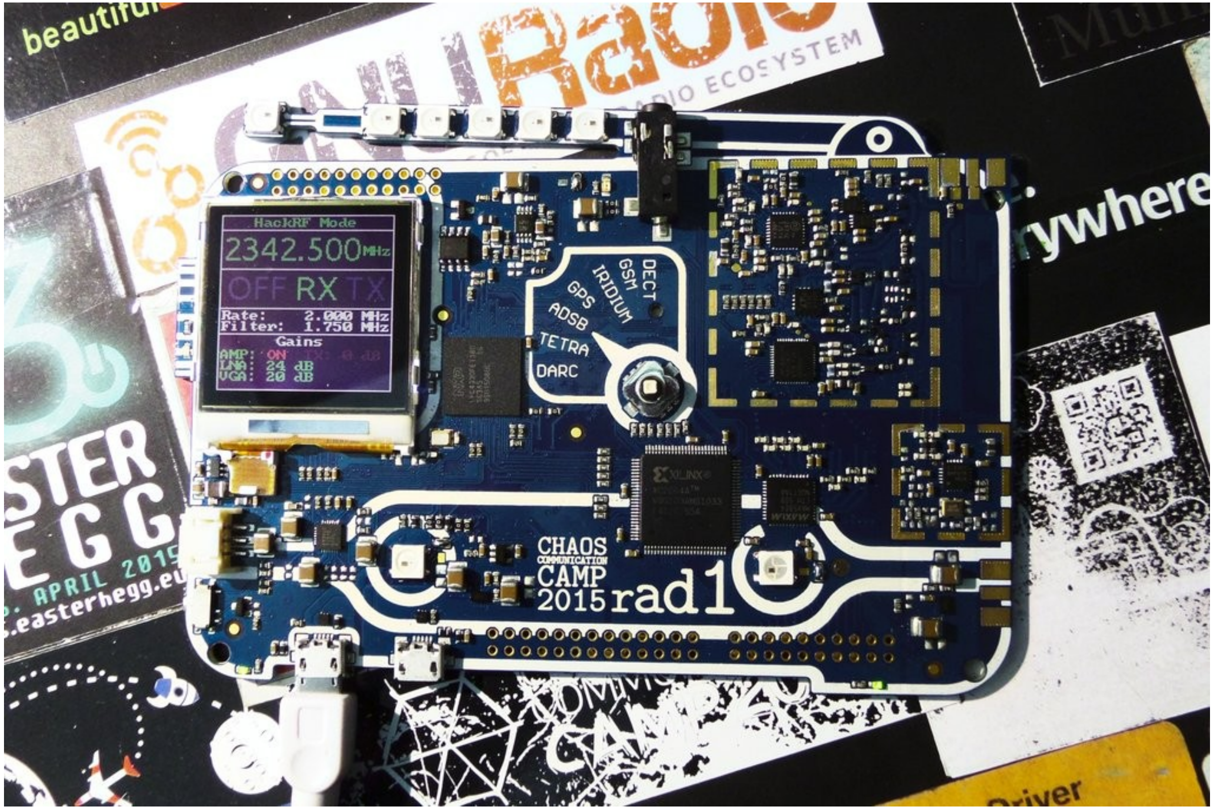
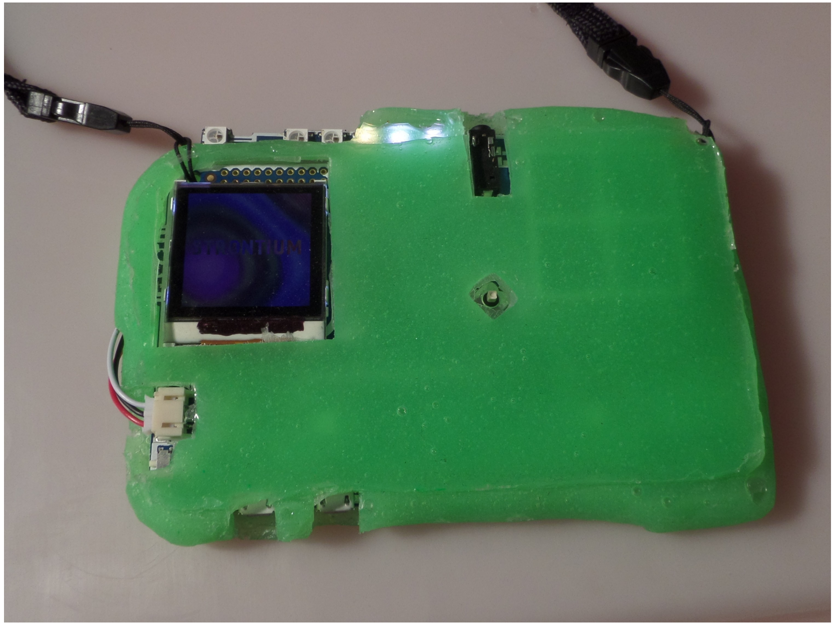
rad1o++



Sec
schneider

What is the rad1o?

- Made for CCCamp15
- Multirole SDR badge
  - Portable SDR that is also a badge
- Compatible with the HackRF
- Dual core ARM (M4 + M0) development platform
- Two USB ports
  - With host support



Why Did We Do It?

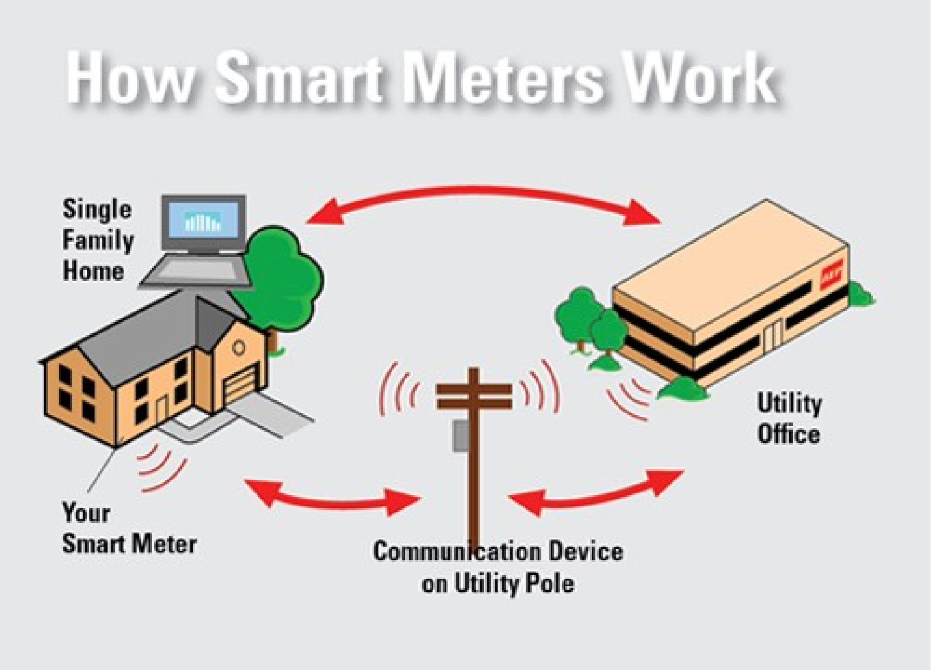
- The badge for CCCamp11 was a blast
- Its goal: Have something reusable that is not an Arduino

Why an SDR?

- Have something useful way after camp
- Don't just put some sensor on it that next phone generation has by default

SDR

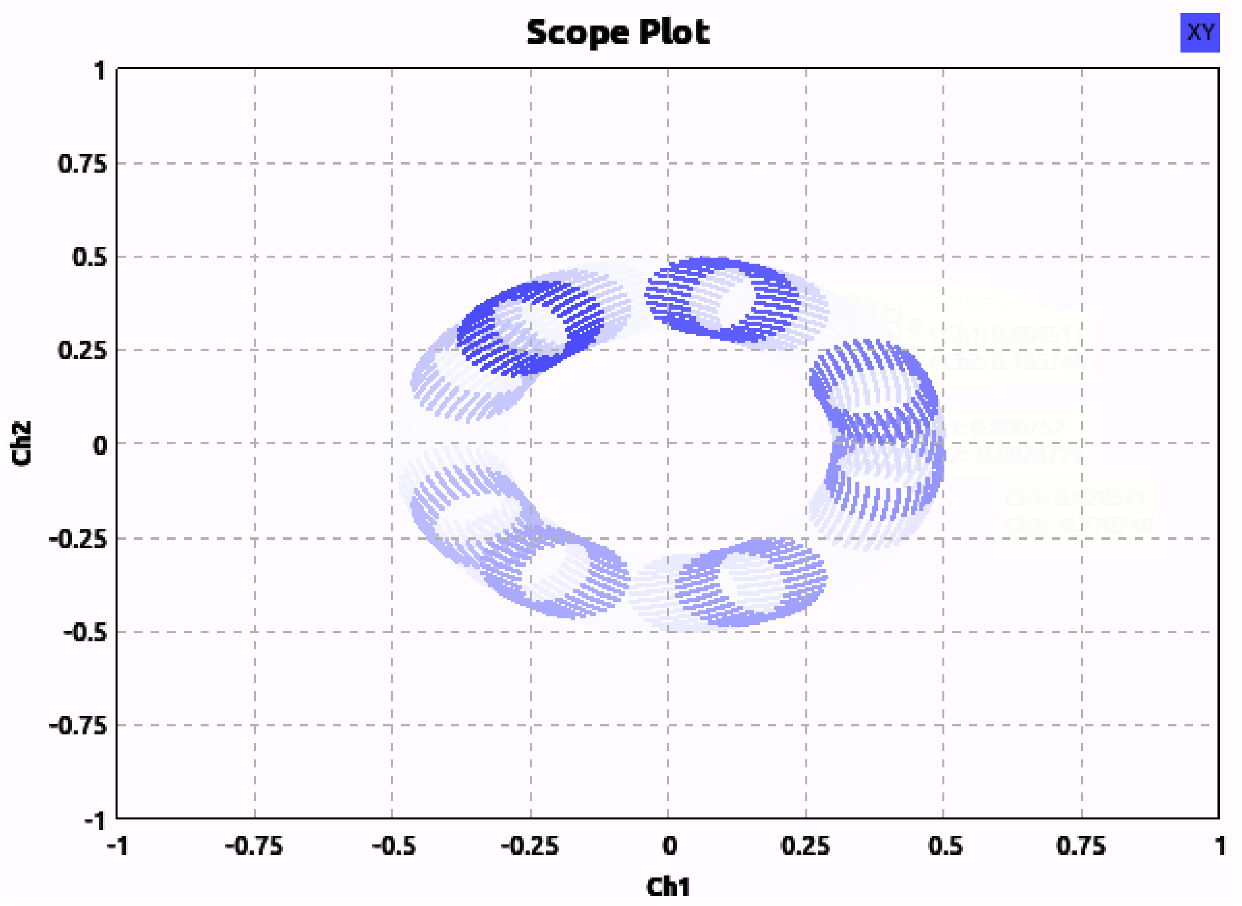
- There's lots of proprietary or inaccessible wireless stuff out there
  - You most likely own such things
  - They might appear next to your door
  - They might drive around or fly over you
- SDR lets us probe and interact with that stuff



SDR

- What you need
  - Motivation
  - Time

- Essential math
  - sin(), cos()
  - Pythagoras

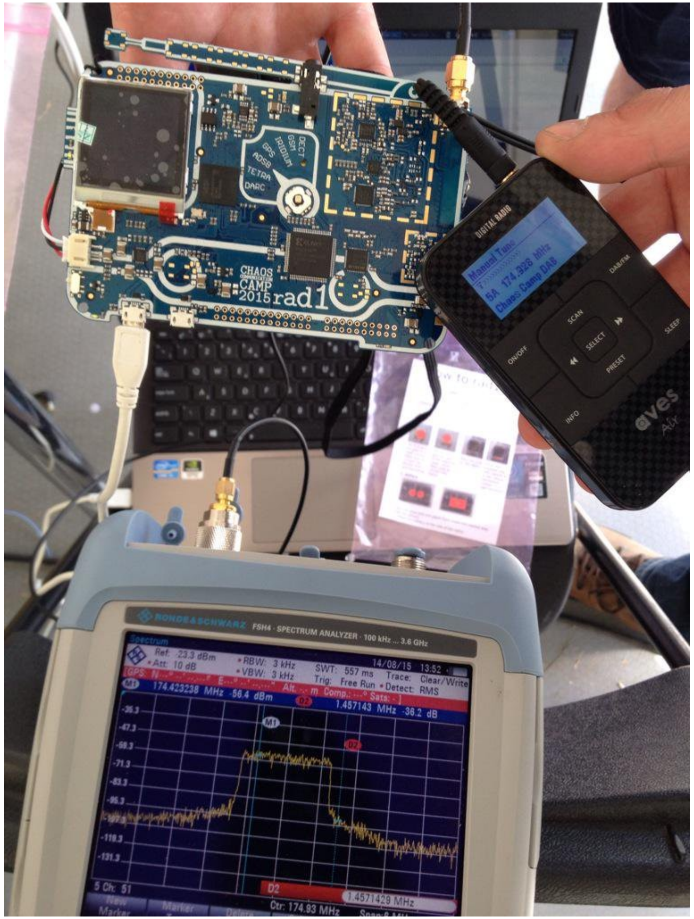


Where can I get one?

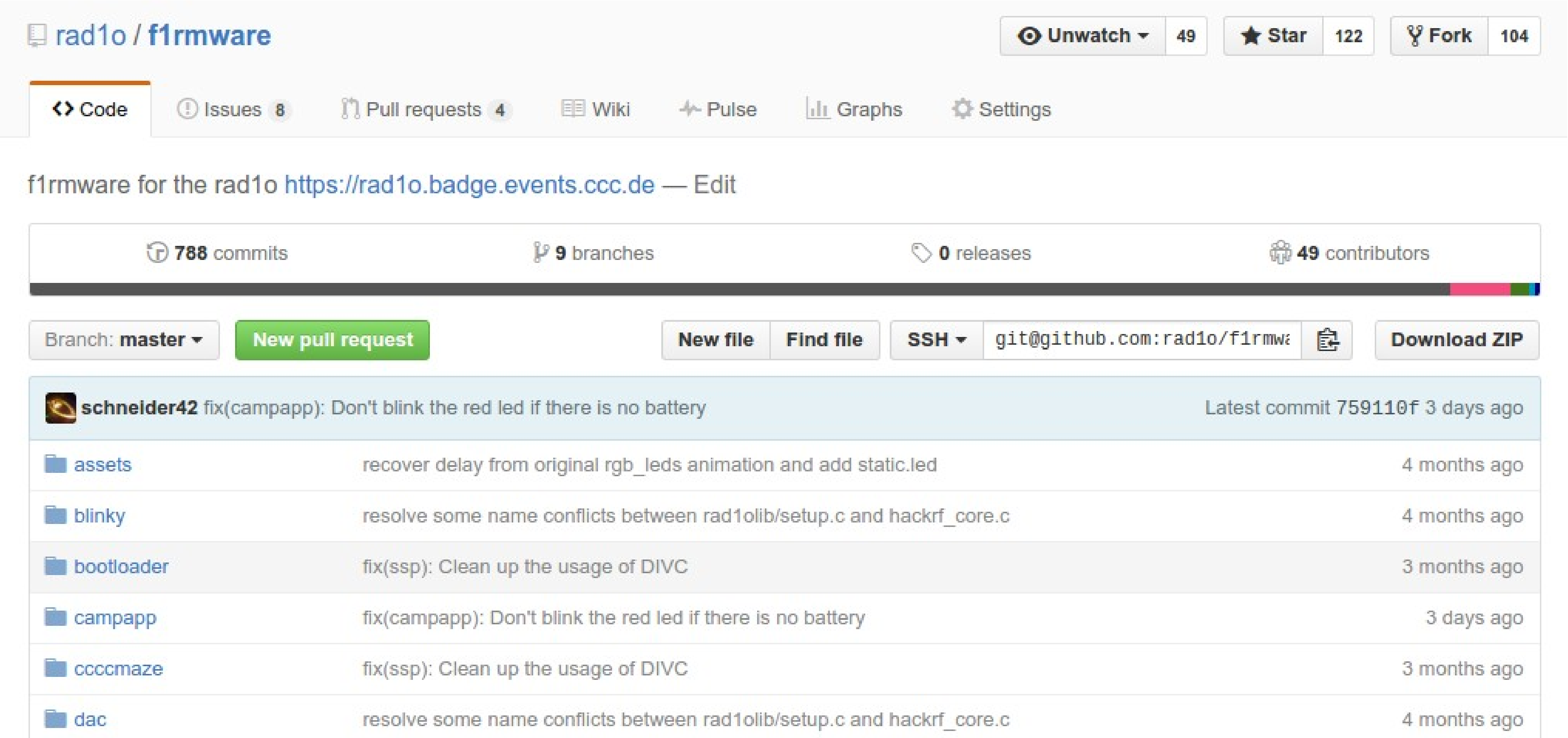
- We won't be selling any rad1os
  - So far no one has stepped up
  - Unlikely that this is going to change next year :/
- But do not despair: It's an open source project after all
- EAGLE files available on GitHub
  - Sorry, didn't have time for KiCad :/
- One of our prototype manufactures is willing to help
  - Contact details at the end of the talk

TOC

- f1rmware
  - Current state
  - New goals
- Hardware
  - Known Issues
  - Maintenance
  - Performance Improvements
- rad1o challenge
- l0unge l1icht
- SDR



f1rmware



f1rmware for the rad1o https://rad1o.badge.events.ccc.de — Edit

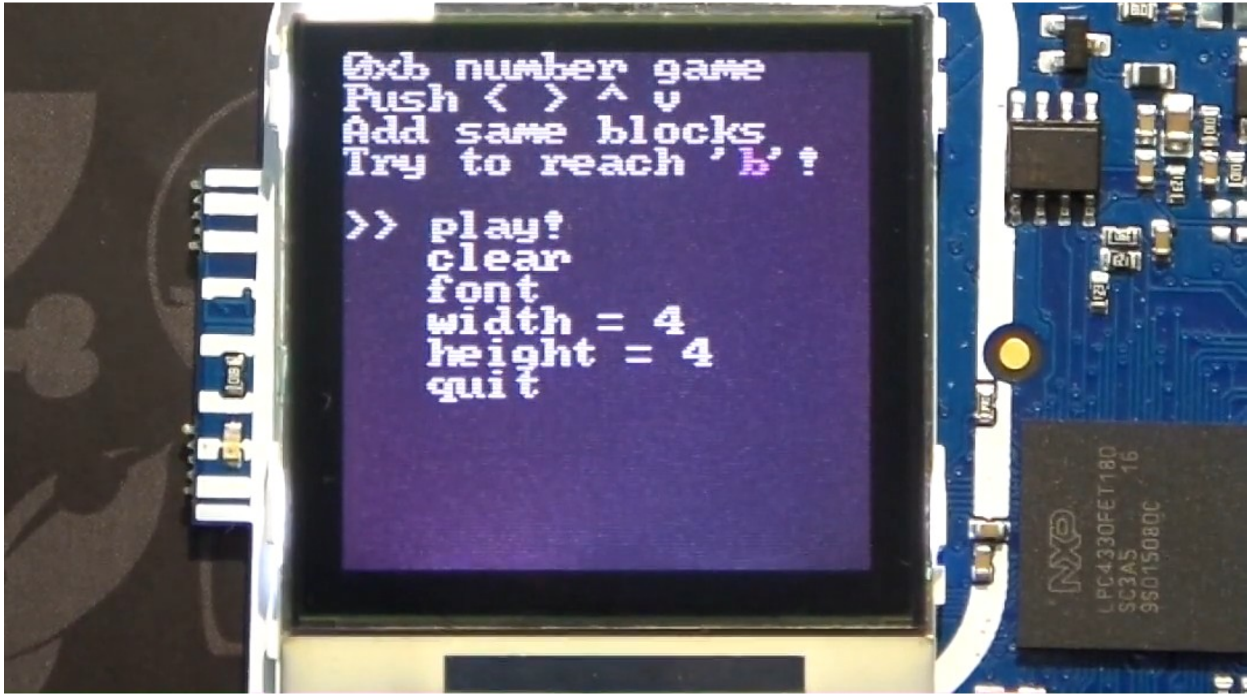
schneider42 fix(campapp): Don't blink the red led if there is no battery Latest commit 759110f 3 days ago

assets	recover delay from original rgb_leds animation and add static.led	4 months ago
blinky	resolve some name conflicts between rad1olib/setup.c and hackrf_core.c	4 months ago
bootloader	fix(ssp): Clean up the usage of DIVC	3 months ago
campapp	fix(campapp): Don't blink the red led if there is no battery	3 days ago
ccccmaze	fix(ssp): Clean up the usage of DIVC	3 months ago
dac	resolve some name conflicts between rad1olib/setup.c and hackrf_core.c	4 months ago

f1rmare: l0dables

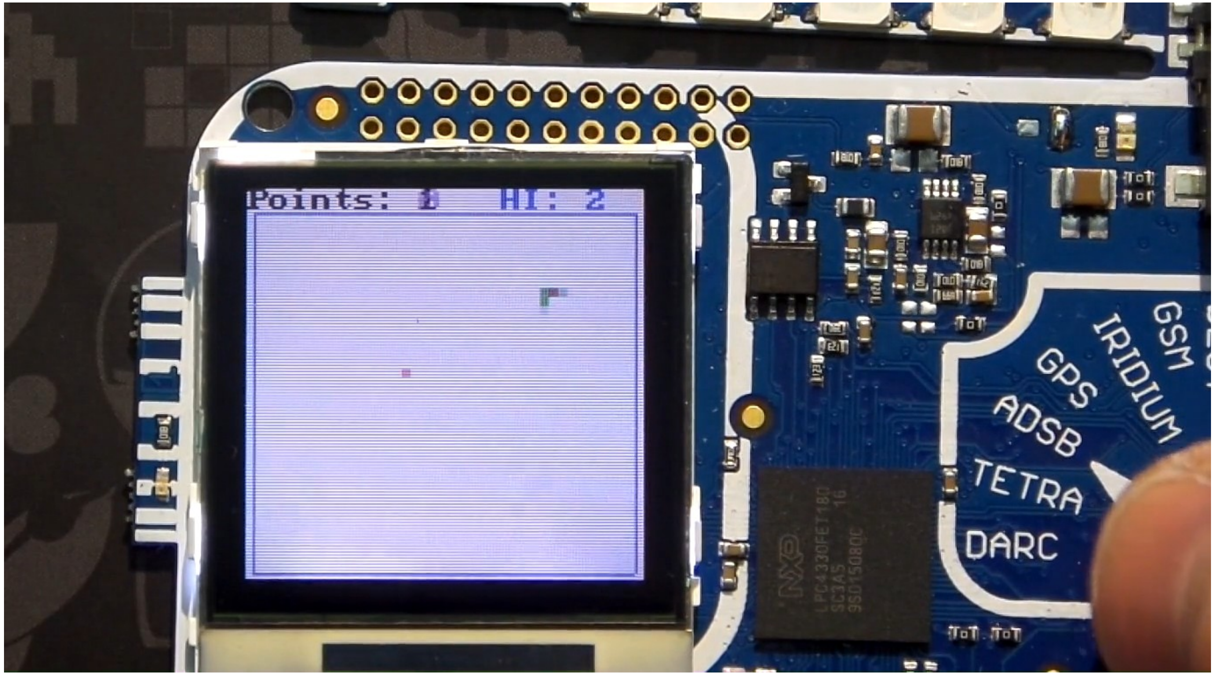
- 0xb
- snake
- tetris
- invaders
- bricks
- cube
- mandel
- fire
- schedule
- wobbel
- sysinfo

l0dable: 0xb

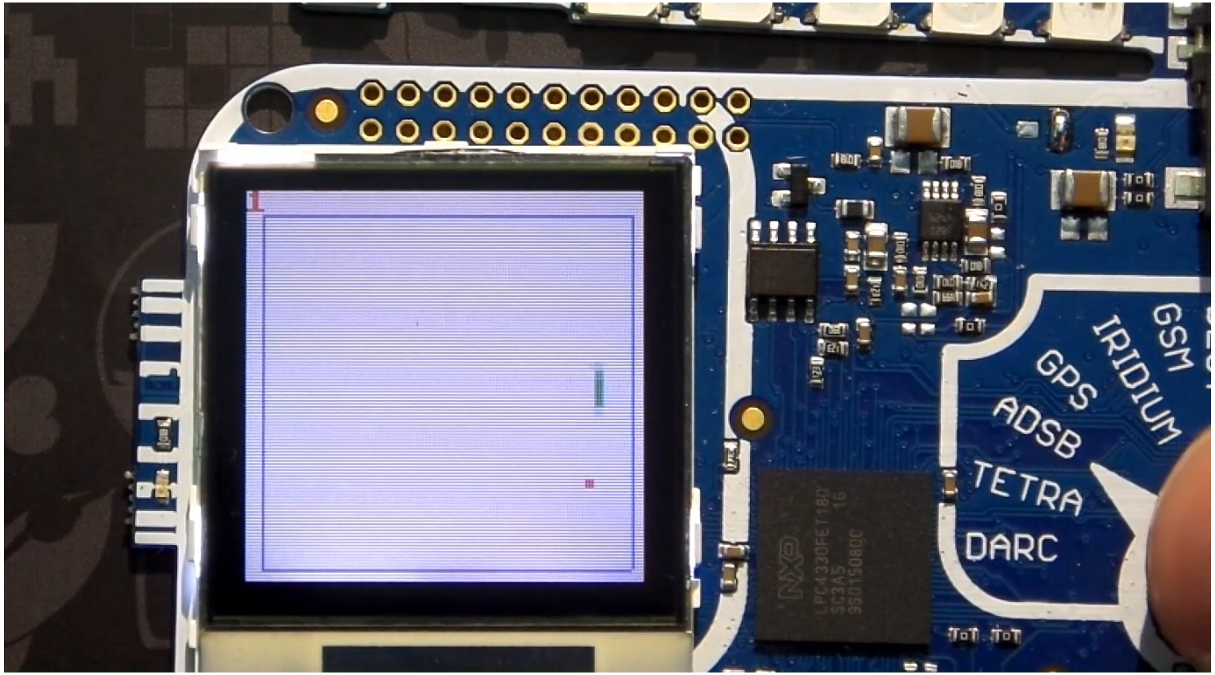


```
0xb number game
Push < > ^ v
Add same blocks
Try to reach 'b'!

>>  play!
    clear
    font
    width = 4
    height = 4
    quit
```

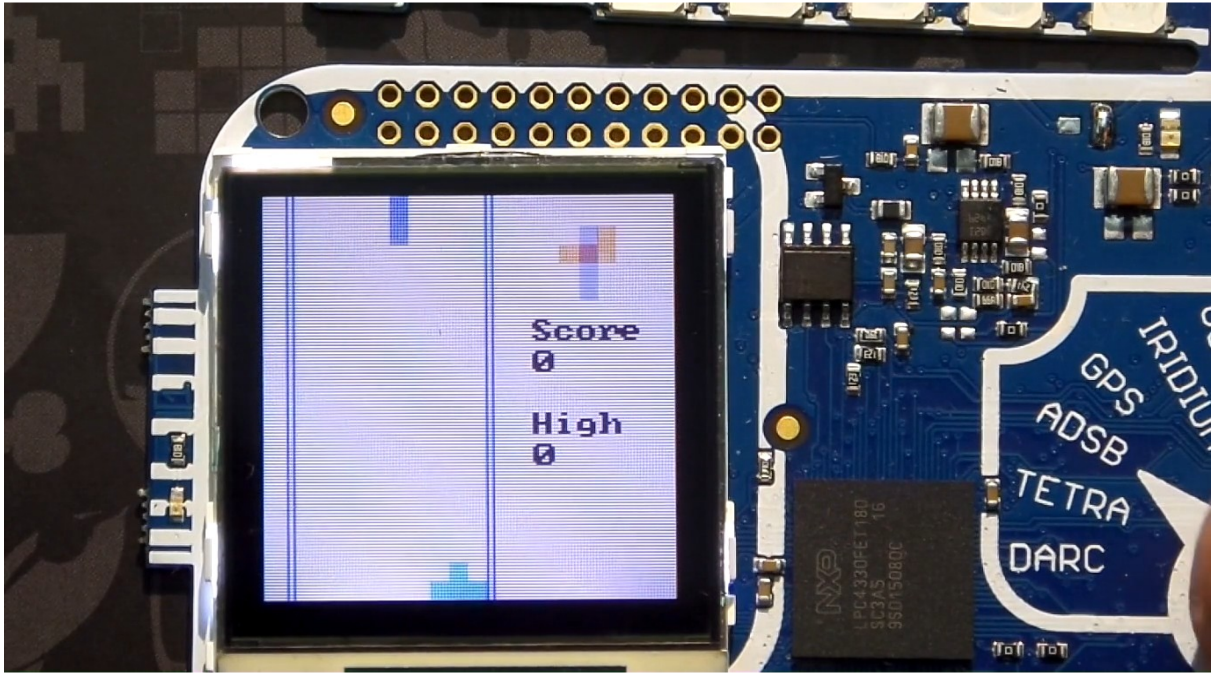
l0dable: snake1



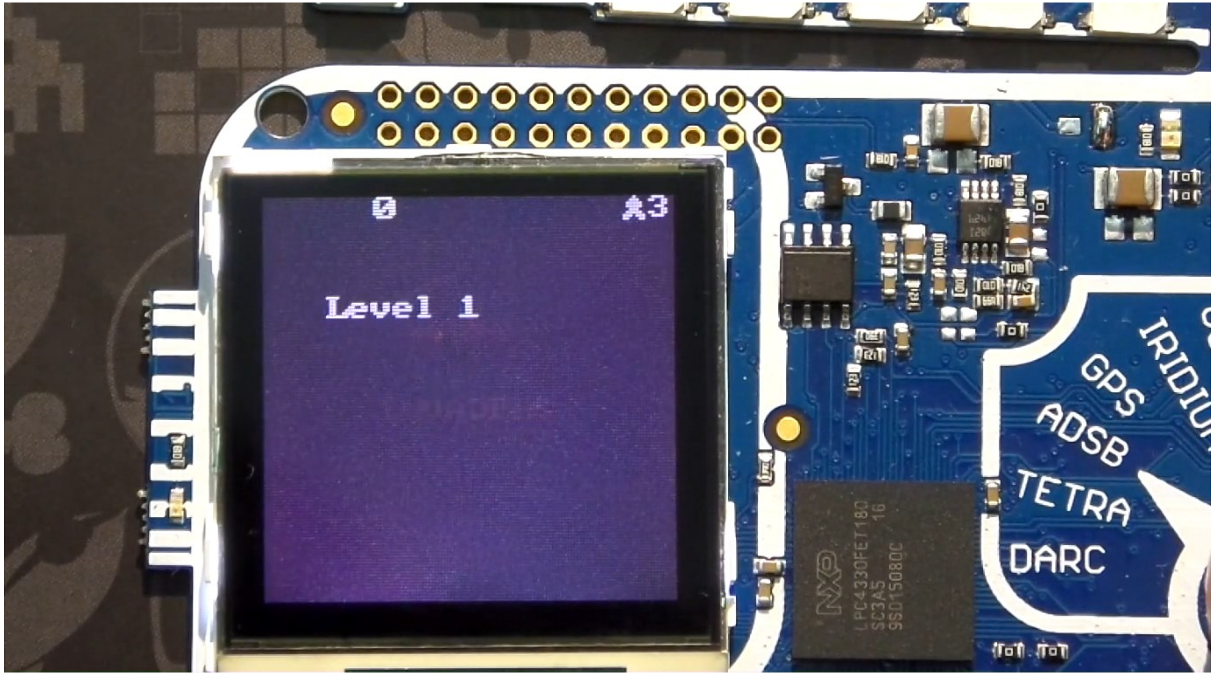
l0dable: snake2



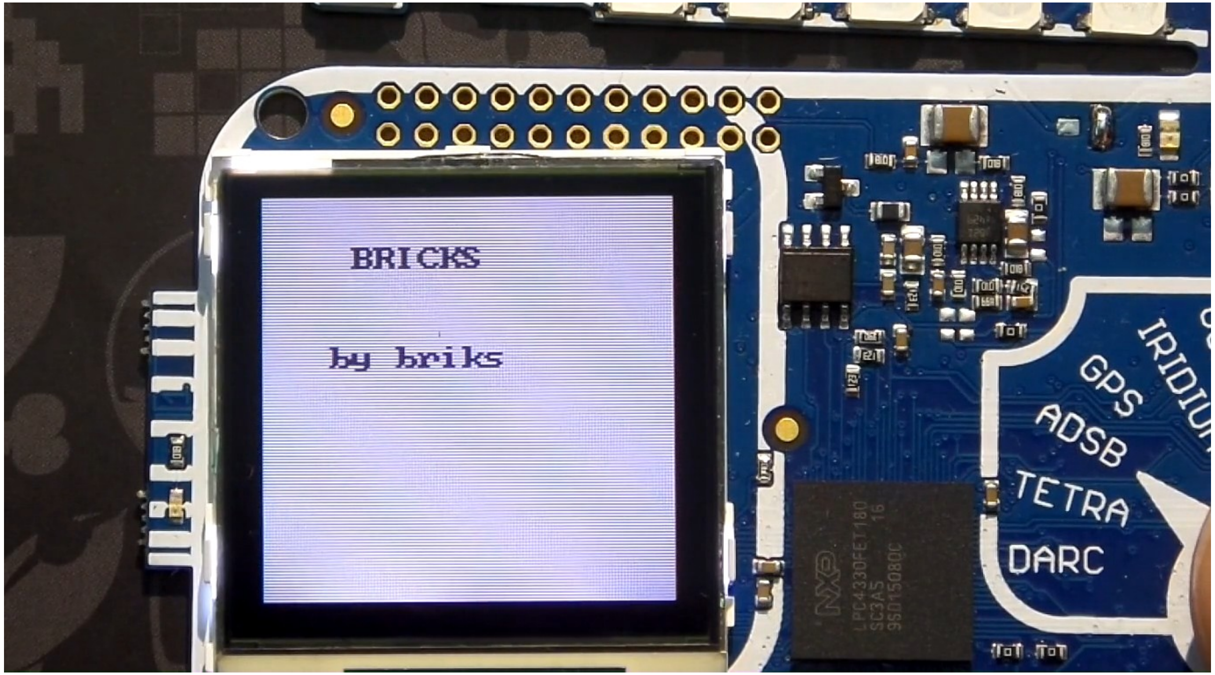
l0dable: tetris



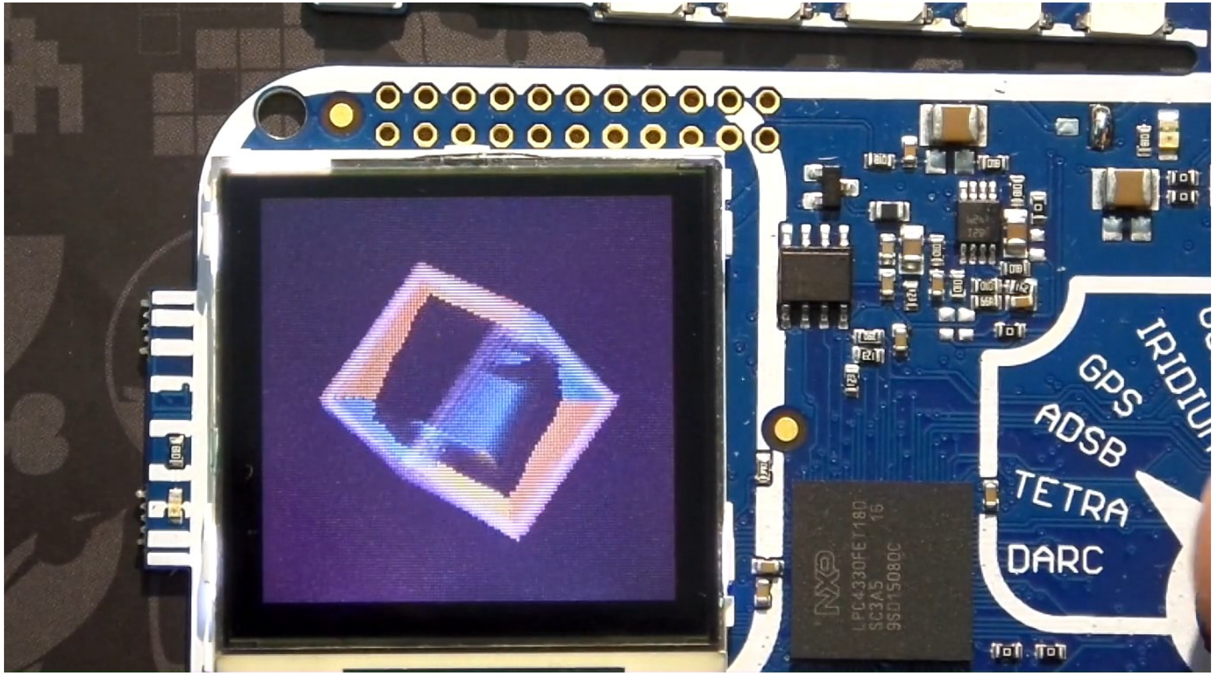
l0dable: invaders



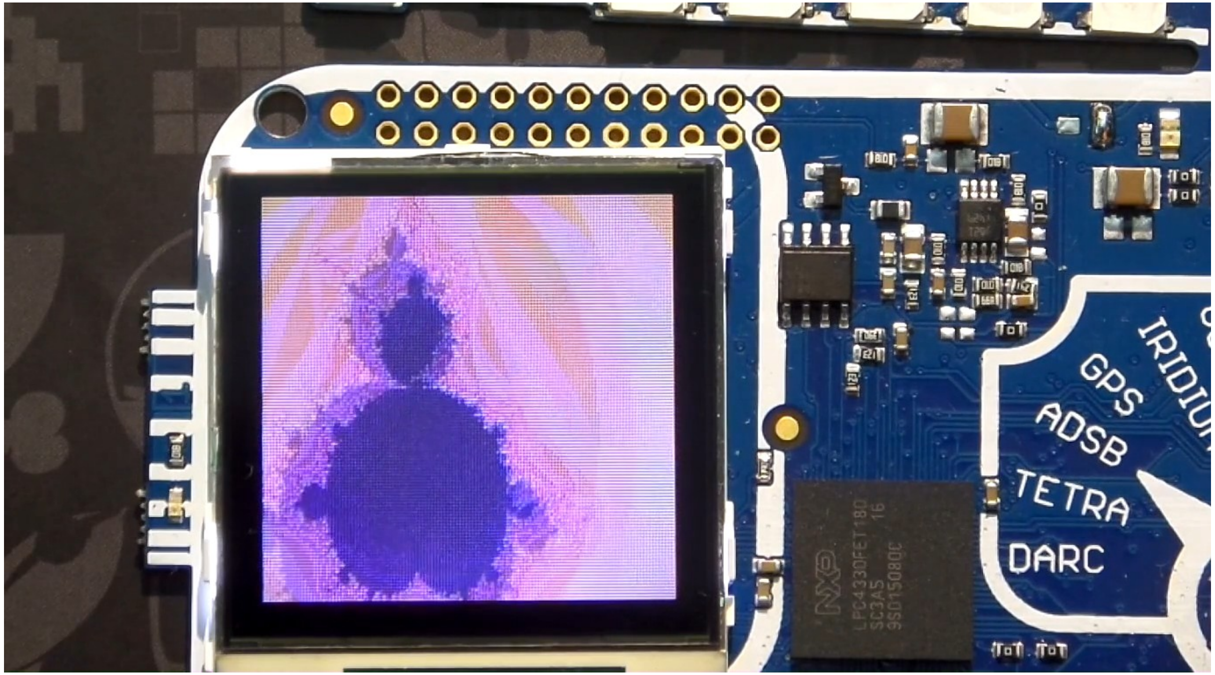
l0dable: bricks



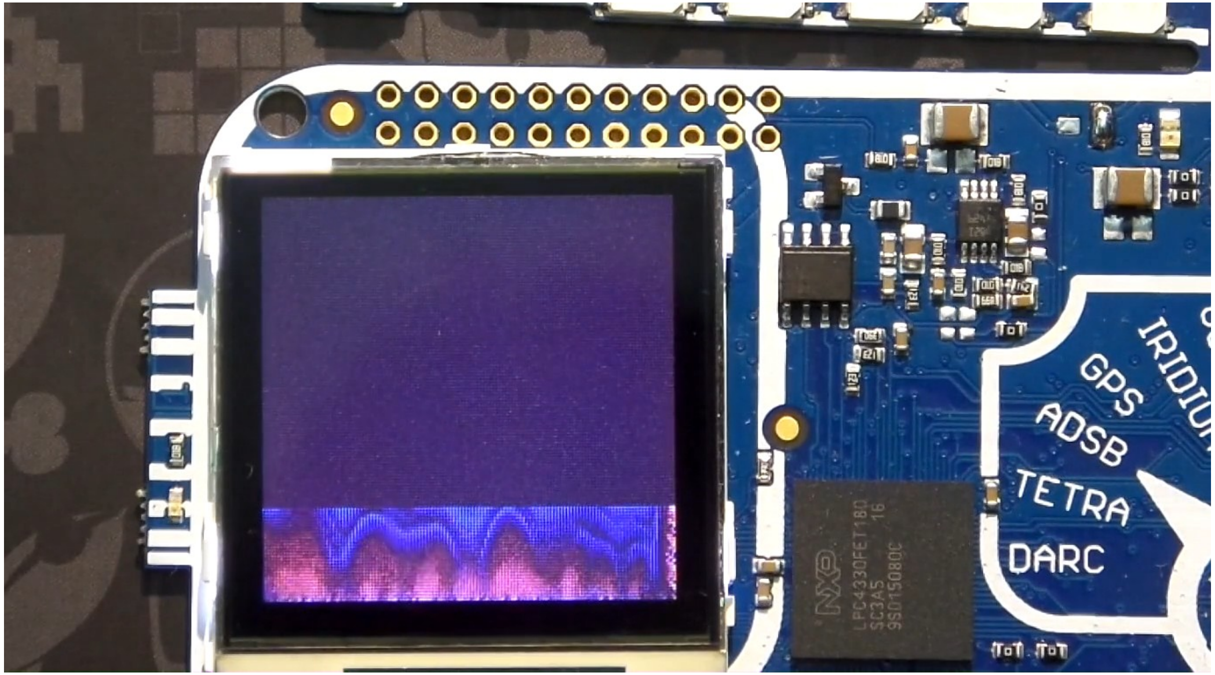
l0dable: cube



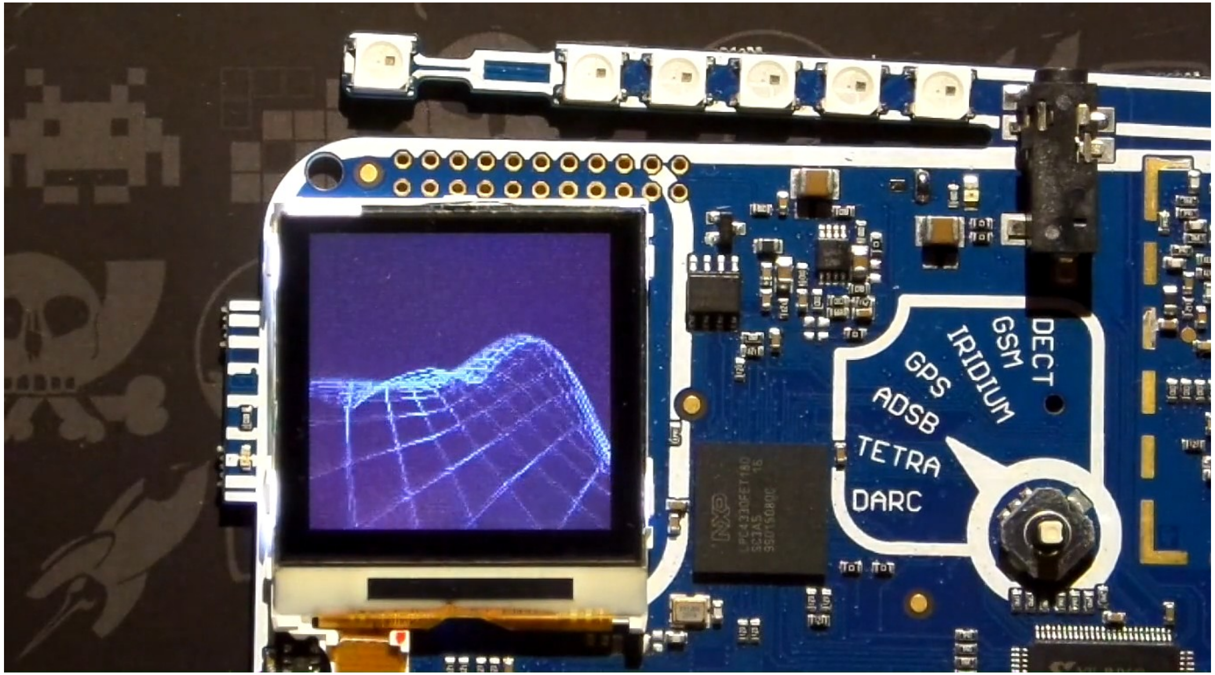
l0dable: mandel



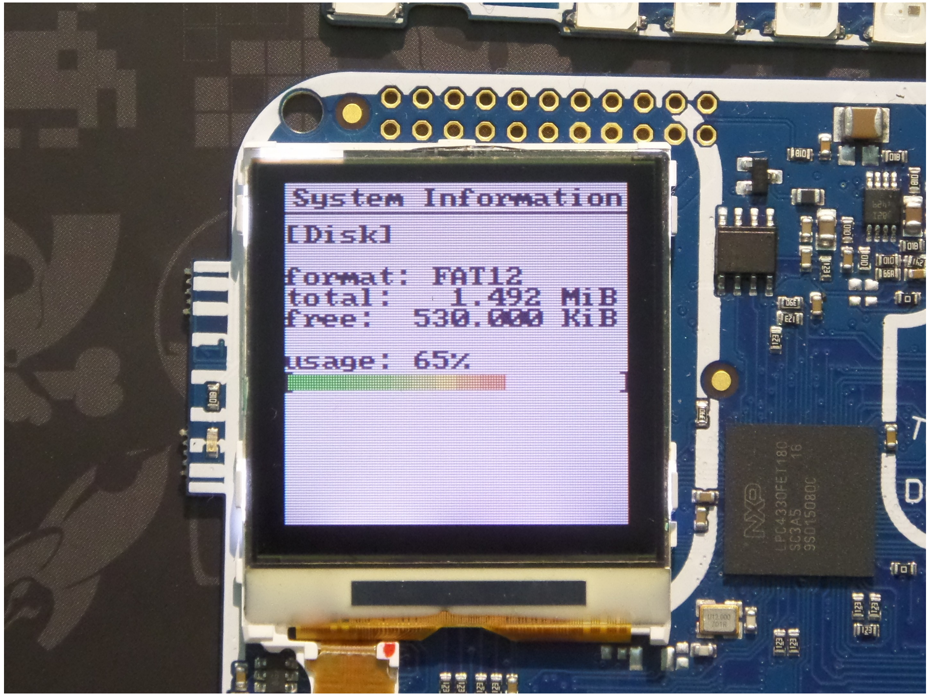
l0dable: fire



l0dables: wobbel

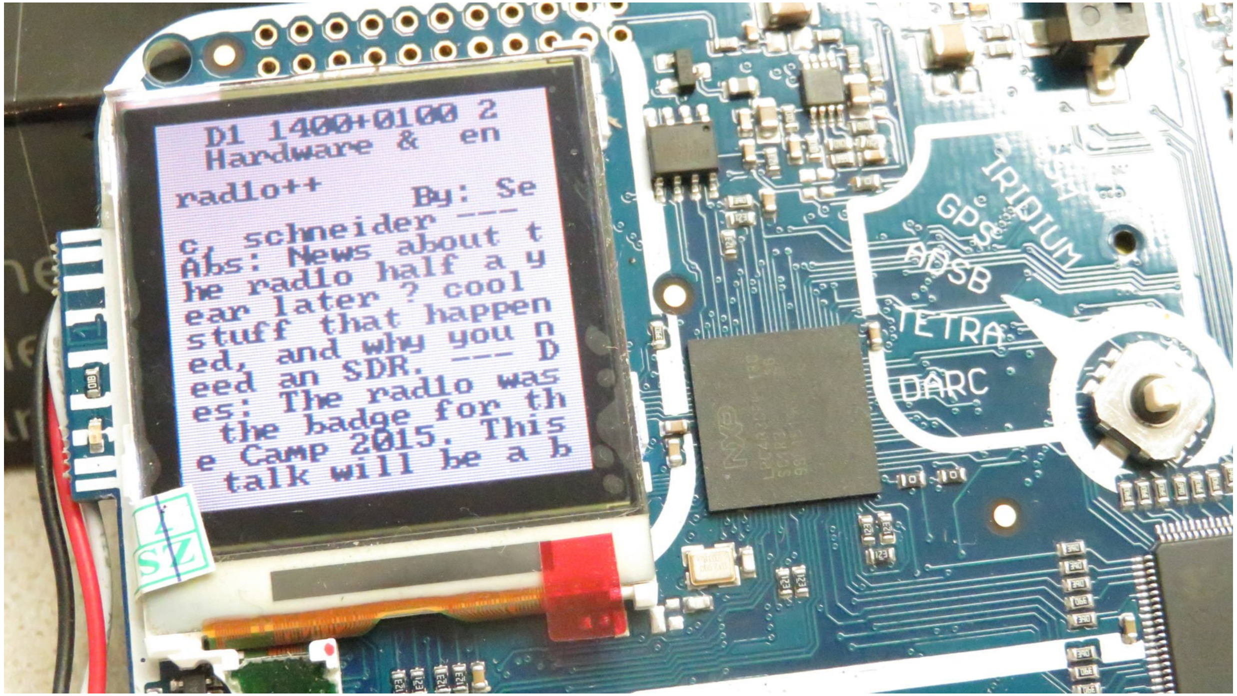


l0dables: sysinfo



```
System Information
[Disk]

format: FAT12
total:    1.492 MiB
free:   530.000 KiB

usage: 65%
```

l0dable: schedule



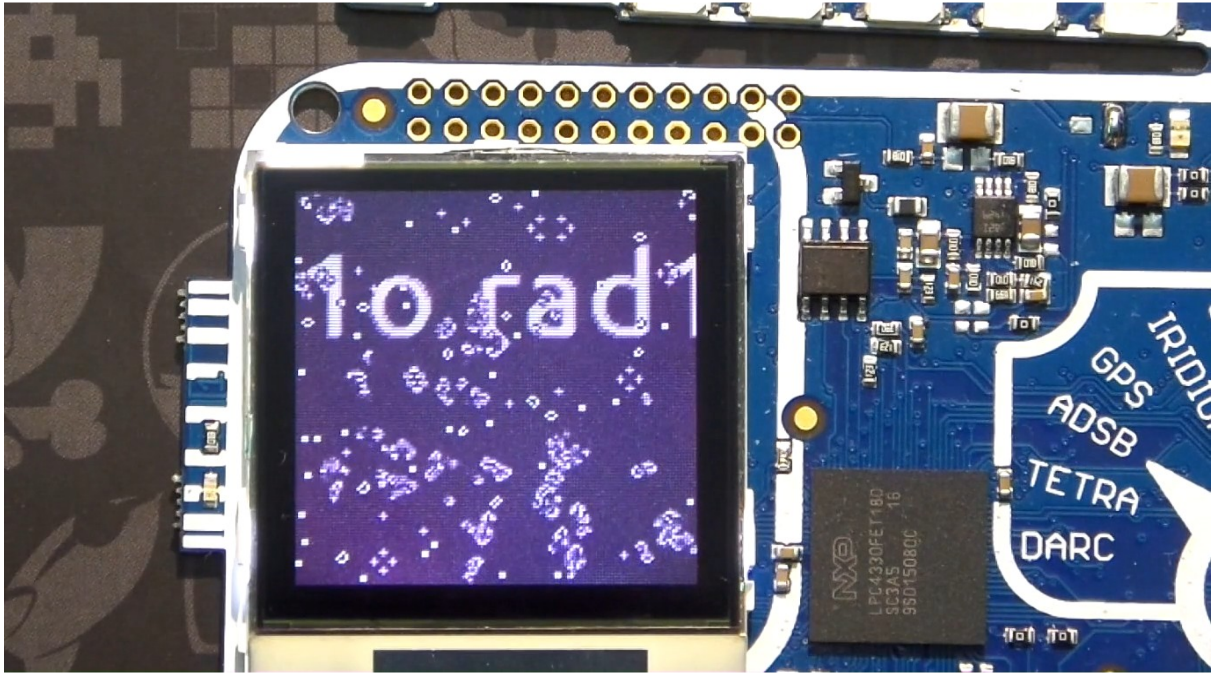
```
D1 1400+0100 2
Hardware &  en
rad1o++      By: Se
c. schneider ---
Abs: News about t
he rad1o half a y
ear later ? cool
stuff that happen
ed, and why you n
eed an SDR. --- D
es: The rad1o was
 the badge for th
e Camp 2015. This
 talk will be a b
```

Check under software in the rad1o Wiki for the 32C3 data file
Also available on the flash station at the assembly

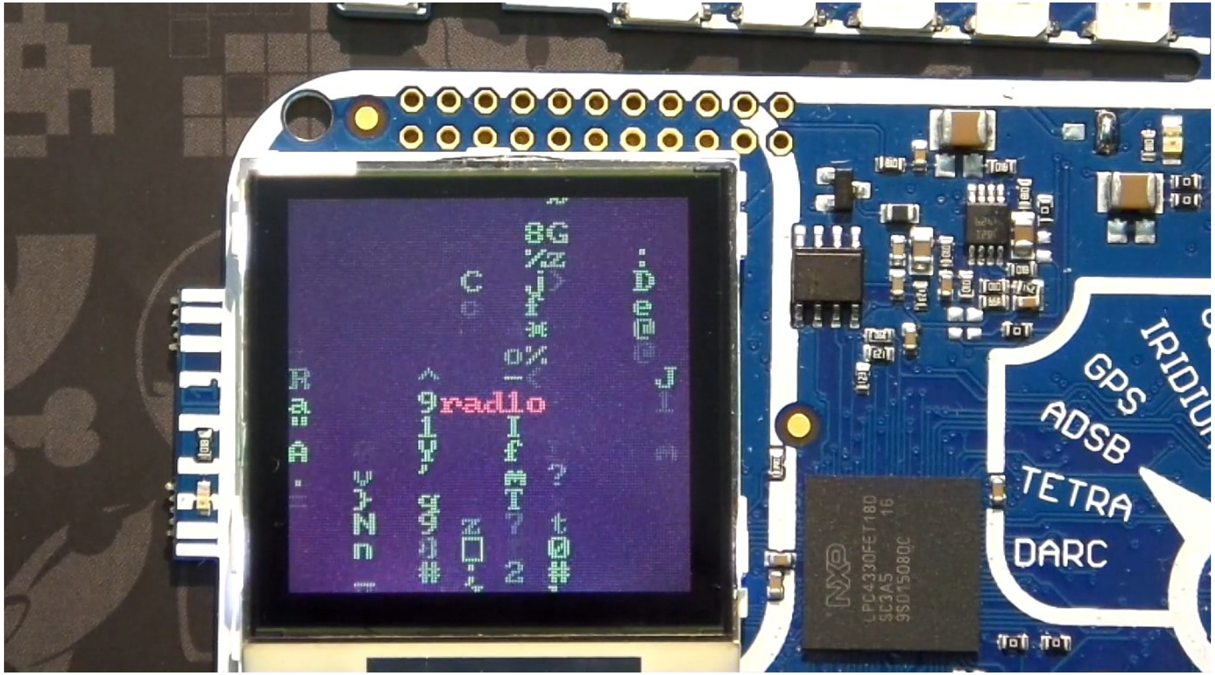
f1rmware: n1ck animations

- life
- matrix
- w0rpcore
- Netz39
- colplasm

- n1ck: life

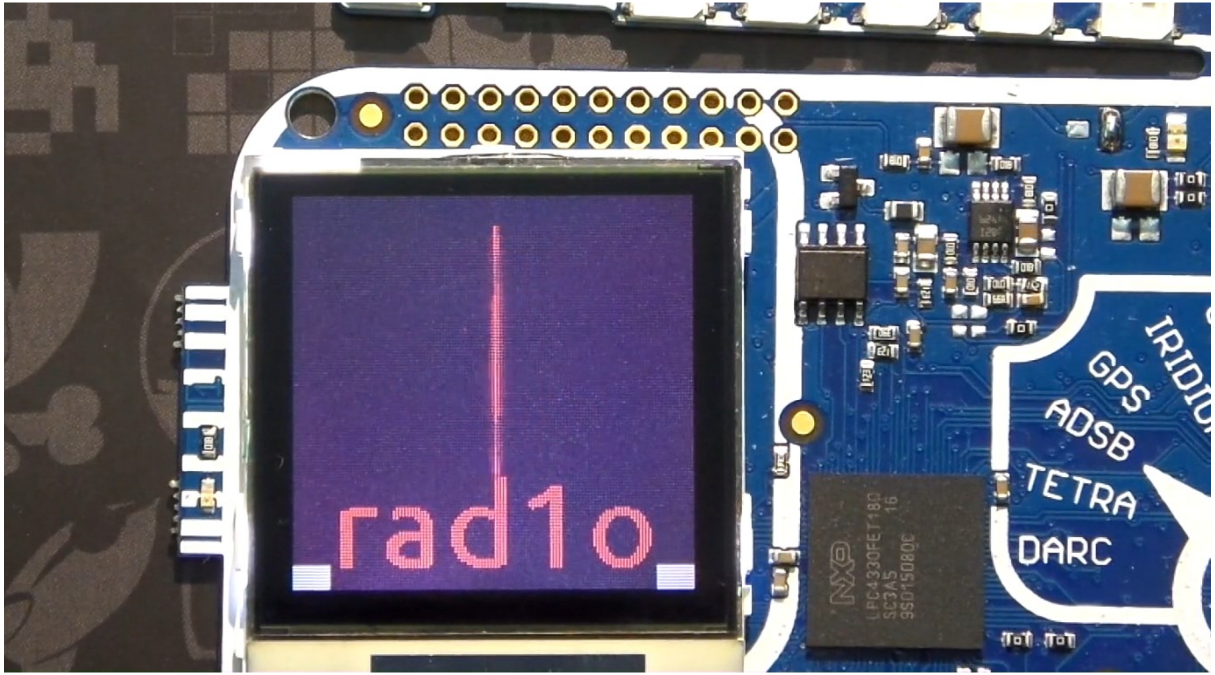


- n1ck: matrix

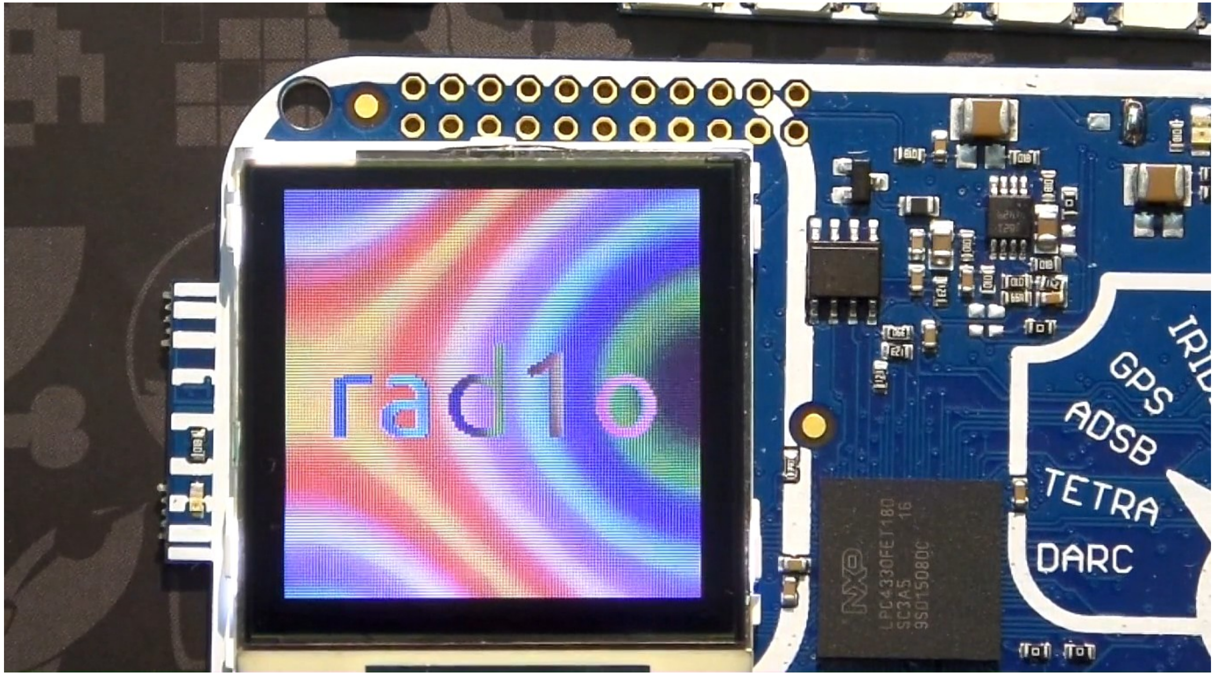


- n1ck: w0rpcore

- n1ck: netz39

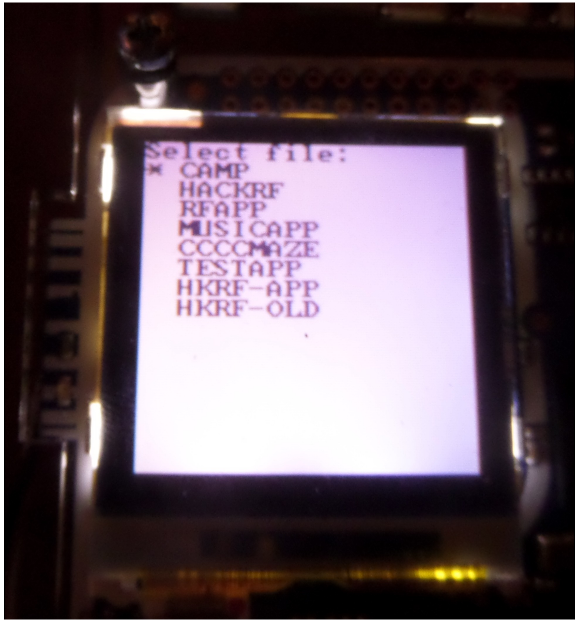

rad1o
IRIDIUM
GPS
ADSB
TETRA
DARC
NXP
LPC4330FET180
SC3A5 16
9SD15080C

- n1ck: colplasm



f1rmware: applications

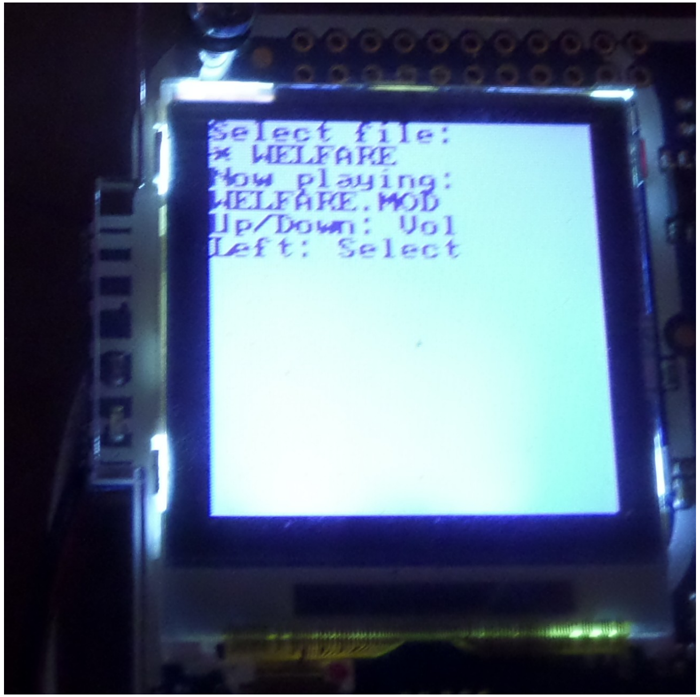
- Pull the joystick left while turning on
- Press enter to set the boot default
- Press right to boot the application once



```
Select file:
* CAMP
  HACKRF
  RFAPP
  MUSICAPP
  CCCCMAZE
  TESTAPP
  HKRF-APP
  HKRF-OLD
```

application: music

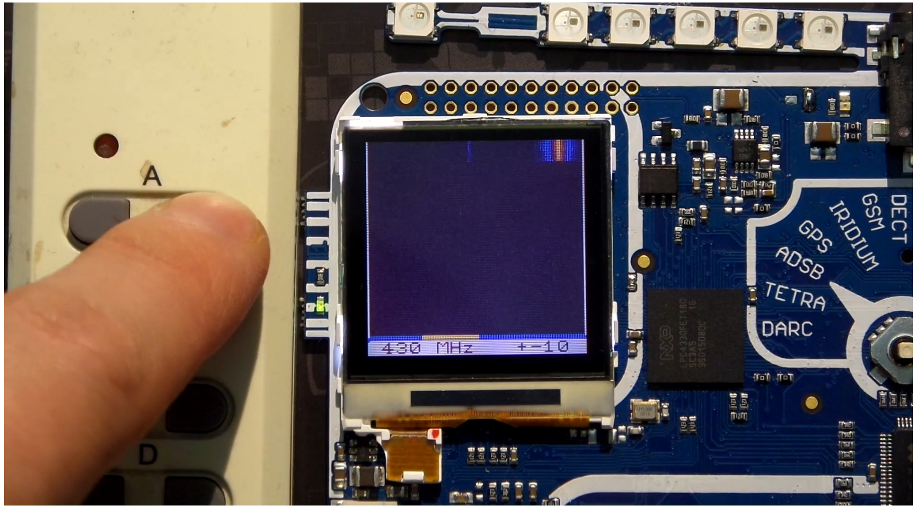
- Plays MOD files
- Uses an audio library based on the Repetitive Interrupt Timer of the LPC4330



```
Select file:
* WELFARE
Now playing:
WELFARE.MOD
Up/Down: Vol
Left: Select
```

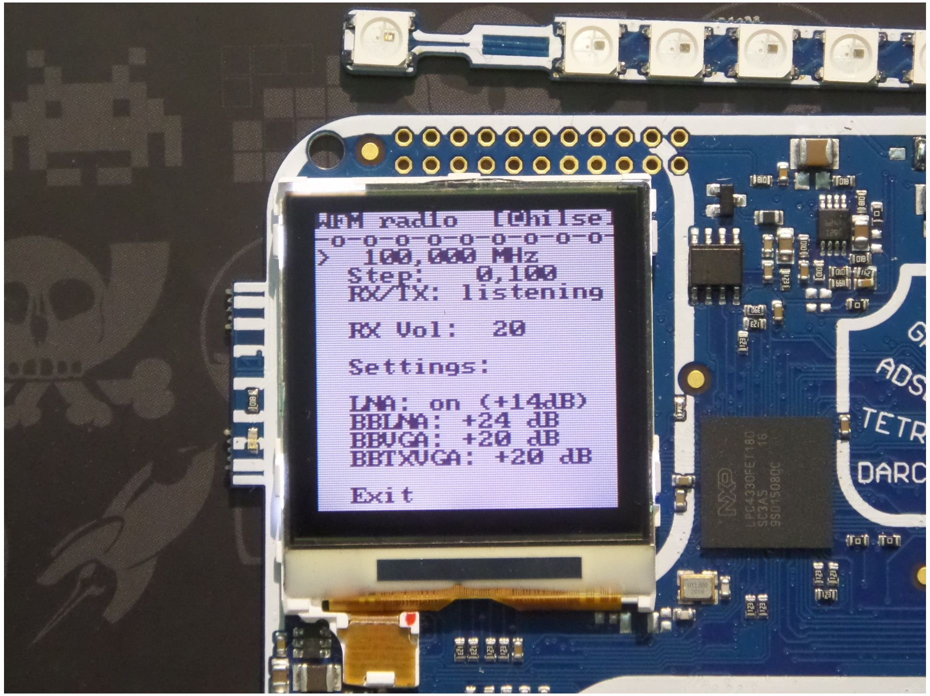
Application: rfapp

- scope
  - Shows an RF waterfall
  - Selectable frequency
  - Selectable timescale
  - Bandwidth: 2 MHz



Application: rfapp

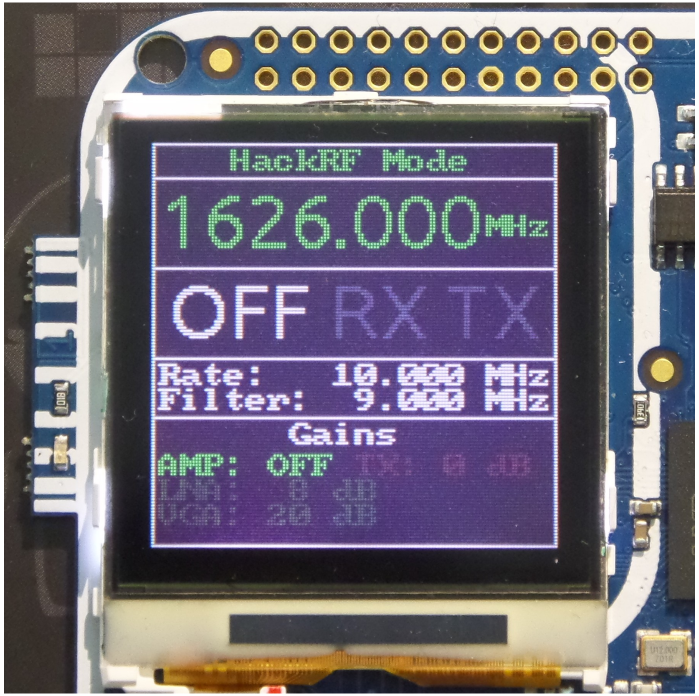
- FM Receiver / Transmitter
  - Wideband FM
  - Push to talk
  - Thanks to @hilse



```
WFM radio  [@hilse]
-o-o-o-o-o-o-o-o-o-
>  100,000 MHz
   Step:    0,100
   RX/TX: listening

   RX Vol:  20

   Settings:

   LNA: on (+14dB)
   BBLNA: +24 dB
   BBVGA: +20 dB
   BBTXVGA: +20 dB

   Exit
```

Application: HackRF

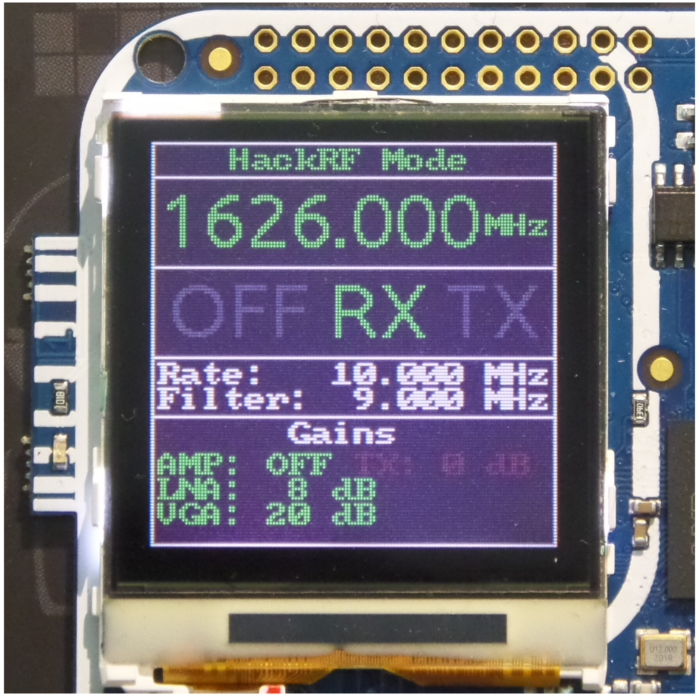
- Status display
- Choose hckrf-app



```
HackRF Mode
1626.000MHz
OFF RX TX
Rate:     10.000 MHz
Filter:    9.000 MHz
Gains
AMP:  OFF  TX:  0 dB
LNA:   0 dB
VGA:  20 dB
```

Application: HackRF

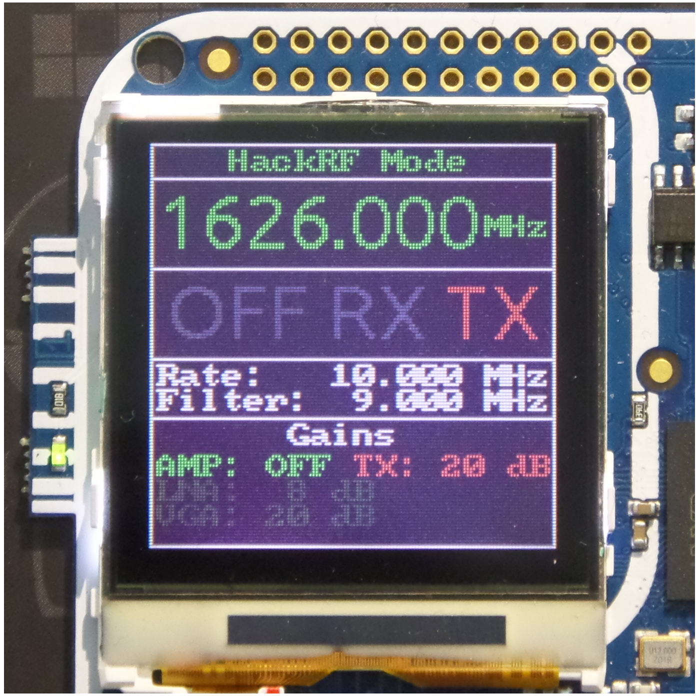
- Status display
- Choose hckrf-app



```
HackRF Mode
1626.000MHz
OFF RX TX
Rate:     10.000 MHz
Filter:    9.000 MHz
Gains
AMP:  OFF  TX:  0 dB
LNA:   8 dB
VGA:  20 dB
```

Application: HackRF

- Status display
- Choose hckrf-app



```
HackRF Mode
1626.000MHz
OFF RX TX
Rate:     10.000 MHz
Filter:    9.000 MHz
Gains
AMP:  OFF TX:  20 dB
LNA:   8 dB
VGA:  20 dB
```

l1braries: rflib

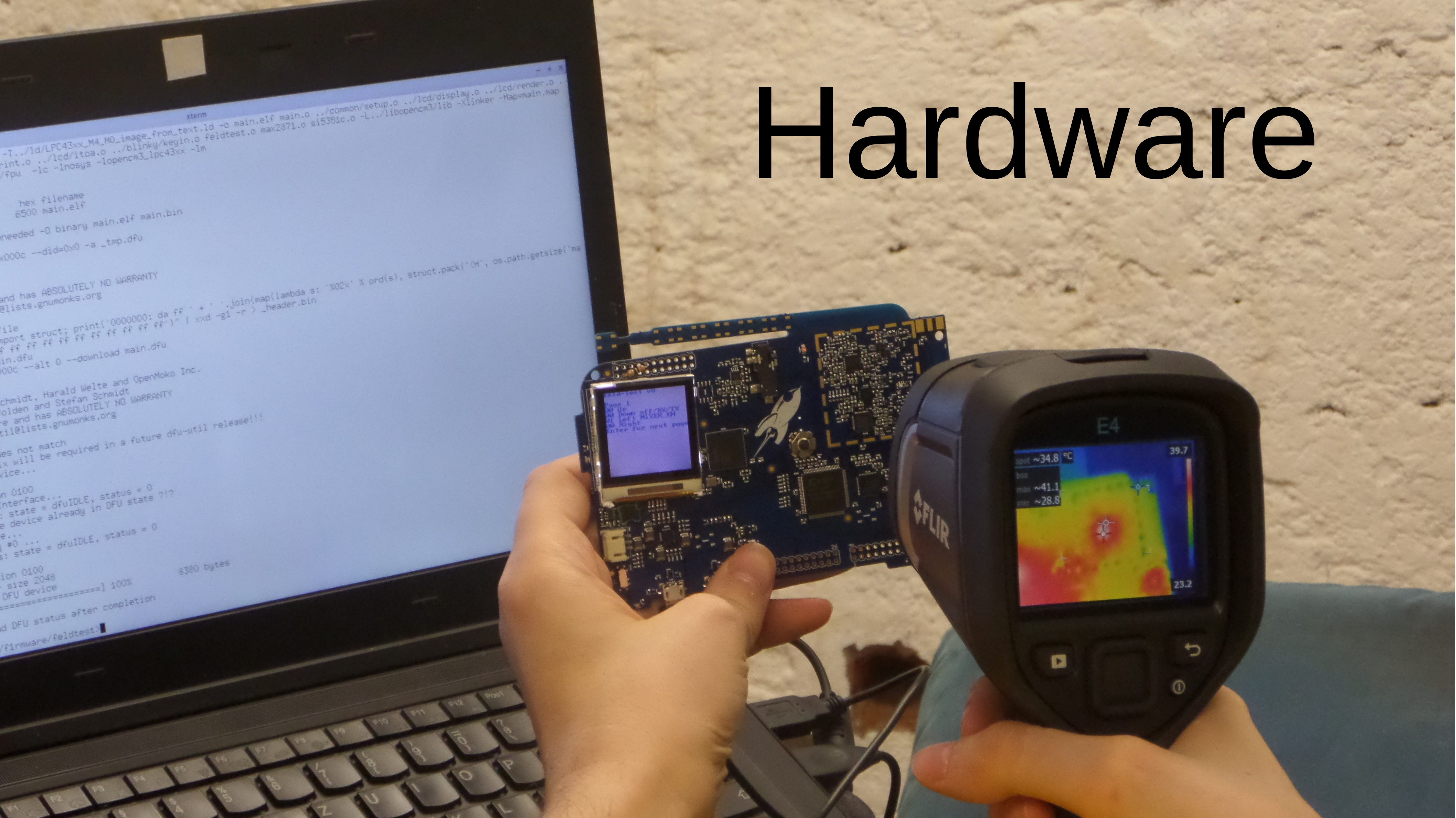
- Easier access to the RF parts from the f1rmware
- Offloads some SDR processing to the M0 core
- BFSK modulation already implemented on the M0
- Kudos to @hilse

```
rflib_init()
rflib_set_freq(2490000000)
len = rflib_bfsk_get_packet
           (rx_pkg, 255)
rflib_bfsk_transmit
           (len, data, true)
rflib_shutdown()

rflib_display()
```

Goals: SDR

- Upstreaming the rad1o changes to the HackRF code
- SD-Card ↔ RF: Listen and replay
  - Some SD-Card support available from @hilse

Hardware

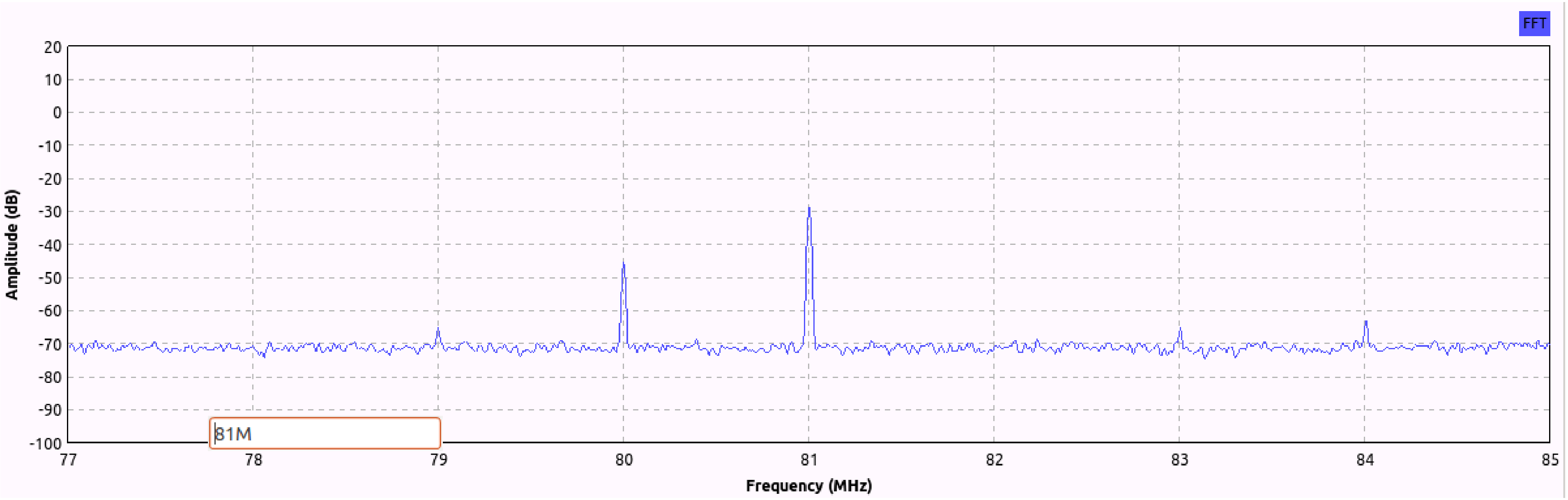


```
-T../ld/LPC43xx_M4_M0_image_from_text.ld -o main.elf main.o ../common/setup.o ../lcd/display.o ../lcd/render.o .
rint.o ../lcd/itoa.o ../blinky/keyin.o feldtest.o max2871.o si5351c.o -L../libopencm3/lib -Xlinker -Map=main.map
/fpu  -lc -lnosys -lopencm3_lpc43xx -lm


  hex filename
 6500 main.elf

needed -O binary main.elf main.bin

x000c --did=0x0 -a _tmp.dfu


and has ABSOLUTELY NO WARRANTY
@lists.gnumonks.org

ile
mport struct; print('0000000: da ff ' + ' '.join(map(lambda s: '%02x' % ord(s), struct.pack('<H', os.path.getsize('ma
f ff ff ff ff ff ff ff ff ff')" | xxd -g1 -r > _header.bin
in.dfu
00c --alt 0 --download main.dfu

chmidt, Harald Welte and OpenMoko Inc.
olden and Stefan Schmidt
e and has ABSOLUTELY NO WARRANTY
til@lists.gnumonks.org

es not match
x will be required in a future dfu-util release!!!
vice...

n 0100
interface...
: state = dfuIDLE, status = 0
e device already in DFU state ?!?
e...
 #0 ...
s: state = dfuIDLE, status = 0

ion 0100
 size 2048                        8380 bytes
 DFU device
===================] 100%
==================== 
d DFU status after completion

/firmware/feldtest>
```

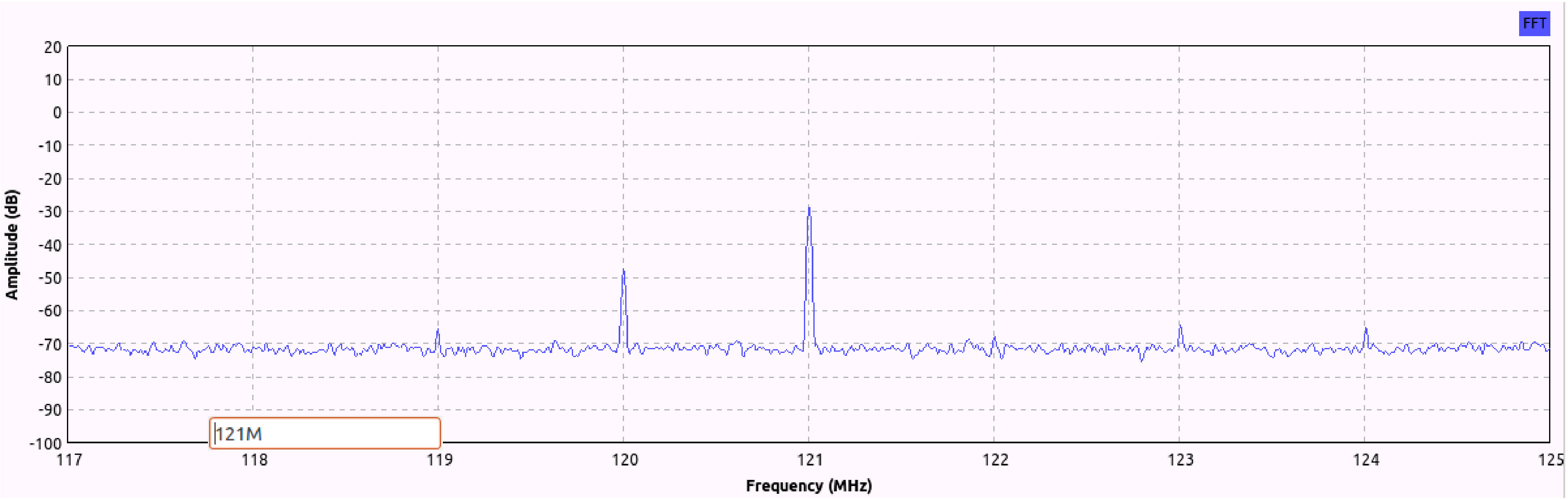
Known Issues: Interferences

- Caused by the various clock signal
  - Sample clock: 2 MHz to 20 MHz
  - Sample clock x2: 4 MHz to 40 MHz
  - Main CPU clock: 204 MHz
  - External clock output: 10 MHz
  - Base clocks for the PLLs: 40 MHz and 50 MHz
- Also at every harmonic of the base frequency
  - They get smaller with each repetition

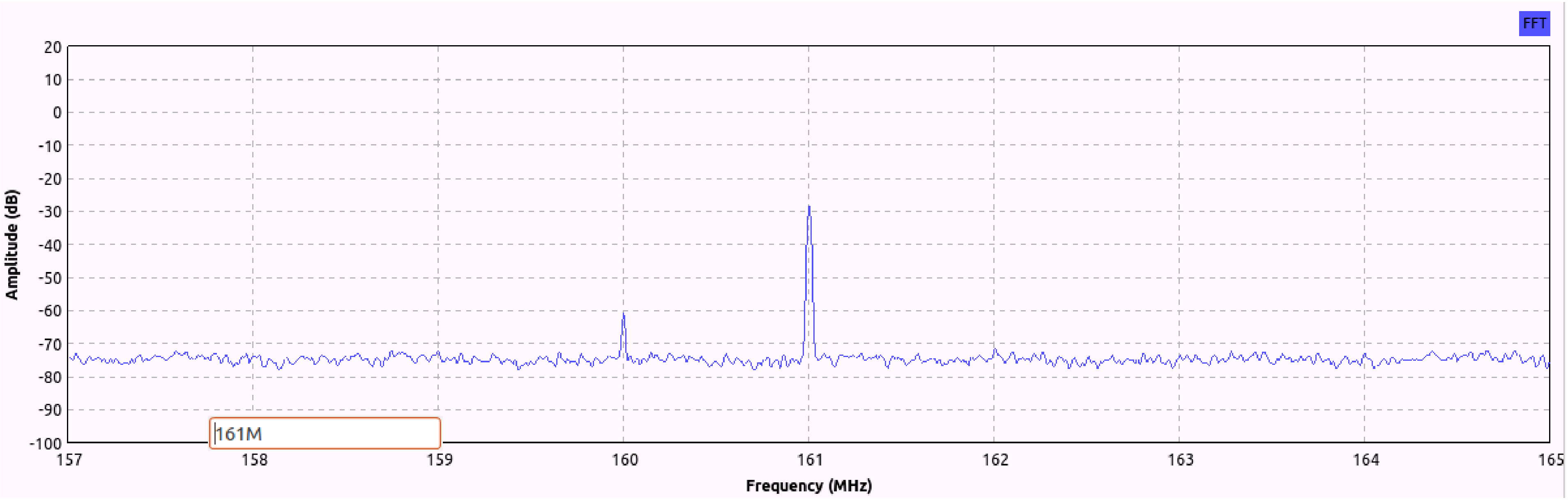
Known Issues: Interferences



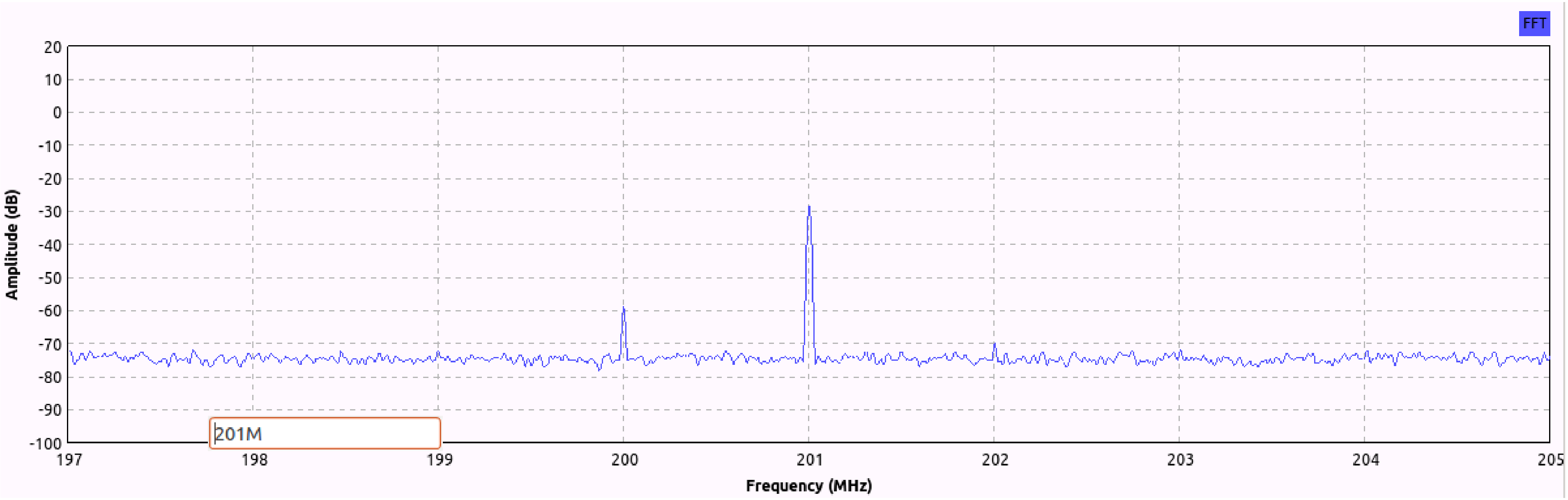
Known Issues: Interferences



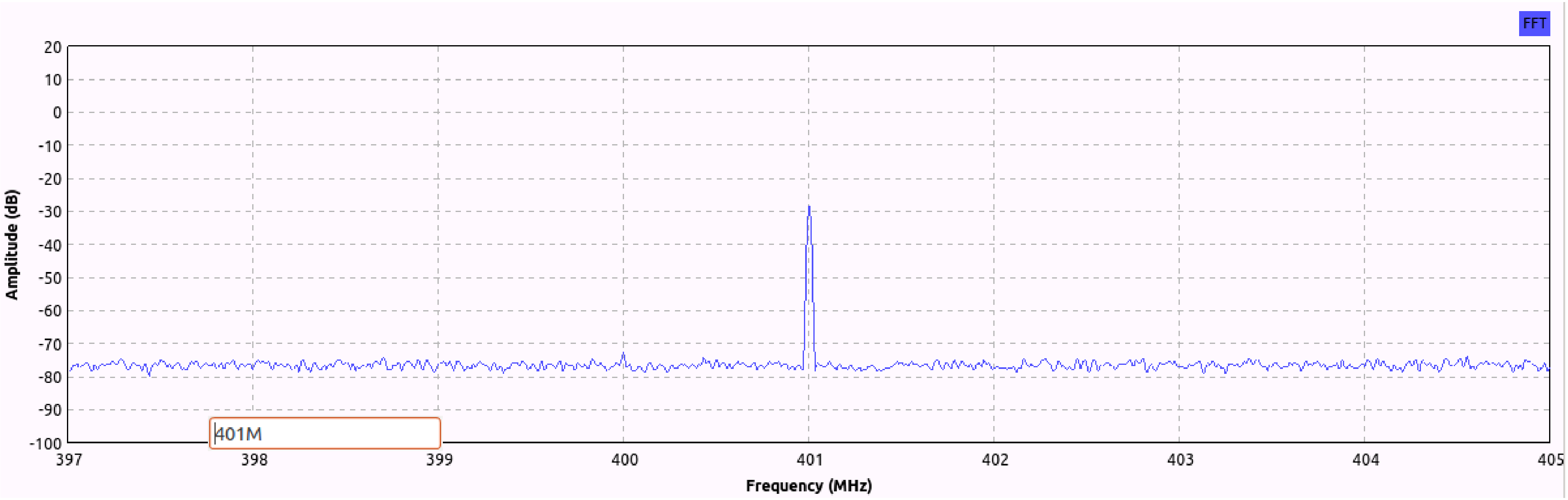
Known Issues: Interferences



Known Issues: Interferences

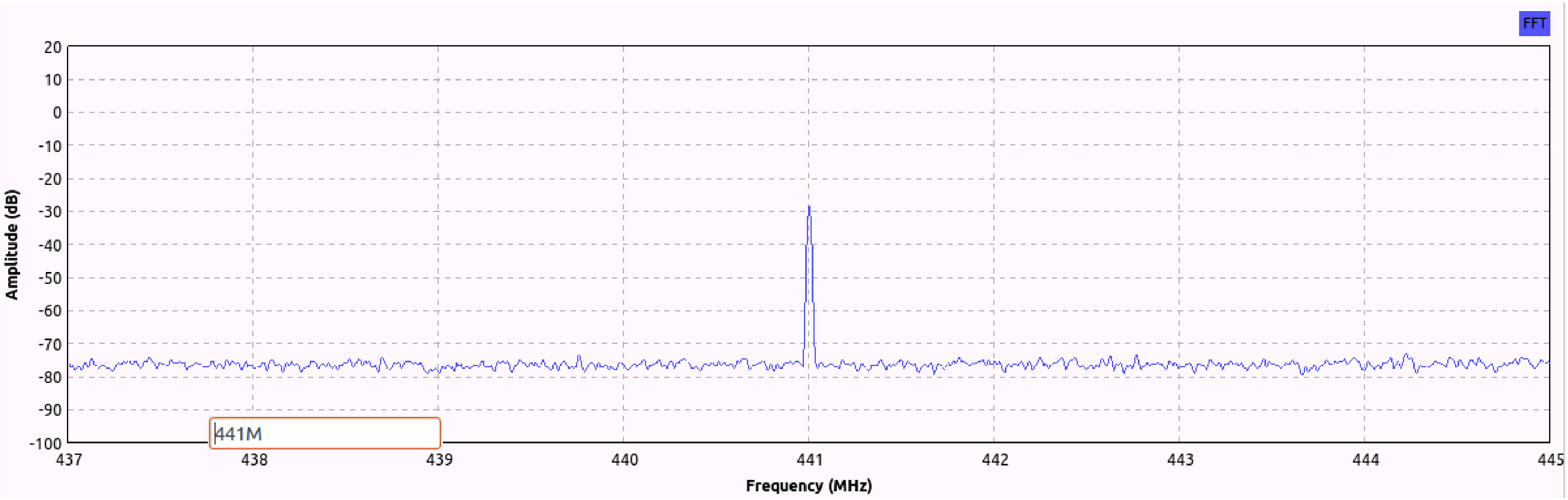


Known Issues: Interferences



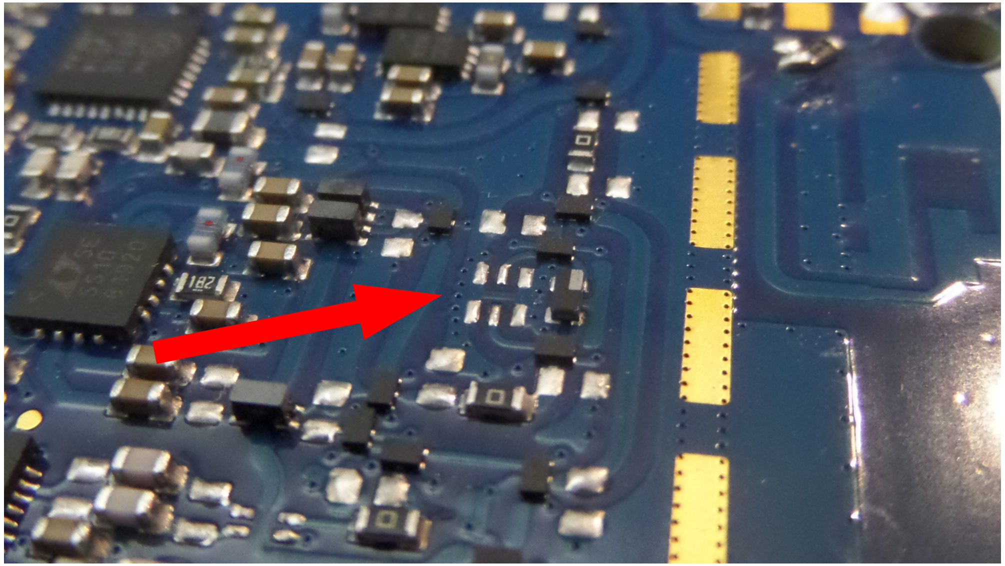
401M

Known Issues: Interferences



Known Issues: Missing High Pass

- There is no high pass populated (FL301)
  - Had to save cost

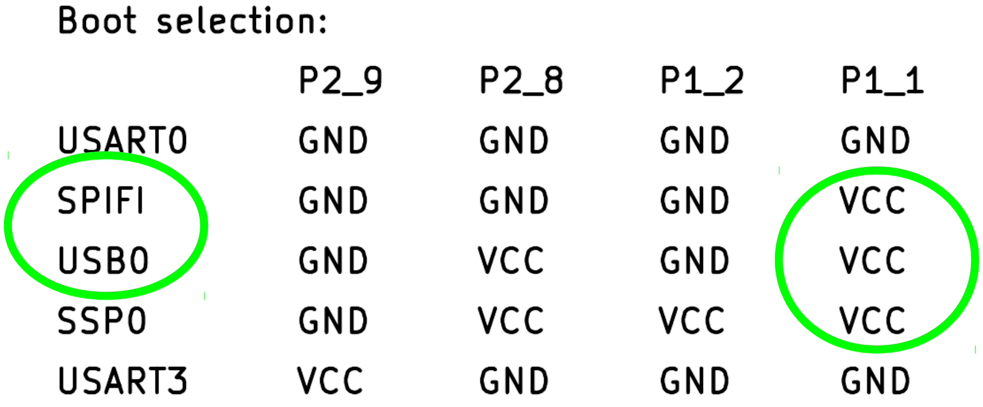


Known Issues: Missing High Pass

- RX/TX > 2.75 GHz is not possible without modifications
- Solutions
  - Populate the high pass
  - Bridge the high pass and add an external filter
- For RX, a bridge on the high pass should be OK

Known Issues: Backlight Stays On

- Caused by a pull-up on LCD_BL_EN
  - LCD_BL_EN is on P1_1 which selects the boot mode
- Not an easy fix
  - Pulling the signal low will prevent boot up
  - Unplug the battery when not used



Boot selection:

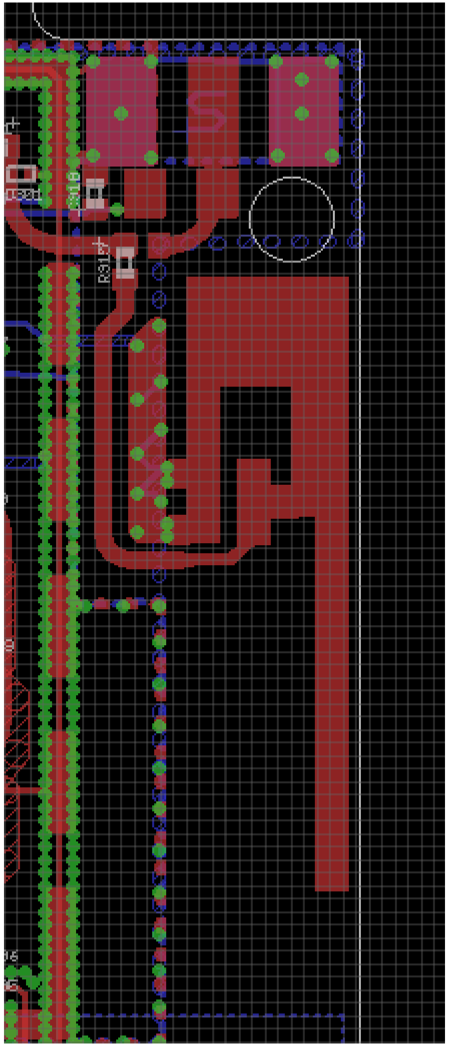
	P2_9	P2_8	P1_2	P1_1
USART0	GND	GND	GND	GND
SPIFI	GND	GND	GND	VCC
USB0	GND	VCC	GND	VCC
SSP0	GND	VCC	VCC	VCC
USART3	VCC	GND	GND	GND

Known Issues: Antenna

- Idea: there is a bit of free space above WiFi in the 2.4 GHz ISM Band
  - 2.480 GHz to 2.500 GHz

- Measurements put the antenna at around 2.35 GHz :/

- Still quite OK between 2.4 GHz and 2.5 GHz



Known Issues: USB power

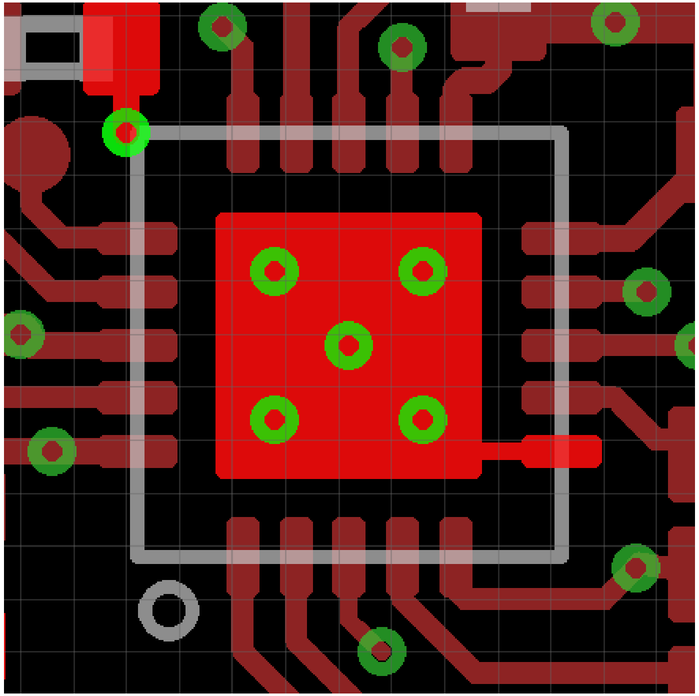
- First USB always takes precedence for the power supply
  - Draws up to 700 mA while transmitting

  → Can be a problem for Raspberry Pi etc.
- Second port is limited to 475 mA

- Solutions:
  - Patch HackRF to use the second port for data
  - Use/build a USB cable which has a separate connector for power

Known Issues: Clock Input

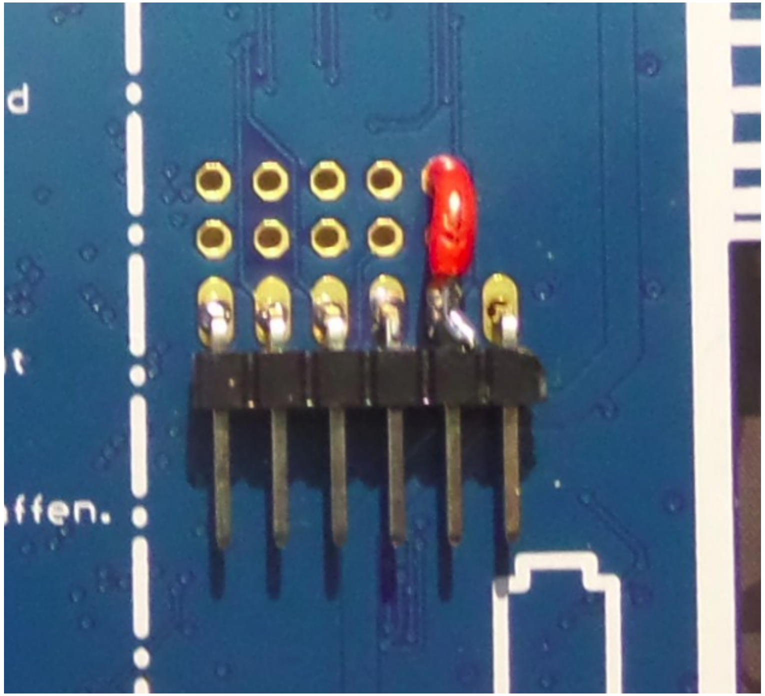
- One third of the badges have a clock generator with an external clock input
- But: The corresponding pin is always connected to ground
- The only way to input a clock is through the pads of the crystal



Known Issues: ISP Pin Floating

- The ISP pin is missing a pull-up
- May cause the rad1o to not boot
- Apparently not an issue, but the pin is very touchy

- Solution:
  - Pull the line high



Known Issues: Touchy Reset Pin

- Connecting anything will trigger a reset
- Although there is a 12 k pull-up
- Just be careful when adding anything to that pin

Maintenance: Typical Problems

- Broken display
  - You can get spares on ebay: Nokia 6100
  - We have a few with us at the assembly
  - r0ket displays won't work

Maintenance: Typical Problems

- Broken display
  - You can get spares on ebay: Nokia 6100
  - We have a few with us at the assembly
  - r0ket displays won't work
- No audio input / output
  - Check the solder joints on the connector
  - Rotate your headset a bit

Maintenance: Typical Problems

- Broken display
  - You can get spares on ebay: Nokia 6100
  - We have a few with us at the assembly
  - r0ket displays won't work
- No audio input / output
  - Check the solder joints on the connector
  - Rotate your headset a bit
- Bad power switch
  - Replace it with a jumper

Maintenance: Typical Problems

- Broken display
  - You can get spares on ebay: Nokia 6100
  - We have a few with us at the assembly
  - r0ket displays won't work
- No audio input / output
  - Check the solder joints on the connector
  - Rotate your headset a bit
- Bad power switch
  - Replace it with a jumper
- All working, but no data flowing
  - Check with another/shorter USB cable

Maintenance: Typical Problems

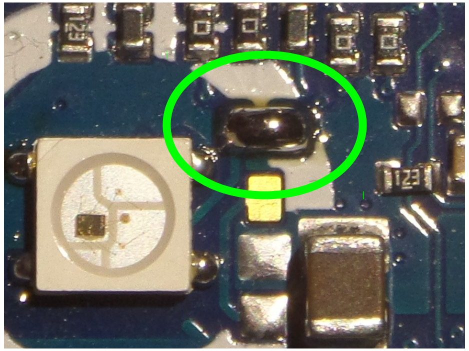
- Broken display
  - You can get spares on ebay: Nokia 6100
  - We have a few with us at the assembly
  - r0ket displays won't work
- No audio input / output
  - Check the solder joints on the connector
  - Rotate your headset a bit
- Bad power switch
  - Replace it with a jumper
- All working, but no data flowing
  - Check with another/shorter USB cable
- Display flickering
  - Charge your battery :)

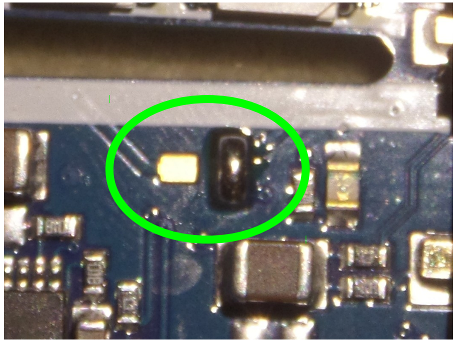
Maintenance: Typical Problems

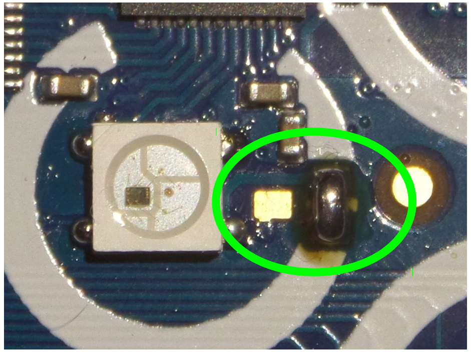
- Broken display
  - You can get spares on ebay: Nokia 6100
  - We have a few with us at the assembly
  - r0ket displays won't work
- No audio input / output
  - Check the solder joints on the connector
  - Rotate your headset a bit
- Bad power switch
  - Replace it with a jumper
- All working, but no data flowing
  - Check with another/shorter USB cable
- Display flickering
  - Charge your battery :)
- Data transfer to the file system takes very long
  - Yes it takes very long. Please wait and use the “Safe eject” feature of your OS (Linux: use 'sync').

Maintenance: RGB LEDs

- RGB LED power supply
  - Made a mistake in the layout
  - Made a mistake documenting it
  - Result: Lots of superstition out there
- The simple solution is perfectly fine:
  - Bridge two pads on each transistor
  - Check the Wiki

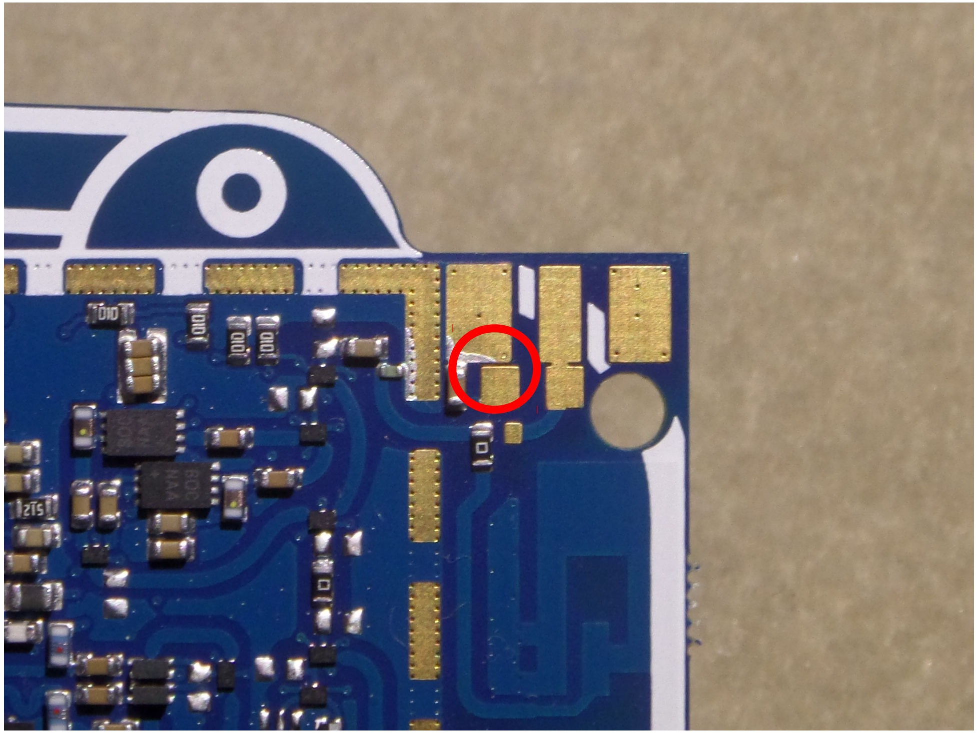






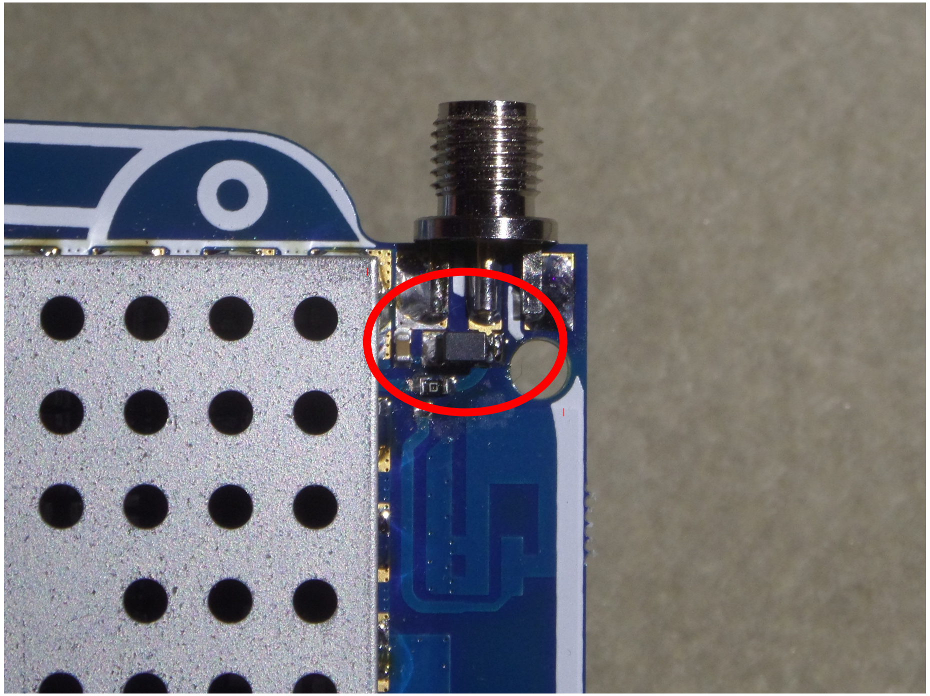
Maintenance: Antenna Connector

- Take care to not bridge these two pads



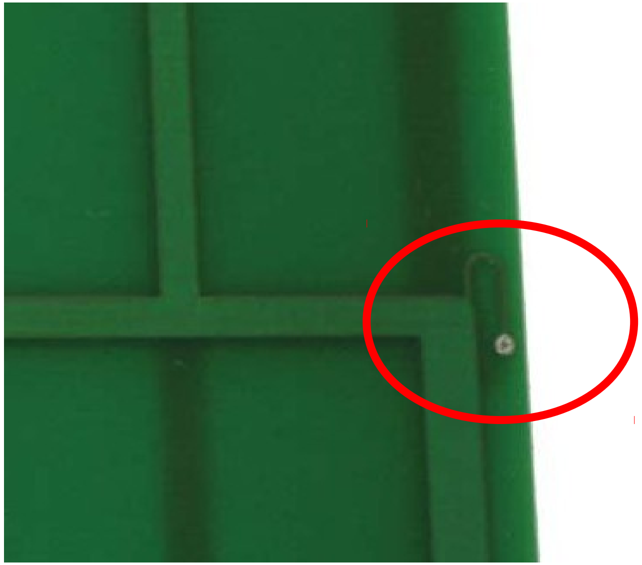
Maintenance: Bias-T

- Useful for active antennas
- The HackRF One can control it via SW
  - We had to save money and time
- Pads for a “large” inductor directly at the antenna



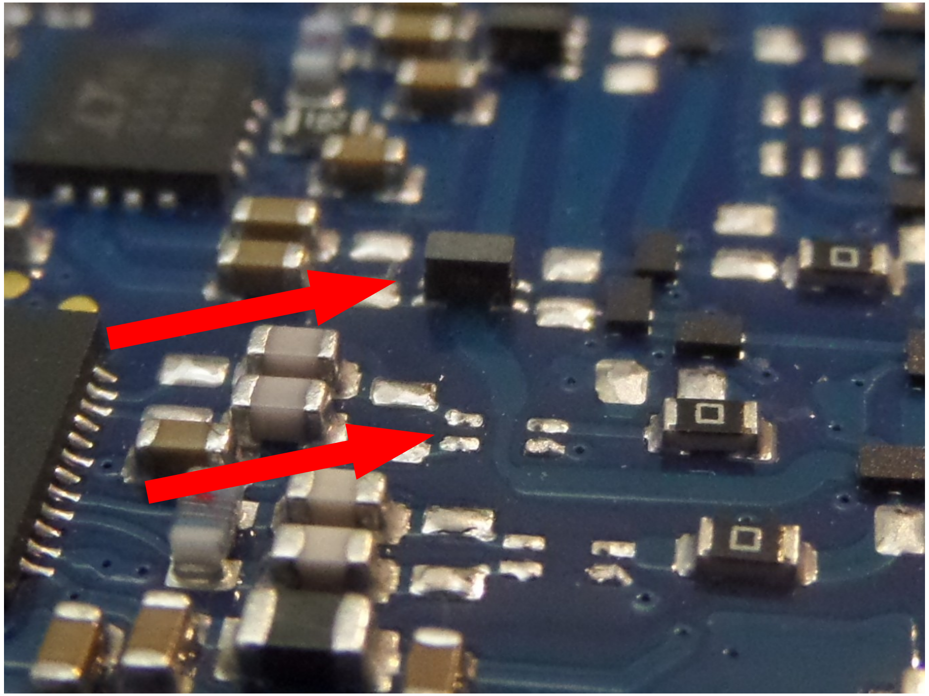
Maintenance: Bias-T

- Be careful if your antenna has a DC path!
  - It might burn out the inductor



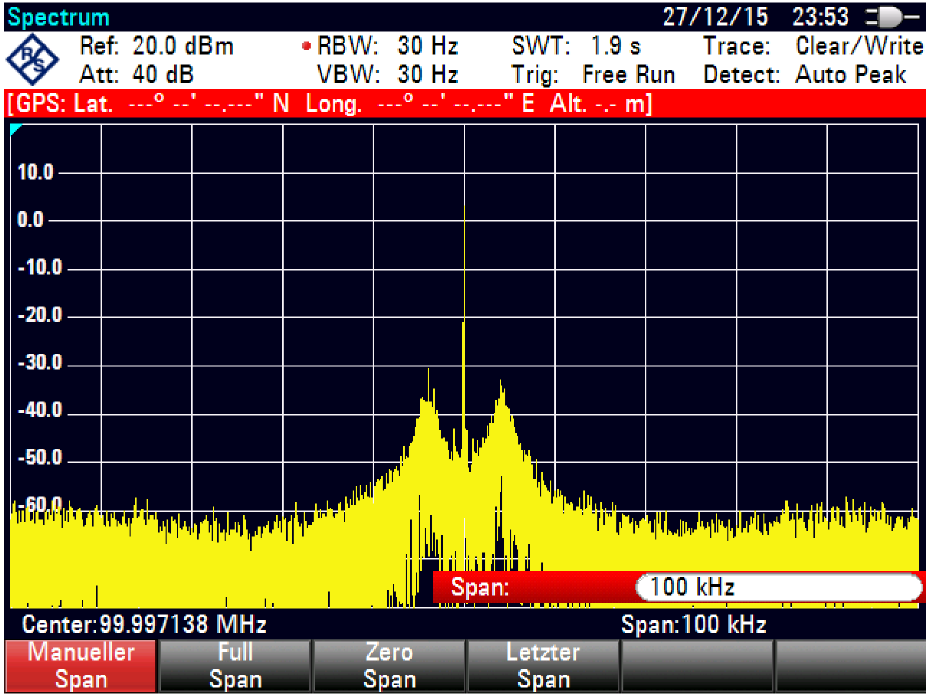
Maintenance: Protection

- Mechanic protection
- The display and some inductors are very fragile
- Take care to protect the HF section
  - Either with a case
  - Or with shields
- Be careful when transporting the rad1o



Performance Improvement: PLL

- The original rad1o firmware had trouble with the external PLL
- Higher than necessary noise
- Unstable/intermittent behavior



Spectrum 27/12/15 23:53

Ref: 20.0 dBm • RBW: 30 Hz SWT: 1.9 s Trace: Clear/Write

Att: 40 dB VBW: 30 Hz Trig: Free Run Detect: Auto Peak

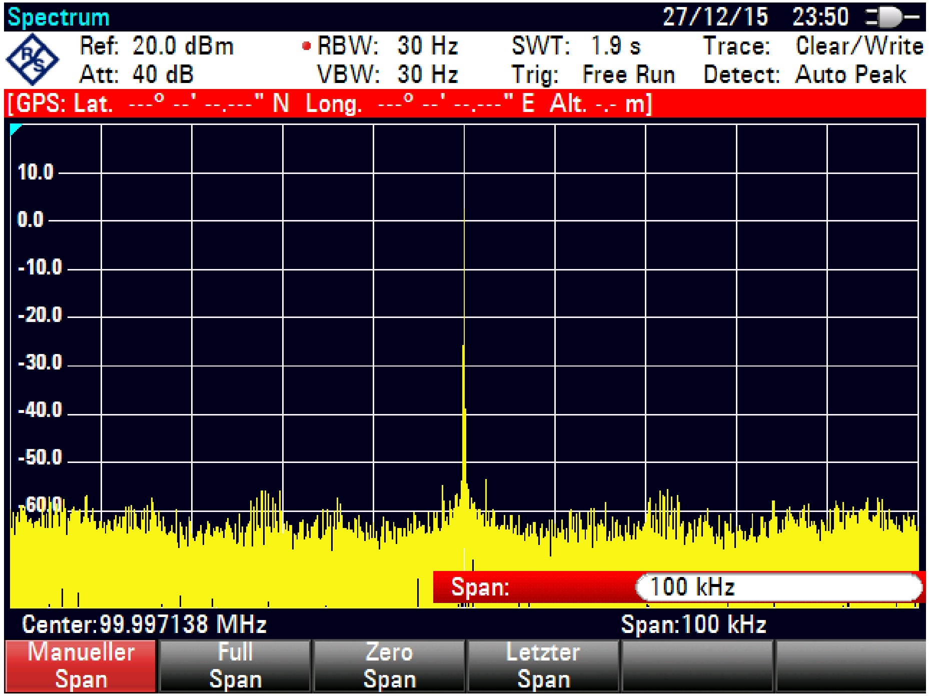
[GPS: Lat. ---° --' --.---" N Long. ---° --' --.---" E Alt. -.- m]

Span: 100 kHz

Center:99.997138 MHz Span:100 kHz

Performance Improvement: PLL

- Recent code improved PLL behavior
- Improved performance at frequencies < 2.15 GHz
- You want to update your f1rmware!



Spectrum 27/12/15 23:50

Ref: 20.0 dBm
Att: 40 dB
RBW: 30 Hz
VBW: 30 Hz
SWT: 1.9 s
Trig: Free Run
Trace: Clear/Write
Detect: Auto Peak

[GPS: Lat. ---° --' --.---" N Long. ---° --' --.---" E Alt. -.- m]

Span: 100 kHz

Center:99.997138 MHz Span:100 kHz

Performance Improvement: Interferences

- Disabled the 10 MHz reference output
  - Most likely unused by most people
- Clock for transceiver and PLL are now both 40 MHz
  - No extra spurs caused by the 50 MHz PLL clock

- Another reason to update your f1rmware

rad1o challenge

rad1o challenge

- We believe that SDR is fun and want to introduce more people to it.
- But: SDR seems difficult and obscure from the outside
- If we can get people to play with it, they will see the light
- How can we get people to try it?

→ rad1o challenge

rad1o challenge

- Starting with easy problems
- Slowly increase difficulty
  - We were short on time
  - Only 8 (9) challenges
- Web interface for solution tracking

rad1o challenge

1) Flash test

- Flash some code
  - Idea was so they know how to update their firmware.
  - Also maybe get them to develop something :)

2) Waterfall

- Open some waterfall and measure something in the time domain
  - They need to install some SDR tools

3) Signal Hunt

- Find frequency of a signal
  - Familiarize with Waterfall
  - Also: move around

rad1o challenge

4) Listen to me

- Listen to FM
  - Something we discussed at the SDR workshop
  - Also easy with gqrx

5) Where am I

- Locate signal source
  - Get familiar with your setup
  - Wanted to see people pass by our village

6) Power control

- hx2262 decoding
  - Also discussed at SDR workshop
  - But also doable with fast waterfall and patience

rad1o challenge

7) Turn me on

- hx2262 encoding
  - May have been to difficult
    - Or we f***d something up :-/
  - Nearly no-one got it correct

8) BEEP, BEEP, BEEP

- Locate signal source + Morse code
  - Similar to 5, but bigger area
  - Also look up Morse code
- Unintended hunt when we needed to get it back :)
  - Just borrowed a random laptop and rad1o
  - Surprisingly difficult without directional antenna

rad1o challenge

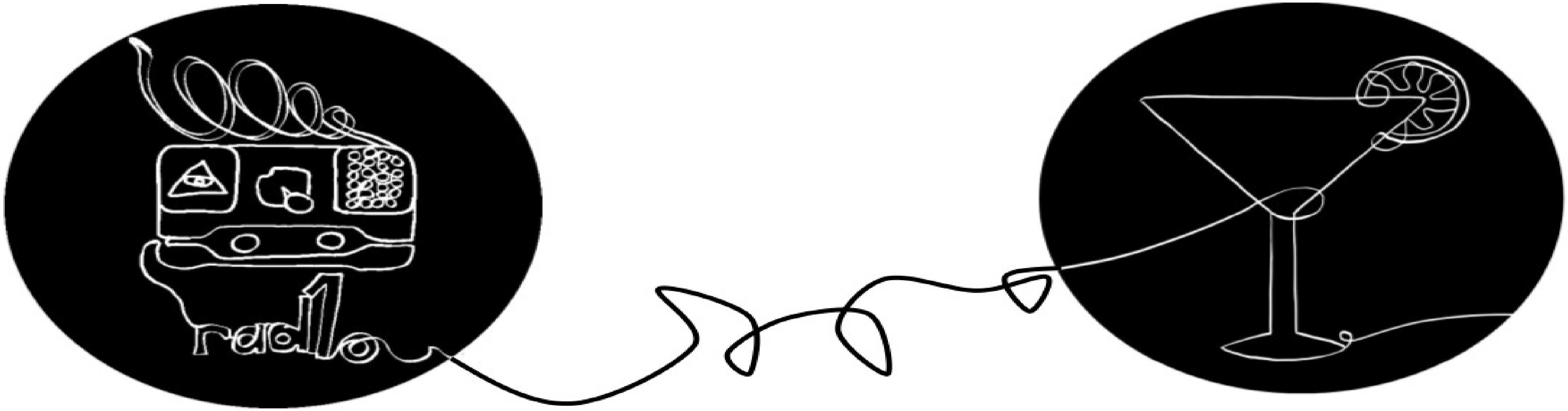
- Was fun to create
- Unfortunately only few people took part
- Feedback was positive

- Revival of the challenge:
  - Stop by rad1o assembly after talk

rad1o challenge

- Extra credit:
- We've got a few Mi-lights and a remote at the assembly
- The first rad1o stand alone application gets two lamps
- Stop by at the assembly and start hacking

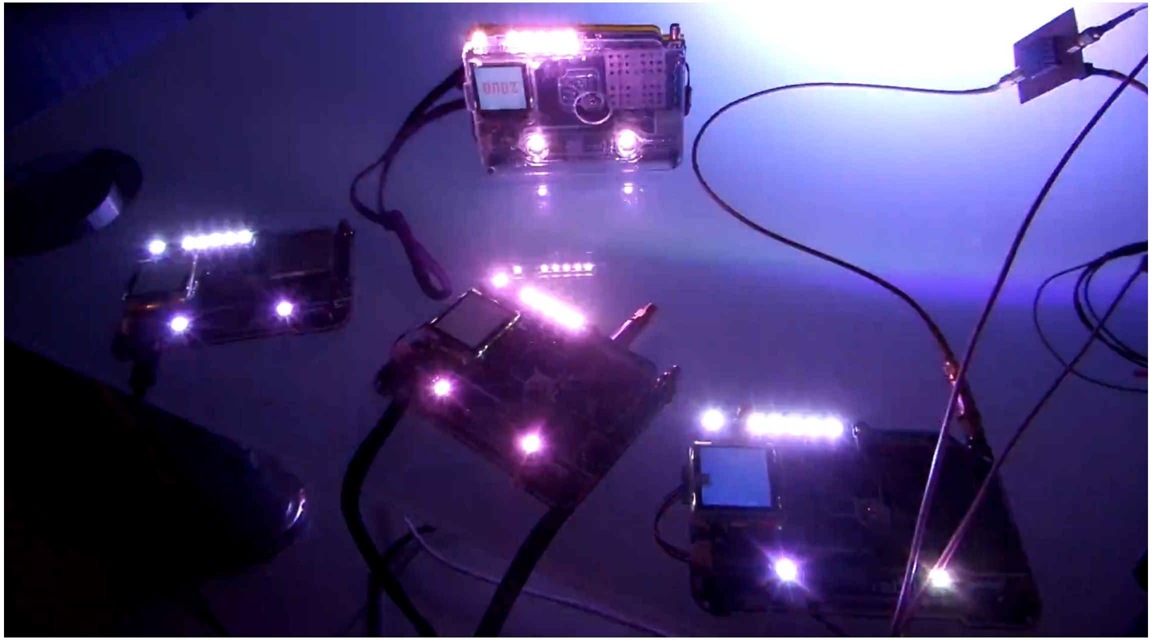
l0ungel1cht



L0unge-L1cht

l0ungel1cht: Overview

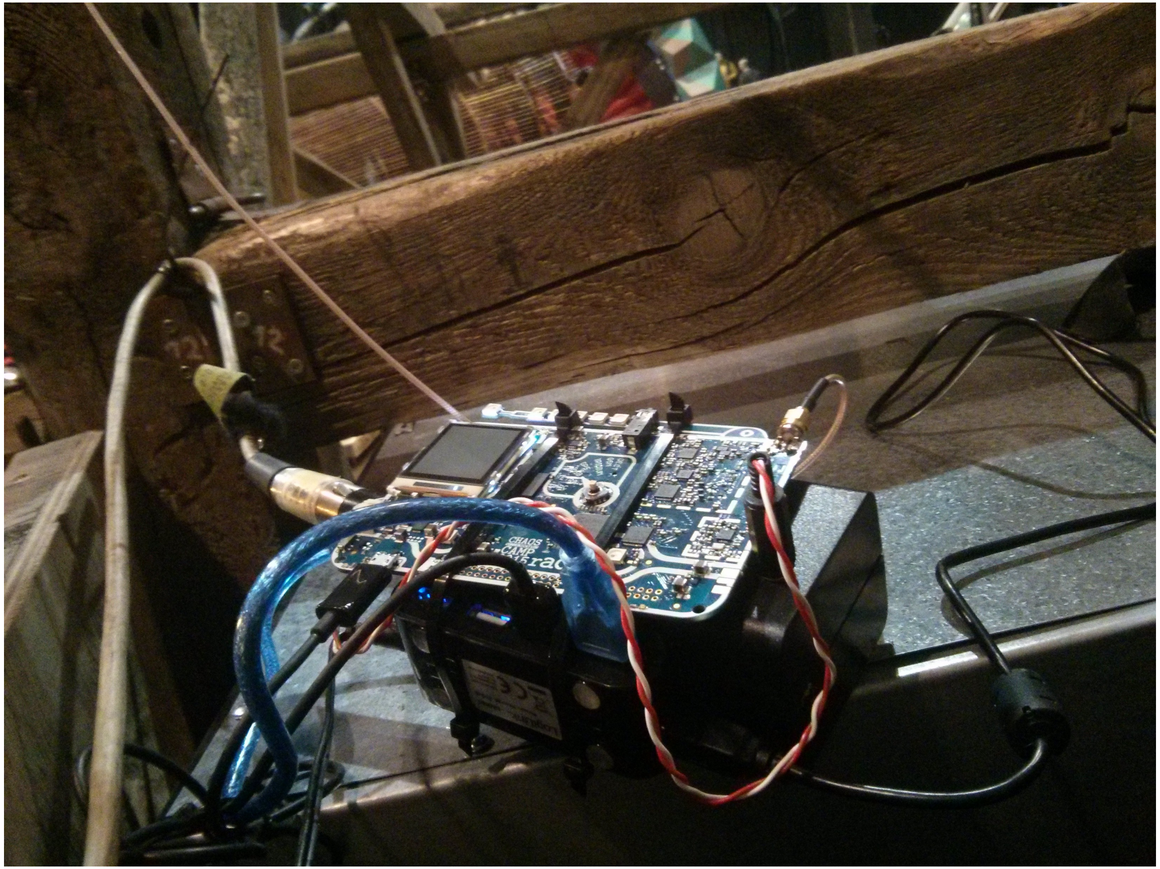
- Takes DMX data and transmits commands to other rad1os
- Using rflib from @hilse



l0ungel1cht: Protocol

```
### LED Subframe
Type 0x10-0x1F (0x1 == (TypeId >> 4))
| TypeId  | size | Description              | Data                     |
+---------+------+--------------------------+--------------------------+
| 0x10    | 0    | All LEDs and Display off | -                        |
| 0x11    | 3    | All LEDs same Color      | RGB                      |
| 0x12    | 3    | Display Color            | RGB                      |
| 0x13    | 1    | Run LED animation Number | N                        |
| 0x14    | 1    | Run Display animation No | N                        |
| 0x15    | 4    | LED x Color              | x RGB                    |
| 0x1D    | 24   | All LEDs different Color | RGBRGBRGBRGBRGBRGBRGBRGB |
| 0x1E    | -    | -                        | -                        |
| 0x1F    | -    | -                        | -                        |
```

l0ungel1cht: Hardware



We've got LOADS of RGB LED's at the rad1o assembly

l0ungel1cht: Application

- Shows your nick
- Fades background color and RGB LEDs when inside the lounge

- Get it at the rad1o assembly flash station or from GitHub

SDR

Recent SDR hacks

- Iridium: https://github.com/muccc/iridium-toolkit
- Globalstar: https://github.com/synack/globalstar
- ZigBee: https://www.sans.org/reading-room/whitepapers/threats/software-defined-radio-attack-smart-home-systems-35922
- Public transport
  - Munich: https://github.com/muccc/darc
  - Paderborn: http://www.bastibl.net/reversing-bus-telemetry/
- Tesla charge port vs. HackRF
- https://github.com/osqzss/gps-sdr-sim
  - Needs an external clock to work
- https://hackaday.com/tag/sdr/

Interesting Protocols/Signals

- Satellites
- Airplanes
- DECT
- Tetra
- FM (hidden data channels)
- ZigBee
- BLE
- GSM
- < 1 GHz building automation
- NRF2401: r0ket, keyboards, quad copters
- Other stuff you own

Possible Standalone Applications for the rad1o

- No WiFi jammers please :)
- RF replay device
- Self made home automation
- Passive indoor localization
- (Analog) video streaming
- USB filter
- USB exfiltration

- Have a look at https://media.ccc.de/v/dg56-Hands-on_Rad1o
  - In German

Getting a rad1o

- One of our prototype manufactures can help you
  - Dietz ELEKTRONIK MANUFAKTUR
  - Please get together to make things easier
    - Organize on the rad1o mailing list
  - We will prepare a complete data package for you
    - Please have a few days of patience after congress

- Mailing list: rad1o@lists.muc.ccc.de
- GitHub: https://github.com/rad1o/
- Wiki: https://rad1o.badge.events.ccc.de
- twitter: @rad1obadge

- **Get the latest firmware at the flash station at the rad1o assembly**
- Take your rad1o to the lounge

- **Join the rad1o assembly**
- There's LEDs, SMA connectors, and cases available at the assembly half an hour after the talk
  - SuperQ from Milliways had 8 RF kits left this morning