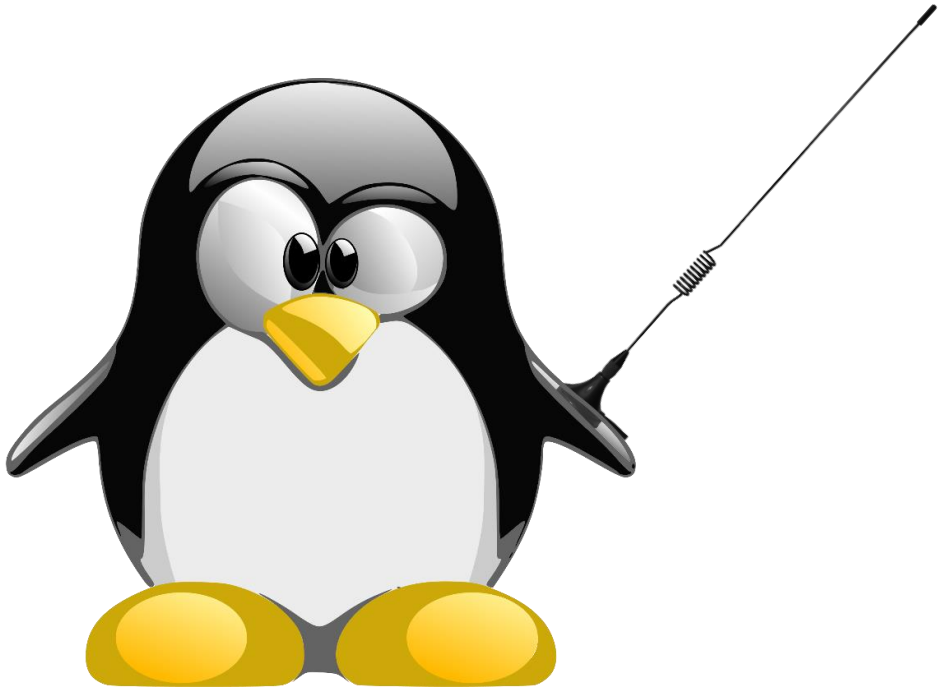
Software Defined Radio

Open Source Wireless Hacking

TECHNISCHE UNIVERSITÄT DARMSTADT



CROSSING

SEEMO SECURE MOBILE NETWORKING

Jiska Classen

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
jclassen@seemoo.tu-darmstadt.de
Tel.+49 6151 16-70924, Fax. +49 6151 16-70921
https://seemoo.de/jclassen

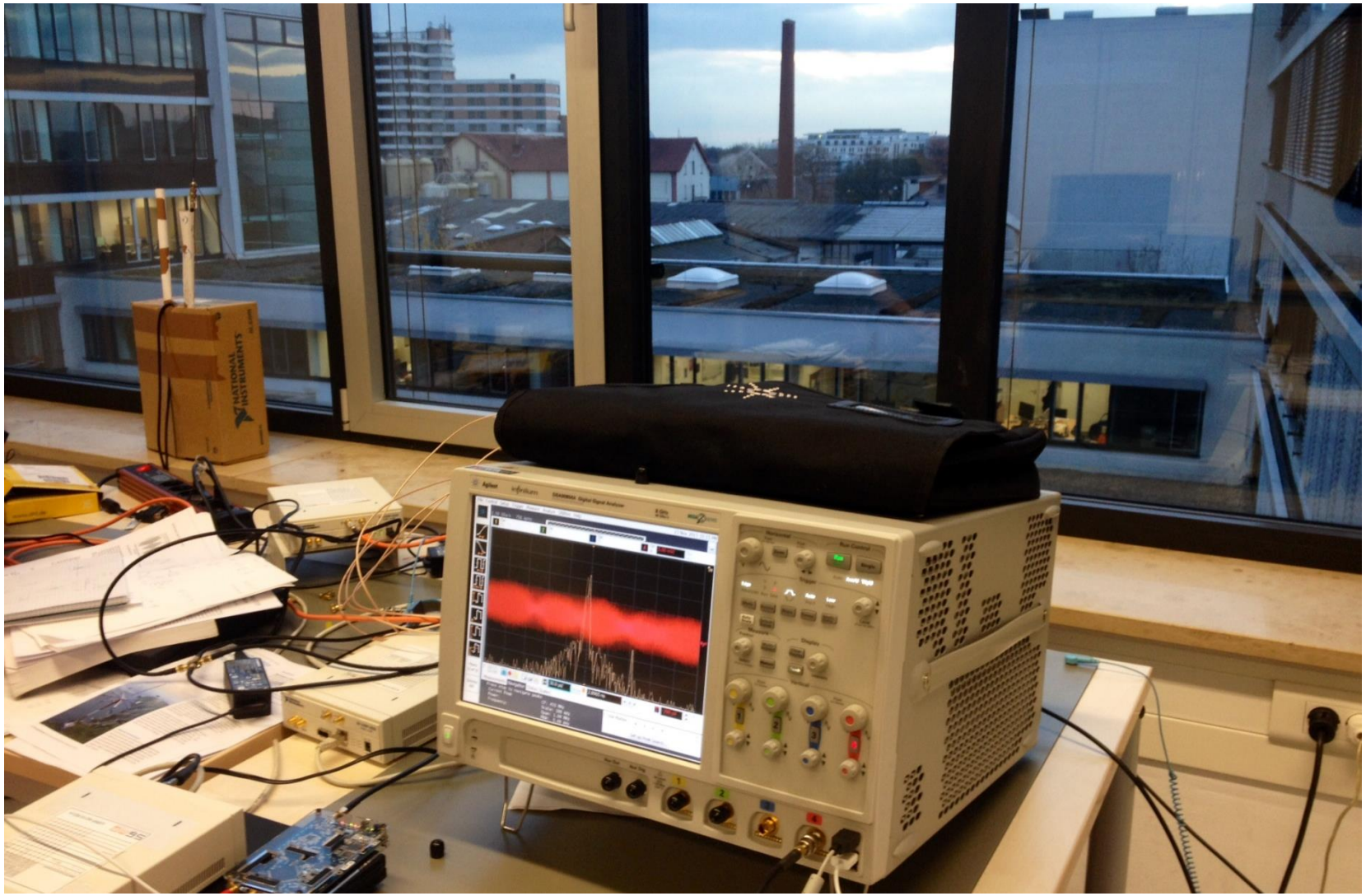
15. Augsburger Linux-Infotag 2016

Overview

(1) Problem Statement
(2) Hardware Overview
(3) Interesting Frequencies
(4) gqrx Demo
(5) gnuradio Demo
(6) Getting Started
(7) Q&A

Problem Statement

Spectrum Analyzer or Oscilloscope



Remaining Problems

Great hardware, goes up to 28GHz, 160MHz bandwith ☺

In CROSSING, we do mobile device pairing and trust models, but…

- **Mobile experiments** – hard to move
- **Distributed experiments** – only one device

Working with students…

- Teaching with **30+ students** – only one device…
- Students should be able to do some wireless hacking with **hardware they can afford** after the course

Hardware Overview

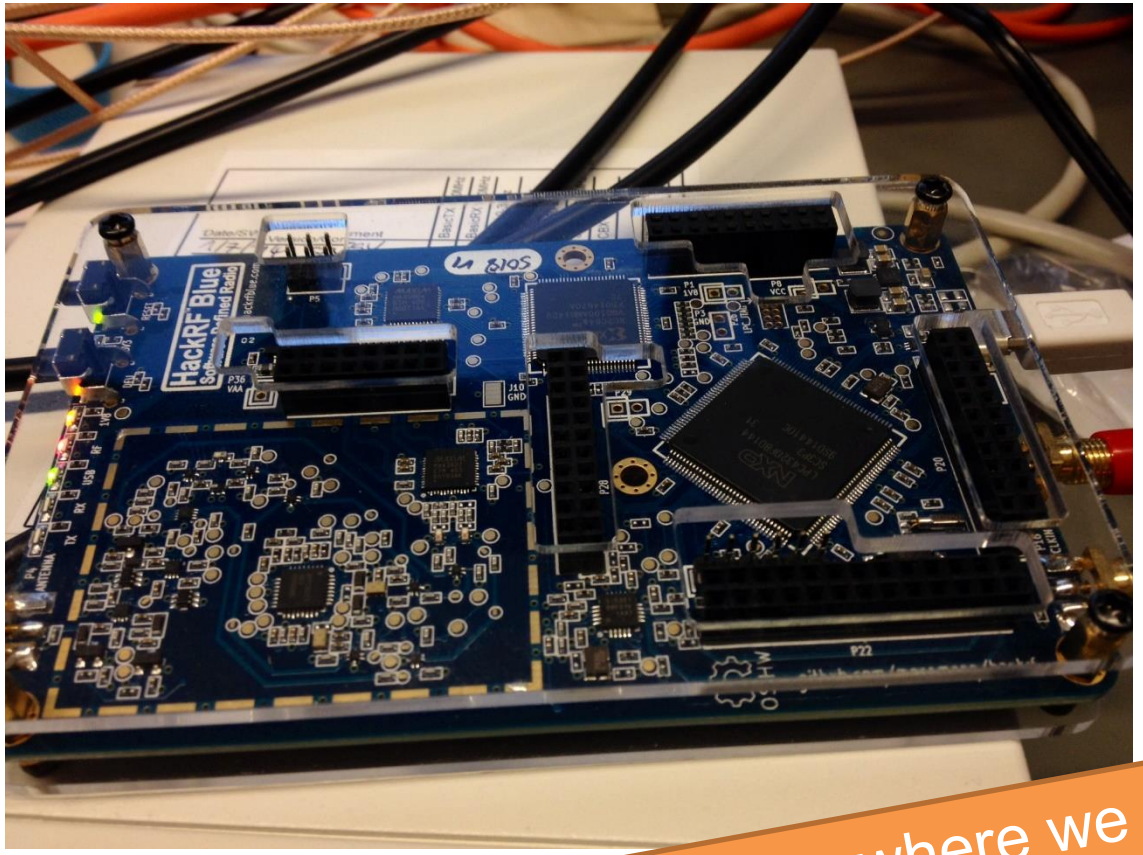
USRP

- Simultaneous transmission and reception
- Many different models available, from 700€
- Even within one model, different daughterboards are available
- Most popular for **research projects**
- Requires flashing a **Linux compatible** image (works with `uhd-host 3.9.3-1` in Debian testing)

For PhD projects

- What I brought today:
  - USRP **N210** – 1810€
  - **SBX** daughterboard – 495€
    400MHz-4.4GHz frequency range,
    40MHz bandwidth (=2 WiFi channels)
  - Also see: `uhd_usrp_probe -args addr=192.168.10.2`

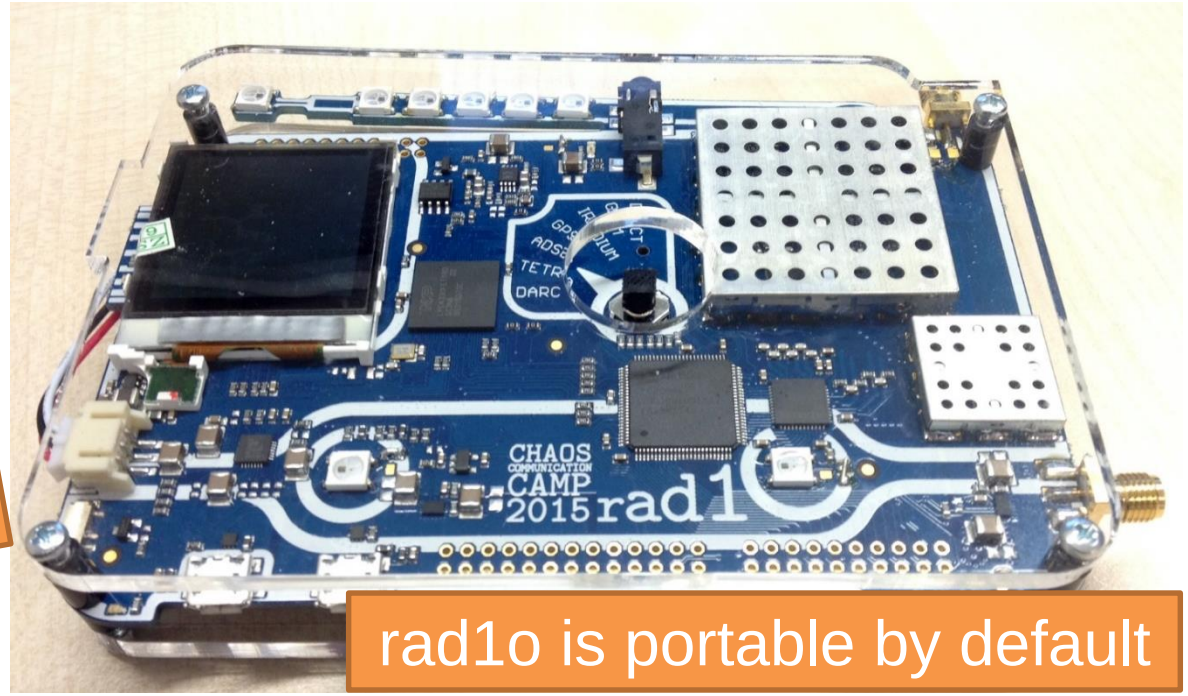
rad1o badge / HackRF



HackRF Blue

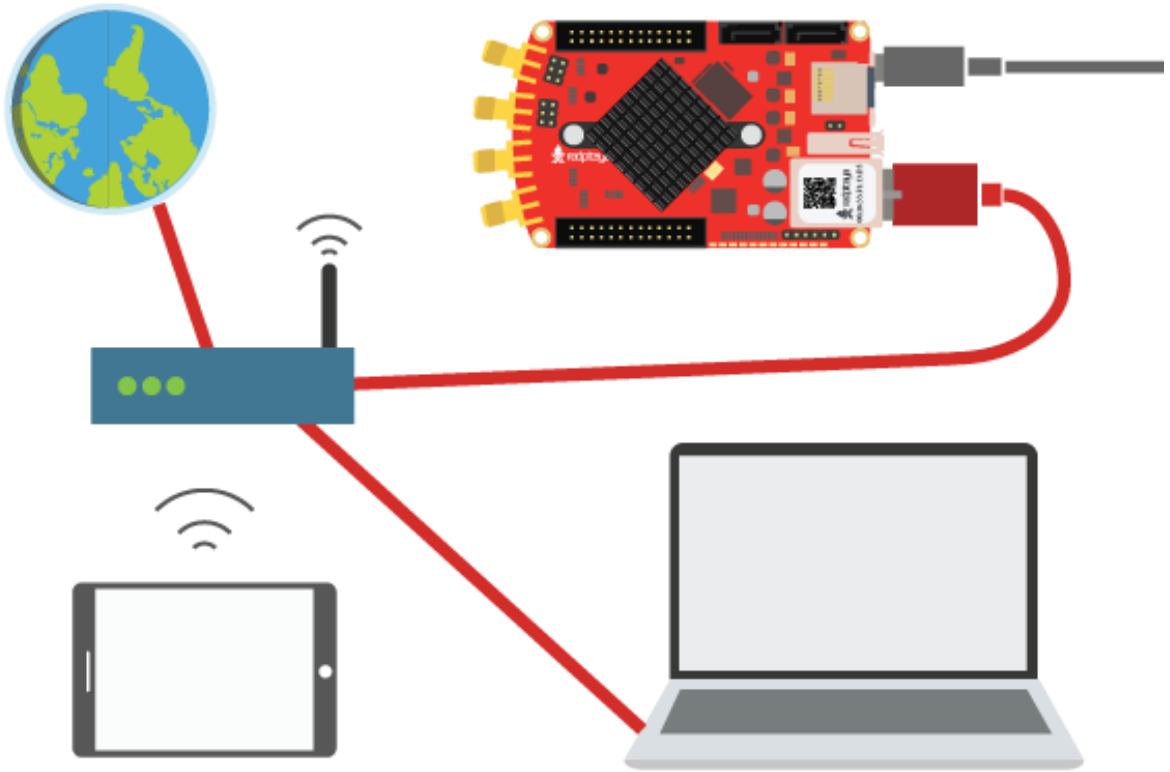
- Open source hardware
- Receiver or transmitter
- 1MHz-6GHz, 20Msps (**rad1o**: 1MHz-4GHz)
- 200€

In a price range where we can borrow it to students ☺



rad1o is portable by default

Red Pitaya



- Provides **open source applications** that run on the board:
  - Oscilloscope
  - Spectrum Analyzer
  - …
- Close to typical software defined radio features, but more powerful
- **Low frequency range:** 0-50MHz
- 234€ on reichelt

In a price range where we can borrow it to students ☺

DVB-T Sticks

We can borrow these to a whole course, or they buy these themselves…

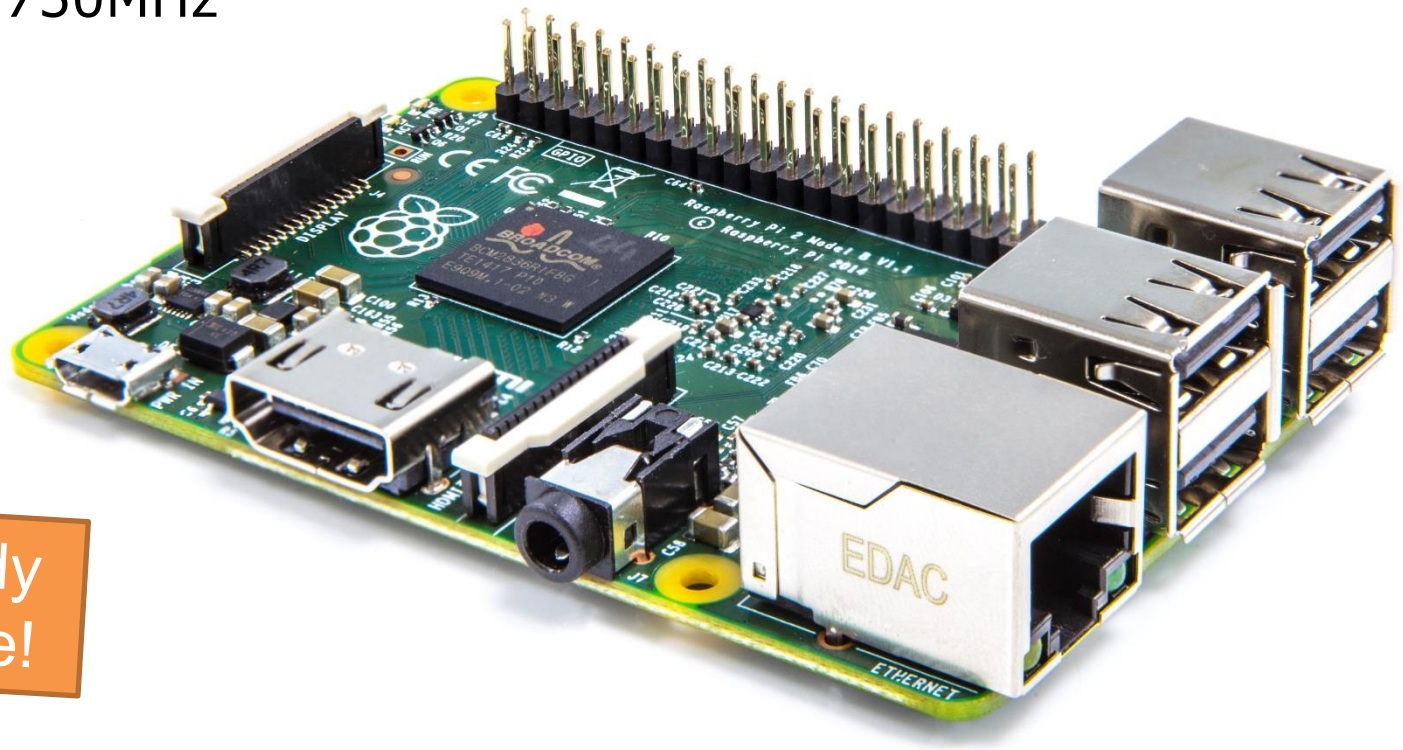
- Receiver for 22MHz-2.2GHz, frequencies vary depending on the actual model, ~2Msps
- From 7€

Tuner	Frequency range
Elonics E4000	52 – 1100 Mhz, 1250 – 2200 MHz
Rafael Micro R820T	24 – 1766 MHz
Rafael Micro R828D	24 – 1766 MHz
Fitipower FC0013	22 – 1100 MHz
Fitipower FC0012	22 – 948.6 MHz
FCI FC2580	146 – 308 MHz, 438 – 924 MHz

http://sdr.osmocom.org/trac/wiki/rtl-sdr

rpitx

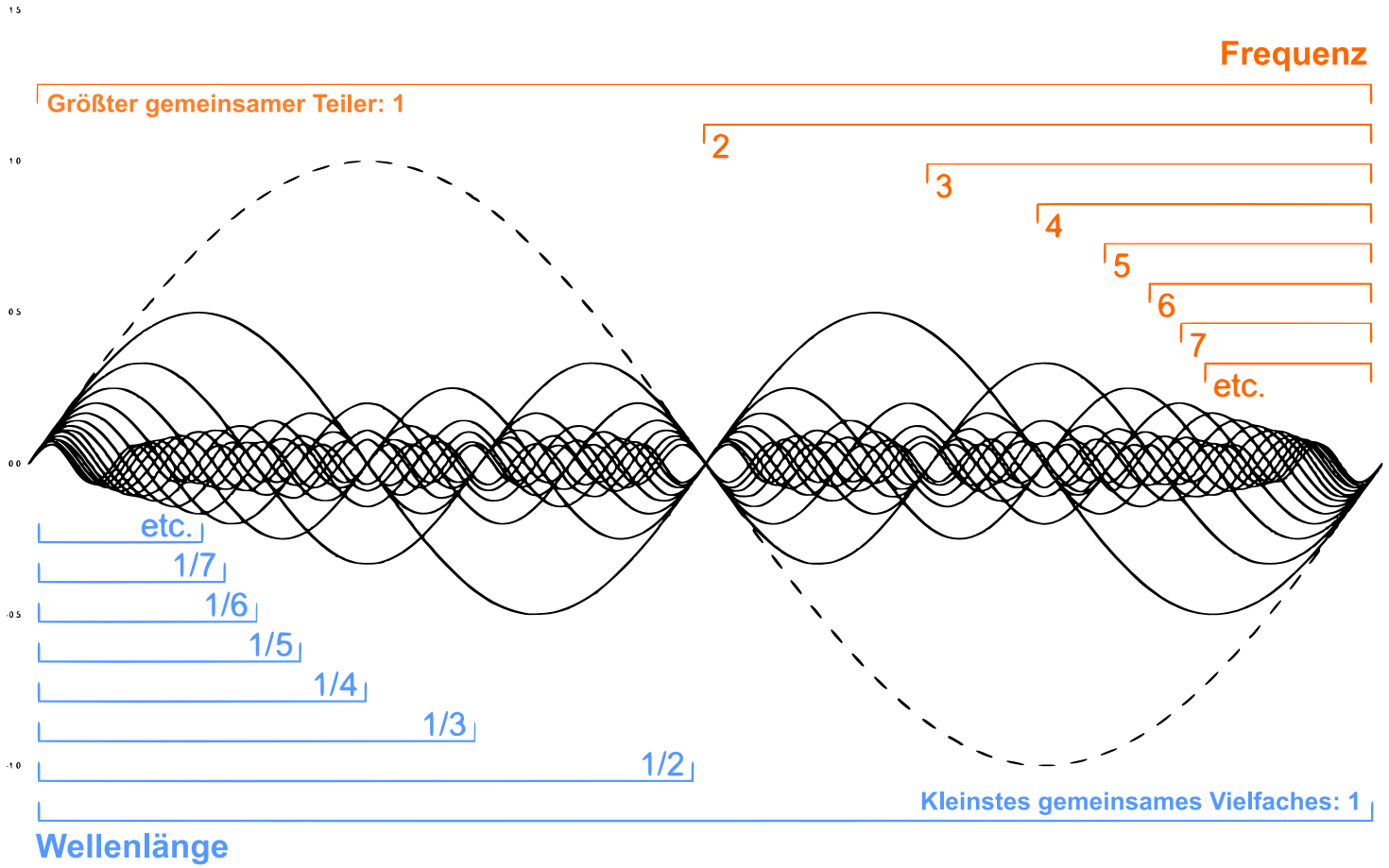
- Cheap transmitter for Raspberry Pi (B, B+ and PI2)
- Use GPIO pins + long wire as antenna
- Low frequency signals: 130kHz-750MHz
- 35€



Many nerds already have this hardware!

Interesting Frequencies

Wavelength vs. Frequency



$$f \sim \frac{1}{\lambda}$$

http://upload.wikimedia.org/wikipedia/commons/7/71/Missing_fundamental_Fourier_series.png

Low Frequency (2200m)

- Long wavelength requires huge antennas
- Transmitter for „Deutschlandfunk“: 153 kHz (1960m wavelength) is 363m high

http://de.wikipedia.org/wiki/Sender_Donebach

LF	MF	HF	VHF	UHF	SHF	EHF

Medium Frequency (160m)

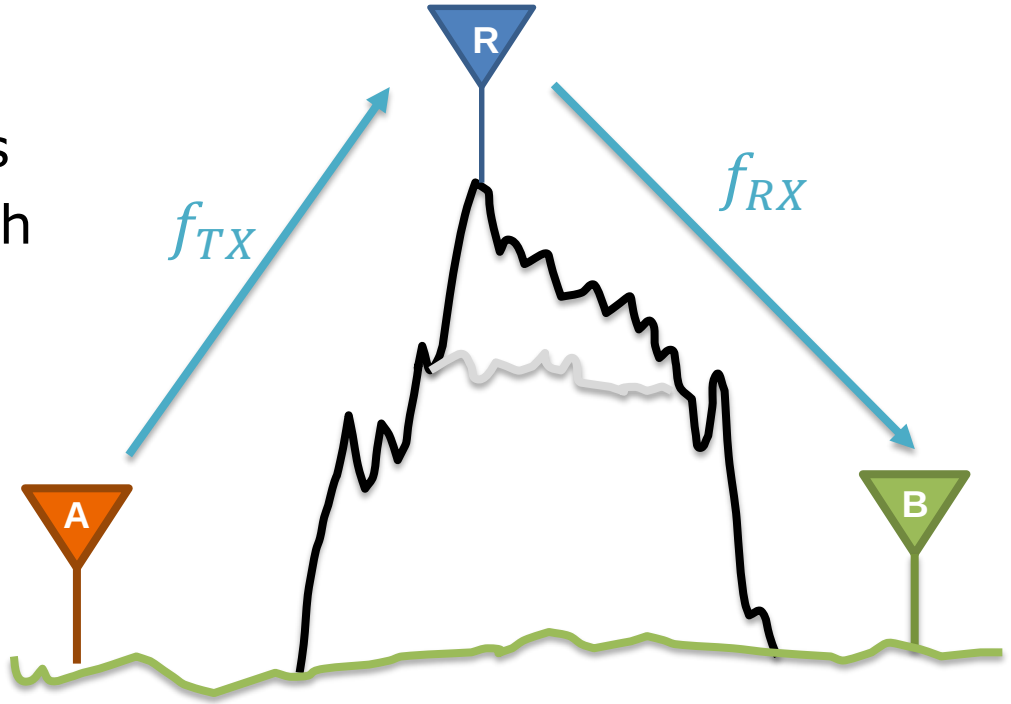
High Frequency
(80m, 40m, 30m, 20m, 17m, 15m, 12m, 10m)

- 80m, 40m, 20m used for long distances in ham radio (DX)
- Transmissions from Europe to USA or even Japan possible

Very High Frequency (6m, 2m)

- 2m and 70cm used for handheld receivers
- Small sizes possilbe
- **Relays** required for longer distances
- FM radio stations: ca. 3m wavelength

https://www.flickr.com/photos/alexkerhead/3608747482



Ultra High Frequency (70cm, 23cm, 13cm)

- 12.5cm: 2.4GHz **WLAN**
- 900MHz and 1.8GHz **GSM**

Super High Frequency (9cm, 6cm, 3cm, 1.2cm)

- 6cm: 5GHz WLAN

Millimiter Wave (6mm, 4mm, 2.5mm, 2mm, 1.2mm)

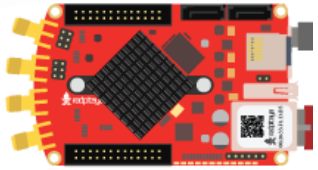
- mmWave/60GHz WLAN
- Only a few meters range
- Walls etc. completely block the signal
- Typical application scenarios are indoor, e.g. wireless docking stations

Hardware Capabilities

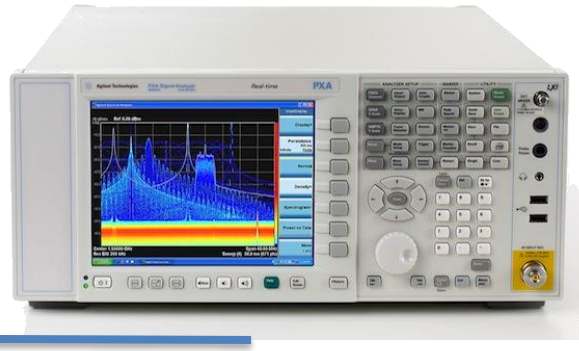
TX

RX

RX|TX



RX&TX



RX&TX

RX

LF | MF | HF | VHF | UHF | SHF | EHF

Frequenznutzungsplan

Details, **wer** welche **Frequenz** mit welcher **Betriebsart** und mit welcher **Leistung** nutzen darf, sind dem Frequenznutzungsplan der Bundesnetzagentur zu entnehmen.

http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Grundlagen/Frequenzplan/frequenzplan-node.html

Demo
gqrx

Features

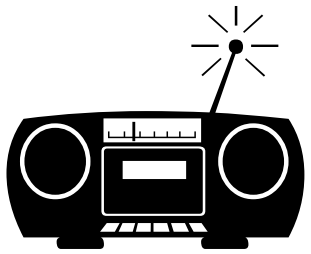
- Signal reception and **capture**
- Basic **demodulation** schemes, e.g. AM, FM, SSB
- Compatible to **HackRF, rad1o, Red Pitaya, DVB-T sticks** and more
- Typical application: check if signal reception is working, signal processing in external software

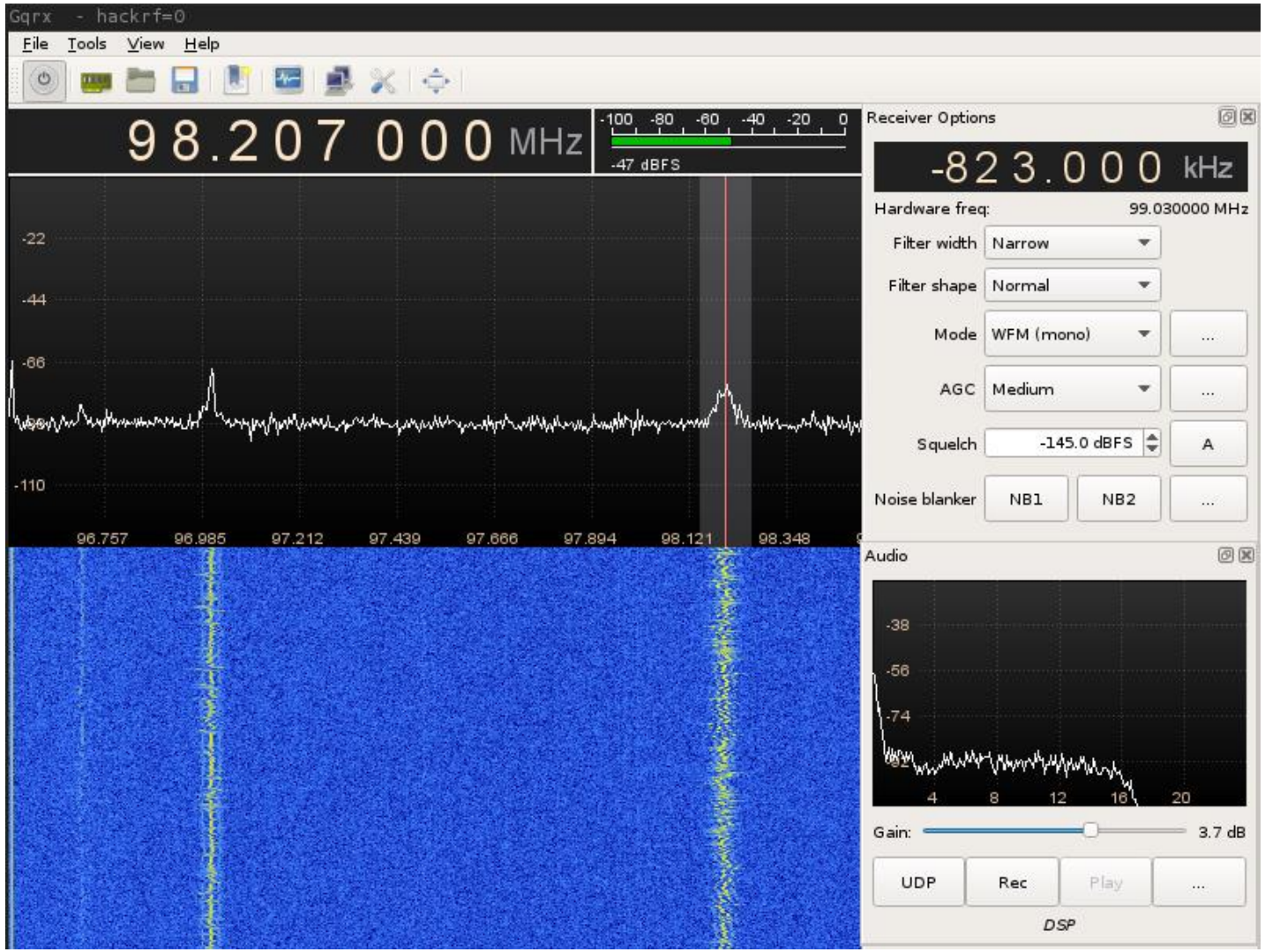
Demo

- Receive nearby FM radio stations (DVB-T, rad1o)
- Check frequencies of GSM stations (DVB-T, USRP, rad1o)
- Check frequencies of WiFi access points (rad1o, USRP)

Listen to the radio

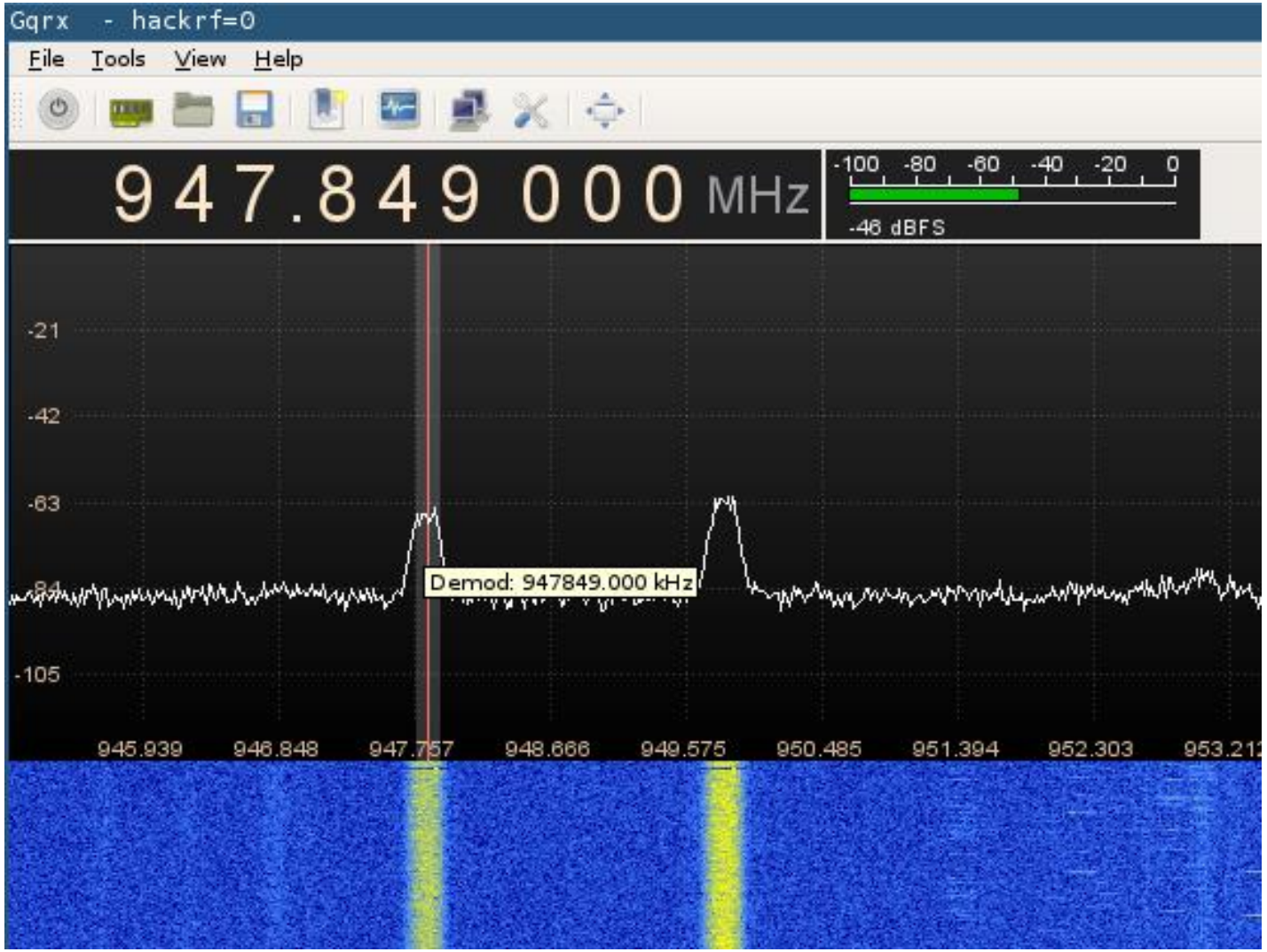
- German FM stations are located between 87.5MHz and 108MHz
- Set demodulation to „WFM (stereo)“
- For a noisy signal: update Squelch setting
- Adjust volume by setting the audio gain





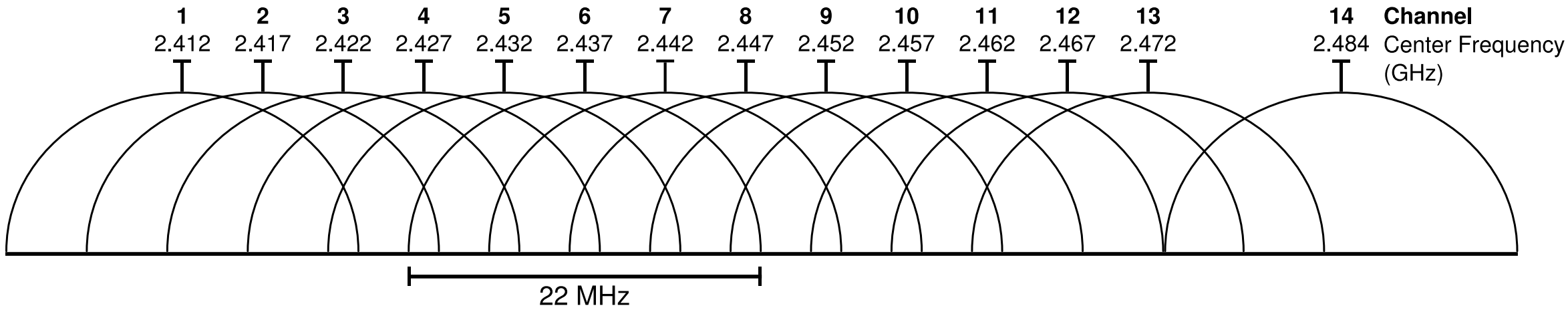
GSM

- GSM downlink is located between 925MHz and 960GHz (Germany)
- Set maximum sampling rate + bandwidth to find ARFCNs in use

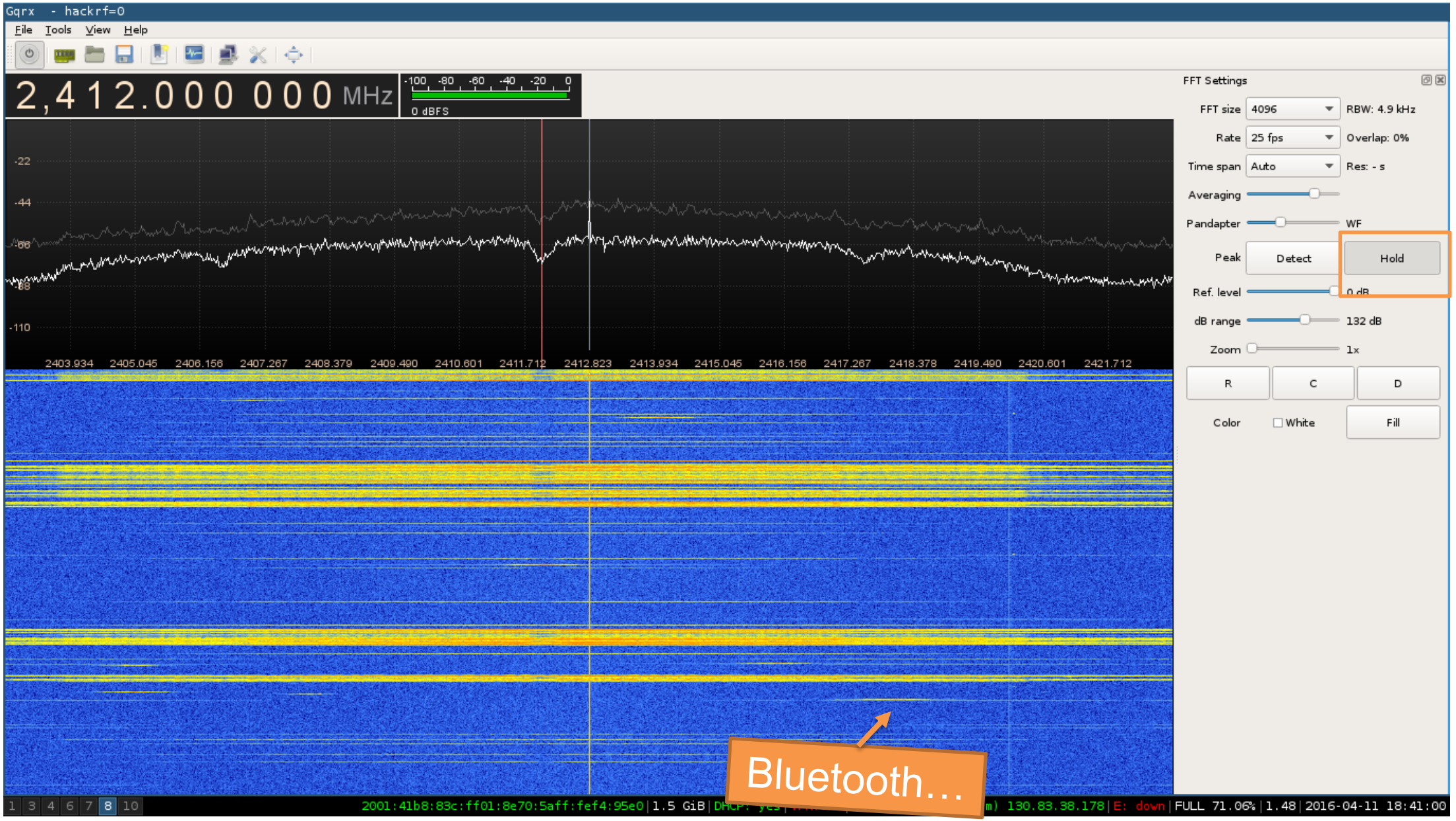


WiFi

- A bandwidth of 20MHz is required – does not work with DVB-T sticks!
- Also, DVB-T sticks only go up to 2.2GHz…
- We need to select a channel center frequency for WiFi sniffing:



https://en.wikipedia.org/wiki/IEEE_802.11#/media/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg


Gqrx - hackrf=0
File Tools View Help
2,412.000 000 MHz
-100 -80 -60 -40 -20 0
0 dBFS
-22
-44
-66
-88
-110
2403.934 2405.045 2406.156 2407.267 2408.379 2409.490 2410.601 2411.712 2412.823 2413.934 2415.045 2416.156 2417.267 2418.378 2419.490 2420.601 2421.712
FFT Settings
FFT size 4096
RBW: 4.9 kHz
Rate 25 fps
Overlap: 0%
Time span Auto
Res: - s
Averaging
Pandapter
WF
Peak
Detect
Hold
Ref. level
0 dB
dB range
132 dB
Zoom
1x
R
C
D
Color
White
Fill
Bluetooth…
1 3 4 6 7 8 10
2001:41b8:83c:ff01:8e70:5aff:fef4:95e0 | 1.5 GiB | 130.83.38.178 | E: down | FULL 71.06% | 1.48 | 2016-04-11 18:41:00

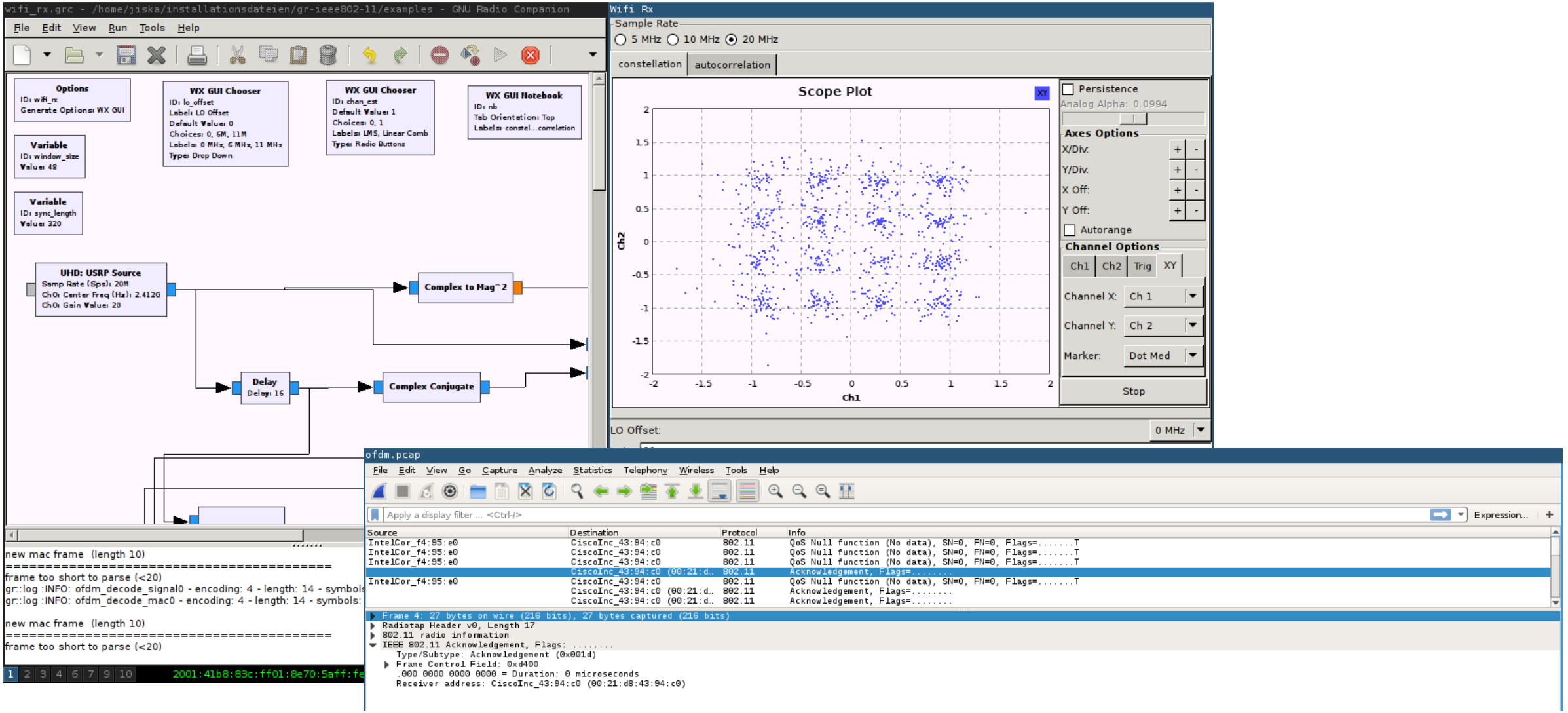
Demo gnuradio

Features

- Open source **signal processing**
- Many interesting projects available, e.g. GSM, Bluetooth, WiFi, TETRA
- Supports HackRF, rad1o, USRP, …

- Demo projects:
  - `gr-ieee80211`
  - `gr-gsm`

gr-ieee802-11



gr-gsm

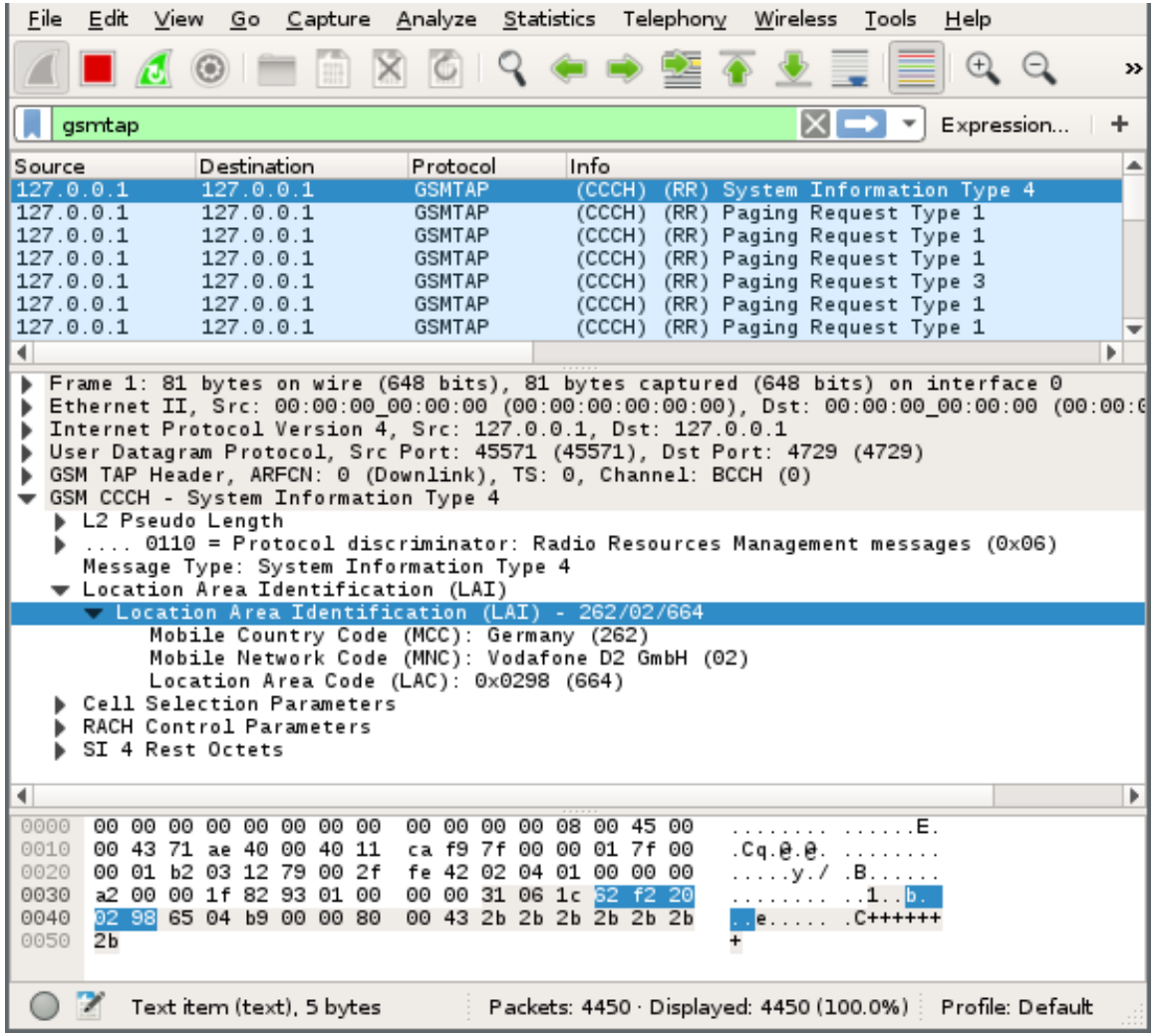
ARFCN from gqrx:

$$947.8MHz = 890MHz + 0.2MHz * 64 + 45MHz$$

```
grgsm_capture -a 64 -c output.gsm

wireshark -k -f udp -Y gsmtap -i
lo

grgsm_decode -a 64 -c output.gsm
```



Where to start?

Getting Started

- Get a **rtl-sdr** compatible DVB-T stick
- Connecting software defined radios to **virtual machines can cause data loss**!
- Some software might also run under Windows, but even harder to install…
- Use a **Live CD**, e.g. Kali Linux ☺

- Demo today used:
  - Debian testing packets with `gnuradio 3.7.9.1-2+b1`
  - `gr-ieee802-11` and `gr-gsm` built from github sources on April 11 2016

Q&A