

# UBA Belgian SDR Meetup 3

Kristoff Bonne (ON1ARF)  
30/10/2020

# BE.SDR Meetup 3: Agenda

- 20:00
  - Question time + Introduce yourself
  - Some news about BE.SDR
- 20:30
  - Solution of CTF1 and CTF2
  - The elektor SDR receiver shield  
"Learning SDR hardware: A bare minimum SDR receiver"
- 21:40
  - Open discussion on BE.SDR

# BE.SDR Meetup 3: Agenda

- 20:00
  - Question time + Introduce yourself
  - Some news about BE.SDR
- 20:30
  - Solution of CTF1 and CTF2
  - The elektor SDR receiver shield  
“Learning SDR hardware: A bare minimum SDR receiver”
- 21:40
  - Open discussion on BE.SDR

# Practical Issues

This is a video-conference, so please follow these rules

- Use a headset
- Best browsers:
  - chrome / chromium / ...
  - Firefox
- Mute mic if you have nothing to say
- Switch off your camera if you have nothing to show

# Practical Issues

This is a video-conference, so please follow these rules

- Feel free to give feedback!
  - There are three “question time” moments
  - You can also use the “chat”
  - Feel free to use your own language to ask questions
    - I will reply in English

# Practical Issues

The video-presentation will be recorded and can be placed online.

Note, that, if you speak, your video (if on) and your name / call will be visible!

# Legal

This presentation are distributed under the Creative Commons “BY-SA 4.0” License:

<https://creativecommons.org/licenses/by-sa/4.0/>

Images used in the presentation may come with their own license.

All care has been taken that all images may be used publicly. If you own the copyright to an image and consider its use in this document improper, please contact the author of this document.

# BE.SDR Meetup 3: Agenda

- 20:00
  - Question time + Introduce yourself
  - Some news about BE.SDR
- 20:30
  - Solution of CTF1 and CTF2
  - The elektor SDR receiver shield  
“Learning SDR hardware: A bare minimum SDR receiver”
- 21:40
  - Open discussion on BE.SDR

# PySDR



## PySDR: A Guide to SDR and DSP using Python

By Dr. Marc Lichtman

### Navigation

- 1. Introduction
- 2. Frequency Domain
- 3. IQ Sampling
- 4. Digital Modulation
- 5. PlutoSDR Basics
- 6. PlutoSDR Advanced Topics
- 7. Noise and dB
- 8. Filters
- 9. Link Budgets
- 10. Channel Coding
- 11. IQ Files
- 12. Multipath Fading
- 13. Pulse Shaping
- 14. Synchronization
- 15. Textbook Comparison
- 16. About the Author

Online Python Console

Quick search

Go

[1. Introduction →](#)

## PySDR: A Guide to SDR and DSP using Python

by [Dr. Marc Lichtman](#)

- [1. Introduction](#)
  - [Purpose and Target Audience](#)
  - [Contributing](#)
  - [Acknowledgements](#)
- [2. Frequency Domain](#)
  - [Fourier Series](#)
  - [Time-Frequency Pairs](#)
  - [Fourier Transform](#)
  - [Time-Frequency Properties](#)
  - [Fast Fourier Transform \(FFT\)](#)
  - [Negative Frequencies](#)
  - [Order in Time Doesn't Matter](#)
  - [FFT in Python](#)
  - [Windowing](#)
  - [FFT Sizing](#)
  - [Spectrogram/Waterfall](#)
- [3. IQ Sampling](#)
  - [Sampling Basics](#)
  - [Nyquist Sampling](#)
  - [Quadrature Sampling](#)
  - [Complex Numbers](#)
  - [Receiver Side](#)
  - [Receiver Architectures](#)
  - [Carrier and Downconversion](#)
  - [Baseband and Bandpass Signals](#)
  - [DC Spike and Offset Tuning](#)
  - [Sampling Using the PlutoSDR](#)
  - [Calculating Average Power](#)

# PySDR

“SDR explained for Programmers”

- Relative little math
- Very well explained
- Examples using py (scipy, numpy, matplotlib)

# GNU Radio chat

<https://chat.gnuradio.org/>

The screenshot shows a dark-themed chat interface. On the left, a sidebar lists rooms: Kristoff Bonne (ON1ARF), Favorites, education, Ham Radio (which is selected and highlighted in grey), People, Rooms, and General Chat. The main area is a conversation in the 'Ham Radio' room. A message from Kristoff Bonne (ON1ARF) at 16:52 says: "Hi all, F.Y.I. for who does not follow the GNU Radio mailing-list. A quick reminder for the 3th UBA Belgian (online) SDR Meetup, that will be held this evening. As the previous meetups, the event will be held online (jitsi link, see below), starting at 20:00 CET (19:00 UTC). The agenda is as follows:

- Question & Answer round:  
This allows everybody to ask questions on SDR, show off any SDR related projects you are working on, or just introduce yourself.
- Some news about SDR
- The solution of the two CTF challenges.
- A small presentation of the 'Elektor SDR shield' project.

What have we learned so far? How well does it work?  
How does SDR receiver hardware actually work and what are the pitfalls?

- Time permitting, we can have a free discussion afterwards on any SDR related topic.

Like last time, the Meetup starts at 20:00.  
The presentations start around 20:30 and should be finished between 21:30-22:00

The URL of the jitsi meeting is:  
<https://meet.jit.si/UBABelgianSDRMeetup>

# Monthly GNU Radio Amateur Radio Meeting

<https://wiki.gnuradio.org/index.php/User:Duggabe>

## Contents [hide]

- 1 GNU Radio Amateur Radio meeting agenda
  - 1.1 Introductions
  - 1.2 Brief walk-through of Simulation example: FSK
  - 1.3 Presentation of gr-RTTY-basics package
    - 1.3.1 Audio loopback demo
    - 1.3.2 Live Over-the-Air demo
  - 1.4 Notes

## GNU Radio Amateur Radio meeting agenda [\[edit\]](#)

Our first video meeting was held 17 October. Due to some technical difficulties with Big Blue Button, we moved to Zoom and succeeded in doing the planned agenda. For those who missed the meeting because of scheduling or time of day, **the next meeting will be on Saturday 7 November 16:00 UTC**. If you have any questions about your local time, go to <https://www.timeanddate.com/worldclock/timezone/utc>

Link: <https://cardiff.zoom.us/j/82317845680?pwd=SFg4eEdDZFNYODF1V0hEYmE3Y2hpZz09>

## Introductions [\[edit\]](#)

Host: Barry Duggan, KV4FV

Co-host: Derek Kozel, MW0LNA & KOZEL

## Brief walk-through of Simulation example: FSK [\[edit\]](#)

[https://wiki.gnuradio.org/index.php/Simulation\\_example:\\_FSK](https://wiki.gnuradio.org/index.php/Simulation_example:_FSK)

## Presentation of gr-RTTY-basics package [\[edit\]](#)

<https://github.com/duggabe/gr-RTTY-basics>

<https://github.com/duggabe/gr-webserver>

## Audio loopback demo [\[edit\]](#)

# BE.SDR Meetup 3: Agenda

- 20:00
  - Question time + Introduce yourself
  - Some news about BE.SDR
- 20:30
  - Solution of CTF1 and CTF2
  - The elektor SDR receiver shield  
“Learning SDR hardware: A bare minimum SDR receiver”
- 21:40
  - Open discussion on BE.SDR

# CTF: Capture the Flag

## **What is a “Capture the flag”**

- Started out as outdoor game
- Later: Cybersecurity events
  - 2 teams against eachother
  - Or CTF against the organisation of the cybersec event: (e.g. find hidden text key in file, disassembler application, ...)
- RF Cybersecurity:  
Extract hidden message from IQ file

# CTF: The GOAL

Learn SDR, GNU Radio and Tools in a fun way

- Learn how to demodulate signals
- Learn how to decode signals
  - Formatting and encoding of data
  - Error Detection / Error Correction
  - ...
- Practice your coding skills

# CTF1

- 2 'iq' files:
  - 20200919\_1210Z\_490Khz\_1200sps
  - 20200919\_1240Z\_518Khz\_1200sps
- Decoder: <https://github.com/on1arf/py-navtexdec>
- Hint: 2nd Belgian SDR Meetup

# CTF2

- iq file:  
Ctf2\_1200bps.iq
- The question of this ctf is this:  
When (date/time) was this recording made?
- Hint: The question of the ctf is a hint by itself.

# CTF: Scoreboard

- CTF 1:
  - Jan ON6LM
- CTF 2:
  - Laurein ON4CG
  - Jan ON6LM

# BE.SDR Meetup 3: Agenda

- 20:00
  - Question time + Introduce yourself
  - Some news about BE.SDR
- 20:30
  - Solution of CTF1 and CTF2
  - The elektor SDR receiver shield  
"Learning SDR hardware: A bare minimum SDR receiver"
- 21:40
  - Open discussion on BE.SDR

# Project: the elektor SDR Shield

Learning SDR Hardware, using a very basic SDR Receiver



Elektor SDR Shield 2.0 (Module | 170515-91)

★★★★★ 1 Review | Add Your Review

A newer version of the **Elektor SDR Reloaded (150515-91)**, the difference is that on this new version with two PLL outputs and two LF-outputs, which are accessible via additional connectors on the board (not included in the kit). This allows the user to use this Arduino shield as a signal generator, SW transmitter or even transceiver.

Please note: The module doesn't come pre-soldered.

[Read more](#)



# the elektor SDR Shield: Schematics

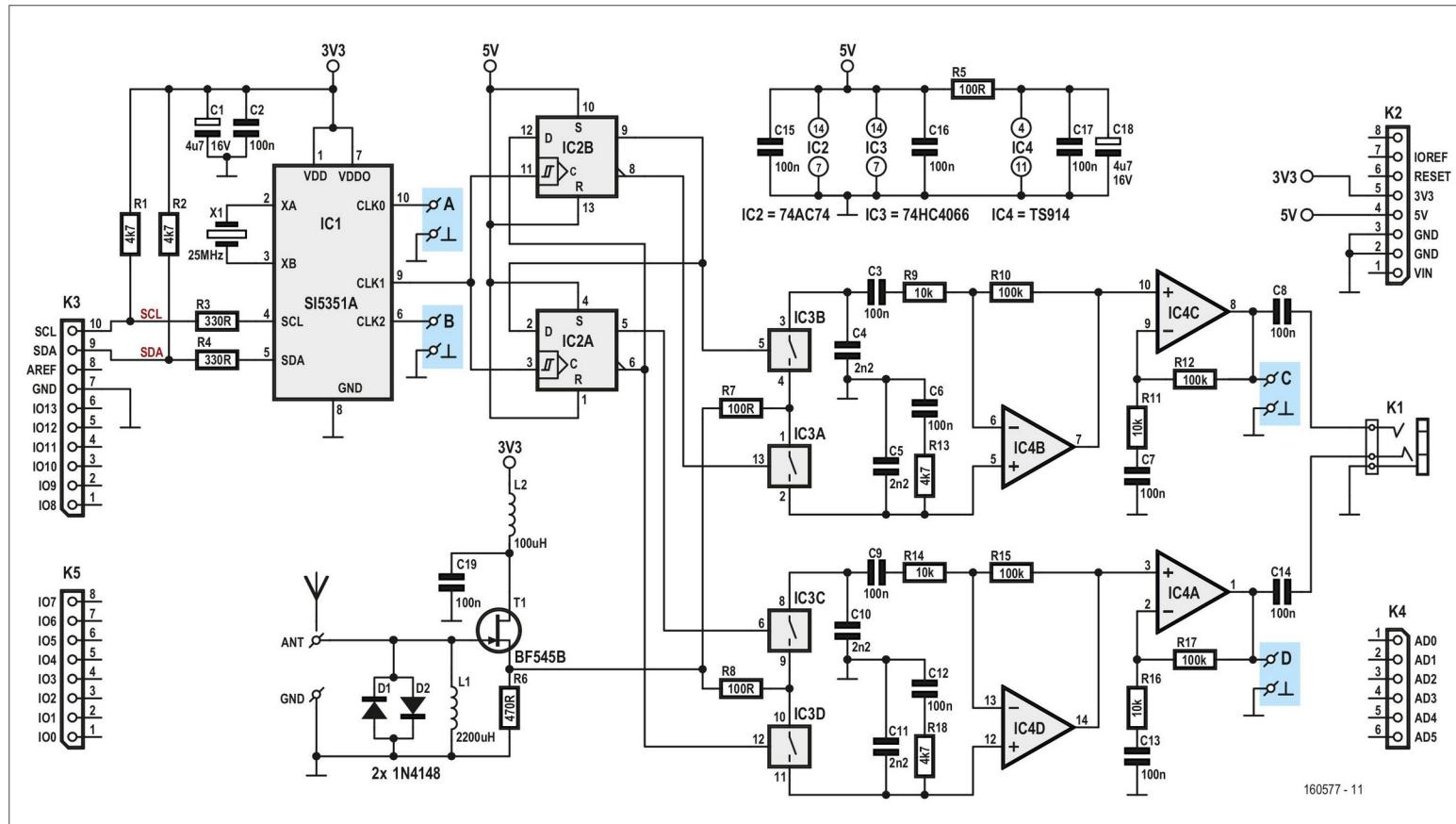
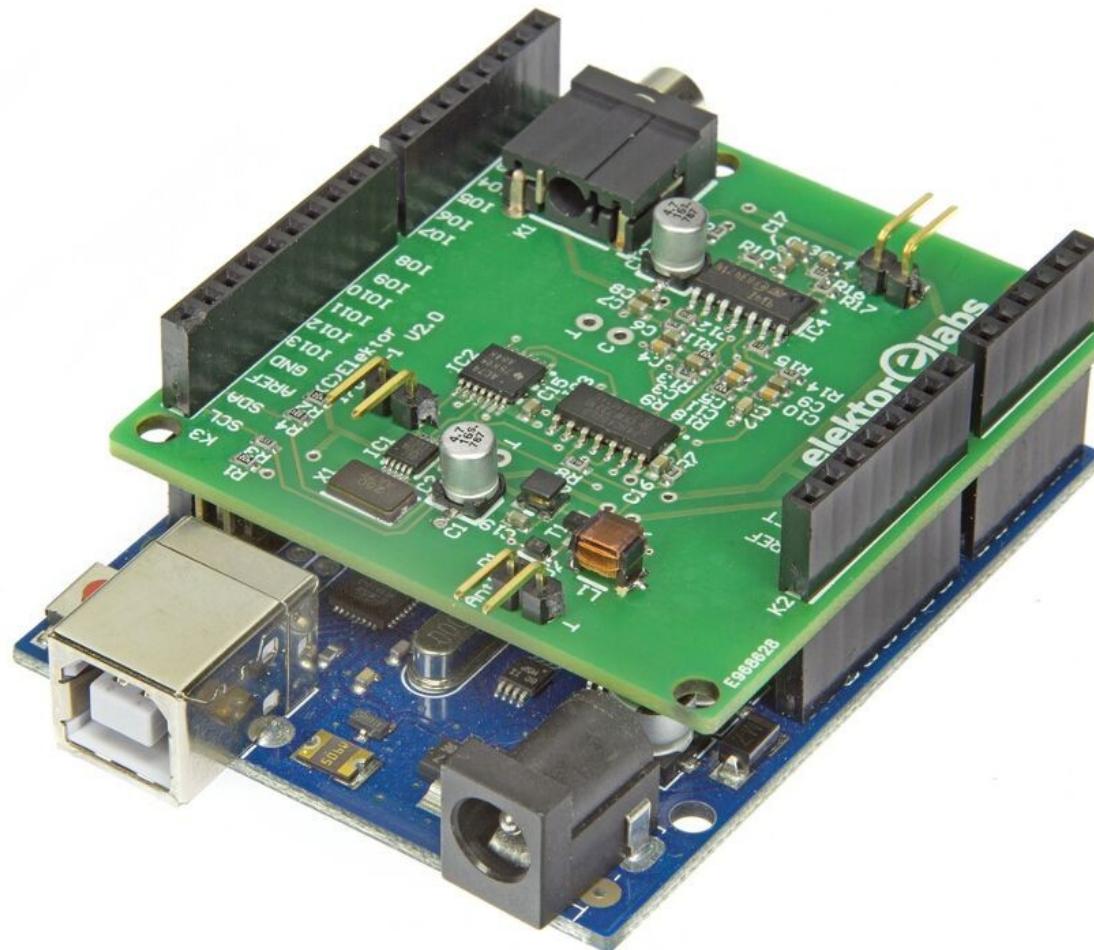


Figure 1. The new connections are highlighted in the schematic.

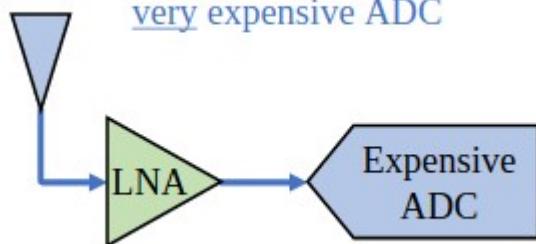
# the elektor SDR Shield: On arduino



# SDR receivers: 3 types

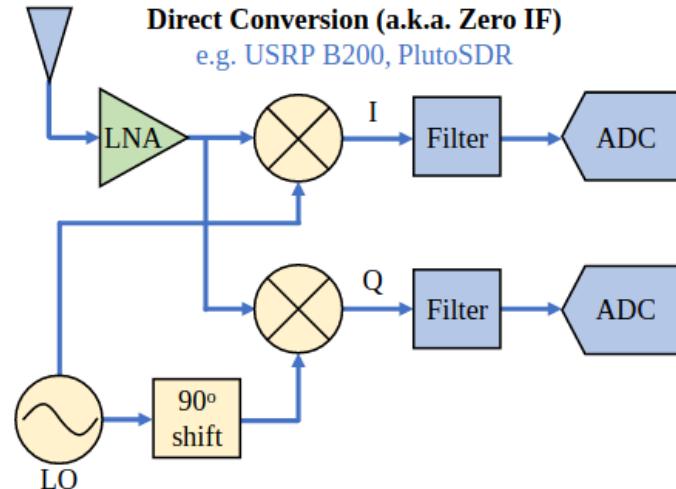
**Direct Sampling (a.k.a. Direct RF)**

very expensive ADC



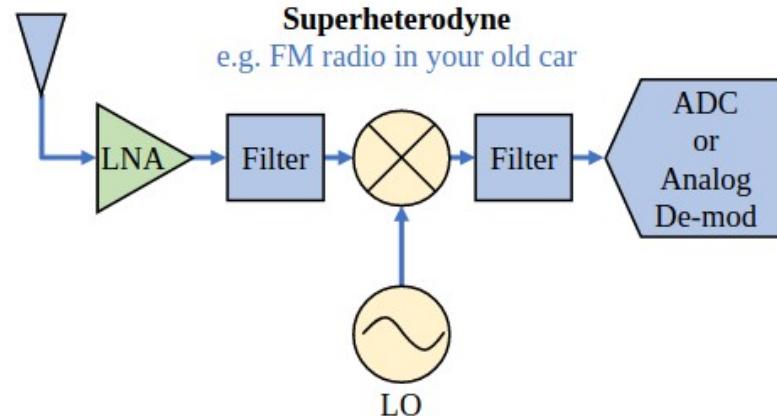
**Direct Conversion (a.k.a. Zero IF)**

e.g. USRP B200, PlutoSDR



**Superheterodyne**

e.g. FM radio in your old car



# SDR receiver: Direct Conversion

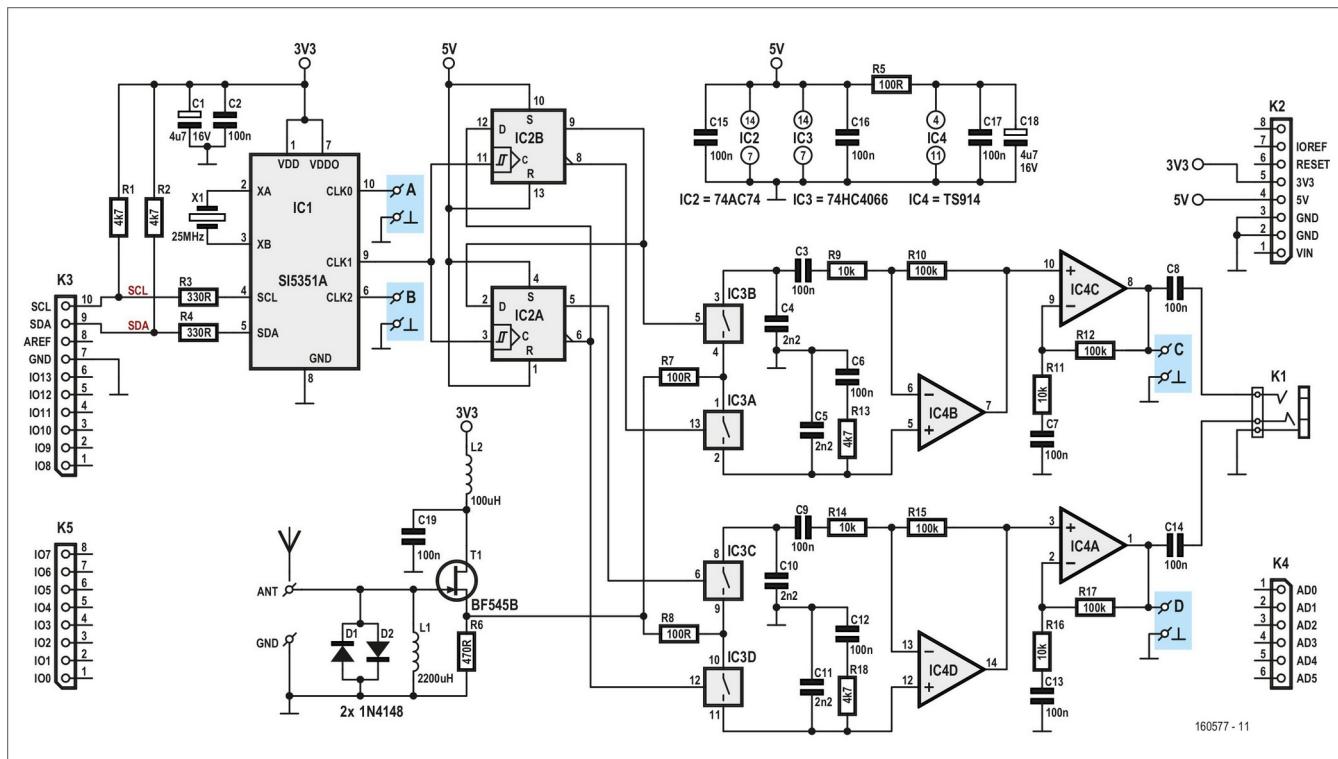
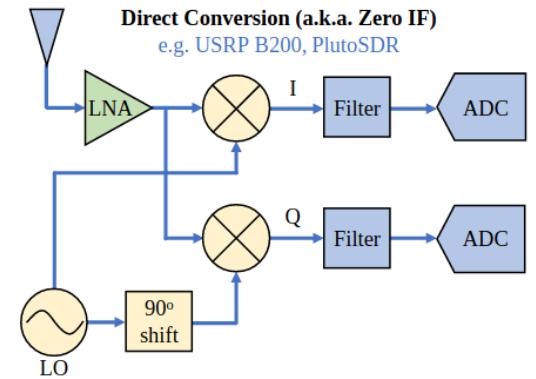


Figure 1. The new connections are highlighted in the schematic.



# SDR receiver: Direct Conversion (2)

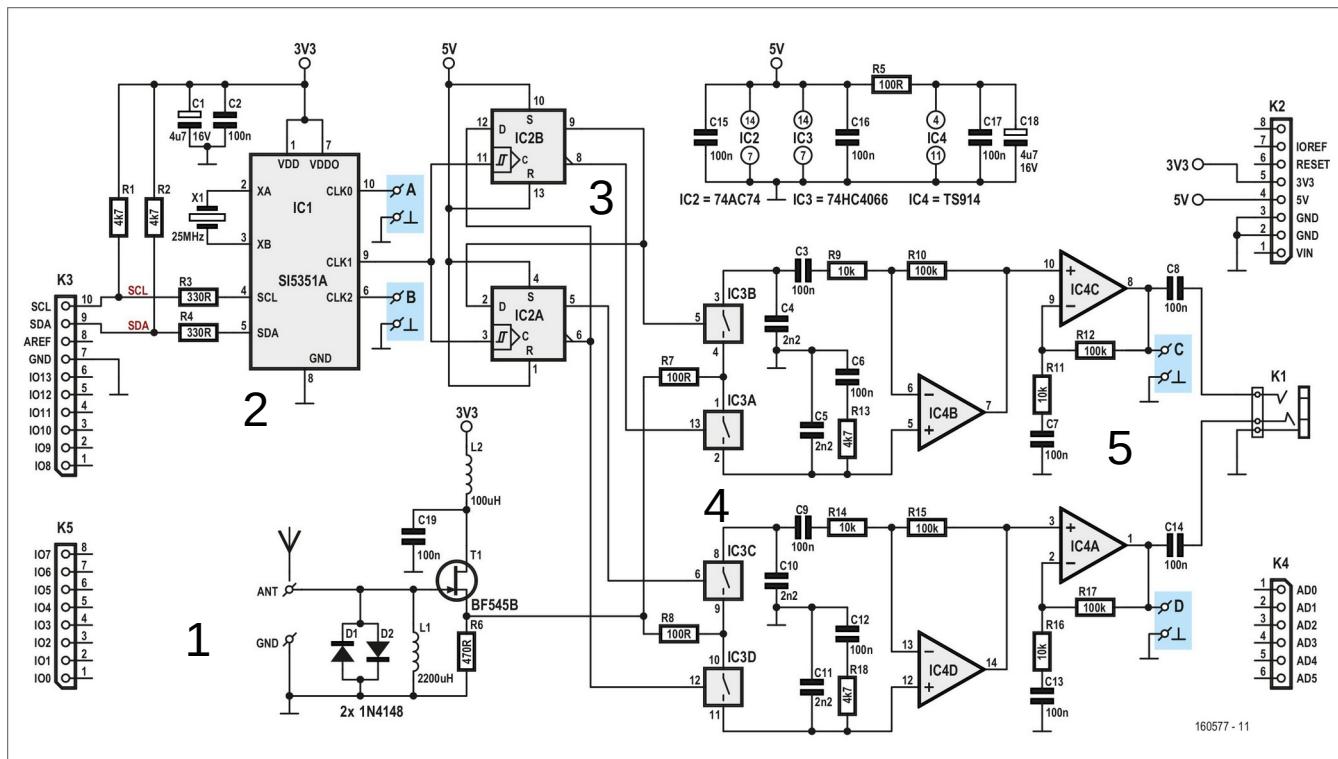
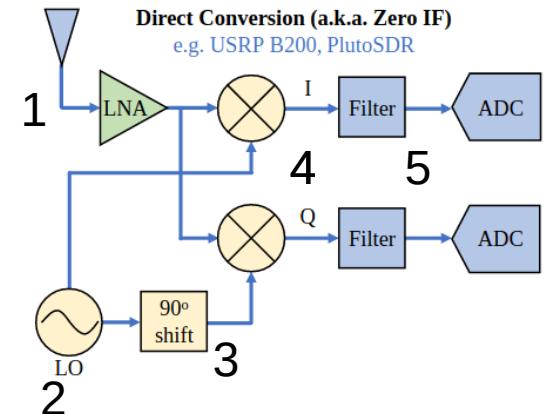
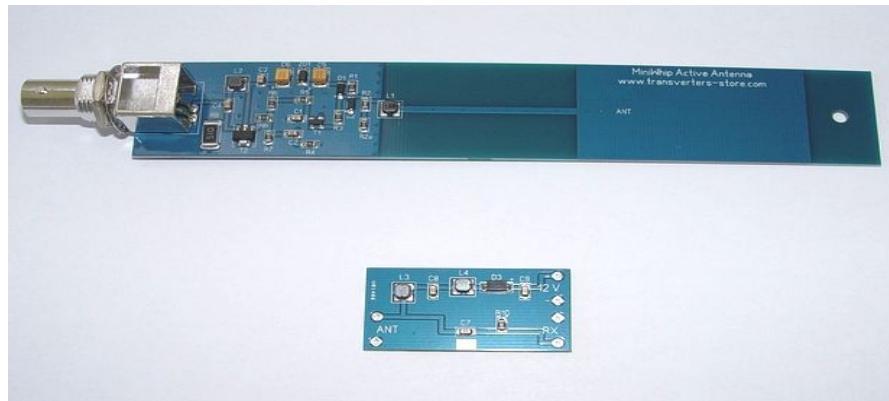


Figure 1. The new connections are highlighted in the schematic.

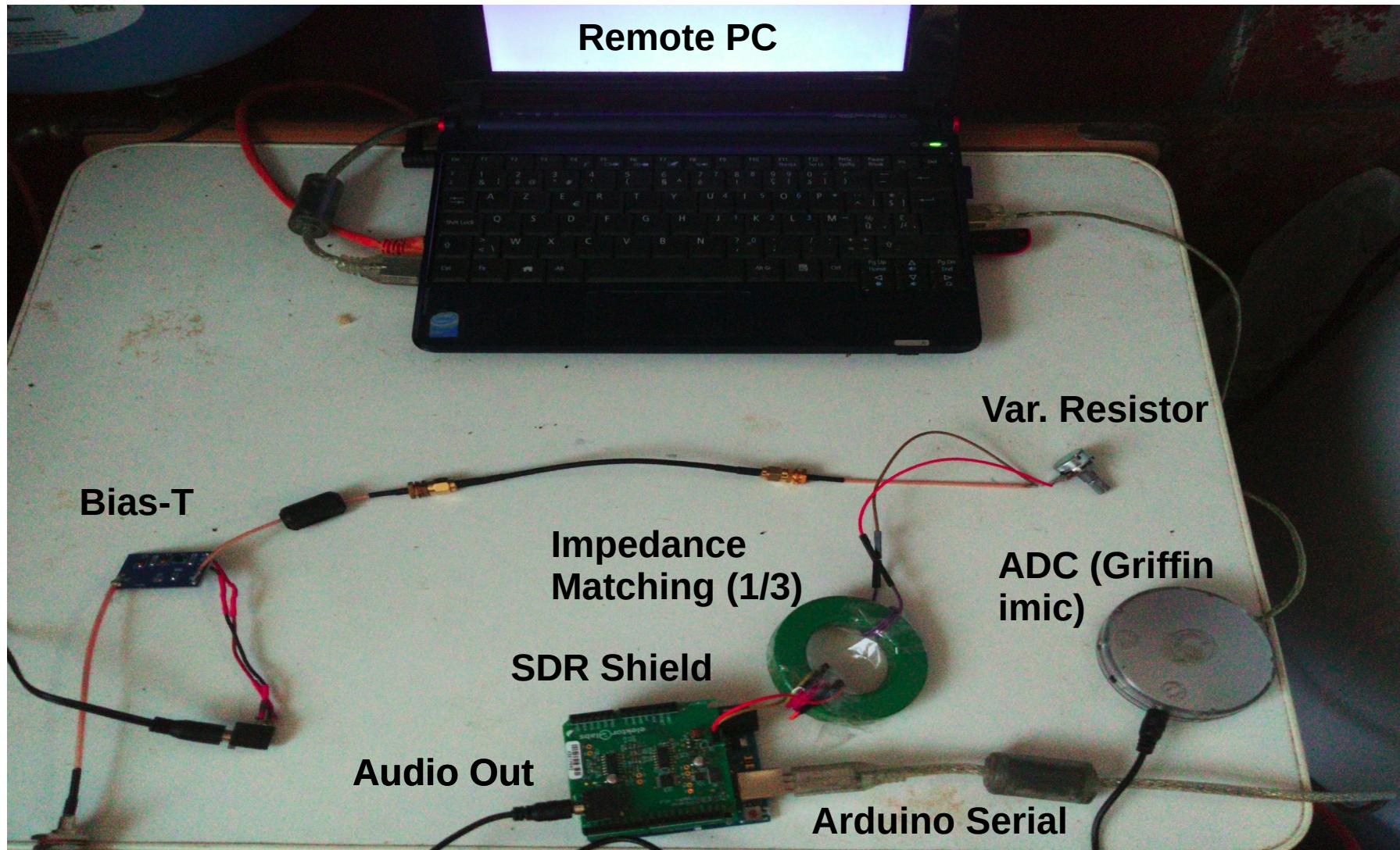


# My setup: Antenna



Antenna: active whip-antenna:  
<http://transverters-store.com/whippcb.htm>

# My setup: Receiver hardware

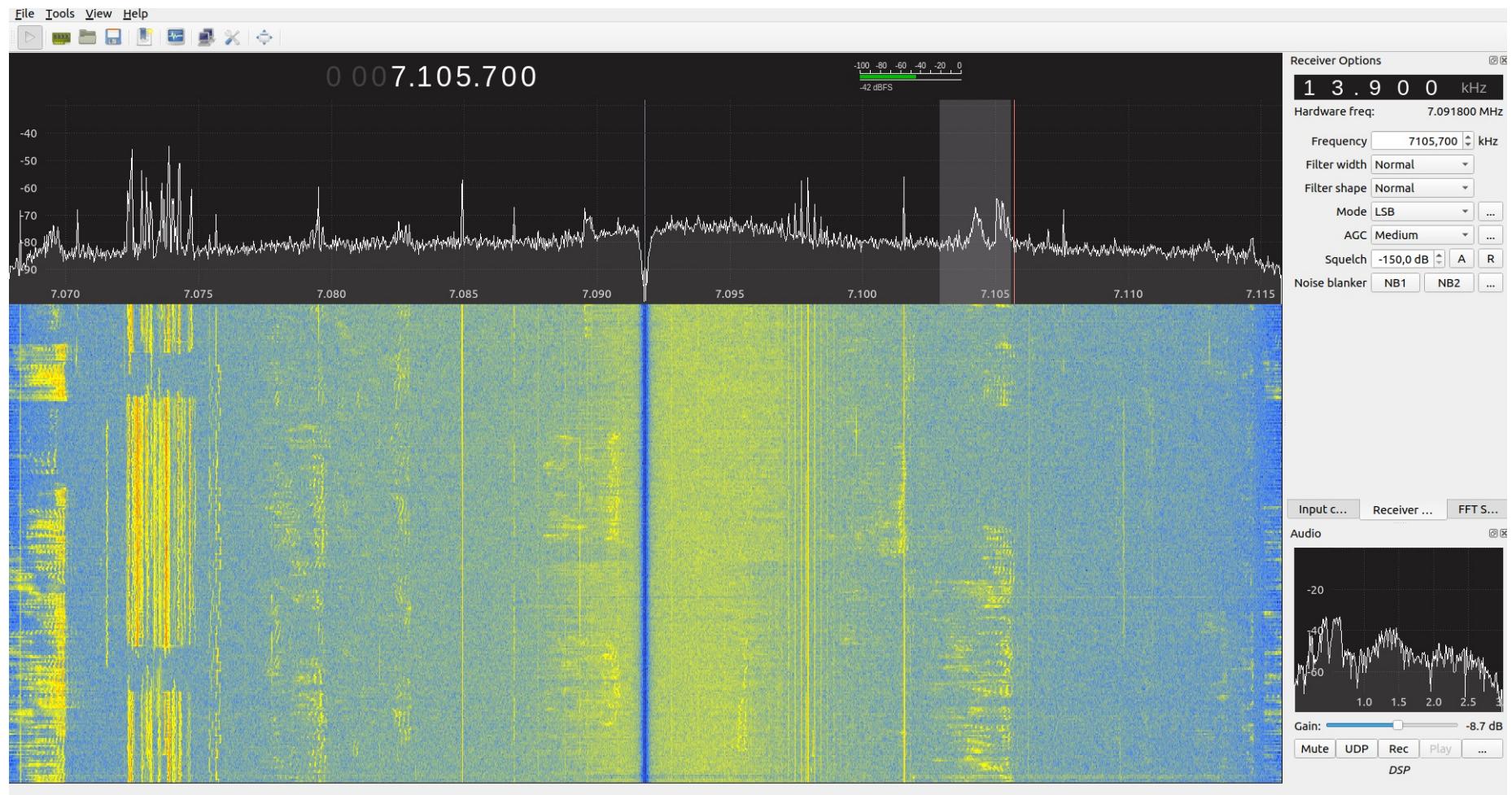


# My setup: Software

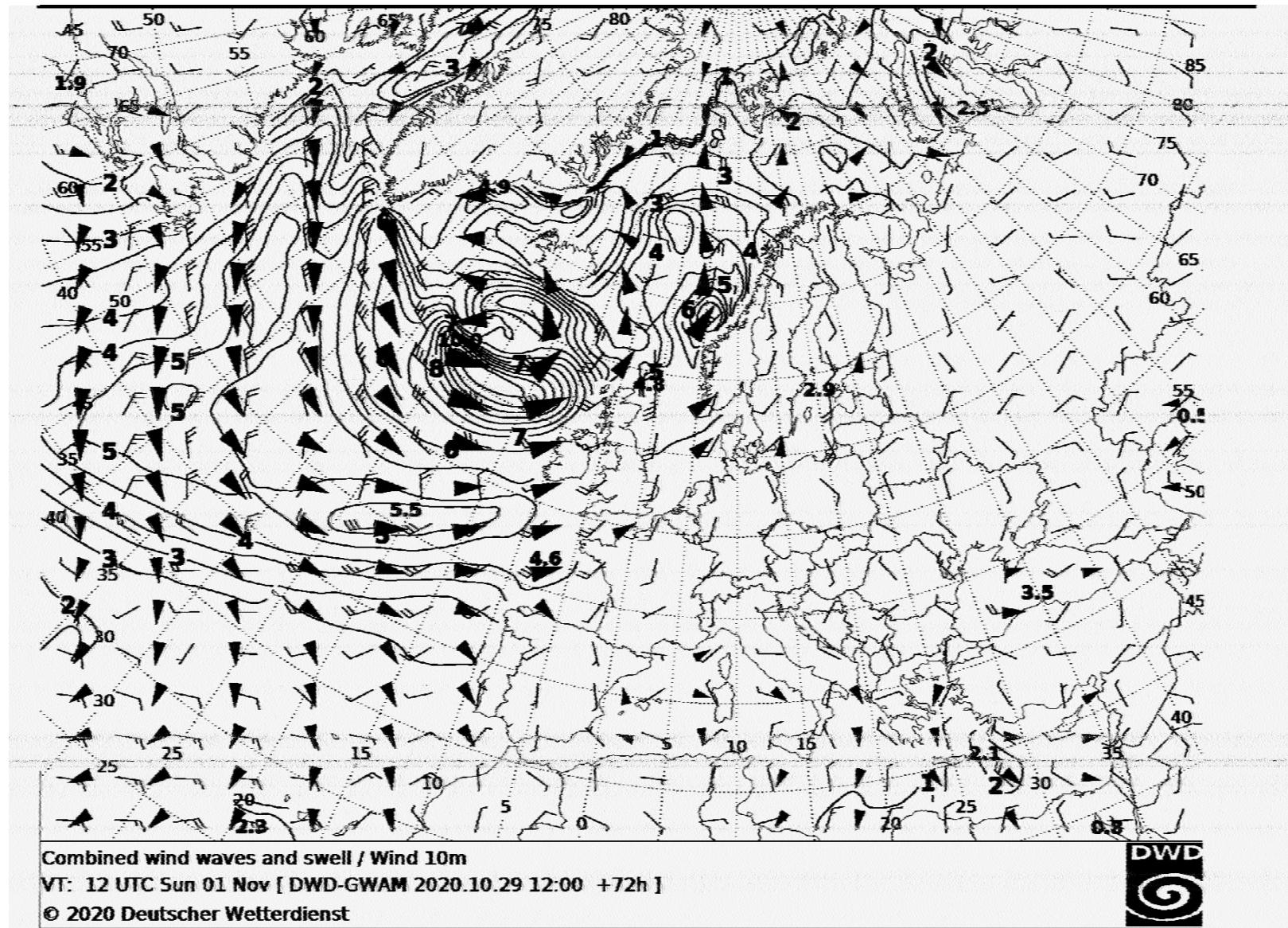
Linux based:

- arecord → import audio
  - pipe to FIFO (named pipe)
  - GQRX
- Fldigi
- Picocom (control frequency)

# And Does it work?



# And Does it work? (2)



# So all is perfect?

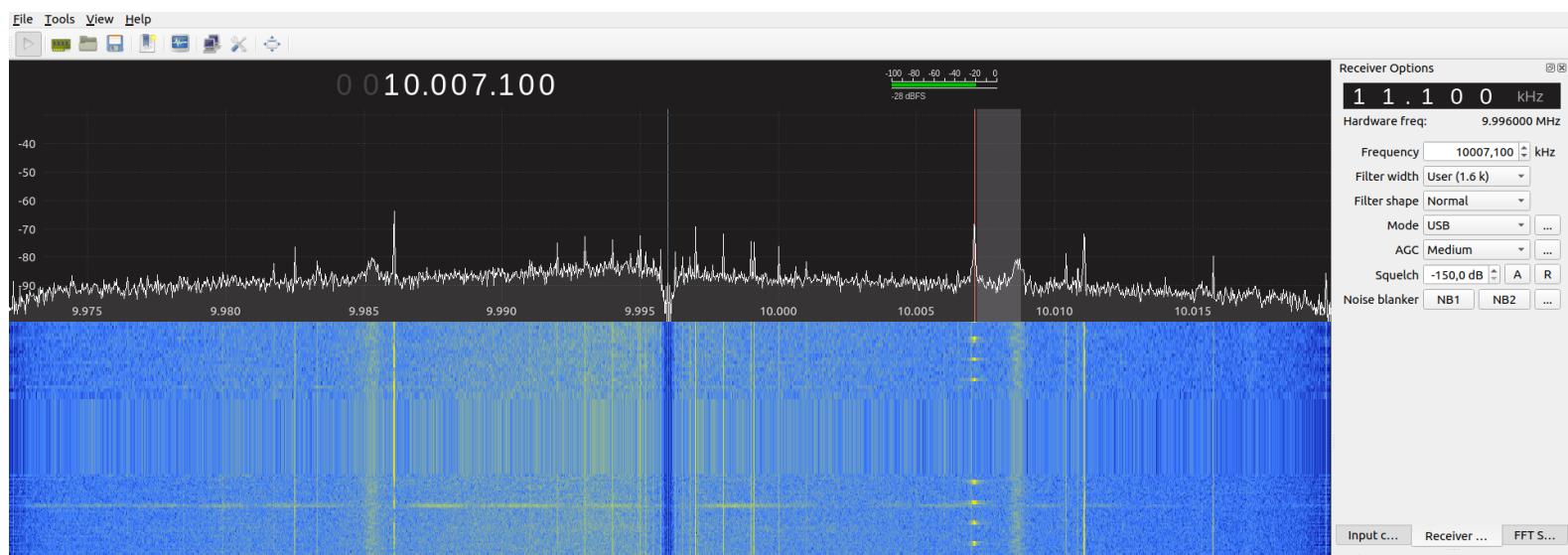
- Software:
  - Interface is not user-friendly (e.g. frequency-control is not integrated into application)
  - Windows / mac
  - Integrate into rtl\_tcp ?

# So all is perfect?

- Hardware:
  - Filtering in ADC needs to be done in ADC of the PC (very little filtering done on the shield) → make sure you have a good ADC
  - No hardware protection on DC overvoltage on the input (bias-T)
  - NO RF shielding: noise generated by arduino, by PC
    - Use external AudioDongle (ADC)

# So all is perfect?

- Hardware (2):
  - Frequency-offset (by > 11 KHz ) → need to be corrected



+11.6 KHz @ 4996 KHz

+11.1 KHz @ 9996 KHz

# So all is perfect?

- Sampling:
  - Sampling at freq.  $x$ , will also sample at uneven harmonics of that freq.

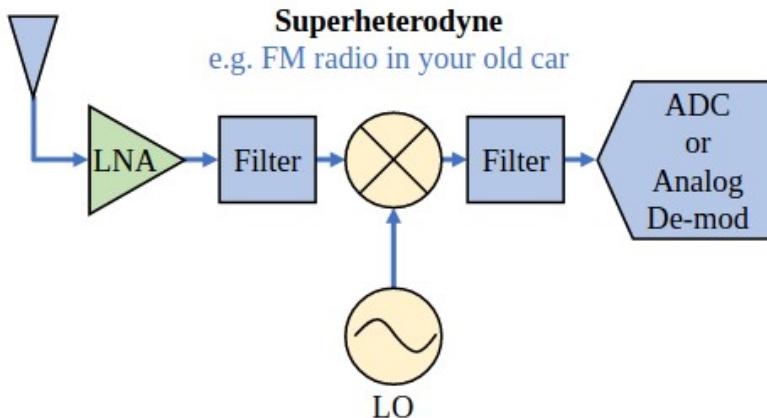
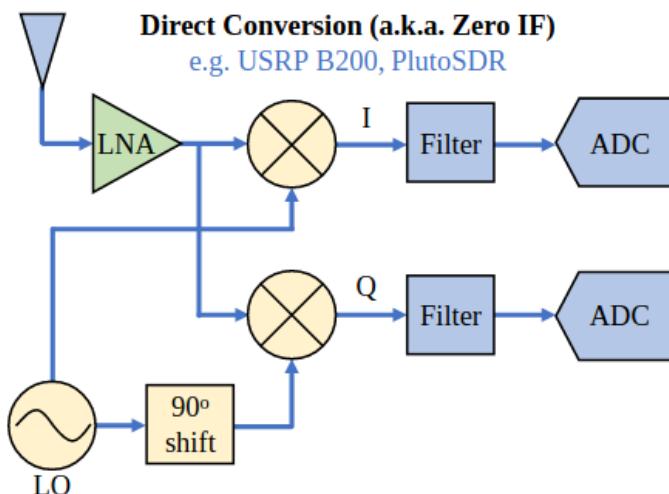


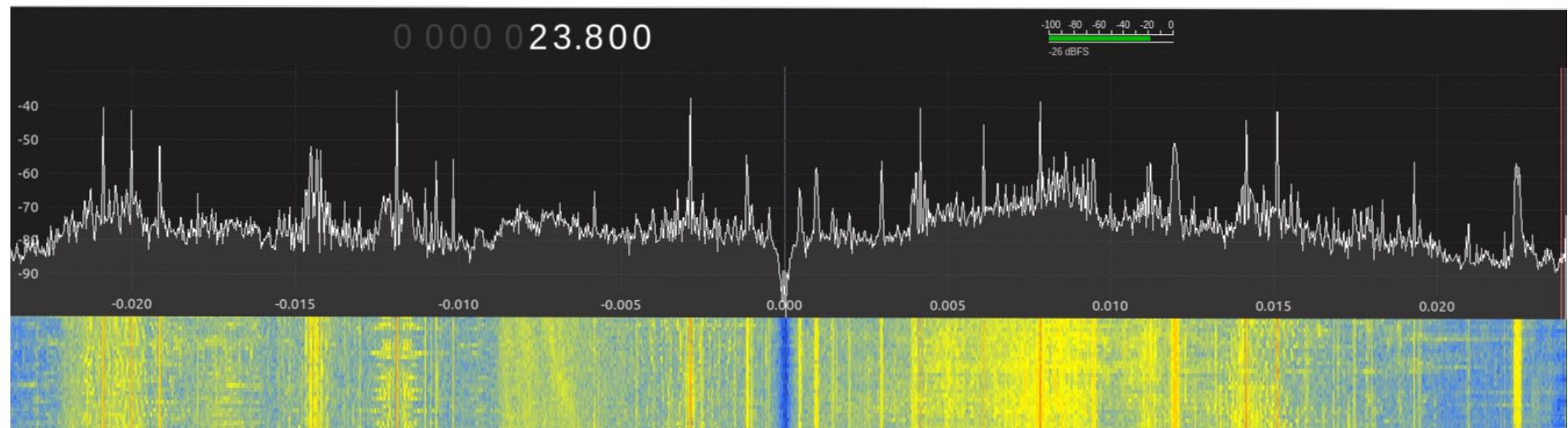
Image that the LO oscillator is a square wave

# So all is perfect?

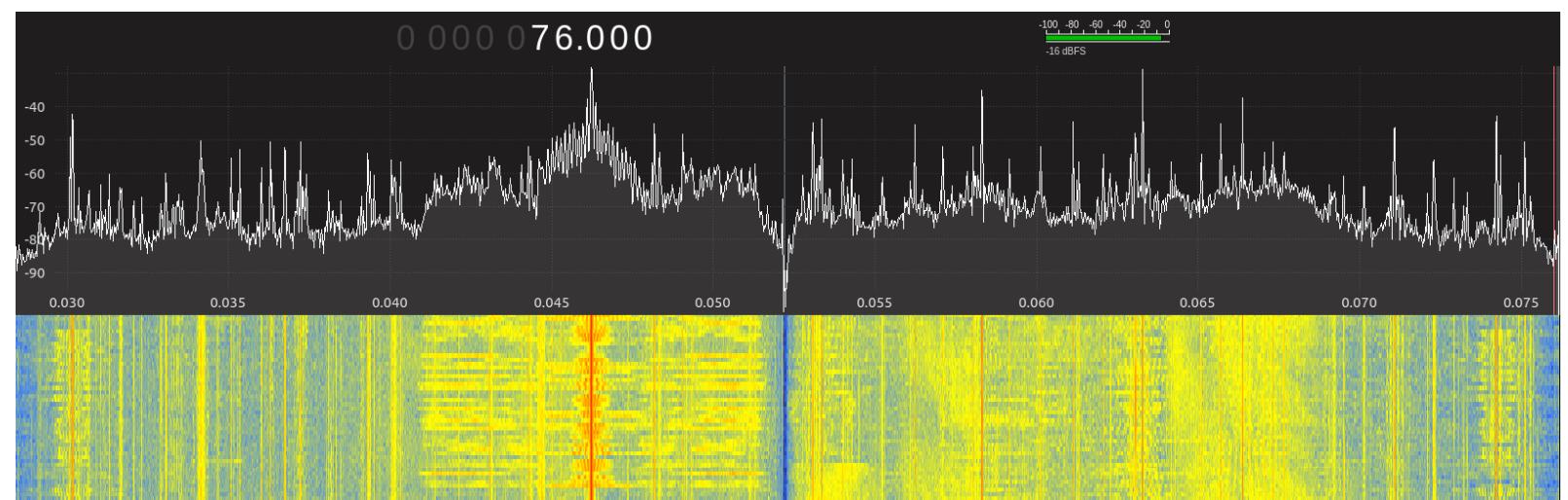
- Tuned to 1 MHz:
  - 976 – 1024 KHz
  - 2976 – 3024 KHz
  - 4976 – 5024 KHz
  - ...

# Sampling harmonics

302 KHz

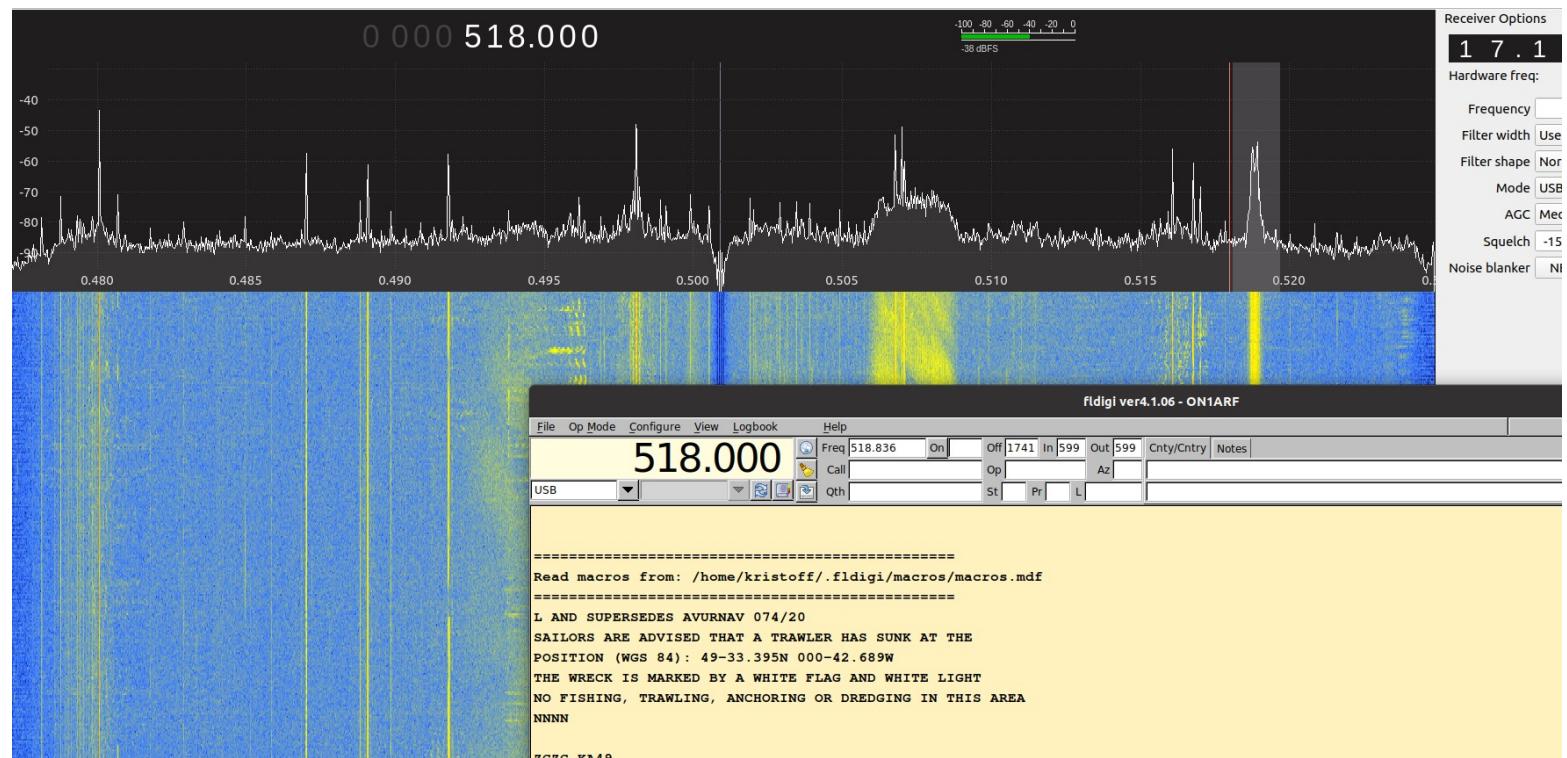


76 KHz



# Sampling harmonics (2)

518 KHz (tuned to 512 KHz)



# Sampling harmonics (3)

## Solutions

- (Selectable) Input filters → look lima SDR
- Selective Antenna (magnetic loop)
- Increase sampling-rate
  - e.g. RTL-dongle: 2.4 Msamples/sec (1.2 MHz bandwidth)
  - Tune to 1.2 MHz (freq. range: 0 – 2.4 MHz)
  - Next harmonic: 3.6 MHz → outside broadcast band + a lot easier to filter

# Conclusion of the Elektor SDR Shield (so far)

Interesting learning Experience

- Works pretty good for certain applications (e.g. HF)
- Can be made better
  - Input filters / selective antenna
  - RF shielding cases
  - DC overvoltage protection
  - Better software integration

# BE.SDR Meetup 3: Agenda

- 20:00
  - Question time + Introduce yourself
  - Some news about BE.SDR
- 20:30
  - Solution of CTF1 and CTF2
  - The elektor SDR receiver shield
    - “Learning SDR hardware: A bare minimum SDR receiver”
- 21:40
  - Open discussion on BE.SDR

# Other ideas for BE.SDR

Separate meetings for

- Encoding / decoding software (e.g. DGPS decoder, amateur-radio protocols)
  - For people with software background
- CTFs
  - Best way to get started with GNU radio