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 feelback!
  - 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

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

Online Python Console

Quick search

Go

PySDR: A Guide to SDR and DSP using Python

by Dr. Marc Lichtman

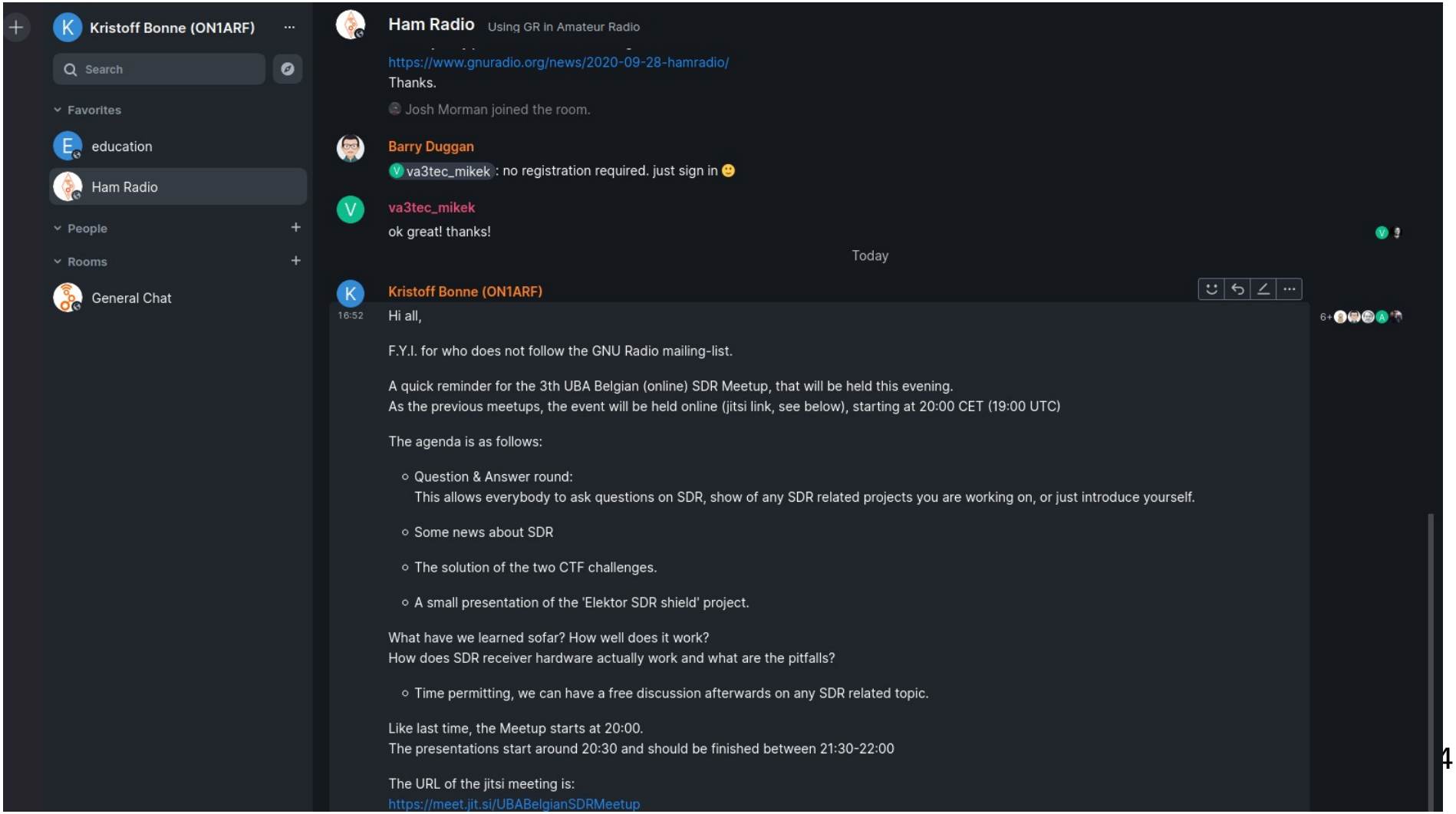
PySDR

“SDR explained for Programmers”

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

GNU Radio chat

https://chat.gnuradio.org/



Monthly GNU Radio Amateur Radio Meeting

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

Contents [hide]

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 & K0ZEL

Brief walk-through of Simulation example: FSK [edit]

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

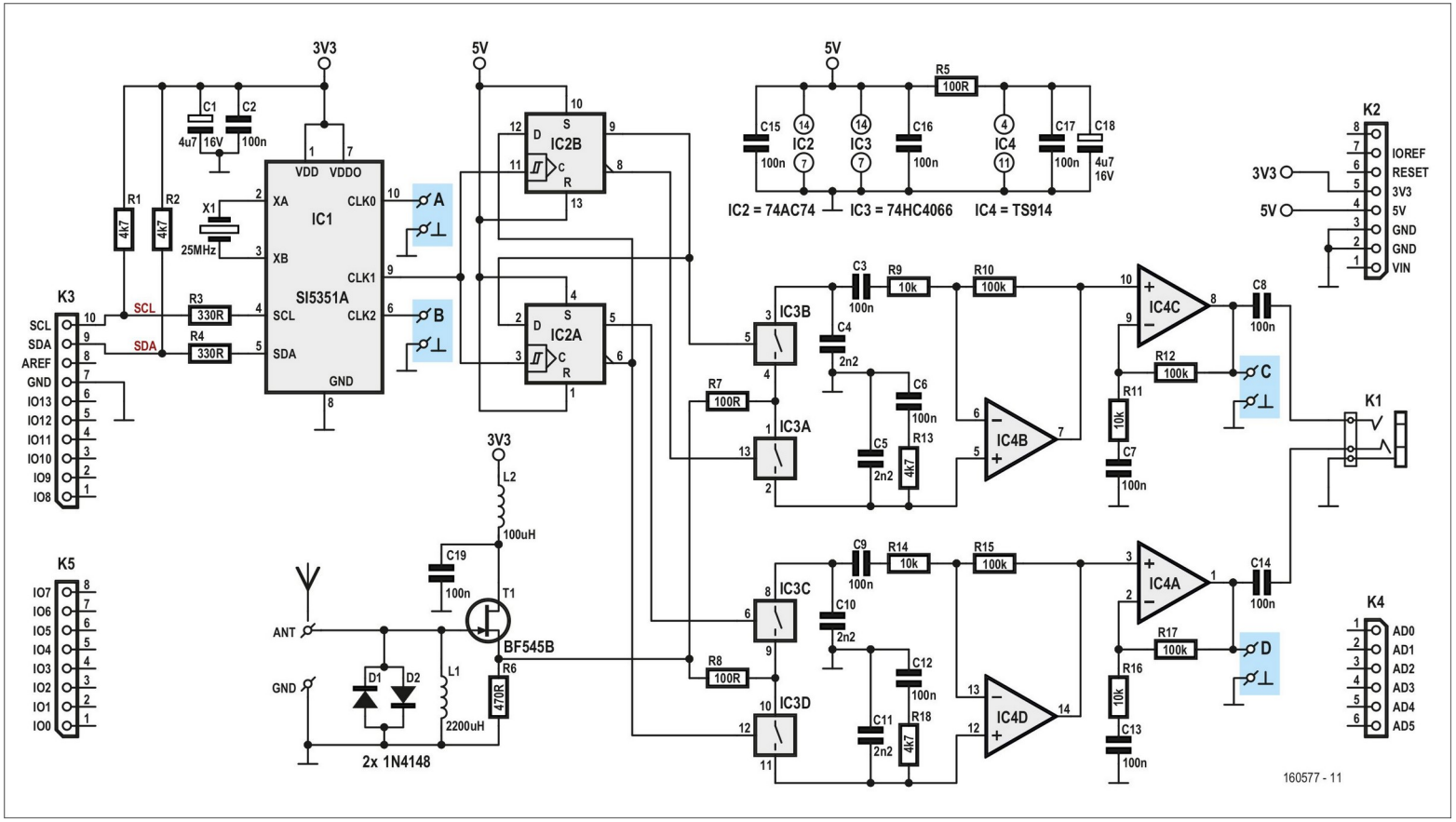
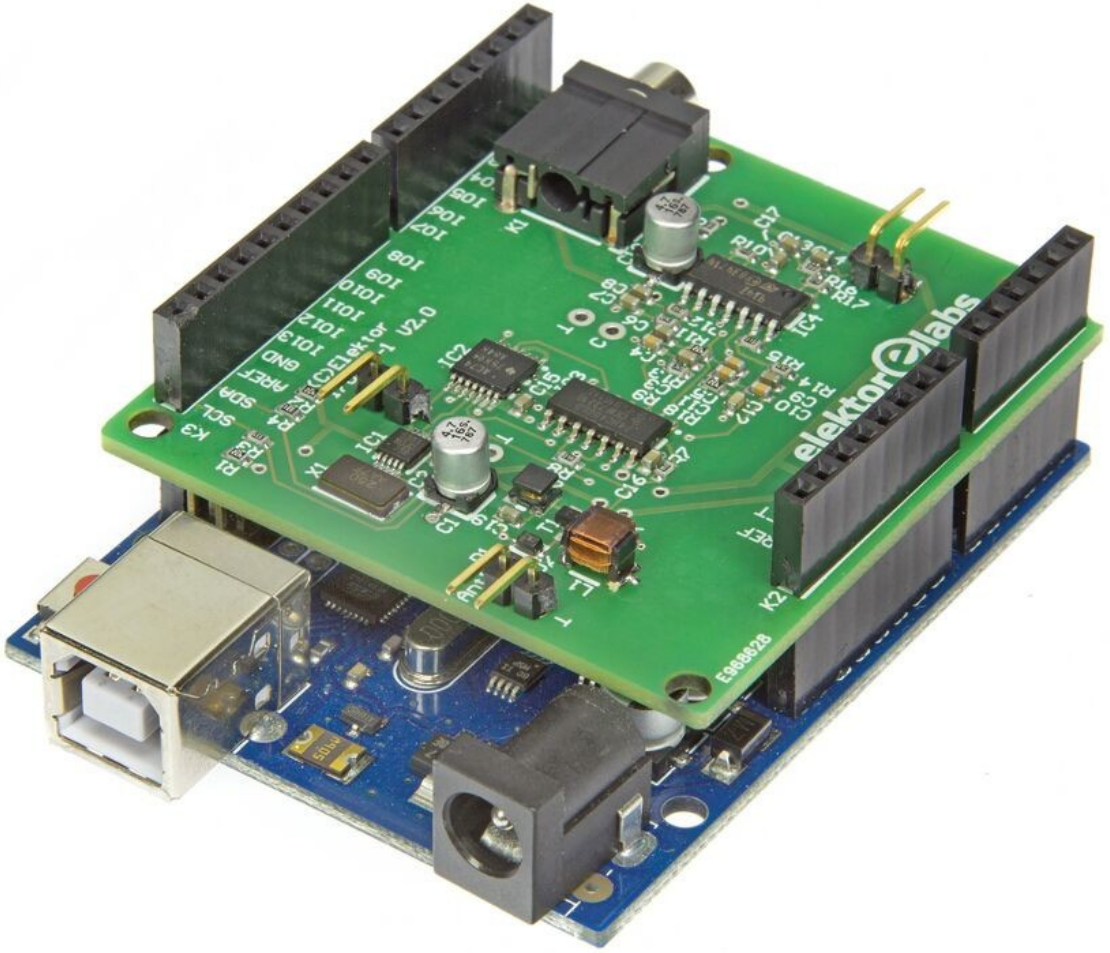
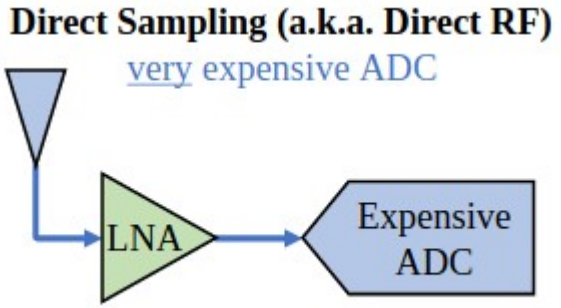


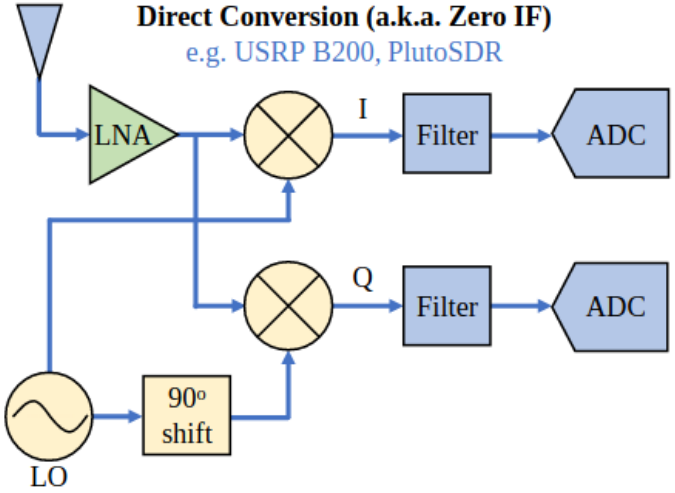
Figure 1. The new connections are highlighted in the schematic.

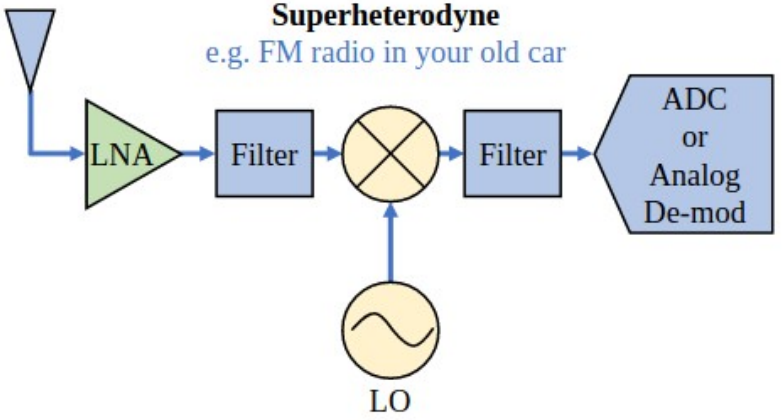
the elektor SDR Shield: On arduino



SDR receivers: 3 types

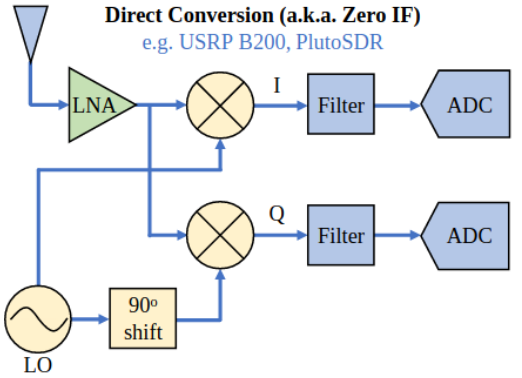






https://pysdr.org/content/sampling.html#receiver-architectures

SDR receiver: Direct Conversion



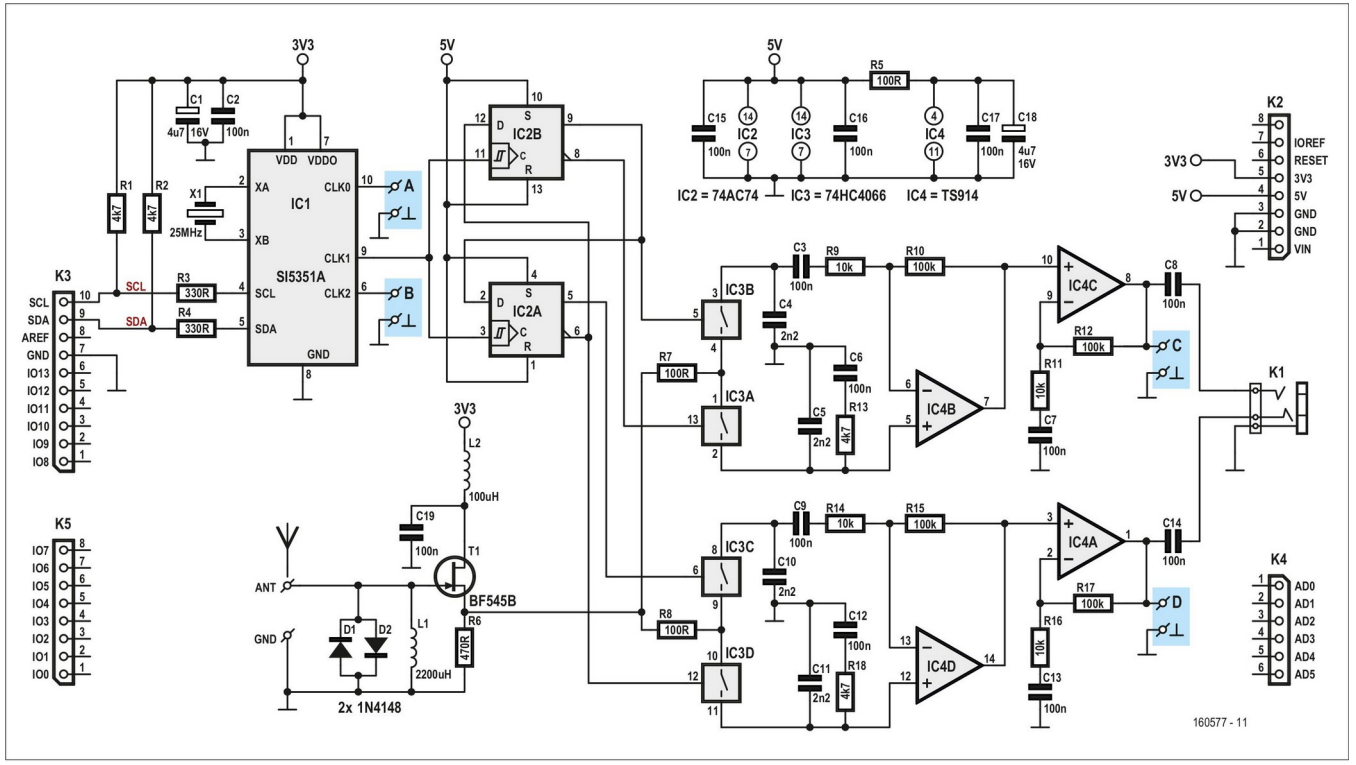


Figure 1. The new connections are highlighted in the schematic.

SDR receiver: Direct Conversion (2)

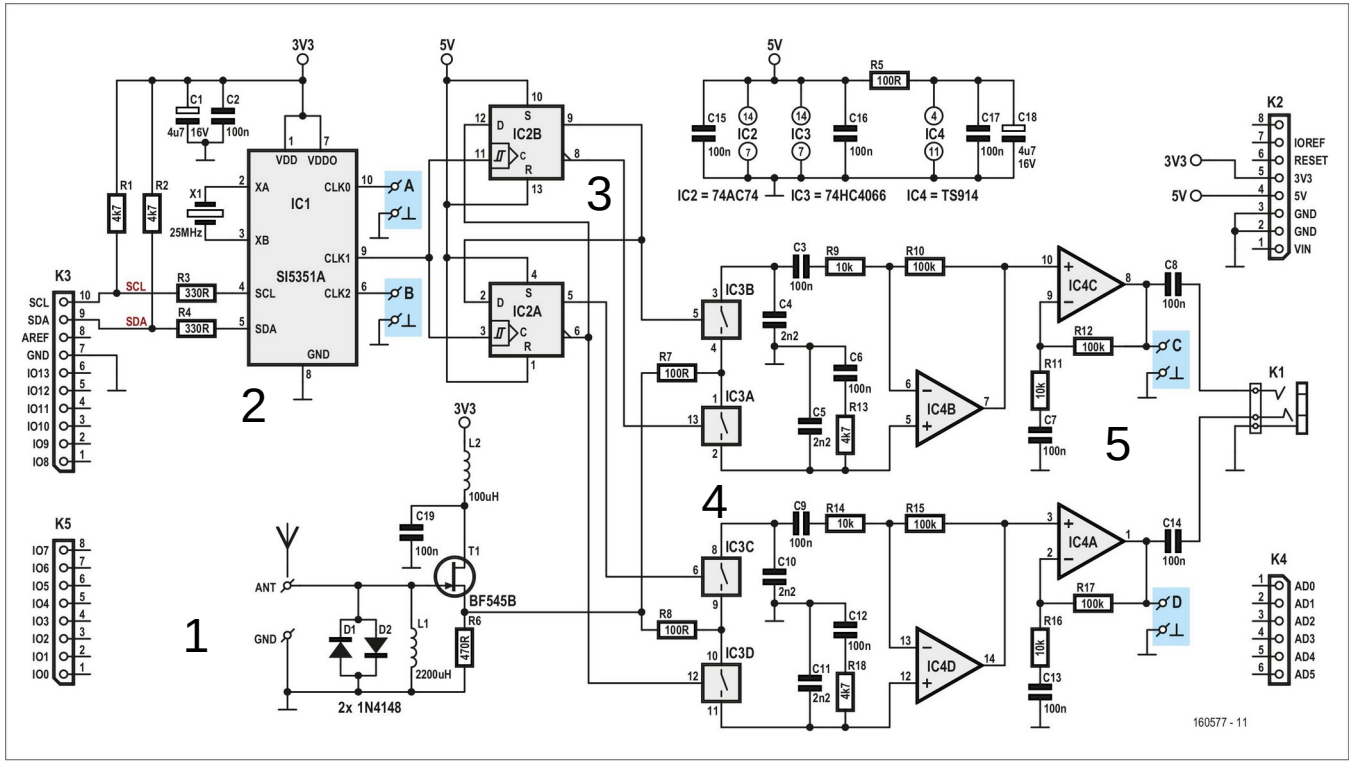
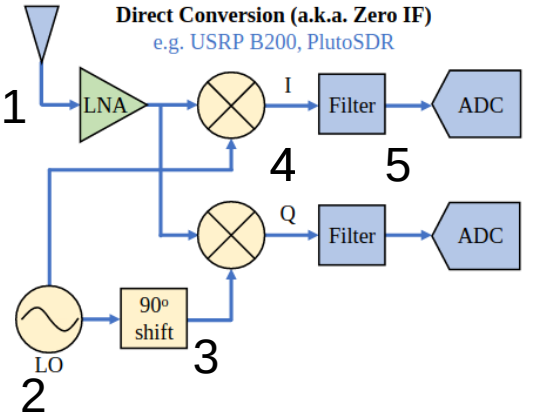
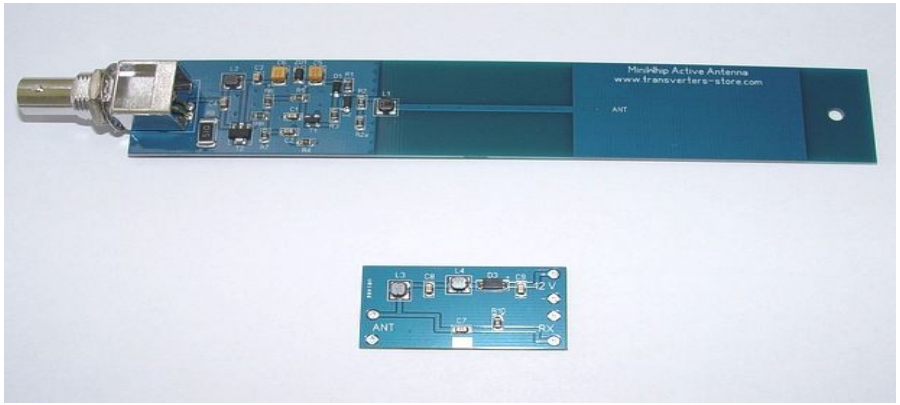


Figure 1. The new connections are highlighted in the schematic.

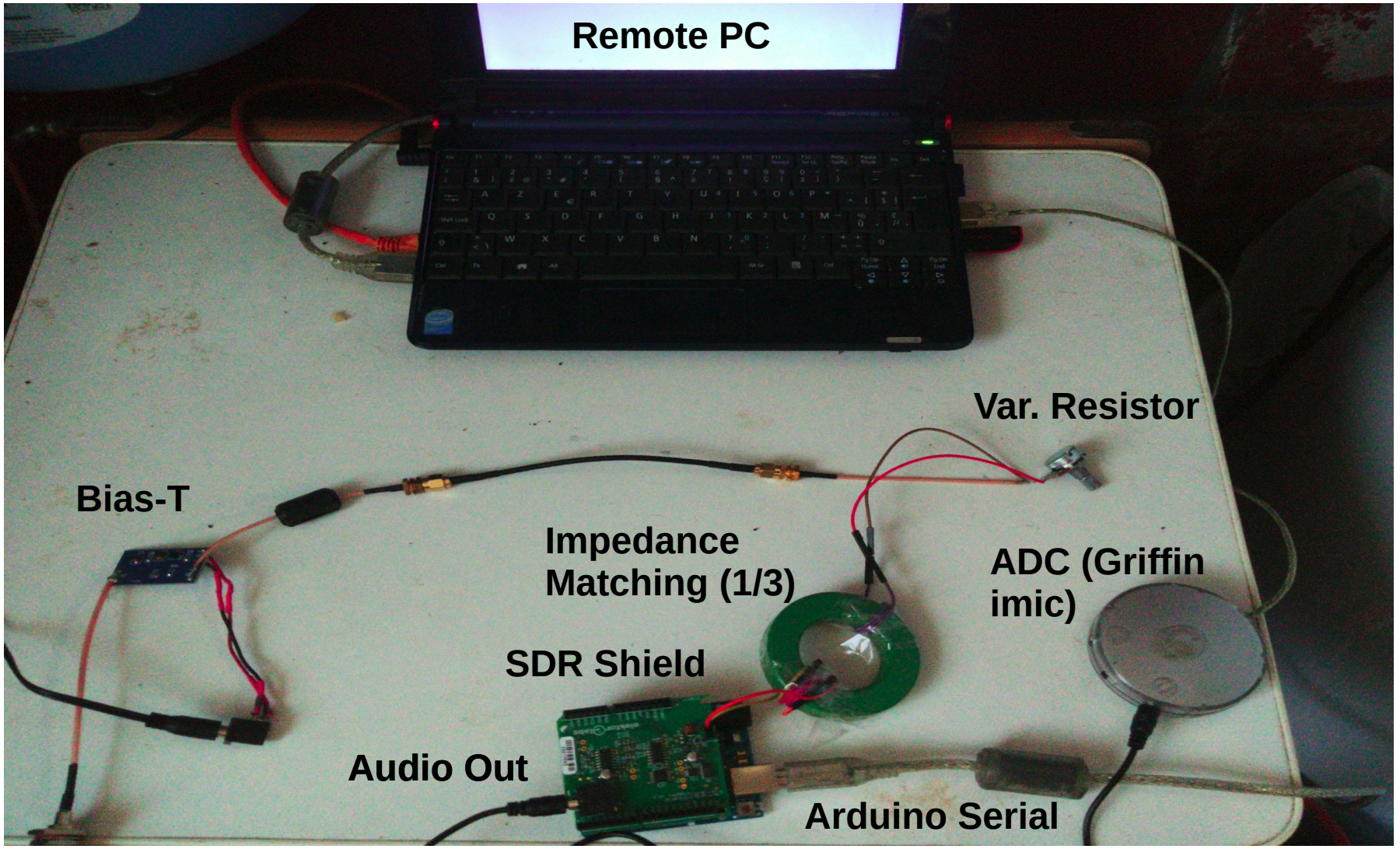


My setup: Antenna



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

My setup: Receiver hardware

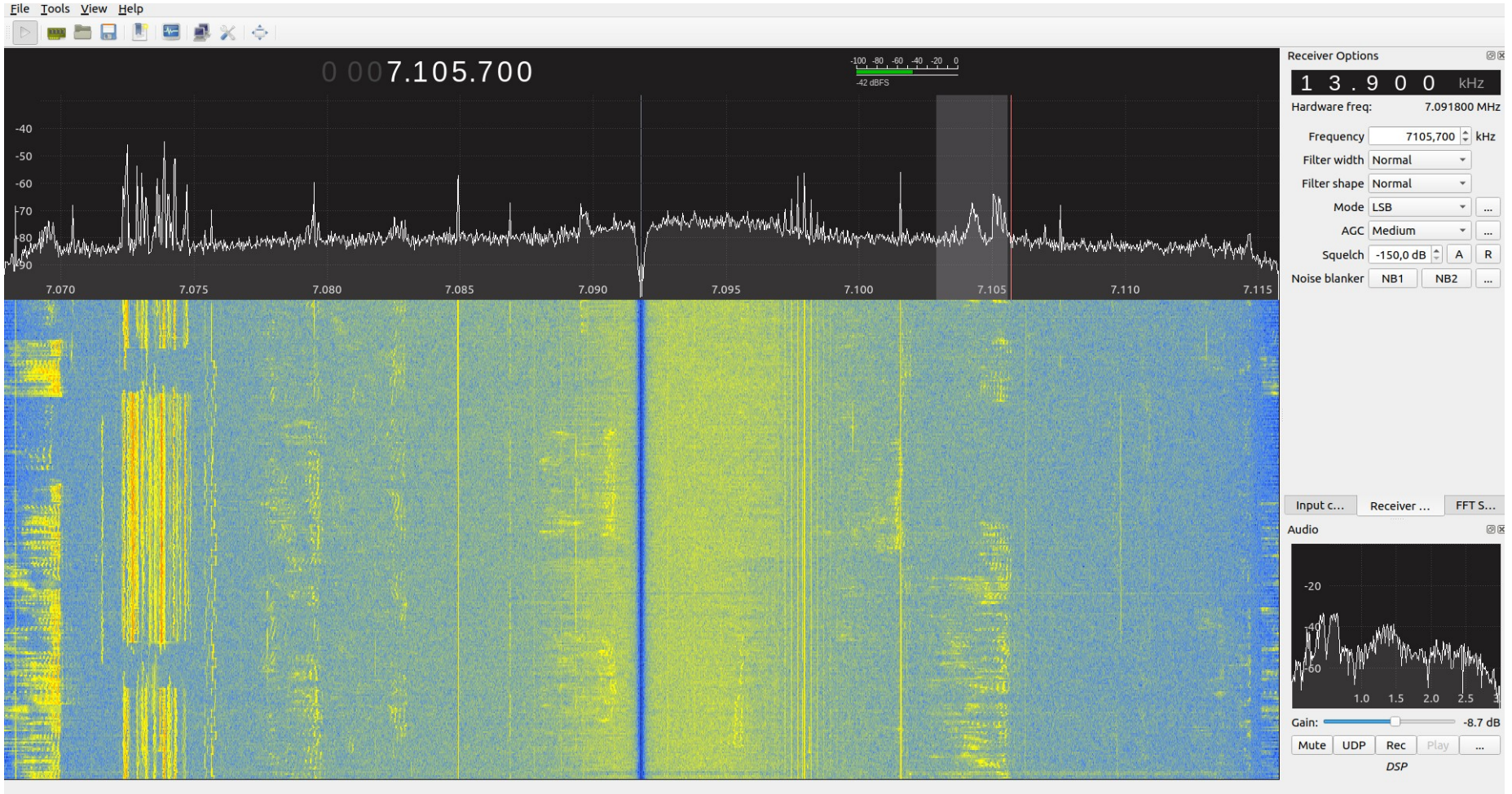


My setup: Software

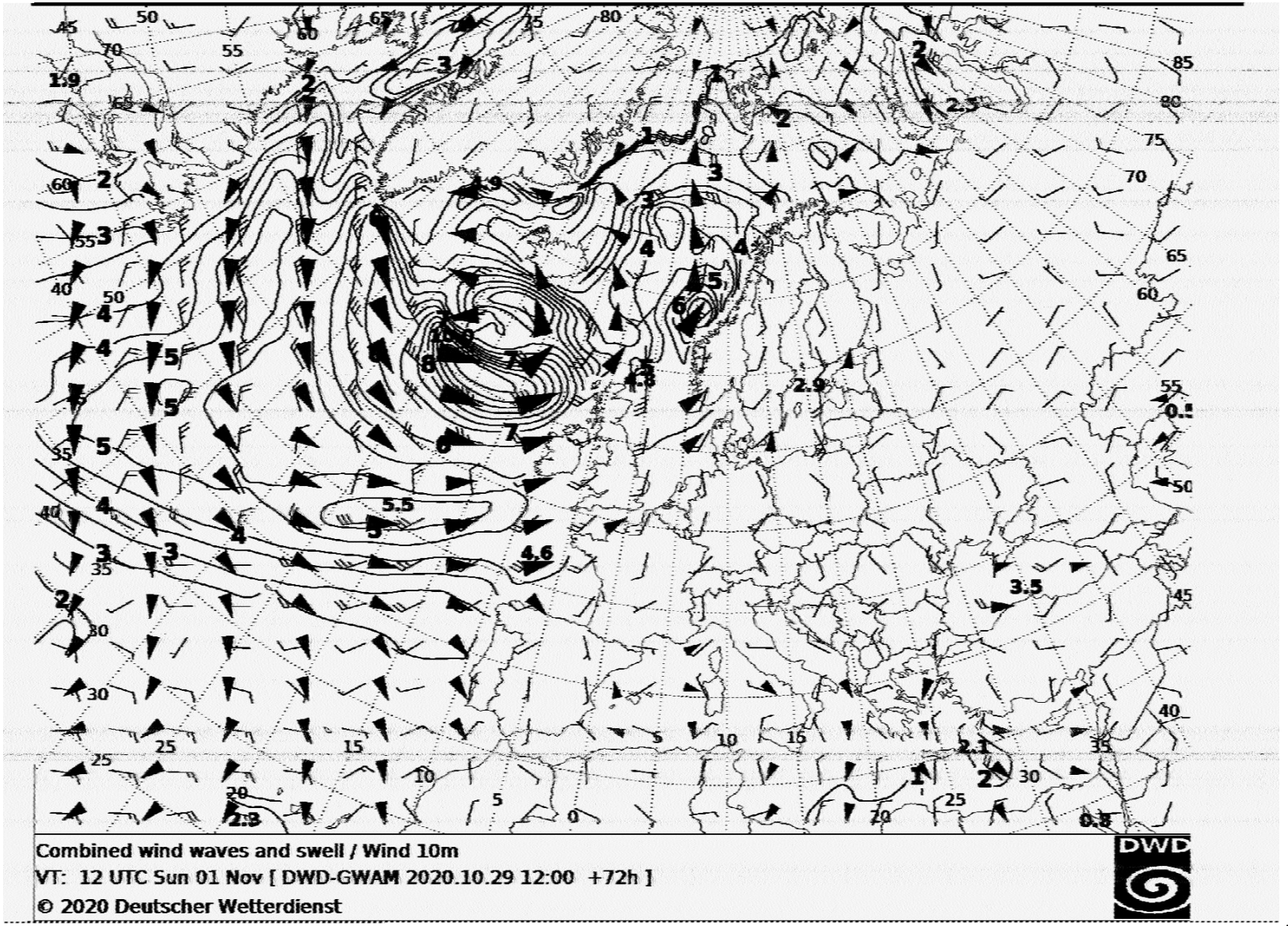
Linux based:

- 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 ?

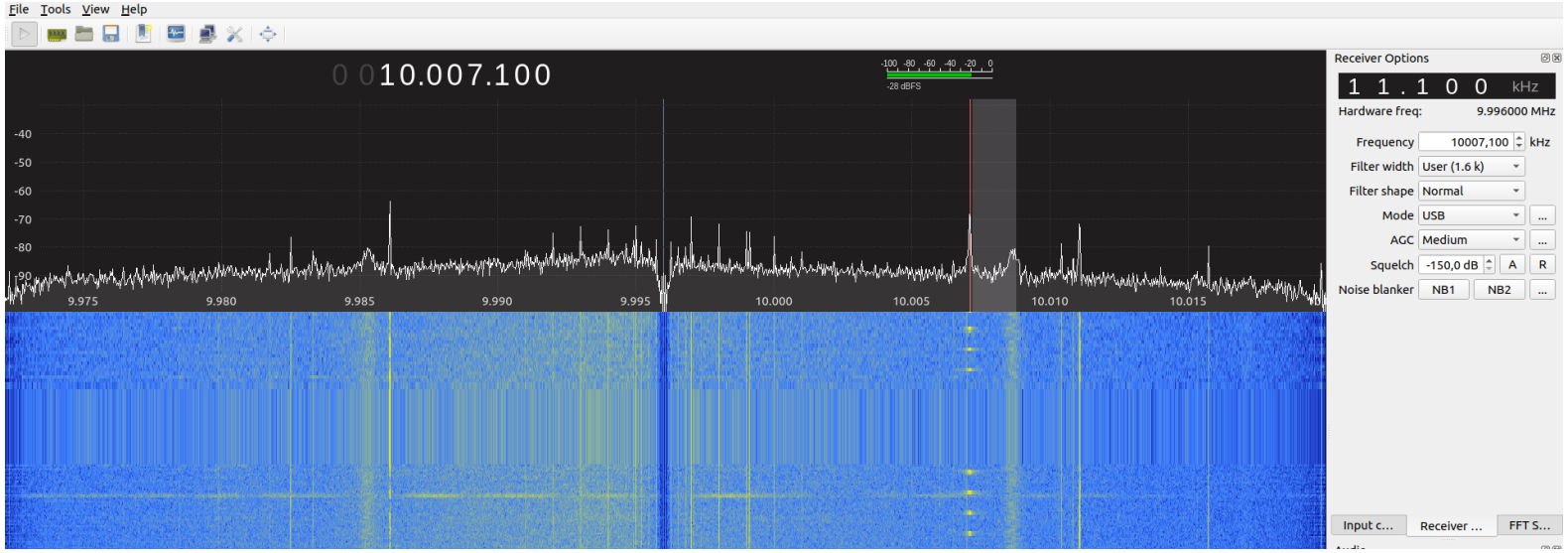
So all is perfect?

- 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

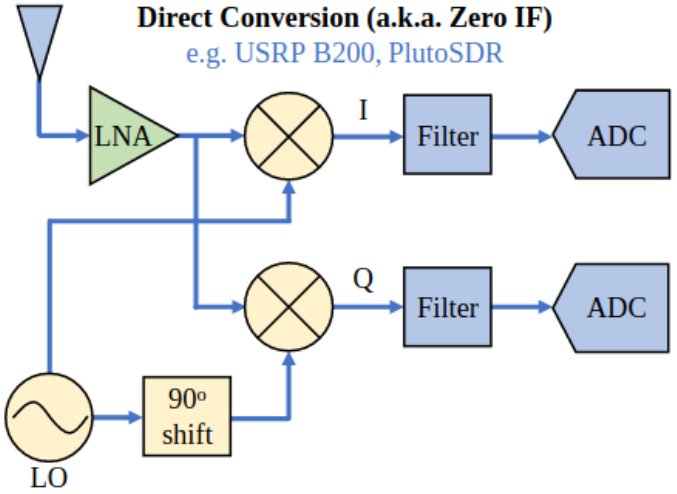


+11.6 KHz @ 4996 KHz

+11.1 KHz @ 9996 KHz

So all is perfect?

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



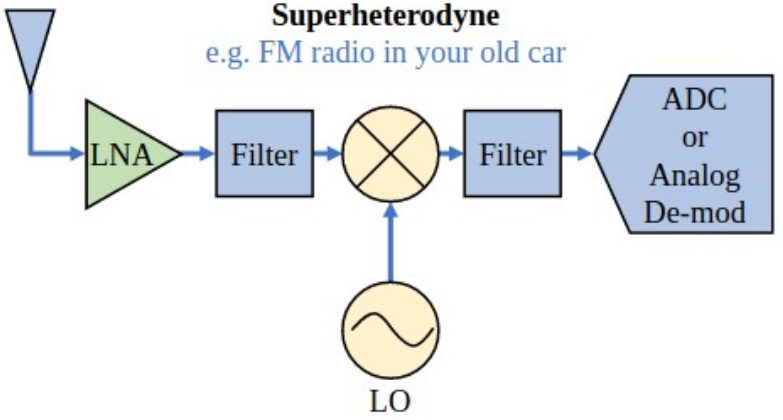


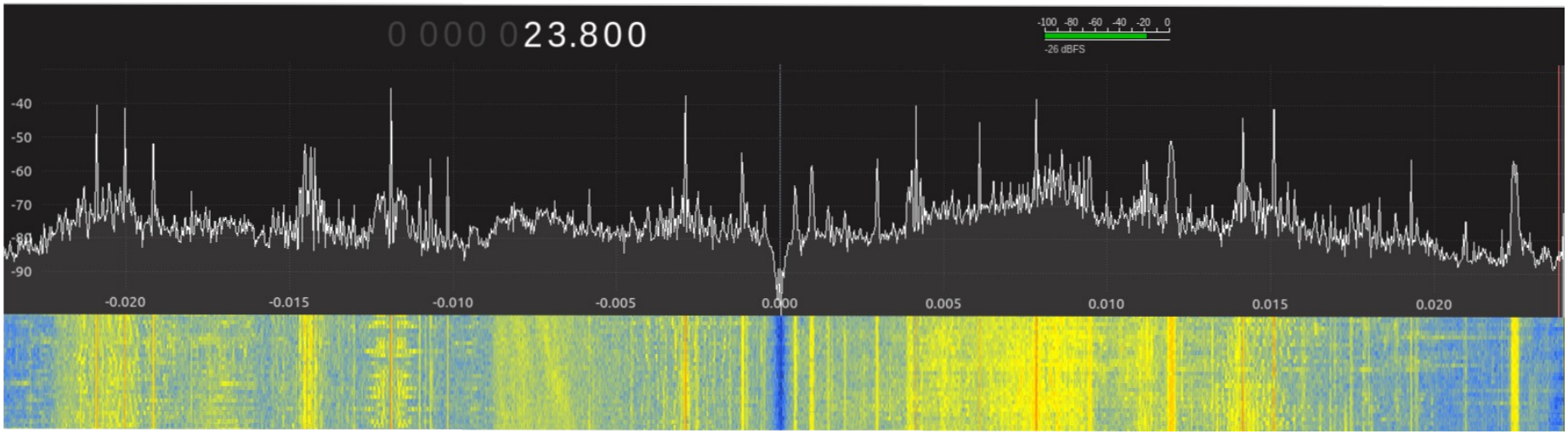
Image that the LO oscilator is a square wave

So all is perfect?

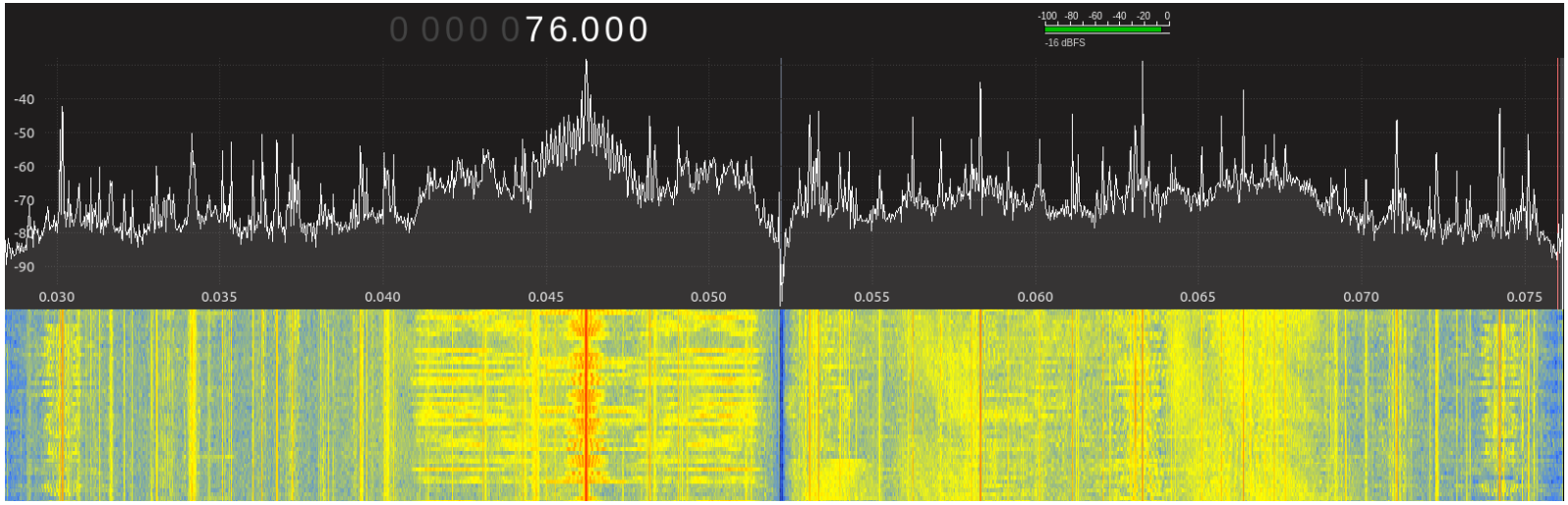
- Tuned to 1 MHz:
  - 976 – 1024 KHz
  - 2976 – 3024 KHz
  - 4976 – 5024 KHz
  - ...

Sampling harmonics

302 KHz

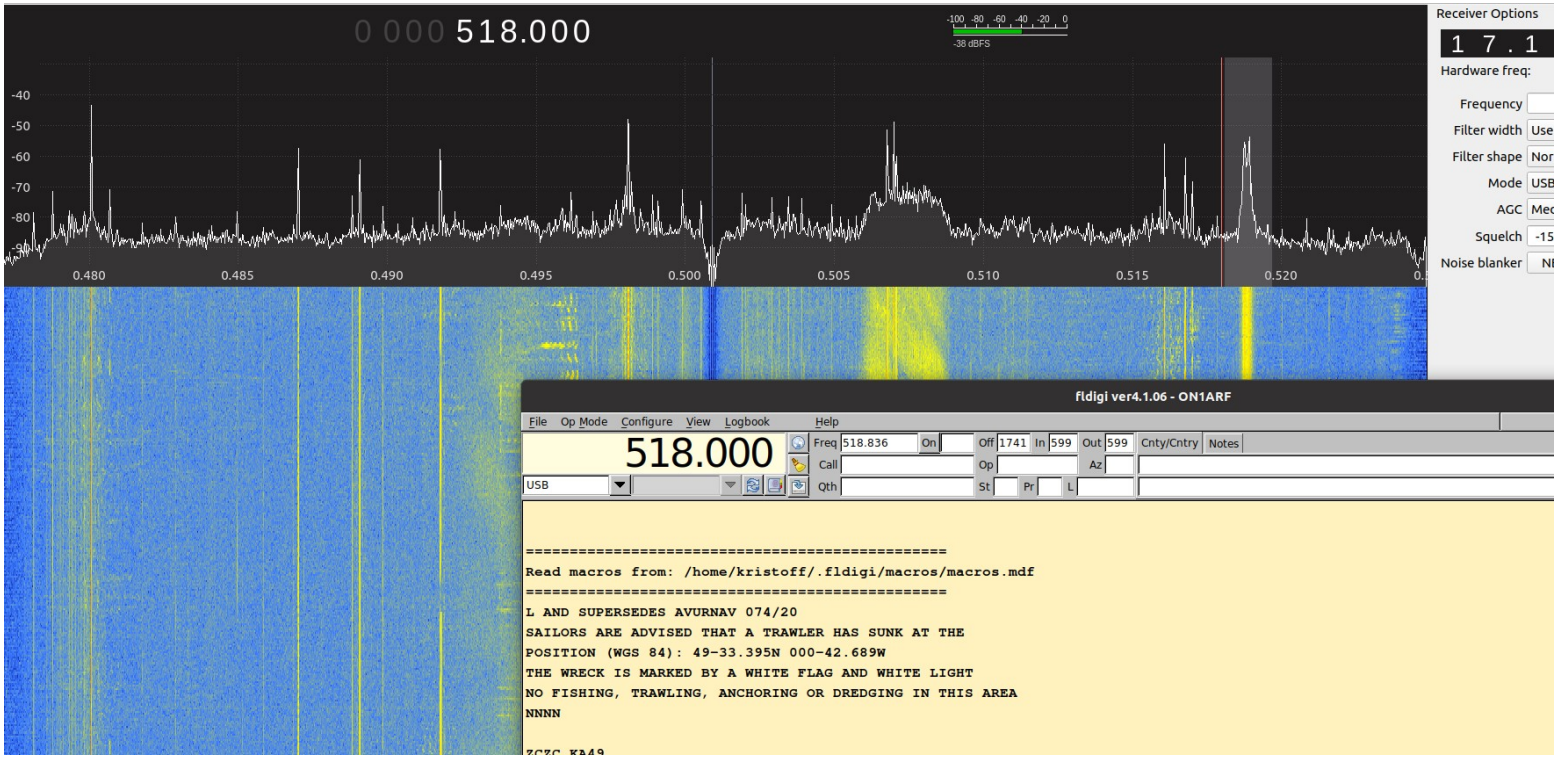


76 KHz



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

Conclussion 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

Seperate 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