UBA Belgian SDR Group

# Workshop Getting started with GNU Radio for CTFs

Kristoff Bonne (ON1ARF)
13/11/2020

# BE.SDR GR workshop 1

- Introduction to GNU Radio
- Looking into GRC2 (AM demod - DCF 77)
- (If time remaining)
  - GRC2 long-dcf77
  - GRC1

# Introduction to GNU Radio

- What is GNU Radio and GNU Radio Companion?
- General Overview of GRC
- Different types of block
- Datatypes

- How to get started

# Practical Issues

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

- Use a headset
- Best browsers:
  - chrome / chromium / ...
  - Firefox
- Use Screen-sharing

# Legal

# GNU Radio and GRC

GNU Radio (GR)

- Framework for signal-processing
- Uses python as wrapper around C++ code
- Can be used for any kind of signals: RF, AF, DSP, visualisation, ...

GNU Radio Companion (GRC)

- Graphical Usertool to create GR “flowgraphs”
- Creates python or C++ on the backend

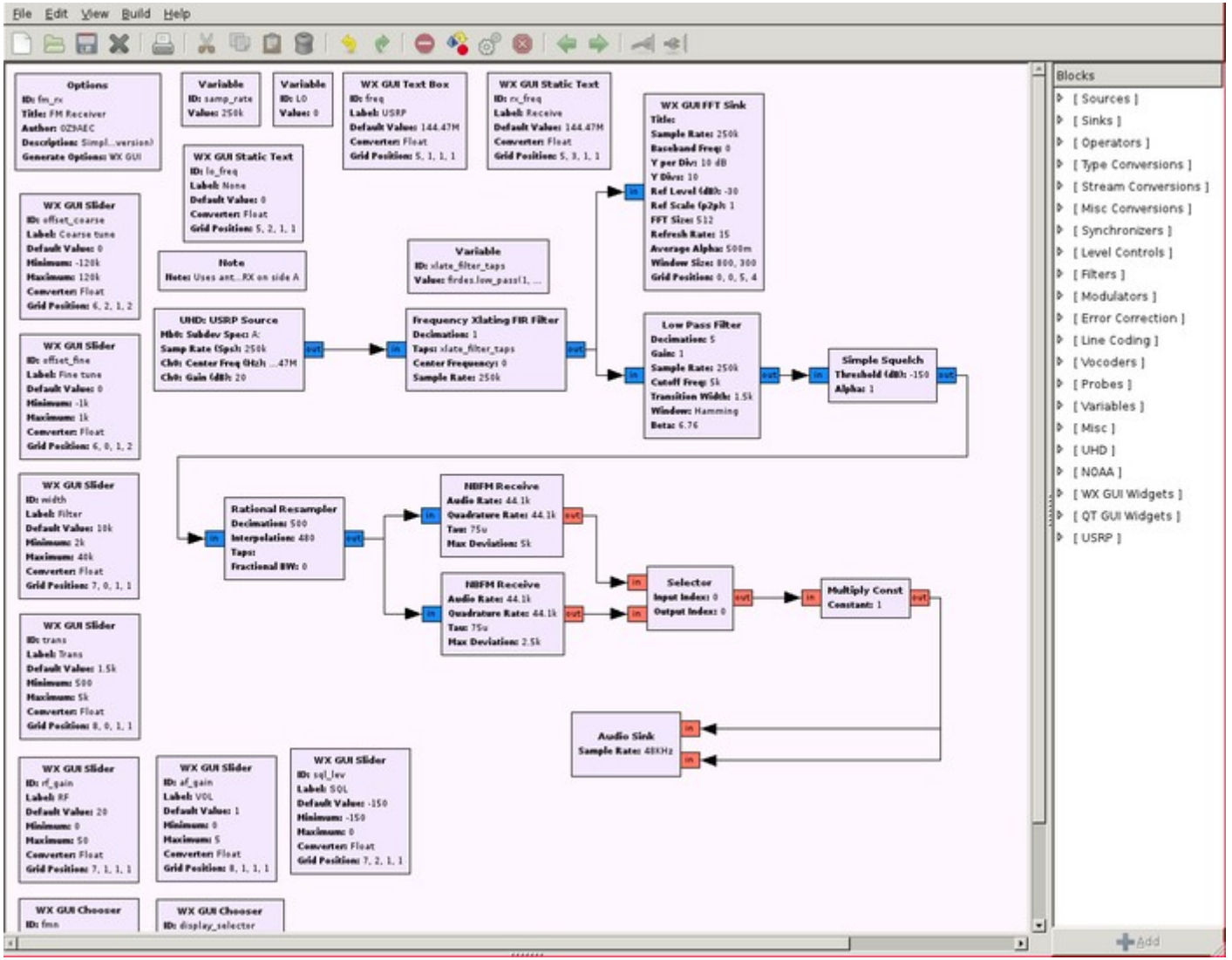
# GNU Radio .. what it is NOT

- Not a “click and play” tool.

  You do need to know SDR, DSP and signal-processing

- Not an end-user application
  - Toolkit!
  - You can use it to create applications
    - gqrx
    - QRadioLink

# GRC


File Edit View Build Help
Options
Variable
Variable
WX GUI Text Box
WX GUI Static Text
WX GUI FFT Sink
WX GUI Static Text
WX GUI Slider
Note
Variable
UHD: USRP Source
Frequency Xlating FIR Filter
Low Pass Filter
Simple Squelch
WX GUI Slider
WX GUI Slider
Rational Resampler
NBFM Receive
NBFM Receive
Selector
Multiply Const
WX GUI Slider
Audio Sink
WX GUI Slider
WX GUI Slider
WX GUI Slider
WX GUI Chooser
WX GUI Chooser
Blocks
[ Sources ]
[ Sinks ]
[ Operators ]
[ Type Conversions ]
[ Stream Conversions ]
[ Misc Conversions ]
[ Synchronizers ]
[ Level Controls ]
[ Filters ]
[ Modulators ]
[ Error Correction ]
[ Line Coding ]
[ Vocoders ]
[ Probes ]
[ Variables ]
[ Misc ]
[ UHD ]
[ NOAA ]
[ WX GUI Widgets ]
[ QT GUI Widgets ]
[ USRP ]
Add

# GRC Getting started

Let’s get started

- Start GRC
- Different parts
  - Menu
  - Buttons
  - Main screen
  - Side Pannel
  - Console

# GRC Menus

- File menu
  - Read
  - Write / write-as
- View
  - Block tree
  - Console Panel
  - Variable editor
  - Find

# GRC Getting started

- Top buttons
  - Start / stop
  - Show Errors !! (flow-graph errors)

- SideBar
  - Block tree
- Console: Errors!!! (Runtime Errors)
- Variable editor (can be part of sidebar)

# The GNU Radio blocks

Types of Blocks:

- Input / Output
- Processing
- Math operations
- Variables
- Instrumentation blocks (probes)
- Embedded python blocks
- Misc (!)

# The GNU Radio blocks (2)

Questions:

- What is the correct block to use?
- What are the correct parameters of the block?

Note:
I do not know all the blocks neither.

# The I/O blocks (1)

Input (read): Source
Output (write): Sink

- Devices: like SDR rx/tx → osmocom block
- Audio interface (mono or stereo)
- Signal-source
  - Incl. Noise sources

# The I/O blocks (2)

- File block:
  - File source / sink (including FIFO)
  - Wave source / sink
- Network (UDP, TCP, ZeroMQ)

Note:
Type of device determines datatype

# The Processing blocks

"Process" (whatever that may be)

- DSP/SDR functions:
  - Filters
  - Modulator / demodulator
  - Frequency Mixers
  - Channel simulators
- Samplerate Conversions
- Datatype conversions
- Threshhold blocks

# Math Operations

- Add / subtract / multiply / divide
- Abs(), min(), max(), ...

- Different uses: (e.g.) Multiply:
  - Multiply two streams: mixer
  - Multiply with constant: amplifier
  - Multiply with -1 (invert)
  - Multiply with 0 or 1 (switch on/off)

# Variables

- Is used as parameter in block

  (e.g. inside I/O block): “frequency”
  - Fixed value (“variable” block)
  - “Entry” field
  - Range (slider)
  - Chooser (selection)
- Can contain other variable or function
  - AudioRate = int(samp_rate / decim)
  - Filtertaps = f(AudioRate,maxfreq)

# Instrumentation

Visualisation tools
very important to examine signals

(“QT GUI sink”)

- Time sink (osciloscoop)
- Frequency sink
- Waterfall sink...
- Histogram sink
- Number sink
- Constellation sink
- ...

# Instrumentation (2)

“QT GUI Time sink” and “QT GUI Frequency sink”

- Note the “Control Panel” option in the “config” tab

# Embedded python blocks

Allows to create your own blocks

- Not that difficult

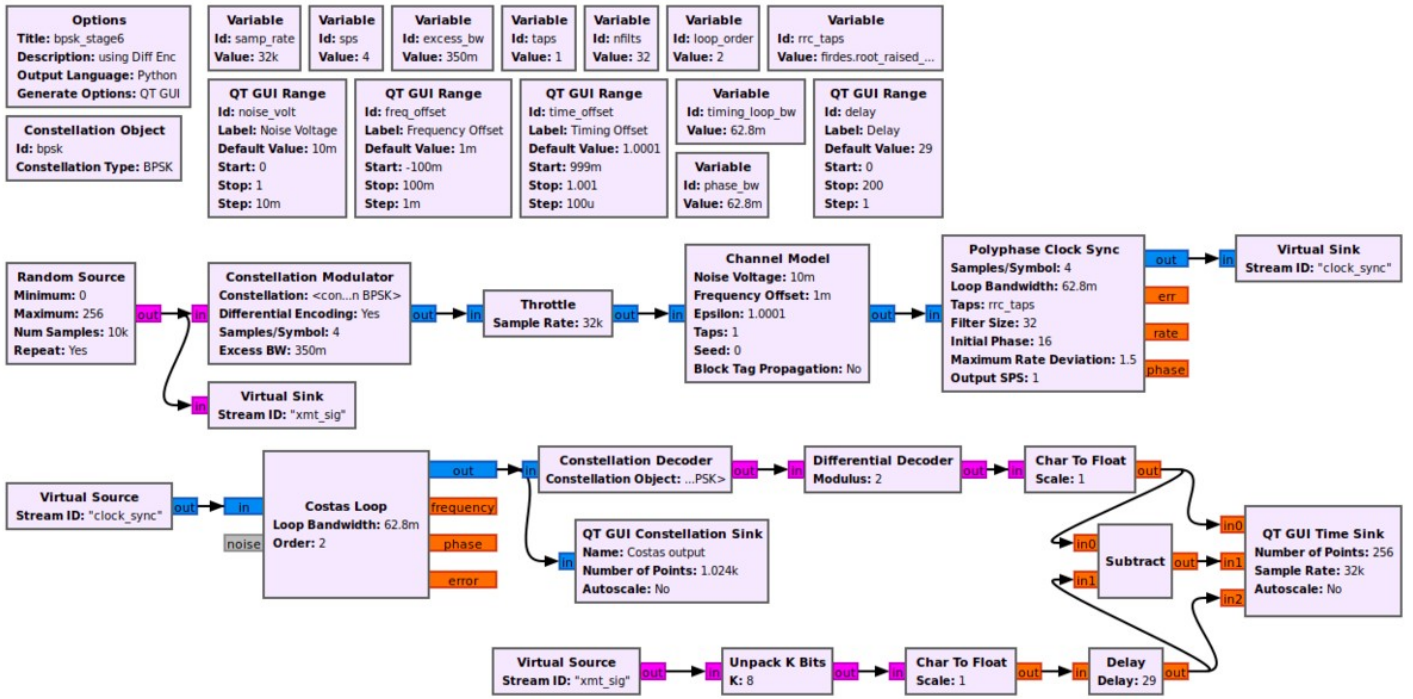
  (A lot of examples)

# Misc blocks

- Throttle block
  - VERY IMPORTANT
  - Necessairy when no “physical” blocks (no SDR rx/tx, no audio source/sink, …)
- Comment blocks

# Misc blocks

- Virtual Source / sink
  - Keeps you flowgraph clean



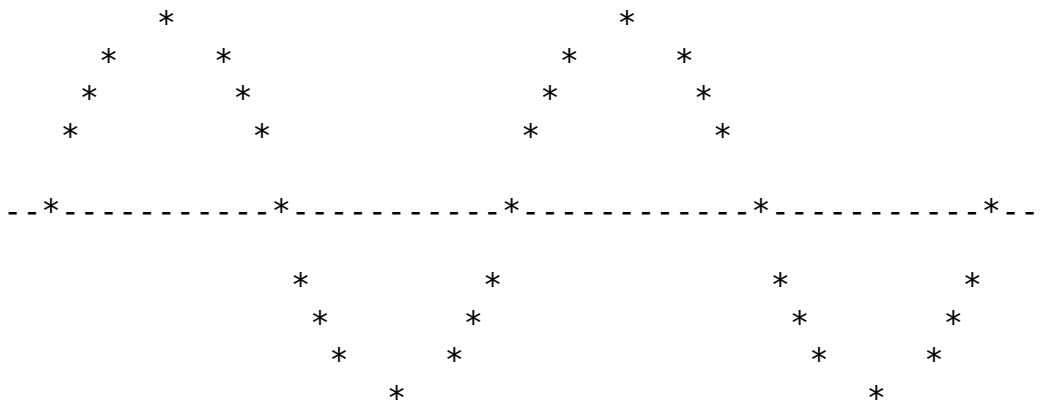
# DataTypes

- Byte (8 bit), Short (16 bit), Int (32 bit)
- Float (32 bit)

- Complex (I/Q samples)
  - 2 * float

- Messages

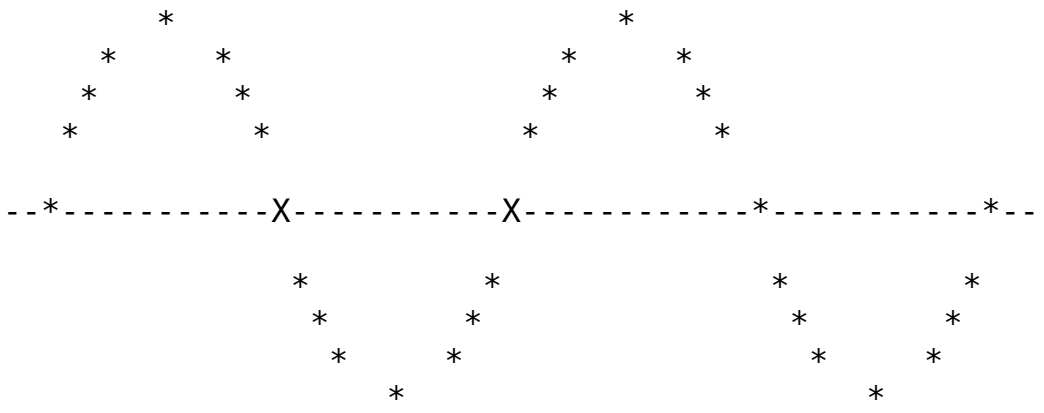
# I/Q signals



Disclaimer: This is only one of the ways to explain I/Q sampling (but it’s the one that is most intuitive, and it is how it is used in most ham-radio SDR receivers)

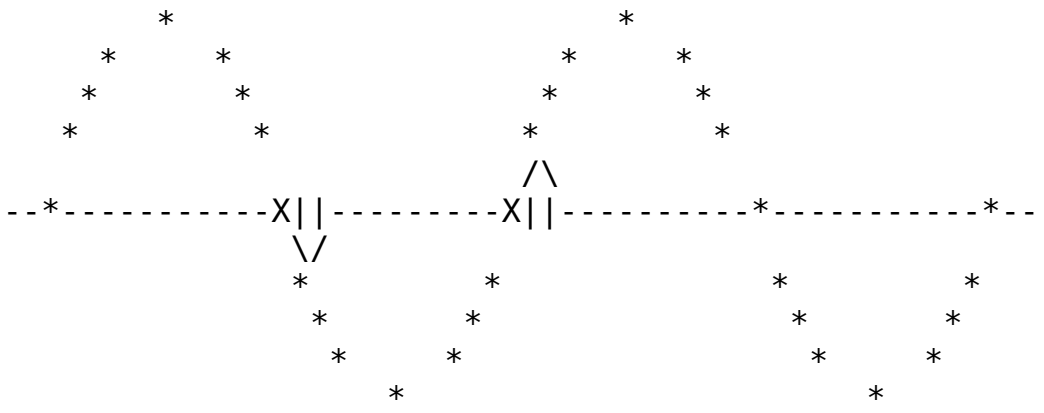
# I/Q signals

What Direction (up/down) does the signal travel at the points ‘X’?



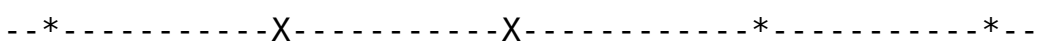
# I/Q signals

What Direction (up/down) does the signal travel at the points ‘X’?



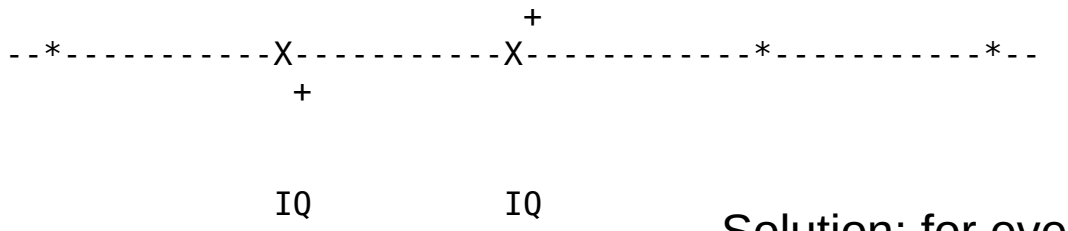
# I/Q signals

What Direction (up/down) does the signal travel at the points ‘X’?
When you only have the information at point ‘t’?



# I/Q signals

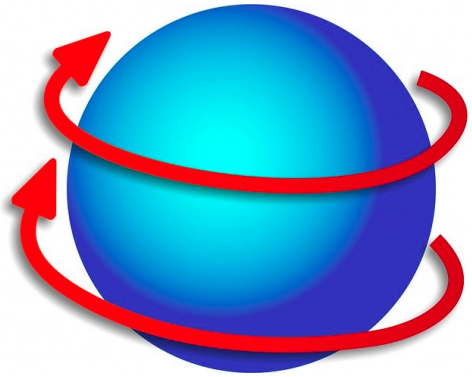
What Direction (up/down) does the signal travel at the points ‘X’?
When you only have the information at point ‘t’?

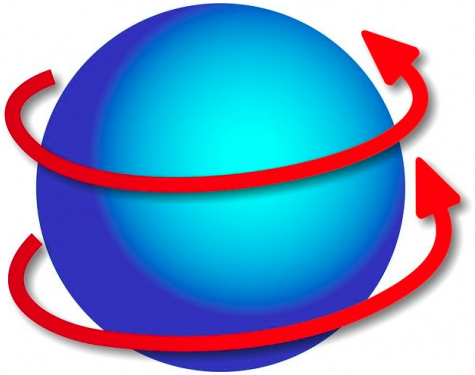



Solution: for every point “t”, take a 2nd sample, ¼*t later

# I/Q signals: negative frequencies

So why is this important?
Positive / Negative frequency



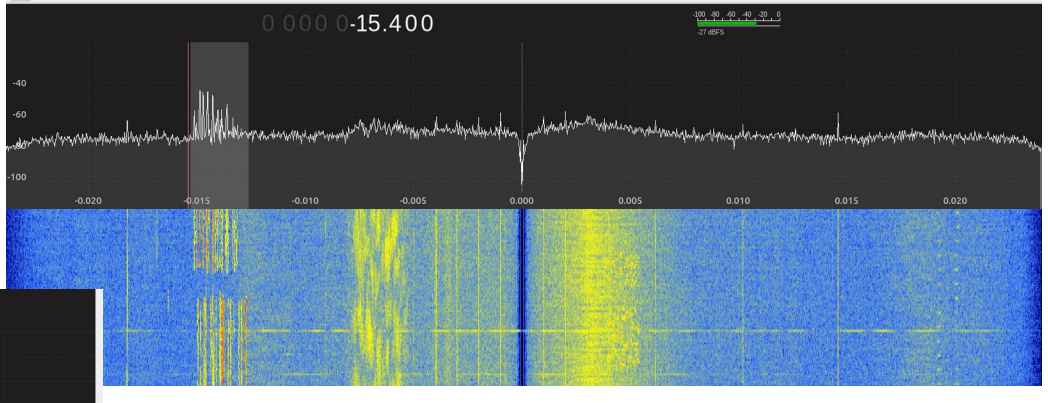


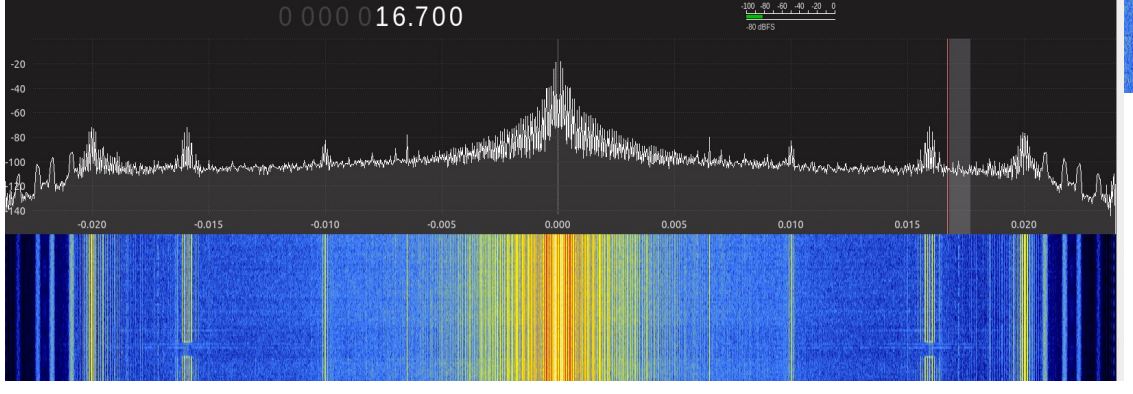
```
                +                                                +
--*-----------X-----------X-----------*----      --*-----------X-----------X-----------*---
                          +                                    +

               IQ          IQ                                 IQ          IQ
```

https://en.wikipedia.org/wiki/Spinning_dancer
https://pixabay.com/illustrations/ball-sphere-shape-spin-spinning-313522/

# I/Q sampling

- For every periode “t”, two sample-actions are done: “I” (In phase) and “Q” (quadrature)
- This provides information about the “direction” of a frequency: positive or negative
-



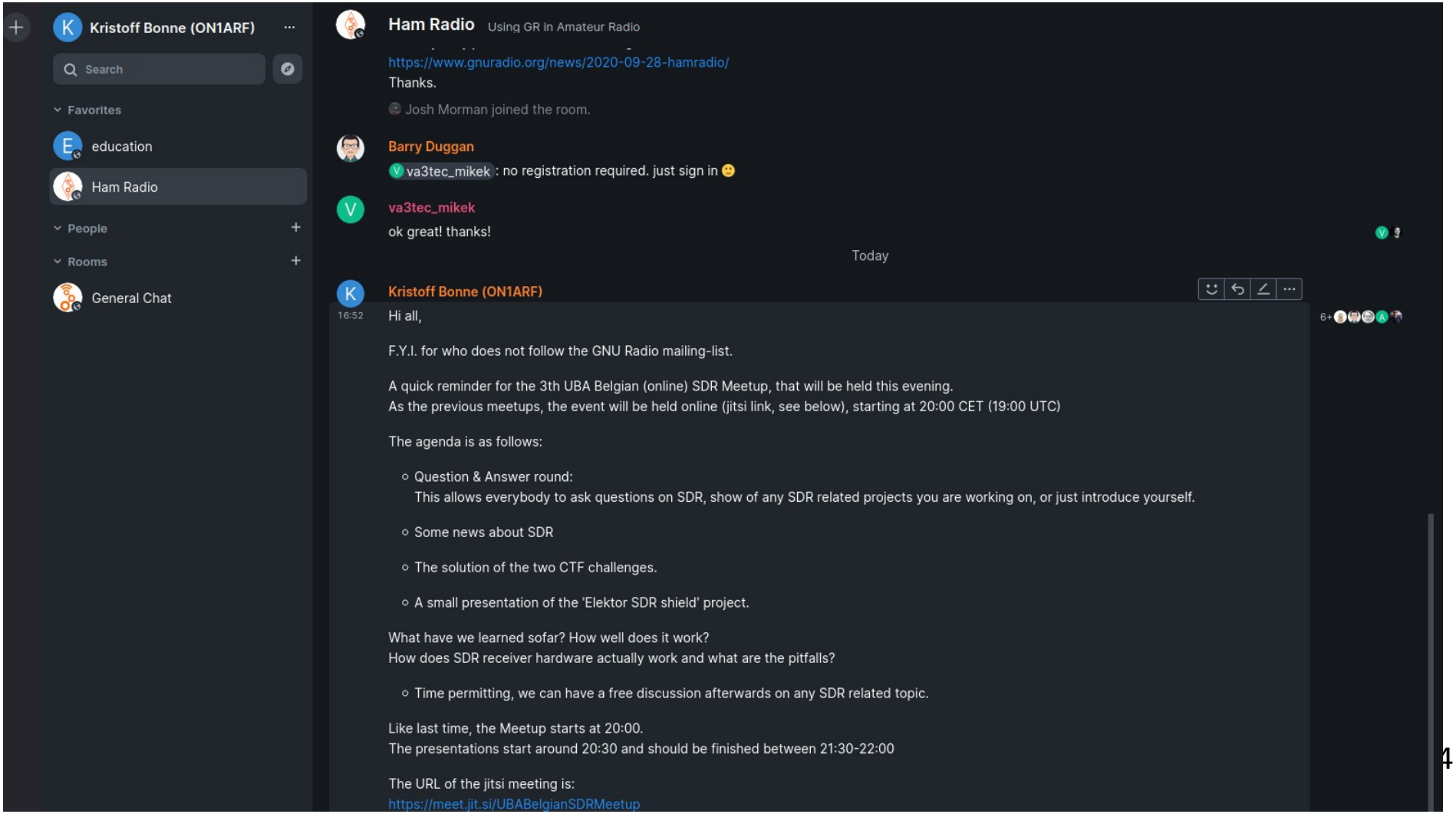



# To do

- Still a lot to learn (also for me!)

# 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]

# 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.

# CTF2

- File input:
  - File source block
  - Verify datatype
  - Check sample-rate
    - → variable “samp_rate”

# CTF2

- Throttle-block
  - If no physical interfaces, insert throttle-block

# CTF2

- Instrumentation
  - Time sink
  - Frequency Sink
  - Waterfall

  → Let’s run it, but first
  - Options block → id
  - Save → name

  What kind of signal is it?

# CTF2

- Instrumentation
  - Time sink
  - Frequency Sink
  - Waterfall

  Zoom in, control-pannel, ...

  What kind of signal is it?

# CTF2

- AM-signal
  - “AM demod” → try : does not work
  - Complex_to_amplitude^2
    - Add time sink

- Once ok, disable other sinks

# CTF2

- To much noise
  - Low-pass filter
    - Most easy LPF: moving average filter
    - Length → slider
    - Scale
  - What is effect → time sink, 2 input

# CTF2

- AGC block ?
  - Gain, max. gain, reference ?
    - Help !
  - → change default values of time sink

# CTF2

- What signal is this?
  - Hint: “the question of the CTF is a hint by itself:
  - When (time/date) was this recorded
    - Time → dcf77
    - https://en.wikipedia.org/wiki/DCF77
      - > dcf77 time format

# Threshold

- Time to use virtual sink (?)
- Threshhold block
  - Where to set threshhold value?
    - Variable “QT enter” block

# Threshold

- Use virtual sink (?)
- Threshhold block
  - Where to set threshhold value?
    - Variable “QT enter” block

# Write to File

- Convert to a more easy format (byte)
- Write to file
  - Fifo ?
  - od -t x1 -v fifo.f

# Some other things that might be usefull

- FM / FSK demod
  - Quadrature demodulator
- To receive real signals
  - Frequency xlat FIR filter
  - Sample rate !!!
  - filters