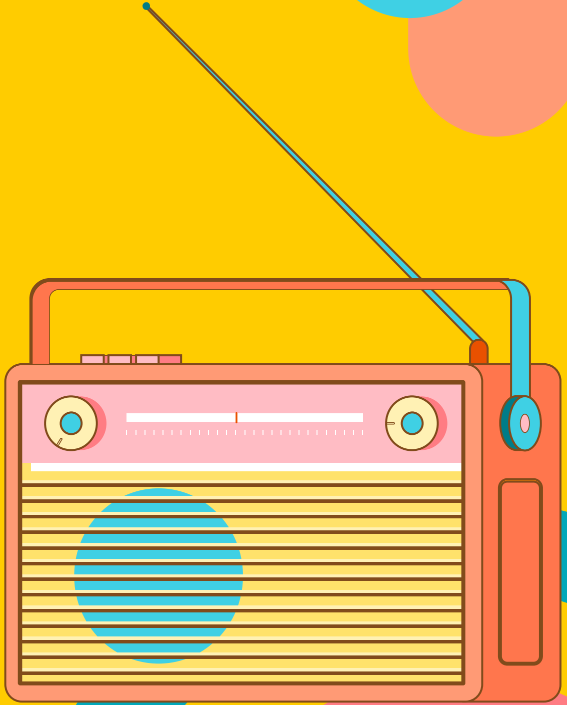
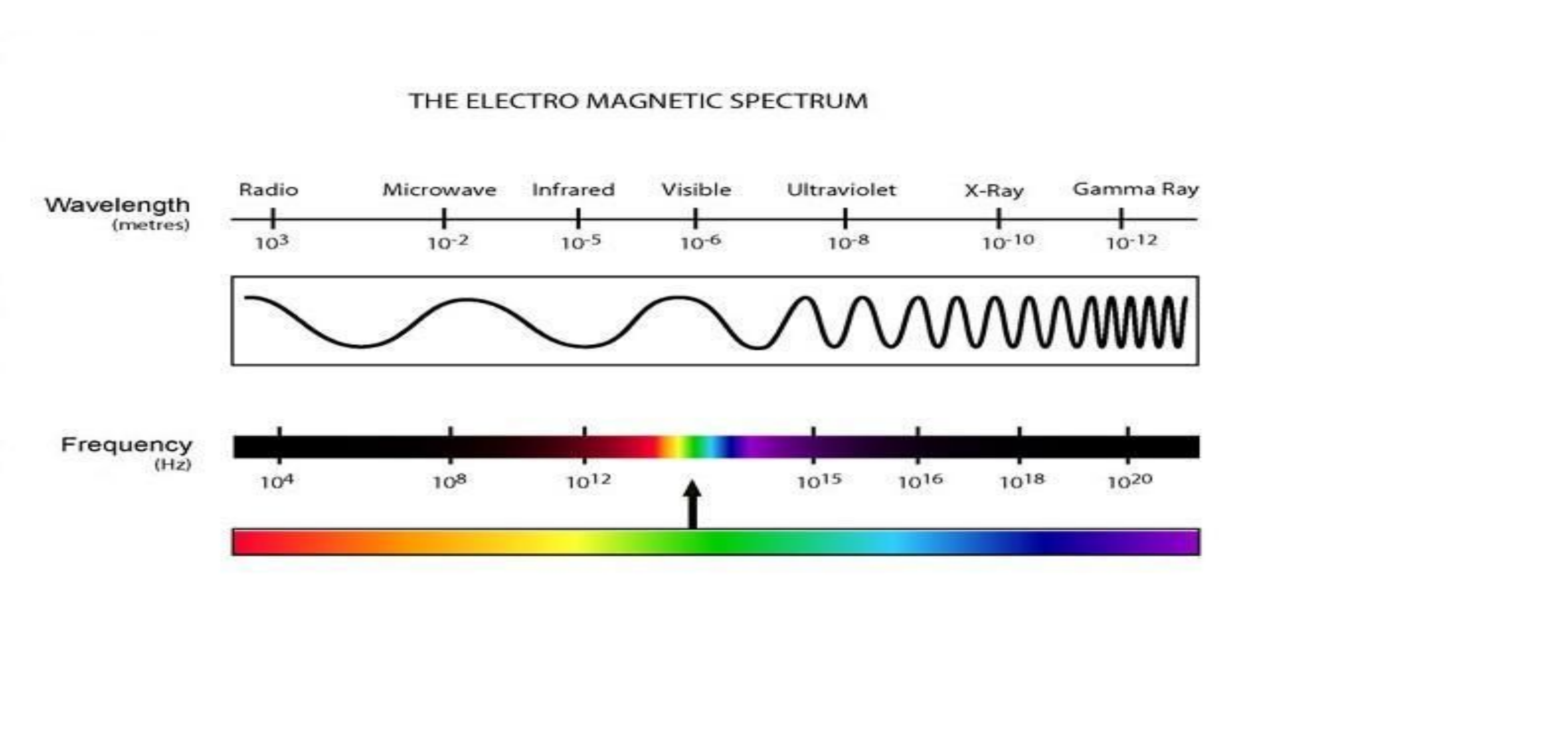
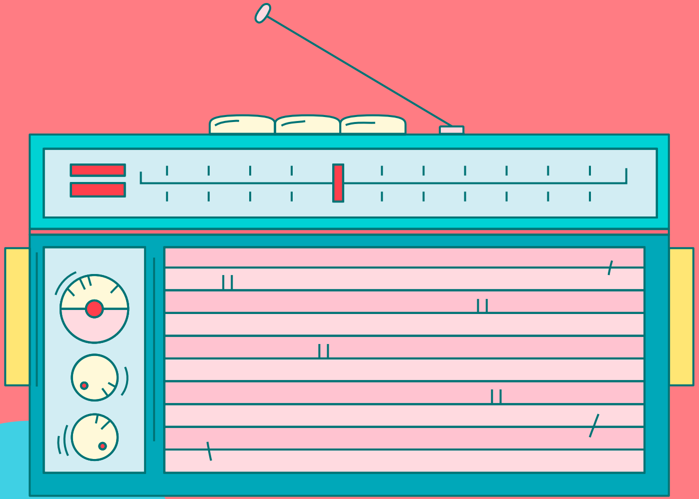
Software Defined RADIO

Hacking Wireless Devices



ABOUT THE RADIO

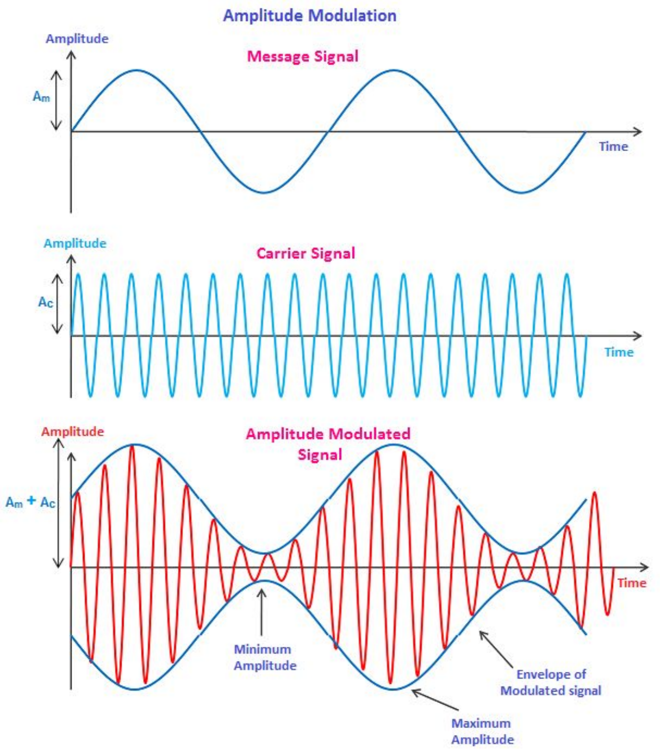




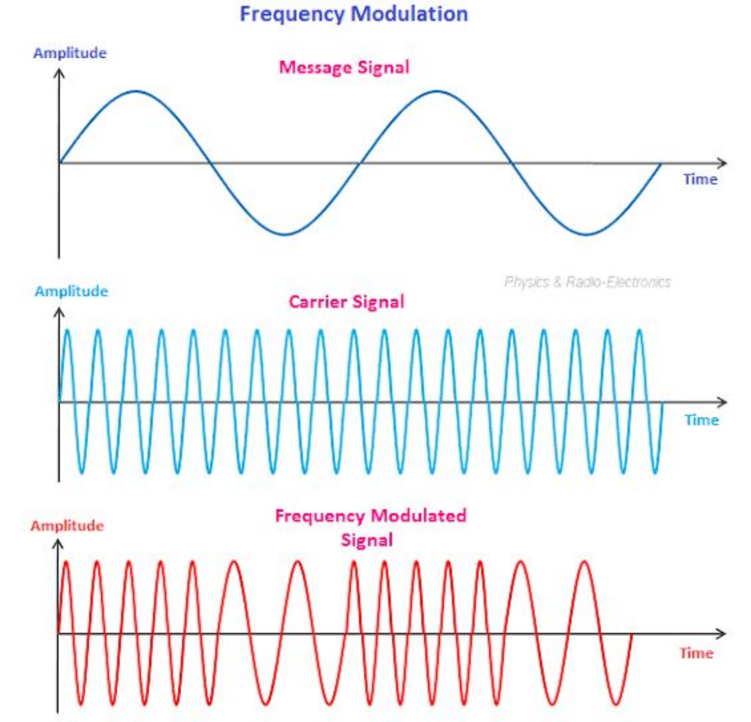
Radio Waves

(X, Y, Z) - Amplitude, Frequency, Phase

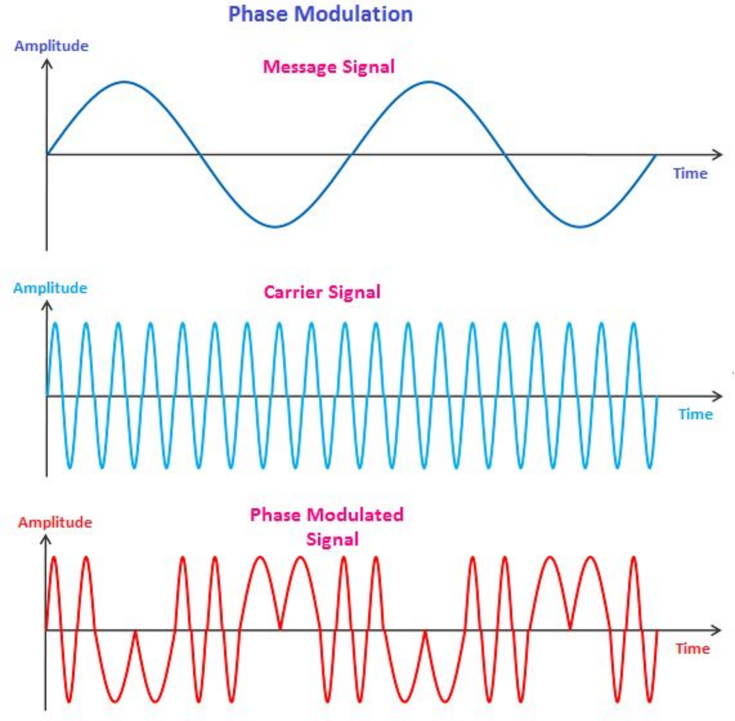
Modulation - Amplitude



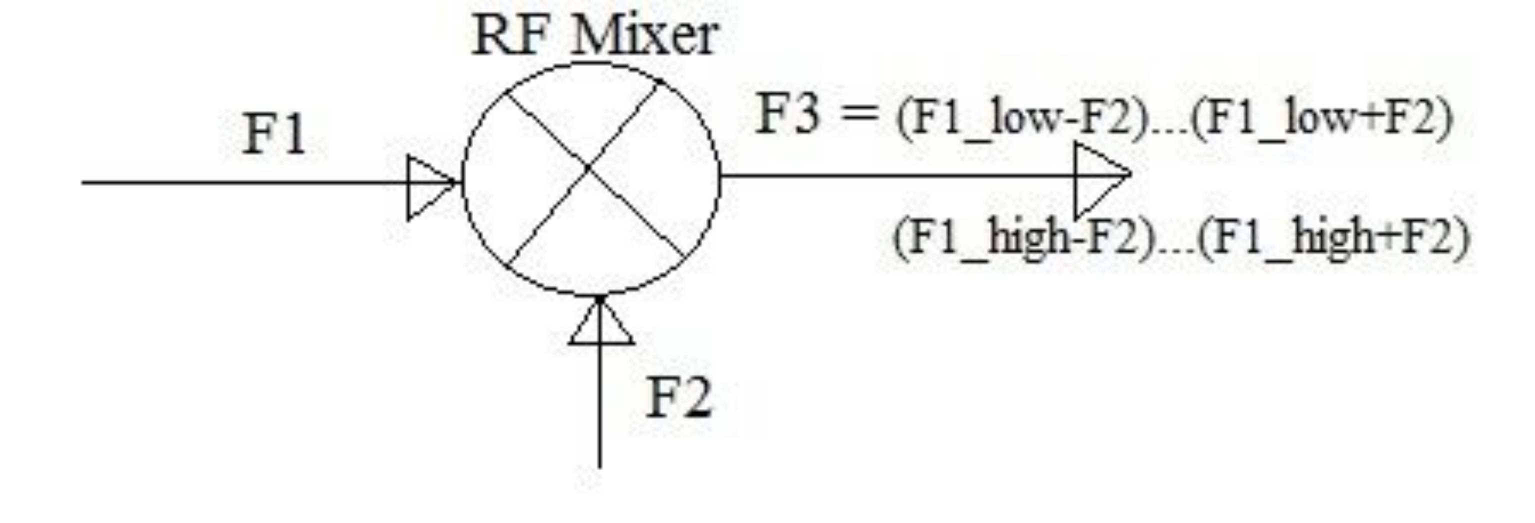
Modulation - Frequency



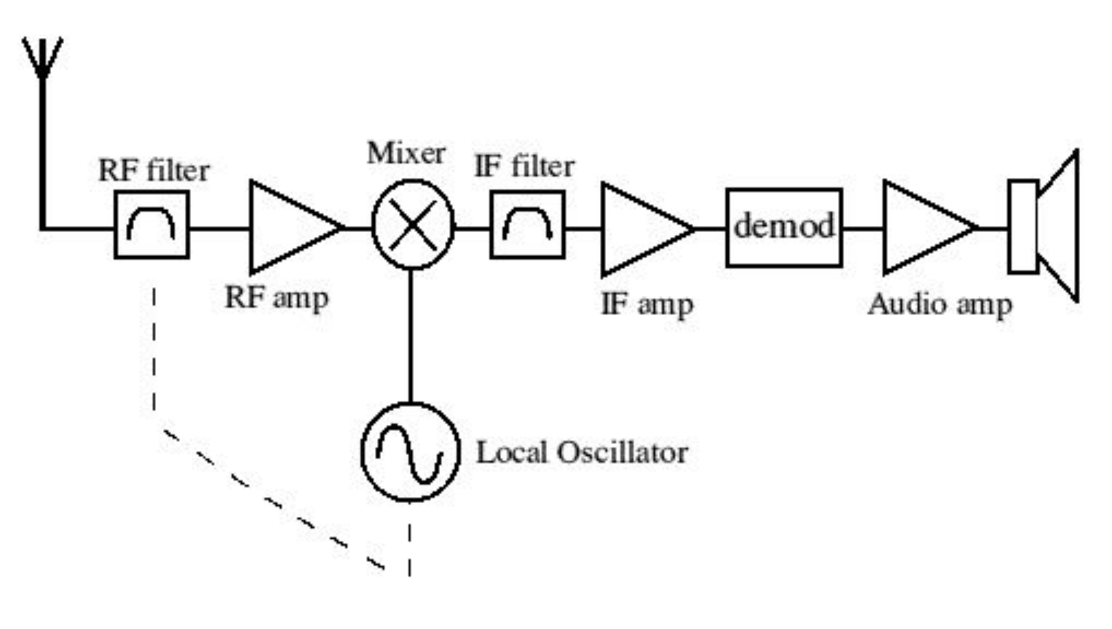
Modulation - Phase

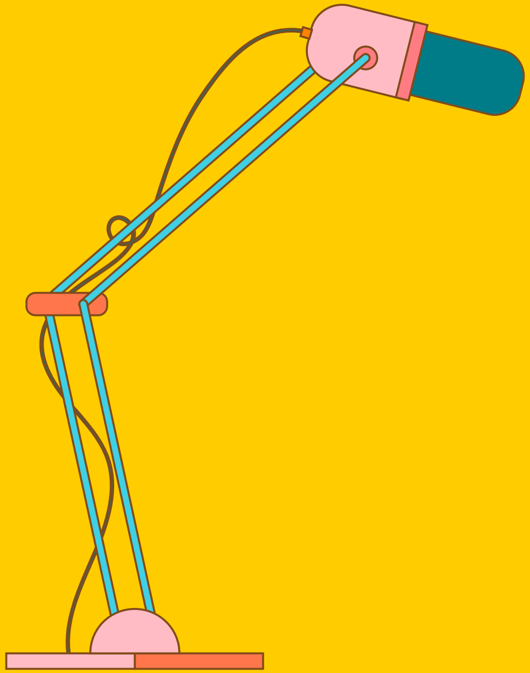


Mixers - Multiply Signals



SDR - Architecture





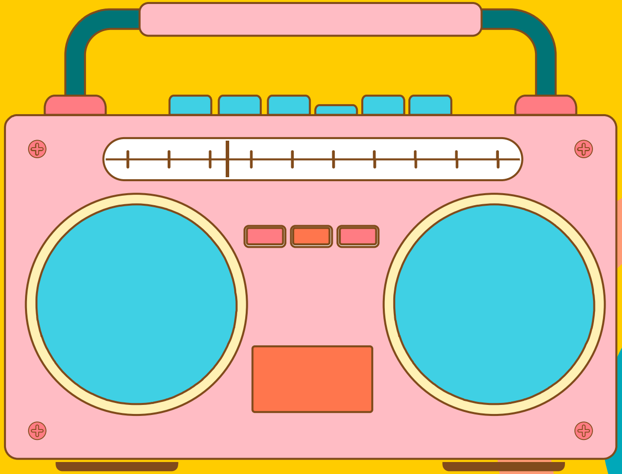
Hardware

Receive and Transmit

RTL-SDR VS HackRF

Object Of Study

Remote electrical Plug



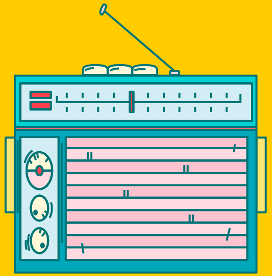
Find a Target

ANACOM

AUTORIDADE
NACIONAL
DE COMUNICAÇÕES

https://www.anacom.pt/

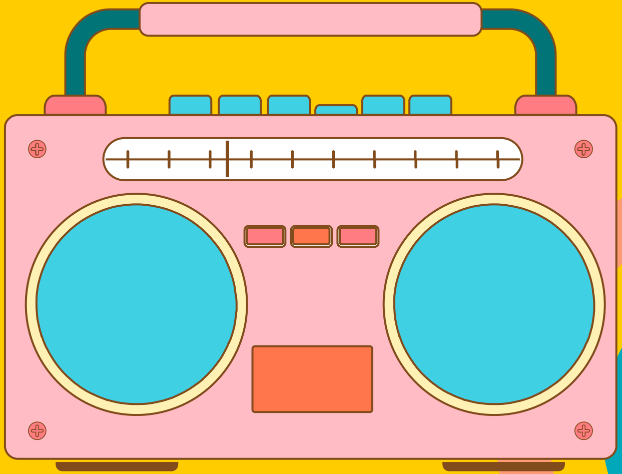
The Process

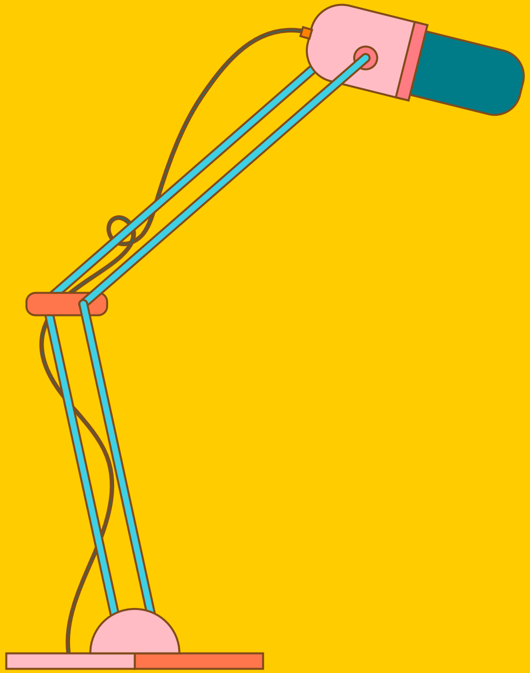


1. Identify Frequency
2. Identify Modulation
3. Demodulate Signal
4. Extract Data

Tooling

You can enter a subtitle here if you need it

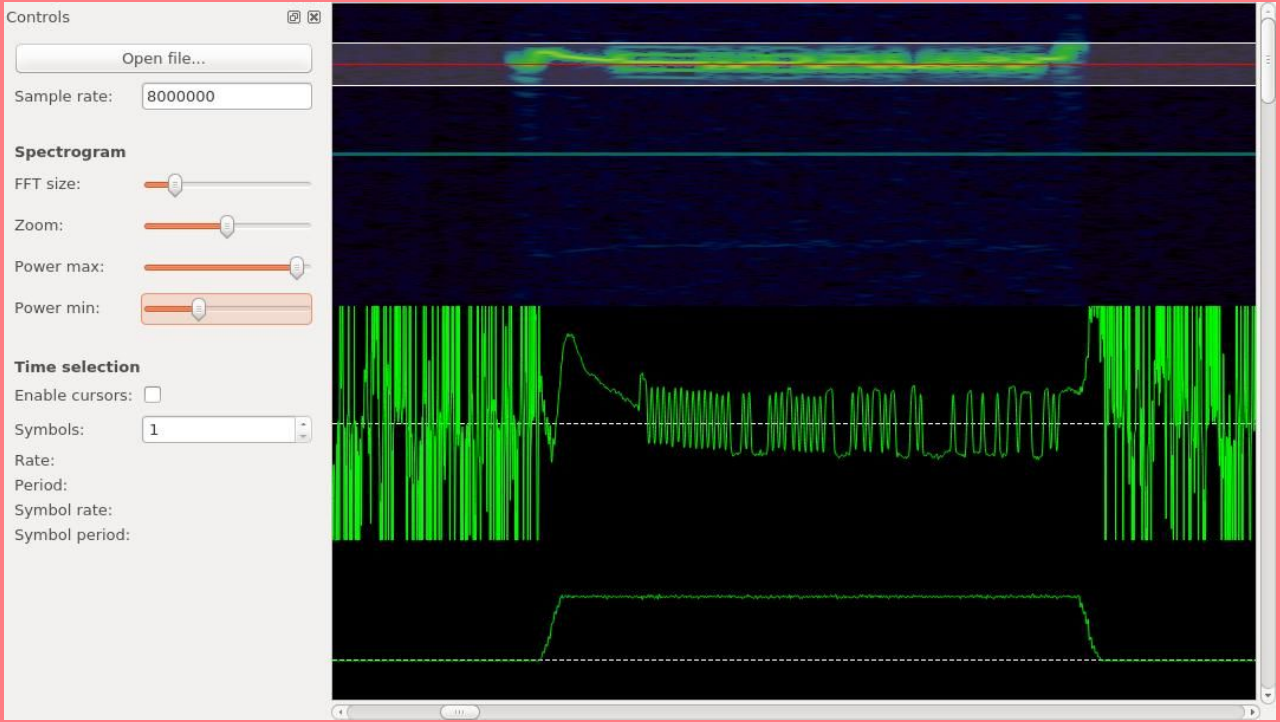




Inspectrum

inspectrum is a tool for analysing captured signals, primarily from software-defined radio receivers

Inspectrum Analysing Tool



Controls

Sample rate: 8000000

Spectrogram

FFT size:

Zoom:

Power max:

Power min:

Time selection

Enable cursors: □

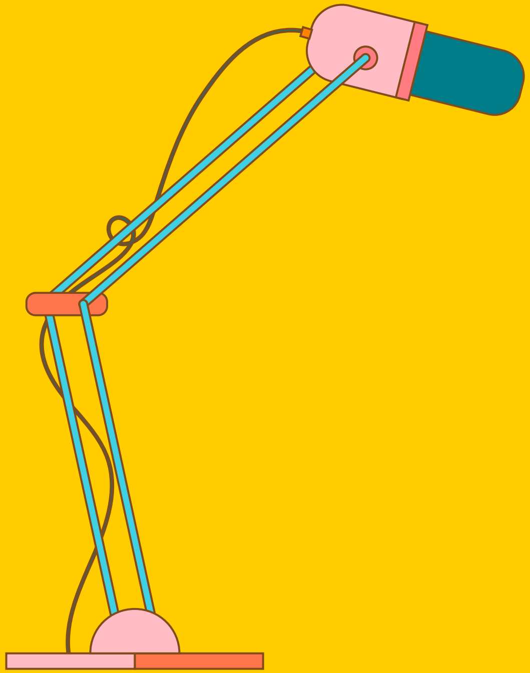
Symbols: 1

Rate:

Period:

Symbol rate:

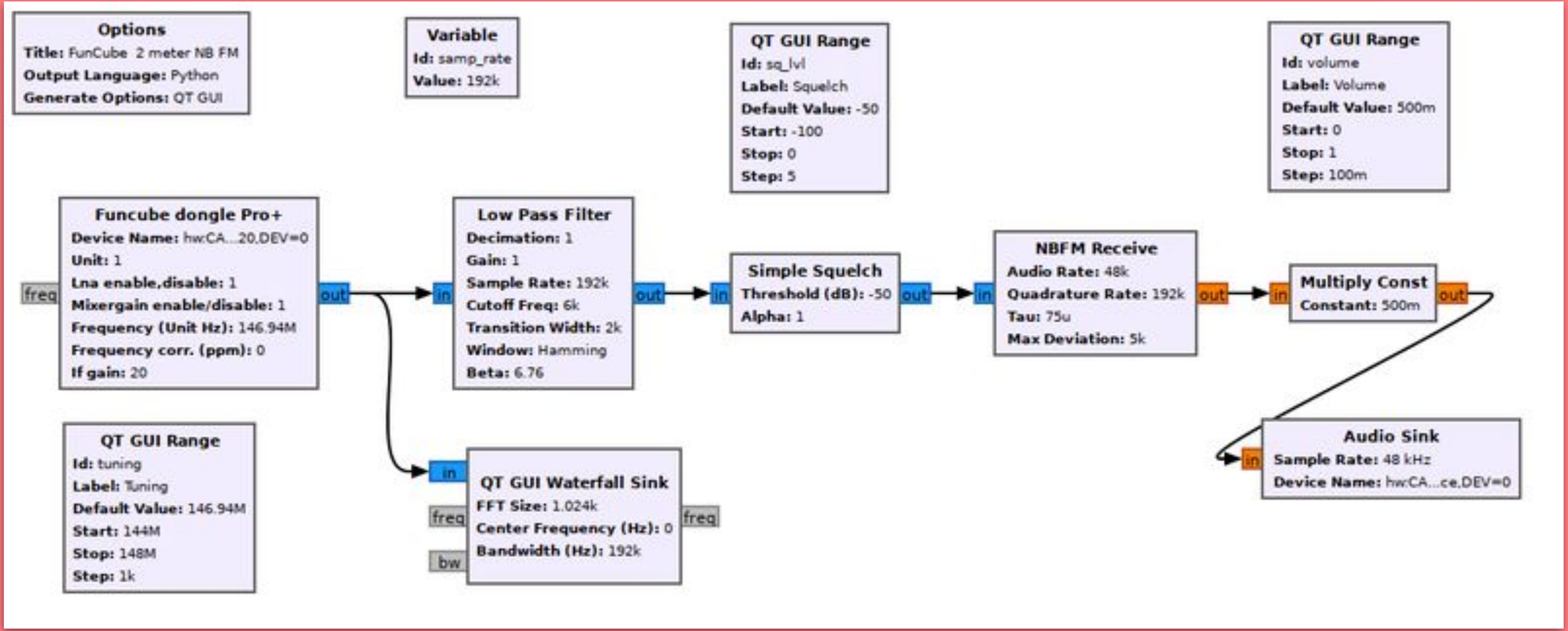
Symbol period:



GnuRadio

GNU Radio is a free & open-source software development toolkit that provides signal processing blocks to implement software radios

Gnuradio Flow Graph



Options
Title: FunCube 2 meter NB FM
Output Language: Python
Generate Options: QT GUI

Variable
Id: samp_rate
Value: 192k

QT GUI Range
Id: sq_lvl
Label: Squelch
Default Value: -50
Start: -100
Stop: 0
Step: 5

QT GUI Range
Id: volume
Label: Volume
Default Value: 500m
Start: 0
Stop: 1
Step: 100m

Funcube dongle Pro+
Device Name: hw:CA...20,DEV=0
Unit: 1
Lna enable,disable: 1
Mixergain enable/disable: 1
Frequency (Unit Hz): 146.94M
Frequency corr. (ppm): 0
If gain: 20

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 192k
Cutoff Freq: 6k
Transition Width: 2k
Window: Hamming
Beta: 6.76

Simple Squelch
Threshold (dB): -50
Alpha: 1

NBFM Receive
Audio Rate: 48k
Quadrature Rate: 192k
Tau: 75u
Max Deviation: 5k

Multiply Const
Constant: 500m

QT GUI Range
Id: tuning
Label: Tuning
Default Value: 146.94M
Start: 144M
Stop: 148M
Step: 1k

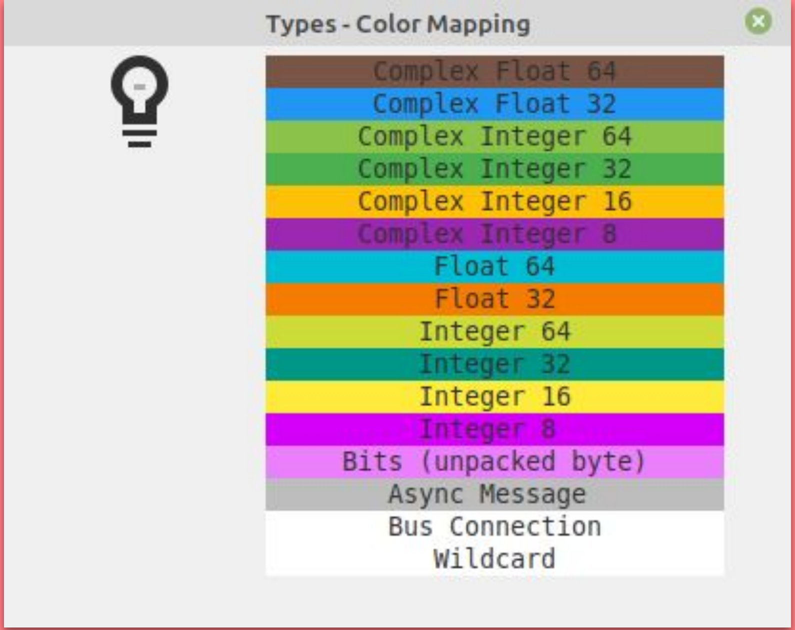
QT GUI Waterfall Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 192k

Audio Sink
Sample Rate: 48 kHz
Device Name: hw:CA...ce,DEV=0

GnuRadio

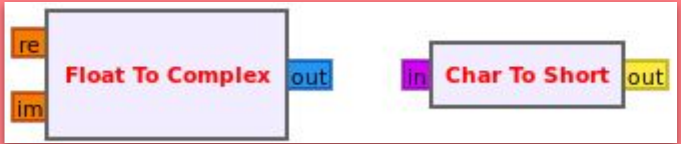
The Basics

Components - Types

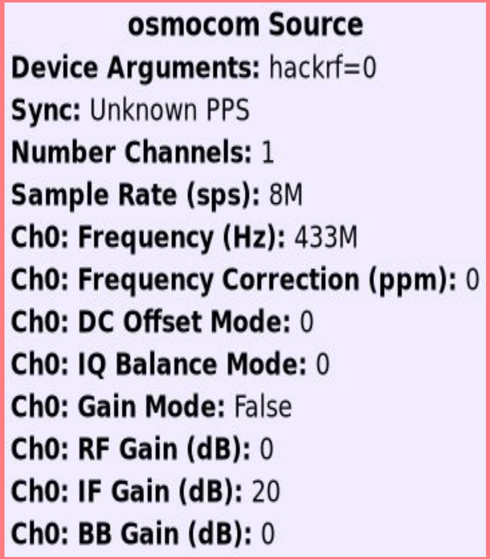


Types - Color Mapping

Complex Float 64
Complex Float 32
Complex Integer 64
Complex Integer 32
Complex Integer 16
Complex Integer 8
Float 64
Float 32
Integer 64
Integer 32
Integer 16
Integer 8
Bits (unpacked byte)
Async Message
Bus Connection
Wildcard

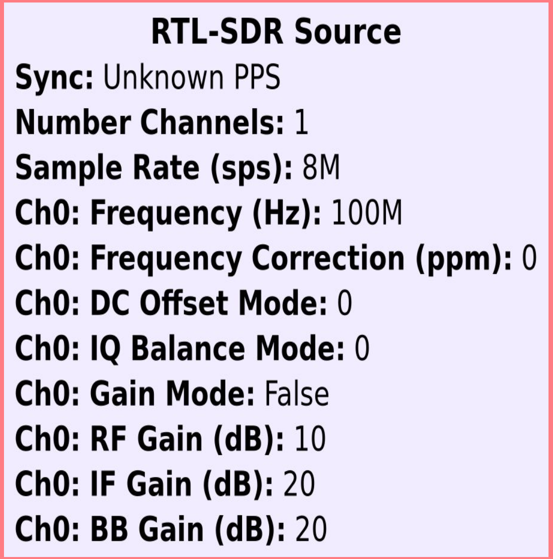


Components - Sources



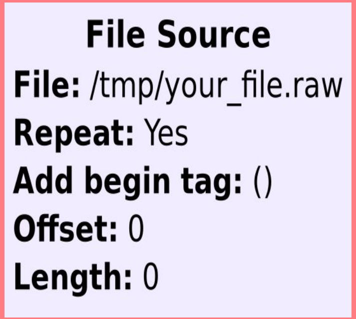
osmocom Source

Device Arguments: hackrf=0
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 8M
Ch0: Frequency (Hz): 433M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 0
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 0



RTL-SDR Source

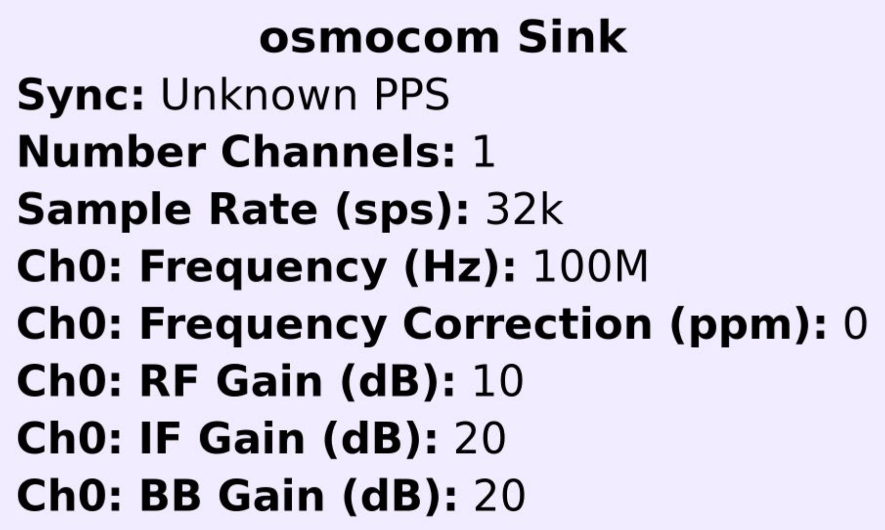
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 8M
Ch0: Frequency (Hz): 100M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20



File Source

File: /tmp/your_file.raw
Repeat: Yes
Add begin tag: ()
Offset: 0
Length: 0

Components - Sinks



osmocom Sink

Sync: Unknown PPS

Number Channels: 1

Sample Rate (sps): 32k

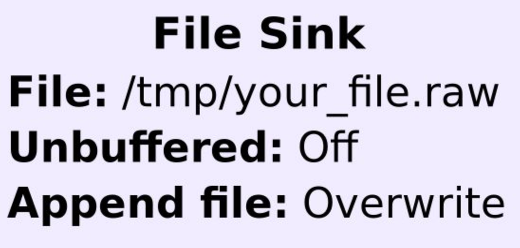
Ch0: Frequency (Hz): 100M

Ch0: Frequency Correction (ppm): 0

Ch0: RF Gain (dB): 10

Ch0: IF Gain (dB): 20

Ch0: BB Gain (dB): 20



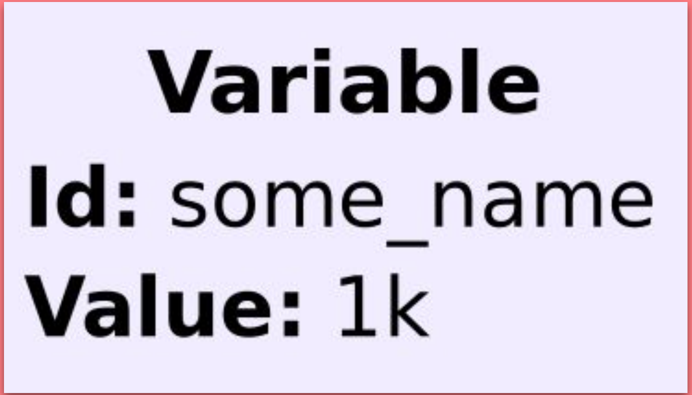
File Sink

File: /tmp/your_file.raw

Unbuffered: Off

Append file: Overwrite

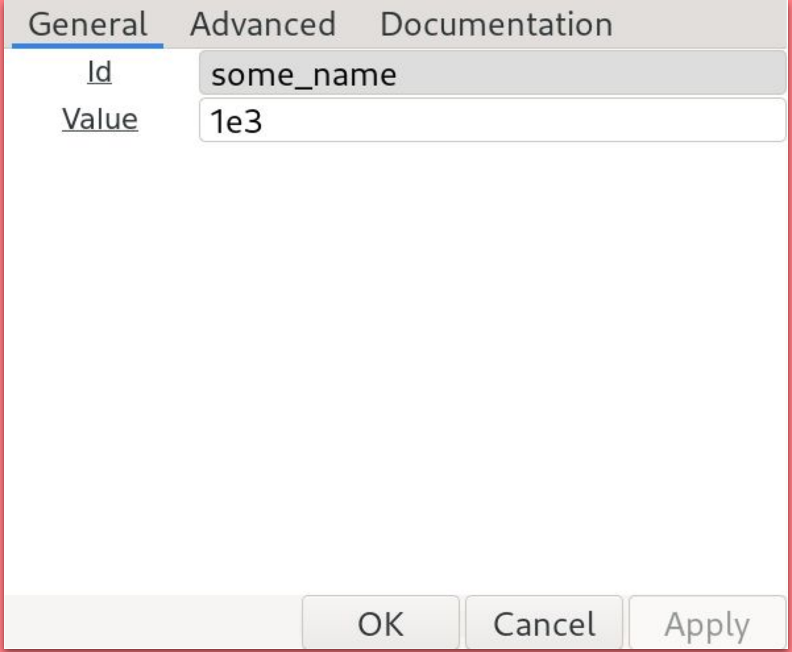
Components - UI and Variables



Variable

Id: some_name

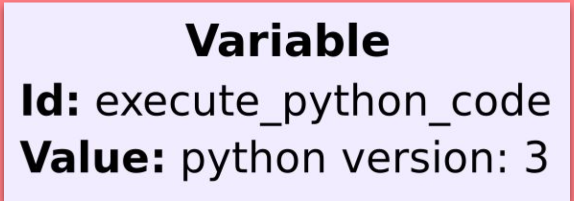
Value: 1k



Id: some_name

Value: 1e3

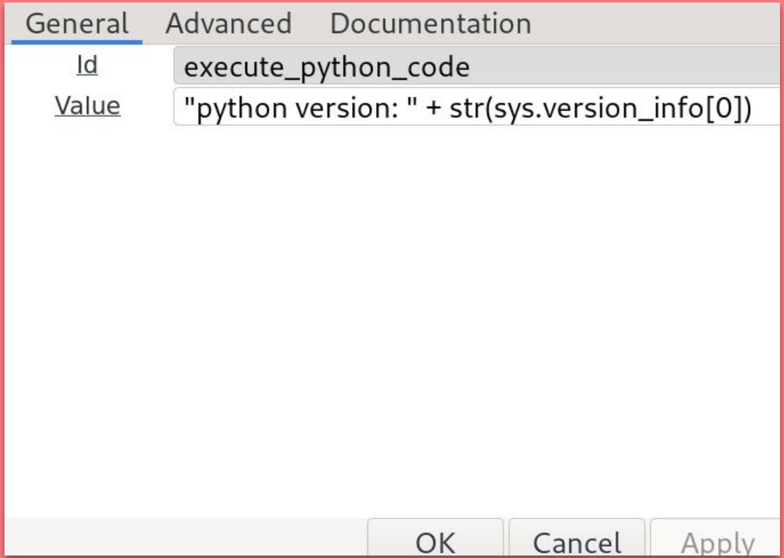
Components - UI and Variables



Variable

Id: execute_python_code

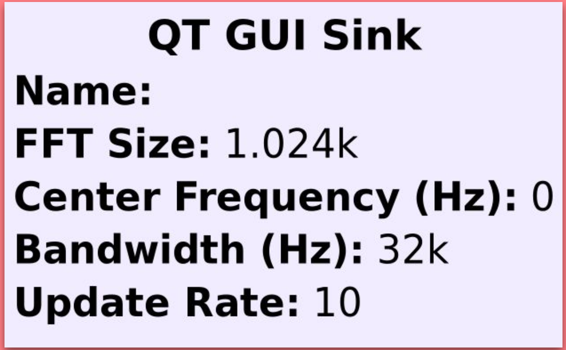
Value: python version: 3



Id: execute_python_code

Value: "python version: " + str(sys.version_info[0])

Components - UI and Variables



QT GUI Sink

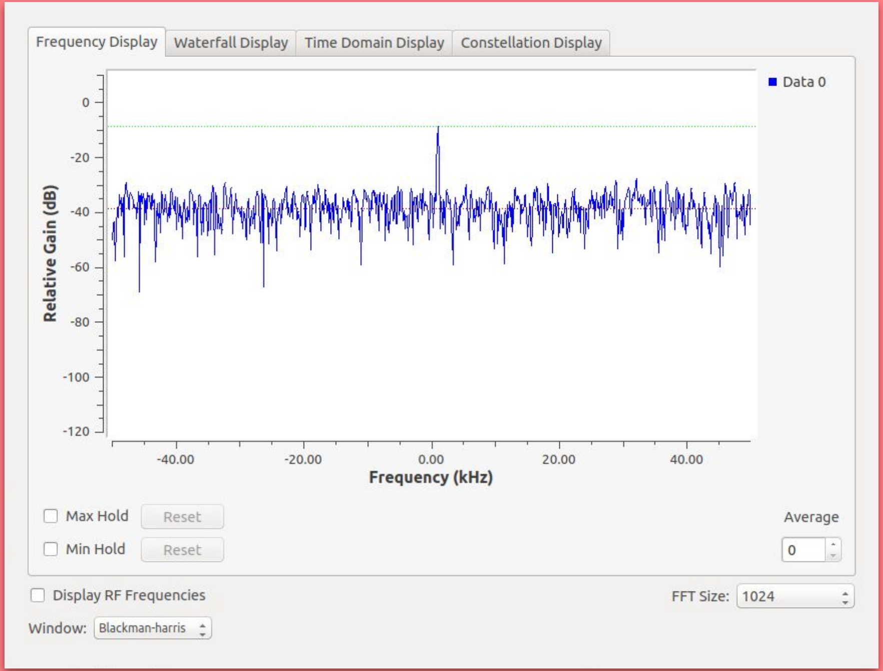
Name:

FFT Size: 1.024k

Center Frequency (Hz): 0

Bandwidth (Hz): 32k

Update Rate: 10



☐ Max Hold

☐ Min Hold

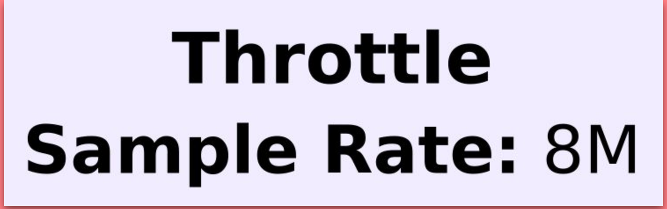
Average: 0

☐ Display RF Frequencies

FFT Size: 1024

Window: Blackman-harris

Components - Throttle



Throttle

Sample Rate: 8M

Components - Math

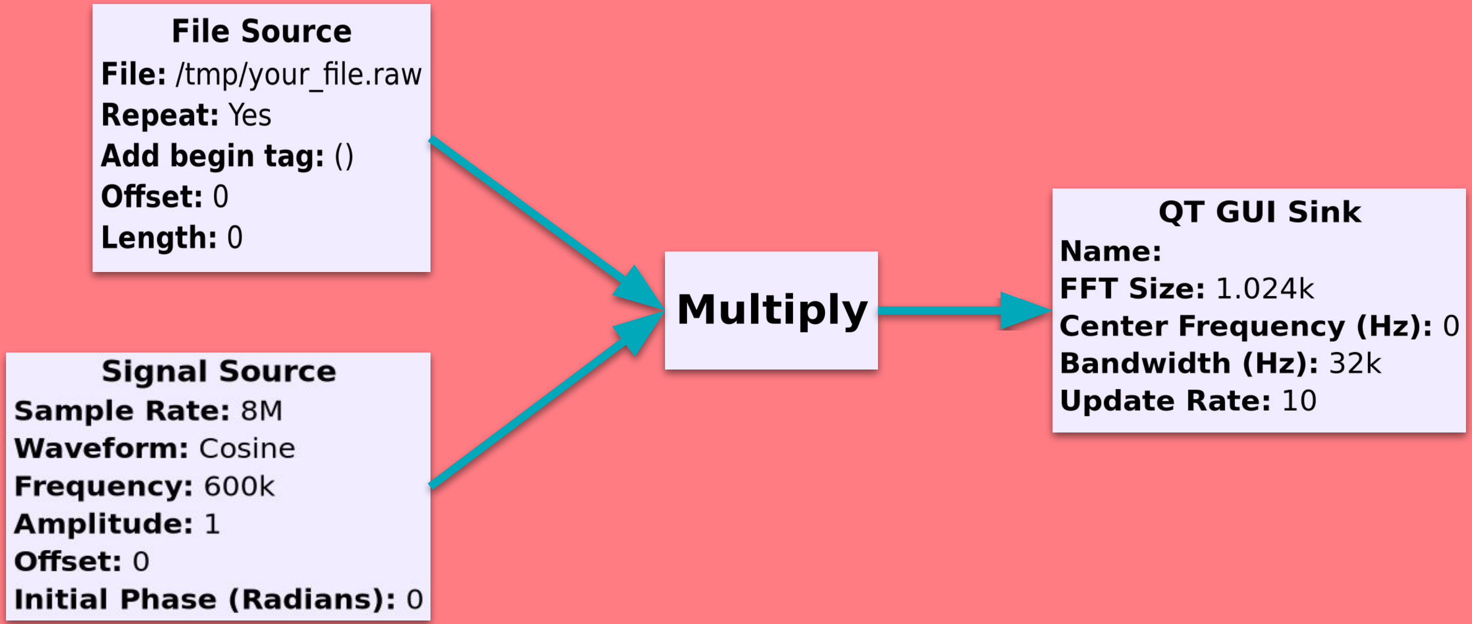
Multiply

Divide

Add

Subtract

Components - Shift Signal



File Source

File: /tmp/your_file.raw

Repeat: Yes

Add begin tag: ()

Offset: 0

Length: 0

Signal Source

Sample Rate: 8M

Waveform: Cosine

Frequency: 600k

Amplitude: 1

Offset: 0

Initial Phase (Radians): 0

Multiply

QT GUI Sink

Name:

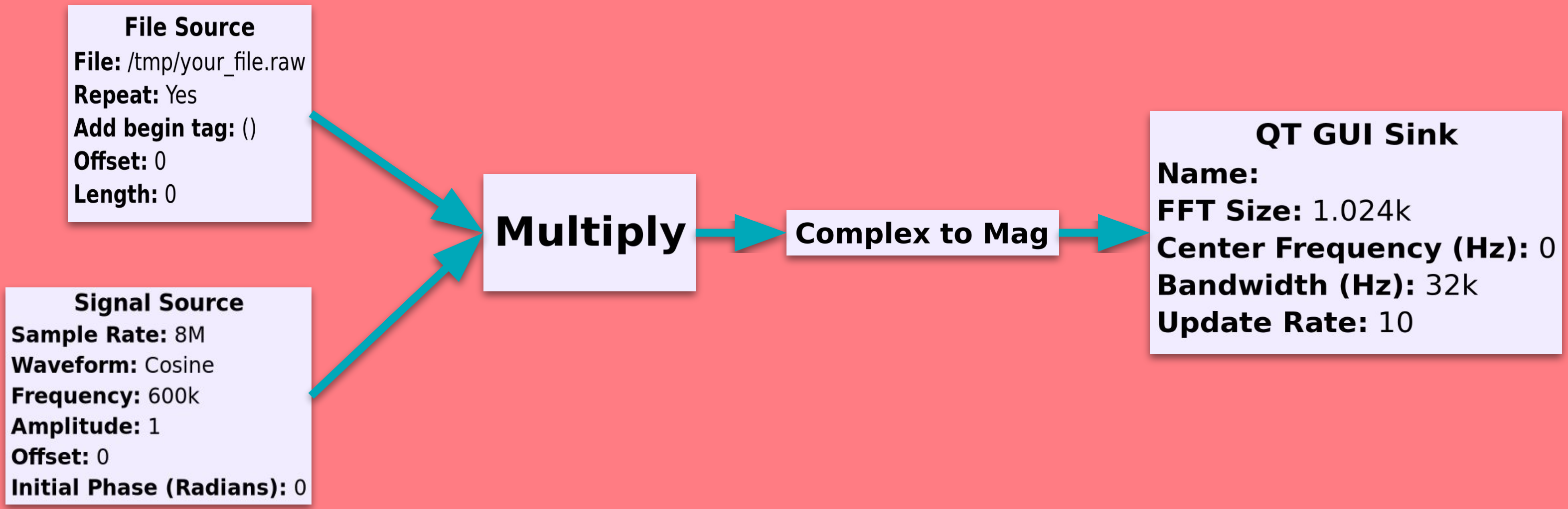
FFT Size: 1.024k

Center Frequency (Hz): 0

Bandwidth (Hz): 32k

Update Rate: 10

Components - Decode Modulations



File Source
File: /tmp/your_file.raw
Repeat: Yes
Add begin tag: ()
Offset: 0
Length: 0

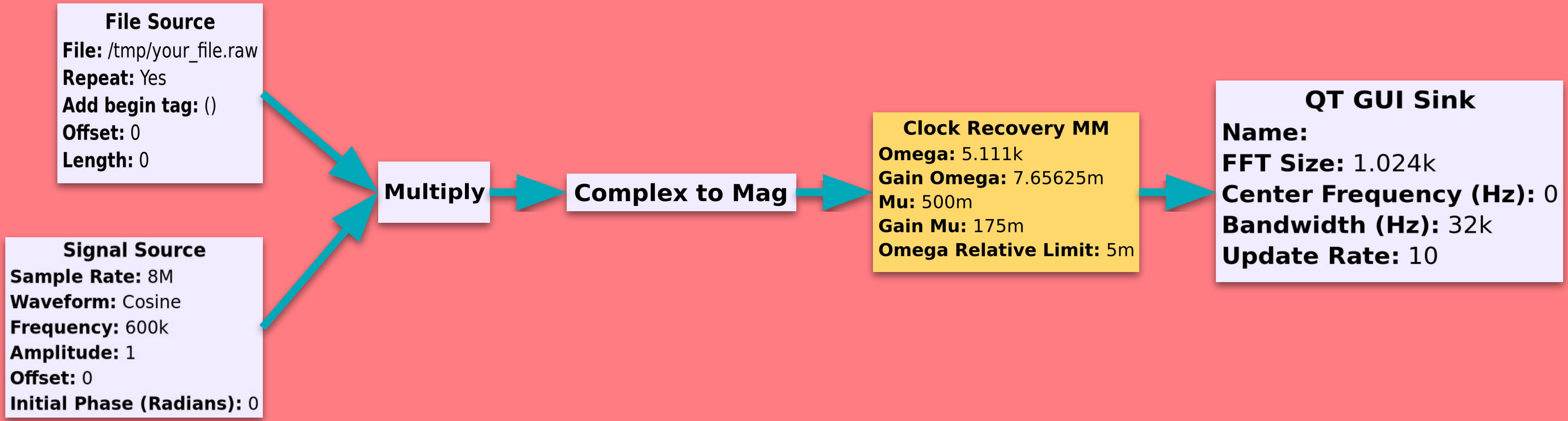
Signal Source
Sample Rate: 8M
Waveform: Cosine
Frequency: 600k
Amplitude: 1
Offset: 0
Initial Phase (Radians): 0

Multiply

Complex to Mag

QT GUI Sink
Name:
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 32k
Update Rate: 10

Components - Clock Recovery



File Source
File: /tmp/your_file.raw
Repeat: Yes
Add begin tag: ()
Offset: 0
Length: 0

Signal Source
Sample Rate: 8M
Waveform: Cosine
Frequency: 600k
Amplitude: 1
Offset: 0
Initial Phase (Radians): 0

Multiply

Complex to Mag

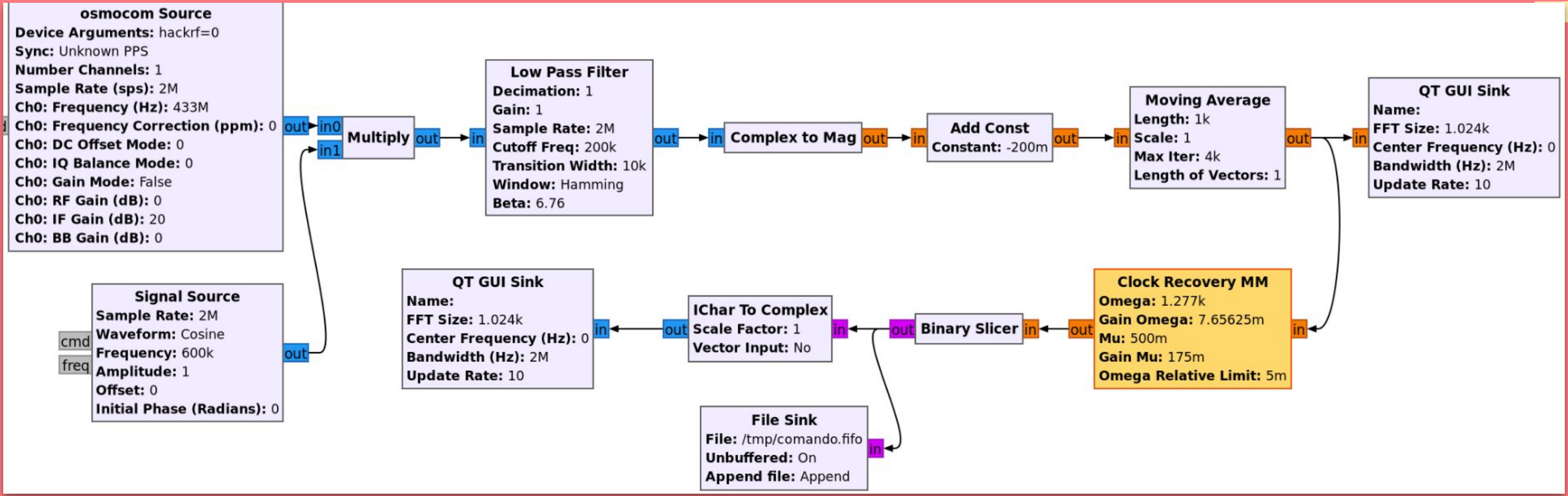
Clock Recovery MM
Omega: 5.111k
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

QT GUI Sink
Name:
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 32k
Update Rate: 10

Hands-On

RTl-SDR + GnuRadio = PWN!!

GnuRadio - Receive



osmocom Source
Device Arguments: hackrf=0
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 433M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 0
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 0

Signal Source
Sample Rate: 2M
Waveform: Cosine
Frequency: 600k
Amplitude: 1
Offset: 0
Initial Phase (Radians): 0

Multiply

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 2M
Cutoff Freq: 200k
Transition Width: 10k
Window: Hamming
Beta: 6.76

Complex to Mag

Add Const
Constant: -200m

Moving Average
Length: 1k
Scale: 1
Max Iter: 4k
Length of Vectors: 1

QT GUI Sink
Name:
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
Update Rate: 10

Clock Recovery MM
Omega: 1.277k
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

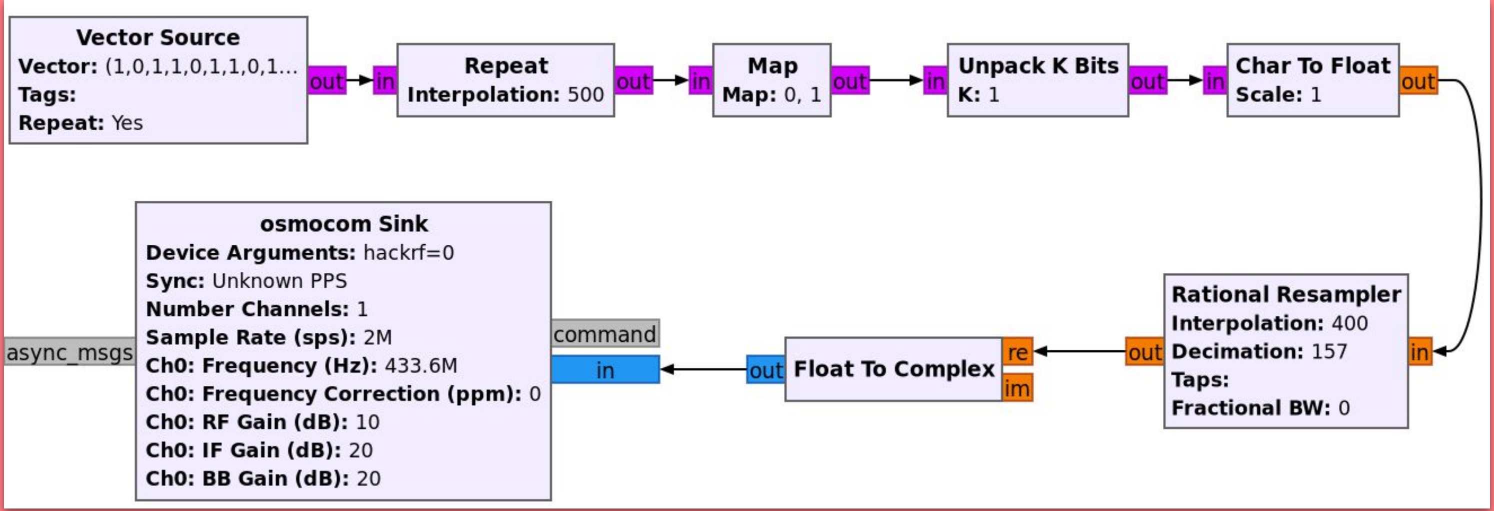
Binary Slicer

IChar To Complex
Scale Factor: 1
Vector Input: No

QT GUI Sink
Name:
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
Update Rate: 10

File Sink
File: /tmp/comando.fifo
Unbuffered: On
Append file: Append

GnuRadio - Transmit



Vector Source
Vector: (1,0,1,1,0,1,1,0,1...
Tags:
Repeat: Yes

Repeat
Interpolation: 500

Map
Map: 0, 1

Unpack K Bits
K: 1

Char To Float
Scale: 1

Rational Resampler
Interpolation: 400
Decimation: 157
Taps:
Fractional BW: 0

Float To Complex

osmocom Sink
Device Arguments: hackrf=0
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 433.6M
Ch0: Frequency Correction (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20

Stay Tuned For Another Cartoon

0xz3z4d45

THANKS!

Do you have any questions?

youremail@freepik.com
+91 620 421 838
yourcompany.com

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon** and infographics & images by **Freepik**

Please keep this slide for attribution