Reverse Engineering Digital Signals

Bastian Bloessl
<bloessl@ccs-labs.org>

HAM RADIO 2015 ▪ SDR Academy ▪ June 27, 2015

About Me

- PhD Student @ University of Paderborn
- Distributed Embedded Systems Group
- Work on GNU Radio OOT Modules
  - WiFi, ZigBee, RDS, WeatherSonde

DF1BBL

Reverse Engineering

Reverse engineering is taking apart an object to see how it works in order to duplicate or enhance the object. The practice, taken from older industries, is now frequently used on computer hardware and software.

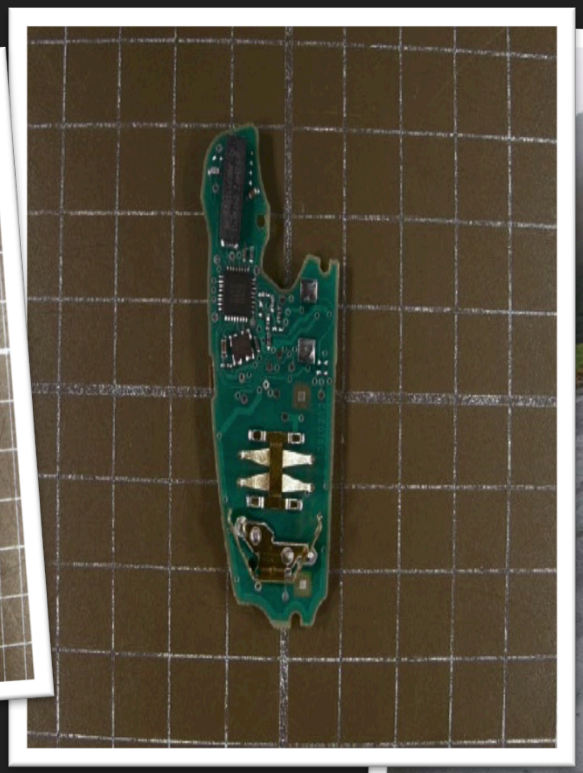
Definition from whatis.com

Reverse Engineering

- Frequency
- Modulation
- Bitrate
- Encoding
- Frame format

FCC Database

- Usually really helpful: http://fcc.gov/data/



FCC Database

- Usually really helpful: http://fcc.gov/data/

Hella KGaA Hueck & Co. would like the following documents regarding this submission for FCC ID: NBG010180T to be kept confidential.

Block diagrams
Technical / Operational description
Schematics
Bills of material

NR.653 S.3/4

19.JUN.2009 11:14

Hella KGaA Hueck & Co.

Federal Communications Commission

Your reference
Your letter dated
Our reference GE-A / Ho
Phone +49 2941 38- 8392
Fax +49 2941 38- 478392
E-mail heinz-theo.holle@hella.com
Date 2009-06-19
Subject **Certification Application of RF devices in USA, FCC ID: NBG010180T, Confidentiality Request,**

Postal Address
Hella KGaA Hueck & Co.
Rixbecker Straße 75
59552 Lippstadt/Germany

Telephone
Switchboard
+49 2941 38-0

Telefax
Switchboard
+49 2941 38-7133

Internet
www.hella.com

Head Office
Lippstadt

Commercial Register
Local Court Paderborn
HRB 6857

Bank
Deutsche Bank AG, Lippstadt
Kto. 6 095 013, BLZ 416 700 27
IBAN DE59 4167 0027 0609 5013 00
SWIFT DEUTDE 3B416

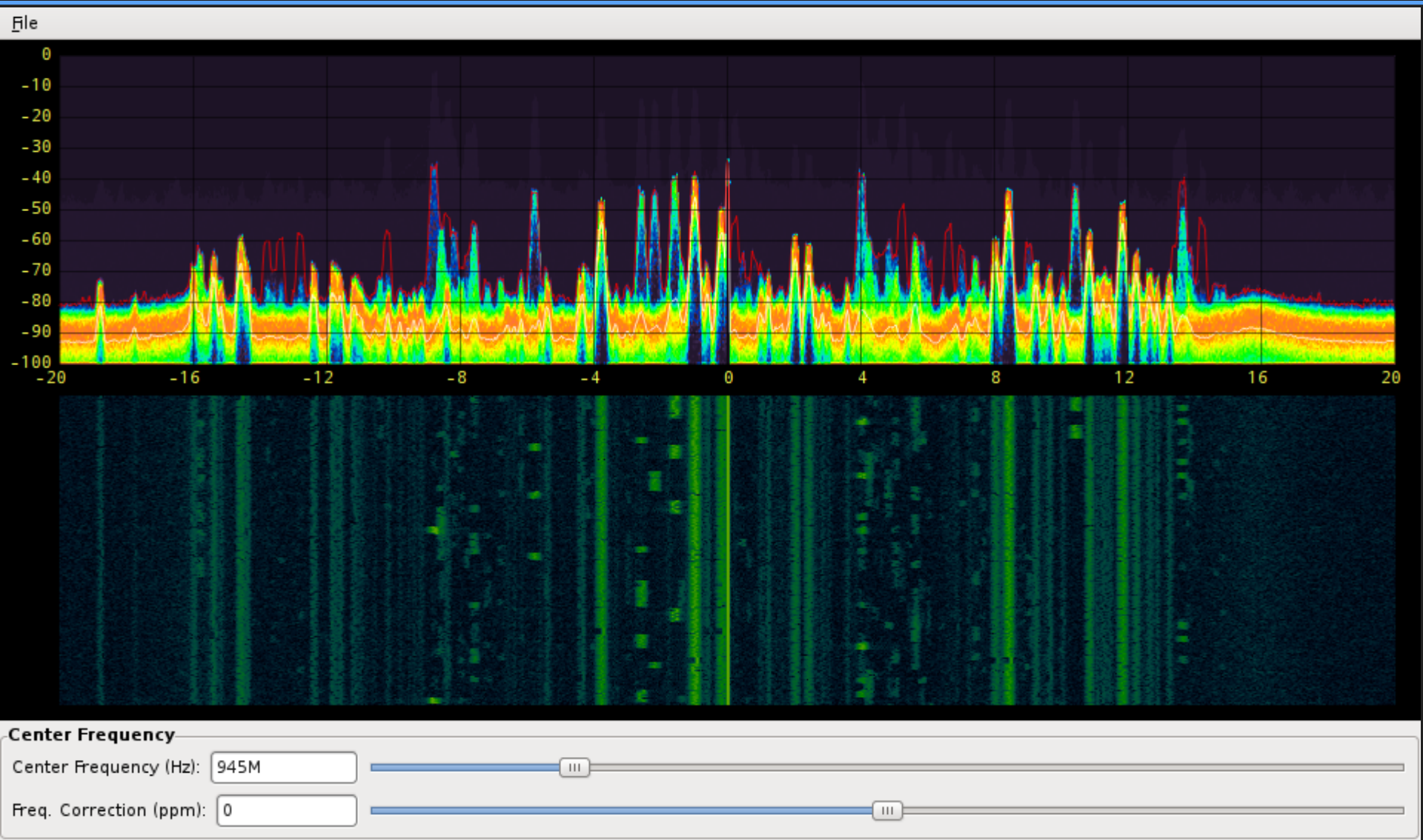
VAT Ident. No.
DE813932619

Frequency

- Easy

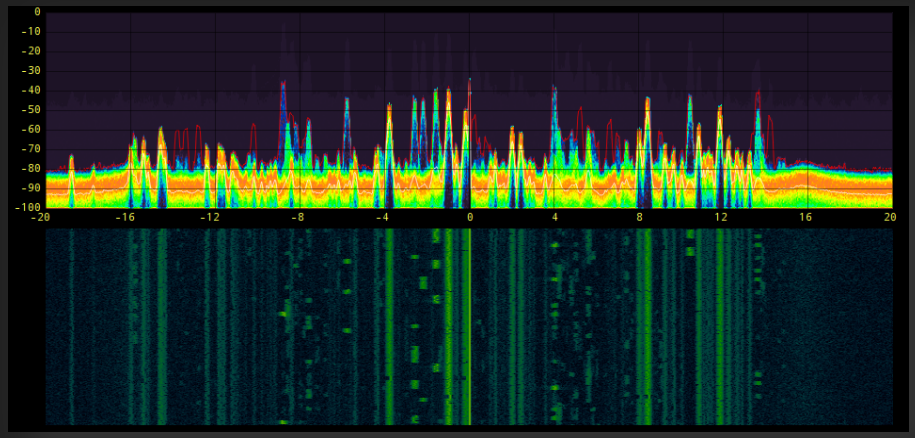
  (in that case)

GR-Fosphor

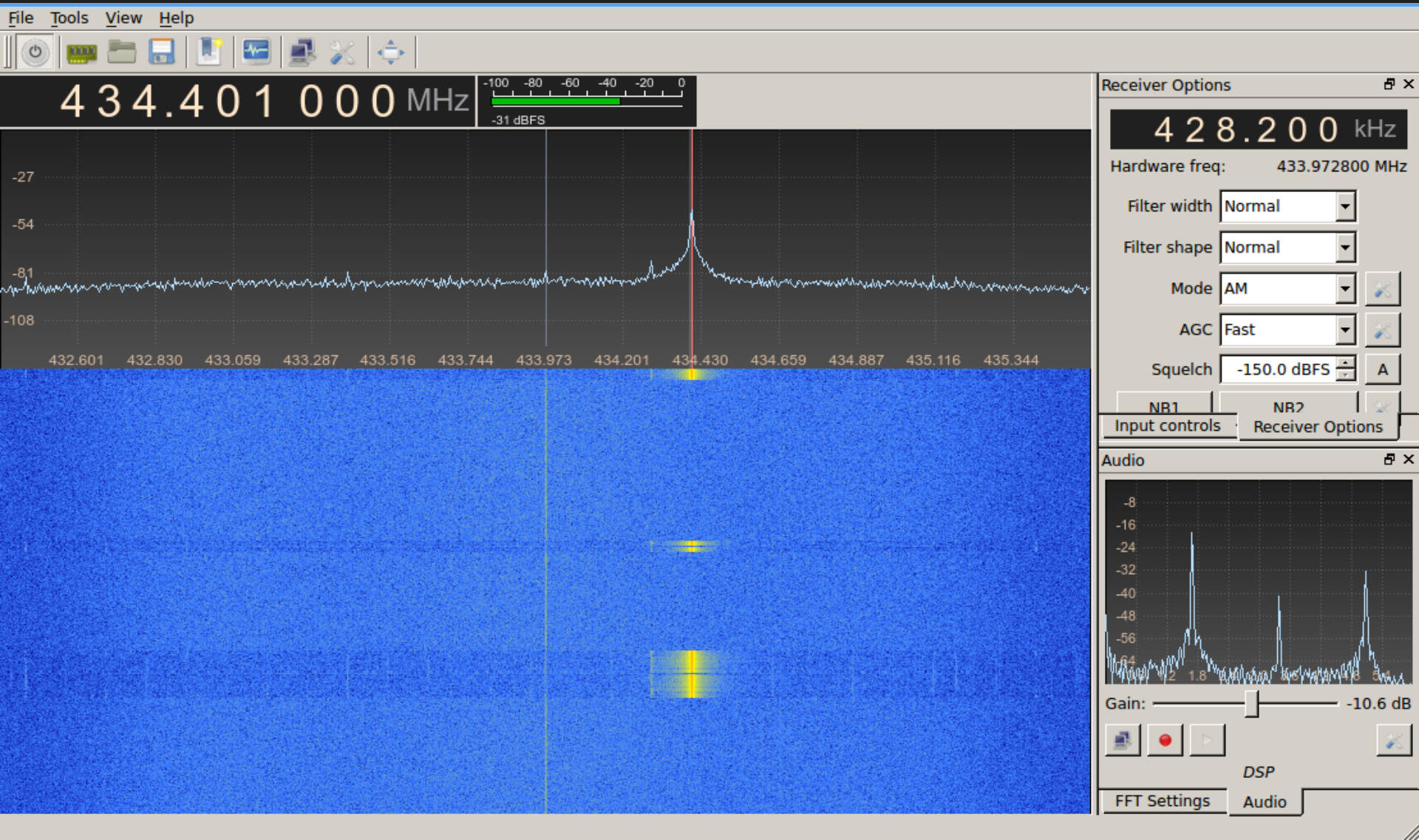

File
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-20
-16
-12
-8
-4
0
4
8
12
16
20
Center Frequency
Center Frequency (Hz):
945M
Freq. Correction (ppm):
0

GR-Fosphor

- Visualization only
- Power spectrum
- Waterfall
- Uses **all** samples
  - Low duty-cycle
- Beautiful

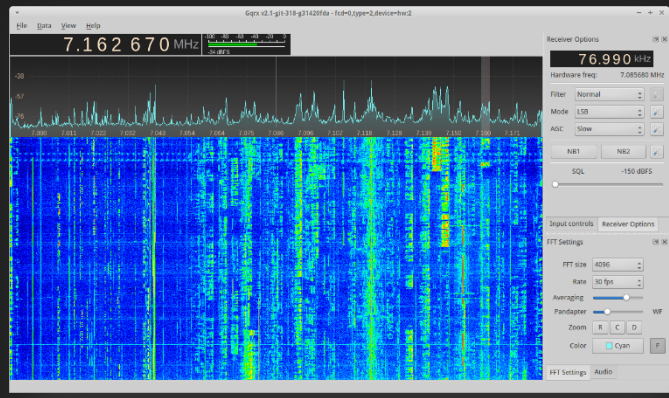


Gqrx

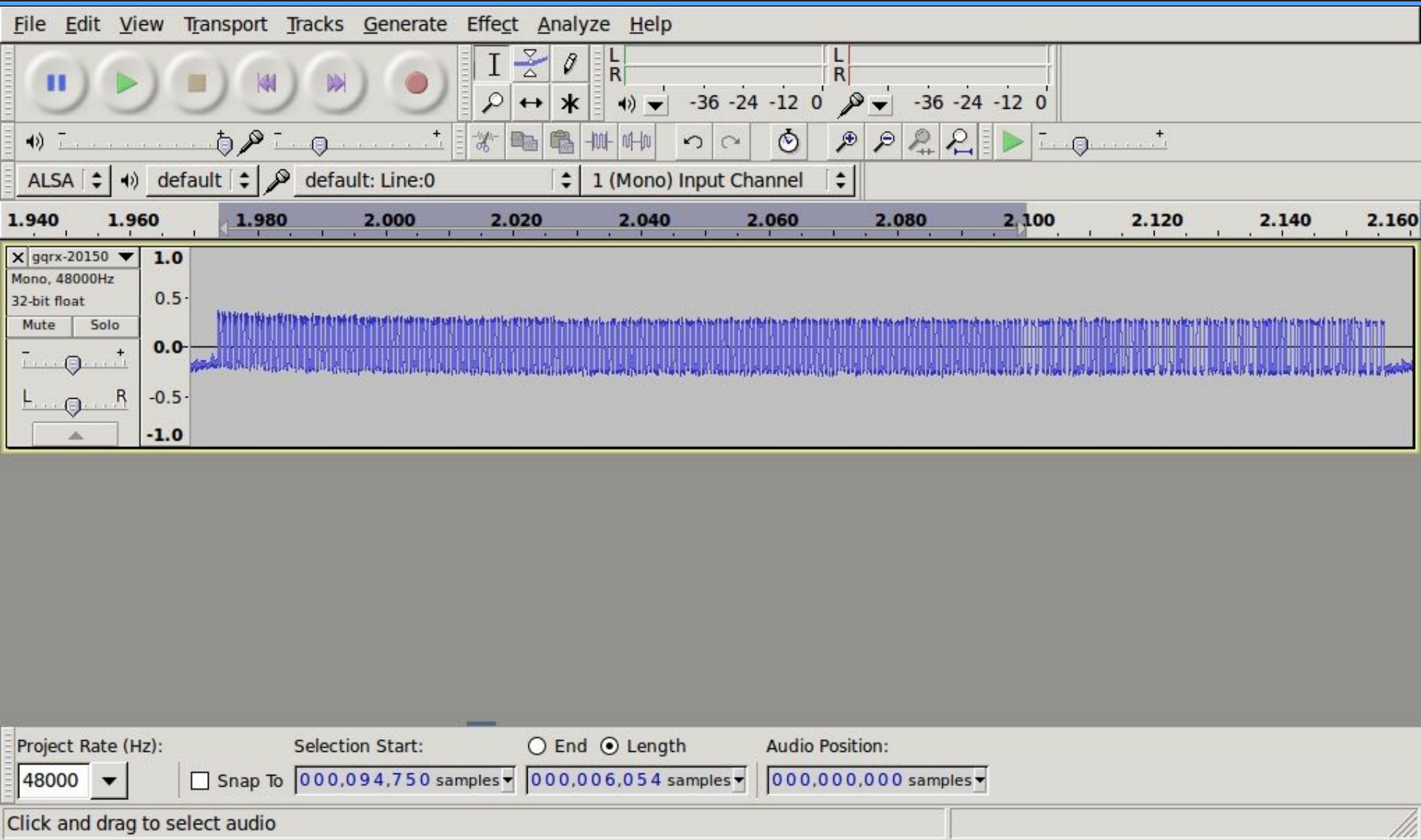

File Tools View Help
434.401 000 MHz
-100 -80 -60 -40 -20 0
-31 dBFS
-27
-54
-81
-108
432.601 432.830 433.059 433.287 433.516 433.744 433.973 434.201 434.430 434.659 434.887 435.116 435.344
Receiver Options
428.200 kHz
Hardware freq: 433.972800 MHz
Filter width Normal
Filter shape Normal
Mode AM
AGC Fast
Squelch -150.0 dBFS
A
NB1
NB2
Input controls
Receiver Options
Audio
-8
-16
-24
-32
-40
-48
-56
-64
Gain: -10.6 dB
DSP
FFT Settings
Audio

Gqrx

- Developed by Alexandru Csete (OZ9AEC)
- Visualization
- Decoders
- Audio recording / streaming

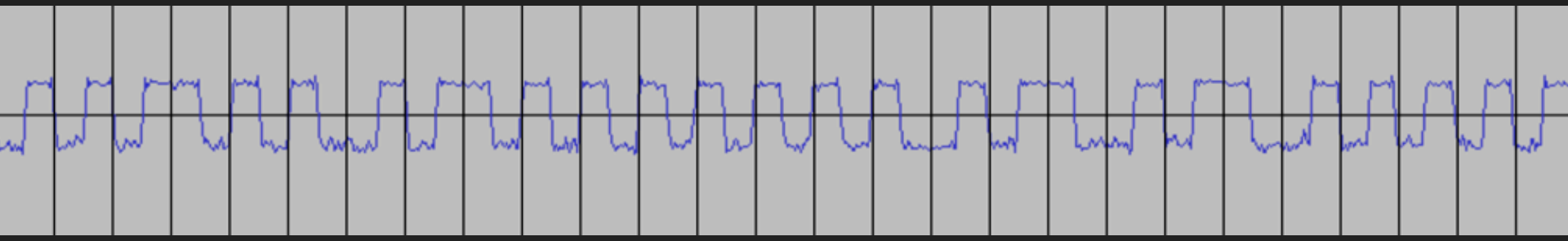


Audacity

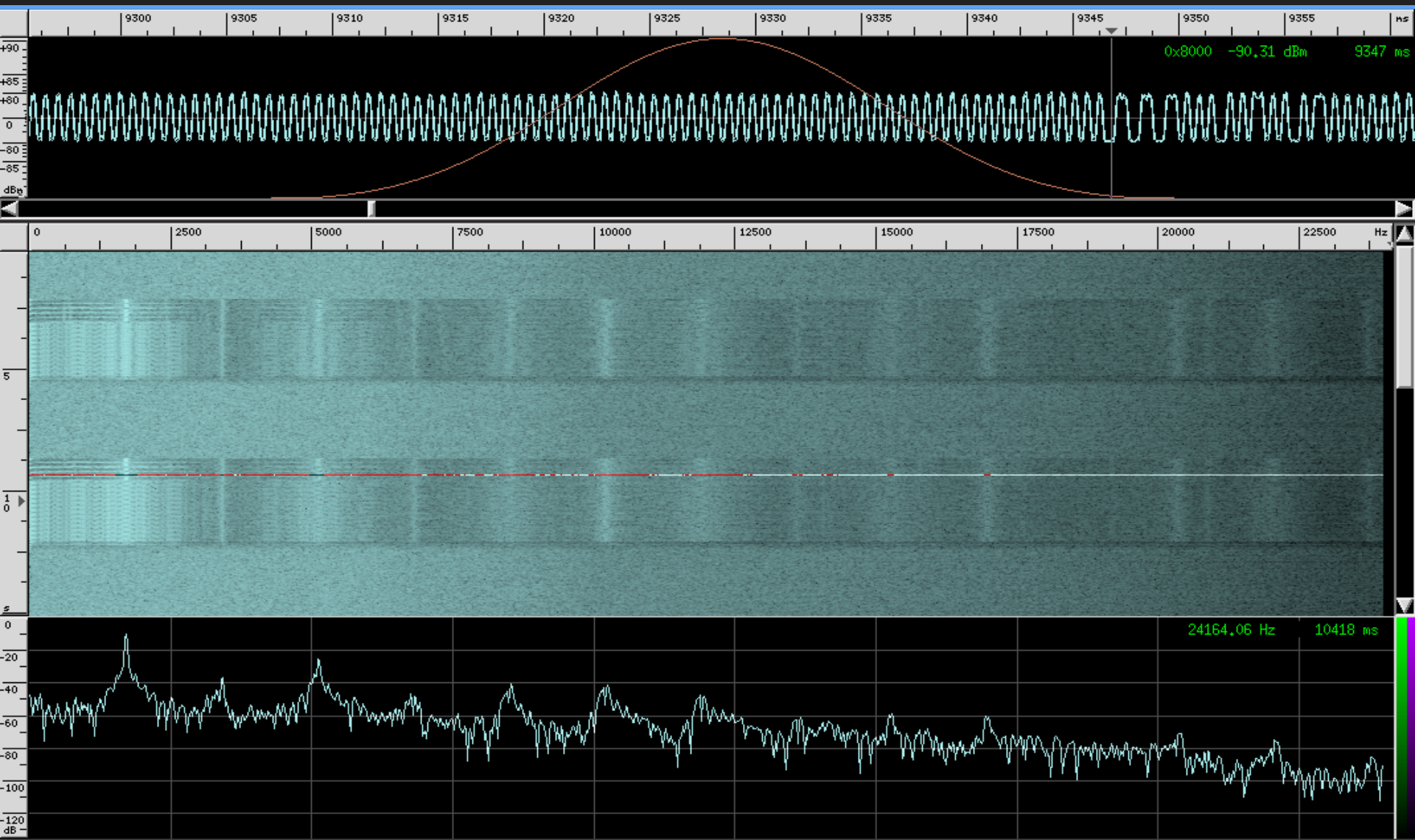

File Edit View Transport Tracks Generate Effect Analyze Help
-36 -24 -12 0
ALSA
default
default: Line:0
1 (Mono) Input Channel
1.940 1.960 1.980 2.000 2.020 2.040 2.060 2.080 2.100 2.120 2.140 2.160
gqrx-20150
Mono, 48000Hz
32-bit float
Mute Solo
1.0 0.5 0.0 -0.5 -1.0
Project Rate (Hz):
48000
Snap To
Selection Start:
End Length
Audio Position:
000,094,750 samples
000,006,054 samples
000,000,000 samples
Click and drag to select audio

Audacity

- Audio tool
- … and a waveform explorer



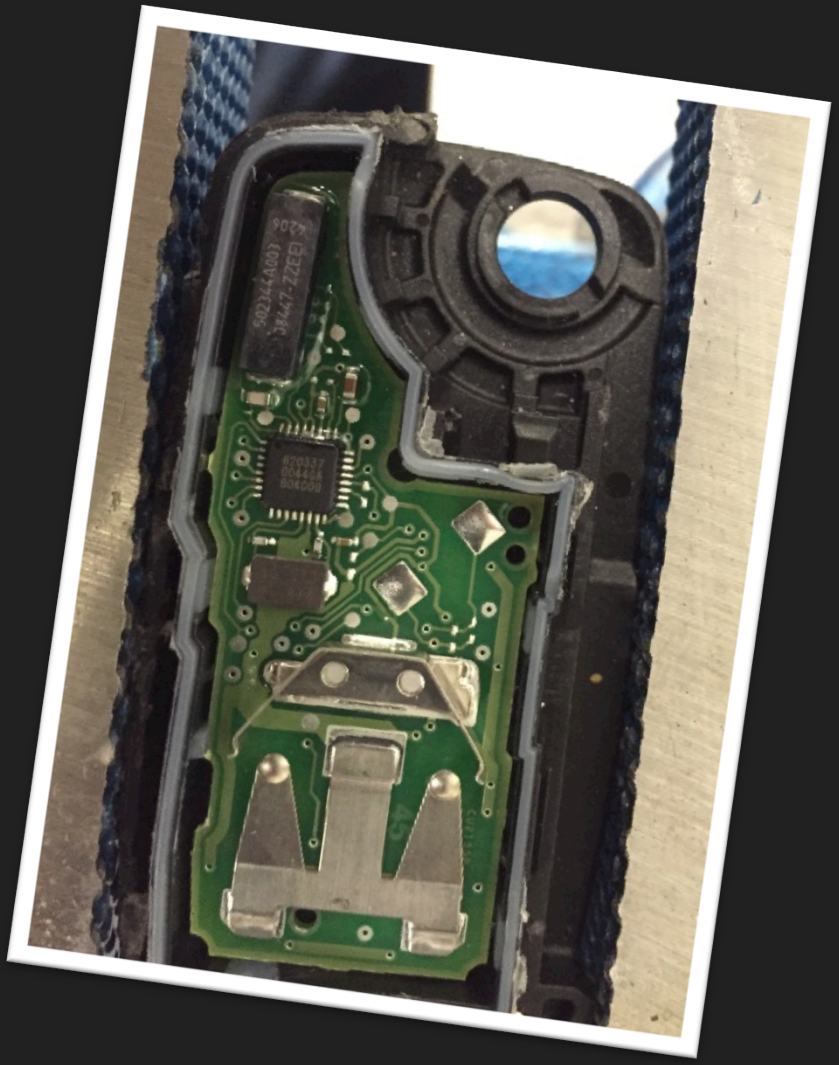
Baudline


9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
ms
+90
+85
+80
0
-80
-85
dBm
0x8000 -90.31 dBm 9347 ms
0
2500
5000
7500
10000
12500
15000
17500
20000
22500
Hz
5
1
0
0
-20
-40
-60
-80
-100
-120
dB
24164.06 Hz 10418 ms

Checklist

- ✔ Frequency: ~434.4 MHz
- ✔ Modulation: On-Off Keying
- ✔ Encoding: Manchester
- ✔ Bit rate: ~1700 bit/s
- ✔ Start of frame pattern: 10101000

Disassemble Key Fob

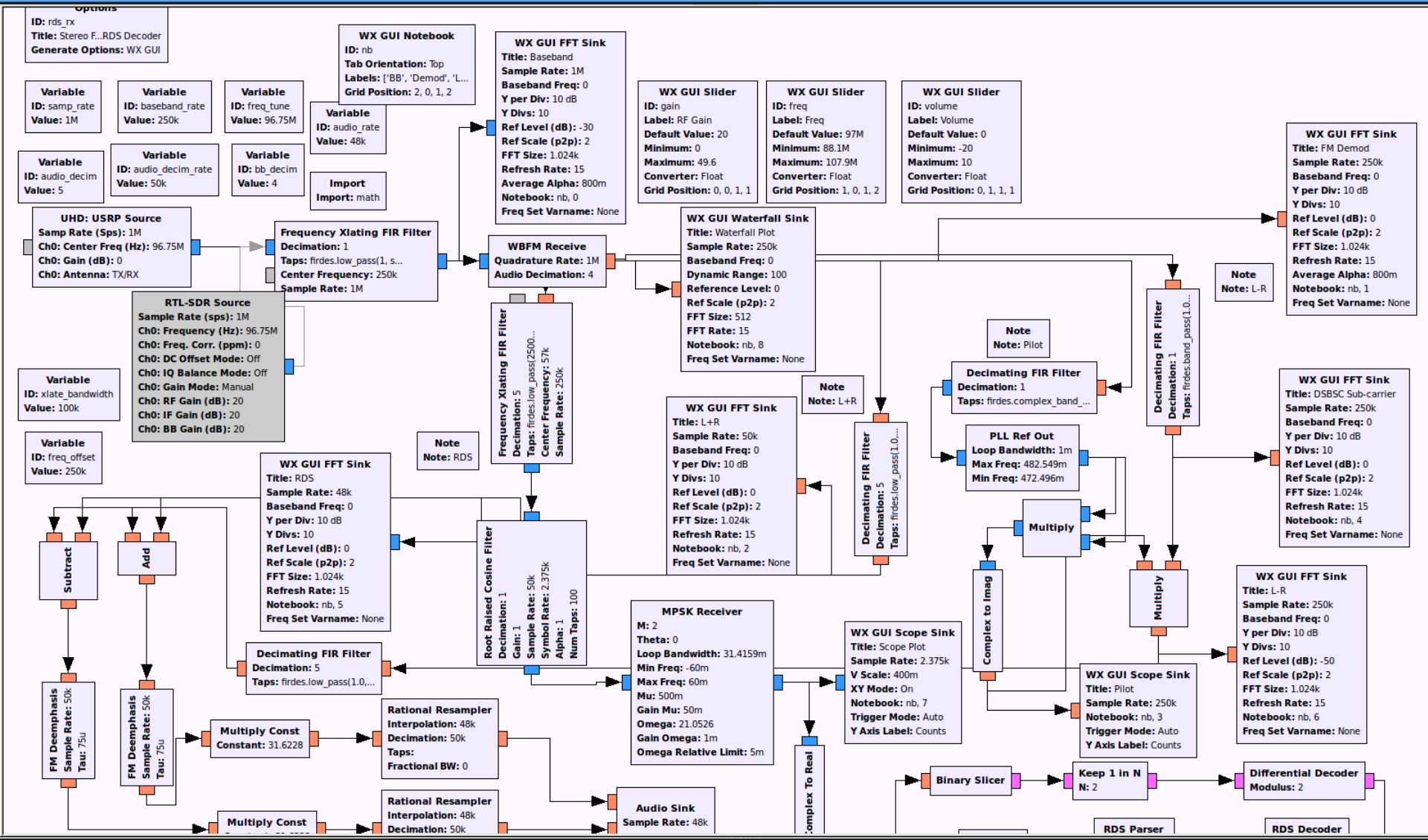


Disassemble Key Fob

- Oscillator 13.575MHz

- 13.575 MHz / 8000 = 1697 Hz
- 13.575 MHz * 32 = 434.4 MHz

GNU Radio


Options
ID: rds_rx
Title: Stereo F...RDS Decoder
Generate Options: WX GUI
WX GUI Notebook
ID: nb
Tab Orientation: Top
Labels: ['BB', 'Demod', 'L...
Grid Position: 2, 0, 1, 2
WX GUI FFT Sink
Title: Baseband
Sample Rate: 1M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -30
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 800m
Notebook: nb, 0
Freq Set Varname: None
WX GUI Slider
ID: gain
Label: RF Gain
Default Value: 20
Minimum: 0
Maximum: 49.6
Converter: Float
Grid Position: 0, 0, 1, 1
WX GUI Slider
ID: freq
Label: Freq
Default Value: 97M
Minimum: 88.1M
Maximum: 107.9M
Converter: Float
Grid Position: 1, 0, 1, 2
WX GUI Slider
ID: volume
Label: Volume
Default Value: 0
Minimum: -20
Maximum: 10
Converter: Float
Grid Position: 0, 1, 1, 1
Variable
ID: samp_rate
Value: 1M
Variable
ID: baseband_rate
Value: 250k
Variable
ID: freq_tune
Value: 96.75M
Variable
ID: audio_rate
Value: 48k
Variable
ID: audio_decim
Value: 5
Variable
ID: audio_decim_rate
Value: 50k
Variable
ID: bb_decim
Value: 4
Import
Import: math
UHD: USRP Source
Samp Rate (Sps): 1M
Ch0: Center Freq (Hz): 96.75M
Ch0: Gain (dB): 0
Ch0: Antenna: TX/RX
Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1, s...
Center Frequency: 250k
Sample Rate: 1M
WBFM Receive
Quadrature Rate: 1M
Audio Decimation: 4
WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 250k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Notebook: nb, 8
Freq Set Varname: None
WX GUI FFT Sink
Title: FM Demod
Sample Rate: 250k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 800m
Notebook: nb, 1
Freq Set Varname: None
Note
Note: L-R
RTL-SDR Source
Sample Rate (sps): 1M
Ch0: Frequency (Hz): 96.75M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 20
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Frequency Xlating FIR Filter
Decimation: 5
Taps: firdes.low_pass(2500...
Center Frequency: 57k
Sample Rate: 250k
Note
Note: Pilot
Decimating FIR Filter
Decimation: 1
Taps: firdes.complex_band_...
Decimating FIR Filter
Decimation: 1
Taps: firdes.band_pass(1.0...
Variable
ID: xlate_bandwidth
Value: 100k
Note
Note: L+R
WX GUI FFT Sink
Title: L+R
Sample Rate: 50k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 2
Freq Set Varname: None
Decimating FIR Filter
Decimation: 5
Taps: firdes.low_pass(1.0,...
PLL Ref Out
Loop Bandwidth: 1m
Max Freq: 482.549m
Min Freq: 472.496m
WX GUI FFT Sink
Title: DSBSC Sub-carrier
Sample Rate: 250k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 4
Freq Set Varname: None
Variable
ID: freq_offset
Value: 250k
Note
Note: RDS
WX GUI FFT Sink
Title: RDS
Sample Rate: 48k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 5
Freq Set Varname: None
Multiply
Subtract
Add
Root Raised Cosine Filter
Decimation: 1
Gain: 1
Sample Rate: 50k
Symbol Rate: 2.375k
Alpha: 1
Num Taps: 100
Complex to Imag
Multiply
WX GUI FFT Sink
Title: L-R
Sample Rate: 250k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): -50
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Notebook: nb, 6
Freq Set Varname: None
Decimating FIR Filter
Decimation: 5
Taps: firdes.low_pass(1.0,...
MPSK Receiver
M: 2
Theta: 0
Loop Bandwidth: 31.4159m
Min Freq: -60m
Max Freq: 60m
Mu: 500m
Gain Mu: 50m
Omega: 21.0526
Gain Omega: 1m
Omega Relative Limit: 5m
WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 2.375k
V Scale: 400m
XY Mode: On
Notebook: nb, 7
Trigger Mode: Auto
Y Axis Label: Counts
WX GUI Scope Sink
Title: Pilot
Sample Rate: 250k
Notebook: nb, 3
Trigger Mode: Auto
Y Axis Label: Counts
FM Deemphasis
Sample Rate: 50k
Tau: 75u
FM Deemphasis
Sample Rate: 50k
Tau: 75u
Multiply Const
Constant: 31.6228
Rational Resampler
Interpolation: 48k
Decimation: 50k
Taps:
Fractional BW: 0
Complex To Real
Binary Slicer
Keep 1 in N
N: 2
Differential Decoder
Modulus: 2
Multiply Const
Rational Resampler
Interpolation: 48k
Decimation: 50k
Audio Sink
Sample Rate: 48k
RDS Parser
RDS Decoder

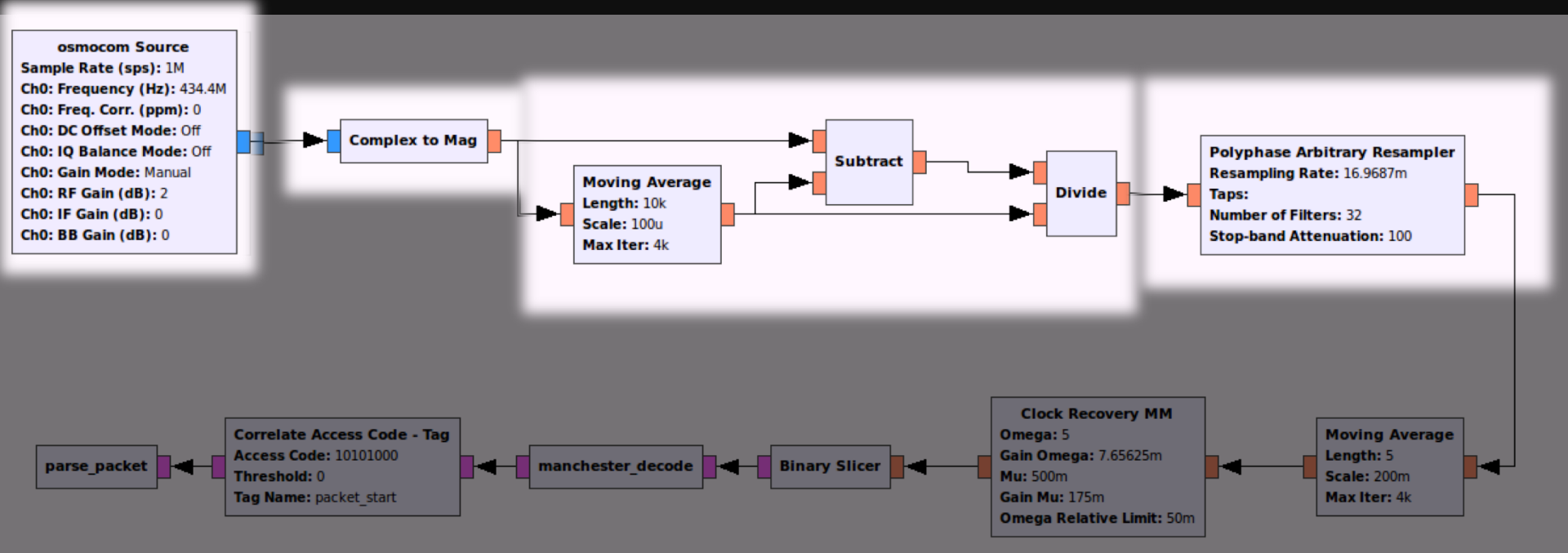
GNU Radio

Sample Source

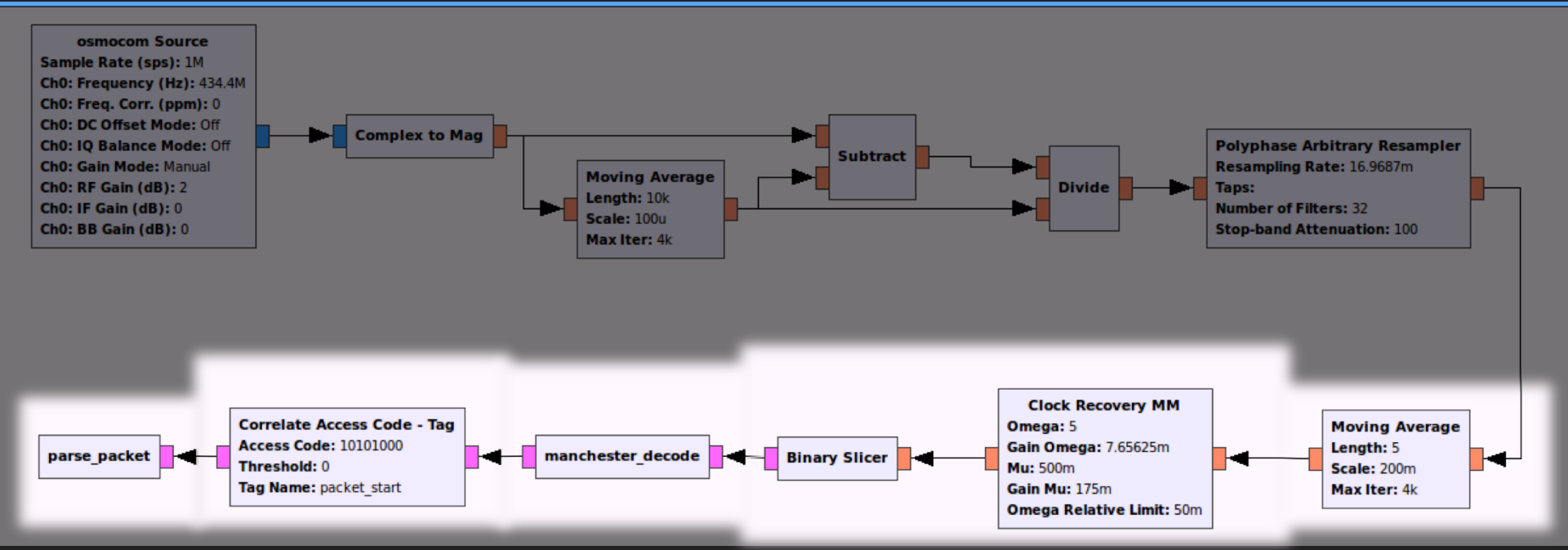
Magnitude

Normalize

Resample



GNU Radio



Parse

SFD Search

Decode

Clock Recovery

Filter

GNURadio

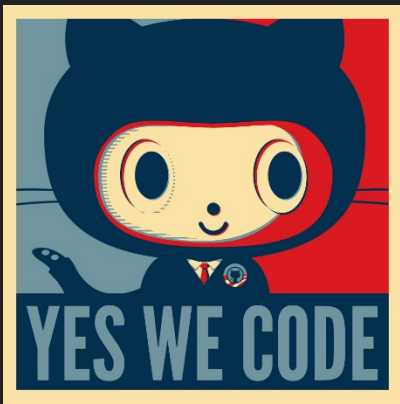
```
11001010101010000110111010011111011001100011110101011101001110110 00101010 CLOSE
11001010101010000110111010011111011001100011110101011101001110110 00101010 CLOSE
11001010101010000110111010011111011001100011110101011101001110110 00101010 CLOSE
00111010100100101111111110111001010000011100100001010110100101000 01000110 TRUNK
00111010100100101111111110111001010000011100100001010110100101000 01000110 TRUNK
00111010100100101111111110111001010000011100100001010110100101000 01000110 TRUNK
10111001101010101110100010011111110010000011100111011010010101000 00011100 OPEN
10111001101010101110100010011111110010000011100111011010010101000 00011100 OPEN
10111001101010101110100010011111110010000011100111011010010101000 00011100 OPEN
```

Rolling Code

Command

Conclusion

- Overview of tools / workflow
- Open Source
- http://github.com/bastibl/gr-keyfob/
- Study rolling codes



Thanks to Freepik @ www.flaticon.com for beautiful icons.

Reverse Engineering Digital Signals

Bastian Bloessl

✉ bloessl@ccs-labs.org

http://www.bastibl.net

HAM RADIO 2015 ▪ SDR Academy ▪ June 27, 2015