Signal SAFARI

MWR LABS

BSidesNYC 2018

Welcome!

- Curious about RF?
- Looking for awesome new projects?
- Seeking adventure?

MWR LABS

Agenda

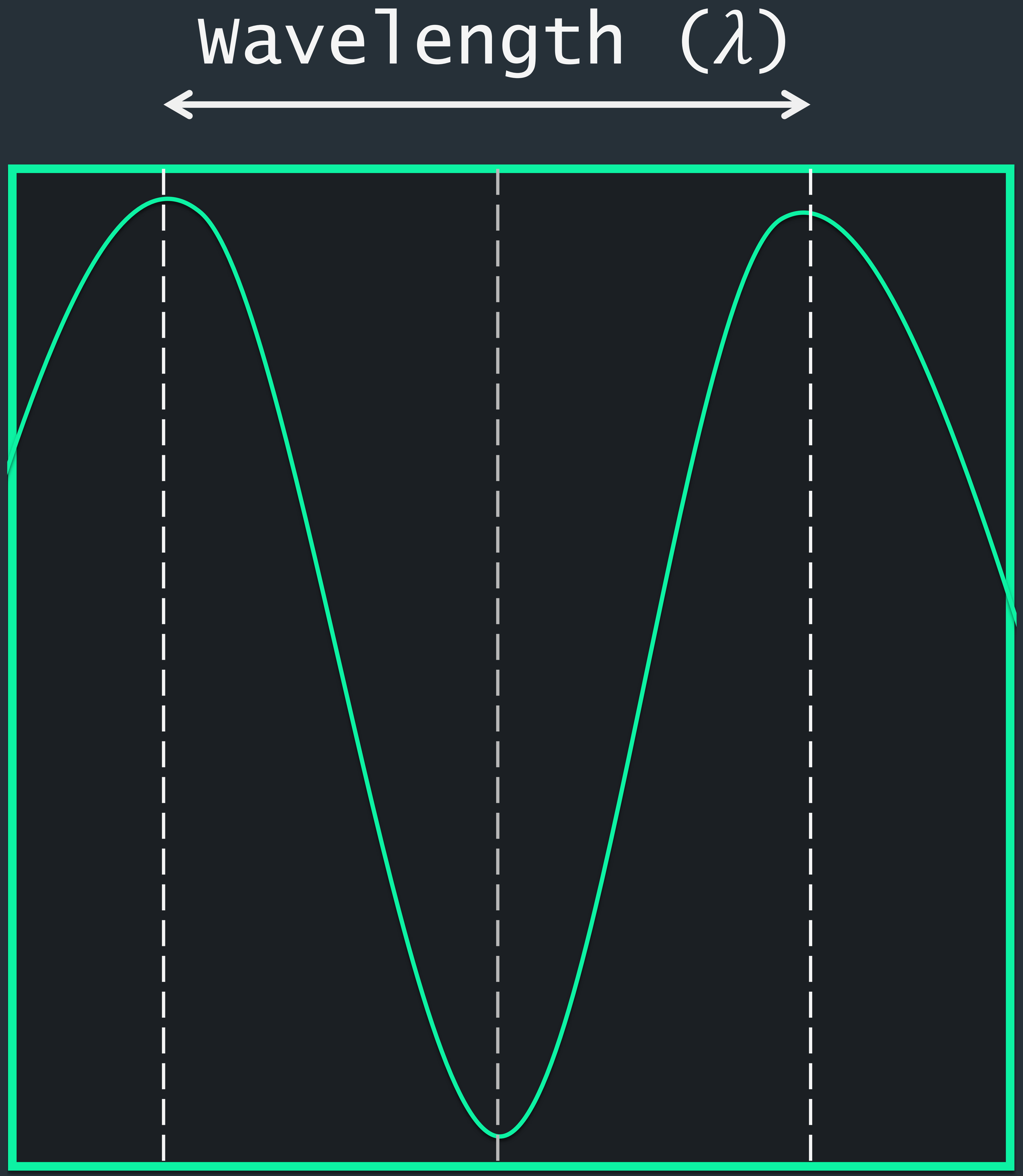
- RF Overview / Exploration
  - GQRX
- Light Switch Reversing
  - RTL_433
- Fan Controller
  - GNU Radio Companion (GRC)
- Signal Security
- Continuing the Adventure

Safari Guide

Katie Knowles, @_sigil

- Security Consultant, MWR InfoSecurity
- RF Enthusiast
- Infosec Explorer

MWR INFOSECURITY



Fundamentals

- RF travels as electromagnetic (EM) waves
- EM waves travel at the speed of light (c)
- Wavelength (λ): The length of the wave
- Frequency (f): How many wavelengths happen in a unit of time, based on the wave’s speed
- Multiplying Wavelength (λ) by Frequency (f) will always equal the speed of light (c)

$$c = 3 * 10^8\, m/s = f * \lambda$$

Investigating Unknown Signals:

RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3

+

=

✨

RTL-SDR

(~$30)

Linux

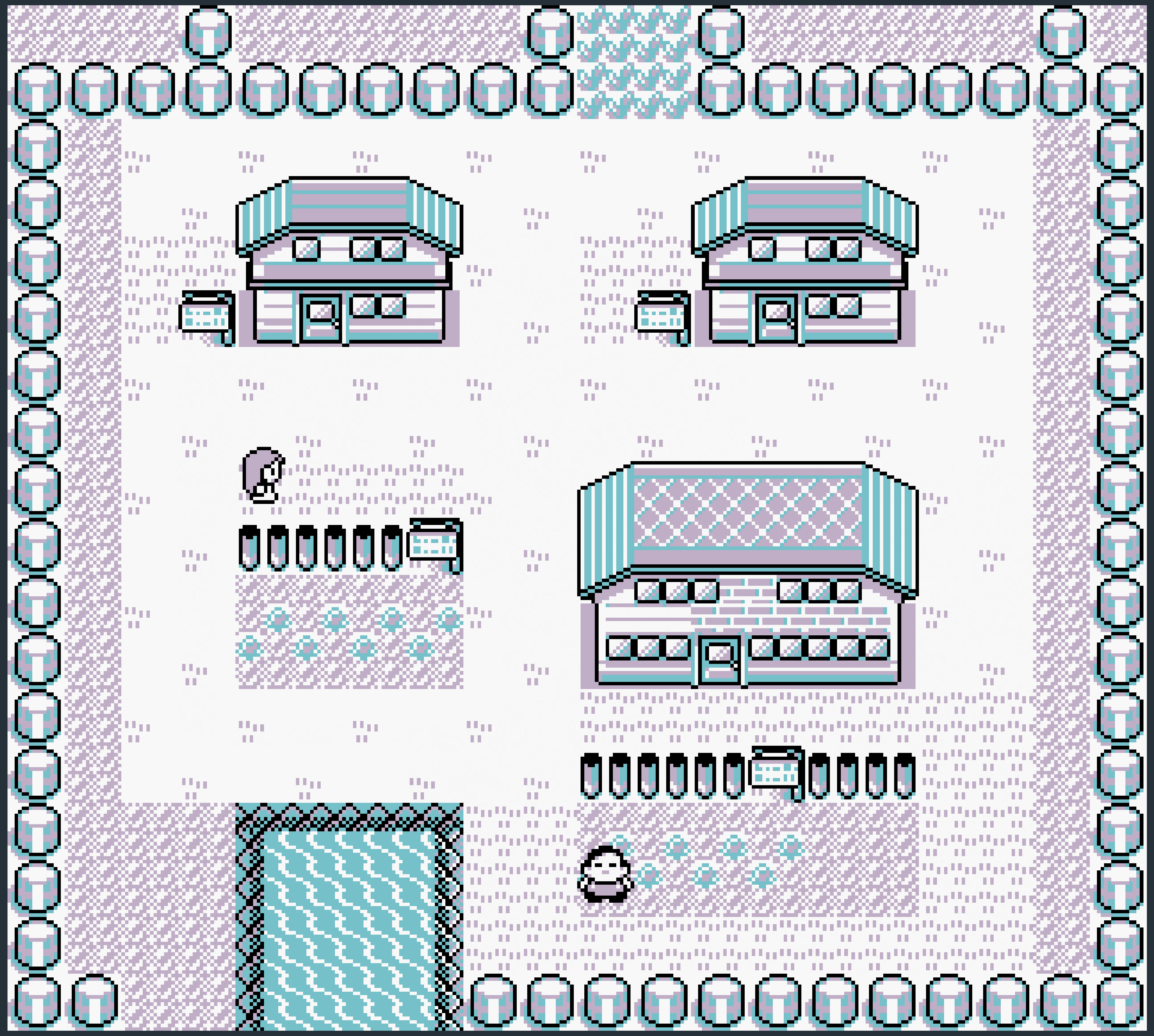
(Free)

MAGIC!

(Priceless)

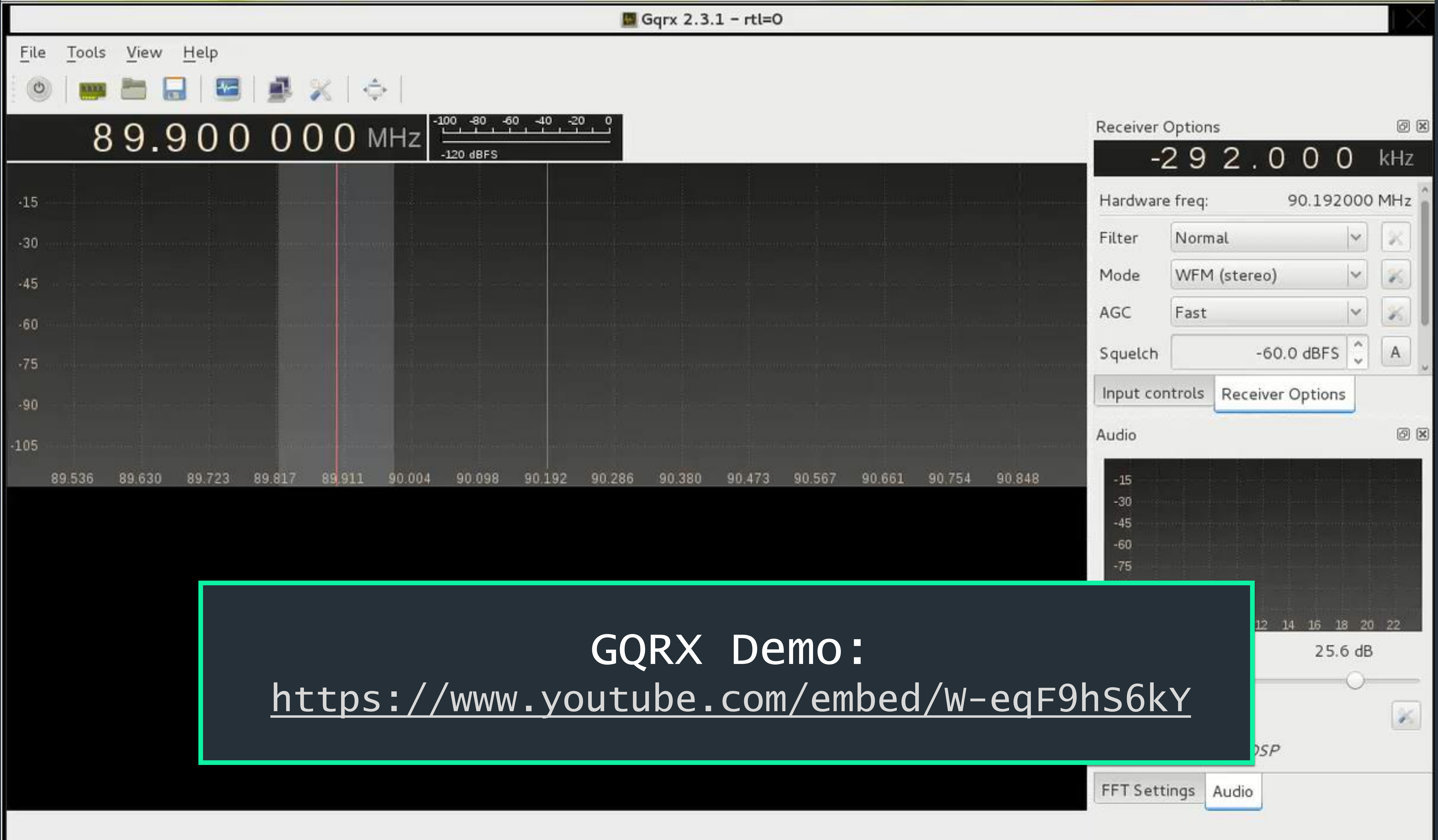
MWR LABS

First Steps with GQRX



- Simple program for tuning Software Defined Radios (SDRs)
- “Waterfall” view of activity at different frequencies over time
- Frequency range limited based on hardware of SDR in use

http://gqrx.dk/



89.900 000 MHz

-292.000 kHz

Hardware freq: 90.192000 MHz

Filter: Normal

Mode: WFM (stereo)

AGC: Fast

Squelch: -60.0 dBFS

25.6 dB

GQRX Demo:

https://www.youtube.com/embed/W-eqF9hS6kY

Signal Safari

MWR LABS

AM Radio
525-1705 kHz

“Ham” Radio

FM Radio
88-108 MHz

Television
54-88 MHz
174-216 MHz
480-806 MHz

WiFi
2.4 GHz
5 GHz

Cell

MF

HF

VHF

UHF

SHF

300 kHz

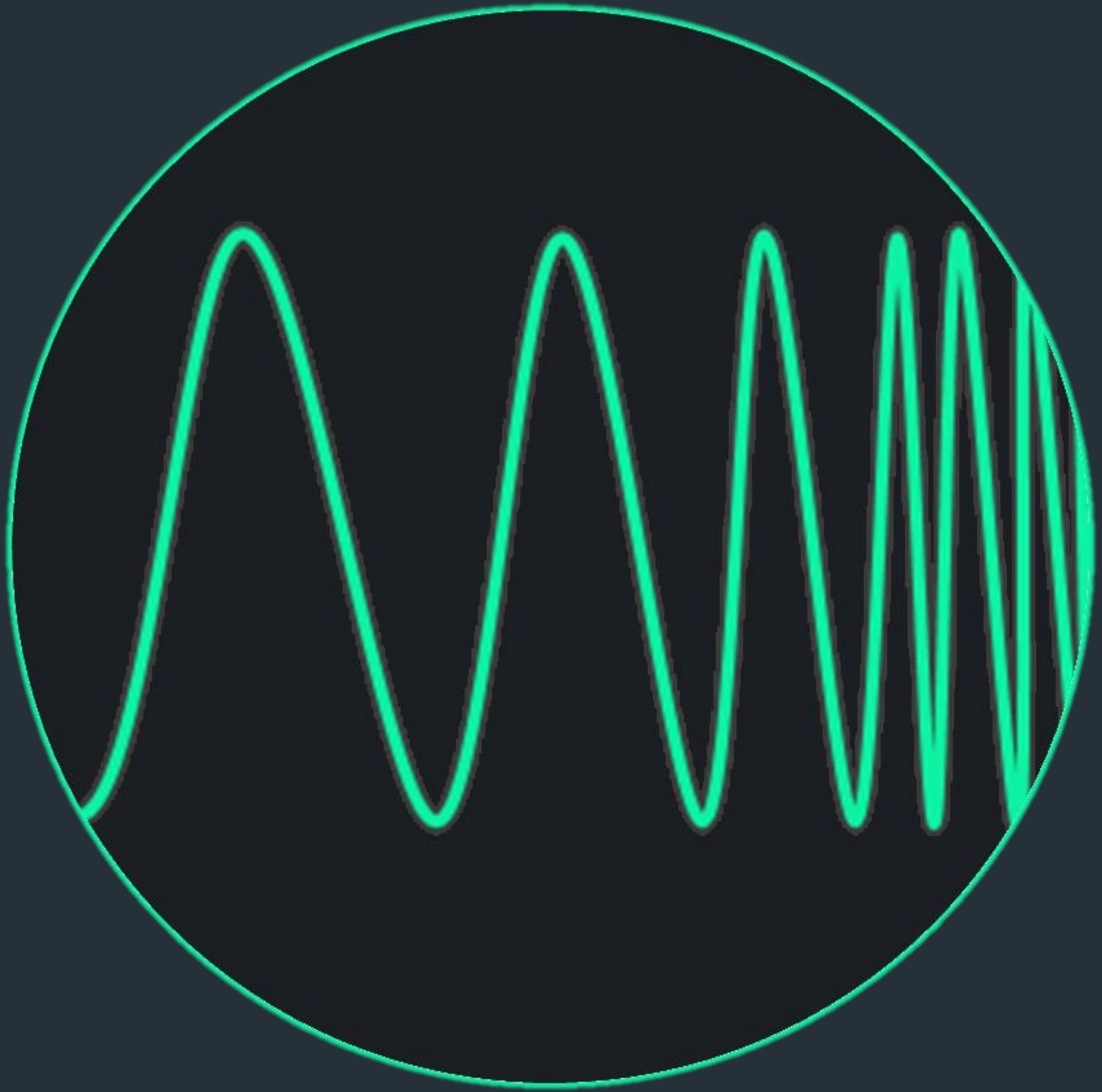
3 MHz

30 MHz

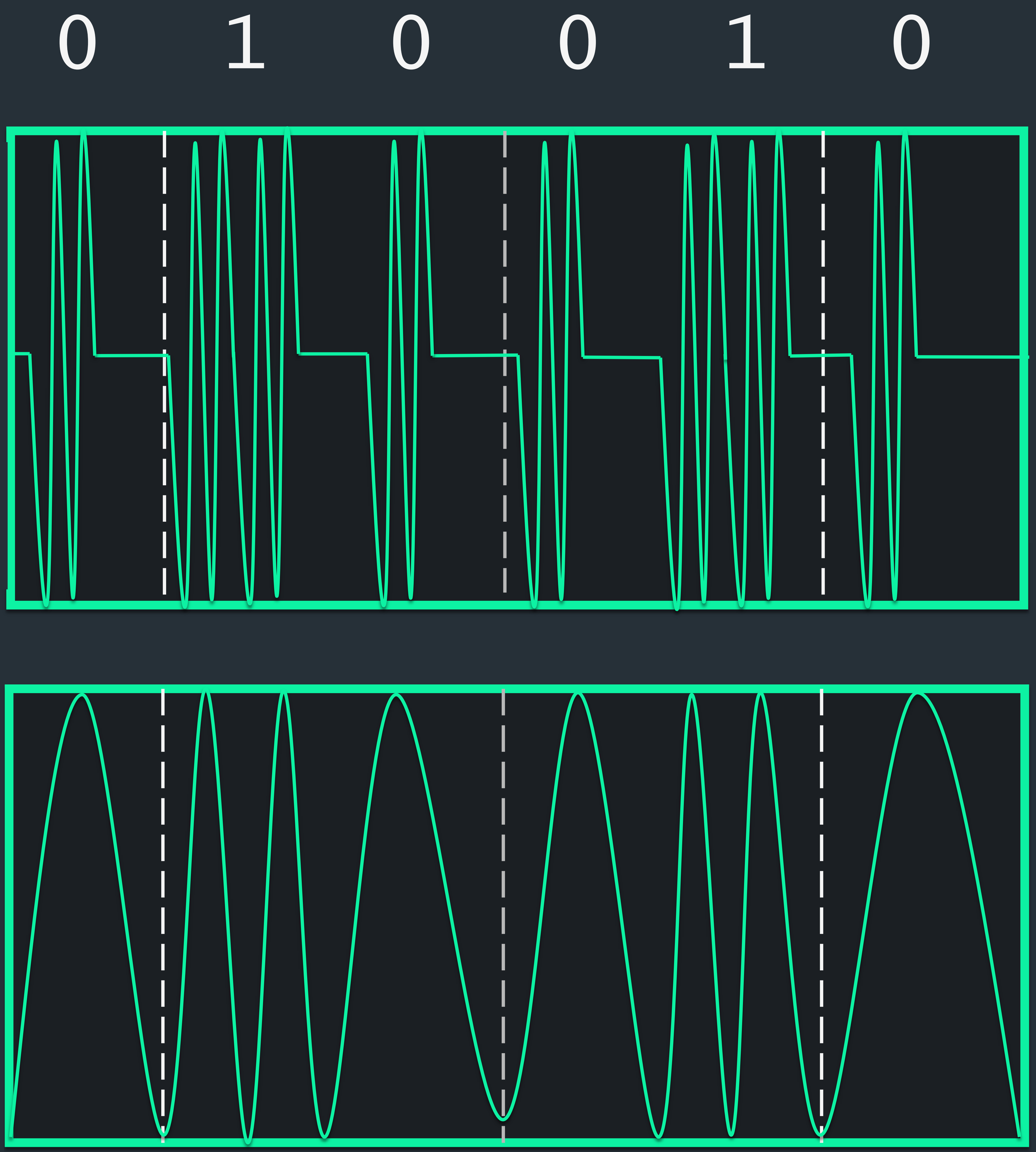
300 MHz

3 GHz

Short-Range Device Frequencies



Center *f*	Starts at:	Ends at:	Type
433 MHz	433.05 MHz	434.79 MHz	ISM
915 MHz	902 MHz	928 MHz	ISM
2.45 GHz	2.4 GHz	2.5 GHz	ISM
5.8 GHz	5.725 GHz	5.875 GHz	ISM
315 MHz	285 MHz	322 MHz	Unlicensed



Simple Control Signals

+ ASK: Amplitude-Shift Keying

Amplitude (strength) of signal communicates 1 or 0.

Pictured: A short pulse is 0, and a long pulse is 1. Also known as On-Off Keying (OOK).

+ FSK: Frequency-Shift Keying

Frequency (f) of signal communicates 1 or 0.

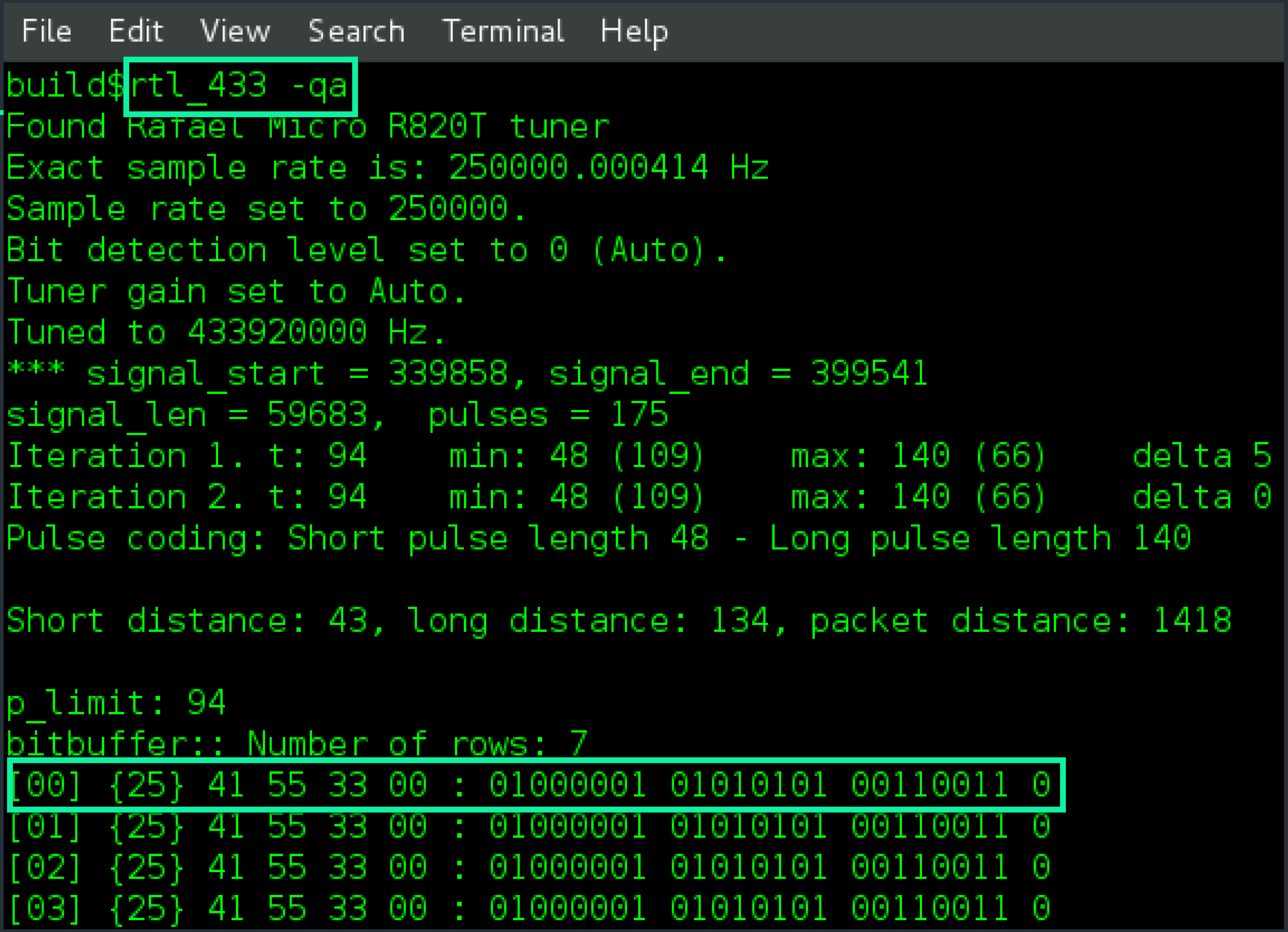
Pictured: A low frequency is 0, and a high frequency is 1.

MYSTERY SIGNAL!

Signal Safari

If only we had a tool...

SIGNAL FOUND:
010000010101010100111100

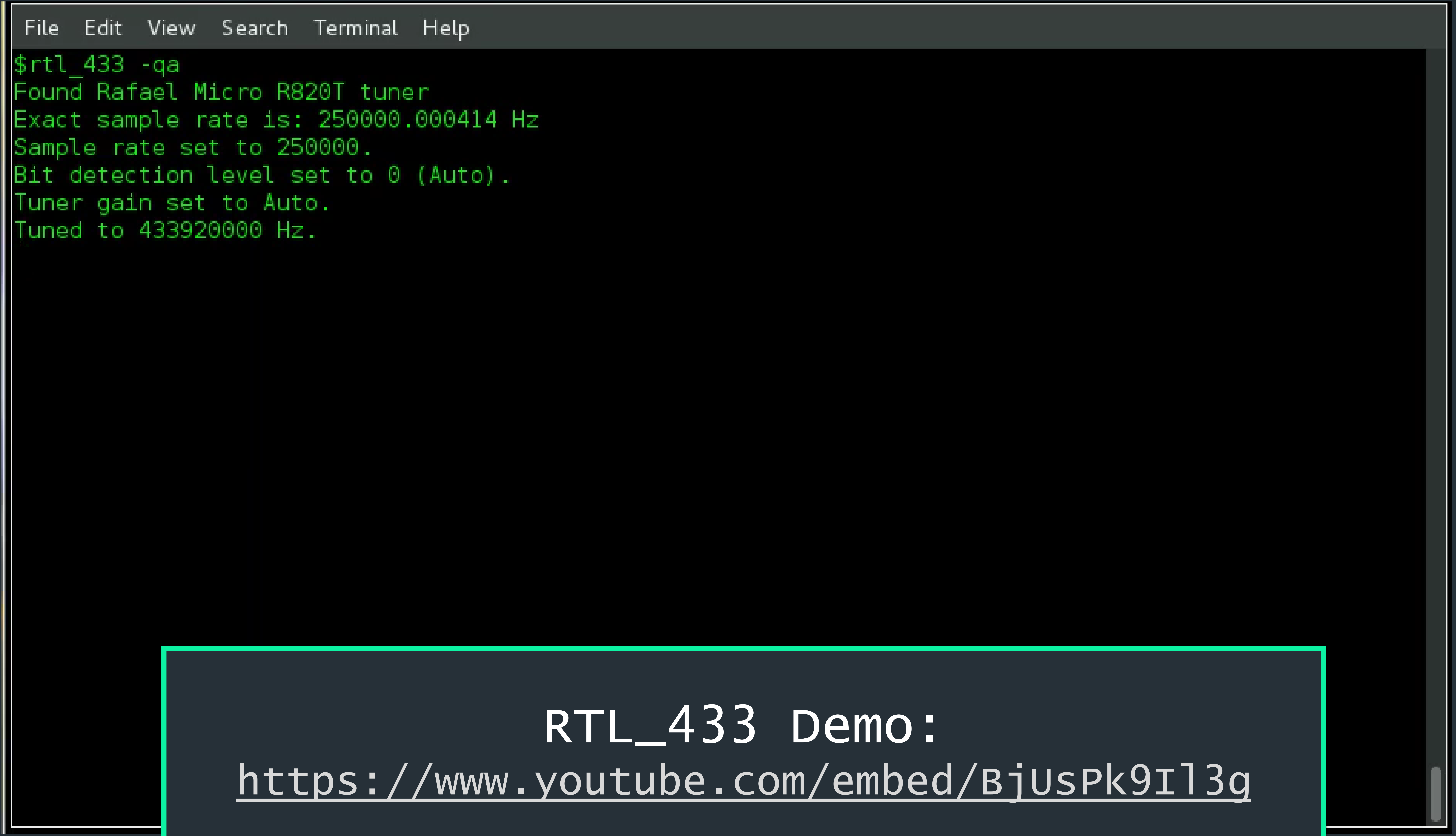


```
build$rtl_433 -qa
Found Rafael Micro R820T tuner
Exact sample rate is: 250000.000414 Hz
Sample rate set to 250000.
Bit detection level set to 0 (Auto).
Tuner gain set to Auto.
Tuned to 433920000 Hz.
*** signal_start = 339858, signal_end = 399541
signal_len = 59683,  pulses = 175
Iteration 1. t: 94    min: 48 (109)    max: 140 (66)    delta 5
Iteration 2. t: 94    min: 48 (109)    max: 140 (66)    delta 0
Pulse coding: Short pulse length 48 - Long pulse length 140

Short distance: 43, long distance: 134, packet distance: 1418

p_limit: 94
bitbuffer:: Number of rows: 7
[00] {25} 41 55 33 00 : 01000001 01010101 00110011 0
[01] {25} 41 55 33 00 : 01000001 01010101 00110011 0
[02] {25} 41 55 33 00 : 01000001 01010101 00110011 0
[03] {25} 41 55 33 00 : 01000001 01010101 00110011 0
```

https://github.com/merbanan/rtl_433

RTL_433

- Command-line
- Identifies unknown signals
- Focused on 433 MHz range
- Can be tuned to search at specific frequencies and other ranges



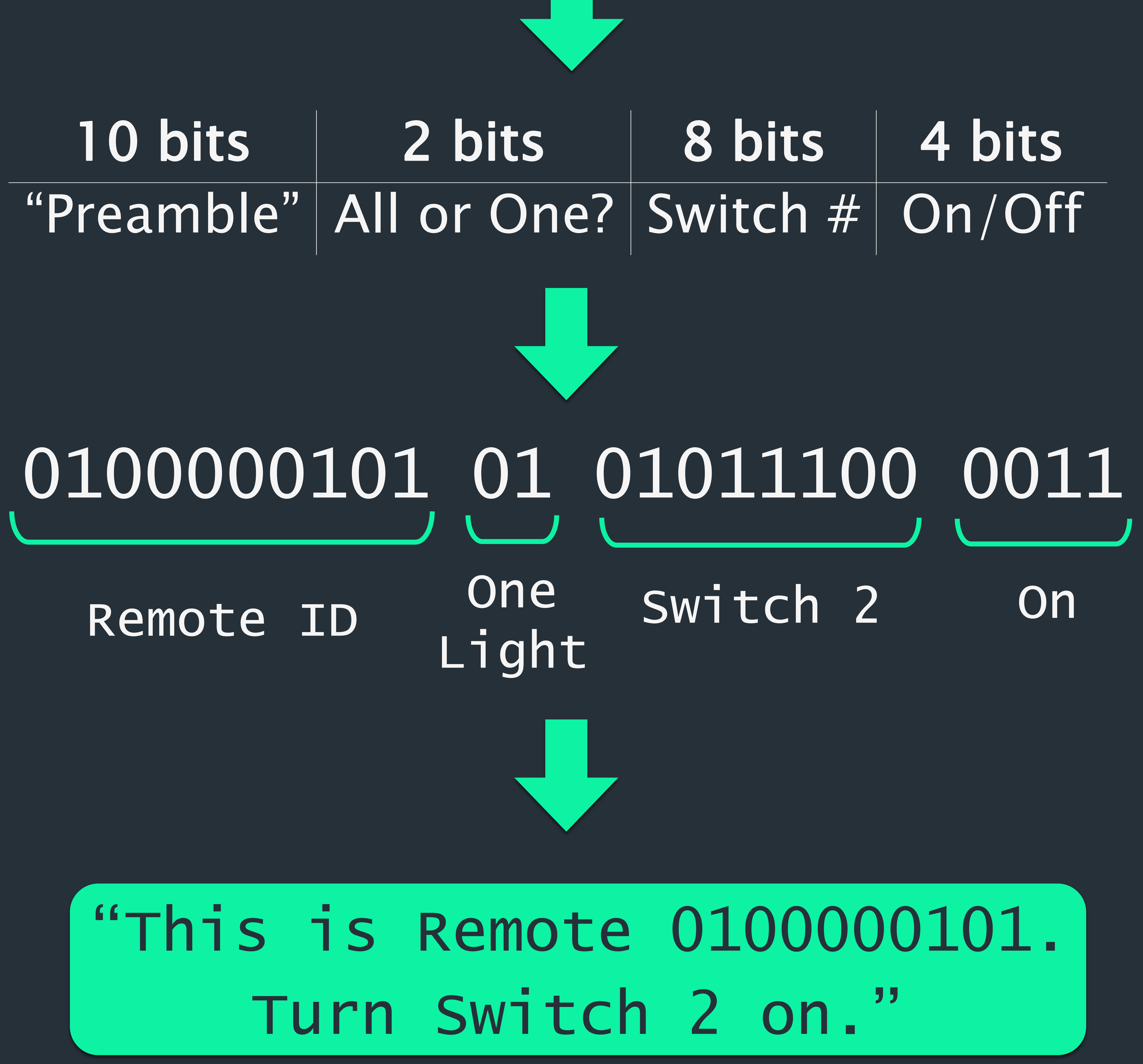
```
$rtl_433 -qa
Found Rafael Micro R820T tuner
Exact sample rate is: 250000.000414 Hz
Sample rate set to 250000.
Bit detection level set to 0 (Auto).
Tuner gain set to Auto.
Tuned to 433920000 Hz.
```

RTL_433 Demo:

https://www.youtube.com/embed/BjUsPk9Il3g

Command Map

Switch	State	RF Command
1	On	0100000101 01 01010011 0011
1	Off	0100000101 01 01010011 1100
2	On	0100000101 01 01011100 0011
2	Off	0100000101 01 01011100 1100
3	On	0100000101 01 01110000 0011
3	Off	0100000101 01 01110000 1100
4	On	0100000101 01 11010000 0011
4	Off	0100000101 01 11010000 1100
All	On	0100000101 11 01010000 0011
All	Off	0100000101 11 01010000 1100



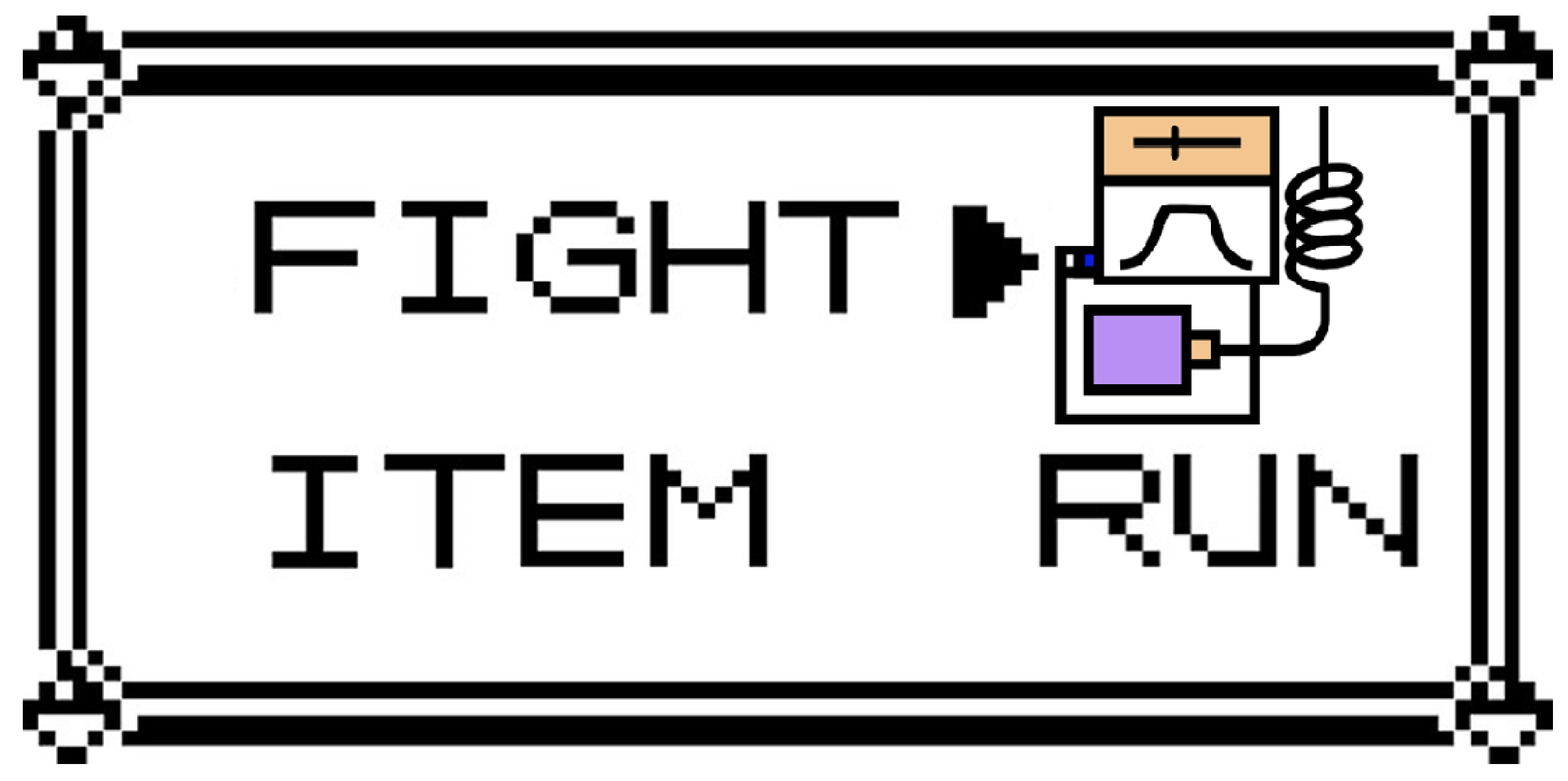
10 bits	2 bits	8 bits	4 bits
"Preamble"	All or One?	Switch #	On/Off

$$\underbrace{0100000101}_{\text{Remote ID}}\ \underbrace{01}_{\text{One Light}}\ \underbrace{01011100}_{\text{Switch 2}}\ \underbrace{0011}_{\text{On}}$$

"This is Remote 0100000101. Turn Switch 2 on."

MYSTERY SIGNAL!

New Challenges, New Tools



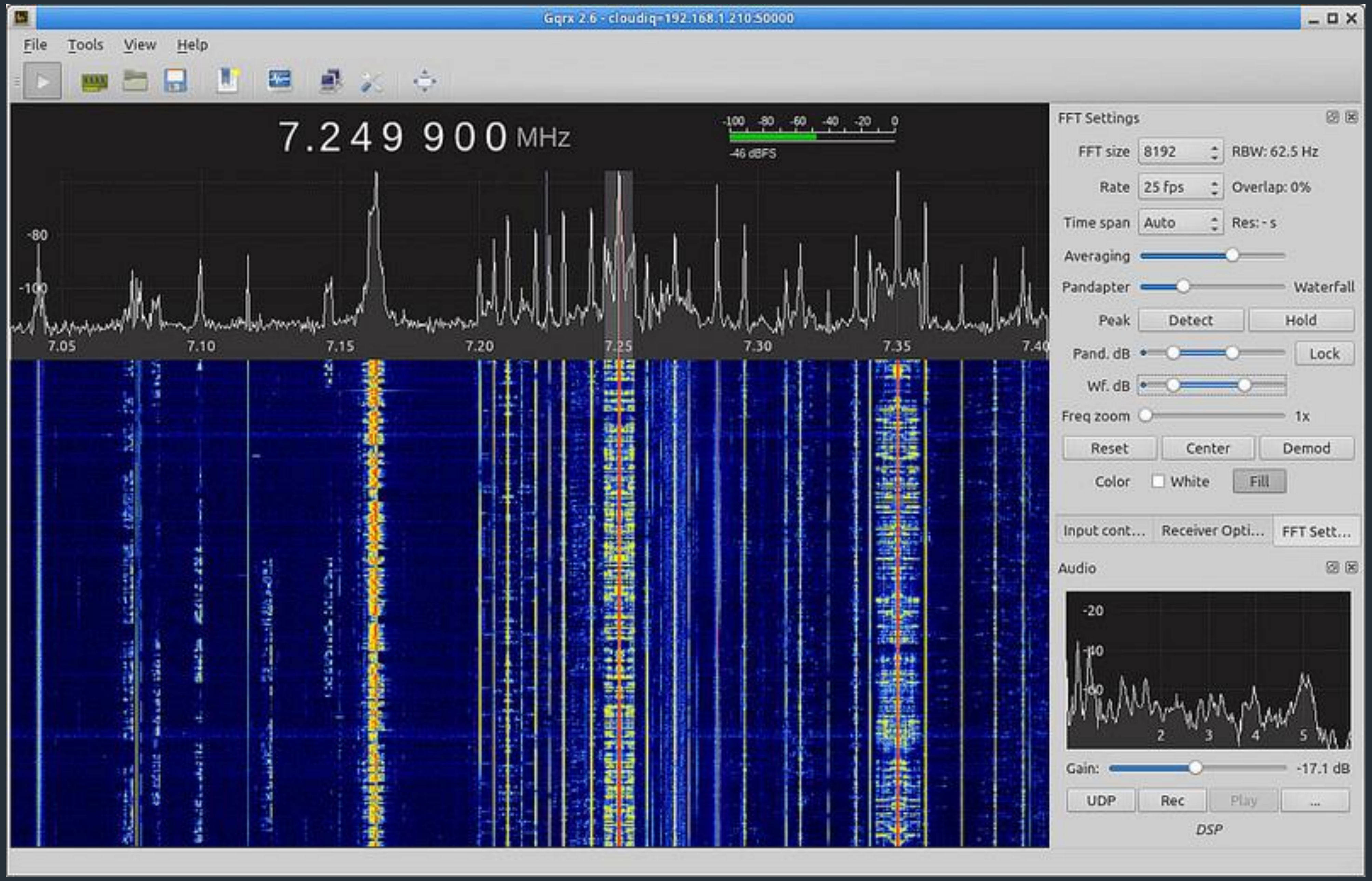
- RTL_433 won’t discover signals without a “nearby” frequency to look at
- GQRX is good for tuning, but has limited features and views
- GNU Radio Companion (GRC) can create software radio systems
- Simple, block-based design generates code using GNU Radio in Python

https://wiki.gnuradio.org/index.php/GNURadioCompanion

Signal Safari

MWR LABS

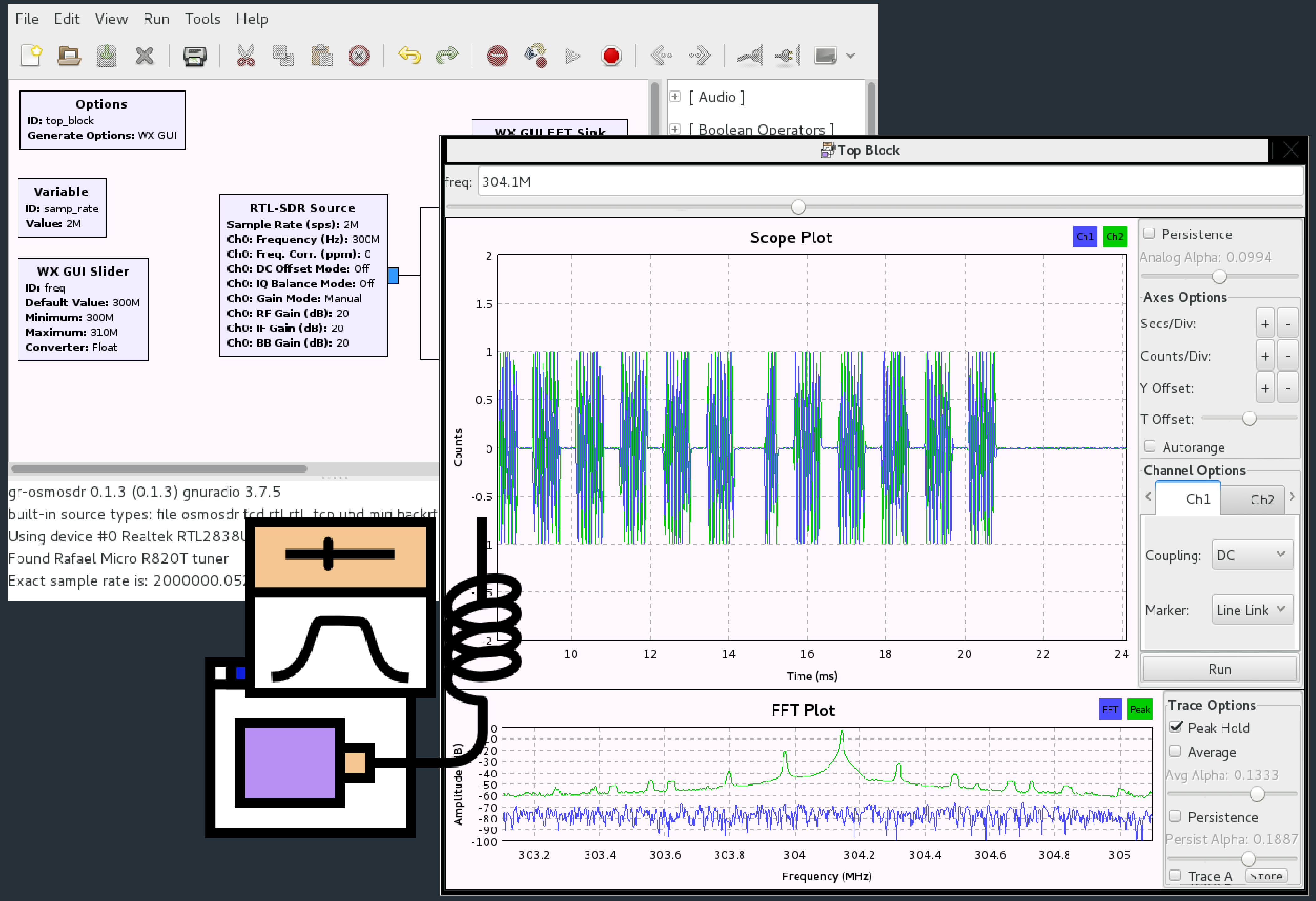
GQRX



FFT size: 8192 RBW: 62.5 Hz
Rate: 25 fps Overlap: 0%
Time span: Auto Res: - s
Gain: -17.1 dB

Tool that uses GNURadio

GRC



Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 2M

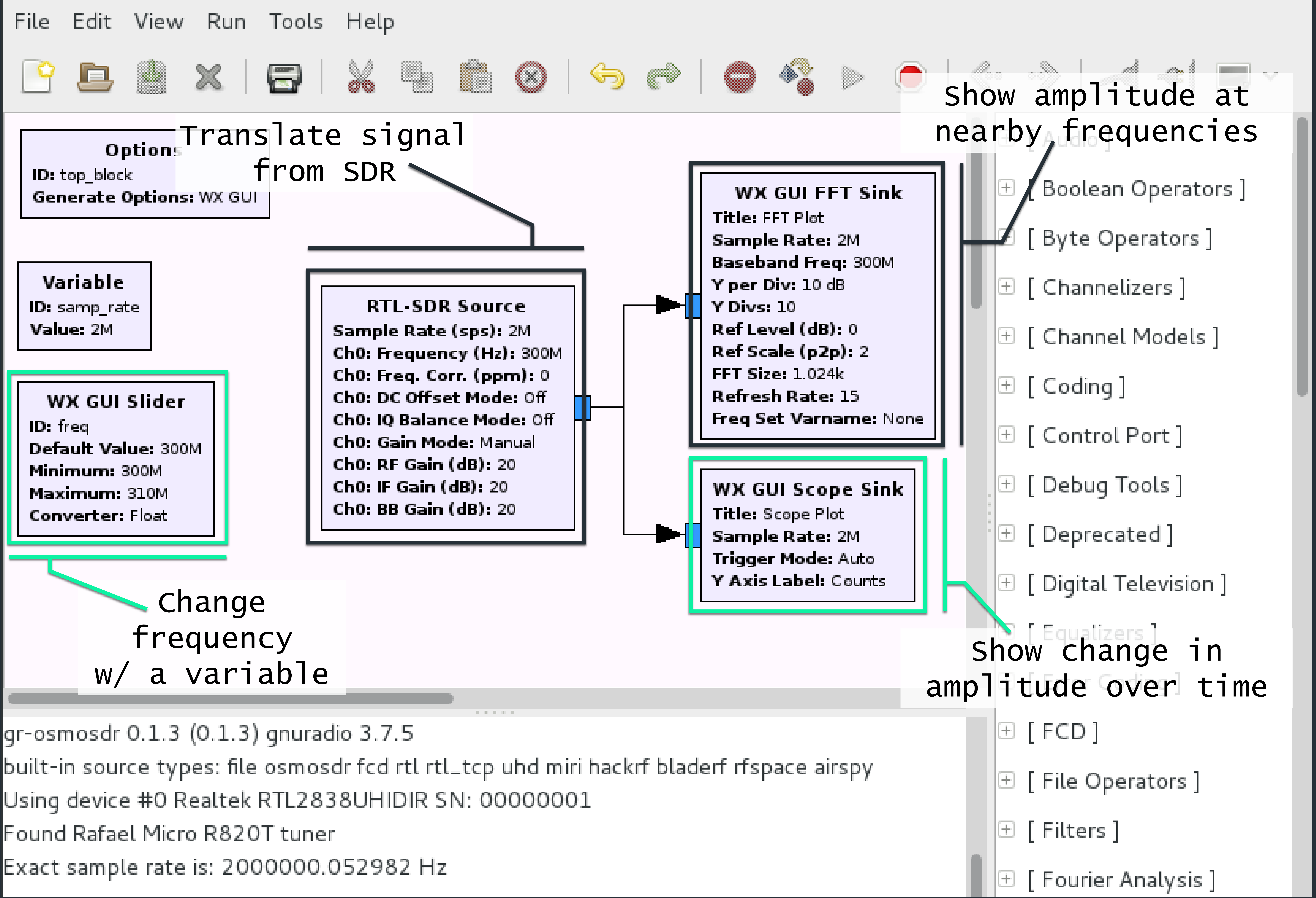
WX GUI Slider
ID: freq
Default Value: 300M
Minimum: 300M
Maximum: 310M
Converter: Float

RTL-SDR Source
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 300M
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

```
gr-osmosdr 0.1.3 (0.1.3) gnuradio 3.7.5
built-in source types: file osmosdr fcd rtl rtl_tcp uhd miri hackrf
Using device #0 Realtek RTL2838U
Found Rafael Micro R820T tuner
Exact sample rate is: 2000000.05
```

freq: 304.1M

Builds tools that use GNURadio



Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 2M

WX GUI Slider
ID: freq
Default Value: 300M
Minimum: 300M
Maximum: 310M
Converter: Float

RTL-SDR Source
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 300M
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

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 2M
Baseband Freq: 300M
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 2M
Trigger Mode: Auto
Y Axis Label: Counts

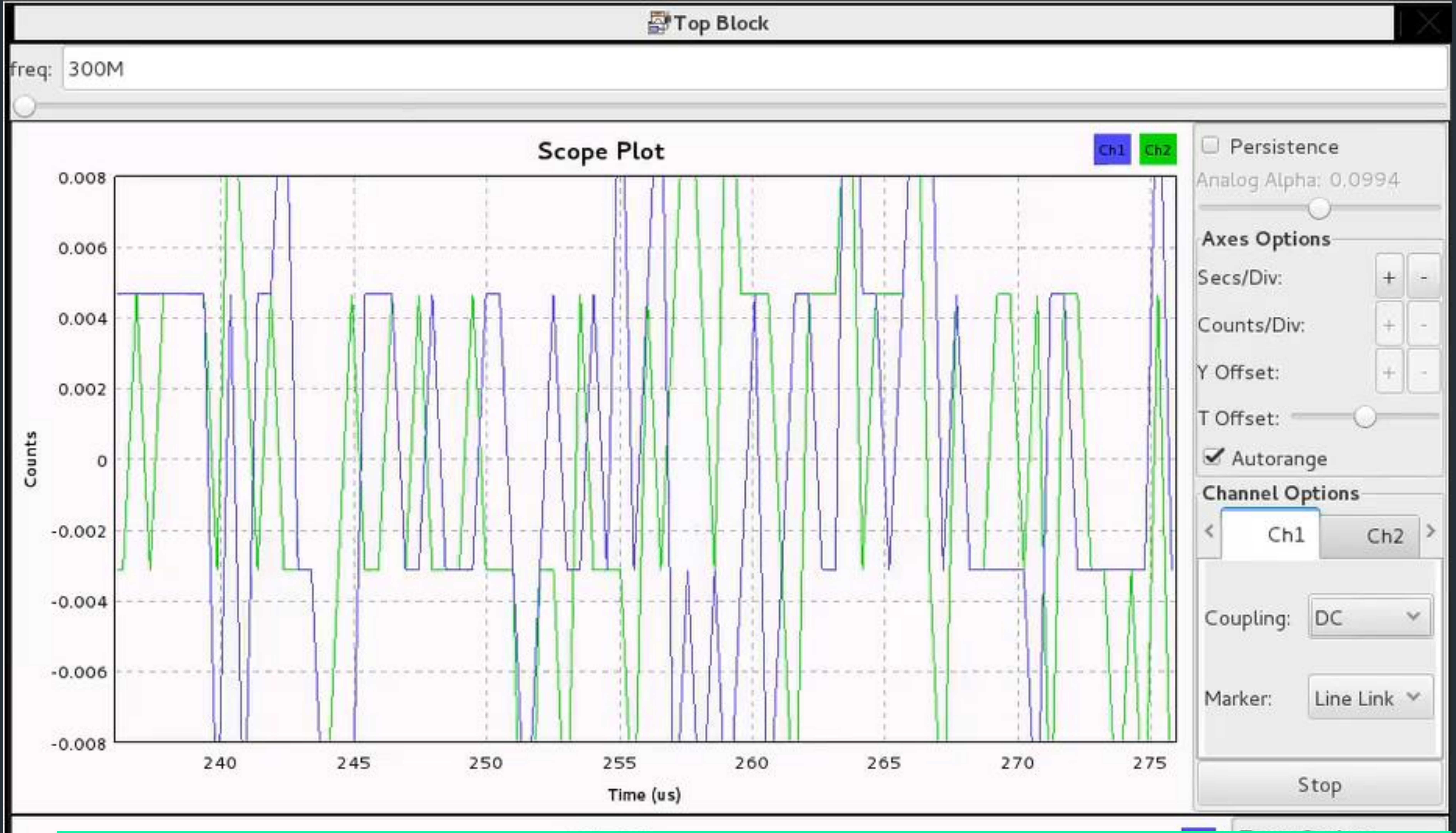
```
gr-osmosdr 0.1.3 (0.1.3) gnuradio 3.7.5
built-in source types: file osmosdr fcd rtl rtl_tcp uhd miri hackrf bladerf rfspace airspy
Using device #0 Realtek RTL2838UHIDIR SN: 00000001
Found Rafael Micro R820T tuner
Exact sample rate is: 2000000.052982 Hz
```

Translate signal from SDR

Show amplitude at nearby frequencies

Change frequency w/ a variable

Show change in amplitude over time



Top Block

freq: 300M

□ Persistence

Analog Alpha: 0.0994

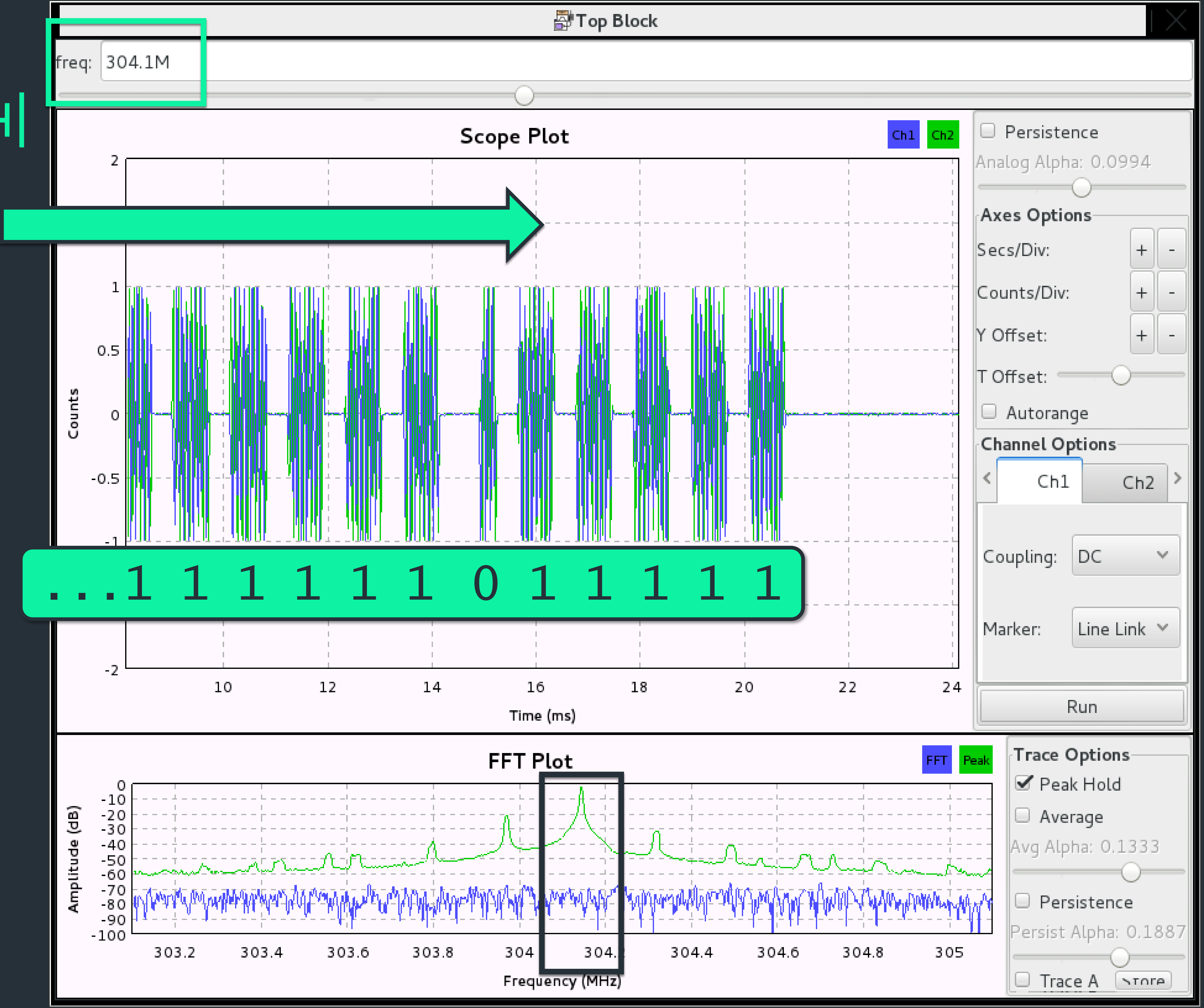
☑ Autorange

Coupling: DC

Marker: Line Link

GRC Demo:

https://www.youtube.com/embed/CMfnIXyjXJ0



freq: 304.1M

☐ Persistence

Analog Alpha: 0.0994

☐ Autorange

Coupling: DC

Marker: Line Link

☑ Peak Hold

☐ Average

Avg Alpha: 0.1333

☐ Persistence

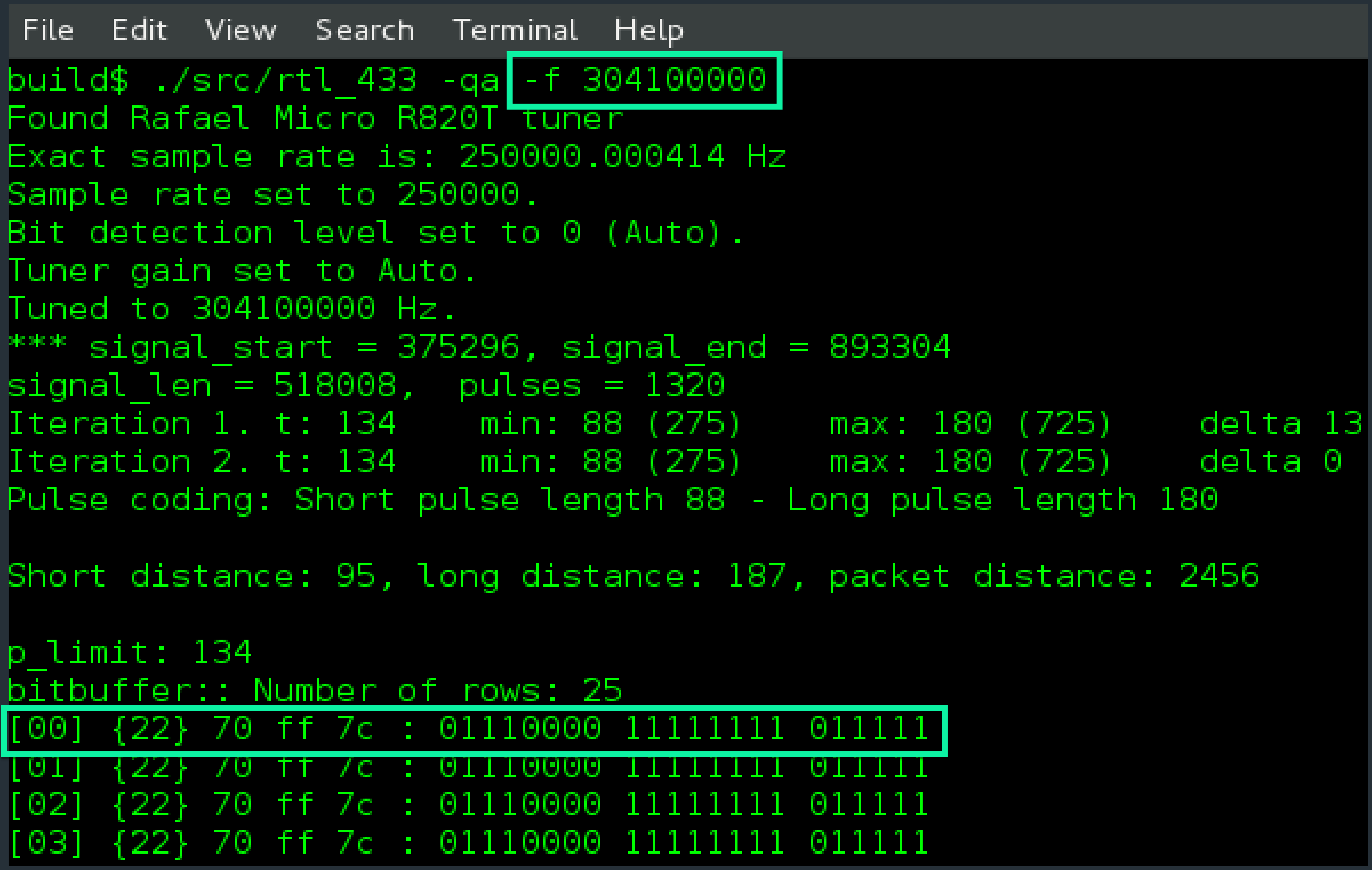
Persist Alpha: 0.1887

☐ Trace A

...1 1 1 1 1 1 0 1 1 1 1 1

- Slider for *freq* variable tunes from 300–310 MHz
- FFT sink plot shows highest signals near current center frequency
- GUI scope plot shows signal strength at center frequency over time

With *f* known, RTL_433 can handle the rest...



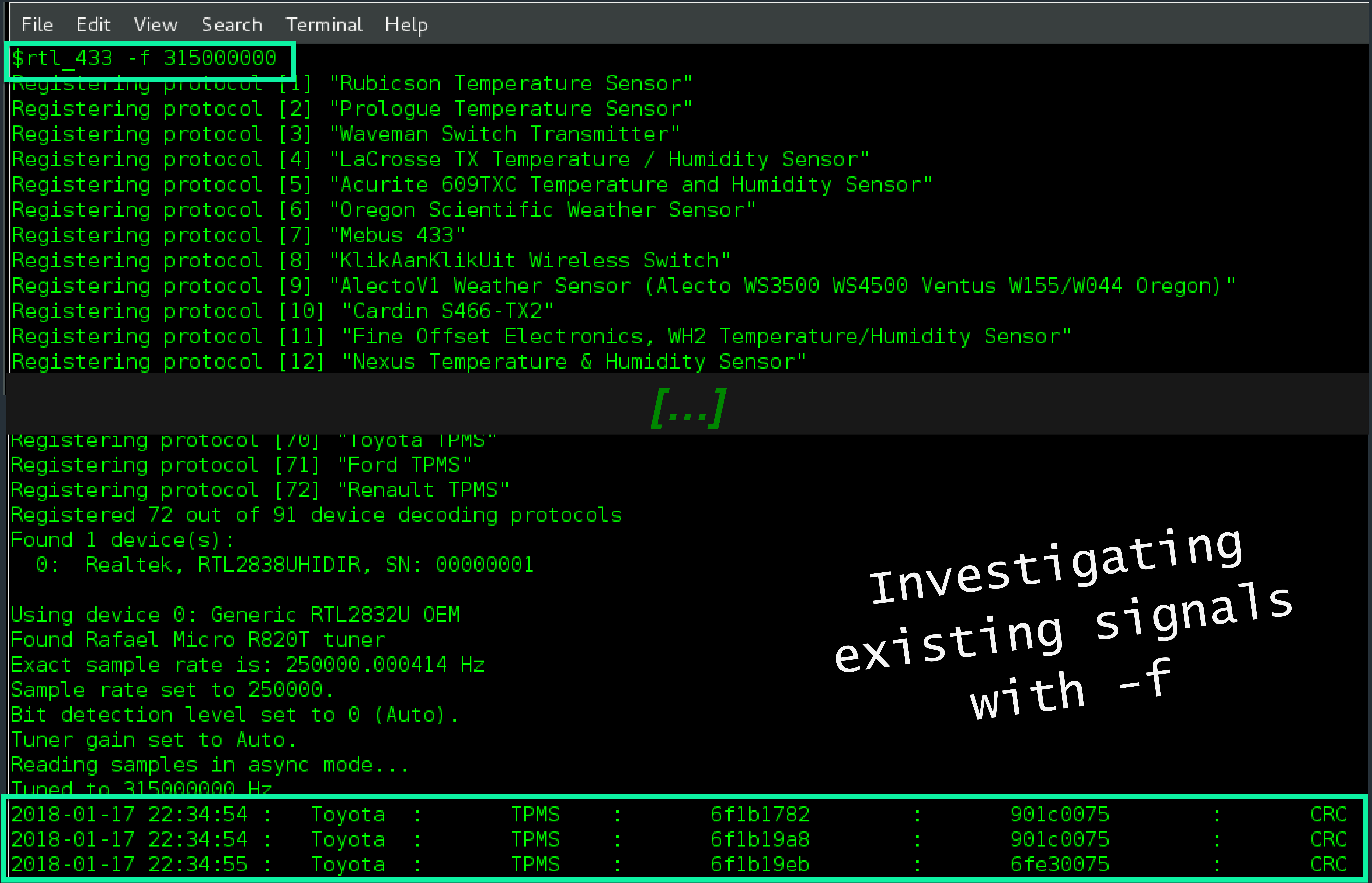
```
build$ ./src/rtl_433 -qa -f 304100000
Found Rafael Micro R820T tuner
Exact sample rate is: 250000.000414 Hz
Sample rate set to 250000.
Bit detection level set to 0 (Auto).
Tuner gain set to Auto.
Tuned to 304100000 Hz.
*** signal_start = 375296, signal_end = 893304
signal_len = 518008,  pulses = 1320
Iteration 1. t: 134    min: 88 (275)    max: 180 (725)    delta 13
Iteration 2. t: 134    min: 88 (275)    max: 180 (725)    delta 0
Pulse coding: Short pulse length 88 - Long pulse length 180

Short distance: 95, long distance: 187, packet distance: 2456

p_limit: 134
bitbuffer:: Number of rows: 25
[00] {22} 70 ff 7c : 01110000 11111111 011111
[01] {22} 70 ff 7c : 01110000 11111111 011111
[02] {22} 70 ff 7c : 01110000 11111111 011111
[03] {22} 70 ff 7c : 01110000 11111111 011111
```

MYSTERY SIGNAL!

File
Edit
View
Search
Terminal
Help

```
User cancel, exiting...
$rtl_433 -qa -f 315000000
Found Rafael Micro R820T tuner
Exact sample rate is: 250000.000414 Hz
Sample rate set to 250000.
Bit detection level set to 0 (Auto).
Tuner gain set to Auto.
Tuned to 315000000 Hz.
*** signal_start = 291725, signal_end = 405307
signal_len = 113582,  pulses = 582
Iteration 1. t: 116    min: 80 (540)    max: 153 (42)    delta 8
Iteration 2. t: 116    min: 80 (540)    max: 153 (42)    delta 0
Distance coding: Pulse length 116

Short distance: 66, long distance: 140, packet distance: 1928

p_limit: 116
bitbuffer:: Number of rows: 2
[00] {290} 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 88 40 22 10 05 4e 48 48 a2 00
[01] {290} 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 88 40 22 10 05 4e 48 48 a2 00
*** signal_start = 470452, signal_end = 584008
signal_len = 113556,  pulses = 580
Iteration 1. t: 116    min: 80 (536)    max: 153 (44)    delta 8
Iteration 2. t: 116    min: 80 (536)    max: 153 (44)    delta 0
Distance coding: Pulse length 116

Short distance: 66, long distance: 140, packet distance: 1903

p_limit: 116
bitbuffer:: Number of rows: 2
[00] {289} 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 88 40 04 42 24 aa 61 4a 44 00
[01] {289} 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 88 40 04 42 24 aa 61 4a 44 00
*** signal_start = 653918, signal_end = 767543
```

Receiving unlock code with known device *f*



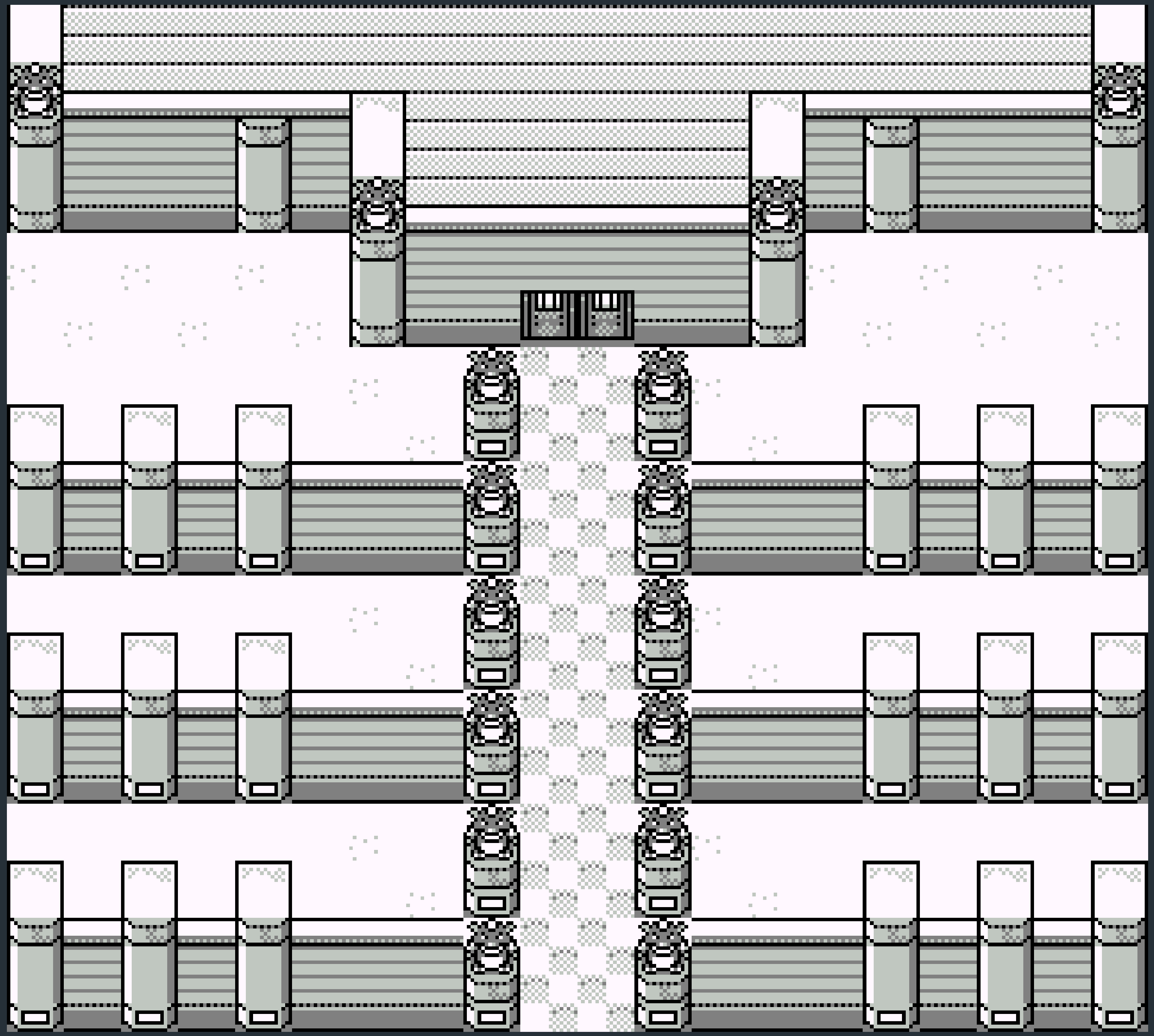
```
$rtl_433 -f 315000000
Registering protocol [1] "Rubicson Temperature Sensor"
Registering protocol [2] "Prologue Temperature Sensor"
Registering protocol [3] "Waveman Switch Transmitter"
Registering protocol [4] "LaCrosse TX Temperature / Humidity Sensor"
Registering protocol [5] "Acurite 609TXC Temperature and Humidity Sensor"
Registering protocol [6] "Oregon Scientific Weather Sensor"
Registering protocol [7] "Mebus 433"
Registering protocol [8] "KlikAanKlikUit Wireless Switch"
Registering protocol [9] "AlectoV1 Weather Sensor (Alecto WS3500 WS4500 Ventus W155/W044 Oregon)"
Registering protocol [10] "Cardin S466-TX2"
Registering protocol [11] "Fine Offset Electronics, WH2 Temperature/Humidity Sensor"
Registering protocol [12] "Nexus Temperature & Humidity Sensor"
```

[...]

```
Registering protocol [70] "Toyota TPMS"
Registering protocol [71] "Ford TPMS"
Registering protocol [72] "Renault TPMS"
Registered 72 out of 91 device decoding protocols
Found 1 device(s):
  0:  Realtek, RTL2838UHIDIR, SN: 00000001

Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
Exact sample rate is: 250000.000414 Hz
Sample rate set to 250000.
Bit detection level set to 0 (Auto).
Tuner gain set to Auto.
Reading samples in async mode...
Tuned to 315000000 Hz
2018-01-17 22:34:54 :   Toyota  :       TPMS    :       6f1b1782        :       901c0075        :       CRC
2018-01-17 22:34:54 :   Toyota  :       TPMS    :       6f1b19a8        :       901c0075        :       CRC
2018-01-17 22:34:55 :   Toyota  :       TPMS    :       6f1b19eb        :       6fe30075        :       CRC
```

Investigating existing signals with -f

RF Signal Security



- Securing RF systems can be tricky
- Hardware design, limited resources make improvements difficult
- Things are (slowly) improving
- Each niche in security offers its own unique challenges. Don’t be afraid to explore!

More Curiosity => More Solutions

Continue Your Safari:

Flavio D. Garcia:

USENIX Security ’16,
“Lock It and Still Lose It: On the (In)Security of Automotive Remote Keyless Entry Systems”

Samy Kamkar:

DC 23,“Drive It Like You Hacked It”

Digital Ding Dong Ditch
https://github.com/samyk/dingdong

Michael Ossman:

Software Defined Radio with HackRF
https://greatscottgadgets.com/sdr/

FCC ID Search:
https://www.fcc.gov/oet/ea/fccid

Browse new registrations:
https://fccid.io/#fccid-today

ARRL, Amateur Radio:
https://www.arrl.org/

Questions?

Reach out at:

🐦 @_sigil

✉ Katie.Knowles@mwrinfosecurity.com