What’s on the Wireless?

Automating RF Signal Identification

Dominic Spill
Michael Ossmann

Black Hat USA 2017

Dominic Spill

Senior Security Researcher at Great Scott Gadgets

Open source software developer

- HackRF
- GreatFET
- Ubertooth

@dominicgs

Michael Ossmann

Founder of Great Scott Gadgets

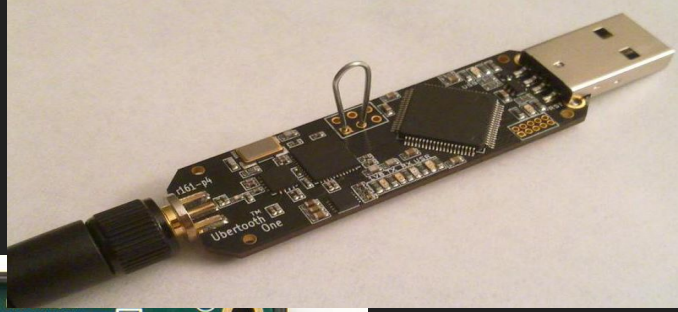
Open source hardware developer

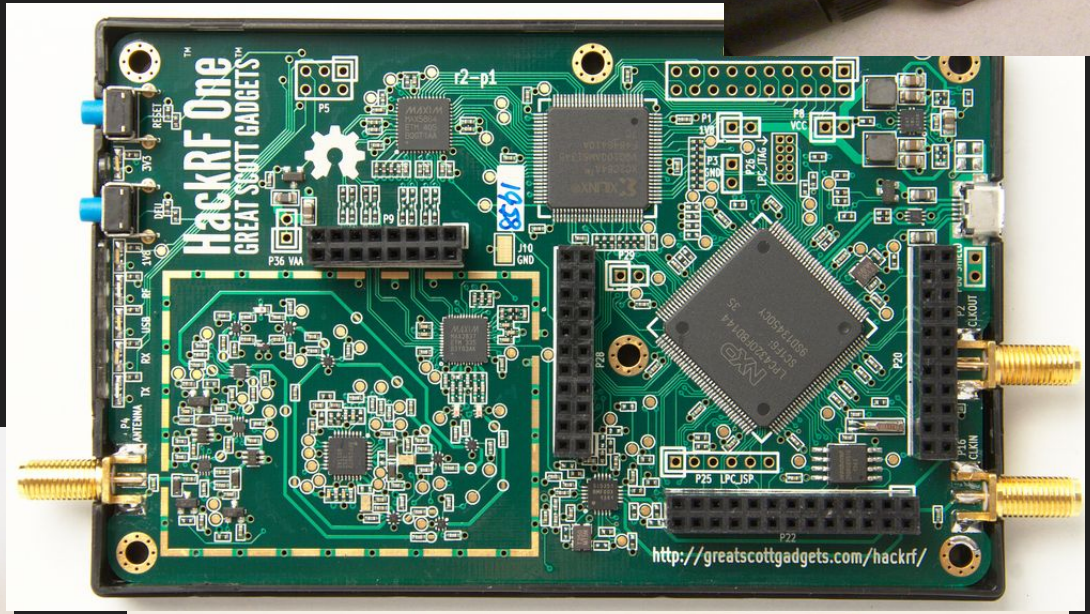
- HackRF
- GreatFET
- Ubertooth

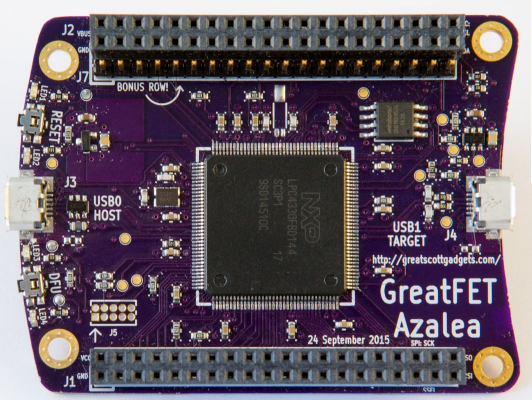
@michaelossmann

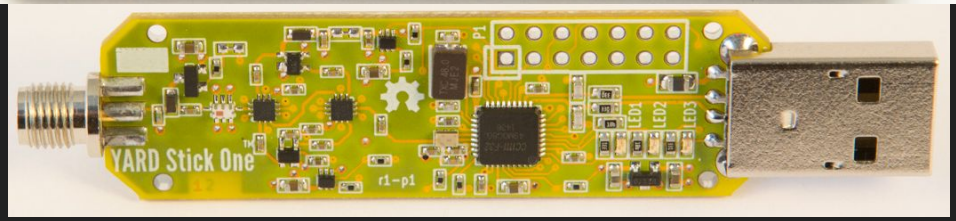
Great Scott Gadgets

- HackRF One
- Ubertooth
- YARD Stick One
- GreatFET









For sale on Amazon, hacking gadget that is a car thief's dream

By **Ben Ellery** and **Simon Murphy**

A GADGET that allows thieves to break into cars with electronic locks in minutes is being openly sold on Amazon and eBay.

Priced at £257, the device lets criminals intercept the radio signal from the key as a car owner unlocks the vehicle. It is downloaded to a laptop and the thieves then transmit the stolen signal to break in when the owner leaves it unattended.

Called 'HackRF One' the radio device works from up to 30ft away, allowing the crook to remain hidden. YouTube videos demonstrating how to use the gadget to break into a car have been watched tens of thousands of times online.

After watching the videos, The Mail on Sunday was able to use the HackRF One to break into a top-of-the-range £105,000 Range Rover Vogue SE in two minutes – with the permission of the vehicle's owner.

'This problem is only going to get worse'

Experts have responded to our investigation by calling for the Home Office to launch a probe into the availability of the HackRF One and similar devices.

Made by Great Scott Gadgets, the HackRF One is marketed for 'development of modern and next generation radio technologies'. The box displays the disclaimer: 'You are responsible for using your HackRF One legally'.

However, Andrew Miller, chief technical officer at the motor insurers' centre Thatcham Research, the availability of these items.' Car manufacturers have introduced encryption on key fobs in an attempt to overcome 'signal grabbing' but the HackRF One features

... and MoS team using it took just two minutes to break into this £100k Range Rover

OPEN SESAME: The HackRF One captures key's signal and downloads it to a laptop. We used a volunteer's car

month thieves were caught on camera using a laptop to break into a £35,000 Mercedes and driving off.

A Land Rover spokesman said: 'Jaguar Land Rover is concerned

these criminal gangs, who are continually attempting to devise new ways of hacking into vehicles.'

EBay rules state it does not sell illegal items but using one of these

of uses. We have not been advised of any restrictions on its sale.' Amazon declined to comment.

Founder of Great Scott Gadgets Michael Ossmann said: 'We encourage auto makers and automobile owners to use test equipment such as HackRF One to

© PHILIP IDE

Explanation of terms

Software Defined Radio (SDR) -

Digital Signal Processing of radio signals

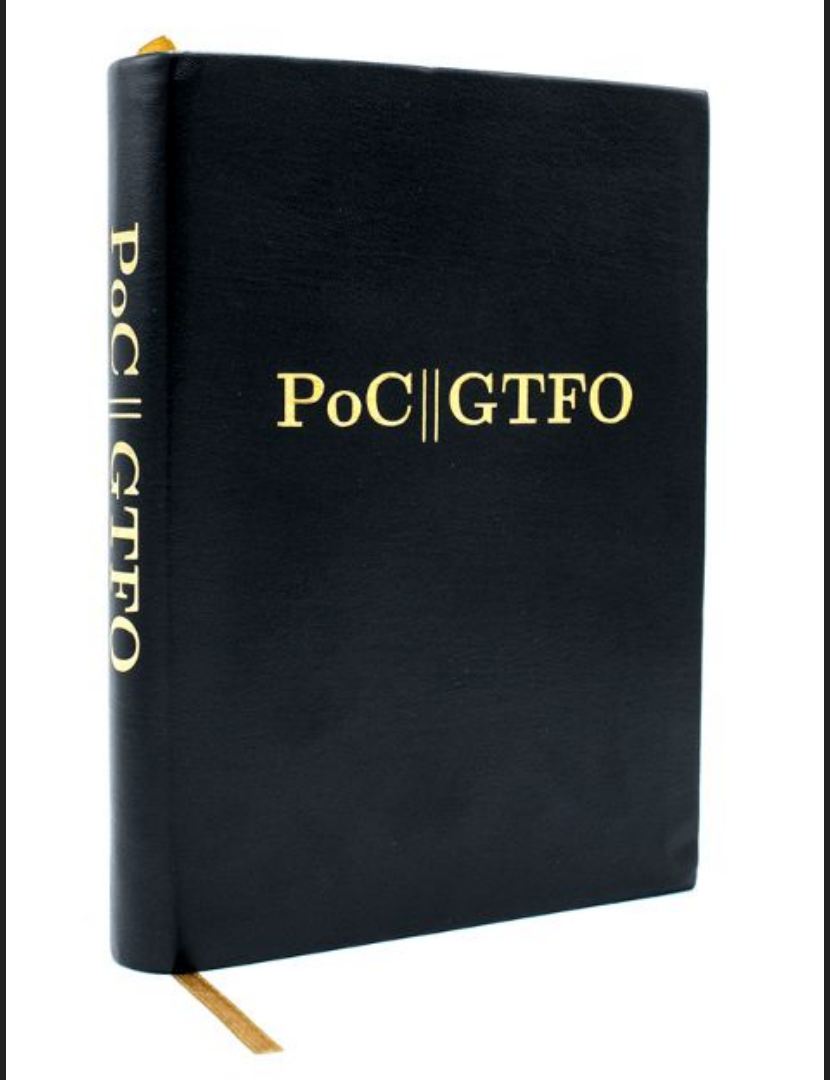
Waterfall - moving spectrogram showing power vs. frequency vs. time

Signal Analysis - Extracting metadata about a given radio signal

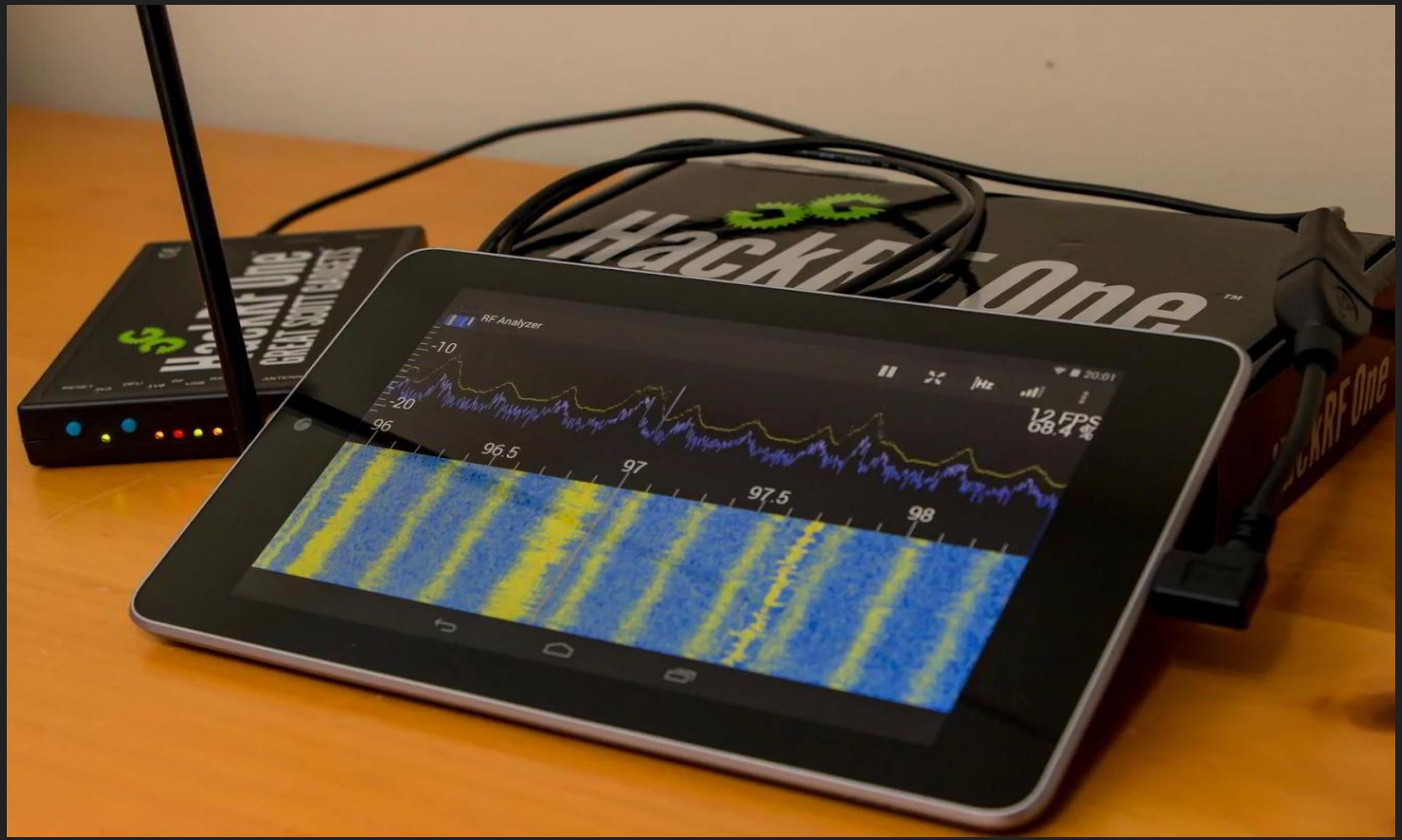
frequency, modulation, bandwidth, duty cycle

Signal Identification - Determining protocol in use by signal analysis

AMC - Automatic Modulation Classification


PoC||GTFO
PoC||GTFO

Waterfall Plots



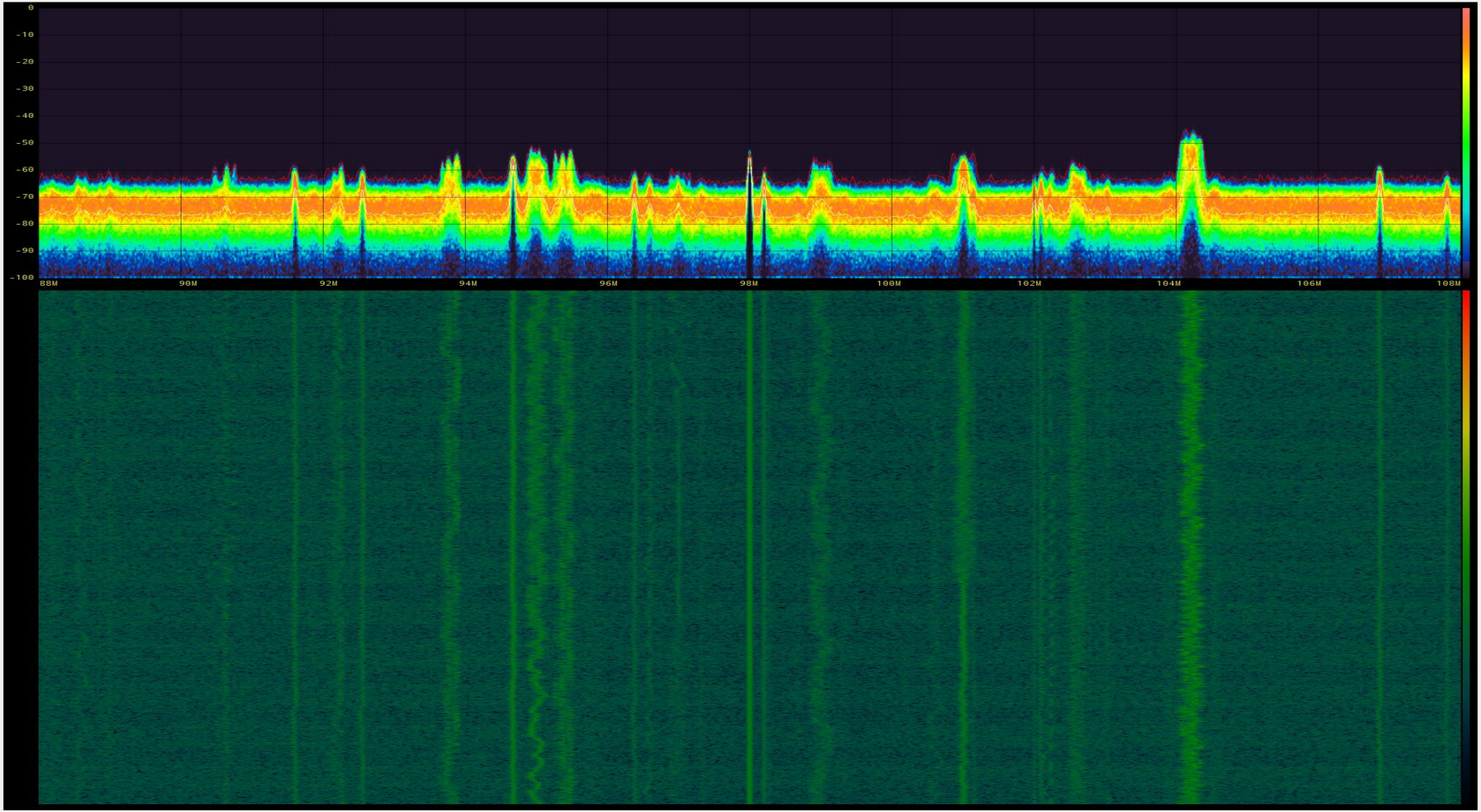
Waterfall Drawbacks

Missing transient events

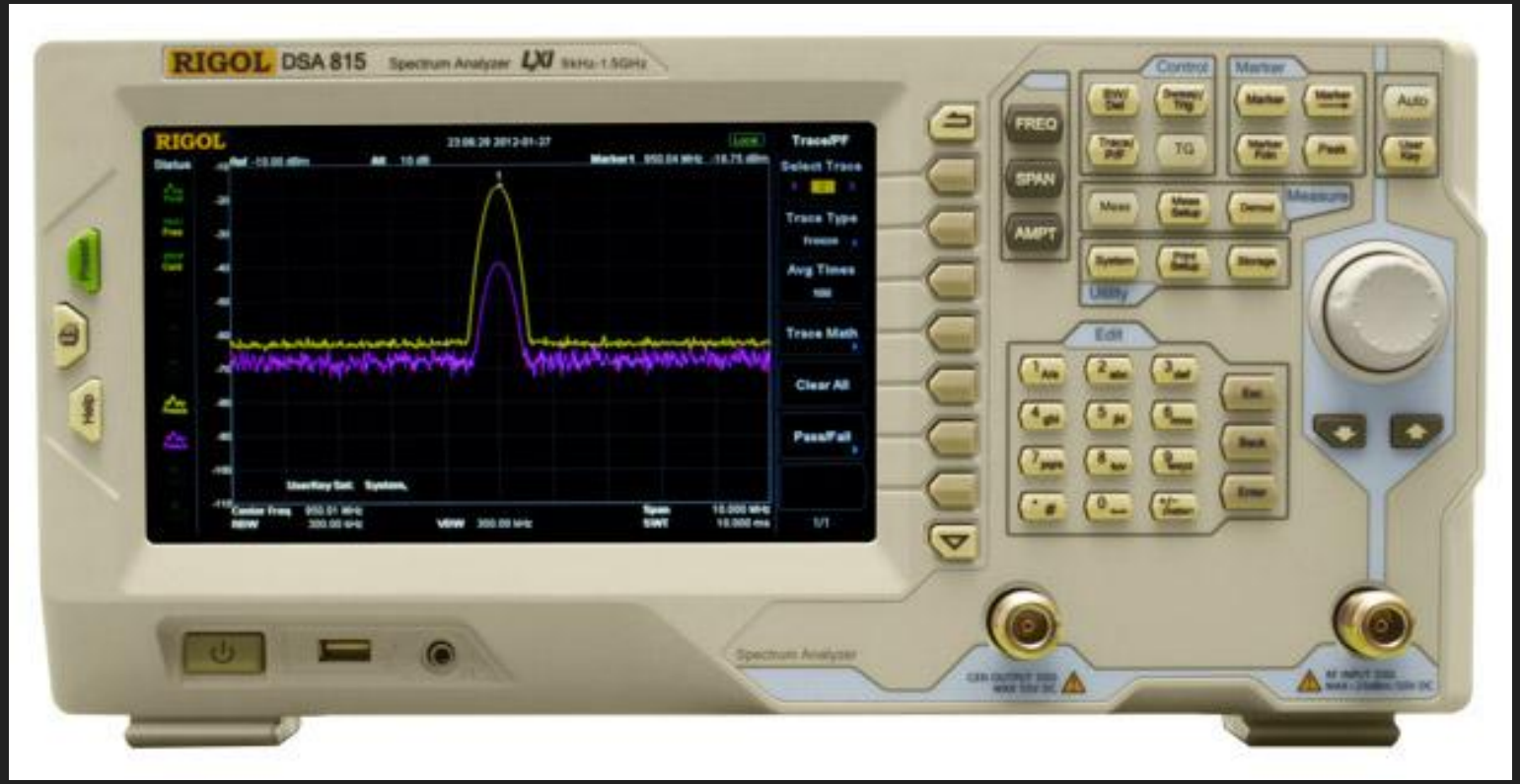
Limited time displayed

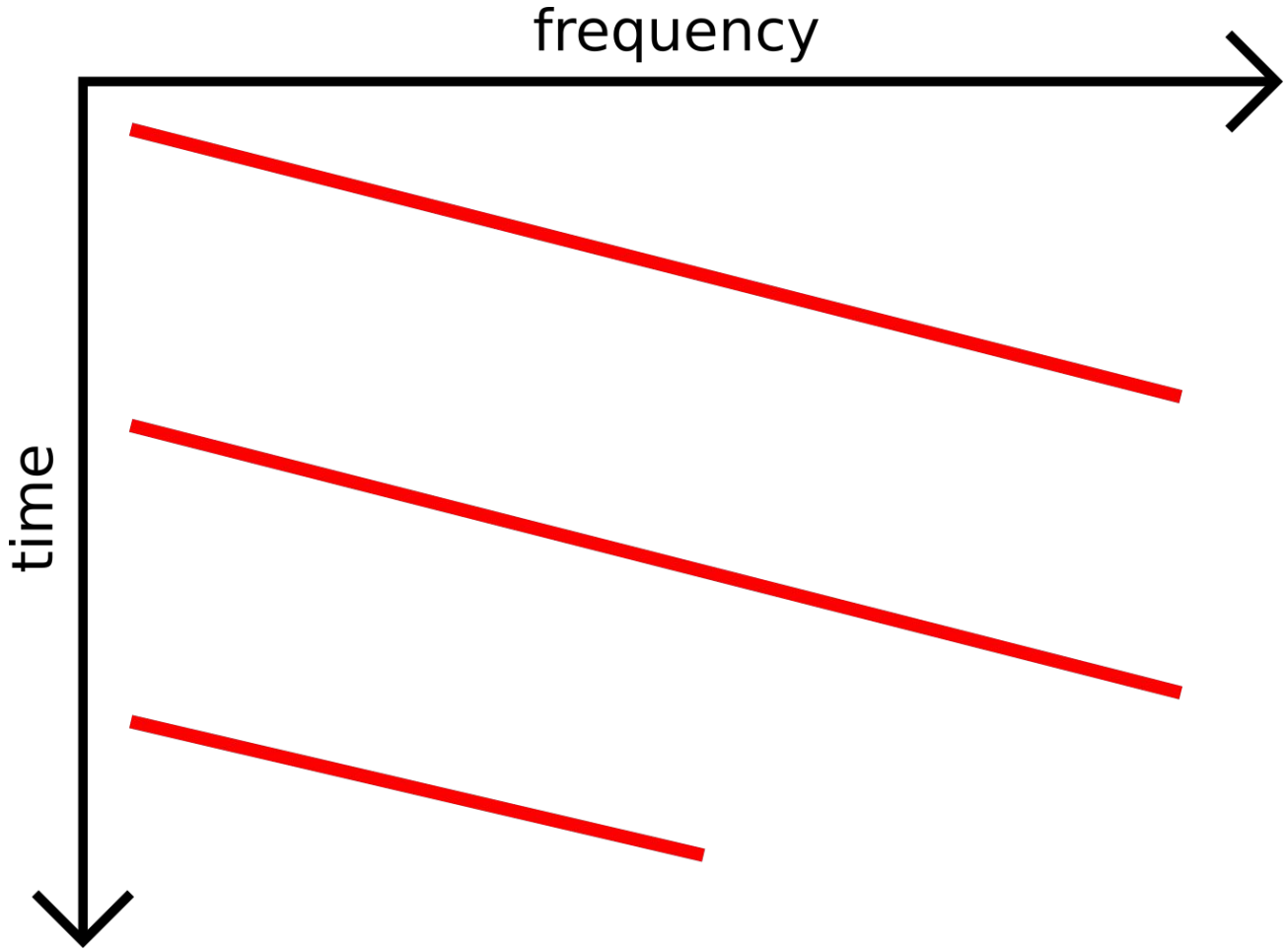
Limited bandwidth displayed

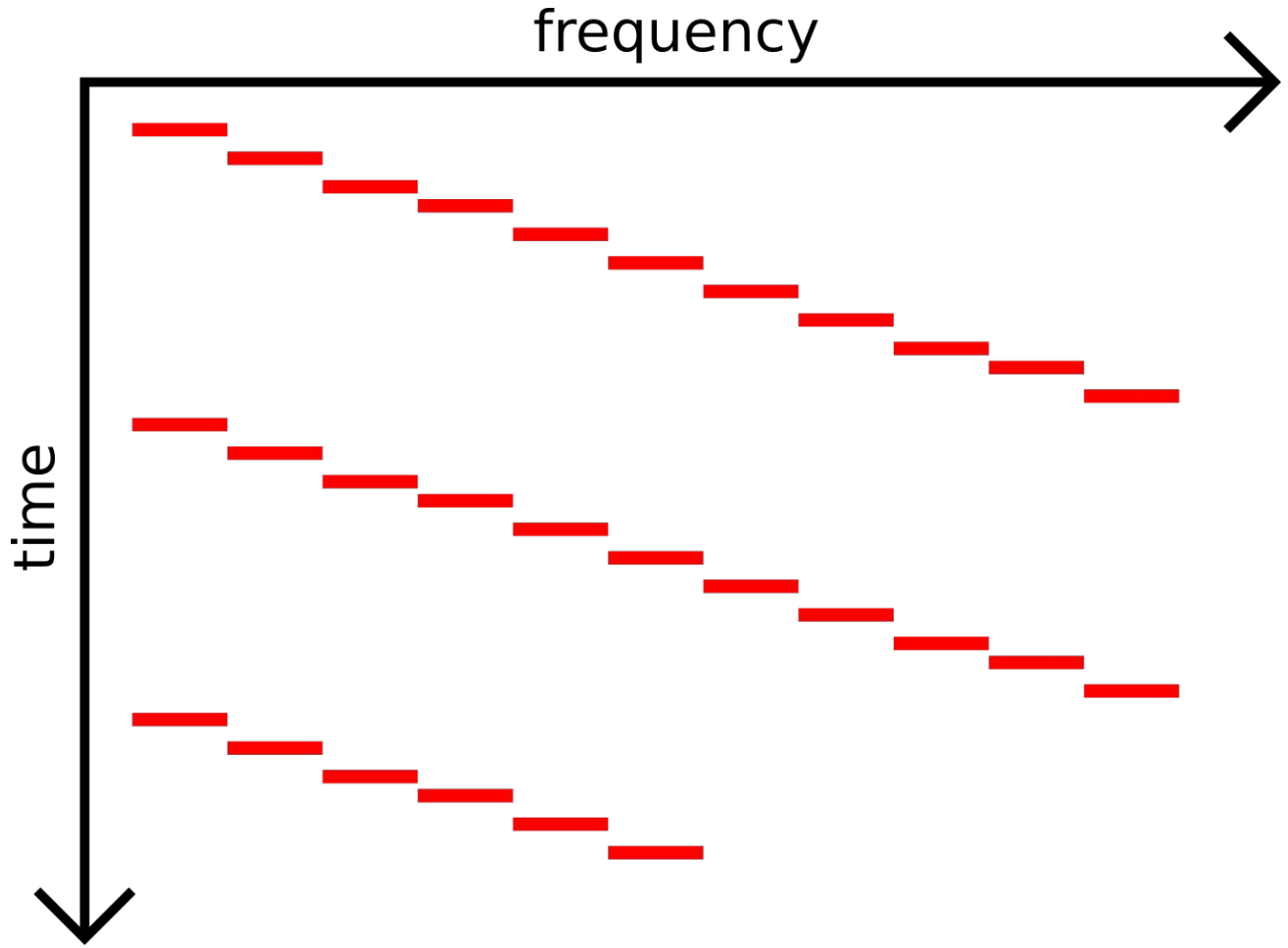
Top Block


0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
88M
90M
92M
94M
96M
98M
100M
102M
104M
106M
108M

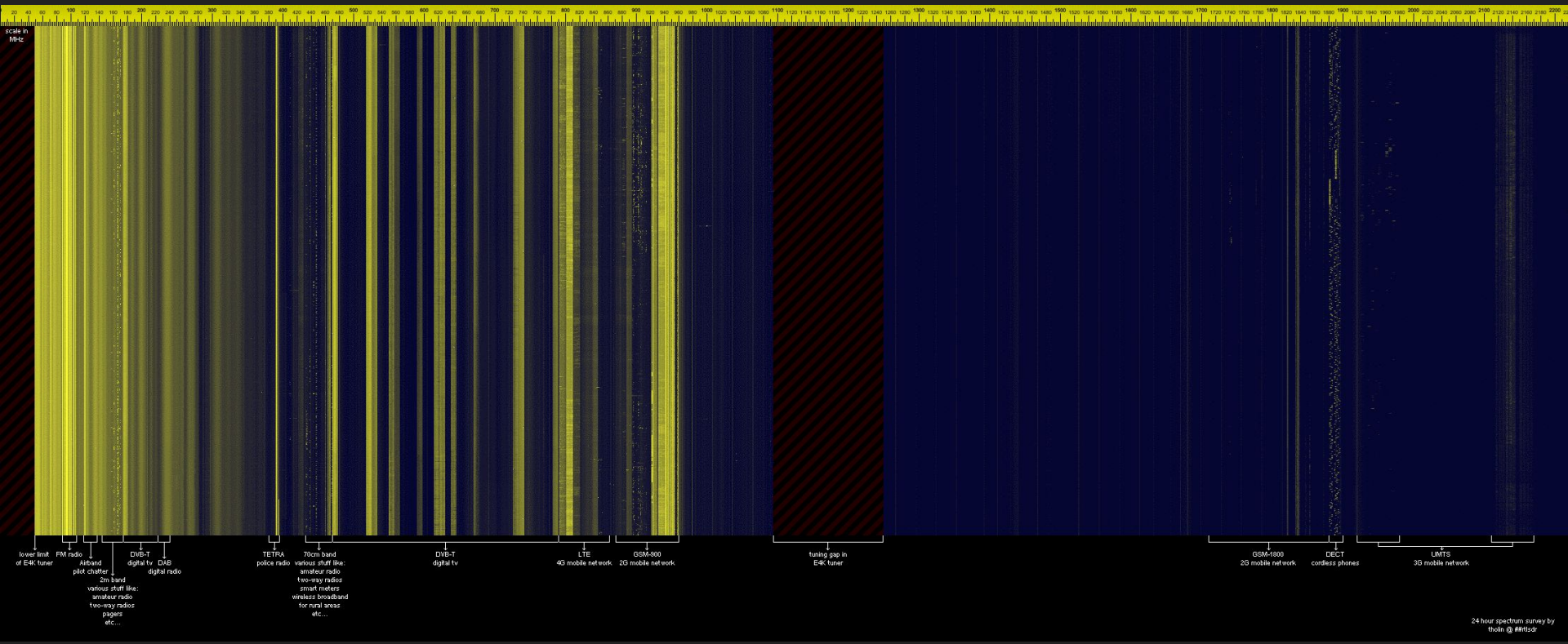
Spectrum Analyzer

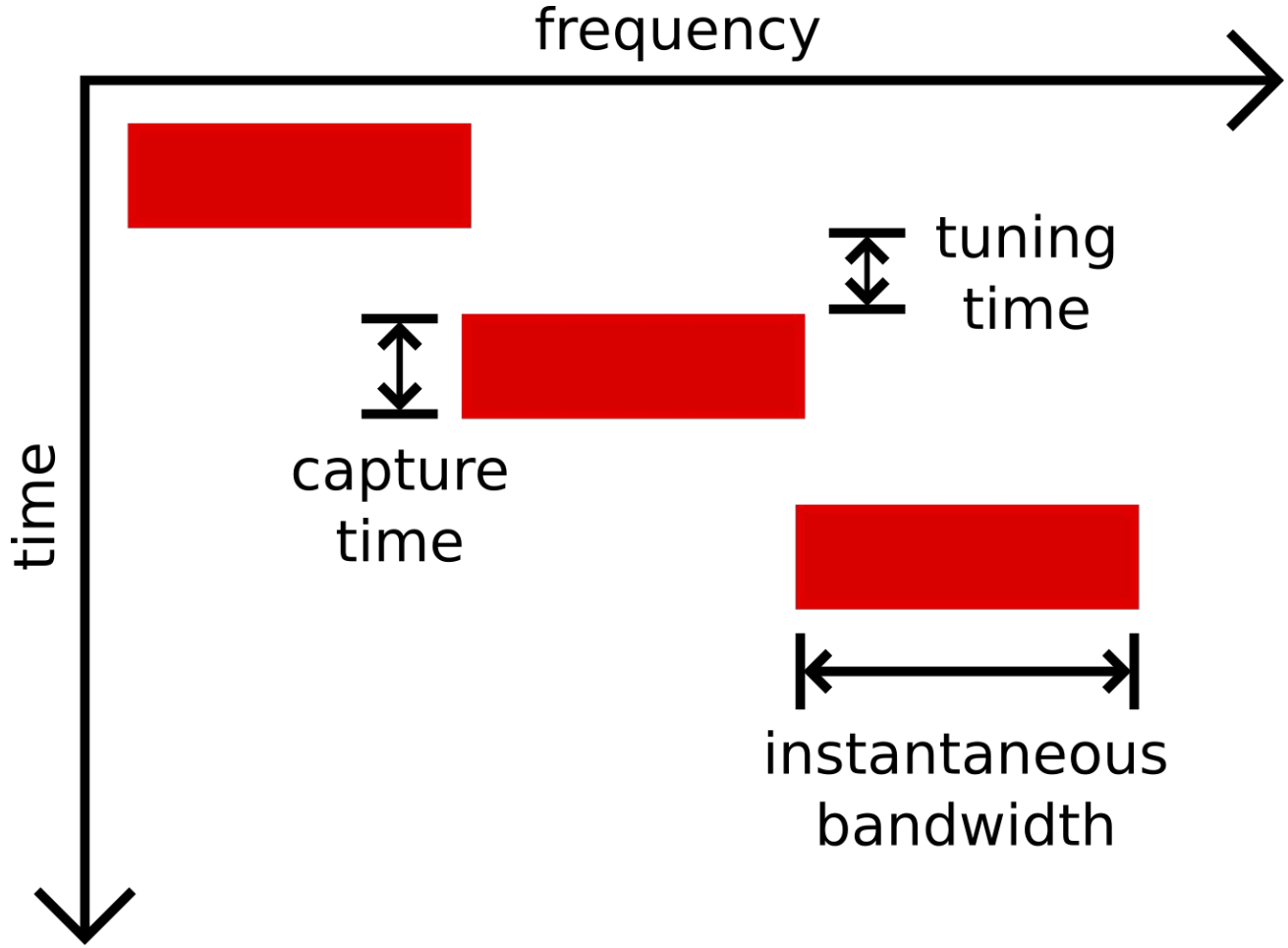



frequency
time

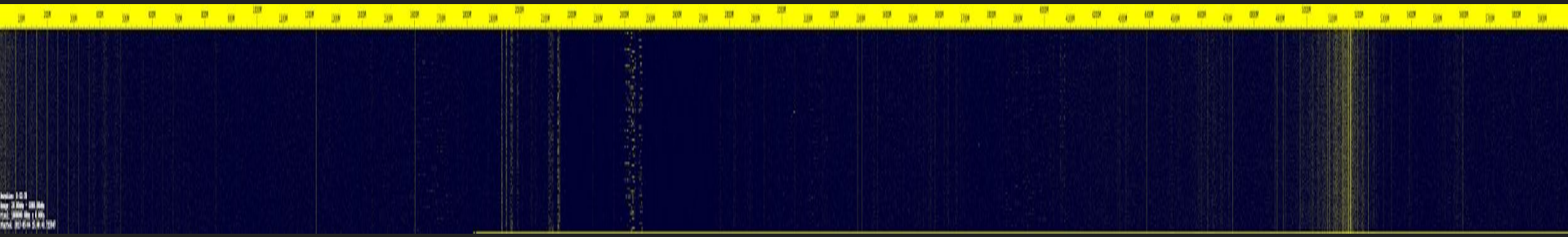

frequency
time

rtl_power + heatmap.py




frequency
time
tuning
time
capture
time
instantaneous
bandwidth

hackrf_sweep + heatmap.py

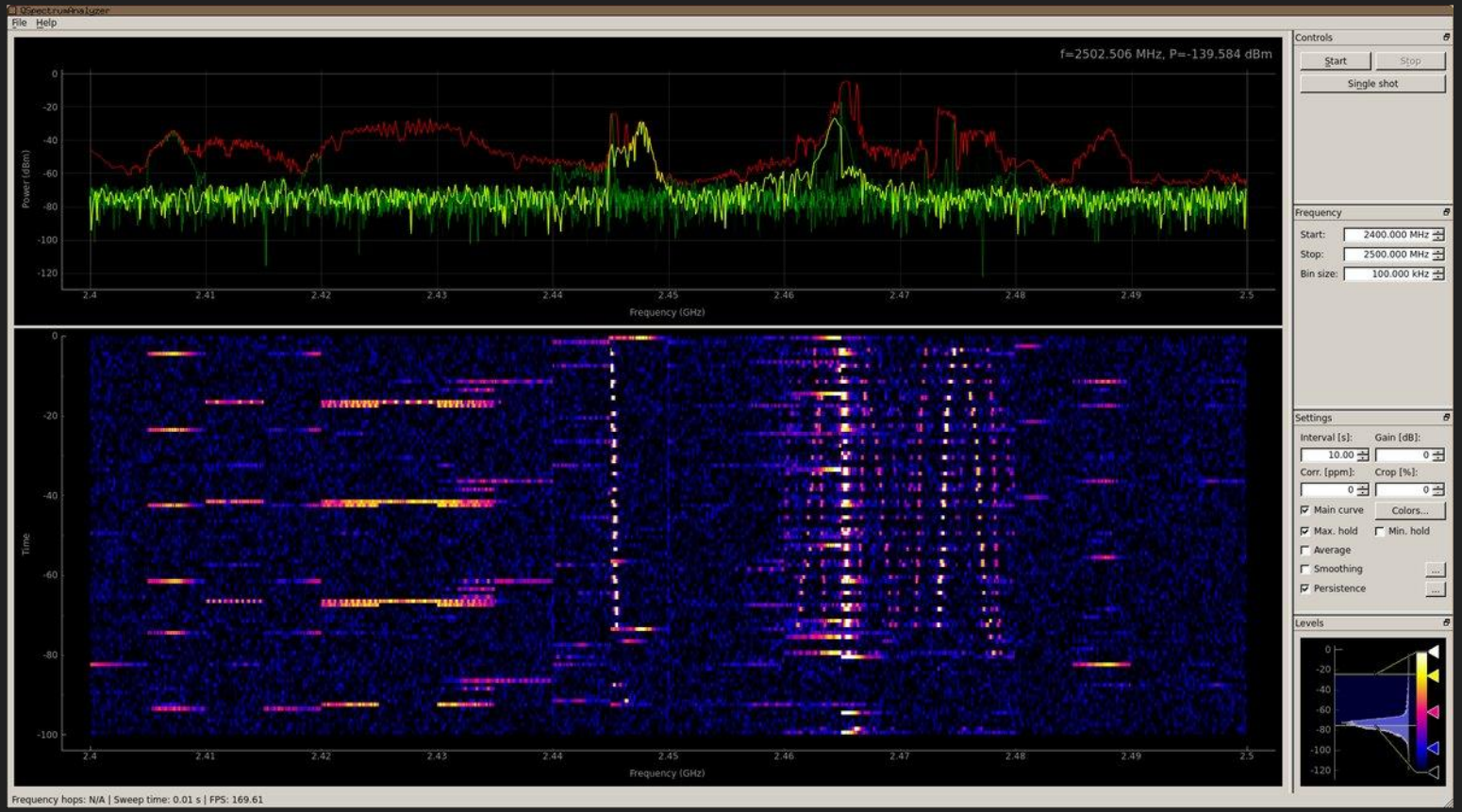


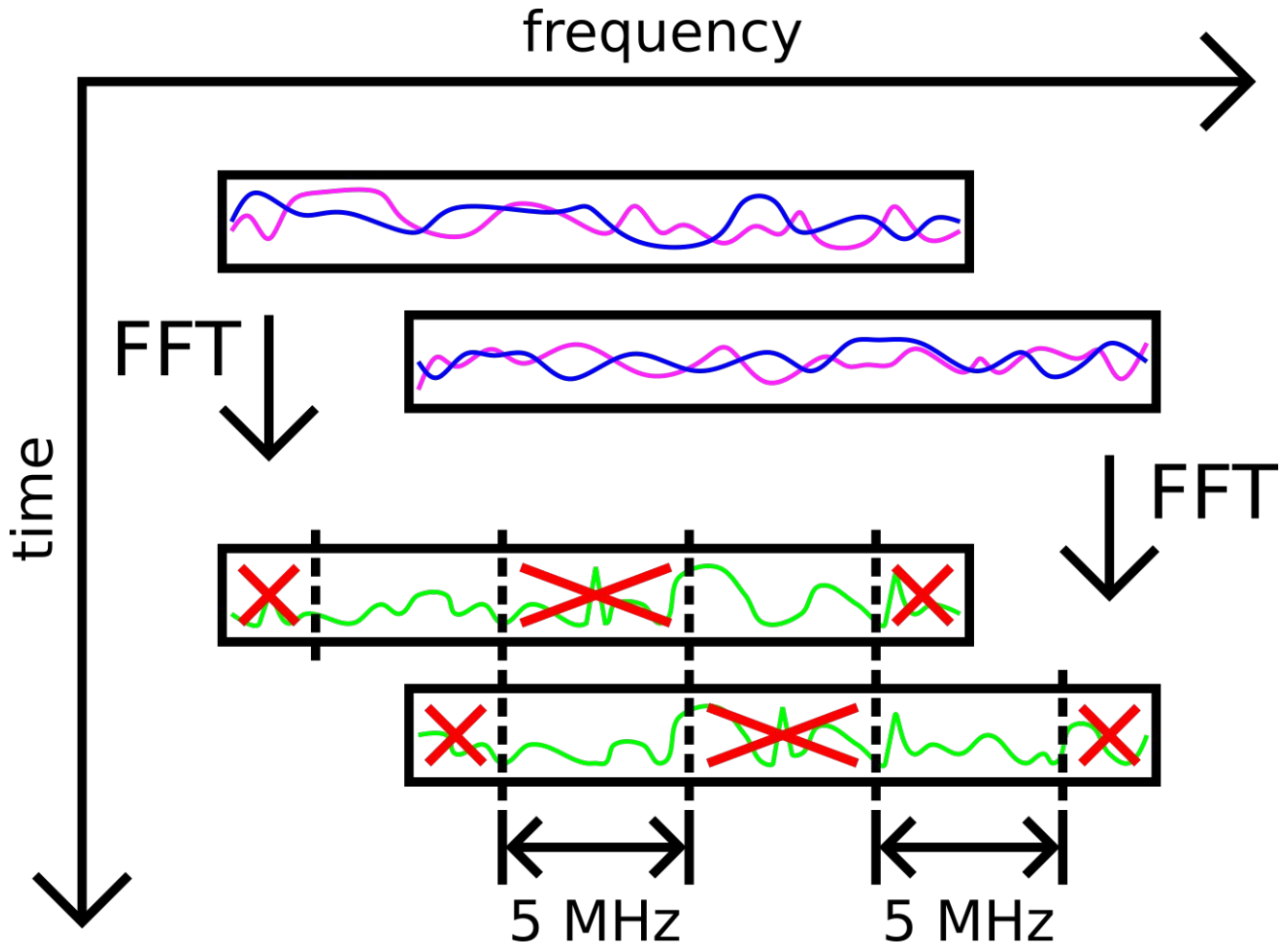
Real time visualization demo

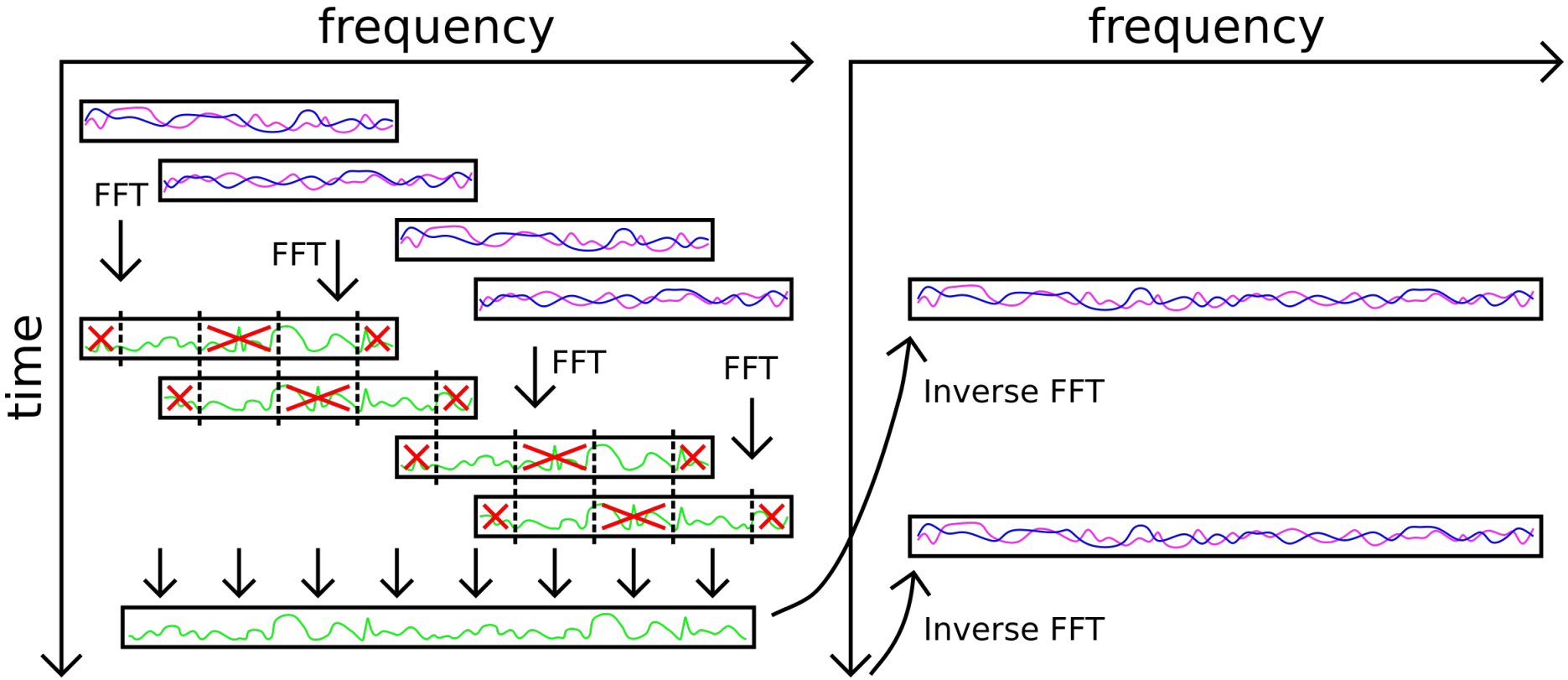
QSpectrumAnalyzer

github.com/xmikos/qspectrumanalyzer

QSpectrumAnalyzer




frequency
time
FFT
FFT
5 MHz
5 MHz


frequency
time
FFT
FFT
FFT
FFT
frequency
Inverse FFT
Inverse FFT

gr-fosphor + hackrf_sweep demo

ShinySDR

Web based tool by Kevin Reid

Waterfall plot, demodulators, band tagging

Can be extended

ShinySDR - Chromium

ShinySDR | GrOsmoSDR - SDR

localhost:8100/public/

ShinySDR

- RF Spectrum
- Audio Spectrum
- Map
- Telemetry
- Radio Config
- Frequency DB
- ShinySDR Manual
- Debug: flow graph
- ▶ *audio stream*

Theme: Gray

RF Spectrum Rate 488.28 Hz Resolution 4096 Pause

a
2.45 GHz
AM

▶ Options

Fixed, Mobile, Radiolocat... | Amateur | ISM: Worldwide | Radiolocation | Fixed, Mobile

2.38G 2.39G 2.4G 2.41G 2.42G 2.43G 2.44G 2.45G 2.46G 2.47G

Radio Config

RF source

OsmoSDR file=/tmp/2400.cfile,rate=100000000,f

Manual Gain | Stages

0.00 dB

▼ *more*

Freq.corr. 0 ppm

Use IQ balancer

Receiver a

Frequency | Follow device

2,450,000,000

AM | AM unselective | CW | Narrow FM | Broadcast FM | LSB | USB | Raw I/Q | VOR

RF -93.07

Squelch -100.00

AM demodulation Asynchronous

Audio -24.41

Vol -6.00

Dest Client L R

+ Save to database

Frequency DB

Type Channel

Freq

Mode —

Location

Label

Filter channels...

0.01	*Radionavigation*
0.01	*Radionavigation*
0.01	*Fixed, Maritime Mobile*
0.02	*Fixed, Maritime Mobile*
0.02	*Fixed, Maritime Mobile*
0.06	*Fixed, Maritime Mobile*
0.06	WWVB
0.06	*Fixed, Maritime Mobile, Radiolocation*
0.09	*Fixed, Maritime Mobile, Radiolocation*
0.09	*Radionavigation*
0.11	*Radionavigation*
0.11	*Fixed, Maritime Mobile, Radiolocation*
0.19	*Fixed, Maritime Mobile, Radiolocation*
0.19 AM	*Aeronautical Radionavigation (Non-directional beacons)*
0.41	*Maritime Mobile*
0.43 AM	*Aeronautical Radionavigation (Non-directional beacons)*
0.50	*Mobile (Distress and Calling)*
0.51 AM	*Aeronautical Radionavigation (Non-directional beacons)*
0.53	*Maritime Mobile*
0.53 AM	*Aeronautical Radionavigation (Non-directional beacons)*
0.53 AM	Traveler's Information
0.53 AM	*AM broadcast*
1.61 AM	Traveler's Information
1.71 AM	*AM broadcast*
1.71	*Fixed, Mobile, Radiolocation*
1.80	*Fixed, Mobile, Radiolocation*
1.80	*160-meter amateur*
1.90	*Radiolocation*
2.00	*160-meter amateur*
2.00	*Radiolocation*
2.00	*Fixed, Mobile, Maritime Mobile,*

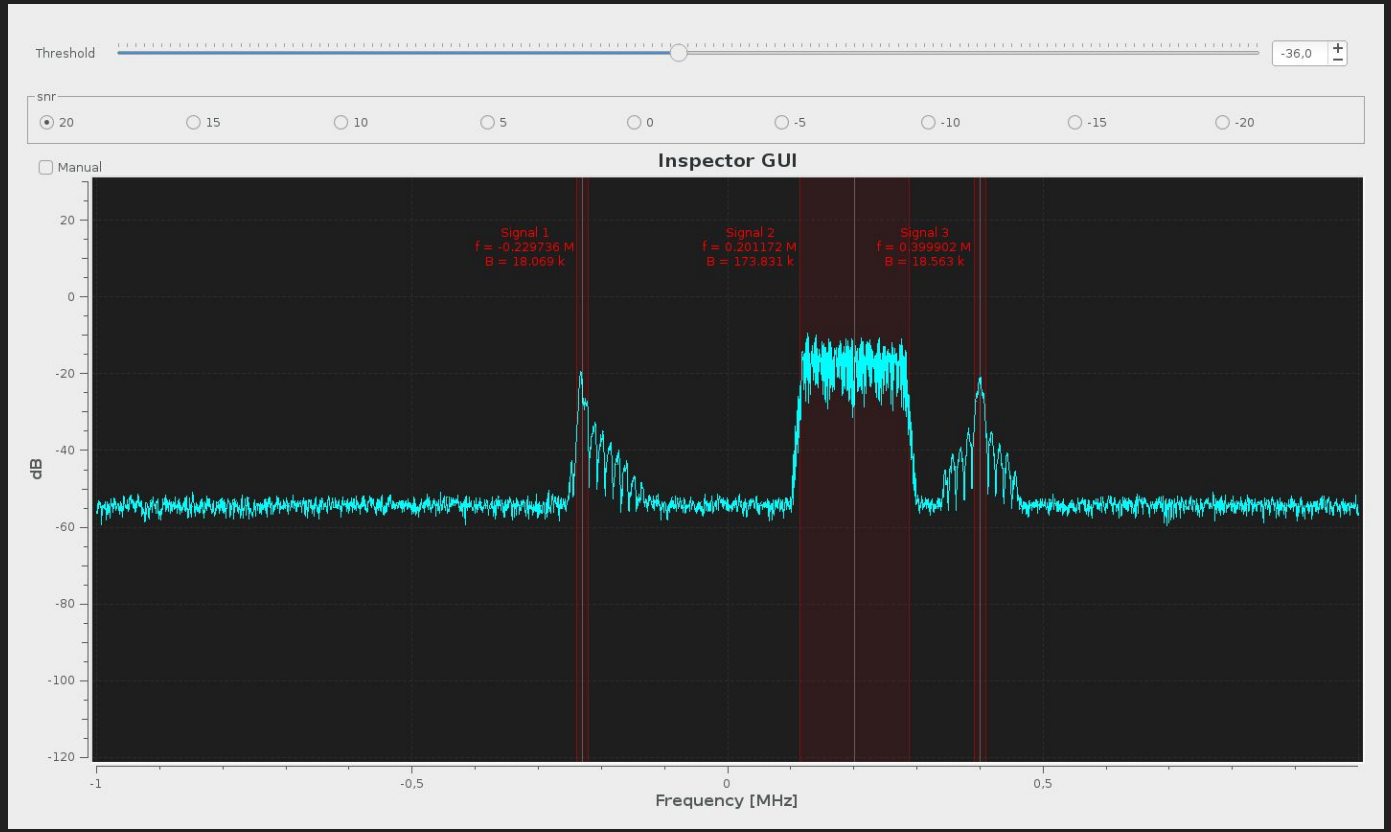
Receive all in search

▶ Choose databases

Automatic Modulation Classification in gr-inspector

8PSK
AM-DSB
AM-SSB
BPSK
CPFSK
GFSK
PAM4
QAM16
QAM64
QPSK
WBFM

gr-inspector



Waterfall Drawbacks

Missing transient events

Limited time displayed

Limited bandwidth displayed

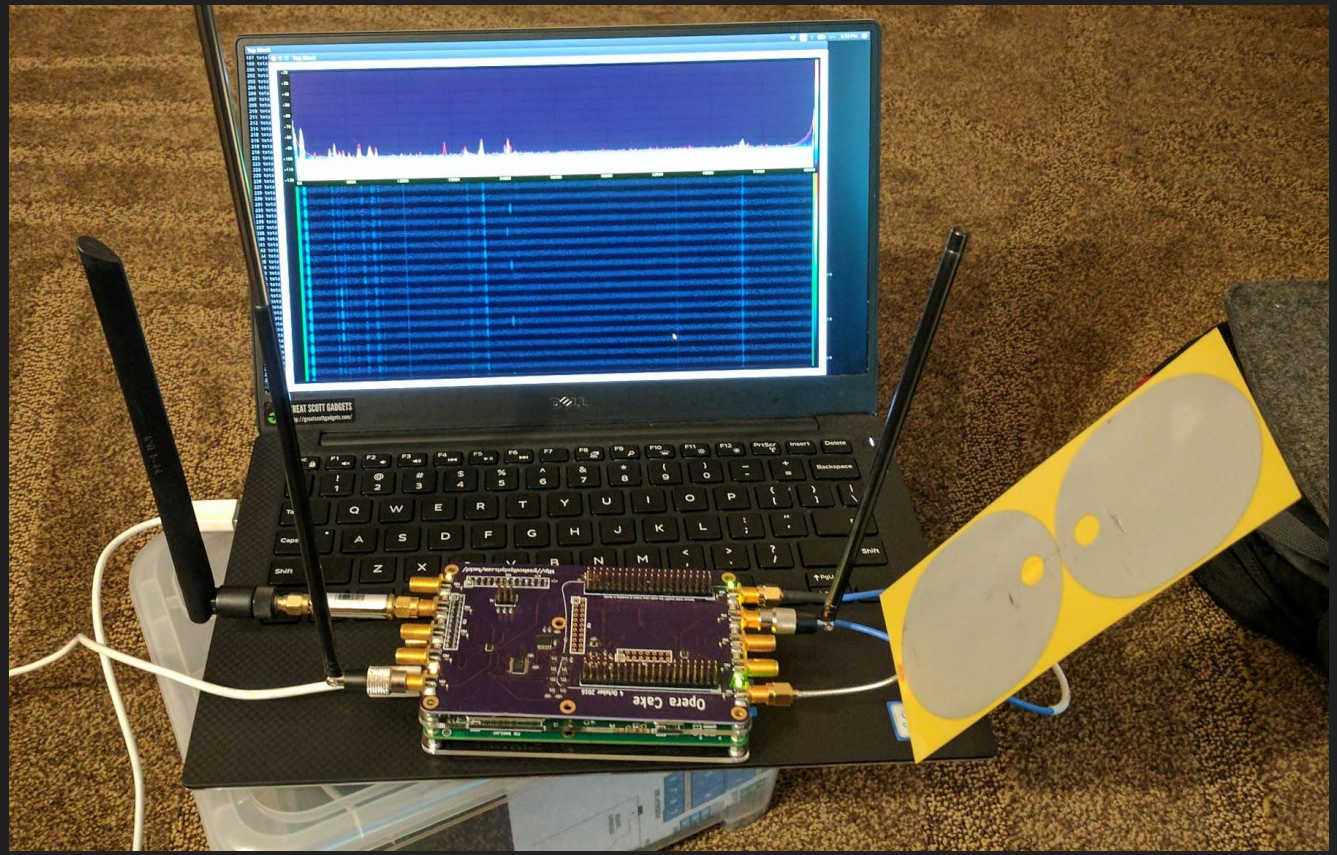
Antenna Selection

Sweeping a wide range of frequencies means a wide range of wavelengths

- 1 MHz / 300 m
- 6 GHz / 5 cm

Choosing an antenna to cover this range is complicated

Antenna Switching



Direction Finding

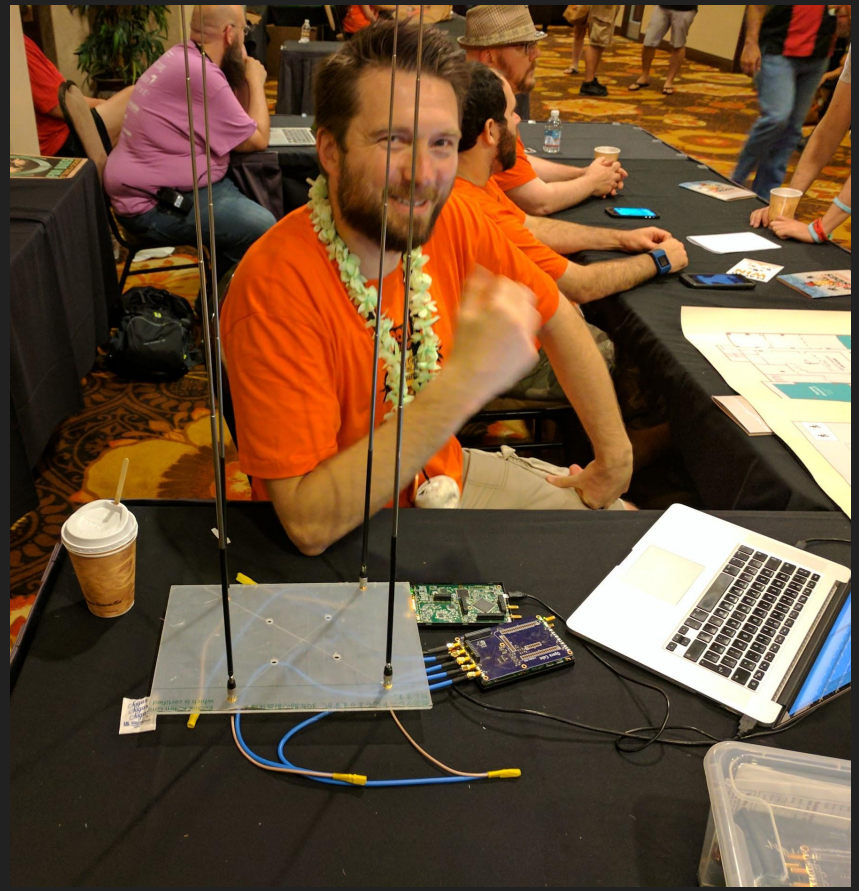
Doppler radar

Pseudo-Doppler

Directional antennas

Mike Davis - Cyberspectrum

6:30pm SYN Shop hackerspace



Thanks

Kevin Reid

Mike Walters

Michal Krenek

Great Scott Gadgets Interns:

- Jacob Graves
- Ellie Puls

Questions?

http://greatscottgadgets.com/spectrummonitoring/

http://greatscottgadgets.com/hackrf/

@dominicgs / @michaelossmann / @GSGlabs