DRIVE IT LIKE YOU HACKED IT

DEFCON 23 [2015]

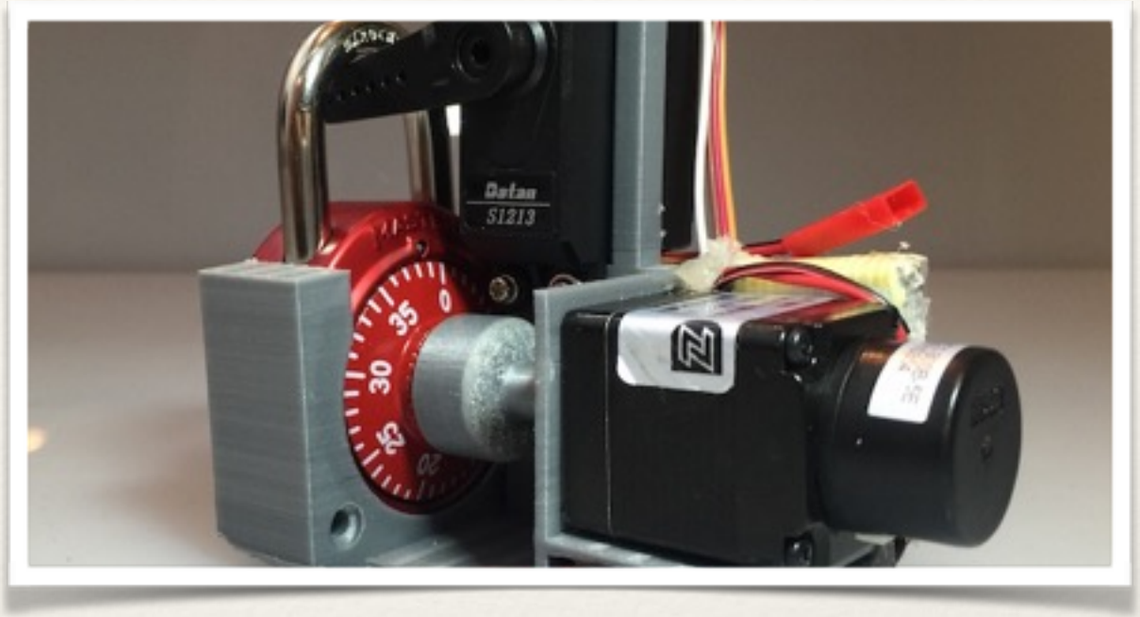
@SamyKamkar

http://samy.pl

Security Researcher

SkyJack

Combo Breaker



KeySweeper

MySpace Worm

evercookie

OwnStar pwnat

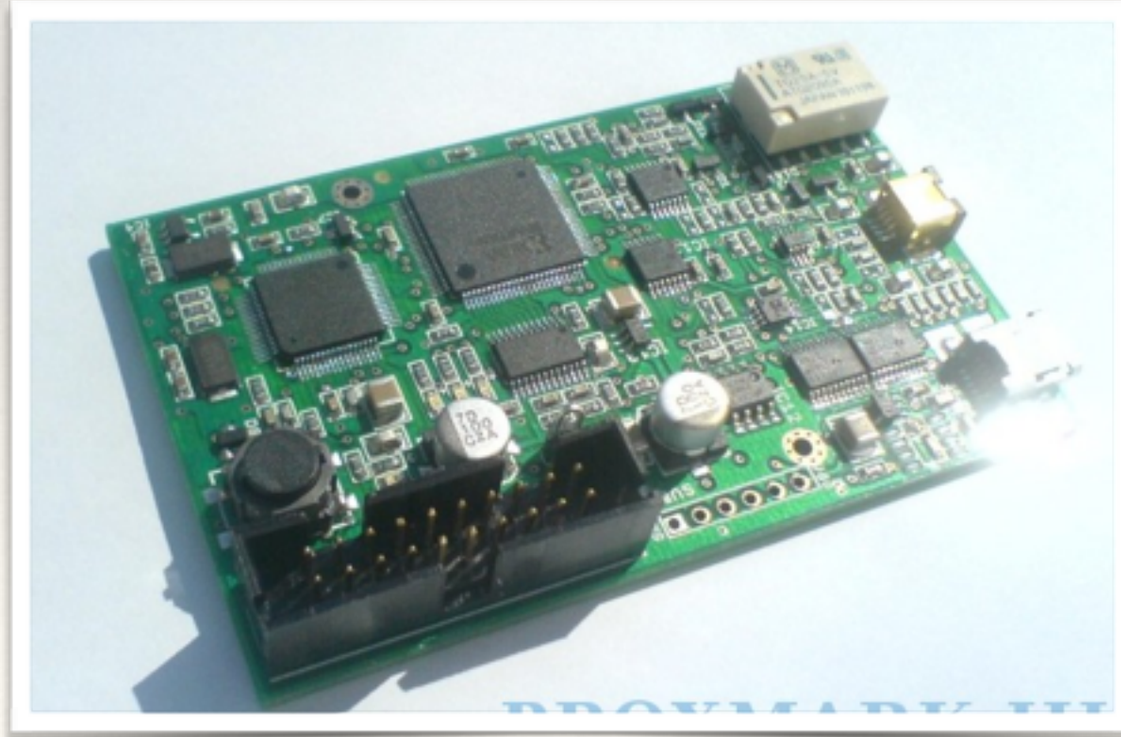
OpenSesame

USBdriveby

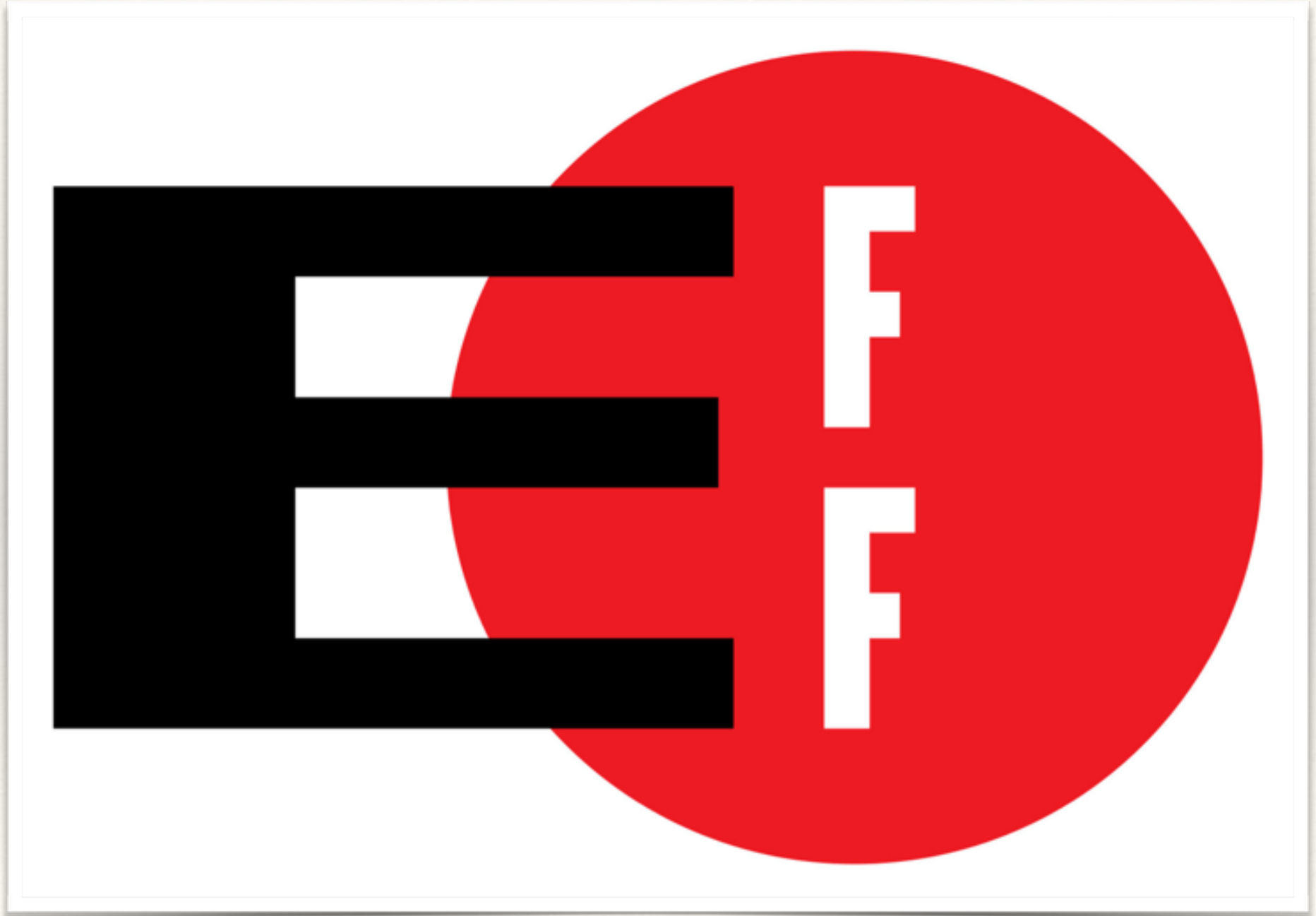
ProxyGambit

Other Works

- Charlie Miller & Chris Valasek
- 2010: UCSD/UW Research (CD player, Bluetooth, etc)
- Relay Attacks (Amplification) on PKES
- Tesla talk later today!
- Cryptographic attacks on KeeLoq
- HiTag2 Immobilizer Disabling
- OpenGarages
- iamthecavalry
- Lots of others…

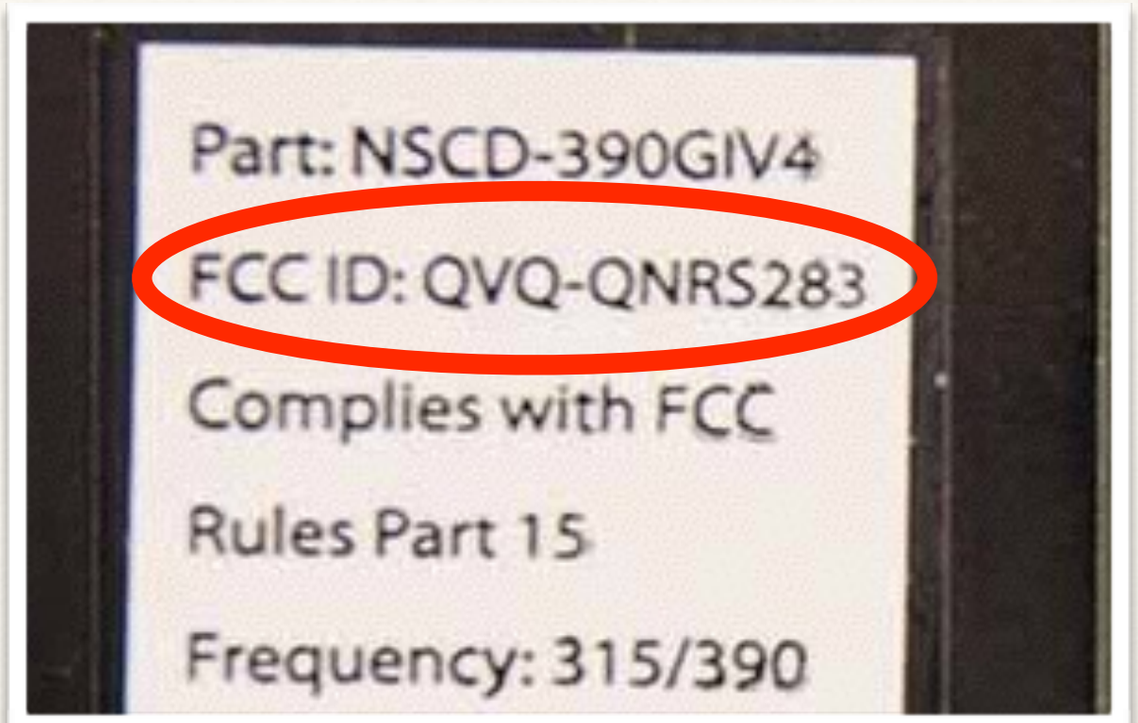


Thanks EFF!




GONE IN
60
SECONDS
www.wallpapers.cz


Part: NSCD-390GIV4
FCC ID: QVQ-QNRS283
Complies with FCC
Rules Part 15
Frequency: 315/390
northshorecommercialdoor.com

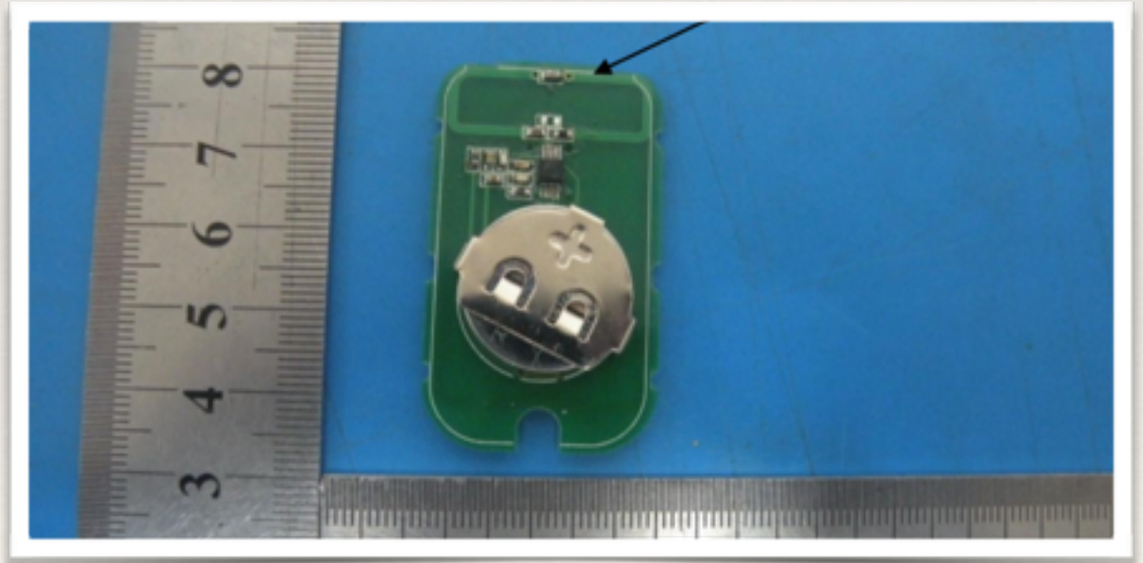

Part: NSCD-390GIV4
FCC ID: QVQ-QNRS283
Complies with FCC
Rules Part 15
Frequency: 315/390

http://fcc.io/qvq-qnrs283

http://fcc.io/qvq-qnrs283

8 Matches found for FCC ID QVQ-QNRS283

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type
Cover letter	Cover Letter(s)	11/29/2014	pdf
Cover letter	Cover Letter(s)	11/29/2014	pdf
External photos	External Photos	11/29/2014	pdf
Label	ID Label/Location Info	11/29/2014	pdf
Internal photos	Internal Photos	11/29/2014	pdf
Test report	Test Report	11/29/2014	pdf
Test setup	Test Setup Photos	11/29/2014	pdf
User manual	Users Manual	11/29/2014	pdf



use fcc.io, thanks Dominic Spill!

1 results were found that match the search criteria:

Grantee Code: qvq Product Code: -qnrs283

Displaying records 1 through 1 of 1.

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Qinuo Electronics Co., Ltd	3/F, Bldg.A, Yucheng Base, Keji Rd., High-tech Industrial Park, Fengze, Quanzhou, Fujian	Quanzhou	N/A	China	362000	QVQ-QNRS283	Original Equipment	11/29/2014	390.0	390.0

Perform Search Again

OET Exhibits List

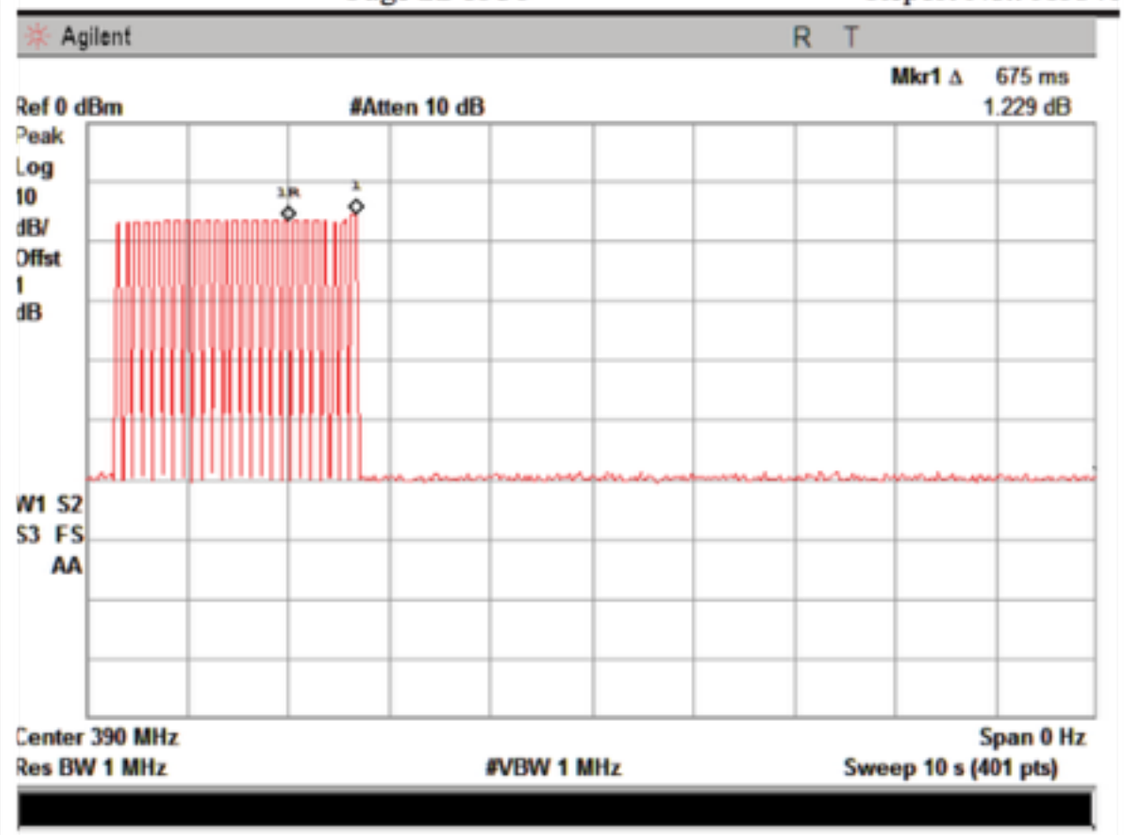
8 Matches found for FCC ID QVQ-QNRS283

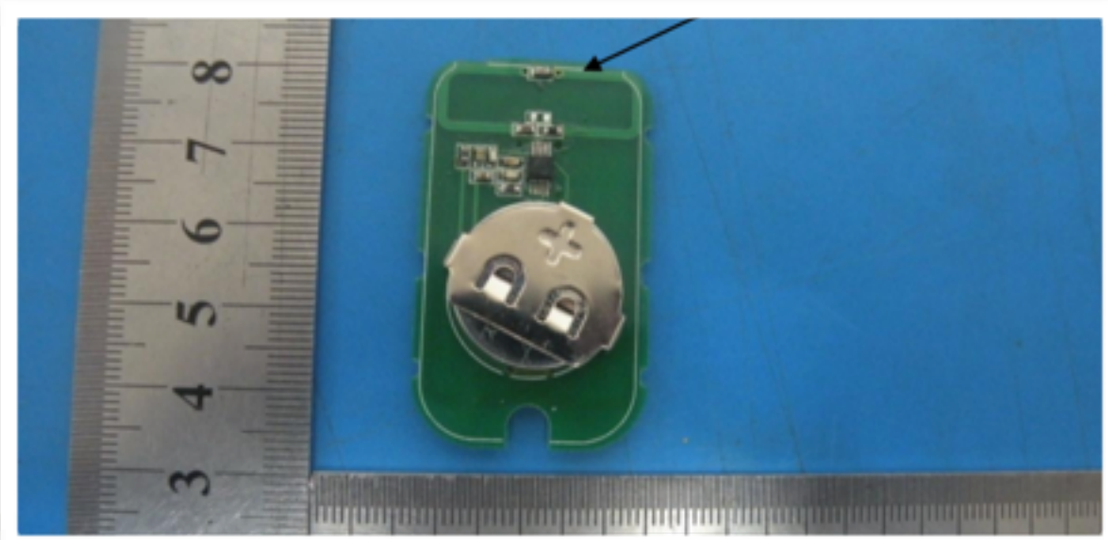
View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Cover letter	Cover Letter(s)	11/29/2014	pdf	11/29/2014
Cover letter	Cover Letter(s)	11/29/2014	pdf	11/29/2014
External photos	External Photos	11/29/2014	pdf	11/29/2014
Label	ID Label/Location Info	11/29/2014	pdf	11/29/2014
Internal photos	Internal Photos	11/29/2014	pdf	11/29/2014
Test report	Test Report	11/29/2014	pdf	11/29/2014
Test setup	Test Setup Photos	11/29/2014	pdf	11/29/2014
User manual	Users Manual	11/29/2014	pdf	11/29/2014

Federal Communications Commission [US] https

Operation Frequency	:	390 MHz
Channel number	:	1
Modulation type	:	ASK
Power Supply	:	DC 3V Supply l
Applicant	:	Qinuo Electroni
Address	:	3/F, Bldg. A, Yu Fengze, Quanzh
Manufacturer	:	Qinuo Electroni
Address	:	3/F, Bldg. A, Yu Fengze, Quanzh

Commission [US] https://apps.fcc.gov/eas/GetApplicationAttachment.html?





HackRF One

from Michael Ossmann

1 MHz - 6 GHz
half-duplex transceiver
raw I/Q samples
open source software / hardware
GNU Radio, SDR#, more

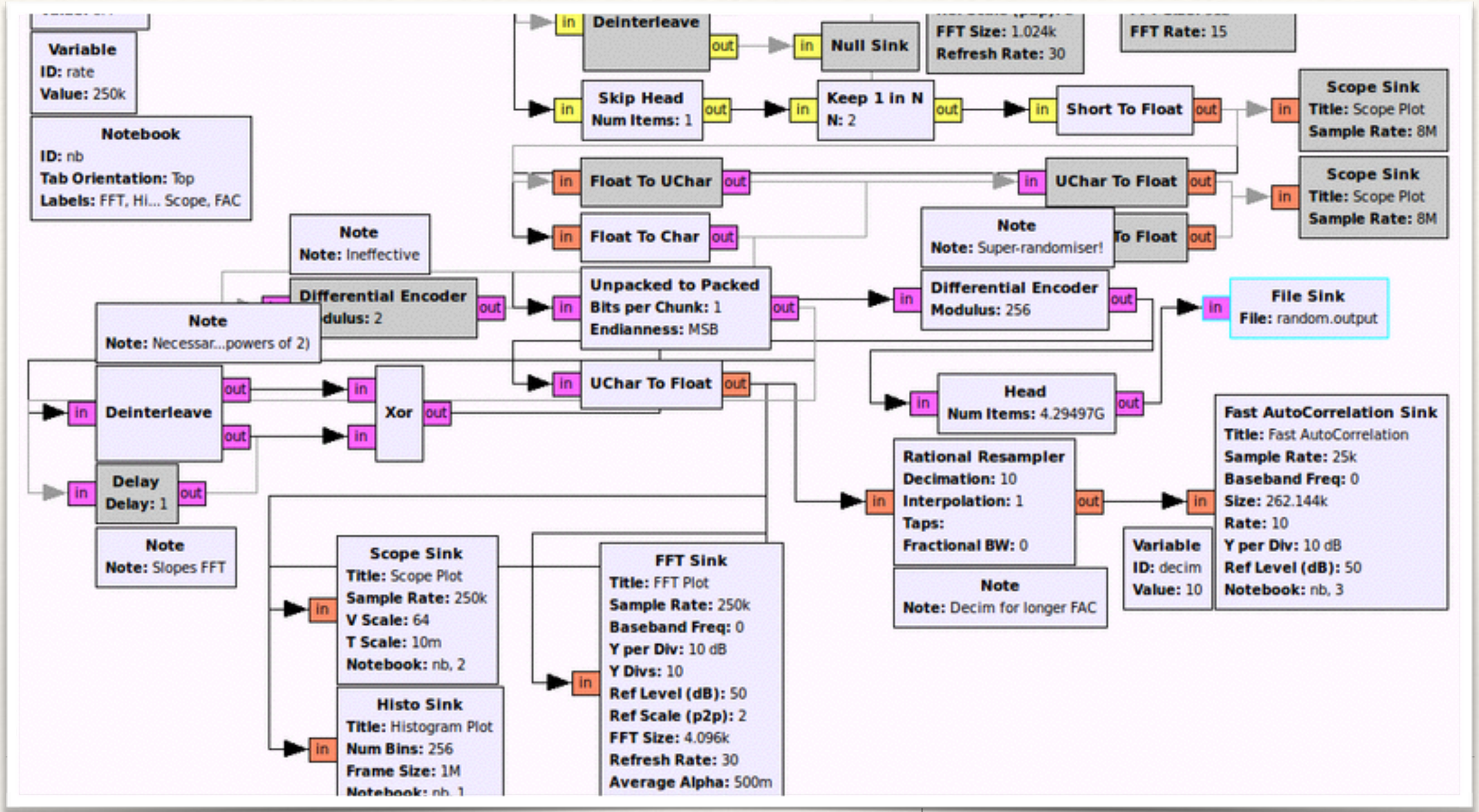
dope as shit

Replay Attack w/HackRF

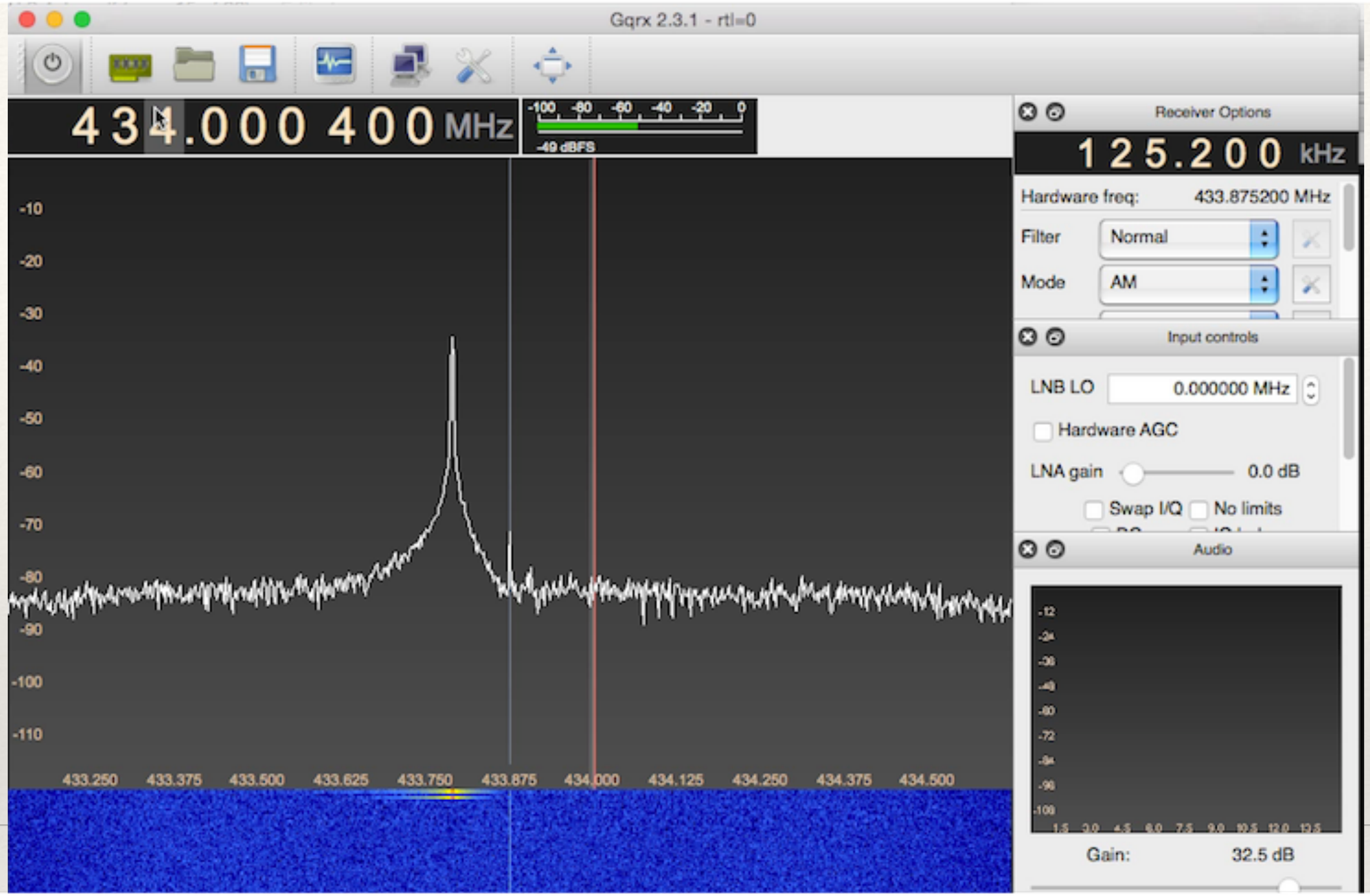
- **hackrf_transfer -r 390_data.raw -f 390000000 # listen**
- **hackrf_transfer -t 390_data.raw -f 390000000 # transmit**
- # profit
- Don't need baud rate
- Don't need modulation/demodulation
- Can be within 20MHz
- Can act as a "raw" code grabber/replayer…but it's more interesting than that.

RTL-SDR

24 - 1766 MHz
raw I/Q samples
RX only
RTL2832U



GNU Radio
(the stick shift of SDR)



waterfall views
demodulation
save to WAV

pretty
Linux & OS X Only

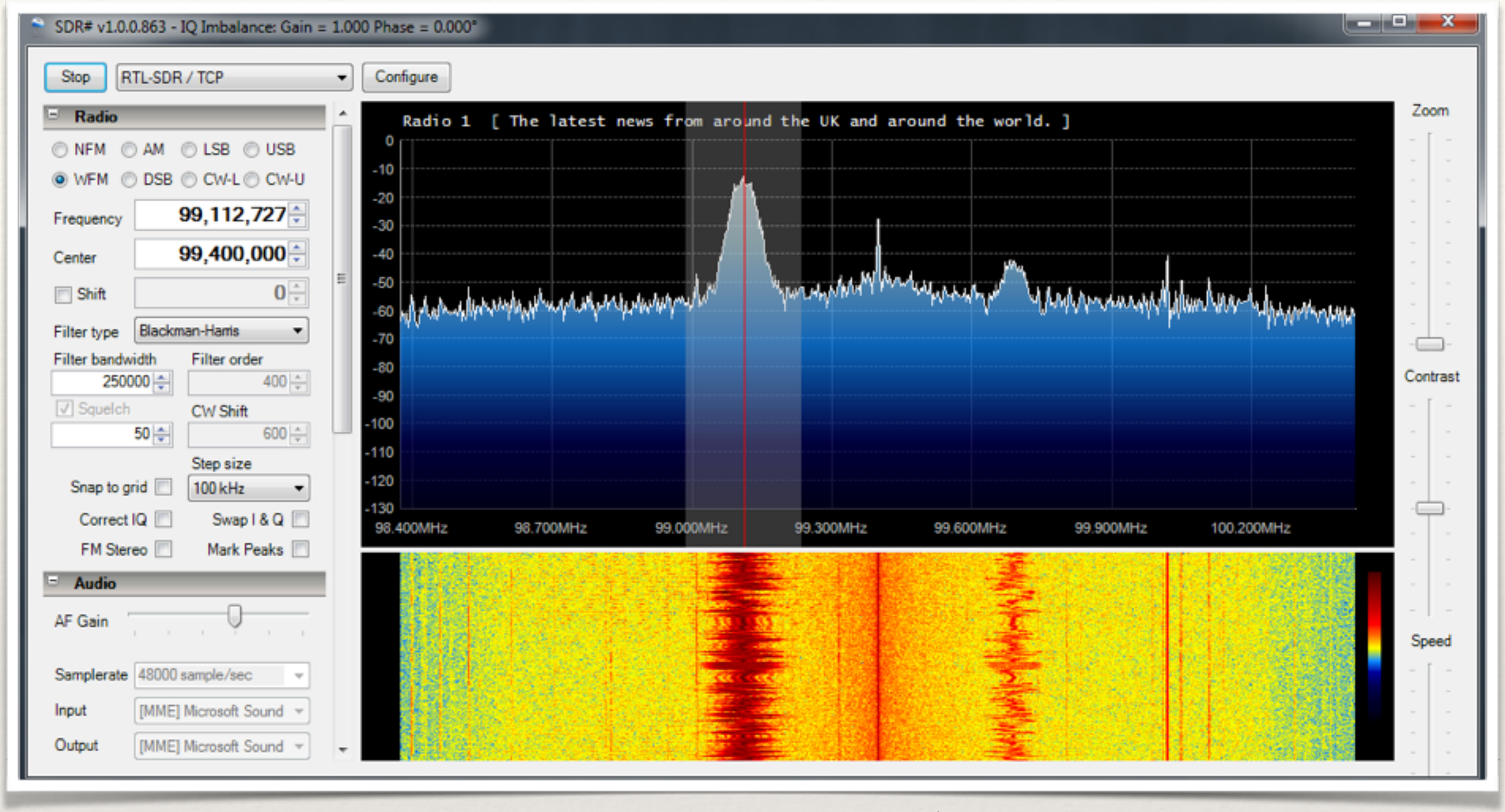
GQRX

Windows Technical Preview Setup

Something happened

Something happened

Close



SDR#

Works on Windows
Sorta kinda on OS X

```
tigerblood:/Users/samy/code/garage$ rtl_fm -h
rtl_fm, a simple narrow band FM demodulator for RTL2832 based DVB-T receivers

Use:    rtl_fm -f freq [-options] [filename]
        -f frequency_to_tune_to [Hz]
           use multiple -f for scanning (requires squelch)
           ranges supported, -f 118M:137M:25k
        [-M modulation (default: fm)]
           fm, wbfm, raw, am, usb, lsb
           wbfm == -M fm -s 170k -o 4 -A fast -r 32k -l 0 -E deemp
           raw mode outputs 2x16 bit IQ pairs
        [-s sample_rate (default: 24k)]
        [-d device_index (default: 0)]
        [-g tuner_gain (default: automatic)]
        [-l squelch_level (default: 0/off)]
        [-p ppm_error (default: 0)]
        [-E enable_option (default: none)]
           use multiple -E to enable multiple options
           edge:   enable lower edge tuning
```

rtl_fm

terminal based
quick and easy
demodulates

OET Exhibits List

8 Matches found for FCC ID QVQ-QNRS283

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Cover letter	Cover Letter(s)	11/29/2014	pdf	11/29/2014
Cover letter	Cover Letter(s)	11/29/2014	pdf	11/29/2014
External photos	External Photos	11/29/2014	pdf	11/29/2014
Label	ID Label/Location Info	11/29/2014	pdf	11/29/2014
Internal photos	Internal Photos	11/29/2014	pdf	11/29/2014
Test report	Test Report	11/29/2014	pdf	11/29/2014
Test setup	Test Setup Photos	11/29/2014	pdf	11/29/2014
User manual	Users Manual	11/29/2014	pdf	11/29/2014

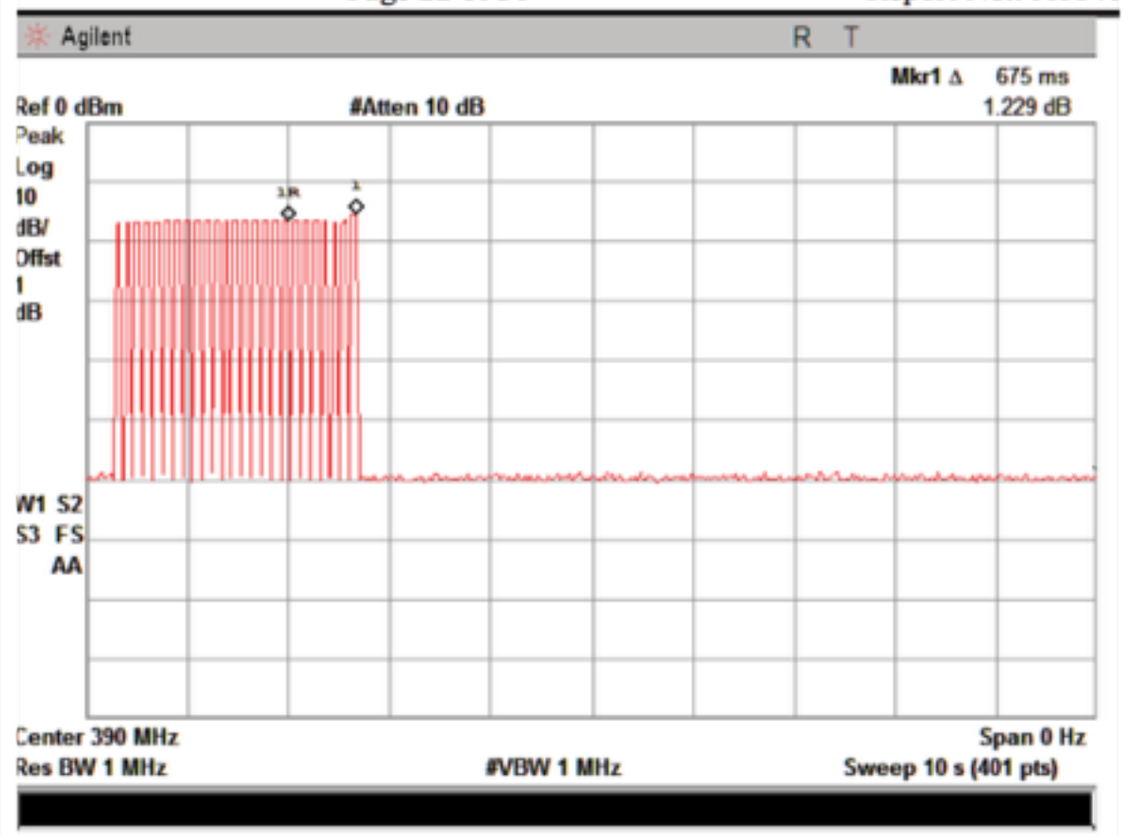
Test Report

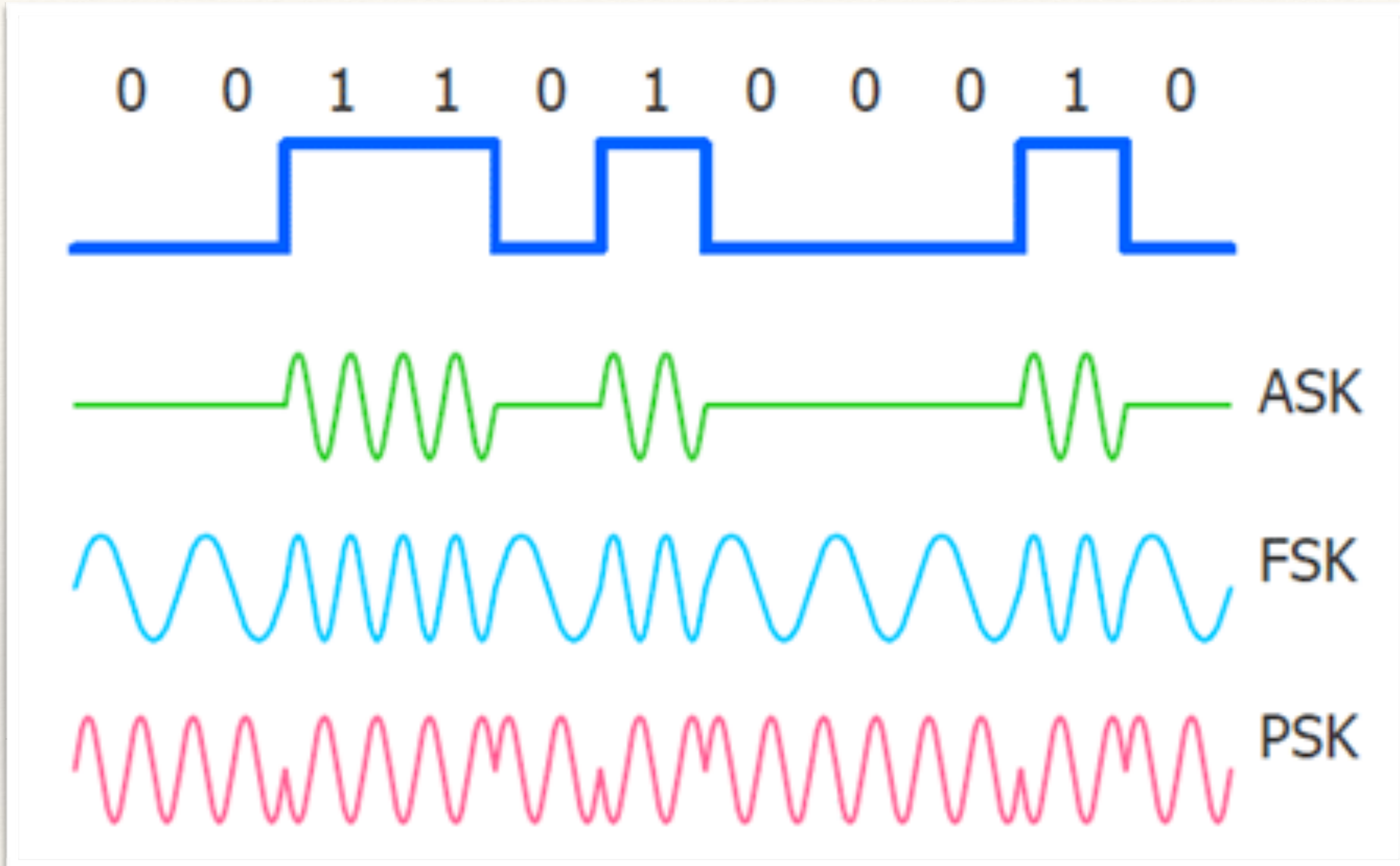
Federal Communications Commission [US] https

Operation Frequency	:	390 MHz
Channel number	:	1
Modulation type		ASK
Power Supply	:	DC 3V Supply l
Applicant	:	Qinuo Electroni
Address	:	3/F, Bldg. A, Yu Fengze, Quanzh
Manufacturer	:	Qinuo Electroni
Address	:	3/F, Bldg. A, Yu Fengze, Quanzh

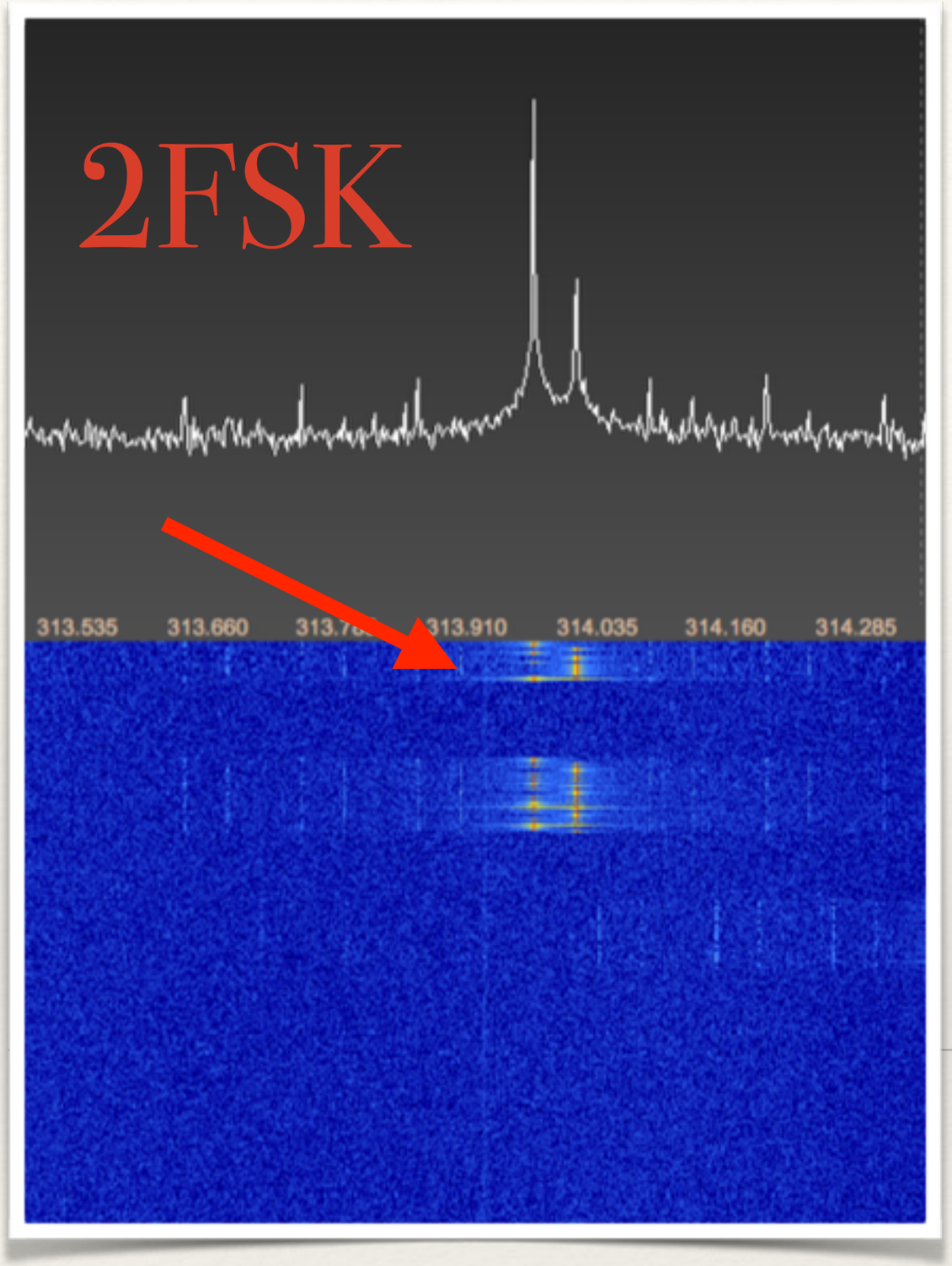
Commission [US] https://apps.fcc.gov/eas/GetApplicationAttachment.html?

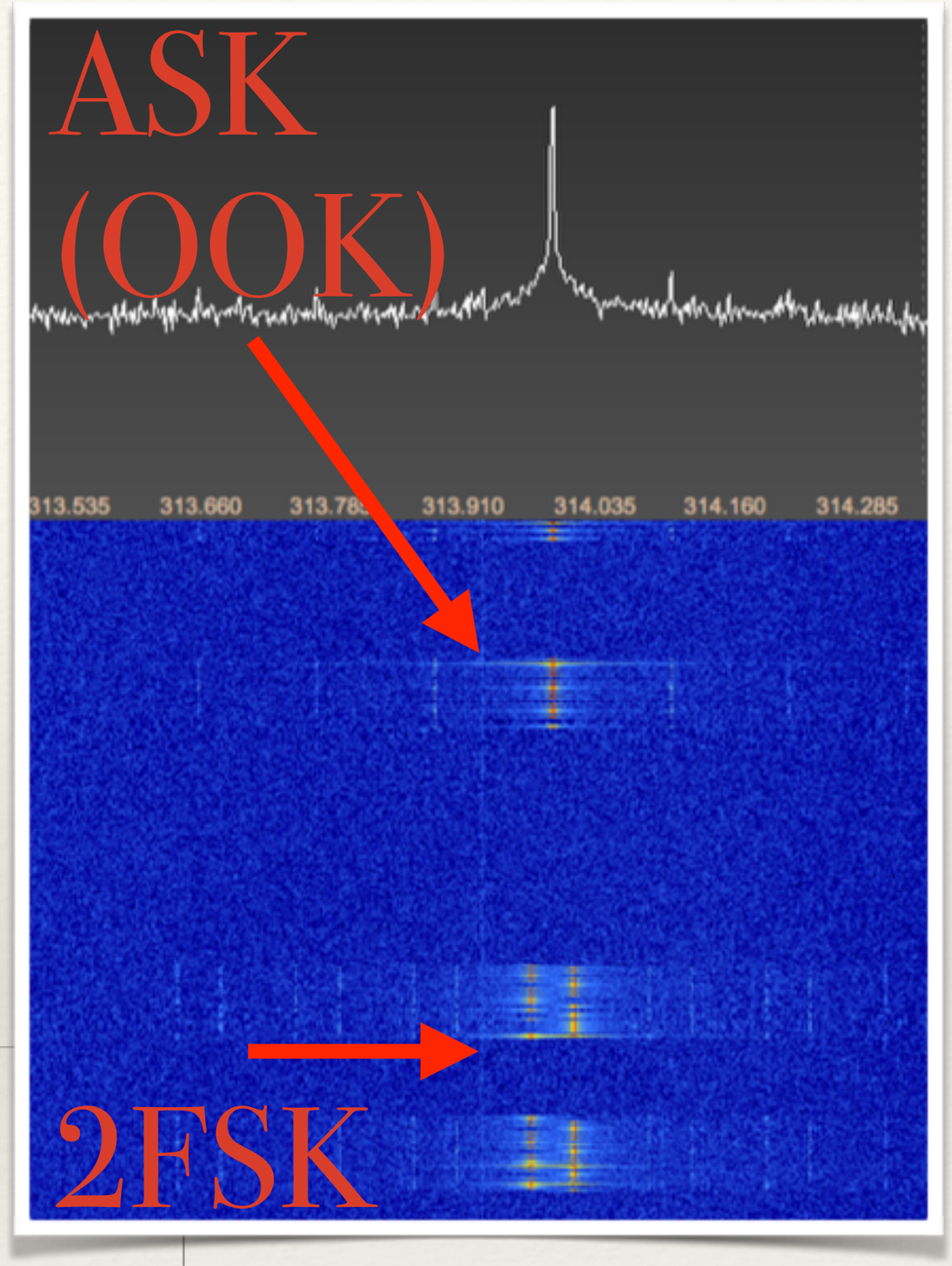
Page 22 of 30 Report No.: A1840



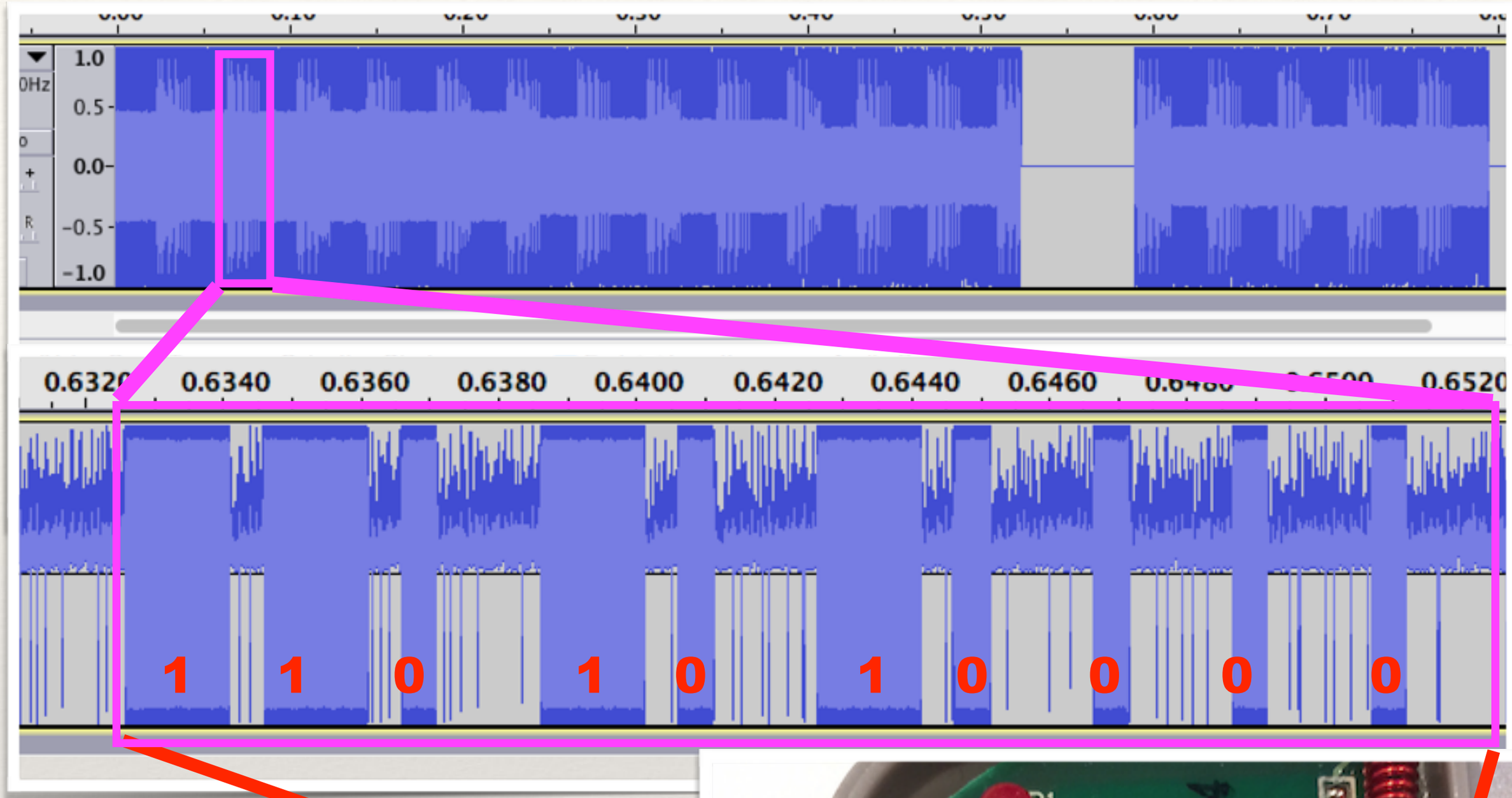


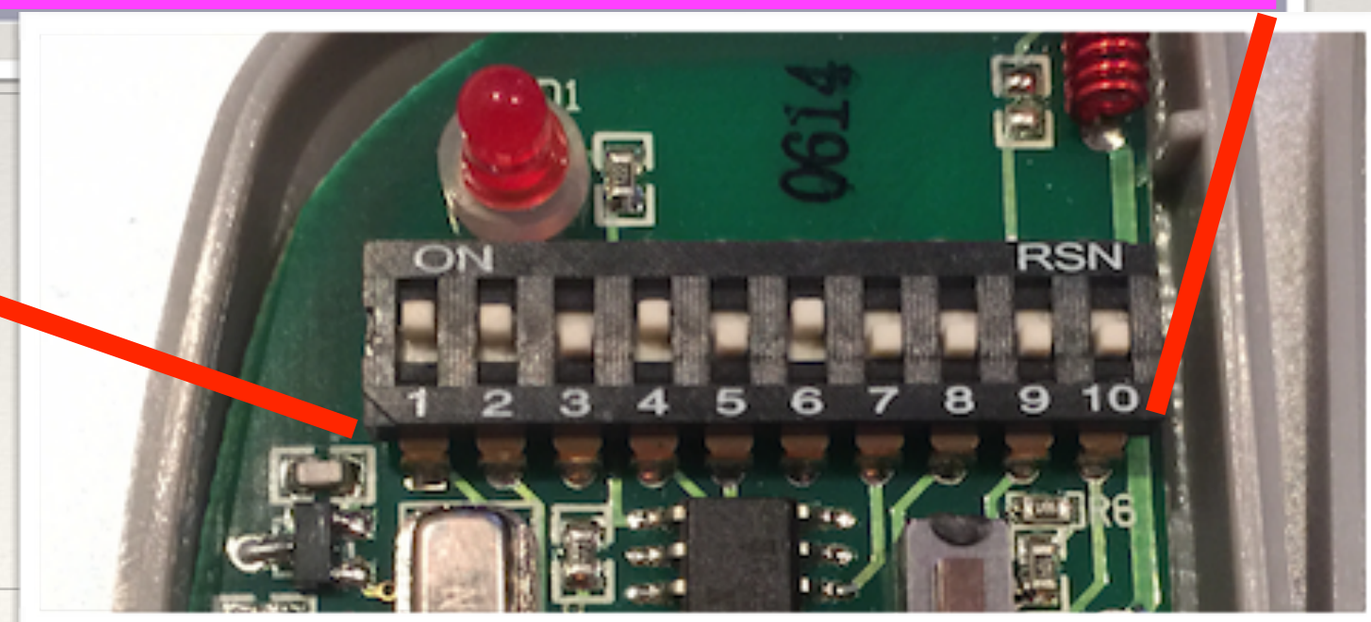
Modulation Schemes





Modulation Schemes





ASK (OOK) 10-bit Garage

Fixed Code Garages

8 - 12 bit code

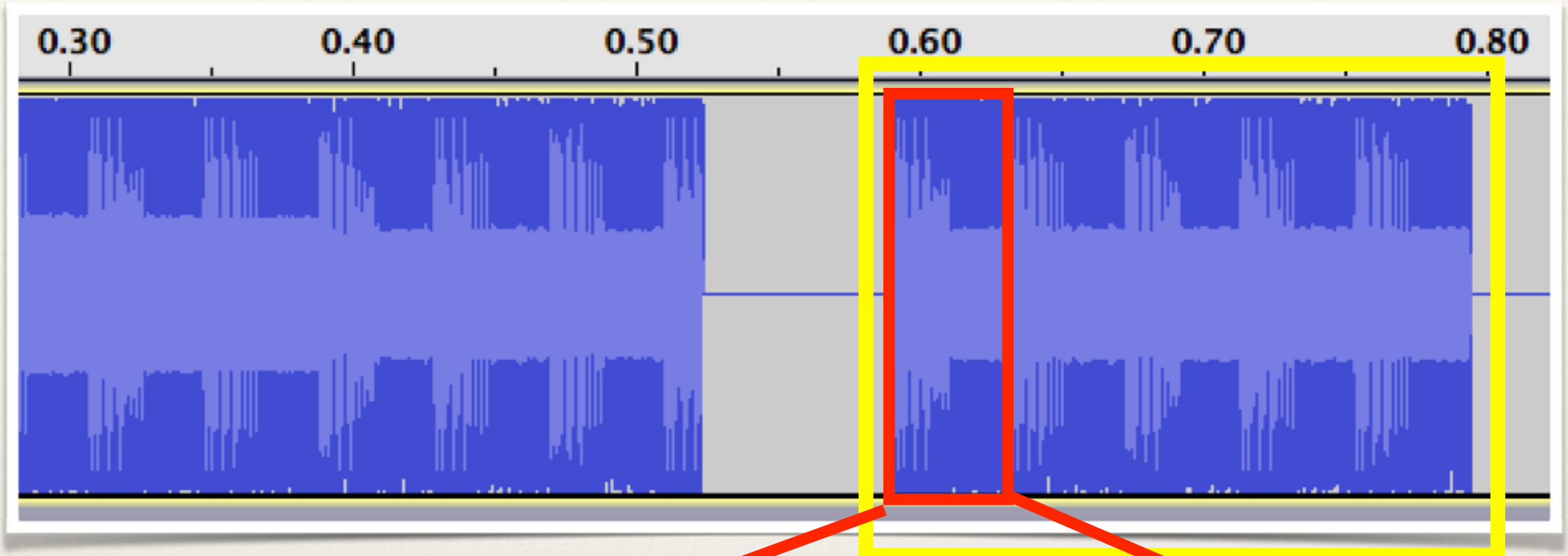
~2ms per bit + ~2ms delay

5 signals per transmission

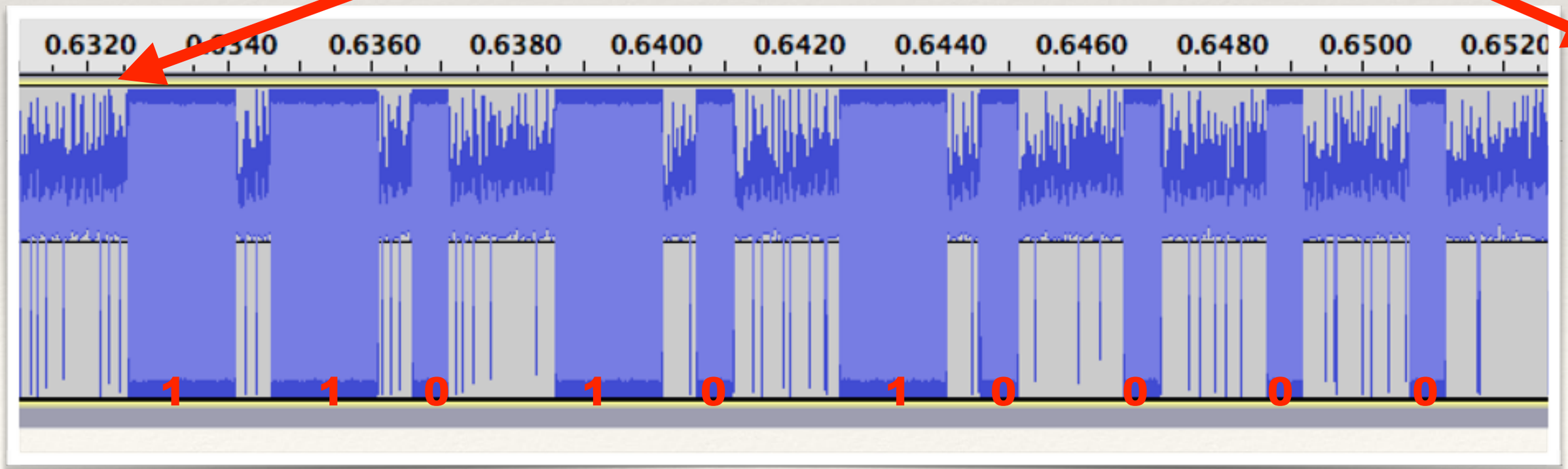
(((2 ** 12)*12) +
((2 ** 11)*11) +
((2 ** 10)*10) +
((2 ** 9)*9) +
((2 ** 8)*8)) = **88576 bits**

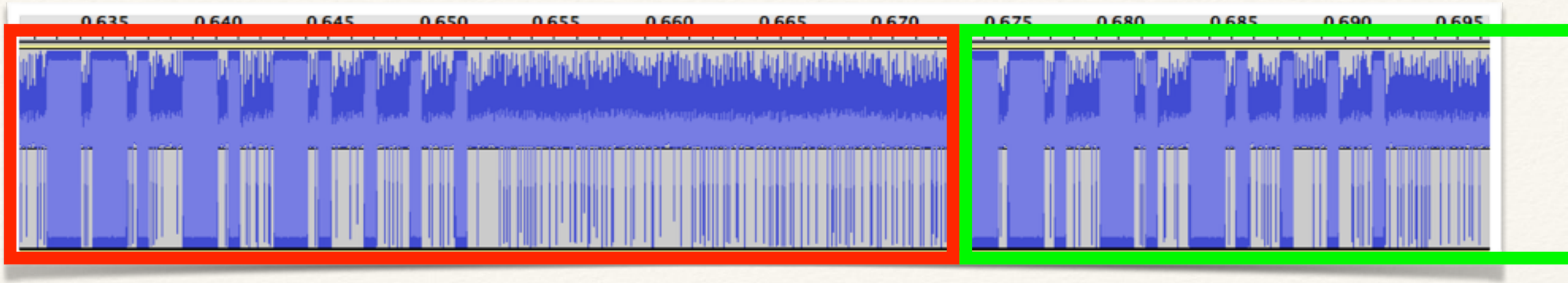
88576 bits * (2ms signal + 2ms delay) * 5 transmissions = 1771520ms = 1771secs =

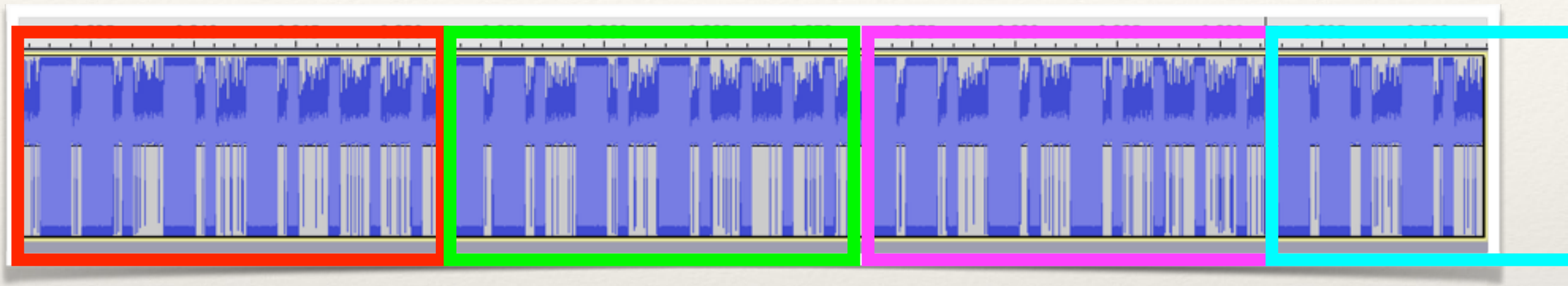
29.5 minutes



1771 secs / 5 = 354.2 = **6 mins**







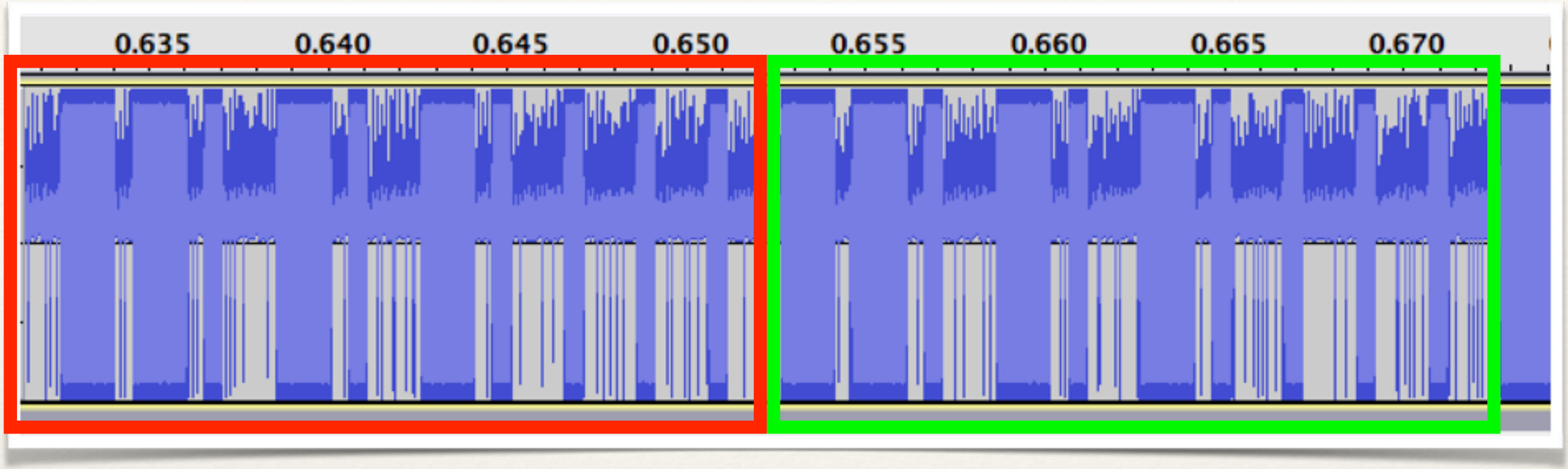
354.2 secs / 2 = 177 secs = **3 mins**

Thanks Mike Ryan!

Saturday, 3pm, Track Two

Hacking Electric Skateboards

Mike Ryan & Richo Healey



Where does one code end and the other begin?

Bit shift register?

Bit Shift Register

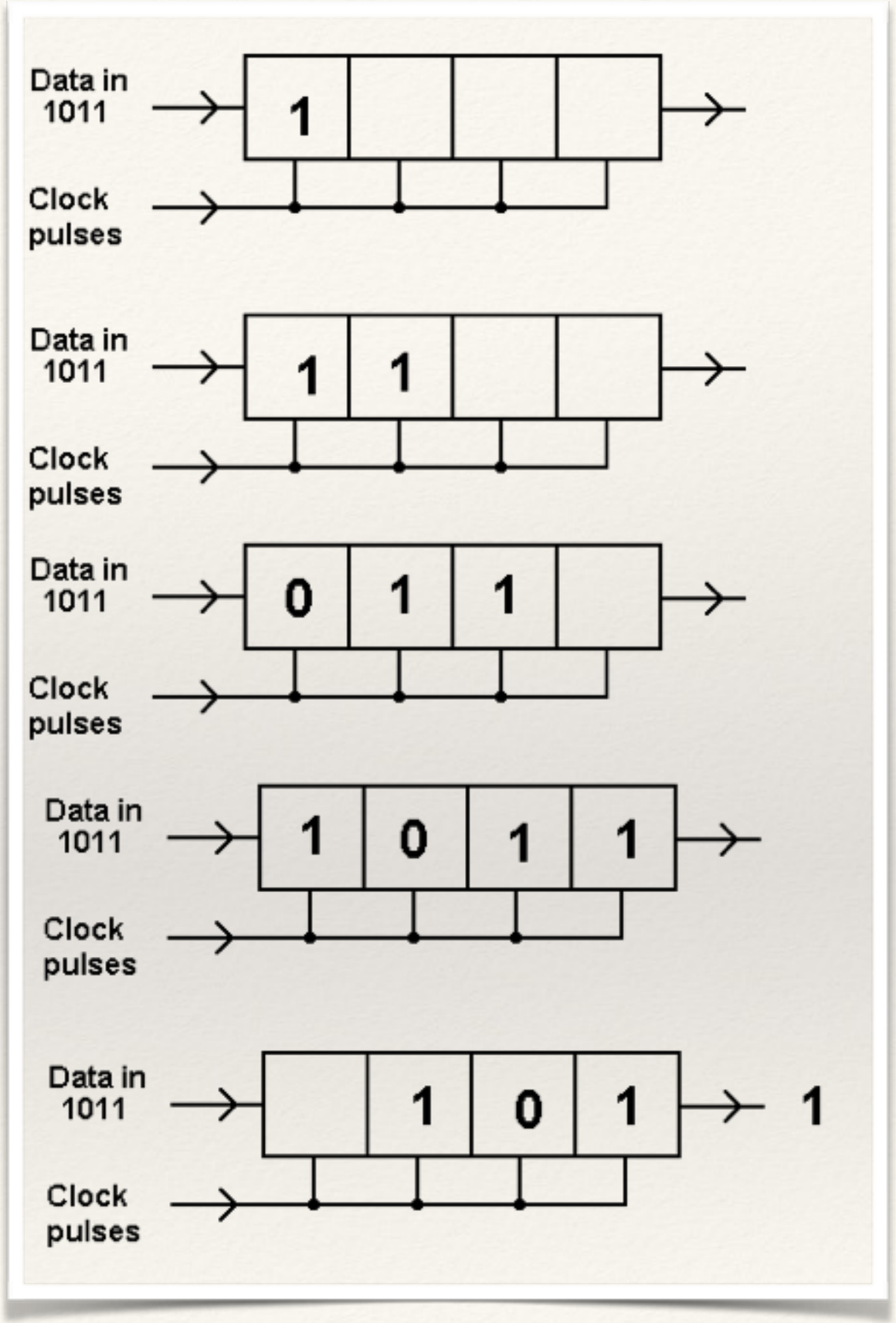
Code only clears one bit at a time while pulling in next bit

A 13 bit code tests two different 12 bit codes!

1000000000001

1000000000000

~~1~~000000000001



De Bruijn Sequence

00110 (5 bits) tests all 4 different 2-bit sequences instead of 8 bits total

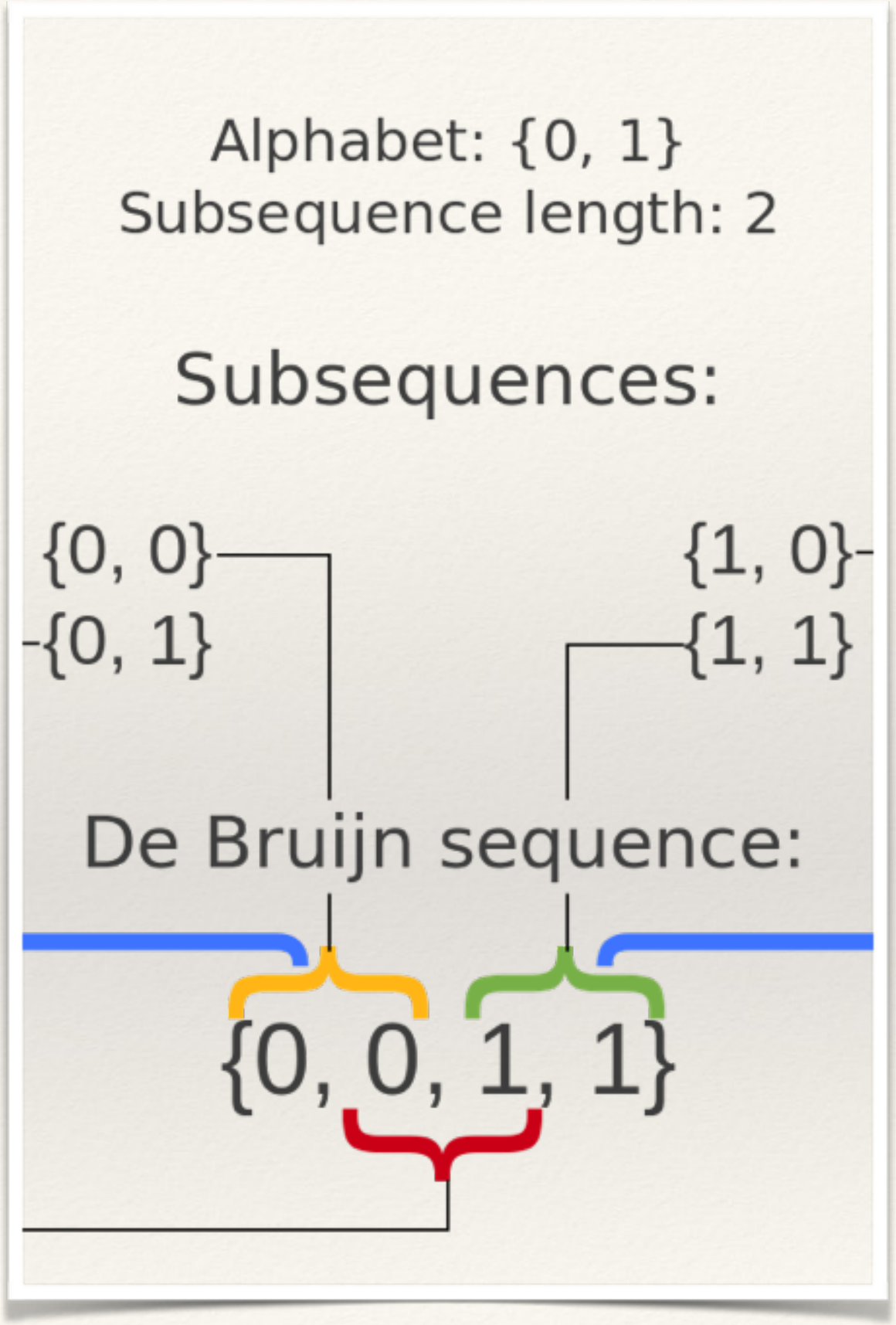
00110

0**01**10

00**11**0

001**10**

vs **00011110**



Brute forcing a 3-bit code

```
    1 bit      10 bits    20 bits    30 bits    40 bits    50 bits
bit 0123456789012345678901234567890123456789012345678901234567890
    000---001---010---101---011---111---110---100--- <--48 bits
```

OpenSesame Attack

First, remove the wait periods (reduces 50%):

```
    1 bit      10 bits    20 bits    30 bits    40 bits    50 bits
bit 0123456789012345678901234567890123456789012345678901234567890
    000001010101011111110100 <-- 24 bits
```

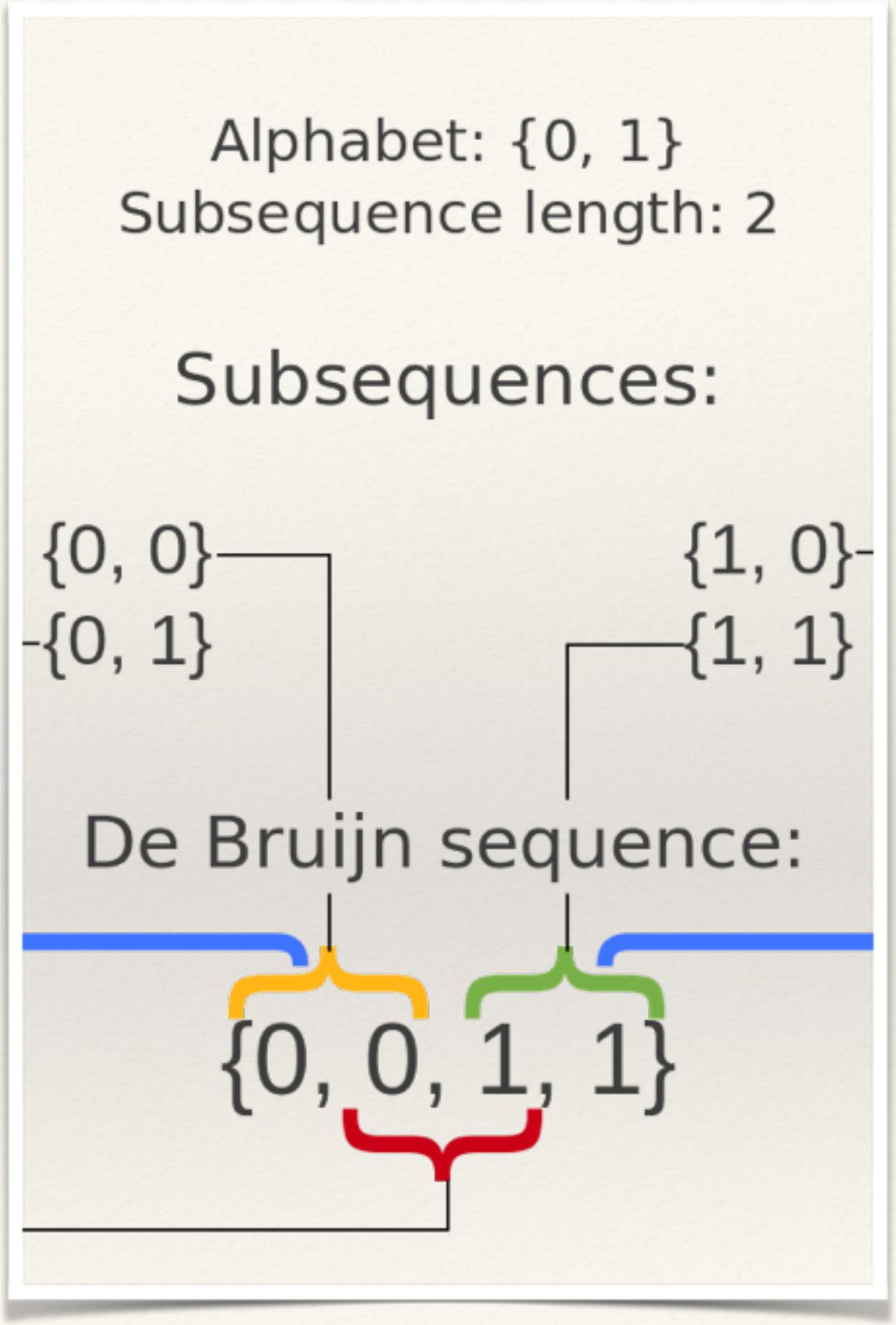
By overlapping (De Bruijn), we reduce another ~62%:

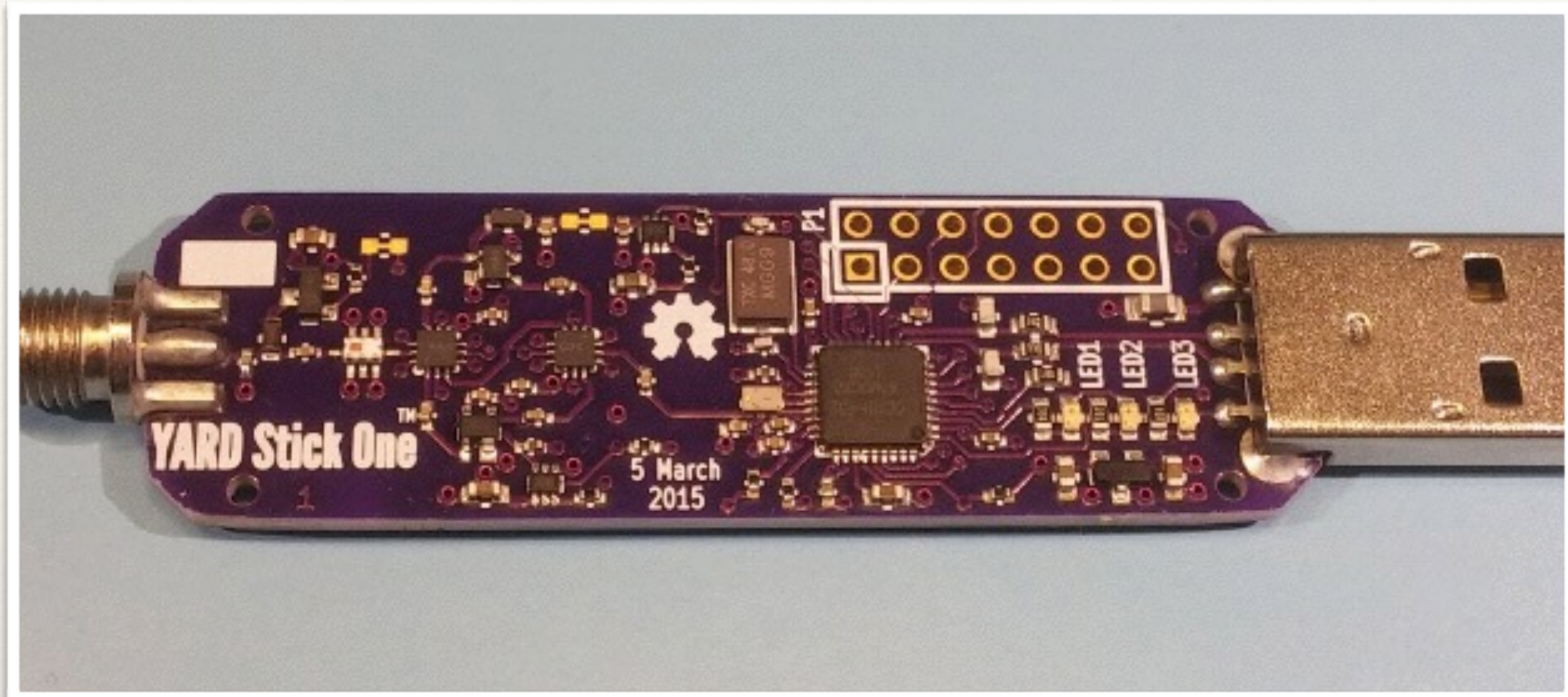
```
    000 011
     001 111
      010 110
       101 100
    0001011100  <-- 10 bits!
```

De Bruijn Sequence

For every 8 to 12 bit garage code

((2 ** 12) + 11) *
4ms / 2 =
8214ms =
8.214 seconds





Yard Stick One

by Michael Ossmann

TI CC1111 chipset

rfcat

by atlas

Friday, 5pm, Track Two

Fun with Symboliks

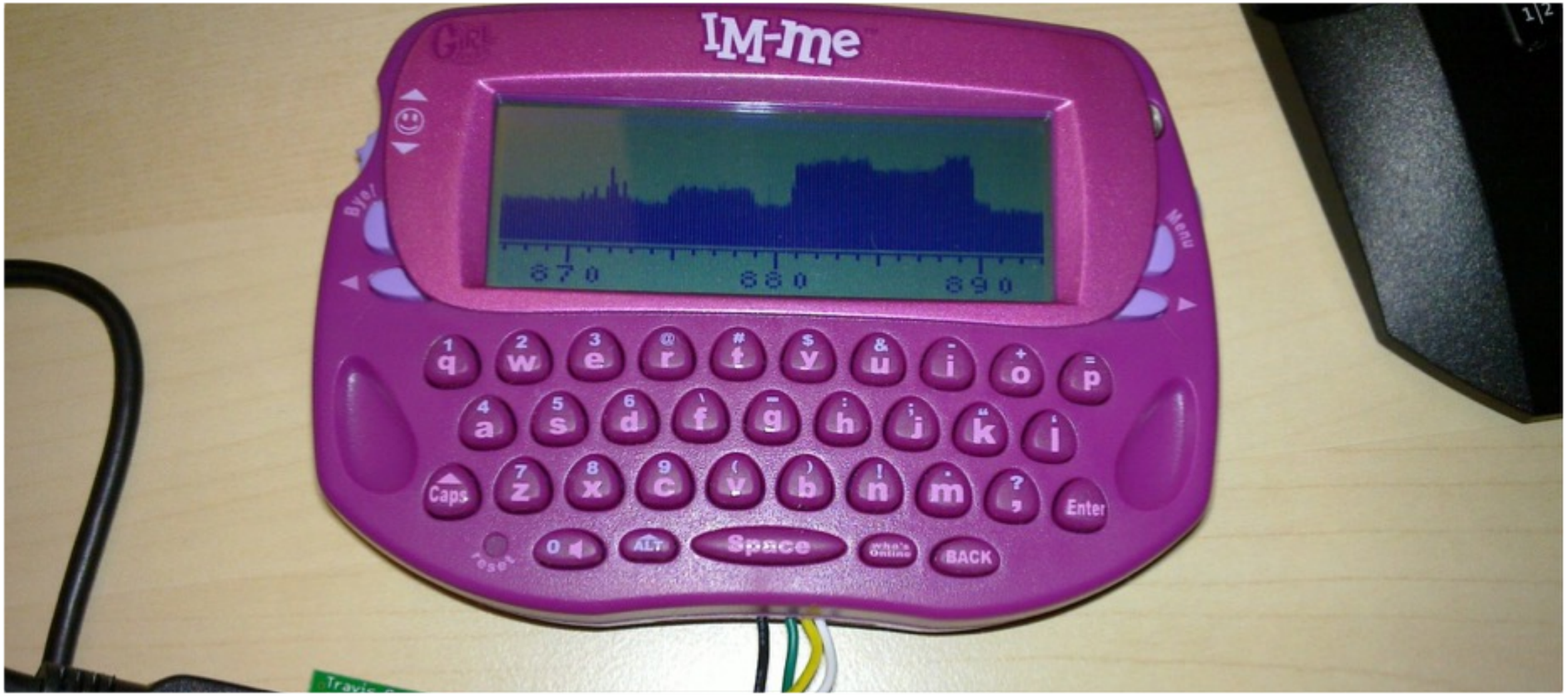
```
Research Mode: enjoy the raw power of rflib

currently your environment has an object cal
you interact with the rfcat dongle:
    >>> d.ping()
    >>> d.setFreq(433000000)
    >>> d.setMdmModulation(MOD_ASK_OOK)
    >>> d.makePktFLEN(250)
    >>> d.RFxmit("HALLO")
    >>> d.RFrecv()
    >>> print d.reprRadioConfig()
```

```
es"><span class="price">$97.00</span><
="map-text">For a better price, Add to
In [1]: business day</td></tr><tr><td
```

#ImAnEngineer

At the local hacker space, Barbie has been working with Evelina where they've developed firmware for their favorite Mattel toy, the IM-ME, to perform RF jamming, automated sniffing, demodulation, and replay attacks on ISM bands under 1GHz.

MATTEL ®



Mattel IM-ME

TI CC1101 chipset

sub-GHz transceiver

screen, backlight, keyboard, stylish

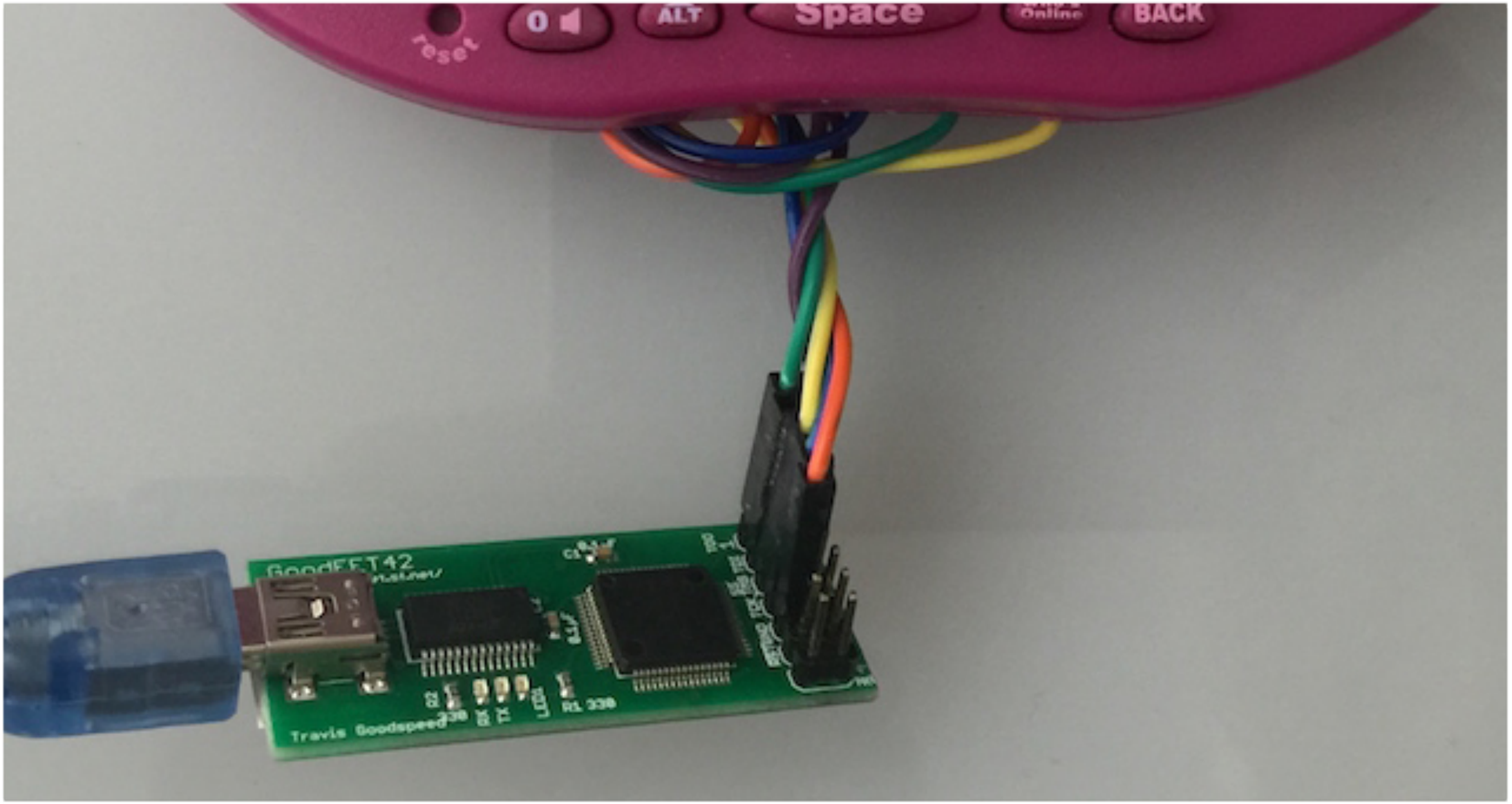
Previously hacked by:

Dave

Michael Ossmann

Travis Goodspeed

Hacker Barbie

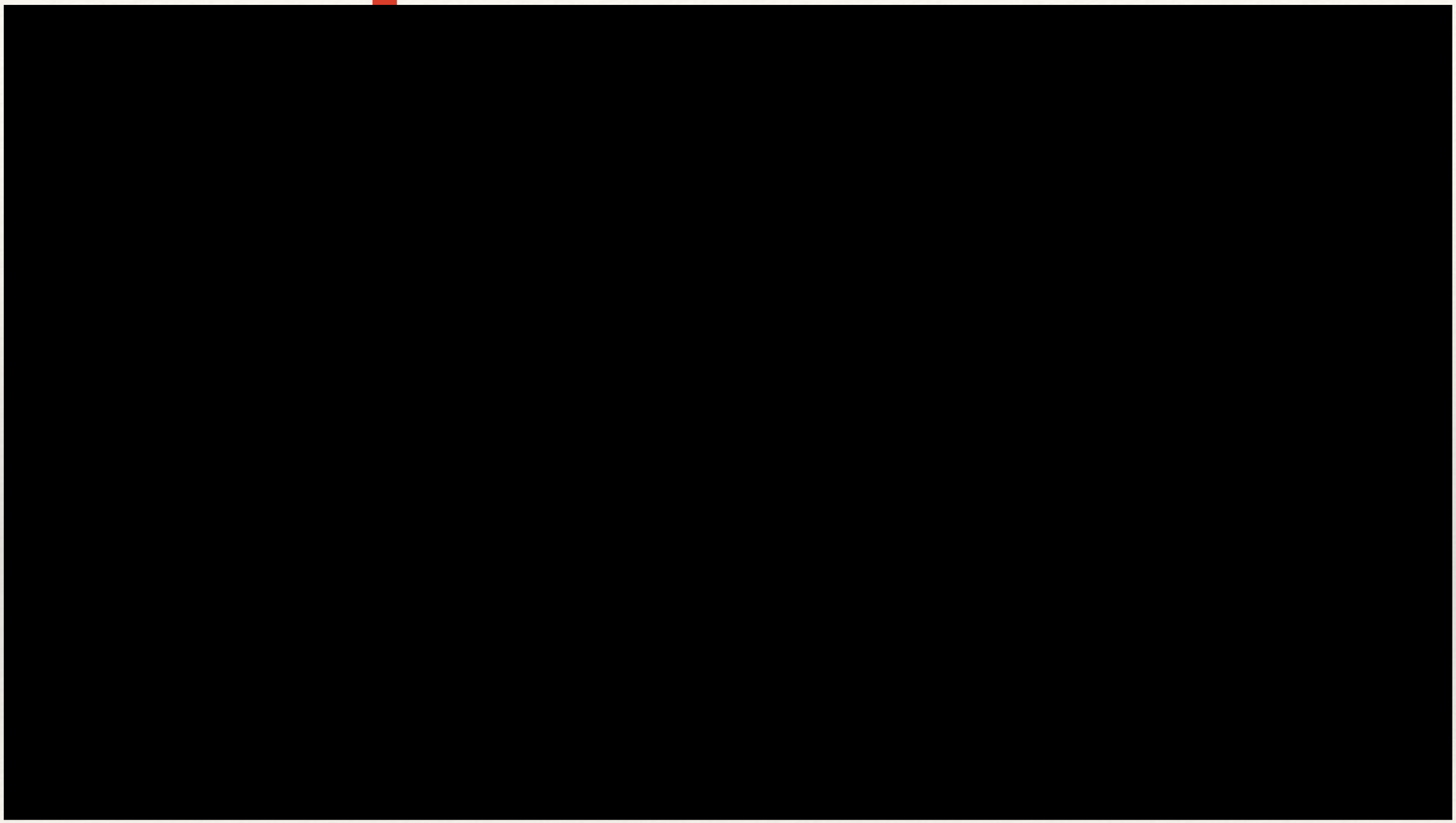


GoodFET

by Travis Goodspeed

open source JTAG adapter / universal serial bus interface

OpenSesame



based off of Michael Ossmann's opensesame ASK transmitter
https://github.com/mossmann/im-me/tree/master/garage

| Listed in category: Toys & Hobbies > Radio Control & Control Line > Radio Control Vehicles > Ca

Radica IM Me Wireless Handh

1 viewed per hour

Item condition: **New**

Quantity: 1 3 availa

Price: **US $909.83**

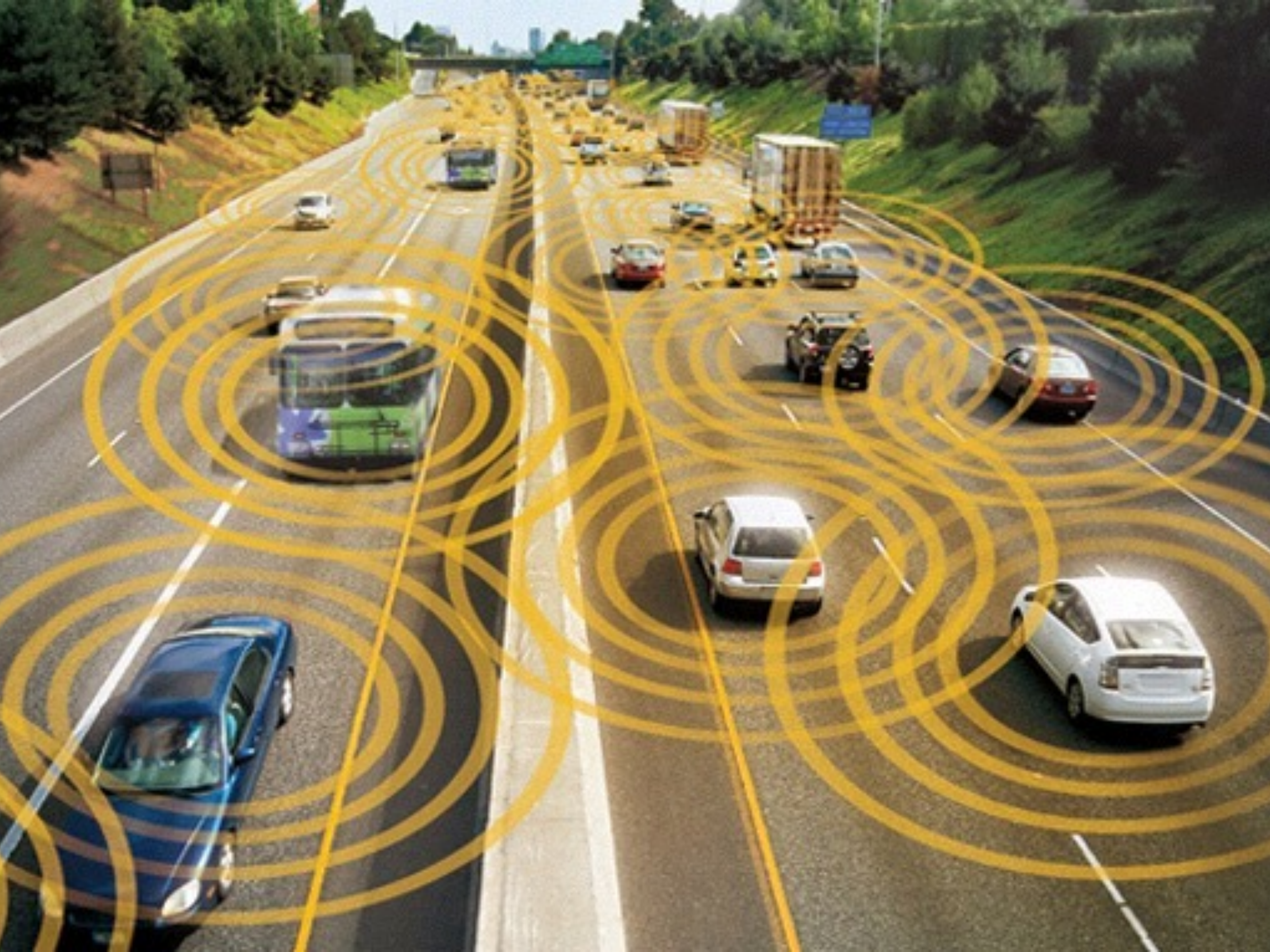
5 watching

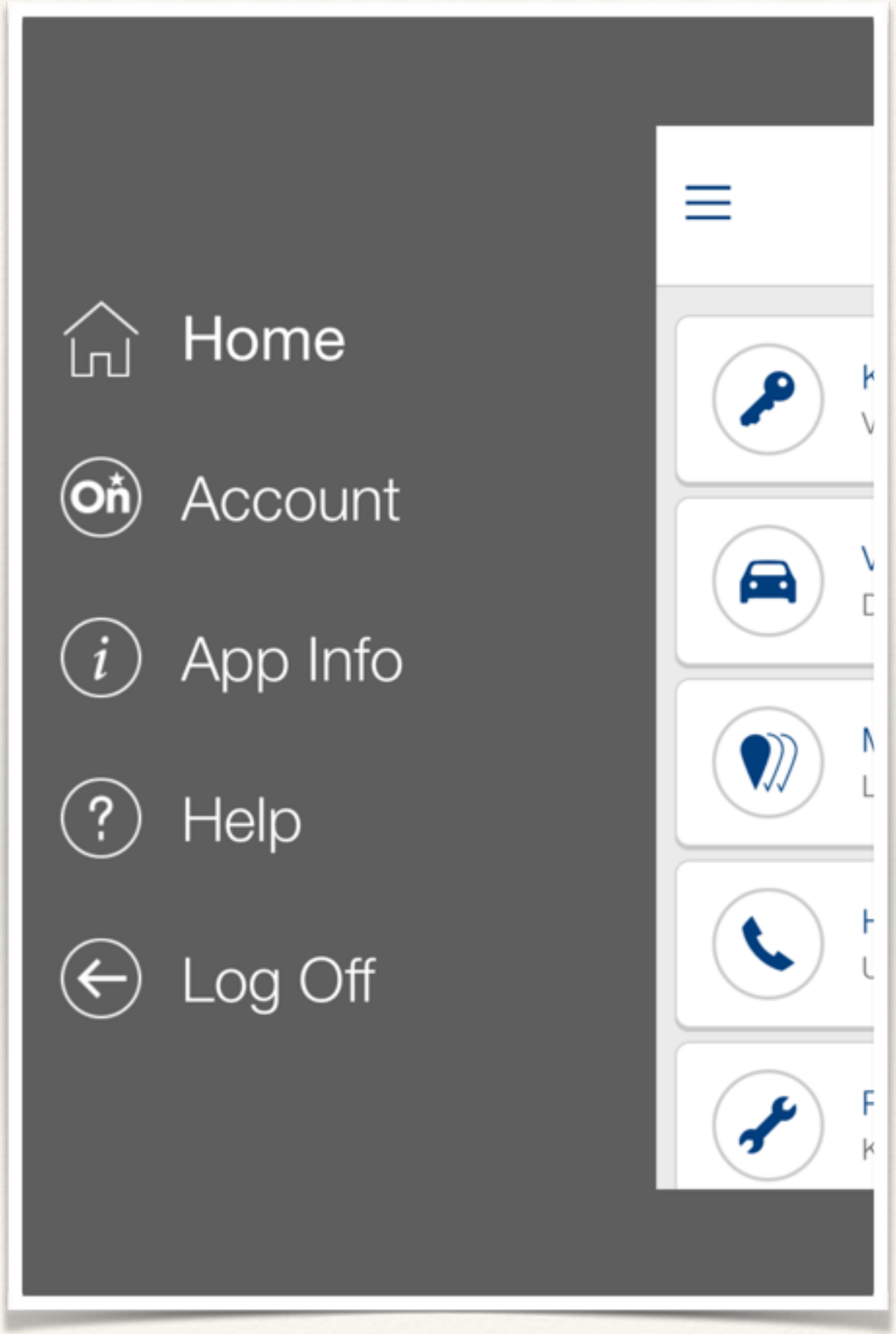
Free delivery in 4 days

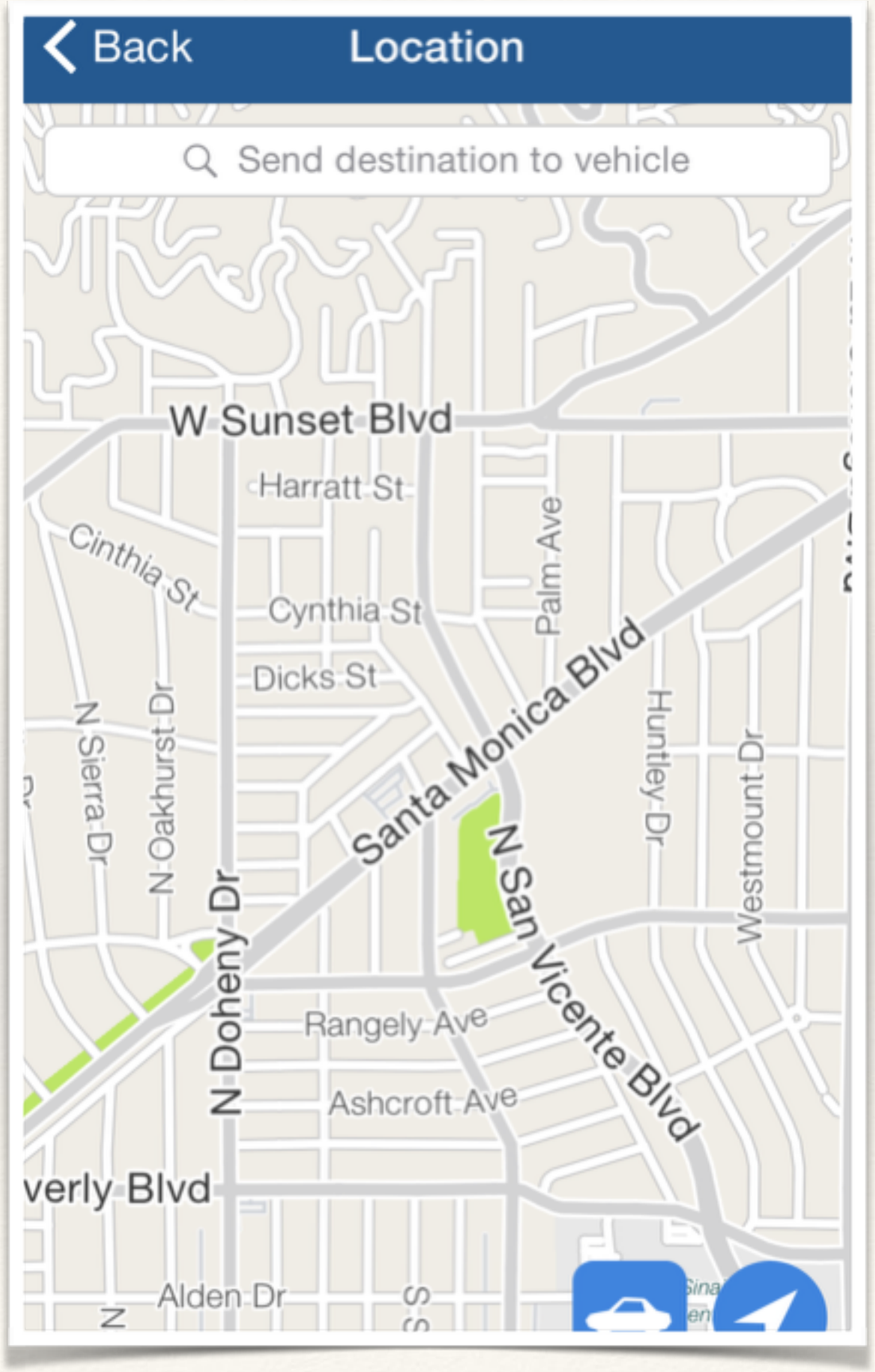
Hassle-fre

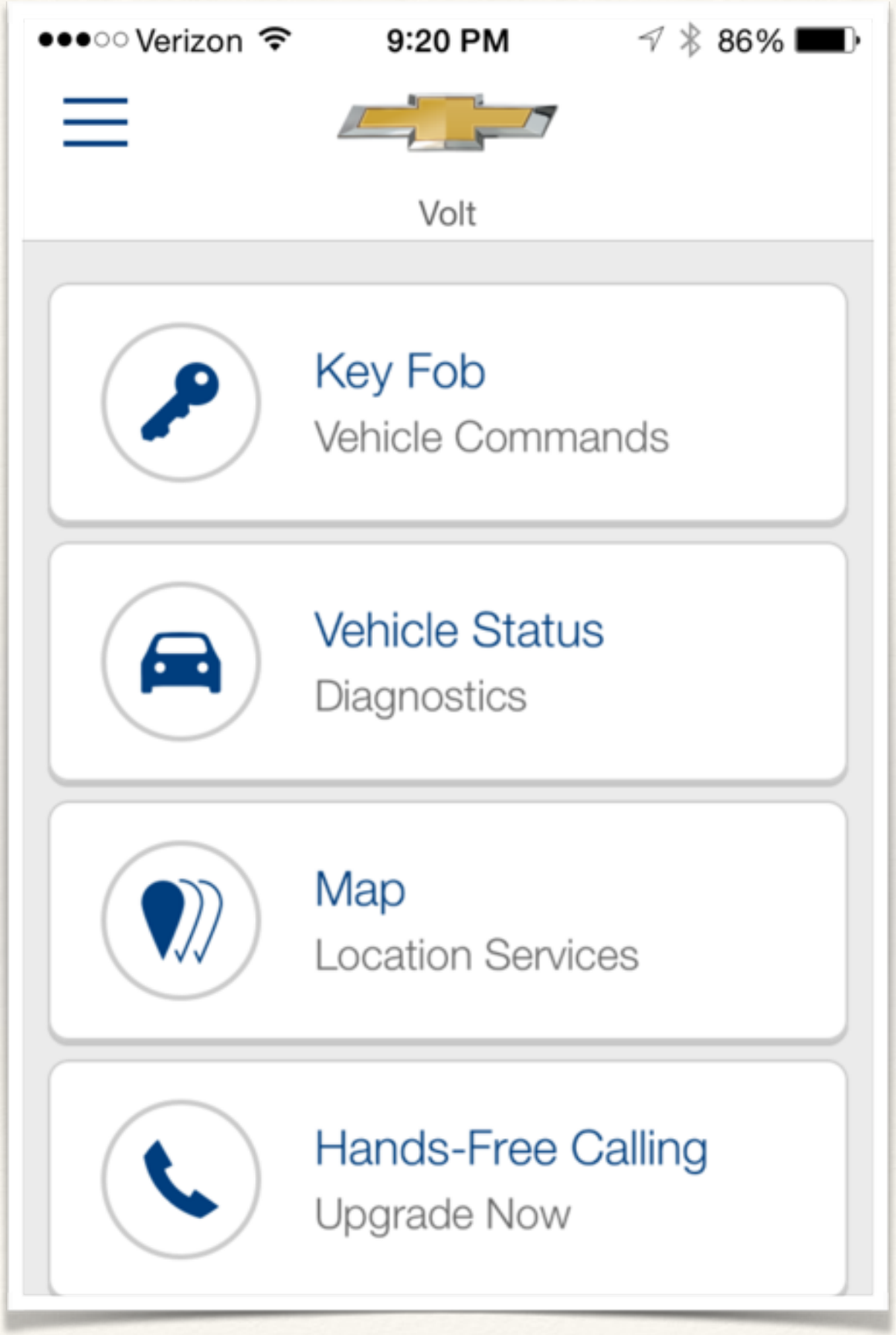
Lessons

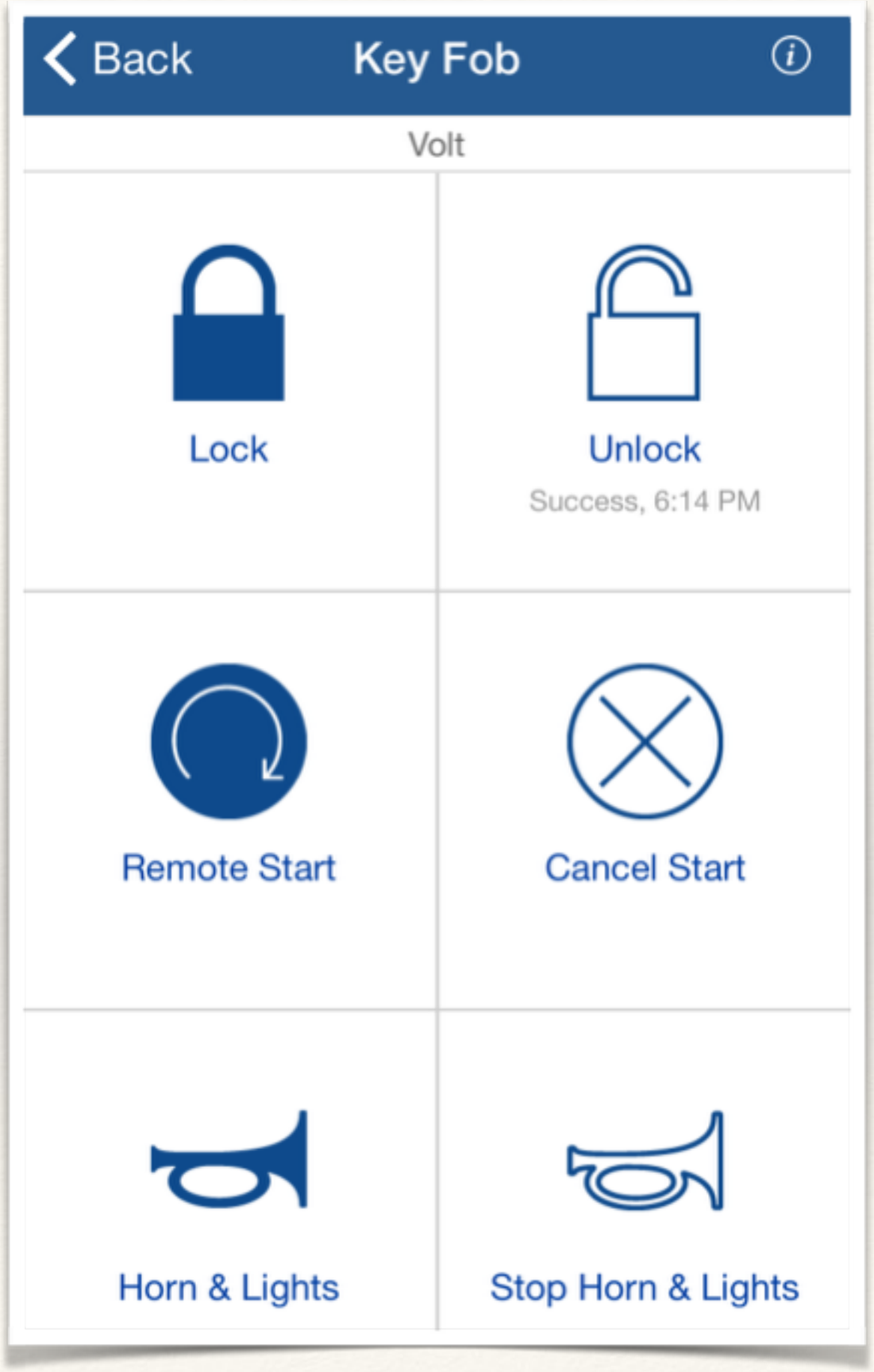
- Don’t use a ridiculously small key space (duh)
- Require a preamble/sync word for beginning of each key
- Use rolling codes…




Home
Account
App Info
Help
Log Off


Back
Location
Send destination to vehicle
W Sunset Blvd
Harratt St
Cinthia St
Cynthia St
Dicks St
Palm Ave
Santa Monica Blvd
N Sierra Dr
N Oakhurst Dr
N Doheny Dr
N San Vicente Blvd
Huntley Dr
Westmount Dr
Rangely Ave
Ashcroft Ave
verly Blvd
Alden Dr


Verizon
9:20 PM
86%
Volt
Key Fob
Vehicle Commands
Vehicle Status
Diagnostics
Map
Location Services
Hands-Free Calling
Upgrade Now


Back
Key Fob
Volt
Lock
Unlock
Success, 6:14 PM
Remote Start
Cancel Start
Horn & Lights
Stop Horn & Lights

```
# https://api.gm.com/api/v1/oauth/token
POST /api/v1/oauth/token HTTP/1.1
Host: api.gm.com
Content-Type: text/plain
Connection: keep-alive
Proxy-Connection: keep-alive
Accept: application/json
User-Agent: RemoteLink/1022 CFNetwork/711.1.16 Darwin/14.0.0
Accept-Language: en
Accept-Encoding: gzip, deflate
Content-Length: 422

eyJ0eXAiOiJKV1MiLCJhbGciOiJIUzI1NiJ9.eyJwYXNzd29yZCI6InRlc3RwYXNzIiwiZGV
2aWNlX2lkIjoiMDdBNTE2NkItNjE4Mi00NTBGLUJCMTQtQzY0MkU5MkZFMkVCIiwic2NvcGU
iOiJwcml2IG1zc28iLCJncmFudF90eXBlIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6InRlc3R
1c2VyIiwidGltZXN0YW1wIjoiMjAxNS0wNy0yNFQyMzox0DoxNy43NzlaIiwiY2xpZW50X2l
kIjoiUkxfaU9TLWk3OF8yMDMiLCJub25jZSI6IjM3Qzg5Q0E4LTM5RUUtNDM2NS1CQjA3LUU
zQzU1REUyNUIyMyJ9.3C0rc8RUuHwQBDylnswoSPDE9QeUfvDZEJjstjXkzko=
```

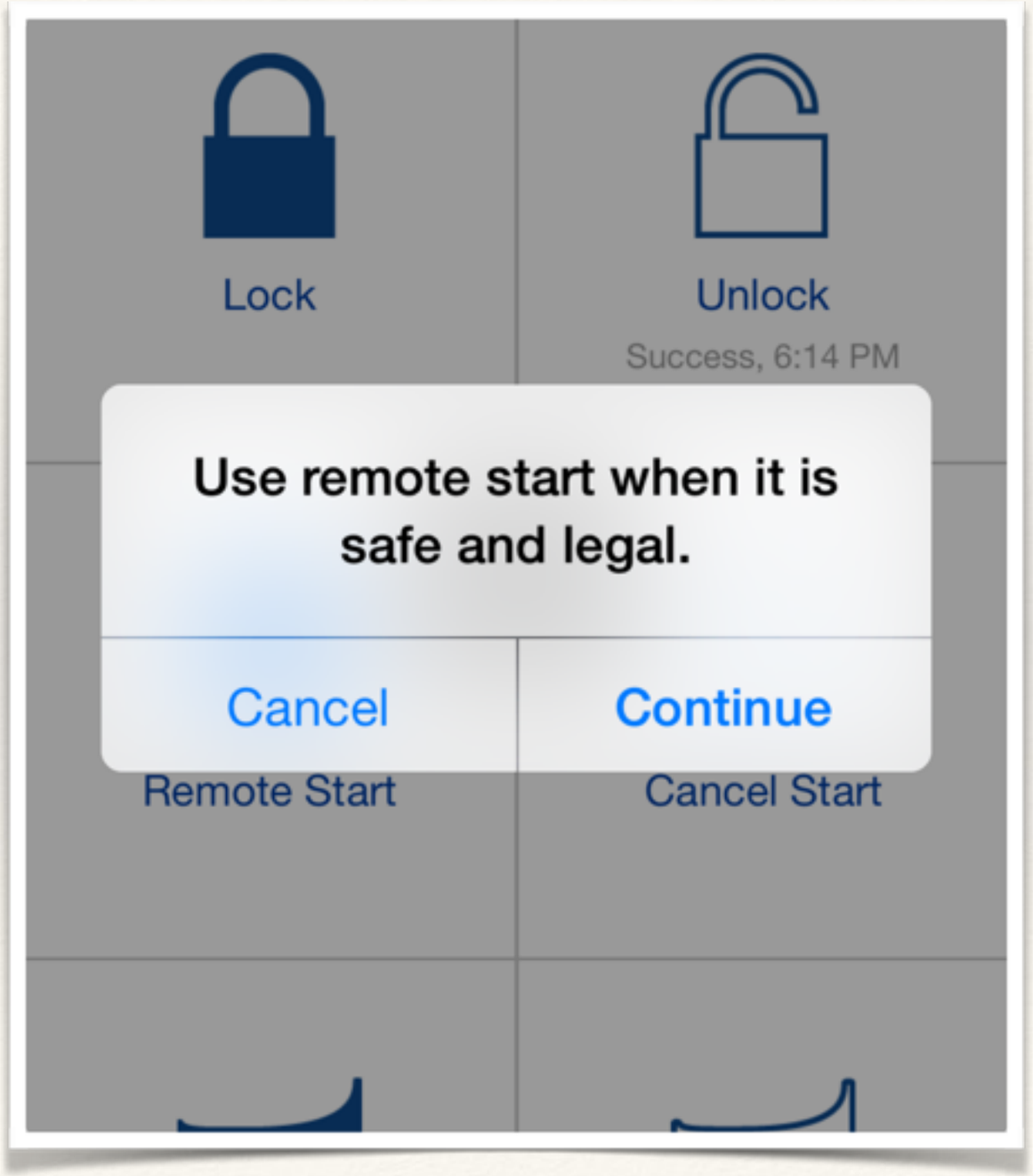
RemoteLink Login

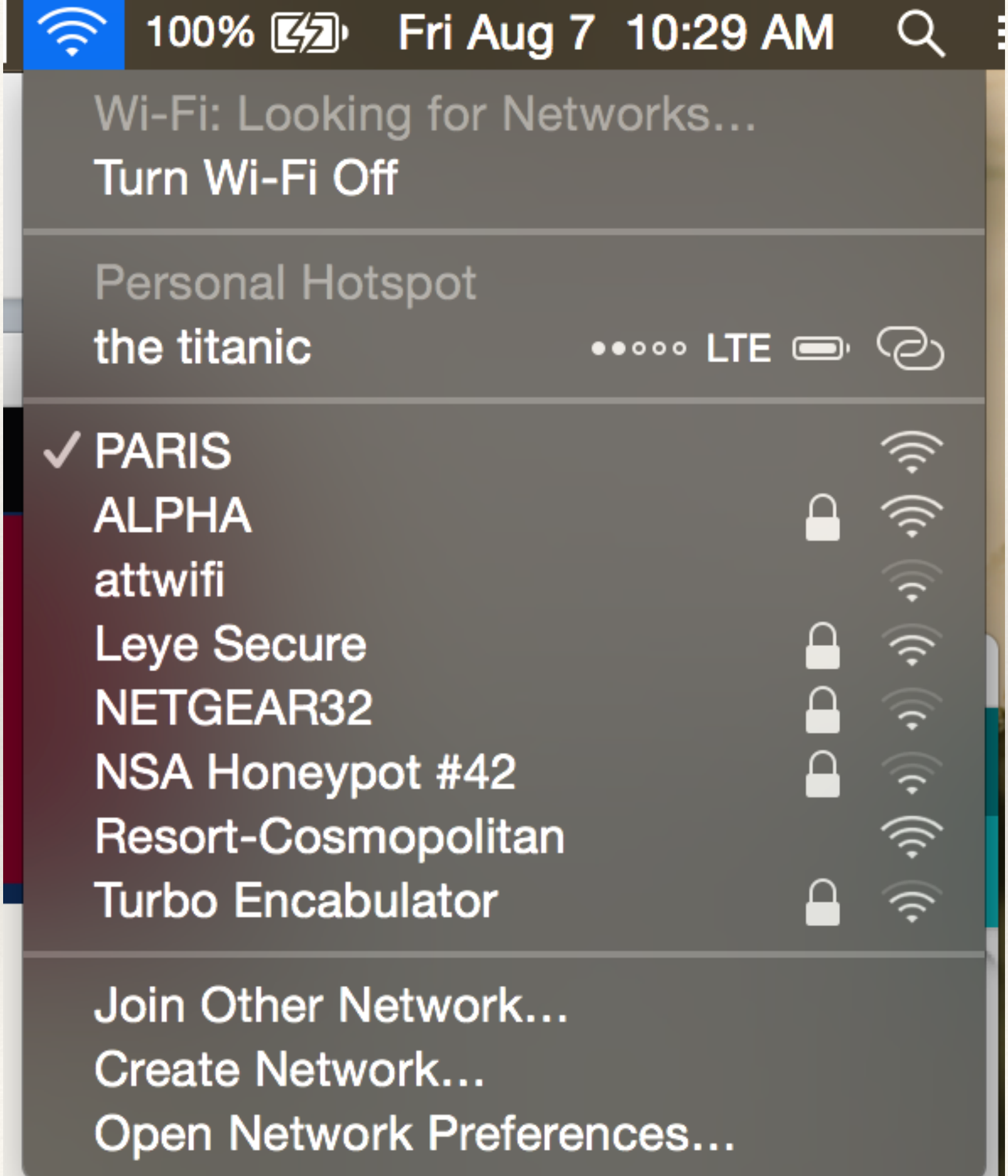
```
{
    "typ": "JWS",
    "alg": "HS256"
} {
    "password": "testpass",
    "device_id": "07A5166B-6182-450F-BB14-C642E92FE2EB",
    "scope": "priv msso",
    "grant_type": "password",
    "username": "testuser",
    "timestamp": "2015-07-24T23:18:17.779Z",
    "client_id": "RL_iOS-i78_203",
    "nonce": "37C89CA8-39EE-4365-BB07-E3C55DE25B23"
}
00000000  dc 2d 2b 73 c4 54 b8 7c  10 04 3c a5 9e cc 28 48
00000010  f0 c4 f5 07 94 7e f0 d9  10 98 ec b6 35
```

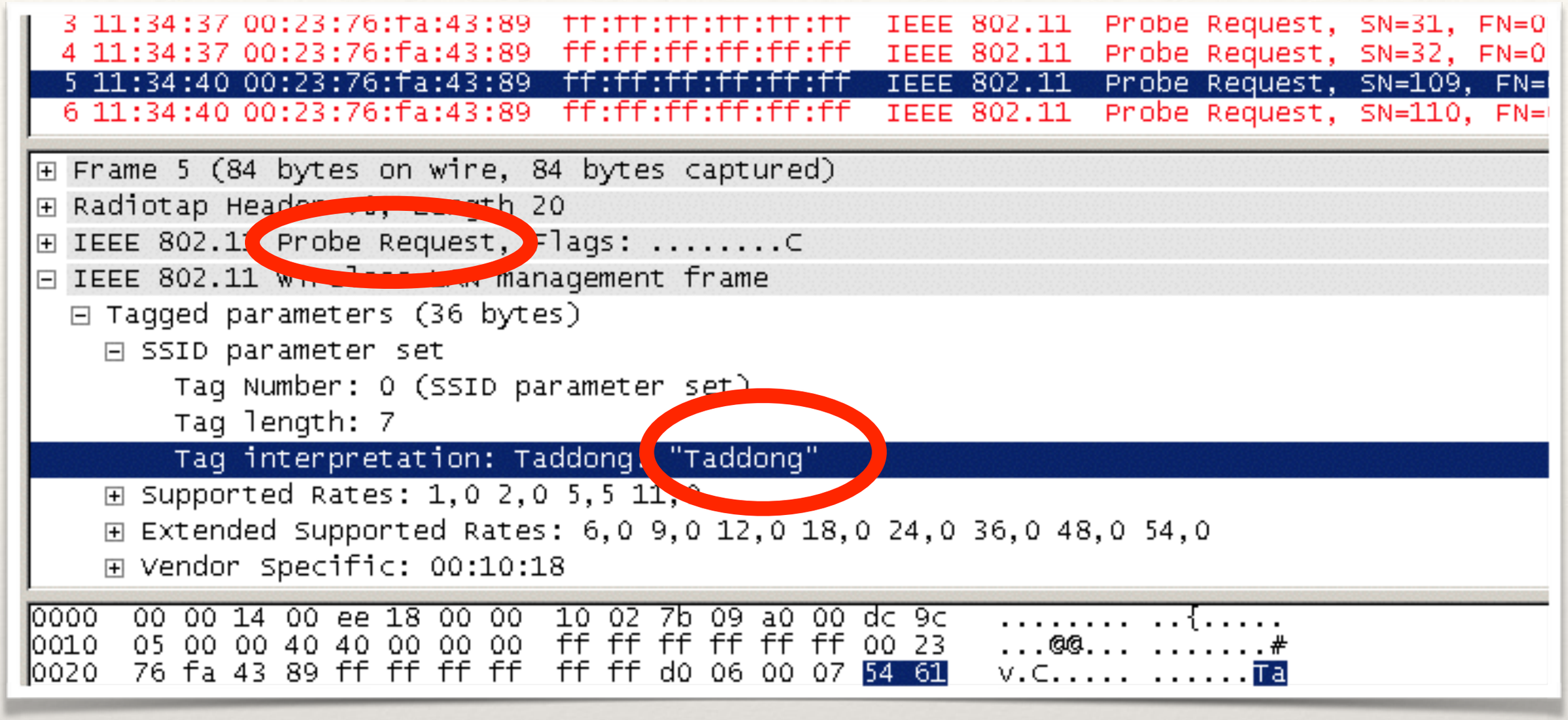
RemoteLink Login (base64 decoded)

SSL MITMA

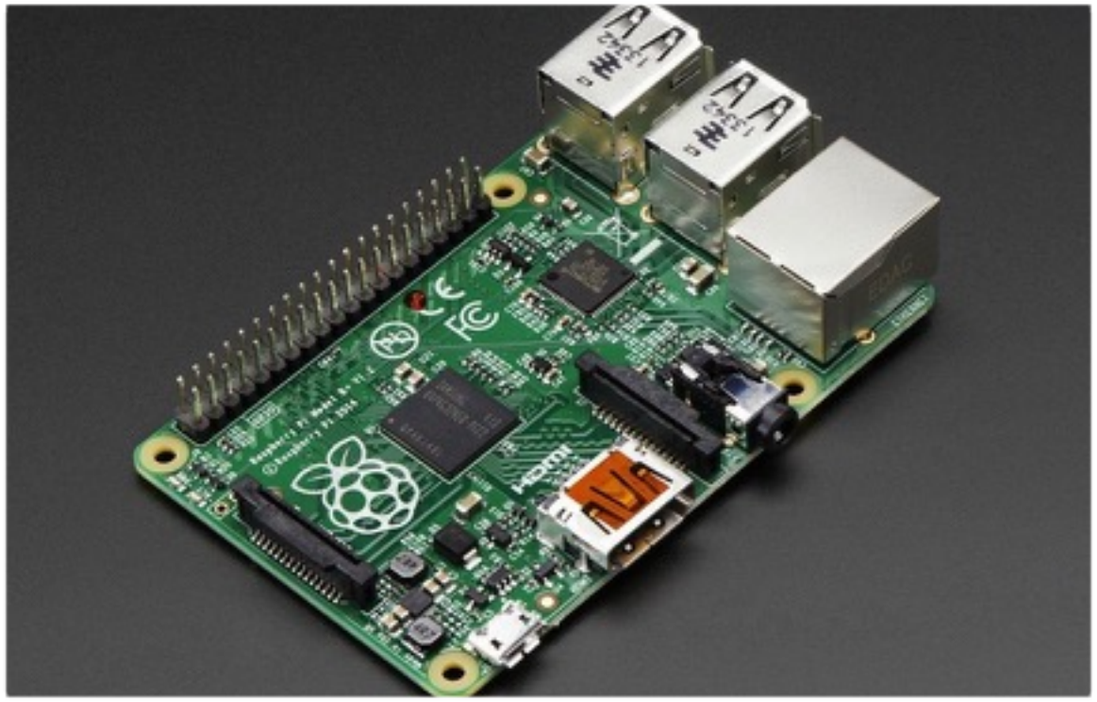
- Raspberry Pi
- FONA GSM board
- mallory (SSL MITMA)
- dns spoofing (api.gm.com)
- iptables
- Alfa AWUS036h
- Edimax Wifi dongle
- pre-paid SIM card




100%
Fri Aug 7 10:29 AM
Wi-Fi: Looking for Networks...
Turn Wi-Fi Off
Personal Hotspot
the titanic
LTE
PARIS
ALPHA
attwifi
Leye Secure
NETGEAR32
NSA Honeypot #42
Resort-Cosmopolitan
Turbo Encabulator
Join Other Network...
Create Network...
Open Network Preferences...



802.11 Probe Requests

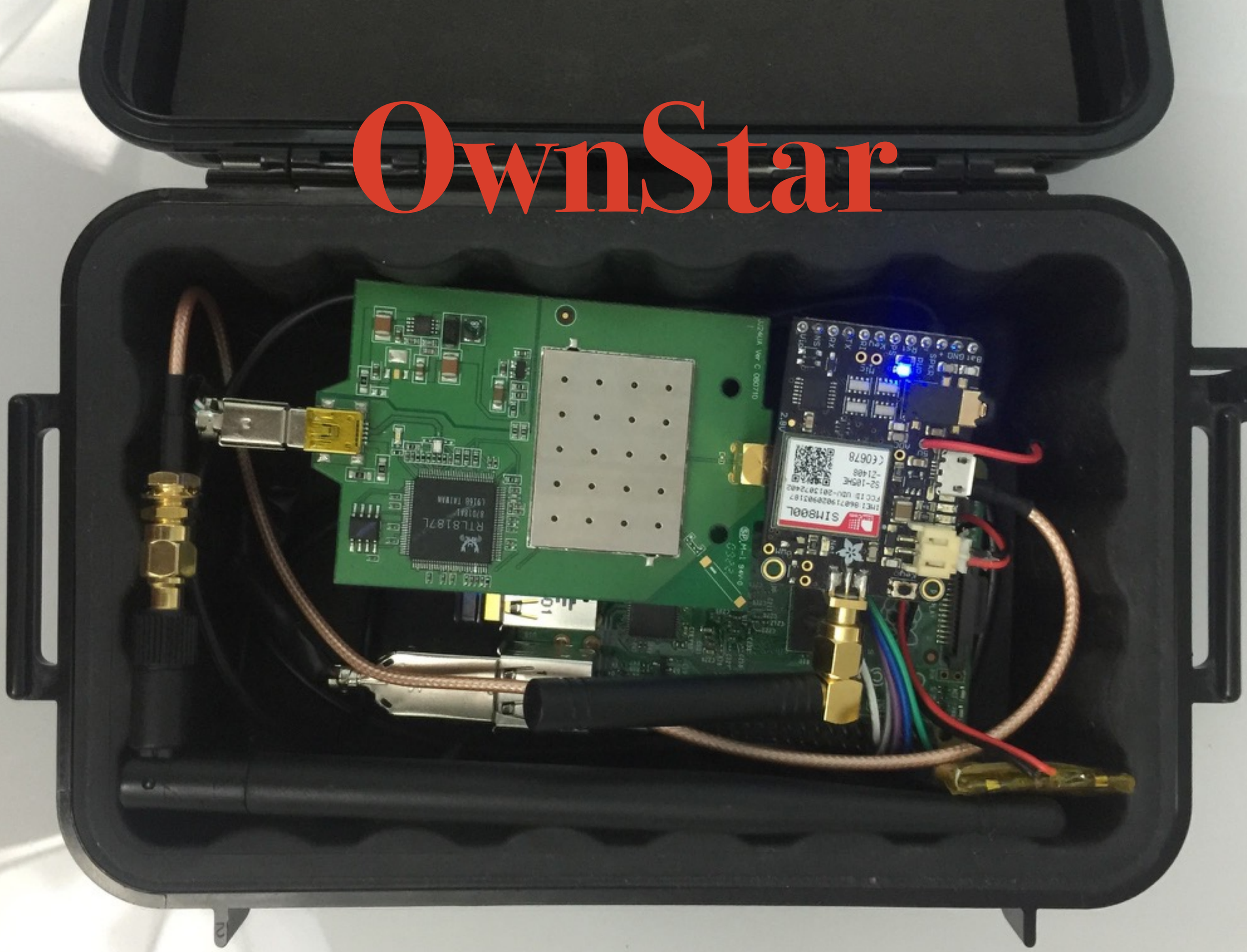



EDIMAX


ALFA
NETWORK


SIM800L

OwnStar



OwnStar

Lessons

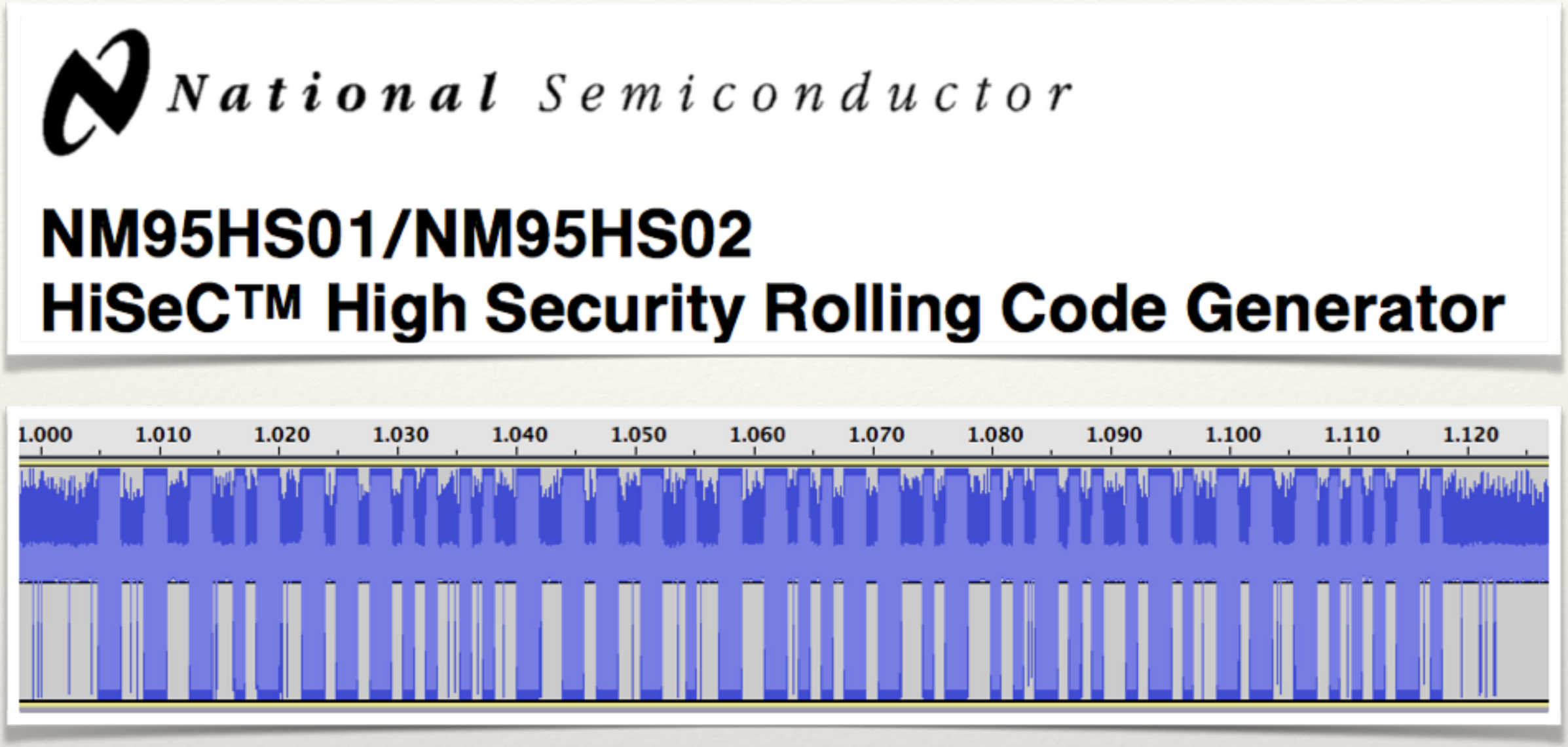
- Validate certificates from CA

Press Release issued on 19 April 2010
Hongkong Post Certification Authority's root certificate included in Mozilla Firefox web browser

- **Better yet,** use certificate pinning and ignore CAs altogether
- Hash password with random salt on authentication (challenge-response)
- **Always assume you're on a hostile network**

BACK TO THE PWN

Key Fobs & Rolling Codes



National Semiconductor "High Security Rolling Code" chip

Thanks Michael Ossmann for helping decipher this!

Rolling Codes

- PRNG in key and car
- Synced seed + counter
- Hit button, key sends code
- Hit button again, key sends next code
- If Eve replays the code, car rejects it because already used
- Should be difficult to predict
- Prevents replay attacks

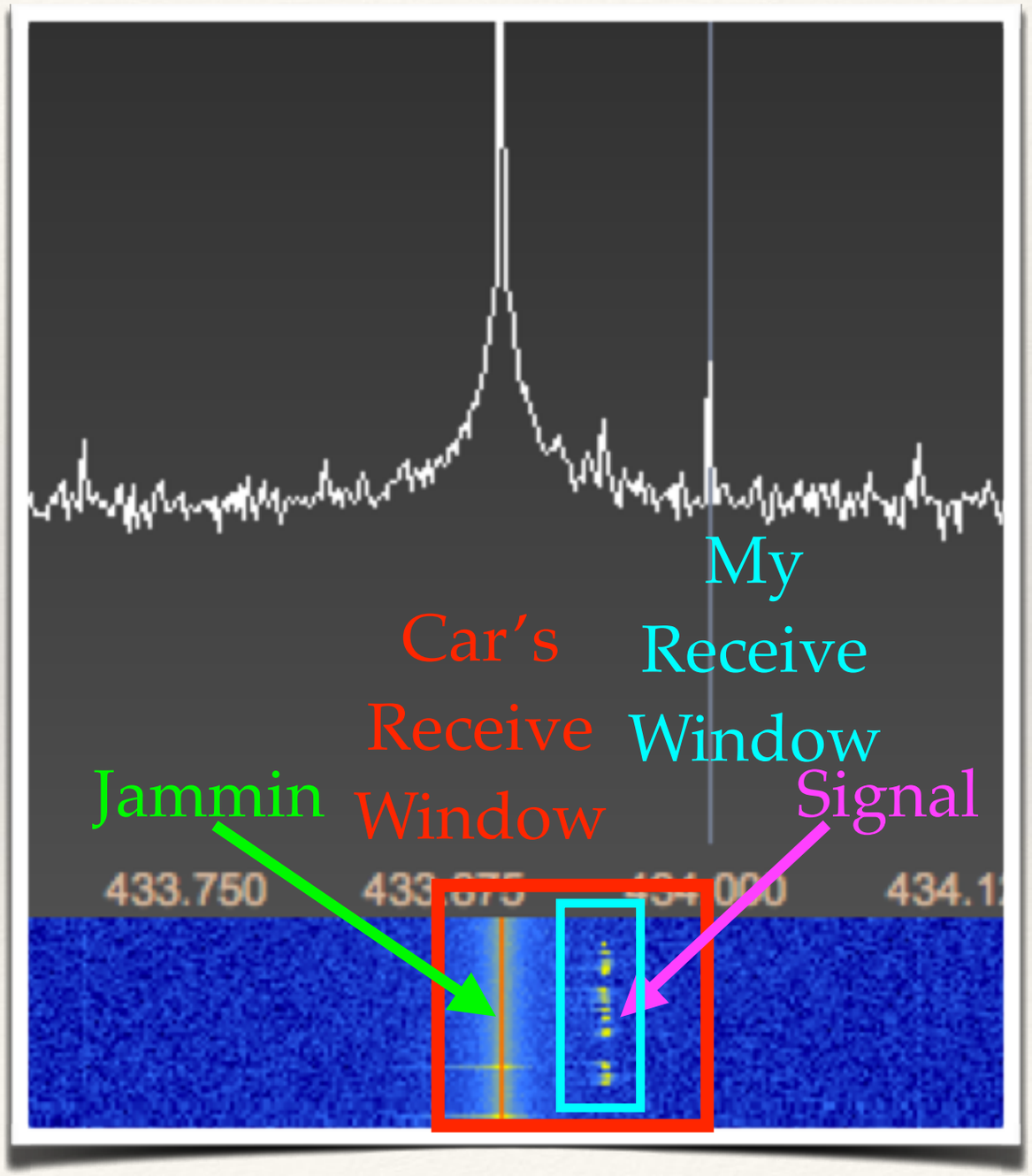
Replaying Rolling Codes

- Capture signal while remote out of range from vehicle/garage
- Replay later
- This is lame since we have to have access to the key, and it has to be far from the car

We're Jammin

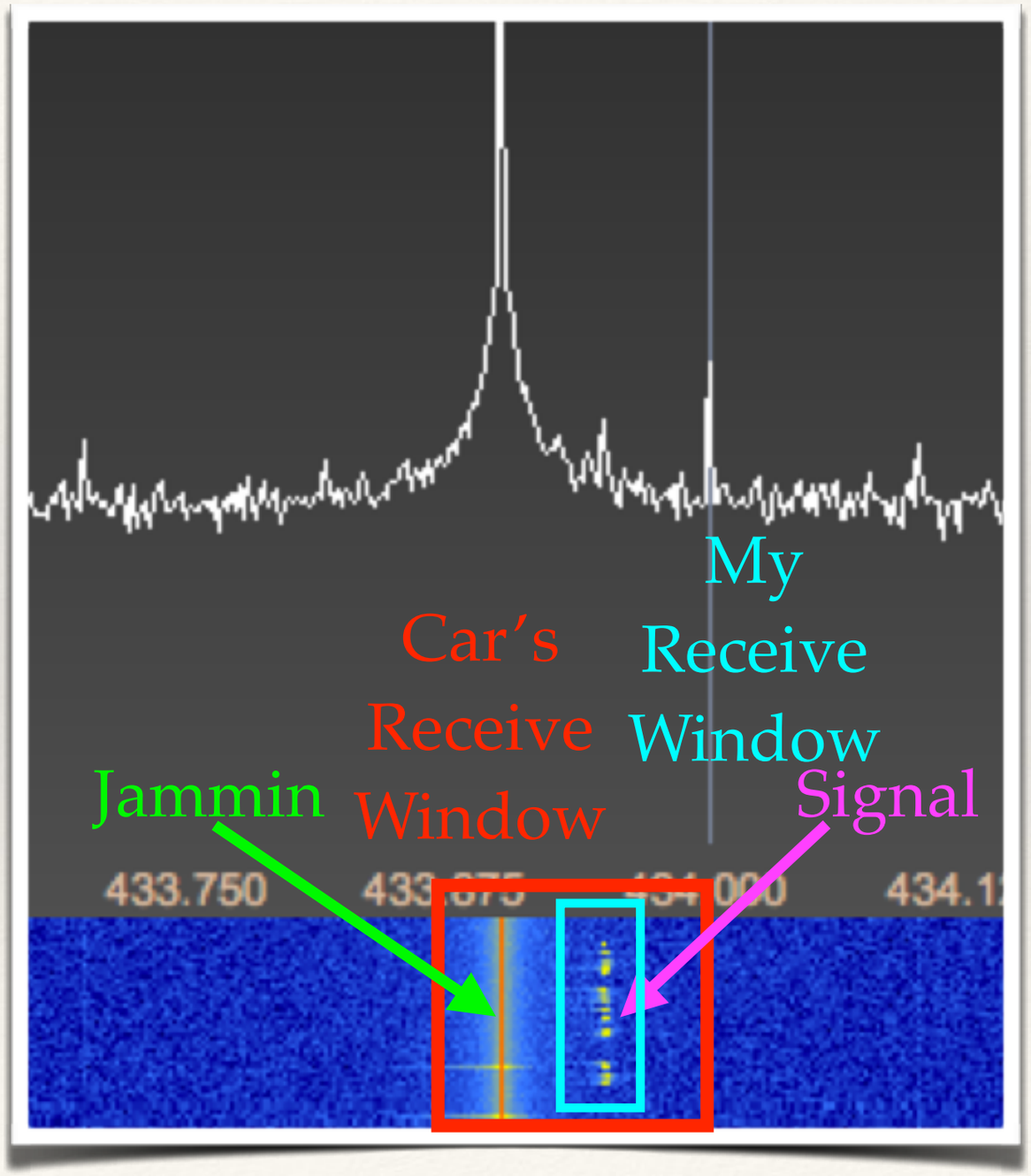
Jam + Listen, Replay

- Jam at slightly deviated frequency
- Receive at frequency with tight receive filter bandwidth to evade jamming
- User presses key but car can't read signal due to jamming
- Once we have code, we stop jamming and can replay
- **But**…once user does get a keypress in, new code invalidates our code!



Jam+Listen(1), Jam+Listen(2), Replay (1)

- Jam at slightly deviated frequency
- Receive at frequency with tight receive filter bandwidth to evade jamming
- User presses key but car can't read signal due to jamming
- User presses key again — you now have **two** rolling codes
- Replay **first** code so user gets into car, we **still have second code**



0/11 bits	0/8 bits	0/20/24 bits	4 bits	24/36 bits	0/8 bits	1 bit
Preamble	**Sync Field**	**Key ID Field**	**Data Field**	**Dynamic Code**	**Parity Field**	**Stop Bit**

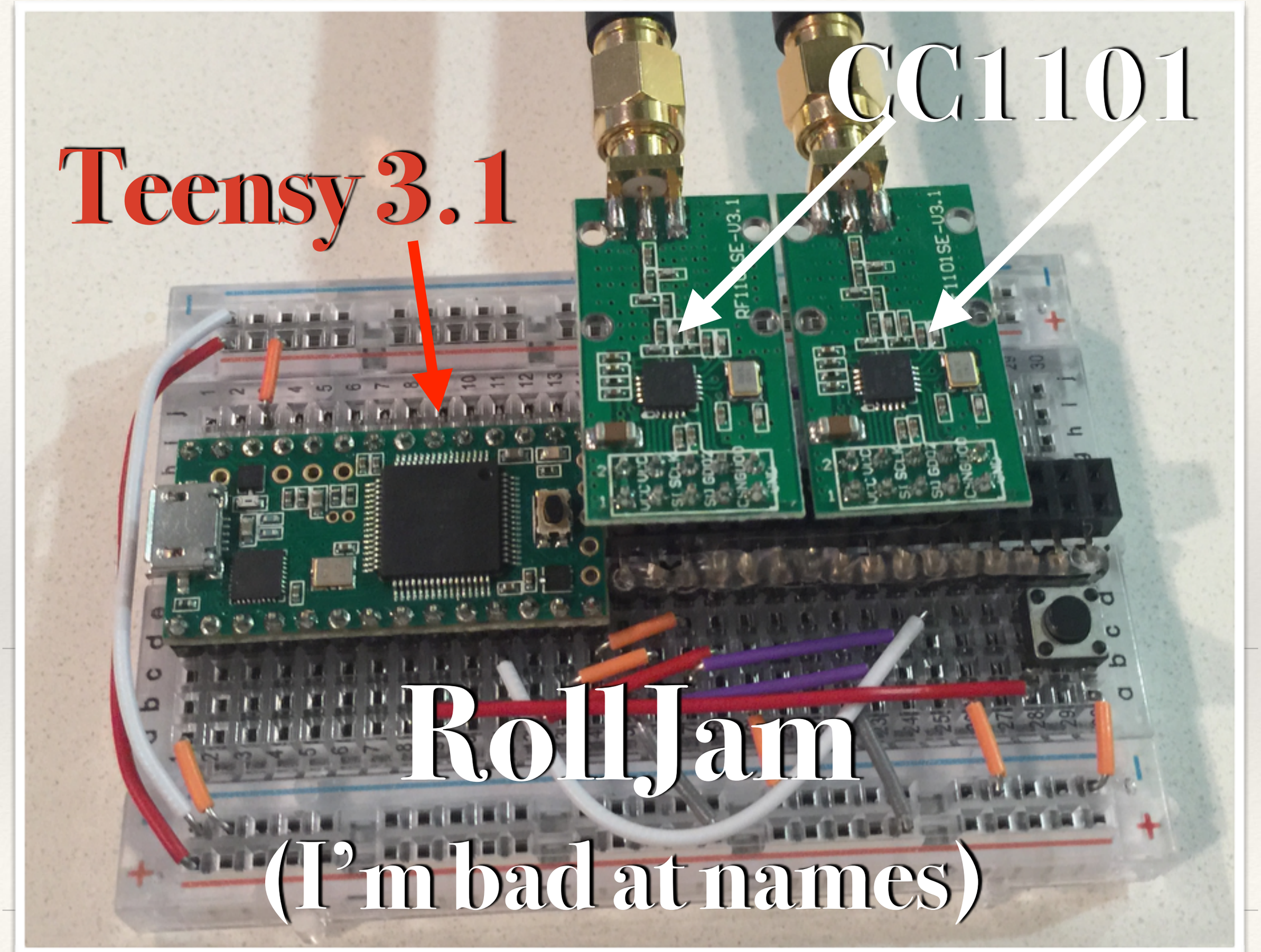
FIGURE 4. Normal Data Frame Configuration

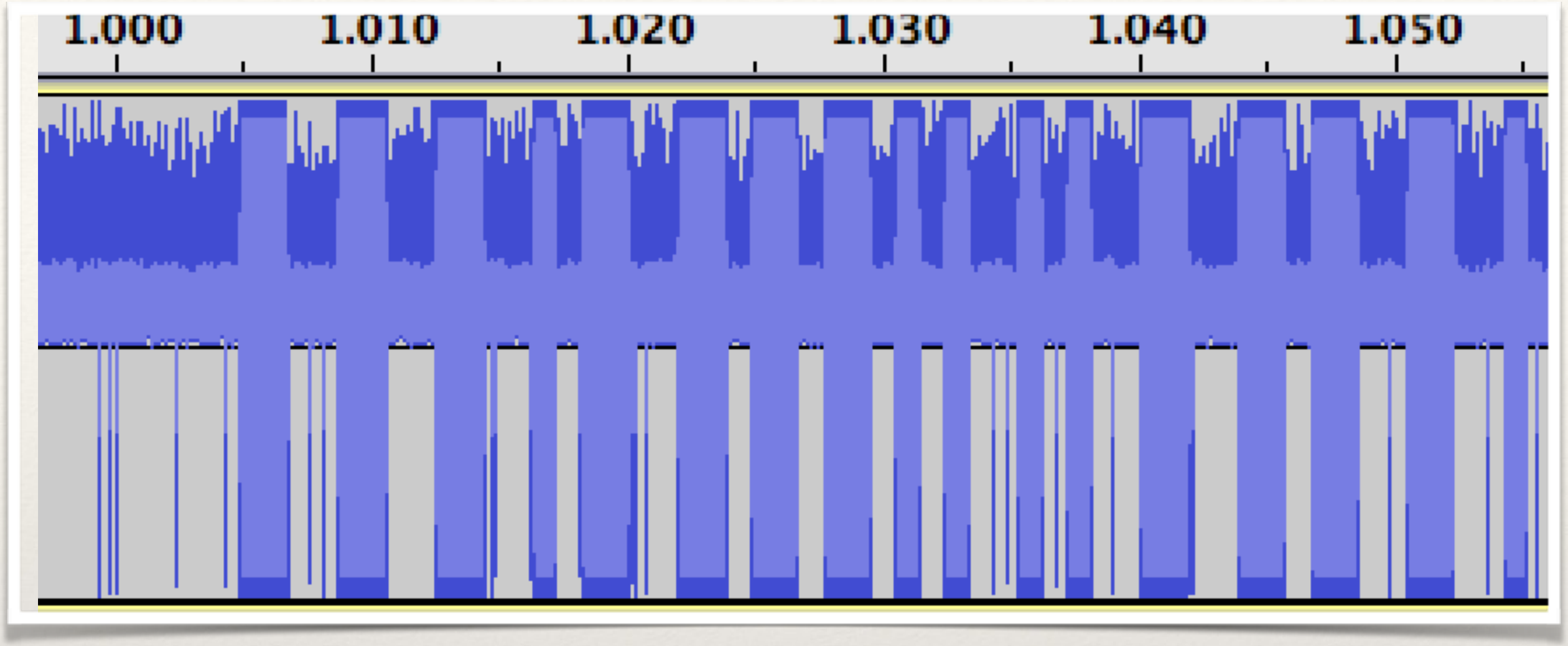
The primary use of the data field is to indicate which key switch has been pressed. Since each key switch input can be associated with a particular application, the decoder can determine which function to initiate.

DYNAMIC CODE FIELD

The dynamic code field is transmitted with every frame, and its length is programmable. If DynSize = 0, a 24-bit field is sent; if DynSize = 1, a 36-bit field is sent. Its function is to provide a secure dynamic code which changes with each new transmission. The field is the result of combining the

Protocol Abuse


Teensy 3.1
CC1101
RollJam
(I'm bad at names)



National Semiconductor "High Security Rolling Code" chip

Thanks Michael Ossmann for helping decipher this!

Lessons

- Encrypt/hash the button/action
- HMAC to prevent bit flipping if encrypted
- Use time-based algorithm (e.g. RSA SecurID **[20 years old]**, "Dual KeeLoq" does this as of 2014)
- OR challenge/response via transceivers instead of one-way communication
- Many vehicles have keys that RX+TX yet the remote unlock signal is still one-way and not timing based

Thank **You**!!!

YOU!
EFF
Michael Ossmann
Travis Goodspeed
Andy Greenberg
atlas of d00m

My mom
Defcon
TI
#hackrf
#ubertooth

Charlie Miller
Chris Valasek
Mike Ryan
Andrew Crocker
Nate Cardozo
Kurt Opsahl

@SamyKamkar **http://samy.pl**

http://samy.pl/youtube