BISHOPFOX

HAMHACKS

BREAKING INTO SOFTWARE DEFINED RADIO

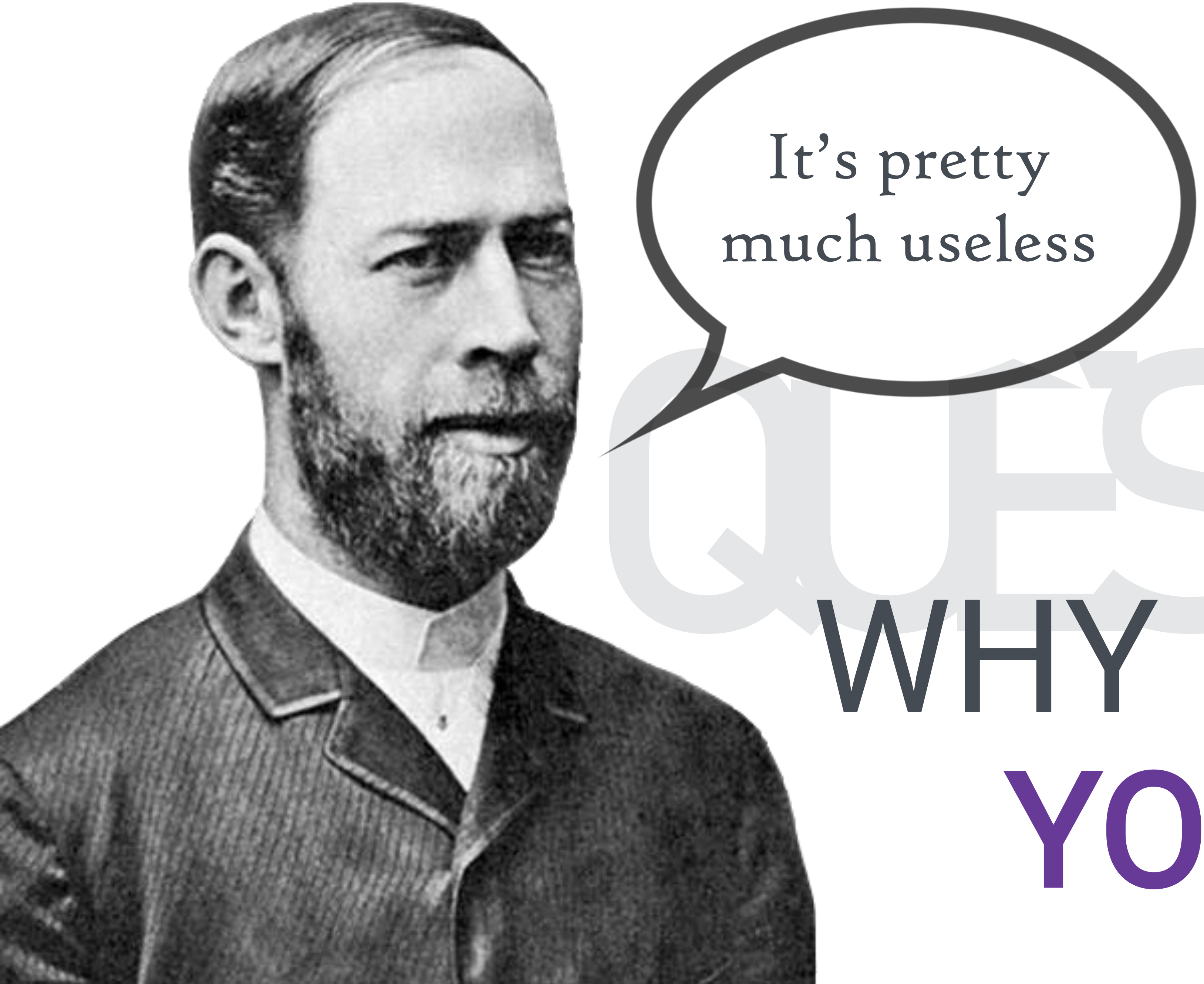
Presented by Kelly Albrink

WHOAMI

Kelly Albrink

- Pentester at Bishop Fox
- Specialize in network, wireless, and hardware security
- Member of Noisebridge Hackerspace in San Francisco
- Loves 3D printing, science fiction, and reading your emails

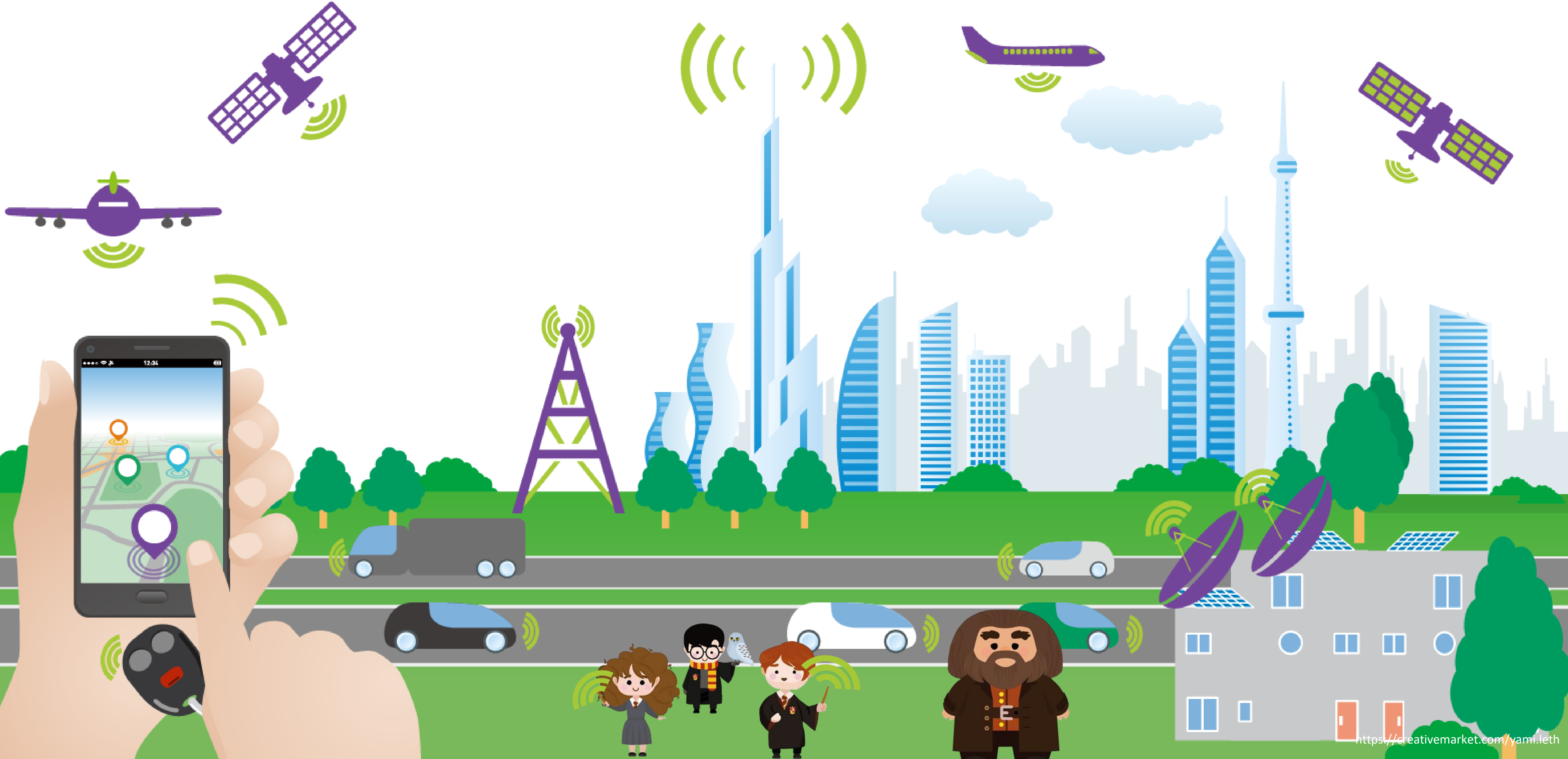
@Justified_Salt



QUESTION

WHY SHOULD YOU CARE?

RF IS MAGIC



https://creativemarket.com/yami.leth

AGENDA

1. Radio basics
2. Software Defined Radio (SDR) Hardware and Software
3. How hackers use SDR

Disclaimer: We're not going to talk specifically or in depth about Ham radio hacking.

BECOMING

A HAM

- You get transmit privileges on amateur bands
- Three levels of ham licenses: Technician, General, Extra
- Each license level allows additional frequencies & privileges
- Contests, fox hunting, DXing, collecting QSL cards
- Communicate with the ISS
- Packet radio, Echolink

QUESTION

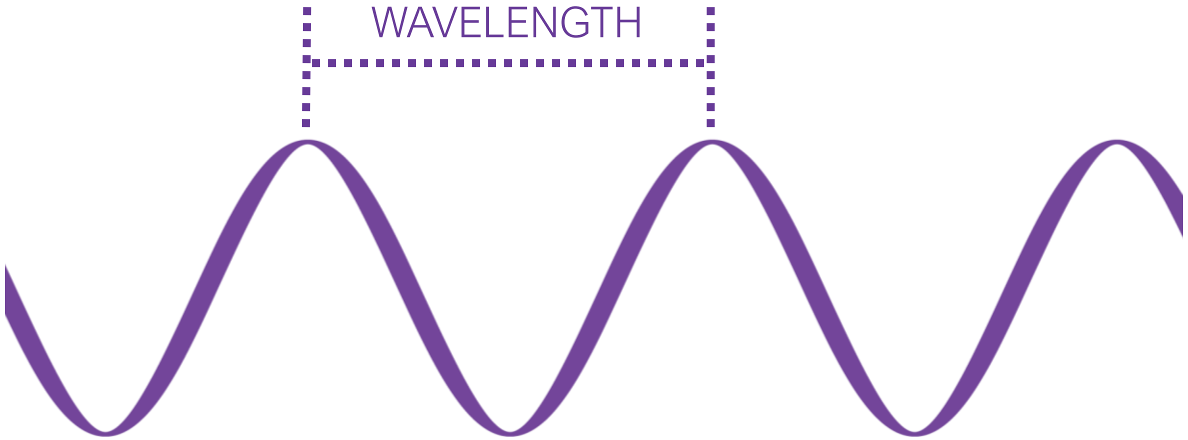
WHAT IS RF?

TERMINOLOGY

Wavelength and Frequency

WAVELENGTH:

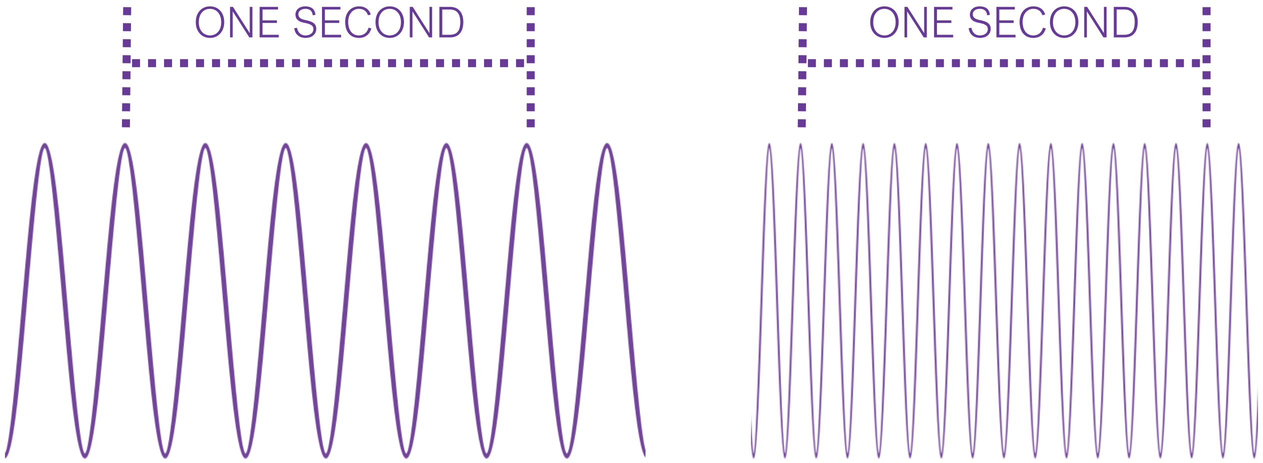
The actual distance between the peaks of 2 waves.



- Long wavelength
- Low frequency
- Low energy

FREQUENCY:

How many waves pass per second.



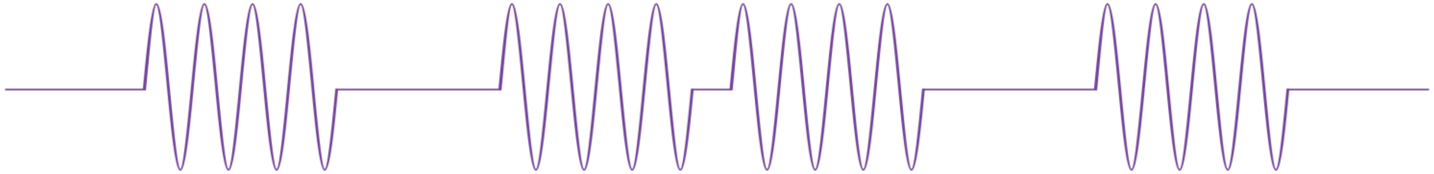
- Short wavelength
- High frequency
- High energy

ANALOG MODULATION

You’re telling me the files are *in* the wave?

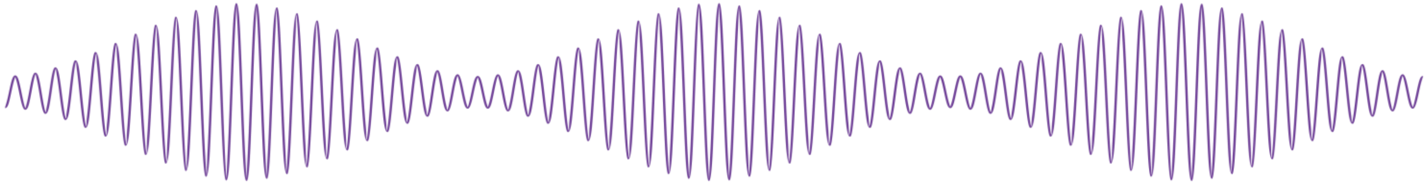
OOK

Pulse Modulation or On Off Keying



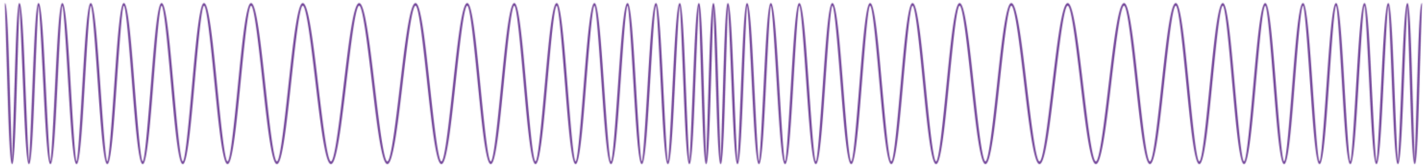
AM

Amplitude Modulation



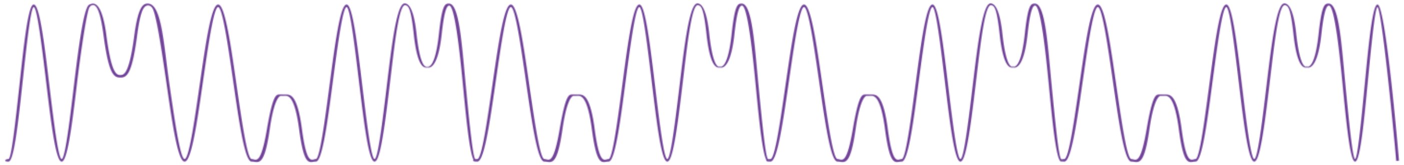
FM

Frequency Modulation



PM

Phase Modulation

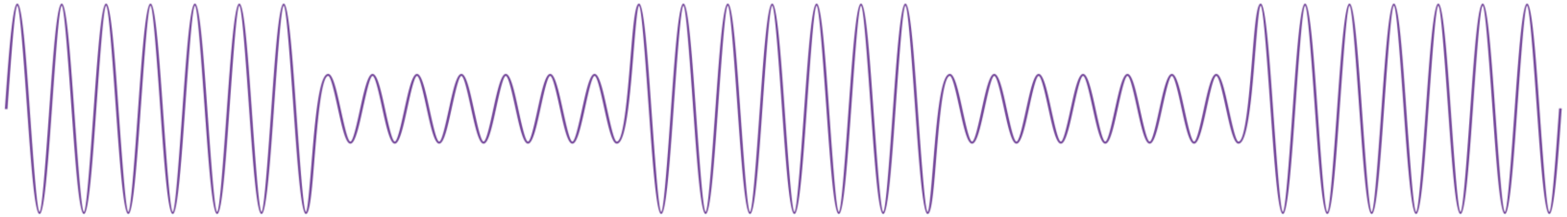


DIGITAL MODULATION

You're telling me the files are *in* the wave?

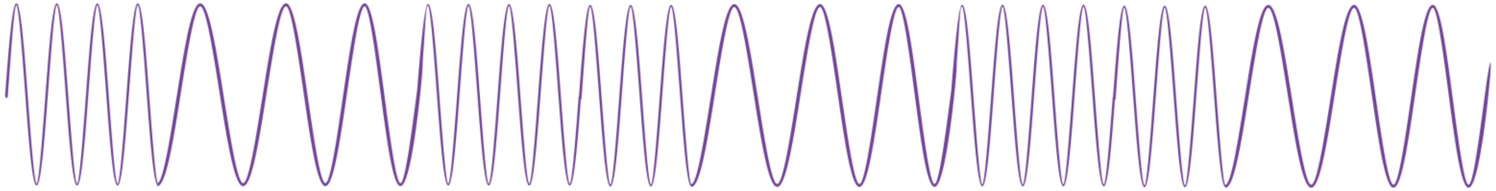
ASK

Amplitude Shift Keying



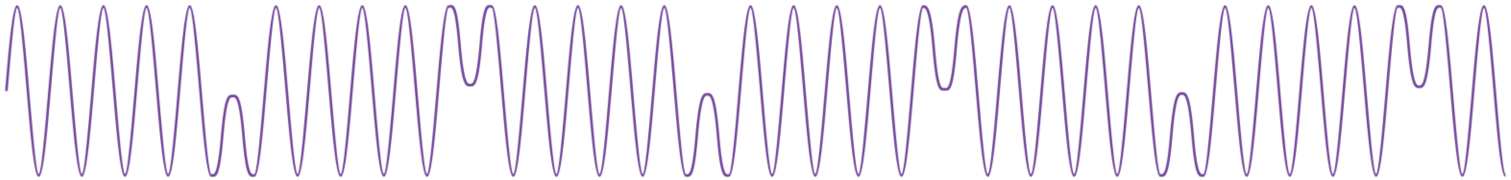
FSK

Frequency Shift Keying

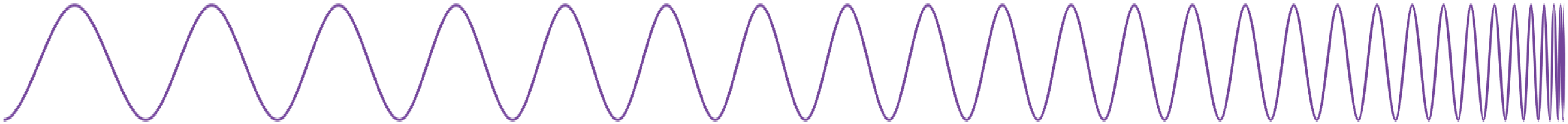


PSK

Phase Shift Keying



RF BANDS

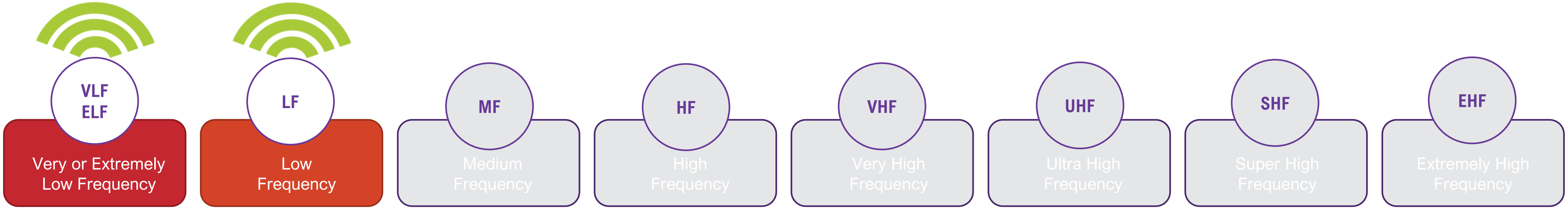


VLF ELF	LF	MF	HF	VHF	UHF	SHF	EHF
Very or Extremely Low Frequency	Low Frequency	Medium Frequency	High Frequency	Very High Frequency	Ultra High Frequency	Super High Frequency	Extremely High Frequency
3-30KHz	30-300KHz	300KHz-3MHz	3MHz-30MHz	30MHz-300MHz	300MHz-3GHz	3GHz-30GHz	30GHz-300GHz

RF BANDS

VLF-ELF-LF

- Mostly government use
- Maritime radio navigation
- Submarines



VLF ELF
Very or Extremely Low Frequency

LF
Low Frequency

MF
Medium Frequency

HF
High Frequency

VHF
Very High Frequency

UHF
Ultra High Frequency

SHF
Super High Frequency

EHF
Extremely High Frequency

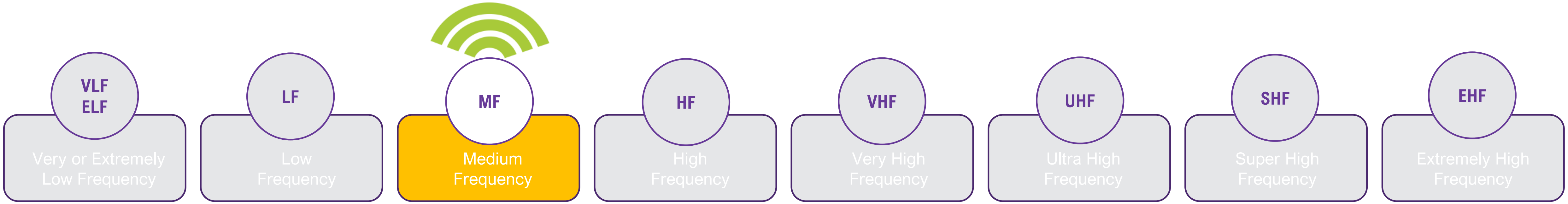
3-30 KHz

30-300KHz

RF BANDS

MF

- AM Radio
- Aviation Radio



VLF
ELF
Very or Extremely Low Frequency

LF
Low Frequency

MF
Medium Frequency

HF
High Frequency

VHF
Very High Frequency

UHF
Ultra High Frequency

SHF
Super High Frequency

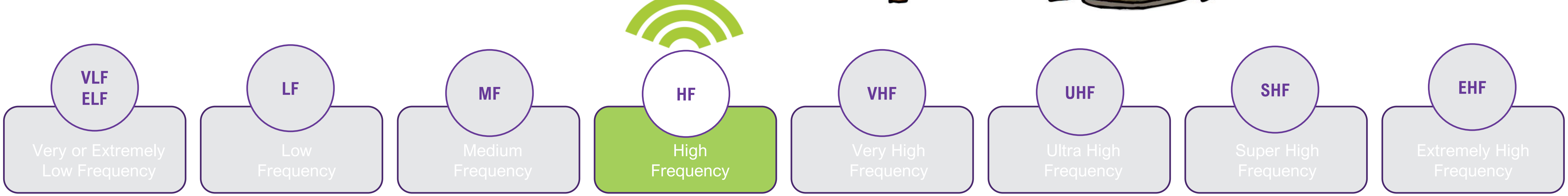
EHF
Extremely High Frequency

300KHz-3MHz

RF BANDS

HF

- Amateur Radio
- “short wave”
- NFC/RFID
- Weather Broadcast



VLF ELF
Very or Extremely Low Frequency

LF
Low Frequency

MF
Medium Frequency

HF
High Frequency

VHF
Very High Frequency

UHF
Ultra High Frequency

SHF
Super High Frequency

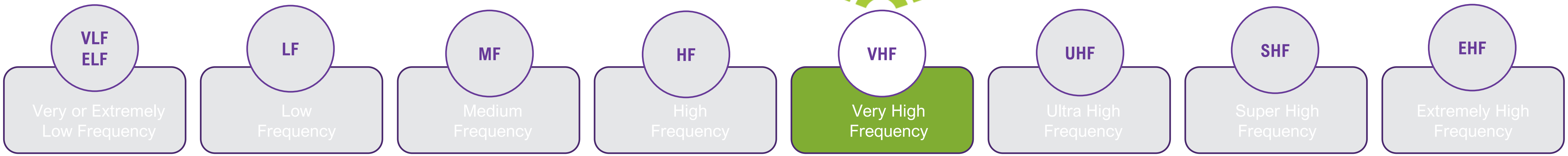
EHF
Extremely High Frequency

3MHz-30MHz

RF BANDS

VHF

- FM Radio
- VHF Television


VLF ELF
Very or Extremely Low Frequency

LF
Low Frequency

MF
Medium Frequency

HF
High Frequency

VHF
Very High Frequency

UHF
Ultra High Frequency

SHF
Super High Frequency

EHF
Extremely High Frequency

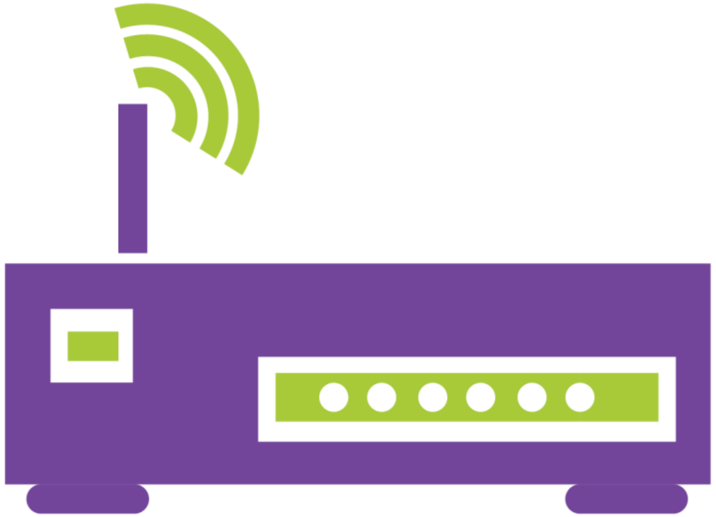
30MHz-300MHz

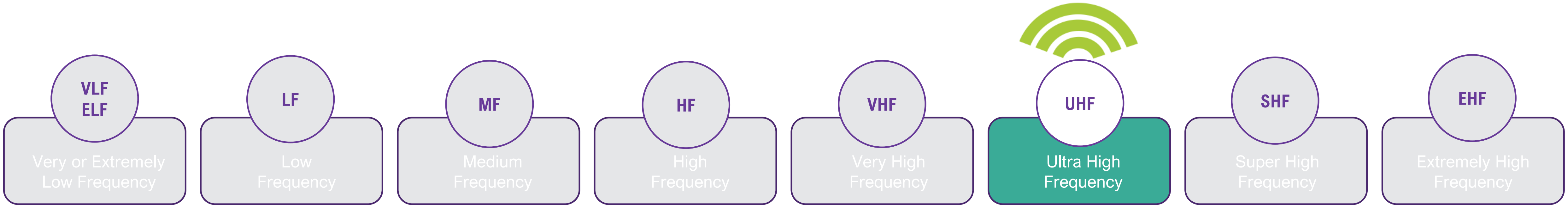
RF BANDS

UHF

Most Modern RF Tech:

- Wi-Fi
- UHF television
- Microwaves
- GPS
- Mobile/4G
- Car keys
- RC toys





VLF ELF — Very or Extremely Low Frequency

LF — Low Frequency

MF — Medium Frequency

HF — High Frequency

VHF — Very High Frequency

UHF — Ultra High Frequency

SHF — Super High Frequency

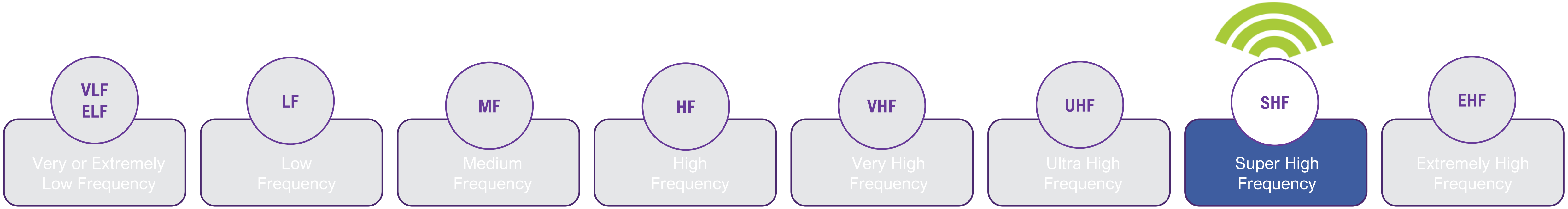
EHF — Extremely High Frequency

300MHz-3GHz

RF BANDS

SHF

- Wi-Fi
- Satellite Communications



VLF
ELF
Very or Extremely Low Frequency

LF
Low Frequency

MF
Medium Frequency

HF
High Frequency

VHF
Very High Frequency

UHF
Ultra High Frequency

SHF
Super High Frequency

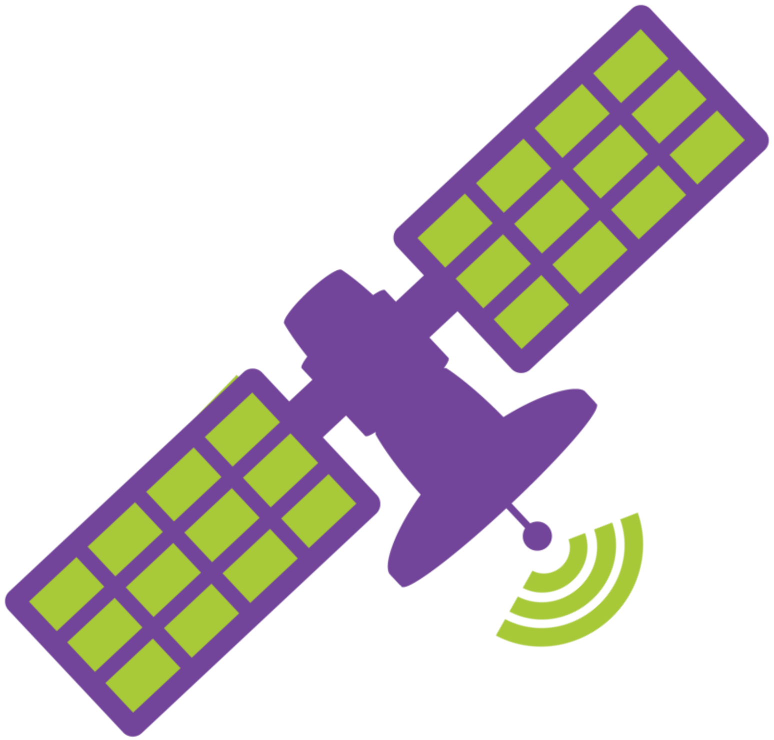
EHF
Extremely High Frequency

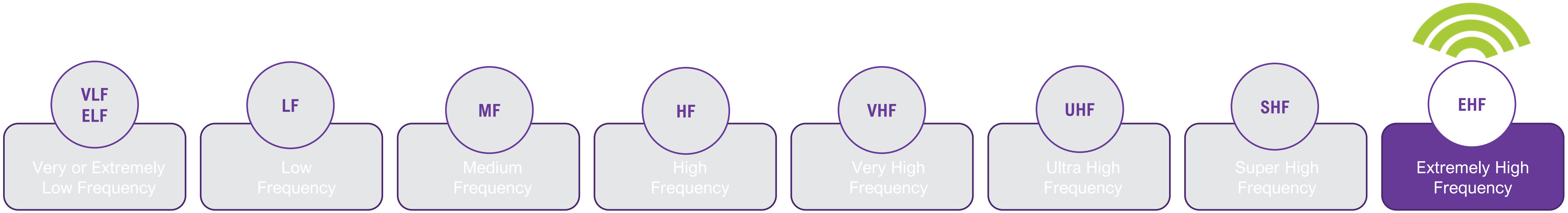
3GHz-30GHz

RF BANDS

EHF

- Radio Astronomy
- More Satellites





VLF ELF

Very or Extremely Low Frequency

LF

Low Frequency

MF

Medium Frequency

HF

High Frequency

VHF

Very High Frequency

UHF

Ultra High Frequency

SHF

Super High Frequency

EHF

Extremely High Frequency

30GHz-300GHz

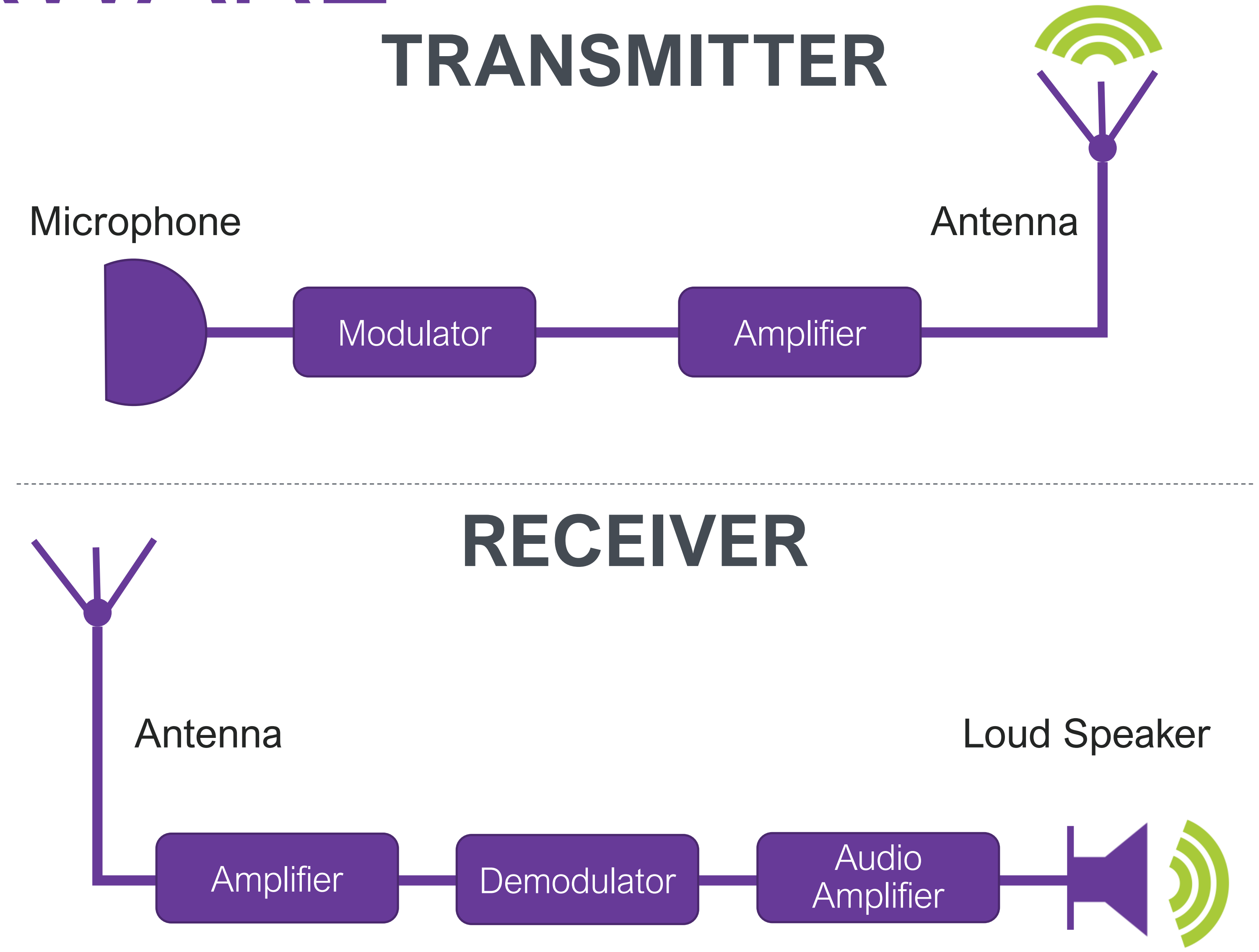
QUESTION

SO, WHAT IS SOFTWARE DEFINED RADIO?

RADIO HARWARE

COMPONENTS:

- Antenna
- Transmitter
- Receiver
- Amplifiers
- Filters
- Modulators/Demodulators



TRANSMITTER

Microphone

Modulator

Amplifier

Antenna

RECEIVER

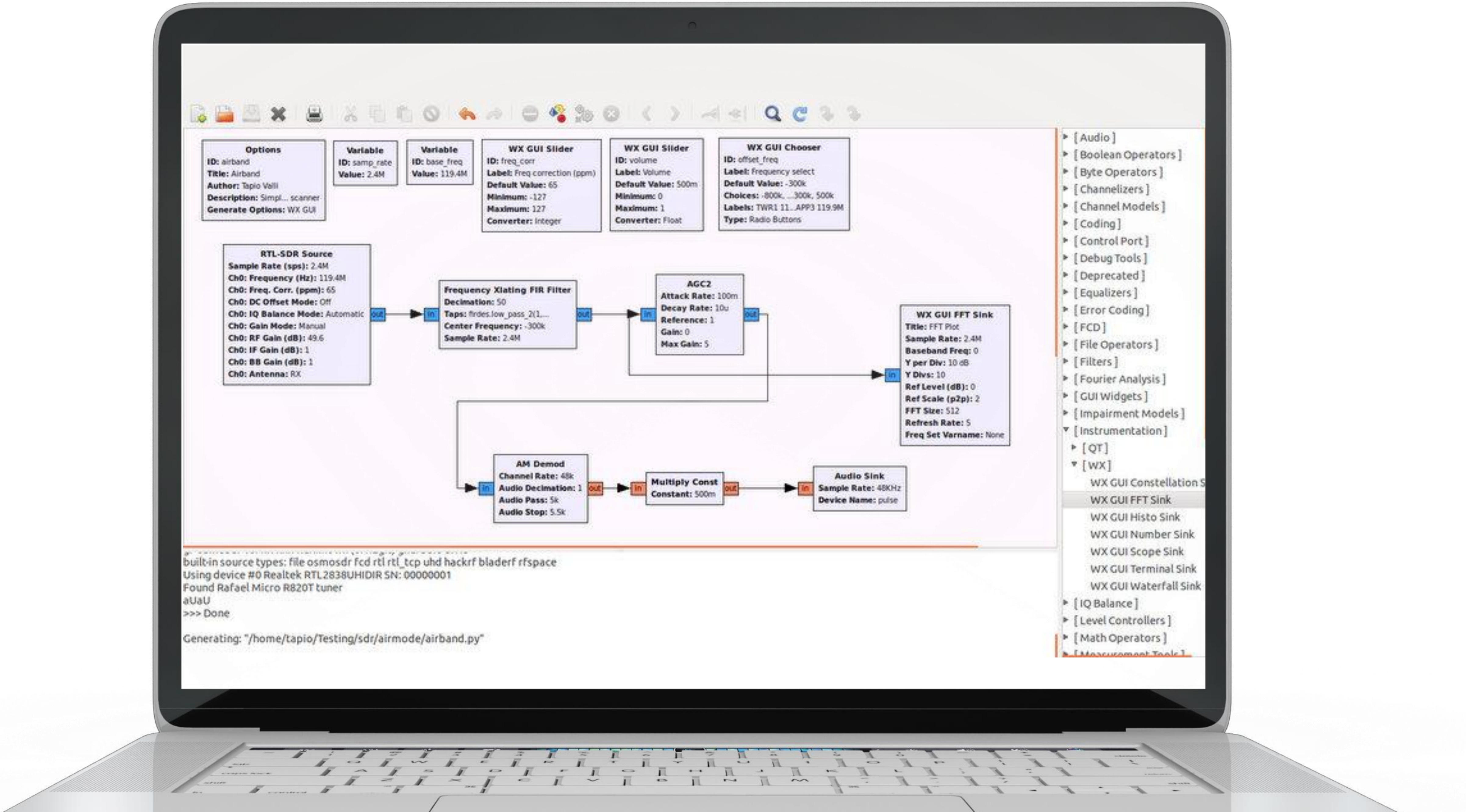
Antenna

Amplifier

Demodulator

Audio Amplifier

Loud Speaker



Options
ID: airband
Title: Airband
Author: Tapio Valli
Description: Simpl... scanner
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 2.4M

Variable
ID: base_freq
Value: 119.4M

WX GUI Slider
ID: freq_corr
Label: Freq correction (ppm)
Default Value: 65
Minimum: -127
Maximum: 127
Converter: Integer

WX GUI Slider
ID: volume
Label: Volume
Default Value: 500m
Minimum: 0
Maximum: 1
Converter: Float

WX GUI Chooser
ID: offset_freq
Label: Frequency select
Default Value: -300k
Choices: -800k, ...300k, 500k
Labels: TWR1 11...APP3 119.9M
Type: Radio Buttons

RTL-SDR Source
Sample Rate (sps): 2.4M
Ch0: Frequency (Hz): 119.4M
Ch0: Freq. Corr. (ppm): 65
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Automatic
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 49.6
Ch0: IF Gain (dB): 1
Ch0: BB Gain (dB): 1
Ch0: Antenna: RX

Frequency Xlating FIR Filter
Decimation: 50
Taps: firdes.low_pass_2(1,...
Center Frequency: -300k
Sample Rate: 2.4M

AGC2
Attack Rate: 100m
Decay Rate: 10u
Reference: 1
Gain: 0
Max Gain: 5

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 2.4M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 512
Refresh Rate: 5
Freq Set Varname: None

AM Demod
Channel Rate: 48k
Audio Decimation: 1
Audio Pass: 5k
Audio Stop: 5.5k

Multiply Const
Constant: 500m

Audio Sink
Sample Rate: 48KHz
Device Name: pulse

```
built-in source types: file osmosdr fcd rtl rtl_tcp uhd hackrf bladerf rfspace
Using device #0 Realtek RTL2838UHIDIR SN: 00000001
Found Rafael Micro R820T tuner
aUaU
>>> Done

Generating: "/home/tapio/Testing/sdr/airmode/airband.py"
```

REQUIRED HARDWARE

CHOOSING AN SDR

TUNER RANGE

The range of frequencies the radio can see

TRANSMIT CAPABILITY

Some platforms are receive only

SAMPLE RATE

Limits the max observable bandwidth at one time

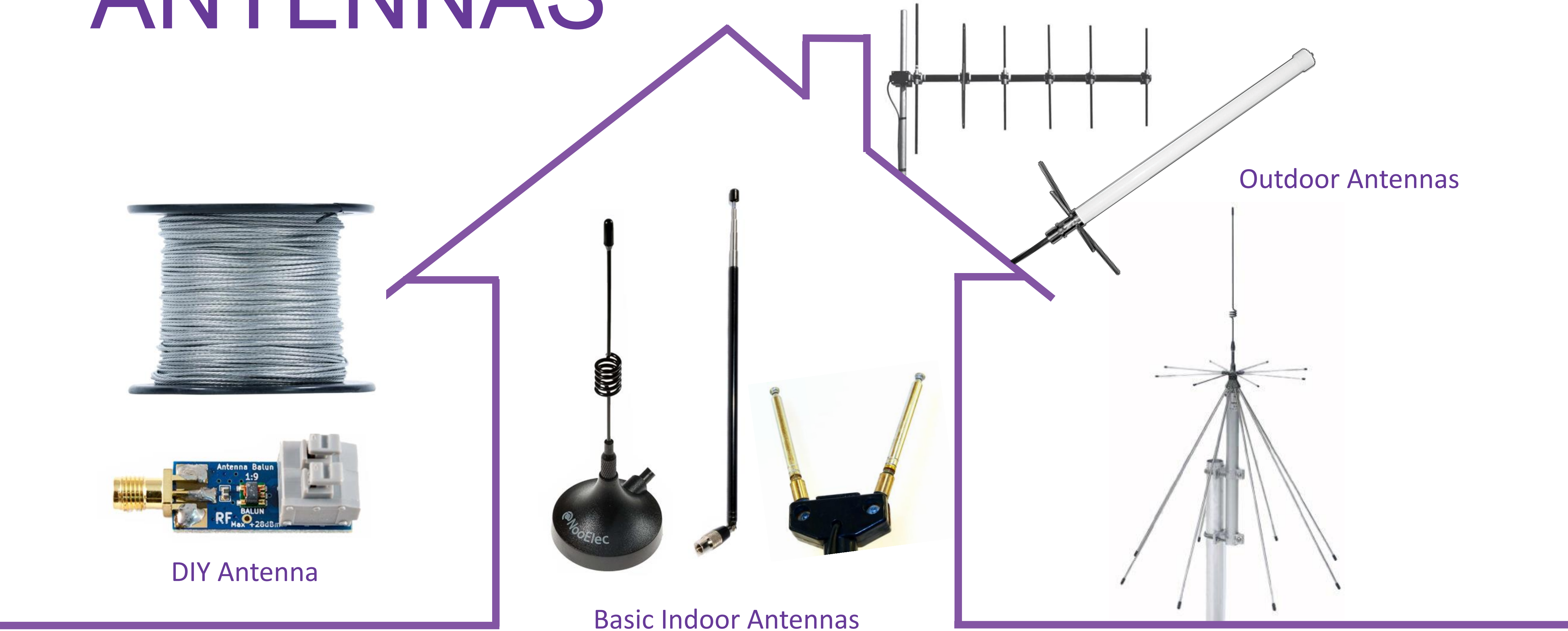
DYNAMIC RANGE / ADC RESOLUTION

Bits per sample value

POPULAR SDR PLATFORMS

Hardware	Platform	Tuner Range	Transmit Capability	Max Sample Rate	ADC	Cost
	RTL-SDR	~50MHz - 1.7GHz	Receive Only	3.2 MSPS	8 bits	$25
	HackRF	10MHz - 6GHz	Half Duplex	20 MSPS	8 bits	$330
	LimeSDR	100kHz - 3.8GHz	Full Duplex (4ch)	61.44 MSPS	12 bits	$299
	LimeSDR mini	10MHz- 3.5GHz	Full Duplex (2ch)	30.72 MSPS	12 bits	$159
	BladeRF	300MHz - 3.8GHz	Full Duplex (4ch)	40 MSPS	12 bits	$420

ANTENNAS



DIY Antenna

Basic Indoor Antennas

Outdoor Antennas

SIGNAL REVERSE ENGINEERING

WORKFLOW:

STEP 1
Find the signal

STEP 2
Capture the signal

STEP 3
Analyze the signal

GOALS

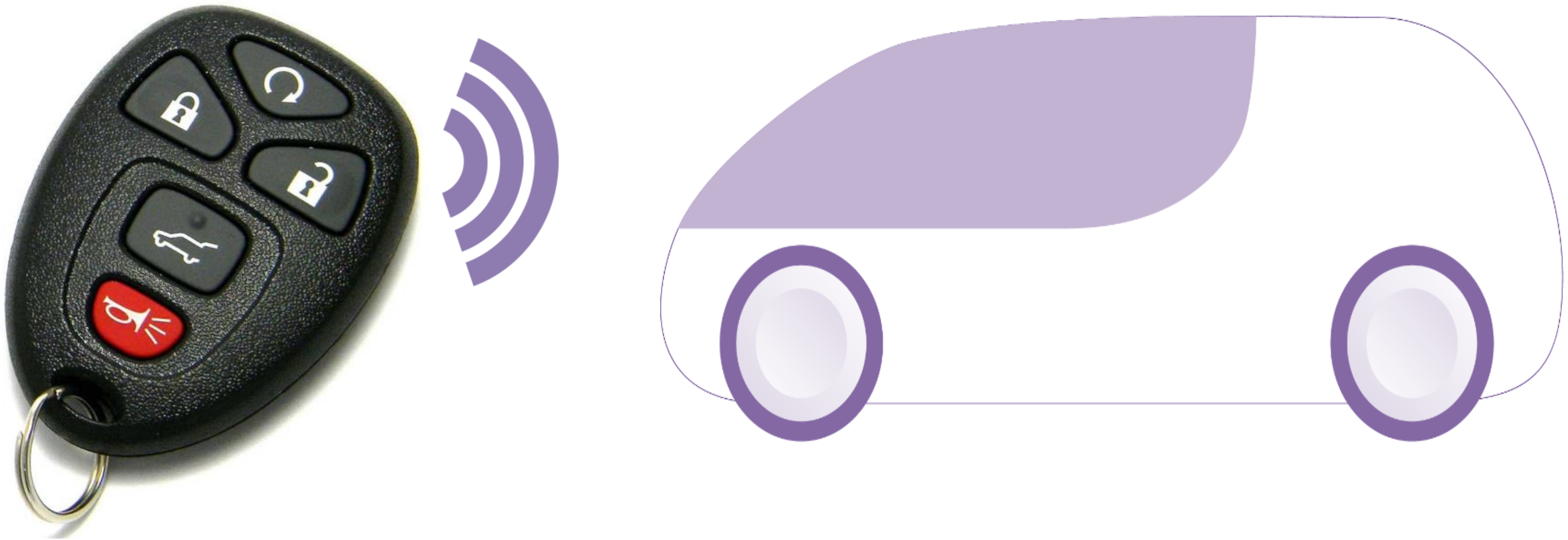
Identify the following:

- Frequency
- Bandwidth
- Modulation
- Symbol rate/ Data rate/ Baud rate
- Packet structure elements
(Preamble, Sync Word, CRC, Fields, Field sizes)

STEP 1

FIND THE SIGNAL

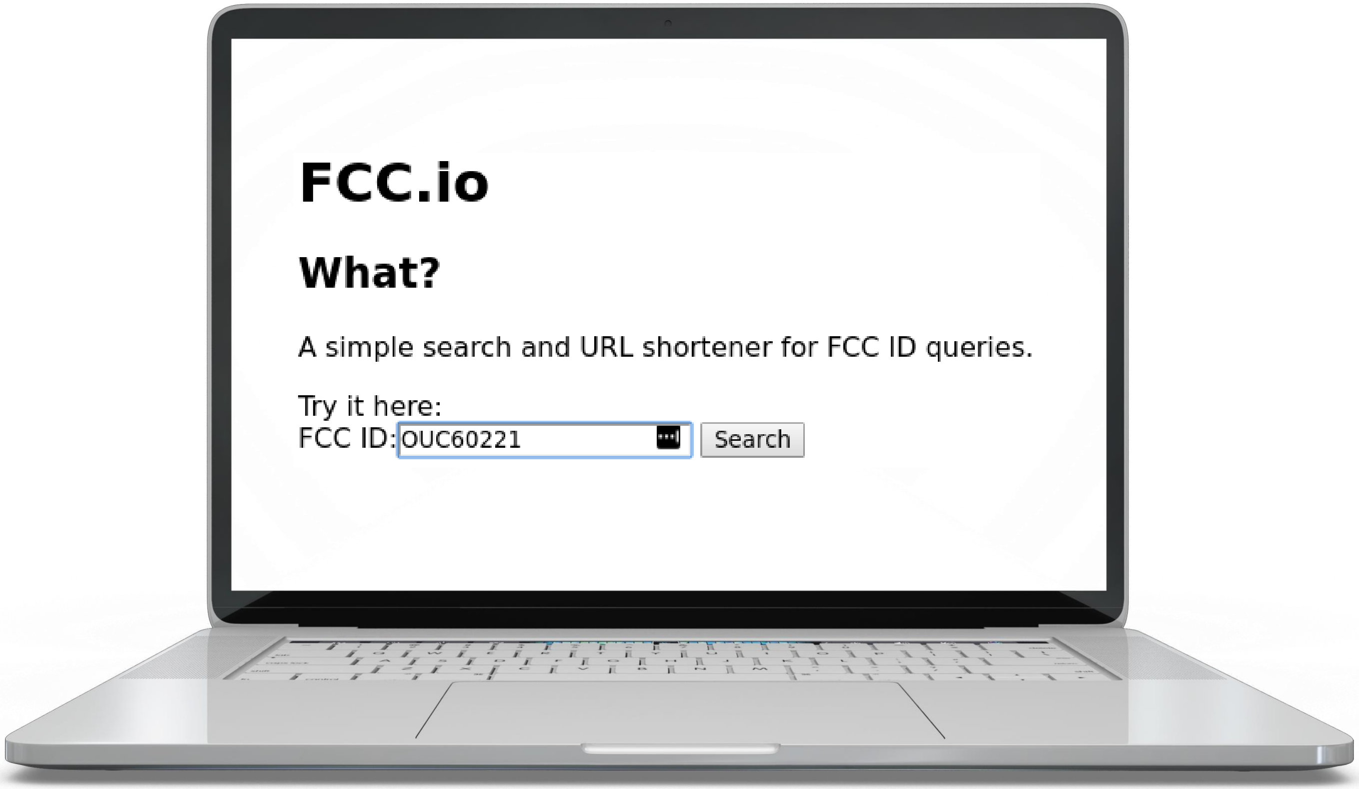
In these examples we’re going to be looking at some car key fobs



STEP 1

FIND THE SIGNAL

Use the FCC ID to quickly identify the frequency/bandwidth



FCC.io

What?

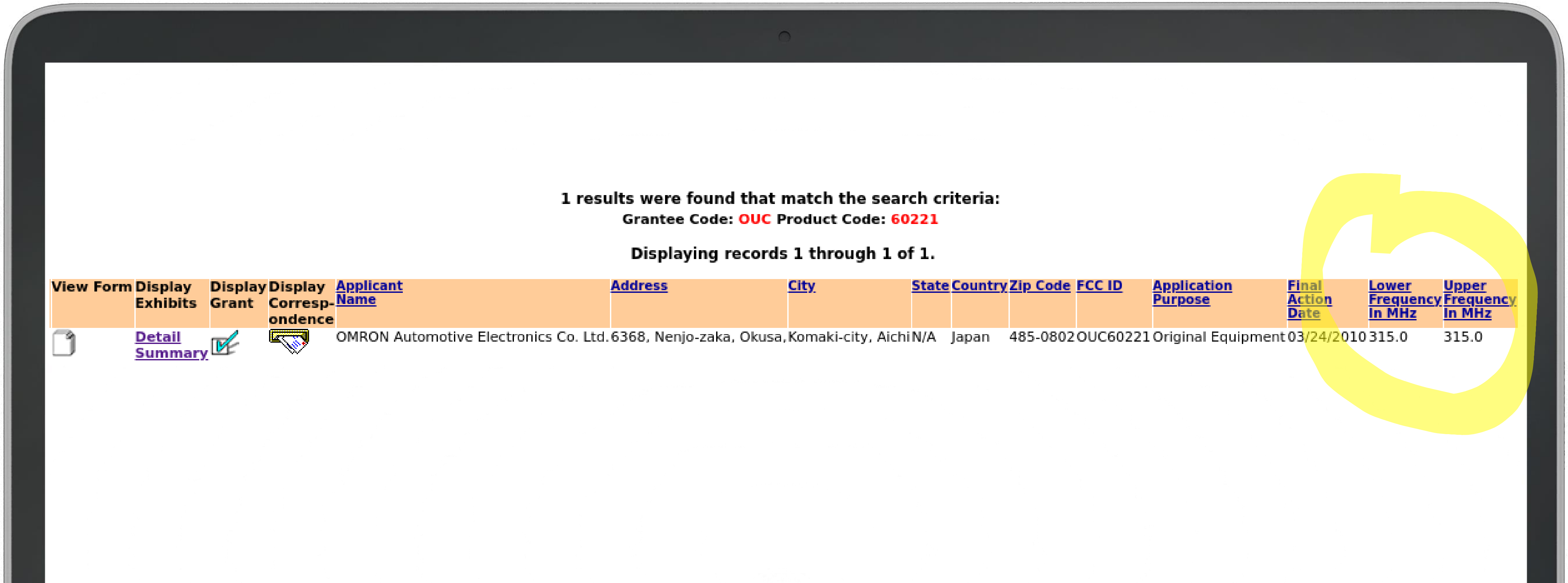
A simple search and URL shortener for FCC ID queries.

Try it here:
FCC ID: OUC60221

STEP 1

FIND THE SIGNAL

Use the FCC ID to quickly identify the frequency/bandwidth



1 results were found that match the search criteria:

Grantee Code: OUC Product Code: 60221

Displaying records 1 through 1 of 1.

View Form	Display Exhibits	Display Grant	Display Corresp-ondence	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	✓		OMRON Automotive Electronics Co. Ltd.	6368, Nenjo-zaka, Okusa,	Komaki-city, Aichi	N/A	Japan	485-0802	OUC60221	Original Equipment	03/24/2010	315.0	315.0

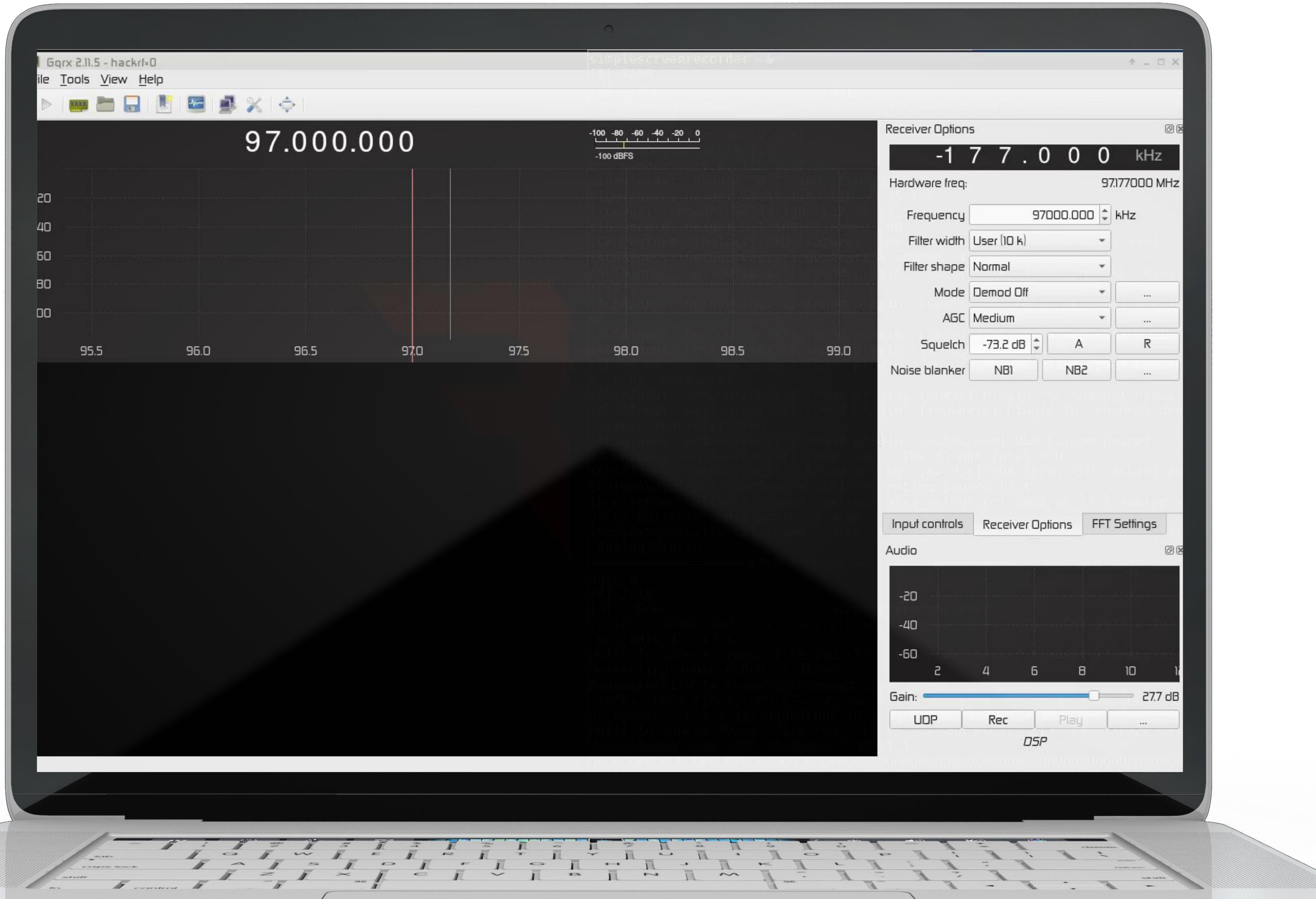
STEP 1

FIND THE SIGNAL

Confirm the frequency & bandwidth

with a tool like GQRX, SDR#, or Baudline

Watch in action: https://youtu.be/RAoWL7dLnME



Gqrx 2.11.5 - hackrf=0

97.000.000

Receiver Options

-1 7 7 . 0 0 0 kHz

Hardware freq: 97.177000 MHz

Frequency 97000.000 kHz

Filter width User (10 k)

Filter shape Normal

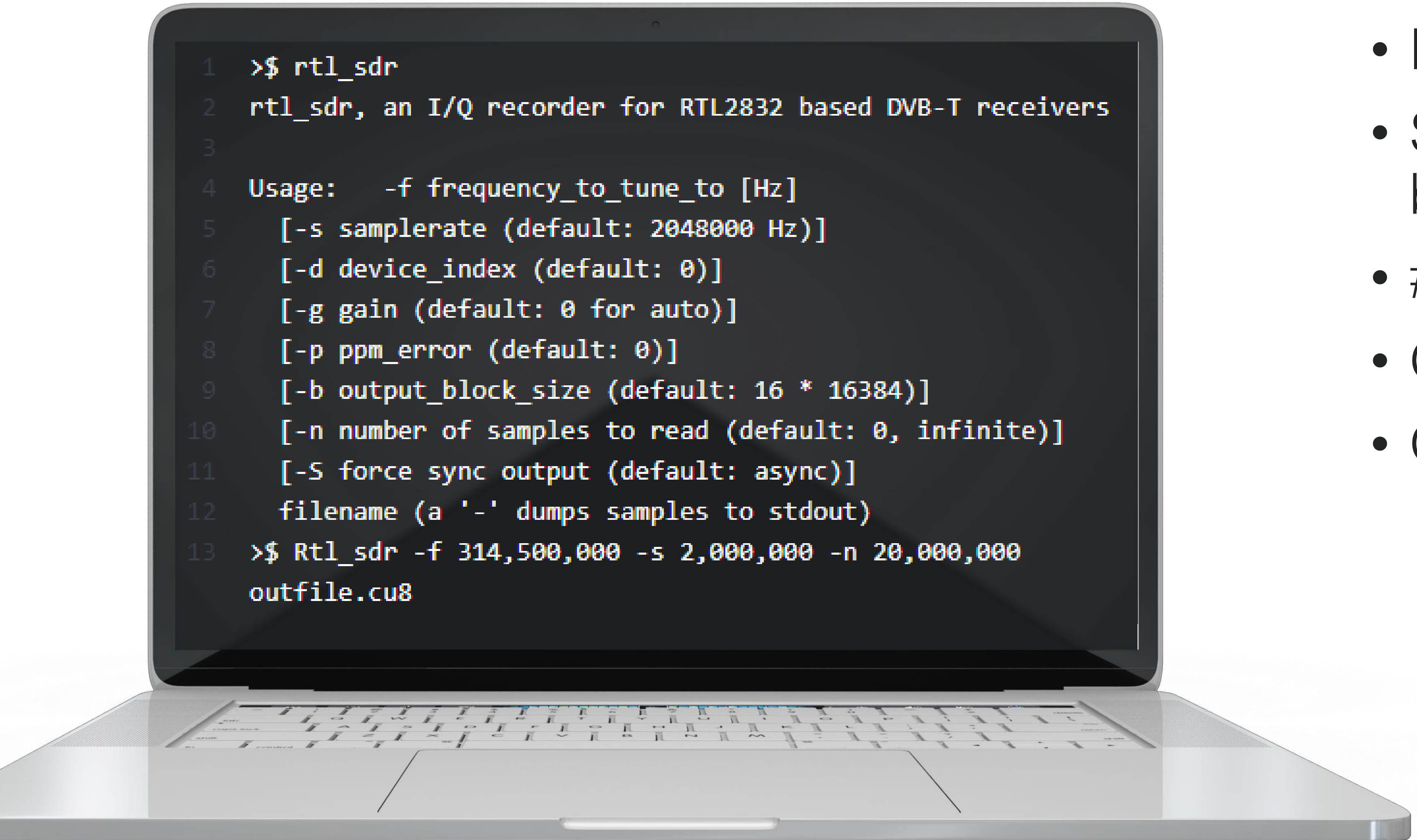
Mode Demod Off

AGC Medium

Squelch -73.2 dB

Gain: 27.7 dB

STEP 2
CAPTURE THE SIGNAL



```
>$ rtl_sdr
rtl_sdr, an I/Q recorder for RTL2832 based DVB-T receivers

Usage:    -f frequency_to_tune_to [Hz]
  [-s samplerate (default: 2048000 Hz)]
  [-d device_index (default: 0)]
  [-g gain (default: 0 for auto)]
  [-p ppm_error (default: 0)]
  [-b output_block_size (default: 16 * 16384)]
  [-n number of samples to read (default: 0, infinite)]
  [-S force sync output (default: async)]
  filename (a '-' dumps samples to stdout)
>$ Rtl_sdr -f 314,500,000 -s 2,000,000 -n 20,000,000
outfile.cu8
```

- Frequency
- Sample rate / bandwidth
- # of Samples to read
- Gain (usually optional)
- Output file name/type:
  - .cfile
  - .cu8
  - .cs8
  - .cs16

STEP 3

ANALYZE THE SIGNAL

GOAL

Go from signal to bits:

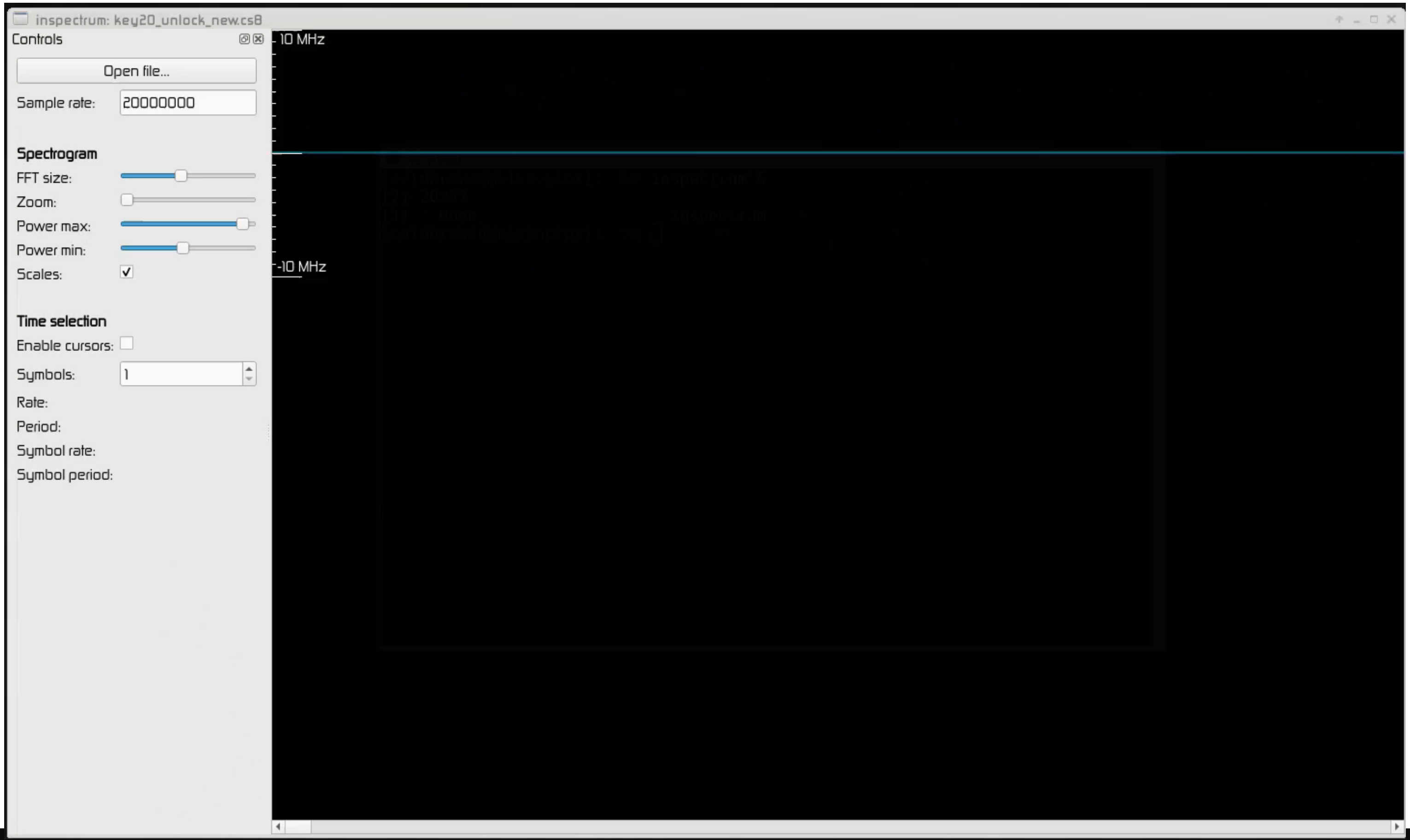
- Identify modulation type
- Symbol rate/baud rate/data rate/
- Identify protocol elements:
  - Preamble & Sync Word
  - Packet structure

Tools

- Inspectrum
- DspectrumGUI
- Universal Radio Hacker

Watch it in action:

https://youtu.be/M6vUJbav1VE



inspectrum: key20_unlock_new.cs8

Controls

Sample rate: 20000000

Spectrogram

FFT size:

Zoom:

Power max:

Power min:

Scales: ☑

Time selection

Enable cursors: □

Symbols: 1

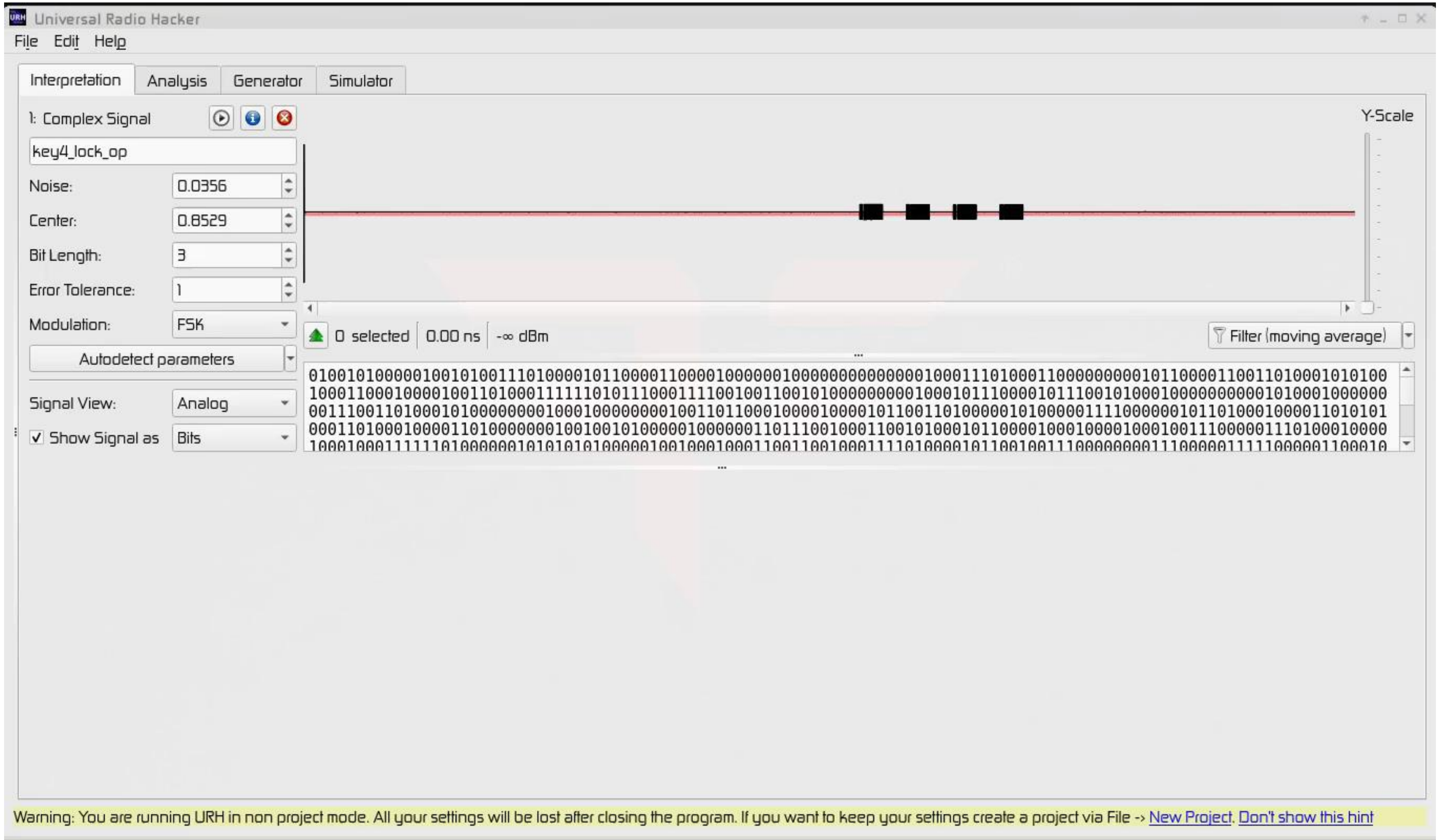
Rate:

Period:

Symbol rate:

Symbol period:

Watch it in action: https://youtu.be/M6vUJbav1VE



key4_lock_op

Noise: 0.0356

Center: 0.8529

Bit Length: 3

Error Tolerance: 1

Modulation: FSK

Signal View: Analog

☑ Show Signal as Bits

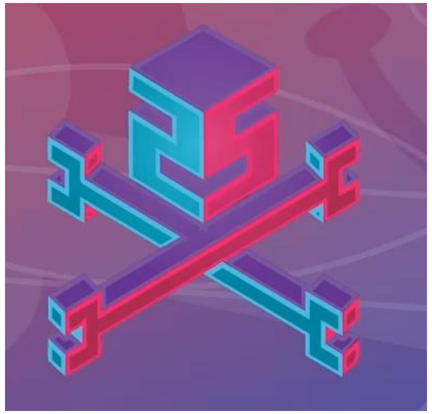
0 selected | 0.00 ns | -∞ dBm

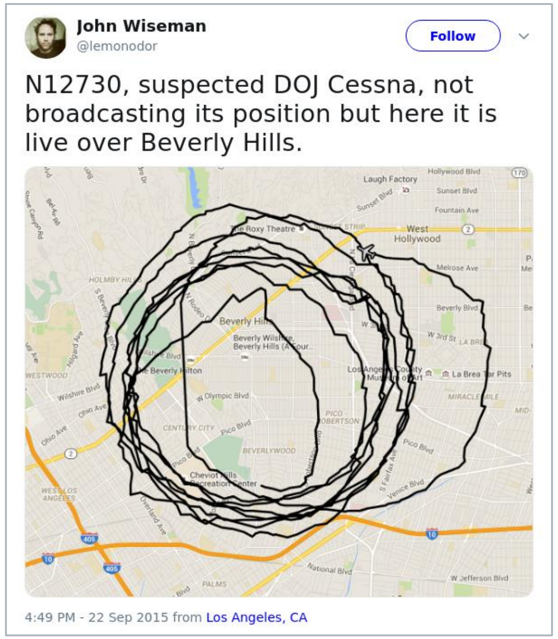
```
010010100000100101001110100001011000011000010000001000000000000001000111010001100000000010110000110011010001010100
100011000100001001101000111111010111000111100100110010100000000010001011100001011100101000100000000001010001000000
0011100110100010100000000100010000000001001101100010000100001011001101000000101000000111100000001011010001000011010101
0001101000100001101000000001001001010000010000001101110010001100101000101100001000100001000100111000001110100010000
10001000111111101000000010101010100000010010001000110011001000111101000010110010011100000000011100000111110000001100010
```

Warning: You are running URH in non project mode. All your settings will be lost after closing the program. If you want to keep your settings create a project via File -> New Project. Don't show this hint

SPIES IN THE SKIES

DEFCON25



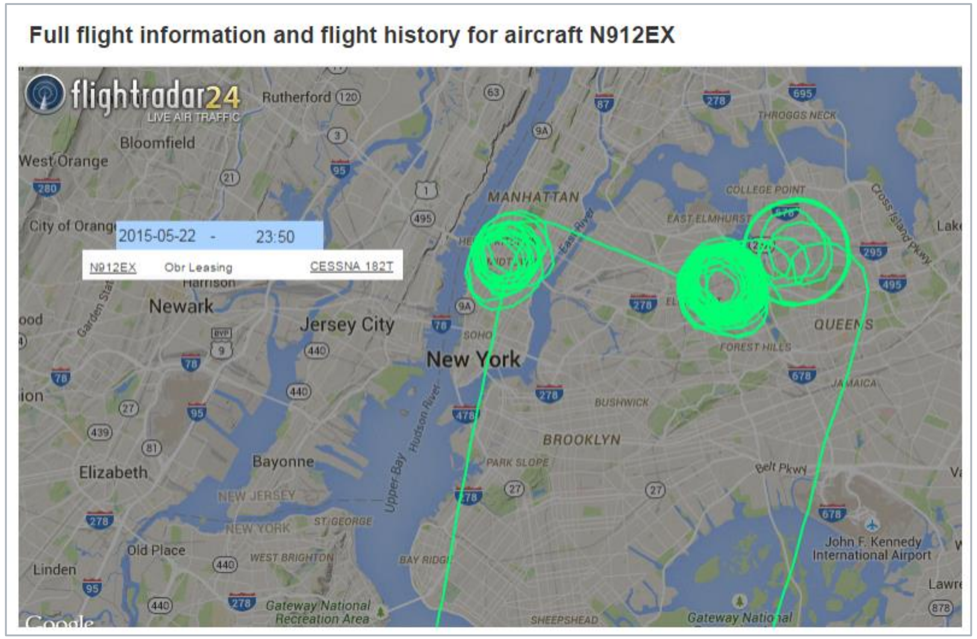


John Wiseman @lemonodor

Follow

N12730, suspected DOJ Cessna, not broadcasting its position but here it is live over Beverly Hills.

4:49 PM - 22 Sep 2015 from Los Angeles, CA

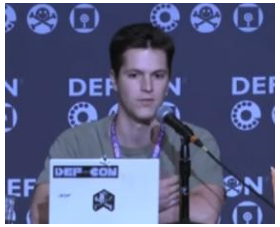


Full flight information and flight history for aircraft N912EX

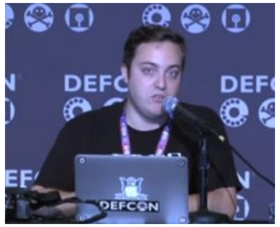
2015-05-22 - 23:50

N912EX Obr Leasing CESSNA 182T

JASON HERNANDEZ
@jason_nstar



SAM RICHARDS
@minneapolisam



JEROD MACDONALD-EVOY
@jerodmacevoy

JOHN WISEMAN*
@lemonodor

DRIVE IT LIKE YOU HACKED IT

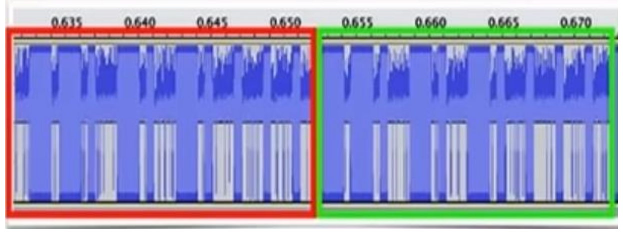
DEFCON23

SAMY
KAMKAR
@samykamkar

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 = 1771 secs = **29.5 minutes**

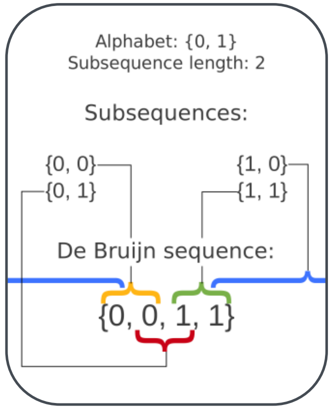
Where does one code end and the other begin?



De Bruijn Sequence

For every 8 to 12 bit garage code
((2**12)+11)*
4ms / 2 =
8214ms =

8.214 seconds



Alphabet: {0, 1}
Subsequence length: 2

Subsequences:

{0, 0}
{0, 1}
{1, 0}
{1, 1}

De Bruijn sequence:

{0, 0, 1, 1}

OTHER COOL HACKS

BALINT SEEBER

@minneapolisam

Rick Rolls San Francisco with emergency broadcast towers

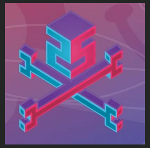
With “All Your RFz Are Belong to Me” Defcon 21

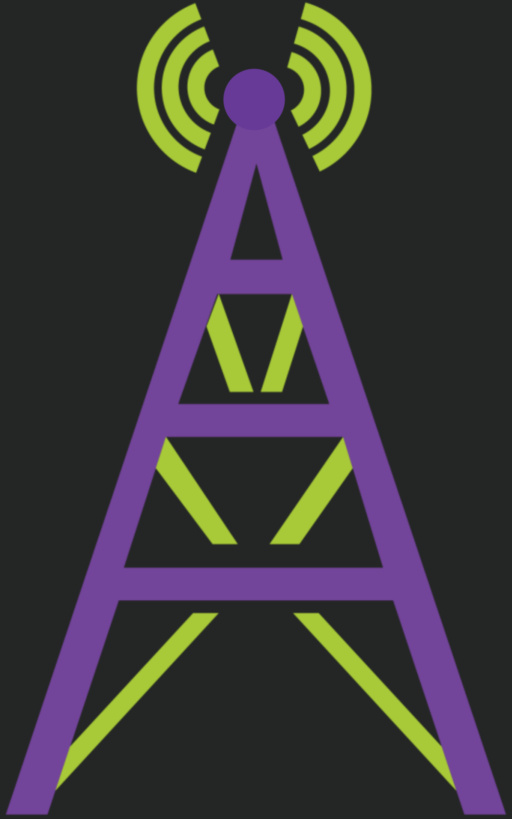
KRISTIN PAGET

@KristinPaget

GSM hacks with “Practical Cellphone Spying

Defcon18





TOOLS WE COVERED

- GnuRadio-companion
- GQRX
- Baudline
- SDR#
- Inspectrum
- DspectrumGUI
- Universal Radio Hacker (urh)

QUESTIONS?

THANK YOU