

# Security Like The ‘80s : How I stole your RF

Exploring CVE-2022-27254 and more!

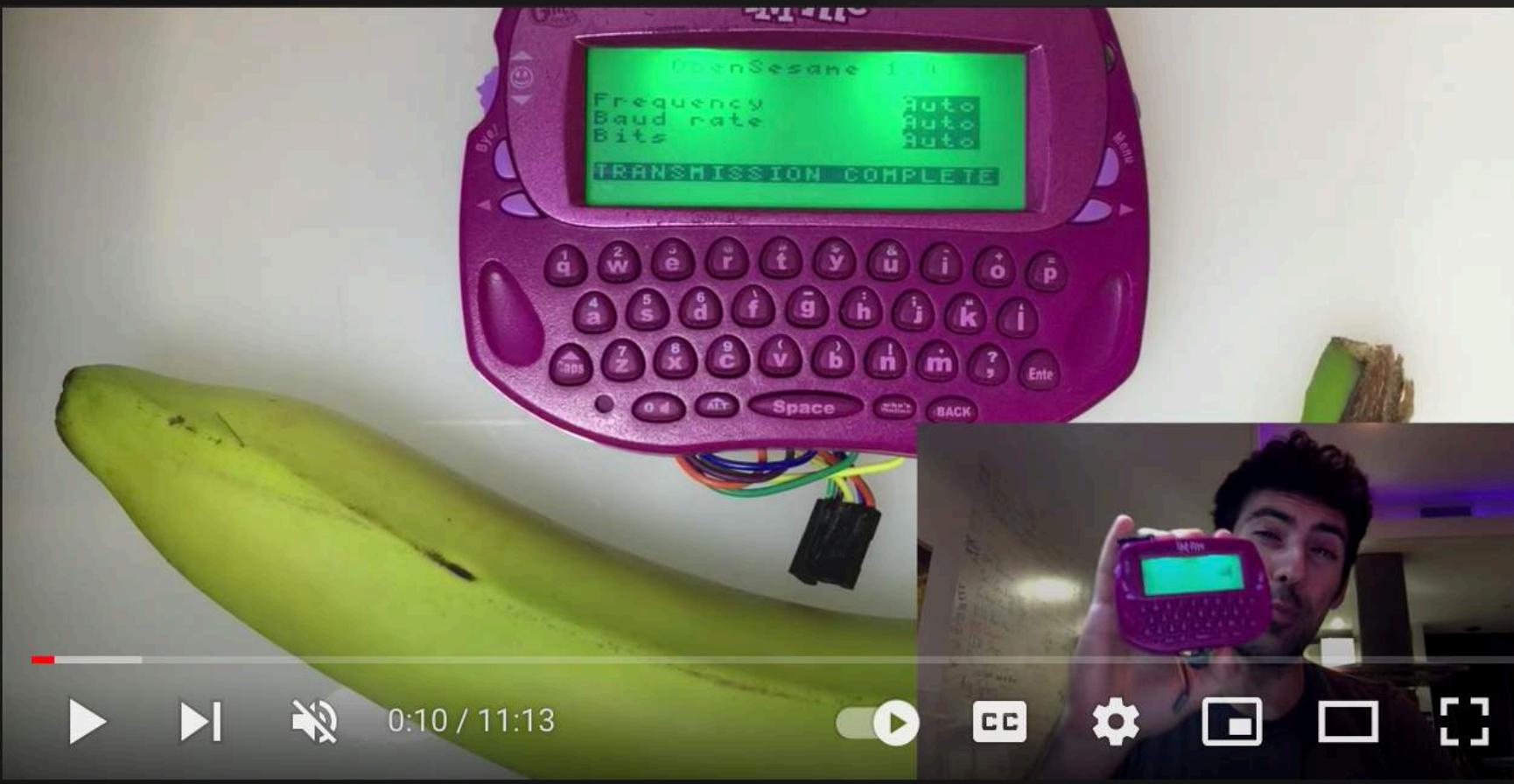


# \$ uname -a

- Ayyappan Rajesh
- Aspiring security researcher and student @UMass Dartmouth
- Twitter: @ayyappan162010 GitHub: @nonamecoder
- Website: [www.ayyappan.me](http://www.ayyappan.me)



- Popov Mikhail aka SkorP
- SubGHz Architect @ Flipper Devices
- Telegram: @SkorP\_SkorP GitHub: @Skorpionm



OpenSesame - hacking garages in seconds using a Mattel toy

486 7.9K DISLIKE SHARE DOWNLOAD CLIP SAVE ...

samy kamkar  
202K subscribers

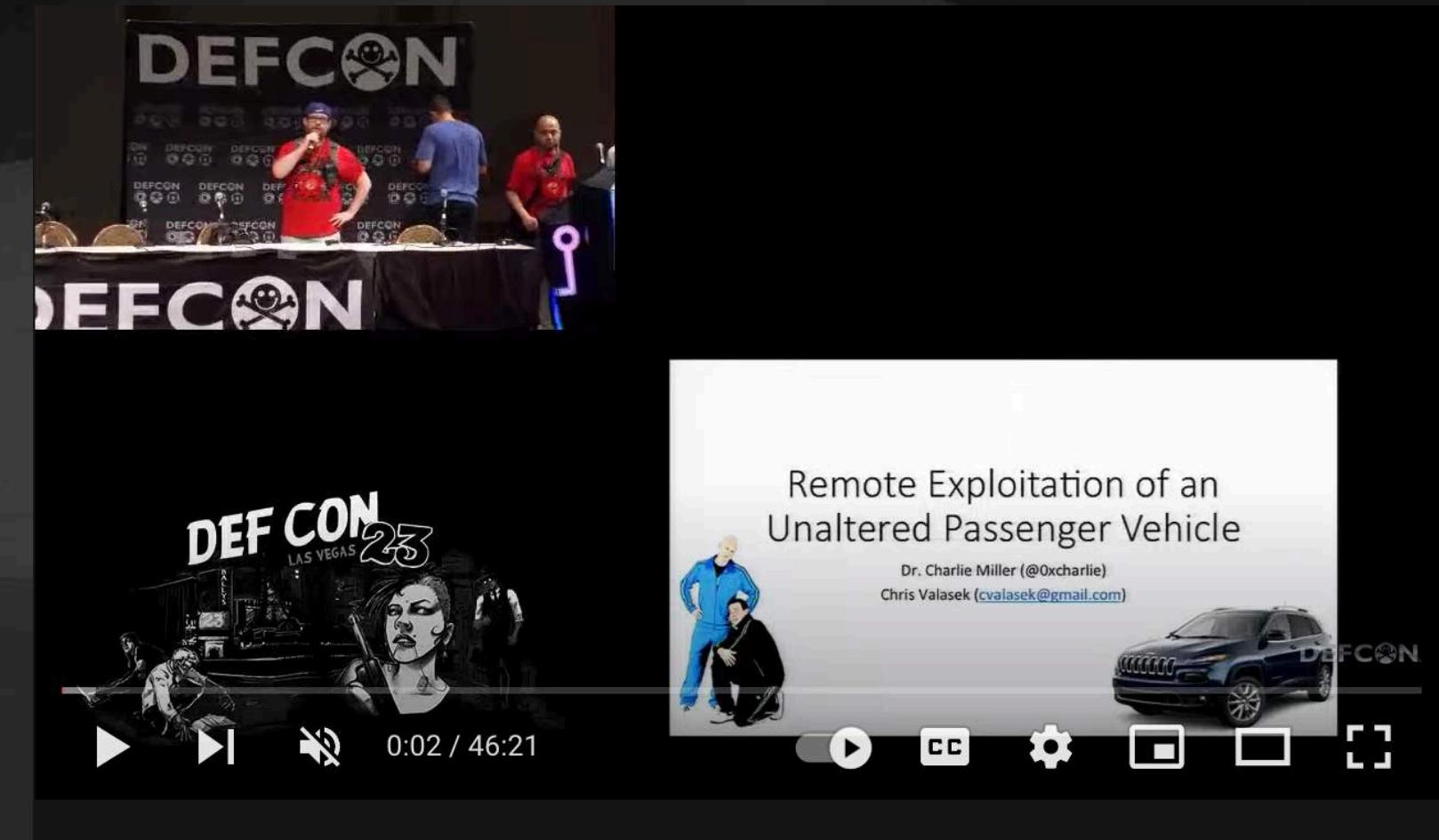
SUBSCRIBE



Radio Hacking: Reverse Engineering Protocols Part 1 - Hak5 1913

40,9 768 DISLIKE SHARE DOWNLOAD CLIP SAVE ...

Hak5 806K subscribers



DEF CON 23 - Charlie Miller & Chris Valasek - Remote Exploitation of an Unaltered Passenger Vehicle

137 1.6K DISLIKE SHARE DOWNLOAD CLIP SAVE ...

DEFCONConference  
229K subscribers

SUBSCRIBE

# Disclaimer

This presentation is for informational and educational purpose only. All demonstrations/videos shown in here were done only on personal vehicles, or with explicit permission from the owner. You shall not misuse the information to gain unauthorized access. This disclaimer may be amended, updated or otherwise changed, at any time and without prior notice.

Most techniques used here are already known for years and can be readily found on the internet.

Everything will be available on my GitHub repository / Website shortly after the presentation. Some files have been altered to prevent misuse.

No key fobs were harmed in the making of this presentation.

# Story time...

**Department of Electrical and Computer Engineering  
University of Massachusetts Dartmouth  
ECE488/548 Cyber Threats and Security Management Prof. Hong Liu**

## Project Assignment

A project (by individual, partner or team) selects either type below and takes 3 stages: <sup>1)</sup>Proposal, <sup>2)</sup>Progress Report, and <sup>3)</sup>Presentation/Demo with Final Report. A leader of 3+ members could earn a bonus of one grade level up upon his/her members' nominations and instructor's approval. Refer to MyCourses for detailed guidelines on each stage.

### **Type A: Experiment a Cybersecurity Solution**

Scope: A state-of-the-art solution such as PKI for Connected Vehicles with Security Credential Management System (SCMS) [www.its.dot.gov/resources/scms.htm](http://www.its.dot.gov/resources/scms.htm) & <https://wiki.campllc.org/display/SCP>

Approach: Experiment/Analyze its vulnerabilities with attack surface/model and demonstrate improved defense scheme

Outcome: Technical report of your solution. Deliverables such as Extended Abstract/Paper Draft to an IEEE conference.

### **Type B: Understand a Cybersecurity Incident**

Scope: A current or infamous incident such as the recent Equifax Data Breach

Approach: Literature Search what went wrong and how to stop it from happening again

Outcome: Research plan with preliminary results. Deliverables such as Master Project/Thesis Proposal for ECE Graduate Program in December or Survey for the topic.

ECE 488, Prof. Hong Liu, University of Massachusetts Dartmouth

# CVE on a car?!

The screenshot shows the NVD interface for a specific vulnerability entry. At the top, the NVD logo is visible next to the text "Information Technology Laboratory" and "NATIONAL VULNERABILITY DATABASE". Below this, there's a green button labeled "VULNERABILITIES". The main content area features a large heading "CVE-2019-20626 Detail" with a magnifying glass icon. Underneath, there's a section titled "Current Description" which states: "The remote keyless system on Honda HR-V 2017 vehicles sends the same RF signal for each door-open request, which might allow a replay attack." Below this description is a link "+View Analysis Description". A "Severity" section is present, with tabs for "CVSS Version 3.x" (selected) and "CVSS Version 2.0". The "CVSS 3.x Severity and Metrics:" section is empty. To the right, a "QUICK INFO" sidebar contains the following information:

|                              |                |
|------------------------------|----------------|
| <b>CVE Dictionary Entry:</b> | CVE-2019-20626 |
| <b>NVD Published Date:</b>   | 03/23/2020     |
| <b>NVD Last Modified:</b>    | 09/14/2021     |
| <b>Source:</b>               | MITRE          |

C

cve-request@mitre.org

Re: [scr1232352] Honda Civic 2018 - Remotes with FCC ID: KR5V2X

To: arajesh@umassd.edu, Cc: cve-request@mitre.org

[EXTERNAL SENDER]

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

[Suggested description]

The remote keyless system on Honda Civic 2018 vehicles sends the same RF signal for each door-open request, which allows for a replay attack, a related issue to CVE-2019-20626.

-----  
[VulnerabilityType Other]

Replay Attack on Honda Civic 2018

-----  
[Vendor of Product]

Honda

-----  
[Affected Product Code Base]

Honda Civic 2018 - Remotes with FCC ID: KR5V2X

-----  
[Attack Type]

Physical

-----  
[Impact Denial of Service]

true

-----  
[CVE Impact Other]

Ability to unlock, lock, remote start and open the trunk of the car

-----  
[Attack Vectors]

User must press either lock or unlock key for attacker to capture data, which can then be replayed

-----  
[Reference]

<https://drive.google.com/file/d/1MtmWfBs1r6Y3JN1HpbNsZqO1GcsdgPdc/view?usp=sharing>

-----  
[Discoverer]

Ayyappan Rajesh, Blake Berry

Use CVE-2022-27254.

---

CVE Assignment Team

M/S M300, 202 Burlington Road, Bedford, MA 01730 USA

[ A PGP key is available for encrypted communications at

[https://cve.mitre.org/cve/request\\_id.html](https://cve.mitre.org/cve/request_id.html) ]

Information Technology Laboratory

## NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

### CVE-2022-27254 Detail

#### Current Description

The remote keyless system on Honda Civic 2018 vehicles sends the same RF signal for each door-open request, which allows for a replay attack, a related issue to CVE-2019-20626.

[+View Analysis Description](#)

**Severity**

CVSS Version 3.x

CVSS Version 2.0

#### QUICK INFO

**CVE Dictionary Entry:**

[CVE-2022-27254](#)

**NVD Published Date:**

03/23/2022

**NVD Last Modified:**

03/31/2022

**Source:**

MITRE

# Media

**Honda downplays vulnerability allowing hackers to lock, unlock and start Civics**

News Technology

[CVE-2022-27254](#) – a replay vulnerability affecting the Remote Keyless System in Honda Civics made between 2016 and 2020.

Researchers released a [detailed breakdown of the issue on GitHub](#), sharing multiple videos showing that the remote keyless system on various Honda vehicles sends the same, unencrypted radio frequency signal for each door-open, door-close, boot-open and remote start command. Cybersecurity researcher Ayyappan Rajesh discovered the vulnerability and worked with developer Blake Berry, his mentor and Cybereason chief security officer Sam Curry as well as his professors Ruolin Zhou and Hong Liu from the University of Massachusetts Dartmouth.

"This allows for an attacker to eavesdrop on the request and conduct a replay attack," the researchers explained.

The researchers said Honda Civic models LX, EX, EX-L, Touring, Si and Type R are affected by the issue. They used several widely-available tools including a HackRF One SDR, a laptop, an account on [FCCID.io](#), access to GQRX software-defined radio receiver software and a GNURadio development toolkit.

All a hacker would need to do is be nearby when a car owner uses their key fob and record the signal it transmits. Once recorded, it could be used to open the car or start it.

**Key fob hacking: How thieves can hack into your car and tips to stop it**

By Christina Gonzalez | Published May 4, 2022 | Technology | FOX 11

[How thieves can hack into your car and tips to stop it](#)

**LOS ANGELES** - "I was surprised how easy it was, an 8-year-old can do it," is how college student Ayyapan Rajesh

**Automaker Cybersecurity Lagging Behind Tech Adoption, Experts Warn**

Author: Becky Bracken | March 31, 2022 / 10:49 am

[Share this article:](#)

**A bug in Honda is indicative of the sprawling car-attack surface that could give cyberattackers easy access to victims, as global**

**Hackers remotely start, unlock Honda Civics with \$300 tech**

Any models made between 2016 and 2020 can have key fob codes sniffed and retransmitted

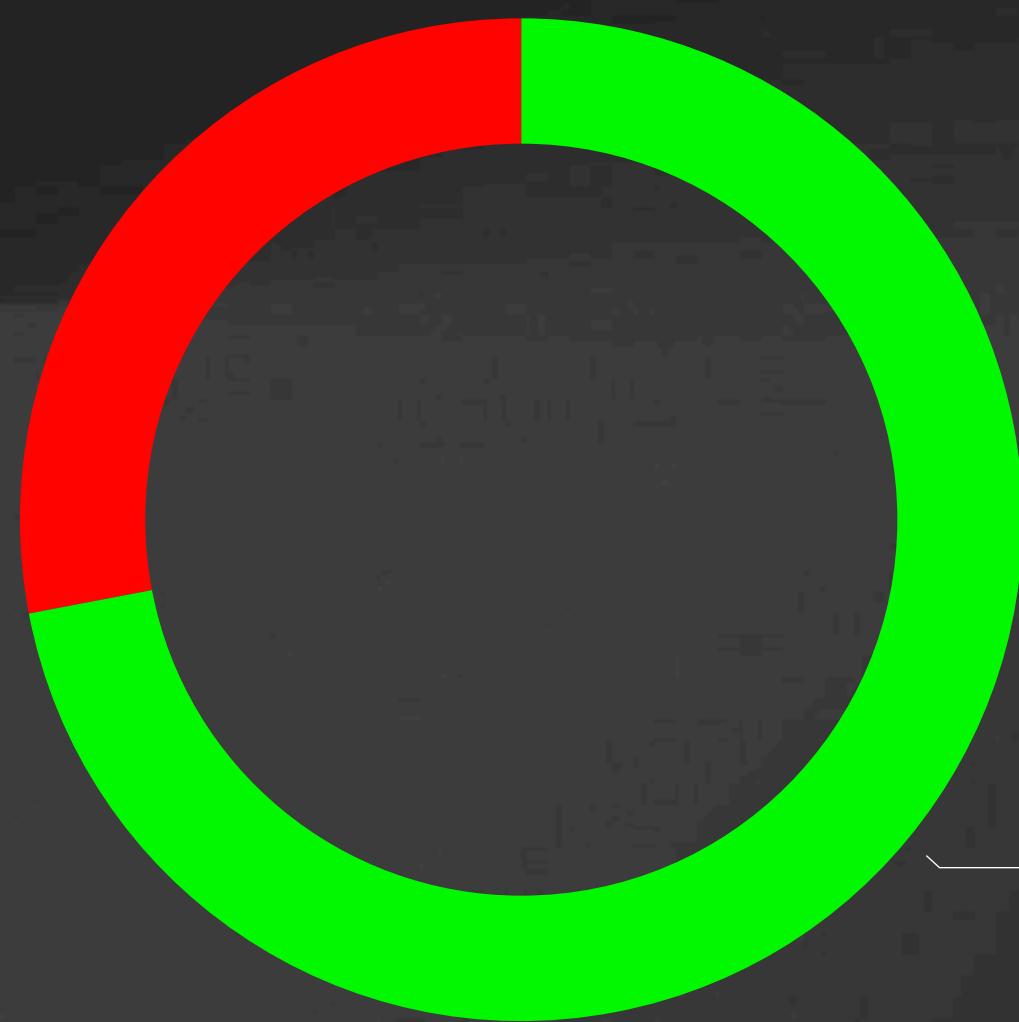
If you're driving a Honda Civic manufactured between 2016 and 2020, this newly reported key fob hijack should start your worry engine.

Keyless entry exploits are nothing new. Anyone armed with the right equipment can sniff out a lock or unlock code and retransmit it. This particular issue with some Honda vehicles is just the latest demonstration that auto manufacturers haven't adapted their technology to keep up with known threats.

This security weakness, tagged [CVE-2022-27254](#), was discovered by Ayyappan Rajesh, a student at University of Massachusetts Dartmouth, and someone with the handle HackingIntoYourHeart. Their [research](#) indicated that Honda Civic LX, EX, EX-L, Touring, Si, and Type R vehicles manufactured between 2016 and 2020 all have this vulnerability.

# Keyless Entry Systems

Keyless entry in  
vehicles after  
2014



Keyless entry in  
vehicles after  
2019

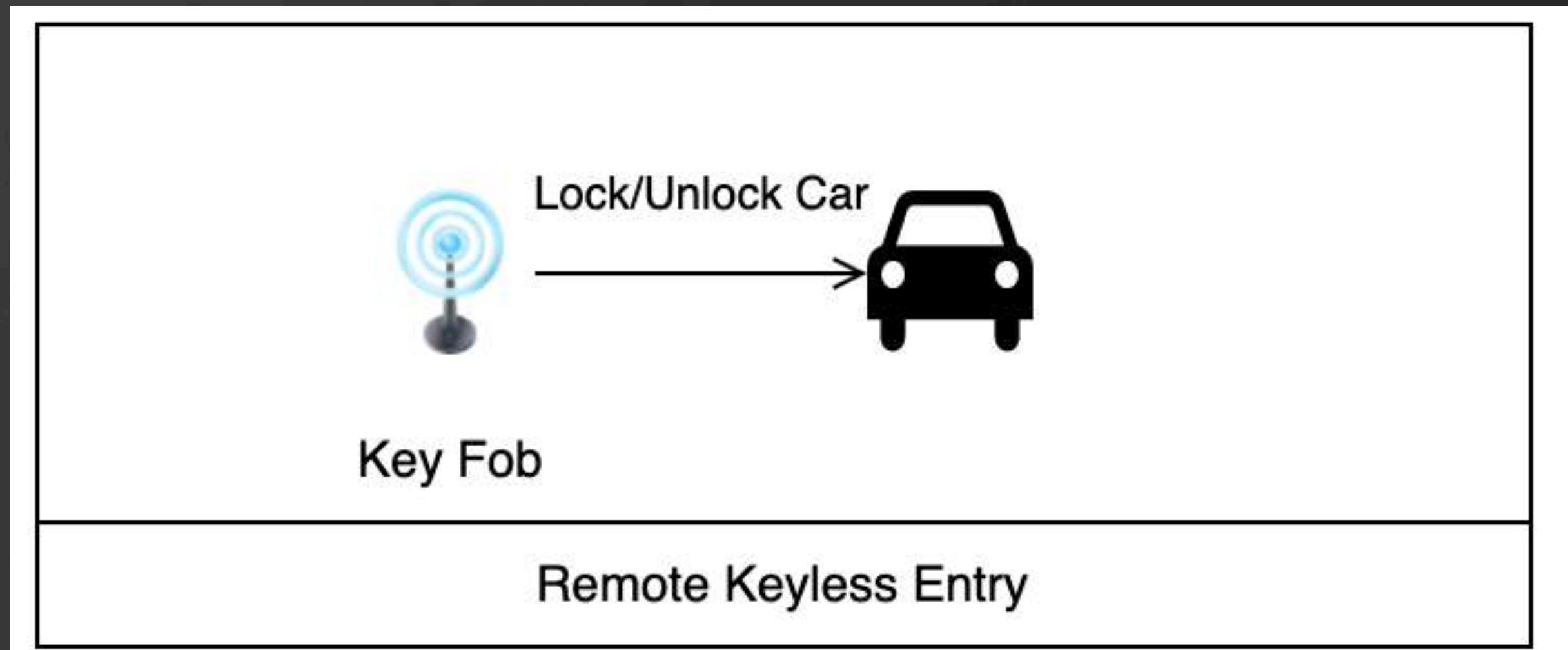


- Equipped with Keyless Entry
- Not equipped

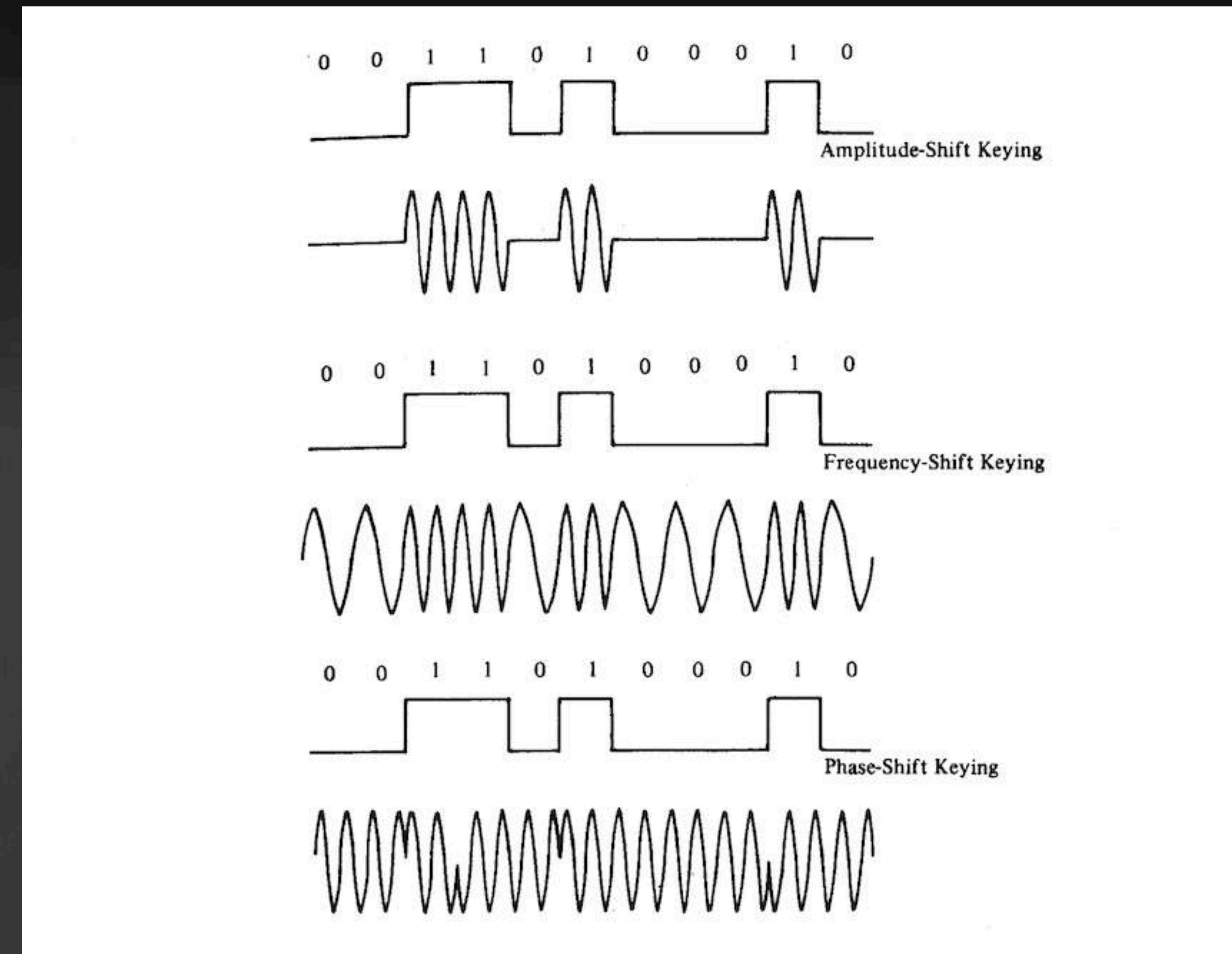
Source : CNBC & Edmunds

# Remote Keyless Entry(RKE)

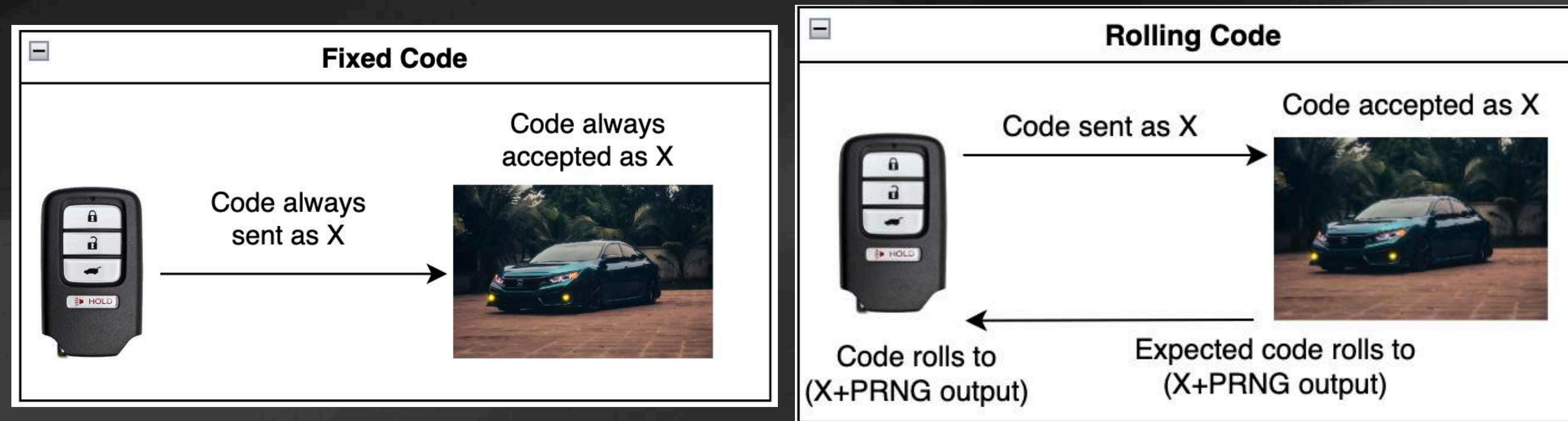
- First introduced in 1982 on a Renault Fuego
- Operates at either 315, 433 or 868MHz



# Modulation



# Static vs. rolling keys

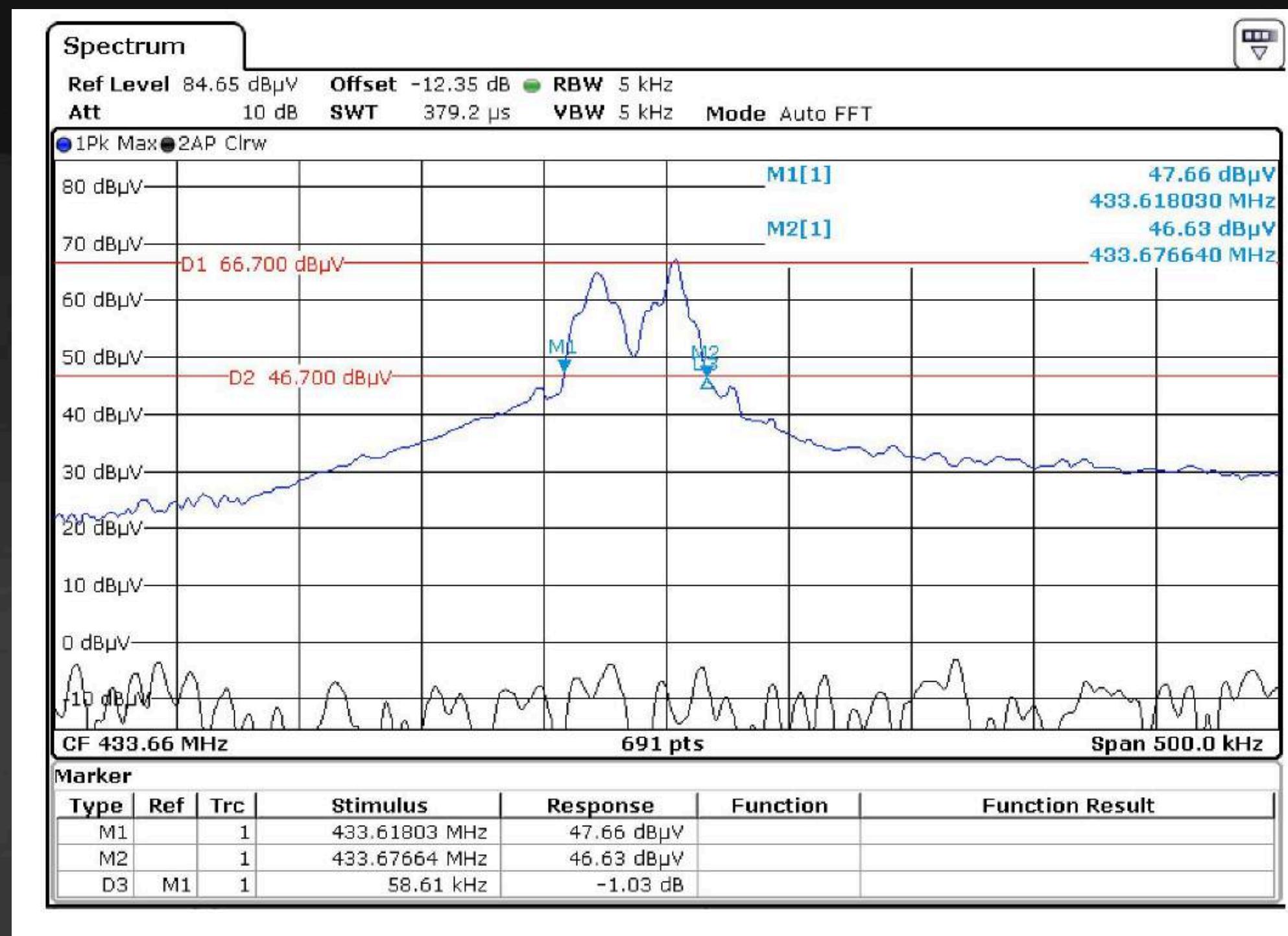


# Tools

- FCCID.IO
- RF transceiver ( HackRF, , USRP N210, Flipper Zero, Yard Stick One...)
- GQRX / AirSpy SDR
- Universal Radio Hacker
- GNURadio

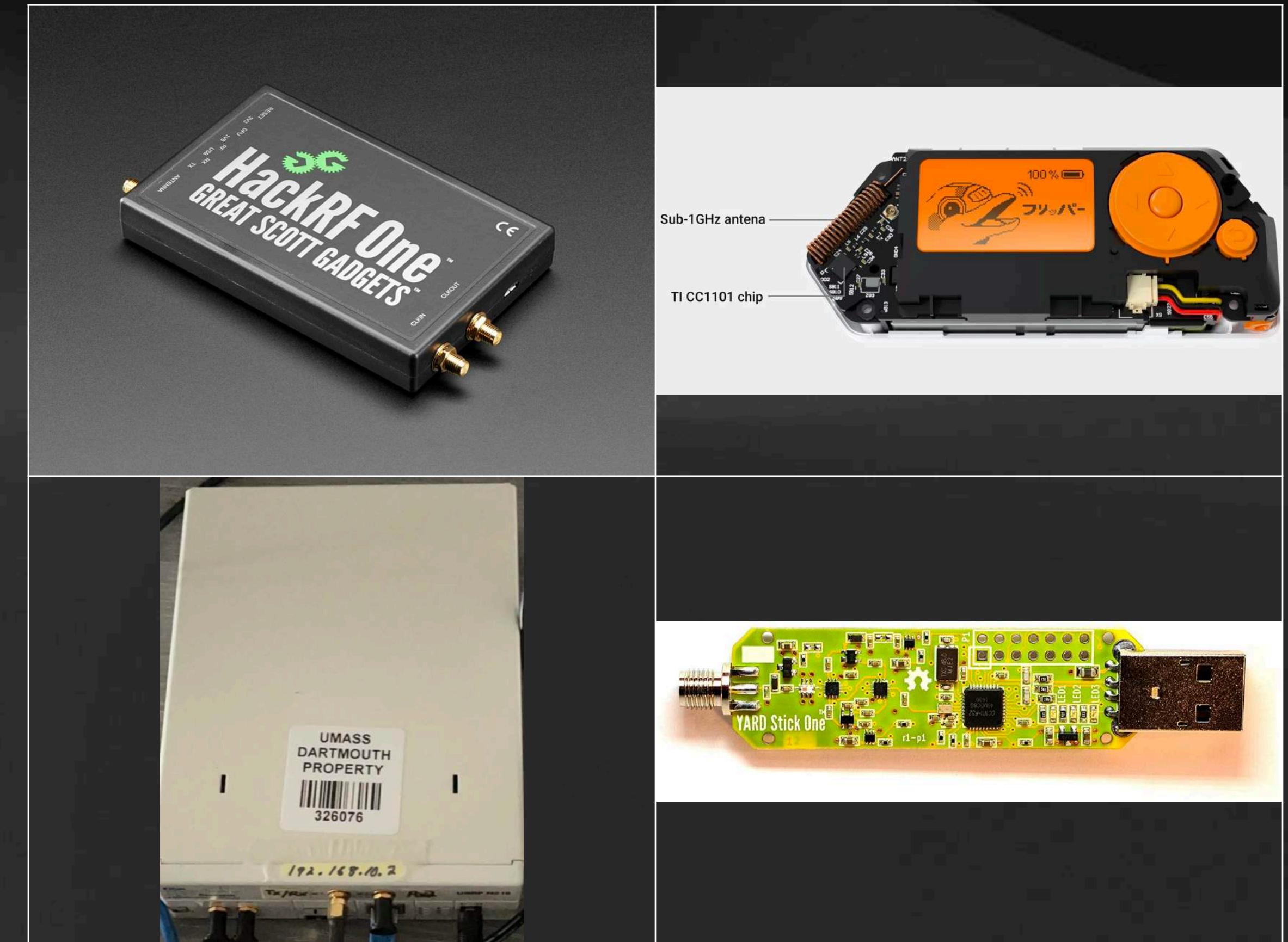
# FCCID.IO

## FCC ID : KRV52X

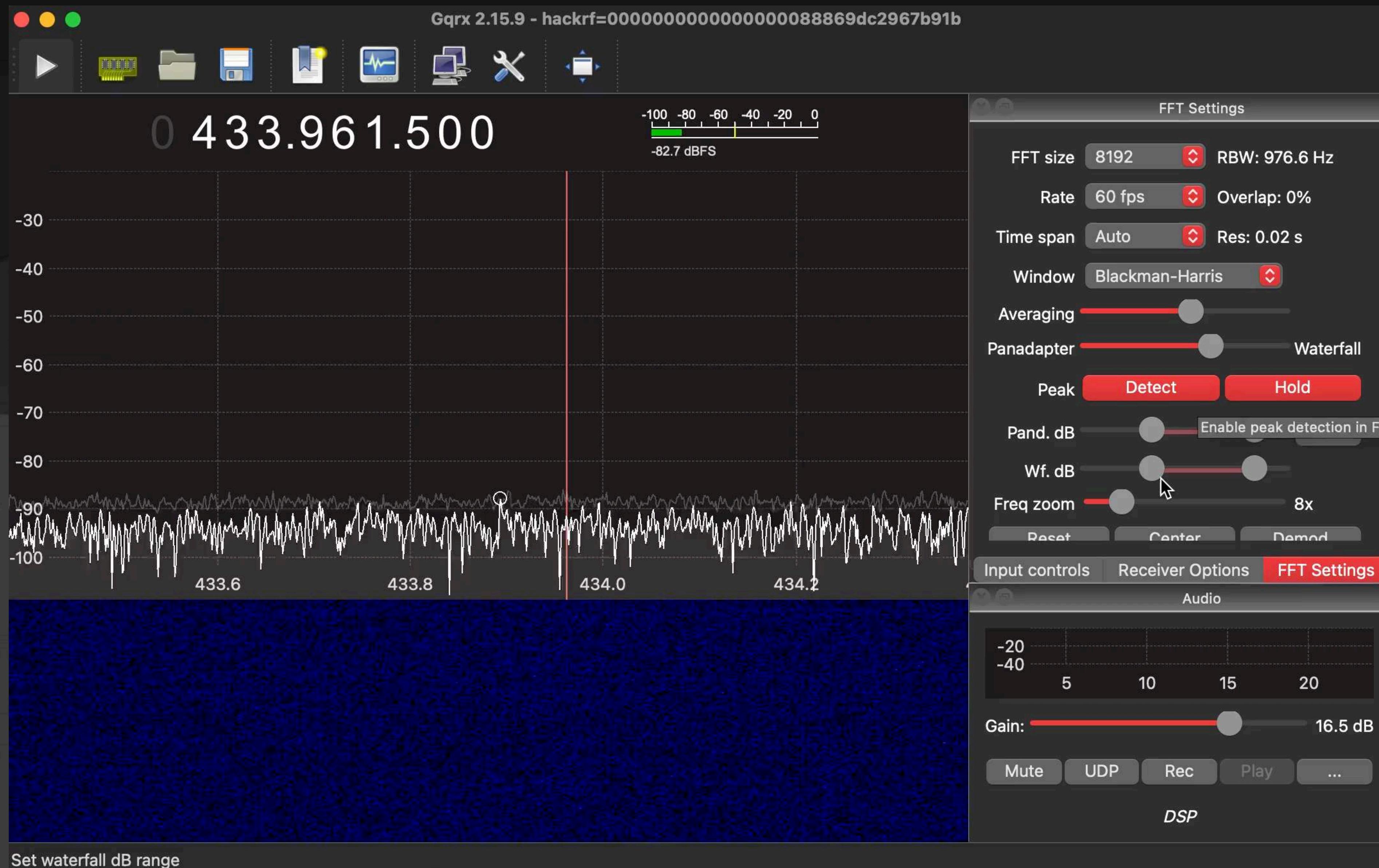


# RF Transceivers

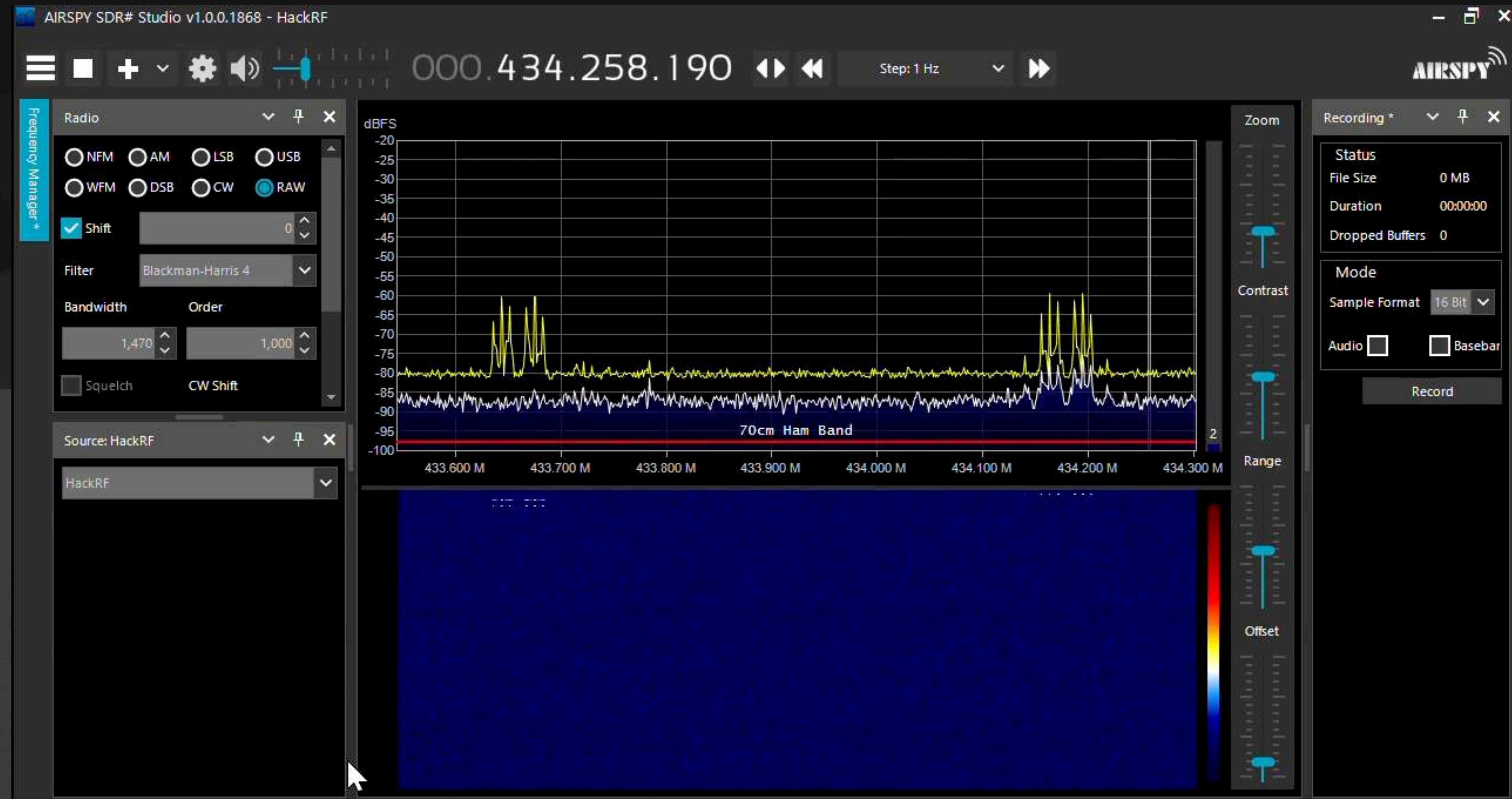
- HackRF
- Flipper Zero
- Yard Stick One
- USRP N210



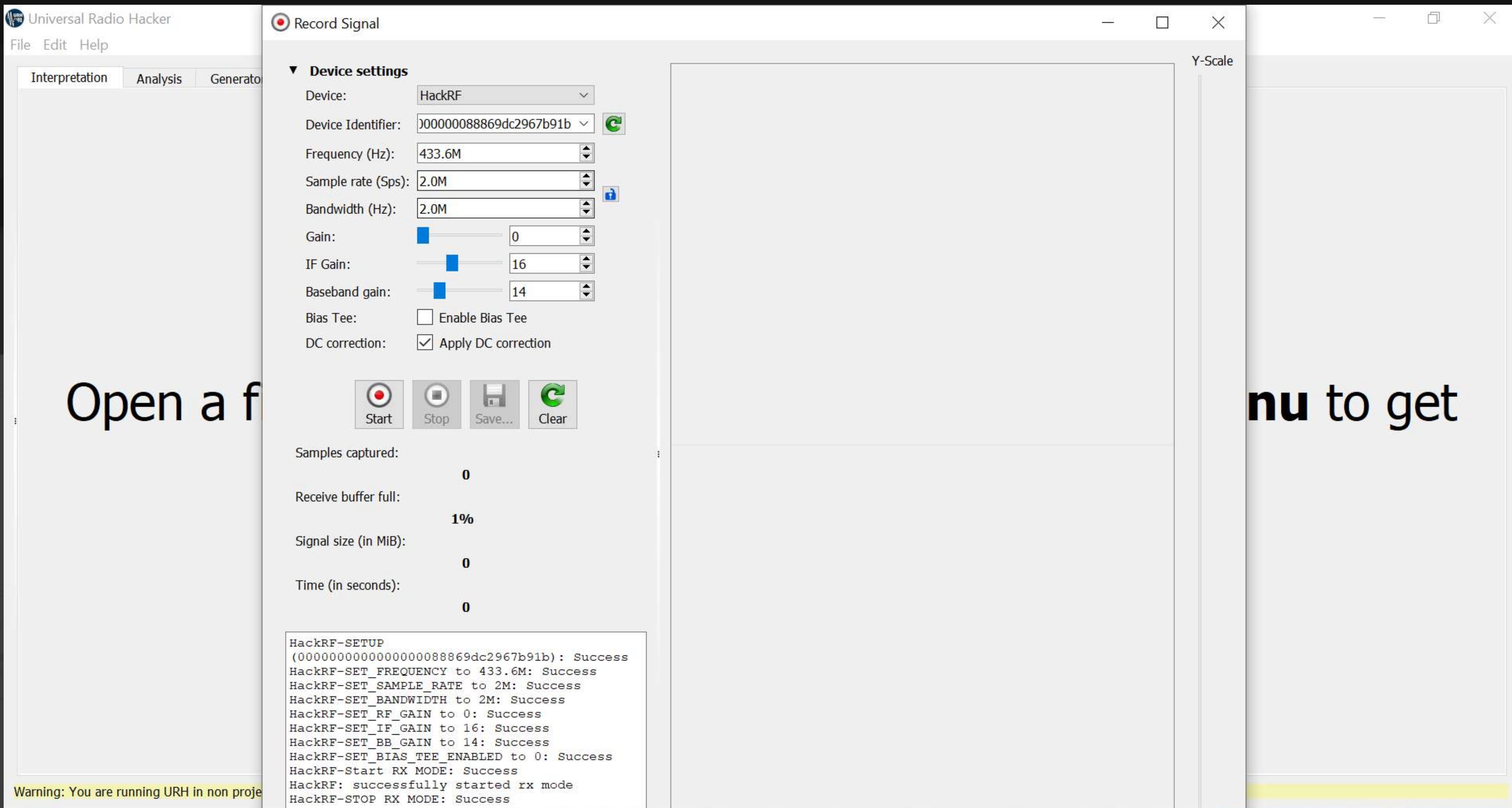
# GQRX



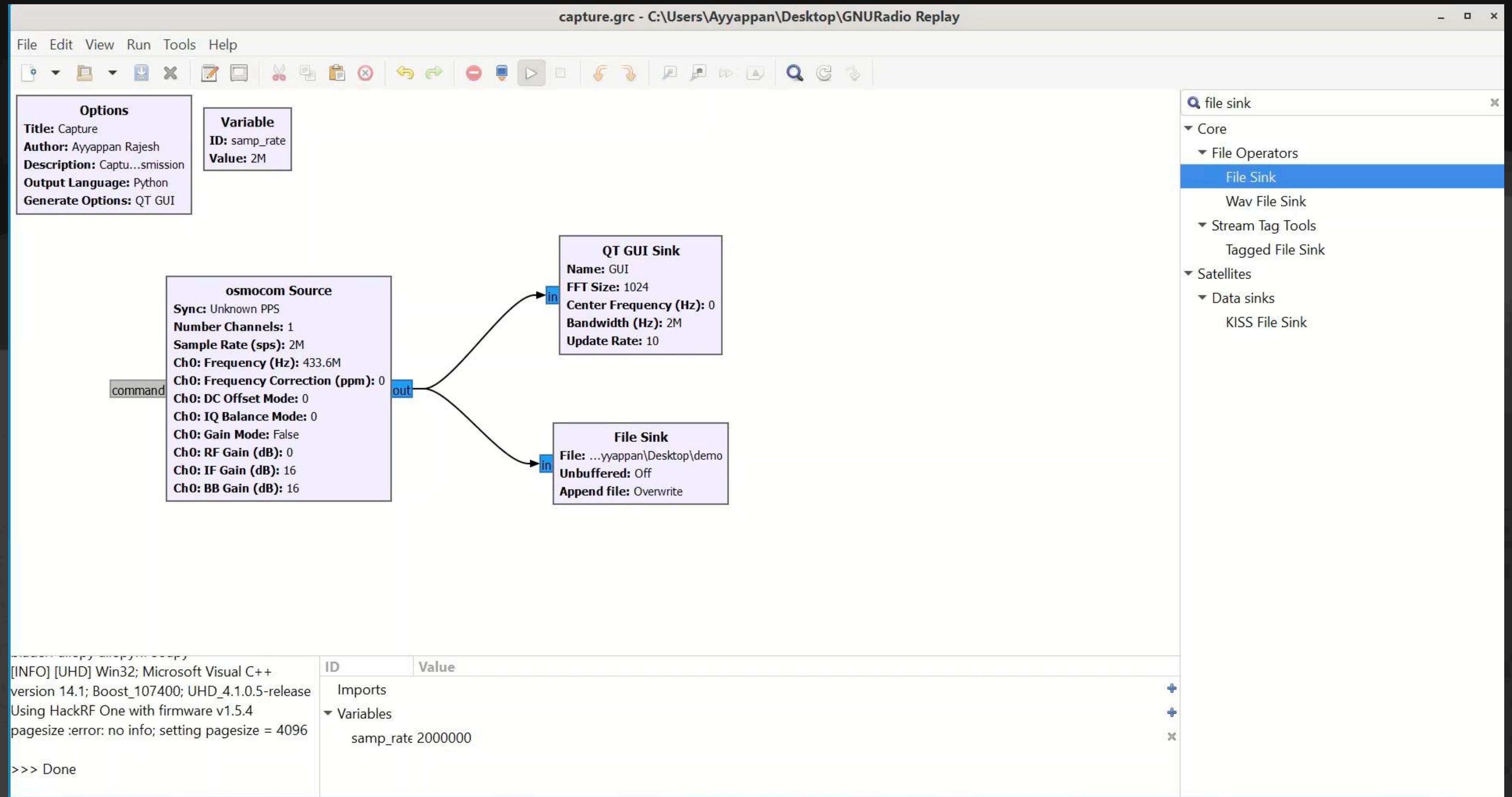
# AirSpy SDR



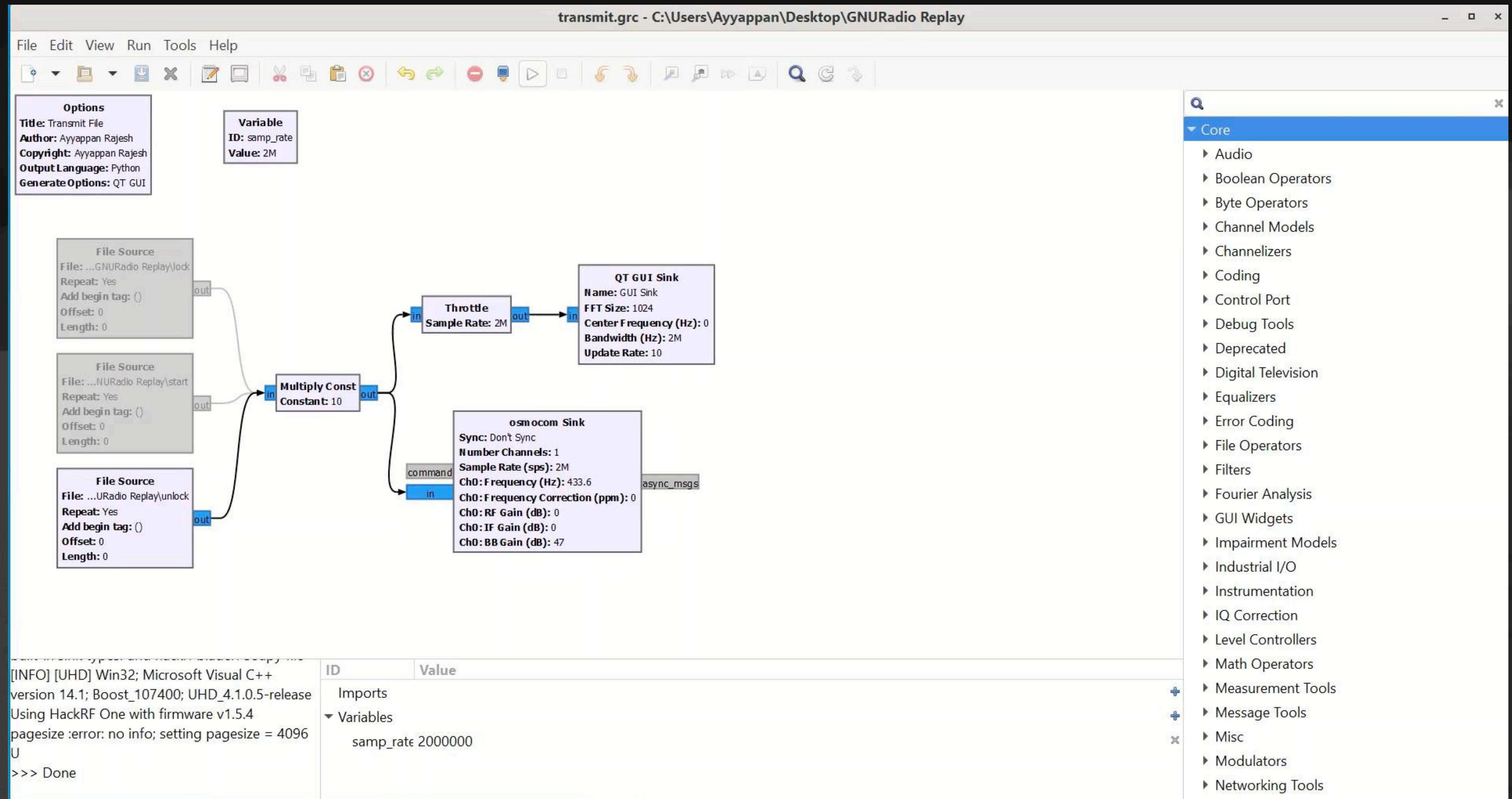
# Universal Radio Hacker (URH)



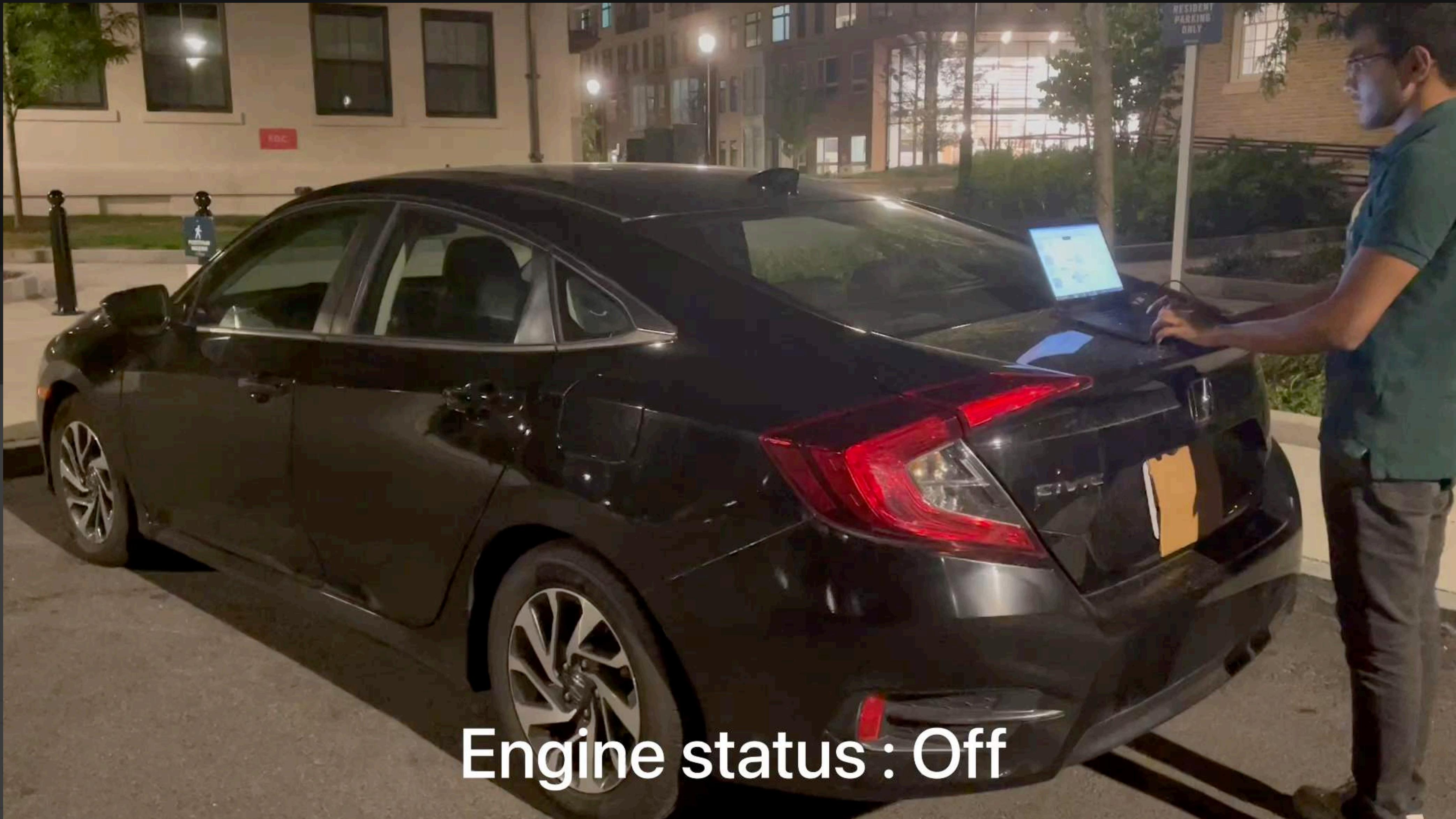
# GNURadio Capture



# GNURadio Transmit

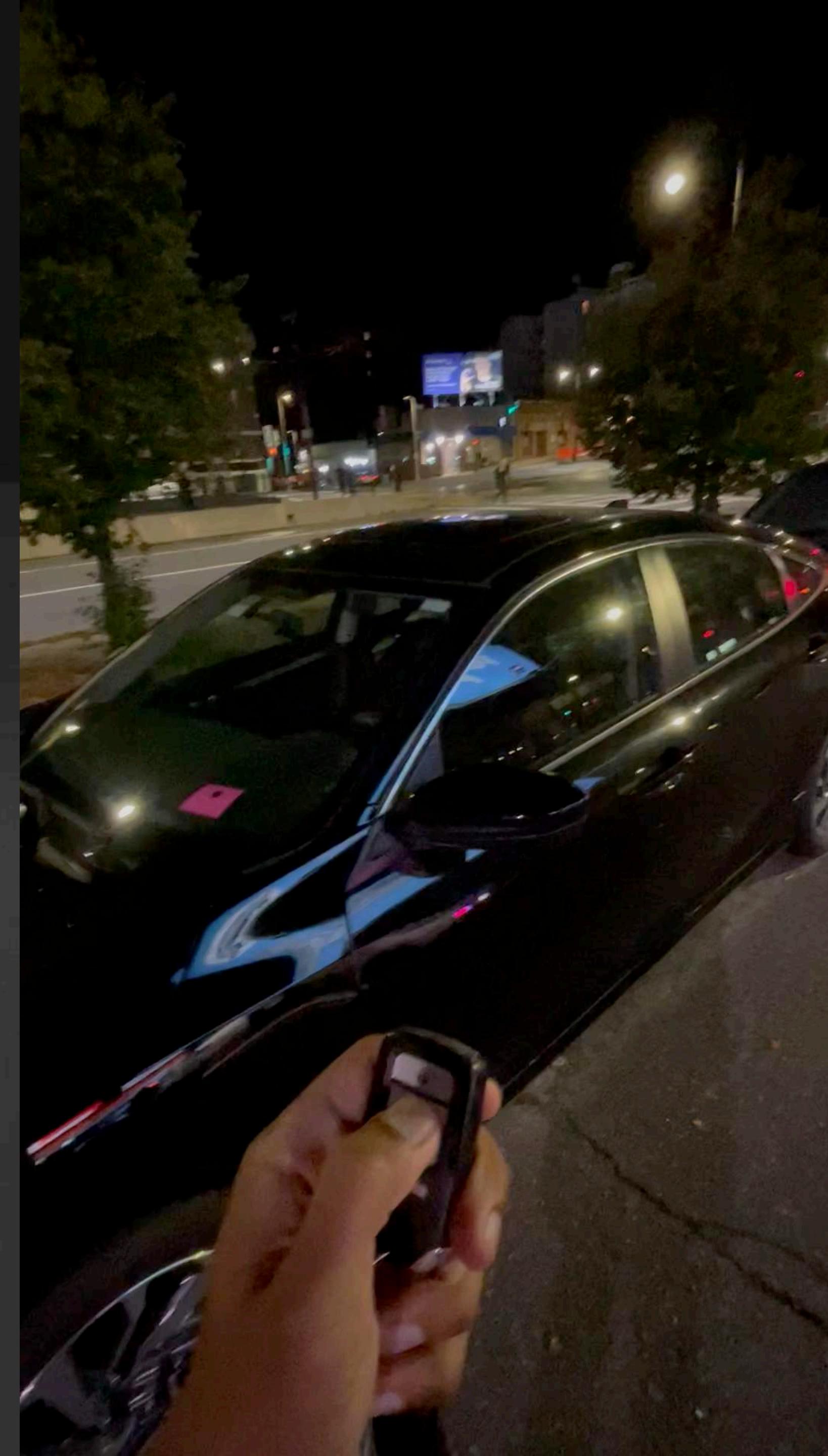


# Gone in 50 seconds



Engine status : Off

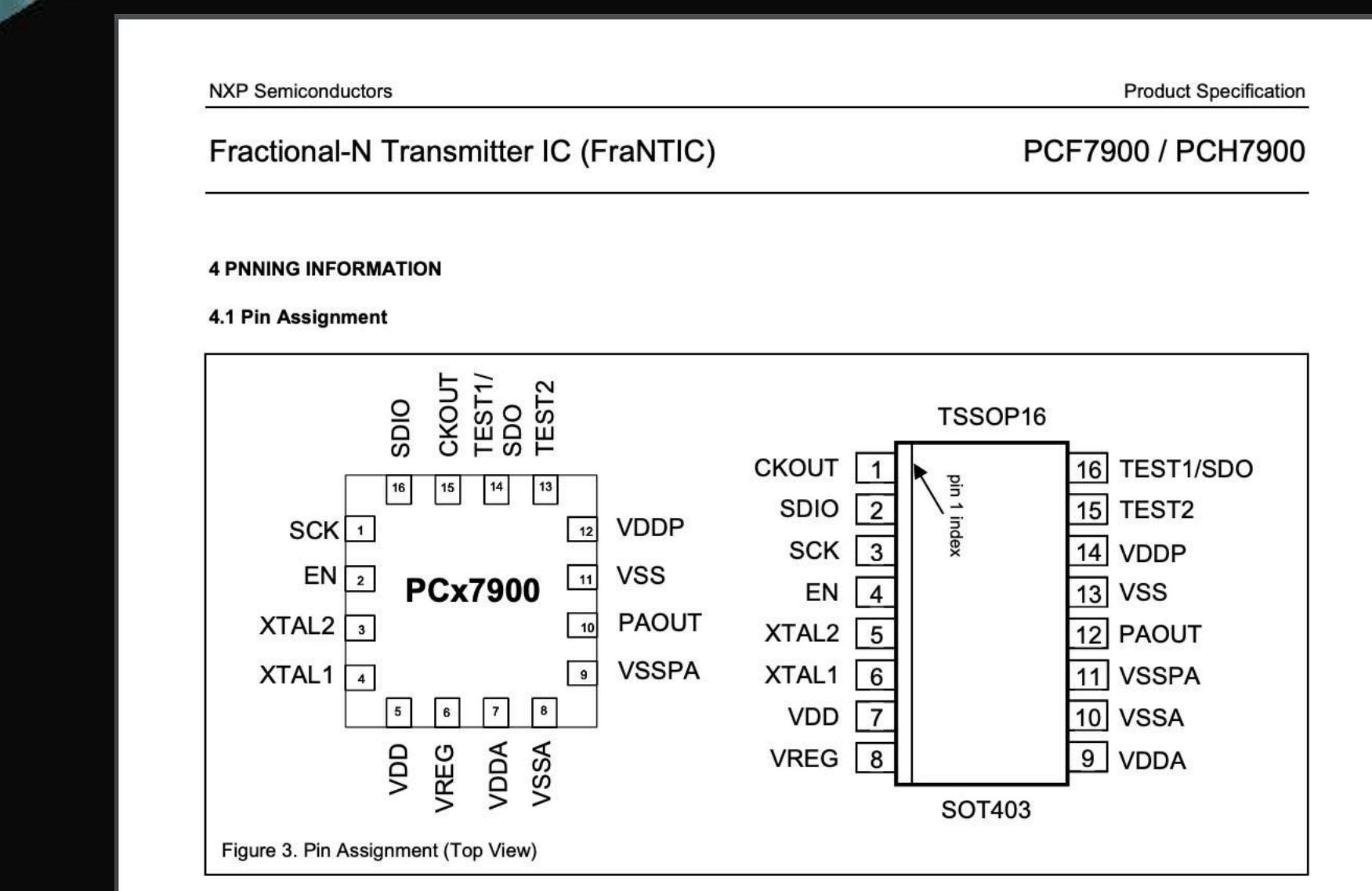
# My favorite...

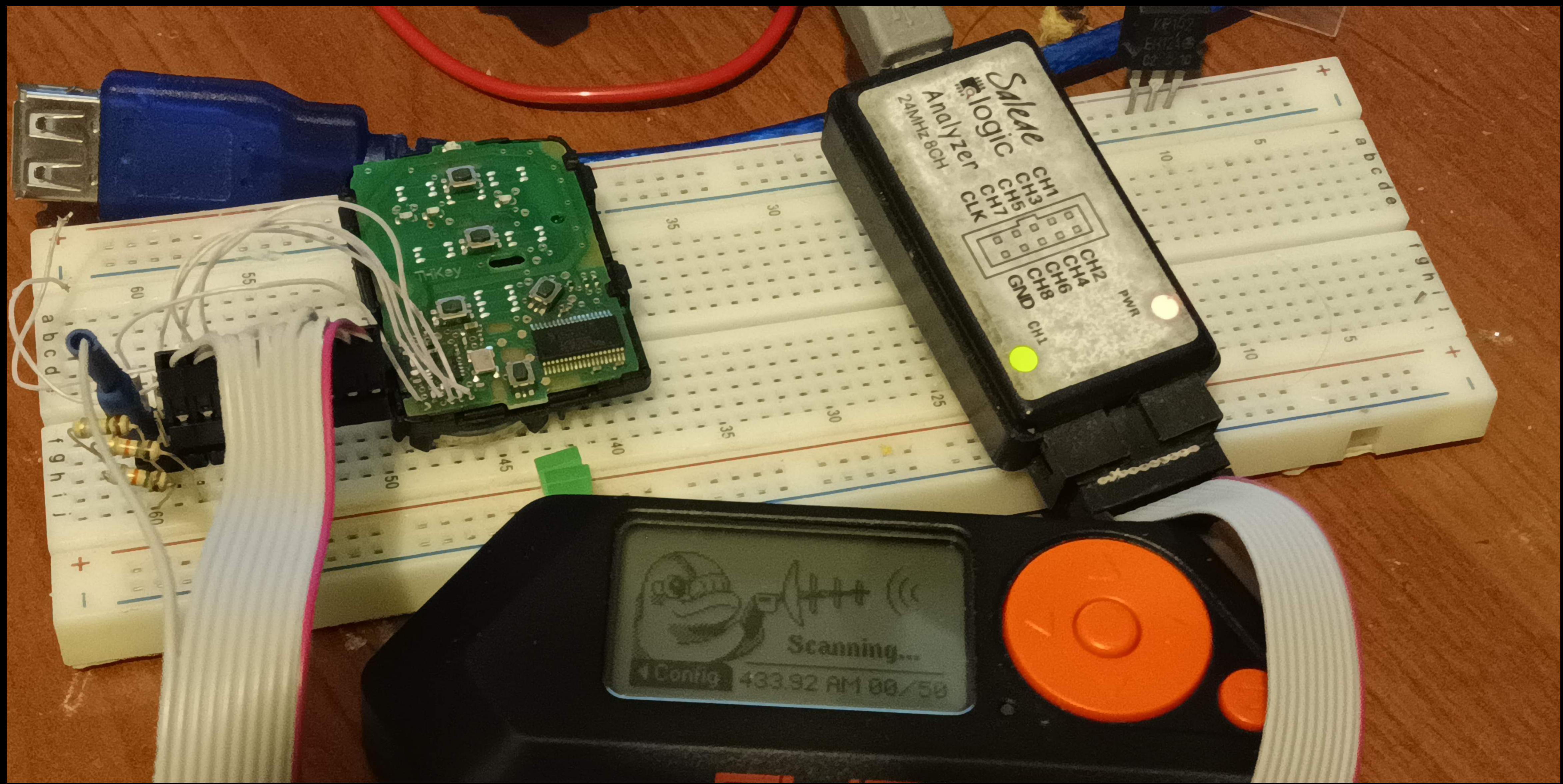




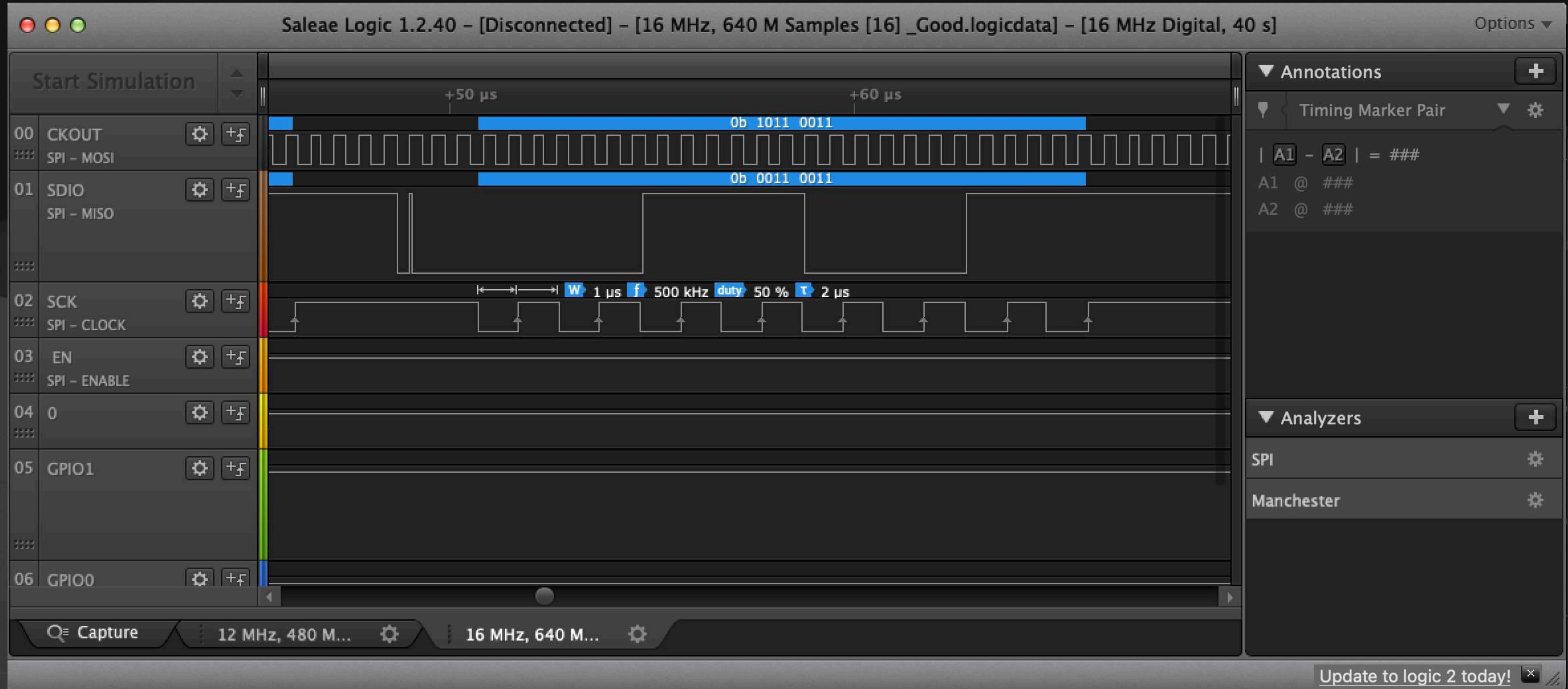
Credit : CBS News

# Digging Deeper





# Logic Analysis



# What do these numbers mean?

“It’s in the data sheet!” - Prof. Viall

datasheet-pdf.com/PDF/PCF7900-Datasheet-NXP-948789

NXP Semiconductors Product Specification

Fractional-N Transmitter IC (FraNTIC) PCF7900 / PCH7900

26

5.9.3 Transmit data command

**Transmit configuration**

Some transmit-configuration bits have to be sent via SPI before every transmit command. (A to F, see transmit data diagram).

Other configuration settings are stored in the registers and the state machine keeps its behaviour until these bits are altered.

5.9.3.1 Description of the configuration bits

**Synchronization:**

**Bit A = 1:** Synchronization of the data at the falling or at the rising edge of SCK with the baud rate clock ( $CLK_{ASC}$ ) (also dependent of register setting)

**Bit A = 0:** no synchronization of the transmit-data

**Power amplifier:**

The power amplifier is always turned on with the ninth non-significant edge of SCK. The configuration bit B is used to turn off the power amplifier.

**Bit B = 1:** The power amplifier is turned off after falling edge of EN (synchronized with baud rate, if enabled). Data is transmitted after the power amplifier is turned on. During transmission EN has to be kept 1 and the data at SDIO is transmitted transparently or synchronized with the baud rate.

**Bit B = 0:** Data transmission starts after the power amplifier is turned on. With the falling edge of EN the actual

data bit at SDIO is latched and a constant carrier will be transmitted either in NRZ mode (bit C=0) or with Manchester coding (bit C=1) until the power amplifier is turned off.

**Data Coding:**

**Bit C = 1:** Data is XOR'd (Manchester generation) with baud rate clock. If C=1 the value of "A" will be ignored and the data transmission will be done synchronized to the baud rate clock.

**Bit C = 0:** NRZ mode selected.

**Modulation and Power Settings:**

**Bit D = 1:** Modulation and amplitude/power settings of ACON1 are applied. (according to Figure 12 )

**Bit D = 0:** Modulation and amplitude/power settings of ACON0 are applied. (according to Figure 12 )

**Frequency Settings**

**Bits E, F:** selection of frequency configuration registers.

27

Table 31 Frequency Selection (Bit E, Bit F)

| Bit E | Bit F | FCON                       | Note |
|-------|-------|----------------------------|------|
| 0     | 0     | FCC1H, FCC1L, F1C16, F1C17 |      |
| 0     | 1     | FCC2H, FCC2L, F2C16, F2C17 |      |
| 1     | 0     | FCC3H, FCC3L, F3C16, F3C17 |      |
| 1     | 1     | FCC4H, FCC4L, F4C16, F4C17 |      |

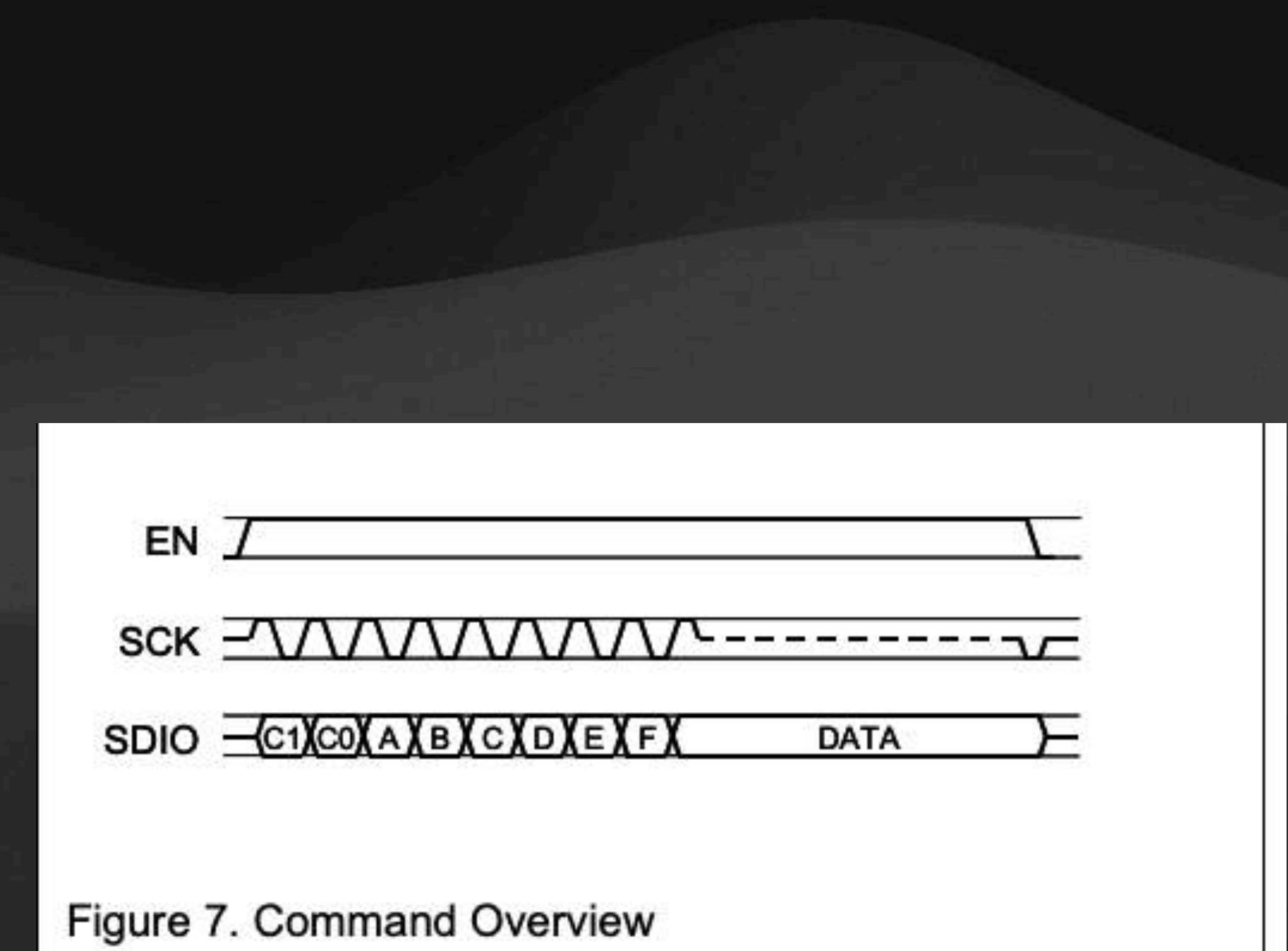
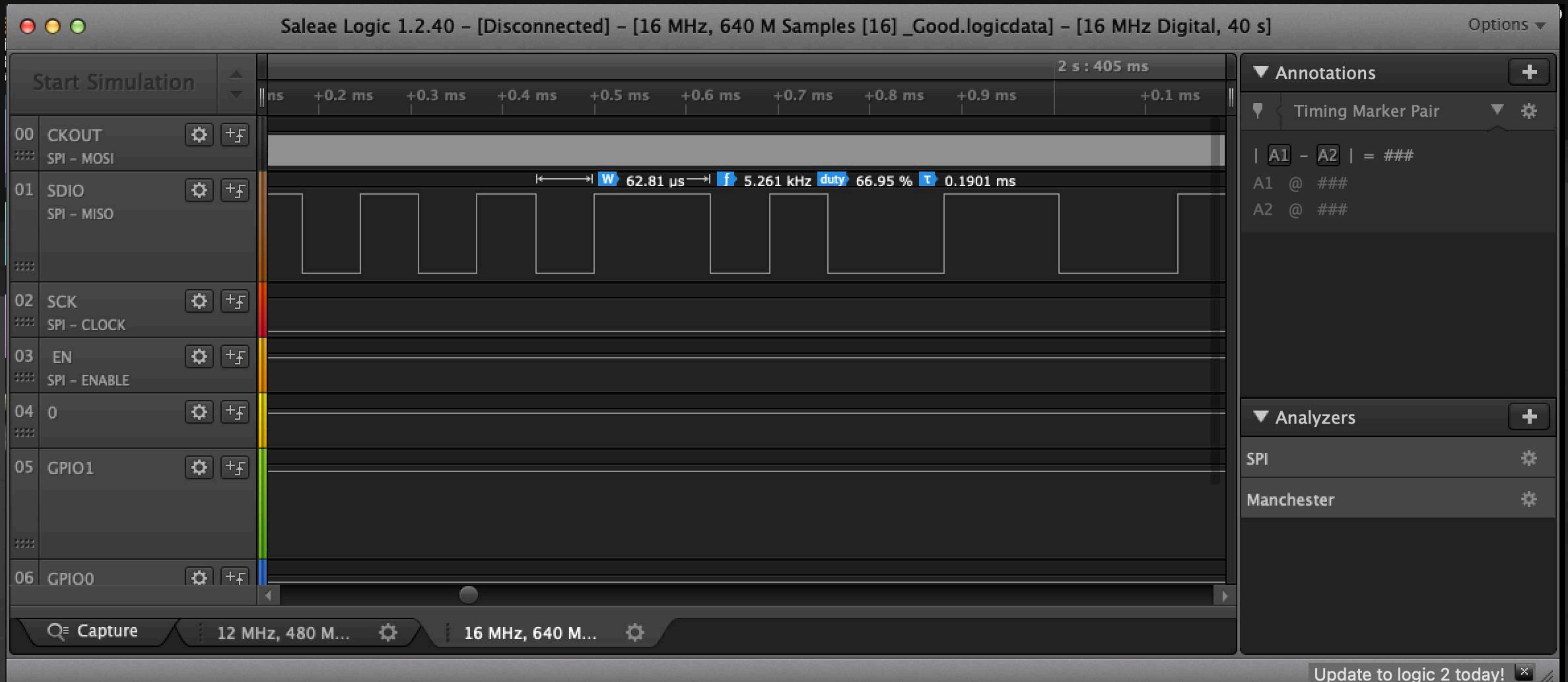


Figure 7. Command Overview

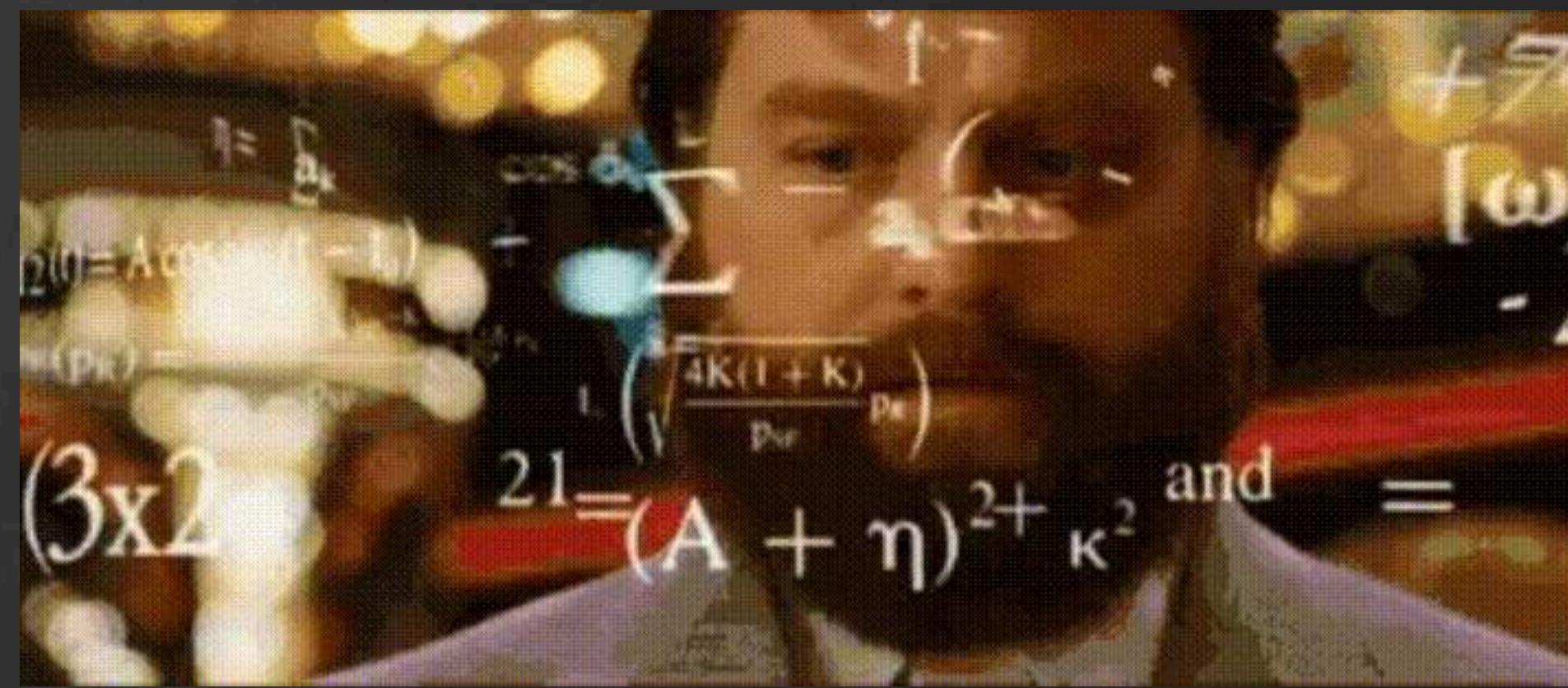
# Extracting useful information

|   |   |
|---|---|
| MISO: 0b 1000 0100 <b>FC1L</b> 01h F1C7 F1C6 F1C5 F1C4<br>F1C3 F1C2 F1C1 F1C0 | 433657070Hz   |
| MISO: 0b 1011 0001 <b>FC2L</b> 03h F2C7 F2C6 F2C5 F2C4<br>F2C3 F2C2 F2C1 F2C0 | 434176948Hz   |
| MISO: 0b 0001 0100 <b>FCON</b> 09h FSK7 FSK6 FSK5 FSK4<br>FSK3 FSK2 FSK1 FSK0 | FSK modulation, with deviation =+- 15968Hz              |
| MISO: 0b 0011 0011 <b>BDSEL</b>   | DIV_bd=51 , Baud rate= CLK/(2*(DIV_bd+1))= 15380 s /sec |

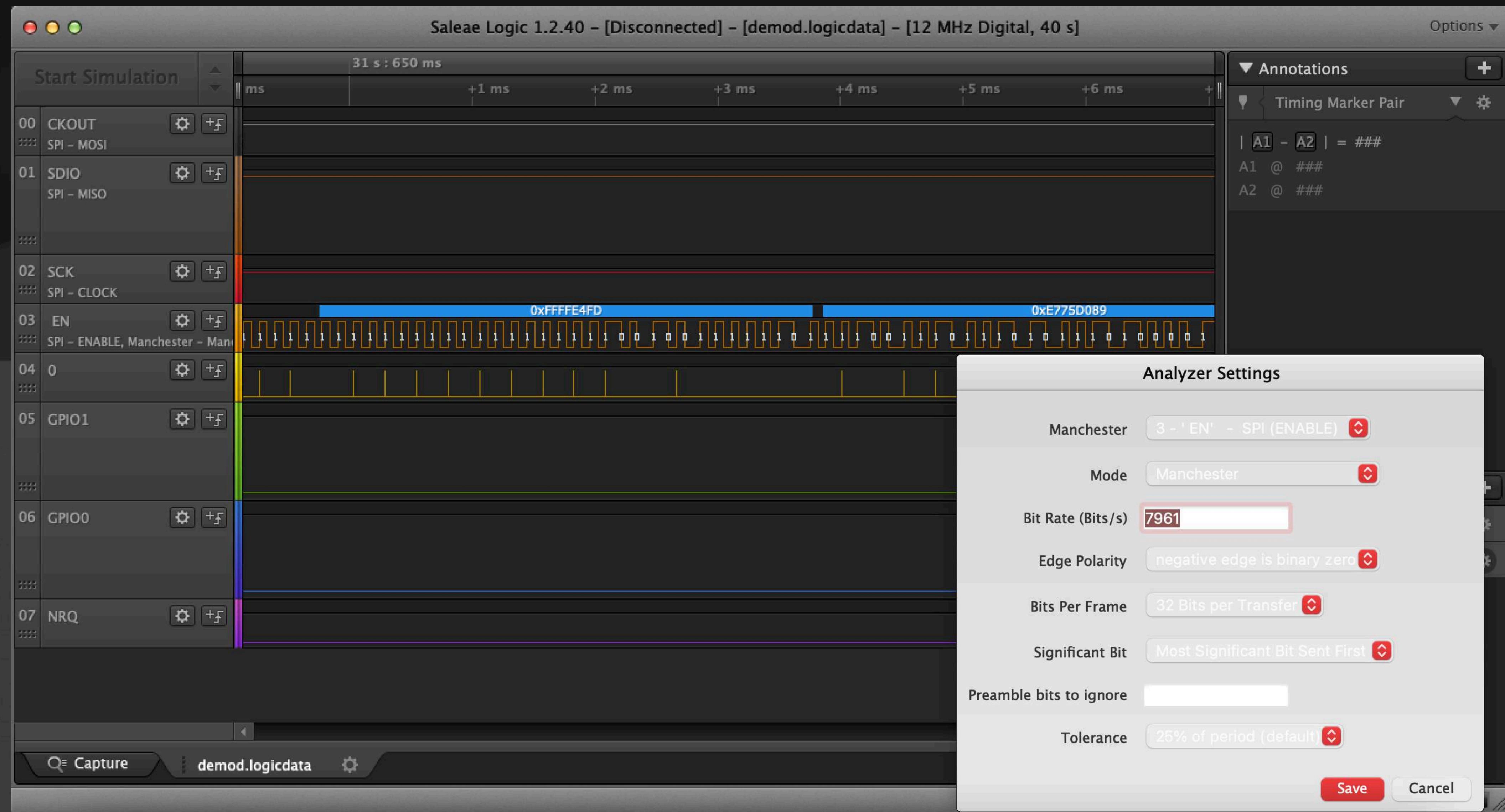
# Calculating Manchester bit rate



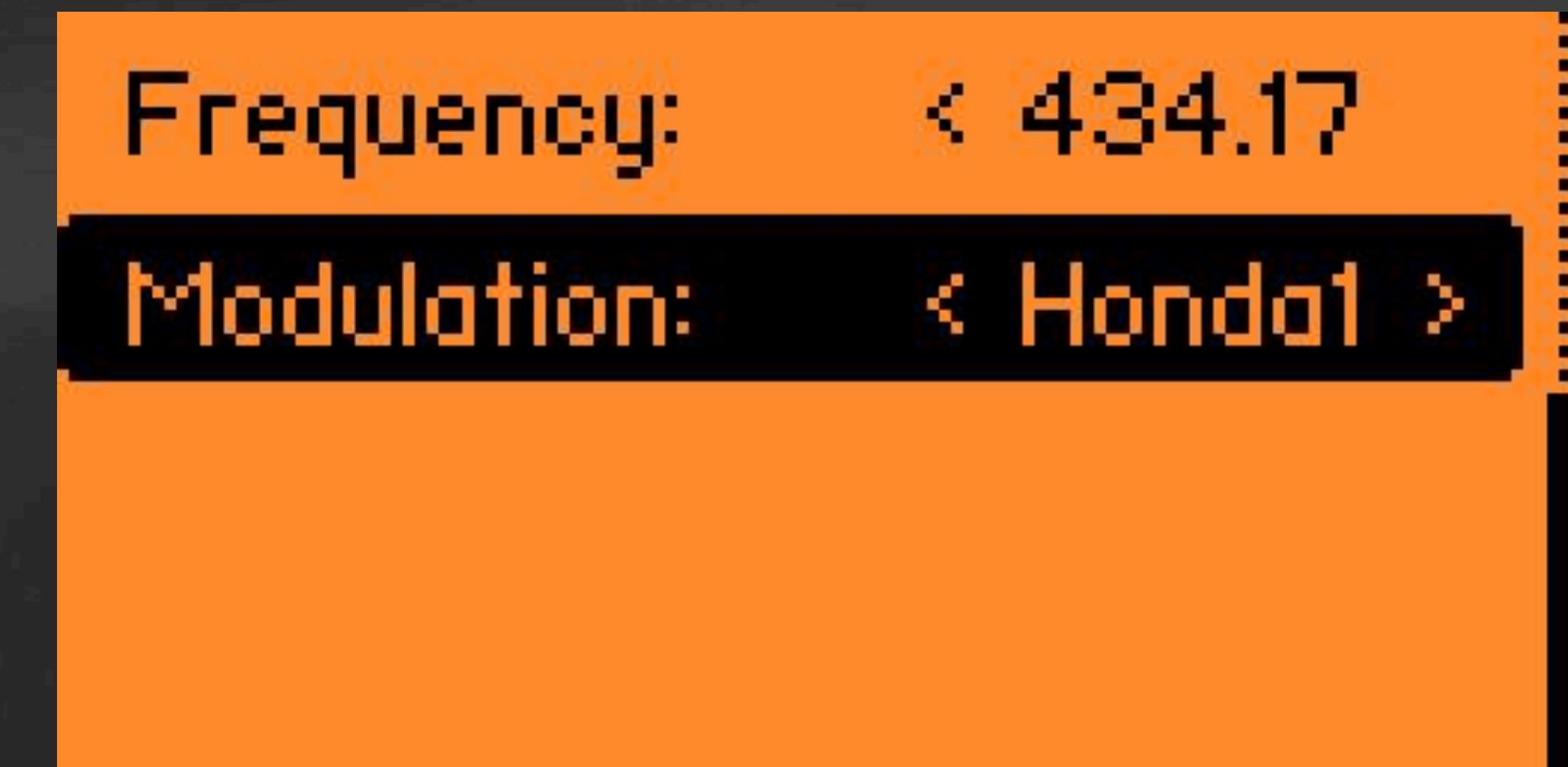
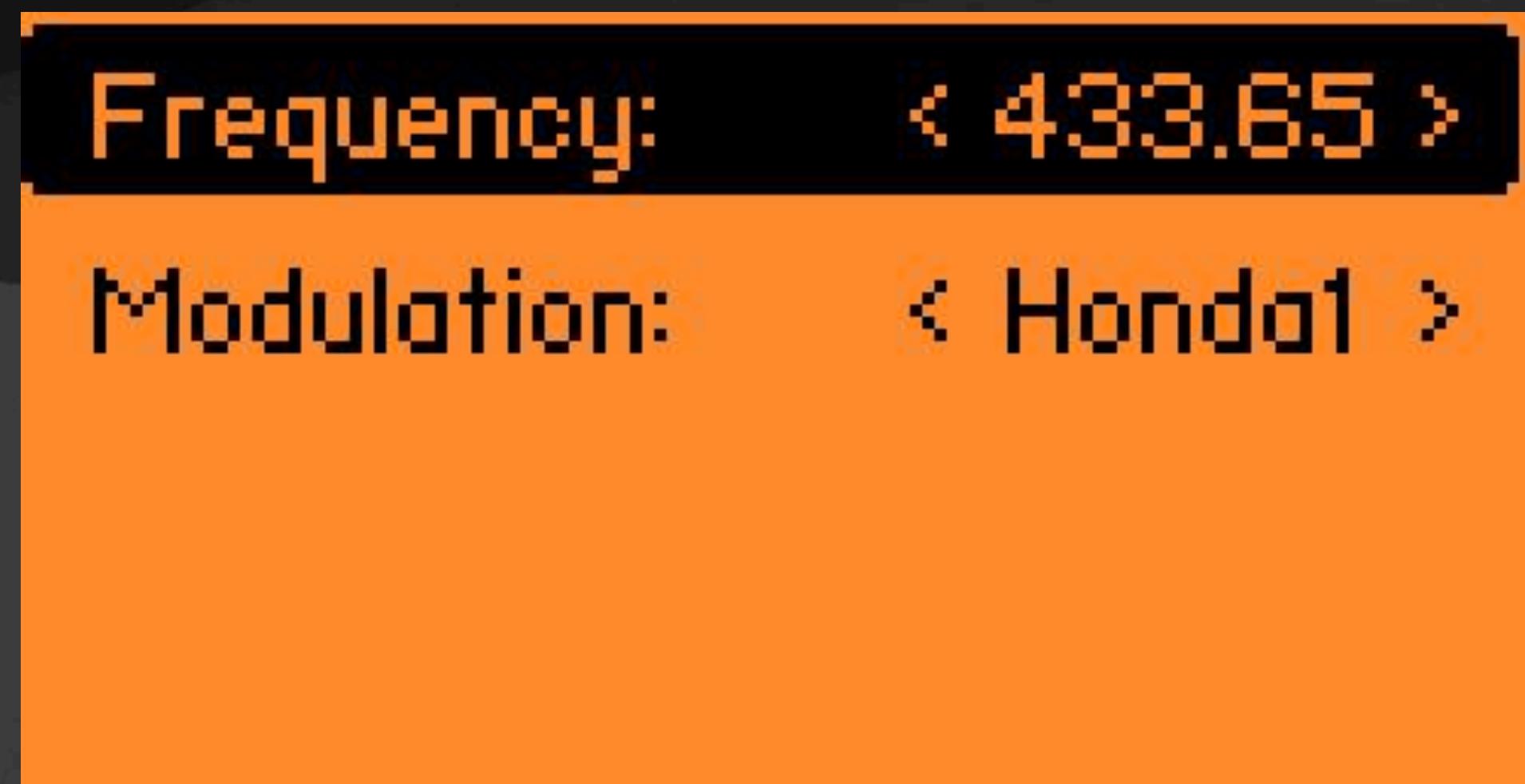
$$\text{Manchester Bit Rate} = \frac{\frac{1 \text{ second}}{\text{Shortest duration}}}{2} = \frac{\frac{1000000 \mu\text{s}}{62.81 \mu\text{s}}}{2} = \frac{15,921.032}{2} = 7960.516 \approx 7961 \text{ Kilobytes per second.}$$



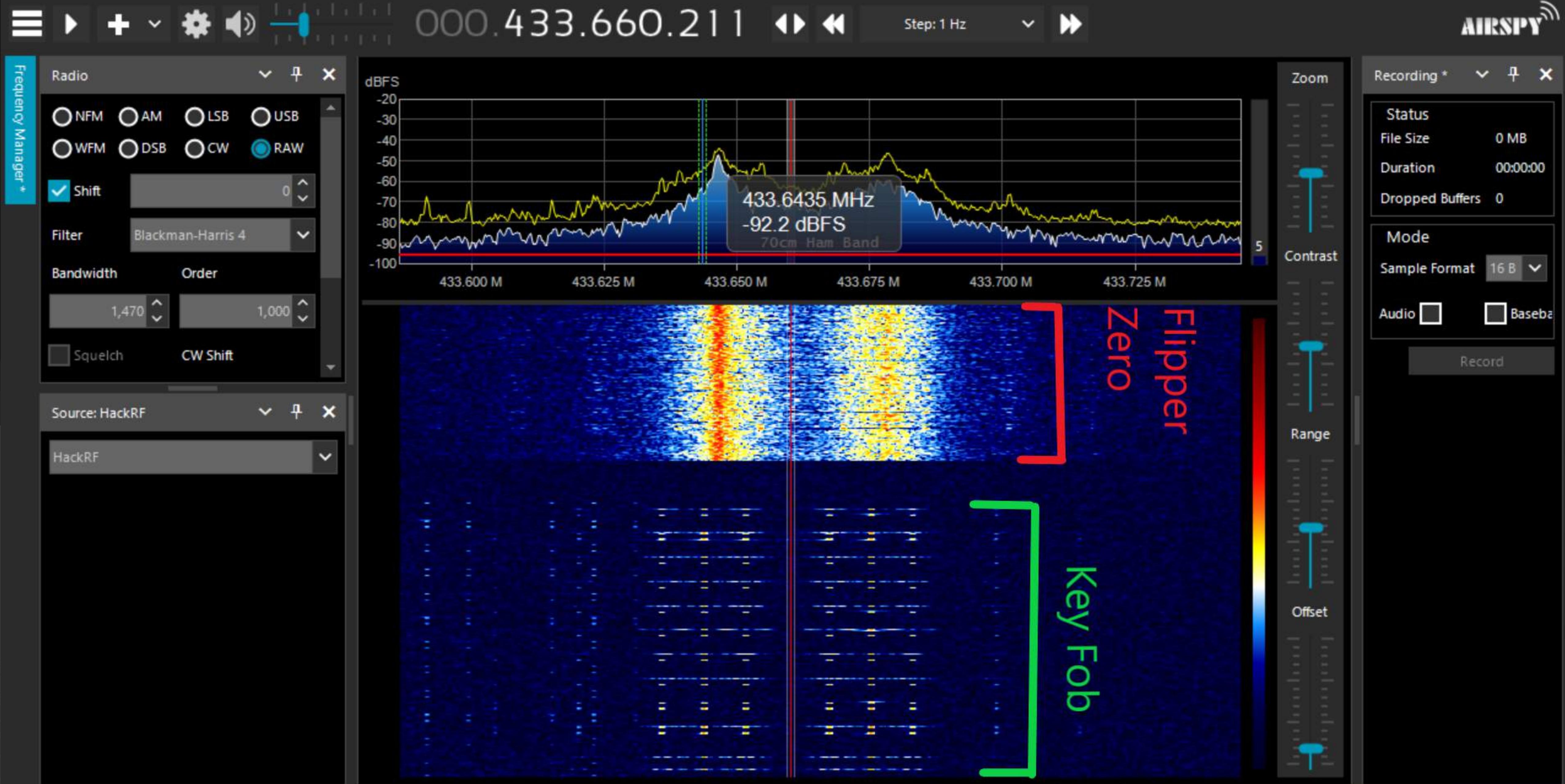
# Decoding Manchester



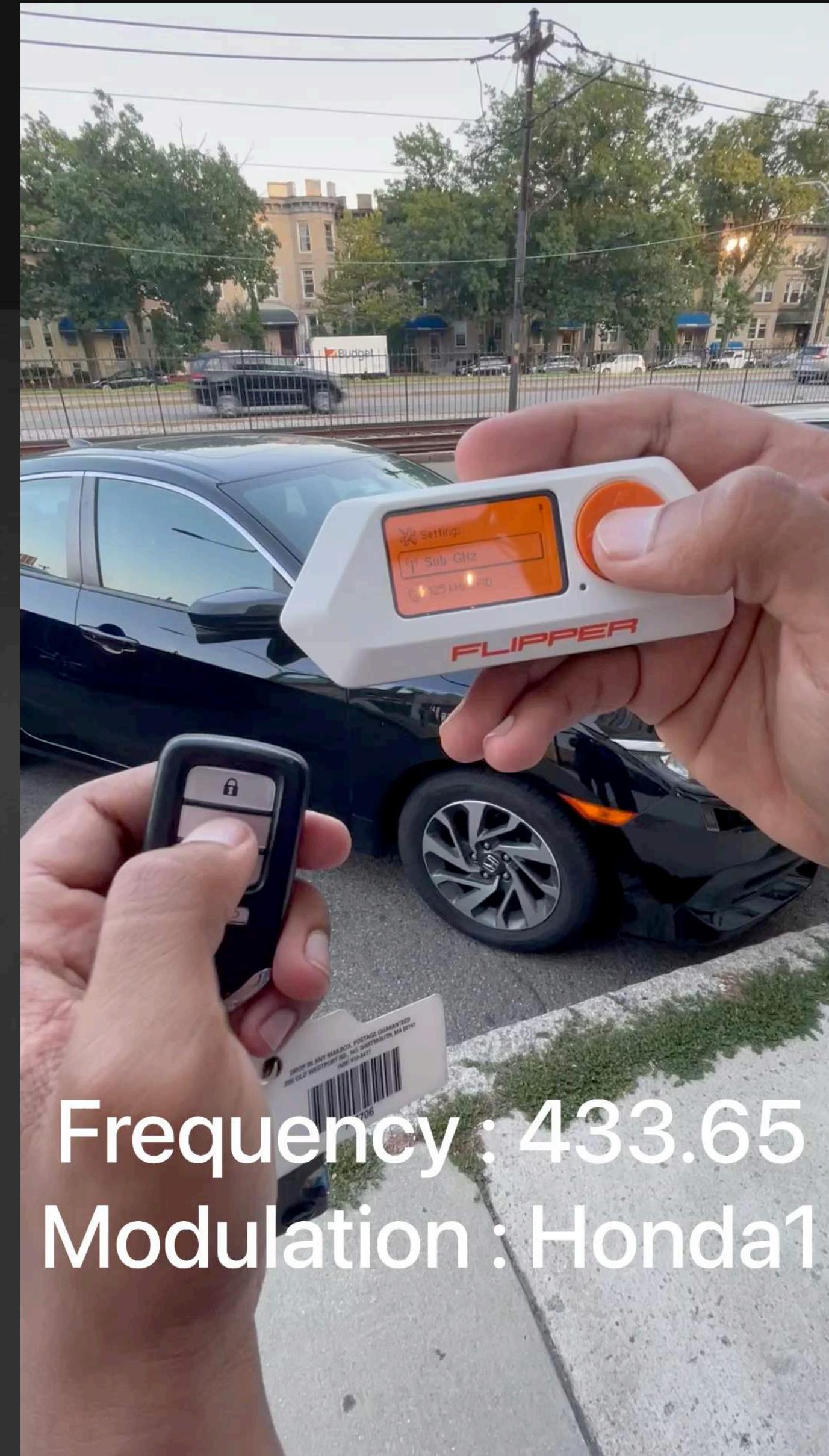
# Adding support for our cyber-dolphin friend : Flipper Zero



Captured using QFlipper App

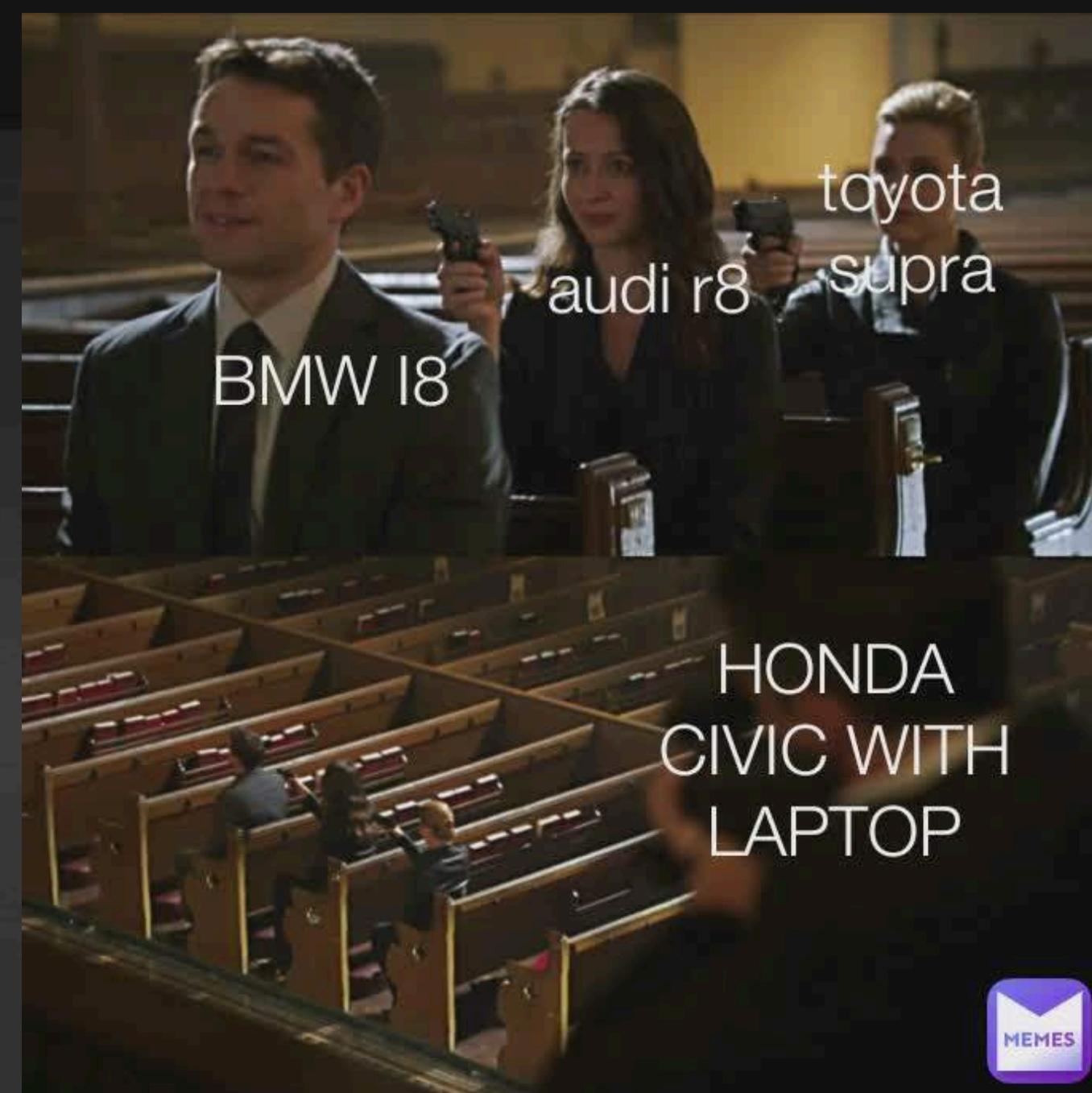
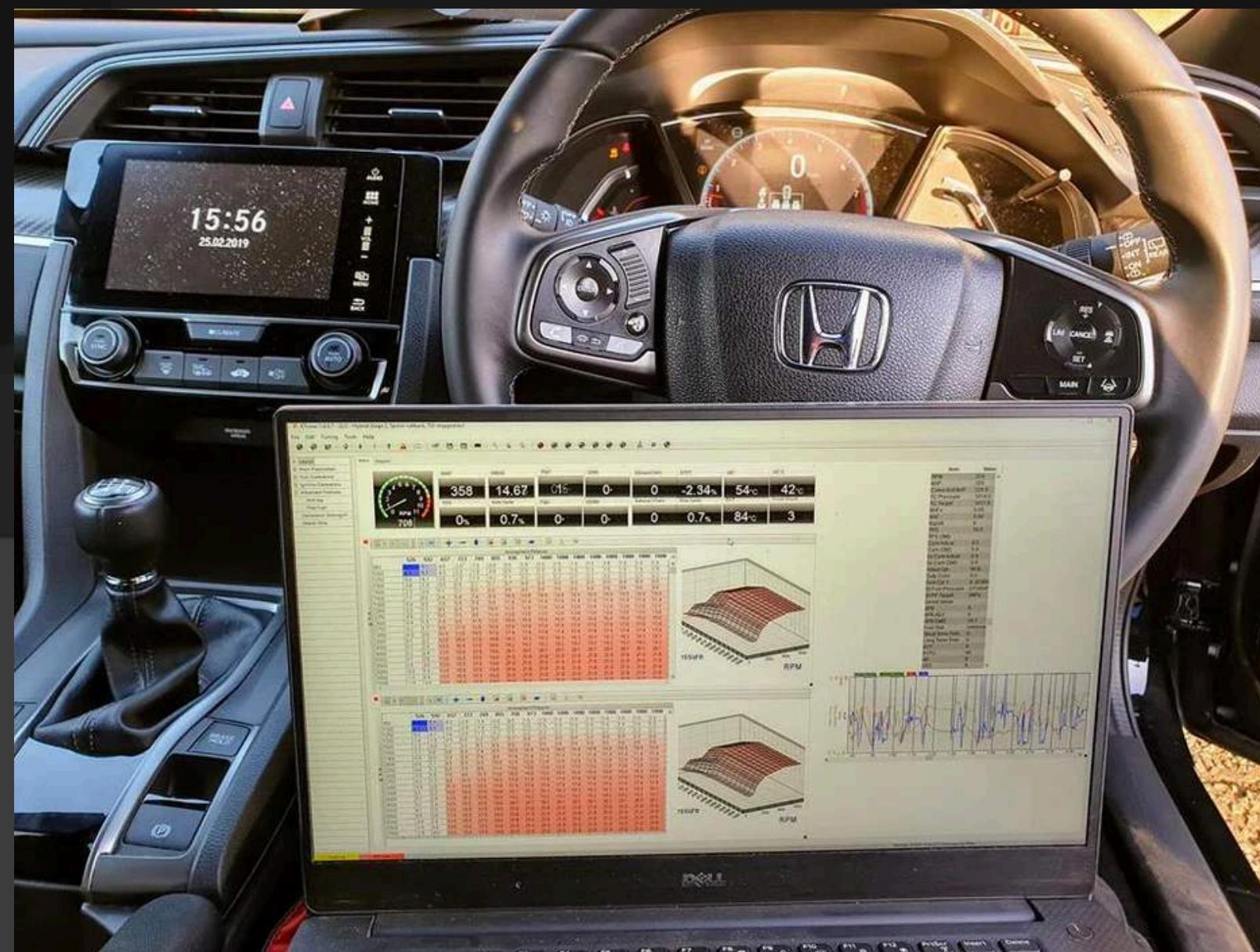


# Flipper Zero Demo



Frequency : 433.65  
Modulation : Honda1

# "Civic with a laptop. The most feared thing in the car community"



Hint: Google the title!

# The Ultimate Wardriving Setup

"Civic with a laptop, and a HackRF One"





# Solution?

Rolling codes, they're safer...right?



# Rolling Codes pwned too?!

**Honda redesigning latest vehicles to address key fob vulnerabilities**

C [therecord.media/honda-redesigning-latest-vehicles-to-address-key-fob-vulnerabilities...](https://therecord.media/honda-redesigning-latest-vehicles-to-address-key-fob-vulnerabilities/) Bookmark Puzzle

**Cybercrime** **News** **Technology**

Honda said it is addressing a spate of recently-discovered vulnerabilities in its newly designed models after researchers found bugs affecting the key fob systems in its vehicles dating back to 2012.

Earlier this year, Honda was [forced to address CVE-2022-27254](#) – a replay vulnerability affecting the Remote Keyless System in Honda Civics made between 2016 and 2020. That bug allowed researchers to eavesdrop on the unencrypted radio frequency signal and recreate it, giving them the ability to open and start vehicles.

In an effort to deal with this issue, Honda and other car manufacturers developed a rolling code system in keyless entry systems that mitigates this vulnerability by using a [Pseudorandom Number Generator](#) (PRNG) to create several different codes between the key fob and the car.

But this week, security researchers from Star-V Lab [released a report](#) showing how the rolling code system could be exploited.

The researchers found a way to effectively capture the different codes generated by the PRNG and use them to eventually open the vehicle.

They tested the 10 most popular models of Honda released since 2012 and found all were susceptible to the attack, leading them to claim all Honda models are vulnerable.

# Rolling Pwn Demo



Video Credits: @Kevin2600

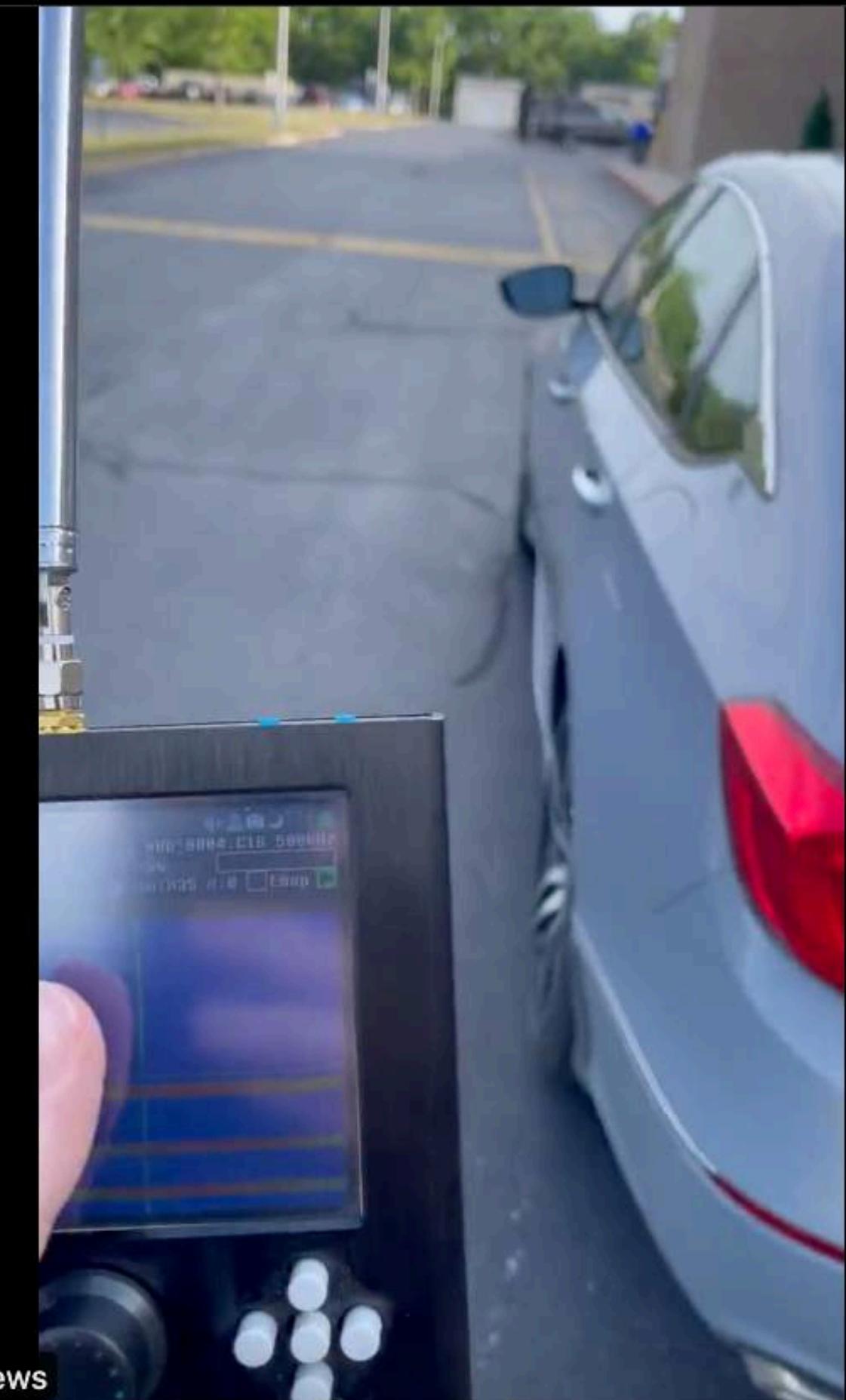


Rob Stumpf   
@RobDrivesCars

...

I was able to replicate the Rolling Pwn exploit using two different key captures from two different times.

So, yes, it definitely works.



0:39 70.6K views

claimed it is not a new discovery and doesn't merit any further reporting.

Martin confirmed that "legacy technology utilized by multiple automakers" may be vulnerable to "determined and very technologically sophisticated thieves."

"Honda has not verified the information reported by researchers and cannot confirm if its vehicles are vulnerable to this type of attack. Honda has no plan to update older vehicles at this time," Martin said.

"It's important to note, while Honda regularly improves security features as new models are introduced, determined and technologically sophisticated thieves are also working to overcome those features. Further, access to a vehicle without other means to drive the vehicle, while hi-tech in nature, does not provide thieves an advantage much greater than more traditional and certainly easier ways to gain entry to a vehicle. And there is no indication that the type of device in question is widely used."

Martin told The Record that if started remotely, Acura and Honda vehicles cannot be driven until a valid key fob with a separate immobilizer chip is present in the vehicle. He added that there is "no indication that the reported vulnerability to door locks has resulted in an ability to actually drive an Acura or Honda vehicle."

Vulcan Cyber's senior technical engineer Mike Parkin said rolling codes were evolved, in part, to deal with the barrage of door openers being susceptible to simple drive-by attacks.

"The surprise is that any major manufacturer would implement an insecure remote opening system. There are several theoretical attacks against current remote controls, some of which have been shown in proof-of-concept form," Parkin said.



**CHALLENGE  
ACCEPTED**

# Gone in 4 minutes





Search or jump to...

/ Pull requests Issues Marketplace Explore

bell + ⌂ profile

(shipcod3 / canTot) Public

Watch 1

Fork 7

Starred 21

Code Issues Pull requests Actions Projects Wiki Security Insights

main

2 branches

0 tags

Go to file

Add file

Code

## About

quick and dirty canbus h4xing framework

canbus car-hacking  
automotive-security

- Readme
- View license
- Code of conduct
- 20 stars
- 1 watching
- 7 forks

|   |                             |                      |            |
|---|-----------------------------|----------------------|------------|
|  shipcod3            | Update README.md            | 94ea8d5 17 hours ago | 15 commits |
|  banners             | Open sourcing canTot now    | 22 days ago          |            |
|  commands            | Update commands.py          | 12 days ago          |            |
|  modules             | Add carfucar to the credits | 21 days ago          |            |
|  .gitignore          | Open sourcing canTot now    | 22 days ago          |            |
|  CODE_OF_CONDUCT.... | Update CODE_OF_CONDUCT.md   | 9 days ago           |            |
|  CONTRIBUTING.md     | Create CONTRIBUTING.md      | 9 days ago           |            |
|  LICENSE.md          | Open sourcing canTot now    | 22 days ago          |            |
|  README.md           | Update README.md            | 17 hours ago         |            |

[NEWS | PRESS](#)

JULY 20, 2022

# SENATOR MARKEY URGES AUTOMAKERS TO REVIEW SAFETY OF KEYLESS SYSTEMS AS TECH-SAVVY THIEVES CIRCUMVENT LOCKS

Washington (July 20, 2022) – Senator Edward J. Markey (D-Mass.), a member of the Commerce, Science, and Transportation Committee, sent letters to 17 major automakers today urging them to review information and standards for their keyless entry systems, which allow users to enter a vehicle and start its engine without inserting and turning a key. Mounting evidence suggests these systems may be contributing to rising rates of vehicle theft across the country, including through ‘relay attacks’ in which a thief uses a signal amplifier to fool the car into believing the owner is nearby.

# What Next?

Join us on this journey!

- Grab a free CVE-2022-27254 or RollingPwn sticker at DEFCON! (Limited availability)
- Help us create a list of every vulnerable vehicle! Sign up at <https://forms.gle/duNtw2UcmPgTdRPM9> or by scanning the QR code below!
- Stop by the Car Hacking Village to grab a copy of the Flipper Zero custom firmware!
- Follow @CarHackVillage on Twitter, for updates on when we will be doing a live demo!



# Thank you!



 College of Engineering  
UMass Dartmouth



# References / Further Reading

- <http://opengarages.org/handbook/ebook/>
- [https://medium.com/@victor\\_14768/replay-attacks-en-autos-206481dcfee1](https://medium.com/@victor_14768/replay-attacks-en-autos-206481dcfee1)
- [https://www.researchgate.net/figure/Rolling-Code-Overview\\_fig2\\_336715499](https://www.researchgate.net/figure/Rolling-Code-Overview_fig2_336715499)
- <https://fccid.io>
- <https://rollingpwn.github.io>
- <https://therecord.media/honda-redesigning-latest-vehicles-to-address-key-fob-vulnerabilities/>
- <https://therecord.media/honda-downplays-vulnerability-allowing-hackers-to-lock-unlock-and-start-civics/>
- <https://www.cnbc.com/2019/11/09/the-demise-of-the-car-key-tesla-lincoln-ditch-keys-for-mobile-entry.html>
- <https://www.youtube.com/watch?v=kuubkTDAxwA>
- [https://www.reddit.com/r/Ubuntu/comments/o8ed5i/never\\_race\\_a\\_honda\\_with\\_a\\_laptop/](https://www.reddit.com/r/Ubuntu/comments/o8ed5i/never_race_a_honda_with_a_laptop/)
- <https://memes.com/m/toyota-supra-audi-r8-bmw-i8-honda-civic-with-5r4MQOxvwRV>
- <https://www.tpwengineering.com/products/honda-civic-fk7-2015-remapping>
- <https://youtu.be/OgJCPQOZvEQ?t=7>
- <https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty>
- [https://www.researchgate.net/figure/Digital-modulation-schemes-ASK-FSK-and-PSK\\_fig3\\_303471153](https://www.researchgate.net/figure/Digital-modulation-schemes-ASK-FSK-and-PSK_fig3_303471153)
- <https://www.cbsnews.com/boston/news/scituate-snow-sunroof-open-weather-minivan/>
- [https://www.youtube.com/watch?v=yHoxOMXK\\_fY](https://www.youtube.com/watch?v=yHoxOMXK_fY)
- <https://www.safercar.gov/vehicle-theft-prevention>