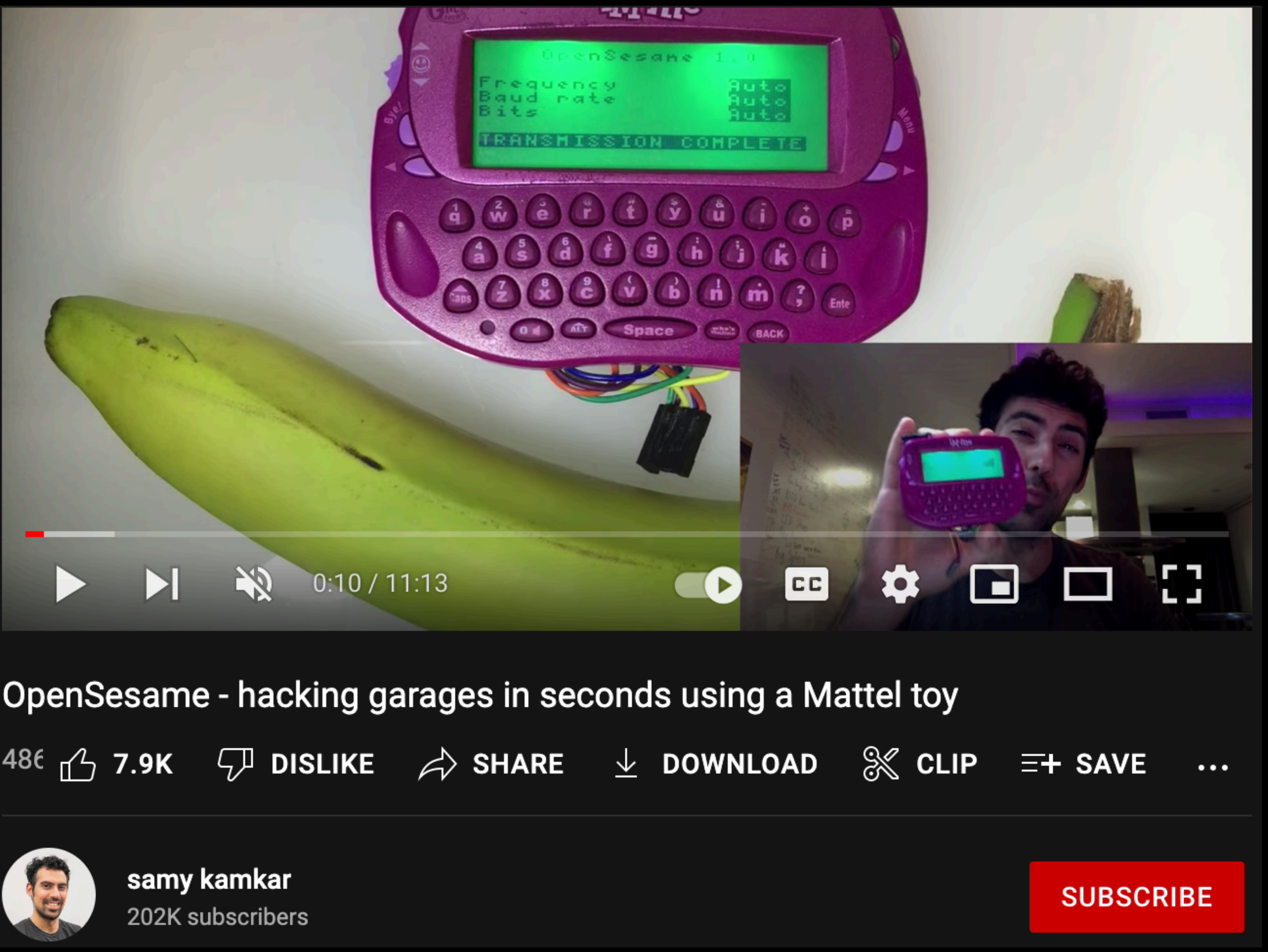
Security Like The ‘80s : How I stole your RF

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

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

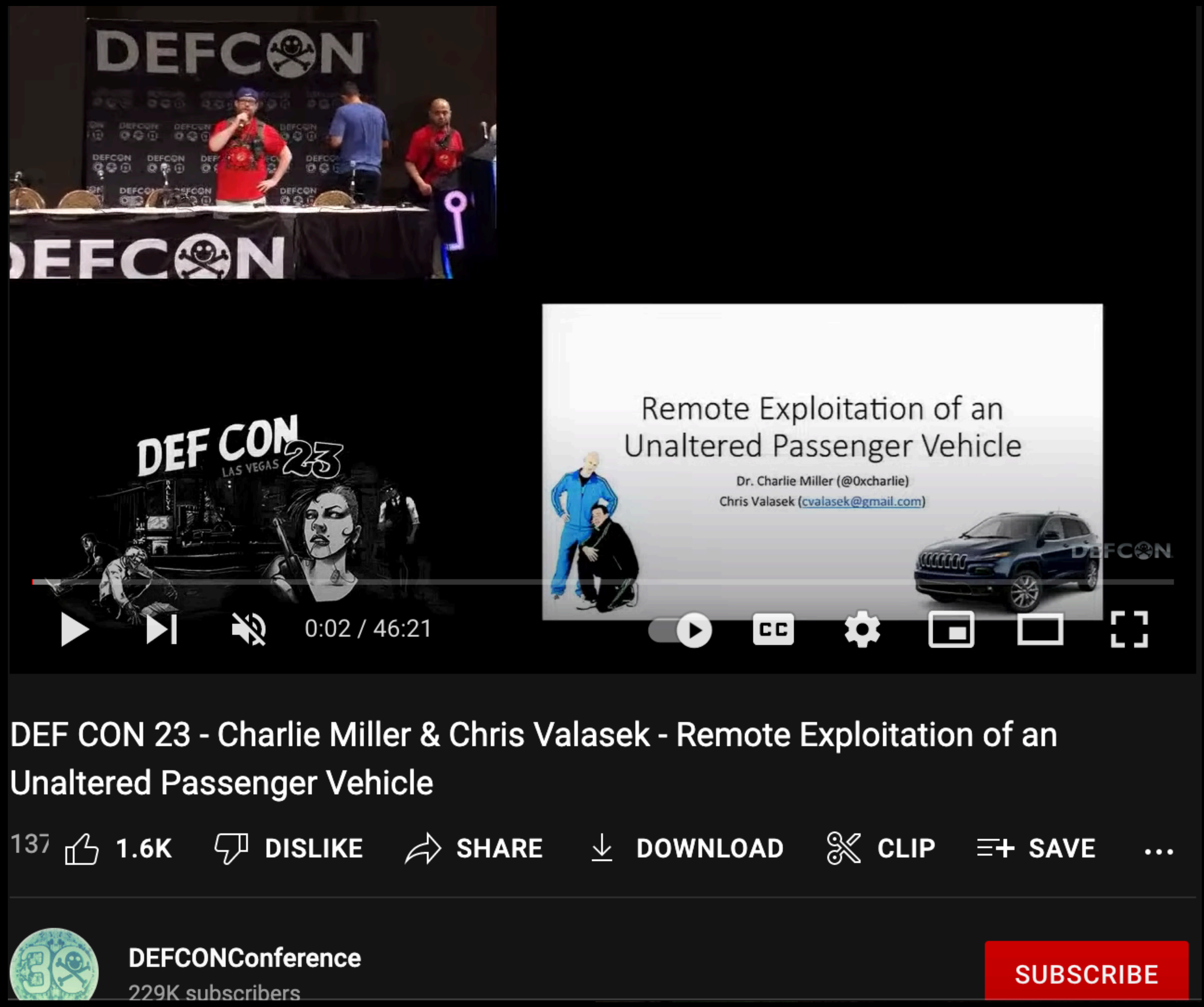


OpenSesame - hacking garages in seconds using a Mattel toy

samy kamkar
202K subscribers

Radio Hacking: Reverse Engineering Protocols Part 1 - Hak5 1913

Hak5
806K subscribers



Remote Exploitation of an Unaltered Passenger Vehicle
Dr. Charlie Miller (@0xcharlie)
Chris Valasek (cvalasek@gmail.com)

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

DEFCONConference
229K subscribers

Disclaimer

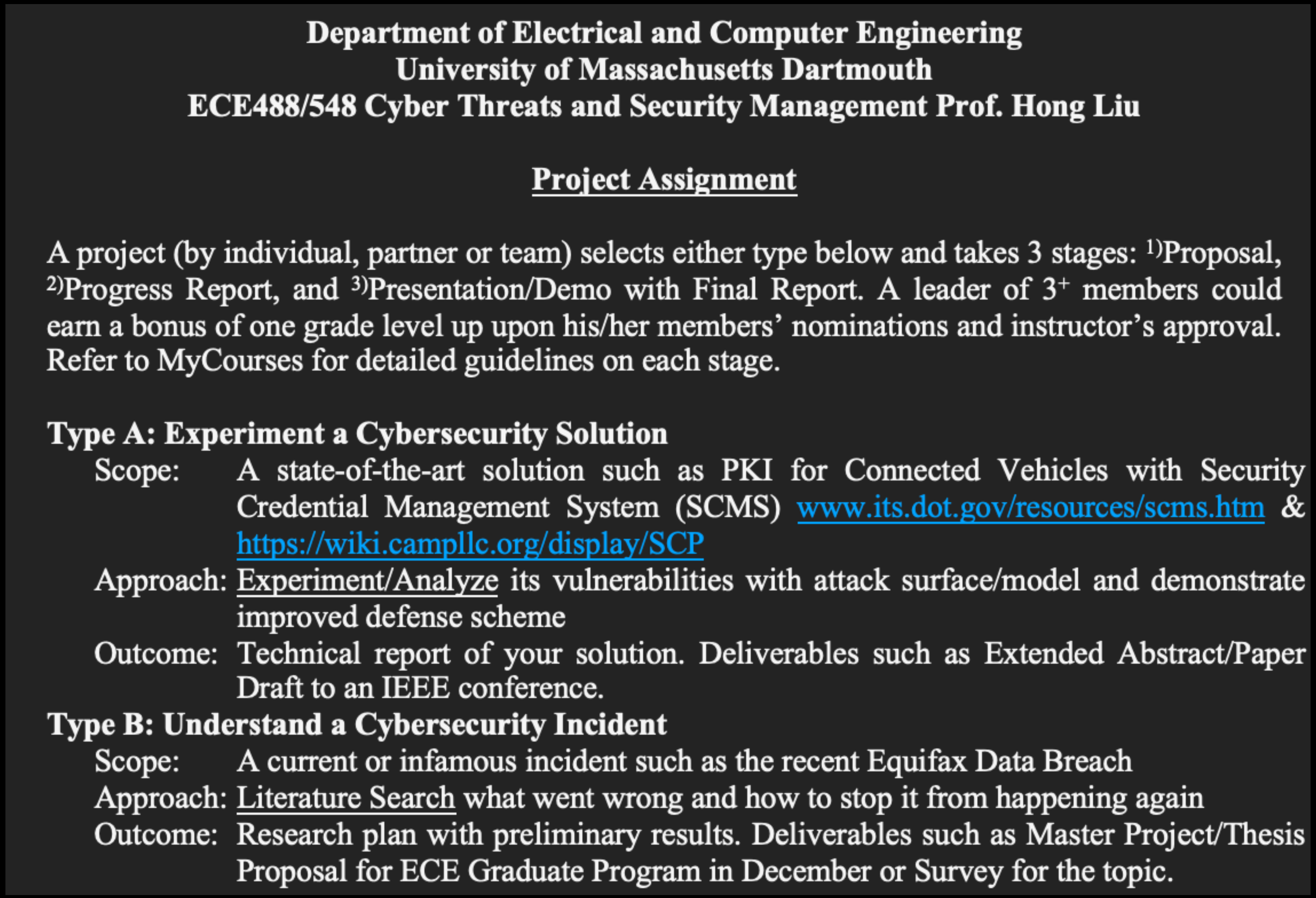
This presentation is for informational and educational purpose only. All demonstrations/videos shown in here were done only on personal vehicles, or with explicit permission from the owner. You shall not misuse the information to gain unauthorized access. This disclaimer may amended, updated or otherwise 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: $^{1)}$Proposal, $^{2)}$Progress Report, and $^{3)}$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 & 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

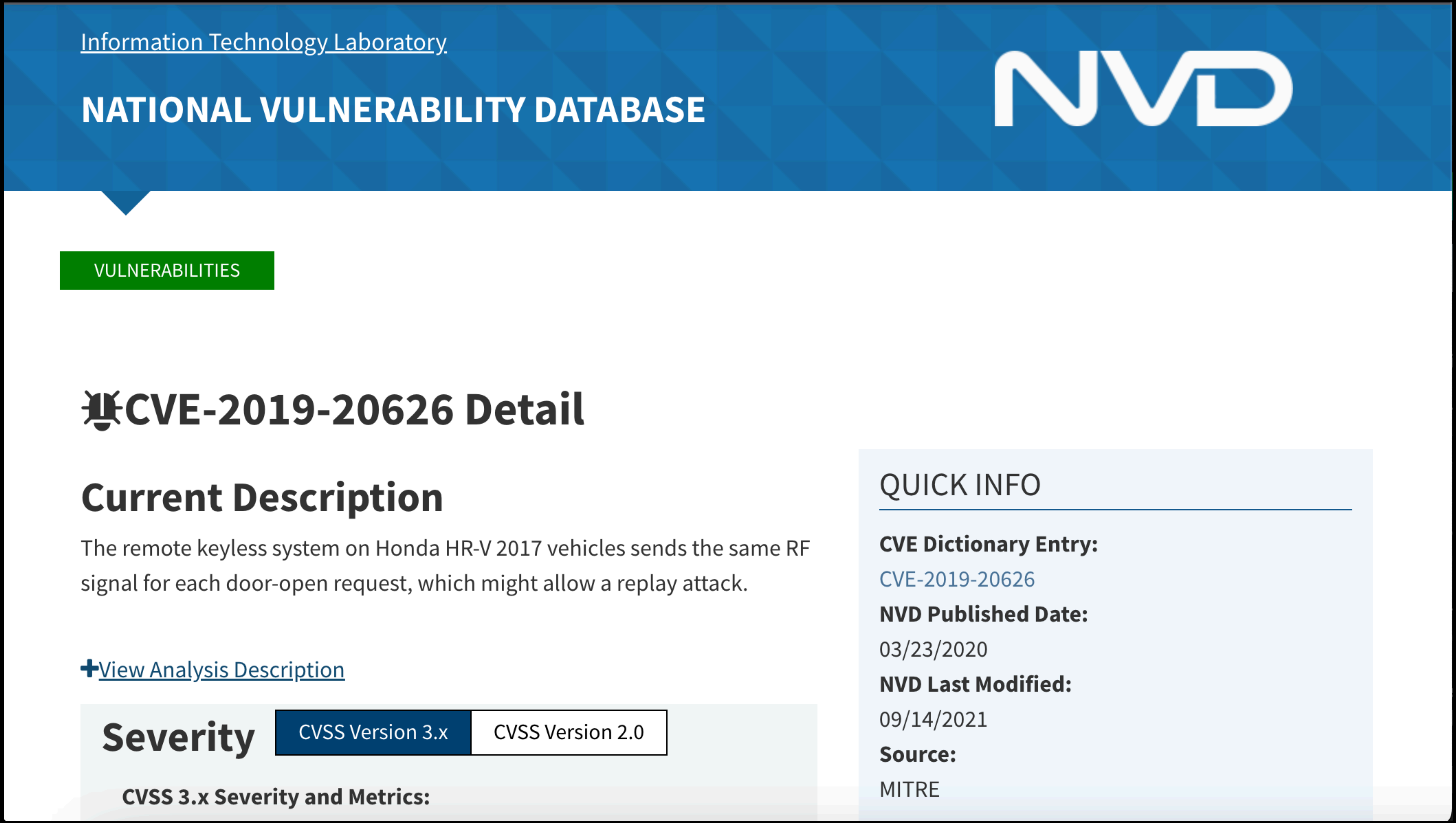
Scope: A current or infamous incident such as the recent Equifax Data Breach

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?!



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2019-20626 Detail

Current Description

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.

+View Analysis Description

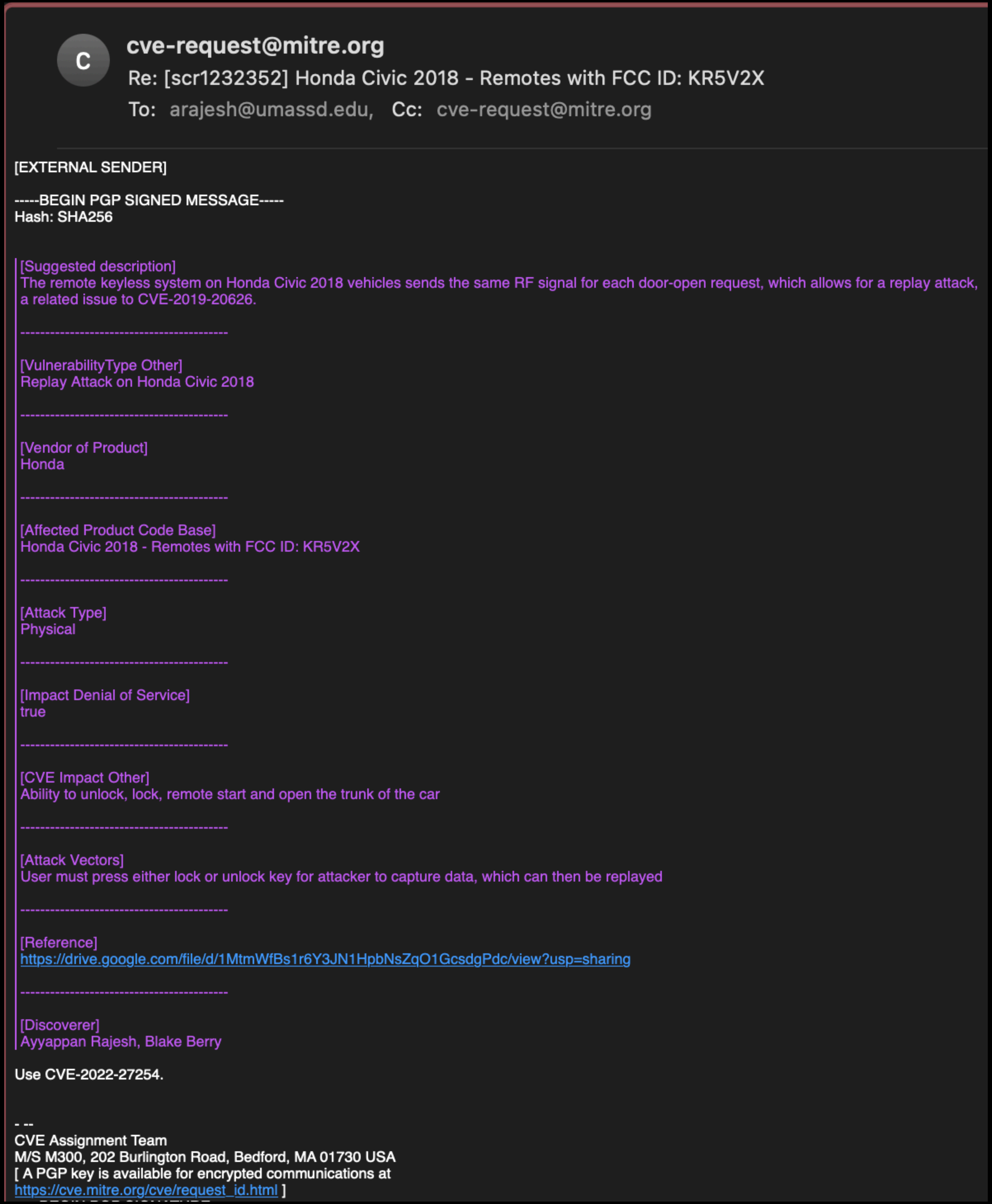
Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

QUICK INFO

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

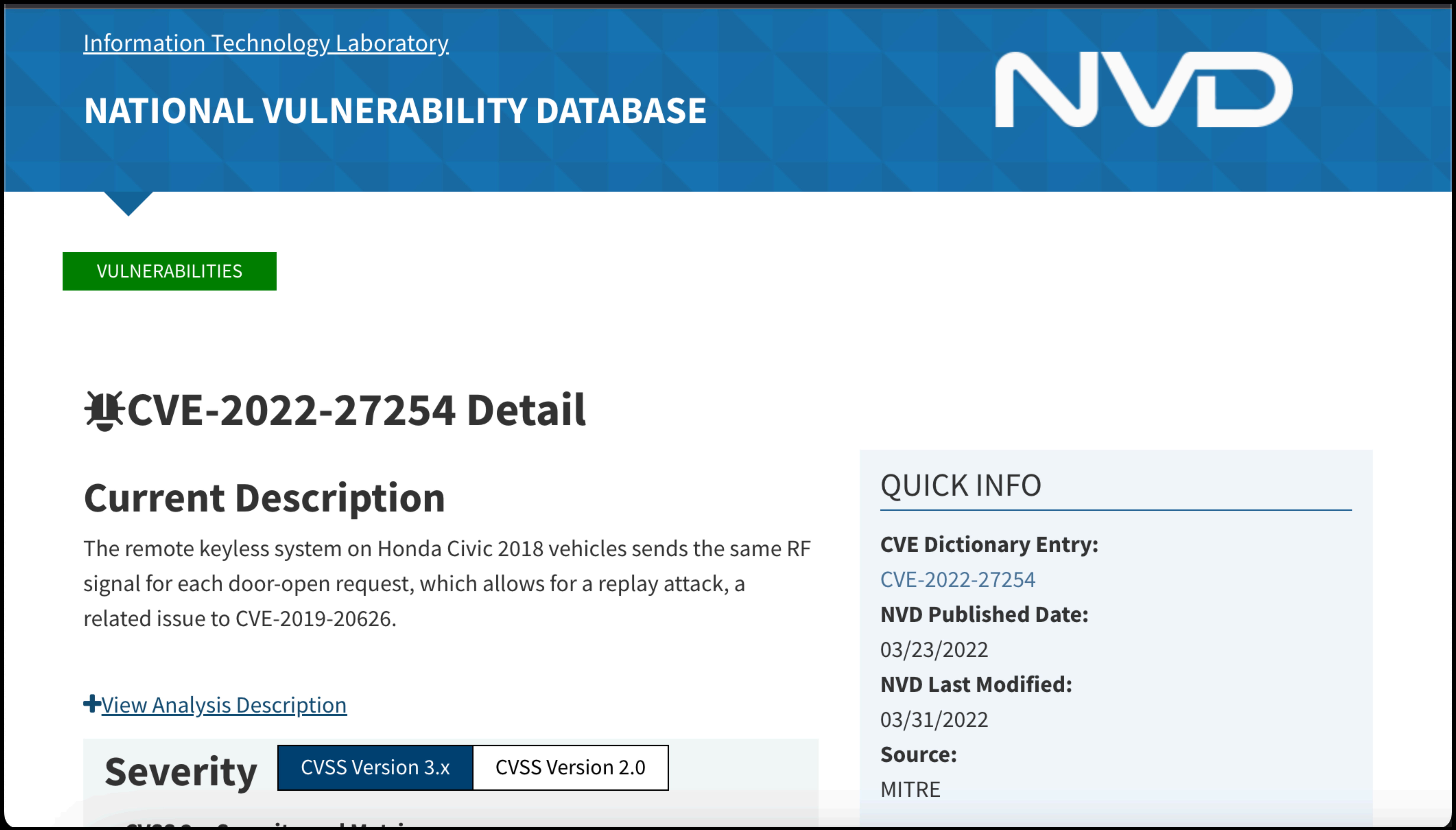
[EXTERNAL SENDER]

-----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]



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

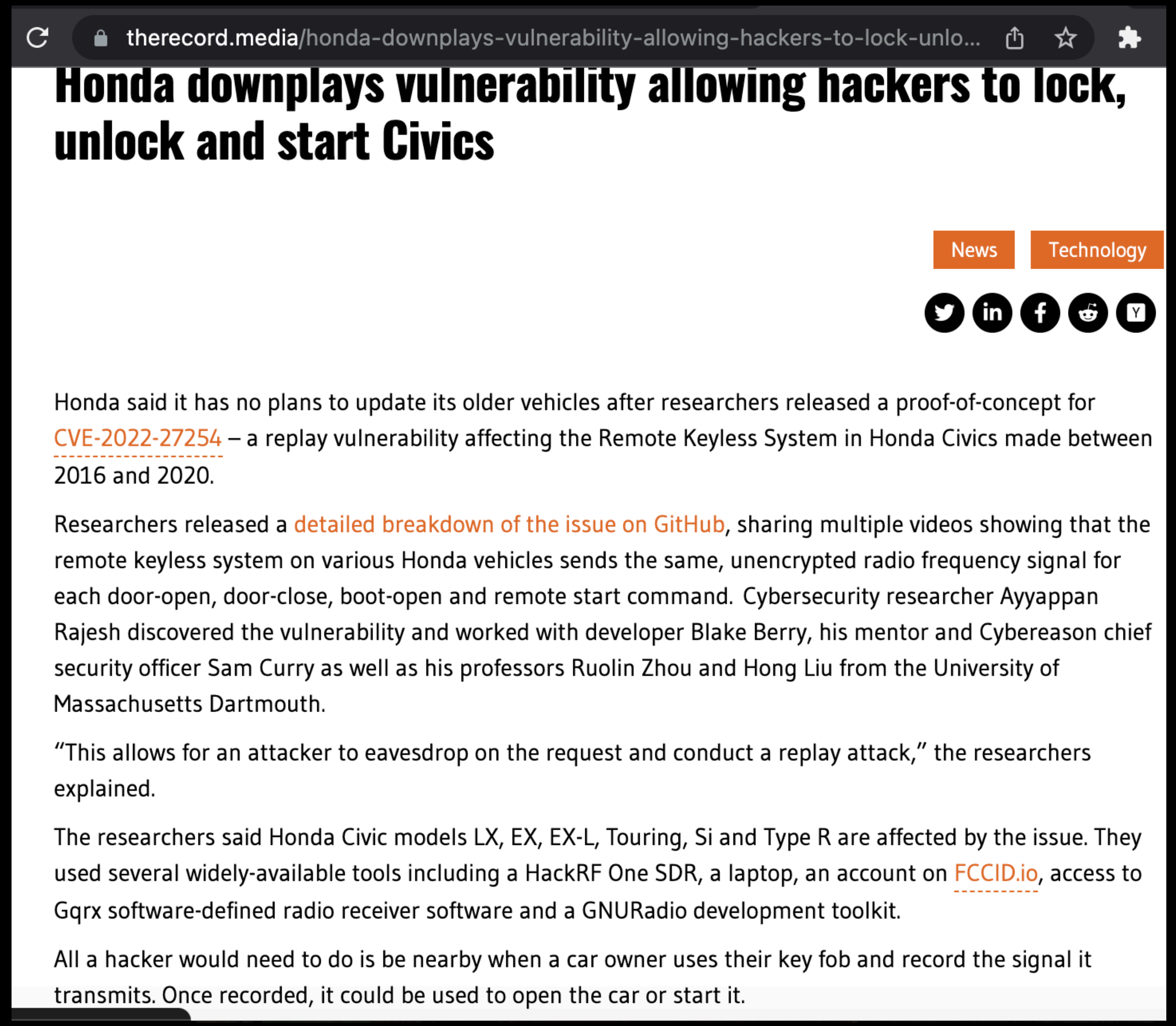
CVE Dictionary Entry:
CVE-2022-27254

NVD Published Date:
03/23/2022

NVD Last Modified:
03/31/2022

Source:
MITRE

Media


therecord.media/honda-downplays-vulnerability-allowing-hackers-to-lock-unlo...

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

News Technology

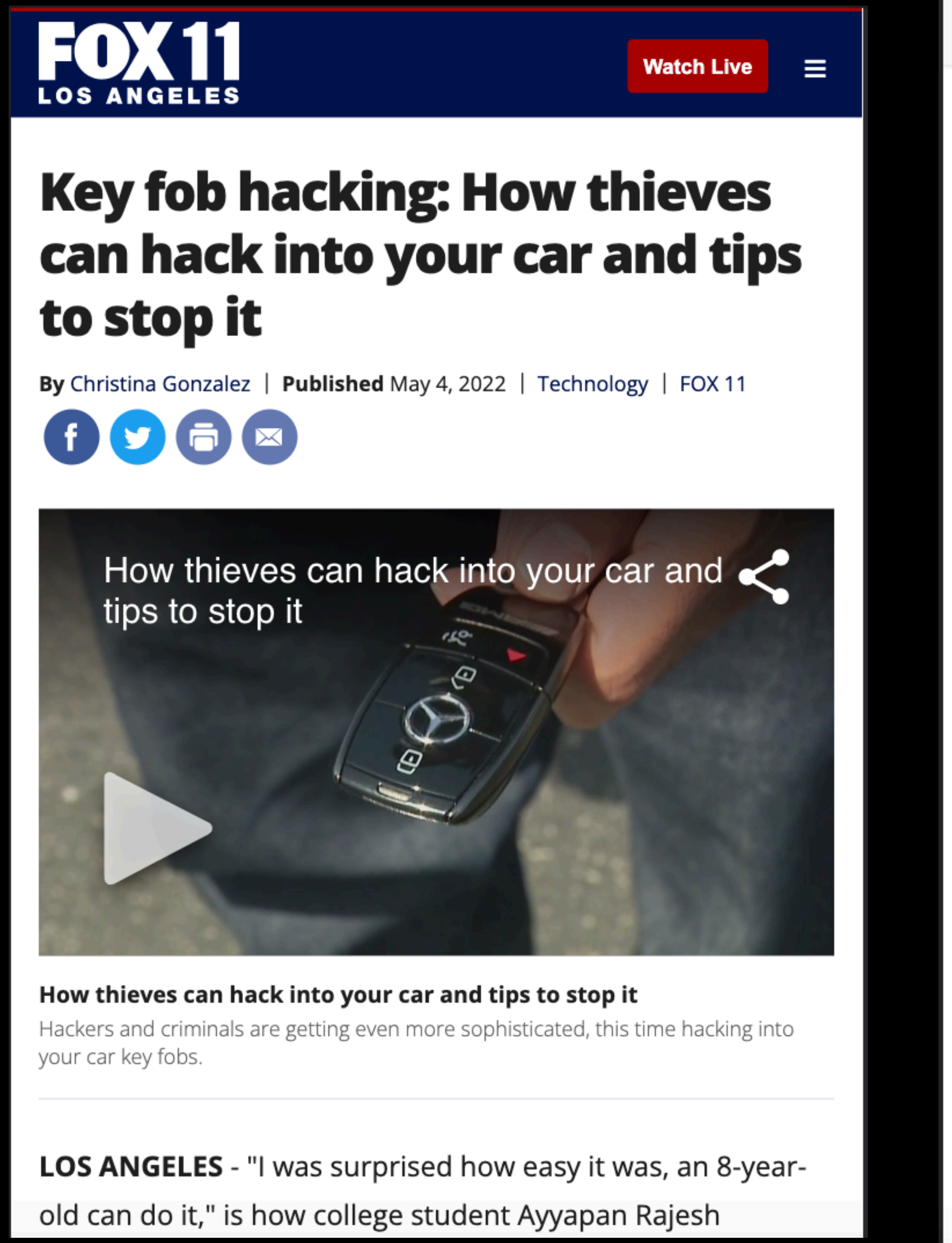
Honda said it has no plans to update its older vehicles after researchers released a proof-of-concept for CVE-2022-27254 – a replay vulnerability affecting the Remote Keyless System in Honda Civics made between 2016 and 2020.

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

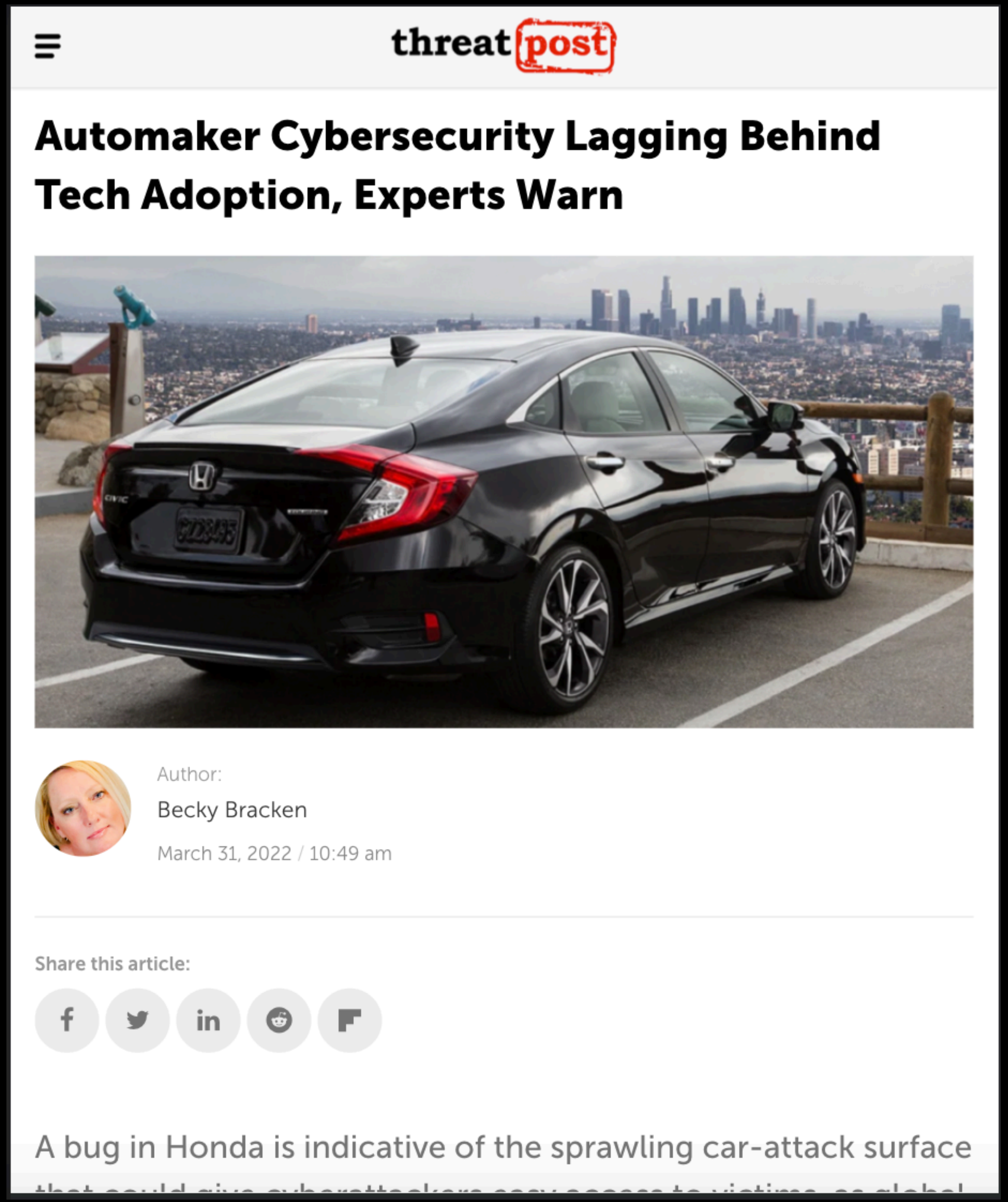
By Christina Gonzalez | Published May 4, 2022 | Technology | FOX 11

How thieves can hack into your car and tips to stop it

How thieves can hack into your car and tips to stop it

Hackers and criminals are getting even more sophisticated, this time hacking into your car key fobs.

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

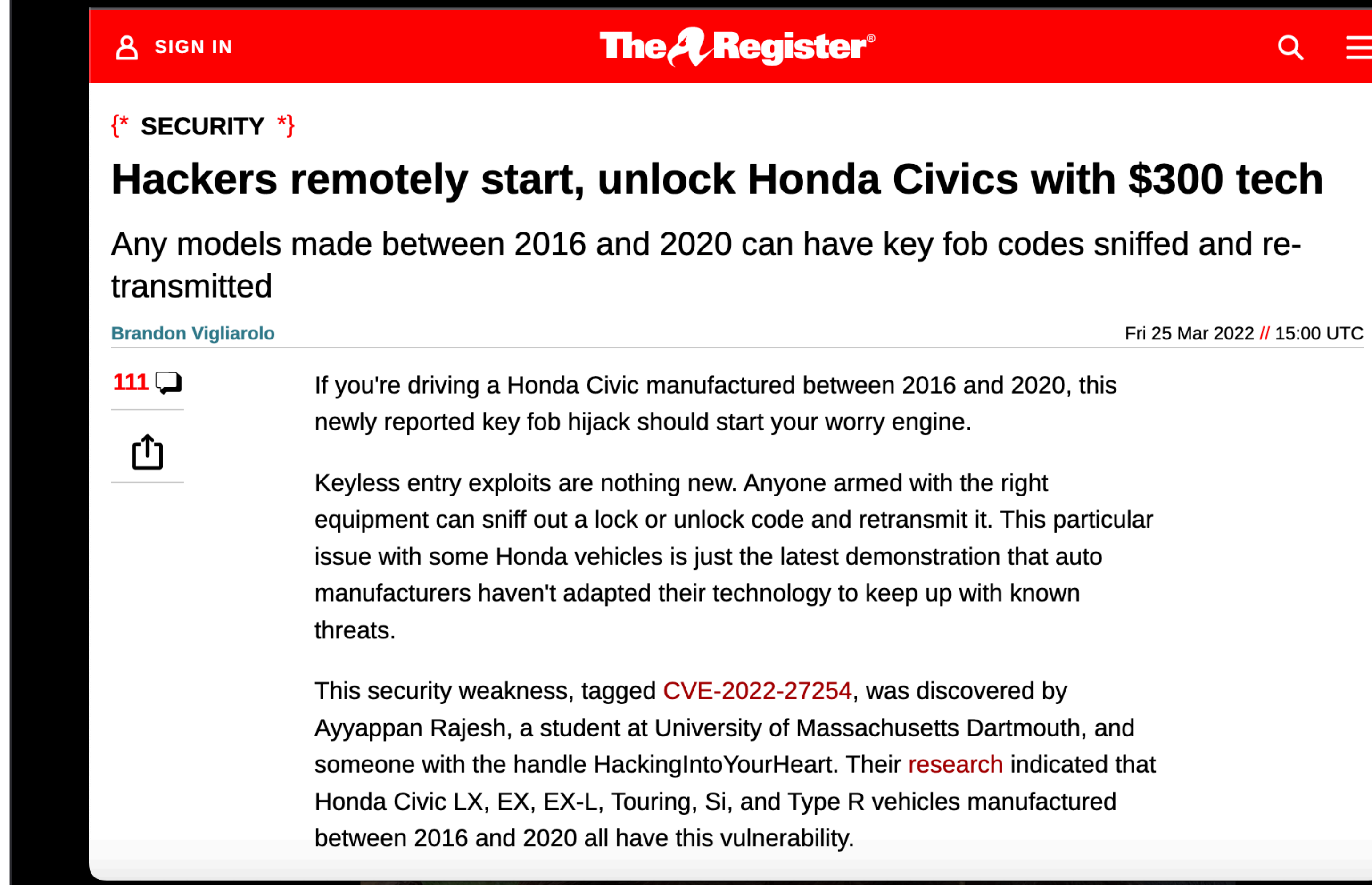


Automaker Cybersecurity Lagging Behind Tech Adoption, Experts Warn

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

Share this article:

A bug in Honda is indicative of the sprawling car-attack surface



{* SECURITY *}

Hackers remotely start, unlock Honda Civics with $300 tech

Any models made between 2016 and 2020 can have key fob codes sniffed and re-transmitted

Brandon Vigliarolo Fri 25 Mar 2022 // 15:00 UTC

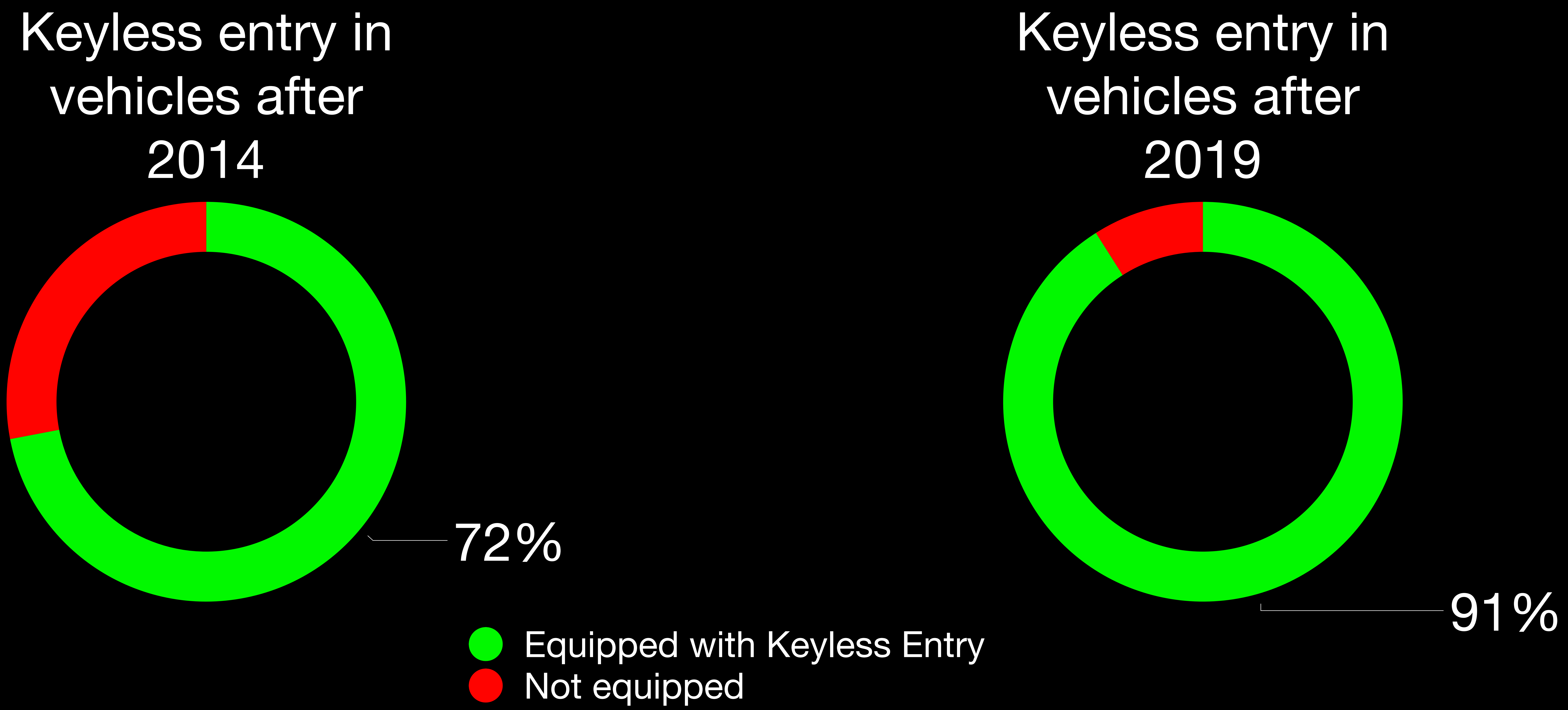
111

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.

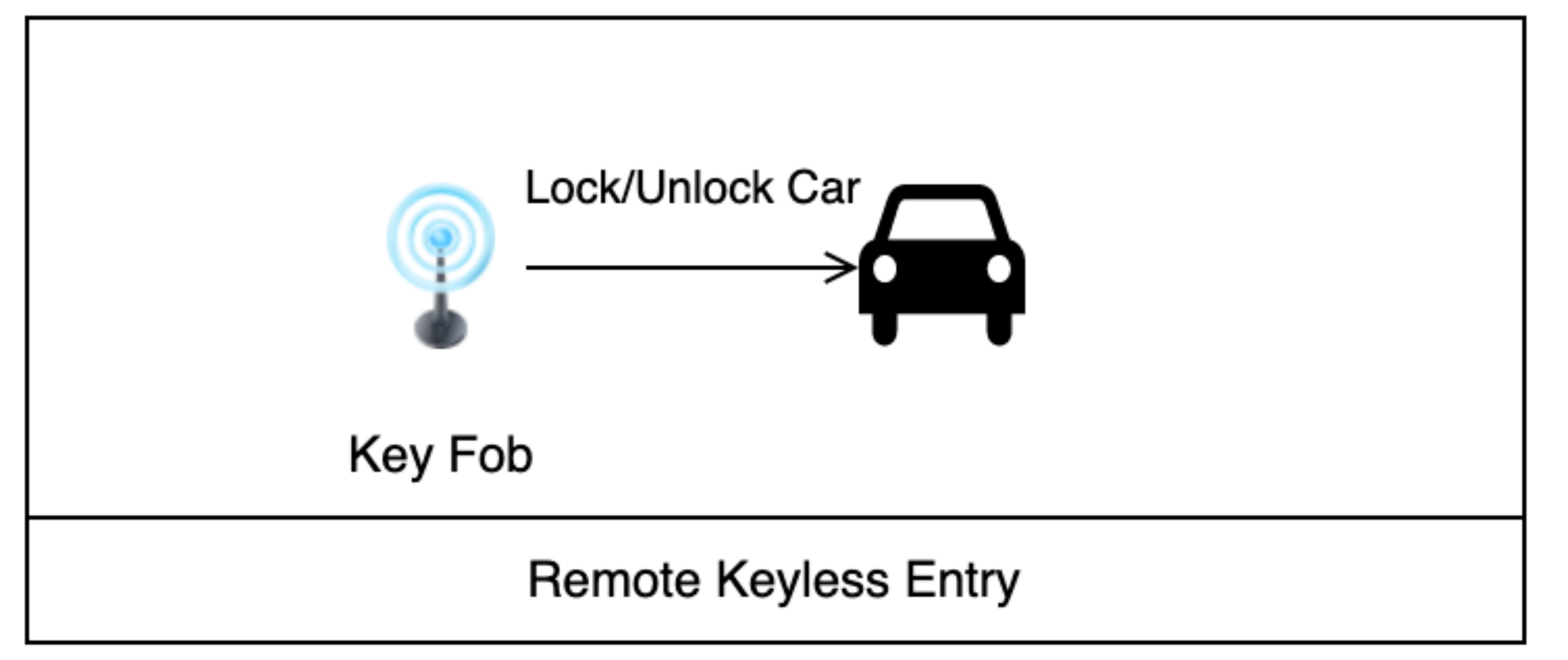
Keyless Entry Systems



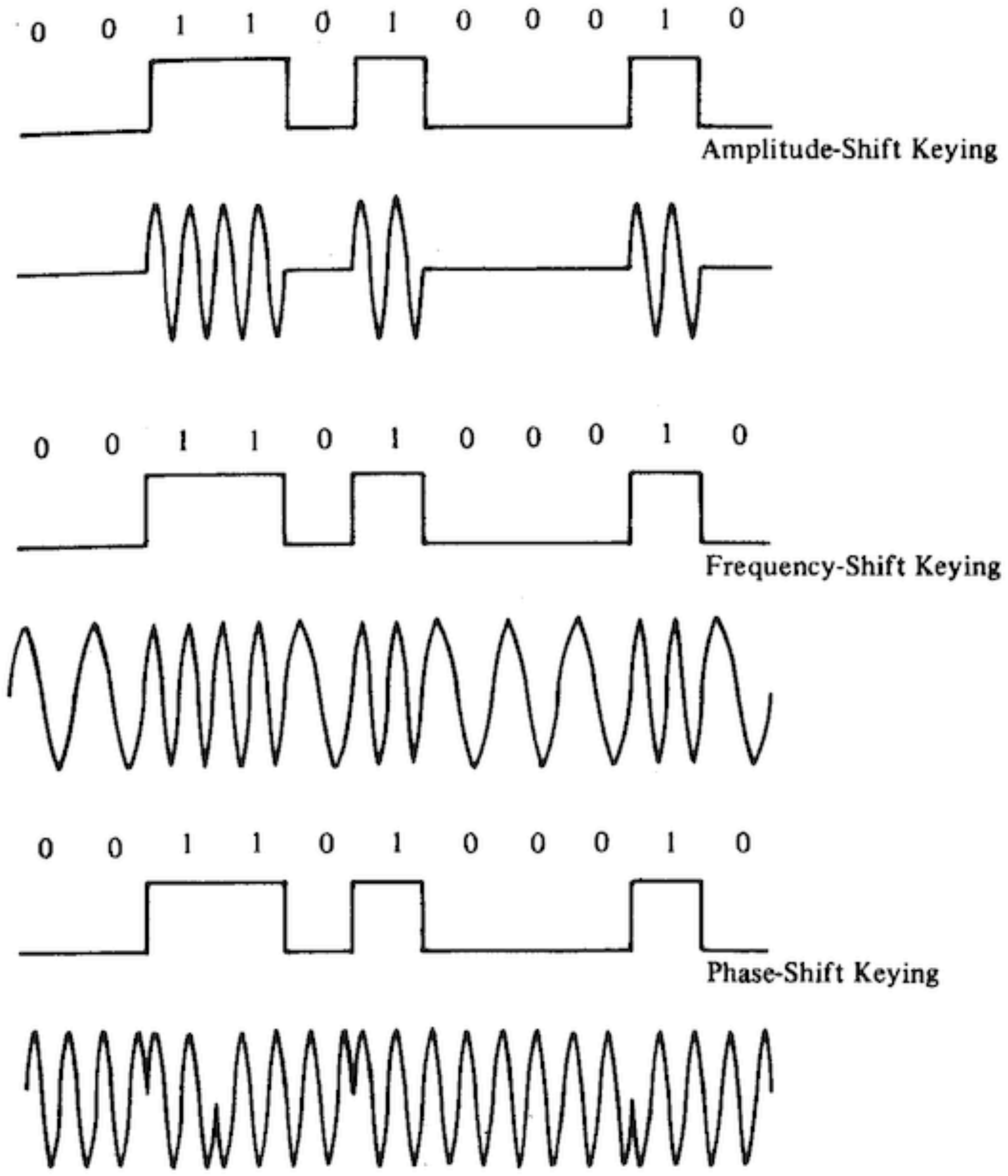
Source : CNBC & Edmunds

Remote Keyless Entry(RKE)

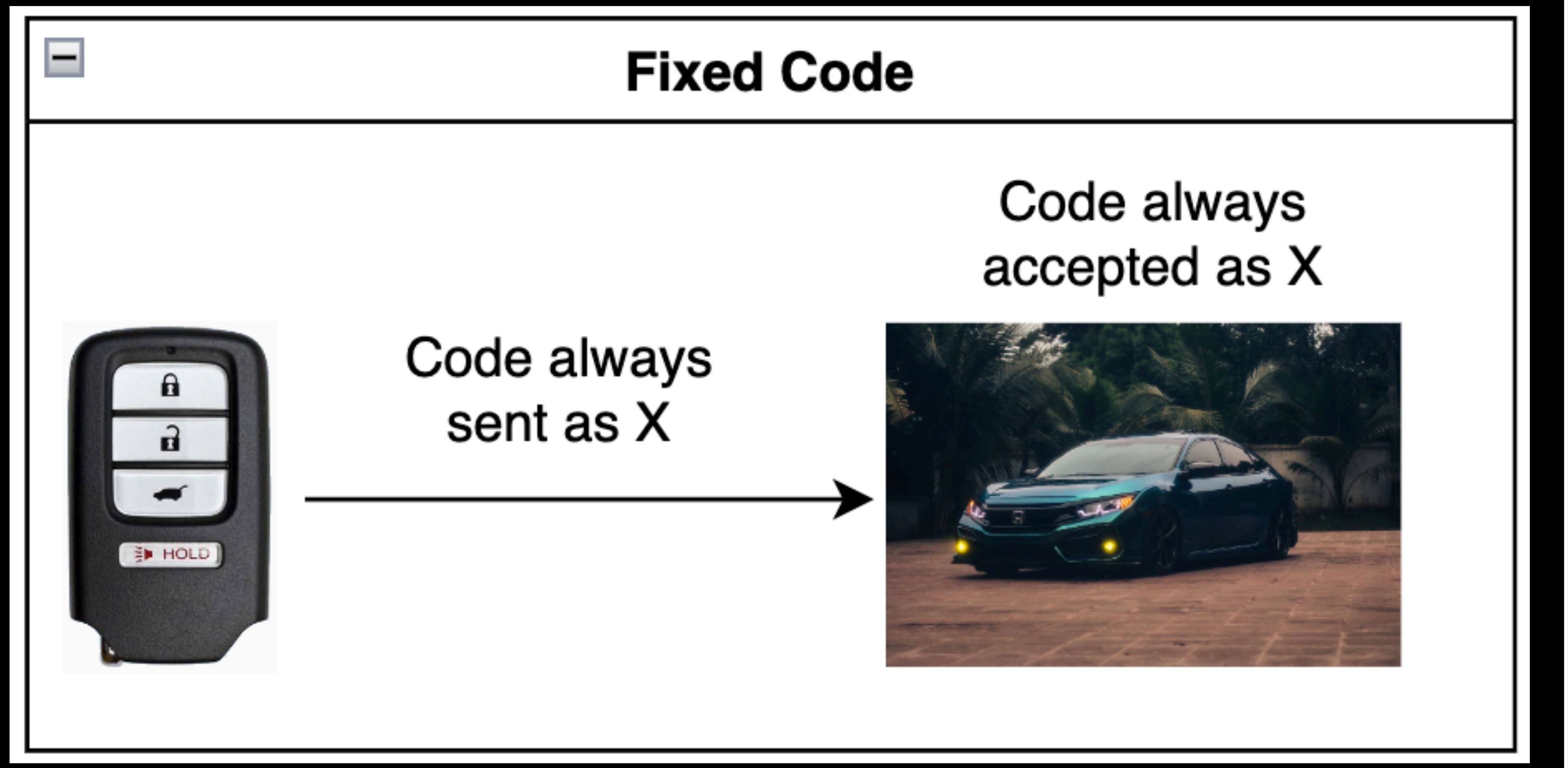
- First introduced in 1982 on a Renault Fuego
- Operates at either 315, 433 or 868MHz



Modulation


0 0 1 1 0 1 0 0 0 1 0
Amplitude-Shift Keying
0 0 1 1 0 1 0 0 0 1 0
Frequency-Shift Keying
0 0 1 1 0 1 0 0 0 1 0
Phase-Shift Keying

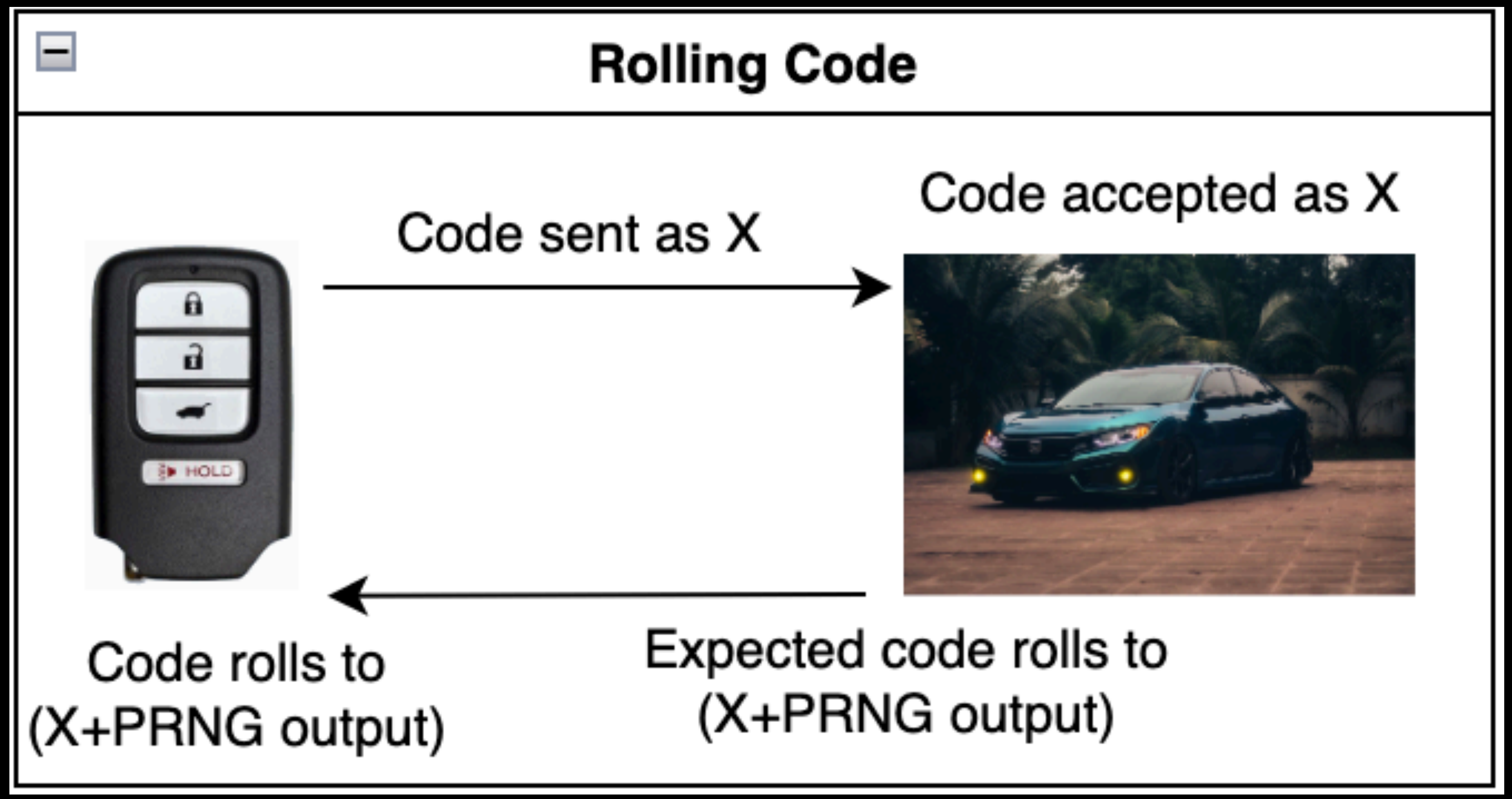
Static vs. rolling keys



Fixed Code

Code always sent as X

Code always accepted as X



Rolling Code

Code sent as X

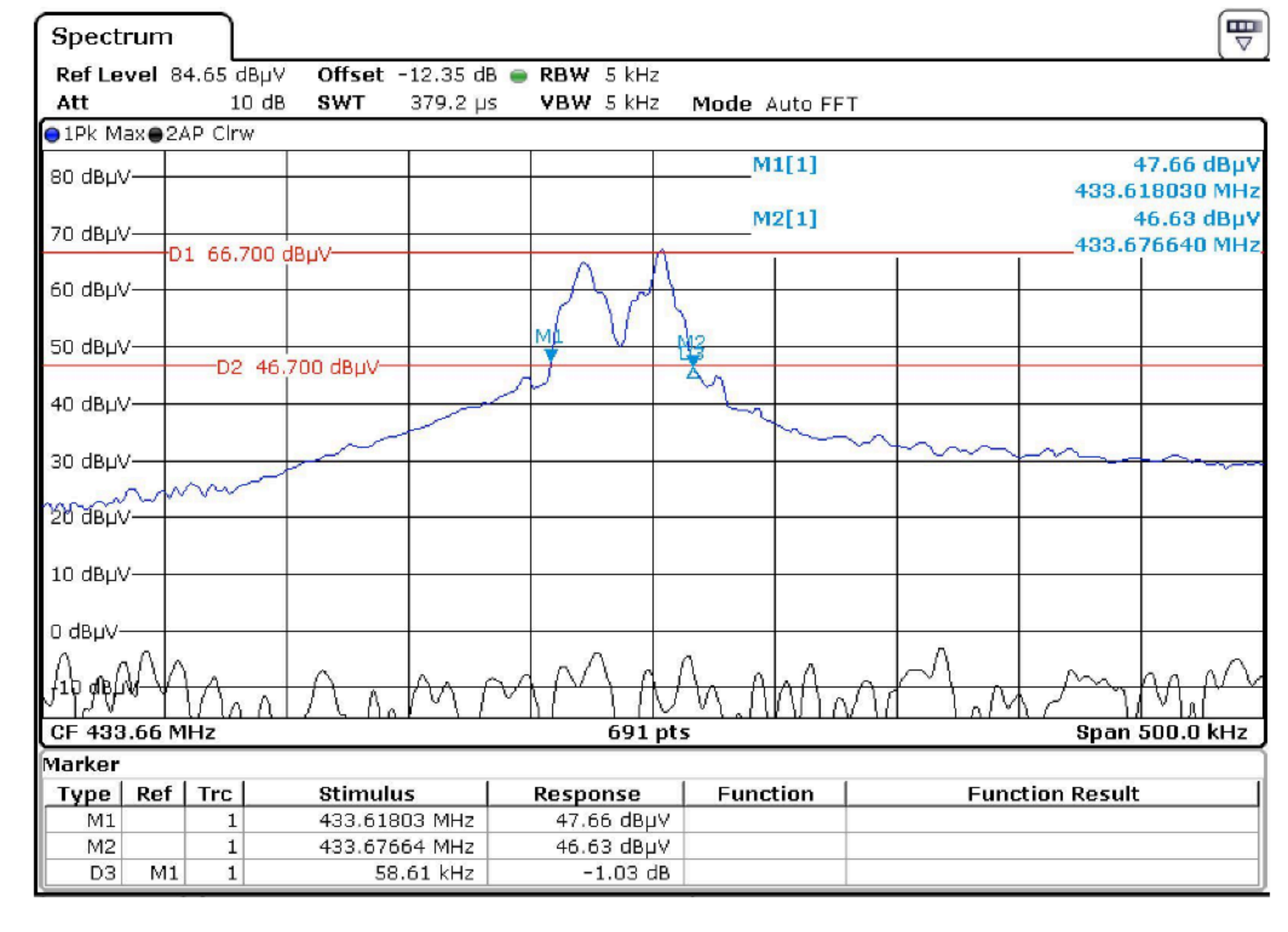
Code accepted as X

Expected code rolls to (X+PRNG output)

Code rolls to (X+PRNG output)

Tools

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



Spectrum

Ref Level 84.65 dBµV   Offset -12.35 dB ● RBW 5 kHz
Att 10 dB   SWT 379.2 µs   VBW 5 kHz   Mode Auto FFT

●1Pk Max ●2AP Clrw

M1[1] 47.66 dBµV
433.618030 MHz
M2[1] 46.63 dBµV
433.676640 MHz

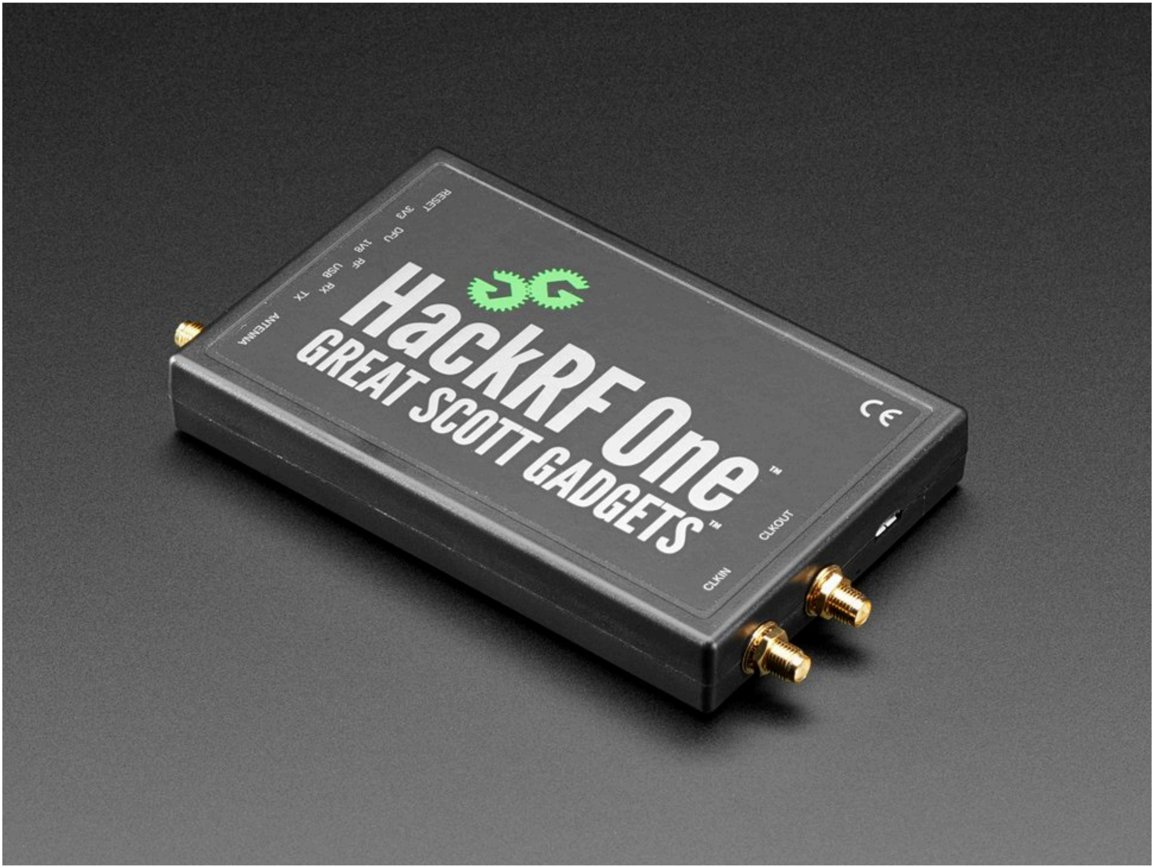
CF 433.66 MHz   691 pts   Span 500.0 kHz

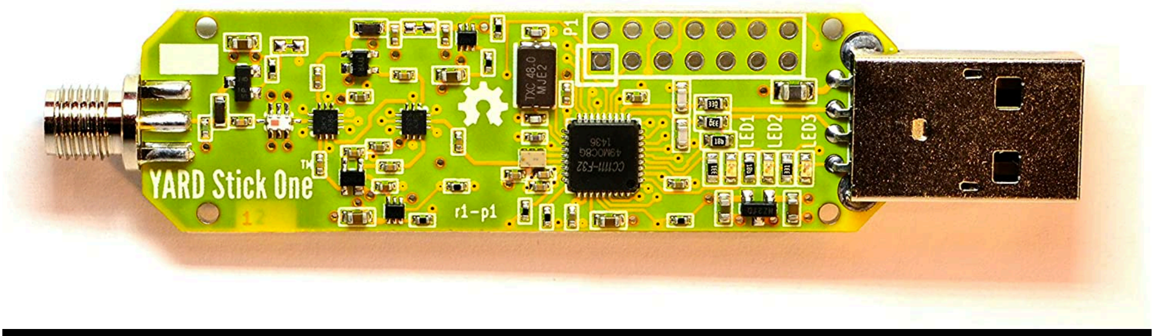
Marker

Type	Ref	Trc	Stimulus	Response	Function	Function Result
M1		1	433.61803 MHz	47.66 dBµV		
M2		1	433.67664 MHz	46.63 dBµV		
D3	M1	1	58.61 kHz	-1.03 dB		

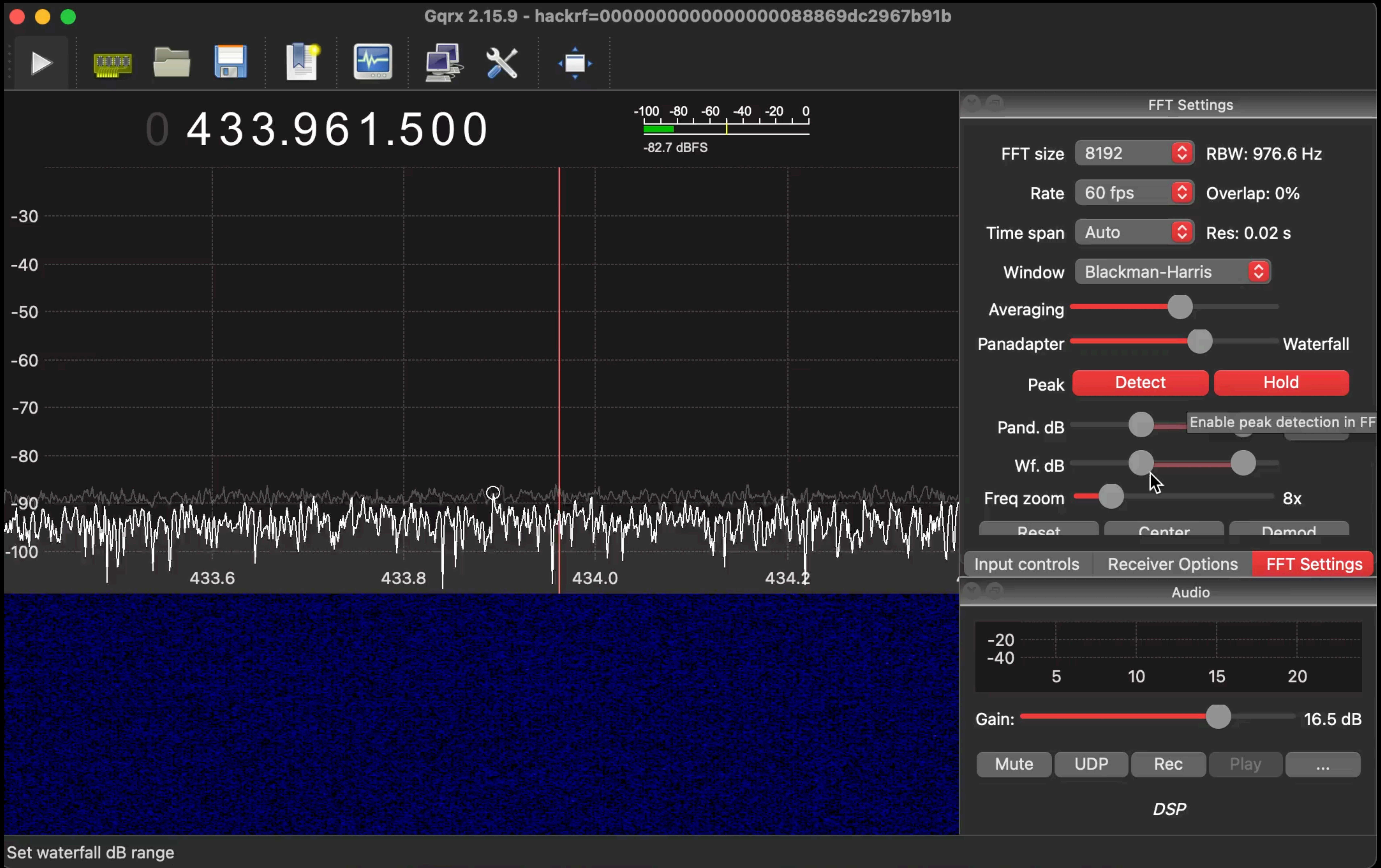
RF Transceivers

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





GQRX



Gqrx 2.15.9 - hackrf=0000000000000000088869dc2967b91b

0 433.961.500

-82.7 dBFS

FFT Settings

FFT size 8192 RBW: 976.6 Hz

Rate 60 fps Overlap: 0%

Time span Auto Res: 0.02 s

Window Blackman-Harris

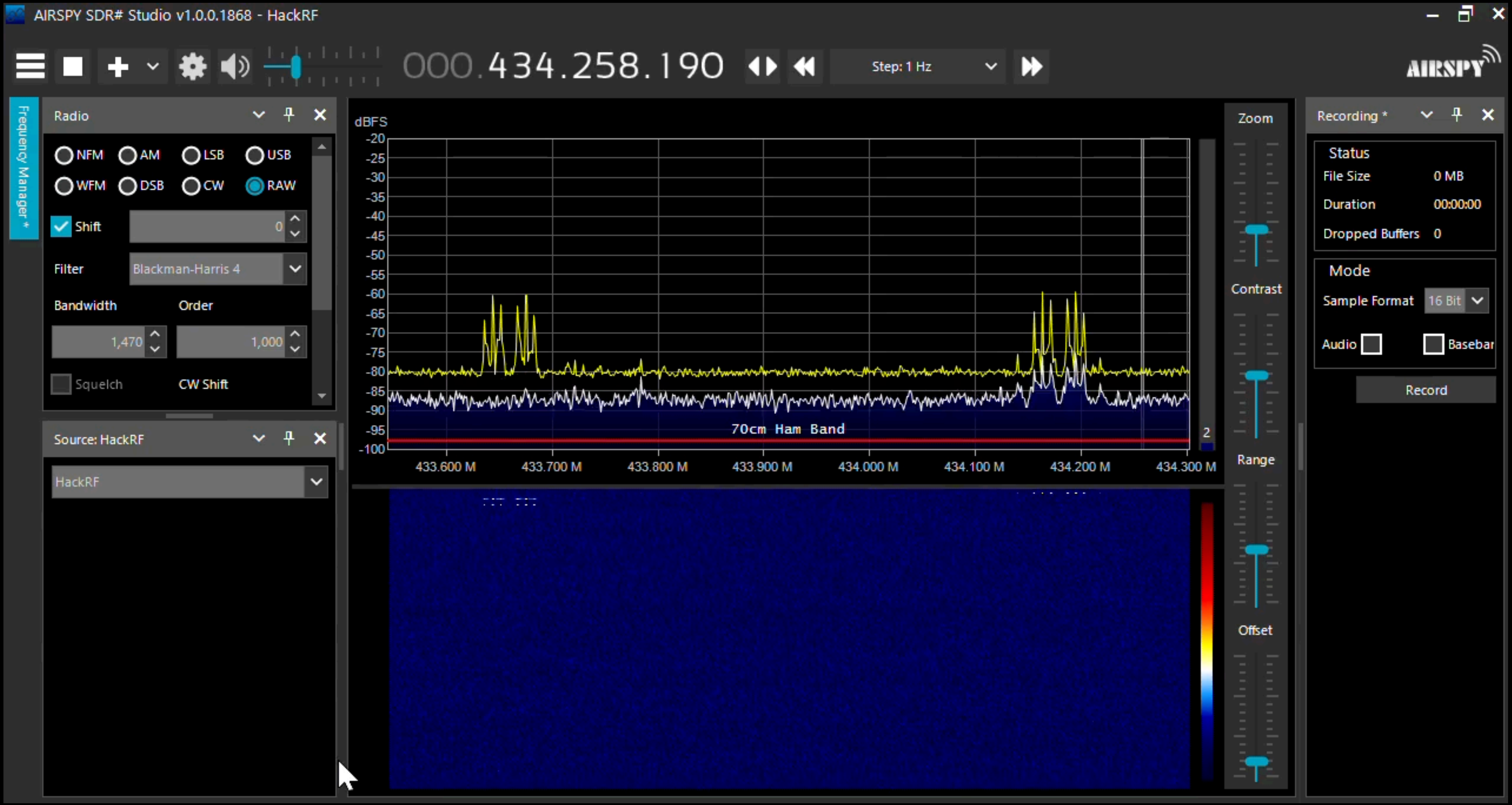
Freq zoom 8x

Audio

Gain: 16.5 dB

Set waterfall dB range

AirSpy SDR



AIRSPY SDR# Studio v1.0.0.1868 - HackRF

000.434.258.190

Step: 1 Hz

Radio

○ NFM ○ AM ○ LSB ○ USB

○ WFM ○ DSB ○ CW ● RAW

☑ Shift 0

Filter: Blackman-Harris 4

Bandwidth: 1,470

Order: 1,000

□ Squelch

CW Shift

Source: HackRF

HackRF

Recording *

Status

File Size	0 MB
Duration	00:00:00
Dropped Buffers	0

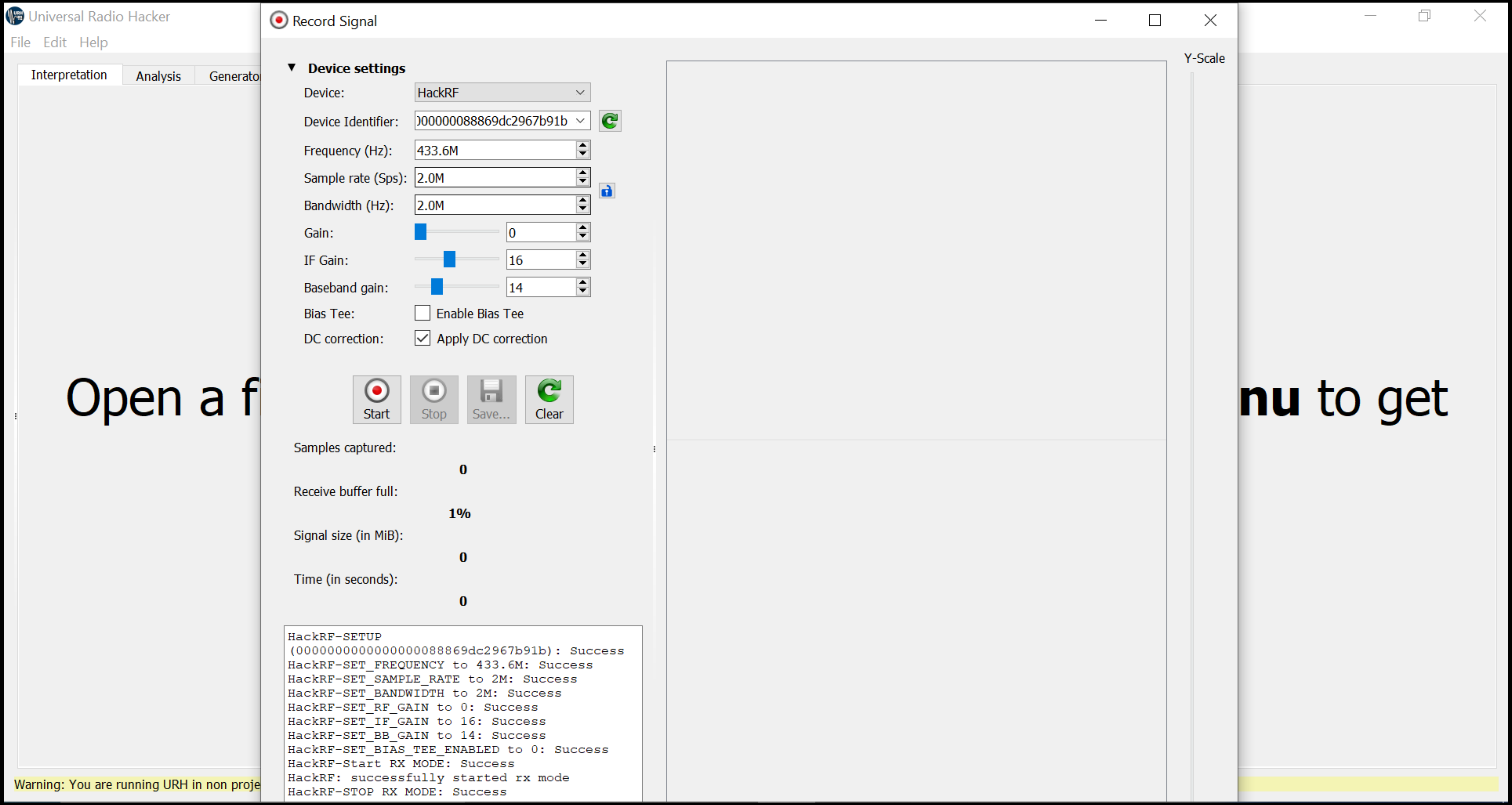
Mode

Sample Format: 16 Bit

Audio □ □ Basebar

Record

Universal Radio Hacker (URH)



Warning: You are running URH in non proje

▼ **Device settings**

Device: HackRF

Device Identifier:)00000088869dc2967b91b

Frequency (Hz): 433.6M

Sample rate (Sps): 2.0M

Bandwidth (Hz): 2.0M

Gain: 0

IF Gain: 16

Baseband gain: 14

Bias Tee: □ Enable Bias Tee

DC correction: ☑ Apply DC correction

Samples captured: **0**

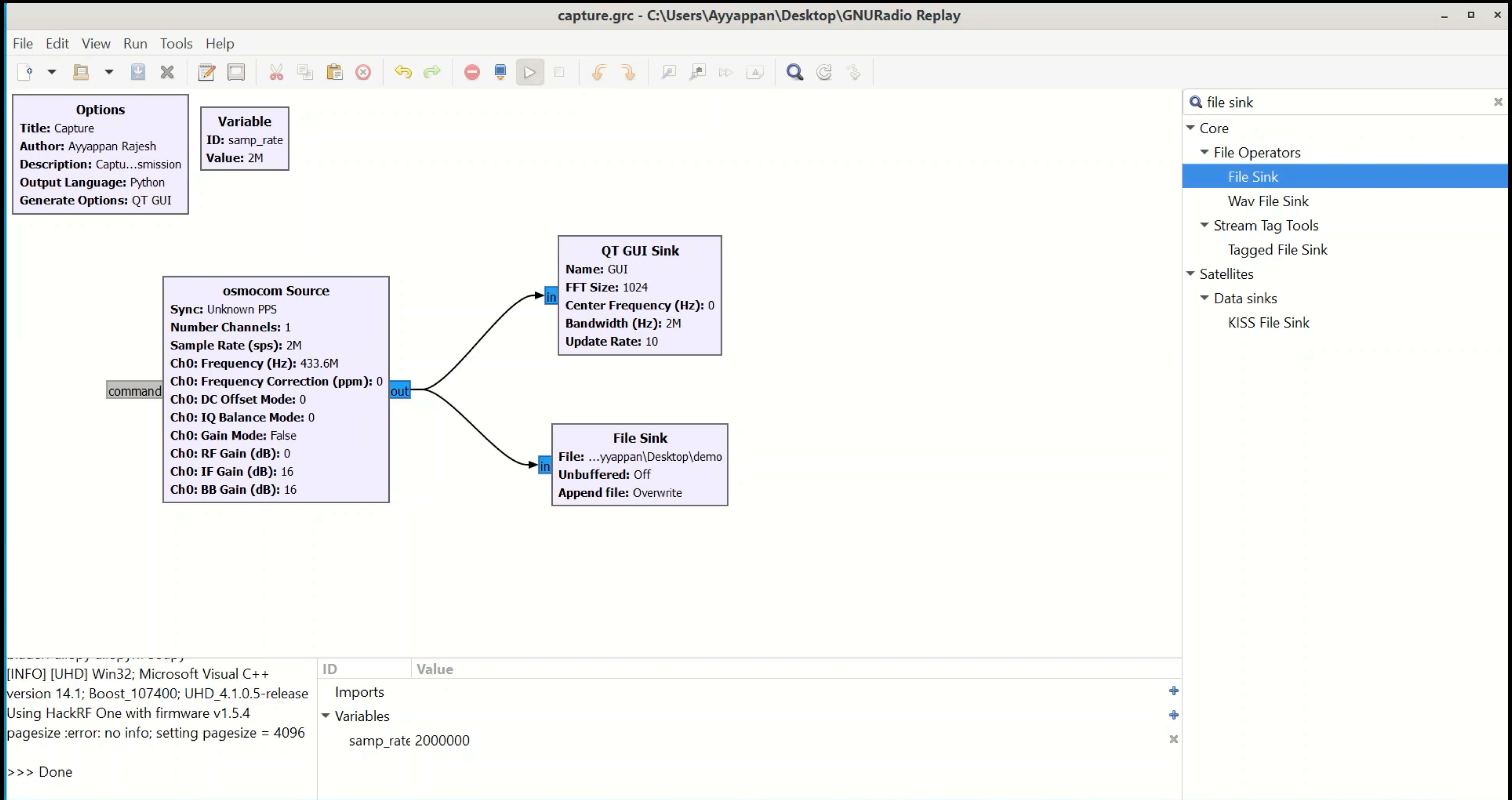
Receive buffer full: **1%**

Signal size (in MiB): **0**

Time (in seconds): **0**

```
HackRF-SETUP
(0000000000000000088869dc2967b91b): Success
HackRF-SET_FREQUENCY to 433.6M: Success
HackRF-SET_SAMPLE_RATE to 2M: Success
HackRF-SET_BANDWIDTH to 2M: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 16: Success
HackRF-SET_BB_GAIN to 14: Success
HackRF-SET_BIAS_TEE_ENABLED to 0: Success
HackRF-Start RX MODE: Success
HackRF: successfully started rx mode
HackRF-STOP RX MODE: Success
```

GNURadio Capture



Options
Title: Capture
Author: Ayyappan Rajesh
Description: Captu...smission
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 2M

osmocom Source
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 433.6M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 0
Ch0: IF Gain (dB): 16
Ch0: BB Gain (dB): 16

QT GUI Sink
Name: GUI
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
Update Rate: 10

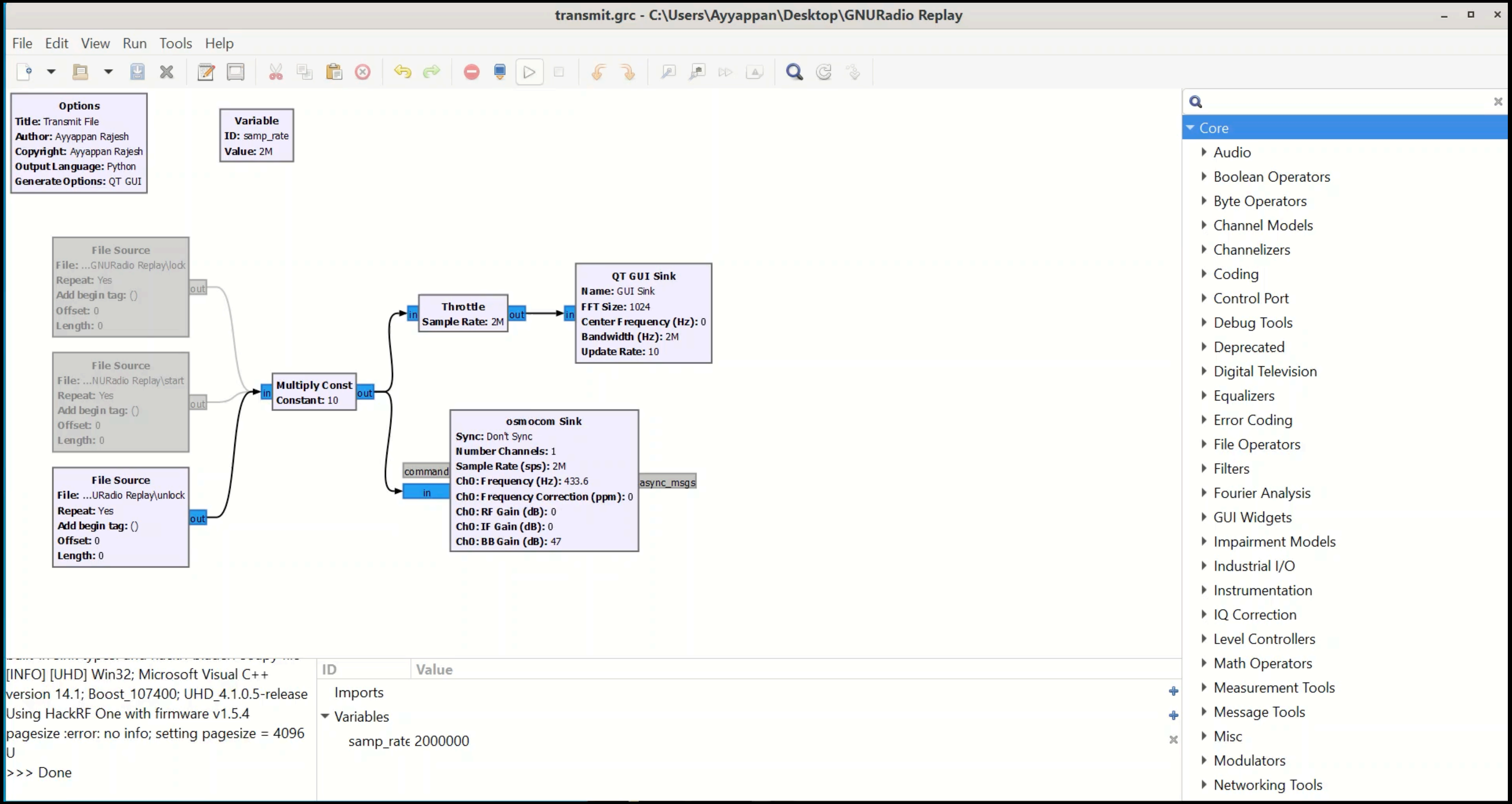
File Sink
File: ...yyappan\Desktop\demo
Unbuffered: Off
Append file: Overwrite

```
[INFO] [UHD] Win32; Microsoft Visual C++
version 14.1; Boost_107400; UHD_4.1.0.5-release
Using HackRF One with firmware v1.5.4
pagesize :error: no info; setting pagesize = 4096

>>> Done
```

ID	Value
Imports	
Variables	
samp_rate	2000000

GNURadio Transmit



Options
Title: Transmit File
Author: Ayyappan Rajesh
Copyright: Ayyappan Rajesh
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 2M

File Source
File: ...GNURadio Replay\lock
Repeat: Yes
Add begin tag: ()
Offset: 0
Length: 0

File Source
File: ...NURadio Replay\start
Repeat: Yes
Add begin tag: ()
Offset: 0
Length: 0

File Source
File: ...URadio Replay\unlock
Repeat: Yes
Add begin tag: ()
Offset: 0
Length: 0

Multiply Const
Constant: 10

Throttle
Sample Rate: 2M

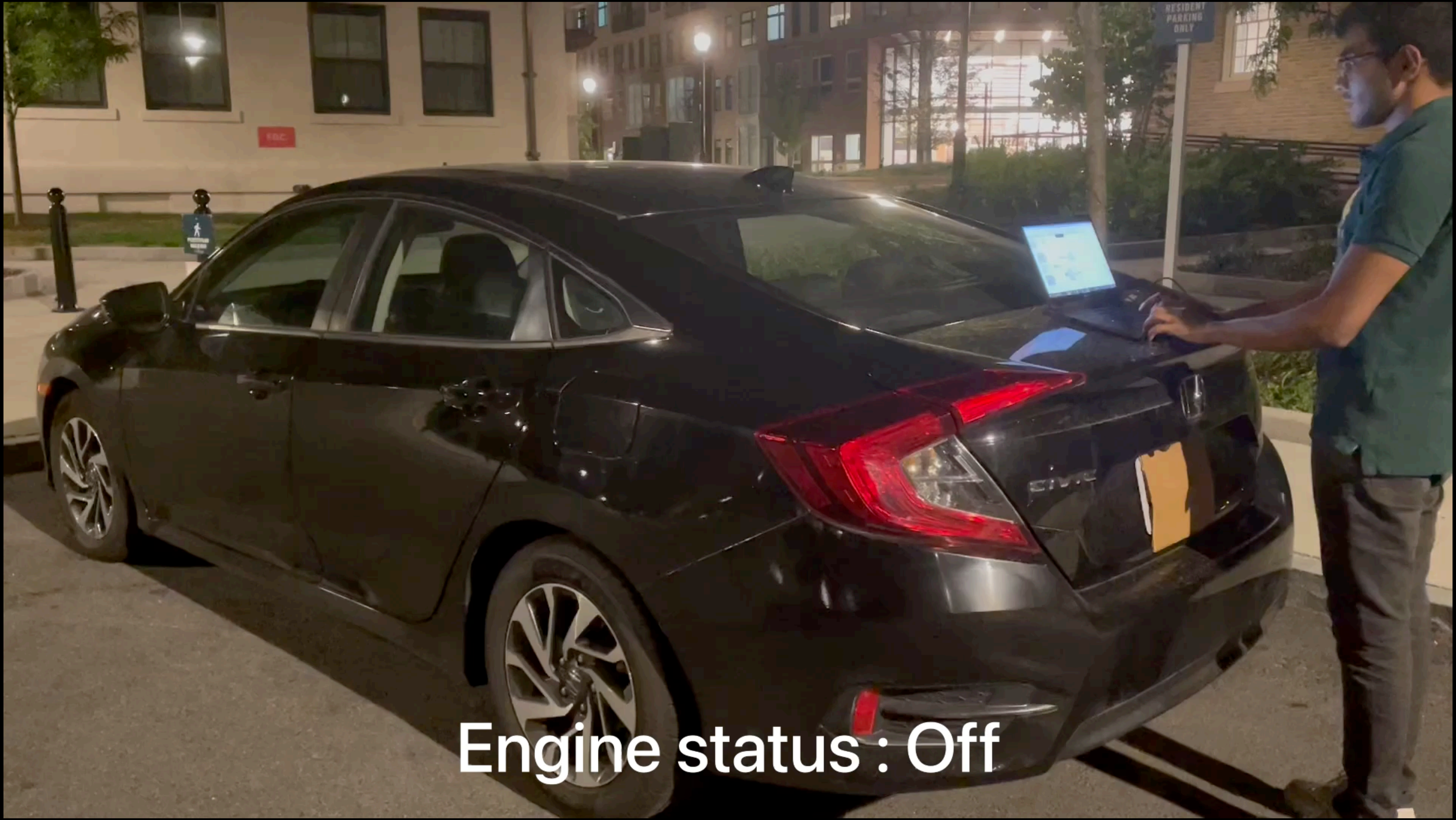
QT GUI Sink
Name: GUI Sink
FFT Size: 1024
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
Update Rate: 10

osmocom Sink
Sync: Don't Sync
Number Channels: 1
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 433.6
Ch0: Frequency Correction (ppm): 0
Ch0: RF Gain (dB): 0
Ch0: IF Gain (dB): 0
Ch0: BB Gain (dB): 47

```
[INFO] [UHD] Win32; Microsoft Visual C++
version 14.1; Boost_107400; UHD_4.1.0.5-release
Using HackRF One with firmware v1.5.4
pagesize :error: no info; setting pagesize = 4096
U
>>> Done
```

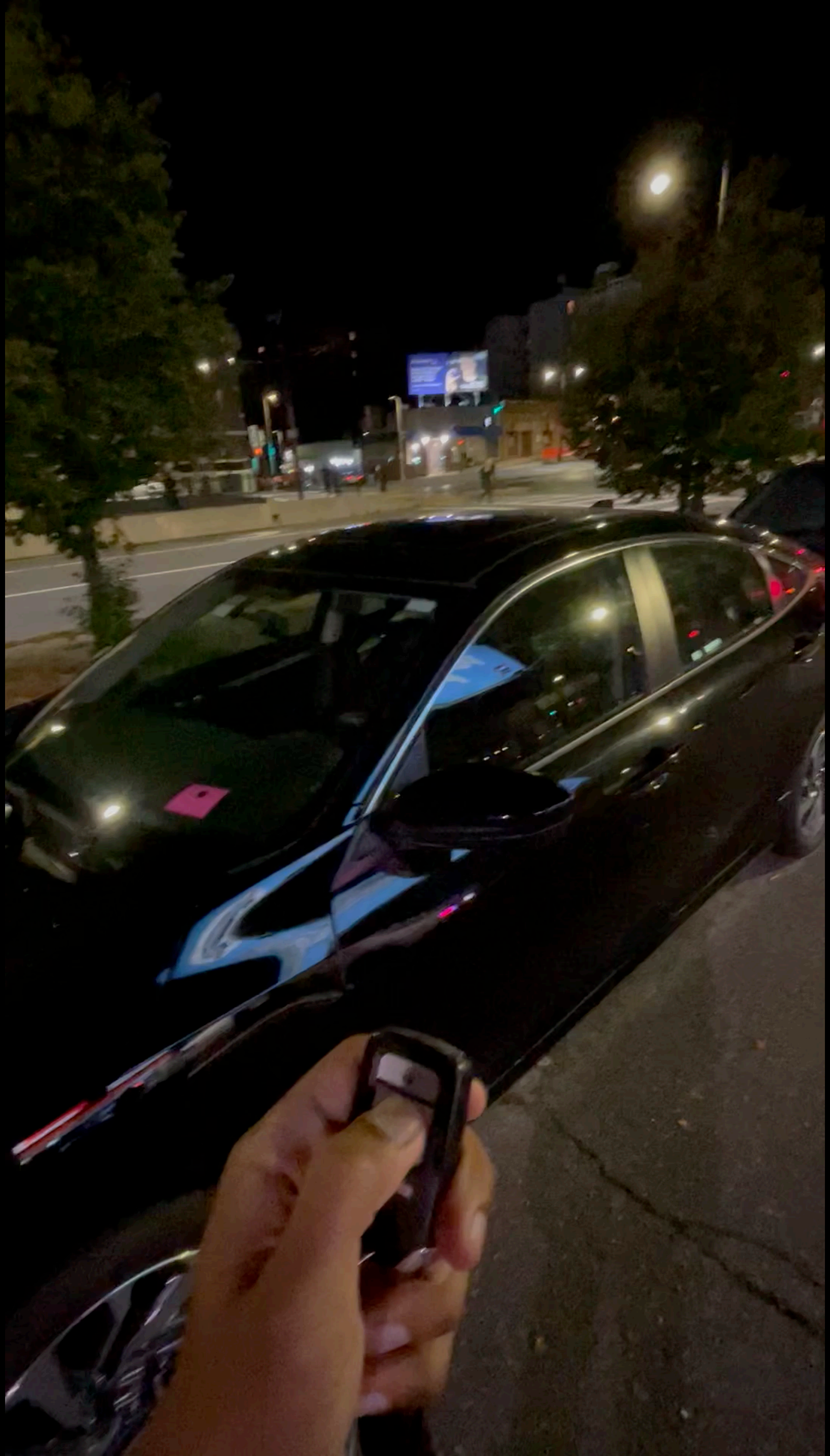
ID	Value
Imports	
Variables	
samp_rate	2000000

Gone in 50 seconds



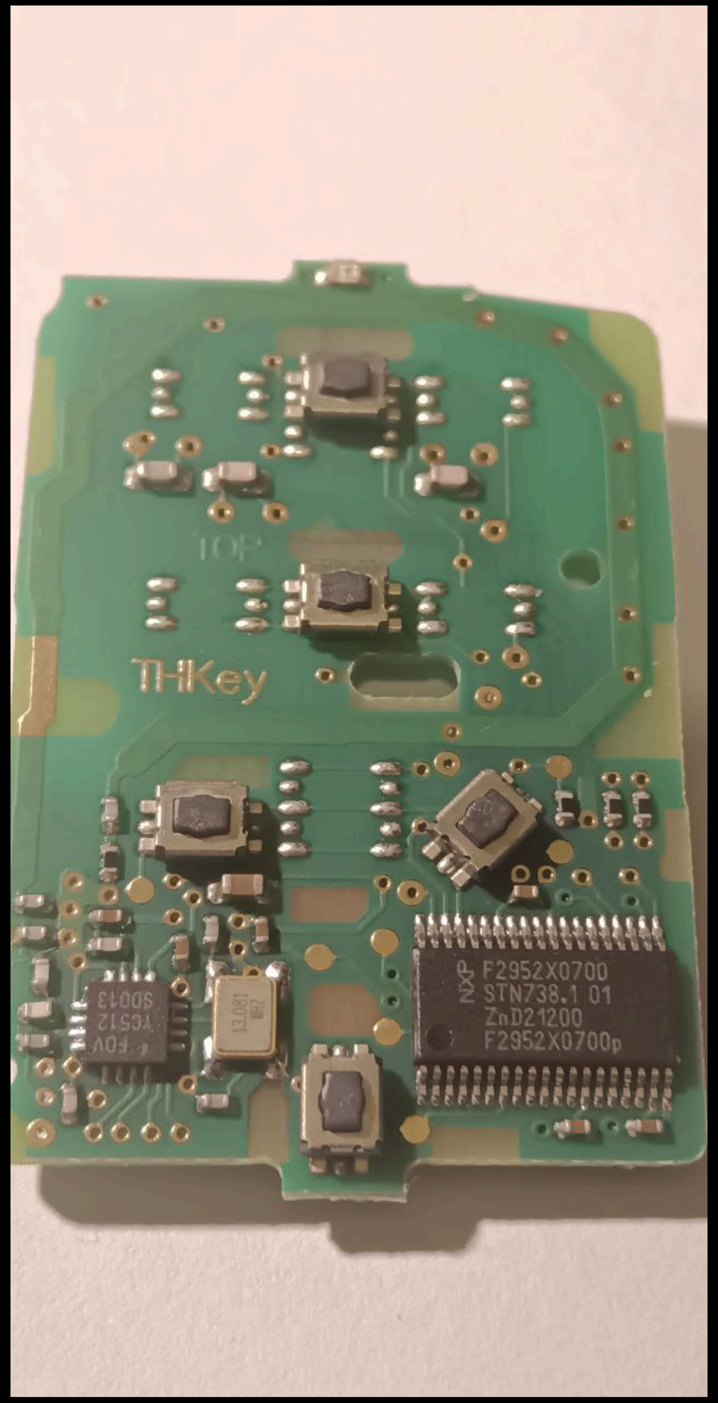
Engine status : Off

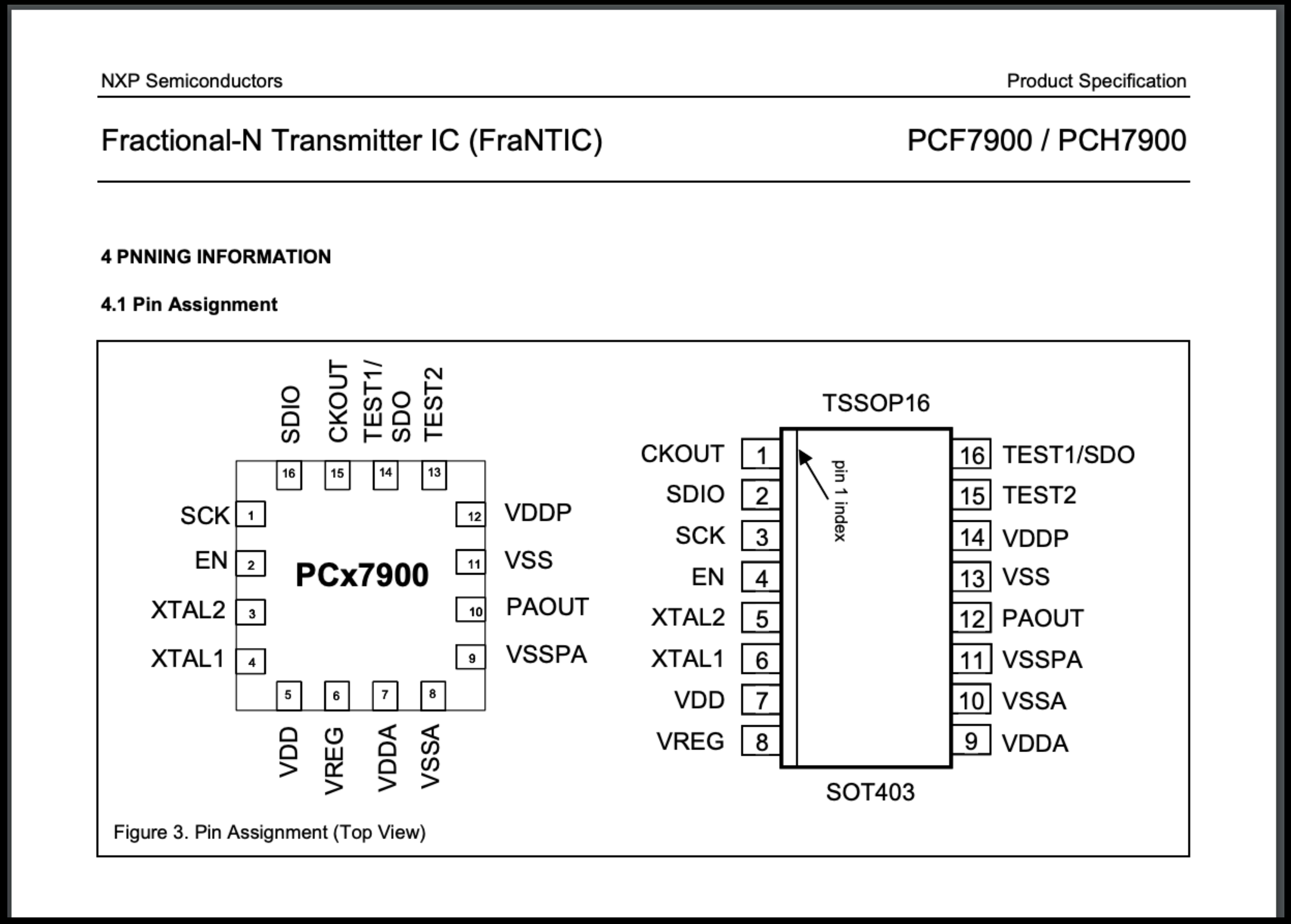
My favorite…



Credit : CBS News

Digging Deeper





NXP Semiconductors — Product Specification

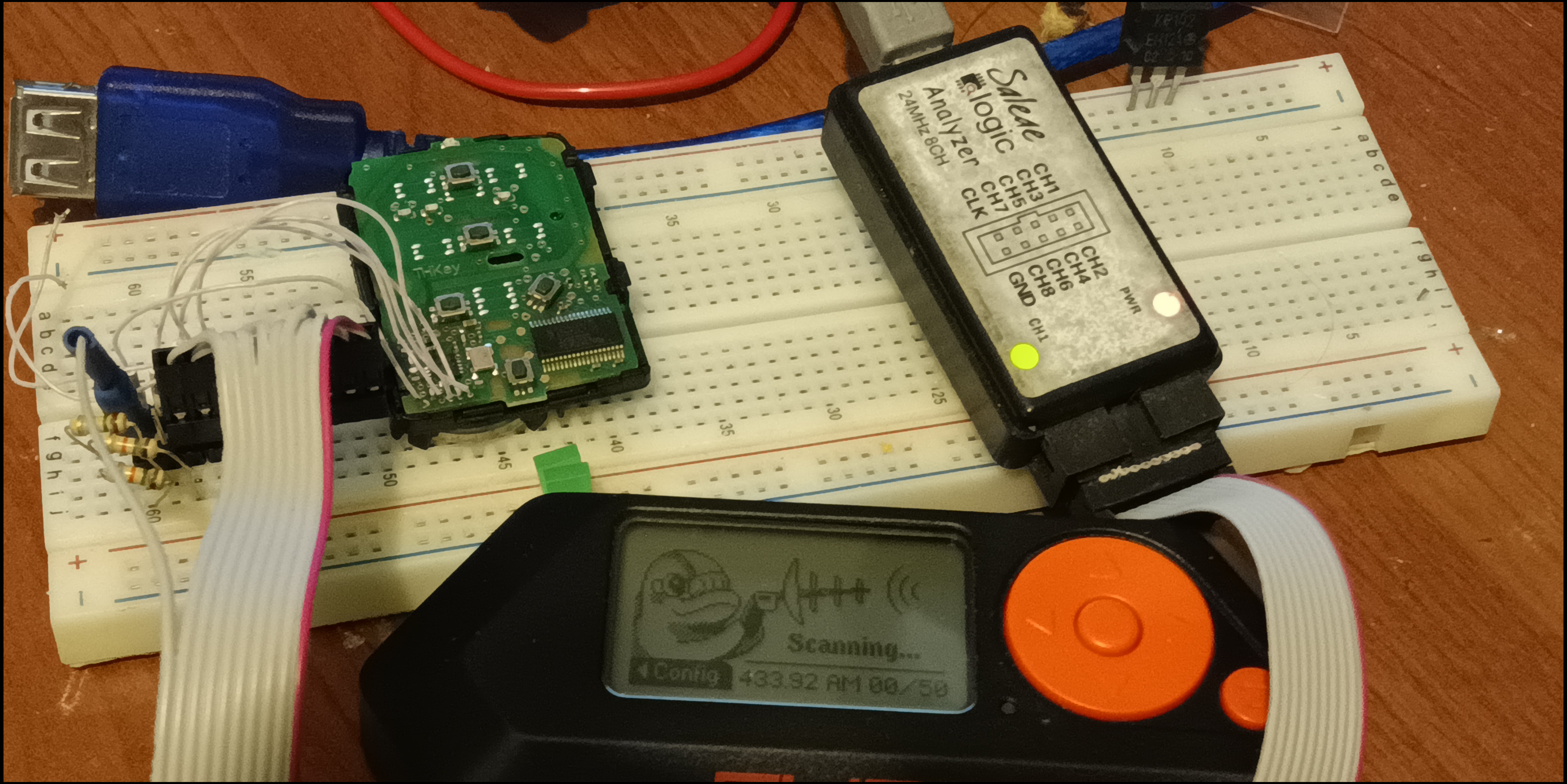
Fractional-N Transmitter IC (FraNTIC) — PCF7900 / PCH7900

4 PNNING INFORMATION

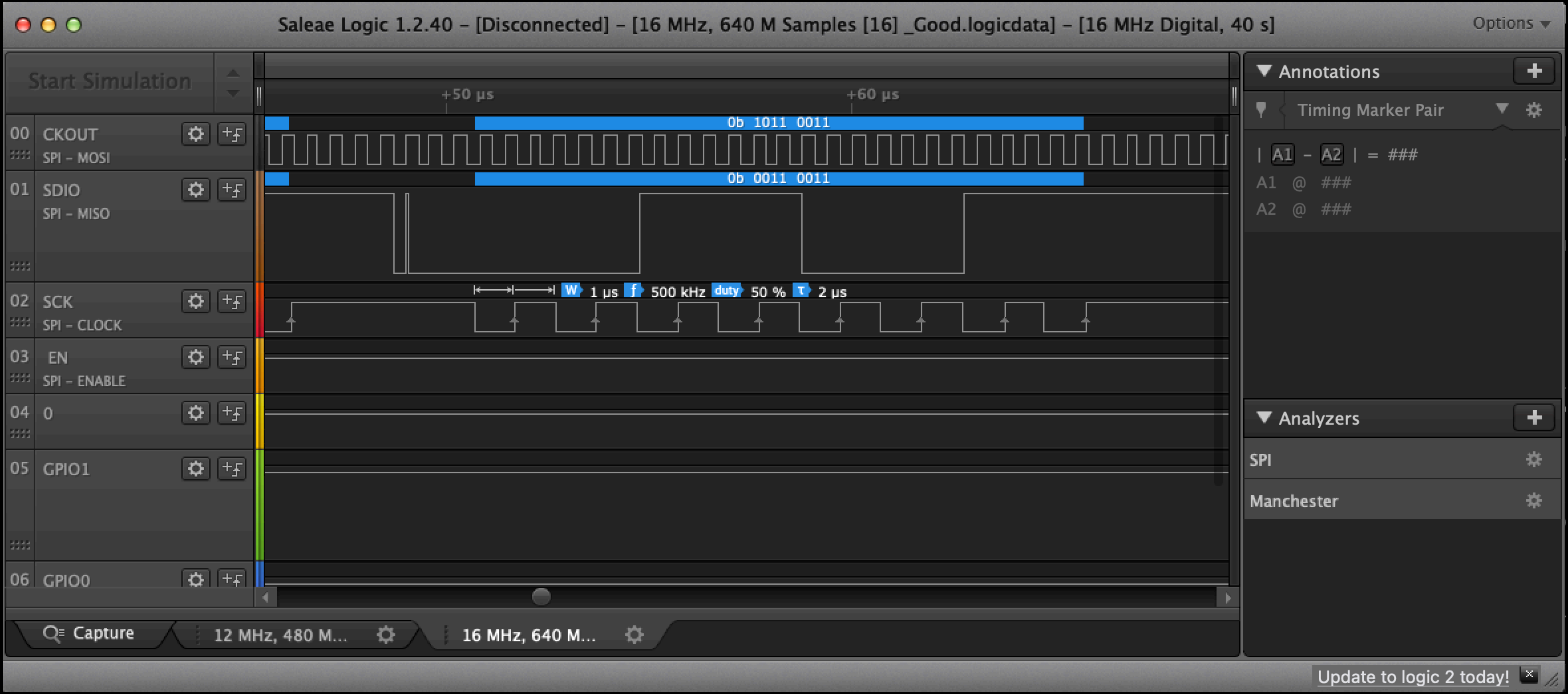
4.1 Pin Assignment

SDIO
CKOUT
TEST1/SDO
TEST2
SCK
EN
XTAL2
XTAL1
PCx7900
VDDP
VSS
PAOUT
VSSPA
VDD
VREG
VDDA
VSSA
TSSOP16
pin 1 index
CKOUT 1
SDIO 2
SCK 3
EN 4
XTAL2 5
XTAL1 6
VDD 7
VREG 8
16 TEST1/SDO
15 TEST2
14 VDDP
13 VSS
12 PAOUT
11 VSSPA
10 VSSA
9 VDDA
SOT403

Figure 3. Pin Assignment (Top View)

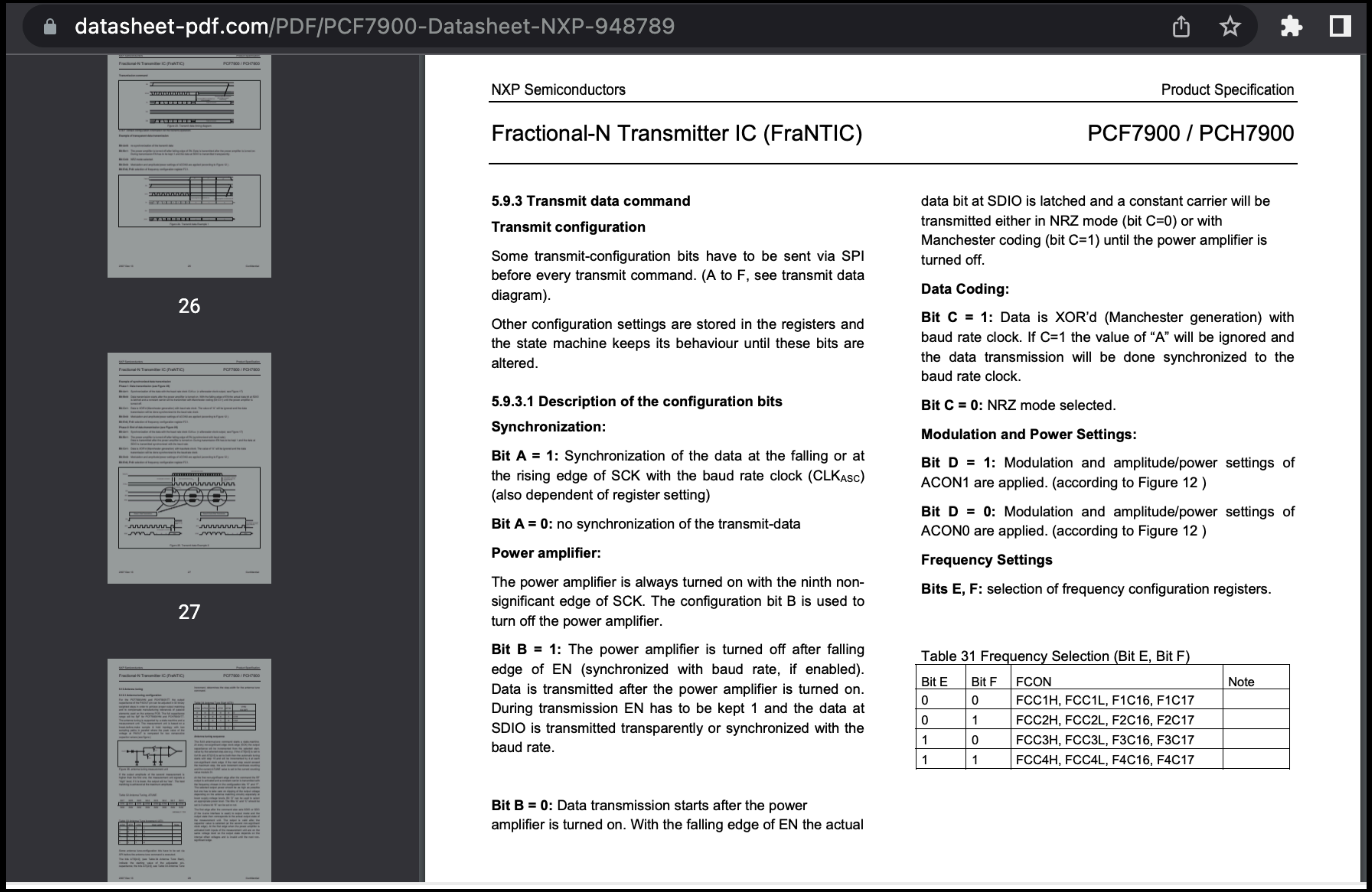

Saleae
logic
Analyzer
24MHz 8CH
CH1
CH3
CH5
CH7
CLK
CH2
CH4
CH6
CH8
GND
PWR
CH1
TriKey
Scanning...
Config
433.92 AM 00/50

Logic Analysis



What do these numbers mean?

“It’s in the data sheet!” - Dr. Viall



NXP Semiconductors — Product Specification

Fractional-N Transmitter IC (FraNTIC) — PCF7900 / PCH7900

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.

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	

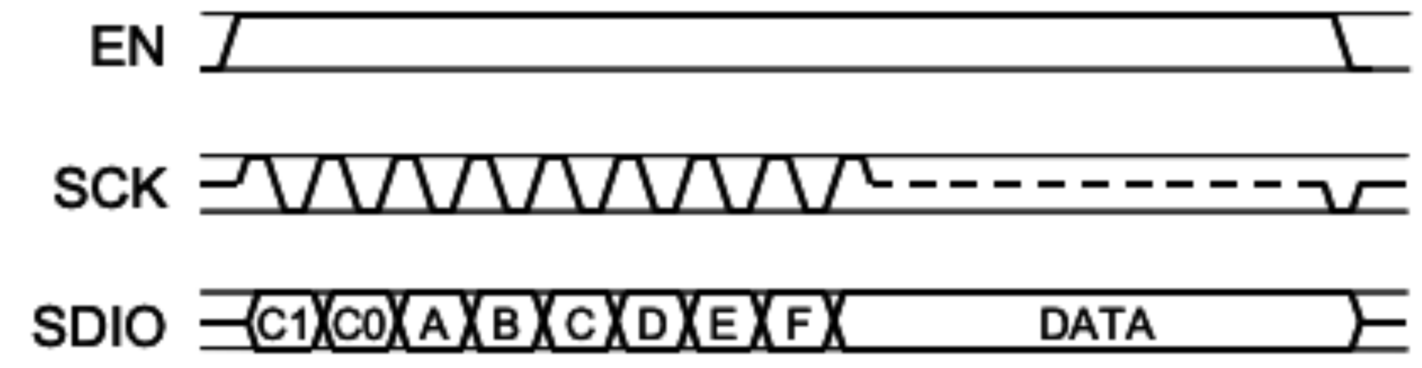
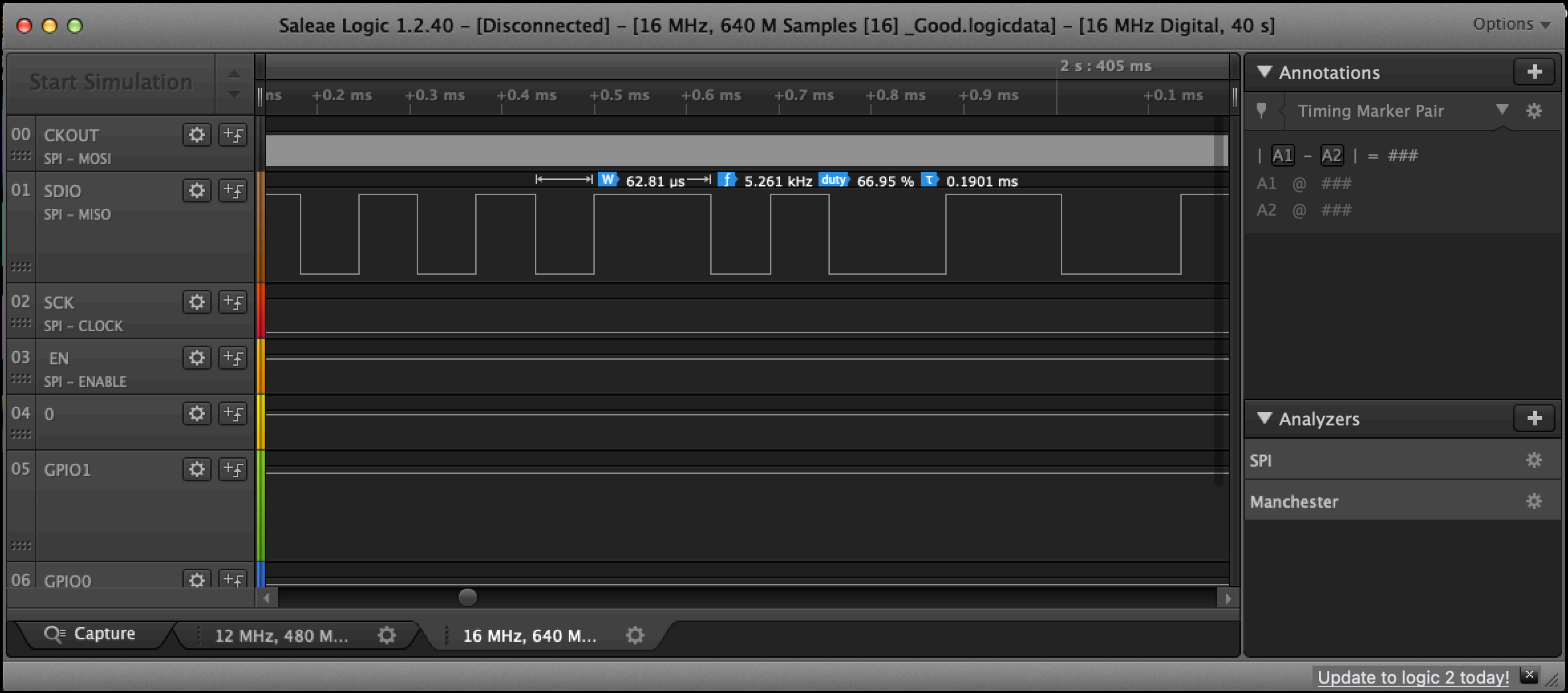


Figure 7. Command Overview

Extracting useful information

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

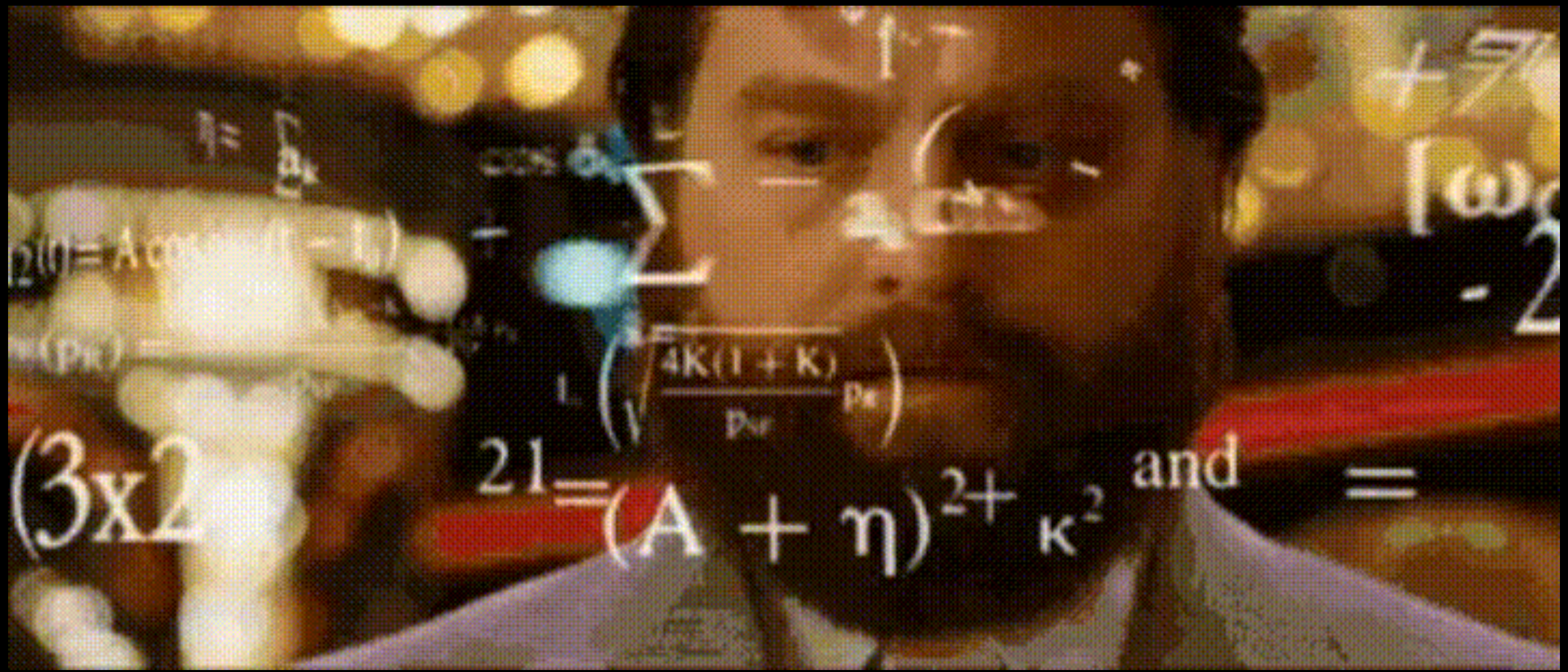
Calculating Manchester bit rate



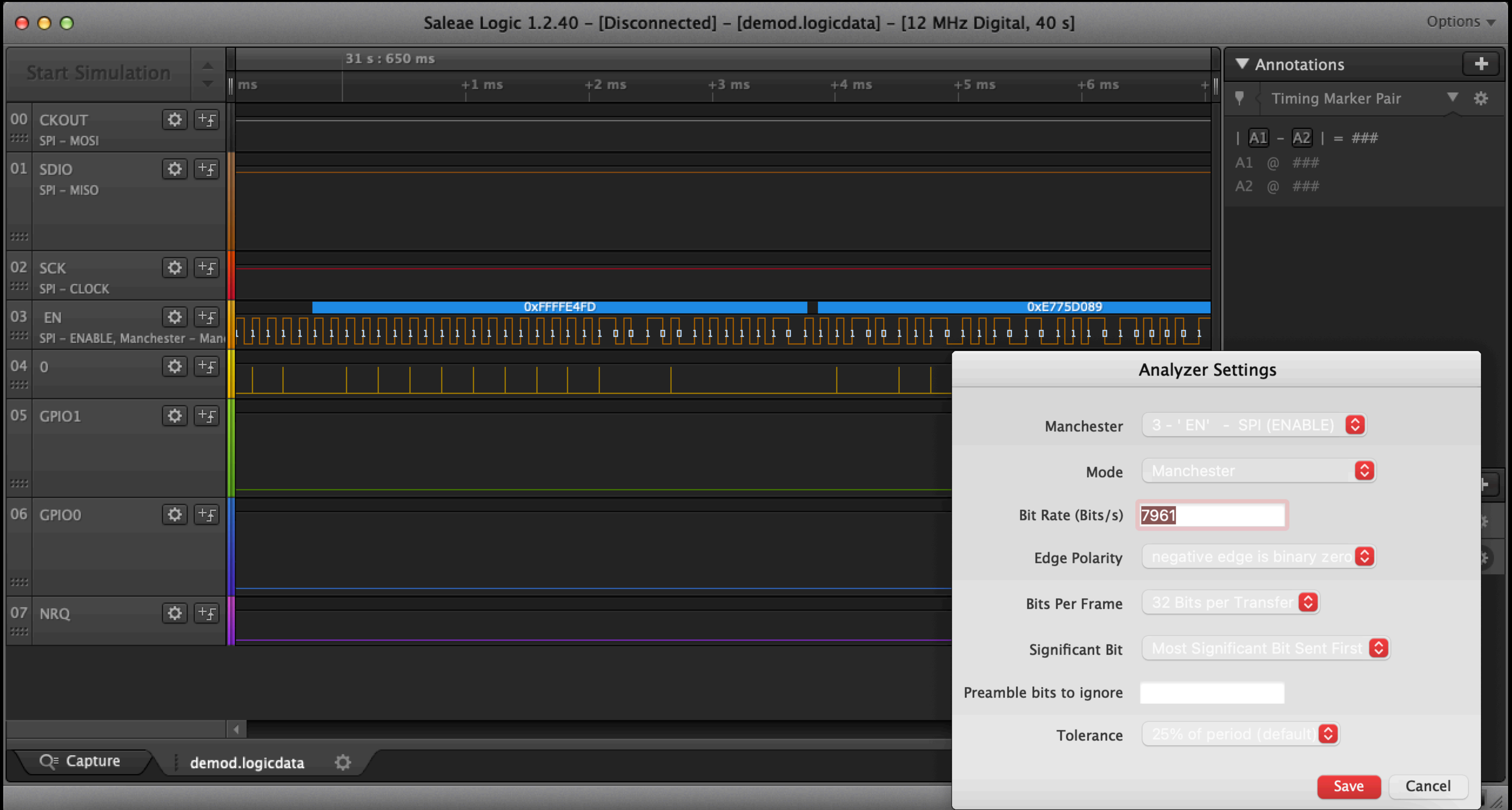
Saleae Logic 1.2.40 – [Disconnected] – [16 MHz, 640 M Samples [16] _Good.logicdata] – [16 MHz Digital, 40 s]

W 62.81 µs f 5.261 kHz duty 66.95 % τ 0.1901 ms

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



Decoding Manchester



Saleae Logic 1.2.40 – [Disconnected] – [demod.logicdata] – [12 MHz Digital, 40 s]

00	CKOUT SPI – MOSI
01	SDIO SPI – MISO
02	SCK SPI – CLOCK
03	EN SPI – ENABLE, Manchester – Man
04	0
05	GPIO1
06	GPIO0
07	NRQ

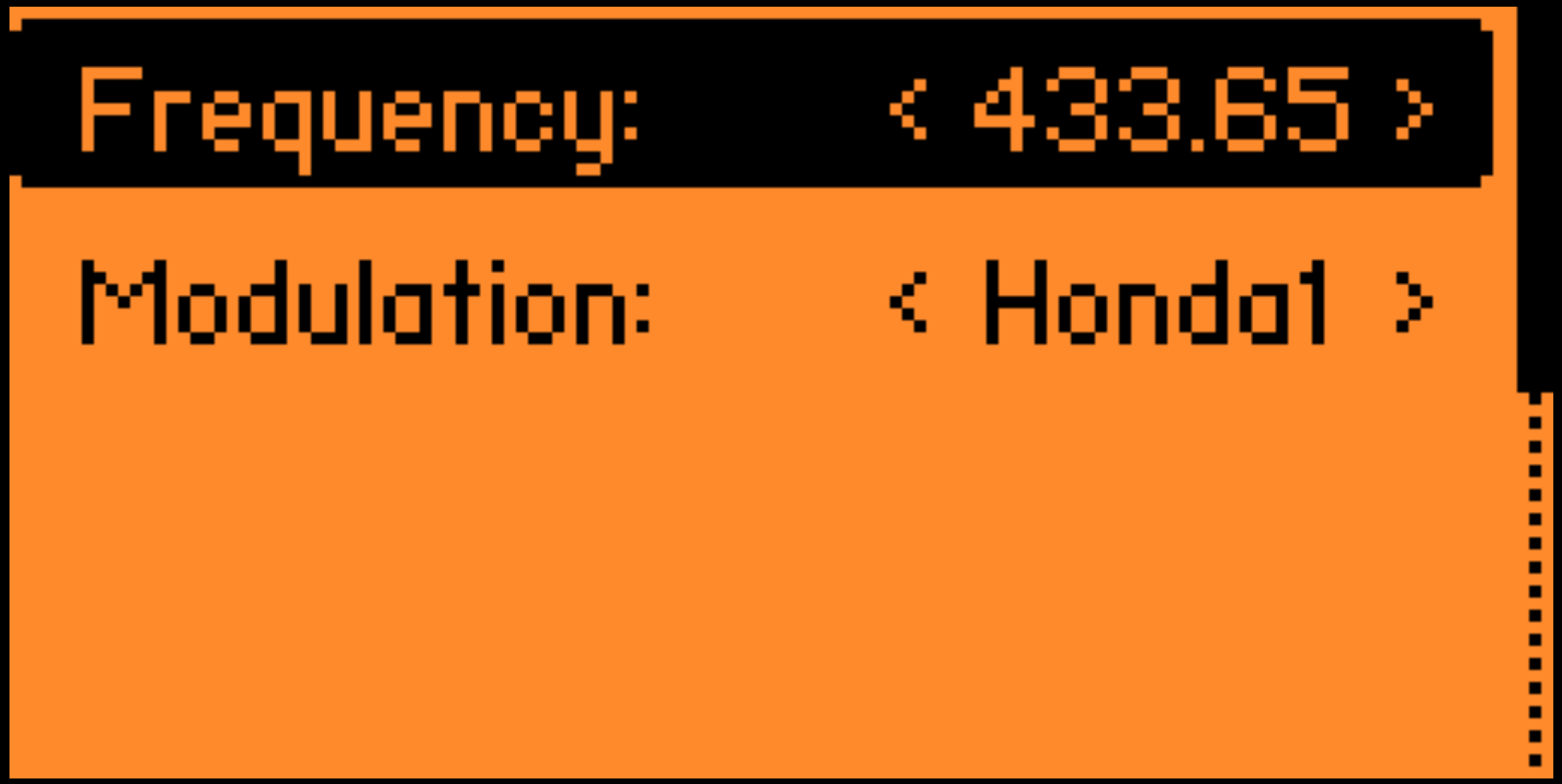
0xFFFFE4FD

0xE775D089

Analyzer Settings

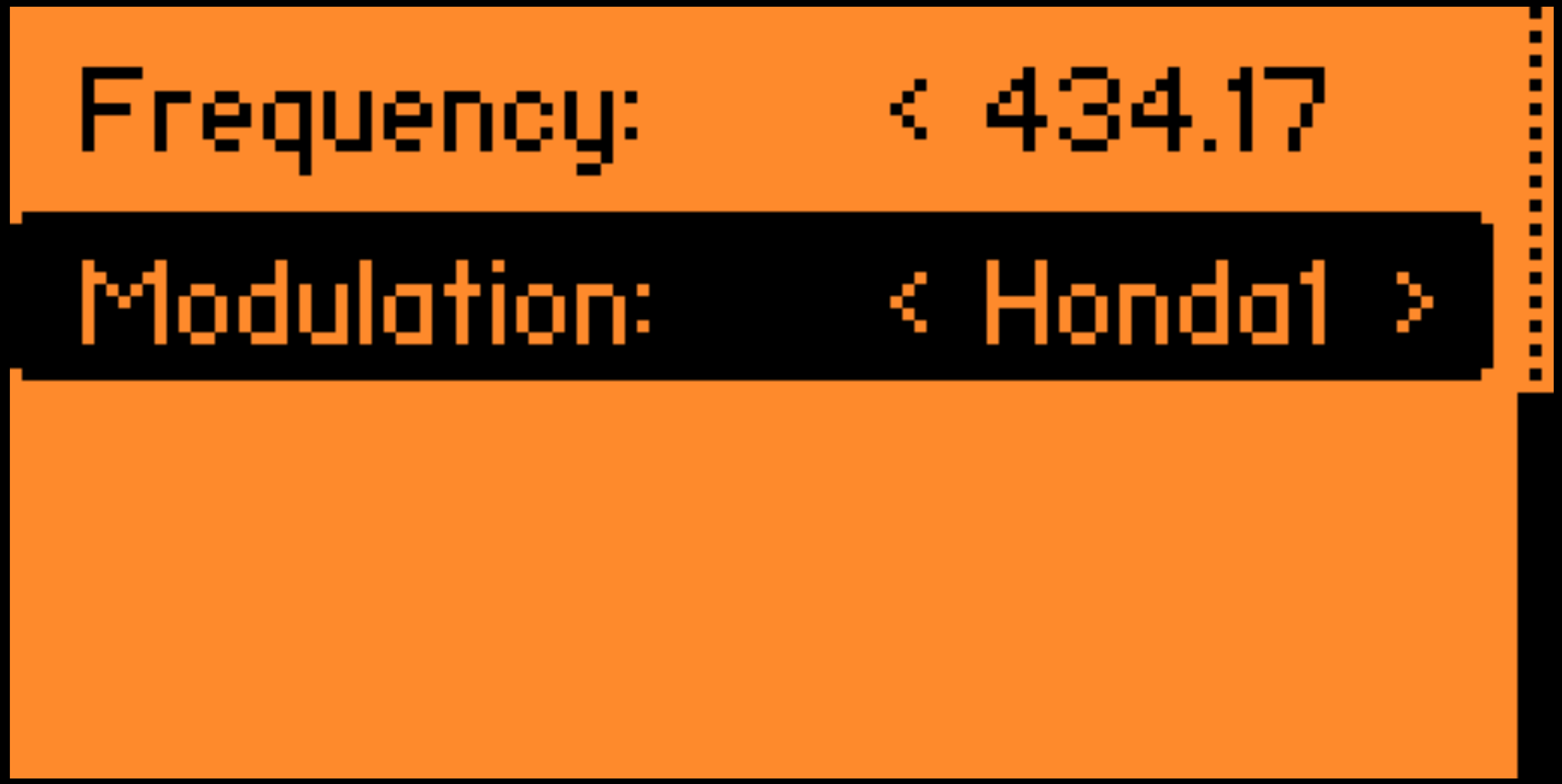
Manchester	3 - ' EN' - SPI (ENABLE)
Mode	Manchester
Bit Rate (Bits/s)	7961
Edge Polarity	negative edge is binary zero
Bits Per Frame	32 Bits per Transfer
Significant Bit	Most Significant Bit Sent First
Preamble bits to ignore	
Tolerance	25% of period (default)

Adding support for our cyber-dolphin friend : Flipper Zero



Frequency: < 433.65 >

Modulation: < Honda1 >



Frequency: < 434.17

Modulation: < Honda1 >

Captured using QFlipper App

AIRSPY SDR# Studio v1.0.0.1868 - HackRF

000.433.660.211

Step: 1 Hz

Radio

○ NFM ○ AM ○ LSB ○ USB
○ WFM ○ DSB ○ CW ● RAW

☑ Shift 0

Filter: Blackman-Harris 4

Bandwidth: 1,470

Order: 1,000

□ Squelch

CW Shift

Source: HackRF

HackRF

Recording *

Status

File Size	0 MB
Duration	00:00:00
Dropped Buffers	0

Mode

Sample Format: 16 B

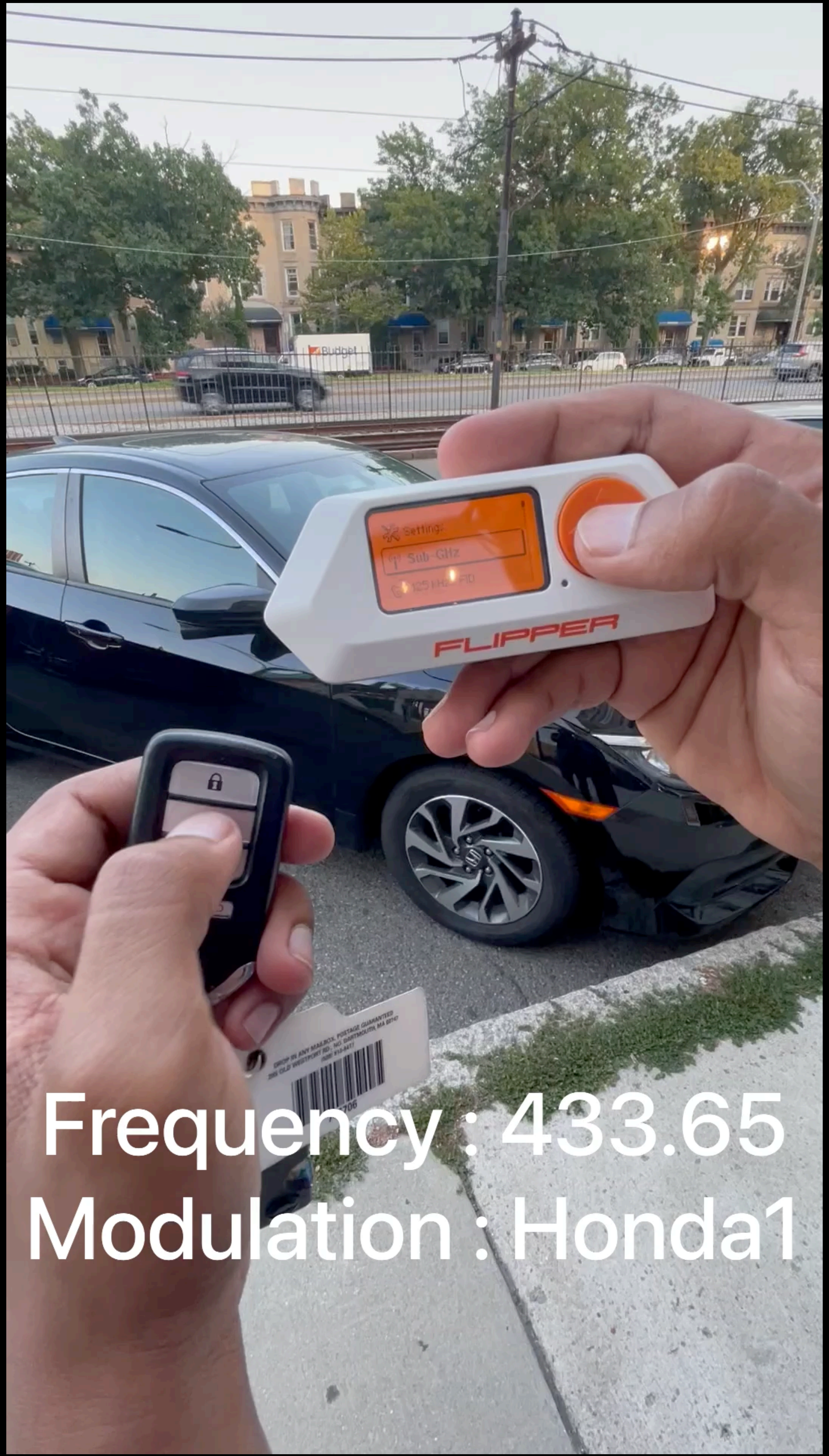
Audio □ □ Baseba

Record

433.6435 MHz
-92.2 dBFS
70cm Ham Band

Frequency Manager *
AIRSPY
dBFS
-20
-30
-40
-50
-60
-70
-80
-90
-100
433.600 M
433.625 M
433.650 M
433.675 M
433.700 M
433.725 M
5
Zoom
Contrast
Range
Offset
Flipper Zero
Key Fob

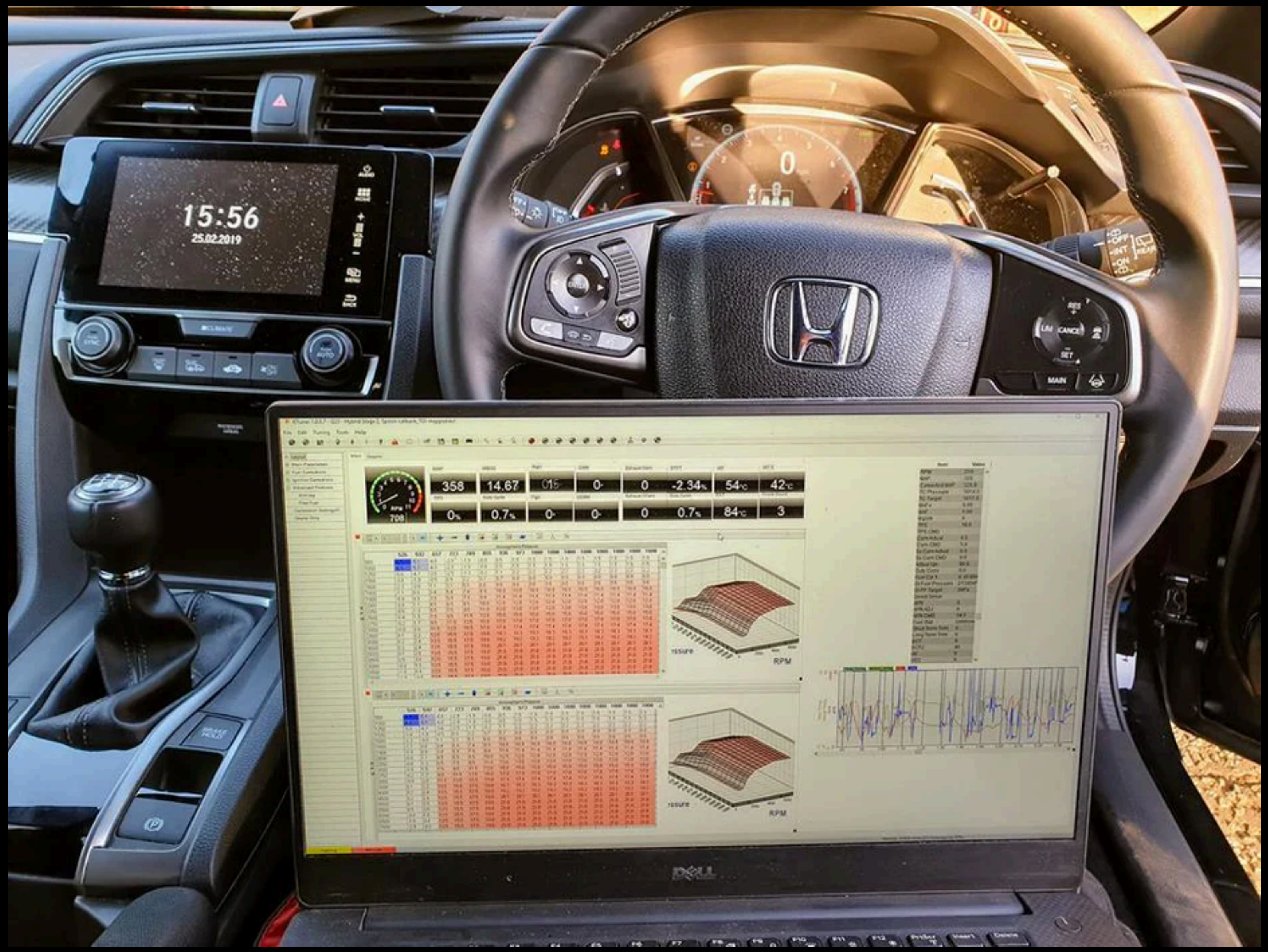
Flipper Zero Demo



Frequency : 433.65

Modulation : Honda1

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



BMW I8
audi r8
toyota supra
HONDA CIVIC WITH LAPTOP
MEMES

Hint: Google the title!

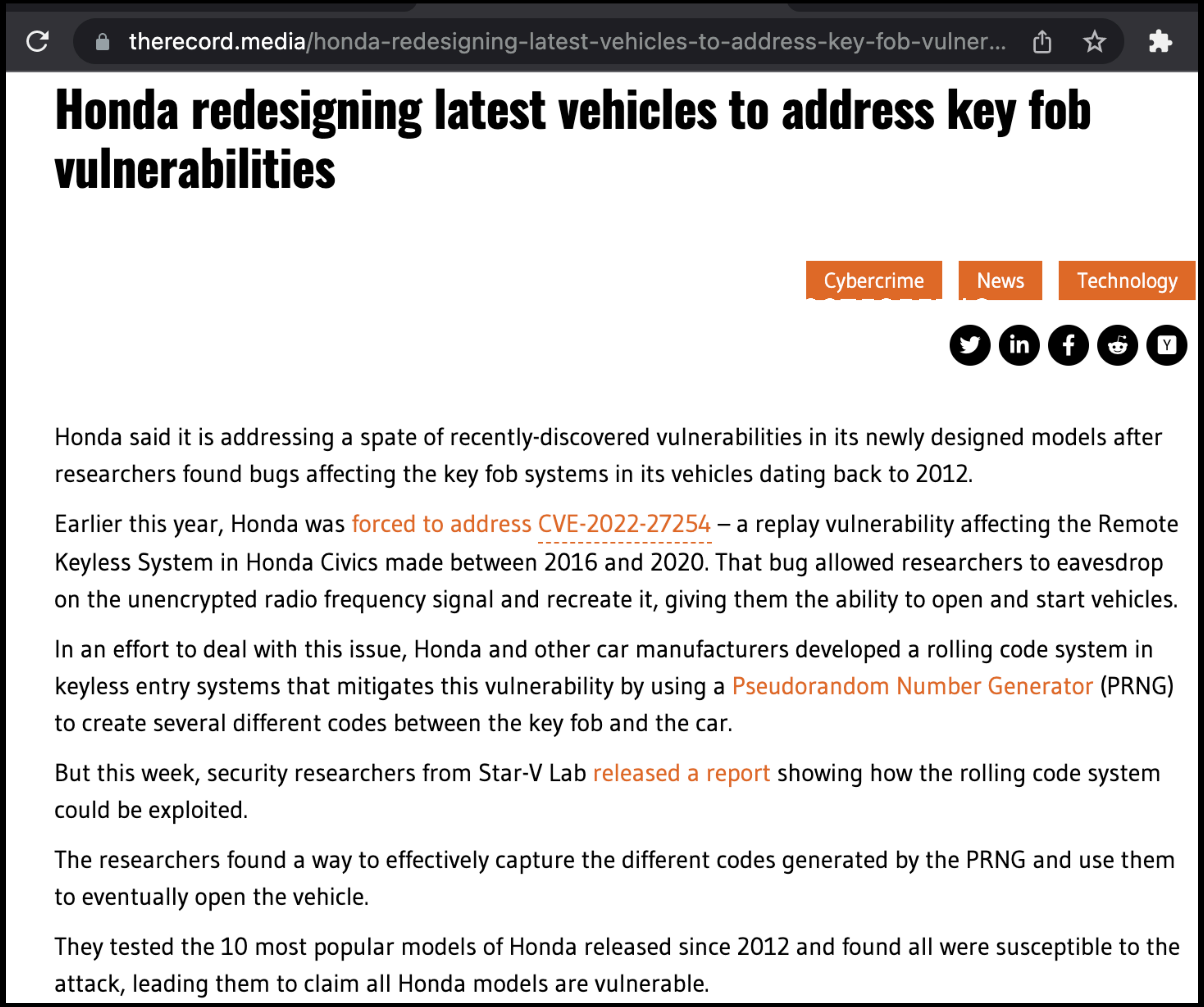
The Ultimate Wardriving Setup

"Civic with a laptop, and a HackRF One”

Solution?

Rolling codes, they’re safer...right?

Rolling Codes pwned too?!



therecord.media/honda-redesigning-latest-vehicles-to-address-key-fob-vulner...

Honda redesigning latest vehicles to address key fob vulnerabilities

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.

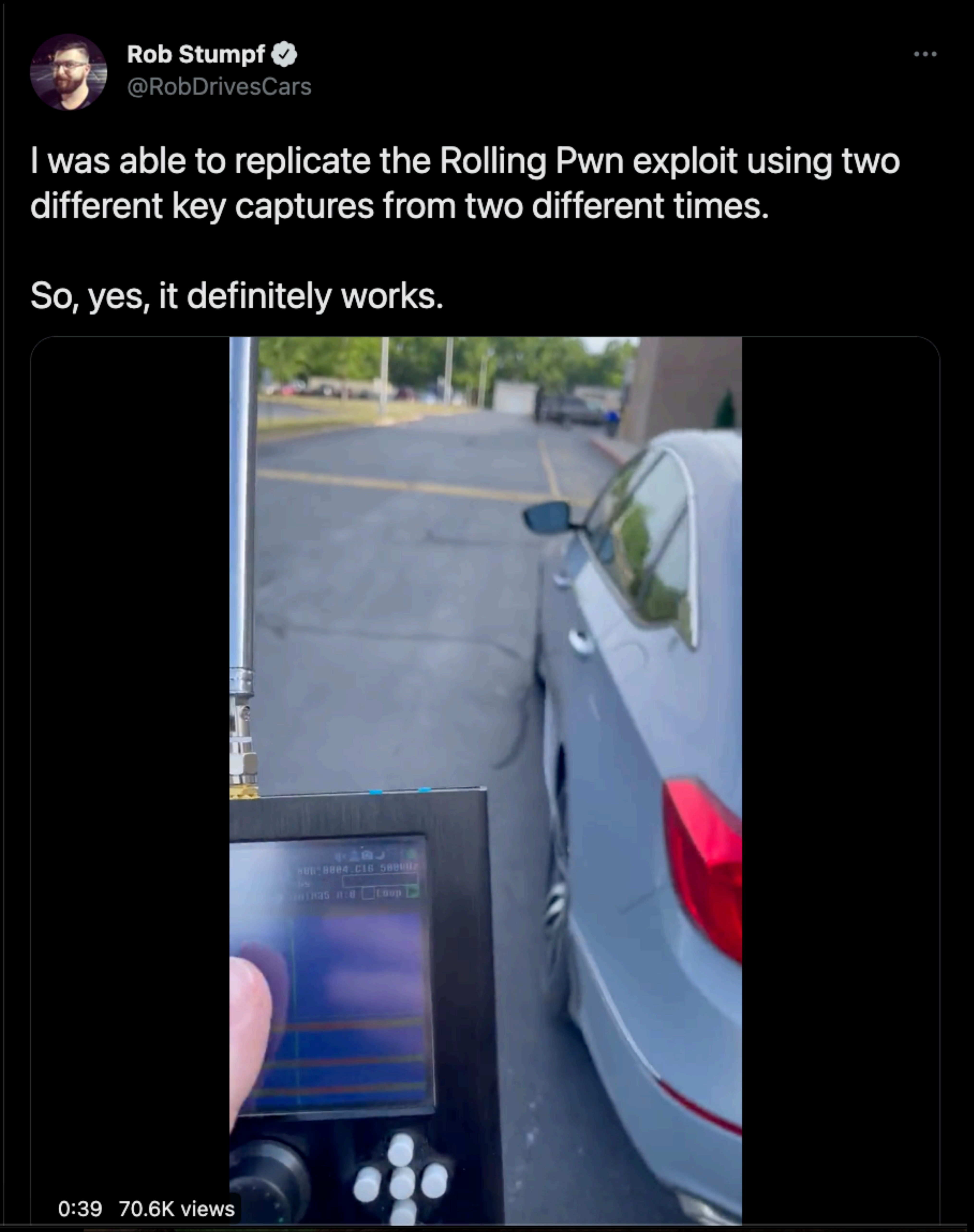
But this week, security researchers from Star-V Lab released a report showing how the rolling code system could be exploited.

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

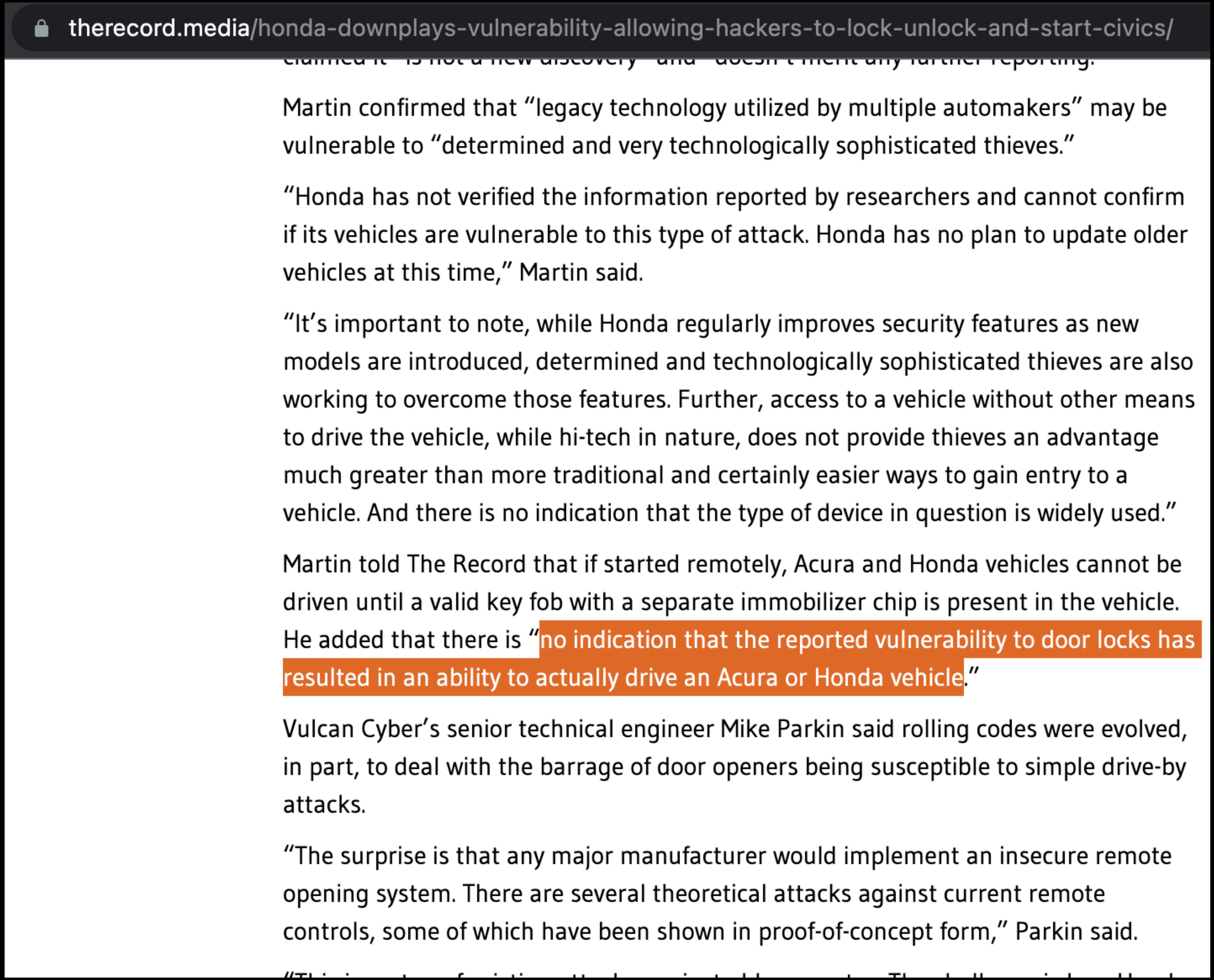


Rob Stumpf
@RobDrivesCars

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



therecord.media/honda-downplays-vulnerability-allowing-hackers-to-lock-unlock-and-start-civics/

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.”

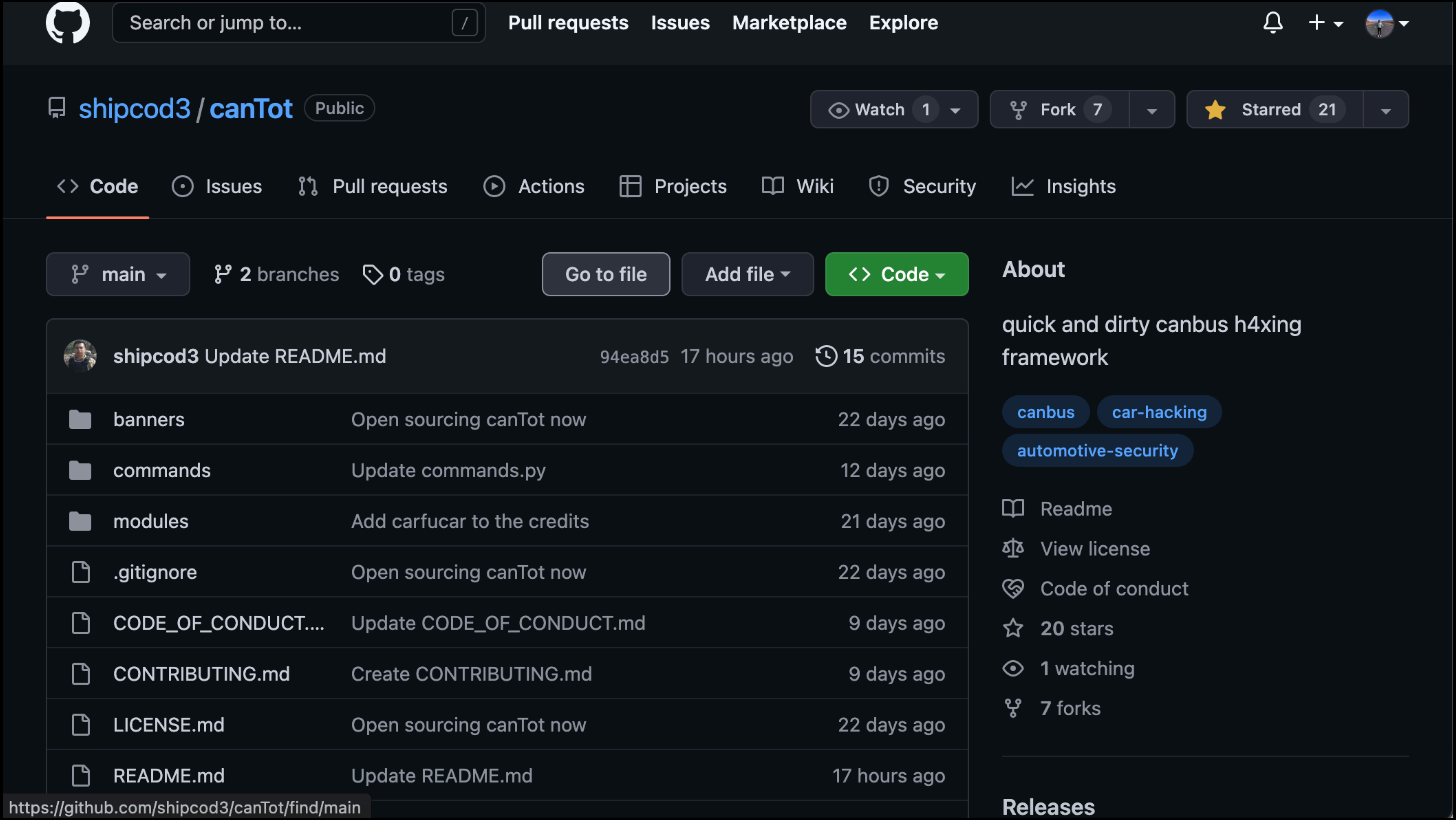
Martin told The Record that if started remotely, Acura and Honda vehicles cannot be driven until a valid key fob with a separate immobilizer chip is present in the vehicle. He added that there is “no indication that the reported vulnerability to door locks has resulted in an ability to actually drive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



shipcod3 / canTot Public

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

About

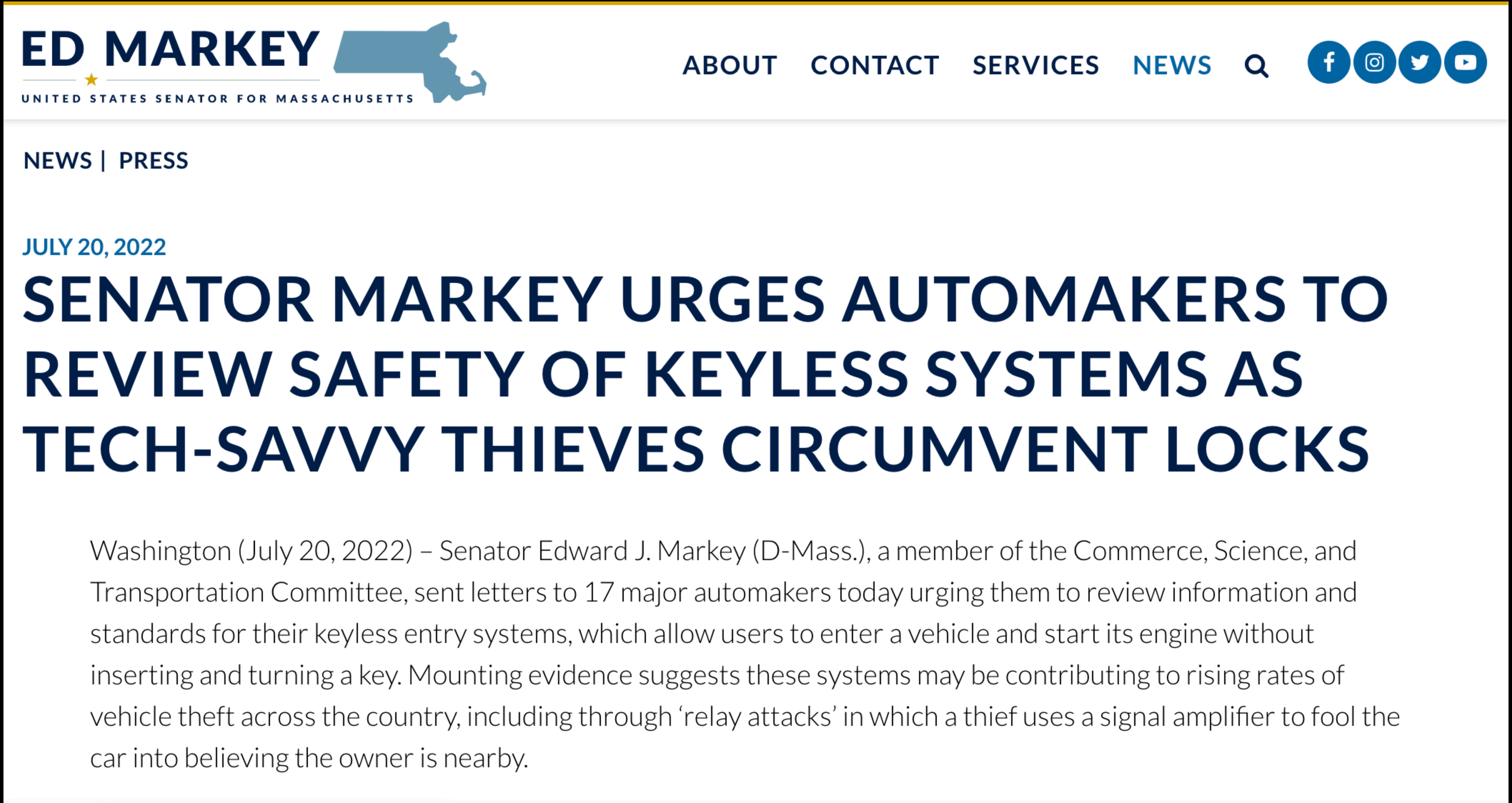
quick and dirty canbus h4xing framework

canbus car-hacking automotive-security

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

Releases

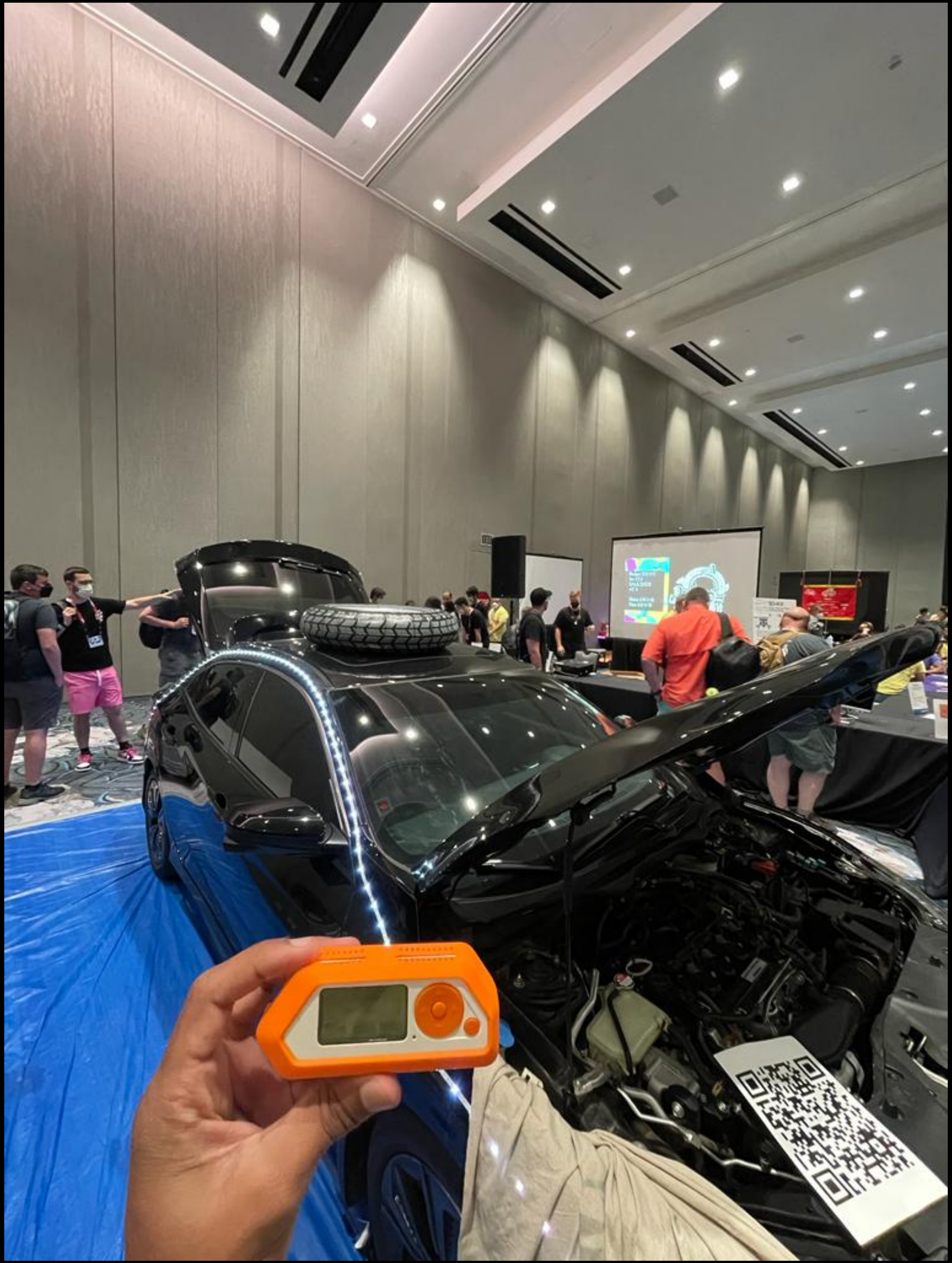
https://github.com/shipcod3/canTot/find/main

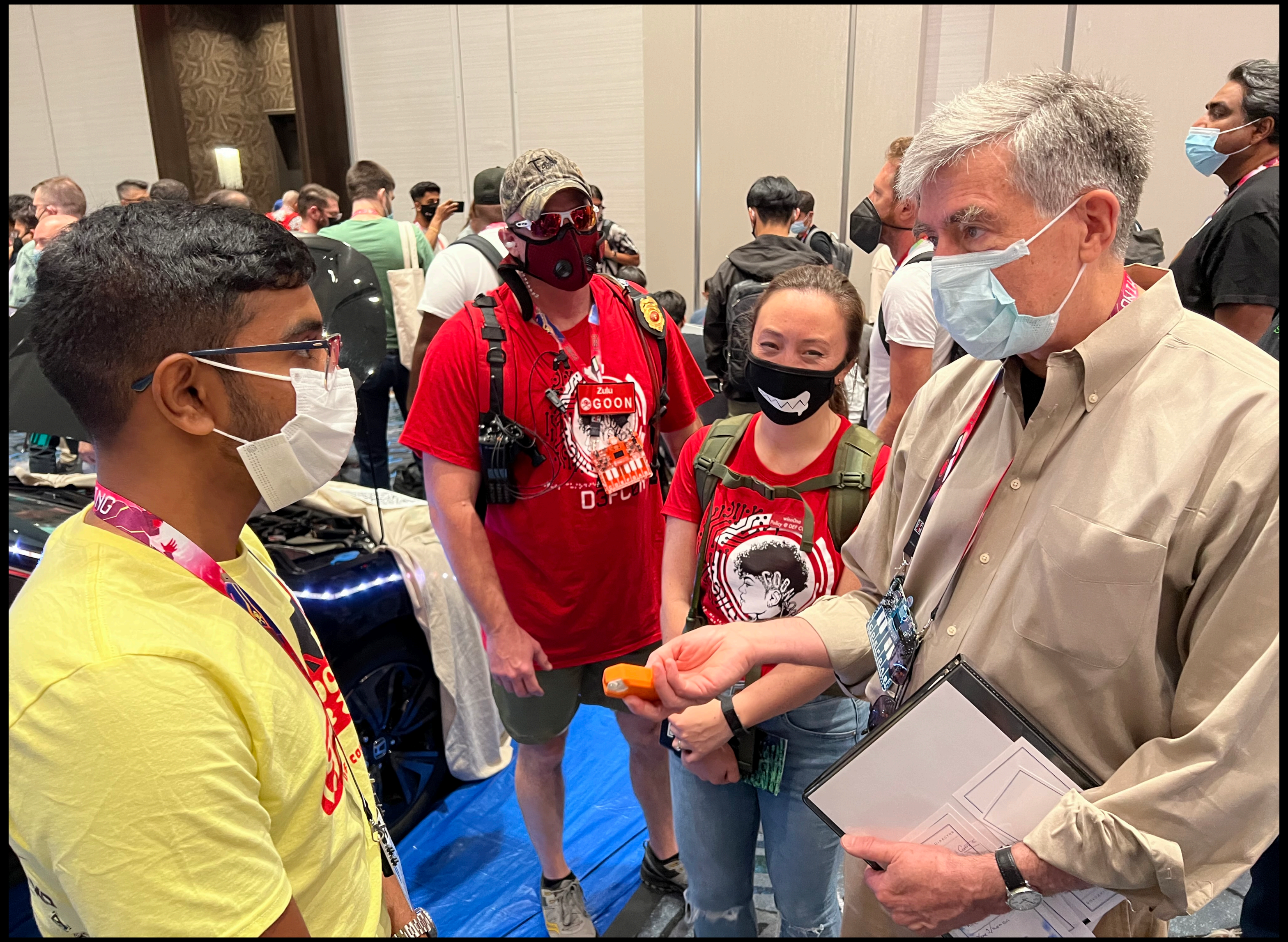


JULY 20, 2022

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.





GOON

What Next?

Join us on this journey!

- Help us create a list of every vulnerable vehicle! Sign up at https://forms.gle/duNtw2UcmPgTdRPM9 or by scanning the QR code below!

- Flipper Zero Custom Firmware is available on GitHub or through Unofficial firmware!

SCAN ME

PWN

Thank you!

College of Engineering
UMass Dartmouth

East Coast
CHIP KEYS
AUTOMOTIVE & MOTORCYCLE LOCKSMITHS

DISCOVER DEFEND
CAR HACKING VILLAGE
SECURING CRITICAL AUTOMOTIVE SYSTEMS

mac-nels™

MassCyberCenter
at the MassTech Collaborative

References / Further Reading

- http://opengarages.org/handbook/ebook/
- https://medium.com/@victor_14768/replay-attacks-en-autos-206481dcfee1
- 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://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.cbsnews.com/boston/news/scituate-snow-sunroof-open-weather-minivan/
- https://www.youtube.com/watch?v=yHoxOMXK_fY
- https://www.nhtsa.gov/road-safety/vehicle-theft-prevention