HOW I DID I END UP IN YOUR CAR

A basic guide in car locking systems and attacks

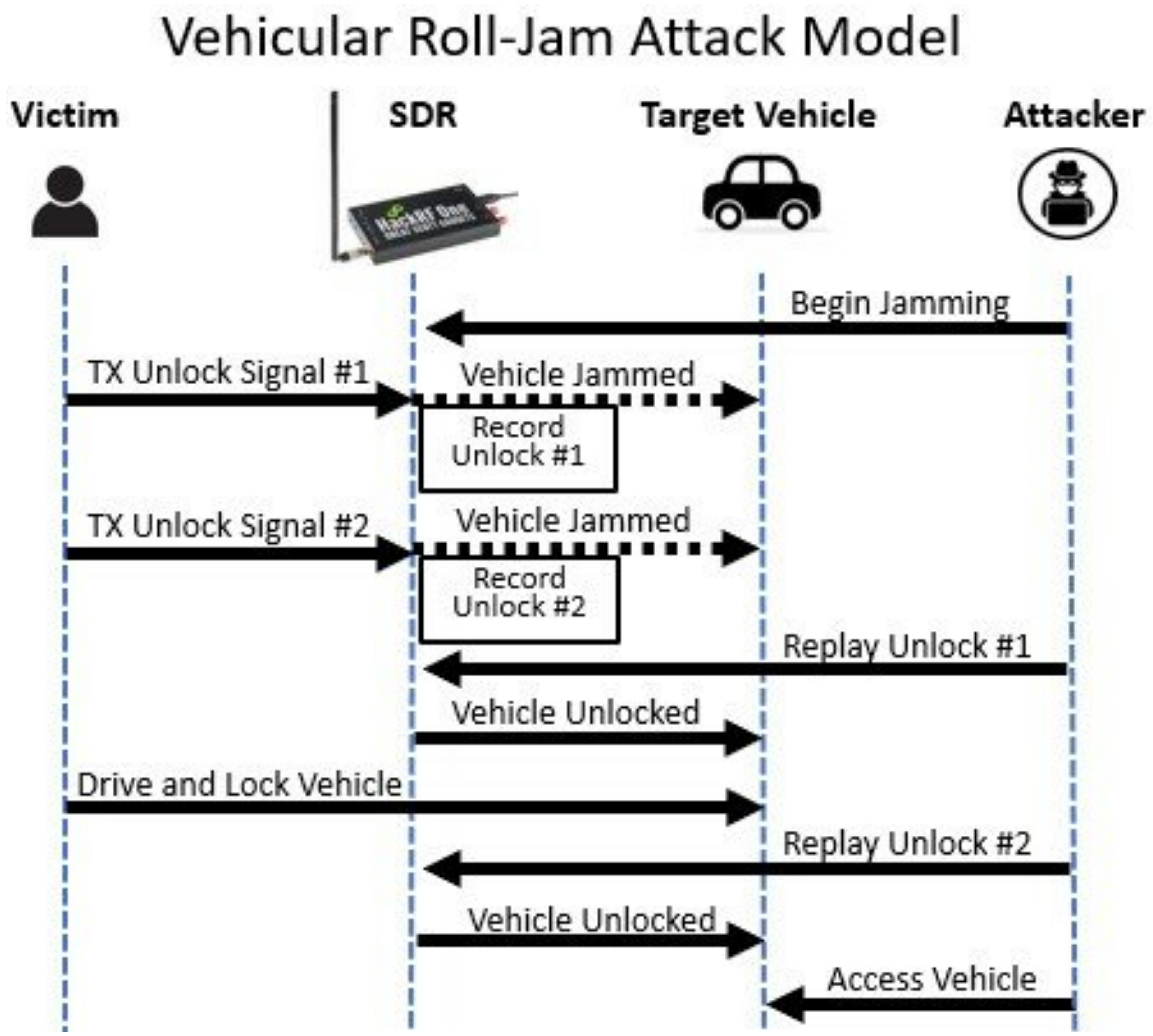
Why does this matter?

Most popular car attacks

- RollJam attack
- RollBack
- Passive car entering systems attack

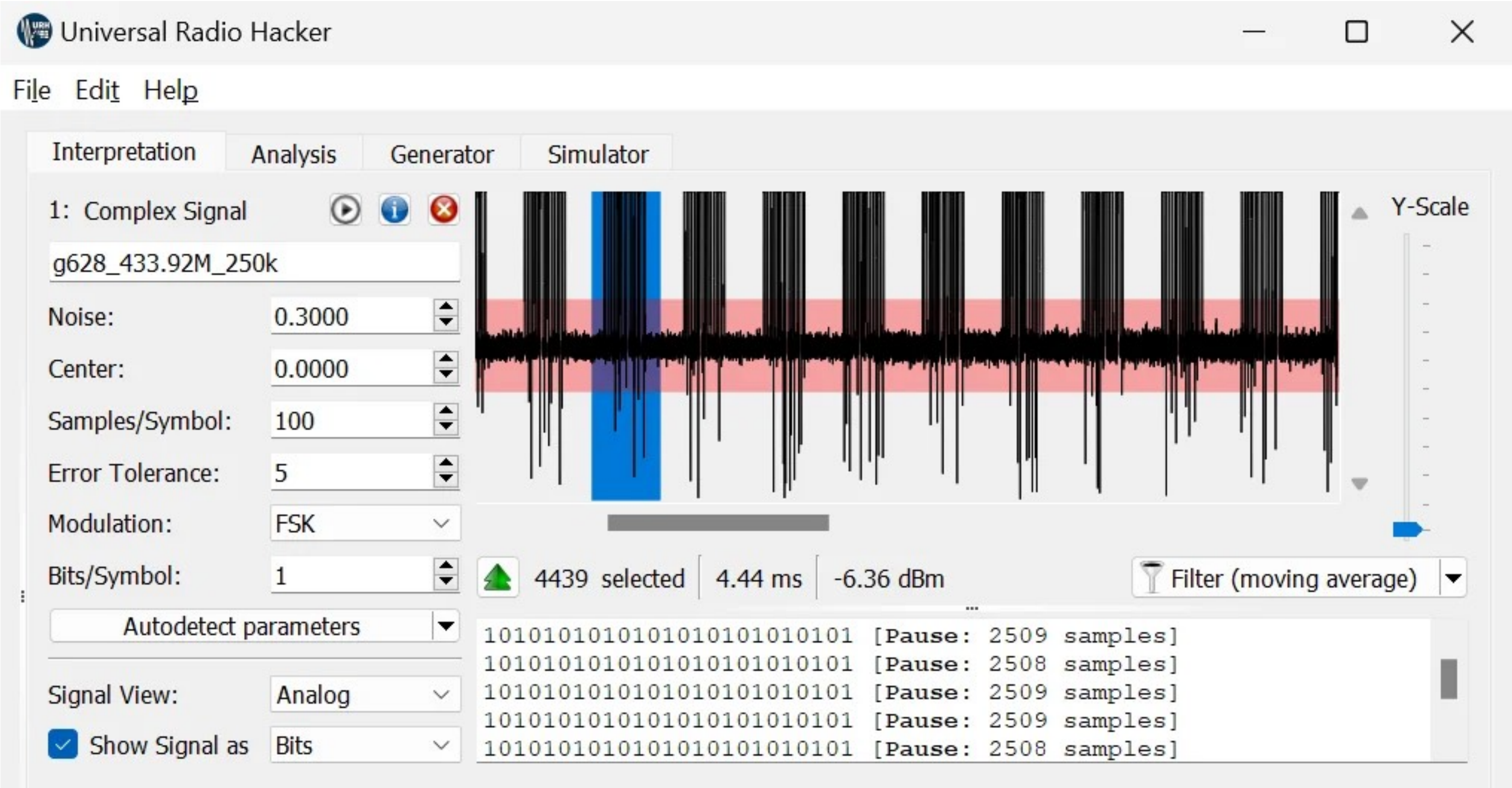
RollJam Attack

Steps of attack



What you get

Radio Hacker for analysis



1: Complex Signal

g628_433.92M_250k

Noise: 0.3000

Center: 0.0000

Samples/Symbol: 100

Error Tolerance: 5

Modulation: FSK

Bits/Symbol: 1

Signal View: Analog

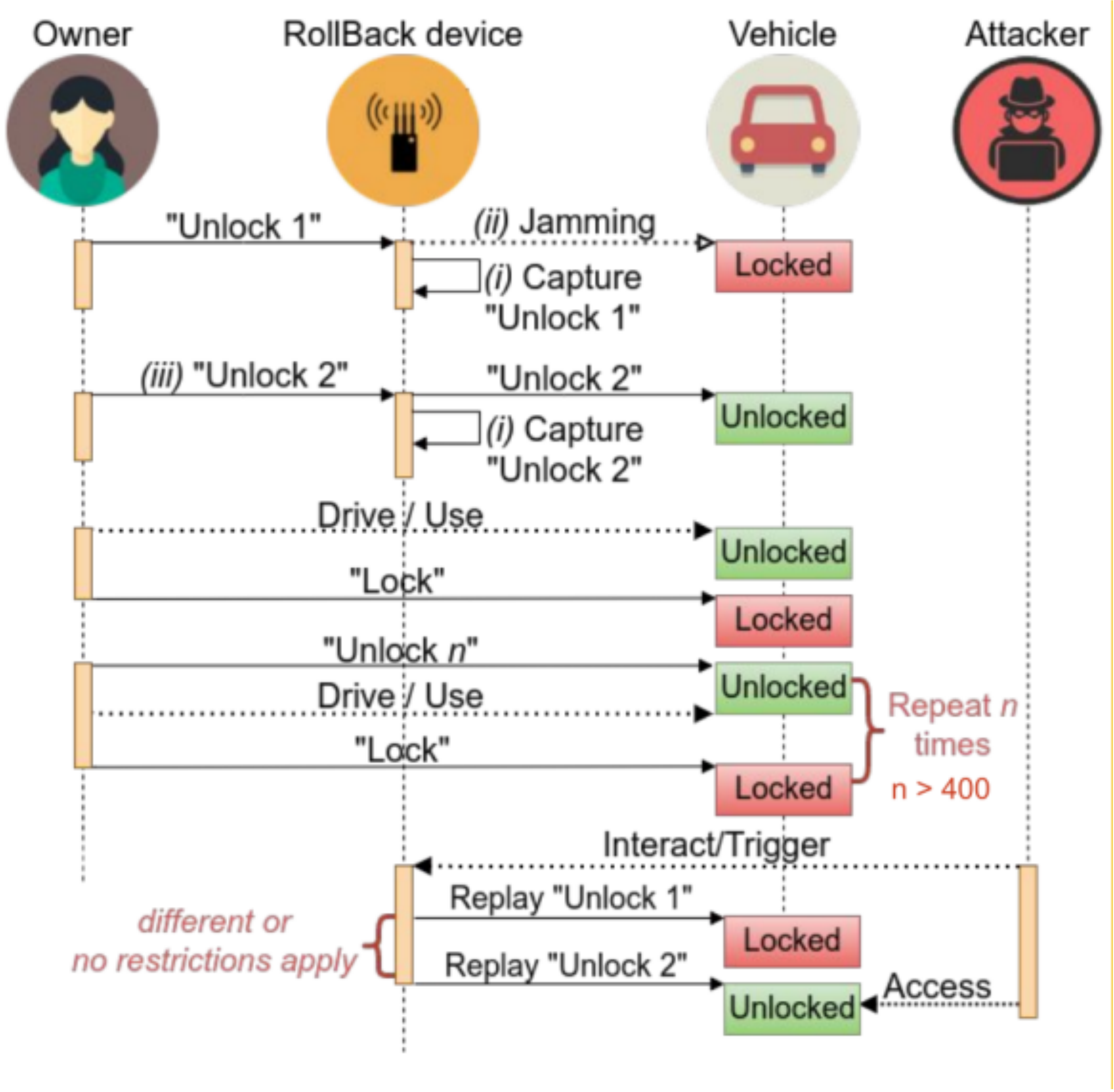
☑ Show Signal as Bits

4439 selected | 4.44 ms | -6.36 dBm

```
1010101010101010101010101 [Pause: 2509 samples]
1010101010101010101010101 [Pause: 2508 samples]
1010101010101010101010101 [Pause: 2509 samples]
1010101010101010101010101 [Pause: 2509 samples]
1010101010101010101010101 [Pause: 2508 samples]
```

RollBack Attack

Restart you lock system

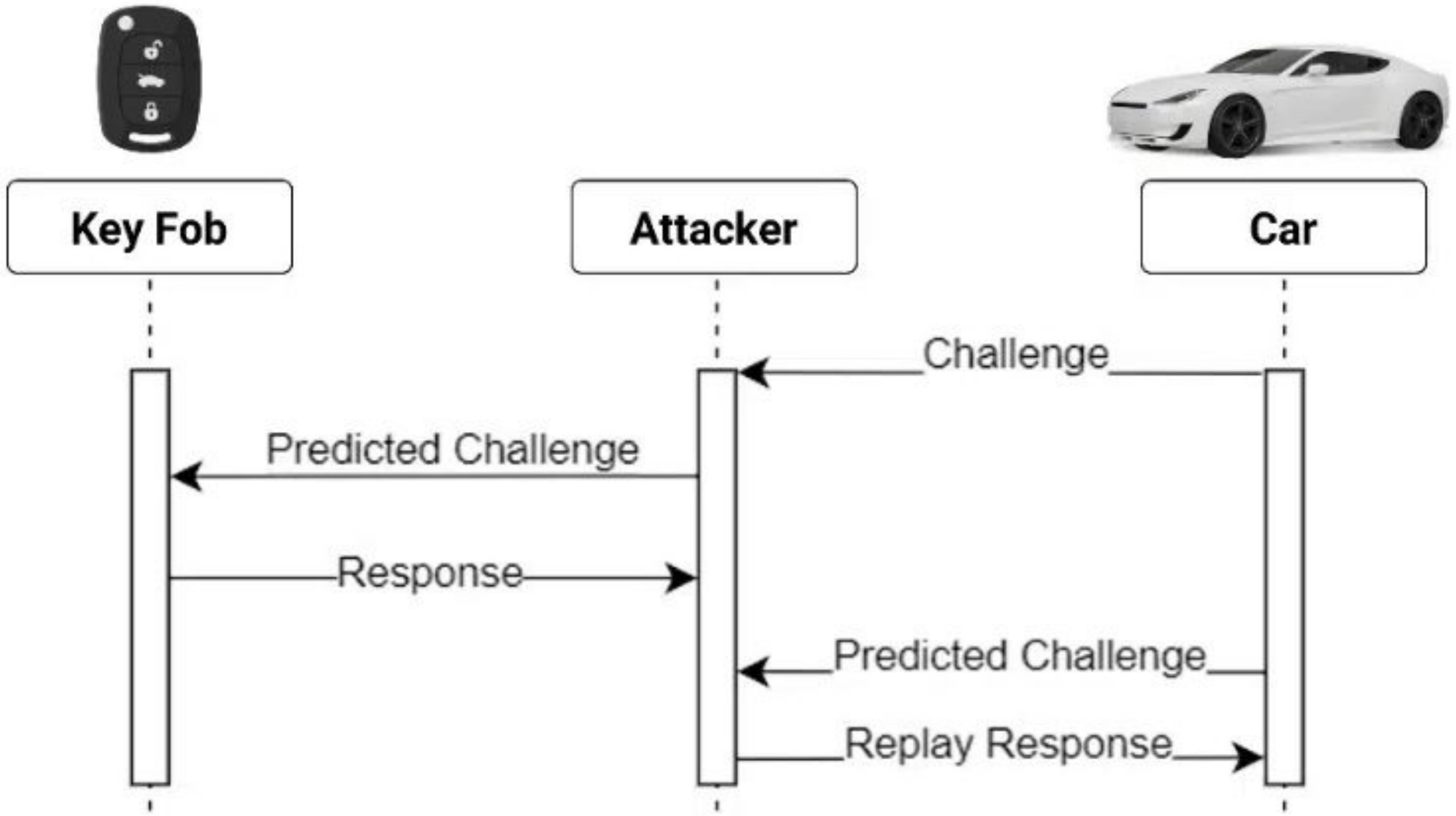


Which model are affected

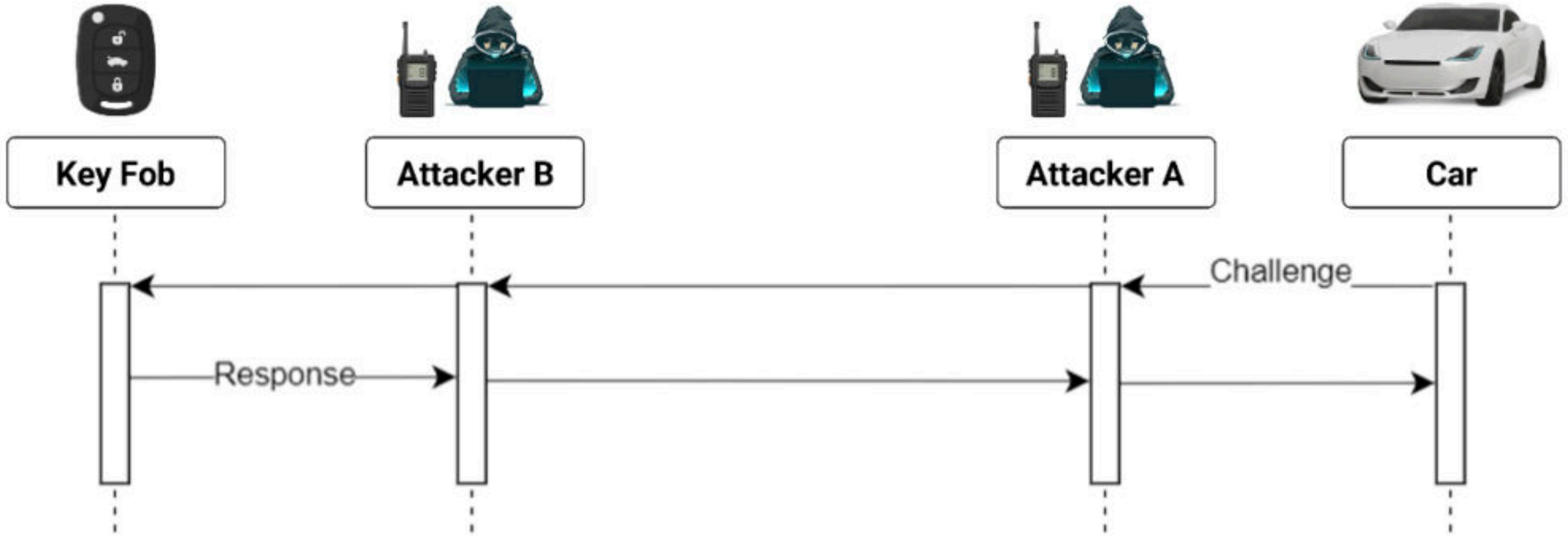
- **Huyndai** - 2015-2021 models
- **KIA** - 2015 - 2021 models
- **Honda -** different models
- **Toyota -** most of US models, some of EU models
- **Tesla 3** - some models and modifications

Keyless entering systems

Relay attack

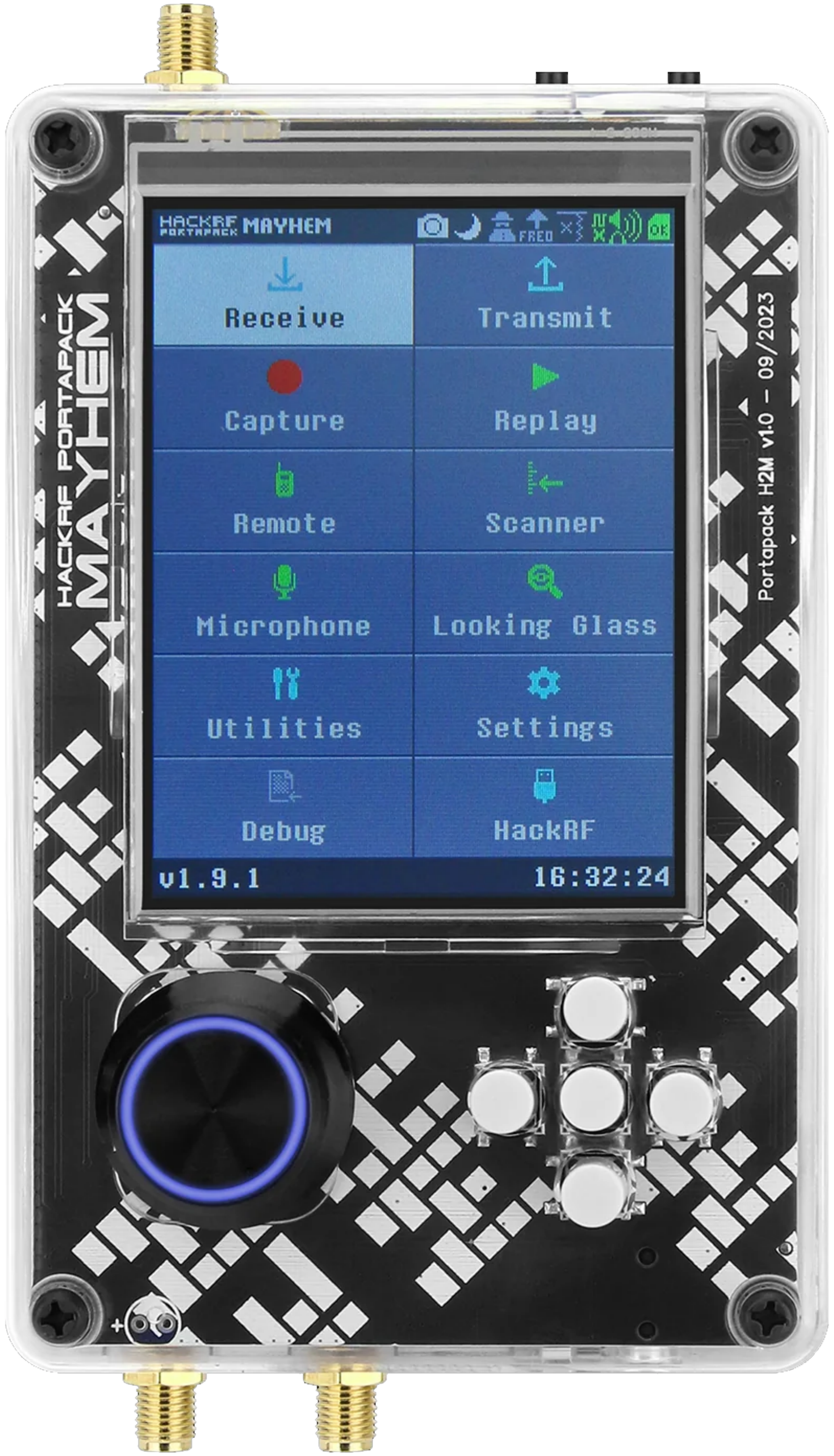


Keyless entering systems



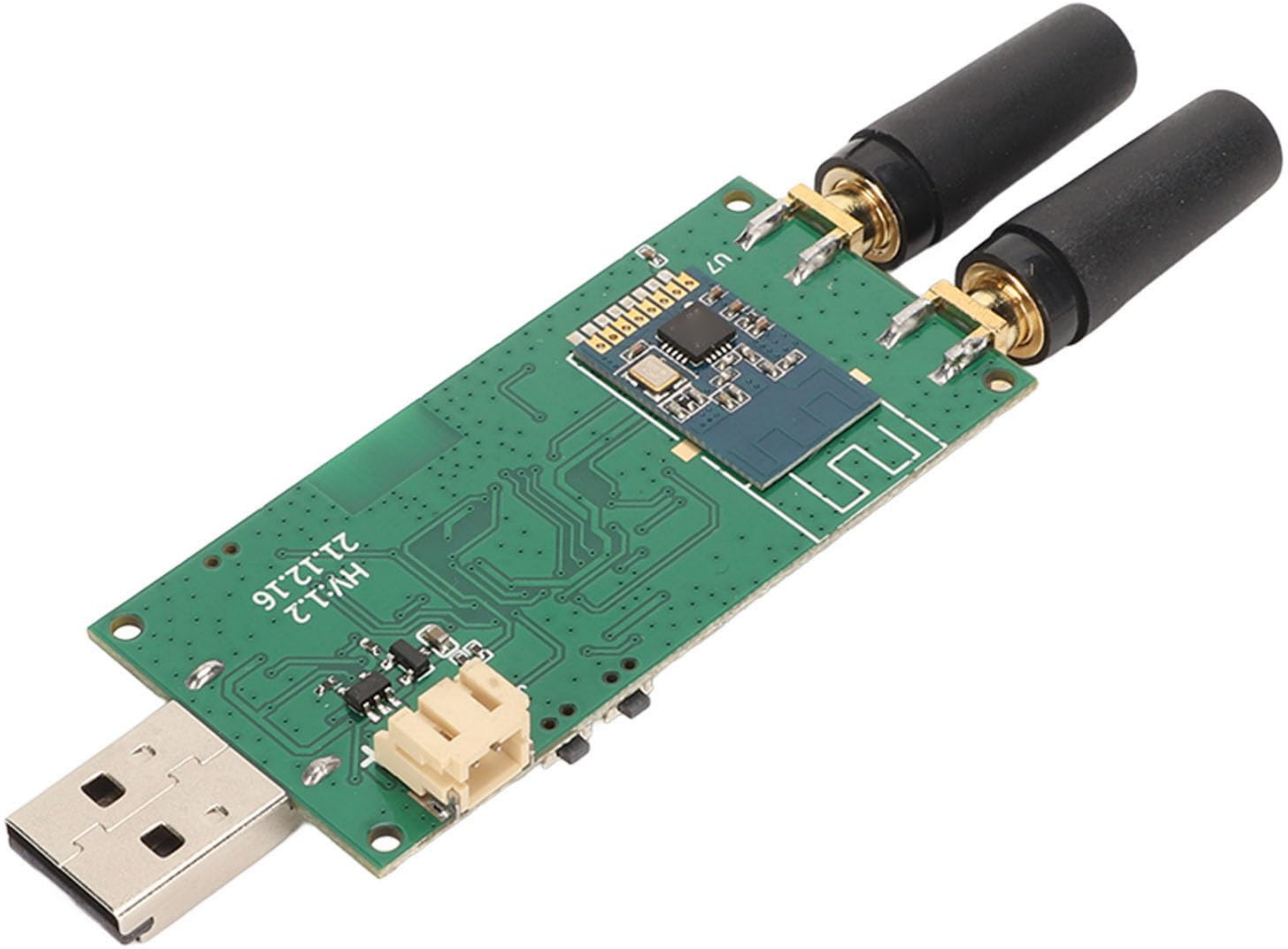
Tools - Hardware

HackRF Portapack



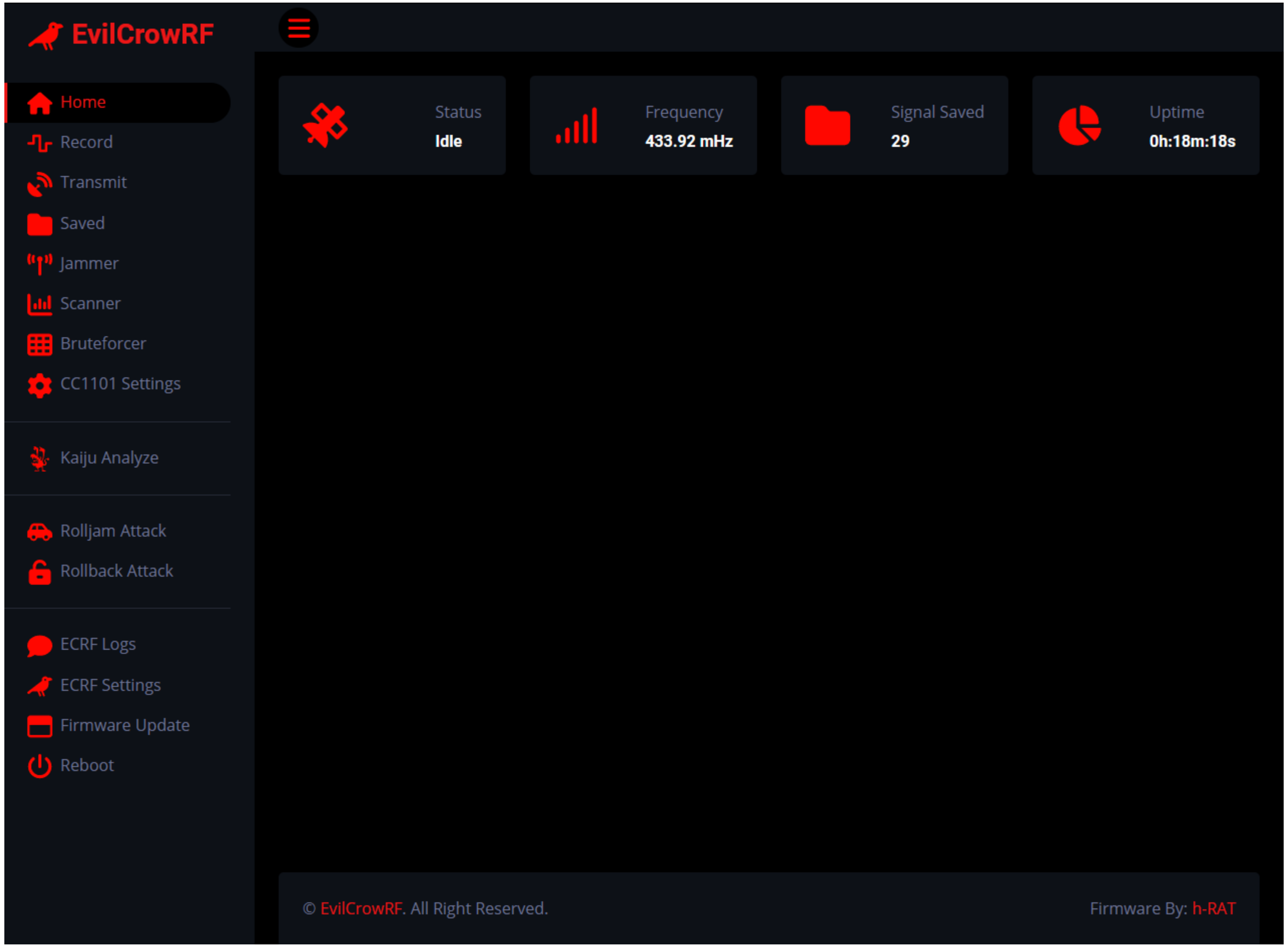
Tools - Hardware

Evil Crow



Tools

Evil Crow H RAT



Status
Idle

Frequency
433.92 mHz

Signal Saved
29

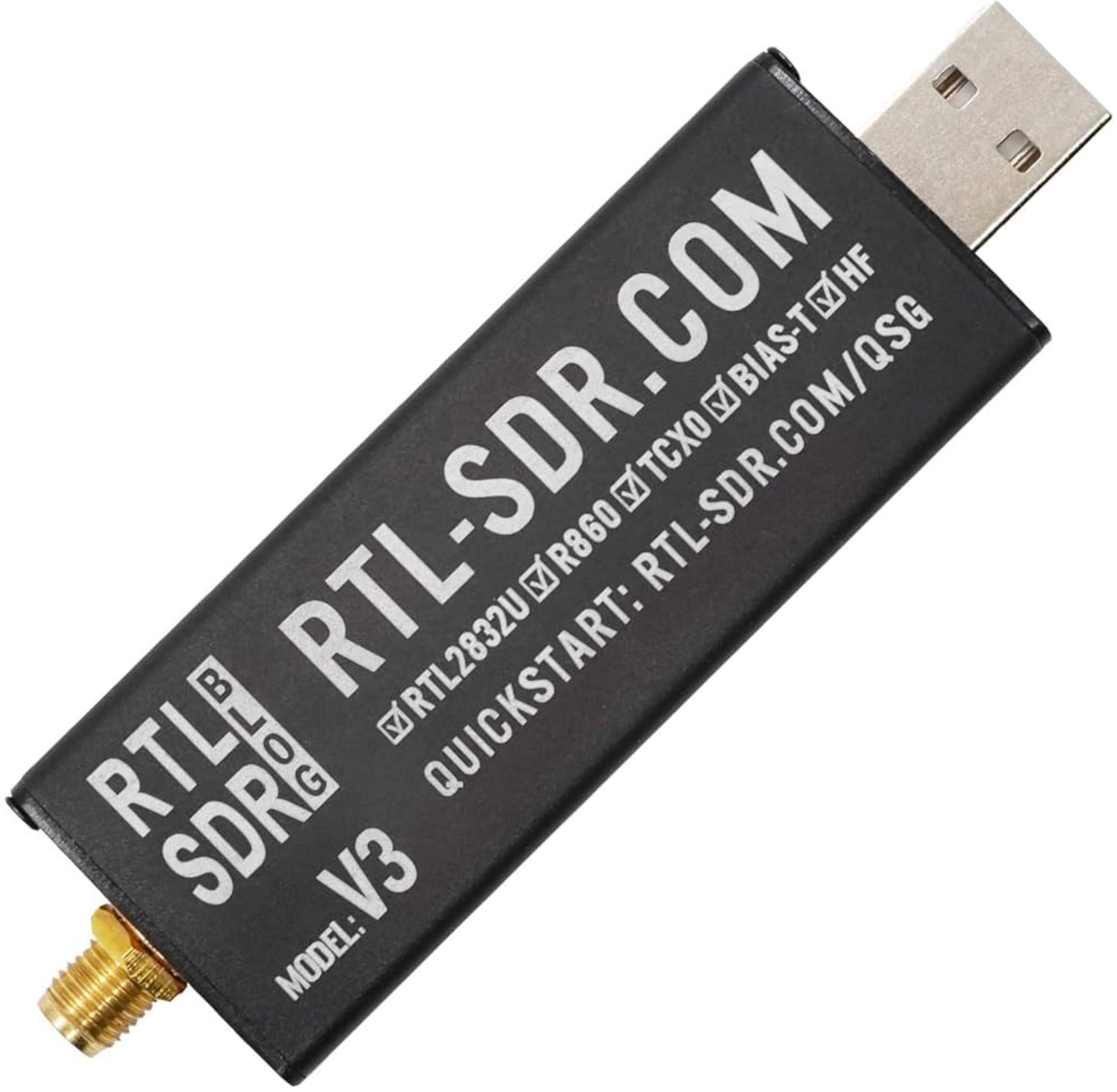
Uptime
0h:18m:18s

© EvilCrowRF. All Right Reserved.

Firmware By: h-RAT

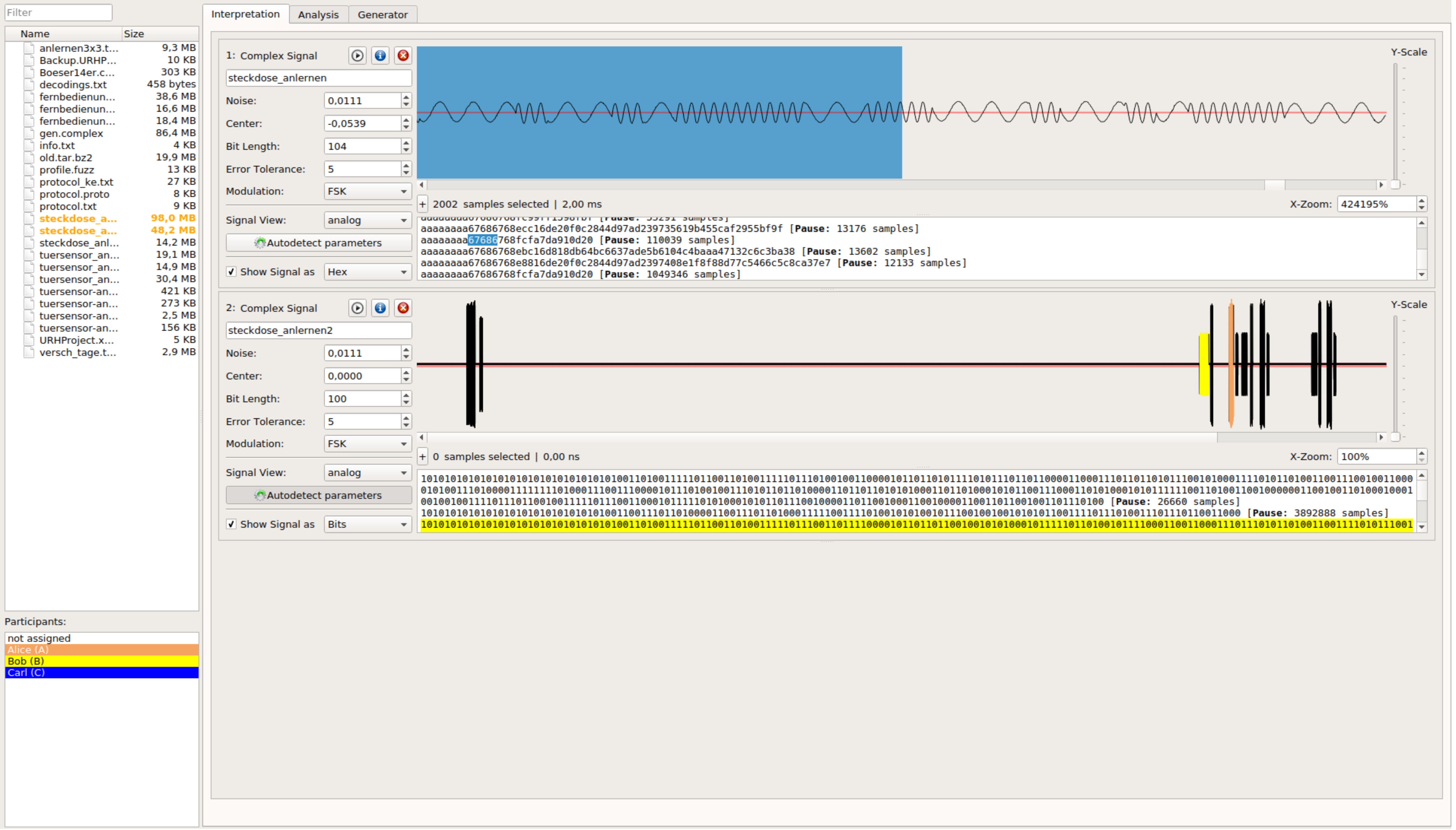
Tools - Hardware

SDR Dongle



Tools - Software

Universal Radio Hacker



Name	Size
anlernen3x3.t...	9,3 MB
Backup.URHP...	10 KB
Boeser14er.c...	303 KB
decodings.txt	458 bytes
fernbedienun...	38,6 MB
fernbedienun...	16,6 MB
fernbedienun...	18,4 MB
gen.complex	86,4 MB
info.txt	4 KB
old.tar.bz2	19,9 MB
profile.fuzz	13 KB
protocol_ke.txt	27 KB
protocol.proto	8 KB
protocol.txt	9 KB
steckdose_a...	**98,0 MB**
steckdose_a...	**48,2 MB**
steckdose_anl...	14,2 MB
tuersensor_an...	19,1 MB
tuersensor_an...	14,9 MB
tuersensor_an...	30,4 MB
tuersensor-an...	421 KB
tuersensor-an...	273 KB
tuersensor-an...	2,5 MB
tuersensor-an...	156 KB
URHProject.x...	5 KB
versch_tage.t...	2,9 MB

Participants:

- not assigned
- Alice (A)
- Bob (B)
- Carl (C)

1: Complex Signal

steckdose_anlernen

Noise: 0,0111
Center: -0,0539
Bit Length: 104
Error Tolerance: 5
Modulation: FSK
Signal View: analog
☑ Show Signal as Hex

X-Zoom: 424195%

+ 2002 samples selected | 2,00 ms

```
aaaaaaaa67686768fc99ff1598fbf [Pause: 55291 samples]
aaaaaaaa67686768ecc16de20f0c2844d97ad239735619b455caf2955bf9f [Pause: 13176 samples]
aaaaaaaa67686768fcfa7da910d20 [Pause: 110039 samples]
aaaaaaaa67686768ebc16d818db64bc6637ade5b6104c4baaa47132c6c3ba38 [Pause: 13602 samples]
aaaaaaaa67686768e8816de20f0c2844d97ad2397408e1f8f88d77c5466c5c8ca37e7 [Pause: 12133 samples]
aaaaaaaa67686768fcfa7da910d20 [Pause: 1049346 samples]
```

2: Complex Signal

steckdose_anlernen2

Noise: 0,0111
Center: 0,0000
Bit Length: 100
Error Tolerance: 5
Modulation: FSK
Signal View: analog
☑ Show Signal as Bits

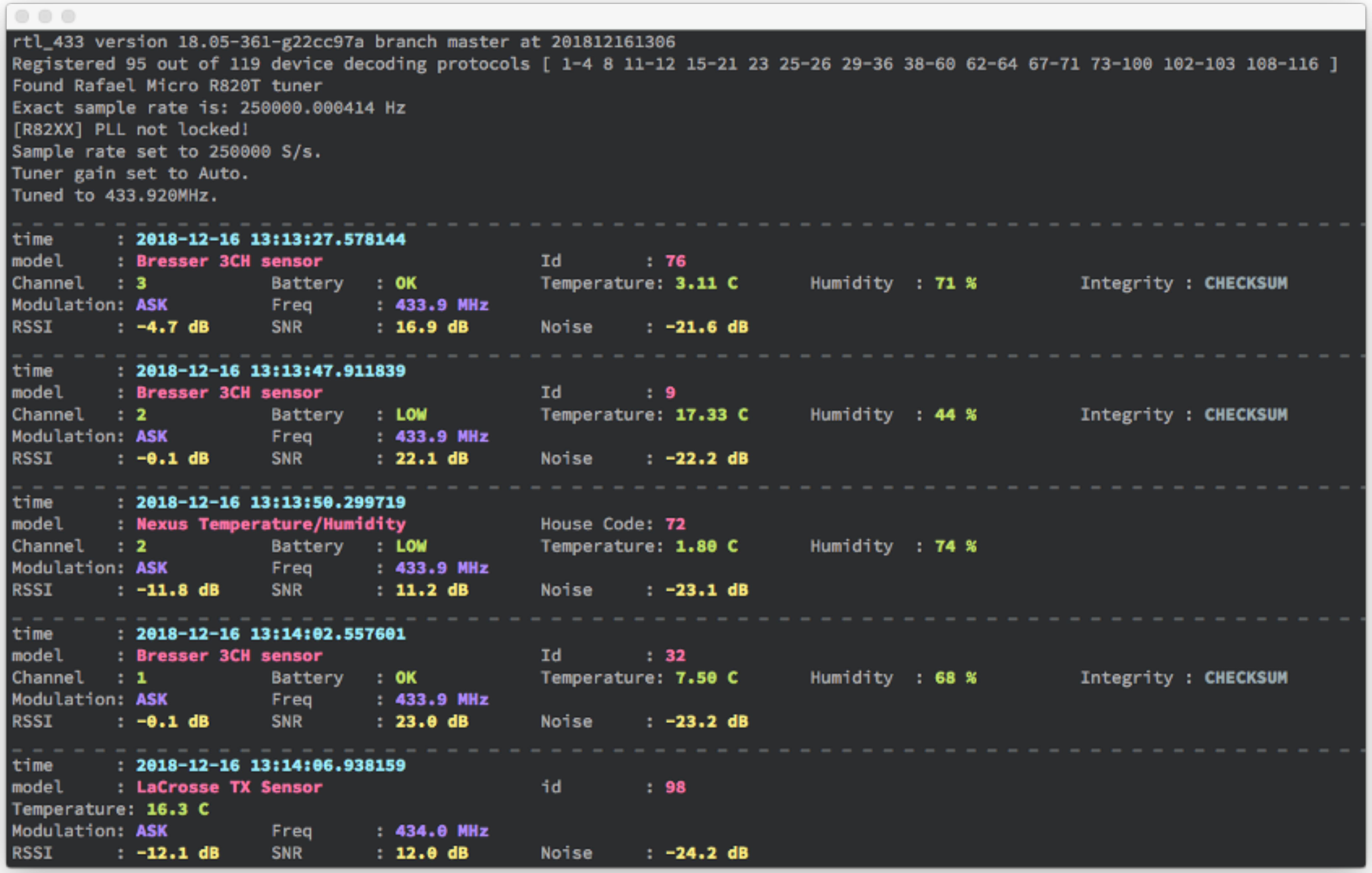
X-Zoom: 100%

+ 0 samples selected | 0,00 ns

```
101010101010101010101010101010101001101001111101100110100111110111010010011000010110110101111010111011011000011000111011011010111001010001111010110100110011100100110000
0101001110100000111111101000111001110000010111010010011101011011010000110110110101010001101101000101011001110001101010001010111111001101001100100000011001001101000100001
0010010011110111011001001111101110011000101111101010001010110111001000011011001000110010000110011011001001101110100 [Pause: 26660 samples]
101010101010101010101010101010100110011101101000011001110110100011111001111010010101001011100100100101010110011110111010011101110110011000 [Pause: 3892888 samples]
1010101010101010101010101010101010011010011111011001101001111101110011011110000101101101100100101010001011111011010010111100011001100011101110101101001100111101011100
```

Tools - Software

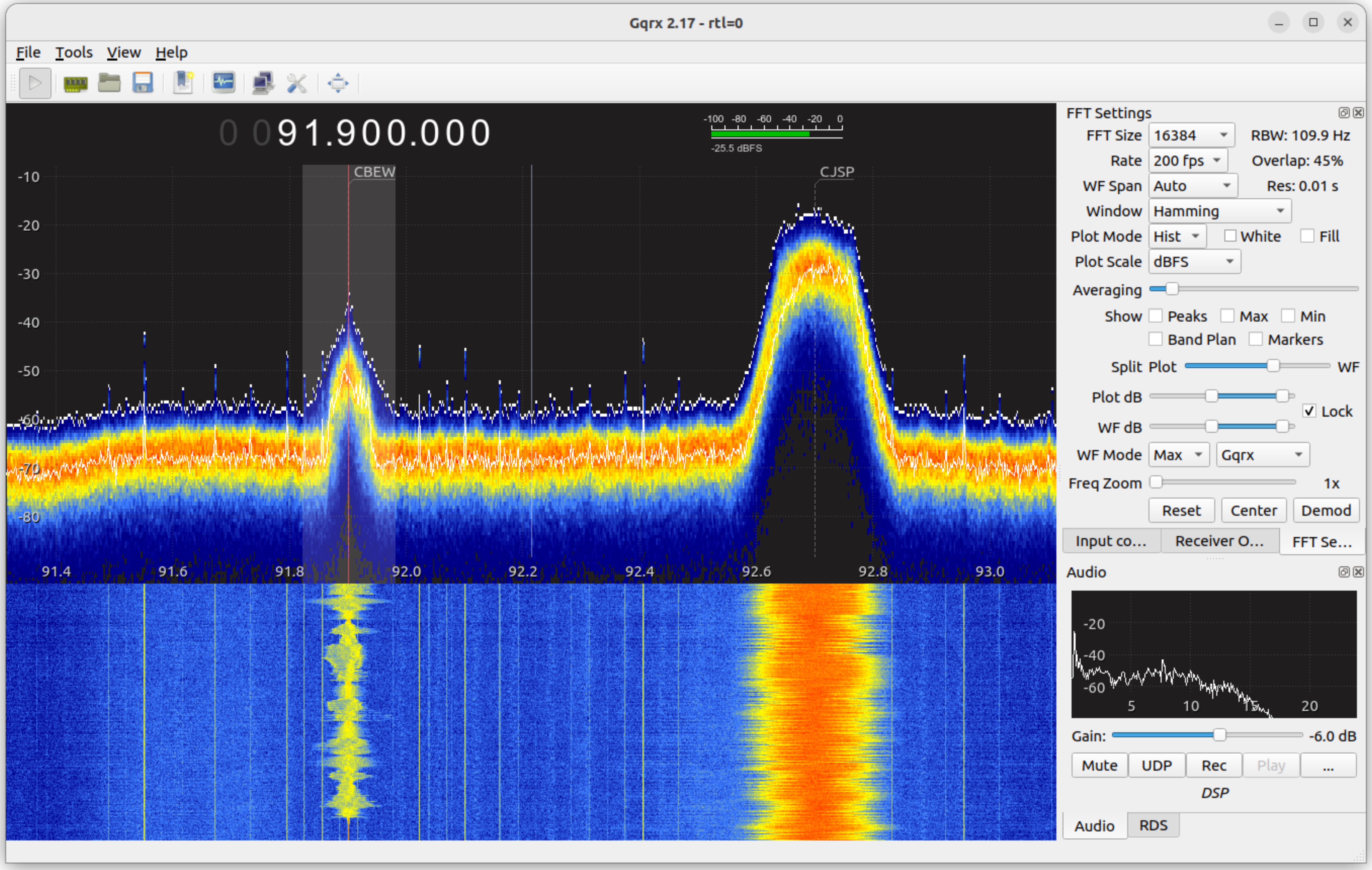
RTL_433



```
rtl_433 version 18.05-361-g22cc97a branch master at 201812161306
Registered 95 out of 119 device decoding protocols [ 1-4 8 11-12 15-21 23 25-26 29-36 38-60 62-64 67-71 73-100 102-103 108-116 ]
Found Rafael Micro R820T tuner
Exact sample rate is: 250000.000414 Hz
[R82XX] PLL not locked!
Sample rate set to 250000 S/s.
Tuner gain set to Auto.
Tuned to 433.920MHz.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
time      : 2018-12-16 13:13:27.578144
model     : Bresser 3CH sensor                      Id        : 76
Channel   : 3            Battery    : OK            Temperature: 3.11 C       Humidity   : 71 %          Integrity : CHECKSUM
Modulation: ASK          Freq       : 433.9 MHz
RSSI      : -4.7 dB      SNR        : 16.9 dB       Noise     : -21.6 dB
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
time      : 2018-12-16 13:13:47.911839
model     : Bresser 3CH sensor                      Id        : 9
Channel   : 2            Battery    : LOW           Temperature: 17.33 C      Humidity   : 44 %          Integrity : CHECKSUM
Modulation: ASK          Freq       : 433.9 MHz
RSSI      : -0.1 dB      SNR        : 22.1 dB       Noise     : -22.2 dB
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
time      : 2018-12-16 13:13:50.299719
model     : Nexus Temperature/Humidity              House Code: 72
Channel   : 2            Battery    : LOW           Temperature: 1.80 C       Humidity   : 74 %
Modulation: ASK          Freq       : 433.9 MHz
RSSI      : -11.8 dB     SNR        : 11.2 dB       Noise     : -23.1 dB
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
time      : 2018-12-16 13:14:02.557601
model     : Bresser 3CH sensor                      Id        : 32
Channel   : 1            Battery    : OK            Temperature: 7.50 C       Humidity   : 68 %          Integrity : CHECKSUM
Modulation: ASK          Freq       : 433.9 MHz
RSSI      : -0.1 dB      SNR        : 23.0 dB       Noise     : -23.2 dB
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
time      : 2018-12-16 13:14:06.938159
model     : LaCrosse TX Sensor                      id        : 98
Temperature: 16.3 C
Modulation: ASK          Freq       : 434.0 MHz
RSSI      : -12.1 dB     SNR        : 12.0 dB       Noise     : -24.2 dB
```

Tools - Software

GQRX



Gqrx 2.17 - rtl=0

0 091.900.000

-25.5 dBFS

FFT Settings

FFT Size 16384 RBW: 109.9 Hz
Rate 200 fps Overlap: 45%
WF Span Auto Res: 0.01 s
Window Hamming
Plot Mode Hist □ White □ Fill
Plot Scale dBFS
Averaging
Show □ Peaks □ Max □ Min
□ Band Plan □ Markers
Split Plot WF
Plot dB ☑ Lock
WF dB
WF Mode Max Gqrx
Freq Zoom 1x

Audio

Gain: -6.0 dB

Tools - DIY

GoGoBark

For relay attack

Tools - DIY

Hack KEY