DoS: Denial Of Shopping

—

Analyzing and Exploiting (Physical) Shopping Cart Immobilization Systems

by Joseph Gabay

A Disclaimer

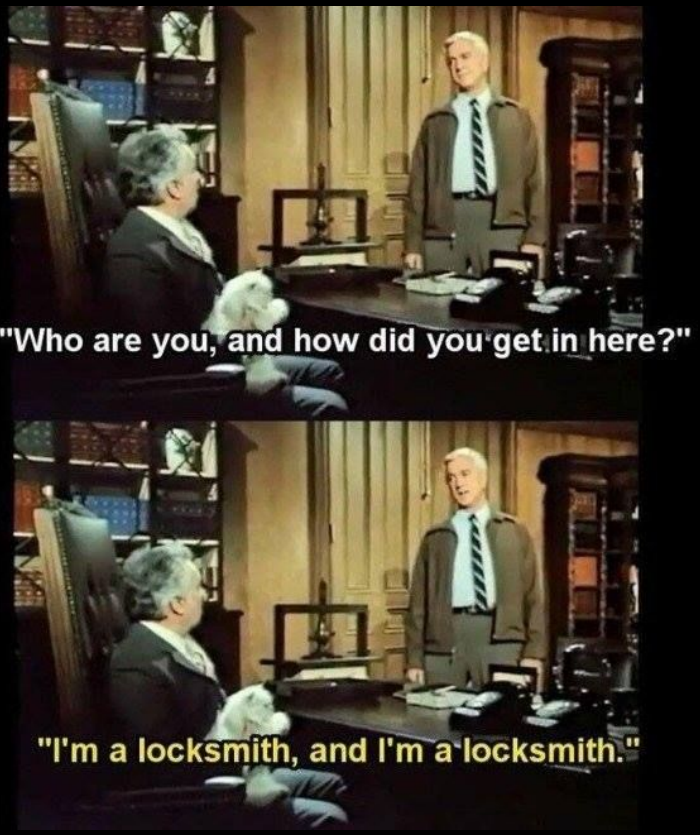
This talk is the result of my personal project.

Any views, opinions, or research presented in this talk are personal and belong solely to me. They do not represent or reflect those of any person, institution, or organization that I may or may not be associated with in a professional or personal capacity unless explicitly stated otherwise.

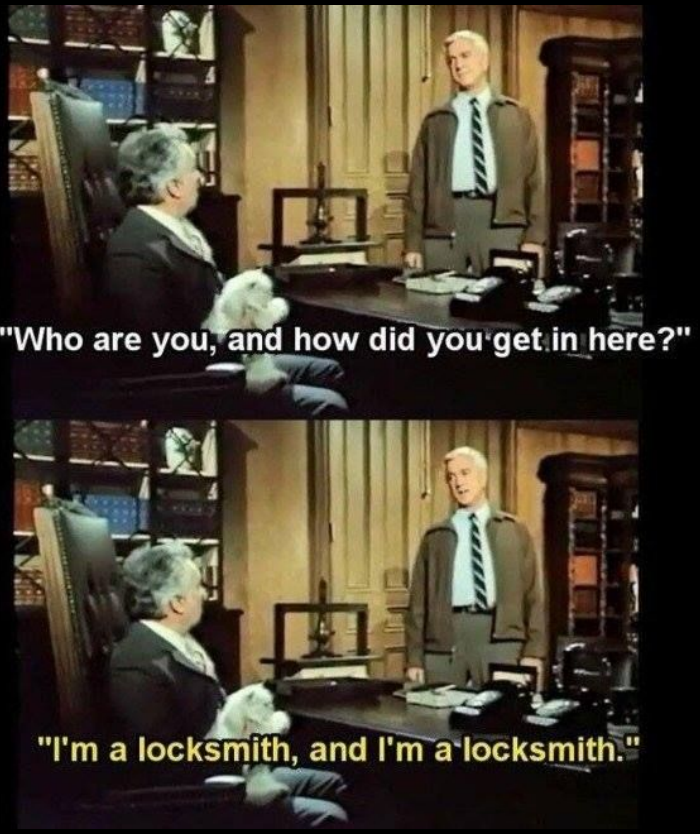
Who are you?

Who are you?

And how did you get in here?



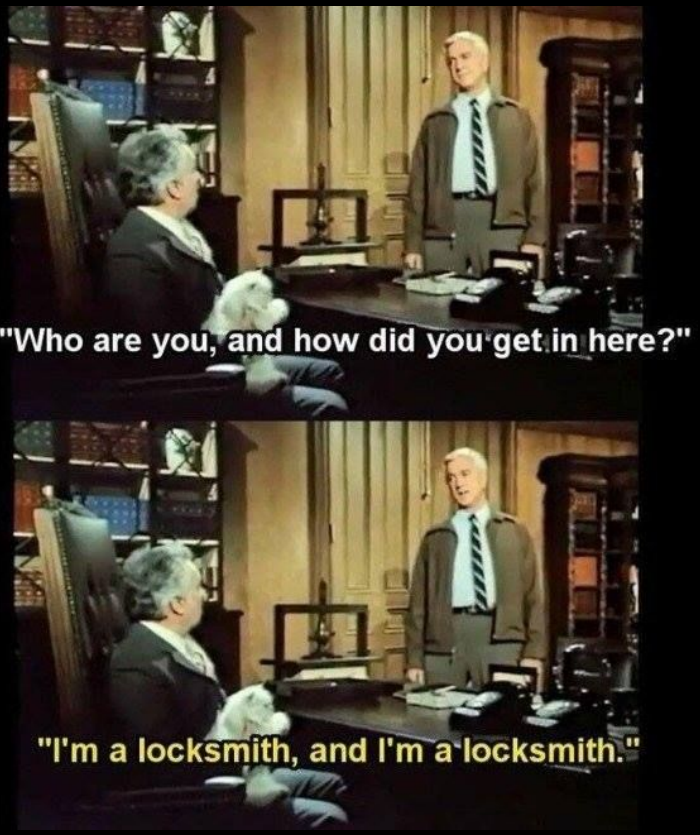
Joseph Gabay



Joseph Gabay

Hacker, Maker, Flat Mooner,
Collector of Silly Domain Names
and Random Certifications.

I also build robots sometimes.



Wait, shopping cart whatnows?

- Invisible fence, for carts.
  - No, really.
- Shopping cart locks when taken out of parking lot
- Other, more niche applications
  - Stopping “runouts”
- Gatekeeper Systems estimates $180 million in annual shopping cart theft

Okay, but why shopping cart wheels?

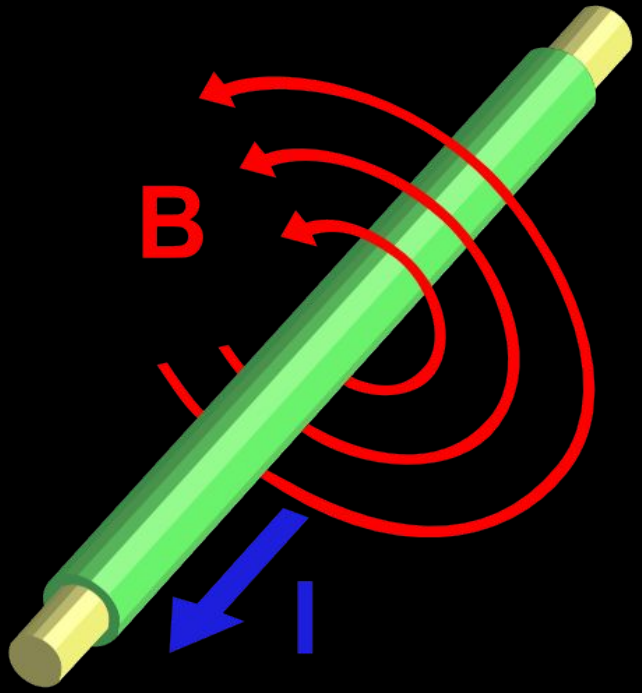
Or, a brief ramble about hacking.

“It's not worth doing something unless someone, somewhere, would much rather you weren't doing it.”

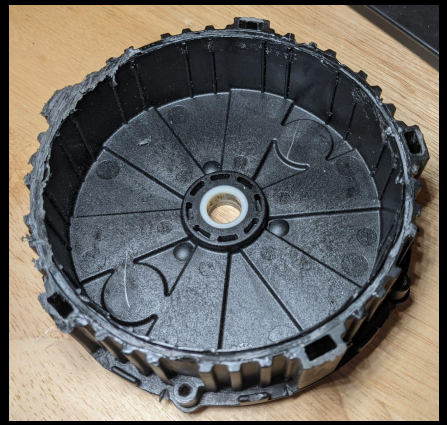
- Sir Terry Pratchett

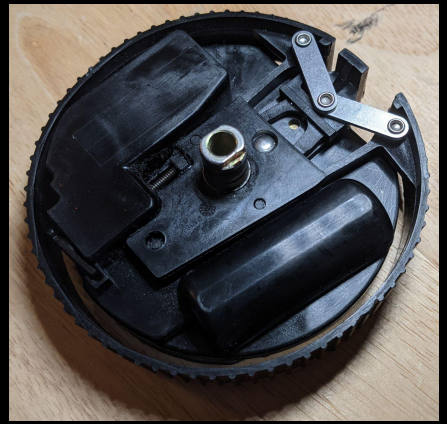
How do they work?

- Magnetic Loop System
  - Underground perimeter wire sends out signal
- Current through wire produces magnetic field
- Cart senses field, locks using internal mechanism
- Store staff has remote that can unlock carts

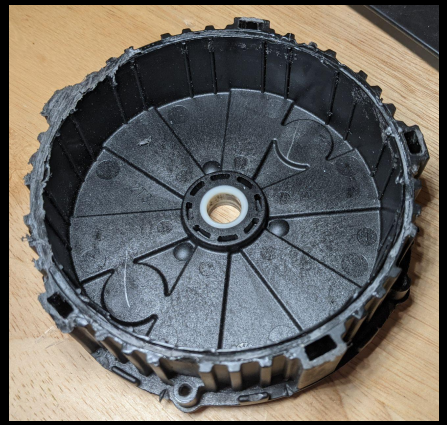


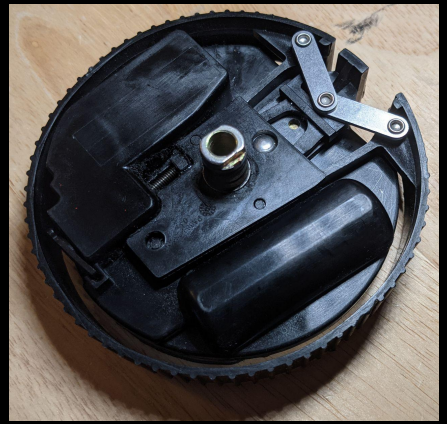
Anatomy of a Shopping Cart Wheel - Locking Mechanism



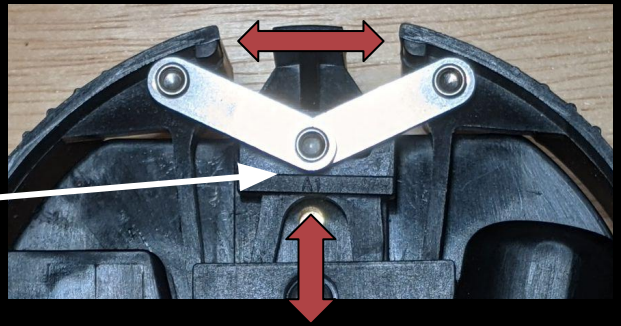


Anatomy of a Shopping Cart Wheel - Locking Mechanism

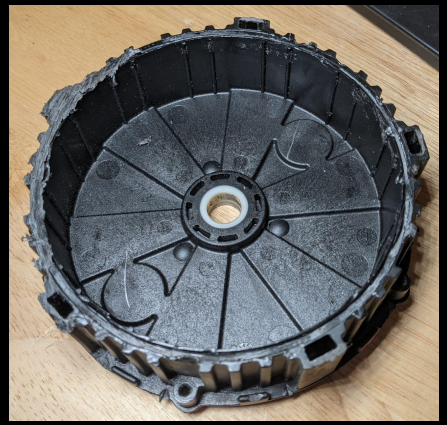


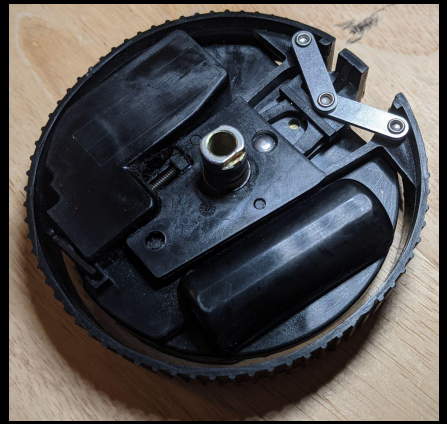


Mechanism expands/contracts inner ring

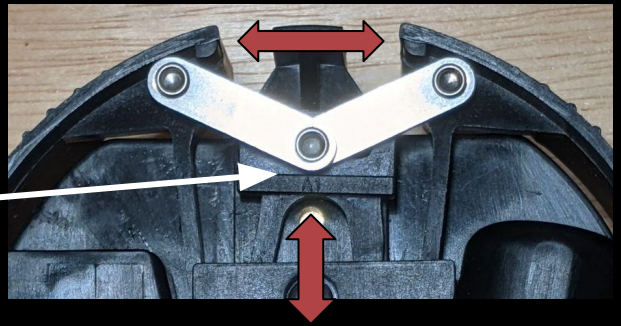


Anatomy of a Shopping Cart Wheel - Locking Mechanism



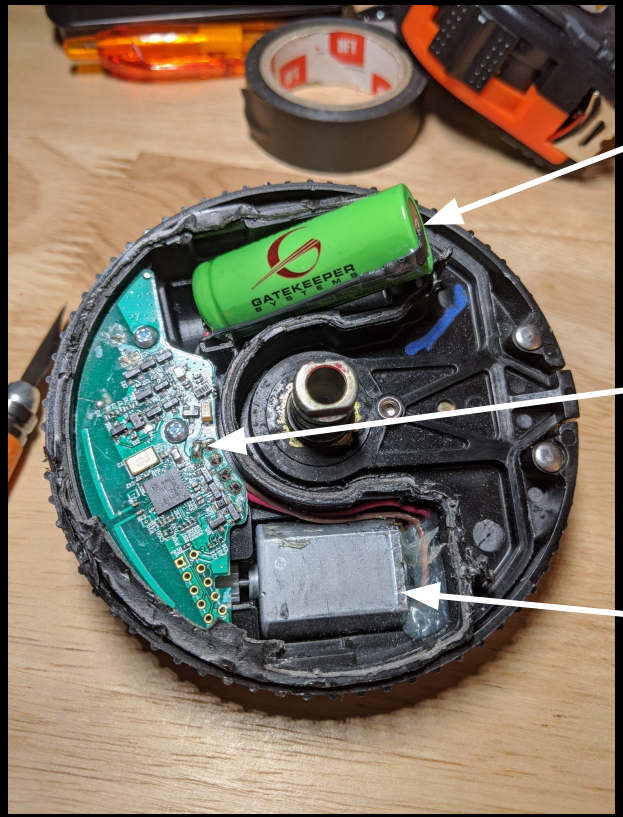


Mechanism expands/contracts inner ring



Ridges on inner ring lock into ridges inside wheel casing

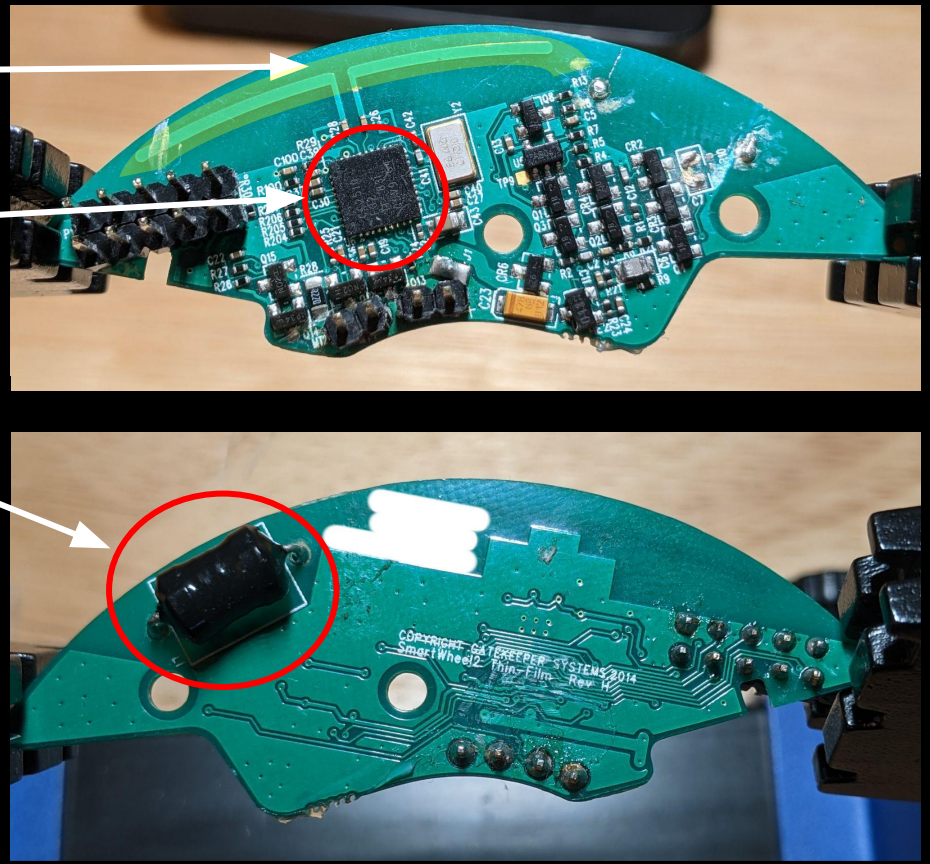
Anatomy of a Shopping Cart Wheel - Internal View



- 3V Lithium Battery
  - μC likely optimized for low power consumption
- DC Motor
  - Drives gearbox to expand/contract ring
- PCBa hosts radios and microcontroller

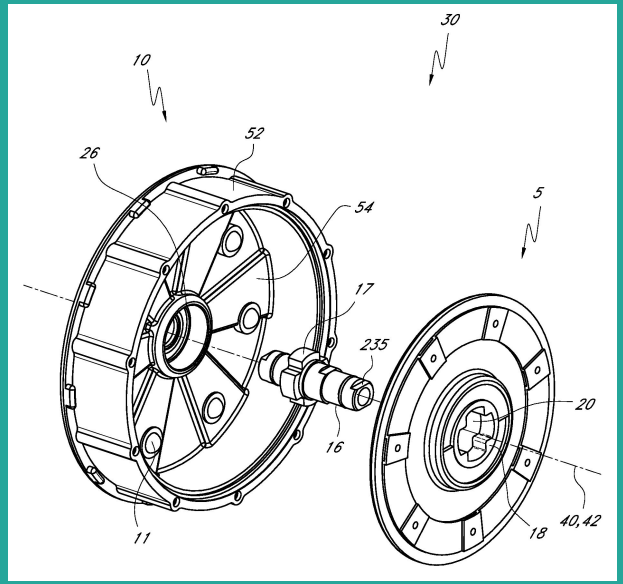
Anatomy of a Shopping Cart Wheel - PCBa

- 2 Separate Antennas
  - 2.4G - PCB Trace
  - 7.8K - Inductor
- TI CC2510 Microcontroller
  - Built-in 2.4 GHz transceiver
  - Low-power modes
- Motor driver circuit
- VLF Amplifier
  - (very curious as to how it works)
- JTAG port for programming chip



8 Matches found for FCC ID W3Z-W9470A

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
letter of appointment	Cover Letter(s)	07/06/2016	pdf	07/06/2016
LTC request	Cover Letter(s)	07/06/2016	pdf	07/06/2016
ext photos	External Photos	07/06/2016	pdf	07/06/2016
Label and location	ID Label/Location Info	07/06/2016	pdf	07/06/2016
int photos	Internal Photos	07/06/2016	pdf	07/06/2016
Test report	Test Report	07/06/2016	pdf	07/06/2016
Test setup photos	Test Setup Photos	07/06/2016	pdf	07/06/2016
user manual	Users Manual	07/06/2016	pdf	07/06/2016



How do we learn more about the lock signal?

- FCC.gov - always a goldmine
- Patent Searches
- Other hackers
  - tmplab.org “consumer-b-gone”

What did we learn?

- Two control frequencies
  - Below 9 KHz (problem)
  - 2.4 GHz ISM band (less problem)
- 2.4 GHz modulated using MSK/FSK

CentralTransmitter	
Microprocessor	Digital circuitry, programmed in the factory and compliant with FCC Part 15 (no testing or certification required).
Power Supply	110/220 VAC, 500mA, 50/60 Hz compliant with ANSI/UL 60950 and CAN/CSA C22.2 No. 60950-00.
Signal Output	Signal frequency is below 9 KHZ (VLF) and complies with FCC Part 15.

1.2 Description of EUT Operation

The Equipment Under Test (EUT) is a Gatekeeper Systems (HK) Ltd., CartKey 2. The transmission transmitter operating in the 2.4GHz ISM frequency band. The EUT continues to transmit while Key is being pressed. Modulation by digital data; and type is MSK/FSK modulation.

source: fcc.gov

Capturing the VLF Signal - Problems

- Signal is Very-Low Frequency (VLF) - $<$ 9 KHz
  - Corresponding wavelengths in 10s of Kms
  - Ideal antennas should be close to wavelength
  - Most SDRs and RF amps expect $>$ 1 MHz

But wait: 9 KHz is in audio range...

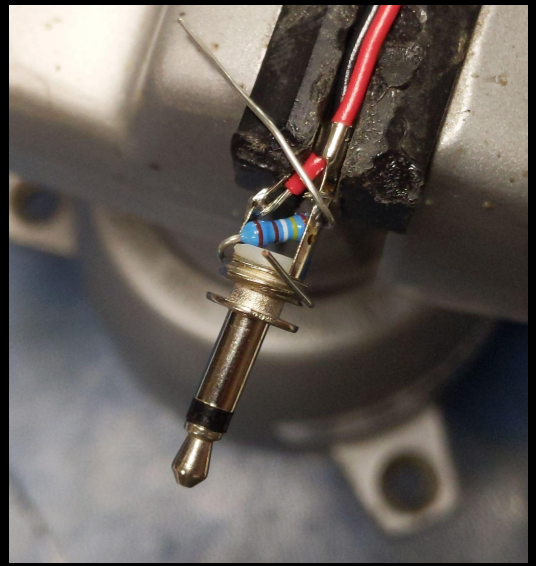
- We can use audio amp equipment!
  - Thanks tmplab.org hackers for the inspiration

A Brief Apology to Any RF Engineers in the Audience.

(I’m not sorry)

RF Engineers... I'm sorry.

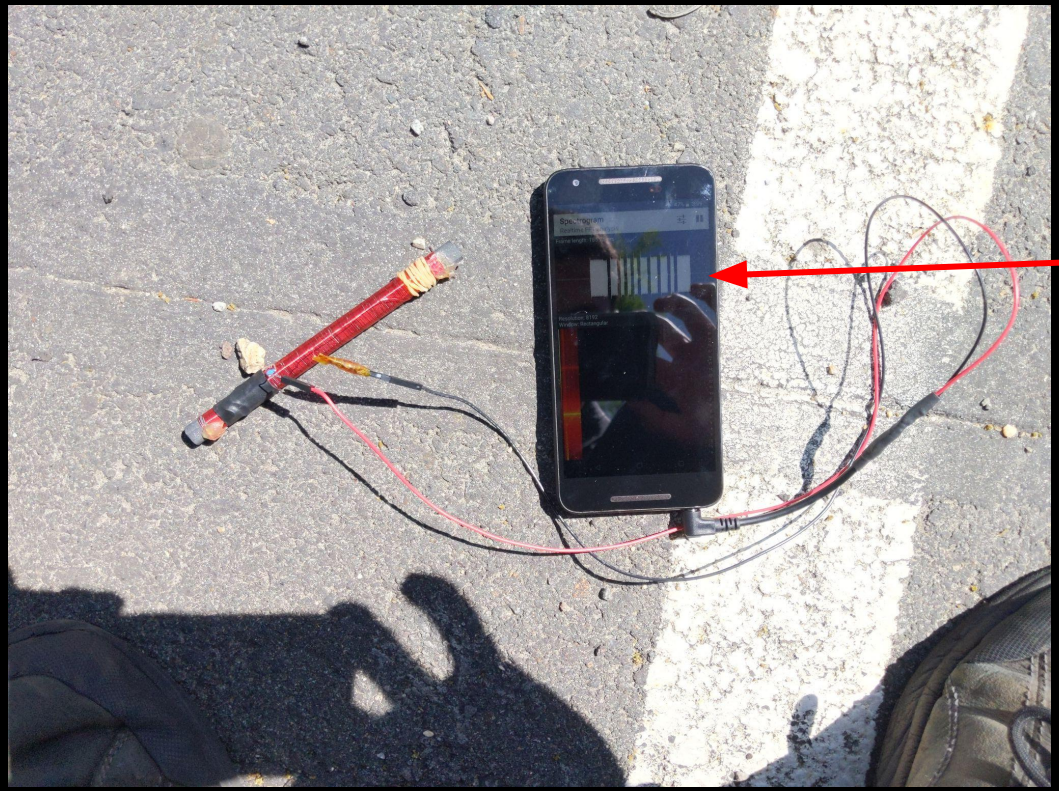
Loopstick Antenna



Wired into 3.5mm Jack

- Basic Loopstick Antenna
  - Ferrite core
  - Magnet wire
  - ~21 mH inductance
  - Tuning capacitor
- 3.5mm Jack
  - 2.5 kΩ resistor to trick audio port into thinking its a microphone
- What could go wrong?

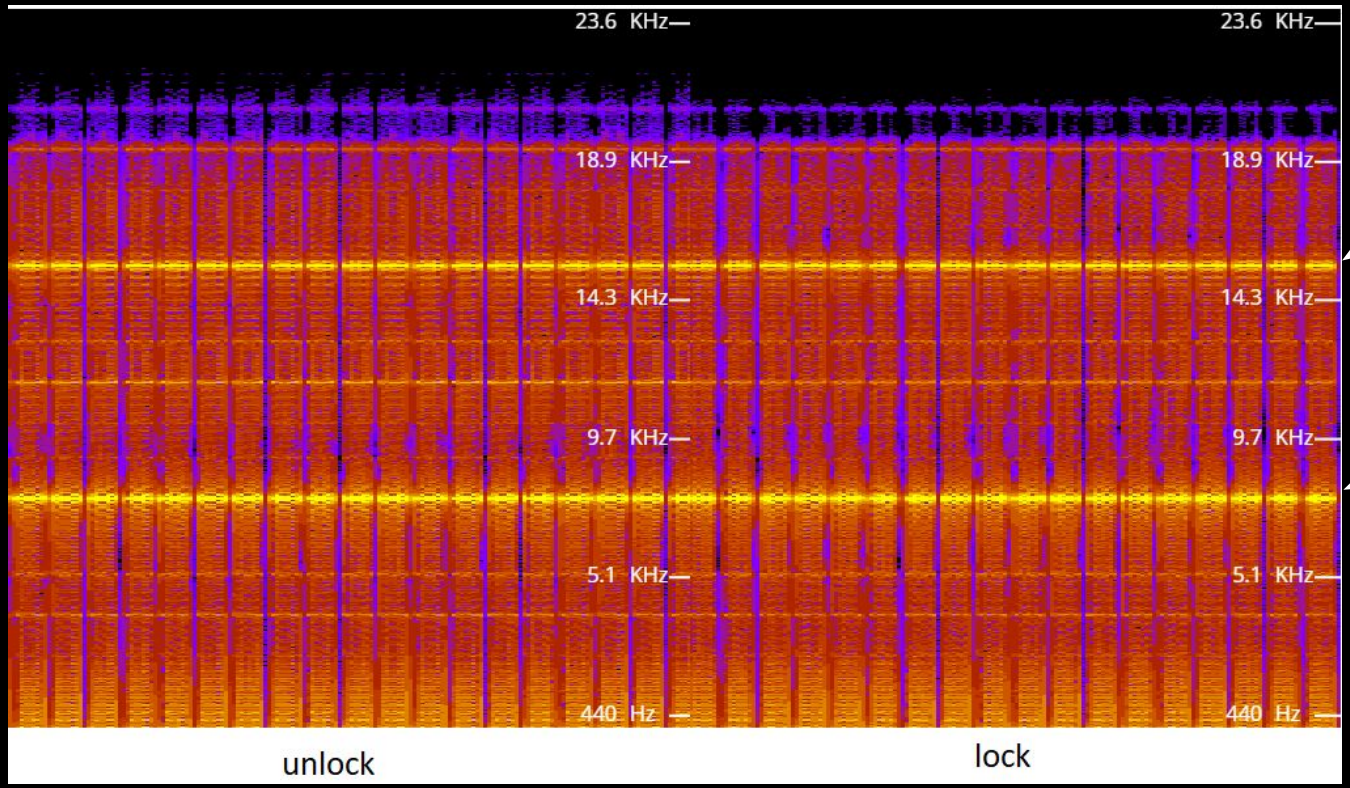
Field trip!



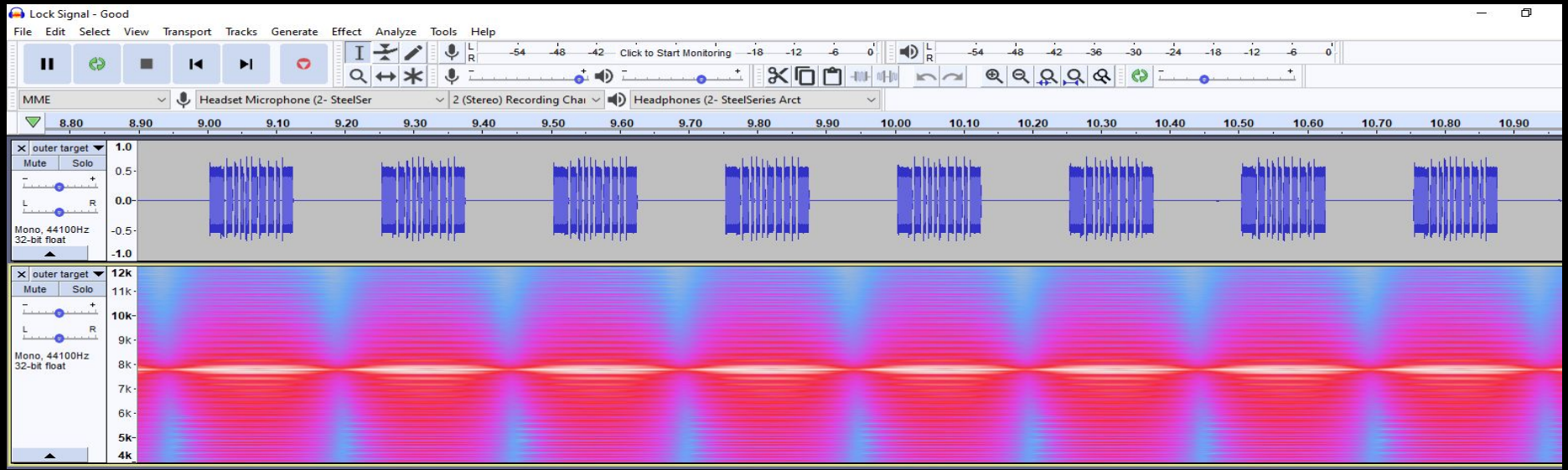
We actually see a signal!

I’m in.

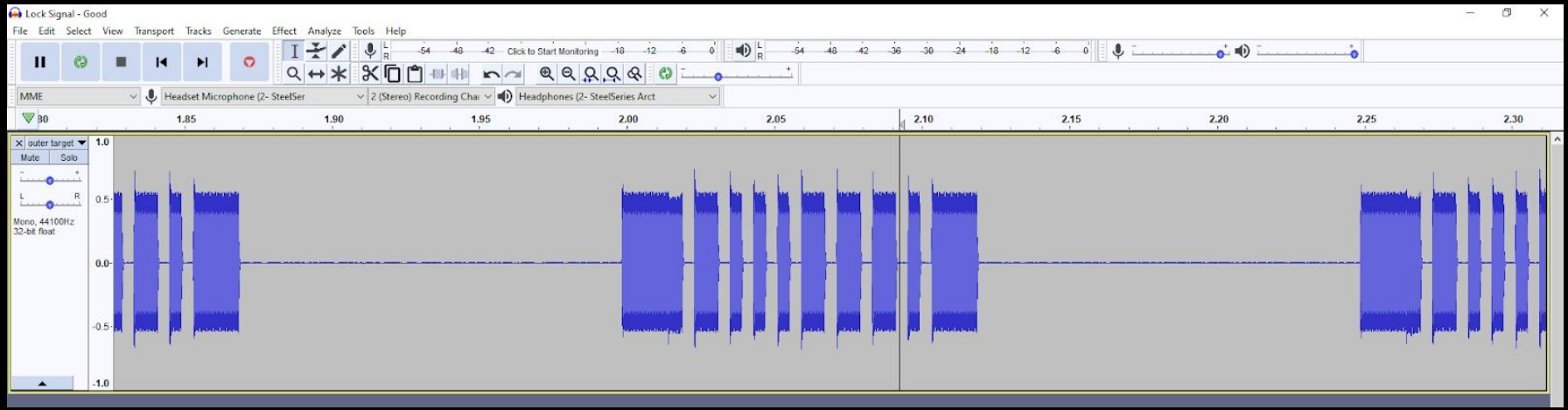
Let’s inspectrogram the spectrogram.



Oh the Audacity...

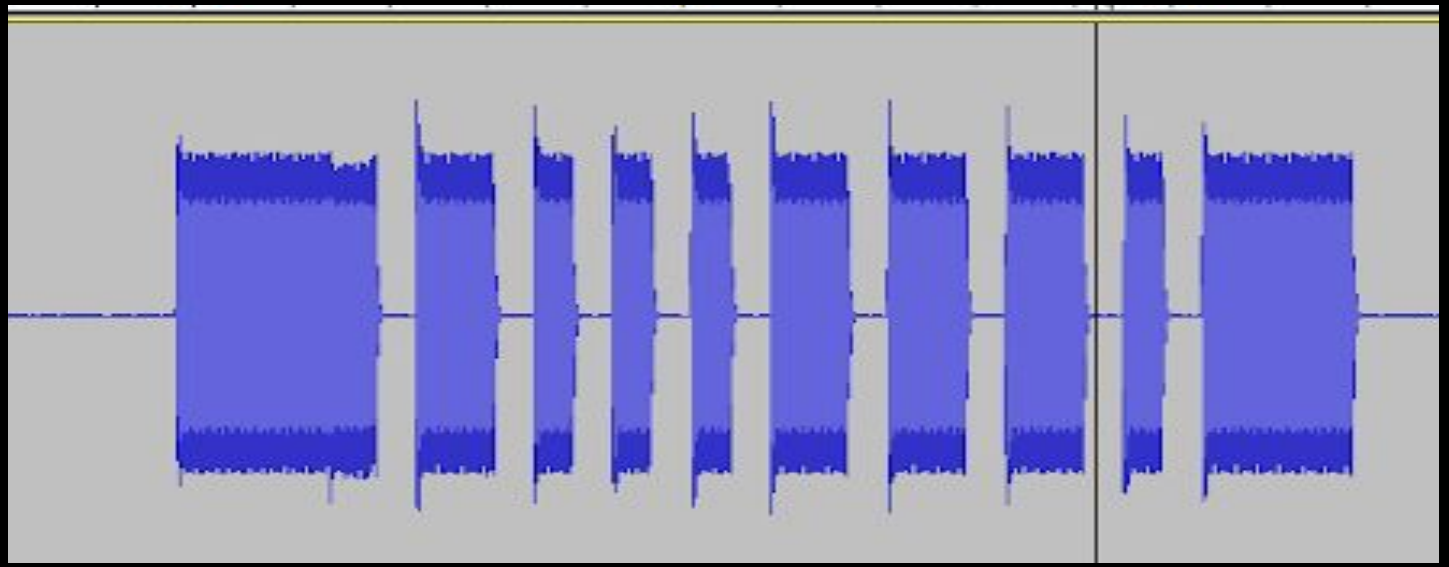


Zoom, enhance!



125 ms 125 ms 125 ms

Bit by bit...

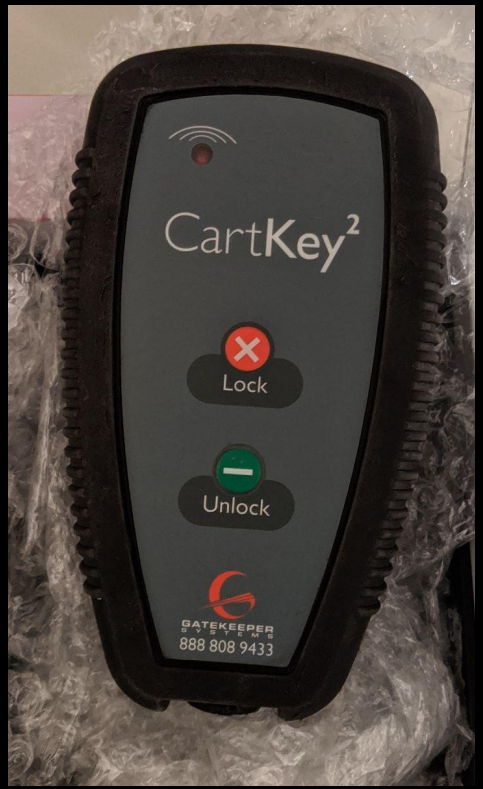


START 1 0 0 0 1 1 1 0 STOP

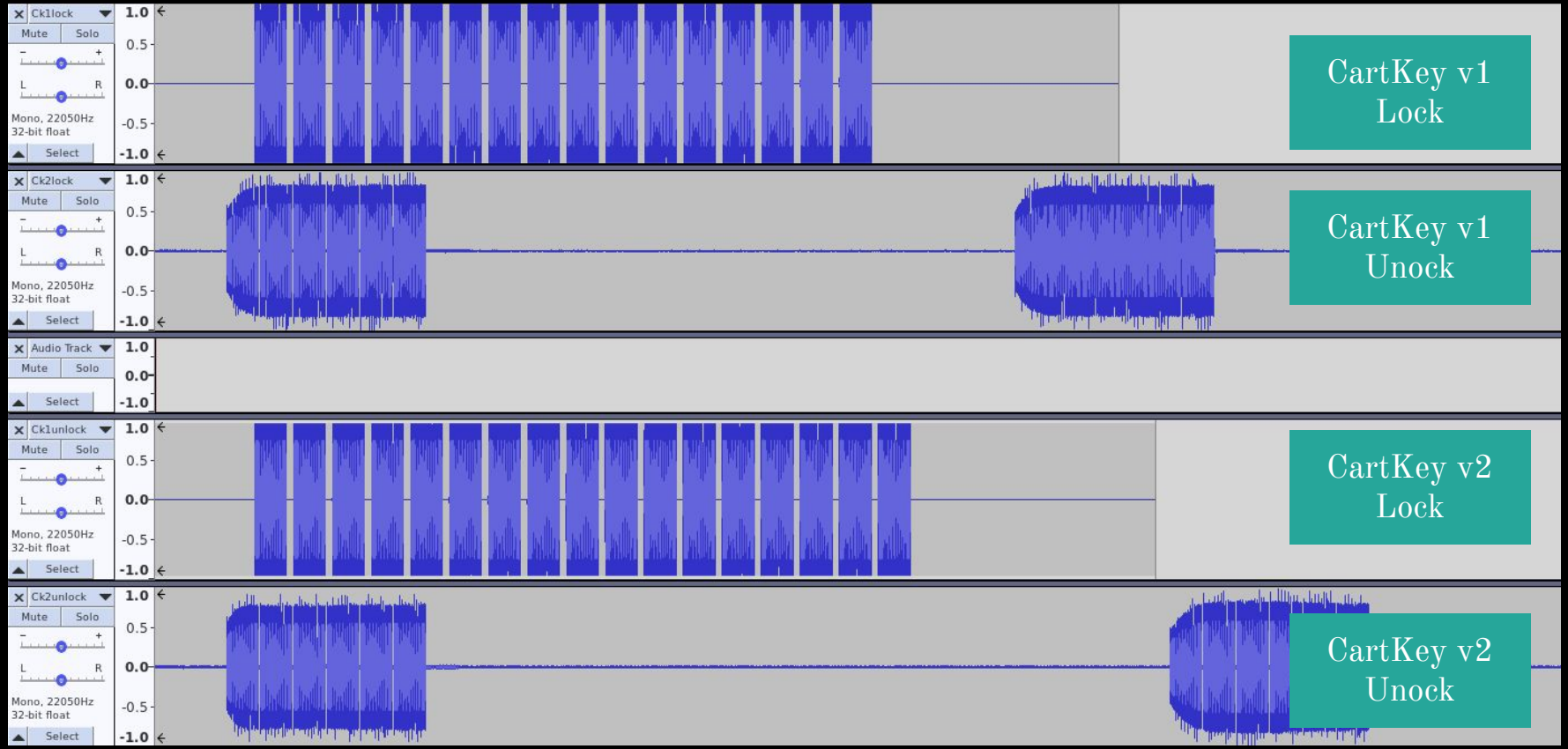
Unlock and 2.4 GHz Signals

- Unlock signal and any 2.4 GHz signals comes from a CartKey
  - Used by stores to lock/unlock carts
  - Unlock is 7.8K/2.4G
  - Lock only broadcasts on 7.8K
- Ebay is a magical place

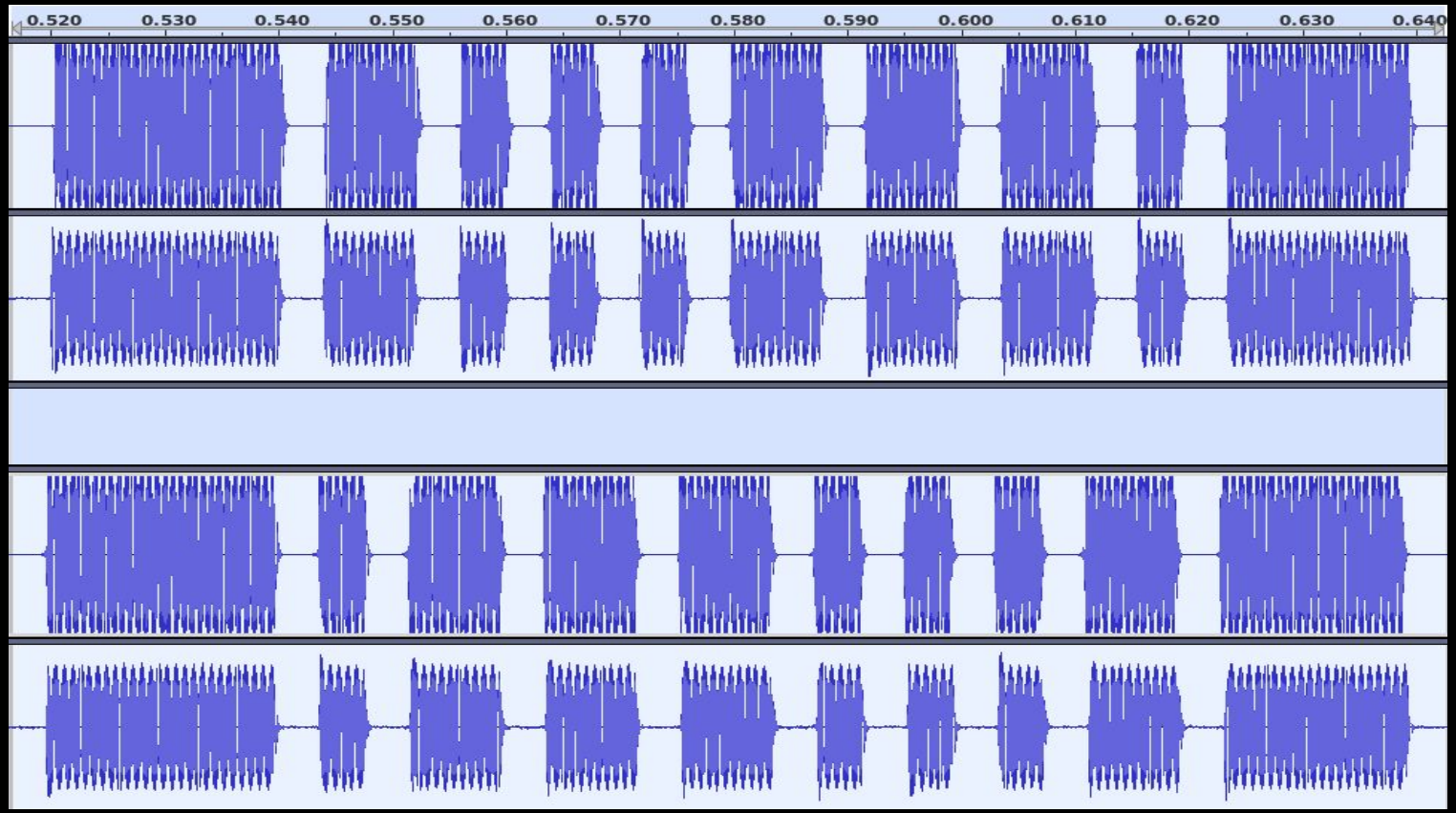
Let’s go and sniff the 7.8K signals.



CartKey Signal Captures - V1 vs V2



CartKey Signal Captures - V1 vs V2



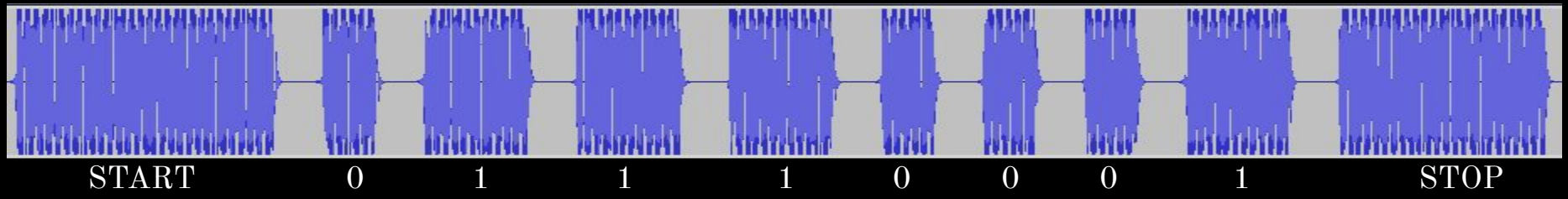
Lock

Unlock

Compare lock/unlock

Lock Signal @ 7.8 kHz

Unlock Signal @ 7.8 kHz




```
Lock:     0b10001110
Unlock:   0b01110001
```

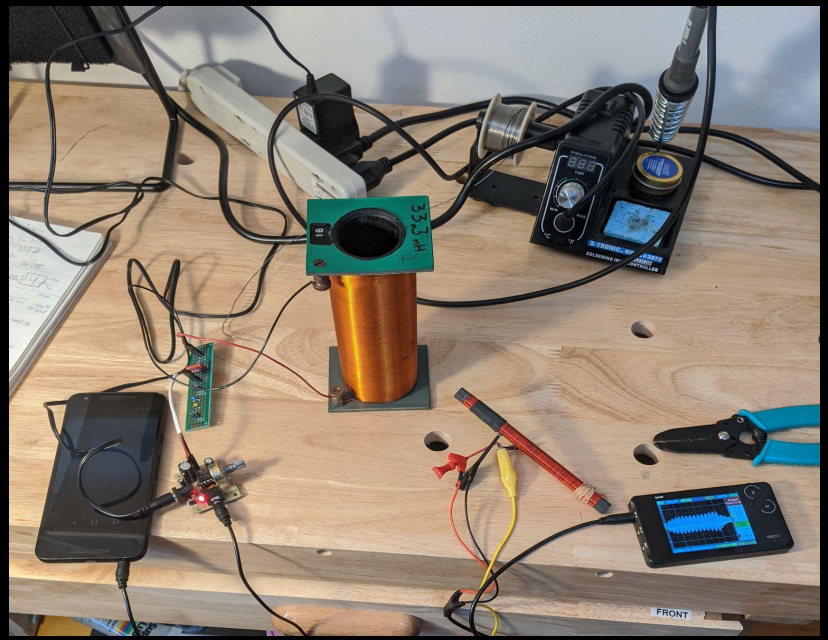
Lock signal is inverse of unlock!

Will a 7.8 KHz replay attack work?

- Can we play the lock/unlock signals back through the loopstick antenna?
- Yes, but the range is short
  - ~2ft with a 10W amplifier
  - Loopstick is a poor transmitter
    - Directional
  - Hard to get around it
- Phone speakers/headphones can also replay
  - Microphones are basically antennas
  - “Parasitic EMF”

Will a 7.8 KHz replay attack work?

Increasing the range?

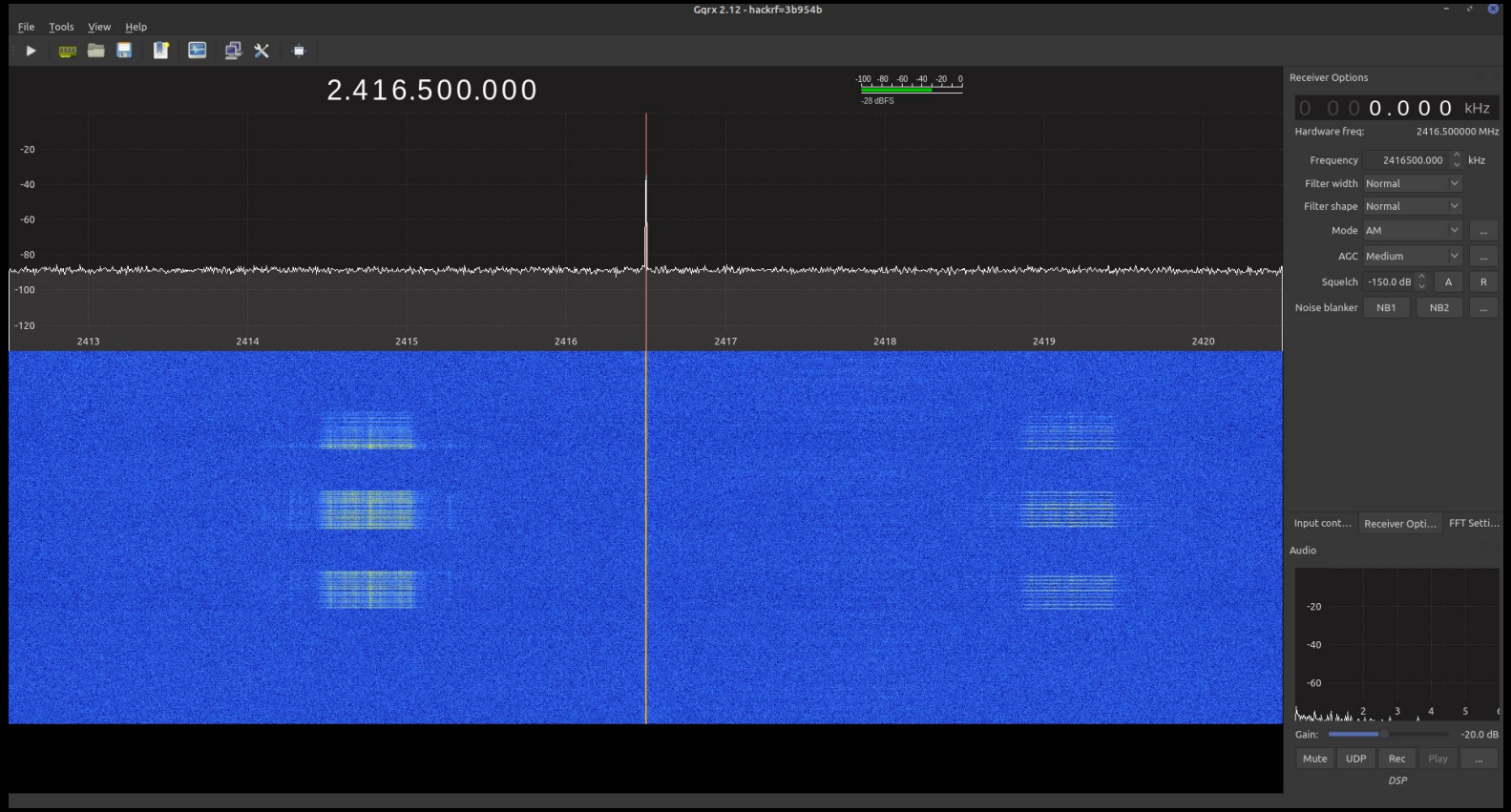


- Bigger coil
  - Found at the MIT Flea
- External Amplifier
  - 10W Audio Amplifier
- Diminishing Returns
  - Inverse square rule
  - Fighting against physics
- Loopsticks are bad at TX

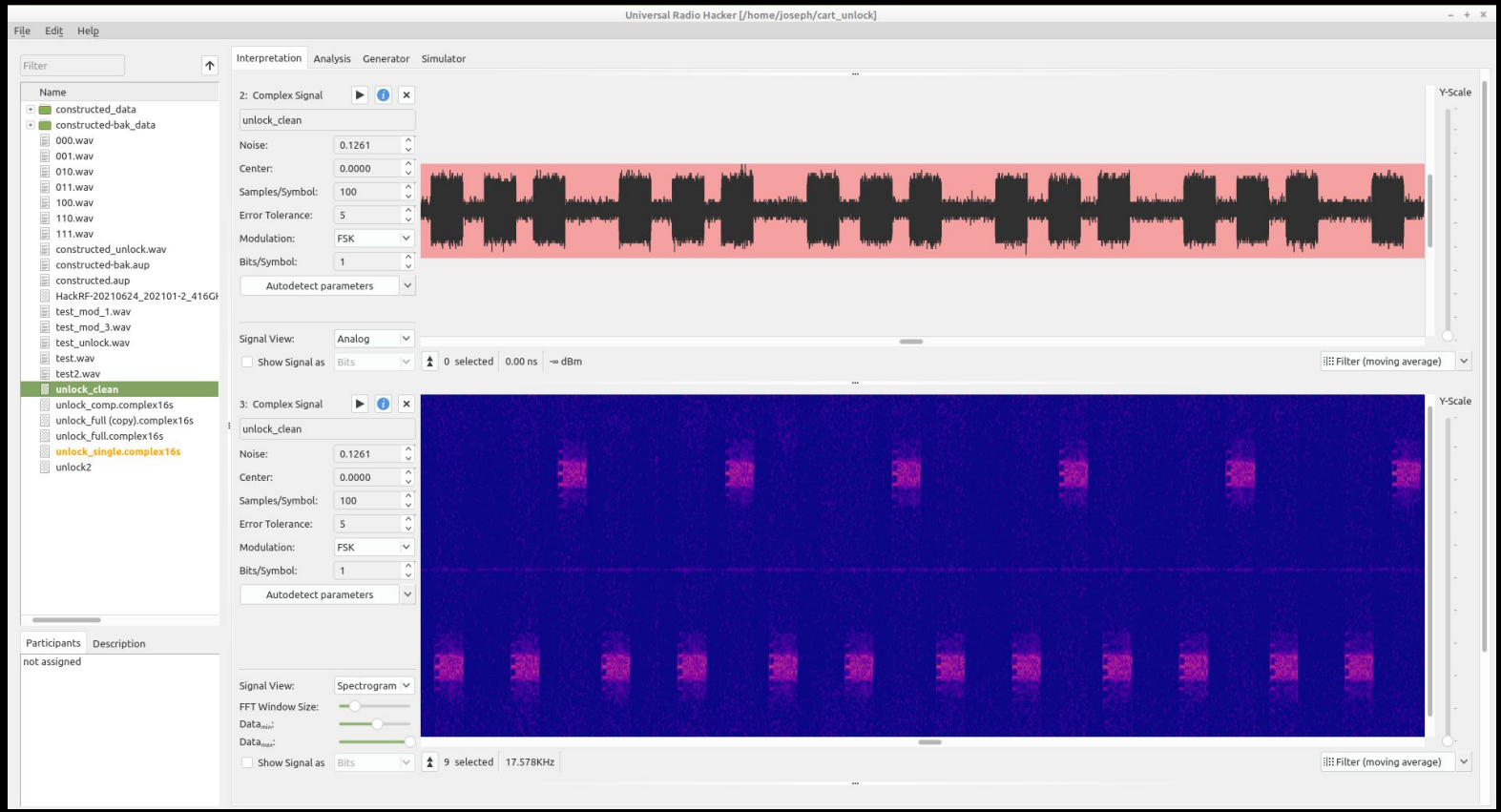
Peeking at the 2.4 GHz Signal

- 2.4 GHz is much easier to work with
- Used a HackRF SDR
  - 1 MHz - 6 GHz range
  - greatscottgadgets.com
- Should let us analyze any 2.4 GHz signals

Peeking at the 2.4 GHz Signal - Gqrx

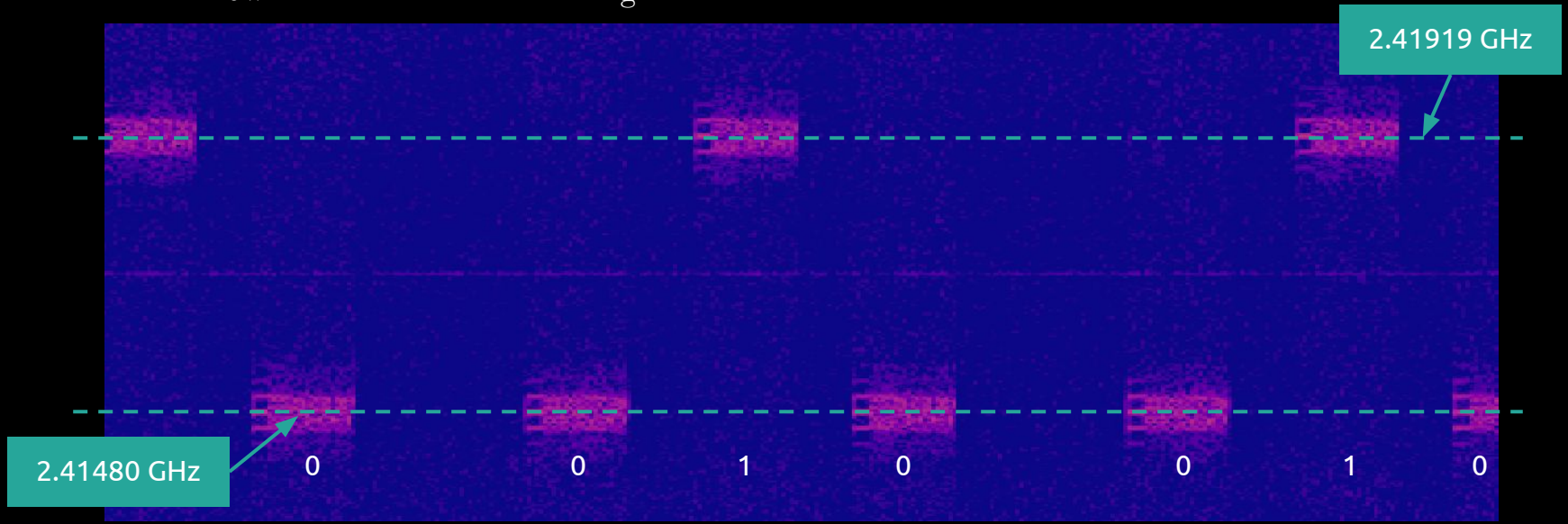


Peeking at the 2.4 GHz Signal - URH



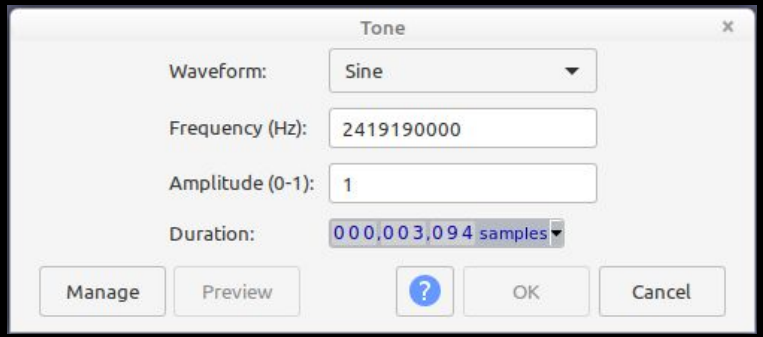
Peeking at the 2.4 GHz Signal - URH

- 2FSK Modulation
- Center freq = 2.417 GHz
- Spacing = 4.4 MHz
- F_{low} = 2.41480G F_{High} = 2.41919G

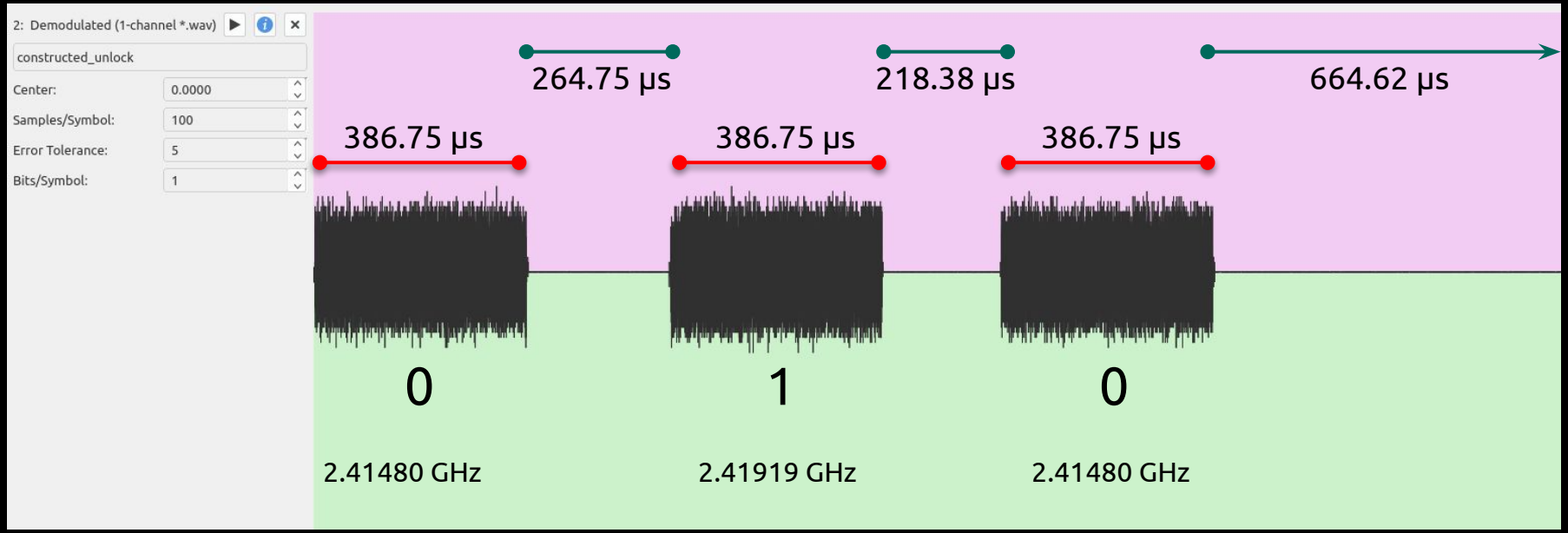


Replaying the 2.4 GHz Unlock Command

- HackRF can act as a transmitter as well
- URH can export captures as .wav files
- Import to Audacity
  - Mono, 8000000Hz 32-bit float lol
  - Slice n' dice waveforms to make new commands
  - Make commands from pure tones
- Play .wav file through HackRF
  - URH is amazing

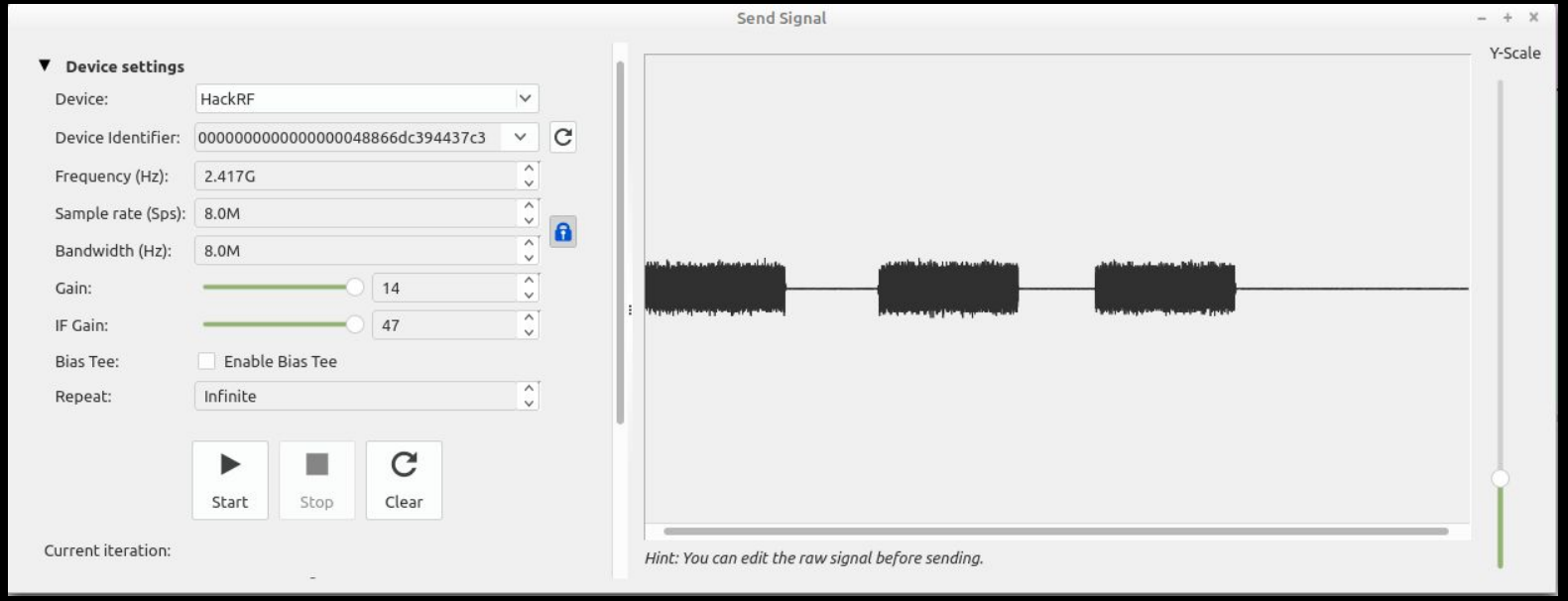


Making a 2.4 GHz Unlock Command From Scratch



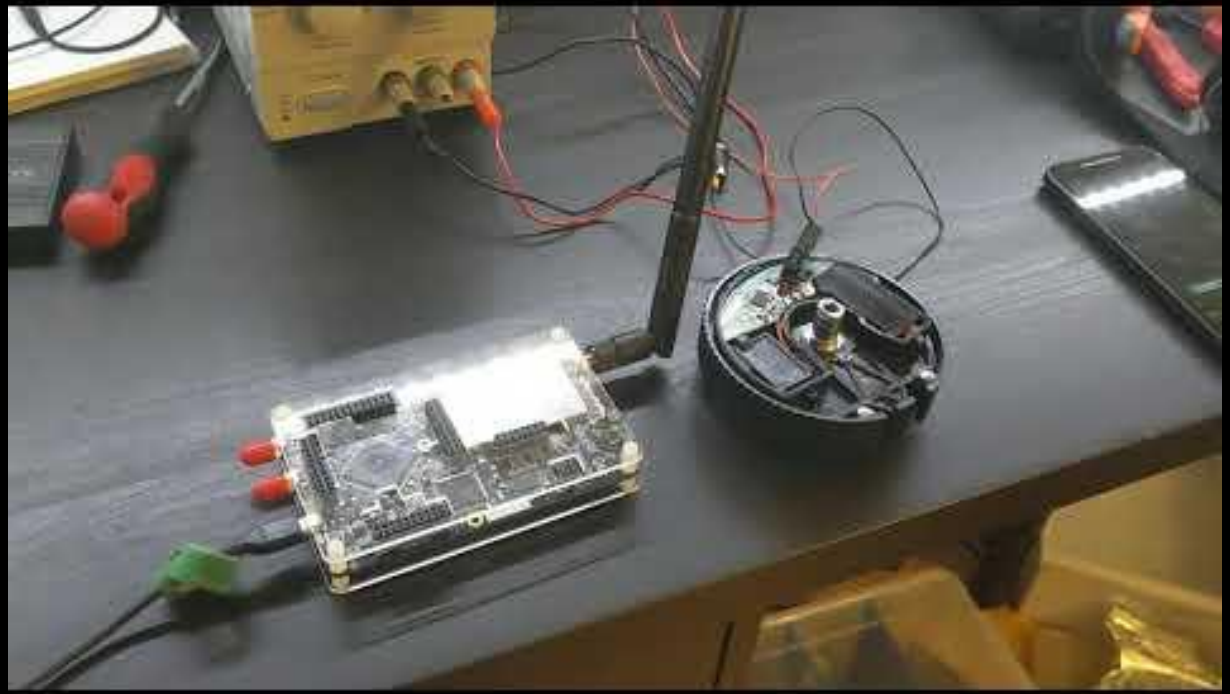
A 2.4 GHz unlock command made from scratch in Audacity.

Testing out our homemade command...



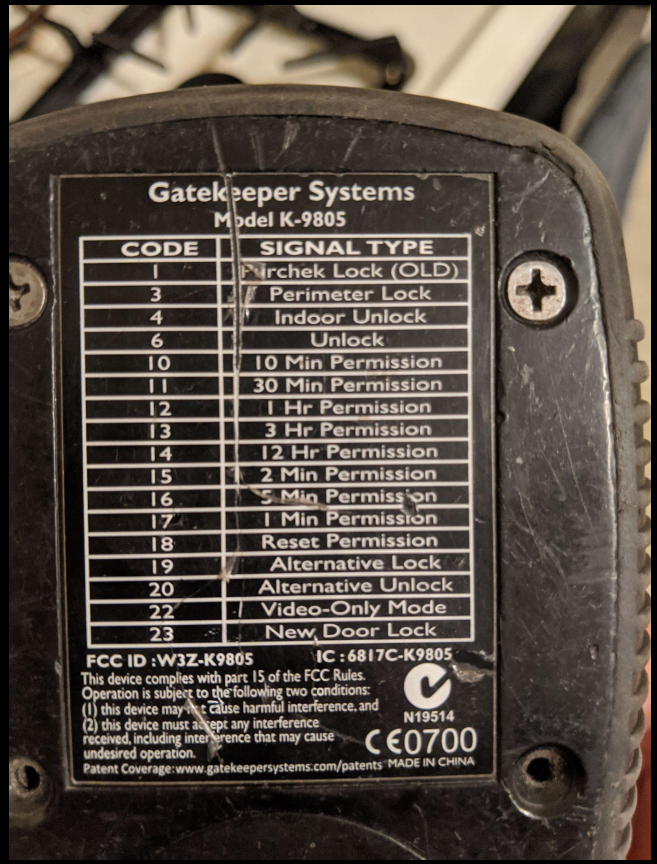
The Audacity-made signal ready for rebroadcast in URH

Playing the 2.4 GHz Command Back



Is there a 2.4 GHz Lock Signal?

- Would be longer range
  - Easier to transmit
- No combination of 1's and 0's like the unlock signal triggered a lock
- Wheels have advanced functionality that is unexplored
- Gatekeeper Systems likely chose not to implement this feature to prevent unintended locking



Mysterious codes on the CartKey, likely for 7.8 KHz

So what can we do with this?

- Short range locking of carts
  - Have to be within a few feet
- Unlock carts that have been locked
  - Much easier ways of getting a cart if that's your goal
  - Shopping cart liberation
- Be content with the knowledge that you know how something hidden works

Please don't be a dick with this.

References, Thanks, and Software Used

References:

- The ARRL handbook for radio communications, 2007. Newington, CT: American Radio Relay League, 2006. Print.
- https://www.tmplab.org/2008/06/18/consumer-b-gone/
- http://www.woodmann.com/fravia/nola_wheel.htm
- The wonderful people over at /r/rfelectronics
- FCC.gov

Software Used:

- Audacity
- URH (Ultimate Radio Hacker)
- Gqrx

Special thanks to the Electronic Frontier Foundation and its Coders' Rights Project for their advice and guidance on doing this talk the right (and legal!) way.

Thanks for coming!

Any questions? Anything I did wrong? Anything I missed?

Projects and Hobbies:
joseph@begaydocrime.com

Professional:
joseph@tethys.cc

@stoppingcart on twitter

Any files I’m able to share will be available at begaydocrime.com/carts