

Warshopping:

Further Phreaking Smart Shopping Cart Wheels Through RF
Sniffing and Hardware Reverse Engineering

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.

What this talk is:

- A journey to reverse engineer and bypass the Rocateq Security Wheel
- Exploring and assessing a device for hardware, firmware, and software vulnerabilities
- Playing around with tools like Pickits, Saleae, and Ghidra
- Warshopping
- Old-school audio phreaking



What this talk isn't:



- 1337 hacking
- Hot new 0-days
- Instructions or endorsement of shoplifting
- Definitive teardown of how this system works

Who am I?

Also, why am I?

- Hacker
- Robotics engineer
- Skydiver
- Shopping cart phreaker
- Flat moon conspiracist



Who I'm not:

- A binary RE expert
- A radio or EE expert
- D. B. Cooper
- 100% Correct



A Quick Recap - What are These Wheels?

2 main players - Gatekeeper Systems and Rocateq

Commonalities:

- Buried wire-loop system around store perimeter
- Use an ultra low frequency band
 - Pain to transmit at
- Lock/Unlock Commands
- Advertise some 2.4 GHz comms possibilities
- Can provide anti-shoplifting features



A Quick Recap - Various Locking Mechanisms



A Quick Recap - Buried Wires

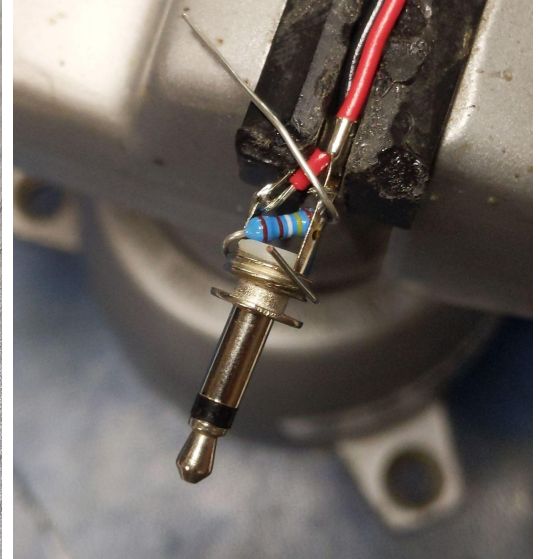


A Quick Recap - Loopstick Antennas as a Microphone

- Okay for RX, not great for TX
 - Still better than nothing
 - Real EE could probably improve
- Enamel Wire + Ferrite Rod
 - Both available on Amazon
- Cordless drill and some patience
 - More turns = more power
- Soldered to 3.5mm headphone jack
 - Anyone remember those?
- Add a resistor to make phone think it's a microphone



Loopstick Antenna



Wired into 3.5mm Jack

A new Challenger Appears!

Rocateq, and a funny story involving my dad



Introducing Rocateq



ATTENTION SHOPPERS

Our shopping carts will stop at the exit if not taken through the checkout lane.



Let's do some research:

Publicly available Information:

- FCC filings
- Patent information
- Marketing information

Field Research:

- Physical Disassembly
- RF Captures
- Reverse Engineering



Marketing Materials

Wheel fitting

Fittable on any cart

Durable bearings

Equipped for a high load capacity

Tread

High driving comfort and hard-wearing

RF receiver

Activates the (un)locking mechanism and can up- and download data

Braking mechanism

Prevents an abrupt stop

Battery

Lasts very long



Marketing Materials

Wheel fitting

Fittable on any cart

Durable bearings

Equipped for a high load capacity

Tread

High driving comfort and hard-wearing



RF receiver

Activates the (un)locking mechanism and can up- and download data

Braking mechanism

Prevents an abrupt stop

Battery

Lasts very long

Marketing Materials

Wheel fitting

Fittable on any cart

Durable bearings

Equipped for a high load capacity

Tread

High driving comfort and hard-wearing



RF receiver

Activates the (un)locking mechanism and can up- and download data

Braking mechanism

Prevents an abrupt stop

Battery

Lasts very long

FCC Filings - Checkout Transmitter

3. OCS RFID Caster Test Delay: When the caster is unlocked, it receives an A signal and receives a wireless signal (B signal) emitted by Wireless 2.4 GHz transmitter after 30 seconds. The receiving time is more than 0 seconds (delay), and then receives an A signal. The caster is unlocked. In this test, the wireless 2.4 GHz transmitter is set with a remote controller to delay 3 seconds, 5 seconds, 10 seconds, 20 seconds, 30 seconds and 60 seconds. In the second test, when the receiving time is greater than or equal to the delay time, the casters are not locked, and when the receiving time is less than the delay time, the casters are locked.

3. Terminology and code

3.1. The B signal (2.4 GHz) emitted by Wireless 2.4 GHz transmitter makes the relevant shopping cart casters unlock after receiving A signal (8.13KHz) again.

4.Shell size (Fig. 1) (Unit: mm)

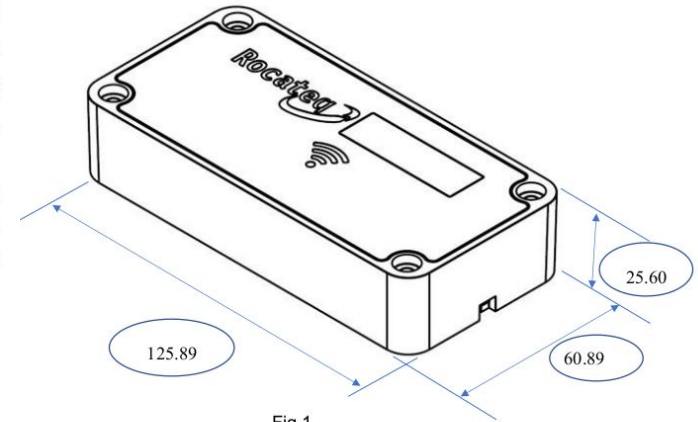
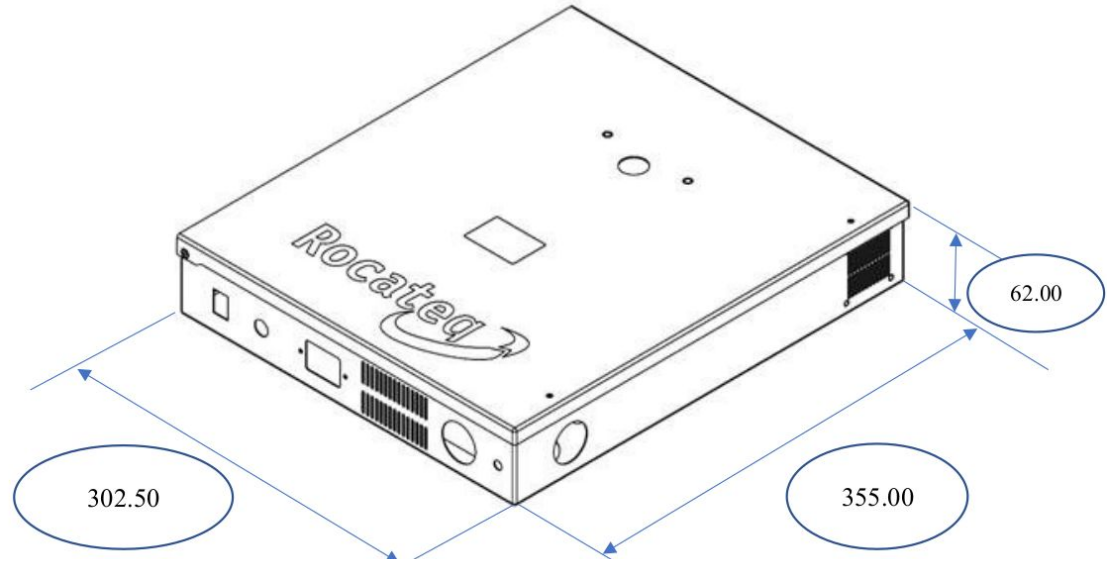


Fig.1

FCC Filings - Loop Controller



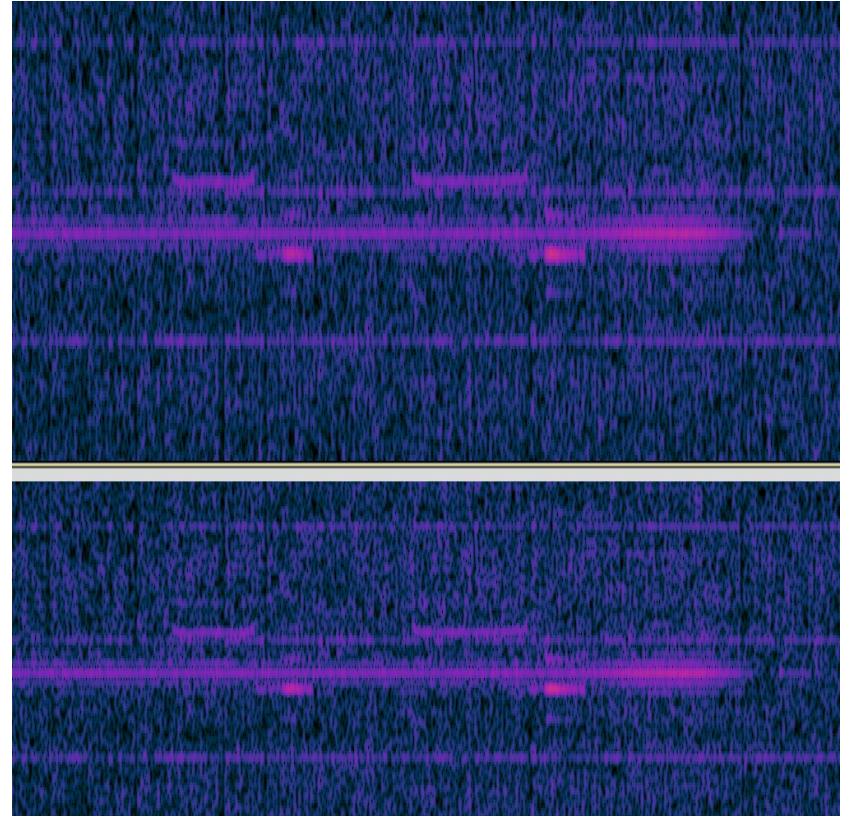
3. Terminology and code

31 Intellibox emits A signal (8.13KHz), C signal (8.13KHz), H signal (8.13KHz), and receives alarm signal (2.4 GHz). Relevant shopping cart casters receive two A signals (8.13KHz) and lock. Intellibox receives alarm signal and will alarm.

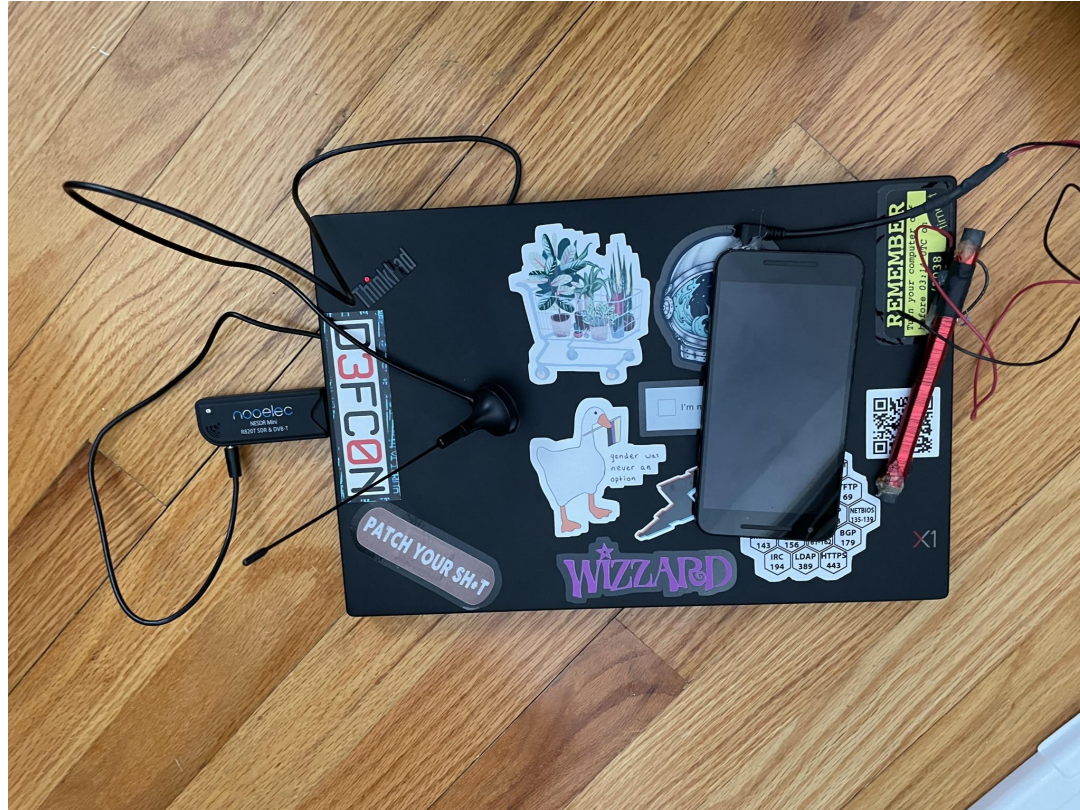
How do we talk to and process these signals?

- kHz radio waves -> in 'audio' range, can use audio amps
- Homemade loopstick antennas
- Manipulate and generate signal captures in Audacity
 - Spectrogram is the most useful presentation

Time to go Warcarting!



Warcarting - The Setup

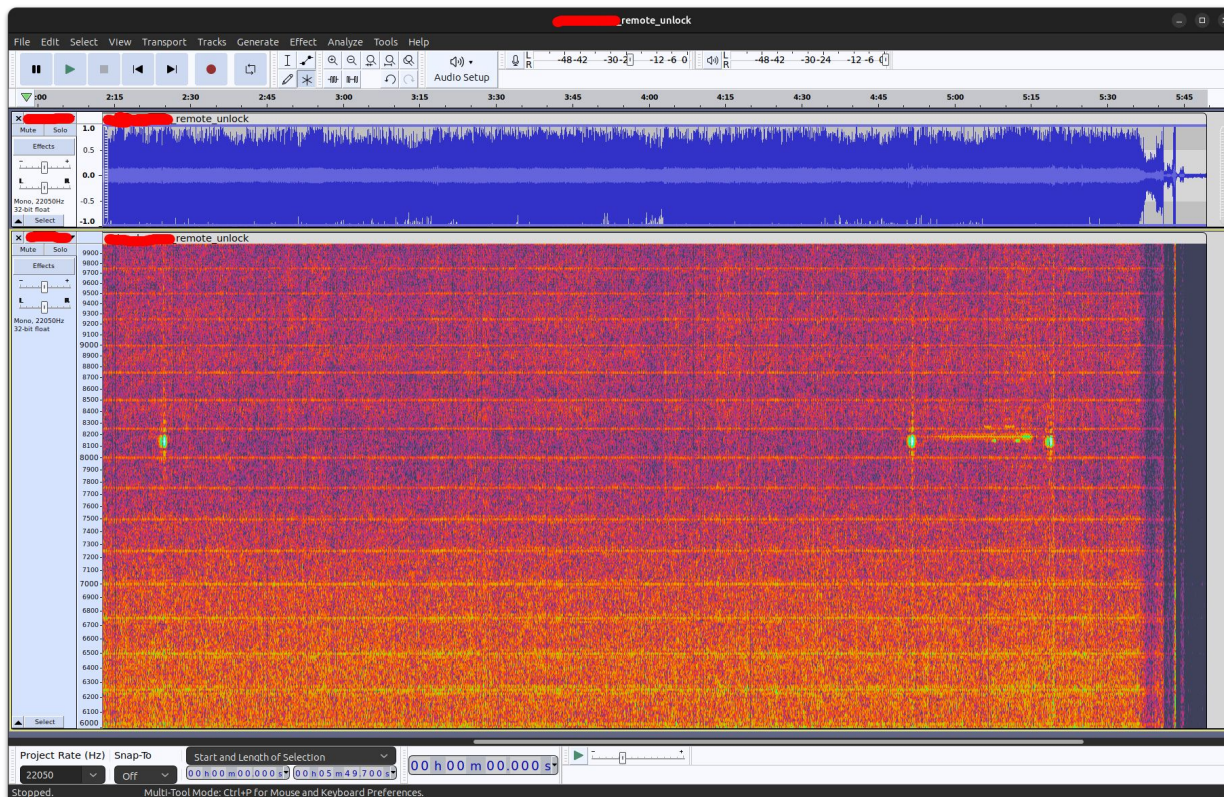


Warcarting - The Heist

- Laptop with SDR in backpack under cart
- Engineer situation that will cause cart to lock, get shopkeeper assistance
- Capture unlock signal from remote when this happens

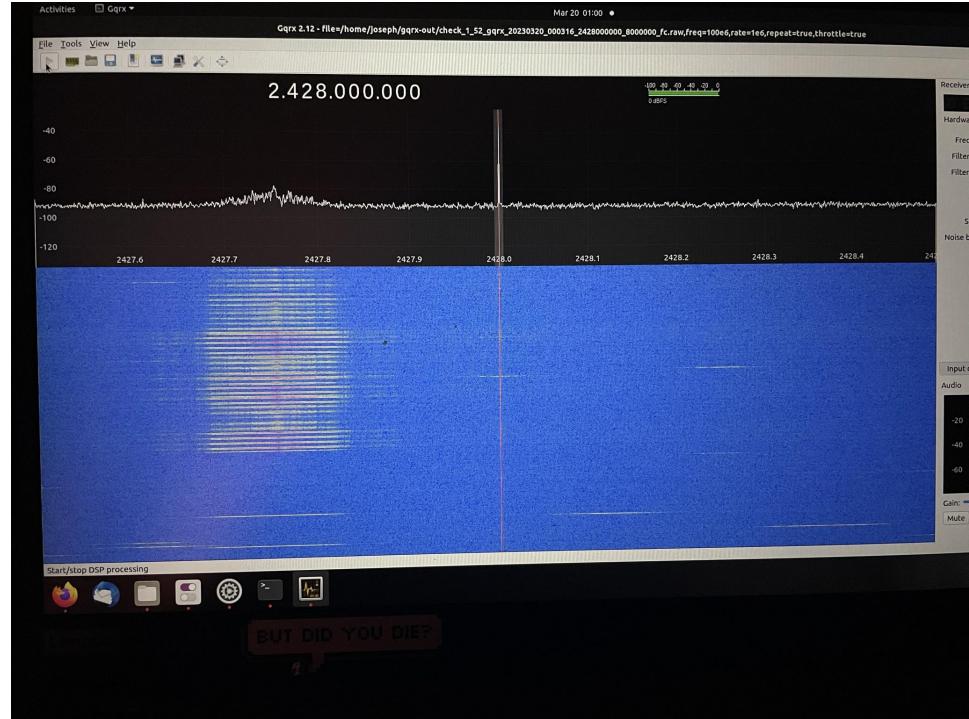


Warcarting - The Payoff



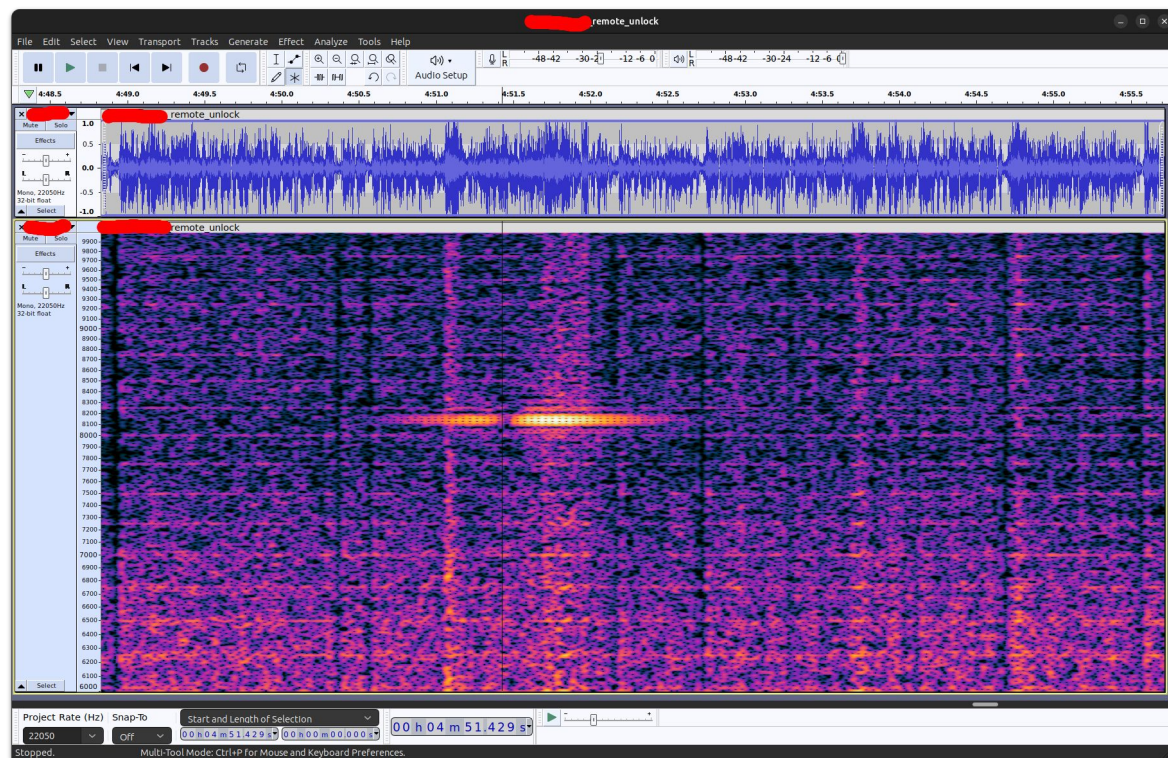
The Signals

- Perimeter lock signal
- Arm lock signal
- Unlock
- Alarm mute
- 'Purcheck'
 - Both at KHz and GHz



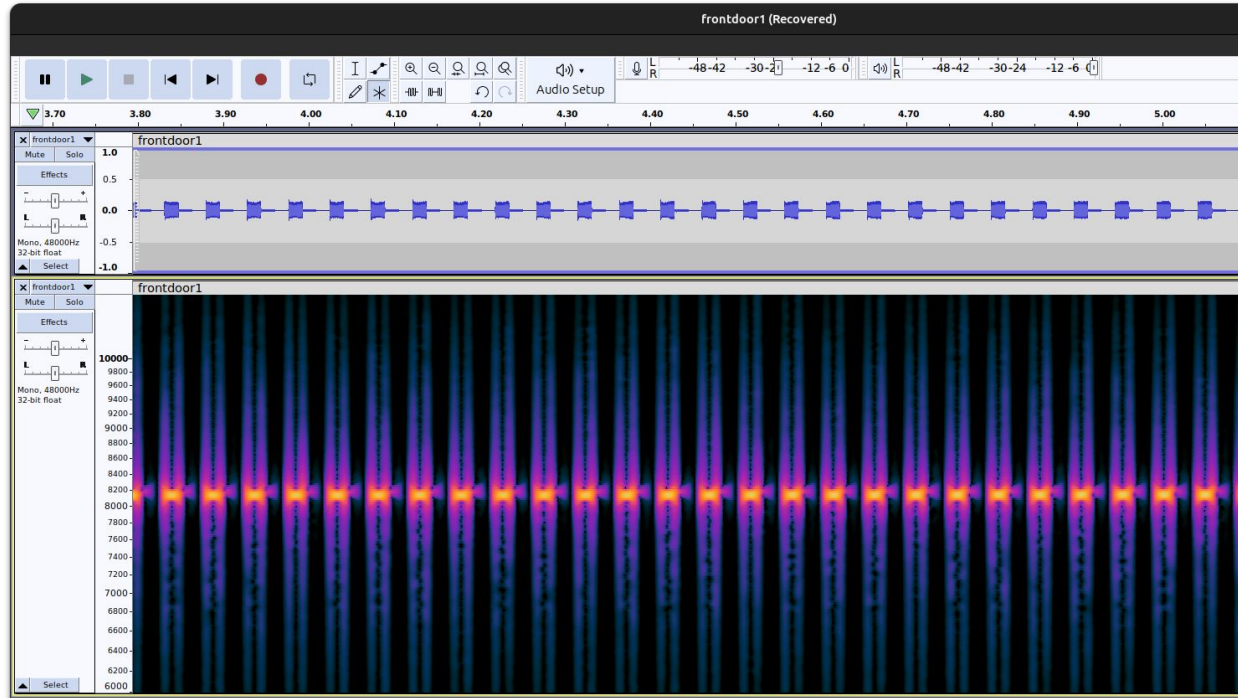
2.4 GHz "Purcheck Signal"

Unlock Signal



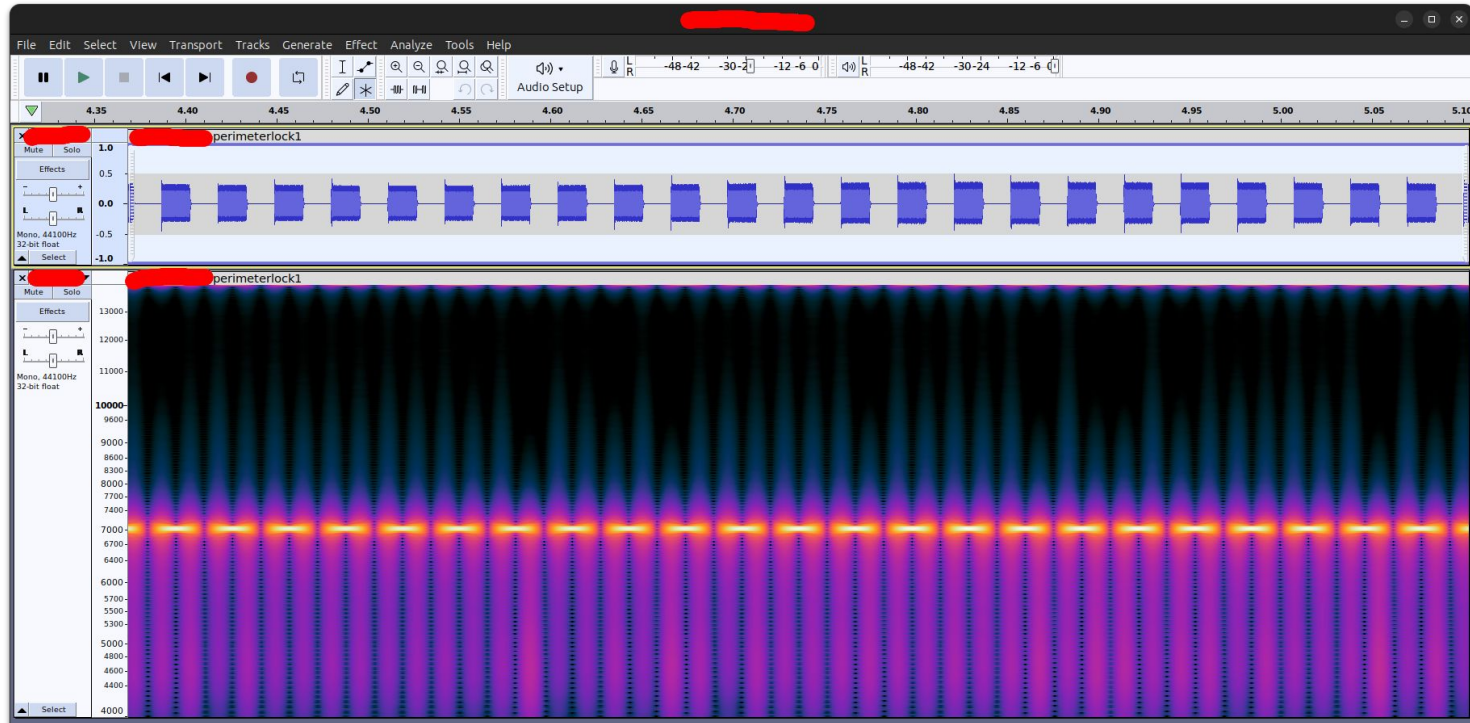
8.150 kHz tone

'Arming' Signal



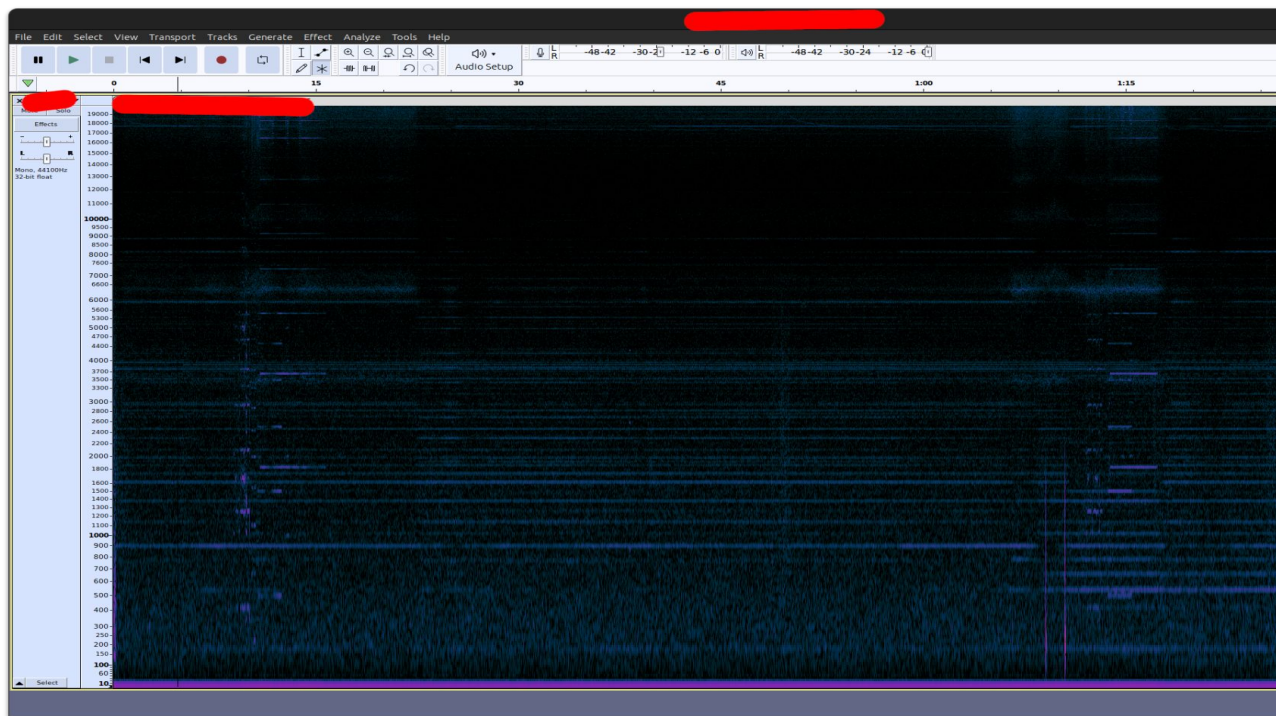
8.150 kHz pulses, 50ms length w/ 33% duty cycle

Lock Signal



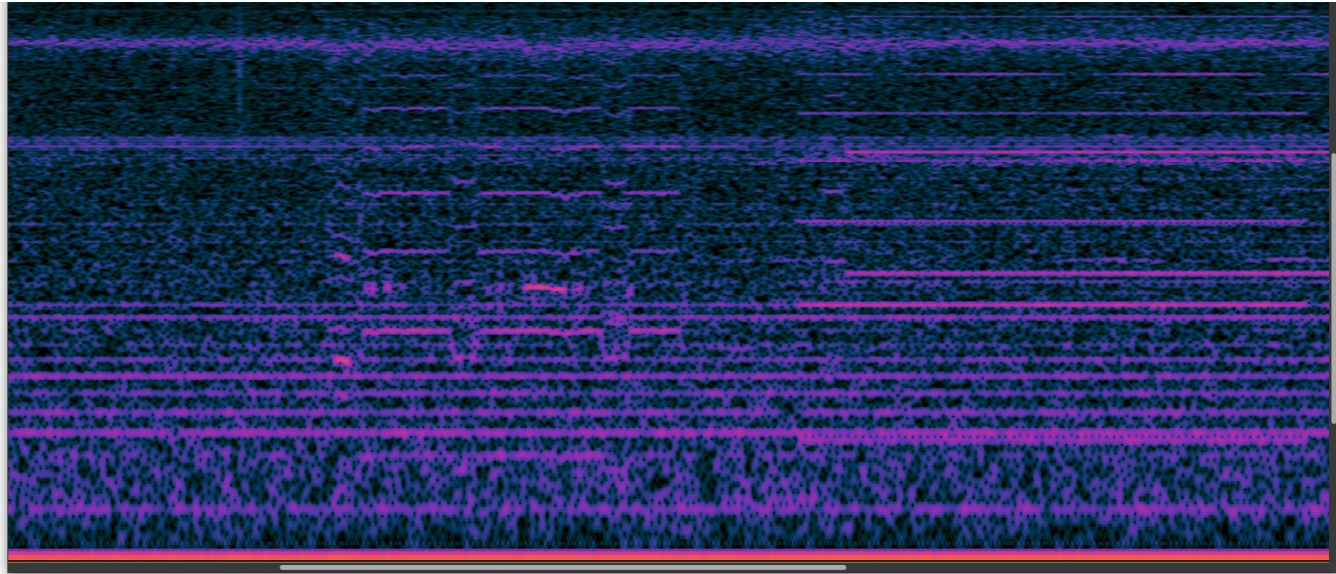
7.000 kHz pulses, 30ms length w/ 50% duty cycle

Purcheck Signal



Tones repeated at various frequencies with brief $\sim 250\text{Hz}$ step down

Purcheck Signal



Tones repeated at various frequencies with brief $\sim 250\text{Hz}$ step down

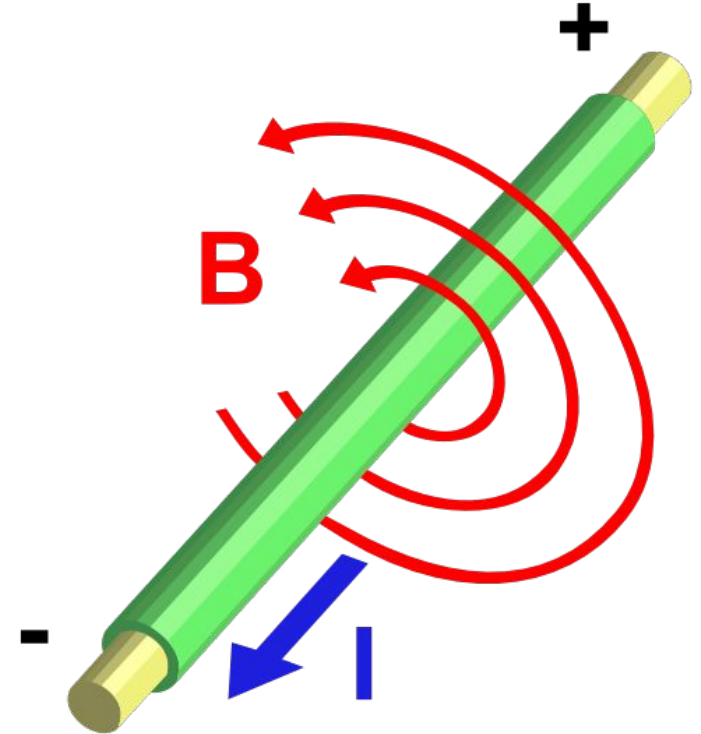
Time to get Phreaky



- Refers back to John Draper using a whistle to control payphones
- These signals lack authentication/security
 - Replay attack will work
- Can replay using loopstick antenna
- Or we can use our phone speaker, playing an MP3 file
- Lock and unlock work, but the arming signal is inconsistent

A brief aside about PARASITIC EMF

- Current moving through a wire generates electrical and magnetic fields
- Governed by the “right-hand rule”
- Speaker coils generate EMF at the radio frequency corresponding to the audio wave
 - Very weak, but enough for shenanigans
- **It's not the sound - but the speaker coil that makes the sound that triggers it**



It works, kinda...

- Replaying signals sometimes works
- Not consistent behavior
 - Could be issues with transmit method being too weak
 - Could be issues with captured samples
 - Could be anything else (spoiler: it was)

Only one thing left to do...

Time to tear one down!

Thanks ebay!



Delivered

Order date: Sep 27, 2022 • Order total: [REDACTED] Order number: [REDACTED]

[View order details](#)

Delivered on Fri, Sep 30

Returns not accepted.

Rocateq Shopping Cart Wheel with RF Security caster. Loss prevention.

Sold by: [REDACTED]

[View similar items](#)[View seller's other items](#)[More actions ▾](#)

A Word on Reverse Engineering

- Limited by scope, time and equipment
- This was a hobby project, and had a tighter scope
- Oftentimes trying to understand design decisions made by others
 - Technical design decisions
 - Business design decisions
 - Security design decisions
- Like looking at footprints and trying to figure out what someone had for lunch

gn̄iṛəəniḡnə

A Quote on Reverse Engineering

“Albert grunted. "Do you know what happens to lads who ask too many questions?"

Mort thought for a moment.

"No," he said eventually, "what?"

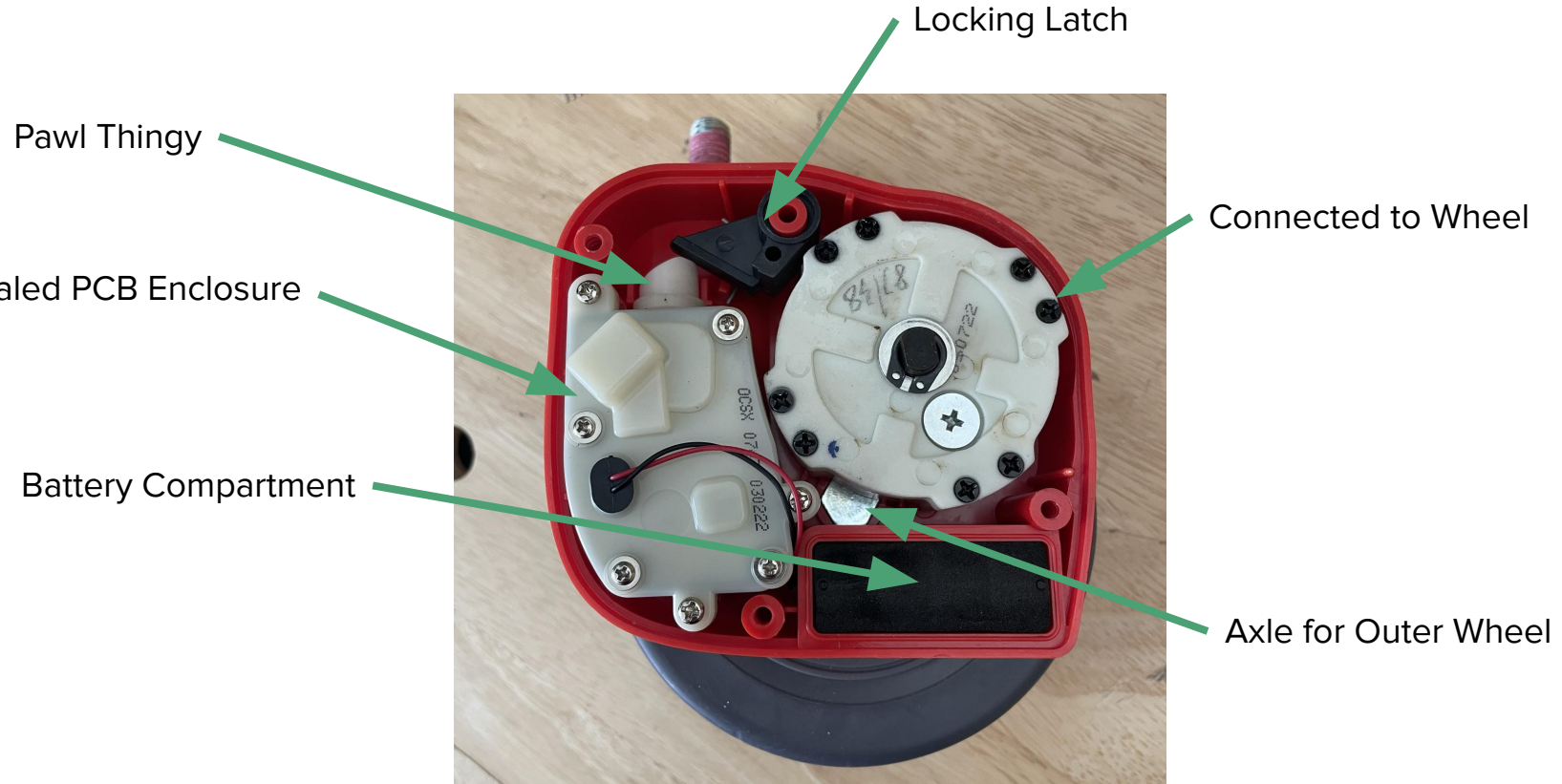
There was silence.

Then Albert straightened up and said, "Damned if I know. Probably they get answers, and serve 'em right."

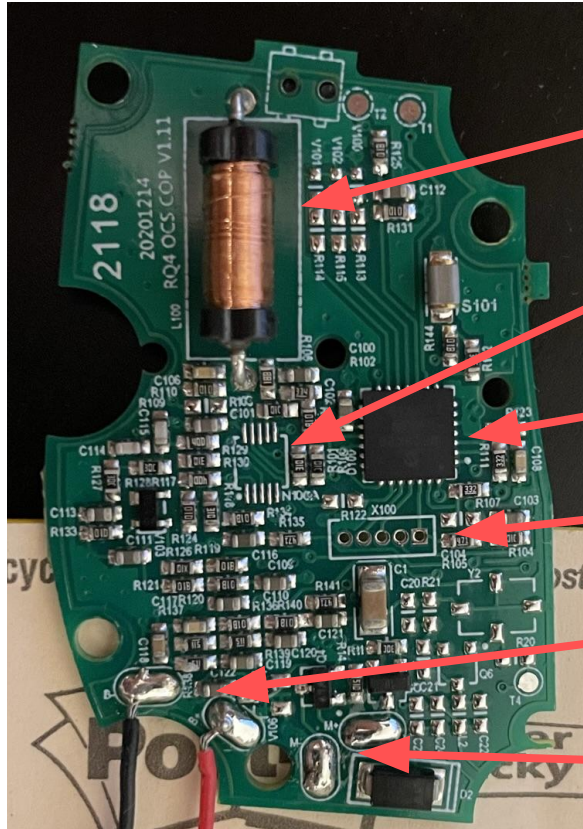
— Terry Pratchett, [Mort](#)



Mechanical Teardown



Electrical Teardown - PCB Front



Kilohertz antenna (inductor)

Missing Chip Footprint (fun!)

Microcontroller (PIC18F23K20)

Programming Header

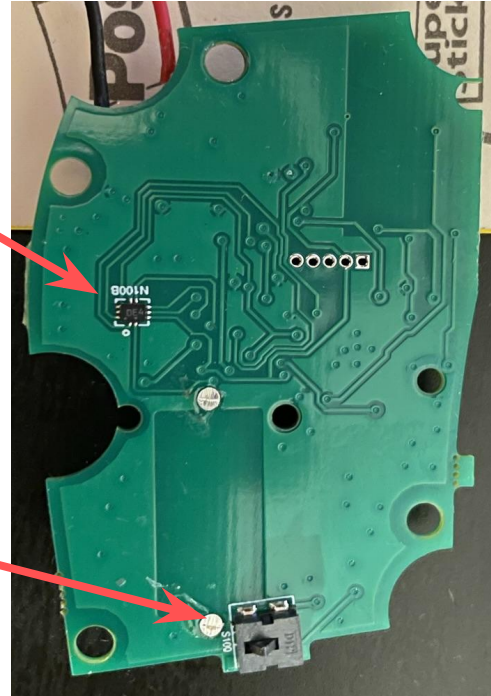
Battery Connector

Motor Connection

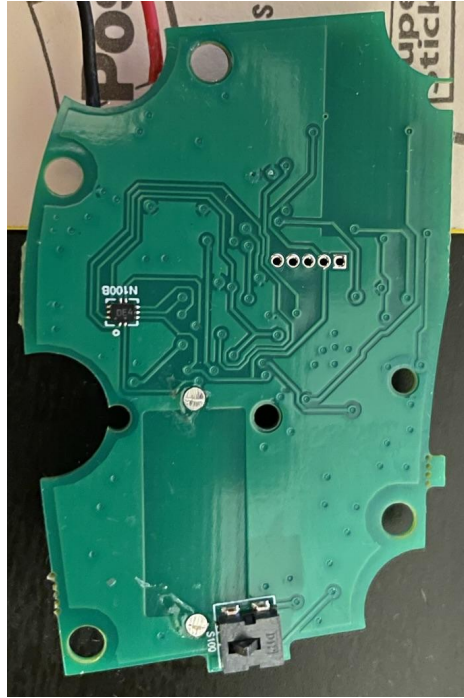
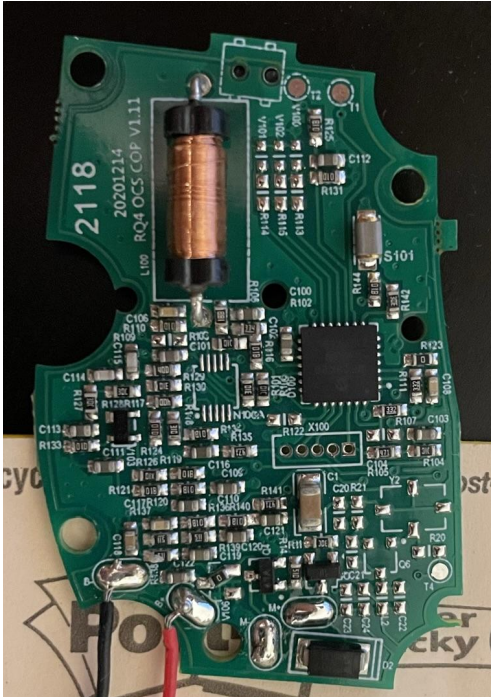
Electrical Teardown - PCB Back

Mystery Chip!

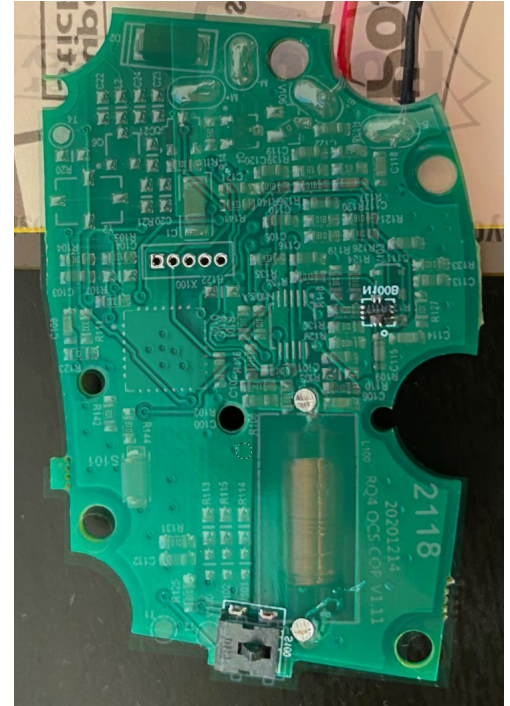
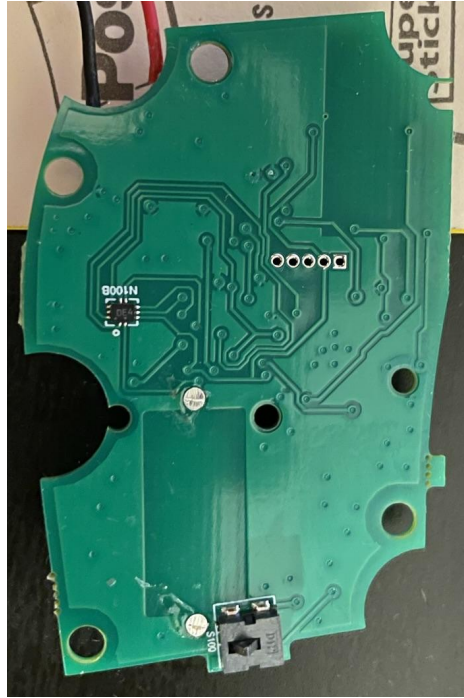
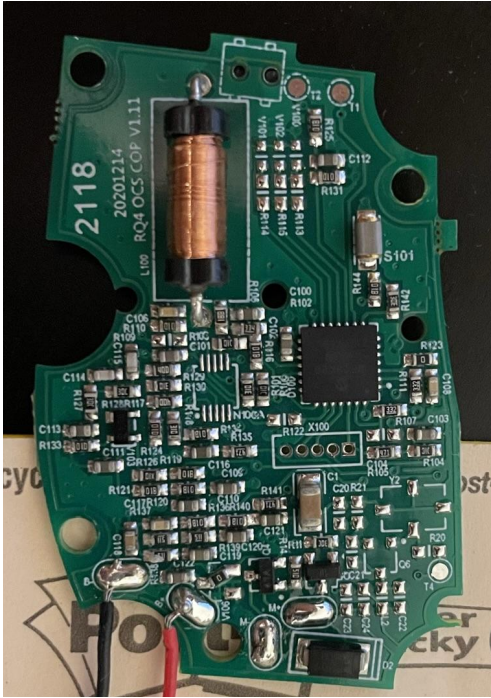
Sensor for Pawl



Tracing PCBs: overlaying images



Tracing PCBs: overlaying images



Tracing PCBs: overlaying images

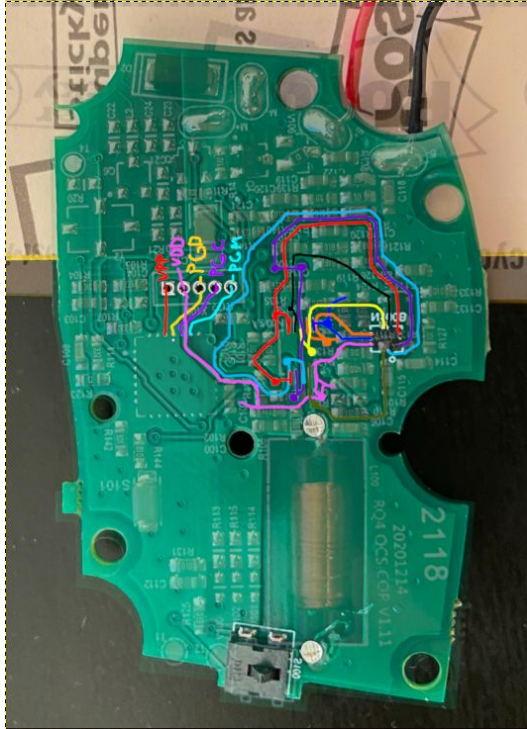
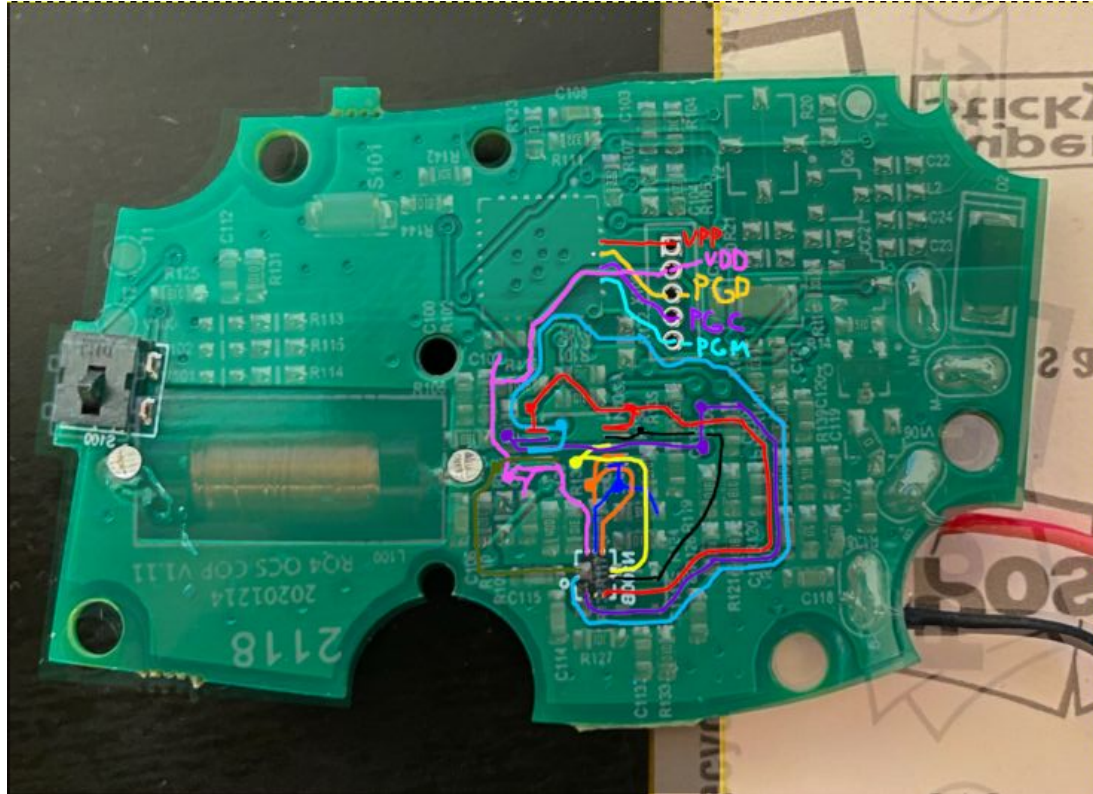


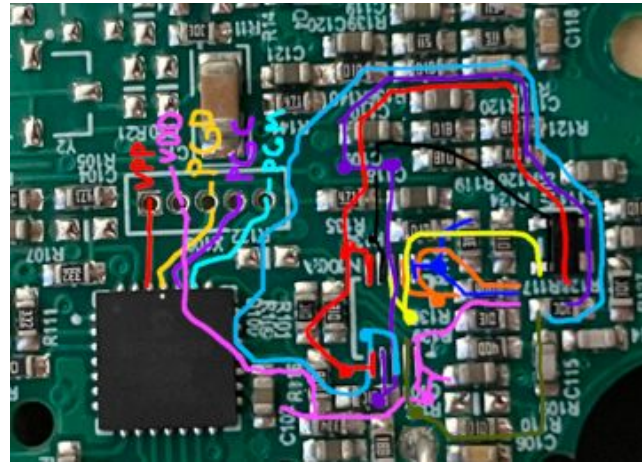
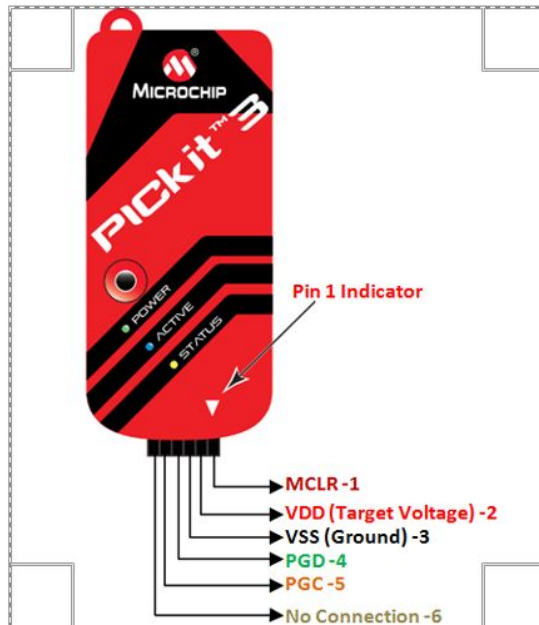
FIGURE 2: 28-PIN QFN/UQFN

[illegible]

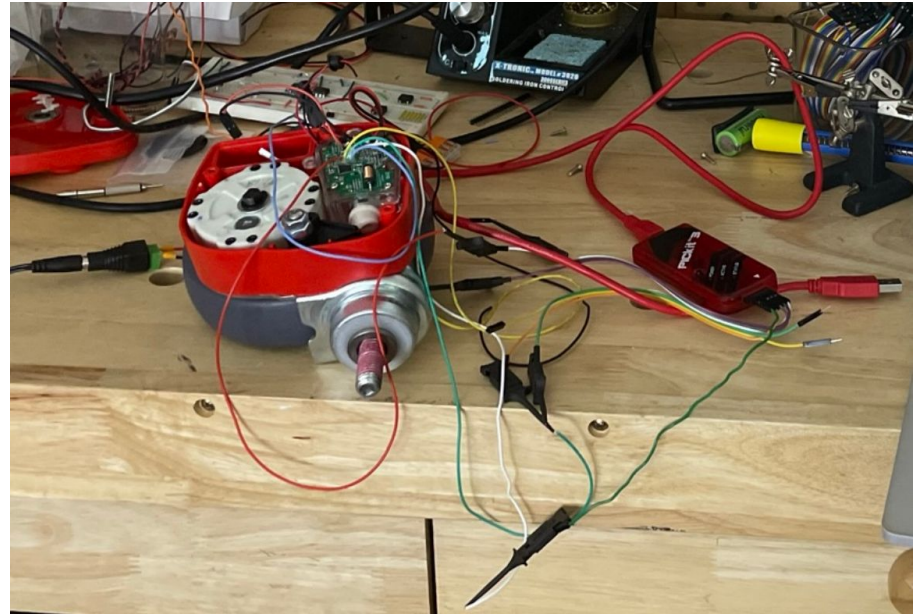
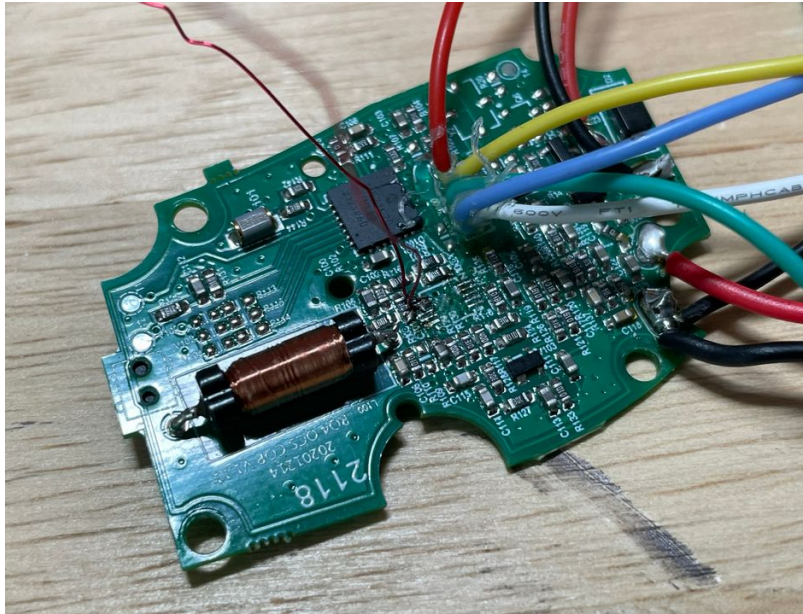
Tracing PCBs: overlaying images



Pulling the firmware off using a PikKit... yoink!

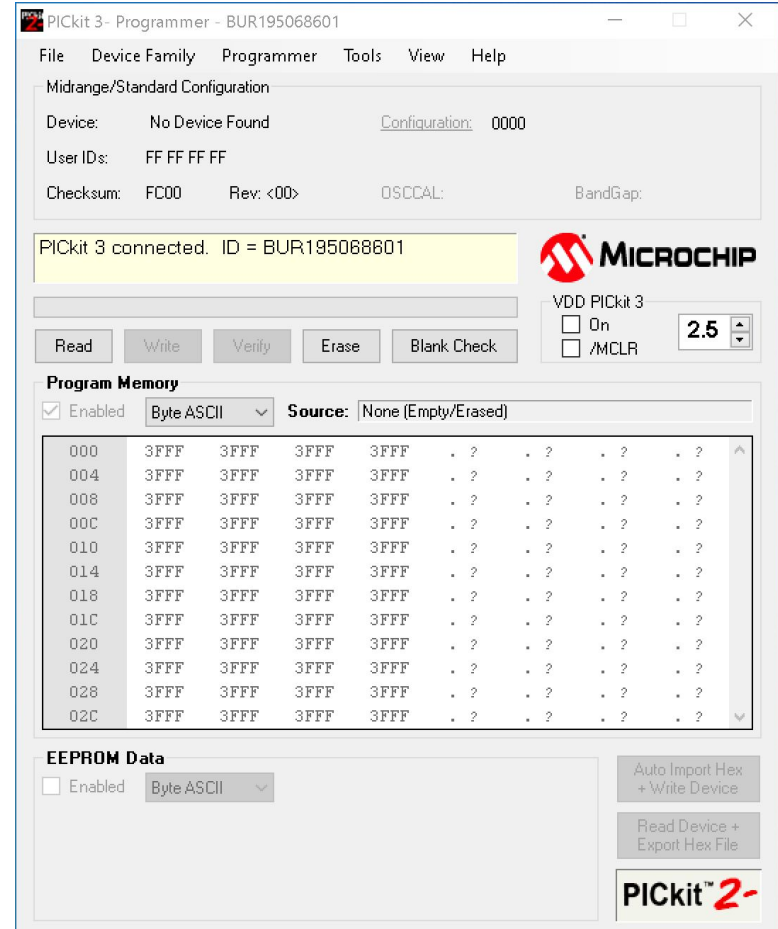


Pulling the firmware off using a PikKit... yoink!



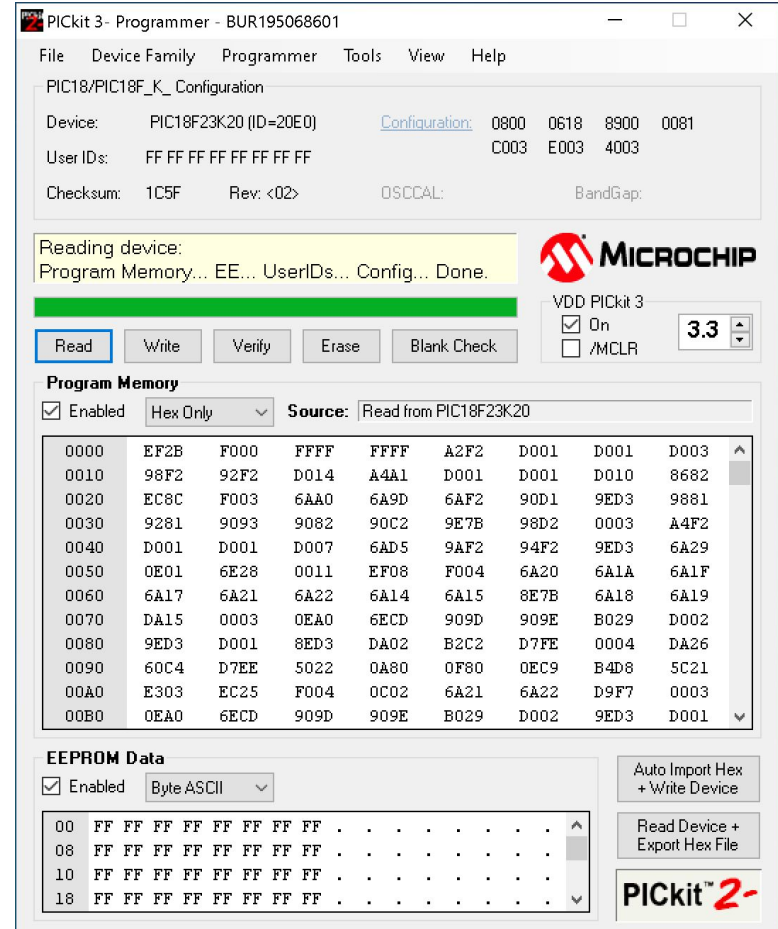
Connecting the PICkit

- PICkit2- is free
 - More limited feature set, but enough for us
- Connect via USB, handle bootloader shenanigans
- Select device and try connecting
 - In this case PIC18F23K20
 - Make sure you actually have all the wires...



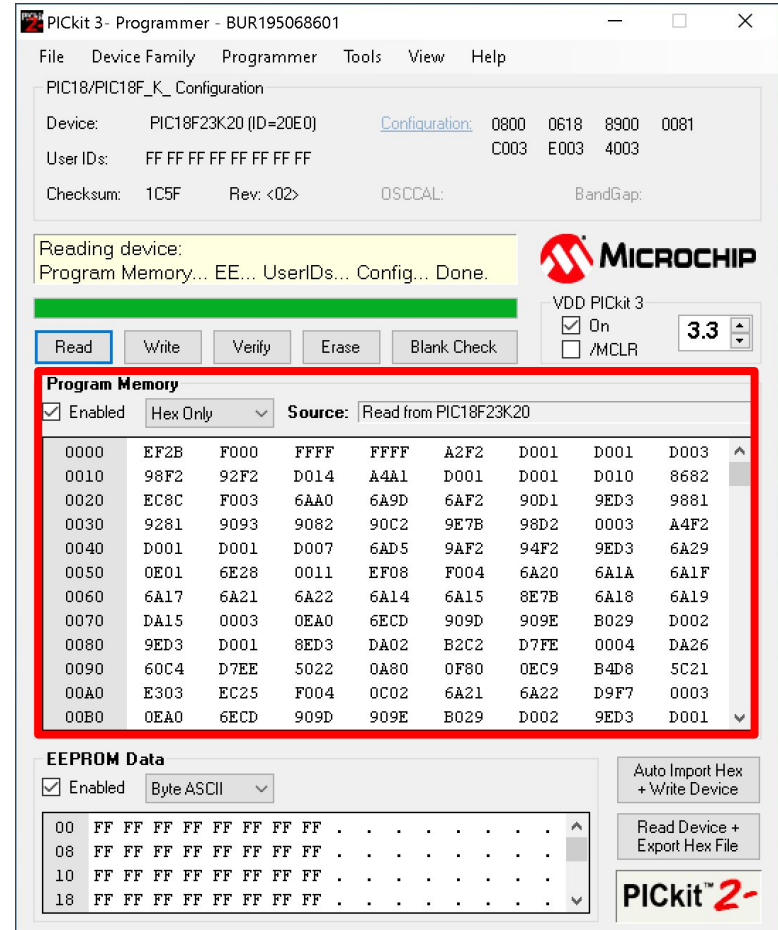
Connecting the PICkit

- PICkit2- is free
 - More limited feature set, but enough for us
- Connect via USB, handle bootloader shenanigans
- Select device and try connecting
 - In this case PIC18F23K20
 - Make sure you actually have all the wires...
- We're in! We can see:
 - Program Memory
 - Config Bits
 - EEPROM Data



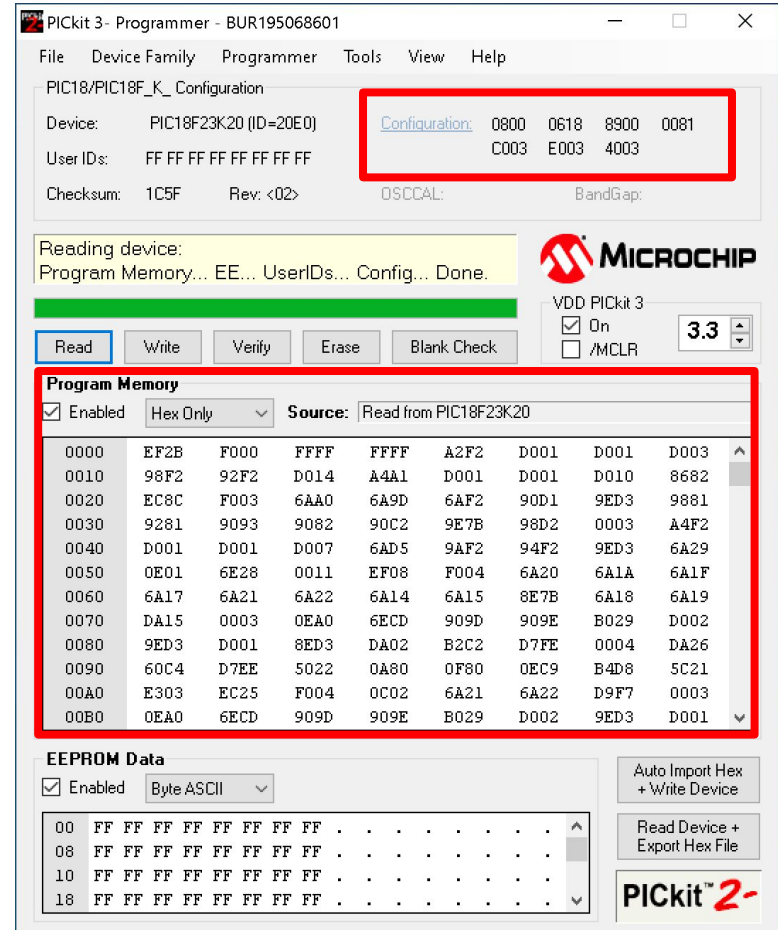
Connecting the PICkit

- PICkit2- is free
 - More limited feature set, but enough for us
- Connect via USB, handle bootloader shenanigans
- Select device and try connecting
 - In this case PIC18F23K20
 - Make sure you actually have all the wires...
- We're in! We can see:
 - Program Memory
 - Config Bits
 - EEPROM Data



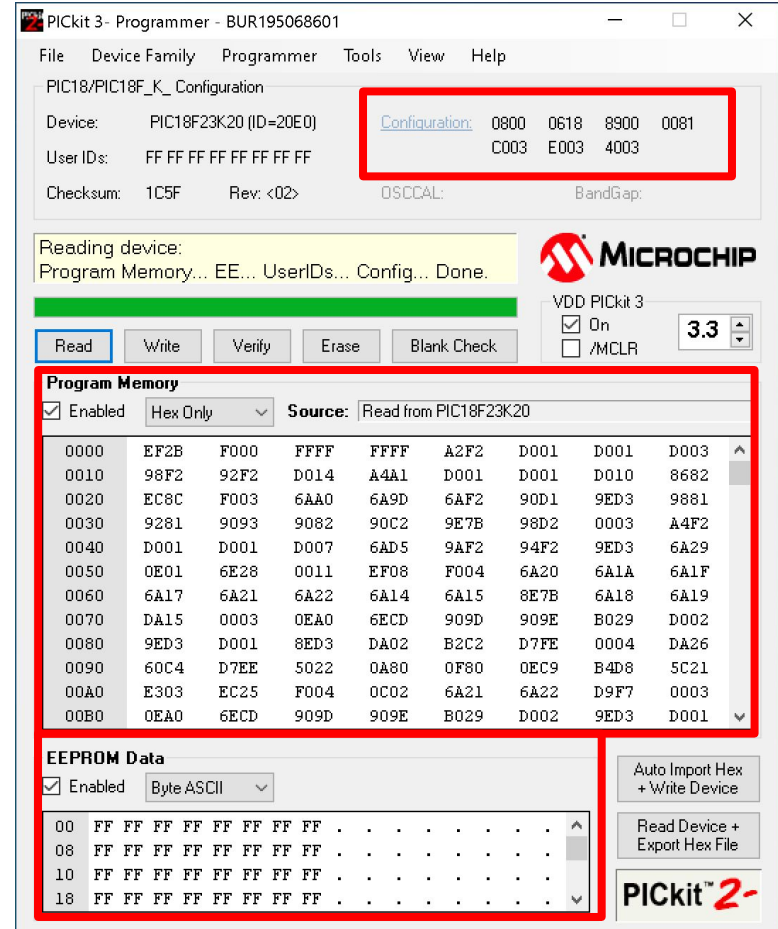
Connecting the PICkit

- PICkit2- is free
 - More limited feature set, but enough for us
- Connect via USB, handle bootloader shenanigans
- Select device and try connecting
 - In this case PIC18F23K20
 - Make sure you actually have all the wires...
- We're in! We can see:
 - Program Memory
 - Config Bits
 - EEPROM Data



Connecting the PICkit

- PICkit2- is free
 - More limited feature set, but enough for us
- Connect via USB, handle bootloader shenanigans
- Select device and try connecting
 - In this case PIC18F23K20
 - Make sure you actually have all the wires...
- We're in! We can see:
 - Program Memory
 - Config Bits
 - EEPROM Data



A Quick Note on Configuration Bits and Security

Configuration Word Editor

Device Configuration Words may be edited here at the bit level. Refer to device datasheet for specific configuration bit functions.

☐ = Unimplemented bit ☒ = Configuration bit. Click to toggle value.

Name	Address	Value	Bit Edit
			15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
CONFIG1	300000	0800	0 8 - - 1 0 0 0 - - - - - - - -
CONFIG2	300002	0618	- - - 0 0 1 1 0 - - - - 1 1 0 0 0
CONFIG3	300004	8900	1 - - - 1 0 0 1 - - - - - - - -
CONFIG4	300006	0081	- - - - - - - 1 0 - - - 0 - 1
CONFIG5	300008	C003	1 1 - - - - - - - - - - 1 1
CONFIG6	30000A	E003	1 1 1 - - - - - - - - 1 1
CONFIG7	30000C	4003	- 1 - - - - - - - - - - 1 1

Unimplemented bits are displayed in the Value column as selected in menu Tools > Display Unimplemented Config Bits

Save Cancel

- Code protection is set by config bits
 - Code-protect (CPn)
 - Write-protect (WRTn)
 - External Block Table Read (EBTRn)
- Which ones do what is available in the data sheet
- None of them are set in the wheels **happy hacker noises**

TABLE 23-3: SUMMARY OF CODE PROTECTION REGISTERS

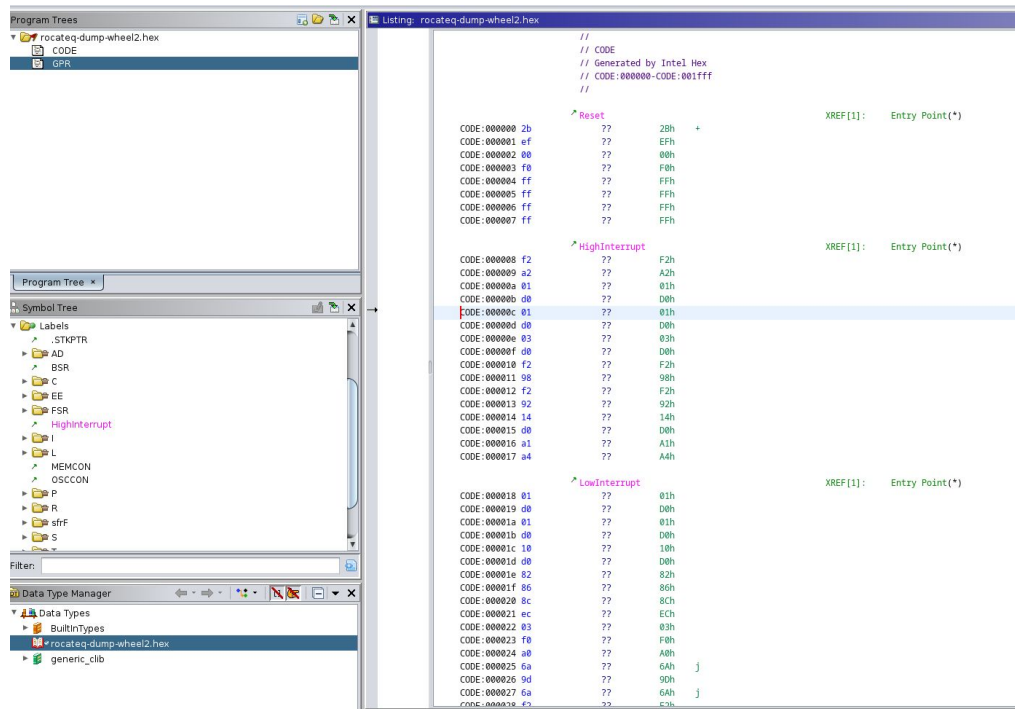
File Name	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
300008h	CONFIG5L	—	—	—	CP3 ⁽¹⁾	CP2 ⁽¹⁾	CP1	CP0
300009h	CONFIG5H	CPD	CPB	—	—	—	—	—
30000Ah	CONFIG6L	—	—	—	WRT3 ⁽¹⁾	WRT2 ⁽¹⁾	WRT1	WRT0
30000Bh	CONFIG6H	WRTD	WRTB	WRTC	—	—	—	—
30000Ch	CONFIG7L	—	—	—	EBTR3 ⁽¹⁾	EBTR2 ⁽¹⁾	EBTR1	EBTR0
30000Dh	CONFIG7H	—	EBTRB	—	—	—	—	—

Legend: Shaded cells are unimplemented.

Dump the firmware, open it up in Ghidra...

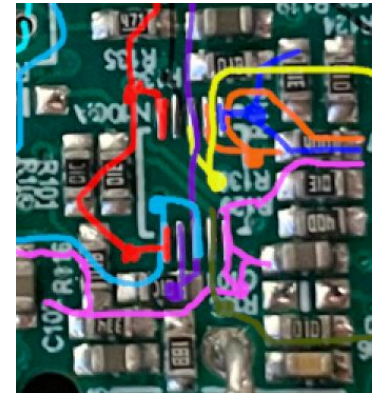
Hmm, there's not a whole lot here...

- Only around 2kb of actual code
 - Rest is set to 0xFF
- Reset, high/low interrupts
- Little bit of other code
- I'm not an RE expert, but it seems like there's something else going on...
- Potentially only for motor control, logic happens elsewhere
 - Mystery chip on back on board?

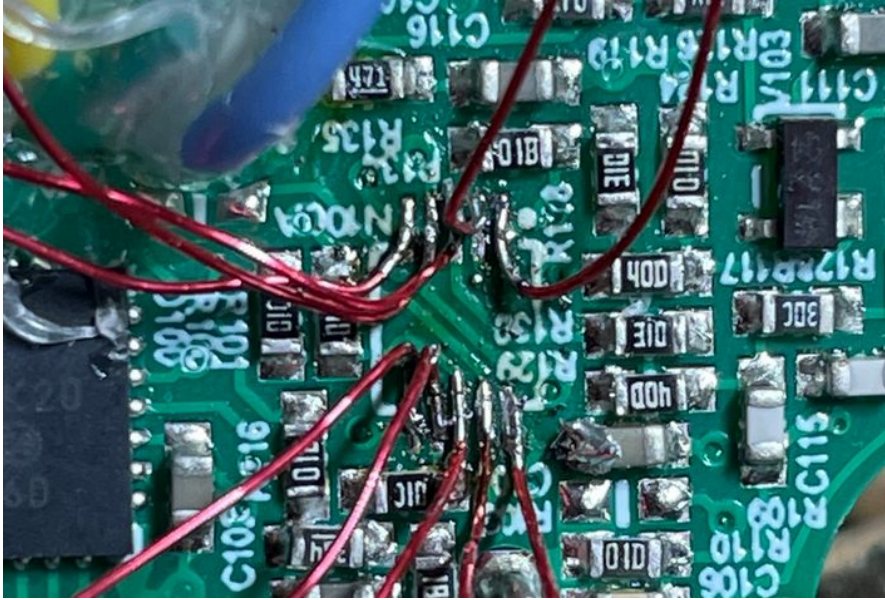


But what about that mystery chip?

Go back to what we traced out... ooh, there's exposed pads!



Tiny tiny soldering....

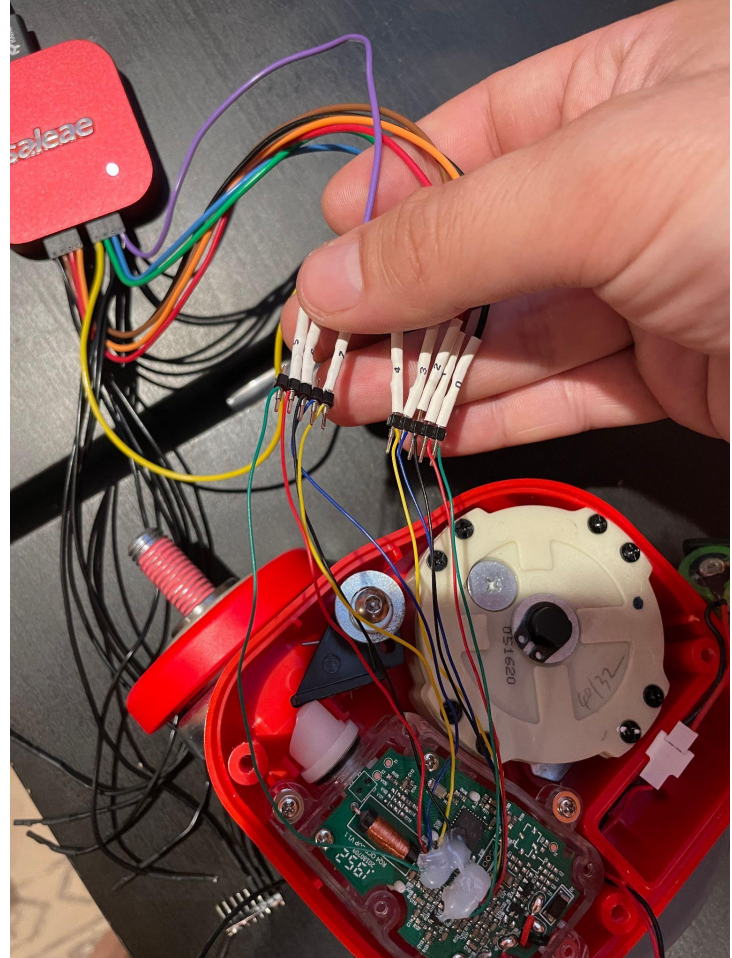


- We've got to solder tiny 'fly wires' onto each pad
 - 30ga solid core wire or enamel wire
 - Wire-wrapped around header pins
- Very small pitch, but still hand-doable
 - Lots of flux
 - Work from one edge out
 - Small, sharp soldering iron tip w/ flat
 - Don't damage the pads!!

Logic Probing

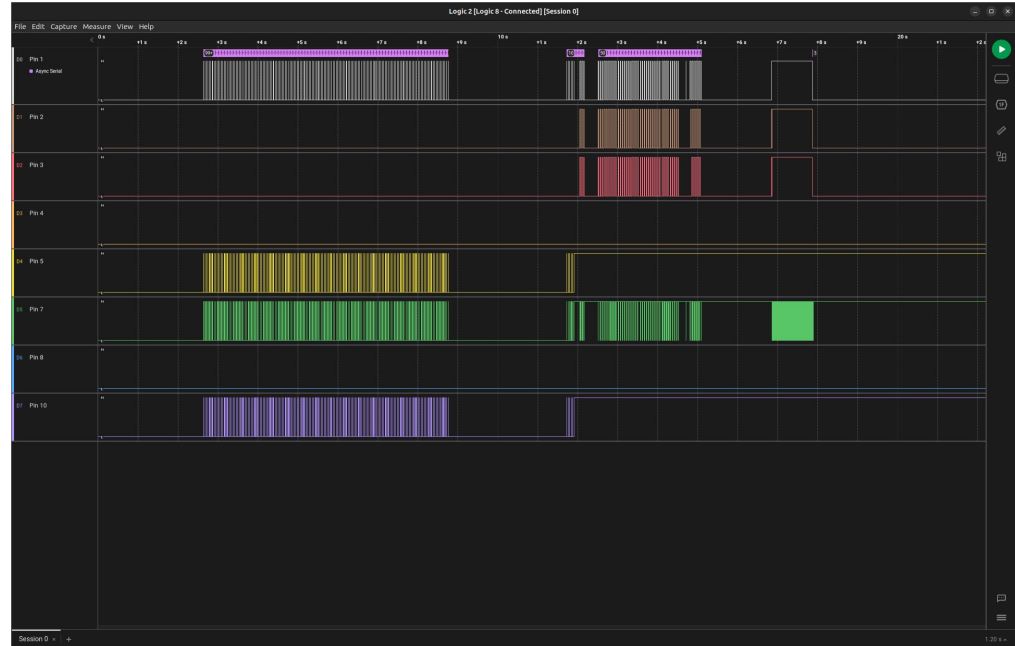
Break out the Saleaeae

- 8 channel logic analyzer
- Can measure digital and analog simultaneously
- Logs and analyzes data
- Basically a super compact 8 (or 16!) channel oscilloscope

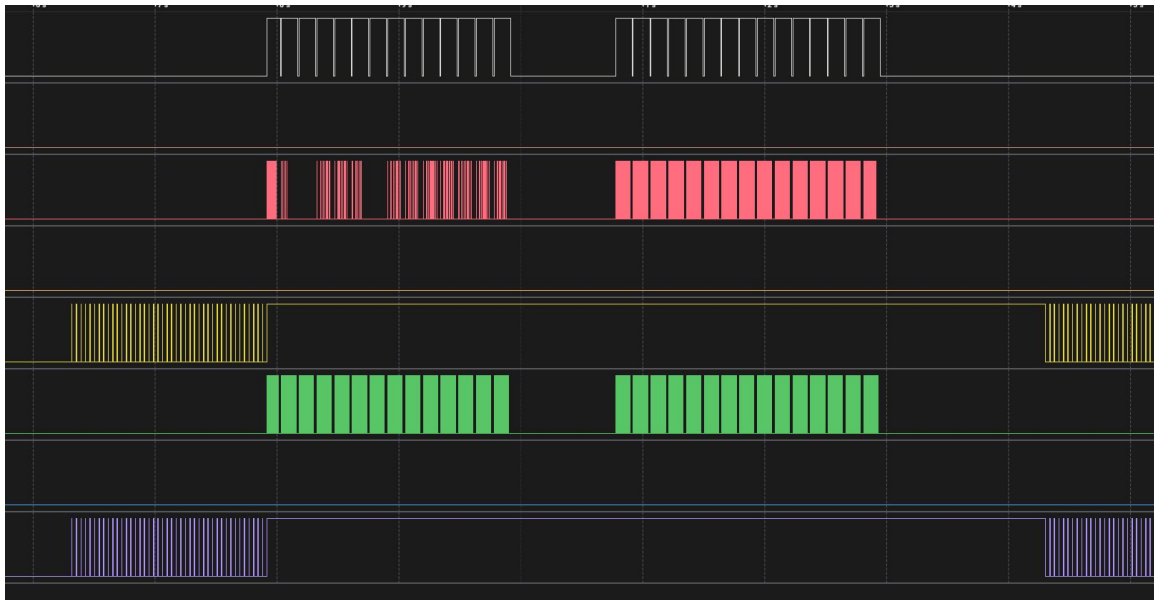


Accelerometer data... interesting!

- Multiple lines oscillate when I move the wheel
- Signals are only processed when the wheel is 'in motion'
 - Likely a power saving feature



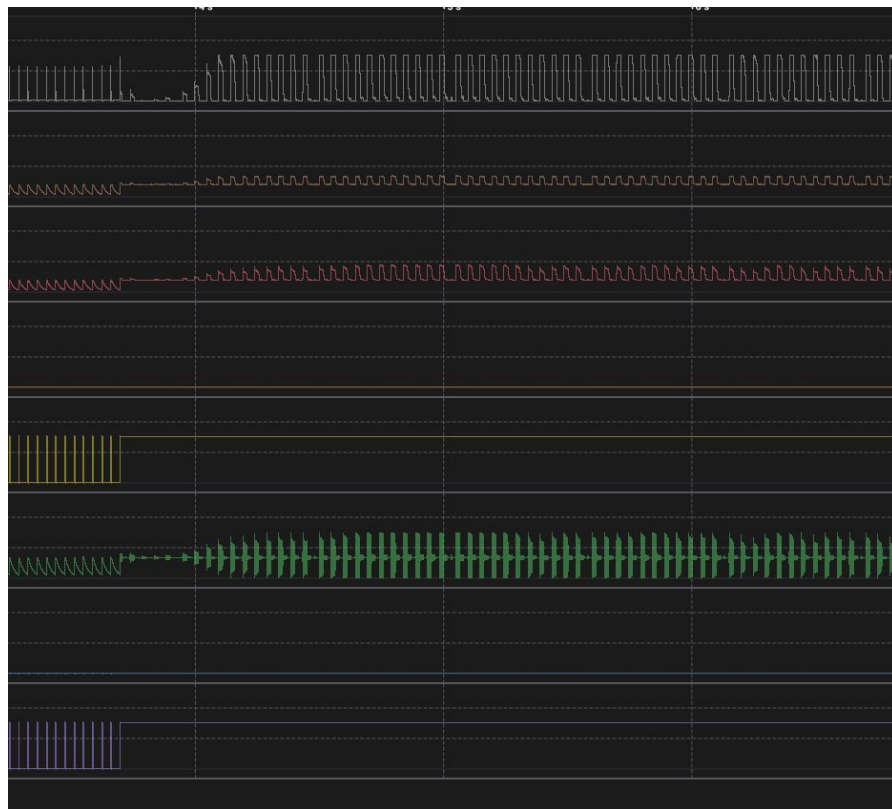
What happens when we send a signal?



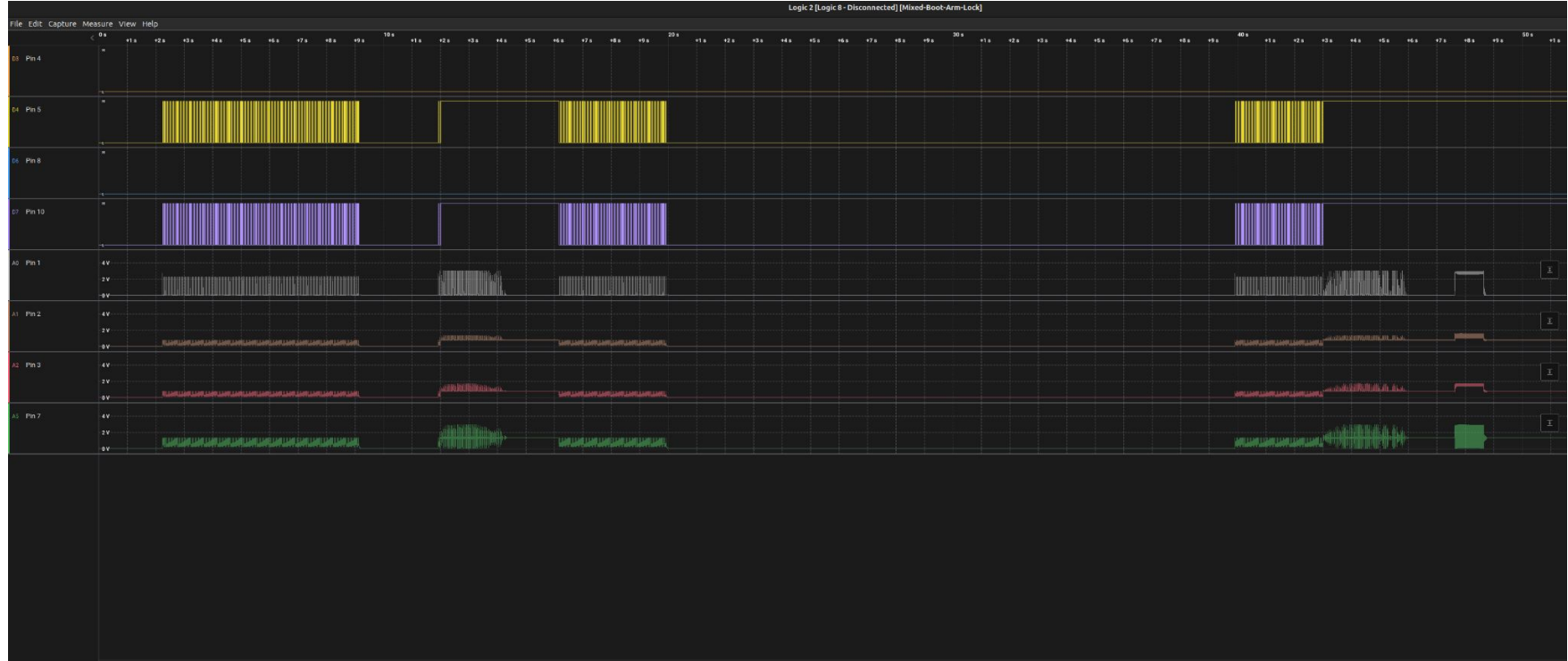
- Accelerometer signals peg high
- 3 lines respond in roughly the same shape as the signal, but different
 - Green is closest
 - Red and white follow shape, but weirdly

Time to get... analog!

- Turns out 3 of the lines are antenna input
- Different lines have different physical filters applied
- Doing math in hardware!
- We can set up mixed digital/analog in the Saleae software

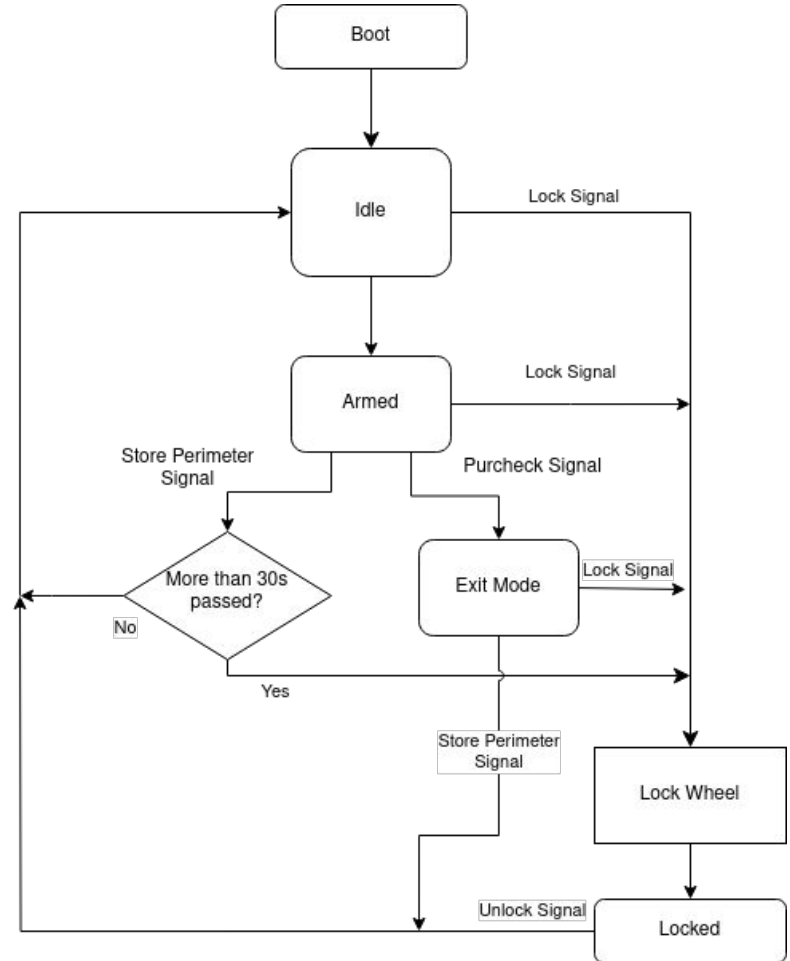


The whole thing put together... boot, arm, and lock.



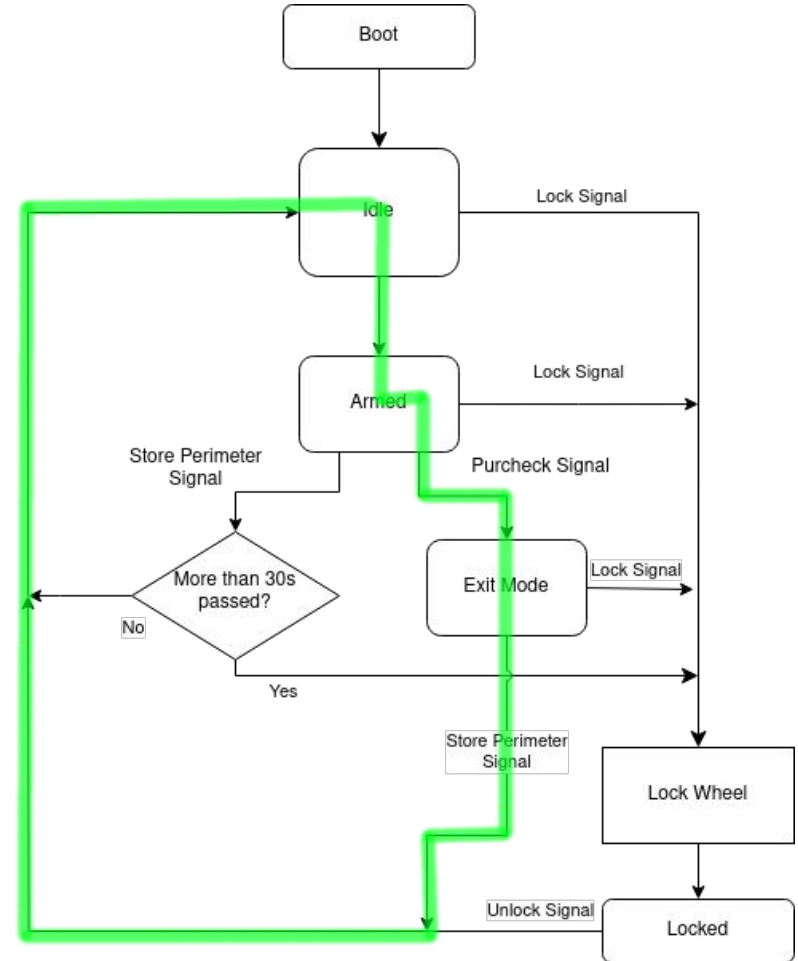
Making a Flowchart

- Lets us map out different states and actions
- Makes potential bypasses easier to see
 - Want to get back to IDLE without locking at door
- Sometimes multiple methods



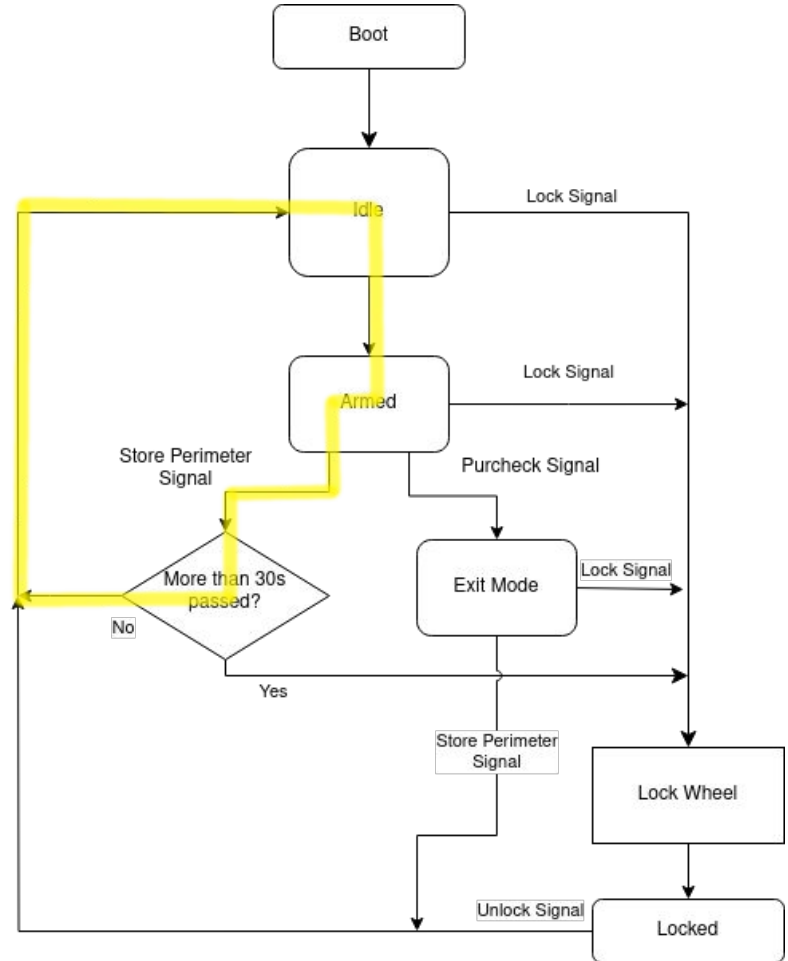
Making a Flowchart

- Lets us map out different states and actions
- Makes potential bypasses easier to see
 - Want to get back to IDLE without locking at door
- Sometimes multiple methods
 - Obvious purchek replay



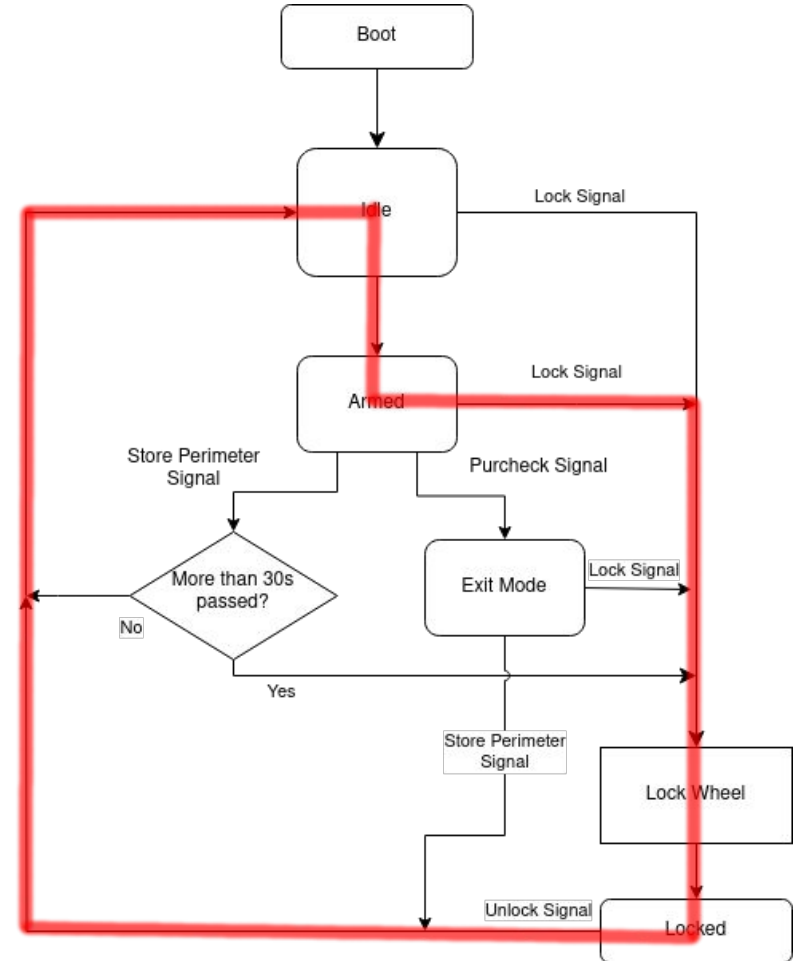
Making a Flowchart

- Lets us map out different states and actions
- Makes potential bypasses easier to see
 - Want to get back to IDLE without locking at door
- Sometimes multiple methods
 - Obvious purcheck replay
 - 30-second disarm



Making a Flowchart

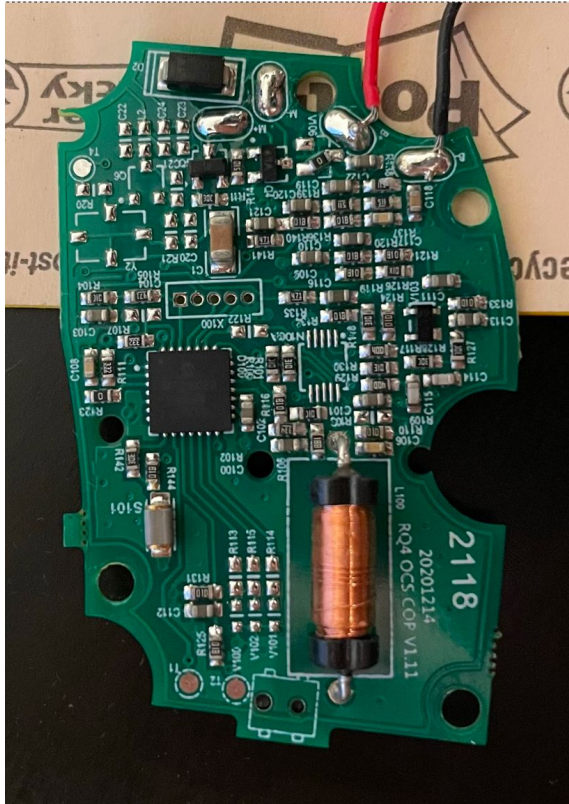
- Lets us map out different states and actions
- Makes potential bypasses easier to see
 - Want to get back to IDLE without locking at door
- Sometimes multiple methods
 - Obvious purchek replay
 - 30-second disarm
 - Manually force a lock cycle



Speculation Time

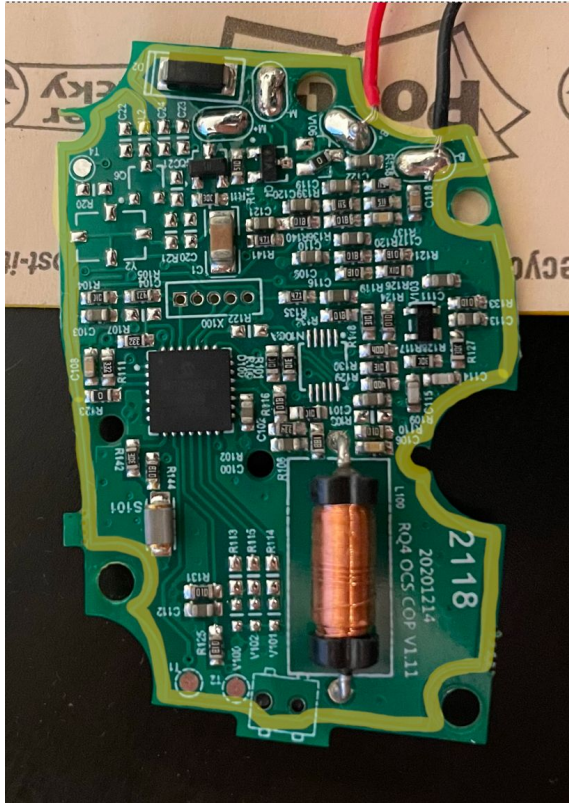
Sometimes the best we can do in reverse engineering.

But what about 2.4 GHz?



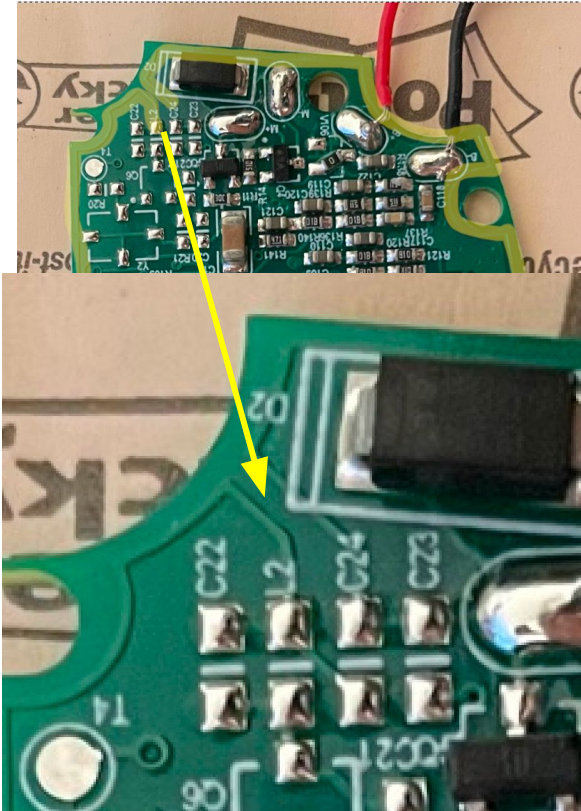
- Documentation and FCC filings indicate 2.4 GHz communication
- Checkout unit sends 2.4 GHz signal
- PIC18 process does not have transceiver built in
- Likely antenna on PCB, but not connected
- Antenna feeds and unused lines (likely serial or other chip-to-chip) support this

But what about 2.4 GHz?



- Documentation and FCC filings indicate 2.4 GHz communication
- Checkout unit sends 2.4 GHz signal
- PIC18 process does not have transceiver built in
- Likely antenna on PCB, but not connected
- Antenna feeds and unused lines (likely serial or other chip-to-chip) support this

But what about 2.4 GHz?



- Documentation and FCC filings indicate 2.4 GHz communication
- Checkout unit sends 2.4 GHz signal
- PIC18 process does not have transceiver built in
- Likely antenna on PCB, but not connected
- Antenna feeds and unused lines (likely serial or other chip-to-chip) support this

And the mystery chip?

If I had to guess:

- Probably the accelerometer
 - Low-power on-motion interrupt functions are common features
 - Basic motion can be
- Could also be a SOC handling 2.4 GHz/ kHz range signal processing
 - Probably handled by unpopulated footprint we used for fly wires

Thanks and shout outs!

- My dad for bringing these wheels to my attention
- DEFCON staff and goons for letting me ramble about shopping carts on stage again
- All my friends and loved ones who have supported my shenanigans
- The makers of audacity, URH, Ghidra, and all the other tools used
- Those random Ebay sellers



References

- - The ARRL handbook for radio communications, 2007. Newington, CT: American Radio Relay League, 2006. Print.
- - /r/rfelectronics
- -FCC.gov
- - My previous talk at DEFCON 29 (“DoS Denial of Shopping Analyzing and Exploiting Physical Shopping Cart”)
- - rocateq.com

Q&A

Come check out the demo booth in the Physical Security Village in the Flamingo!

Contact me:

Twitter @stoppingcart

joseph@begaydocrime.com

Control carts with begaydocrime.com/carts

