Hacking electric skateboards: vehicle research for mortals

Richo Healey & Mike Ryan

Who are these jerks anyway

- richo
- Computer Jerk
- @rich0H
- Duck Enthusiast
- Ran WrongIslandCon

- mike
- Bluetooth Guy
- @mpeg4codec
- Owner/Operator of conscience (sometimes)

Why buy an $nK skateboard?

- Lightweight
- (relatively) inexpensive
- .. maybe wanted on the hype train early

Why buy an $nK skateboard?

- Lightweight
- (relatively) inexpensive
- .. maybe wanted on the hype train early
- Maybe to hax it

Why hax a $1k skateboard?

- Because it’s there
- Vehicle research is cool
    - But not all of us can afford to brick a car
- Figured we might be able to illustrate a point about the state of security research

The boards

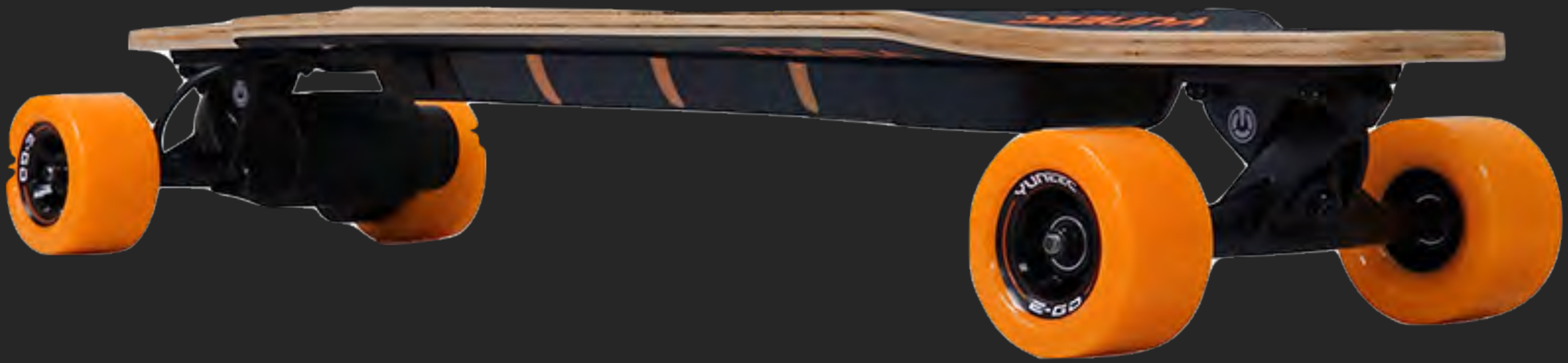
- Boosted

The boards

- Evolve

The boards

- Yuneec E-go



Maybe you’ve spotted the design trend here

Agenda

Hope yer wearin' yer lernin' b00tz

- Boosted
  - Bluetooth GATT
  - Jammers
    - PyBT
- Evolve
  - … bluetooth?
  - Weird RF protocols
- E-go
  - … wifi?!
- Boosted (Redux)
  - Fiiiiiirmware!

Right so like hacking

Or whatever

- Most of these boards use bluetooth
- I know nothing about bluetooth

- I know mike though
- mike knows bluetooth
- How hard can this possibly be?

Boosted

Boosted

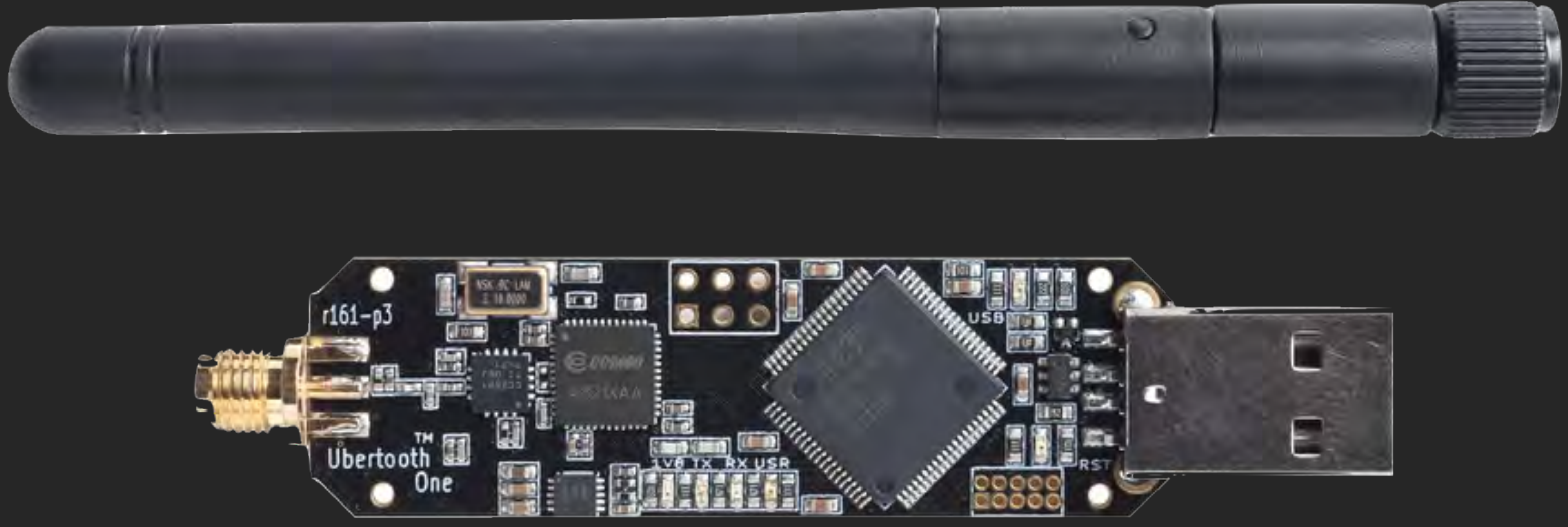
- Bluetooth Remote
- Regenerative Braking
- Firmware Upgradable

Storytime

Bluetooth and You

Co-opting a GATTling gun

- Bought some uberteeth



- Looked at some packets
- Now what?

Bluetooth and You

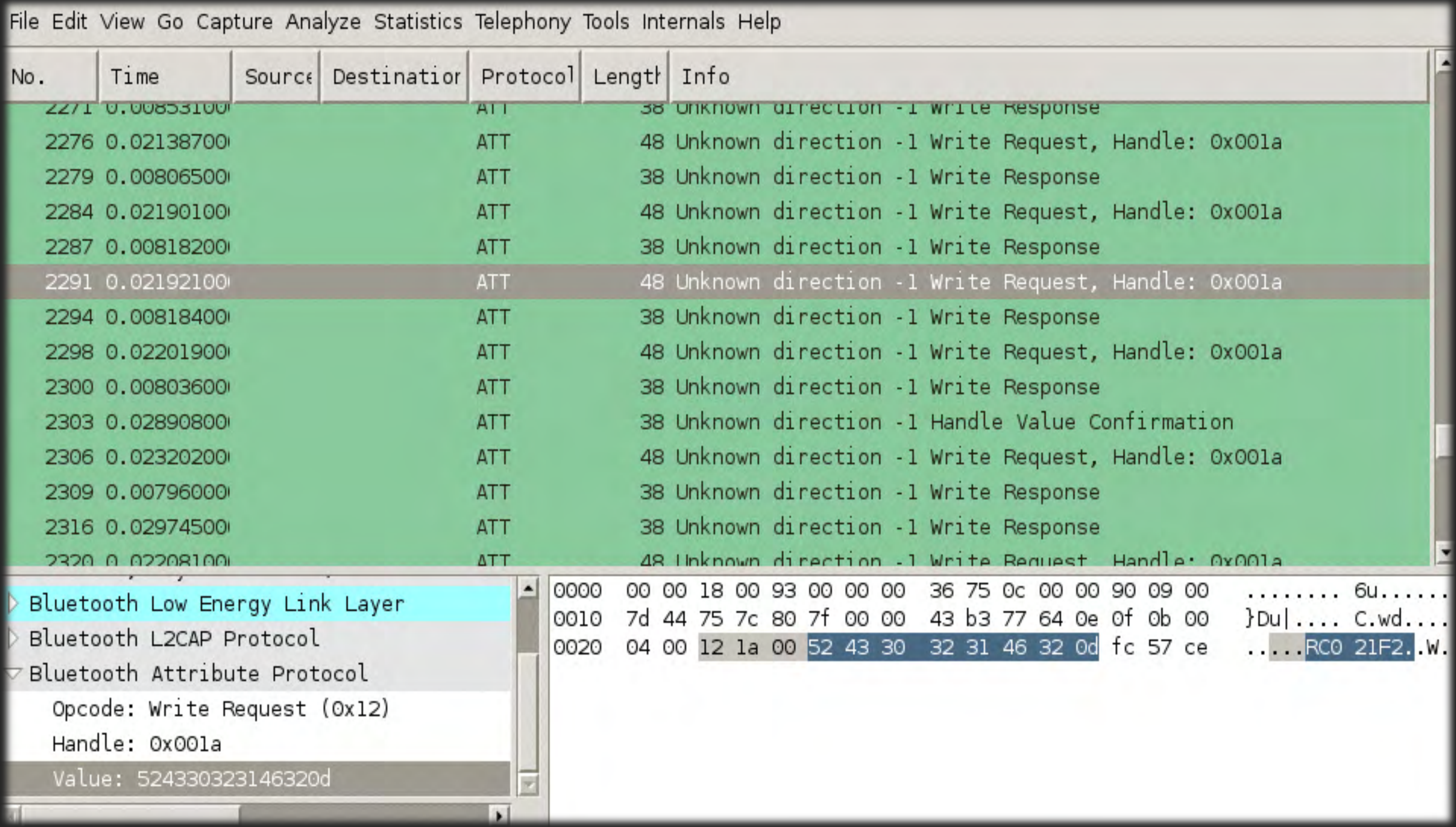
- Modern bluetooth supports some crypto
- Using it would have made our lives annoying
- No crypto though
  - Go team!

GATT

A clever pun about gatt

- Handle-wise communication
- Supports either request-response or datagram like
- Sits on BLE

Looks like dis


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

```
No.    Time       Sourc  Destinatio  Protocol  Lengt  Info
2271 0.00853100              ATT        38 Unknown direction -1 Write Response
2276 0.02138700              ATT        48 Unknown direction -1 Write Request, Handle: 0x001a
2279 0.00806500              ATT        38 Unknown direction -1 Write Response
2284 0.02190100              ATT        48 Unknown direction -1 Write Request, Handle: 0x001a
2287 0.00818200              ATT        38 Unknown direction -1 Write Response
2291 0.02192100              ATT        48 Unknown direction -1 Write Request, Handle: 0x001a
2294 0.00818400              ATT        38 Unknown direction -1 Write Response
2298 0.02201900              ATT        48 Unknown direction -1 Write Request, Handle: 0x001a
2300 0.00803600              ATT        38 Unknown direction -1 Write Response
2303 0.02890800              ATT        38 Unknown direction -1 Handle Value Confirmation
2306 0.02320200              ATT        48 Unknown direction -1 Write Request, Handle: 0x001a
2309 0.00796000              ATT        38 Unknown direction -1 Write Response
2316 0.02974500              ATT        38 Unknown direction -1 Write Response
2320 0.02208100              ATT        48 Unknown direction -1 Write Request, Handle: 0x001a
```

```
▷ Bluetooth Low Energy Link Layer
▷ Bluetooth L2CAP Protocol
▽ Bluetooth Attribute Protocol
    Opcode: Write Request (0x12)
    Handle: 0x001a
    Value: 524330323146320d
```

```
0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 90 09 00   ........ 6u......
0010  7d 44 75 7c 80 7f 00 00  43 b3 77 64 0e 0f 0b 00   }Du|.... C.wd....
0020  04 00 12 1a 00 52 43 30  32 31 46 32 0d fc 57 ce   .....RC0 21F2..W.
```

… many beers later

painstakingly reversed with love

- Simple Duplex protocol
- Controller sends on handle 0x1a
- Reads on handle 0x1c

- Basically a bluetooth -> serial adaptor

… many beers later

painstakingly reversed with love

Message	Direction	Meaning
RC0	Remote -> Board	Speed control
FUEL	Remote -> Board	Fetch current battery load
REXP	Remote -> Board	Set expert mode
RBGN	Remote -> Board	Set beginner mode
GAUGE[1-5]	Board -> Remote	Inform current battery load

We know its language

but how 2 talking?

- Bluetooth comms turn out to be sorta miserable
- Especially for general purpose applications
    - x10000 for ad-hoc, general purpose applications

The old school

- Ubertooth
    - “minimal”
- BlueZ
    - Full featured, but heavy
    - Not super fond of doing obviously broken things
        - (Like fuzzing embedded devices)

PyBT

Welcome to the new school

- Userland bluetooth stack implemented in Python
- Backs onto scapy for actually talking to the wire
- Uses HCI_CHANNEL_USER
- Prototyping++

- https://github.com/mikeryan/PyBT

Neat we can spin the wheels

Now what

- Need to be connected to the board to exploit
- Only one thing can be connected at a time
  - Thinking back to that intersection

- richo demonstrates again that he has no idea:
  - “How hard can jamming bluetooth be?”

Jamming bluetooth:

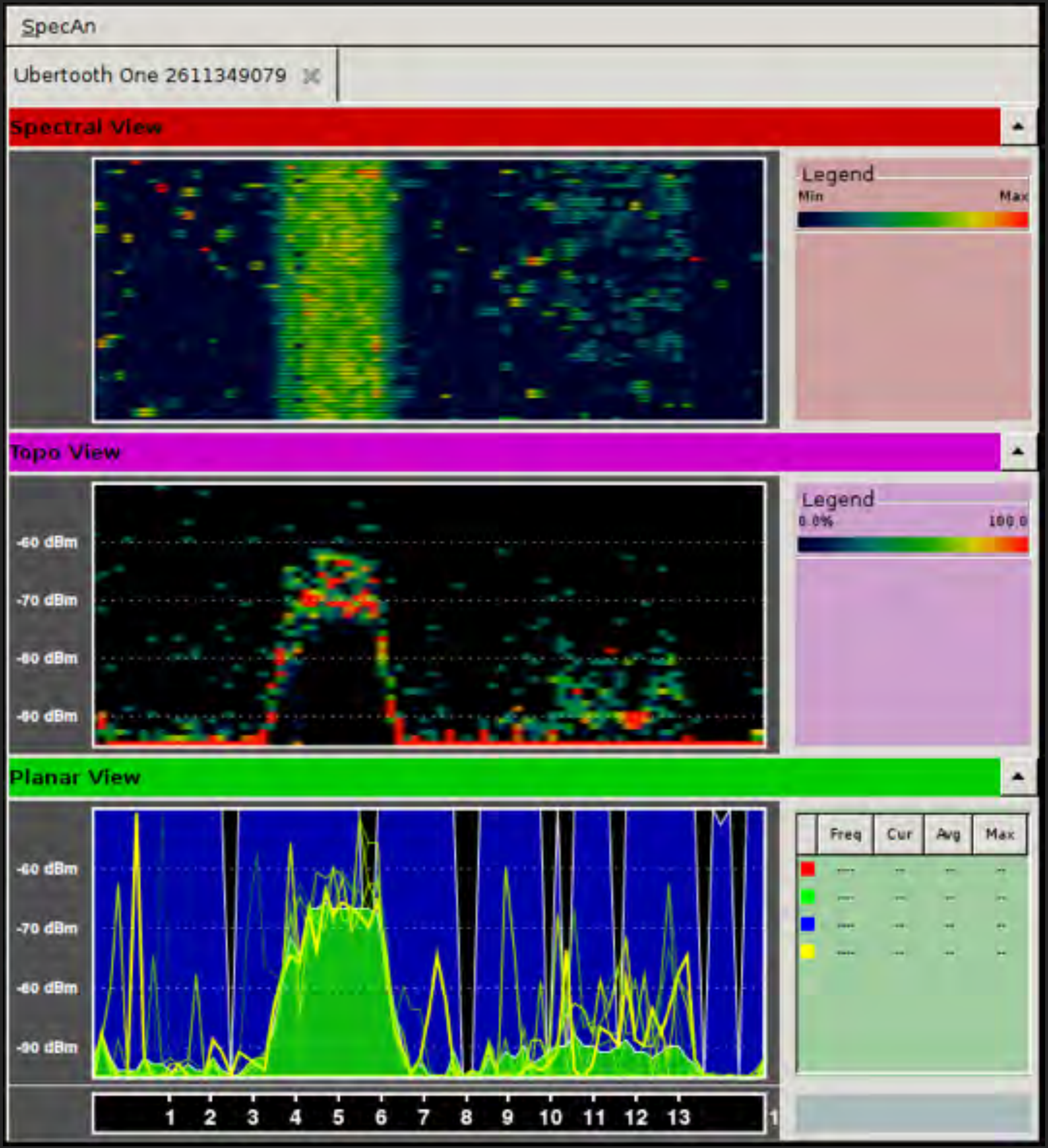
Super hard, it turns out

- Naive approach:
    - Yell really loud
    - Noone can hear anything
    - ??????
    - Profit…..?

What could possibly
go wrong?

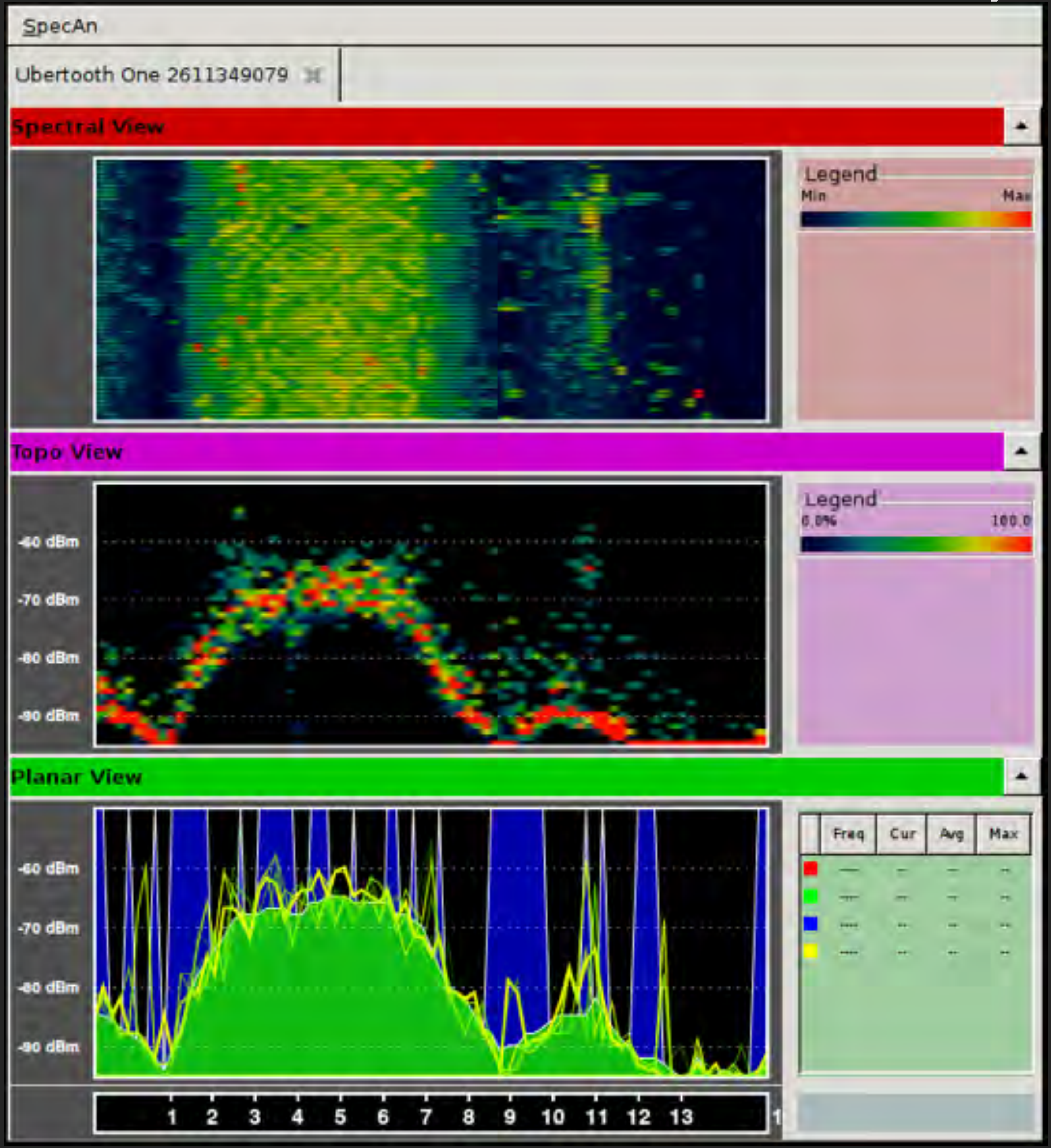
Jamming bluetooth:

Super hard, it turns out



Jamming bluetooth:

Super hard, it turns out



Jamming Bluetooth

Seriously like crazy hard

- It’s like they designed the protocol itself to stop us from doing this exact thing
  - By this point richo is no longer allowed to make suggestions

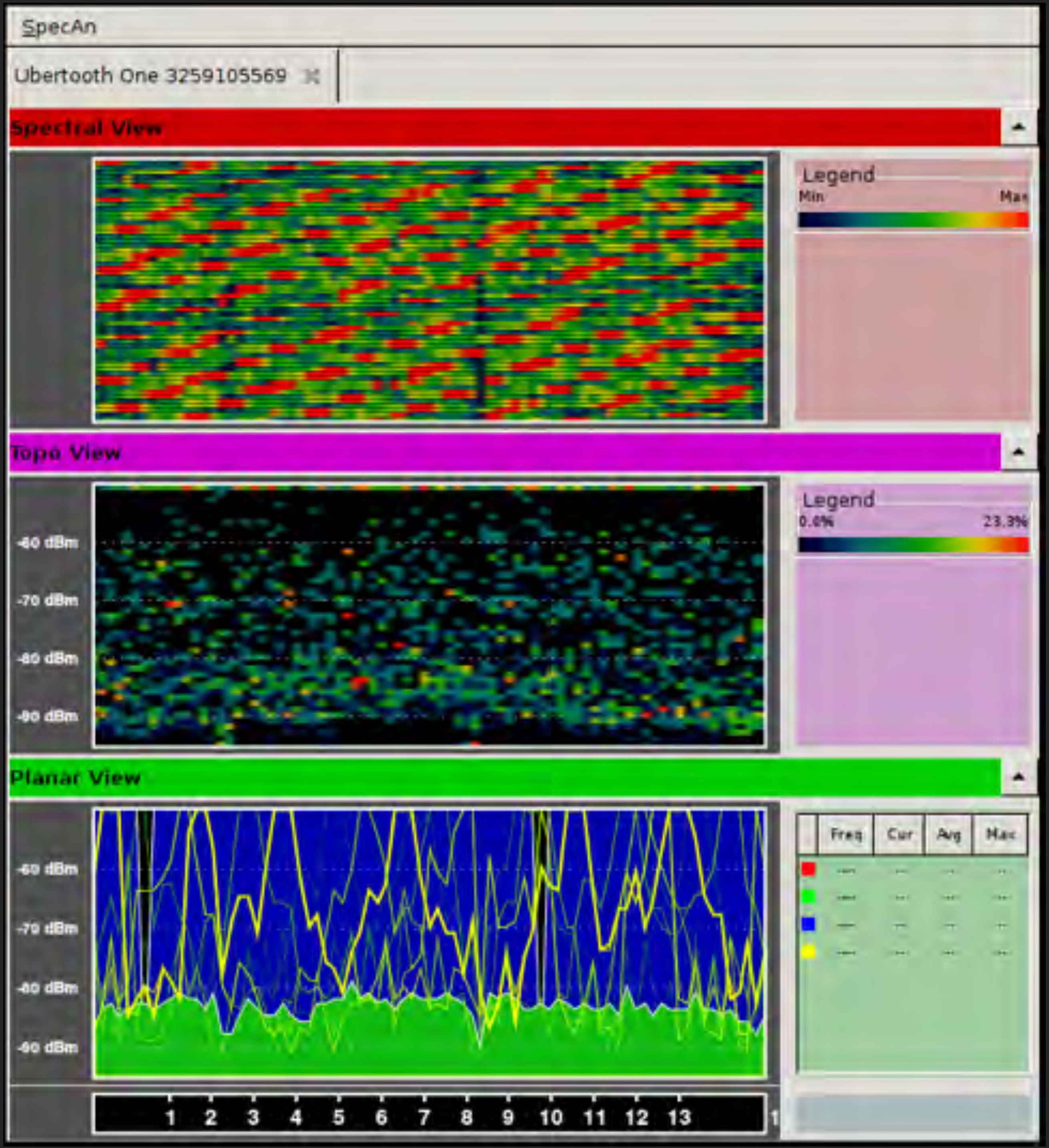
Jamming Bluetooth

Seriously like crazy hard

- Bluetooth’s channel hopping stops us from jamming effectively
- Channel hopping is deterministic
- Need some state- Gotta capture:
  - Access address
  - Hop interval
  - Hop increment

Jamming Bluetooth

Seriously like crazy hard



Upstreamed: https://github.com/greatscottgadgets/ubertooth

Demo Time!

Time to launch some jerks

- The plan:
  - Setup a bunch of jammers
  - Configure our repl to connect and autoreverse throttle
  - Wait for hapless skateboarder
  - Jam
  - Connect
  - Reverse
  - ?????
  - Launch some jerk

Demo Time!

Time to launch some jerks

He’ll be like:

Demo Time!

Time to launch some jerks

And we'll be like:

Demo Time!

Time to launch some jerks

Followup

Boosted Response: not-horrible/10

- Reported to Boosted before Kiwicon last year
- Shaky start
- Wound up working with us
- Implemented a fix! (kinda)

Evolve

Evolve

- Says bluetooth on the site
  - Spoilers: This is not a True Fact™
- Better range than boosted
- Janky looking remote
- Made of carbon though?
  - So that's neat I guess
  - ¯_(ツ)_/¯

Evolution

- It says bluetooth right there on the tin
- We’re crazy cocky at this point
- “We oughta have this done by lunch”

Evolution

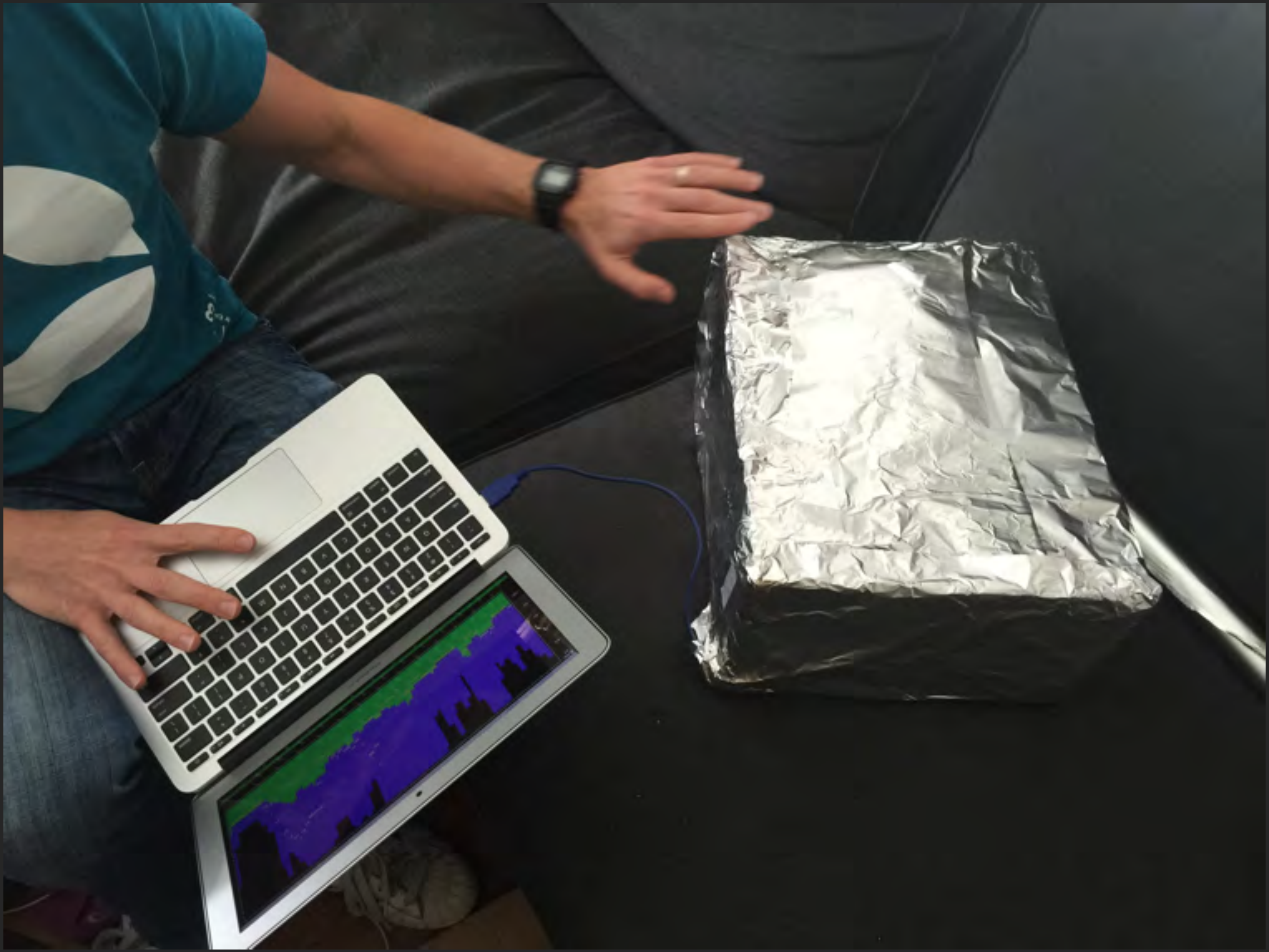
- Pull out the harness we used on Boosted

Evolution

- No packets this time :(
- richo is a goddamn hipster and lives in SF
- goddamn hipsters in SF love wifi/bt
- richo's apartment might be the RF noisiest environment in the whole universe

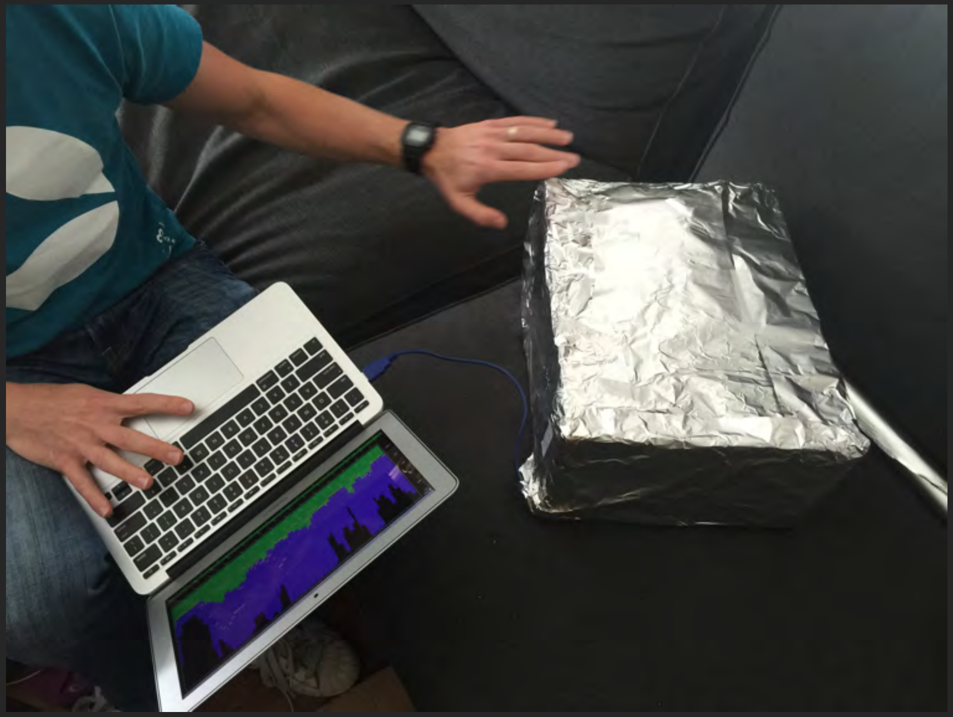
- The moratorium on richo giving advice has expired by this point
- "We'll build a faraday cage!"

Evolution



Evolution

- Snowboard bindings box wrapped in tinfoil
- Works terrifyingly well
- Seriously wtf tho where's the bluetooth



Evolution

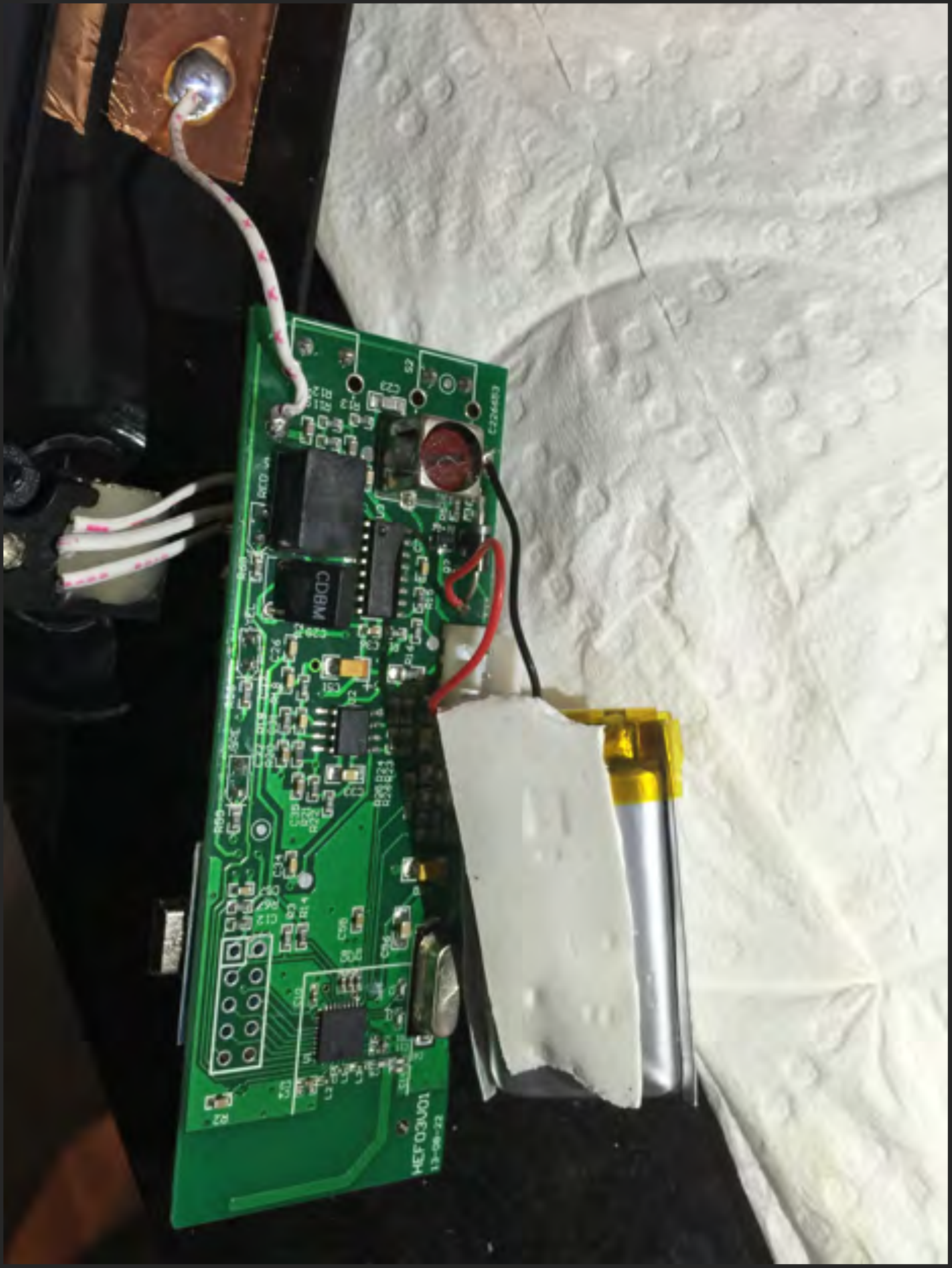
- merijn very kindly lent us his skateboard
- We should probably pull it to pieces and look at it
- Unclear if we ever mentioned that we were going to do this or that we did

- (Hi Merijn btw we pulled apart your skateboard)

Evolution

- Pulled the remote apart
- Looked up the rf part
- er, this is not a bluetooth chip

- Neither of us have even heard of this thing
- nRF24LE



Evolution

- Talks PowerThirst™

POWERTHIRST
POWERTHIRST
www.pi[illegible]cfa[illegible]com

POWERTHIRST
POWERTHIRST
CollegeHumor
GIFSOUP.COM

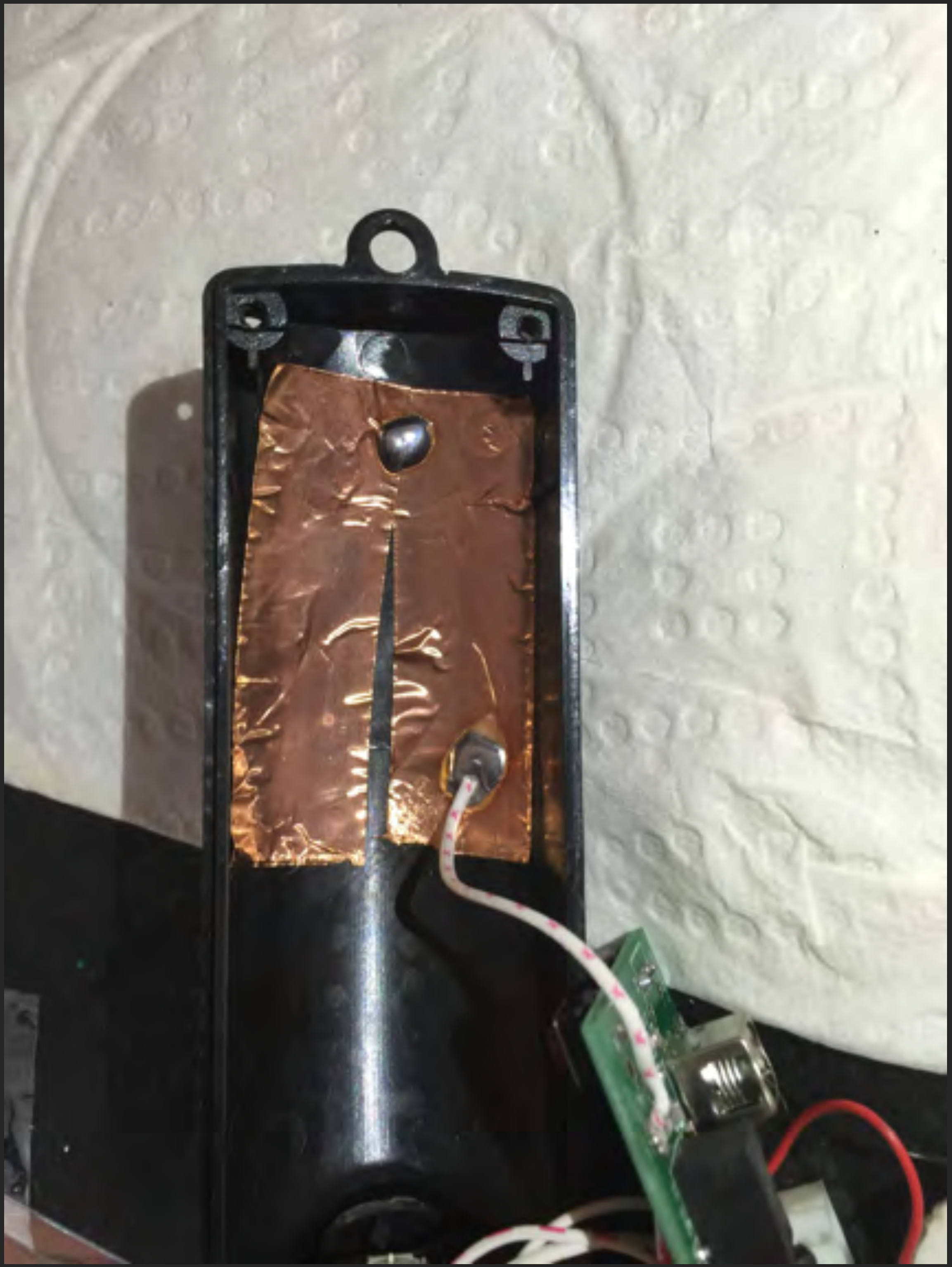
Evolution

- Er, ShockBurst™

Evolution

- WTF is this thing?

- Antennae?
- Way too big for 2.4ghz

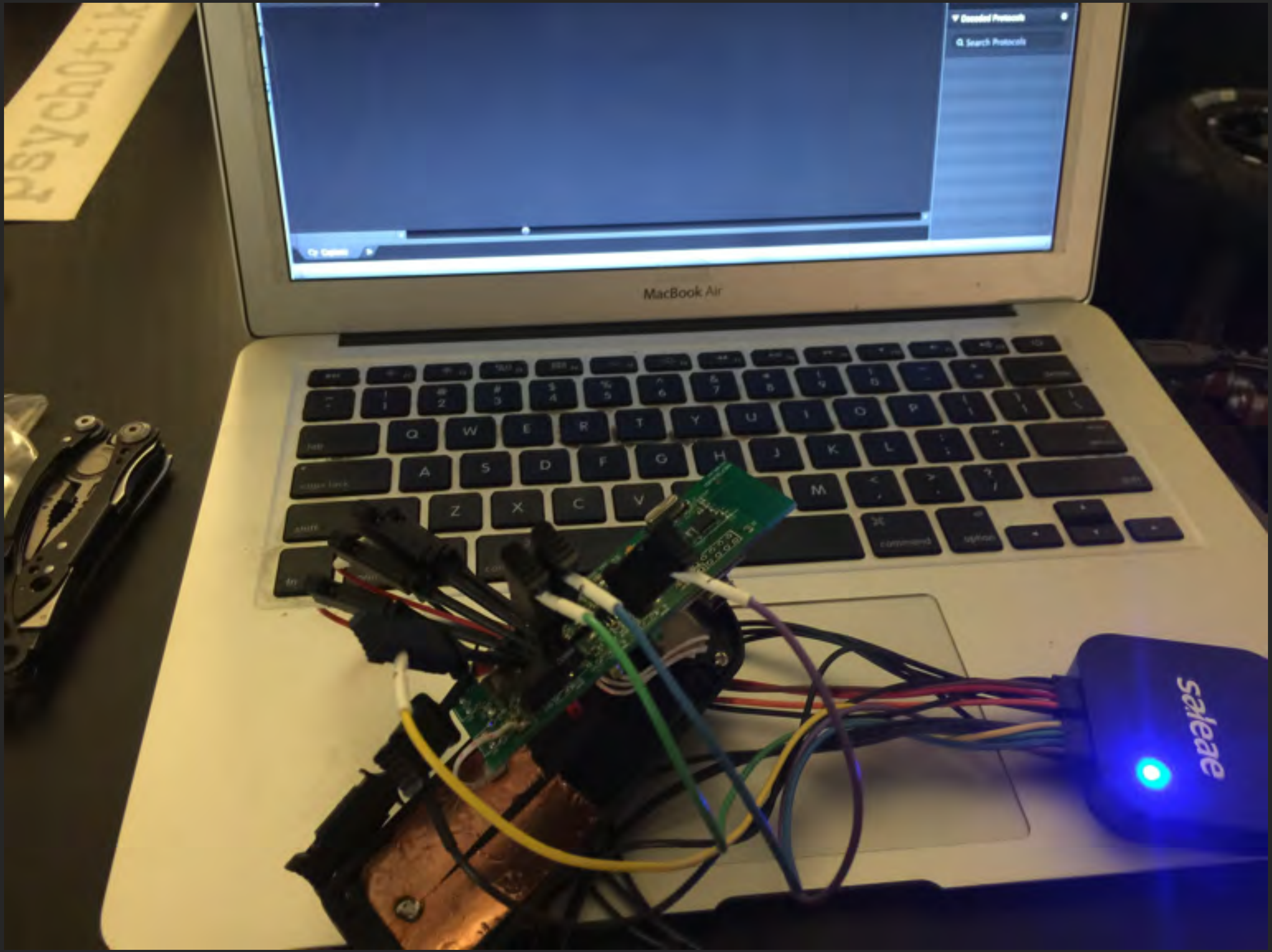


Evolution

- No obvious path to glory
- No hackRF at my place
- Can’t fiddle with its radio today
- Let’s just dump traffic directly

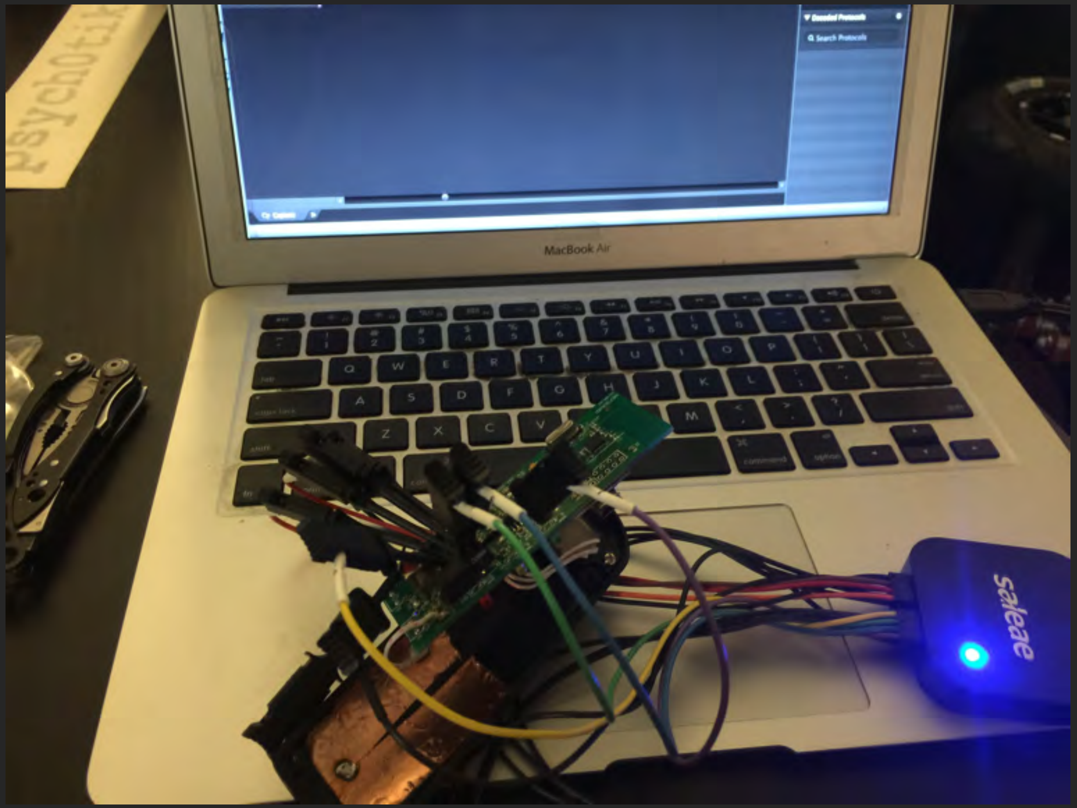
- Hey didn’t I impulse buy a saleae a while ago?

Evolution


psych0tik
Decoded Protocols
Search Protocols
MacBook Air
saleae

Evolution

- Dumped everything
- Nothing terribly interesting looking
- ¯_(ツ)_/¯



Evolution

- No dice on the remote
- Let’s fiddle with the board instead!

- (Hi Merijn)

Evolution

- Cramped AF
- Traced most of it out though
- Off the shelf parts
- Explained a bunch of hilarious bugs

Evolution

- ShockBurst is simplex
  - Hence no data to the remote
- Not especially complex
- Does have a 9 member bitfield though to make our lives miserable
- Less tolerant to interference than BT

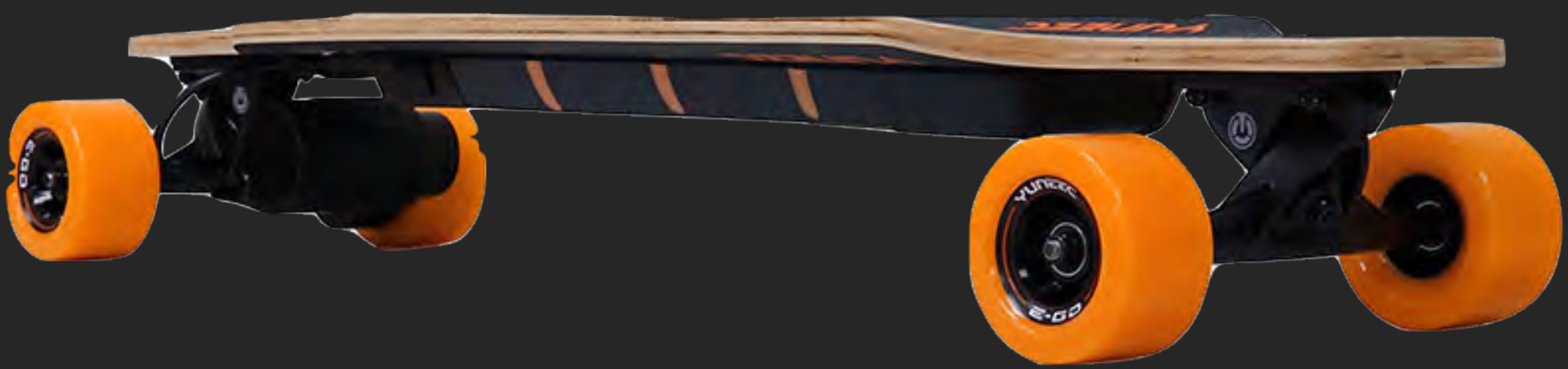
Demo Time!

- Inject packets into evolve
- ????
- Profit!

Evolution

- Sadly not much else to do here
- Outside of "Attacker has physical access" scenarios there's not much to attack

E-go



Taming a wild ego

- Says bluetooth all over it
- Has a smartphone app
- Has to be bluetooth right?

Taming a wild ego

- Didn’t take a good photo :(
- Sadly it can’t actually drive an ubertooth (yet?)
- Sniffed a lot of bluetooth

- No packets again
- WTF?

Taming a wild ego

- WTF is this switch on the side?

- BT|WIFI
- … no
- … … NO

Taming a wild ego

- Yup this damn thing talks bluetooth *and* wifi
- Paired with a phone it's bluetooth
- Paired with the remote it's wifi

Demo: pwning ego

Boosted: Redux

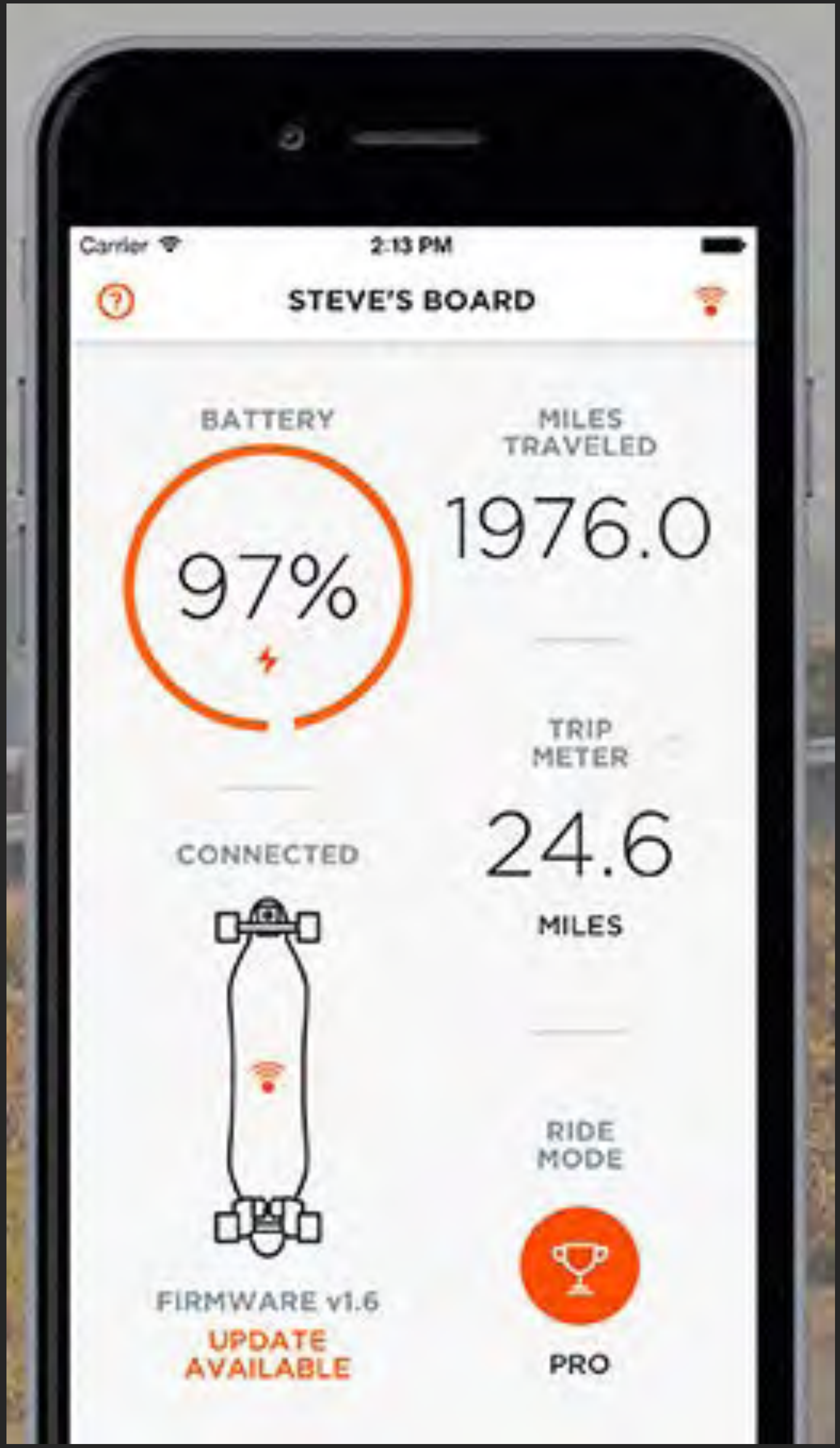
Persistence

Remote code execution on a skateboard, you say?

- From pulling the board apart we knew it was a pic24f
- Didn’t have much luck initially trying to find debug ports on the skateboard
- Later discovered that we missed them
- A few months later though, this happens:

Persistence

Remote code execution on a skateboard, you say?



STEVE'S BOARD

BATTERY
97%

MILES TRAVELED
1976.0

TRIP METER
24.6
MILES

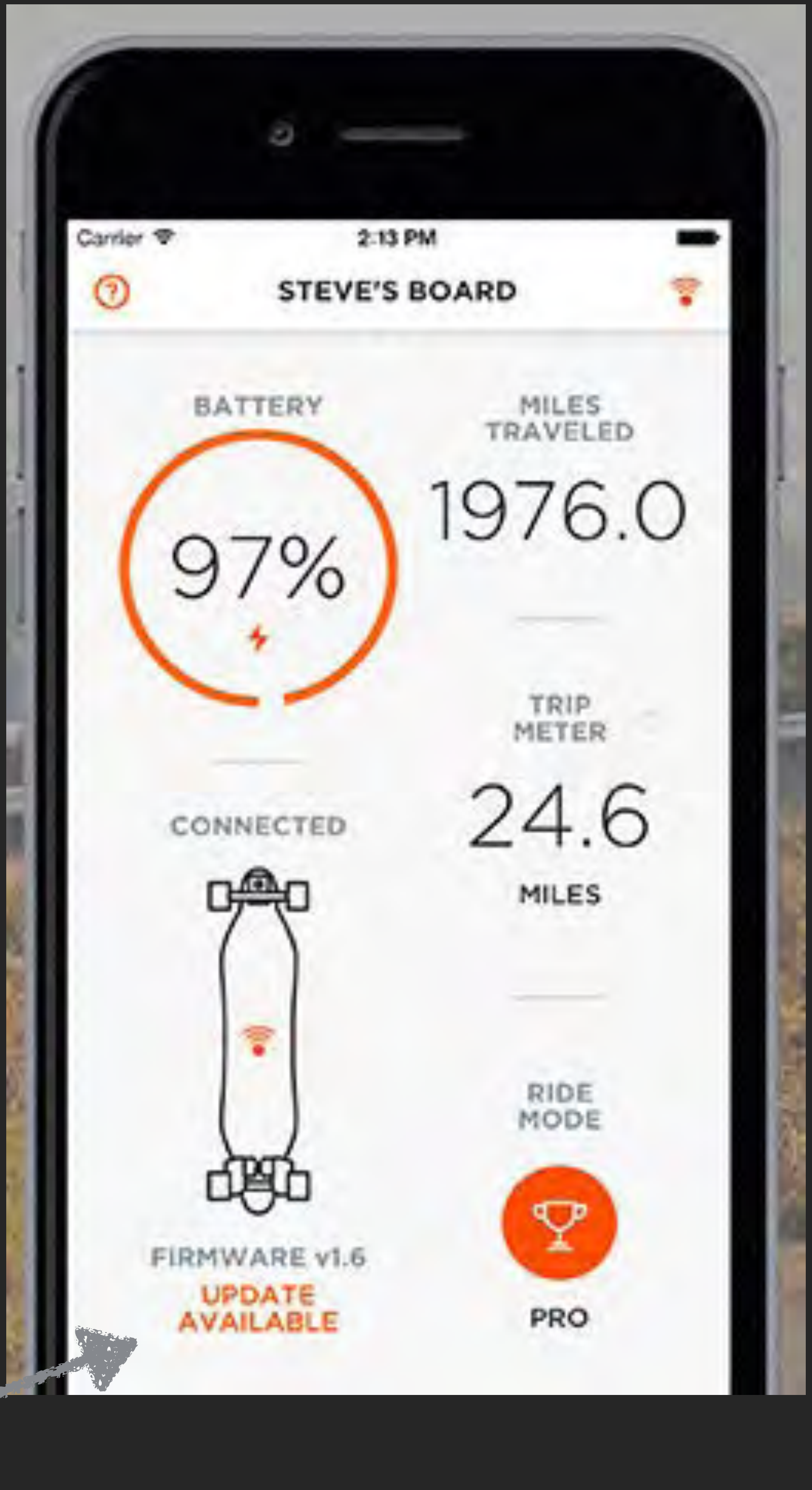
CONNECTED

RIDE MODE
PRO

FIRMWARE v1.6
UPDATE AVAILABLE

Persistence

Remote code execution on a skateboard, you say?



Carrier 2:13 PM

STEVE'S BOARD

BATTERY

97%

MILES TRAVELED

1976.0

TRIP METER

24.6

MILES

CONNECTED

RIDE MODE

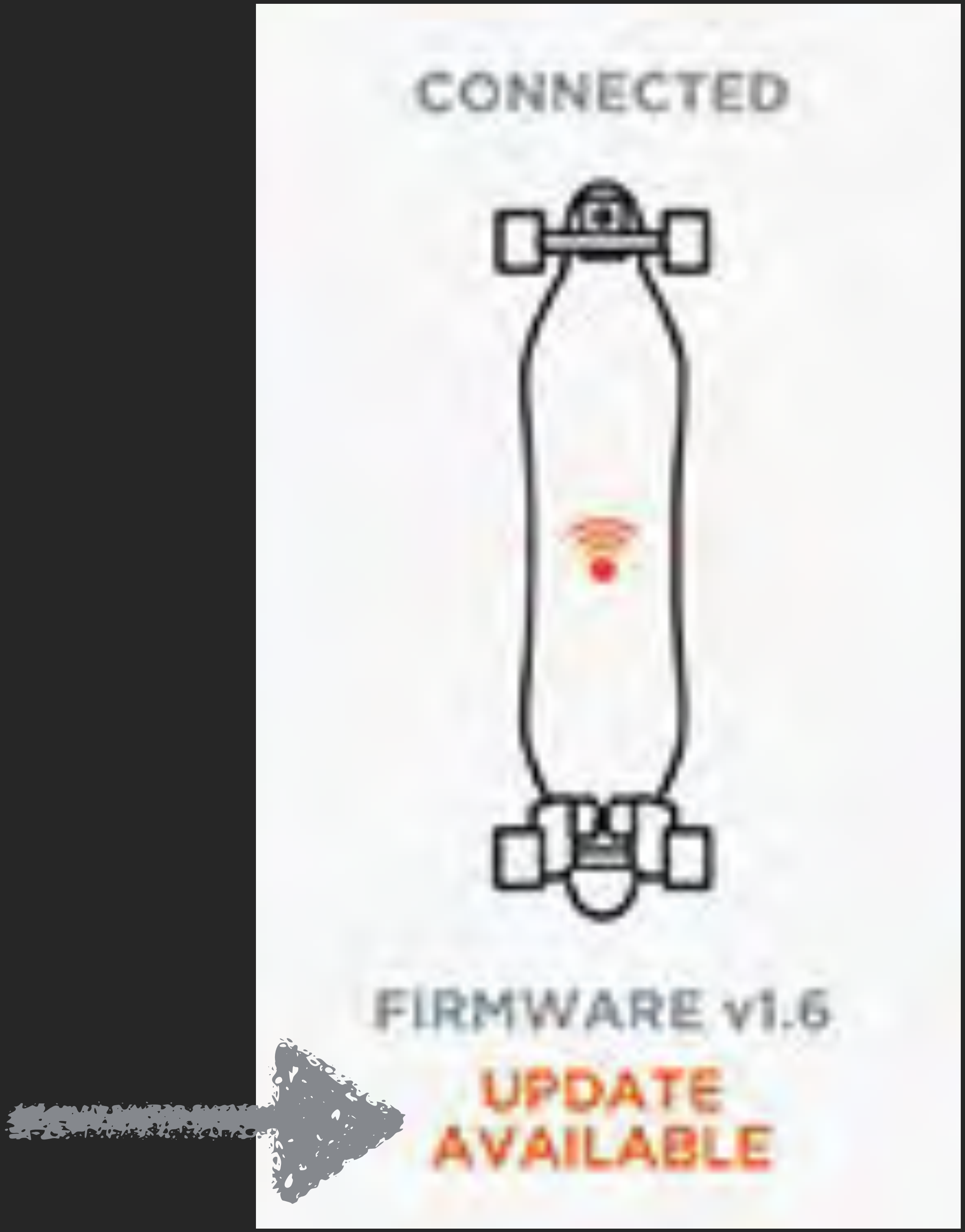
FIRMWARE v1.6

UPDATE AVAILABLE

PRO

Persistence

Remote code execution on a skateboard, you say?



CONNECTED

FIRMWARE v1.6

UPDATE AVAILABLE

Persistence

Remote code execution on a skateboard, you say?

- Has a firmware update facility
- This oughta be good

- Upgrade one of our boards
  - Dump bluetooth traffic with jailbroken iThing
  - Dump https traffic with burp

- Both sides of the conversation, hopefully we learn how to upload + format firmware

Persistence

RCE on a skateboard, you say?

- many hours later we’ve stitched a firmware blob together out of the dumps
- Strings are encoded as, eg:
    - “F\x00U\x00\E\x00L\x00” => “FUEL”
- Write a dumb python script to strip nulls, strings(1) to the rescue

- Learn about a bunch of new commands!

… many many beers later

painstakingly reversed with love

Message	Direction	Meaning
RC0	Remote -> Board	Speed control
FUEL	Remote -> Board	Fetch current battery load
REXP	Remote -> Board	Set expert mode
RBGN	Remote -> Board	Set beginner mode
GAUGE[1-5]	Board -> Remote	Inform current battery load
PING	Remote -> Board	Fetch version information
GIT	Remote -> Board	Fetch git revision of firmware
STAT	Remote -> Board	Fetch detailed diagnostic info
NUMSKL	Remote -> Board	Still no idea. Replies "NUMSKL4"
ODO	Remote -> Board	Fetch current odometer reading
SOC	Remote -> Board	Still no idea

Persistence

RCE on a skateboard, you say?

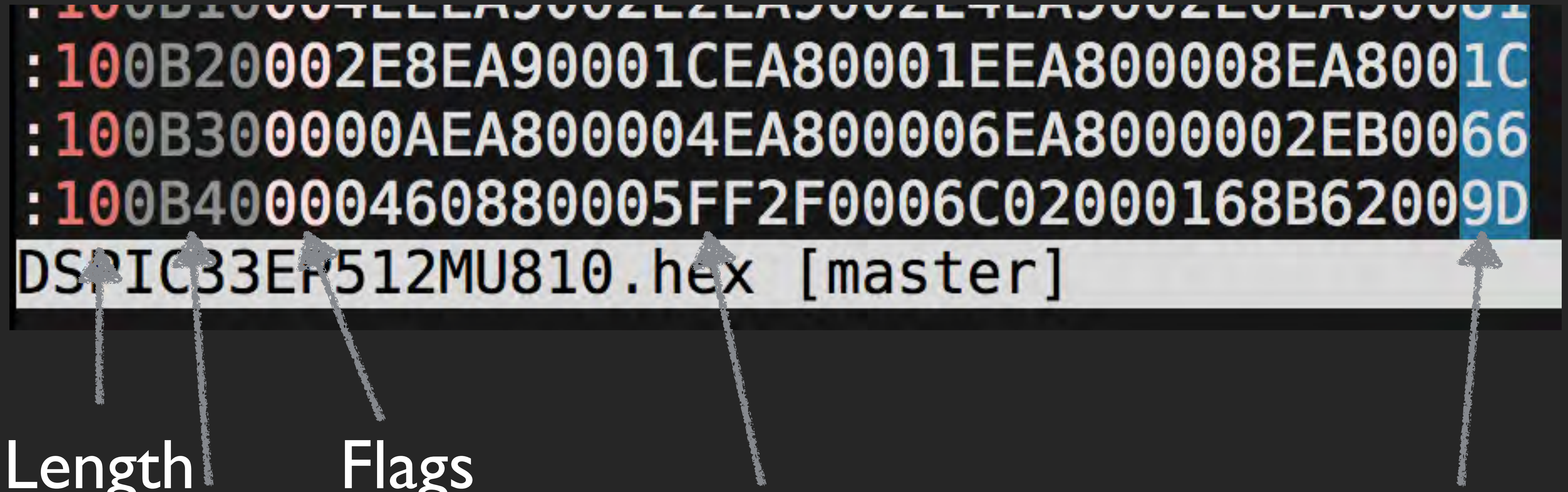
- With this in hand, richo writes a repl for boosted boards
- Nico works out how to unbrick a skateboard when we inevitably screw this up

- https://github.com/richo/skateboard/blob/master/boosted_repl.py

Persistence

RCE on a skateboard, you say?

- Finally, it’s time to reverse the transfer protocol
- Winds up like intel .hex over bluetooth



```
:100B20002E8EA90001CEA80001EEA800008EA8001C
:100B300000AEA800004EA800006EA8000002EB0066
:100B4000004608800005FF2F0006C02000168B62009D
DSPIC33EP512MU810.hex [master]
```

Length

Address

Flags

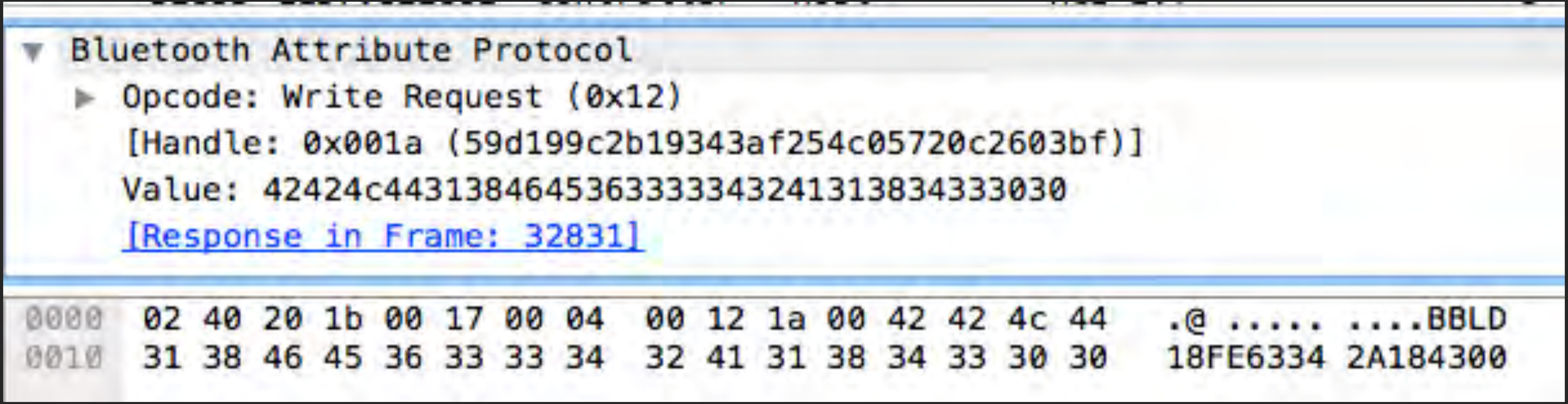
Data

Checksum

Persistence

RCE on a skateboard, you say?

- Becomes:



```
▼ Bluetooth Attribute Protocol
  ▶ Opcode: Write Request (0x12)
    [Handle: 0x001a (59d199c2b19343af254c05720c2603bf)]
    Value: 42424c4431384645363333343241313834333030
    [Response in Frame: 32831]
```

```
0000  02 40 20 1b 00 17 00 04  00 12 1a 00 42 42 4c 44   .@ ..... ....BBLD
0010  31 38 46 45 36 33 33 34  32 41 31 38 34 33 30 30   18FE6334 2A184300
```

Persistence

RCE on a skateboard, you say?

- What do you even *do* with code execution on a skateboard?
- Could definitely make the board dangerous to its rider
- Seemed funnier to make it pretend to be Joshua from WARGAMES

Demo Time!

In which we make a $2k paperweight

Gr33tz and Th4nx

These jerks are alright

- nico, who showed up at the last second and helped us hax firmware, is an Arduino Uno expert
- merijn for lending us his evolve despite it obviously being a Bad Idea
- whatever chump bought the e-go at the auction

- Boosted
- Evolve
- Yuneec