# Wardriving 102: Moving Beyond the Wigle App

Compilation and lessons learned when building custom wardriving hardware.

Bryan Kobe, @kobeski1906, github.com/bkobe

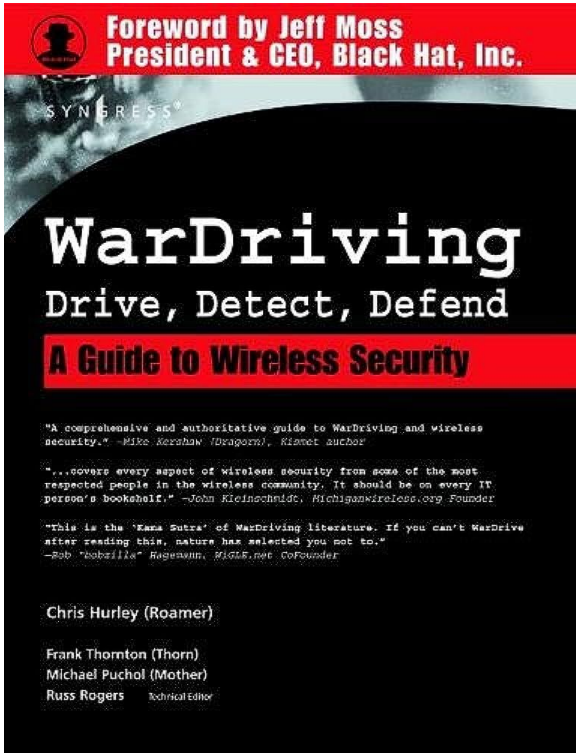
# About Me

- EE degree, focusing in analog/digital circuit design, microcontroller/microprocessors, and wireless/optical electronics.
- Hobbies in ham radio: Radios and repeater infrastructure (tower sites). Own and operate analog/DMR repeaters for general and ARES/RACES use.
- Recent work in software-defined radios and radio mesh networks.
- Member of the Hardhat Brigade (@hardhatbrigade)

# What is wardriving?

- Started as a grass-roots movement to find and log all free/public wifi.  Goal is to map out wireless SSIDs and where you saw them at.

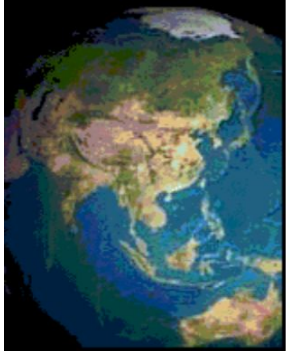
- Part 1 of the RF Hackers Sanctuary Capture the Flag - the World-wide War Drive (WWWD).  Pick a gridsquare, find new wifi, rediscover old ones, get imaginary points at the CTF.
  - A simple android phone is enough to participate running the wigle app. Some phones are better than others.  Most are low cost off ebay
  - Being all in one (wifi, GPS, battery, and screen) are very capable at collecting SSIDs as well as cell towers.



# Wigle and wigle.net

- Aggregating many of many wardriver's datasets into a common service. What started as a pet project, now reached its billionth AP mapped.
- Finding usable network ("Free Net" search)
- Educating the public
- Research projects
- A fun hobby - leads to unique ways beyond The wigle app for collecting information and gain those imaginary points.


"Hackers armed with laptops" are looking for unprotected networks…
***We are making statistical analysis of ALL wireless networks, not just "unprotected" networks***
- C. Hurley/Roamer from DC11 talk

# The First WorldWide WarDrive

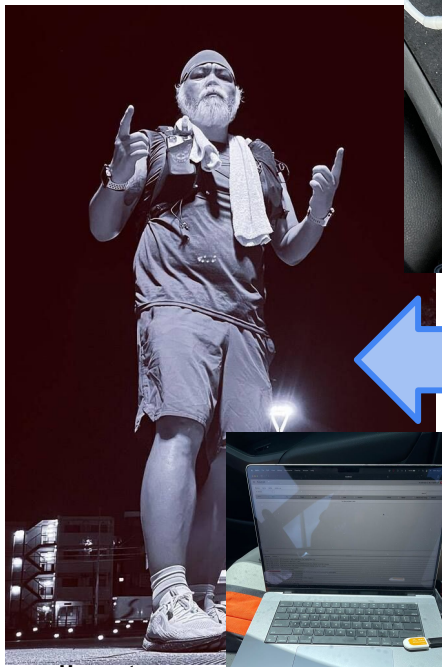
| CATEGORY | TOTAL | PERCENT |
|---|---|---|
| TOTAL APs FOUND | 9374 | 100 |
| WEP Enabled | 2825 | 30.13 |
| No WEP Enabled | 6549 | 69.86 |
| Default SSID | 2768 | 29.53 |
| Default SSID and No WEP | 2497 | 26.64 |
| Unique SSIDs | 3672 | 39.17 |
| Most Common SSID | 1778 | 18.97 |
| Second Most Common SSID | 623 | 6.65 |

Excerpt from Roamer's DC11 talk. First WWWD was 31 AUG to 7 SEP 2002

# Subculture of Wardriving: the Hardware Rig Builds

- Moves beyond the app to custom hardware and software for more radios and features. Each rig has a goal and a story.
- “Bigger” rigs with more hardware capture more, but also aren’t as portable.
- Most using modern linux (Pi/PC) run kismet to do all the software and logging.
  - General rule of thumb is 10 mph per datasource when frequency hopping
  - GPS dongle or card to get time and position (using gpsd)
- Now, not only PC/Pi-based, but moving into microcontrollers using the ESP32/ESP8266.

# Hardware Rigs - Finding a place on the spectrum



elkentaro


aromond

lozaning

w4www raker

d4rkm4tt3r

Simpler

More complex

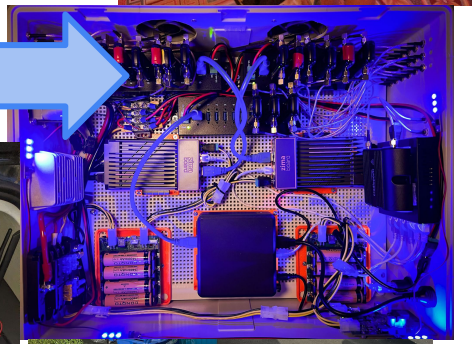


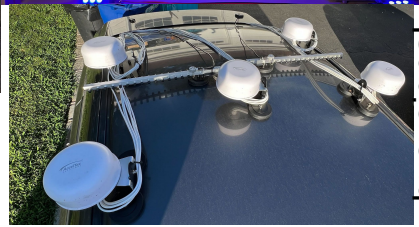
n00bz

CoD_Segfault

syntax976

PanicAcid





busysignal

https://github.com/rfhs/rfhs-wiki/blob/master/pages/DEFCON-30-WWWD-RIGS.md

# Design Brainstorm and Capabilities

- Portability: Drive, bike, walk in a good form factor
- Power: several hours of runtime, redundant
- Multiple radios and configurable options
  - More than a wigle phone, but less than the big rigs
  - Potential for other sources (802.15.4 and SDR) in kismet
- Compute: RPis work well in small form factors
  - USB 2 and 3: for radios (wifi, bluetooth, 802.15.4, SDR, GPS?)
  - GPIO: GPS, PPS, timing

Need to spread apart the USB ports for radio antennas

Water bottle / tennis ball tubes work fairly well to also keep electronics safe.

# Cabling/Radio Issue: USB 3.x

- Depending on radio and cable used, USB 3 can cause electromagnetic interference on GPS.
- As with all EMI, you can mitigate by separating the emitter (USB cable) and victim(s) (GPS antenna)

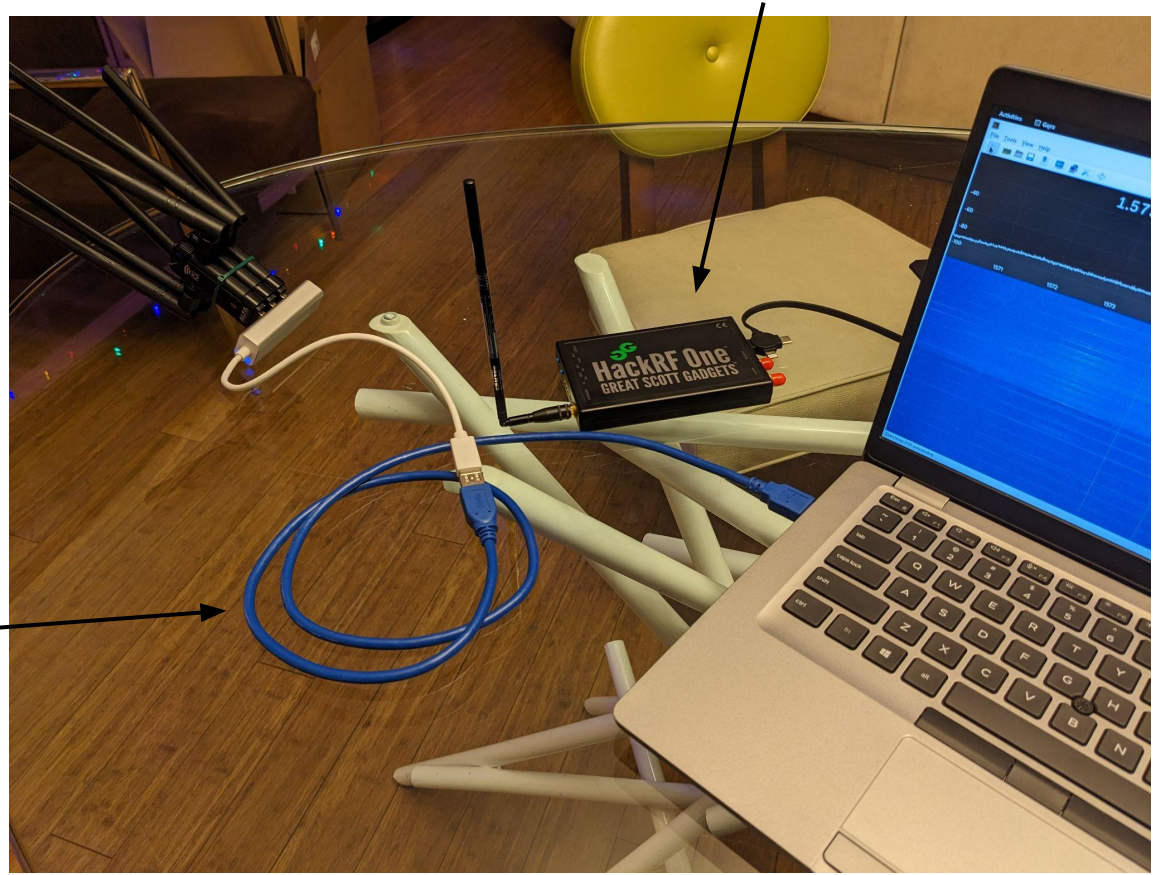
[demo]

Solution: Make all radios use USB 2.0 for communication. There is a limitation on data, but if we are only after metadata (SSIDs, and freq hopping, etc.) it may work.

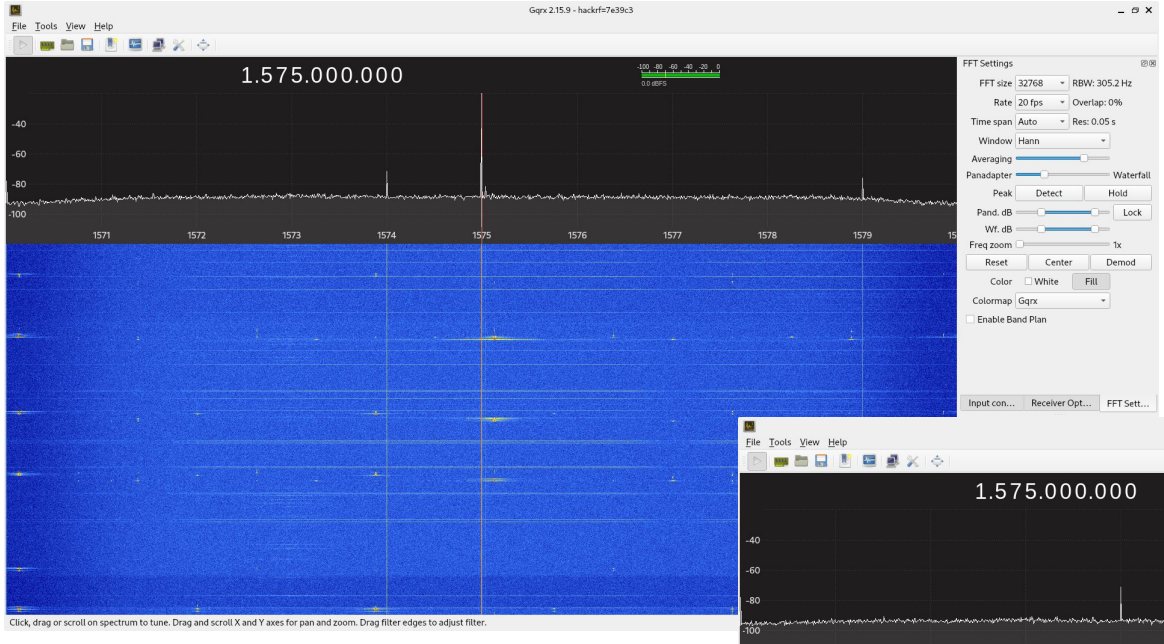
# The Setup

HackRF One (USB 2) receiving on the GPS L1 frequency

Alfa
AWUS036ACM
Cards



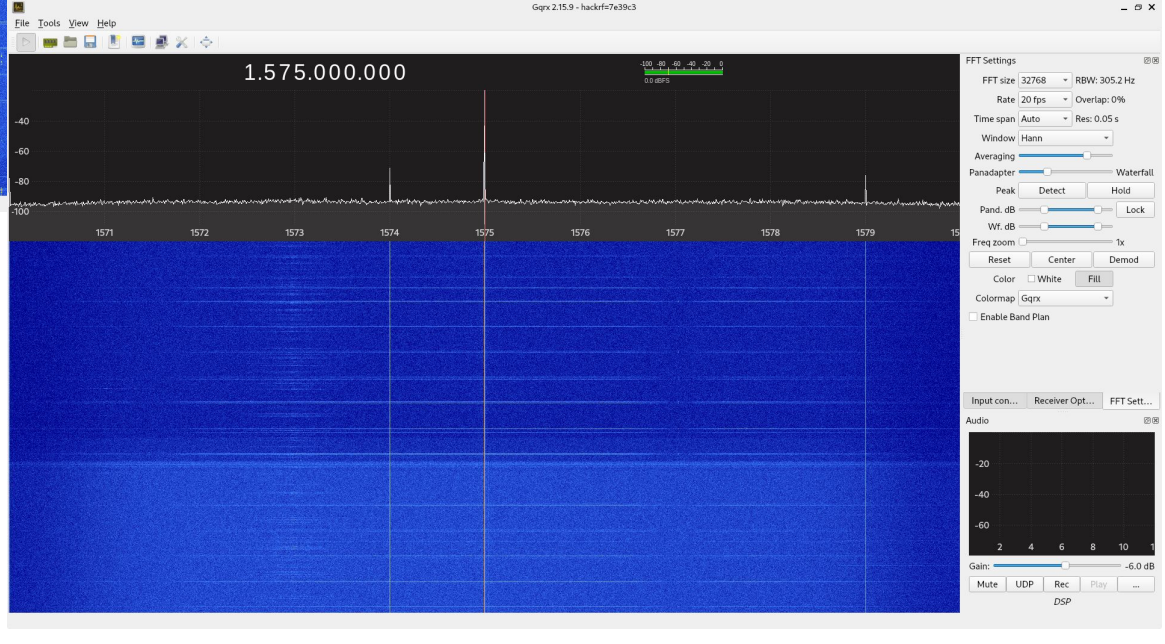

USB 3.0 Cable




<< Cable running 3x Alfa ACM cards on hub. General noise increase with peaks just over 1575 MHz.

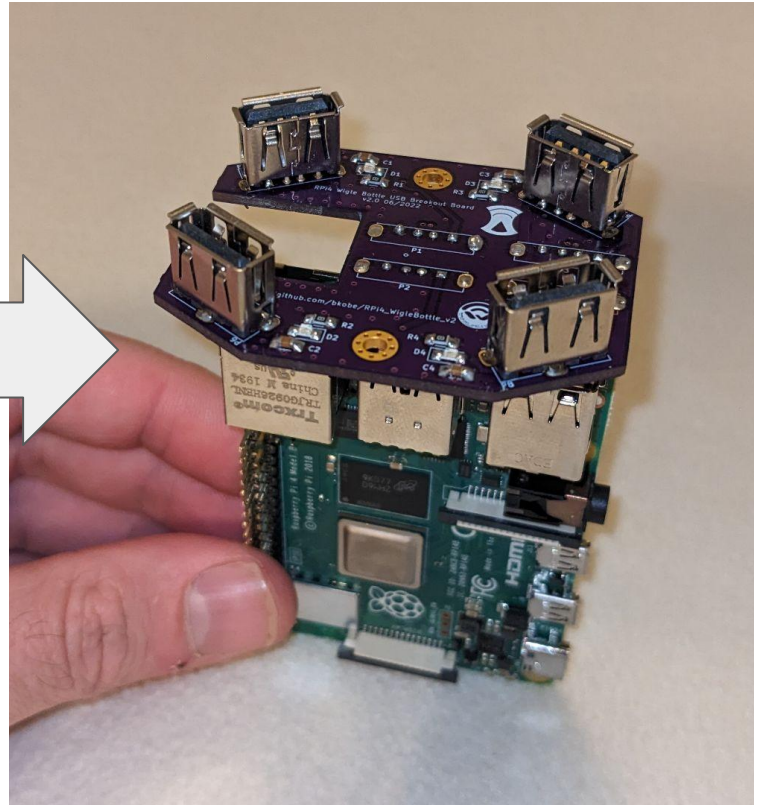
~10 dB decrease in noise when radios unplugged, but extender cable still plugged in. - - - - - - - - - - - - - - - - - - - - >>

Kismet stopped reading alfa cards and idling on bus. - - - - - - - - - - - - - - - - - - >>



# USB Board for the Pi


Version 1 in standard 1L water bottle



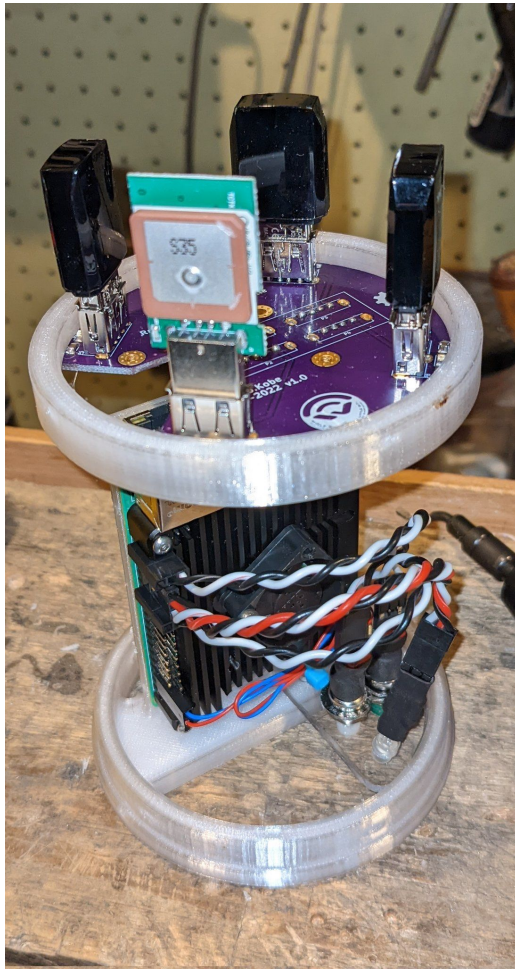
Version 2 in a tennis ball tube form factor

Now that we have communication to the USB data sources, how do we get reliable power?

# Power Supplies and Consumption

- PiSugar and PiJuice to provide dual power to pi for both internal battery and external/charging sources. Micro USB and USB-C inputs for charging and extended running when available
- Heat, and lots of it.
  - WigleBottle V1 used RPi4, which measured ~5W when running
  - WigleBottle V2 used RPi3B, which measured ~2.5W when running
  - Not worrying too much about the compute loss, the 3B+ and 4 are a bit power hungry…
- PiJuice has installed the 1200mAh battery for about 1-2h or runtime.  Options for micro-USB 5v input, as well as external 4-10V input (wired to a USB-C breakout for 5V).

The Pi 3B does the job with less heat generated by the CPU. Smaller/no fans, greater runtime on the battery(ies), no throttling...



Onto GPS and timing…

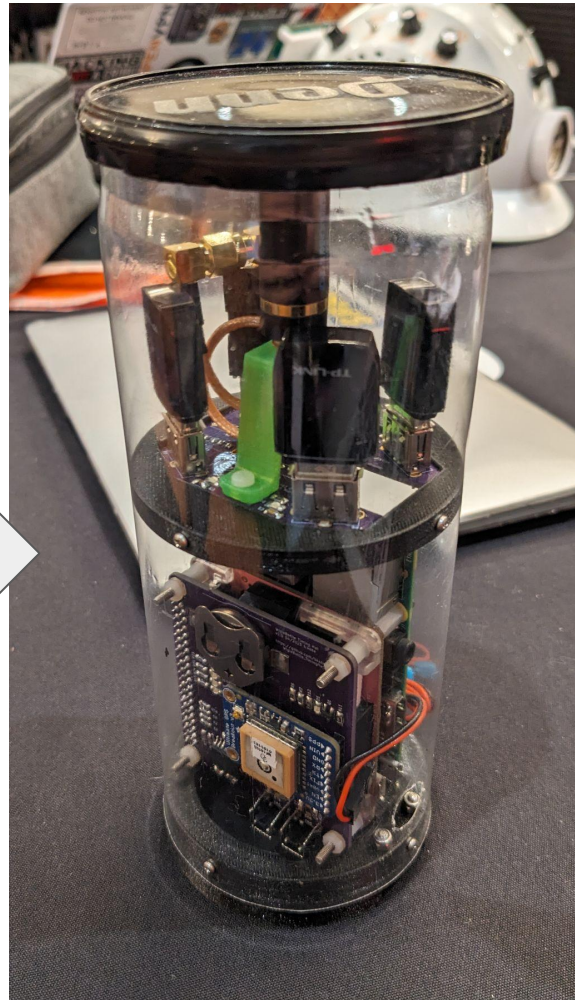
# GPS and Timing

- RESEARCH and CHECK GPSes before use!
  wytshadow has an excellent talk on GPS receivers (DEFCON 28):
  “Wicked Wardriving with GPS and GLONASS”
  https://www.youtube.com/watch?v=2h8H3XEgWvw

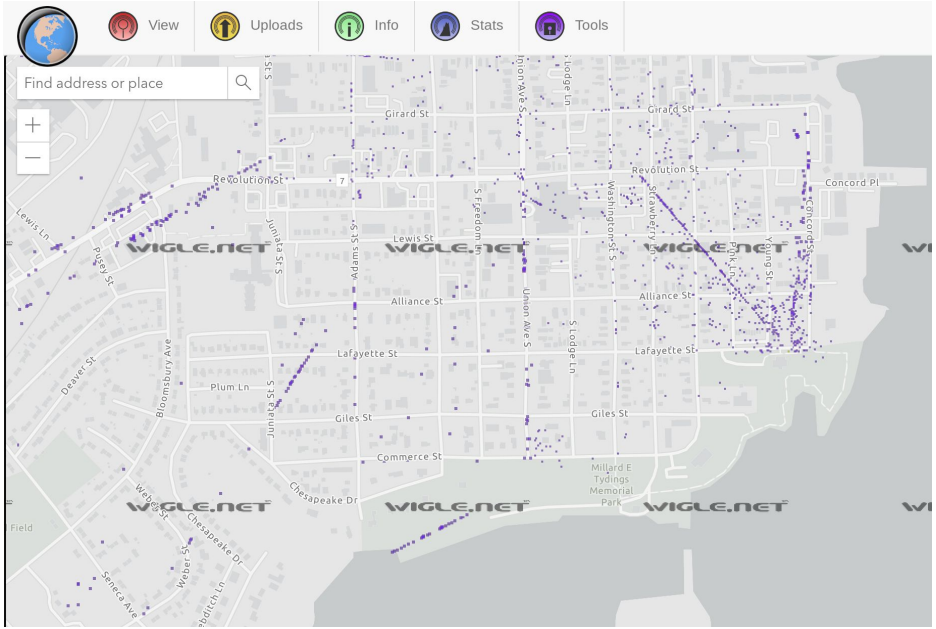
- The USB dongle form factor can work, but preferred mag mount external to the car for good position location (and separation from the other EMI potentials)

- Not all receivers created equal… Remember that GPS dongle from version 1? Although it “worked”, it never continually updated positions to gpsd for kismet to capture, then wigle to trilaterate.

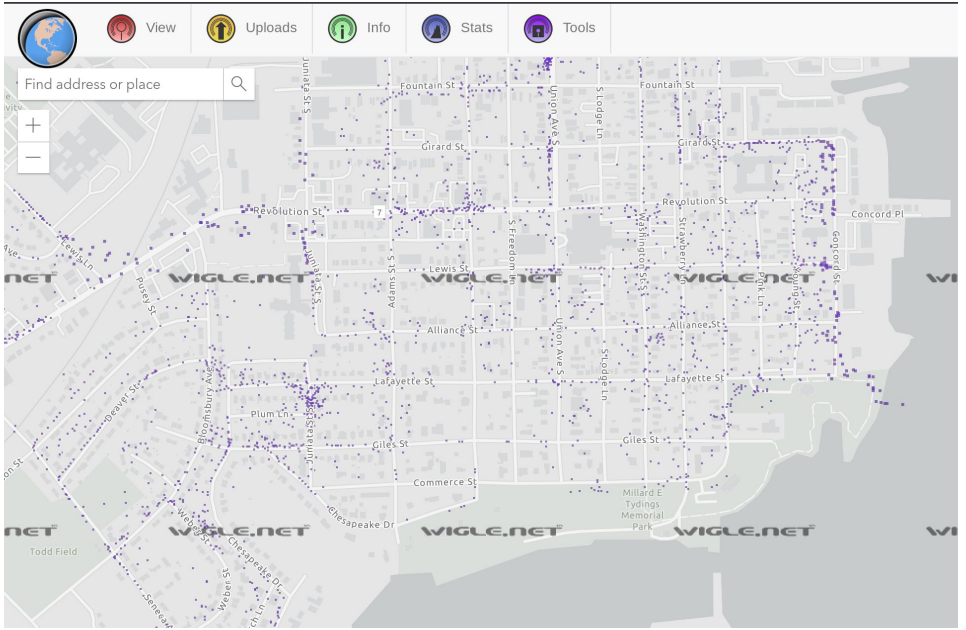
# Remember that v1 bottle GPS?

# GPS Performance V1 to V2 - #ZeroFoxGiven




Version 1 wigle “spray” from last location
Foxes found = 0/?



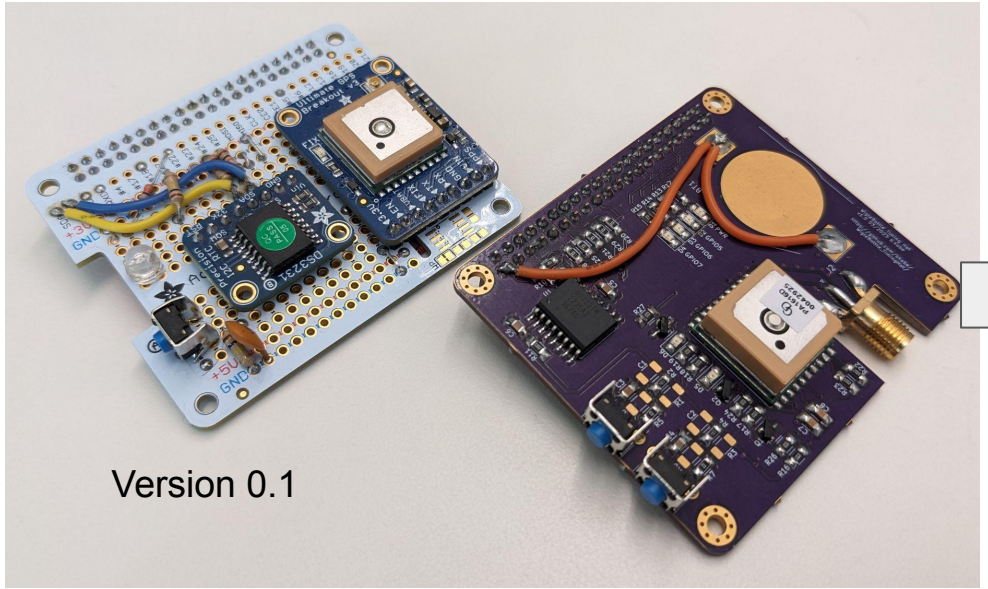

Version 2 updating as normal and trilaterating
Foxes found = 2/8

# Timing (continued)

- **Addition of real time clock (RTC) and battery backup** to pi for calendar and local holdover timekeeping.  When the pi boots, it grabs time from the RTC to initialize with (filesystem dates, etc).
- Chosen for the bottle is a ds3231 RTC, along with a CS2032 coin cell, which powers the battery backup for clock and the GPS (warm starts are really fast).
- **Be careful of I2C bus contention.**  The PiJuice also had an RTC at the same address (0x68) which I had to move off the default to allow the ds3231 to work. You could also use the RTC on PiSugar/PiJuice as well.
- **Integrated the pulse per second (PPS) from GPS** into the pi, and stitched it all together with chronyc.  The PPS and GPS will together “shim” the local clock to all in agreement. Within an hour of running, typically down to sub-microsecond accuracy to UTC.

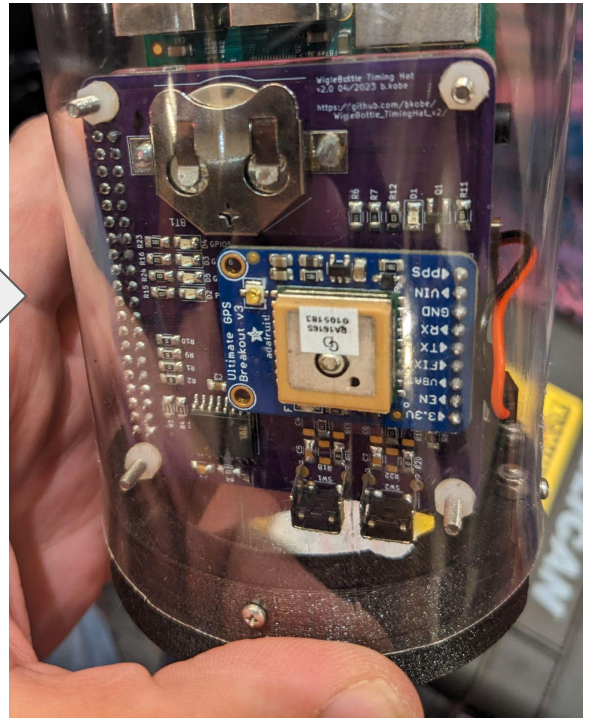
Adafruit has some good tutorials on integrating RTC and PPS to the pi, even syncing with chronyc

# Timing Board - Prototyping Onward…



Version 0.1

Version 1.0



Version 2.0

# Future Work (and lessons learned from WWWD DC31)

- Test rigs before production! Some issues do creep up.
- In using the Pi 3B, potential memory issue.  Bottle would lock up in just over an hour in…
  - Use /tmp/ to ramdrive the database, then copy over less often to SD card?
  - Possibly also routinely restart kismet daemon using a cron, etc.
- Automated way to convert kismet database to wigle CSV, then API upload.
- Future hardware to upgrade GPS to ublox NEO-M9N and possibly put a small OLED on for status.
  - PiJuice buttons and LEDs are a bit fragile.  Half on bottom here do not work. Got bumped at one point, and sheared off. Future buttons on hat daughterboad, not the bottom of PiJuice.

# References


- Roamer's talk in DC11: https://media.defcon.org/DEF%20CON%2011/DEF%20CON%2011%20presentations/dc-11-Hurley-C/DEF%20CON%2011%20-%20hurley-c.pdf

  … And the DC11 Talk at Alexis Park: https://www.youtube.com/watch?v=p6rPRIFCJaM

- Wytshadow's talk at DC28 on GPS: "Wicked Wardriving with GPS and GLONASS" https://www.youtube.com/watch?v=2h8H3XEgWvw

- Wigle: https://wigle.net. Thanks to arkasha, bobzilla, uhtu, thuddwir, wos!

- Kismet Wireless: https://kismetwireless.net. Thanks dragorn!

# References (continued)

- RFHS Wiki Pages
  - https://github.com/rfhs/rfhs-wiki/blob/master/pages/DEFCON-29-WWWD-RIGS.md
  - https://github.com/rfhs/rfhs-wiki/blob/master/pages/DEFCON-30-WWWD-RIGS.md

- Discord: RF Hackers Sanctuary, Kismet Wireless groups

- Personal github: https://github.com/bkobe. Repos (in Kicad) on:
  - RPi4 USB Breakout Board
  - RPi2/3B/3B+ USB Breakout Board
  - GPS Timing Hat
  - Slides from this presentation

Questions?