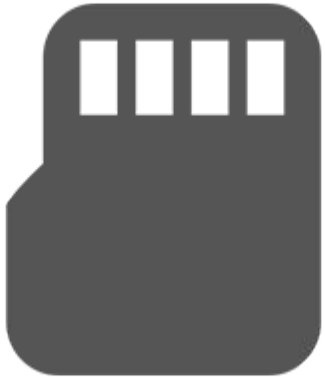
Is That a Wifi Sniffer In Your Pocket?

Jacob Baines

February 29, 2020

Slides, Code, and RPI Image



https://github.com/tenable/pi_sniffer

tenable

albinolobster@ubuntu:~$ whoami

Jacob Baines

Principal Research Engineer @ Tenable

@Junior_Baines

jacob-baines

tenable

Talk Overview

The Problem

Building a Solution

Real World Example

tenable

The Problem

WiFi Sniffing Background

- WiFi Sniffer?
  - A tool that intercepts and processes wireless packets.
  - Generally split into two parts:
    - Hardware (antenna)
    - Software
  - Early software example examples:
    - NetStumbler (2001)
    - Kismet (2002)

tenable

The Problem

What Good is WiFi Sniffing?

[A WarDriving Tutorial]

[Russian Attempt to Hack Chemical Weapons Watchdog in The Hague Thwarted]

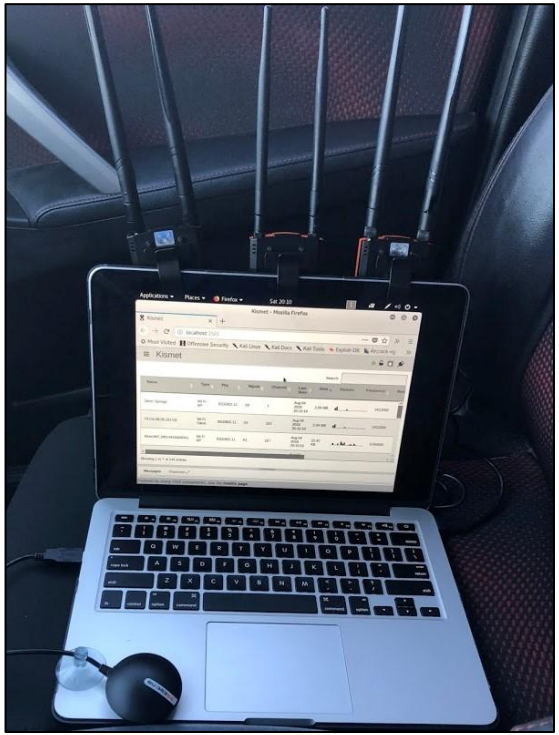
[5 GHz WarDriving]

tenable

The Problem

Endless Configurations

Wifi-box-of-Doom



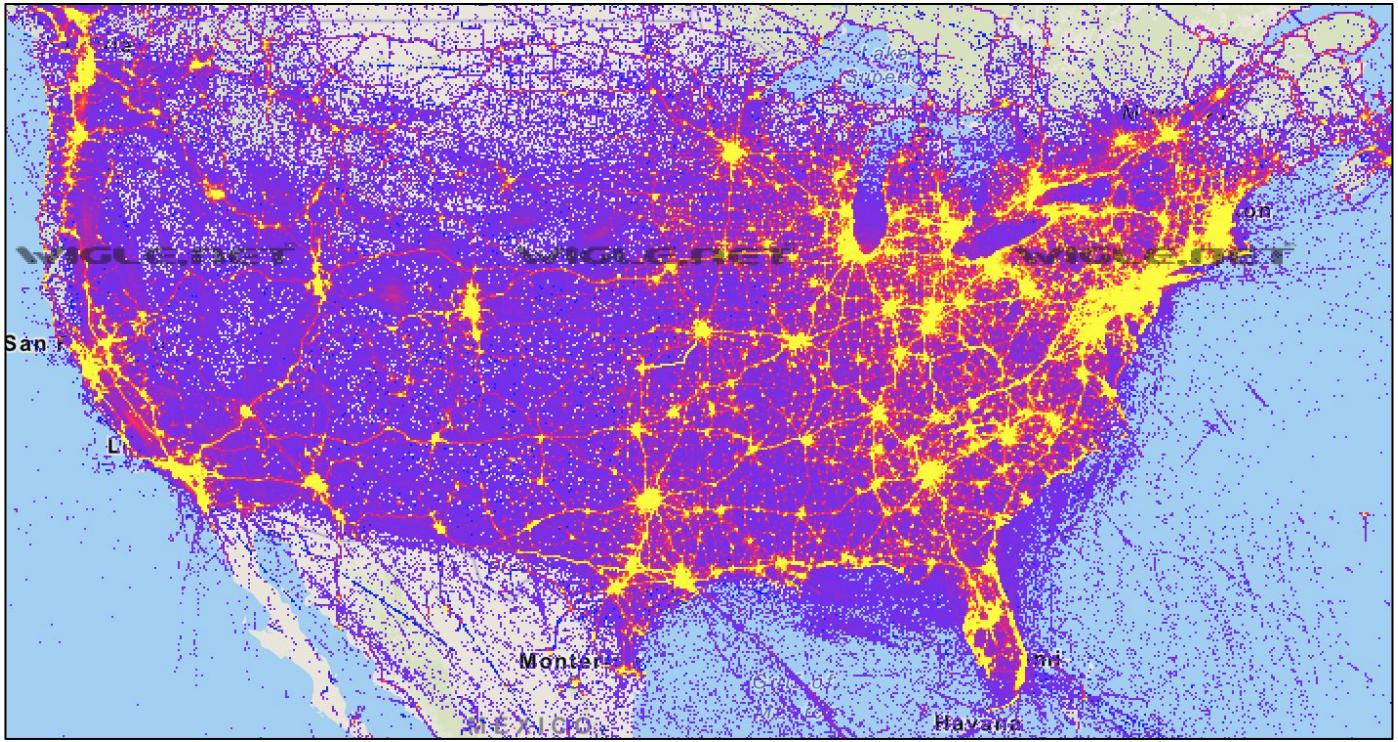
Wardriving Adventures

Building A Red Team WiFI Attack Car

tenable

The Problem

Mapping

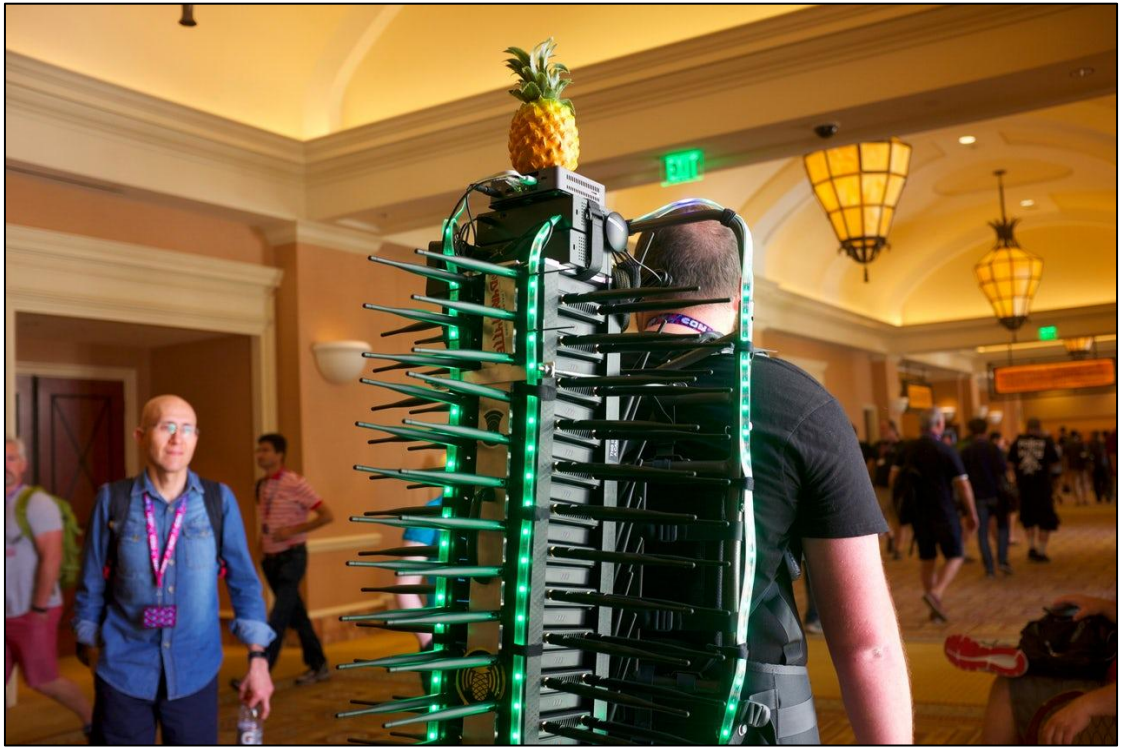


WiGLE

tenable

The Problem

Awesome



WifiCactus by @d4rkm4tter

tenable

The Problem

How the World Perceives Your Antenna and Flashy Lights

tenable

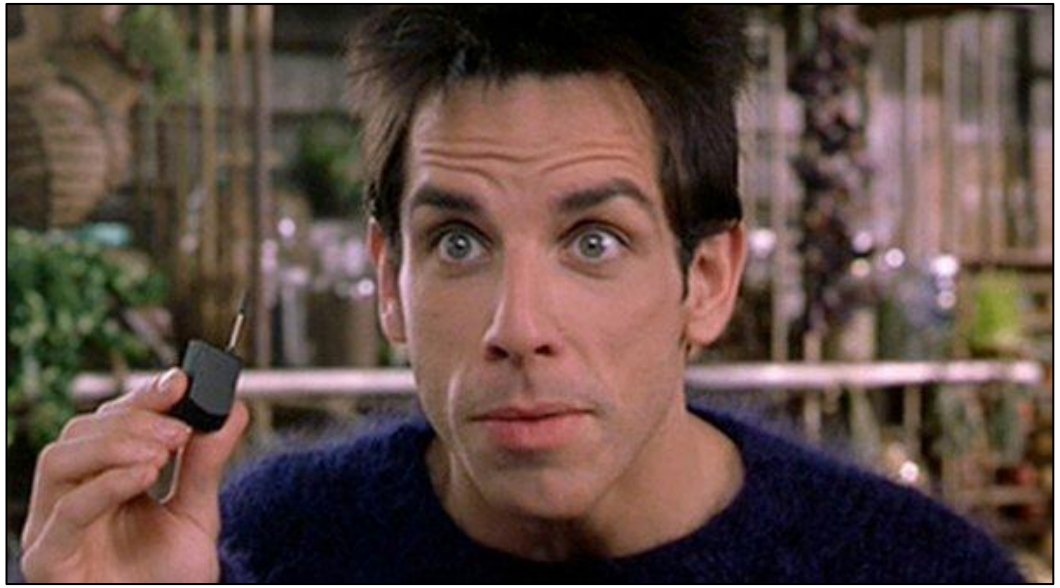
The Problem

How I Want to be Perceived

tenable

The Problem
The Tool I Want

- Easily fit in a pocket
- Must support:
  - UI / User Input
  - GPS
  - Multiple antenna
  - On the fly antenna configuration
  - Deauthentication attacks
  - WEP/WPA decryption
  - Standard output files
    - PCAP, Wigle, KML, HCCAPX
- *No soldering*
- ***Cheap***

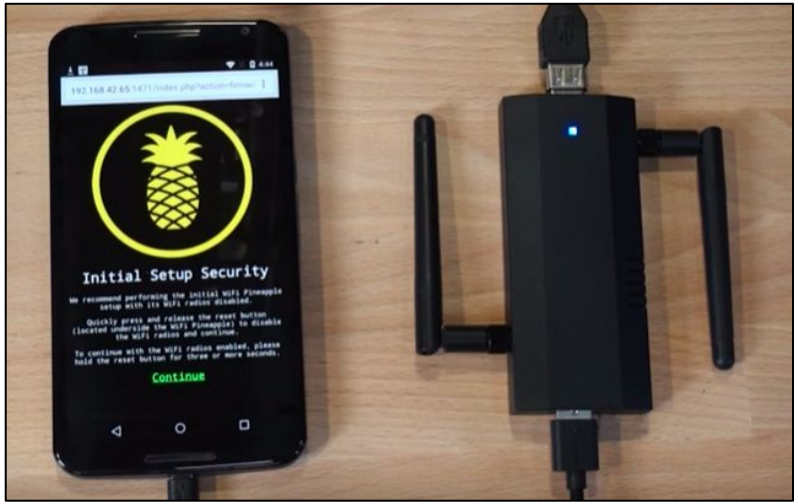


tenable

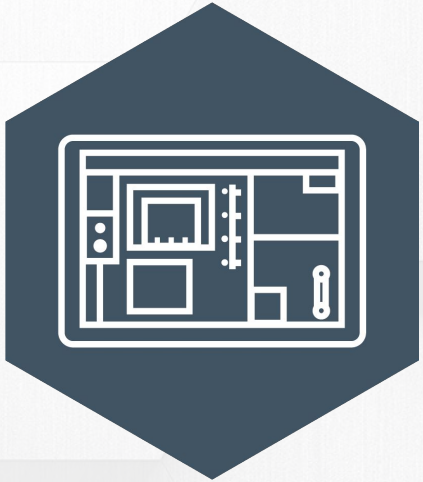
The Problem

Does A Solution Exist?

- Hak5 Pineapple NANO
  - Three separate hardware pieces (NANO, Android Phone, and battery) creates a bulky setup.
- Pwnagotchi
  - An A2C AI that is more focused on capturing WPA key materials and not general WiFi recon.
  - Indiscriminately deauths clients.
  - Lack of on the fly user input.
- Wigle WiFi App
  - Android Wardriving App
  - Insufficient control of the data and output.
  - More a mapping tool and less an offensive tool.
- ESP8266 Deauther

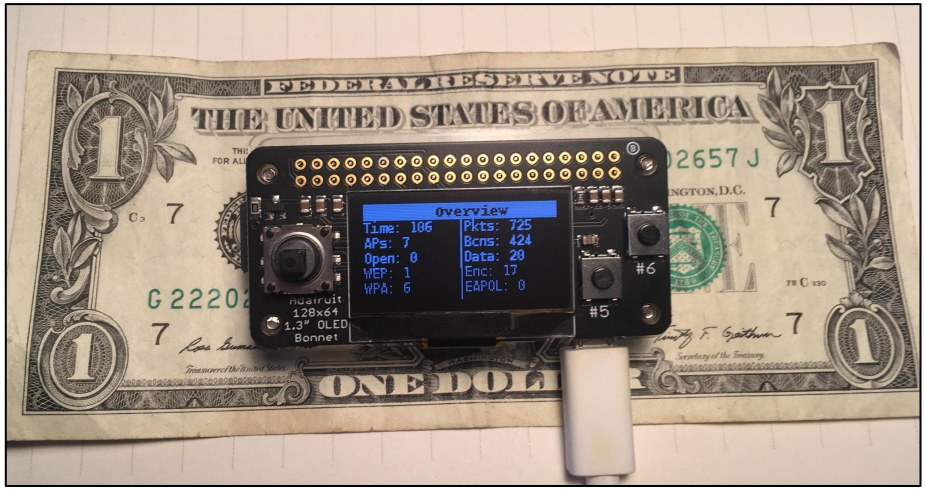


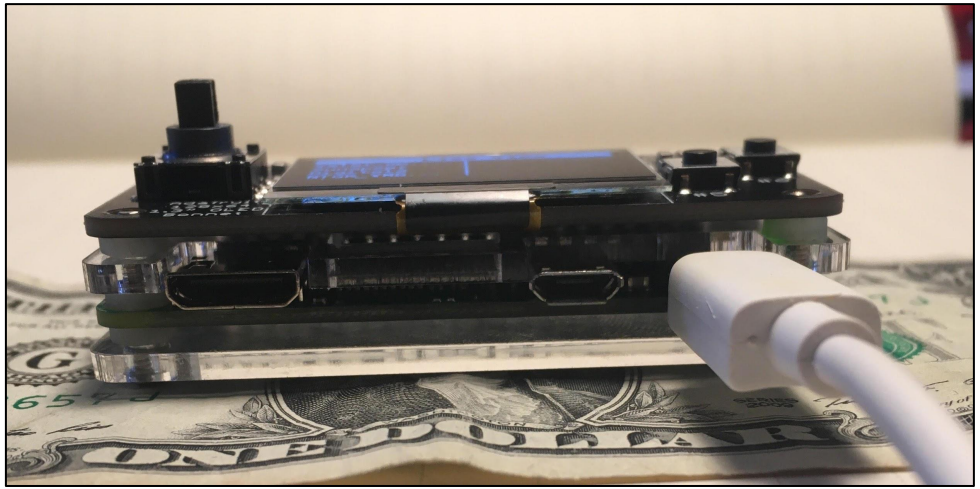
tenable



Building a Solution

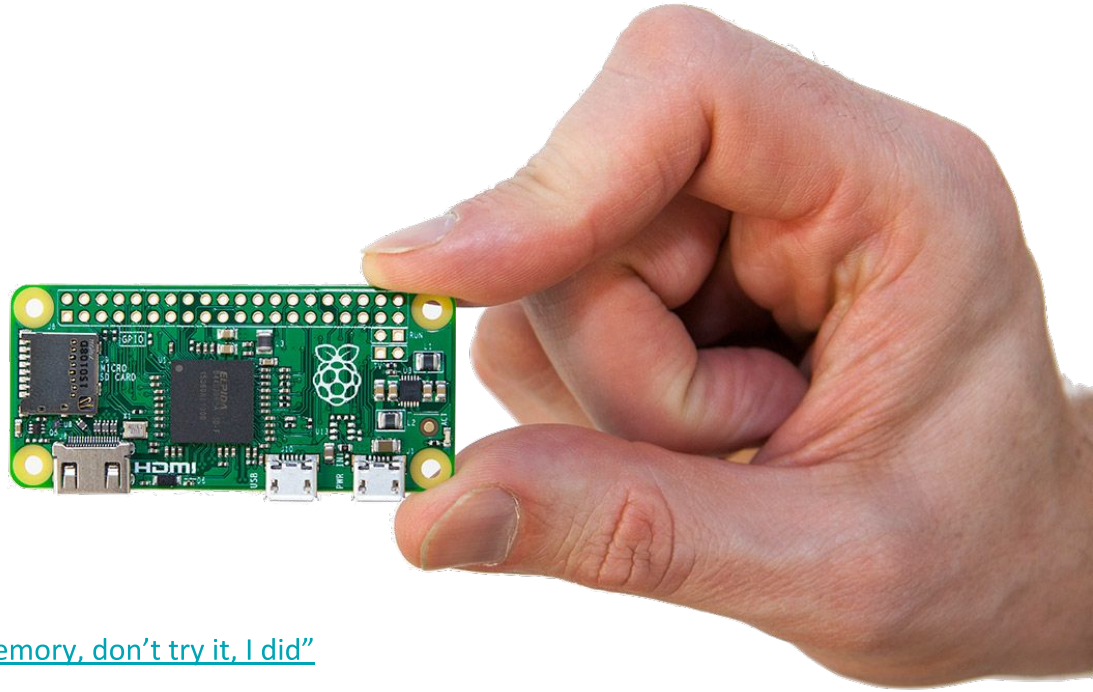
A Wild Solution Appears





Building a Solution
Hardware Platform

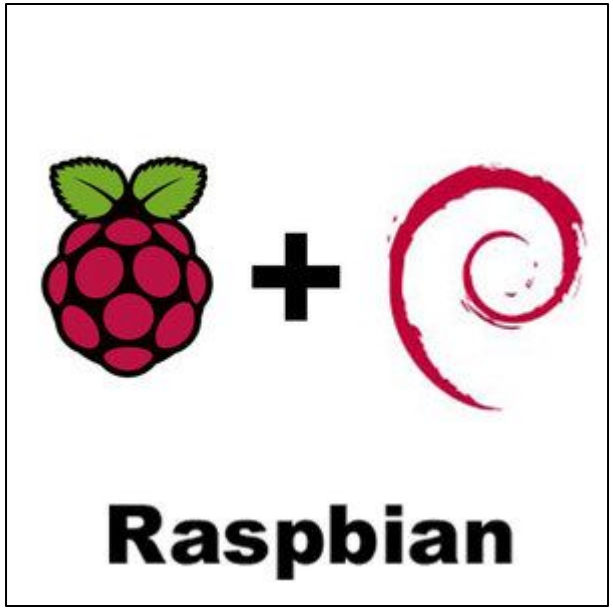
- Raspberry Pi Zero W
- Pros:
  - Supports a variety of Debian-based OS
  - Built-in Antenna
  - Cheap ($10)
  - Supports a variety of peripherals
  - Widely available
- Cons:
  - System resources:
    - 1 GHz Single-core ARMv6 processor
    - 512 MB RAM
    - "Pi Zero does not have enough CPU / Memory, don't try it, I did"
  - Only one micro USB port supports data



tenable

Building a Solution
Software Platform

- Raspbian Lite
  - Stripped down Raspbian.
  - Not the most minimal but supported by the Raspberry Pi Foundation (so unlikely to disappear).
- Re4s0n Kernel
  - Contains the required nexmon patchset to enable monitor mode on the Pi Zero W's internal antenna.



tenable

Building a Solution

Display & Controls: A False Start

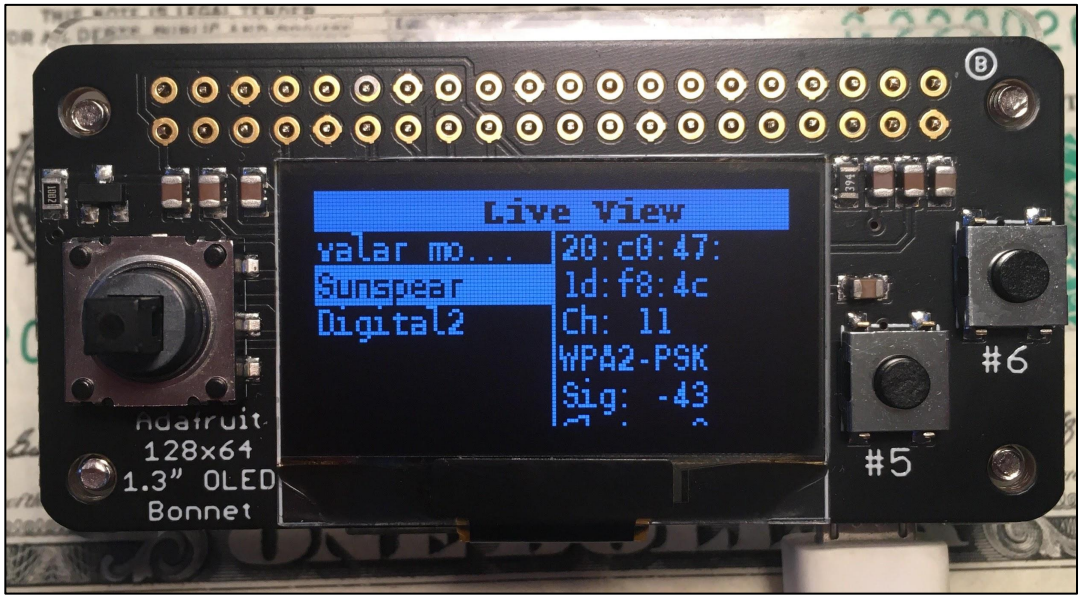
- Originally used an Inky pHAT e-Ink display.
- Pros:
  - Relatively large display (212x104)
  - Low power usage (8mA)
  - Requires no soldering (sits on the 40 pin header)
- Cons:
  - Requires ***15 seconds*** to refresh.
    - Difficult to have a UI that responds so slowly.
  - Leaves minimal room for user controls.
    - Pictured you can see a Button Shim on the right.
    - Button Shim requires soldering
  - Can suffer from burn in.
  - Inky pHAT + Button Shim = **$33.50**

tenable

Building a Solution

Display & Controls

- Switched to an OLED Bonnet
- Pros:
  - Up to 15 FPS
  - Built-in joystick and two buttons.
  - No soldering required.
  - $22.50
- Cons:
  - Tiny display (128x64)

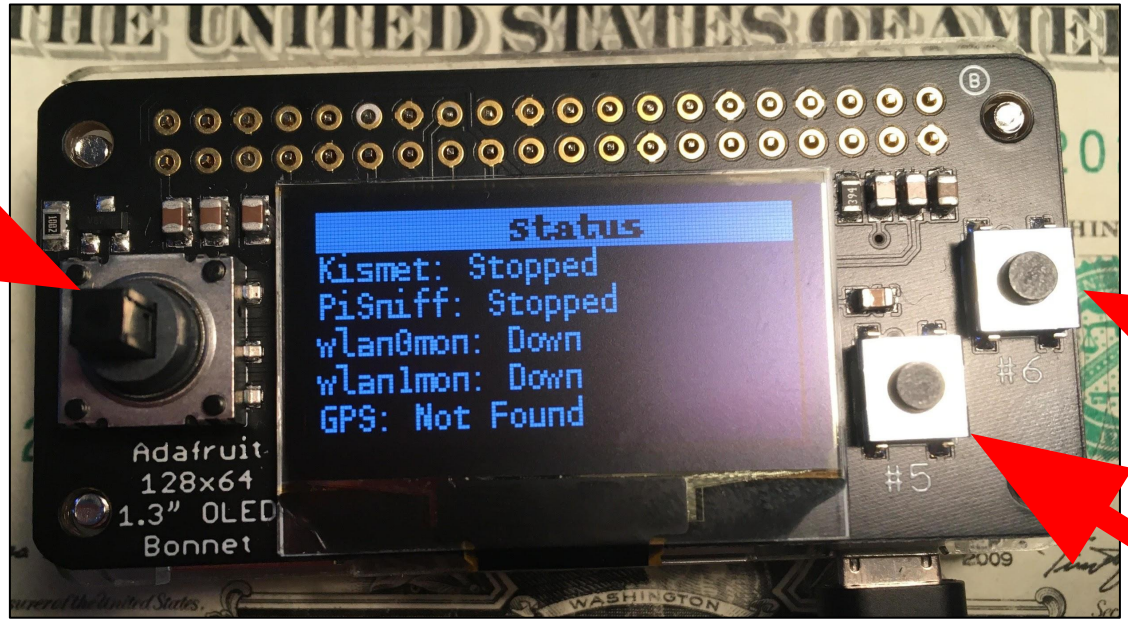


tenable

Building a Solution

Display & Controls

Rotate between views



Start

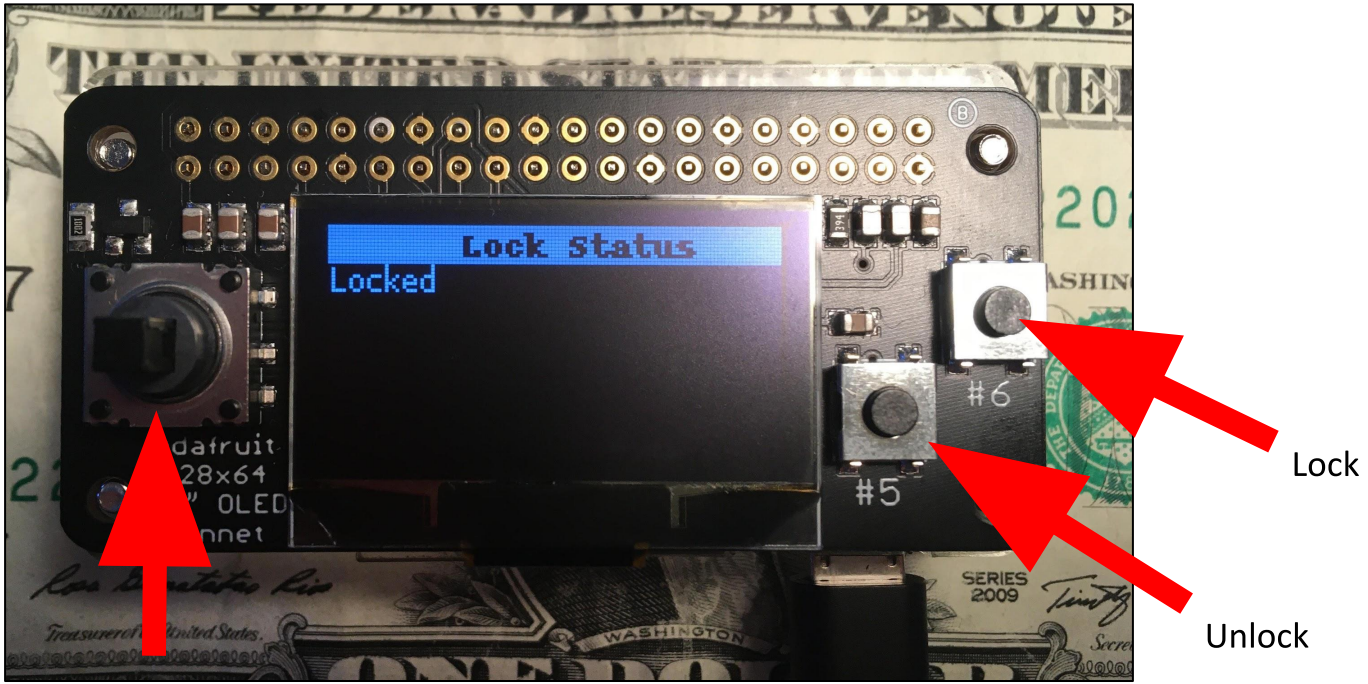
Stop

Start + Stop = Clean Shutdown

tenable

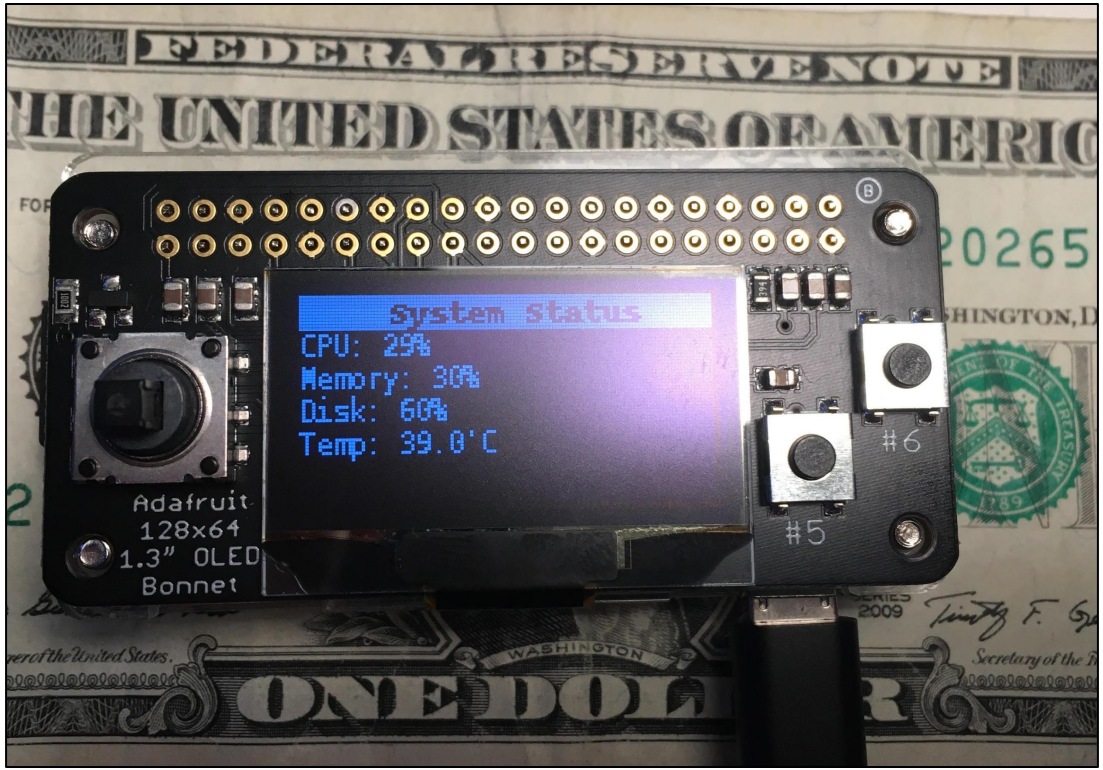
Building a Solution

Display & Controls



Building a Solution

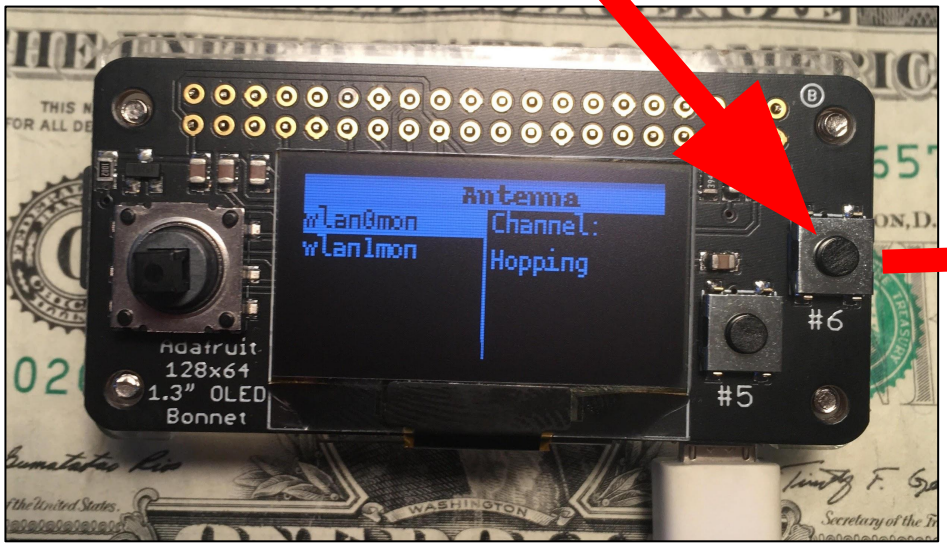
Display & Controls

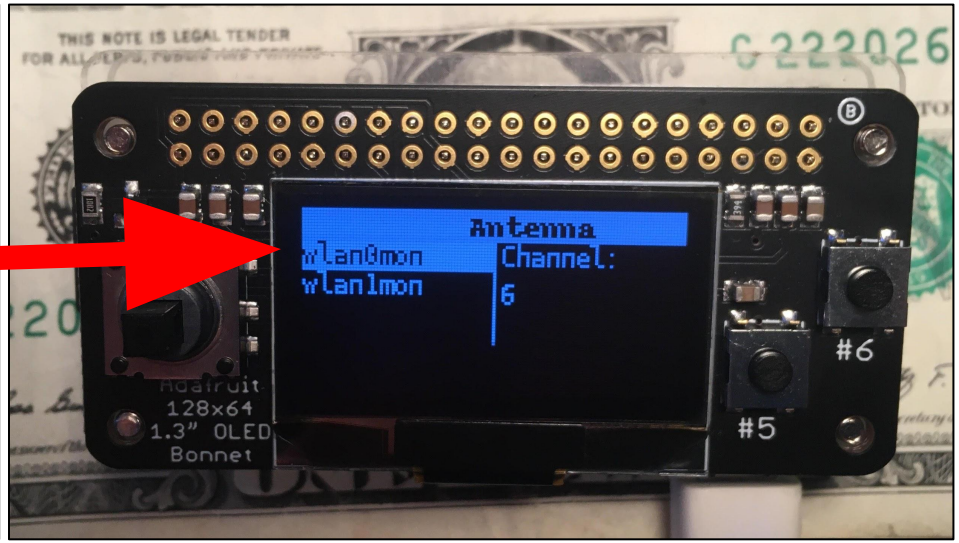


tenable

Building a Solution

Display & Controls



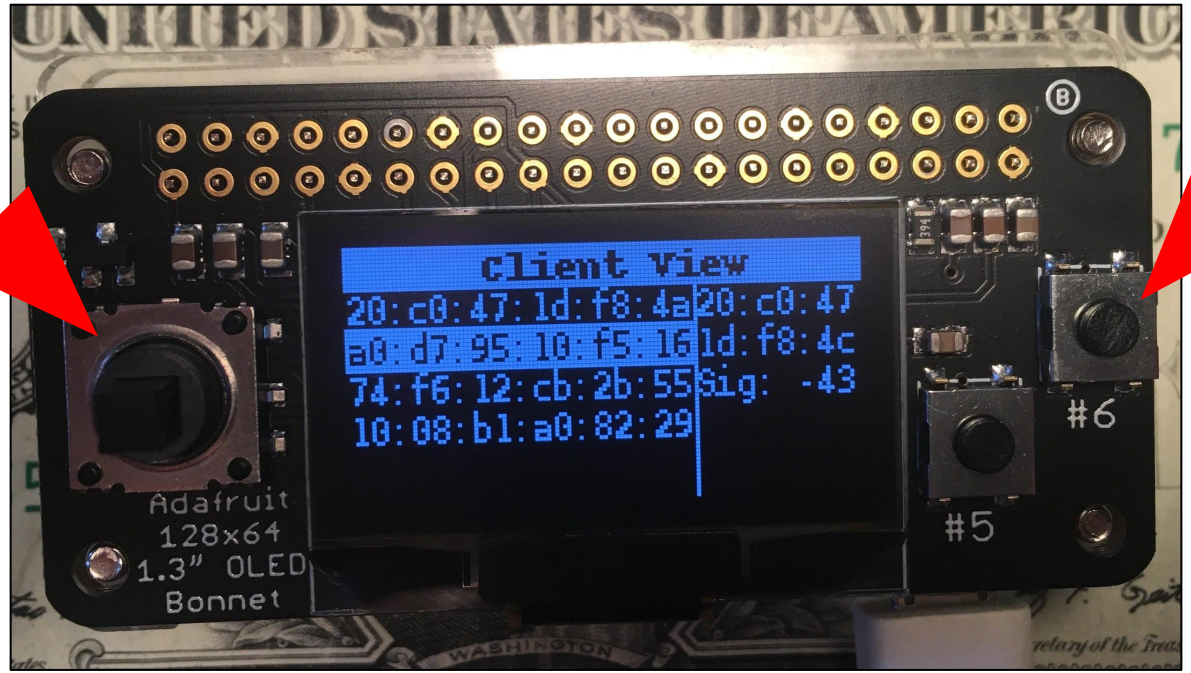


tenable

Building a Solution

Display & Controls

Cycle through views or clients

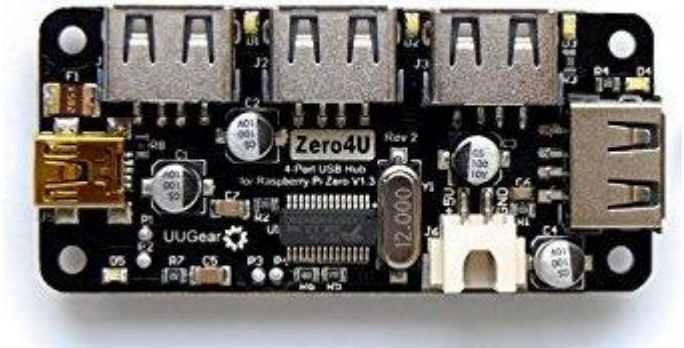


Deauth Attack

tenable

Building a Solution

External Hardware Support

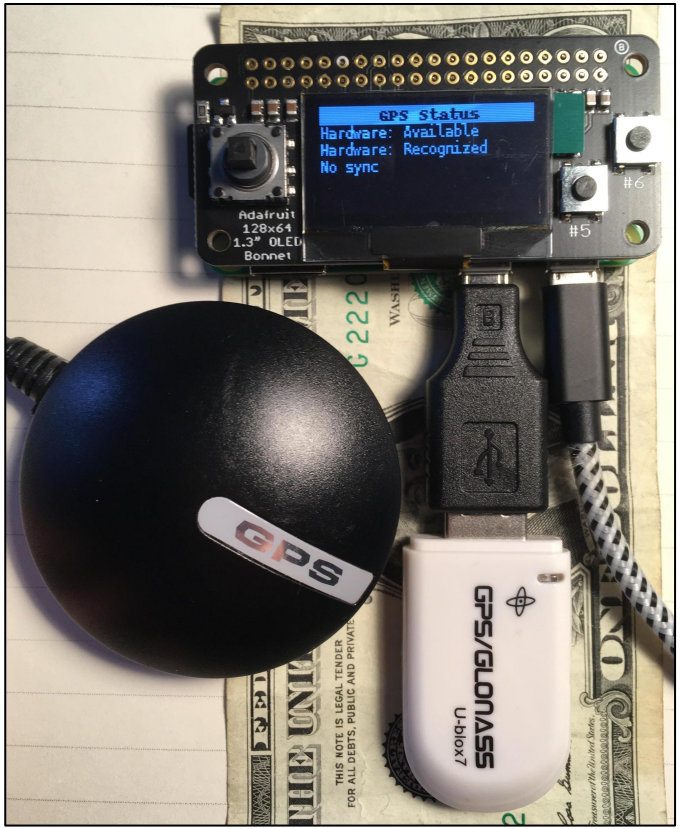


- Antenna/GPS use USB.
- Pi Zero W has ***one*** micro USB port with data.
- Each solution has issues:
  - Single adapter is bulky and limits to one external device.
  - The hub is even bulkier and awkward to handle.
  - The Zero4U limits battery selection and is the most expensive option.

tenable

Building a Solution

GPS



- GlobalSat BU-353 (pictured left) is the traditional GPS for WarDriving.
- However, the U-blox 7 is:
  - Smaller
  - Draws less power. Typical: 26 mA vs. 80 mA
  - About half the price (~$13)

tenable

Building a Solution

External Antenna

- More antennas is better.
  - Internal antenna only supports 2.5 GHz band.
  - Channel hop on one antenna and deauth attack on the other.
- Limiting factors:
  - Antennas are power hungry. 100-500 mA depending.
  - Most antennas are too big to comfortably fit in your pocket.
- Close but just too big:
  - TL-WN722N (version 1: sort of rare)
  - BroTrend AC1200 AC1L.
- Close but infuriating:
  - AWUS036ACS
- What I Use: CanaKit Wireless Dongle
  - Small
  - Lacks 5 GHz band

tenable

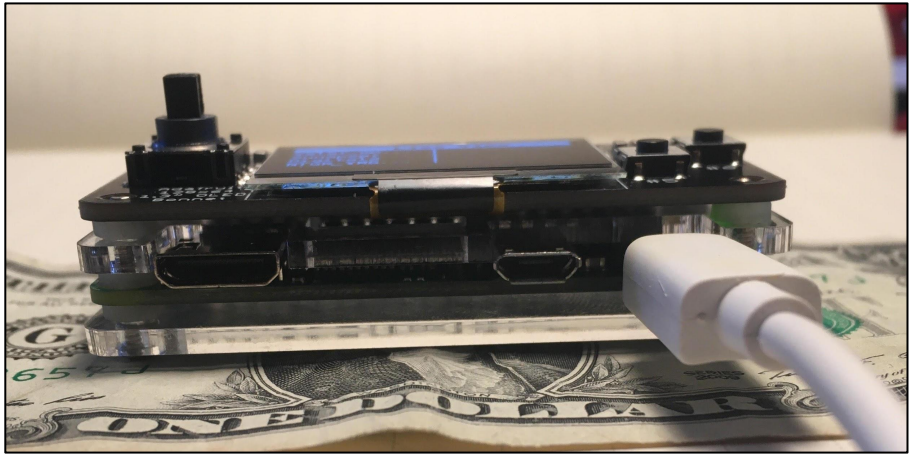
Building a Solution
Power

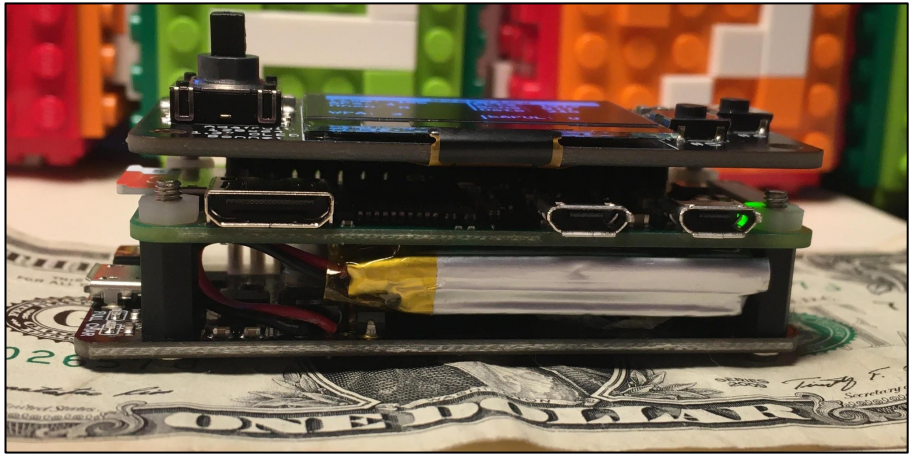
- Main considerations:
  - How long until the power supply runs out of juice?
  - Does it easily fit in a pocket?
  - Is it awkward to handle?
  - Price.
- Pwnagotchi has documented a number of batteries
- Tried and true: Anything by Anker
  - Anker E1 Astro (24 hour charge)
  - Anker PowerCore+ Mini (6 hour charge)
- UPS-Lite by @xiaoj_329 (pictured right)
  - Shipping is slow.
  - Comparatively low battery time: 3 hours.
  - A bit chonky but otherwise slick as hell.

tenable

Building a Solution

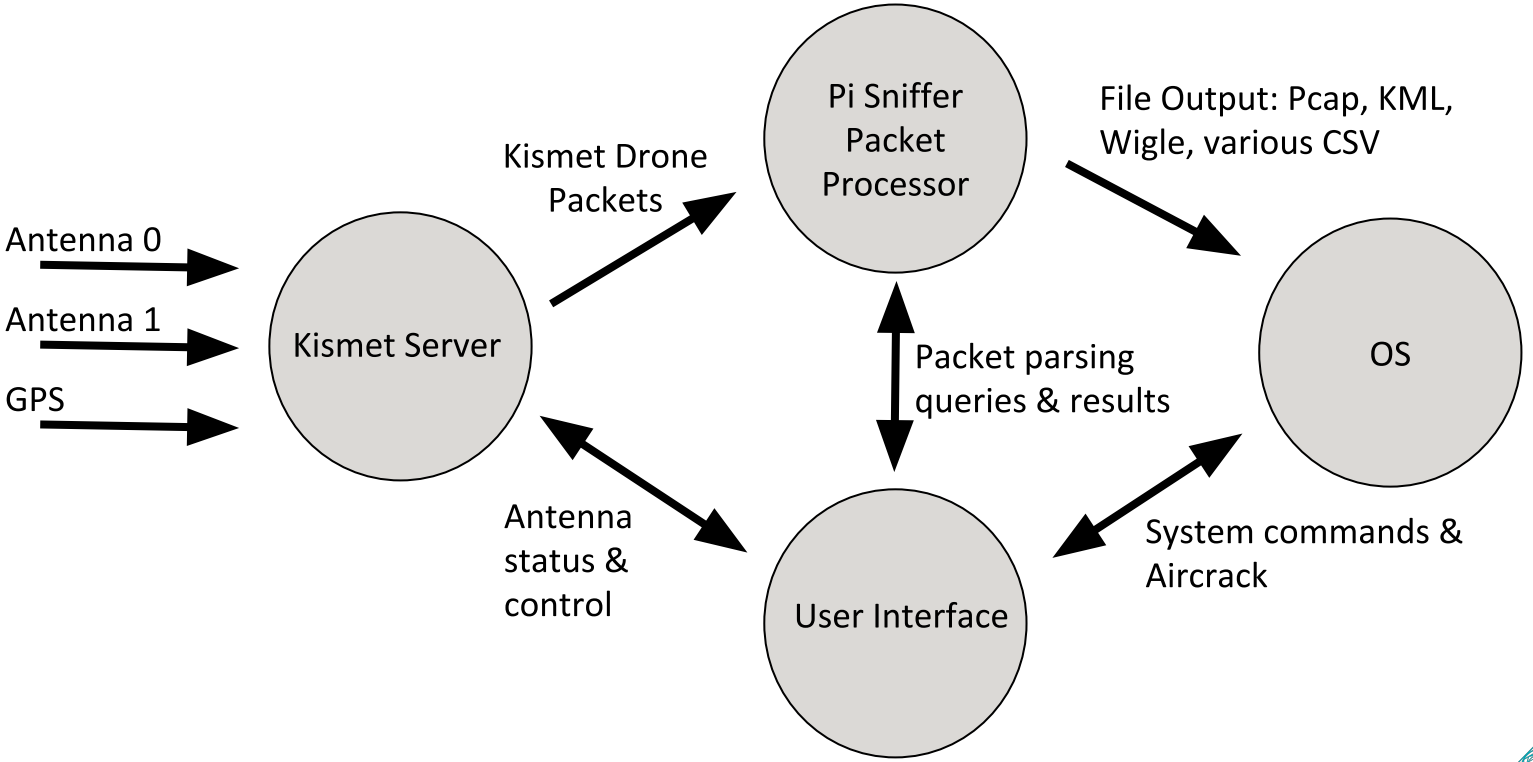
Power





tenable

Building a Solution
Software



tenable

Building a Solution

Price

Base Components

Item	Price
Pi Zero WH	$14
OLED Bonnet	$22.50
Powercore 5000	$19.99
Kingston 8 GB microSDHC	$3.99
Total	***$60.48***

Base + External Antenna

Item	Price
CanaKit WiFi Dongle	$9.99
Micro USB Male to USB Female Adapter	$6.99
Base	$60.48
Total	***$77.46***

Base + External GPS

Item	Price
U-Blox7 GPS	$13.99
Micro USB Male to USB Female Adapter	$6.99
Base	$60.48
Total	***$81.46***

Base + External GPS & External Antenna

Item	Price
U-Blox7 GPS	$13.99
CanaKit WiFi Dongle	$9.99
USB Mini Hub	$4.95
Base	$60.48
Total	***$89.41***

tenable

A Real World Example

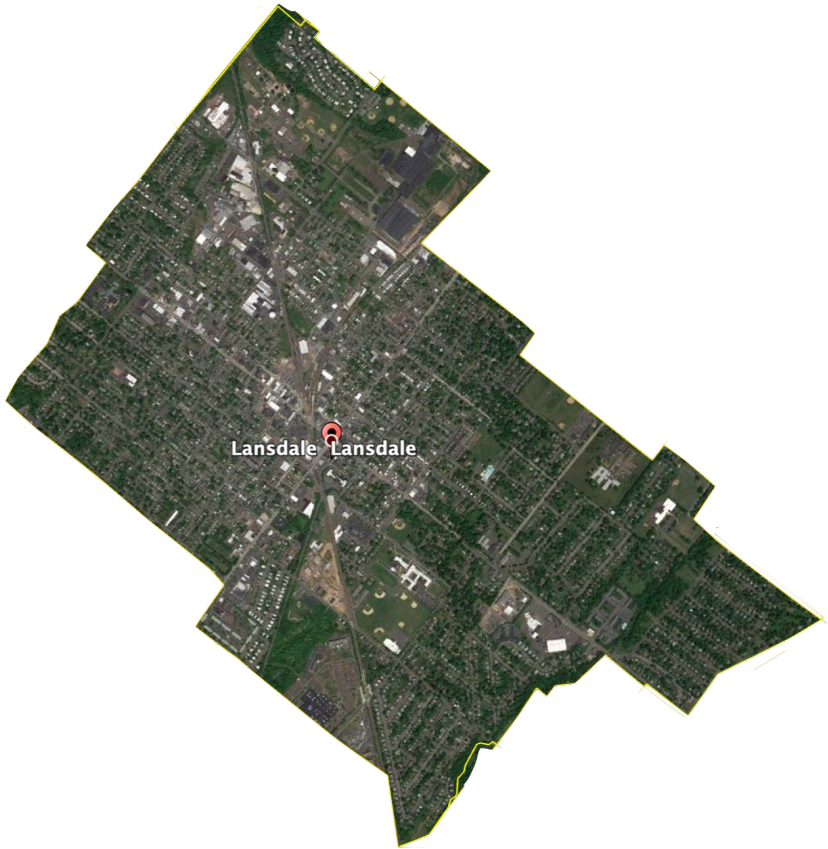
Does This Actually Work?

- Is the device powerful enough?
  - Will the CPU hold up?
  - Will the Pi Zero run out of memory?
  - Is the internal antenna strong enough?
- Gotta test in the real world.
  - Stick the Pi Sniffer in my pocket and go for a nice long walk.

tenable

A Real World Example

Lansdale, PA

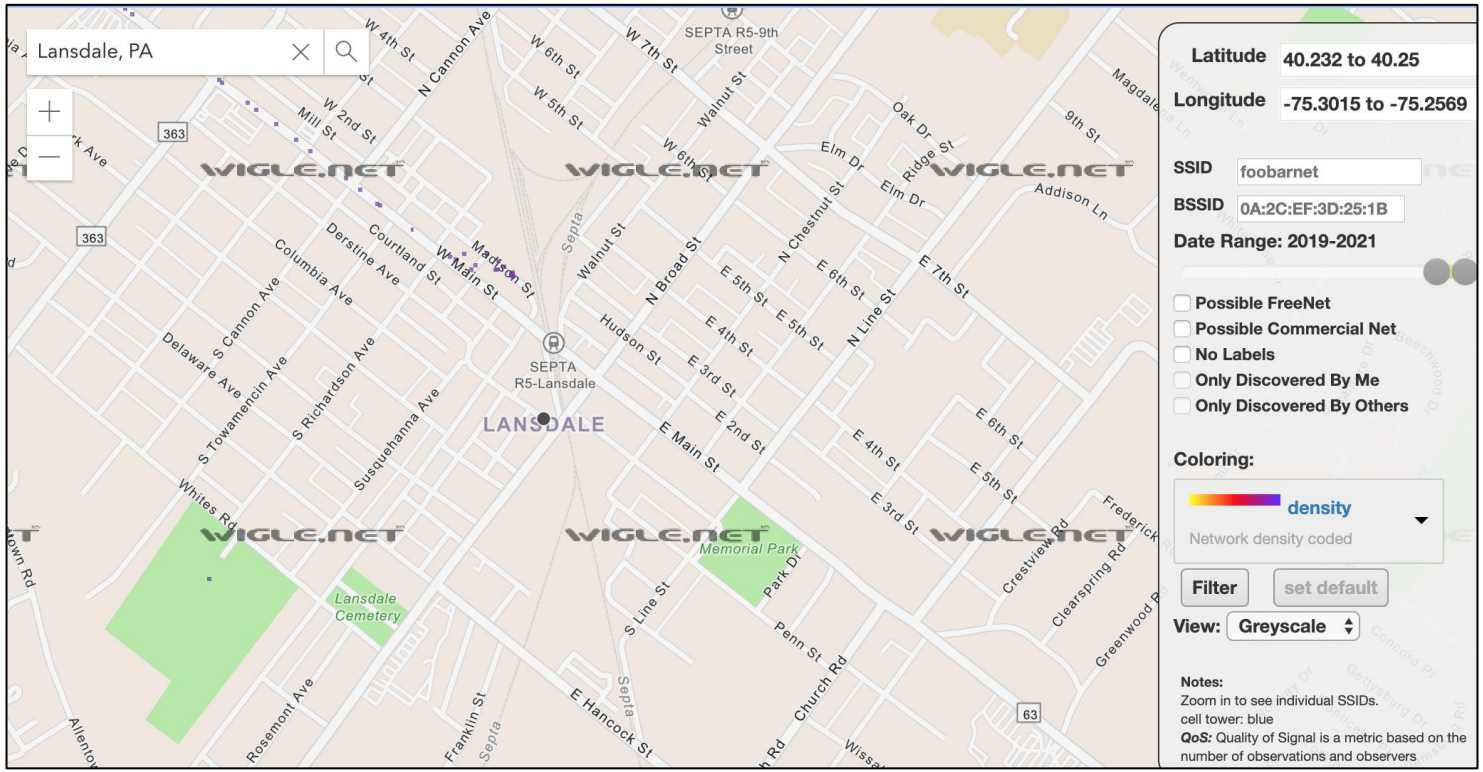


- About 3 square miles.
- ~17,000 residents.
- Many commute via Lansdale/Doylestown SEPTA into Philadelphia.
- Active main street.
- Mix of residential, industrial, and business.
- Most importantly: close to me.

tenable

A Real World Example

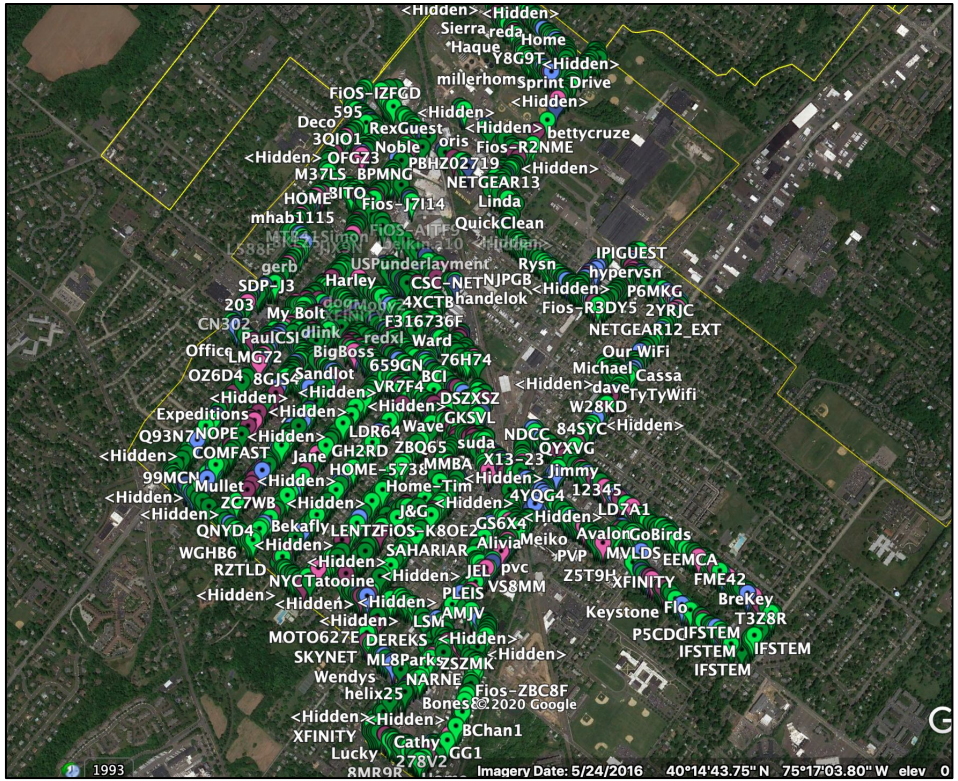
Lansdale, PA



tenable

A Real World Example

Lansdale, PA



- Failed to cover the entire 3 sq miles.
- More than 11,000 AP mapped.
- More than 6,000 clients observed.
- 250 MB pcap recorded.
- 27 hcappx files generated.
- Top three probe requests:
  - Spencershaw181 (totally unexpected)
  - TMobileWingman
  - Xfinitywifi
- Most clients observed on a network:
  - 60 clients on a local schools guest network.
- No memory/CPU issues.

tenable

A Real World Example

Lansdale, PA

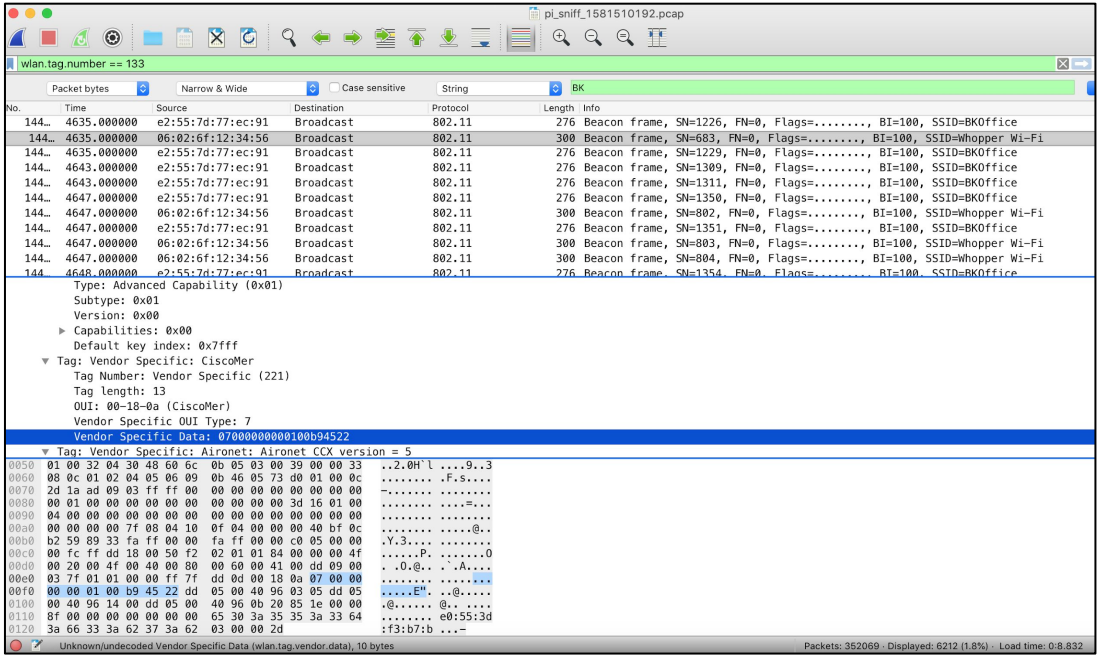
```
pi@raspberrypi:~/pi_sniffer_output $ ls
pi_sniffer_1581698204.pcap           pi_sniffer_map_1581698204_wpa.kml
pi_sniffer_clients_1581698204.csv    pi_sniffer_probes_1581698204.csv
pi_sniffer_map_1581698204_open.kml   pi_sniffer_wigle_1581698204.csv
pi_sniffer_map_1581698204_wep.kml
pi@raspberrypi:~/pi_sniffer_output $
```


tenable

Future Work

What's all that data for?

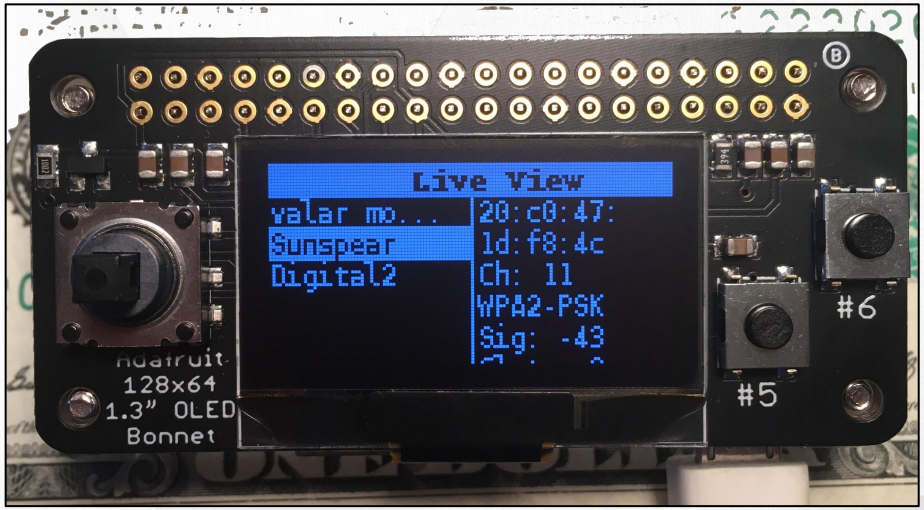
- Vulnerability Hunting Targets.
- Franchise WiFi Deployments.
- Soooo many cars.
- Oddities.



tenable

Thank You and Happy Wireless Hunting!

Slides, Code, and RPI Image



https://github.com/tenable/pi_sniffer

@Junior_Baines