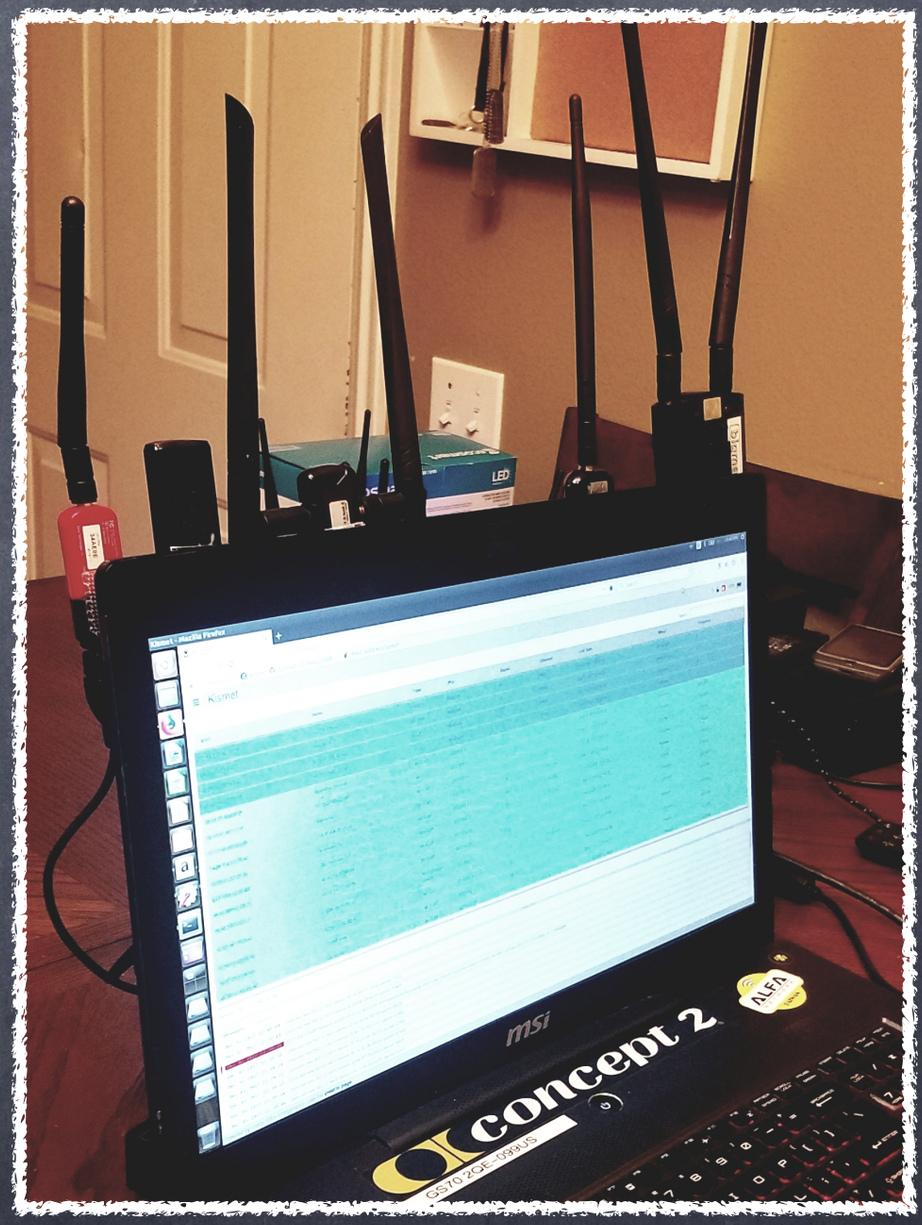
How to build your own wireless packet capture rig.

el kentaro

What is this talk?

- This talk will about the current state of wardriving and wireless communications.
- I will share you tips and tricks that I have learned about building a "mobile packet capture rig"
- It will focus on "making" and "building"
- It will not teach you how to hack your friends facebook. (twitter/instagram) via wifi.



Legal Disclaimer

- I'm not a lawyer.
- There are countries/ places where wireless scanning is considered "wiretapping" and illegal.
- To transmit most likely you need a license.
- STAY LEGAL!

Who am I?

- @elkentaro (twitter/instagram)
- Job: Translator
- Why: I want to be Q.
- Wifi capture is like fishing for me.
- There is no appliance that I havent taken apart.
- How much money do I make "hacking" : $0

I want to be the guy the hero comes to for gadgets and help.

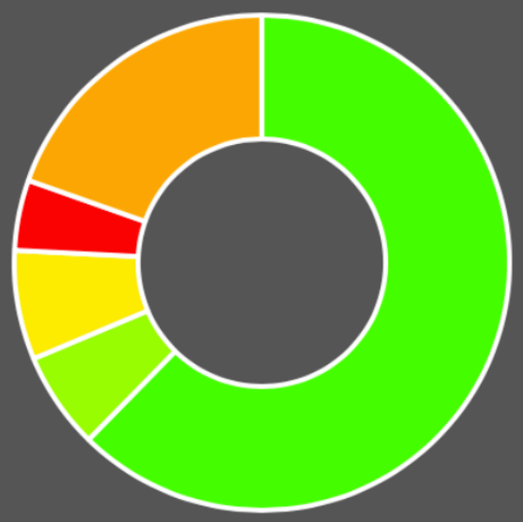
Why wifi capturing ?

- that's for noobs.

- Wardriving used to be "cool." Every hacker does it "once"
- Everything is connected to a network. And many of them are connected wirelessly.
- Tools have advanced to not only capture 802.11 but also BTLE , Zigbee and other protocols, some even use SDR (ie: all the waves)
- Its the basis of "connectivity" to the new Internet era.

Unique WiFi networks in DB:		447,005,868
Unique networks w/ location:		442,443,690
Unique WiFi locations in DB:		6,355,807,195
Unique Cell towers in DB:		9,088,427
Unique Cells w/ location:		9,035,734
Registered Users:		212,861
Networks with default SSID:	12,678,371	(2.84%)
New unique networks today:		51,550
New today with location:		50,934
New yesterday with location:		346,450
Total Files parsed:		2,231,841
Files uploaded today processed:		0
Files 1 day ago / 2 days ago:		0 / 551
Files queued to process:		0

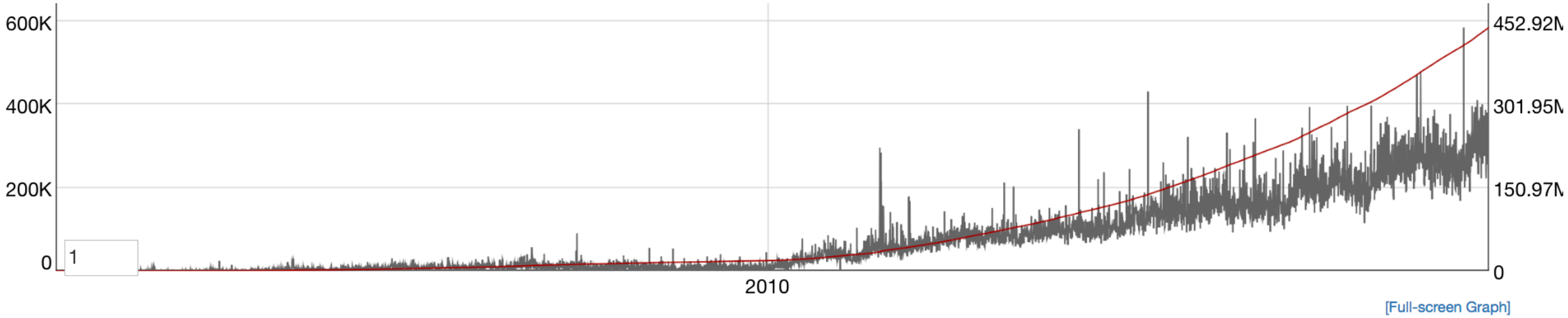
Wireless Encryption



WPA2: 278,959,266 (62.41%)
WPA: 28,335,247 (6.34%)
WEP: 31,926,588 (7.14%)
????: 87,728,291 (19.63%)
None: 20,573,959 (4.60%)

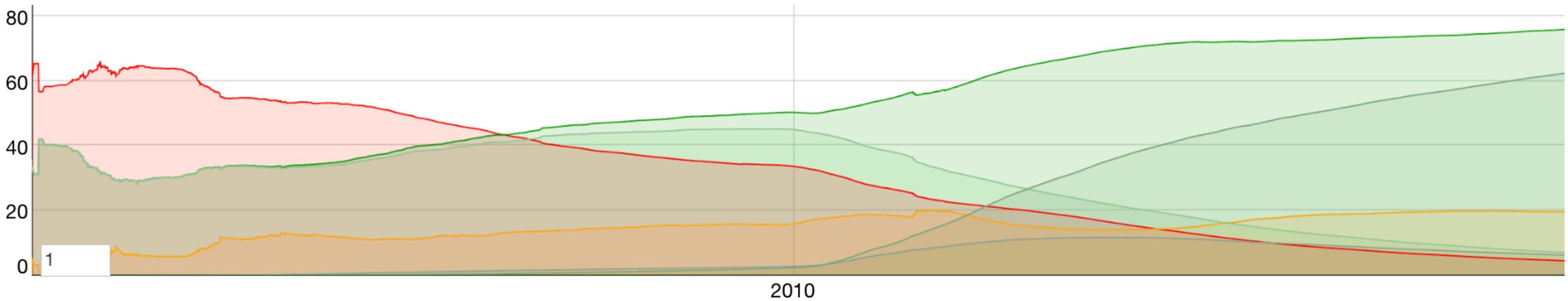
wigle.net Statistics

WiFi Networks Over Time



[Full-screen Graph]

WiFi Encryption Over Time



[Full-screen Graph] [2 Years only Graph]

Mouse-over graphs to interact with data. Select a range to zoom in, double click to zoom back out. Modify the number in the corner to smooth over multiple days. Full-screen graphs available!

wigle.net Statistics

- Wifi based attacks are a real thing.
- Do you know "everything" that is connected to your network?
- How would you find a "rogue AP?"
- Are you sure that "free wifi" is a legitimate service ?
- Wifi is the easiest entry point for further exploitation.

Help Net Security, Help Net Security
June 8, 2018

Wi-Fi phishing attacks discovered around Atlanta City Hall

As Atlanta continues to fully recover from March's ransomware attack, new evidence discovered today by Coronet reveals hundreds of active Wi-Fi phishing attacks currently ongoing both inside of and in close proximity to Atlanta City Hall.

The research also found attacks currently underway in Georgia's State Capitol Building, which is just a few blocks away. In total, Coronet identified 678 active threats within a 5-mile radius of Atlanta's City Hall.

The threats

Specifically, Coronet has validated that an undetermined number of attackers are currently deploying advanced phishing techniques, including but not limited to Evil Twins, Captive Portals and ARP poisoning, in what is likely their attempt to gain unauthorized access to user credentials to cloud services that the government relies on for daily business operations and continuity.

SECURITY

CPSC asks: How dangerous is the internet of things?

The US Consumer Product Safety Commission is investigating the safety of internet-connected devices.

BY **MOLLY PRICE** / MARCH 28, 2018 12:24 PM PDT

The US Consumer Product Safety Commission (CPSC) is holding a public hearing regarding the safety of internet-of-things (IoT) devices.

The hearing was announced in a notice published on the Federal Register Wednesday.

Amazon and eBay pull CloudPets smart toys from sale

6 June 2018 Share

Owners controlled audio recordings by pressing the toys' paws

Amazon and eBay are among retailers pulling a brand of cuddly smart toys from sale after warnings they pose a cyber-security threat.

Concerns were raised about CloudPets products in February 2017 after it was **discovered that millions of owners' voice recordings** were being stored online unprotected.

Manufacturer Spiral Toys claimed to have taken "swift action".

But subsequent research commissioned by Mozilla found other vulnerabilities.

The devices' California-based maker has not responded to requests for comment.

One independent expert told the BBC it was "great to see retailers acting responsibly", but added she wished they had done so sooner.

"It seems that refusing to sell products that threaten customers' security and privacy is the only way to make designers and manufacturers of these products care about these risks," said Angela Sasse, professor of human-centred technology at University College London.

Blueborn

Forbes

YOUR READING LIST


Critical Bluetooth Flaws Put Over 5 Billion Devices At Risk Of Hacking

+1447 views in the last 24 hours


Ant Financial Raises $14B To Fund Global Expansion

+132 views in the last 24 hours


Upstart ByteDance Challenges Tencent With Its Douyin Music App

Active on Facebook


Chinese Giant Ping An Looks Beyond Insurance To A Fintech Future

+1931 views in the last 24 hours


Blockchain Is Critical To The Future Of Data Storage -- Here's Why

+747 views in the last 24 hours


This Hong Kong 'Smart Ring' Startup Raised $2.5M To Crack The Wearables Market

+551 views in the last 24 hours

South Korea's Richest

SEP 12, 2017 @ 09:23 AM 9,143

The Little Black Book of Billionaire Secrets

Critical Bluetooth Flaws Put Over 5 Billion Devices At Risk Of Hacking

Lucian Constantin, CONTRIBUTOR

I cover malware, vulnerabilities, data breaches and security research. FULL BIO

Opinions expressed by Forbes Contributors are their own.

Shutterstock

Bluetooth is one of the most popular short-range wireless communications technologies in use today and is built into many types of devices, from phones, smartwatches and TVs to medical equipment and car infotainment systems. Many of those devices are now at risk of being hacked due to critical flaws found in the Bluetooth implementations of the operating systems they use.

Over the past several months, a team of researchers from IoT security firm Armis have been working with Google, Microsoft, Apple and Linux developers, to silently coordinate the release of patches for eight serious vulnerabilities that could allow attackers to completely take over Bluetooth-enabled devices or to hijack their Internet traffic.

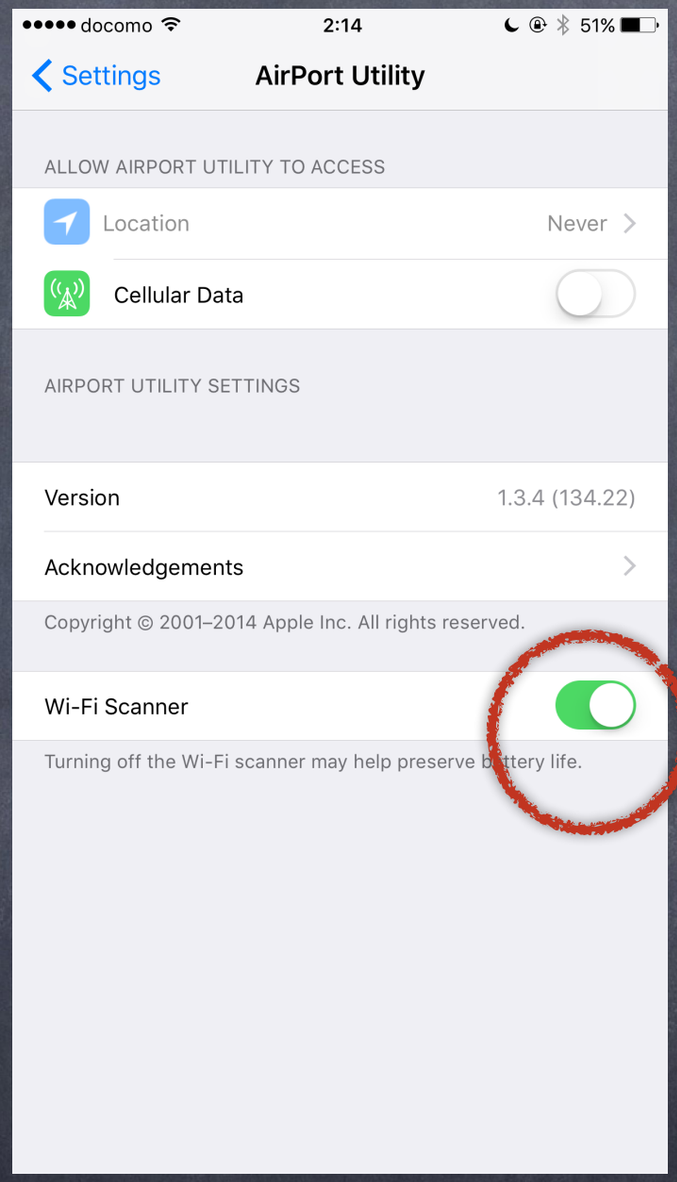
The flaws found by Armis are particularly dangerous because they can be exploited over the air without any type of authentication or device pairing. Simply having Bluetooth enabled on a device is enough to make it vulnerable if patches for these issues are not installed.

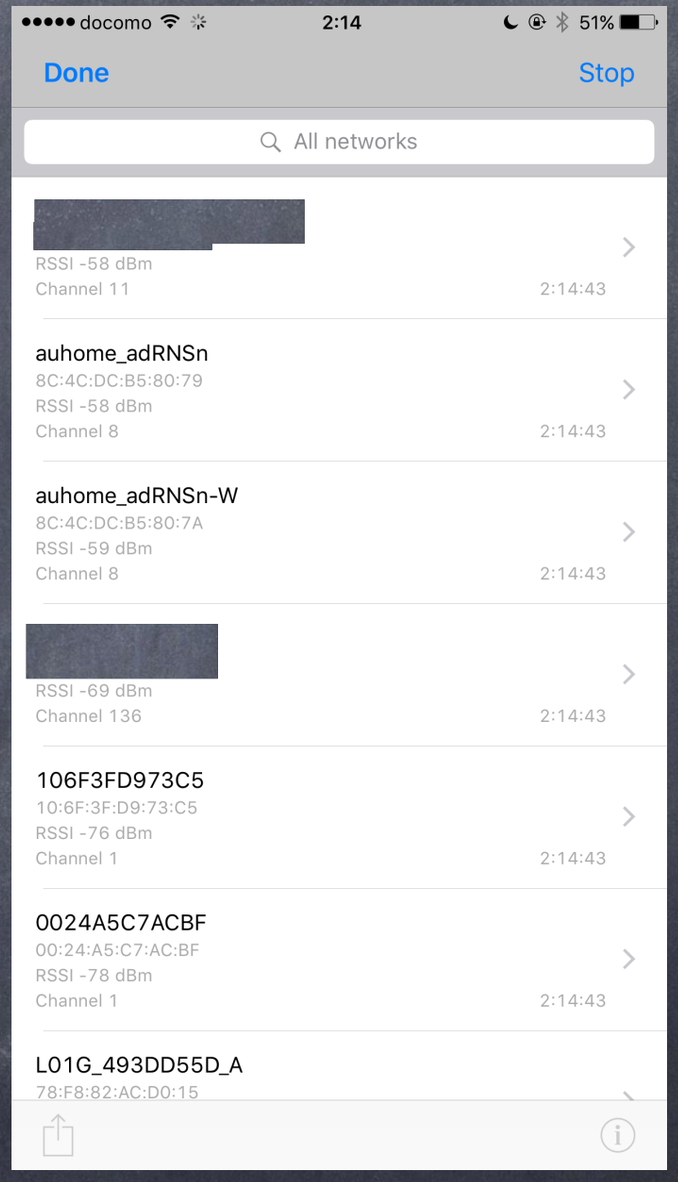
The attacks can be fully automated and they don't require any user interaction, as attackers can force vulnerable devices to open Bluetooth connections. In one scenario, the flaws can be used to build a worm-like

What tools to use?

- Phones/mobile devices.
  - iOS: Even non jail-broken phones you can scan for 802.11 access points.
  - Android: Wiggle client, net hunter Kali etc etc.
- Laptops: using a external 802.11 adaptor. Many single on-board multi protocol chips dont work for "monitor" mode. (ie: intel chipset etc)
- Custom tools:
  - Wifi Pineapple by Haks
  - Many "commercial" and "industrial options" are being sold.

Yes you can use an iOS device to scan





You have to enable the "wifi Scanner" option under "Settings"

DIY: Why?

- You can start with 1 computer and 1 wireless adaptor.
- You can add more adaptors as you need.
- You will learn the fundamentals.
- It usually is "cheaper" than commercial equipment.
- It only has to work for you.

When you get "hooked on wifi"

Specialized Car for wardriving

% @aadvark

Wifi Cactus

% @d4rkmatter

Custom Case and

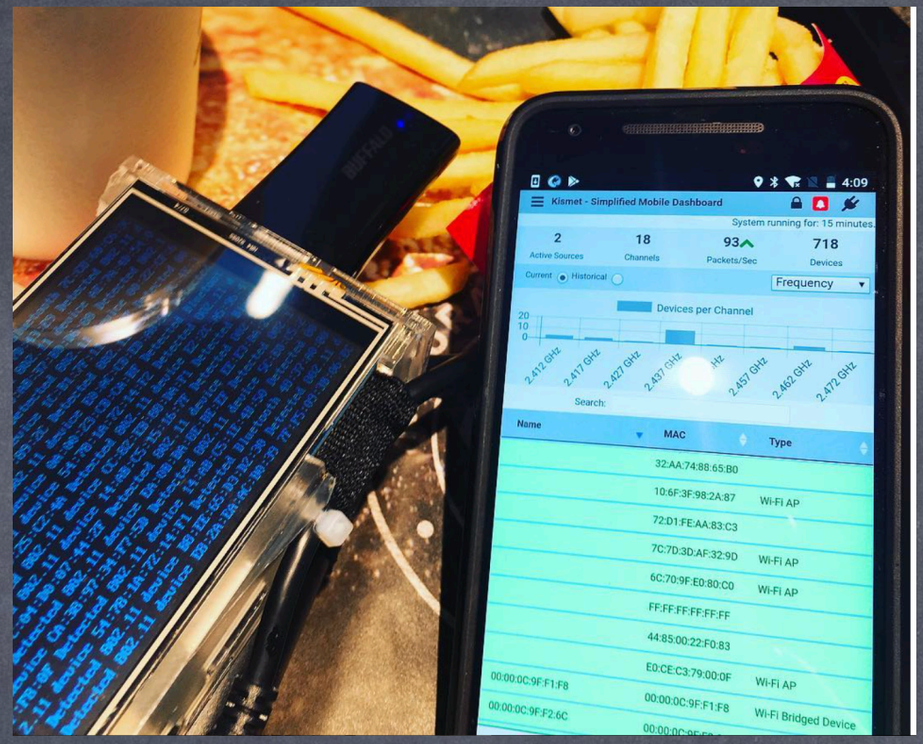
lots of zip ties (8 radios)

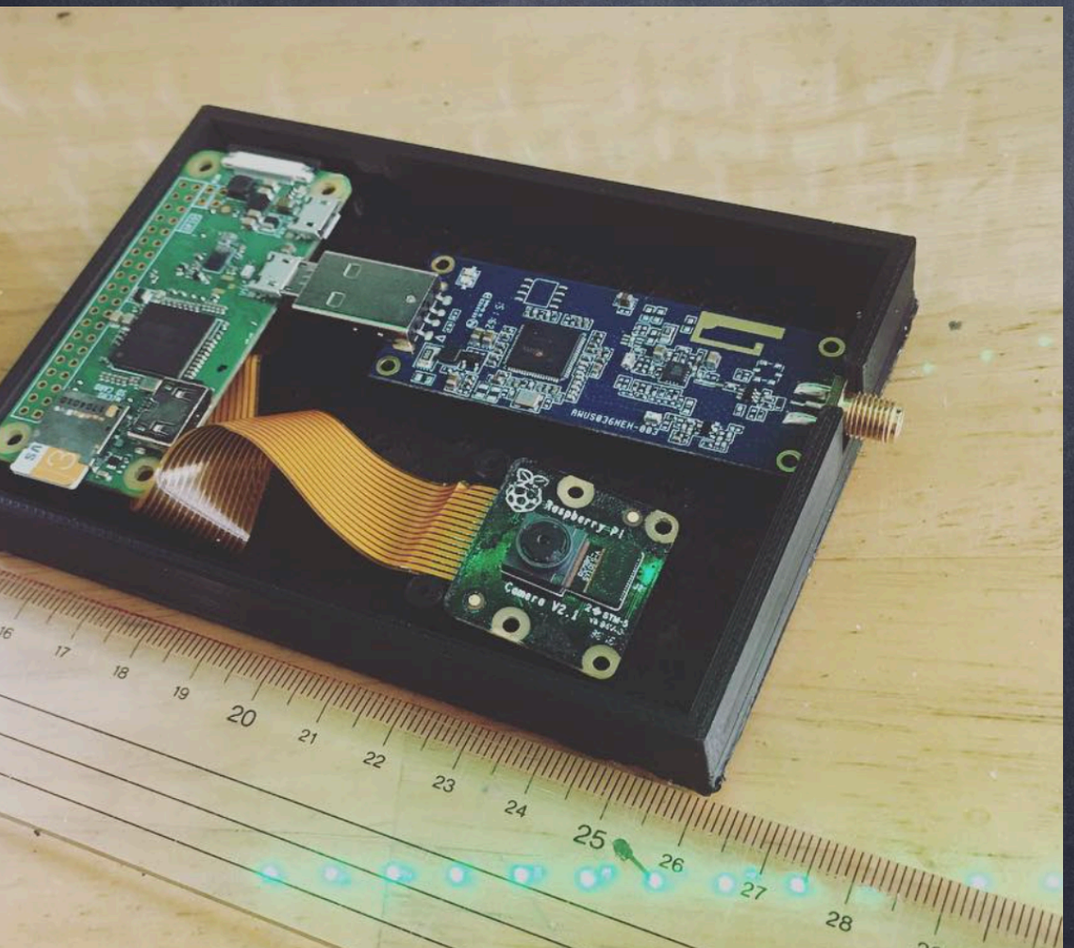
% @kismetwireless

My First time
2014 / Oct.

Its not really
"airport security"
friendly

HackChip





Wifi Centipede

"Makers gonna make"

- Unknown.

The basics.

- The solution is both hardware and software.
- We are going to focus on non-sdr solutions.
- Using SDR is like bringing a nuclear bomb to a bar fight .
  - It will "take care" of everything.
  - Its hard to setup in the beginning
  - Usually higher costs.

Let's build one.

Case Study of building a mobile packet capture rig.

Parts List.

- Raspberry Pi 3+ x 1
- Alfa AWUS AWUS036NEH x 2
- 7 Inch TFT (Waveshare 7 Inch)
- Aukey USB Hub (data ports + power ports)
- Hard Case
- Keyboard
- Optional:
  - Mobile Battery
  - GPS receiver

The Outershell

- Layout all your parts in the case . BEFORE YOU DECIDE TO DRILL HOLES.
- Look for ABS based cases.
  - They are usually sold as , "gun cases" or "tool cases." (* they tend to be cheaper than official Pelican cases)
- Why ABS?
  - You can re-melt ABS to hide your mistakes.
  - ABS when heated cleans up really good.
  - Plastic causes almost no interference with reception.

Before

After

Other Tricks.

- Use masking tape to transfer patterns to a different surface.
- A good drill bit set is worth every penny. (many cheap drill sets are off-axis and/or inaccurate)
- Learn how to tap screw holes (Its super simple)

The "computer" part

- Raspberry Pi 3+ is a great platform.
  - Low power requirement.
  - Costs
  - Readily Available (not Rpi Zero W)
  - Great community support
  - Portability. (airport security friendly)

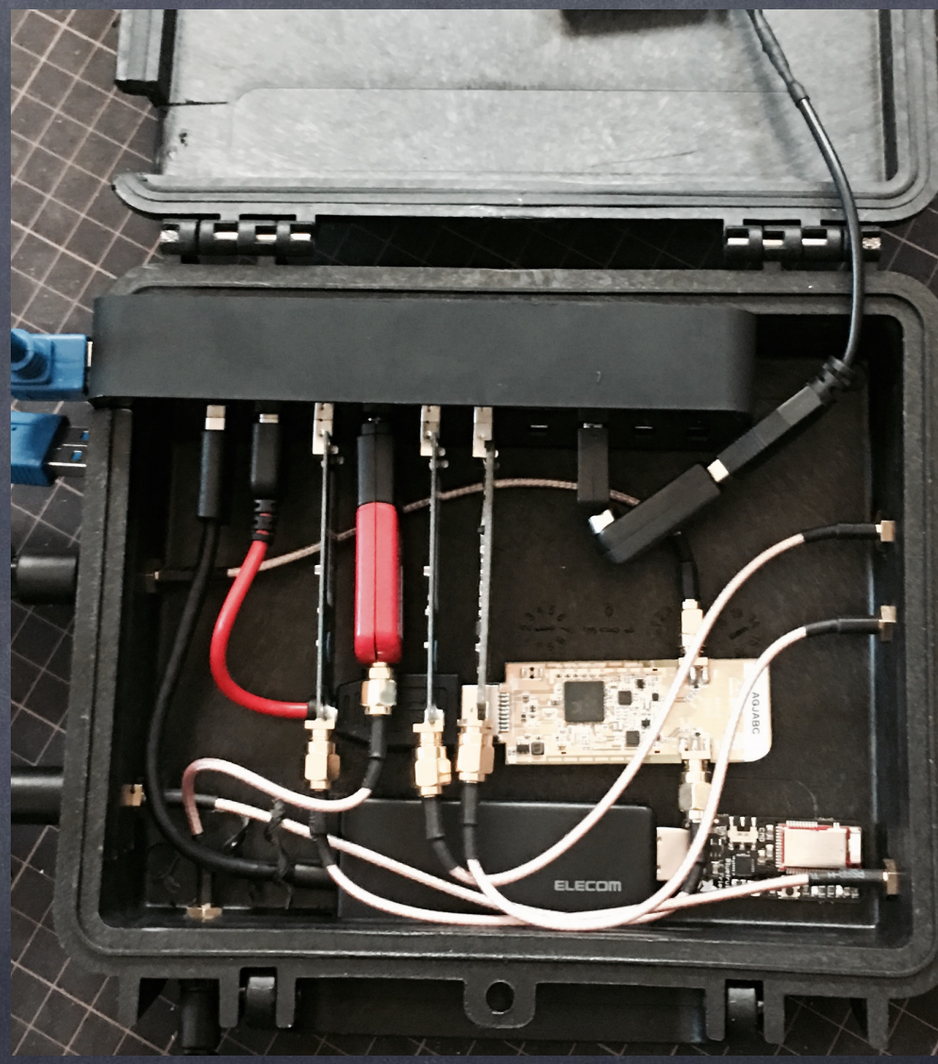
BUT!

The problems with a Rpi.

- The ethernet and USB are all on the same controller.
  - Capturing requires significant power to the usb.
  - Once the controller is saturated the RPi drops the whole controller.
- Not suited for in-depth analysis.
  - off load the analytics to a "real" computer.

Other options.

- Router with DD-WRT firmware.
- Intel Nuc
- Intel Nuc clones.(quality varies...a lot)
- or just build a case for your adaptors and use a laptop as your main computer. #donglelife.



The Adaptors. (802.11)

- Wikidev is your friend.
- Make sure that your adaptor supports "monitor" mode. (or packet injections if you want to "test attacks")
  - The TP-Link WN722N V1 vs. V2 debacle.
  - Atheros ATh9K is the gold standard.

State of the Database

- **5695** Wireless adapters
- **208** Ethernet adapters
- **4823** Wireless embedded systems
- **506** Wired embedded systems
- **116** mobile (non-PC) computers
- **221** USB hubs devices and
- **96** of everything else
- **7739** images, **1354** pages with images

AWUS 306NEH is my favorite.

Look for these chipsets.

- Atheros AR9271
- Ralink RT3070
- Ralink RT3572
- Realtek 8187L (Wireless G adapters)
- Realtek RTL8812AU

Typically the shop people have no idea.
Do the research before you go to a store or buy online.

Other protocols

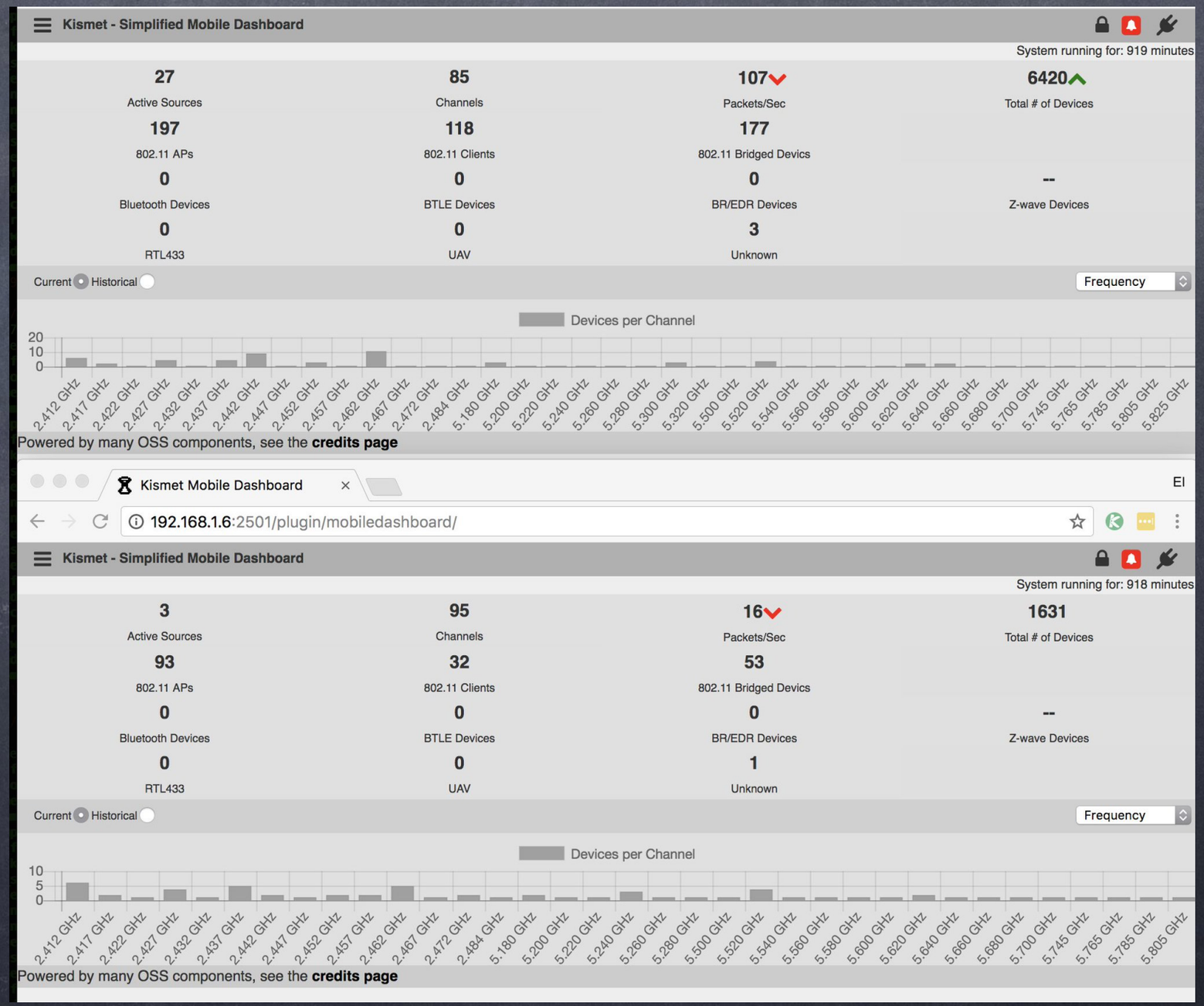
- Bluetooth: Sena Parani-UD-100 (very hard to find)
- BTLE.

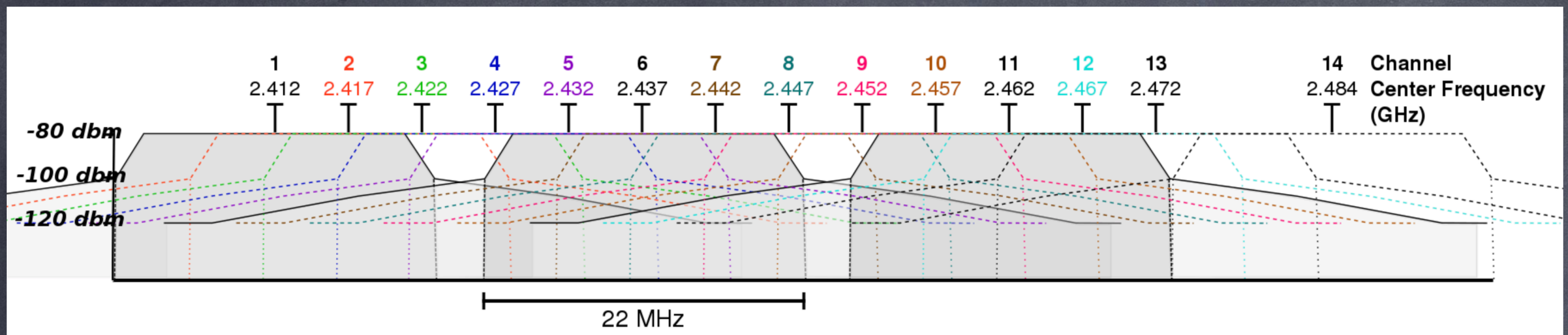
- Pretty much any BTLE external adaptor will work

How Many Adaptors do you need ?

- The more is better.
- But 3 will do . (for 2.4Ghz)
- Depends on your needs.

(27 vs 3)





This is also why your wifi might suck.

(ie:oversaturated channel)

Other parts. (cables & antennas)

- AliExpress is your friend.
- Be careful SMA Male/ Female and RP-SMA Male/Female.(some sellers dont know what they are selling)

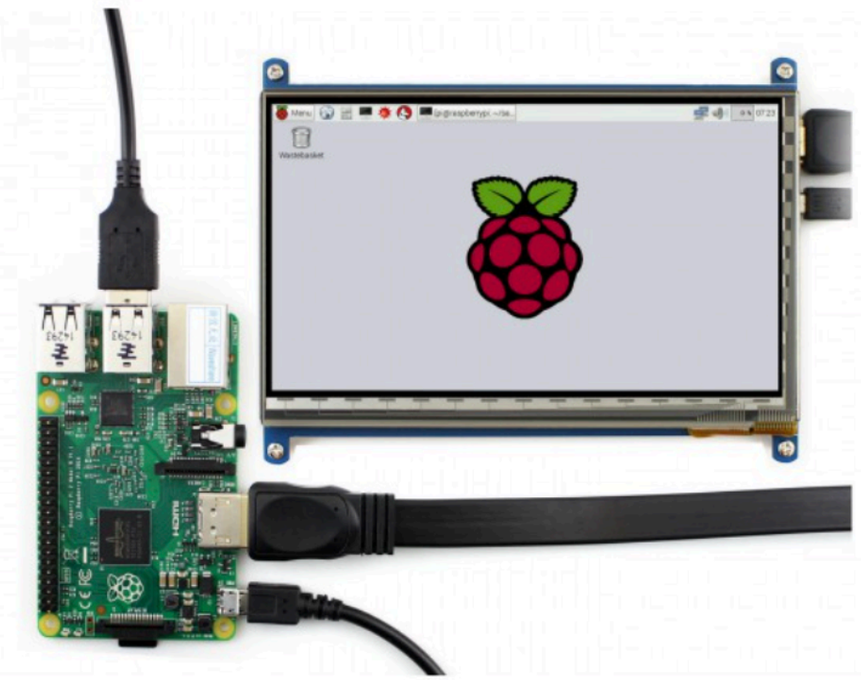
Thank you . FCC.🤦

Antennas: Yagi or Omnidirectional?

- Depends on what you aim to do.
  - Yagi's are great for "finding a specific network"
- But if you are GPS pin pointing, Yagi antenna finds will be mapped to your location.
- Omnidirectionals are better for wardriving and mapping.
- Is bigger antenna better?
  - Nope.

More Parts.

- 7 Inch LCD screen (7inch HDMI LCD, 1024x600, IPS, supports various systems)



- This is screen is great because it can be powered using a usb-micro connector.
- But it is sssloooooowwww.....
- The touch interface is painful. (ie: Use a mouse)

Optional Parts.

- Mobile Battery Pack.
  - Look for mobile batteries that can output to 12V.
    - Because many USB 3.0 hubs will take a external 12v power supply to handle the power requirements of usb connected devices.

- GPS
  - GlobalSat BU-353-S4 USB GPS Receiver
    - This one is my favorite. Its the quickest there are smaller USB dongles but they are very slow in capturing the satellite

Dual USB Plus Another DC Output
Supports simultaneously charging for 3 devices

Roll over image to zoom in

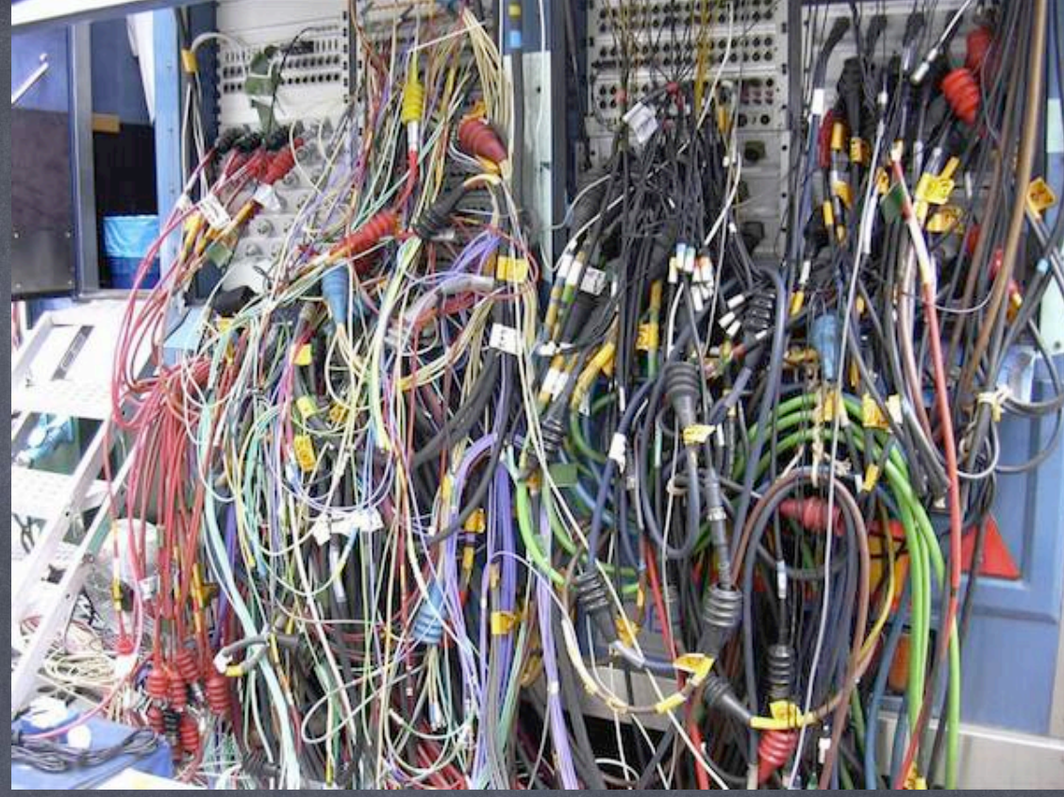
"The whole is greater than the sum of its parts"

-Aristotle

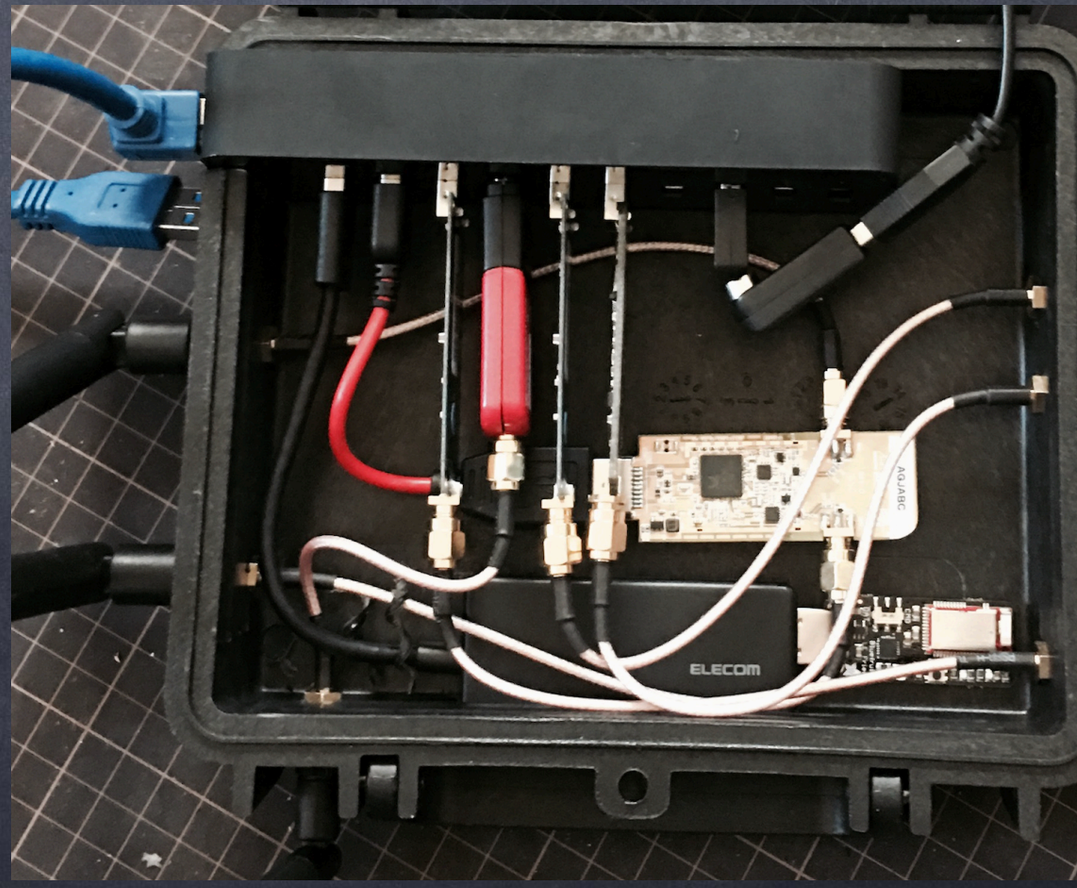
Putting it all together.

Tips and Tricks of putting it together.

- Avoid rat nests. (ie; Cable hell)
- Try minimizing cable usage.
- Use OTG power only micro USB cables for power. (no back-feeding into the usb)



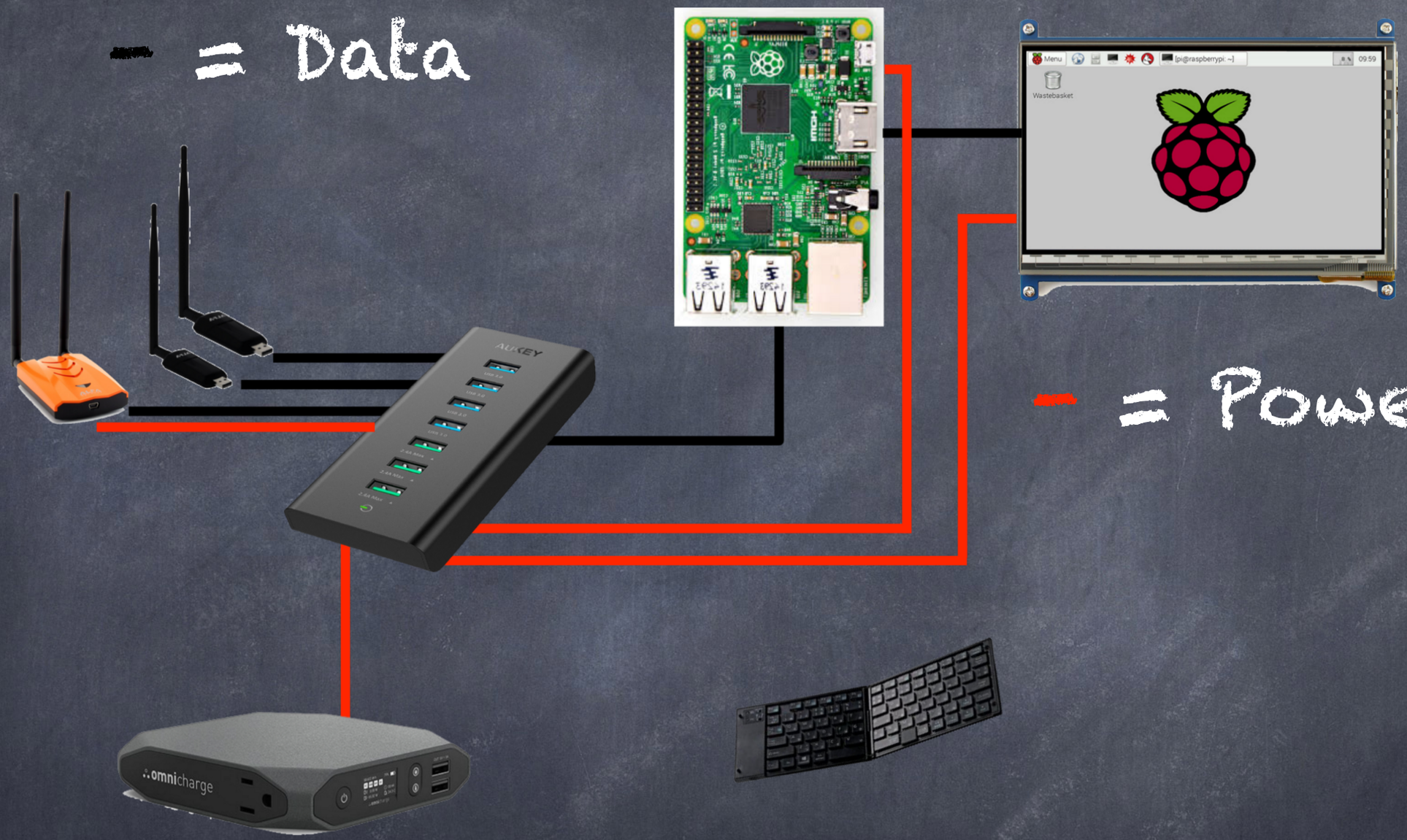
Rat Nest



2 Cables (1 usb and 1 power for 6 adaptors)

Overview of Setup

= Data



= Power

By using a USB hub with power-only ports we can power both the raspberry pi and the LCD screen

"Software."

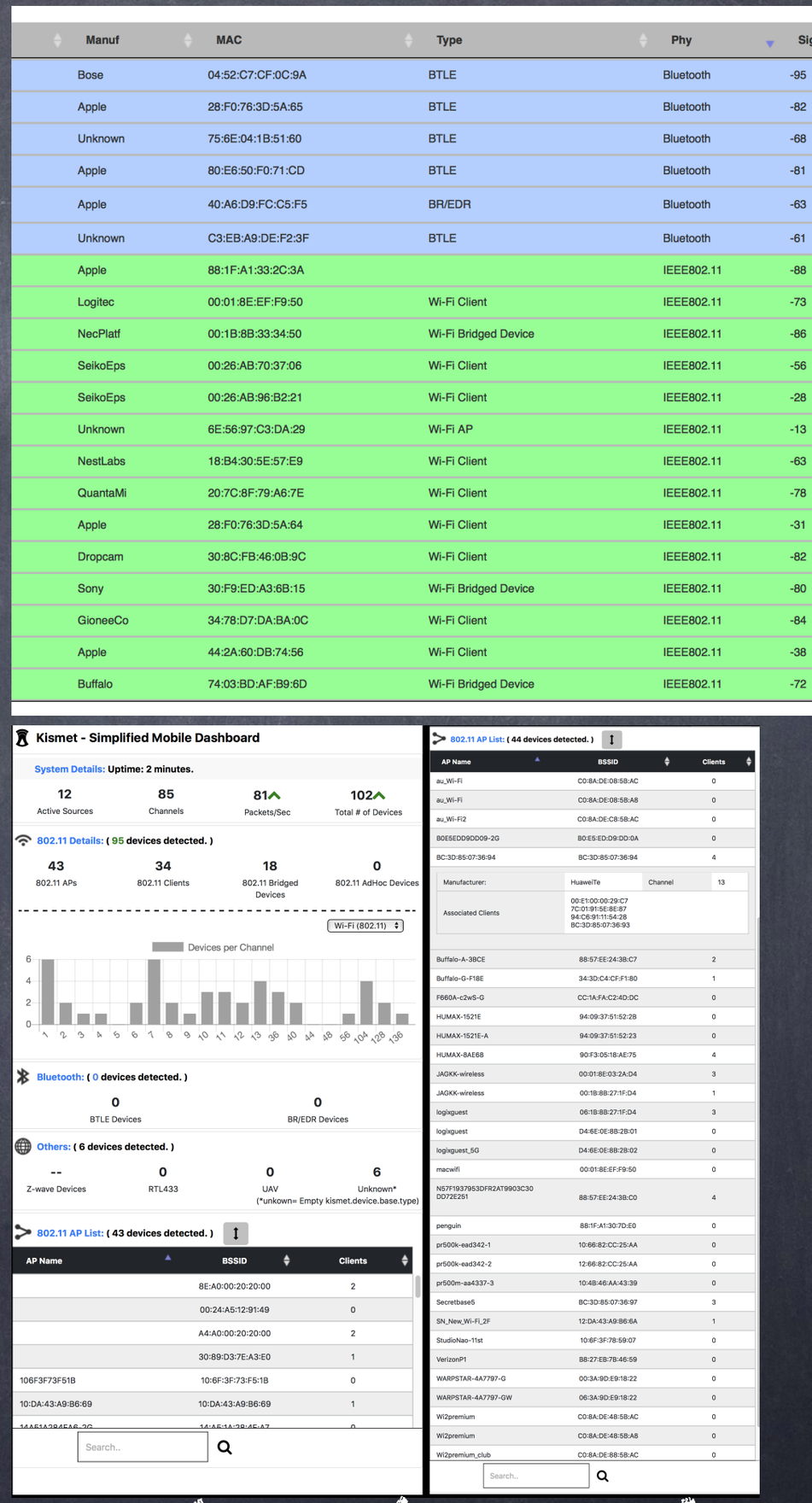
Is Kali the best?

- I rarely use a "full Kali" install.
  - I only need "wireless" related packages.
  - Raspi Stretch is fine as a base to customize.
    - Less driver issues.
    - Extensibility
    - Well maintained/documented
- Pentoo
  - Distro specifically for wireless
    - getting it up and running is painful

The sauce: Software

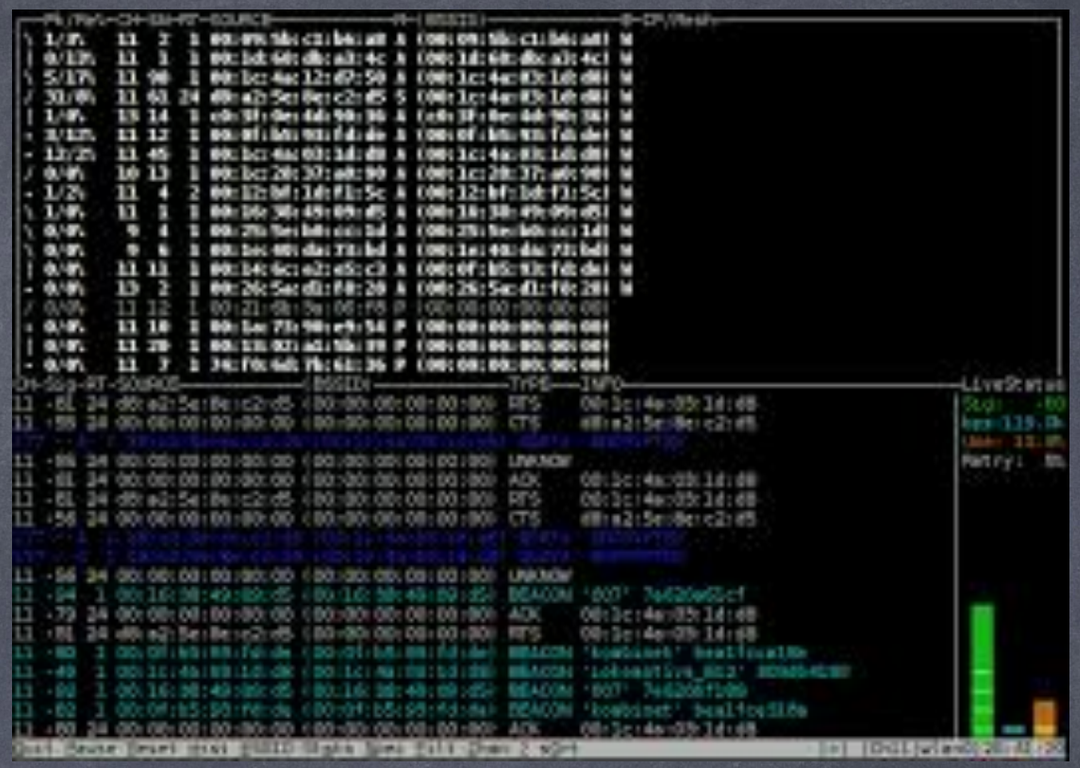
- Kismet (git -master:)
  - The gold standard for wireless related recon.
- Covers a lot of protocols. (802.11,BT,Drones, RTL433,Zigbee)
- Extensive API / extendable via python
- Multiple platforms
- Great community

- https://github.com/kismetwireless/kismet



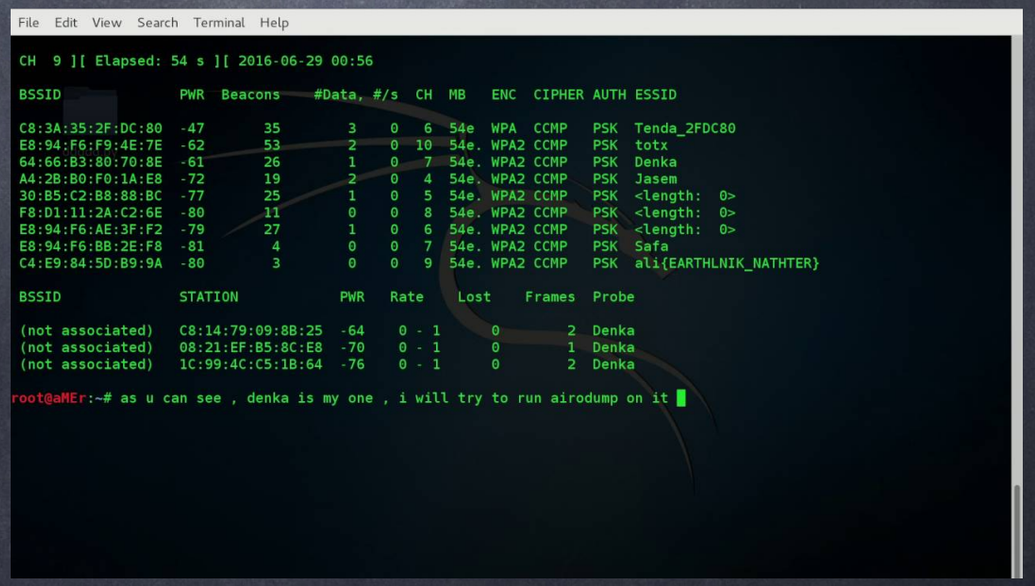
The sauce: Software

- HORST
  - Super lightweight wireless scanning tool



http://br1.einfach.org/tech/horst/

- Airodump-ng
  - Integration into the aircrack-ng

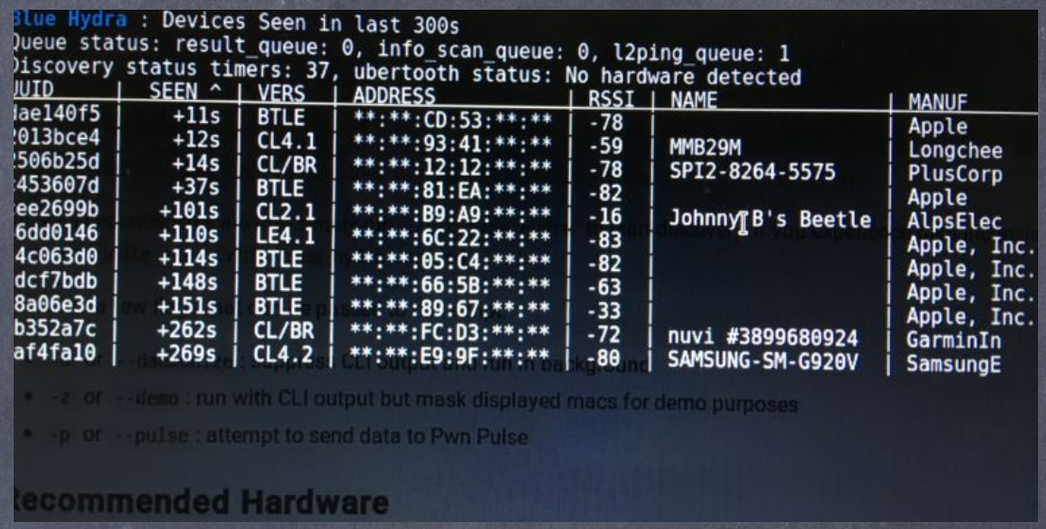


https://www.aircrack-ng.org/

BTLE

BlueHydra

- BTLE scanner. Works great with Ubertooth one to detect "non-visible" BTLE devices.



BLEAH

- Great details on BTLE device.
- Connect to BTLE

WARNING: READ THE DOCUMENTATION!

BETTERCAP

The Swiss Army knife for 802.11, BLE and Ethernet networks reconnaissance and attacks

```
bettercap v2.0.0 (type 'help' for a list of commands)

10.0.2.0/24 > 10.0.2.15 » help

     help MODULE : List available commands or show module specific help if no module name is provided.
           active : Show information about active modules.
             quit : Close the session and exit.
    sleep SECONDS : Sleep for the given amount of seconds.
        get NAME : Get the value of variable NAME, use * for all.
  set NAME VALUE : Set the VALUE of variable NAME.
            clear : Clear the screen.
  include CAPLET : Load and run this caplet in the current session.
       ! COMMAND : Execute a shell command and print its output.
  alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

       api.rest > not running
      arp.spoof > not running
      ble.recon > not running
    dhcp6.spoof > not running
       dns.spoof > not running
  events.stream > running
     http.proxy > not running
    http.server > not running
    https.proxy > not running
    mac.changer > not running
      net.probe > not running
      net.recon > running
      net.sniff > not running
       syn.scan > not running
      tcp.proxy > not running
         ticker > not running
     wifi.recon > not running
            wol > not running

10.0.2.0/24 > 10.0.2.15 » exit

Stopping modules and cleaning session state ...
```

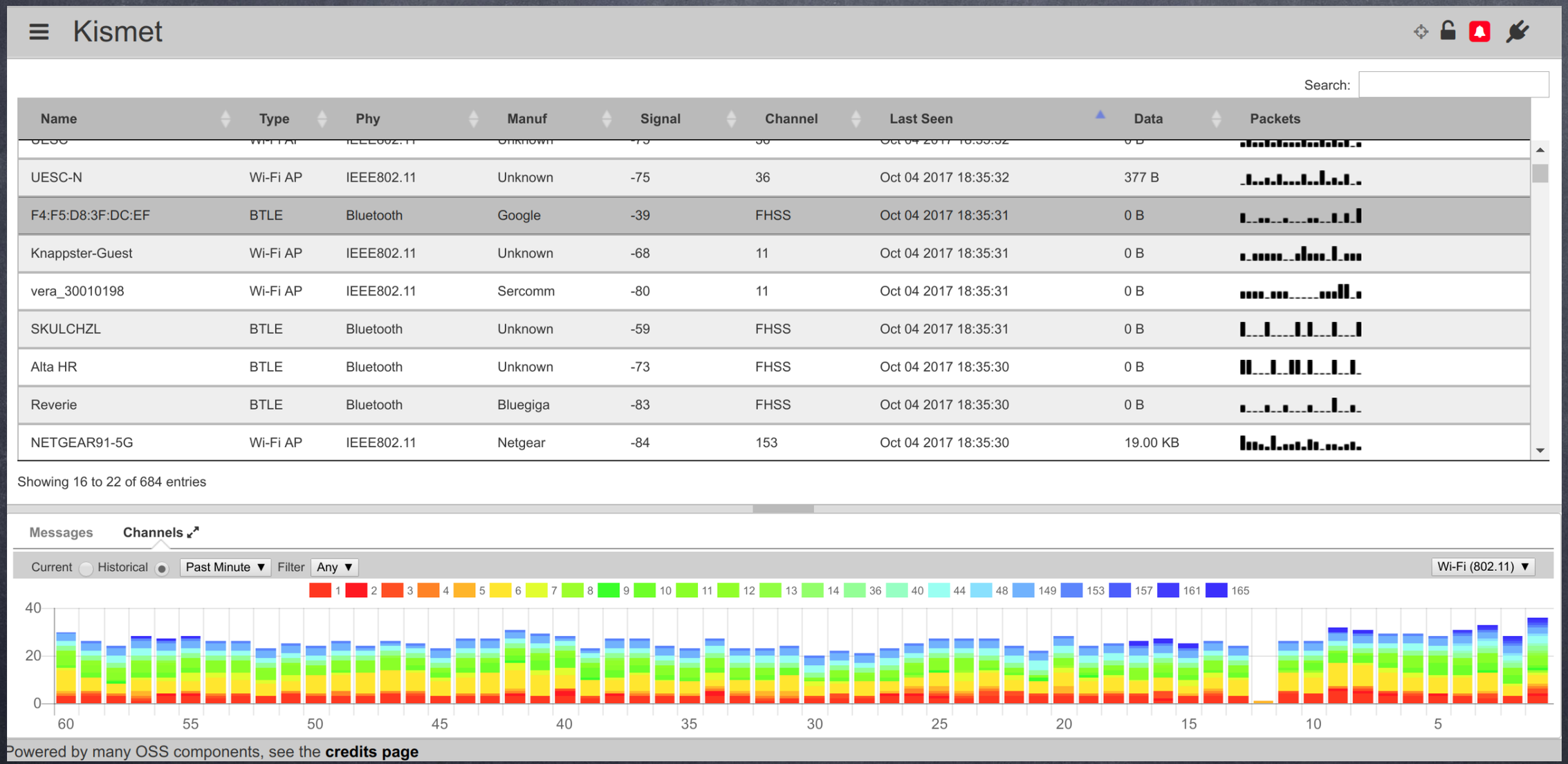
https://github.com/bettercap/bettercap

WARNING: READ THE DOCUMENTATION!

Quick Intro to Kismet

- There are 2 version of Kismet.
  - apt-get Kismet = older version of Kismet
  - git clone https://github.com/kismetwireless/kismet.git
    - (what we users refer to kismet-git-master)
- USE THE NEW VERSION.

The Interface(s)



The main interface

The Interface(s)

Device Details

Device Info

Name	VW BT 7871
MAC Address	AC:7A:4D:35:C1:DE
Manufacturer	AlpsElec
Type	BR/EDR
First Seen	Wed Oct 04 2017 12:08:42 GMT-0400 (EDT)
Last Seen	Wed Oct 04 2017 12:08:43 GMT-0400 (EDT)

Frequencies

Channel	FHSS

Signal

Monitor Signal	**Monitor**
Latest Signal	-78 dBm
Min. Signal	-78 dBm
Max. Signal	-76 dBm

Packets

Total Packets	2

Packet Graphs

Dev/Debug Options

Device Details

Device Info

Wi-Fi (802.11)

Last Beaconed SSID (AP)	UESC
Last Probed SSID (Client)	UESC

Packets

Total Packets	8045789
LLC/Management	8042898
Data Packets	2891
Error/Invalid Packets	0
Fragmented Packets	0
Retried Packets	769
Data (size)	8.78 KB
Retried Data	0 B

WPA Key Exchange

Handshake Packets	17
Handshake PCAP	**Download Pcap File**

Advertised SSIDs

Packet Graphs

Seen By

Dev/Debug Options

Device Details

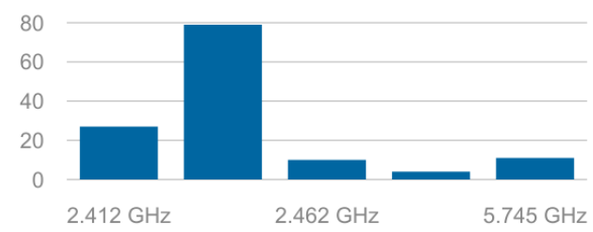
Device Info

Name	04:03:D6:71:39:27
MAC Address	04:03:D6:71:39:27
Manufacturer	Nintendo
Type	Wi-Fi Bridged Device
First Seen	Wed Oct 04 2017 11:00:10 GMT-0400 (EDT)
Last Seen	Wed Oct 04 2017 18:11:48 GMT-0400 (EDT)

Frequencies

Channel	*None Advertised*
Main Frequency	2.437 GHz

Packet Frequency Distribution



Signal

Monitor Signal	**Monitor**
Latest Signal	-68 dBm
Min. Signal	-92 dBm
Max. Signal	-11 dBm

Packets

Wi-Fi (802.11)

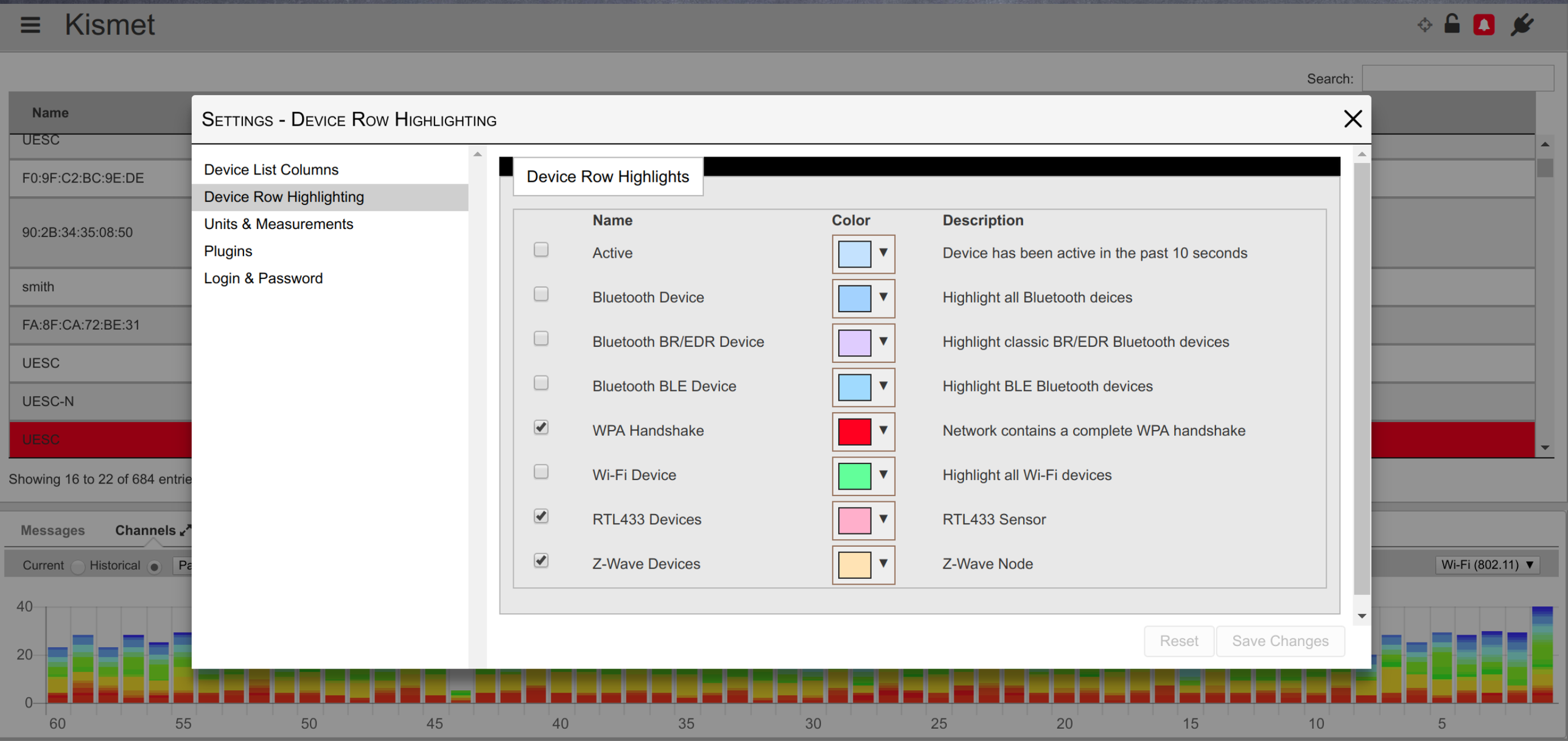
Packet Graphs

Seen By

Dev/Debug Options

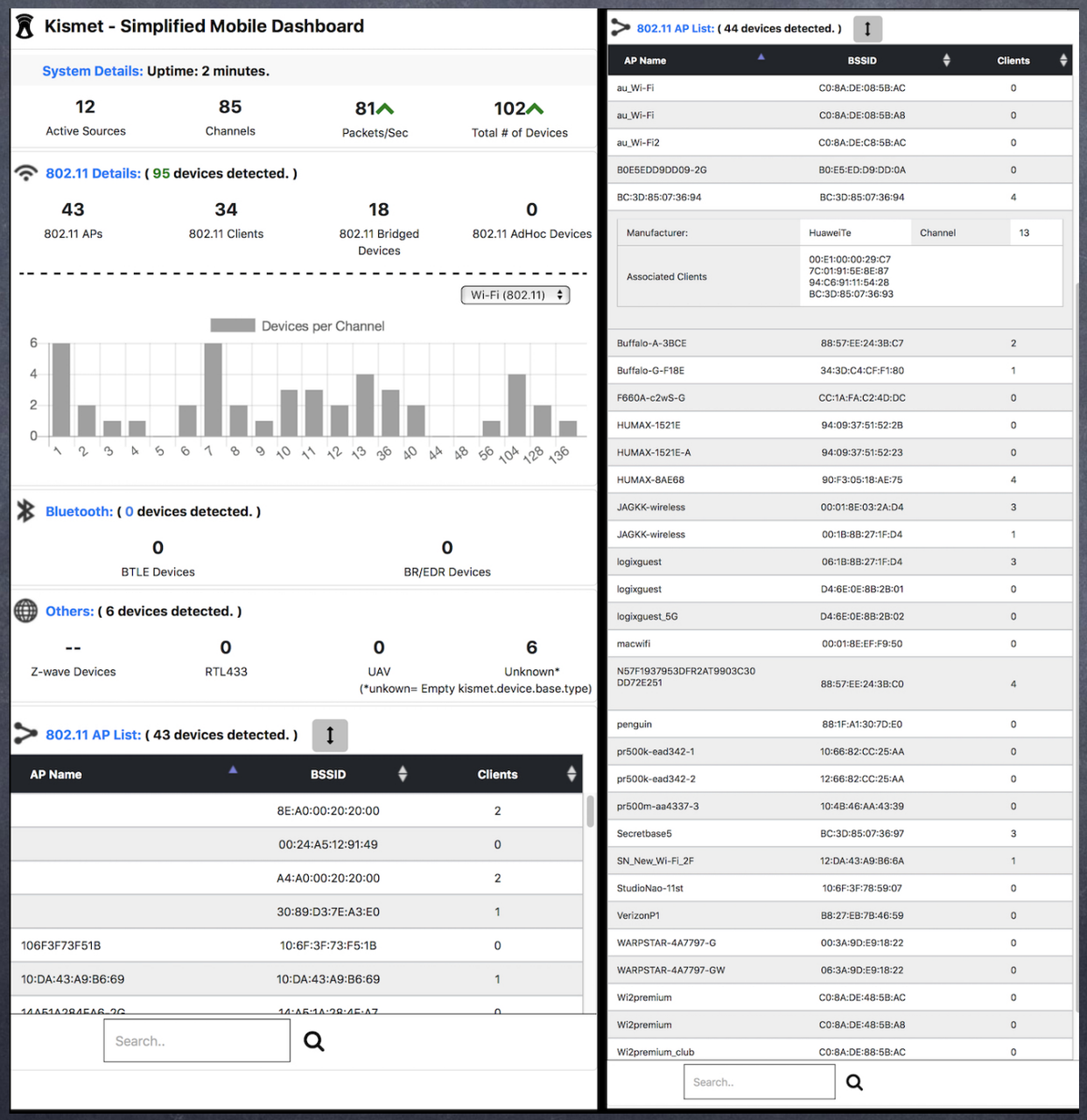
Device Data

The Interface(s)



Settings

The Interface(s)



The Kismet Mobile Dashboard (plugin)

Advantages of Using Kismet

- Comprehensive Data collection
- Supports multiple wireless protocols.
- Per Device data analytics.
- Remote monitoring capabilities.
    - Kismet remotes. (rpi-w,dd-wrt routers etc)
    - Kismet remotes can send data to a central Kismet server instance.
    - The central kismet server can handle the remote datasources as a local source.
        - (ie: Channel hopping etc)
- Open source
- Great support and community
- Very extendable

Disadvantages of using Kismet

- Requires modern web rendering capabilities. (ie:not suited for some SBCs)
- No offensive capabilities.
  - No packet injections
  - No rogue AP
  - no Deauth attacks
- No direct to wigle.net integration
- Technically still in "development" phase.
  - requires regular updates etc.

"I'll show you mine"

-El Kentaro

Video and Demo.(maybe)

Disclaimer: If you do not want to be detected, please put your mobile devices/laptops/Computers in "airplane" mode. now.

"Give a man a fish and you feed him for a day; teach a man to fish and you feed him for life"

-Undetermined origin

Question?

Thank you.

@elkentaro