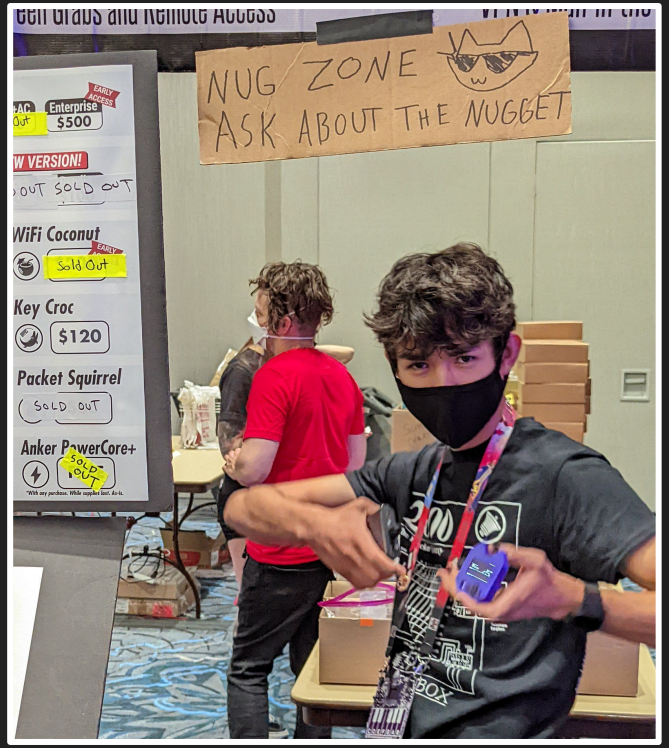
Nugget Wardriving

Basic Wardriving & Data Visualization

[Alex Lynd @ DEFCON Red Team Village]
LyndLabs 08/11/2023

Alex Lynd

- I make videos on the internet ;)
- I hack stuff
- @alexlynd // alexlynd.com



My Work

Wardriving Skateboard WiFi Recon w/ the Raspberry Pi

9.5K views • 4 years ago

How Companies Catch Ransomware Hackers

67K views • 1 year ago

How to Defend Against WiFi Attacks and WiFi Pineapples

19K views • 1 year ago

Can Linux Aliases Steal Your Password? (Bash Bunny Demo)

12K views • 1 year ago

How to Find Hidden Spy Cameras in your Airbnb with Wireshark

44K views • 1 year ago

Update Your Raspberry Pi Over the Air (with Thistle)

167 views • 1 month ago

Visualize WiFi Relationships with AirGraph-ng | HakByte

27K views • 1 year ago

Track WiFi Devices from the Air with a WarFlying Drone

24K views • 1 year ago

Create Rogue Networks on the WiFi Pineapple (PineAP KARMA Attacks)

53K views • 1 year ago

WiFi Coconut: Setup & Recon w/ Wireshark

39K views • 9 months ago

This stealthy device TRACKS YOU with OPEN WIFI NETWORKS

2.1K views • 1 month ago

CreepDetector: Detecting Stalkers with Wardriving

12K views • 3 years ago

How Hackers Exploit Log4J to Get a Reverse Shell (Ghidra Log4Shell Demo) | HakByte

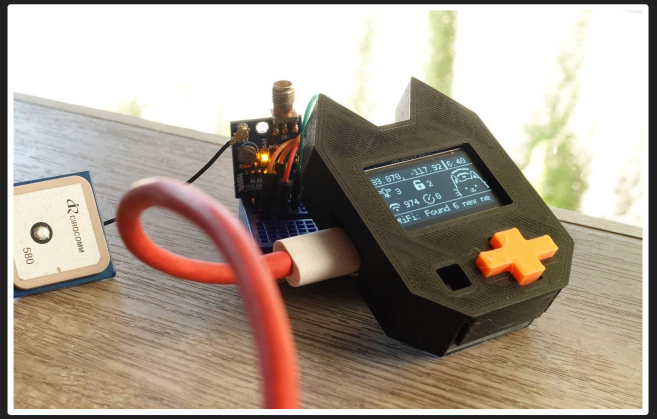
221K views • 1 year ago

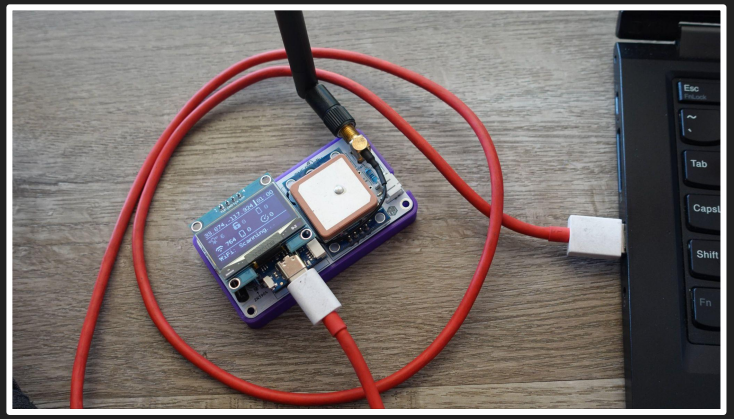
Easy Log4J Exploit Detection with CanaryTokens | HakByte

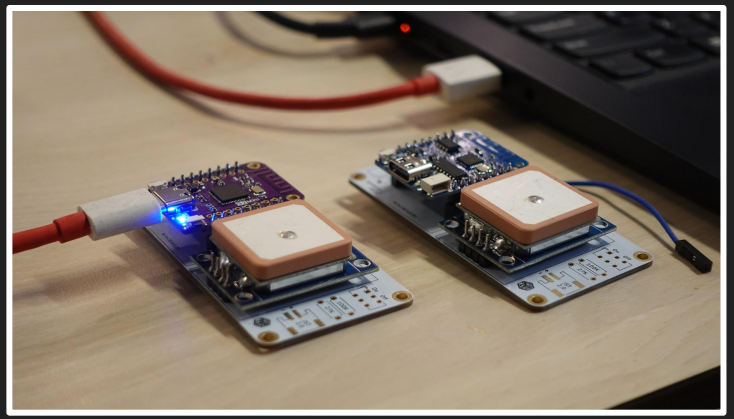
25K views • 1 year ago

How Hackers Use DNS Spoofing to Phish Passwords (WiFi Pineapple Demo)

48K views • 1 year ago

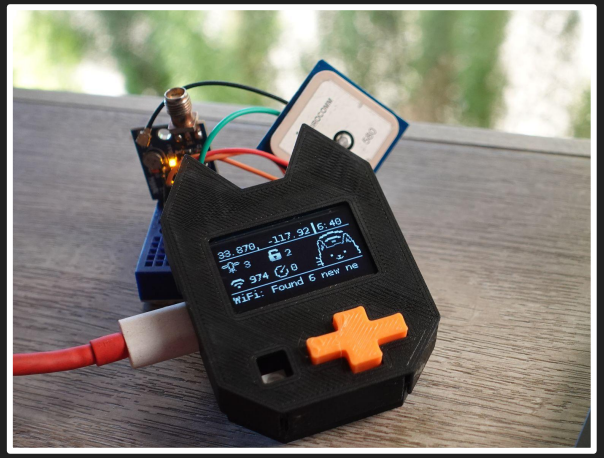

WiFi: Found 6 net

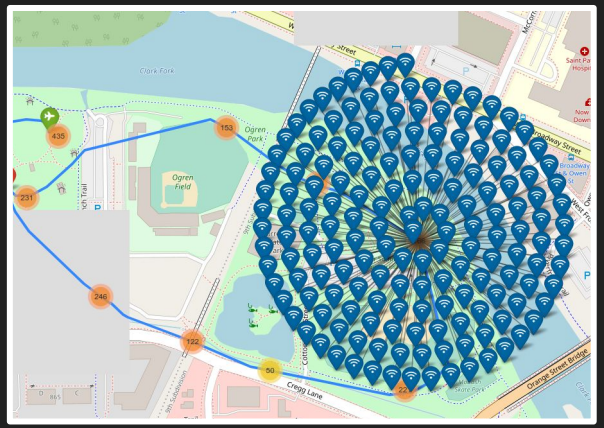




What you're doing today

- 🐈 Soldering a Cat-Shaped hacking tool
- 📡 Learning about Wardriving & WiFi Recon
- 🐍 Creating Interactive Maps through Python
- And more :)

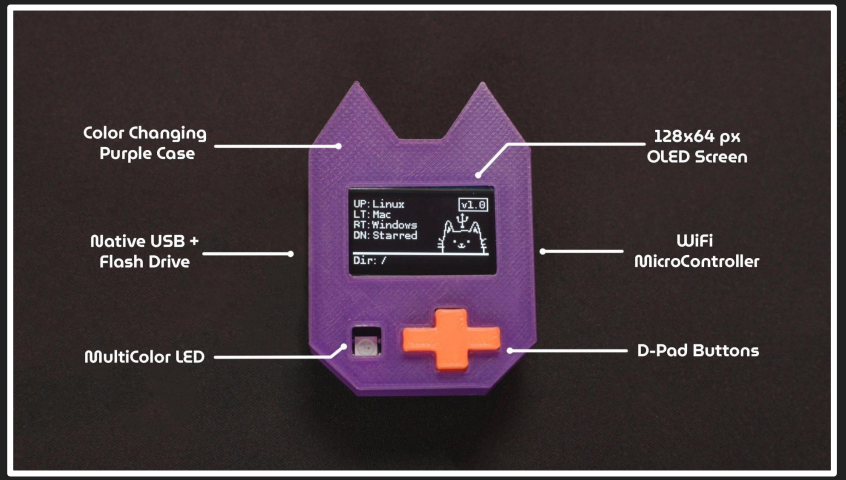




What is the Nugget?

The Nugget is a cat-themed console that makes it fun to learn hacking!

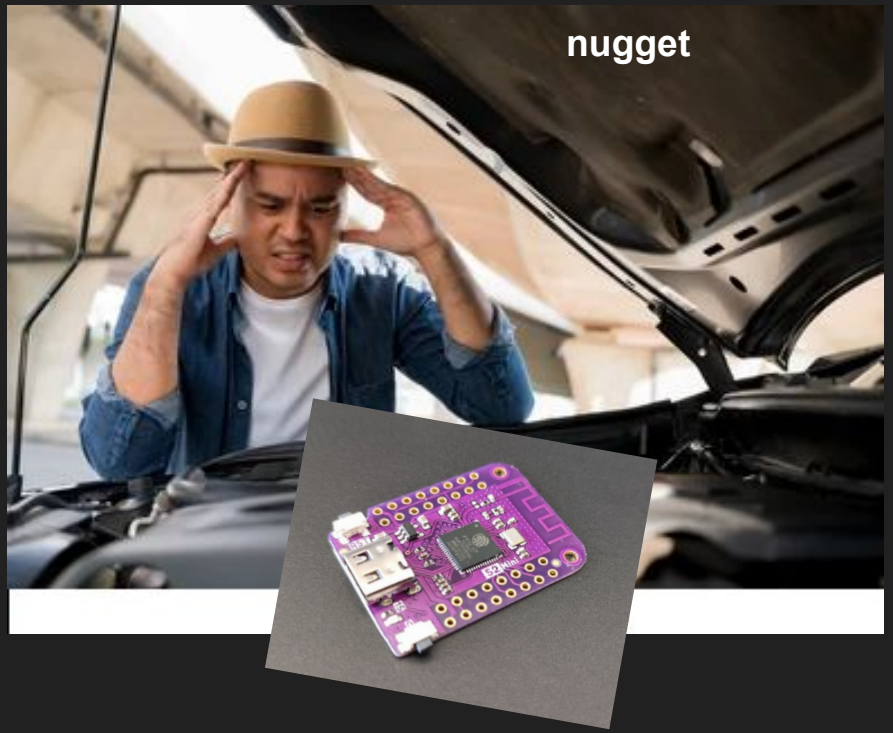
- WiFi & USB Hacking
- Hardware Prototyping
- CircuitPython & Arduino Support



What's under the hood?

ESP32-S2 microcontroller:

- **WiFi** (AP & Client mode)
- **Native USB**
  - Emulate USB Devices
  - Flash Storage
- **Easy Hardware Expansion**



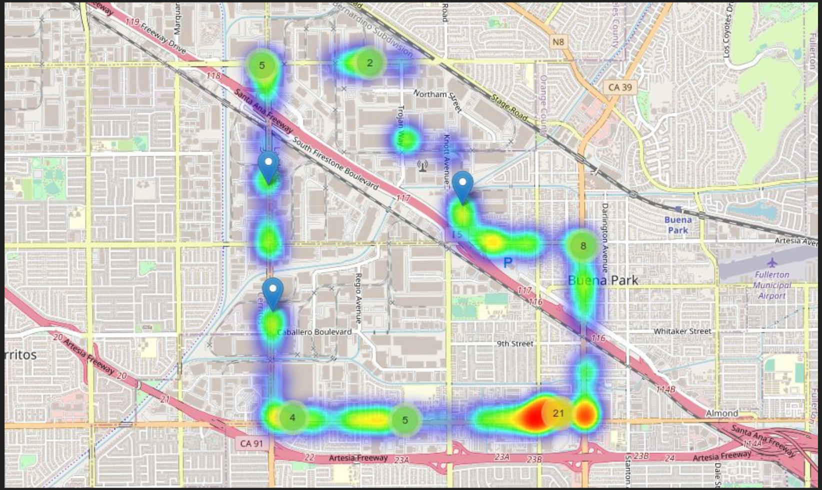
Wardriving

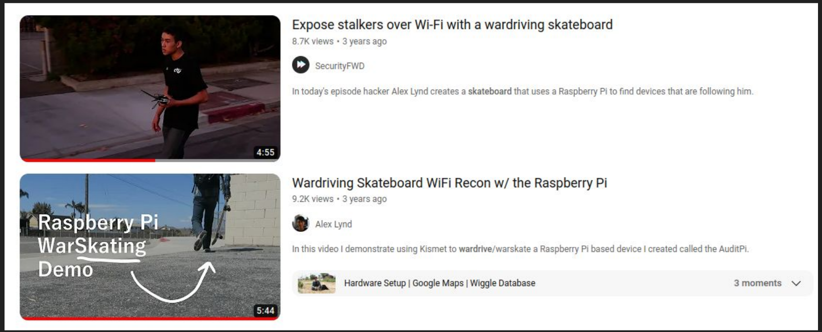
Basic Data Visualization & Recon

What is WarDriving?

- **Map** Wireless Devices!
- WiFi, Bluetooth, etc.

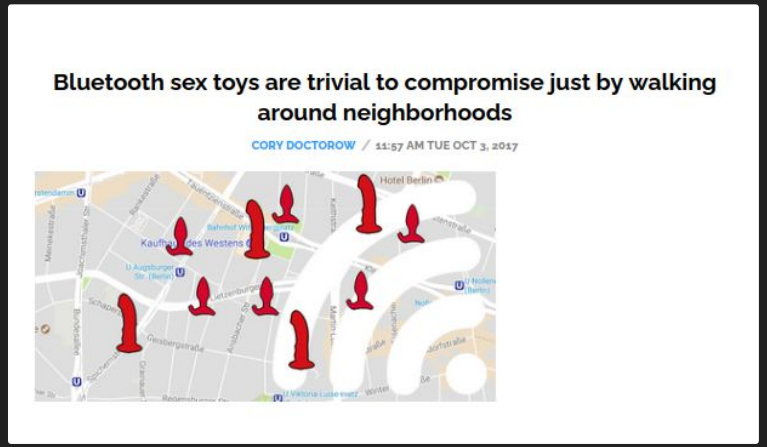
- Create Maps
- Data Visualization





Use Cases

- Detect Stalkers, or Friends!
- Discover vulnerable IoT Devices
- City Planning + Flow Metering
- Visualizations
- “Screwdriving” →

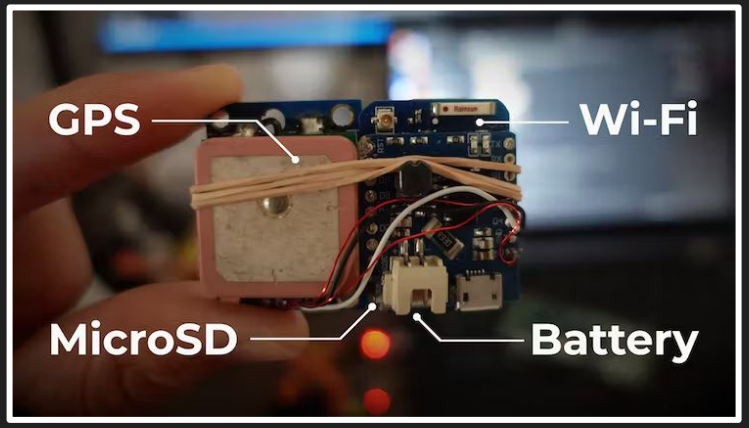


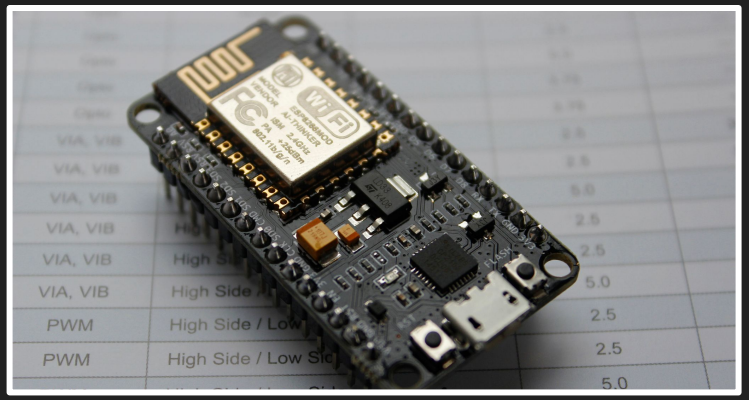
Why Microcontrollers?

- Low-Cost
- Small Form Factor
- Easy to Replicate

Espressif:

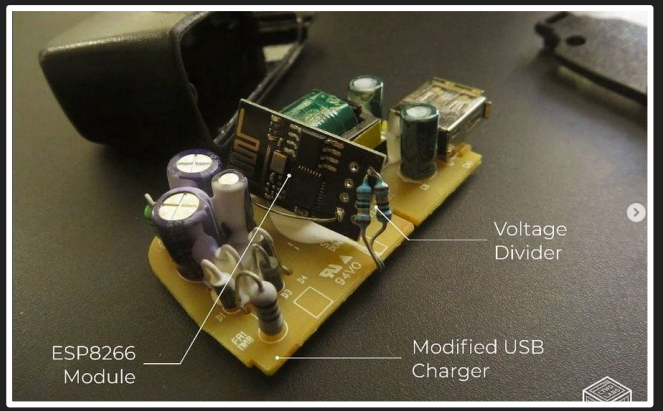
- WiFi Hacking & Recon
- ESP8266: $1-5





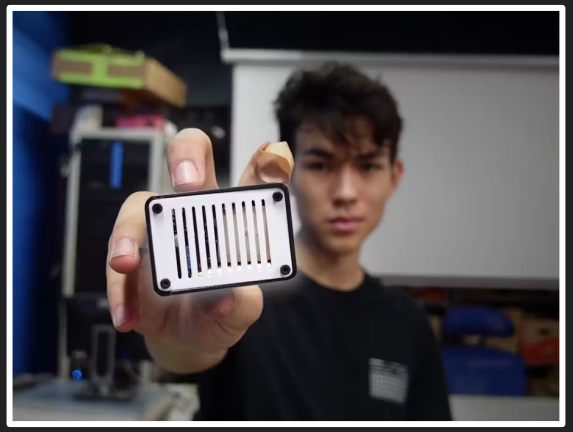
Disposable Payloads

$5 “**Warflying**” Drone Payload



Wall Charger Bug

Disposable Payloads



Low-cost tracking w/ Open WiFi: dnsdriveby.com

Warshipping: Recon in your company's mailroom

Nugget Wardriver

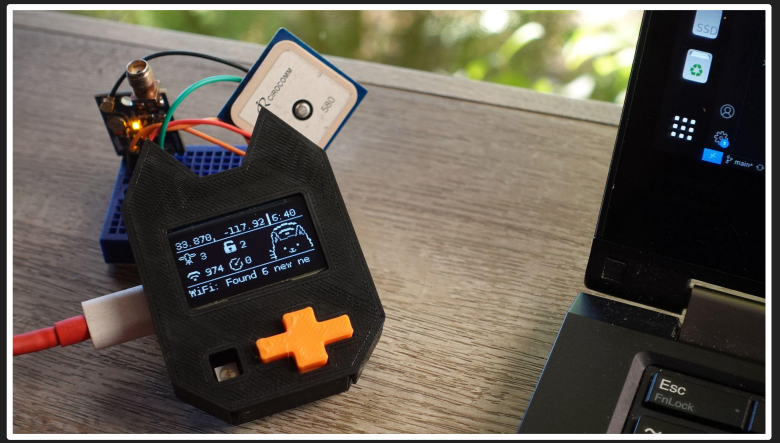
Cat-themed WiFi Recon!

Nugget Wardriver

Gather intel on WiFi networks & clients!

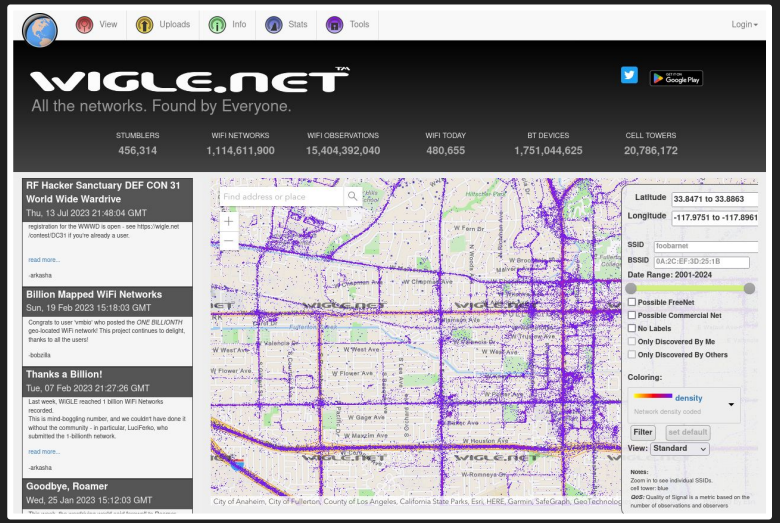
- Cat-Themed!
- Built-In Flash Drive for logs
- WiGLE.net compatible!
- Serial Monitor

Code: github.com/lyndlabs/wardriver



Wigle - Wardriving Database

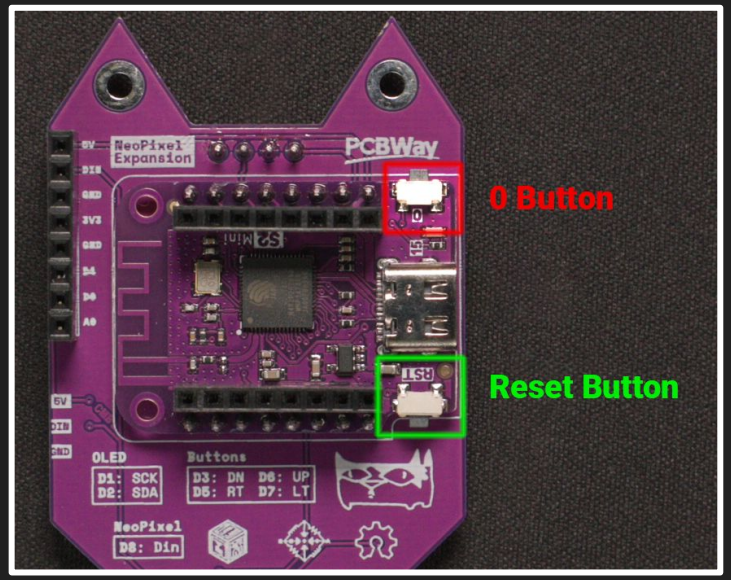
- Crowdsourced Wardriving
- Millions of Networks
- Mobile App & Kismet Compatible
- Open Source



Flashing the Firmware

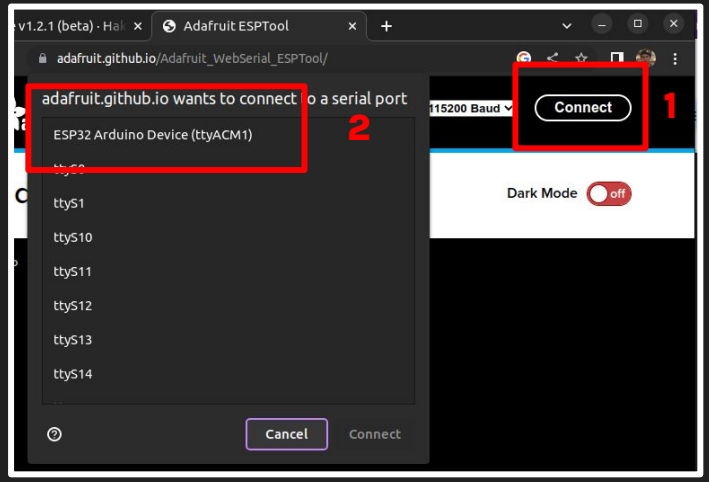
Let’s place your Nugget in “Flash Mode”!

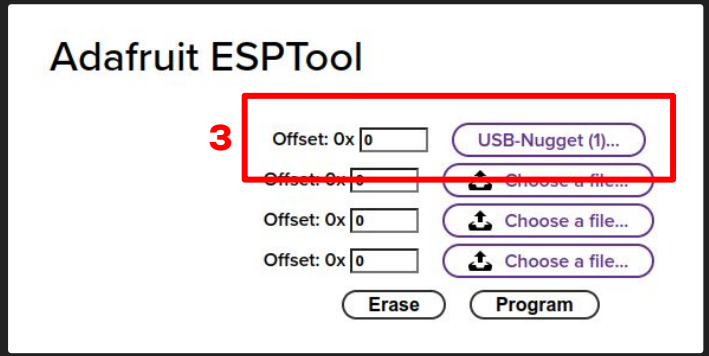
1. **Hold Down** the Boot / 0 Button
2. **Press** & release the Reset Button
3. **Release** the Boot / 0 Button
4. It’s ready to go!



Flashing the Firmware

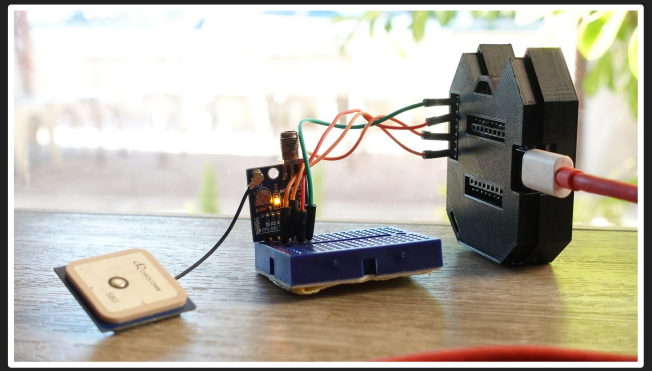
1. Download the Nugget Wardriver Binary FIle
2. Open the Web Flasher in Google Chrome
3. Connect to your Nugget, which should appear as an “ESP32” device
4. Upload the binary file & program it to your board!





Try it Out!

1. Hook up the GPS to your Nugget's expansion pins
2. Plug your Nugget into a power source
3. Monitor output via the screen, or serial!



Pinout at wifinugget.com

Visualize Data with Python

Jupyter Notebook

Jupyter Notebook makes data visualization easy!

- Browser-based
- Python!
- Maps, Charts, Graphs, etc.

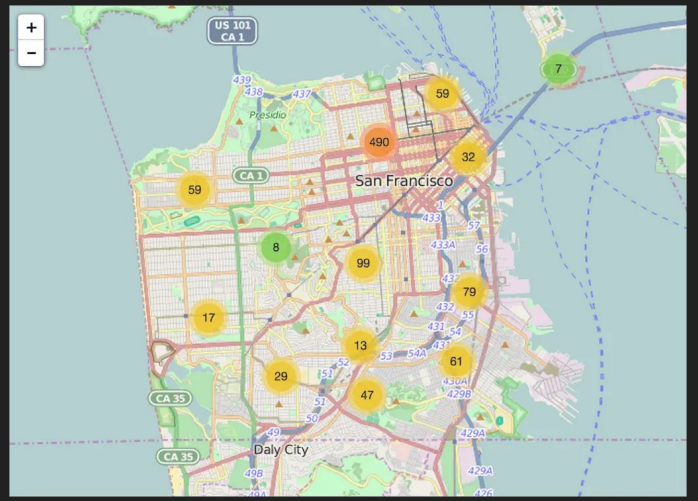
https://colab.research.google.com

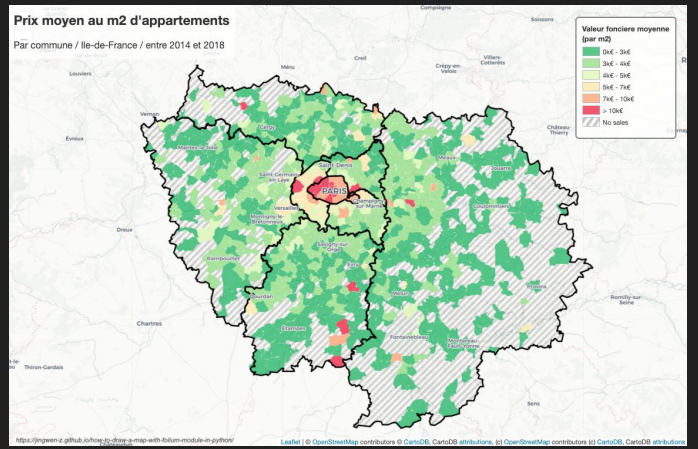
Folium

Folium is a Leaflet based Mapping Library!

- Map Styles (terrain etc)
- Annotations
- Heatmaps, Time Series, Cluster Maps

https://python-visualization.github.io/folium/

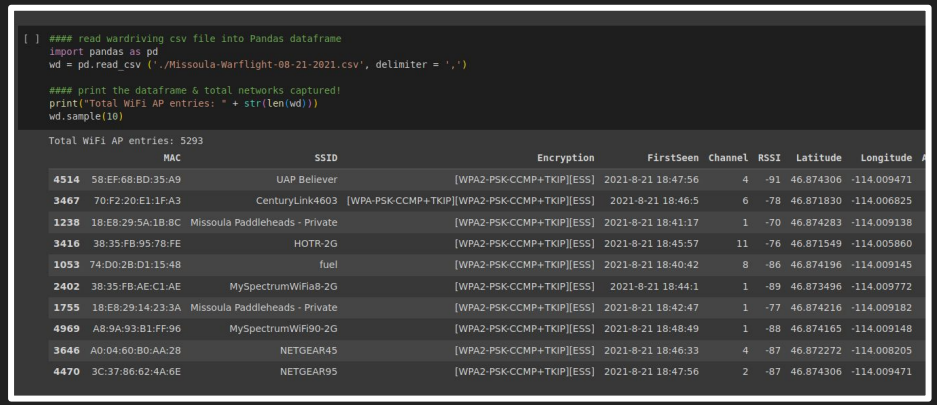




Pandas

Versatile Data Analysis Tool

- Tables (CSV, Excel, similar)
- Data Manipulation
- Easily group or filter for attributes



```
[ ] #### read wardriving csv file into Pandas dataframe
    import pandas as pd
    wd = pd.read_csv ('./Missoula-Warflight-08-21-2021.csv', delimiter = ',')

    #### print the dataframe & total networks captured!
    print("Total WiFi AP entries: " + str(len(wd)))
    wd.sample(10)
```

Total WiFi AP entries: 5293

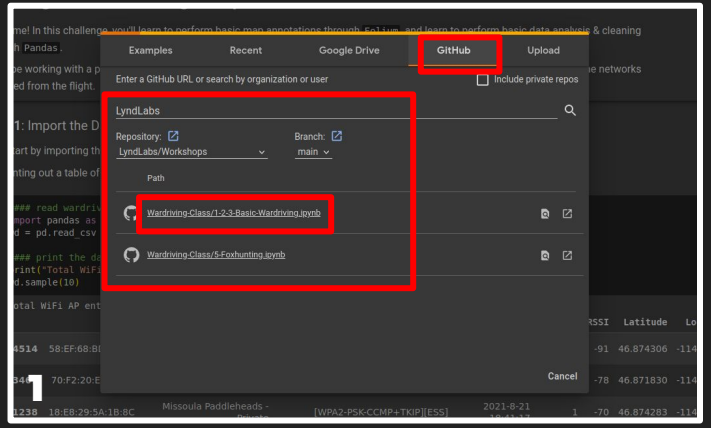
	MAC	SSID	Encryption	FirstSeen	Channel	RSSI	Latitude	Longitude	A
4514	58:EF:68:BD:35:A9	UAP Believer	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:47:56	4	-91	46.874306	-114.009471	
3467	70:F2:20:E1:1F:A3	CenturyLink4603	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:46:5	6	-78	46.871830	-114.006825	
1238	18:E8:29:5A:1B:8C	Missoula Paddleheads - Private	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:41:17	1	-70	46.874283	-114.009138	
3416	38:35:FB:95:78:FE	HOTR-2G	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:45:57	11	-76	46.871549	-114.005860	
1053	74:D0:2B:D1:15:48	fuel	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:40:42	8	-86	46.874196	-114.009145	
2402	38:35:FB:AE:C1:AE	MySpectrumWiFia8-2G	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:44:1	1	-89	46.873496	-114.009772	
1755	18:E8:29:14:23:3A	Missoula Paddleheads - Private	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:42:47	1	-77	46.874216	-114.009182	
4969	A8:9A:93:B1:FF:96	MySpectrumWiFi90-2G	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:48:49	1	-88	46.874165	-114.009148	
3646	A0:04:60:B0:AA:28	NETGEAR45	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:46:33	4	-87	46.872272	-114.008205	
4470	3C:37:86:62:4A:6E	NETGEAR95	[WPA2-PSK-CCMP+TKIP][ESS]	2021-8-21 18:47:56	2	-87	46.874306	-114.009471	

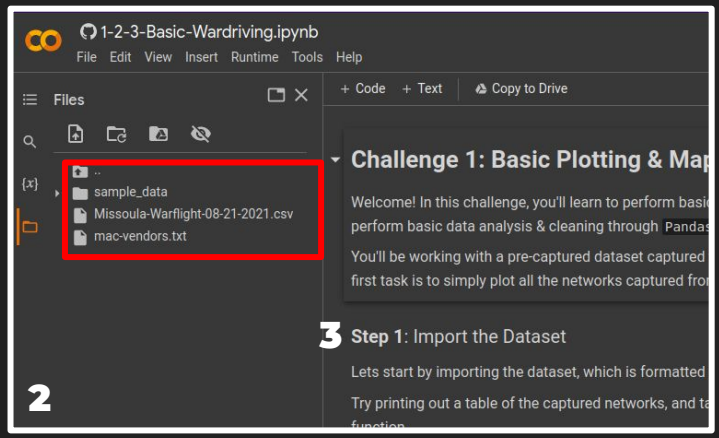
https://pandas.pydata.org

https://github.com/lyndlabs/workshops

Jupyter Notebook Setup

1. Open the Workshop GitHub repo
2. Upload files →
   a. **.csv recon file**
   b. MAC vendor list
3. Try running the first code cell!



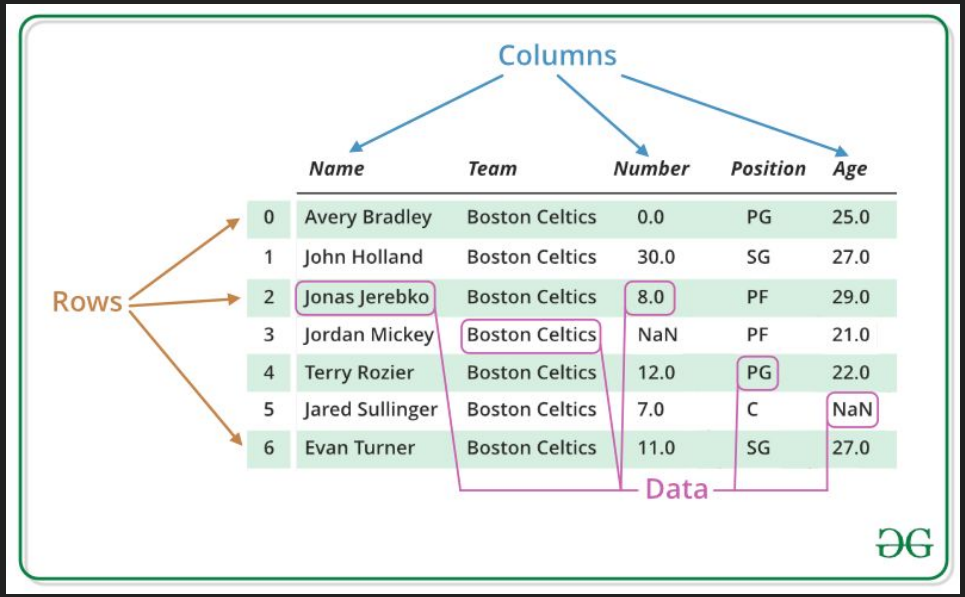


Challenge 1:
Basic Map Annotations

Pandas

Dataframe:

Row / Column based table



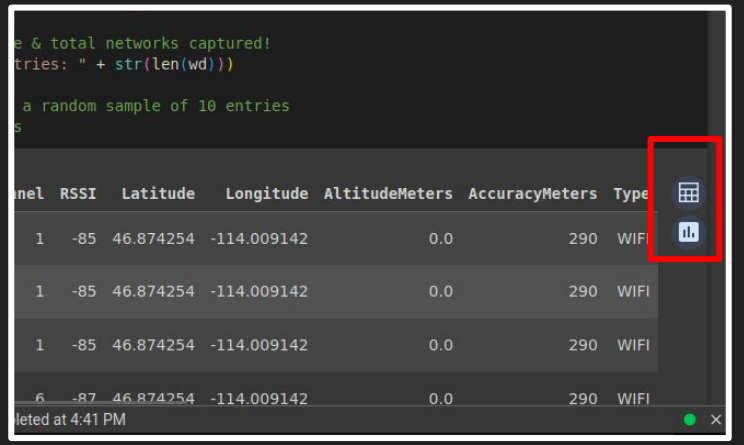
Pandas Basics

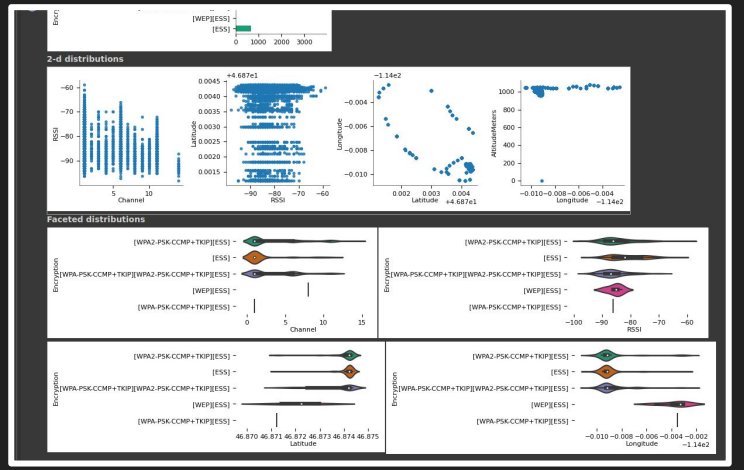
Sample Data

- df.sample(num)

Interactive Data!

- Charts & interactive modes
  →
- No-code filtering
- Suggested charts

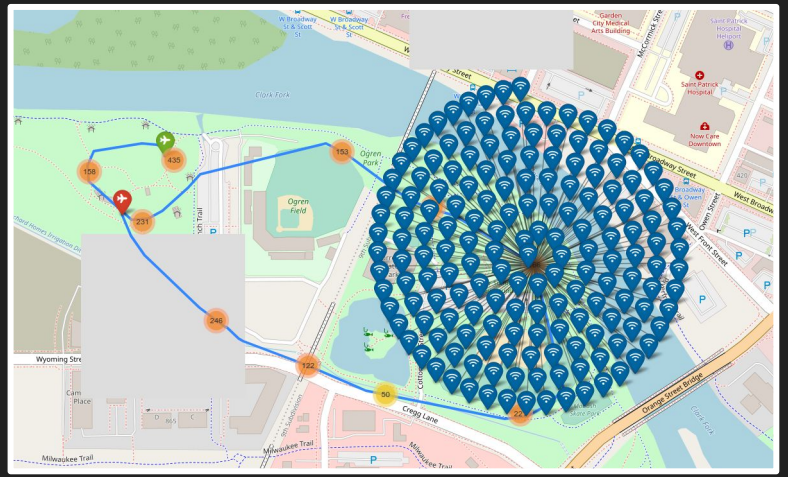




Workflow

1. **Import Dataset**
2. **Clean & Filter Data**
    - Data sometimes has mistakes or unwanted outliers
3. **Perform Map Annotations**
    - Markers, Heatmaps, etc

Objective: Create a basic map from the sample data, plotting spotted networks!



Stacking Pandas Functions

1. Return DataFrame of all “FirstSeen” values in WD
2. Get the indices of the values as a list from WD
3. Drop all the above indices from WD

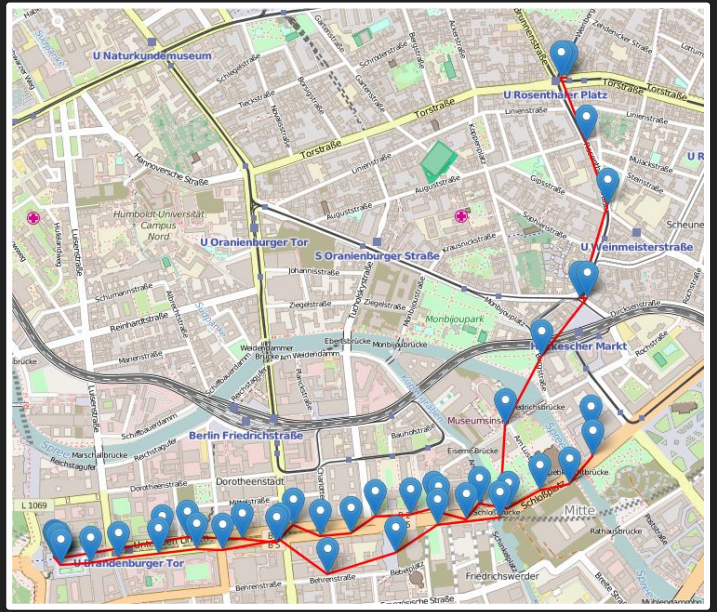
```
# match all the indices of the FirstSeen column less than OR greater than

wd.drop(wd.index[wd["FirstSeen"] <= "2021-8-21 18:43:25"], inplace=True)
wd.drop(wd.index[wd["FirstSeen"] >= "2021-8-21 18:46:58"], inplace=True)

print("Total WiFi AP entries: " + str(len(wd)))
print("Unique network entries: " + str(len(wd.SSID.unique())))
```

```
Total WiFi AP entries: 1038
```

Folium Mapping Challenge

Check out the mapping exercise and try annotating some Las Vegas landmarks!

- Marker
- Polyline



Challenge 2:
Plot Insecure Networks

Scenarios + Use Cases

- Discover IoT Vulnerabilities
- Possible entry points for malicious activity
- Print from random Insecure Printers
- Free WiFi :)

Attacks/Breaches | 4 MIN READ NEWS

Wardriving Burglars Hacked Business Wi-Fi Networks

Three men are indicted for using a tricked-out Mercedes with specialized antennas and network-cracking tools to steal financial data via businesses' wireless networks.

Mathew J. Schwartz
Contributor

September 23, 2011

Strategic Security Survey: Global Threat, Local Pain
(click image for larger view and for full slideshow)

Three men were indicted last week by a federal grand jury for hacking at least 13 Seattle-area businesses' wireless networks to steal sensitive information, as well as burglarizing the premises of at least 41 businesses

Plot Vulnerable Networks

Objective:

- Plot Insecure WiFi Networks:
  - WEP, Open Networks
- Try using Folium's **HeatMap** feature!
- Use a mix of Markers / Heat / Cluster Maps to make your own visualization!

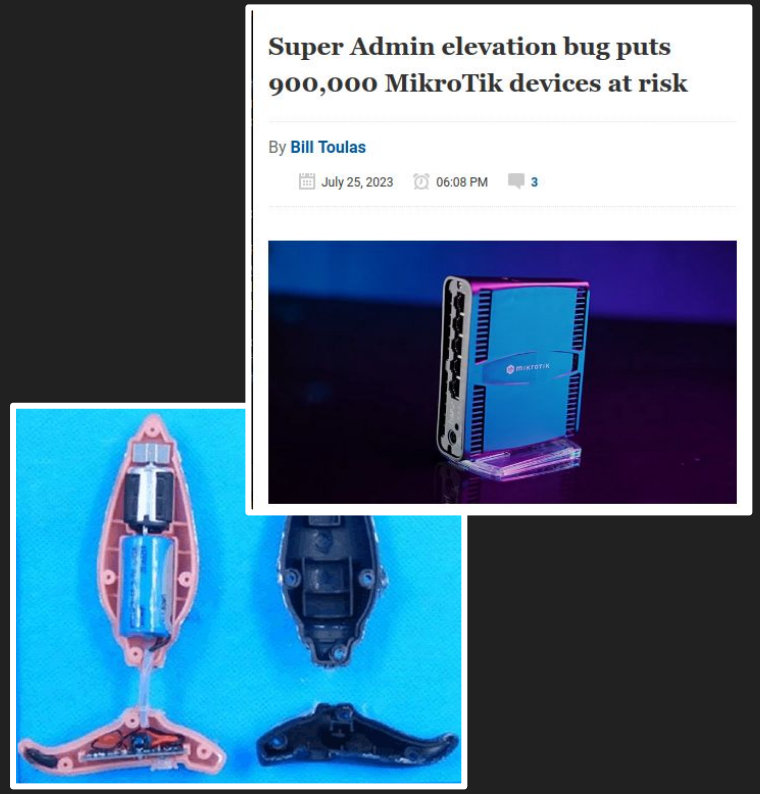
Bonus: Try using **FeatureGroups** to create "layers"!

Challenge 3:
Network & Device Profiling

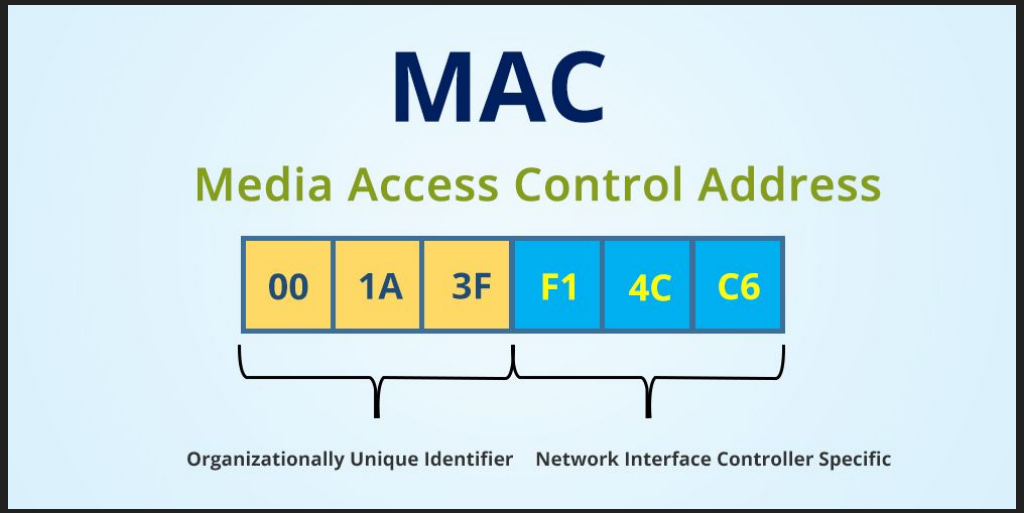
Scenarios + Use Cases

Detect unique devices & vendors:

- Profile vulnerable IoT devices
- Print on every insecure printer in your city
- Find default Access Points
- Detect known devices + friends nearby!
- Detect da Police



MAC Address Structure



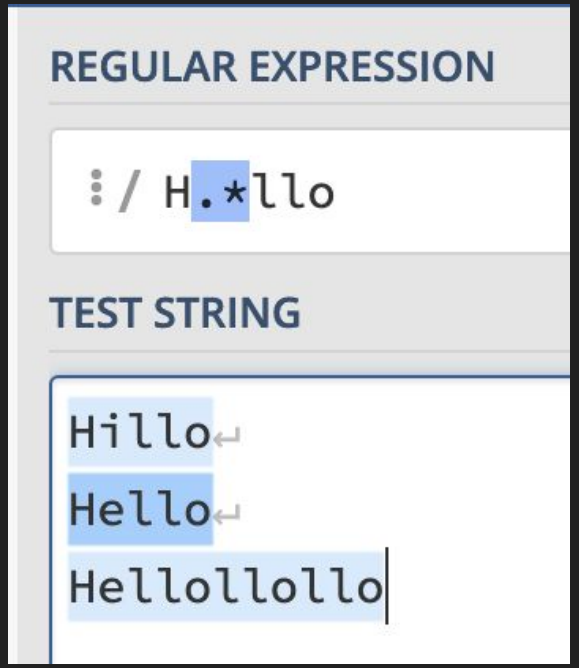
https://www.wireshark.org/tools/oui-lookup.html

E0:43:DB	Shenzhen ViewAt Technology Co.,Ltd.
24:05:F5	Integrated Device Technology (Malaysia) Sdn. Bhd.
2C:30:33	NETGEAR
3C:D9:2B	Hewlett Packard
9C:8E:99	Hewlett Packard
B4:99:BA	Hewlett Packard
1C:C1:DE	Hewlett Packard
3C:35:56	Cognitec Systems GmbH
00:50:BA	D-Link Corporation
00:17:9A	D-Link Corporation
1C:BD:B9	D-Link International
90:94:E4	D-Link International
28:10:7B	D-Link International
1C:7E:E5	D-Link International
C4:A8:1D	D-Link International
18:62:2C	Sagemcom Broadband SAS
7C:03:D8	Sagemcom Broadband SAS
E8:F1:B0	Sagemcom Broadband SAS
00:F8:71	DGS Denmark A/S
20:BB:76	COL GIOVANNI PAOLO SpA
2C:22:8B	CTR SRL
34:8A:AE	Sagemcom Broadband SAS
BC:EC:23	SHENZHEN CHUANGWEI-RGB ELECTRONICS CO.,LTD
8C:E7:48	Private
AC:06:C7	ServerNet S.r.l.
CC:46:D6	Cisco Systems, Inc
48:AD:08	HUAWEI TECHNOLOGIES CO.,LTD
2C:AB:00	HUAWEI TECHNOLOGIES CO.,LTD
00:E0:FC	HUAWEI TECHNOLOGIES CO.,LTD
24:DF:6A	HUAWEI TECHNOLOGIES CO.,LTD
00:9A:CD	HUAWEI TECHNOLOGIES CO.,LTD
00:CD:FE	Apple, Inc.
38:F2:3E	Microsoft Mobile Oy
58:AC:78	Cisco Systems, Inc
90:7F:61	Chicony Electronics Co., Ltd.
28:BC:18	SourcingOverseas Co. Ltd
80:7A:BF	HTC Corporation
40:9F:87	Jide Technology (Hong Kong) Limited
3C:5A:B4	Google, Inc.

Regular Expressions

Regex lets us match patterns in text!

- Find patterns in default networks:
  - MySpectrumSetup-6B
  - NETGEAR66
  - HP-Deskjet...



https://regex101.com/

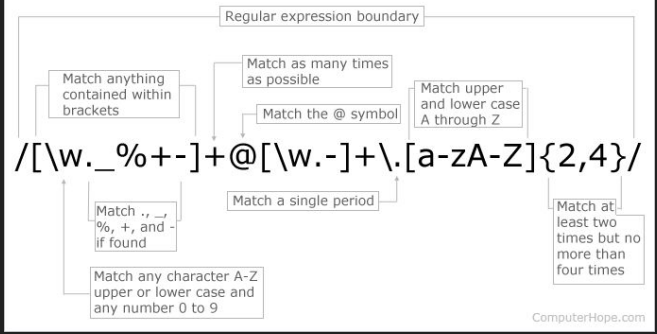
Regular Expressions

Symbol	Description	Symbol	Description
^	Start of line +	?	0 or 1 +
\A	Start of string +	{3}	Exactly 3 +
$	End of line +	{3,}	3 or more +
\Z	End of string +	{3,5}	3, 4 or 5 +
\b	Word boundary +	\	Escape Character +
\B	Not word boundary +	\n	New line +
\<	Start of word	\r	Carriage return +
\>	End of word	\t	Tab +
\s	White space	.	Any character except new line (\n) +
\S	Not white space	(a|b)	a or b +
\d	Digit	[abc]	Range (a or b or c) +
\D	Not digit	[^abc]	Not a or b or c +
\w	Word	[0-7]	Digit between 0 and 7 +
\W	Not word	[a-q]	Letter between a and q +
*	0 or more +	[A-Q]	Upper case letter + between A and Q +
+	1 or more +		

Which of these is RegEx?

1. **(=<`#9]~6ZY327Uv4-QsqpMn&+Ij"'E%e{Ab~w=_**
2. **(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%**
3. **98u9U(9uijd..8/(")+!(="/2)){}1678927(/(')2.9)%&**
4. **7jÉUy¯Ùzè] ÏÌ+É¢4Fïç@{¨P«Ï˜„¼é¼&Nwò›Lõ¸uß(**
5. **(a-z0-9)+[6-9!#$]+(\[◊])a-b(?:-:^-._.+(1-9!#*6942**

Regular Expression E-mail Matching Example

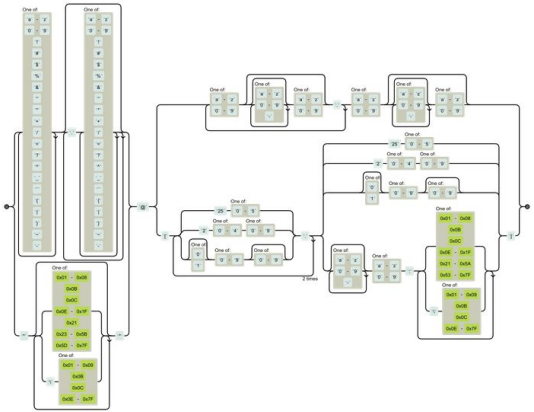


Regular Expression Hell

General Email Regex (RFC 5322 Official Standard)

```
(?:[a-z0-9!#$%&'*+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*+/=?^_`{|}~-]+)*|"(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21\x23-\x5b\x5d-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])*")@(?:(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\.)+[a-z0-9](?:[a-z0-9-]*[a-z0-9])?|\[(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?|[a-z0-9-]*[a-z0-9]:(?:[\x01-\x08\x0b\x0c\x0e-\x1f\x21-\x5a\x53-\x7f]|\\[\x01-\x09\x0b\x0c\x0e-\x7f])+)\])
```

Railroad Diagram of Above Regex (click to enlarge)



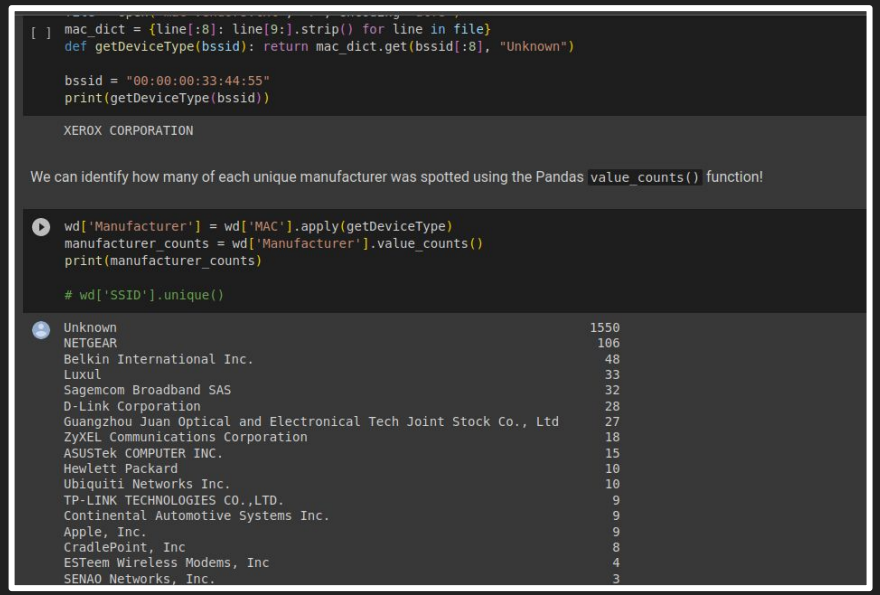
```
(function(a,b){if(/(android|bb\d+|meego).+mobile|avantgo|bada
\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)|iris|kindle|lge
|maemo|midp|mmp|mobile.+firefox|netfront|opera m(ob|in)i|palm(
os)?|phone|p(ixi|re)\/|plucker|pocket|psp|series(4|6)0|symbian|treo|up\.(browser|link)|vodafone|wap|windows
ce|xda|xiino/i.test(a)||/1207|6310|6590|3gso|4thp|50[1-6]i|770s|802s|a
wa|abac|ac(er|oo|s\-)|ai(ko|rn)|al(av|ca|co)|amoi|an(ex|ny|yw)|aptu|ar(ch|go)|as(te|us)|attw|au(di|\-m|r |s
)|avan|be(ck|ll|nq)|bi(lb|rd)|bl(ac|az)|br(e|v)w|bumb|bw\-(n|u)|c55\/|capi|ccwa|cdm\-|cell|chtm|cldc|cmd
\-|co(mp|nd)|craw|da(it|ll|ng)|dbte|dc\-s|devi|dica|dmob|do(c|p)o|ds(12|
\-d)|el(49|ai)|em(l2|ul)|er(ic|k0)|esl8|ez([4-7]0|os|wa|ze)|fetc|fly(\-|_)|g1 u|g560|gene|gf\-5|g\-
mo|go(\.w|od)|gr(ad|un)|haie|hcit|hd\-(m|p|t)|hei\-|hi(pt|ta)|hp( i|ip)|hs\-c|ht(c(\-| |_|a|g|p|s|t)|tp)|hu(aw|tc)|i\-
(20|go|ma)|i230|iac( |\-|\/)|ibro|idea|ig01|ikom|im1k|inno|ipaq|iris|ja(t|v)a|jbro|jemu|jigs|kddi|keji|kgt( |\/)|klon|kpt
|kwc\-|kyo(c|k)|le(no|xi)|lg( g|\/(k|l|u)|50|54|\-[a-w])|libw|lynx|m1\-w|m3ga|m50\/|ma(te|ui|xo)|mc(01|21|ca)|m
\-cr|me(rc|ri)|mi(o8|oa|ts)|mmef|mo(01|02|bi|de|do|t(\-| |o|v)|zz)|mt(50|p1|v
)|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti
|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck|rt|se)|prox|psio|pt\-g|qa
\-a|qc(07|12|21|32|60|\-[2-7]|i\-)|qtek|r380|r600|raks|rim9|ro(ve|zo)|s55\/|sa(ge|ma|mm|ms|ny|va)|sc(01|h\-|oo|p
\-)|sdk\/|se(c(\-|0|1)|47|mc|nd|ri)|sgh\-|shar|sie(\-|m)|sk\-0|sl(45|id)|sm(al|ar|b3|it|t5)|so(ft|ny)|sp(01|h\-|v\-|v
)|sy(01|mb)|t2(18|50)|t6(00|10|18)|ta(gt|lk)|tcl\-|tdg\-|tel(i|m)|tim\-|t\-mo|to(pl|sh)|ts(70|m\-|m3|m5)|tx
\-9|up(\.b|g1|si)|utst|v400|v750|veri|vi(rg|te)|vk(40|5[0-3]|
\-v)|vm40|voda|vulc|vx(52|53|60|61|70|80|81|83|85|98)|w3c(\-| )|webc|whit|wi(g
|nc|nw)|wmlb|wonu|x700|yas\-|your|zeto|zte\-/i.test(a.substr(0,4)))window.location=b})
(navigator.userAgent||navigator.vendor||window.opera,'http://detectmobilebrowser.com/mobile');
```

Challenge: Network & Device Profiling

Write a script that filters for default setup networks or Netgear routers!

Objectives:

- Identify Device Manufacturers by MAC Address
- (or) Use Regular Expressions to match network names



```
[ ] mac_dict = {line[:8]: line[9:].strip() for line in file}
    def getDeviceType(bssid): return mac_dict.get(bssid[:8], "Unknown")

    bssid = "00:00:00:33:44:55"
    print(getDeviceType(bssid))
```

```
XEROX CORPORATION
```

We can identify how many of each unique manufacturer was spotted using the Pandas `value_counts()` function!

```
wd['Manufacturer'] = wd['MAC'].apply(getDeviceType)
manufacturer_counts = wd['Manufacturer'].value_counts()
print(manufacturer_counts)

# wd['SSID'].unique()
```

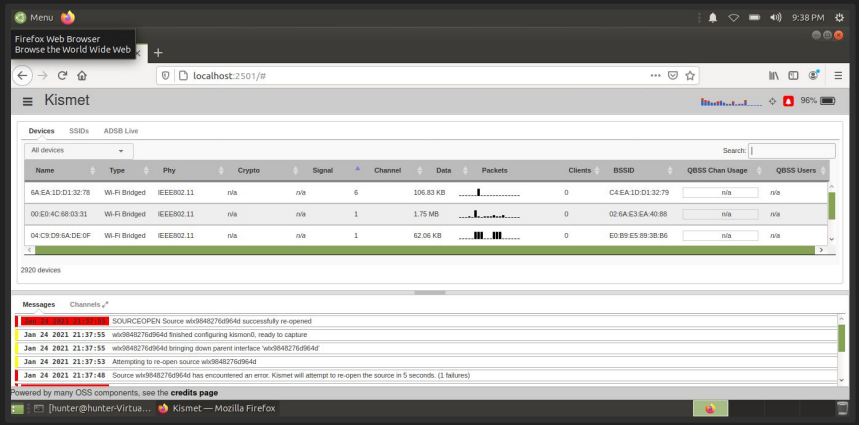
```
Unknown                                                 1550
NETGEAR                                                  106
Belkin International Inc.                                 48
Luxul                                                     33
Sagemcom Broadband SAS                                    32
D-Link Corporation                                        28
Guangzhou Juan Optical and Electronical Tech Joint Stock Co., Ltd  27
ZyXEL Communications Corporation                          18
ASUSTek COMPUTER INC.                                     15
Hewlett Packard                                           10
Ubiquiti Networks Inc.                                    10
TP-LINK TECHNOLOGIES CO.,LTD.                              9
Continental Automotive Systems Inc.                        9
Apple, Inc.                                                9
CradlePoint, Inc                                           8
ESTeem Wireless Modems, Inc                                4
SENAO Networks, Inc.                                       3
```

Challenge 4:
Detecting Stalkers

Client Devices

Wardriving can also be used to profile client devices:

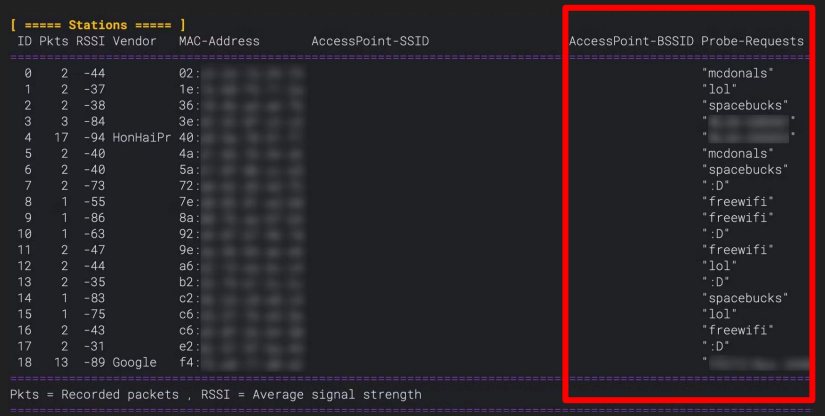
- IoT & Smart-Home Products
- Phones, Laptops, etc
- Determine who owns what



Real World Application

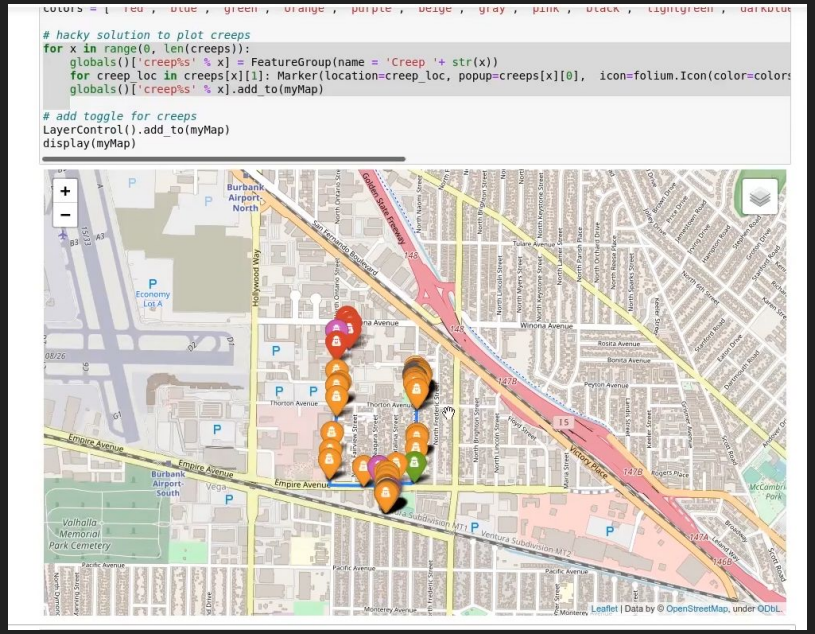
Wardriving can be used to detect if someone is following you!

- Probe Requests look for past networks
- WiFi Devices constantly emit these, even when they're "off"
- We can determine if a unique wifi device pops up at multiple locations!



```
[ ===== Stations ===== ]
 ID Pkts RSSI Vendor   MAC-Address       AccessPoint-SSID                AccessPoint-BSSID Probe-Requests
=============================================================================================================
  0    2  -44          02:[redacted]                                                       "mcdonals"
  1    2  -37          1e:[redacted]                                                       "lol"
  2    2  -38          36:[redacted]                                                       "spacebucks"
  3    3  -84          3e:[redacted]                                                       "[redacted]"
  4   17  -94 HonHaiPr 40:[redacted]                                                       "[redacted]"
  5    2  -40          4a:[redacted]                                                       "mcdonals"
  6    2  -40          5a:[redacted]                                                       "spacebucks"
  7    2  -73          72:[redacted]                                                       ":D"
  8    1  -55          7e:[redacted]                                                       "freewifi"
  9    1  -86          8a:[redacted]                                                       "freewifi"
 10    1  -63          92:[redacted]                                                       ":D"
 11    2  -47          9e:[redacted]                                                       "freewifi"
 12    2  -44          a6:[redacted]                                                       "lol"
 13    2  -35          b2:[redacted]                                                       ":D"
 14    1  -83          c2:[redacted]                                                       "spacebucks"
 15    1  -75          c6:[redacted]                                                       "lol"
 16    2  -43          c6:[redacted]                                                       "freewifi"
 17    2  -31          e2:[redacted]                                                       ":D"
 18   13  -89 Google   f4:[redacted]                                                       "[redacted]
=============================================================================================================
Pkts = Recorded packets , RSSI = Average signal strength
=============================================================================================================
```

Real World Application

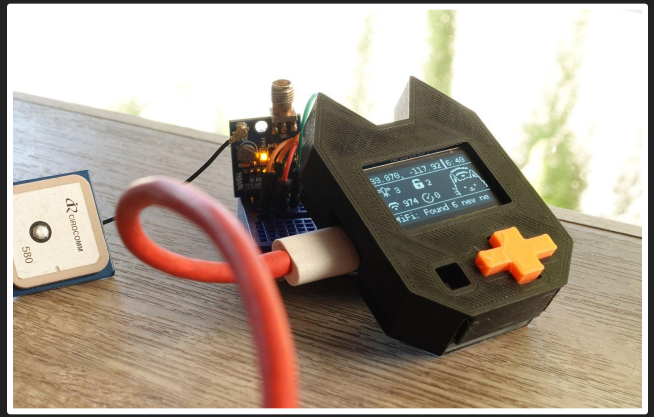


creepdetector.wtf

Taking it Further

Future Wardriver Features

- More cats!
- WiFi Attacks
- Packet Stream to Wireshark
- Multi-Protocol (BT, BLE, Cellular)



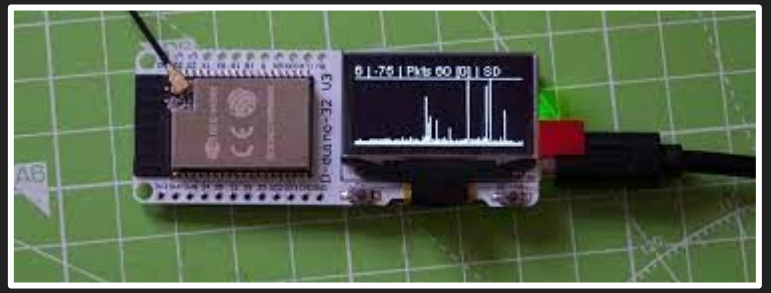
Supported Community Projects

Spacehuhn's PacketMonitor

- Monitor WiFi Traffic
- Signal Foxhunting

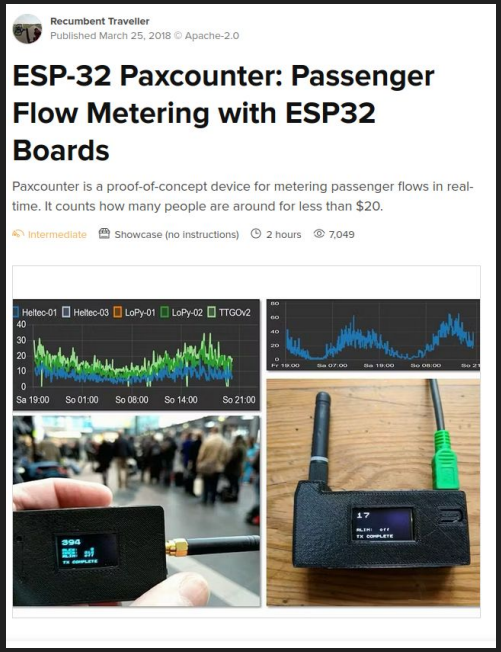
Spacehuhn's ArduinoPCAP

- Stream Packets → Wireshark
- Capture to SD Card



Reconnaissance

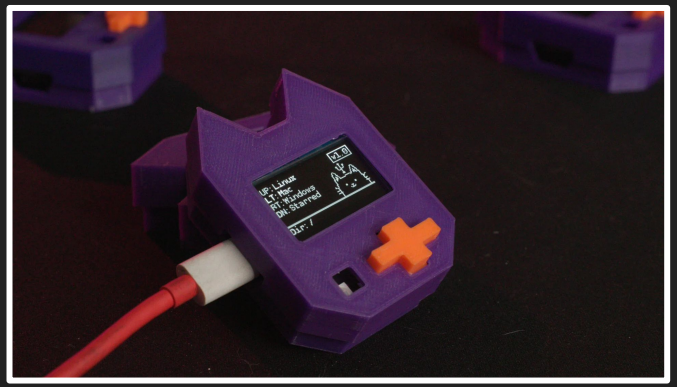
- **Flow Meter**: Simple WiFi + BLE presence detection
- **Constellation Tracking**: Defeat MAC Address randomization using a “cluster” of devices
- **Friend Detector:** Detect known devices using MAC Address



More Nugget Resources

- CircuitPython & Arduino!
  - Easy prototyping / coding
  - Basic recon examples
- Hardware / Sensor Control
- USB Hacking
- Breakout boards!

Learn more at wifinugget.com



Thanks for coming!

Follow **@alexlynd** for upcoming events
& check out **lyndlabs.io** for more info.