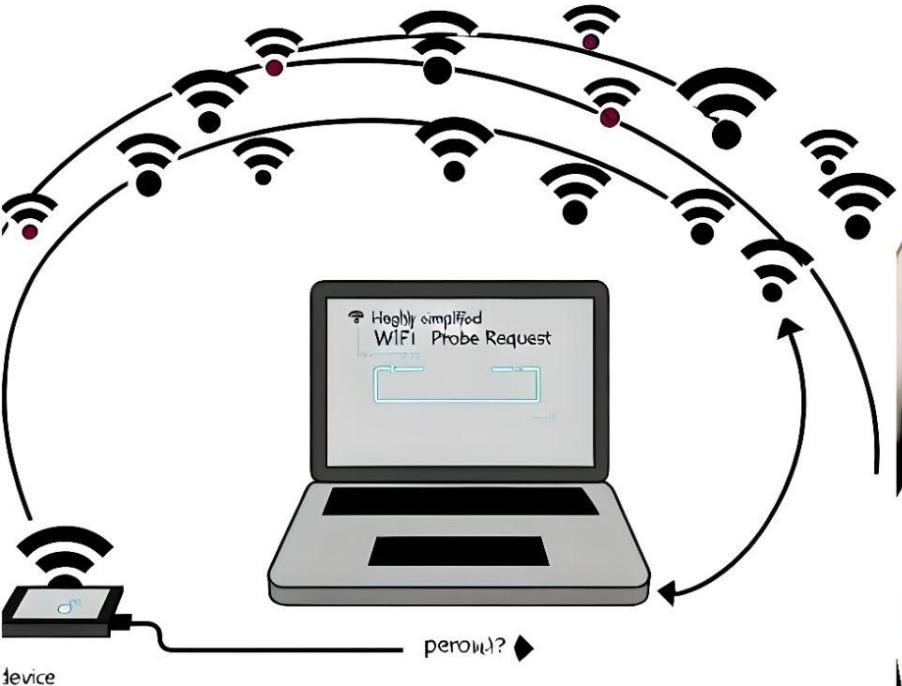


Combining OSINT and SIGINT to Enumerate IRL Threat Actors



\$ whoami

- 20+ years Security
- BS Networking
- MSc Cybersecurity
- CISSP
- GIAC Assessing and Auditing Wireless Networks (GAWN)
- GIAC GPEN

Our mission is to build a *regenerative* digital economy that creates conditions of *prosperity* for all.



@benatcLabs



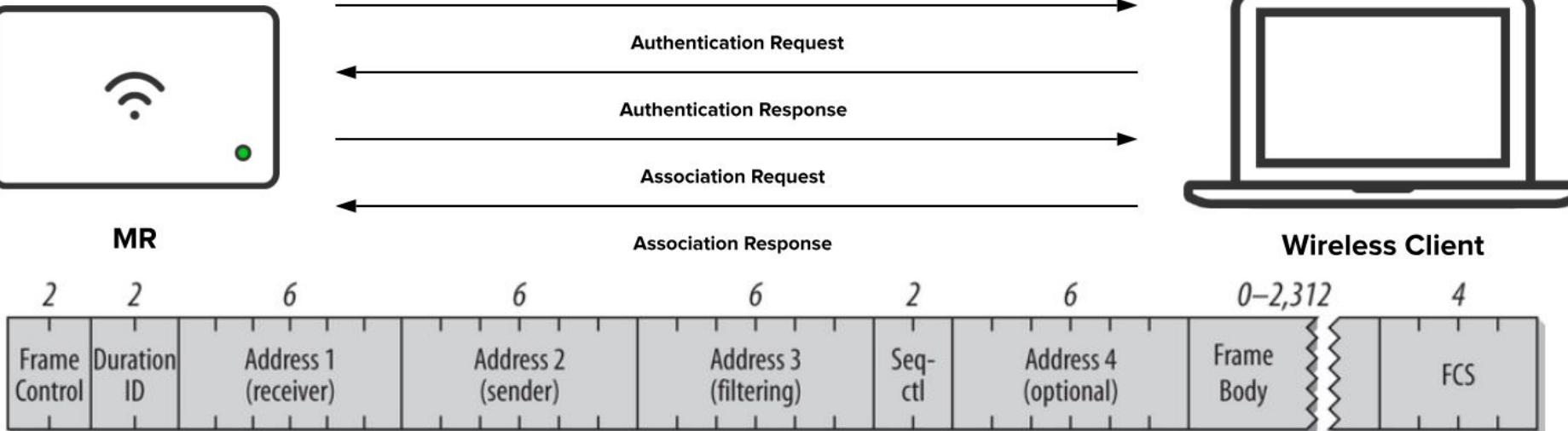
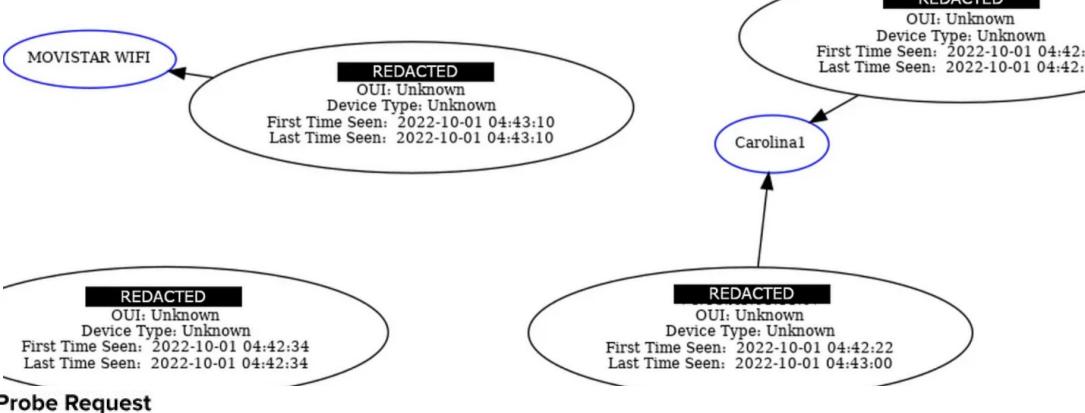
@maxxsyntax

<https://github.com/maxxsyntax/probeprint2/>

Agenda

- Intro
 - What Are Probe Requests
 - MAC Randomization
 - Probing Rounds
 - Who
 - Public Sector
 - Big Data
 - Municipalities
 - Academia
 - Why/Related Works
 - Independent Researchers
 - How
 - Which command
 - Equipment
 - Data Analysis
 - Experiment
 - Observation
 - Conclusion
 - Application
- Key Terms:**
- SSID = Names given to WiFi Access Points
 - MAC = Unique* identifier of network interface card
 - OUI = Organizationally unique identifier (first half of MAC address)
 - PII = Personally Identifiable Information - any information that can be used to distinguish one individual from another

Probe Requests are simple right?



Modern Probe Requests

- Randomized MAC address
 - <10% not randomized (IoT) [5]
- Preferred Network List
- SSID Bursts aka Probing Round
- Even when wifi is off
- OUI's are *not* retained
- Information Elements
 - VHT - 802.11ac Channel Bonding
 - HT - 802.11n Channel Width
 - Country
 - Timezone
 - Antennas
 - Vendor Specific

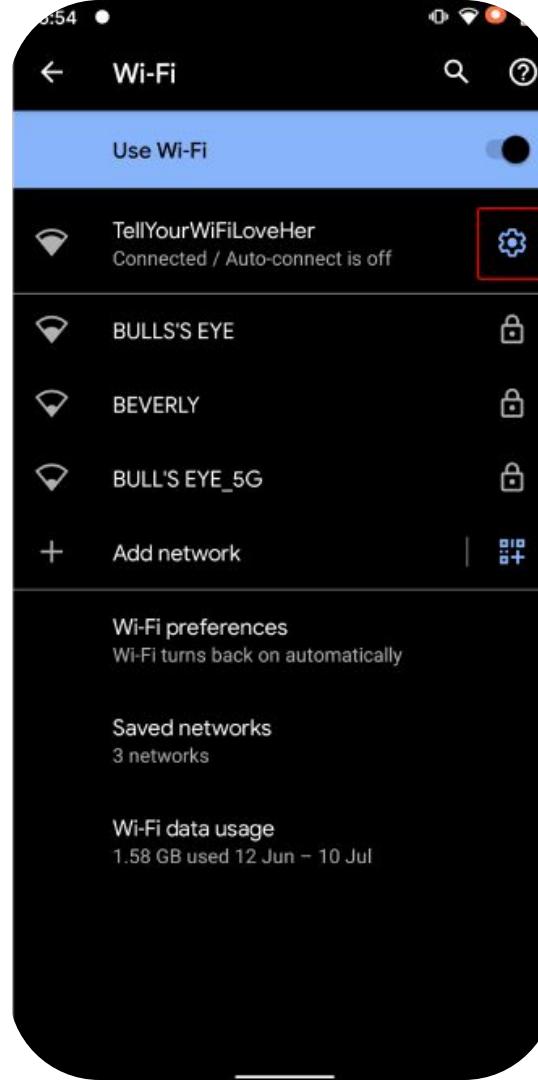


Image credit: <https://techwiser.com>

```
▶ Device Name: Car-8e72 ←
▶ Vendor Extension
▼ Tag: Vendor Specific: Wi-Fi Alliance: P2P
  Tag Number: Vendor Specific (221)
  Tag length: 17
  OUI: 50:6f:9a (Wi-Fi Alliance)
  Vendor Specific OUI Type: 9
  ▶ P2P Capability: Device 0x25 Group 0x0
  ▶ Listen Channel: Operating Class 81 Channel Number 1
▼ Tag: Vendor Specific: Broadcom ←
  Tag Number: Vendor Specific (221)
  Tag length: 9
  OUI: 00:10:18 (Broadcom)
  Vendor Specific OUI Type: 2
  Vendor Specific Data: 020000100000
▼ Tag: Vendor Specific: Epigram, Inc.: HT Capabilities (802.11n)
  Tag Number: Vendor Specific (221)
  Tag length: 30
  OUI: 00:90:4c (Epigram, Inc.) ←
  Vendor Specific OUI Type: 51
  802.11n (Pre) Type: HT Capabilities (802.11n D1.10) (51)
  ▶ HT Capabilities Info (VS): 0x1121 ←
  ▶ A-MPDU Parameters (VS): 0x17
  ▶ Rx Supported Modulation and Coding Scheme Set (VS): MCS Se...
  ▶ HT Extended Capabilities (VS): 0x0000
  ▶ Transmit Beam Forming (TxBF) Capabilities (VS): 0x00000000
  ▶ Antenna Selection (ASEL) Capabilities (VS): 0x00
    .... .0 = Antenna Selection Capable: Not supported
    .... .0. = Explicit CSI Feedback Based Tx ASEL: Not
    .... .0.. = Antenna Indices Feedback Based Tx ASFI
```

“Information Elements” in Probe Requests can be used to de-anonymize devices

Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms

Authors: Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, Frank Piessens

When do Probe Requests Occur?

Device State	Probe Request Interval (smartphone)
Asleep (screen off)	~ once a minute
Standby (screen on)	10 - 15 times per minute
Associated	varies, could require user to manual [6] Cisco

- “500 times in a 24h period” [5]
 - Source: “Tools for Ground-Truth-Free Passive Client Density Mapping in MAC-Randomized Outdoor WiFi Networks”
- “Regardless of whether the device is connected to a WiFi access point” [4]
 - Source: “Crowd Monitoring in Smart Destinations Based on GDPR-Ready Opportunistic RF Scanning and Classification of WiFi Devices to Identify and Classify Visitors’ Origins”

Who's monitoring Probe Requests?



2 files (84 ms) in GendarmerieNationale/ReceptionInfoDrone X

lib/scapy/layers/dot11.py

```
716     name = "802.11 Reassociation Response"  
717  
718  
719 class Dot11ProbeReq(Packet):  
720     name = "802.11 Probe Request"  
721  
722
```

Show 2 more matches



lib/scapy/modules/krack/automaton.py

Python · master

```
18     Dot11Auth, Dot11Beacon, Dot11Elt, Dot11EltRates, Dot11EltRSN, \  
19     Dot11ProbeReq, Dot11ProbeResp, RSNCipherSuite, AKMSuite  
20     from scapy.layers.eap import EAPOL  
  
464         return  
465         if Dot11ProbeReq in pkt and pkt[Dot11Elt::{'ID': 0}].info == self.ssid:  
466             raise self.WAIT_AUTH_REQUEST().action_parameters(pkt)
```

Google admits collecting Wi-Fi data through Street View cars

German request for data audit reveals the web giant 'accidentally' stored payload information from open networks



A screenshot of the Microsoft Developer Center website. The top navigation bar includes links for "Developer Center", "Ways to build", "Use cases", "Business resources", "What's new", and "Docs". Below the navigation is a search bar with the placeholder "Search Microsoft Docs". The main content area shows a "Getting started" section with "Learn", "Develop", "Reference", and "Support" tabs, where "Support" is currently selected. To the right, there's a "Matter" section featuring a "Smart Home" device and a "Capture WLAN traffic" guide.



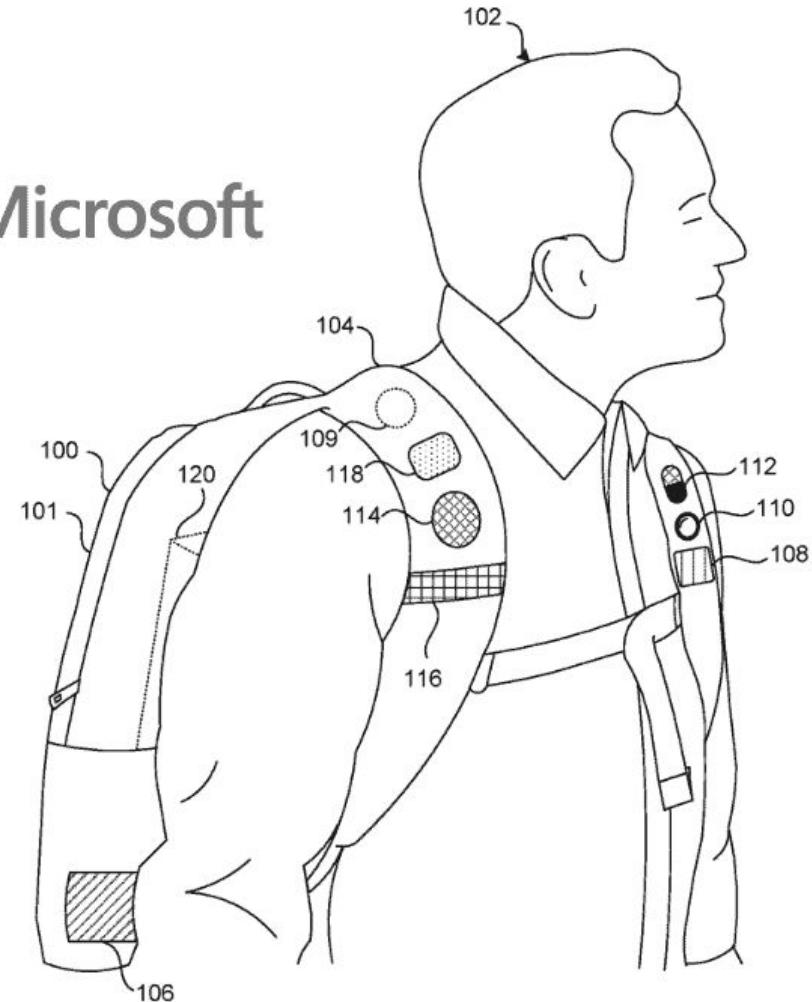
Google Home Developers > Docs > Matter > Support

Capture WLAN traffic

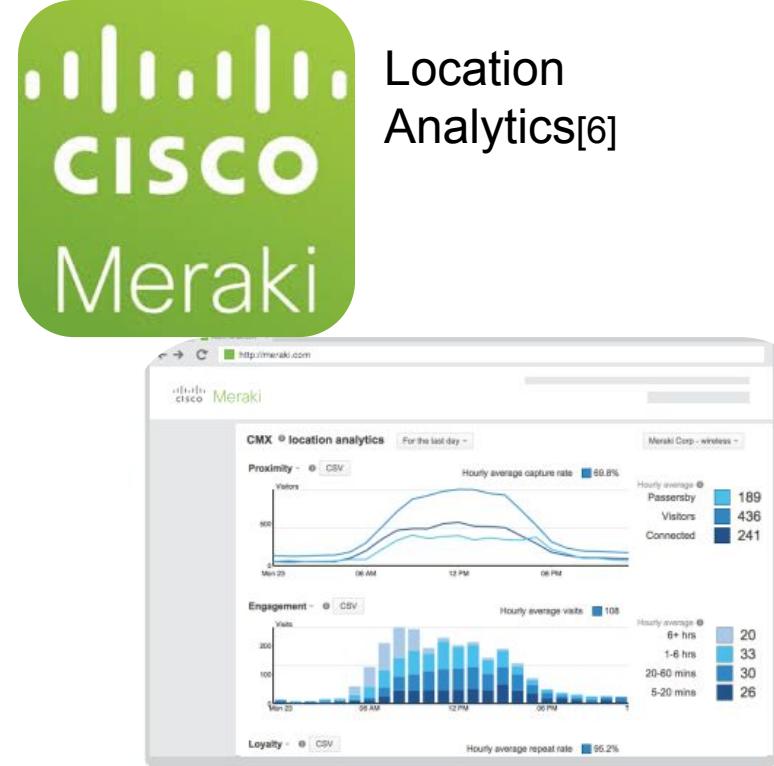
Capturing Wi-Fi packets lets you see details and interact running on a device, making these captures an important

The main steps involved are:

1. Find the right channel to sniff on.
2. Capture the traffic.
3. Share the capture and a hash of your WLAN password.

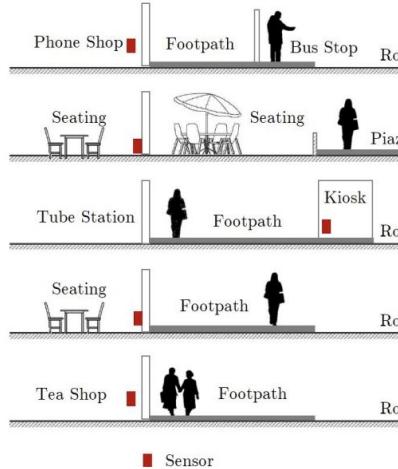
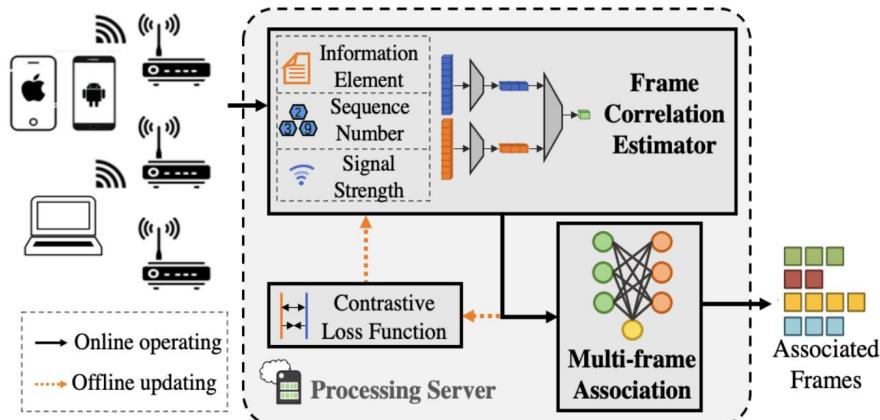


Smart Cities: Smart Spot by Hopu [4]
Advanced Air Quality Monitoring Solution & Calibration
<https://hopu.eu>



Meraki's CMX Location Analytics

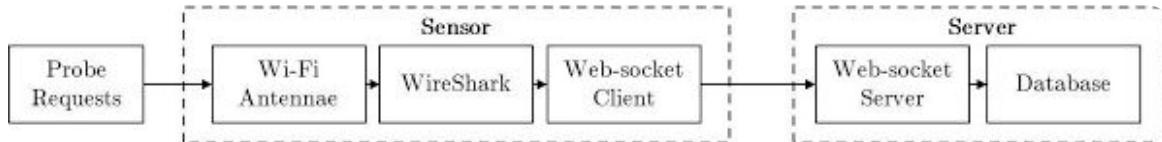
Academia



(a) Installation configuration of sensors at the survey locations (not to scale)

(b) Density distribution of signal strength reported in collected probe requests (lower values show higher signal strength)

Figure 6. Distribution of signal strengths across locations



Independent Researchers



HackHeld
by spacehuhn
(ESP8266)



Flipper Zero WiFi Dev
Board with Marauder
By Justcallmekoko
(ESP32)



WiFi Pineapple
By Hak5



DNS Driveby
By Alex Lynd

Signal Intelligence

```
tcpdump -nei wlan0mon type mgt subtype probe-req  
tshark -Vi wlan0mon -f "wlan subtype probe-req"
```

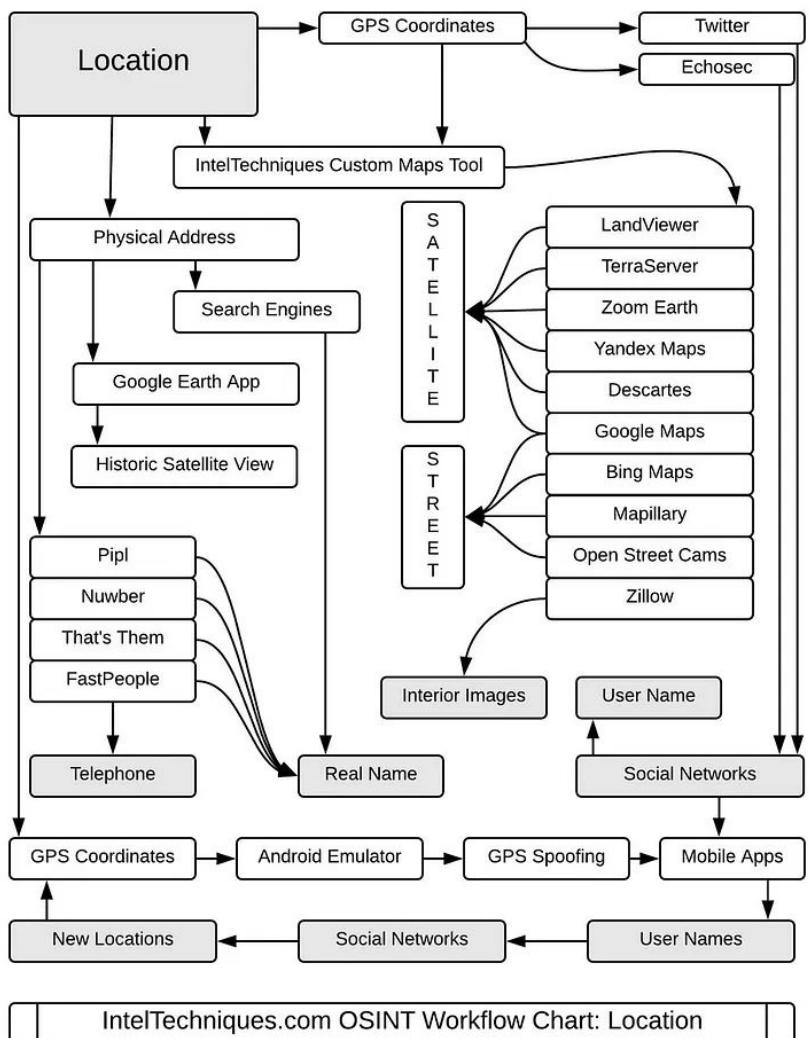
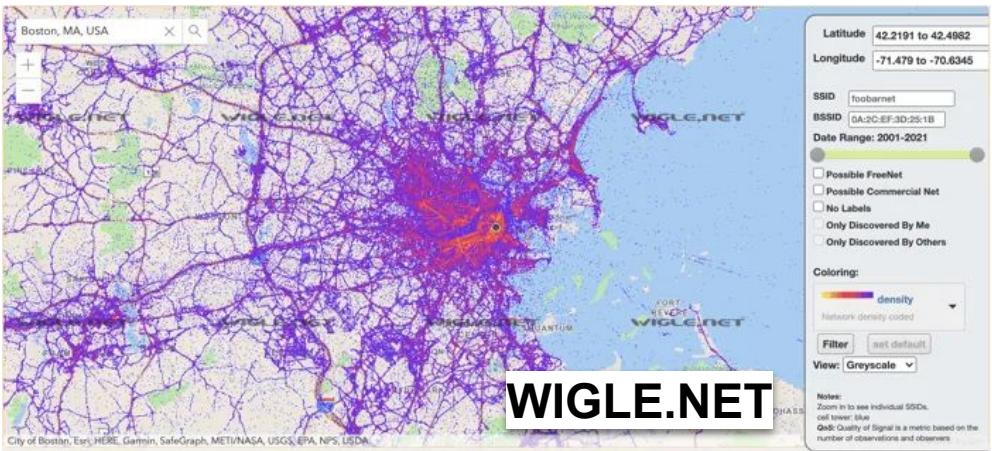
Linux or MacOS super easy

Combined with OSINT

First-hand Account - Venue location, Eye witness, natural correlations in head

Leverage online db's -> osint workflow,

Covert & Realtime!



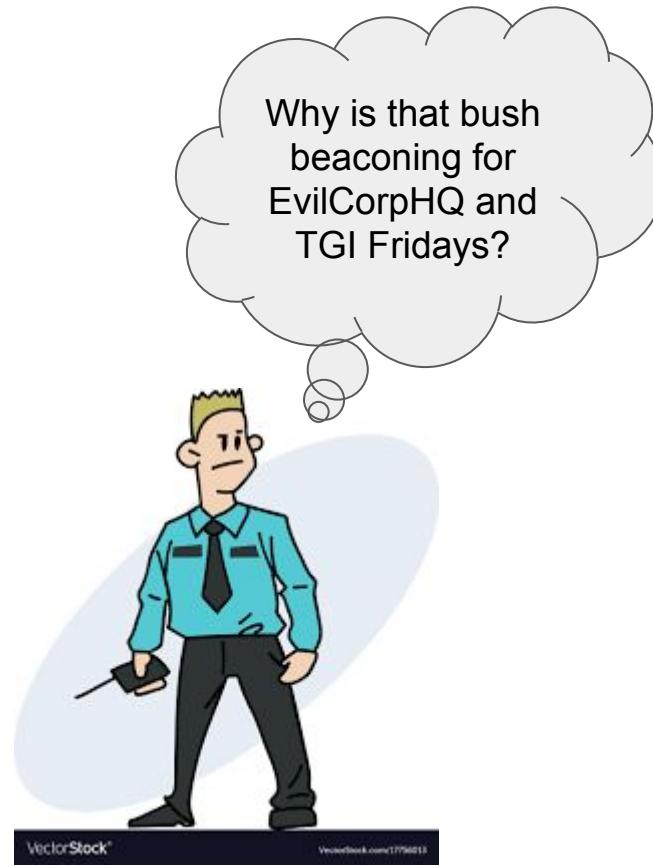


Blue team use case:

Passively obtained,
supplementary authentication
factors

Blue team use case:

Proximity Sensor/Anomaly Detection



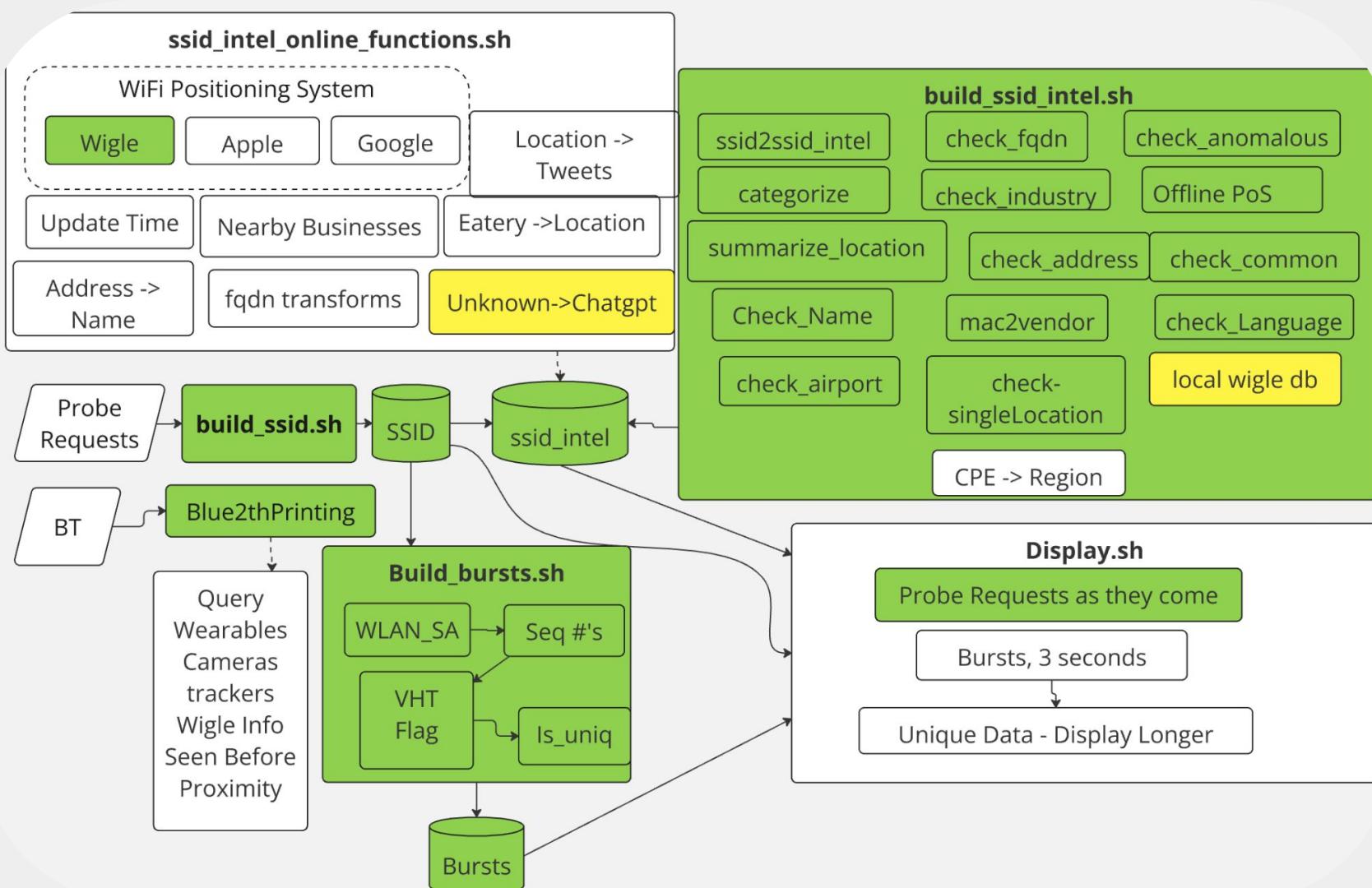
Differentiators

1. SSIDs are artifacts
2. OSInt transforms can be used to build profile
3. Signal Strength to Proximity
4. Incorporate Bluetooth
5. Portable real time display, not-overt
6. Open <https://github.com/maxxsyntax/probeprint2/>
7. Keep it Simple and lightweight

OSI model

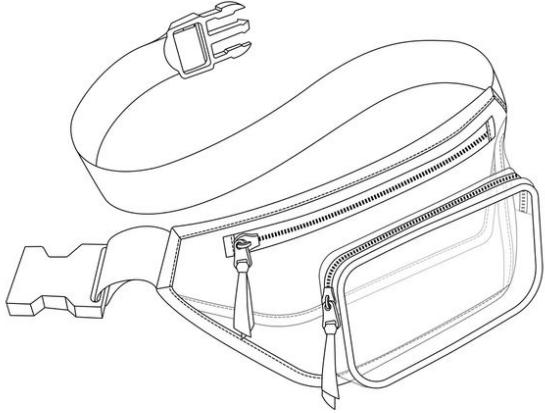
Layer	Protocol data unit (PDU)	Function ^[26]
Host layers	7 Application	High-level protocols such as for resource sharing or remote file access, e.g. HTTP .
	6 Presentation	Translation of data between a networking service and an application; including character encoding , data compression and encryption/decryption
	5 Session	Managing communication sessions , i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4 Transport	Reliable transmission of data segments between points on a network, including segmentation , acknowledgement and multiplexing
Media layers	3 Network	Structuring and managing a multi-node network, including addressing , routing and traffic control
	2 Data link	Transmission of data frames between two nodes connected by a physical layer
	1 Physical	Transmission and reception of raw bit streams over a physical medium





Hardware

1. Raspberry Pi Zero w/ USB HAT
2. Standard Phone as Analysis Console
3. External NIC(s)
4. Nice BT Dongle





Augmented Reality Through Wearable Computing
MIT 1997



Side Quests

802.15.1 Bluetooth

**7.5
BILLION NEW
DEVICES IN 2027**

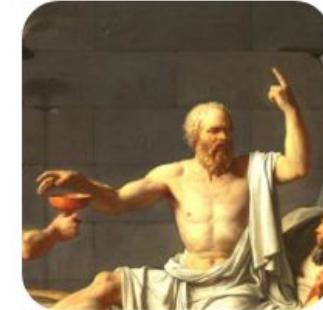
**BROADCASTS
USER-INPUTTED
DATA PUBLICLY**

**BEACONS
GEOLOCATABLE IN WIGLE!**

**MOBILE
PHONES BEACON
EVEN WHEN DEVICE IS OFF!!!**



darkmentorllc/ Blue2thprinting

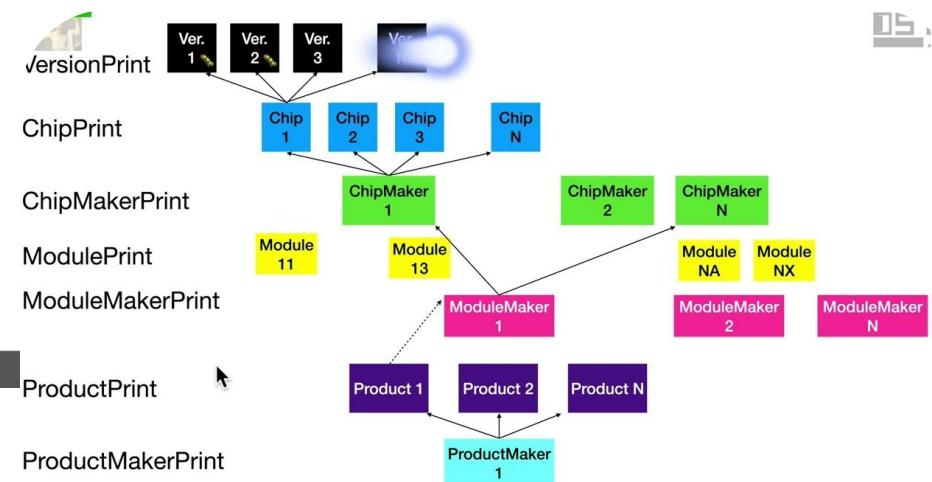


Code associated with talk "Blue2thprinting (blue-[tooth]-printing]: answering the question of 'WTF am I even looking at?!"'

1
Contributor

0
Issues

15
Stars



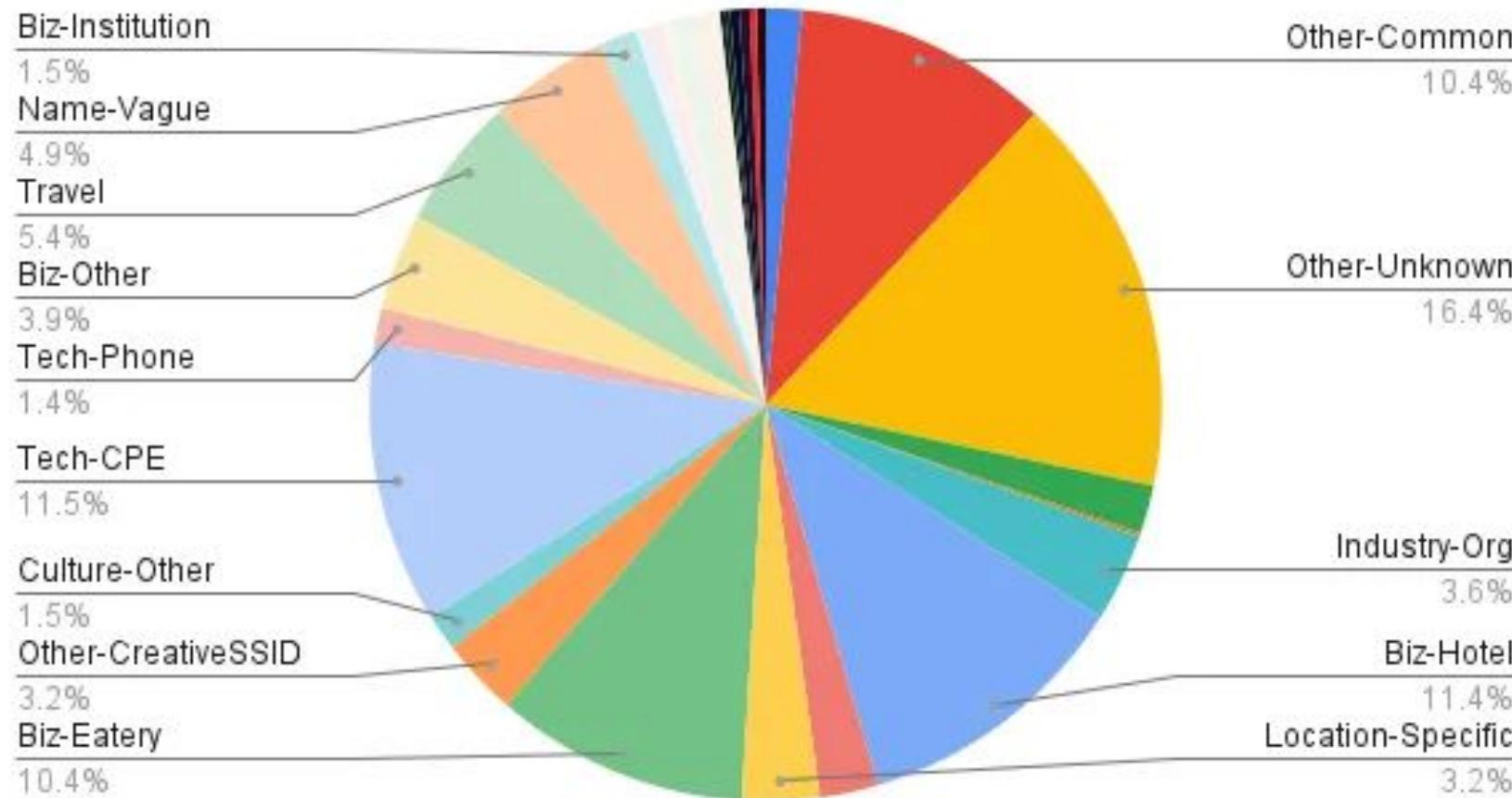
Experiment



Industry Conference
15,000+ attendees
2 hours of pcaps
66,823 Probe Requests
4,015 Unique ESSIDs
594 Bursts of Probe Requests
35 Bursts with 8+ ESSIDs

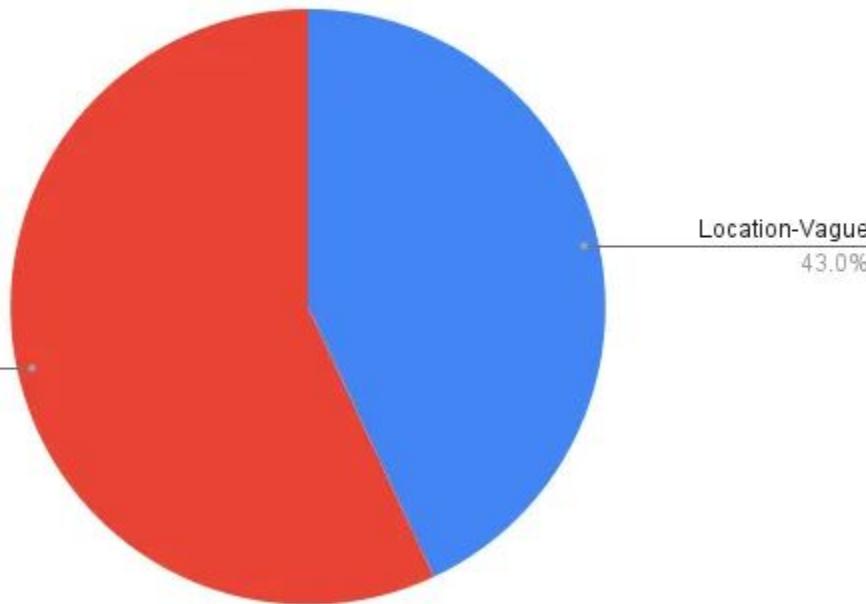
Observations

Count of Categories of SSIDs



Manual Analysis - Locations

Locations



Surprisingly, Specific locations in SSIDs are more common than vague locations. A specific location consists of a house number and street name or a specific building, oppose to just a neighborhood or city.

Anomalous SSIDs (in Hex)

On/Off Pattern

00000000ffffffffffff000000

00000000ffffffffffff000000000000

Possibly just being creative

7c7c7c7c7c7c7c7c7c7c7c7c7c7c7c7c7c7c
|||||||

Bbaaceaad6c7c4dcc9fabbeeb9dd
» ª ¹ | M Ì É ú » ¹ Ÿ

Non-printable Characters

2b89c8402a89c8802a89c800030000

5489c8805389c8c05389c840020000

E29da4efb88ff09f8d9550697a7a61206c6f7665
72



Non-conforming

21333e1b3186dc5ebd44a3b613668671ad99c4ff53834dca9aa857791f5f135edb8eb06d729a98fd60c79fd8193dcff580c042f6ac94b96a4a42ebf237f653389a72b64d2d67451c9f67dc6f7af5ef2f50737a9bbcf808718dd6c46ffee6677e

96 bytes(32 bytes max)

First names are common in SSIDs

iPhone de Ping
iPhone de ronaldo
iPhone de Sara
iPhone de SNEYDER
iPhone von Katrin pri
iPhone von Madeleine
iPhone von Philipp Lo
Isabel's iPhone
Jake's iPhone
Jeremy's iPhone

Mario's Galaxy Z Flip3 5G
Okila's Galaxy A53 5G
Olga's Galaxy A53 5G
Rafa's Galaxy A52s 5G
Robert's Galaxy Z Fold3 5G
Romain's Galaxy A54 5G

```
+-----+-----+-----+-----+
| ssid_hex | wlan_sa | time | rssi |
+-----+-----+-----+-----+
| 416e6120 | 2e:80:37: [REDACTED] | 1718042310.909904838 | -90,-91,-90 |
+-----+-----+-----+-----+
echo -n 416e6120 [REDACTED] | xxd -r -p
Ana [REDACTED]
```

Not Shown: Super-high correlation of known location to where beacons were observed

A Google search results page for the query "Ana". The top result is a blurred profile picture followed by the name "Ana" and the title "Business executive". Below the search bar, there are links for "All", "Images", "News", "Videos", "Maps", "Books", "Web", and "Tools". On the left, there's a blurred LinkedIn profile for "LinkedIn - Ana" with "3.8K+ followers". On the right, there's a blurred Wikipedia link and a "Feedback" button.

Google

All Images News Videos Maps Books Web Tools

Ana [REDACTED]
Business executive

LinkedIn - Ana
3.8K+ followers

Ana

Wikipedia
<https://en.wikipedia.org/wiki/Ana>

Ana

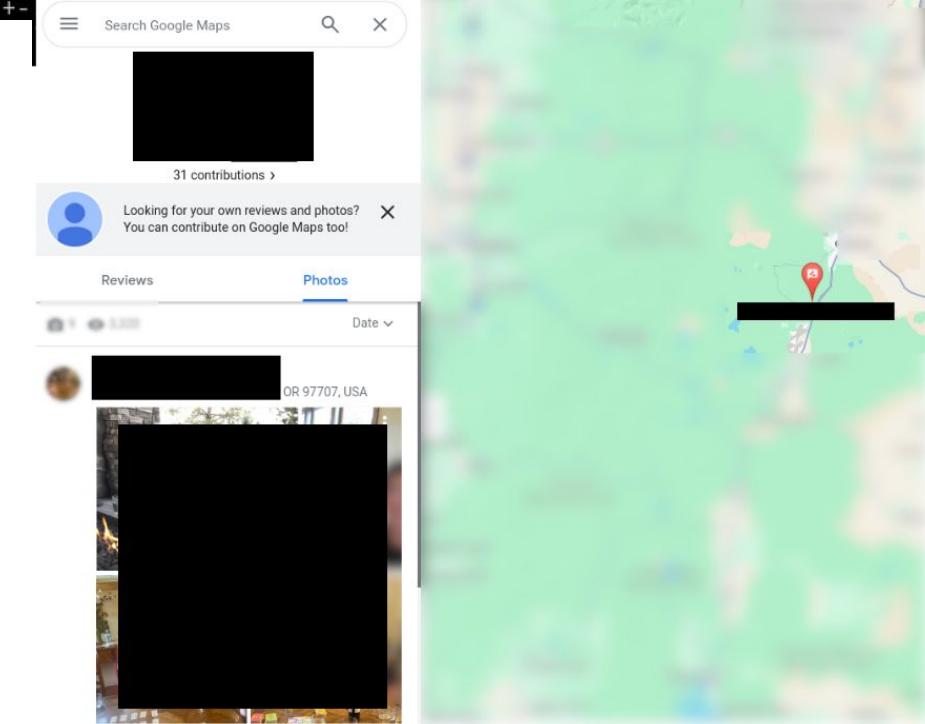
About
Ana
[. Wikipedia](#)

Feedback

Profiles

in

ssid_hex	wlan_sa	time	rssi	freq	seq	vht	is_processed
3536	8e:a3:87:	1709219168.953032000	NULL	NULL			1
3536	f2:51:b3:	1709219168.997215000	NULL	NULL			1
3536	ca:2a:87:	1709219169.278963000	NULL	NULL			100
3536	ca:2a:87:	1709219169.298522000	NULL	NULL			100
3536	b6:68:b5:	1709220147.656812000	NULL	NULL	NULL	0x0f817832	100
3536	b6:68:b5:	1709220147.678076000	NULL	NULL	NULL	0x0f817832	100



<- Street Address as SSID

- Only one result in US
- Residence
- Contributor put pictures from family event on google maps

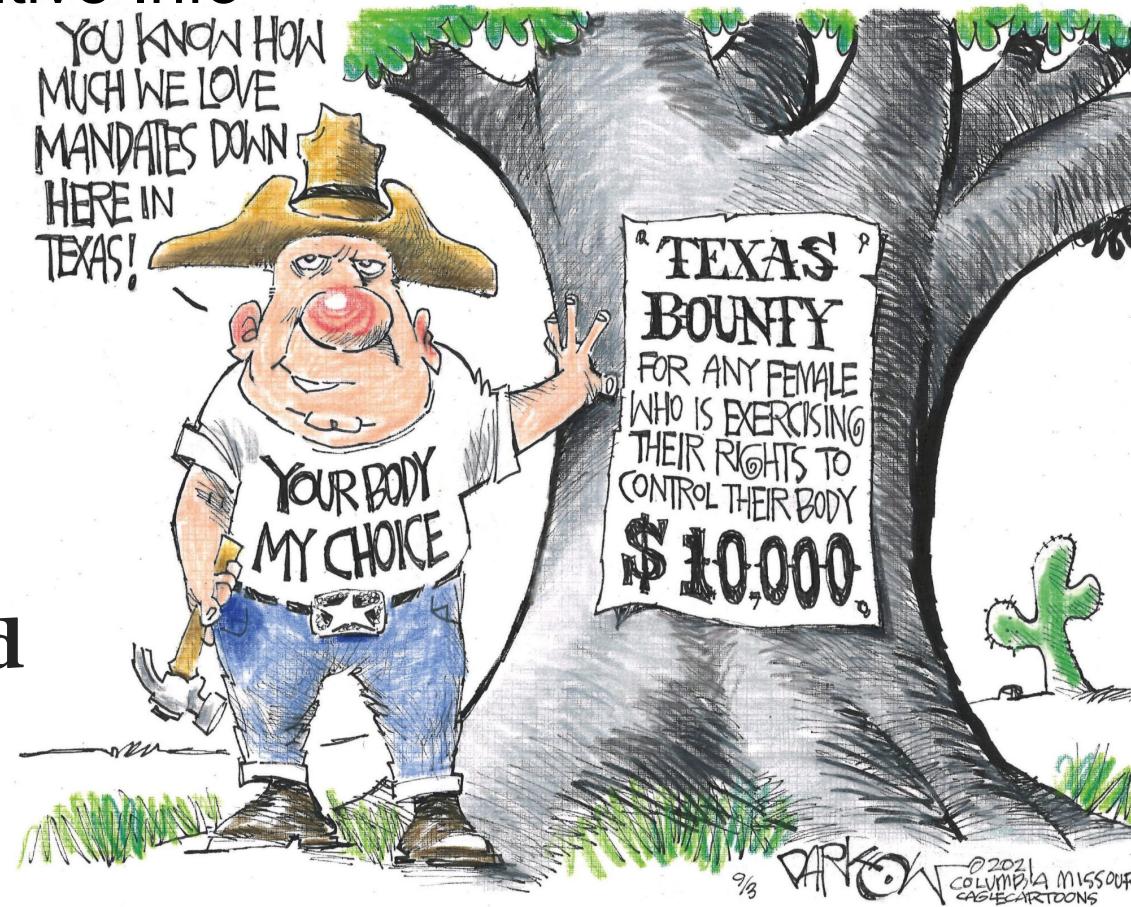
Manual Analysis - Sensitive Info

Out of 4015 SSIDs

11 SSIDs contained first name and last name.

17 SSIDs correlated to healthcare providers.

.5% of SSIDs contained Sensitive Info



Sequence Numbers



frame 115: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
IEEE 802.11 Probe Request, Flags:

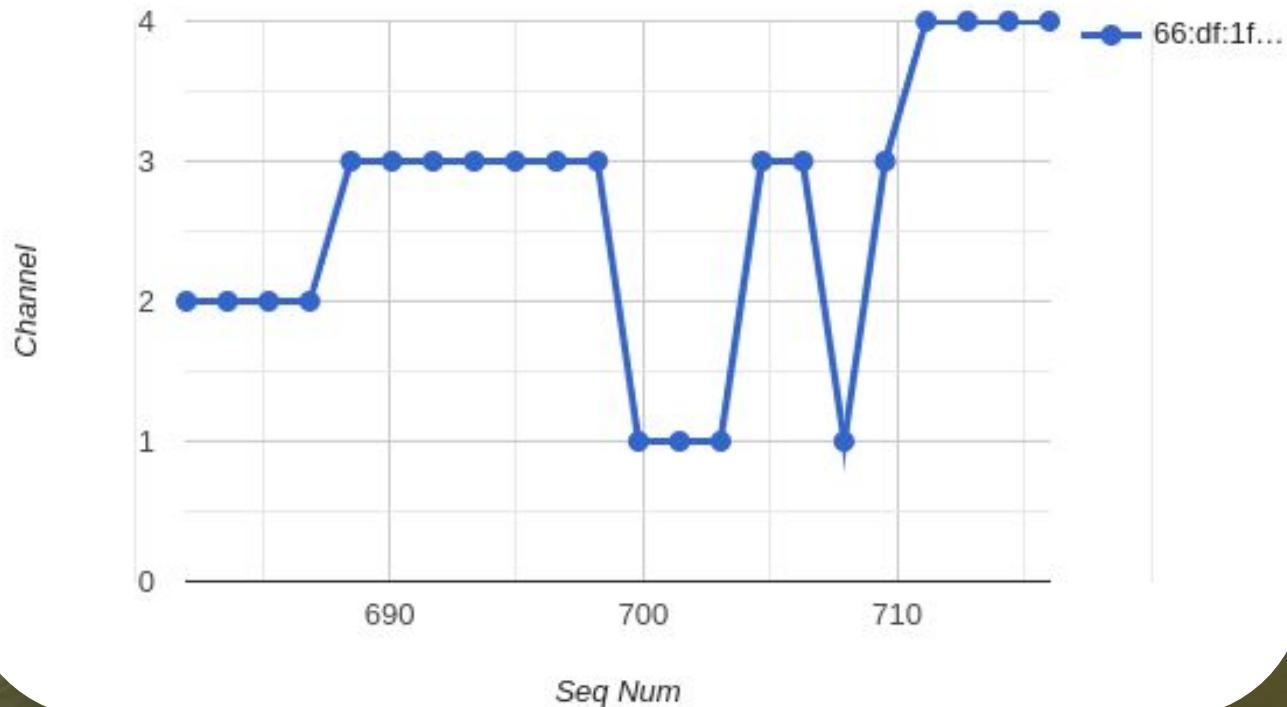
- Type/Subtype: Probe Request (0x0004)
- Frame Control Field: 0x4000
 -00 = Version: 0
 - 00.. = Type: Management frame (0)
 - 0100 = Subtype: 4
- Flags: 0x00
 -00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
 -0.. = More Fragments: This is the last fragment
 - 0... = Retry: Frame is not being retransmitted
 - ..0 = PWR MGT: STA will stay up
 - .0. = More Data: No data buffered
 - .0... = Protected flag: Data is not protected
 - 0.... = +HTC/Order flag: Not strictly ordered
- .000 0000 0000 0000 = Duration: 0 microseconds
- Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
- Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
- Transmitter address: GELighti_7b:ff:7d (34:13:43:7b:ff:7d)
- Source address: GELighti_7b:ff:7d (34:13:43:7b:ff:7d)
- BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
- 0000 = Fragment number: 0
- 0111 0000 1001 = Sequence number: 1801

IEEE 802.11 Wireless Management

- Tagged parameters (41 bytes)
 - Tag: SSID parameter set: "Samsung Galaxy S9+_6236"
 - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
 - Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]

Discovery!

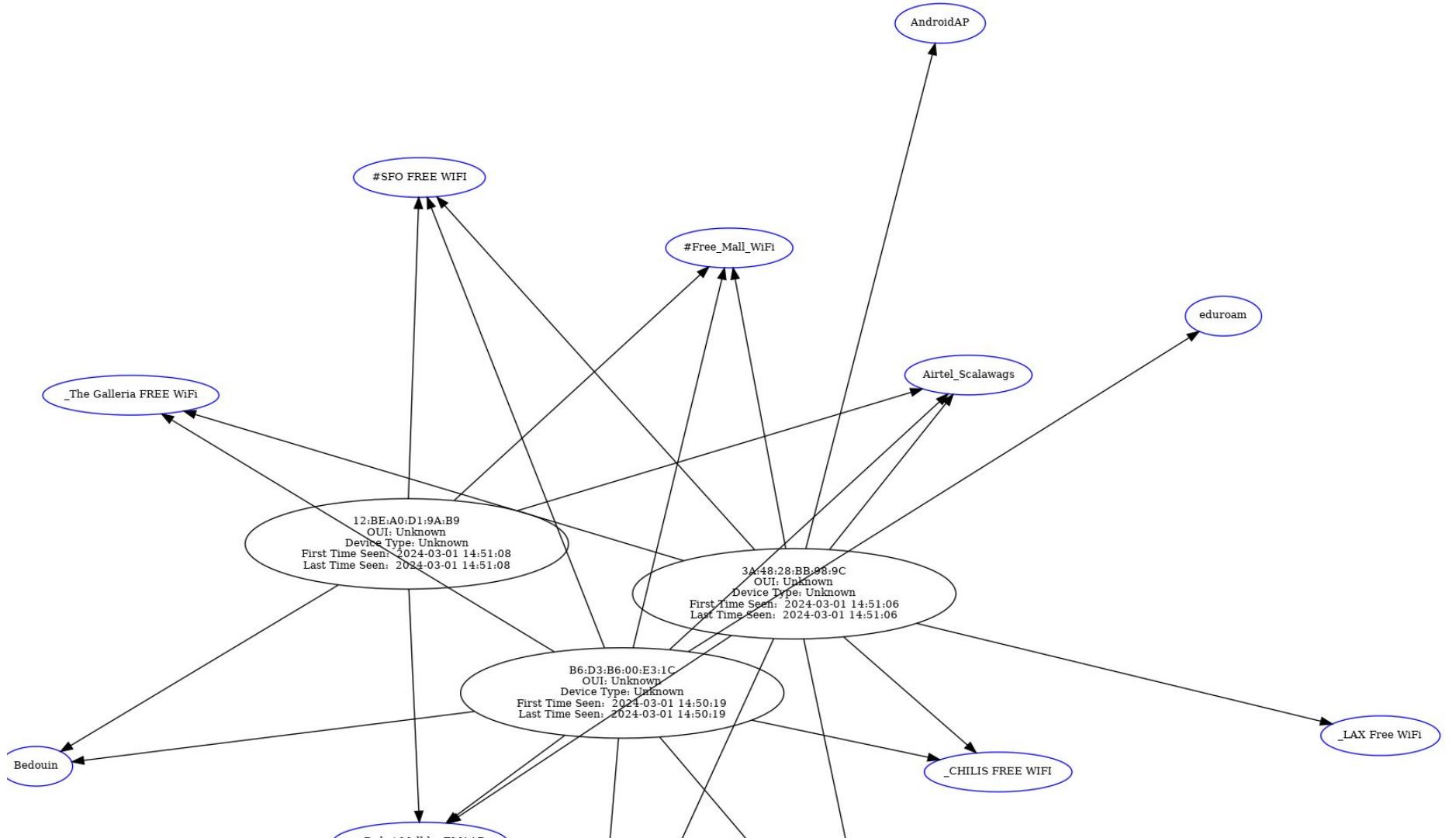
Sequence Number and Channel



Saving...

WiFi Bursts





Defining Bursts

- Method 1
 - Same MAC addresses
 - within 1 second
- Method 2
 - Sequence Number within 60
 - within 1 second
 - RSSI +/- 2
- Method 3
 - Same VHT Capabilities Flag
 - Within 1 second
 - RSSI +/- 1

SSIDs in Burst

More than 7

5.4%

6

2.5%

5

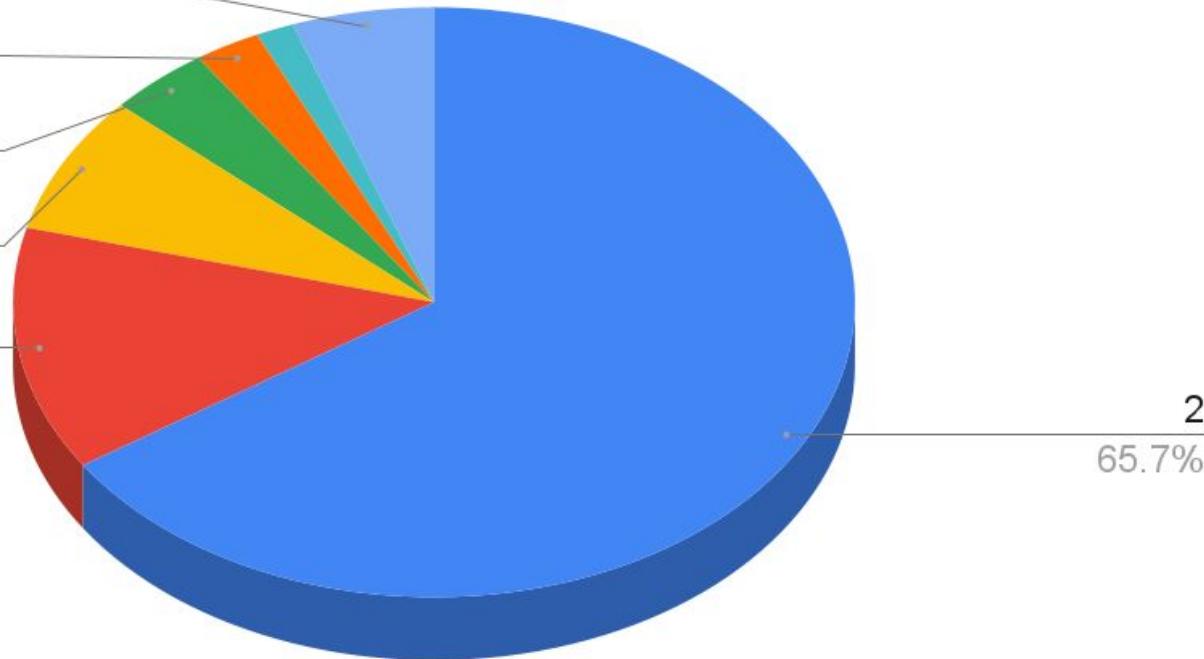
3.9%

4

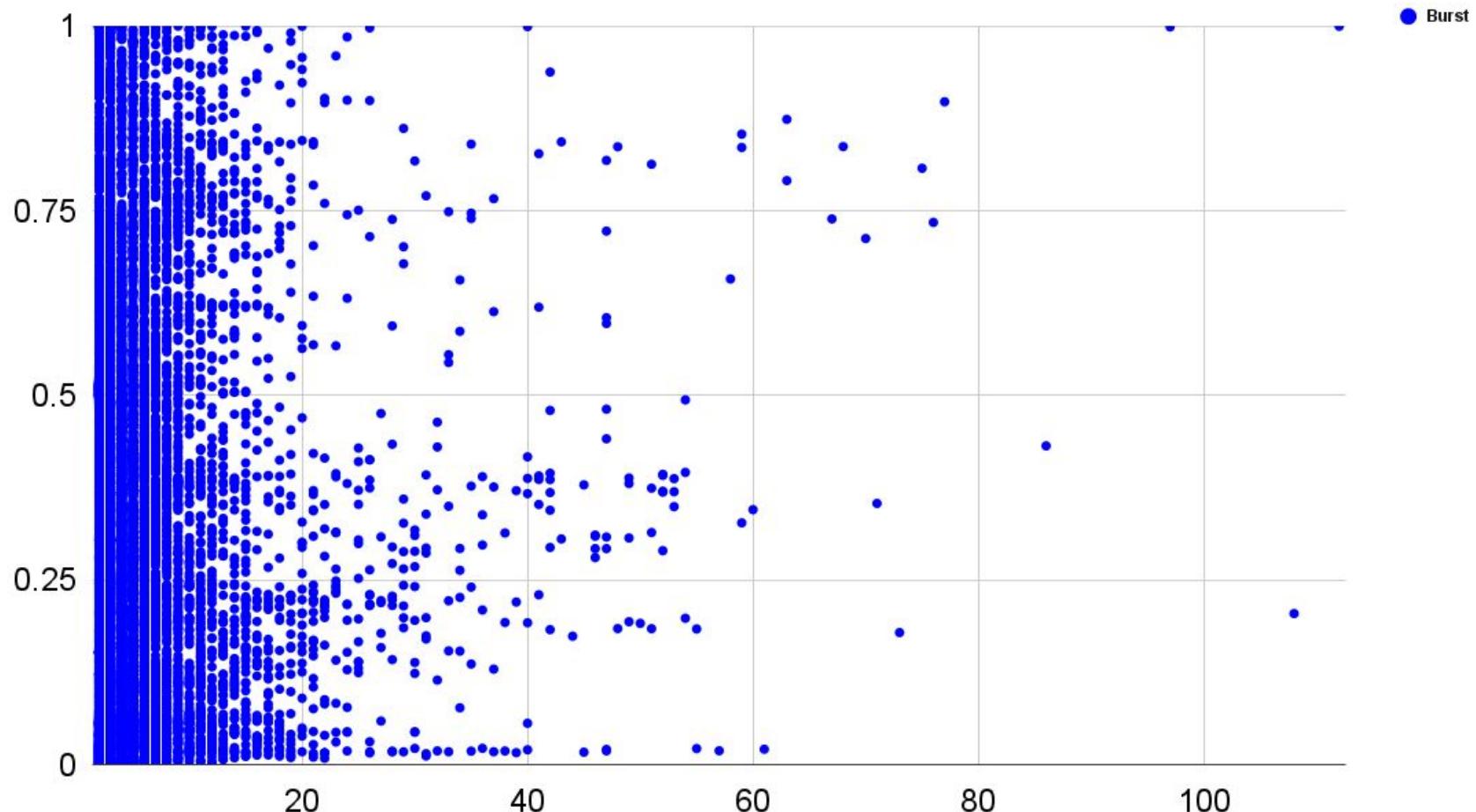
7.6%

3

13.4%



Count vs Duration

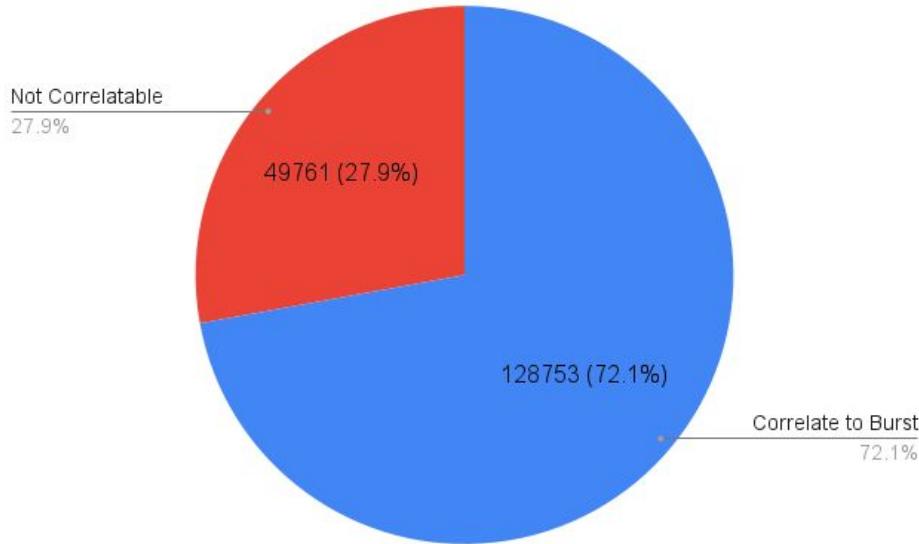


**iDEVICES: 83% CHANCE
BURST IS .02 SECONDS**

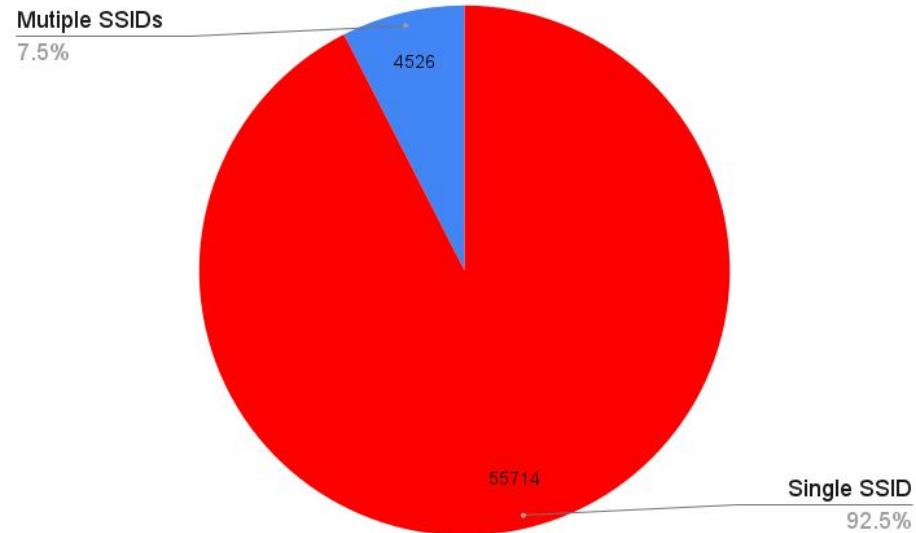


17% CHANCE BURST IS .06 SECONDS

[9]



72% of Probe Requests can be correlated to a Burst



7% of bursts contain multiple SSIDs

Unknown -> ChatGPT



What does ChatGPT
know about WiFi
Names?

Potential for LLM Integration

what is BeTulumGuest-GigNet



BeTulumGuest-GigNet appears to be a Wi-Fi network name or service, likely associated with Be Tulum, a boutique hotel or resort in Tulum, Mexico. GigNet is a company that provides high-speed internet and connectivity solutions. In this context, BeTulumGuest-GigNet would be the Wi-Fi network provided for guests at the Be Tulum hotel, leveraging GigNet's internet services to ensure a reliable and fast connection for visitors. If you need more details about the network or services, contacting the hotel directly or visiting their website might be helpful.



what is "Mercure Debrecen"

"Mercure Debrecen" refers to a hotel located in Debrecen, Hungary. It is part of the Mercure hotel chain, which is a global brand within the Accor group, known for offering mid-range accommodations. The Mercure Debrecen would typically provide amenities such as comfortable rooms, a restaurant, meeting facilities, and possibly other services geared toward business and leisure travelers.

If you need specific details about the hotel, such as services, booking information, or amenities, it would be best to visit their official website or contact them directly.

SSID2Location with LLM

```
"where is MNHN-Openwifi"
```

MNHN-Openwifi is a project by the Muséum national d'Histoire naturelle (MNHN) in France that aims to map open Wi-Fi networks. It is not a physical location but rather a digital project. You can find more information about MNHN-Openwifi on their official website or by searching for their project repository on platforms like GitHub.

Conclusions

- It is highly plausible that threat actors can be identified.
- PII and sensitive information is being leaked through wireless beacons

Takeaways

- Avoid Naming SSIDs with identifiable information
- Digital signature is being tracked
- High probability this can be used for blue team -
 - Vetting new acquaintances
 - Supplementary authentication factors
- Randomization is not enough - Analytics industry is growing

Mitigate the Risk

1. Manage the Preferred Network List with MDM, Purge SSIDs with PII
2. Educate users and encourage common or non-identifying SSIDs
3. Disable Auto-Connect?
4. Restrict Bluetooth wearables for VIPs
5. User Awareness Training

Acknowledgements and Thank yous



Sources

1. Arthur, Charles. "Google Admits Collecting Private Data via Wi-Fi." *The Guardian*, 15 May 2010, www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data.
2. "WiFi Probe Request - A Brief Explanation." *Spacehuhn Blog*, blog.spacehuhn.com/probe-request. Accessed 7 Sept. 2024.
3. "CWAP – HT Capabilities IE." *MRNCCIEW Blog*, 19 Oct. 2014, mrncciew.com/2014/10/19/cwap-ht-capabilities-ie/. Accessed 7 Sept. 2024.
4. "Crowd Monitoring in Smart Destinations Based on GDPR-Ready Opportunistic RF Scanning and Classification of WiFi Devices to Identify and Classify Visitors' Origins." Accessed 7 Sept. 2024.
5. Yang, Fei, Ilias Ahriz, and Bruce Denby. "Tools for Ground-Truth-Free Passive Client Density Mapping in MAC-Randomized Outdoor WiFi Networks." *Sensors (Basel)*, vol. 23, no. 13, 4 July 2023, p. 6142, doi:10.3390/s23136142. PMC10346771.
6. "Location Analytics." *Meraki Documentation*, documentation.meraki.com/MR/Monitoring_and_Reportin
- g/Location_Analytics. Accessed 7 Sept. 2024.
7. "Manage Location Settings." *Google Android Help*, support.google.com/android/answer/3265955. Accessed 7 Sept. 2024.
8. "Global Bluetooth Device Shipment Forecast 2020-2030." *Statista*, www.statista.com/statistics/1220933/global-bluetooth-device-shipment-forecast/. Accessed 7 Sept. 2024.
9. "Enhancing Crowd-Monitoring Through WiFi Fingerprint Analysis." *Politecnico di Torino*, webthesis.biblio.polito.it/secure/28445/1/tesi.pdf. Accessed 7 Sept. 2024.

Demonstration and Q&A

2:00 ▲ ⚡ ▲ ☺ •

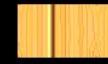


← C2



```
Naples medium range
513 Raymond James WLAN medium range
temp=66.6'CNULL Raymond
NULL Raymond James WLAN medium range
NULL Raymond
RJ Remote Office WLAN medium range
NULL 0
Raymond James WLAN medium range
NULL Raymond
RJ Remote Office WLAN medium range
NULL 0
RJ Remote Office WLAN medium range
NULL 0
Raymond James WLAN medium range
NULL Raymond
RJ Remote Office WLAN medium range
NULL 0
RJ Remote Office WLAN medium range
NULL 0
Raymond James WLAN medium range
NULL Raymond
```

1526
temp=67.1'C



RHOTELS-STAFF near by
BIZ_HOTEL 0

```
SSID medium range
viya medium range
Bell319 medium range
viya medium range
USALobby medium range
SSID medium range
SSID near by
viya near by
USALobby medium range
Bell319 medium range
StreamPineapple medium range
```