DOXing with Wi-Fi probe requests

BONUS PROJECT SEMOSY 2023

YANNIC HEMMER

Probe Request

What are probe requests?

- Used to **establish connections**
- Client-side alternative to beacon frames
- Client searches for **"known" access points**
- Leaking the PNL

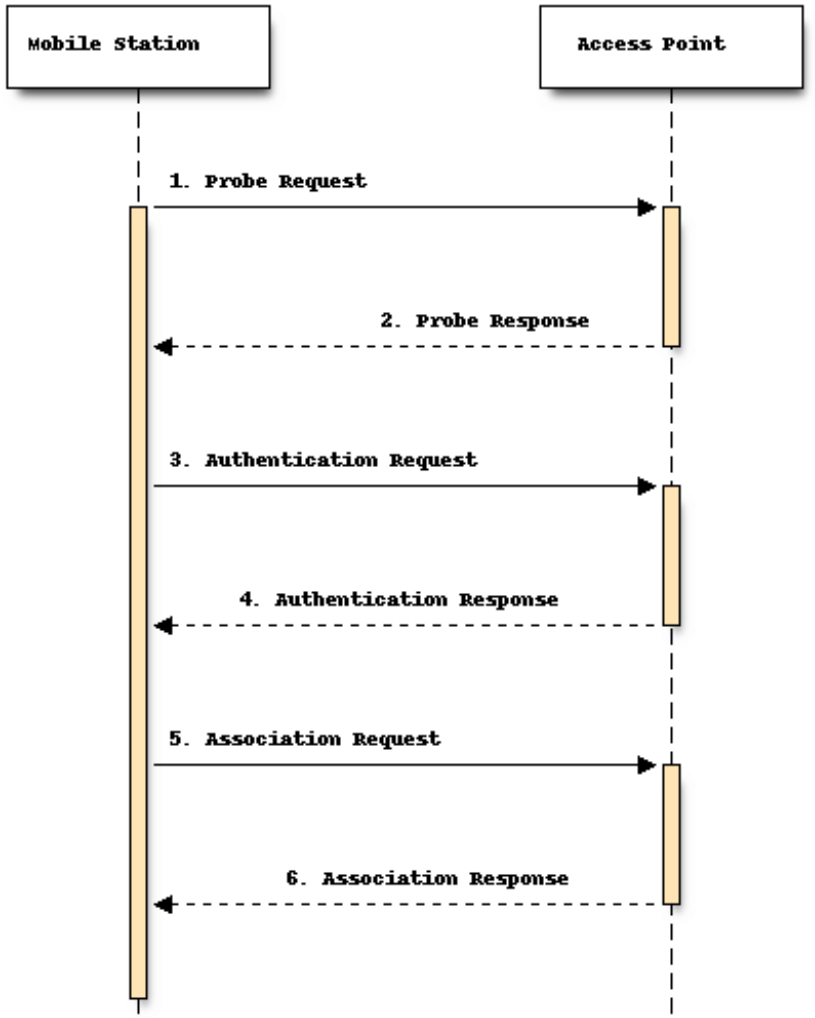


Image source:
https://probequest.readthedocs.io/en/stable/probe_requests.html

Probe Request Frame

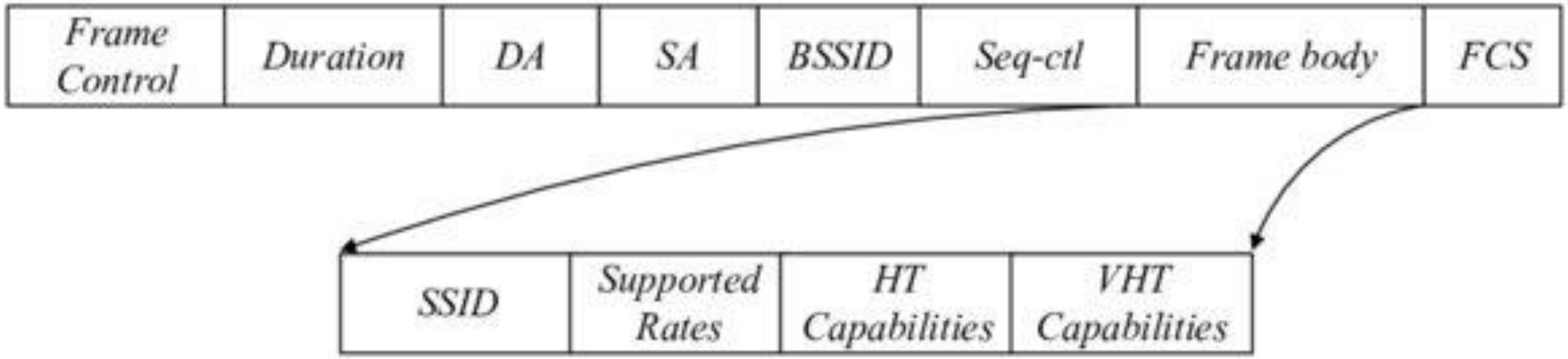


Image source:
http://dx.doi.org/10.3390/s20164620

Useful Information

- ~~Destination Address (DA)~~
  ff:ff:ff:ff:ff:ff
- Source Address (SA)
  unique device identifier
- ~~BSSID~~
  ff:ff:ff:ff:ff:ff
- SSID
  location identifier*

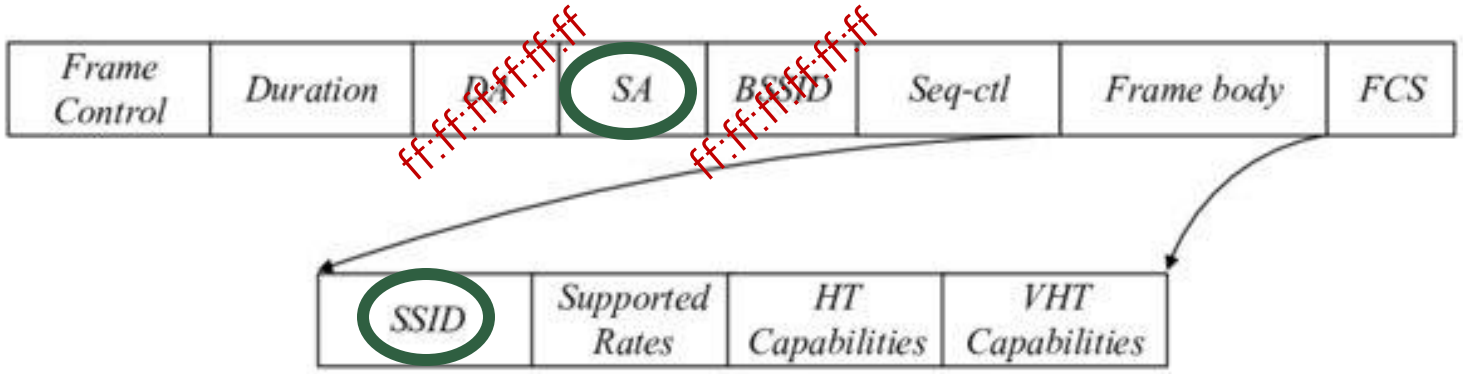
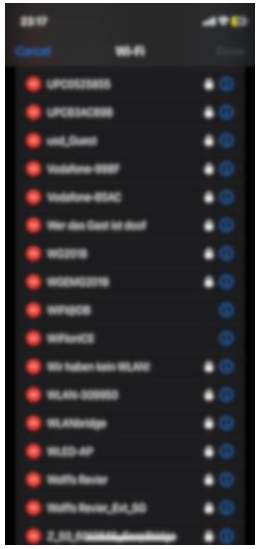
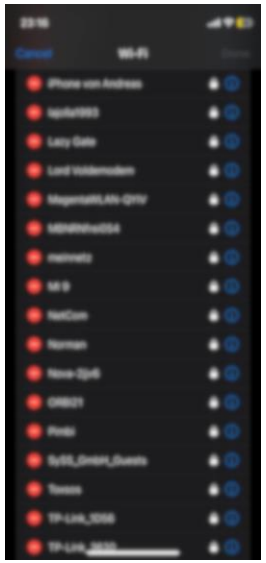
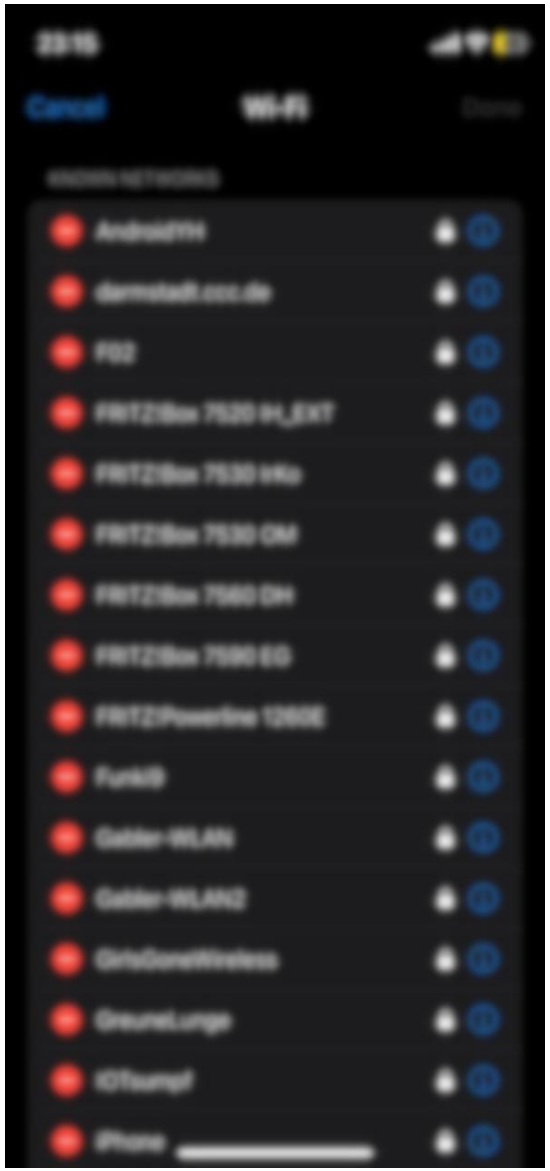


Image source:
http://dx.doi.org/10.3390/s20164620







Preferred Network List (PNL)

Collection tool: probequest

- Installation
  pip3 install --upgrade probequest
- Can create fake data for testing
- Output to csv
- Alternatives:
  - Wi-Fi Pineapple
  - Tcpdump

time	MAC	OUI	SSID

SSID -- ??? --> Location

wigle.net

- Over 1 Billion unique networks
- Germany 2nd place (77 million)
- *Larger databases (google, mozilla)*
- *API (interactive and free with swagger)*
- Higher API limit for "*research purposes*"

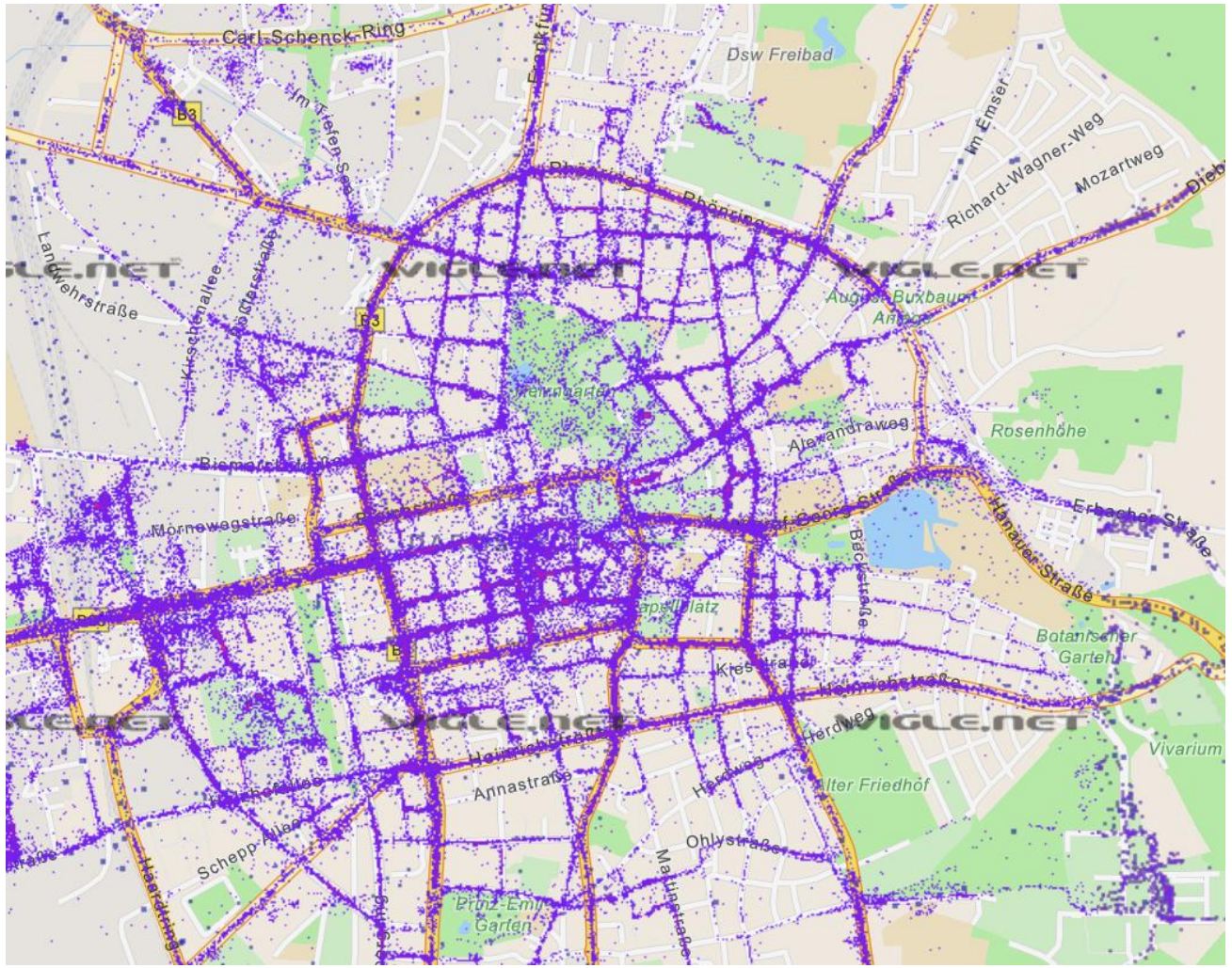


Image creation source:
https://wigle.net/map

My Implementation

- Set Wi-Fi Adapter to Monitoring Mode
- Collect Data with probequest
- Parse Data to hierarchical Structure
  unique MAC –1:m-> SSID
- API Requests to wigle.net for every SSID
- Parse Location Data
  unique MAC --1:m--> SSID --1:n--> Locations (+ Additional Data)
- Visualize Locations on Map

DEMO

https://github.com/MeNoSmartBrain/wifiTracking

In Case Demo doesn't Demo

Further Reading

- Probe Request Based Device Identification Attack and Defense
  https://dx.doi.org/10.3390/s20164620
- Your Mobile Phone is a Traitor! -- Raising Awareness on Ubiquitous Privacy Issues with SASQUATCH
  https://www.researchgate.net/publication/278739961_Your_Mobile_Phone_is_a_Traitor_--_Raising_Awareness_on_Ubiquitous_Privacy_Issues_with_SASQUATCH
- ProbeQuest documentation
  https://probequest.readthedocs.io/en/stable/index.html
- Wigle swagger API
  https://api.wigle.net/swagger