Wi-Fi Leakage

Robin Wood

https://digi.ninja

These slides were presented at Tech for Troops at Sheffield Hallam on 6th March 2016.

The probes analysed were put together specially for the presentation and are not from a real phone.

https://digi.ninja

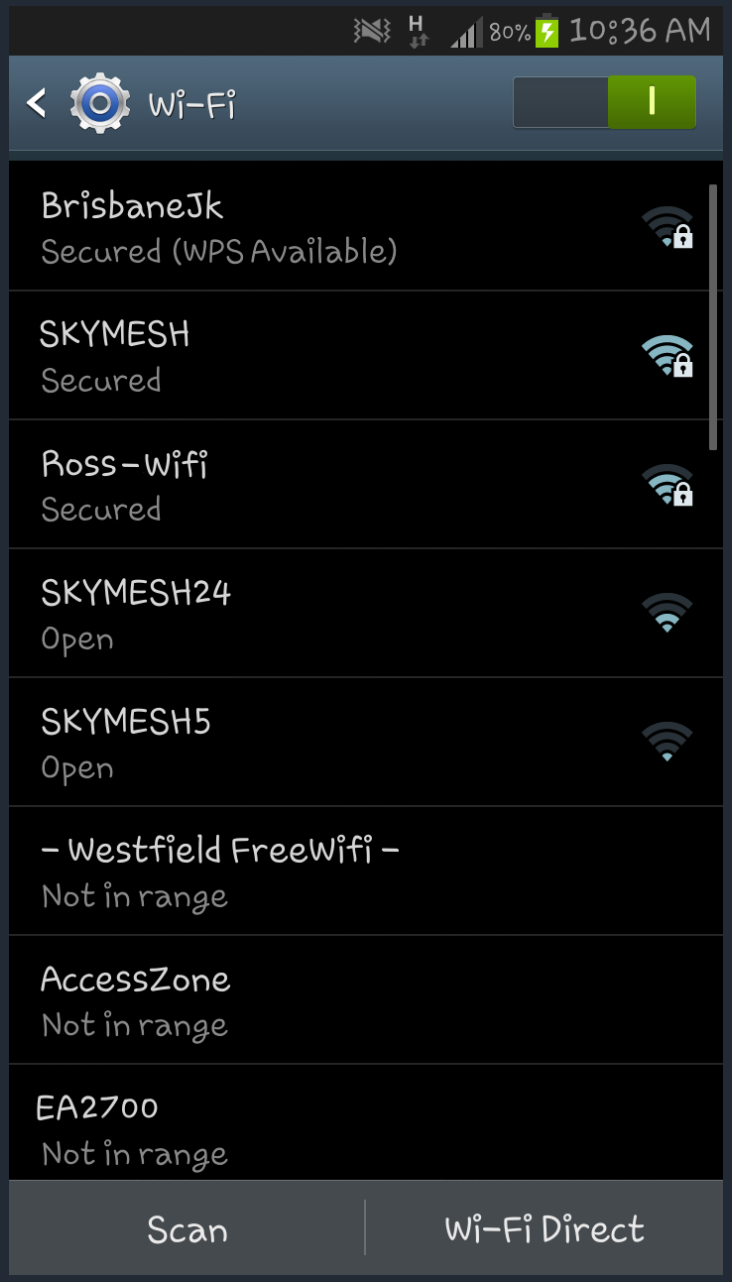
Who am I?

- Freelance security consultant
- In the industry for 8+ years
- Tested for most sectors including banks, casinos, retail and manufacturing

Who uses Wi-Fi on their phone?

Do you turn it off when you are not using it?

Please turn off Wi-Fi now if you do not want to be part of the live demo



https://digi.ninja


Home?
Office?
Yes Office is here
Gym?
Linksys?
MENU

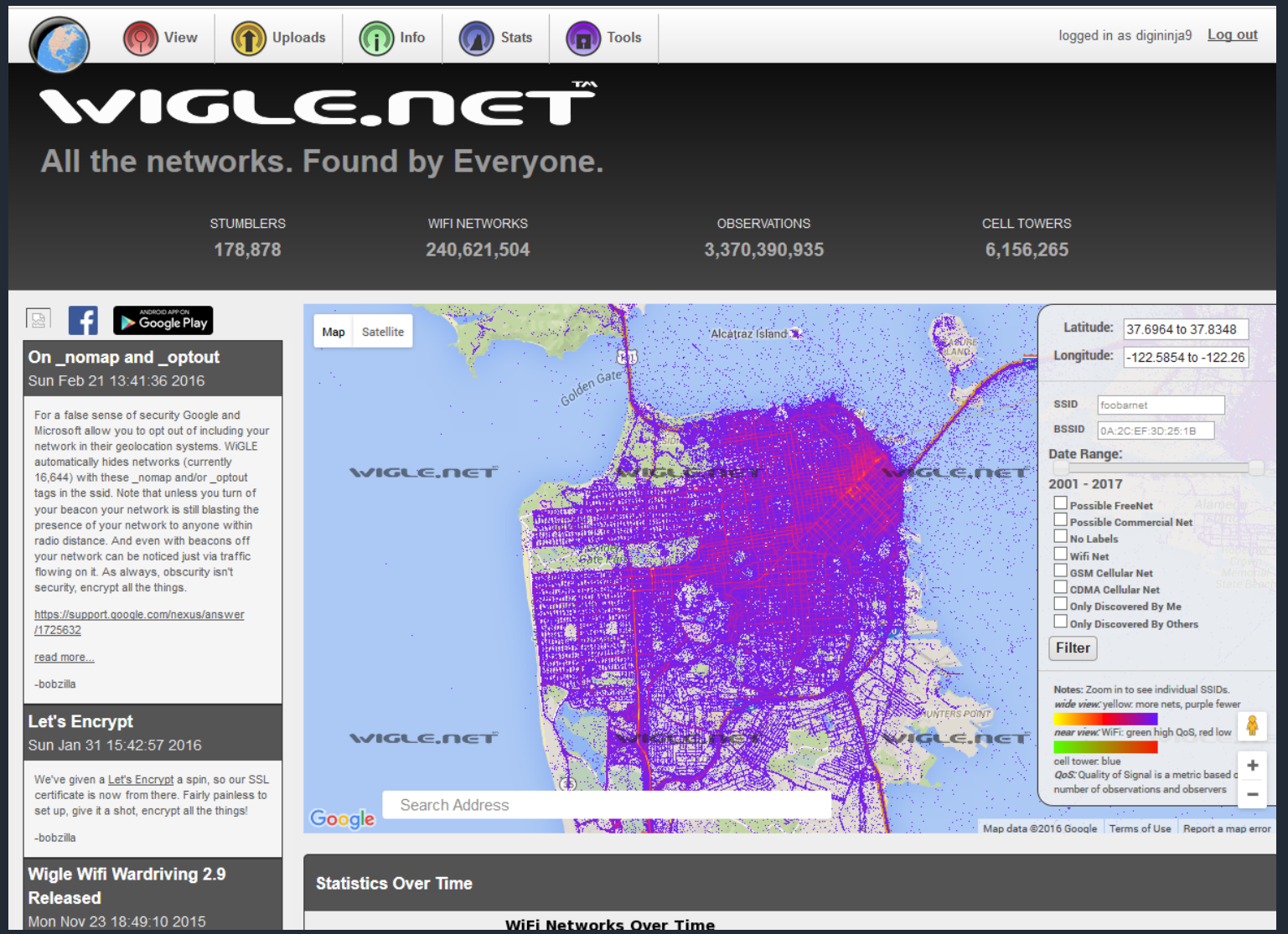
Aircrack-ng Suite

Station MAC, First time seen, Last time seen, Power, # packets, BSSID, Probed ESSIDs
00:26:37:93:D8:E1, 2016-03-02 15:12:37, 2016-03-02 15:12:44, -44, 71, 64:70:02:DE:AF:A7, UNION JACKS, jardinTropicalFREE, 0449woodseat, GDKENERGY, Natwest_Free_WiFi, Sheffield_First_Lounge, eastcoast-wifi, simonsandrawireless, icec-guest

Probe Requests

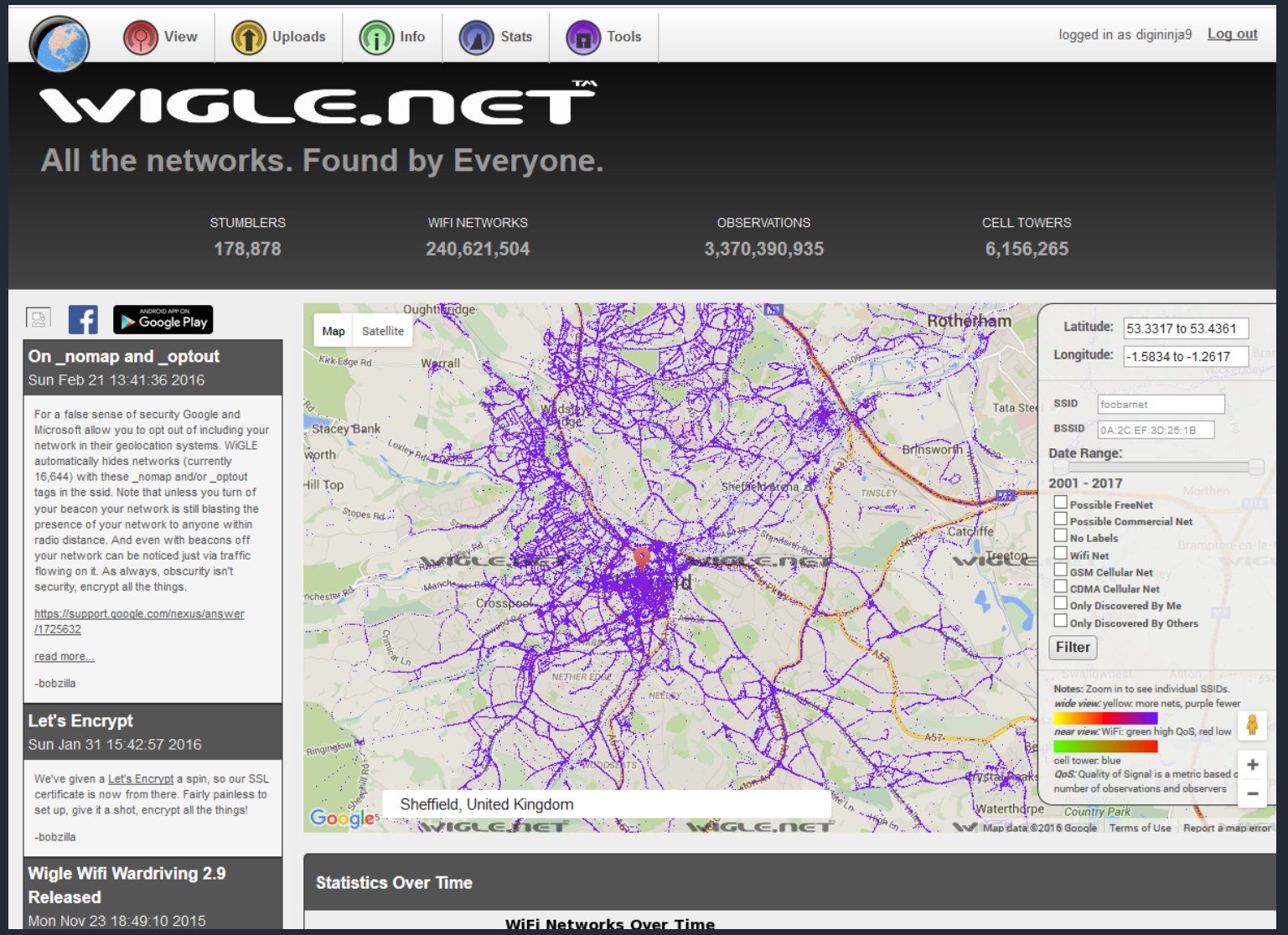
- The_Woodseats_Palace
- Ladbrokes WiFi
- Natwest_Free_WiFi
- 0449woodseat
- Sheffield_First_Lounge
- eastcoast-wifi
- icec-guest
- GDKENERGY
- simonsandrawireless
- jardinTropicalFREE
- UNION JACKS

Wigle.net



https://digi.ninja

Wigle.net Sheffield



https://digi.ninja

0449woodseat

Query for networks

Latitude: 47.25264 to: 47.25265 Longitude: -87.256243 to: -87.256244

Search Radius Tolerance(+/- degrees): 0.010

BSSID/MAC: 0A:2C:EF:3D:25:1B or 1st 3 Octets: 0A:2C:EF

SSID / Network Name (exact match): 0449woodseat

SSID / Network Name (wildcards[1]: % and _): foobar%

Last Observed: 20010925174546

☐ Must Be a FreeNet ☐ Must Be a Commercial Pay Net ☐ Only Networks I Was the First to Discover

Addresses are for the U.S. only (2002 Census data)

Street Address: 1600 Pennsylvania Ave State: DC Zip: 20502

Query **Reset**

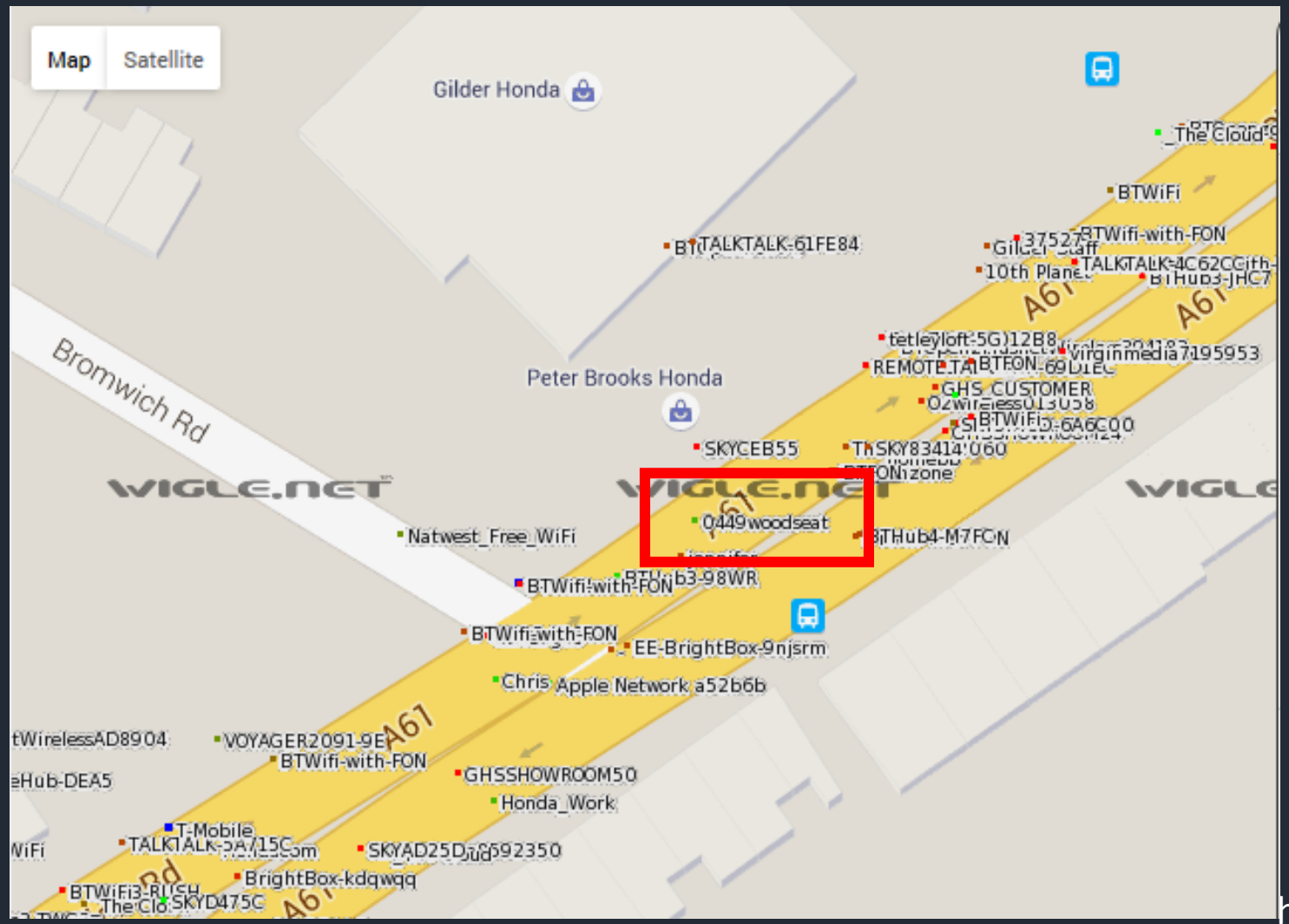
[1] SSID cannot start with a wildcard. '%' means zero-or-more characters, '_' means a single character.

<< | showing records 1 to 1 | >>

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS
map	00:15:70:C8:E5:40	0449woodseat		infra	2011-09-12 20:29:57	2016-02-04 09:40:04	WPA	53.33947754	-1.48069918	13		5

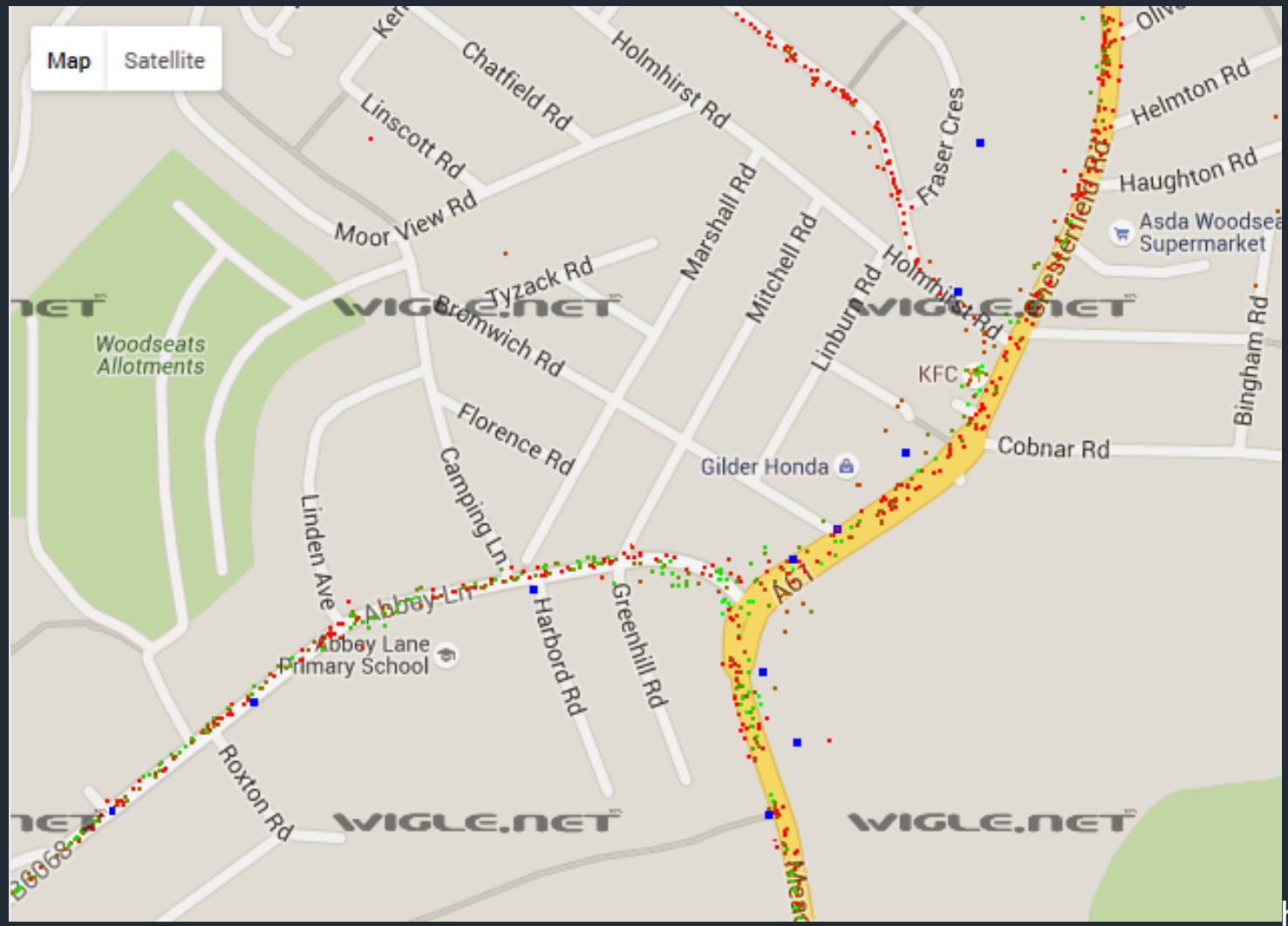
https://digi.ninja

0449woodseat



https://digi.ninja

0449woodseat

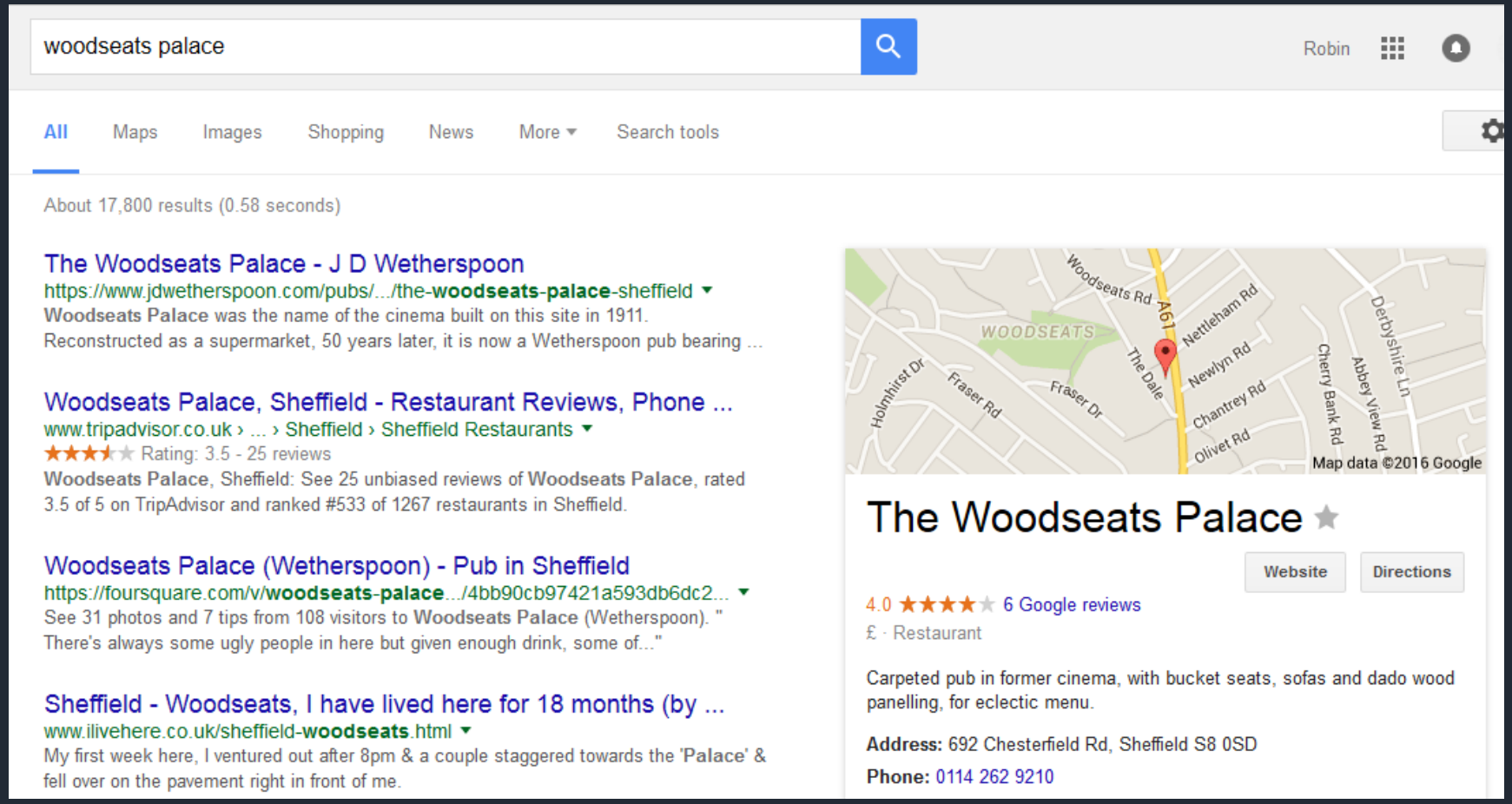


https://digi.ninja

0449woodseat

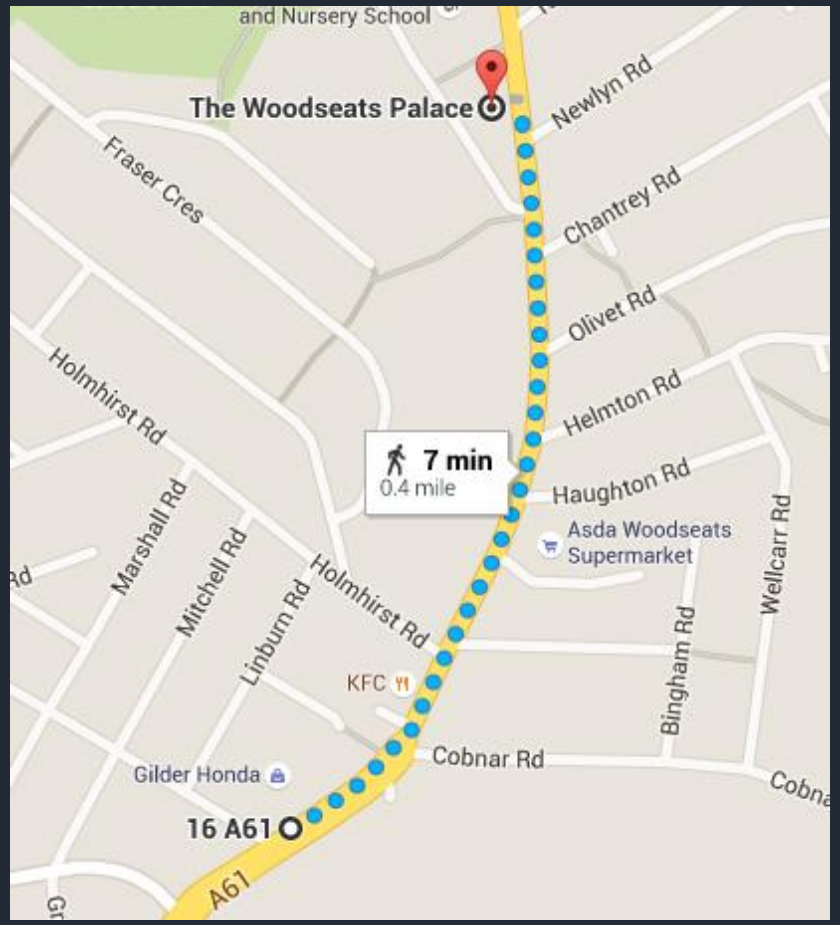
https://digi.ninja

The_Woodseats_Palace



https://digi.ninja

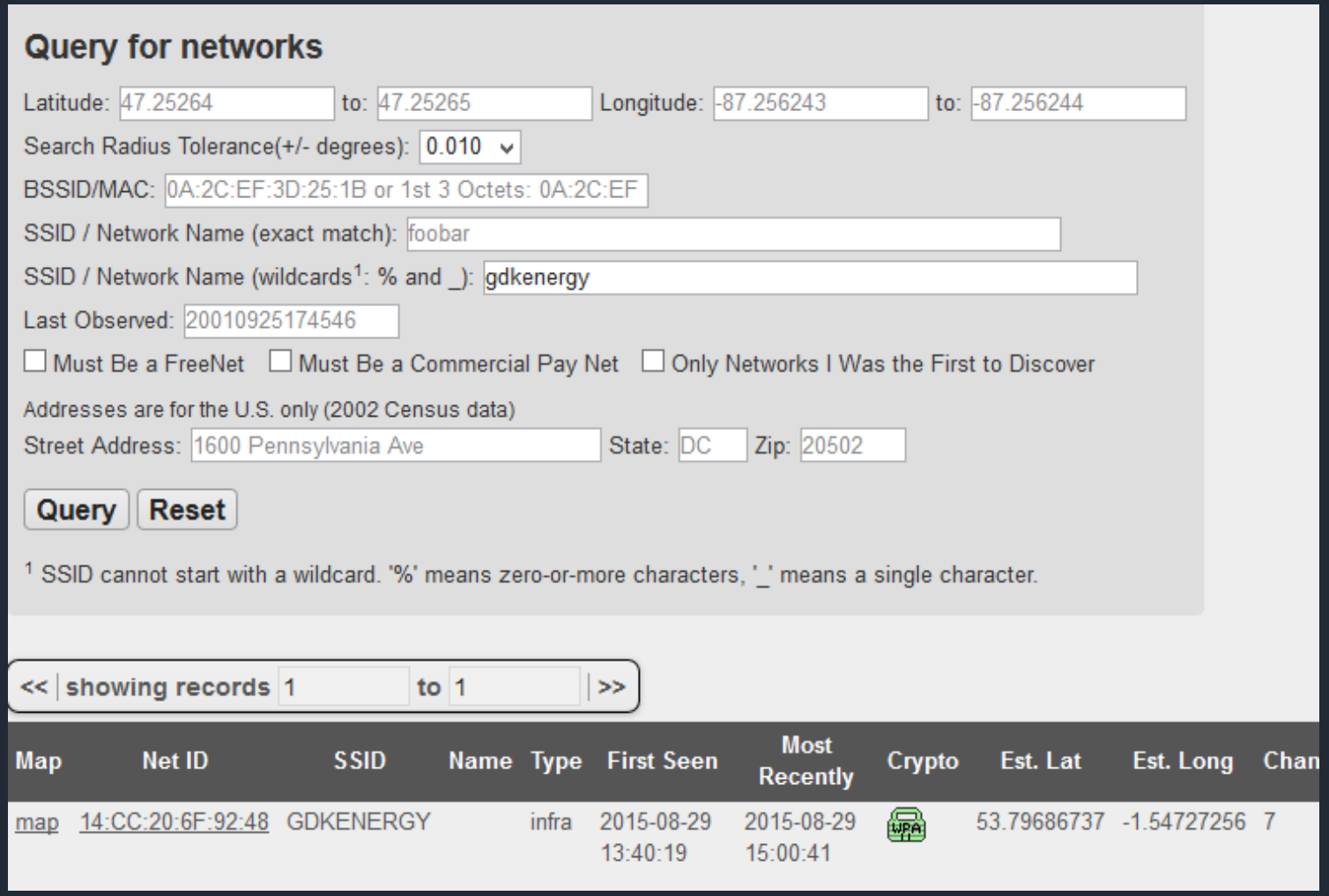
0449woodseat to The_Woodseats_Palace



https://digi.ninja

Ladbrokes

GDKENERGY



Query for networks

Latitude: 47.25264 to: 47.25265 Longitude: -87.256243 to: -87.256244

Search Radius Tolerance(+/- degrees): 0.010

BSSID/MAC: 0A:2C:EF:3D:25:1B or 1st 3 Octets: 0A:2C:EF

SSID / Network Name (exact match): foobar

SSID / Network Name (wildcards[1]: % and _): gdkenergy

Last Observed: 20010925174546

☐ Must Be a FreeNet ☐ Must Be a Commercial Pay Net ☐ Only Networks I Was the First to Discover

Addresses are for the U.S. only (2002 Census data)

Street Address: 1600 Pennsylvania Ave State: DC Zip: 20502

Query **Reset**

[1] SSID cannot start with a wildcard. '%' means zero-or-more characters, '_' means a single character.

<< | showing records 1 to 1 | >>

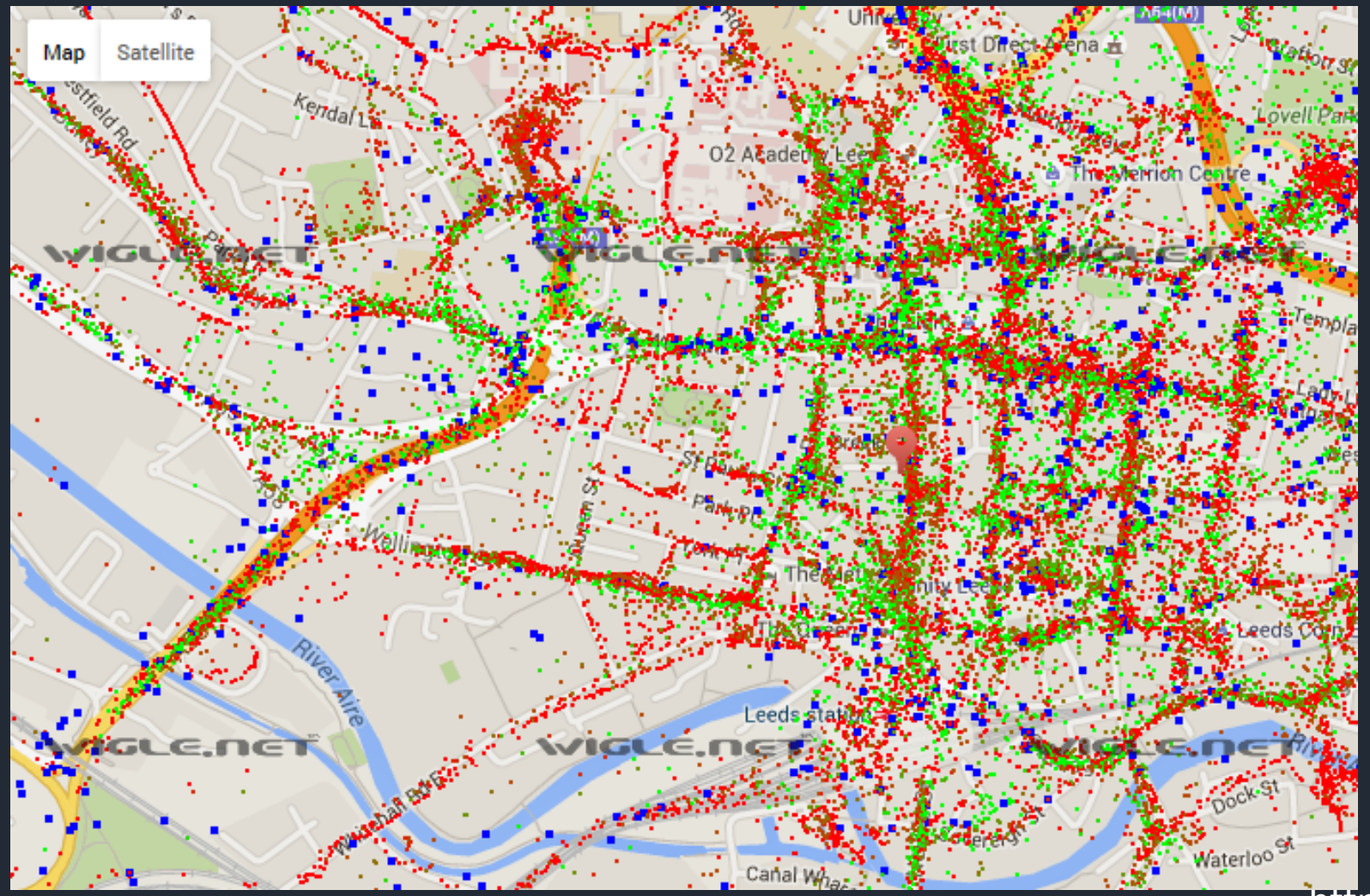
Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Chan
map	14:CC:20:6F:92:48	GDKENERGY		infra	2015-08-29 13:40:19	2015-08-29 15:00:41	WPA	53.79686737	-1.54727256	7

https://digi.ninja

GDKENERGY

https://digi.ninja

GDKENERGY

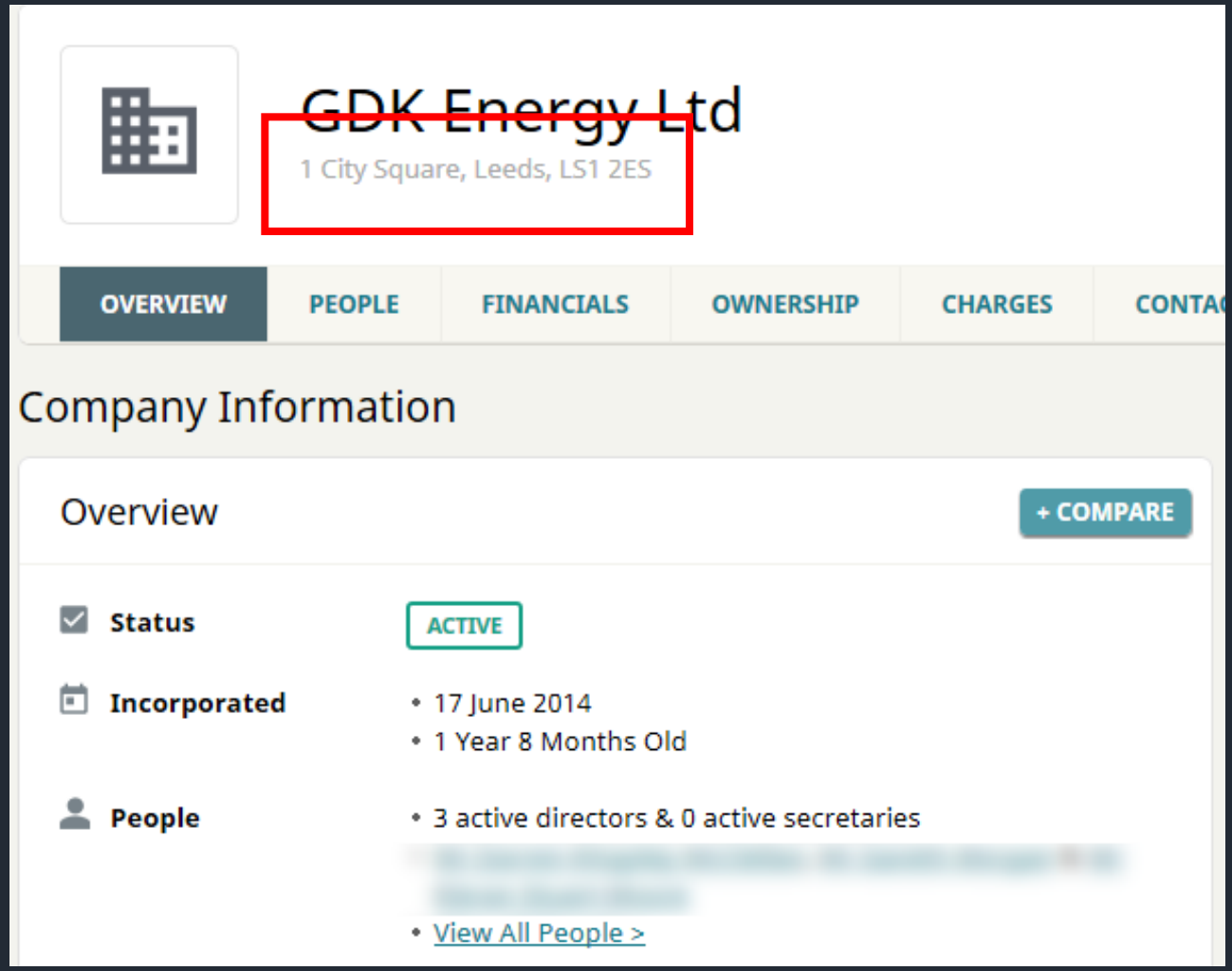


https://digi.ninja

GDK Energy Ltd

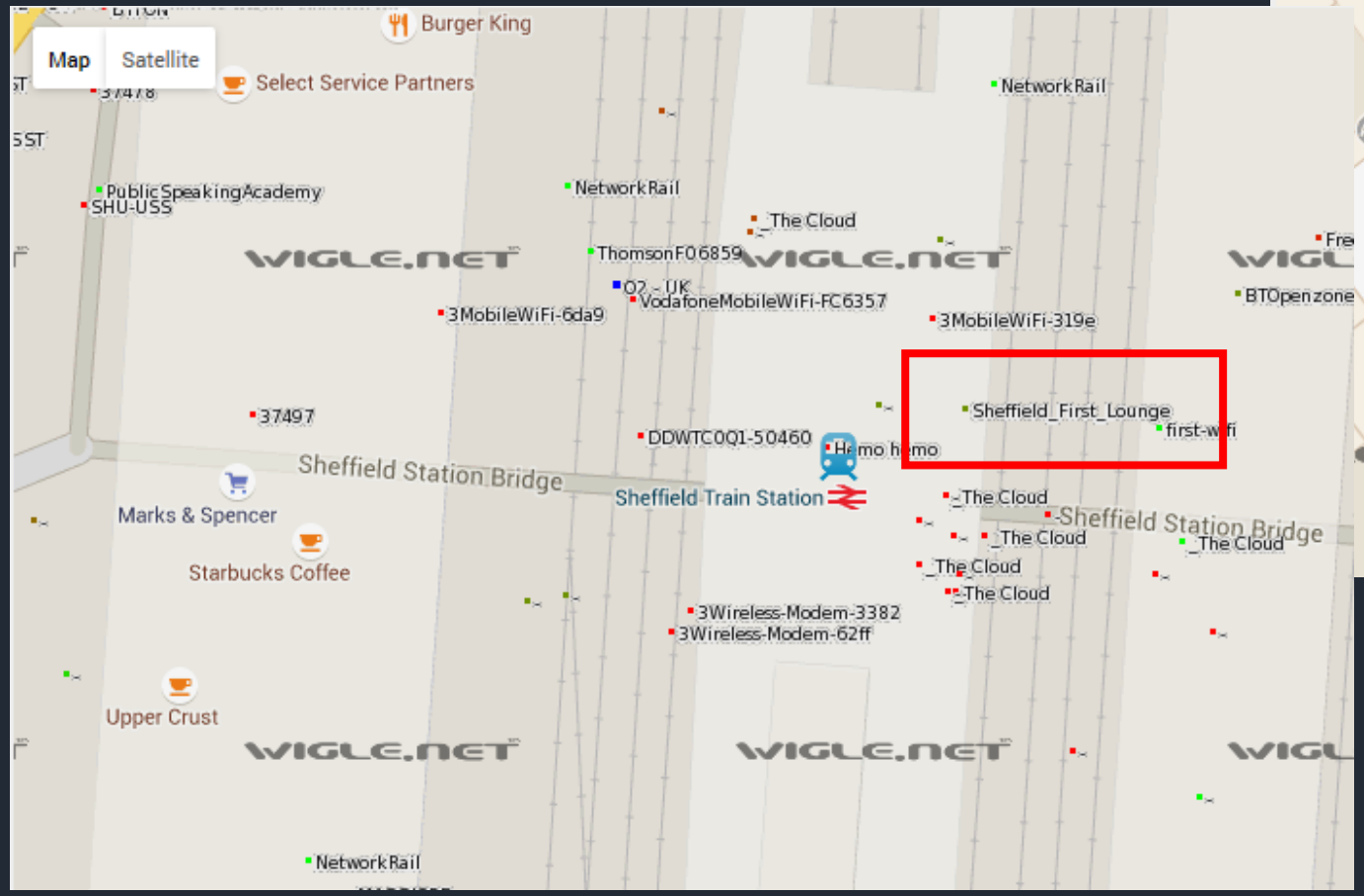
https://digi.ninja

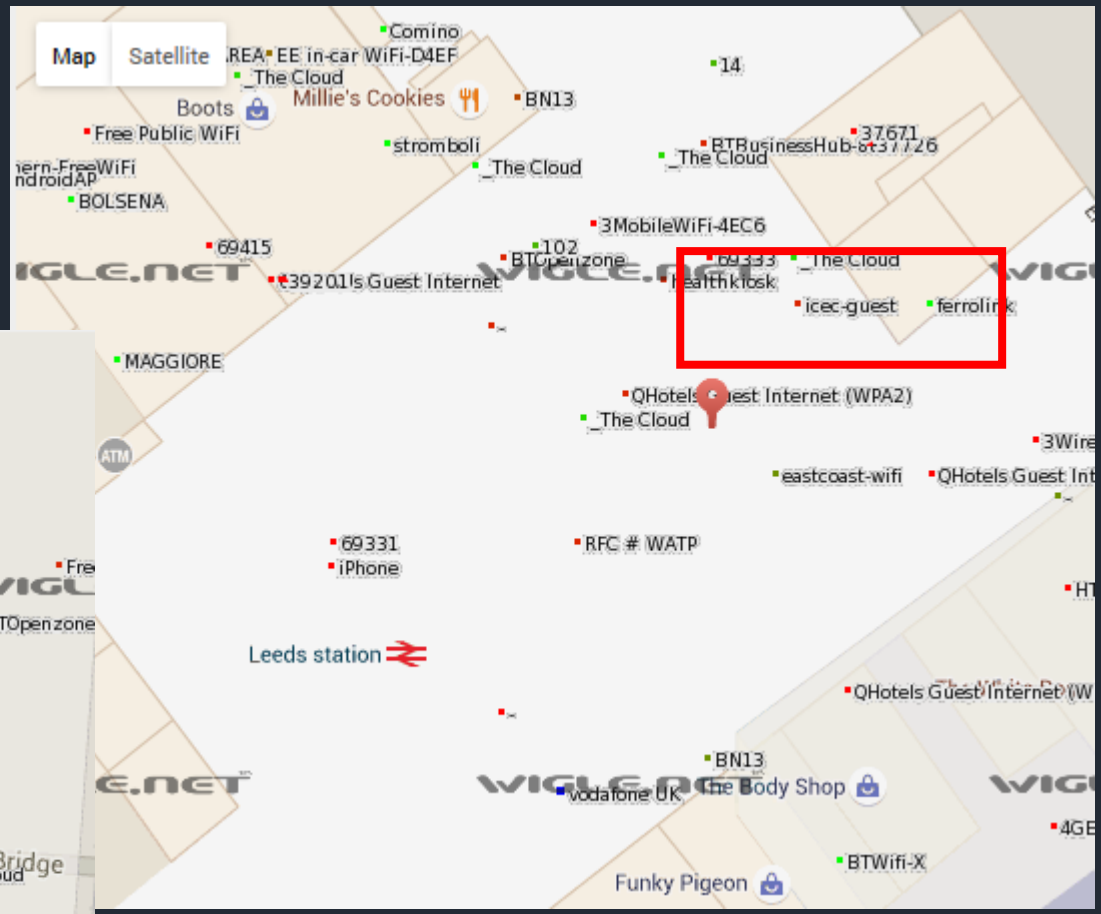
GDK Energy Ltd



https://digi.ninja

Sheffield_First_Lounge icec-guest



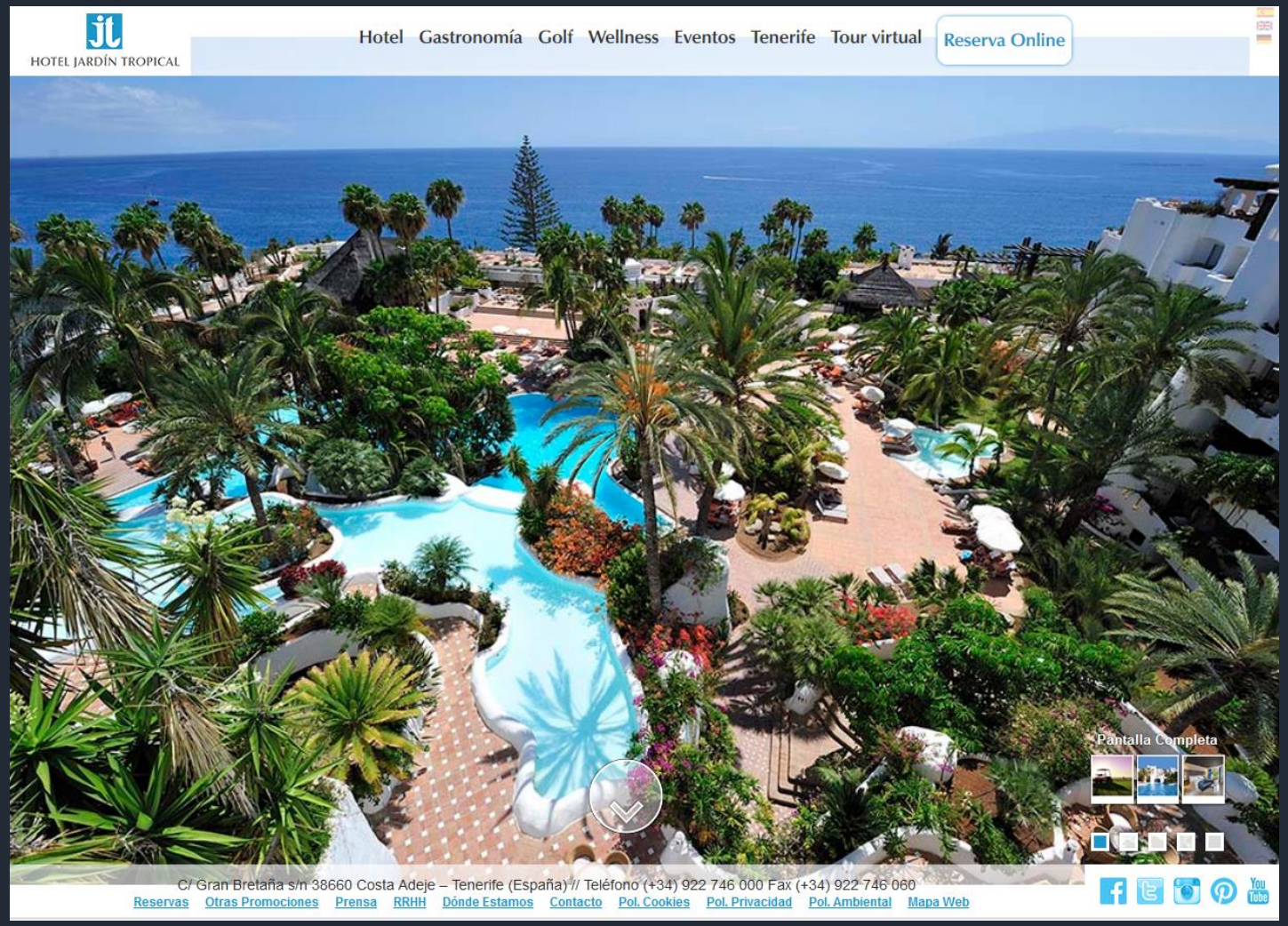


https://digi.ninja

jardinTropicalFREE and UNION JACKS

https://digi.ninja

Hotel Jardin Tropical



https://digi.ninja

Let's Review

- House – Chesterfield Road, Woodseats, Sheffield
- Local – Woodseats Palace
- Interests – Gambling
- Work – GDK Energy Ltd, Leeds
- Travels to work by train
- Holidays in Tenerife

Enough to start a conversation?

What are you leaking?

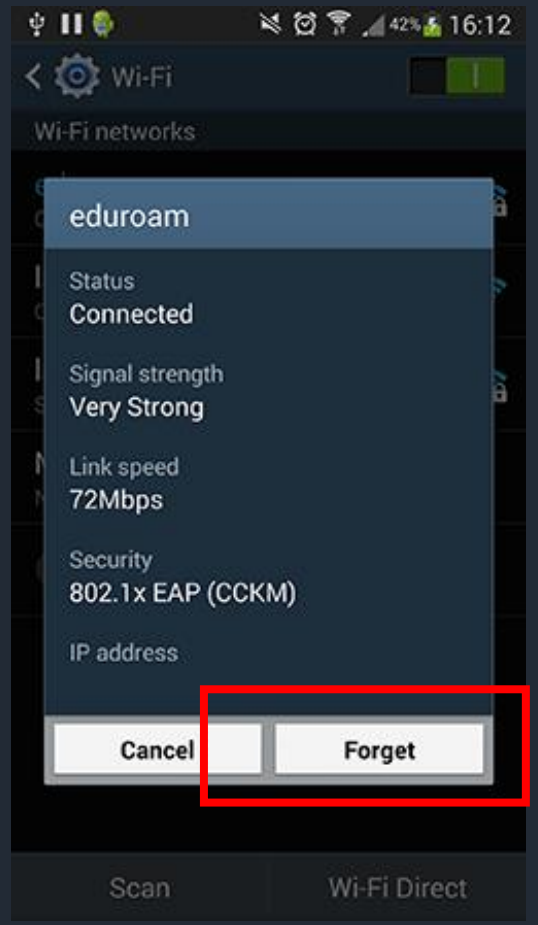
Recently finished active duty?

Is your phone probing for Wi-Fi for local networks where you were stationed?

Protections

- Turn off Wi-Fi when not using it
- Remove networks you don’t connect to regularly
- Consider using common network names for obfuscation

Android Remove Network



https://digi.ninja

iPhone Remove Network

https://digi.ninja

Questions?

Contact

- robin@digi.ninja
- @digininja
- https://digi.ninja