

DigiNinja

Something about Security



# Wi-Fi Leakage

Robin Wood

<https://digi.ninja>



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

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



# 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?

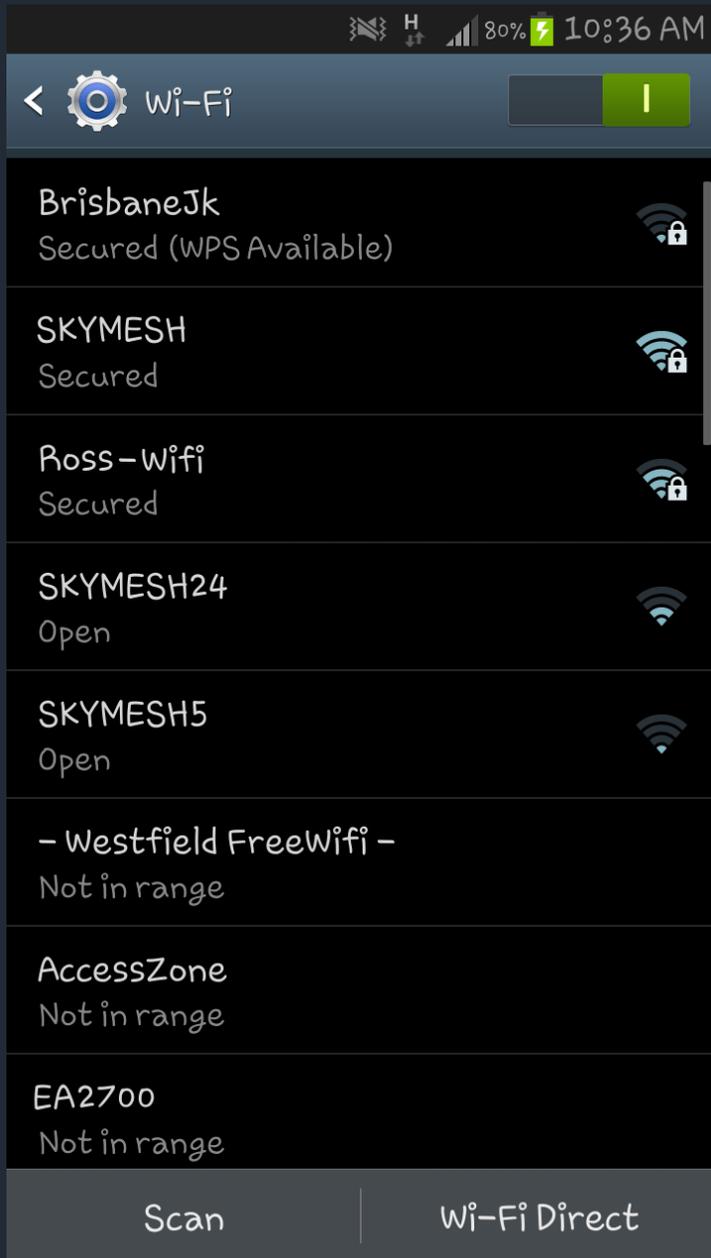


Do you turn it off when you are not using it?



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







Home?



Office?



Yes Office is here



Gym?



Linksys?



# 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

View Uploads Info Stats Tools

logged in as diginja9 [Log out](#)

# WIGLE.NET

All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	OBSERVATIONS	CELL TOWERS
178,878	240,621,504	3,370,390,935	6,156,265

Google Play

### On \_nomap and \_optout

Sun Feb 21 13:41:36 2016

For a false sense of security Google and Microsoft allow you to opt out of including your network in their geolocation systems. WIGLE automatically hides networks (currently 16,644) with these \_nomap and/or \_optout tags in the ssid. Note that unless you turn off your beacon your network is still blasting the presence of your network to anyone within radio distance. And even with beacons off your network can be noticed just via traffic flowing on it. As always, obscurity isn't security, encrypt all the things.

<https://support.google.com/nexus/answer/1725632>

[read more...](#)

-bobzilla

### Let's Encrypt

Sun Jan 31 15:42:57 2016

We've given a [Let's Encrypt](#) a spin, so our SSL certificate is now from there. Fairly painless to set up, give it a shot, encrypt all the things!

-bobzilla

### Wigle Wifi Wardriving 2.9 Released

Mon Nov 23 18:49:10 2015

Map Satellite

Latitude: 37.6964 to 37.8348  
Longitude: -122.5854 to -122.26

SSID: foobar.net  
BSSID: 0A:2C:EF:3D:25:1B  
Date Range: 2001 - 2017

- Possible FreeNet
- Possible Commercial Net
- No Labels
- Wifi Net
- GSM Cellular Net
- CDMA Cellular Net
- Only Discovered By Me
- Only Discovered By Others

Filter

Notes: Zoom in to see individual SSIDs.  
wide view: yellow: more nets, purple fewer  
near view: WiFi: green high QoS, red low  
cell tower: blue  
QoS: Quality of Signal is a metric based on number of observations and observers

Search Address

Map data ©2016 Google Terms of Use Report a map error

### Statistics Over Time

WiFi Networks Over Time



# Wigle.net Sheffield

View Uploads Info Stats Tools

logged in as diginja9 [Log out](#)

# WIGLE.NET

All the networks. Found by Everyone.

STUMBLERS	WIFI NETWORKS	OBSERVATIONS	CELL TOWERS
178,878	240,621,504	3,370,390,935	6,156,265

On \_nomap and \_optout  
Sun Feb 21 13:41:36 2016

For a false sense of security Google and Microsoft allow you to opt out of including your network in their geolocation systems. WIGLE automatically hides networks (currently 16,644) with these \_nomap and/or \_optout tags in the ssid. Note that unless you turn off your beacon your network is still blasting the presence of your network to anyone within radio distance. And even with beacons off your network can be noticed just via traffic flowing on it. As always, obscurity isn't security, encrypt all the things.

<https://support.google.com/nexus/answer/1725632>

read more...

-bobzilla

Let's Encrypt  
Sun Jan 31 15:42:57 2016

We've given a [Let's Encrypt](#) a spin, so our SSL certificate is now from there. Fairly painless to set up, give it a shot, encrypt all the things!

-bobzilla

Wigle Wifi Wardriving 2.9 Released  
Mon Nov 23 18:49:10 2015

Map Satellite

Latitude: 53.3317 to 53.4361  
Longitude: -1.5834 to -1.2617

SSID: foobarnet  
BSSID: 0A:2C:EF:3D:25:1B  
Date Range: 2001 - 2017

- Possible FreeNet
- Possible Commercial Net
- No Labels
- Wifi Net
- GSM Cellular Net
- CDMA Cellular Net
- Only Discovered By Me
- Only Discovered By Others

Filter

Notes: Zoom in to see individual SSIDs.  
wide view: yellow: more nets, purple fewer  
near view: WiFi: green high QoS, red low  
cell tower: blue  
QoS: Quality of Signal is a metric based on number of observations and observers

Statistics Over Time

WiFi Networks Over Time

<https://digi.ninja>



# 0449woodseat

### Query for networks

Latitude:  to:  Longitude:  to:

Search Radius Tolerance(+/- degrees):  ▾

BSSID/MAC:

SSID / Network Name (exact match):

SSID / Network Name (wildcards<sup>1</sup>: % and \_):

Last Observed:

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:  State:  Zip:

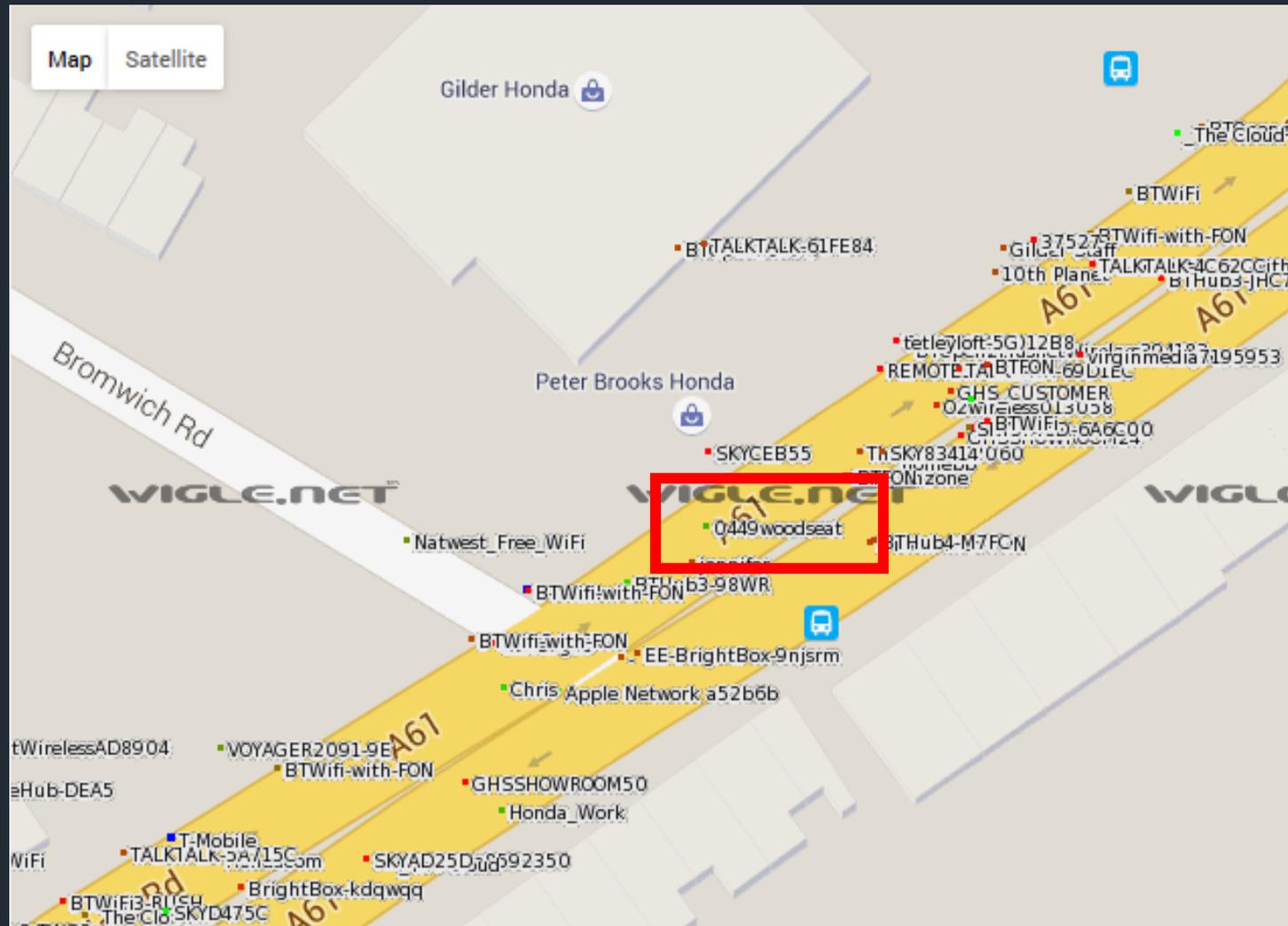
<sup>1</sup> SSID cannot start with a wildcard. '%' means zero-or-more characters, '\_' means a single character.

<< | showing records 1 | to 1 | >>

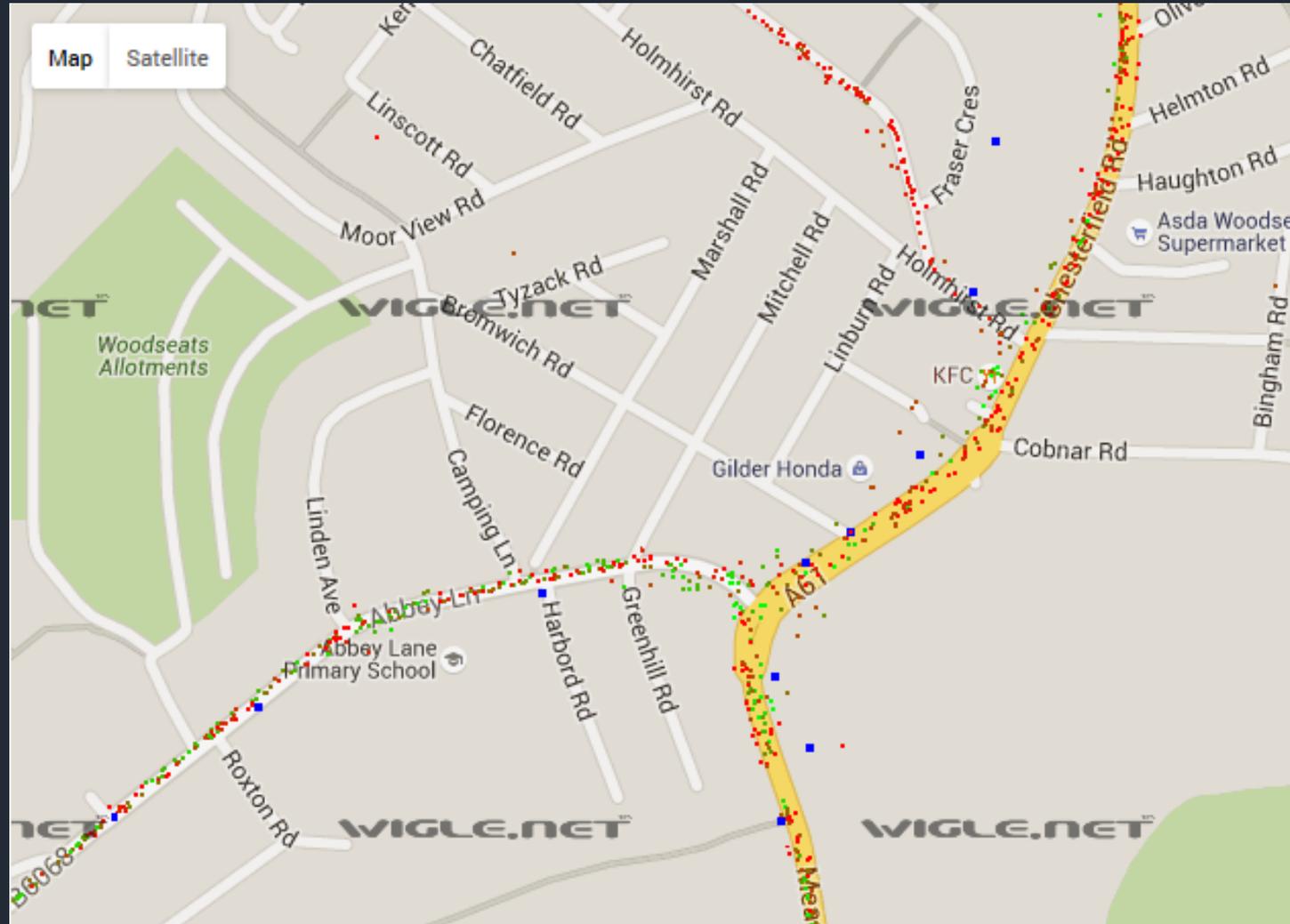
Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS
<a href="#">map</a>	<a href="#">00:15:70:C8:E5:40</a>	0449woodseat		infra	2011-09-12 20:29:57	2016-02-04 09:40:04		53.33947754	-1.48069918	13		5



# 0449woodseat



# 0449woodseat



# 0449woodseat



<https://digi.ninja>



# The\_Woodseats\_Palace

Robin 🔍 🔔

[All](#) [Maps](#) [Images](#) [Shopping](#) [News](#) [More](#) [Search tools](#)

About 17,800 results (0.58 seconds)

**The Woodseats Palace - J D Wetherspoon**  
<https://www.jdwetherspoon.com/pubs/.../the-woodseats-palace-sheffield>  
Woodseats Palace was the name of the cinema built on this site in 1911.  
Reconstructed as a supermarket, 50 years later, it is now a Wetherspoon pub bearing ...

**Woodseats Palace, Sheffield - Restaurant Reviews, Phone ...**  
[www.tripadvisor.co.uk](http://www.tripadvisor.co.uk) > ... > Sheffield > Sheffield Restaurants  
★ ★ ★ ★ ☆ Rating: 3.5 - 25 reviews  
Woodseats Palace, Sheffield: See 25 unbiased reviews of Woodseats Palace, rated 3.5 of 5 on TripAdvisor and ranked #533 of 1267 restaurants in Sheffield.

**Woodseats Palace (Wetherspoon) - Pub in Sheffield**  
<https://foursquare.com/v/woodseats-palace.../4bb90cb97421a593db6dc2...>  
See 31 photos and 7 tips from 108 visitors to Woodseats Palace (Wetherspoon). "There's always some ugly people in here but given enough drink, some of..."

**Sheffield - Woodseats, I have lived here for 18 months (by ...**  
[www.ilivehere.co.uk/sheffield-woodseats.html](http://www.ilivehere.co.uk/sheffield-woodseats.html)  
My first week here, I ventured out after 8pm & a couple staggered towards the 'Palace' & fell over on the pavement right in front of me.



Map data ©2016 Google

## The Woodseats Palace ★

[Website](#) [Directions](#)

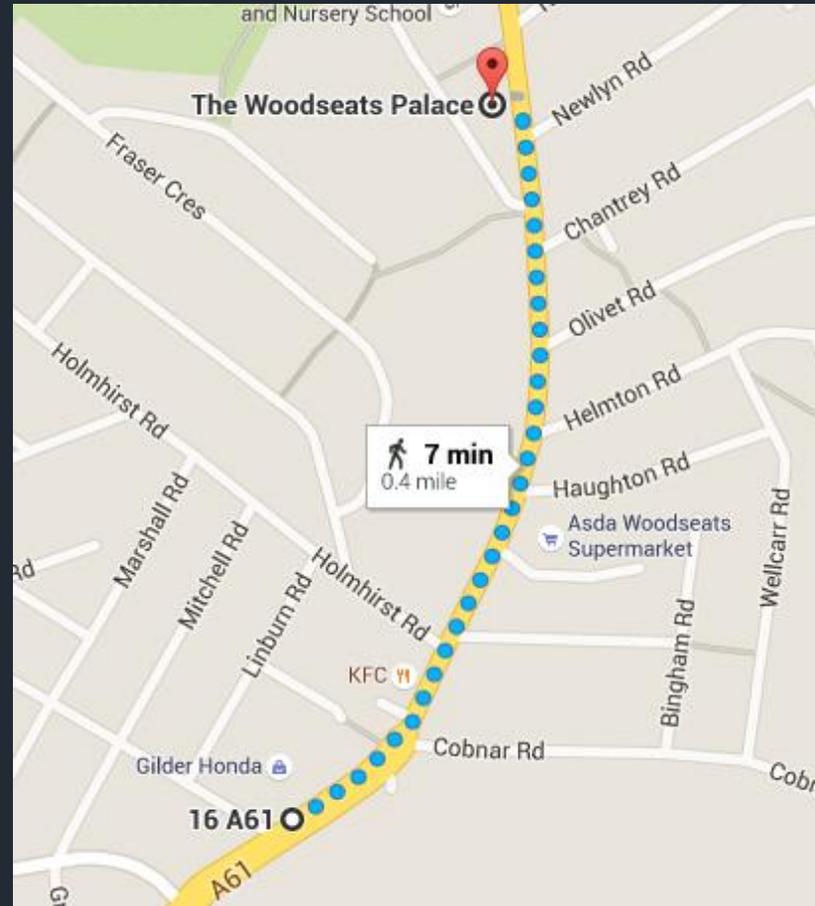
4.0 ★ ★ ★ ★ ☆ 6 Google reviews  
£ · Restaurant

Carpeted pub in former cinema, with bucket seats, sofas and dado wood panelling, for eclectic menu.

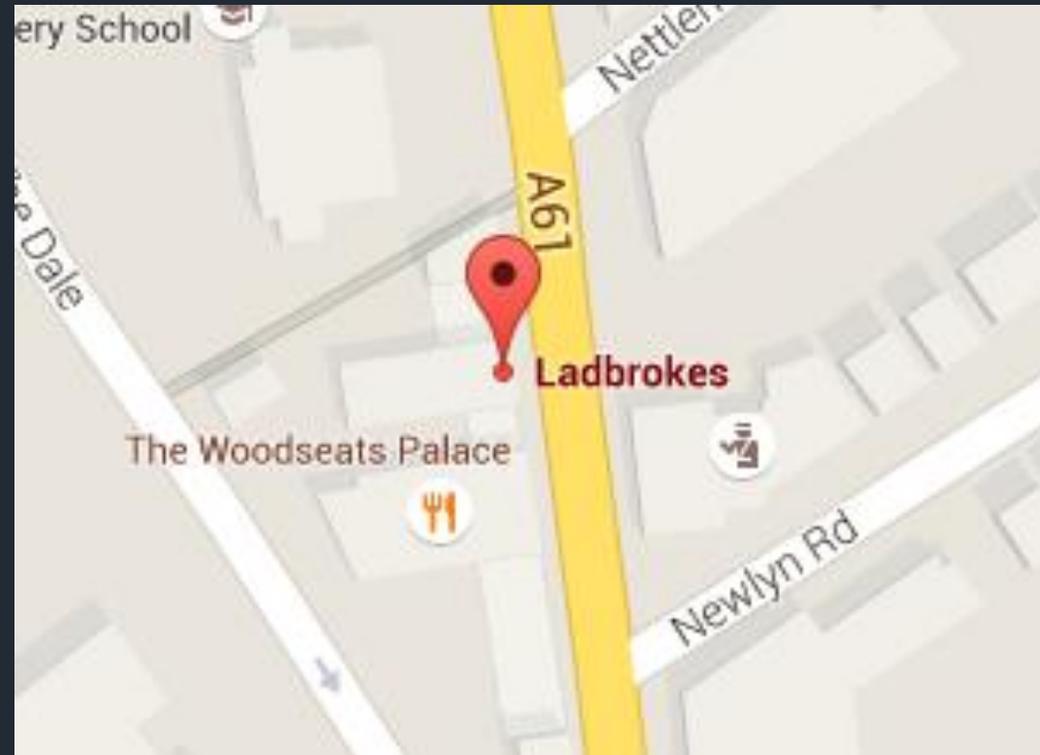
**Address:** 692 Chesterfield Rd, Sheffield S8 0SD  
**Phone:** 0114 262 9210



# 0449woodseat to The\_Woodseats\_Palace



# Ladbrokes



# GDKENERGY

## Query for networks

Latitude:  to:  Longitude:  to:

Search Radius Tolerance(+/- degrees):  ▾

BSSID/MAC:

SSID / Network Name (exact match):

SSID / Network Name (wildcards<sup>1</sup>: % and \_):

Last Observed:

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:  State:  Zip:

<sup>1</sup> SSID cannot start with a wildcard. '%' means zero-or-more characters, '\_' means a single character.

<< | showing records  to  | >>

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



# GDKENERGY





# GDK Energy Ltd



## New Website Under Construction

Our new website is under construction and will be available very soon, if you have a query in the meantime please use the contact details below.

### Contact GDK Energy Ltd

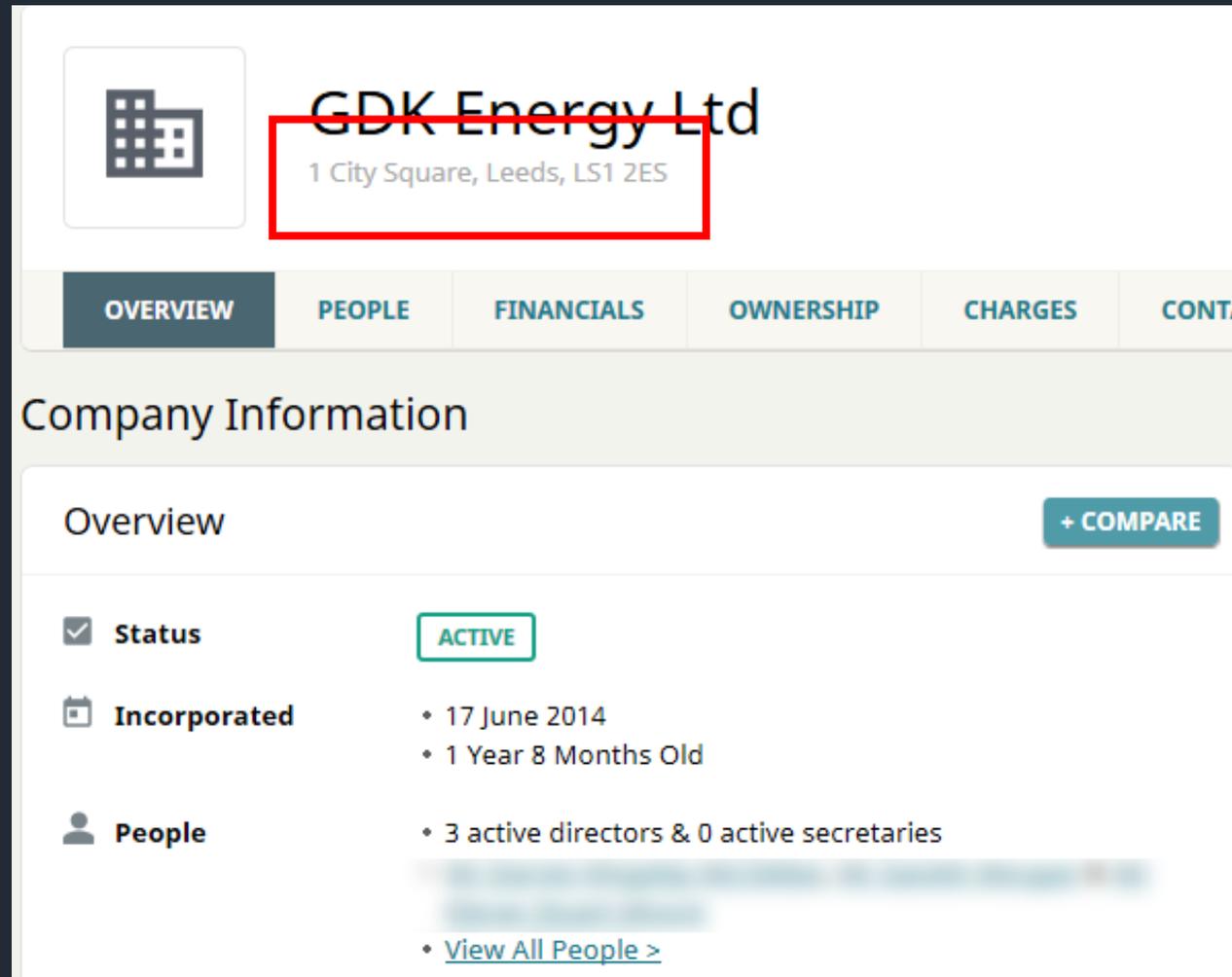
Tel: 08445 436492

Email: [info@gdkenergy.co.uk](mailto:info@gdkenergy.co.uk)

<https://digi.ninja>



# GDK Energy Ltd



 **GDK Energy Ltd**  
1 City Square, Leeds, LS1 2ES

**OVERVIEW** PEOPLE FINANCIALS OWNERSHIP CHARGES CONTACT

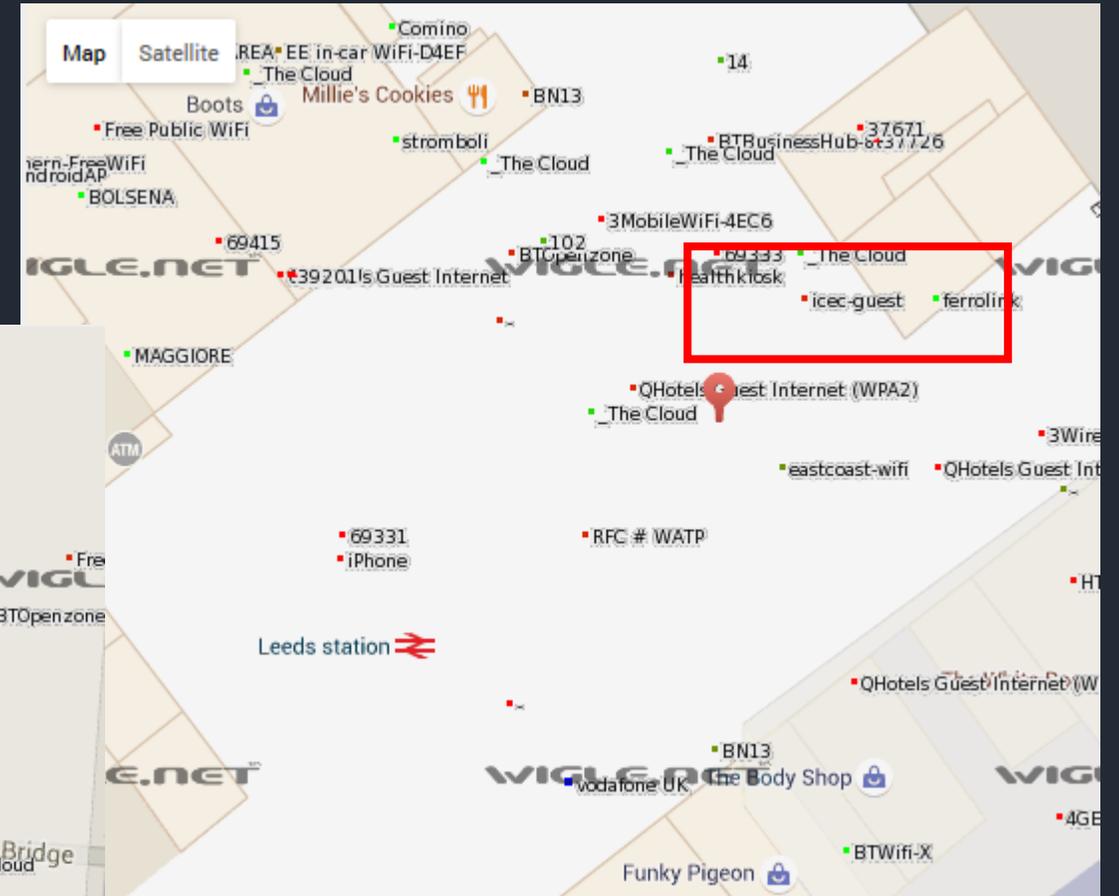
### Company Information

Overview [+ COMPARE](#)

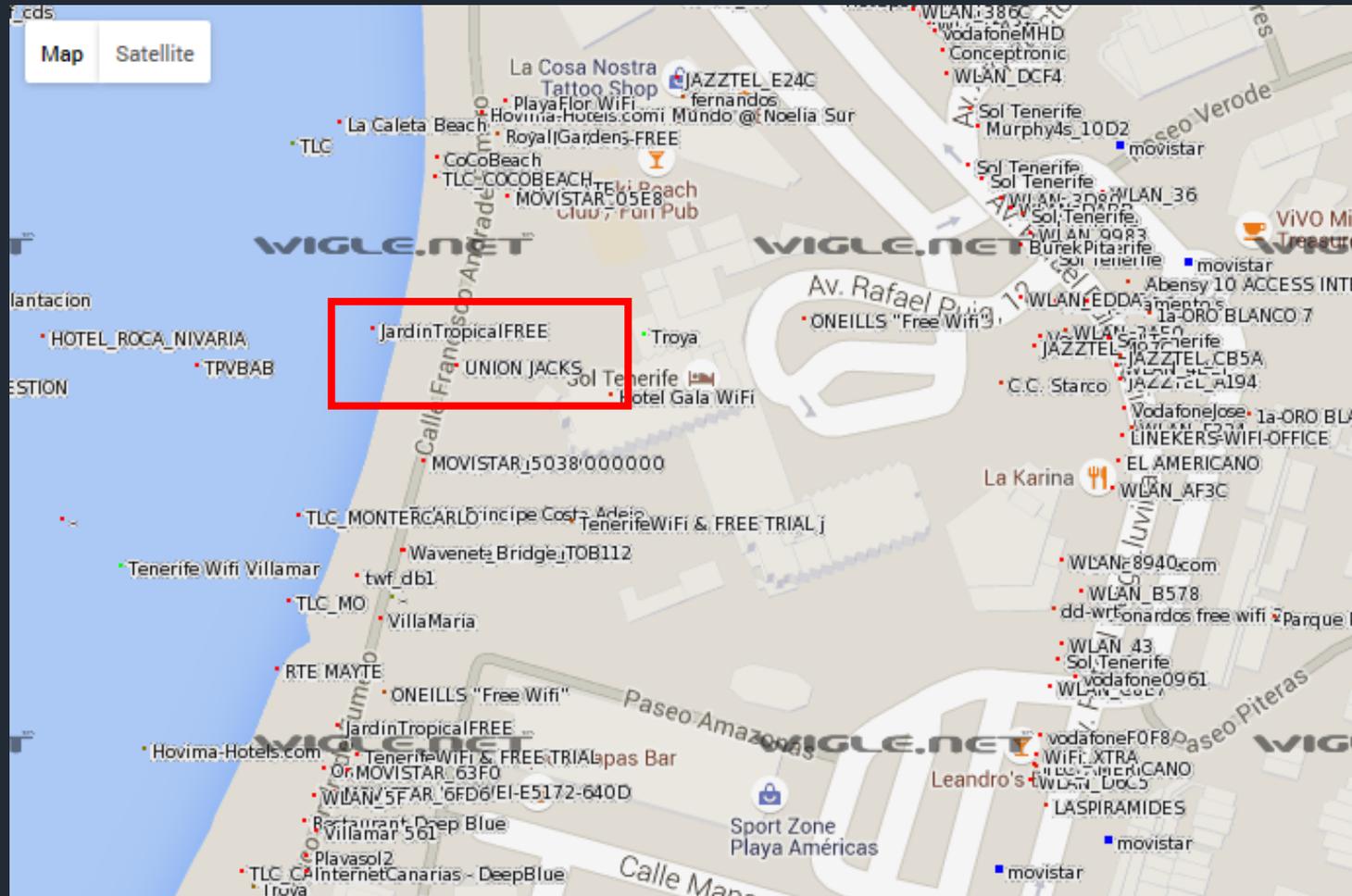
- Status** **ACTIVE**
-  **Incorporated**
  - 17 June 2014
  - 1 Year 8 Months Old
-  **People**
  - 3 active directors & 0 active secretaries
  - [View All People >](#)



# Sheffield\_First\_Lounge icec-guest



# jardinTropicalFREE and UNION JACKS



# Hotel Jardín Tropical

The screenshot displays the website for Hotel Jardín Tropical. At the top left is the logo, a blue square with the letters 'jt' in white, and the text 'HOTEL JARDÍN TROPICAL' below it. To the right of the logo is a navigation menu with the following items: 'Hotel', 'Gastronomía', 'Golf', 'Wellness', 'Eventos', 'Tenerife', 'Tour virtual', and a 'Reserva Online' button. The main content area is a large, vibrant aerial photograph of the resort, featuring a large, winding swimming pool, numerous palm trees, and a view of the ocean. In the bottom right corner of the image, there is a 'Pantalla Completa' (Full Screen) button and a row of social media icons for Facebook, Twitter, Instagram, Pinterest, and YouTube. At the very bottom of the page, there is a footer with the address 'C/ Gran Bretaña s/n 38660 Costa Adeje – Tenerife (España) // Teléfono (+34) 922 746 000 Fax (+34) 922 746 060' and a row of links: 'Reservas', 'Otras Promociones', 'Prensa', 'RRHH', 'Dónde Estamos', 'Contacto', 'Pol. Cookies', 'Pol. Privacidad', 'Pol. Ambiental', and 'Mapa Web'.

<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?

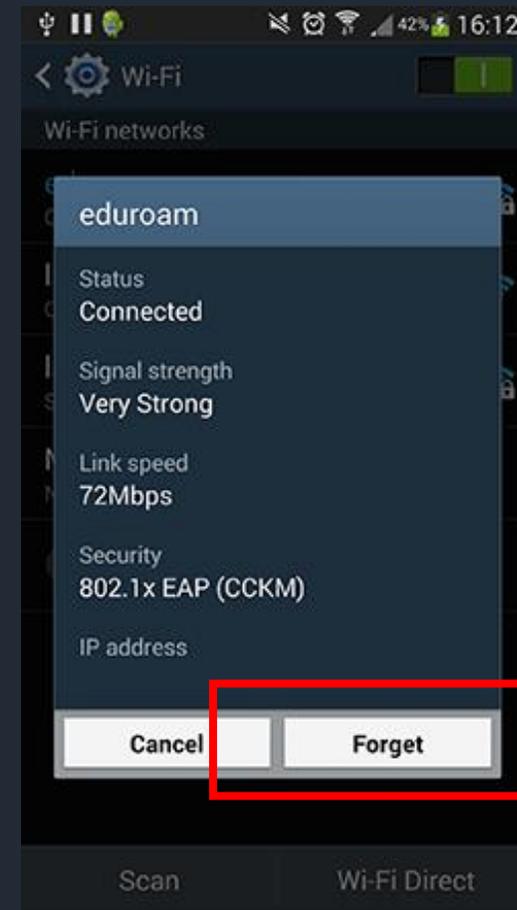


# Protections

- 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



# iPhone Remove Network



# Questions?

## Contact

- [robin@digi.ninja](mailto:robin@digi.ninja)
- [@digininja](#)
- <https://digi.ninja>

