Wi-Fi Leakage

Robin Wood
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.
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
Aircrack-ng Suite
<table>
<thead>
<tr>
<th>Station MAC</th>
<th>First time seen</th>
<th>Last time seen</th>
<th>Power</th>
<th># packets</th>
<th>BSSID</th>
<th>Probed ESSIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:26:37:93:D8:E1</td>
<td>2016-03-02 15:12:37</td>
<td>2016-03-02 15:12:44</td>
<td>-44</td>
<td>71</td>
<td>64:70:02:DE:AF:A7, UNION</td>
<td>JACKS, jardinTropicalFREE, 0449woodseat, GDKENERGY, Natwest_Free_WiFi,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sheffield_First_Lounge, eastcoast-wifi, simonsandrawireless, icec-guest</td>
</tr>
</tbody>
</table>
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

Wigle.net is a network discovery platform that allows anyone to find and map Wi-Fi networks. It is a database of Wi-Fi networks that has been created by users over time. The platform is open-source and anyone can contribute to it by adding Wi-Fi networks they discover.

The platform provides a variety of features, including:

- A map interface that allows users to view Wi-Fi networks in their area.
- A database of Wi-Fi networks that can be searched by location or name.
- Tools for wardriving, which is the process of finding and mapping Wi-Fi networks.
- A community of users who share their discoveries and contribute to the database.

Wigle.net is a valuable resource for anyone interested in Wi-Fi networks, from casual users to professionals in the field of computer networking.
Wigle.net
Sheffield
### Query for networks

**Latitude:** 47.26254 to 47.26256  
**Longitude:** -87.256243 to -87.256244

**Search Radius Tolerance (+/- degrees):** 0.010

**BSSID/MAC:** 0A:2C:EF:3D:26:1B or 1st 3 Octets: 0A:2C:EF

**SSID / Network Name (exact match):** 0449woodseat

**SSID / Network Name (wildcards**: % and _): foo%bar%

**Last Observed:** 2001-09-25 17:46:56

- [ ] 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

### Showing records

<table>
<thead>
<tr>
<th>Map</th>
<th>Net ID</th>
<th>SSID</th>
<th>Name</th>
<th>Type</th>
<th>First Seen</th>
<th>Most Recently</th>
<th>Crypto</th>
<th>Est. Lat</th>
<th>Est. Long</th>
<th>Channel</th>
<th>Bcn Int</th>
<th>QoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>map</td>
<td>00:15:70:C8:E6:40</td>
<td>0449woodseat</td>
<td>infra</td>
<td></td>
<td>2011-09-12</td>
<td>2016-02-04</td>
<td>65</td>
<td>53.3397754</td>
<td>-1.48069918</td>
<td>13</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

1. SSID cannot start with a wildcard. % means zero-or-more characters, _ means a single character.
0449woodseat

https://digi.ninja
The Woodseats Palace

Woodseats Palace, Sheffield - Restaurant Reviews, Phone ... www.tripadvisor.co.uk ... Sheffield > Sheffield Restaurants

Woodseats Palace, Sheffield: See 25 unbiased reviews of Woodseats Palace, rated 3.5 of 5 on TripAdvisor and ranked #633 of 1267 restaurants in Sheffield.

Woodseats Palace (Wetherspoon) - Pub in Sheffield
https://foursquare.com/v/woodseats-palace-6dab9b0cb97421a593db3b6dc2

Sheffield - Woodseats, I have lived here for 18 months (by ... www.livhere.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.

https://digi.ninja
0449 Woodseats to The_Woodseats_Palace
Ladbrokes
GDKENERGY

https://digi.ninja
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: 08446 436492
Email: info@gdkenergy.co.uk

https://digi.ninja
GDK Energy Ltd

1 City Square, Leeds, LS1 2ES

Overview

Status: ACTIVE

Incorporated:
- 17 June 2014
- 1 Year 8 Months Old

People:
- 3 active directors & 0 active secretaries

https://digi.ninja
Sheffield_First_Lounge
icec-guest
jardinTropicalFREE and UNION JACKS
Hotel Jardin Tropical
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

- Select the network you want to remove (e.g., SKYMESH).
- Tap the "Forget" button to remove the network.
iPhone Remove Network

1. Go to Settings.
2. Tap on Wi-Fi.
3. Select the network you want to forget.
4. Tap the lock icon to unlock the Wi-Fi settings.
5. Tap the network you want to forget to select it.
6. Tap the red 'Forget this Network' button.
Questions?

Contact
• robin@digi.ninja
• @digininja
• https://digi.ninja