

We are OSINTCurio.us

WIGLE.NETTM

All the networks. Found by Everyone.

STUMBLERS

225,481

WIFI NETWORKS

511,584,727

OBSERVATIONS

7,315,730,862

Half a Billion WiFi Networks Geolocated

Wed, 26 Dec 2018 03:51:31 GMT

That... is one big pile of WiFi. 500,000,000 Networks! Congrats to user 'WKSUK' for putting the counter over this huge milestone! Can we hit....one billion networks?

-bobzilla

RF Fingerprinting

Tue, 18 Sep 2018 17:51:00 GMT

Check out @acyberexpert's presentation from BSides Perth - <https://obvi.us/presentation/rf-sig/> . In addition to mentioning WIGLE (!), it's jam packed with exactly the kind of information and security/privacy concerns about wireless WIGLE exists to highlight!

-arkasha

Google Pie and Wifi Wardriving

Tue, 07 Aug 2018 21:38:49 GMT

Google has throttled scan initiation in Android P - 4 scans/2 minute maximum. Feel free to "star" the issue to help raise awareness within Google. Bug: <https://issuetracker.google.com/issues/79906367> Feature Request: <https://issuetracker.google.com/issues/112688545>

[read more...](#)

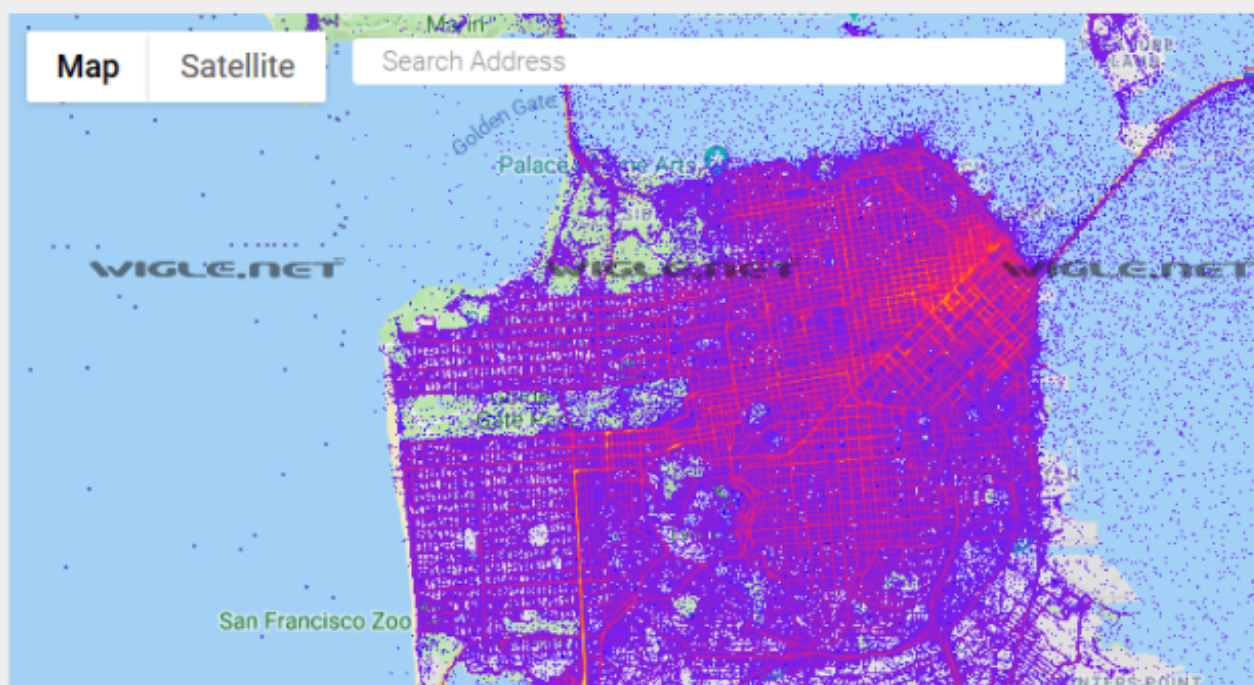
-arkasha

Call for input

Mon, 09 Jul 2018 17:17:07 GMT

Want to help support WiGLE?

You can allow WIGLE to use your data for commercial purposes. We never do this without your permission, and



Tracking All the WiFi Things

Do you use a WiFi tether to get your laptop and other devices on the internet when there is no WiFi access point around. I'm betting many of you do. You turn on that *Personal Hotspot* setting on your phone and magically you have a WiFi access point for your equipment.

Would you be surprised if I told that, if you use a MiFi or WiFi tether, people are tracking your location? They are and have been since the year 2000. But before we jump to our evidence, let's learn a bit about wireless networking, Wardriving, SSID's, MAC addresses and hotspots.

Wireless Primer

Before we dive into the details, let's first go over some basic terminology in regards to WiFi. Even though everybody uses it, there is more to explain than it being just a wireless network. First of all we have the network name, or SSID (Service Set identifier), that you connect to. Even

though this name doesn't have to be unique, it can sometimes reveal information about the people or company it belongs to.

Then we have the BSSID (Basic Service Set identifier) that is the MAC address of the access point. A MAC address (Media Access Control address) is a unique identifier that is used by a network device to identify itself on the underlying network. Like the SSID is used to identify itself to an end-user, the MAC address or BSSID is used by the hardware for things like routing in the rest of the network. And even though someone who connects to a WiFi hotspot doesn't usually see that address, it is of utmost importance for your connection.

When we start a hotspot on our phone for other devices to use the same internet connection, we call that "tethering". When you fire up your WiFi connection on your phone while being out, you will probably see examples popup like "*John's iPhone*" or the default "*AndroidAP*".

War Xing

Around 2000 an engineer by the name of **Peter Shipley** decided to map out insecure WiFi endpoints. By mounting a WiFi antenna on his car and

by using a GPS receiver he was able to map out the wireless networking signals in areas fast and accurately. He coined the term **Wardriving** to describe this practice. Some other less known variants of mapping the geolocation of wireless networks are “*Warcycling*” (using a bicycle), “*Warwalking*” (on foot) or “*Wardroning*” (by using a drone).

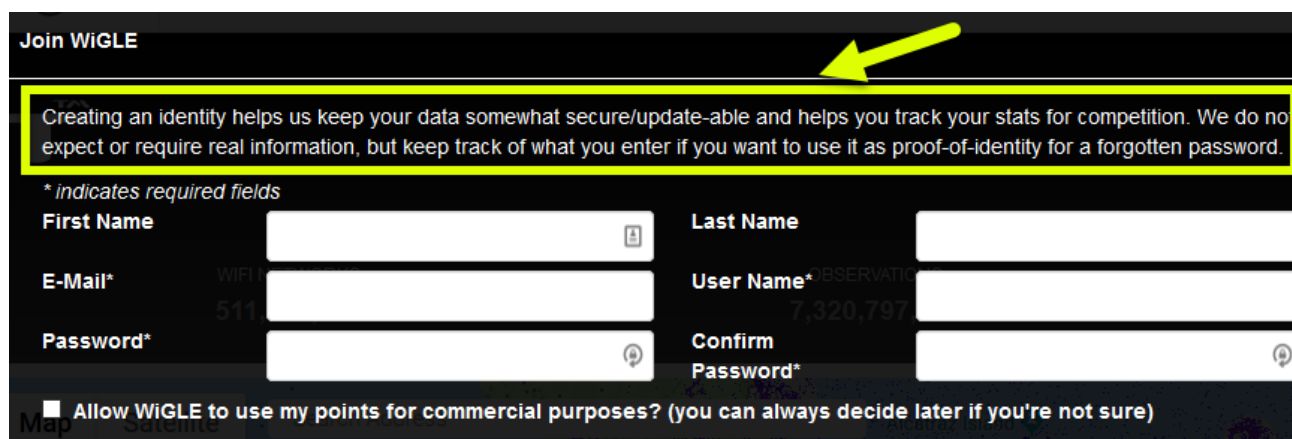
Wigle.net

Since the early 2000s, **Wigle.net** has been an amazing resource to the community. It is the one-stop-shop for user-reported wireless network data. We know that others, such as Google (<https://arstechnica.com/tech-policy/2010/05/google-says-wifi-data-collection-was-a-mistake/>), have collected wireless network data to use in their private services (such as Google’s WiFi Location Services). Wigle.net gives us access to similar data from computer systems around the world.

Wigle.net’s data is uploaded to the site by people that collect this information on their phones, tablets, and laptops using WiFi-sniffing tools or **Wigle’s own Android app**. Once uploaded, users like ourselves can search and map the content and use it in our investigations

Create a Free Account

While you “can” access Wigle.net via an anonymous account, the searching features that you likely will want to use, require you to be authenticated. Their accounts are free and they note that you do not need to provide them a REAL email address, just something unique (see image below).

The image shows the 'Join WIGLE' registration page. At the top, a yellow box highlights a disclaimer: 'Creating an identity helps us keep your data somewhat secure/update-able and helps you track your stats for competition. We do not expect or require real information, but keep track of what you enter if you want to use it as proof-of-identity for a forgotten password.' Below this, a note states '* indicates required fields'. The form contains several input fields: 'First Name', 'Last Name', 'E-Mail*', 'User Name*', 'Password*', and 'Confirm Password*'. At the bottom, there is a checkbox labeled 'Allow WIGLE to use my points for commercial purposes? (you can always decide later if you're not sure)'. A yellow arrow points to the top right corner of the registration form area.

Wigle.net's Registration Page

The Time-Traveling BSSID

For our first OSINT example, let's head over to London, Great Britain.
The De Vere Grand Connaught Rooms (**61-65 Great Queen Street**

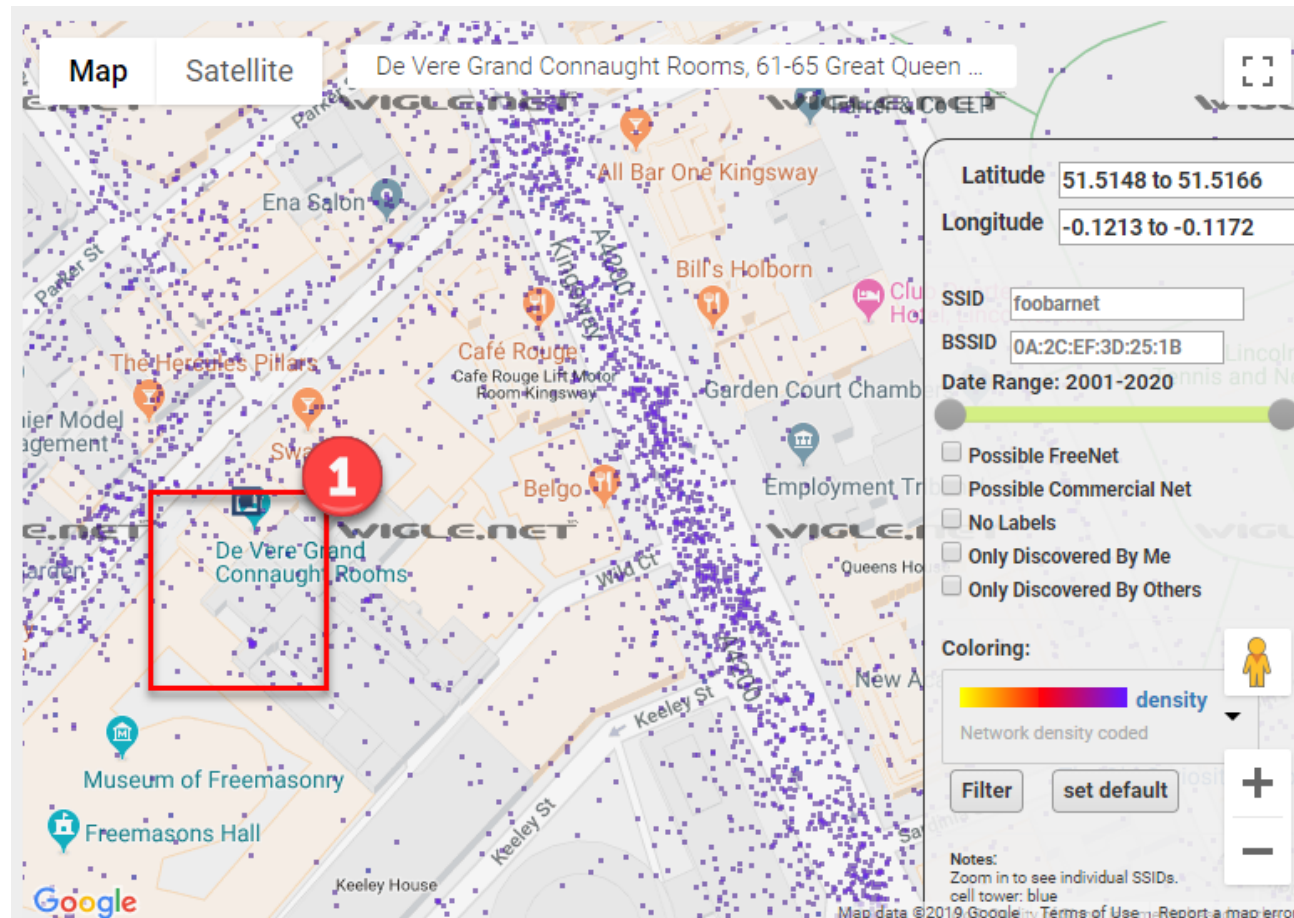
London, WC2B 5DA GB) conference center is where the **SANS Institute has many of their London events**. Know how we know this? The WiFi networks tell us!

Below is a normal Google Map of the area.



De Vere Grand Connaught Rooms from Google Maps 2019

Looking at this same region in the Wigle.net site by searching for that address yields the image below.

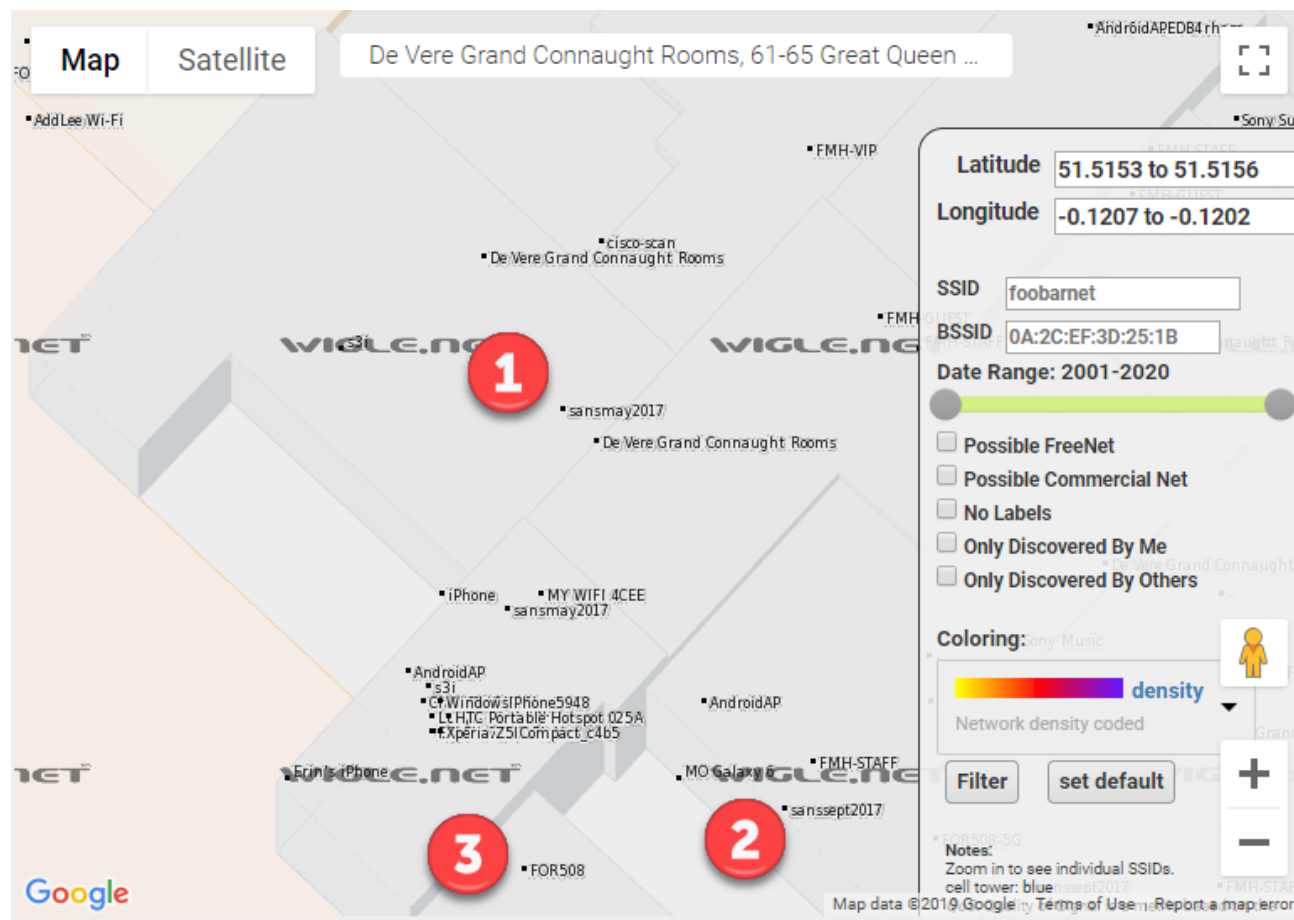


De Vere Grand Connaught Rooms from Wigle.net 2019

Wow! That is one BUSY-looking image. Each of those purple dots represents a wireless network that someone's device "found" and then

was uploaded to the Wigle.net site. It is common for densely-populated regions to look like this, with hundreds or thousands of WiFi networks noted within a very small region. This, of course, makes actually using this data more-challenging.

To read the information attached to each purple dot we need to zoom in. In the above image, we will zoom into the rectangle marked with a “1” on the left.



Detailed Map View of Wigle.net 2019

In the above map, we zoomed in a huge amount and still the font size of the Wigle.net wireless networks are tiny. We can see some interesting wireless network names at this level. Let's examine those three points in the above image with the 1, 2, and 3 near them.

- 1 – **sansmay2017** – General wireless network for the SANS training event in May 2017 at this location.
- 2 – **sanssept2017** – General wireless network for the SANS training event in September 2017 at this location.
- 3 – **FOR508** – Wireless network for the FOR508 SANS class when it was run at some point from this location.

From an OSINT perspective, numbers 1 and 2 above might be interesting. We have 2 wireless networks that state that they are for events across time. Here we learn both what the wireless network naming scheme is and when certain events might have been.

In OSINT, collecting data is important. Analysis of that data is essential. Let's perform a search on the "sansmay2017" networks and see when they were discovered by the Wigle.net user that uploaded them. The <https://wagle.net/search?ssid=sansmay2017> page performs the search we want and the output from that, is shown below.

Minimum data quality⁰: 0 Encryption status: ▼

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







SSID / Network Name (exact match): sansmay2017

SSID / Network Name (wildcards¹: % and _):

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

⁰ 0-7 Product of number of observers and observations.
¹ '%' means zero-or-more characters, '_' means a single character.

<< | showing records 1 to 6 of 6 >> 1 2

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel
map	04:4F:AA:72:9C:58	sansmay2017		infra	2014-03-14T14:00:00.000Z	2017-09-07T09:00:00.000Z		51.51570511	-0.12061119	11
map	54:3D:37:38:73:98	sansmay2017		infra	2015-07-14T12:00:00.000Z	2017-05-23T05:00:00.000Z		51.51551437	-0.12096739	1
map	24:C9:A1:16:CD:38	sansmay2017		infra	2014-02-19T17:00:00.000Z	2017-05-23T05:00:00.000Z		51.51546097	-0.12049258	1
map	24:C9:A1:16:CD:3C	sansmay2017		infra	2014-02-19T17:00:00.000Z	2017-05-23T05:00:00.000Z		51.51541138	-0.1205148	100
map	04:4F:AA:72:9E:B8	sansmay2017		infra	2001-01-01T01:00:00.000Z	2017-05-23T05:00:00.000Z		51.51571274	-0.1205722	1
map	54:3D:37:38:73:9C	sansmay2017		infra	2015-07-14T12:00:00.000Z	2017-05-23T05:00:00.000Z		51.51547241	-0.12086184	36

Detailed View from Wigle.net on Network sansmay2017

In the above image, something appears to be wrong. I mean, the access point name clearly states “sansmay2017”, right? But people discovered these WAY before May 2017 (column marked with a 1). Did they time-

travel? Is something suspicious going on here? Nope. It is basic wireless networking.

What happens is that Wigle notes when the transmitter (BSSID/MAC address) for a device was first and last seen. Because the wireless network (SSID) for a device can change, cataloging a device by its BSSID, which should not change, is better since that will be unique and long-lasting.

OK, so what is going on in the image above? Chances are good that these wireless transmitters (think routers or access point devices) were used in the past and were discovered earlier than the May 2017 event. Let's check that out by clicking on the first BSSID 04:4F:AA:72:9C:58.

Observations:

netid	name	ssid	month
		sansmay2017	2017-09
		sansmay2017	2017-05
		sansmay2017	2017-05
		sansmay2017	2017-05
		sansmarch2017	2017-03
		sansmay2017	2017-05
		sansmay2017	2017-05
		sansmay2017	2017-05
		SANSLondon	2015-11
		SANSLondon	2015-11

Detailed Device View of BSSID 04:4F:AA:72:9C:58

YES! We were correct! The image above shows that this transmitter (BSSID) was discovered transmitting other wireless network names before the May 2017 event.

Tracking Your iPhone

So let's think about that last example for a moment. There was a device that transmitted a wireless network that was noted several times in the same location. OK. Many of you carry a wireless network transmitter with you in your purse, pocket, or man-bag: your cell phone or MiFi. These devices have unique BSSIDs and, when you wirelessly tether to them, they emit an SSID that can be recorded in Wigle.

We shall pick on iPhones since they make this example simpler. When get an iPhone, you enter your first name (or a name you pick) into the device at the initial configuration. When you enable the WiFi tethering or mobile hotspot feature, the iPhone creates a wireless network with "YOURNAME's iPhone". If, for example, I put the name "Micah" into my new iPhone when I configured it, when I turn on the WiFi tethering, I'd expect a wireless network name (SSID) of "Micah's iPhone".

Now that we understand how this device works, let's head over to Wigle.net and perform a wildcard SSID search for "'s iphone" and see what comes back.

1

%s iphone

☐ Must Be a FreeNet ☐ Must Be a Commercial Pay Net ☐ Only Networks I

Query Reset

⁰ 0-7 Product of number of observers and observations.
¹ '%' means zero-or-more characters, '_' means a single character.

2

<< | showing records 1 to 100 of 363343 | >>

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long
map	00:1D:6A:E4:E3:3A	Heber's iphone			2001-01-01T00:00:00.000Z	2008-10-30T19:00:00.000Z		34.09346771	-118.33631134
map	00:1D:73:B2:98:2B	69's iPhone		infra	2016-08-27T13:00:00.000Z	2016-08-27T00:00:00.000Z		13.81340122	100.56222534
map	00:1C:D7:6A:23:45	LUKA's IPhone		infra	2018-01-10T17:00:00.000Z	2018-01-12T09:00:00.000Z		51.31475067	7.3219099
map	00:1D:7E:F9:FE:C4	Sam's iPhone		infra	2011-06-12T19:00:00.000Z	2015-05-15T16:00:00.000Z		32.7215538	-114.6366806
map	00:24:FB:13:4C:F2	Sandra's iPhone		infra	2017-05-21T14:00:00.000Z	2017-05-21T12:00:00.000Z		30.22789192	-97.77940369
map	00:1F:33:44:74:7E	Mathias's iPhone		infra	2016-08-13T19:00:00.000Z	2016-10-19T06:00:00.000Z		57.0494957	9.9154892
map	00:1B:63:C6:C3:BF	rvb's iphone	Apple Inc.	BSS	2009-05-11T01:00:00.000Z	2009-05-10T23:00:00.000Z		47.61297989	-122.32182312
map	00:25:9D:49:0B:C2	Jason's iPhone		infra	2017-07-20T21:00:00.000Z	2017-07-21T04:00:00.000Z		30.23638725	-97.73978424
map	00:25:DF:6E:08:8D	Roy's iPhone		infra	2017-09-07T09:00:00.000Z	2017-09-07T07:00:00.000Z		30.19904518	-97.80830383
map	00:26:75:EF:FE:82	Jaime's iPhone		infra	2015-02-11T08:00:00.000Z	2016-04-24T17:00:00.000Z		47.15561295	-81.31772614

Wigle.net Search for "%s iphone" 2019

OH MY! We were WILDLY successful with that search retrieving over 363,000 entries dating back to 2001. The actual search we submitted (arrow 1 above) is “%’s iphone”, where the “%” is a wildcard telling Wigle to match to anything that comes before it.

Well this could be bad for someone’s privacy. Notice that each SSID above (arrow 2) has a geographic location where it was found. What if we pivot into one of those entries and discovered ALL the places where the wireless network was geolocated. What if it was found at:

- the device owner’s home?
- the device owner’s work?
- the device owner’s client site?
- bars, coffee shops, airports, hotels, and other places the owner might use it?

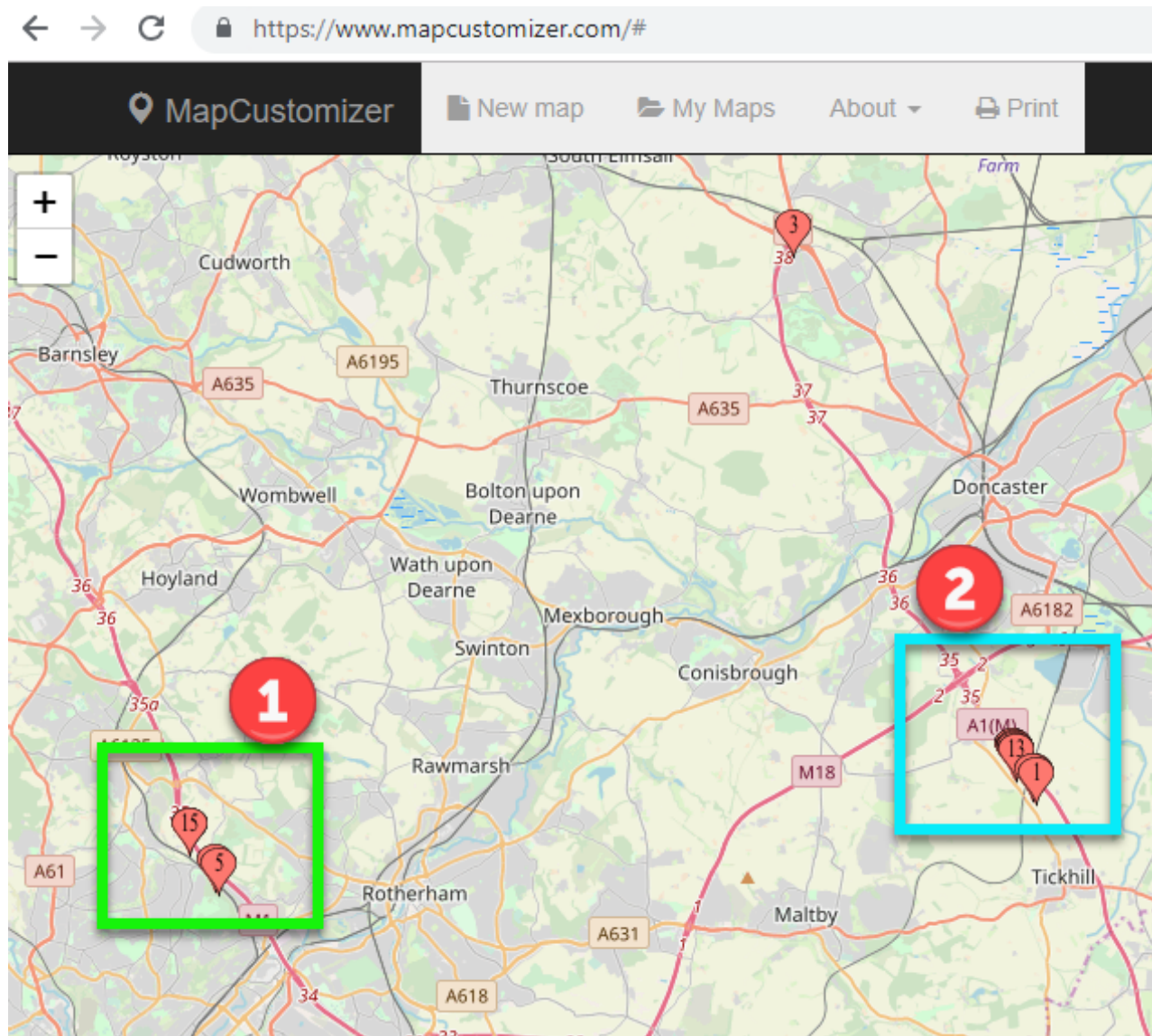
[For this next section, we are using real data from the Wigle.net site and, while it is public, we are blurring out specific details to somewhat protect the privacy of the owner of the device. On the Wigle.net site, you can see all of this data.]

We will pick a random “%’s iphone” and see if multiple locations are noted in the Wigle.net system. For the owner’s privacy, we are not going to tell you which SSID we chose, but the image below shows that, yes, yes you can find devices noted at different locations.

ssid	month	signal	latitude	longitude
hy's iphone	2018-02	-82	53.4553	-1.1167
hy's iphone	2018-02	-82	53.4555	-1.1266
hy's iphone	2017-12	-83	53.5066	-1.2066
hy's iphone	2017-12	-83	53.5066	-1.2069
hy's iphone	2018-02	-85	53.4551	-1.4454
hy's iphone	2018-02	-86	53.4533	-1.4265
hy's iphone	2018-02	-86	53.4533	-1.4279
hy's iphone	2018-04	-89	53.4526	-1.1203
hy's iphone	2018-04	-89	53.4524	-1.1296
hy's iphone	2018-04	-89	53.4578	-1.1207
hy's iphone	2018-04	-89	53.4597	-1.1207
hy's iphone	2018-04	-89	53.4516	-1.1231
hy's iphone	2018-04	-89	53.4517	-1.1296
hy's iphone	2018-04	-89	53.4518	-1.1204
hy's iphone	2018-04	-89	53.4545	-1.1231
hy's iphone	2018-02	-91	53.4506	-1.1233
hy's iphone	2018-02	-93	53.4551	-1.4454

Detailed Wigle.net Results on a Single SSID 2019

Since we have the latitudes and longitudes, we can use an online mapping site to plot the points. We chose the <https://www.mapcustomizer.com/> site but there are many to choose from (or you can use Google Earth or another local piece of software). The image of the points plotted are shown below and clearly show groupings (marked 1 and 2) that could be home and office or coffee shop and hotel.



[While, in a real OSINT investigation, we would drill down into those groupings to discover what buildings, residences, and businesses are there,

for the sake of the iPhone owner's privacy, we will stop here.]

One caveat. Anyone can make their MiFi or phone or even home wireless network have the “%’s iphone” name format. Just because the wireless network name uses this format, we cannot assume that the device is, in fact, an Apple device. We can find this out using the BSSID data.

BSSID Searches for Company

The IEEE (<http://ieee.org>) maintains the authoritative list of what MAC address (BSSID) is registered to what company. See, the first 6 digits in the BSSID are the company that made the transmitter or the device (it depends). We can look up this information at <http://standards-oui.ieee.org/oui/oui.txt>.

So if I see a device that has a BSSID of “A0:04:60:1A:33:8C”, I can search for the “A0:04:60” in the IEEE list (translate the format to use “-” instead of “:”) and find that the device owner/manufacture is “Netgear” (see below).

A4-2B-8C	(hex)	NETGEAR
A42B8C	(base 16)	NETGEAR
		350 East Plumeria Drive
		San Jose CA 95134
		US
A0-04-60	(hex)	NETGEAR
A00460	(base 16)	NETGEAR
		350 East Plumeria Drive
		San Jose CA 95134
		US
9C-3D-CF	(hex)	NETGEAR
9C3DCF	(base 16)	NETGEAR
		350 East Plumeria Drive
		San Jose CA 95134
		US

IEEE.org Search for "A0-04-60" 2019

Going back to verifying our Wigle.net data. Let's look at the list of devices and the first 6 digits of their BSSIDs and look one up. Wigle.net identifies the following device as using the network name of "paolo's iphone". But is it an Apple device?

08:EC:A9:5B:C8:34 paolo's iphone

Let's look up 08-EC-A9 in the **IEEE list**.

08-EC-A9	(hex)	Samsung Electronics Co.,Ltd
08ECA9	(base 16)	Samsung Electronics Co.,Ltd
		#94-1, Imsoo-Dong
		Gumi Gyeongbuk 730-350
		KR

Wait a second! That is not an Apple device. That wireless transmitter is registered to the Samsung Electronics company. There are a number of reasons we might see this type of mismatch in the BSSID and network name including the device is a Samsung device and is using the “paolo’s iphone” wireless name to fool people into thinking it is an iPhone device.

Conclusions

Wireless network data and geolocation information need to be interpreted to be useful. Once again, the analysis of the data becomes important in the OSINT work. We see that wireless network information has been stored and is accessible online since 2001. Even with the uncertainties, this wireless data can be valuable in your OSINT work.

From a privacy perspective, we have some outcomes from our work here too:

1. **Do not use your device to wirelessly tether devices.** Instead, use USB tethering.
2. Understand that devices transmitting wireless signals are being recorded and cataloged and can give away locations and dates. If you have a MiFi device and travel with it, you may be providing others locations of where your device (and you) were at certain dates and times.
3. Understand that the SSID name you choose can make it easier or harder to find your device(s) in Wigle.net.
4. Remove your networks from the Wigle.net database (see below for details).

The folks at Wigle provide an amazing resource for WiFi mapping. They also respect the privacy of anyone who requests their information to be removed from the database as seen at the bottom of the website:

” *“WiGLE respects your privacy. To have records of your access point removed from our database, or if you have any questions or suggestions, send an email to: WiGLE-admin[at]WiGLE.net (please include BSSID (MAC) in removal requests).”*

<https://wisle.net>

One other thing you can do to improve the privacy of your WiFi networks is append the tag ‘_nomap’ or ‘_optout’ to your SSID.

” “WiGLE automatically hides networks (currently 16,644) with these _nomap and/or _optout tags in the ssid.”

<https://wagle.net/phpbb/viewtopic.php?t=2330>

Blog written by: Micah Hoffman, Sector035, baywolf88.

WEBBREACHER

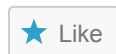
2019-01-15

#PRIVACY, #WARDRIVING, #WIFI, #WIGLE, #WIRELESS

SHARE THIS:



LIKE THIS:



Be the first to like this.

Related



Muting the Twitter algorithm and using basic search operators for better OSINT research

IN "BROWSER"



Making Sense of OSINT Cell Tower Data for DFIR

IN "FORENSICS"



How to search effectively and efficiently - Part I: basic principles, tips and tricks for OSINT

IN "BROWSER"

3 thoughts on “Tracking All the WiFi Things”

Pingback: [WiGILE.Net – Brian.Carnell.Com](#)

Signs You Should Not Break Up

2019-08-07 AT 15:35

I really liked reading your post!. Quality content. With such a valuable blog i believe you deserve to be ranking even higher in the search engines 😊

★ Like

REPLY

Jerrold Villaquiran

2019-08-20 AT 02:53

I have to get across my passion for your kind-heartedness supporting men and women that actually need guidance on that concern. Your very own dedication to getting the message all-around became really interesting and has in every case helped associates like me to achieve their goals. Your interesting tutorial can mean a lot to me and especially to my office workers. Thank you; from all of us.

★ Like

REPLY

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)

PREVIOUS

Thank you for not paying your bill....

NEXT

Five Things You Can Do To Stay OSINT Curious



A WordPress.com Website.