



Rando MAC

@bugg

Focus → iPhone 5 iOS 12.1

- Also did minimal testing with a Samsung running Android 6.0.1
- Want more?
 - Give me your phone!
- Excuse: It's what I had laying around
- It's mostly a software thing so it still relevant for most iPhones
- Android are all over the board cause manufacturers suck (especially Samsung)

Background



- Android
 - Implemented 2014/5 w/Android 6
- iOS
 - Implemented 2014 w/iOS 8.0
- Before:
 - Broadcasted full name and MAC of all known WiFi
- Now:
 - Many rumors and *fake news* that we're gonna clear up
- Too Long Didn't Stay: Apple rules Android drools
(nobody's perfect)

Background

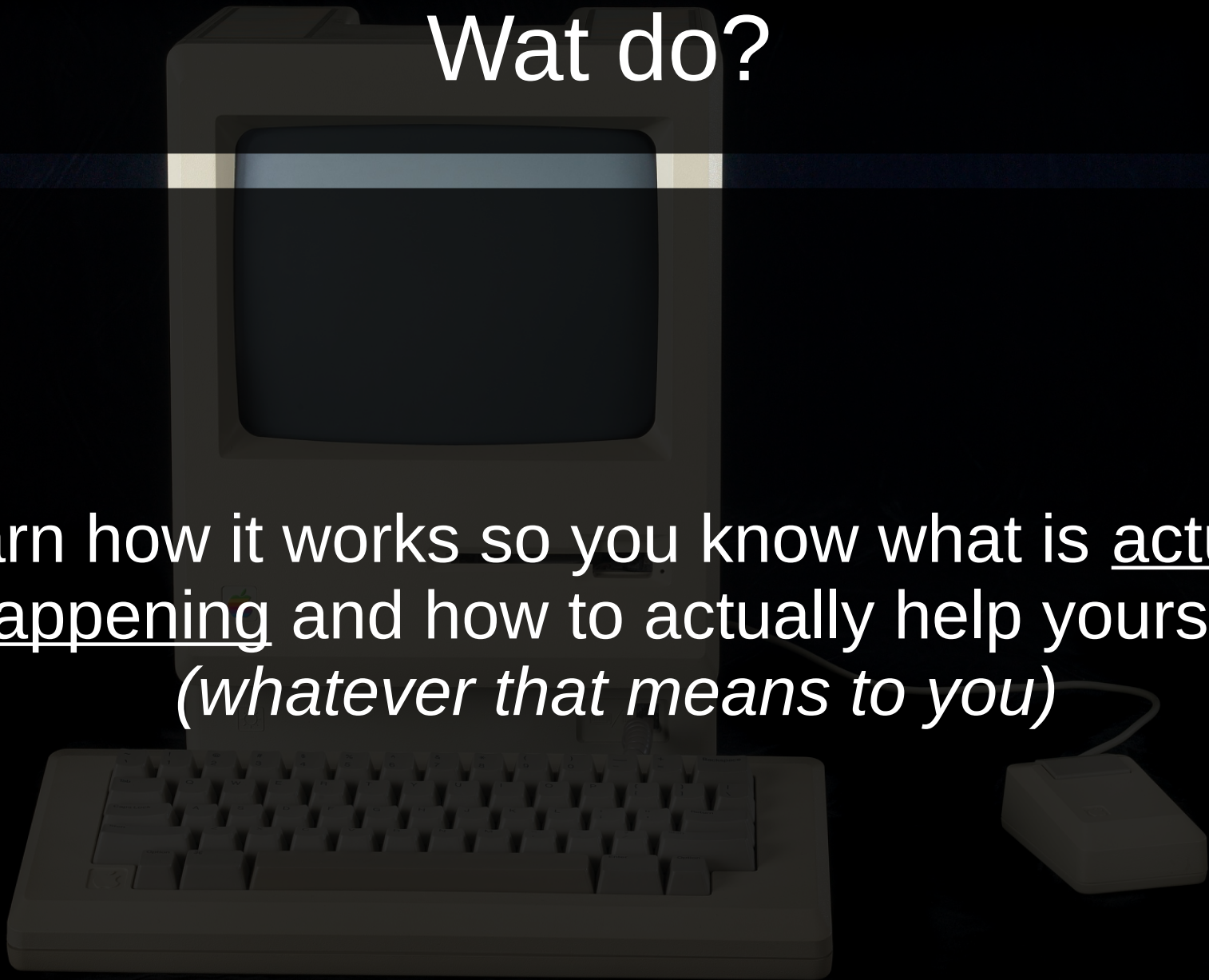
- WiFi (aka 802.11) is some Radio Frequencies that devices use to communicate
- Your phone uses WiFi to bring you internetz
- It talks to Access Points (APs) using the WiFi protocol
- Part of the protocol means that in order for the AP to tell your packetz from the rest, your device (phone in this case) sends a unique identifier (hex value) along with every packet it broadcasts
- This unique identifier is called a Media Access Control (MAC) Address

So What?

- Once-upon-a-time this was just fine
- Now this MAC is used to track you
- This is not a conspiracy theory, this is a fact
 - Yes, the government tracks you with this
 - Yes, foreign governments track you with this
 - Yes, businesses track you with this
 - Yes, institutions track you with this
 - Yes, criminals track you with this
- Don't Care? Cool. This is not for you.


Wat do?

Learn how it works so you know what is actually happening and how to actually help yourself
(whatever that means to you)



Nominal Analysis



- Simple analysis will give you 90% of the problem/solution
- No need for fancy tools or statistical analysis
- Tools:
 - Wireshark 
 - Wireless card in Monitor Mode
 - Access to the device you want to analyze
 - Access to an AP the device is familiar with
- Lets do this!

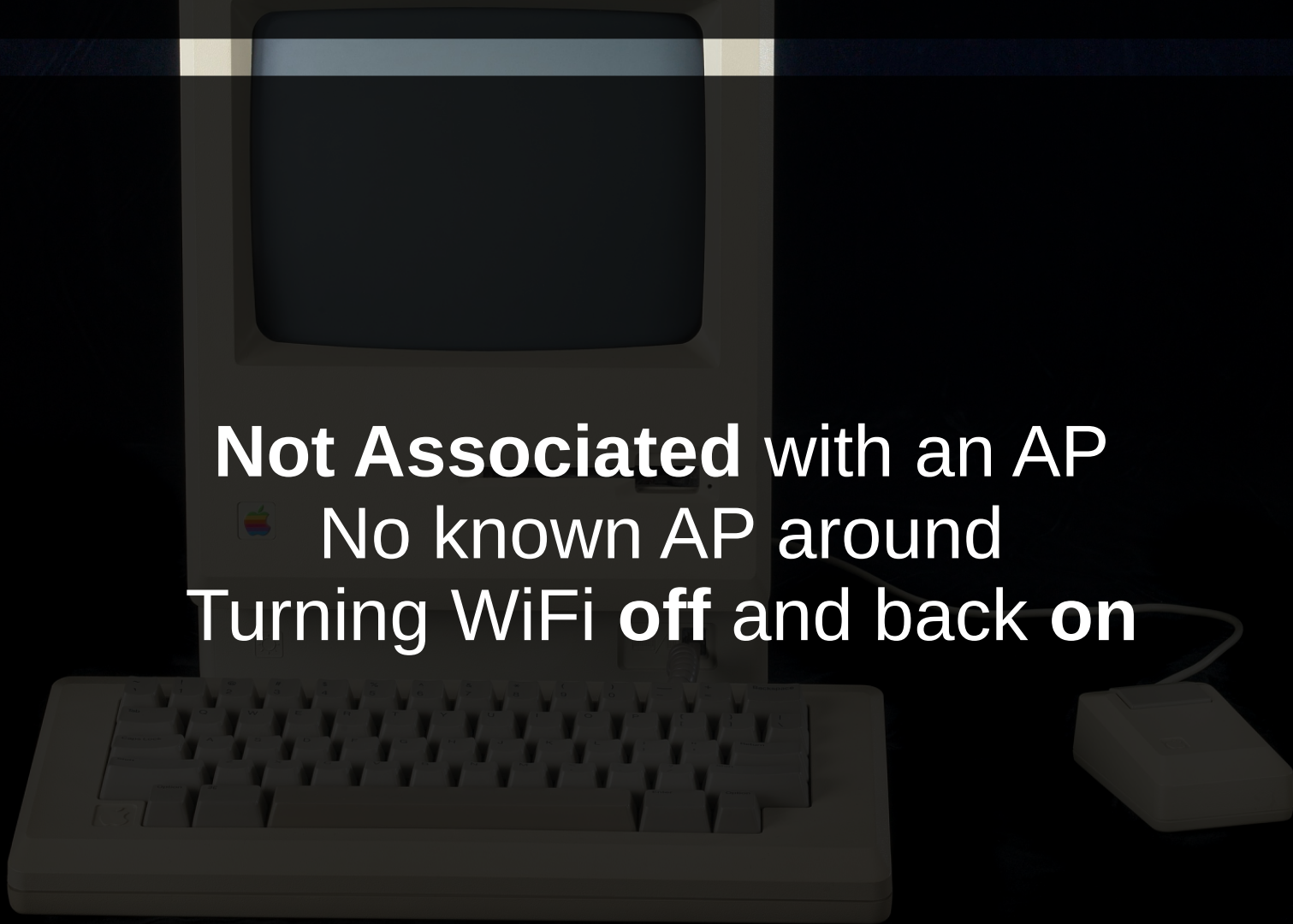
iPhone 5s – iOS 12.1

Not Associated with an AP



No known AP around


Turning WiFi off and back on



iPhone 5s – iOS 12.1

Time	Source	Destination	Info
3.400553011	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=1, FN=0, Flags=....., SSID=Broadcast
3.446173084	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=2, FN=0, Flags=....., SSID=Broadcast
3.487201770	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=3, FN=0, Flags=....., SSID=Broadcast
3.527399075	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=4, FN=0, Flags=....., SSID=Broadcast
6.604503118	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=27, FN=0, Flags=....., SSID=Broadcast
6.652230435	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=28, FN=0, Flags=....., SSID=Broadcast
6.692444796	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=29, FN=0, Flags=....., SSID=Broadcast
6.735449704	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=30, FN=0, Flags=....., SSID=Broadcast
6.780621477	4a:ac:e7:7e:04:71	Broadcast	Probe Request, SN=31, FN=0, Flags=....., SSID=Broadcast
18.218588737	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=2, FN=0, Flags=....., SSID=Broadcast
18.262010736	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=3, FN=0, Flags=....., SSID=Broadcast
18.304699985	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=4, FN=0, Flags=....., SSID=Broadcast
19.075492535	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=15, FN=0, Flags=....., SSID=Broadcast
21.355655007	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=26, FN=0, Flags=....., SSID=Broadcast
21.398756240	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=27, FN=0, Flags=....., SSID=Broadcast
25.282744555	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=7, FN=0, Flags=....., SSID=Broadcast
25.328418724	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=8, FN=0, Flags=....., SSID=Broadcast
25.369181515	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=9, FN=0, Flags=....., SSID=Broadcast
32.144915622	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=1, FN=0, Flags=....., SSID=Broadcast
32.187782961	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=2, FN=0, Flags=....., SSID=Broadcast
32.234299722	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=3, FN=0, Flags=....., SSID=Broadcast
32.276744561	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=4, FN=0, Flags=....., SSID=Broadcast
33.227045571	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=19, FN=0, Flags=....., SSID=Broadcast
33.269544671	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=20, FN=0, Flags=....., SSID=Broadcast
33.314023185	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=21, FN=0, Flags=....., SSID=Broadcast
33.358277628	8e:7c:e4:c0:a3:91	Broadcast	Probe Request, SN=22, FN=0, Flags=....., SSID=Broadcast

iPhone 5s – iOS 12.1

Associated with an AP
 **Keeping WiFi on**
Going out of range of AP



iPhone 5s – iOS 12.1

Time	Source	Destination	Info
395.321790093	Apple	Broadcast	Probe Request, SN=1457, FN=0, Flags=....., SSID=Broadcast
818.461270954	Apple	Broadcast	Probe Request, SN=1775, FN=0, Flags=....., SSID=Broadcast
818.486336701	Apple	Broadcast	Probe Request, SN=1776, FN=0, Flags=....., SSID=Broadcast
818.680278545	Apple	Broadcast	Probe Request, SN=1783, FN=0, Flags=....., SSID=Broadcast
818.702807097	Apple	Broadcast	Probe Request, SN=1784, FN=0, Flags=....., SSID=Broadcast
832.574851942	Apple	Broadcast	Probe Request, SN=1941, FN=0, Flags=....., SSID=Broadcast
832.630875127	Apple	Broadcast	Probe Request, SN=1943, FN=0, Flags=....., SSID=Broadcast
832.653920659	Apple	Broadcast	Probe Request, SN=1944, FN=0, Flags=....., SSID=Broadcast
832.677161432	Apple	Broadcast	Probe Request, SN=1945, FN=0, Flags=....., SSID=Broadcast
846.766266207	Apple	Broadcast	Probe Request, SN=2013, FN=0, Flags=....., SSID=Broadcast
859.251481709	Apple	Broadcast	Probe Request, SN=2076, FN=0, Flags=....., SSID=
859.483304500	Apple	Broadcast	Probe Request, SN=2079, FN=0, Flags=....., SSID=
859.508930004	Apple	Broadcast	Probe Request, SN=2080, FN=0, Flags=....., SSID=
859.530185429	Apple	Broadcast	Probe Request, SN=2081, FN=0, Flags=....., SSID=
859.553029001	Apple	Broadcast	Probe Request, SN=2082, FN=0, Flags=....., SSID=
859.815386794	Apple	Broadcast	Probe Request, SN=2089, FN=0, Flags=....., SSID=
861.197139906	Apple	Broadcast	Probe Request, SN=2107, FN=0, Flags=....., SSID=Broadcast
861.226702269	Apple	Broadcast	Probe Request, SN=2108, FN=0, Flags=....., SSID=Broadcast
861.246590685	Apple	Broadcast	Probe Request, SN=2109, FN=0, Flags=....., SSID=Broadcast
866.164738541	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2150, FN=0, Flags=....., SSID=Broadcast
866.601354849	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2155, FN=0, Flags=....., SSID=Broadcast
866.642983231	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2156, FN=0, Flags=....., SSID=Broadcast
866.685539396	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2157, FN=0, Flags=....., SSID=Broadcast
866.729913158	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2158, FN=0, Flags=....., SSID=Broadcast
866.940976823	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2163, FN=0, Flags=....., SSID=Broadcast
870.275621046	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=1, FN=0, Flags=....., SSID=Broadcast
870.316039115	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2, FN=0, Flags=....., SSID=Broadcast
870.488103543	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=6, FN=0, Flags=....., SSID=Broadcast
877.118926484	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=1, FN=0, Flags=....., SSID=Broadcast
877.161417534	3e:a3:b5:76:3a:eb	Broadcast	Probe Request, SN=2, FN=0, Flags=....., SSID=Broadcast

Samsung – Android 6.0.1

Not Associated with an AP



No known AP around


Turning WiFi off and back on



Samsung – Android 6.0.1

Time	Source	Destination	Info
10.203758...	SamsungE	broadcast	Probe Request, SN=110, FN=0, Flags=....., SSID=Broadcast
10.229443...	SamsungE	broadcast	Probe Request, SN=111, FN=0, Flags=....., SSID=Broadcast
10.296299...	SamsungE	broadcast	Probe Request, SN=112, FN=0, Flags=....., SSID=Broadcast
10.326208...	SamsungE	broadcast	Probe Request, SN=113, FN=0, Flags=....., SSID=Broadcast
10.385318...	SamsungE	broadcast	Probe Request, SN=114, FN=0, Flags=....., SSID=Broadcast
10.405803...	SamsungE	broadcast	Probe Request, SN=115, FN=0, Flags=....., SSID=Broadcast
10.693013...	SamsungE	broadcast	Probe Request, SN=121, FN=0, Flags=....., SSID=Broadcast
10.755328...	SamsungE	broadcast	Probe Request, SN=122, FN=0, Flags=....., SSID=Broadcast
10.965871...	SamsungE	broadcast	Probe Request, SN=127, FN=0, Flags=....., SSID=Broadcast
11.029871...	SamsungE	broadcast	Probe Request, SN=128, FN=0, Flags=....., SSID=Broadcast
11.045744...	SamsungE	broadcast	Probe Request, SN=129, FN=0, Flags=....., SSID=Broadcast
11.115877...	SamsungE	broadcast	Probe Request, SN=130, FN=0, Flags=....., SSID=Broadcast
11.146545...	SamsungE	broadcast	Probe Request, SN=131, FN=0, Flags=....., SSID=Broadcast
43.351038...	SamsungE	broadcast	Probe Request, SN=134, FN=0, Flags=....., SSID=Broadcast
43.376799...	SamsungE	broadcast	Probe Request, SN=135, FN=0, Flags=....., SSID=Broadcast
43.461017...	SamsungE	broadcast	Probe Request, SN=136, FN=0, Flags=....., SSID=Broadcast
43.488222...	SamsungE	broadcast	Probe Request, SN=137, FN=0, Flags=....., SSID=Broadcast
43.857707...	SamsungE	broadcast	Probe Request, SN=144, FN=0, Flags=....., SSID=Broadcast
43.886082...	SamsungE	broadcast	Probe Request, SN=145, FN=0, Flags=....., SSID=Broadcast
43.950771...	SamsungE	broadcast	Probe Request, SN=146, FN=0, Flags=....., SSID=Broadcast
43.976011...	SamsungE	broadcast	Probe Request, SN=147, FN=0, Flags=....., SSID=Broadcast
44.087430...	SamsungE	broadcast	Probe Request, SN=149, FN=0, Flags=....., SSID=Broadcast
44.160737...	SamsungE	broadcast	Probe Request, SN=150, FN=0, Flags=....., SSID=Broadcast
44.191040...	SamsungE	broadcast	Probe Request, SN=151, FN=0, Flags=....., SSID=Broadcast
44.251997...	SamsungE	broadcast	Probe Request, SN=152, FN=0, Flags=....., SSID=Broadcast
44.279404...	SamsungE	broadcast	Probe Request, SN=153, FN=0, Flags=....., SSID=Broadcast
82.123746...	SamsungE	broadcast	Probe Request, SN=154, FN=0, Flags=....., SSID=Broadcast
82.155905...	SamsungE	broadcast	Probe Request, SN=155, FN=0, Flags=....., SSID=Broadcast
82.214447...	SamsungE	broadcast	Probe Request, SN=156, FN=0, Flags=....., SSID=Broadcast

Samsung – Android 6.0.1

Associated with an AP
 **Keeping WiFi on**
Going out of range of AP



Samsung – Android 6.0.1

Time	Source	Destination	Info
268.40248...	SamsungE	broadcast	Probe Request, SN=179, FN=0, Flags=....., SSID=Broadcast
268.41648...	SamsungE	broadcast	Probe Request, SN=180, FN=0, Flags=....., SSID=Broadcast
268.45215...	SamsungE	broadcast	Probe Request, SN=181, FN=0, Flags=....., SSID=Broadcast
268.46239...	SamsungE	broadcast	Probe Request, SN=182, FN=0, Flags=....., SSID=Broadcast
302.90710...	SamsungE	broadcast	Probe Request, SN=185, FN=0, Flags=....., SSID=Broadcast
302.91282...	SamsungE	broadcast	Probe Request, SN=186, FN=0, Flags=....., SSID=Broadcast
302.96592...	SamsungE	broadcast	Probe Request, SN=187, FN=0, Flags=....., SSID=Broadcast
302.97319...	SamsungE	broadcast	Probe Request, SN=188, FN=0, Flags=....., SSID=Broadcast
303.02320...	SamsungE	broadcast	Probe Request, SN=189, FN=0, Flags=....., SSID=Broadcast
303.03214...	SamsungE	broadcast	Probe Request, SN=190, FN=0, Flags=....., SSID=Broadcast
303.27228...	SamsungE	broadcast	Probe Request, SN=195, FN=0, Flags=....., SSID=Broadcast
303.29131...	SamsungE	broadcast	Probe Request, SN=196, FN=0, Flags=....., SSID=Broadcast
303.68522...	SamsungE	broadcast	Probe Request, SN=203, FN=0, Flags=....., SSID=Broadcast
303.69254...	SamsungE	broadcast	Probe Request, SN=204, FN=0, Flags=....., SSID=Broadcast
303.74146...	SamsungE	broadcast	Probe Request, SN=205, FN=0, Flags=....., SSID=Broadcast
303.74424...	SamsungE	broadcast	Probe Request, SN=206, FN=0, Flags=....., SSID=Broadcast
312.95256...	SamsungE	broadcast	Probe Request, SN=209, FN=0, Flags=....., SSID=Broadcast
312.96214...	SamsungE	broadcast	Probe Request, SN=210, FN=0, Flags=....., SSID=Broadcast
313.19287...	SamsungE	broadcast	Probe Request, SN=216, FN=0, Flags=....., SSID=Broadcast
313.75345...	SamsungE	broadcast	Probe Request, SN=227, FN=0, Flags=....., SSID=Broadcast
313.77052...	SamsungE	broadcast	Probe Request, SN=228, FN=0, Flags=....., SSID=Broadcast
319.41677...	SamsungE	broadcast	Probe Request, SN=231, FN=0, Flags=....., SSID=Broadcast
319.43192...	SamsungE	broadcast	Probe Request, SN=232, FN=0, Flags=....., SSID=Broadcast
319.96944...	SamsungE	broadcast	Probe Request, SN=255, FN=0, Flags=....., SSID=Broadcast
319.98461...	SamsungE	broadcast	Probe Request, SN=256, FN=0, Flags=....., SSID=Broadcast
323.91397...	SamsungE	Raspberr_...	Probe Request, SN=257, FN=0, Flags=....., SSID=Broadcast
323.91515...	SamsungE	Raspberr_...	Probe Request, SN=257, FN=0, Flags=....R..., SSID=Broadcast
323.91611...	SamsungE	Raspberr_...	Probe Request, SN=257, FN=0, Flags=....R..., SSID=Broadcast
323.91745...	SamsungE	Raspberr_...	Probe Request, SN=257, FN=0, Flags=....R..., SSID=Broadcast
323.91875...	SamsungE	Raspberr_...	Probe Request, SN=257, FN=0, Flags=....R..., SSID=Broadcast
323.91971...	SamsungE	Raspberr_...	Probe Request, SN=257, FN=0, Flags=....R..., SSID=Broadcast

Conclusions

- Direct Analysis:
 - iPhone running iOS 12.1
 - Fully Randomizes MAC when not associating/ed with known AP
 - Changes random MAC on every AP disassociation or network rotation (on/off)
 - Samsung running Android 6.0.1
 - Performs no MAC randomization whatsoever
- Research Analysis:
 - IOS 10+
 - Generally proper randomization with the exception of a control frame which identifies the 'random' device as an iPhone
 - Android 6+
 - Differs from version to version and manufacturer to manufacturer
 - Worst: No Randomization + Always Broadcasting SSIDs
 - Best: Random Probing mixed with real-MAC probing



Sources

- Martin, Jeremy, et al. "A study of MAC address randomization in mobile devices and when it fails." Proceedings on Privacy Enhancing Technologies 2017.4 (2017): 365-383.
- Vanhoef, Mathy, et al. "Why MAC address randomization is not enough: An analysis of Wi-Fi network discovery mechanisms." Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016.
- AirTightTeam. "iOS8 MAC Randomization – Analyzed!" Mojo Networks Blog, blog.mojonetworks.com/ios8-mac-randomization-analyzed/.
- "Android 6.0 Changes | Android Developers." Android Developers, developer.android.com/about/versions/marshmallow/android-6.0-changes.
- Gallagher, Sean. "Where've You Been? Your Smartphone's Wi-Fi Is Telling Everyone. [Updated]." Ars Technica, Ars Technica, 5 Nov. 2014, arstechnica.com/information-technology/2014/11/where-have-you-been-your-smartphones-wi-fi-is-telling-everyone/.
- Miorandi, Daniele. "I Lie, You Lie, Everybody Lies: WiFi Tracking in the Era of MAC Randomization." Medium.com, Medium, 10 Apr. 2017, medium.com/@DanieleMiorandi/i-lie-you-lie-everybody-lies-wifi-tracking-in-the-era-of-mac-randomization-2ab147857b24.
- Blix. "Tourism Footfall Analytics | Tourism Foot Traffic Counters | Tourism People Counter." Blix, www.getblix.com/tourism-footfall-analytics.
- Cooney, Michael. "How Do Mobile Location Services Threaten Users?" Network World, Network World, 5 June 2014, www.networkworld.com/article/2360206/mobile-security/how-do-mobile-location-services-threaten-users.html.
- Corfield, Gareth. "TfL to Track Tube Users in Stations by Their MAC Addresses." The Register® - Biting the Hand That Feeds IT, The Register, 17 Nov. 2016, www.theregister.co.uk/2016/11/17/tfl_to_track_tube_users_by_wifi_device_mac_address/.
- "My Phone at Your Service." Federal Trade Commission, 17 Dec. 2014, www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service.