


I Know What  
You Are By the  
Smell of Your  
Wi-Fi



Denton Gentry

Try It!

SSID: SmellOfWifiTalk

Poll: Wi-Fi at DEFCON for a demo

bad idea. 1%

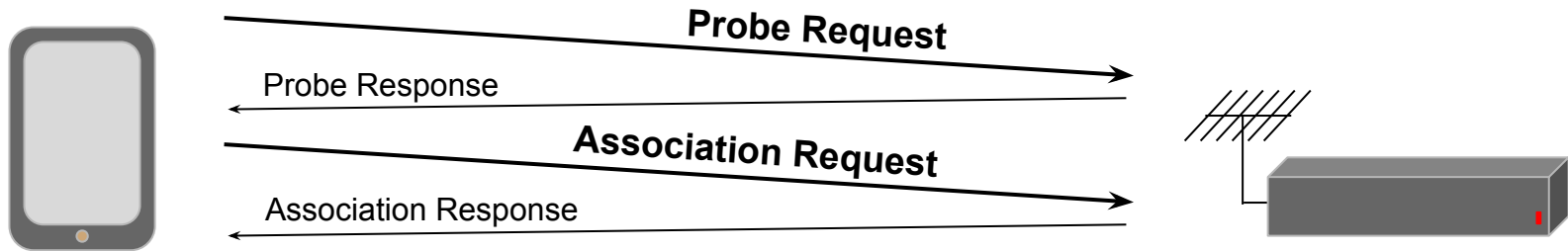
worst idea. 10%

what could go wrong? 89%

# MAC Sublayer Management Entity (MLME)

**Probe Request:** Asks nearby APs to respond.

**Association Request:** join the Wi-Fi network



# Signature: Information Elements

- ▶ Frame 9: 199 bytes on wire (1592 bits), 199 bytes captured
- ▶ Radiotap Header v0, Length 25
- ▶ 802.11 radio information
- ▶ IEEE 802.11 Association Request, Flags: .....
- ▼ IEEE 802.11 wireless LAN management frame
  - ▶ Fixed parameters (4 bytes)
  - ▼ Tagged parameters (142 bytes)
    - ▶ Tag: SSID parameter set: XXXXXXXXXXXX
    - ▶ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B),
    - ▶ Tag: Power Capability Min: 249, Max :19
    - ▶ Tag: Supported Channels
    - ▶ Tag: RSN Information
    - ▶ Tag: RM Enabled Capabilities (5 octets)
    - ▶ Tag: HT Capabilities (802.11n D1.10)
    - ▶ Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
    - ▶ Tag: Vendor Specific: Apple
    - ▶ Tag: Vendor Specific: Broadcom
    - ▶ Tag: Vendor Specific: Microsoft: WMM/WME: Informi

- Tag #0
- Tag #1
- Tag #33
- Tag #36
- Tag #48
- Tag #70
- Tag #45
- Tag #191
- Tag #221, Vendor OUI 00:17:f2, #10
- Tag #221, Vendor OUI 00:10:18, #2
- Tag #221, Vendor OUI 00:50:f2, #2

0, 1, 33, 36, 48, 70, 45, 191, 221(0017f2, 10), 221(001018, 2), 221(0050f2, 2)

# Signature: Capability bitmasks

- ▼ Tag: Power Capability Min: 249, Max :19
  - Tag Number: Power Capability (33)
  - Tag length: 2
  - Minimum Transmit Power: 249 (0xf9)
  - Maximum Transmit Power: 19 (0x13)
- ▶ Tag: Supported Channels
- ▶ Tag: RSN Information
- ▶ Tag: RM Enabled Capabilities (5 octets)
- ▼ Tag: HT Capabilities (802.11n D1.10)
  - Tag Number: HT Capabilities (802.11n D1.
  - Tag length: 26
  - ▶ HT Capabilities Info: 0x006f
  - ▶ A-MPDU Parameters: 0x17
  - ▶ Rx Supported Modulation and Coding Schem
  - ▶ HT Extended Capabilities: 0x0000
  - ▶ Transmit Beam Forming (TxBF) Capabilitie
  - ▶ Antenna Selection (ASEL) Capabilities: 0
- ▼ Tag: VHT Capabilities (IEEE Std 802.11ac/D.
  - Tag Number: VHT Capabilities (IEEE Std 8
  - Tag length: 12
  - ▶ VHT Capabilities Info: 0x0f811032
  - ▶ VHT Supported MCS Set

Transmit power  
HT Capabilities bitmask (802.11n)  
VHT Capabilities bitmask (802.11ac)

0, 1, 33, 36, 48, 70, 45, 191, 221  
(0017f2, 10), 221(001018, 2),  
221(0050f2, 2), **txpow: 13f9,**  
**htcap: 006f, vhtcap: 0f811032**

# Distinctiveness Over Time

## iPhone, 2007

0,1,48,50

## iPhone 4s, 2011

0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),  
htcap:0100,htag:19,htmcs:00000ff

## iPhone 7, 2016

0,1,33,36,48,70,54,45,127,191,199,221(0017f2,10),221(001  
018,2),221(0050f2,2),htcap:006f,htag:17,htmcs:0000ffff,  
vhtcap:0f811032,vhtrxmcs:0000fffa,vhttzmcs:0000fffa,txpo  
w:13f9,extcap:000008

# Signatures in their Final Form

## Xbox One

```
wifi4|probe:0,1,45,50,htcap:058f,htagg:03,htmcs:0000ffff|assoc:0,1,33,36,221(0050f2,2),45,htcap:058f,htagg:03,htmcs:0000ffff,txpow:1208
```

## Nest Thermostat v3

```
wifi4|probe:0,1,45,221(001018,2),221(00904c,51),htcap:0062,htagg:1a,htmcs:000000ff|assoc:0,1,33,36,48,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:0062,htagg:1a,htmcs:000000ff,txpow:0f09
```

## Chromecast v1

```
wifi4|probe:0,1,3,45,50,htcap:0120,htagg:03,htmcs:00000000|assoc:0,1,48,50,127,221(0050f2,2),45,htcap:012c,htagg:03,htmcs:000000ff,extcap:00000000000000140
```

# Multiple Signatures

```
wifi4|probe:0,1,45,221(0050f2,8),191,127,htcap:01ef,htagg:1f,htmcs:0000ffff,vhtcap:339071b2,vhtrxmscs:030cffffa,vhttxmscs:030cffffa,extcap:04000000000004080|assoc:0,1,48,45,221(0050f2,2),191,127,htcap:01ef,htagg:1f,htmcs:0000ffff,vhtcap:339071b2,vhtrxmscs:030cffffa,vhttxmscs:030cffffa,extcap:04000a020100004080
```

```
wifi4|probe:0,1,45,221(0050f2,8),191,127,htcap:01ef,htagg:1f,htmcs:0000ffff,vhtcap:339031b2,vhtrxmscs:030cffffa,vhttxmscs:030cffffa,extcap:04000000000004080|assoc:0,1,48,45,221(0050f2,2),191,127,htcap:01ef,htagg:1f,htmcs:0000ffff,vhtcap:339031b2,vhtrxmscs:030cffffa,vhttxmscs:030cffffa,extcap:04000a020100004080
```



# Signature Aliasing

## Amazon Dash Button

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff

## First Alert Thermostat

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff

## Nexus 7 (2012 edition)

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff

## Roku HD

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff

## Withings Scale

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff

# Signature Disambiguation

## Amazon Dash Button

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff|oui:amazon

## First Alert Thermostat

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff|oui:firstalert

## Nexus 7 (2012 edition)

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff|oui:asus

## Roku HD

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff|os:roku

## Withings Scale

wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htag:19,htmcs:000000ff|assoc:0,1,48,50,45,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htag:19,htmcs:000000ff|oui:withings

# Mobile Only!

Taxonomy identifies the Wi-Fi circuitry, device driver, and OS.

- Works for highly integrated devices: mobile and IOT.
- With a Wi-Fi card in a laptop... it identifies the card.

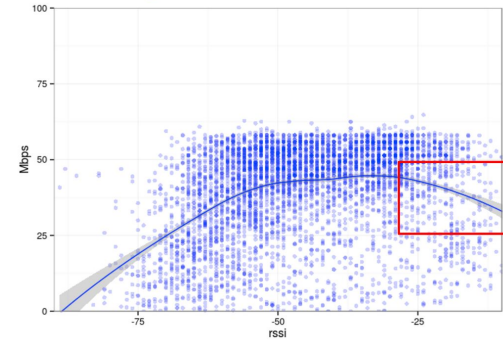
# Uses of Wi-Fi Taxonomy

## Current

- List of Connected Clients in UI
- Correlate with other data

## Future

- Optimize for client ?
- WIDS ?



# Current Status

- hostapd 2.7 added CONFIG\_TAXONOMY.
  - hostapd\_cli command: signature
- Database of known signatures:
  - [https://github.com/NetworkDeviceTaxonomy/wifi\\_taxonomy](https://github.com/NetworkDeviceTaxonomy/wifi_taxonomy)
  - Mobile & IOT, not laptops/desktops
  - ~60% of connected Wifi devices

# Other resources

- Published paper  
<https://research.google.com/pubs/pub45429.html>  
<https://arxiv.org/abs/1608.01725>
- *“Measuring wifi performance across all Google Fiber customers”*  
Avery Pennarun, Netdev 1.1, 2015  
<https://youtu.be/yZcHbD84j5Y>  
<http://apenwarr.ca/diary/wifi-data-apenwarr-201602.pdf>
- <https://github.com/NetworkDeviceTaxonomy>