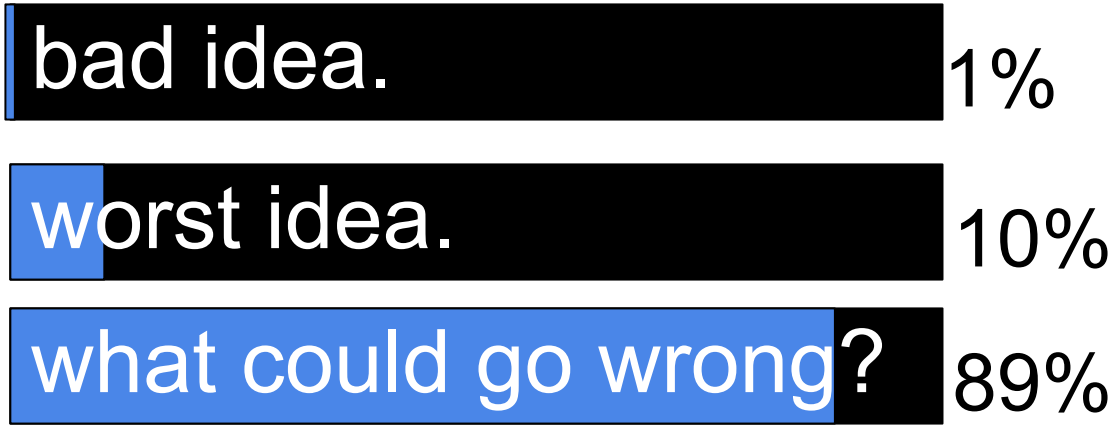
I Know What You Are By the Smell of Your Wi-Fi

Denton Gentry

Try It!

SSID: SmellOfWifiTalk

Poll: Wi-Fi at DEFCON for a demo

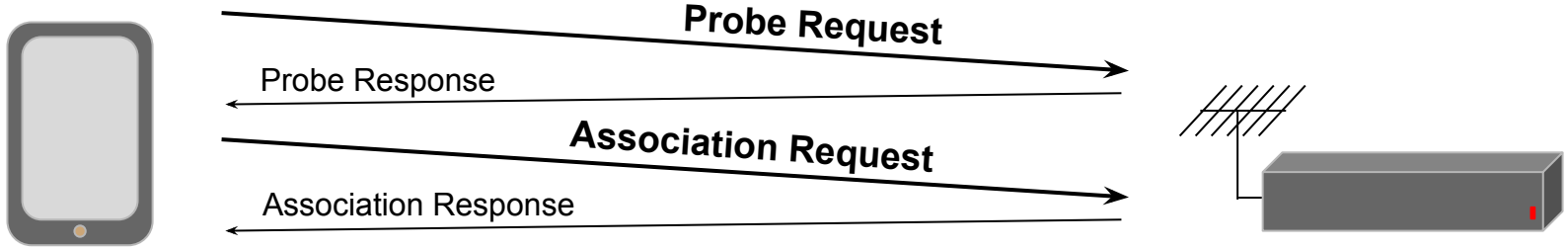


Try It! SSID: SmellOfWifiTalk

MAC Sublayer Management Entity (MLME)

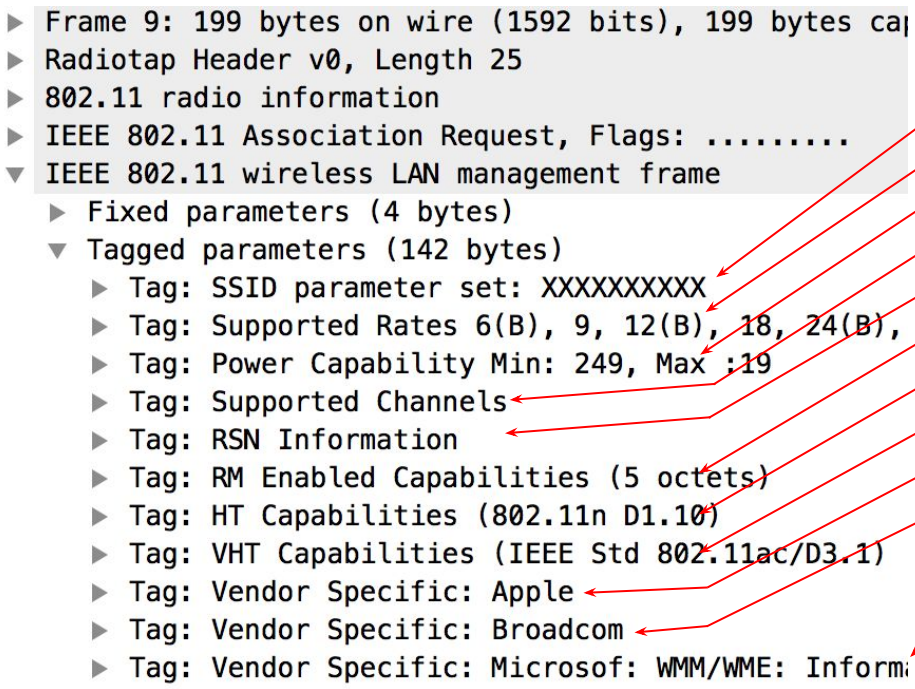
Probe Request: Asks nearby APs to respond.

Association Request: join the Wi-Fi network



Try It! SSID: SmellOfWifiTalk

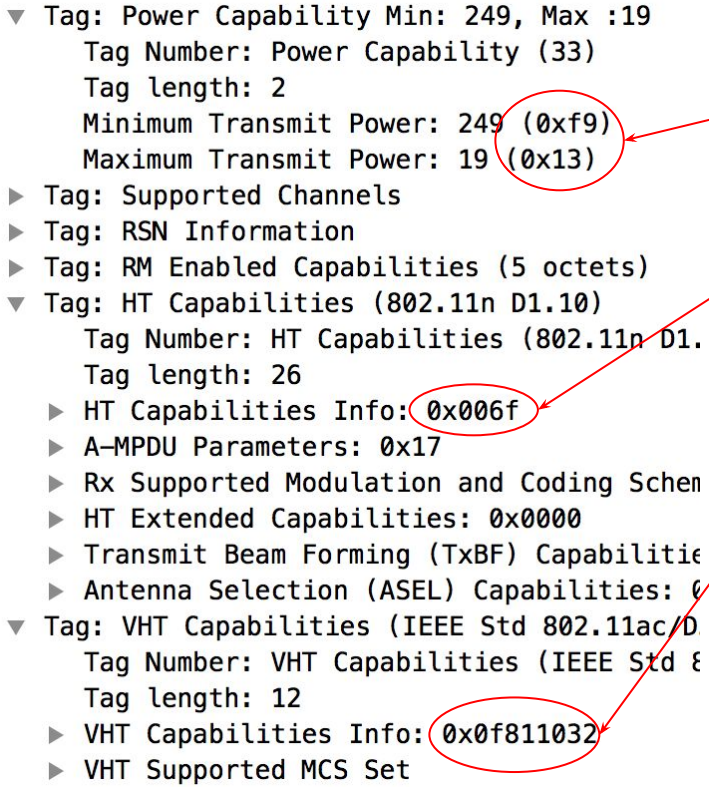
Signature: Information Elements



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



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,htagg:19,htmcs:000000ff
```

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,htagg:17,htmcs:0000ffff,
vhtcap:0f811032,vhtrxmcs:0000fffa,vhttxmcs: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,h
tmcs: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:
0000000000000140
```

Multiple Signatures

```
wifi4|probe:0,1,45,221(0050f2,8),191,127,htcap:01ef,htagg:1f,htmcs:0000ff
ff,vhtcap:339071b2,vhtrxmcs:030cfffa,vhttxmcs:030cfffa,extcap:04000000000
0004080|assoc:0,1,48,45,221(0050f2,2),191,127,htcap:01ef,htagg:1f,htmcs:0
000ffff,vhtcap:339071b2,vhtrxmcs:030cfffa,vhttxmcs:030cfffa,extcap:04000a
020100004080
```

```
wifi4|probe:0,1,45,221(0050f2,8),191,127,htcap:01ef,htagg:1f,htmcs:0000ff
ff,vhtcap:339031b2,vhtrxmcs:030cfffa,vhttxmcs:030cfffa,extcap:04000000000
0004080|assoc:0,1,48,45,221(0050f2,2),191,127,htcap:01ef,htagg:1f,htmcs:0
000ffff,vhtcap:339031b2,vhtrxmcs:030cfffa,vhttxmcs:030cfffa,extcap:04000a
020100004080
```

Try It! SSID: SmellOfWifiTalk

Signature Aliasing

Amazon Dash Button

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff
```

First Alert Thermostat

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff
```

Nexus 7 (2012 edition)

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff
```

Roku HD

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff
```

Withings Scale

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff
```

Try It! SSID: SmellOfWifiTalk

Signature Disambiguation

Amazon Dash Button

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff|oui:amazon
```

First Alert Thermostat

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff|oui:firstalert
```

Nexus 7 (2012 edition)

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff|oui:asus
```

Roku HD

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff|os:roku
```

Withings Scale

```
wifi4|probe:0,1,50,45,3,221(001018,2),221(00904c,51),htcap:110c,htagg:19,htmcs:000000ff|assoc:0,1,48,50,4
5,221(001018,2),221(00904c,51),221(0050f2,2),htcap:110c,htagg:19,htmcs:000000ff|oui:withings
```

Try It! SSID: SmellOfWifiTalk

Mobile Only!

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

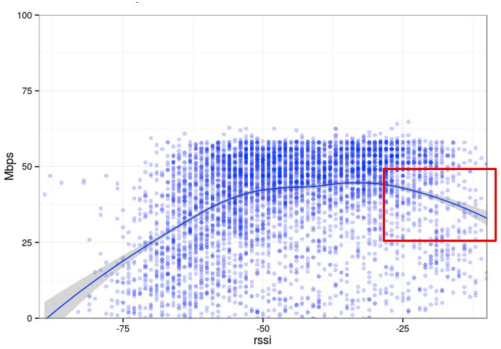
- Works for highly integrated devices: mobile and IOT.
- With a Wi-Fi card in a laptop... it identifies the card.

Try It! SSID: SmellOfWifiTalk

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
  - 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