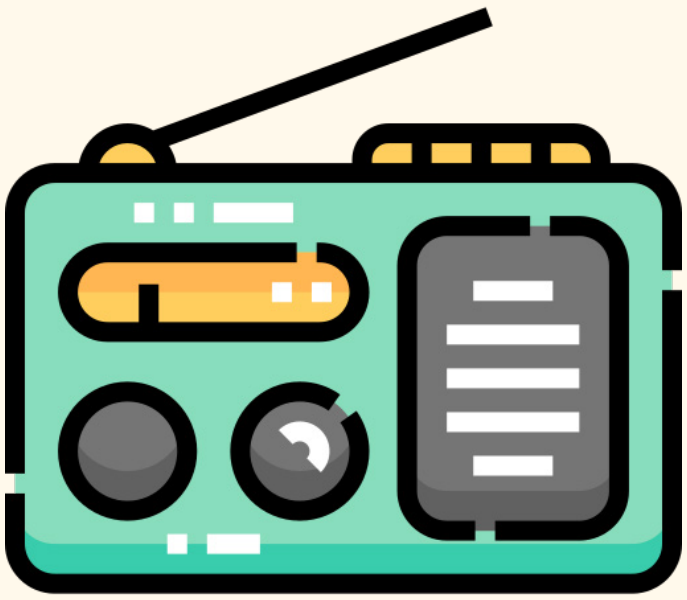
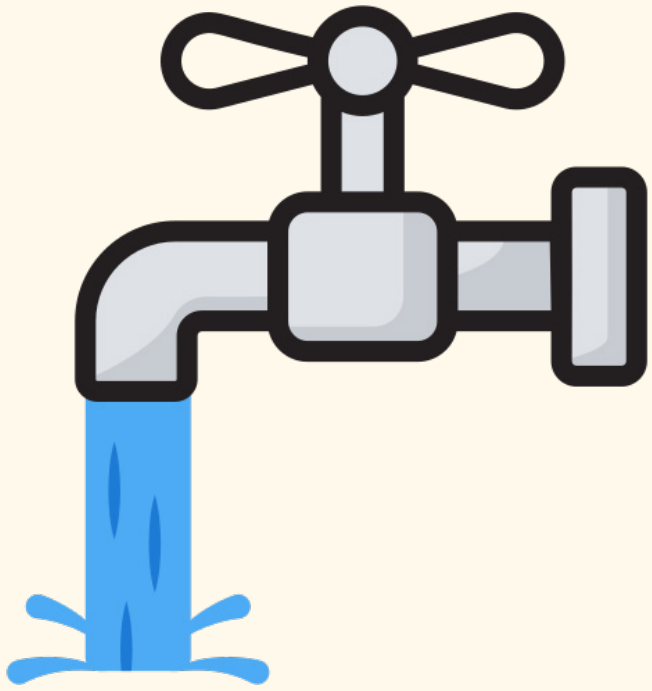
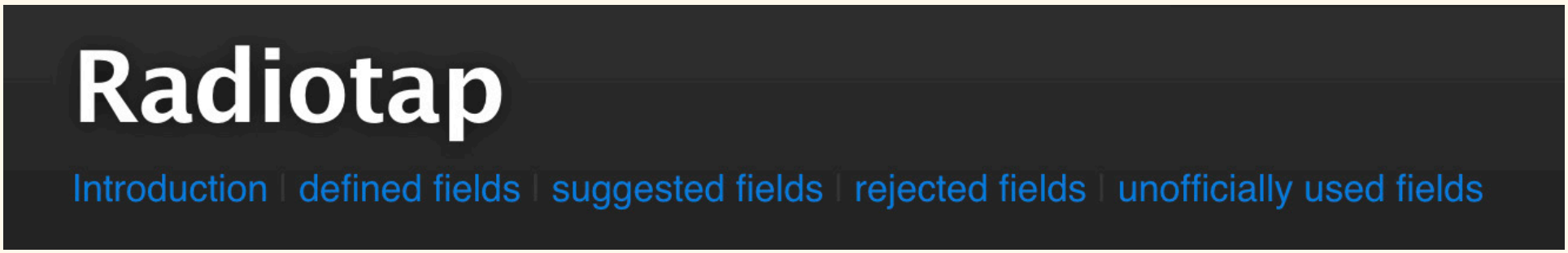
Radiotap Headers for Troubleshooting





WiFrizzy.com | Eva Santos

What is it?



- A standard for 802.11 frame injection and reception compatible with many OSs

-When viewing packet captures, it provides information from the drivers about signal quality and PHY standards.

-Not actually part of the frame for frame length purposes

Keep in Mind

-This information is added by the **capturing** driver

-The information is only as good as the driver/radio/antenna capturing the frames

-Let's look at some examples

MacBook Capture

-Here are two frames captured from my MacBook Air

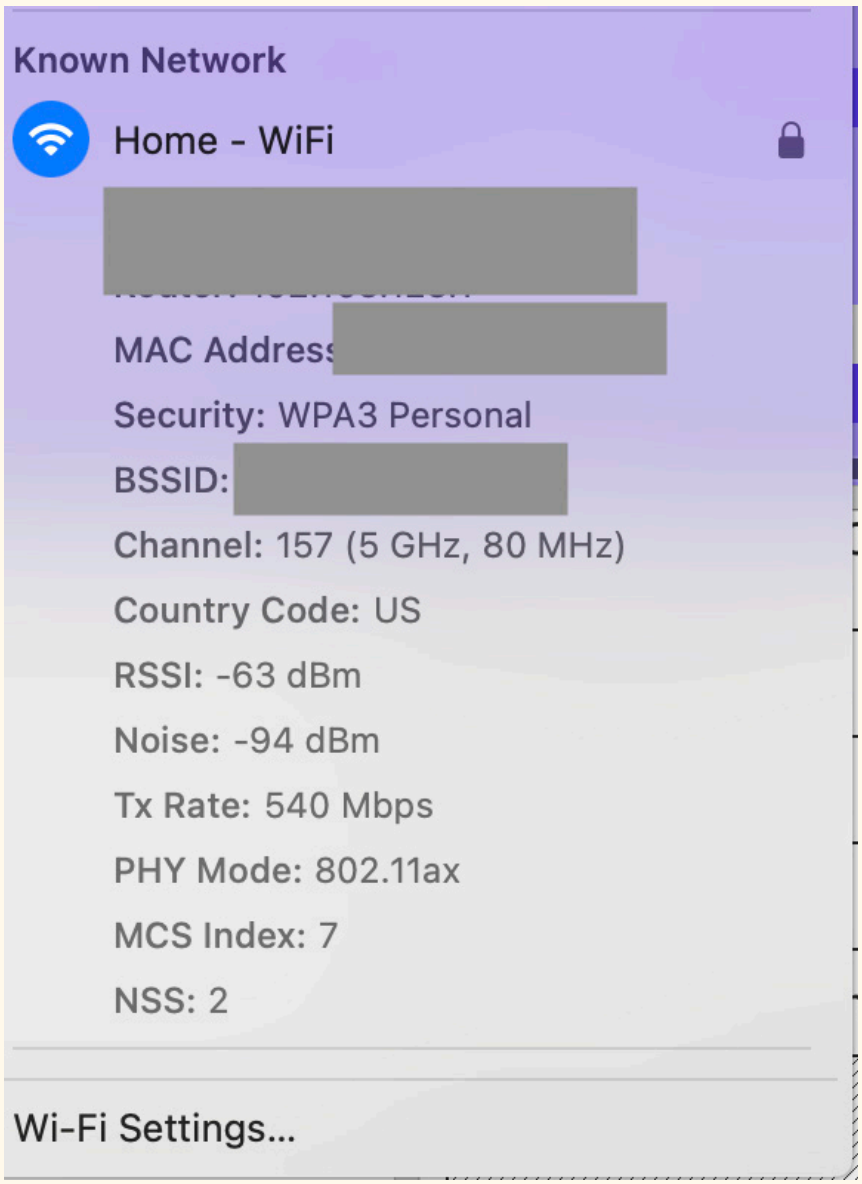
No.	Time	Transmitter	Receiver	Frame Type	Channel
323	0.264462	Eva's-MBA	Eva's-MR36	QoS Data	157
324	0.264468	Eva's-MBA	Eva's-MR36	QoS Data	157

-Frame 323 shows 0 dBm signal whereas Frame 324 shows -42 dBm signal

```
> Frame 323: 325 bytes on wire (2600 bit
v Radiotap Header v0, Length 60
    Header revision: 0
    Header pad: 0
    Header length: 60
  > Present flags
    MAC timestamp: 4042444298
  > Flags: 0x14
    Channel frequency: 5785 [5 GHz 157]
  > Channel flags: 0x0140, Orthogonal Fr
    Antenna signal: 0 dBm
    Antenna noise: -93 dBm
    Antenna: 1
```

```
> Frame 324: 157 bytes on wire (1256 bi
v Radiotap Header v0, Length 58
    Header revision: 0
    Header pad: 0
    Header length: 58
  > Present flags
    MAC timestamp: 4042444298
  > Flags: 0x14
    Channel frequency: 5785 [5 GHz 157]
  > Channel flags: 0x0140, Orthogonal F
    Antenna signal: -42 dBm
    Antenna noise: -93 dBm
    Antenna: 1
```

UI Perspective



-I suspect Frame 324 is closer to reality.

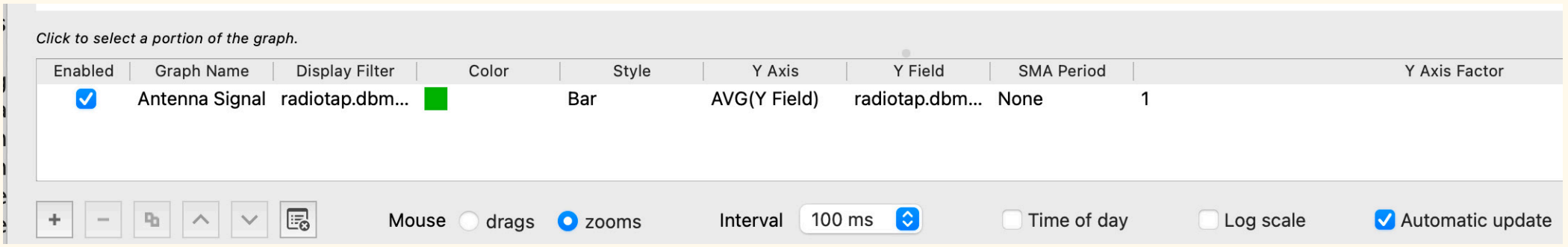
According to Opt + Click on the Wi-Fi icon, it still seems off at -63 dBm.

Is there a better way?

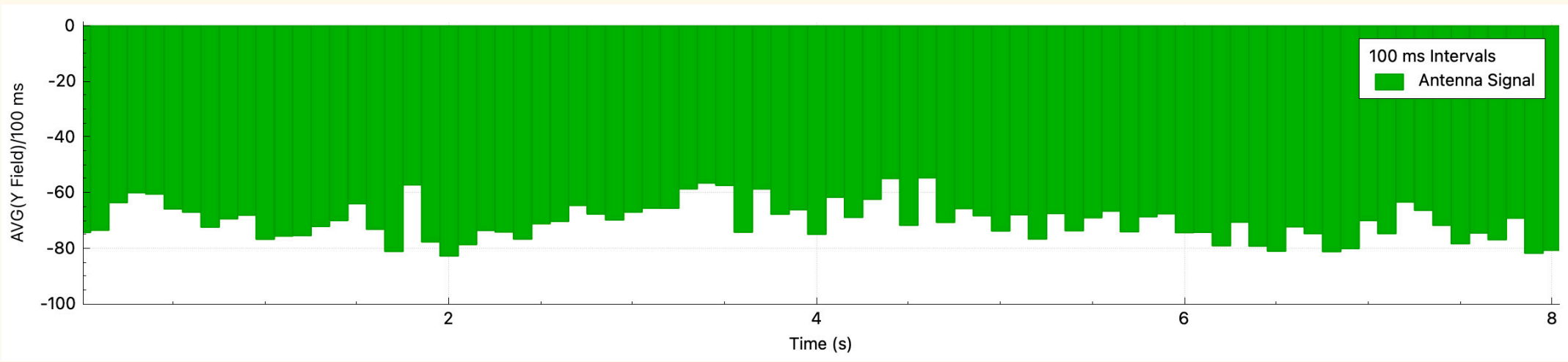
I/O Graph

-In Wireshark, go to Statistics -> I/O Graph

-Set a graph as shown:



-Even for a short time period, signal strength varies greatly each frame.



Add as Column

-I can also add the antenna signal value as a column:

Time	Transmitter	Receiver	Antenna signal
18.891676	Eva's-MBA	Eva's-MR36	-43 dBm
18.891710	Eva's-MBA	Eva's-MR36	0 dBm
18.891723	Eva's-MBA	Eva's-MR36	-62 dBm
18.891739	Eva's-MBA	Eva's-MR36	0 dBm
18.891752	Eva's-MBA	Eva's-MR36	-42 dBm
18.891781	Eva's-MBA	Eva's-MR36	-43 dBm
18.891823	Eva's-MBA	Eva's-MR36	-43 dBm
18.891855	Eva's-MBA	Eva's-MR36	-43 dBm
18.898079	Eva's-MBA	Eva's-MR36	-43 dBm
18.909482	Eva's-MBA	Eva's-MR36	-43 dBm
18.909518	Eva's-MBA	Eva's-MR36	-43 dBm

-However, instances where the driver fails to capture the signal strenghth do occur. (0 dBm readings)

Takeaways

-RSSI readings from the client device UI have more steady measurements than directly from driver readings.

-Radiotap headers still help gauge RF quality from various perspecives (AP capture, client capture, 3rd party devices)

-Take larger samples than individual frames

Sources/Credits

-https://wifinigel.blogspot.com/2013/11/what-are-radiotap-headers.html

-https://www.radiotap.org/

This post has been designed using resources from Flaticon.com (Artist: Freepik, vectorspoint)