Wireshark

Install

> *brew install wireshark*

Monitoring DNS activity

Using tcpdump

> *sudo tcpdump port 53*

```
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
12:27:52.082198 IP macbook-work-john.jmehan.com.54756 > pihole.jmehan.com.domain: 48879+ [1au] TXT? debug.
opendns.com. (46)
12:27:52.083731 IP macbook-work-john.jmehan.com.58540 > pihole.jmehan.com.domain: 27053+ PTR? 103.1.168.192.in-
addr.arpa. (44)
12:27:52.105710 IP pihole.jmehan.com.domain > macbook-work-john.jmehan.com.58540: 27053* 1/0/0 PTR macbook-work-
john.jmehan.com. (86)
12:27:52.106758 IP macbook-work-john.jmehan.com.55467 > pihole.jmehan.com.domain: 54939+ PTR? 51.1.168.192.in-
addr.arpa. (43)
12:27:52.108117 IP pihole.jmehan.com.domain > macbook-work-john.jmehan.com.55467: 54939* 1/0/0 PTR pihole.
jmehan.com. (74)
12:27:52.125754 IP pihole.jmehan.com.domain > macbook-work-john.jmehan.com.54756: 48879 0/1/1 (92)
```

Using WireShark

> *sudo tshark port 53*

```
Capturing on 'Wi-Fi: en0'
    1   0.000000 192.168.1.103  192.168.1.51 DNS 88 Standard query 0xbeef TXT debug.opendns.com OPT
    2   0.002039 192.168.1.51  192.168.1.103 DNS 93 Standard query response 0xbeef TXT debug.opendns.com A
0.0.0.0
    3  10.029922 192.168.1.103  192.168.1.51 DNS 88 Standard query 0xbeef TXT debug.opendns.com OPT
    4  10.052718 192.168.1.51  192.168.1.103 DNS 93 Standard query response 0xbeef TXT debug.opendns.com A
0.0.0.0
    5  15.225558 192.168.1.103  192.168.1.51 DNS 77 Standard query 0xf12b A pihole.jmehan.com
    6  15.226956 192.168.1.51  192.168.1.103 DNS 93 Standard query response 0xf12b A pihole.jmehan.com A
192.168.1.51
    7  20.130287 192.168.1.103  192.168.1.51 DNS 88 Standard query 0xbeef TXT debug.opendns.com OPT
    8  20.131470 192.168.1.51  192.168.1.103 DNS 93 Standard query response 0xbeef TXT debug.opendns.com A
0.0.0.0
    9  30.159960 192.168.1.103  192.168.1.51 DNS 88 Standard query 0xbeef TXT debug.opendns.com OPT
   10  30.161476 192.168.1.51  192.168.1.103 DNS 93 Standard query response 0xbeef TXT debug.opendns.com A
0.0.0.0
```

Using the Wireshark App