

Wireshark

- [Install](#)
- [Monitoring DNS activity](#)

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.jmeha.com
6 15.226956 192.168.1.51 192.168.1.103 DNS 93 Standard query response 0xf12b A pihole.jmeha.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

Capturing from Wi-Fi: en0 and Thunderbolt 1: en1

dns

No.	Time	Source	Destination	Protocol	Length	Info
1	0...	10.10.1.6	10.10.1.1	DNS	70	Standard query 0x5b55 A google.com
2	0...	10.10.1.1	10.10.1.6	DNS	86	Standard query response 0x5b55 A google.com A 216.58.211.206

▶ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Apple_21:75:a2 (80:e6:50:21:75:a2), Dst: Cisco-Li_ff:4d:b2 (00:1c:10:ff:4d:b2)
▶ Internet Protocol Version 4, Src: 10.10.1.6, Dst: 10.10.1.1
▶ User Datagram Protocol, Src Port: 60631 (60631), Dst Port: 53 (53)
▶ Domain Name System (query)

0000 00 1c 10 ff 4d b2 80 e6 50 21 75 a2 08 00 45 00 ...M... P!u...E.
0010 00 38 4c 56 00 00 40 11 18 45 0a 0a 01 06 0a 0a .8LV..@. .E.....
0020 01 01 ec d7 00 35 00 24 8d 70 5b 55 01 00 00 015.\$.p!U....
0030 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6fg oogle.co
0040 6d 00 00 01 00 01 m.....

Packets: 192 - Displayed: 2 (1.0%) Profile: Default