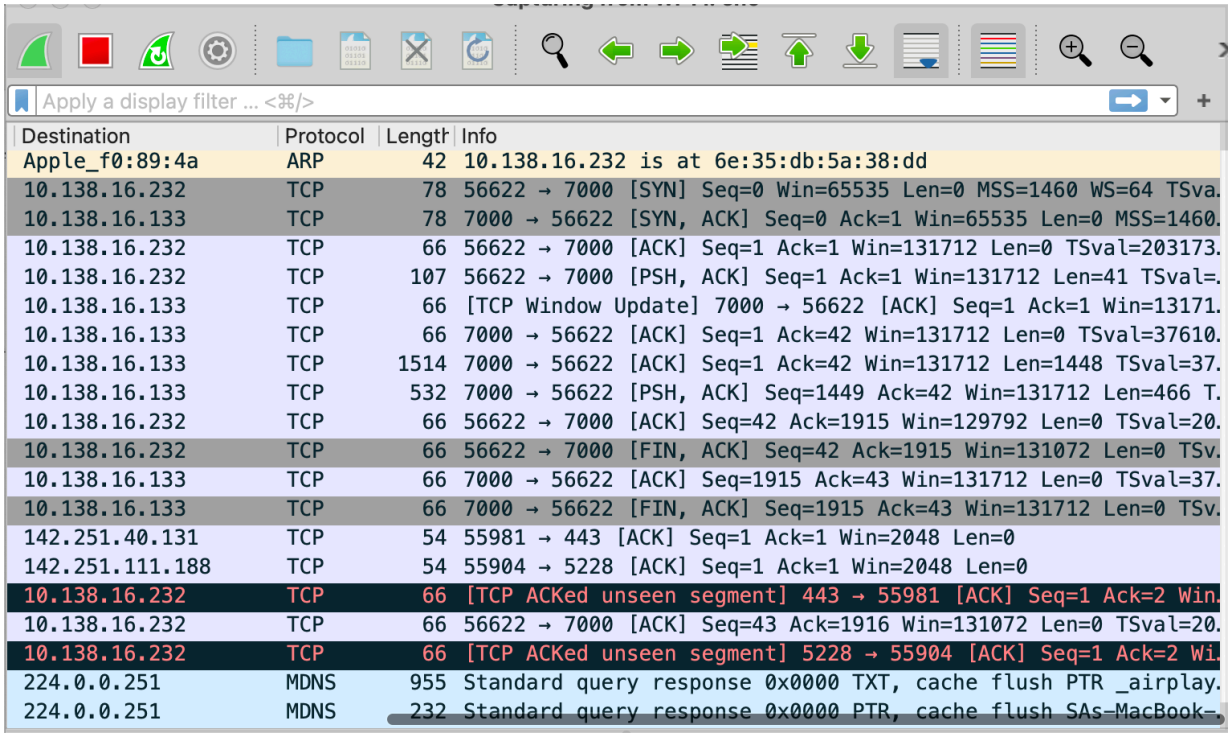
Network Protocol & Traffic Analysis

A:

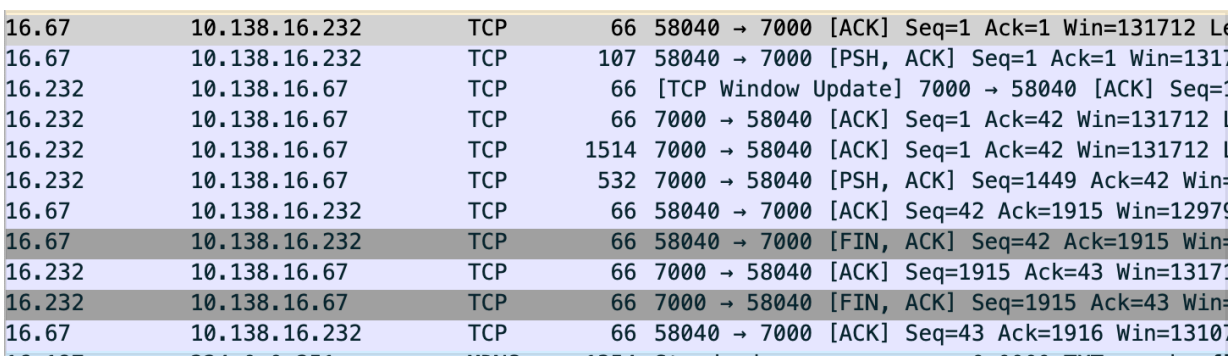


Apply a display filter ... <⌘/>

Destination	Protocol	Length	Info
Apple_f0:89:4a	ARP	42	10.138.16.232 is at 6e:35:db:5a:38:dd
10.138.16.232	TCP	78	56622 → 7000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSva.
10.138.16.133	TCP	78	7000 → 56622 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460.
10.138.16.232	TCP	66	56622 → 7000 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=203173.
10.138.16.232	TCP	107	56622 → 7000 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=41 TSval=.
10.138.16.133	TCP	66	[TCP Window Update] 7000 → 56622 [ACK] Seq=1 Ack=1 Win=13171.
10.138.16.133	TCP	66	7000 → 56622 [ACK] Seq=1 Ack=42 Win=131712 Len=0 TSval=37610.
10.138.16.133	TCP	1514	7000 → 56622 [ACK] Seq=1 Ack=42 Win=131712 Len=1448 TSval=37.
10.138.16.133	TCP	532	7000 → 56622 [PSH, ACK] Seq=1449 Ack=42 Win=131712 Len=466 T.
10.138.16.232	TCP	66	56622 → 7000 [ACK] Seq=42 Ack=1915 Win=129792 Len=0 TSval=20.
10.138.16.232	TCP	66	56622 → 7000 [FIN, ACK] Seq=42 Ack=1915 Win=131072 Len=0 TSv.
10.138.16.133	TCP	66	7000 → 56622 [ACK] Seq=1915 Ack=43 Win=131712 Len=0 TSval=37.
10.138.16.133	TCP	66	7000 → 56622 [FIN, ACK] Seq=1915 Ack=43 Win=131712 Len=0 TSv.
142.251.40.131	TCP	54	55981 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
142.251.111.188	TCP	54	55904 → 5228 [ACK] Seq=1 Ack=1 Win=2048 Len=0
10.138.16.232	TCP	66	[TCP ACKed unseen segment] 443 → 55981 [ACK] Seq=1 Ack=2 Win.
10.138.16.232	TCP	66	56622 → 7000 [ACK] Seq=43 Ack=1916 Win=131072 Len=0 TSval=20.
10.138.16.232	TCP	66	[TCP ACKed unseen segment] 5228 → 55904 [ACK] Seq=1 Ack=2 Wi.
224.0.0.251	MDNS	955	Standard query response 0x0000 TXT, cache flush PTR _airplay.
224.0.0.251	MDNS	232	Standard query response 0x0000 PTR, cache flush SAs-MacBook-.

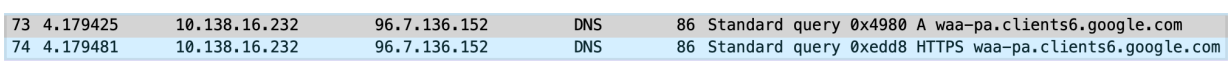
*Captured a Wireshark traffic

B:



16.67	10.138.16.232	TCP	66	58040 → 7000 [ACK] Seq=1 Ack=1 Win=131712 Le
16.67	10.138.16.232	TCP	107	58040 → 7000 [PSH, ACK] Seq=1 Ack=1 Win=1317
16.232	10.138.16.67	TCP	66	[TCP Window Update] 7000 → 58040 [ACK] Seq=1
16.232	10.138.16.67	TCP	66	7000 → 58040 [ACK] Seq=1 Ack=42 Win=131712 L
16.232	10.138.16.67	TCP	1514	7000 → 58040 [ACK] Seq=1 Ack=42 Win=131712 L
16.232	10.138.16.67	TCP	532	7000 → 58040 [PSH, ACK] Seq=1449 Ack=42 Win=
16.67	10.138.16.232	TCP	66	58040 → 7000 [ACK] Seq=42 Ack=1915 Win=1297
16.67	10.138.16.232	TCP	66	58040 → 7000 [FIN, ACK] Seq=42 Ack=1915 Win=
16.232	10.138.16.67	TCP	66	7000 → 58040 [ACK] Seq=1915 Ack=43 Win=1317
16.232	10.138.16.67	TCP	66	7000 → 58040 [FIN, ACK] Seq=1915 Ack=43 Win=
16.67	10.138.16.232	TCP	66	58040 → 7000 [ACK] Seq=43 Ack=1916 Win=1310

**Filtered TCP Traffic



73	4.179425	10.138.16.232	96.7.136.152	DNS	86 Standard query 0x4980 A waa-pa.clients6.google.com
74	4.179481	10.138.16.232	96.7.136.152	DNS	86 Standard query 0xedd8 HTTPS waa-pa.clients6.google.com

** Filtered DNS Traffic

C:

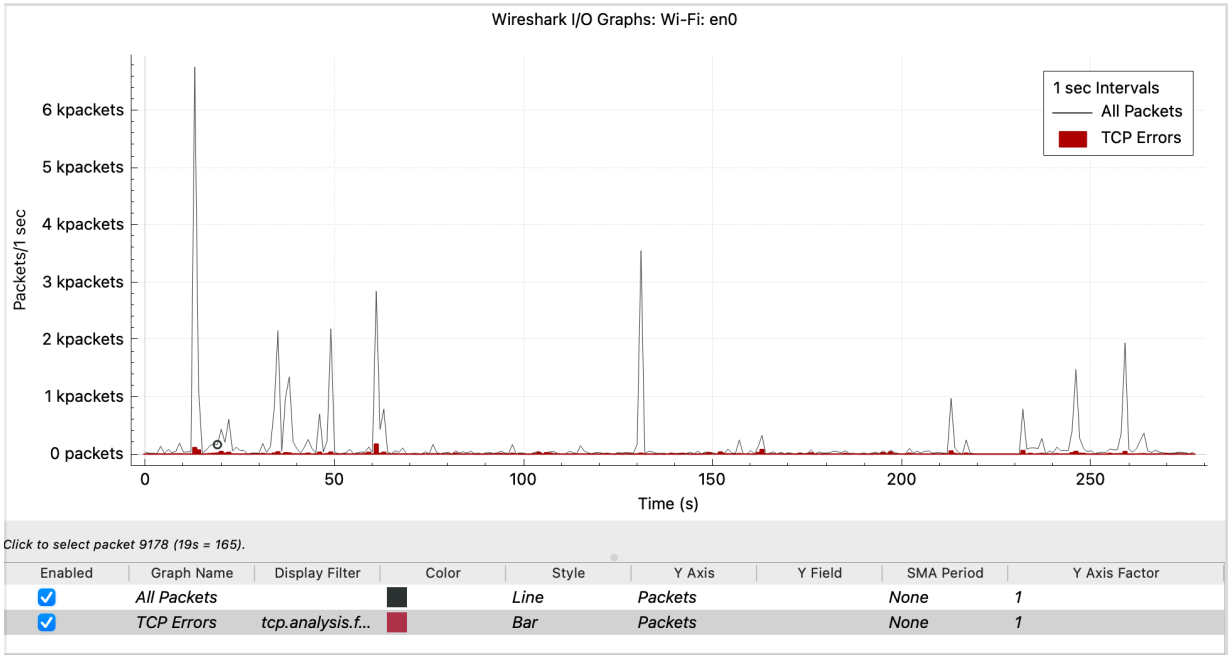
```
justin@Justins-MacBook-Pro ~ % nmap -sV -p 23 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 17:12 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s latency).

PORT   STATE  SERVICE VERSION
23/tcp closed telnet

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
justin@Justins-MacBook-Pro ~ %
```

Telnet sends data in plaintext and is vulnerable to eavesdropping.

D:



A spike in traffic was observed when the initial connection occurs (TCP handshake).

E:

There are no SYN Packets. The network is safe

F:

We captured Tcp and DNS. There were no vulnerabilties were found. There is no suspicious activities.