

Homework 2

1. 3 different protocols: TCP, UDP, ARP

(a) TCP, UDP → transport layer

(pass segments and destination address to network)

→ TCP

- breaks long message into shorter segments

- guaranteed delivery of application-layer messages

→ UDP

- provides connectionless service to its applications

(b) ARP → network layer

The Wireshark interface is shown capturing traffic from Wi-Fi interface en0. The main pane lists 282 total packets, with 282 displayed. The selected packet (No. 3) is a TCP segment (Seq=64, Ack=1, Len=0) between 17.248.223.5 and 192.168.0.14. The bottom pane shows the raw bytes (hex and ASCII) of this selected packet.

| No. | Time | Source | Destination | Protocol | length | Info |
|-----|-----------|-------------------|-------------------|----------|--------|--|
| 1 | 0.000000 | 17.248.223.5 | 192.168.0.14 | TLSv1... | 105 | Application Data |
| 2 | 0.000002 | 17.248.223.5 | 192.168.0.14 | TLSv1... | 90 | Application Data |
| 3 | 0.000003 | 17.248.223.5 | 192.168.0.14 | TCP | 66 | 443 → 51549 [FIN, ACK] Seq=64 Ack=1 Win=1768 Len=0 TStamp=1910782587 TSectr=2595467658 |
| 4 | 0.000381 | 192.168.0.14 | 17.248.223.5 | TCP | 66 | 51549 → 443 [ACK] Seq=1 Ack=64 Win=2047 Len=0 TStamp=2595497561 TSectr=1910782587 |
| 5 | 0.000388 | 192.168.0.14 | 17.248.223.5 | TCP | 66 | 51549 → 443 [ACK] Seq=1 Ack=65 Win=2047 Len=0 TStamp=2595497561 TSectr=1910782587 |
| 6 | 0.000770 | 192.168.0.14 | 17.248.223.5 | TLSv1... | 105 | Application Data |
| 7 | 0.001546 | 192.168.0.14 | 17.248.223.5 | TLSv1... | 90 | Application Data |
| 8 | 0.001772 | 192.168.0.14 | 17.248.223.5 | TCP | 66 | 51549 → 443 [FIN, ACK] Seq=64 Ack=65 Win=2048 Len=0 TStamp=2595497563 TSectr=1910782587 |
| 9 | 0.051004 | 17.248.223.5 | 192.168.0.14 | TCP | 66 | [TCP Retransmission] 443 → 51549 [FIN, ACK] Seq=64 Ack=1 Win=1768 Len=0 TStamp=1910782725 TSectr=2595467 |
| 10 | 0.051186 | 192.168.0.14 | 17.248.223.5 | TCP | 66 | [TCP Retransmission] 51549 → 443 [FIN, ACK] Seq=64 Ack=65 Win=2048 Len=0 TStamp=2595497612 TSectr=191078 |
| 11 | 0.058161 | 17.248.223.5 | 192.168.0.14 | TCP | 66 | 443 → 51549 [ACK] Seq=65 Ack=40 Win=1768 Len=0 TStamp=1910782730 TSectr=2595497561 |
| 12 | 0.058162 | 17.248.223.5 | 192.168.0.14 | TCP | 66 | 443 → 51549 [RST, ACK] Seq=65 Ack=40 Win=1768 Len=0 TStamp=1910782730 TSectr=2595497561 |
| 13 | 0.058162 | 17.248.223.5 | 192.168.0.14 | TCP | 54 | 443 → 51549 [RST] Seq=65 Win=0 Len=0 |
| 14 | 0.058162 | 17.248.223.5 | 192.168.0.14 | TCP | 54 | 443 → 51549 [RST] Seq=65 Win=0 Len=0 |
| 15 | 0.086847 | 17.248.223.5 | 192.168.0.14 | TCP | 54 | 443 → 51549 [RST] Seq=65 Win=0 Len=0 |
| 16 | 4.002015 | 192.168.0.14 | 17.250.122.134 | UDP | 71 | 49742 → 443 Len=29 |
| 17 | 4.070419 | 17.250.122.134 | 192.168.0.14 | UDP | 75 | 443 → 49742 Len=33 |
| 18 | 4.353875 | 192.168.0.14 | 17.250.122.133 | UDP | 83 | 59147 → 443 Len=41 |
| 19 | 4.397200 | 17.250.122.133 | 192.168.0.14 | UDP | 73 | 443 → 59147 Len=31 |
| 20 | 7.397401 | 192.168.0.14 | 17.250.122.133 | UDP | 71 | 59147 → 443 Len=29 |
| 21 | 7.468083 | 17.250.122.133 | 192.168.0.14 | UDP | 75 | 443 → 59147 Len=33 |
| 22 | 9.810795 | 192.168.0.14 | 17.250.122.134 | UDP | 83 | 49742 → 443 Len=41 |
| 23 | 9.856465 | 17.250.122.134 | 192.168.0.14 | UDP | 73 | 443 → 49742 Len=31 |
| 24 | 10.141021 | ZioncomE_83:00:64 | Apple_6:a:c:f:59 | ARP | 42 | Who has 192.168.0.14? Tell 192.168.0.1 |
| 25 | 10.141096 | Apple_6:a:c:f:59 | ZioncomE_83:00:64 | ARP | 42 | 192.168.0.14 is at a4:83:e7:6:a:c:f:59 |
| 26 | 20.588280 | 13.114.154.168 | 192.168.0.14 | TLSv1... | 105 | Application Data |
| 27 | 20.597922 | 192.168.0.14 | 13.114.154.168 | TCP | 66 | 51503 → 443 [ACK] Seq=1 Ack=40 Win=2047 Len=0 TStamp=1978665750 TSectr=745594942 |
| 28 | 20.599021 | 192.168.0.14 | 13.114.154.168 | TLSv1... | 105 | Application Data |
| 29 | 20.599021 | 192.168.0.14 | 13.114.154.168 | TLSv1... | 00 | Application Data |

> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: ZioncomE_83:00:64 (40:ee:15:83:00:64), Dst: Apple_6:a:c:f:59 (a4:83:e7:6:a:c:f:59)
> Internet Protocol Version 4, Src: 17.248.223.5, Dst: 192.168.0.14
> Transmission Control Protocol, Src Port: 443, Dst Port: 51549, Seq: 64, Ack: 1, Len: 0

0000 a4 83 e7 6a cf 59 40 ee 15 83 00 64 08 00 45 00 ...j.Y@...d.E-
0010 00 34 95 44 40 00 30 06 03 cc 1f f8 df 05 c0 a8 .4.D@.0...]
0020 00 0e 01 bb c9 5d 4a 6c 0c df ae 38 b8 80 11

0030 06 e8 3c 43 00 00 01 01 08 0a 71 e4 3a 7b 9a b3 ..<C...q:{...
0040 b1 8a

different
protocol
types

2. ARP protocol - Ethernet 和 IP 地址的轉換

- host 要找另一個 host 時，會用 broadcast 發出一個 ARP query (查詢)
而 ARP query 中包含了想查詢的 IP，又：是 broadcast，所以網段中
所有 host 都會收到，但只有符合 IP 的 host 收到後會回覆。
包含它自己的 MAC Address。而查詢方會把 MAC Address 紀錄到
ARP Table 中。

Method to find ARP in wireshark

1. choose the interface(s) you want to capture

2. type "arp" in the display filter

3. you can find out ARP packets of the interface(s)

arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|--------|-----------|-------------------|-------------------|----------|--------|---|
| 1437 | 11.848190 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.107.247? Tell 172.18.106.123 |
| 1482 | 12.138284 | 8e:50:b3:0b:aa:b4 | Apple_6a:cf:59 | ARP | 42 | 172.18.107.247 is at 8e:50:b3:0b:aa:b4 |
| 1989 | 17.967999 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.107.235? Tell 172.18.106.123 |
| 1990 | 17.974265 | 3e:bf:82:6f:9e:a5 | Apple_6a:cf:59 | ARP | 42 | 172.18.107.235 is at 3e:bf:82:6f:9e:a5 |
| 2613 | 21.313488 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.105.250? Tell 172.18.106.123 |
| 2618 | 21.334139 | 1e:f1:4e:1b:d0:fc | Apple_6a:cf:59 | ARP | 56 | 172.18.105.250 is at 1e:f1:4e:1b:d0:fc |
| 3074 | 24.468163 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.108.63? Tell 172.18.106.123 |
| 3084 | 24.492568 | 36:86:09:0a:b4:da | Apple_6a:cf:59 | ARP | 42 | 172.18.108.63 is at 36:86:09:0a:b4:da |
| 3689 | 28.782344 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.108.80? Tell 172.18.106.123 |
| 3690 | 28.797812 | 0a:1e:43:14:79:29 | Apple_6a:cf:59 | ARP | 42 | 172.18.108.80 is at 0a:1e:43:14:79:29 |
| 6058 | 45.550587 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.104.21? Tell 172.18.106.123 |
| 6061 | 45.561020 | Apple_8c:85:51 | Apple_6a:cf:59 | ARP | 42 | 172.18.104.21 is at f8:4d:89:8c:85:51 |
| 6279 | 47.542422 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.109.42? Tell 172.18.106.123 |
| 6280 | 47.880147 | 92:77:2f:0c:28:0e | Apple_6a:cf:59 | ARP | 42 | 172.18.109.42 is at 92:77:2f:0c:28:0e |
| 8330 | 62.030644 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.106.129? Tell 172.18.106.123 |
| 8333 | 62.037394 | e2:f1:a8:8c:96:87 | Apple_6a:cf:59 | ARP | 42 | 172.18.106.129 is at e2:f1:a8:8c:96:87 |
| 8392 | 62.130764 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.106.89? Tell 172.18.106.123 |
| 8393 | 62.254028 | ee:0d:c9:1f:da:55 | Apple_6a:cf:59 | ARP | 42 | 172.18.106.89 is at ee:0d:c9:1f:da:55 |
| 8952 | 66.146035 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.106.114? Tell 172.18.106.123 |
| 8973 | 66.193075 | 26:69:ea:60:eb:83 | Apple_6a:cf:59 | ARP | 42 | 172.18.106.114 is at 26:69:ea:60:eb:83 |
| 9459 | 69.913785 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.108.67? Tell 172.18.106.123 |
| 9492 | 69.963370 | babf:a4:f3:66:7c | Apple_6a:cf:59 | ARP | 42 | 172.18.108.67 is at babf:a4:f3:66:7c |
| 113... | 77.234037 | Apple_6a:cf:59 | Broadcast | ARP | 42 | Who has 172.18.110.105? Tell 172.18.106.123 |
| 113... | 77.248581 | d2:2d:b9:d1:49:9b | Apple_6a:cf:59 | ARP | 56 | 172.18.110.105 is at d2:2d:b9:d1:49:9b |
| 113... | 77.647931 | JuniperN_56:41:f0 | Apple_6a:cf:59 | ARP | 60 | 172.18.111.254 is at 58:00:bb:56:41:f0 |
| 119... | 80.329106 | 66:ab:da:c9:bf:c1 | Apple_6a:cf:59 | ARP | 56 | Who has 172.18.106.123? Tell 172.18.111.234 |
| 119... | 80.329201 | Apple_6a:cf:59 | 66:ab:da:c9:bf:c1 | ARP | 42 | 172.18.106.123 is at a4:83:e7:6a:cf:59 |
| 119... | 80.360865 | 66:19:f6:78:64:2e | Apple_6a:cf:59 | ARP | 56 | Who has 172.18.106.123? Tell 172.18.108.72 |

Frame 1437: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0

Ethernet II, Src: Apple_6a:cf:59 (a4:83:e7:6a:cf:59), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff) 目的位址,广播位址

> Source: Apple_6a:cf:59 (a4:83:e7:6a:cf:59) 來源位址

Type: ARP (0x0806) ARP封包 48 bits

Address Resolution Protocol (request)

Hardware type: Ethernet (Ethernet 網路介面)

Protocol type: IPv4 (0x0800) IP protocol

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)

Sender IP address: 172.18.106.123

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 172.18.107.247

ARP request封包標頭

Ethernet II 封包標頭

由主機發送出去 ARP request 封包

Packets: 36562 · Displayed: 75 (0.2%)

Profile: Default

點開想分析的 packet，即可看到它的內容

ex. 點開 No. 1437 packet

3. ICMP protocol → 解析封包或分析路由 (藉由回傳的錯誤訊息分析)

① generate errors to share with the sending device in the event that any of the data didn't get to the destination.

② perform network diagnostic

Method to find ICMP in wireshark

1. choose the interface(s) you want to capture

2. open the terminal in your computer

3. type "ping 8.8.8.8" in command line

4. go back to wireshark and type "icmp" in the display filter

5. you can find out ICMP packets of the interface(s)

The screenshot shows the Wireshark interface capturing from Wi-Fi interface en0. A red circle highlights the 'icmp' display filter in the top bar. A pink box labeled 'terminal (after step 3.)' covers the bottom right of the interface list. The interface list shows many ICMP echo requests and replies between 172.18.106.123 and 8.8.8.8.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|----------|----------------|----------------|----------|--------|---|
| 39 | 0.207102 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=60/15360, ttl=64 (reply in 75) |
| 75 | 0.243796 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=60/15360, ttl=60 (request in 39) |
| 375 | 1.207643 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=61/15616, ttl=64 (reply in 376) |
| 376 | 1.213976 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=61/15616, ttl=60 (request in 375) |
| 717 | 2.212986 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=62/15872, ttl=64 (reply in 718) |
| 718 | 2.222132 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=62/15872, ttl=60 (request in 717) |
| 1043 | 3.217730 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=63/16128, ttl=64 (reply in 1044) |
| 1044 | 3.233996 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=63/16128, ttl=60 (request in 1043) |
| 1261 | 4.220751 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=64/16384, ttl=64 (reply in 1276) |
| 1276 | 4.232400 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=64/16384, ttl=60 (request in 1261) |
| 1643 | 5.224141 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=65/16640, ttl=64 (reply in 1677) |
| 1677 | 5.239529 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=65/16640, ttl=60 (request in 1643) |
| 1962 | 6.227701 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=66/16896, ttl=64 (reply in 1968) |
| 1968 | 6.244628 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=66/16896, ttl=60 (request in 1962) |
| 2314 | 7.232205 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=67/17152, ttl=64 (reply in 2315) |
| 2315 | 7.244792 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=67/17152, ttl=60 (request in 2314) |
| 2574 | 8.235484 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=68/17312, ttl=64 (reply in 2575) |
| 2575 | 8.249761 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=68/17312, ttl=60 (request in 2574) |
| 2854 | 9.240468 | 172.18.106.123 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x372c, seq=69/17472, ttl=64 (reply in 2855) |
| 2855 | 9.248096 | 8.8.8.8 | 172.18.106.123 | ICMP | 102 | Echo (ping) reply id=0x372c, seq=69/17472, ttl=60 (request in 2854) |

terminal (after step 3.)

The terminal window shows the command "candy - ping 8.8.8.8 - 80x24" was run, resulting in 80 ICMP echo requests sent to 8.8.8.8.

The Wireshark interface list shows many ICMP echo requests and replies between 172.18.106.123 and 8.8.8.8.

和ARP相比沒有 "source" & "destination" 的 port numbers

① ICMP是用來交換 network layer 中 host 和 router 間的訊息

非 application layer process

② 每一個 ICMP封包都有 "type" 和 "code", 結合這兩者就可识别訊息

∴ 就不用 port 去指示

Homework 3

1. HTTP Packet Counter statistics

The screenshot shows the Wireshark interface with the following details:

- Left Pane (Frame List):** Shows 209 frames captured on interface en0. The selected frame is frame 209, which is highlighted in yellow.
- Right Pane (Details View):** Frame 209 details:
 - Capture File Properties:** Source 17.248.1b4.114, Destination 192.168.0.1, Time 1b / 1.1/8145.
 - Resolved Addresses:** 17.248.1b4.114, 192.168.0.1.
 - Protocol Hierarchy:** TCP > IP > Ethernet.
 - Conversations:** 17.248.164.114 ↔ 192.168.0.1.
 - Endpoints:** 17.248.164.114, 192.168.0.1.
 - Packet Lengths:** 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface en0, id 0.
 - I/O Graphs:** 17.248.164.114 ↔ 192.168.0.1.
 - Service Response Time:** 17.248.164.114 ↔ 192.168.0.1.
- Bottom Status Bar:** Packets: 2260 - Displayed: 2260 (100.0%) | Profile: Default

6

Choose statistics → HTTP → Packet Counter

| Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start |
|-----------------------|-------|---------|---------|---------|-----------|---------|------------|-------------|
| Total HTTP Packets | 8 | 0.0001 | 100% | 0.0200 | 2.184 | | | |
| Other HTTP Packets | 0 | 0.0000 | 0.00% | - | - | | | |
| HTTP Response Packets | 4 | 0.0000 | 50.00% | 0.0100 | 2.191 | | | |
| ???: broken | 0 | 0.0000 | 0.00% | - | - | | | |
| 5xx: Server Error | 0 | 0.0000 | 0.00% | - | - | | | |
| 4xx: Client Error | 0 | 0.0000 | 0.00% | - | - | | | |
| 3xx: Redirection | 0 | 0.0000 | 0.00% | - | - | | | |
| 2xx: Success | 4 | 0.0000 | 100.00% | 0.0100 | 2.191 | | | |
| 200 OK | 4 | 0.0000 | 100.00% | 0.0100 | 2.191 | | | |
| 1xx: Informational | 0 | 0.0000 | 0.00% | - | - | | | |
| HTTP Request Packets | 4 | 0.0000 | 50.00% | 0.0100 | 2.184 | | | |
| GET | 2 | 0.0000 | 50.00% | 0.0100 | 129.568 | | | |
| CONNECT | 2 | 0.0000 | 50.00% | 0.0100 | 2.184 | | | |

2. QUIC benefits

(1) Reduce connection establishment latency

QUIC: a single handshake to establish a secure session

(2) Multiplexing without head-of-line blocking

QUIC: 多路複用

(在同一個連線中進行多個 stream 的傳輸, ∵ 某一個 stream 中的 packet 遺失時, 其他 stream 仍可正常傳輸)

3. add constrain to filter (!ip && !ipv6)

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|-------------------|-------------------|----------|--------|--|
| 810 | 57.855690 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | Who has 192.168.0.14? Tell 192.168.0.1 |
| 811 | 57.855756 | Apple_6a:cf:59 | ZioncomE_83:00:64 | ARP | 42 | 192.168.0.14 is at a4:83:e7:6a:cf:59 |
| 851 | 65.392029 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | 192.168.0.1 is at 40:ee:15:83:00:64 |
| 931 | 114.674735 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | Who has 192.168.0.14? Tell 192.168.0.1 |
| 932 | 114.674810 | Apple_6a:cf:59 | ZioncomE_83:00:64 | ARP | 42 | 192.168.0.14 is at a4:83:e7:6a:cf:59 |
| 2141 | 155.357324 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | 192.168.0.1 is at 40:ee:15:83:00:64 |
| 2150 | 167.033841 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | Who has 192.168.0.14? Tell 192.168.0.1 |
| 2157 | 167.033917 | Apple_6a:cf:59 | ZioncomE_83:00:64 | ARP | 42 | 192.168.0.14 is at a4:83:e7:6a:cf:59 |
| 2257 | 209.664835 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | Who has 192.168.0.14? Tell 192.168.0.1 |
| 2258 | 209.664874 | Apple_6a:cf:59 | ZioncomE_83:00:64 | ARP | 42 | 192.168.0.14 is at a4:83:e7:6a:cf:59 |
| 2341 | 245.373895 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | 192.168.0.1 is at 40:ee:15:83:00:64 |
| 6014 | 253.664523 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | Who has 192.168.0.14? Tell 192.168.0.1 |
| 6015 | 253.664572 | Apple_6a:cf:59 | ZioncomE_83:00:64 | ARP | 42 | 192.168.0.14 is at a4:83:e7:6a:cf:59 |
| 8008 | 297.077958 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | Who has 192.168.0.14? Tell 192.168.0.1 |
| 8009 | 297.078014 | Apple_6a:cf:59 | ZioncomE_83:00:64 | ARP | 42 | 192.168.0.14 is at a4:83:e7:6a:cf:59 |
| 8057 | 335.375611 | ZioncomE_83:00:64 | Apple_6a:cf:59 | ARP | 42 | 192.168.0.1 is at 40:ee:15:83:00:64 |

> Frame 810: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
Internet Protocol Version 6: Protocol

Packets: 8092 - Displayed: 16 (0.2%)

Profile: Default

4. (1) TTL:

represents the amount of time when the packet is floating on a network

(2)

The screenshot shows a list of TCP packets captured on interface en0. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The 'Info' column provides detailed protocol analysis for each packet. For example, packet 523 shows the following details:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--|
| 519 | 12.819836 | 192.168.0.14 | 44.241.46.204 | TCP | 1514 | 59912 → 443 [ACK] Seq=34800 Ack=43 Win=2048 Len=1448 TStamp=21077476 TSecr=4165254411 [TCP segment of a ...] |
| 520 | 12.819838 | 192.168.0.14 | 44.241.46.204 | TCP | 1514 | 59912 → 443 [ACK] Seq=36256 Ack=43 Win=2048 Len=1448 TStamp=21077476 TSecr=4165254411 [TCP segment of a ...] |
| 521 | 12.865521 | 44.241.46.204 | 192.168.0.14 | TCP | 66 | 443 → 59912 [ACK] Seq=43 Ack=13088 Win=1471 Len=0 TStamp=4165254454 TSecr=21077324 |
| 522 | 12.865698 | 192.168.0.14 | 44.241.46.204 | TCP | 1514 | 59912 → 443 [ACK] Seq=37704 Ack=43 Win=2048 Len=1448 TStamp=21077522 TSecr=4165254454 [TCP segment of a ...] |
| 523 | 12.865704 | 192.168.0.14 | 44.241.46.204 | TCP | 1514 | 59912 → 443 [ACK] Seq=39152 Ack=43 Win=2048 Len=1448 TStamp=21077522 TSecr=4165254454 [TCP segment of a ...] |
| 524 | 13.186953 | 44.241.46.204 | 192.168.0.14 | TCP | 66 | 443 → 59912 [ACK] Seq=43 Ack=14536 Win=1471 Len=0 TStamp=4165254558 TSecr=21077474 |
| 525 | 13.186954 | 44.241.46.204 | 192.168.0.14 | TCP | 66 | 443 → 59912 [ACK] Seq=43 Ack=15984 Win=1471 Len=0 TStamp=4165254562 TSecr=21077476 |
| 526 | 13.186954 | 44.241.46.204 | 192.168.0.14 | TCP | 66 | 443 → 59912 [ACK] Seq=43 Ack=17432 Win=1471 Len=0 TStamp=4165254562 TSecr=21077476 |
| 527 | 13.187094 | 192.168.0.14 | 44.241.46.204 | TCP | 1514 | 59912 → 443 [ACK] Seq=40600 Ack=43 Win=2048 Len=1448 TStamp=21077843 TSecr=4165254558 [TCP segment of a ...] |
| 528 | 13.187098 | 192.168.0.14 | 44.241.46.204 | TCP | 1514 | 59912 → 443 [ACK] Seq=40600 Ack=43 Win=2048 Len=1448 TStamp=21077843 TSecr=4165254558 [TCP segment of a ...] |

Details for packet 523:

```
> Frame 523: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
> Ethernet II, Src: Apple_6a:c:f59 (a4:83:e7:6a:c:f59), Dst: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
  Internet Protocol Version 4, Src: 192.168.0.14, Dst: 44.241.46.204
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x02 (DS2: CS0, ECN: ECT(0))
      Total Length: 1500
      Identification: 0x0000
      Flags: 0x0000 (Don't fragment)
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0x18a7 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.0.14
      Destination Address: 44.241.46.204
    > Transmission Control Protocol, Src Port: 59912, Dst Port: 443, Seq: 39152, Ack: 43, Len: 1448
```

Choose No. 523 → Internet Protocol Version 4

Then we'll get No. 523's Time to Live = 64

5. UDP

The screenshot shows a list of QUIC packets captured on interface en0. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The 'Info' column provides detailed protocol analysis for each packet. For example, packet 1044 shows the following details:

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|----------------|----------------|----------|--------|--|
| 1044 | 129.291936 | 192.168.0.14 | 17.250.122.132 | QUIC | 1392 | Initial, DCID=ca1973d49c125fb4, SCID=a3504cd313c6f82, PKN: 0, CRYPTO, PADDING |
| 1053 | 129.329464 | 17.250.122.132 | 192.168.0.14 | QUIC | 1242 | Handshake, DCID=a3504cd313c6f82, SCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43 |
| 1055 | 129.334709 | 192.168.0.14 | 17.250.122.132 | QUIC | 156 | Handshake, DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43, SCID=a3504cd313c6f82 |
| 1056 | 129.334716 | 192.168.0.14 | 17.250.122.132 | QUIC | 1392 | Initial, DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43, SCID=a3504cd313c6f82, PKN: 1, ACK, PADDING |
| 1057 | 129.335109 | 192.168.0.14 | 17.250.122.132 | QUIC | 111 | Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43 |
| 1058 | 129.343337 | 192.168.0.14 | 17.250.122.132 | QUIC | 562 | Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43 |
| 1059 | 129.343462 | 192.168.0.14 | 17.250.122.132 | QUIC | 1388 | Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43 |
| 1060 | 129.368433 | 192.168.0.14 | 17.250.122.132 | QUIC | 164 | Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43 |
| 1061 | 129.373877 | 17.250.122.132 | 192.168.0.14 | QUIC | 915 | Protected Payload (KP0), DCID=a3504cd313c6f82 |
| 1062 | 129.373877 | 17.250.122.132 | 192.168.0.14 | QUIC | 74 | Protected Payload (KP0), DCID=a3504cd313c6f82 |

Details for packet 1044:

```
> Frame 1044: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface en0, id 0
> Ethernet II, Src: Apple_6a:c:f59 (a4:83:e7:6a:c:f59), Dst: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
  Internet Protocol Version 4, Src: 192.168.0.14, Dst: 17.250.122.132
  User Datagram Protocol, Src Port: 57829, Dst Port: 443
    Source Port: 57829
    Destination Port: 443
    Length: 1358
    Checksum: 0x1875 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 40]
    > [Timestamps]
    UDP payload (1350 bytes)
  > QUIC IETF
```

Protocol use in transport layer
→ UDP

Type "quic" in the display filter → choose anyone you like
for example choose No. 1044
→ It shows "User Datagram Protocol"

6.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|----------------|----------------|----------|--------|--|
| 438 | 12:22:51.1 | 192.168.0.14 | 17.253.117.203 | TLSv1... | 103 | Application Data |
| 844 | 62.901834 | 192.168.0.14 | 17.253.117.203 | TLSv1... | 90 | Application Data |
| 1112 | 129.568290 | 192.168.0.14 | 142.251.42.227 | HTTP | 433 | GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCggQUxy55it3%2FYTSuu1H0ri7xsAkB2MEFip0f6%2BFze6VzT2c00JGFpnxNR0nAh. |
| 1114 | 129.581286 | 142.251.42.227 | 192.168.0.14 | HTTP | 778 | Response |
| 1568 | 131.513436 | 192.168.0.14 | 142.251.42.227 | HTTP | 437 | GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCggQUxy55it3%2FYTSuu1H0ri7xsAkB2MEFip0f6%2BFze6VzT2c00JGFpnxNR0nAh. |
| 1569 | 131.513437 | 142.251.42.227 | 192.168.0.14 | HTTP | 778 | Response |
| 1913 | 141.184525 | 192.168.0.14 | 17.253.85.207 | HTTP | 219 | CONNECT proxy-safebrowsing.googleapis.com:443 HTTP/1.1 |
| 1917 | 141.285818 | 17.253.85.207 | 192.168.0.14 | HTTP | 293 | HTTP/1.1 200 OK |
| 1919 | 141.285945 | 192.168.0.14 | 17.253.85.208 | TCP | 219 | 59948 -> 80 [PSH, ACK] Seq=1 Ack=1 Win=2944 Len=153 TSval=3195349518 TSecr=1806080513 |
| 1921 | 141.287475 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 583 | Client Hello |
| 1924 | 141.313681 | 17.253.85.208 | 192.168.0.14 | TCP | 293 | HTTP/1.1 200 OK [TCP segment of a reassembled PDU] |
| 1929 | 141.389585 | 17.253.85.207 | 192.168.0.14 | TLSv1... | 1510 | Server Hello, Change Cipher Spec |
| 1934 | 141.481903 | 17.253.85.207 | 192.168.0.14 | TLSv1... | 414 | Application Data |
| 1936 | 141.491917 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 130 | Change Cipher Spec, Application Data |
| 1937 | 141.493679 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 617 | Application Data |
| 1939 | 141.564583 | 17.253.85.207 | 192.168.0.14 | TLSv1... | 680 | Application Data, Application Data |
| 1941 | 141.565353 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 97 | Application Data |
| 1943 | 141.566099 | 17.253.85.207 | 192.168.0.14 | TLSv1... | 97 | Application Data |
| 1945 | 141.578852 | 17.253.85.207 | 192.168.0.14 | TLSv1... | 533 | Application Data, Application Data, Application Data, Application Data |
| 1947 | 141.579804 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 105 | Application Data |
| 1985 | 143.265648 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 264 | Application Data |
| 1987 | 143.348086 | 17.253.85.207 | 192.168.0.14 | TLSv1... | 218 | Application Data, Application Data |
| 1988 | 143.348443 | 17.253.85.207 | 192.168.0.14 | TLSv1... | 136 | Application Data, Application Data |
| 1992 | 143.349192 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 105 | Application Data |
| 2248 | 203.669302 | 192.168.0.14 | 17.253.85.207 | TLSv1... | 90 | Application Data |
| 2395 | 249.781297 | 192.168.0.14 | 142.251.42.227 | HTTP | 435 | GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCggQUxy55it3%2FYTSuu1H0ri7xsAkB2MEFip0f6%2BFze6VzT2c00JGFpnxNR0nAh. |
| 2397 | 249.787654 | 142.251.42.227 | 192.168.0.14 | OCSP | 778 | Response |
| 3095 | 250.613175 | 192.168.0.14 | 142.251.42.227 | HTTP | 427 | GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCggQUxy55it3%2FYTSuu1H0ri7xsAkB2MEFip0f6%2BFze6VzT2c00JGFpnxNR0nAh. |
| 3100 | 250.621219 | 142.251.42.227 | 192.168.0.14 | OCSP | 777 | Response |
| 4740 | 251.653754 | 192.168.0.14 | 142.251.42.227 | HTTP | 429 | GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCggQUxy55it3%2FYTSuu1H0ri7xsAkB2MEFip0f6%2BFze6VzT2c00JGFpnxNR0nAh. |
| 4741 | 251.659888 | 142.251.42.227 | 192.168.0.14 | OCSP | 777 | Response |
| 4904 | 251.853510 | 192.168.0.14 | 142.251.42.227 | HTTP | 429 | GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCggQUxy55it3%2FYTSuu1H0ri7xsAkB2MEFip0f6%2BFze6VzT2c00JGFpnxNR0nAh. |
| 4926 | 251.860268 | 142.251.42.227 | 192.168.0.14 | OCSP | 777 | Response |
| 7647 | 257.415047 | 192.168.0.14 | 142.251.42.227 | HTTP | 425 | GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCggQUxy55it3%2FYTSuu1H0ri7xsAkB2MEFip0f6%2BFze6VzT2c00JGFpnxNR0nAh. |
| 7648 | 257.421380 | 142.251.42.227 | 192.168.0.14 | OCSP | 778 | Response |
| 9781 | 596.021487 | 192.168.0.14 | 34.223.124.45 | HTTP | 432 | GET / HTTP/1.1 |
| 9784 | 596.169001 | 34.223.124.45 | 192.168.0.14 | HTTP | 893 | HTTP/1.1 200 OK (text/html) |
| 9803 | 597.065055 | 192.168.0.14 | 34.223.124.45 | HTTP | 492 | GET /online HTTP/1.1 |
| 9805 | 597.209963 | 34.223.124.45 | 192.168.0.14 | HTTP | 605 | HTTP/1.1 301 Moved Permanently (text/html) |
| 9807 | 597.225370 | 192.168.0.14 | 34.223.124.45 | HTTP | 493 | GET /online/ HTTP/1.1 |
| 9809 | 597.592394 | 34.223.124.45 | 192.168.0.14 | HTTP | 137 | HTTP/1.1 200 OK (text/html) |
| 9820 | 597.817909 | 192.168.0.14 | 34.223.124.45 | HTTP | 437 | GET /favicon.ico HTTP/1.1 |
| 9822 | 598.110280 | 34.223.124.45 | 192.168.0.14 | HTTP | 509 | HTTP/1.1 200 OK (PNG) |

Frame 9781: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface en0, id 0

Packets: 10096 · Displayed: 54 (0.5%)

Profile: Default

Info time

GET 596.021487

OK 596.169001

 $\Delta t = 596.169001 - 596.021487$

Type "http" in the display filter

→ find two packets which Info says GET and OK

with the opposite source and destination

→ calculate the time difference

$$= 0.147514 \text{ (s)}$$

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------------|----------------------|----------|--------|---|
| 680 | 31.252652 | 192.168.0.14 | 17.248.223.35 | TCP | 66 | 59930 → 443 [FIN, ACK] Seq=6300 ACK=313 Win=2048 Len=0 TSval=2934032763 TSecr=3128433554 |
| 681 | 31.536552 | 17.248.223.35 | 192.168.0.14 | TCP | 66 | 443 → 59930 [ACK] Seq=313 Ack=599 Win=501 Len=0 TSval=3128433558 TSecr=2934032762 |
| 682 | 31.536553 | 17.248.223.35 | 192.168.0.14 | TCP | 66 | 443 → 59930 [RST, ACK] Seq=313 Ack=599 Win=501 Len=0 TSval=3128433558 TSecr=2934032762 |
| 683 | 31.536553 | 17.248.223.35 | 192.168.0.14 | TCP | 54 | 443 → 59930 [RST] Seq=313 Win=0 Len=0 |
| 684 | 31.536553 | 17.248.223.35 | 192.168.0.14 | TCP | 54 | 443 → 59930 [RST] Seq=313 Win=0 Len=0 |
| 685 | 32.423932 | fe80::1857:b9e4:4a.. | fe80::68:e5a1:f7fb.. | TCP | 344 | 49257 → 63751 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=258 TSval=567241267 TSecr=2840867048 |
| 686 | 32.597239 | fe80::1857:b9e4:4a.. | fe80::68:e5a1:f7fb.. | TCP | 344 | [TCP Retransmission] 49257 → 63751 [PSH, ACK] Seq=1 Ack=1 Win=258 Len=258 TSval=567241440 TSecr=2840867048 |
| 687 | 33.010459 | fe80::1857:b9e4:4a.. | fe80::68:e5a1:f7fb.. | TCP | 344 | [TCP Retransmission] 49257 → 63751 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=258 TSval=567241853 TSecr=2840867048 |
| 688 | 33.109627 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 86 | 63751 → 49257 [ACK] Seq=1 Ack=259 Win=2043 Len=0 TSval=2840862382 TSecr=567241267 |
| 689 | 33.109628 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 98 | [TCP Dup ACK 68#1] 63751 → 49257 [ACK] Seq=1 Ack=259 Win=2043 Len=0 TSval=2840862382 TSecr=567241440 |
| 690 | 33.109629 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 806 | 63751 → 49257 [PSH, ACK] Seq=1 Ack=259 Win=2048 Len=720 TSval=2840862400 TSecr=567241440 |
| 691 | 33.109770 | fe80::68:e5a1:f7fb.. | fe80::68:e5a1:f7fb.. | TCP | 86 | 49257 → 63751 [ACK] Seq=259 Ack=721 Win=2036 Len=0 TSval=567241952 TSecr=2840862400 |
| 692 | 33.133036 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 98 | [TCP Dup ACK 68#2] 63751 → 49257 [ACK] Seq=721 Ack=259 Win=2048 Len=0 TSval=2840862521 TSecr=567241853 |
| 693 | 33.347207 | fe80::1857:b9e4:4a.. | fe80::68:e5a1:f7fb.. | TCP | 491 | 49257 → 63751 [PSH, ACK] Seq=259 Ack=721 Win=2044 Len=405 TSval=567242190 TSecr=2840862521 |
| 694 | 33.519447 | fe80::68:e5a1:f7fb.. | fe80::68:e5a1:f7fb.. | TCP | 491 | [TCP Retransmission] 49257 → 63751 [PSH, ACK] Seq=259 Ack=721 Win=2048 Len=405 TSval=567242362 TSecr=2840862521 |
| 695 | 33.636678 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 86 | 63751 → 49257 [ACK] Seq=721 Ack=664 Win=2041 Len=0 TSval=2840862740 TSecr=567242190 |
| 696 | 33.636679 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 499 | 63751 → 49257 [PSH, ACK] Seq=721 Ack=664 Win=2048 Len=413 TSval=2840862785 TSecr=567242190 |
| 697 | 33.636819 | fe80::1857:b9e4:4a.. | fe80::68:e5a1:f7fb.. | TCP | 86 | 49257 → 63751 [ACK] Seq=664 Ack=1134 Win=2041 Len=0 TSval=567242479 TSecr=2840862785 |
| 698 | 33.690733 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 499 | [TCP Spurious Retransmission] 63751 → 49257 [PSH, ACK] Seq=721 Ack=664 Win=2048 Len=413 TSval=2840862785 |
| 699 | 33.690813 | fe80::1857:b9e4:4a.. | fe80::68:e5a1:f7fb.. | TCP | 98 | [TCP Window Update] 49257 → 63751 [ACK] Seq=664 Ack=1134 Win=2048 Len=0 TSval=567242533 TSecr=2840862785 |
| 700 | 33.694458 | fe80::68:e5a1:f7fb.. | fe80::1857:b9e4:4a.. | TCP | 98 | [TCP Dup ACK 69#1] 63751 → 49257 [ACK] Seq=1134 Ack=664 Win=2048 Len=0 TSval=2840863082 TSecr=56724233 |
| 701 | 36.246431 | 192.168.0.14 | 52.38.7.83 | TCP | 129 | [TCP Retransmission] 59904 → 443 [FIN, PSH, ACK] Seq=1 Ack=1 Win=2048 Len=63 TSval=2409514183 TSecr=15 |
| 702 | 36.269630 | 17.57.145.25 | 192.168.0.14 | TLSv1.. | 399 | Application Data |
| 703 | 36.269905 | 192.168.0.14 | 17.57.145.25 | TCP | 66 | 59081 → 5223 [ACK] Seq=129 Ack=1666 Win=2042 Len=0 TSval=787768066 TSecr=4220313282 |
| 704 | 36.272825 | 192.168.0.14 | 17.57.145.25 | TLSv1.. | 98 | Application Data |
| 705 | 36.310021 | 17.57.145.25 | 192.168.0.14 | TCP | 66 | 5223 → 59081 [ACK] Seq=1666 Ack=161 Win=501 Len=0 TSval=4220313318 TSecr=787768069 |
| 706 | 36.582565 | 192.168.0.14 | 17.248.223.6 | TLSv1.. | 97 | Encrypted Alert |
| 707 | 36.583307 | 192.168.0.14 | 17.248.223.6 | TLSv1.. | 97 | Encrypted Alert |
| 708 | 36.583580 | 192.168.0.14 | 17.248.223.6 | TCP | 66 | 59985 → 443 [FIN, ACK] Seq=32 Ack=1 Win=2048 Len=0 TSval=567495518 TSecr=666034846 |
| 709 | 36.584159 | 192.168.0.14 | 17.248.223.6 | TCP | 66 | 59985 → 443 [FIN, ACK] Seq=32 Ack=1 Win=2048 Len=0 TSval=4079753581 TSecr=3300535222 |
| 710 | 36.813133 | 17.248.223.6 | 192.168.0.14 | TCP | 66 | 443 → 59905 [ACK] Seq=1 Ack=32 Win=504 Len=0 TSval=666093916 TSecr=567495517 |
| 711 | 36.813134 | 17.248.223.6 | 192.168.0.14 | TCP | 66 | 443 → 59905 [FIN, ACK] Seq=1 Ack=33 Win=504 Len=0 TSval=666093917 TSecr=567495518 |
| 712 | 36.813134 | 17.248.223.6 | 192.168.0.14 | TCP | 66 | 443 → 59906 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=3300590263 TSecr=4079753580 |
| 713 | 36.813134 | 17.248.223.6 | 192.168.0.14 | TCP | 66 | [TCP Previous segment not captured] 443 → 59906 [FIN, ACK] Seq=1 Ack=33 Win=501 Len=0 TSval=3300590263 TSecr=4079753580 |
| 714 | 36.813135 | 17.248.223.6 | 192.168.0.14 | TCP | 66 | [TCP Retransmission] 443 → 59906 [FIN, ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=3300590263 TSecr=4079753580 |
| 715 | 36.813396 | 192.168.0.14 | 17.248.223.6 | TCP | 66 | 59985 → 443 [ACK] Seq=33 Ack=2 Win=2048 Len=0 TSval=567495748 TSecr=666093917 |
| 716 | 36.813402 | 192.168.0.14 | 17.248.223.6 | TCP | 66 | 59986 → 443 [ACK] Seq=33 Ack=2 Win=2048 Len=0 TSval=4079753811 TSecr=3300590263 |
| 717 | 37.493650 | 17.57.145.25 | 192.168.0.14 | TLSv1.. | 399 | Application Data |
| 718 | 37.493964 | 192.168.0.14 | 17.57.145.25 | TCP | 66 | 59081 → 5223 [ACK] Seq=161 Ack=1999 Win=2042 Len=0 TSval=787769290 TSecr=4220314426 |
| 719 | 37.497172 | 192.168.0.14 | 17.57.145.25 | TLSv1.. | 98 | Application Data |
| 720 | 37.538167 | 17.57.145.25 | 192.168.0.14 | TCP | 66 | 5223 → 59081 [ACK] Seq=1999 Ack=193 Win=501 Len=0 TSval=4220314543 TSecr=787769294 |
| 721 | 41.690469 | 192.168.0.125 | 224.0.0.251 | MDNS | 145 | Standard query response 0x0000 PTR 1比鵠鵠._rdlink.local TXT |
| 722 | 41.690471 | fe80::68:e5a1:f7fb.. | ff02::fb | MDNS | 165 | Standard query response 0x0000 PTR 1比鵠鵠._rdlink.local TXT |

No.702 → IPv4

```
> Frame 702: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface en0, id 0
> Ethernet II, Src: ZioncomE_83:00:64 (40:ee:15:83:00:64), Dst: Apple_6a:cfc:59 (a4:83:e7:6a:cfc:59)
> Internet Protocol Version 4 Src: 17.57.145.25, Dst: 192.168.0.14
> Transmission Control Protocol, Src Port: 5223, Dst Port: 59081, Seq: 1333, Ack: 129, Len: 333
> Transport Layer Security
```

No.700 → IPv6

```
> Frame 700: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: c6:18:84:a0:da:39 (c6:18:84:a0:da:39), Dst: Apple_6a:cfc:59 (a4:83:e7:6a:cfc:59)
> Internet Protocol Version 6 Src: fe80::68:e5a1:f7fb:f907, Dst: fe80::1857:b9e4:4a0a:5a4b
> Transmission Control Protocol, Src Port: 49257, Seq: 1134, Ack: 664, Len: 0
```

8.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|---|
| 55 | 1.345510 | 192.168.0.14 | 192.168.0.1 | DNS | 94 | Standard query 0x6e7d HTTPS edge-063.sgsin8.icloud-content.com |
| 56 | 1.345923 | 192.168.0.14 | 192.168.0.1 | DNS | 94 | Standard query 0x4e6a A edge-063.sgsin8.icloud-content.com |
| 57 | 1.353809 | 192.168.0.1 | 192.168.0.14 | DNS | 216 | Standard query response 0x6e7d HTTPS edge-063.sgsin8.icloud-content.com CNAME edge-063.sgsin8.ce.apple. |
| 58 | 1.354412 | 192.168.0.1 | 192.168.0.14 | DNS | 156 | Standard query response 0x4e6a A edge-063.sgsin8.icloud-content.com CNAME edge-063.sgsin8.ce.apple-dns. |
| 59 | 1.354421 | 192.168.0.14 | 192.168.0.1 | DNS | 92 | Standard query 0x6a93 HTTPS edge-063.sgsin8.ce.apple-dns.net |
| 60 | 1.360124 | 192.168.0.1 | 192.168.0.14 | DNS | 171 | Standard query response 0x6a93 HTTPS edge-063.sgsin8.ce.apple-dns.net SOA ns-1643.awsdns-13.co.uk |
| 138 | 1.873498 | 192.168.0.14 | 192.168.0.1 | DNS | 92 | Standard query 0x0fef HTTPS safebrowsing-proxy.g.applimg.com |
| 139 | 1.873638 | 192.168.0.14 | 192.168.0.1 | DNS | 92 | Standard query 0x906d A safebrowsing-proxy.g.applimg.com |
| 144 | 1.887003 | 192.168.0.1 | 192.168.0.14 | DNS | 156 | Standard query response 0x906d A safebrowsing-proxy.g.applimg.com A 17.253.117.203 A 17.253.87.207 A 1. |

No.55

```
> Frame 55: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface en0, id 0
> Ethernet II, Src: Apple_Ga:cf:59 (a4:83:e7:6a:cf:59), Dst: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
└ Internet Protocol Version 4, Src: 192.168.0.14, Dst: 192.168.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)
  Total Length: 80
  Identification: 0xfefc (61212)
  .... 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xa21 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.14
  Destination Address: 192.168.0.1
  User Datagram Protocol, Src Port: 53259, Dst Port: 53
  Domain Name System (query)
```

Type "DNS" in display filter → choose any one you like

for example choose No.55

→ Internet Protocol Version 4

→ You'll get No.55's TTL = 54

9.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--|
| 22 | 4.128330 | 192.168.0.14 | 128.119.245.12 | HTTP | 477 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 25 | 4.326866 | 128.119.245.12 | 192.168.0.14 | HTTP | 1367 | HTTP/1.1 200 OK (text/html) |
| 27 | 4.351948 | 192.168.0.14 | 128.119.245.12 | HTTP | 503 | GET /pearson.png HTTP/1.1 |
| 31 | 4.552341 | 128.119.245.12 | 192.168.0.14 | HTTP | 781 | HTTP/1.1 200 OK (PNG) |
| 36 | 4.652715 | 192.168.0.14 | 178.79.137.164 | HTTP | 470 | GET /BE_cover_small.jpg HTTP/1.1 |
| 38 | 5.126274 | 178.79.137.164 | 192.168.0.14 | HTTP | 237 | HTTP/1.1 301 Moved Permanently |
| 654 | 9.976534 | 192.168.0.14 | 128.119.245.12 | HTTP | 434 | GET /favicon.ico HTTP/1.1 |
| 656 | 10.165049 | 128.119.245.12 | 192.168.0.14 | HTTP | 551 | HTTP/1.1 404 Not Found (text/html) |

(a) ① 4

② 128.119.245.12

128.119.245.12

178.79.137.164

128.119.245.12

(b) ① Serially

② because second image's "GET" is sent after receiving first image