

Quiz 2

Question 1

Screenshot of my DNS Query and response for www.example.com webpage with HTTPS, IPv4 and IPv6 packets :

The screenshot shows a Wireshark packet capture with a display filter of <all>. The packet list shows 23 packets. Packet 13 is a DNS Standard query from 2601:280:5c80:b400:: to 2001:558:feed::1. Packet 14 is the corresponding response. Packets 19-23 show an HTTPS transaction (TCP, SYN, ACK, and data). The packet details pane for packet 13 shows the Ethernet II, Internet Protocol Version 6, and Internet Control Message Protocol v6 layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Standard Query IPv4 Screenshot 1:

The screenshot shows a Wireshark packet capture with a display filter of <all>. The packet list shows 23 packets. Packet 13 is a DNS Standard query from 2601:280:5c80:b400:: to 2001:558:feed::1. Packet 14 is the corresponding response. Packets 19-23 show an HTTPS transaction (TCP, SYN, ACK, and data). The packet details pane for packet 13 shows the Ethernet II, Internet Protocol Version 6, and Internet Control Message Protocol v6 layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Apply a display filter ... <37>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--|--|----------|--------|---|
| 12 | 3.424927 | 18.0.0.163 | 44.235.85.225 | TCP | 66 | 49436 → 443 [ACK] Seq=381 Ack=863 Win=2837 Len=0 TSval=1854535338 TSecr=35628660 |
| 13 | 3.893853 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2081:558::feed:1 | DNS | 95 | Standard query RtoA1 HTTPS www.example.com |
| 14 | 3.893782 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2081:558::feed:1 | DNS | 95 | Standard query RtoC1 AAAA www.example.com |
| 15 | 3.893783 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2081:558::feed:1 | DNS | 95 | Standard query RtoS2 www.example.com |
| 16 | 3.914451 | 2081:558::feed:1 | 2681:208:5c8b:b408:457c:354b:da97:1225 | DNS | 113 | Standard query response RtoS2A A www.example.com A 93.184.216.34 |
| 17 | 3.914585 | 2081:558::feed:1 | 2681:208:5c8b:b408:457c:354b:da97:1225 | DNS | 123 | Standard query response RtoC1 AAAA www.example.com AAAA 2686:2088:228:1:248:1893 |
| 18 | 3.947569 | 2081:558::feed:1 | 2681:208:5c8b:b408:457c:354b:da97:1225 | DNS | 155 | Standard query response RtoA1 HTTPS www.example.com SOA ns.icann.org |
| 19 | 3.950229 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2086:2080:228:1:248:1893:25c8:1946 | TCP | 90 | 49587 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 MSG=4 TSval=2072345715 TSecr=0 |
| 20 | 3.956489 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2086:2080:228:1:248:1893:25c8:1946 | TCP | 90 | 49588 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 MSG=4 TSval=358475868 TSecr=0 |
| 21 | 3.974848 | 2686:2080:228:1:248:1893:25c8:1946 | 2681:208:5c8b:b408:457c:354b:da97:1225 | TCP | 94 | 80 → 49587 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1228 SACK_PERM=1 TSval=1182 |
| 22 | 3.974844 | 2686:2080:228:1:248:1893:25c8:1946 | 2681:208:5c8b:b408:457c:354b:da97:1225 | TCP | 94 | 80 → 49588 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1228 SACK_PERM=1 TSval=2513 |
| 23 | 3.975882 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2086:2080:228:1:248:1893:25c8:1946 | TCP | 86 | 49587 → 80 [ACK] Seq=1 Ack=1 Win=131648 Len=0 TSval=2072345746 TSecr=1182614349 |
| 24 | 3.975882 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2086:2080:228:1:248:1893:25c8:1946 | TCP | 86 | 49588 → 80 [ACK] Seq=1 Ack=1 Win=131648 Len=0 TSval=3584758693 TSecr=3518349636 |
| 25 | 3.977776 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2086:2080:228:1:248:1893:25c8:1946 | HTTP | 482 | GET / HTTP/1.1 |
| 26 | 4.004797 | 2686:2080:228:1:248:1893:25c8:1946 | 2681:208:5c8b:b408:457c:354b:da97:1225 | TCP | 86 | 80 → 49588 [ACK] Seq=1 Ack=377 Win=67872 Len=0 TSval=3518384969 TSecr=3584765896 |
| 27 | 4.004818 | 2686:2080:228:1:248:1893:25c8:1946 | 2081:558::feed:1 | HTTP | 1188 | HTTP/1.1 200 OK (text/html) |
| 28 | 4.004977 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2086:2080:228:1:248:1893:25c8:1946 | TCP | 86 | 49588 → 80 [ACK] Seq=377 Ack=1823 Win=138624 Len=0 TSval=3584765123 TSecr=351838 |
| 29 | 4.038182 | 2681:208:5c8b:b408:457c:354b:da97:1225 | 2081:558::feed:1 | DNS | 92 | Standard query RtoB4 A www.lima.org |
| 30 | 4.043002 | 2686:2080:228:1:248:1893:25c8:1946 | 2086:2080:228:1:248:1893:25c8:1946 | TCP | 86 | 49588 → 80 [ACK] Seq=377 Ack=1823 Win=138624 Len=0 TSval=3584765123 TSecr=351838 |

```
> Frame 30: 85 bytes on wire (708 bits), 85 bytes captured (708 bits) on interface eth_0
> Ethernet II, Src: Apple_bau5a:90:48(d8:08:b3:a5:90:48), Dst: AR02:5c:cb:b0:d8 (08:0f:c2:b3:bd:08)
> Internet Protocol Version 6, Src: 2081:208:5c8b:b408:457c:354b:da97:1225, Dst: 2081:558::feed:1
> User Datagram Protocol, Src Port: 64373, Dst Port: 53

<> Domain Name System (dns)
  Transaction ID: 0xb5a2
    Flags: 0x0100 Standard query
      RQ: ..... = Response: Message is a query
      QR: ..... = Opcode: Standard query (0)
      AA: ..... = Truncated: Message is not truncated
      TC: ..... = Recursion desired: Do query recursively
      RD: ..... = Z: reserved (0)
      AD: ..... = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries
  www.example.com: type A, class IN
    Name: www.example.com
    Name Length: 15
    Label Count: 3
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    (Response Rr: 15)

0000 80 ef 16 cb 8d 48 d7 05 ba 59 39 86 dd 68 8e          . . . . . TO
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . E
0020 35 4b da 97 12 25 05 16 cd 00 00 00 00 00 00 00 00  . . . . . X
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . .
0040 00 00 00 00 00 01 fa 0b 35 48 2f fe 05 c2          . . . . .
0050 78 65 cd 78 ce e5 83 83 0f 64 00 00 01 00 01       xample.c om
```

Domain Name System (dns). 33 bytes Packets: 57 · Displayed: 57 (100.0%) Profile: Default

The image shows a Wireshark packet capture analysis of a DNS query and response. The packet list on the left shows 23 packets. The packet details pane on the right shows the structure of the selected packet (No. 18, 151 bytes). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Packet List:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------|--|----------|--------|--|
| 1 | 0.000000 | -- | ff02::1 | ICMPv6 | 174 | Router Advertisement from 88:ef:16:cb:88:8d |
| 2 | 0.548101 | -- | 239.255.255.250 | SSDP | 218 | M-SEARCH * HTTP/1.1 |
| 3 | 0.923873 | -- | 239.255.255.250 | SSDP | 167 | M-SEARCH * HTTP/1.1 |
| 4 | 1.116463 | -- | 239.255.255.250 | SSDP | 167 | M-SEARCH * HTTP/1.1 |
| 5 | 1.535769 | -- | 239.255.255.250 | SSDP | 167 | M-SEARCH * HTTP/1.1 |
| 6 | 2.458163 | -- | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 7 | 3.067367 | -- | ff02::1 | ICMPv6 | 174 | Router Advertisement from 88:ef:16:cb:88:8d |
| 8 | 3.377709 | -- | 44.235.85.225 | TLSv1 | 366 | Application Data |
| 9 | 3.378846 | -- | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 10 | 3.424787 | -- | 10.0.0.163 | TLSv1 | 131 | Application Data |
| 11 | 3.424794 | -- | 10.0.0.163 | TLSv1 | 663 | Application Data |
| 12 | 3.424927 | -- | 44.235.85.225 | TCP | 66 | 49430 -> 443 [ACK] Seq=301 Ack=663 Win=2037 Len=0 TSval=1854535338 TSecr=3562886852 |
| 13 | 3.891853 | -- | 2001:558:feed::1 | DNS | 95 | Standard query 0x3e41 HTTPS www.example.com |
| 14 | 3.891782 | -- | 2001:558:feed::1 | DNS | 95 | Standard query 0xedc1 AAAA www.example.com |
| 15 | 3.891783 | -- | 2001:558:feed::1 | DNS | 95 | Standard query 0xb5a2 A www.example.com |
| 16 | 3.918481 | -- | 2601:280:5c80:b400:457c:354b:da97:1225 | DNS | 111 | Standard query response 0xb5a2 A www.example.com A 93.184.216.34 |
| 17 | 3.918485 | -- | 2601:280:5c80:b400:457c:354b:da97:1225 | DNS | 123 | Standard query response 0xedc1 AAAA www.example.com AAAA 2606:2800:220:1:248:1893:25c8:1946 |
| 18 | 3.947569 | -- | 2601:280:5c80:b400:457c:354b:da97:1225 | DNS | 151 | Standard query response 0x3e41 HTTPS www.example.com SOA ns.icann.org |
| 19 | 3.950289 | -- | 2606:2800:220:1:248:1893:25c8:1946 | TCP | 98 | 49507 -> 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=2672345715 TSecr=0 SACK_PERM=1 |
| 20 | 3.950489 | -- | 2606:2800:220:1:248:1893:25c8:1946 | TCP | 98 | 49508 -> 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=3584765068 TSecr=0 SACK_PERM=1 |
| 21 | 3.974840 | -- | 2601:280:5c80:b400:457c:354b:da97:1225 | TCP | 94 | 80 -> 49507 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1220 SACK_PERM=1 TSval=1182643439 TSecr=0 |
| 22 | 3.974844 | -- | 2601:280:5c80:b400:457c:354b:da97:1225 | TCP | 94 | 80 -> 49508 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1220 SACK_PERM=1 TSval=3518384936 TSecr=0 |
| 23 | 3.975802 | -- | 2606:2800:220:1:248:1893:25c8:1946 | TCP | 86 | 49507 -> 80 [ACK] Seq=1 Ack=1 Win=131648 Len=0 TSval=2672345740 TSecr=1182643439 |

Packet Details (No. 18):

- Frame 18: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface en0, id 0
- Ethernet II, Src: ARISGro_cb:88:8d (88:ef:16:cb:88:8d), Dst: Apple_ba:54:39 (48:d7:05:ba:54:39)
- Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:280:5c80:b400:457c:354b:da97:1225
- User Datagram Protocol, Src Port: 53, Dst Port: 57640
- Domain Name System (response)

Packet Bytes:

```

0000  48 d7 05 ba 54 39 88 ef 16 cb 88 8d 86 dd 60 00  H...T9...
0010  00 00 00 61 11 38 20 01 05 58 fe ed 00 00 00 00  ...a.8...X...
0020  00 00 00 00 00 01 26 01 82 80 5c 80 b4 00 45 7c  ......&...[E]
0030  35 4b da 97 12 25 80 35 e1 20 00 61 f0 19 3e 41  5K...&5...>A
  
```

Interface Info (Frame.Interface.id):

Packets: 57 · Displayed: 57 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Standard Response IPv4 Screenshot 2:

Apply a display filter ... <37>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--|--|----------|--------|---|
| 12 | 3.424927 | 10.0.0.165 | 44.235.85.225 | TCP | 66 | 4938 → 443 [ACK] Seq=381 Acs=663 Win=2037 Len=0 TSval=1854535338 TSecr=356286868 |
| 13 | 3.891853 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2081:558::feed:1 | DNS | 95 | Standard query 8x341 HTTPS www.example.com. |
| 14 | 3.891782 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2081:558::feed:1 | DNS | 95 | Standard query 8x62 AAAA www.example.com. |
| 15 | 3.891783 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2081:558::feed:1 | DNS | 95 | Standard query 8x62 AAAA www.example.com. |
| 16 | 3.915118 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2081:558::feed:1 | DNS | 115 | Standard query response 8x341 HTTPS www.example.com. A 5341482161 |
| 17 | 3.914865 | 2081:558::feed:1 | 2081:2081::c8b:b400:457c:354b:d97:1225 | DNS | 323 | Standard query response 8x62 AAAA www.example.com. AAAA 2686:2089:220:1:248:1893 |
| 18 | 3.947569 | 2081:558::feed:1 | 2081:2081::c8b:b400:457c:354b:d97:1225 | DNS | 151 | Standard query response 8x341 HTTPS www.example.com. SOA ns.icann.org. |
| 19 | 3.958209 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2081:2081::c8b:b400:457c:354b:d97:1225 | TCP | 98 | 49507 → 80 [SYN] Seq=81 Win=65535 Len=0 MSS=1448 WS=64 TSval=2672345715 TSecr=0 S |
| 20 | 3.958449 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2081:2081::c8b:b400:457c:354b:d97:1225 | TCP | 98 | 49508 → 80 [SYN] Seq=81 Win=65535 Len=0 MSS=1448 WS=64 TSval=304756848 TSecr=0 S |
| 21 | 3.974848 | 2086:2086:220:1:248:1893:25c8:1946 | 2081:2081::c8b:b400:457c:354b:d97:1225 | TCP | 94 | 80 → 49507 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=1228 SCAP_FPM=1 TSval=1181 |
| 22 | 3.974844 | 2086:2086:220:1:248:1893:25c8:1946 | 2081:2081::c8b:b400:457c:354b:d97:1225 | TCP | 94 | 80 → 49508 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=1228 SCAP_FPM=1 TSval=3513 |
| 23 | 3.975882 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2086:2086:220:1:248:1893:25c8:1946 | TCP | 86 | 49507 → 80 [ACK] Seq=1 Ack=1 Win=315448 Len=0 TSval=2672345715 TSecr=136263439 |
| 24 | 3.975882 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2086:2086:220:1:248:1893:25c8:1946 | TCP | 86 | 49508 → 80 [ACK] Seq=1 Ack=1 Win=315448 Len=0 TSval=3584765903 TSecr=3518384936 |
| 25 | 3.977776 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2086:2086:220:1:248:1893:25c8:1946 | HTTP | 62 | GET / HTTP/1.1 |
| 26 | 4.004797 | 2086:2086:220:1:248:1893:25c8:1946 | 2081:2081::c8b:b400:457c:354b:d97:1225 | TCP | 66 | 80 → 49508 [ACK] Seq=1 Ack=377 Win=67872 Len=0 TSval=3518204969 TSecr=3304765094 |
| 27 | 4.004810 | 2086:2086:220:1:248:1893:25c8:1946 | 2081:2081::c8b:b400:457c:354b:d97:1225 | HTTP | 1108 | HTTP/1.1 200 OK (text/html) |
| 28 | 4.004971 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2086:2086:220:1:248:1893:25c8:1946 | TCP | 86 | 49508 → 80 [ACK] Seq=377 Ack=1823 Win=138624 Len=0 TSval=3584765123 TSecr=351838 |
| 29 | 4.008182 | 2081:2081::c8b:b400:457c:354b:d97:1225 | 2081:558::feed:1 | DNS | 92 | Standard query 8x684 A www.lima.org |

> Frame 16: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface em0, id 0
 > Ethernet II, Src: ARS55Dg-mib400 (08:00:27:00:00:00), Dst: AppleBasEtnP (08:00:27:00:00:00)
 > Internet Protocol Version 6, Src: 2081:558::feed:1, Dst: 2081:2081::c8b:b400:457c:354b:d97:1225
 > User Datagram Protocol, Src Port: 53, Dst Port: 64371

Domain Name System (dns) 15

- Transaction ID: 0x05a2
- Flags: 0x0180 Standard query response, No error
- Response Message is a response
- Opcode: Standard query (0)
- Authoritative Server is not an authority for domain
- Truncated: Message is not truncated
- Recursion desired: Do not recurse recursively
- Recursion available: Server can do recursive queries
- Z: reserved (0)
- Answer authenticated: Answer/authority portion was not authenticated by the server
- Non-authenticated data: Unacceptable
- Reply code: No error (0)
- Question: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 0
- Queries
- www.example.com: type A, class IN
- Name: www.example.com
- (Name Length: 15)
- (Label Count: 3)
- Type: A (Host Address) (1)
- Class: IN (0x0001)
- Answers
- (Request Info: 15)
- [Time: 0.026598000 seconds]

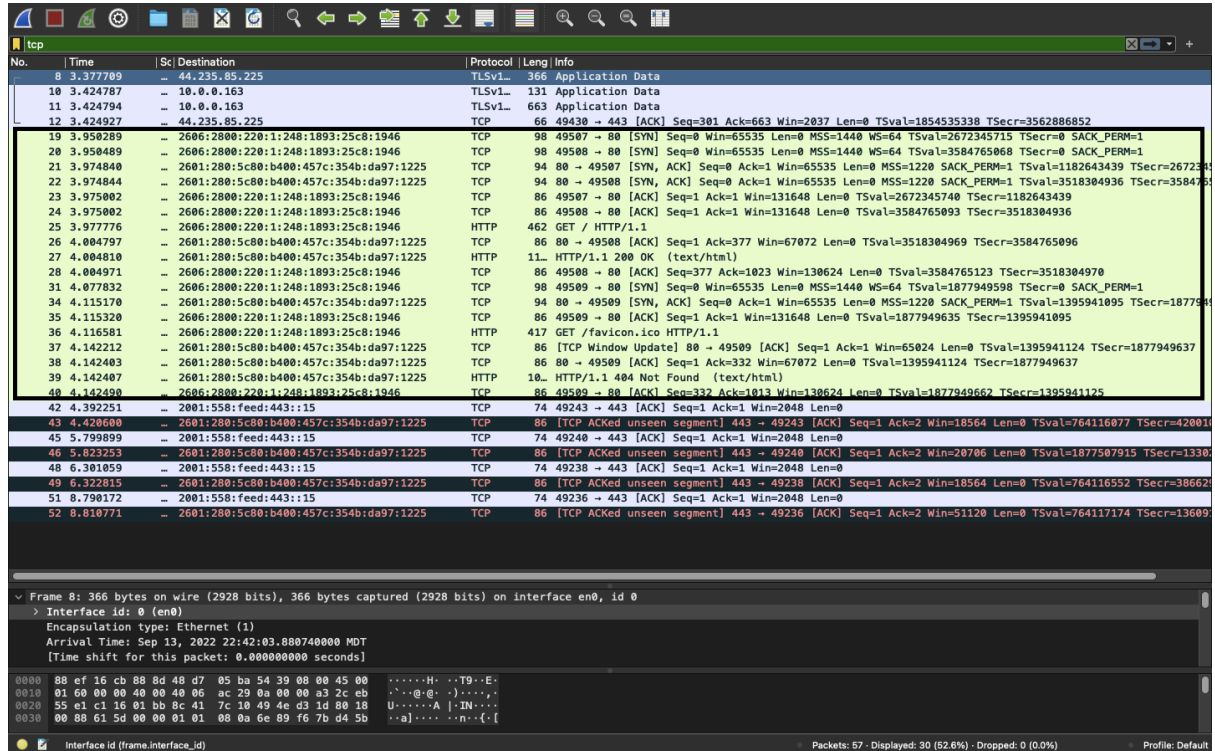
```

0000  00 27 00 b4 5d 30 00 0f 16 c8 8b 00 00 00 00 00  H: TP...
0001  00 00 00 39 11 30 28 20 01 55 58 fe d0 00 00 00  .B...X..
0002  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0003  35 4b da 97 12 25 30 f1 ff aa 00 39 38 20 80 55 a2  SK...S...[
0004  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....w...e
0005  00 00 00 70 80 81 80 80 80 80 80 80 80 80 80 80  ....x...m...e...l...
0006  8c 00 01 00 01 00 00 cd aa 00 54 dd db dd 22     ....j...
  
```

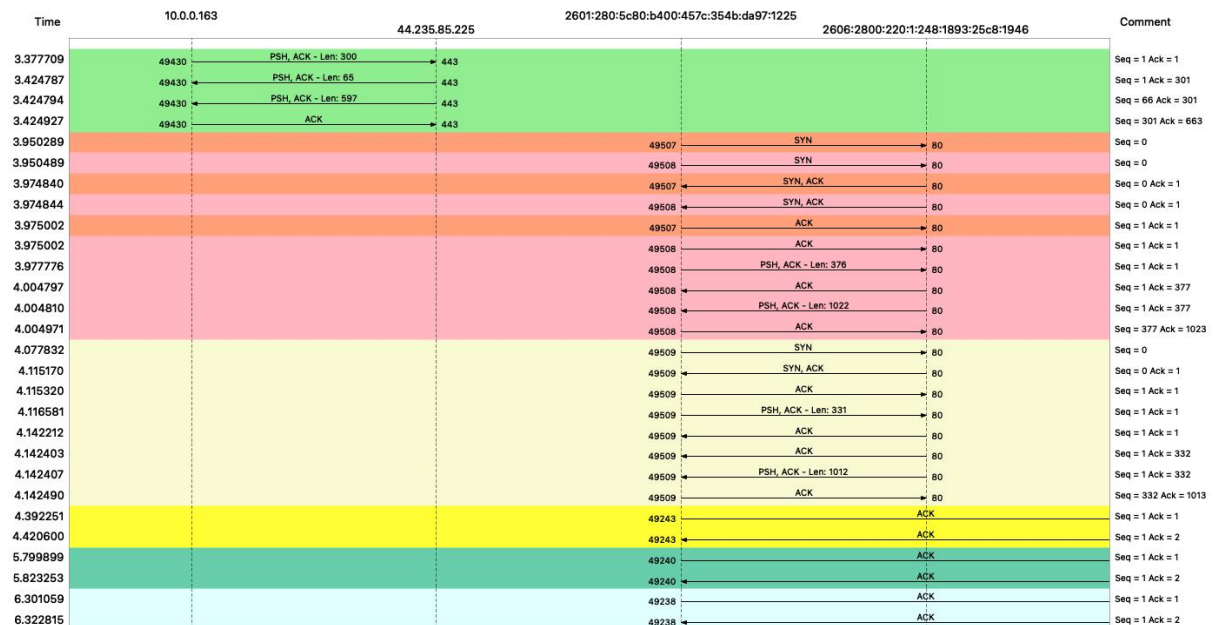
Domain Name System (dns). 49 bytes Packets: 57 · Displayed: 57 (100.0%) Profile: Default

Question 2

Screenshot of my TCP 3-way handshake connecting to the webpage:

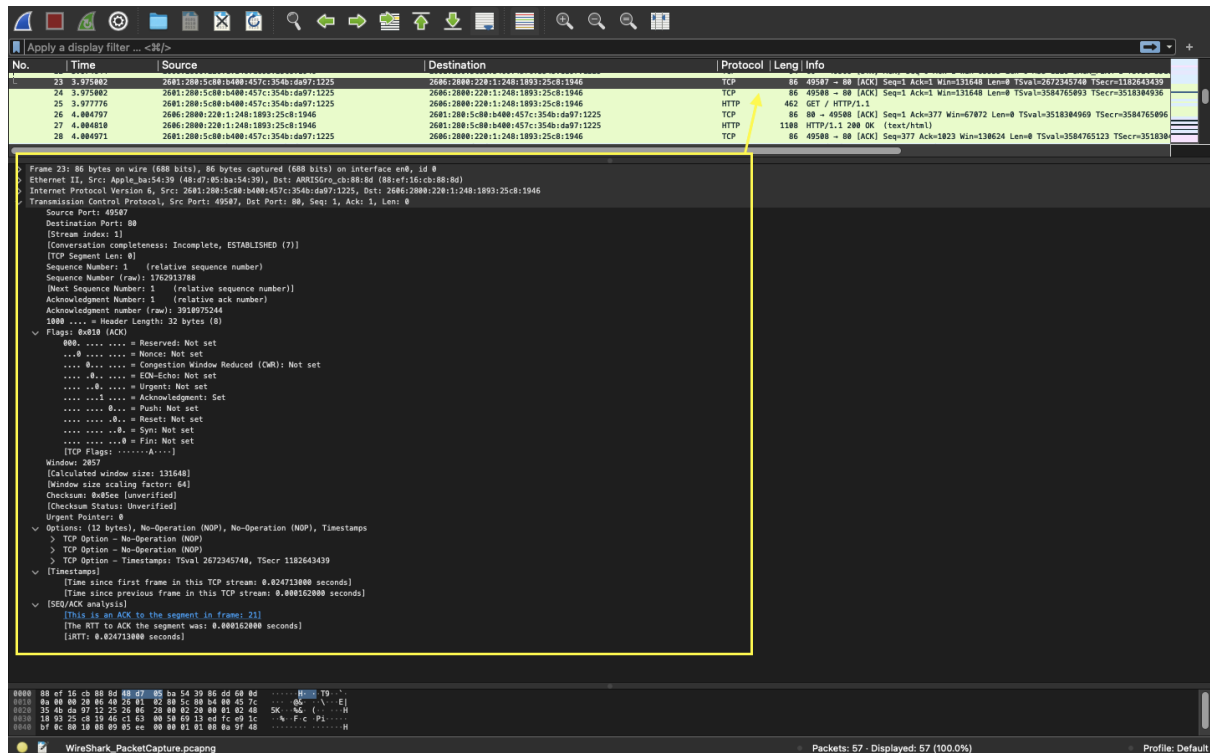


TCP Flow Chart Obtained for Statistics is as follows:

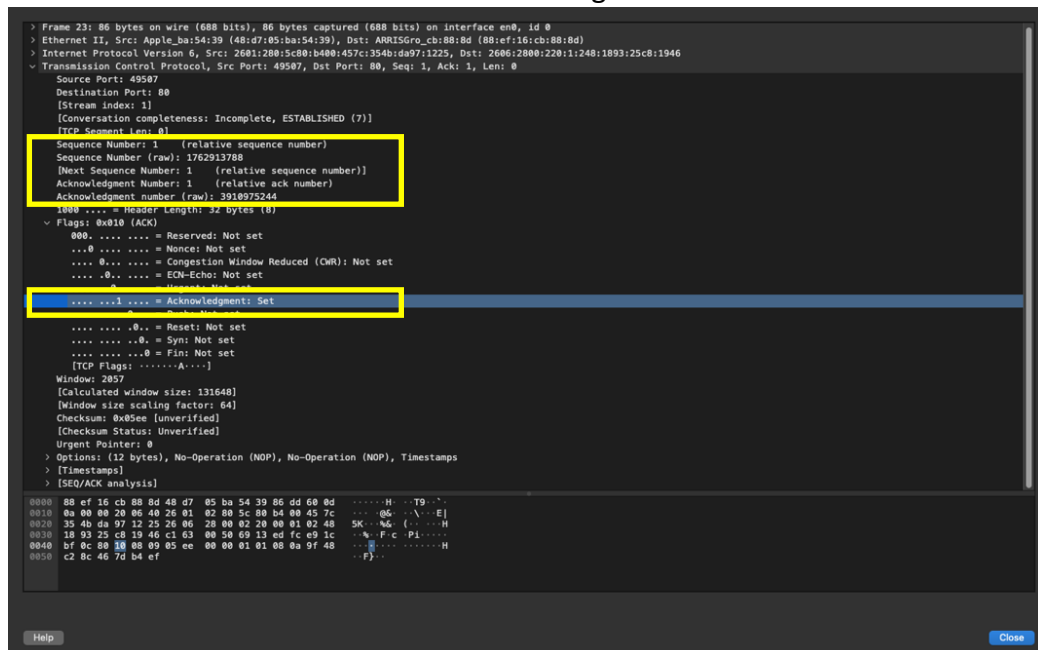


Question 3

Screenshot of an ACK



Detailed View of ACK Packet with Acknowledgement bit set to 1:



As seen in the screenshot attached, please find the sequence and acknowledge number as follows:

Sequence Number: 1 (relative sequence number)

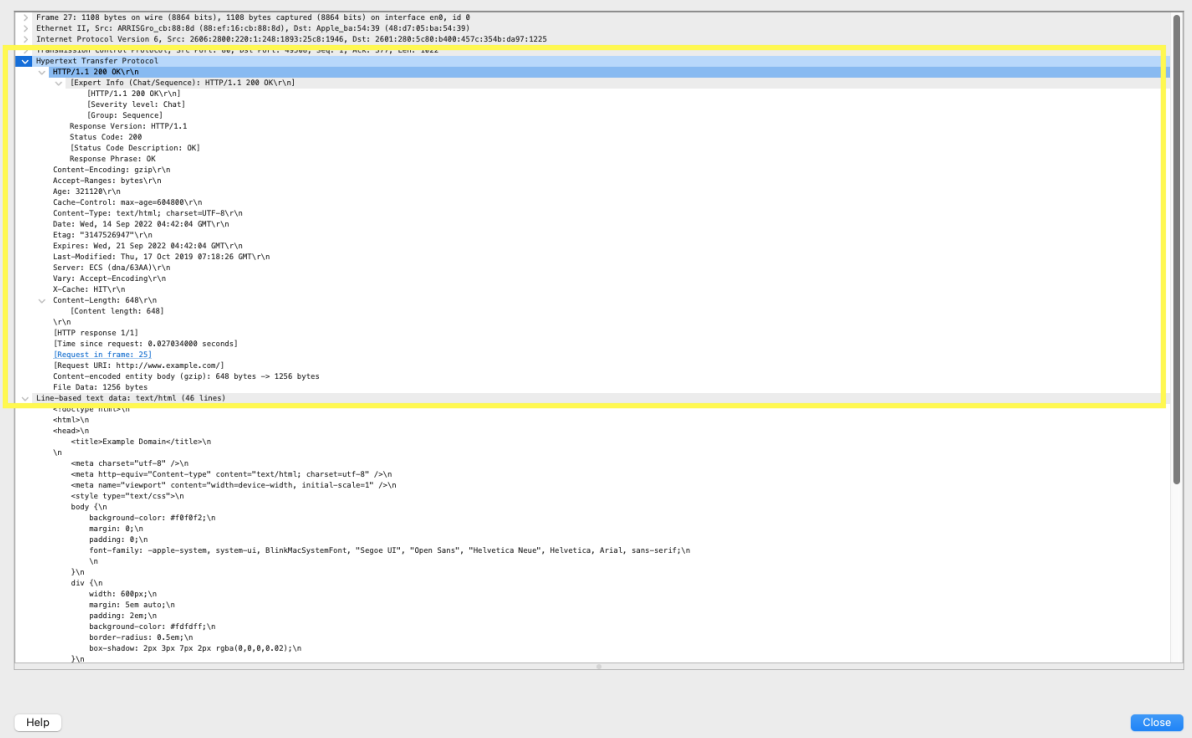
Sequence Number (raw): 1808727242

Acknowledgment Number: 1 (relative ack number)

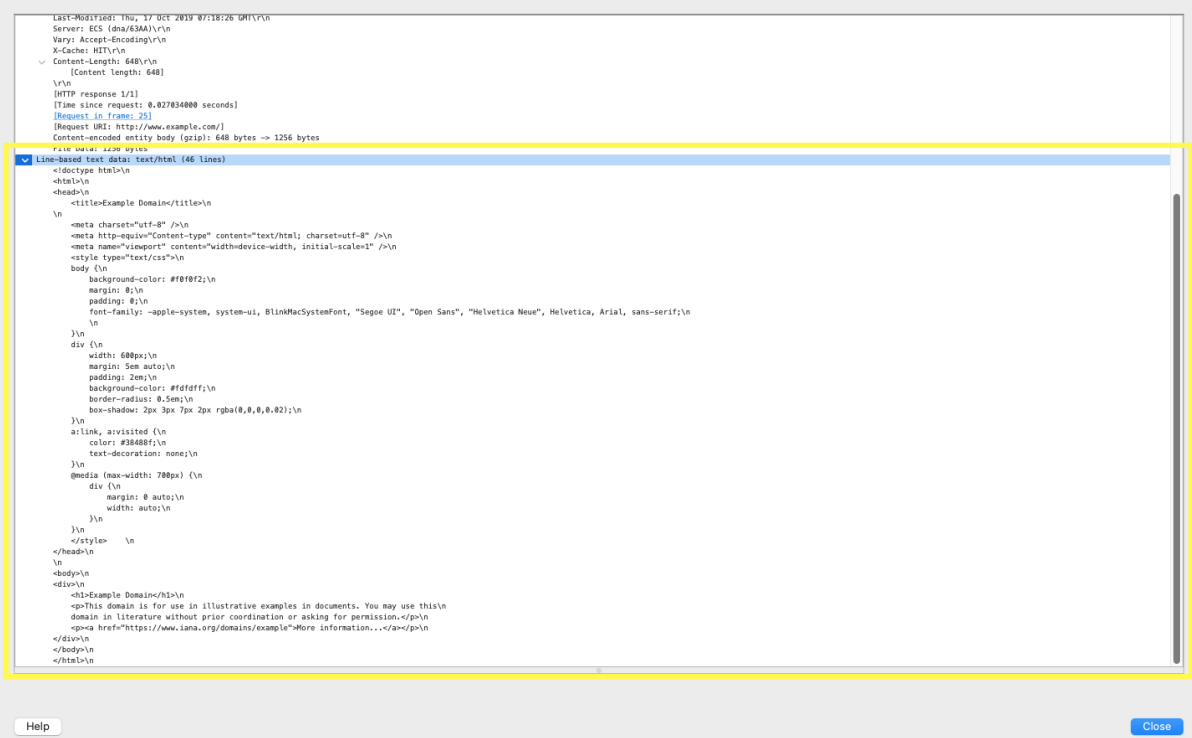
Acknowledgment number (raw): 1110471532

Question 4

Below screenshot shows the HTTP packet where html file from server is loaded into browser



Detailed text/HTML code obtained as a line-based text data:



Question 5

List the values your computer used for:

- a. Source MAC Apple_ba:54:39 (48:d7:05:ba:54:39)
- b. Destination MAC ARRISGro_cb:88:8d (88:ef:16:cb:88:8d)
- c. Source IP 2601:280:5c80:b400:457c:354b:da97:1225
- d. Destination IP 2606:2800:220:1:248:1893:25c8:1946
- e. Source TCP Port 49508
- f. Destination TCP Port 80