Lab 3:

Wireshark Introduction

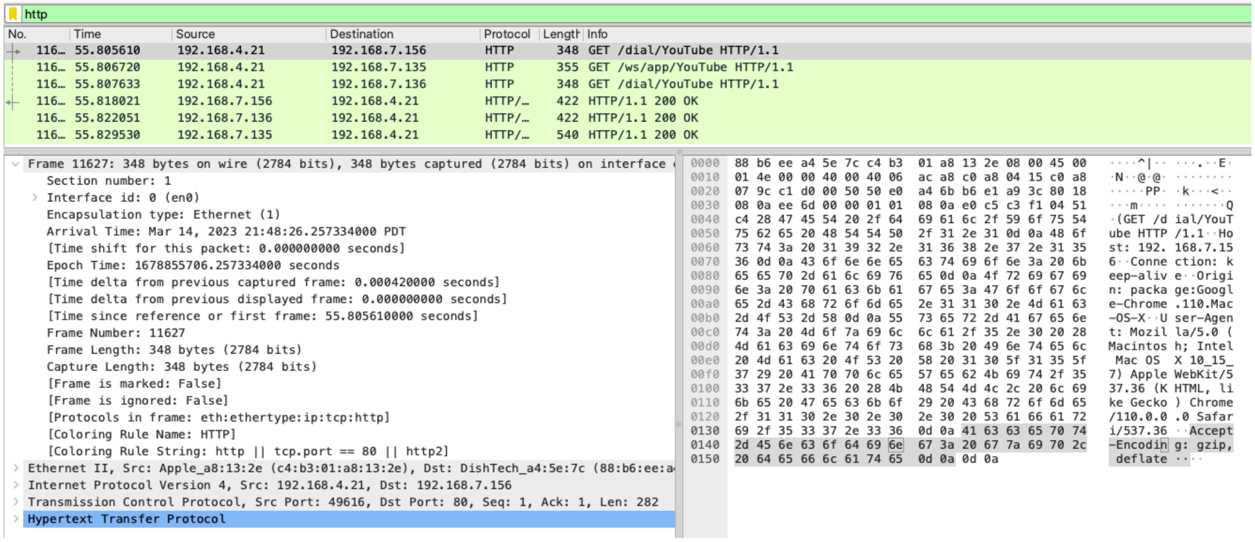
San Francisco State University

ENGR 476-01 Computer Communication Networks
Spring 2023

Christie Lai

Date of submission: 3/15/2023

Screenshot of Captured

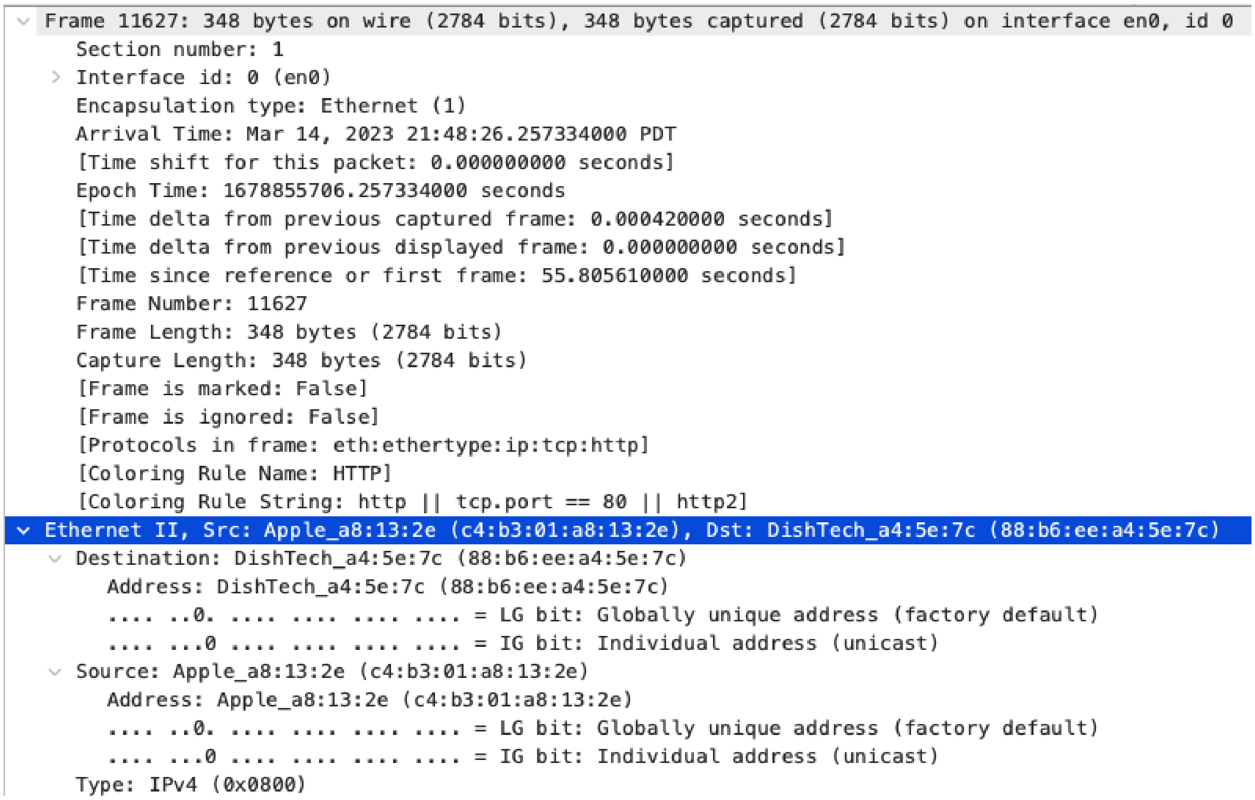


http

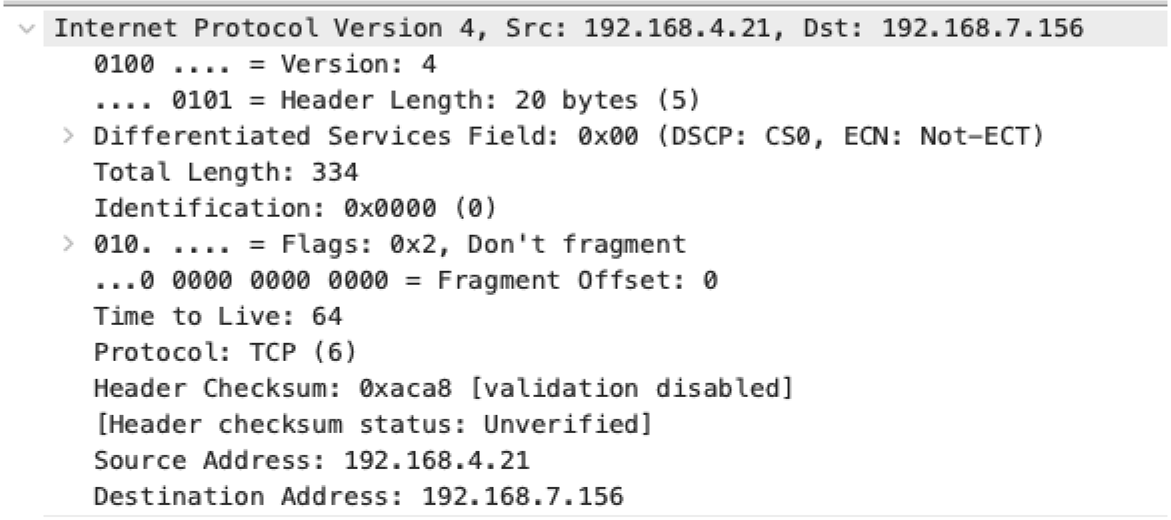
No.	Time	Source	Destination	Protocol	Length	Info
116…	55.805610	192.168.4.21	192.168.7.156	HTTP	348	GET /dial/YouTube HTTP/1.1
116…	55.806720	192.168.4.21	192.168.7.135	HTTP	355	GET /ws/app/YouTube HTTP/1.1
116…	55.807633	192.168.4.21	192.168.7.136	HTTP	348	GET /dial/YouTube HTTP/1.1
116…	55.818021	192.168.7.156	192.168.4.21	HTTP/…	422	HTTP/1.1 200 OK
116…	55.822051	192.168.7.136	192.168.4.21	HTTP/…	422	HTTP/1.1 200 OK
116…	55.829530	192.168.7.135	192.168.4.21	HTTP/…	540	HTTP/1.1 200 OK

```
Frame 11627: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface
    Section number: 1
  > Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 14, 2023 21:48:26.257334000 PDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1678855706.257334000 seconds
    [Time delta from previous captured frame: 0.000420000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 55.805610000 seconds]
    Frame Number: 11627
    Frame Length: 348 bytes (2784 bits)
    Capture Length: 348 bytes (2784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: Apple_a8:13:2e (c4:b3:01:a8:13:2e), Dst: DishTech_a4:5e:7c (88:b6:ee:a
> Internet Protocol Version 4, Src: 192.168.4.21, Dst: 192.168.7.156
> Transmission Control Protocol, Src Port: 49616, Dst Port: 80, Seq: 1, Ack: 1, Len: 282
> Hypertext Transfer Protocol
```

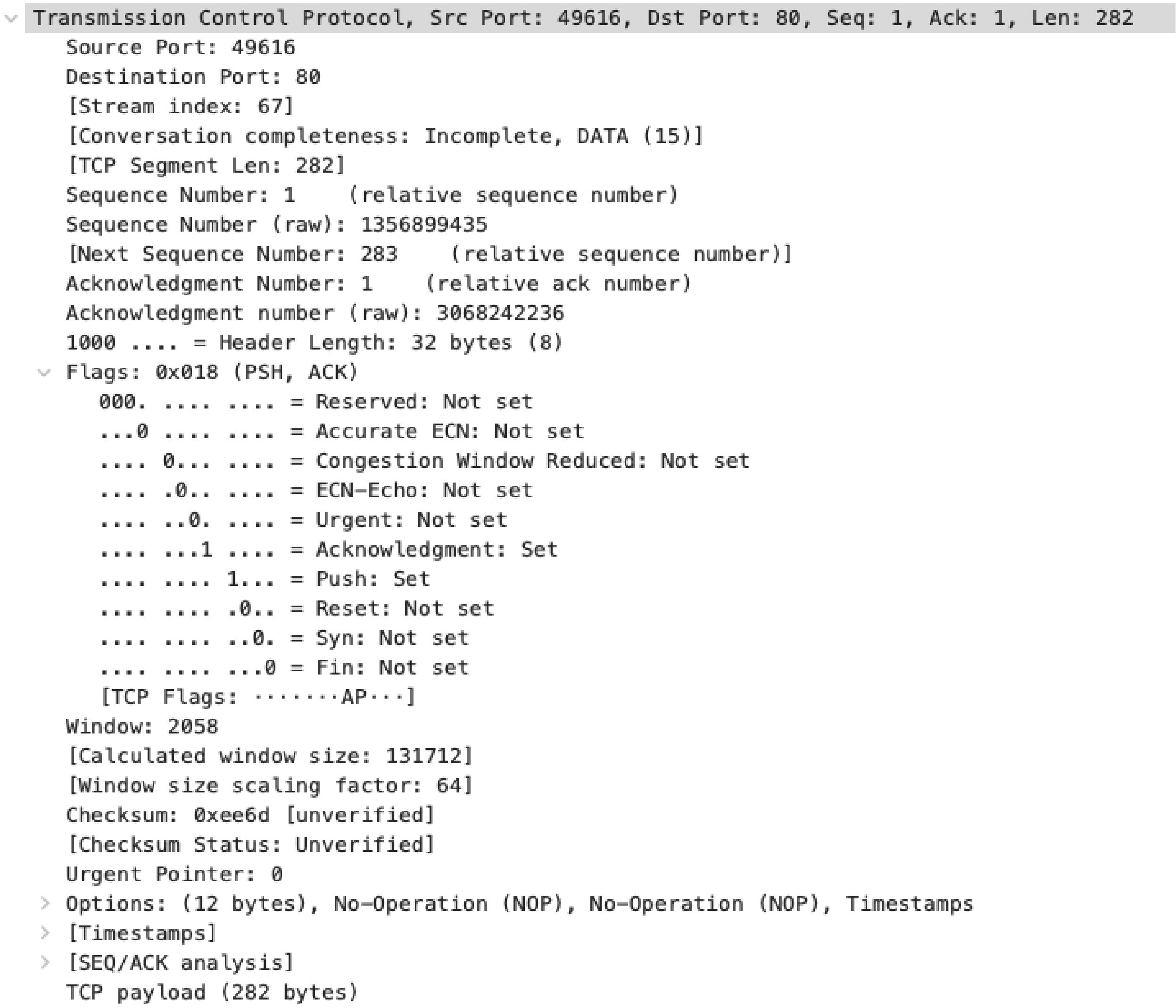
```
0000  88 b6 ee a4 5e 7c c4 b3  01 a8 13 2e 08 00 45 00   ····^|·· ·····.··E·
0010  01 4e 00 00 40 00 40 06  ac a8 c0 a8 04 15 c0 a8   ·N··@·@· ········
0020  07 9c c1 d0 00 50 50 e0  a4 6b b6 e1 a9 3c 80 18   ·····PP· ·k···<··
0030  08 0a ee 6d 00 00 01 01  08 0a e0 c5 c3 f1 04 51   ···m···· ·······Q
0040  c4 28 47 45 54 20 2f 64  69 61 6c 2f 59 6f 75 54   ·(GET /d ial/YouT
0050  75 62 65 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   ube HTTP /1.1··Ho
0060  73 74 3a 20 31 39 32 2e  31 36 38 2e 37 2e 31 35   st: 192. 168.7.15
0070  36 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   6··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 4f 72 69 67 69   eep-aliv e··Origi
0090  6e 3a 20 70 61 63 6b 61  67 65 3a 47 6f 6f 67 6c   n: packa ge:Googl
00a0  65 2d 43 68 72 6f 6d 65  2e 31 31 30 2e 4d 61 63   e-Chrome .110.Mac
00b0  2d 4f 53 2d 58 0d 0a 55  73 65 72 2d 41 67 65 6e   -OS-X··U ser-Agen
00c0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00d0  4d 61 63 69 6e 74 6f 73  68 3b 20 49 6e 74 65 6c   Macintos h; Intel
00e0  20 4d 61 63 20 4f 53 20  58 20 31 30 5f 31 35 5f    Mac OS  X 10_15_
00f0  37 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   7) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 31 30 2e 30 2e 30  2e 30 20 53 61 66 61 72   /110.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  0d 0a 41 63 63 65 70 74   i/537.36 ··Accept
0140  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0150  20 64 65 66 6c 61 74 65  0d 0a 0d 0a                deflate ····
```



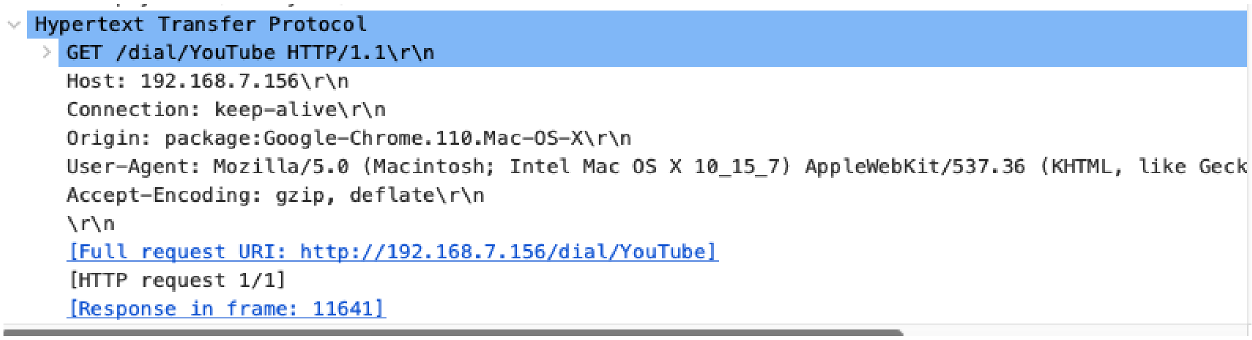
```
v Frame 11627: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface en0, id 0
    Section number: 1
  > Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 14, 2023 21:48:26.257334000 PDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1678855706.257334000 seconds
    [Time delta from previous captured frame: 0.000420000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 55.805610000 seconds]
    Frame Number: 11627
    Frame Length: 348 bytes (2784 bits)
    Capture Length: 348 bytes (2784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
v Ethernet II, Src: Apple_a8:13:2e (c4:b3:01:a8:13:2e), Dst: DishTech_a4:5e:7c (88:b6:ee:a4:5e:7c)
  v Destination: DishTech_a4:5e:7c (88:b6:ee:a4:5e:7c)
      Address: DishTech_a4:5e:7c (88:b6:ee:a4:5e:7c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Apple_a8:13:2e (c4:b3:01:a8:13:2e)
      Address: Apple_a8:13:2e (c4:b3:01:a8:13:2e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```



```
⌄ Internet Protocol Version 4, Src: 192.168.4.21, Dst: 192.168.7.156
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 334
    Identification: 0x0000 (0)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xaca8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.4.21
    Destination Address: 192.168.7.156
```



```
⌄ Transmission Control Protocol, Src Port: 49616, Dst Port: 80, Seq: 1, Ack: 1, Len: 282
    Source Port: 49616
    Destination Port: 80
    [Stream index: 67]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 282]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1356899435
    [Next Sequence Number: 283    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3068242236
    1000 .... = Header Length: 32 bytes (8)
  ⌄ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window: 2058
    [Calculated window size: 131712]
    [Window size scaling factor: 64]
    Checksum: 0xee6d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  › [Timestamps]
  › [SEQ/ACK analysis]
    TCP payload (282 bytes)
```



```
Hypertext Transfer Protocol
  GET /dial/YouTube HTTP/1.1\r\n
    Host: 192.168.7.156\r\n
    Connection: keep-alive\r\n
    Origin: package:Google-Chrome.110.Mac-OS-X\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Geck
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://192.168.7.156/dial/YouTube]
    [HTTP request 1/1]
    [Response in frame: 11641]
```

Questions: Using the first frame with the source protocol HTTP, answer the following question in your lab-report sheet.

1. Is the frame an outgoing or an incoming frame?

Using the first frame with the source protocol http, the frame is an outgoing frame because the source address is host I am working with.

2. What is the source IP address of the network-layer header in the frame?

The source IP address of the network-layer header in the frame is 192.168.4.21.

3. What is the destination IP address of the network-layer header in the frame?

The destination IP address of the network-layer header in the frame is 192.168.7.156.

4. What is the total number of bytes in the whole frame?

The total number of bytes in the whole frame is 348 bytes.

5. What is the number of bytes in the Ethernet (data-link layer) header?

The total number of bytes in the Ethernet header is 14 bytes. I just subtracted the total number of bytes which is 348 in the whole frame from the total length in the IP, which is 334.

6. What is the number of bytes in the IP header?

The number of bytes in the IP header is 20 bytes.

7. What is the number of bytes in the TCP header?

The number of bytes in the TCP header is 32 bytes.

8. What is the total bytes in the message (at the application layer)?

The total bytes in the message is 334 – 20 – 32 = 282 bytes. Where there is 334 in the total length of the IP and 20 bytes in there and 32 in the TCP header.