

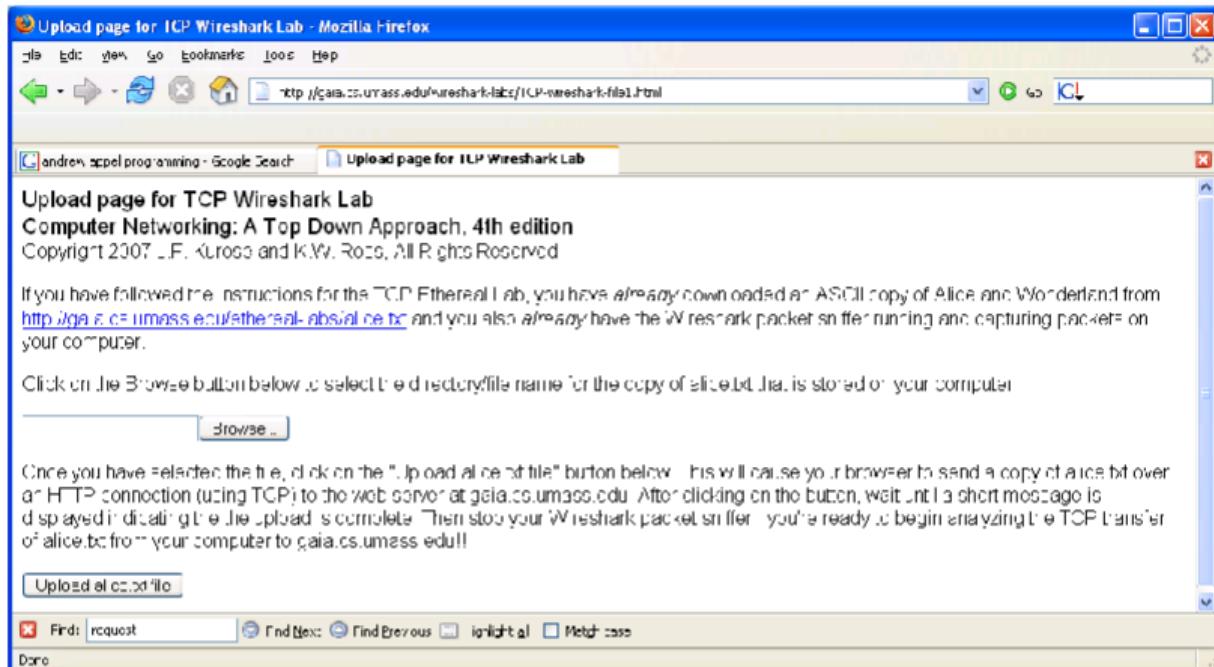
Wireshark Lab - TCP

1. Capturing a bulk TCP transfer from your computer to a remote server

Before beginning our exploration of TCP, we'll need to use Wireshark to obtain a packet trace of the TCP transfer of a file from your computer to a remote server. You'll do so by accessing a Web page that will allow you to enter the name of a file stored on your computer (which contains the ASCII text of Alice in Wonderland), and then transfer the file to a Web server using the HTTP POST method (see section 2.2.3 in the text). We're using the POST method rather than the GET method as we'd like to transfer a large amount of data from your computer to another computer. Of course, we'll be running Wireshark during this time to obtain the trace of the TCP segments sent and received from your computer.

Do the following:

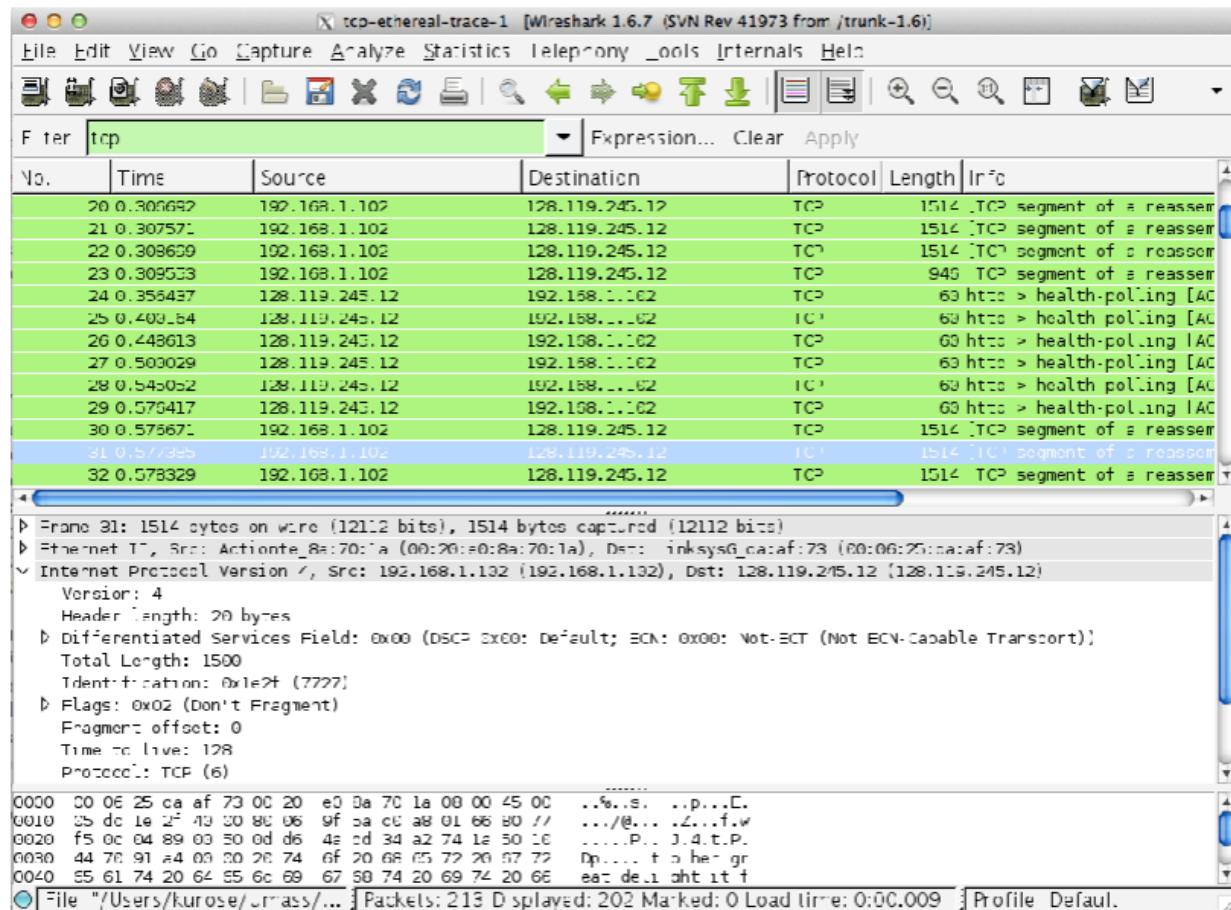
- Start up your web browser. Go the <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> and retrieve an ASCII copy of Alice in Wonderland. Store this file somewhere on your computer.
- Next go to <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.
- You should see a screen that looks like:



- Use the Browse button in this form to enter the name of the file (full path name)

on your computer containing Alice in Wonderland (or do so manually). Don't yet press the "Upload alice.txt file" button.

- Now start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Returning to your browser, press the "Upload alice.txt file" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture. Your Wireshark window should look similar to the window shown below.



If you are unable to run Wireshark on a live network connection, you can download a packet trace file that was captured while following the steps above on one of the author's computers². You may well find it valuable to download this trace even if you've captured your own trace and use it, as well as your own trace, when you explore the questions below.

2. A first look at the captured trace.

Before analyzing the behavior of the TCP connection in detail, let's take a high level

view of the trace.

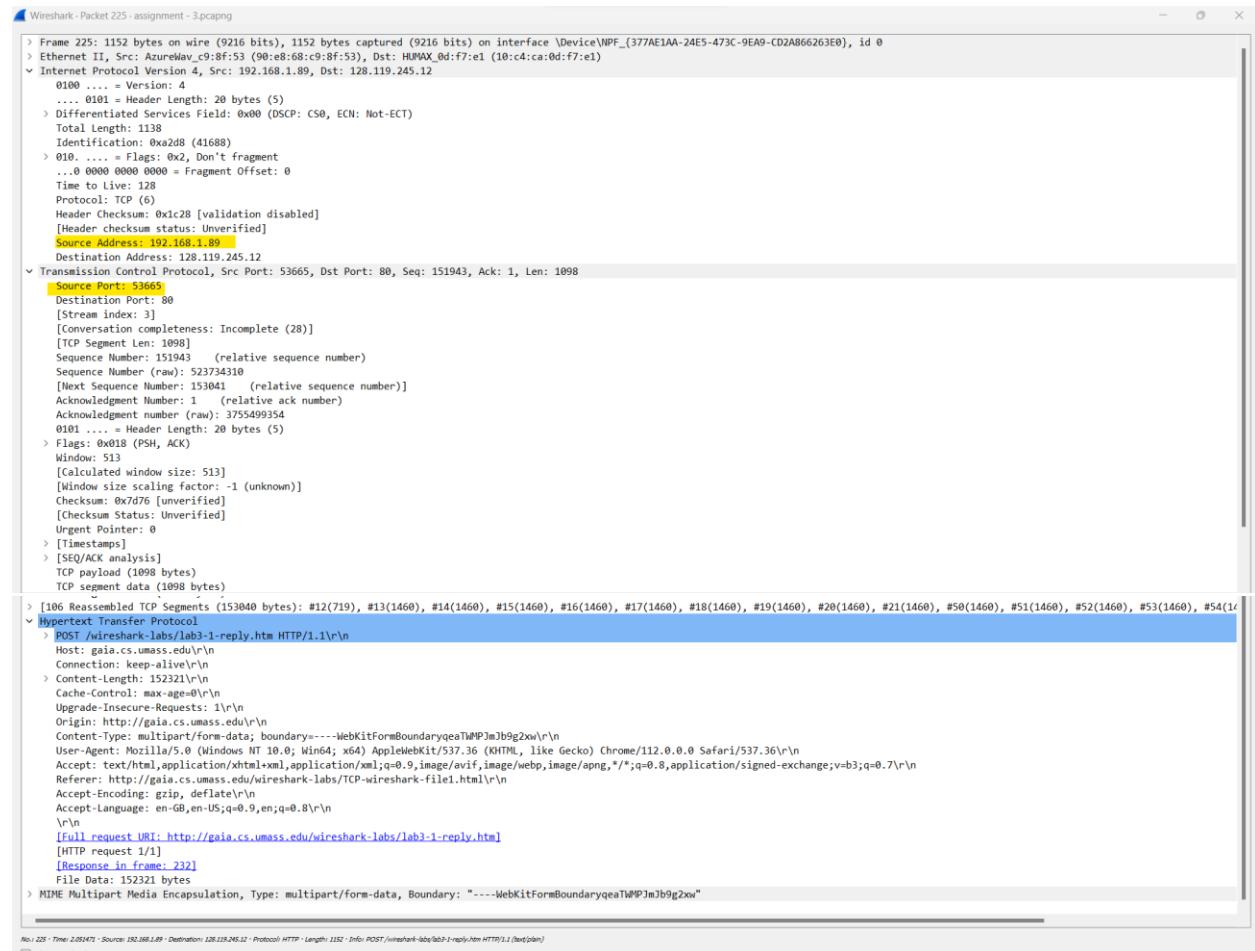
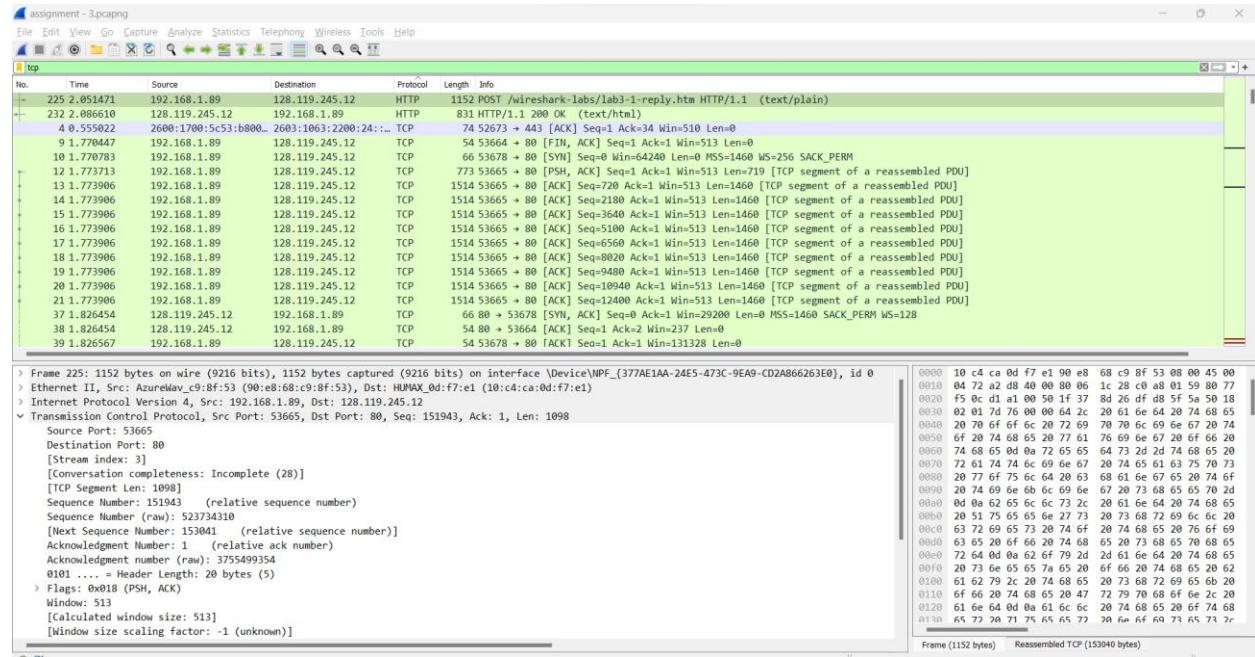
- First, filter the packets displayed in the Wireshark window by entering “tcp” (lowercase, no quotes, and don’t forget to press return after entering!) into the display filter specification window towards the top of the Wireshark window. What you should see is series of TCP and HTTP messages between your computer and gaia.cs.umass.edu. You should see the initial three-way handshake containing a SYN message. You should see an HTTP POST message. Depending on the version of Wireshark you are using, you might see a series of “HTTP Continuation” messages being sent from your computer to gaia.cs.umass.edu. Recall from our discussion in the earlier HTTP Wireshark lab, that is no such thing as an HTTP Continuation message – this is Wireshark’s way of indicating that there are multiple TCP segments being used to carry a single HTTP message. In more recent versions of Wireshark, you’ll see “[TCP segment of a reassembled PDU]” in the Info column of the Wireshark display to indicate that this TCP segment contained data that belonged to an upper layer protocol message (in our case here, HTTP). You should also see TCP ACK segments being returned from gaia.cs.umass.edu to your computer.

Answer the following questions, by opening the Wireshark captured packet file tcp-ethereal-trace-1 in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> (that is download the trace and open that trace in Wireshark; see footnote 2). Whenever possible, when answering a question, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout³ to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

1. **What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you’re uncertain about the Wireshark windows.**

IP address: 192.168.1.89 (source IP)

TCP port number: 53665 (source), 80 (destination)



2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

gaia.cs.umass.edu IP address: 128.119.245.12

Sending data on the below port:

TCP port number: 80

Wireshark - Packet 232 - assignment - 3.pcapng

Frame 232: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA0-CD2A866263E0}, id 0

> Ethernet II, Src: HUMAX_0d:f7:e8 (10:c4:ca:0d:f7:e8), Dst: AzureWave_c9:8f:53 (90:e8:68:c9:8f:53)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.89

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 817
Identification: 0xe08c (57484)
010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 45
Protocol: TCP (6)
Header Checksum: 0x32b5 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.1.89

Transmission Control Protocol, Src Port: 80, Dst Port: 53665, Seq: 1, Ack: 153041, Len: 777

Source Port: 80
Destination Port: 53665
[Stream index: 3]
[Conversation completeness: Incomplete (28)]
[TCP Segment Len: 777]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3755499354
[Next Sequence Number: 778 (relative sequence number)]
Acknowledgment Number: 153041 (relative ack number)
Acknowledgment number (raw): 523735408
0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 1432
[Calculated window size: 1432]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xb53e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (777 bytes)
> Hypertext Transfer Protocol
> Line-based text data: text/html (11 lines)

No. 232 - Time: 2.086619 - Source: 128.119.245.12 - Destination: 192.168.1.89 - Protocol: HTTP - Length: 831 - Info: HTTP/2.0 200 OK (text/html)

Show packet bytes

Receiving data on below address and port:

TCP port number: 80

Wireshark - Packet 225 - assignment - 3.pcapng

Frame 225: 1152 bytes on wire (9216 bits), 1152 bytes captured (9216 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA0-CD2A866263E0}, id 0

> Ethernet II, Src: AzureWave_c9:8f:53 (90:e8:68:c9:8f:53), Dst: HUMAX_0d:f7:e1 (10:c4:ca:0d:f7:e1)

> Internet Protocol Version 4, Src: 192.168.1.89, Dst: 128.119.245.12

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1138
Identification: 0xa2d8 (41688)
010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x1c28 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.89
Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 53665, Dst Port: 80, Seq: 151943, Ack: 1, Len: 1098

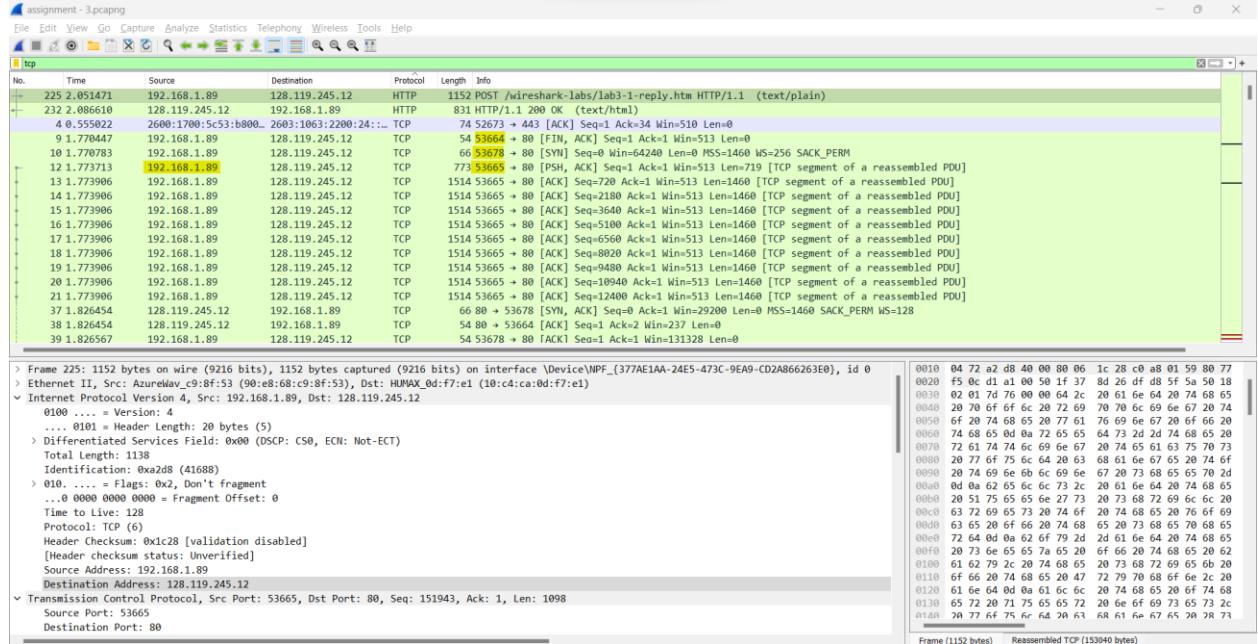
Source Port: 53665
Destination Port: 80
[Stream index: 3]
[Conversation completeness: Incomplete (28)]
[TCP Segment Len: 1098]
Sequence Number: 151943 (relative sequence number)
Sequence Number (raw): 523734310
[Next Sequence Number: 153041 (relative sequence number)]
Acknowledgment Number: 151943 (relative ack number)
Acknowledgment number (raw): 3755499354
0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 513]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xd76 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (1098 bytes)
TCP segment data (1098 bytes)

No. 225 - Time: 2.091479 - Source: 192.168.1.89 - Destination: 128.119.245.12 - Protocol: HTTP - Length: 1152 - Info: POST /view/arts-labs/2b3-1-reply.htm HTTP/1.1 (text/plain)

3. What is the IP address and TCP port number used by your client's computer (source) to transfer the file to gaia.cs.umass.edu?

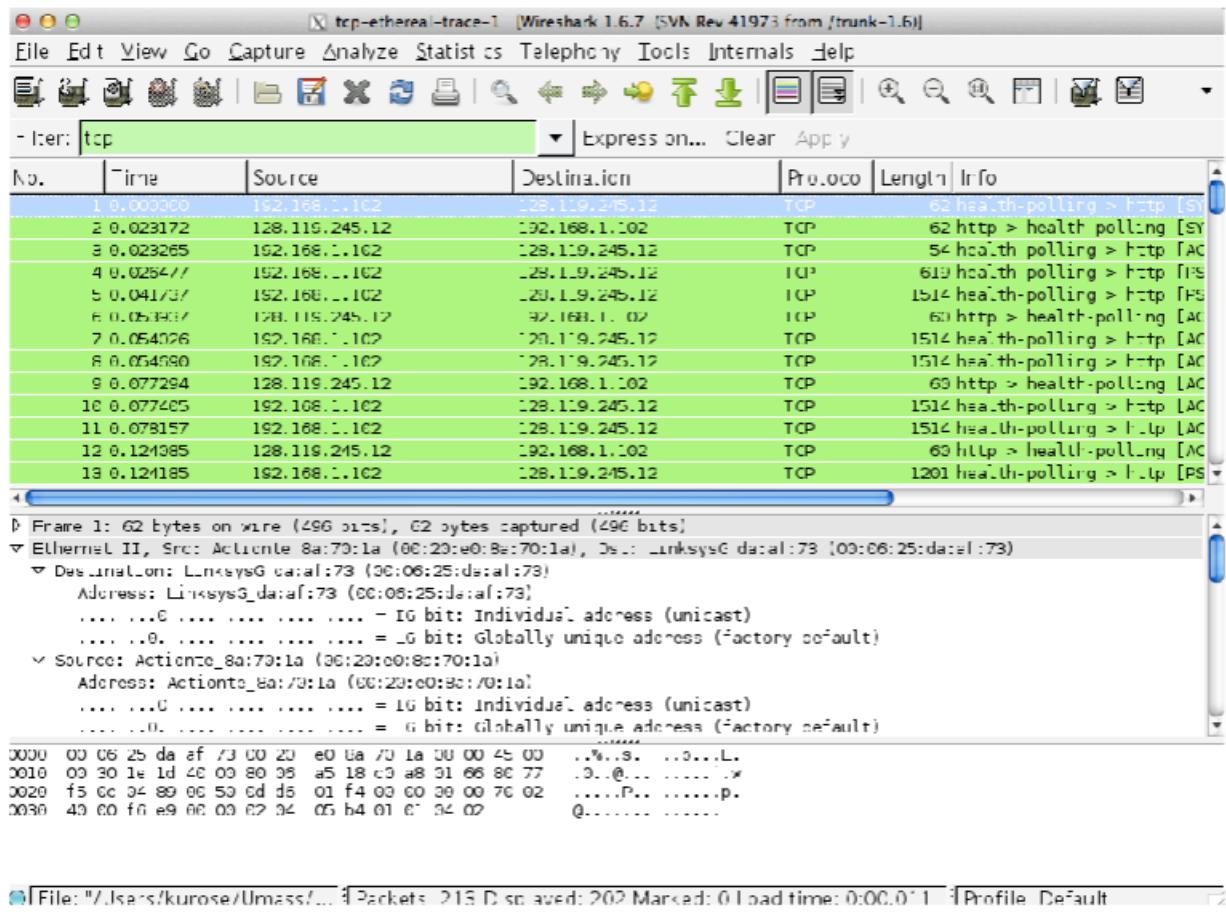
IP address: 192.168.1.89

TCP port number: 53665 is being used for the transfer of files (It is also using 53664 for FIN, ACK, and 53678 for SYN)



Since this lab is about TCP rather than HTTP, let's change Wireshark's "listing of captured packets" window so that it shows information about the TCP segments containing the HTTP messages, rather than about the HTTP messages. To have Wireshark do this, select Analyze->Enabled Protocols. Then uncheck the HTTP box and

select OK. You should now see a Wireshark window that looks like:



This is what we're looking for - a series of TCP segments sent between your computer and gaia.cs.umass.edu. We will use the packet trace that you have captured (and/or the packet trace `tcp-ethereal-trace-1` in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>; see earlier footnote) to study TCP behavior in the rest of this lab.

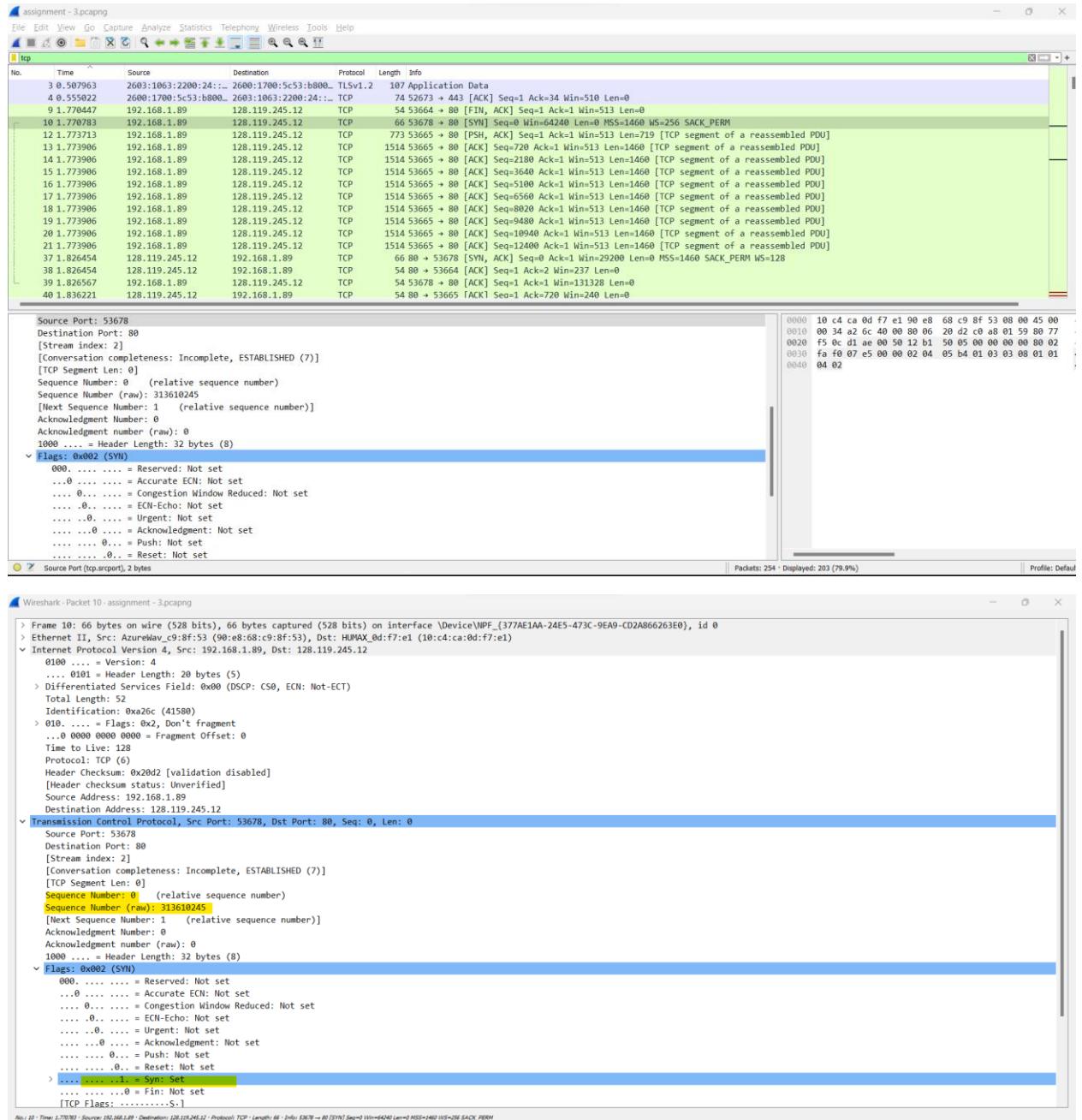
3. TCP Basics

Answer the following questions for the TCP segments:

Note: Close the tab in which you've received the congratulation.

- 4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as an SYN segment?**

The sequence number of the TCP SYN segment used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is 0. The SYN flag is set to 1 and it indicates that this segment is a SYN segment.



5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

assignment - 3.pcapng

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
19	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 80 [ACK] Seq=9480 Ack=1 Win=1460 [TCP segment of a reassembled PDU]
20	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 80 [ACK] Seq=10940 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
21	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 80 [ACK] Seq=12400 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
37	1.826454	128.119.245.12	192.168.1.89	TCP	66	80 → 53678 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
38	1.826454	128.119.245.12	192.168.1.89	TCP	54	80 → 53664 [ACK] Seq=1 Ack=2 Win=257 Len=0
39	1.826567	192.168.1.89	128.119.245.12	TCP	54	53678 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
40	1.836221	128.119.245.12	192.168.1.89	TCP	54	80 → 53665 [ACK] Seq=1 Ack=728 Win=240 Len=0
41	1.836221	128.119.245.12	192.168.1.89	TCP	54	80 → 53665 [ACK] Seq=1 Ack=2180 Win=63 Len=0
42	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=5160 Win=308 Len=0
43	1.836221	128.119.245.12	192.168.1.89	TCP	54	80 → 53665 [ACK] Seq=1 Ack=3648 Win=285 Len=0
44	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=5560 Win=331 Len=0
45	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=8020 Win=354 Len=0
46	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=9480 Win=377 Len=0
47	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=10940 Win=400 Len=0
48	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=12400 Win=422 Len=0
49	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=13860 Win=445 Len=0
50	1.836390	192.168.1.89	128.119.245.12	TCP	1514	53665 → 80 [ACK] Seq=13860 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
51	1.836390	192.168.1.89	128.119.245.12	TCP	1514	53665 → 80 [ACK] Seq=15320 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]

[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2262807227
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 313610246
1000 = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
000. = Reserved: Not set
...0 = Accurate ECH: Not set
...0.... = Congestion Window Reduced: Not set
...0.... = ECN-Echo: Not set
...0.... = Urgent: Not set
...1.... = Acknowledgment: Set
...0.... = Push: Not set
...0.... = Reset: Not set
> ...1.... = Sync: Set
...0.... = Fin: Not set
[TCP Flags:A-S.]
Window: 29200

0000 90 e8 68 c9 8f 53 10 c4 ca 0d f7 e8 08 00 45 00
0020 00 34 00 00 40 00 2d 06 16 3f 88 77 f5 0c c0 a8
0020 01 59 00 50 d1 ae 86 df b2 bb 12 b1 50 06 80 82
0030 72 18 57 1a 00 00 02 04 05 b4 01 01 04 02 01 03
0040 03 07

⊕ Acknowledgment (tcp.flags.ack), 1 byte

Packets: 254 · Displayed: 203 (79.9%)

Profile: Default

The Sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0. The raw value is 2262807227.

Wireshark - Packet 37 - assignment - 3.pcapng

> Frame 37: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: HUMAX_0d:f7:e8 (10:c4:ca:0d:f7:e8), Dst: AzureWay_c9:8f:53 (00:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.89
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x00000 (0)
> 010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 45
Protocol: TCP (6)
Header Checksum: 0x163f [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.1.89
> Transmission Control Protocol, Src Port: 80, Dst Port: 53678, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 53678
[Stream index: 2]
[Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2262807227
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 313610246
1000 = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
000. = Received: Not set
...0 = Accurate ECH: Not set
...0.... = Congestion Window Reduced: Not set
...0.... = ECN-Echo: Not set
...0.... = Urgent: Not set
...1.... = Acknowledgment: Set
...0.... = Push: Not set
...0.... = Reset: Not set
> ...1.... = Sync: Set
...0.... = Fin: Not set
[TCP Flags:A-S.]

No. 37 - Time: 1.826454 - Source: 128.119.245.12 - Destination: 192.168.1.89 - Protocol: TCP - Length: 66 - Info: 80 → 53678 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128

⊕ Show packet bytes

Close Help

The value of the Acknowledgement field in the SYNACK segment is 1. The raw value is 313610246.

```

> Frame 37: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: HUNMAX_00:ff:ff (10:4:ca:0d:f7:e8), Dst: AzureWay_c9:8f:53 (90:e8:68:c9:8f:53)
< Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.89
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
    .... 0.... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 45
    Protocol: TCP (6)
    Header Checksum: 0x163f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.1.89
< Transmission Control Protocol, Src Port: 80, Dst Port: 53678, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 53678
    [Stream index: 2]
    [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 2262807227
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 313610246
    1000 .... = Header Length: 32 bytes (8)
< Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... 0. .... = ECH-Echo: Not set
    .... 0. .... = Urgent: Not set
    .... 0.... = Push: Not set
    .... 0.... = Reset: Not set
    .... 1.... = Acknowledgment: Set
    .... 0... = Syn: Set
    .... 0.... = Fin: Not set
    [TCP Flags: ....A-S..]
No. 37 - Time: 1.626494 - Source: 128.119.245.12 - Destination: 192.168.1.89 - Protocol: TCP - Length: 66 - Info: 00 → E678 [SYN, ACK] Seq=0 Ack=1 Win=28200 Len=0 MSS=1460 SACK_PERM WS=128
 Show packet bytes

```

The value of the Acknowledgement field in the SYNACK segment is determined by gaia.cs.umass.edu by adding 1 to the initial sequence number of the SYN segment that was received from the client computer. Also, the acknowledgment number of SYN,ACK is equal to the sequence number of the next ACK segment.

The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.

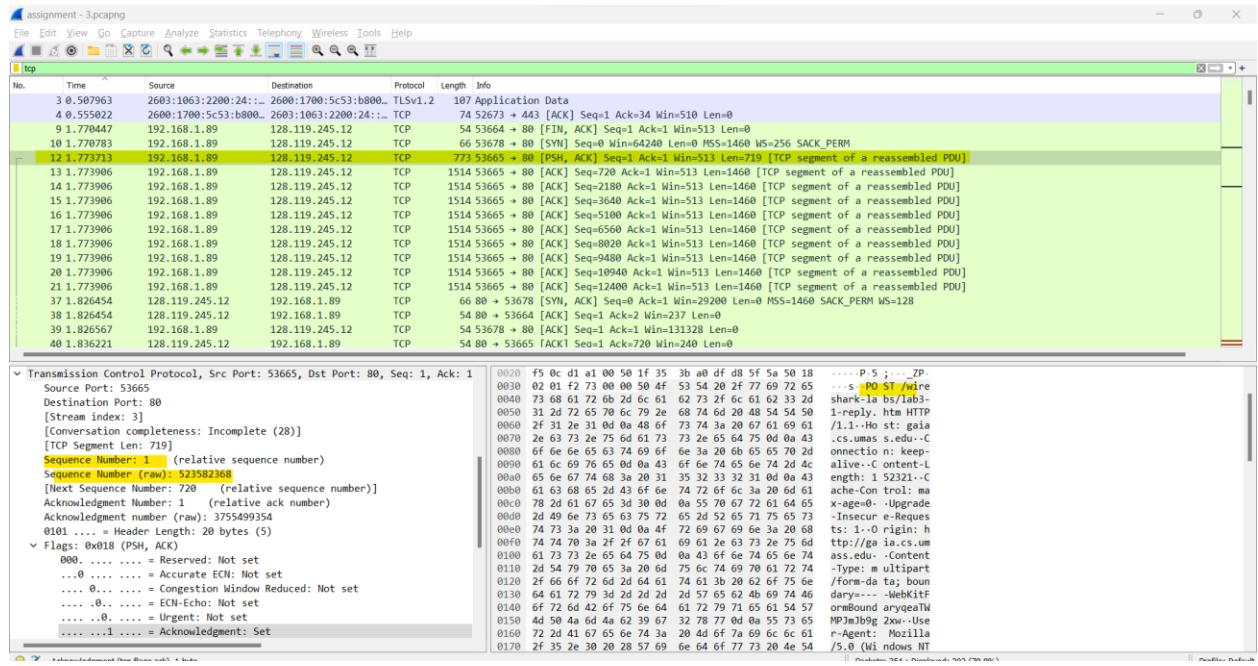
```

> Frame 37: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: HUNMAX_00:ff:ff (10:4:ca:0d:f7:e8), Dst: AzureWay_c9:8f:53 (90:e8:68:c9:8f:53)
< Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.89
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
    .... 0.... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 45
    Protocol: TCP (6)
    Header Checksum: 0x163f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.1.89
< Transmission Control Protocol, Src Port: 80, Dst Port: 53678, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 53678
    [Stream index: 2]
    [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 2262807227
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 313610246
    1000 .... = Header Length: 32 bytes (8)
< Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... 0. .... = ECH-Echo: Not set
    .... 0. .... = Urgent: Not set
    .... 0.... = Push: Not set
    .... 0.... = Reset: Not set
    .... 1.... = Acknowledgment: Set
    .... 0... = Syn: Set
    .... 0.... = Fin: Not set
    [TCP Flags: ....A-S..]
No. 37 - Time: 1.626494 - Source: 128.119.245.12 - Destination: 192.168.1.89 - Protocol: TCP - Length: 66 - Info: 00 → E678 [SYN, ACK] Seq=0 Ack=1 Win=28200 Len=0 MSS=1460 SACK_PERM WS=128
 Show packet bytes

```

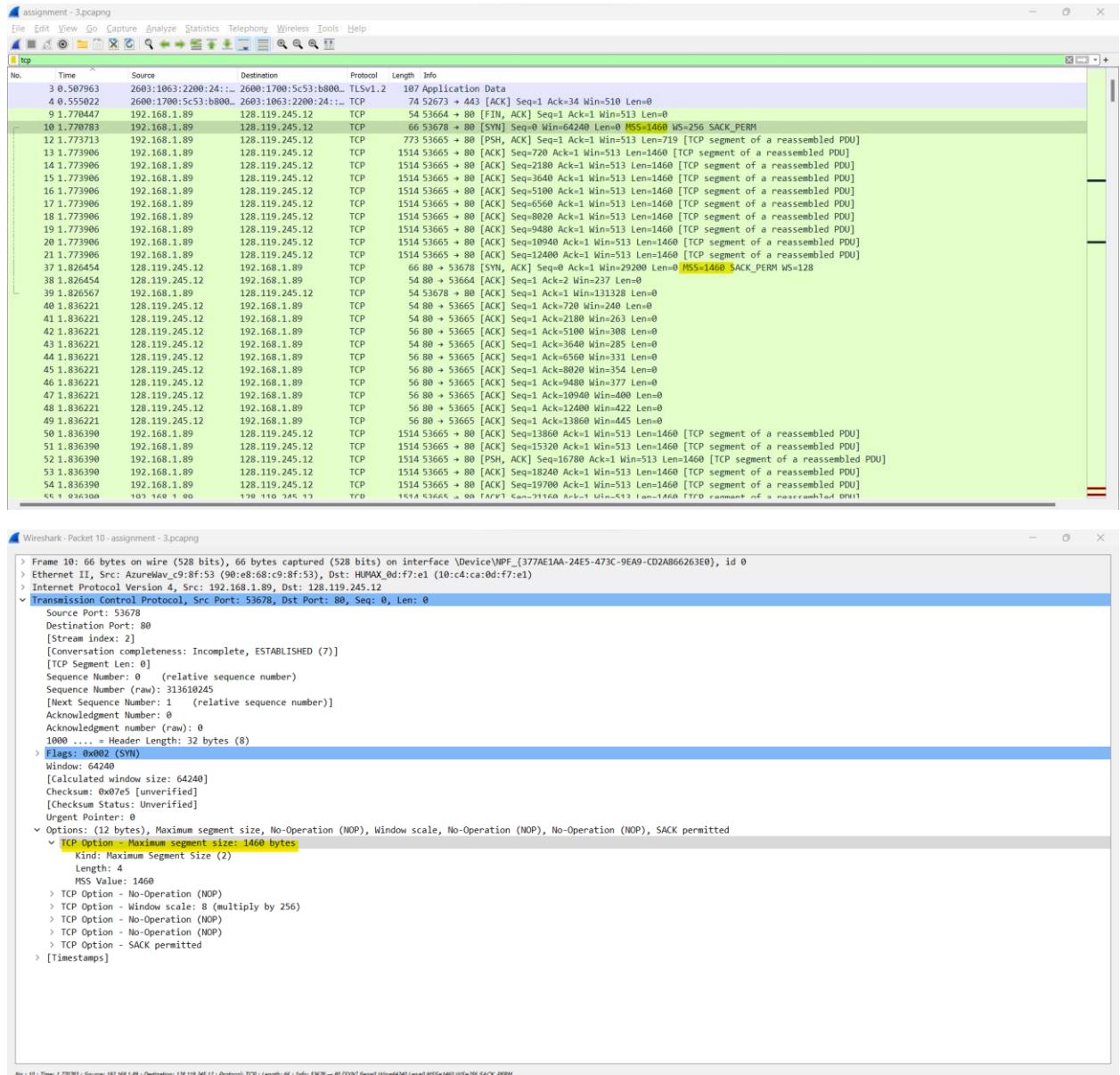
- 6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a “POST” within its DATA field.**

The sequence number of the TCP segment containing the HTTP POST command is 1. The raw value is 523582368.



- 7. What is the maximum segment size in the first ACK by the server?**

MSS = 1460 (It is found in SYN or SYN, ACK segments, in other segments its indicated using the length field)



8. What is the round-trip time(RRT) for the ACK received by the server?

Round trip time by taking the time difference between the SYN and the SYN/ACK packets.

We can Calculate the RTT by subtracting the timestamp of the original data packet from the client and the timestamp of the ACK packet from the server.

$$\text{RTT} = 17:34:50.795298000 - 17:34:50.85761300 = 0.062315$$

Or

$$\text{RTT} = 0.062508000 - 0.000193000 = 0.062315$$

The packets are highlighted below:

assignment - 3.pcapng

tcp.stream eq 3						
No.	Time	Source	Destination	Protocol	Length	Info
225	2.051471	192.168.1.89	128.119.245.12	HTTP	1152	POST /wireshark-k-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
232	2.086610	128.119.245.12	192.168.1.89	HTTP	831	HTTP/1.1 200 OK (text/html)
13	1.773713	192.168.1.89	128.119.245.12	TCP	773	53665 → 88 [PSH, ACK] Seq=1 Ack=1 Win=513 Len=719 [TCP segment of a reassembled PDU]
14	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=720 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
15	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=3640 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
16	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=5160 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
17	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=6560 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
18	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=8028 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
19	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=9480 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
20	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=10940 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
21	1.773906	192.168.1.89	128.119.245.12	TCP	1514	53665 → 88 [ACK] Seq=12400 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]
40	1.836221	128.119.245.12	192.168.1.89	TCP	54	80 → 53665 [ACK] Seq=1 Ack=720 Win=240 Len=0
41	1.836221	128.119.245.12	192.168.1.89	TCP	54	80 → 53665 [ACK] Seq=1 Ack=2180 Win=263 Len=0
42	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=5100 Win=308 Len=0
43	1.836221	128.119.245.12	192.168.1.89	TCP	54	80 → 53665 [ACK] Seq=1 Ack=3640 Win=285 Len=0
44	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=6560 Win=331 Len=0
45	1.836221	128.119.245.12	192.168.1.89	TCP	56	80 → 53665 [ACK] Seq=1 Ack=8028 Win=354 Len=0

Wireshark - Packet 13 - assignment - 3.pcapng

Arrival Time: Apr 15, 2023 17:34:50.795298000 Central Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1681598090.795298000 seconds
[Time delta from previous captured frame: 0.000193000 seconds]
[Time delta from previous displayed frame: 0.000193000 seconds]
[Time since reference or first frame: 1.773906000 seconds]
Frame Number: 13
Frame Length: 1514 bytes (12112 bits)
Capture Length: 1514 bytes (12112 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:etherype:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: Azurekav_c9:8f:53 (90:8f:68:c9:8f:53), Dst: HUMAX_0d:f7:e1 (10:c4:ca:0d:f7:e1)
> Internet Protocol Version 4, Src: 192.168.1.89, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53665, Dst Port: 80, Seq: 720, Ack: 1, Len: 1460
Source Port: 53665
Destination Port: 80
[Stream index: 3]
[Conversation completeness: Incomplete (28)]
[TCP Segment Len: 1460]
Sequence Number: 720 (relative sequence number)
Sequence Number (raw): 52358387
[Next Sequence Number: 2180 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3755499354
0101 = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window: 513
[Calculated window size: 513]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xd1df [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
< [Timestamps]
[Time since first frame in this TCP stream: 0.000193000 seconds]
[Time since previous frame in this TCP stream: 0.000193000 seconds]
< [SEQ/ACK analysis]
[Bytes in flight: 2179]

No.: 13 | Time: 1.773906 | Source: 192.168.1.89 | Destination: 128.119.245.12 | Protocol: TCP | Length: 1514 | Info: 53665 → 80 [ACK] Seq=720 Ack=1 Win=513 Len=1460 [TCP segment of a reassembled PDU]

Show packet bytes

```

Wireshark - Packet 40 - assignment - 3.pcapng
Encapsulation type: Ethernet (1)
Arrival time: Apr 15, 2023 17:34:50.857613000 Central Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch time: 1681598090.857613000 seconds
[Time delta from previous captured frame: 0.009654000 seconds]
[Time delta from previous displayed frame: 0.062315000 seconds]
[Time since reference or first frame: 1.836221000 seconds]
Frame Number: 40
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ether:type:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: HUMAX_0d:f7:e8 (10:c4:ca:0d:f7:e8), Dst: AzureWave_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.89
> Transmission Control Protocol, Src Port: 80, Dst Port: 53665, Seq: 1, Ack: 720, Len: 0
    Source Port: 80
    Destination Port: 53665
    [Stream index: 3]
    [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 0]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 3755499354
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 720 (relative ack number)
    Acknowledgment number (raw): 523583087
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 240
    [Calculated window size: 240]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x0896 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > [Timestamps]
        [Time since first frame in this TCP stream: 0.062508000 seconds]
        [Time since previous frame in this TCP stream: 0.062315000 seconds]
    > [SEQ/ACK analysis]

```

9. What is the calculated window size and checksum in the HTTP first packet?

The window field controls the flow of data. It is a new window size that has been requested.

The checksum field is to ensure that the TCP segment reaches the destination without any errors. It is used for error detection.

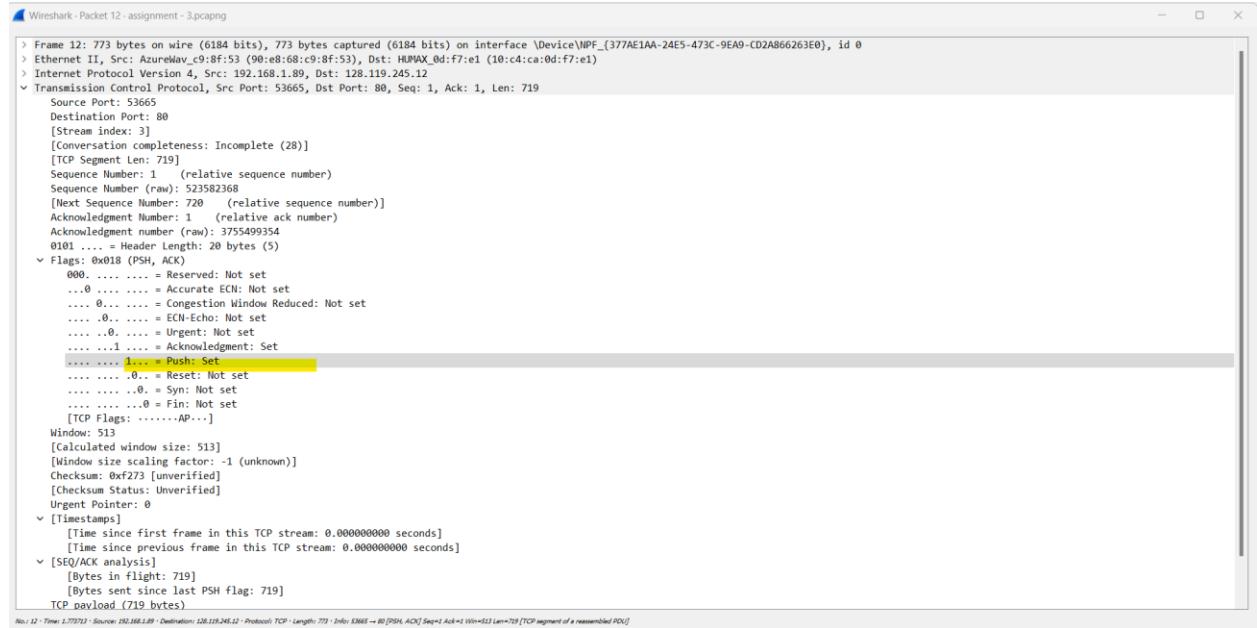
```

Wireshark - Packet 225 - assignment - 3.pcapng
> Frame 225: 1152 bytes on wire (9216 bits), 1152 bytes captured (9216 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: AzurWave_c9:8f:53 (90:e8:68:c9:8f:53), Dst: HUMAX_0d:f7:e1 (10:c4:ca:0d:f7:e1)
> Internet Protocol Version 4, Src: 192.168.1.89, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53665, Dst Port: 80, Seq: 151943, Ack: 1, Len: 1098
    Source Port: 53665
    Destination Port: 80
    [Stream index: 3]
    [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 1098]
    Sequence Number: 151943 (relative sequence number)
    Sequence Number (raw): 523734310
    [Next Sequence Number: 153045 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 3755499354
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x0108 (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: 513
    [Calculated window size: 513]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x7d76 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > [Timestamps]
    > [SEQ/ACK analysis]
    TCP payload (1098 bytes)
    TCP segment data (1098 bytes)
    > [106 Reassembled TCP Segments (153040 bytes): #12(719), #13(1460), #14(1460), #15(1460), #16(1460), #17(1460), #18(1460), #19(1460), #20(1460), #21(1460), #50(1460), #51(1460), #52(1460), #53(1460), #54(1460)]
    > Hypertext Transfer Protocol

```

10. Is the PUSH flag set? If yes? What is its significance?

Yes, the PUSH flag is set. The PUSH flag instructs the receiving application to process the data as soon as possible rather than waiting for additional data to arrive, which can enhance the program's overall performance. Additionally, it can serve as a reminder for the sender to transmit data as soon as feasible.



Wireshark - Packet 12 - assignment - 3.pcapng

```

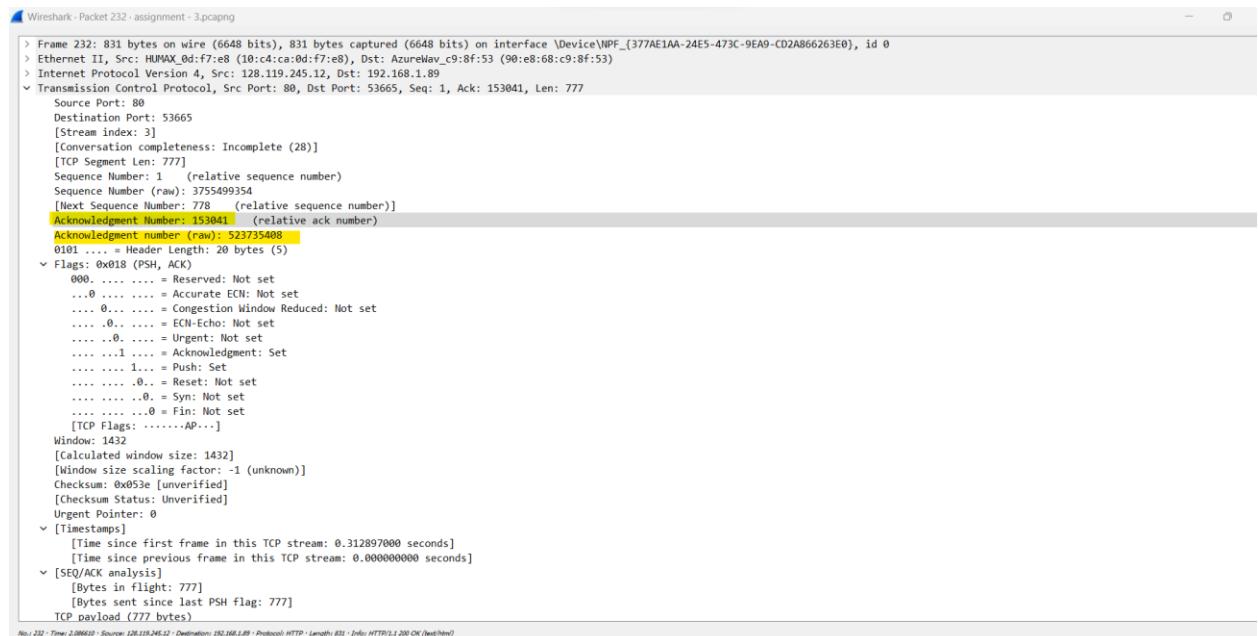
> Frame 12: 773 bytes on wire (6184 bits), 773 bytes captured (6184 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-C02A866263E0}, id 0
> Ethernet II, Src: AzureNav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: HUMAX_0d:f7:e1 (10:c4:ca:0d:f7:e1)
> Internet Protocol Version 4, Src: 192.168.1.89, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53665, Dst Port: 80, Seq: 1, Ack: 1, Len: 719
    Source Port: 53665
    Destination Port: 80
    [Stream index: 3]
    [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 719]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 523582368
    [Next Sequence Number: 720 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 3755499354
    0101 .... = Header Length: 20 bytes (5)
    < 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: 513
    [Calculated window size: 513]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xf273 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    < [Timestamps]
        [Time since first frame in this TCP stream: 0.000000000 seconds]
        [Time since previous frame in this TCP stream: 0.000000000 seconds]
    > [SEQ/ACK analysis]
        [Bytes in flight: 719]
        [Bytes sent since last PSH flag: 719]
    TCP payload (719 bytes)

```

No. 12 - Time: 1.770723 - Source: 192.168.1.89 - Destination: 128.119.245.12 - Protocol: TCP - Length: 773 - Info: X3665 → 80 [PSH, ACK] Seq=1 Ack=1 Win=513 Len=719 [TCP segment of a reassembled PDU]

11. What are the font face and acknowledgment number of the HTTP packet which has the status of 200 OK?

The font face is Arial, Helvetica, and Sans-serif. The acknowledgment number is 153041.



Wireshark - Packet 232 - assignment - 3.pcapng

```

> Frame 232: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-C02A866263E0}, id 0
> Ethernet II, Src: HUMAX_0d:f7:e8 (10:c4:ca:0d:f7:e8), Dst: AzureNav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.89
> Transmission Control Protocol, Src Port: 80, Dst Port: 53665, Seq: 1, Ack: 153041, Len: 777
    Source Port: 80
    Destination Port: 53665
    [Stream index: 3]
    [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 777]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 3755499354
    [Next Sequence Number: 778 (relative sequence number)]
    Acknowledgment Number: 153041 (relative ack number)
    Acknowledgment number (raw): 523735408
    0101 .... = Header Length: 20 bytes (5)
    < 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: 1432
    [Calculated window size: 1432]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x053a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    < [Timestamps]
        [Time since first frame in this TCP stream: 0.312897000 seconds]
        [Time since previous frame in this TCP stream: 0.000000000 seconds]
    > [SEQ/ACK analysis]
        [Bytes in flight: 777]
        [Bytes sent since last PSH flag: 777]
    TCP payload (777 bytes)

```

No. 232 - Time: 2.086610 - Source: 128.119.245.12 - Destination: 192.168.1.89 - Protocol: HTTP - Length: 831 - Info: HTTP/1.1 200 OK (text/html)

```

Checksum: 0xb93e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
▼ [Timestamps]
  [Time since first frame in this TCP stream: 0.312897000 seconds]
  [Time since previous frame in this TCP stream: 0.000000000 seconds]
▼ [SEQ/ACK analysis]
  [Bytes sent since last PSH flag: 777]
  [TCP payload (777 bytes)]
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 15 Apr 2023 22:34:50 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 06 Feb 2021 18:23:47 GMT\r\n
    ETag: "1a2-5baaf9ab0d709"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 418\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.035139000 seconds]
  [Request in frame: 255]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm]
  File Data: 418 bytes
▼ Line-based text data: text/html (11 lines)
<TITLE>Upload page for TCP Wireshark Lab</TITLE>\n<body color="#FFFFFF">\n<p><font face="Arial, Helvetica, sans-serif" size="4"> Congratulations! <br> </font>\n<br>\n<p><font face="Arial, Helvetica, sans-serif"> You've now transferred a copy of alice.txt from\nyour computer to \n\n<br>\n</font>\n</p>\n</body>\n</html>

```

12. How is the connection closed? (Hint: FIN flag) Attach the screenshot of the flags which are set at the end?

The FIN flag is used to indicate that the sender has no more data to send.

There are three ways a TCP connection is closed:

- By sending a FIN packet to the server, the client takes the initiative to cut off the connection.
- By sending a FIN packet to the client, the server starts the connection from being closed.
- The connection is cut off by both the client and the server.

The ACK and FIN flags are set at the end.

Frame 9: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{377E1AA-24E5-473C-9EA9-C02A866263E0}, id 0

Ethernet II, Src: AzuréMav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: HUMAX_0d:f7:e1 (10:c4:ca:0d:f7:e1)

Internet Protocol Version 4, Src: 192.168.1.89, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 53664, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 53664
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3616110415
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2782149289
0101 = Header Length: 20 bytes (5)
Flags: 0x0111 (FIN, 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
....0.... = Push: Not set
....0.... = Reset: Not set
....0.... = Syn: Not set
>0.... = Fin: Set
> [TCP Flags:A..F]
Window: 513
[Calculated window size: 513]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x7505 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]

13. Who has set the FIN bit? Is it server or client? Attach the screenshot.

The client set the FIN flag first.

The FIN flag is set in two packets:

1. Frame 9: Source IP - 192.168.1.89 (Client), Destination IP - 128.119.245.12 (Server)
2. Frame 251: Source IP - 128.119.245.12 (Server), Destination IP - 192.168.1.89 (Client)

Ethernet II, Src: AzuréMav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: HUMAX_0d:f7:e1 (10:c4:ca:0d:f7:e1)

Internet Protocol Version 4, Src: 192.168.1.89, Dst: 128.119.245.12

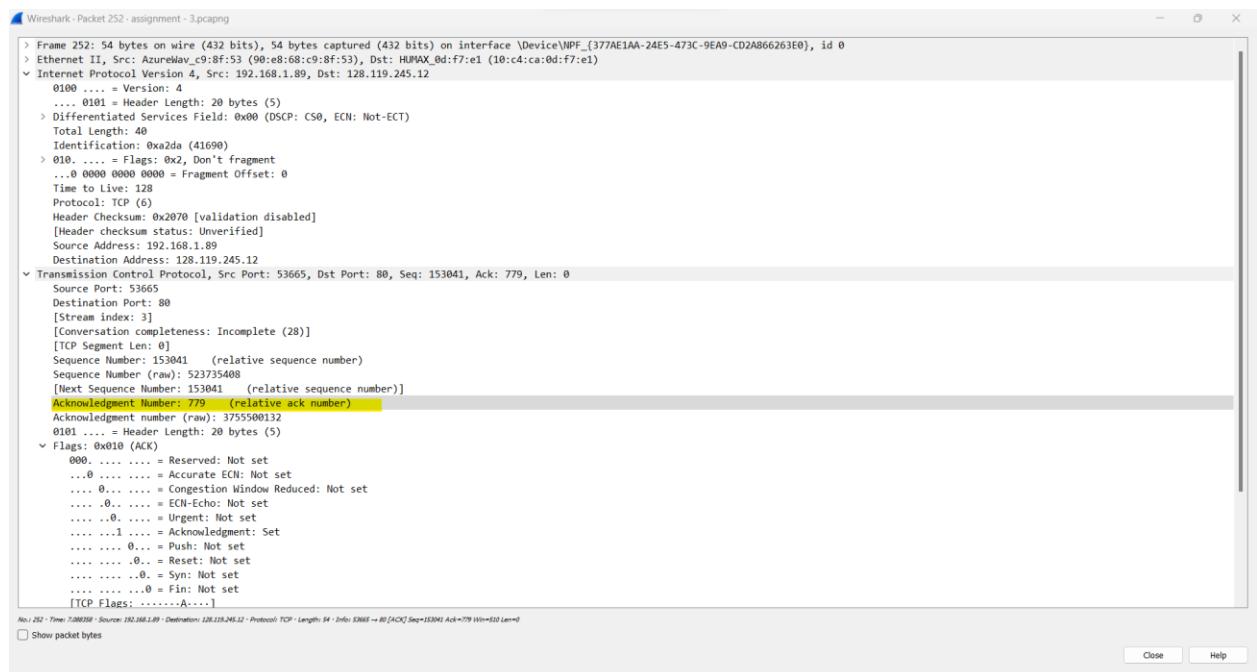
0100 = Version: 4
....001 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DS2P: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xa26b (41579)
> 010 = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x20df [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.89
Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 53664, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 53664
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3616110415
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2782149289
0101 = Header Length: 20 bytes (5)
Flags: 0x0111 (FIN, 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
....0.... = Push: Not set
....0.... = Reset: Not set
....0.... = Syn: Not set
>1.... = Fin: Set
> [TCP Flags:A..F]
Window: 513

14. What is the acknowledgment number of the last TCP ACK?

The acknowledgment number of the last TCP ACK is 779.



Wireshark - Packet 252 - assignment - 3.pcapng

> Frame 252: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0

> Ethernet II, Src: AzureMav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: HUMAX_0d:f7:e1 (10:c4:ca:0d:f7:e1)

Internet Protocol Version 4, Src: 192.168.1.89, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0xa2da (41690)

010. = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x2070 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.89

Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 53665, Dst Port: 80, Seq: 153041, Ack: 779, Len: 0

Source Port: 53665

Destination Port: 80

[Stream index: 3]

[Conversation completeness: Incomplete (28)]

[TCP Segment Len: 0]

Sequence Number: 153041 (relative sequence number)

Sequence Number (raw): 523735408

[Next Sequence Number: 153041 (relative sequence number)]

Acknowledgment Number: 779 (relative ack number)

Acknowledgment number (raw): 3755500132

0101 = Header Length: 20 bytes (5)

Flags: 0x010 (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

.... 0... = Push: Not set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

[TCP Flags:A....]

No. 252 - Time: 7.080398 - Source: 192.168.1.89 - Destination: 128.119.245.12 - Protocol: TCP - Length: 54 - Info: 53665 → 80 [ACK] Seq=153041 Ack=779 Win=120 Len=0

Show packet bytes

Close Help