

Wireshark Lab 3

Jennifer Hurst

My IP address is shown below, 192.168.1.17 in this terminal screen shot.

The image shows a Wireshark network traffic capture. The top pane displays a list of 189 packets. The 'Destination' column for the first few packets is circled in red, showing the IP address 192.168.1.17. The bottom pane shows the details of the selected packet (Frame 1: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0). The packet is identified as Ethernet II, Src: HewlettP_10:65:3e (70:5a:0f:10:65:3e), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02). The Internet Protocol Version 6, Src: fe80::725a:fff:fe10:653e, Dst: ff02::1:2. The User Datagram Protocol, Src Port: 546, Dst Port: 547. The DHCPv6 section shows the packet type as NPI10653 and the length as 45.

No.	Time	Source	Destination	Protocol	Length	Info
180	17:02:11.091216	54.186.163.246	192.168.1.17	TCP	60	443 → 55147 [ACK] Seq=3015 Ack=1448 Win=31356 Len=0
181	17:02:11.091275	54.186.163.246	192.168.1.17	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
182	17:02:11.092082	54.186.163.246	192.168.1.17	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
183	17:02:11.097283	54.186.163.246	192.168.1.17	TLSv1.2	309	Application Data
184	17:02:11.097364	192.168.1.17	54.186.163.246	TCP	54	55147 → 443 [ACK] Seq=1448 Ack=3321 Win=63934 Len=0
185	17:02:11.098654	54.186.163.246	192.168.1.17	TLSv1.2	309	Application Data
186	17:02:11.098722	192.168.1.17	54.186.163.246	TCP	54	55148 → 443 [ACK] Seq=1448 Ack=3321 Win=63934 Len=0
187	17:02:11.502539	35.163.53.118	192.168.1.17	TLSv1.2	85	Application Data
188	17:02:11.504665	192.168.1.17	35.163.53.118	TLSv1.2	89	Application Data
189	17:02:11.638725	35.163.53.118	192.168.1.17	TCP	60	443 → 54984 [ACK] Seq=32 Ack=36 Win=119 Len=0

> Frame 1: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0
> Ethernet II, Src: HewlettP_10:65:3e (70:5a:0f:10:65:3e), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::725a:fff:fe10:653e, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
> DHCPv6

0000 33 33 00 01 00 02 70 5a 0f 10 65 3e 86 dd 60 00 33...pZ...e>...
0010 00 00 00 6b 11 01 fe 80 00 00 00 00 00 00 72 5a ...k...rZ
0020 0f ff fe 10 65 3e ff 02 00 00 00 00 00 00 00 00 ...e>...
0030 00 00 00 01 00 02 02 22 02 23 00 6b 41 f1 01 b1 ...#kA...
0040 ec 49 00 08 00 02 ff ff 00 01 00 0a de ad be ef .I.....
0050 de ad be ef de ad 00 03 00 28 00 00 00 02 00 00
0060 38 40 00 00 54 60 00 05 00 18 00 00 00 00 00 00 8@..T...
0070 00 00 00 00 00 00 00 00 00 00 00 00 70 80 00 00p...
0080 8c a0 00 06 00 0c 00 0d 00 0c 00 17 00 18 00 27
0090 00 07 00 27 00 0b 01 09 4e 50 49 31 30 36 35 33NPI10653
00a0 45 E

1. What is the **TCP port number** used by your computer to communicate with gaia.cs.umass.edu? The TCP port number is 55163

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
724	17:02:58.031243	192.168.1.17	52.114.158.52	TCP	54	55164 → 443 [ACK] Seq=7224 Ack=6154 Win=261376 Len=0
727	17:02:59.655264	52.1.140.142	192.168.1.17	TLSv1.2	85	Encrypted Alert
728	17:02:59.655387	192.168.1.17	52.1.140.142	TCP	54	55141 → 443 [ACK] Seq=1 Ack=32 Win=1021 Len=0
729	17:02:59.935272	128.119.245.12	192.168.1.17	TCP	60	80 → 55163 [FIN, ACK] Seq=778 Ack=152894 Win=262912 Len=0
730	17:02:59.935392	192.168.1.17	128.119.245.12	TCP	54	55163 → 80 [ACK] Seq=152894 Ack=779 Win=64768 Len=0
731	17:02:59.935559	192.168.1.17	128.119.245.12	TCP	54	55163 → 80 [FIN, ACK] Seq=152894 Ack=779 Win=64768 Len=0
732	17:02:59.963567	128.119.245.12	192.168.1.17	TCP	60	80 → 55163 [ACK] Seq=779 Ack=152895 Win=262912 Len=0
733	17:03:00.932982	192.168.1.17	13.107.42.12	TCP	66	55165 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
734	17:03:00.934706	192.168.1.17	13.107.42.12	TCP	66	55166 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
735	17:03:00.936648	192.168.1.17	13.107.42.12	TCP	66	55167 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 730: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 > Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear_bd73:8c (50:6a:03:bd:73:8c)
 > Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 55163, Dst Port: 80, Seq: 152894, Ack: 779, Len: 0

0000 50 6a 03 bd 73 8c 98 ee cb 7e 38 bb 08 00 45 00 Pj...s... ..8...E-
 0010 00 28 55 59 40 00 00 06 00 00 c0 a8 01 11 80 77 (UY@... ..w
 0020 f5 0c d7 7b 00 50 27 42 9a fa 44 a1 98 43 50 10 ...{P'B ..D..CP-
 0030 00 fd 37 58 00 00 ..7X..

Transmission Control Protocol: Protocol

Packets: 819 · Displayed: 770 (94.0%) · Dropped: 0 (0.0%) Profile: Default

Type here to search

5:08 PM 2/17/2019

2. What is the **TCP port number used by gaia.cs.umass.edu** to communicate with your computer? The port number is 80

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
724	17:02:58.031243	192.168.1.17	52.114.158.52	TCP	54	55164 → 443 [ACK] Seq=7224 Ack=6154 Win=261376 Len=0
727	17:02:59.655264	52.1.140.142	192.168.1.17	TLSv1.2	85	Encrypted Alert
728	17:02:59.655387	192.168.1.17	52.1.140.142	TCP	54	55141 → 443 [ACK] Seq=1 Ack=32 Win=1021 Len=0
729	17:02:59.935272	128.119.245.12	192.168.1.17	TCP	60	80 → 55163 [FIN, ACK] Seq=778 Ack=152894 Win=262912 Len=0
730	17:02:59.935392	192.168.1.17	128.119.245.12	TCP	54	55163 → 80 [ACK] Seq=152894 Ack=779 Win=64768 Len=0
731	17:02:59.935559	192.168.1.17	128.119.245.12	TCP	54	55163 → 80 [FIN, ACK] Seq=152894 Ack=779 Win=64768 Len=0
732	17:02:59.963567	128.119.245.12	192.168.1.17	TCP	60	80 → 55163 [ACK] Seq=779 Ack=152895 Win=262912 Len=0
733	17:03:00.932982	192.168.1.17	13.107.42.12	TCP	66	55165 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
734	17:03:00.934706	192.168.1.17	13.107.42.12	TCP	66	55166 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
735	17:03:00.936648	192.168.1.17	13.107.42.12	TCP	66	55167 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 730: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 > Ethernet II, Src: WistronI_7e:38:bb (98:ee:cb:7e:38:bb), Dst: Netgear_bd73:8c (50:6a:03:bd:73:8c)
 > Internet Protocol Version 4, Src: 192.168.1.17, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 55163, Dst Port: 80, Seq: 152894, Ack: 779, Len: 0

0000 50 6a 03 bd 73 8c 98 ee cb 7e 38 bb 08 00 45 00 Pj...s... ..8...E-
 0010 00 28 55 59 40 00 00 06 00 00 c0 a8 01 11 80 77 (UY@... ..w
 0020 f5 0c d7 7b 00 50 27 42 9a fa 44 a1 98 43 50 10 ...{P'B ..D..CP-
 0030 00 fd 37 58 00 00 ..7X..

Transmission Control Protocol: Protocol

Packets: 819 · Displayed: 770 (94.0%) · Dropped: 0 (0.0%) Profile: Default

Type here to search

5:10 PM 2/17/2019

3. What is the **sequence number of the TCP SYN** segment that is used to initiate the TCP connection between your computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment? The sequence number of the TCP SYN segment is 0. In the Flags section, the SYN flag is set to 1 which indicates that this segment is a SYN segment.

The image shows a Wireshark packet capture of a TCP connection. The packet list pane shows a SYN segment from 192.168.1.17 to 128.119.245.12. The packet details pane shows the following information:

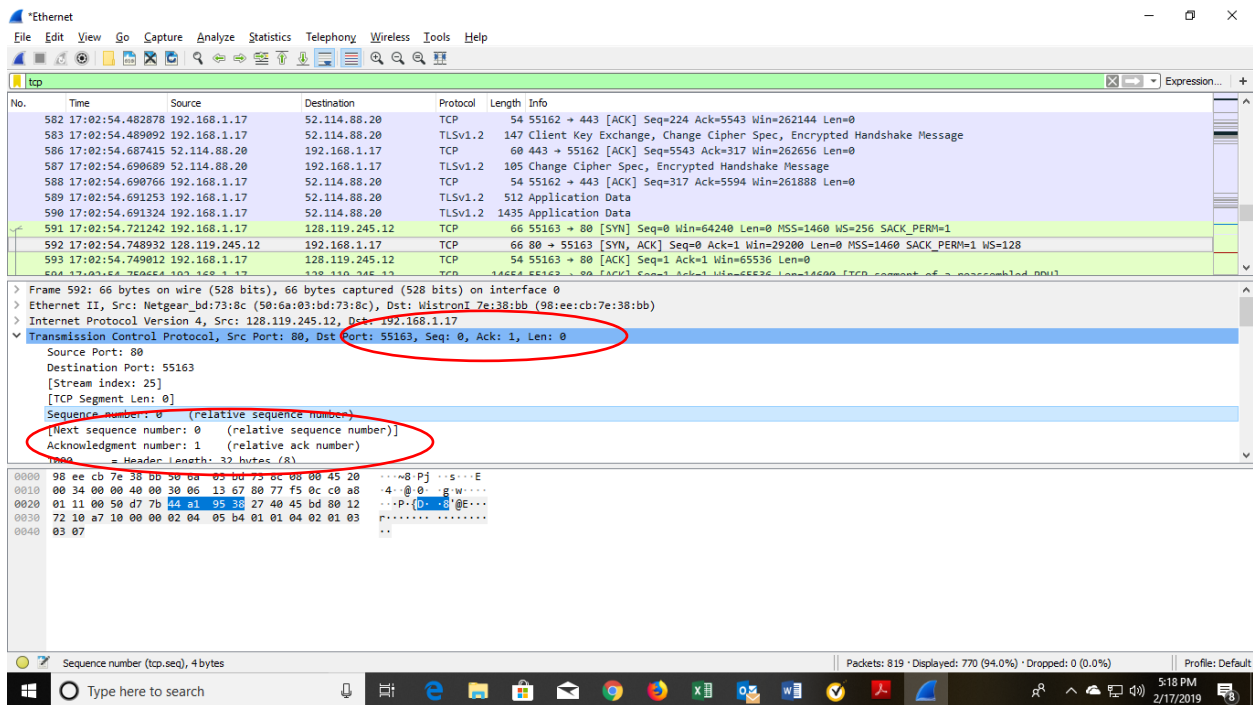
- Flags:** 0x002 (SYN)
 - ...0... = Reserved: Not set
 - ...0... = Nonce: Not set
 - ...0... = Congestion Window Reduced (CWR): Not set
 - ...0... = ECN-Echo: Not set
 - ...0... = Urgent: Not set
 - ...0... = Acknowledgment: Not set
 - ...0... = Push: Not set
 - ...0... = Reset: Not set
 - ...1... = Syn: Set
- [Expert Info (Chat/Sequence):]** Connection establish request (SYN): server port 80
- [Connection establish request (SYN): server port 80]**

The packet bytes pane shows the raw data of the SYN segment:

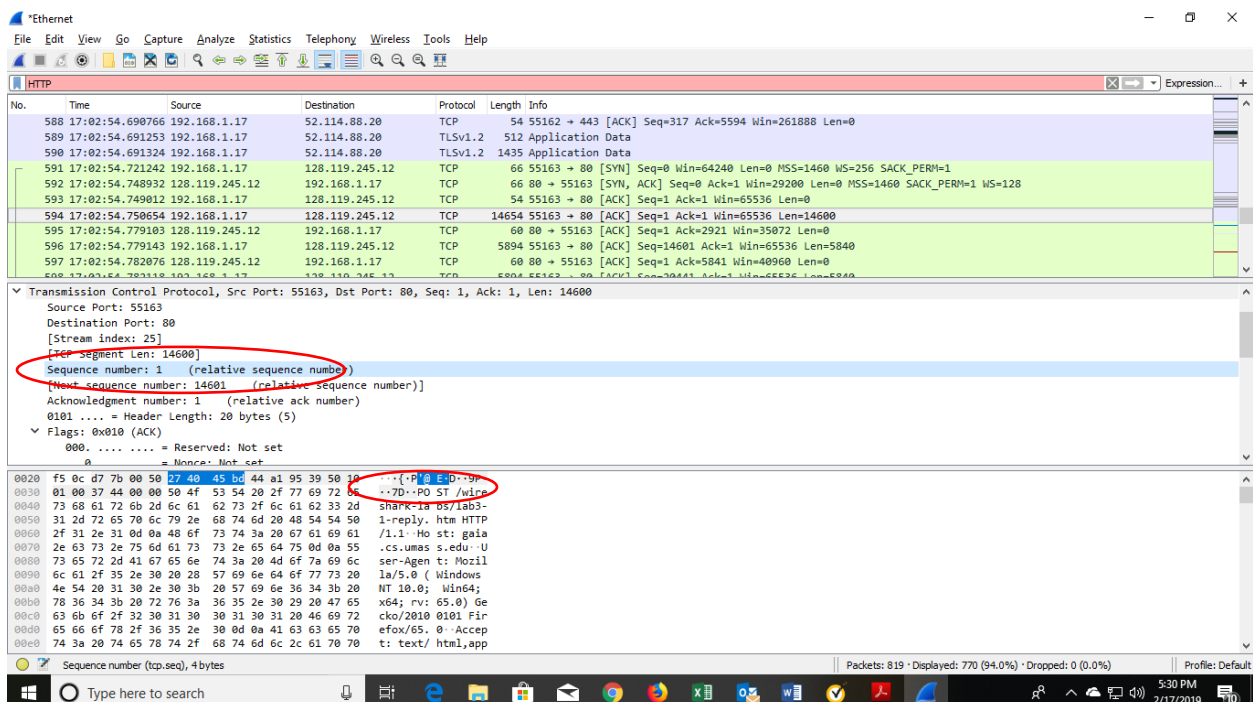
```

0000 50 6a 03 bd 73 8c 98 ee cb 7e 38 bb 08 00 45 00  Pj...s... ..8...E
0010 00 34 54 d9 40 00 80 06 00 00 c0 a8 01 11 80 77  4T.0.....w
0020 f5 0c 07 70 00 50 27 40 45 0c 00 00 60 00 00 02  [P]@E.....
0030 fa f0 37 64 00 00 02 04 05 b4 01 03 05 08 01 01  7d.....
0040 04 02
  
```

4. What is the **sequence number of the SYNACK** segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? - **You must dig deep and find the ACK from** gaia.cs.umass.edu. The sequence number of the SYN_ACK in reply to the SYN is 0.



5. 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.



Print screen, final page.

The image shows the Wireshark network protocol analyzer interface. A packet capture is loaded, and packet 597 is selected. The details pane shows the following information:

- Transmission Control Protocol:** Src Port: 55163, Dst Port: 80, Stream Index: 25, Sequence number: 14601 (relative sequence number), Acknowledgment number: 1 (relative ack number), Window Length: 20 bytes (5), Flags: 0x010 (ACK), 000. = Reserved: Not set, 000. = Nonce: Not set.
- Hypertext Transfer Protocol:** 56 SACK_PERM=1, S=1460 SACK_PERM=1 WS=128

The 'Wireshark - Print' dialog box is open, showing the following options:

- Packet Format:** ☒ Summary line, ☒ Include column headings, ☒ Details, ☐ All collapsed, ☒ As displayed, ☐ All expanded, ☐ Bytes, ☐ Print each packet on a new page.
- Packet Range:** ☐ All packets, ☒ Selected packets only, ☐ Marked packets only, ☐ First to last marked, ☐ Range: [], ☐ Remove ignored packets.
- Display:** ☐ Captured, ☒ Displayed.
- Buttons:** Page Setup..., Print..., Cancel, Help.

The bottom status bar shows: Packets: 819 · Displayed: 770 (94.0%) · Dropped: 0 (0.0%) · Profile: Default.