

```
Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 12:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2600:8806:6202:1d00:b91c:fc89:27b8:2bb
Temporary IPv6 Address. . . . . : 2600:8806:6202:1d00:557e:6847:6640:e95b
Link-local IPv6 Address . . . . . : fe80::b91c:fc89:27b8:2bb%6
IPv4 Address. . . . . : 192.168.0.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::3e37:86ff:fe08:bada%6
192.168.0.1

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\yddi>
```

Questions:

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

Destination Port: 80

Wireshark Lab 3_Yakubu Iddirisuv2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	20:08:13.887757	192.168.0.15	198.91.36.196	TCP	55	59480 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled
2	20:08:13.890684	192.168.0.15	198.91.36.196	TCP	55	59305 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled
3	20:08:13.919249	198.91.36.196	192.168.0.15	TCP	66	443 → 59305 [ACK] Seq=1 Ack=2 Win=513 Len=0 SLE=1 SRE=2
4	20:08:13.919251	198.91.36.196	192.168.0.15	TCP	66	443 → 59480 [ACK] Seq=1 Ack=2 Win=513 Len=0 SLE=1 SRE=2
19	20:08:24.781703	192.168.0.15	128.119.245.12	TCP	66	59488 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	20:08:24.781703	192.168.0.15	128.119.245.12	TCP	66	59487 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)

> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 59488, Dst Port: 80, Seq: 0, Len: 0

Source Port: 59488

Destination Port: 80

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 0

0000 3c 37 86 08 ba da f8 34 41 ac dc da 08 00 45 00 <7....4 A.....E.

0010 00 34 1e 91 40 00 80 06 a5 f7 c0 a8 00 0f 80 77 -4-..@... ..w

0020 f5 0c e8 60 00 50 a1 81 1e b9 00 00 00 80 02 ...-P-

0030 ff ff 8f e9 00 00 02 04 05 b4 01 03 03 08 01 01 ...-..

0040 04 02 ..

Transmission Control Protocol: Protocol

Packets: 279 · Displayed: 263 (94.3%) · Marked: 1 (0.4%) · Dropped: 0 (0.0%) Profile: Default

Type here to search

8:23 PM 3/5/2019

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

Destination Port: 59488

Wireshark Lab 3_Yakubu Iddirisuv2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
4	20:08:13.919251	198.91.36.196	192.168.0.15	TCP	66	443 → 59488 [ACK] Seq=1 Ack=2 Win=513 Len=0 SLE=1 SRE=2
19	20:08:24.781703	192.168.0.15	128.119.245.12	TCP	66	59488 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	20:08:24.781703	192.168.0.15	128.119.245.12	TCP	66	59487 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
21	20:08:24.792155	192.168.0.15	128.119.245.12	TCP	66	59489 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	20:08:24.805411	128.119.245.12	192.168.0.15	TCP	66	80 → 59488 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
23	20:08:24.805516	192.168.0.15	128.119.245.12	TCP	54	59488 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0

> Frame 22: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.15

> Transmission Control Protocol, Src Port: 80, Dst Port: 59488, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 59488

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0000 f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00 .4A...<7E.

0010 00 34 00 00 40 00 fc 06 48 88 80 77 f5 0c c0 a8 .4...@...H..w...

0020 00 0f 00 50 e8 60 4e cb 26 7e a1 81 1e ba 80 12 ...P..N..&~.....

0030 72 10 a8 7f 00 00 02 04 05 b4 01 01 04 02 01 03 r... ..

0040 03 07 ..

Transmission Control Protocol: Protocol

Packets: 279 · Displayed: 263 (94.3%) · Marked: 1 (0.4%) · Dropped: 0 (0.0%) Profile: Default

Type here to search

8:44 PM 3/5/2019

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?
Seq. 0

It is the Sequence number that identifies the segment as a SYN segment. The SYN segment does not include an ACK. It is the initial communication between the source IP address and the destination IP Address. And requests for permission to establish initial connection between the source IP and destination IP.

The image shows a Wireshark packet capture window titled "Wireshark Lab 3_Yakubu Iddirisuv2.pcapng". The packet list on the left shows several TCP segments. Packet 19 is a SYN segment from 192.168.0.15 to 128.119.245.12 with Seq=0. The packet details pane for packet 19 shows the following information:

- Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
- Internet Protocol Version 4, Src: 192.168.0.15, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 59488, Dst Port: 80, Seq: 0, Len: 0
 - Source Port: 59488
 - Destination Port: 80
 - [Stream index: 2]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - [Next sequence number: 0 (relative sequence number)]
 - Acknowledgment number: 0

The packet bytes pane shows the raw data of the segment, with the sequence number 0 highlighted in blue.

At the bottom of the window, the status bar indicates: Packets: 279 · Displayed: 263 (94.3%) · Marked: 1 (0.4%) · Dropped: 0 (0.0%) · Profile: Default

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.

Seq 0.

The image shows a Wireshark packet capture of a TCP connection. The packet list at the top shows several packets, with packet 22 highlighted in red. Packet 22 is a SYNACK segment from 192.168.0.15 to 128.119.245.12, with sequence number 0 and acknowledgment number 1. The packet details pane shows the following information:

- Frame 22: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.15
- Transmission Control Protocol, Src Port: 80, Dst Port: 59488, Seq: 0, Ack: 1, Len: 0
- Source Port: 80
- Destination Port: 59488
- [Stream index: 2]
- [TCP Segment Len: 0]
- Sequence number: 0 (relative sequence number)
- [Next sequence number: 0 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)

The packet bytes pane shows the raw data of the packet, with the sequence number 0 highlighted in blue.

Transmission Control Protocol: Protocol | Packets: 279 · Displayed: 263 (94.3%) · Marked: 1 (0.4%) · Dropped: 0 (0.0%) | Profile: Default

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.

Seq 151565

Wireshark Lab 3_Yakubu Iddrisu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
243	22:31:09.521507	128.119.245.12	192.168.0.15	TCP	60	80 → 53068 [ACK] Seq=1 Ack=68483 Win=166272 Len=0
244	22:31:09.521557	192.168.0.15	128.119.245.12	TCP	1514	53068 → 80 [ACK] Seq=148645 Ack=1 Win=17408 Len=1460 [TCP segment of
245	22:31:09.521567	192.168.0.15	128.119.245.12	TCP	1514	53068 → 80 [ACK] Seq=150105 Ack=1 Win=17408 Len=1460 [TCP segment of
246	22:31:09.522442	128.119.245.12	192.168.0.15	TCP	60	80 → 53068 [ACK] Seq=1 Ack=69943 Win=169088 Len=0
247	22:31:09.522491	192.168.0.15	128.119.245.12	HTTP	1472	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
248	22:31:09.527774	128.119.245.12	192.168.0.15	TCP	60	80 → 53068 [ACK] Seq=1 Ack=71403 Win=172032 Len=0

> Frame 247: 1472 bytes on wire (11776 bits), 1472 bytes captured (11776 bits) on interface 0

> Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)

> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 53068, Dst Port: 80, Seq: 151565, Ack: 1, Len: 1418

Source Port: 53068

Destination Port: 80

[Stream index: 10]

[TCP Segment Len: 1418]

Sequence number: 151565 (relative sequence number)

[Next sequence number: 152983 (relative sequence number)]

0000 3c 37 86 08 ba da f8 34 41 ac dc da 08 00 45 00 <7-----4 A-----E

0010 05 b2 02 24 40 00 80 06 bc e6 c0 a8 00 0f 80 77 --.\$@-- --w

0020 f5 0c cf 4c 00 50 89 b2 49 c8 c6 f7 f9 f1 50 18 --.L.P-- I-----P-

0030 00 44 6a ab 00 00 66 20 74 68 65 20 73 75 70 70 -Dj---f the supp

Frame (1472 bytes) Reassembled TCP (152982 bytes)

Transmission Control Protocol: Protocol

Packets: 321 · Displayed: 286 (89.1%)

Profile: Default

Type here to search

8:00 PM 2/23/2019

Wireshark Lab 3_Yakubu Iddrisu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
286	22:31:09.713822	128.119.245.12	192.168.0.15	TCP	60	80 → 53068 [ACK] Seq=1 Ack=145725 Win=183296 Len=0
287	22:31:09.722655	128.119.245.12	192.168.0.15	TCP	60	80 → 53068 [ACK] Seq=1 Ack=148645 Win=183296 Len=0
288	22:31:09.728103	128.119.245.12	192.168.0.15	TCP	60	80 → 53068 [ACK] Seq=1 Ack=151565 Win=183296 Len=0
289	22:31:09.732473	128.119.245.12	192.168.0.15	TCP	60	80 → 53068 [ACK] Seq=1 Ack=152983 Win=183296 Len=0
290	22:31:09.733157	128.119.245.12	192.168.0.15	HTTP	831	HTTP/1.1 200 OK (text/html)
291	22:31:09.774032	192.168.0.15	128.119.245.12	TCP	54	53068 → 80 [ACK] Seq=152983 Ack=778 Win=16640 Len=0

> Frame 290: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0

> Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.15

> Transmission Control Protocol, Src Port: 80, Dst Port: 53068, Seq: 1, Ack: 152983, Len: 777

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Wed, 20 Feb 2019 03:31:09 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Sat, 23 Oct 2010 11:38:58 GMT\r\n

ETag: "1a2-4934734677880"\r\n

Accept-Ranges: bytes\r\n

0000	f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00	4A...<7E
0010	03 31 04 54 40 00 fc 06 41 37 80 77 f5 0c c0 a8	1T@... A7.w...
0020	00 0f 00 50 cf 4c c6 f7 f9 f1 89 b2 4f 52 50 18	...P.L... ..ORP
0030	05 98 85 36 00 00 48 54 54 50 2f 31 2e 31 20 32	...6...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64	00 OK... ate: Wed
0050	2c 20 32 30 20 46 65 62 20 32 30 31 39 20 30 33	, 20 Feb 2019 03

Transmission Control Protocol: Protocol

Packets: 321 · Displayed: 286 (89.1%)

Profile: Default

Type here to search

9:06 PM 2/23/2019