

Wireshark Lab 3 - TCP

IT 520 –A – Enterprise Infrastructure & Networks

David Gogolkiewicz

Recycle Bin, Nokia Suite, videos, SMS Op in, authorization, untitled, Test Newsletter..., icon_loading..., Writings, HomePage

Command Prompt

Ethernet adapter Ethernet:

Connection-specific DNS Suffix	:	firos-router.home
Link-local IPv6 Address	:	fe80::7dd2:65fe:cb63:5d58%4
IPv4 Address	:	192.168.1.195
Subnet Mask	:	255.255.255.0
Default Gateway	:	192.168.1.1

Wireless LAN adapter Local Area Connection* 5:

Media State	:	Media disconnected
Connection-specific DNS Suffix	:	

Wireless LAN adapter Local Area Connection* 6:

Media State	:	Media disconnected
Connection-specific DNS Suffix	:	

Wireless LAN adapter Wi-Fi:

Media State	:	Media disconnected
Connection-specific DNS Suffix	:	firos-router.home

Ethernet adapter Bluetooth Network Connection:

Media State	:	Media disconnected
Connection-specific DNS Suffix	:	

C:\Users\dgogo>

Address

11:48 AM 2/16/2019

My Private IP Address

Question 1

Wireshark interface showing a packet capture on the 'tcp' filter. The selected packet (No. 203) is a TCP segment from 192.168.1.195 to 128.119.245.12, port 80. The packet details show the source port is 63314.

What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?
-63314

Source Port: 63314

Destination Port: 80

[Stream index: 7]

[TCP Segment Len: 29200]

Sequence number: 102821 (relative sequence number)

[Next sequence number: 132021 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window size value: 1024

[Calculated window size: 262144]

[Window size scaling factor: 256]

Checksum: 0x37f6 [unverified]

[Checksum Status: Unverified]

0020 f5 0c f7 52 00 50 ab ac 0b 1f 4c 1f 36 67 50 10 ..R.P... ..L.GpP..

0030 04 00 37 f6 00 00 79 20 61 6c 6c 20 74 68 72 65 ..7...y all thre

0040 65 20 74 6f 0d 0a 73 65 74 74 6c 65 20 74 68 65 e to use title the

0050 20 71 75 65 73 74 69 6f 6e 2c 20 61 6e 64 20 74 question, and t

0060 68 65 79 20 72 65 70 65 61 74 65 64 20 74 68 65 hey repe ated the

0070 69 72 20 61 72 67 75 6d 65 6e 74 73 20 74 6f 20 in argum ents to

0080 68 65 72 2c 0d 0a 74 68 6f 75 67 68 2c 20 61 73 her, though, as

0090 20 74 68 65 79 20 61 6c 6c 20 73 70 6f 6b 65 20 they al l spoke

00a0 61 74 20 6f 6e 63 65 2c 20 73 68 65 20 66 6f 75 at once, she fou

00b0 6e 64 20 69 74 20 76 65 72 79 20 68 61 72 64 20 nd it ve ry hard

00c0 69 6e 64 65 65 64 0d 0a 74 6f 20 6d 61 6b 65 20 indee to make

00d0 6f 75 74 20 65 78 61 63 74 6c 79 20 77 68 61 74 out exac tly what

00e0 20 74 68 65 79 20 73 61 69 64 2e 0d 0a 0d 0a 20 they sa id....

00f0 20 54 68 65 20 65 78 65 63 75 74 69 6f 6e 65 72 The exe cutioneer

0100 27 73 20 61 72 67 75 6d 65 6e 74 20 77 61 73 2c 's argum ent was,

0110 20 74 68 61 74 20 79 6f 75 20 63 6f 75 6c 64 6e that yo u couldn

0120 27 74 20 63 75 74 20 6f 66 66 20 61 0d 0a 68 65 't cut o ff a he

0130 61 64 20 75 6e 6c 65 73 73 20 74 68 65 72 65 20 ad unles s there

0140 77 61 73 20 61 20 62 6f 64 79 20 74 6f 20 63 75 was a bo dy to cu

0150 74 20 69 74 20 6f 66 66 20 66 72 6f 6d 3a 20 20 t it off from:

Packets: 313 · Displayed: 167 (53.4%) · Dropped: 0 (0.0%)

Profile: Default

Address Links

12:08 PM 2/16/2019

Question 2

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
191	56.538850	192.168.1.195	128.119.245.12	TCP	17574	63314 → 80 [ACK] Seq=44421 Ack=1 Win=262144 Len=17520 [TCP segment of a reassembled PDU]
192	56.539436	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=31281 Win=91776 Len=0
193	56.539487	192.168.1.195	128.119.245.12	TCP	14654	63314 → 80 [ACK] Seq=61941 Ack=1 Win=262144 Len=14600 [TCP segment of a reassembled PDU]
194	56.545812	40.114.79.69	192.168.1.195	TCP	60	443 → 63315 [ACK] Seq=7846 Ack=2666 Win=262144 Len=0
195	56.548255	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=35661 Win=100608 Len=0
196	56.548257	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=41501 Win=112256 Len=0
197	56.548387	192.168.1.195	128.119.245.12	TCP	20494	63314 → 80 [ACK] Seq=76541 Ack=1 Win=262144 Len=20440 [TCP segment of a reassembled PDU]
198	56.557158	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=42961 Win=115200 Len=0
199	56.557160	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=44421 Win=118144 Len=0
200	56.557246	192.168.1.195	128.119.245.12	TCP	5894	63314 → 80 [ACK] Seq=96981 Ack=1 Win=262144 Len=5840 [TCP segment of a reassembled PDU]
201	56.563255	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=59021 Win=147328 Len=0
202	56.563257	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=60481 Win=150272 Len=0
203	56.563377	192.168.1.195	128.119.245.12	TCP	29254	63314 → 80 [ACK] Seq=102821 Ack=1 Win=262144 Len=29200 [TCP segment of a reassembled PDU]
204	56.569869	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=61941 Win=153088 Len=0
205	56.569871	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=76541 Win=173696 Len=0
206	56.569993	192.168.1.195	128.119.245.12	HTTP	20996	POST /wiresark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
207	56.570029	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=78001 Win=172672 Len=0

> Frame 203: 29254 bytes on wire (234032 bits), 29254 bytes captured (234032 bits) on interface 0

> Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)

> Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 63314, Dst Port: 80, Seq: 102821, Ack: 1, Len: 29200

Source Port: 63314

Destination Port: 80

[Stream index: 7]

[TCP Segment Len: 29200]

Sequence number: 102821 (relative sequence number)

[Next sequence number: 132021 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window size value: 1024

[Calculated window size: 262144]

[Window size scaling factor: 256]

Checksum: 0x37f6 [unverified]

[Checksum Status: Unverified]

0020 f5 0c f7 52 00 50 ab ac 0b 1f 4c 1f 36 67 50 10 ...R.P...L.GpP...

0030 04 00 37 f6 00 00 79 20 61 6c 6c 20 74 68 72 65 ...7...y all thre

0040 65 20 74 6f 0d 0a 73 65 74 74 6c 65 20 74 68 65 e to use title the

0050 20 71 75 65 73 74 69 6f 6e 2c 20 61 6e 64 20 74 question, and t

0060 68 65 79 20 72 65 70 65 61 74 65 64 20 74 68 65 hey repe ated the

0070 69 72 20 61 72 67 75 6d 65 6e 74 73 20 74 6f 20 in argum ents to

0080 68 65 72 2c 0d 0a 74 68 6f 75 67 68 2c 20 61 73 her, though, as

0090 20 74 68 65 79 20 61 6c 6c 20 73 70 6f 6b 65 20 they al l spoke

00a0 61 74 20 6f 6e 63 65 2c 20 73 68 65 20 66 6f 75 at once, she fou

00b0 6e 64 20 69 74 20 76 65 72 79 20 68 61 72 64 20 nd it ve ry hard

00c0 69 6e 64 65 65 64 0d 0a 74 6f 20 6d 61 6b 65 20 indee to make

00d0 6f 75 74 20 65 78 61 63 74 6c 79 20 77 68 61 74 out exac tly what

00e0 20 74 68 65 79 20 73 61 69 64 2e 0d 0a 0d 0a 20 they sa id....

00f0 20 54 68 65 20 65 78 65 63 75 74 69 6f 6e 65 72 The exe cutioneer

0100 27 73 20 61 72 67 75 6d 65 6e 74 20 77 61 73 2c 's argum ent was,

0110 20 74 68 61 74 20 79 6f 75 20 63 6f 75 6c 64 6e that yo u couldn

0120 27 74 20 63 75 74 20 6f 66 66 20 61 0d 0a 68 65 't cut o ff a he

0130 61 64 20 75 6e 6c 65 73 73 20 74 68 65 72 65 20 ad unles s there

0140 77 61 73 20 61 20 62 6f 64 79 20 74 6f 20 63 75 was a bo dy to cu

0150 74 20 69 74 20 6f 66 66 20 66 72 6f 6d 3a 20 20 t it off from:

Destination Port (tcp.dstport), 2 bytes

Packets: 313 · Displayed: 167 (53.4%) · Dropped: 0 (0.0%)

Profile: Default

Type here to search

Address Links

12:09 PM 2/16/2019

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

- 80

Question 3

Wireshark interface showing a packet capture on the 'tcp' filter. The packet list shows a SYN segment (No. 87) from 192.168.1.195 to 192.168.1.195, Seq=0, Len=0. The packet details pane shows the TCP segment structure, including the Flags field where the SYN flag is set to 1.

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?
- 0

What is it in the segment that identifies the segment as a SYN segment?
- SYN flag is set to 1

Question 4

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
183	56.519880	40.114.79.69	192.168.1.195	TCP	60	443 → 63315 [ACK] Seq=7210 Ack=2263 Win=262656 Len=0
184	56.528690	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=15221 Win=59648 Len=0
185	56.528755	192.168.1.195	128.119.245.12	TCP	2974	63314 → 80 [ACK] Seq=41501 Ack=1 Win=262144 Len=2920 [TCP segment of a reassembled PDU]
186	56.531947	40.114.79.69	192.168.1.195	TLSv1.2	689	Application Data
187	56.532049	192.168.1.195	40.114.79.69	TCP	54	63315 → 443 [ACK] Seq=2665 Ack=7846 Win=261376 Len=0
188	56.532191	192.168.1.195	40.114.79.69	TCP	54	63315 → 443 [FIN, ACK] Seq=2665 Ack=7846 Win=261376 Len=0
189	56.538727	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=16681 Win=62592 Len=0
190	56.538729	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=23981 Win=77184 Len=0
191	56.538850	192.168.1.195	128.119.245.12	TCP	17574	63314 → 80 [ACK] Seq=44421 Ack=1 Win=262144 Len=17520 [TCP segment of a reassembled PDU]
192	56.539436	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=31281 Win=91776 Len=0
193	56.539487	192.168.1.195	128.119.245.12	TCP	14654	63314 → 80 [ACK] Seq=61941 Ack=1 Win=262144 Len=14600 [TCP segment of a reassembled PDU]
194	56.545812	40.114.79.69	192.168.1.195	TCP	60	443 → 63315 [ACK] Seq=7846 Ack=2666 Win=262144 Len=0
195	56.548255	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=35661 Win=100608 Len=0
196	56.548257	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=41501 Win=112256 Len=0
197	56.548387	192.168.1.195	128.119.245.12	TCP	20494	63314 → 80 [ACK] Seq=76541 Ack=1 Win=262144 Len=20440 [TCP segment of a reassembled PDU]
198	56.557158	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=42961 Win=115200 Len=0
199	56.557160	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=44421 Win=118144 Len=0

Transmission Control Protocol, Src Port: 80, Dst Port: 63314, Seq: 1, Ack: 15221, Len: 0

Source Port: 80
Destination Port: 63314
[Stream index: 7]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 15221 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
0000 = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): 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.....]
Window size value: 466
[Calculated window size: 59648]

0000 00 01 6c d1 d3 8c 48 5d 36 68 c5 b8 08 00 45 00 ...1...H] 6h...E
0010 00 28 1b 8e 40 00 35 06 f2 52 80 77 f5 0c c0 a8 ...@.5...R.w...
0020 01 c3 00 50 f7 52 4c 1f 36 67 ab aa b4 ef 50 1c ...P.RL. 6g...P
0030 01 d2 9b 4f 00 00 00 00 00 00 00 00 00 00 ...O....

Acknowledgment (tcp.flags.ack), 1 byte

Packets: 313 · Displayed: 167 (53.4%) · Dropped: 0 (0.0%) Profile: Default

Address Links 12:54 PM 2/16/2019

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.

-ACK Flag set to 1
-Sequence #: 1

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
194	56.545812	40.114.79.69	192.168.1.195	TCP	60	443 → 63315 [ACK] Seq=7846 Ack=2666 Win=262144 Len=0
195	56.548255	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=35661 Win=100608 Len=0
196	56.548257	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=41501 Win=112256 Len=0
197	56.548387	192.168.1.195	128.119.245.12	TCP	20494	63314 → 80 [ACK] Seq=76541 Ack=1 Win=262144 Len=20440 [TCP segment of a reassembled PDU]
198	56.557158	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=42961 Win=115200 Len=0
199	56.557160	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=44421 Win=118144 Len=0
200	56.557246	192.168.1.195	128.119.245.12	TCP	5894	63314 → 80 [ACK] Seq=96981 Ack=1 Win=262144 Len=5840 [TCP segment of a reassembled PDU]
201	56.563255	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=59021 Win=147328 Len=0
202	56.563257	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=60481 Win=150272 Len=0
203	56.563377	192.168.1.195	128.119.245.12	TCP	29254	63314 → 80 [ACK] Seq=102821 Ack=1 Win=262144 Len=29200 [TCP segment of a reassembled PDU]
204	56.569869	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=61941 Win=153088 Len=0
205	56.569871	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=76541 Win=173696 Len=0
206	56.569993	192.168.1.195	128.119.245.12	HTTP	20996	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
207	56.570829	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=78001 Win=172672 Len=0
208	56.576559	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=86761 Win=178560 Len=0
209	56.576561	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=95521 Win=172672 Len=0
210	56.583261	128.119.245.12	192.168.1.195	TCP	60	80 → 63314 [ACK] Seq=1 Ack=96981 Win=183296 Len=0

> Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 63314, Dst Port: 80, Seq: 132021, Ack: 1, Len: 20942

Source Port: 63314

Destination Port: 80

[Stream index: 7]

[TCP Segment Len: 20942]

Sequence number: 132021 (relative sequence number)

[Next sequence number: 152963 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

...0 = Congestion Window Reduced (CWR): 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 size value: 1024

00000000 50 4f 53 54 20 2f 77 69 72 65 73 68 61 72 6b 2d POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1

00000010 6c 61 62 73 2f 6c 61 62 33 2d 31 2d 72 65 70 6c y.htm HTTP/1.1

00000020 79 2e 68 74 6d 20 48 54 54 50 2f 31 2e 31 0d 0a Referer: http://

00000030 52 65 66 65 72 65 72 3a 20 68 74 70 3a 2f 2f gaia.cs.umass.edu

00000040 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 u/wireshark-labs

00000050 75 2f 77 69 72 65 73 68 61 72 6b 2d 6c 61 62 73 /TCP-wireshark-f

00000060 2f 54 43 50 2d 77 69 72 65 73 68 61 72 6b 2d 66 ile1.htm l::Cache

00000070 69 6c 65 31 2e 68 74 6d 6c 0d 0a 43 61 63 68 65 -Control: max-age=0

00000080 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 e=0

00000090 65 3d 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 e=0

000000a0 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 e: multipart/form

000000b0 6d 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 79 m-data; boundary

000000c0 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d

Frame (20996 bytes) Reassembled TCP (152962 bytes)

Transmission Control Protocol: Protocol

Packets: 313 · Displayed: 167 (53.4%) · Dropped: 0 (0.0%) Profile: Default

1:07 PM 2/16/2019

What is the sequence number of the TCP segment containing the HTTP POST command?

- 132021

C:\Users\dgogo\AppData\Local\Temp\wireshark_0AEACC56-2C54-40D3-A2B1-ESA421CEA2E2_20190216112206_a16340.pcapng 313 total packets, 8 shown

No.	Time	Source	Destination	Protocol	Length	Info
221	56.599061	128.119.245.12	192.168.1.195	HTTP	831	HTTP/1.1 200 OK (text/html)

Frame 221: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
Ethernet II, Src: Verizon_68:c5:b8 (48:5d:36:68:c5:b8), Dst: Foxconn_d1:d3:8c (08:01:6c:d1:d3:8c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.195
Transmission Control Protocol, Src Port: 80, Dst Port: 63314, Seq: 1, Ack: 152963, Len: 777
Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
 Date: Sat, 16 Feb 2019 16:23:00 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 11:30:58 GMT\r\n
 ETag: "1a2-4934734677880"\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: 0.029068000 seconds]
 [Request in frame: 206]
 File Data: 418 bytes
 Line-based text data: text/html (11 lines)