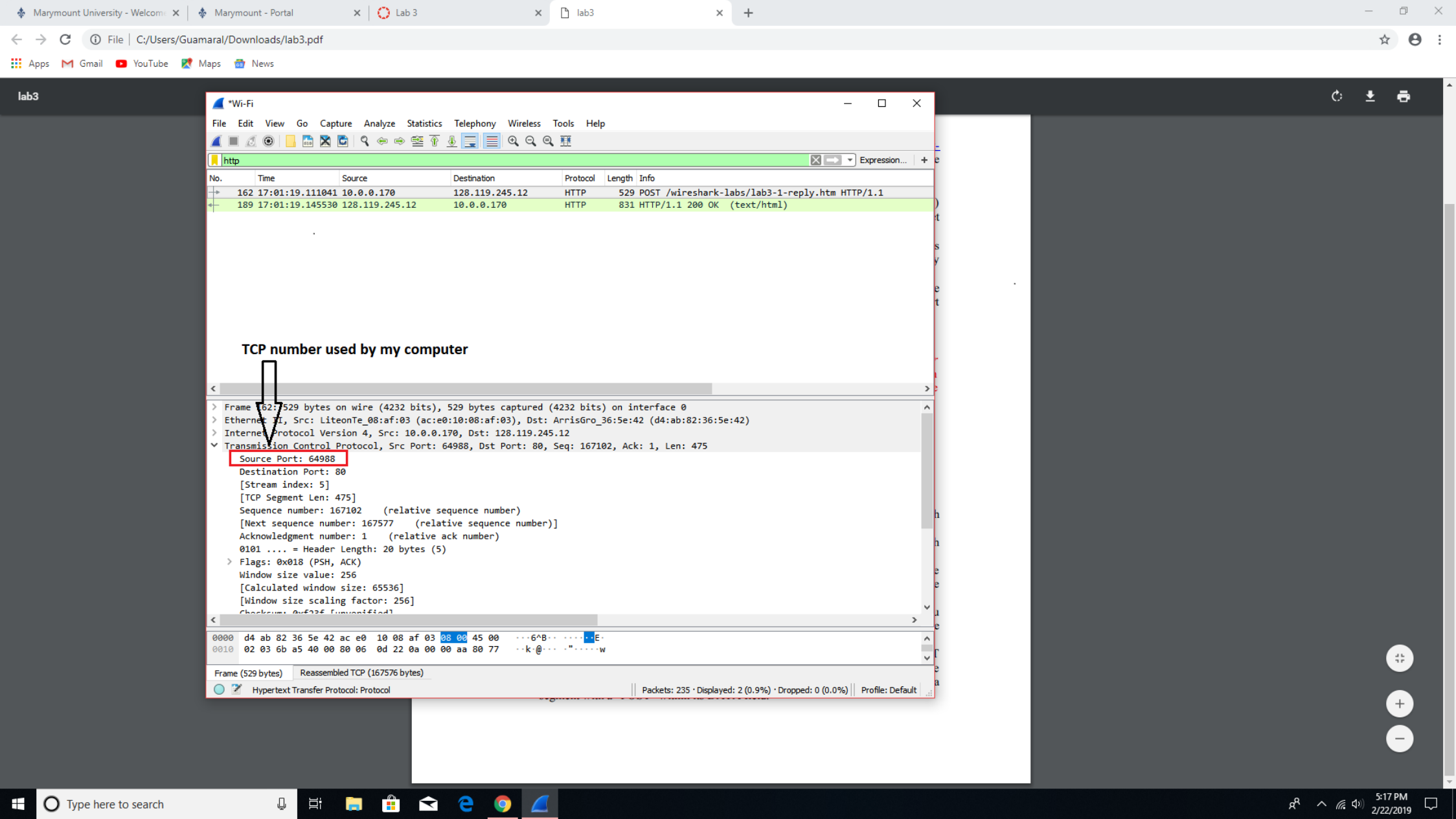
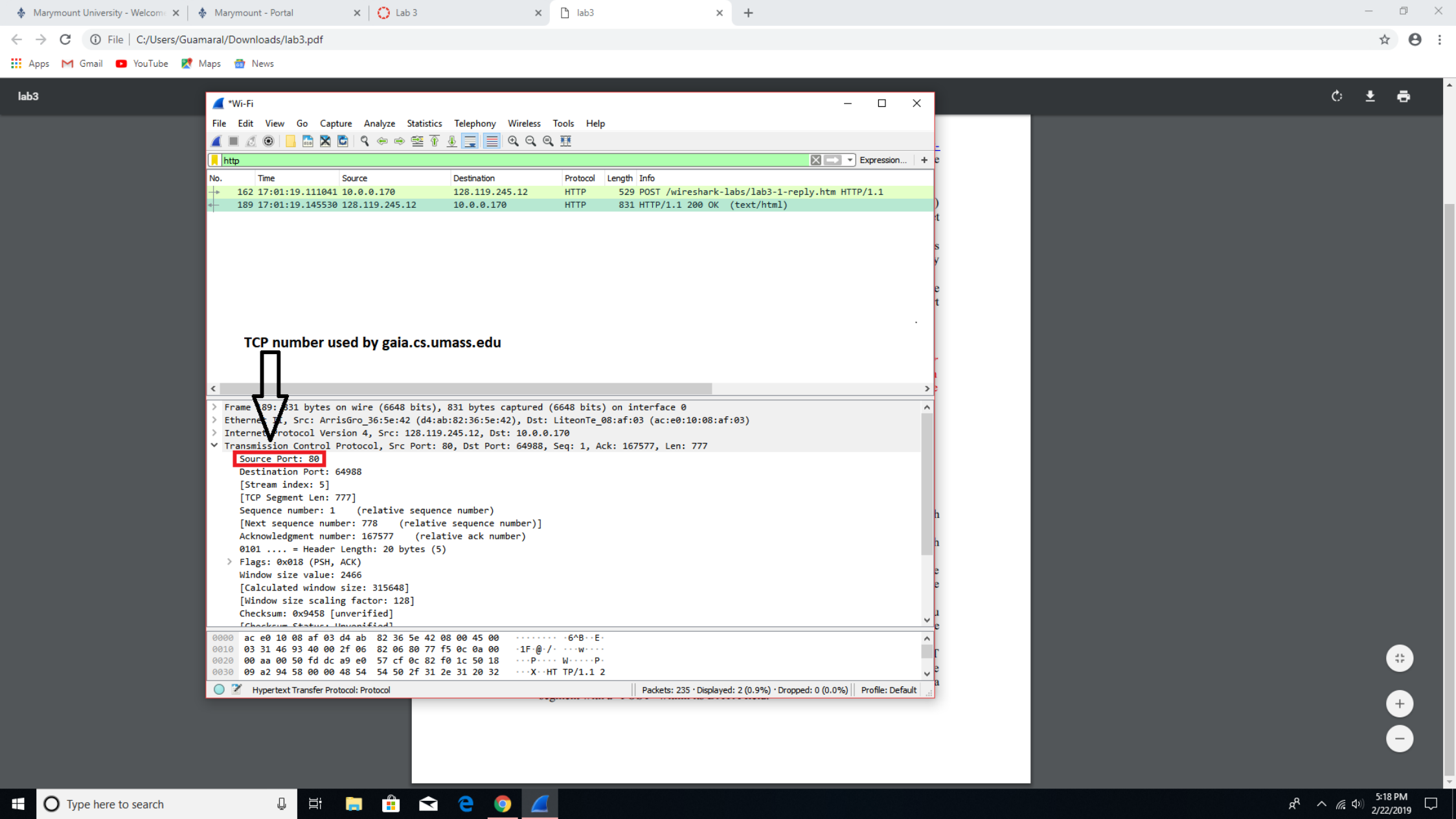


IT-520-A > Assignments > Lab 3

My IP Address

```
Command Prompt
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : hsd1.va.comcast.net
IPv6 Address. . . . . : 2601:140:8f00:8c0::27c8
IPv6 Address. . . . . : 2601:140:8f00:8c0:499a:f6d6:8fa8:97ca
Temporary IPv6 Address. . . . . : 2601:140:8f00:8c0:19d:2e15:3f29:d86f
Link-local IPv6 Address . . . . . : fe80::499a:f6d6:8fa8:97ca%6
IPv4 Address. . . . . : 10.0.0.170
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::d6ab:82ff:fe36:5e42%6
10.0.0.1
Ethernet adapter Bluetooth Network Connection 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\Guamaral>
```





TCP number used by gaia.cs.umass.edu

Source Port: 80

Destination Port: 64988

[Stream index: 5]

[TCP Segment Len: 777]

Sequence number: 1 (relative sequence number)

[Next sequence number: 778 (relative sequence number)]

Acknowledgment number: 167577 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 2466

[Calculated window size: 315648]

[Window size scaling factor: 128]

Checksum: 0x9458 [unverified]

[Checksum Status: Unverified]

0000 ac e0 10 08 af 03 d4 ab 82 36 5e 42 08 00 45 006^B...E
0010 03 31 46 93 40 00 2f 06 82 06 80 77 f5 0c 0a 00 ...1F:@/-...w....
0020 00 aa 00 50 fd dc a9 e0 57 cf 0c 82 f0 1c 50 18 ...P...W...P...
0030 09 a2 94 58 00 00 48 54 54 50 2f 31 2e 31 20 32 ...X..HT P/1.1 2

Hypertext Transfer Protocol: Protocol

Packets: 235 · Displayed: 2 (0.9%) · Dropped: 0 (0.0%)

Profile: Default

Seq. Number of the TCP SYN

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
7	17:01:16.680390	2607:f8b0:4004:805::...	2601:140:8f00:8c0:1...	TCP	86	443 → 64971 [ACK] Seq=1 Ack=2 Win=136 Len=0 SLE=1
8	17:01:16.818981	23.194.116.100	10.0.0.170	TLSv1.2	85	Encrypted Alert
9	17:01:16.818983	23.194.116.100	10.0.0.170	TCP	56	443 → 64981 [FIN, ACK] Seq=32 Ack=1 Win=245 Len=0
10	17:01:16.819070	10.0.0.170	23.194.116.100	TCP	54	64981 → 443 [ACK] Seq=1 Ack=33 Win=1019 Len=0
11	17:01:18.462287	fe80::d6ab:82ff:fe3...	ff02::1	ICMPv6	174	Router Advertisement from d4:ab:82:36:5e:42
12	17:01:18.962354	10.0.0.170	128.119.245.12	TCP	54	64986 → 80 [FIN, ACK] Seq=2 Ack=1 Win=256 Len=0
13	17:01:18.962654	10.0.0.170	128.119.245.12	TCP	54	64985 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
14	17:01:18.962983	10.0.0.170	128.119.245.12	TCP	66	64988 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
15	17:01:18.963230	10.0.0.170	128.119.245.12	TCP	66	64989 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
16	17:01:18.994366	128.119.245.12	10.0.0.170	TCP	56	80 → 64986 [FIN, ACK] Seq=1 Ack=3 Win=229 Len=0
17	17:01:18.994405	10.0.0.170	128.119.245.12	TCP	54	64986 → 80 [ACK] Seq=3 Ack=2 Win=256 Len=0
18	17:01:19.002547	128.119.245.12	10.0.0.170	TCP	66	80 → 64988 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
19	17:01:19.002610	10.0.0.170	128.119.245.12	TCP	54	64988 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20	17:01:19.003221	10.0.0.170	128.119.245.12	TCP	715	64988 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=6
21	17:01:19.003424	10.0.0.170	128.119.245.12	TCP	1514	64988 → 80 [ACK] Seq=662 Ack=1 Win=65536 Len=1460

> Frame 14: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: LiteonTe_08:af:03 (ac:e0:10:08:af:03), Dst: ArrisGro_36:5e:42 (d4:ab:82:36:5e:42)

> Internet Protocol Version 4, Src: 10.0.0.170, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 64988, Dst Port: 80, Seq: 0, Len: 0

Source Port: 64988

Destination Port: 80

[Stream index: 5]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

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

Acknowledgment number: 0

1000 = Header Length: 32 bytes (8)

> Flags: 0x002 (SYN)

Window size value: 64240

[Calculated window size: 64240]

Checksum: 0x87c1 [unverified]

[Checksum Status: Unverified]

0010 00 34 6b 2d 40 00 80 06 0f 69 0a 00 00 aa 80 77 4k-@... i...w

0020 f5 0c fd dc 00 50 0c 80 61 83 00 00 00 00 80 02P... a.....

0030 fa f0 87 c1 00 00 02 04 05 b4 01 03 03 08 01 01

0040 04 02

Sequence number (tcp.seq), 4 bytes

Packets: 235 · Displayed: 235 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

Wi-Fi
 File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
7	17:01:16.680390	2607:f8b0:4004:805::...	2601:140:8f00:8c0:1...	TCP	86	443 → 64971 [ACK] Seq=1 Ack=2 Win=136 Len=0 SLE=1
8	17:01:16.818981	23.194.116.100	10.0.0.170	TLSv1.2	85	Encrypted Alert
9	17:01:16.818983	23.194.116.100	10.0.0.170	TCP	56	443 → 64981 [FIN, ACK] Seq=32 Ack=1 Win=245 Len=0
10	17:01:16.819070	10.0.0.170	23.194.116.100	TCP	54	64981 → 443 [ACK] Seq=1 Ack=33 Win=1019 Len=0
11	17:01:18.462287	fe80::d6ab:82ff:fe3...	ff02::1	ICMPv6	174	Router Advertisement from d4:ab:82:36:5e:42
12	17:01:18.962354	10.0.0.170	128.119.245.12	TCP	54	64986 → 80 [FIN, ACK] Seq=2 Ack=1 Win=256 Len=0
13	17:01:18.962654	10.0.0.170	128.119.245.12	TCP	54	64985 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
14	17:01:18.962983	10.0.0.170	128.119.245.12	TCP	66	64988 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
15	17:01:18.963230	10.0.0.170	128.119.245.12	TCP	66	64989 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
16	17:01:18.994366	128.119.245.12	10.0.0.170	TCP	56	80 → 64986 [FIN, ACK] Seq=1 Ack=3 Win=229 Len=0
17	17:01:18.994405	10.0.0.170	128.119.245.12	TCP	54	64986 → 80 [ACK] Seq=3 Ack=2 Win=256 Len=0
18	17:01:19.002547	128.119.245.12	10.0.0.170	TCP	66	80 → 64988 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
19	17:01:19.002610	10.0.0.170	128.119.245.12	TCP	54	64988 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20	17:01:19.003221	10.0.0.170	128.119.245.12	TCP	715	64988 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=6
21	17:01:19.003424	10.0.0.170	128.119.245.12	TCP	1514	64988 → 80 [ACK] Seq=662 Ack=1 Win=65536 Len=1460

[Next sequence number: 0 (relative sequence number)]
 Acknowledgment number: 0
 1000 = Header Length: 32 bytes (8)
 > **Flags: 0x002 (SYN)**
 000. = 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
 > **... ..1. = Syn: Set**
0 = Fin: Not set
 [TCP Flags:S.]
 Window size value: 64240
 [Calculated window size: 64240]

0010 00 34 b6 2d 40 00 80 06 0f 69 0a 00 00 aa 80 77 4k-@... i...w
 0020 f5 0c fd dc 00 50 0c 80 61 83 00 00 00 00 80 02P... a.....
 0030 fa f0 87 c1 00 00 02 04 05 b4 01 03 03 08 01 01
 0040 04 02 ..

Sequence number (tcp.seq), 4 bytes

Packets: 235 · Displayed: 235 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

SYN flag is set to 1



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?

Solution: Sequence number of the SYNACK segment from gaia.cs.umass.edu to the

Marymount University - Welcom...x

Lab 3

lab3

File | C:/Users/Guamaral/Downloads/lab3.pdf

Apps Gmail YouTube Maps News

lab31/1

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
7	17:01:16.680390	2607:f8b0:4004:805:...	2601:140:8f00:8c0:1...	TCP	86	443 → 64971 [ACK] Seq=1 Ack=2 Win=136 Len=0 SLE=1
8	17:01:16.818981	23.194.116.100	10.0.0.170	TLSv1.2	85	Encrypted Alert
9	17:01:16.818983	23.194.116.100	10.0.0.170	TCP	56	443 → 64981 [FIN, ACK] Seq=32 Ack=1 Win=245 Len=0
10	17:01:16.819070	10.0.0.170	23.194.116.100	TCP	54	64981 → 443 [ACK] Seq=1 Ack=33 Win=1019 Len=0
11	17:01:18.462287	fe80::d6ab:82ff:fe3...	ff02::1	ICMPv6	174	Router Advertisement from d4:ab:82:36:5e:42
12	17:01:18.962354	10.0.0.170	128.119.245.12	TCP	54	64986 → 80 [FIN, ACK] Seq=2 Ack=1 Win=256 Len=0
13	17:01:18.962654	10.0.0.170	128.119.245.12	TCP	54	64985 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
14	17:01:18.962983	10.0.0.170	128.119.245.12	TCP	66	64988 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
15	17:01:18.963230	10.0.0.170	128.119.245.12	TCP	66	64989 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
16	17:01:18.994366	128.119.245.12	10.0.0.170	TCP	56	80 → 64986 [FIN, ACK] Seq=1 Ack=3 Win=229 Len=0
17	17:01:18.994405	10.0.0.170	128.119.245.12	TCP	54	64986 → 80 [ACK] Seq=3 Ack=2 Win=256 Len=0
18	17:01:19.002547	128.119.245.12	10.0.0.170	TCP	66	80 → 64988 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
19	17:01:19.002610	10.0.0.170	128.119.245.12	TCP	54	64988 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
20	17:01:19.003221	10.0.0.170	128.119.245.12	TCP	715	64988 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=6
21	17:01:19.003424	10.0.0.170	128.119.245.12	TCP	1514	64988 → 80 [ACK] Seq=662 Ack=1 Win=65536 Len=1460

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.170

Transmission Control Protocol, Src Port: 80, Dst Port: 64988, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 64988

[Stream index: 5]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Next sequence number: 0 (relative sequence number)

Acknowledgment number: 1 (relative ack number)

1000 = Header Length: 32 bytes (8)

Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

...0 = Congestion Window Reduced (CWR): Not set

....0... = ECN-Echo: Not set

....10. = Urgent: Not set

0010 00 34 00 00 40 00 2f 06 cb 96 80 77 f5 0c 0a 00

0020 00 aa 00 50 fd d9 a9 e0 57 ce 0c 80 61 84 80 12

0030 72 10 0e e3 00 00 02 04 05 b4 01 01 04 02 01 03

0040 03 07

Next sequence number (tcp.nextseq)Packets: 235 · Displayed: 235 (100.0%) · Dropped: 0 (0.0%)Profile: Default

reshark-
e this file

html.

th name)
Don't yet

hen press
select any

upload the
l, a short

it to your
bmission
and date

page
page.

cate with

cate with

nitiate the
s it in the

mass.edu
find the

TP POST

into the
ng for a

Type here to search

2/22/2019

lab3

1/1

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No. Time Source Destination Protocol Length Info

162 17:01:19.111041 10.0.0.170 128.119.245.12 HTTP 529 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1

189 17:01:19.145530 128.119.245.12 10.0.0.170 HTTP 831 HTTP/1.1 200 OK (text/html)

Sequence number of the TCP segment containing the HTTP POST command

Sequence number: 167102 (relative sequence number)

[Next sequence number: 167577 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

0020 f5 0c fd dc 00 50 0c 82 ee 41 a9 e0 57 cf 50 18

0030 01 00 f2 3f 00 00 68 69 6c 64 68 6f 6f 64 3a 20

Frame (529 bytes) Reassembled TCP (167576 bytes)

Sequence number (tcp.seq), 4 bytes

Packets: 235 · Displayed: 2 (0.9%) · Dropped: 0 (0.0%) Profile: Default

Wireshark

this file

html.

with name)

Don't yet

then press

select any

upload the

l, a short

it to your

omission

and date

page

page.

cate with

cate with

nitiate the

s it in the

mass.edu

find the

TP POST

into the

ng for a

Type here to search

5:33 PM 2/22/2019

Lab 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
162	17:01:19.111041	10.0.0.170	128.119.245.12	HTTP	529	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1
189	17:01:19.145530	128.119.245.12	10.0.0.170	HTTP	831	HTTP/1.1 200 OK (text/html)

> Frame 162: 529 bytes on wire (4232 bits) captured (4232 bits) on 0

> Ethernet II, Src: LiteonTe_08:00:27:00:00:00, Dst: 10:00:00:00:00:00

> Internet Protocol Version 4, Src: 10.0.0.170, Destination: 128.119.245.12

> Transmission Control Protocol, Src Port: 64988, Destination Port: 80, [Stream index: 5]

> [TCP Segment Len: 475]

> Sequence number: 167102

> [Next sequence number: 167536]

> Acknowledgment number: 1

> 0101 = Header Length: 10 bytes

> Flags: 0x018 (PSH, ACK)

> Window size value: 256

> [Calculated window size: 65536]

> [Window size scaling factor: 256]

> Checksum: 0xf32f (unverified)

0020 f5 0c fd dc 00 50 0c 82 ee 41 a9 e0 57 cf 50 18P...A..W..

0030 01 00 f2 3f 00 00 68 69 6c 64 68 6f 6f 64 3a 20 ...?..hi ldhoo:

Frame (529 bytes) Reassembled TCP (167576 bytes)

Sequence number (tcp.seq), 4 bytes

Packets: 235 · Displayed: 2 (0.9%) · Dropped: 0 (0.0%) Profile: Default

Wireshark · Print

?

X

Packet Format

☒ Summary line

☒ Include column headings

Details:

☐ All collapsed

☒ As displayed

☐ All expanded

☐ Bytes

☐ Print each packet on a new page

+ and - zoom, 0 resets

Packet Range

☐ Captured

☒ Displayed

☐ All packets

☒ Selected packets only

☐ Marked packets only

☐ First to last marked

Range:

☐ Remove ignored packets

235 2

1 1

0 0

0 0

0 0

0 0

Page Setup...

Print...

Cancel

Help

wireshark-
e this file

html.

th name)
Don't yet

then press
select any

pload the
i, a short

it to your
bmission
and date

page
page.

No.	Time	Source	Destination	Protocol	Length	Info
162	17:01:19.111041	10.0.0.170	128.119.245.12	HTTP	529	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1

Frame 162: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface 0
Ethernet II, Src: LiteonTe_08:af:03 (ac:e0:10:08:af:03), Dst: ArrisGro_36:5e:42 (d4:ab:82:36:5e:42)
Internet Protocol Version 4, Src: 10.0.0.170, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64988, Dst Port: 80, Seq: 167102, Ack: 1, Len: 475
Source Port: 64988
Destination Port: 80
[Stream index: 5]
[TCP Segment Len: 475]
Sequence number: 167102 (relative sequence number)
[Next sequence number: 167577 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 256
[Calculated window size: 65536]
[Window size scaling factor: 256]
Checksum: 0xf23f [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (475 bytes)
TCP segment data (475 bytes)
[116 Reassembled TCP Segments (167576 bytes): #20(661), #21(1460), #22(1460), #23(1460), #24(1460), #25(1460), #26(1460), #27(1460), #28(1460), #29(1460), #34(1460), #35(1460), #36(1460), #37(1460), #38(1460), #40(1460), #41(1460), #44(1460)]
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryBLTA1Cu81Hkj07Ry"