

Shahad bin himd
IT520
LAB3

MY IP 10.0.0.133

Wireshark interface showing a packet capture of a TCP connection. The selected packet (No. 78) is a FIN, ACK segment from 128.119.245.12 to 10.0.0.133. The packet details pane shows the following structure:

- Frame 78: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: Technico_3c:55:7a (44:1c:12:3c:55:7a), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:2e)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133
- Transmission Control Protocol, Src Port: 80, Dst Port: 57058, Seq: 1, Ack: 1, Len: 0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 f0 b4 79 18 2e 2e 44 1c 12 3c 55 7a 08 00 45 00  ..y..D..<Uz..E.
0010 00 34 80 e4 40 00 30 06 49 d7 80 77 f5 0c 0a 00  .4..@.0. I..w...
0020 00 85 00 50 de e2 3e de c4 c3 c1 e3 96 46 80 11  ...P..>.....F..
0030 00 e3 70 fc 00 00 01 01 08 0a 41 54 92 5b 1e 9c  ..p.....AT.[..
0040 57 89                                             W.
```

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

57068

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help 82% Tue Feb 19 8:07 PM

lab3.pcapng

tcp

No.	Time	Source	Destination	Protocol	Length	Info
97	15.127421	10.0.0.133	128.119.245.12	TCP	66	57058 → 80 [FIN, ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513589259 TSecr=109600
98	15.127664	10.0.0.133	128.119.245.12	TCP	66	57059 → 80 [FIN, ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513589259 TSecr=109600
99	15.127817	10.0.0.133	128.119.245.12	TCP	78	57068 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589259 TSecr=109600
100	15.133320	10.0.0.133	128.119.245.12	TCP	78	57069 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589264 TSecr=109600
101	15.162703	128.119.245.12	10.0.0.133	TCP	66	80 → 57058 [ACK] Seq=2 Ack=2 Win=227 Len=0 TSval=1096068312 TSecr=513589259
102	15.162718	128.119.245.12	10.0.0.133	TCP	74	80 → 57068 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1096068312 TSecr=513589259
103	15.162938	10.0.0.133	128.119.245.12	TCP	66	57068 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=513589293 TSecr=109600
104	15.163560	10.0.0.133	128.119.245.12	TCP	742	57068 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=676 TSval=513589293 TSecr=109600
105	15.163722	10.0.0.133	128.119.245.12	TCP	1514	57068 → 80 [ACK] Seq=677 Ack=1 Win=131744 Len=1448 TSval=513589293 TSecr=109600
106	15.163723	10.0.0.133	128.119.245.12	TCP	1514	57068 → 80 [ACK] Seq=2125 Ack=1 Win=131744 Len=1448 TSval=513589293 TSecr=109600

Frame 99: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0

Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:55:7a)

Internet Protocol Version 4, Src: 10.0.0.133, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 57068, Dst Port: 80, Seq: 0, Len: 0

Source Port: 57068

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

0000 44 1c 12 3c 55 7a f0 b4 79 18 2e 2e 08 00 45 00 D...<Uz..y....E-

0010 00 40 00 00 40 00 40 06 ba af 0a 00 00 85 80 77 .@.@@.....w

0020 f5 0c de ec 00 50 91 04 ee 1e 00 00 00 00 b0 02P.....

0030 ff ff 79 ec 00 00 02 04 05 b4 01 03 03 05 01 01 ..y.....

0040 08 0a 1e 9c c0 0b 00 00 00 00 04 02 00 00

Transmission Control Protocol (tcp), 44 bytes

Packets: 478 · Displayed: 385 (80.5%) · Dropped: 0 (0.0%) Profile: Default

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

PORT: 80

The image shows a Wireshark packet capture of a network traffic. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets, with packet 102 selected. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
97	15.127421	10.0.0.133	128.119.245.12	TCP	66	57058 → 80 [FIN, ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513589259 TSecr=109600
98	15.127664	10.0.0.133	128.119.245.12	TCP	66	57059 → 80 [FIN, ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513589259 TSecr=109600
99	15.127817	10.0.0.133	128.119.245.12	TCP	78	57068 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589259 TSecr=109600
100	15.133320	10.0.0.133	128.119.245.12	TCP	78	57069 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589264 TSecr=109600
101	15.162703	128.119.245.12	10.0.0.133	TCP	66	80 → 57058 [ACK] Seq=2 Ack=2 Win=227 Len=0 TSval=1096068312 TSecr=513589259
102	15.162718	128.119.245.12	10.0.0.133	TCP	74	80 → 57068 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1096068312 TSecr=513589259
103	15.162938	10.0.0.133	128.119.245.12	TCP	66	57068 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=513589293 TSecr=109600
104	15.163560	10.0.0.133	128.119.245.12	TCP	742	57068 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=676 TSval=513589293 TSecr=109600
105	15.163722	10.0.0.133	128.119.245.12	TCP	1514	57068 → 80 [ACK] Seq=677 Ack=1 Win=131744 Len=1448 TSval=513589293 TSecr=109600
106	15.163723	10.0.0.133	128.119.245.12	TCP	1514	57068 → 80 [ACK] Seq=2125 Ack=1 Win=131744 Len=1448 TSval=513589293 TSecr=109600

Packet Details:

- Frame 102: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: Technico_3c:55:7a (44:1c:12:3c:55:7a), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:2e)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133
- Transmission Control Protocol, Src Port: 80, Dst Port: 57068, Seq: 0, Ack: 1, Len: 0
 - Source Port: 80
 - Destination Port: 57068
 - [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)

Packet Bytes:

```
0000 f0 b4 79 18 2e 2e 44 1c 12 3c 55 7a 08 00 45 00  ..y...D...<Uz...E..
0010 00 3c 00 00 40 00 2f 06 cb b3 80 77 f5 0c 0a 00  <...@/...w....
0020 00 85 00 50 de ec 0e 6b 19 d1 91 04 ee 1f a0 12  ...P...k.....
0030 71 20 03 55 00 00 02 04 05 b4 04 02 08 0a 41 54  q·U... ..AT
0040 ac d8 1e 9c c0 0b 01 03 03 07
```

Status Bar: Transmission Control Protocol (tcp), 40 bytes | Packets: 478 · Displayed: 385 (80.5%) · Dropped: 0 (0.0%) | Profile: Default

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?

Segment : 0 syn seg: 1

The image shows a Wireshark packet capture of a TCP connection. The packet list pane shows several packets, with packet 99 highlighted. The packet details pane shows the flags for packet 99, which is a SYN segment. The flags are: Reserved: Not set, Nonce: Not set, Congestion Window Reduced (CWR): Not set, ECN-Echo: Not set, Urgent: Not set, Acknowledgment: Not set, Push: Not set, Reset: Not set, and Syn: Set. A red arrow points to the 'Syn: Set' flag. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
80	8.603500	10.0.0.133	128.119.245.12	TCP	66	57058 → 80 [ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513582736 TSecr=1096061
97	15.127421	10.0.0.133	128.119.245.12	TCP	66	57058 → 80 [FIN, ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513589259 TSecr=10
98	15.127664	10.0.0.133	128.119.245.12	TCP	66	57059 → 80 [FIN, ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513589259 TSecr=10
99	15.127817	10.0.0.133	128.119.245.12	TCP	78	57068 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589259 TSecr=10
100	15.133320	10.0.0.133	128.119.245.12	TCP	78	57069 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589264 TSecr=10
101	15.162703	128.119.245.12	10.0.0.133	TCP	66	80 → 57058 [ACK] Seq=2 Ack=2 Win=227 Len=0 TSval=1096068312 TSecr=5135892
102	15.162718	128.119.245.12	10.0.0.133	TCP	74	80 → 57068 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
103	15.162938	10.0.0.133	128.119.245.12	TCP	66	57068 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=513589293 TSecr=10960
104	15.163560	10.0.0.133	128.119.245.12	TCP	742	57068 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=676 TSval=513589293 TSecr=10
105	15.163722	10.0.0.133	128.119.245.12	TCP	1514	57068 → 80 [ACK] Seq=677 Ack=1 Win=131744 Len=1448 TSval=513589293 TSecr=10

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
-0.. = Reset: Not set
- ▶1. = Syn: Set
-0 = Fin: Not set

0000 44 1c 12 3c 55 7a f0 b4 79 18 2e 2e 08 00 45 00 D...<Uz...y...E

0010 00 40 00 00 40 00 40 06 ba af 0a 00 00 85 80 77 .@...@...w

0020 f5 0c de ec 00 50 91 04 ee 1e 00 00 00 00 b0 02P.....

0030 ff ff 79 ec 00 00 02 04 05 b4 01 03 03 05 01 01 ...y.....

0040 08 0a 1e 9c c0 0b 00 00 00 00 04 02 00 00

Transmission Control Protocol (tcp), 44 bytes

Packets: 478 · Displayed: 385 (80.5%) · 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.

sequence: 0

The image shows a Wireshark packet capture of a TCP connection. The packet list shows a SYNACK segment (No. 102) from 128.119.245.12 to 10.0.0.133. The packet details show the sequence number as 0, which is highlighted with a red box and an arrow pointing to the text "(relative sequence number)".

No.	Time	Source	Destination	Protocol	Length	Info
98	15.127664	10.0.0.133	128.119.245.12	TCP	66	57059 → 80 [FIN, ACK] Seq=1 Ack=2 Win=4117 Len=0 TSval=513589259 TSecr=1096068317
99	15.127817	10.0.0.133	128.119.245.12	TCP	78	57068 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589259 TSecr=1096068317
100	15.133320	10.0.0.133	128.119.245.12	TCP	78	57069 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=513589264 TSecr=1096068317
101	15.162703	128.119.245.12	10.0.0.133	TCP	66	80 → 57058 [ACK] Seq=2 Ack=2 Win=227 Len=0 TSval=1096068312 TSecr=513589259
102	15.162718	128.119.245.12	10.0.0.133	TCP	74	80 → 57068 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=513589259 TSecr=1096068317
103	15.162938	10.0.0.133	128.119.245.12	TCP	66	57068 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=513589293 TSecr=1096068317
104	15.163560	10.0.0.133	128.119.245.12	TCP	742	57068 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=676 TSval=513589293 TSecr=1096068317
105	15.163722	10.0.0.133	128.119.245.12	TCP	1514	57068 → 80 [ACK] Seq=677 Ack=1 Win=131744 Len=1448 TSval=513589293 TSecr=1096068317
106	15.163723	10.0.0.133	128.119.245.12	TCP	1514	57068 → 80 [ACK] Seq=2125 Ack=1 Win=131744 Len=1448 TSval=513589293 TSecr=1096068317
107	15.166986	128.119.245.12	10.0.0.133	TCP	66	80 → 57059 [ACK] Seq=2 Ack=2 Win=227 Len=0 TSval=1096068317 TSecr=513589259

Packet 102 details:

- Ethernet II, Src: Technico_3c:55:7a (44:1c:12:3c:55:7a), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:2e)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133
- Transmission Control Protocol, Src Port: 80, Dst Port: 57068, Seq: 0, Ack: 1, Len: 0
 - Source Port: 80
 - Destination Port: 57068
 - [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)
 - 1010 = Header Length: 40 bytes (10)

Packet 102 hex dump:

```
0000 f0 b4 79 18 2e 2e 44 1c 12 3c 55 7a 08 00 45 00  ..y...D...<Uz...E..
0010 00 3c 00 00 40 00 2f 06 cb b3 80 77 f5 0c 0a 00  <...@/...w....
0020 00 85 00 50 de ec 0e 6b 19 d1 91 04 ee 1f a0 12  ...P...k.....
0030 71 20 03 55 00 00 02 04 05 b4 04 02 08 0a 41 54  q U.....AT
0040 ac d8 1e 9c c0 0b 01 03 03 07 .....
```

5.

seq: 229461

The image shows a Wireshark packet capture of an HTTP transaction. The packet list shows four packets: a 304 Not Modified response, a GET request, a POST request (packet 320), and a 200 OK response (packet 350). The packet details for packet 320 are expanded, showing the TCP segment with sequence number 229461, which is highlighted with a red box and an arrow. The packet bytes show the raw data of the HTTP POST request.

No.	Time	Source	Destination	Protocol	Length	Info
11	4.919437	10.0.0.179	10.0.0.133	HTTP	310	HTTP/1.1 304 Not Modified
18	4.981996	10.0.0.133	10.0.0.179	HTTP	187	GET /EventMgmt/EventTable?timeout=300 HTTP/1.1
320	15.378478	10.0.0.133	128.119.245.12	HTTP	1139	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (application/vnd.openxmlforma...
350	15.415237	128.119.245.12	10.0.0.133	HTTP	843	HTTP/1.1 200 OK (text/html)

Frame 320: 1139 bytes on wire (9112 bits), 1139 bytes captured (9112 bits) on interface 0

Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:55:7a)

Internet Protocol Version 4, Src: 10.0.0.133, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 57068, Dst Port: 80, Seq: 229461, Ack: 1, Len: 1073

Source Port: 57068

Destination Port: 80

[Stream index: 5]

[TCP Segment Len: 1073]

Sequence number: 229461 (relative sequence number)

[Next sequence number: 230534 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0020 f5 0c de ec 00 50 91 08 6e 73 0e 6b 19 d2 80 18P...ns.k....

0030 10 15 e6 2f 00 00 01 01 08 0a 1e 9c c0 f8 41 54 .../....AT

0040 ad b1 c5 bd 90 da 26 17 87 22 bb 00 5b ee 02 42&...["B

0050 74 40 f9 1a 74 3a e6 40 cb 12 7e 6a 4b 91 ea ea t@.t:@...~jK...

0060 62 0d 6c 5a 53 ca 20 fa 20 fc 40 c9 be 6d 72 d6 b.lZS...@.mr...

0070 b9 86 83 14 06 f7 04 83 77 c2 44 04 f6 29 c0 dew.D...)...

0080 8d 5e d8 23 ff ae ed 9d 1e 55 21 1d 25 ff d0 f2 .^.#....!U!%...

0090 9c 97 f8 e8 5b 77 9b b9 7d fc fc b7 b8 38 f9 b3[w...}....8...

00a0 4e c3 c1 0b 99 a3 9d 5f 36 e7 17 4b 06 8b 26 1c N....._6..K...&...

00b0 08 16 2a 3a d1 c9 f2 53 80 3b ba ad 60 f2 5c e2 .*:...S...'\...

00c0 67 7b 54 a7 3d ff 36 32 d5 a7 e9 d9 d2 c0 55 45 g{T=-62.....UE

00d0 df 1f 86 27 8d 20 cc ef 89 ff 06 00 00 ff ff 03 ...'..

Frame (1139 bytes) Reassembled TCP (230533 bytes)

Sequence number (tcp.seq), 4 bytes

Packets: 478 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) Profile: Default

/Users/therbh/lab3.pcapng 478 total packets, 4 shown

No.	Time	Source	Destination	Protocol	Length	Info
350	15.415237	128.119.245.12	10.0.0.133	HTTP	843	HTTP/1.1 200

OK (text/html)

Frame 350: 843 bytes on wire (6744 bits), 843 bytes captured (6744 bits) on interface 0

Ethernet II, Src: Technico_3c:55:7a (44:1c:12:3c:55:7a), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:2e)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133

Transmission Control Protocol, Src Port: 80, Dst Port: 57068, Seq: 1, Ack: 230534, Len: 777

Source Port: 80

Destination Port: 57068

[Stream index: 5]

[TCP Segment Len: 777]

Sequence number: 1 (relative sequence number)

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

Acknowledgment number: 230534 (relative ack number)

1000 = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window size value: 2037

[Calculated window size: 260736]

[Window size scaling factor: 128]

Checksum: 0x8c9c [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

[Timestamps]

TCP payload (777 bytes)

Hypertext Transfer Protocol

Line-based text data: text/html (11 lines)