

Question 1

- What is the IP address of the client that sends the HTTP GET request in the nat-inside-wireshark-trace1-1.pcapng trace?

Answer: 192.168.10.11

Screenshot:

```

3 0.00287... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=322727252 TSecr=802266926
4 0.02736... 192.168.10.11 138.76.29.8 HTTP 396 GET / HTTP/1.1
5 0.02939... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TStamp=802266954 TSecr=322727277
6 0.03067... 138.76.29.8 192.168.10.11 HTTP 613 HTTP/1.1 200 OK (text/html)
7 0.03146... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TStamp=322727281 TSecr=802266955
8 0.23140... 192.168.10.11 138.76.29.8 HTTP 317 GET /favicon.ico HTTP/1.1
9 0.23289... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TStamp=802267157 TSecr=322727481
10 0.23307... 138.76.29.8 192.168.10.11 HTTP 555 HTTP/1.1 404 Not Found (text/html)
11 0.23370... 192.168.10.11 138.76.29.8 TCP 66 53924 → 88 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TStamp=322727483 TSecr=802267158
12 5.18977... PCSSystemtec_82_ PCSSystemtec_89_ ARP 42 Who has 192.168.10.11? Tell 192.168.10.254
13 5.19179... PCSSystemtec_89_ PCSSystemtec_82_ ARP 60 192.168.10.11 is at 08:00:27:89:c7:7c
14 5.23454... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TStamp=802272158 TSecr=322727483
15 5.23470... 192.168.10.11 138.76.29.8 TCP 66 53924 → 88 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TStamp=322732484 TSecr=802267158
16 5.23614... 192.168.10.11 138.76.29.8 TCP 66 53924 → 88 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TStamp=322732485 TSecr=802272158
17 5.23804... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TStamp=802272161 TSecr=322732484
18 5.24172... PCSSystemtec_89_ PCSSystemtec_82_ ARP 60 Who has 192.168.10.254? Tell 192.168.10.11
19 5.24184... 192.168.10.11 138.76.29.8 TCP 42 192.168.10.254 is at 08:00:27:89:c7:7c

```

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 382
Identification: 0x6296 (25238)
0x10. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x64dc [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.10.11
Destination Address: 138.76.29.8
[Stream index: 0]

Explanation: The HTTP GET request is packet 4 in the pcap. The source IP is 192.168.10.11.

- What is the source port number of the TCP segment inside of this datagram containing the HTTP GET request sent by this client in the nat-inside-wireshark-trace1-1.pcapng trace?

Answer: 53924

Screenshot:

```

3 0.00287... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=1 ACK=1 Win=64256 Len=0 TStamp=322727252 TSecr=802266926
4 0.02736... 192.168.10.11 138.76.29.8 HTTP 396 GET / HTTP/1.1
5 0.02939... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TStamp=802266954 TSecr=322727277
6 0.03067... 138.76.29.8 192.168.10.11 HTTP 613 HTTP/1.1 200 OK (text/html)
7 0.03146... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TStamp=322727281 TSecr=802266955
8 0.23140... 192.168.10.11 138.76.29.8 HTTP 317 GET /favicon.ico HTTP/1.1
9 0.23289... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TStamp=802267157 TSecr=322727481
10 0.23307... 192.168.10.11 138.76.29.8 TCP 555 HTTP/1.1 404 Not Found (text/html)
11 0.23370... 192.168.10.11 138.76.29.8 TCP 66 53924 → 88 [ACK] Seq=582 Ack=1837 Win=64128 Len=0 TStamp=322727483 TSecr=802267158
12 5.18977... PCSSystemtec_82_ PCSSystemtec_89_ ARP 42 Who has 192.168.10.11? Tell 192.168.10.254
13 5.19179... PCSSystemtec_89_ PCSSystemtec_82_ ARP 60 192.168.10.11 is at 08:00:27:89:c7:7c
14 5.23454... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TStamp=802272158 TSecr=322727483
15 5.23470... 192.168.10.11 138.76.29.8 TCP 66 53924 → 88 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TStamp=322732484 TSecr=802267158
16 5.23614... 192.168.10.11 138.76.29.8 TCP 66 53924 → 88 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TStamp=322732485 TSecr=802272158
17 5.23804... 138.76.29.8 192.168.10.11 TCP 66 88 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TStamp=802272161 TSecr=322732484
18 5.24172... PCSSystemtec_89_ PCSSystemtec_82_ ARP 60 Who has 192.168.10.254? Tell 192.168.10.11
19 5.24184... 192.168.10.11 138.76.29.8 TCP 42 192.168.10.254 is at 08:00:27:89:c7:7c

```

Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x64dc [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.10.11
Destination Address: 138.76.29.8
[Stream index: 0]

Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Source Port: 53924
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 4]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 330]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 272978995
[Next Sequence Number: 331 (relative sequence number)]

Explanation: The HTTP GET message is 4 and under the TCP the source port is 53924.

3. What is the IP destination address of this datagram containing the HTTP GET request in the nat-inside-wireshark-trace1-1.pcapng trace?

Answer: 138.76.29.8.

Screenshot:

```

3 0.00287... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=322727252 TSecr=802266926
4 0.02736... 192.168.10.11 138.76.29.8 HTTP 396 GET / HTTP/1.1
5 0.02939... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TStamp=802266954 TSecr=322727277
6 0.03067... 138.76.29.8 192.168.10.11 HTTP 613 HTTP/1.1 200 OK (text/html)
7 0.03146... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TStamp=322727281 TSecr=802266955
8 0.23140... 192.168.10.11 138.76.29.8 HTTP 317 GET /favicon.ico HTTP/1.1
9 0.23289... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TStamp=802267157 TSecr=322727481
10 0.23307... 138.76.29.8 192.168.10.11 HTTP 555 HTTP/1.1 404 Not Found (text/html)
11 0.23370... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TStamp=322727483 TSecr=802267158
12 5.18977... PCSSystemtec_82.. PCSSystemtec_89.. ARP 42 Who has 192.168.10.11? Tell 192.168.10.254
13 5.19179... PCSSystemtec_89.. PCSSystemtec_82.. ARP 60 192.168.10.11 is at 08:00:27:89:c7:7c
14 5.23454... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TStamp=802272158 TSecr=322727483
15 5.23470... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TStamp=322732484 TSecr=802267158
16 5.23614... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TStamp=322732485 TSecr=802272158
17 5.23804... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TStamp=802272161 TSecr=322732484
18 5.24172... PCSSystemtec_89.. PCSSystemtec_82.. ARP 60 Who has 192.168.10.254? Tell 192.168.10.11
19 5.24172... PCSSystemtec_82.. PCSSystemtec_89.. ARP 60 192.168.10.254 is at 08:00:27:89:c7:7c

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 382
Identification: 0x6296 (25238)
0x0. .... = Flags: 0x2, Don't fragment
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x64dc [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.10.11
Destination Address: 138.76.29.8
[Stream index: 0]

```

Explanation: This is the same packet number 4 so if you look in the Internet Protocol tab it says Destination Address: 138.76.29.8.

4. What is the destination port number of the TCP segment in this datagram containing the HTTP GET request sent by this client in the nat-inside-wireshark-trace1-1.pcapng trace?

Answer: 80.

Screenshot:

```

3 0.00287... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=1 ACK=1 Win=64256 Len=0 TStamp=322727252 TSecr=802266926
4 0.02736... 192.168.10.11 138.76.29.8 HTTP 396 GET / HTTP/1.1
5 0.02939... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TStamp=802266954 TSecr=322727277
6 0.03067... 138.76.29.8 192.168.10.11 HTTP 613 HTTP/1.1 200 OK (text/html)
7 0.03146... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TStamp=322727281 TSecr=802266955
8 0.23140... 192.168.10.11 138.76.29.8 HTTP 317 GET /favicon.ico HTTP/1.1
9 0.23289... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TStamp=802267157 TSecr=322727481
10 0.23307... 138.76.29.8 192.168.10.11 HTTP 555 HTTP/1.1 404 Not Found (text/html)
11 0.23370... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TStamp=322727483 TSecr=802267158
12 5.18977... PCSSystemtec_82.. PCSSystemtec_89.. ARP 42 Who has 192.168.10.11? Tell 192.168.10.254
13 5.19179... PCSSystemtec_89.. PCSSystemtec_82.. ARP 60 192.168.10.11 is at 08:00:27:89:c7:7c
14 5.23454... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TStamp=802272158 TSecr=322727483
15 5.23470... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TStamp=322732484 TSecr=802267158
16 5.23614... 192.168.10.11 138.76.29.8 TCP 66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TStamp=322732485 TSecr=802272158
17 5.23804... 138.76.29.8 192.168.10.11 TCP 66 80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TStamp=802272161 TSecr=322732484
18 5.24172... PCSSystemtec_89.. PCSSystemtec_82.. ARP 60 Who has 192.168.10.254? Tell 192.168.10.11
19 5.24172... PCSSystemtec_82.. PCSSystemtec_89.. ARP 60 192.168.10.254 is at 08:00:27:89:c7:7c

Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x64dc [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.10.11
Destination Address: 138.76.29.8
[Stream index: 0]

Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Source Port: 53924
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 4]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 330]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2729789955
[Next Sequence Number: 331 (relative sequence number)]

```

Explanation: We are still in packet 4 which is the HTTP GET message. If you look under the transmission control protocol section it says destination port 80.

5. What is the destination IP address of the IP datagram carrying this HTTP 200 OK message?

Answer: 192.168.10.11.

Screenshot:

```

5 0.02939... 138.76.29.8      192.168.10.11    TCP      66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6 0.03067... 138.76.29.8      192.168.10.11    HTTP     613 HTTP/1.1 200 OK (text/html)
7 0.03146... 192.168.10.11    138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8 0.23140... 192.168.10.11    138.76.29.8      HTTP     317 GET /favicon.ico HTTP/1.1
9 0.23289... 138.76.29.8      192.168.10.11    TCP      66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10 0.23387... 138.76.29.8     192.168.10.11    TCP      555 HTTP/1.1 404 Not Found (text/html)
11 0.23370... 192.168.10.11    138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12 5.18977... PCSSystemtec_82.. PCSSystemtec_89.. ARP     42 Who has 192.168.10.11? Tell 192.168.10.254
13 5.19179... PCSSystemtec_89.. PCSSystemtec_82.. ARP     60 192.168.10.11 is at 08:00:27:89:c7:7c
14 5.23454... 138.76.29.8      192.168.10.11    TCP      66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
15 5.23470... 192.168.10.11    138.76.29.8      TCP      66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
16 5.23614... 192.168.10.11    138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
17 5.23804... 138.76.29.8      192.168.10.11    TCP      66 80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484
18 5.24172... PCSSystemtec_89.. PCSSystemtec_82.. ARP     60 Who has 192.168.10.254? Tell 192.168.10.11
19 5.24174... 0x666...        192.168.10.11    ARP     10:10.166.10.254.1 10:00:27:89:c7:7c 17

```

Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 599
 Identification: 0x6c7c (27772)
 > 010. = Flags: 0x2, Don't fragment
 ..0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 62
 Protocol: TCP (6)
 Header Checksum: 0x651d [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 138.76.29.8
 Destination Address: 192.168.10.11
 [Stream index: 0]

Explanation: The HTTP OK message is sent in packet 6 so if you look under the Internet Protocol Version under Destination Address it is 192.169.10.11.

6. What is the source IP address of the IP datagram carrying this HTTP GET message (as recorded in the nat-outside-wireshark-trace1-1.pcapng trace file)?

Answer: 10.0.1.254

Screenshot:

```

4 0.02735... 10.0.1.254      138.76.29.8      HTTP     396 GET / HTTP/1.1
5 0.02933... 138.76.29.8      10.0.1.254      TCP      66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6 0.03062... 138.76.29.8      10.0.1.254      TCP      613 HTTP/1.1 200 OK (text/html)
7 0.03144... 10.0.1.254      138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8 0.23140... 10.0.1.254      138.76.29.8      HTTP     317 GET /favicon.ico HTTP/1.1
9 0.23286... 138.76.29.8      10.0.1.254      TCP      66 80 → 53924 [ACK] Seq=548 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10 0.23368... 10.0.1.254      138.76.29.8      TCP      555 HTTP/1.1 404 Not Found (text/html)
11 0.23368... 10.0.1.254      138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12 5.18983... PCSSystemtec_43.. PCSSystemtec_22.. ARP     42 Who has 10.0.1.254? Tell 10.0.1.253
13 5.19170... PCSSystemtec_22.. PCSSystemtec_43.. ARP     60 10.0.1.253 is at 08:00:27:22:fd:74
14 5.23166... PCSSystemtec_22.. PCSSystemtec_43.. ARP     60 Who has 10.0.1.254? Tell 10.0.1.253
15 5.23170... PCSSystemtec_43.. PCSSystemtec_22.. ARP     42 10.0.1.254 is at 08:00:27:43:65:cd
16 5.23448... 138.76.29.8      10.0.1.254      TCP      66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
17 5.23470... 10.0.1.254      138.76.29.8      TCP      66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
18 5.23614... 10.0.1.254      138.76.29.8      TCP      66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
19 5.23804... 138.76.29.8      10.0.1.254      TCP      66 80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484
20 5.24172... 138.76.29.8      10.0.1.254      ARP     66 00:0c:29:4f:4e:00 → 00:0c:29:4f:4e:00 TSecr=322732485

Frame 4: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0 0000:08 00:27 22 fd 74 08:00:27 43 65 cd 08:00:45 00:01:00:00:00:00
Ethernet II, Src: PCSSystemtec_43:65:cd (08:00:27:43:65:cd), Dst: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74)
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 382
Identification: 0x6296 (25238)
> 010. .... = Flags: 0x2, Don't fragment
..0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 63
Protocol: TCP (6)
Header Checksum: 0x2492 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.1.254
Destination Address: 138.76.29.8
[Stream index: 0]

Frame 5: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0 0000:08 00:27 22 fd 74 08:00:27 43 65 cd 08:00:45 00:01:00:00:00:00
Ethernet II, Src: PCSSystemtec_22:fd:74 (08:00:27:22:fd:74), Dst: PCSSystemtec_43:65:cd (08:00:27:43:65:cd)
Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 599
Identification: 0x6c7c (27772)
> 010. .... = Flags: 0x2, Don't fragment
..0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 62
Protocol: TCP (6)
Header Checksum: 0x651d [validation disabled]
[Header checksum status: Unverified]
Source Address: 138.76.29.8
Destination Address: 10.0.1.254
[Stream index: 0]

```

Explanation: The packet is packet 4 so if you look under the Internet Protocol Version tab and look for source address 10.0.1.254.

7. What is the source port number of the TCP segment in the IP datagram carrying this HTTP GET message?

Answer: 53924

Screenshot:

```

Frame 4: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_43.. (08:00:27:43:65:cd), Dst: PCSSystemtec_22.. (08:00:27:22:fd:74)
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Source Port: 53924
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 4]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 330]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2729789995
[Next Sequence Number: 331 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2574368014
1000 .... = Header Length: 32 bytes (8)

```

Explanation: This is the same packet as the last question but to find the TCP source port look under the Transmission Control Protocol tab and by source port which is 53924.

8. Which of these four fields – IP source and destination addresses and TCP source and destination port numbers – are changed as the datagram carrying the HTTP GET message passed through the NAT router?

Answer: IP source address

Screenshot: inside

```

Frame 4: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_43.. (08:00:27:43:65:cd), Dst: PCSSystemtec_22.. (08:00:27:22:fd:74)
Internet Protocol Version 4, Src: 192.168.10.11, Dst: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Source Port: 53924
Destination Port: 80
[Stream index: 0]
[Stream Packet Number: 4]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 330]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2729789995
[Next Sequence Number: 331 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2574368014
1000 .... = Header Length: 32 bytes (8)

```

Outside

4 0.02735... 10.0.1.254	138.76.29.8	HTTP	396 GET / HTTP/1.1	
5 0.02933... 138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277	
6 0.03062... 138.76.29.8	10.0.1.254	HTTP	613 HTTP/1.1 200 OK (text/html)	
7 0.03144... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955	
8 0.03140... 10.0.1.254	138.76.29.8	HTTP	317 GET /favicon.ico HTTP/1.1	
9 0.03286... 138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481	
10 0.03304... 138.76.29.8	10.0.1.254	HTTP	555 HTTP/1.1 404 Not Found (text/html)	
11 0.03368... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158	
12 5.18983... PCSSystemtec_43.. PCSSystemtec_22.. ARP			42 Who has 10.0.1.253? Tell 10.0.1.254	
13 5.19170... PCSSystemtec_22.. PCSSystemtec_43.. ARP			60 10.0.1.253 is at 08:00:27:22:fd:74	
14 5.23166... PCSSystemtec_22.. PCSSystemtec_43.. ARP			60 Who has 10.0.1.254? Tell 10.0.1.253	
15 5.23170... PCSSystemtec_43.. PCSSystemtec_22.. ARP			42 10.0.1.254 is at 08:00:27:43:65:cd	
16 5.23448... 138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483	
17 5.23470... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158	
18 5.23614... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158	
19 5.23980... 10.0.1.254	138.76.29.8	TCP	66 80 → 53924 [FIN, ACK] Seq=1039 Win=64768 Len=0 TSval=322732485 TSecr=802272158	

Explanation: The IP source address in the inside file is 192.168.10.11 and when you look at the outside file it is 10.0.1.254.

9. Which of the following fields in the IP datagram carrying the HTTP GET are changed from the datagram received on the local area network (inside) to the corresponding datagram forwarded on the Internet side (outside) of the NAT router?

Answer:

Screenshot:

Explanation:

10. What is the destination IP address of the IP datagram carrying this HTTP reply (“200 OK”) message that is forwarded from the router to the destination host?

Answer: 10.0.1.254

Screenshot:

6 0.03062... 138.76.29.8	10.0.1.254	TCP	613 HTTP/1.1 200 OK (text/html)	
7 0.03144... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955	
8 0.03140... 10.0.1.254	138.76.29.8	HTTP	317 GET /favicon.ico HTTP/1.1	
9 0.03286... 138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481	
10 0.03304... 138.76.29.8	10.0.1.254	HTTP	555 HTTP/1.1 404 Not Found (text/html)	
11 0.03368... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158	
12 5.18983... PCSSystemtec_43.. PCSSystemtec_22.. ARP			42 Who has 10.0.1.253? Tell 10.0.1.254	
13 5.19170... PCSSystemtec_22.. PCSSystemtec_43.. ARP			60 10.0.1.253 is at 08:00:27:22:fd:74	
14 5.23166... PCSSystemtec_22.. PCSSystemtec_43.. ARP			60 Who has 10.0.1.254? Tell 10.0.1.253	
15 5.23170... PCSSystemtec_43.. PCSSystemtec_22.. ARP			42 10.0.1.254 is at 08:00:27:43:65:cd	
16 5.23448... 138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483	
17 5.23470... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158	
18 5.23614... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158	
19 5.23980... 10.0.1.254	138.76.29.8	TCP	66 80 → 53924 [FIN, ACK] Seq=1039 Win=64768 Len=0 TSval=322732485 TSecr=802272158	

6 0.03062... 138.76.29.8	10.0.1.254	TCP	613 HTTP/1.1 200 OK (text/html)	
7 0.03144... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955	
8 0.03140... 10.0.1.254	138.76.29.8	HTTP	317 GET /favicon.ico HTTP/1.1	
9 0.03286... 138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481	
10 0.03304... 138.76.29.8	10.0.1.254	HTTP	555 HTTP/1.1 404 Not Found (text/html)	
11 0.03368... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158	
12 5.18983... PCSSystemtec_43.. PCSSystemtec_22.. ARP			42 Who has 10.0.1.253? Tell 10.0.1.254	
13 5.19170... PCSSystemtec_22.. PCSSystemtec_43.. ARP			60 10.0.1.253 is at 08:00:27:22:fd:74	
14 5.23166... PCSSystemtec_22.. PCSSystemtec_43.. ARP			60 Who has 10.0.1.254? Tell 10.0.1.253	
15 5.23170... PCSSystemtec_43.. PCSSystemtec_22.. ARP			42 10.0.1.254 is at 08:00:27:43:65:cd	
16 5.23448... 138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483	
17 5.23470... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158	
18 5.23614... 10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158	
19 5.23980... 10.0.1.254	138.76.29.8	TCP	66 80 → 53924 [FIN, ACK] Seq=1039 Win=64768 Len=0 TSval=322732485 TSecr=802272158	

Explanation: Since this message is coming from the router we have to look at the outside pcap. If you look at the HTTP OK under Internet Protocol Version you will find the destination address as 10.0.1.254.

Question 2

- What is the IP address of the client computer (source) that is transferring the file to gaia.cs.umass.edu? Enter the IP address in dotted decimal notation (include each dot, and omit any leading zeros for any byte, e.g., 10.1.216.54):

Answer: 192.168.1.187

Screenshot:

```

Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{AA627FA5-5A5C-42FA-BF66-47E61A6EC4C0}, id 0
Ethernet II, Src: Intel_a9:d3:a0 (cc:2f:71:a9:d3:a0), Dst: Verizon_d6:a6:72 (48:5d:36:d6:a6:72)
Internet Protocol Version 4, Src: 192.168.1.187, Dst: 128.119.245.12
    Identification: 0xe390 (58256)
    Flags: 0x02, Don't fragment
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xdf57 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.187
    Destination Address: 128.119.245.12
    [Stream index: 1]

```

Explanation: This is the beginning of the file transfer so I looked to see what the source is under Internet Protocol Version tab. It is 192.168.1.187.

- What is the client-side port number of the client computer (source) that is transferring the file to gaia.cs.umass.edu? Enter the port integer port number (digits only, no commas), with no leading 0's:

Answer: 6186

Screenshot:

```

Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{AA627FA5-5A5C-42FA-BF66-47E61A6EC4C0}, id 0
Ethernet II, Src: Intel_a9:d3:a0 (cc:2f:71:a9:d3:a0), Dst: Verizon_d6:a6:72 (48:5d:36:d6:a6:72)
Internet Protocol Version 4, Src: 192.168.1.187, Dst: 128.119.245.12
    Identification: 0xe390 (58256)
    Flags: 0x02, Don't fragment
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xdf57 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.187
    Destination Address: 128.119.245.12
    [Stream index: 1]

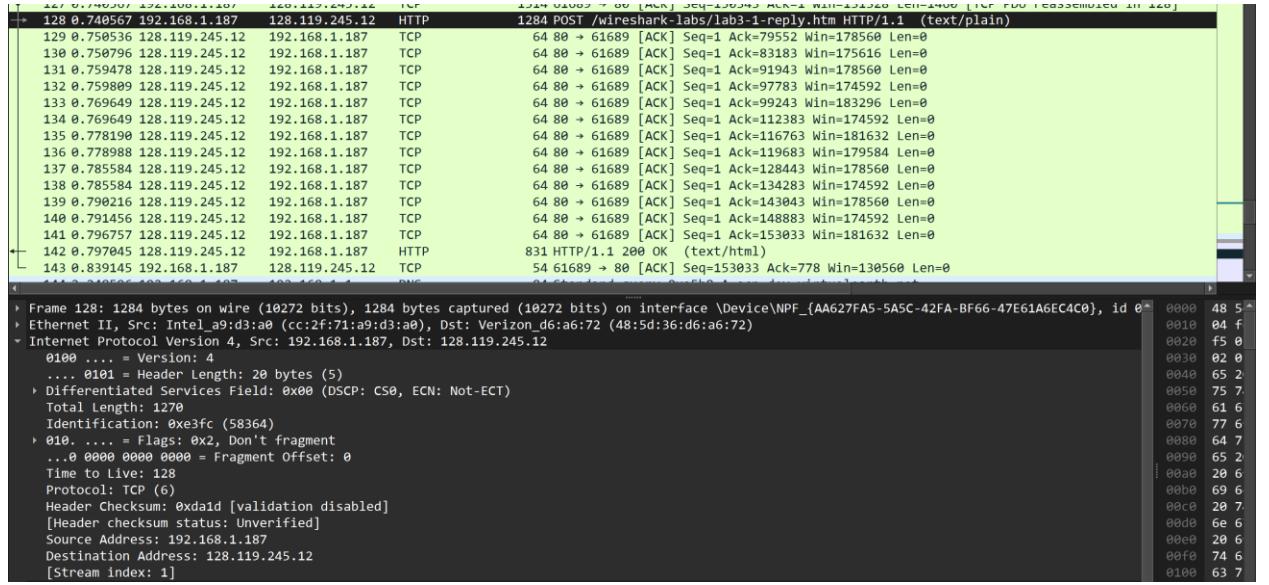
```

Explanation: This is in packet 2 so if you look under the transmission control protocol tab you will see source port. The source port is equal to 61686.

- What is the IP address of the gaia.cs.umass.edu server to which the alice.txt file will be uploaded via the HTTP POST? Enter the IP address in dotted decimal notation (include each dot, and omit any leading zeros for any byte, e.g., 10.1.216.54):

Answer: 128.119.245.12

Screenshot:

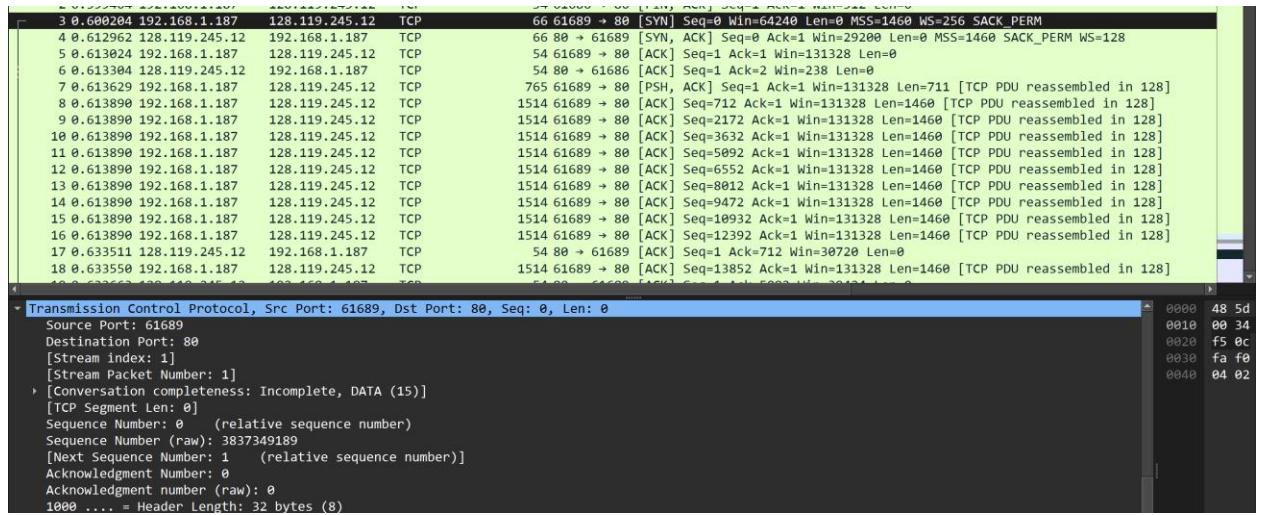


Explanation: The HTTP POST packet number is 128. If you look under the Internet Protocol Version tab you should then look under Destination address and you will see 128.119.245.12

- What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? Enter the sequence number (digits only, no commas), with no leading 0's:

Answer: 0 (relative) and 3837349189 (raw)

Screenshot:

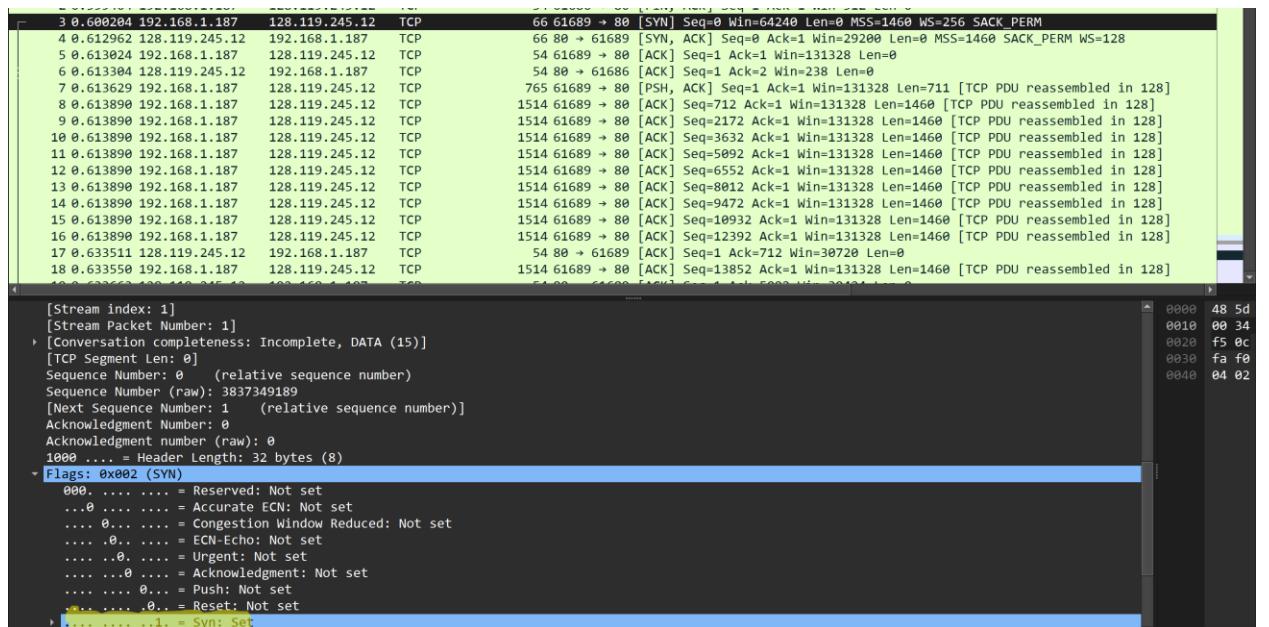


Explanation: The TCP SYN message is the first one that starts the file transfer. If you look under the transmission control protocol tab you can see the sequence number. The relative sequence number is 0 and the raw sequence number is 3837349189. I included both just in case.

- What is it in this TCP segment that identifies the segment as a SYN segment?

Answer: The SYN Flag is set by being set to 1.

Screenshot:



Explanation: If you look in packet 3 under the transmission control protocol tab you will be the flags section. This identifies packets. In our selected packet you can see that the Syn flag is set by being set to 1.

6. What is the value in the Acknowledgment field of the TCP SYNACK segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? Enter the acknowledgment number (digits only, no commas), with no leading 0's:

Answer: 1 (relative ack) and 3837349190 (raw)

Screenshot:

```

[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3837349190
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
    000.... = Reserved: Not set
    ...0.... = Accurate ECN: Not set
    ....0... = Congestion Window Reduced: Not set
    ....0.. = ECN-Echo: Not set
    ....0.. = Urgent: Not set
    ....1.... = Acknowledgment: Set
    ....0... = Push: Not set
    ....0.. = Reset: Not set
    ....1.. = Syn: Set
    [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
        [Connection establish acknowledge (SYN+ACK): server port 80]
        [Severity level: Chat]
        [Group: Sequence]
    ....0.. = Fin: Not set
    [TCP Flags: .....A..S.]

```

Explanation: If you look in packet 4 which is the TCP SYNACK packet under the transmission control protocol tab you will see the acknowledgement numbers. The relative number is 1 and the raw number is 3837349190.

7. Are there any retransmitted segments in the trace file? YES or NO:

Answer: No

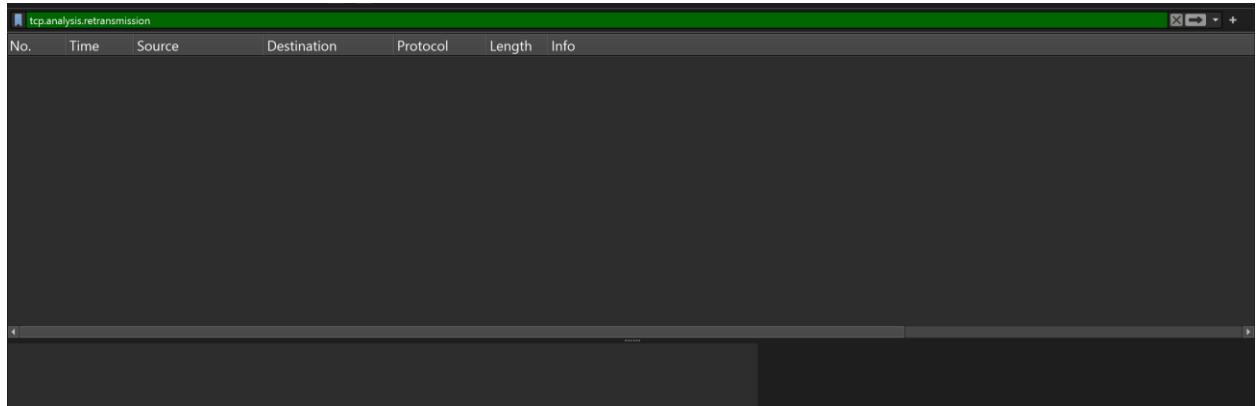
Screenshot:

Explanation: There is nothing shown when I filter for tcp.analysis.retransmission.

8. How did you determine whether or not there were retransmitted segments?

Answer: I filtered the packets with `tcp.analysis.retransmission`.

Screenshot:

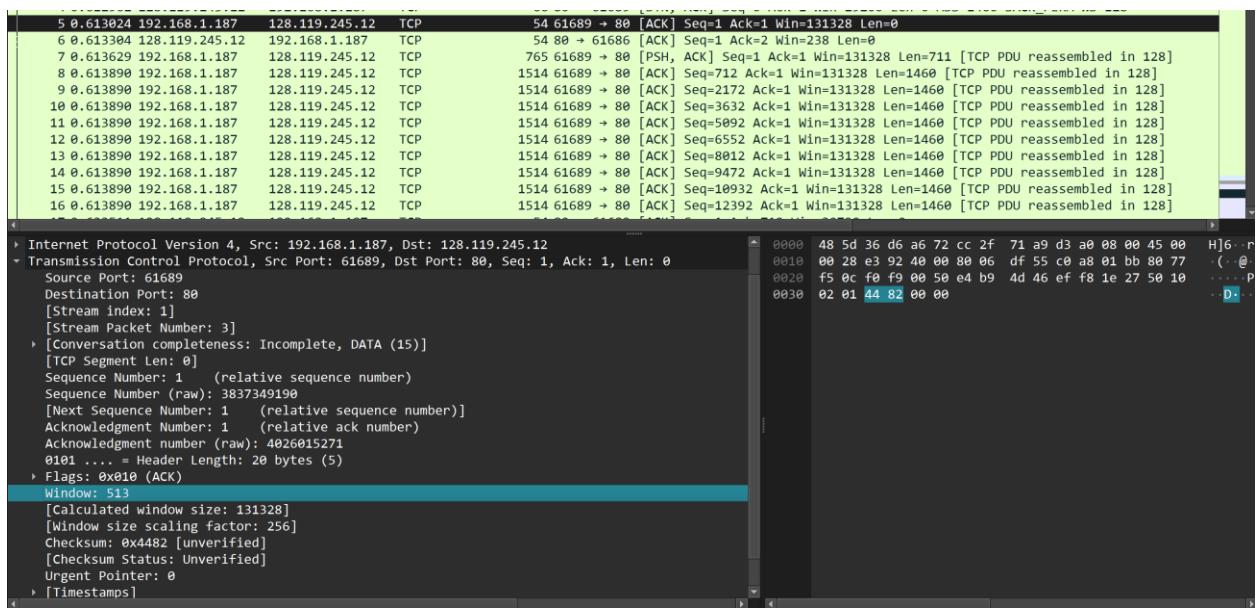


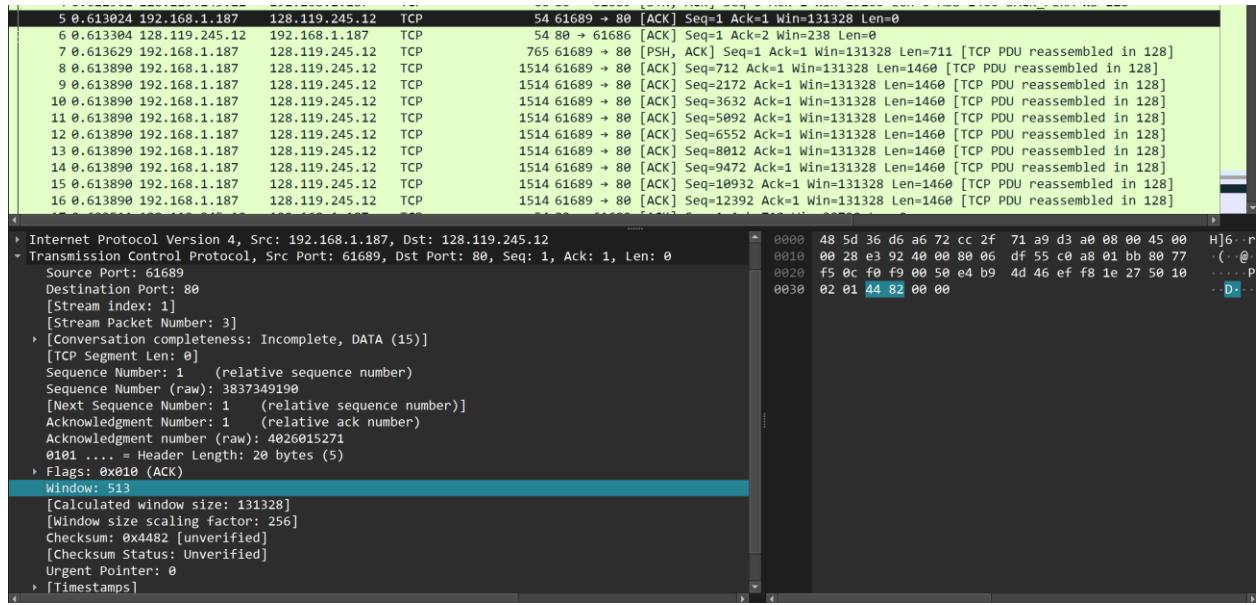
Explanation: This scans to see if any empty window sizes are sent. This sees if any not complete ones make it.

9. How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to `gaia.cs.umass.edu`?

Answer: Mainly 513

Screenshot:





Explanation: Most of them transmit 513 bytes but one does 238.

10. What is the throughput (bytes transferred per unit time) for the TCP connection?

Answer: 153032bytes / 0.740567seconds

Screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
•	119 0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=140123 Ack=1 Win=1313
•	120 0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=141583 Ack=1 Win=1313
•	121 0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=143043 Ack=1 Win=1313
•	122 0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=144503 Ack=1 Win=1313
•	123 0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=145963 Ack=1 Win=1313
•	124 0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [PSH, ACK] Seq=147423 Ack=1 Win
•	125 0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=148883 Ack=1 Win=1313
•	126 0.740531	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=70792 Win=17088
•	127 0.740567	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=150343 Ack=1 Win=1313
→	128 0.740567	192.168.1.187	128.119.245.12	HTTP	1284	POST /wireshark-labs/lab3-1-reply.htm HTTP
	129 0.750536	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=79552 Win=17856
	130 0.750796	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=83183 Win=17561
	131 0.759478	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=91943 Win=17856
	132 0.759809	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=97783 Win=17459
	133 0.769649	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=99243 Win=18329
	134 0.769649	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=112383 Win=1745
	135 0.778190	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=116763 Win=1816
	136 0.778988	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=119683 Win=1795

Sequence Number (raw): 3837500992
[Next Sequence Number: 153033 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 4026015271
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x35a6 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
▶ [Timestamps]
▶ [SEQ/ACK analysis]
TCP payload (1230 bytes)
TCP segment data (1230 bytes)
▶ [106 Reassembled TCP Segments (153032 bytes): #7(711), #8(1460), #9(1460), #10(1460), #11(1460)

Explanation: Divide $153032 / 0.740567$. This is taken by the TCP segments 153032 bytes and the time that was found then.

11. How did you calculate the throughput (bytes transferred per unit time) for the TCP connection?

Answer: You take the total bytes that are sent and divide it by the time at the final TCP connection.

Screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
• 119	0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=140123 Ack=1 Win=1313
• 120	0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=141583 Ack=1 Win=1313
• 121	0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=143043 Ack=1 Win=1313
• 122	0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=144503 Ack=1 Win=1313
• 123	0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=145963 Ack=1 Win=1313
• 124	0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [PSH, ACK] Seq=147423 Ack=1 Win=1313
• 125	0.730862	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=148883 Ack=1 Win=1313
126	0.740531	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=70792 Win=17088
127	0.740567	192.168.1.187	128.119.245.12	TCP	1514	61689 → 80 [ACK] Seq=150343 Ack=1 Win=1313
→ 128	0.740567	192.168.1.187	128.119.245.12	HTTP	1284	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1
129	0.750536	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=79552 Win=17856
130	0.750796	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=83183 Win=17561
131	0.759478	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=91943 Win=17856
132	0.759809	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=97783 Win=17459
133	0.769649	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=99243 Win=18329
134	0.769649	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=112383 Win=1745
135	0.778190	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=116763 Win=1816
136	0.778988	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=119683 Win=1795
137	0.785501	128.119.245.12	192.168.1.187	TCP	64	80 → 61689 [ACK] Seq=1 Ack=120142 Win=17088

Sequence Number (raw): 3837500992
[Next Sequence Number: 153033 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 4026015271
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x35a6 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (1230 bytes)
TCP segment data (1230 bytes)
[106 Reassembled TCP Segments (153032 bytes): #7(711), #8(1460), #9(1460), #10(1460), #11(1460)]

Explanation: This was found by looking at the POST reply and seeing the total bytes at that moment and divide it by that time.