CIS-427

With Dr. Zheng Song

Student: Demetrius Johnson

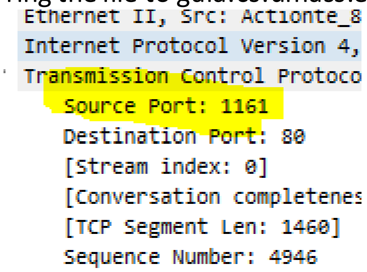
Program Assignment 2: WireShark

10 December 2022

Part 2: Analyzing TCP

1.

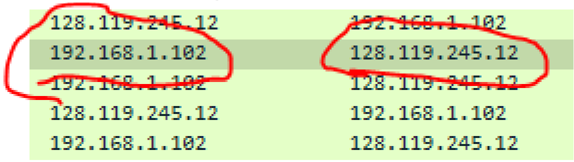
What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?



```
Ethernet II, Src: Actionte_8
Internet Protocol Version 4,
Transmission Control Protoco
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [Conversation completenes
    [TCP Segment Len: 1460]
    Sequence Number: 4946
```

- Source port as shown in the screenshot of client is **1161**,

What is the IP address of gaia.cs.umass.edu?



```
128.119.245.12      192.168.1.102
192.168.1.102       128.119.245.12
192.168.1.102       128.119.245.12
128.119.245.12      192.168.1.102
192.168.1.102       128.119.245.12
```

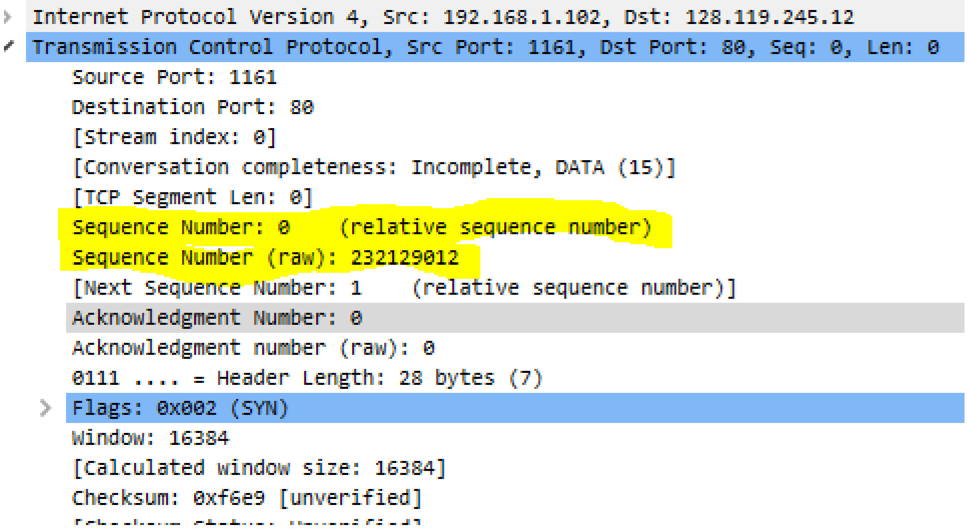
- **192.168.1.102** is the client IP, and **128.119.245.12** is the IP address of gaia.cs.umass.edu.

On what port number is it sending and receiving TCP segments for this connection?

- As in the screenshot from the first part of this question, data is being sent via TCP over HTTP port **80** (unsecure/unencrypted web server port).

2.

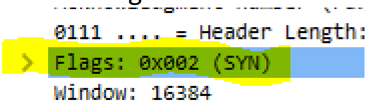
What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu?



```
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
      Source Port: 1161
      Destination Port: 80
      [Stream index: 0]
      [Conversation completeness: Incomplete, DATA (15)]
      [TCP Segment Len: 0]
      Sequence Number: 0    (relative sequence number)
      Sequence Number (raw): 232129012
      [Next Sequence Number: 1    (relative sequence number)]
      Acknowledgment Number: 0
      Acknowledgment number (raw): 0
      0111 .... = Header Length: 28 bytes (7)
    > Flags: 0x002 (SYN)
      Window: 16384
      [Calculated window size: 16384]
      Checksum: 0xf6e9 [unverified]
      [Checksum Status: Unverified]
```

- As shown above, The raw base/initial sequence number (which is randomly generated for security purposes) is **232129012.** This is the origin/start byte for the connection, so Wireshark sets relative sequence number = 0 (it adds this field as part of the program to make it easy for us to follow how many and which bytes are sent in a packet over TCP).

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

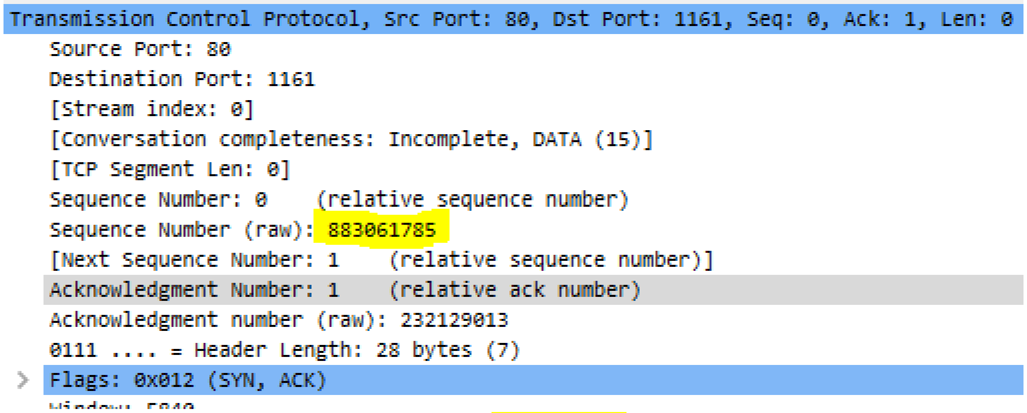


```
0111 .... = Header Length:
> Flags: 0x002 (SYN)
  Window: 16384
```

- The SYN flag bit in the TCP header is set, denoting that the message is a SYN segment/message.

3.

What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?



```
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 883061785
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 232129013
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x012 (SYN, ACK)
    Window: 5840
```

- The raw sequence number sent by gaia is **883061785**, as shown in the screenshot.

What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value?

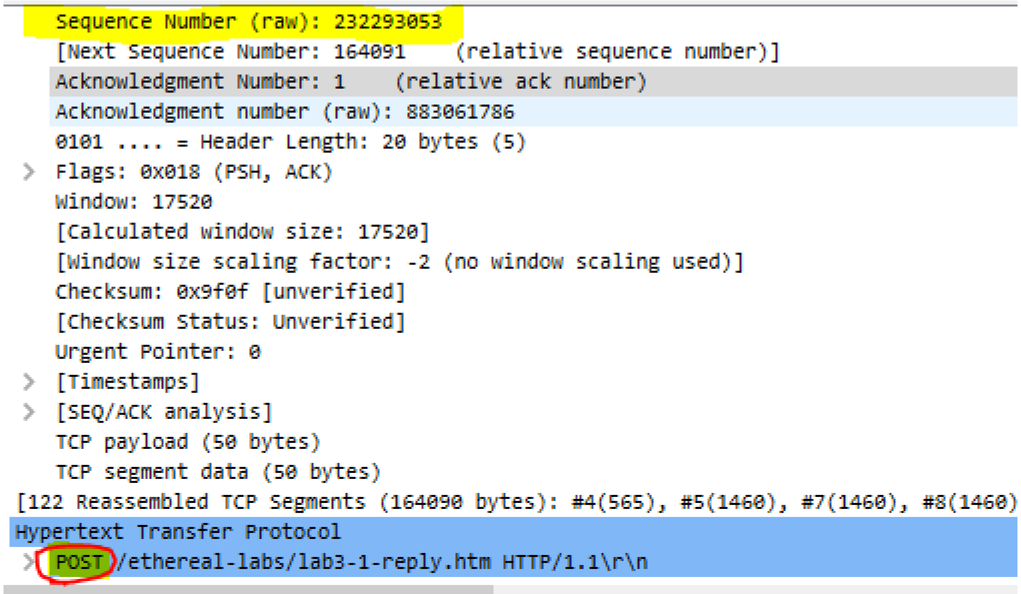
- The value of the ACK (as shown in the above screenshot) is **232129013**. It is determined by the sequence number that was sent by the client from the initial SYN message, and as you notice it is +1 more than the sequence number sent by the client because it means that it received 1 byte, and it is ready for the next stream of bytes starting at the ACK number that it sends to the client.

What is it in the segment that identifies the segment as a SYNACK segment?

- All PSH, SYN, FIN, ACK messages are denoted by the respective bit being set to true (1) in the header. Thus, in the SYNACK message (as shown in the screenshot above), the SYN and ACK bits were both set.

4.

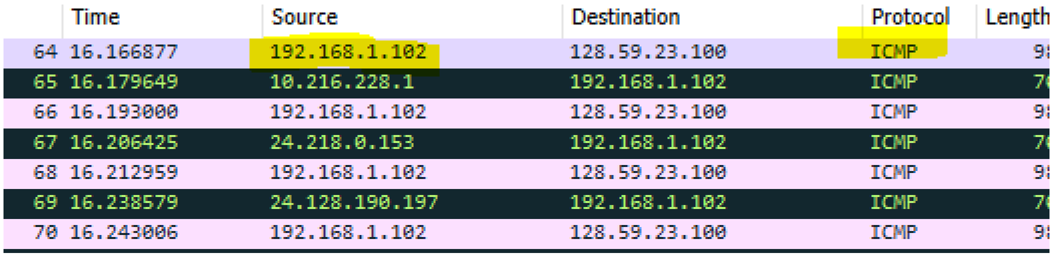
What is the sequence number of the TCP segment containing the HTTP POST command?



```
    Sequence Number (raw): 232293053
    [Next Sequence Number: 164091    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 883061786
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x9f0f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (50 bytes)
    TCP segment data (50 bytes)
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460)
Hypertext Transfer Protocol
  > POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1\r\n
```

- As shown, sequence number of the POST message (sent by client requesting that server make updates to its database based on data sent with the POST message) is **232293053** as the *raw sequence number* (**164091** for *relative*, meaning (*164091 - 1)* number of bytes have been transmitted from the client to the server and the next stream starting at that byte number is being sent with the POST message).

Part 3: Analyzing IP



	Time	Source	Destination	Protocol	Length
64	16.166877	192.168.1.102	128.59.23.100	ICMP	9
65	16.179649	10.216.228.1	192.168.1.102	ICMP	7
66	16.193000	192.168.1.102	128.59.23.100	ICMP	9
67	16.206425	24.218.0.153	192.168.1.102	ICMP	7
68	16.212959	192.168.1.102	128.59.23.100	ICMP	9
69	16.238579	24.128.190.197	192.168.1.102	ICMP	7
70	16.243006	192.168.1.102	128.59.23.100	ICMP	9

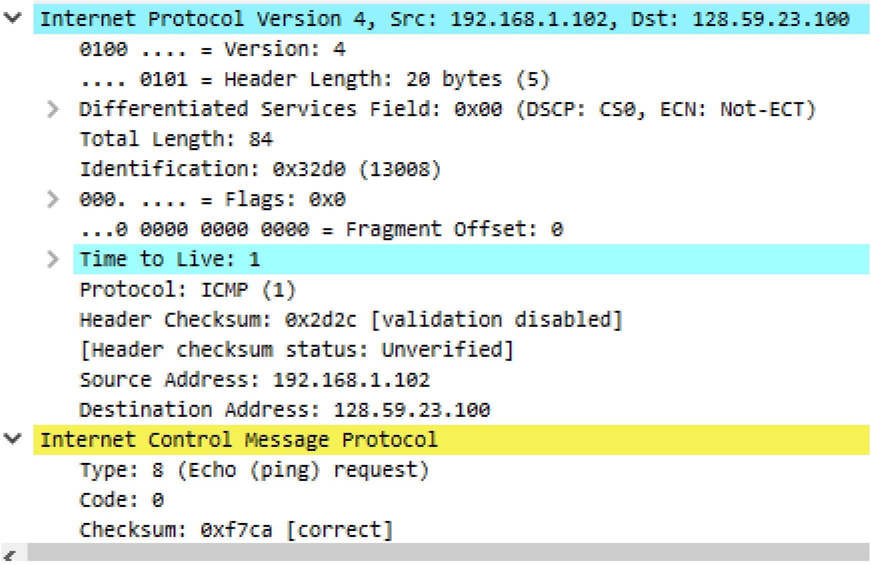
5.

What is the IP address of the computer running traceroute?

- 192.168.1.102

6.

Select the first ICMP Echo Request message, and expand the Internet Protocol part of the packet in the packet details window. Within the IP packet header, what is the value in the upper layer protocol field?



```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 84
     Identification: 0x32d0 (13008)
   > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
   > Time to Live: 1
     Protocol: ICMP (1)
     Header Checksum: 0x2d2c [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.102
     Destination Address: 128.59.23.100
v Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0xf7ca [correct]
```

- IP Version 4 (denoted in ASCII by “45 E”)

7.

How many bytes are in the IP header?

- 20 bytes

How many bytes are in the payload of the IP datagram?

- The IP datagram is 84 bytes in total (including header).

Explain how you determined the number of payload bytes.

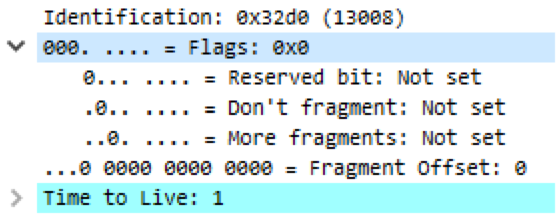
- You simply look inside of the IP information that Wireshark provides and it will tell you "Total Length"; this is not to be confused with "Length" field for the entire datagram, which includes the length of all encapsulated layers combined.

8.

Has this IP datagram been fragmented?

- No it was not fragmented.

Explain how you determined whether or not the datagram has been fragmented.



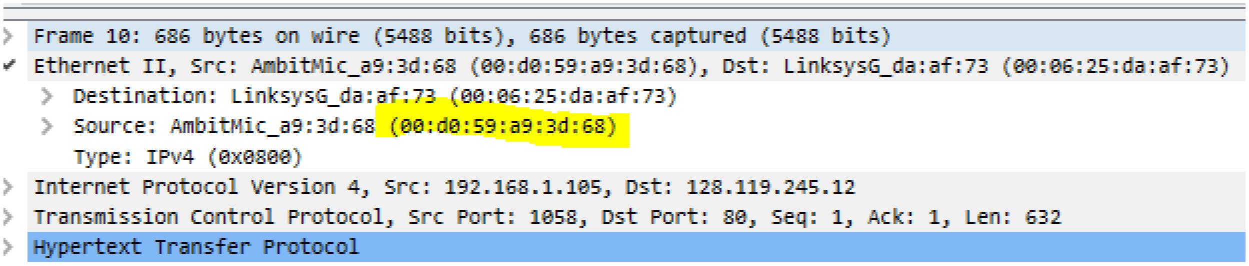
```
   Identification: 0x32d0 (13008)
v  000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment Offset: 0
>  Time to Live: 1
```

- As shown in the screenshot above, we can see that the datagram was not formed from IP fragmentation (and thus fragment flag bits are not set), which is not necessary for ICMP messages which are small enough that they can be sent by one IP packet. In fact, ICMP is not really encapsulated by IP but rather implemented and ran in parallel/tandem with IP protocol and is a connectionless protocol.

Part 4: Analyzing Ethernet Frames

9.

What is the 48-bit Ethernet address of the host that browses the webpage http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html?

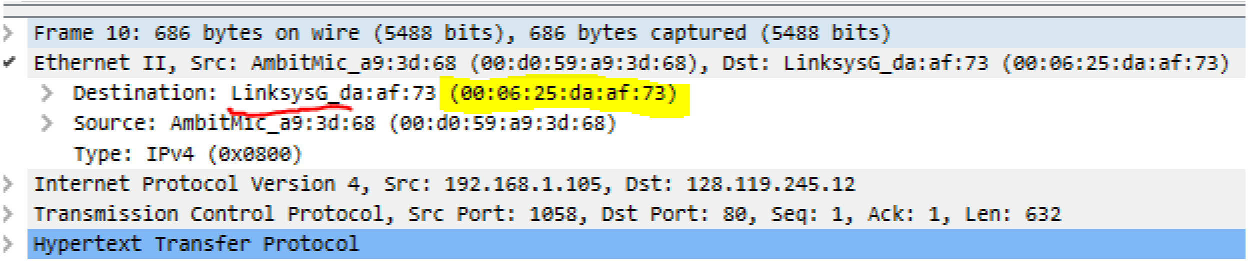


```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
✓ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
> Hypertext Transfer Protocol
```

- 48-bit MAC address (output in hexadecimal) of the host is shown highlighted above.

10.

What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?



```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
✔ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
> Hypertext Transfer Protocol
```

-
- The MAC address of the destination is highlighted above; the red underline denotes the manufacturer who is identified by the first 32 bits of the 48-bit MAC. It is the address of the default gateway → the local router to which the host is connected to and is depending on to route its traffic to the next hop on the public side (the internet).