Name: Muhammad Hamza Khan

Roll Number: 21L-5654

**Lab Number 8**

**Lab Statement 1:**

Question 1:

What is the IP address and TCP port number used by the client computer

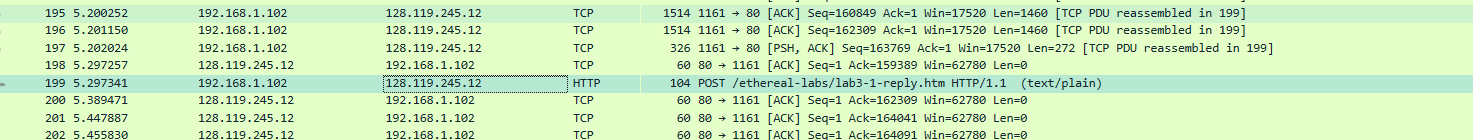
(source) that is transferring the file to gaia.cs.umass.edu?

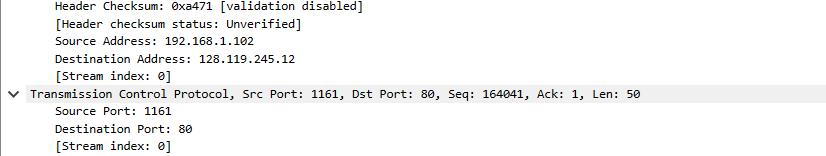
Ans:

Client:

IP address of client : 192.168.1.102

TCP port number of client: 1161





Question 2:

What is the IP address of gaia.cs.umass.edu? On what port number is it

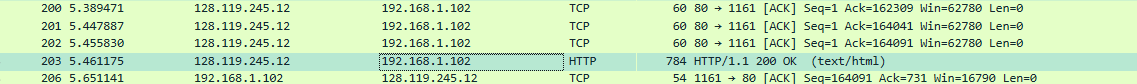
sending and receiving TCP segments for this connection?

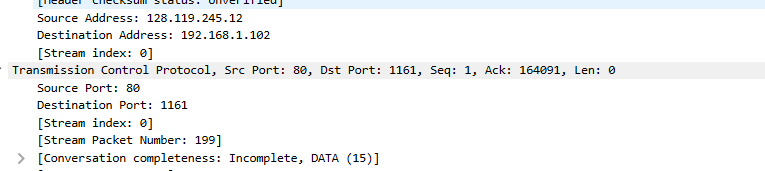
Ans:

gaia.cs.umass.edu:

IP address: 128.119.245.12

TCP port number of gaia.cs.umass.edu : 80





Question 3:

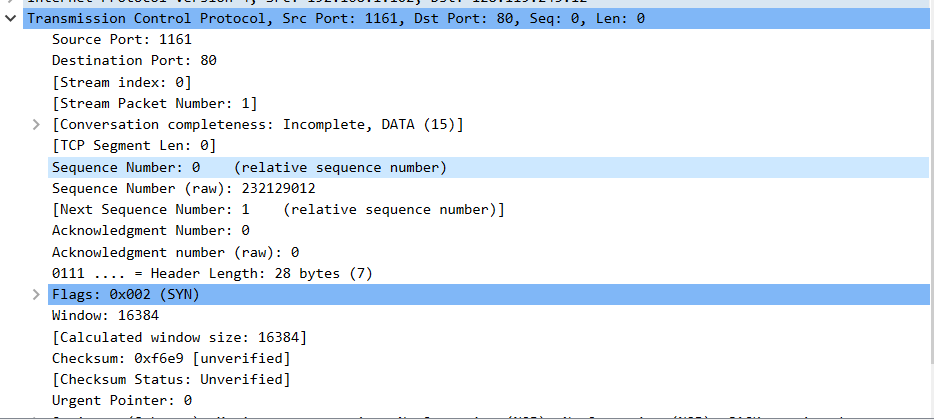
What is the sequence number of the TCP SYN segment that is used to initiate

the TCP connection between the client computer and gaia.cs.umass.edu? What is in the

segment that identifies the segment as a SYN segment?

Ans:

SYN Flag: The TCP header will indicate that the SYN flag is set to 1. This is crucial as it distinguishes a SYN segment from other types of segments (like data or ACK segments)



Sequence Number of the TCP SYN segment:

Relative Sequence Number: 0

Raw Sequence Number: 232129012.

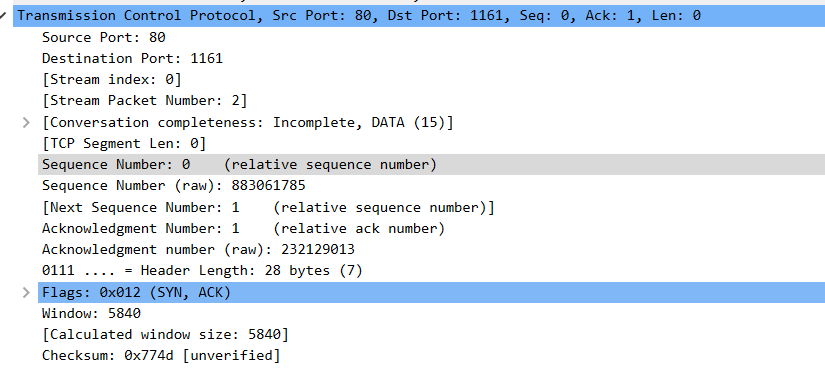
The Flags field shows a value of 0x002(initiate TCP), which corresponds to the SYN flag.

So, the sequence number for the TCP SYN segment is 232129012 (raw), and it is identified as a SYN segment by the SYN flag set in the Flags field.

Question 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? What is the value of the Acknowledgement field in the SYNACK segment? What is it in the segment that identifies the segment as a SYNACK segment?

Ans:



Sequence Number (SYN-ACK): 883061785.

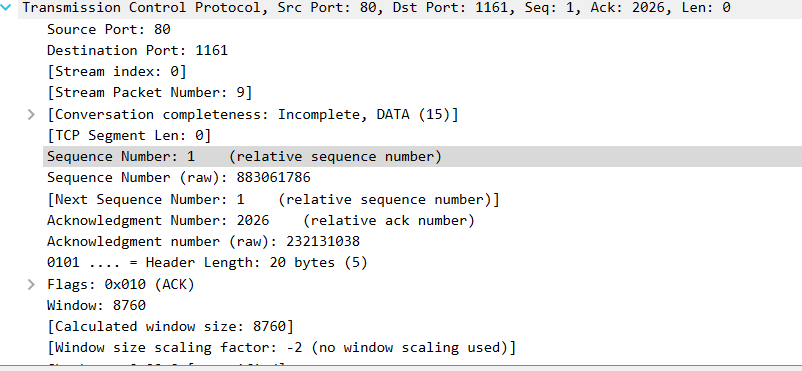
Acknowledgment Number (SYN-ACK): 232129013.

Identifying the SYN-ACK: The flags set to SYN (0x012)and ACK (0x010) flags.

Question 5:

In packet 9, Ack = 2026 and Seq = 1. Explain these values?

Ans:



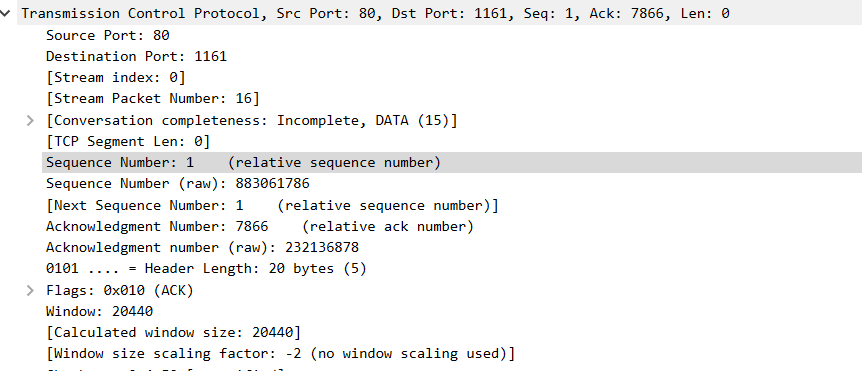
Seq = 1: The client is sending data starting from sequence number 1. It is initial handshake, where sequence number 0 does not contain actual data, so the first data-carrying packet starts with sequence number 1.

And Ack = 2026: The client has received all data from the server up to sequence number 2025. The acknowledgment number 2026 tells the server that the client is ready to receive the next byte from 2026 onward.

Question 6:

In packet 16, Ack = 7866 and Seq = 1. Explain these values?

Ans:



Seq = 1: First data segement sent to client.

Ack = 7866: Ack of 7866 means that data is received up to sequence number 7865 and is now expecting the next sequence number 7866.

Question 7:

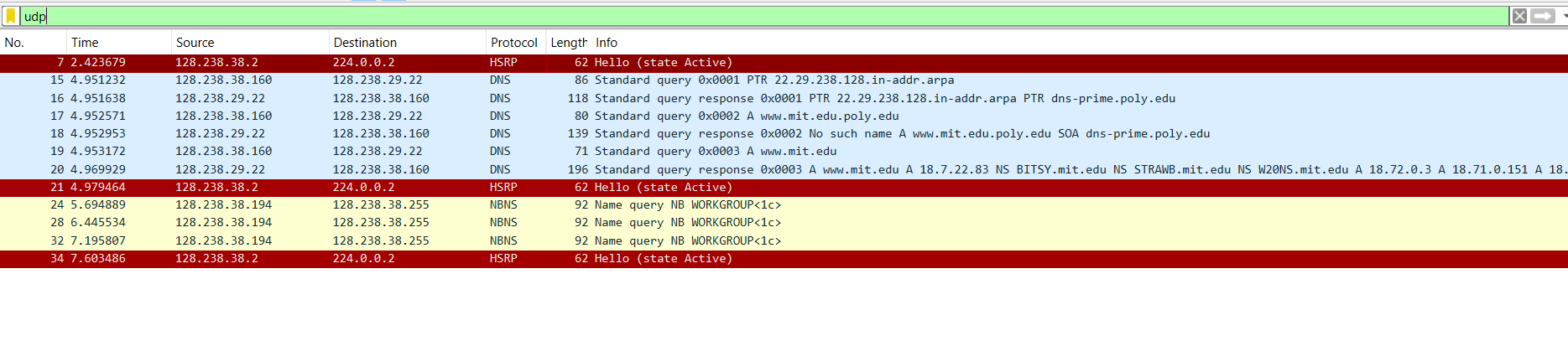
Why Wireshark uses relative sequence and ack?

Ans:

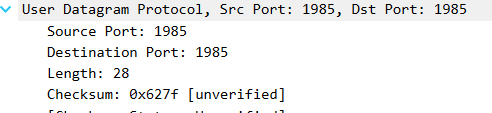
Wireshark uses relative sequence and acknowledgment numbers to make TCP analysis easier by:

* Readable: Relative numbers start at 0,easy tracking.
* Track of reodering of packets over network.
* Providing consistency

**Lab Statement 2:**



Question 1:



It has 4 fields i.e source port,Dest port,Length and checksum

Question 2:

From the packet content field (click on any header and observe the display in

the Packet Bytes Window), determine the length (in bytes) of each of the UDP header fields.

Ans:

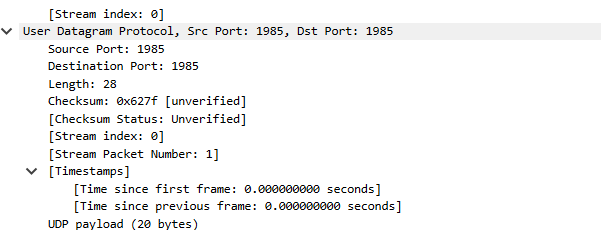
Fields are Source Port: 2 bytes

Destination Port: 2 bytes

Length: 2 bytes

Checksum: 2 bytes

Total UDP Header Length:8 bytes

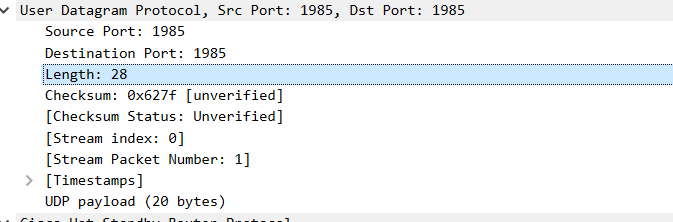


Question 3:

The value in the Length field is the length of what? Verify your claim using

the selected packet.

Ans:

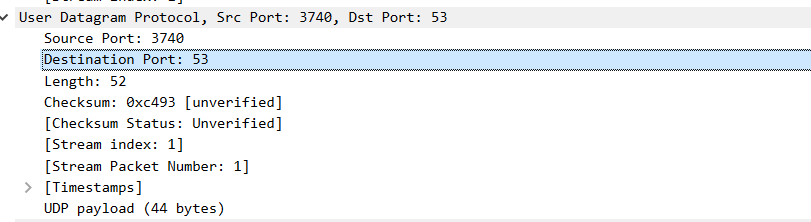


The "Length" field shown in the screenshot indicates the total length of the UDP packet, which includes the length of both the UDP header and the data (payload).

Length = 28.

Question 4:

What is the port number to query the DNS Server?



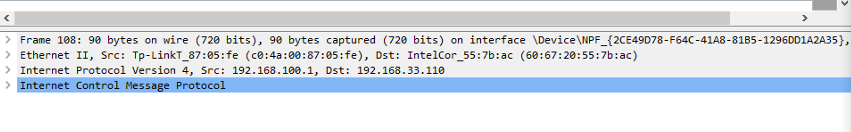
53 Port Number is used as dest DNS .

Lab Statement 3:

1. Are ICMP messages sent over UDP or TCP?

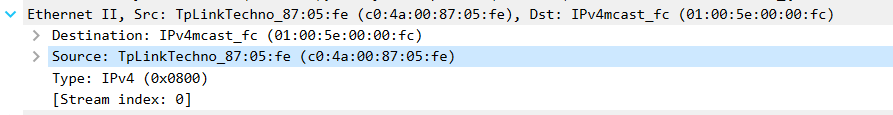
Ans:

ICMP messages don’t use the transport layer, so they neither use UDP nor TCP because they are not sent between a client and server instead, they are sent between a router and an end host. That’s why you don't see a TCP or UDP header in an ICMP packet.



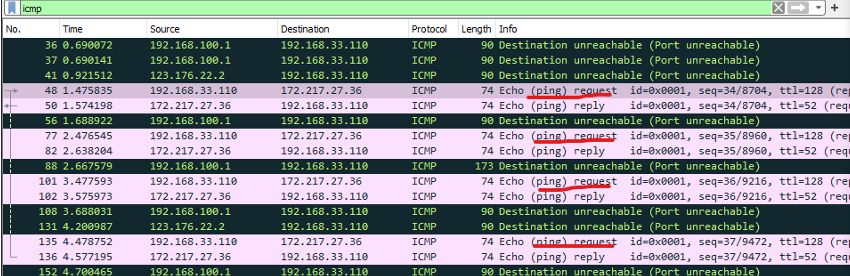
1. What is the link-layer (e.g., Ethernet) address of the host?

The MAC address (link-layer address) of the host is: Tp-LinkT\_87:05:fe (c0:4a:00:87:05:fe)



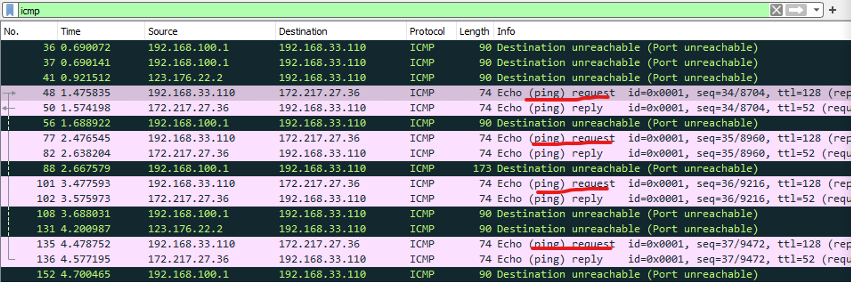
1. Which kind of request is sent through these ICMP packets?

Ans: ICMP packets are usually used to send ping requests. ICMP packets are also used to send back information of the packets that could not reach their destination.



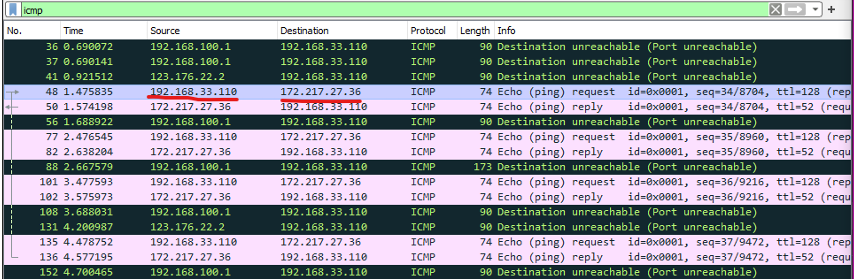
1. How many requests are sent through the host?

There were ping requests sent through the host.



1. What is the IP address of your host? What is the IP address of the destination host?

The IP address of my host is: 192.168.33.110 and the IP address of my destination host is: 172.217.27.36.

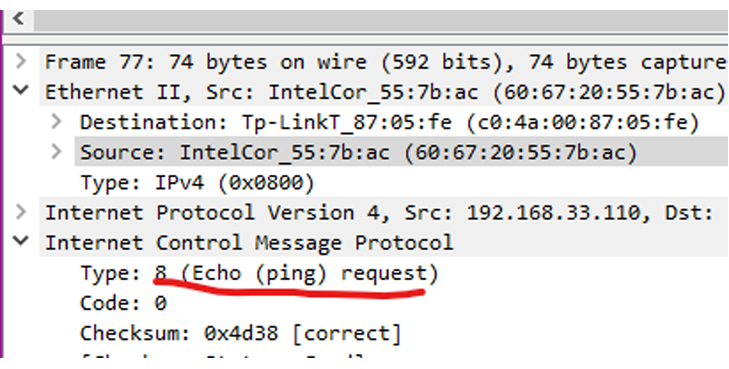


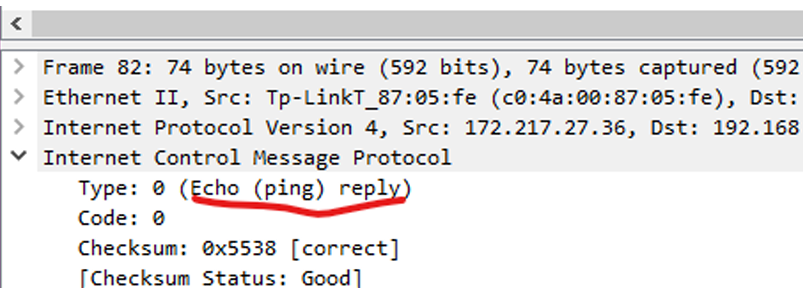
1. Why is it that an ICMP packet does not have source and destination port numbers?

Source and Destination port numbers are used to identify application layer processes running on an end host, as the ICMP runs on a router only used for error handling while transferring packets along a network they are not associated with any process hence they don't require a transport layer header, so they don’t have any source and destination port numbers.

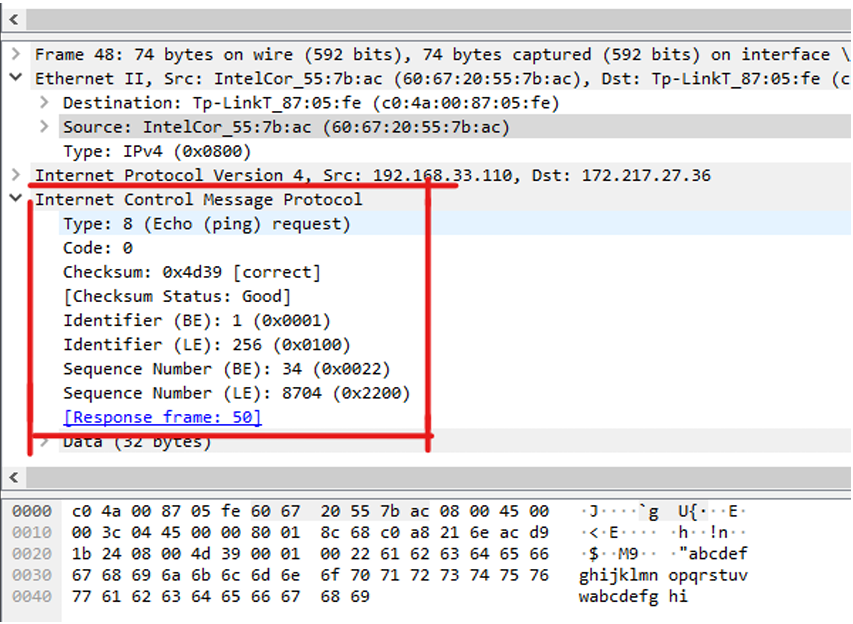
1. What values in the ICMP request message differentiate this message from the ICMP reply message?

Ans: The type in the ICMP request message differentiates this message from the ICMP reply message. For ICMP request message the type is 8 and for an ICMP reply message the type is 0.



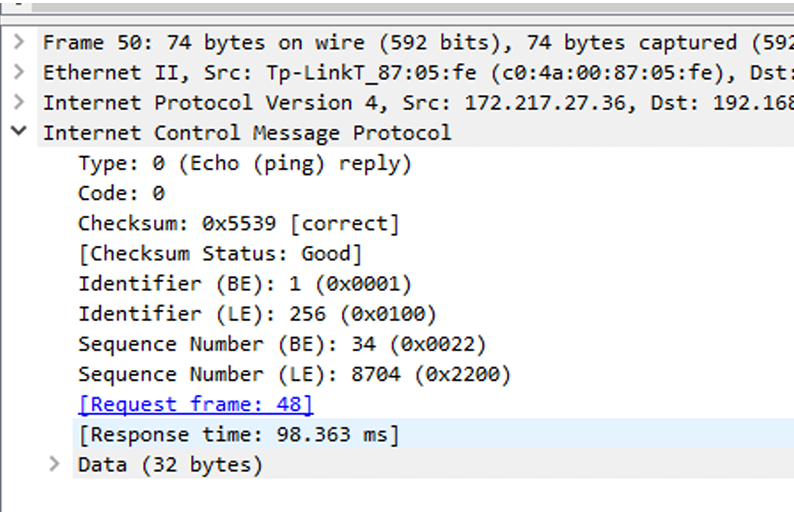


1. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?



The Type tells what type of ICMP message it is, many ICMP type messages Code field to further classify a message. In this case Type is 8 (ping request) and Code is 0 (no code). The other fields are Checksum, Identifier, and Sequence Number. Identifier and Sequence Number are represented in both little endian and big-endian formats. Each of these fields have 2 bytes of data.

1. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?



The Type in this case is 0 (ping reply) and Code is 0 (no code). The other fields are Checksum, Identifier, and Sequence Number. Identifier and Sequence Number are represented in both little endian and big-endian formats. Each of these fields have 2 bytes of data.

1. Examine packet no 56. What are the ICMP type and code numbers? Why is the IP and TCP Header included in the ICMP Header? What do these headers depict?

Ans: The Type in this case is 3 (Destination unreachable) and Code is 3 (Port unreachable).

The IP and TCP headers belong to the packet whose destination port was not reachable, these headers are sent back to the source to tell the source host that “this” packet could not reach its destination.