**Lab 10**

**Farhan Bukhari**

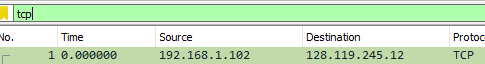
**21L-5247**

**BCS-5F1**

**Lab Statement 1**

**Q1**

IP Address is 192.168.1.102



Port 1161



**Q2**

IP Address is 128.119.245.12

****

Port 80

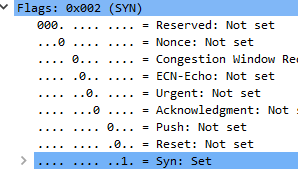


**Q3**

Sequence number is:



SYN flag is set



**Q4**

Sequence number is:



Below info tells it is SYN+ACK Packet



**Q5**

Ack =2026 determines that it has successfully read 2026 bytes of data.

As for seq=1, It is the Ack number of the last connection which was Ack =1 in frame =11.

In frame 11 if we add seq num and Len of the bytes we get 2026 which is the Ack number.

**Q6**

Ack =7866 determines that it has successfully read 7866 bytes of data.

As for seq=1, It is the Ack number of the last connection which was Ack =1 in frame =11.

In frame 11 if we add seq num and Len of the bytes we get 7866 which is the Ack number.

**Q7**

Using relative sequence numbers is a usability enhancement, making the numbers easier to read and compare. In order to compare a dissection with data from a less advanced analyzer

that can not handle relative sequence numbers it might be required to temporarily disable this

feature in Wireshark.

The ACK indicates that a host is acknowledging having received some data, and the PSH,

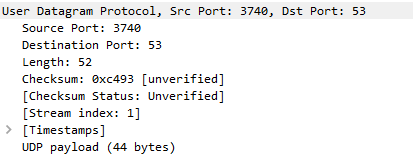
ACK indicates the host is acknowledging receipt of some previous data and also transmitting

some more data.

**Lab Statement 2**

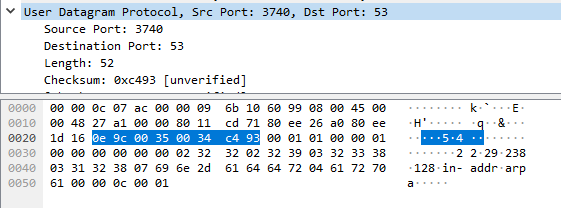
**Q1**

There are 4 header fields in DNS



**Q2**

The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.



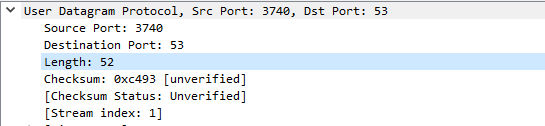
**Q3**

The length field indicates the number of bytes in the UDP segment (header and data).

An explicit length value is required because the data field size can vary from UDP segment to UDP segment.

The UDP payload length of the selected packet is 44 bytes.

52 bytes - 8 bytes = 44 bytes.

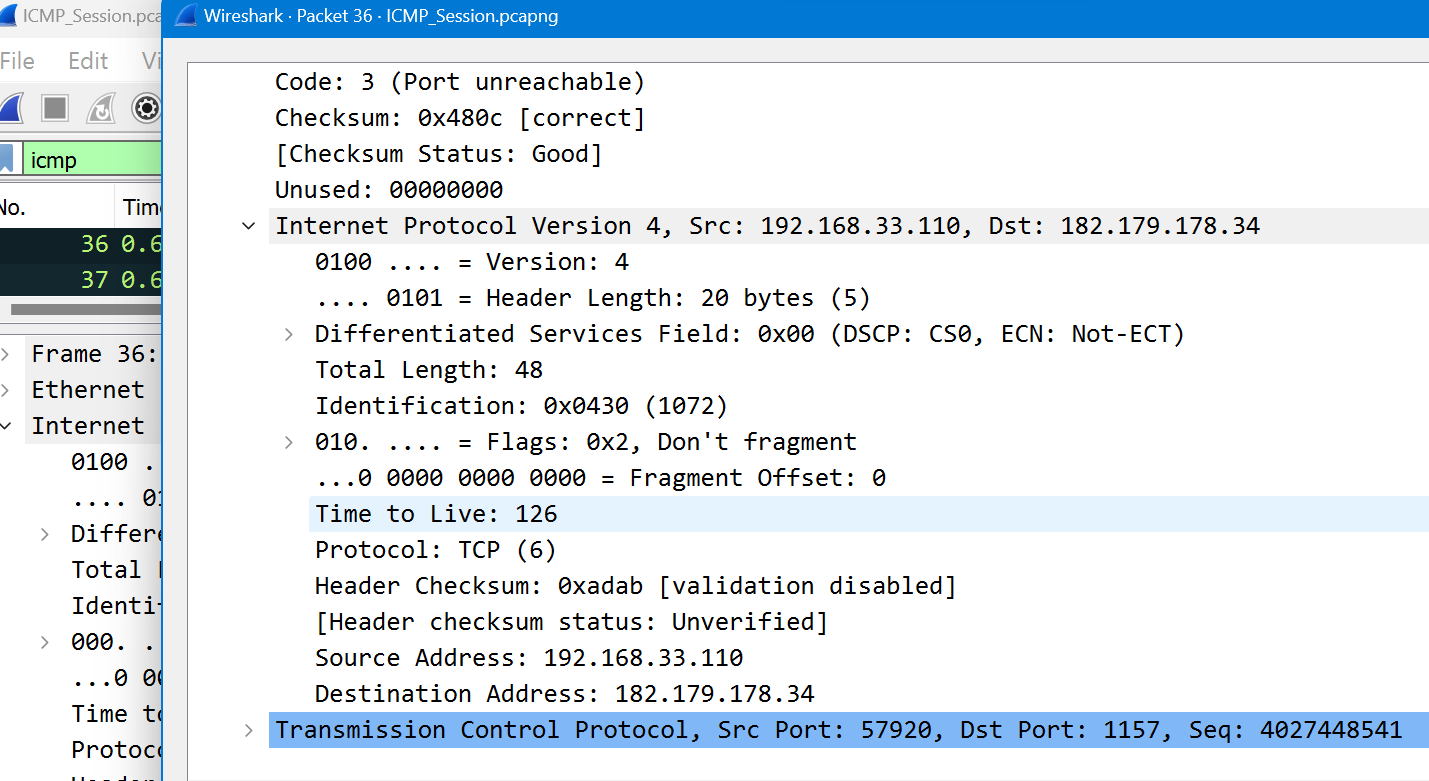


**Q4**

The Domain Name System (DNS) uses TCP port 53 and UDP port 53.

**Lab Statement 3**

**Q1**

****

Therefore, the data is transferred through TCP Protocol

**Q2**

Ethernet Address is:



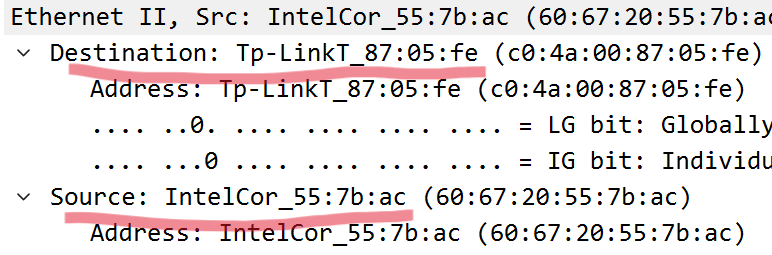
**Q3**

**ECHO** requests are being sent through packets.

**Q4**

Host is sending 4 requests.

**Q5**



**Q6**

ICMP (Internet Control Message Protocol) packets do not have source and destination port numbers because ICMP operates at the IP (Internet Protocol) layer, which is a lower layer than the transport layer where port numbers are used.

**Q7**

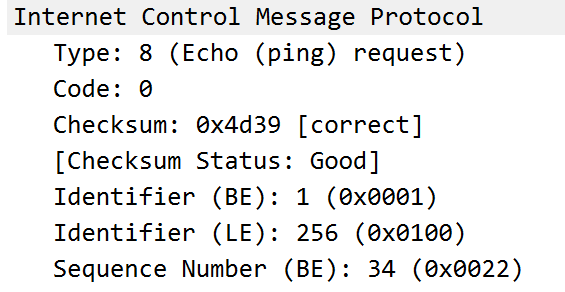
These are differentiated on following basis:

**ICMP Echo Request**: The ICMP Type value for an Echo Request message is typically 8. This message is used to request an Echo Reply from the destination device.

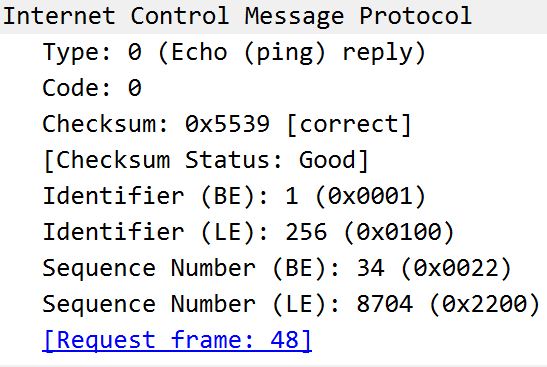
**ICMP Echo Reply**: The ICMP Type value for an Echo Reply message is usually 0. It is sent by the destination device in response to an Echo Request.

Also the ICMP identifiers and sequence numbers are different.

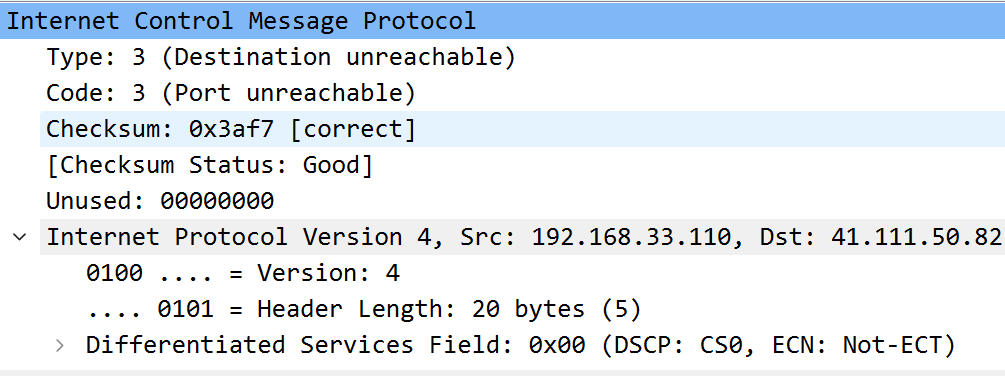
**Q8**



**Q9**



**Q10**



In some ICMP (Internet Control Message Protocol) packets, the IP (Internet Protocol) and TCP (Transmission Control Protocol) headers may be included as part of the ICMP header for specific types of ICMP messages. This is known as an ICMP error message. It occurs when destination in unreachable.