Muhammad Laraib Akhtar

21l-5294

BCS-5B

Lab 10

**Lab Statement 1: Analyzing TCP Packets using Wireshark (10)**

**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?**

IP address: 192.168.1.102

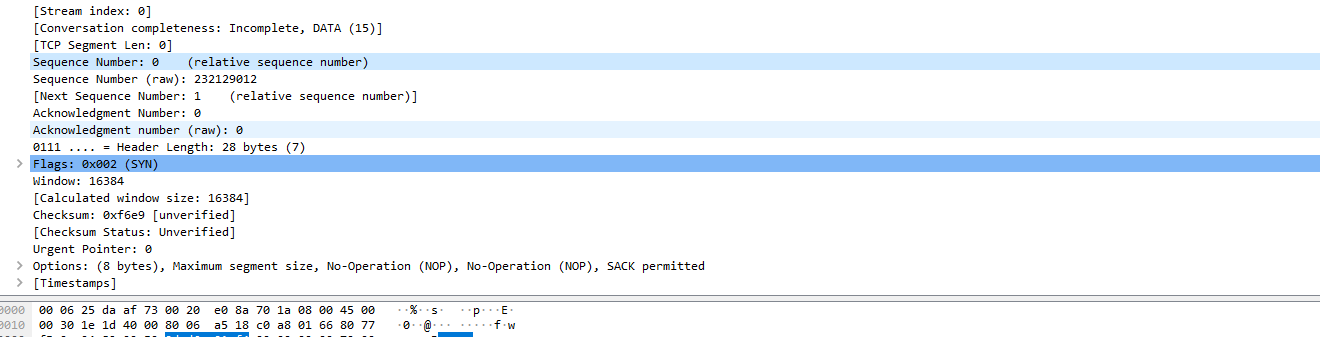
TCP port: 1161

**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?**

IP address: 128.119.245.12

TCP port: 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?**

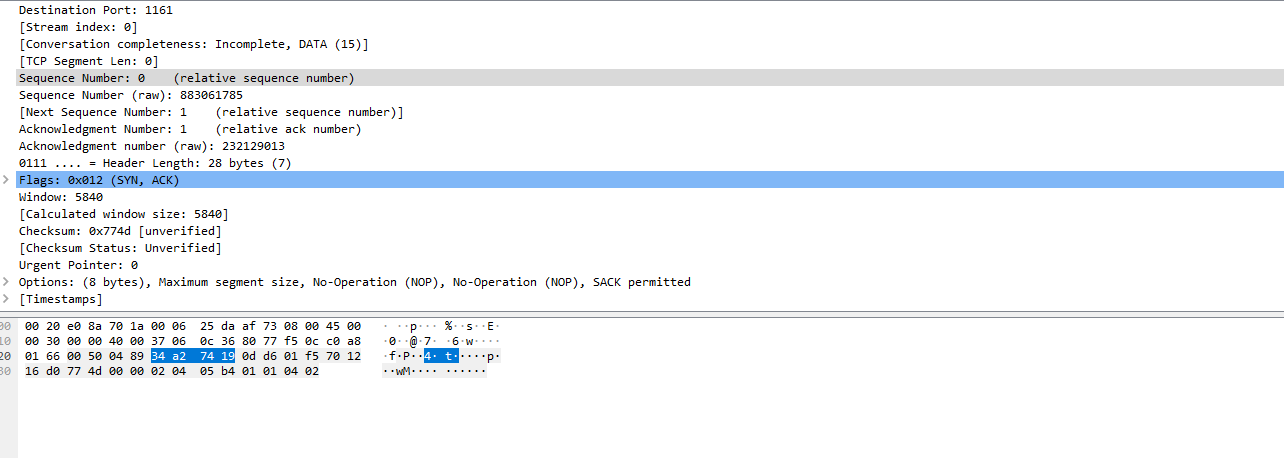


Sequence number: 0

Flag bit is on to recognize this as a SYN segment.

**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?**

****

Sequence number: 0

Acknowledgement Number: 1

Flag bit is on to recognize this as a SYNACK segment

**\*Question 5: In packet 9, Ack = 2026 and Seq = 1. Explain these values?**

Bytes up to 2026 have been acknowledged and seq 1 is a relative number asking the client to send the next bit.

**\*Question 6: In packet 16, Ack = 7866 and Seq = 1. Explain these values?**

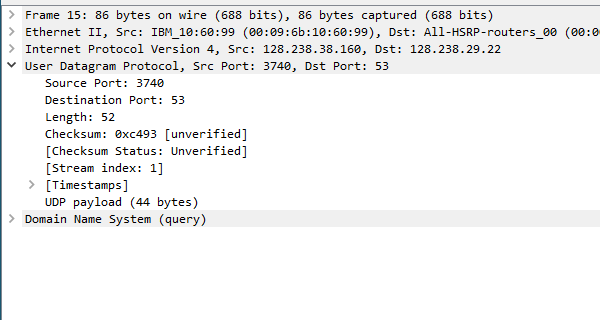
Bytes up to 7866 have been acknowledged and seq 1 is a relative number asking the client to send the next bit.

**Question 7: Why Wireshark uses relative sequence and ack?**

WireShark groups TCP sessions and assigns them relative sequence (and acknowledgment) numbers which start from 0 (and incrementing by 1 as it seems, for each subsequent packet) so the user can identify the sequence of events.

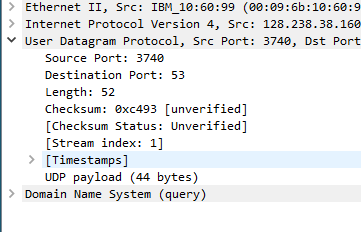
**Lab Statement 2: Analyzing UDP Packets using Wireshark (5)**

**Question 1: Select the first DNS packet in the trace. Determine, how many fields there are in the UDP header**

****

Number of fields in UDP: 4

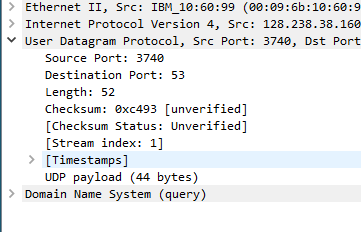
**Question 2: From the packet content field (click on any header and observe the display in the Packet Bytes Window), determine the length (in bytes) of each of the UDP header fields.**

****

Source Port = Destination Port = Length = Checksum = 2 bytes

Total: 8 bytes

**Question 3: The value in the Length field is the length of what? Verify your claim using the selected packet.**

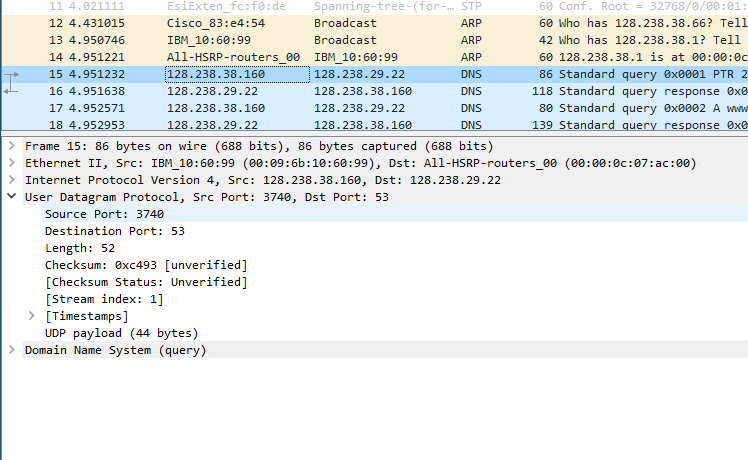
****

Payload; 44 bytes

UDP Header length = 8 bytes

Length = 8+44 = 52 bytes

**Question 4: What is the port number to query the DNS Server?**



DNS Port: 53

**Lab Statement 3: Analyzing ICMP Packets using Wireshark (5)**

|  |  |
| --- | --- |
| **1-** Are ICMP messages sent over UDP or TCP? | Unlike the Internet Protocol (IP), ICMP is not associated with a transport layer protocol such as TCP or UDP. This makes ICMP a connectionless protocol: one device does not need to open a connection with another device before sending an ICMP message. |
| **2-** What is the link-layer (e.g., Ethernet) address of the host? |  |
| **3-** Which kind of request is sent through these ICMP packets? | 1) Echo Request and Echo Reply (Ping). |
| **4-** How many requests are sent through the host? | 4 |
| **5-** What is the IP address of your host? What is the IP address of the destination host? | Source host:192.168.33.110  Destination host:172.217.27.36 |
| **6-** Why is it that an ICMP packet does not have source and destination port numbers? | ICMP (Internet Control Message Protocol) packets do not have source and destination port  numbers because ICMP operates at a different layer of the network stack compared to protocols  like TCP and UDP. ICMP and TCP/UDP serve different purposes in the network stack. ICMP is  focused on network control and diagnostics, while TCP and UDP are used for end-to-end  application data transfer. As a result, ICMP packets lack the concept of source and destination  port numbers, which are specific to transport layer protocols like TCP and UDP. |
| **7-** What values in the ICMP request message differentiate this message from the ICMP reply message? | Request: The Type field is set to 8    Reply: The Type field is set to 0 |
| **8-** 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? | A screenshot of a computer  Description automatically generated |
| **9-** 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? | A screenshot of a computer program  Description automatically generated |
| **10-** Examine the packet no 56. What are the ICMP type and code numbers? Why is the IP and TCP Header included in the ICMP Header? What does these headers depict? | The IP and TCP headers are not included within the ICMP header; rather, ICMP messages are encapsulated within IP packets, and the IP and TCP headers provide necessary information for routing and delivering the ICMP packet. By including these headers, the ICMP message provides detailed information to the sender about why a particular packet was unreachable or encountered an issue. It helps in diagnosing network problems and understanding the specific cause of the problem. |

