National University of Computer and Emerging Sciences



**Laboratory Manuals**

*for*

**Computer Networks**

(CL -307)

|  |  |
| --- | --- |
| Course Instructor |  |
| Lab Instructor(s) |  |
| Section |  |
| Semester |  |

Department of Computer Science

FAST-NU, Lahore, Pakistan

**Lab Manual 07**

# Objective:

* Observing the structure and working of **TCP**, **UDP** and **ICMP** Protocols in Wireshark.

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

* **Step 1:** Run Wireshark.
* **Step 2:** Load the trace file **tcp-ethereal-trace-1**
* **Step 3:** Now filter out all TCP packets by typing “tcp” (without quotes) in the filter field towards the top of the Wireshark window. You should see a series of TCP and HTTP messages between the host in MIT and gaia.cs.umass.edu. The first three packets of the trace consist of the initial *three-way handshake* containing the SYN, SYN ACK and ACK messages. You should see a series of “TCP Segment of Reassembled PDU” messages being sent from the host in MIT to gaia.cs.umass.edu. Recall from the previous lab that there is no such thing as an HTTP Continuation message – this is Wireshark’s way of indicating that there are multiple segments being used to carry a single HTTP message. You should also see TCP ACK segments being returned from gaia.cs.umass.edu to the host in MIT.

**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**: IP address: 192.168.1.102

TCP port number: 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**: IP address: 128.119.245.12

TCP port number: 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**: Seq No: 0

Flag SYN is set that identifies the segment 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?

**Ans**: Seq No: 0

Ack: 1

Flag SYN and Acknowledgement is set that identifies the segment as a SYN ACK segment.

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

**Ans**: Data segment up to 2026 has been received.

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

**Ans**: Data segment up to 7866 has been received.

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

**Ans**:

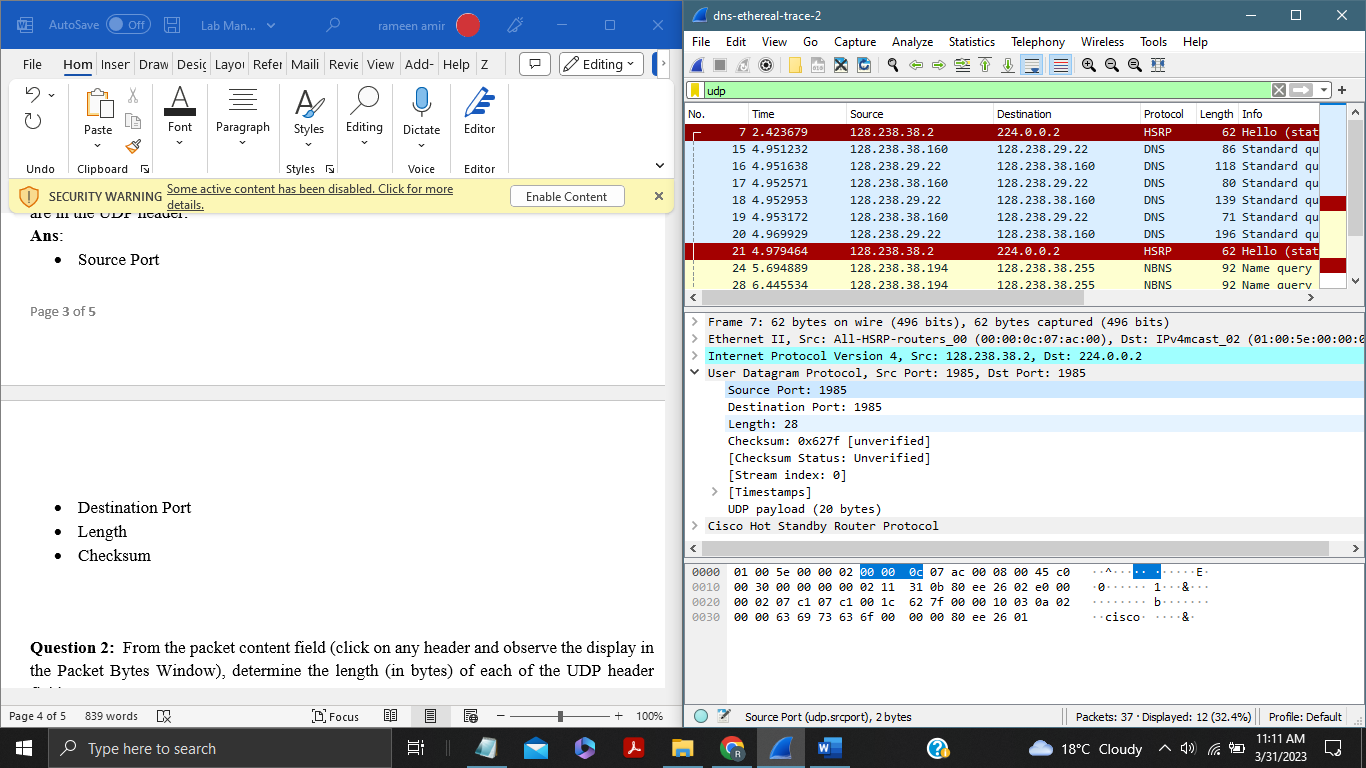
**Lab Statement 2: Analyzing UDP Packets using Wireshark (5)**

* **Step 1:** Run Wireshark
* **Step 2:** Load the trace file **dns-ethereal-trace-2.**
* **Step 3:** Now filter out all non-UDP packets by typing “udp” (without quotes) in the filter field towards the top of the Wireshark window.
* **Step 4:** Analyze the UDP Packets and answer the following questions.

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

**Ans**:

* Source Port
* Destination Port
* Length
* 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: The UDP header has a fixed length of 8 bytes. So each field is of 2 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 specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the UDP segments may differ from each other.

The length of UDP payload for selected packet is 58. 58-8 = 40 bytes.

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

Ans: DNS uses port 53.

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

* **Step 1:** Run Wireshark
* **Step 2:** Load the Session file **ICMP\_Session**
* **Step 3:** Now filter out all non-ICMP packets by typing “icmp” (without quotes) in the filter field towards the top of the Wireshark window
* **Step 4:** Analyze the ICMP Packets and answer the following questions

|  |  |
| --- | --- |
| 1. Are ICMP messages sent over UDP or TCP? | TCP |
| 1. What is the link-layer (e.g., Ethernet) address of the host? | Address: IntelCor\_55:7b:ac (60:67:20:55:7b:ac) |
| 1. Which kind of request is sent through these ICMP packets? | PING echo request |
| 1. How many requests are sent through the host? | 4 |
| 1. What is the IP address of your host? What is the IP address of the destination host? | Source Address: 192.168.33.110 Destination Address: 172.217.27.36 |
| 1. Why is it that an ICMP packet does not have source and destination port numbers? | Because it is designed to communicate network layer information between hosts and routers not between application. |
| 1. What values in the ICMP request message differentiate this message from the ICMP reply message? |  |
| 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? |  |
| 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? |  |
| 1. 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? |  |