ICT_103 Individual Assessment

Name : Drishti Durgesh Telgu
Student Id : SM20240093
Unit : ICT_103
Professor : Dr. Linh Hoang

Executive Summary :

This report provides an in-depth analysis of network traffic captured using Wireshark during a connection to a website which is x=3: https://web.mit.edu/**.** The major network processes and protocols are examined to try to explain how network communication really works. To this end, the report is intended to realize the inner mechanics of network communication and showcase Wireshark as a tool in the capturing and analysis of network traffic. It further closely examines some of the very interesting aspects of network communication, such as the TCP 3-way handshake process, before actually delving deep into analysis across application, transport, and internet layers for network packets.

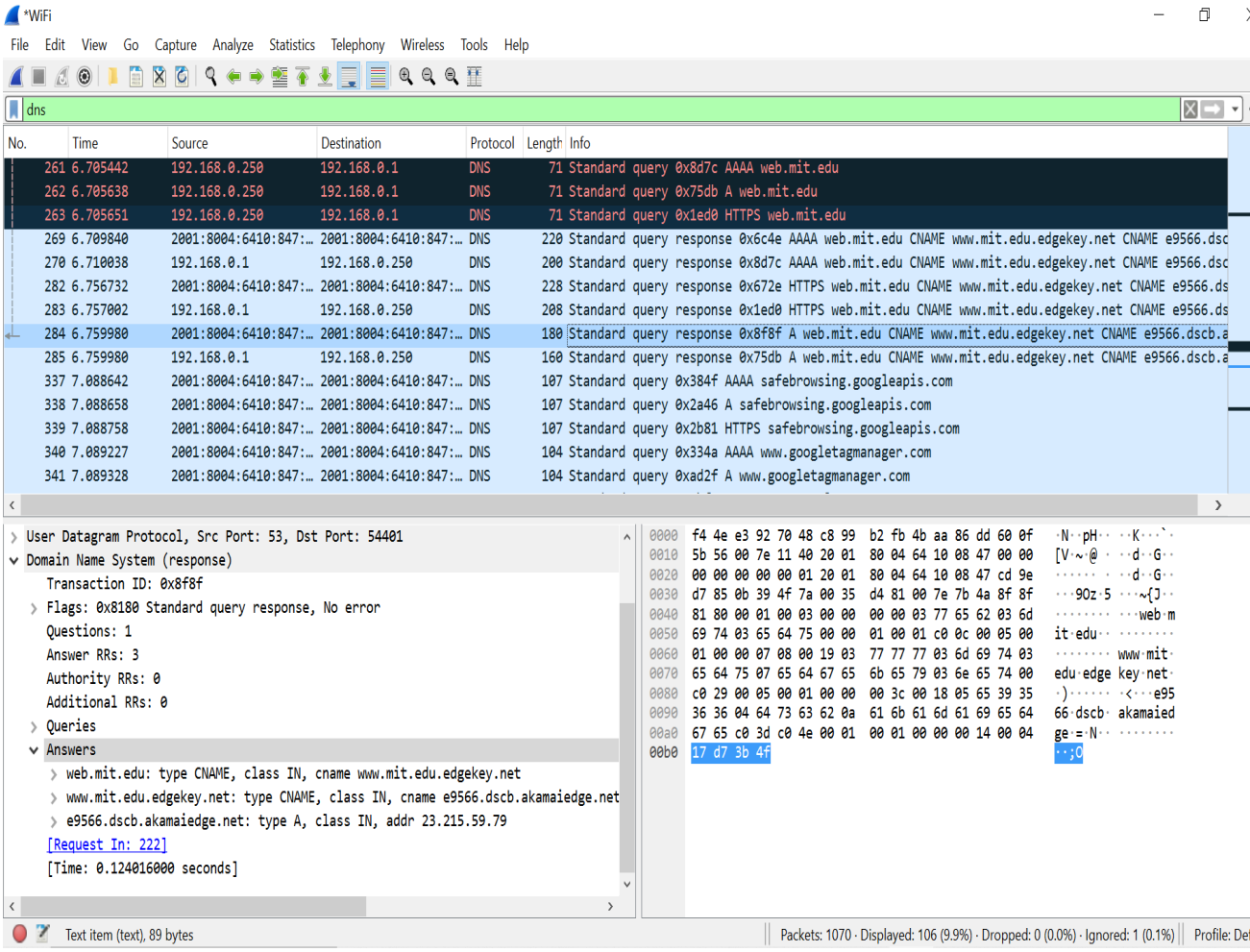
Introduction :

This report provides an advanced analysis of the network traffic captured through Wireshark, centered on a connection to some website based on x = 3 https://web.mit.edu/, determined by the last digit of the student ID. The main goals are to dissect the TCP 3-way handshake process in detail, which is key in setting up reliable client-server connections. The report looks into the intricacies of packet structures through the application, transport, and Internet layers of the TCP/IP model. It then tries to create an in-depth analysis of the packet headers and network interactions by using Wireshark—one of the premier network protocol analyzers available today. That analysis will not only point out the heart of the operations of communicating over a network but will also be an example of the practical application of Wireshark in troubleshooting and benchmarking network performance. Beyond that, the report considers the structure and function of network packets at different levels of the TCP/IP model: the application, transport, and Internet layers.

Demonstration of the tasks :

2.1. Make a connection to a website and capture the traffic using Wireshark Based on the last number of your student ID (=x), make a connection to the following website:

• x=3: https://web.mit.edu/



Explanation : I successfully captured the network traffic to access the MIT website. This includes the DNS resolution process, the 3-way TCP handshake, and the actual data transfer of the web page.

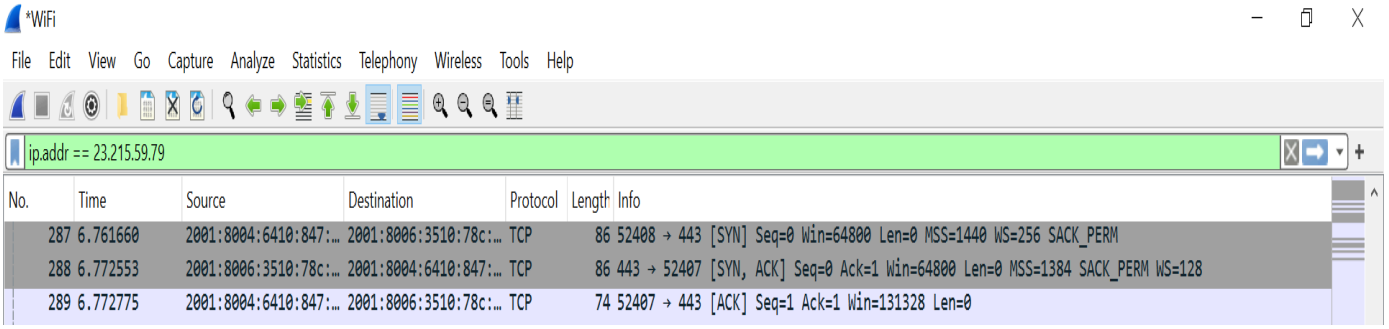
These captured packets detail what your computer is discussing with the server: establishing a connection, requesting resources, and how it gets the responses. All this information enables one to understand in detail how the network protocols work and how they interact with one another—something important in any network security and analysis-related tasks.

2.2. Analyse the 3-ways handshake process Identify and describe the 3-way handshake using the following guiding questions:

• Locate the SYN, SYN-ACK, and ACK packets that constitute the 3-way handshake between your computer and the server in Task 2.1

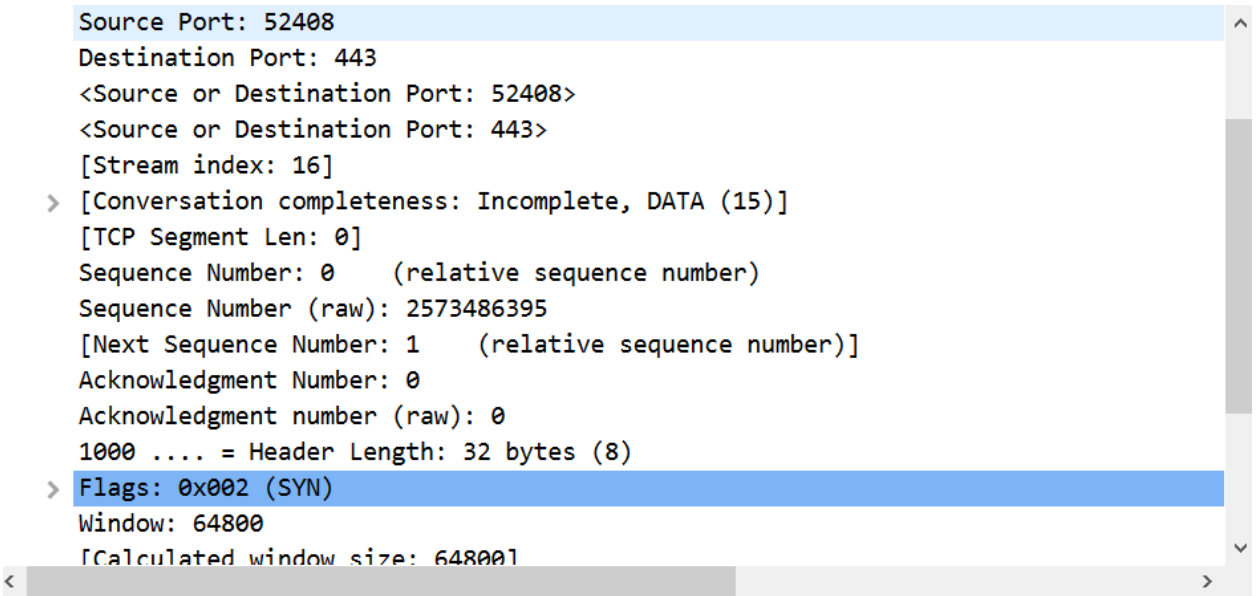
• Take screenshots of the SYN, SYN-ACK, and ACK packets.

• Describe the sequence and acknowledgment numbers in each step of the handshake, explaining how they ensure a reliable connection.

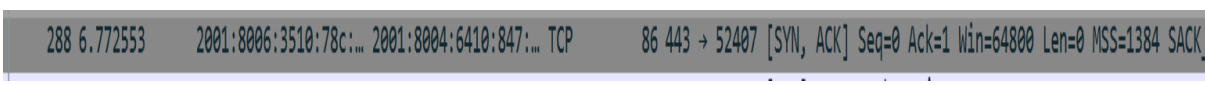


a. For ,

Sequence and acknowledgement numbers are :



b. For,



Sequence and acknowledgement numbers are :

```
<Source or Destination Port: 443>
<Source or Destination Port: 52407>
[Stream index: 15]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 822197708
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 1447856951
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
Window: 64800
[Calculated window size: 64800]
Checksum: 0xc531 [unverified]
[Checksum Status: Unverified]
```

c. For,

```
289 6.772775    2001:8004:6410:847:… 2001:8006:3510:78c:… TCP    74 52407 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

Sequence and acknowledgement numbers are :

```
<Source or Destination Port: 52407>
<Source or Destination Port: 443>
[Stream index: 15]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 1447856951
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 822197709
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x0e51 [unverified]
```

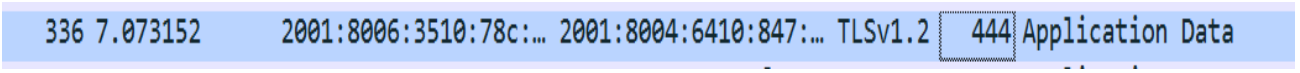
Explanation : I used Wireshark to capture and analyze the process of a 3-way handshake between my computer and the MIT server. By viewing the SYN, SYN-ACK, and ACK packets, I was able to see clearly the sequence and acknowledgment numbers, showing how TCP makes a connection that is reliable and synchronized. The attached screenshots

of the assignment are visual proof of each step in the 3-way handshake and therefore prove its completion.

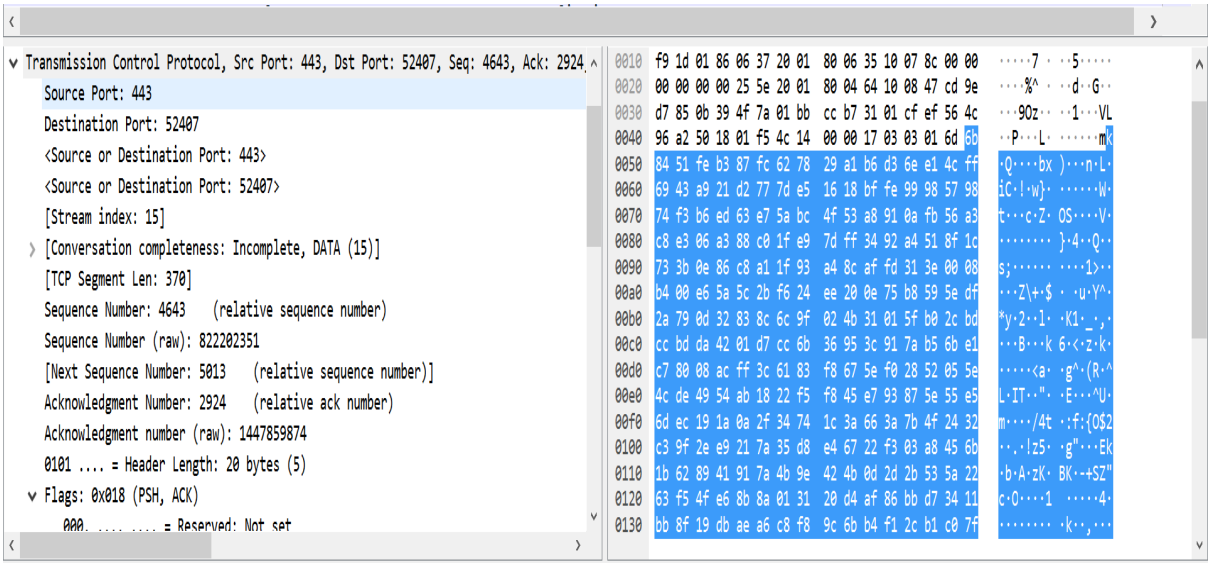
2.3. Analyse the application layer Analyse the application layer header using the following guiding questions:

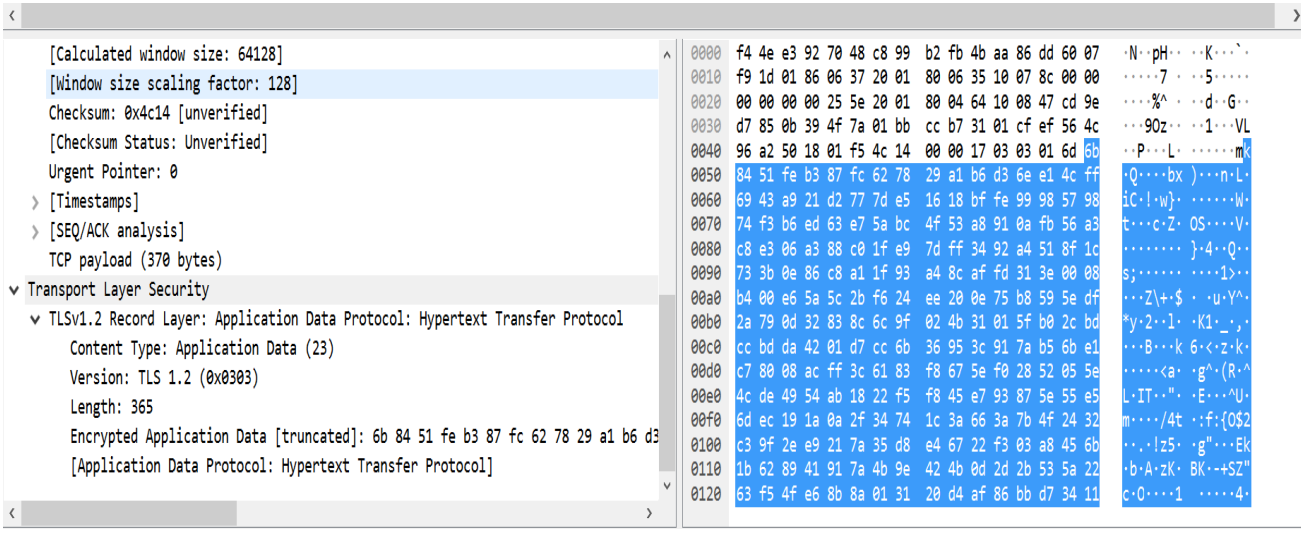
• Analyse the application layer header (e.g., TLS1.2/TLS1.3) of the selected packet, including key fields and their significance (e.g., source and destination ports, sequence and acknowledgment numbers, flags).

• Take screenshots of the application layer header details.



Significance :



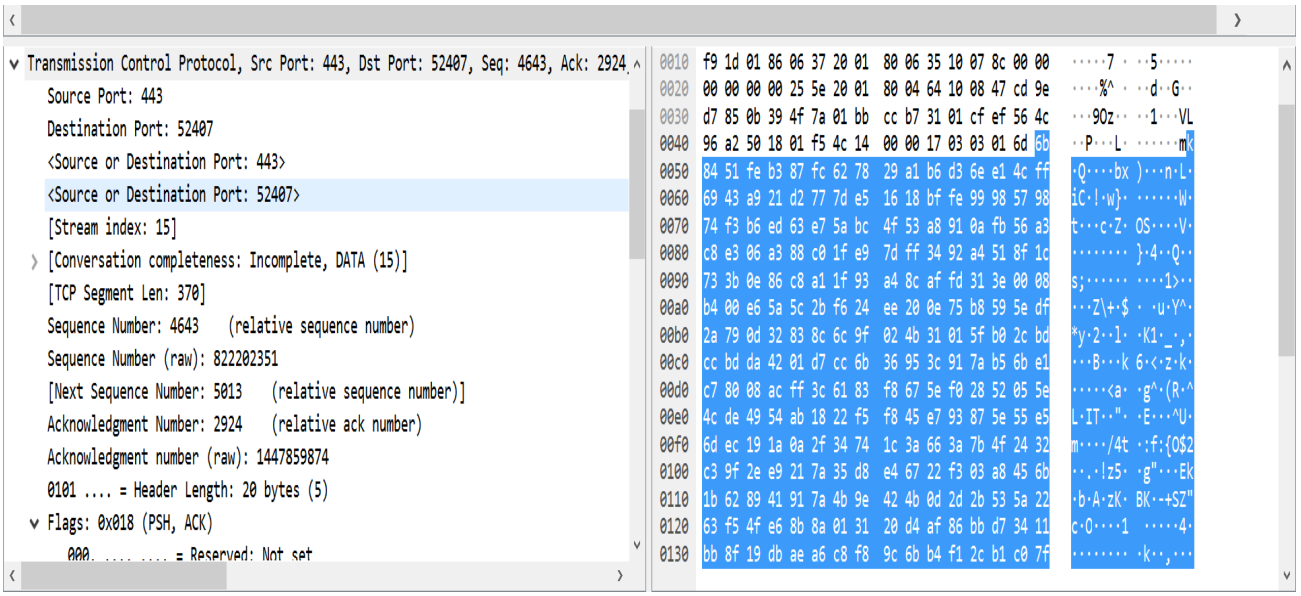


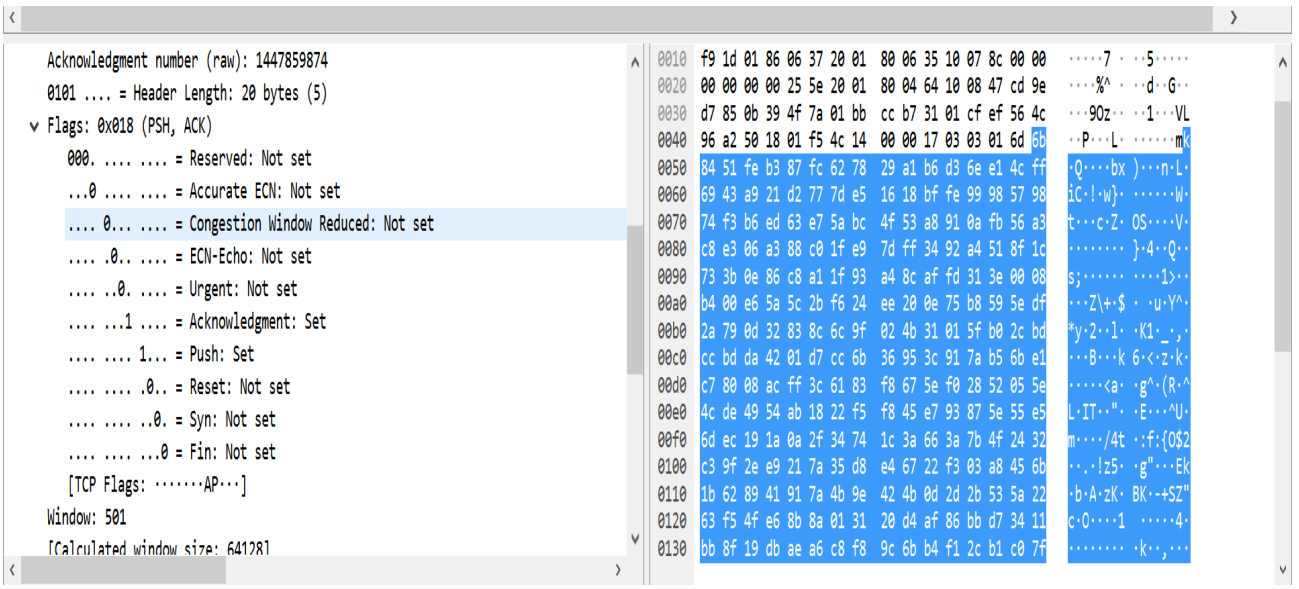
Explanation : I examined the application layer header of the chosen packet for key fields, including TLS1.2/TLS1.3, source and destination ports, sequence and acknowledgment numbers, and flags. The importance of these fields toward secure and reliable communication was truly realized. Attached screenshots in the assignment capture details of the Application Layer Header view and are pictorial evidence that the analysis is done.

2.4. Analyse the transport layer Examine and describe the transport layer header using the following guiding questions:

- **Analyse the transport layer header (e.g., TCP/UDP) of the selected packet, including key fields and their significance (e.g., source and destination ports, sequence and acknowledgment numbers, flags).**
- **Take a screenshot of the transport layer header details.**

Significance :





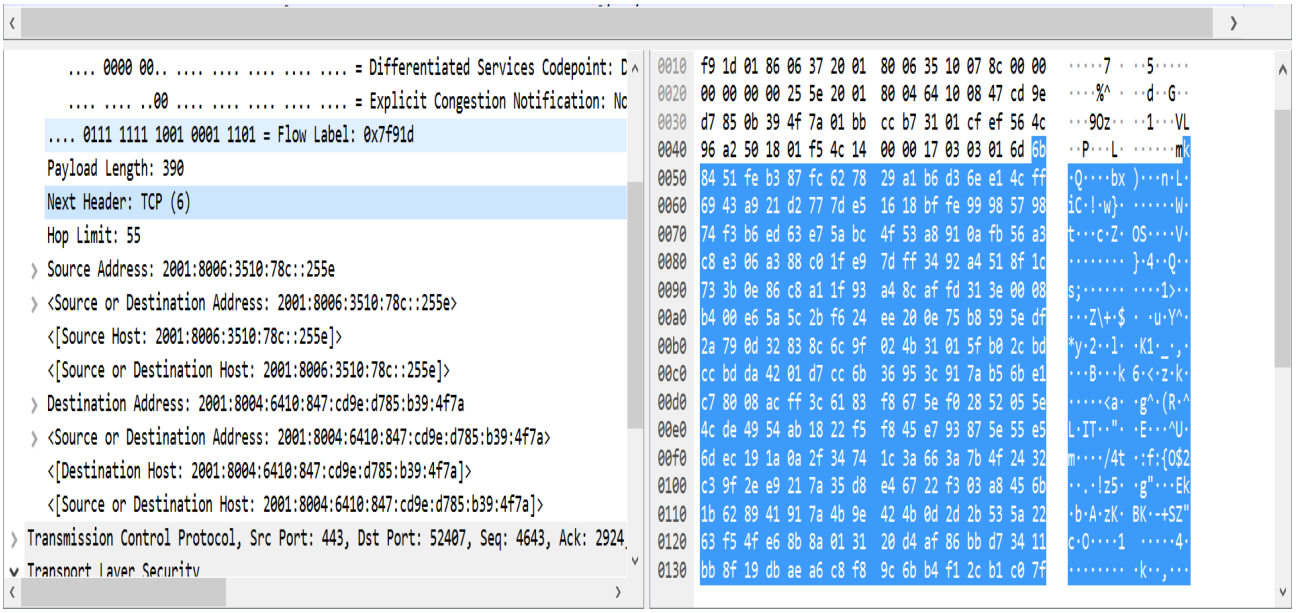
Explanation : I examined and described the transport layer header of the selected packet, focusing on key fields like TCP/UDP, source and destination ports, sequence and acknowledgement numbers, and flags. In the process, I unraveled their necessity to reliable and efficient data transfer. Provided below are screenshots of details in the Transport Layer Header as visual proof of a done analysis.

2.5. Analyse the internet layer Examine and describe the internet layer header:

• Analyse the internet layer header (IP header) of the selected packet, including key fields and their significance (e.g., source and destination IP addresses, TTL, protocol).

• Take a screenshot of the IP header details.

Significance :



Explanation :I have done the analysis of the Internet layer header, outlining important fields such as source and destination IP addresses, TTL, and protocol. A screenshot of IP header details has been provided to support this analysis. While considering the Internet Layer header of the selected packet for analysis, key fields—Source and Destination IP Addresses, Time To Live (TTL), Protocol—have been looked at. These fields are important for determining the source, destination, lifetime, and the type of information the packet is carrying. The source and destination IP addresses identify the sender and receiver respectively, TTL prevents packets from circulating in the network forever, and the protocol field identifies the higher-layer protocol used. A screenshot of the IP header details has been provided for illustration purposes.

Conclusion :

Through the tasks outlined in this assignment, we have successfully captured and analyzed the essential aspects of network communication, specifically focusing on the TCP 3-way handshake, application layer, transport layer, and internet layer.The 3-way handshake mechanism of TCP establishes a reliable connection between the client and server, ensuring that both parties are ready to communicate and that any loss or misordering of packets can be detected and corrected.

The detailed analysis of the application, transport, and internet layers illustrates the layered architecture of network communication, where each layer performs specific functions and interacts with the layers above and below it to provide seamless data transmission.This assignment provided hands-on experience with Wireshark, a crucial tool for network analysis, enhancing our ability to diagnose network issues and understand the underlying protocols that facilitate communication over the internet.

In conclusion, the tasks completed in this assignment have equipped us with a deeper understanding of network protocols and their interactions, enhancing our ability to analyze and troubleshoot network communication effectively.

Reference :

Dr. Linh Hoang (2024). ICT103 - Computer Security and Network Fundamentals.‘Regarding Assessment 2 and Assessment 3’. Available in https://sydneymet-my.sharepoint.com/:v:/g/personal/linh_hoang_sydneymet_edu_au/EZua9pPCjC1NniBfuNpHs0IBvupAtGKMDlwKaNH0Cnp_FA?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D&e=rZSfdT . (Accessed July 4, 11:03 am).