Portfolio-1

Nivethitha Muthuraman

8830593

INFO8491-Network Security – 1

Table of Contents

[Lab 1 - Simple Network Topology 3](#_Toc167902763)

[Description: 3](#_Toc167902764)

[Part 1- Building the Topology 3](#_Toc167902765)

[Preparation: 3](#_Toc167902766)

[Observation: 4](#_Toc167902767)

[Screenshot: 4](#_Toc167902768)

[Part 2 – Configuring the Topology 4](#_Toc167902769)

[Part 3 – Configuring the Privileged Mode Password 5](#_Toc167902770)

[Part 4 – Enforcing login 7](#_Toc167902771)

[Reflection: 9](#_Toc167902772)

[**Session - II** 10](#_Toc167902773)

[Description 10](#_Toc167902774)

[Preparation 10](#_Toc167902775)

[Observation 10](#_Toc167902776)

[Screenshots: 11](#_Toc167902777)

[Reflection 16](#_Toc167902778)

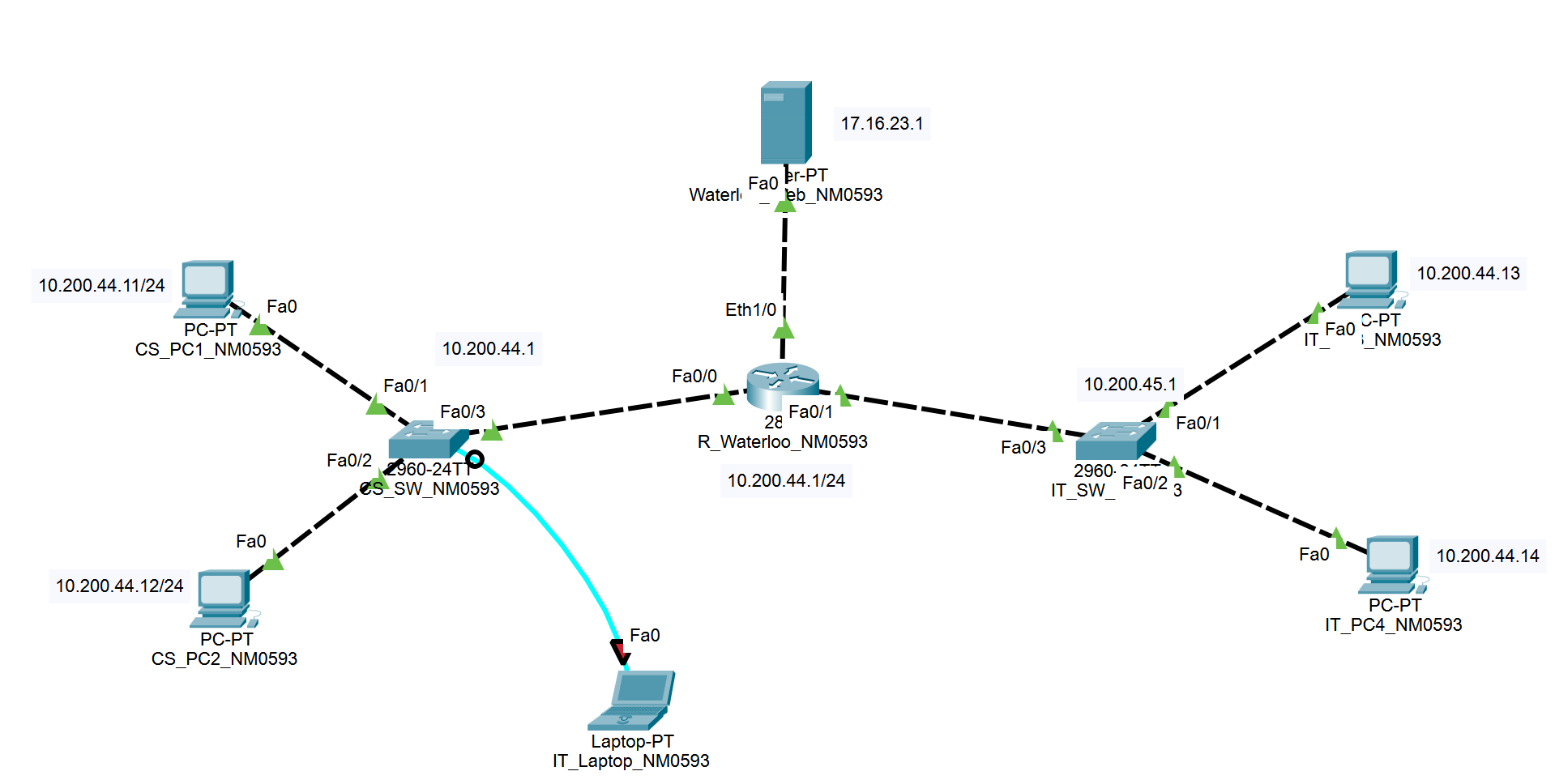
# Lab 1 - Simple Network Topology

# Description:

In our lab, we're focusing on configuring different network devices to ensure both connectivity and security. We'll set up a basic network that includes two layer 2 switches, a router, a web server, and several workstations. Our tasks involve setting passwords, configuring MOTD banners, enforcing login requirements for console and virtual terminal access, enabling SSH for remote access, and assigning IP addresses.

The main goal is establishing a secure and functional network that allows secure remote access via SSH and smooth communication between all devices. This hands-on exercise will give us practical experience setting up devices and implementing security measures. We'll aim to complete several key outcomes: screenshots of our configurations, successful ping tests to confirm connectivity, verified access to the web server, and establishing SSH connections between devices as required.

## Part 1- Building the Topology



# Preparation:

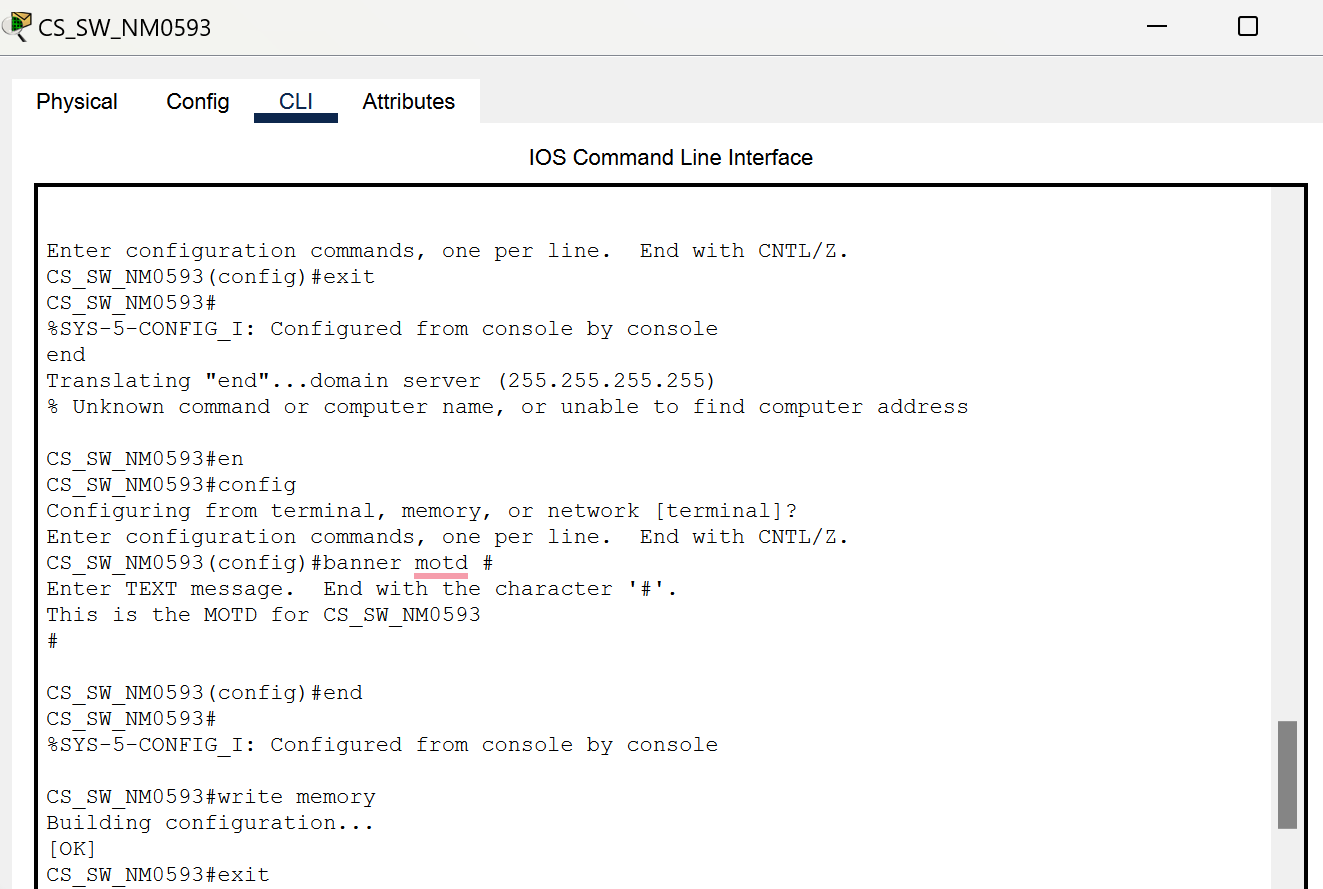
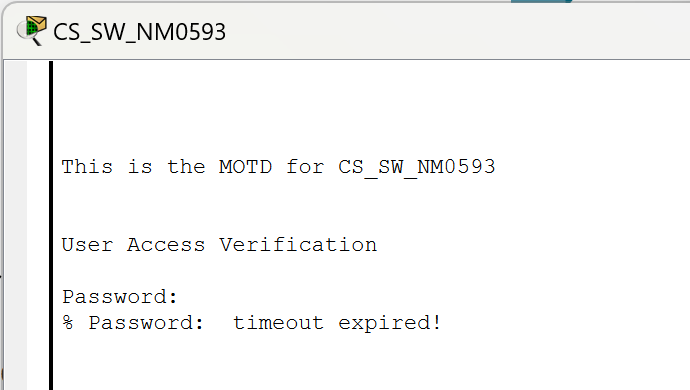
I got all the necessary hardware and software resources, including the latest version of Packet Tracer, to effectively set up the network as required for the lab. I also gathered the virtual and physical equipment specified and ensured I had the correct IP addresses for each component based on the file “INFO8490-20F-Portfolio-1-Subnets.” By thoroughly reviewing the lab instructions, I ensured I understood the tasks and objectives and was well-prepared to create and configure the network according to the guidelines.

# Observation:

I successfully built a network topology that included all the necessary components during this lab project. I set up Message of the Day (MOTD) banners, configured privileged mode passwords, and enforced login restrictions as instructed. I also assigned IP addresses to each device and ensured their default gateways were correctly set. One significant challenge I faced was accurately assigning IP addresses and ensuring the default gateway configurations were correct, as even small mistakes could cause connectivity issues. Despite this, I managed to resolve any issues by carefully following the instructions and cross-referencing setup examples from the Cisco website, ensuring the network had reliable connectivity.

# Screenshot:

## Part 2 – Configuring the Topology

Figure 1.1-Displaying MOTD for CS\_SW\_NM0593

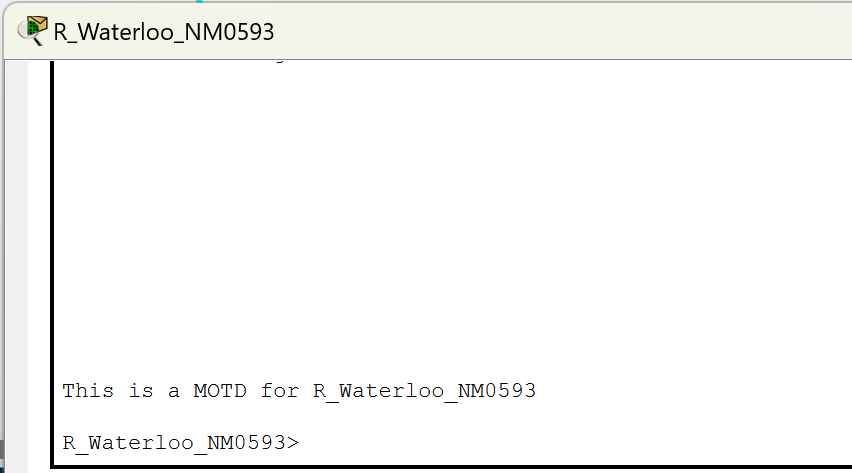


Figure 1.2-Displaying MOTD for R\_Waterloo\_NM0593

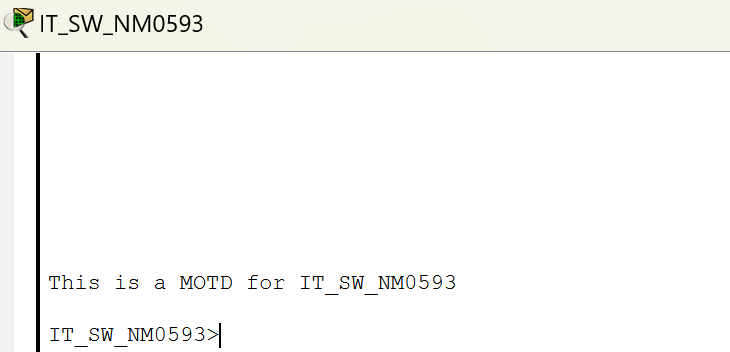


Figure 1.3-Displaying MOTD for IT\_SW\_NM0593

## Part 3 – Configuring the Privileged Mode Password

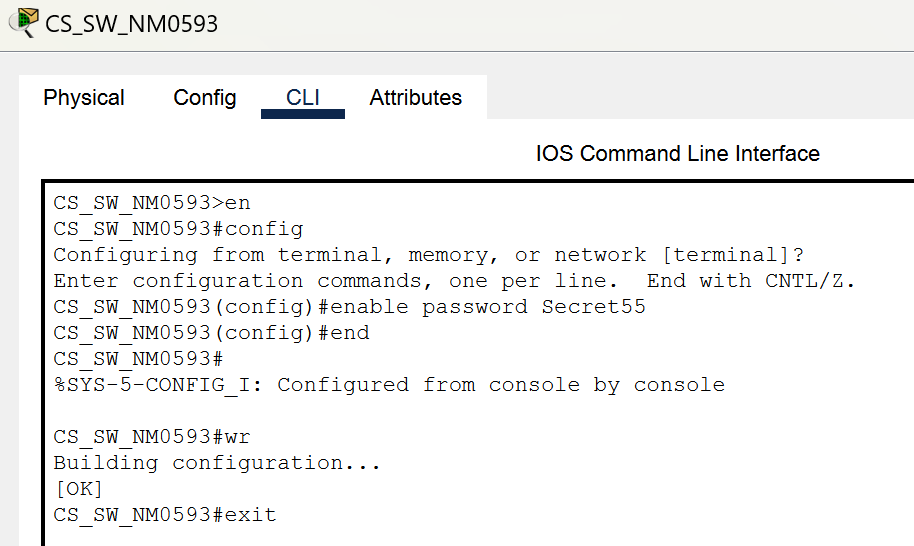


Figure 1.4- Showing privileged password mode for CS\_SW\_NM0593

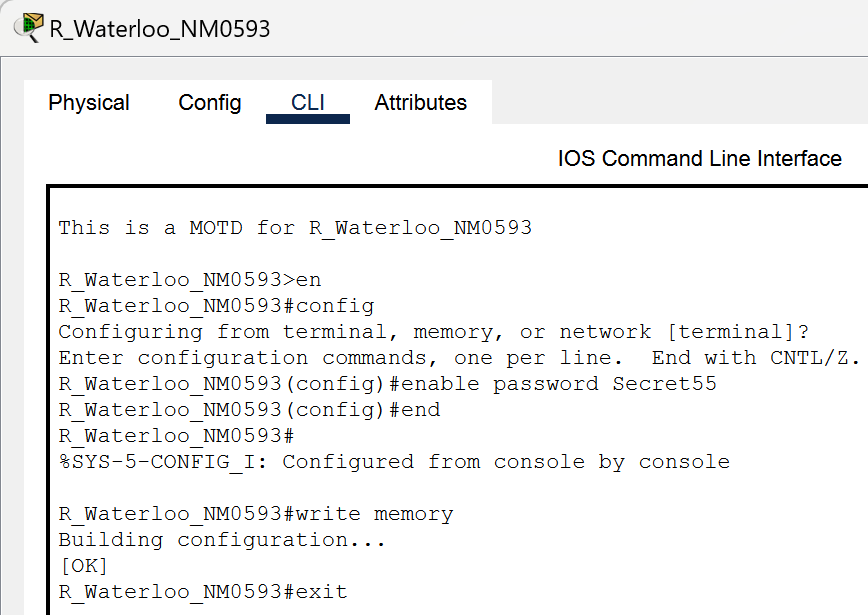
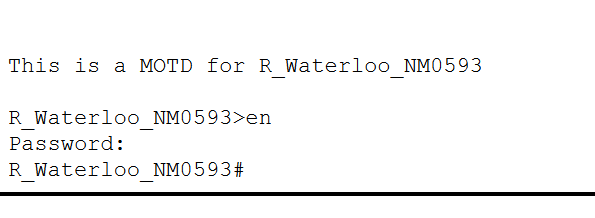
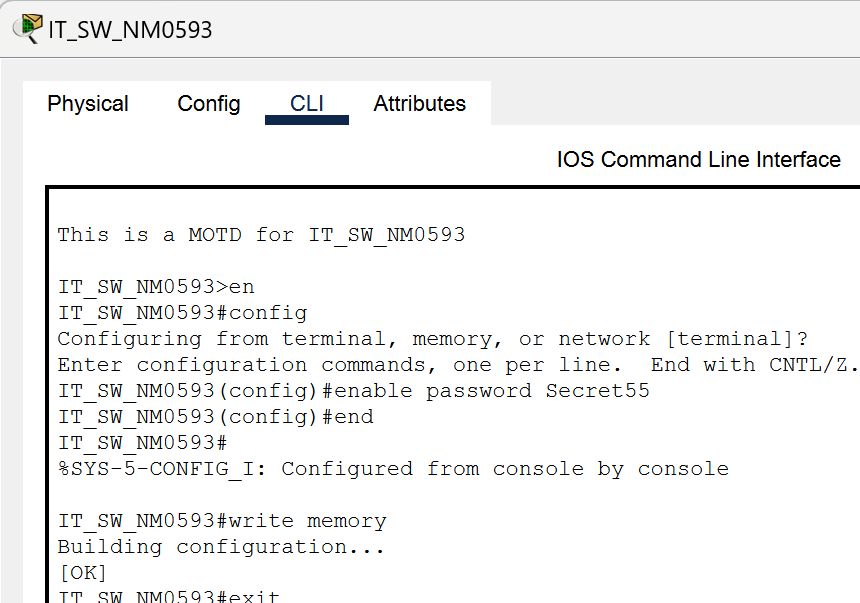
 

Figure 1.5 - Showing privileged password mode for R\_Waterloo\_NM0593



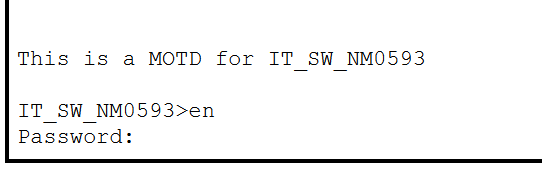


Figure 1.6 - Showing privileged password mode for IT\_SW\_NM0593

## Part 4 – Enforcing login

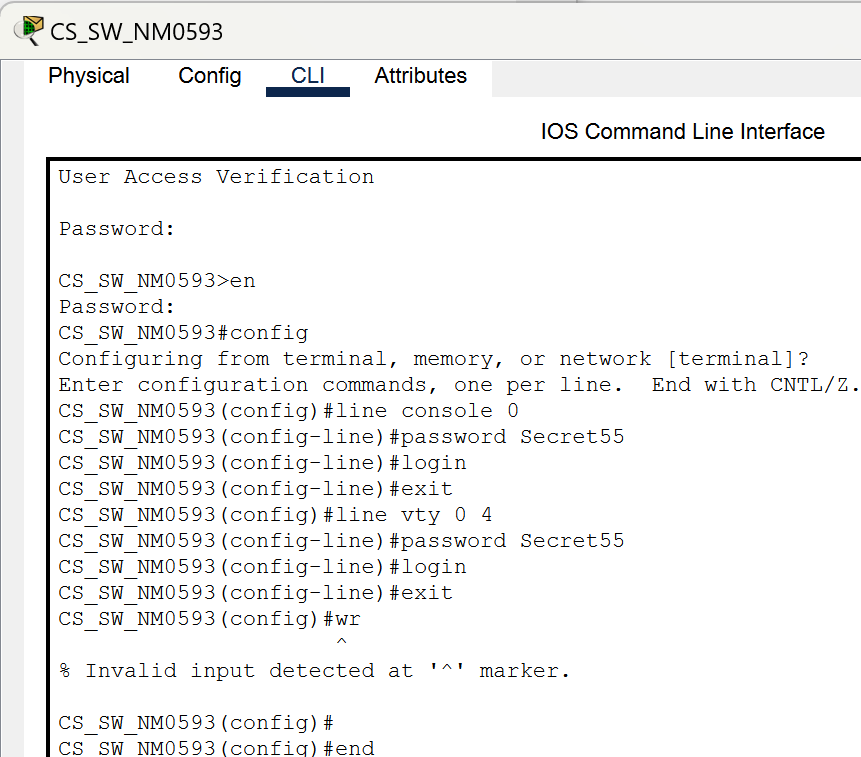
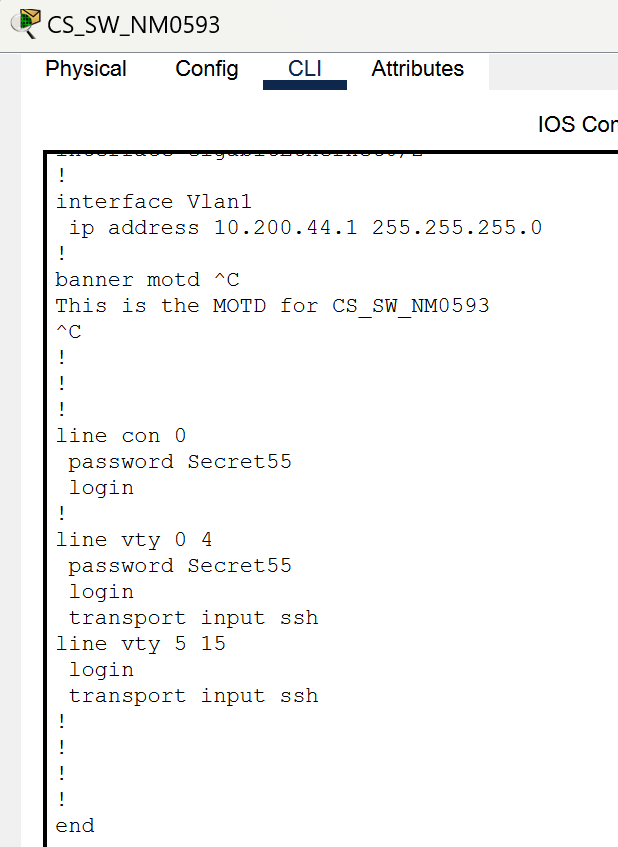
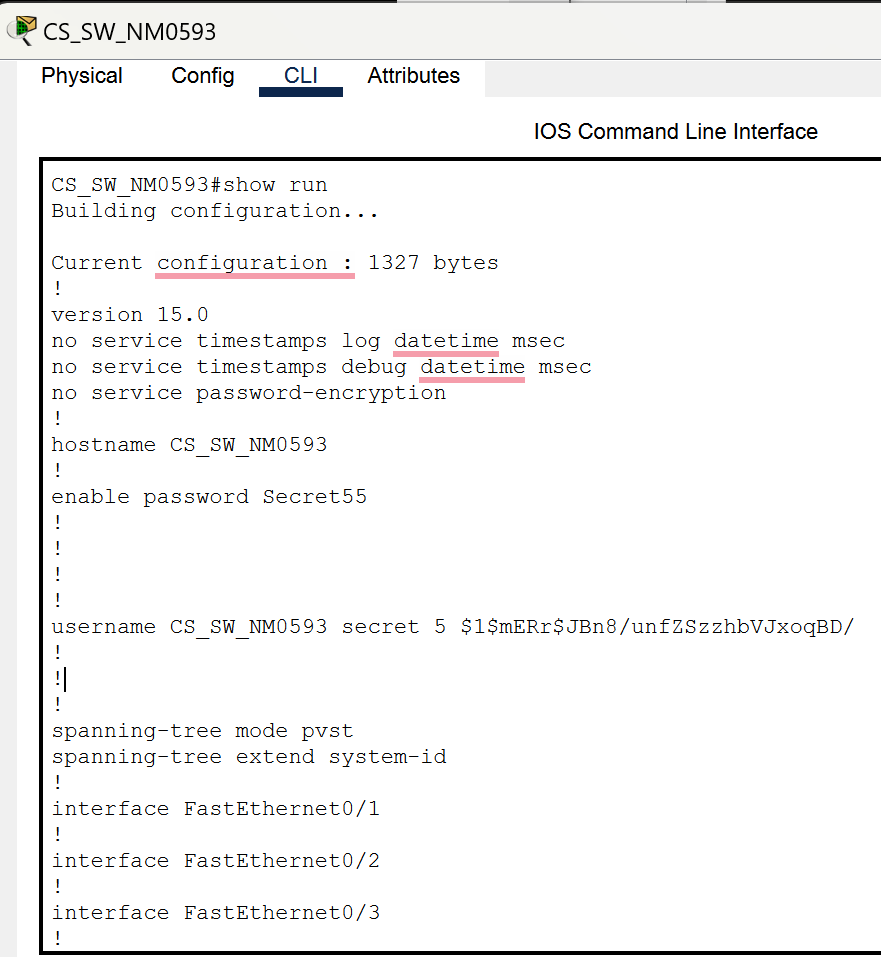
 

Figure 1.7 – Showing encryption password of line console and vty for CS\_SW\_NM0593

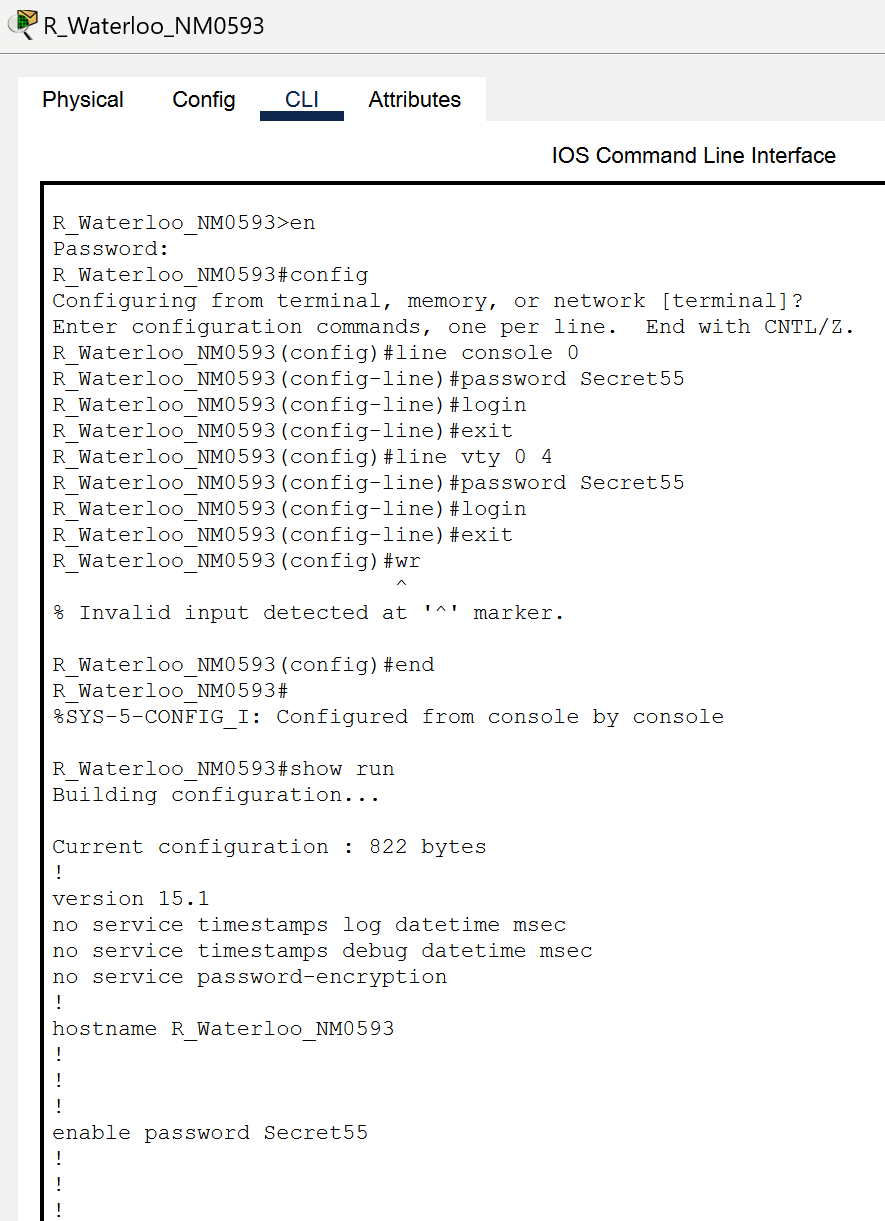
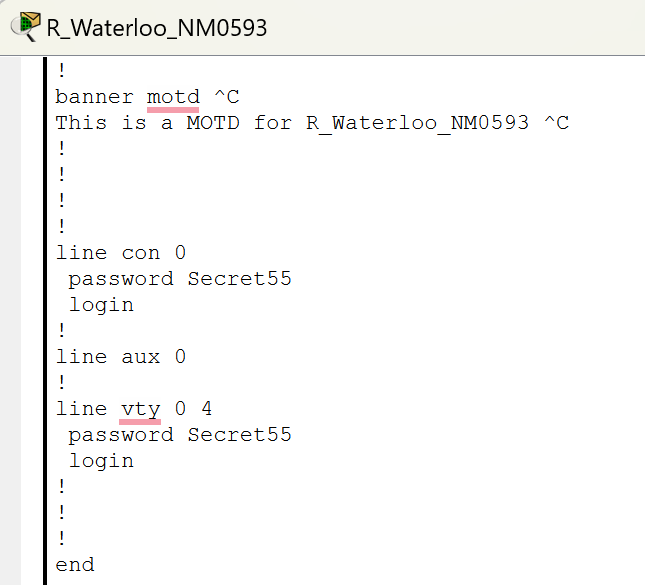


Figure 1.7 – Showing encryption password of line console and vty for R\_Waterloo\_NM0593

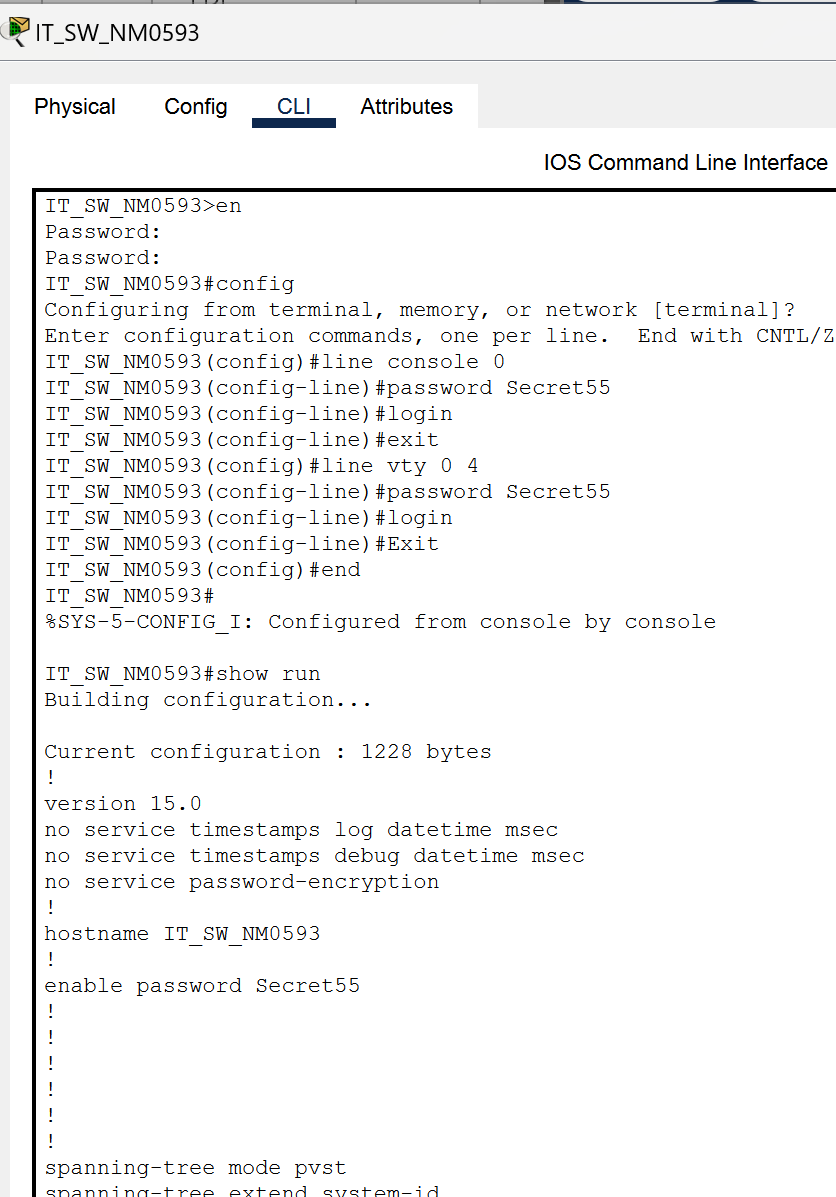
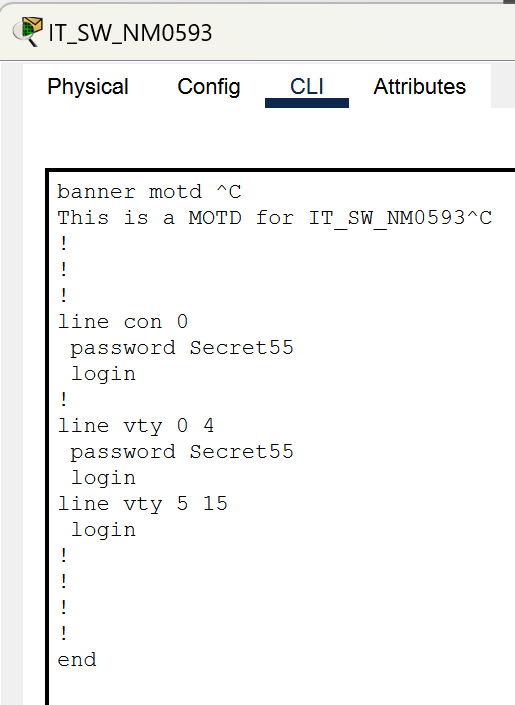


Figure 1.7 – Showing encryption password of line console and vty for IT\_SW\_NM0593

# Reflection:

This network setup project taught me a lot about building and securing network topologies. It showed me how important it is to be well-prepared and detail-oriented when configuring network devices. One of the main challenges I faced was correctly assigning IP addresses, subnets, and default gateways. To tackle this, I carefully reviewed the assignment sheet and used resources like the Cisco website to ensure my IP assignments were accurate. This project highlighted the importance of getting IP address allocation right and how even small mistakes can mess up network connectivity. It improved my practical skills in setting up network devices and reinforced the importance of precise IP address allocation for network setup and security.

# **Session - II**

### Description

In this assignment, we used Wireshark to capture and analyze network packets. Wireshark is a powerful tool for network troubleshooting and protocol analysis. We performed three main tasks: observing the Wireshark interface, capturing and analyzing ping packets, and triggering a DHCP renewal to capture related packets.

### Preparation

First, I installed Wireshark on my computer, ensuring it was ready for use. I identified the correct network interface for capturing packets, which, in my case, was the Wi-Fi interface with the IPv4 address 10.0.0.221. I also prepared the Command Prompt for executing network commands needed for the assignment. This setup was crucial for capturing and analyzing the necessary packets effectively.

### Observation

**Investigate Capture Window:** I started Wireshark and selected the Wi-Fi interface. After clicking the blue **Start** button to begin capturing packets, I observed the packets appearing in the capture window to familiarize myself with the layout and functionalities of Wireshark. Once I felt comfortable with the interface and had seen enough packets, I stopped the capture by clicking the red **Stop** button.

**Capture and Analyse Ping Packets:** I began a new capture session by clicking the blue **Start** button. I opened the Command Prompt and typed ping 10.0.0.1 to send ICMP packets to my default gateway. In Wireshark, I observed the ICMP packets corresponding to the ping command. After seeing several ICMP packets in Wireshark, I stopped the capture and recorded the IP addresses 10.0.0.221 (source) and 10.0.0.1 (destination). I took a screenshot of Wireshark showing the captured ICMP packets and filled out the necessary details in Table 1.

**Trigger DHCP Renew and Capture UDP Packets:** I started a new capture session and opened Command Prompt for the final part. I released my current IP address by typing ipconfig /release and then renewed it by typing ipconfig /renew. While Wireshark was capturing packets, I observed the DHCP packets in the capture window. I took a screenshot of the Command Prompt showing the results of the ipconfig /release and ipconfig /renew commands. I stopped the capture after seeing Wireshark's DHCP Discover, Offer, Request, and ACK packets. I sorted the packets by clicking the Protocol column header and located the DHCP packets. I took screenshots of the DHCP Discover and ACK packets, highlighting the relevant details. Finally, I filled out Tables 2 and 3 with the captured packet details.

## Investigate Capture Window

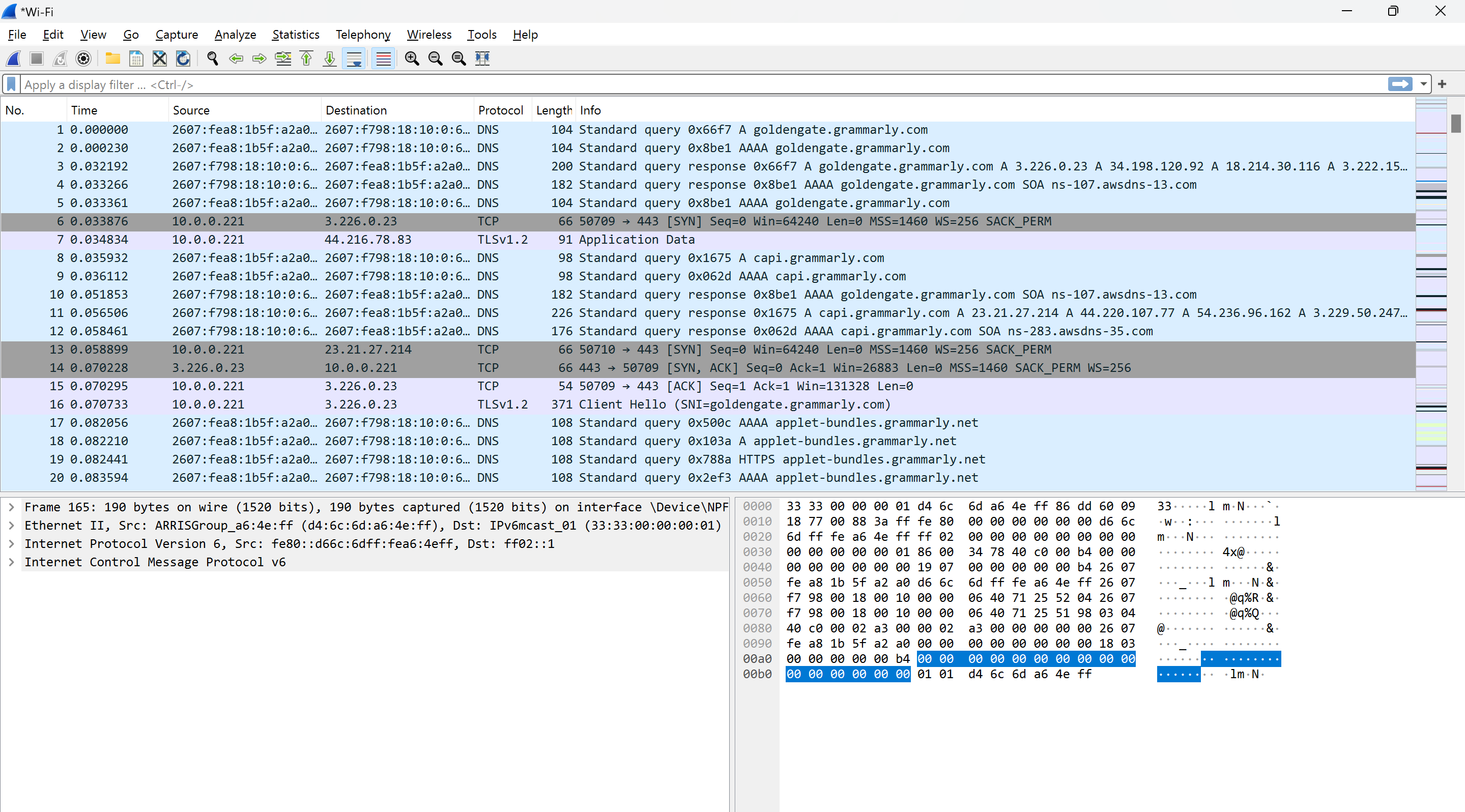


Figure 2.1- Wireshark interface after initial packet capture.

## Capture and Analyze Captured Packets

|  |  |
| --- | --- |
| Your IP address | 10.0.0.221 |
| Other IP address | 10.0.0.1 |

### Table 1: Ping Results

|  |  |  |
| --- | --- | --- |
| S.NO | Item | Value |
| 1 | Layer 2 protocol | Ethernet |
| 2 | Frame size (byte) | 74 Bytes |
| 3 | Capture time | 33.790448 Seconds |
| 4 | Layer 3 protocol | IP |
| 5 | Protocol value inside layer 3 (i.e. the value in the ‘Protocol’ column) | ICMP |
| 6 | Destination MAC address | 38:7a:0e:d1:70:22 |
| 7 | Source MAC address | d4:6c:6d:a6:4e:ff |
| 8 | Destination IP address | 10.0.0.1 |
| 9 | Source IP address | 10.0.0.221 |
| 10 | Data (see the ASCII values in the lower pane) | 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869 |

### Trigger DHCP renew and capture UDP Packets

Table 2: DHCP Request Packet

|  |  |  |
| --- | --- | --- |
| SN | Item | Value |
| 1 | Source MAC Address | 38 : 7a : 0e : d1 : 70 : 22 |
| 2 | Destination MAC Address | Boardcase (ff:ff:ff:ff:ff:ff) |
| 3 | Source IP Address | 0.0.0.0 |
| 4 | Destination IP Address | 255.255.255.255 |
| 5 | Protocol Value in IP Address | UDP |
| 6 | UDP source port | 68 |
| 7 | UDP destination port | 67 |

Table 3: DHCP ACK Packet

|  |  |  |
| --- | --- | --- |
| SN | Item | Value |
| 1 | Source MAC Address | d4:6c:6d:a6:4e:ff |
| 2 | Destination MAC Address | Boardcase (ff:ff:ff:ff:ff:ff) |
| 3 | Source IP Address | 10.0.0.1 |
| 4 | Destination IP Address | 255.255.255.255 |
| 5 | Protocol Value in IP Address | 17 (UDP) |
| 6 | UDP source port | 67 |
| 7 | UDP destination port | 68 |

## Screenshots:

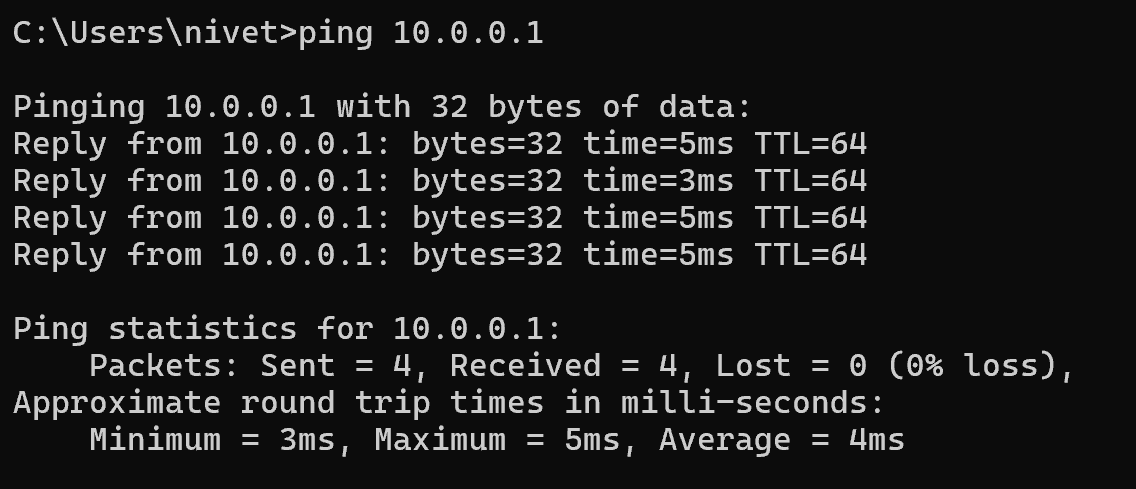


Figure 2.2 - Command Prompt showing ping command results.

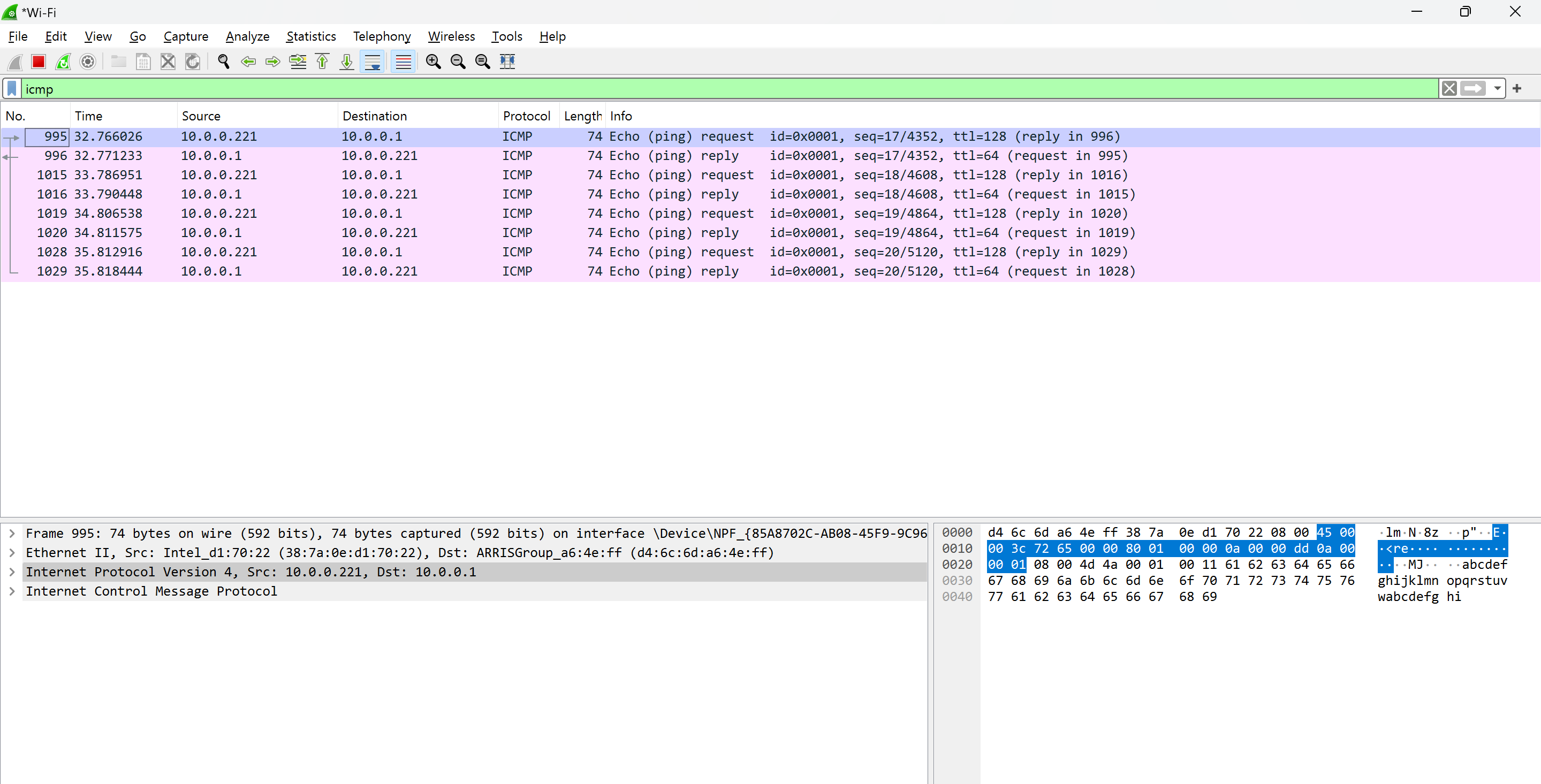
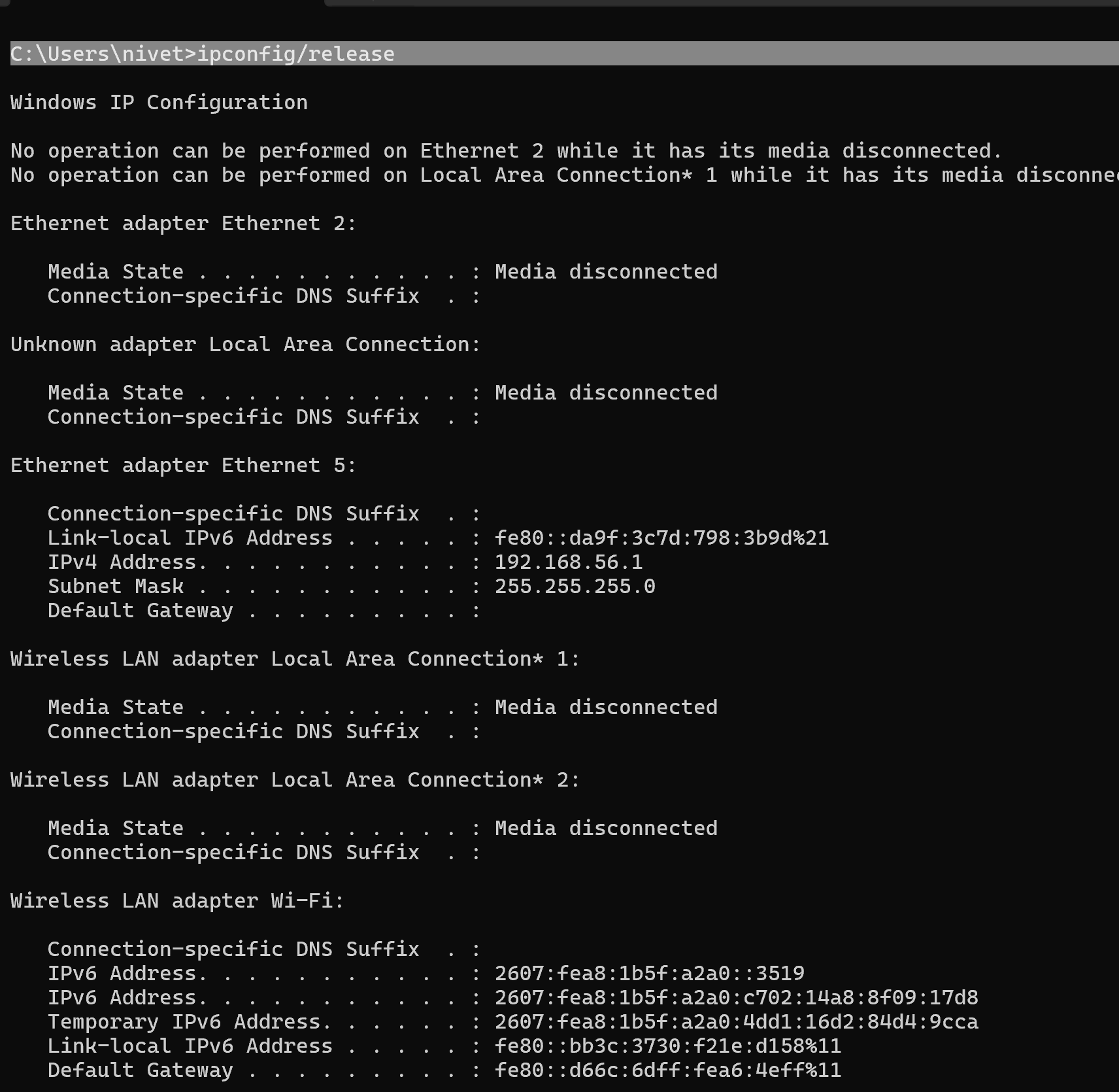


Figure 2.3 - Wireshark captures ICMP packets from the ping command.



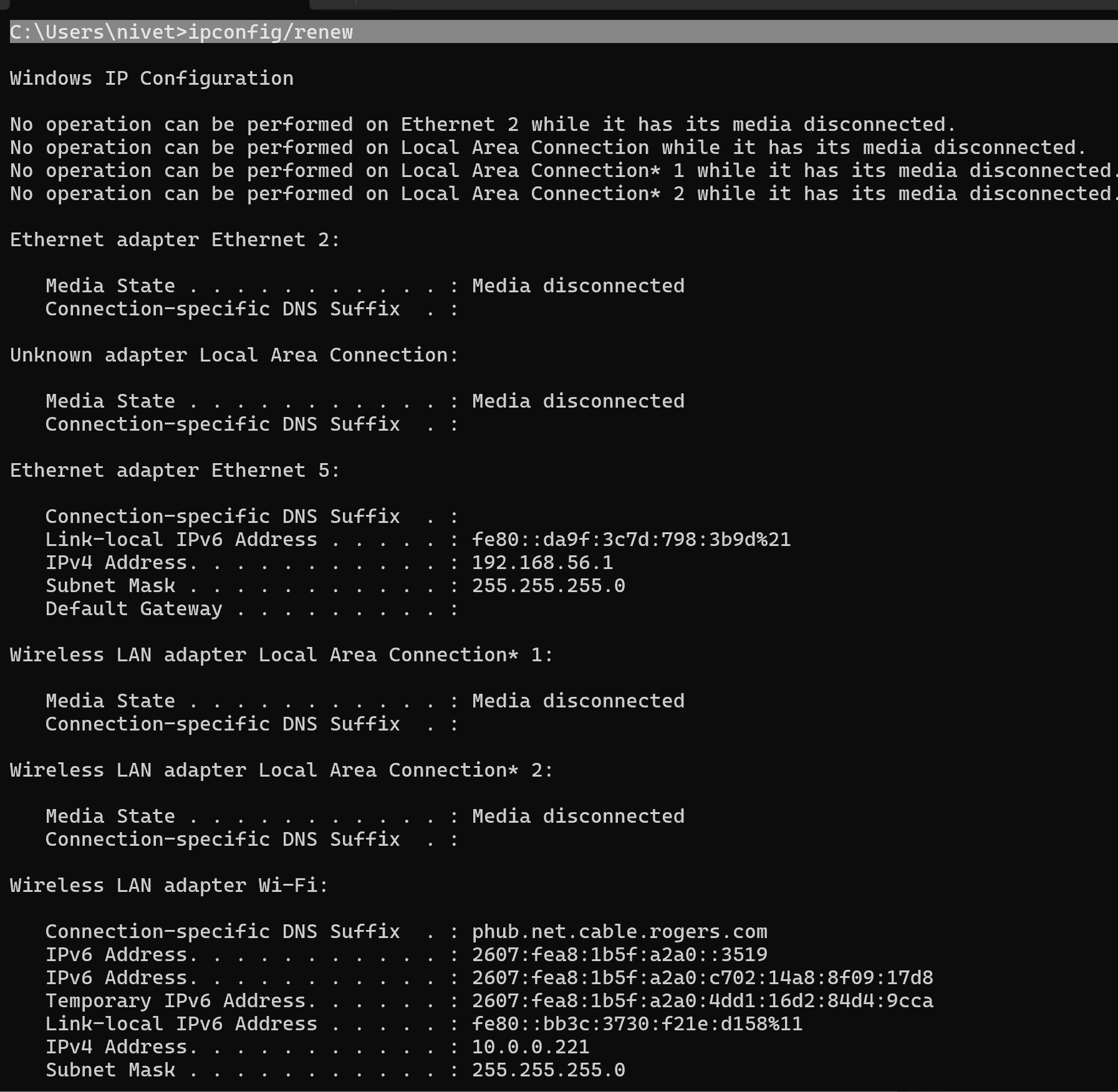


Figure 2.4 - Command Prompt showing ipconfig /release and ipconfig /renew results.

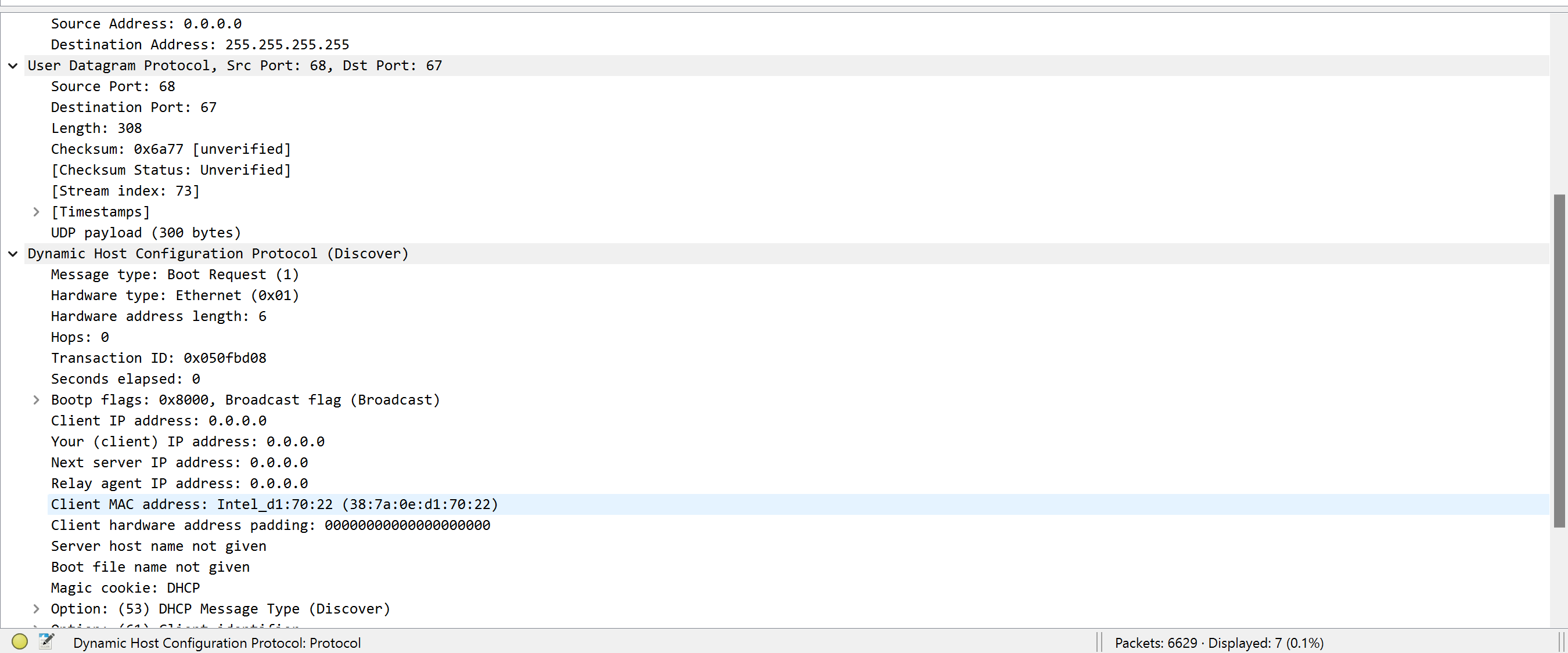
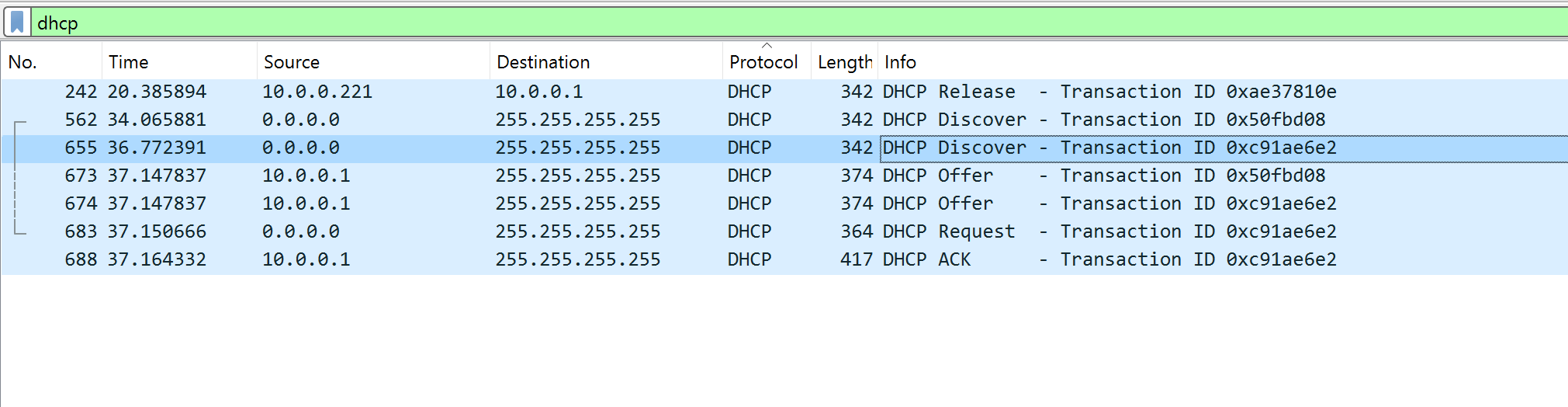


Figure 2.5 - Wireshark highlighting the DHCP Discover packet.

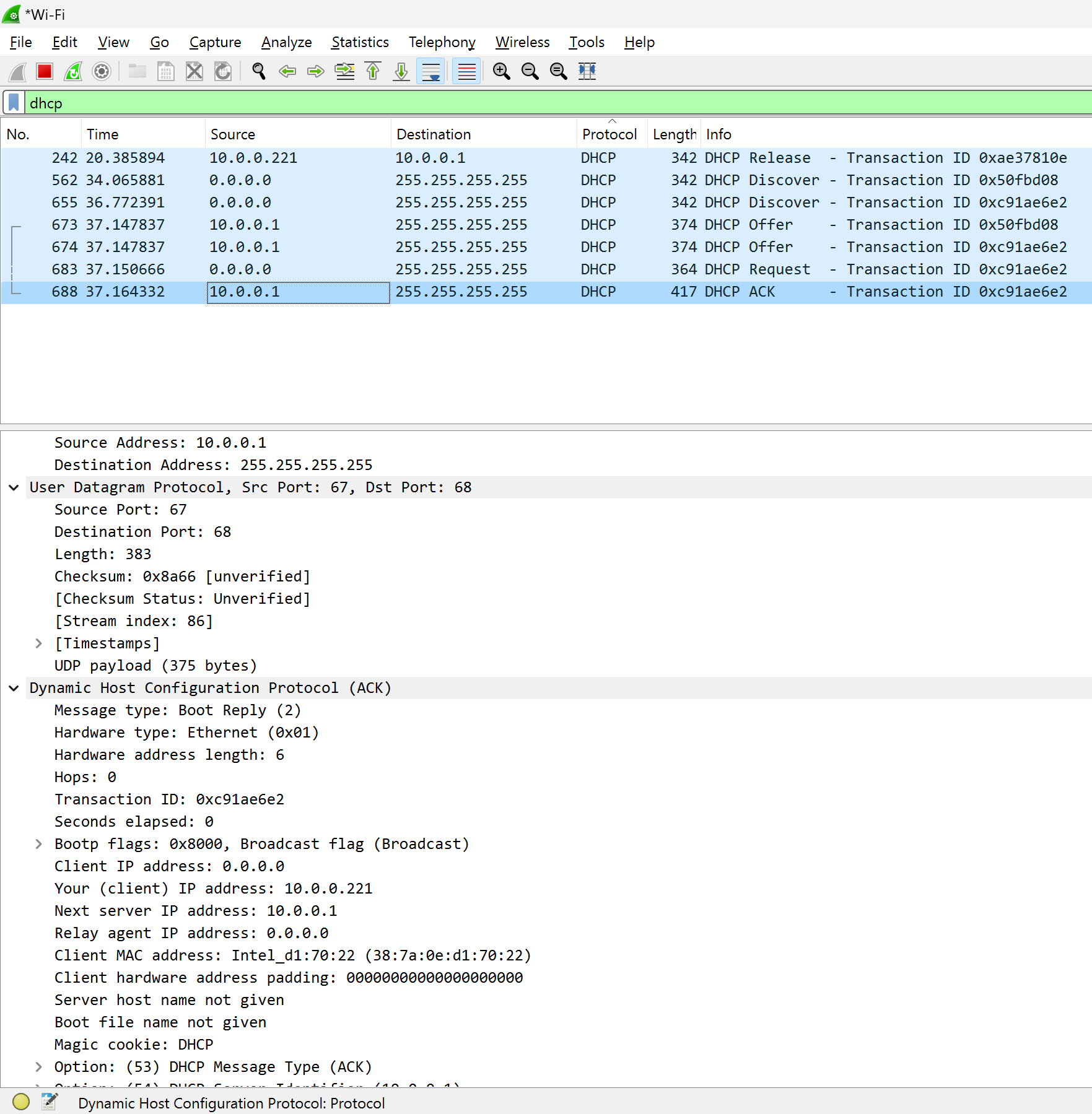


Figure 2.6 - Wireshark highlighting the DHCP ACK packet.

### Reflection

Through this assignment, I gained hands-on experience with Wireshark, learning how to capture and analyze network packets. Observing the ICMP packets from the ping command helped me understand the structure and flow of network traffic. The DHCP renew process highlighted how DHCP packets facilitate IP address allocation. These exercises reinforced my understanding of network protocols and the importance of packet analysis in network troubleshooting.

# Report Submission

### Submission Check List

|  |  |  |
| --- | --- | --- |
| S.NO | TO DO | DONE |
| 1 | Respond to all outputs and answer the questions | ✔️ |
| 2 | Give appropriate title or captions (small description) to all the output screenshots | ✔️ |
| 3 | Rename this file according to your work. Example name: Name-A1.docx | ✔️ |
| 4 | Submit the Assignment report in eConestoga dropbox before 11:30 PM on Wed May 29 Late submission will not be accepted | ✔️ |
| 5 | Include a cover page including your name, title of work, course #, instructor’s name and date. Reports will be judged on the basis of visual appearance, the grammatical correctness and quality of writing, as well as their contents | ✔️ |