**TASK 5 - Packet Capture using Wireshark**

**Wireshark**

1. Click on the Wi-Fi tab below after opening the Wireshark tool

A screenshot of a computer

AI-generated content may be incorrect.

1. Open the command prompt and ping any domain of your choice

A screenshot of a computer program

AI-generated content may be incorrect.

1. All the packets are captured by the Wireshark tool
2. Stop the capture and save the file

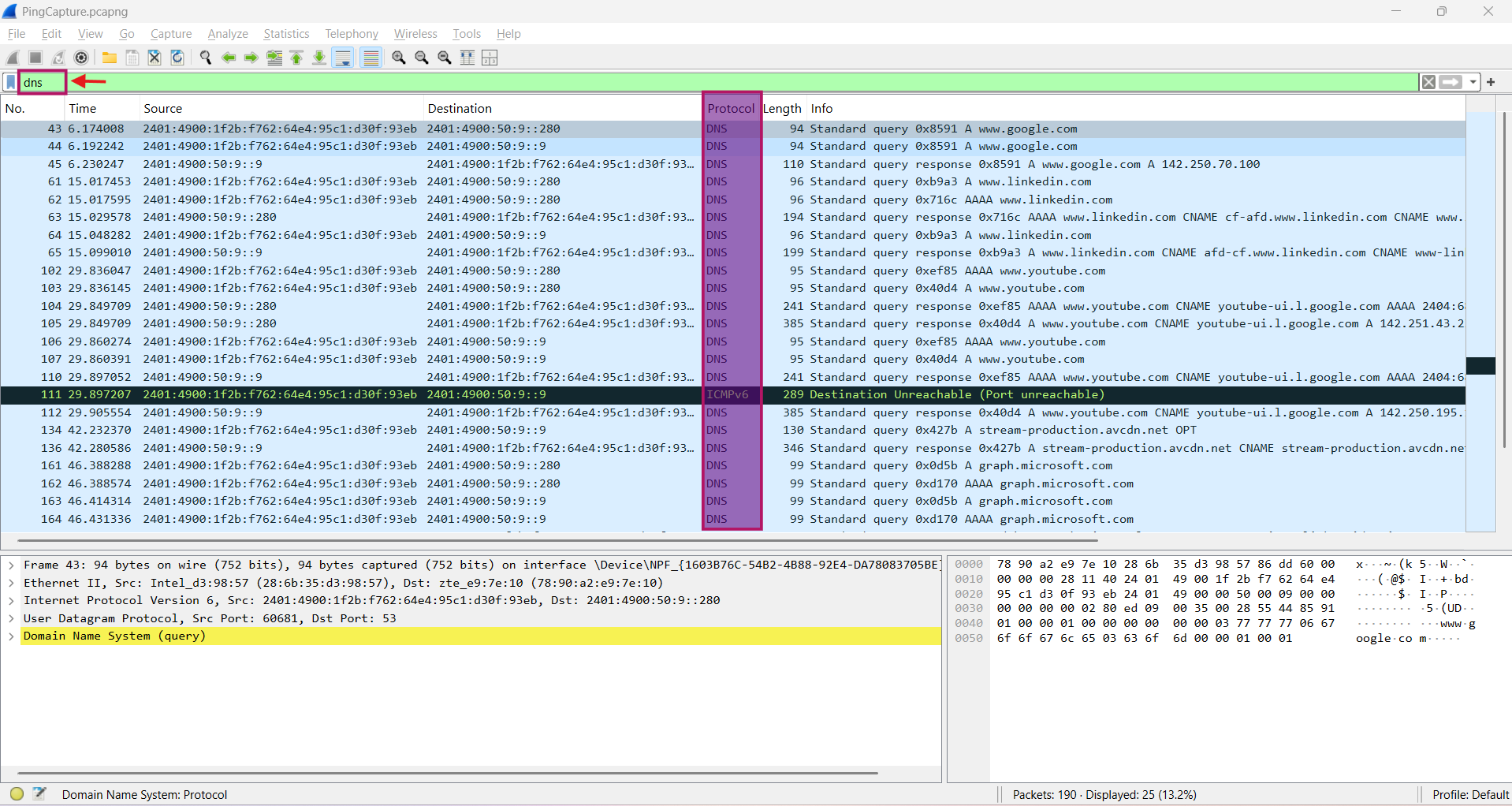
**Packet Analysis**

1. Open the saved Wireshark file to analyze the packets

**A screenshot of a computer

AI-generated content may be incorrect.**

1. Filtered the packets with **DNS** protocol

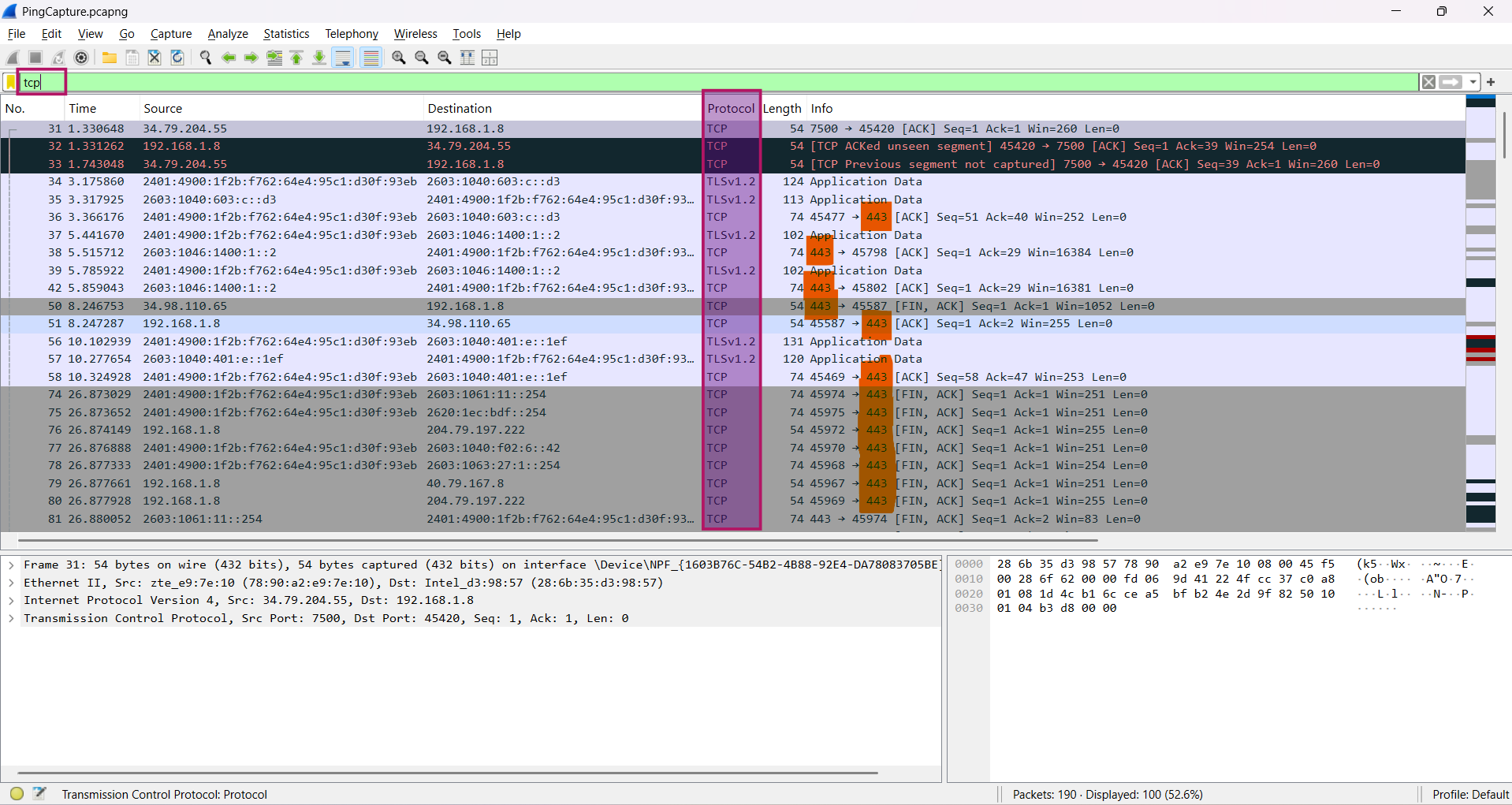


1. There are packets with DNS queries sent for each domain that are pinged using command prompt and the respective response
2. Let us filter the **HTTP** packets from the saved file

A screenshot of a computer

AI-generated content may be incorrect.

1. Filtering the packets with **TCP** protocol



1. In this capture, we can also look at the port numbers associated with the protocol. Port number 443 indicates that it uses a secure communication method
2. We can also filter protocols along with port numbers. There are no port numbers **80** in the captured packets

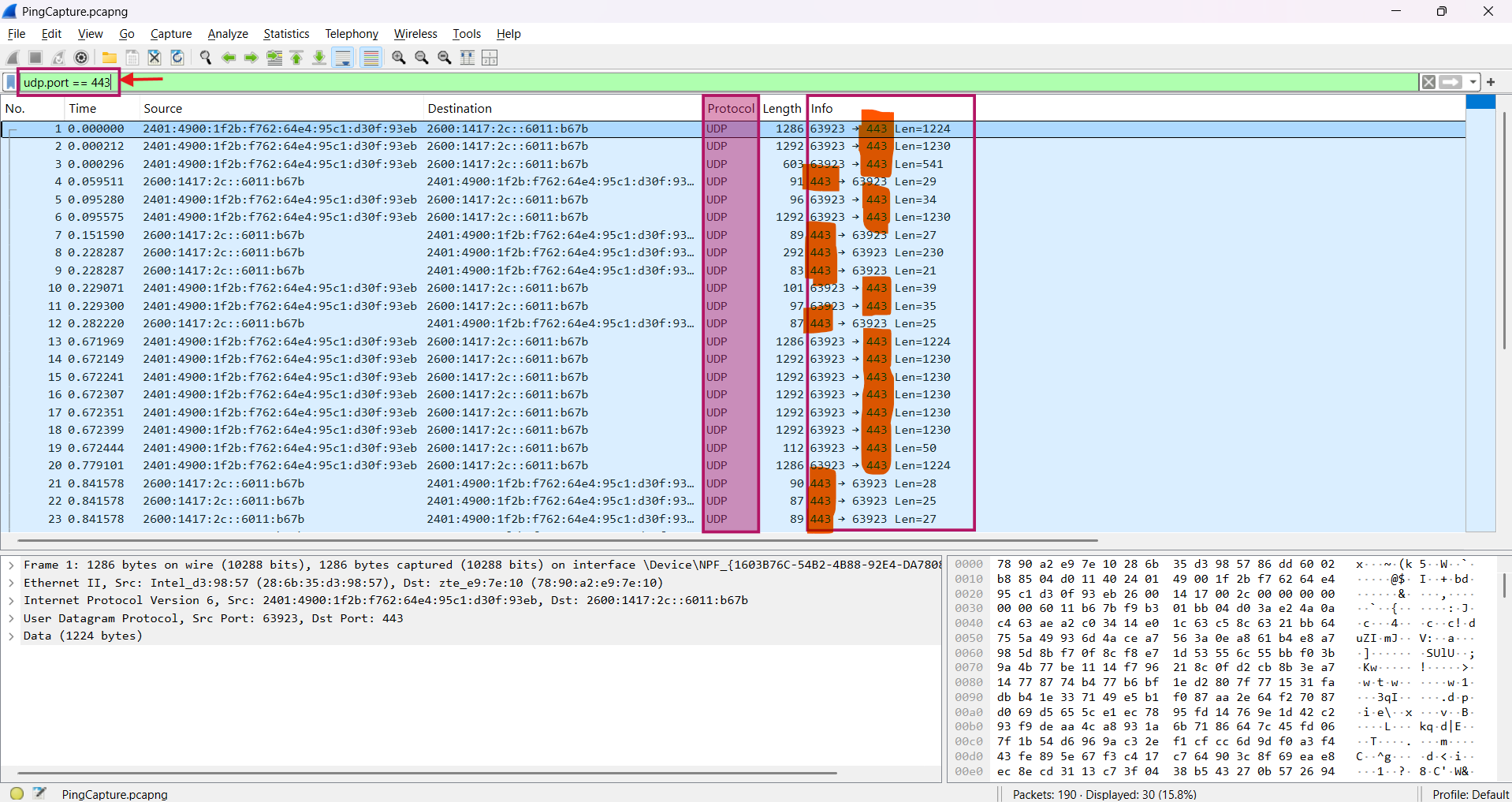
A screenshot of a computer

AI-generated content may be incorrect.

1. Let us try using the **UDP** protocol with port numbers **80** and **443**

A screenshot of a computer

AI-generated content may be incorrect.



1. In the filter below for **ARP**, we can see the broadcast request asking for the corresponding MAC address to the known IP address

A screenshot of a computer

AI-generated content may be incorrect.