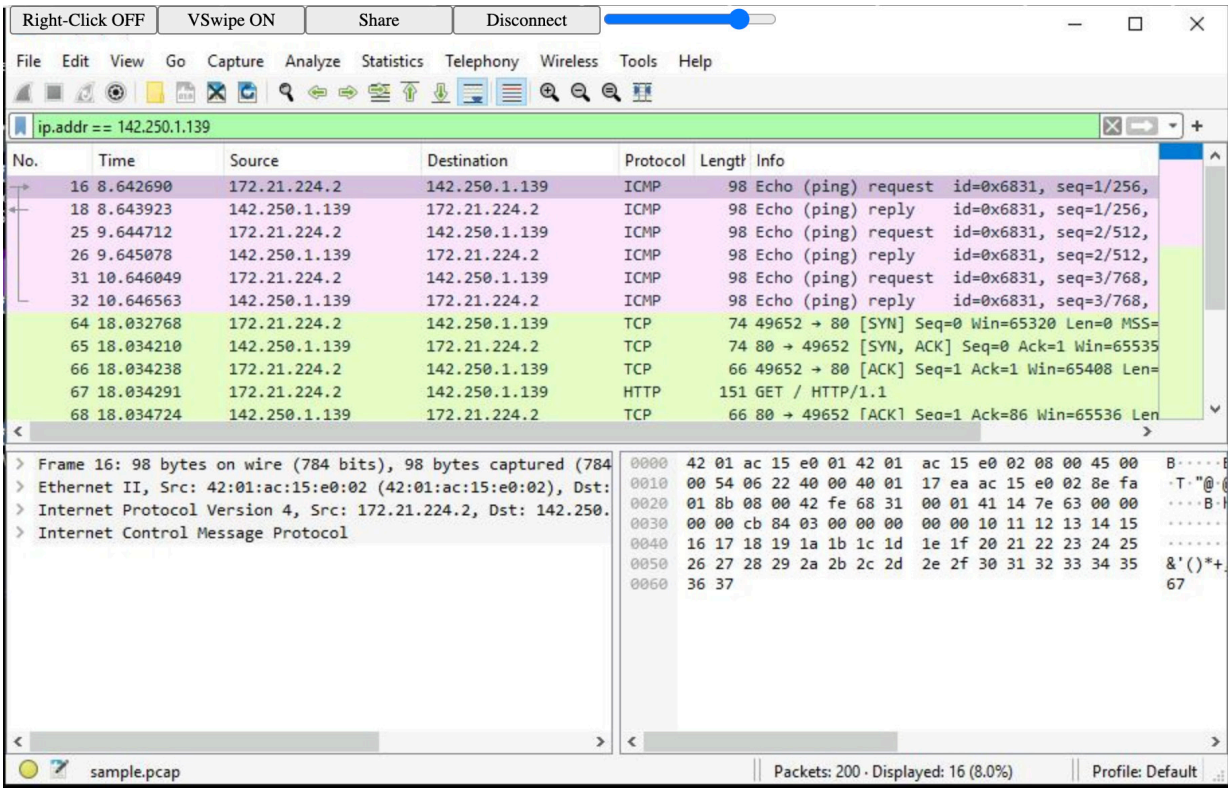
Project

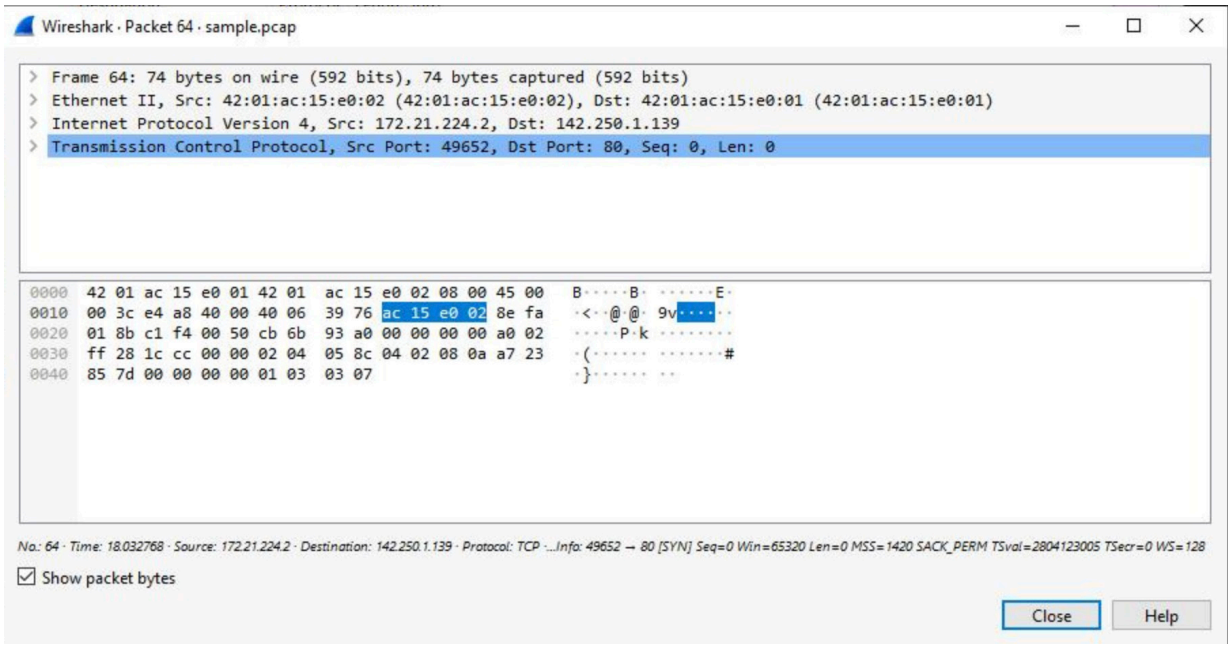
In this project, I will analyze a network packet capture file to determine the source and destination IP addresses involved in a web browsing session. I will investigate the protocols used during the connection to the website, such as TCP, HTTP, or DNS. Additionally, I will inspect specific data packets to identify the type of information being transmitted between systems, including headers, payloads, and metadata

To accomplish this, I will employ tools like Wireshark or tcpdump to capture and filter network traffic effectively. These tools will enable me to dissect packets by applying filters, such as IP address or protocol-specific filters, for focused analysis. Through this project, I aim to gain insights into how data flows across the network during a browsing session, highlighting communication patterns and potential anomalies. Ultimately, this experience will enhance my skills in network traffic analysis and improve my ability to monitor and interpret traffic for operational and security purposes.

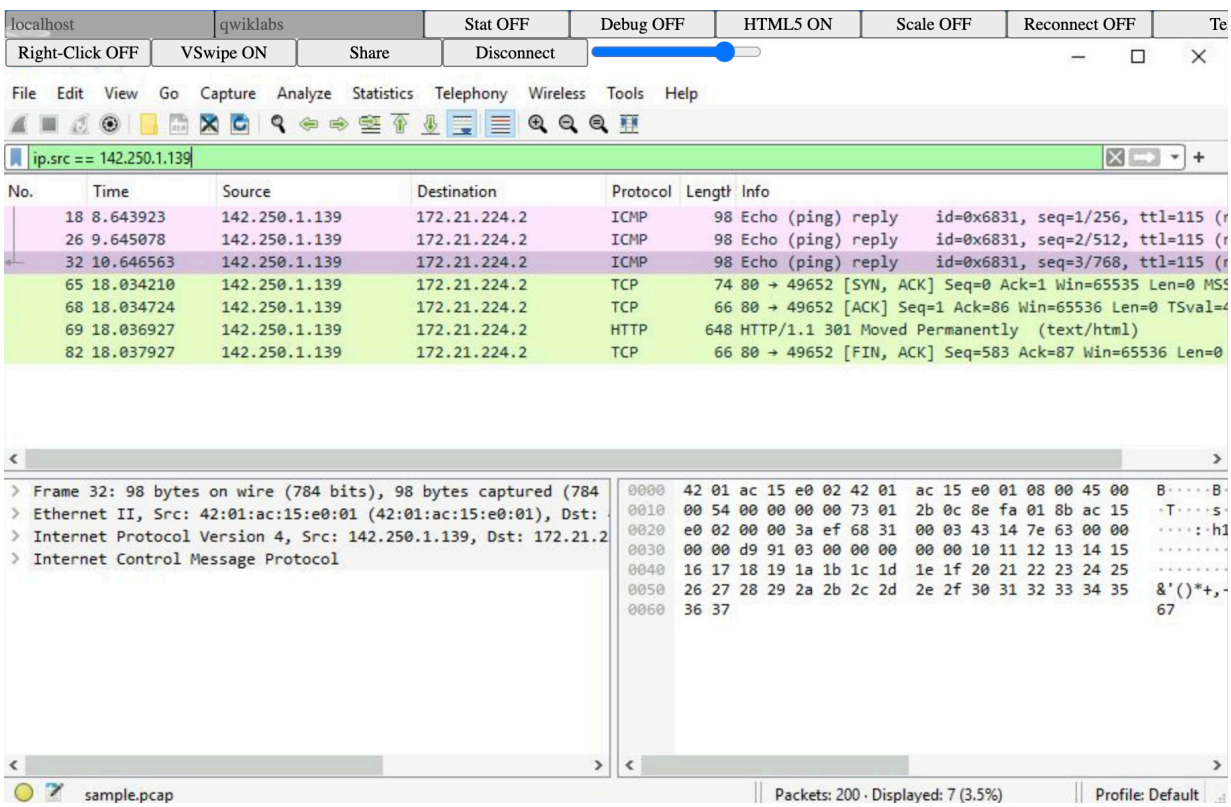
I opened a packet in Wireshark for detailed exploration and applied a display filter to inspect the network layers and protocols contained within the packet. Specifically, I entered the command ip.addr == 142.250.1.139 in the "Apply a display filter..." text box located just above the packet list. This filter allowed me to isolate and view all traffic associated with that specific IP address, enabling a focused analysis of the relevant packets.



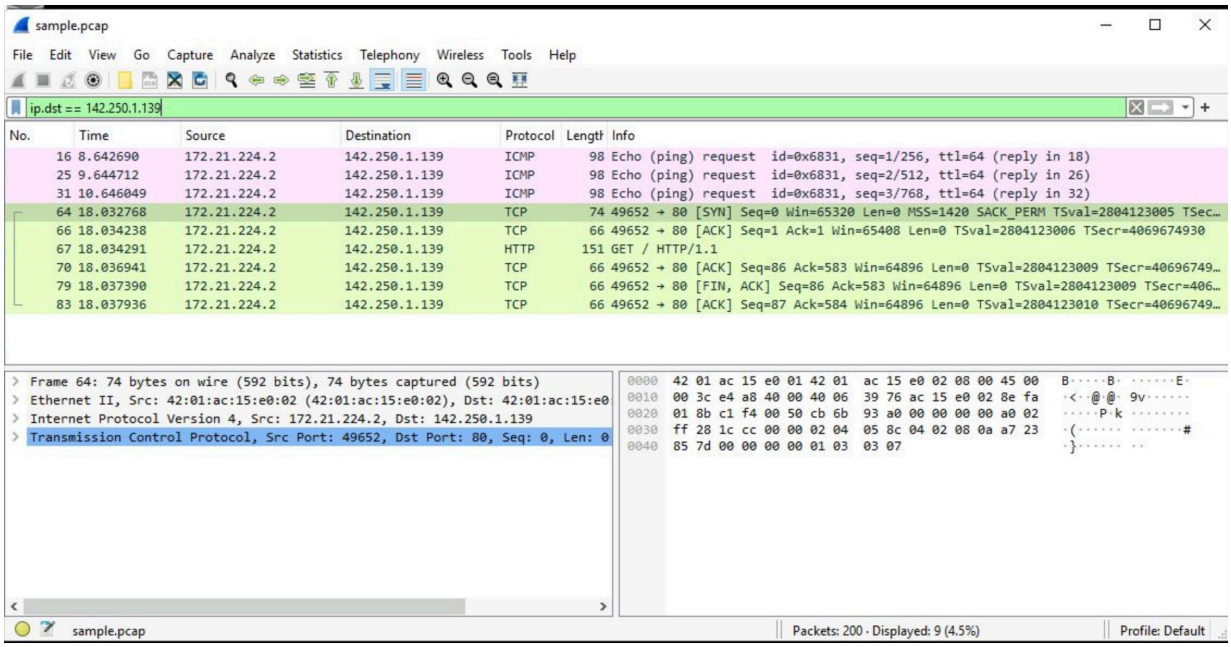
I was then tasked with identifying the destination port of the first TCP packet. To do this, I double-clicked on the Transmission Control Protocol subtree, which revealed that the destination port is 80.



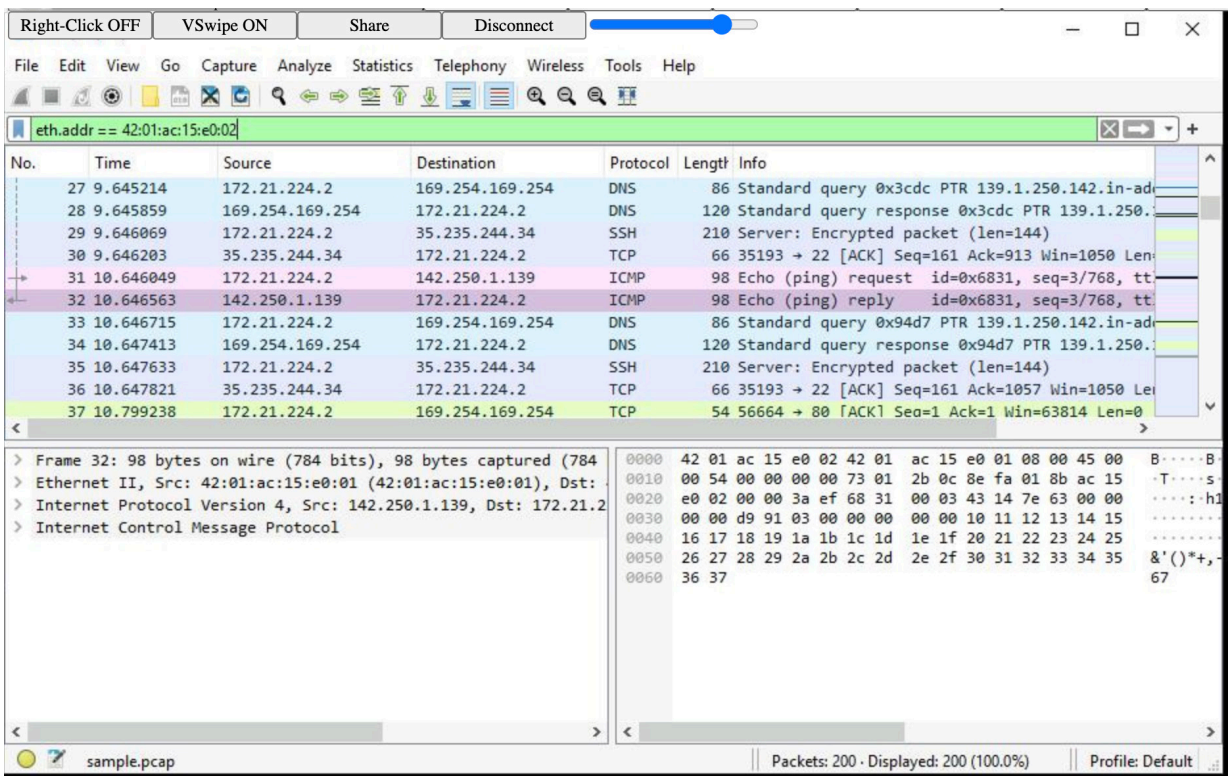
In this task, I used the command ip.src == 142.250.1.139 to filter and analyze specific network packets based on their source or destination. I explored how to select packets using either their physical Ethernet Media Access Control (MAC) address or their Internet Protocol (IP) address.



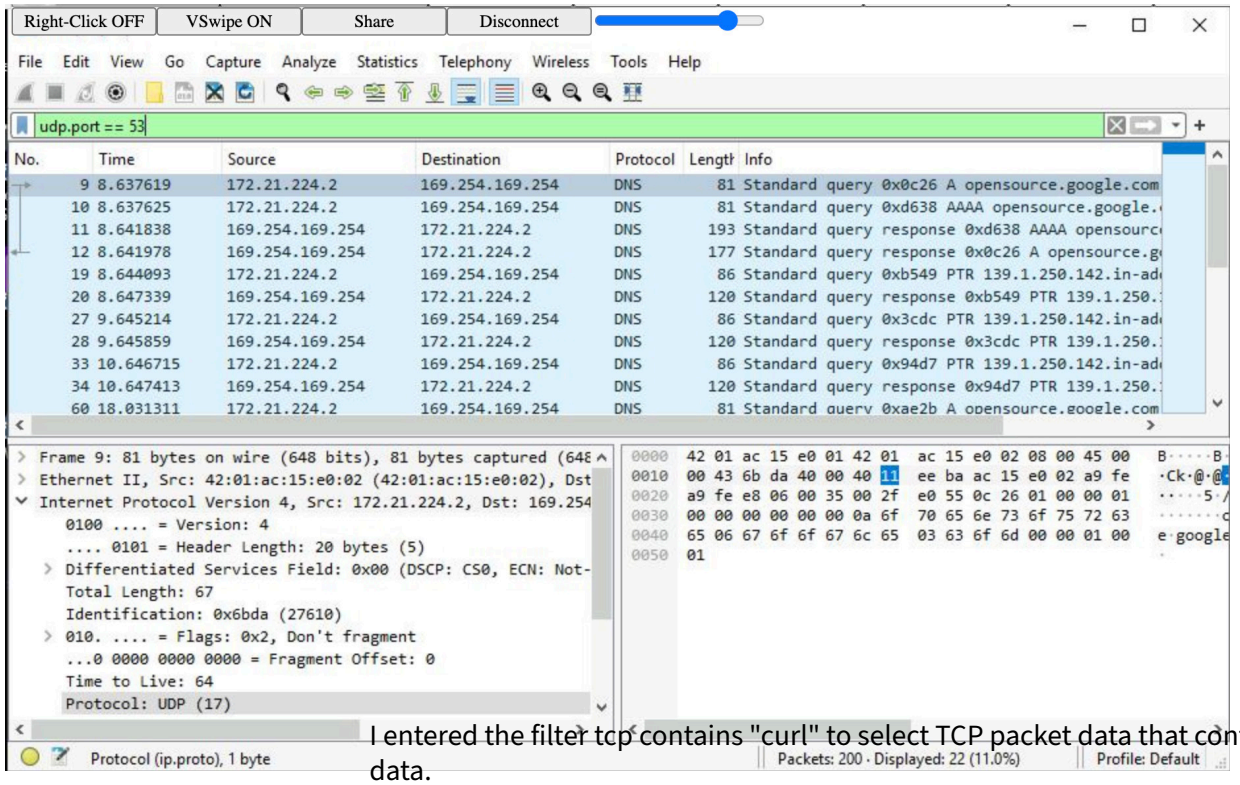
I entered the following filter to select traffic for a specific destination IP address: ip.dst == 142.250.1.139.



I used the command eth.addr == 42:01:ac:15:e0:02 to select traffic to or from a specific Ethernet MAC address.

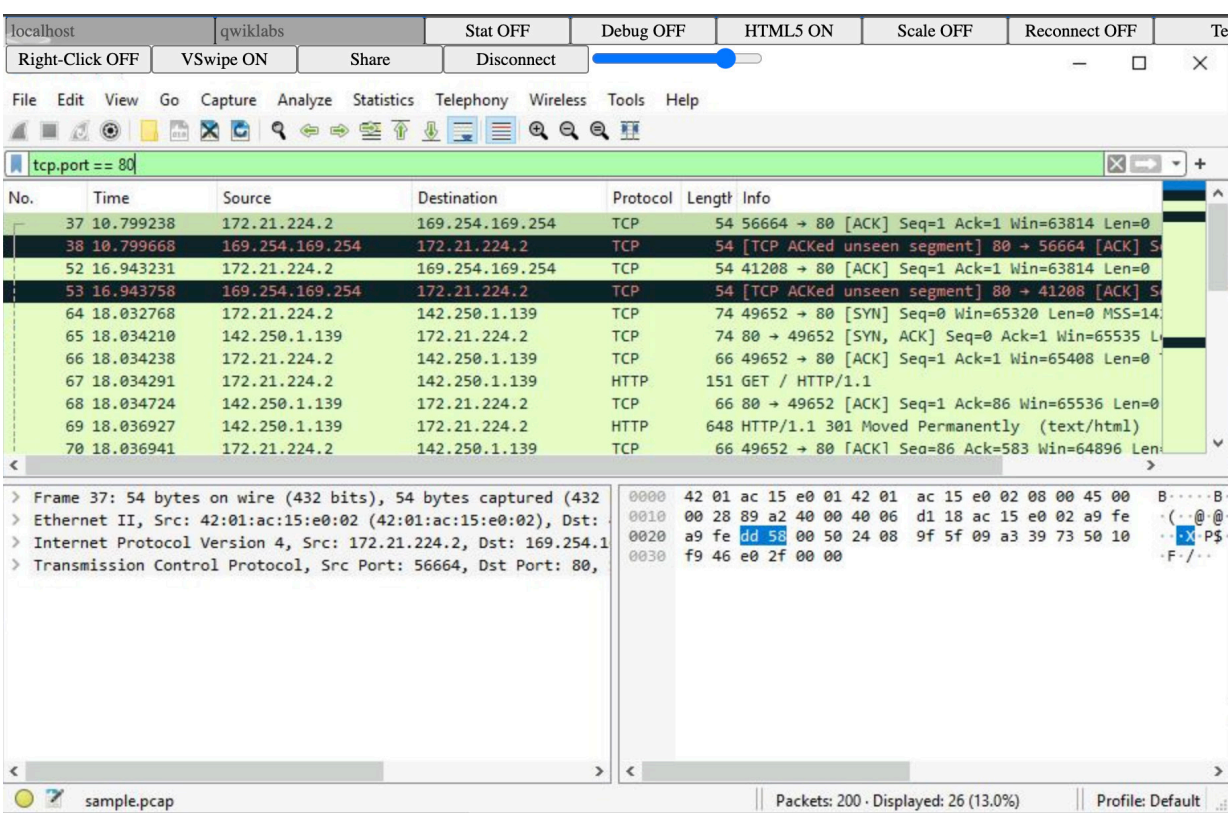


I entered the filter udp.port == 53 to select UDP port 53 traffic, which is used for DNS queries and responses:



I entered the filter tcp contains "curl" to select TCP packet data that contains specific text data.

I entered the filter tcp.port == 80 to select TCP port 80 traffic, which is the default port associated with web traffic.



I entered the filter tcp contains "curl" to select TCP packet data that contains specific text data.