

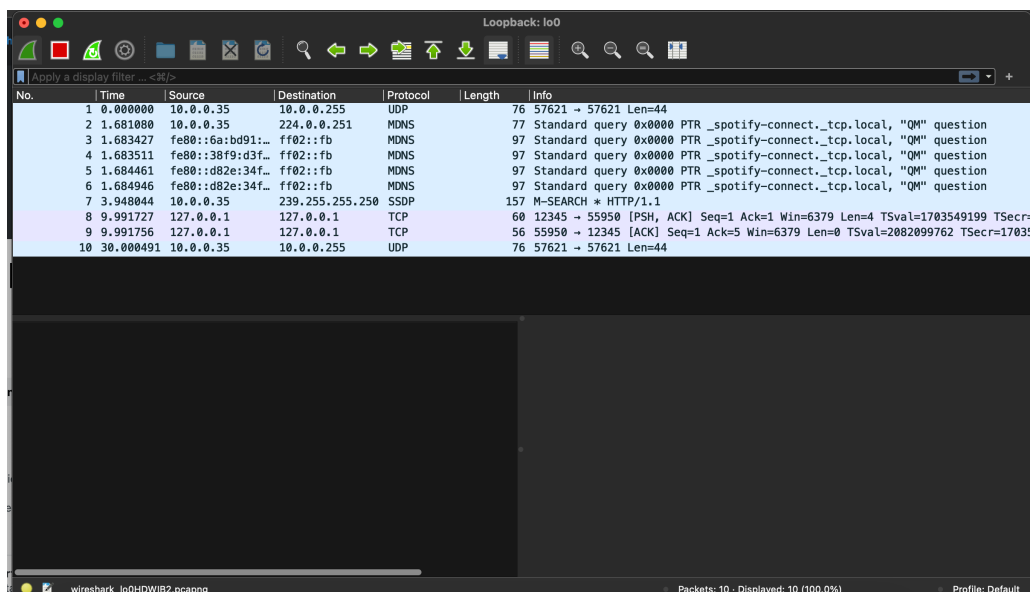
# Capturing and Analyzing TCP Traffic with Wireshark

## Introduction

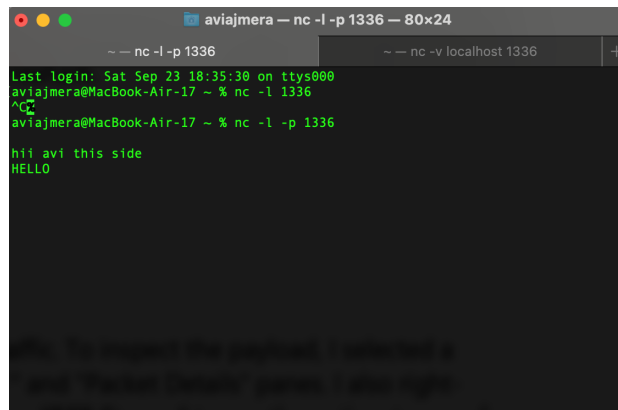
In this assignment, I will explore the process of capturing TCP (Transmission Control Protocol) traffic using Wireshark, a popular network protocol analyzer. This exercise will provide me with practical experience in analyzing network traffic.

## Steps to Capture and Analyze TCP Traffic

In Wireshark, I selected the network interface I wanted to capture traffic from. I typically chose the interface that connects to the network I wanted to monitor. Then, I clicked the "Start" button to begin capturing traffic.

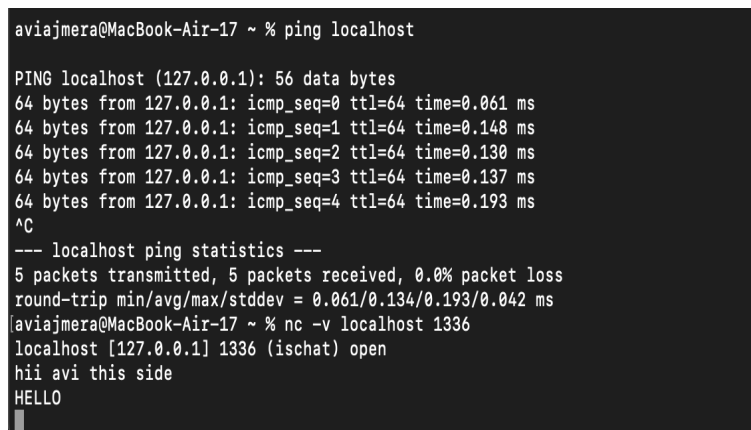


I opened a new terminal window and used Netcat to create a TCP connection to a remote host and port.



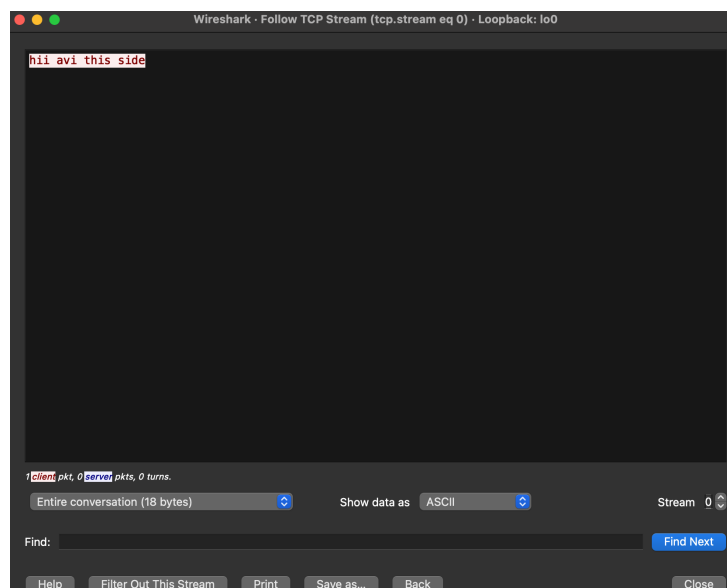
```
aviajmera — nc -l -p 1336 — 80x24
~ -- nc -l -p 1336
Last login: Sat Sep 23 18:35:30 on ttys000
aviajmera@MacBook-Air-17 ~ % nc -l 1336
^C
aviajmera@MacBook-Air-17 ~ % nc -l -p 1336
hii avi this side
HELLO
```

In the terminal where I initiated the Netcat connection, I typed and sent data. I knew that this data would be captured by Wireshark.



```
aviajmera@MacBook-Air-17 ~ % ping localhost
PING localhost (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.061 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.148 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.130 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.137 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.193 ms
^C
--- localhost ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.061/0.134/0.193/0.042 ms
aviajmera@MacBook-Air-17 ~ % nc -v localhost 1336
localhost [127.0.0.1] 1336 (ischat) open
hii avi this side
HELLO
```

In Wireshark, I saw the captured TCP traffic. To inspect the payload, I selected a packet and looked at the "Packet Bytes" and "Packet Details" panes. I also right-clicked on a packet and chose "Follow" > "TCP Stream" to see the entire stream of data.



In this assignment, I successfully captured and analyzed TCP traffic using Wireshark. I learned how to initiate a TCP connection, send data, and capture network traffic.