Spring 2025

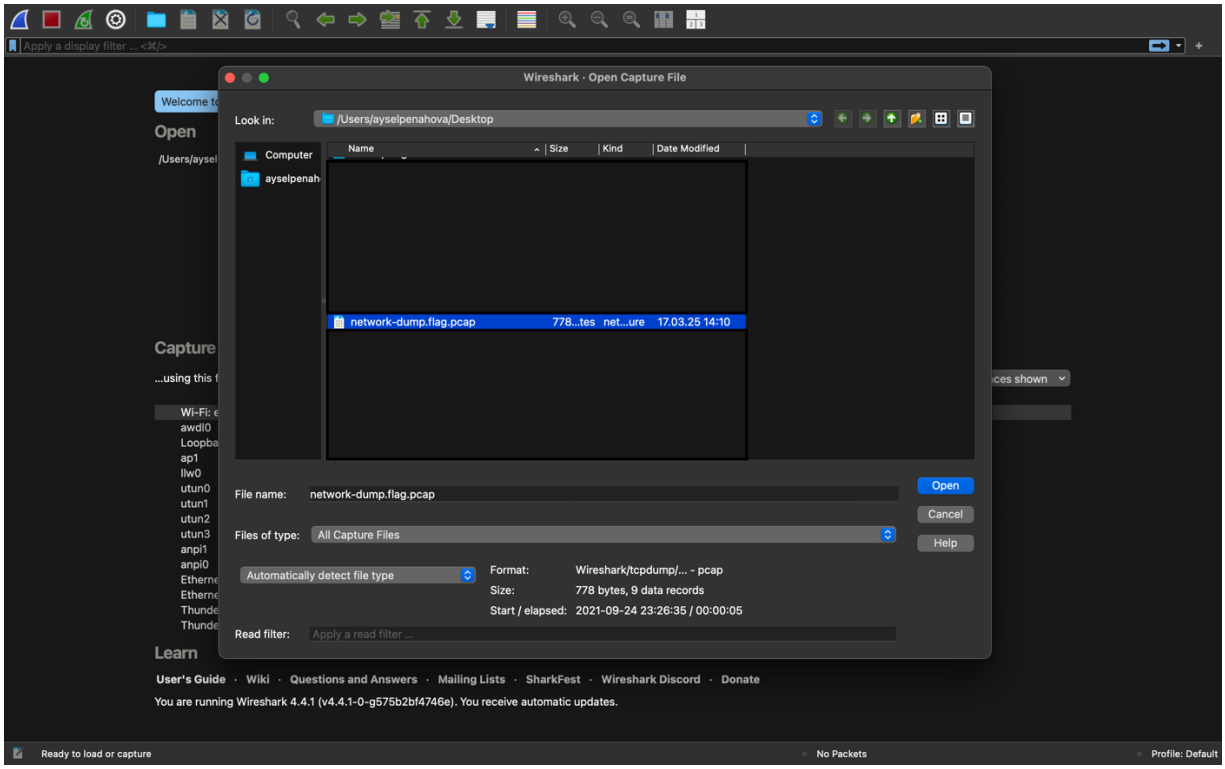
Cyber Security Fundamentals (INFT-3508 - 20332)

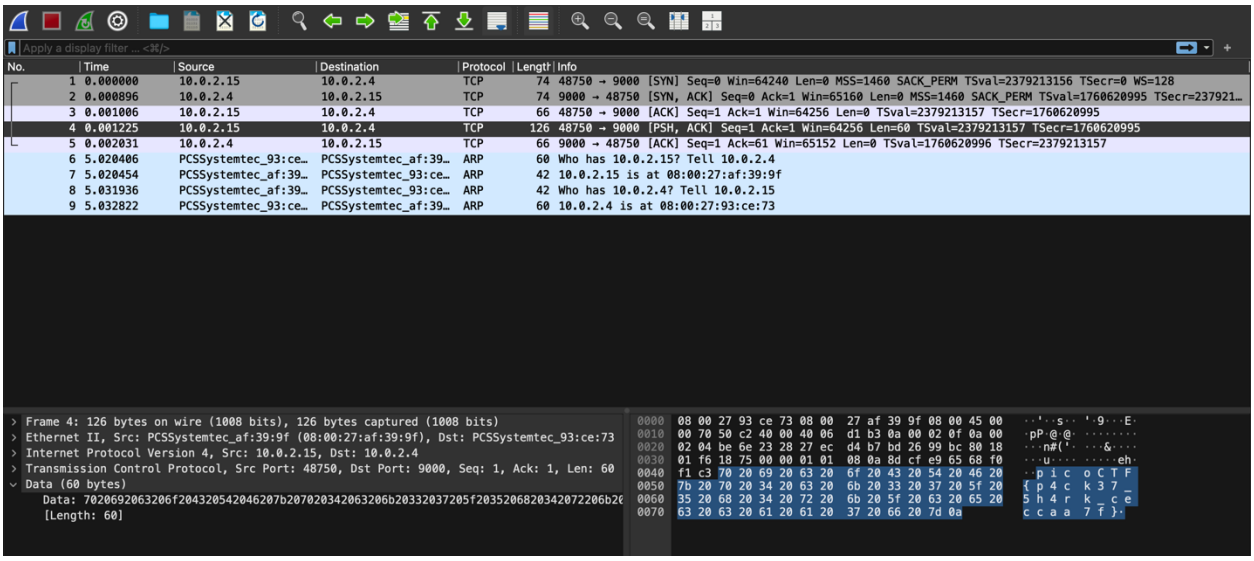
PicoCTF Assignment - Quiz 5

Packets Primer

In this assignment, we need to download the package, which is highlighted as “Download packet capture.” For this task, we need to download the Wireshark application. Wireshark is a popular, free tool that monitors and analyzes network activity. It captures live network data and displays detailed information about the traffic flowing through a network. This makes it useful for diagnosing network problems, studying how different network protocols work, and improving security by detecting unusual activity.

First, we need to download the attached file and open the file in Wireshark.





This is the screenshot of Wireshark when I open the file. The top section shows a list of captured network packets, with each row representing a packet and displaying details like time, source and destination IP addresses, protocol type, and additional information. The Bottom left section provides a breakdown of the selected packet, showing different layers of network communication, such as Ethernet (MAC addresses), source and destination IP addresses, and TCP (port numbers and sequence numbers). On the other hand, the bottom right section displays the raw data of the packet in hexadecimal and a message or a flag, such as “picoCTF{…}”. This indicates that Wireshark captured data being sent over the network.

However, there is a very interesting part. Why is the flag visible when the packet length is 126 bytes but not in packets 74, 66, 60, or 42 bytes? The flag appears in the 126-byte packet because the smaller packet is only acknowledgment (a signal used in networking that confirms successful data reception and is essential in the Three-Way Handshake for establishing a TCP connection), meaning it does not carry actual data. The larger packet includes both an acknowledgment (ACK) and a data payload, which is where the packet is stored. Since only packets with a payload can contain meaningful content, the flag is found in the 126-byte packet.