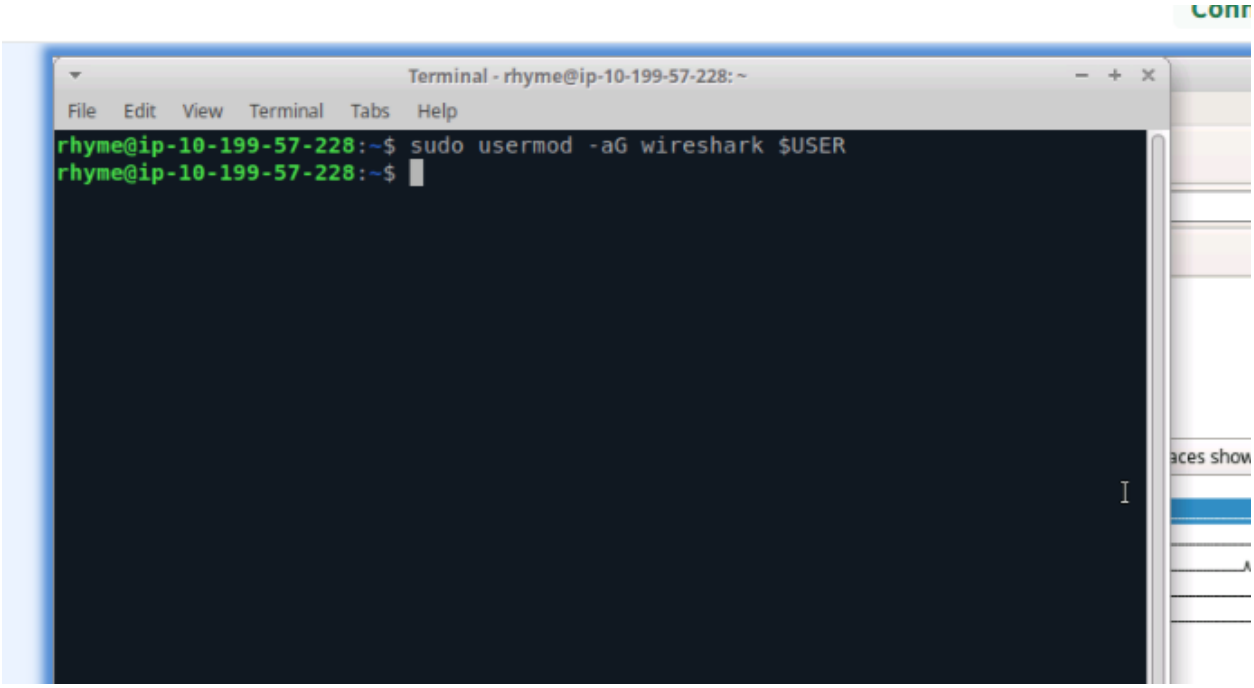
Wireshark Capturing packets

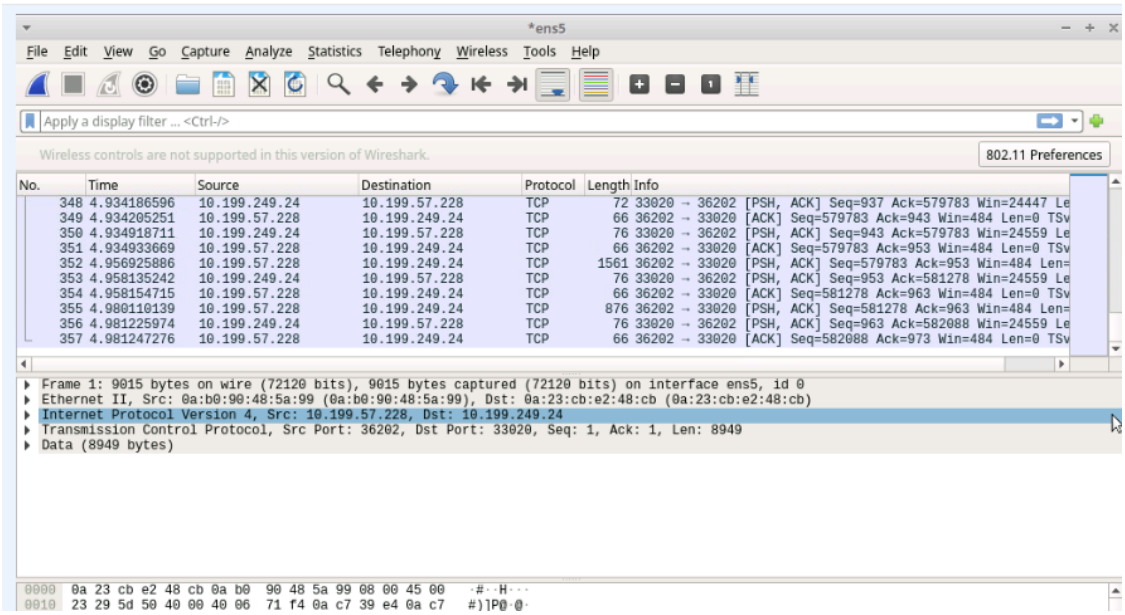
In this guided lab I learned how to install wireshark on Ubuntu, practiced my ability to detect certain network traffic by analyzing and capturing web traffic. Great examples on how to use the display filter to detect IP addresses in packets as well as using the display filter to detect HTTP and HTTPS packets.

- Installed latest version of wireshark on Ubuntu Linux
- Best not not to run as Superuser
- User can be added to Wireshark group to add packet capture capabilities with command



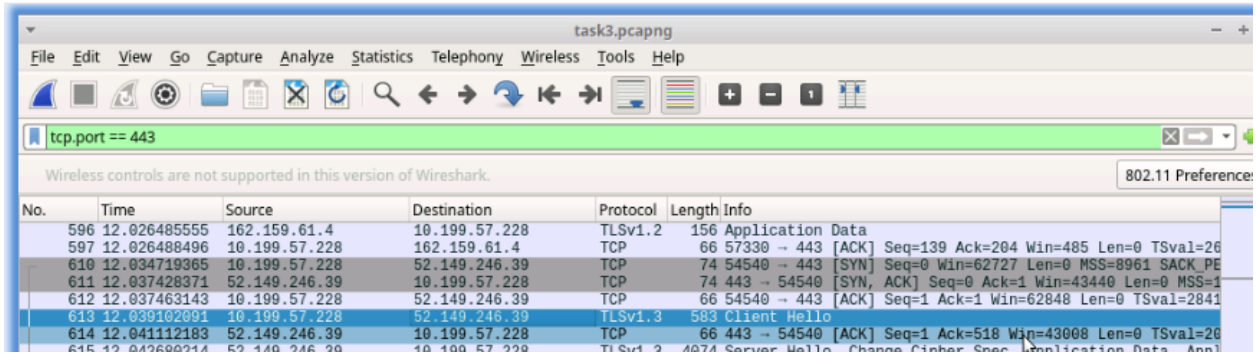
Used WireShark to capture packets on a ethernet port and save captured packets to file

- Wireshark app built in to start,stop,load and save options for me to choose from

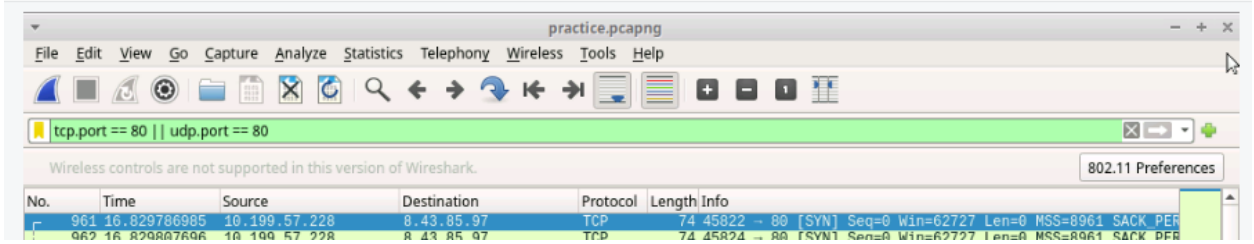


- Used Wireshark to display filter that detects HTTPS packets

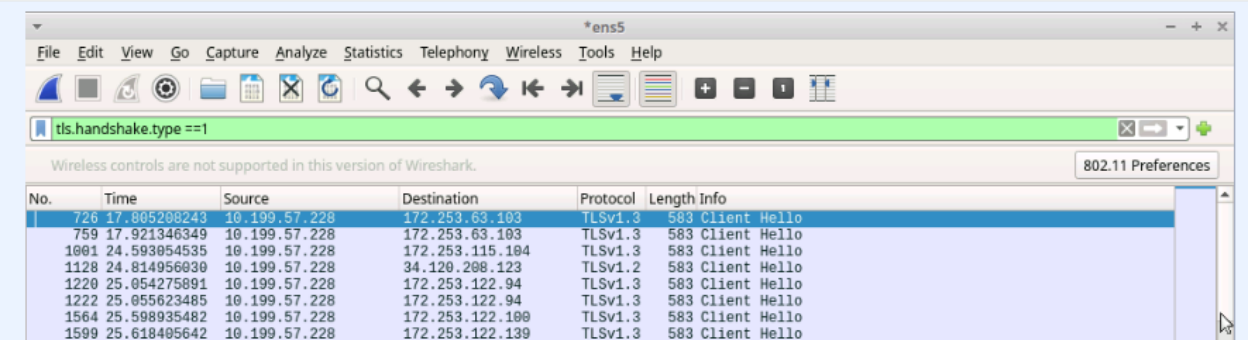
-Displaying only HTTPS traffic use filter tcp.port ==443



-Displaying only HTTP packets traffic in display filter



-Learned to enter the proper display filter for tls handshake image shows first stepin handshake when communicating with server



- Also can filter by a particular ip address with ip.addr == “enter address”

-Learned to exclude a particular ip address and add ports 443 and 80 in the display field when filtering packets: