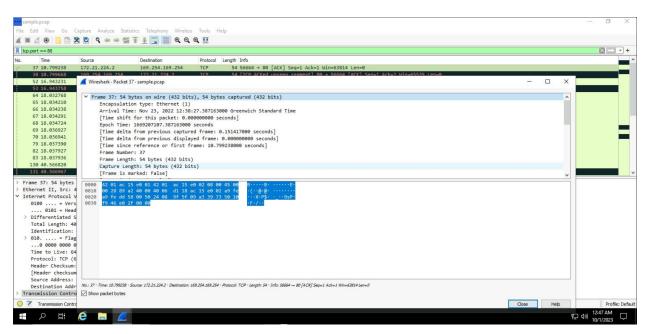
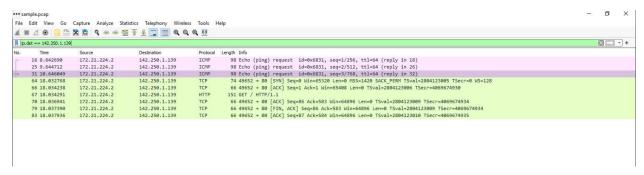
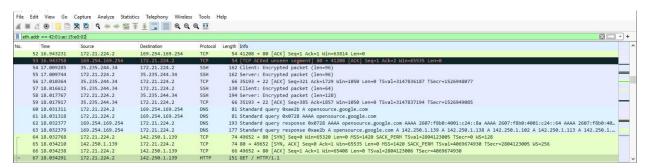
UTILIZATION OF FILTERS IN WIRESHARK PACKET SNIFFER.



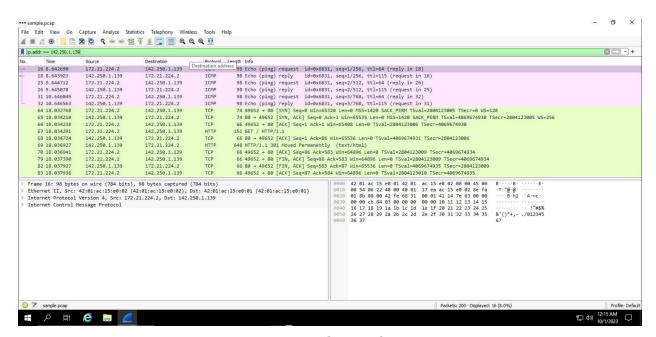
In the screenshot above, I explored the port 80 TCP Packets by using a filter; tcp.port == 80 through the top filter execution bar. This command displayed numerous information about the particular port like the Internet Protocol, Time Stamp, Time To Live (TTL), Source IP, Destination IP, etc.



In the above screenshot, I inspected the destination IP address packets with an *ip.dst* filter. The dst in this filter means destination and the IP means Internet Protocol which is a unique address that identifies a device on the internet or on a local network.



Selecting traffic from a specific ethernet MAC address by using this filter; *eth.addr* == 42.01:ac.15.e0:02. "Eth" from the filter means ethernet, "addr" means address and the combination of numbers and alphabets is the MAC address being scrutinized.



Inspecting a packet with a basic WireShark filter; *ip.addr* == 142.250.1.139. The "ip.addr" part of the filter means IP address and the other numbers that follow; 142.250.1.139 is the particular IP address being inspected.