Contents

Scenario:

- Working for a company that wants to detect certain TCP/IP network traffic on their server
- IT manager wants to be able to capture ethernet network web traffic on the server and be able to detect certain IP addresses as well

Task 1 : Install and set up Wireshark

1. To get the latest stable version of Wireshark on Ubuntu Linux, use the add-apt-repository command: ***sudo add-apt-repository ppa:wireshark-dev/stable***

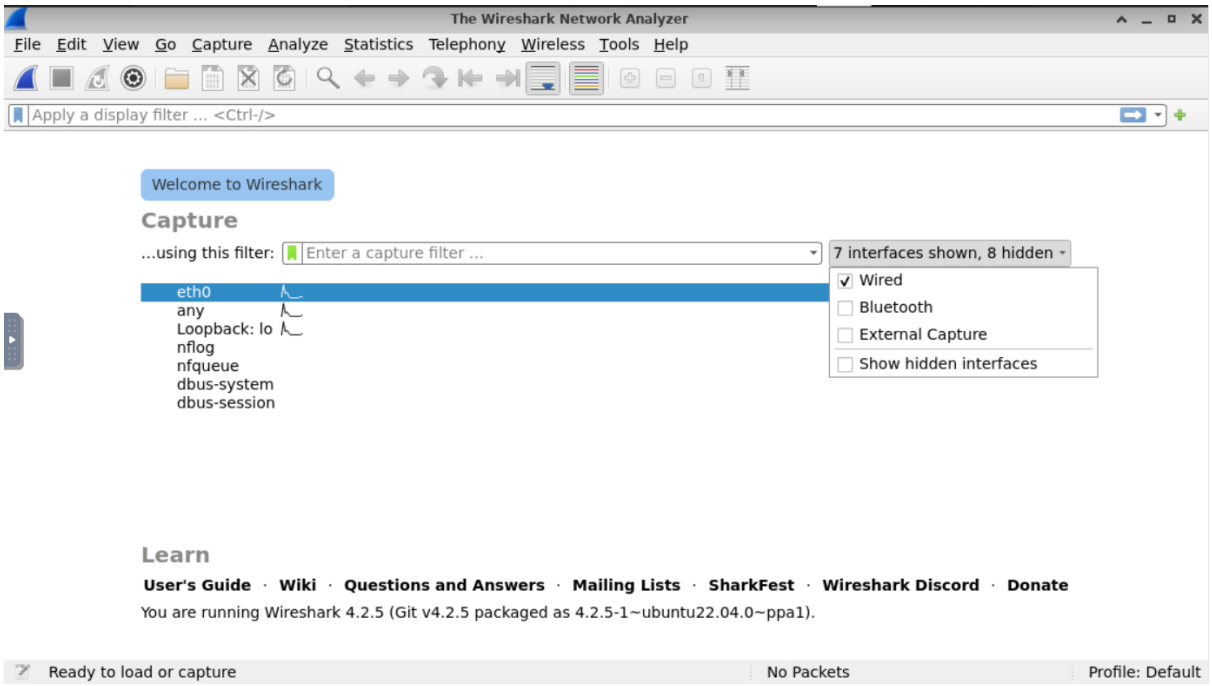
NOTE: Wireshark should not be run as superuser for security reasons.

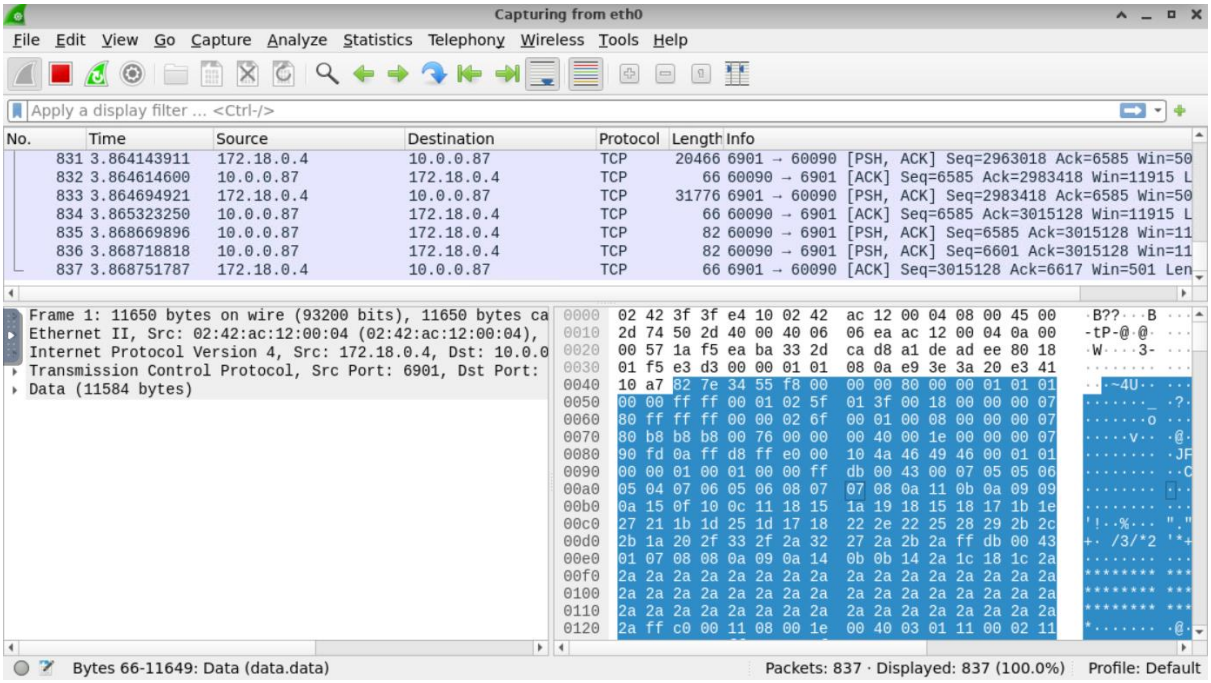
2. The user can be added to the Wireshark group to add packet capture capabilities: ***sudo usermod -aG wireshark $USER***

NOTE: the -a means to append a user, G is a group

Task 2: Start Packet capture on an ethernet port and save it to a file

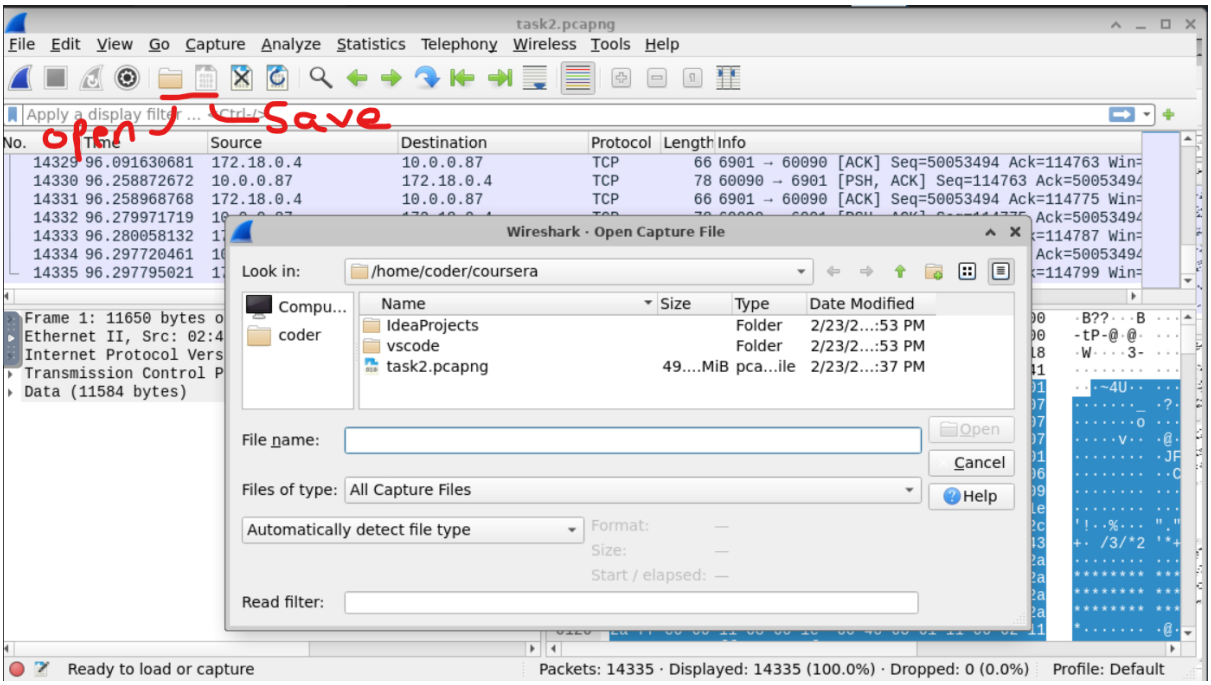
1. Filter to the wired connections and select the ethernet option. Press the blue shark on the top left to start capturing packets





NOTE: Press the stop button to stop capturing packets. If you let it continue you could run out of memory.

2. Save and open the capture file

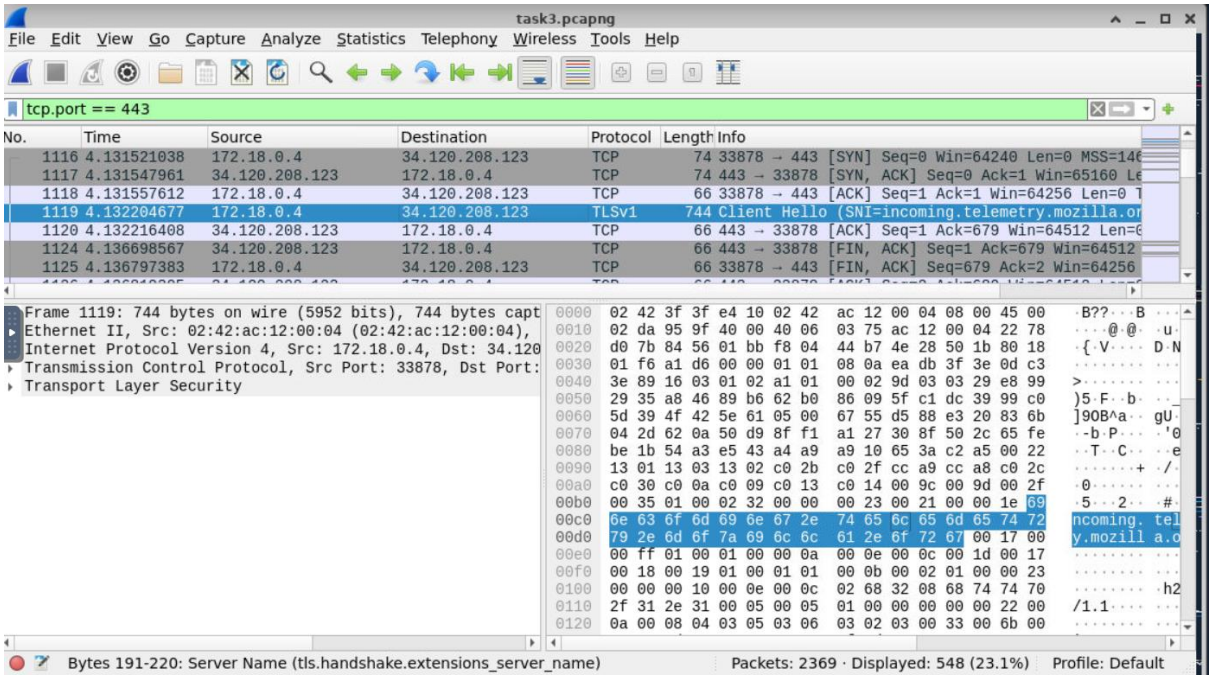


NOTE: You cannot save a capture if it is running

Task 3: Use a display filter to detect HTTPS packets

1. Start capturing packets, search duckduckgo on the internet, stop capturing packets and save the capture.

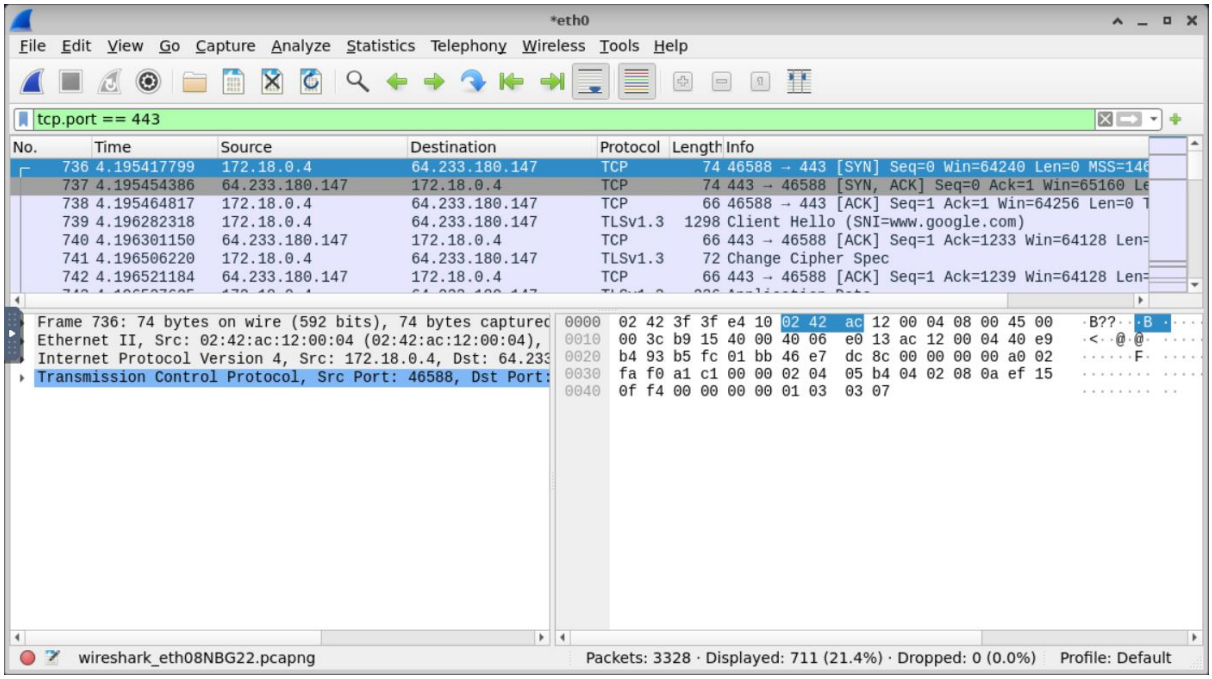
2. Use the display filter to find all activity on port 443



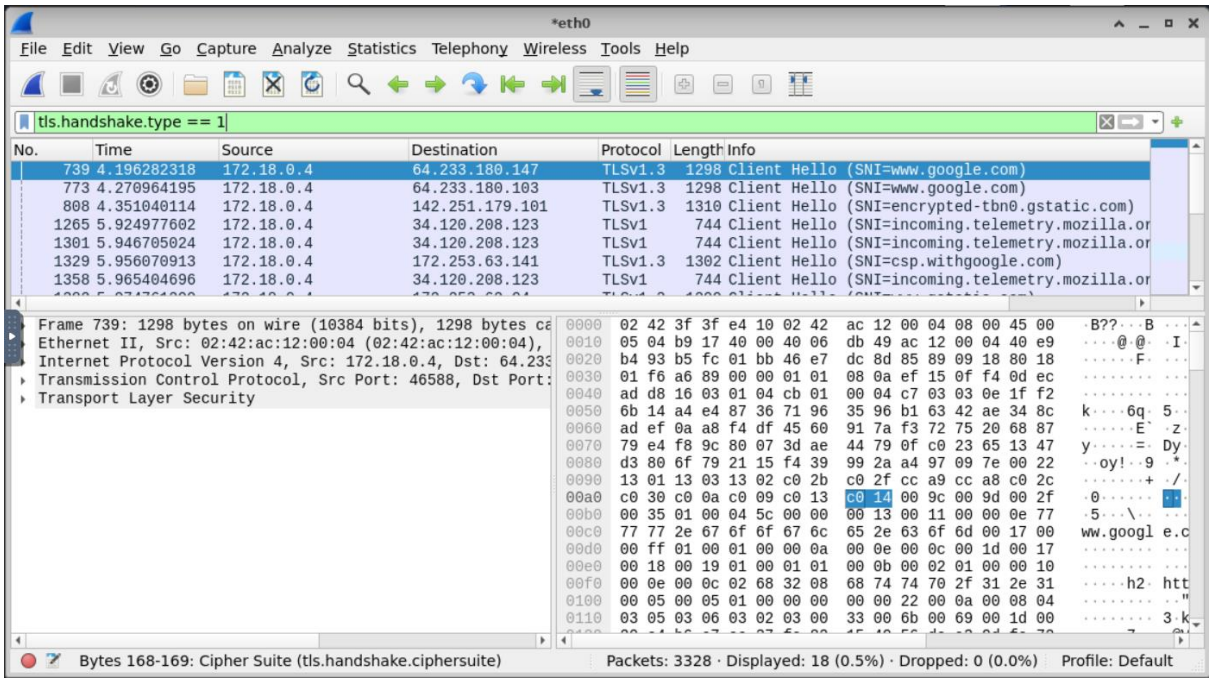
NOTE: the packet with the 'Client Hello' is the search for DuckDuckGo, if you copy the destination IP and paste into your browser, it will take you to DuckDuckGo. You get additional information by double clicking on that packet.

Task 4: Visit webpage and detect its IP address using a display filter

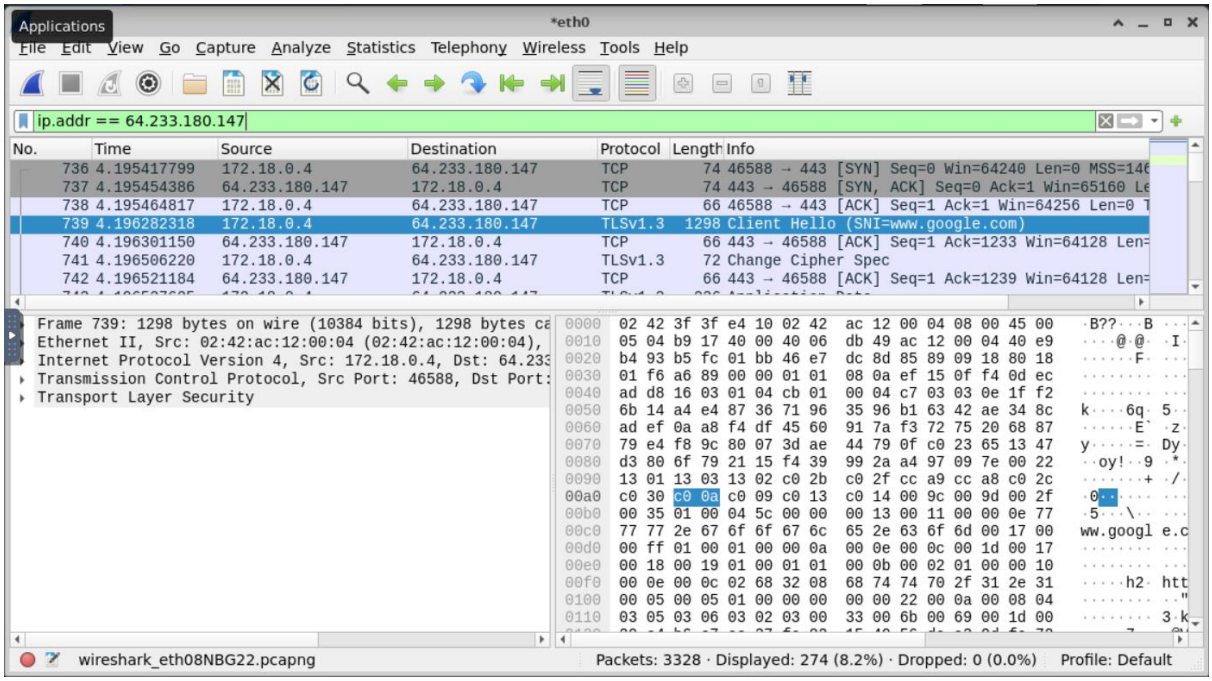
1. Capture packets for a search for google and check port 443 for https packets.



2. Change the display filters to present the first step of the tls handshake



3. We can use another display filter to view all packets associated with the specified IP address

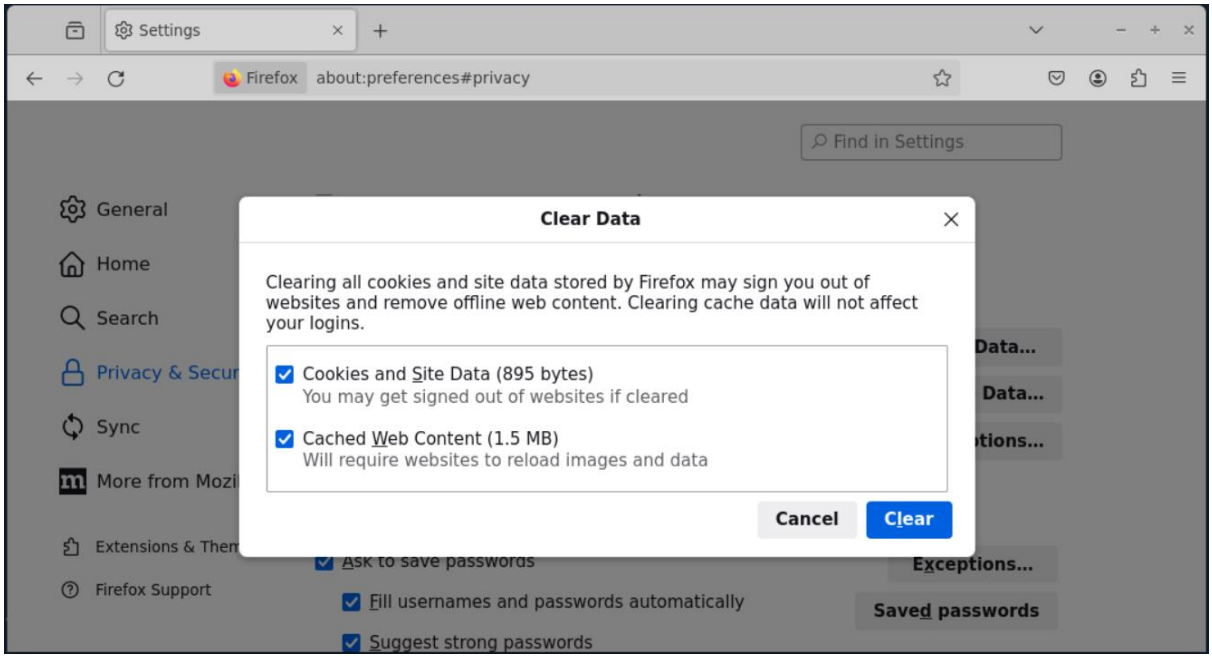


NOTE: There are additional filters like ‘ip.src’ and ‘ip.dst’ to view all packets with a source or destination with the IP specified.

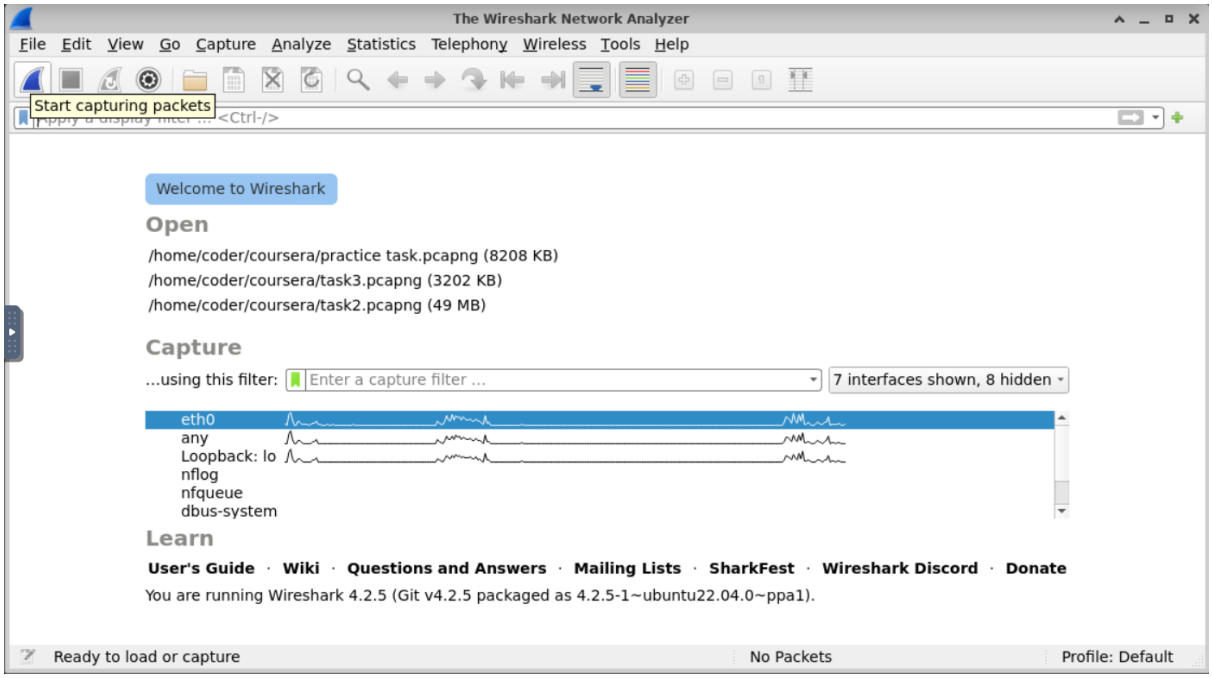
NOTE: We can also use conditional filters using ‘and’, ‘or’, and ‘!([enter filters])’(for NOT).

Capstone task: You are to use Wireshark to create a capture file and then use a display filter to list all https and http packets. You will then eliminate one IP address from the capture using a display filter.

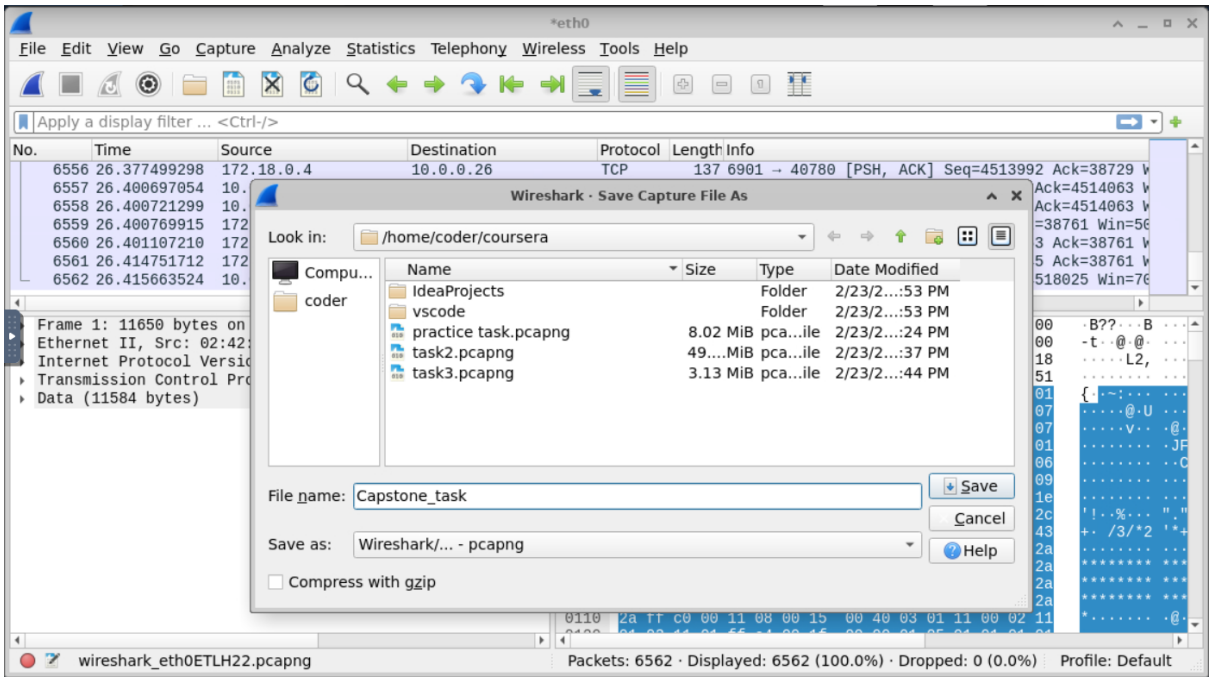
1. Clear the cache in the Firefox browser



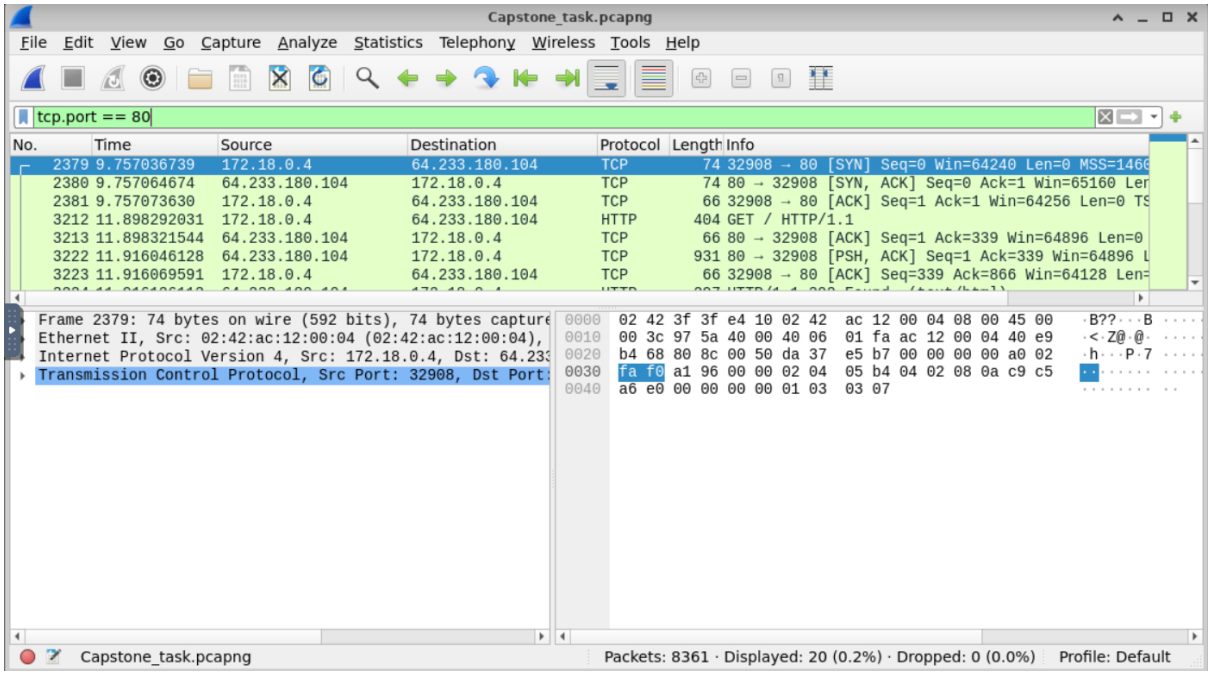
2. Start a packet capture on the ethernet in Wireshark and visit google.com, duckduckgo.com, and http://cygwin.com (not https)



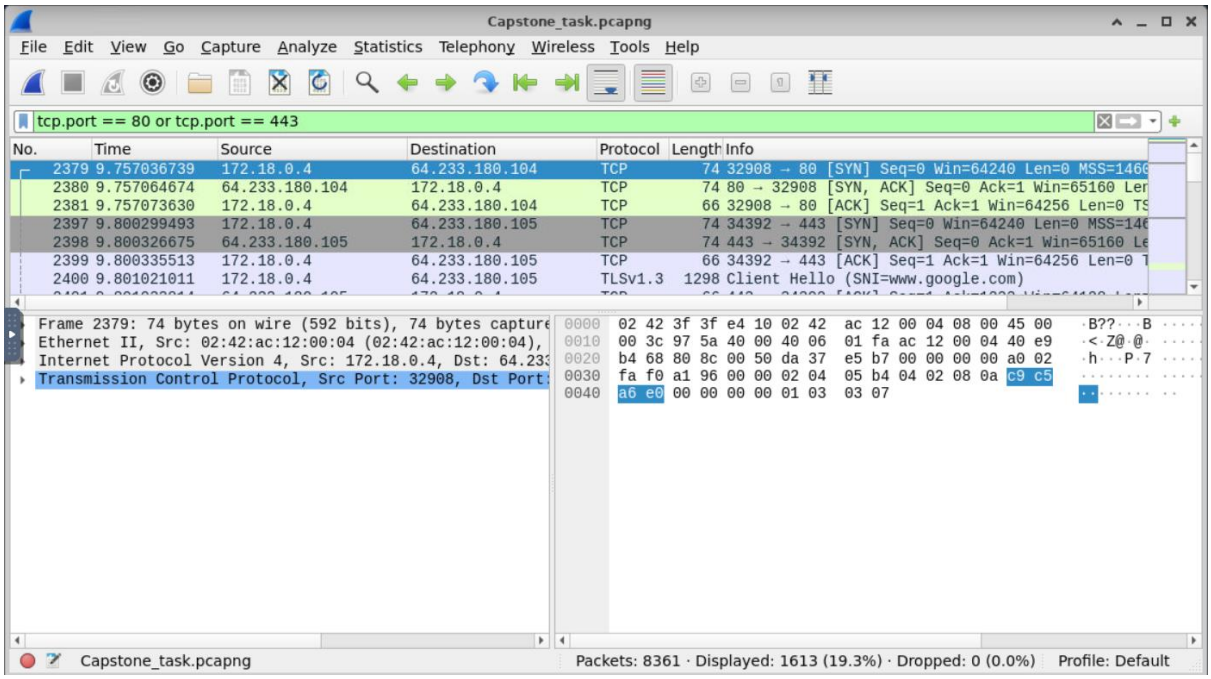
3. Stop the packet capture in Wireshark and save the capture to a file



4. Create a filter to just display port 80 TCP data. This should give you the IP address of Cygwin.



5. Create a filter to display only HTTP AND HTTPS packets



6. Eliminate the Cygwin site visits from the displayed packets