Aim: Using Wireshark Tool.

Wireshark is a network packet analyzer that intercepts, captures and logs information about packets
passing through a network interface. This is useful for analyzing network problems, detecting network
intrusions, network misuse, and other security problems, monitor usage and gather statistics, and many other applications.

Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount, of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

We can also click the Analyze menu and select Display Filters to create a new filter Click on Ok

Another interesting thing you can do **is right-click a packet** and **select Follow TCP Stream.** You'll see the full conversation between the client and the server.

Close the window and you'll find a filter has been applied automatically — Wireshark is showing you
the packets that make up the conversation

Step 1: Exploring Wireshark

- On menu bar **select Capture Option**
- Select Once you **click on start**
- Wireshark starts to capture the packets on that interface.

Step 2: Filter packets with HTTP protocol

- A file with only text:

msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?0a9109c2b28701dc

Step 3: Applying different filters using expressions.

- Filtering HTTP POST request
- **Click on Expression** and Select the following and **Click on OK**
- **Filtering HTTP REQUEST==1**