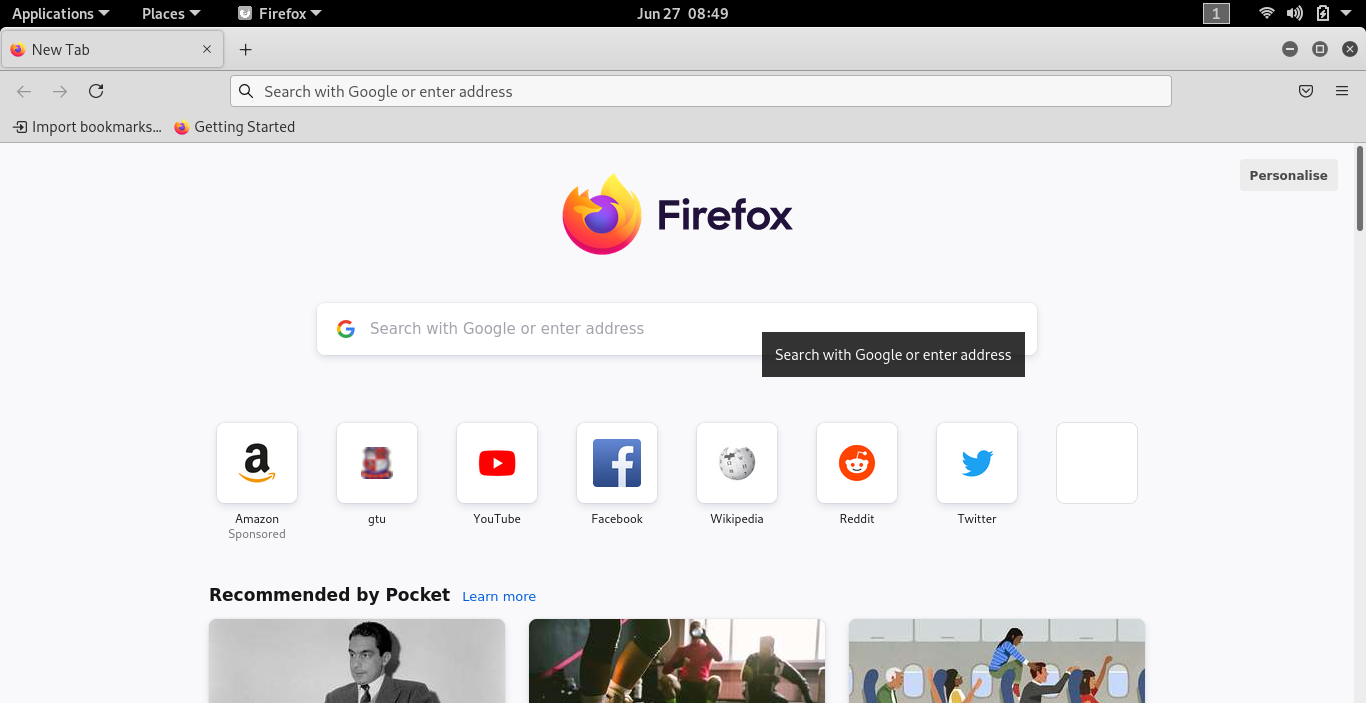
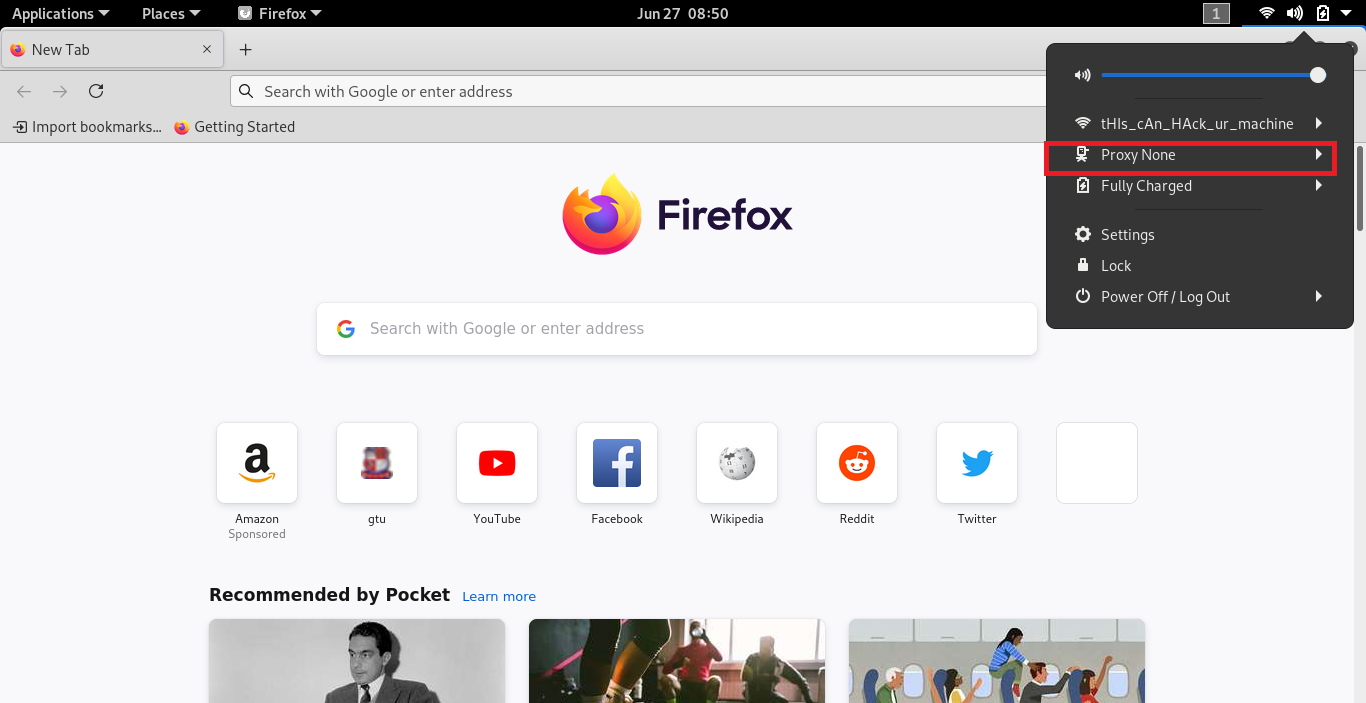
**1. List up to IO different protocols that appear in the protocol column in the unfiltered**

**packet-listing window.**

Here, I started Firefox browser which u like very much and which was displayed homepage like above one

1. **If you are using a proxy (especially a host-based one), disable it if possible to examine uncached network traffic**

****

Above image show that currently I’m not using proxy

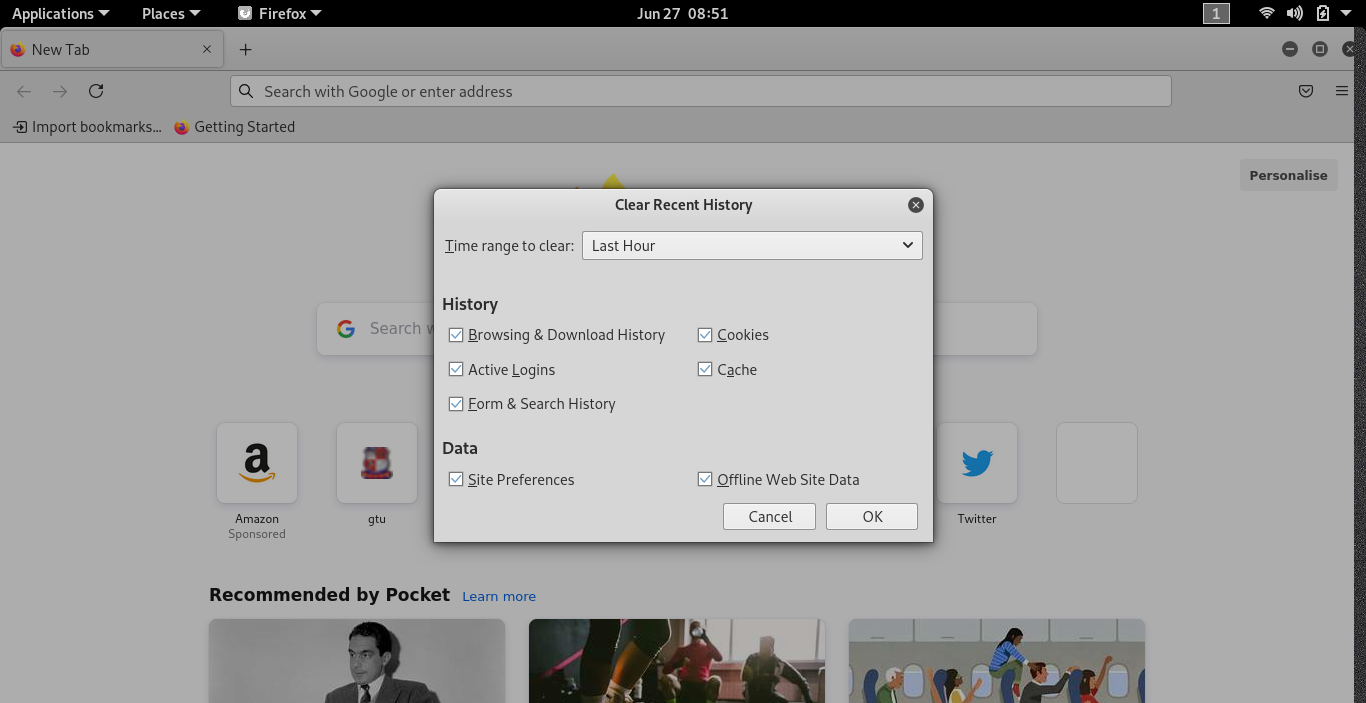
{

If you are on windows to that follow this step to check

First open control panel> Network and Internet> internet option > open connection tab> Lan Setting   
Here you have to make sure **use a proxy server for your lan** is unchecked

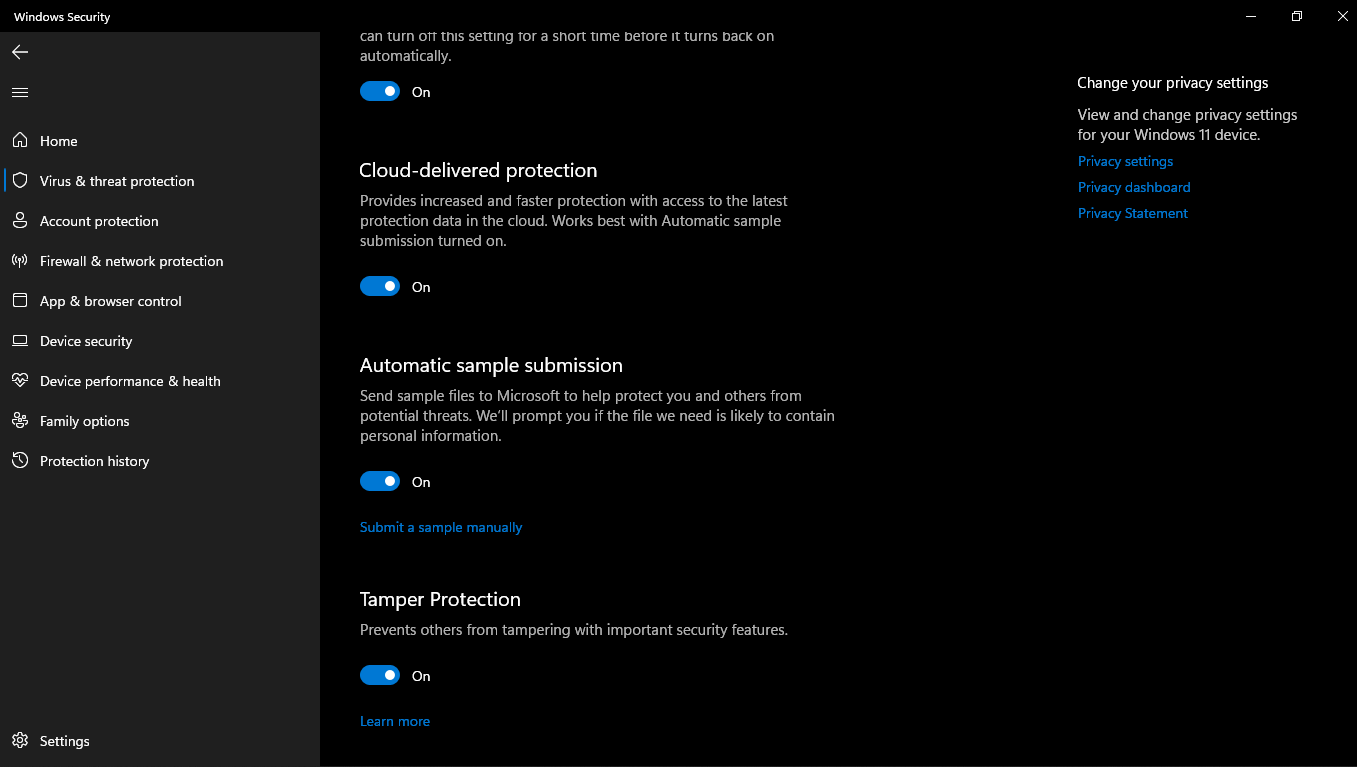
}

1. **Also better to clear browser cache, cookies if you have previously displayed this page**

****

In any browser just press CTRL + SHIFT + DLT and press Clear now or okay to clear cookie and cache

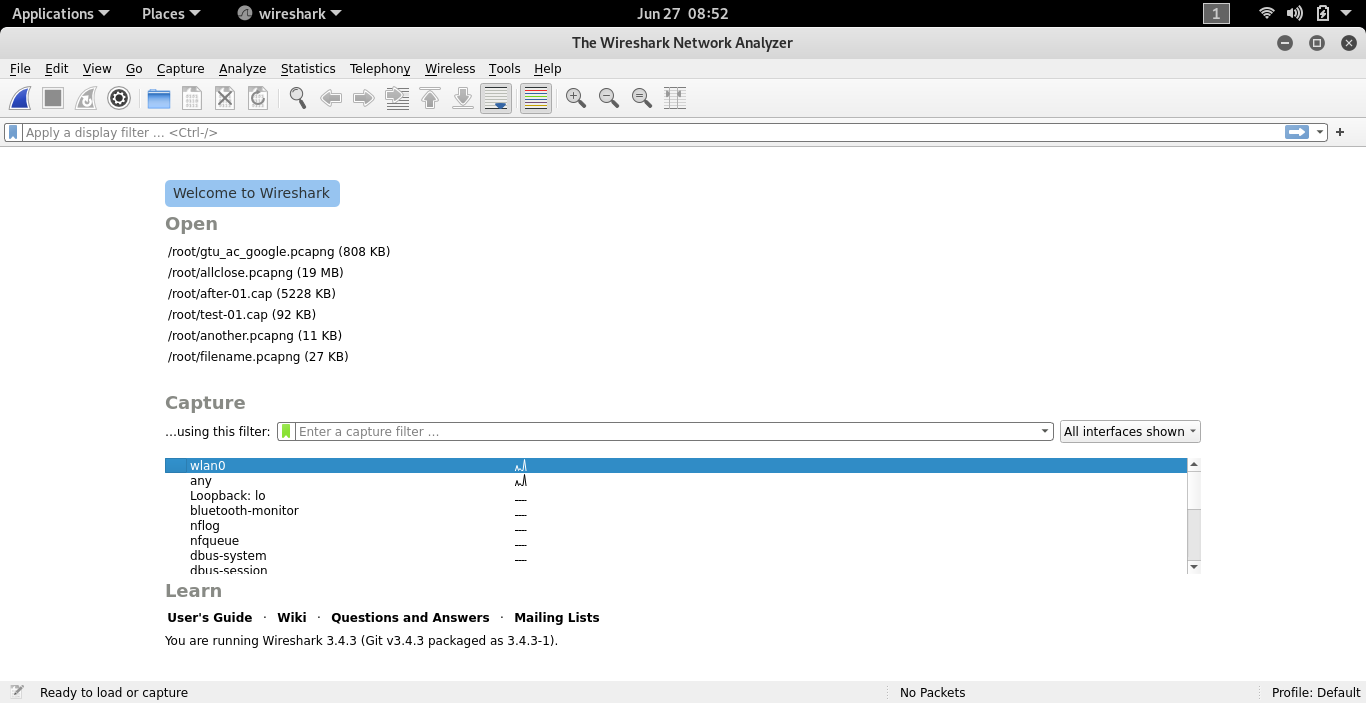
1. **Disable anti-virus protection software before your own IP address will show up in captured data.**



In windows 10 or later uncheck this all btns

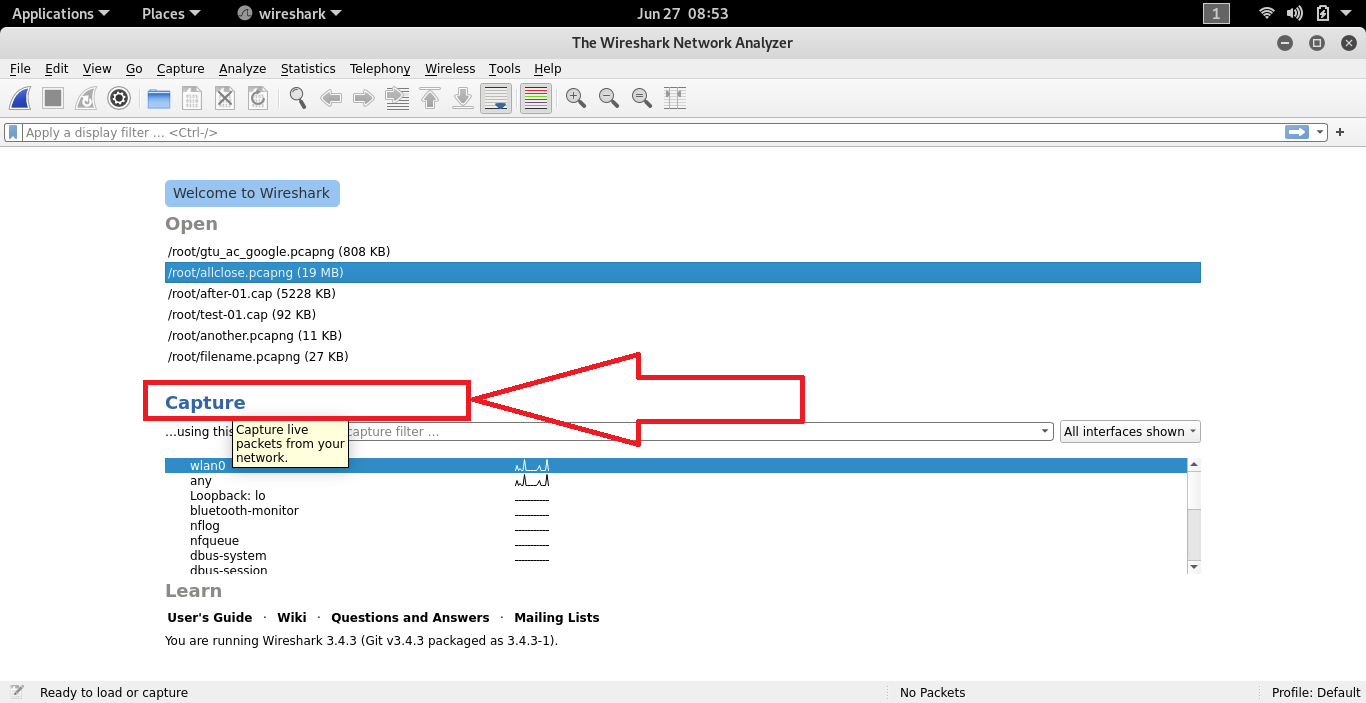
Here im using linux so I did’nt have any antivirus

1. **Start up the Wireshark software, look like following figure**

****

Above Image Shows that Wireshark software look like this

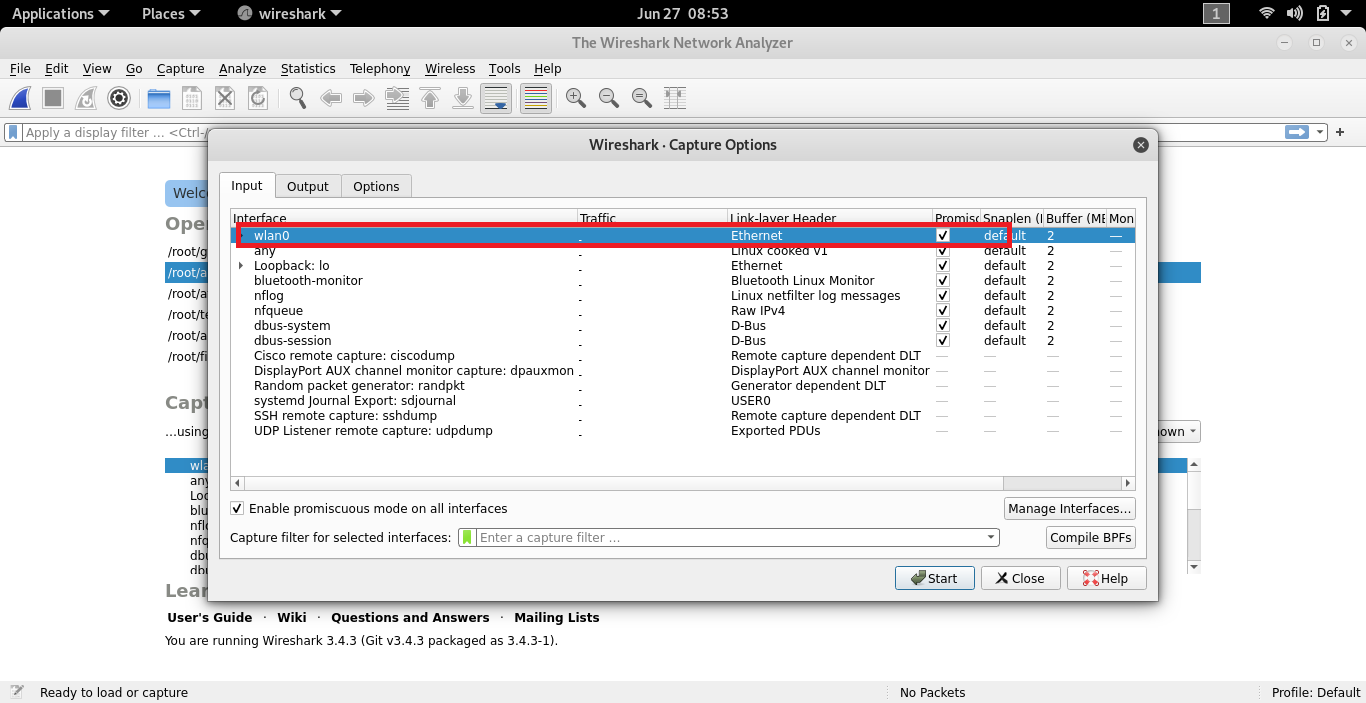
1. **To begin packet capture, select the Capture pull down menu and select Options. This will cause the “Wireshark: Capture Options” window to be displayed**

****

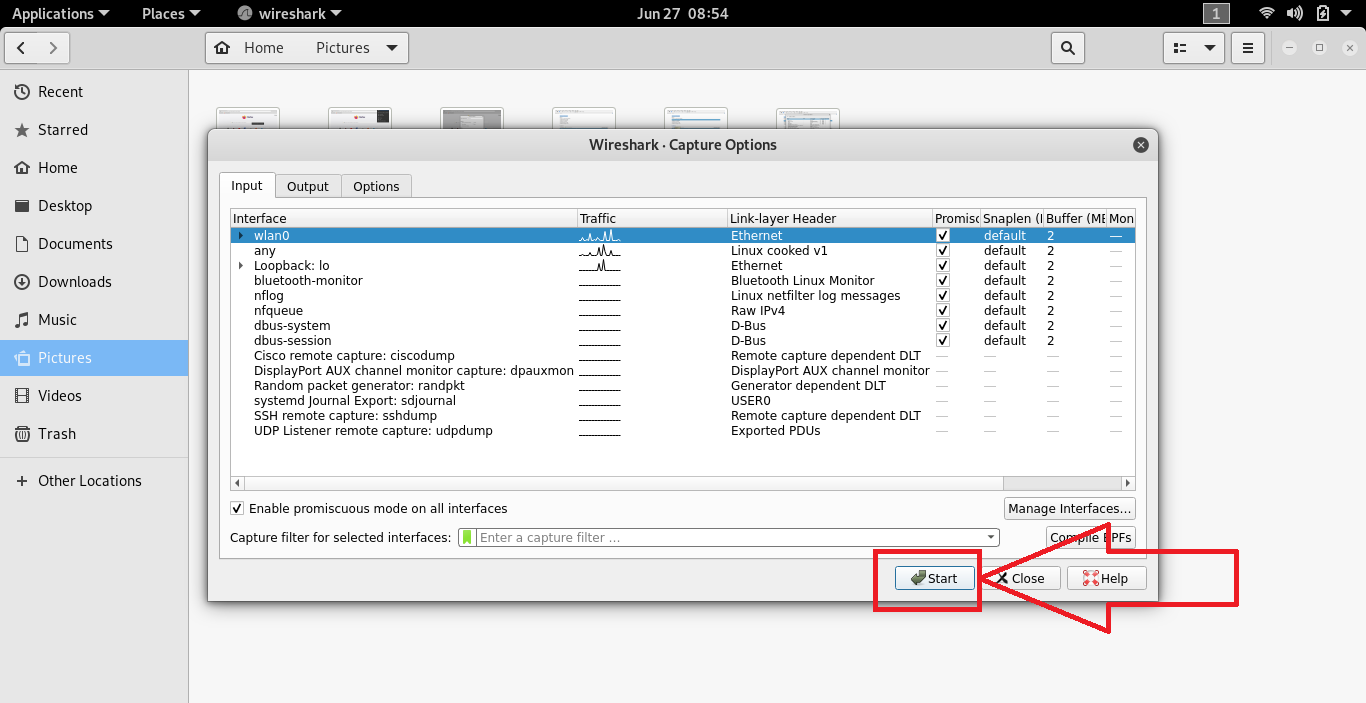
Click on capture btn to move ahead.

**NOTE -: You can use most of the default values in this window. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull down menu at the top of the Capture Options window. In case your computer has more than one active network interface (e.g., if you have both a wireless and a wired Ethernet connection), you will need to select an interface that is being used to send and receive packets (mostly likely the wired interface). After selecting the network interface (or using the default interface chosen by Wireshark), click Start. Packet capture will now begin - all live packets being sent/received from/by your computer are now being captured by Wireshark!**

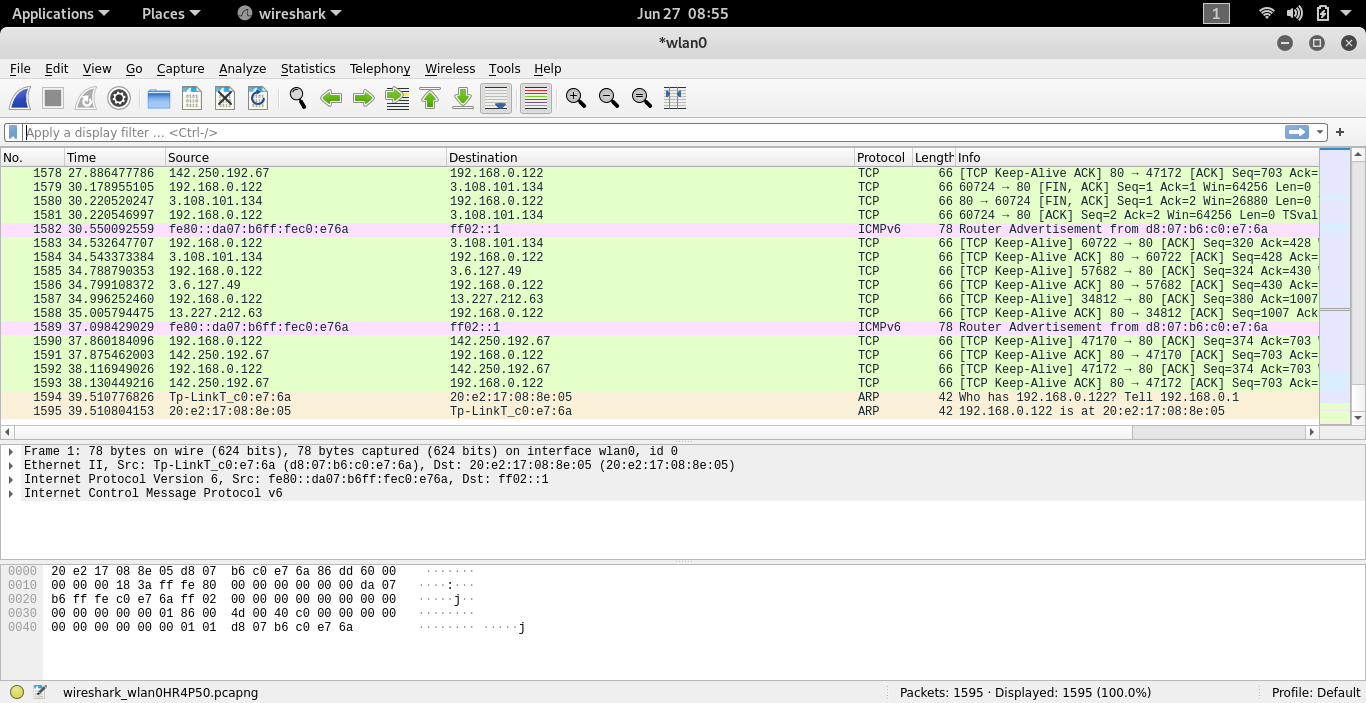
1. **Once you begin packet capture, a packet capture summary window will appear. This window summarizes the number of packets of various types that are being captured, and (importantly!) contains the Stop button that will allow you to stop packet capture. Don’t stop packet capture yet**

****

Select your wireless interface in my case I have a wlan0 wireless interface which is connected with another wireless card adapter…



Click on start



After click on start button your packets start capture like this

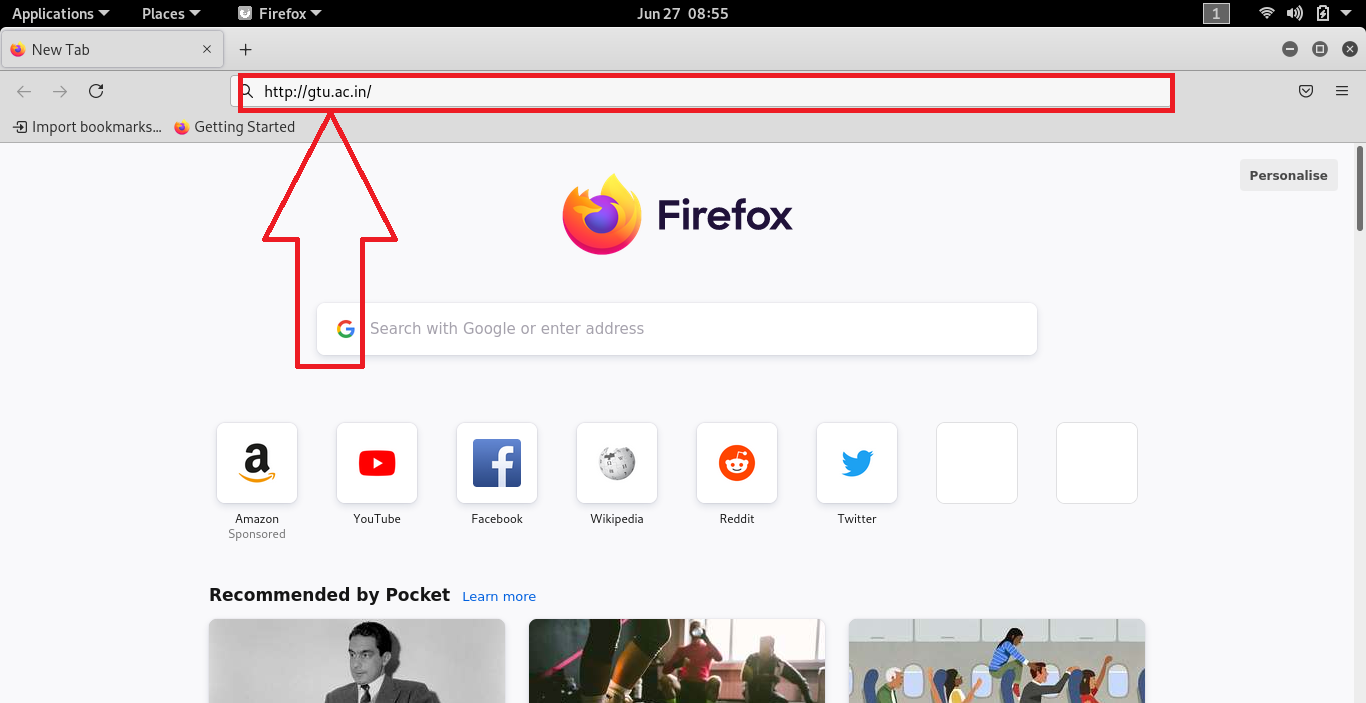
This section divide into three category

1)**Packet List Pane 🡪** The first pane displays a list containing packets in the current capture file. Its displayed as a table and the columns contain: the packet number, the time captured, packet source and destination, packet’s protocol, and some general information found in the packet.

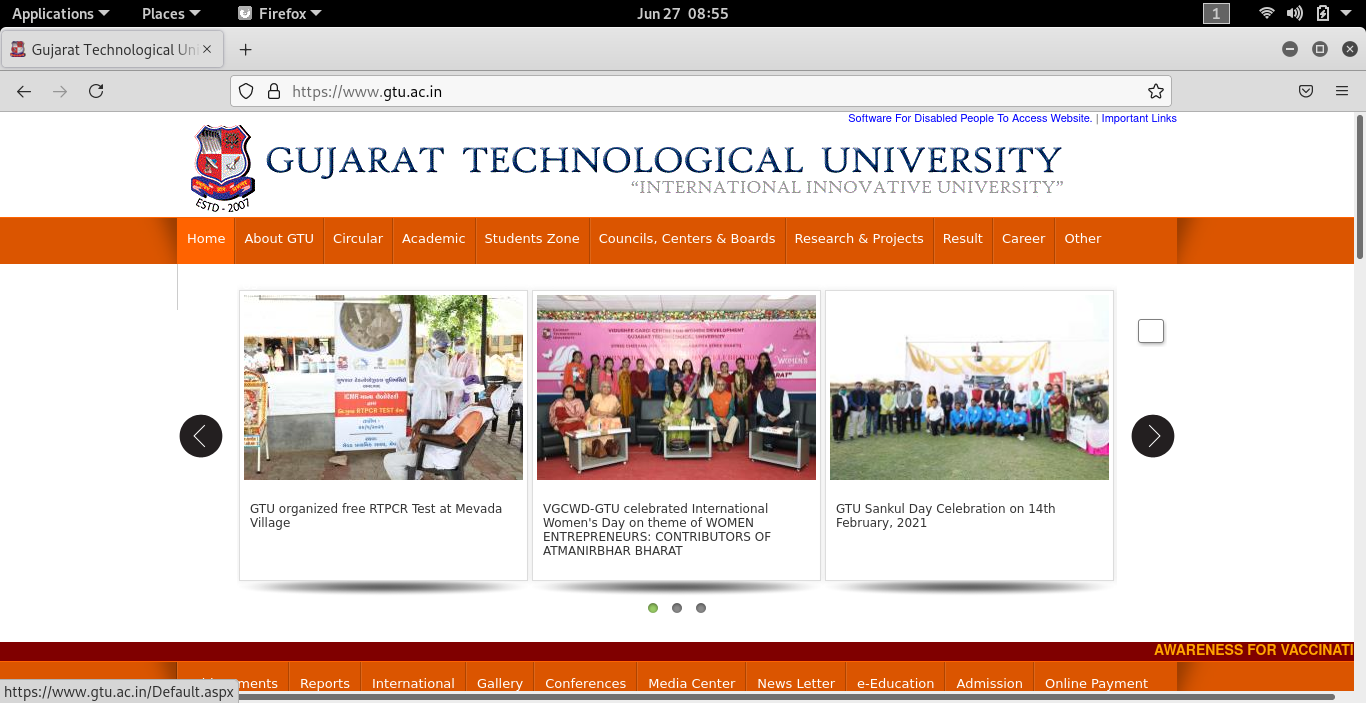
2) **Packet Details Pane 🡪** The second pane contains a hierarchical display of information about a single packet. Click the “collapsed and expanded” to show all of the information collected about an individual packet.

3) **Packet Bytes Pane 🡪** The third pane contain encoded packet data, displays a packet in its raw, unprocessed form.

1. **While Wireshark is running, enter the URL:** [**http://gtu.ac.in**](http://gtu.ac.in)

****

Add <http://gtu.ac.in> url as shown in above image

****

Make sure interface of your url looklike this (Start or Index Page)

**10. After your browser has displayed the web page, stop Wireshark packet capture by**

**selecting stop in the Wireshark capture window. This will cause the Wireshark capture**

**window to disappear and the main Wireshark window to display all packets captured since**

**you began packet capture. You now have live packet data that contains all protocol**

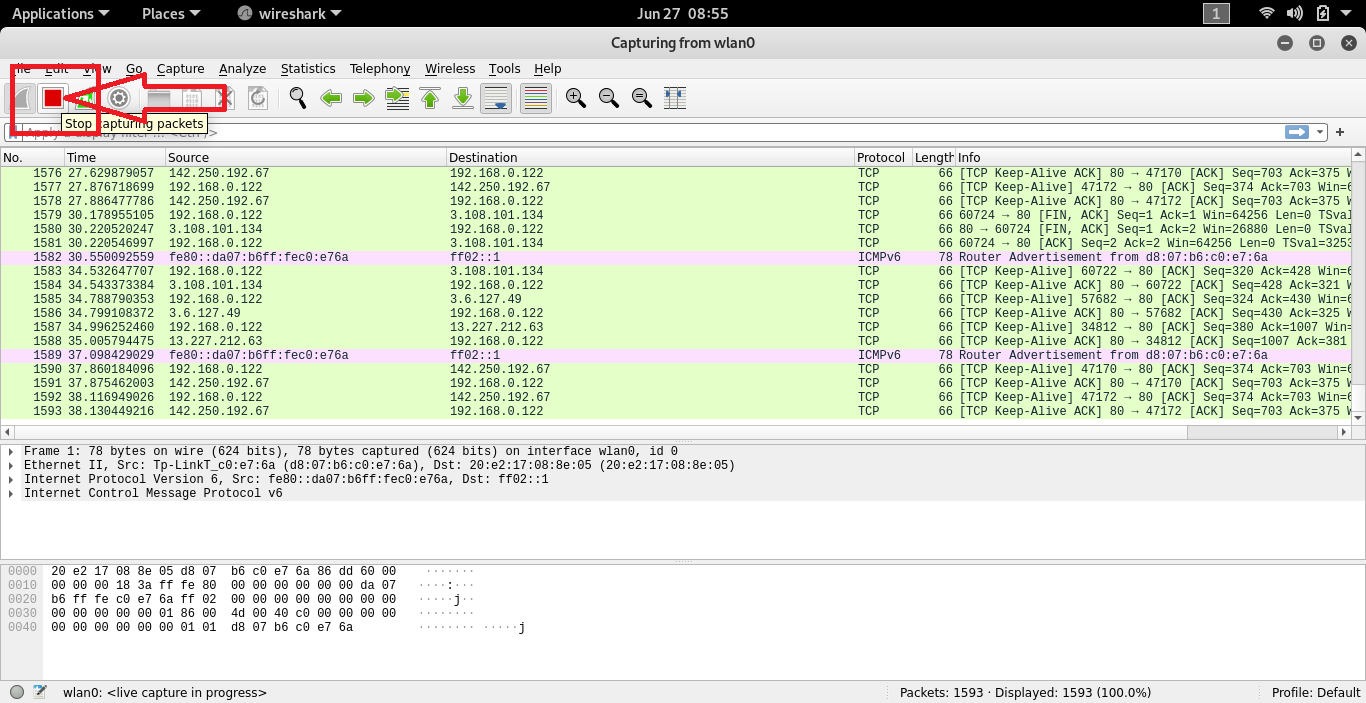
**messages exchanged between your computer and other network entities! The HTTP**

**message exchanges with the http://gtu.ac.in should appear somewhere in the listing of**

**packets captured. But there will be many other types of packets displayed as well. Even**

**though the only action you took was to download a web page, there were evidently many**

**other protocols running on your computer that are unseen by the user.**

****

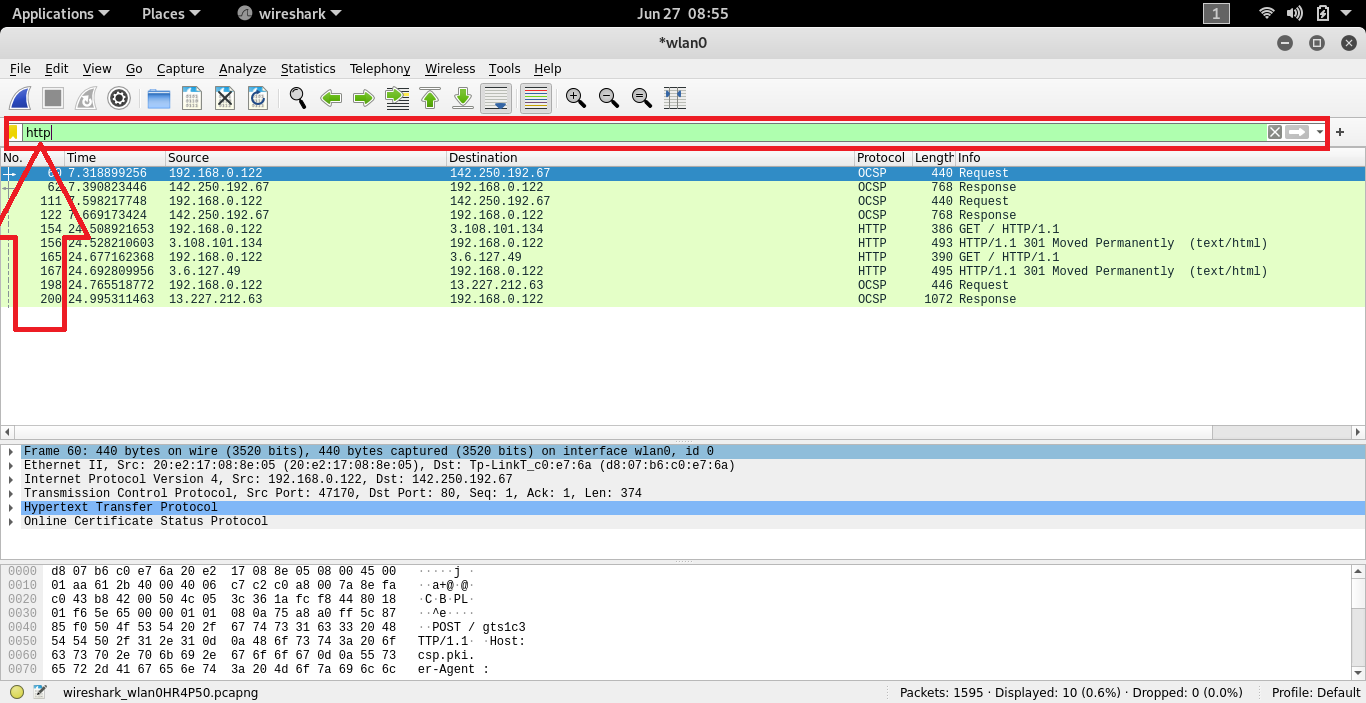
Click on stop btn

**11. Type in “http” (without the quotes, and in lower case – all protocol names are in lower**

**case in Wireshark) into the display filter specification window at the top of the main**

**Wireshark window. Then select Apply (to the right of where you entered “http”). This will**

**cause only HTTP message to be displayed in the packet-listing window.**

****

Enter http protocol in apply filter section

**13. Type in http into the display filter, select “Apply” in the filter toolbar. This will cause**

**only HTTP message to be displayed in the packet-listing window. Add the filter ip.src ==**

**<your IP address> || ip.dst == <your IP address> to filter out traffic that isn’t going to or**

**from your computer. This will keep other people’s traffic private and get rid of lots of HTTP**

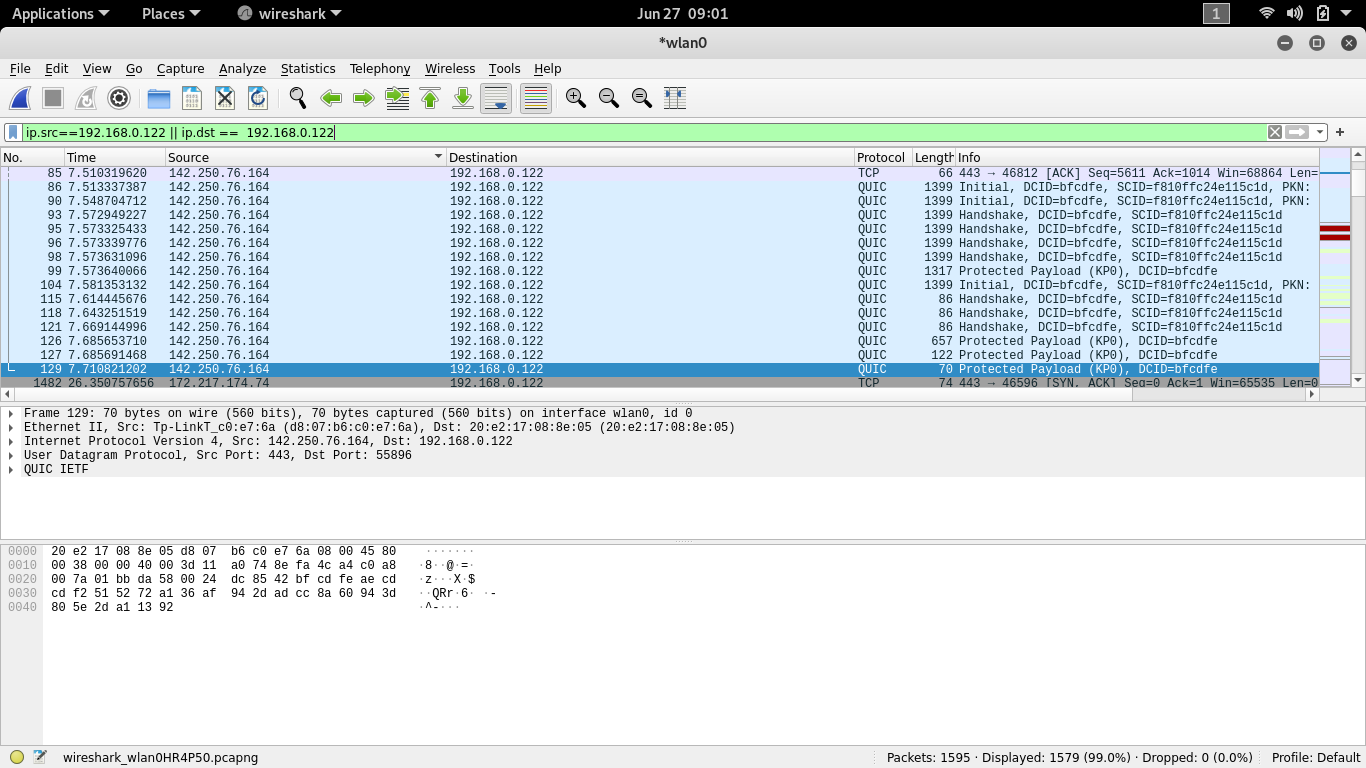
**exchanges from other computers that you don’t care about. Filters are combined with C**

**operators. For example, if your IP address is 169.1.19.87, then your filter should be http**

**&& (ip.src == 169.1.19.87 || ip.dst == 169.1.19.87). You can also use a more English-like**

**term to describe the same operators. For instance, ip.src eq 169.1.19.87 or ip.dst eq**

**169.1.19.87.**

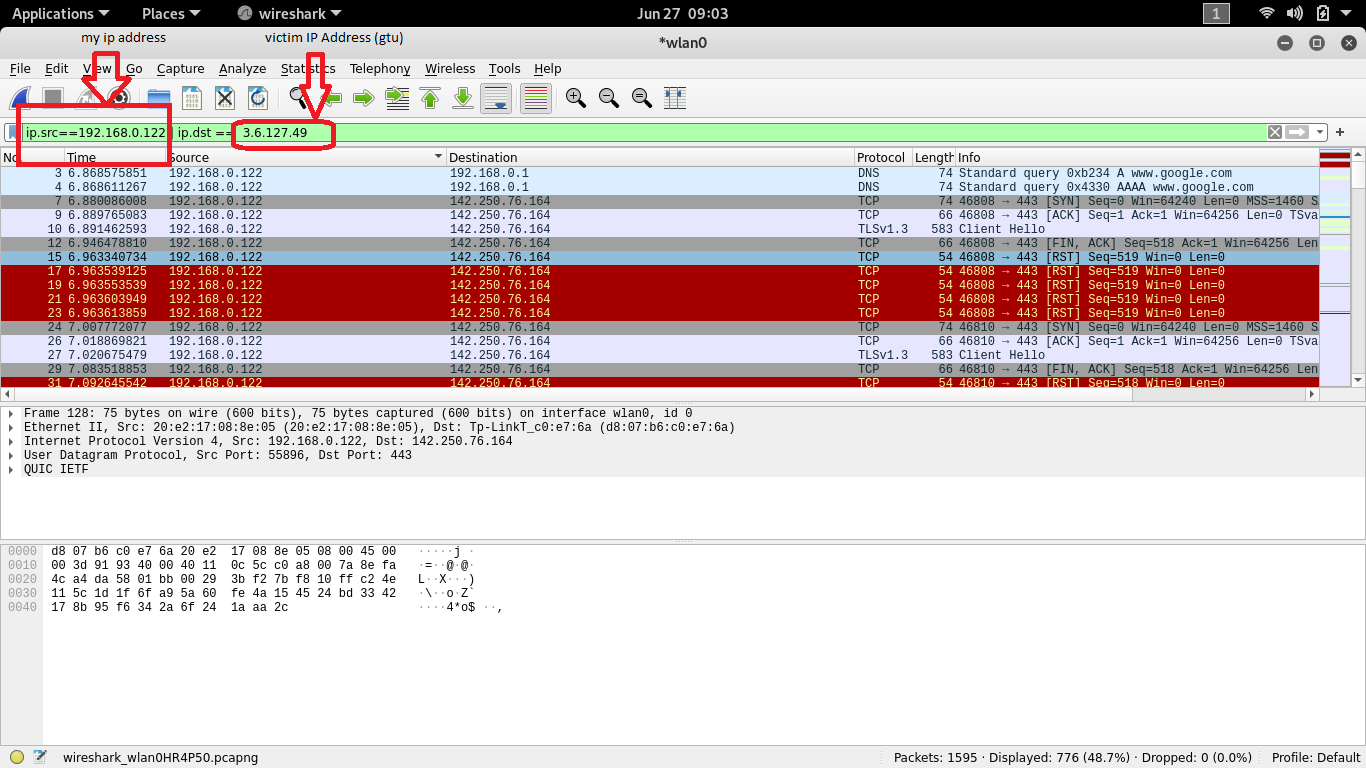
****

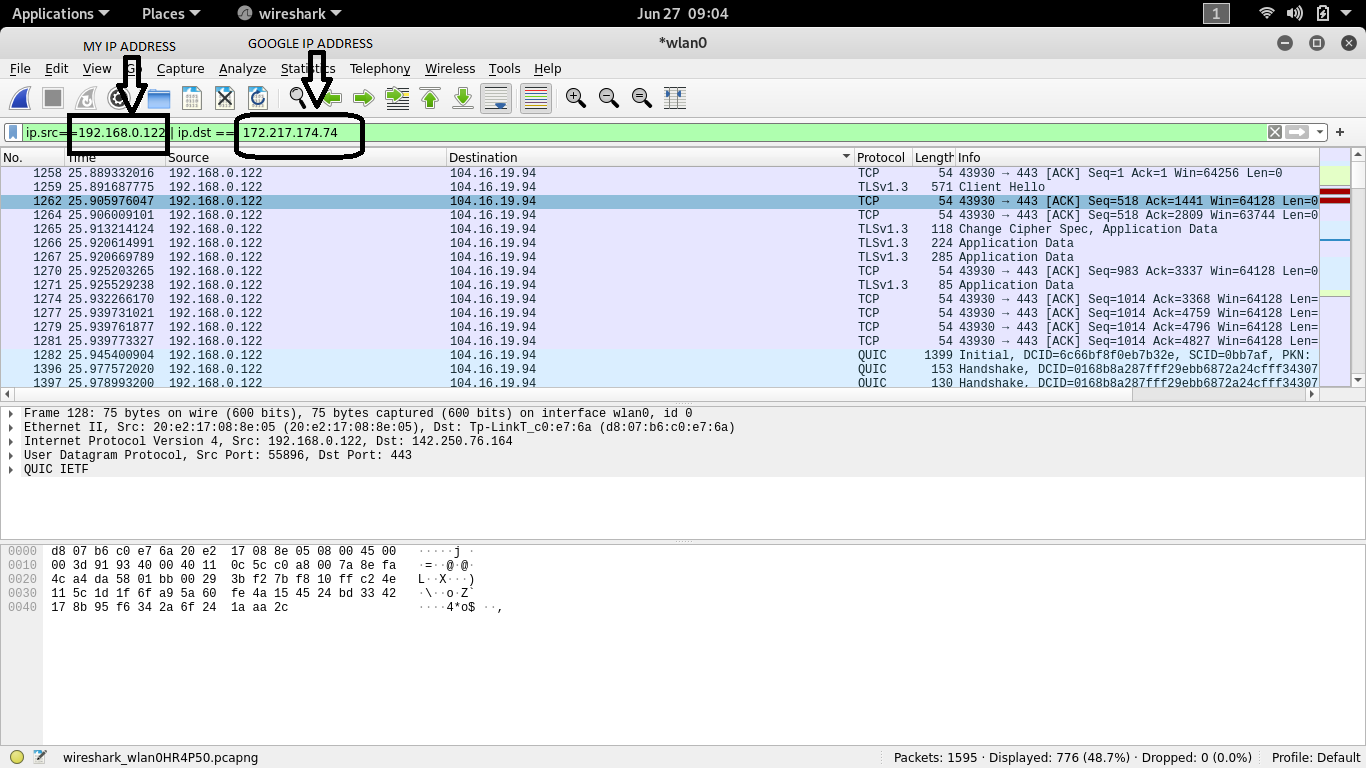
Above image shows that packet receive between my SOURCE IP and my destination iP

Here 192.168.0.172 is my IP

To hold the packets of this ip simply u can type ip.src == 192.168.0.122

**This all about my machine IP. using wireshark you can get the packets of victim’s website or something else….look at below image**

****

****Above image shows received packets between my ip and google ip

**14. The capture time of each packet is quite important, so is displayed in the packet listing**

**area as the second column. By default, this time is "number of seconds since the**

**beginning of capture." However, you have control over what is displayed. Explore the View**

**➙Time Display Format menu to see display formats as well as precision choices. Also of**

**interest is the ability to change the time reference so that all times are displayed relative**

**to the capture time of a chosen packet. First, chose a packet from the display list by**

**clicking on it. Then, go to the Edit ➙ Set/Unset Time Reference, which will toggle your**

**choice to use the chosen packet as the reference. When set, you will see the time for that**

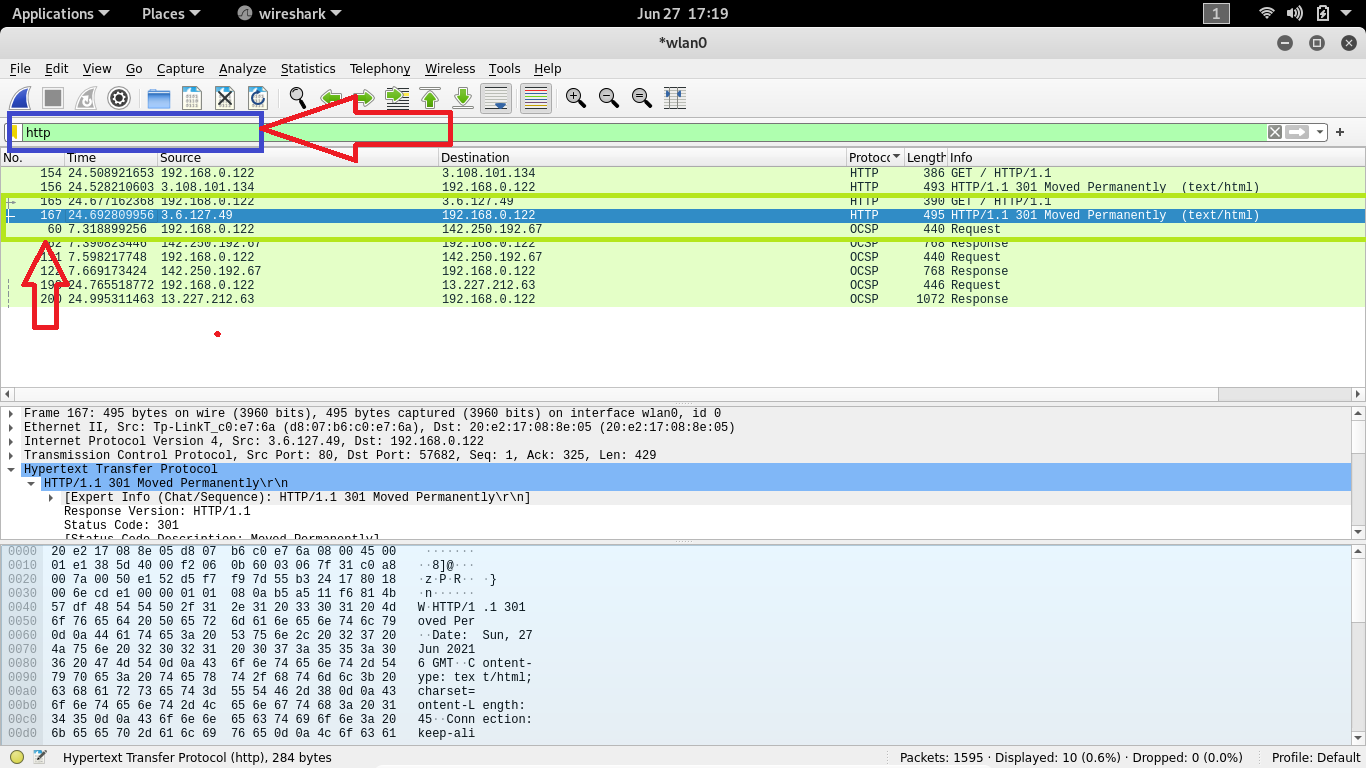
**packet changed to "\*REF\*" All other packet's time has been changed to seconds before**

**or after the capture of that reference packet. This is a particularly handy way to figure out**

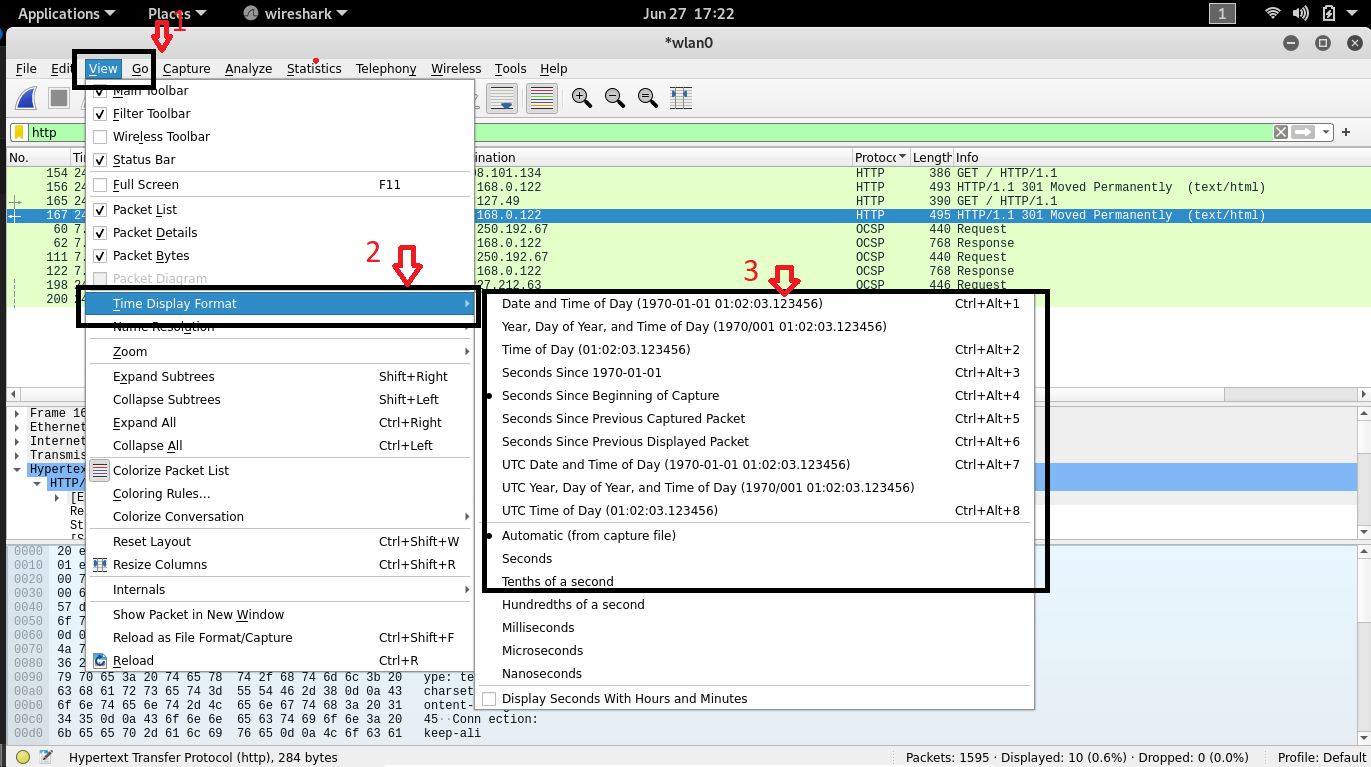
**round-trip-time. Set the request packet as the reference, then find the reply packet. The**

**time given on that packet will be the number of seconds it took from the request packet**

**for it to arrive. No arithmetic necessary!**

****

First filter the http protocol then select target victim as your source ip and then clicn on it(only single click)

****

After click on it Go to View menu then after select Time Display Format and choose as per requirement