St. Francis Institute of Technology
Department of Computer Engineering

COMPUTER NETWORK LAB

EXPERIMENT NO.5

AIM: Use Wire shark to understand the operation of TCP/IP layers:

- Ethernet Layer: Frame header, Frame size etc.
- Data Link Layer: MAC address, ARP (IP and MAC address binding)
- Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo)
- Transport Layer: TCP Ports, TCP handshake segments etc.

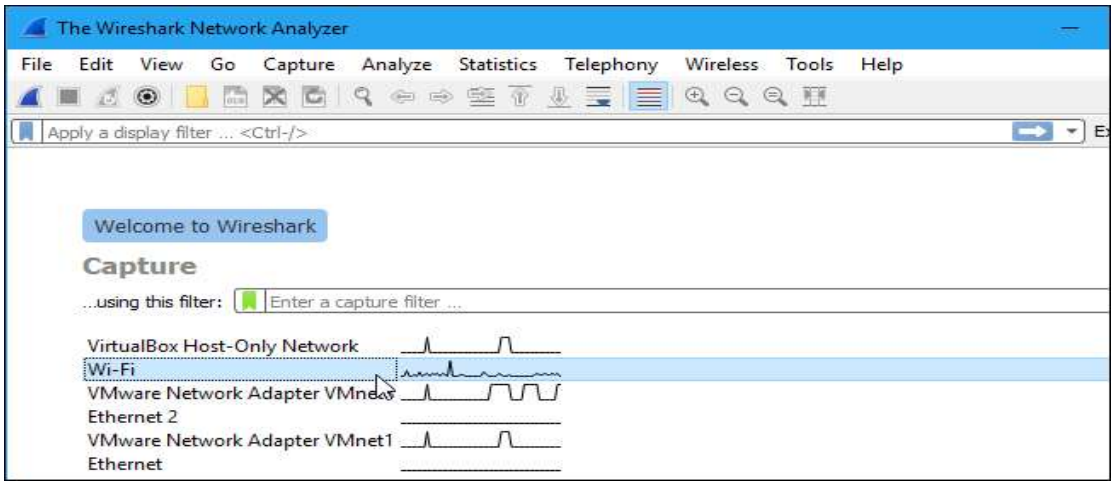
Application Layer: DHCP, FTP, HTTP header formats

THEORY:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

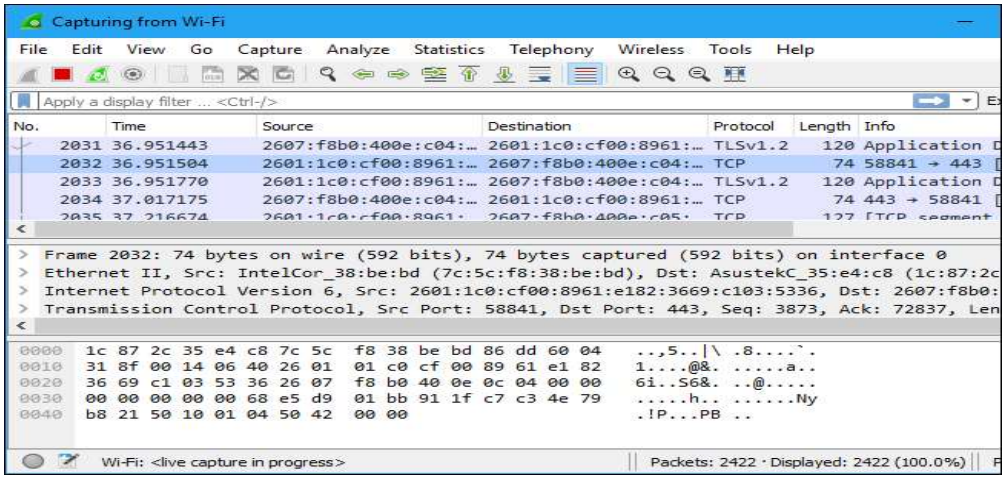
Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.

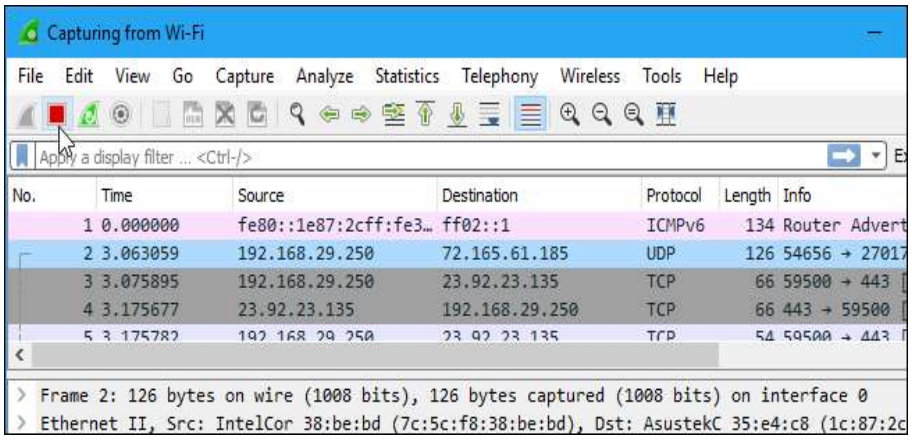


As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



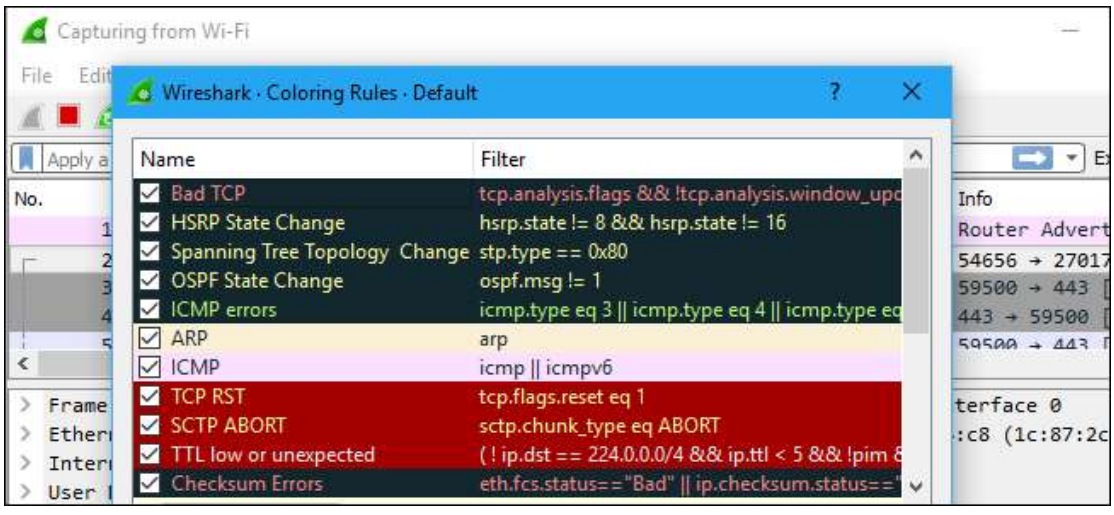
Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.



Color Coding

You’ll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

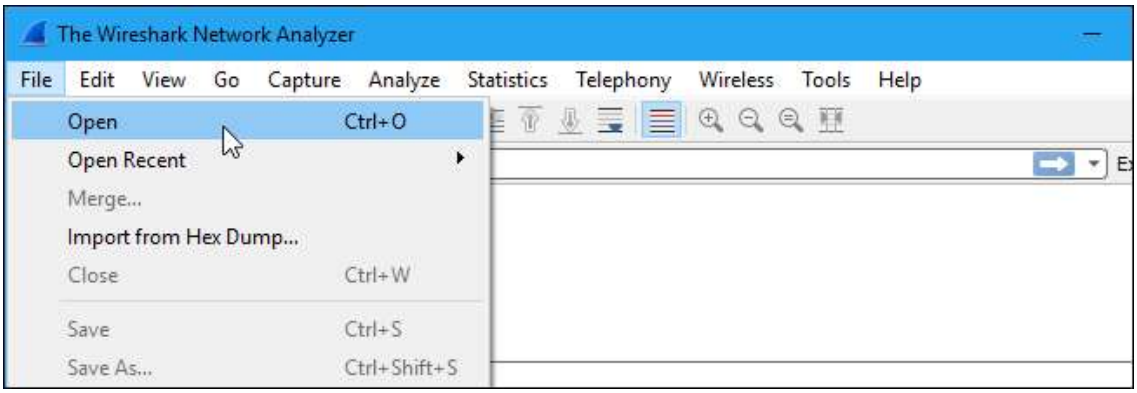
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

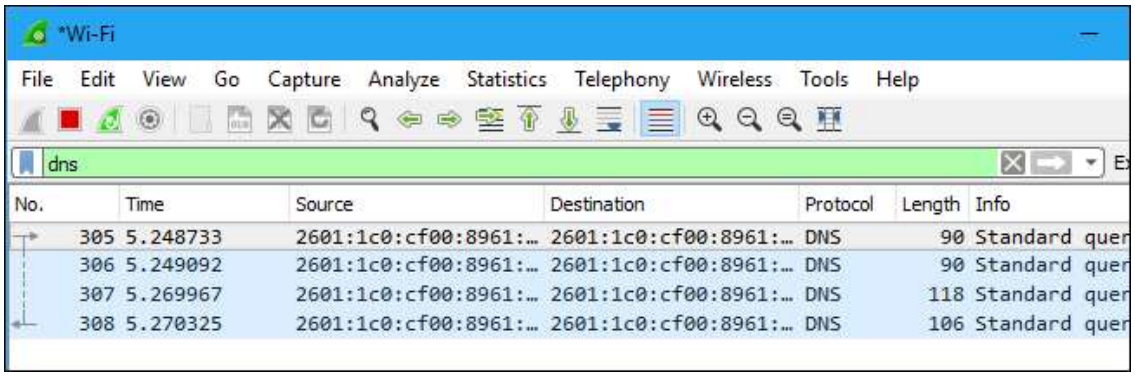
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



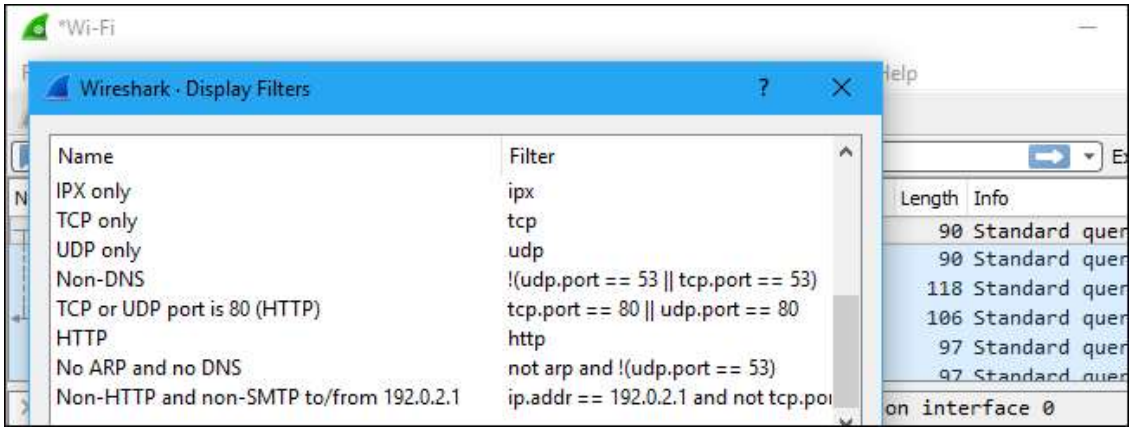
Filtering Packets

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.

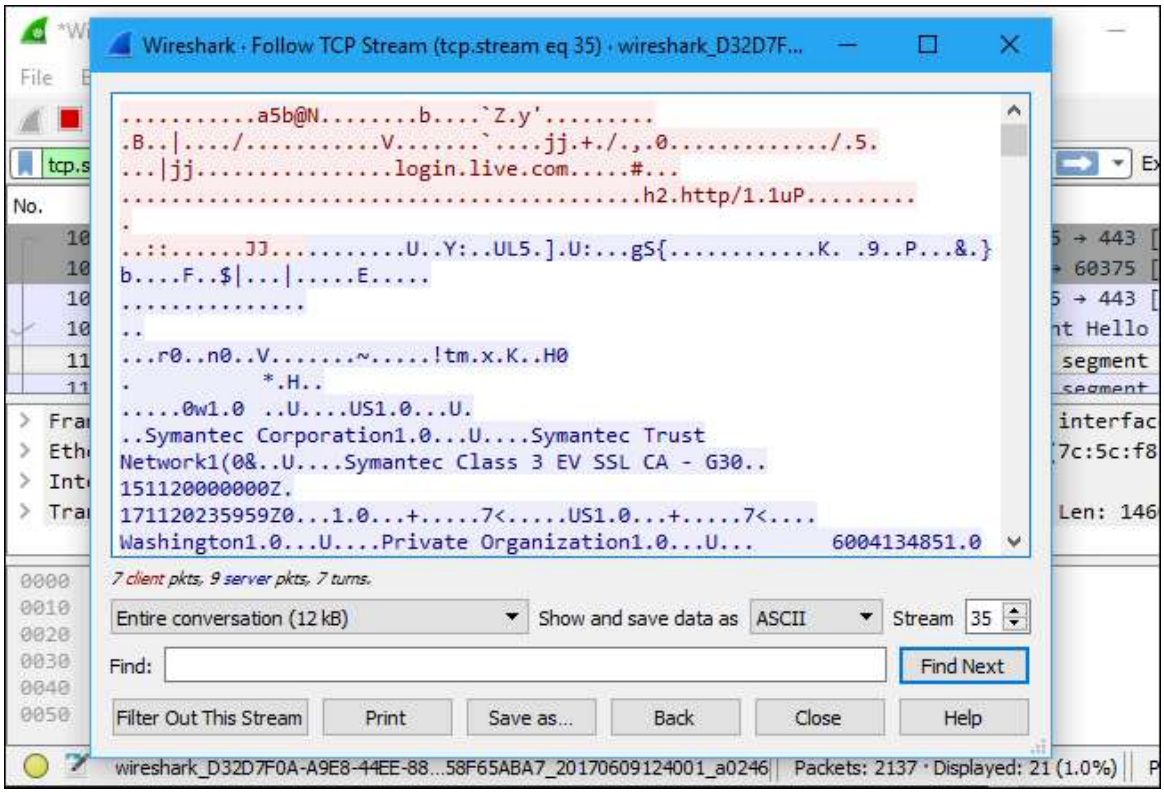


You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

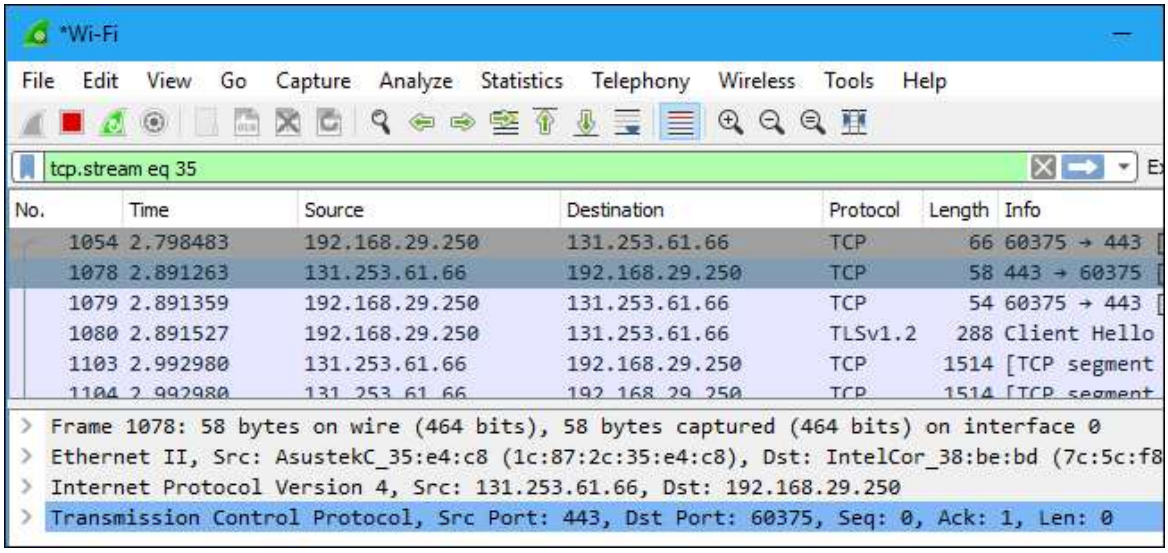


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

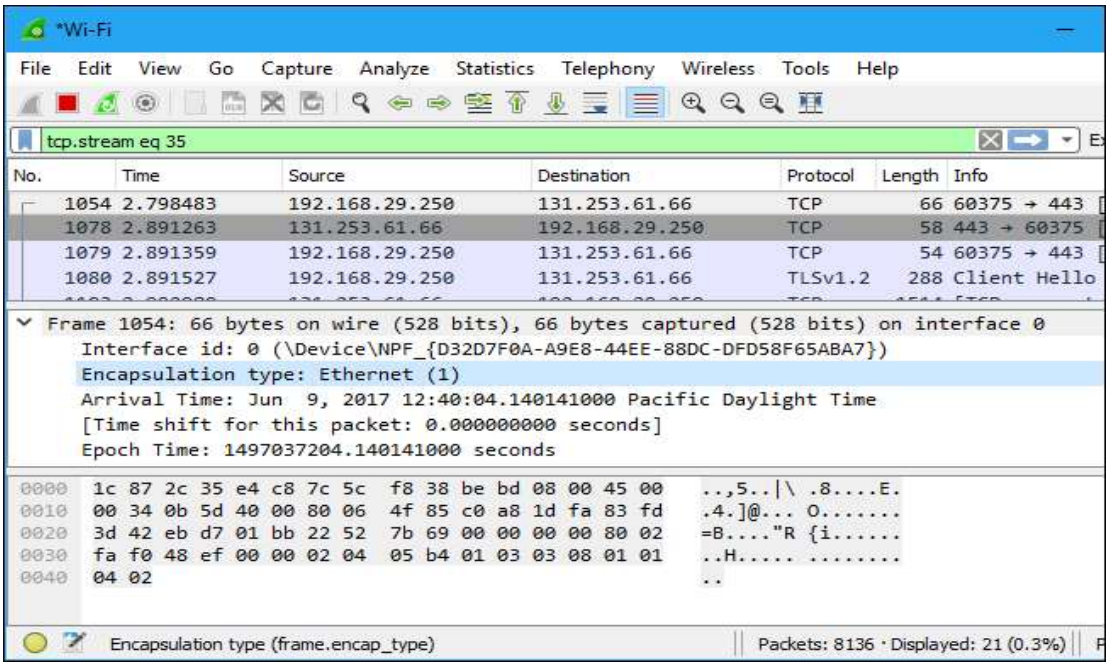


Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

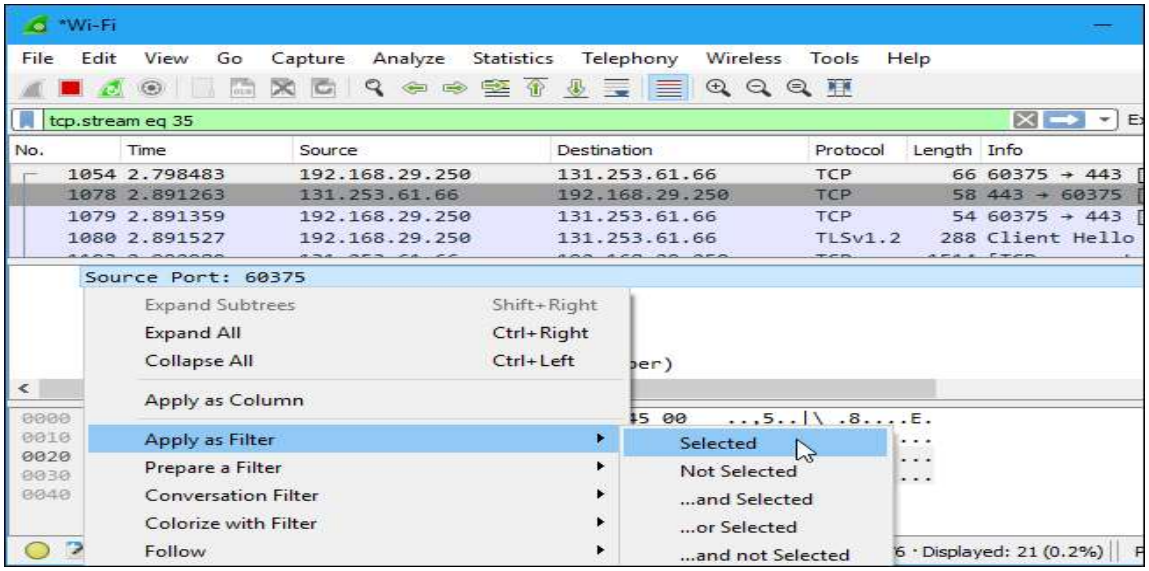


Inspecting Packets

Click a packet to select it and you can dig down to view its details.



You can also create filters from here hu— just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



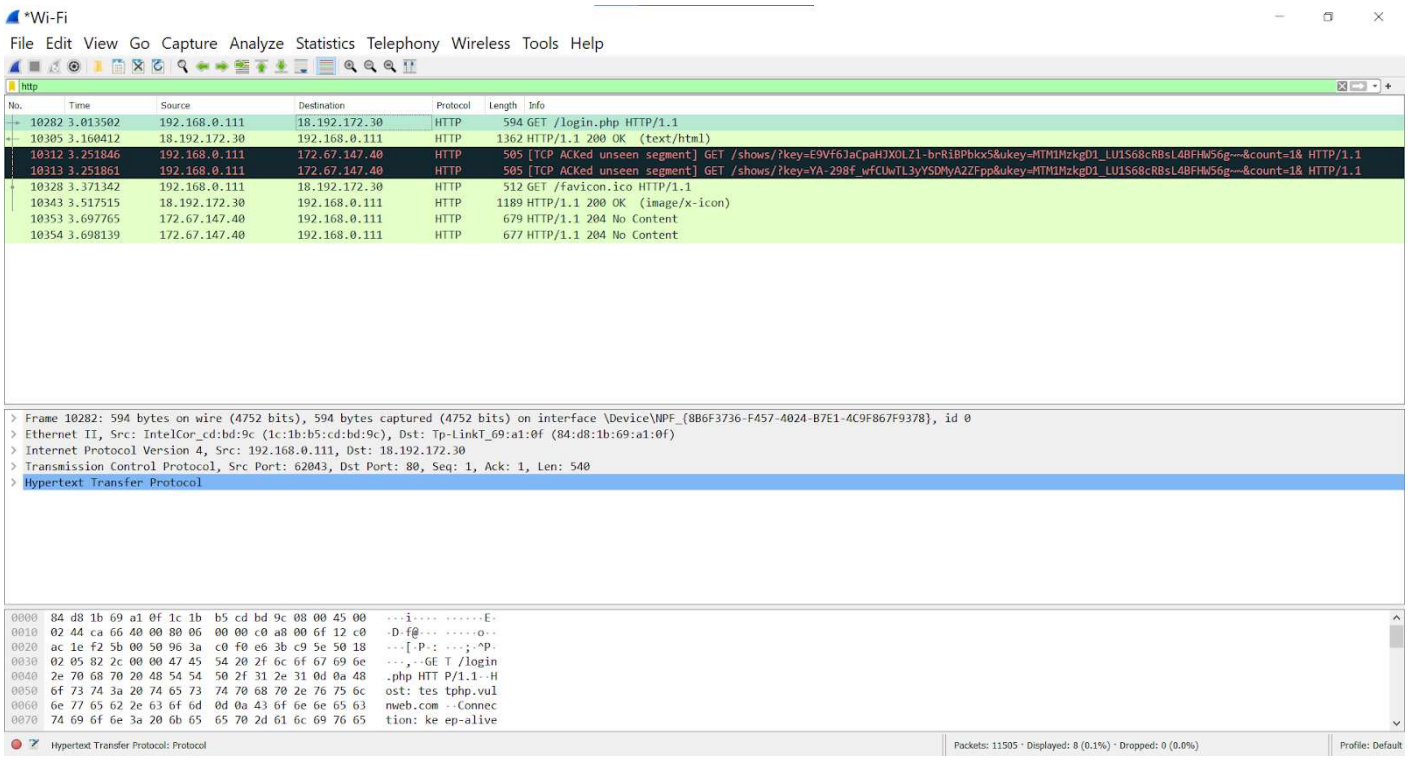
Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

INPUT and OUTPUT :- *(Apply all these filters and write the Steps and also paste Screen Shot)*

1. Which filter is used to check all incoming packets to HTTP web server?

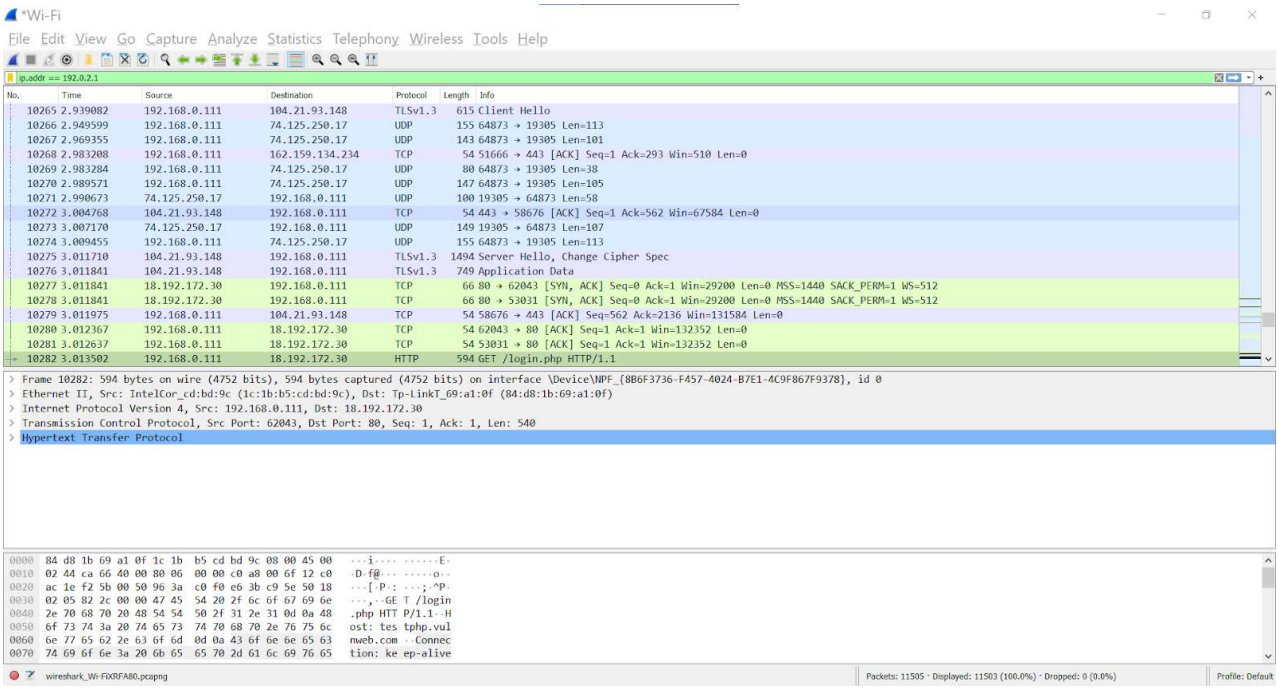
   Step1: click the interface's name, packets start to appear in real time

   Step2: To filter just type HTTP in the filter box at the top of the window and click Apply .



2. Which filter is used to monitor all outgoing packets from specific system on a network ?

ip.src==address



3. How to use wireshark to find password in any network.

HTTP typically runs on port 80/tcp and since it is a plain text protocol, it offers very little to no privacy to the communicating parties.Anybody who is in position to eavesdrop on the communication can capture everything over this channel, including password.Even though there has been a tremendous effort done by all major browser vendors to discourage usage of HTTP as much as possible, we can still see HTTP being used on internal networks during penetration tests. Here's an example of login credentials captured in a HTTP communication in a POST request

step1:Go to http website and try to login

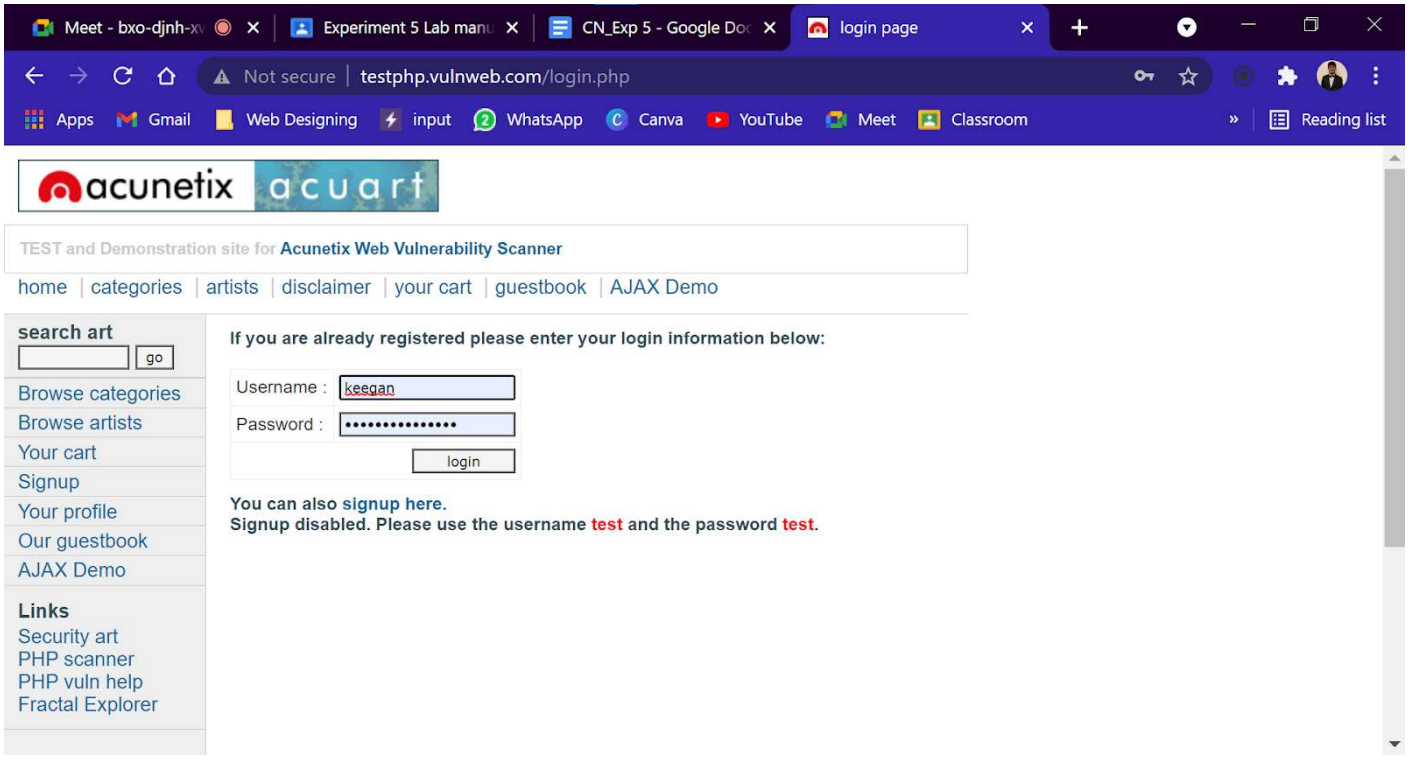
step2:Open wireshark and type http in the filter bar.

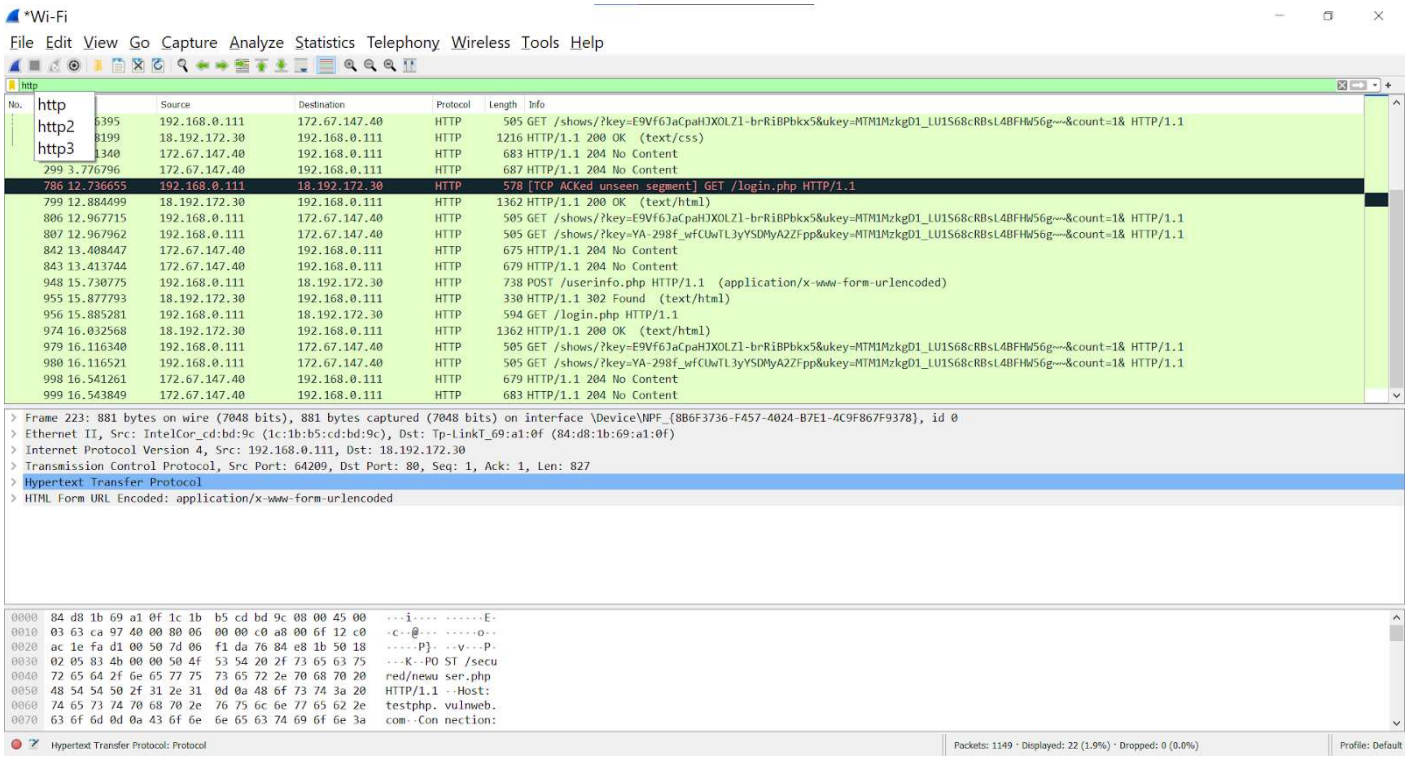
step3:Now try to login on http website .

step4:Capture the post request in wireshark.

step5:click on it you will see the password you entered.

Name:Keegan Vaz TE CMPN B RollNo.:28 PID:192120





```
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 2/3]
    [Prev request in frame: 786]
    [Response in frame: 955]
    [Next request in frame: 956]
    File Data: 35 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "keegan"
  › Form item: "pass" = "Y9A3xEiqXFpwh4@"
```

4. Explain wireshark coloring rules

There are two types of coloring rules in Wireshark: temporary rules that are only in effect until you quit the program, and permanent rules that are saved in a preference file so that they are available the next time you run Wireshark. Temporary rules can be added by selecting a packet and pressing the **Ctrl** key together with one of the number keys. This will create a coloring rule based on the currently selected conversation. It will try to create a conversation filter based on TCP first, then UDP, then IP and at last Ethernet. Temporary filters can also be created by selecting the Colorize with Filter → Color X menu items when right-clicking in the packet detail pane.

CONCLUSION: Thus, we have studied the working of Wire Shark Packet Capture.