NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

LAB 08

LAB 08: Study of packet sniffer tools Wireshark:

a. Observer performance in promiscuous and non-promiscuous modes.
b. Show the packets can be traced based on different filters.

ROLL NO	52
NAME	Sarvesh Patil
CLASS	D15A
SUBJECT	Internet Security Lab
LO MAPPED	LO3: Explore the different network reconnaissance tools to gather information about networks

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

AIM:

Study of packet sniffer tools Wireshark:

a. Observer performance in promiscuous and non-promiscuous modes.
b. Show the packets can be traced based on different filters.

INTRODUCTION:

What Is Wireshark and How Is It Used?

What-Is-WiresharkFew tools are as useful to the IT professional as Wireshark, the go-to network packet capture tool. Wireshark will help you capture network packets and display them at a granular level. Once these packets are broken down, you can use them for real-time or offline analysis. This tool lets you put your network traffic under a microscope, and then filter and drill down into it, zooming in on the root cause of problems, assisting with network analysis and ultimately network security. This free Wireshark tutorial will teach you how to capture, interpret, filter, and inspect data packets to effectively troubleshoot.

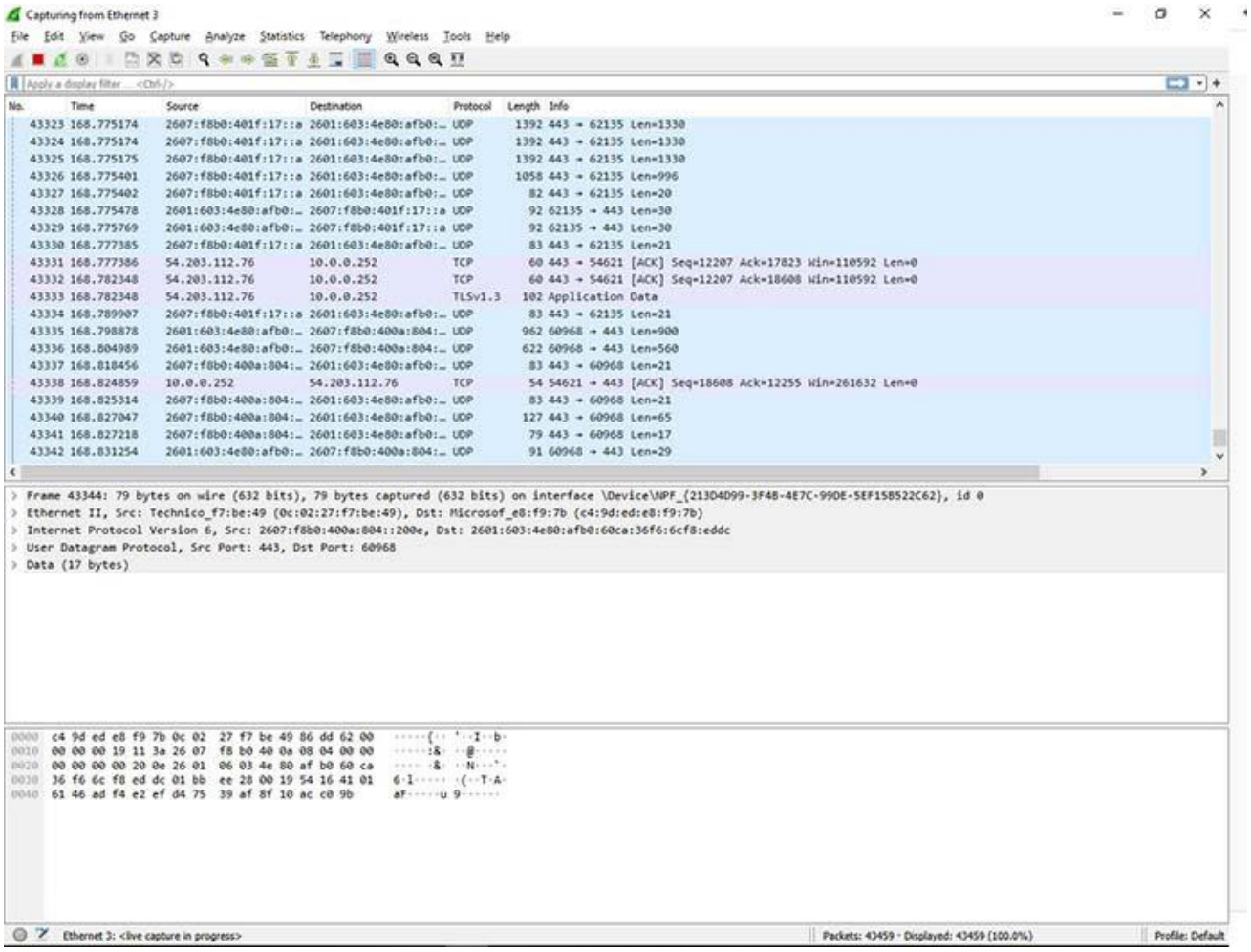
What Is Wireshark?

Wireshark is a network protocol analyzer or an application that captures packets from a network connection, such as from your computer to your home office or the internet. The packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. Packet Capture: Wireshark listens to a network connection in real-time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. Filtering: Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. Visualization: Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52



Packet sniffing can be compared to spelunking – going inside a cave and hiking around. Folks who use Wireshark on a network are kind of like those who use flashlights to see what cool things they can find. After all, when using Wireshark on a network connection (or a flashlight in a cave), you're effectively using a tool to hunt around tunnels and tubes to see what you can see.

What Is Wireshark Used For?
Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions, and identify bursts of network traffic. It's a major part of any IT pro's toolkit – and hopefully, the IT pro has the knowledge to use it.

When Should Wireshark Be Used?
Wireshark is a safe tool used by government agencies, educational institutions, corporations, small businesses, and nonprofits alike to troubleshoot network issues. Additionally, Wireshark can be used as a learning tool.

Those new to information security can use Wireshark as a tool to understand network traffic analysis, how communication takes place when particular protocols are involved and where it goes wrong when certain issues occur.

Of course, Wireshark can't do everything.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

First of all, it can't help a user who has little understanding of network protocols. No tool, no matter how cool, replaces knowledge very well. In other words, to properly use Wireshark, you need to learn exactly how a network operates. That means you need to understand things such as the three-way TCP handshake and various protocols, including TCP, UDP, DHCP, and ICMP.

Second, Wireshark can't grab traffic from all of the other systems on the network under normal circumstances. On modern networks that use devices called switches, Wireshark (or any other standard packet-capturing tool) can only sniff traffic between your local computer and the remote system it is talking to.

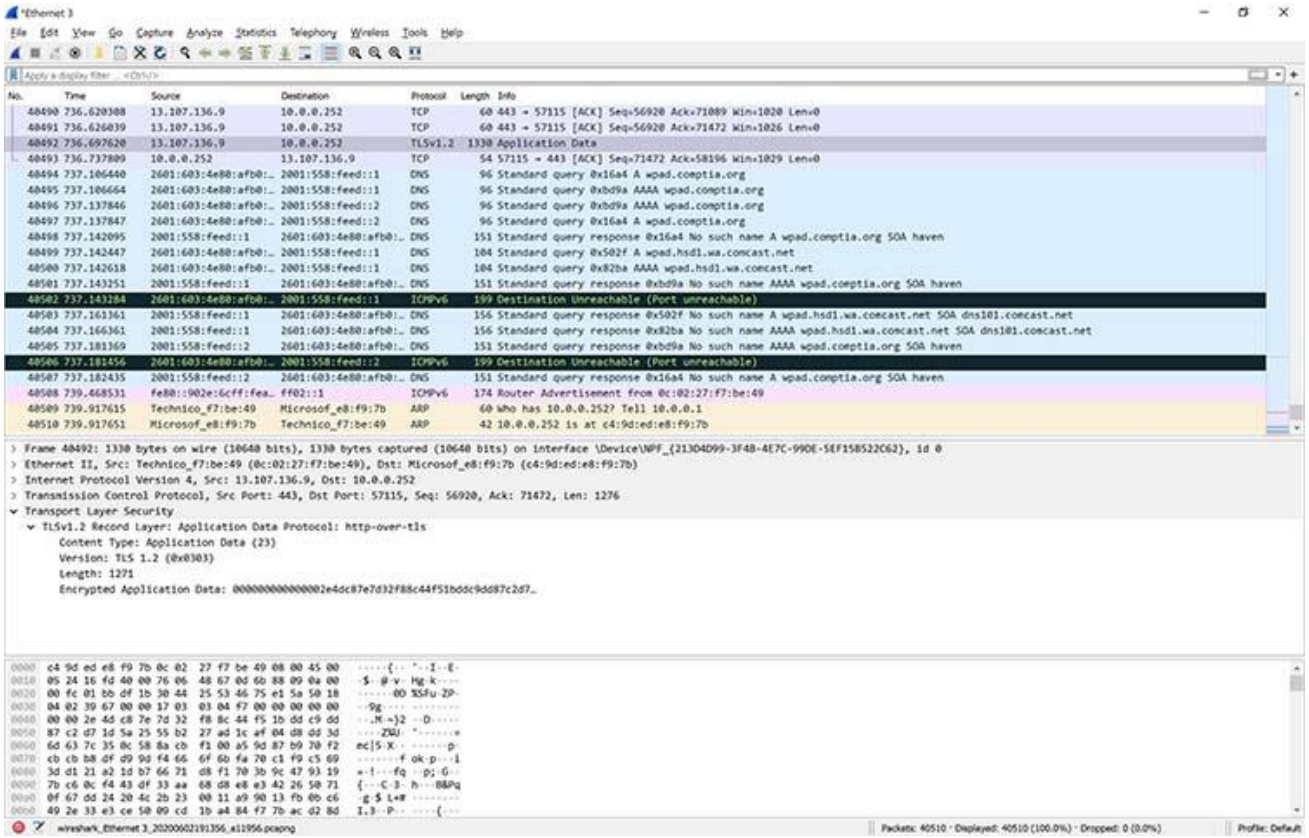
Third, while Wireshark can show malformed packets and apply color coding, it doesn't have actual alerts; Wireshark isn't an intrusion detection system (IDS).

Fourth, Wireshark can't help with decryption with regard to encrypted traffic.

And finally, it is quite easy to spoof IPv4 packets. Wireshark can't really tell you if a particular IP address it finds in a captured packet is a real one or not. That requires a bit more know-how on the part of an IT pro, as well as an additional software.

Common Wireshark Use Cases

Here's a common example of how a Wireshark capture can assist in identifying a problem. The figure below shows an issue on a home network, where the internet connection was very slow. As the figure shows, the router thought a common destination was unreachable. This was discovered by drilling down into the IPv6 Internet Message Control Protocol (ICMP) traffic, which is marked in black. In Wireshark, any packet marked in black is considered to reflect some sort of issue.



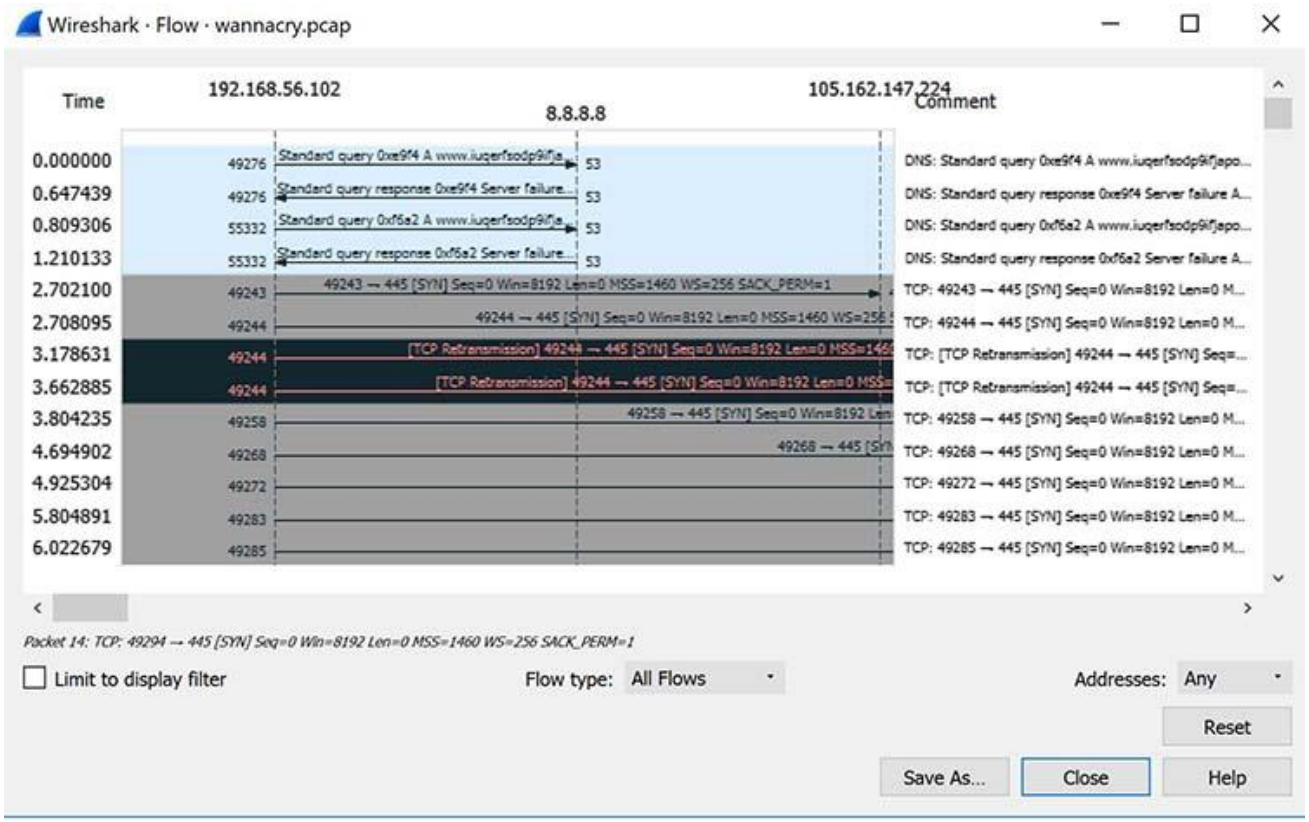
NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

In this case, Wireshark helped determine that the router wasn't working properly and couldn't find YouTube very easily. The problem was resolved by restarting the cable modem. Of course, while this particular problem didn't necessitate using Wireshark, it's kind of cool to authoritatively finalize the issue.

When you take another look at the bottom of Figure 2, you can see that a specific packet is highlighted. This shows the innards of a TCP packet that is part of a transport layer security (TLS) conversation. This is a great example of how you can drill down into the captured packet.

Using Wireshark doesn't allow you to read the encrypted contents of the packet, but you can identify the version of TLS the browser and YouTube are using to encrypt things. Interestingly enough, the encryption shifted to TLS version 1.2 during the listening.

Wireshark is often used to identify more complex network issues. For example, if a network experiences too many retransmissions, congestion can occur. By using Wireshark, you can identify specific retransmission issues, as shown below in Figure 3.



By confirming this type of issue, you can then reconfigure the router or switch to speed up traffic.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

How to Use Wireshark

You can download Wireshark for free at www.wireshark.org. It's also freely available, as an open source application under the GNU General Public License version 2.

How to Install Wireshark on Windows

If you're a Windows operating system user, download the version appropriate for your particular version. If you use Windows 10, for example, you'd grab the 64-bit Windows installer and follow the wizard to install. To install, you'll need administrator permissions.
How to Install Wireshark on Linux

If you have a Linux system, you'd install Wireshark using the following sequence (notice that you'll need to have root permissions):

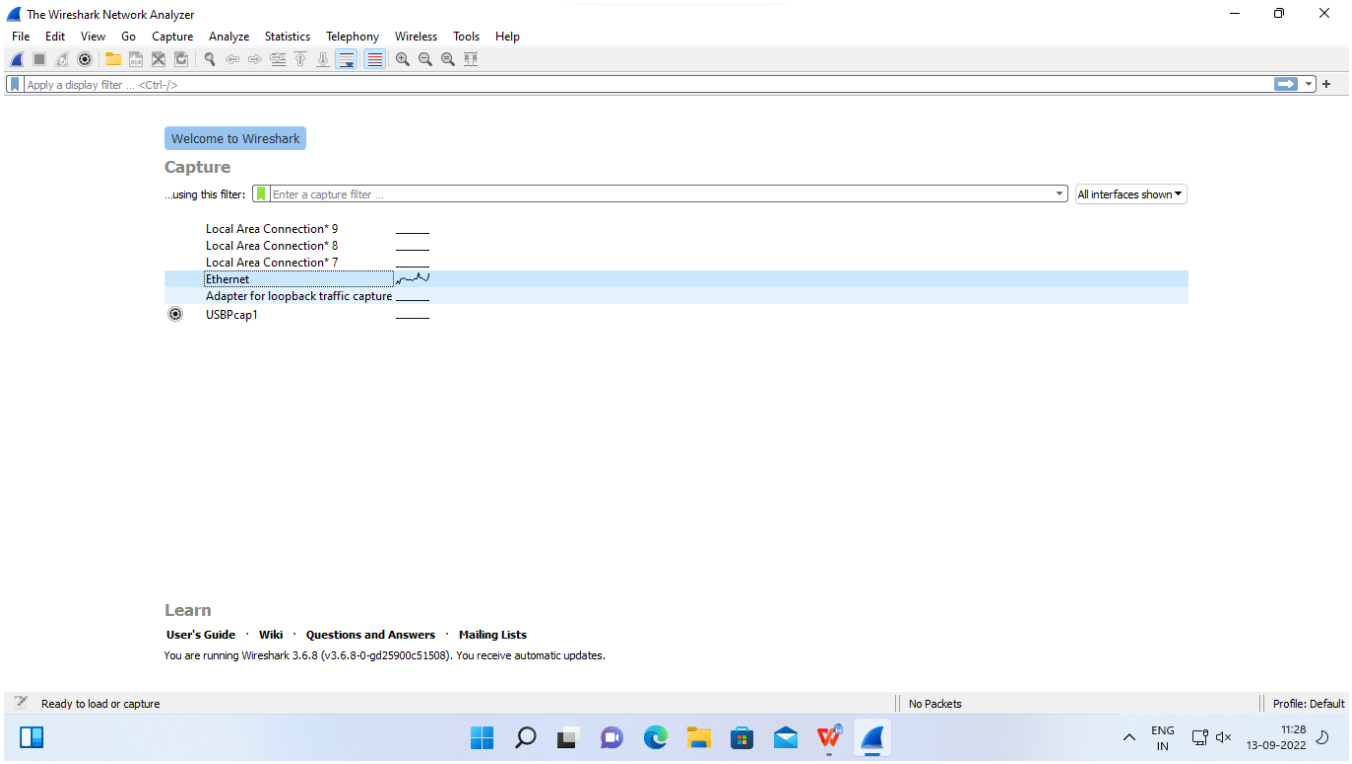
$ sudo apt-get install wireshark
$ sudo dpkg-reconfigure wireshark-common
$ sudo usermod -a -G wireshark $USER
$ newgrp wireshark

Once you have completed the above steps, you then log out and log back in, and then start Wireshark:
$ wireshark &

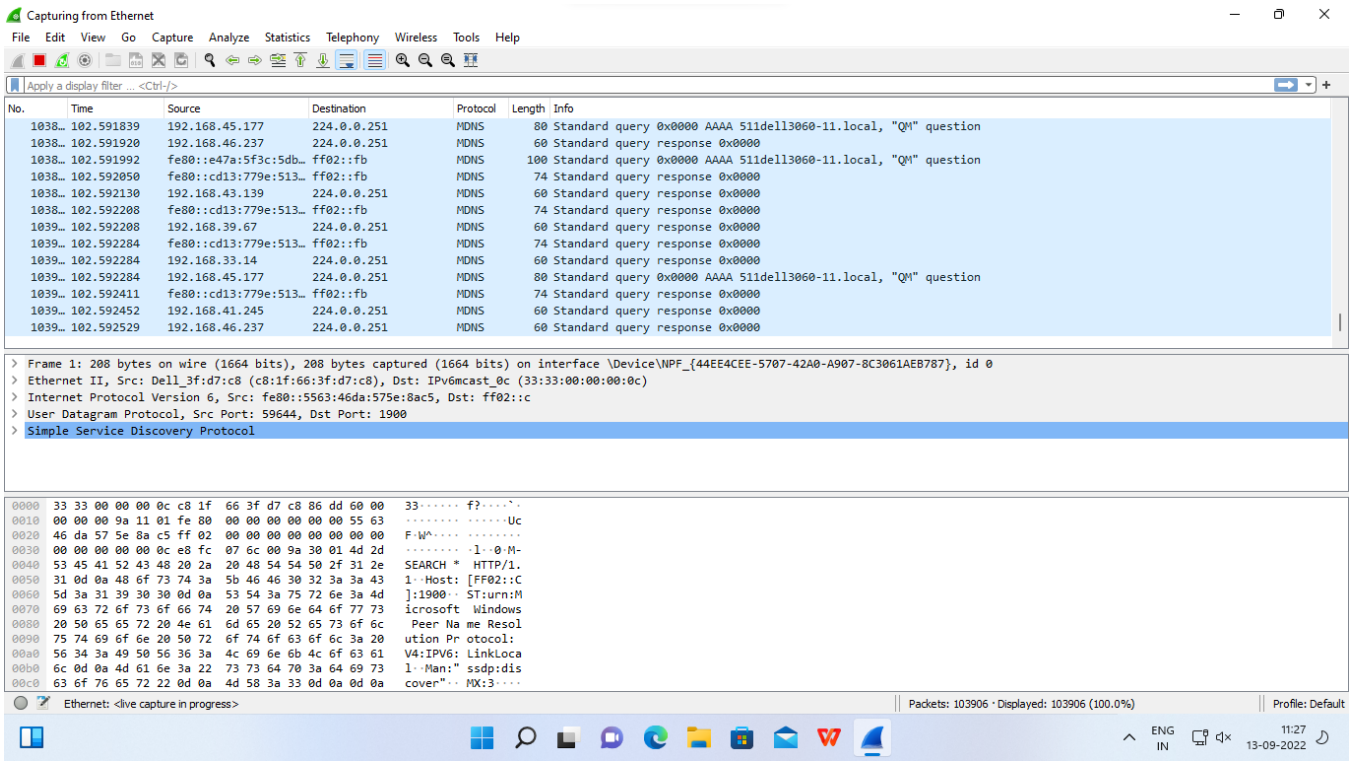
NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

SCREENSHOTS:

1. Select Capture >> Options from the main window.



2. This window will list all available interfaces. In this case, Wireshark provides several to choose from. For this example, we'll select the Ethernet 3 interface, which is the most active interface. Wireshark visualizes the traffic by showing a moving line, which represents the packets on the network.



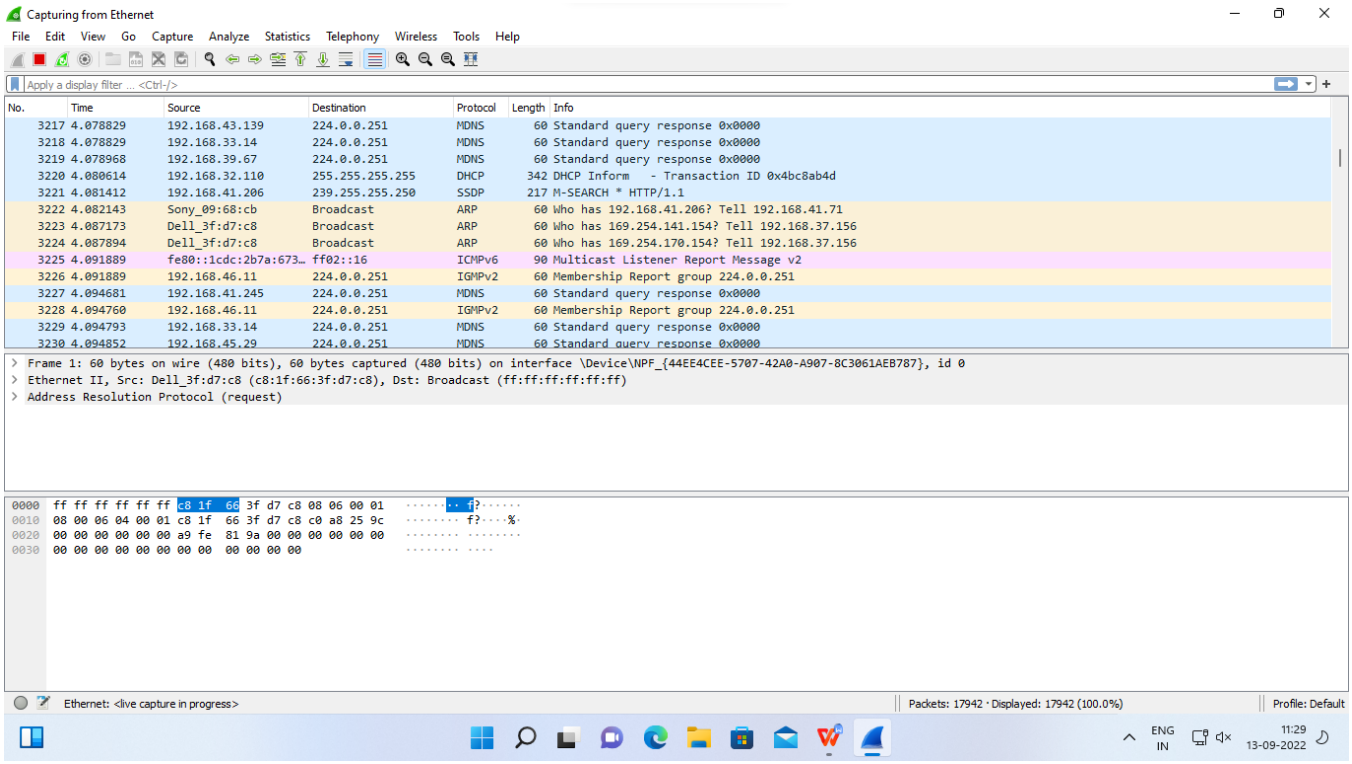
NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

3. Color coding in Wireshark

Color in Wireshark	Packet Type
Light purple	TCP
Light blue	UDP
Black	Packets with errors
Light green	HTTP traffic
Light yellow	Windows-specific traffic, including Server Message Blocks (SMB) and NetBIOS
Dark yellow	Routing
Dark gray	TCP SYN, FIN and ACK traffic

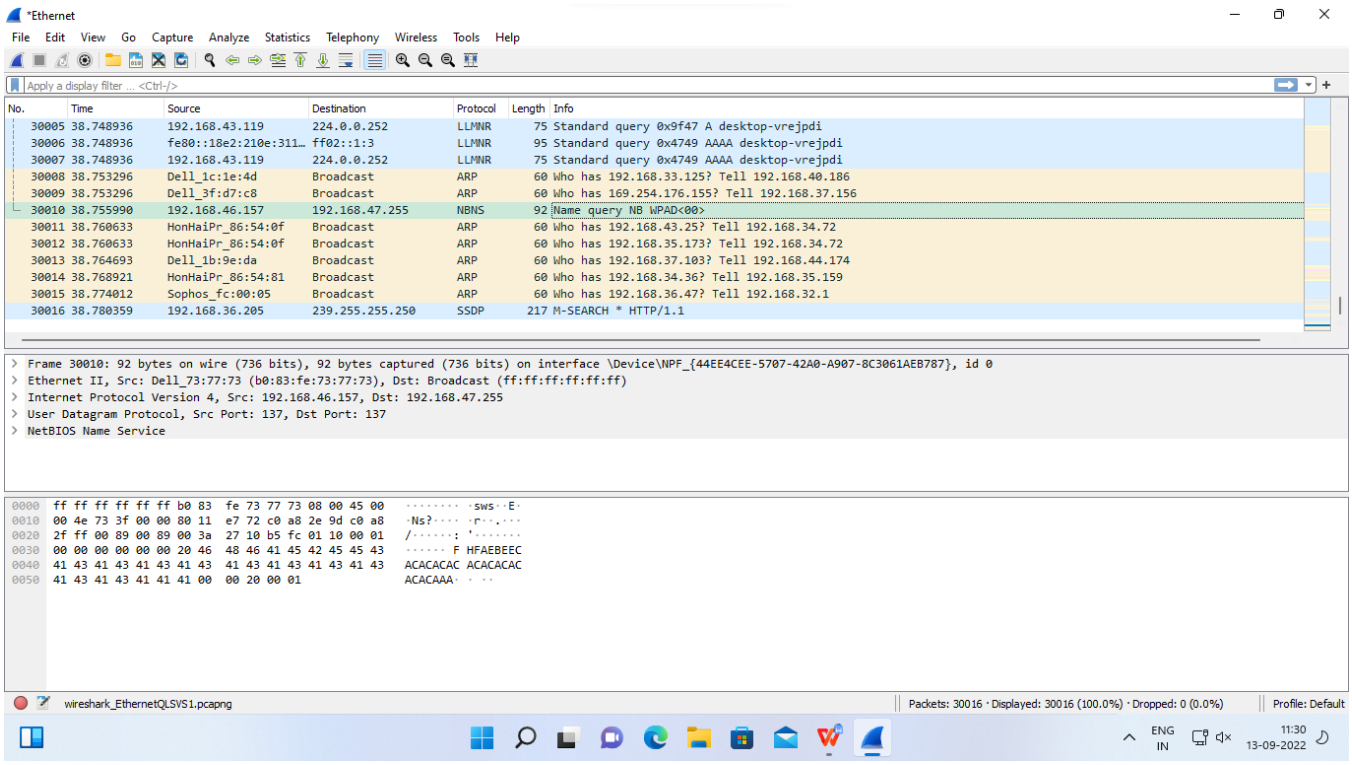
NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

In the Figure below, you can see standard UDP (light blue), routing (dark yellow), and routing traffic (light yellow).



4. By clicking on the red square ‘stop capturing packets’ operation, we can stop the process of packet capturing.

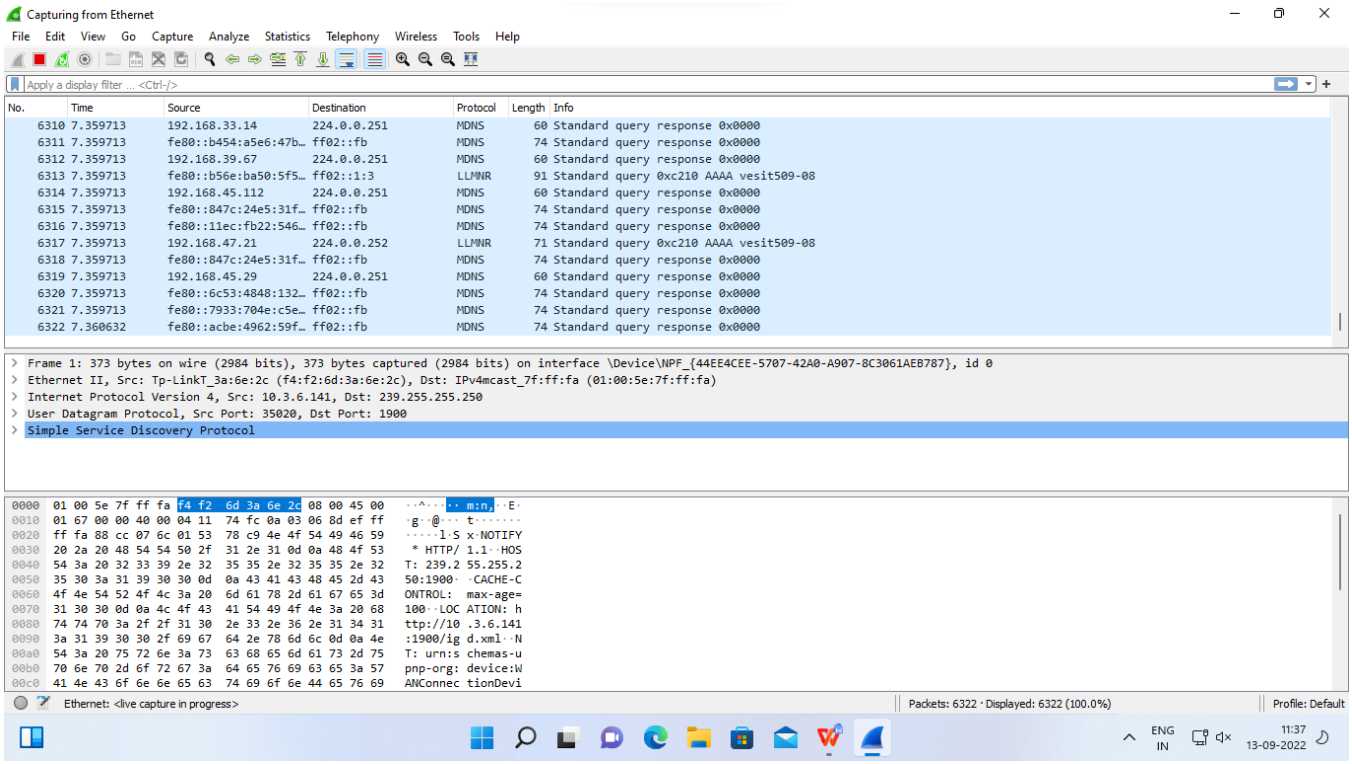
As shown in the figure, Wireshark has stopped capturing packets:



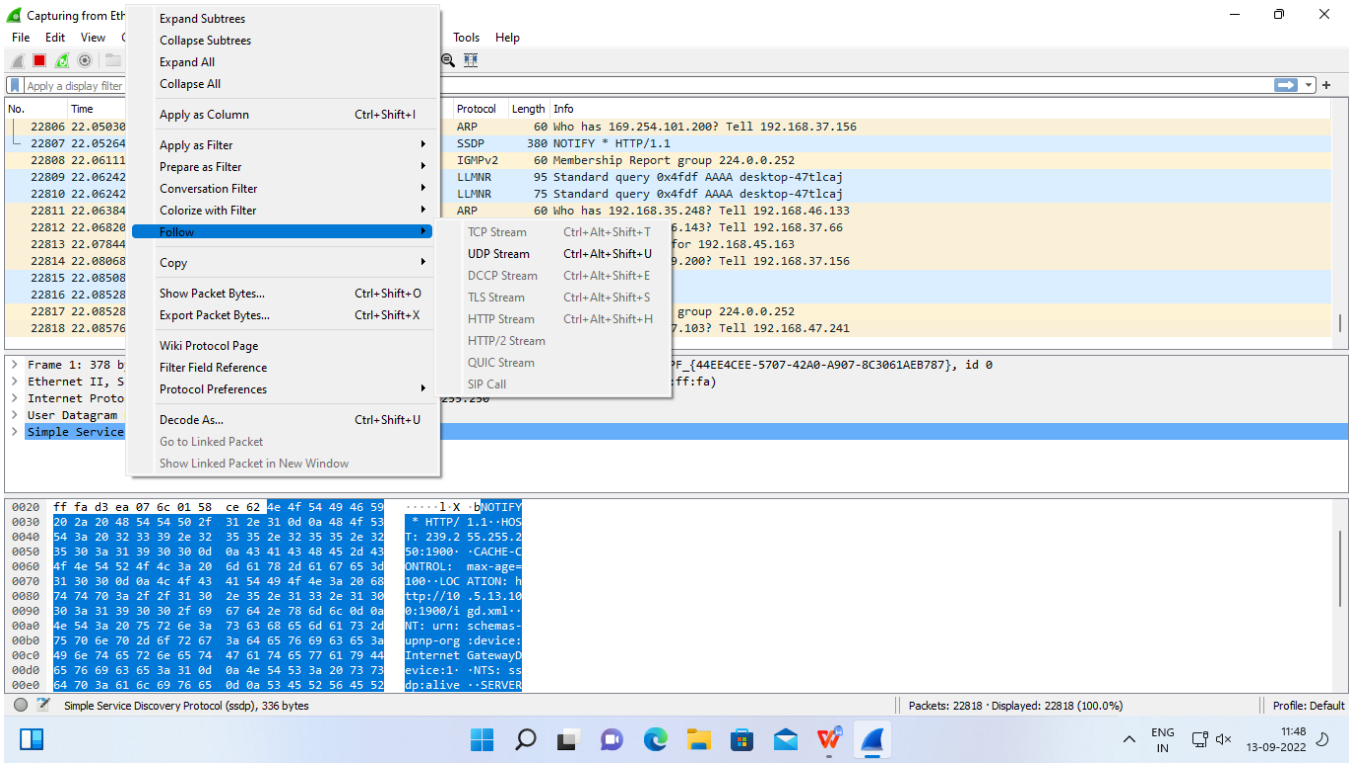
NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

5. Filtering packets:

In the given figure, we are filtering packets of the HTTP protocol.

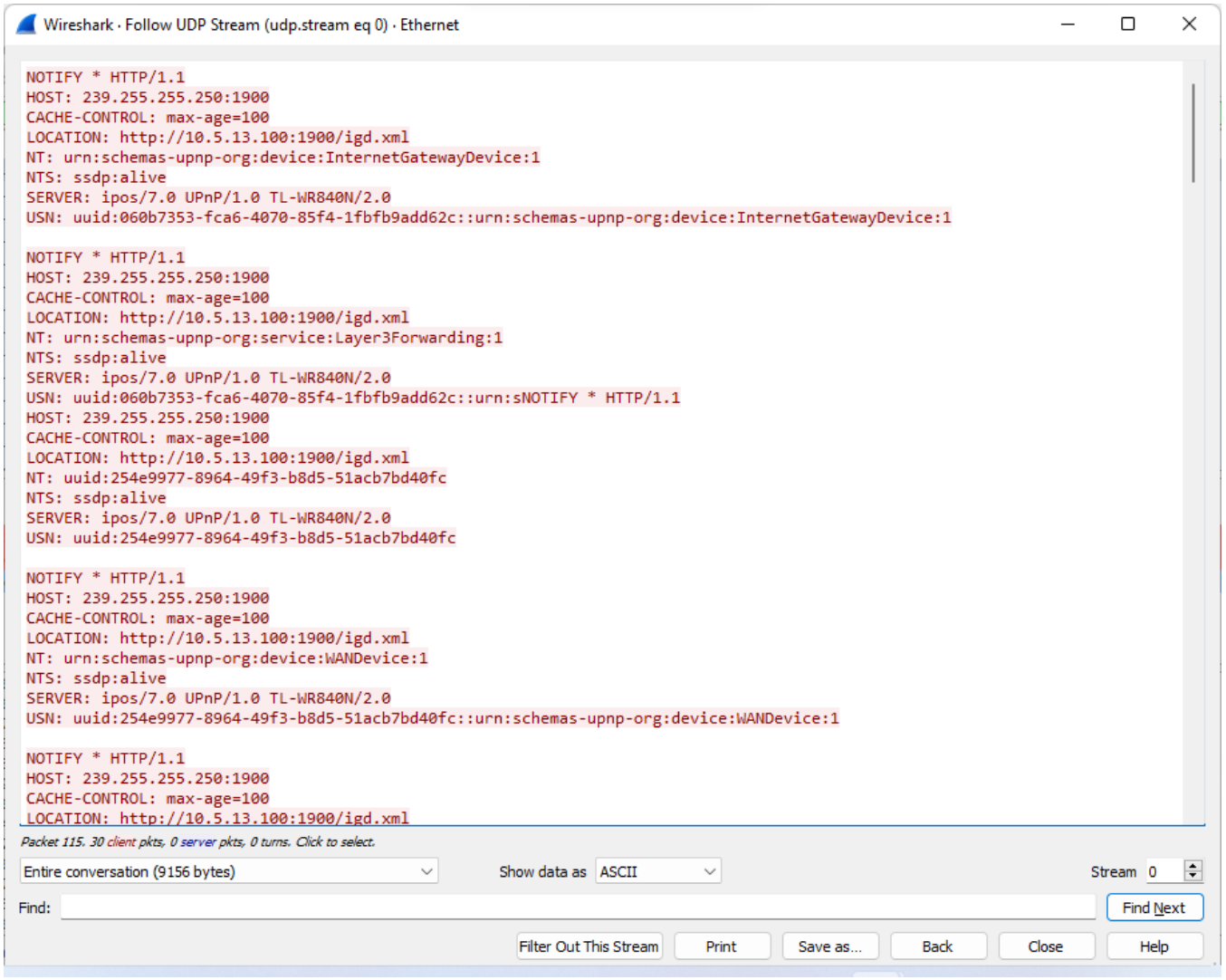


6. Following a protocol stream applies a display filter that selects all the packets in the current stream. Some people open the “Follow TCP Stream” dialog and immediately close it as a quick way to isolate a particular stream. Closing the dialog with the “Back” button will reset the display filter if this behavior is not desired.



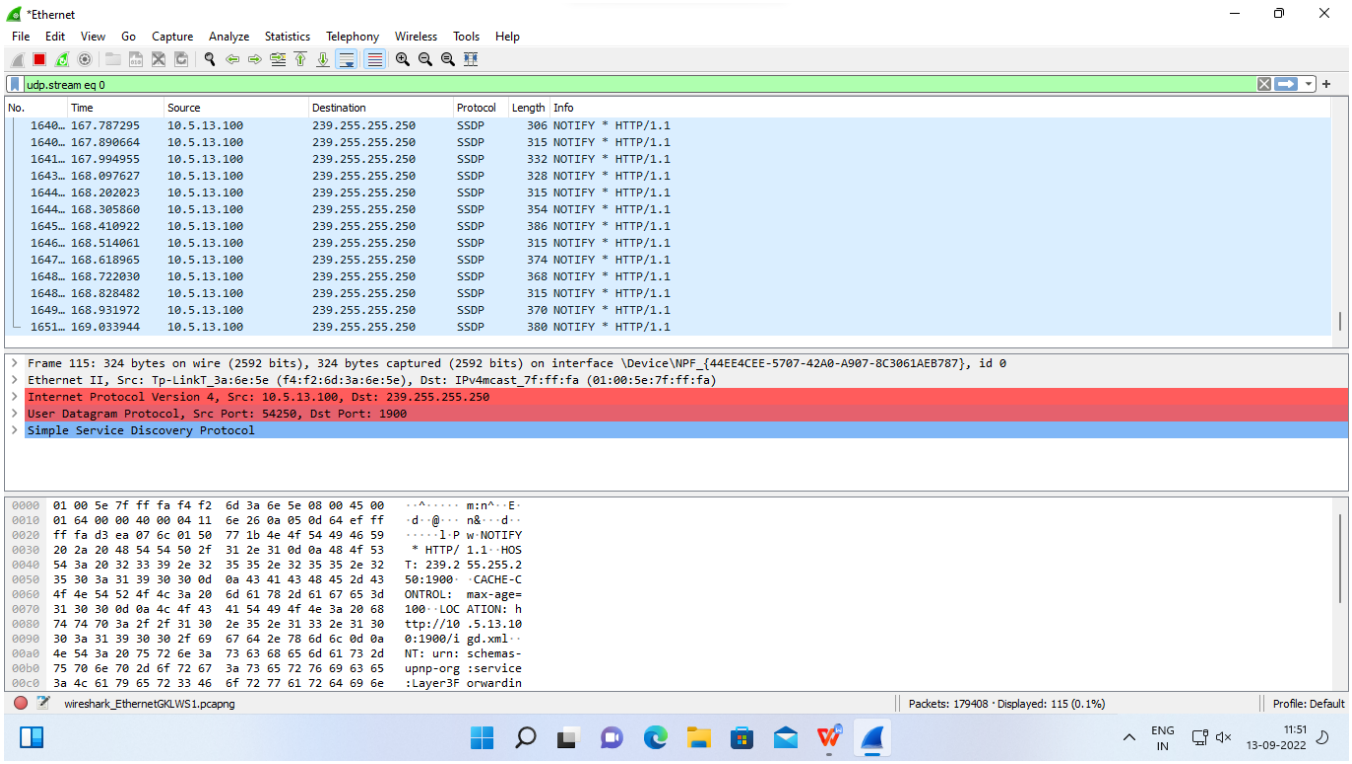
NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

The “Follow TCP Stream” dialog box:

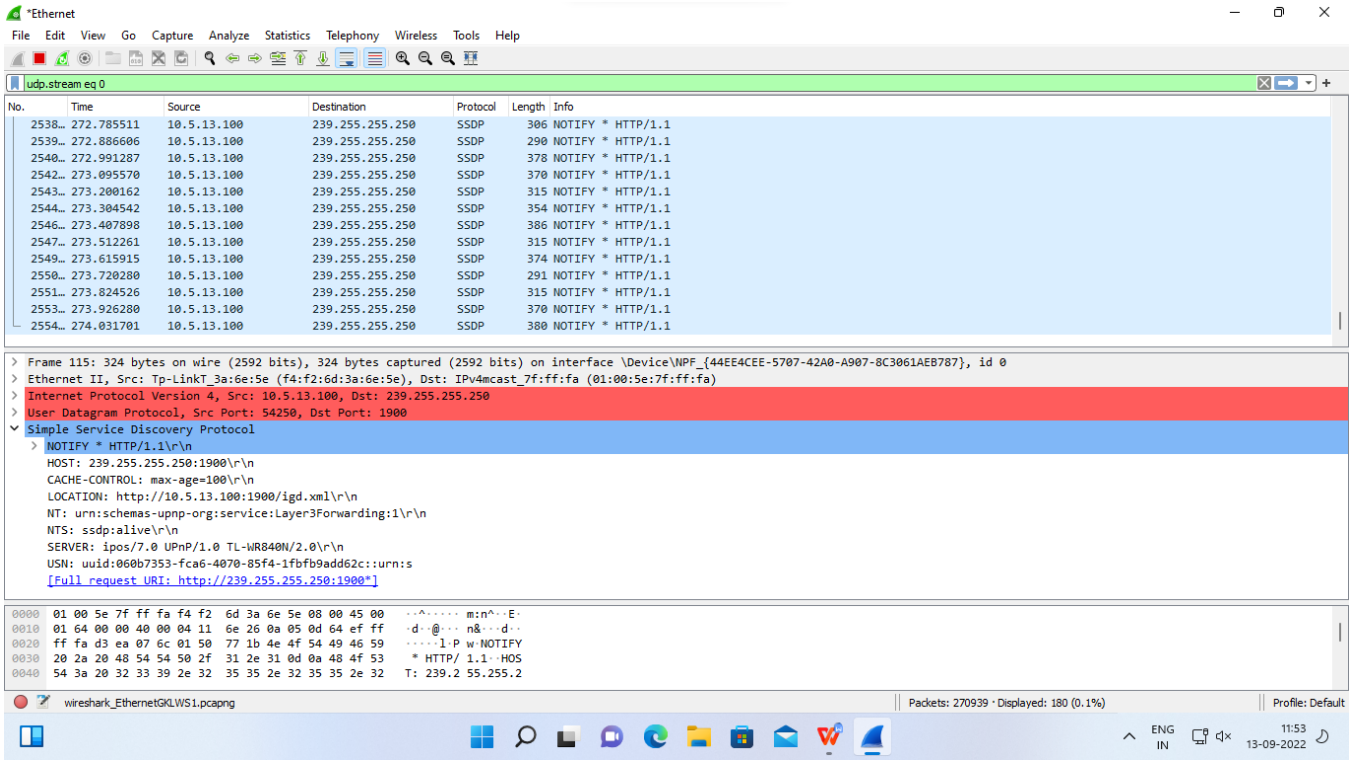


NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

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

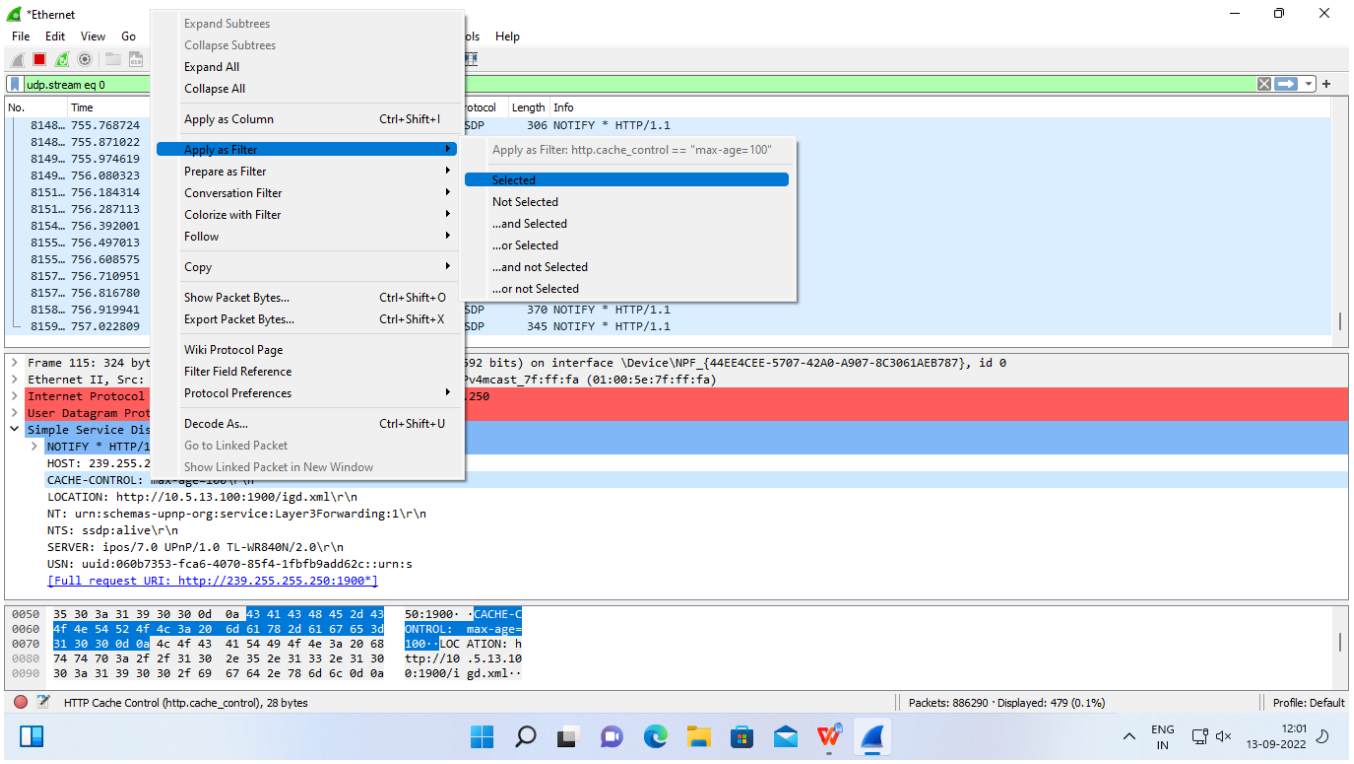


8. Inspecting packets
   Click the specific packet to dig down into more details.



NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

9. Apply as a filter.



CONCLUSION:

Thus we studied and implemented Wireshark.