PRACTICAL: 11

AIM:

Wireshark is an open-source tool for profiling network traffic and analyzing packets. It is often referred to as a network analyzer, network protocol analyzer, or sniffer. Wireshark intercepts traffic and converts that binary traffic into a human-readable format. Network administrators, Network security engineers, QA engineers, Developers, and other people to troubleshoot network problems, examine security problems, verify network applications, debug protocol implementations, and learn network protocol internals respectively, can use it. A practical approach to study Wireshark from network security concept.

THEORY:

Wireshark:

Wireshark is a free and open-source packet analyzer software used for network troubleshooting, analysis, software and communications protocol development, and education. It captures network traffic and displays it in a graphical format that is easy to understand. Wireshark can be used on a variety of platforms including Windows, macOS, and Linux.

Wireshark can capture and analyzing packets from a wide range of network protocols such as TCP, UDP, HTTP, DNS, and many others. It allows users to filter and search through network traffic to identify specific packets and protocol details. The software can also decode and display encrypted traffic for analysis.

Wireshark has a user-friendly interface and can be used by both novice and advanced users. It also provides a variety of tools and features to analyze network traffic, including packet capture filters, coloring rules, and the ability to export captured data in different formats.

Overall, Wireshark is an essential tool for network administrators, security professionals, and anyone who needs to troubleshoot or analyze network traffic.

Wireshark works by capturing and analyzing network packets that are sent and received on a network interface. The software captures packets in real-time as they are transmitted over the network and displays them in a user-friendly graphical format for analysis.

To capture packets, Wireshark uses a network interface to read all traffic on the network that the interface is connected to. This can be either a physical network interface card or a virtual interface created by a software application, such as a virtual machine or VPN.

Once the packets are captured, Wireshark displays them in a packet list that shows information about each packet, such as the source and destination addresses, protocol, and timestamp. Users can then drill down into individual packets to view more detailed information, such as the packet payload, protocol headers, and timing information.

Overall, Wireshark provides a powerful and flexible tool for network analysis that is used by network administrators, security professionals, and software developers around the world.

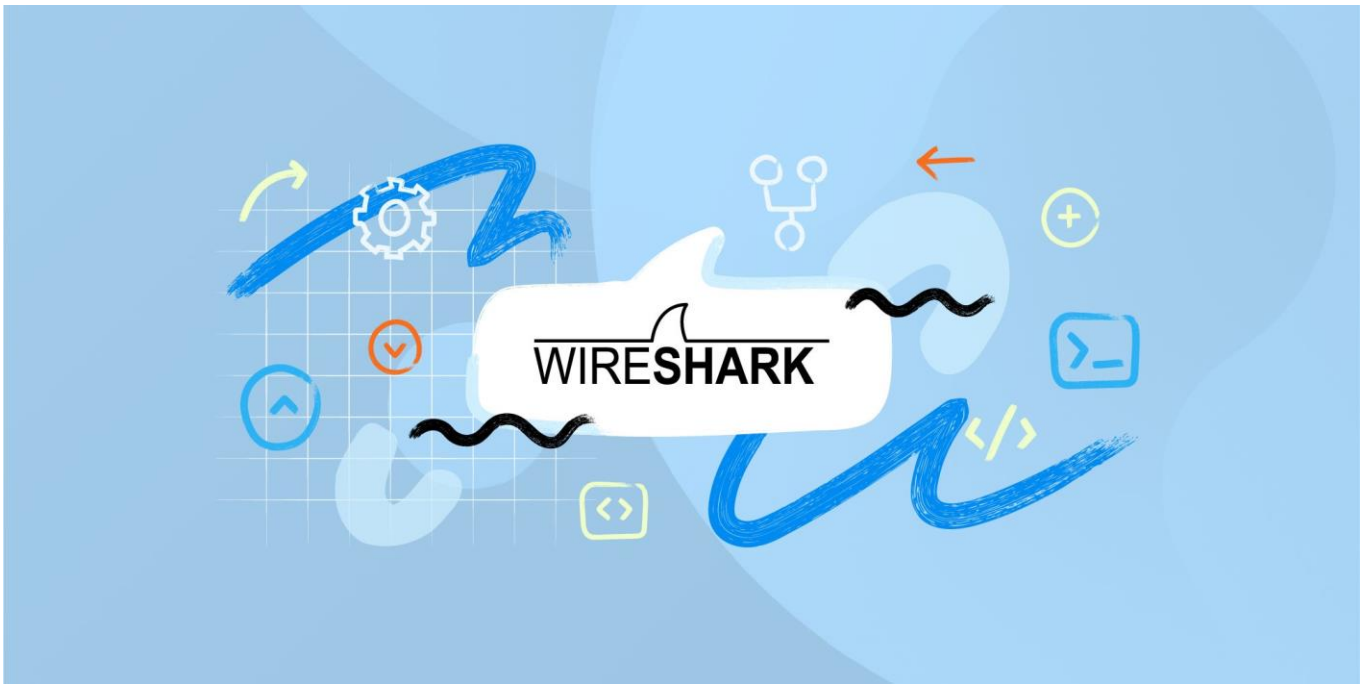
Wireshark can be a valuable tool in an Intrusion Detection System (IDS) for network security. By capturing and analyzing network packets, Wireshark can be used to detect and alert on suspicious or malicious activity on the network.

To use Wireshark as part of an IDS, the software is typically configured to capture and analyze network traffic in real-time. The captured packets are then analyzed using rules or signatures that are designed to detect specific types of network activity that may indicate an intrusion or attack.

For example, an IDS rule may be created to detect packets that contain a particular sequence of bytes or that are associated with a known attack vector. When Wireshark captures packets that match the rule criteria, it can generate an alert or trigger an action to block the offending traffic.

Wireshark can also be used to analyze network traffic after an attack has occurred to identify the root cause and determine the extent of the damage. By analyzing packet captures, it may be possible to identify the attacker, the attack method, and the damage caused to the network.

Overall, Wireshark can be a valuable tool in an IDS system for network security, providing real-time and post-attack analysis capabilities that help to detect and respond to threats on the network.



OUTPUT:

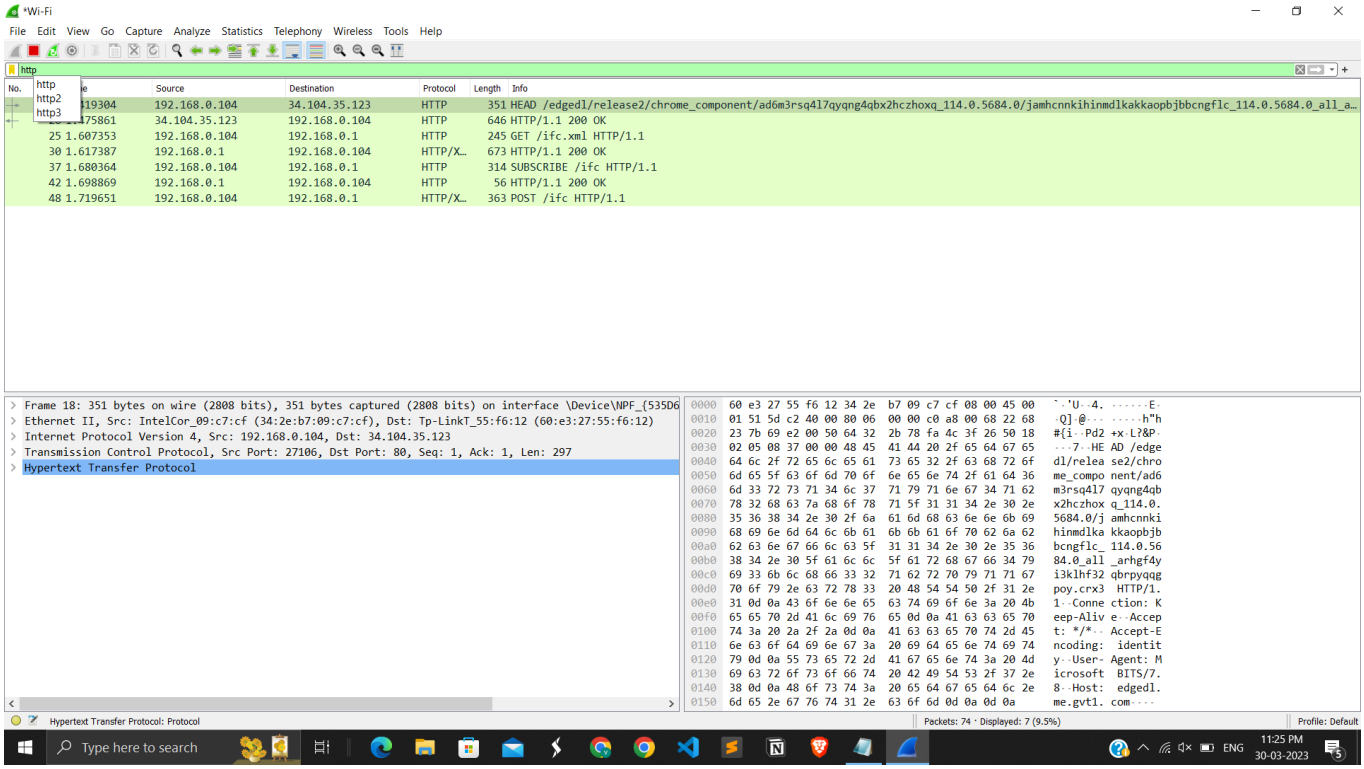


Fig 11.1 http filter in Wireshark.

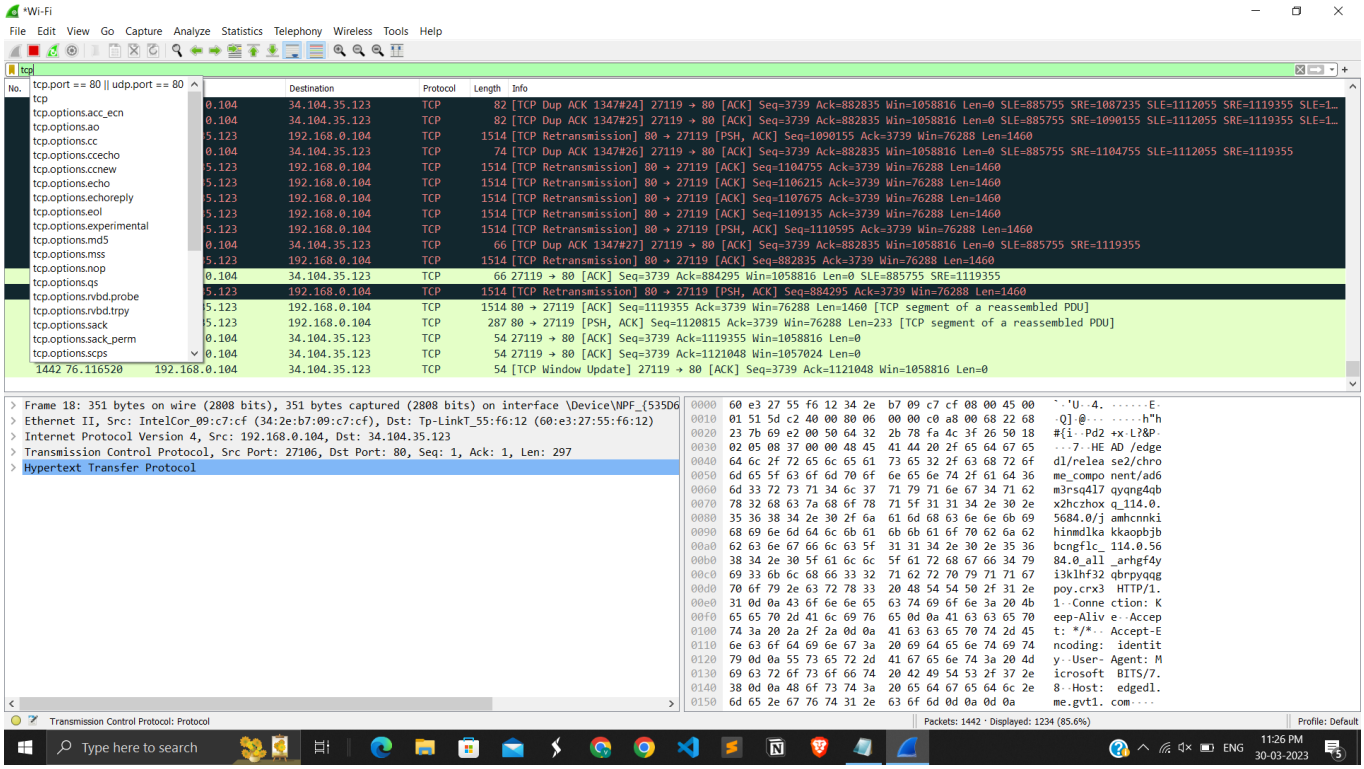


Fig 11.2 TCP filter in Wireshark.

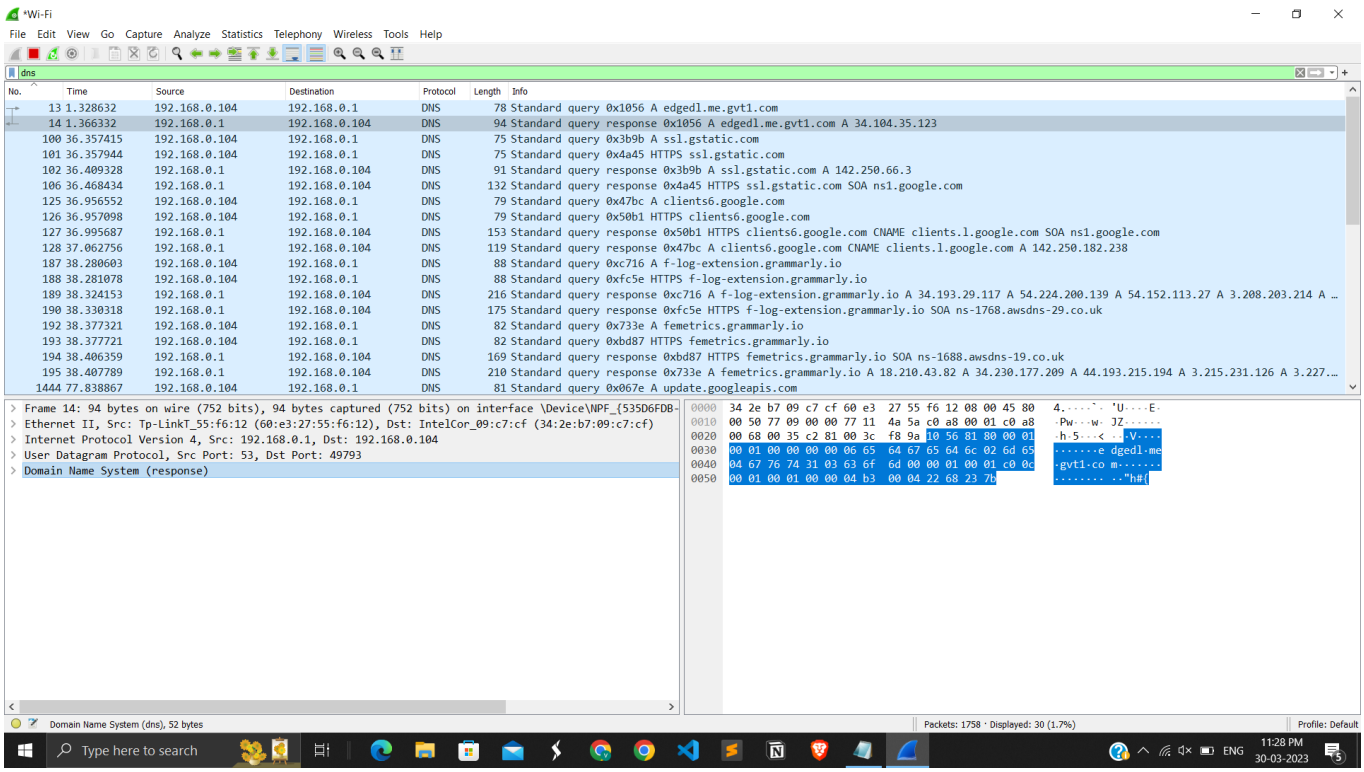


Fig 11.3 dns filter in Wireshark.

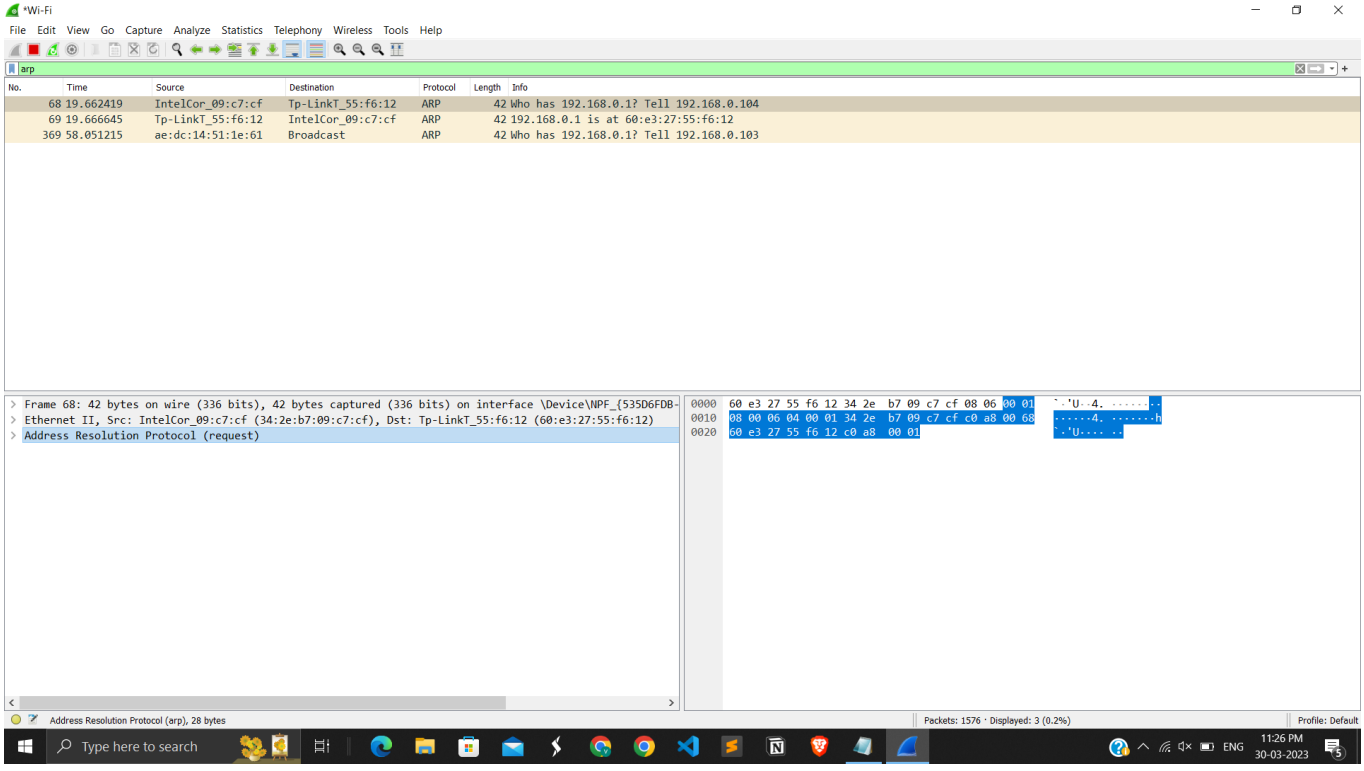


Fig 11.5 ARP filter in Wireshark.

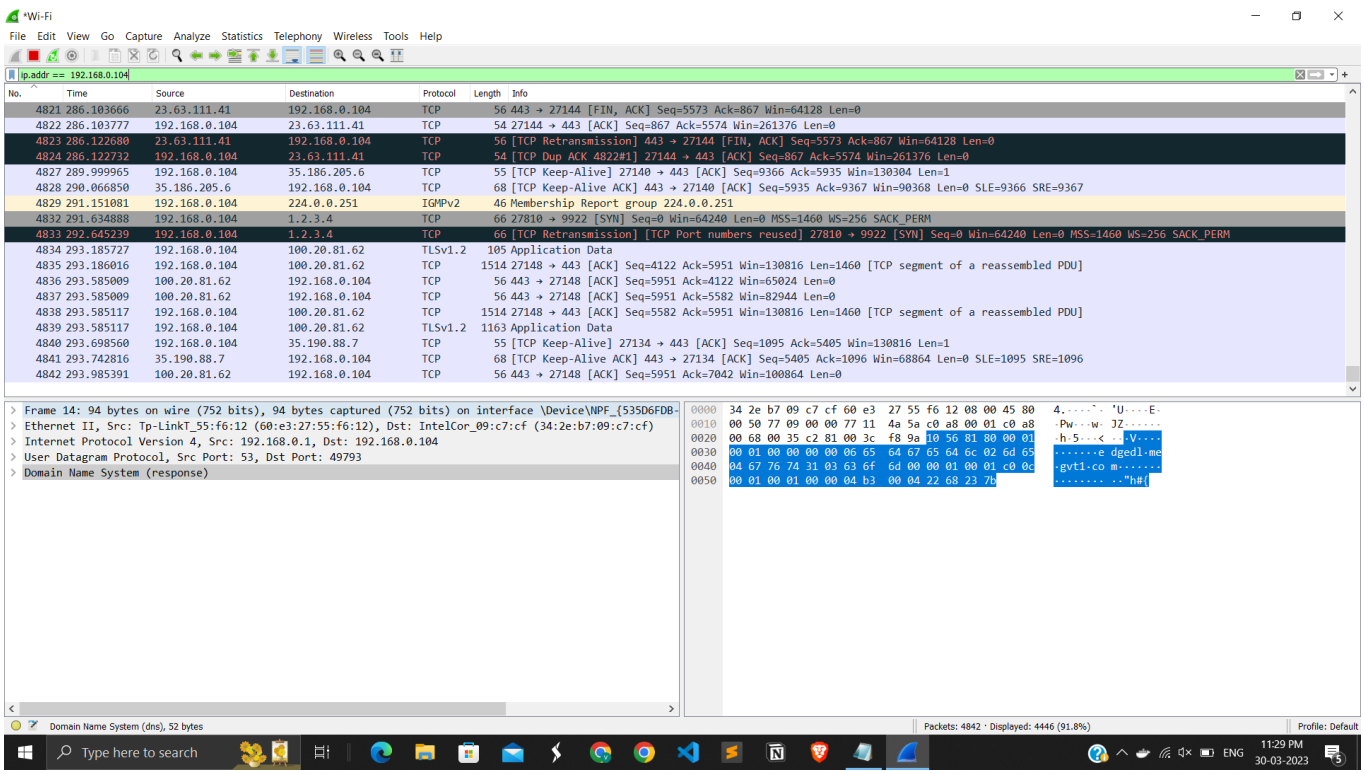


Fig 11.6 ip.addr filter will show the all the query been run from this ip address.

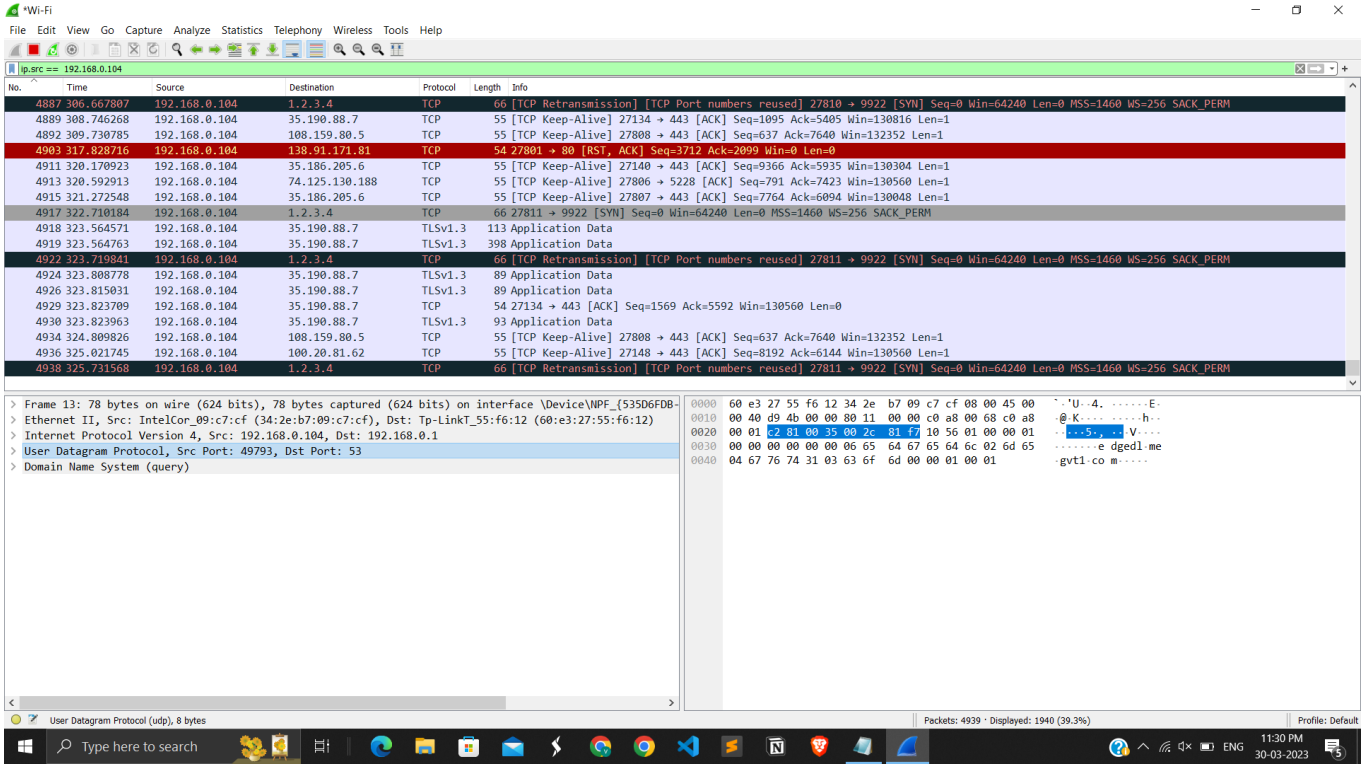


Fig 11.7 ip.src will find out the query been run by the source ip onto any website.

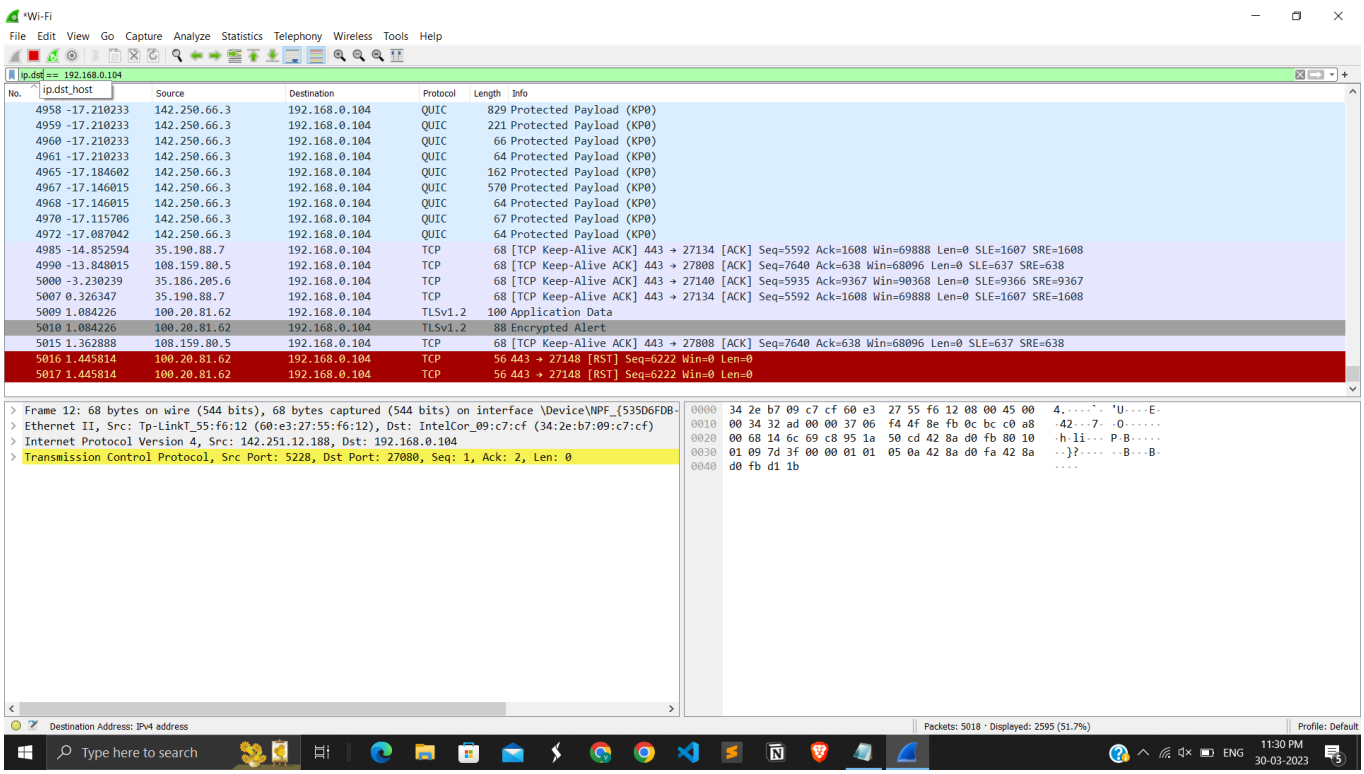


Fig 11.8 ip.dst will fetch the acknowledgement from any website from the outer network.

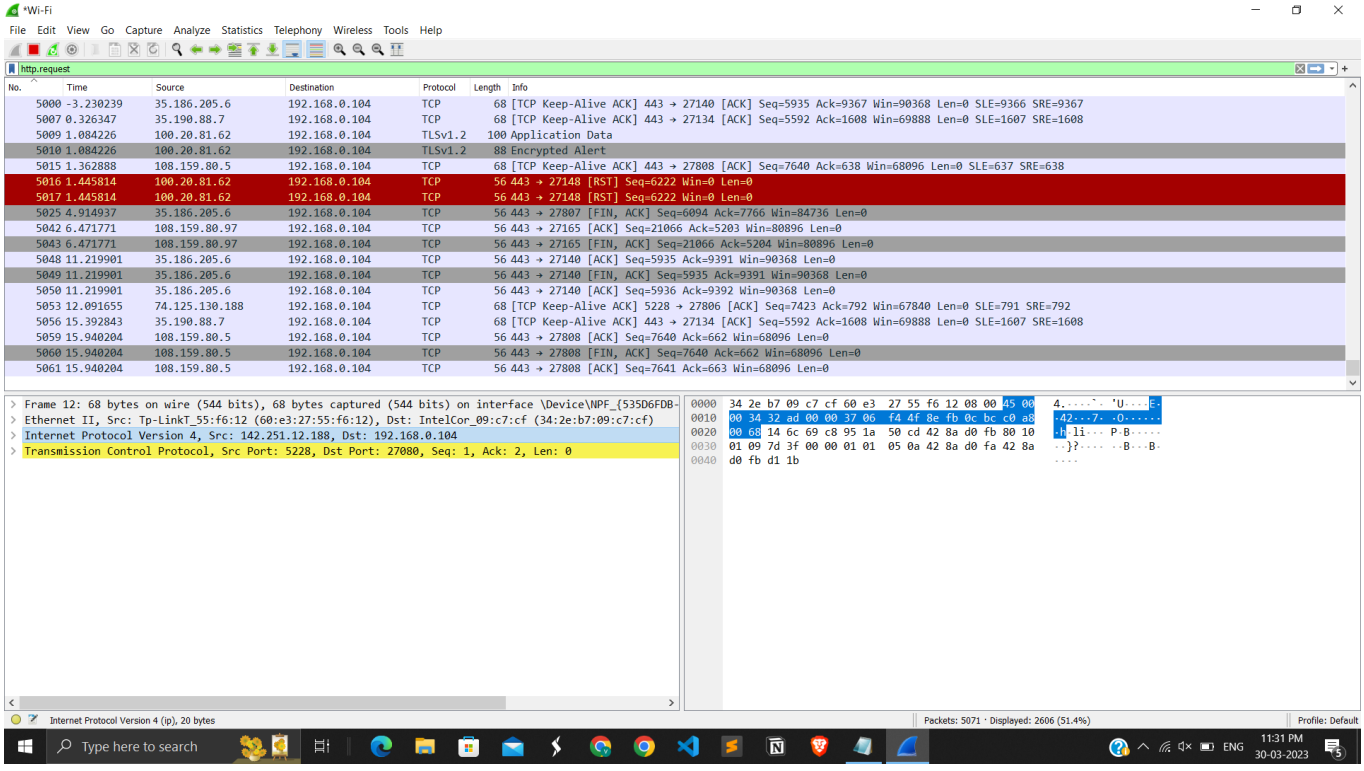


Fig 11.9 http.request filter will filter out the packets which were been queried to http.

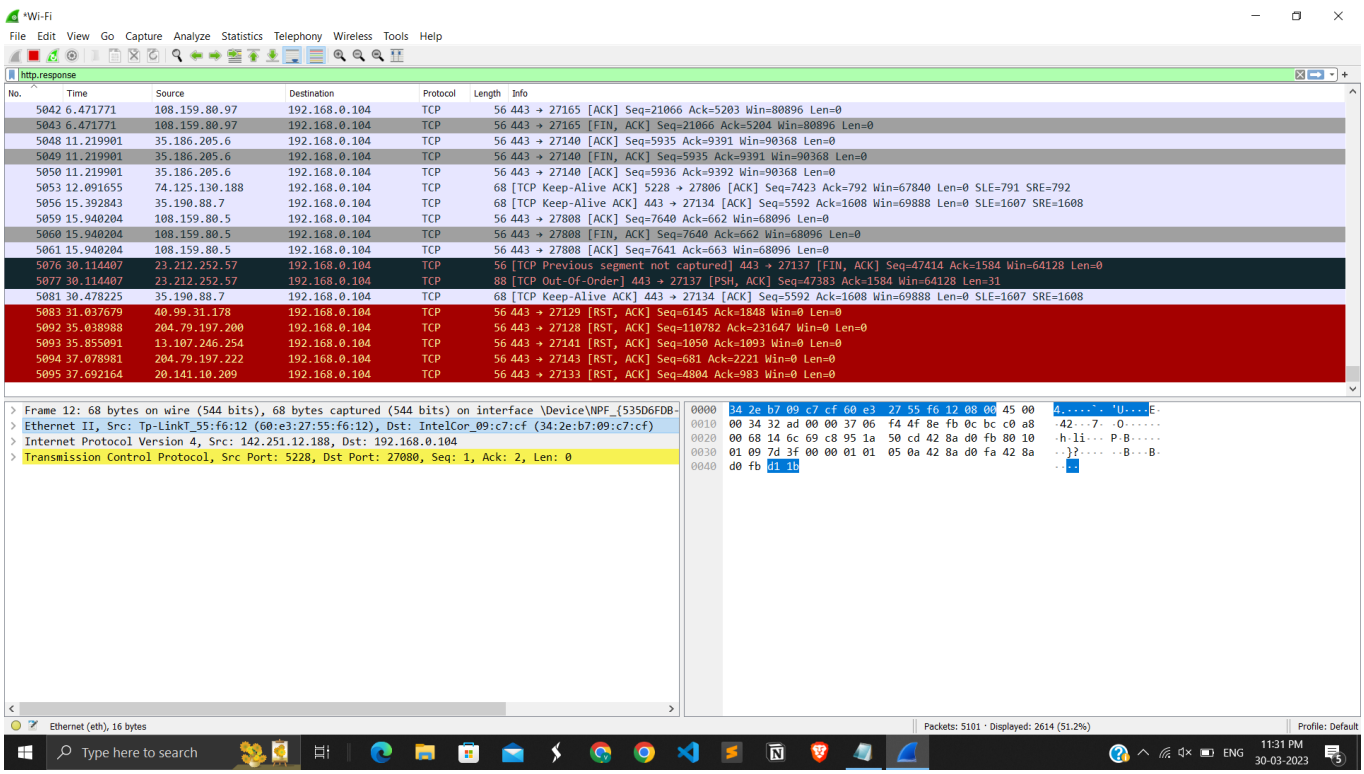


Fig 11.10 http.response filter will filter out the packets which were been acknowledged by http.

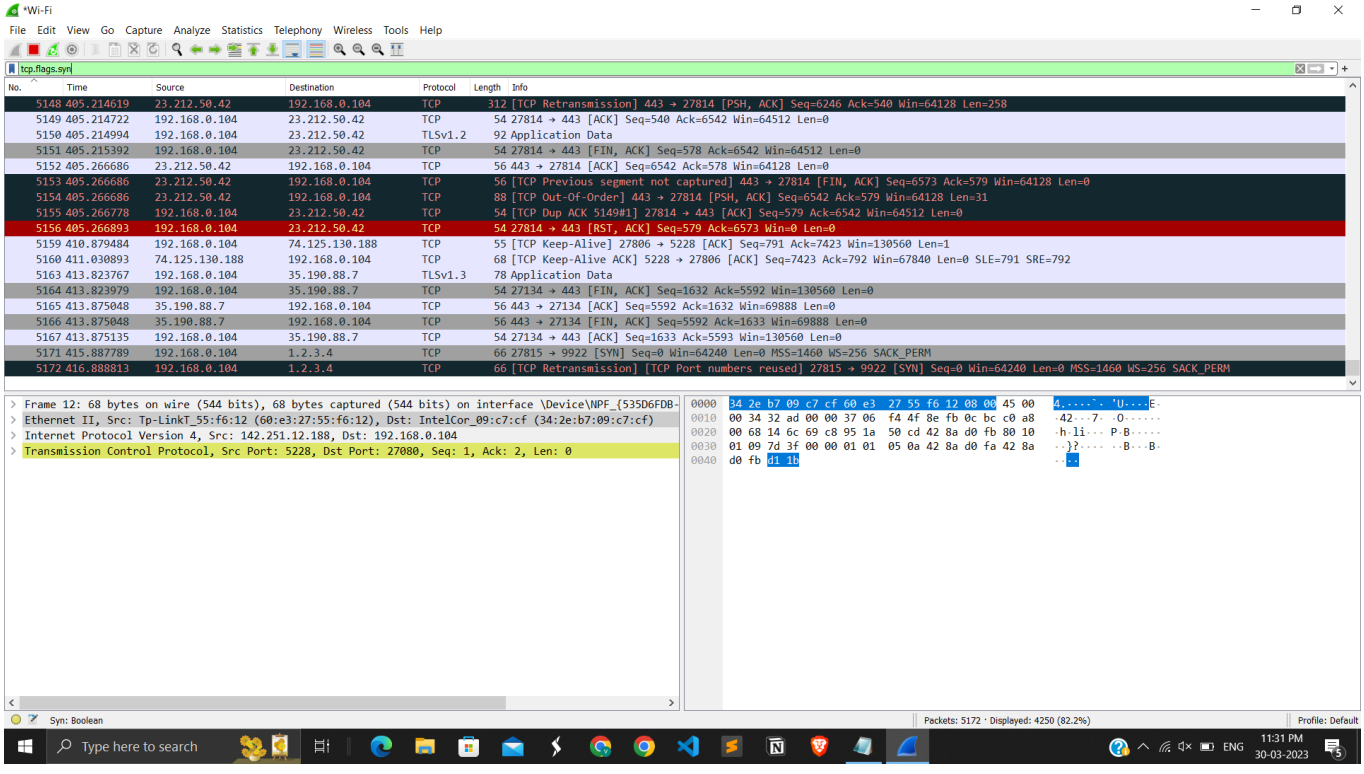


Fig 11.11 tcp.flags.syn will list out the syn of packets to tcp.

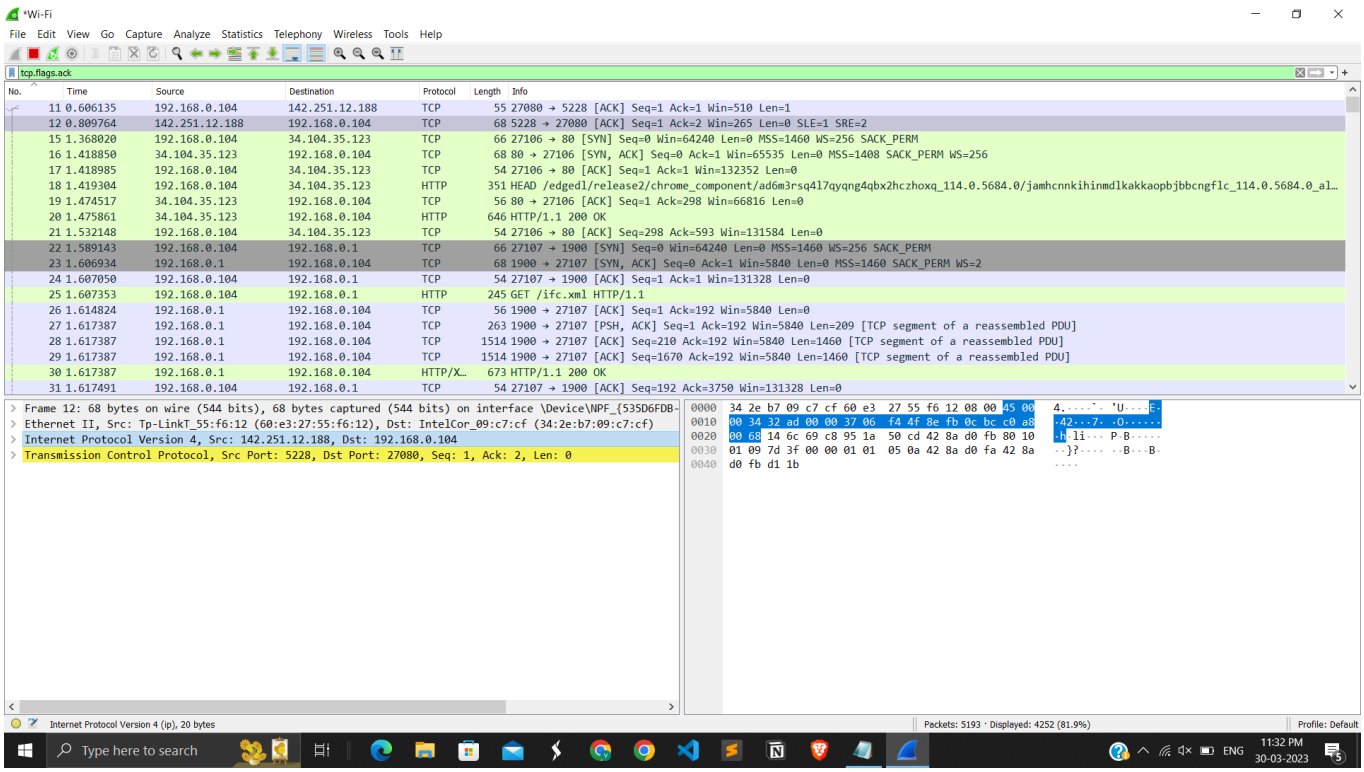


Fig 11.12 tcp.flags.ack will list all the acknowledgement received from tcp.

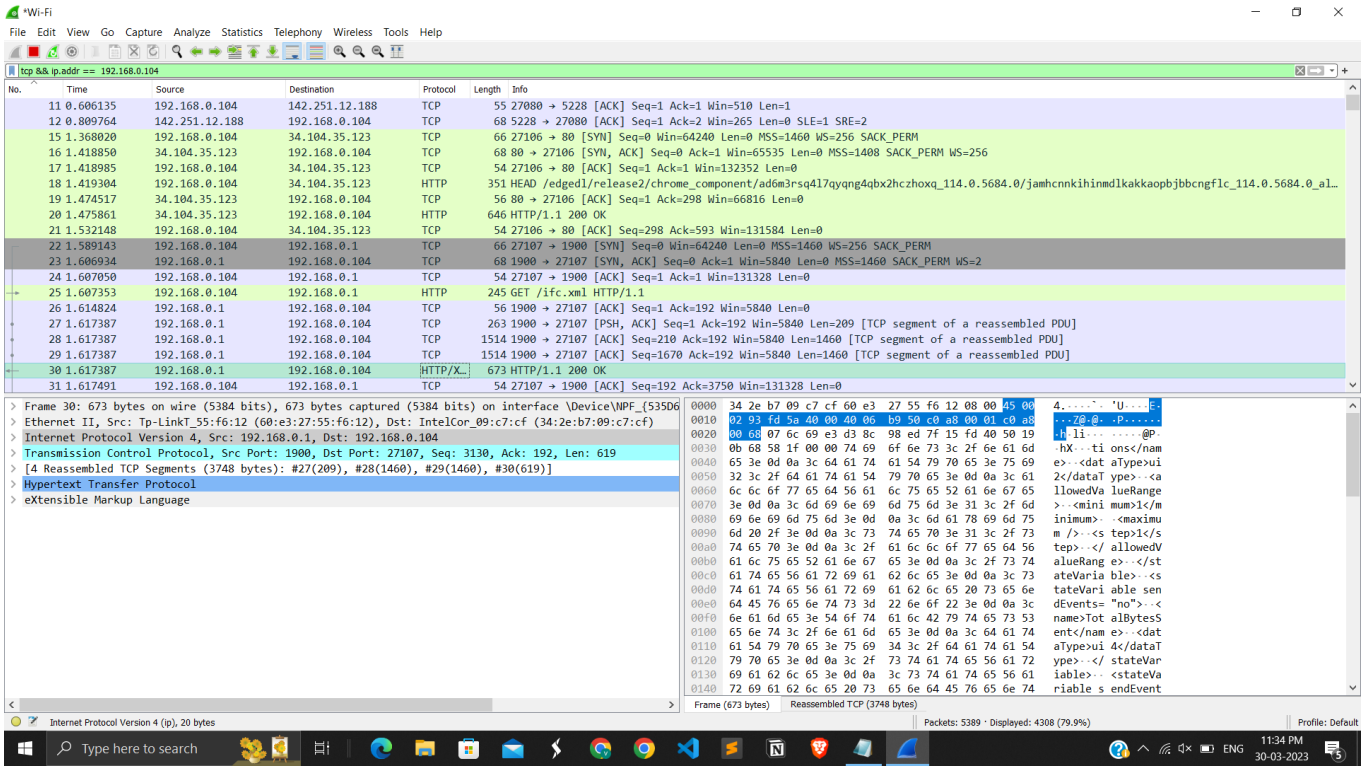


Fig 11.15 combine filter of tcp and ip.addr.

LATEST APPLICATIONS:

1. **5G Networks:** With the increasing adoption of 5G networks, Wireshark has become an essential tool for network engineers and security professionals to analyze and troubleshoot 5G network

traffic. Wireshark can capture and analyze 5G packet data and provide insights into the performance and security of 5G networks.

2. **Cloud Computing:** As more organizations move their applications and services to the cloud, Wireshark has become a useful tool for analyzing network traffic in cloud environments. Wireshark can capture and analyze packets in cloud-based networks and provide insights into network performance and security.
3. **Internet of Things (IoT):** With the growth of IoT devices, Wireshark can be used to capture and analyze network traffic generated by IoT devices. Wireshark can help identify security vulnerabilities in IoT devices and provide insights into the performance and behavior of IoT devices on the network.
4. **VoIP and Video Conferencing:** Wireshark can capture and analyze Voice over IP (VoIP) and video conferencing traffic, providing insights into the quality of the audio and video streams. Wireshark can help identify issues with call quality, such as jitter, latency, and packet loss.
5. **Security Analysis:** Wireshark can be used for security analysis, including intrusion detection, malware analysis, and network forensics. Wireshark can capture and analyze network traffic to identify suspicious or malicious activity on the network, and help identify the root cause of security incidents.

Overall, Wireshark continues to be a powerful and versatile tool for network analysis, troubleshooting, and security analysis across a wide range of applications and industries.

LEARNING OUTCOME:

- In this task I got to know about Network Troubleshooting Skills, Protocol Analysis, Security Analysis, Network Optimization, Technical Analysis.
- Overall, Wireshark can provide users with a range of valuable technical skills and knowledge that can be applied in a variety of industries and job roles, including network engineering, security analysis, and technical support.

REFERENCES:

1. Wireshark software: https://www.wireshark.org/
2. Document briefing of Wireshark: https://blog.wireshark.org/
3. Documentation reference : https://blog.wireshark.org/