Practical 9
Packet capture and header analysis by wire-shark (TCP, UDP, IP etc.)

Aim: Using Wire-shark to capture and analyse Packets

Theory:

Wireshark is popular and powerful network protocol analyzer software. It is primarily used for:

1. Network Troubleshooting: Wireshark allows you to capture and inspect network traffic in real-time or from previously captured packet data. This is invaluable for diagnosing and resolving network problems, such as connectivity issues, slow network performance, and packet loss. You can identify where packets are being dropped or delayed and pinpoint the source of network issues.

2. Security Analysis: Wireshark can be used to detect and investigate security breaches and malicious activity on a network. By examining network traffic, security professionals can identify suspicious or unauthorized activities, such as intrusion attempts, malware infections, and data exfiltration. It's an essential tool for network security monitoring.

3. Network Protocol Analysis: Wireshark supports a wide range of network protocols, and it allows you to analyze and decode packets to understand how different devices and applications communicate over the network. This is helpful for developers, network administrators, and security analysts who need to understand the behavior of network protocols and applications.

4. Network Performance Optimization: By analyzing network traffic patterns, Wireshark can help optimize network performance. You can identify bandwidth hogs, inefficient network configurations, and bottlenecks in the network infrastructure. This information can be used to fine-tune network settings and improve overall performance.

5. Educational and Training Purposes: Wireshark is often used in educational settings and for training purposes to teach networking concepts and packet analysis techniques. It provides a hands-on way to learn about network protocols and their interactions.

6. Compliance and Auditing: Some organizations use Wireshark for compliance and auditing purposes. It helps ensure that network traffic conforms to security policies and regulatory requirements. Organizations can use Wireshark to monitor and record network activities for auditing and legal purposes.

7. Software Development: Developers use Wireshark to debug network-related issues in their applications. It can help identify problems with network communication and assist in troubleshooting.

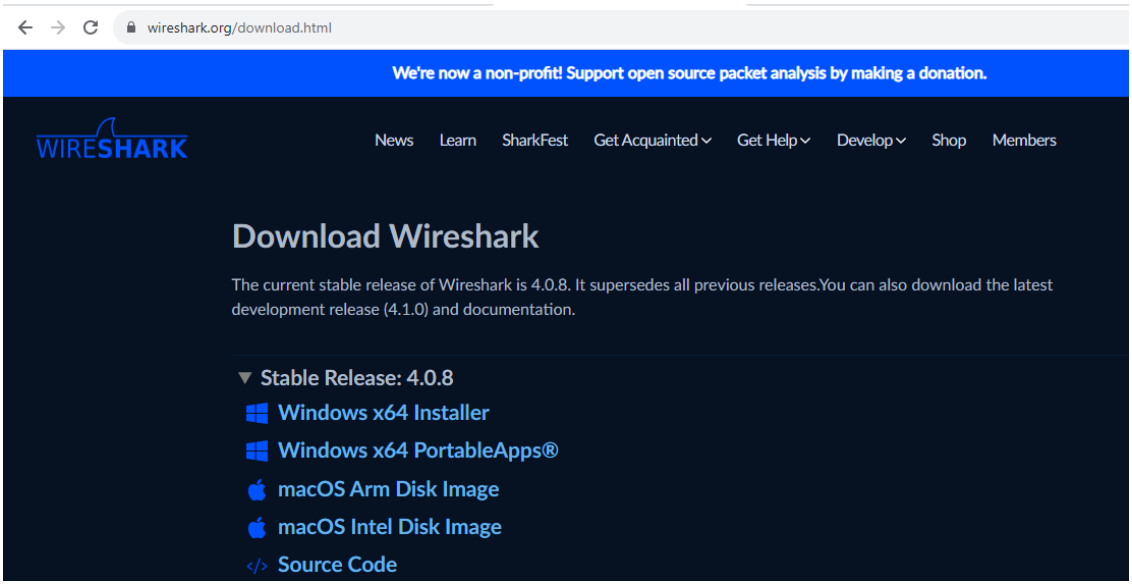
8. Packet Capture and Analysis: Wireshark allows you to capture packets from various network interfaces and save them for later analysis. You can filter and search through the captured data to extract specific information and gain insights into network behaviour.

9. Prototyping and Testing: Wireshark can be used to test and validate network configurations and prototypes before they are deployed in a production environment. It helps ensure that new network setups work as expected and meet performance criteria.

Wireshark's user-friendly interface, extensive protocol support, and robust filtering capabilities make it a valuable tool for anyone involved in networking, security, or network-related development tasks. However, it's important to note that using Wireshark to capture and analyze network traffic may have legal and privacy considerations, so it should be used responsibly and in compliance with applicable laws and policies.

Install Wireshark:

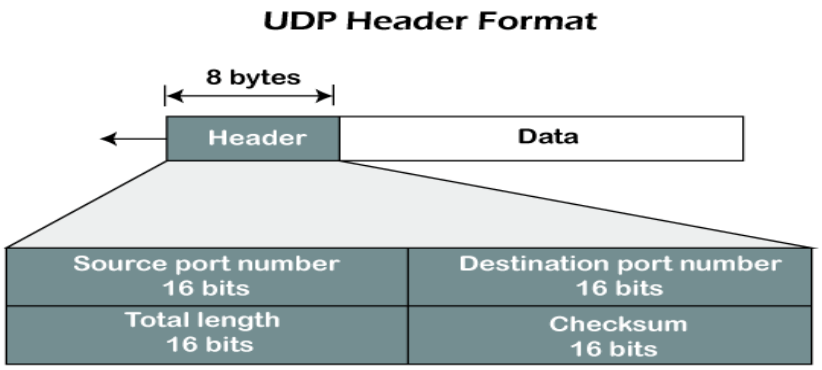
In order to demonstrate the packet capture and analysis, we install Wireshark by visiting the website www.wireshark.org/download
And download the software according to our OS



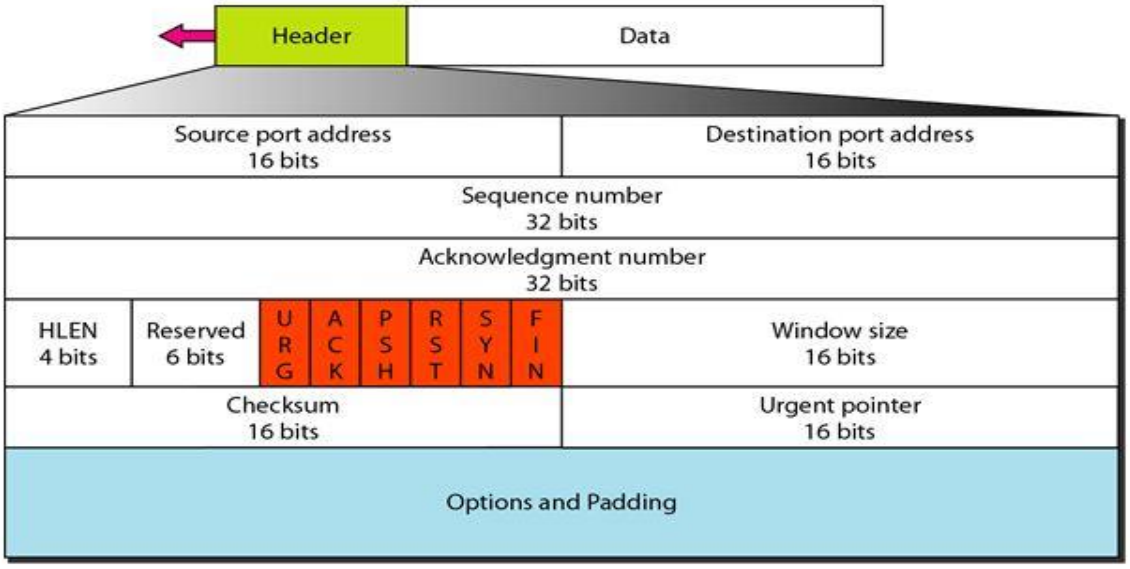
Analysis:

Before doing the analysis of the packets, we must first know the UDP, TCP and IP packet format

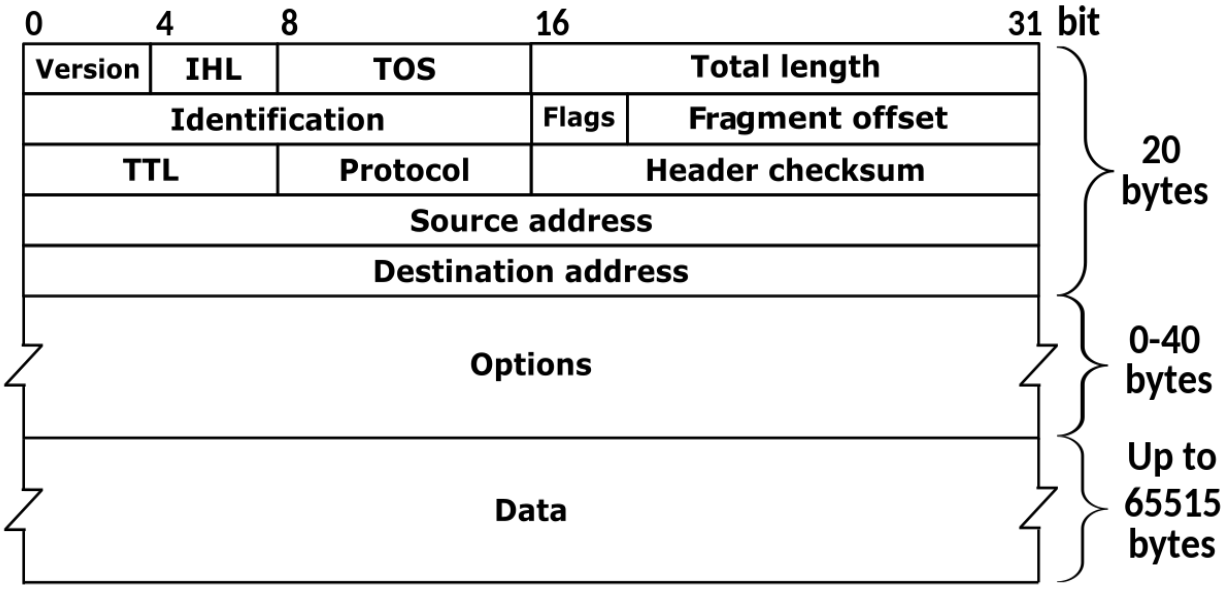
UDP Packet format



TCP Segment format:

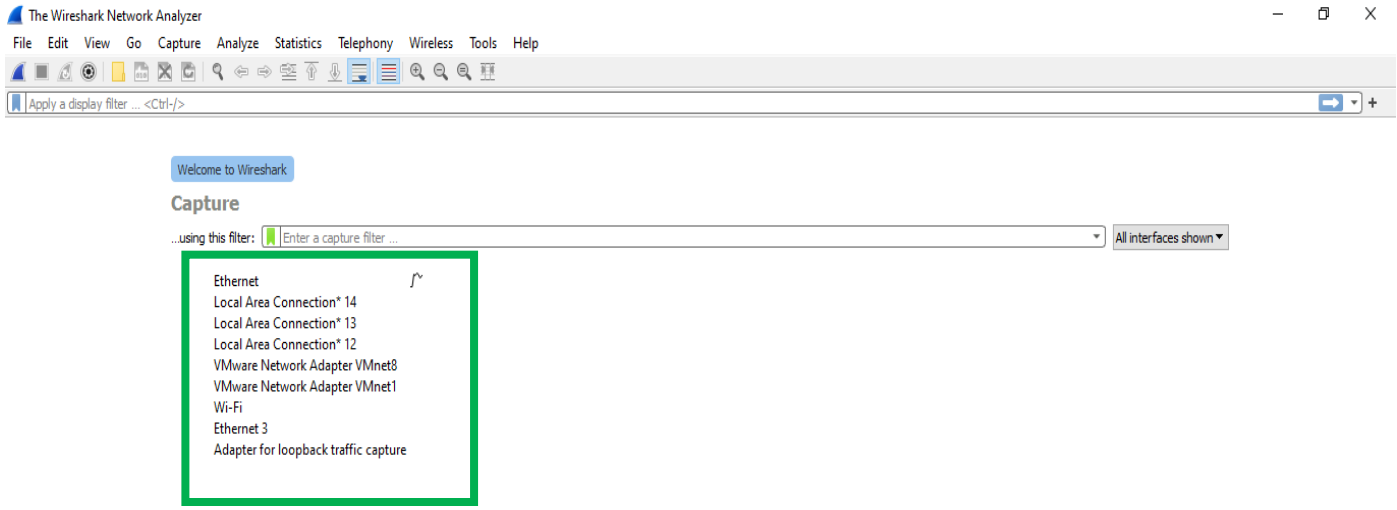


IP packet format:

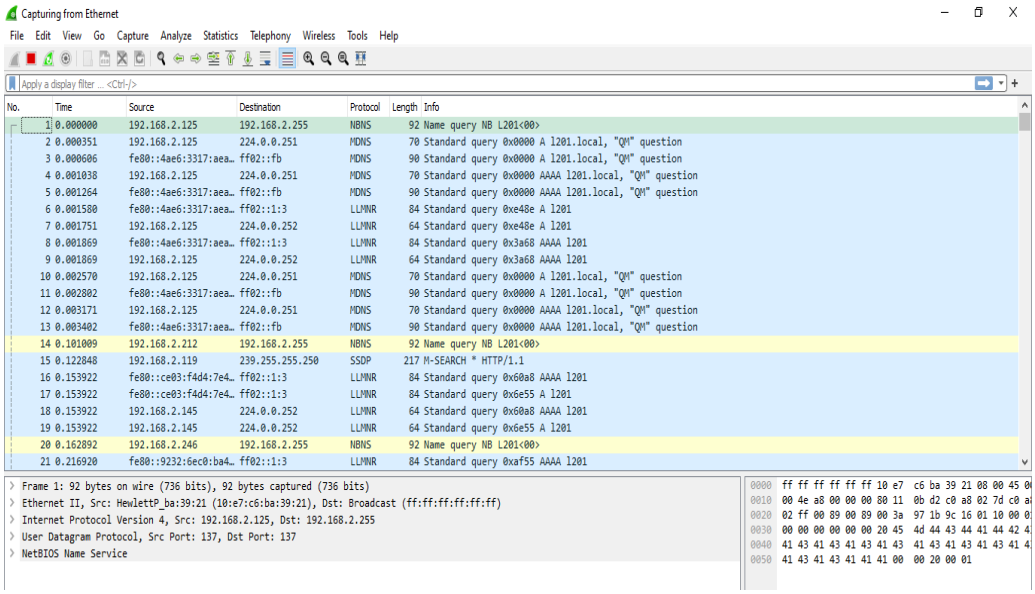


Using Wire-Shark:

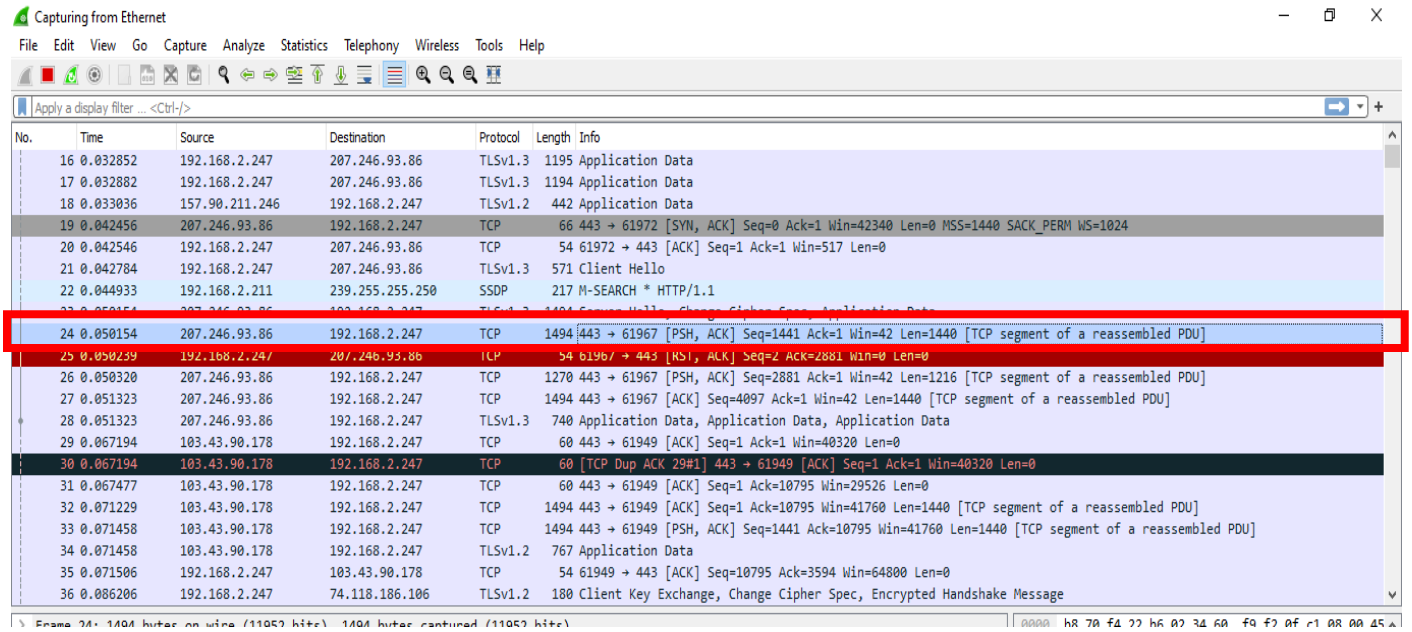
We use Wireshark to do the analysis of the packet, we get the following interface when we start Wireshark



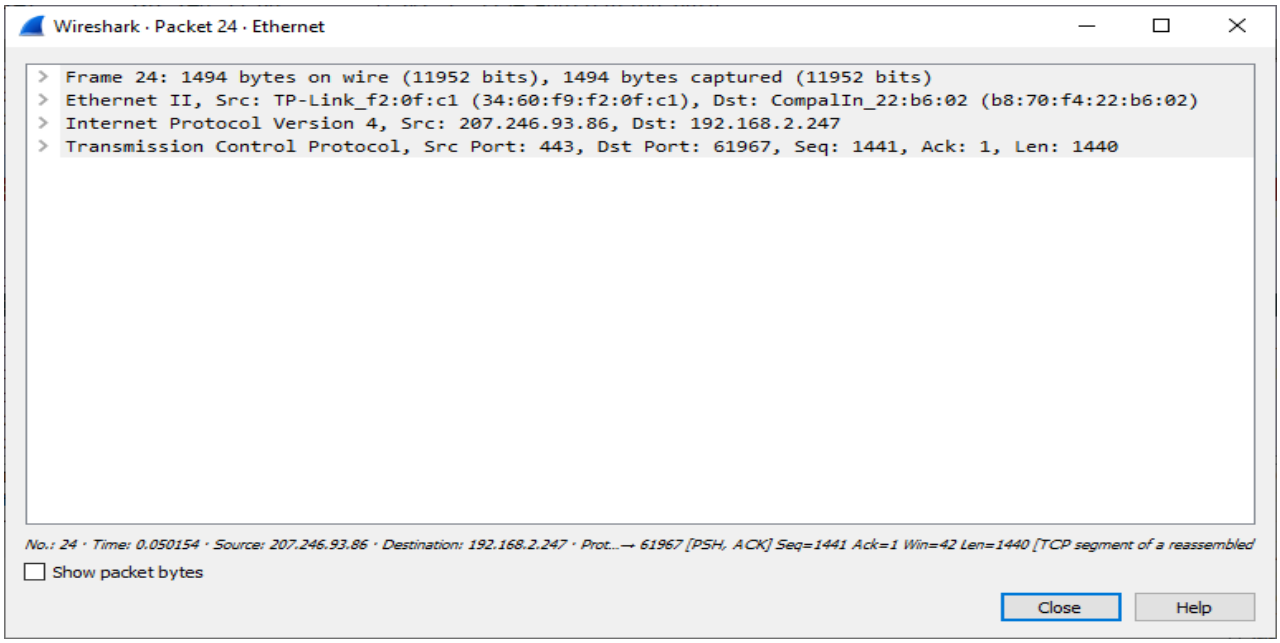
The above interfaces are shown, as in our case the internet connection is available on the Ethernet interface, we double click on this interface and get the following



Now we click on any TCP packet and analyse it,

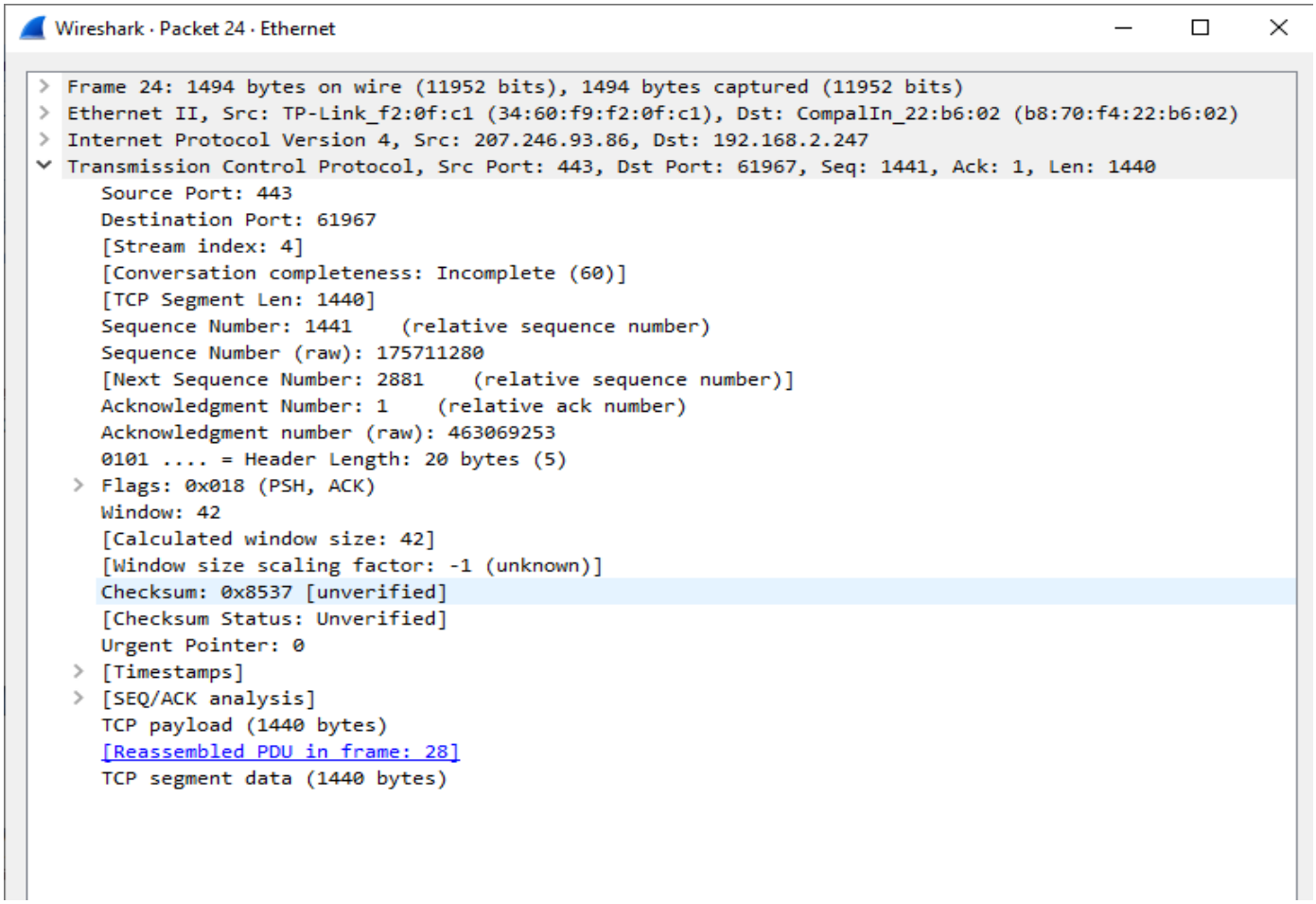


When we double click on the above TCP packet (packet 24) in the above case we get



TCP segment analysis:

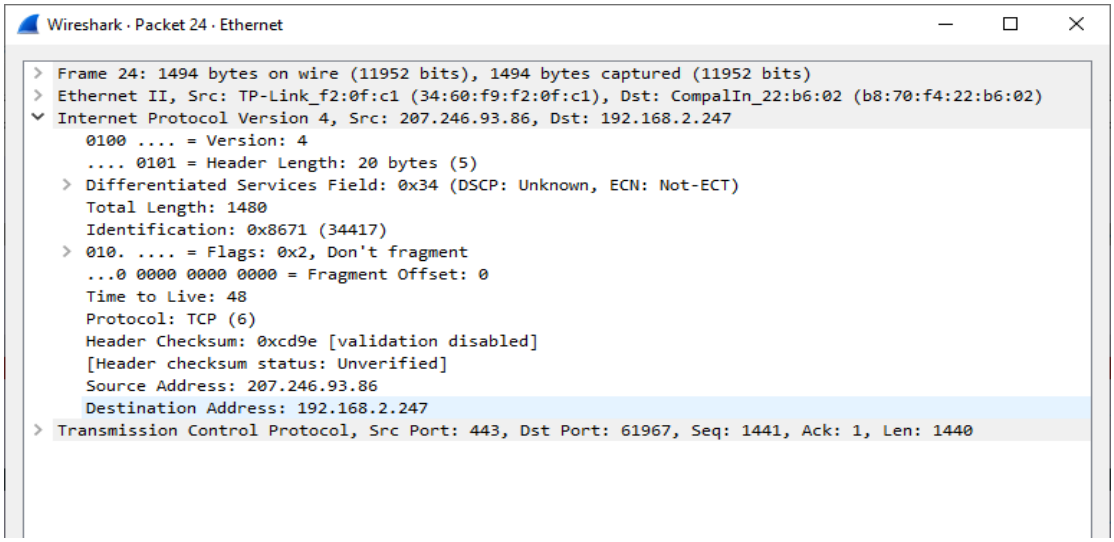
When we click on Transmission Control Protocol (TCP), we get the information about the TCP segment and we can analyse the segment



As seen from the above we get
Source Port: 443
Destination Port: 61967
Sequence number1441
Acknowledgement Number: 1
And also the other information such Flags, Window, Urgent Pointer etc

IP packet analysis:

When we click on Internet Protocol Version 4, we get the information about the IPv4 packet and we can analyse it



We can easily analyse the packet and get the information about the IP packet
Source IP address: 207.246.93.86
Destination IP address: 192.168.2.247
Header Length: 20 bytes
Total Length: 1480
Other fields are also seen

Similarly we can also analyse any UDP packet

For the video demonstration of the practical click on the link below or scan the QR-code

https://youtu.be/pT93ag0zSXQ