



School Of Engineering second year CSE (Hons) Project in  
Principle of Data Networks.

**Assignment Title:**

Data Networking Protocol Analysis Using emulation and  
simulation tools.

Student ID: 4120846

Submission Date: Tuesday, 5 December 2023, 5:00 PM.

Project Supervisor: Dr. Muhammad Alam.

## Table of Contents:

<b>1. Introduction.....</b>	<b>7</b>
• Overview of Data Networking and protocol analysis.....	
.8	
• Importance of tools in network analysis.....	
.....8	

## Part A:

<b>2. Protocol analysis using Wireshark.....</b>	<b>9</b>
• Preparing for analysis: clear ARP cache and Browser History.....	
...10	
• Starting packet capture with Wireshark.....	
.11	
• Surfing the internet for data collection.....	12
• Stopping packet capture and Initial Observation.....	1
3	

## Questions Answer:

<b>3. Explanation of the TCP/IP handshake process.....</b>	<b>14</b>
--	-----------

• Importance of packet sniffing in Network analysis.....	1
5	
• Practical example with an explanation.....	
15	
<b>4. Foot printing and its application in Cybersecurity.....</b>	<b>16</b>
• How Hackers use Wireshark for Foot printing.....	1
7	
• Illustrative Example.....	18
<b>5. Explanation of the ARP Broadcast on a Network.....</b>	<b>18</b>
• How ARP Spoofing Work.....	19
• Using Wireshark for ARP spoofing.....	19
• Example scenario.....	20
<b>6. Detailed analysis with Wireshark.....</b>	<b>20</b>
• Monitoring network threats with Wireshark.....	20
• Proactive, Reactive and Active Monitoring Techniques.....	21,22, 23
<b>7. Troubleshooting Network Issues.....</b>	<b>23, 24</b>

• Practical Example and technical Explanation.....	25, 26, 27
<b>8. Using Wireshark Provide a figure.....</b>	<b>28</b>
• Display all TCP and UDP packets.....	28, 29
• Display packets from specific IP Host.....	29
• Display packets from multiple IPS.....	29
• Exclude an IP address.....	30
• Display URL.....	30
• Show the TCP handshake Process.....	31
• Show the TCP header format.....	31
• Display the TCP error packets.....	32
• Measure the latency.....	32
• Measure the Throughput.....	33
<b>9. Advanced Wireshark Functions.....</b>	<b>33</b>
• Applying 3 Logical Operations in Display Filters.....	33, 34.
<b>10. Understanding and configuring RIP (Routing Information Protocol) .....</b>	<b>34</b>
• Explanation of RIP protocol.....	35
• Step-by-Step network Configuration guide.....	36,37,38.
<b>11. References.....</b>	<b>39,40.</b>

## Table of Figures:

1.1: Clear ARP cache.....	8
1.2: Clear Browser History.....	9
1.3: use the command Ipconfig.....	9
1.4: capturing live data using Wireshark.....	10
1.5: surfing the internet.....	10
1.6: Stop live capturing data.....	11
2.00: Traffic visualization.....	13
2.01: Wireshark display with different protocol.....	14
2.02: Illustrative example of foot printing.....	16
2.03: ARP packet capture and spoofing with Wireshark..	17
2.04: Unusual large packets .....	19
2.05: Unusual DNS request .....	20
2.06: Inspect HTTP traffic.....	21
2.07: Search for known malicious domain.....	21
2.08: packet analysis to check any packet loss.....	22
2.09: check three-way handshake process.....	24

3.00: use the display filter icmpv6 to check traffic.....	25
3.01: Use the specific IP address to analyze specific data packet.....	26
3.02: Troubleshooting network Issues.....	26
3.03: Security analysis using Wireshark.....	27
3.04: Display all TCP packets.....	28
3.05: Display all UDP packets.....	28
3.06: display filter from specific IP.....	28
3.07: Display filter from multiple IPS.....	29
3.08: exclude an IP address.....	29
3.09: display URL.....	30
4.00: Three-way handshake process.....	30
4.01: TCP header Format.....	31
4.02: duplicate TCP error packets.....	31
4.03: measure the latency .....	32
4.04: And Logical Operator.....	33
4.05: OR logical operator .....	33
4.06: Not logical Operator.....	34
4.07: RIP configuration for router 0.....	37
4.08: RIP configuration for Router 1 .....	38
4.09: packets send successfully from one network to another...	39

## 1. Introduction:

In the complex Domain of modern computer networks, transparent information exchange depends on robust data

networks protocols. At the same time, Understanding and analyzing this protocol is critical to ensuring the efficiency and security of networked systems.

Although briefly explored the multifaceted field of data networking and protocol analysis, shedding light on the fundamental principles, tools, and methods that underpin the robust performance of computer networks. Besides that, using industry-standard packet analysis tools such as Wireshark emphasize is on practical knowledge.

This exploration with a detailed overview of data networking and protocol analysis. Additionally, some more topic is covered here such as fundamental principles to the intricate workings of communication protocols, troubleshooting networking issues and delving into the intricacies of TCP and UDP packets, and each section provides hands on insights.

Another important part is covered here is Routing Information protocol (RIP) using Packet Tracer networks configuration Tools. With the illustrative examples and screenshots, it makes sure that the clear understanding of the protocol and its role of networking.

In conclusion, this report encapsulates key learnings and summarizes the essential aspects of data networking and protocol analysis.

- **Overview of Data networking and protocol analysis:**

**Data Network explanation:**

A data network is a system for transmitting data from one network access point to another or multiple network access points using data switching, transmission lines and system controls. Data networks consist of communication systems such as circuit

switches, leased lines and packet switching networks. Data networks and data networking solutions impact all modern means of communication such as telecommunication and the internet.

The main goal of data transfer and networking is to enable communication and exchange of data between people and organizations. Two main types of data networks exist. Broadcast networks: where one node sends information to multiple nodes at once. Point to point networks: where each sender sends information to a single receiver.

Data communication through different networks such as Personal Area Network (PAN), Local Area Network (LAN), and Wide Area Network (WAN) etc.

Resource: Overview of Data Networks (URL <https://www.wwt.com/article/what-is-a-data-network> last access 25<sup>th</sup> November 2023)

### **Importance of tools in network analysis:**

In the case of Networking analysis, tools are playing a vital role. For example, Wireshark and cisco packet tracer tools for this report are used on various prospective. Here are some key aspects highlighting the importance of tools:

- Visibility and monitoring.
- Troubleshooting.
- Security.
- Performance Optimization.
- Configuration management.
- Reporting and analysis.
- Network building.

### **Part A:**



## 1. Protocol Analysis using Wireshark:

Wireshark is an open-source packet analyzer that can be used for a variety of purposes, including Network troubleshooting, Network Analysis, software and communication protocol Development, and Education. Wireshark was originally known as Ethereal but was renamed in May 2006 because of a trademark issue.

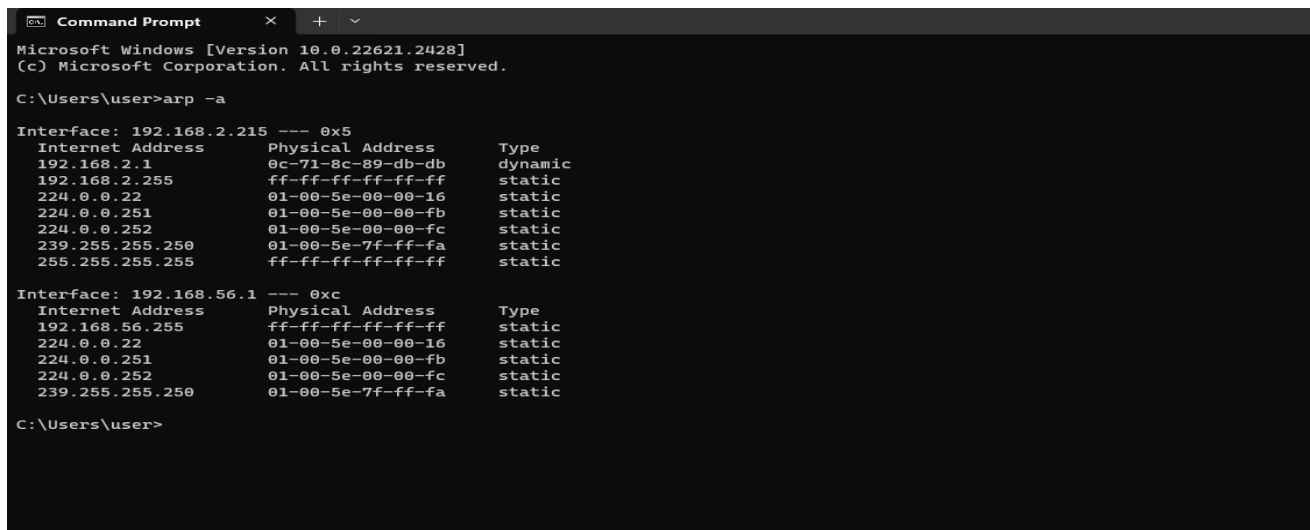
Resource: Protocol analysis using Wireshark (URL <https://en.wikipedia.org/wiki/Wireshark> last access 25<sup>th</sup> November 2023).

In terms of Protocol analysis, Wireshark use is based on various layers.

Here is the example of 7 distinct layers of the OSI model:

- Physical layer.
  - Data link layer.
  - Network layer.
  - Transport layer.
  - Session layer.
  - Presentation layer.
  - Application layer.
- 
- **Preparing for analysis: clear ARP cache and Browser History.**

This process is Start with opening a command prompt as a system administrator and use the command arp -a allow to see the IP (Internet Protocol) with the physical address.



```

Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>arp -a

Interface: 192.168.2.215 --- 0x5
    Internet Address      Physical Address      Type
    192.168.2.1           0c-71-8c-89-db-db    dynamic
    192.168.2.255         ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static

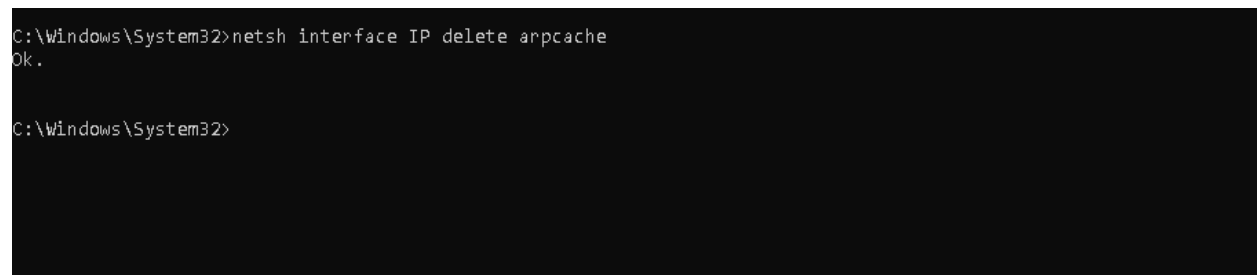
Interface: 192.168.56.1 --- 0xc
    Internet Address      Physical Address      Type
    192.168.56.255       ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static

C:\Users\user>

```

Figure 1: visible IP address with Physical location.

After that use the command “netsh interface IP delete Arp cache” to clear the ARP (Address Resolution Protocol) cache. Here is the output of clear the Arp cache:



```

C:\Windows\System32>netsh interface IP delete arpccache
Ok.

C:\Windows\System32>

```

Figure 1.1: Clear ARP cache.

### Clear the Browser history:

Clearing the browser history needs to open the chrome browser and clear the browser history from the setting section. Here is the output of clear Browser history:

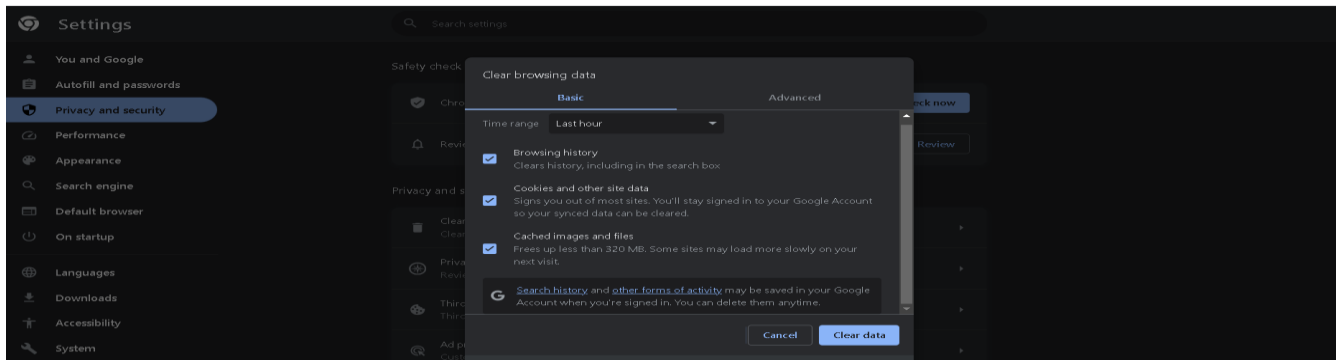


Figure 1.2: Clear Browser History.

- **Starting Packet Capture with Wireshark:**

Before starting the packet capturing using Wireshark need to check the network connection because when will open the Wireshark it will ask for the network connection. Here is the example:

```
PS C:\Users\user> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ab5:1095:ab98:ce3b%13
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix  . : lan
    Link-local IPv6 Address . . . . . : fe80::d53d:c5ca:fb29:b576%5
    IPv4 Address. . . . . : 192.168.2.215
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

PS C:\Users\user>
```

Figure 1.3: check the network connection using command ipconfig. Here is the example of live capturing the data packet using Wireshark:

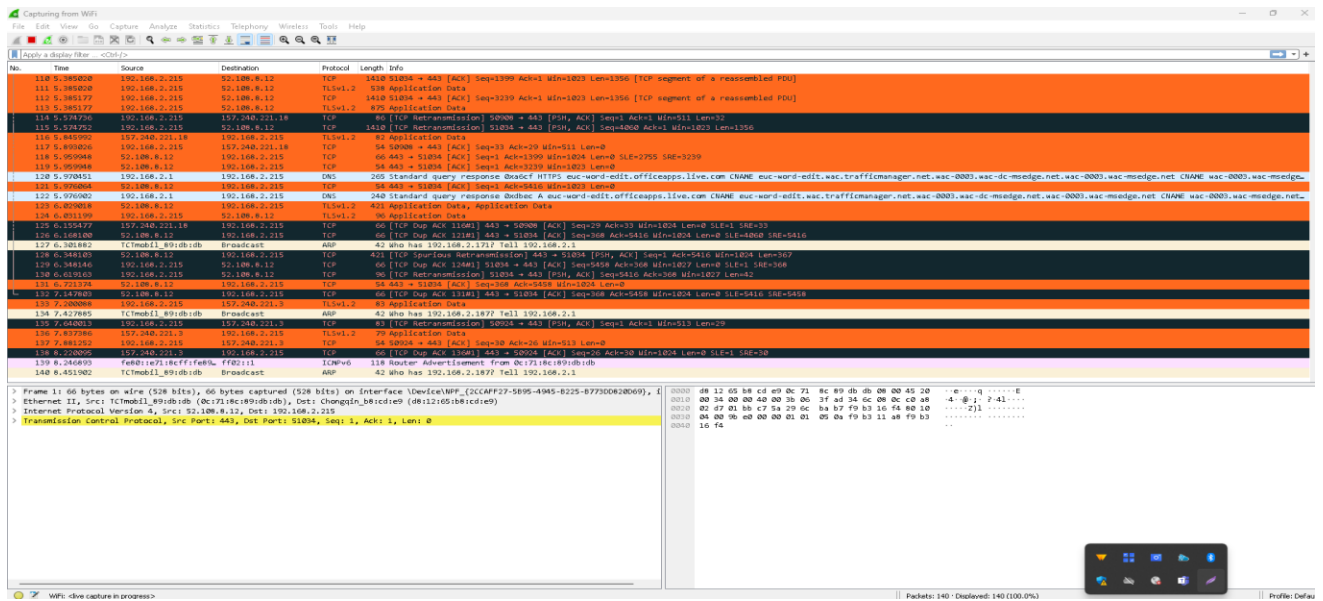


Figure 1.4: capturing Live data using Wireshark.

- **Surfing the internet for data collection:** Here is the example of surfing the internet for data collection:

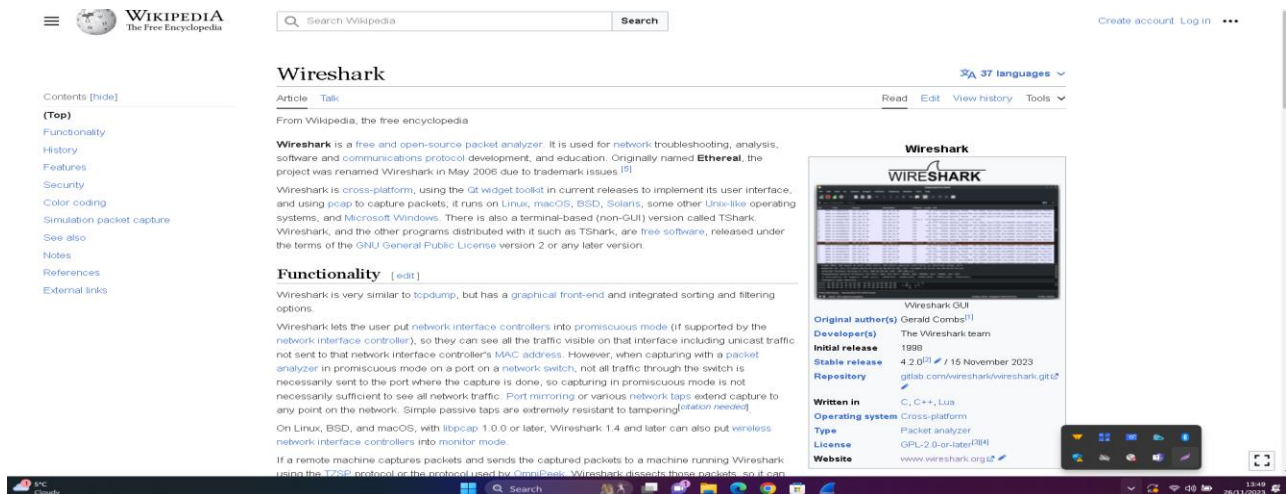


Figure 1.5: Surfing the internet.

- **Stopping packet capture and initial observation:**

Here is the brief explanation about the total amount of data was captured by Wireshark:

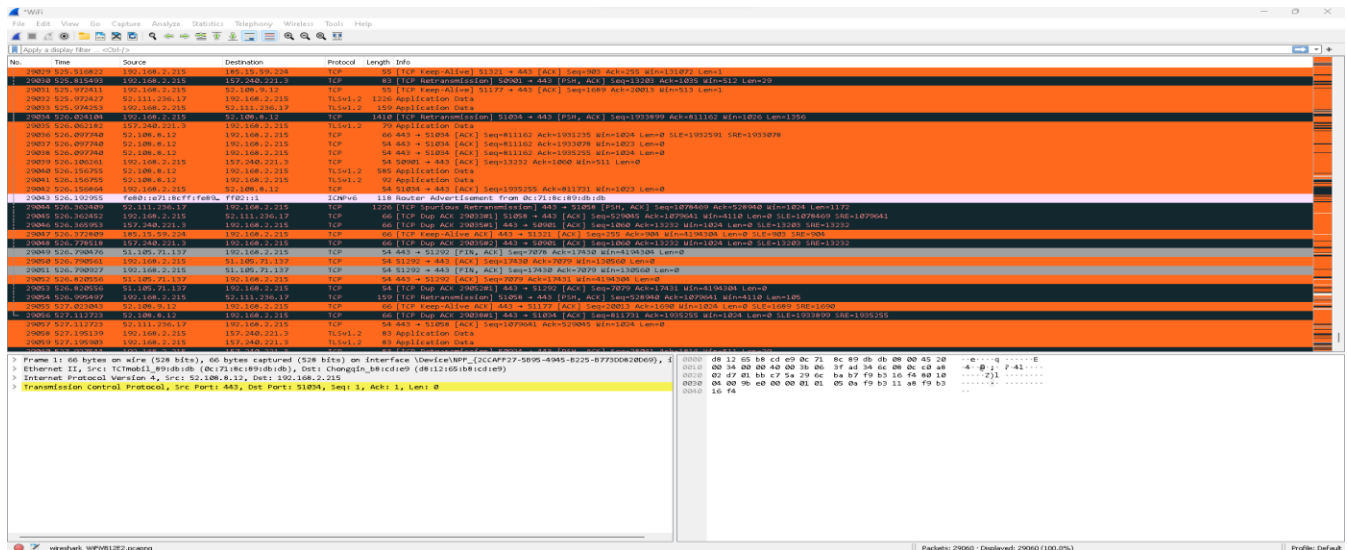


Figure 1.6: Stop the live capturing data in Wireshark display.

During the live capturing data packet, 29060k data was captured.

This is the basic explanation about Wireshark interface:

Time definition is time of capturing the packet, Source meaning is source IP and destination meaning is destination IP and the protocol meaning is the protocol name such as TCP, UDP, SSDP and ARP etc. Info showed the brief description of the packet data.

## Questions Answer:

### 2. Explanation the TCP/IP Handshake Process:

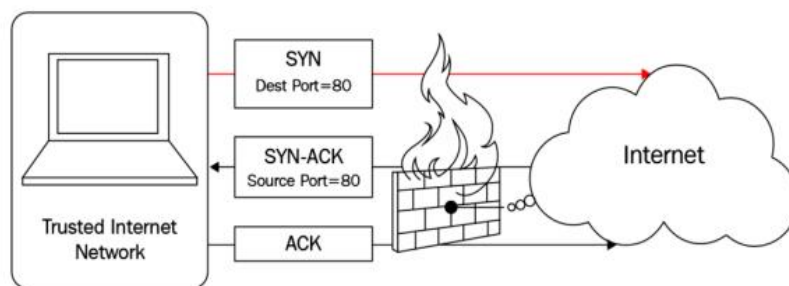


Image source: Coursework specification

This image shows a concept from computer networking related to the TCP (Transmission control protocol) three-way handshake

mechanism used to establish a TCP/IP network connection over an IP-based network. The three-way handshake process is used to process a connection between a client and a server. Here is the brief explanation how this process used to build a connection:

**SYN:** The client wants to establish a connection with a server, so it sends a SYN (synchronize) message to the server. The syn message specifies the client's initial sequence number for the data packets that it will send, and it may also specify the destination port (like port 80 for HTTP traffic).

**SYN-ACK:** Upon receiving the SYN message, the server responds with a SYN-ACK (synchronize Acknowledge) message. This message acknowledges receipt of the SYN from the client (by incrementing the sequence number by one) and includes the server's initial sequence number for the packets it will send to the client.

**ACK:** The client receives the SYN-ACK from the server and completes the three-way handshake by sending an ACK (acknowledge) message back to the server. This ACK message includes the incremented sequence number to confirm that it received the server's SYN-ACK.

The illustration also includes a firewall depicted as a brick wall with a lock on it. For example, the security system with flames could symbolize a security measure that is actively blocking or filtering the connection attempt. Firewalls are used to prevent unauthorized access to or from a private network and can be configured to allow or block specific traffic based on defined security rules.

- **Importance of packet sniffing in network analysis:**

Here is the brief explanation of how Wireshark packet sniffing significantly contribute to network analysis based on the three-way handshake process:

- **Traffic Visualization:**

Wireshark captures and visualizes all the packets throughout the network. This allows network administrator or analysis to see what type of traffic is passing through the network, which is crucial for both understanding normal network behavior and identifying anomalies.

- **Practical example with an explanation:**

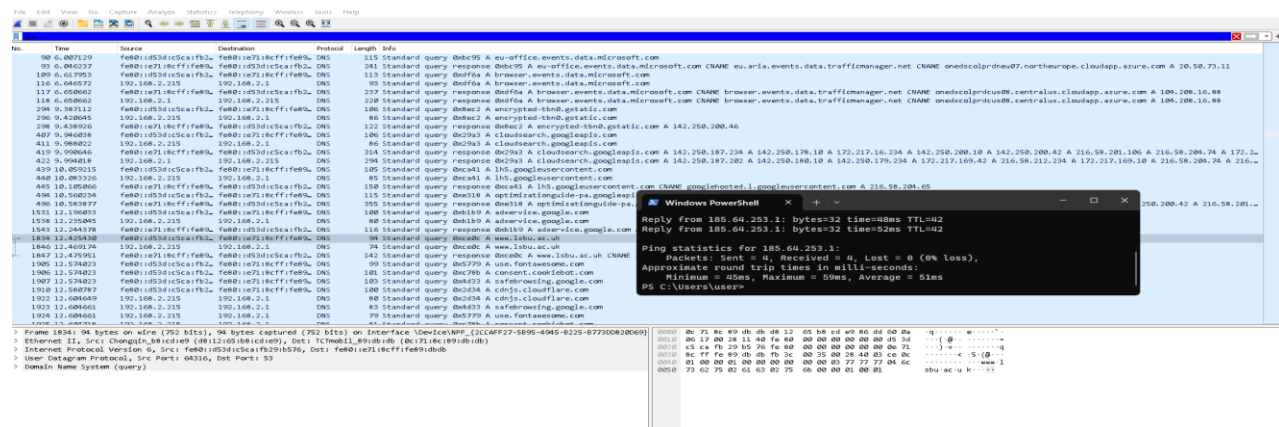


Figure 2: Traffic Visualization.

During the live capture data using Wireshark, author visited LSBU website and using the ping command in terminal get the information about IP server and after that in the Wireshark display Filter section search for protocol type DNS and got the information about the LSBU which is significantly contribute to the network analysis. In the following section, here are some more screenshots about different protocols:





Figure 2.1: Wireshark display Filters with different protocols for traffic Visualization.

#### 4. Foot Printing and it is application in cyber security:

Foot printing in cybersecurity refers to the process of collecting as much information as possible about a target system, network, or organization to find ways to infiltrate it. This is often the first step in a cyber-attack, where hackers gather publicly available information and use various tools to understand the network's structure, discover vulnerabilities, and plan their attack strategies.

- **How hackers use Wireshark for Foot Printing:**

## Network Mapping:



Hackers can use Wireshark to capture packets and analyze them to understand the network's topology. By examining the headers of packets, they can identify IP addresses, operating systems, device types, and network protocols.

### **Identifying Active machines:**

By capturing and analyzing network traffic, hackers can identify which machines are active on the network, what services they are running and if there are any insecure communication channels.

### **Sniffing for Credentials:**

Undecrypted traffic can be a goldmine for hackers. Wireshark can be used to sniff the network for unencrypted usernames and passwords, and other sensitive information.

### **Discover network services and ports:**

By analyzing traffic, Hackers can discover open ports and running services which might have known vulnerabilities that can be exploited.

- **Illustrative Example:**

Imagine a given scenario which is a company network, and it has been targeted by hackers. The hackers begin by using Wireshark to capture packets transmitted over the network. By analyzing these packets, the hackers discover that a particular server is communicating over HTTP rather than HTTPS, indicating that the data is unencrypted. After that the hackers can put more focus on the specific server and can capture more data which will help hackers to get login credentials transmitted in plain text and this is how a hacker can get access to the server. Here is a provided screenshot showing how hackers can access to the server on specific network:

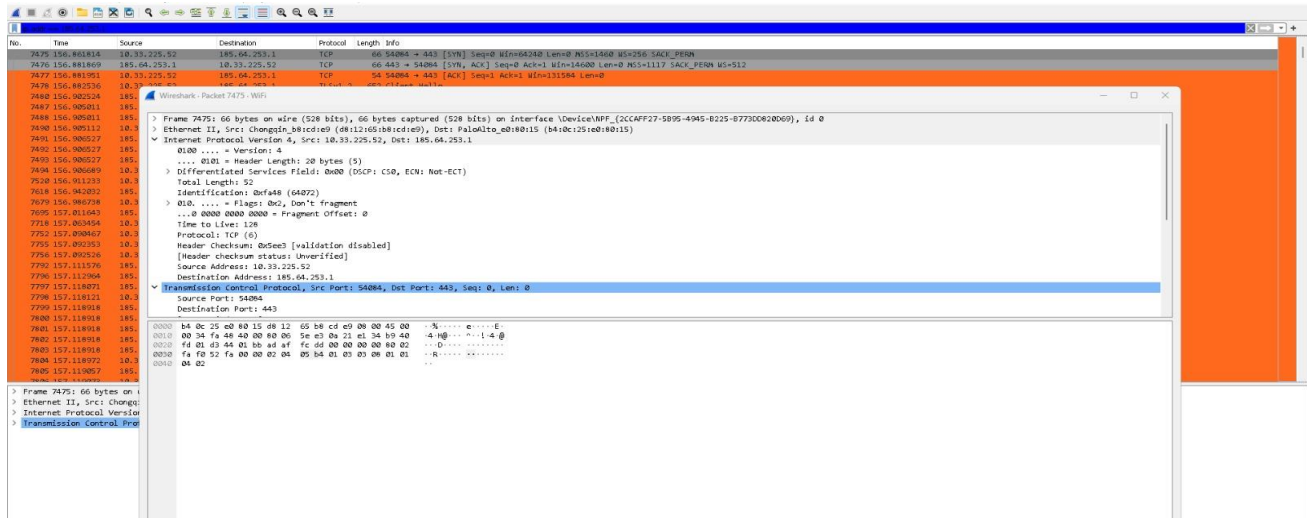


Figure 2.2: Illustrative example of foot printing.

Imagine this LSBU address is targeted by hackers. Hackers can use Wireshark on specific networks and can capture more data and after that analyze those data. A hacker can get sensitive information such as login details as a text in the packets. At the same time analyzing those sender IP and receiver IP, port number hacker can get an idea about this server, and this is how a hacker use the Wireshark and this is called foot printing.

## 5. Explanation of the ARP Broadcast on a Network.

Address Resolution Protocol (ARP) spoofing is a type of attack in which an attacker sends falsified ARP messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker has linked their MAC address to an IP address, they can begin intercepting data that was intended for that IP address.

- **How ARP spoofing works:**

### ARP Basics:

Arp is used to convert an IP address into a physical MAC address in a local area network. When a device wants to communicate

with another device on the same network, it sends an ARP request to find out the MAC address associated with the desired IP address.

### **Spoofing Process:**

In an ARP spoofing attack, the attackers send fake ARP messages to a local area network. These messages associated the attacker's MAC address with the IP address of a legitimate network member, such as a server or a client.

### **Traffic interception:**

Due to this spoofing, traffic meant for the legitimate IP address is now sent to the attacker. This allows the attacker to intercept, modify, or block data before it reaches its intended destination.

- **Using Wireshark for ARP spoofing:**

While Wireshark itself is not a tool for launching ARP spoofing attack, it can be used to monitor and analyze network traffic, including ARP spoofing activities. Here is the following section showed how ARP spoofing works in Wireshark:

**Detection of ARP Spoofing:** Wireshark can capture and display all ARP packets on the network. By examining these packets, one can detect unusual ARP responses or requests that might indicate ARP spoofing. Here in the provided screenshot showing how ARP spoofing work in Wireshark:

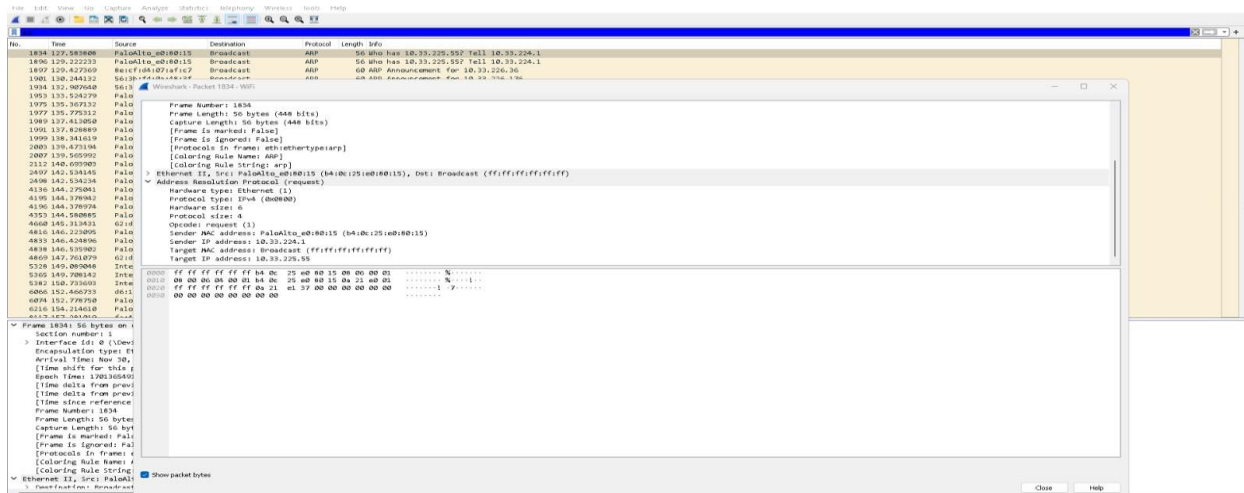


Figure 2.3: ARP packet capture and spoofing with Wireshark.

In this provided screenshot it is truly clear how Wireshark is using ARP spoofing work because under the ARP section it is showing the sender IP and MAC address, and this sender is asking for the target MAC address.

## 6. Detailed Analysis with Wireshark:

Wireshark is a free packet capturing tool used for analyzing data captured based on the different networks. Here is the explanation that how Wireshark can be used to monitor threats:

- **Monitoring network threats with Wireshark:**

Wireshark can be used to monitor threats in a network environment. It is a powerful tool for analyzing network traffic, which can reveal potential security threats. However, it is important to note that Wireshark is primarily a network analysis tool, and not a dedicated security monitoring solution. Its effectiveness in threat monitoring depends on the skill and experience of the user in interpreting the network data. Here are the three monitoring threats with technical explanations and example:

### Proactive monitoring:

This involves predicting and avoiding risks before they arise. Regular network scans, vulnerability assessments, and the usage of intrusion detection systems (IDS) to uncover security issues are all part of proactive monitoring.

## Technical explanation:

Proactive monitoring sometimes involves setting up Wireshark to capture and network traffic simultaneously or during specific periods. Analysis looks for unusual patterns that could indicate security threats, such as unusual spikes in traffic, unrecognized protocols, or traffic from suspicious IP addresses.

## Example:

By using this display filters, A user can identify the monitoring threats for example 'frame.len > 1500' can indicate unusually large packets, which could indicate data exfiltration.

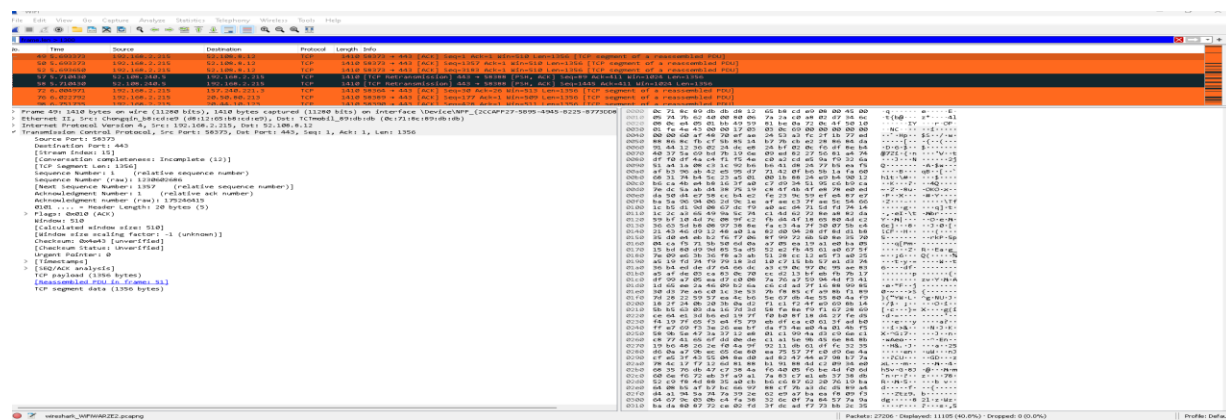


Figure 2.4: Unusual large packets.

Look for unusual DNS patterns, which can be helpful for unusual monitoring threats:

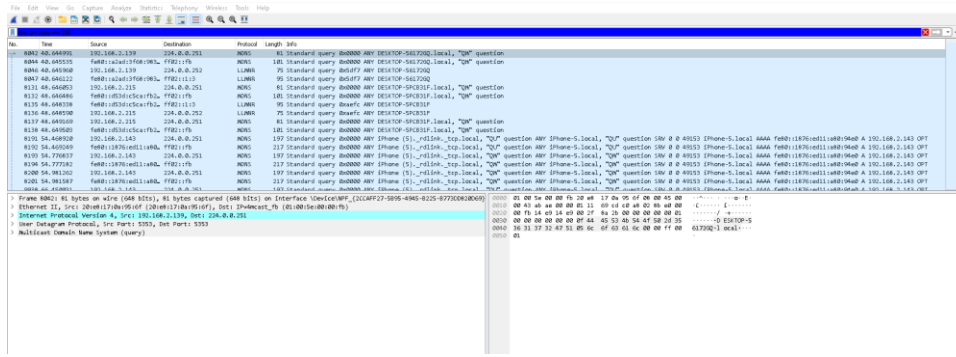


Figure 2.5: Unusual DNS request

## Reactive Monitoring:

This strategy addresses handling dangers once they have materialized. It entails actions like assessing the effect of an assault, carrying out forensic investigation, and putting preventative measures in place.

## Technical Explanations:

In reactive monitoring, Wireshark can be used to analyze network traffic logs after a security incident has been detected. This helps understand the attack's nature, the extent of the compromise and the method of entry.

## Example:

Searching for malware signatures in network traffic using Wireshark involves looking for patterns or characteristics that match known signatures associated with malicious activities. Here is some example HTTP requests and responses, search for known malicious domain for unusual patterns:

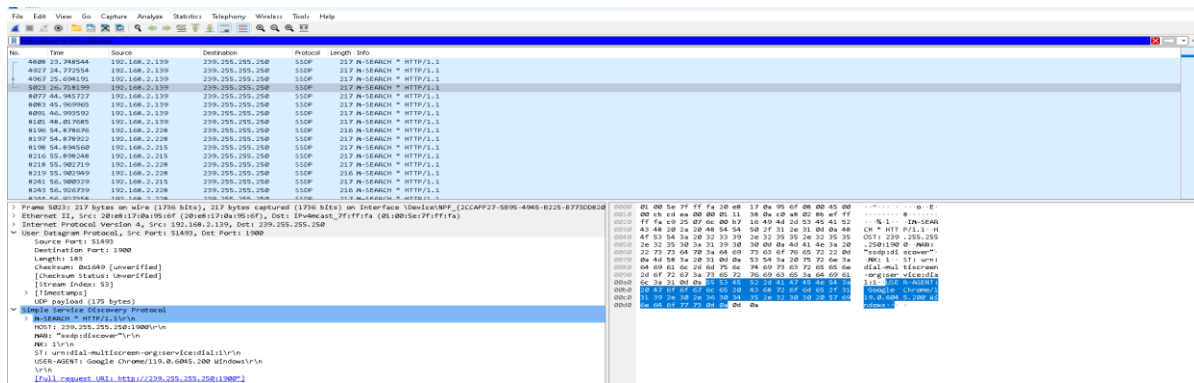


Figure 2.6: Inspect HTTP traffic.

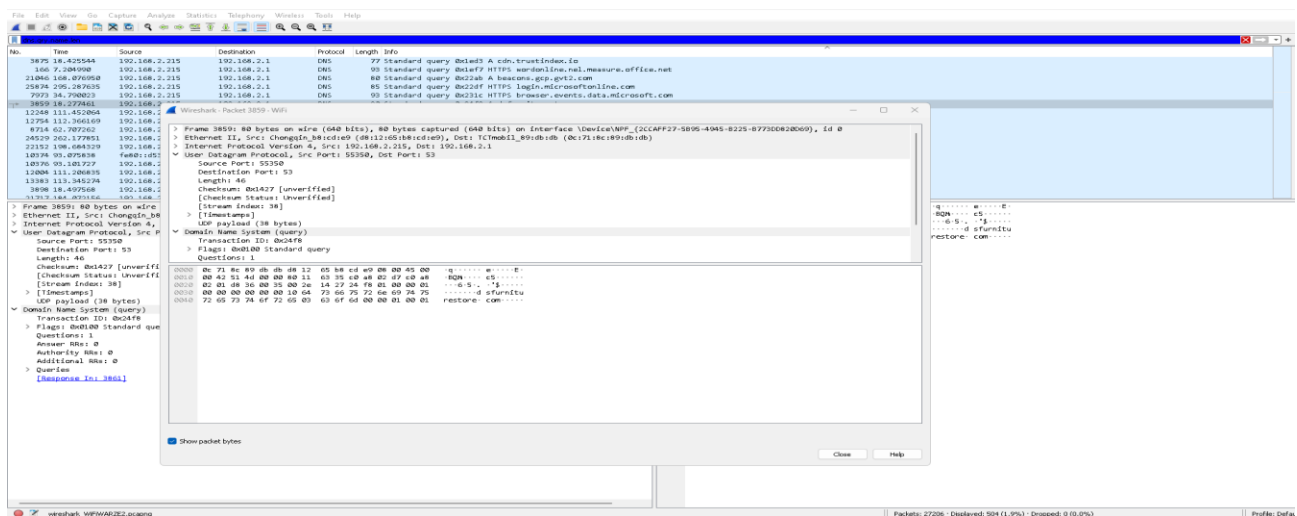


Figure 2.7: search for known malicious domain.

## Active monitoring:

Active Monitoring is a continuous process of scanning and assessing the network to detect and respond to threats in real-time. Active monitoring is a combined element of both Proactive and active monitoring.

## 7. Troubleshoot Network Issues:

Wireshark is a highly effective tool for network troubleshooting as it can capture and analyze network traffic in real time and due to all those functionalities, it allows network administrator to identify

a various problem of network for example from performance problems to security breaches.

In the following part, I am going to do the technical explanation and practical example that how Wireshark used to troubleshoot the network:

## • Packet Analysis:

Wireshark captures every packet that travels through the network, allowing for detailed inspection of each packet. This is crucial for identifying problems such as lost packets, delays, or malformed packets.

Example:

In the following figures, use the display filters 'tcp.analysis.duplicate\_ack' to check is there any packet loss or not.

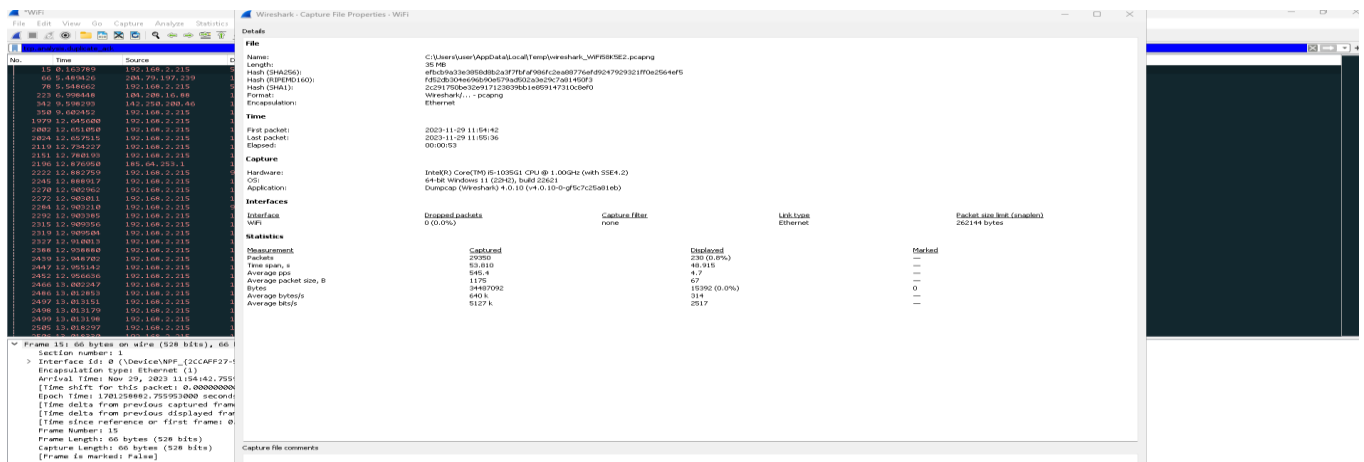


Figure 2.8: Packet Analysis to check any packet loss.

## • Protocol analysis:

Wireshark supports a wide range of protocols and can decode and display the contents of packets using these protocols. This



helps in identifying misconfiguration or issues specific to certain protocols.

## Example:

For example, when running the Wireshark interface, it shows several types of protocols. The figure provided is captured from Wi-Fi based network and checking the handshake process and if there is any handshake process failing it could indicate a protocol mismatch or configuration error.

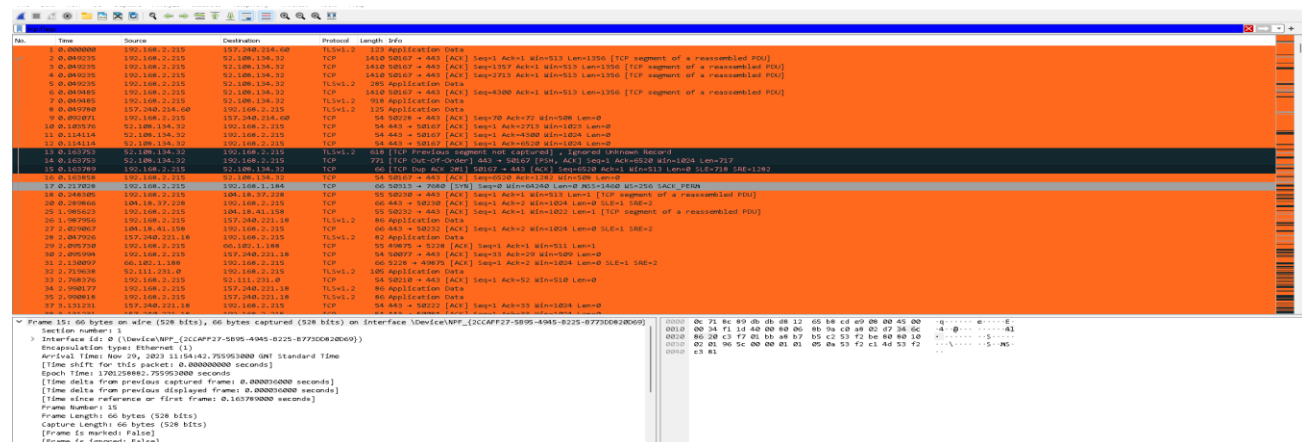


Figure 2.9: Check Three-way handshake process using different display filters.

In the provided screenshot, first use the display filter 'tcp.flags' to check that which packets involves in the tcp handshake process and after that using the display filter 'tcp.flags.syn == 1 or tcp.flags.ack == 1' to check where the SYN (Synchronize) flag is set and where the ACK (Acknowledgement) filter is set. The TCP handshake involves the exchange of SYN and ACK flags between the server and client.

- **Identifying Traffic Patterns:**

By analyzing traffic patterns, Wireshark can help identify unusual spikes in traffic or the presence of non-standard protocols, which

could be symptomatic of a network instruction or a malfunctioning application.

## Example:

Identifying traffic patterns in Wireshark involves using display filters to focus on specific types of network traffic. Here is some screenshot provided that used in the Wireshark display Filters for identifying traffic patterns:

## Filter by icmpv6 protocol:

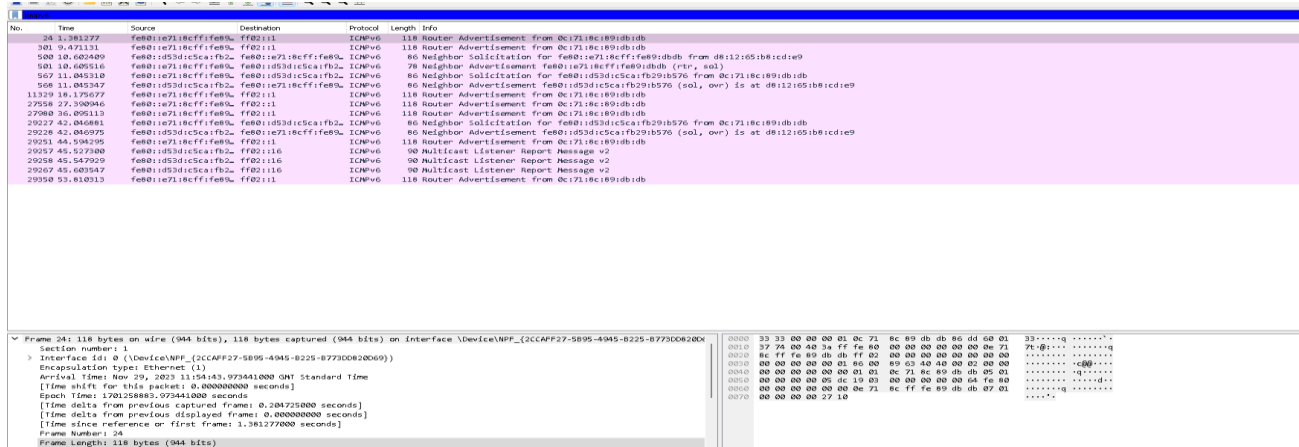


Figure 3.00: use the display filter icmpv6 to check traffic patterns.

## Filter by IP address:

In the terminal, using ping www.lsbu.ac.uk A user can get the IP and using this IP in the Wireshark display filters to check that it was captured or not.

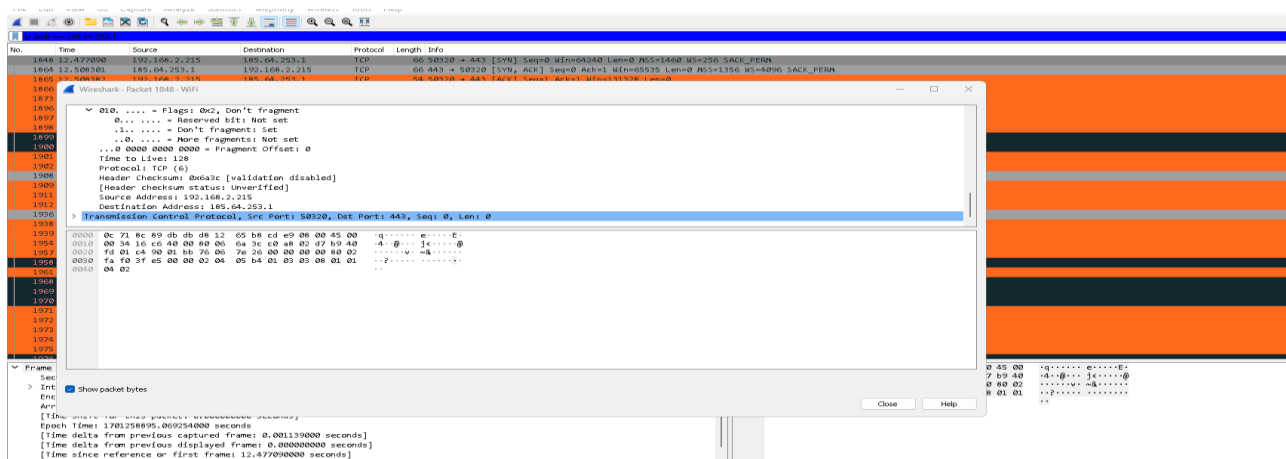


Figure 3.01: Use the specific IP address on display filters to analyze specific data packets.

By analyzing packet data, Wireshark can help identify the source of network problems. This could include issues like packet loss, excessive latency, or unusual traffic patterns that might indicate a network malfunctioning hardware. In the following part, there are some examples that how Wireshark use for troubleshooting the network:

- **Practical example with an explanation:**

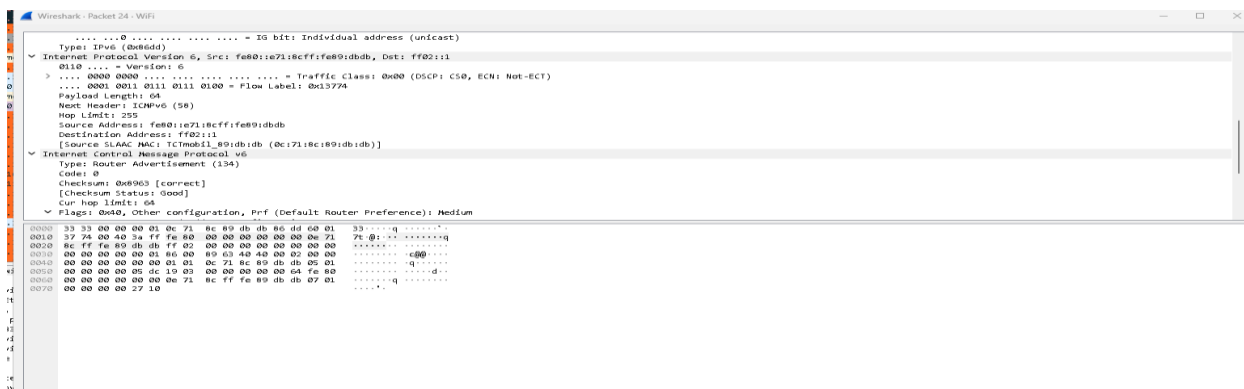


Figure 3.02: Troubleshooting network Issues.

Analyzing one data packet for troubleshooting in Wireshark is visible under the ICMP (Internet Control Message Protocol) section about the network issue. Though this provided data packet shows the checksum and other connection is good and verified. But if there is any problem, in this section will show the

issues such as unverified then its need to be troubleshoot and this is how Wireshark helps network analyzer to find network issues.

- **Security Analysis:**

Wireshark can be used to detect security threats such as malware communication, unauthorized data exfoliation, or suspicious traffic patterns. By examining packet contents, it is possible to uncover potential security breaches or attacks in progress.

- **Practical example with an explanation:**

```

> Frame 4: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 bits) on Interface \Device\NPF_{2CCAFF27-5895-4945-B225-0773D0628069}, Id 0
> Ethernet II, Src: Chonglin_Nic (08:12:45:18:cde:09), Dst: Tcmobli_g02db:db (0c:71:bc:c9:db:db)
> Internet Protocol Version 4, Src: 192.168.2.215, Dst: 52.100.134.32
> Transmission Control Protocol, Src Port: 50167, Dst Port: 443, Seq: 2713, Ack: 1, Len: 1356

0100 76 df 19 f2 e3 17 07 6a d1 f6 6d b9 55 92 11 f6 8.....j..mU...
0110 57 f6 7d 48 01 48 e6 13 0e 0a c7 3c 95 76 df b4 8j}H...+...
0120 3e a5 15 f5 a0 f9 2c b4 96 d7 a7 ba f5 a5 fe a5 }.....+.....
0130 6e f7 c8 e7 1b 46 c5 f5 11 c0 08 62 59 a9 79 .....E...-bV...
0140 a7 87 6e 67 e7 9d 68 21 f5 29 3f 7e 2b b2 a1 78 ..ng<L..}l...+...
0150 2f cd ad 58 6d ad d8 e2 f3 a8 dd b4 00 c2 4e db />K...+...B...
0160 ea 65 b7 52 68 33 43 66 5a c8 42 78 95 6c cc 78 ..R>K 2...L...
0170 a5 01 a7 ca 11 3c 6a 42 47 e2 32 93 a1 96 b2 68 .....J 0 2...h
0180 42 d1 e8 8b bf d8 8e 7e 6c 15 29 e4 c8 c2 5b f7 B.....L...+...
0190 b6 06 cc f7 a6 a3 a5 b0 fd cd 08 3a f9 28 c2 a5 .....C...+...
01a0 6f fc e4 33 3c 69 e5 00 d7 66 a8 3e 2b c1 a9 59 o-3&...f>+...Y
01b0 75 67 f0 c7 83 9f eb b0 d3 2b 74 85 1a b0 8f 0p.....+...+...
01c0 e2 da f1 46 a6 3b a5 6e 53 65 e9 79 d3 09 2c 1c ..F..jE Se...y...
01d0 69 ae 2d 1d 0a 0b 90 7a 1c 36 04 f0 b7 79 06 52 1.....2..6...y/2
01e0 41 a2 33 4c f2 1c f6 bf 86 0a 56 67 07 a9 0b b6 A&L.....+ng>...
01f0 d8 89 08 4b b0 89 f5 40 e5 4a fe cc 3f b7 3b c0 ...K...Q..}...?..
0200 00 e3 b9 08 15 17 38 fd 62 ac f9 28 f8 04 67 db .....8..b...+...g
0210 40 09 42 16 03 67 a7 7d 5f a7 d9 bb 8b 40 af 9e I>+<g>...+...@...
0220 c7 e5 99 74 8f a6 a1 f9 0e 0a 83 23 35 04 25 e5 ...E.....J...8...

```

Figure 3.03: Security analysis using Wireshark on specific data packets.

For example, hackers are analyzing that above data packet and from that packet he can get a many information such as source IP, destination IP, MAC address and based on that information a hacker can do further research and analyze and can target a specific network which will be the reason of security threats.

## 8. Using Wireshark Provide a Figure:

- Display all TCP and UDP packets:

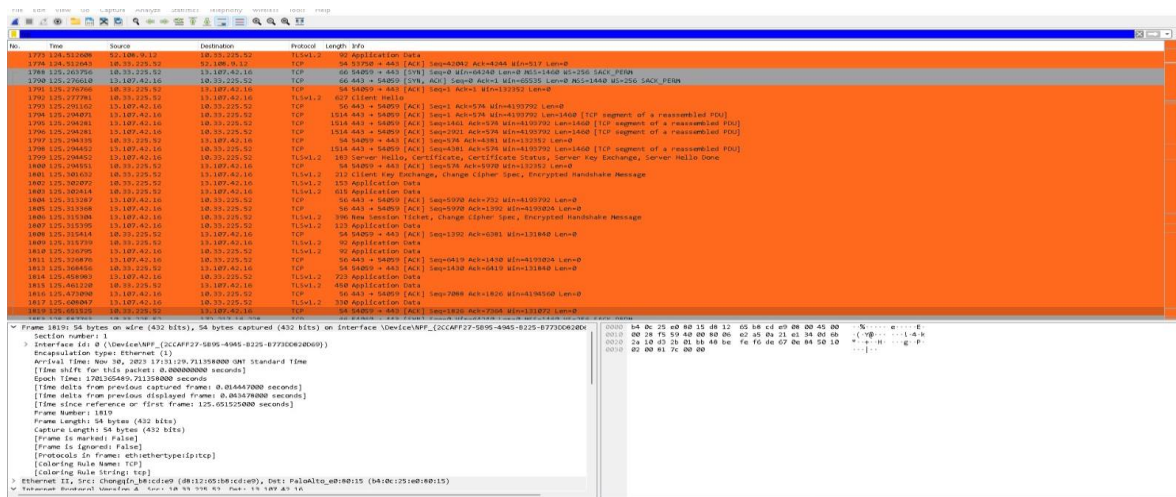


Figure 3.04: Display all TCP packets.

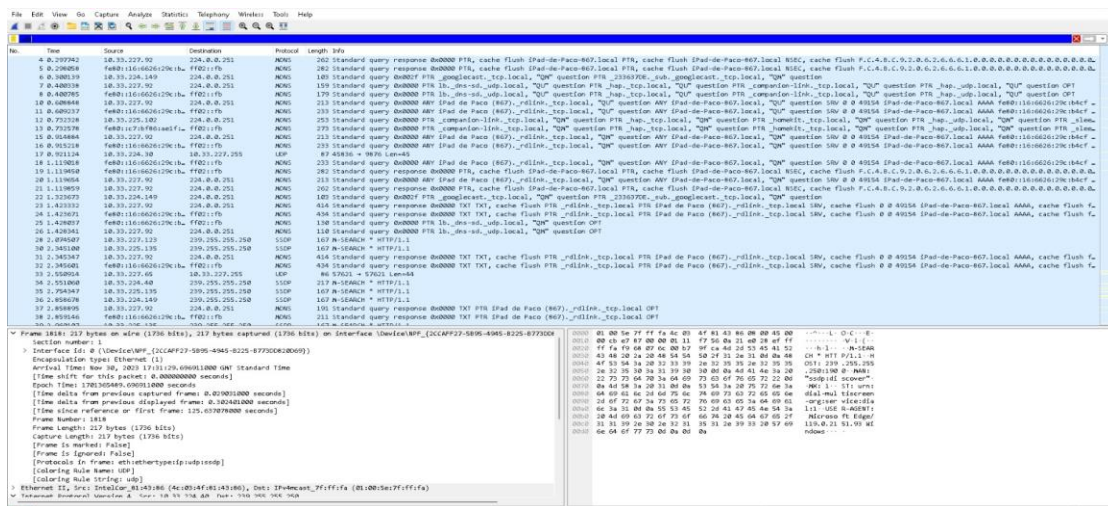


Figure 3.05: Display all UDP packets.

- Display packets from specific IP:

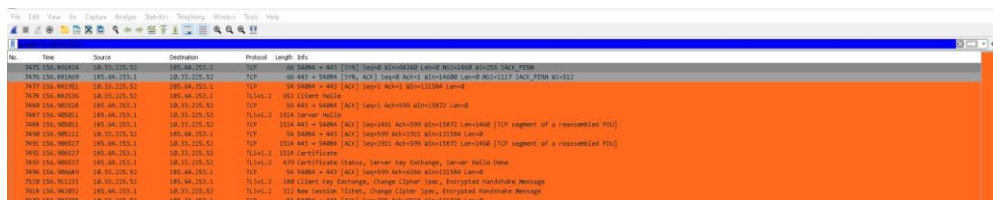


Figure 3.06: display filter from specific IP.

- Display packets from multiple IPs:



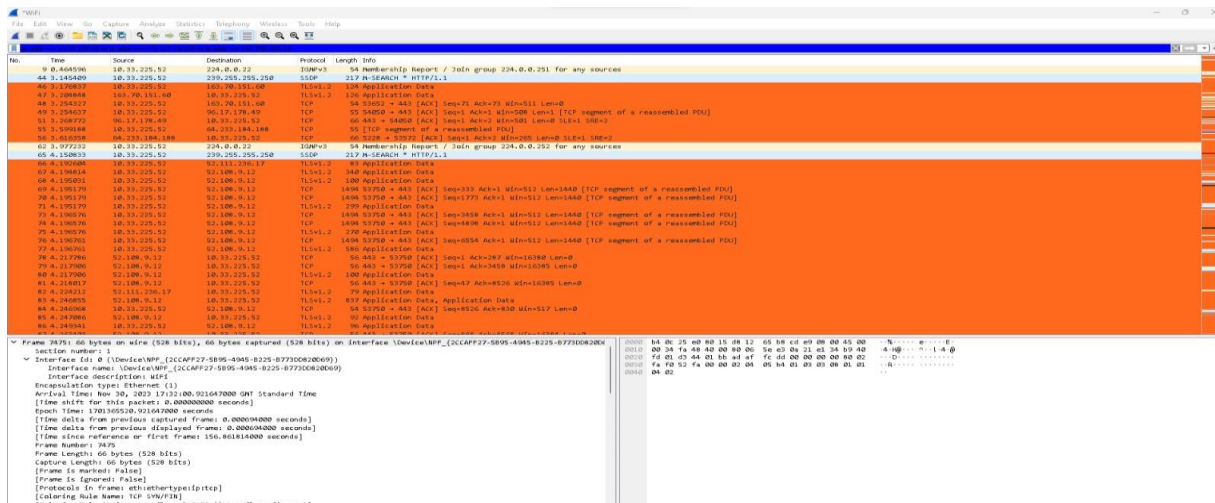


Figure 3.07: Display filter from multiple IPS.

- **Exclude an IP address:**

The following figure shows the excluded IP address with the display filter not `'ip.addr == 10.33.225.52'`.

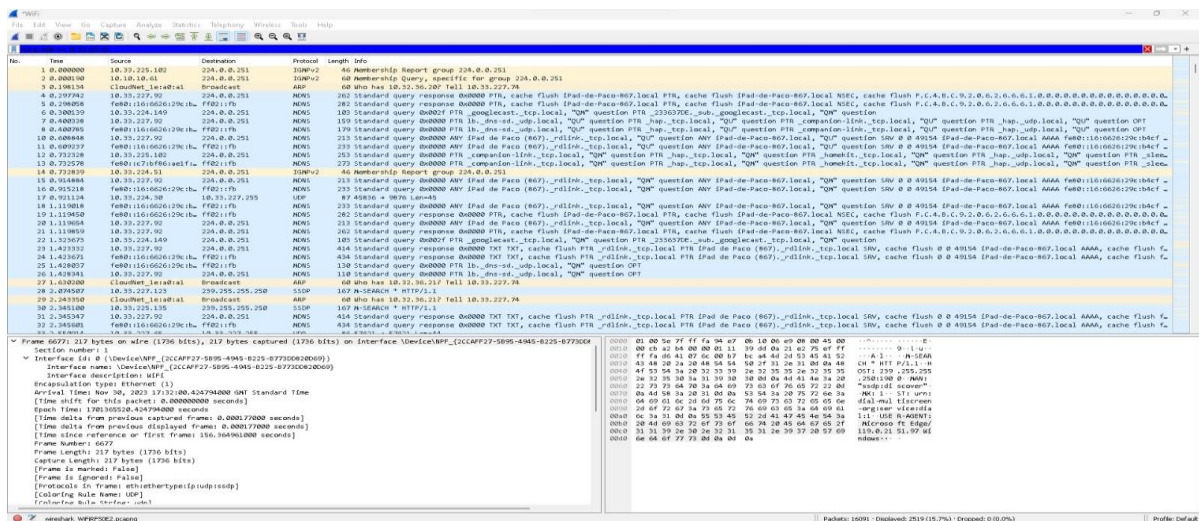


Figure 3.08: Exclude an IP address.

- **Display URL:**

This general filter allows to capture URLs in all protocols.

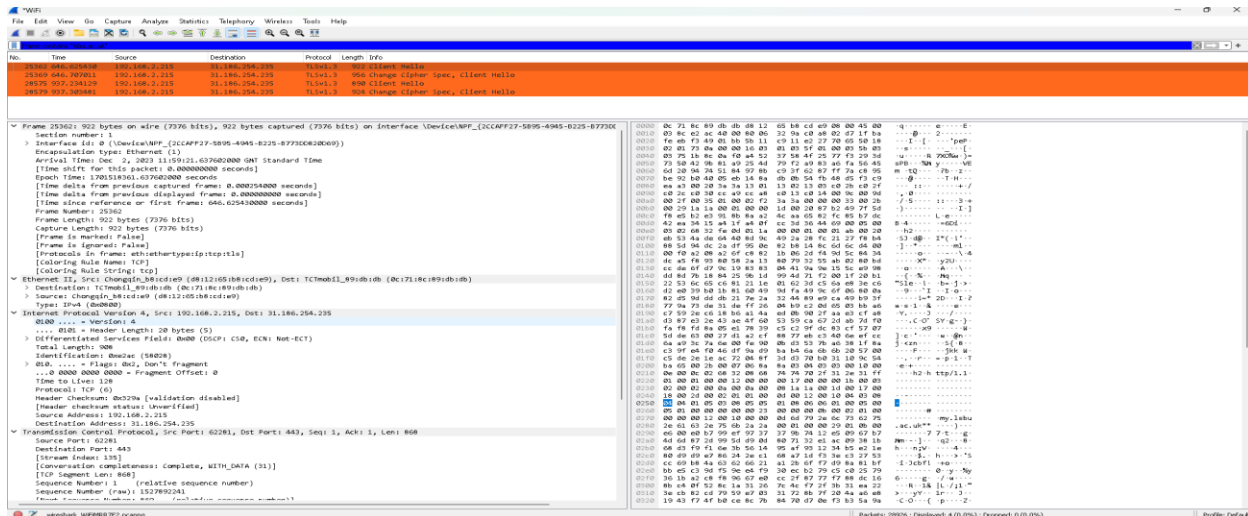


Figure 3.09: Display URL.

- **Show the TCP handshake Process.**

In the process of TCP handshake process First we need to identify the client IP and server IP and after that search in display filters such as 'ip.addr == 192.168.2.215 and ip.addr == 172.217.169.10 and tcp' which will show specifically which data packet is involved in this process with the above specific client and server IP. Here is the example:

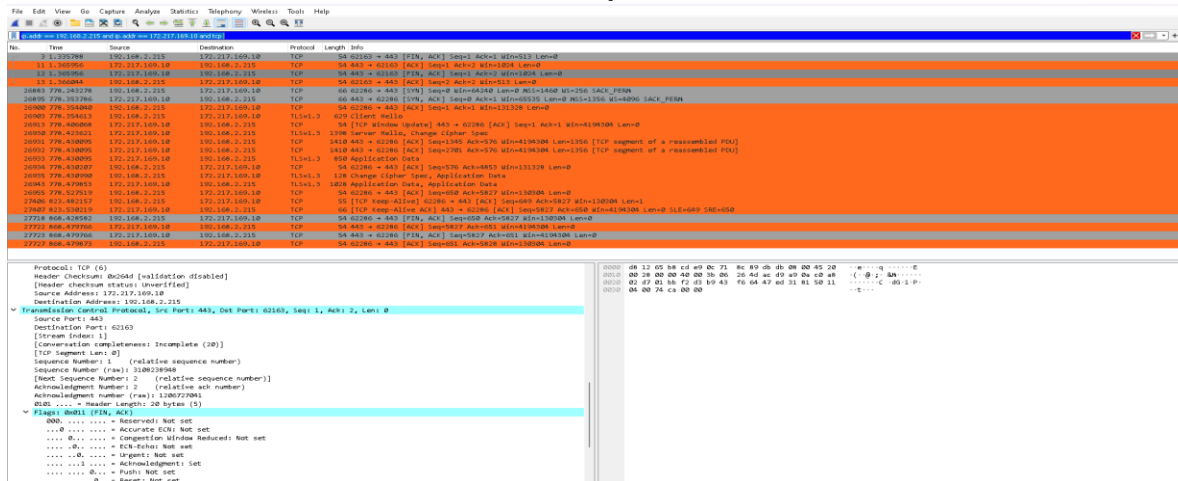


Figure 4.00: Three-way handshake process.

- **Show TCP header Format.**



Figure 4.01: TCP header format.

In this above figure, under the Transmission control protocol showing the header information and format such as src port, dst port, seq, ack and Len etc.

- **Display TCP error packets.**

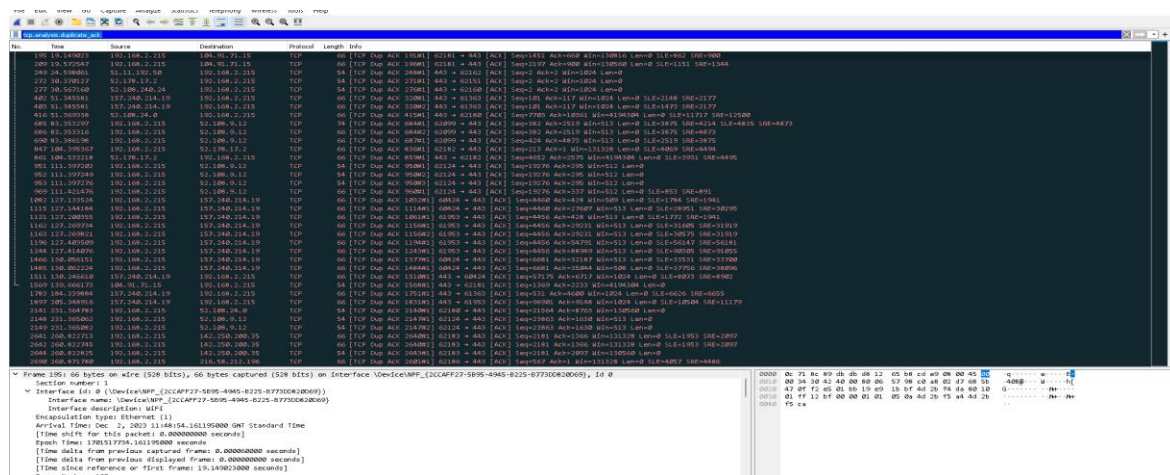


Figure 4.02: Duplicate TCP error packets.

Duplicate acknowledgement can indicate issues with packet loss or out-of-order delivery.

- **Measure the Latency.**

Measuring latency involves determining the time it takes for data to travel from one point to another in a network. Here is the example as in the following figure showing based on the specific



## Client Ip and server IP in TCP protocol type under the Timestamps section:

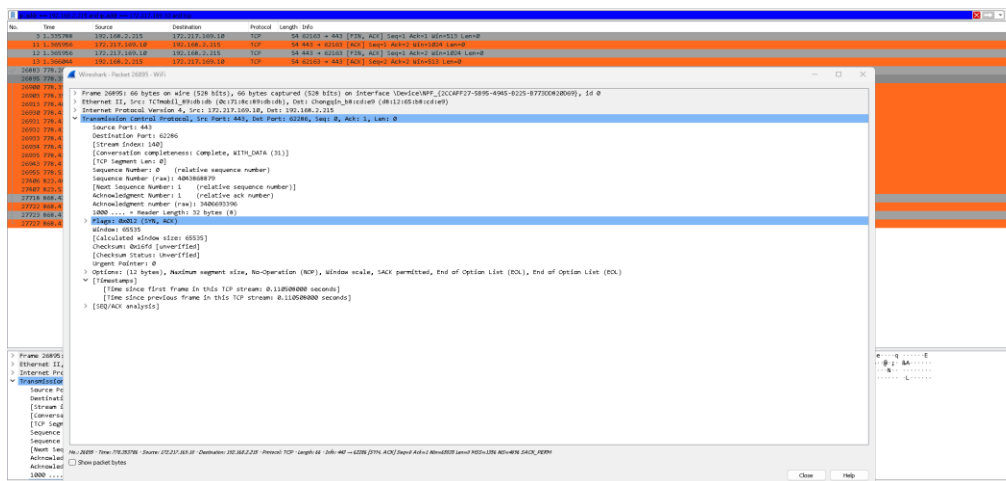


Figure 4.03: Measure the latency.

Latency = 0.110508000 s + 0.110508000 s = 0.221016 seconds.

- **Measure the Throughput.**

Measuring Throughput involves determining the amount of data transferred over a network during a specific period.

Here is the example:

Throughput = Total Data size/Time.

Throughput = 60000 bytes / 0.200 s = 300,000 B/s

We can convert B/s to Mbit/s by multiply 8.

## 9. Advanced Wireshark Function:

Logical operators are used to create complex display filters for packet analysis. Display filter helps to focus on specific network traffic based on various criteria.

- **Applying 3 Logical Operations in Display Filters.**

First logical operator is used here in the following figure based on specific source IP 192.168.2.215 and destination IP 172.217.169.10 using '&&' logical operator.

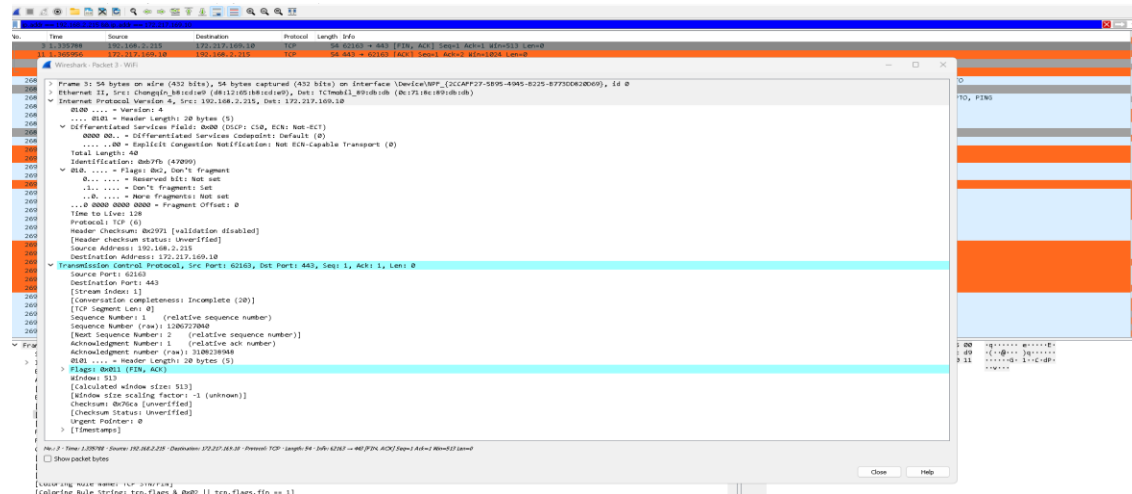


Figure 4.04: And logical operator.

Secondly use the || operator in the display filter. In the following figure displaying the TCP packets where source Port is either 62163 || 443:

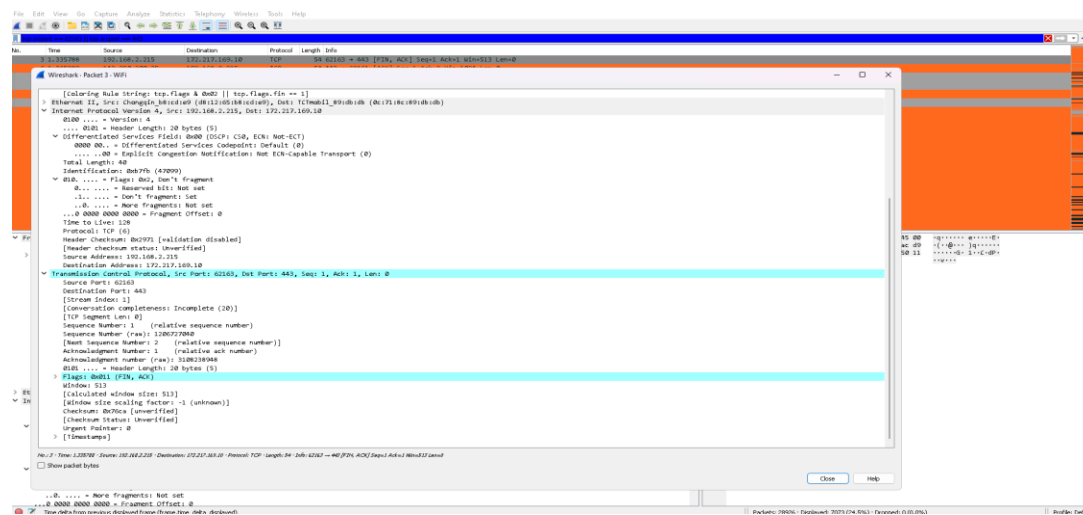


Figure 4.05: Use the (||) operator.

Thirdly use the not operator displaying packets that are not TCP type.

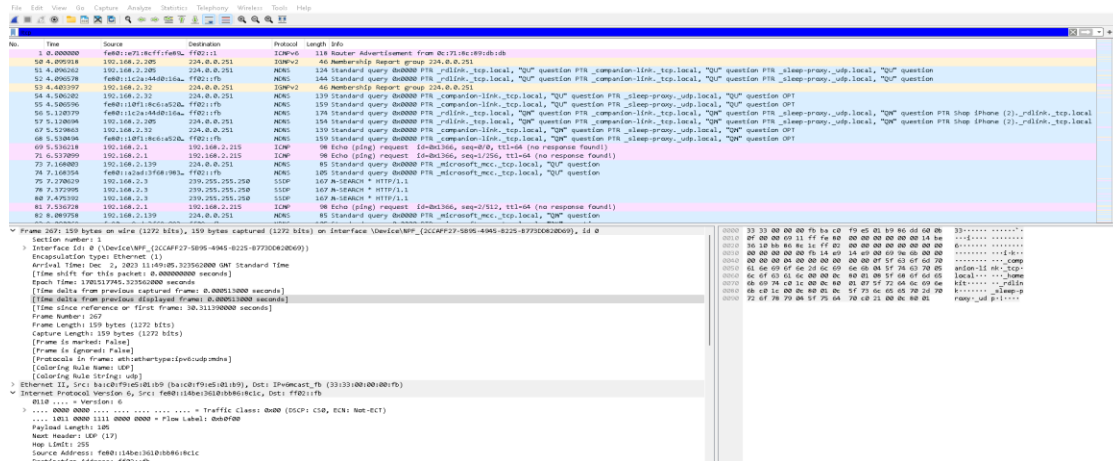


Figure 4.06: use (!) operator.

## 10. Understanding and configuring RIP (Routing Information Protocol).

The routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employs the hop count as a routing metric. RIP is used for managing router information within a local network or a group of networks. It uses a simple algorithm to determine the best route for data packets.

### • Explanation of RIP protocol.

### Hop count as a metric:

RIP uses the hop count as the metric for path selection. Each hop in a network is counted as a single metric, and the path with the least number of hops to a destination is considered the best path.

### Limit of Hops:

RIP limits the number of hops to 15, which prevents routing loops. Any route discovered with a hop count of 16 or more is considered unreachable.

### Timers:

RIP uses various timers to regulate its performance, including an update timer (every 30 seconds), invalid timers, hold down timer and flush timer.

- Step-by-Step network Configuration guide.
- In this part, we configured RIP (Routing Information Protocol) using cisco packet tracer. So, before starting anything we did use 4 end devices for 2 different network like how we did in the tutorial class but in the class, we did use static Ip but here we use RIP. Here is the brief explanation step by step:
- Total end devices we use 4 PC's, 2 switches, and 2 routers and we connected them using connectors and after that we give them different IP (Internet Protocol) addresses.
- Here is the brief explanation about different network used IP and default Gateway:

First network:

Pc 0 IP address is 192.168.1.2 and Default Gateway 192.168.1.4

Pc 1 IP address is 192.168.1.3 and Default Gateway is 192.168.1.4

And the network is for these end devices is 192.168.1.0

Second network:

Pc 2 Ip address 192.168.2.2 and default Gateway is 192.168.2.4

Pc 3 IP address 192.168.2.3 and default gateway is 192.168.2.4

And the network IP is 192.168.2.0

Router IP and network address:

Router Network address 192.168.3.0

Router 0 IP is 192.168.3.2

Router 1 IP is 192.168.3.3

This first router relates to the first network through Default Gateway 192.168.1.4. and after that we configure the RIP.

Here is the example of configure RIP for router 0:

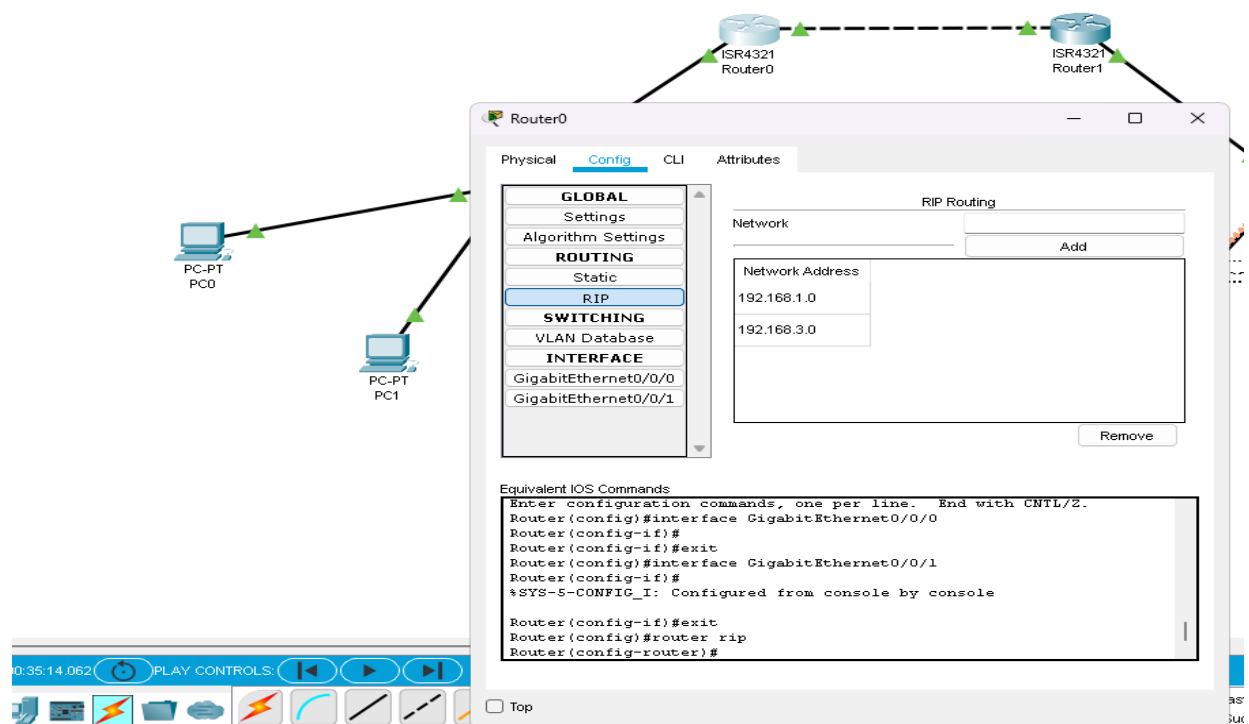
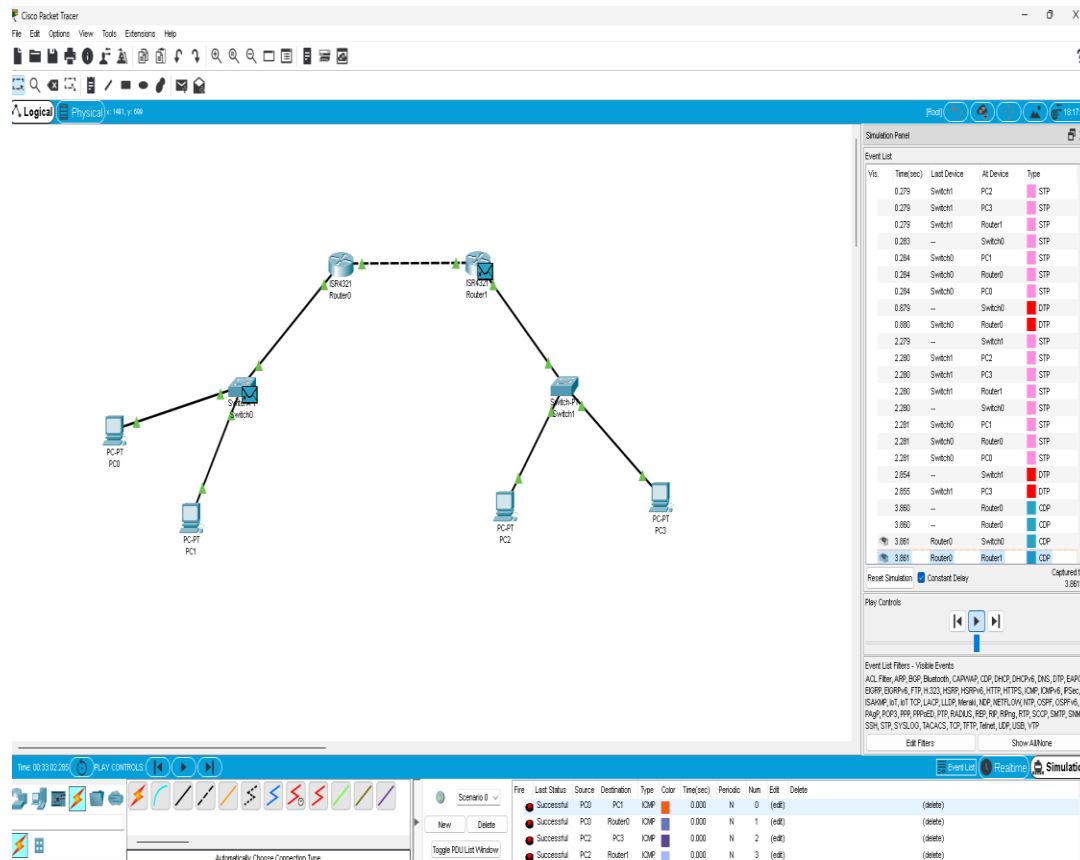






Figure 4.07: RIP configuration for Router 0.

The second router is connected with the second network by default gateway 192.168.2.4. After that, we configure the RIP for the second router. Here is the example:

This is how we connected devices from different networks and here is the final output after completing all the configuration:



ire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	Router0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	Router1	ICMP		0.000	N	3	(edit)	(delete)

4.09: packets send successfully from one network to another.

Here we can see that all the packets were sent successfully from one end device to another device in a different network.

## 11. References.

1. Wireshark official website (URL <https://www.wireshark.org/> last access 26<sup>th</sup> November 2023).
2. Wireshark user guide (URL <https://www.wireshark.org/> last access 26<sup>th</sup> November 2023).
3. TCP/IP guide (URL <http://www.tcpipguide.com/> last access 26<sup>th</sup> November 2023)
4. Network analysis by Wireshark (URL <http://www.tcpipguide.com/> last access 26<sup>th</sup> November).
5. what is foot printing and how does it work? (URL <https://www.techtarget.com/searchsecurity/definition/footprinting> last access 26<sup>th</sup> November 2023).
6. Cisco packet tracer (URL <https://www.netacad.com/> last access 27<sup>th</sup> November 2023).
7. RIP protocol explained (URL <https://www.ciscopress.com/articles/article.asp?p=24090> last access 27<sup>th</sup> November 2023).
8. Configuring static network (URL [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/unicast/503\\_u1\\_2/nexus3000\\_unicast\\_config\\_gd\\_503\\_u1\\_2/13\\_route.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/unicast/503_u1_2/nexus3000_unicast_config_gd_503_u1_2/13_route.html) last access 29<sup>th</sup> of November 2023)

9. Flush ARP cache Windows (URL <https://www.technipages.com/windows-10-flush-arp-cache/> last access 26<sup>th</sup> November)
10. TCP three-way handshake Process (URL <https://www.geeksforgeeks.org/tcp-3-way-handshake-process/> last access 1<sup>st</sup> December 2023).
11. Measuring network performance (URL <https://accedian.com/blog/measuring-network-performance-latency-throughput-packet-loss/> last access 2<sup>nd</sup> December 2023).
12. Address Resolution Protocol ( URL <https://www.techtarget.com/searchnetworking/definition/Address-Resolution-Protocol-ARP> last access 3<sup>rd</sup> December 2023).
13. RIP configuration (URL [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html) last access 4<sup>th</sup> December 2023).



