

Name: Yash Dave

Branch: TE-IT-A

Roll No: 18

## EXPERIMENT 7

**Aim:** Study of packet sniffer tools Wireshark,- 1. Observer performance in promiscuous as well as non-promiscuous mode. 2. Show the packets can be traced based on different filters

**Learning Objective:** Students will be able to:

### 1. Observer Performance Evaluation:

- Understand the difference between promiscuous and non-promiscuous mode in packet sniffers.
- Learn how to configure Wireshark to operate in both modes.
- Evaluate and compare the performance and capabilities of Wireshark in these modes.

### 2. Packet Tracing and Filtering:

- Learn how to set up and apply filters in Wireshark to capture specific packets.
- Explore various filtering criteria, such as source/destination IP, port numbers, protocols, and packet content.
- Understand the practical applications of packet filtering in network analysis.

## Related Theory:

### Promiscuous Mode and Security:

- While promiscuous mode is essential for comprehensive network analysis, it can also raise security concerns. In promiscuous mode, the network adapter captures all traffic on the network segment, including potentially sensitive data not intended for the capturing device. This mode may require special permissions or administrative access.
- In non-promiscuous mode, the network adapter only captures packets explicitly addressed to it, which is generally considered more secure. However, it may limit the scope of network analysis.

### Packet Capturing Challenges:

- Modern networks often use encryption and encapsulation to secure data during transmission. Packet sniffers may encounter difficulties in analyzing encrypted or encapsulated traffic.
- In such cases, packet sniffers can still capture packets but may not be able to decipher the content. Understanding encryption and encapsulation methods is essential for effective network analysis.

Name: Yash Dave

Branch: TE-IT-A

Roll No: 18

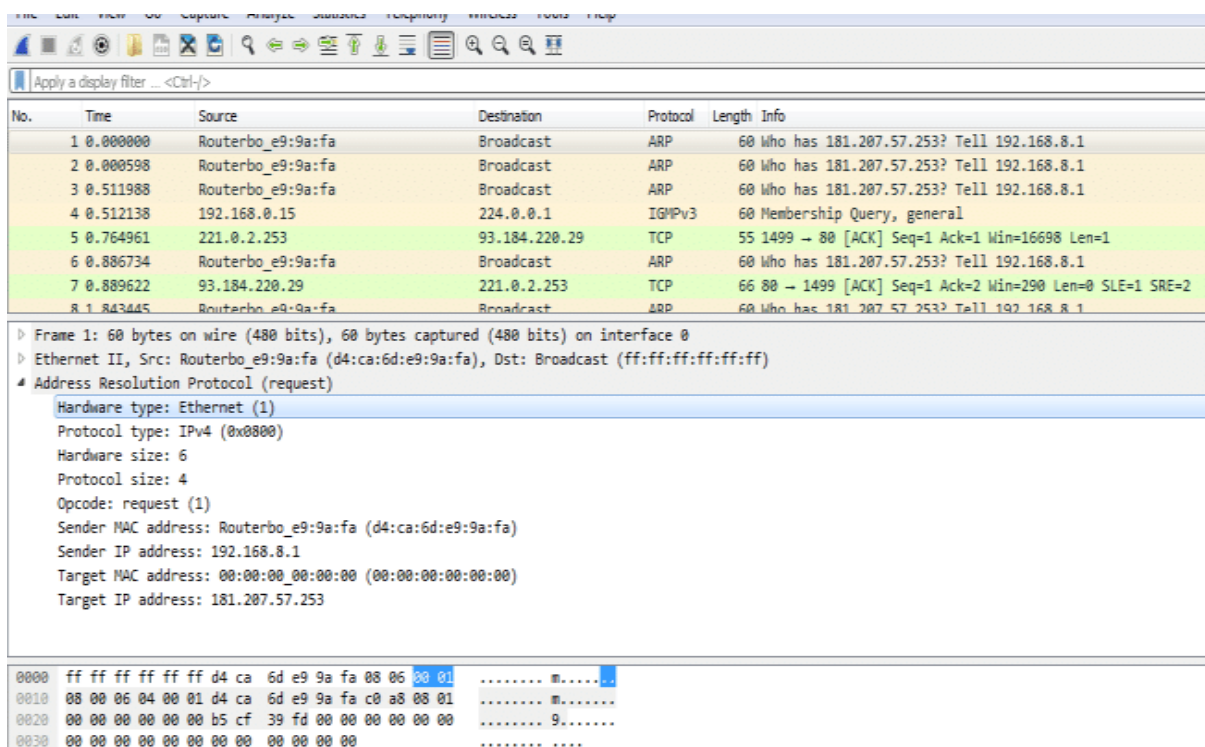
### Protocol Analysis:

- Packet sniffers like Wireshark allow for in-depth protocol analysis. This involves examining packets to identify the specific network protocols and application-layer services in use.
- Protocol analysis helps in diagnosing network issues, monitoring application performance, and detecting anomalies or security threats.

### Practical Applications of Packet Sniffing:

- Packet sniffers are indispensable tools for network troubleshooting, performance optimization, and security monitoring. They are used in various scenarios, including:
  - Network performance analysis to identify bottlenecks and latency issues.
  - Security analysis to detect and respond to security breaches, intrusion attempts, and malware.
  - Network monitoring for compliance with data privacy regulations.
  - Troubleshooting network connectivity problems and application performance issues.

### Implementation:



The screenshot shows a Wireshark capture of network traffic on interface 0. The packet list pane displays several packets, with packet 8 selected. The packet details pane shows the structure of an ARP request (Ethernet II, Internet Protocol Version 4, Address Resolution Protocol). The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Routerbo_e9:9a:fa	Broadcast	ARP	60	Who has 181.207.57.253? Tell 192.168.8.1
2	0.000598	Routerbo_e9:9a:fa	Broadcast	ARP	60	Who has 181.207.57.253? Tell 192.168.8.1
3	0.511988	Routerbo_e9:9a:fa	Broadcast	ARP	60	Who has 181.207.57.253? Tell 192.168.8.1
4	0.512138	192.168.0.15	224.0.0.1	IGMPv3	60	Membership Query, general
5	0.764961	221.0.2.253	93.184.220.29	TCP	55	1499 → 80 [ACK] Seq=1 Ack=1 Win=16698 Len=1
6	0.886734	Routerbo_e9:9a:fa	Broadcast	ARP	60	Who has 181.207.57.253? Tell 192.168.8.1
7	0.889622	93.184.220.29	221.0.2.253	TCP	66	80 → 1499 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
8	1.843445	Routerbo_e9:9a:fa	Broadcast	ARP	60	Who has 181.207.57.253? Tell 192.168.8.1

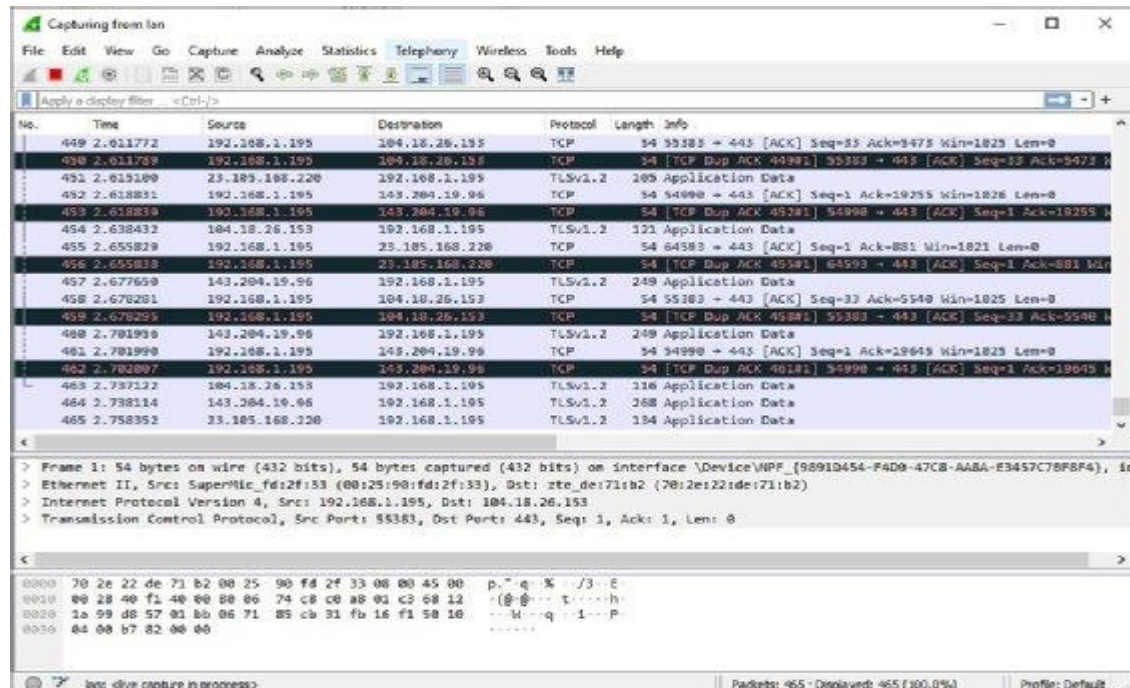
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: Routerbo\_e9:9a:fa (d4:ca:6d:e9:9a:fa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Address Resolution Protocol (request)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: request (1)  
 Sender MAC address: Routerbo\_e9:9a:fa (d4:ca:6d:e9:9a:fa)  
 Sender IP address: 192.168.8.1  
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
 Target IP address: 181.207.57.253

0000 ff ff ff ff ff d4 ca 6d e9 9a fa 08 06 00 01 ..... m.....  
 0010 00 00 06 04 00 01 d4 ca 6d e9 9a fa c0 a8 08 01 ..... m.....  
 0020 00 00 00 00 00 00 b5 cf 39 fd 00 00 00 00 00 00 ..... 9.....  
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....

Name: Yash Dave

Branch: TE-IT-A

Roll No: 18



## Learning Outcomes: Students will be able to:

1. Distinguish between promiscuous and non-promiscuous modes and understand their implications in network analysis.
2. Configure Wireshark to operate in both modes, and assess the differences in the data captured.
3. Create and apply packet filters using Wireshark to capture and analyze specific network traffic patterns.
4. Recognize the practical applications of packet filtering in monitoring, troubleshooting, and securing networks.

## Result and Discussion:

The results of this study demonstrate that Wireshark, operating in promiscuous mode, captures a more extensive range of network traffic compared to non-promiscuous mode. This broader capture capability allows for in-depth network analysis but may require elevated privileges. Participants successfully learned to configure and switch between these modes. Additionally, participants gained proficiency in using Wireshark's filtering features. They were able to capture and analyze packets based on various criteria, helping to isolate and inspect specific network activities. This knowledge is particularly valuable for diagnosing network issues, monitoring for security threats, and conducting network performance analysis.



Name: Yash Dave

Branch: TE-IT-A

Roll No: 18

### **Conclusion:**

This study has provided valuable insights into the functionality and practical applications of packet sniffer tools, with a specific focus on Wireshark. Participants have learned how to leverage promiscuous and non-promiscuous modes to adapt to different network analysis scenarios. They have also acquired the skill of filtering packets based on specific criteria, enhancing their ability to perform focused network analysis and troubleshooting. This knowledge is essential for network administrators, security professionals, and anyone involved in maintaining the integrity and security of networked systems.