

## Practical-2

**Aim:** Packet capture and analysis using Wireshark or tcpdump to capture and analyze network traffic for potential security threats.

### introduction to Packet Capture

Packet capture is the process of intercepting and logging network traffic that passes through a computer or network interface. This data can be analyzed to detect anomalies, diagnose issues or investigate potential security threats.

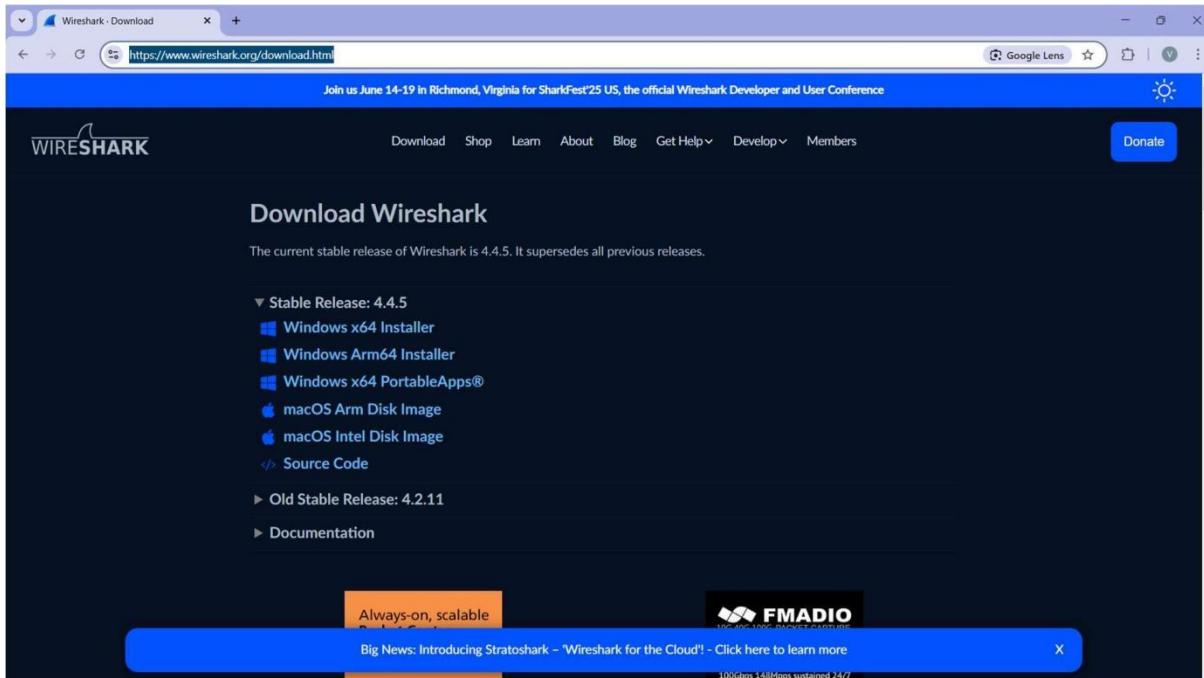
### Tools for Packet Capture:

- **Wireshark** – A graphical tool with deep packet inspection and filtering capabilities.
- **tcpdump** – A command-line tool for quick packet captures, often used on Linux servers.

### Steps to Capture Packets in Wireshark

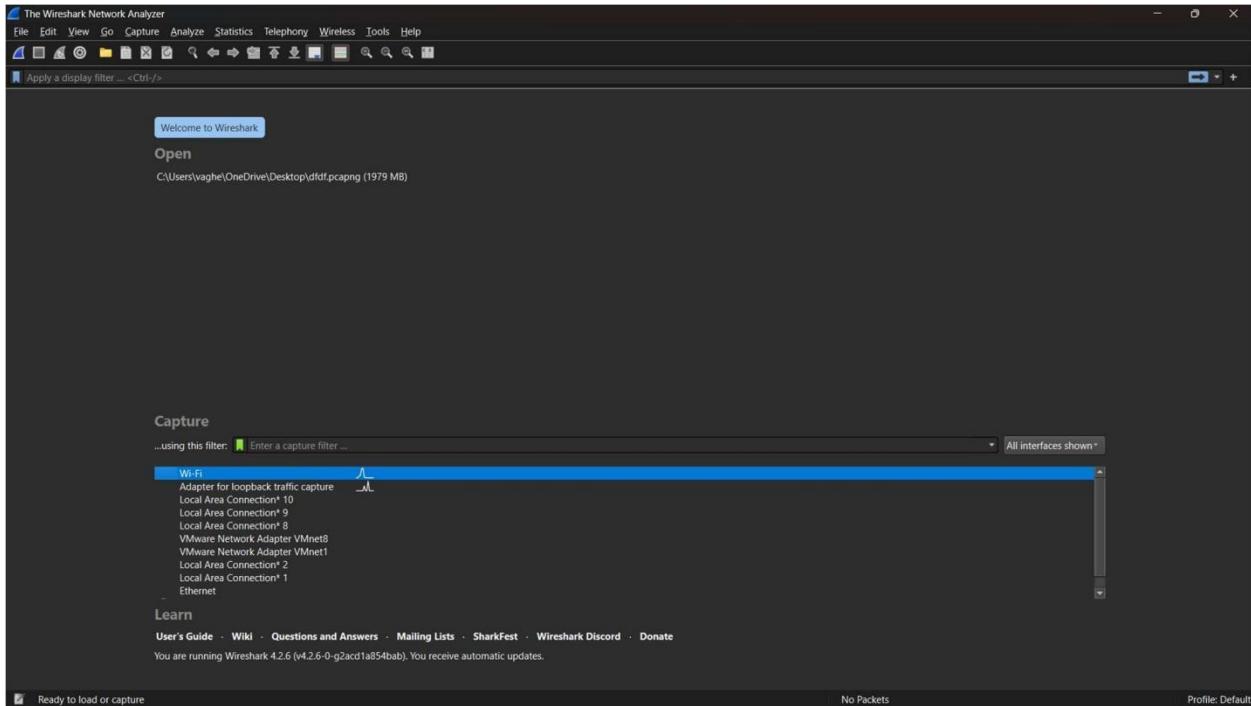
#### 1. Download and Install Wireshark

- Available for Windows, macOS and Linux.
- <https://www.wireshark.org/download.html>



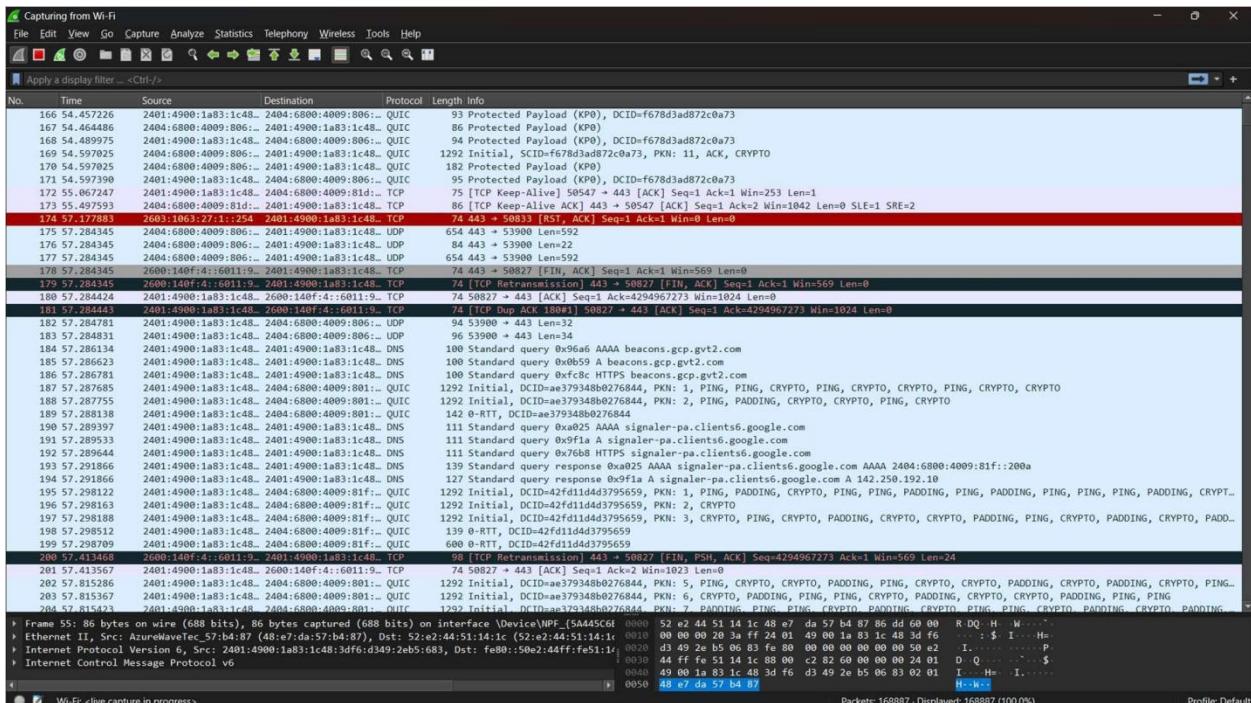
## 2. Select a Network Interface

- Open Wireshark and choose the network adapter you want to monitor (e.g., Ethernet or Wi-Fi).



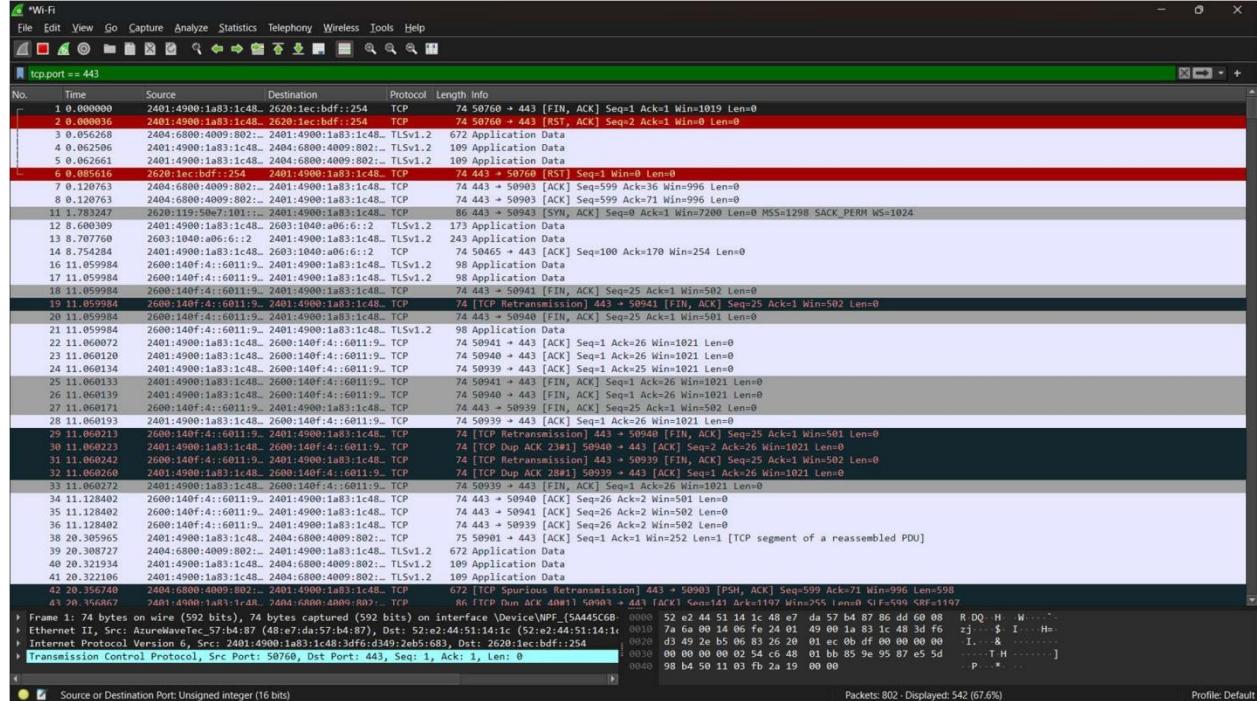
## 3. Start Capturing Packets

- Click the "Start" button to begin capturing network traffic.



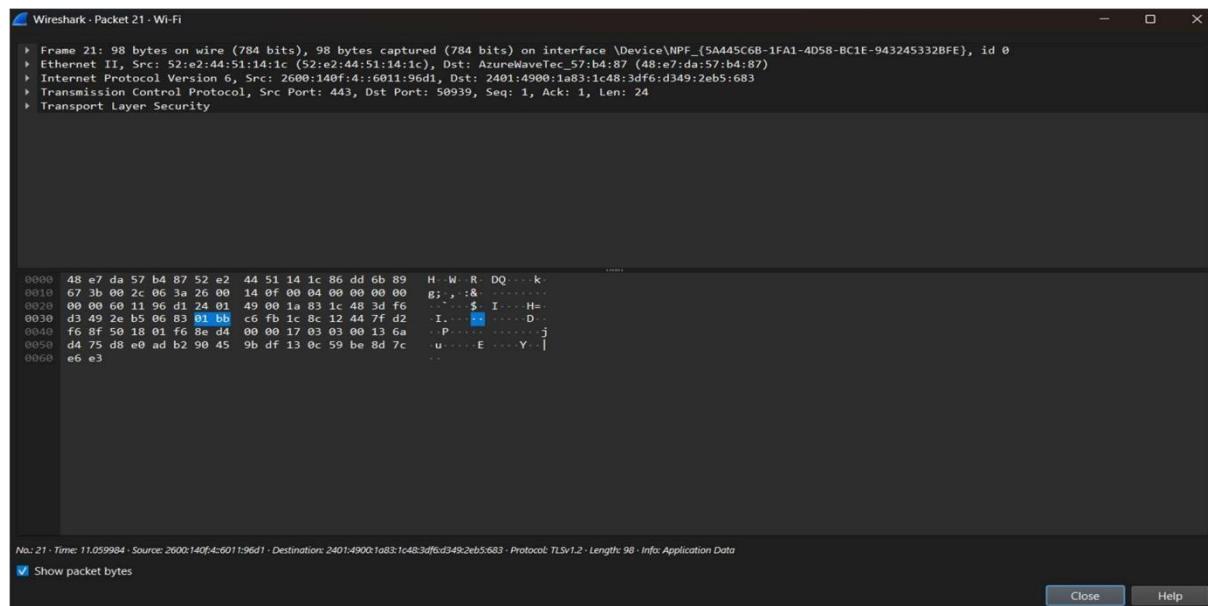
## 4. Apply Filters (Optional but Recommended)

- o Use display filters like:
  - `tcp.port == 443` → Capture only HTTPS traffic.



## 5. Analyze Captured Packets

- o Click on a packet to inspect details :



## Conclusion

Both **Wireshark** and **tcpdump** are powerful tools for **packet capture and analysis**. Wireshark is ideal for deep packet inspection with a graphical interface, while tcpdump is lightweight and perfect for command-line environments. By monitoring and analyzing network traffic, security threats like **intrusions, malware activity and data exfiltration** can be detected early.