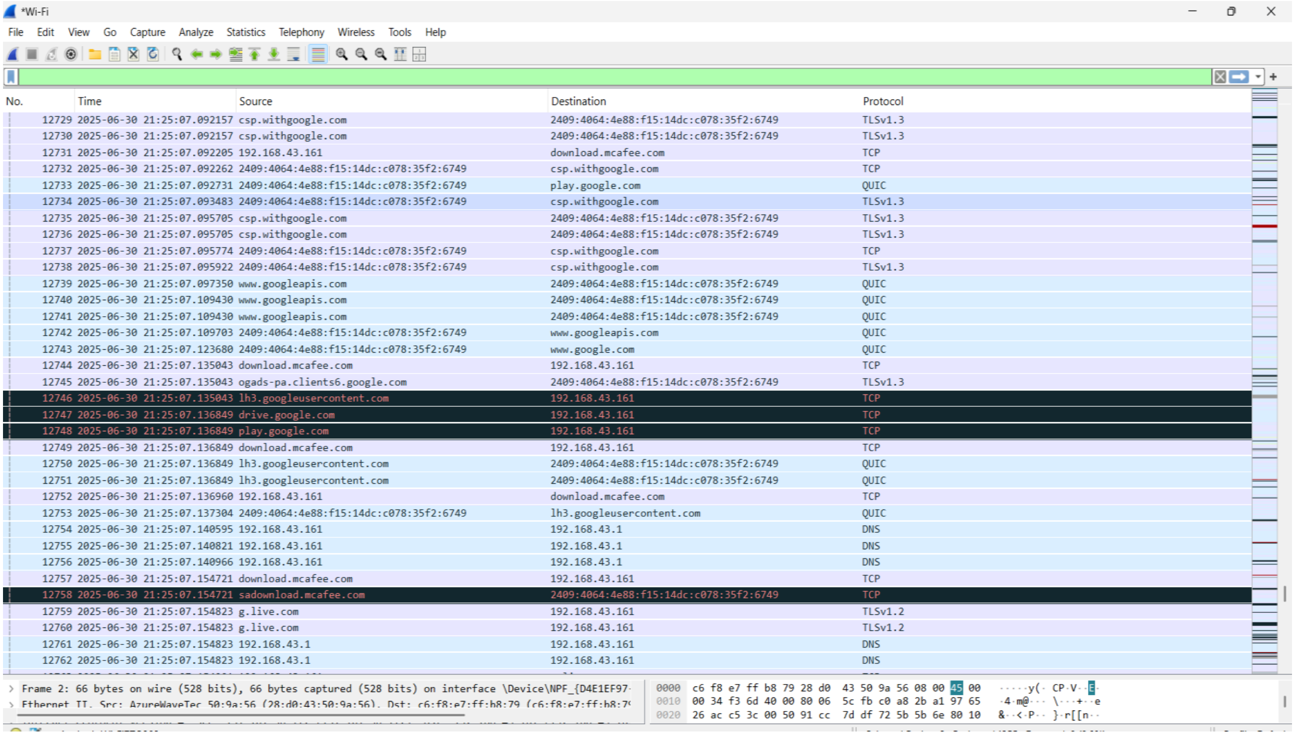
# Task 5 : Capture and Analyze Network Traffic Using Wireshark.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

| No. | Time | Source | Destination | Protocol |
|---|---|---|---|---|
| 12729 | 2025-06-30 21:25:07.092157 | csp.withgoogle.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | TLSv1.3 |
| 12730 | 2025-06-30 21:25:07.092157 | csp.withgoogle.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | TLSv1.3 |
| 12731 | 2025-06-30 21:25:07.092205 | 192.168.43.161 | download.mcafee.com | TCP |
| 12732 | 2025-06-30 21:25:07.092262 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | csp.withgoogle.com | TCP |
| 12733 | 2025-06-30 21:25:07.092731 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | play.google.com | QUIC |
| 12734 | 2025-06-30 21:25:07.093483 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | csp.withgoogle.com | TLSv1.3 |
| 12735 | 2025-06-30 21:25:07.095705 | csp.withgoogle.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | TLSv1.3 |
| 12736 | 2025-06-30 21:25:07.095705 | csp.withgoogle.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | TLSv1.3 |
| 12737 | 2025-06-30 21:25:07.095774 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | csp.withgoogle.com | TCP |
| 12738 | 2025-06-30 21:25:07.095922 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | csp.withgoogle.com | TLSv1.3 |
| 12739 | 2025-06-30 21:25:07.097350 | www.googleapis.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | QUIC |
| 12740 | 2025-06-30 21:25:07.109430 | www.googleapis.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | QUIC |
| 12741 | 2025-06-30 21:25:07.109430 | www.googleapis.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | QUIC |
| 12742 | 2025-06-30 21:25:07.109703 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | www.googleapis.com | QUIC |
| 12743 | 2025-06-30 21:25:07.123680 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | www.google.com | QUIC |
| 12744 | 2025-06-30 21:25:07.135043 | download.mcafee.com | 192.168.43.161 | TCP |
| 12745 | 2025-06-30 21:25:07.135043 | ogads-pa.clients6.google.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | TLSv1.3 |
| 12746 | 2025-06-30 21:25:07.135043 | lh3.googleusercontent.com | 192.168.43.161 | TCP |
| 12747 | 2025-06-30 21:25:07.136849 | drive.google.com | 192.168.43.161 | TCP |
| 12748 | 2025-06-30 21:25:07.136849 | play.google.com | 192.168.43.161 | TCP |
| 12749 | 2025-06-30 21:25:07.136849 | download.mcafee.com | 192.168.43.161 | TCP |
| 12750 | 2025-06-30 21:25:07.136849 | lh3.googleusercontent.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | QUIC |
| 12751 | 2025-06-30 21:25:07.136849 | lh3.googleusercontent.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | QUIC |
| 12752 | 2025-06-30 21:25:07.136960 | 192.168.43.161 | download.mcafee.com | TCP |
| 12753 | 2025-06-30 21:25:07.137304 | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | lh3.googleusercontent.com | QUIC |
| 12754 | 2025-06-30 21:25:07.140595 | 192.168.43.161 | 192.168.43.1 | DNS |
| 12755 | 2025-06-30 21:25:07.140821 | 192.168.43.161 | 192.168.43.1 | DNS |
| 12756 | 2025-06-30 21:25:07.140966 | 192.168.43.161 | 192.168.43.1 | DNS |
| 12757 | 2025-06-30 21:25:07.154721 | download.mcafee.com | 192.168.43.161 | TCP |
| 12758 | 2025-06-30 21:25:07.154721 | sadownload.mcafee.com | 2409:4064:4e88:f15:14dc:c078:35f2:6749 | TCP |
| 12759 | 2025-06-30 21:25:07.154823 | g.live.com | 192.168.43.161 | TLSv1.2 |
| 12760 | 2025-06-30 21:25:07.154823 | g.live.com | 192.168.43.161 | TLSv1.2 |
| 12761 | 2025-06-30 21:25:07.154823 | 192.168.43.1 | 192.168.43.161 | DNS |
| 12762 | 2025-06-30 21:25:07.154823 | 192.168.43.1 | 192.168.43.161 | DNS |

```
> Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D4E1EF97-
> Ethernet II, Src: AzureWaveTec 50:9a:56 (28:d0:43:50:9a:56), Dst: c6:f8:e7:ff:b8:79 (c6:f8:e7:ff:b8:7

0000  c6 f8 e7 ff b8 79 28 d0  43 50 9a 56 08 00 45 00   ·····y(· CP·V··E·
0010  00 34 f3 6d 40 00 80 06  5c fb c0 a8 2b a1 97 65   ·4·m@··· \···+··e
0020  26 ac c5 3c 00 50 91 cc  7d df 72 5b 5b 6e 80 10   &··<·P·· }·r[[n··
```

## Conclusion

- No immediate signs of malicious activity in the visible packets.
- Mostly legitimate traffic to known services: Google, McAfee, and system DNS.
- You can further investigate:
  - Unexpected, repeated connections.
  - Non-standard ports (not shown here).
  - High-frequency connections to unknown domains.

1.What is Wireshark used for?

Wireshark is a tool used to capture and analyze network traffic. It helps see what data is being sent and received on a network, useful for:

- Troubleshooting network issues
- Detecting suspicious activity
- Learning how network protocols work

2. What is a packet?

A packet is a small unit of data sent over a network.
When you send a message or file online, it is broken into packets and sent one by one.

3. How to filter packets in Wireshark?

You can use the filter bar at the top to focus on specific packets.
Examples:

- ip. Addr == 192.168.1.1 → Shows packets to or from that IP
- http → Shows only HTTP traffic
- tcp. Port == 80 → Filters TCP packets on port 80

4. What is the difference between TCP and UDP?

| Feature | TCP | UDP |
|---|---|---|
| Full form | Transmission Control Protocol | User Datagram Protocol |
| Reliable | Yes | No |
| Speed | Slower | Faster |
| Use Case | Web browsing, emails | Video streaming, gaming |

5. What is a DNS query packet?

A DNS query packet is a request sent by your device to find the IP address of a website name.
Example: When you visit www.google.com, a DNS query asks, “What is the IP of google.com?”

6. How can packet capture help in troubleshooting?

Packet capture shows exactly what data is going over the network. It helps:

- Find slow or failing connections
- Detect if a server is not responding
- Check if malware or suspicious traffic is present

7. What is a protocol?

A protocol is a set of rules for how devices communicate on a network. Examples:

- HTTP – for websites
- DNS – for finding IP addresses
- TCP/UDP – for sending data

8. Can Wireshark decrypt encrypted traffic?

Usually, no — Wireshark cannot read encrypted data like HTTPS unless:

- You have the encryption keys
- Or the traffic is using a method Wireshark supports with the right setup

So, encrypted traffic mostly looks like random data unless you prepare special settings.