Wireshark Network Traffic Analysis Report

Wireshark is a **free and open-source network protocol analyzer**. It is one of the most widely used tools for **network troubleshooting, analysis, and security auditing**.

- **What Wireshark Does:**

Wireshark lets you **capture and inspect packets** (tiny chunks of data) that are traveling across a network — like your home Wi-Fi or your organization's internal network.

- You can see:
  - Who is communicating (IP addresses, MAC addresses)
  - What protocol is being used (HTTP, DNS, TCP, etc.)
  - What data is being sent (request, response, etc.)

- **Typical Use Cases:**
  - Troubleshooting slow or broken networks.
  - Monitoring traffic to or from suspicious IPs.
  - Understanding what apps/devices are doing on a network.
  - Learning how protocols like HTTP, DNS, or TCP work.

- **Where to Get It:**

- Download Wireshark

Task Name: Task 5 – Capture and Analyze Network Traffic Using Wireshark

System: Windows 11

Tool Used: Wireshark

Capture File: my_capture.pcapng

Date of Capture: 30-June-2025

Submitted by: Utsav Bhayani

🎯 Objective

To capture live network traffic on an active network interface using Wireshark, filter it using relevant protocol expressions, and analyze at least three different protocols (DNS, TCP, ICMP) to understand their purpose and behavior in real time.

🗂️ Screenshots Summary

You have filtered and analyzed traffic using three protocols:

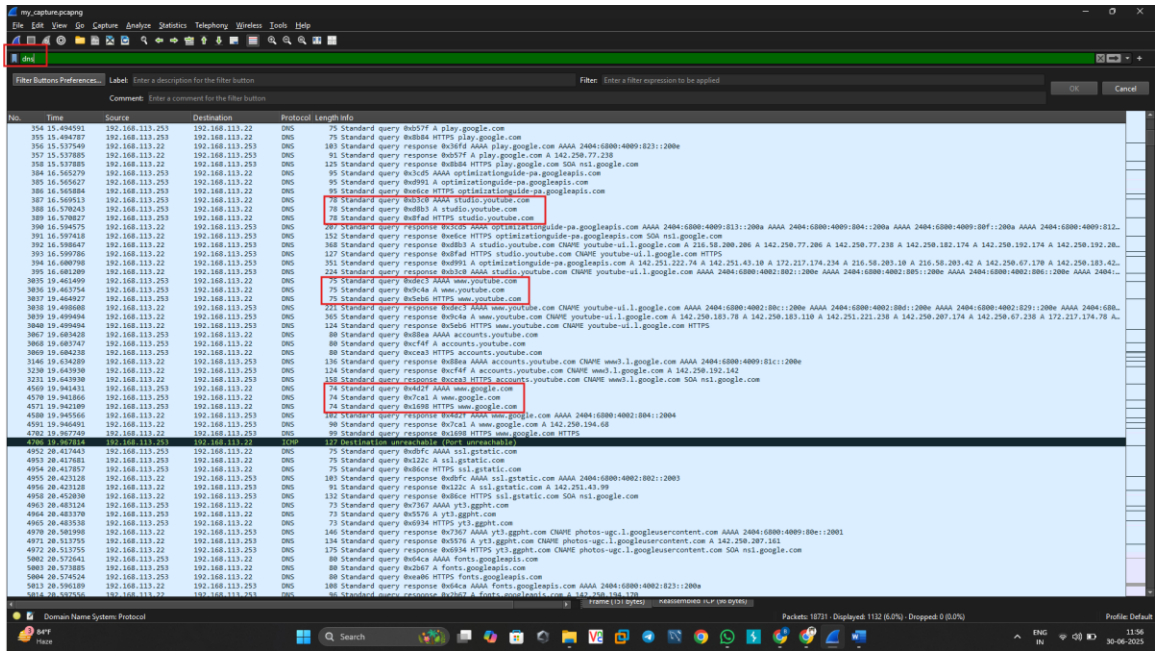
✅ dns
✅ tcp
✅ icmp

🔍 Protocols Identified and Analysis

1. DNS (Domain Name System)

- Filter Applied: dns
- Purpose: DNS translates domain names like www.youtube.com into IP addresses so browsers can load them.

- Key Findings:
  - Numerous Standard query and response packets captured.
  - Example queries: play.google.com, www.youtube.com, www.google.com
  - DNS server: 192.168.113.253
  - Returned IPs include IPv4 and IPv6 addresses like 142.250.192.206 and 2404:6800:4009:804::200e
  - Observation: The DNS protocol is actively resolving domains related to Google, YouTube, and Gstatic.

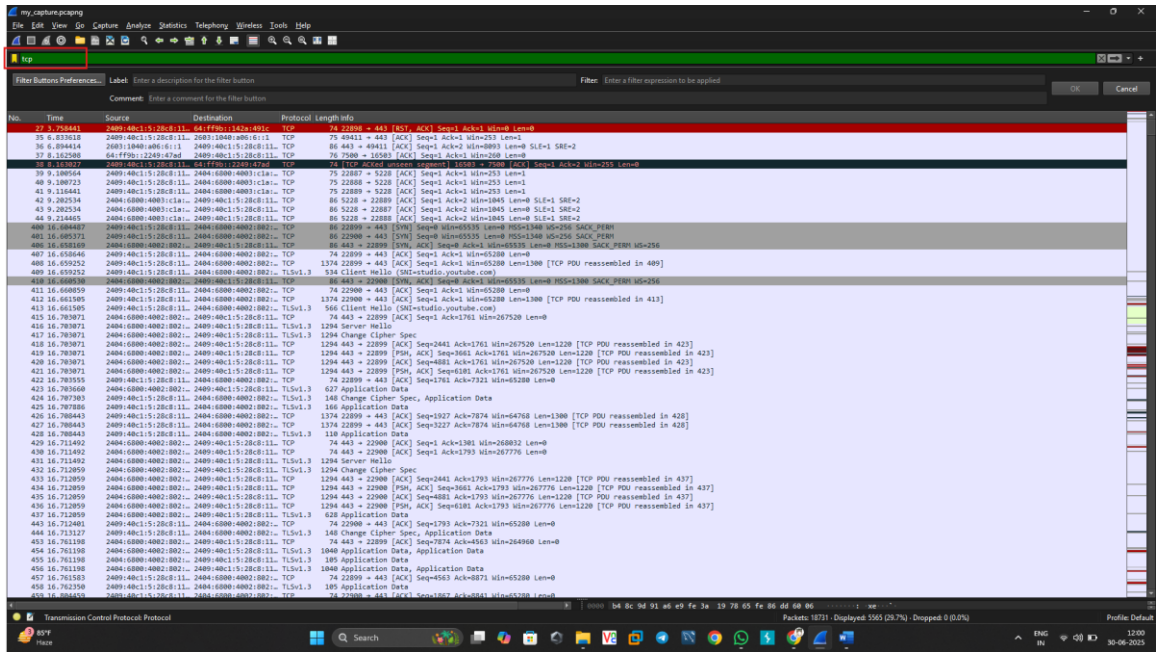

my_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Filter Buttons Preferences...
Label: Enter a description for the filter button
Filter: Enter a filter expression to be applied
Comment: Enter a comment for the filter button
OK
Cancel
No. Time Source Destination Protocol Length Info
354 15.494591 192.168.113.253 192.168.113.22 DNS 75 Standard query 0xb57f A play.google.com
355 15.494787 192.168.113.253 192.168.113.22 DNS 75 Standard query 0x8b84 HTTPS play.google.com
356 15.537549 192.168.113.22 192.168.113.253 DNS 103 Standard query response 0x36fd AAAA play.google.com AAAA 2404:6800:4009:823::200e
357 15.537885 192.168.113.22 192.168.113.253 DNS 91 Standard query response 0xb57f A play.google.com A 142.250.77.238
358 15.537885 192.168.113.22 192.168.113.253 DNS 125 Standard query response 0x8b84 HTTPS play.google.com SOA ns1.google.com
384 16.565279 192.168.113.253 192.168.113.22 DNS 95 Standard query 0x3cd5 AAAA optimizationguide-pa.googleapis.com
385 16.565627 192.168.113.253 192.168.113.22 DNS 95 Standard query 0xd991 A optimizationguide-pa.googleapis.com
386 16.565884 192.168.113.253 192.168.113.22 DNS 95 Standard query 0xe6ce HTTPS optimizationguide-pa.googleapis.com
387 16.569513 192.168.113.253 192.168.113.22 DNS 79 Standard query 0xb3c0 AAAA studio.youtube.com
388 16.570243 192.168.113.253 192.168.113.22 DNS 78 Standard query 0xd8b3 A studio.youtube.com
389 16.570827 192.168.113.253 192.168.113.22 DNS 78 Standard query 0xdfad HTTPS studio.youtube.com
390 16.594575 192.168.113.22 192.168.113.253 DNS 287 Standard query response 0x3cd5 AAAA optimizationguide-pa.googleapis.com AAAA 2404:6800:4009:813::200a AAAA 2404:6800:4009:804::200a AAAA 2404:6800:4009:80f::200a AAAA 2404:6800:4009:812…
391 16.597418 192.168.113.22 192.168.113.253 DNS 152 Standard query response 0xe6ce HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
392 16.598647 192.168.113.22 192.168.113.253 DNS 368 Standard query response 0xd8b3 A studio.youtube.com CNAME youtube-ui.l.google.com A 216.58.200.206 A 142.250.77.206 A 142.250.77.238 A 142.250.182.174 A 142.250.192.174 A 142.250.192.20…
393 16.599786 192.168.113.22 192.168.113.253 DNS 127 Standard query response 0xdfad HTTPS studio.youtube.com CNAME youtube-ui.l.google.com HTTPS
394 16.600790 192.168.113.22 192.168.113.253 DNS 351 Standard query response 0xd991 A optimizationguide-pa.googleapis.com A 142.251.222.74 A 142.251.43.10 A 172.217.174.234 A 216.58.203.10 A 216.58.203.42 A 142.250.67.170 A 142.250.183.42…
395 16.601209 192.168.113.22 192.168.113.253 DNS 224 Standard query response 0xb3c0 AAAA studio.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:4002:802::200e AAAA 2404:6800:4002:805::200e AAAA 2404:6800:4002:806::200e AAAA 2404:…
3035 19.461499 192.168.113.253 192.168.113.22 DNS 75 Standard query 0xdec3 AAAA www.youtube.com
3036 19.463754 192.168.113.253 192.168.113.22 DNS 75 Standard query 0x9c4a A www.youtube.com
3037 19.464927 192.168.113.253 192.168.113.22 DNS 75 Standard query 0x5eb6 HTTPS www.youtube.com
3038 19.498600 192.168.113.22 192.168.113.253 DNS 221 Standard query response 0xdec3 AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:4002:80c::200e AAAA 2404:6800:4002:80d::200e AAAA 2404:6800:4002:829::200e AAAA 2404:680…
3039 19.499494 192.168.113.22 192.168.113.253 DNS 365 Standard query response 0x9c4a A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.183.78 A 142.250.183.110 A 142.251.221.238 A 142.250.207.174 A 142.250.67.238 A 172.217.174.78 A…
3040 19.499494 192.168.113.22 192.168.113.253 DNS 124 Standard query response 0x5eb6 HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS
3067 19.603428 192.168.113.253 192.168.113.22 DNS 80 Standard query 0x88ea AAAA accounts.youtube.com
3068 19.603747 192.168.113.253 192.168.113.22 DNS 80 Standard query 0xcf4f A accounts.youtube.com
3069 19.604238 192.168.113.253 192.168.113.22 DNS 80 Standard query 0xcea3 HTTPS accounts.youtube.com
3146 19.634289 192.168.113.22 192.168.113.253 DNS 136 Standard query response 0x88ea AAAA accounts.youtube.com CNAME www3.l.google.com AAAA 2404:6800:4009:81c::200e
3230 19.643930 192.168.113.22 192.168.113.253 DNS 124 Standard query response 0xcf4f A accounts.youtube.com CNAME www3.l.google.com A 142.250.192.142
3231 19.643930 192.168.113.22 192.168.113.253 DNS 158 Standard query response 0xcea3 HTTPS accounts.youtube.com CNAME www3.l.google.com SOA ns1.google.com
4569 19.941431 192.168.113.253 192.168.113.22 DNS 74 Standard query 0x4d2f AAAA www.google.com
4570 19.941866 192.168.113.253 192.168.113.22 DNS 74 Standard query 0x7ca1 A www.google.com
4571 19.942109 192.168.113.253 192.168.113.22 DNS 74 Standard query 0x1698 HTTPS www.google.com
4580 19.945566 192.168.113.22 192.168.113.253 DNS 182 Standard query response 0x4d2f AAAA www.google.com AAAA 2404:6800:4002:804::2004
4591 19.946491 192.168.113.22 192.168.113.253 DNS 90 Standard query response 0x7ca1 A www.google.com A 142.250.194.68
4702 19.967749 192.168.113.22 192.168.113.253 DNS 99 Standard query response 0x1698 HTTPS www.google.com HTTPS
4706 19.967814 192.168.113.253 192.168.113.22 ICMP 123 Destination unreachable (Port unreachable)
4952 20.417443 192.168.113.253 192.168.113.22 DNS 75 Standard query 0xdbfc AAAA ssl.gstatic.com
4953 20.417681 192.168.113.253 192.168.113.22 DNS 75 Standard query 0x122c A ssl.gstatic.com
4954 20.417857 192.168.113.253 192.168.113.22 DNS 75 Standard query 0x86ce HTTPS ssl.gstatic.com
4955 20.423128 192.168.113.22 192.168.113.253 DNS 103 Standard query response 0xdbfc AAAA ssl.gstatic.com AAAA 2404:6800:4002:802::2003
4956 20.423128 192.168.113.22 192.168.113.253 DNS 91 Standard query response 0x122c A ssl.gstatic.com A 142.251.43.99
4958 20.452030 192.168.113.22 192.168.113.253 DNS 132 Standard query response 0x86ce HTTPS ssl.gstatic.com SOA ns1.google.com
4963 20.483124 192.168.113.253 192.168.113.22 DNS 73 Standard query 0x7367 AAAA yt3.ggpht.com
4964 20.483370 192.168.113.253 192.168.113.22 DNS 73 Standard query 0x5576 A yt3.ggpht.com
4965 20.483538 192.168.113.253 192.168.113.22 DNS 73 Standard query 0x6934 HTTPS yt3.ggpht.com
4970 20.501998 192.168.113.22 192.168.113.253 DNS 146 Standard query response 0x7367 AAAA yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com AAAA 2404:6800:4009:80e::2001
4971 20.513755 192.168.113.22 192.168.113.253 DNS 134 Standard query response 0x5576 A yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com A 142.250.207.161
4972 20.513755 192.168.113.22 192.168.113.253 DNS 175 Standard query response 0x6934 HTTPS yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com SOA ns1.google.com
5002 20.572641 192.168.113.253 192.168.113.22 DNS 80 Standard query 0x64ca AAAA fonts.googleapis.com
5003 20.573885 192.168.113.253 192.168.113.22 DNS 80 Standard query 0x2b67 A fonts.googleapis.com
5004 20.574524 192.168.113.253 192.168.113.22 DNS 80 Standard query 0xea06 HTTPS fonts.googleapis.com
5013 20.596189 192.168.113.22 192.168.113.253 DNS 108 Standard query response 0x64ca AAAA fonts.googleapis.com AAAA 2404:6800:4002:823::200a
5014 20.597556 192.168.113.22 192.168.113.253 DNS 96 Standard query response 0x2b67 A fonts.googleapis.com A 142.250.194.170
Frame (131 bytes) Reassembled TCP (36 bytes)
Domain Name System: Protocol
Packets: 18731 · Displayed: 1132 (6.0%) · Dropped: 0 (0.0%)
Profile: Default
84°F Haze
Search
ENG IN
11:56 30-06-2025

2. TCP (Transmission Control Protocol)

- Filter Applied: tcp
- Purpose: TCP is a transport layer protocol that provides reliable, ordered, and error-checked delivery of data.

Key Findings:

- TCP traffic observed to/from port 443 (HTTPS).
- SYN, SYN-ACK, ACK observed — indicating successful 3-way handshake.
- TLS 1.3 encrypted communication shown over TCP.
- Observation: TCP forms the backbone of secure web communication using HTTPS.

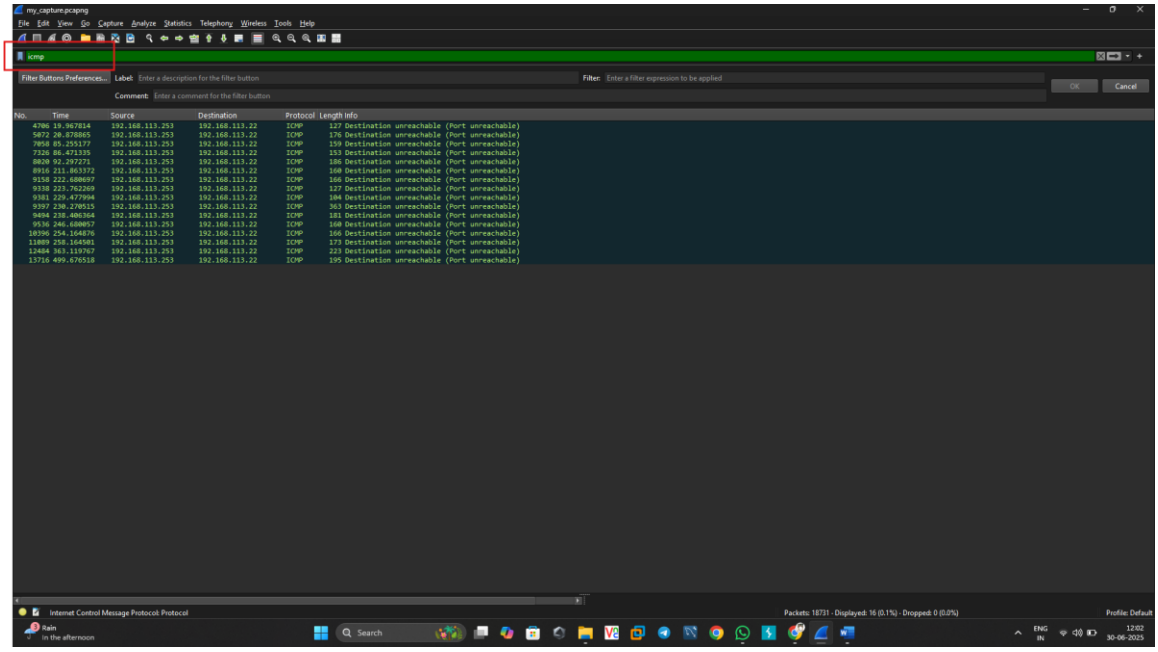


3. ICMP (Internet Control Message Protocol)

- Filter Applied: icmp
- Purpose: Used for error messages and diagnostic operations like ping.

Key Findings:

- ICMP 'Destination Unreachable (Port unreachable)' messages captured.
- Source: 192.168.113.253 → Destination: 192.168.113.22
- Observation: These ICMP packets suggest blocked or inactive ports in the destination device.



Summary Table

Protocol	Description	Filter Used	Example Traffic Details
DNS	Domain name resolution	dns	Queries for google.com, youtube.com → IPs like 142.250.xxx.xxx
TCP	Reliable data transfer protocol	tcp	TLS over TCP port 443, secure web traffic
ICMP	Diagnostics & error reporting	icmp	Destination unreachable messages to 192.168.113.22

Deliverables

✅ my_capture.pcapng: The Wireshark capture file

✅ This report: wireshark_analysis_report.docx

Conclusion

- This exercise successfully demonstrates how to:
- Capture real-time network traffic
- Filter and isolate different protocols
- Analyze packet-level data
- Understand the role of DNS, TCP, and ICMP in a network

You now have hands-on experience with Wireshark — a critical tool for cybersecurity, troubleshooting, and protocol analysis.