



# DNS traffic filtering

 DNS Protocol Analysis — Wireshark Capture


 Protocol: \*\*Domain Name System (DNS)\*\*

**\*\*Port:\*\*** UDP 53

**\*\*Purpose:\*\*** Resolves human-readable domain names (e.g., `www.jio.com`) to IP addresses.

###  Captured DNS Packet Flow

Packet No.	Source IP	Destination IP	Type	Query/Response	Resolved IP
963	192.168.220.236	192.168.220.12	DNS Query	A record for www.jio.com	—
964	192.168.220.236	192.168.220.12	DNS Query (Repeat)	Duplicate A query	—
965	192.168.220.12	192.168.220.236	DNS Response	Response with A record	49.40.8.179

###  Key Observations:

- The client (`192.168.220.236`) issued two **\*\*consecutive DNS queries\*\***, likely due to a timeout or retry.
- The local DNS resolver (`192.168.220.12`) returned a valid IP address mapping for **\*\*`www.jio.com`\*\***.
- DNS traffic was successfully captured, showing the classic **\*\*query-response lifecycle\*\*** of a UDP-based DNS lookup.

# ICMP traffic filtering

 ICMP Protocol Analysis — Wireshark Capture


 Protocol: **\*\*Internet Control Message Protocol (ICMP)\*\***

**\*\*Purpose:\*\*** Used for network diagnostics and connectivity checks (e.g., the `ping` command).

**\*\*Default Behavior:\*\*** Sends Echo Requests and expects Echo Replies to validate reachability.


###  Captured ICMP Packet Flow


Packet No.	Source IP	Destination IP	Type	ID / Sequence	Round-Trip Pair
4951	192.168.220.236	8.8.8.8	Echo Request	ID=0x0001, Seq=9	Reply in 4956
4956	8.8.8.8	192.168.220.236	Echo Reply	ID=0x0001, Seq=9	Matches 4951
4981	192.168.220.236	8.8.8.8	Echo Request	ID=0x0001, Seq=10	Reply in 4980
4980	8.8.8.8	192.168.220.236	Echo Reply	ID=0x0001, Seq=10	Matches 4981
4993	192.168.220.236	8.8.8.8	Echo Request	ID=0x0001, Seq=11	Reply in 4997
4997	8.8.8.8	192.168.220.236	Echo Reply	ID=0x0001, Seq=11	Matches 4993
5044	192.168.220.236	8.8.8.8	Echo Request	ID=0x0001, Seq=12	Reply in 5053
5053	8.8.8.8	192.168.220.236	Echo Reply	ID=0x0001, Seq=12	Matches 5044

###  Key Observations:

- **Consistent bidirectional flow** of Echo Requests and Replies indicates stable connectivity with `8.8.8.8` (Google DNS).
- Sequence numbers increment logically, matching responses accurately.
- No packet loss or unusual latency patterns were observed during this segment.

## HTTP traffic filtering

 HTTP Protocol Analysis — Wireshark Capture


 Protocol: **Hypertext Transfer Protocol (HTTP)**

**Port:** TCP 80

**Purpose:** Facilitates communication between web clients (browsers) and servers using plaintext requests and responses.

###  Captured HTTP Transaction Summary

Packet No.	Source IP	Destination IP	Type	HTTP Method / Status	Description
1074	192.168.220.236	49.40.8.179	HTTP Request	GET / HTTP/1.1	Client requests root page
1083	49.40.8.179	192.168.220.236	HTTP Response	HTTP/1.1 302 Found	Server issues redirection

###  Key Observations:

- The client initiated a **GET** request for the homepage (likely during manual browsing).
- The server responded with a **302 status code**, indicating a **temporary redirect**, possibly to a login page or dynamic content server.
- Traffic confirms functional HTTP interaction over **unencrypted TCP** — a potential risk point in production environments if sensitive data were involved.