Task-1: DNS resolver

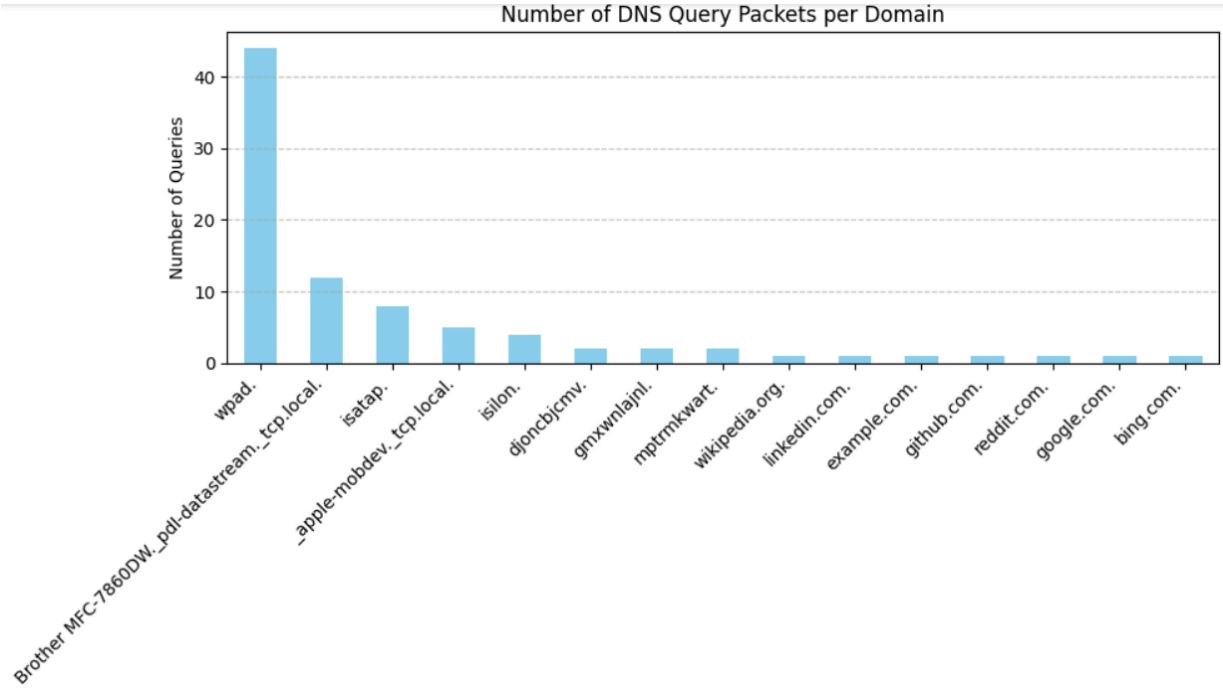
custom_header	domain_name	resolved_ip
9330000	_apple-mobdev._tcp.local.	192.168.1.1
9330001	_apple-mobdev._tcp.local.	192.168.1.2
9330002	linkedin.com.	192.168.1.3
9330003	wikipedia.org.	192.168.1.4
9330004	wpad.	192.168.1.5
9330005	wpad.	192.168.1.1
9330006	wpad.	192.168.1.2
9330007	wpad.	192.168.1.3
9330008	wpad.	192.168.1.4
9330009	wpad.	192.168.1.5
9330010	wpad.	192.168.1.1
9330011	wpad.	192.168.1.2
9330012	gmxwnlajnl.	192.168.1.3
9330013	djoncbjcmv.	192.168.1.4
9330014	mptrmkwart.	192.168.1.5
9330015	djoncbjcmv.	192.168.1.1
9330016	gmxwnlajnl.	192.168.1.2
9330017	mptrmkwart.	192.168.1.3
9330018	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.4
9330019	Brother MFC-7860DW._pdl-datastream._tcp.local.	192.168.1.5
9330020	example.com.	192.168.1.1

9330021	wpad.	192.168.1.2
9330022	wpad.	192.168.1.3
9330023	wpad.	192.168.1.4

Most frequent domains

domain_name	
wpad.	44
Brother MFC-7860DW._pdl-datastream._tcp.local.	12
isatap.	8
_apple-mobdev._tcp.local.	5
isilon.	4
djoncbjcmv.	2
gmxwnlajnl.	2
mptrmkwart.	2
wikipedia.org.	1
linkedin.com.	1
example.com.	1
github.com.	1
reddit.com.	1
google.com.	1
bing.com.	1

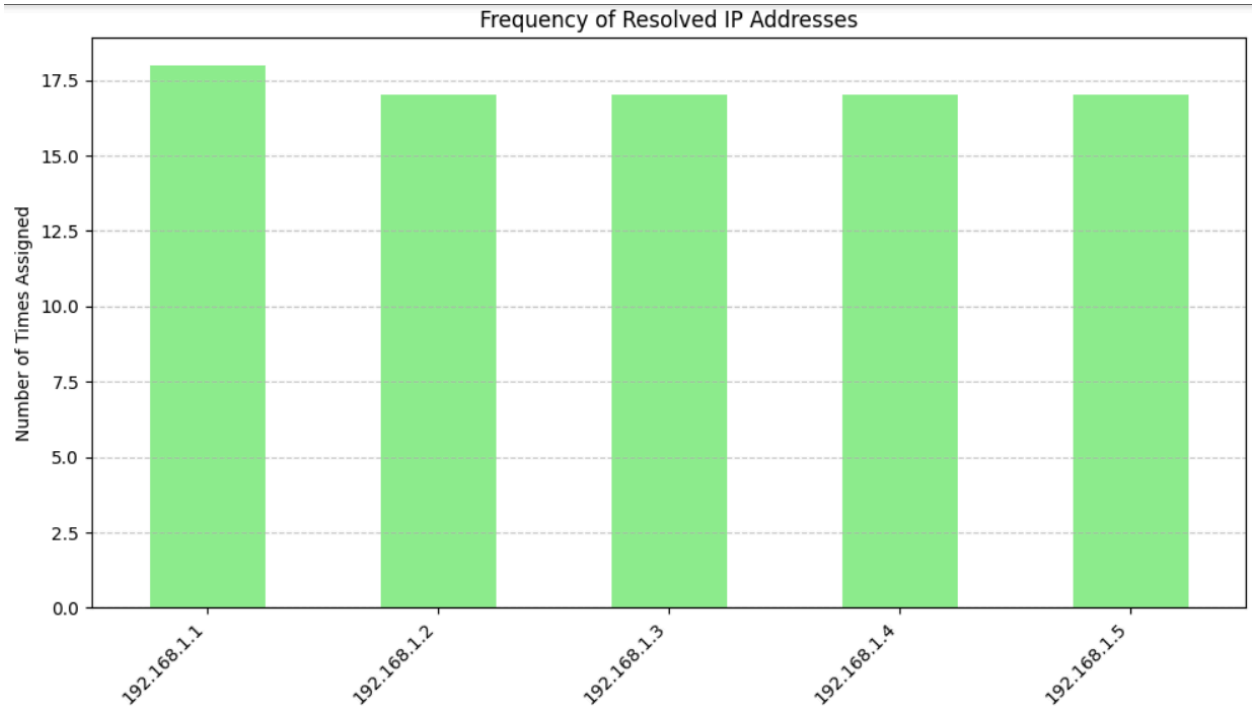
Graphical distribution of domains frequency



Resolved IPs count

resolved_ip	count
192.168.1.1	18
192.168.1.2	17
192.168.1.3	17
192.168.1.4	17
192.168.1.5	17

Graphical representation of Resolved IPs



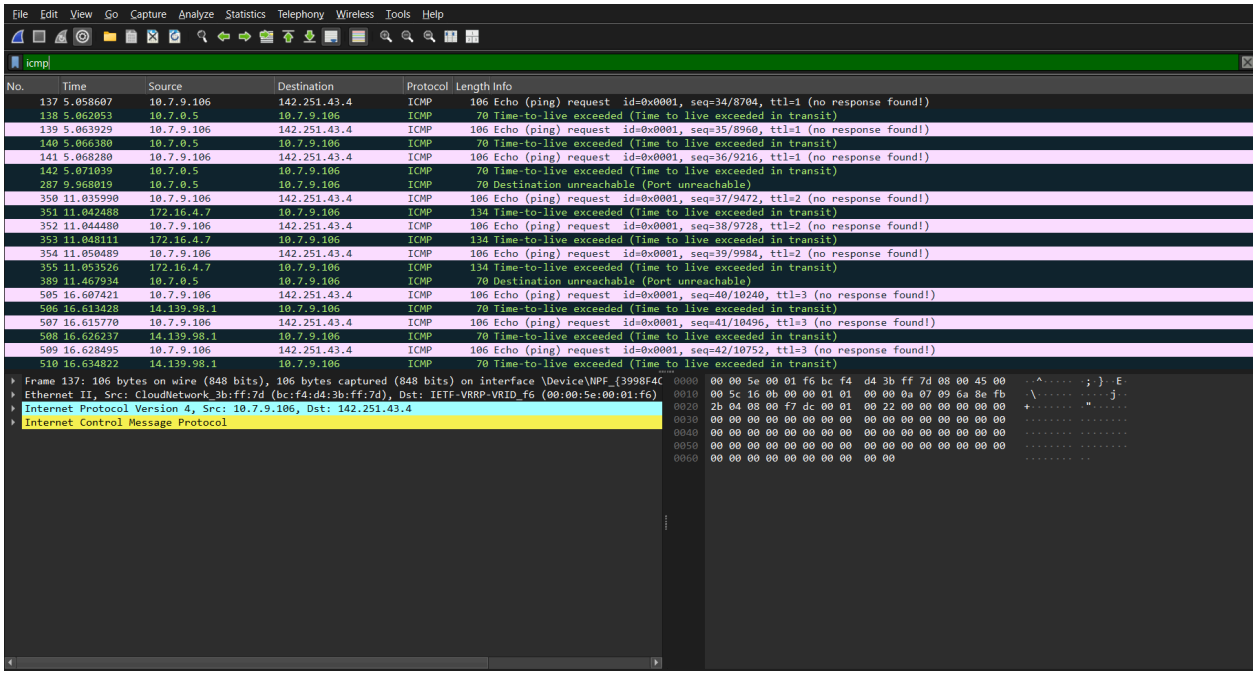
Task-2: Traceroute Protocol Behavior

```
C:\Users\ayush>tracert www.google.com

Tracing route to www.google.com [142.251.220.4]
over a maximum of 30 hops:

  1     5 ms     4 ms     3 ms  10.7.0.5
  2     3 ms     3 ms     2 ms  172.16.4.7
  3     6 ms     5 ms     5 ms  14.139.98.1
  4     4 ms     3 ms     3 ms  10.117.81.253
  5    80 ms    28 ms    22 ms  10.154.8.137
  6    24 ms    14 ms    11 ms  10.255.239.170
  7    15 ms    11 ms    11 ms  10.152.7.214
  8    14 ms    14 ms    13 ms  142.250.172.80
  9    18 ms    24 ms    17 ms  142.251.76.31
 10    28 ms    15 ms    15 ms  142.251.64.13
 11    15 ms    13 ms    13 ms  pnbomb-ay-in-f4.1e100.net [142.251.220.4]

Trace complete.
```

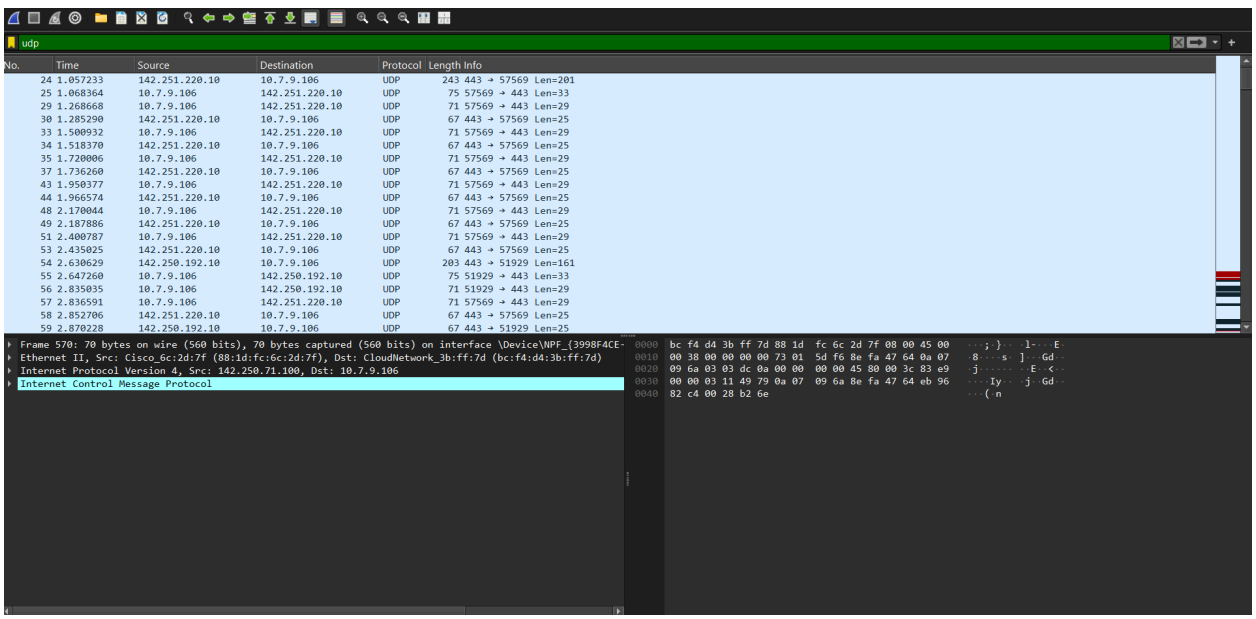
```
ayush@Honormagicbook:/mnt/c/WINDOWS/system32$ traceroute www.google.com
traceroute to www.google.com (142.250.71.100), 30 hops max, 60 byte packets
 1  Honormagicbook.mshome.net (172.20.0.1)  0.679 ms  0.913 ms  0.897 ms
 2  10.7.0.5 (10.7.0.5)  4.810 ms  4.770 ms  4.755 ms
 3  172.16.4.7 (172.16.4.7)  2.993 ms  2.979 ms  2.930 ms
 4  14.139.98.1 (14.139.98.1)  5.609 ms  5.464 ms  5.400 ms
 5  10.117.81.253 (10.117.81.253)  4.354 ms  4.334 ms  4.318 ms
 6  10.154.8.137 (10.154.8.137)  12.461 ms  11.886 ms  11.854 ms
 7  10.255.239.170 (10.255.239.170)  11.912 ms  11.864 ms  12.961 ms
 8  10.152.7.214 (10.152.7.214)  11.772 ms  11.161 ms  10.903 ms
 9  72.14.204.62 (72.14.204.62)  12.042 ms *  11.916 ms
10  * * *
11  142.251.77.98 (142.251.77.98)  13.163 ms 216.239.50.166 (216.239.50.166)  16.803 ms 142.251.69.44 (142.251.69.44)  14.099 ms
12  192.178.110.104 (192.178.110.104)  12.780 ms  12.764 ms 192.178.86.247 (192.178.86.247)  13.876 ms
13  pnbomb-ad-in-f4.1e100.net (142.250.71.100)  14.782 ms  14.764 ms 142.250.209.71 (142.250.209.71)  13.828 ms
```

Q1. What protocol does Windows tracert use by default, and what protocol does Linux traceroute use by default ?

→ Windows tracert



Linux traceroute



Windows tracert uses ICMP Echo Request by default. When we put the filter icmp in wireshark we can see

- Packets labeled as Echo (ping) request
- ICMP Time Exceeded (TTL expired)
- Final Echo Reply

Linux traceroute uses UDP by default. When we put the filter as udp

- UDP packets sent from client.
- ICMP Time Exceeded.
- ICMP Destination Unreachable (Port Unreachable).

Q2. Some hops in your traceroute output may show . Provide at least two reasons why a router might not reply.

→ Some hops show *** because:

1. Firewall blocking ICMP or TTL Expired packets:
2. Rate-limiting prevents replying to every probe and drops some probs.

   This is evident in Wireshark where no ICMP Time Exceeded is received for certain TTLs.

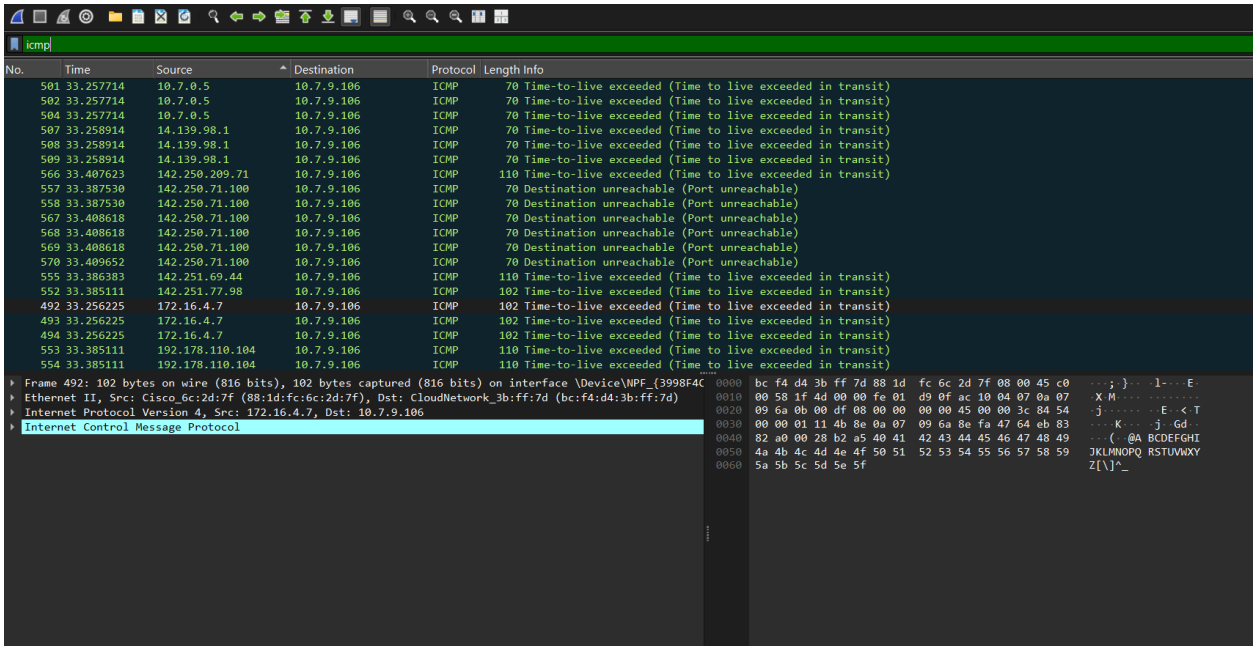
Q3. In Linux traceroute, which field in the probe packets changes between successive probes sent to the destination?

→ The UDP source port number changes in each probe packet.

Q4. At the final hop, how is the response different compared to the intermediate hop?

→ Intermediate hop sends ICMP Time Exceeded.

Final hop (destination reached) sends ICMP Destination Unreachable (Destination Unreachable Port Unreachable,).



Q5. Suppose a firewall blocks UDP traffic but allows ICMP — how would this affect the results of Linux traceroute vs. Windows tracert?

→ **Windows tracert (ICMP-based)** Works normally:

ICMP Echo Requests and Replies continue without issue, it means everything is visible.

Linux traceroute (UDP-based) Will fail to get responses:

No ICMP Time Exceeded or Destination Unreachable packets returned. Shows only UDP packets going out, it means no ICMP replies received.