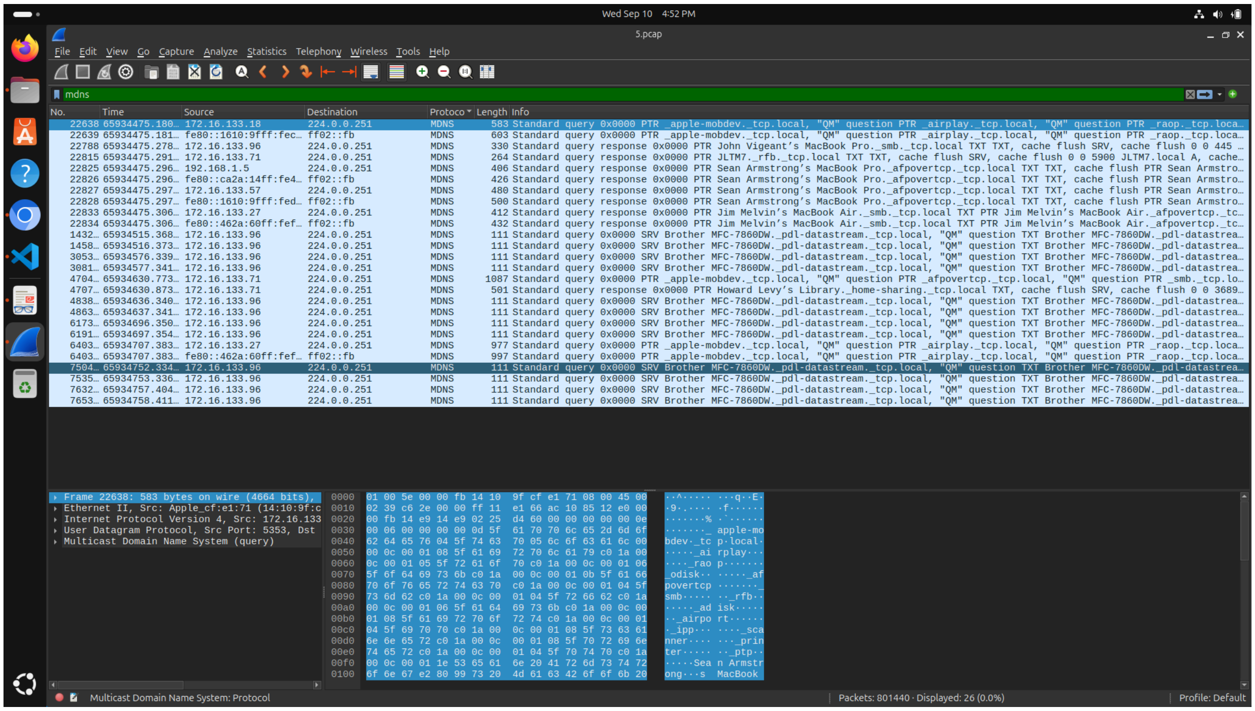
CS331: Computer Networks Assignment 1

Group Members: Burra Saharsh (23110071), Surriya Gokul (23110324)

Task - 1:

Filtered out the MDNS protocols with UDP

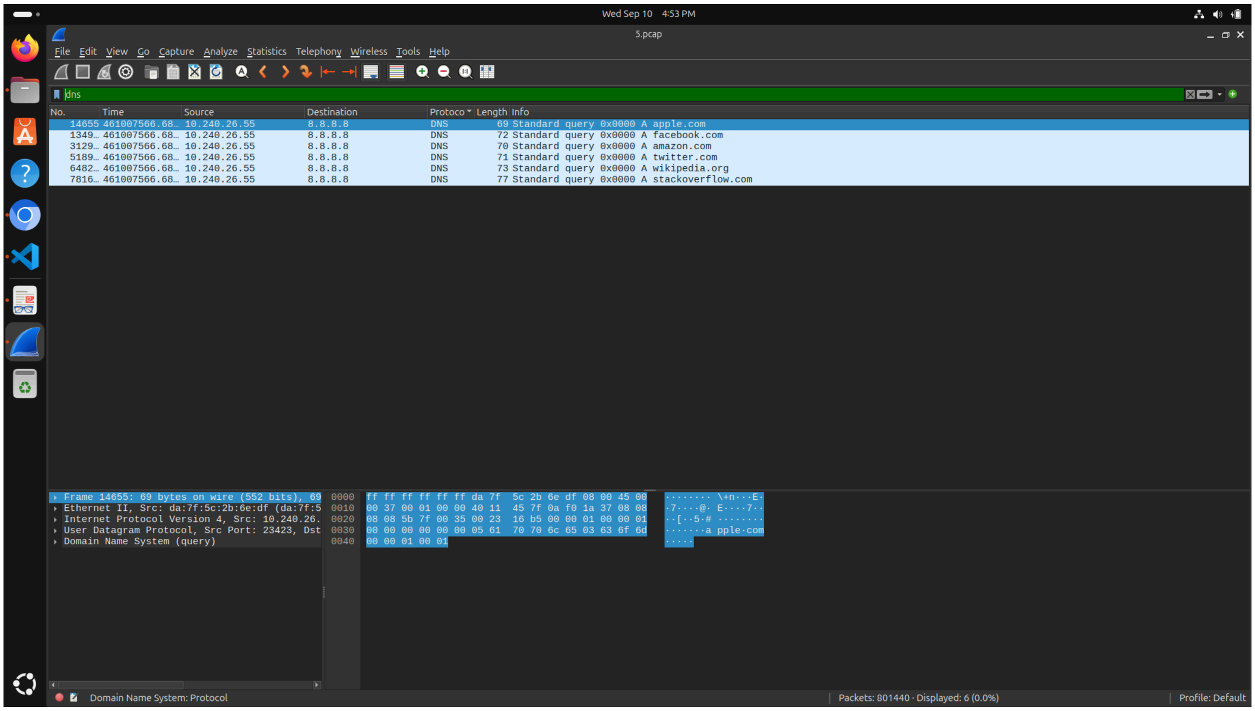

Wed Sep 10 4:52 PM
5.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
mdns
No.     Time              Source                   Destination   Protoco Length Info
  22638 65934475.180…  172.16.133.18             224.0.0.251   MDNS     583 Standard query 0x0000 PTR _apple-mobdev._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.loca…
  22639 65934475.181…  fe80::1610:9fff:fec…      ff02::fb      MDNS     603 Standard query 0x0000 PTR _apple-mobdev._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.loca…
  22788 65934475.278…  172.16.133.96             224.0.0.251   MDNS     330 Standard query response 0x0000 PTR John Vigeant’s MacBook Pro._smb._tcp.local TXT TXT, cache flush SRV, cache flush 0 0 445 …
  22815 65934475.291…  172.16.133.71             224.0.0.251   MDNS     264 Standard query response 0x0000 PTR JLTM7._rfb._tcp.local TXT TXT, cache flush SRV, cache flush 0 0 5900 JLTM7.local A, cache…
  22825 65934475.296…  192.168.1.5               224.0.0.251   MDNS     406 Standard query response 0x0000 PTR Sean Armstrong’s MacBook Pro._afpovertcp._tcp.local TXT TXT, cache flush PTR Sean Armstro…
  22826 65934475.296…  fe80::ca2a:14ff:fe4…      ff02::fb      MDNS     426 Standard query response 0x0000 PTR Sean Armstrong’s MacBook Pro._afpovertcp._tcp.local TXT TXT, cache flush PTR Sean Armstro…
  22827 65934475.297…  172.16.133.57             224.0.0.251   MDNS     480 Standard query response 0x0000 PTR Sean Armstrong’s MacBook Pro._afpovertcp._tcp.local TXT TXT, cache flush PTR Sean Armstro…
  22828 65934475.297…  fe80::1610:9fff:fed…      ff02::fb      MDNS     500 Standard query response 0x0000 PTR Sean Armstrong’s MacBook Pro._afpovertcp._tcp.local TXT TXT, cache flush PTR Sean Armstro…
  22833 65934475.306…  172.16.133.27             224.0.0.251   MDNS     412 Standard query response 0x0000 PTR Jim Melvin’s MacBook Air._smb._tcp.local TXT PTR Jim Melvin’s MacBook Air._afpovertcp._tc…
  22834 65934475.306…  fe80::462a:60ff:fef…      ff02::fb      MDNS     432 Standard query response 0x0000 PTR Jim Melvin’s MacBook Air._smb._tcp.local TXT PTR Jim Melvin’s MacBook Air._afpovertcp._tc…
  1432… 65934515.368…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  1458… 65934516.373…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  3053… 65934576.339…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  3081… 65934577.341…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  4704… 65934630.773…  172.16.133.71             224.0.0.251   MDNS    1087 Standard query 0x0000 PTR _apple-mobdev._tcp.local, "QM" question PTR _afpovertcp._tcp.local, "QM" question PTR _smb._tcp.lo…
  4707… 65934630.873…  172.16.133.71             224.0.0.251   MDNS     501 Standard query response 0x0000 PTR Howard Levy’s Library._home-sharing._tcp.local TXT, cache flush SRV, cache flush 0 0 3689…
  4838… 65934636.340…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  4863… 65934637.341…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  6173… 65934696.350…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  6191… 65934697.354…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  6403… 65934707.383…  172.16.133.27             224.0.0.251   MDNS     977 Standard query 0x0000 PTR _apple-mobdev._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.loca…
  6403… 65934707.383…  fe80::462a:60ff:fef…      ff02::fb      MDNS     997 Standard query 0x0000 PTR _apple-mobdev._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.loca…
  7504… 65934752.334…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  7535… 65934753.336…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  7632… 65934757.404…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
  7653… 65934758.411…  172.16.133.96             224.0.0.251   MDNS     111 Standard query 0x0000 SRV Brother MFC-7860DW._pdl-datastream._tcp.local, "QM" question TXT Brother MFC-7860DW._pdl-datastrea…
```

```
› Frame 22638: 583 bytes on wire (4664 bits),     0000  01 00 5e 00 00 fb 14 10  9f cf e1 71 08 00 45 00   ··^····· ···q··E·
› Ethernet II, Src: Apple_cf:e1:71 (14:10:9f:c     0010  02 39 c6 2e 00 00 ff 11  e1 66 ac 10 85 12 e0 00   ·9·.···· ·f······
› Internet Protocol Version 4, Src: 172.16.133    0020  00 fb 14 e9 14 e9 02 25  d4 60 00 00 00 00 00 0e   ·······% ·`······
› User Datagram Protocol, Src Port: 5353, Dst     0030  00 06 00 00 00 00 0d 5f  61 70 70 6c 65 2d 6d 6f   ·······_ apple-mo
› Multicast Domain Name System (query)            0040  62 64 65 76 04 5f 74 63  70 05 6c 6f 63 61 6c 00   bdev·_tc p·local·
                                                  0050  00 0c 00 01 08 5f 61 69  72 70 6c 61 79 c0 1a 00   ·····_ai rplay···
                                                  0060  0c 00 01 05 5f 72 61 6f  70 c0 1a 00 0c 00 01 06   ····_rao p·······
                                                  0070  5f 6f 64 69 73 6b c0 1a  00 0c 00 01 0b 5f 61 66   _odisk·· ·····_af
                                                  0080  70 6f 76 65 72 74 63 70  c0 1a 00 0c 00 01 04 5f   povertcp ·······_
                                                  0090  73 6d 62 c0 1a 00 0c 00  01 04 5f 72 66 62 c0 1a   smb····· ··_rfb··
                                                  00a0  00 0c 00 01 06 5f 61 64  69 73 6b c0 1a 00 0c 00   ·····_ad isk·····
                                                  00b0  01 08 5f 61 69 72 70 6f  72 74 c0 1a 00 0c 00 01   ··_airpo rt······
                                                  00c0  04 5f 69 70 70 c0 1a 00  0c 00 01 08 5f 73 63 61   ·_ipp··· ····_sca
                                                  00d0  6e 6e 65 72 c0 1a 00 0c  00 01 08 5f 70 72 69 6e   nner···· ···_prin
                                                  00e0  74 65 72 c0 1a 00 0c 00  01 04 5f 70 74 70 c0 1a   ter····· ··_ptp··
                                                  00f0  00 0c 00 01 1e 53 65 61  6e 20 41 72 6d 73 74 72   ·····Sea n Armstr
                                                  0100  6f 6e 67 e2 80 99 73 20  4d 61 63 42 6f 6f 6b 20   ong···s  MacBook
```

```
Multicast Domain Name System: Protocol        Packets: 801440 · Displayed: 26 (0.0%)        Profile: Default
```

Checking for the number of DNS packets


Wed Sep 10 4:53 PM
5.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
No.     Time              Source         Destination   Protoco Length Info
  14655 461007566.68…  10.240.26.55   8.8.8.8       DNS       69 Standard query 0x0000 A apple.com
  1349… 461007566.68…  10.240.26.55   8.8.8.8       DNS       72 Standard query 0x0000 A facebook.com
  3129… 461007566.68…  10.240.26.55   8.8.8.8       DNS       70 Standard query 0x0000 A amazon.com
  5189… 461007566.68…  10.240.26.55   8.8.8.8       DNS       71 Standard query 0x0000 A twitter.com
  6482… 461007566.68…  10.240.26.55   8.8.8.8       DNS       73 Standard query 0x0000 A wikipedia.org
  7816… 461007566.68…  10.240.26.55   8.8.8.8       DNS       77 Standard query 0x0000 A stackoverflow.com
```

```
› Frame 14655: 69 bytes on wire (552 bits), 69    0000  ff ff ff ff ff ff da 7f  5c 2b 6e df 08 00 45 00   ········ \+n···E·
› Ethernet II, Src: da:7f:5c:2b:6e:df (da:7f:5    0010  00 37 00 01 00 00 40 11  45 7f 0a f0 1a 37 08 08   ·7····@· E····7··
› Internet Protocol Version 4, Src: 10.240.26.    0020  08 08 5b 7f 00 35 00 23  16 b5 00 00 01 00 00 01   ··[··5·# ········
› User Datagram Protocol, Src Port: 23423, Dst    0030  00 00 00 00 00 00 05 61  70 70 6c 65 03 63 6f 6d   ·······a pple·com
› Domain Name System (query)                      0040  00 00 01 00 01                                     ·····
```

```
Domain Name System: Protocol        Packets: 801440 · Displayed: 6 (0.0%)        Profile: Default
```

Custom header value (HHMMSSID)	Domain name	Resolved IP address
18041600	apple.com	192.168.1.6
18041601	facebook.com	192.168.1.7
18041602	amazon.com	192.168.1.8
18041603	twitter.com	192.168.1.9
18041604	wikipedia.org	192.168.1.10
18041605	stackoverflow.com	192.168.1.6

Task-2: Traceroute Protocol Behaviour

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

By default, Windows tracert uses the ICMP Protocol. We can see from the figure that when we apply the ICMP filter and then run the command of tracert, then the packets are being captured, and whereas Linux uses the UDP protocol by default, as shown in the Wireshark packet captures.

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

1. Either the packets are blocked due to the Firewall or security settings.

2. Overload at the intermediate routers can also cause the drop of packets
   Rate limiting - intentionally enforces a cap on how many ICMP responses it will send per second.
   This is a policy decision (to prevent ICMP floods from consuming resources).

3. Router too busy / configured not to reply
   The router has higher-priority tasks (forwarding traffic) and may drop control-plane packets like traceroute probes if CPU or buffer resources are strained.
   This is due to resource constraints or configuration, not a fixed rate policy.

4. Here, since we have used VM for Linux os, an intermediate box like NAT may not translate or forward them correctly. This is due to resource constraints or configuration, not a fixed rate policy.

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

The IP header's TTL (Time To Live) field changes between successive probes. Each router that decrements the TTL to zero sends back an ICMP Time Exceeded, which allows traceroute to discover that hop.

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

Linux traceroute (default, UDP probes)
Intermediate hops → send ICMP Time Exceeded (when TTL = 0)

Final destination → sends ICMP Port Unreachable (because the UDP probe was sent to a high, unused port).

Windows tracert (ICMP Echo probes)
Intermediate hops → send ICMP Time Exceeded (when TTL = 0).

Final destination → sends ICMP Echo Reply (because the ICMP Echo Request actually reached it).

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

If UDP is blocked but ICMP is allowed, Linux traceroute fails (stars only), while Windows tracert still works correctly.

Linux traceroute (default = UDP probes)

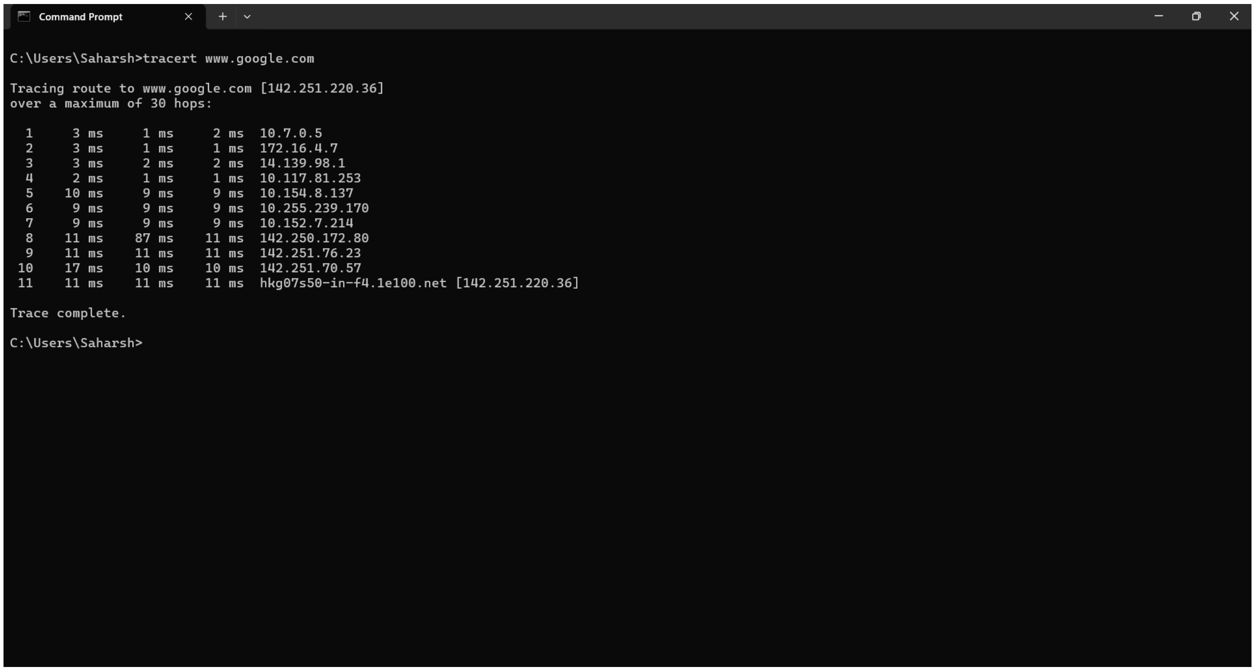
- Outbound UDP probes → Blocked by firewall
- That means the probes never reach the destination, and no ICMP replies come back.
- Result: traceroute output will mostly be `* * *` (no responses), i.e. it fails to trace the path.

Windows tracert (default = ICMP Echo probes)

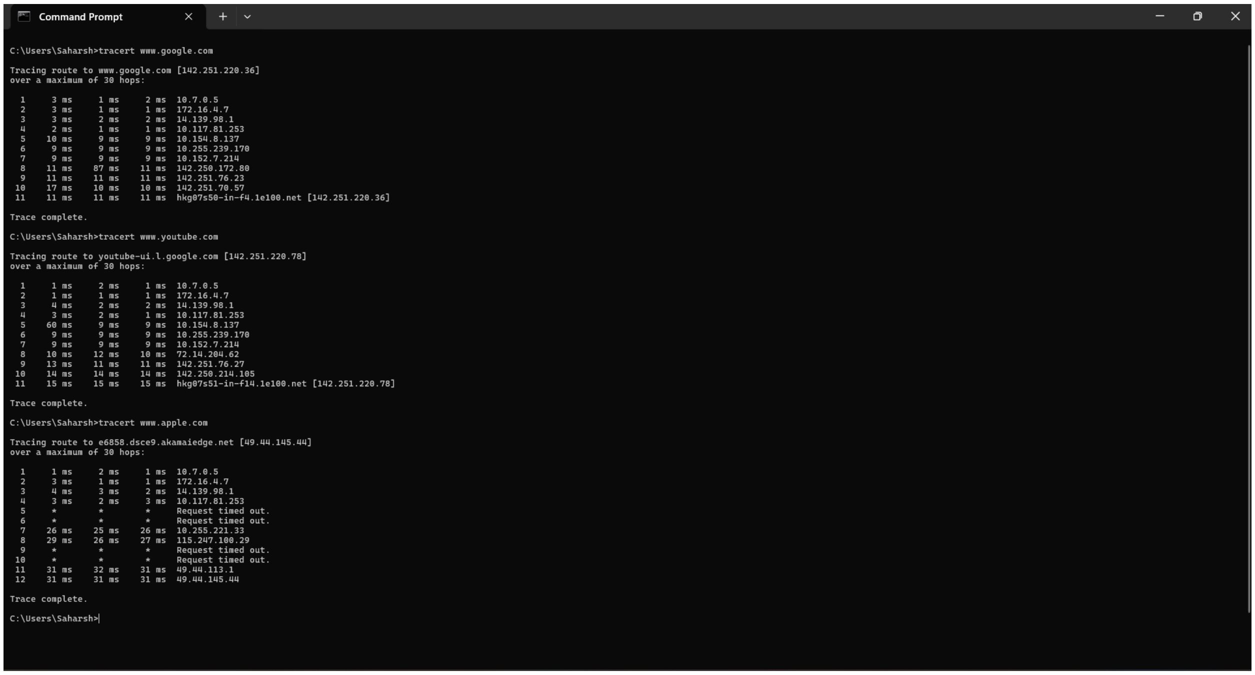
- Outbound ICMP Echo Requests → Allowed by firewall
- So probes go through, and intermediate routers send ICMP Time Exceeded as normal, and the destination sends ICMP Echo Reply

Result: tracert works normally and shows the route, while the Linux traceroute fails.

Windows:

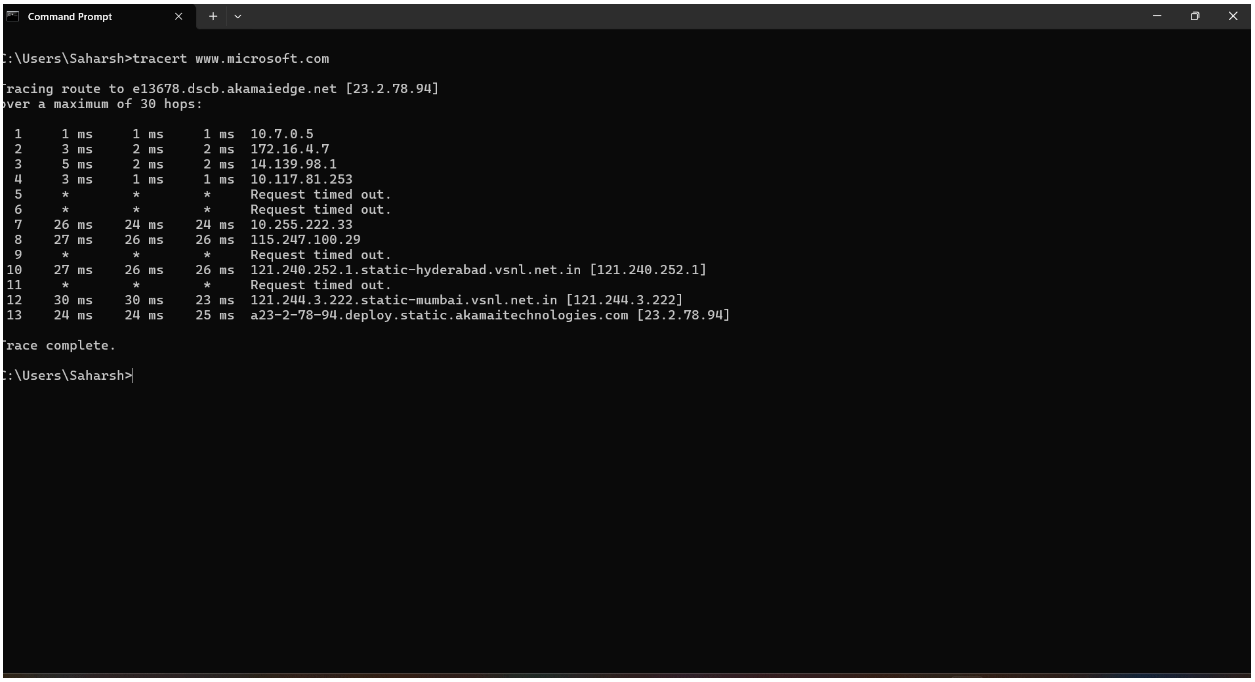


```
C:\Users\Saharsh>tracert www.google.com

Tracing route to www.google.com [142.251.220.36]
over a maximum of 30 hops:

  1     3 ms     1 ms     2 ms  10.7.0.5
  2     3 ms     1 ms     1 ms  172.16.4.7
  3     3 ms     2 ms     2 ms  14.139.98.1
  4     2 ms     1 ms     1 ms  10.117.81.253
  5    10 ms     9 ms     9 ms  10.154.8.137
  6     9 ms     9 ms     9 ms  10.255.239.170
  7     9 ms     9 ms     9 ms  10.152.7.214
  8    11 ms    87 ms    11 ms  142.250.172.80
  9    11 ms    11 ms    11 ms  142.251.76.23
 10    17 ms    10 ms    10 ms  142.251.70.57
 11    11 ms    11 ms    11 ms  hkg07s50-in-f4.1e100.net [142.251.220.36]

Trace complete.

C:\Users\Saharsh>
```

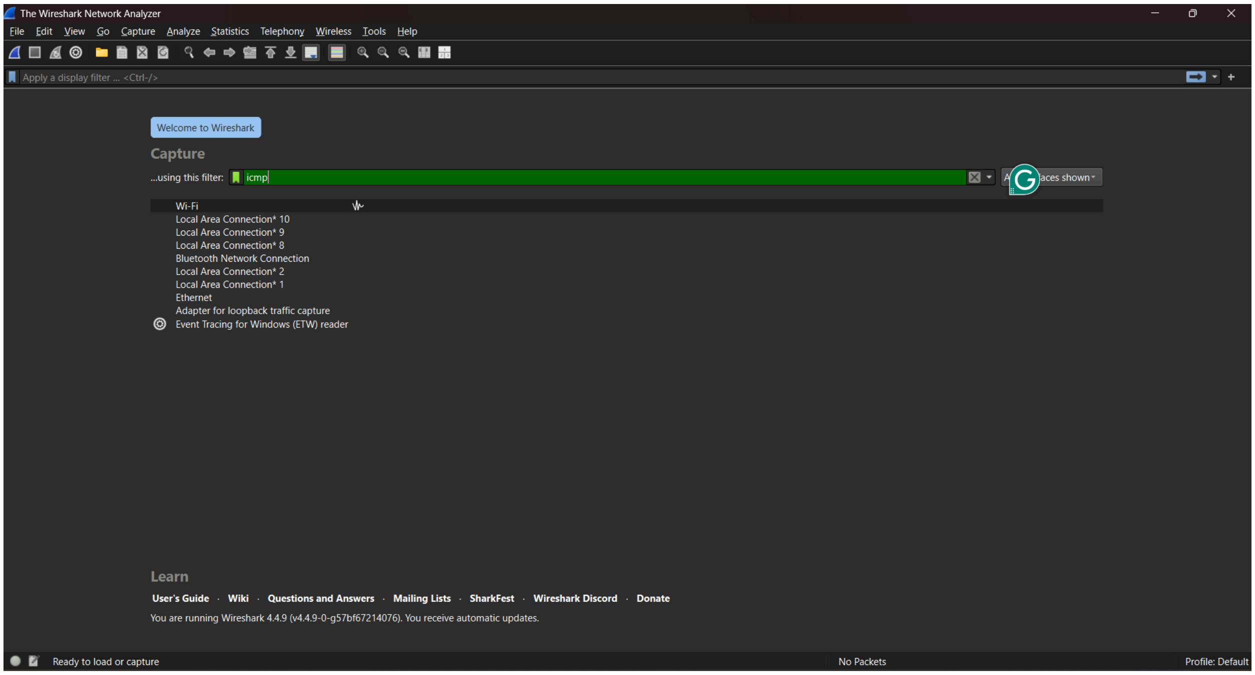


```
C:\Users\Saharsh>tracert www.google.com

Tracing route to www.google.com [142.251.220.36]
over a maximum of 30 hops:

  1     3 ms     1 ms     2 ms  10.7.0.5
  2     3 ms     1 ms     1 ms  172.16.4.7
  3     3 ms     2 ms     2 ms  14.139.98.1
  4     2 ms     1 ms     1 ms  10.117.81.253
  5    10 ms     9 ms     9 ms  10.154.8.137
  6     9 ms     9 ms     9 ms  10.255.239.170
  7     9 ms     9 ms     9 ms  10.152.7.214
  8    11 ms    87 ms    11 ms  142.250.172.80
  9    11 ms    11 ms    11 ms  142.251.76.23
 10    17 ms    10 ms    10 ms  142.251.70.57
 11    11 ms    11 ms    11 ms  hkg07s50-in-f4.1e100.net [142.251.220.36]

Trace complete.
```

```
C:\Users\Saharsh>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.251.220.78]
over a maximum of 30 hops:

  1     1 ms     2 ms     1 ms  10.7.0.5
  2     1 ms     1 ms     1 ms  172.16.4.7
  3     4 ms     2 ms     2 ms  14.139.98.1
  4     3 ms     2 ms     1 ms  10.117.81.253
  5    60 ms     9 ms     9 ms  10.154.8.137
  6     9 ms     9 ms     9 ms  10.255.239.170
  7     9 ms     9 ms     9 ms  10.152.7.214
  8    10 ms    12 ms    10 ms  72.14.204.62
  9    13 ms    11 ms    11 ms  142.251.76.27
 10    14 ms    14 ms    14 ms  142.250.214.105
 11    15 ms    15 ms    15 ms  hkg07s51-in-f14.1e100.net [142.251.220.78]

Trace complete.

C:\Users\Saharsh>tracert www.apple.com

Tracing route to e6858.dsce9.akamaiedge.net [49.44.145.44]
over a maximum of 30 hops:

  1     1 ms     2 ms     1 ms  10.7.0.5
  2     3 ms     1 ms     1 ms  172.16.4.7
  3     4 ms     3 ms     2 ms  14.139.98.1
  4     3 ms     2 ms     3 ms  10.117.81.253
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    26 ms    25 ms    26 ms  10.255.221.33
  8    29 ms    26 ms    27 ms  115.247.100.29
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    31 ms    32 ms    31 ms  49.44.113.1
 12    31 ms    31 ms    31 ms  49.44.145.44

Trace complete.

C:\Users\Saharsh>
```



```
:\Users\Saharsh>tracert www.microsoft.com

racing route to e13678.dscb.akamaiedge.net [23.2.78.94]
ver a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  10.7.0.5
  2     3 ms     2 ms     2 ms  172.16.4.7
  3     5 ms     2 ms     2 ms  14.139.98.1
  4     3 ms     1 ms     1 ms  10.117.81.253
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    26 ms    24 ms    24 ms  10.255.222.33
  8    27 ms    26 ms    26 ms  115.247.100.29
  9     *        *        *     Request timed out.
 10    27 ms    26 ms    26 ms  121.240.252.1.static-hyderabad.vsnl.net.in [121.240.252.1]
 11     *        *        *     Request timed out.
 12    30 ms    30 ms    23 ms  121.244.3.222.static-mumbai.vsnl.net.in [121.244.3.222]
 13    24 ms    24 ms    25 ms  a23-2-78-94.deploy.static.akamaitechnologies.com [23.2.78.94]

race complete.

:\Users\Saharsh>
```



Capture

...using this filter: icmp

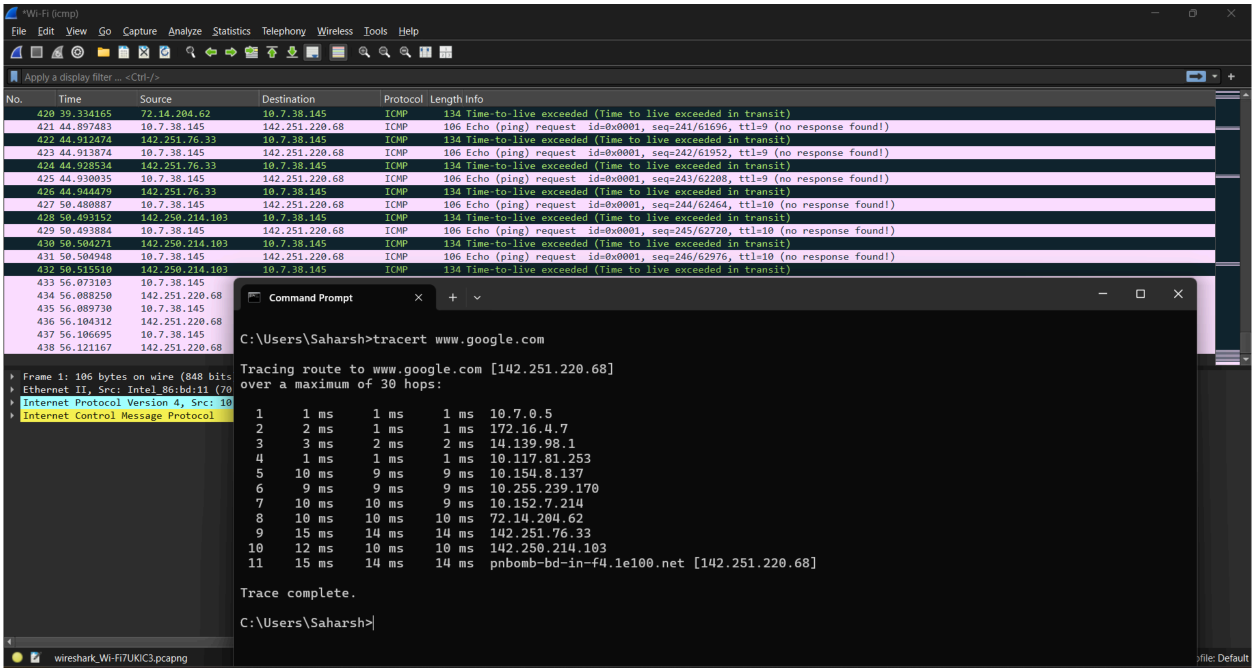
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Ethernet
Adapter for loopback traffic capture
Event Tracing for Windows (ETW) reader

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.9 (v4.4.9-0-g57bf67214076). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default



*Wi-Fi (icmp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

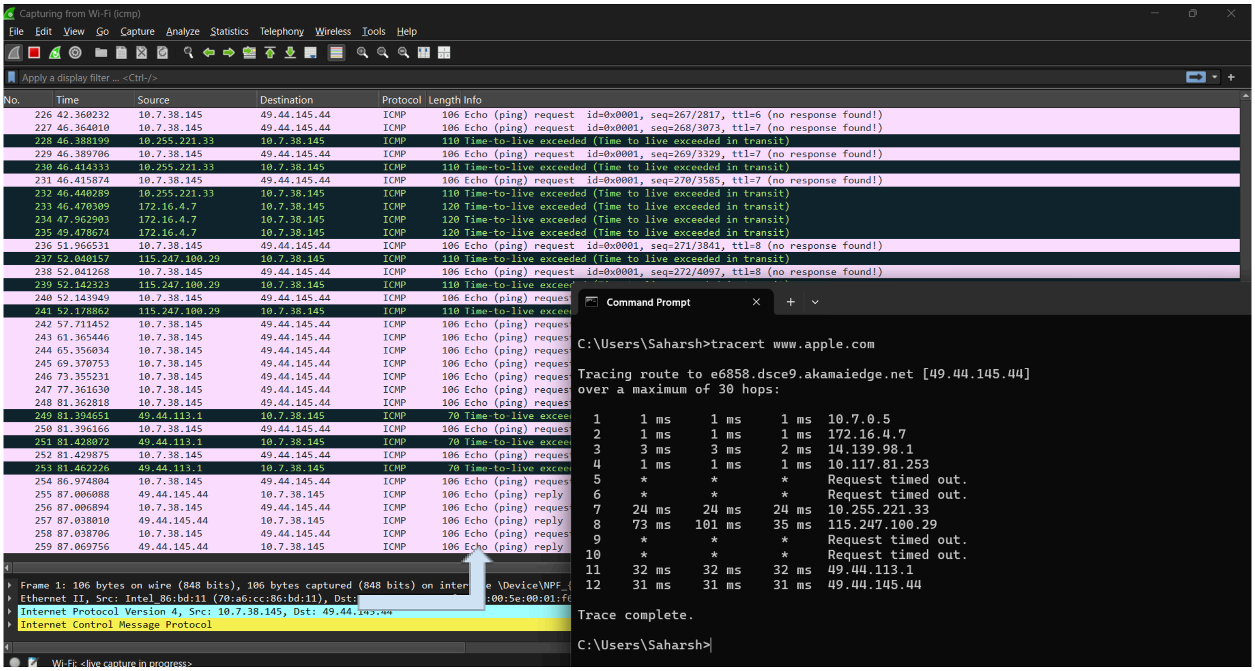
```
No.   Time          Source            Destination       Protocol Length Info
  420 39.334165     72.14.204.62      10.7.38.145       ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  421 44.897483     10.7.38.145       142.251.220.68    ICMP     106 Echo (ping) request  id=0x0001, seq=241/61696, ttl=9 (no response found!)
  422 44.912474     142.251.76.33     10.7.38.145       ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  423 44.913874     10.7.38.145       142.251.220.68    ICMP     106 Echo (ping) request  id=0x0001, seq=242/61952, ttl=9 (no response found!)
  424 44.928534     142.251.76.33     10.7.38.145       ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  425 44.930035     10.7.38.145       142.251.220.68    ICMP     106 Echo (ping) request  id=0x0001, seq=243/62208, ttl=9 (no response found!)
  426 44.944479     142.251.76.33     10.7.38.145       ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  427 50.480887     10.7.38.145       142.251.220.68    ICMP     106 Echo (ping) request  id=0x0001, seq=244/62464, ttl=10 (no response found!)
  428 50.493152     142.250.214.103   10.7.38.145       ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  429 50.493884     10.7.38.145       142.251.220.68    ICMP     106 Echo (ping) request  id=0x0001, seq=245/62720, ttl=10 (no response found!)
  430 50.504271     142.250.214.103   10.7.38.145       ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  431 50.504948     10.7.38.145       142.251.220.68    ICMP     106 Echo (ping) request  id=0x0001, seq=246/62976, ttl=10 (no response found!)
  432 50.515510     142.250.214.103   10.7.38.145       ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  433 56.073103     10.7.38.145
  434 56.088250     142.251.220.68
  435 56.089730     10.7.38.145
  436 56.104312     142.251.220.68
  437 56.106695     10.7.38.145
  438 56.121167     142.251.220.68

▸ Frame 1: 106 bytes on wire (848 bits
▸ Ethernet II, Src: Intel_86:bd:11 (70
▸ Internet Protocol Version 4, Src: 10
▸ Internet Control Message Protocol
```

wireshark_Wi-Fi7UKIC3.pcapng

ofile: Default

Command Prompt

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

Tracing route to www.google.com [142.251.220.68]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  10.7.0.5
  2     2 ms     1 ms     1 ms  172.16.4.7
  3     3 ms     2 ms     2 ms  14.139.98.1
  4     1 ms     1 ms     1 ms  10.117.81.253
  5    10 ms     9 ms     9 ms  10.154.8.137
  6     9 ms     9 ms     9 ms  10.255.239.170
  7    10 ms    10 ms     9 ms  10.152.7.214
  8    10 ms    10 ms    10 ms  72.14.204.62
  9    15 ms    14 ms    14 ms  142.251.76.33
 10    12 ms    10 ms    10 ms  142.250.214.103
 11    15 ms    14 ms    14 ms  pnbomb-bd-in-f4.1e100.net [142.251.220.68]

Trace complete.

C:\Users\Saharsh>
```



Capturing from Wi-Fi (icmp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source            Destination       Protocol Length Info
  226 42.360232     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) request  id=0x0001, seq=267/2817, ttl=6 (no response found!)
  227 46.364010     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) request  id=0x0001, seq=268/3073, ttl=7 (no response found!)
  228 46.388199     10.255.221.33     10.7.38.145       ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
  229 46.389706     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) request  id=0x0001, seq=269/3329, ttl=7 (no response found!)
  230 46.414333     10.255.221.33     10.7.38.145       ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
  231 46.415874     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) request  id=0x0001, seq=270/3585, ttl=7 (no response found!)
  232 46.440289     10.255.221.33     10.7.38.145       ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
  233 46.470309     172.16.4.7        10.7.38.145       ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
  234 47.962903     172.16.4.7        10.7.38.145       ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
  235 49.478674     172.16.4.7        10.7.38.145       ICMP     120 Time-to-live exceeded (Time to live exceeded in transit)
  236 51.966531     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) request  id=0x0001, seq=271/3841, ttl=8 (no response found!)
  237 52.040157     115.247.100.29    10.7.38.145       ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
  238 52.041268     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) request  id=0x0001, seq=272/4097, ttl=8 (no response found!)
  239 52.142323     115.247.100.29    10.7.38.145       ICMP     110 Time-to-live exceed
  240 52.143949     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  241 52.178862     115.247.100.29    10.7.38.145       ICMP     110 Time-to-live excee
  242 57.711452     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  243 61.365446     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  244 65.356034     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  245 69.370753     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  246 73.355231     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  247 77.361630     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  248 81.362818     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  249 81.394651     49.44.113.1       10.7.38.145       ICMP      70 Time-to-live excee
  250 81.396166     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  251 81.428072     49.44.113.1       10.7.38.145       ICMP      70 Time-to-live excee
  252 81.429875     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  253 81.462226     49.44.113.1       10.7.38.145       ICMP      70 Time-to-live excee
  254 86.974804     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  255 87.006088     49.44.145.44      10.7.38.145       ICMP     106 Echo (ping) reply
  256 87.006894     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  257 87.038010     49.44.145.44      10.7.38.145       ICMP     106 Echo (ping) reply
  258 87.038706     10.7.38.145       49.44.145.44      ICMP     106 Echo (ping) reques
  259 87.069756     49.44.145.44      10.7.38.145       ICMP     106 Echo (ping) reply

▸ Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on inter  e \Device\NPF_
▸ Ethernet II, Src: Intel_86:bd:11 (70:a6:cc:86:bd:11), Dst:          :00:5e:00:01:f
▸ Internet Protocol Version 4, Src: 10.7.38.145, Dst: 49.44.
▸ Internet Control Message Protocol
```

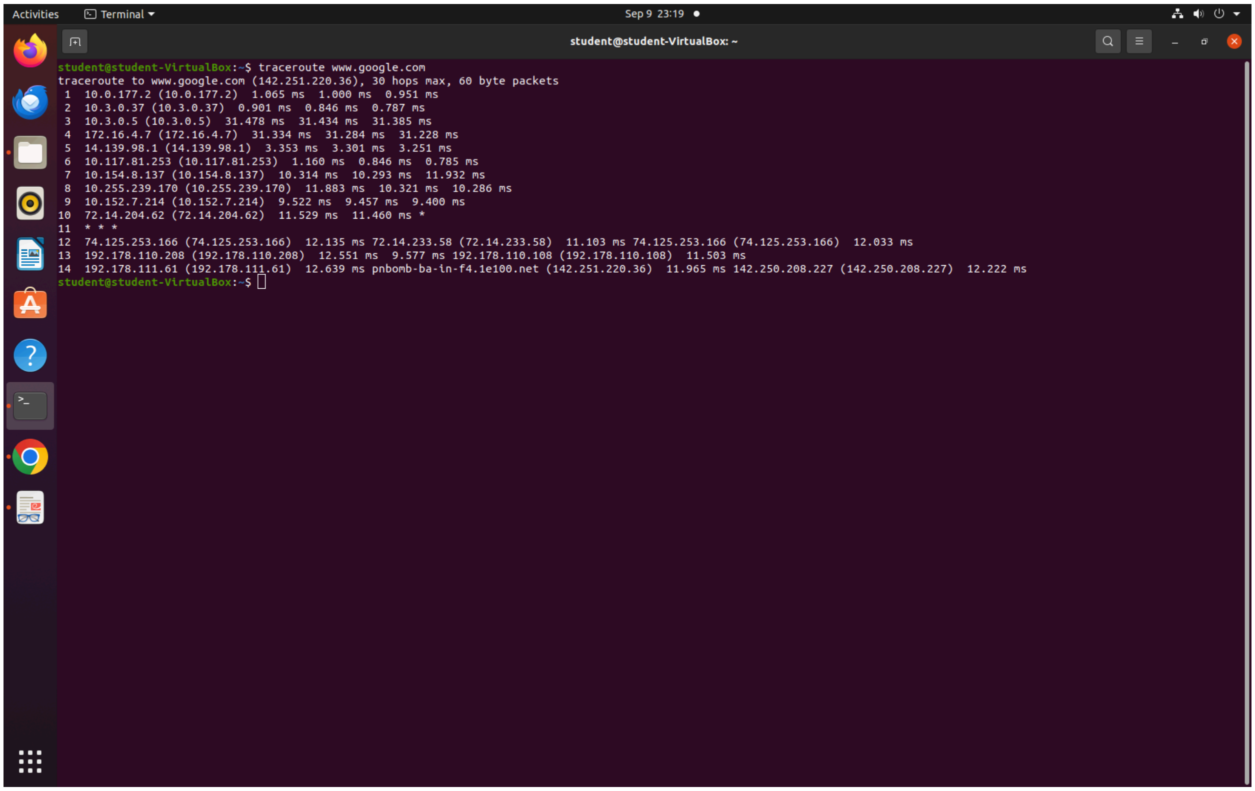
Wi-Fi: <live capture in progress>

Command Prompt

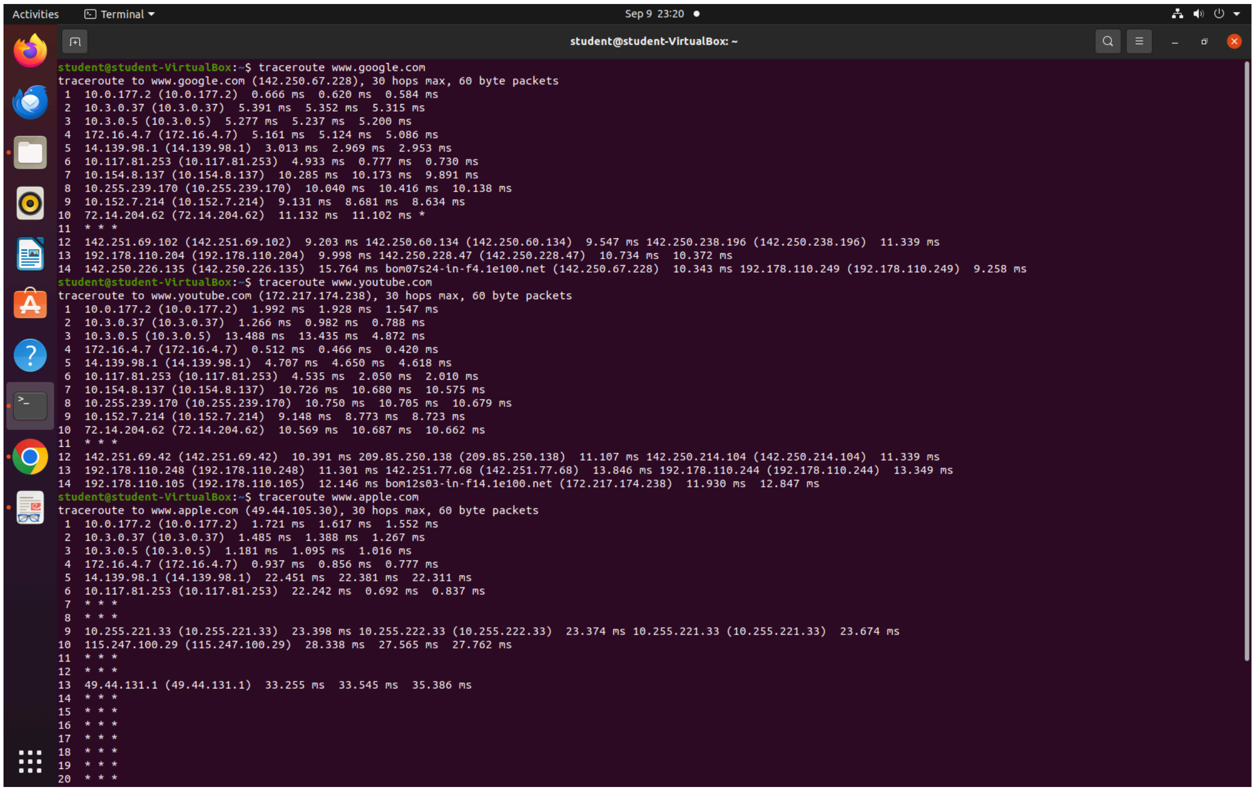
```
C:\Users\Saharsh>tracert www.apple.com

Tracing route to e6858.dsce9.akamaiedge.net [49.44.145.44]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  10.7.0.5
  2     1 ms     1 ms     1 ms  172.16.4.7
  3     3 ms     3 ms     2 ms  14.139.98.1
  4     1 ms     1 ms     1 ms  10.117.81.253
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    24 ms    24 ms    24 ms  10.255.221.33
  8    73 ms   101 ms    35 ms  115.247.100.29
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    32 ms    32 ms    32 ms  49.44.113.1
 12    31 ms    31 ms    31 ms  49.44.145.44

Trace complete.

C:\Users\Saharsh>
```

Here, we can see the final packet has an Echo reply in case of Windows

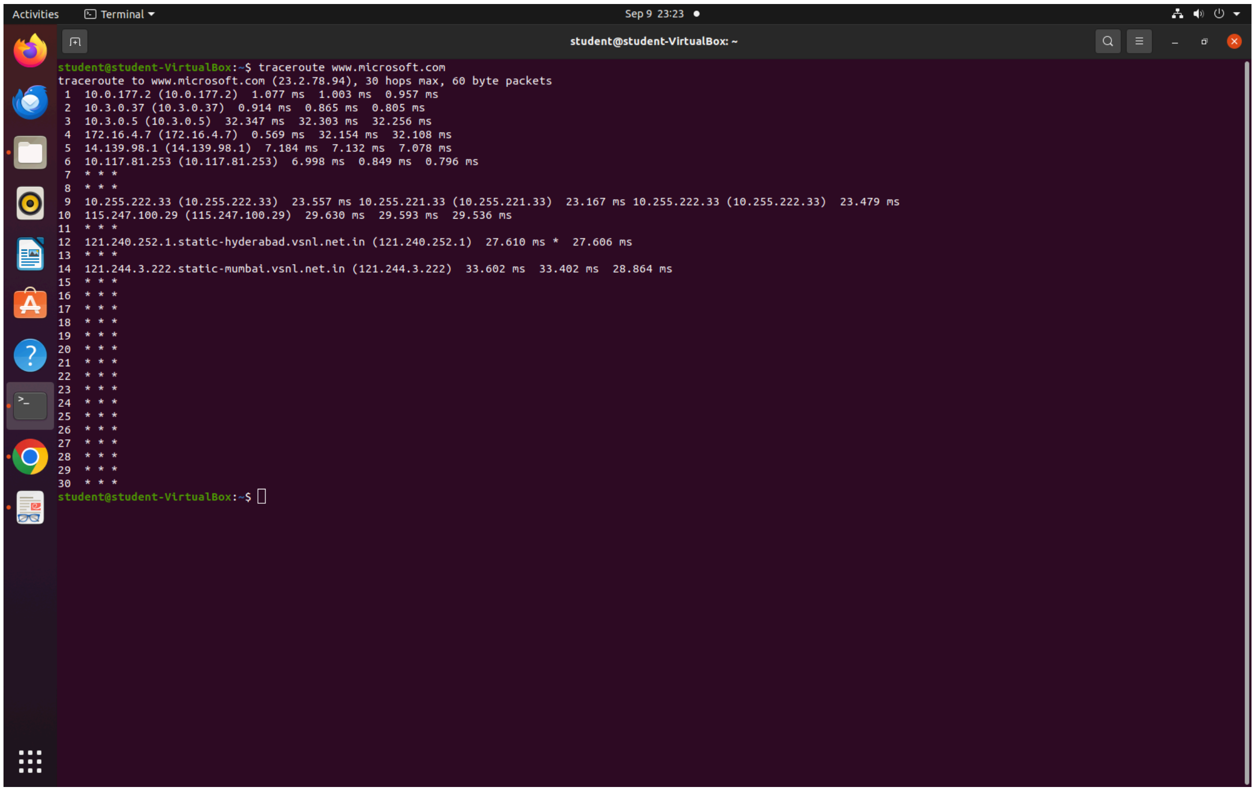
Linux:



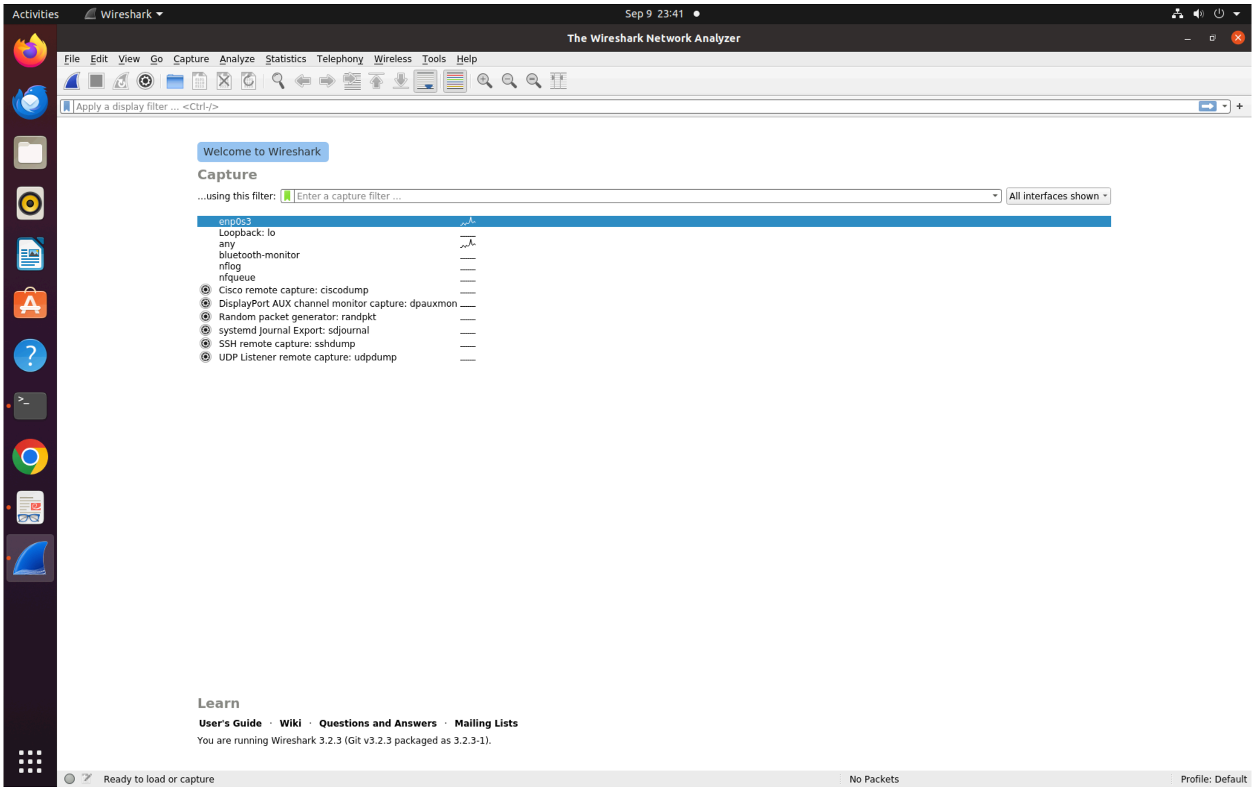
```
student@student-VirtualBox:~$ traceroute www.google.com
traceroute to www.google.com (142.251.220.36), 30 hops max, 60 byte packets
 1  10.0.177.2 (10.0.177.2)  1.065 ms  1.000 ms  0.951 ms
 2  10.3.0.37 (10.3.0.37)  0.901 ms  0.846 ms  0.787 ms
 3  10.3.0.5 (10.3.0.5)  31.478 ms  31.434 ms  31.385 ms
 4  172.16.4.7 (172.16.4.7)  31.334 ms  31.284 ms  31.228 ms
 5  14.139.98.1 (14.139.98.1)  3.353 ms  3.301 ms  3.251 ms
 6  10.117.81.253 (10.117.81.253)  1.160 ms  0.846 ms  0.785 ms
 7  10.154.8.137 (10.154.8.137)  10.314 ms  10.293 ms  11.932 ms
 8  10.255.239.170 (10.255.239.170)  11.883 ms  10.321 ms  10.286 ms
 9  10.152.7.214 (10.152.7.214)  9.522 ms  9.457 ms  9.400 ms
10  72.14.204.62 (72.14.204.62)  11.529 ms  11.460 ms *
11  * * *
12  74.125.253.166 (74.125.253.166)  12.135 ms 72.14.233.58 (72.14.233.58)  11.103 ms 74.125.253.166 (74.125.253.166)  12.033 ms
13  192.178.110.208 (192.178.110.208)  12.551 ms  9.577 ms 192.178.110.108 (192.178.110.108)  11.503 ms
14  192.178.111.61 (192.178.111.61)  12.639 ms pnbomb-ba-in-f4.1e100.net (142.251.220.36)  11.965 ms 142.250.208.227 (142.250.208.227)  12.222 ms
student@student-VirtualBox:~$ 
```



```
student@student-VirtualBox:~$ traceroute www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1  10.0.177.2 (10.0.177.2)  0.666 ms  0.620 ms  0.584 ms
 2  10.3.0.37 (10.3.0.37)  5.391 ms  5.352 ms  5.315 ms
 3  10.3.0.5 (10.3.0.5)  5.277 ms  5.237 ms  5.200 ms
 4  172.16.4.7 (172.16.4.7)  5.161 ms  5.124 ms  5.086 ms
 5  14.139.98.1 (14.139.98.1)  3.013 ms  2.969 ms  2.953 ms
 6  10.117.81.253 (10.117.81.253)  4.933 ms  0.777 ms  0.730 ms
 7  10.154.8.137 (10.154.8.137)  10.285 ms  10.173 ms  9.891 ms
 8  10.255.239.170 (10.255.239.170)  10.040 ms  10.416 ms  10.138 ms
 9  10.152.7.214 (10.152.7.214)  9.131 ms  8.681 ms  8.634 ms
10  72.14.204.62 (72.14.204.62)  11.132 ms  11.102 ms *
11  * * *
12  142.251.69.102 (142.251.69.102)  9.203 ms 142.250.60.134 (142.250.60.134)  9.547 ms 142.250.238.196 (142.250.238.196)  11.339 ms
13  192.178.110.204 (192.178.110.204)  9.998 ms 142.250.228.47 (142.250.228.47)  10.734 ms  10.372 ms
14  142.250.226.135 (142.250.226.135)  15.764 ms bom07s24-in-f4.1e100.net (142.250.67.228)  10.343 ms 192.178.110.249 (192.178.110.249)  9.258 ms
student@student-VirtualBox:~$ traceroute www.youtube.com
traceroute to www.youtube.com (172.217.174.238), 30 hops max, 60 byte packets
 1  10.0.177.2 (10.0.177.2)  1.992 ms  1.928 ms  1.547 ms
 2  10.3.0.37 (10.3.0.37)  1.266 ms  0.982 ms  0.788 ms
 3  10.3.0.5 (10.3.0.5)  13.488 ms  13.435 ms  4.872 ms
 4  172.16.4.7 (172.16.4.7)  0.512 ms  0.466 ms  0.420 ms
 5  14.139.98.1 (14.139.98.1)  4.707 ms  4.650 ms  4.618 ms
 6  10.117.81.253 (10.117.81.253)  4.535 ms  2.050 ms  2.010 ms
 7  10.154.8.137 (10.154.8.137)  10.726 ms  10.680 ms  10.575 ms
 8  10.255.239.170 (10.255.239.170)  10.750 ms  10.705 ms  10.679 ms
 9  10.152.7.214 (10.152.7.214)  9.148 ms  8.773 ms  8.723 ms
10  72.14.204.62 (72.14.204.62)  10.569 ms  10.687 ms  10.662 ms
11  * * *
12  142.251.69.42 (142.251.69.42)  10.391 ms 209.85.250.138 (209.85.250.138)  11.107 ms 142.250.214.104 (142.250.214.104)  11.339 ms
13  192.178.110.248 (192.178.110.248)  11.301 ms 142.251.77.68 (142.251.77.68)  13.846 ms 192.178.110.244 (192.178.110.244)  13.349 ms
14  192.178.110.105 (192.178.110.105)  12.146 ms bom12s03-in-f14.1e100.net (172.217.174.238)  11.930 ms  12.847 ms
student@student-VirtualBox:~$ traceroute www.apple.com
traceroute to www.apple.com (49.44.105.30), 30 hops max, 60 byte packets
 1  10.0.177.2 (10.0.177.2)  1.721 ms  1.617 ms  1.552 ms
 2  10.3.0.37 (10.3.0.37)  1.485 ms  1.388 ms  1.267 ms
 3  10.3.0.5 (10.3.0.5)  1.181 ms  1.095 ms  1.016 ms
 4  172.16.4.7 (172.16.4.7)  0.937 ms  0.856 ms  0.777 ms
 5  14.139.98.1 (14.139.98.1)  22.451 ms  22.381 ms  22.311 ms
 6  10.117.81.253 (10.117.81.253)  22.242 ms  0.692 ms  0.837 ms
 7  * * *
 8  * * *
 9  10.255.221.33 (10.255.221.33)  23.398 ms 10.255.222.33 (10.255.222.33)  23.374 ms 10.255.221.33 (10.255.221.33)  23.674 ms
10  115.247.100.29 (115.247.100.29)  28.338 ms  27.565 ms  27.762 ms
11  * * *
12  * * *
13  49.44.131.1 (49.44.131.1)  33.255 ms  33.545 ms  35.386 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
```



```
student@student-VirtualBox:~$ traceroute www.microsoft.com
traceroute to www.microsoft.com (23.2.78.94), 30 hops max, 60 byte packets
 1  10.0.177.2 (10.0.177.2)  1.077 ms  1.003 ms  0.957 ms
 2  10.3.0.37 (10.3.0.37)  0.914 ms  0.865 ms  0.805 ms
 3  10.3.0.5 (10.3.0.5)  32.347 ms  32.303 ms  32.256 ms
 4  172.16.4.7 (172.16.4.7)  0.569 ms  32.154 ms  32.108 ms
 5  14.139.98.1 (14.139.98.1)  7.184 ms  7.132 ms  7.078 ms
 6  10.117.81.253 (10.117.81.253)  6.998 ms  0.849 ms  0.796 ms
 7  * * *
 8  * * *
 9  10.255.222.33 (10.255.222.33)  23.557 ms 10.255.221.33 (10.255.221.33)  23.167 ms 10.255.222.33 (10.255.222.33)  23.479 ms
10  115.247.100.29 (115.247.100.29)  29.630 ms  29.593 ms  29.536 ms
11  * * *
12  121.240.252.1.static-hyderabad.vsnl.net.in (121.240.252.1)  27.610 ms *  27.606 ms
13  * * *
14  121.244.3.222.static-mumbai.vsnl.net.in (121.244.3.222)  33.602 ms  33.402 ms  28.864 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
student@student-VirtualBox:~$ 
```



Activities
Wireshark
Sep 9 23:41
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Capture

...using this filter: Enter a capture filter … All interfaces shown

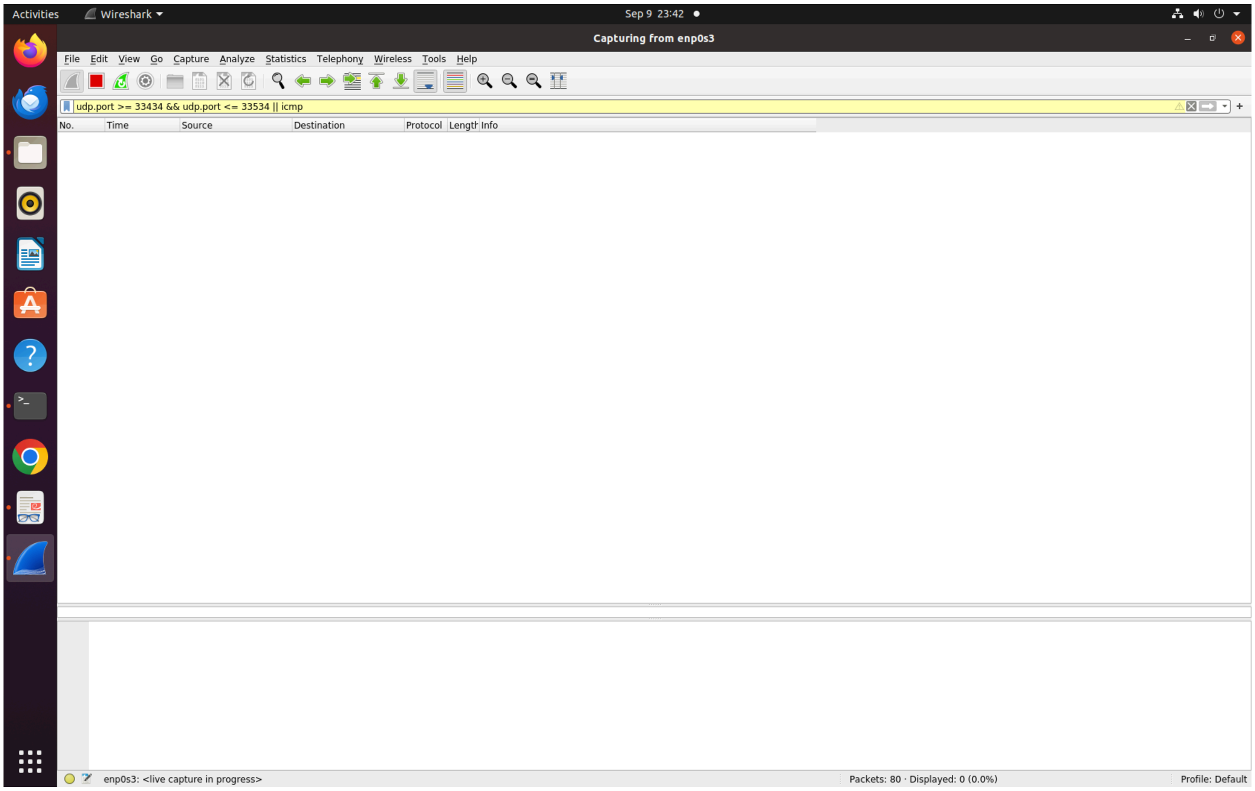
enp0s3
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

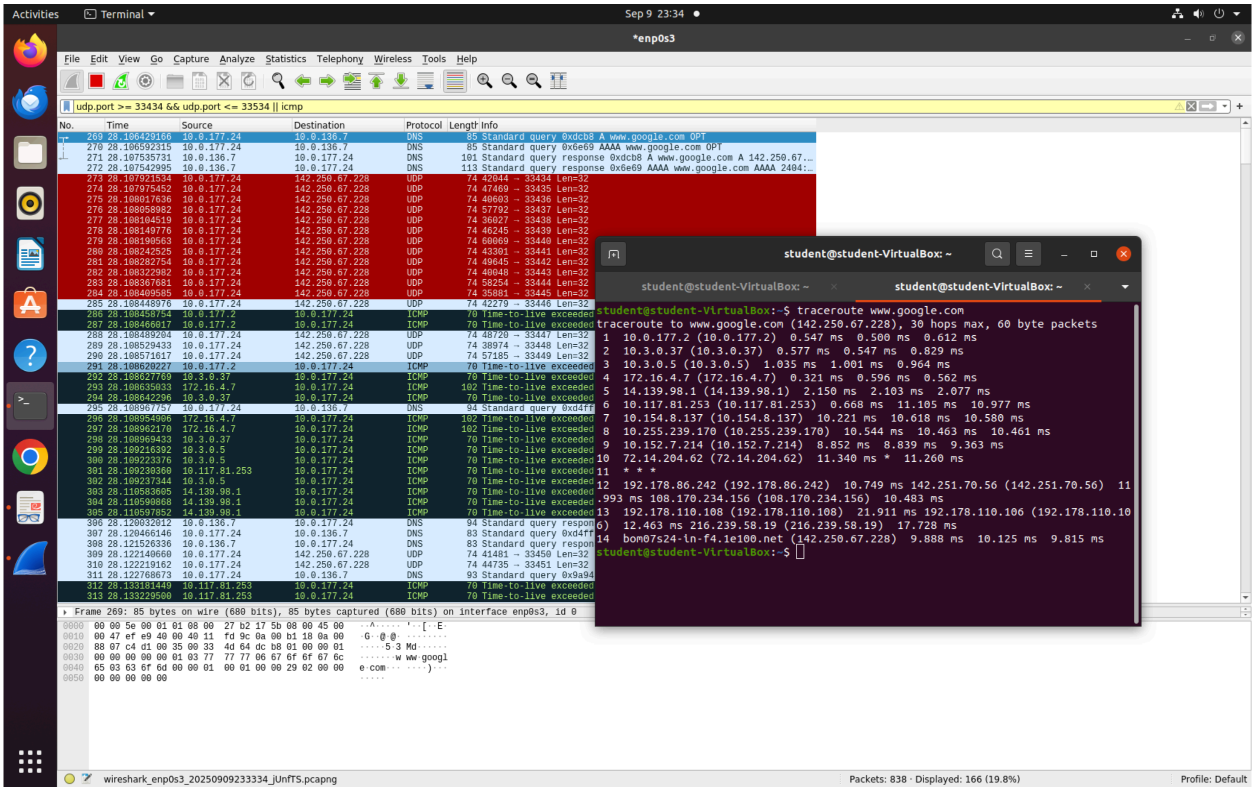
Ready to load or capture   No Packets   Profile: Default


Activities
Wireshark
Sep 9 23:42
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port >= 33434 && udp.port <= 33534 || icmp
```

```
No.   Time   Source   Destination   Protocol   Length Info
```

```
enp0s3: <live capture in progress>                Packets: 80 · Displayed: 0 (0.0%)                Profile: Default
```


Activities
Terminal
Sep 9 23:34
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port >= 33434 && udp.port <= 33534 || icmp
```

```
No.   Time          Source         Destination    Protocol Length Info
  269 28.106429166  10.0.177.24    10.0.136.7     DNS       85 Standard query 0xdcb8 A www.google.com OPT
  270 28.106592315  10.0.177.24    10.0.136.7     DNS       85 Standard query 0x6e69 AAAA www.google.com OPT
  271 28.107535731  10.0.136.7     10.0.177.24    DNS      101 Standard query response 0xdcb8 A www.google.com A 142.250.67.…
  272 28.107542995  10.0.136.7     10.0.177.24    DNS      113 Standard query response 0x6e69 AAAA www.google.com AAAA 2404:…
  273 28.107921534  10.0.177.24    142.250.67.228 UDP       74 42044 → 33434 Len=32
  274 28.107975452  10.0.177.24    142.250.67.228 UDP       74 47469 → 33435 Len=32
  275 28.108017636  10.0.177.24    142.250.67.228 UDP       74 40603 → 33436 Len=32
  276 28.108058982  10.0.177.24    142.250.67.228 UDP       74 57792 → 33437 Len=32
  277 28.108104519  10.0.177.24    142.250.67.228 UDP       74 36027 → 33438 Len=32
  278 28.108149776  10.0.177.24    142.250.67.228 UDP       74 46245 → 33439 Len=32
  279 28.108190563  10.0.177.24    142.250.67.228 UDP       74 60069 → 33440 Len=32
  280 28.108242525  10.0.177.24    142.250.67.228 UDP       74 43301 → 33441 Len=32
  281 28.108282754  10.0.177.24    142.250.67.228 UDP       74 49645 → 33442 Len=32
  282 28.108322982  10.0.177.24    142.250.67.228 UDP       74 40048 → 33443 Len=32
  283 28.108367681  10.0.177.24    142.250.67.228 UDP       74 58254 → 33444 Len=32
  284 28.108409585  10.0.177.24    142.250.67.228 UDP       74 35881 → 33445 Len=32
  285 28.108448976  10.0.177.24    142.250.67.228 UDP       74 42279 → 33446 Len=32
  286 28.108458754  10.0.177.2     10.0.177.24    ICMP      70 Time-to-live exceeded
  287 28.108466017  10.0.177.2     10.0.177.24    ICMP      70 Time-to-live exceeded
  288 28.108489204  10.0.177.24    142.250.67.228 UDP       74 48720 → 33447 Len=32
  289 28.108529433  10.0.177.24    142.250.67.228 UDP       74 38974 → 33448 Len=32
  290 28.108571617  10.0.177.24    142.250.67.228 UDP       74 57185 → 33449 Len=32
  291 28.108620227  10.0.177.2     10.0.177.24    ICMP      70 Time-to-live exceeded
  292 28.108627769  10.3.0.37      10.0.177.24    ICMP      70 Time-to-live exceeded
  293 28.108635033  172.16.4.7     10.0.177.24    ICMP     102 Time-to-live exceeded
  294 28.108642296  10.3.0.37      10.0.177.24    ICMP      70 Time-to-live exceeded
  295 28.108967757  10.0.177.24    10.0.136.7     DNS       94 Standard query 0xd4ff
  296 28.108954906  172.16.4.7     10.0.177.24    ICMP     102 Time-to-live exceeded
  297 28.108962170  172.16.4.7     10.0.177.24    ICMP     102 Time-to-live exceeded
  298 28.108969433  10.3.0.37      10.0.177.24    ICMP      70 Time-to-live exceeded
  299 28.109216392  10.3.0.5       10.0.177.24    ICMP      70 Time-to-live exceeded
  300 28.109223376  10.3.0.5       10.0.177.24    ICMP      70 Time-to-live exceeded
  301 28.109230360  10.117.81.253  10.0.177.24    ICMP      70 Time-to-live exceeded
  302 28.109237344  10.3.0.5       10.0.177.24    ICMP      70 Time-to-live exceeded
  303 28.110583605  14.139.98.1    10.0.177.24    ICMP      70 Time-to-live exceeded
  304 28.110590868  14.139.98.1    10.0.177.24    ICMP      70 Time-to-live exceeded
  305 28.110597852  14.139.98.1    10.0.177.24    ICMP      70 Time-to-live exceeded
  306 28.120032012  10.0.136.7     10.0.177.24    DNS       94 Standard query respon
  307 28.120466146  10.0.177.24    10.0.136.7     DNS       83 Standard query 0xd4ff
  308 28.121526336  10.0.136.7     10.0.177.24    DNS       83 Standard query respon
  309 28.122140660  10.0.177.24    142.250.67.228 UDP       74 41481 → 33450 Len=32
  310 28.122219162  10.0.177.24    142.250.67.228 UDP       74 44735 → 33451 Len=32
  311 28.122768673  10.0.177.24    10.0.136.7     DNS       93 Standard query 0x9a94
  312 28.133181449  10.117.81.253  10.0.177.24    ICMP      70 Time-to-live exceeded
  313 28.133229500  10.117.81.253  10.0.177.24    ICMP      70 Time-to-live exceeded
```

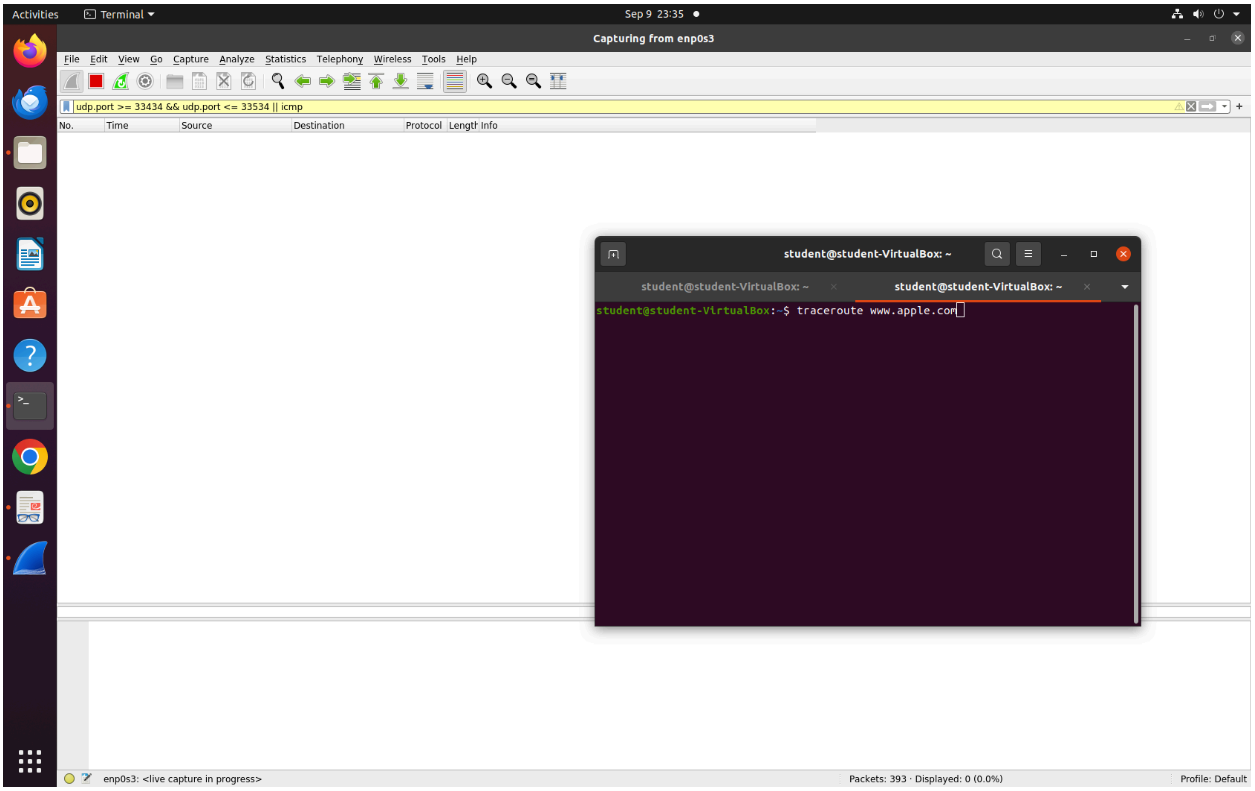
```
Frame 269: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface enp0s3, id 0
```

```
0000  00 00 5e 00 01 01 08 00  27 b2 17 5b 08 00 45 00   ··^·····'··[··E·
0010  00 47 ef e9 40 00 40 11  fd 9c 0a 00 b1 18 0a 00   ·G··@·@·········
0020  88 07 c4 d1 00 35 00 33  4d 64 dc b8 01 00 00 01   ·····5·3Md······
0030  00 00 00 00 00 01 03 77  77 77 06 67 6f 6f 67 6c   ·······www·googl
0040  65 03 63 6f 6d 00 00 01  00 01 00 00 29 02 00 00   e·com·······)···
0050  00 00 00 00 00                                     ·····
```

student@student-VirtualBox: ~
student@student-VirtualBox: ~
student@student-VirtualBox: ~

```
student@student-VirtualBox:~$ traceroute www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1  10.0.177.2 (10.0.177.2)  0.547 ms  0.500 ms  0.612 ms
 2  10.3.0.37 (10.3.0.37)  0.577 ms  0.547 ms  0.829 ms
 3  10.3.0.5 (10.3.0.5)  1.035 ms  1.001 ms  0.964 ms
 4  172.16.4.7 (172.16.4.7)  0.321 ms  0.596 ms  0.562 ms
 5  14.139.98.1 (14.139.98.1)  2.150 ms  2.103 ms  2.077 ms
 6  10.117.81.253 (10.117.81.253)  0.668 ms  11.105 ms  10.977 ms
 7  10.154.8.137 (10.154.8.137)  10.221 ms  10.618 ms  10.580 ms
 8  10.255.239.170 (10.255.239.170)  10.544 ms  10.463 ms  10.461 ms
 9  10.152.7.214 (10.152.7.214)  8.852 ms  8.839 ms  9.363 ms
10  72.14.204.62 (72.14.204.62)  11.340 ms *  11.260 ms
11  * * *
12  192.178.86.242 (192.178.86.242)  10.749 ms 142.251.70.56 (142.251.70.56)  11
.993 ms 108.170.234.156 (108.170.234.156)  10.483 ms
13  192.178.110.108 (192.178.110.108)  21.911 ms 192.178.110.106 (192.178.110.10
6)  12.463 ms 216.239.58.19 (216.239.58.19)  17.728 ms
14  bom07s24-in-f4.1e100.net (142.250.67.228)  9.888 ms  10.125 ms  9.815 ms
student@student-VirtualBox:~$ 
```

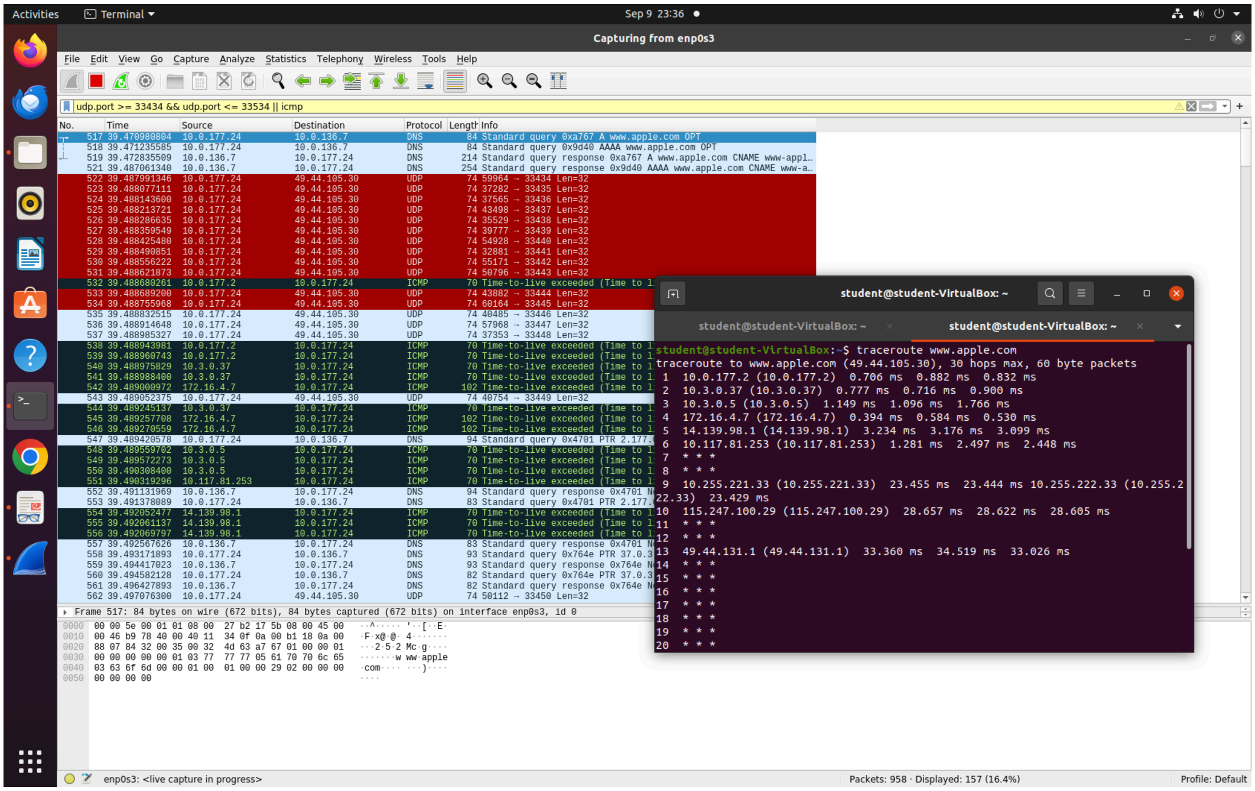
```
wireshark_enp0s3_20250909233334_jUnfTS.pcapng                Packets: 838 · Displayed: 166 (19.8%)                Profile: Default
```


Activities
Terminal
Sep 9 23:35
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
student@student-VirtualBox: ~
student@student-VirtualBox: ~
student@student-VirtualBox: ~

```
udp.port >= 33434 && udp.port <= 33534 || icmp
```

```
student@student-VirtualBox:~$ traceroute www.apple.com
```

enp0s3: <live capture in progress>   Packets: 393 · Displayed: 0 (0.0%)   Profile: Default


Activities
Terminal
Sep 9 23:36
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
student@student-VirtualBox: ~
student@student-VirtualBox: ~
student@student-VirtualBox: ~

```
udp.port >= 33434 && udp.port <= 33534 || icmp
```

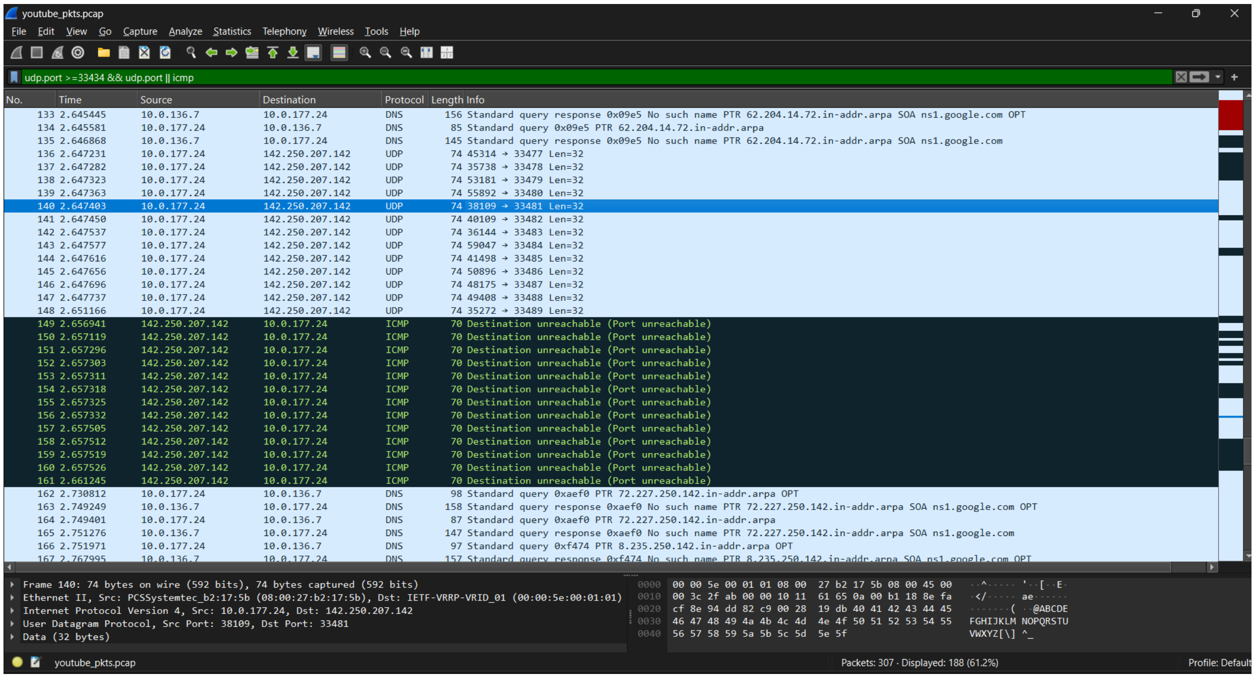
```
No.  Time          Source         Destination    Protocol Length Info
 517 39.470980804  10.0.177.24    10.0.136.7     DNS       84 Standard query 0xa767 A www.apple.com OPT
 518 39.471235585  10.0.177.24    10.0.136.7     DNS       84 Standard query 0x9d40 AAAA www.apple.com OPT
 519 39.472835509  10.0.136.7     10.0.177.24    DNS      214 Standard query response 0xa767 A www.apple.com CNAME www-appl…
 521 39.487061340  10.0.136.7     10.0.177.24    DNS      254 Standard query response 0x9d40 AAAA www.apple.com CNAME www-a…
 522 39.487991346  10.0.177.24    49.44.105.30   UDP       74 59964 → 33434 Len=32
 523 39.488077111  10.0.177.24    49.44.105.30   UDP       74 37282 → 33435 Len=32
 524 39.488143600  10.0.177.24    49.44.105.30   UDP       74 37565 → 33436 Len=32
 525 39.488213721  10.0.177.24    49.44.105.30   UDP       74 43498 → 33437 Len=32
 526 39.488286635  10.0.177.24    49.44.105.30   UDP       74 35529 → 33438 Len=32
 527 39.488359549  10.0.177.24    49.44.105.30   UDP       74 39777 → 33439 Len=32
 528 39.488425480  10.0.177.24    49.44.105.30   UDP       74 54928 → 33440 Len=32
 529 39.488490851  10.0.177.24    49.44.105.30   UDP       74 32881 → 33441 Len=32
 530 39.488556222  10.0.177.24    49.44.105.30   UDP       74 55171 → 33442 Len=32
 531 39.488621873  10.0.177.24    49.44.105.30   UDP       74 50796 → 33443 Len=32
 532 39.488680261  10.0.177.2     10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 533 39.488689200  10.0.177.24    49.44.105.30   UDP       74 43882 → 33444 Len=32
 534 39.488755968  10.0.177.24    49.44.105.30   UDP       74 60164 → 33445 Len=32
 535 39.488832515  10.0.177.24    49.44.105.30   UDP       74 40485 → 33446 Len=32
 536 39.488914648  10.0.177.24    49.44.105.30   UDP       74 57968 → 33447 Len=32
 537 39.488985327  10.0.177.24    49.44.105.30   UDP       74 37353 → 33448 Len=32
 538 39.488943981  10.0.177.2     10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 539 39.488960743  10.0.177.2     10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 540 39.488975829  10.3.0.37      10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 541 39.488988400  10.3.0.37      10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 542 39.489000972  172.16.4.7     10.0.177.24    ICMP     102 Time-to-live exceeded (Time to l
 543 39.489052375  10.0.177.24    49.44.105.30   UDP       74 40754 → 33449 Len=32
 544 39.489245137  10.3.0.37      10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 545 39.489257708  172.16.4.7     10.0.177.24    ICMP     102 Time-to-live exceeded (Time to l
 546 39.489270559  172.16.4.7     10.0.177.24    ICMP     102 Time-to-live exceeded (Time to l
 547 39.489420578  10.0.177.24    10.0.136.7     DNS       94 Standard query 0x4701 PTR 2.177.
 548 39.489559702  10.3.0.5       10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 549 39.489572273  10.3.0.5       10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 550 39.490308400  10.3.0.5       10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 551 39.490319296  10.117.81.253  10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 552 39.491131969  10.0.136.7     10.0.177.24    DNS       94 Standard query response 0x4701 N
 553 39.491378089  10.0.177.24    10.0.136.7     DNS       83 Standard query 0x4701 PTR 2.177.
 554 39.492052477  14.139.98.1    10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 555 39.492061137  14.139.98.1    10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 556 39.492069797  14.139.98.1    10.0.177.24    ICMP      70 Time-to-live exceeded (Time to l
 557 39.492567626  10.0.136.7     10.0.177.24    DNS       83 Standard query response 0x4701 N
 558 39.493171893  10.0.177.24    10.0.136.7     DNS       93 Standard query 0x764e PTR 37.0.3
 559 39.494417023  10.0.136.7     10.0.177.24    DNS       93 Standard query response 0x764e N
 560 39.494582128  10.0.177.24    10.0.136.7     DNS       82 Standard query 0x764e PTR 37.0.3
 561 39.496427893  10.0.136.7     10.0.177.24    DNS       82 Standard query response 0x764e N
 562 39.497076300  10.0.177.24    49.44.105.30   UDP       74 50112 → 33450 Len=32
```

```
Frame 517: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface enp0s3, id 0
```

```
0000  00 00 5e 00 01 01 08 00  27 b2 17 5b 08 00 45 00   ··^·····'··[··E·
0010  00 46 b9 78 40 00 40 11  34 0f 0a 00 b1 18 0a 00   ·F·x@·@·4·······
0020  88 07 84 32 00 35 00 32  4d 63 a7 67 01 00 00 01   ···2·5·2Mc·g····
0030  00 00 00 00 00 01 03 77  77 77 05 61 70 70 6c 65   ·······www·apple
0040  03 63 6f 6d 00 00 01 00  01 00 00 29 02 00 00 00   ·com·······)····
0050  00 00 00 00                                        ····
```

```
student@student-VirtualBox:~$ traceroute www.apple.com
traceroute to www.apple.com (49.44.105.30), 30 hops max, 60 byte packets
 1  10.0.177.2 (10.0.177.2)  0.706 ms  0.882 ms  0.832 ms
 2  10.3.0.37 (10.3.0.37)  0.777 ms  0.716 ms  0.900 ms
 3  10.3.0.5 (10.3.0.5)  1.149 ms  1.096 ms  1.766 ms
 4  172.16.4.7 (172.16.4.7)  0.394 ms  0.584 ms  0.530 ms
 5  14.139.98.1 (14.139.98.1)  3.234 ms  3.176 ms  3.099 ms
 6  10.117.81.253 (10.117.81.253)  1.281 ms  2.497 ms  2.448 ms
 7  * * *
 8  * * *
 9  10.255.221.33 (10.255.221.33)  23.455 ms  23.444 ms 10.255.222.33 (10.255.2
22.33)  23.429 ms
10  115.247.100.29 (115.247.100.29)  28.657 ms  28.622 ms  28.605 ms
11  * * *
12  * * *
13  49.44.131.1 (49.44.131.1)  33.360 ms  34.519 ms  33.026 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
```

enp0s3: <live capture in progress>   Packets: 958 · Displayed: 157 (16.4%)   Profile: Default



```
udp.port >=33434 && udp.port || icmp
```

```
No.   Time        Source           Destination      Protocol Length Info
  133 2.645445    10.0.136.7       10.0.177.24      DNS       156 Standard query response 0x09e5 No such name PTR 62.204.14.72.in-addr.arpa SOA ns1.google.com OPT
  134 2.645581    10.0.177.24      10.0.136.7       DNS        85 Standard query 0x09e5 PTR 62.204.14.72.in-addr.arpa
  135 2.646868    10.0.136.7       10.0.177.24      DNS       145 Standard query response 0x09e5 No such name PTR 62.204.14.72.in-addr.arpa SOA ns1.google.com
  136 2.647231    10.0.177.24      142.250.207.142  UDP        74 45314 → 33477 Len=32
  137 2.647282    10.0.177.24      142.250.207.142  UDP        74 35738 → 33478 Len=32
  138 2.647323    10.0.177.24      142.250.207.142  UDP        74 53181 → 33479 Len=32
  139 2.647363    10.0.177.24      142.250.207.142  UDP        74 55892 → 33480 Len=32
  140 2.647403    10.0.177.24      142.250.207.142  UDP        74 38109 → 33481 Len=32
  141 2.647450    10.0.177.24      142.250.207.142  UDP        74 40109 → 33482 Len=32
  142 2.647537    10.0.177.24      142.250.207.142  UDP        74 36144 → 33483 Len=32
  143 2.647577    10.0.177.24      142.250.207.142  UDP        74 59047 → 33484 Len=32
  144 2.647616    10.0.177.24      142.250.207.142  UDP        74 41498 → 33485 Len=32
  145 2.647656    10.0.177.24      142.250.207.142  UDP        74 50896 → 33486 Len=32
  146 2.647696    10.0.177.24      142.250.207.142  UDP        74 48175 → 33487 Len=32
  147 2.647737    10.0.177.24      142.250.207.142  UDP        74 49408 → 33488 Len=32
  148 2.651166    10.0.177.24      142.250.207.142  UDP        74 35272 → 33489 Len=32
  149 2.656941    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  150 2.657119    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  151 2.657296    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  152 2.657303    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  153 2.657311    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  154 2.657318    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  155 2.657325    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  156 2.657332    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  157 2.657505    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  158 2.657512    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  159 2.657519    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  160 2.657526    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  161 2.661245    142.250.207.142  10.0.177.24      ICMP       70 Destination unreachable (Port unreachable)
  162 2.730812    10.0.177.24      10.0.136.7       DNS        98 Standard query 0xaef0 PTR 72.227.250.142.in-addr.arpa OPT
  163 2.749249    10.0.136.7       10.0.177.24      DNS       158 Standard query response 0xaef0 No such name PTR 72.227.250.142.in-addr.arpa SOA ns1.google.com OPT
  164 2.749401    10.0.177.24      10.0.136.7       DNS        87 Standard query 0xaef0 PTR 72.227.250.142.in-addr.arpa
  165 2.751276    10.0.136.7       10.0.177.24      DNS       147 Standard query response 0xaef0 No such name PTR 72.227.250.142.in-addr.arpa SOA ns1.google.com
  166 2.751971    10.0.177.24      10.0.136.7       DNS        97 Standard query 0xf474 PTR 8.235.250.142.in-addr.arpa OPT
  167 2.767995    10.0.136.7       10.0.177.24      DNS       157 Standard query response 0xf474 No such name PTR 8.235.250.142.in-addr.arpa SOA ns1.google.com OPT
```

```
Frame 140: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PCSSystemtec_b2:17:5b (08:00:27:b2:17:5b), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.0.177.24, Dst: 142.250.207.142
User Datagram Protocol, Src Port: 38109, Dst Port: 33481
Data (32 bytes)
```

```
0000  00 00 5e 00 01 01 08 00  27 b2 17 5b 08 00 45 00   ··^·····'··[··E·
0010  00 3c 2f ab 00 00 10 11  61 65 0a 00 b1 18 8e fa   ·</·····ae······
0020  cf 8e 94 dd 82 c9 00 28  19 db 40 41 42 43 44 45   ·······(··@ABCDE
0030  46 47 48 49 4a 4b 4c 4d  4e 4f 50 51 52 53 54 55   FGHIJKLM NOPQRSTU
0040  56 57 58 59 5a 5b 5c 5d  5e 5f                     VWXYZ[\] ^_
```

youtube_pkts.pcap   Packets: 307 · Displayed: 188 (61.2%)   Profile: Default

Here, for the Linux OS, we can see that Destination Unreachable (Port Unreachable)