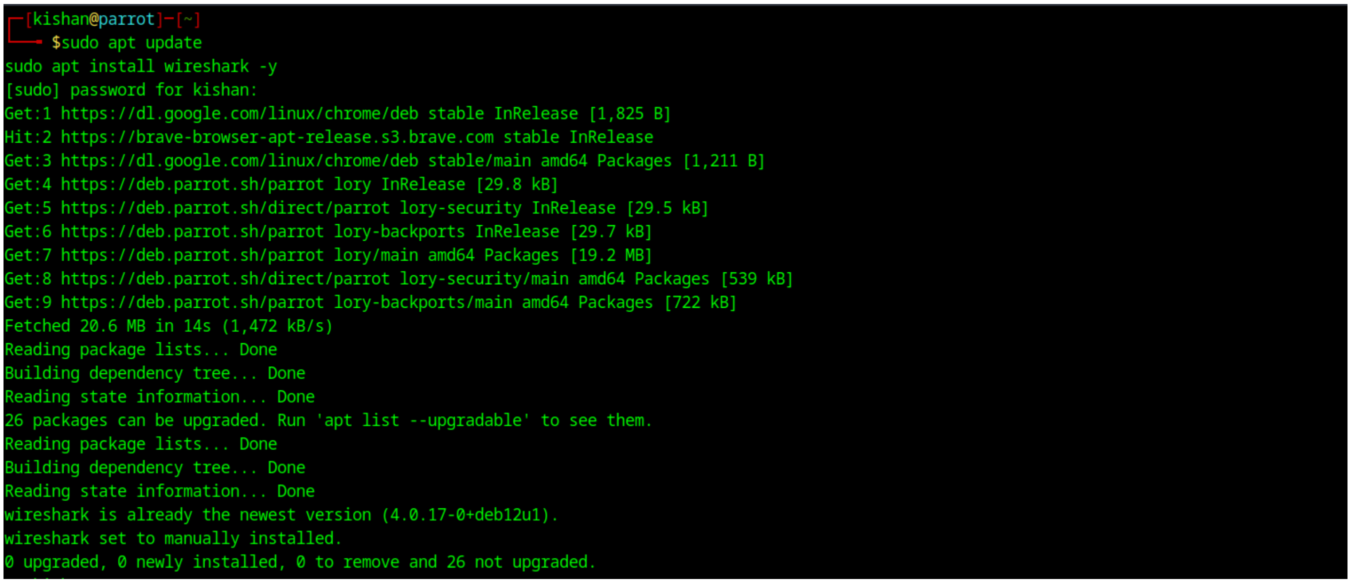
Task 5: Capture and Analyze Network Traffic Using Wireshark

Task Objective : To capture live network packets on a Linux system using Wireshark and analyze the traffic to identify common protocols like HTTP, DNS, TCP, and ICMP.

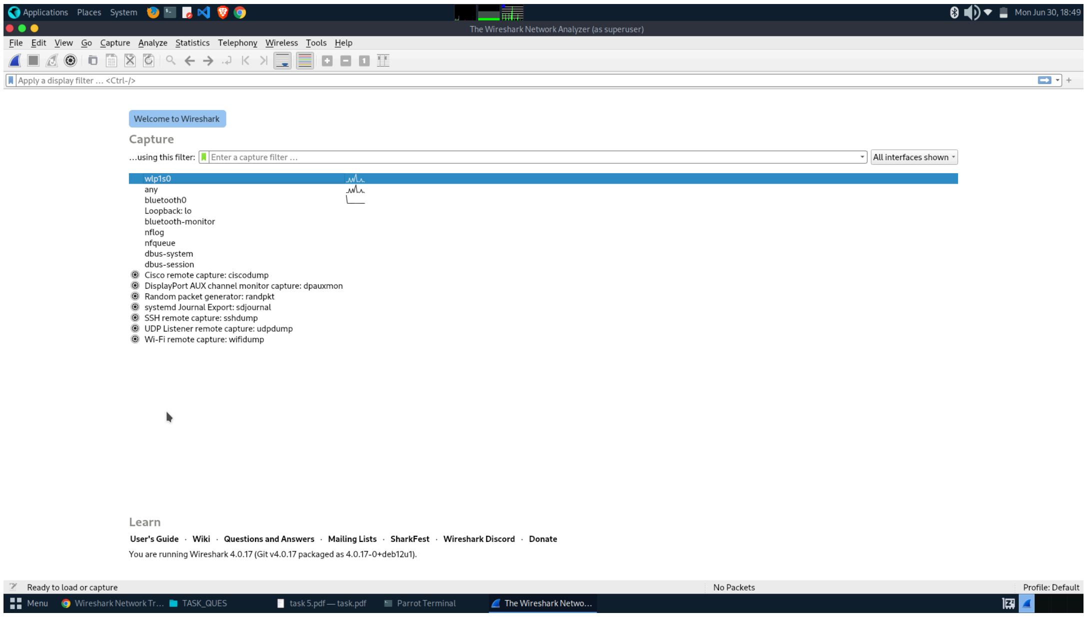
1. Install Wireshark.



```
┌─[kishan@parrot]─[~]
└──╼ $sudo apt update
sudo apt install wireshark -y
[sudo] password for kishan:
Get:1 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Hit:2 https://brave-browser-apt-release.s3.brave.com stable InRelease
Get:3 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,211 B]
Get:4 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]
Get:5 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.5 kB]
Get:6 https://deb.parrot.sh/parrot lory-backports InRelease [29.7 kB]
Get:7 https://deb.parrot.sh/parrot lory/main amd64 Packages [19.2 MB]
Get:8 https://deb.parrot.sh/direct/parrot lory-security/main amd64 Packages [539 kB]
Get:9 https://deb.parrot.sh/parrot lory-backports/main amd64 Packages [722 kB]
Fetched 20.6 MB in 14s (1,472 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
26 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (4.0.17-0+deb12u1).
wireshark set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
```

2. Start capturing on your active network interface.

The GUI of wireshark will be like this. Now I will select wlp1s0. This is a wireless (Wi-Fi) interface connected on PCI bus 1, slot 0.



Capture

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

```
wlp1s0
any
bluetooth0
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
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
Wi-Fi remote capture: wifidump
```

You are running Wireshark 4.0.17 (Git v4.0.17 packaged as 4.0.17-0+deb12u1).

Ready to load or capture   No Packets   Profile: Default

3. Browse a website or ping a server to generate traffic.

After starting the capture, a new terminal window was opened and the following command was run to ping Google, which generates ICMP packets.

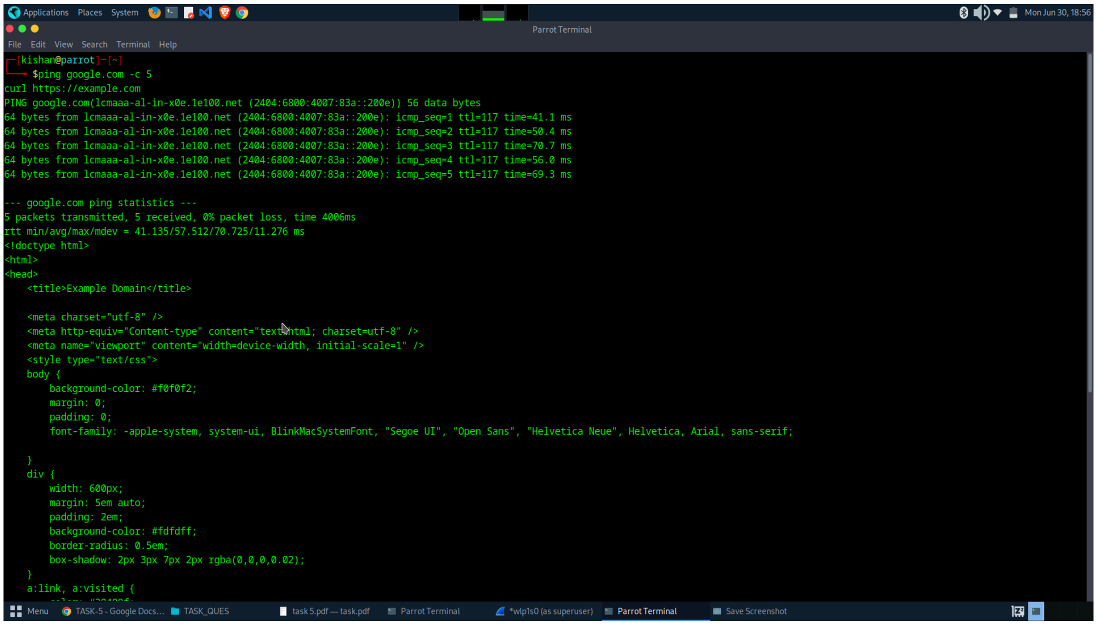
```
ping google.com -c 5
```

Then, to generate HTTP, HTTPS, and DNS traffic, a website was accessed using

```
curl https://example.com
```

This simulates real-world browsing activity and helps capture various protocol packets like DNS (for name resolution), TCP (for reliable transport), and HTTP/HTTPS (for web content).

This is the interface where i have pressed the commands


Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
Menu TASK-5 - Google Docs... TASK_QUES task 5.pdf — task.pdf Parrot Terminal *wlp1s0 (as superuser) Parrot Terminal Save Screenshot
Mon Jun 30, 18:56

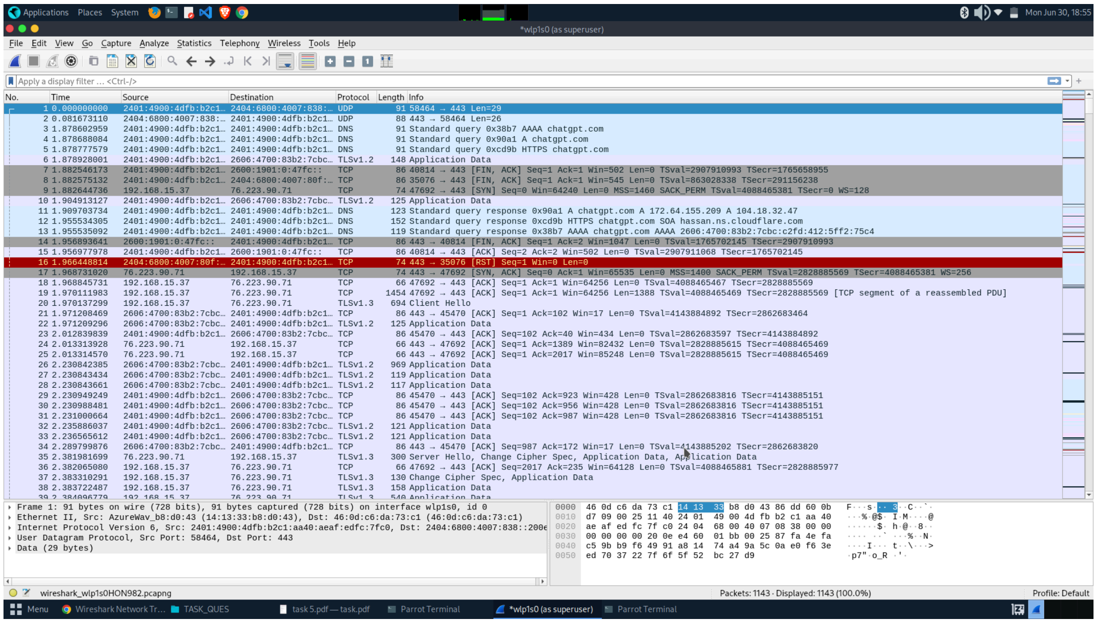
```
┌─[kishan@parrot]─[~]
└──╼ $ping google.com -c 5
curl https://example.com
PING google.com(lcmaaa-al-in-x0e.1e100.net (2404:6800:4007:83a::200e)) 56 data bytes
64 bytes from lcmaaa-al-in-x0e.1e100.net (2404:6800:4007:83a::200e): icmp_seq=1 ttl=117 time=41.1 ms
64 bytes from lcmaaa-al-in-x0e.1e100.net (2404:6800:4007:83a::200e): icmp_seq=2 ttl=117 time=50.4 ms
64 bytes from lcmaaa-al-in-x0e.1e100.net (2404:6800:4007:83a::200e): icmp_seq=3 ttl=117 time=70.7 ms
64 bytes from lcmaaa-al-in-x0e.1e100.net (2404:6800:4007:83a::200e): icmp_seq=4 ttl=117 time=56.0 ms
64 bytes from lcmaaa-al-in-x0e.1e100.net (2404:6800:4007:83a::200e): icmp_seq=5 ttl=117 time=69.3 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 41.135/57.512/70.725/11.276 ms
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
```

This is the traffic captured


Applications Places System
*wlp1s0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Menu Wireshark Network Tr... TASK_QUES task 5.pdf — task.pdf Parrot Terminal *wlp1s0 (as superuser) Parrot Terminal
Mon Jun 30, 18:55

```
No.  Time         Source              Destination         Protocol Length Info
   1 0.000000000  2401:4900:4dfb:b2c1… 2404:6800:4007:838:… UDP        91 58464 → 443 Len=29
   2 0.081673110  2404:6800:4007:838:… 2401:4900:4dfb:b2c1… UDP        88 443 → 58464 Len=26
   3 1.878602959  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS        91 Standard query 0x38b7 AAAA chatgpt.com
   4 1.878688084  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS        91 Standard query 0x90a1 A chatgpt.com
   5 1.878777579  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS        91 Standard query 0xcd9b HTTPS chatgpt.com
   6 1.878928001  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2   148 Application Data
   7 1.882546173  2401:4900:4dfb:b2c1… 2600:1901:0:47fc::   TCP        86 40814 → 443 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=2907910993 TSecr=1765658955
   8 1.882575132  2401:4900:4dfb:b2c1… 2404:6800:4007:80f:… TCP        86 35076 → 443 [FIN, ACK] Seq=1 Ack=1 Win=545 Len=0 TSval=863028338 TSecr=291156238
   9 1.882644736  192.168.15.37       76.223.90.71        TCP        74 47692 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4088465381 TSecr=0 WS=128
  10 1.904913127  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2   125 Application Data
  11 1.909703734  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS       123 Standard query response 0x90a1 A chatgpt.com A 172.64.155.209 A 104.18.32.47
  12 1.955534305  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS       152 Standard query response 0xcd9b HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
  13 1.955535092  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS       119 Standard query response 0x38b7 AAAA chatgpt.com AAAA 2606:4700:83b2:7cbc:c2fd:412:5ff2:75c4
  14 1.956893641  2600:1901:0:47fc::   2401:4900:4dfb:b2c1… TCP        86 443 → 40814 [FIN, ACK] Seq=1 Ack=2 Win=1047 Len=0 TSval=1765702145 TSecr=2907910993
  15 1.956977978  2401:4900:4dfb:b2c1… 2600:1901:0:47fc::   TCP        86 40814 → 443 [ACK] Seq=2 Ack=2 Win=502 Len=0 TSval=2907911068 TSecr=1765702145
  16 1.966448814  2404:6800:4007:80f:… 2401:4900:4dfb:b2c1… TCP        74 443 → 35076 [RST] Seq=1 Win=0 Len=0
  17 1.968731020  76.223.90.71        192.168.15.37       TCP        74 443 → 47692 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM TSval=2828885569 TSecr=4088465381 WS=256
  18 1.968845731  192.168.15.37       76.223.90.71        TCP        66 47692 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4088465467 TSecr=2828885569
  19 1.970111983  192.168.15.37       76.223.90.71        TCP      1454 47692 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=1388 TSval=4088465469 TSecr=2828885569 [TCP segment of a reassembled PDU]
  20 1.970137299  192.168.15.37       76.223.90.71        TLSv1.3   694 Client Hello
  21 1.971208469  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TCP        86 443 → 45470 [ACK] Seq=1 Ack=102 Win=17 Len=0 TSval=4143884892 TSecr=2862683464
  22 1.971209296  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2   125 Application Data
  23 2.012839839  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP        86 45470 → 443 [ACK] Seq=102 Ack=40 Win=434 Len=0 TSval=2862683597 TSecr=4143884892
  24 2.013313928  76.223.90.71        192.168.15.37       TCP        66 443 → 47692 [ACK] Seq=1 Ack=1389 Win=82432 Len=0 TSval=2828885615 TSecr=4088465469
  25 2.013314570  76.223.90.71        192.168.15.37       TCP        66 443 → 47692 [ACK] Seq=1 Ack=2017 Win=85248 Len=0 TSval=2828885615 TSecr=4088465469
  26 2.230842385  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2   969 Application Data
  27 2.230843434  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2   119 Application Data
  28 2.230843661  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2   117 Application Data
  29 2.230949249  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP        86 45470 → 443 [ACK] Seq=102 Ack=923 Win=428 Len=0 TSval=2862683816 TSecr=4143885151
  30 2.230988481  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP        86 45470 → 443 [ACK] Seq=102 Ack=956 Win=428 Len=0 TSval=2862683816 TSecr=4143885151
  31 2.231000664  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP        86 45470 → 443 [ACK] Seq=102 Ack=987 Win=428 Len=0 TSval=2862683816 TSecr=4143885151
  32 2.235886037  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2   121 Application Data
  33 2.236565612  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2   121 Application Data
  34 2.289799876  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TCP        86 443 → 45470 [ACK] Seq=987 Ack=172 Win=17 Len=0 TSval=4143885202 TSecr=2862683820
  35 2.381981699  76.223.90.71        192.168.15.37       TLSv1.3   300 Server Hello, Change Cipher Spec, Application Data, Application Data
  36 2.382065080  192.168.15.37       76.223.90.71        TCP        66 47692 → 443 [ACK] Seq=2017 Ack=235 Win=64128 Len=0 TSval=4088465881 TSecr=2828885977
  37 2.383310291  192.168.15.37       76.223.90.71        TLSv1.3   130 Change Cipher Spec, Application Data
  38 2.383722487  192.168.15.37       76.223.90.71        TLSv1.3   158 Application Data
  39 2.384096779  192.168.15.37       76.223.90.71        TLSv1.3   540 Application Data
```

```
› Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlp1s0, id 0
› Ethernet II, Src: AzureWav_b8:d0:43 (14:13:33:b8:d0:43), Dst: 46:0d:c6:da:73:c1 (46:0d:c6:da:73:c1)
› Internet Protocol Version 6, Src: 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0, Dst: 2404:6800:4007:838::200e
› User Datagram Protocol, Src Port: 58464, Dst Port: 443
› Data (29 bytes)
```

```
0000  46 0d c6 da 73 c1 14 13  33 b8 d0 43 86 dd 60 0b   F···s···3··C··`·
0010  d7 09 00 25 11 40 24 01  49 00 4d fb b2 c1 aa 40   ···%·@$· I·M···@
0020  ae af ed fc 7f c0 24 04  68 00 40 07 08 38 00 00   ······$· h·@··8··
0030  00 00 00 00 20 0e e4 60  01 bb 00 25 87 fa 4e fa   ···· ··` ···%··N·
0040  c5 9b b9 f6 49 91 a8 14  74 a4 9a 5c 0a e0 f6 3e   ····I··· t··\···>
0050  ed 70 37 22 7f 6f 5f 52  bc 27 d9                  ·p7"·o_R ·'·
```

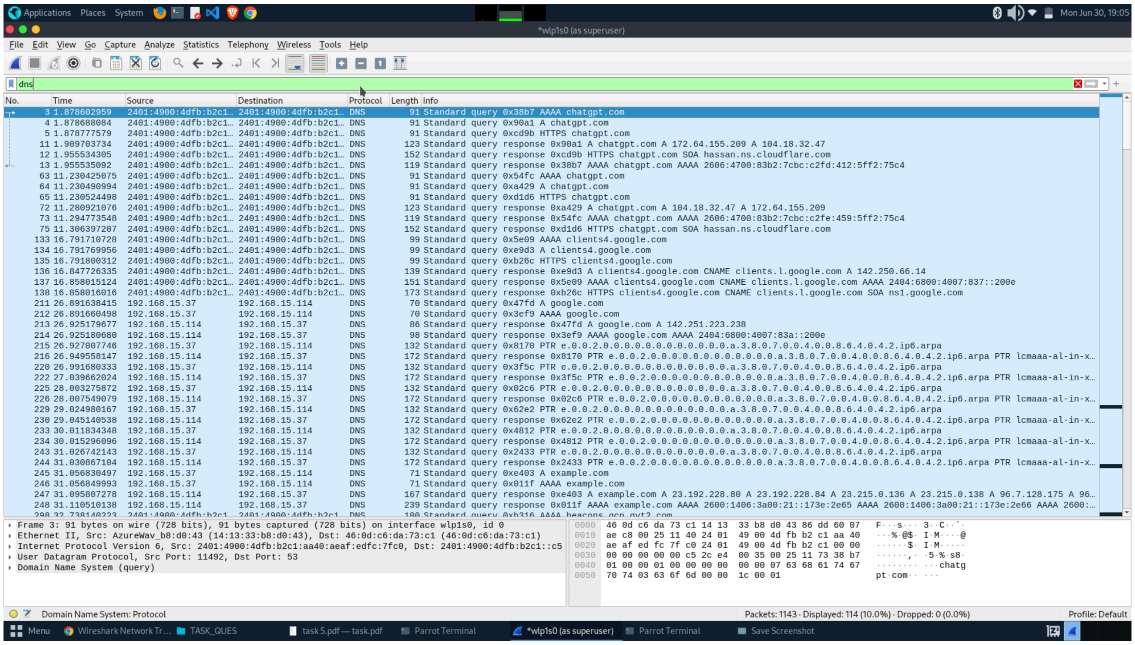
wireshark_wlp1s0HON982.pcapng   Packets: 1143 · Displayed: 1143 (100.0%)   Profile: Default

4. Stop capture after a minute.

I have stopped it after a min

5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

Used the Display Filter bar at the top of Wireshark to isolate specific types of packets.



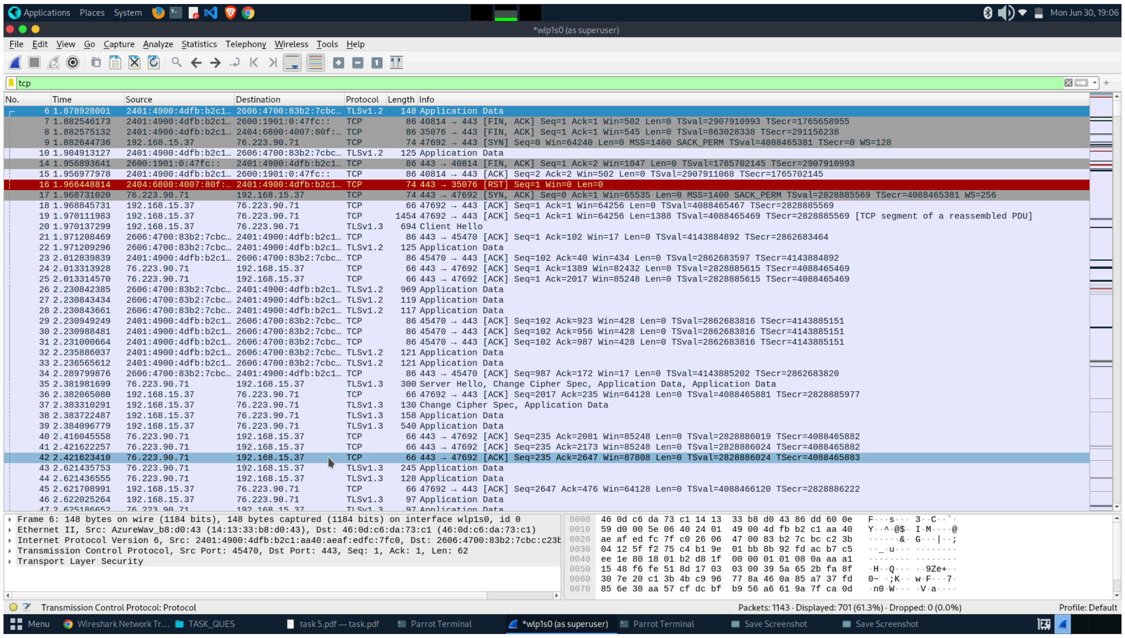
```
dns
No.  Time          Source               Destination          Protocol Length Info
   3 1.878602959   2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      91 Standard query 0x38b7 AAAA chatgpt.com
   4 1.878688084   2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      91 Standard query 0x90a1 A chatgpt.com
   5 1.878777579   2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      91 Standard query 0xcd9b HTTPS chatgpt.com
  11 1.909703734   2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     123 Standard query response 0x90a1 A chatgpt.com A 172.64.155.209 A 104.18.32.47
  12 1.955534305   2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     152 Standard query response 0xcd9b HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
  13 1.955535092   2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     119 Standard query response 0x38b7 AAAA chatgpt.com AAAA 2606:4700:83b2:7cbc:c2fd:412:5ff2:75c4
  63 11.230425075  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      91 Standard query 0x54fc AAAA chatgpt.com
  64 11.230490994  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      91 Standard query 0xa429 A chatgpt.com
  65 11.230524498  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      91 Standard query 0xd1d6 HTTPS chatgpt.com
  72 11.280921076  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     123 Standard query response 0xa429 A chatgpt.com A 104.18.32.47 A 172.64.155.209
  73 11.294773548  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     119 Standard query response 0x54fc AAAA chatgpt.com AAAA 2606:4700:83b2:7cbc:c2fe:459:5ff2:75c4
  75 11.306397207  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     152 Standard query response 0xd1d6 HTTPS chatgpt.com SOA hassan.ns.cloudflare.com
 133 16.791710728  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      99 Standard query 0x5e09 AAAA clients4.google.com
 134 16.791769956  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      99 Standard query 0xe9d3 A clients4.google.com
 135 16.791800312  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS      99 Standard query 0xb26c HTTPS clients4.google.com
 136 16.847726335  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     139 Standard query response 0xe9d3 A clients4.google.com CNAME clients.l.google.com A 142.250.66.14
 137 16.858015124  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     151 Standard query response 0x5e09 AAAA clients4.google.com CNAME clients.l.google.com AAAA 2404:6800:4007:837::200e
 138 16.858016016  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     173 Standard query response 0xb26c HTTPS clients4.google.com CNAME clients.l.google.com SOA ns1.google.com
 211 26.891638415  192.168.15.37        192.168.15.114       DNS      70 Standard query 0x47fd A google.com
 212 26.891660498  192.168.15.37        192.168.15.114       DNS      70 Standard query 0x3ef9 AAAA google.com
 213 26.925179677  192.168.15.114       192.168.15.37        DNS      86 Standard query response 0x47fd A google.com A 142.251.223.238
 214 26.925180680  192.168.15.114       192.168.15.37        DNS      98 Standard query response 0x3ef9 AAAA google.com AAAA 2404:6800:4007:83a::200e
 215 26.927007746  192.168.15.37        192.168.15.114       DNS     132 Standard query 0x8170 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa
 216 26.949558147  192.168.15.114       192.168.15.37        DNS     172 Standard query response 0x8170 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa PTR lcmaaa-al-in-x…
 220 26.991680333  192.168.15.37        192.168.15.114       DNS     132 Standard query 0x3f5c PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa
 222 27.039662024  192.168.15.114       192.168.15.37        DNS     172 Standard query response 0x3f5c PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa PTR lcmaaa-al-in-x…
 225 28.003275872  192.168.15.37        192.168.15.114       DNS     132 Standard query 0x02c6 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa
 226 28.007549079  192.168.15.114       192.168.15.37        DNS     172 Standard query response 0x02c6 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa PTR lcmaaa-al-in-x…
 229 29.024980167  192.168.15.37        192.168.15.114       DNS     132 Standard query 0x62e2 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa
 230 29.045140538  192.168.15.114       192.168.15.37        DNS     172 Standard query response 0x62e2 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa PTR lcmaaa-al-in-x…
 233 30.011834348  192.168.15.37        192.168.15.114       DNS     132 Standard query 0x4812 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa
 234 30.015296096  192.168.15.114       192.168.15.37        DNS     172 Standard query response 0x4812 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa PTR lcmaaa-al-in-x…
 243 31.026742143  192.168.15.37        192.168.15.114       DNS     132 Standard query 0x2433 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa
 244 31.030867104  192.168.15.114       192.168.15.37        DNS     172 Standard query response 0x2433 PTR e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.a.3.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa PTR lcmaaa-al-in-x…
 245 31.056830497  192.168.15.37        192.168.15.114       DNS      71 Standard query 0xe403 A example.com
 246 31.056849993  192.168.15.37        192.168.15.114       DNS      71 Standard query 0x011f AAAA example.com
 247 31.095807278  192.168.15.114       192.168.15.37        DNS     167 Standard query response 0xe403 A example.com A 23.192.228.80 A 23.192.228.84 A 23.215.0.136 A 23.215.0.138 A 96.7.128.175 A 96…
 248 31.110510138  192.168.15.114       192.168.15.37        DNS     239 Standard query response 0x011f AAAA example.com AAAA 2600:1406:3a00:21::173e:2e65 AAAA 2600:1406:3a00:21::173e:2e66 AAAA 2600:…
 298 32.738140223  2401:4900:4dfb:b2c1… 2401:4900:4dfb:b2c1… DNS     100 Standard query 0xb316 AAAA beacons.gcp.gvt2.com

› Frame 3: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface wlp1s0, id 0
› Ethernet II, Src: AzureWav_b8:d0:43 (14:13:33:b8:d0:43), Dst: 46:0d:c6:da:73:c1 (46:0d:c6:da:73:c1)
› Internet Protocol Version 6, Src: 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0, Dst: 2401:4900:4dfb:b2c1::c5
› User Datagram Protocol, Src Port: 11492, Dst Port: 53
› Domain Name System (query)

0000  46 0d c6 da 73 c1 14 13  33 b8 d0 43 86 dd 60 07   F···s··· 3··C··`·
0010  ae c8 00 25 11 40 24 01  49 00 4d fb b2 c1 aa 40   ···%·@$· I·M····@
0020  ae af ed fc 7f c0 24 01  49 00 4d fb b2 c1 00 00   ······$· I·M·····
0030  00 00 00 00 00 c5 2c e4  00 35 00 25 11 73 38 b7   ······,· ·5·%·s8·
0040  01 00 00 01 00 00 00 00  00 00 07 63 68 61 74 67   ········ ···chatg
0050  70 74 03 63 6f 6d 00 00  1c 00 01                  pt·com·· ···

Domain Name System: Protocol          Packets: 1143 · Displayed: 114 (10.0%) · Dropped: 0 (0.0%)          Profile: Default
```

dns → filters DNS queries and responses



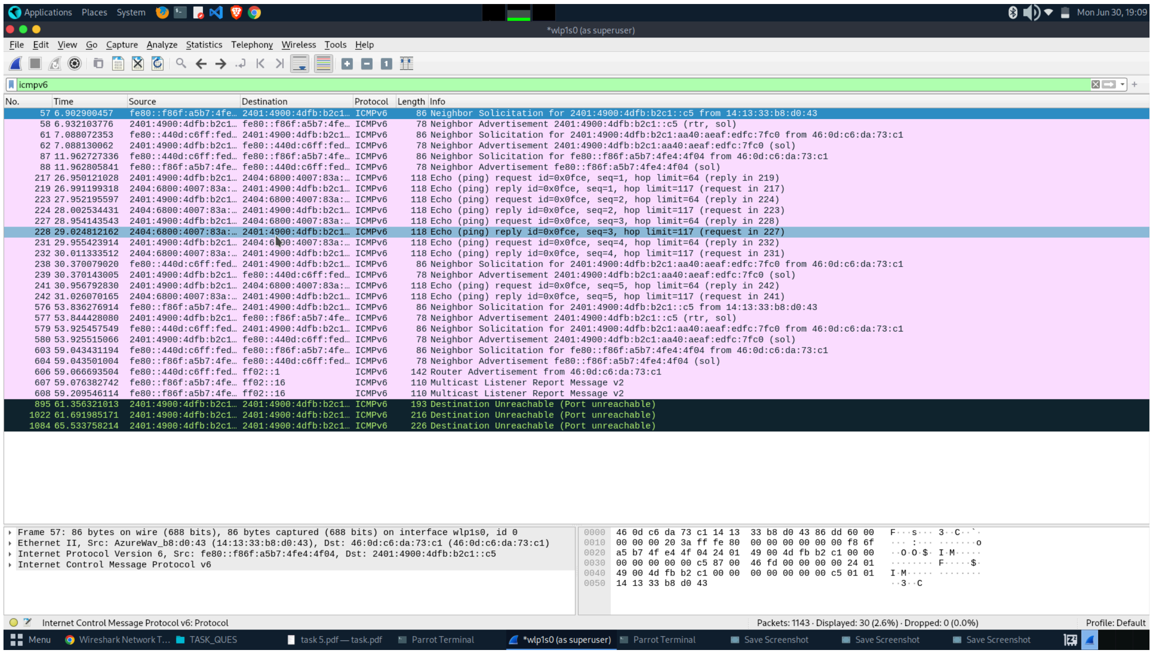
```
tcp
No.  Time         Source               Destination          Protocol Length Info
   6 1.878928001  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2  148 Application Data
   7 1.882546173  2401:4900:4dfb:b2c1… 2600:1901:0:47fc::   TCP       86 40814 → 443 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=2907910993 TSecr=1765658955
   8 1.882575132  2401:4900:4dfb:b2c1… 2404:6800:4007:80f:… TCP       86 35076 → 443 [FIN, ACK] Seq=1 Ack=1 Win=545 Len=0 TSval=863028338 TSecr=291156238
   9 1.882644736  192.168.15.37        76.223.90.71         TCP       74 47692 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4088465381 TSecr=0 WS=128
  10 1.904913127  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2  125 Application Data
  14 1.956893641  2600:1901:0:47fc::   2401:4900:4dfb:b2c1… TCP       86 443 → 40814 [FIN, ACK] Seq=1 Ack=2 Win=1047 Len=0 TSval=1765702145 TSecr=2907910993
  15 1.956977978  2401:4900:4dfb:b2c1… 2600:1901:0:47fc::   TCP       86 40814 → 443 [ACK] Seq=2 Ack=2 Win=502 Len=0 TSval=2907911068 TSecr=1765702145
  16 1.966448814  2404:6800:4007:80f:… 2401:4900:4dfb:b2c1… TCP       74 443 → 35076 [RST] Seq=1 Win=0 Len=0
  17 1.968731020  76.223.90.71         192.168.15.37        TCP       74 443 → 47692 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM TSval=2828885569 TSecr=4088465381 WS=256
  18 1.968845731  192.168.15.37        76.223.90.71         TCP       66 47692 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4088465467 TSecr=2828885569
  19 1.970111983  192.168.15.37        76.223.90.71         TCP     1454 47692 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=1388 TSval=4088465469 TSecr=2828885569 [TCP segment of a reassembled PDU]
  20 1.970137299  192.168.15.37        76.223.90.71         TLSv1.3  694 Client Hello
  21 1.971208469  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TCP       86 443 → 45470 [ACK] Seq=1 Ack=102 Win=17 Len=0 TSval=4143884892 TSecr=2862683464
  22 1.971209296  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2  125 Application Data
  23 2.012839839  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP       86 45470 → 443 [ACK] Seq=102 Ack=40 Win=434 Len=0 TSval=2862683597 TSecr=4143884892
  24 2.013313928  76.223.90.71         192.168.15.37        TCP       66 443 → 47692 [ACK] Seq=1 Ack=1389 Win=82432 Len=0 TSval=2828885615 TSecr=4088465469
  25 2.013314570  76.223.90.71         192.168.15.37        TCP       66 443 → 47692 [ACK] Seq=1 Ack=2017 Win=85248 Len=0 TSval=2828885615 TSecr=4088465469
  26 2.230842385  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2  969 Application Data
  27 2.230843434  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2  119 Application Data
  28 2.230843661  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TLSv1.2  117 Application Data
  29 2.230949249  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP       86 45470 → 443 [ACK] Seq=102 Ack=923 Win=428 Len=0 TSval=2862683816 TSecr=4143885151
  30 2.230988481  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP       86 45470 → 443 [ACK] Seq=102 Ack=956 Win=428 Len=0 TSval=2862683816 TSecr=4143885151
  31 2.231000664  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TCP       86 45470 → 443 [ACK] Seq=102 Ack=987 Win=428 Len=0 TSval=2862683816 TSecr=4143885151
  32 2.235886037  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2  121 Application Data
  33 2.236565612  2401:4900:4dfb:b2c1… 2606:4700:83b2:7cbc… TLSv1.2  121 Application Data
  34 2.289799876  2606:4700:83b2:7cbc… 2401:4900:4dfb:b2c1… TCP       86 443 → 45470 [ACK] Seq=987 Ack=172 Win=17 Len=0 TSval=4143885202 TSecr=2862683820
  35 2.381981699  76.223.90.71         192.168.15.37        TLSv1.3  300 Server Hello, Change Cipher Spec, Application Data, Application Data
  36 2.382065080  192.168.15.37        76.223.90.71         TCP       66 47692 → 443 [ACK] Seq=2017 Ack=235 Win=64128 Len=0 TSval=4088465881 TSecr=2828885977
  37 2.383310291  192.168.15.37        76.223.90.71         TLSv1.3  130 Change Cipher Spec, Application Data
  38 2.383722487  192.168.15.37        76.223.90.71         TLSv1.3  158 Application Data
  39 2.384096779  192.168.15.37        76.223.90.71         TLSv1.3  540 Application Data
  40 2.416045558  76.223.90.71         192.168.15.37        TCP       66 443 → 47692 [ACK] Seq=235 Ack=2081 Win=85248 Len=0 TSval=2828886019 TSecr=4088465882
  41 2.421622257  76.223.90.71         192.168.15.37        TCP       66 443 → 47692 [ACK] Seq=235 Ack=2173 Win=85248 Len=0 TSval=2828886024 TSecr=4088465882
  42 2.421623410  76.223.90.71         192.168.15.37        TCP       66 443 → 47692 [ACK] Seq=235 Ack=2647 Win=87808 Len=0 TSval=2828886024 TSecr=4088465883
  43 2.621435753  76.223.90.71         192.168.15.37        TLSv1.3  245 Application Data
  44 2.621436555  76.223.90.71         192.168.15.37        TLSv1.3  128 Application Data
  45 2.621708991  192.168.15.37        76.223.90.71         TCP       66 47692 → 443 [ACK] Seq=2647 Ack=476 Win=64128 Len=0 TSval=4088466120 TSecr=2828886222
  46 2.622025264  192.168.15.37        76.223.90.71         TLSv1.3   97 Application Data
  47 2.625186652  76.223.90.71         192.168.15.37        TLSv1.3   97 Application Data

› Frame 6: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface wlp1s0, id 0
› Ethernet II, Src: AzureWav_b8:d0:43 (14:13:33:b8:d0:43), Dst: 46:0d:c6:da:73:c1 (46:0d:c6:da:73:c1)
› Internet Protocol Version 6, Src: 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0, Dst: 2606:4700:83b2:7cbc:c23b
› Transmission Control Protocol, Src Port: 45470, Dst Port: 443, Seq: 1, Ack: 1, Len: 62
› Transport Layer Security

0000  46 0d c6 da 73 c1 14 13  33 b8 d0 43 86 dd 60 0e   F···s··· 3··C··`·
0010  59 d0 00 5e 06 40 24 01  49 00 4d fb b2 c1 aa 40   Y··^·@$· I·M····@
0020  ae af ed fc 7f c0 26 06  47 00 83 b2 7c bc c2 3b   ······&· G···|··;
0030  04 12 5f f2 75 c4 b1 9e  01 bb 8b 92 fd ac b7 c5   ··_·u··· ········
0040  ee 1e 80 18 01 b2 d8 1f  00 00 01 01 08 0a aa a1   ········ ········
0050  15 48 f6 fe 51 8d 17 03  03 00 39 5a 65 2b fa 8f   ·H··Q··· ··9Ze+··
0060  30 7e 20 c1 3b 4b c9 96  77 8a 46 0a 85 a7 37 fd   0~ ·;K·· w·F···7·
0070  85 6e 30 aa 57 cf dc bf  b9 56 a6 61 9a 7f ca 0d   ·n0·W··· ·V·a····

Transmission Control Protocol: Protocol          Packets: 1143 · Displayed: 701 (61.3%) · Dropped: 0 (0.0%)          Profile: Default
```

tcp → shows only TCP traffic



Applications Places System
*wlp1s0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpv6

```
No.    Time          Source                Destination           Protocol Length Info
    57 6.902900457   fe80::f86f:a5b7:4fe…  2401:4900:4dfb:b2c1…  ICMPv6     86 Neighbor Solicitation for 2401:4900:4dfb:b2c1::c5 from 14:13:33:b8:d0:43
    58 6.932103776   2401:4900:4dfb:b2c1…  fe80::f86f:a5b7:4fe…  ICMPv6     78 Neighbor Advertisement 2401:4900:4dfb:b2c1::c5 (rtr, sol)
    61 7.088072353   fe80::440d:c6ff:fed…  2401:4900:4dfb:b2c1…  ICMPv6     86 Neighbor Solicitation for 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0 from 46:0d:c6:da:73:c1
    62 7.088130062   2401:4900:4dfb:b2c1…  fe80::440d:c6ff:fed…  ICMPv6     78 Neighbor Advertisement 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0 (sol)
    87 11.962727336  fe80::440d:c6ff:fed…  fe80::f86f:a5b7:4fe…  ICMPv6     86 Neighbor Solicitation for fe80::f86f:a5b7:4fe4:4f04 from 46:0d:c6:da:73:c1
    88 11.962805841  fe80::f86f:a5b7:4fe…  fe80::440d:c6ff:fed…  ICMPv6     78 Neighbor Advertisement fe80::f86f:a5b7:4fe4:4f04 (sol)
   217 26.950121028  2401:4900:4dfb:b2c1…  2404:6800:4007:83a:…  ICMPv6    118 Echo (ping) request id=0x0fce, seq=1, hop limit=64 (reply in 219)
   219 26.991199318  2404:6800:4007:83a:…  2401:4900:4dfb:b2c1…  ICMPv6    118 Echo (ping) reply id=0x0fce, seq=1, hop limit=117 (request in 217)
   223 27.952195597  2401:4900:4dfb:b2c1…  2404:6800:4007:83a:…  ICMPv6    118 Echo (ping) request id=0x0fce, seq=2, hop limit=64 (reply in 224)
   224 28.002534431  2404:6800:4007:83a:…  2401:4900:4dfb:b2c1…  ICMPv6    118 Echo (ping) reply id=0x0fce, seq=2, hop limit=117 (request in 223)
   227 28.954143543  2401:4900:4dfb:b2c1…  2404:6800:4007:83a:…  ICMPv6    118 Echo (ping) request id=0x0fce, seq=3, hop limit=64 (reply in 228)
   228 29.024812162  2404:6800:4007:83a:…  2401:4900:4dfb:b2c1…  ICMPv6    118 Echo (ping) reply id=0x0fce, seq=3, hop limit=117 (request in 227)
   231 29.955423914  2401:4900:4dfb:b2c1…  2404:6800:4007:83a:…  ICMPv6    118 Echo (ping) request id=0x0fce, seq=4, hop limit=64 (reply in 232)
   232 30.011333512  2404:6800:4007:83a:…  2401:4900:4dfb:b2c1…  ICMPv6    118 Echo (ping) reply id=0x0fce, seq=4, hop limit=117 (request in 231)
   238 30.370079020  fe80::440d:c6ff:fed…  2401:4900:4dfb:b2c1…  ICMPv6     86 Neighbor Solicitation for 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0 from 46:0d:c6:da:73:c1
   239 30.370143005  2401:4900:4dfb:b2c1…  fe80::440d:c6ff:fed…  ICMPv6     78 Neighbor Advertisement 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0 (sol)
   241 30.956792830  2401:4900:4dfb:b2c1…  2404:6800:4007:83a:…  ICMPv6    118 Echo (ping) request id=0x0fce, seq=5, hop limit=64 (reply in 242)
   242 31.026070165  2404:6800:4007:83a:…  2401:4900:4dfb:b2c1…  ICMPv6    118 Echo (ping) reply id=0x0fce, seq=5, hop limit=117 (request in 241)
   576 53.836276914  fe80::f86f:a5b7:4fe…  2401:4900:4dfb:b2c1…  ICMPv6     86 Neighbor Solicitation for 2401:4900:4dfb:b2c1::c5 from 14:13:33:b8:d0:43
   577 53.844428080  2401:4900:4dfb:b2c1…  fe80::f86f:a5b7:4fe…  ICMPv6     78 Neighbor Advertisement 2401:4900:4dfb:b2c1::c5 (rtr, sol)
   579 53.925457549  fe80::440d:c6ff:fed…  2401:4900:4dfb:b2c1…  ICMPv6     86 Neighbor Solicitation for 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0 from 46:0d:c6:da:73:c1
   580 53.925515066  2401:4900:4dfb:b2c1…  fe80::440d:c6ff:fed…  ICMPv6     78 Neighbor Advertisement 2401:4900:4dfb:b2c1:aa40:aeaf:edfc:7fc0 (sol)
   603 59.043431194  fe80::440d:c6ff:fed…  fe80::f86f:a5b7:4fe…  ICMPv6     86 Neighbor Solicitation for fe80::f86f:a5b7:4fe4:4f04 from 46:0d:c6:da:73:c1
   604 59.043501004  fe80::f86f:a5b7:4fe…  fe80::440d:c6ff:fed…  ICMPv6     78 Neighbor Advertisement fe80::f86f:a5b7:4fe4:4f04 (sol)
   606 59.066693504  fe80::440d:c6ff:fed…  ff02::1               ICMPv6    142 Router Advertisement from 46:0d:c6:da:73:c1
   607 59.076382742  fe80::f86f:a5b7:4fe…  ff02::16              ICMPv6    110 Multicast Listener Report Message v2
   608 59.209546114  fe80::f86f:a5b7:4fe…  ff02::16              ICMPv6    110 Multicast Listener Report Message v2
   895 61.356321013  2401:4900:4dfb:b2c1…  2401:4900:4dfb:b2c1…  ICMPv6    193 Destination Unreachable (Port unreachable)
  1022 61.691985171  2401:4900:4dfb:b2c1…  2401:4900:4dfb:b2c1…  ICMPv6    216 Destination Unreachable (Port unreachable)
  1084 65.533758214  2401:4900:4dfb:b2c1…  2401:4900:4dfb:b2c1…  ICMPv6    226 Destination Unreachable (Port unreachable)
```

```
› Frame 57: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlp1s0, id 0
› Ethernet II, Src: AzureWav_b8:d0:43 (14:13:33:b8:d0:43), Dst: 46:0d:c6:da:73:c1 (46:0d:c6:da:73:c1)
› Internet Protocol Version 6, Src: fe80::f86f:a5b7:4fe4:4f04, Dst: 2401:4900:4dfb:b2c1::c5
› Internet Control Message Protocol v6
```

```
0000  46 0d c6 da 73 c1 14 13  33 b8 d0 43 86 dd 60 00   F···s··· 3··C··`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 f8 6f   ··· :··· ·······o
0020  a5 b7 4f e4 4f 04 24 01  49 00 4d fb b2 c1 00 00   ··O·O·$· I·M·····
0030  00 00 00 00 00 c5 87 00  46 fd 00 00 00 00 24 01   ········ F·····$·
0040  49 00 4d fb b2 c1 00 00  00 00 00 00 00 c5 01 01   I·M····· ········
0050  14 13 33 b8 d0 43                                  ··3··C
```

Internet Control Message Protocol v6: Protocol   Packets: 1143 · Displayed: 30 (2.6%) · Dropped: 0 (0.0%)   Profile: Default

icmp → shows ping request/reply

No Http traffic was captured

6. Identify at least 3 different protocols in the capture.

I have ICMP , TCP and DNS packets that were captured on my wire shark i will say what are those and what will they do shortly

1. ICMP (Internet Control Message Protocol)

- **Purpose:** Used for network diagnostics.
- **Example:** ping google.com sends ICMP Echo Requests and receives Echo Replies.
- **Use Case:** Helps check if a host is reachable and measures round-trip time.

2. TCP (Transmission Control Protocol)

- **Purpose:** Ensures reliable and ordered data delivery between devices.
- **Example:** Used in protocols like HTTP, HTTPS, FTP.

- **Use Case:** Establishes a connection (3-way handshake), ensures all data reaches correctly.

3. DNS (Domain Name System)

- **Purpose:** Resolves human-readable domain names into IP addresses.
- **Example:** When accessing example.com, your system sends a DNS query to find its IP.
- **Use Case:** First step in web browsing — without DNS, the browser can't find the server.

7. Export the capture as a .pcap file.

I have exported the capture

8. Summarize your findings and packet details.

During the network capture, three main types of packets were identified: ICMP, TCP, and DNS. Each of these serves a distinct role in network communication:

ICMP (Internet Control Message Protocol)

- Used for diagnostic and error-reporting functions.
- Commonly seen in tools like ping.
- Helps determine if a host is reachable and measures latency.

TCP (Transmission Control Protocol)

- A connection-oriented protocol that ensures reliable data transfer.
- Used in web browsing (HTTP/HTTPS), file transfers (FTP), emails, etc.
- Establishes a connection using a 3-way handshake before transmitting data.

DNS (Domain Name System)

- Resolves domain names (like google.com) to their respective IP addresses.

- Works before any website or online service can be accessed.
- Uses UDP or TCP on port 53, depending on the query type.