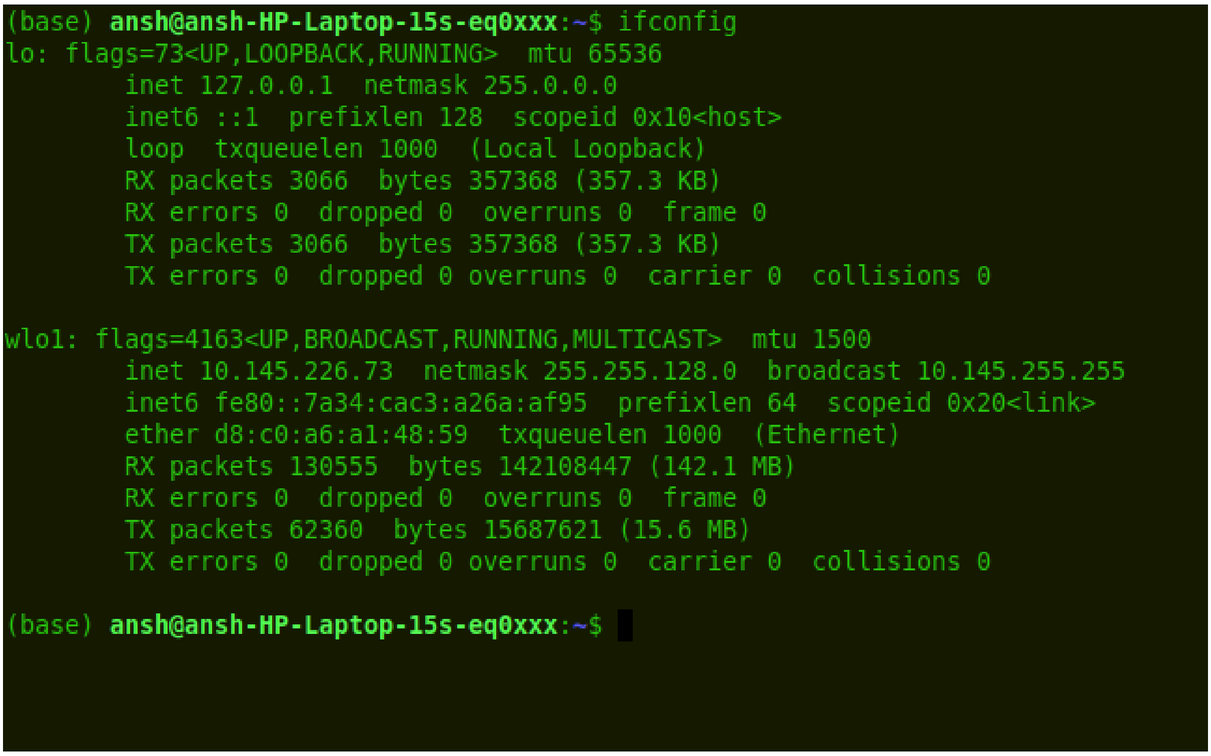
NAME : ANSH SAHU **ROLL NO : 22CS30010**

NETWORKING_LAB_ASSIGNMENT : 1

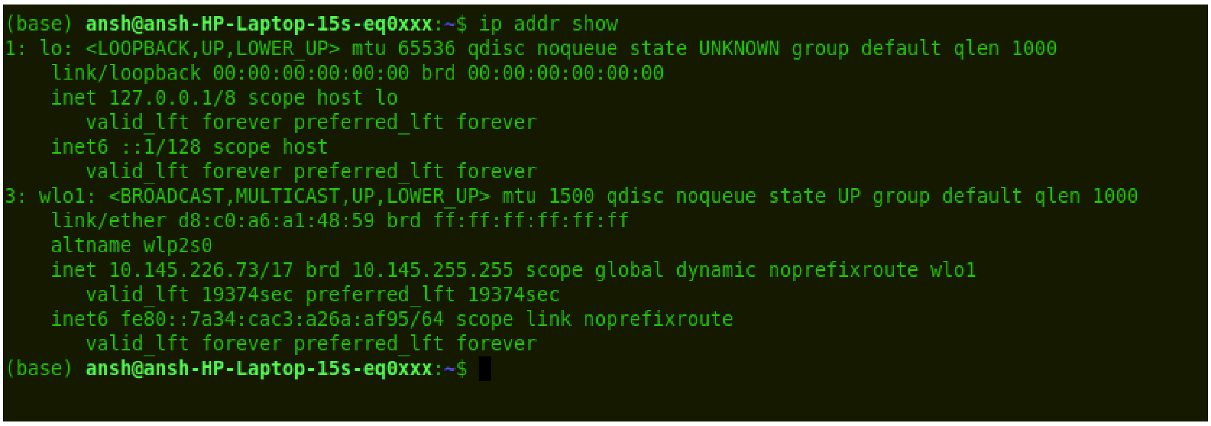
PART 1: NETWORKING TOOLS

1. Find the IP address of your machine, subnet mask, and network ID of your subnet.

Answer :

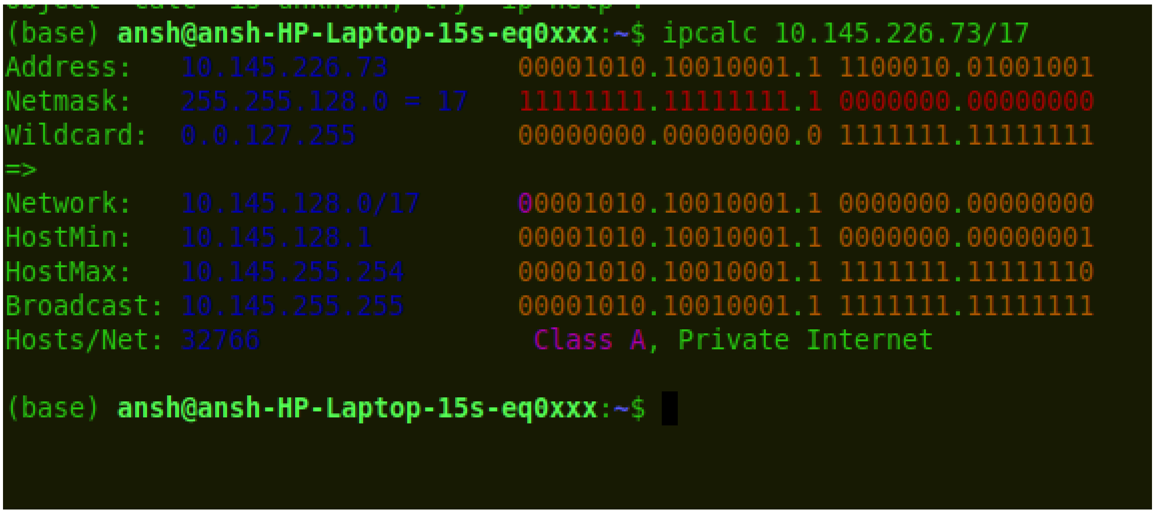


```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3066  bytes 357368 (357.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3066  bytes 357368 (357.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.145.226.73  netmask 255.255.128.0  broadcast 10.145.255.255
        inet6 fe80::7a34:cac3:a26a:af95  prefixlen 64  scopeid 0x20<link>
        ether d8:c0:a6:a1:48:59  txqueuelen 1000  (Ethernet)
        RX packets 130555  bytes 142108447 (142.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62360  bytes 15687621 (15.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ 
```



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether d8:c0:a6:a1:48:59 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
    inet 10.145.226.73/17 brd 10.145.255.255 scope global dynamic noprefixroute wlo1
       valid_lft 19374sec preferred_lft 19374sec
    inet6 fe80::7a34:cac3:a26a:af95/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ 
```

For wireless network
Ip address : 10.145.226.73
Netmask: 255.255.128.0/17

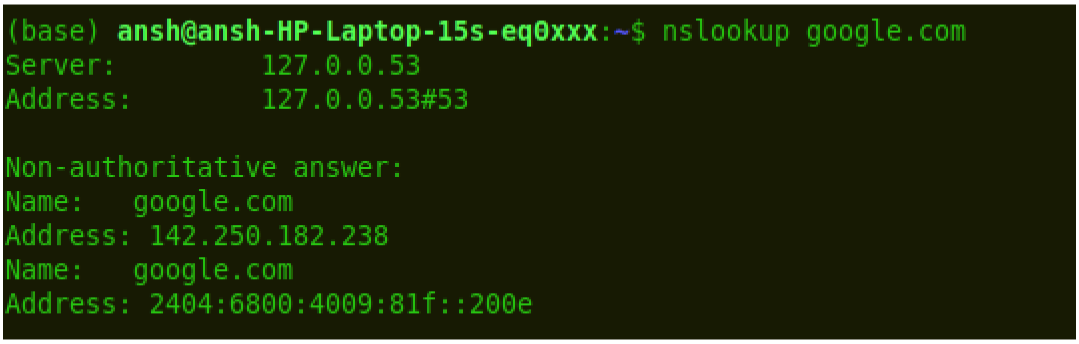


```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ ipcalc 10.145.226.73/17
Address:   10.145.226.73        00001010.10010001.1 1100010.01001001
Netmask:   255.255.128.0 = 17   11111111.11111111.1 0000000.00000000
Wildcard:  0.0.127.255          00000000.00000000.0 1111111.11111111
=>
Network:   10.145.128.0/17      00001010.10010001.1 0000000.00000000
HostMin:   10.145.128.1         00001010.10010001.1 0000000.00000001
HostMax:   10.145.255.254       00001010.10010001.1 1111111.11111110
Broadcast: 10.145.255.255       00001010.10010001.1 1111111.11111111
Hosts/Net: 32766                 Class A, Private Internet

(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ 
```

Network Id : 10.145.128.0/17

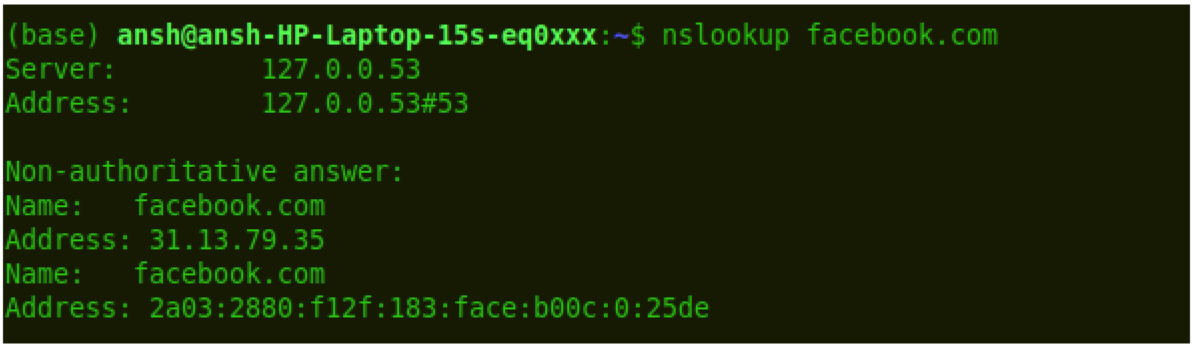
2.Find the IP address associated with www.google.com and www.facebook.com using nslookup. Change the DNS server address in the nslookup command to the following four IP addresses: 172.16.1.164, 172.16.1.180, 172.16.1.165, and 172.16.1.166, and see whether the IP address of the above domain name (www.google.com) changes. If you see a change in the IP address of www.google.com, can you think of the reason behind the same?

Answer :



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.238
Name:   google.com
Address: 2404:6800:4009:81f::200e
```

Ip address of google : 142.250.182.238

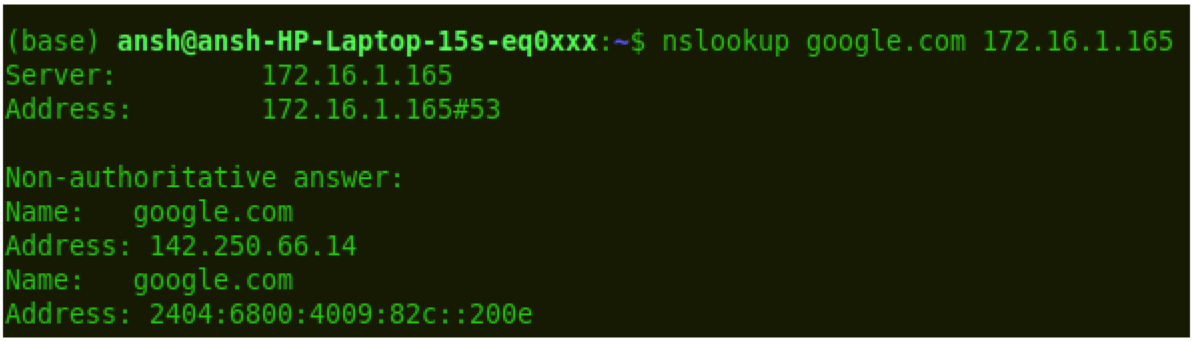


```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ nslookup facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   facebook.com
Address: 31.13.79.35
Name:   facebook.com
Address: 2a03:2880:f12f:183:face:b00c:0:25de
```

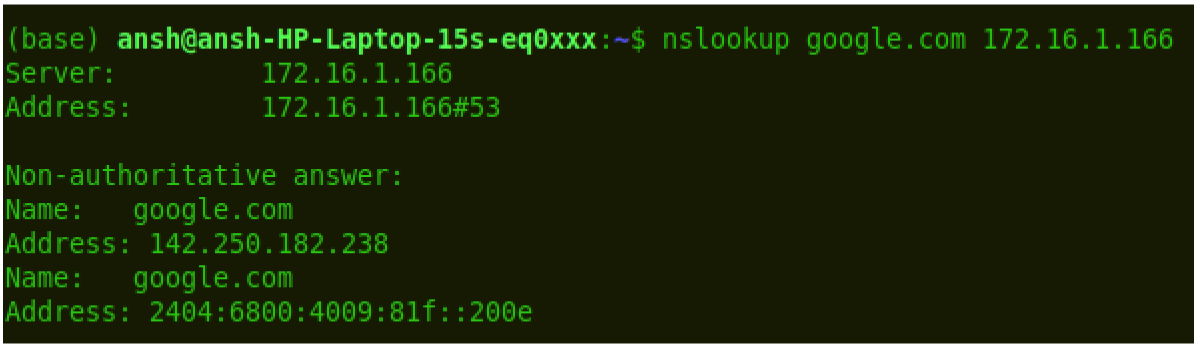
Ip address of facebook : 31.13.79.35

We get different ip address of google this is the reason behind it

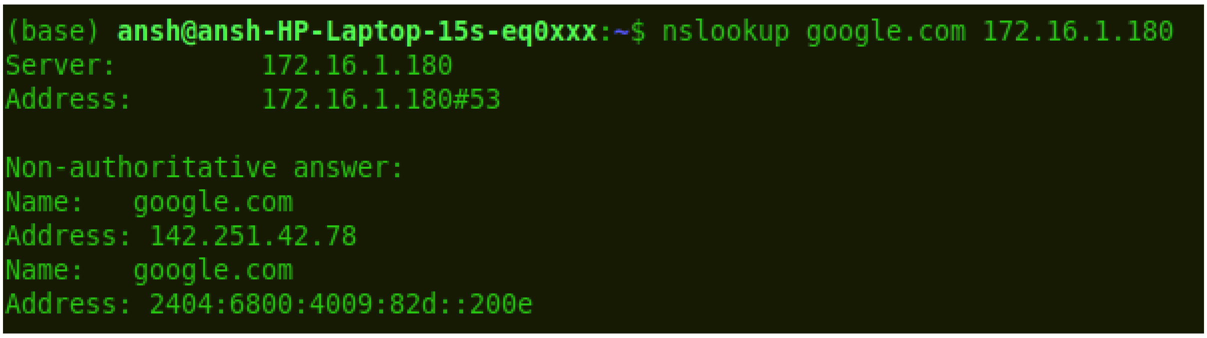
When using `nslookup` with different DNS servers, you get different IPs for Google because it uses multiple IPs for load balancing, Anycast routing directs requests to the nearest data center, GeoDNS assigns IPs based on the DNS server's location, different DNS servers may have varying cached records, and Google's CDN routes users to the closest server. This optimizes speed, reduces latency, and improves global performance.



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ nslookup google.com 172.16.1.165
Server:         172.16.1.165
Address:        172.16.1.165#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.66.14
Name:   google.com
Address: 2404:6800:4009:82c::200e
```



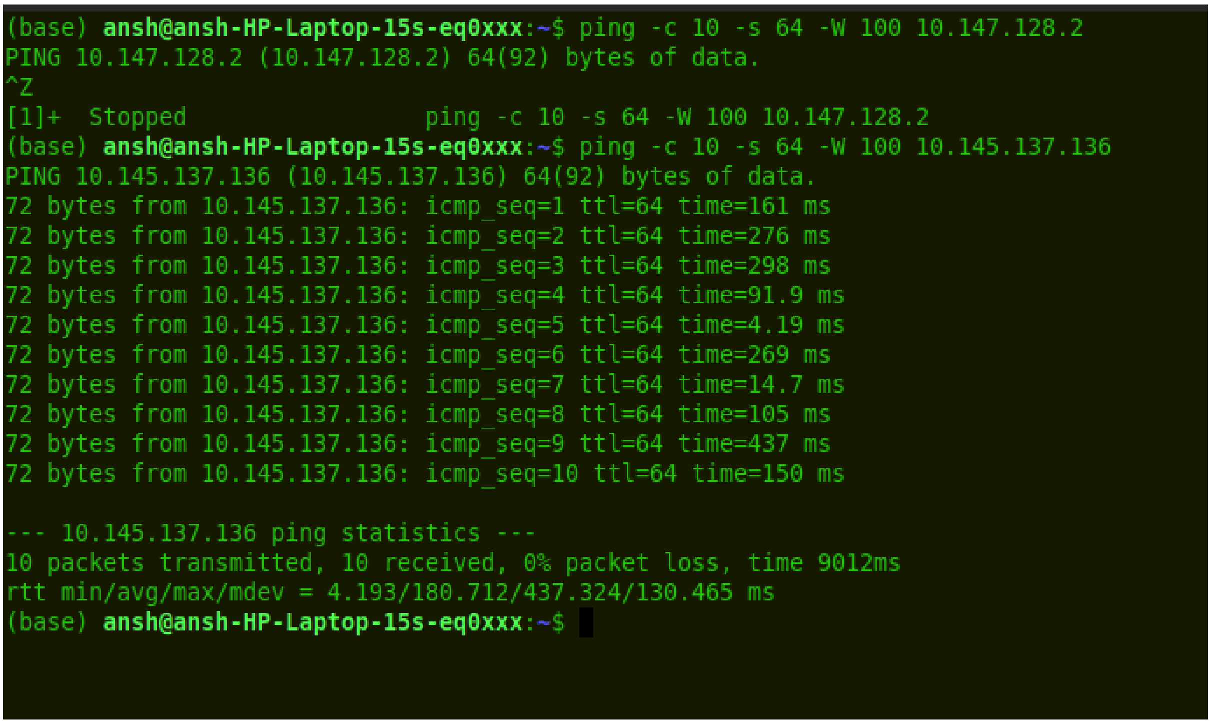
```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ nslookup google.com 172.16.1.166
Server:         172.16.1.166
Address:        172.16.1.166#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.238
Name:   google.com
Address: 2404:6800:4009:81f::200e
```



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ nslookup google.com 172.16.1.180
Server:         172.16.1.180
Address:        172.16.1.180#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.42.78
Name:   google.com
Address: 2404:6800:4009:82d::200e
```

3.Ping the IP address of one of your friend's machine IP within the software lab. Send the ping packets with different packet sizes (64, 128, 512 bytes) and timeout (100) for reporting packet loss percentage, min, avg, max, and stddev of round-trip time.

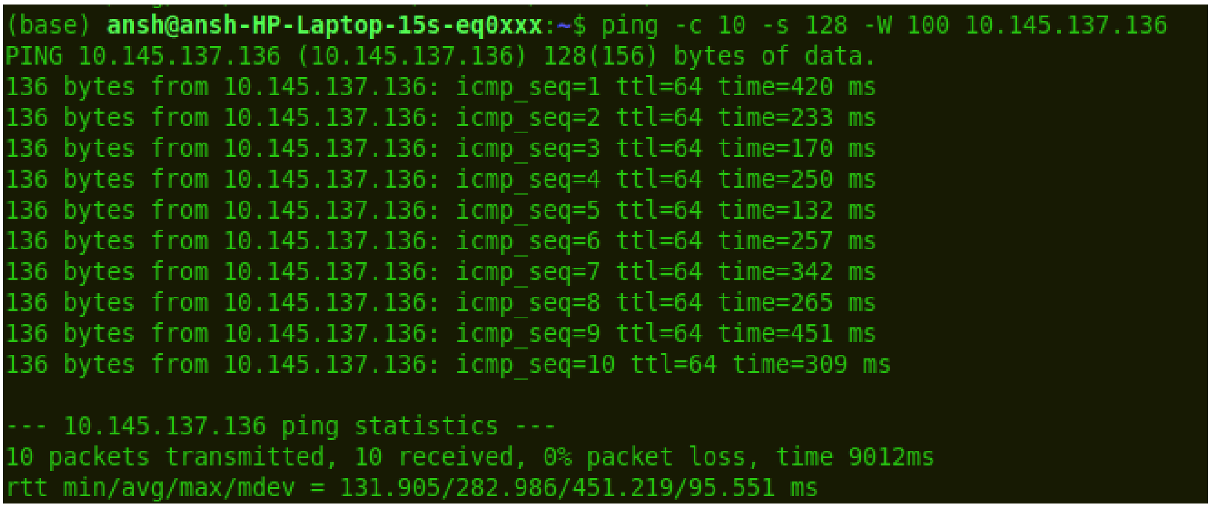
Answer :
I have send the packet to my phone which is connected to institute wifi
For packet size 64 byte after padding the packet become 72 bytes



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ ping -c 10 -s 64 -W 100 10.147.128.2
PING 10.147.128.2 (10.147.128.2) 64(92) bytes of data.
^Z
[1]+  Stopped                 ping -c 10 -s 64 -W 100 10.147.128.2
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ ping -c 10 -s 64 -W 100 10.145.137.136
PING 10.145.137.136 (10.145.137.136) 64(92) bytes of data.
72 bytes from 10.145.137.136: icmp_seq=1 ttl=64 time=161 ms
72 bytes from 10.145.137.136: icmp_seq=2 ttl=64 time=276 ms
72 bytes from 10.145.137.136: icmp_seq=3 ttl=64 time=298 ms
72 bytes from 10.145.137.136: icmp_seq=4 ttl=64 time=91.9 ms
72 bytes from 10.145.137.136: icmp_seq=5 ttl=64 time=4.19 ms
72 bytes from 10.145.137.136: icmp_seq=6 ttl=64 time=269 ms
72 bytes from 10.145.137.136: icmp_seq=7 ttl=64 time=14.7 ms
72 bytes from 10.145.137.136: icmp_seq=8 ttl=64 time=105 ms
72 bytes from 10.145.137.136: icmp_seq=9 ttl=64 time=437 ms
72 bytes from 10.145.137.136: icmp_seq=10 ttl=64 time=150 ms

--- 10.145.137.136 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 4.193/180.712/437.324/130.465 ms
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ 
```

Percentage of loss of the packets : 0%
Min time of the round trip : 4.193 ms
Max time of the round trip : 437.324 ms
Avg time of the round trip : 180.712 ms
Stddev of the round trip : 130.465 ms

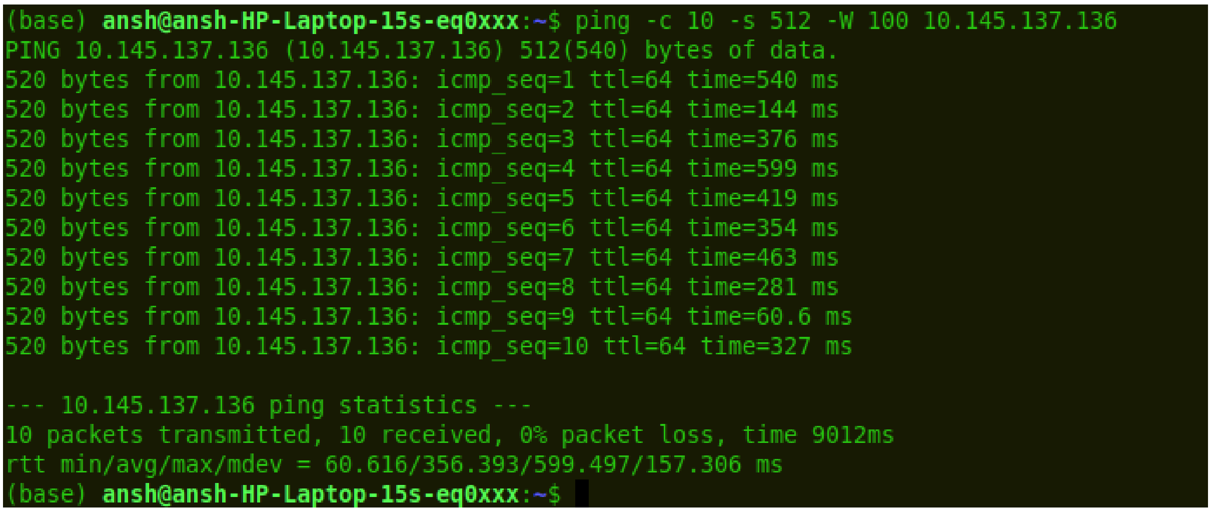
For packet size 128 byte after padding the packet become 136 bytes



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ ping -c 10 -s 128 -W 100 10.145.137.136
PING 10.145.137.136 (10.145.137.136) 128(156) bytes of data.
136 bytes from 10.145.137.136: icmp_seq=1 ttl=64 time=420 ms
136 bytes from 10.145.137.136: icmp_seq=2 ttl=64 time=233 ms
136 bytes from 10.145.137.136: icmp_seq=3 ttl=64 time=170 ms
136 bytes from 10.145.137.136: icmp_seq=4 ttl=64 time=250 ms
136 bytes from 10.145.137.136: icmp_seq=5 ttl=64 time=132 ms
136 bytes from 10.145.137.136: icmp_seq=6 ttl=64 time=257 ms
136 bytes from 10.145.137.136: icmp_seq=7 ttl=64 time=342 ms
136 bytes from 10.145.137.136: icmp_seq=8 ttl=64 time=265 ms
136 bytes from 10.145.137.136: icmp_seq=9 ttl=64 time=451 ms
136 bytes from 10.145.137.136: icmp_seq=10 ttl=64 time=309 ms

--- 10.145.137.136 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 131.905/282.986/451.219/95.551 ms
```

Percentage of loss of the packets : 0%
Min time of the round trip : 131.905 ms
Max time of the round trip : 451.219 ms
Avg time of the round trip : 282.986 ms
Stddev of the round trip : 95.551 ms

For packet size 512 byte after padding the packet become 520 bytes

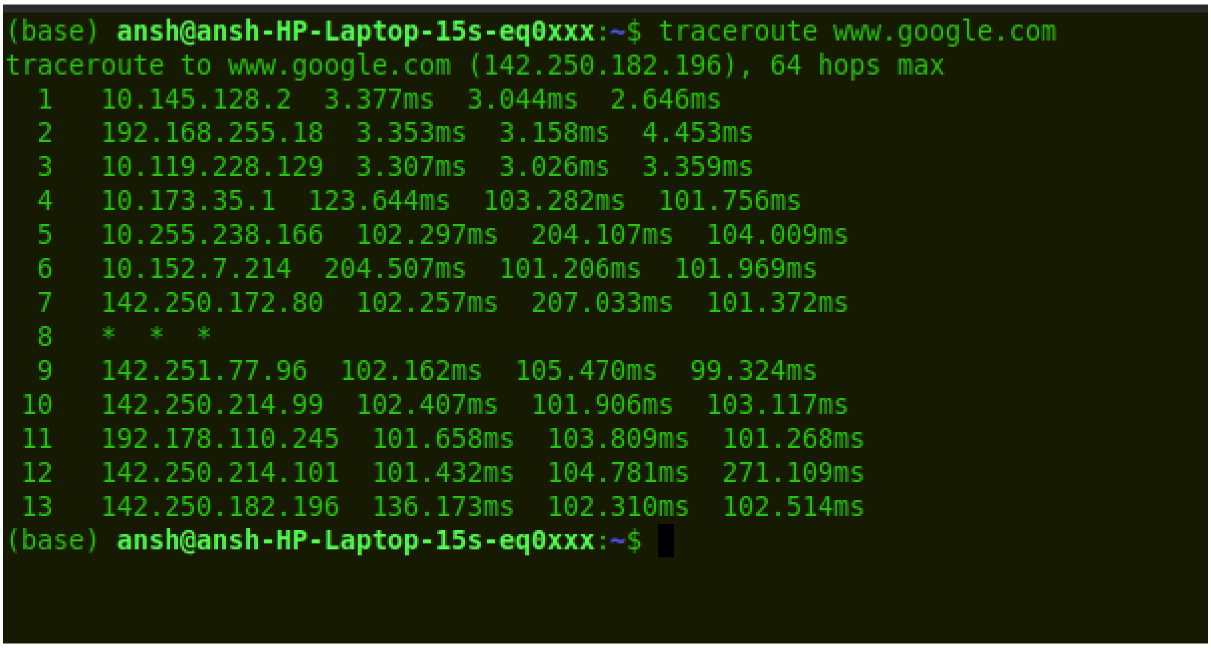


```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ ping -c 10 -s 512 -W 100 10.145.137.136
PING 10.145.137.136 (10.145.137.136) 512(540) bytes of data.
520 bytes from 10.145.137.136: icmp_seq=1 ttl=64 time=540 ms
520 bytes from 10.145.137.136: icmp_seq=2 ttl=64 time=144 ms
520 bytes from 10.145.137.136: icmp_seq=3 ttl=64 time=376 ms
520 bytes from 10.145.137.136: icmp_seq=4 ttl=64 time=599 ms
520 bytes from 10.145.137.136: icmp_seq=5 ttl=64 time=419 ms
520 bytes from 10.145.137.136: icmp_seq=6 ttl=64 time=354 ms
520 bytes from 10.145.137.136: icmp_seq=7 ttl=64 time=463 ms
520 bytes from 10.145.137.136: icmp_seq=8 ttl=64 time=281 ms
520 bytes from 10.145.137.136: icmp_seq=9 ttl=64 time=60.6 ms
520 bytes from 10.145.137.136: icmp_seq=10 ttl=64 time=327 ms

--- 10.145.137.136 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 60.616/356.393/599.497/157.306 ms
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ 
```

Percentage of loss of the packets : 0%
Min time of the round trip : 60.616 ms
Max time of the round trip : 599.497 ms
Avg time of the round trip : 356.393 ms
Stddev of the round trip : 157.306 ms

4. Run traceroute for www.google.com and print the summary. Count the number of hosts involved in the path from source to destination. Why do you see some "* * *" in the intermediate hops?

Answer :



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ traceroute www.google.com
traceroute to www.google.com (142.250.182.196), 64 hops max
  1   10.145.128.2  3.377ms  3.044ms  2.646ms
  2   192.168.255.18  3.353ms  3.158ms  4.453ms
  3   10.119.228.129  3.307ms  3.026ms  3.359ms
  4   10.173.35.1  123.644ms  103.282ms  101.756ms
  5   10.255.238.166  102.297ms  204.107ms  104.009ms
  6   10.152.7.214  204.507ms  101.206ms  101.969ms
  7   142.250.172.80  102.257ms  207.033ms  101.372ms
  8   *  *  *
  9   142.251.77.96  102.162ms  105.470ms  99.324ms
 10   142.250.214.99  102.407ms  101.906ms  103.117ms
 11   192.178.110.245  101.658ms  103.809ms  101.268ms
 12   142.250.214.101  101.432ms  104.781ms  271.109ms
 13   142.250.182.196  136.173ms  102.310ms  102.514ms
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ 
```

No of host involved in the source to destination route 12(excluding)

The * * * appears when a router does not respond to the traceroute request. This happens due to:

- **Security Rules** – Some ISPs or companies block ICMP (ping) requests.

- **Rate Limiting** – Some routers limit how often they respond to traceroute.
- **Packet Loss** – Network issues can cause dropped responses.
- **Hidden Routers** – Some intermediate routers do not reveal their presence for security reasons.

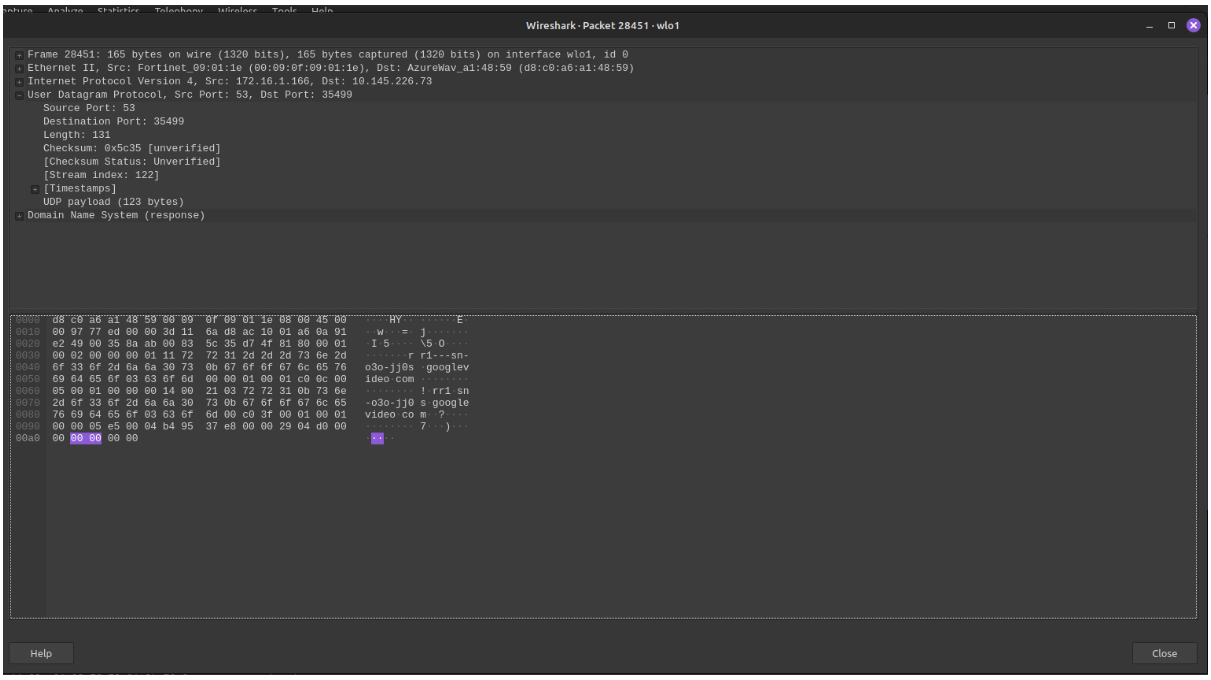
PART 2 : PACKET ANALYSIS

1. Analysis of DNS Packets: Structure and its Traffic

a) Locate the DNS query and response messages. Is DNS using UDP or TCP in the observed packets?

Answer

We observe udp protocol in dns response

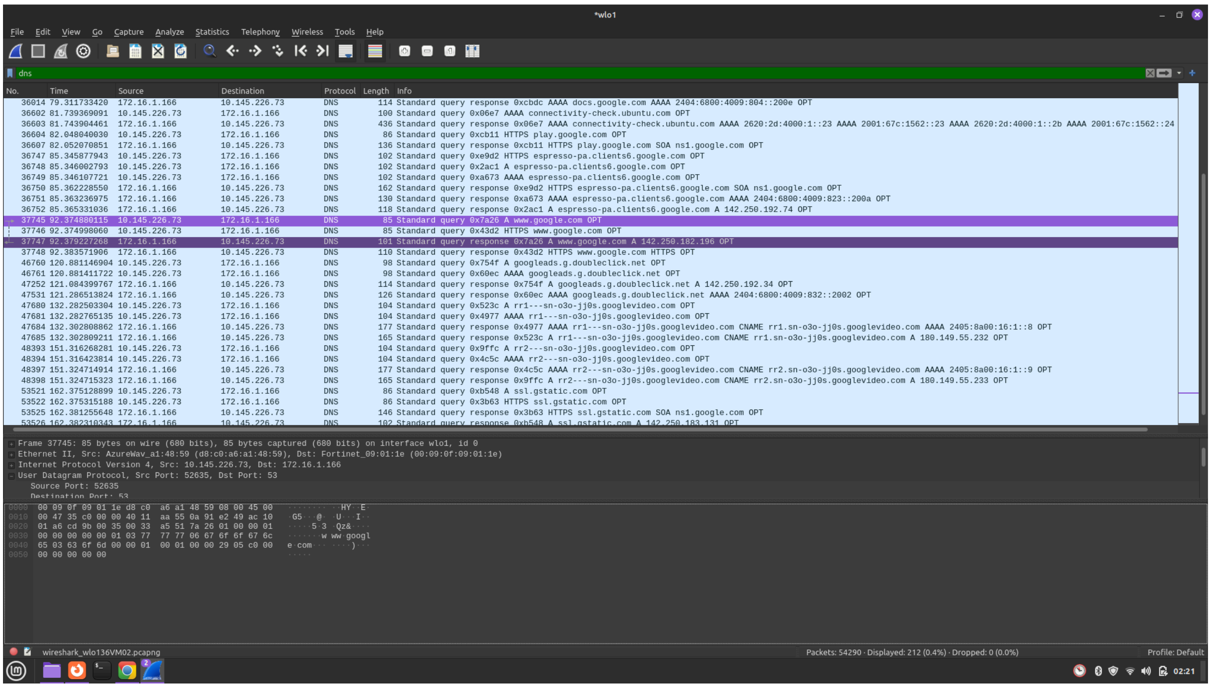


```
+ Frame 28451: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface wlo1, id 0
+ Ethernet II, Src: Fortinet_09:01:1e (00:09:0f:09:01:1e), Dst: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59)
+ Internet Protocol Version 4, Src: 172.16.1.166, Dst: 10.145.226.73
- User Datagram Protocol, Src Port: 53, Dst Port: 35499
    Source Port: 53
    Destination Port: 35499
    Length: 131
    Checksum: 0x5c35 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 122]
  + [Timestamps]
    UDP payload (123 bytes)
+ Domain Name System (response)
```

```
0000  d8 c0 a6 a1 48 59 00 09  0f 09 01 1e 08 00 45 00   ····HY·· ······E·
0010  00 97 77 ed 00 00 3d 11  6a d8 ac 10 01 a6 0a 91   ··w···=· j·······
0020  e2 49 00 35 8a ab 00 83  5c 35 d7 4f 81 80 00 01   ·I·5···· \5·O····
0030  00 02 00 00 00 01 11 72  72 31 2d 2d 2d 73 6e 2d   ·······r r1---sn-
0040  6f 33 6f 2d 6a 6a 30 73  0b 67 6f 6f 67 6c 65 76   o3o-jj0s ·googlev
0050  69 64 65 6f 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ideo·com ········
0060  05 00 01 00 00 00 14 00  21 03 72 72 31 0b 73 6e   ········ !·rr1·sn
0070  2d 6f 33 6f 2d 6a 6a 30  73 0b 67 6f 6f 67 6c 65   -o3o-jj0 s·google
0080  76 69 64 65 6f 03 63 6f  6d 00 c0 3f 00 01 00 01   video·co m··?····
0090  00 00 05 e5 00 04 b4 95  37 e8 00 00 29 04 d0 00   ········ 7···)···
00a0  00 00 00 00 00                                     ·····
```

b) Check the source and destination IP address of the DNS query

Answer :



*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time          Source          Destination     Protocol Length Info
36014 79.311733420  172.16.1.166    10.145.226.73   DNS      114 Standard query response 0xcbdc AAAA docs.google.com AAAA 2404:6800:4009:804::200e OPT
36602 81.739369091  10.145.226.73   172.16.1.166    DNS      100 Standard query 0x06e7 AAAA connectivity-check.ubuntu.com OPT
36603 81.743904461  172.16.1.166    10.145.226.73   DNS      436 Standard query response 0x06e7 AAAA connectivity-check.ubuntu.com AAAA 2620:2d:4000:1::23 AAAA 2001:67c:1562::23 AAAA 2620:2d:4000:1::2b AAAA 2001:67c:1562::24
36604 82.048040030  10.145.226.73   172.16.1.166    DNS       86 Standard query 0xcb11 HTTPS play.google.com OPT
36607 82.052070851  172.16.1.166    10.145.226.73   DNS      136 Standard query response 0xcb11 HTTPS play.google.com SOA ns1.google.com OPT
36747 85.345877943  10.145.226.73   172.16.1.166    DNS      102 Standard query 0xe9d2 HTTPS espresso-pa.clients6.google.com OPT
36748 85.346002793  10.145.226.73   172.16.1.166    DNS      102 Standard query 0x2ac1 A espresso-pa.clients6.google.com OPT
36749 85.346107721  10.145.226.73   172.16.1.166    DNS      102 Standard query 0xa673 AAAA espresso-pa.clients6.google.com OPT
36750 85.362228550  172.16.1.166    10.145.226.73   DNS      162 Standard query response 0xe9d2 HTTPS espresso-pa.clients6.google.com SOA ns1.google.com OPT
36751 85.363236975  172.16.1.166    10.145.226.73   DNS      130 Standard query response 0xa673 AAAA espresso-pa.clients6.google.com AAAA 2404:6800:4009:823::200a OPT
36752 85.365331036  172.16.1.166    10.145.226.73   DNS      118 Standard query response 0x2ac1 A espresso-pa.clients6.google.com A 142.250.192.74 OPT
37745 92.374880115  10.145.226.73   172.16.1.166    DNS       85 Standard query 0x7a26 A www.google.com OPT
37746 92.374998060  10.145.226.73   172.16.1.166    DNS       85 Standard query 0x43d2 HTTPS www.google.com OPT
37747 92.379227268  172.16.1.166    10.145.226.73   DNS      101 Standard query response 0x7a26 A www.google.com A 142.250.182.196 OPT
37748 92.383571906  172.16.1.166    10.145.226.73   DNS      110 Standard query response 0x43d2 HTTPS www.google.com HTTPS OPT
46760 120.881146904 10.145.226.73   172.16.1.166    DNS       98 Standard query 0x754f A googleads.g.doubleclick.net OPT
46761 120.881411722 10.145.226.73   172.16.1.166    DNS       98 Standard query 0x60ec AAAA googleads.g.doubleclick.net OPT
47252 121.084399767 172.16.1.166    10.145.226.73   DNS      114 Standard query response 0x754f A googleads.g.doubleclick.net A 142.250.192.34 OPT
47531 121.286513824 172.16.1.166    10.145.226.73   DNS      126 Standard query response 0x60ec AAAA googleads.g.doubleclick.net AAAA 2404:6800:4009:832::2002 OPT
47680 132.282503304 10.145.226.73   172.16.1.166    DNS      104 Standard query 0x523c A rr1---sn-o3o-jj0s.googlevideo.com OPT
47681 132.282765135 10.145.226.73   172.16.1.166    DNS      104 Standard query 0x4977 AAAA rr1---sn-o3o-jj0s.googlevideo.com OPT
47684 132.302808862 172.16.1.166    10.145.226.73   DNS      177 Standard query response 0x4977 AAAA rr1---sn-o3o-jj0s.googlevideo.com CNAME rr1.sn-o3o-jj0s.googlevideo.com AAAA 2405:8a00:16:1::8 OPT
47685 132.302809211 172.16.1.166    10.145.226.73   DNS      165 Standard query response 0x523c A rr1---sn-o3o-jj0s.googlevideo.com CNAME rr1.sn-o3o-jj0s.googlevideo.com A 180.149.55.232 OPT
48393 151.316268281 10.145.226.73   172.16.1.166    DNS      104 Standard query 0x9ffc A rr2---sn-o3o-jj0s.googlevideo.com OPT
48394 151.316423814 10.145.226.73   172.16.1.166    DNS      104 Standard query 0x4c5c AAAA rr2---sn-o3o-jj0s.googlevideo.com OPT
48397 151.324714914 172.16.1.166    10.145.226.73   DNS      177 Standard query response 0x4c5c AAAA rr2---sn-o3o-jj0s.googlevideo.com CNAME rr2.sn-o3o-jj0s.googlevideo.com AAAA 2405:8a00:16:1::9 OPT
48398 151.324715323 172.16.1.166    10.145.226.73   DNS      165 Standard query response 0x9ffc A rr2---sn-o3o-jj0s.googlevideo.com CNAME rr2.sn-o3o-jj0s.googlevideo.com A 180.149.55.233 OPT
53521 162.375128899 10.145.226.73   172.16.1.166    DNS       86 Standard query 0xb548 A ssl.gstatic.com OPT
53522 162.375315188 10.145.226.73   172.16.1.166    DNS       86 Standard query 0x3b63 HTTPS ssl.gstatic.com OPT
53525 162.381255648 172.16.1.166    10.145.226.73   DNS      146 Standard query response 0x3b63 HTTPS ssl.gstatic.com SOA ns1.google.com OPT
53526 162.382310343 172.16.1.166    10.145.226.73   DNS      102 Standard query response 0xb548 A ssl.gstatic.com A 142.250.183.131 OPT
```

```
+ Frame 37745: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface wlo1, id 0
+ Ethernet II, Src: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59), Dst: Fortinet_09:01:1e (00:09:0f:09:01:1e)
+ Internet Protocol Version 4, Src: 10.145.226.73, Dst: 172.16.1.166
- User Datagram Protocol, Src Port: 52635, Dst Port: 53
    Source Port: 52635
    Destination Port: 53
```

```
0000  00 09 0f 09 01 1e d8 c0  a6 a1 48 59 08 00 45 00   ··········HY··E·
0010  00 47 35 c0 00 00 40 11  aa 55 0a 91 e2 49 ac 10   ·G5···@··U···I··
0020  01 a6 cd 9b 00 35 00 33  a5 51 7a 26 01 00 00 01   ·····5·3·Qz&····
0030  00 00 00 00 00 01 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01 00 00 29 05 c0 00   e·com·······)···
0050  00 00 00 00 00                                     ·····
```

wireshark_wlo136VM02.pcapng
Packets: 54290 · Displayed: 212 (0.4%) · Dropped: 0 (0.0%)
Profile: Default
02:21

Source ip address : 10.145.226.73

Destination ip address : 172.16.1.166

c) How many DNS queries are sent from your browser (host machine) to DNS Server(s) during the name-to-IP resolution?

Answer : it sends 3 queries from my machine to the dns server machine for name to ip-resolution.

d) Which DNS Server replies with actual IP Address(es).

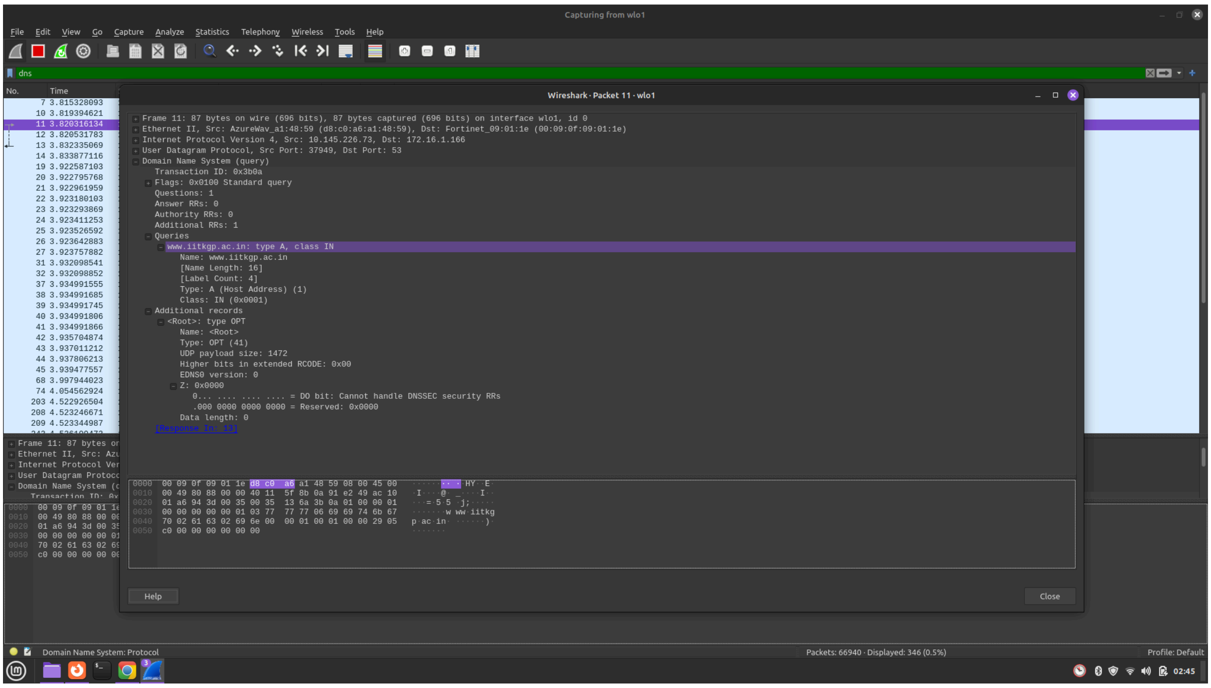
Answer : dns server of ip address 172.16.1.166 give the ip address of iitkgp.ac.in.

e) How many DNS servers are involved? Do all DNS servers respond?

Answer : only 1 dns server is involved. The server is responding to the query of the name ip query.

f) Clearly list the resource records involved in resolving the site's IP address, mentioning Name, Type, Class, TTL, Data length, and resolved IP address appropriately in the complete resolving process of this DNS conversation, including query/queries and response/answer(s).

Answer :

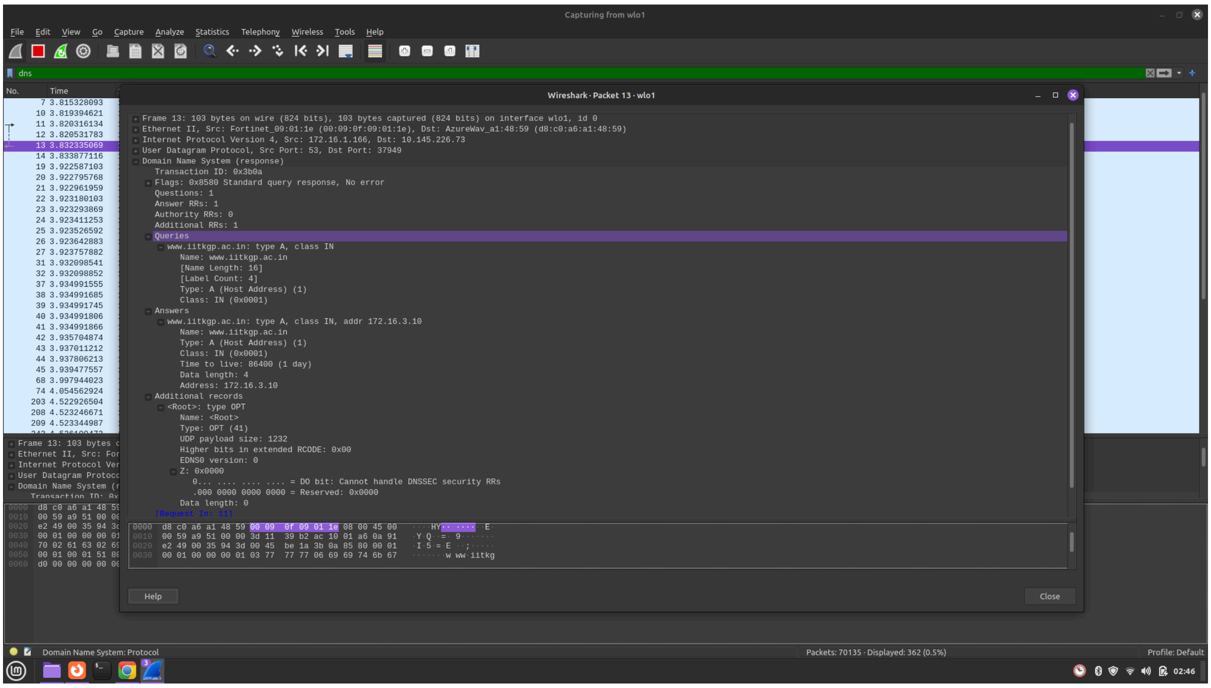

Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Wireshark · Packet 11 · wlo1
Help
Close

```
No.  Time
  7 3.815328093
 10 3.819394621
 11 3.820316134
 12 3.820531783
 13 3.832335069
 14 3.833877116
 19 3.922587103
 20 3.922795768
 21 3.922961959
 22 3.923180103
 23 3.923293869
 24 3.923411253
 25 3.923526592
 26 3.923642883
 27 3.923757882
 31 3.932098541
 32 3.932098852
 37 3.934991555
 38 3.934991685
 39 3.934991745
 40 3.934991806
 41 3.934991866
 42 3.935704874
 43 3.937011212
 44 3.937806213
 45 3.939477557
 68 3.997944023
 74 4.054562924
203 4.522926504
208 4.523246671
209 4.523344987
```

```
Frame 11: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface wlo1, id 0
Ethernet II, Src: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59), Dst: Fortinet_09:01:1e (00:09:0f:09:01:1e)
Internet Protocol Version 4, Src: 10.145.226.73, Dst: 172.16.1.166
User Datagram Protocol, Src Port: 37949, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x3b0a
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    www.iitkgp.ac.in: type A, class IN
      Name: www.iitkgp.ac.in
      [Name Length: 16]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 1472
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
      Z: 0x0000
        0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
        .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 0
  [Response In: 13]
```

```
0000  00 09 0f 09 01 1e d8 c0  a6 a1 48 59 08 00 45 00   ······ ·· ·HY··E·
0010  00 49 80 88 00 00 40 11  5f 8b 0a 91 e2 49 ac 10   ·I····@· _····I··
0020  01 a6 94 3d 00 35 00 35  13 6a 3b 0a 01 00 00 01   ···=·5·5 ·j;·····
0030  00 00 00 00 00 01 03 77  77 77 06 69 69 74 6b 67   ·······w ww·iitkg
0040  70 02 61 63 02 69 6e 00  00 01 00 01 00 00 29 05   p·ac·in· ······)·
0050  c0 00 00 00 00 00 00                               ·······
```

Domain Name System: Protocol · Packets: 66940 · Displayed: 346 (0.5%) · Profile: Default · 02:45

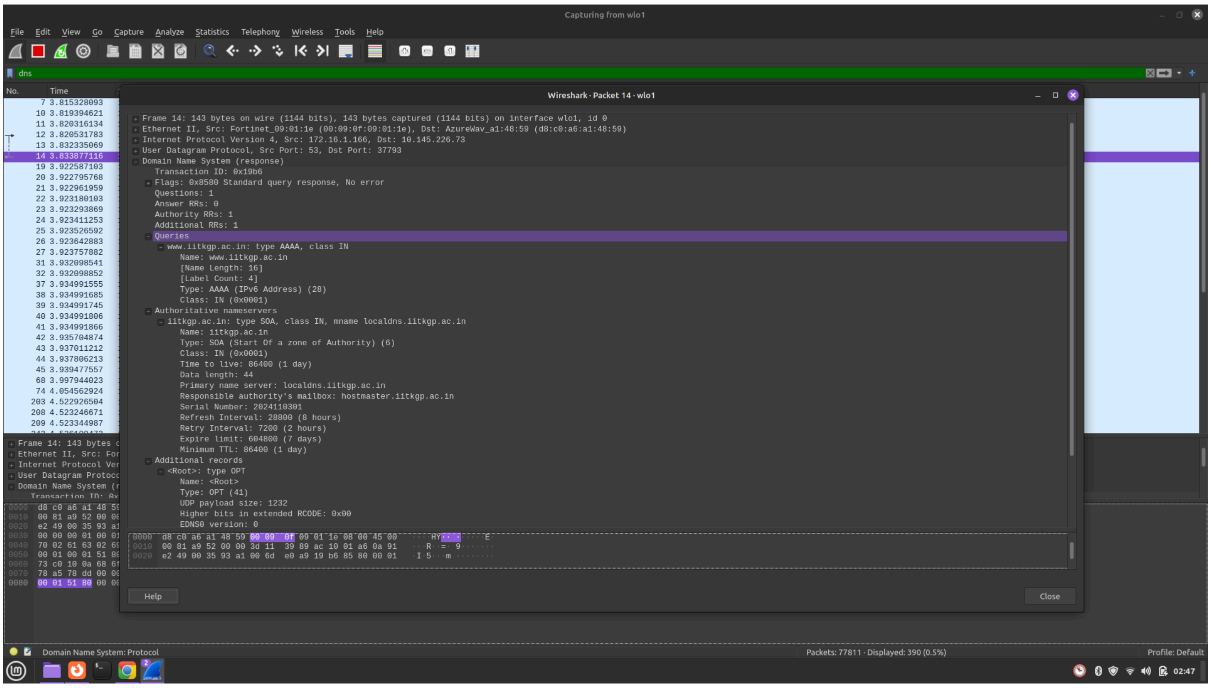

Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Wireshark · Packet 13 · wlo1
Help
Close

```
No.  Time
  7 3.815328093
 10 3.819394621
 11 3.820316134
 12 3.820531783
 13 3.832335069
 14 3.833877116
 19 3.922587103
 20 3.922795768
 21 3.922961959
 22 3.923180103
 23 3.923293869
 24 3.923411253
 25 3.923526592
 26 3.923642883
 27 3.923757882
 31 3.932098541
 32 3.932098852
 37 3.934991555
 38 3.934991685
 39 3.934991745
 40 3.934991806
 41 3.934991866
 42 3.935704874
 43 3.937011212
 44 3.937806213
 45 3.939477557
 68 3.997944023
 74 4.054562924
203 4.522926504
208 4.523246671
209 4.523344987
```

```
Frame 13: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface wlo1, id 0
Ethernet II, Src: Fortinet_09:01:1e (00:09:0f:09:01:1e), Dst: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59)
Internet Protocol Version 4, Src: 172.16.1.166, Dst: 10.145.226.73
User Datagram Protocol, Src Port: 53, Dst Port: 37949
Domain Name System (response)
  Transaction ID: 0x3b0a
  Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 1
  Queries
    www.iitkgp.ac.in: type A, class IN
      Name: www.iitkgp.ac.in
      [Name Length: 16]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Answers
    www.iitkgp.ac.in: type A, class IN, addr 172.16.3.10
      Name: www.iitkgp.ac.in
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 4
      Address: 172.16.3.10
  Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 1232
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
      Z: 0x0000
        0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
        .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 0
  [Request In: 11]
```

```
0000  d8 c0 a6 a1 48 59 00 09  0f 09 01 1e 08 00 45 00   ····HY·· ····  ··E·
0010  00 59 a9 51 00 00 3d 11  39 b2 ac 10 01 a6 0a 91   ·Y·Q··=· 9·······
0020  e2 49 00 35 94 3d 00 45  be 1a 3b 0a 85 80 00 01   ·I·5·=·E ··;·····
0030  00 01 00 00 00 01 03 77  77 77 06 69 69 74 6b 67   ·······w ww·iitkg
```

Domain Name System: Protocol · Packets: 70135 · Displayed: 362 (0.5%) · Profile: Default · 02:46



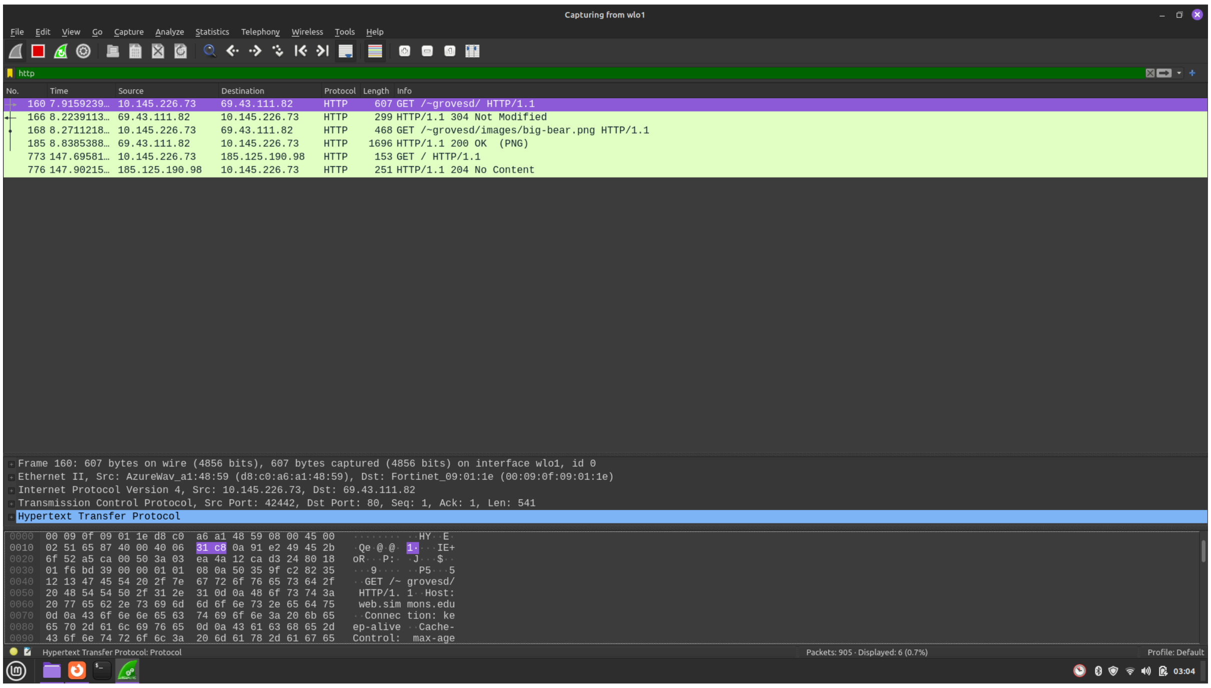
```
Frame 14: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface wlo1, id 0
Ethernet II, Src: Fortinet_09:01:1e (00:09:0f:09:01:1e), Dst: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59)
Internet Protocol Version 4, Src: 172.16.1.166, Dst: 10.145.226.73
User Datagram Protocol, Src Port: 53, Dst Port: 37793
Domain Name System (response)
  Transaction ID: 0x19b6
  Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 1
  Queries
    www.iitkgp.ac.in: type AAAA, class IN
      Name: www.iitkgp.ac.in
      [Name Length: 16]
      [Label Count: 4]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
  Authoritative nameservers
    iitkgp.ac.in: type SOA, class IN, mname localdns.iitkgp.ac.in
      Name: iitkgp.ac.in
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 44
      Primary name server: localdns.iitkgp.ac.in
      Responsible authority's mailbox: hostmaster.iitkgp.ac.in
      Serial Number: 2024110301
      Refresh Interval: 28800 (8 hours)
      Retry Interval: 7200 (2 hours)
      Expire limit: 604800 (7 days)
      Minimum TTL: 86400 (1 day)
  Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 1232
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0

0000  d8 c0 a6 a1 48 59 00 09  0f 09 01 1e 08 00 45 00   ····HY·· ·····E·
0010  00 81 a9 52 00 00 3d 11  39 89 ac 10 01 a6 0a 91   ···R··=· 9·······
0020  e2 49 00 35 93 a1 00 6d  e0 a9 19 b6 85 80 00 01   ·I·5···m ········
```

2. Web Traffic (HTTP)

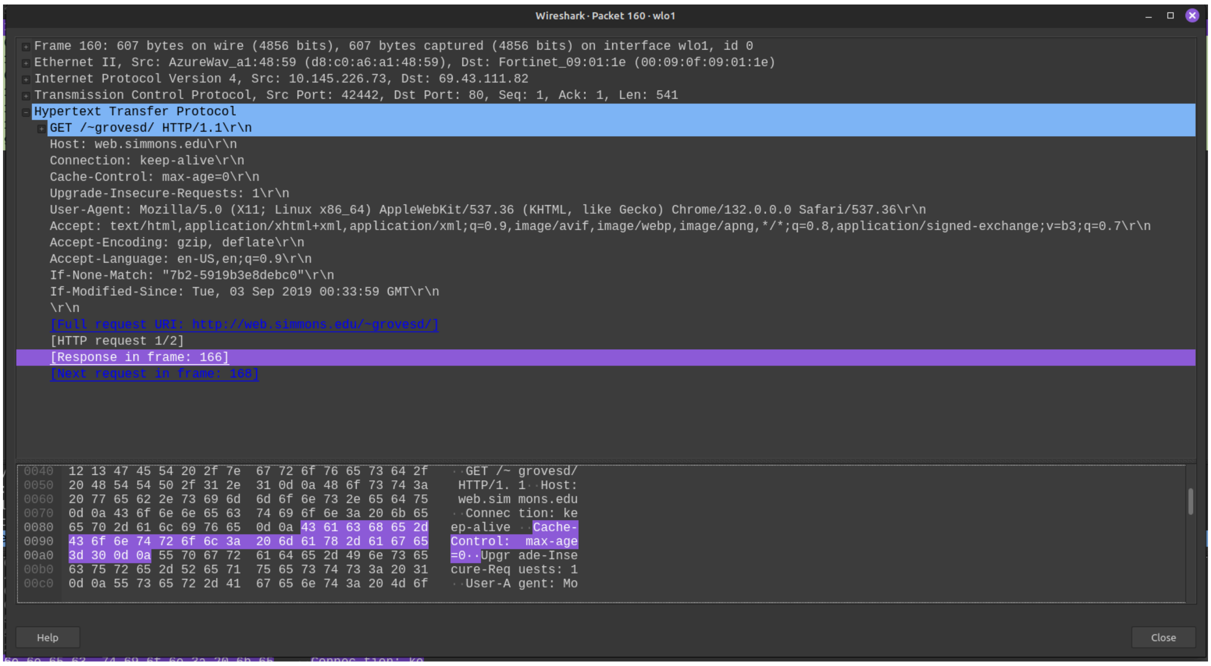
Initiate web traffic for the web server- http://web.simmons.edu/~grovesd/ through the browser from your local machine and do the following list of tasks in Wireshark.

a) Filter the HTTP packets and observe traffic between the client and the web server.

Answer :

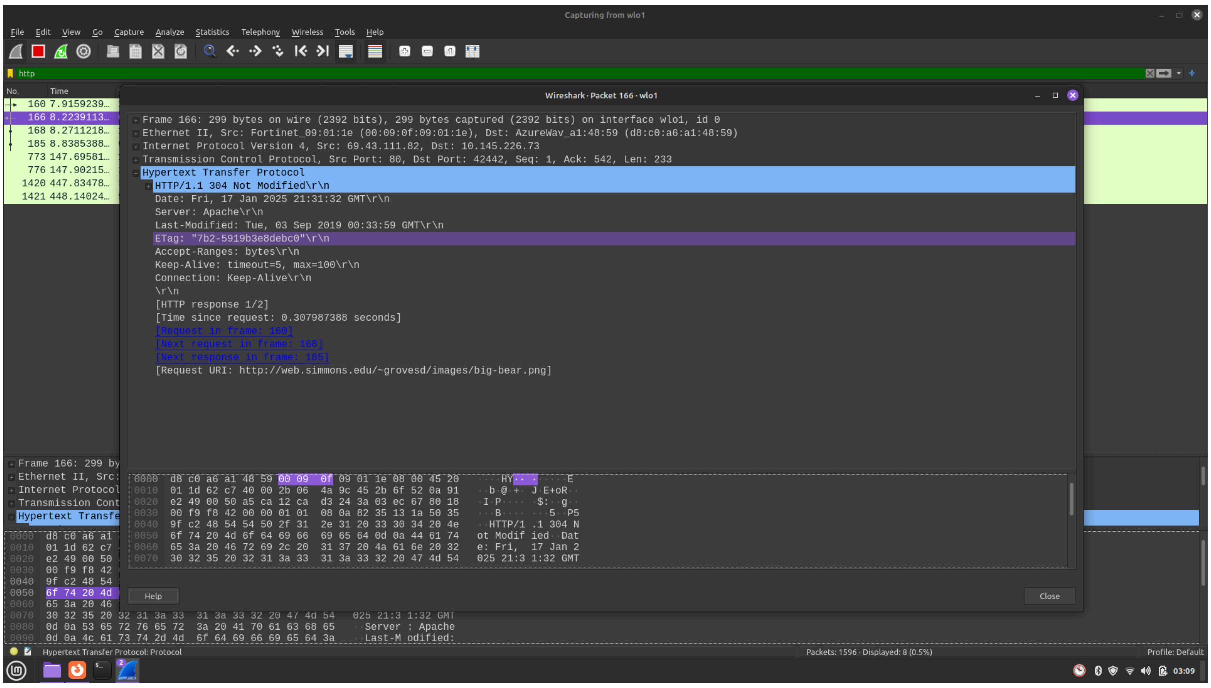


```
No.  Time          Source           Destination      Protocol Length Info
 160 7.9159239…   10.145.226.73    69.43.111.82     HTTP      607 GET /~grovesd/ HTTP/1.1
 166 8.2239113…   69.43.111.82     10.145.226.73    HTTP      299 HTTP/1.1 304 Not Modified
 168 8.2711218…   10.145.226.73    69.43.111.82     HTTP      468 GET /~grovesd/images/big-bear.png HTTP/1.1
 185 8.8385388…   69.43.111.82     10.145.226.73    HTTP     1696 HTTP/1.1 200 OK  (PNG)
 773 147.69581…   10.145.226.73    185.125.190.98   HTTP      153 GET / HTTP/1.1
 776 147.90215…   185.125.190.98   10.145.226.73    HTTP      251 HTTP/1.1 204 No Content

Frame 160: 607 bytes on wire (4856 bits), 607 bytes captured (4856 bits) on interface wlo1, id 0
Ethernet II, Src: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59), Dst: Fortinet_09:01:1e (00:09:0f:09:01:1e)
Internet Protocol Version 4, Src: 10.145.226.73, Dst: 69.43.111.82
Transmission Control Protocol, Src Port: 42442, Dst Port: 80, Seq: 1, Ack: 1, Len: 541
Hypertext Transfer Protocol

0000  00 09 0f 09 01 1e d8 c0  a6 a1 48 59 08 00 45 00   ········ ··HY··E·
0010  02 51 65 87 40 00 40 06  31 c8 0a 91 e2 49 45 2b   ·Qe·@·@· 1····IE+
0020  6f 52 a5 ca 00 50 3a 03  ea 4a 12 ca d3 24 80 18   oR···P:· ·J···$··
0030  01 f6 bd 39 00 00 01 01  08 0a 50 35 9f c2 82 35   ···9···· ··P5···5
0040  12 13 47 45 54 20 2f 7e  67 72 6f 76 65 73 64 2f   ··GET /~ grovesd/
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0060  20 77 65 62 2e 73 69 6d  6d 6f 6e 73 2e 65 64 75    web.sim mons.edu
0070  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec tion: ke
0080  65 70 2d 61 6c 69 76 65  0d 0a 43 61 63 68 65 2d   ep-alive ··Cache-
0090  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
```



```
Frame 160: 607 bytes on wire (4856 bits), 607 bytes captured (4856 bits) on interface wlo1, id 0
Ethernet II, Src: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59), Dst: Fortinet_09:01:1e (00:09:0f:09:01:1e)
Internet Protocol Version 4, Src: 10.145.226.73, Dst: 69.43.111.82
Transmission Control Protocol, Src Port: 42442, Dst Port: 80, Seq: 1, Ack: 1, Len: 541
Hypertext Transfer Protocol
  GET /~grovesd/ HTTP/1.1\r\n
  Host: web.simmons.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "7b2-5919b3e8debc0"\r\n
  If-Modified-Since: Tue, 03 Sep 2019 00:33:59 GMT\r\n
  \r\n
  [Full request URI: http://web.simmons.edu/~grovesd/]
  [HTTP request 1/2]
  [Response in frame: 166]
  [Next request in frame: 168]
```

```
0040  12 13 47 45 54 20 2f 7e  67 72 6f 76 65 73 64 2f   ··GET /~ grovesd/
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0060  20 77 65 62 2e 73 69 6d  6d 6f 6e 73 2e 65 64 75    web.sim mons.edu
0070  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec tion: ke
0080  65 70 2d 61 6c 69 76 65  0d 0a 43 61 63 68 65 2d   ep-alive ··Cache-
0090  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00a0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr ade-Inse
00b0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00c0  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
```



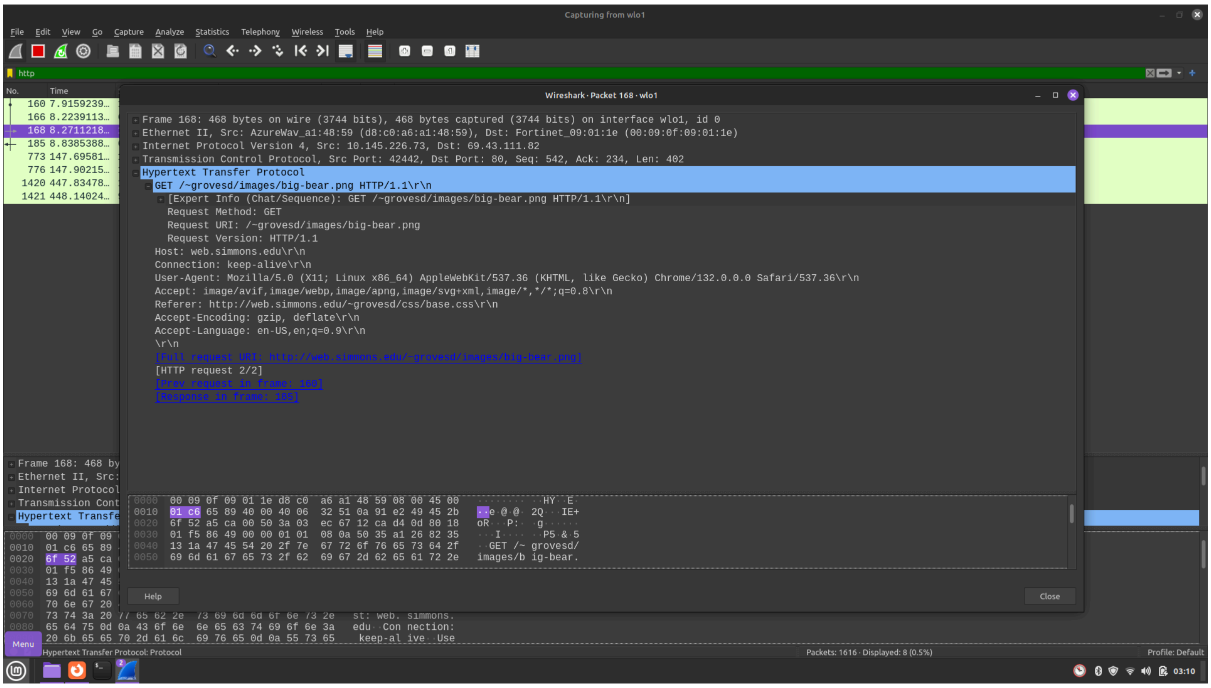
```
 160 7.9159239…
 166 8.2239113…
 168 8.2711218…
 185 8.8385388…
 773 147.69581…
 776 147.90215…
1420 447.83478…
1421 448.14024…
```

```
Frame 166: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits) on interface wlo1, id 0
Ethernet II, Src: Fortinet_09:01:1e (00:09:0f:09:01:1e), Dst: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59)
Internet Protocol Version 4, Src: 69.43.111.82, Dst: 10.145.226.73
Transmission Control Protocol, Src Port: 80, Dst Port: 42442, Seq: 1, Ack: 542, Len: 233
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Fri, 17 Jan 2025 21:31:32 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Tue, 03 Sep 2019 00:33:59 GMT\r\n
  ETag: "7b2-5919b3e8debc0"\r\n
  Accept-Ranges: bytes\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.307987388 seconds]
  [Request in frame: 160]
  [Next request in frame: 168]
  [Next response in frame: 185]
  [Request URI: http://web.simmons.edu/~grovesd/images/big-bear.png]
```

```
0000  d8 c0 a6 a1 48 59 00 09  0f 09 01 1e 08 00 45 20   ····HY·· ······E
0010  01 1d 62 c7 40 00 2b 06  4a 9c 45 2b 6f 52 0a 91   ··b·@·+· J·E+oR··
0020  e2 49 00 50 a5 ca 12 ca  d3 24 3a 03 ec 67 80 18   ·I·P···· ·$:··g··
0030  00 f9 f8 42 00 00 01 01  08 0a 82 35 13 1a 50 35   ···B···· ···5··P5
0040  9f c2 48 54 54 50 2f 31  2e 31 20 33 30 34 20 4e   ··HTTP/1 .1 304 N
0050  6f 74 20 4d 6f 64 69 66  69 65 64 0d 0a 44 61 74   ot Modif ied··Dat
0060  65 3a 20 46 72 69 2c 20  31 37 20 4a 61 6e 20 32   e: Fri,  17 Jan 2
0070  30 32 35 20 32 31 3a 33  31 3a 33 32 20 47 4d 54   025 21:3 1:32 GMT
```

```
0080  0d 0a 53 65 72 76 65 72  3a 20 41 70 61 63 68 65   ··Server : Apache
0090  0d 0a 4c 61 73 74 2d 4d  6f 64 69 66 69 65 64 3a   ··Last-M odified:
```

Hypertext Transfer Protocol: Protocol

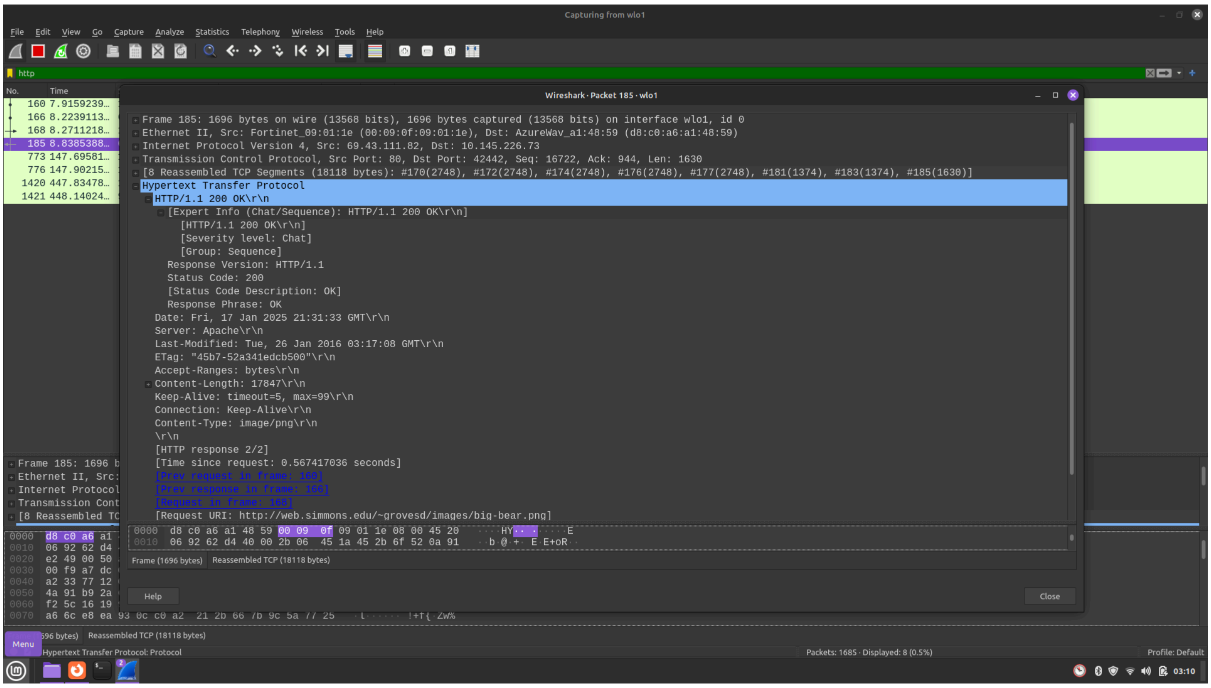

Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 168 · wlo1
Help
Close
Menu
Hypertext Transfer Protocol: Protocol
Packets: 1616 · Displayed: 8 (0.5%)
Profile: Default
03:10

```
No.  Time
 160 7.9159239…
 166 8.2239113…
 168 8.2711218…
 185 8.8385388…
 773 147.69581…
 776 147.90215…
1420 447.83478…
1421 448.14024…
```

```
Frame 168: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface wlo1, id 0
Ethernet II, Src: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59), Dst: Fortinet_09:01:1e (00:09:0f:09:01:1e)
Internet Protocol Version 4, Src: 10.145.226.73, Dst: 69.43.111.82
Transmission Control Protocol, Src Port: 42442, Dst Port: 80, Seq: 542, Ack: 234, Len: 402
Hypertext Transfer Protocol
  GET /~grovesd/images/big-bear.png HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /~grovesd/images/big-bear.png HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /~grovesd/images/big-bear.png
    Request Version: HTTP/1.1
  Host: web.simmons.edu\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36\r\n
  Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
  Referer: http://web.simmons.edu/~grovesd/css/base.css\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://web.simmons.edu/~grovesd/images/big-bear.png]
  [HTTP request 2/2]
  [Prev request in frame: 160]
  [Response in frame: 185]
```

```
0000  00 09 0f 09 01 1e d8 c0  a6 a1 48 59 08 00 45 00   ········ ··HY··E·
0010  01 c6 65 89 40 00 40 06  32 51 0a 91 e2 49 45 2b   ··e·@·@· 2Q···IE+
0020  6f 52 a5 ca 00 50 3a 03  ec 67 12 ca d4 0d 80 18   oR···P:· ·g······
0030  01 f5 86 49 00 00 01 01  08 0a 50 35 a1 26 82 35   ···I···· ··P5·&·5
0040  13 1a 47 45 54 20 2f 7e  67 72 6f 76 65 73 64 2f   ··GET /~ grovesd/
0050  69 6d 61 67 65 73 2f 62  69 67 2d 62 65 61 72 2e   images/b ig-bear.
```

```
0070  73 74 3a 20 77 65 62 2e  73 69 6d 6d 6f 6e 73 2e   st: web. simmons.
0080  65 64 75 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   edu··Con nection:
      20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 55 73 65    keep-al ive··Use
```


Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 185 · wlo1
Frame (1696 bytes)
Reassembled TCP (18118 bytes)
Help
Close
Menu
Hypertext Transfer Protocol: Protocol
Packets: 1685 · Displayed: 8 (0.5%)
Profile: Default
03:10

```
Frame 185: 1696 bytes on wire (13568 bits), 1696 bytes captured (13568 bits) on interface wlo1, id 0
Ethernet II, Src: Fortinet_09:01:1e (00:09:0f:09:01:1e), Dst: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59)
Internet Protocol Version 4, Src: 69.43.111.82, Dst: 10.145.226.73
Transmission Control Protocol, Src Port: 80, Dst Port: 42442, Seq: 16722, Ack: 944, Len: 1630
[8 Reassembled TCP Segments (18118 bytes): #170(2748), #172(2748), #174(2748), #176(2748), #177(2748), #181(1374), #183(1374), #185(1630)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Fri, 17 Jan 2025 21:31:33 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Tue, 26 Jan 2016 03:17:08 GMT\r\n
  ETag: "45b7-52a341edcb500"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 17847\r\n
  Keep-Alive: timeout=5, max=99\r\n
  Connection: Keep-Alive\r\n
  Content-Type: image/png\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.567417036 seconds]
  [Prev request in frame: 160]
  [Prev response in frame: 166]
  [Request in frame: 168]
  [Request URI: http://web.simmons.edu/~grovesd/images/big-bear.png]
```

```
0000  d8 c0 a6 a1 48 59 00 09  0f 09 01 1e 08 00 45 20   ····HY·· ·····E 
0010  06 92 62 d4 40 00 2b 06  45 1a 45 2b 6f 52 0a 91   ··b·@·+· E·E+oR··
```

b) Check the header of the HTTP packet and try to identify the HTTP request and response.

Answer :

In request packet we got

Request method: get

URI: /~grovesd/ ,/connecttest.txt

Request Version: HTTP/1.1

In response packet we got

Response Version: HTTP/1.1

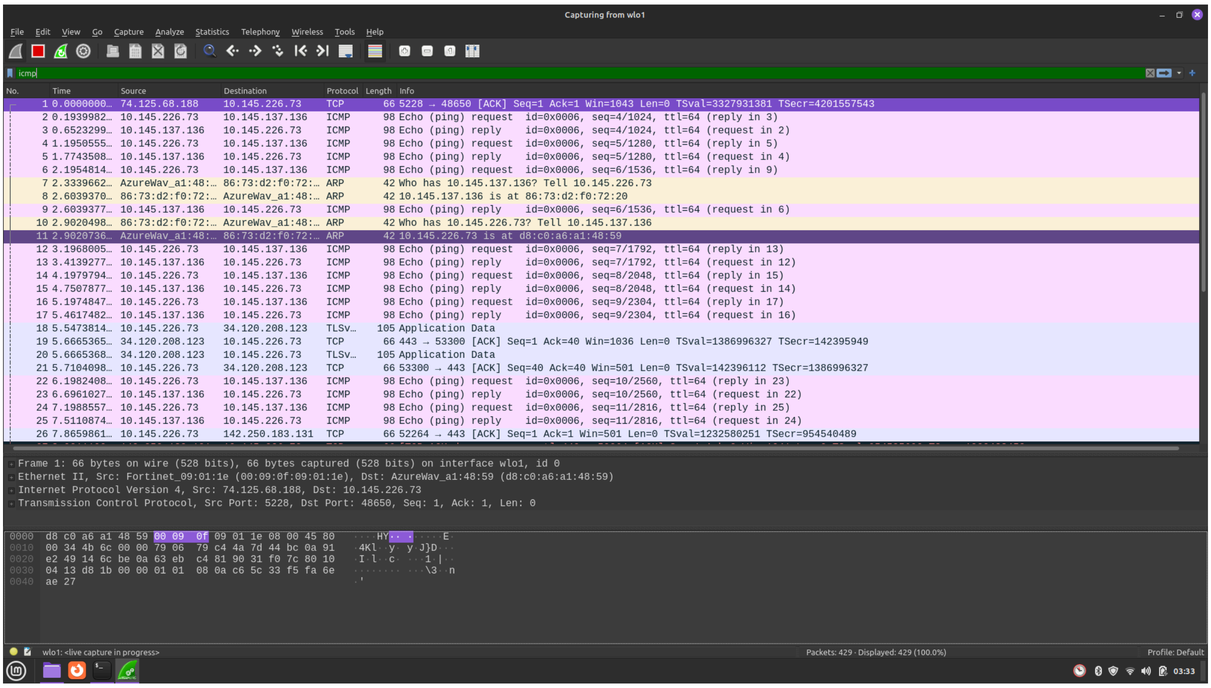
Status Code: 304 , 200

Response Phrase: Not Modified , OK

c) How many HTTP packets are exchanged between client and server to load an entire web page?
Answer: from observation 4 packets exchanged between client and server to load the entire web page.

3. ICMP Traffic (Ping/Traceroute)

a) Run ‘ping’ and ‘traceroute’ commands to initiate ICMP traffic for your friend's machine and capture it through Wireshark. Inspect & crosscheck the Source and Destination IP address of captured ICMP packets.
Answer:
For reachable host(my mobile phone) using ping command



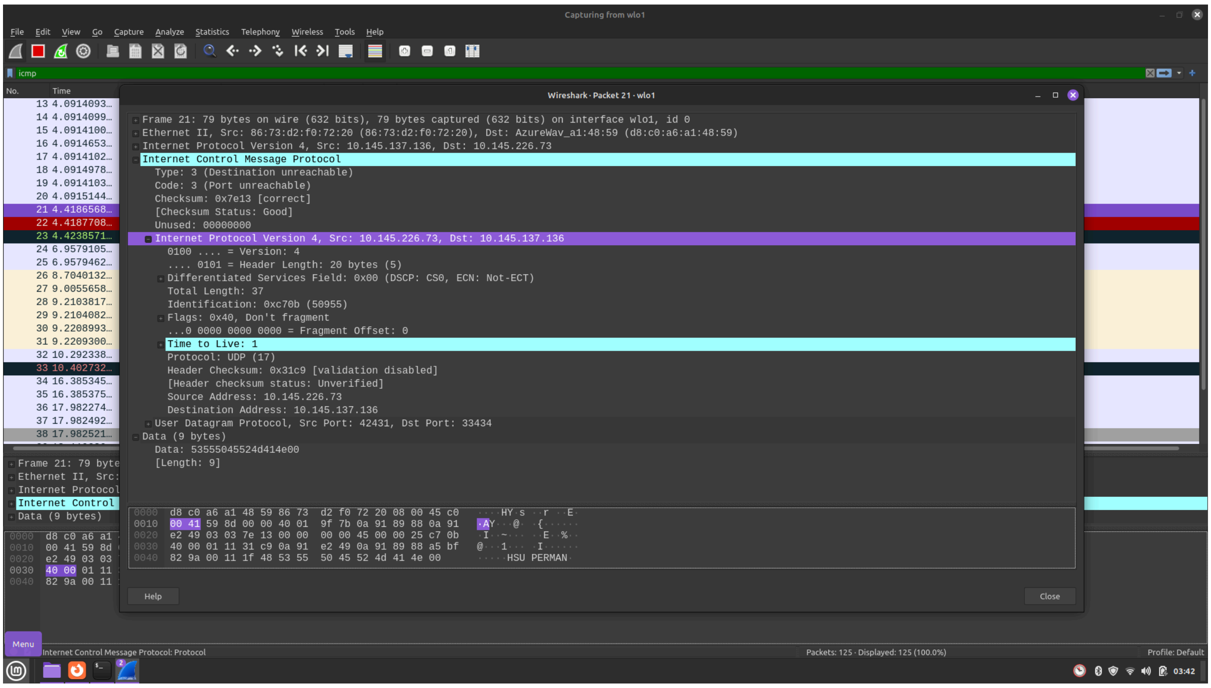
```
No.  Time          Source            Destination       Protocol Length Info
   1 0.0000000…  74.125.68.188     10.145.226.73     TCP       66 5228 → 48650 [ACK] Seq=1 Ack=1 Win=1043 Len=0 TSval=3327931381 TSecr=4201557543
   2 0.1939982…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=4/1024, ttl=64 (reply in 3)
   3 0.6523299…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=4/1024, ttl=64 (request in 2)
   4 1.1950555…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=5/1280, ttl=64 (reply in 5)
   5 1.7743508…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=5/1280, ttl=64 (request in 4)
   6 2.1954814…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=6/1536, ttl=64 (reply in 9)
   7 2.3339662…  AzureWav_a1:48:…  86:73:d2:f0:72:…  ARP       42 Who has 10.145.137.136? Tell 10.145.226.73
   8 2.6039370…  86:73:d2:f0:72:…  AzureWav_a1:48:…  ARP       42 10.145.137.136 is at 86:73:d2:f0:72:20
   9 2.6039377…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=6/1536, ttl=64 (request in 6)
  10 2.9020498…  86:73:d2:f0:72:…  AzureWav_a1:48:…  ARP       42 Who has 10.145.226.73? Tell 10.145.137.136
  11 2.9020736…  AzureWav_a1:48:…  86:73:d2:f0:72:…  ARP       42 10.145.226.73 is at d8:c0:a6:a1:48:59
  12 3.1968005…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=7/1792, ttl=64 (reply in 13)
  13 3.4139277…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=7/1792, ttl=64 (request in 12)
  14 4.1979794…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=8/2048, ttl=64 (reply in 15)
  15 4.7507877…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=8/2048, ttl=64 (request in 14)
  16 5.1974847…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=9/2304, ttl=64 (reply in 17)
  17 5.4617482…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=9/2304, ttl=64 (request in 16)
  18 5.5473814…  10.145.226.73     34.120.208.123    TLSv…    105 Application Data
  19 5.6665365…  34.120.208.123    10.145.226.73     TCP       66 443 → 53300 [ACK] Seq=1 Ack=40 Win=1036 Len=0 TSval=1386996327 TSecr=142395949
  20 5.6665368…  34.120.208.123    10.145.226.73     TLSv…    105 Application Data
  21 5.7104098…  10.145.226.73     34.120.208.123    TCP       66 53300 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=142396112 TSecr=1386996327
  22 6.1982408…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=10/2560, ttl=64 (reply in 23)
  23 6.6961027…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=10/2560, ttl=64 (request in 22)
  24 7.1988557…  10.145.226.73     10.145.137.136    ICMP      98 Echo (ping) request  id=0x0006, seq=11/2816, ttl=64 (reply in 25)
  25 7.5110874…  10.145.137.136    10.145.226.73     ICMP      98 Echo (ping) reply    id=0x0006, seq=11/2816, ttl=64 (request in 24)
  26 7.8659861…  10.145.226.73     142.250.183.131   TCP       66 52264 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1232580251 TSecr=954540489
```

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlo1, id 0
Ethernet II, Src: Fortinet_09:01:1e (00:09:0f:09:01:1e), Dst: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59)
Internet Protocol Version 4, Src: 74.125.68.188, Dst: 10.145.226.73
Transmission Control Protocol, Src Port: 5228, Dst Port: 48650, Seq: 1, Ack: 1, Len: 0
```

```
0000  d8 c0 a6 a1 48 59 00 09  0f 09 01 1e 08 00 45 80   ····HY·· ······E·
0010  00 34 4b 6c 00 00 79 06  79 c4 4a 7d 44 bc 0a 91   ·4Kl··y· y·J}D···
0020  e2 49 14 6c be 0a 63 eb  c4 81 90 31 f0 7c 80 10   ·I·l··c· ···1·|··
0030  04 13 d8 1b 00 00 01 01  08 0a c6 5c 33 f5 fa 6e   ········ ···\3··n
0040  ae 27                                              ·'
```

Observation : each packet of type icmp type 0 for echo reply and type 8 for echo request.

For reachable host(my mobile phone) using traceroute command



Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Wireshark · Packet 21 · wlo1
Help
Close
Menu

```
No.  Time
13 4.0914093…
14 4.0914099…
15 4.0914100…
16 4.0914653…
17 4.0914102…
18 4.0914978…
19 4.0914103…
20 4.0915144…
21 4.4186568…
22 4.4187708…
23 4.4238571…
24 6.9579105…
25 6.9579462…
26 8.7040132…
27 9.0055658…
28 9.2103817…
29 9.2104082…
30 9.2208993…
31 9.2209300…
32 10.292338…
33 10.402732…
34 16.385345…
35 16.385375…
36 17.982274…
37 17.982492…
38 17.982521…
```

```
Frame 21: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface wlo1, id 0
Ethernet II, Src: 86:73:d2:f0:72:20 (86:73:d2:f0:72:20), Dst: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59)
Internet Protocol Version 4, Src: 10.145.137.136, Dst: 10.145.226.73
Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 3 (Port unreachable)
  Checksum: 0x7e13 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  Internet Protocol Version 4, Src: 10.145.226.73, Dst: 10.145.137.136
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 37
    Identification: 0xc70b (50955)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x31c9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.145.226.73
    Destination Address: 10.145.137.136
  User Datagram Protocol, Src Port: 42431, Dst Port: 33434
Data (9 bytes)
  Data: 53555045524d414e00
  [Length: 9]
```

```
0000  d8 c0 a6 a1 48 59 86 73  d2 f0 72 20 08 00 45 c0   ····HY·s ··r ··E·
0010  00 41 59 8d 00 00 40 01  9f 7b 0a 91 89 88 0a 91   ·AY···@· ·{······
0020  e2 49 03 03 7e 13 00 00  00 00 45 00 00 25 c7 0b   ·I··~··· ··E··%··
0030  40 00 01 11 31 c9 0a 91  e2 49 0a 91 89 88 a5 bf   @···1··· ·I······
0040  82 9a 00 11 1f 48 53 55  50 45 52 4d 41 4e 00      ·····HSU PERMAN·
```

```
Frame 21: 79 byte
Ethernet II, Src:
Internet Protocol
Internet Control
Data (9 bytes)
```

```
0000  d8 c0 a6 a1
0010  00 41 59 8d
0020  e2 49 03 03
0030  40 00 01 11
0040  82 9a 00 11
```

Internet Control Message Protocol: Protocol

Packets: 125 · Displayed: 125 (100.0%)

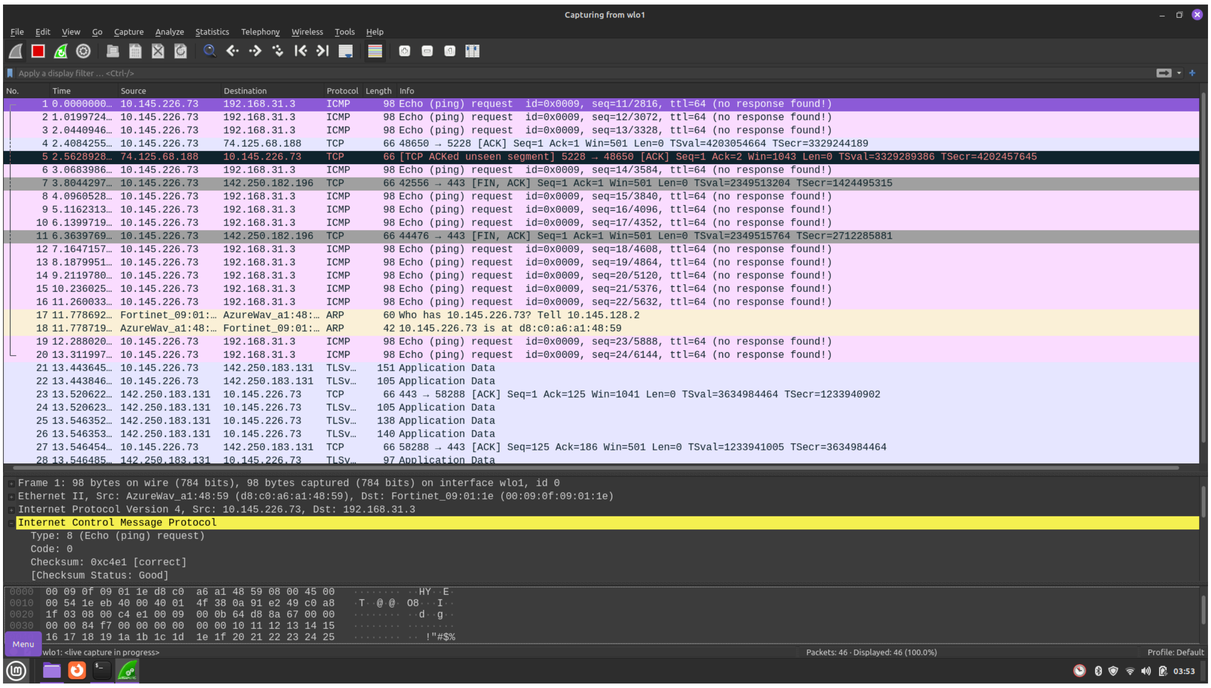
Profile: Default

03:42

The traceroute command sends packets with progressively increasing TTL values. Each hop along the route responds with a "Time-to-Live exceeded" message until the packet either reaches its destination or expires at an intermediate device. Once the destination is reached, it may reply with an ICMP Echo Reply or a Destination Unreachable message.

b) Send a ping to an unreachable host (e.g., a host with IP 192.168.31.3 does not exist in the IIT KGP network) and analyze ICMP no-response packets.

Answer



Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Menu

```
No. Time         Source             Destination        Protocol Length Info
  1 0.0000000…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=11/2816, ttl=64 (no response found!)
  2 1.0199724…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=12/3072, ttl=64 (no response found!)
  3 2.0440946…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=13/3328, ttl=64 (no response found!)
  4 2.4084255…   10.145.226.73      74.125.68.188      TCP       66 48650 → 5228 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=4203054664 TSecr=3329244189
  5 2.5628928…   74.125.68.188      10.145.226.73      TCP       66 [TCP ACKed unseen segment] 5228 → 48650 [ACK] Seq=1 Ack=2 Win=1043 Len=0 TSval=3329289386 TSecr=4202457645
  6 3.0683986…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=14/3584, ttl=64 (no response found!)
  7 3.8044297…   10.145.226.73      142.250.182.196    TCP       66 42556 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2349513204 TSecr=1424495315
  8 4.0960528…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=15/3840, ttl=64 (no response found!)
  9 5.1162313…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=16/4096, ttl=64 (no response found!)
 10 6.1399719…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=17/4352, ttl=64 (no response found!)
 11 6.3639769…   10.145.226.73      142.250.182.196    TCP       66 44476 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2349515764 TSecr=2712285881
 12 7.1647157…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=18/4608, ttl=64 (no response found!)
 13 8.1879951…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=19/4864, ttl=64 (no response found!)
 14 9.2119780…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=20/5120, ttl=64 (no response found!)
 15 10.236025…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=21/5376, ttl=64 (no response found!)
 16 11.260033…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=22/5632, ttl=64 (no response found!)
 17 11.778692…   Fortinet_09:01:…   AzureWav_a1:48:…   ARP       60 Who has 10.145.226.73? Tell 10.145.128.2
 18 11.778719…   AzureWav_a1:48:…   Fortinet_09:01:…   ARP       42 10.145.226.73 is at d8:c0:a6:a1:48:59
 19 12.288020…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=23/5888, ttl=64 (no response found!)
 20 13.311997…   10.145.226.73      192.168.31.3       ICMP      98 Echo (ping) request  id=0x0009, seq=24/6144, ttl=64 (no response found!)
 21 13.443645…   10.145.226.73      142.250.183.131    TLSv…    151 Application Data
 22 13.443846…   10.145.226.73      142.250.183.131    TLSv…    105 Application Data
 23 13.520622…   142.250.183.131    10.145.226.73      TCP       66 443 → 58288 [ACK] Seq=1 Ack=125 Win=1041 Len=0 TSval=3634984464 TSecr=1233940902
 24 13.520623…   142.250.183.131    10.145.226.73      TLSv…    105 Application Data
 25 13.546352…   142.250.183.131    10.145.226.73      TLSv…    138 Application Data
 26 13.546353…   142.250.183.131    10.145.226.73      TLSv…    140 Application Data
 27 13.546454…   10.145.226.73      142.250.183.131    TCP       66 58288 → 443 [ACK] Seq=125 Ack=186 Win=501 Len=0 TSval=1233941005 TSecr=3634984464
 28 13.546485…   142.250.183.131    10.145.226.73      TLSv…     97 Application Data
```

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
Ethernet II, Src: AzureWav_a1:48:59 (d8:c0:a6:a1:48:59), Dst: Fortinet_09:01:1e (00:09:0f:09:01:1e)
Internet Protocol Version 4, Src: 10.145.226.73, Dst: 192.168.31.3
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xc4e1 [correct]
  [Checksum Status: Good]
```

```
0000  00 09 0f 09 01 1e d8 c0  a6 a1 48 59 08 00 45 00   ········ ··HY··E·
0010  00 54 1e eb 40 00 40 01  4f 38 0a 91 e2 49 c0 a8   ·T··@·@· O8···I··
0020  1f 03 08 00 c4 e1 00 09  00 0b 64 d8 8a 67 00 00   ········ ··d··g··
0030  00 00 84 f7 00 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
```

wlo1: <live capture in progress>

Packets: 46 · Displayed: 46 (100.0%)

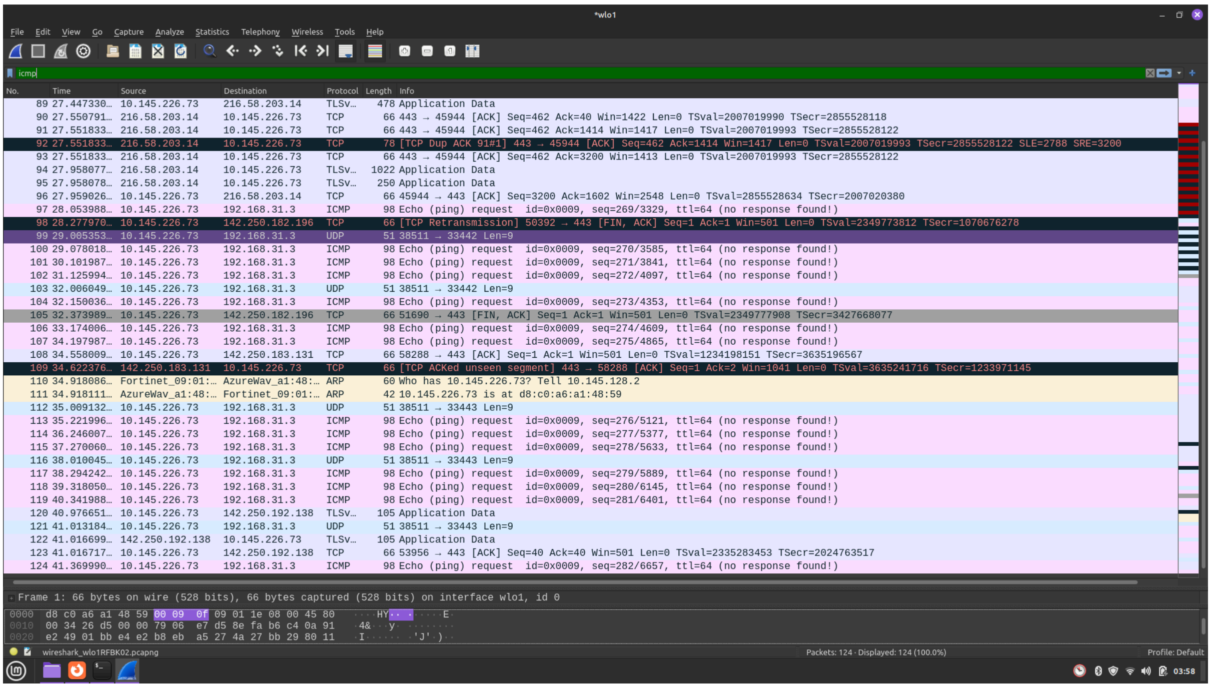
Profile: Default

03:53

In the terminal, it shows 100% packet loss and, in wireshark it shows no response found.

c) Perform a ‘traceroute’ operation for both reachable and unreachable hosts and prepare a brief report of your observation using Wireshark.

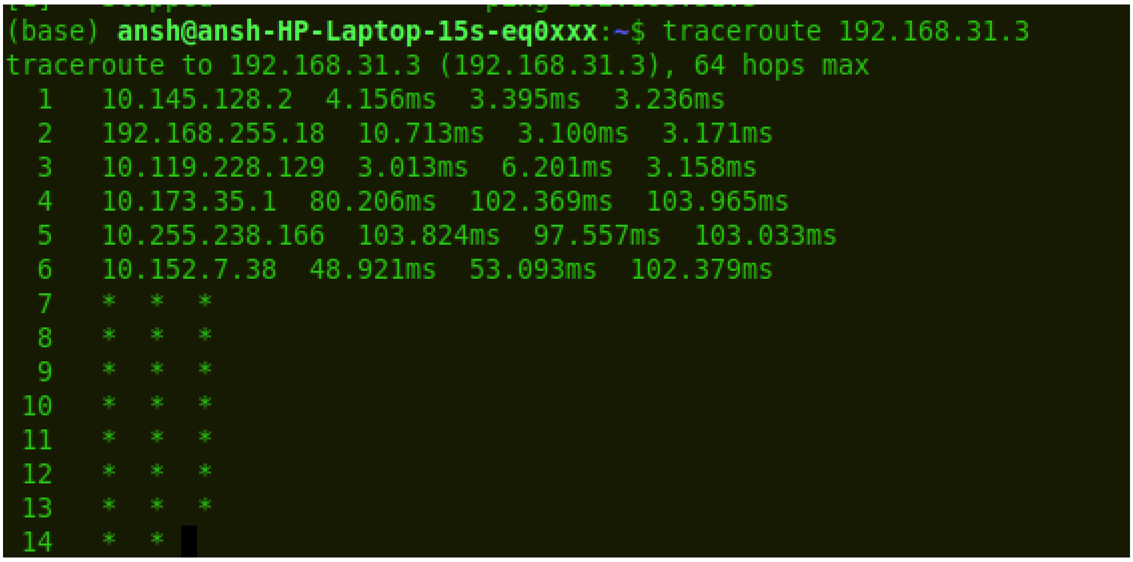
Answer : for unreachable host


*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

```
No.  Time         Source            Destination       Protocol Length Info
 89 27.447330…  10.145.226.73     216.58.203.14     TLSv…    478 Application Data
 90 27.550791…  216.58.203.14     10.145.226.73     TCP       66 443 → 45944 [ACK] Seq=462 Ack=40 Win=1422 Len=0 TSval=2007019990 TSecr=2855528118
 91 27.551833…  216.58.203.14     10.145.226.73     TCP       66 443 → 45944 [ACK] Seq=462 Ack=1414 Win=1417 Len=0 TSval=2007019993 TSecr=2855528122
 92 27.551833…  216.58.203.14     10.145.226.73     TCP       78 [TCP Dup ACK 91#1] 443 → 45944 [ACK] Seq=462 Ack=1414 Win=1417 Len=0 TSval=2007019993 TSecr=2855528122 SLE=2788 SRE=3200
 93 27.551833…  216.58.203.14     10.145.226.73     TCP       66 443 → 45944 [ACK] Seq=462 Ack=3200 Win=1413 Len=0 TSval=2007019993 TSecr=2855528122
 94 27.958077…  216.58.203.14     10.145.226.73     TLSv…   1022 Application Data
 95 27.958078…  216.58.203.14     10.145.226.73     TLSv…    250 Application Data
 96 27.959026…  10.145.226.73     216.58.203.14     TCP       66 45944 → 443 [ACK] Seq=3200 Ack=1602 Win=2548 Len=0 TSval=2855528634 TSecr=2007020380
 97 28.053988…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=269/3329, ttl=64 (no response found!)
 98 28.277970…  10.145.226.73     142.250.182.196   TCP       66 [TCP Retransmission] 50392 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2349773812 TSecr=1070676278
 99 29.005353…  10.145.226.73     192.168.31.3      UDP       51 38511 → 33442 Len=9
100 29.078018…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=270/3585, ttl=64 (no response found!)
101 30.101987…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=271/3841, ttl=64 (no response found!)
102 31.125994…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=272/4097, ttl=64 (no response found!)
103 32.006049…  10.145.226.73     192.168.31.3      UDP       51 38511 → 33442 Len=9
104 32.150036…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=273/4353, ttl=64 (no response found!)
105 32.373989…  10.145.226.73     142.250.182.196   TCP       66 51690 → 443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2349777908 TSecr=3427668077
106 33.174006…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=274/4609, ttl=64 (no response found!)
107 34.197987…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=275/4865, ttl=64 (no response found!)
108 34.558009…  10.145.226.73     142.250.183.131   TCP       66 58288 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1234198151 TSecr=3635196567
109 34.622376…  142.250.183.131   10.145.226.73     TCP       66 [TCP ACKed unseen segment] 443 → 58288 [ACK] Seq=1 Ack=2 Win=1041 Len=0 TSval=3635241716 TSecr=1233971145
110 34.918086…  Fortinet_09:01:…  AzureWav_a1:48:…  ARP       60 Who has 10.145.226.73? Tell 10.145.128.2
111 34.918111…  AzureWav_a1:48:…  Fortinet_09:01:…  ARP       42 10.145.226.73 is at d8:c0:a6:a1:48:59
112 35.009132…  10.145.226.73     192.168.31.3      UDP       51 38511 → 33443 Len=9
113 35.221996…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=276/5121, ttl=64 (no response found!)
114 36.246007…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=277/5377, ttl=64 (no response found!)
115 37.270060…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=278/5633, ttl=64 (no response found!)
116 38.010045…  10.145.226.73     192.168.31.3      UDP       51 38511 → 33443 Len=9
117 38.294242…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=279/5889, ttl=64 (no response found!)
118 39.318050…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=280/6145, ttl=64 (no response found!)
119 40.341988…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=281/6401, ttl=64 (no response found!)
120 40.976651…  10.145.226.73     142.250.192.138   TLSv…    105 Application Data
121 41.013184…  10.145.226.73     192.168.31.3      UDP       51 38511 → 33443 Len=9
122 41.016699…  142.250.192.138   10.145.226.73     TLSv…    105 Application Data
123 41.016717…  10.145.226.73     142.250.192.138   TCP       66 53956 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=2335283453 TSecr=2024763517
124 41.369990…  10.145.226.73     192.168.31.3      ICMP      98 Echo (ping) request  id=0x0009, seq=282/6657, ttl=64 (no response found!)

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlo1, id 0

0000  d8 c0 a6 a1 48 59 00 09  0f 09 01 1e 08 00 45 80   ····HY·· ·····E·
0010  00 34 26 d5 00 00 79 06  e7 d5 8e fa b6 c4 0a 91   ·4&···y· ········
0020  e2 49 01 bb e4 e2 b8 eb  a5 27 4a 27 bb 29 80 11   ·I······ ·'J'·)··
```

wireshark_wlo1RFBK02.pcapng   Packets: 124 · Displayed: 124 (100.0%)   Profile: Default



```
(base) ansh@ansh-HP-Laptop-15s-eq0xxx:~$ traceroute 192.168.31.3
traceroute to 192.168.31.3 (192.168.31.3), 64 hops max
  1   10.145.128.2  4.156ms  3.395ms  3.236ms
  2   192.168.255.18  10.713ms  3.100ms  3.171ms
  3   10.119.228.129  3.013ms  6.201ms  3.158ms
  4   10.173.35.1  80.206ms  102.369ms  103.965ms
  5   10.255.238.166  103.824ms  97.557ms  103.033ms
  6   10.152.7.38  48.921ms  53.093ms  102.379ms
  7   *  *  *
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *
```

In wireshark, no confirmation message is received since the target is not reached and all the packets in between the path die out(ttl expires). In terminal,continuous **** are shown.