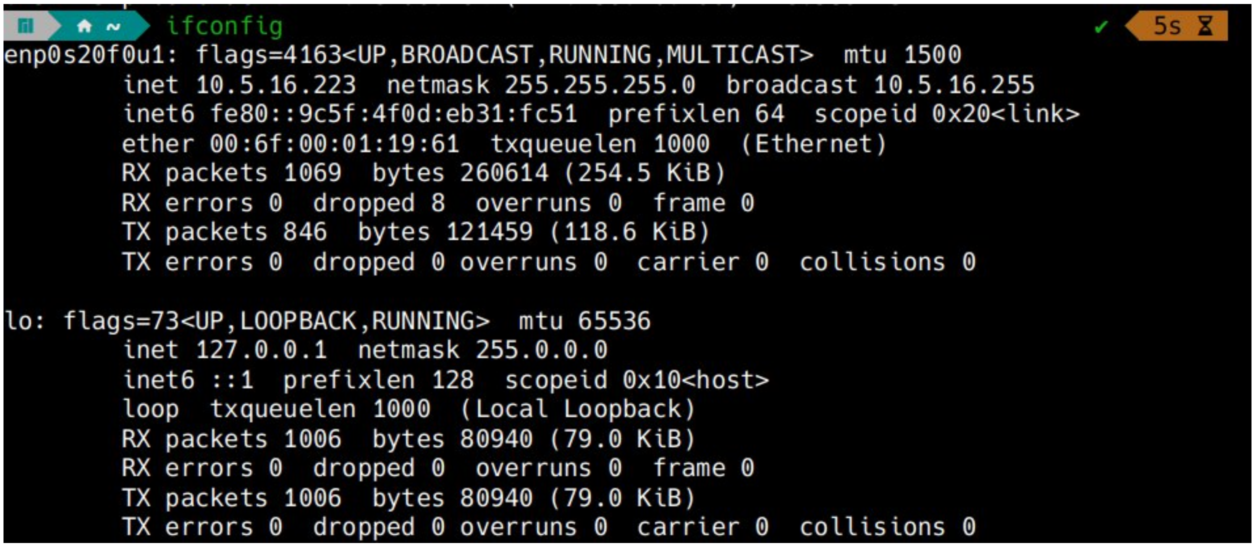
Part 1

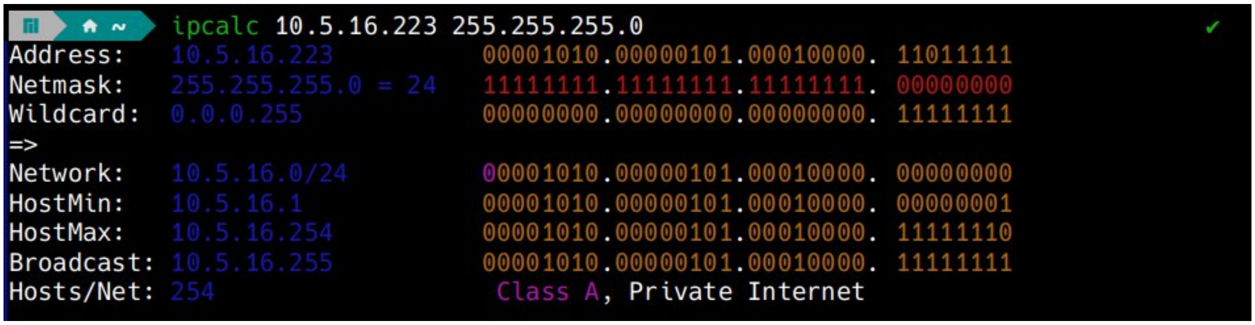
1.



```
ifconfig                                                                     ✔  5s
enp0s20f0u1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.5.16.223  netmask 255.255.255.0  broadcast 10.5.16.255
        inet6 fe80::9c5f:4f0d:eb31:fc51  prefixlen 64  scopeid 0x20<link>
        ether 00:6f:00:01:19:61  txqueuelen 1000  (Ethernet)
        RX packets 1069  bytes 260614 (254.5 KiB)
        RX errors 0  dropped 8  overruns 0  frame 0
        TX packets 846  bytes 121459 (118.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 1006  bytes 80940 (79.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1006  bytes 80940 (79.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

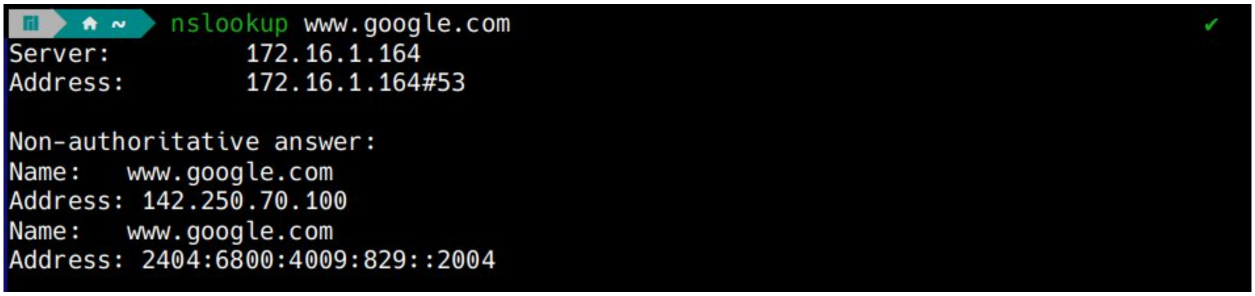
So my IP Address for the Ethernet connection is 10.5.16.223(enp0s20f0u1, the other is for the localhost).

As in the screenshot, the subnet mask is 255.255.255.0.



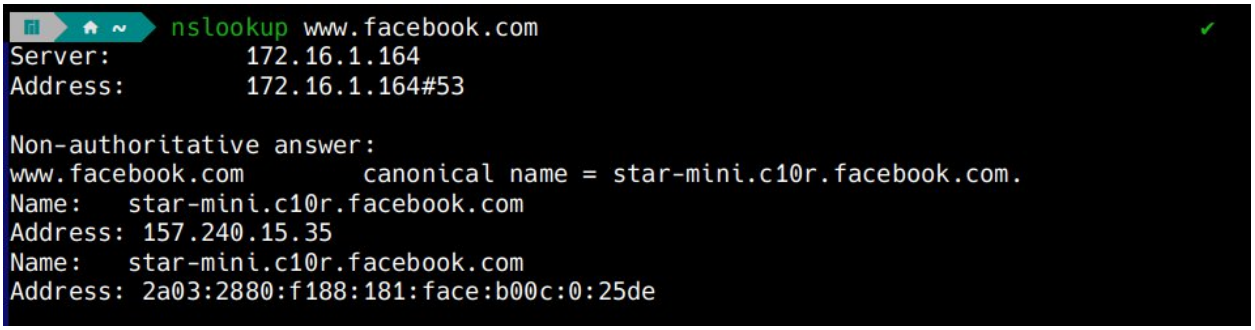
```
ipcalc 10.5.16.223 255.255.255.0                                                   ✔
Address:   10.5.16.223          00001010.00000101.00010000. 11011111
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   10.5.16.0/24         00001010.00000101.00010000. 00000000
HostMin:   10.5.16.1            00001010.00000101.00010000. 00000001
HostMax:   10.5.16.254          00001010.00000101.00010000. 11111110
Broadcast: 10.5.16.255          00001010.00000101.00010000. 11111111
Hosts/Net: 254                   Class A, Private Internet
```

The Network ID is the AND of IP Address and Subnet Mask, we can see it using ipcalc. It is 10.5.16.0/24.



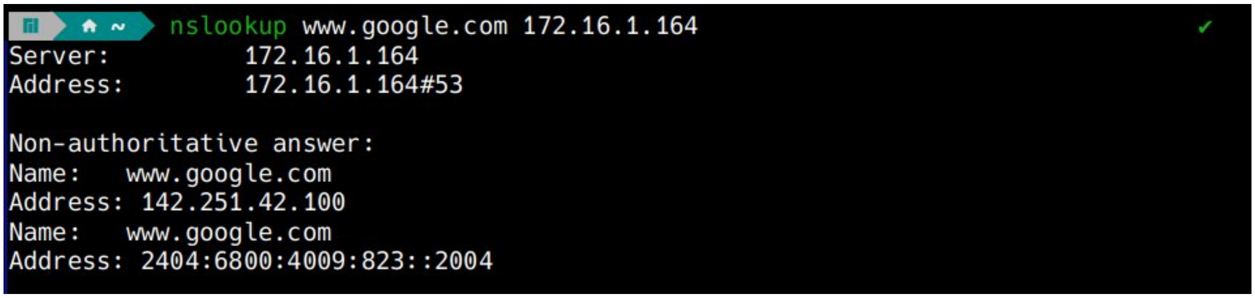
```
nslookup www.google.com                                                            ✔
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.70.100
Name:   www.google.com
Address: 2404:6800:4009:829::2004
```

2. The IP Address associated with www.google.com is 142.250.70.100 (IPv4).

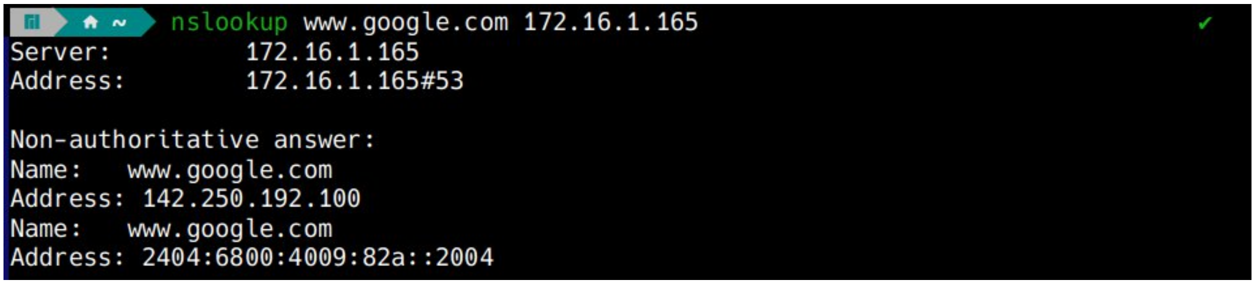


```
nslookup www.facebook.com
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.15.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f188:181:face:b00c:0:25de
```

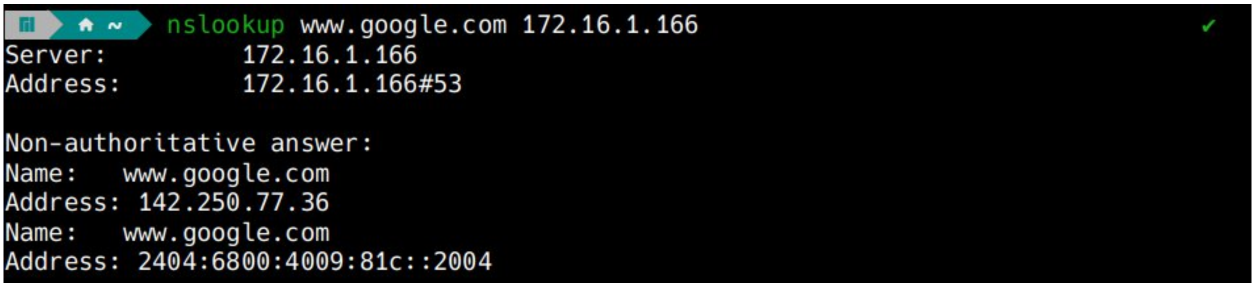
The IP Address associated with www.facebook.com is 157.240.15.35 (IPv4).



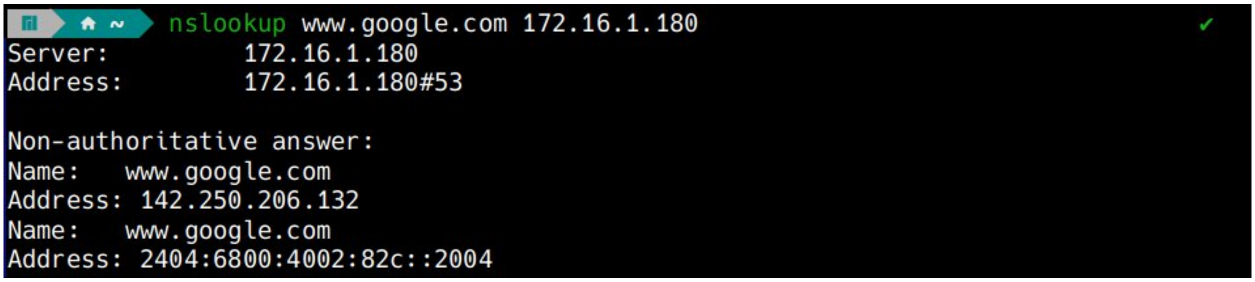
```
nslookup www.google.com 172.16.1.164
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.251.42.100
Name:   www.google.com
Address: 2404:6800:4009:823::2004
```



```
nslookup www.google.com 172.16.1.165
Server:         172.16.1.165
Address:        172.16.1.165#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.100
Name:   www.google.com
Address: 2404:6800:4009:82a::2004
```



```
nslookup www.google.com 172.16.1.166
Server:         172.16.1.166
Address:        172.16.1.166#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.77.36
Name:   www.google.com
Address: 2404:6800:4009:81c::2004
```

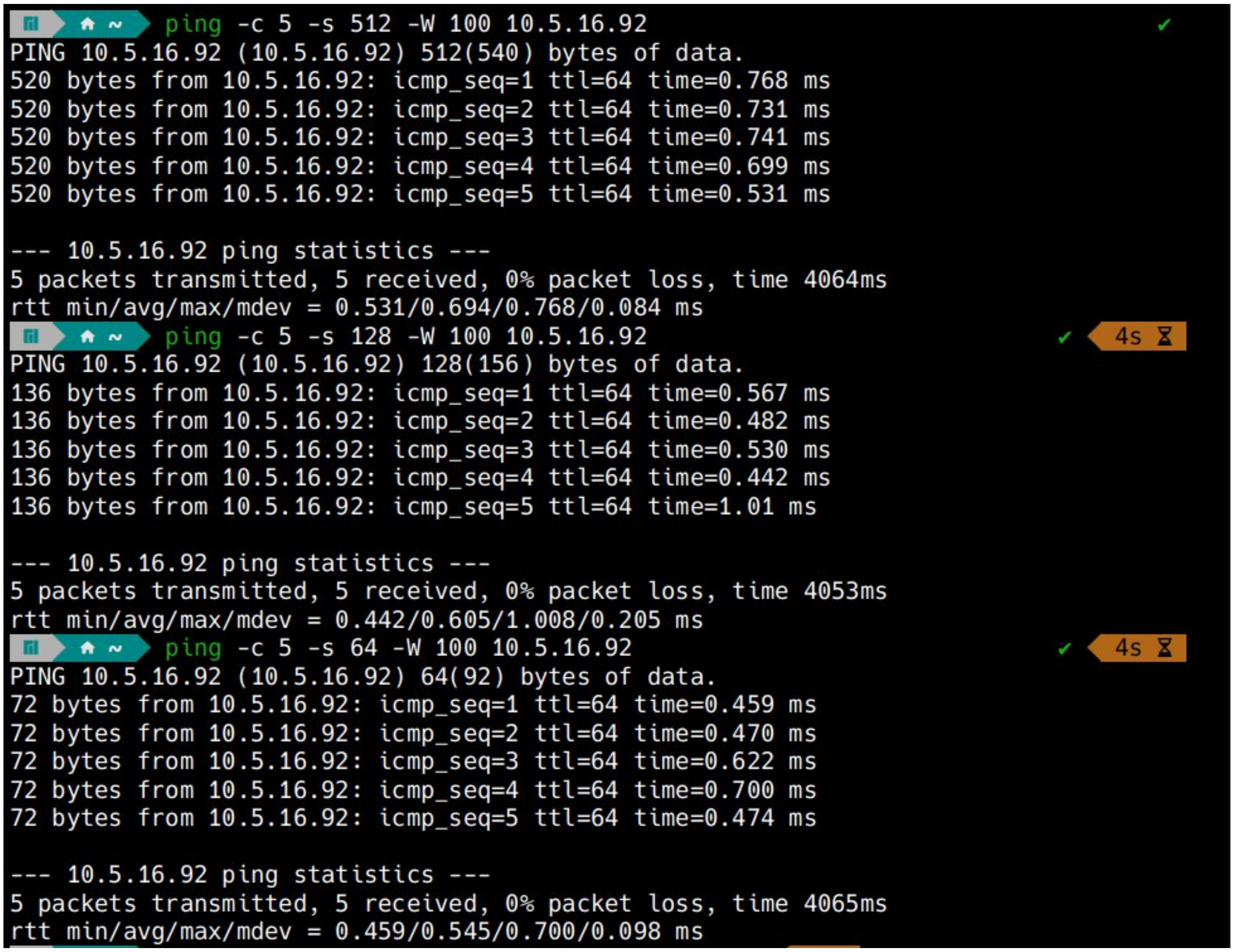


```
nslookup www.google.com 172.16.1.180
Server:         172.16.1.180
Address:        172.16.1.180#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.206.132
Name:   www.google.com
Address: 2404:6800:4002:82c::2004
```

So yes, the IP Address indeed does change.

Google uses DNS Load Balancing to distribute traffic across multiple servers. This distributes the user traffic, reduces latency and provides fault tolerance if one of the servers is accidentally down. The different DNS Servers return different IP Addresses from Google's pool of IP Addresses.

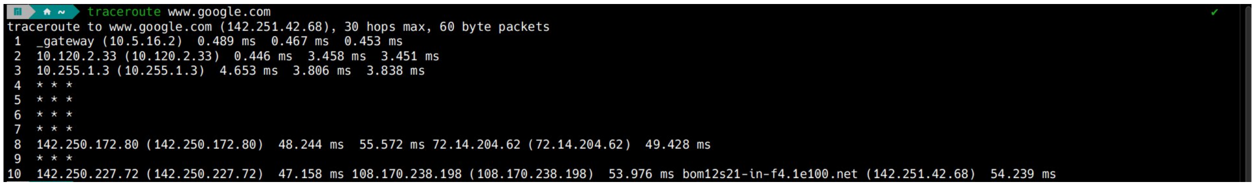
3.



```
 ~ ping -c 5 -s 512 -W 100 10.5.16.92                                              ✔
PING 10.5.16.92 (10.5.16.92) 512(540) bytes of data.
520 bytes from 10.5.16.92: icmp_seq=1 ttl=64 time=0.768 ms
520 bytes from 10.5.16.92: icmp_seq=2 ttl=64 time=0.731 ms
520 bytes from 10.5.16.92: icmp_seq=3 ttl=64 time=0.741 ms
520 bytes from 10.5.16.92: icmp_seq=4 ttl=64 time=0.699 ms
520 bytes from 10.5.16.92: icmp_seq=5 ttl=64 time=0.531 ms

--- 10.5.16.92 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4064ms
rtt min/avg/max/mdev = 0.531/0.694/0.768/0.084 ms
 ~ ping -c 5 -s 128 -W 100 10.5.16.92                                         ✔  4s ⌛
PING 10.5.16.92 (10.5.16.92) 128(156) bytes of data.
136 bytes from 10.5.16.92: icmp_seq=1 ttl=64 time=0.567 ms
136 bytes from 10.5.16.92: icmp_seq=2 ttl=64 time=0.482 ms
136 bytes from 10.5.16.92: icmp_seq=3 ttl=64 time=0.530 ms
136 bytes from 10.5.16.92: icmp_seq=4 ttl=64 time=0.442 ms
136 bytes from 10.5.16.92: icmp_seq=5 ttl=64 time=1.01 ms

--- 10.5.16.92 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4053ms
rtt min/avg/max/mdev = 0.442/0.605/1.008/0.205 ms
 ~ ping -c 5 -s 64 -W 100 10.5.16.92                                          ✔  4s ⌛
PING 10.5.16.92 (10.5.16.92) 64(92) bytes of data.
72 bytes from 10.5.16.92: icmp_seq=1 ttl=64 time=0.459 ms
72 bytes from 10.5.16.92: icmp_seq=2 ttl=64 time=0.470 ms
72 bytes from 10.5.16.92: icmp_seq=3 ttl=64 time=0.622 ms
72 bytes from 10.5.16.92: icmp_seq=4 ttl=64 time=0.700 ms
72 bytes from 10.5.16.92: icmp_seq=5 ttl=64 time=0.474 ms

--- 10.5.16.92 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4065ms
rtt min/avg/max/mdev = 0.459/0.545/0.700/0.098 ms
```

Above is the result of pinging my friends IP Address with different packet sizes of 64, 128, 512 bytes and timeout 100. The terminal output shows the packet loss percentage, min, avg, max, and mdev/stddev of round-trip time.

4.



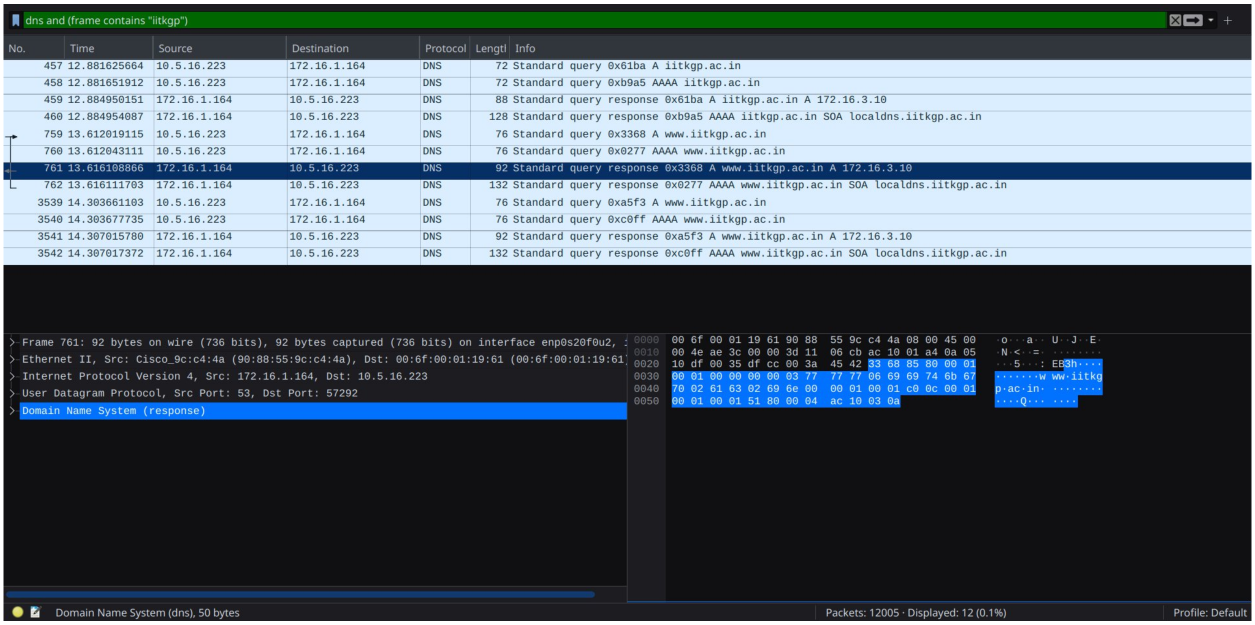
```
 ~ traceroute www.google.com                                                        ✔
traceroute to www.google.com (142.251.42.68), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.489 ms  0.467 ms  0.453 ms
 2  10.120.2.33 (10.120.2.33)  0.446 ms  3.458 ms  3.451 ms
 3  10.255.1.3 (10.255.1.3)  4.653 ms  3.806 ms  3.838 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  142.250.172.80 (142.250.172.80)  48.244 ms  55.572 ms 72.14.204.62 (72.14.204.62)  49.428 ms
 9  * * *
10  142.250.227.72 (142.250.227.72)  47.158 ms 108.170.238.198 (108.170.238.198)  53.976 ms bom12s21-in-f4.1e100.net (142.251.42.68)  54.239 ms
```

Above is the report of running traceroute for www.google.com. There are 10 lines, so 10 hosts.

The “* * *” basically means that the hop did not respond, which can be due to various reasons like Firewall blocking ICMP, router not responding, packet loss etc

Part 2

1.



dns and (frame contains "iitkgp")

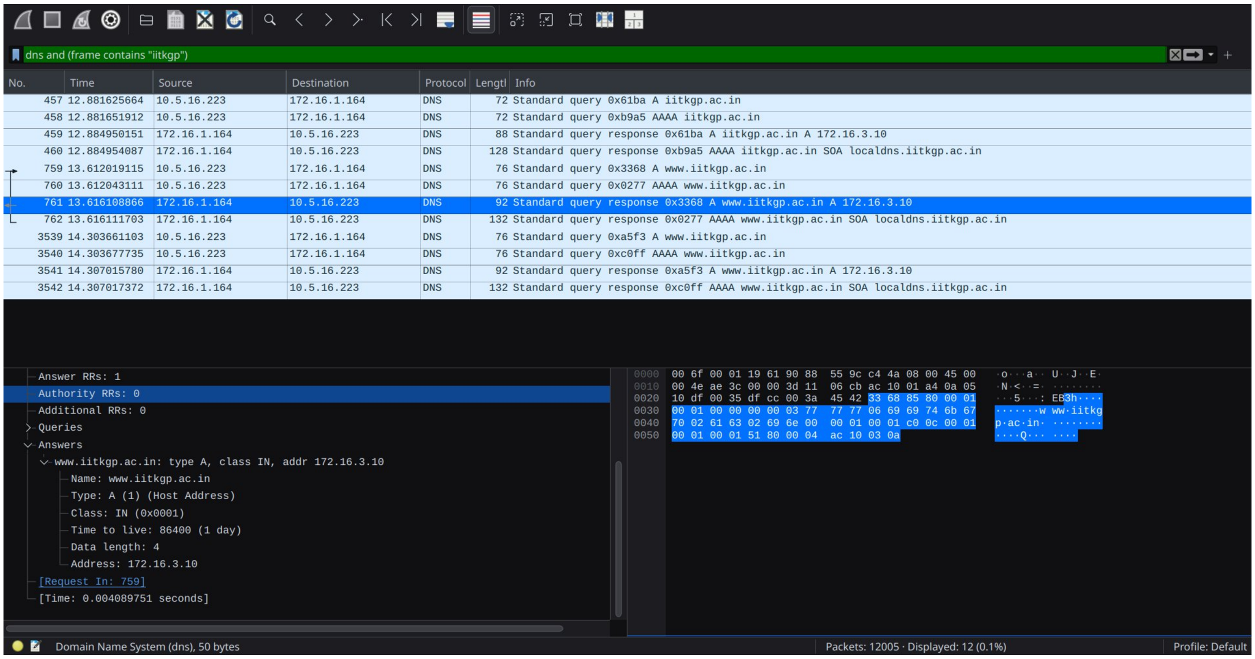
No.	Time	Source	Destination	Protocol	Lengtl	Info
457	12.881625664	10.5.16.223	172.16.1.164	DNS	72	Standard query 0x61ba A iitkgp.ac.in
458	12.881651912	10.5.16.223	172.16.1.164	DNS	72	Standard query 0xb9a5 AAAA iitkgp.ac.in
459	12.884950151	172.16.1.164	10.5.16.223	DNS	88	Standard query response 0x61ba A iitkgp.ac.in A 172.16.3.10
460	12.884954087	172.16.1.164	10.5.16.223	DNS	128	Standard query response 0xb9a5 AAAA iitkgp.ac.in SOA localdns.iitkgp.ac.in
759	13.612019115	10.5.16.223	172.16.1.164	DNS	76	Standard query 0x3368 A www.iitkgp.ac.in
760	13.612043111	10.5.16.223	172.16.1.164	DNS	76	Standard query 0x0277 AAAA www.iitkgp.ac.in
761	13.616108866	172.16.1.164	10.5.16.223	DNS	92	Standard query response 0x3368 A www.iitkgp.ac.in A 172.16.3.10
762	13.616111703	172.16.1.164	10.5.16.223	DNS	132	Standard query response 0x0277 AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in
3539	14.303661103	10.5.16.223	172.16.1.164	DNS	76	Standard query 0xa5f3 A www.iitkgp.ac.in
3540	14.303677735	10.5.16.223	172.16.1.164	DNS	76	Standard query 0xc0ff AAAA www.iitkgp.ac.in
3541	14.307015780	172.16.1.164	10.5.16.223	DNS	92	Standard query response 0xa5f3 A www.iitkgp.ac.in A 172.16.3.10
3542	14.307017372	172.16.1.164	10.5.16.223	DNS	132	Standard query response 0xc0ff AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in

```
> Frame 761: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface enp0s20f0u2, i
> Ethernet II, Src: Cisco_9c:c4:4a (90:88:55:9c:c4:4a), Dst: 00:6f:00:01:19:61 (00:6f:00:01:19:61)
> Internet Protocol Version 4, Src: 172.16.1.164, Dst: 10.5.16.223
> User Datagram Protocol, Src Port: 53, Dst Port: 57292
> Domain Name System (response)
```

```
0000  00 6f 00 01 19 61 90 88  55 9c c4 4a 08 00 45 00   ·o···a·· U··J··E·
0010  00 4e ae 3c 00 00 3d 11  06 cb ac 10 01 a4 0a 05   ·N·<··=· ········
0020  10 df 00 35 df cc 00 3a  45 42 33 68 85 80 00 01   ···5···: EB3h····
0030  00 01 00 00 00 00 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 c0 0c 00 01   p·ac·in· ········
0050  00 01 00 01 51 80 00 04  ac 10 03 0a               ····Q··· ····
```

Domain Name System (dns), 50 bytes | Packets: 12005 · Displayed: 12 (0.1%) | Profile: Default

a) From the screenshot, we can see that DNS is using UDP in the observed packets.



dns and (frame contains "iitkgp")

No.	Time	Source	Destination	Protocol	Lengtl	Info
457	12.881625664	10.5.16.223	172.16.1.164	DNS	72	Standard query 0x61ba A iitkgp.ac.in
458	12.881651912	10.5.16.223	172.16.1.164	DNS	72	Standard query 0xb9a5 AAAA iitkgp.ac.in
459	12.884950151	172.16.1.164	10.5.16.223	DNS	88	Standard query response 0x61ba A iitkgp.ac.in A 172.16.3.10
460	12.884954087	172.16.1.164	10.5.16.223	DNS	128	Standard query response 0xb9a5 AAAA iitkgp.ac.in SOA localdns.iitkgp.ac.in
759	13.612019115	10.5.16.223	172.16.1.164	DNS	76	Standard query 0x3368 A www.iitkgp.ac.in
760	13.612043111	10.5.16.223	172.16.1.164	DNS	76	Standard query 0x0277 AAAA www.iitkgp.ac.in
761	13.616108866	172.16.1.164	10.5.16.223	DNS	92	Standard query response 0x3368 A www.iitkgp.ac.in A 172.16.3.10
762	13.616111703	172.16.1.164	10.5.16.223	DNS	132	Standard query response 0x0277 AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in
3539	14.303661103	10.5.16.223	172.16.1.164	DNS	76	Standard query 0xa5f3 A www.iitkgp.ac.in
3540	14.303677735	10.5.16.223	172.16.1.164	DNS	76	Standard query 0xc0ff AAAA www.iitkgp.ac.in
3541	14.307015780	172.16.1.164	10.5.16.223	DNS	92	Standard query response 0xa5f3 A www.iitkgp.ac.in A 172.16.3.10
3542	14.307017372	172.16.1.164	10.5.16.223	DNS	132	Standard query response 0xc0ff AAAA www.iitkgp.ac.in SOA localdns.iitkgp.ac.in

```
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
> Queries
v Answers
  v www.iitkgp.ac.in: type A, class IN, addr 172.16.3.10
      Name: www.iitkgp.ac.in
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 86400 (1 day)
      Data length: 4
      Address: 172.16.3.10
  [Request In: 759]
  [Time: 0.004089751 seconds]
```

```
0000  00 6f 00 01 19 61 90 88  55 9c c4 4a 08 00 45 00   ·o···a·· U··J··E·
0010  00 4e ae 3c 00 00 3d 11  06 cb ac 10 01 a4 0a 05   ·N·<··=· ········
0020  10 df 00 35 df cc 00 3a  45 42 33 68 85 80 00 01   ···5···: EB3h····
0030  00 01 00 00 00 00 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 c0 0c 00 01   p·ac·in· ········
0050  00 01 00 01 51 80 00 04  ac 10 03 0a               ····Q··· ····
```

Domain Name System (dns), 50 bytes | Packets: 12005 · Displayed: 12 (0.1%) | Profile: Default

b) The source IP Address of the DNS Query is 10.5.16.223.

The destination IP Address of the DNS Query is 172.16.1.164.

c) As we see in the screenshot, 6 queries are sent from the machine to DNS server during name-to-IP resolution.

d) The DNS Server 172.16.1.164 replies with actual IP Addresses.

e) Only one DNS server is involved, and it does respond.

f) From the screenshot,

Name : iitkgp.ac.in

Type : A (1) (Host Address)

Class : IN (0x0001)

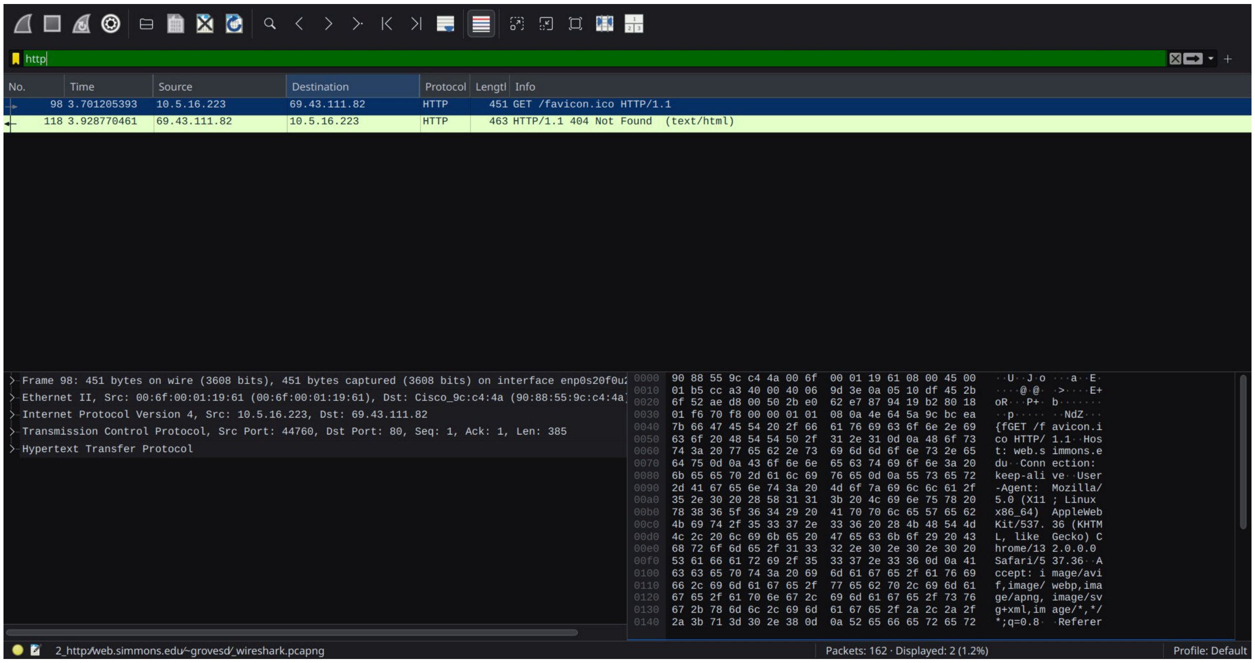
TTL : 86400 (1 day)

Resolved IP Address : 172.16.3.10

Data length : 4

2.

a)



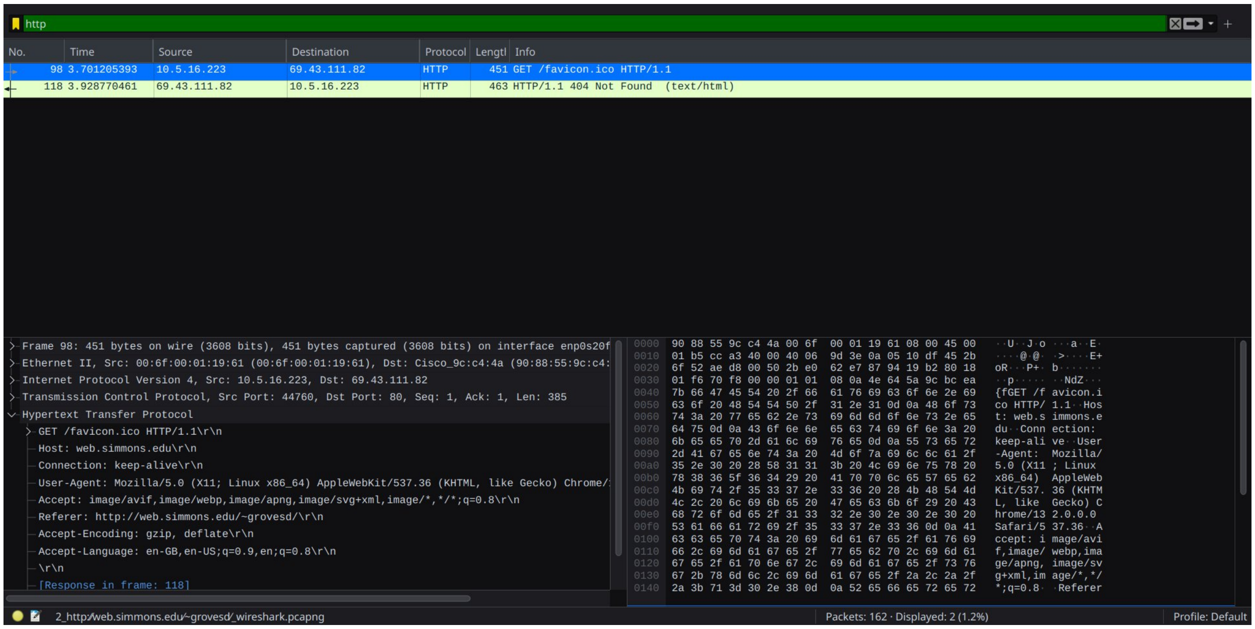
```
No.   Time         Source        Destination   Protocol Lengtl Info
   98 3.701205393  10.5.16.223   69.43.111.82  HTTP        451 GET /favicon.ico HTTP/1.1
  118 3.928770461  69.43.111.82  10.5.16.223   HTTP        463 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 98: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface enp0s20f0u2
> Ethernet II, Src: 00:6f:00:01:19:61 (00:6f:00:01:19:61), Dst: Cisco_9c:c4:4a (90:88:55:9c:c4:4a)
> Internet Protocol Version 4, Src: 10.5.16.223, Dst: 69.43.111.82
> Transmission Control Protocol, Src Port: 44760, Dst Port: 80, Seq: 1, Ack: 1, Len: 385
> Hypertext Transfer Protocol
```

```
0000  90 88 55 9c c4 4a 00 6f  00 01 19 61 08 00 45 00   ··U··J·o ···a··E·
0010  01 b5 cc a3 40 00 40 06  9d 3e 0a 05 10 df 45 2b   ····@·@· ·>····E+
0020  6f 52 ae d8 00 50 2b e0  62 e7 87 94 19 b2 80 18   oR···P+· b·······
0030  01 f6 70 f8 00 00 01 01  08 0a 4e 64 5a 9c bc ea   ··p····· ··NdZ···
0040  7b 66 47 45 54 20 2f 66  61 76 69 63 6f 6e 2e 69   {fGET /f avicon.i
0050  63 6f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   co HTTP/ 1.1··Hos
0060  74 3a 20 77 65 62 2e 73  69 6d 6d 6f 6e 73 2e 65   t: web.s immons.e
0070  64 75 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   du··Conn ection: 
0080  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 73 65 72   keep-ali ve··User
0090  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00a0  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e 75 78 20   5.0 (X11 ; Linux 
00b0  78 38 36 5f 36 34 29 20  41 70 70 6c 65 57 65 62   x86_64)  AppleWeb
00c0  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
00d0  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
00e0  68 72 6f 6d 65 2f 31 33  32 2e 30 2e 30 2e 30 20   hrome/13 2.0.0.0 
00f0  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0100  63 63 65 70 74 3a 20 69  6d 61 67 65 2f 61 76 69   ccept: i mage/avi
0110  66 2c 69 6d 61 67 65 2f  77 65 62 70 2c 69 6d 61   f,image/ webp,ima
0120  67 65 2f 61 70 6e 67 2c  69 6d 61 67 65 2f 73 76   ge/apng, image/sv
0130  67 2b 78 6d 6c 2c 69 6d  61 67 65 2f 2a 2c 2a 2f   g+xml,im age/*,*/
0140  2a 3b 71 3d 30 2e 38 0d  0a 52 65 66 65 72 65 72   *;q=0.8· ·Referer
```

2_http:/web.simmons.edu/~grovesd/_wireshark.pcapng | Packets: 162 · Displayed: 2 (1.2%) | Profile: Default

Above is a screenshot of the result after initiating web traffic for the web server http://web.simmons.edu/~grovesd/ and filtering for http in Wireshark.



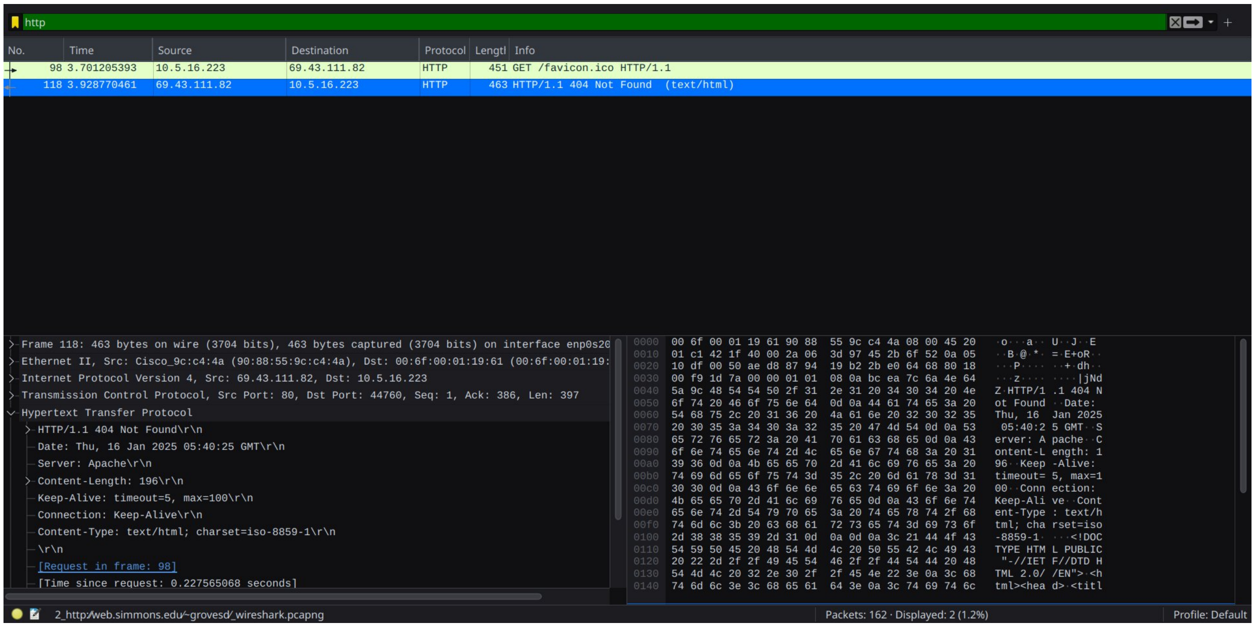
```
http

No.   Time         Source        Destination   Protocol Length Info
   98 3.701205393  10.5.16.223   69.43.111.82  HTTP      451 GET /favicon.ico HTTP/1.1
  118 3.928770461  69.43.111.82  10.5.16.223   HTTP      463 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 98: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface enp0s20f
> Ethernet II, Src: 00:6f:00:01:19:61 (00:6f:00:01:19:61), Dst: Cisco_9c:c4:4a (90:88:55:9c:c4:
> Internet Protocol Version 4, Src: 10.5.16.223, Dst: 69.43.111.82
> Transmission Control Protocol, Src Port: 44760, Dst Port: 80, Seq: 1, Ack: 1, Len: 385
v Hypertext Transfer Protocol
  > GET /favicon.ico HTTP/1.1\r\n
    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/
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://web.simmons.edu/~grovesd/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Response in frame: 118]
```

```
0000  90 88 55 9c c4 4a 00 6f  00 01 19 61 08 00 45 00   ··U··J·o ···a··E·
0010  01 b5 cc a3 40 00 40 06  9d 3e 0a 05 10 df 45 2b   ····@·@· ·>····E+
0020  6f 52 ae d8 00 50 2b e0  62 e7 87 94 19 b2 80 18   oR···P+· b·······
0030  01 f6 70 f8 00 00 01 01  08 0a 4e 64 5a 9c bc ea   ··p····· ··NdZ···
0040  7b 66 47 45 54 20 2f 66  61 76 69 63 6f 6e 2e 69   {fGET /f avicon.i
0050  63 6f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   co HTTP/ 1.1··Hos
0060  74 3a 20 77 65 62 2e 73  69 6d 6d 6f 6e 73 2e 65   t: web.s immons.e
0070  64 75 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   du··Conn ection: 
0080  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 73 65 72   keep-ali ve··User
0090  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00a0  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e 75 78 20   5.0 (X11 ; Linux 
00b0  78 38 36 5f 36 34 29 20  41 70 70 6c 65 57 65 62   x86_64)  AppleWeb
00c0  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
00d0  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
00e0  68 72 6f 6d 65 2f 31 33  32 2e 30 2e 30 2e 30 20   hrome/13 2.0.0.0 
00f0  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0100  63 63 65 70 74 3a 20 69  6d 61 67 65 2f 61 76 69   ccept: i mage/avi
0110  66 2c 69 6d 61 67 65 2f  77 65 62 70 2c 69 6d 61   f,image/ webp,ima
0120  67 65 2f 61 70 6e 67 2c  69 6d 61 67 65 2f 73 76   ge/apng, image/sv
0130  67 2b 78 6d 6c 2c 69 6d  61 67 65 2f 2a 2c 2a 2f   g+xml,im age/*,*/
0140  2a 3b 71 3d 30 2e 38 0d  0a 52 65 66 65 72 65 72   *;q=0.8· ·Referer
```

2_http:/web.simmons.edu/~grovesd/_wireshark.pcapng · Packets: 162 · Displayed: 2 (1.2%) · Profile: Default

b) This is a screenshot of the above window, with the http request.



```
http

No.   Time         Source        Destination   Protocol Length Info
   98 3.701205393  10.5.16.223   69.43.111.82  HTTP      451 GET /favicon.ico HTTP/1.1
  118 3.928770461  69.43.111.82  10.5.16.223   HTTP      463 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 118: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface enp0s20
> Ethernet II, Src: Cisco_9c:c4:4a (90:88:55:9c:c4:4a), Dst: 00:6f:00:01:19:61 (00:6f:00:01:19:
> Internet Protocol Version 4, Src: 69.43.111.82, Dst: 10.5.16.223
> Transmission Control Protocol, Src Port: 80, Dst Port: 44760, Seq: 1, Ack: 386, Len: 397
v Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Thu, 16 Jan 2025 05:40:25 GMT\r\n
    Server: Apache\r\n
  > Content-Length: 196\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [Request in frame: 98]
    [Time since request: 0.227565068 seconds]
```

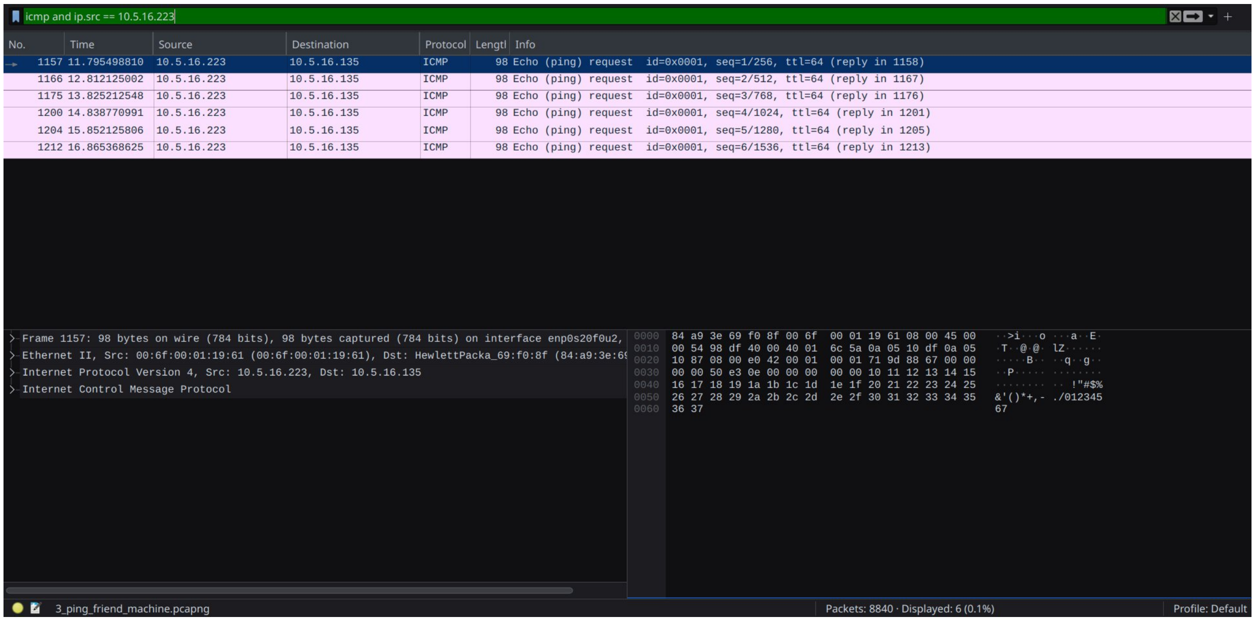
```
0000  00 6f 00 01 19 61 90 88  55 9c c4 4a 08 00 45 20   ·o···a·· U··J··E 
0010  01 c1 42 1f 40 00 2a 06  3d 97 45 2b 6f 52 0a 05   ··B·@·*· =·E+oR··
0020  10 df 00 50 ae d8 87 94  19 b2 2b e0 64 68 80 18   ···P···· ··+·dh··
0030  00 f9 1d 7a 00 00 01 01  08 0a bc ea 7c 6a 4e 64   ···z···· ····|jNd
0040  5a 9c 48 54 54 50 2f 31  2e 31 20 34 30 34 20 4e   Z·HTTP/1 .1 404 N
0050  6f 74 20 46 6f 75 6e 64  0d 0a 44 61 74 65 3a 20   ot Found ··Date: 
0060  54 68 75 2c 20 31 36 20  4a 61 6e 20 32 30 32 35   Thu, 16  Jan 2025
0070  20 30 35 3a 34 30 3a 32  35 20 47 4d 54 0d 0a 53    05:40:2 5 GMT··S
0080  65 72 76 65 72 3a 20 41  70 61 63 68 65 0d 0a 43   erver: A pache··C
0090  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 31   ontent-L ength: 1
00a0  39 36 0d 0a 4b 65 65 70  2d 41 6c 69 76 65 3a 20   96··Keep -Alive: 
00b0  74 69 6d 65 6f 75 74 3d  35 2c 20 6d 61 78 3d 31   timeout= 5, max=1
00c0  30 30 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   00··Conn ection: 
00d0  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 43 6f 6e 74   Keep-Ali ve··Cont
00e0  65 6e 74 2d 54 79 70 65  3a 20 74 65 78 74 2f 68   ent-Type : text/h
00f0  74 6d 6c 3b 20 63 68 61  72 73 65 74 3d 69 73 6f   tml; cha rset=iso
0100  2d 38 38 35 39 2d 31 0d  0a 0d 0a 3c 21 44 4f 43   -8859-1· ···<!DOC
0110  54 59 50 45 20 48 54 4d  4c 20 50 55 42 4c 49 43   TYPE HTM L PUBLIC
0120  20 22 2d 2f 2f 49 45 54  46 2f 2f 44 54 44 20 48    "-//IET F//DTD H
0130  54 4d 4c 20 32 2e 30 2f  2f 45 4e 22 3e 0a 3c 68   TML 2.0/ /EN">·<h
0140  74 6d 6c 3e 3c 68 65 61  64 3e 0a 3c 74 69 74 6c   tml><hea d>·<titl
```

2_http:/web.simmons.edu/~grovesd/_wireshark.pcapng · Packets: 162 · Displayed: 2 (1.2%) · Profile: Default

This is a screenshot of the above window, capturing the http response.

c) As we can see, 2 http packets have been exchange between the client and the server.

3.



```
icmp and ip.src == 10.5.16.223
```

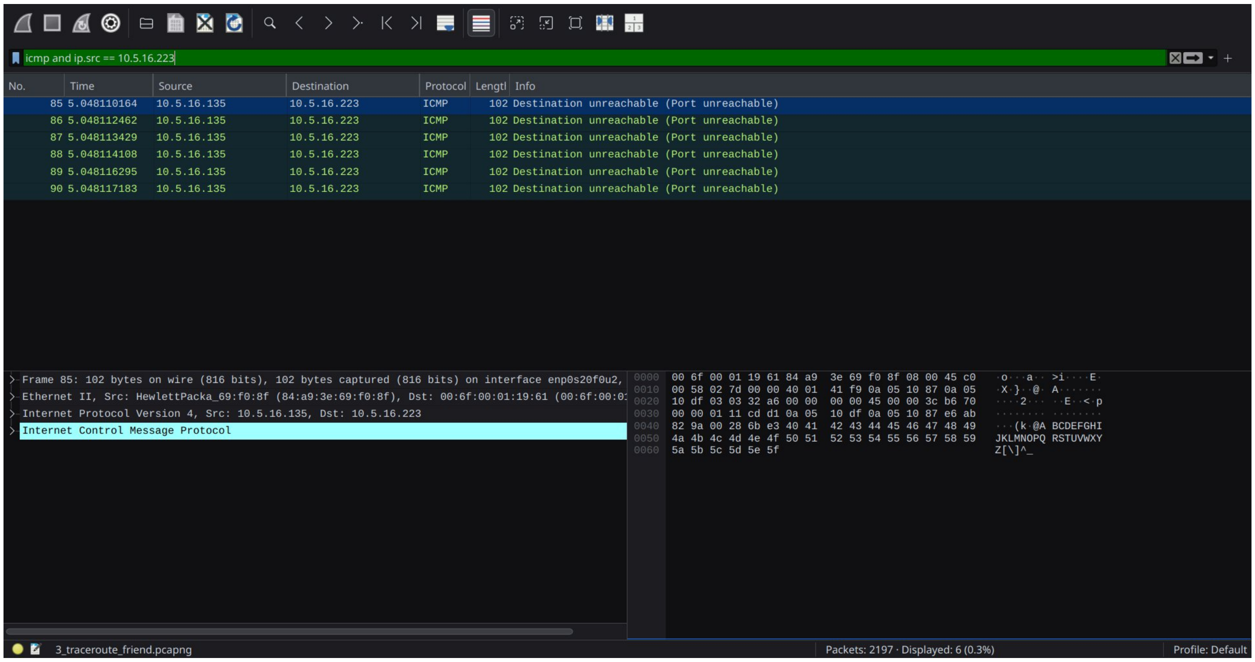
```
No.   Time          Source         Destination    Protocol Lengtl Info
 1157 11.795498810  10.5.16.223    10.5.16.135    ICMP       98 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (reply in 1158)
 1166 12.812125002  10.5.16.223    10.5.16.135    ICMP       98 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (reply in 1167)
 1175 13.825212548  10.5.16.223    10.5.16.135    ICMP       98 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (reply in 1176)
 1200 14.838770991  10.5.16.223    10.5.16.135    ICMP       98 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (reply in 1201)
 1204 15.852125806  10.5.16.223    10.5.16.135    ICMP       98 Echo (ping) request  id=0x0001, seq=5/1280, ttl=64 (reply in 1205)
 1212 16.865368625  10.5.16.223    10.5.16.135    ICMP       98 Echo (ping) request  id=0x0001, seq=6/1536, ttl=64 (reply in 1213)
```

```
> Frame 1157: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s20f0u2,
> Ethernet II, Src: 00:6f:00:01:19:61 (00:6f:00:01:19:61), Dst: HewlettPacka_69:f0:8f (84:a9:3e:69
> Internet Protocol Version 4, Src: 10.5.16.223, Dst: 10.5.16.135
> Internet Control Message Protocol
```

```
0000  84 a9 3e 69 f0 8f 00 6f  00 01 19 61 08 00 45 00   ··>i···o ···a··E·
0010  00 54 98 df 40 00 40 01  6c 5a 0a 05 10 df 0a 05   ·T··@·@· lZ······
0020  10 87 08 00 e0 42 00 01  00 01 71 9d 88 67 00 00   ·····B·· ··q··g··
0030  00 00 50 e3 0e 00 00 00  00 00 10 11 12 13 14 15   ··P····· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

```
3_ping_friend_machine.pcapng          Packets: 8840 · Displayed: 6 (0.1%)          Profile: Default
```

a) Above is a result of running ping command to generate ICMP traffic for my friends machine(10.5.16.135) and capturing it in Wireshark.



```
icmp and ip.src == 10.5.16.223
```

```
No.   Time          Source         Destination    Protocol Lengtl Info
   85 5.048110164   10.5.16.135    10.5.16.223    ICMP      102 Destination unreachable (Port unreachable)
   86 5.048112462   10.5.16.135    10.5.16.223    ICMP      102 Destination unreachable (Port unreachable)
   87 5.048113429   10.5.16.135    10.5.16.223    ICMP      102 Destination unreachable (Port unreachable)
   88 5.048114108   10.5.16.135    10.5.16.223    ICMP      102 Destination unreachable (Port unreachable)
   89 5.048116295   10.5.16.135    10.5.16.223    ICMP      102 Destination unreachable (Port unreachable)
   90 5.048117183   10.5.16.135    10.5.16.223    ICMP      102 Destination unreachable (Port unreachable)
```

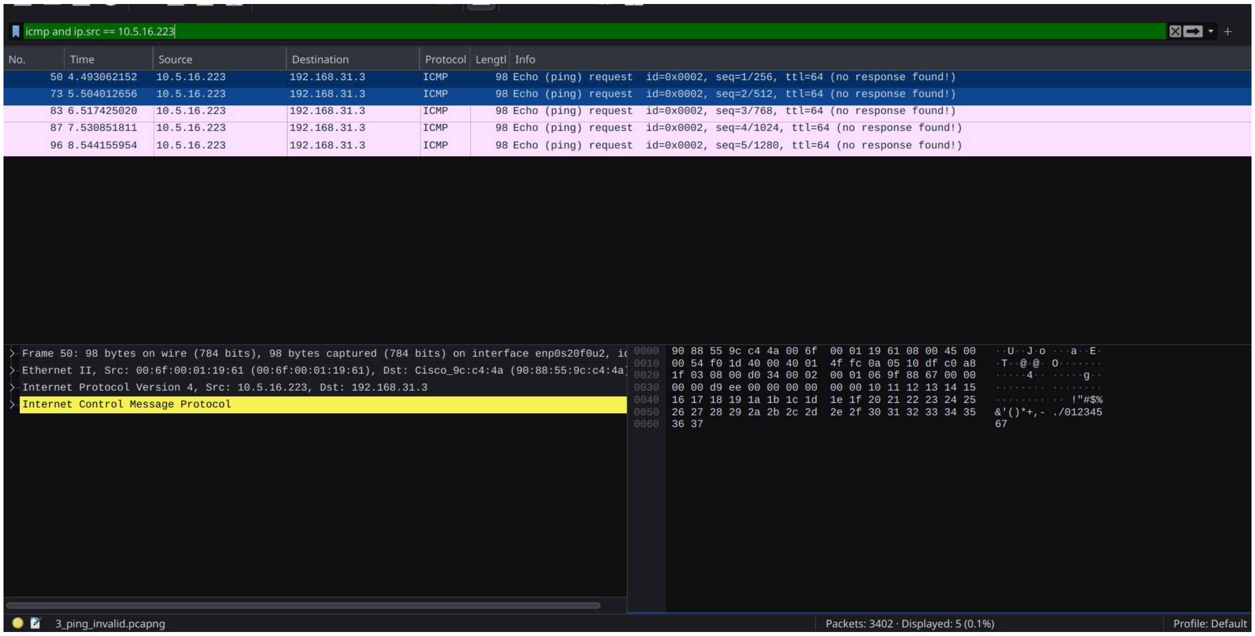
```
> Frame 85: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enp0s20f0u2,
> Ethernet II, Src: HewlettPacka_69:f0:8f (84:a9:3e:69:f0:8f), Dst: 00:6f:00:01:19:61 (00:6f:00:01
> Internet Protocol Version 4, Src: 10.5.16.135, Dst: 10.5.16.223
> Internet Control Message Protocol
```

```
0000  00 6f 00 01 19 61 84 a9  3e 69 f0 8f 08 00 45 c0   ·o···a·· >i····E·
0010  00 58 02 7d 00 00 40 01  41 f9 0a 05 10 87 0a 05   ·X·}··@· A·······
0020  10 df 03 03 32 a6 00 00  00 00 45 00 00 3c b6 70   ····2··· ··E··<·p
0030  00 00 01 11 cd d1 0a 05  10 df 0a 05 10 87 e6 ab   ········ ········
0040  82 9a 00 28 6b e3 40 41  42 43 44 45 46 47 48 49   ···(k·@A BCDEFGHI
0050  4a 4b 4c 4d 4e 4f 50 51  52 53 54 55 56 57 58 59   JKLMNOPQ RSTUVWXY
0060  5a 5b 5c 5d 5e 5f                                  Z[\]^_
```

```
3_traceroute_friend.pcapng          Packets: 2197 · Displayed: 6 (0.3%)          Profile: Default
```

Above is a result of running traceroute command to generate ICMP traffic for my friends machine(10.5.16.135) and capturing it in Wireshark.I don’t kow the correct reason behind the “port unreachable” messages, but it seems to me that the Institute network uses NAT, which translates the internal IP addresses into a single external IP address.This is probably interfering with the normal operation of traceroute and leading to these messages.

b)



```
icmp and ip.src == 10.5.16.223

No.   Time          Source         Destination    Protocol Lengtl Info
   50 4.493062152   10.5.16.223    192.168.31.3   ICMP      98 Echo (ping) request  id=0x0002, seq=1/256, ttl=64 (no response found!)
   73 5.504012656   10.5.16.223    192.168.31.3   ICMP      98 Echo (ping) request  id=0x0002, seq=2/512, ttl=64 (no response found!)
   83 6.517425020   10.5.16.223    192.168.31.3   ICMP      98 Echo (ping) request  id=0x0002, seq=3/768, ttl=64 (no response found!)
   87 7.530851811   10.5.16.223    192.168.31.3   ICMP      98 Echo (ping) request  id=0x0002, seq=4/1024, ttl=64 (no response found!)
   96 8.544155954   10.5.16.223    192.168.31.3   ICMP      98 Echo (ping) request  id=0x0002, seq=5/1280, ttl=64 (no response found!)
```

```
> Frame 50: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s20f0u2, ic
> Ethernet II, Src: 00:6f:00:01:19:61 (00:6f:00:01:19:61), Dst: Cisco_9c:c4:4a (90:88:55:9c:c4:4a)
> Internet Protocol Version 4, Src: 10.5.16.223, Dst: 192.168.31.3
> Internet Control Message Protocol
```

```
0000  90 88 55 9c c4 4a 00 6f  00 01 19 61 08 00 45 00   ··U··J·o ···a··E·
0010  00 54 f0 1d 40 00 40 01  4f fc 0a 05 10 df c0 a8   ·T··@·@· O·······
0020  1f 03 08 00 d0 34 00 02  00 01 06 9f 88 67 00 00   ·····4·· ·····g··
0030  00 00 d9 ee 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   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

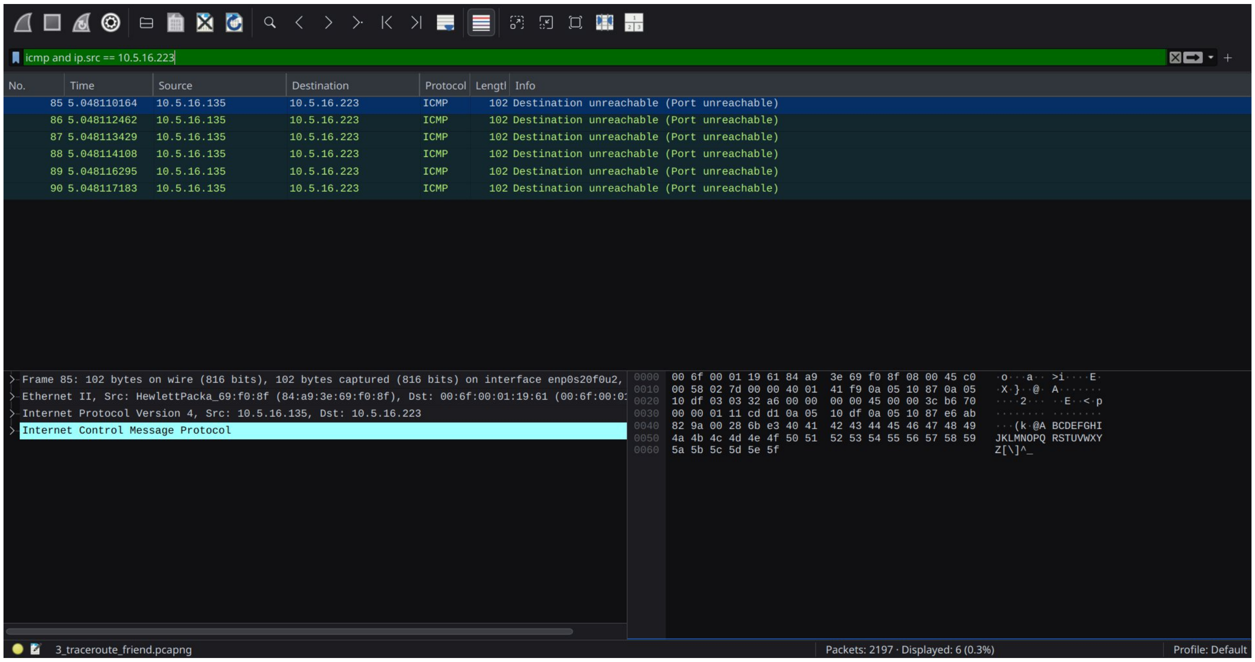
3_ping_invalid.pcapng

Packets: 3402 · Displayed: 5 (0.1%)

Profile: Default

Above is the result of sending a ping to 192.168.31.3 and capturing the network traffic in Wireshark.When a ping (ICMP Echo Request) is sent to a host that is unreachable , there will be no ICMP Echo Reply. Wireshark will capture the outgoing ICMP Echo Request, but there won't be a corresponding ICMP Echo Reply. That’s why we can see in the brackets - “no response found”.

c)



icmp and ip.src == 10.5.16.223

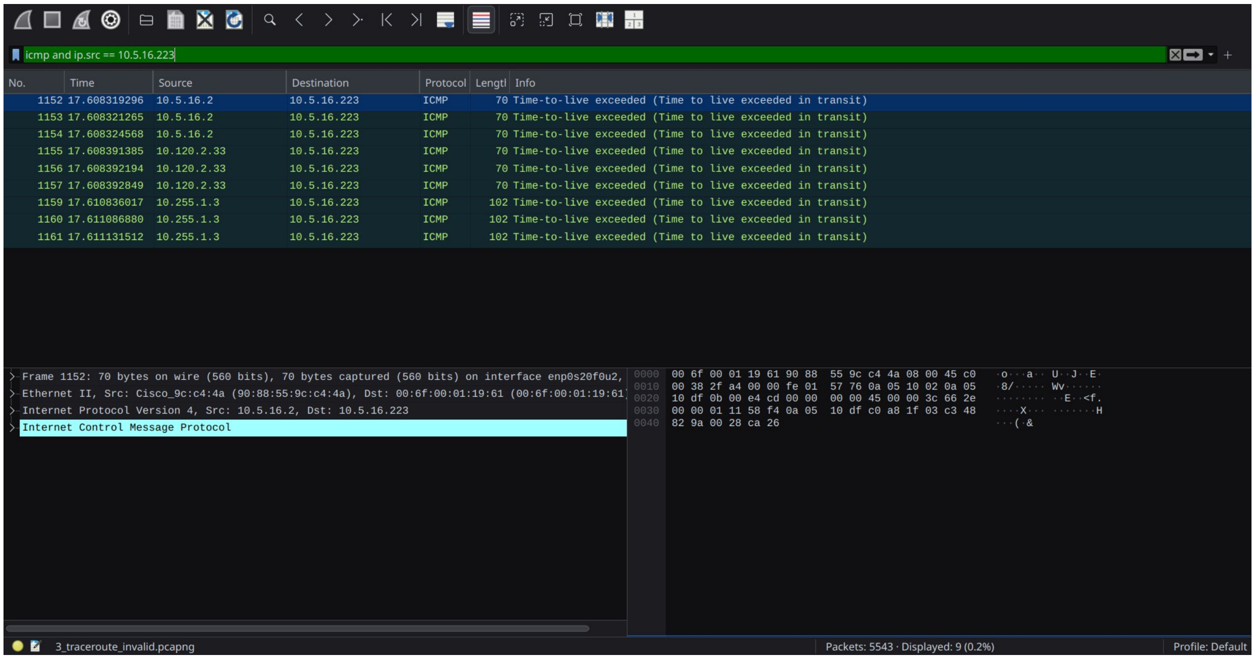
```
No.   Time          Source        Destination   Protocol Lengtl Info
   85 5.048110164   10.5.16.135   10.5.16.223   ICMP     102 Destination unreachable (Port unreachable)
   86 5.048112462   10.5.16.135   10.5.16.223   ICMP     102 Destination unreachable (Port unreachable)
   87 5.048113429   10.5.16.135   10.5.16.223   ICMP     102 Destination unreachable (Port unreachable)
   88 5.048114108   10.5.16.135   10.5.16.223   ICMP     102 Destination unreachable (Port unreachable)
   89 5.048116295   10.5.16.135   10.5.16.223   ICMP     102 Destination unreachable (Port unreachable)
   90 5.048117183   10.5.16.135   10.5.16.223   ICMP     102 Destination unreachable (Port unreachable)
```

```
> Frame 85: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enp0s20f0u2,
> Ethernet II, Src: HewlettPacka_69:f0:8f (84:a9:3e:69:f0:8f), Dst: 00:6f:00:01:19:61 (00:6f:00:0
> Internet Protocol Version 4, Src: 10.5.16.135, Dst: 10.5.16.223
> Internet Control Message Protocol
```

```
0000  00 6f 00 01 19 61 84 a9  3e 69 f0 8f 08 00 45 c0   ·o···a·· >i····E·
0010  00 58 02 7d 00 00 40 01  41 f9 0a 05 10 87 0a 05   ·X·}··@· A·······
0020  10 df 03 03 32 a6 00 00  00 00 45 00 00 3c b6 70   ····2··· ··E··<·p
0030  00 00 01 11 cd d1 0a 05  10 df 0a 05 10 87 e6 ab   ········ ········
0040  82 9a 00 28 6b e3 40 41  42 43 44 45 46 47 48 49   ···(k·@A BCDEFGHI
0050  4a 4b 4c 4d 4e 4f 50 51  52 53 54 55 56 57 58 59   JKLMNOPQ RSTUVWXY
0060  5a 5b 5c 5d 5e 5f                                  Z[\]^_
```

3_traceroute_friend.pcapng   Packets: 2197 · Displayed: 6 (0.3%)   Profile: Default

Above is the result of running traceroute for my friend’s machine(reachable host).



icmp and ip.src == 10.5.16.223

```
No.   Time           Source        Destination   Protocol Lengtl Info
 1152 17.608319296   10.5.16.2     10.5.16.223   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 1153 17.608321265   10.5.16.2     10.5.16.223   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 1154 17.608324568   10.5.16.2     10.5.16.223   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 1155 17.608391385   10.120.2.33   10.5.16.223   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 1156 17.608392194   10.120.2.33   10.5.16.223   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 1157 17.608392849   10.120.2.33   10.5.16.223   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 1159 17.610836017   10.255.1.3    10.5.16.223   ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 1160 17.611086880   10.255.1.3    10.5.16.223   ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
 1161 17.611131512   10.255.1.3    10.5.16.223   ICMP     102 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 1152: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface enp0s20f0u2,
> Ethernet II, Src: Cisco_9c:c4:4a (90:88:55:9c:c4:4a), Dst: 00:6f:00:01:19:61 (00:6f:00:01:19:61)
> Internet Protocol Version 4, Src: 10.5.16.2, Dst: 10.5.16.223
> Internet Control Message Protocol
```

```
0000  00 6f 00 01 19 61 90 88  55 9c c4 4a 08 00 45 c0   ·o···a·· U··J··E·
0010  00 38 2f a4 00 00 fe 01  57 76 0a 05 10 02 0a 05   ·8/····· Wv······
0020  10 df 0b 00 e4 cd 00 00  00 00 45 00 00 3c 66 2e   ········ ··E··<f.
0030  00 00 01 11 58 f4 0a 05  10 df c0 a8 1f 03 c3 48   ····X··· ·······H
0040  82 9a 00 28 ca 26                                  ···(·&
```

3_traceroute_invalid.pcapng   Packets: 5543 · Displayed: 9 (0.2%)   Profile: Default

Above is the result of running traceroute for `192.168.31.3`, an unreachable host.

When we run a traceroute to an unreachable host, the packets are sent out with increasing TTL values. Each router along the way decrements the TTL until it reaches zero. If the host is unreachable, the packets never reach their destination. Instead, an intermediate router will eventually send back an ICMP "time to live exceeded in transit" message, indicating that the packet was discarded because the TTL expired. This is the reason behind the “Time to live exceeded in transit” messages.