COMPUTER NETWORKS

Lab Assignment 1

Karan Kumar Sethi, 22CS30034

Part 1: Networking Tools

1. IP address of my machine: 10.5.16.65 (computer used in Software lab)

   Subnet Mask: 255.255.255.0

   Network ID: 10.5.16.0 (By taking bitwise and operation)

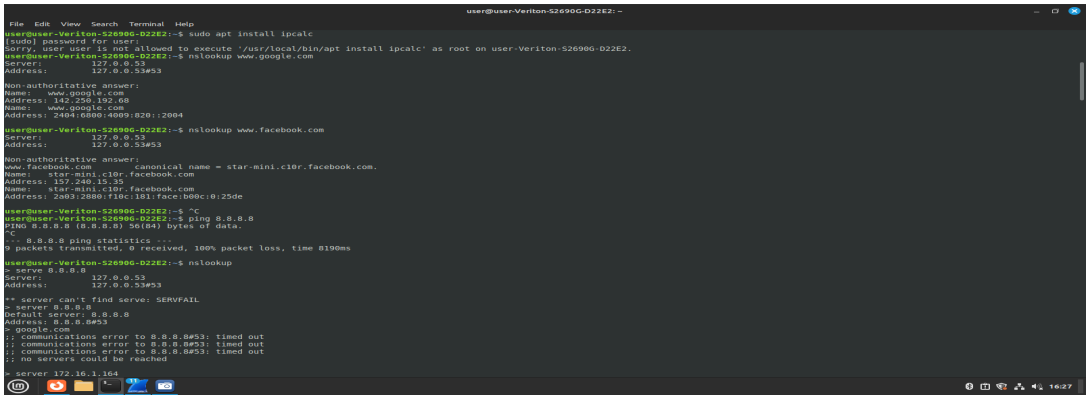
   Command used: ifconfig (in ubuntu)

   ipconfig (in powershell)

2. By using nslookup command, the address found

   For google.com: 142.250.192.68

   For facebook.com: 157.240.15.35



   Changing the DNS server address in the nslookup command to the following four IP addresses:

   172.16.1.164 - **142.250.192.78**

   172.16.1.180 - **142.250.194.14**

   172.16.1.165 - **142.250.183.206**

   172.16.1.166 - **142.250.77.78**

```
user@user-Veriton-S2690G-D22E2: ~
File  Edit  View  Search  Terminal  Help
> server 172.16.1.164
Default server: 172.16.1.164
Address: 172.16.1.164#53
> google.com
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.78
Name:   google.com
Address: 2404:6800:4009:831::200e
> google.com
Server:         172.16.1.164
Address:        172.16.1.164#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.78
Name:   google.com
Address: 2404:6800:4009:831::200e
> server 172.16.1.180
Default server: 172.16.1.180
Address: 172.16.1.180#53
> google.com
Server:         172.16.1.180
Address:        172.16.1.180#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.194.14
Name:   google.com
Address: 2404:6800:4009:832::200e
> server 172.16.1.165
Default server: 172.16.1.165
Address: 172.16.1.165#53
> google.com
Server:         172.16.1.165
Address:        172.16.1.165#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.206
Name:   google.com
Address: 2404:6800:4009:826::200e
> server 172.16.1.166
```

Google has numerous data centers worldwide, which is the reason for the change in the IP address of www.google.com. Google's address may change if we ask other DNS servers. In order to disperse traffic and avoid crashes, it often provides the IP addresses of Google servers that are located closest to the location from which the DNS query originated.

3. Send the ping packets with different packet sizes

```
user@user-Veriton-S2690G-D22E2: ~
File  Edit  View  Search  Terminal  Help
user@user-Veriton-S2690G-D22E2:~$ ping -s 64 -W 5 10.145.126.226
PING 10.145.126.226 (10.145.126.226) 64(92) bytes of data.
^C
--- 10.145.126.226 ping statistics ---
23 packets transmitted, 0 received, 100% packet loss, time 22514ms

user@user-Veriton-S2690G-D22E2:~$ ping -s 64 -W 1 10.5.16.66
PING 10.5.16.66 (10.5.16.66) 64(92) bytes of data.
72 bytes from 10.5.16.66: icmp_seq=1 ttl=64 time=0.571 ms
72 bytes from 10.5.16.66: icmp_seq=2 ttl=64 time=0.712 ms
72 bytes from 10.5.16.66: icmp_seq=3 ttl=64 time=0.716 ms
72 bytes from 10.5.16.66: icmp_seq=4 ttl=64 time=0.580 ms
72 bytes from 10.5.16.66: icmp_seq=5 ttl=64 time=0.550 ms
72 bytes from 10.5.16.66: icmp_seq=6 ttl=64 time=0.661 ms
72 bytes from 10.5.16.66: icmp_seq=7 ttl=64 time=0.555 ms
72 bytes from 10.5.16.66: icmp_seq=8 ttl=64 time=0.520 ms
72 bytes from 10.5.16.66: icmp_seq=9 ttl=64 time=0.707 ms
72 bytes from 10.5.16.66: icmp_seq=10 ttl=64 time=0.543 ms
72 bytes from 10.5.16.66: icmp_seq=11 ttl=64 time=0.518 ms
72 bytes from 10.5.16.66: icmp_seq=12 ttl=64 time=0.674 ms
72 bytes from 10.5.16.66: icmp_seq=13 ttl=64 time=0.714 ms
72 bytes from 10.5.16.66: icmp_seq=14 ttl=64 time=0.697 ms
^C
--- 10.5.16.66 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13247ms
rtt min/avg/max/mdev = 0.518/0.622/0.716/0.077 ms
user@user-Veriton-S2690G-D22E2:~$ ping -s 64 -W 1 10.5.16.66
PING 10.5.16.66 (10.5.16.66) 64(92) bytes of data.
72 bytes from 10.5.16.66: icmp_seq=1 ttl=64 time=0.533 ms
72 bytes from 10.5.16.66: icmp_seq=2 ttl=64 time=0.516 ms
72 bytes from 10.5.16.66: icmp_seq=3 ttl=64 time=0.512 ms
72 bytes from 10.5.16.66: icmp_seq=4 ttl=64 time=0.538 ms
72 bytes from 10.5.16.66: icmp_seq=5 ttl=64 time=0.599 ms
72 bytes from 10.5.16.66: icmp_seq=6 ttl=64 time=0.359 ms
72 bytes from 10.5.16.66: icmp_seq=7 ttl=64 time=0.475 ms
^C
--- 10.5.16.66 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6124ms
rtt min/avg/max/mdev = 0.359/0.504/0.599/0.068 ms
user@user-Veriton-S2690G-D22E2:~$ traceout
traceout: command not found
user@user-Veriton-S2690G-D22E2:~$ traceout 8.8.8.8
traceout: command not found
user@user-Veriton-S2690G-D22E2:~$ traceout www.google.com
traceout: command not found
user@user-Veriton-S2690G-D22E2:~$ traceroute www.google.com
traceroute to www.google.com (142.250.206.132), 30 hops max, 60 byte packets
```

Min/avg/max/mdev for a 64-byte packet transfer: 0.518/0.622/0.716/0.077

I experienced 100% packet loss when sending to a friend with a different network ID, but 0% packet loss occurred during the transfer of 14 packets to a friend having the same network ID.

```
karan@DELL:~$ ping -s 128 -W 1 10.102.45.237
PING 10.102.45.237 (10.102.45.237) 128(156) bytes of data.
136 bytes from 10.102.45.237: icmp_seq=1 ttl=127 time=187 ms
136 bytes from 10.102.45.237: icmp_seq=2 ttl=127 time=9.60 ms
136 bytes from 10.102.45.237: icmp_seq=3 ttl=127 time=14.4 ms
136 bytes from 10.102.45.237: icmp_seq=4 ttl=127 time=75.1 ms
136 bytes from 10.102.45.237: icmp_seq=5 ttl=127 time=82.5 ms
136 bytes from 10.102.45.237: icmp_seq=6 ttl=127 time=5.27 ms
136 bytes from 10.102.45.237: icmp_seq=7 ttl=127 time=6.89 ms
^C
--- 10.102.45.237 ping statistics ---
8 packets transmitted, 7 received, 12.5% packet loss, time 7011ms
rtt min/avg/max/mdev = 5.270/54.427/187.280/62.286 ms
karan@DELL:~$ ping -s 512 -W 1 10.102.45.237
PING 10.102.45.237 (10.102.45.237) 512(540) bytes of data.
520 bytes from 10.102.45.237: icmp_seq=1 ttl=127 time=46.5 ms
520 bytes from 10.102.45.237: icmp_seq=2 ttl=127 time=61.9 ms
520 bytes from 10.102.45.237: icmp_seq=3 ttl=127 time=92.3 ms
520 bytes from 10.102.45.237: icmp_seq=4 ttl=127 time=197 ms
520 bytes from 10.102.45.237: icmp_seq=5 ttl=127 time=11.3 ms
520 bytes from 10.102.45.237: icmp_seq=6 ttl=127 time=11.5 ms
520 bytes from 10.102.45.237: icmp_seq=7 ttl=127 time=3.60 ms
^C
--- 10.102.45.237 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 3.598/60.631/197.334/63.241 ms
karan@DELL:~$
```

4. Based on the traceroute output to `www.google.com` visible in your screenshot, here is the summary and explanation:

```
user@user-Veriton-S2690G-D22E2: ~
File  Edit  View  Search  Terminal  Help
^C
--- 10.5.16.66 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6124ms
rtt min/avg/max/mdev = 0.359/0.504/0.599/0.068 ms
user@user-Veriton-S2690G-D22E2:~$ traceout
traceout: command not found
user@user-Veriton-S2690G-D22E2:~$ traceout 8.8.8.8
traceout: command not found
user@user-Veriton-S2690G-D22E2:~$ traceout www.google.com
traceout: command not found
user@user-Veriton-S2690G-D22E2:~$ traceroute www.google.com
traceroute to www.google.com (142.250.206.132), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.453 ms  0.430 ms  0.417 ms
 2  10.120.2.33 (10.120.2.33)  0.344 ms  0.332 ms  0.321 ms
 3  10.255.1.3 (10.255.1.3)  3.022 ms  3.455 ms  2.940 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  142.250.172.80 (142.250.172.80)  59.641 ms 72.14.204.62 (72.14.204.62)  45.380 ms  57.189 ms
 9  * * *
10  192.178.86.244 (192.178.86.244)  59.289 ms 216.239.58.18 (216.239.58.18)  48.278 ms 108.170.231.78 (108.170.231.78)  56.445 ms
11  192.178.110.198 (192.178.110.198)  47.299 ms 142.250.226.66 (142.250.226.66)  55.631 ms 192.178.110.108 (192.178.110.108)  46.637 ms
12  142.251.48.137 (142.251.48.137)  69.682 ms 172.253.68.120 (172.253.68.120)  57.482 ms 172.253.68.121 (172.253.68.121)  68.862 ms
13  192.178.82.239 (192.178.82.239)  101.411 ms 192.178.82.233 (192.178.82.233)  63.846 ms 142.251.255.57 (142.251.255.57)  69.772 ms
14  142.251.76.199 (142.251.76.199)  68.211 ms 142.251.255.55 (142.251.255.55)  64.181 ms 142.251.76.197 (142.251.76.197)  90.261 ms
15  192.178.82.239 (192.178.82.239)  71.234 ms 142.251.76.197 (142.251.76.197)  78.432 ms  72.770 ms
16  del11s21-in-f4.1e100.net (142.250.206.132)  67.657 ms 142.251.76.197 (142.251.76.197)  76.212 ms del11s21-in-f4.1e100.net (142.250.206.132)  78.009 ms
user@user-Veriton-S2690G-D22E2:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.386 ms  0.391 ms  0.388 ms
 2  10.120.2.33 (10.120.2.33)  0.370 ms  0.368 ms  0.365 ms
 3  10.255.1.3 (10.255.1.3)  2.742 ms  2.680 ms  2.737 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  72.14.204.62 (72.14.204.62)  55.182 ms 142.250.172.80 (142.250.172.80)  46.375 ms  47.068 ms
 9  * * *
10  dns.google (8.8.8.8)  46.059 ms  45.744 ms  37.702 ms
user@user-Veriton-S2690G-D22E2:~$ traceroute www.google.com
traceroute to www.google.com (142.250.206.132), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.357 ms  0.320 ms  0.303 ms
 2  10.120.2.33 (10.120.2.33)  0.283 ms  0.312 ms  0.296 ms
 3  10.255.1.3 (10.255.1.3)  2.839 ms  2.823 ms  5.971 ms
 4  * * *
 5  * * *
```

Summarize the result for the first part call of traceroute for google.com

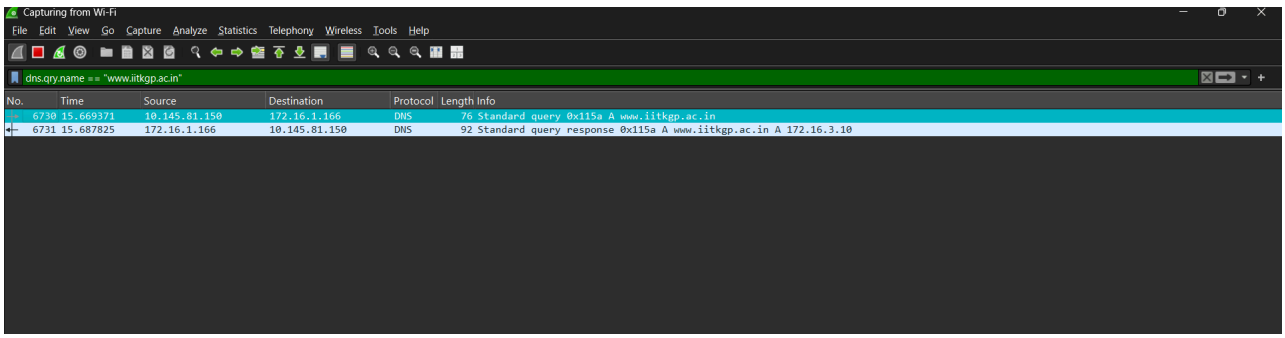
Number of hosts = 11

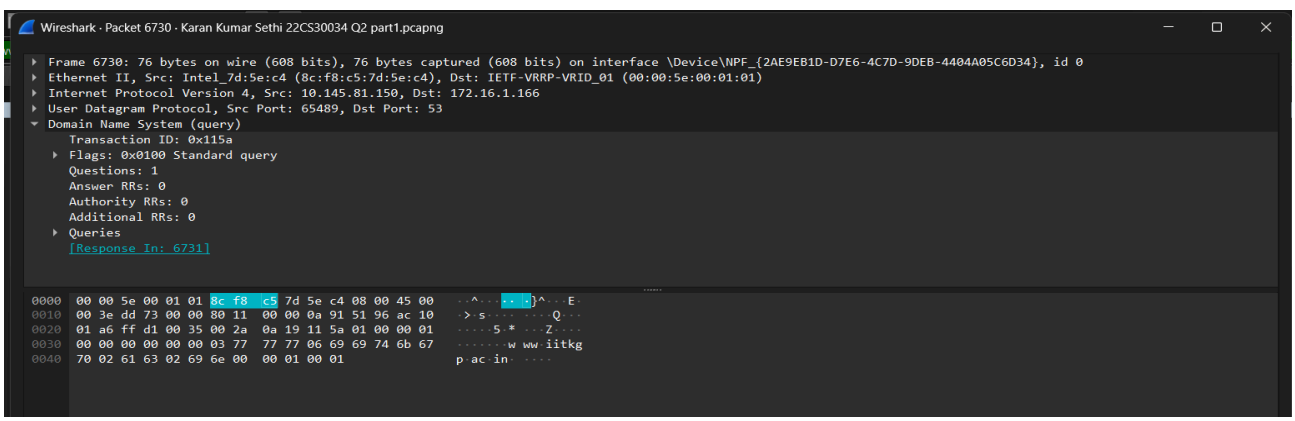
The *** entries in traceroute output occur when the intermediate router does not respond to the ICMP packets used for traceroute. This can happen due to:

- Router configuration to not respond to traceroute packets.
- Network congestion or timeouts at that hop.

Part 2: Packet Analysis

1. Analysis of DNS Packets: Structure and Traffic





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

- **Observation**: In your Wireshark screenshots, DNS packets are using **UDP**. confirmation by noting "User Datagram Protocol" in the packet details section.

b) Check the source and destination IP addresses of the DNS query.

- **DNS query packet (frame 6730)**:

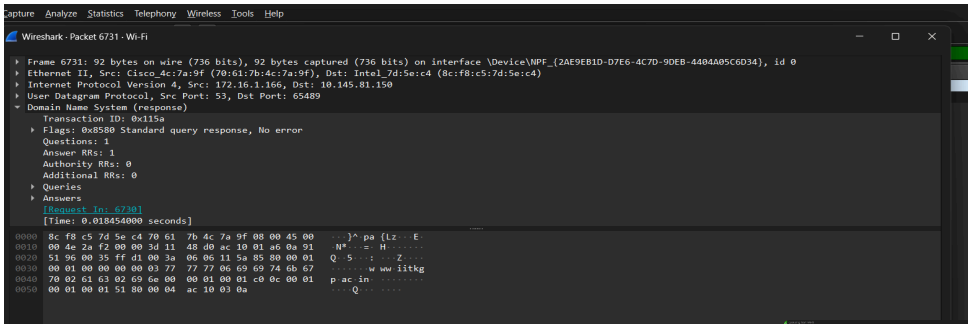
- **Source IP**: `10.145.81.150` (my laptop's IP).
- **Destination IP**: `172.16.1.166` (DNS server's IP).

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

- **Observation: 1 DNS query** was sent to resolve `www.iitkgp.ac.in`.

d) Which DNS server replies with actual IP address(es)?

- **DNS Response Packet (Frame 6731)**:
  - The **DNS server at 172.16.1.166** replies with the resolved IP address `172.16.3.10`.



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

- **Observation: 1 DNS server (172.16.1.166)** is involved in this specific query, and it responds to the query.

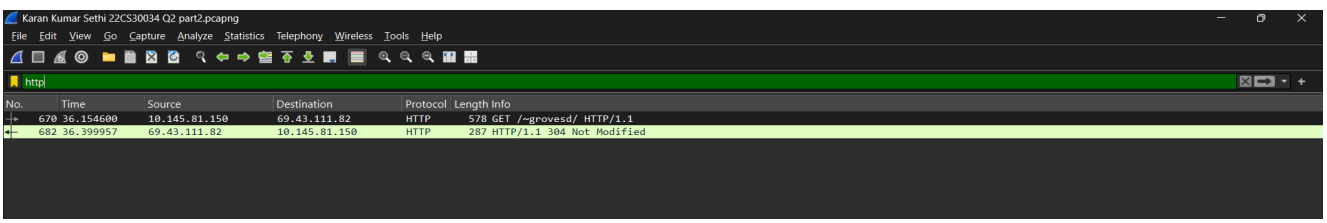
f) List the resource records involved in resolving the site's IP address.

- From the DNS response, the following Resource Record (RR) details can be inferred:
  - **Name**: `www.iitkgp.ac.in`
  - **Type**: `A` (1) (Host Address)
  - **Class**: `IN` (Internet)
  - **TTL**: 86400 (1 day)
  - **Data length**: 4
  - **Resolved IP Address**: `172.16.3.10`

```
▸ Frame 6731: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{2AE9EB1D-D7E6-4C7D-9DEB-4404A05C6D34}, id 0
▸ Ethernet II, Src: Cisco_4c:7a:9f (70:61:7b:4c:7a:9f), Dst: Intel_7d:5e:c4 (8c:f8:c5:7d:5e:c4)
▸ Internet Protocol Version 4, Src: 172.16.1.166, Dst: 10.145.81.150
▸ User Datagram Protocol, Src Port: 53, Dst Port: 65489
▾ Domain Name System (response)
    Transaction ID: 0x115a
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▾ 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: 6730]
    [Time: 0.018454000 seconds]
```

2. Web Traffic (HTTP)

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



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

```
Wireshark · Packet 670 · Karan Kumar Sethi 22CS30034 Q2 part2.pcapng

▸ Frame 670: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface \Device\NPF_{2AE9EB1D-D7E6-4C7D-9DEB-4404A05C6D34}, id 0
▸ Ethernet II, Src: Intel_7d:5e:c4 (8c:f8:c5:7d:5e:c4), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
▸ Internet Protocol Version 4, Src: 10.145.81.150, Dst: 69.43.111.82
▸ Transmission Control Protocol, Src Port: 52348, Dst Port: 80, Seq: 1, Ack: 1, Len: 524
▾ 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 (Windows NT 10.0; Win64; x64) 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\r\n
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    If-None-Match: "7b2-5919b3e8debc0"\r\n
    If-Modified-Since: Tue, 03 Sep 2019 00:33:59 GMT\r\n
    \r\n
    [Response in frame: 682]
    [Full request URI: http://web.simmons.edu/~grovesd/]
```

```
▸ Frame 682: 287 bytes on wire (2296 bits), 287 bytes captured (2296 bits) on interface \Device\NPF_{2AE9EB1D-D7E6-4C7D-9DEB-4404A05C6D34}, id 0
▸ Ethernet II, Src: Cisco_4c:7a:9f (70:61:7b:4c:7a:9f), Dst: Intel_7d:5e:c4 (8c:f8:c5:7d:5e:c4)
▸ Internet Protocol Version 4, Src: 69.43.111.82, Dst: 10.145.81.150
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 52348, Seq: 1, Ack: 525, Len: 233
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 304 Not Modified\r\n
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Fri, 17 Jan 2025 07:40:33 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
    [Request in frame: 670]
    [Time since request: 0.245357000 seconds]
    [Request URI: /~grovesd/]
    [Full request URI: http://web.simmons.edu/~grovesd/]
```

c) 2 packets are exchanged between the client and server to load an 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 & cross-check the source and destination IP addresses of captured ICMP packets.

```
PS C:\Users\karan> ping 10.102.45.237

Pinging 10.102.45.237 with 32 bytes of data:
Reply from 10.102.45.237: bytes=32 time=35ms TTL=128
Reply from 10.102.45.237: bytes=32 time=15ms TTL=128
Reply from 10.102.45.237: bytes=32 time=8ms TTL=128
Reply from 10.102.45.237: bytes=32 time=83ms TTL=128

Ping statistics for 10.102.45.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 83ms, Average = 35ms
PS C:\Users\karan>
```

No.	Time	Source	Destination	Protocol	Length	Info
60	8.044598	10.102.45.16	10.102.45.237	ICMP	74	Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (reply in 61)
61	8.080369	10.102.45.237	10.102.45.16	ICMP	74	Echo (ping) reply id=0x0001, seq=146/37376, ttl=128 (request in 60)
63	9.068510	10.102.45.16	10.102.45.237	ICMP	74	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (reply in 64)
64	9.084102	10.102.45.237	10.102.45.16	ICMP	74	Echo (ping) reply id=0x0001, seq=147/37632, ttl=128 (request in 63)
66	10.080641	10.102.45.16	10.102.45.237	ICMP	74	Echo (ping) request id=0x0001, seq=148/37888, ttl=128 (reply in 68)
68	10.089446	10.102.45.237	10.102.45.16	ICMP	74	Echo (ping) reply id=0x0001, seq=148/37888, ttl=128 (request in 66)
72	11.096324	10.102.45.16	10.102.45.237	ICMP	74	Echo (ping) request id=0x0001, seq=149/38144, ttl=128 (reply in 73)
73	11.179427	10.102.45.237	10.102.45.16	ICMP	74	Echo (ping) reply id=0x0001, seq=149/38144, ttl=128 (request in 72)

Source : 10.102.45.16 (My IP address)

Destination : 10.102.45.237 (My friend's IP address)

traceroute/tracert(for windows) to a reachable IP

```
PS C:\Users\karan> tracert 10.102.45.237

Tracing route to Manash_Laptop [10.102.45.237]
over a maximum of 30 hops:

  1     8 ms    13 ms    21 ms  Manash_Laptop [10.102.45.237]

Trace complete.
PS C:\Users\karan>
```

No.	Time	Source	Destination	Protocol	Length	Info
58	8.643086	10.102.45.16	10.102.45.237	ICMP	106	Echo (ping) request id=0x0001, seq=153/39168, ttl=1 (reply in 59)
59	8.651153	10.102.45.237	10.102.45.16	ICMP	106	Echo (ping) reply id=0x0001, seq=153/39168, ttl=128 (request in 58)
60	8.654235	10.102.45.16	10.102.45.237	ICMP	106	Echo (ping) request id=0x0001, seq=154/39424, ttl=1 (reply in 61)
61	8.667564	10.102.45.237	10.102.45.16	ICMP	106	Echo (ping) reply id=0x0001, seq=154/39424, ttl=128 (request in 60)
62	8.671007	10.102.45.16	10.102.45.237	ICMP	106	Echo (ping) request id=0x0001, seq=155/39680, ttl=1 (reply in 63)
63	8.692187	10.102.45.237	10.102.45.16	ICMP	106	Echo (ping) reply id=0x0001, seq=155/39680, ttl=128 (request in 62)

It is evident from the details that my friend's device and IP have been successfully traced.

```
▸ Frame 63: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{2AE9EB1D-D7E6-4C7D-9DEB-4404A05C6D34}, id 0
▸ Ethernet II, Src: AzureWaveTec_e4:15:93 (34:6f:24:e4:15:93), Dst: Intel_7d:5e:c4 (8c:f8:c5:7d:5e:c4)
▸ Internet Protocol Version 4, Src: 10.102.45.237, Dst: 10.102.45.16
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff63 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 155 (0x009b)
    Sequence Number (LE): 39680 (0x9b00)
    [Request frame: 62]
    [Response time: 21.180 ms]
  ▾ Data (64 bytes)
      Data: 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
      [Length: 64]
```

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.

```
PS C:\Users\karan> ping 192.168.31.3

Pinging 192.168.31.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.31.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\karan>
```

wireshark:

15814	754.627385	10.102.45.16	192.168.31.3	ICMP	74	Echo (ping) request id=0x0001, seq=246/62976, ttl=128 (no response found!)
15903	759.538555	10.102.45.16	192.168.31.3	ICMP	74	Echo (ping) request id=0x0001, seq=247/63232, ttl=128 (no response found!)
15991	764.528755	10.102.45.16	192.168.31.3	ICMP	74	Echo (ping) request id=0x0001, seq=248/63488, ttl=128 (no response found!)
16027	769.527073	10.102.45.16	192.168.31.3	ICMP	74	Echo (ping) request id=0x0001, seq=249/63744, ttl=128 (no response found!)

There is no response when attempting to ping an IP address that does not exist or is outside my network's range, making it impossible to receive a reply.

```
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4c62 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 249 (0x00f9)
    Sequence Number (LE): 63744 (0xf900)
  ▾ [No response seen]
    ▾ [Expert Info (Warning/Sequence): No response seen to ICMP request]
        [No response seen to ICMP request]
        [Severity level: Warning]
        [Group: Sequence]
  ▾ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761626364656667686 9
      [Length: 32]
```

c) performing a ‘traceroute’ operation for unreachable hosts and preparing a brief report of your observation using Wireshark.

5769	226.195500	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=156/39936, ttl=1 (no response found!)
5770	226.226165	10.102.45.2	10.102.45.16	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5771	226.230251	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=157/40192, ttl=1 (no response found!)
5772	226.239345	10.102.45.2	10.102.45.16	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5773	226.241427	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=158/40448, ttl=1 (no response found!)
5774	226.244563	10.102.45.2	10.102.45.16	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5806	232.421097	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=159/40704, ttl=2 (no response found!)
5807	232.425743	10.120.1.1	10.102.45.16	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5808	232.427981	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=160/40960, ttl=2 (no response found!)
5809	232.433007	10.120.1.1	10.102.45.16	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5810	232.435589	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=161/41216, ttl=2 (no response found!)
5811	232.436904	10.120.1.1	10.102.45.16	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5840	239.118141	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=162/41472, ttl=3 (no response found!)
5864	243.015431	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=163/41728, ttl=3 (no response found!)
5876	247.010978	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=164/41984, ttl=3 (no response found!)
5905	251.018642	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=165/42240, ttl=4 (no response found!)
5927	255.013770	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=166/42496, ttl=4 (no response found!)
5933	259.013679	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=167/42752, ttl=4 (no response found!)
5935	263.025840	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=168/43008, ttl=5 (no response found!)
5947	267.020884	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=169/43264, ttl=5 (no response found!)
5950	271.015392	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=170/43520, ttl=5 (no response found!)
5958	275.024686	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=171/43776, ttl=6 (no response found!)
5988	279.010833	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=172/44032, ttl=6 (no response found!)
6028	283.013186	10.102.45.16	192.168.31.3	ICMP	106	Echo (ping) request id=0x0001, seq=173/44288, ttl=6 (no response found!)

- Wireshark recorded time-to-live exceeded ICMP messages when tracing an unreachable IP outside the network. This indicates that the packets were discarded by intermediate routers due to the TTL reaching 0.
- The target IP is unreachable and not a part of the network, as confirmed by the lack of a definitive response.
- Both successful and unsuccessful pings were examined in ICMP packets (Echo Request and Echo Reply). For unreachable hosts, "Time-to-live exceeded" messages dominated.
- Sequence numbers and TTL values in ICMP Echo Request/Reply packets showed successful communication for reachable hosts.
- Although traceroute operations displayed intermediate hops, the trace ended prematurely with repeated "Request timed out" entries for hosts that could not be reached.

```
PS C:\Users\karan> tracert 192.168.31.3

Tracing route to 192.168.31.3 over a maximum of 30 hops

  1    30 ms     9 ms     3 ms  10.102.45.2
  2     4 ms     5 ms     1 ms  10.120.1.1
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
PS C:\Users\karan>
```