

Assignment 1

Networking Tools and Wireshark

Part 1: Networking Tools

1.1 ifconfig

```
user@user-Veriton-S2690G-D22E2:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.5.16.206 netmask 255.255.255.0 broadcast 10.5.16.255
    inet6 fe80::8aae:ddff:fe33:9e85 prefixlen 64 scopeid 0x20<link>
    ether 88:ae:dd:33:9e:85 txqueuelen 1000 (Ethernet)
    RX packets 82017 bytes 64901365 (64.9 MB)
    RX errors 0 dropped 197 overruns 0 frame 0
    TX packets 33480 bytes 6649883 (6.6 MB)
    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 3785 bytes 744256 (744.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3785 bytes 744256 (744.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

IP Address	10.5.16.206
Subnet Mask	255.255.255.0
Network ID (NID)	10.5.16.0 (logical AND of IP address and subnet mask)
Host ID (HID)	206

1.2 nslookup

IP address associated with www.google.com and www.facebook.com using the default (system's configured) DNS server:

```
user@user-Veriton-S2690G-D22E2:~$ nslookup www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.206.164
Name:   www.google.com
Address: 2404:6800:4002:82c::2004

user@user-Veriton-S2690G-D22E2:~$ nslookup www.facebook.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.facebook.com      canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 31.13.79.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f188:84:face:b00c:0:25de
```

The IP address changes when specifying a different DNS server for querying the same domain name (www.google.com). This may happen due to several reasons, such as Load Balancing, CDNs.

```
user@user-Veriton-S2690G-D22E2:~$ 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: 2404:6800:4002:81a::2004

user@user-Veriton-S2690G-D22E2:~$ 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: 142.250.207.228
Name:   www.google.com
Address: 2404:6800:4002:82c::2004

user@user-Veriton-S2690G-D22E2:~$ 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

user@user-Veriton-S2690G-D22E2:~$ 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
```

Moreover, querying with the same DNS server (after some time gap) also returns different IP addresses. A possible reason for this could be the short TTL (Time To Live) of DNS Caching.

```
user@user-Veriton-S2690G-D22E2:~$ 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: 142.250.70.100
Name:   www.google.com
Address: 2404:6800:4009:828::2004

user@user-Veriton-S2690G-D22E2:~$ 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: 142.250.194.196
Name:   www.google.com
Address: 2404:6800:4009:829::2004
```

1.3 ping

Packet Size: 64 bytes (+8 bytes for ICMP header data)

```
user@user-Veriton-S2690G-D22E2:~$ ping -s 64 -w 100 10.5.16.205
PING 10.5.16.205 (10.5.16.205) 64(92) bytes of data.
72 bytes from 10.5.16.205: icmp_seq=1 ttl=64 time=0.426 ms
72 bytes from 10.5.16.205: icmp_seq=2 ttl=64 time=0.424 ms
72 bytes from 10.5.16.205: icmp_seq=3 ttl=64 time=0.442 ms
72 bytes from 10.5.16.205: icmp_seq=4 ttl=64 time=0.432 ms
72 bytes from 10.5.16.205: icmp_seq=5 ttl=64 time=0.427 ms
72 bytes from 10.5.16.205: icmp_seq=96 ttl=64 time=0.452 ms
72 bytes from 10.5.16.205: icmp_seq=97 ttl=64 time=0.444 ms
72 bytes from 10.5.16.205: icmp_seq=98 ttl=64 time=0.444 ms

--- 10.5.16.205 ping statistics ---
98 packets transmitted, 98 received, 0% packet loss, time 99331ms
rtt min/avg/max/mdev = 0.265/0.414/0.498/0.049 ms
```

Packet Loss	0%
Min RTT	0.265 ms
Avg RTT	0.414 ms
Max RTT	0.498 ms
Stddev RTT	0.049ms

Packet Size: 128 (+8) bytes

```
user@user-Veriton-S2690G-D22E2:~$ ping -s 128 -w 100 10.5.16.205
PING 10.5.16.205 (10.5.16.205) 128(156) bytes of data.
136 bytes from 10.5.16.205: icmp_seq=1 ttl=64 time=0.297 ms
136 bytes from 10.5.16.205: icmp_seq=2 ttl=64 time=0.310 ms
136 bytes from 10.5.16.205: icmp_seq=3 ttl=64 time=0.238 ms
136 bytes from 10.5.16.205: icmp_seq=96 ttl=64 time=0.243 ms
136 bytes from 10.5.16.205: icmp_seq=97 ttl=64 time=0.260 ms
136 bytes from 10.5.16.205: icmp_seq=98 ttl=64 time=0.294 ms

--- 10.5.16.205 ping statistics ---
98 packets transmitted, 98 received, 0% packet loss, time 99322ms
rtt min/avg/max/mdev = 0.113/0.244/0.447/0.059 ms
```

Packet Loss	0%
Min RTT	0.113 ms

Avg RTT	0.244 ms
Max RTT	0.447 ms
Stddev RTT	0.059ms

Packet Size: 512 (+8) bytes

```

user@user-Veriton-S2690G-D22E2:~$ ping -s 512 -w 100 10.5.16.205
PING 10.5.16.205 (10.5.16.205) 512(540) bytes of data.
520 bytes from 10.5.16.205: icmp_seq=1 ttl=64 time=0.143 ms
520 bytes from 10.5.16.205: icmp_seq=2 ttl=64 time=0.416 ms
520 bytes from 10.5.16.205: icmp_seq=3 ttl=64 time=0.193 ms
520 bytes from 10.5.16.205: icmp_seq=96 ttl=64 time=0.451 ms
520 bytes from 10.5.16.205: icmp_seq=97 ttl=64 time=0.226 ms
520 bytes from 10.5.16.205: icmp_seq=98 ttl=64 time=0.276 ms

--- 10.5.16.205 ping statistics ---
98 packets transmitted, 98 received, 0% packet loss, time 99306ms
rtt min/avg/max/mdev = 0.143/0.324/0.477/0.103 ms

```

Packet Loss	0%
Min RTT	0.143 ms
Avg RTT	0.324 ms
Max RTT	0.477 ms
Stddev RTT	0.103ms

1.4 traceroute

```
user@user-Veriton-S26906-D22E2:~$ traceroute www.google.com
traceroute to www.google.com (142.250.207.228), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.387 ms  0.368 ms  0.360 ms
 2  10.120.2.33 (10.120.2.33)  0.350 ms  0.341 ms  0.332 ms
 3  10.255.1.3 (10.255.1.3)  4.227 ms  3.478 ms  4.424 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  142.250.172.80 (142.250.172.80)  47.422 ms  72.14.204.62 (72.14.204.62)  46.284 ms  142.250.172.80 (142.250.172.80)  57.426 ms
 9  * * *
10  142.250.228.50 (142.250.228.50)  55.745 ms  209.85.142.84 (209.85.142.84)  39.537 ms  142.250.238.200 (142.250.238.200)  54.772 ms
11  192.178.110.204 (192.178.110.204)  45.325 ms  192.178.110.206 (192.178.110.206)  56.989 ms  142.250.209.70 (142.250.209.70)  40.014 ms
12  142.251.48.137 (142.251.48.137)  75.954 ms  216.239.48.65 (216.239.48.65)  56.522 ms  108.170.232.203 (108.170.232.203)  70.507 ms
13  192.178.83.225 (192.178.83.225)  68.523 ms  142.251.48.137 (142.251.48.137)  76.463 ms  216.239.50.23 (216.239.50.23)  69.222 ms
14  142.251.76.173 (142.251.76.173)  78.851 ms  142.251.76.175 (142.251.76.175)  67.452 ms  68.479 ms
15  192.178.83.215 (192.178.83.215)  72.316 ms  216.239.62.219 (216.239.62.219)  59.334 ms  del12s11-in-f4.1e100.net (142.250.207.228)  77.226 ms
```

No. of hops: **15**

No. of visible hosts: $3+7*3 = \mathbf{24}$

Meaning of * * *

Traceroute requires a response from the target server and each intermediate hop to create its output. Some routers don't respond because of overload, and some can't because of small TTL of packets. But since every time, even after increasing TTL, tracerouting www.google.com generates * * * on hops 4,5,6,7,9, the reason could be the configuration of the routers to not respond to the type of packets traceroute sends. *Three asterisks* as traceroute sends three probe packets by default.

Part 2: Packet Analysis

2.1 Analysis of DNS Packets: Structure and its Traffic

dns contains "iitkgp"					
No.	Time	Source	Destination	Protocol	Length Info
128	17.874137	10.5.16.206	172.16.1.180	DNS	72 Standard query 0xf8ca A iitkgp.ac.in
129	17.874170	10.5.16.206	172.16.1.180	DNS	72 Standard query 0xb60 HTTPS iitkgp.ac.in
130	17.875758	172.16.1.180	10.5.16.206	DNS	88 Standard query response 0xf8ca A iitkgp.ac.in A 172.16.3.10
131	17.878306	172.16.1.180	10.5.16.206	DNS	128 Standard query response 0xb60 HTTPS iitkgp.ac.in SOA localdns.iitkgp.ac.in
185	27.556878	10.5.16.206	172.16.1.180	DNS	76 Standard query 0x8bbe HTTPS www.iitkgp.ac.in
187	27.563835	172.16.1.180	10.5.16.206	DNS	132 Standard query response 0x8bbe HTTPS www.iitkgp.ac.in SOA localdns.iitkgp.ac.in

Frame 128: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)	0000	90 88 55 9c c4 4a 88 ae dd 33 9e 85 08 00 45 00
Ethernet II, Src: EliteGroupCo_33:9e:85 (88:ae:dd:33:9e:85), Dst: Cisco_9c:c4:4a (90:88:55:9c:c4:4a)	0010	00 3a e5 79 00 00 40 11 cc a2 0a 05 10 ce ac 10
Internet Protocol Version 4, Src: 10.5.16.206, Dst: 172.16.1.180	0020	01 b4 b5 e8 00 35 00 26 c8 ce f8 ca 01 00 00 01
User Datagram Protocol, Src Port: 46568, Dst Port: 53	0030	00 00 00 00 00 00 06 69 69 74 6b 67 70 02 61 63
Source Port: 46568	0040	82 69 6e 00 00 01 00 01
Destination Port: 53		
Length: 38		
Checksum: 0xc8ce [unverified]		
[Checksum Status: Unverified]		
[Stream index: 9]		
[Timestamps]		
UDP payload (38 bytes)		
Domain Name System (query)		

- DNS uses User Datagram Protocol (**UDP**) in the observed packets.
- Source IP Address of DNS Query: **10.5.16.206**
Destination IP Address of DNS Query: **172.16.1.180**
- During the name-to-IP resolution, **three** queries were sent from the host machine to the DNS Server(s).

dns contains "iitkgp"					
No.	Time	Source	Destination	Protocol	Length Info
128	17.874137	10.5.16.206	172.16.1.180	DNS	72 Standard query 0xf8ca A iitkgp.ac.in
129	17.874170	10.5.16.206	172.16.1.180	DNS	72 Standard query 0xb60 HTTPS iitkgp.ac.in
130	17.875758	172.16.1.180	10.5.16.206	DNS	88 Standard query response 0xf8ca A iitkgp.ac.in A 172.16.3.10
131	17.878306	172.16.1.180	10.5.16.206	DNS	128 Standard query response 0xb60 HTTPS iitkgp.ac.in SOA locald
185	27.556878	10.5.16.206	172.16.1.180	DNS	76 Standard query 0x8bbe HTTPS www.iitkgp.ac.in
187	27.563835	172.16.1.180	10.5.16.206	DNS	132 Standard query response 0x8bbe HTTPS www.iitkgp.ac.in SOA lo

Frame 130: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)	0000	88 ae dd 33 9e 85 00 88 5
Ethernet II, Src: Cisco_9c:c4:4a (90:88:55:9c:c4:4a), Dst: EliteGroupCo_33:9e:85 (88:ae:dd:33:9e:85)	0010	00 4a 89 ac 00 00 3d 11 2
Internet Protocol Version 4, Src: 172.16.1.180, Dst: 10.5.16.206	0020	10 ce 00 35 b5 e8 00 36 2
User Datagram Protocol, Src Port: 53, Dst Port: 46568	0030	00 01 00 00 00 00 06 69 6
Domain Name System (response)	0040	02 69 6e 00 00 01 00 01 c
Transaction ID: 0xf8ca	0050	51 80 00 04 ac 10 03 0a
Flags: 0x8580 Standard query response, No error		
Questions: 1		
Answer RRs: 1		
Authority RRs: 0		
Additional RRs: 0		
Queries		
Answers		
iitkgp.ac.in: type A, class IN, addr 172.16.3.10		
Name: 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: 128]		
[Time: 0.001621000 seconds]		

- DNS Server with IP Address **172.16.1.180** and port **53** responded with the actual IP Address.
- One DNS Server is involved, which responded.


```

> Frame 130: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: Cisco_9c:c4:4a (90:88:55:9c:c4:4a), Dst: EliteGroupCo_33:9e:85 (88:ae:dd:33:9e:85)
> Internet Protocol Version 4, Src: 172.16.1.180, Dst: 10.5.16.206
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 74
    Identification: 0x89ac (35244)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 61
    Protocol: UDP (17)
    Header Checksum: 0x2b60 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.1.180
    Destination Address: 10.5.16.206
  > User Datagram Protocol, Src Port: 53, Dst Port: 46568
  > Domain Name System (response)
    Transaction ID: 0xf8ca
    > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    > iitkgp.ac.in: type A, class IN
      Name: iitkgp.ac.in
      [Name Length: 12]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  > Answers
    > iitkgp.ac.in: type A, class IN, addr 172.16.3.10
      Name: 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: 128]
    [Time: 0.001621000 seconds]

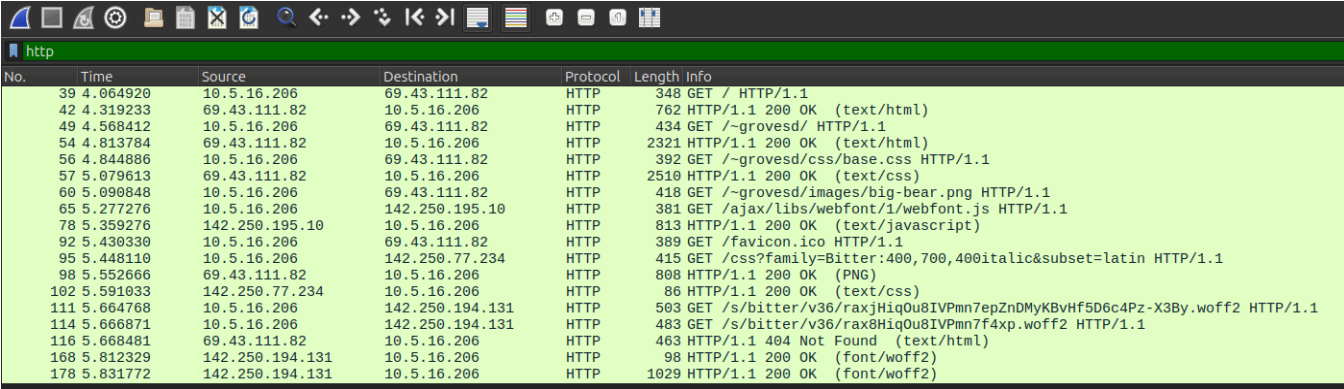
```

f) Resource records involved:

Name	iitkgp.ac.in
Type	A
Class	IN
TTL	86400
Data Length	4
Resolved IP Address	172.16.3.10

2.2 Web Traffic (HTTP)

a) HTTP packets exchanged:



No.	Time	Source	Destination	Protocol	Length	Info
39	4.064920	10.5.16.206	69.43.111.82	HTTP	348	GET / HTTP/1.1
42	4.319233	69.43.111.82	10.5.16.206	HTTP	762	HTTP/1.1 200 OK (text/html)
49	4.568412	10.5.16.206	69.43.111.82	HTTP	434	GET /~grovesd/ HTTP/1.1
54	4.813784	69.43.111.82	10.5.16.206	HTTP	2321	HTTP/1.1 200 OK (text/html)
56	4.844886	10.5.16.206	69.43.111.82	HTTP	392	GET /~grovesd/css/base.css HTTP/1.1
57	5.079613	69.43.111.82	10.5.16.206	HTTP	2510	HTTP/1.1 200 OK (text/css)
60	5.090848	10.5.16.206	69.43.111.82	HTTP	418	GET /~grovesd/images/big-bear.png HTTP/1.1
65	5.277276	10.5.16.206	142.250.195.10	HTTP	381	GET /ajax/libs/webfont/1/webfont.js HTTP/1.1
78	5.359276	142.250.195.10	10.5.16.206	HTTP	813	HTTP/1.1 200 OK (text/javascript)
92	5.430330	10.5.16.206	69.43.111.82	HTTP	389	GET /favicon.ico HTTP/1.1
95	5.448110	10.5.16.206	142.250.77.234	HTTP	415	GET /css?family=Bitter:400,700,400italic&subset=latin HTTP/1.1
98	5.552666	69.43.111.82	10.5.16.206	HTTP	808	HTTP/1.1 200 OK (PNG)
102	5.591033	142.250.77.234	10.5.16.206	HTTP	86	HTTP/1.1 200 OK (text/css)
111	5.664768	10.5.16.206	142.250.194.131	HTTP	503	GET /s/bitter/v36/raxjHiq0u8IVPmn7epZnDMYKBvHf5D6c4Pz-X3By.woff2 HTTP/1.1
114	5.666871	10.5.16.206	142.250.194.131	HTTP	483	GET /s/bitter/v36/rax8Hiq0u8IVPmn7f4xp.woff2 HTTP/1.1
116	5.668481	69.43.111.82	10.5.16.206	HTTP	463	HTTP/1.1 404 Not Found (text/html)
168	5.812329	142.250.194.131	10.5.16.206	HTTP	98	HTTP/1.1 200 OK (font/woff2)
178	5.831772	142.250.194.131	10.5.16.206	HTTP	1029	HTTP/1.1 200 OK (font/woff2)

b) HTTP request headers contain fields like Request Method, Request URI, Request Version, Host, User-Agent, Referrer etc. HTTP response headers have fields like Response Version, Status Code, Response Phrase, Date, Content-Type etc. Screenshots are pasted in next few pages.

c) Total of **18** HTTP packets are exchanged:

10 packets between the client (10.5.16.206) and server (69.43.111.82) to load HTML, CSS and PNG.

8 packets between client (10.5.16.206) and external servers (142.250.195.10, 142.250.77.234, 142.250.194.131) to load the font & related CSS, JS.

HTML of page at root (/)

```
▼ Hypertext Transfer Protocol
  ▼ GET / HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: web.simmons.edu\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: */*\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Sec-GPC: 1\r\n
      Connection: keep-alive\r\n
      Pragma: no-cache\r\n
      Cache-Control: no-cache\r\n
      \r\n
      [Full request URI: http://web.simmons.edu/]
      [HTTP request 1/1]
      [Response in frame: 42]
```

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Tue, 14 Jan 2025 18:20:23 GMT\r\n
      Server: Apache\r\n
      Last-Modified: Wed, 06 Mar 2024 15:36:23 GMT\r\n
      ETag: "19c-612ffb89b8b71"\r\n
      Accept-Ranges: bytes\r\n
      ▶ Content-Length: 412\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.254313000 seconds]
      [Request in frame: 39]
      [Request URI: http://web.simmons.edu/]
      File Data: 412 bytes
      ▶ Line-based text data: text/html (9 lines)
```

HTML of page at path /~grovesd/

```
▼ Hypertext Transfer Protocol
  ▼ GET /~grovesd/ HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /~grovesd/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /~grovesd/
      Request Version: HTTP/1.1
      Host: web.simmons.edu\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      DNT: 1\r\n
      Sec-GPC: 1\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Full request URI: http://web.simmons.edu/~grovesd/]
      [HTTP request 1/3]
      [Response in frame: 54]
      [Next request in frame: 56]
```

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Tue, 14 Jan 2025 18:20:23 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
      ▶ Content-Length: 1970\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [HTTP response 1/3]
      [Time since request: 0.245372000 seconds]
      [Request in frame: 49]
      [Next request in frame: 56]
      [Next response in frame: 57]
      [Request URI: http://web.simmons.edu/~grovesd/]
      File Data: 1970 bytes
```

CSS of page at path /~grovesd/

```
▼ Hypertext Transfer Protocol
  ▼ GET /~grovesd/css/base.css HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /~grovesd/css/base.css HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /~grovesd/css/base.css
      Request Version: HTTP/1.1
      Host: web.simmons.edu\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: text/css,*/*;q=0.1\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      DNT: 1\r\n
      Sec-GPC: 1\r\n
      Connection: keep-alive\r\n
      Referer: http://web.simmons.edu/~grovesd/\r\n
      \r\n
```

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Tue, 14 Jan 2025 18:20:23 GMT\r\n
      Server: Apache\r\n
      Last-Modified: Tue, 26 Jan 2016 03:17:08 GMT\r\n
      ETag: "880-52a341edcb500"\r\n
      Accept-Ranges: bytes\r\n
      ▶ Content-Length: 2176\r\n
      Keep-Alive: timeout=5, max=99\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/css\r\n
      \r\n
      [HTTP response 2/3]
      [Time since request: 0.234727000 seconds]
      [Prev request in frame: 49]
      [Prev response in frame: 54]
      [Request in frame: 56]
      [Next request in frame: 60]
      [Next response in frame: 98]
      [Request URI: http://web.simmons.edu/~grovesd/css/base.css]
      File Data: 2176 bytes
```

Image(s) on page at path /~grovesd/

```
▼ 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
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: image/avif,image/webp,*/*\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      DNT: 1\r\n
      Sec-GPC: 1\r\n
      Connection: keep-alive\r\n
      Referer: http://web.simmons.edu/~grovesd/css/base.css\r\n
      \r\n
      [Full request URI: http://web.simmons.edu/~grovesd/images/big-bear.png]
      [HTTP request 3/3]
      [Prev request in frame: 56]
      [Response in frame: 98]
```

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Tue, 14 Jan 2025 18:20:24 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=98\r\n
      Connection: Keep-Alive\r\n
      Content-Type: image/png\r\n
      \r\n
      [HTTP response 3/3]
      [Time since request: 0.461818000 seconds]
      [Prev request in frame: 56]
      [Prev response in frame: 57]
      [Request in frame: 60]
      [Request URI: http://web.simmons.edu/~grovesd/images/big-bear.png]
      File Data: 17847 bytes
```

Favicon:

```
▼ Hypertext Transfer Protocol
  ▼ GET /favicon.ico HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /favicon.ico
      Request Version: HTTP/1.1
      Host: web.simmons.edu\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: image/avif,image/webp,*/*\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      DNT: 1\r\n
      Sec-GPC: 1\r\n
      Connection: keep-alive\r\n
      Referer: http://web.simmons.edu/~grovesd/\r\n
      \r\n
      [Full request URI: http://web.simmons.edu/favicon.ico]
      [HTTP request 1/1]
      [Response in frame: 116]
```

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 404 Not Found\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
      Date: Tue, 14 Jan 2025 18:20:24 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
      [HTTP response 1/1]
      [Time since request: 0.238151000 seconds]
      [Request in frame: 92]
      [Request URI: http://web.simmons.edu/favicon.ico]
      File Data: 196 bytes
```

2.3 ICMP Traffic (ping/traceroute)

a) pinging and tracerouting 10.5.16.205

```
user@user-Veriton-S2690G-D22E2:~$ ping 10.5.16.205
PING 10.5.16.205 (10.5.16.205) 56(84) bytes of data.
64 bytes from 10.5.16.205: icmp_seq=1 ttl=64 time=0.444 ms
64 bytes from 10.5.16.205: icmp_seq=2 ttl=64 time=0.647 ms
64 bytes from 10.5.16.205: icmp_seq=3 ttl=64 time=0.301 ms
^C
--- 10.5.16.205 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.301/0.464/0.647/0.141 ms
user@user-Veriton-S2690G-D22E2:~$ traceroute 10.5.16.205
traceroute to 10.5.16.205 (10.5.16.205), 30 hops max, 60 byte packets
 1  10.5.16.205 (10.5.16.205)  0.361 ms  0.329 ms  0.304 ms
```

icmp							
No.	Time	Source	Destination	Protocol	Length	Info	
131	11.318050	10.5.16.206	10.5.16.205	ICMP	98	Echo (ping) request	id=0x000d, seq=1/256, ttl=64 (reply in 132)
132	11.318475	10.5.16.205	10.5.16.206	ICMP	98	Echo (ping) reply	id=0x000d, seq=1/256, ttl=64 (request in 131)
139	12.322921	10.5.16.206	10.5.16.205	ICMP	98	Echo (ping) request	id=0x000d, seq=2/512, ttl=64 (reply in 140)
140	12.323537	10.5.16.205	10.5.16.206	ICMP	98	Echo (ping) reply	id=0x000d, seq=2/512, ttl=64 (request in 139)
147	13.346929	10.5.16.206	10.5.16.205	ICMP	98	Echo (ping) request	id=0x000d, seq=3/768, ttl=64 (reply in 148)
148	13.347201	10.5.16.205	10.5.16.206	ICMP	98	Echo (ping) reply	id=0x000d, seq=3/768, ttl=64 (request in 147)
242	23.222779	10.5.16.205	10.5.16.206	ICMP	102	Destination unreachable	(Port unreachable)
243	23.222780	10.5.16.205	10.5.16.206	ICMP	102	Destination unreachable	(Port unreachable)
244	23.222780	10.5.16.205	10.5.16.206	ICMP	102	Destination unreachable	(Port unreachable)
245	23.222780	10.5.16.205	10.5.16.206	ICMP	102	Destination unreachable	(Port unreachable)
246	23.222780	10.5.16.205	10.5.16.206	ICMP	102	Destination unreachable	(Port unreachable)
247	23.222780	10.5.16.205	10.5.16.206	ICMP	102	Destination unreachable	(Port unreachable)

Ping request	
Source IP	10.5.16.206
Dest IP	10.5.16.205
Ping response	
Source IP	10.5.16.205
Dest IP	10.5.16.206
Traceroute response	
Source IP	10.5.16.205
Dest IP	10.5.16.206
Header of traceroute response	
Source IP	10.5.16.206
Dest IP	10.5.16.205

Ping:

```
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf767 [correct]
  [Checksum Status: Good]
  Identifier (BE): 13 (0x000d)
  Identifier (LE): 3328 (0x0d00)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Response frame: 132]
  Timestamp from icmp data: Jan 15, 2025 22:34:40.681223000 IST
  [Timestamp from icmp data (relative): 0.000019000 seconds]
▼ Data (40 bytes)
  Data: 101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
  [Length: 40]
```

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xff67 [correct]
  [Checksum Status: Good]
  Identifier (BE): 13 (0x000d)
  Identifier (LE): 3328 (0x0d00)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Request frame: 131]
  [Response time: 0.425 ms]
  Timestamp from icmp data: Jan 15, 2025 22:34:40.681223000 IST
  [Timestamp from icmp data (relative): 0.000444000 seconds]
▼ Data (40 bytes)
  Data: 101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
  [Length: 40]
```

Traceroute:

3 packets have TTL = 1 and 3 have TTL = 2, which is the expected behaviour according to tracerouting algorithm.

```

▼ Internet Protocol Version 4, Src: 10.5.16.205, Dst: 10.5.16.206
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 88
    Identification: 0xfa11 (64017)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x4a2f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.5.16.205
    Destination Address: 10.5.16.206
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 3 (Port unreachable)
  Checksum: 0x32db [correct]
  [Checksum Status: Good]
  Unused: 00000000
▼ Internet Protocol Version 4, Src: 10.5.16.206, Dst: 10.5.16.205
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x2fc3 (12227)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▶ Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x544a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.5.16.206
    Destination Address: 10.5.16.205

```

```

▼ Internet Protocol Version 4, Src: 10.5.16.205, Dst: 10.5.16.206
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 88
    Identification: 0xfa14 (64020)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x4a2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.5.16.205
    Destination Address: 10.5.16.206
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 3 (Port unreachable)
  Checksum: 0x32db [correct]
  [Checksum Status: Good]
  Unused: 00000000
▼ Internet Protocol Version 4, Src: 10.5.16.206, Dst: 10.5.16.205
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xae9a (44698)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▶ Time to Live: 2
    Protocol: UDP (17)
    Header Checksum: 0xd472 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.5.16.206
    Destination Address: 10.5.16.205

```

b) Ping unreachable host

```
user@user-Veriton-S2690G-D22E2:~$ ping 192.168.31.3
PING 192.168.31.3 (192.168.31.3) 56(84) bytes of data.
^C
--- 192.168.31.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3051ms
```

No-response packets:

535	36.535433	10.5.16.206	192.168.31.3	ICMP	98 Echo (ping) request	id=0x000e, seq=1/256, ttl=64 (no response found!)
543	37.538883	10.5.16.206	192.168.31.3	ICMP	98 Echo (ping) request	id=0x000e, seq=2/512, ttl=64 (no response found!)
555	38.562891	10.5.16.206	192.168.31.3	ICMP	98 Echo (ping) request	id=0x000e, seq=3/768, ttl=64 (no response found!)
565	39.586935	10.5.16.206	192.168.31.3	ICMP	98 Echo (ping) request	id=0x000e, seq=4/1024, ttl=64 (no response found!)

```
Source Address: 10.5.16.206
Destination Address: 192.168.31.3
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xb115 [correct]
  [Checksum Status: Good]
  Identifier (BE): 14 (0x000e)
  Identifier (LE): 3584 (0x0e00)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
▶ [No response seen]
```

- c) Traceroute tracks the path to a target host by sending packets with increasing TTL values (starting from 1). Each router decrements TTL, and when TTL hits zero, the router returns a TTL exceeded message. This process reveals the route, hop by hop, until the destination is reached or a maximum hop limit (default 30) is hit. By default, traceroute sends three probe packets to each hop in the path.

Tracerouting reachable host:

```
user@user-Veriton-S2690G-D22E2:~$ traceroute 10.145.187.17
traceroute to 10.145.187.17 (10.145.187.17), 30 hops max, 60 byte packets
 1 _gateway (10.5.16.2)  0.499 ms  0.469 ms  0.459 ms
 2 10.120.2.33 (10.120.2.33)  0.292 ms  0.338 ms  0.330 ms
 3 10.250.1.2 (10.250.1.2)  0.086 ms  0.118 ms  0.109 ms
 4 10.145.187.17 (10.145.187.17)  95.854 ms  95.843 ms  96.824 ms
```

```
876 84.617866 10.250.1.2 10.5.16.206 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
878 84.617907 10.250.1.2 10.5.16.206 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
879 84.617907 10.250.1.2 10.5.16.206 ICMP 102 Time-to-live exceeded (Time to live exceeded in transit)
883 84.618045 10.120.2.33 10.5.16.206 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
884 84.618100 10.120.2.33 10.5.16.206 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
885 84.618101 10.120.2.33 10.5.16.206 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
887 84.618202 10.5.16.2 10.5.16.206 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
888 84.618203 10.5.16.2 10.5.16.206 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
889 84.618203 10.5.16.2 10.5.16.206 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
901 84.713661 10.145.187.17 10.5.16.206 ICMP 102 Destination unreachable (Port unreachable)
902 84.713662 10.145.187.17 10.5.16.206 ICMP 102 Destination unreachable (Port unreachable)
904 84.714652 10.145.187.17 10.5.16.206 ICMP 102 Destination unreachable (Port unreachable)
906 84.720592 10.145.187.17 10.5.16.206 ICMP 102 Destination unreachable (Port unreachable)
907 84.720593 10.145.187.17 10.5.16.206 ICMP 102 Destination unreachable (Port unreachable)
908 84.722054 10.145.187.17 10.5.16.206 ICMP 102 Destination unreachable (Port unreachable)
```

Destination is reached in 4 hops. 9 ICMP packets with *TTL exceeded* response (3 packets each for 3 hops). 6 ICMP packets with *Port unreachable* response from the destination address (3 with TTL=1, 3 with TTL=2).

Tracerouting unreachable host:

```
user@user-Veriton-S2690G-D22E2:~$ traceroute 192.168.31.3
traceroute to 192.168.31.3 (192.168.31.3), 30 hops max, 60 byte packets
 1  _gateway (10.5.16.2)  0.593 ms  0.558 ms  0.546 ms
 2  10.120.2.33 (10.120.2.33)  0.331 ms  0.319 ms  0.308 ms
 3  10.255.1.3 (10.255.1.3)  2.747 ms  4.702 ms  3.370 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

1081	98.987158	10.120.2.33	10.5.16.206	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1082	98.987158	10.120.2.33	10.5.16.206	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1083	98.987158	10.120.2.33	10.5.16.206	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1087	98.987361	10.5.16.2	10.5.16.206	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1088	98.987362	10.5.16.2	10.5.16.206	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1089	98.987362	10.5.16.2	10.5.16.206	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
1091	98.989607	10.255.1.3	10.5.16.206	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
1092	98.990253	10.255.1.3	10.5.16.206	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
1094	98.991573	10.255.1.3	10.5.16.206	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)

Destination is not reached. 9 ICMP packets with *TTL exceeded* response (3 packets each for 3 hops). After that, no ICMP packets exchanged.