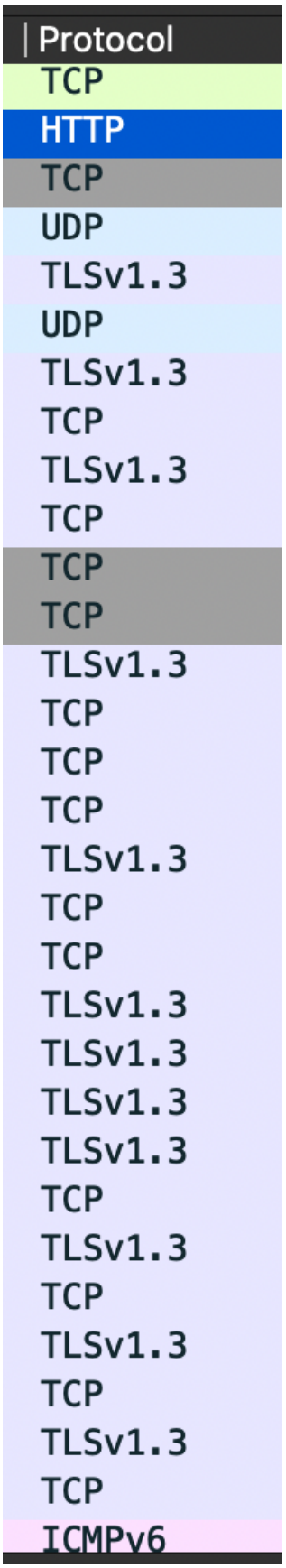
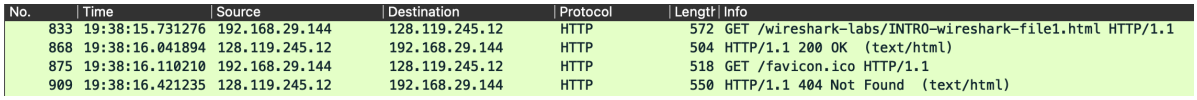
2019A7PS0134G_L2

- **QUESTION 1**
  - The different protocols include **TCP, TLSv1.2, SSDP, TLSv1.3,HTTP, ICMPV6**


Protocol
TCP
HTTP
TCP
UDP
TLSv1.3
UDP
TLSv1.3
TCP
TLSv1.3
TCP
TCP
TCP
TLSv1.3
TCP
TCP
TCP
TLSv1.3
TCP
TCP
TLSv1.3
TLSv1.3
TLSv1.3
TLSv1.3
TCP
TLSv1.3
TCP
TLSv1.3
TCP
TLSv1.3
TCP
ICMPv6

- **QUESTION 2**



No.	Time	Source	Destination	Protocol	Length	Info
833	19:38:15.731276	192.168.29.144	128.119.245.12	HTTP	572	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
868	19:38:16.041894	128.119.245.12	192.168.29.144	HTTP	504	HTTP/1.1 200 OK (text/html)
875	19:38:16.110210	192.168.29.144	128.119.245.12	HTTP	518	GET /favicon.ico HTTP/1.1
909	19:38:16.421235	128.119.245.12	192.168.29.144	HTTP	550	HTTP/1.1 404 Not Found (text/html)

The GET response is at time = 19:38:15:731276

The OK response is at time = 19:38:16:041894

Therefore, the time difference is **≈ 0.3seconds**

- **QUESTION 3**

Internet address of the gaia.cs.umass.edu : **128.119.245.12**

Internet address of the my laptop : **192.168.29.144**

- **QUESTION 4**

GET Request

/var/folders/g_/4d7_njz15hnfbqp75cb_ttm40000gn/T/wireshark_Wi-Fil4LZG1.pcapng 1364 total packets, 1364 shown

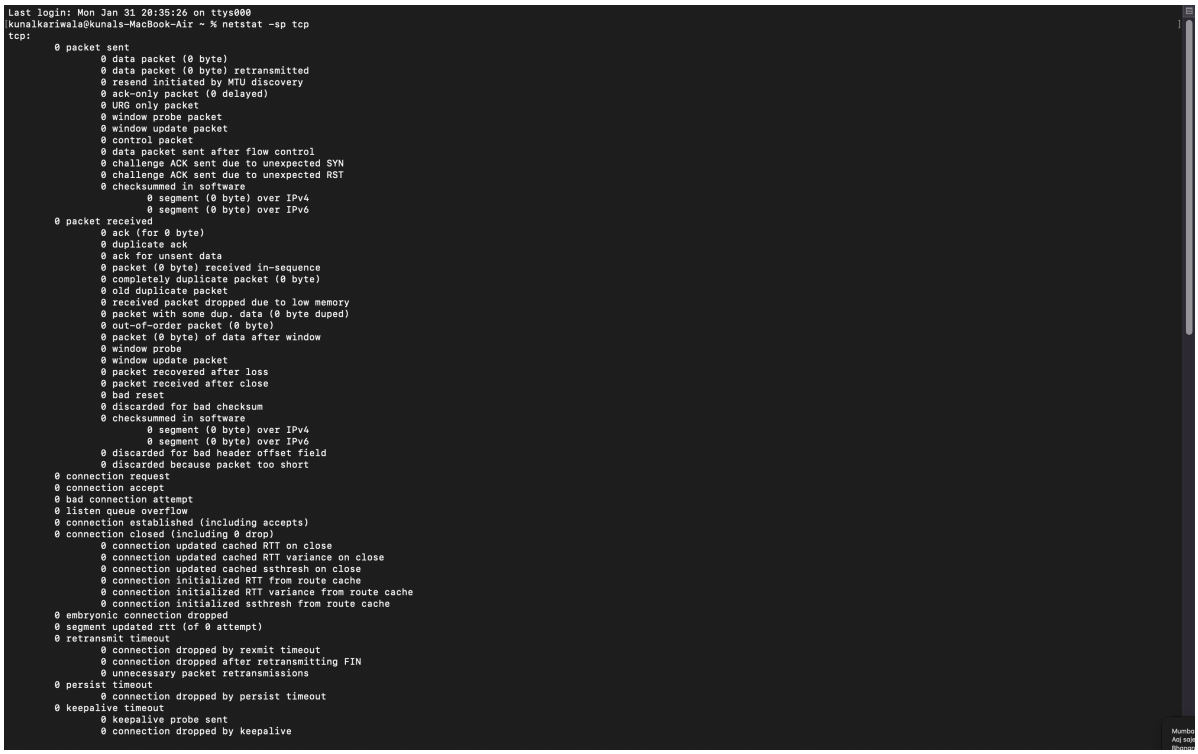
```
No.     Time               Source                Destination           Protocol Length Info
    833 19:38:15.731276    192.168.29.144        128.119.245.12        HTTP     572    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 833: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits) on interface en0, id 0
Ethernet II, Src: Apple_15:98:3d (b0:be:83:15:98:3d), Dst: Serverco_14:bf:02 (a8:da:0c:14:bf:
02)
Internet Protocol Version 4, Src: 192.168.29.144, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60144, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/97.0.4692.99 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Sec-GPC: 1\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
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 868]
    [Next request in frame: 875]
```

OK Request

```
/var/folders/g_/4d7_njz15hnfbqp75cb_ttm40000gn/T/wireshark_Wi-Fil4LZG1.pcapng 1364 total packets, 1364 shown

No.     Time               Source                Destination           Protocol Length Info
    868 19:38:16.041894    128.119.245.12        192.168.29.144        HTTP     504    HTTP/1.1
200 OK  (text/html)
Frame 868: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0
Ethernet II, Src: Serverco_14:bf:02 (a8:da:0c:14:bf:02), Dst: Apple_15:98:3d (b0:be:
83:15:98:3d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.29.144
Transmission Control Protocol, Src Port: 80, Dst Port: 60144, Seq: 1, Ack: 507, Len: 438
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: Mon, 31 Jan 2022 14:08:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/
v5.16.3\r\n
    Last-Modified: Mon, 31 Jan 2022 06:59:01 GMT\r\n
    ETag: "51-5d6db51c455ed"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\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 1/2]
    [Time since request: 0.310618000 seconds]
    [Request in frame: 833]
    [Next request in frame: 875]
    [Next response in frame: 909]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

- **QUESTION 5**

> This can be done on a Linux machine using the command **netstat -stu**
>
> On a unix machine, we can use **netstat -sp tcp** for TCP and **netstat -sp udp** for UDP

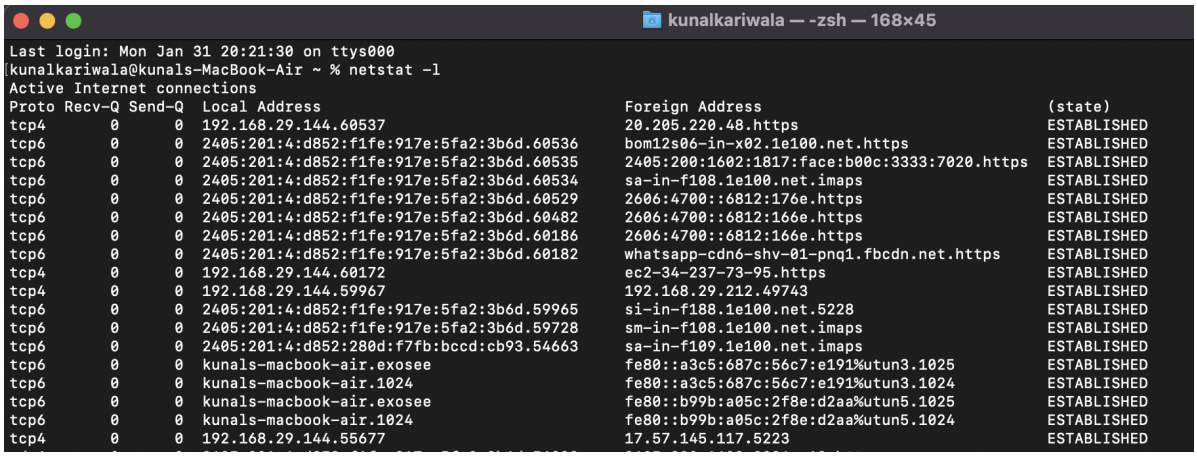


```
Last login: Mon Jan 31 20:35:26 on ttys000
kunalkariwala@kunals-MacBook-Air ~ % netstat -sp tcp
tcp:
        0 packet sent
                0 data packet (0 byte)
                0 data packet (0 byte) retransmitted
                0 resend initiated by MTU discovery
                0 ack-only packet (0 delayed)
                0 URG only packet
                0 window probe packet
                0 window update packet
                0 control packet
                0 data packet sent after flow control
                0 challenge ACK sent due to unexpected SYN
                0 challenge ACK sent due to unexpected RST
                0 checksummed in software
                        0 segment (0 byte) over IPv4
                        0 segment (0 byte) over IPv6
        0 packet received
                0 ack (for 0 byte)
                0 duplicate ack
                0 ack for unsent data
                0 packet (0 byte) received in-sequence
                0 completely duplicate packet (0 byte)
                0 old duplicate packet
                0 received packet dropped due to low memory
                0 packet with some dup. data (0 byte duped)
                0 out-of-order packet (0 byte)
                0 packet (0 byte) of data after window
                0 window probe
                0 window update packet
                0 packet recovered after loss
                0 packet received after close
                0 bad reset
                0 discarded for bad checksum
                0 checksummed in software
                        0 segment (0 byte) over IPv4
                        0 segment (0 byte) over IPv6
                0 discarded for bad header offset field
                0 discarded because packet too short
        0 connection request
        0 connection accept
        0 bad connection attempt
        0 listen queue overflow
        0 connection established (including accepts)
        0 connection closed (including 0 drop)
                0 connection updated cached RTT on close
                0 connection updated cached RTT variance on close
                0 connection updated cached ssthresh on close
                0 connection initialized RTT from route cache
                0 connection initialized RTT variance from route cache
                0 connection initialized ssthresh from route cache
        0 embryonic connection dropped
        0 segment updated rtt (of 0 attempt)
        0 retransmit timeout
                0 connection dropped by rexmit timeout
                0 connection dropped after retransmitting FIN
                0 unnecessary packet retransmissions
        0 persist timeout
                0 connection dropped by persist timeout
        0 keepalive timeout
                0 keepalive probe sent
                0 connection dropped by keepalive
```

```
kunalkariwala@kunals-MacBook-Air ~ % netstat -sp udp
udp:
        12645231 datagrams received
                0 with incomplete header
                0 with bad data length field
                0 with bad checksum
                4 with no checksum
                5963 checksummed in software
                        226 datagrams (57632 bytes) over IPv4
                        5737 datagrams (1147769 bytes) over IPv6
                3669 dropped due to no socket
                569 broadcast/multicast datagrams undelivered
                0 time multicast source filter matched
                0 dropped due to full socket buffers
                0 not for hashed pcb
                12640993 delivered
        2560809 datagrams output
                75139 checksummed in software
                        135 datagrams (40822 bytes) over IPv4
                        75004 datagrams (28759760 bytes) over IPv6
kunalkariwala@kunals-MacBook-Air ~ %
```

- **QUESTION 6**

> This can be done using **netstat -l**



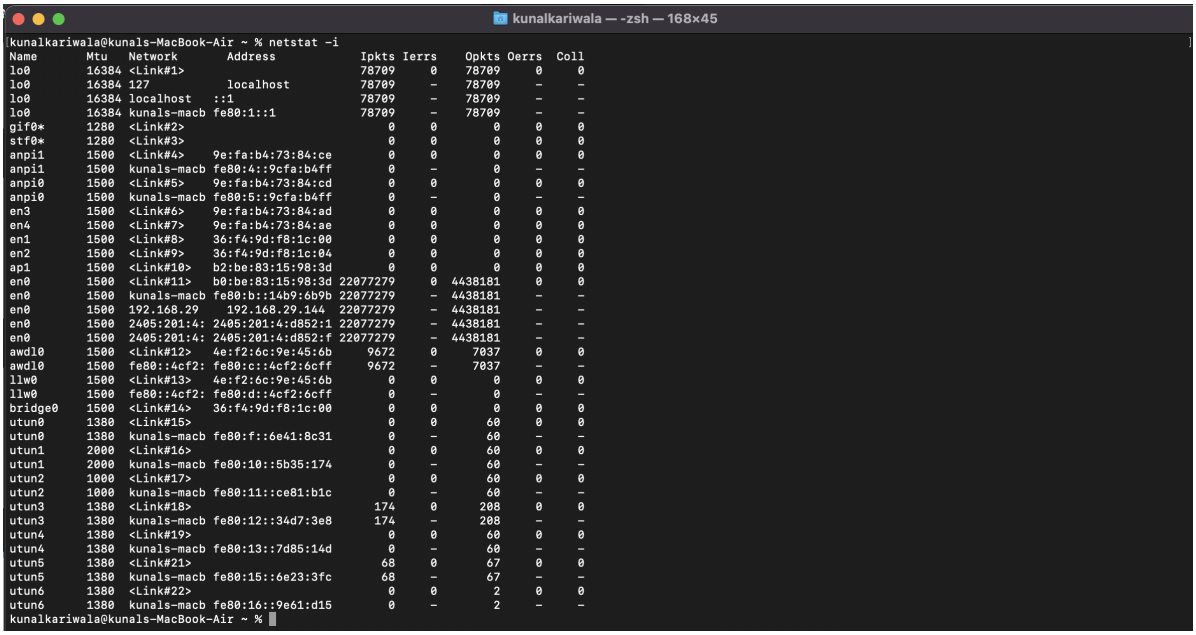
- **QUESTION 7**

> This can be done using **dig www.gmail.com MX**

```
kunalkariwala@kunals-MacBook-Air ~ % dig www.gmail.com MX

; <<>> DiG 9.10.6 <<>> www.gmail.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15627
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gmail.com.                 IN      MX

;; ANSWER SECTION:
www.gmail.com.          22000   IN      CNAME   mail.google.com.
mail.google.com.        116428  IN      CNAME   googlemail.l.google.com.

;; AUTHORITY SECTION:
l.google.com.           60      IN      SOA     ns1.google.com. dns-admin.google.com. 425175900 900 900 1800 60

;; Query time: 72 msec
;; SERVER: 2405:201:4:d852::c0a8:1d01#53(2405:201:4:d852::c0a8:1d01)
;; WHEN: Mon Jan 31 20:39:56 IST 2022
;; MSG SIZE  rcvd: 145
```

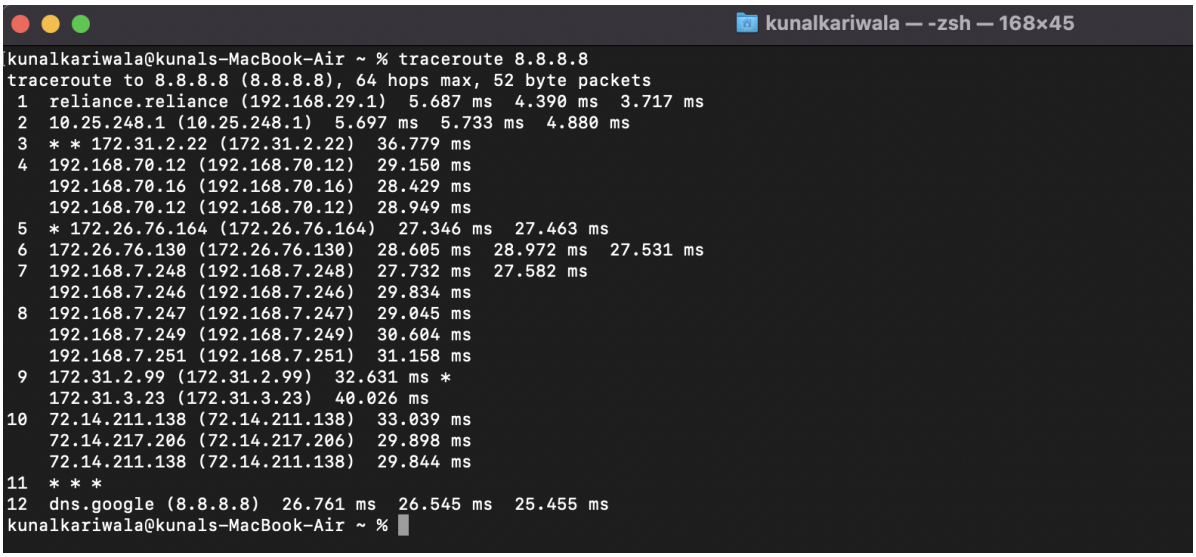
- **QUESTION 8**

> This can be done using **netstat -i**



- **QUESTION 9**

> This can be done using **traceroute 8.8.8.8**

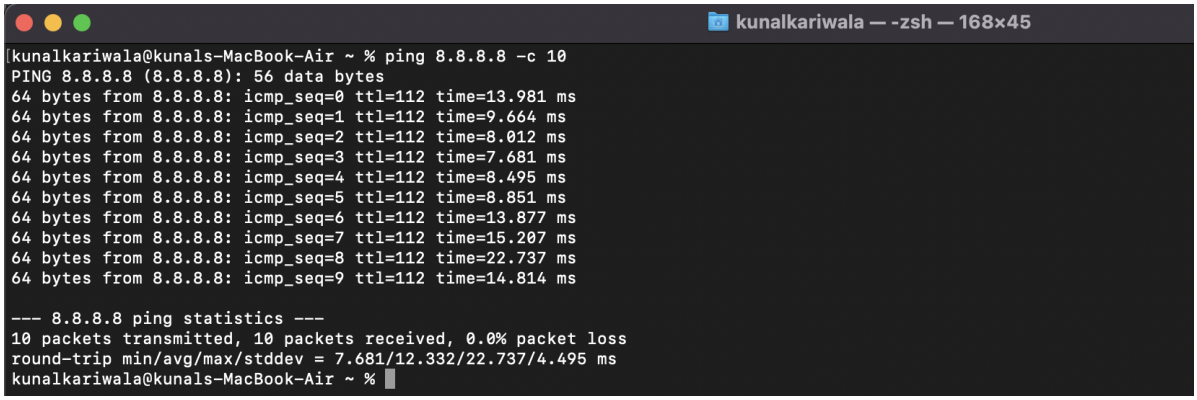


To read the latency:-

The times to the right hand side of every index can be used to get latency. It corresponds to the time required to send the packet to the address + time to return.

- **QUESTION 10**

> This can be done using **ping 8.8.8.8 -c 10**



- **QUESTION 11**

> This can be done using
> **nslookup www.bits-pilani.ac.in** or **dig www.bits-pilani.ac.in**