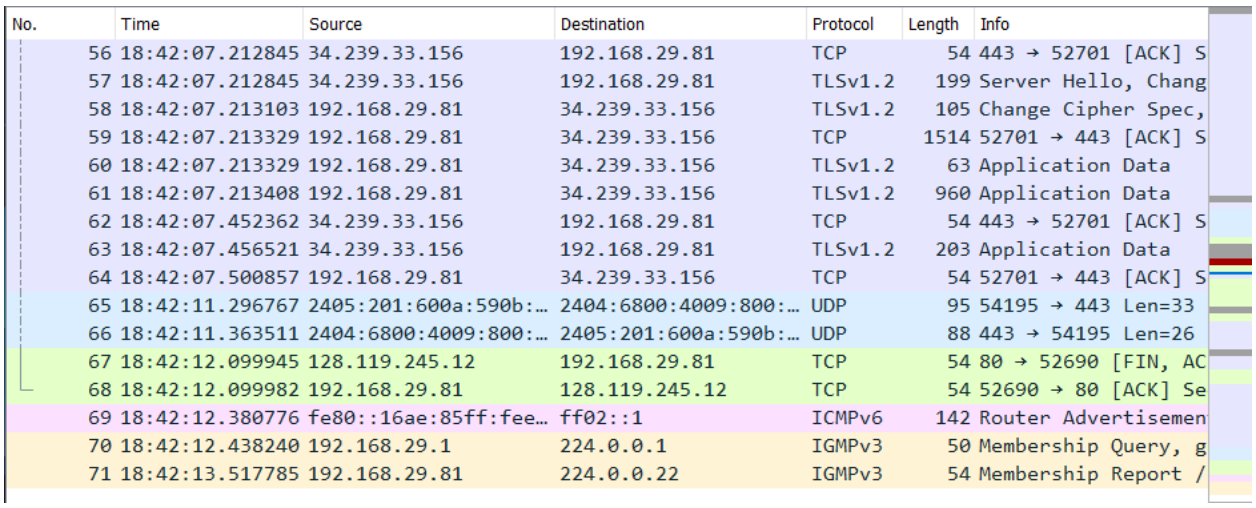
LAB 2 - Introduction to Wireshark and Use of Network Commands

NAME - DEV GOEL
ID - 2019A7PS0236G

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above. (1.5 marks)

Ans - 3 different protocols that occur are:

- TCP,
- UDP and
- IGMPv3



No.	Time	Source	Destination	Protocol	Length	Info
56	18:42:07.212845	34.239.33.156	192.168.29.81	TCP	54	443 → 52701 [ACK] S
57	18:42:07.212845	34.239.33.156	192.168.29.81	TLSv1.2	199	Server Hello, Chang
58	18:42:07.213103	192.168.29.81	34.239.33.156	TLSv1.2	105	Change Cipher Spec,
59	18:42:07.213329	192.168.29.81	34.239.33.156	TCP	1514	52701 → 443 [ACK] S
60	18:42:07.213329	192.168.29.81	34.239.33.156	TLSv1.2	63	Application Data
61	18:42:07.213408	192.168.29.81	34.239.33.156	TLSv1.2	960	Application Data
62	18:42:07.452362	34.239.33.156	192.168.29.81	TCP	54	443 → 52701 [ACK] S
63	18:42:07.456521	34.239.33.156	192.168.29.81	TLSv1.2	203	Application Data
64	18:42:07.500857	192.168.29.81	34.239.33.156	TCP	54	52701 → 443 [ACK] S
65	18:42:11.296767	2405:201:600a:590b:…	2404:6800:4009:800:…	UDP	95	54195 → 443 Len=33
66	18:42:11.363511	2404:6800:4009:800:…	2405:201:600a:590b:…	UDP	88	443 → 54195 Len=26
67	18:42:12.099945	128.119.245.12	192.168.29.81	TCP	54	80 → 52690 [FIN, AC
68	18:42:12.099982	192.168.29.81	128.119.245.12	TCP	54	52690 → 80 [ACK] Se
69	18:42:12.380776	fe80::16ae:85ff:fee…	ff02::1	ICMPv6	142	Router Advertisemen
70	18:42:12.438240	192.168.29.1	224.0.0.1	IGMPv3	50	Membership Query, g
71	18:42:13.517785	192.168.29.81	224.0.0.22	IGMPv3	54	Membership Report /

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet- listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.) (0.5 marks)

Ans -
The HTTP GET request was sent at 18:42:06.275160
Let this time be T_send = 18:42:06.275160

The HTTP OK request was received at 18:42:06.609869
Let this time be T_receive = 18:42:06.609869

Therefore, the difference in time is = T_receive - T_send = 0.334709 seconds

No.	Time	Source	Destination	Protocol	Length	Info
39	18:42:06.275160	192.168.29.81	128.119.245.12	HTTP	585	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
43	18:42:06.609869	128.119.245.12	192.168.29.81	HTTP	492	HTTP/1.1 200 OK (text/html)
46	18:42:06.764143	192.168.29.81	128.119.245.12	HTTP	531	GET /favicon.ico HTTP/1.1
54	18:42:07.094930	128.119.245.12	192.168.29.81	HTTP	538	HTTP/1.1 404 Not Found (text/html)

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer? (1 mark)

Ans -

The internet address of gaia.cs.umass.edu is 128.119.245.12
The internet address of my own computer is 192.168.29.81

No.	Time	Source	Destination	Protocol	Length	Info
39	18:42:06.275160	192.168.29.81	128.119.245.12	HTTP	585	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
43	18:42:06.609869	128.119.245.12	192.168.29.81	HTTP	492	HTTP/1.1 200 OK (text/html)
46	18:42:06.764143	192.168.29.81	128.119.245.12	HTTP	531	GET /favicon.ico HTTP/1.1
54	18:42:07.094930	128.119.245.12	192.168.29.81	HTTP	538	HTTP/1.1 404 Not Found (text/html)

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK. (1 mark)

Ans -

```
No.     Time               Source                Destination           Protocol Length Info
      2 19:02:35.330943    192.168.29.81         128.119.245.12        HTTP     579    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 2: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits) on interface \Device\NPF_{15DD42EB-6362-4EC8-BB13-C68F9E5C4528}, id
0
Ethernet II, Src: LiteonTe_4d:bb:cf (3c:91:80:4d:bb:cf), Dst: Sercomm_0c:f4:a3 (14:ae:85:ec:f4:a3)
Internet Protocol Version 4, Src: 192.168.29.81, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52816, Dst Port: 80, Seq: 1, Ack: 1, Len: 525
Hypertext Transfer Protocol
No.     Time               Source                Destination           Protocol Length Info
      7 19:02:35.655507    128.119.245.12        192.168.29.81         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 7: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{15DD42EB-6362-4EC8-BB13-C68F9E5C4528}, id
0
Ethernet II, Src: Sercomm_0c:f4:a3 (14:ae:85:ec:f4:a3), Dst: LiteonTe_4d:bb:cf (3c:91:80:4d:bb:cf)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.29.81
Transmission Control Protocol, Src Port: 80, Dst Port: 52816, Seq: 1, Ack: 526, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

---

5. How do you see the statistics of TCP and UDP ports on Linux machines? (1 mark)

Ans -
The `**netstat**` command is used to view the network statistics on Linux.
Specifically, the command `**netstat -st**` can be used to list statistics for TCP ports,
and the command `**netstat -st**` can be used to list statistics for UDP ports.

```
goeldev@pop-os:~$ netstat -st
IcmpMsg:
    InType3: 40
    OutType3: 100
Tcp:
    718 active connection openings
    1 passive connection openings
    4 failed connection attempts
    119 connection resets received
    20 connections established
    128901 segments received
    103216 segments sent out
    274 segments retransmitted
    5 bad segments received
    469 resets sent
UdpLite:
TcpExt:
    179 TCP sockets finished time wait in fast timer
    209 packetes rejected in established connections because of timestamp
    229 delayed acks sent
    1 delayed acks further delayed because of locked socket
    Quick ack mode was activated 1614 times
    67824 packet headers predicted
    5478 acknowledgments not containing data payload received
    5624 predicted acknowledgments
    TCPSackRecovery: 19
    Detected reordering 1 times using SACK
    TCPDSACKUndo: 9
    5 congestion windows recovered without slow start after partial ack
    TCPSackFailures: 1
    36 fast retransmits
    TCPTimeouts: 18
    TCPLossProbes: 223
    TCPLossProbeRecovery: 10
    TCPSackRecoveryFail: 1
    TCPBacklogCoalesce: 52
    TCPDSACKOldSent: 1641
    TCPDSACKOfoSent: 94
    TCPDSACKRecv: 180
    TCPDSACKOfoRecv: 1
    102 connections reset due to unexpected data
    37 connections reset due to early user close
```

```
goeldev@pop-os:~$ netstat -su
IcmpMsg:
    InType3: 40
    OutType3: 100
Udp:
    15447 packets received
    100 packets to unknown port received
    36 packet receive errors
    7831 packets sent
    36 receive buffer errors
    1 send buffer errors
    IgnoredMulti: 1392
UdpLite:
IpExt:
    InMcastPkts: 2420
    OutMcastPkts: 704
    InBcastPkts: 1570
    OutBcastPkts: 200
    InOctets: 77149694
    OutOctets: 3087222
    InMcastOctets: 651370
    OutMcastOctets: 74838
    InBcastOctets: 111953
    OutBcastOctets: 14502
    InNoECTPkts: 68810
MPTcpExt:
goeldev@pop-os:~$
```

---

6. How do you enlist the listening ports on your machine? (1 mark)

Ans -
`netstat -l` command lists all the listening ports on the machine. The screenshot below shows the listening ports on my machine.

```
goeldev@pop-os:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:6463          0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:51951           0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:57621           0.0.0.0:*               LISTEN
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:41236           0.0.0.0:*
udp        0      0 0.0.0.0:57621           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:1900            0.0.0.0:*
udp        0      0 0.0.0.0:43211           0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 pop-os:dhcpv6-client    [::]:*
udp6       0      0 [::]:44318              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     25834    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     42228    /tmp/ssh-waK7k1NAWiAk/agent.1953
unix  2      [ ACC ]     STREAM     LISTENING     36721    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     38534    /run/user/110/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     36726    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     38539    /run/user/110/bus
unix  2      [ ACC ]     STREAM     LISTENING     36727    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     38540    /run/user/110/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     36728    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     38541    /run/user/110/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     36729    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     38542    /run/user/110/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     36730    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     38543    /run/user/110/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     36731    /run/user/1000/gnupg/S.gpg-agent
```

7. How do you see the mail xchange (MX) record for www.gmail.com . (2 marks)

Ans -

The command `**nslookup**` can be used to query internet domain name servers. With the query type set as ‘mx’ (mail exchange), we can see the mail exchange record for the given server. The screenshot below shows the nslookup command. The `**set type=mx**` is used to change the type of information query to ‘mx’.

For the below operation, we can also use the shorthand `**nslookup -q=mx gmail.com**`

```
goeldev@pop-os:~$ nslookup
> set type=mx
> gmail.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
gmail.com       mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 5 gmail-smtp-in.l.google.com.
```

---

8. Display the all network interfaces on your machine. (2 marks)

Ans -

The command `**ifconfig -a**` displays all the network interfaces on the machine which are currently available, even if they are down.

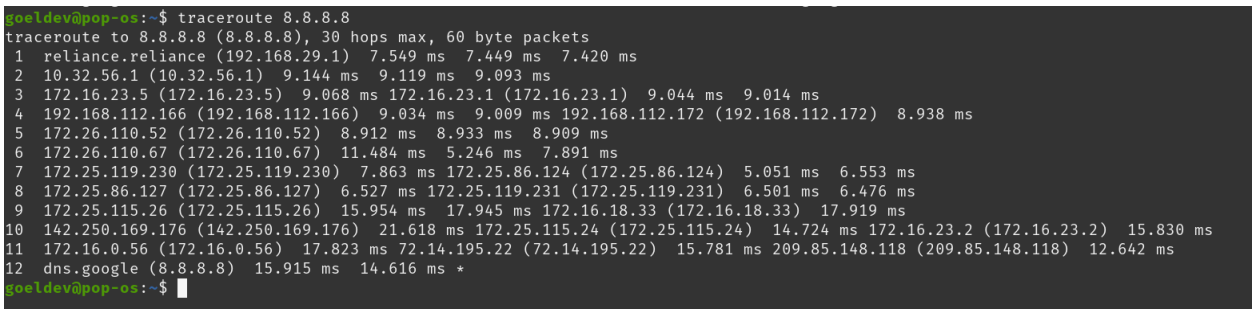
```
goeldev@pop-os:~$ ifconfig -a
enp8s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 98:fa:9b:02:a5:6b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 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 896  bytes 87988 (87.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 896  bytes 87988 (87.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp7s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.29.81  netmask 255.255.255.0  broadcast 192.168.29.255
        inet6 fe80::5bed:5d4e:fa44:5090  prefixlen 64  scopeid 0x20<link>
        inet6 2405:201:600a:590b:9eb2:9205:1f67:992f  prefixlen 64  scopeid 0x
0<global>
        inet6 2405:201:600a:590b:5149:d4a3:bdd2:f35b  prefixlen 64  scopeid 0x
0<global>
        ether 3c:91:80:4d:bb:cf  txqueuelen 1000  (Ethernet)
        RX packets 40746  bytes 49060883 (49.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17687  bytes 3443860 (3.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

9. How do you find the list of intermediate routers to reach 8.8.8.8 from your machine? How do you read the latency. (2 marks)

Ans -

`**traceroute**` command tracks the route packets taken from an IP network on their way to a given host.

To read the latency we observe the three values that are specified after the domain address in each row representing each hop. These values are the amount of time taken (in milliseconds), for a packet to get to the hop address and back to our computer. The command sends three such packets to each hop, corresponding to these three values we see in the screenshot below. Using these three values we can measure how consistent the latency is at that time.



10. How do you send 10 Echo requests to the 8.8.8.8 server from your machine? (1 mark)

Ans -
Using the `**ping**` command we can send ECHO_REQUEST to a host or gateway.

```
goeldev@pop-os:~$ ping 8.8.8.8 -c 10
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=34.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=21.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=14.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=14.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=14.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=111 time=14.6 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=111 time=14.6 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=111 time=13.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=111 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=111 time=19.5 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 13.782/17.700/34.716/6.205 ms
goeldev@pop-os:~$
```

---

11. How do you get the IP address of www.bits-pilani.ac.in domain? (1 mark)

Ans -
The IP address can be found using the `**nslookup**` command. The IP address for the given domain is 127.0.0.53.

```
goeldev@pop-os:~$ nslookup www.bits-pilani.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.bits-pilani.ac.in   canonical name = universe.bits-pilani.ac.in.
Name:   universe.bits-pilani.ac.in
Address: 14.139.243.20
Name:   universe.bits-pilani.ac.in
Address: 103.144.92.33

goeldev@pop-os:~$
```
