CO-223

LABORATORY SESSION 2

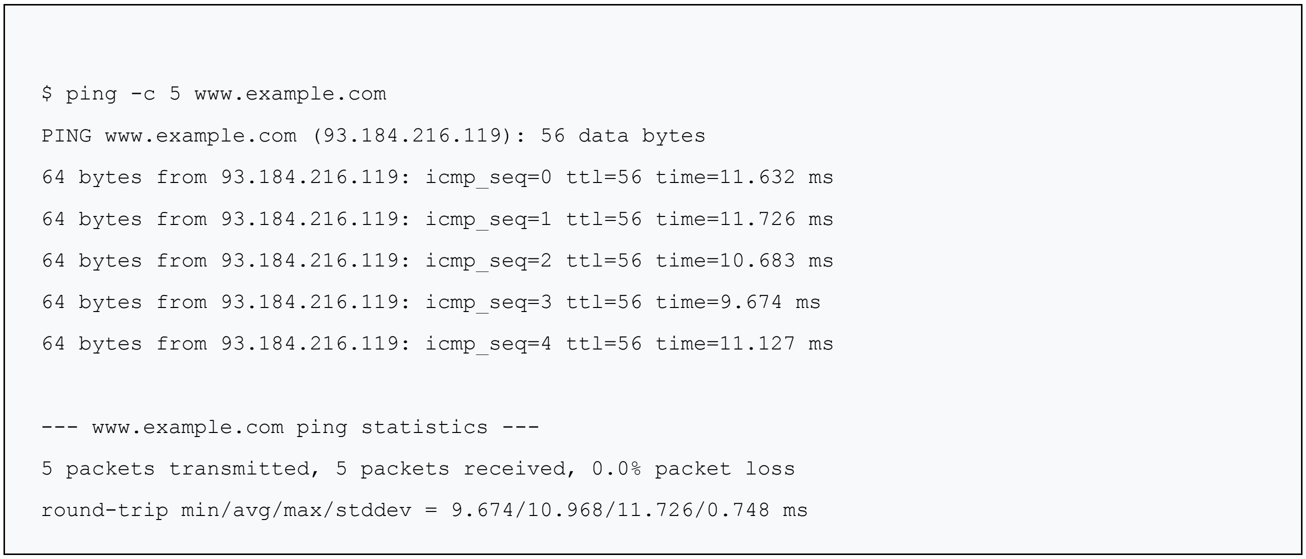
NAME	:	WIMALASIRI KPGP
REG NO	:	E/14/403
SEMESTER	:	3RD
GROUP	:	15
DATE	:	06/02/2017

Part-1 Network tools

a) Ping

- Ping is a network utility tool that provides information about the reachability of a host over an Internet Protocol network. This tool work by sending ICMP (Internet Control Message Protocol) to the target host, waiting for the echo reply of it and analyzing the time taken and the echo received. By using ‘ping’ not only the time, but also the number of network hops to the host can be discovered. (Number of network hops is equal to the number of routers that passed through)

  In order to do the pinging of a certain host address first of all the command ‘ping’ and the host address (IP address) should be entered to the ‘cmd’ in windows or ‘terminal’ in the Linux OS. Then the ICMP packet transfer process starts. In windows it normally stops after 4 packet transfers. In Linux OS process should be terminated by pressing ctrl+c.



```
$ ping -c 5 www.example.com
PING www.example.com (93.184.216.119): 56 data bytes
64 bytes from 93.184.216.119: icmp_seq=0 ttl=56 time=11.632 ms
64 bytes from 93.184.216.119: icmp_seq=1 ttl=56 time=11.726 ms
64 bytes from 93.184.216.119: icmp_seq=2 ttl=56 time=10.683 ms
64 bytes from 93.184.216.119: icmp_seq=3 ttl=56 time=9.674 ms
64 bytes from 93.184.216.119: icmp_seq=4 ttl=56 time=11.127 ms

--- www.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.674/10.968/11.726/0.748 ms
```

Figure 1

- Figure 1 shows the resulting text of the previous procedure when using Linux OS. In here each ICMP packet is 64 bytes. The term ‘icmp seq’ means the order of packets. This sequence can be changed as the packets are transferred in different routes. Term ‘ttl’ is referred to ‘time to live’, which is an indication of number of routers, passed through while the packet transferring. The ttl number can be defined earlier. If the ttl number decreases more while transferring, the number of network hops is greater to the host. If the ttl value is zero when a packet transfer through a router, that packet is discarded. The time shown in above figure is the total time that taken to the round trip. At the end there is a statistics report which shows the number of total transmitted packets, the number of received packets and the lost percentage. It shows the minimum, maximum, average and the deviation time that is taken to the round trip.

- With the help of the given time values the delay can be measured. Both delay and jitter can be measured using this data, as there are distinct values of time taken by each packet while transferring from client to host. Delay can be measured by multiplying the average time by the total packet transferred. We can get an idea about jitter value with the help of the value of deviation time. But in here the four sources of packet delay (nodal processing, queuing, transmission and propagation) can't be recognize separately. The delay shown here is the total of each type.
- Delay measurement in the network = avg. round trip time / 2
  = 10.968ms / 2
  = 5.484ms**

**This measurement is according to the example given in figure 1.

b) Traceroute (or tracert)

- Traceroute (or tracert) is a known as a network diagnostic tool which display paths and the transit delays of packets transferring. With the help of this traceroute (or tracert) tool the network interfaces in between the local computer and the host and the routing time (round trip time) of data packets to each network interface can be identified. By default traceroute tool sends 3 data packets to measure time with respect to a certain network interface.

```
traceroute google.com
traceroute to google.com (172.217.23.14), 30 hops max, 60 byte packets
 1  10.8.8.1 (10.8.8.1)  14.499 ms  15.335 ms  15.956 ms
 2  h37-220-13-49.host.redstation.co.uk (37.220.13.49)  17.811 ms  18.669 ms  19.346 ms
 3  92.zone.2.c.dc9.redstation.co.uk (185.20.96.137)  19.096 ms  19.757 ms  20.892 ms
 4  203.lc3.redstation.co.uk (185.5.3.221)  28.160 ms  28.415 ms  28.665 ms
 5  100.core1.the.as20860.net (62.128.218.33)  26.739 ms  27.840 ms  28.847 ms
 6  110.core2.thn.as20860.net (62.128.218.26)  29.112 ms  18.466 ms  19.835 ms
 7  be97.asr01.thn.as20860.net (62.128.222.205)  19.986 ms  20.488 ms  21.354 ms
 8  * * *
 9  216.239.48.143 (216.239.48.143)  24.364 ms 216.239.48.113 (216.239.48.113)  25.069 ms  25.592 ms
10  108.170.233.199 (108.170.233.199)  26.239 ms  27.369 ms  28.031 ms
11  lhr35s01-in-f14.1e100.net (172.217.23.14)  28.642 ms  29.311 ms  29.815 ms
```

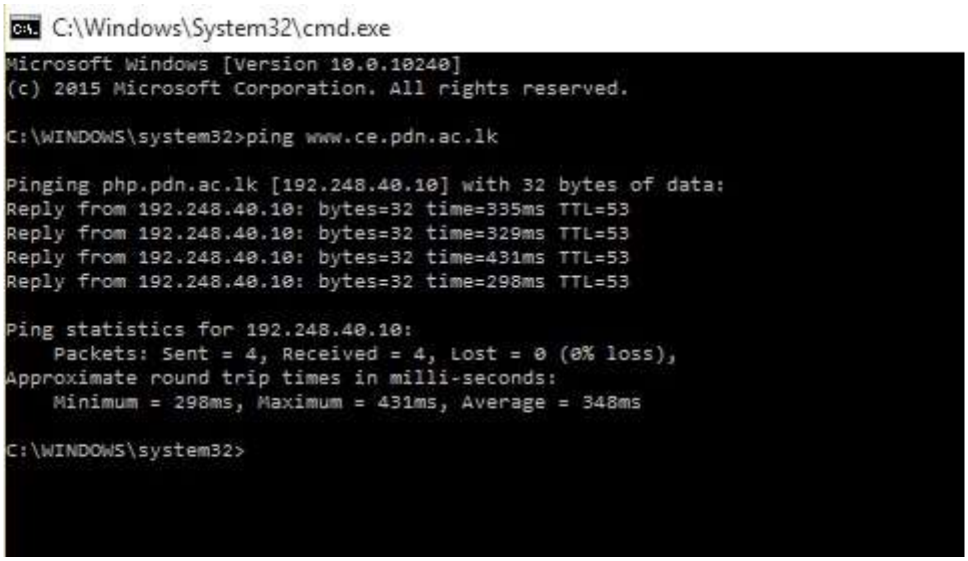
Figure 2

There are differences between the ping tool and the traceroute tool. When using ping tool the time measurements are taken considering whole route, the time taken to transfer a data packet from local to the host. But in traceroute it's about the time taken to transfer a data packet from local to each intermediate network interfaces.

- In above example (figure 2) the maximum number of hops are limited to 30, which means that a host over 30 hops might not be connected through this. The size of the transferring packet is given next to that as '60 byte packets'. After that list of hops are given. The host names also given (if there is) with the IP addresses and the time values which the three packets are taken to complete the route to the particular network interface. Three star marks ('*') in 8th line indicates that the packets sent, are lost.
- This tool provides time measurements of data transferring to each hops in between the host and the local. Therefore, the total of nodal processing, queuing, transmission and propagation delay between any to network interfaces can be interpreted using these values. Total delay and some idea about jitter also can be gain by this method as it sends 3 packets in a row to the same network interface.
- Delay measurement in the network = avg. round time value / 2
  = {(28.642+29.311+29.815)ms / 3} / 2
  = 14.628 ms**

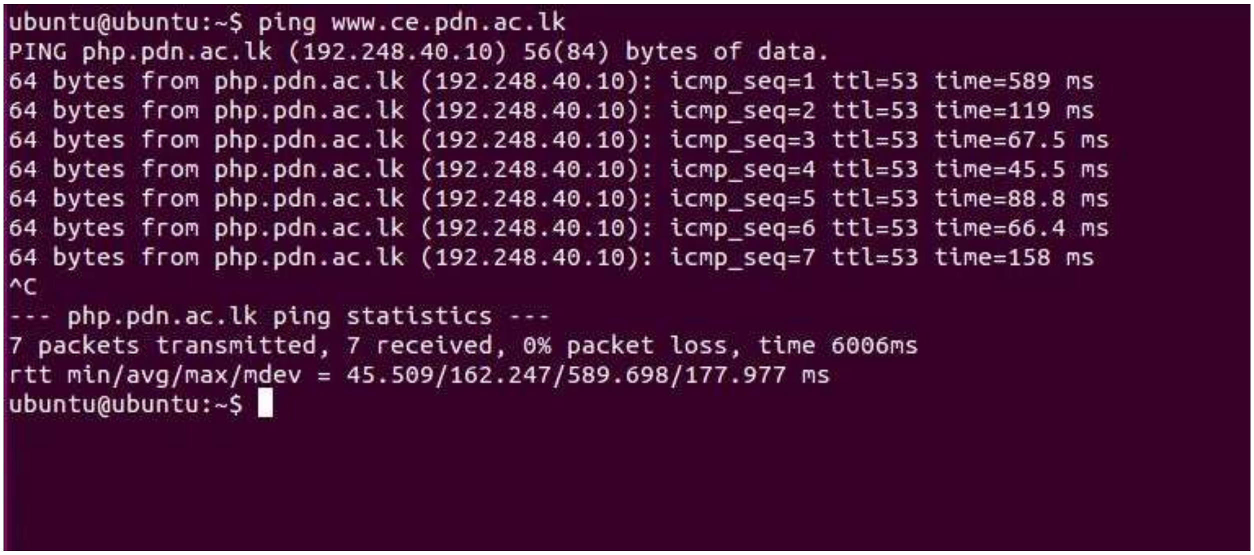
  (Considering the last IP address in the list)
  **This measurement is according to the example given in figure 2.

c) (1) ping test for www.ce.pdn.ac.lk



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.ce.pdn.ac.lk

Pinging php.pdn.ac.lk [192.248.40.10] with 32 bytes of data:
Reply from 192.248.40.10: bytes=32 time=335ms TTL=53
Reply from 192.248.40.10: bytes=32 time=329ms TTL=53
Reply from 192.248.40.10: bytes=32 time=431ms TTL=53
Reply from 192.248.40.10: bytes=32 time=298ms TTL=53

Ping statistics for 192.248.40.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 298ms, Maximum = 431ms, Average = 348ms

C:\WINDOWS\system32>
```

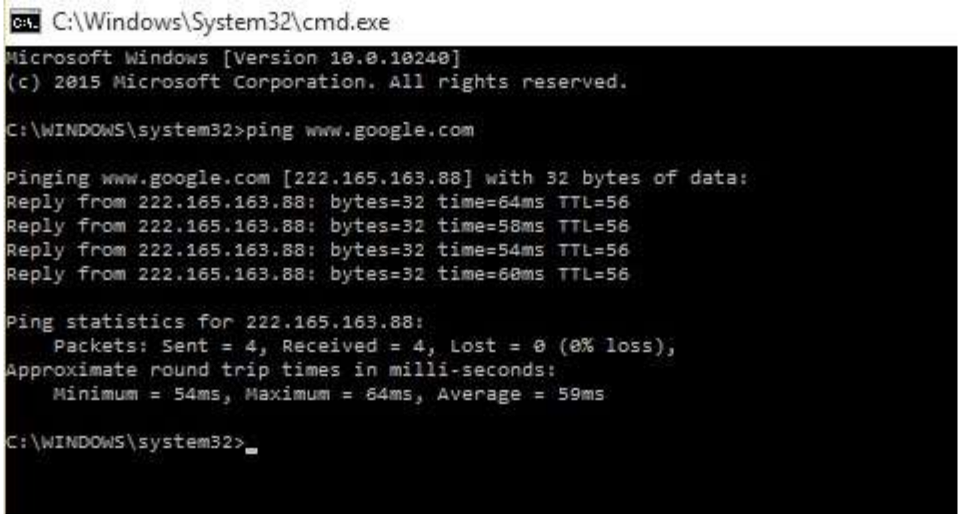
Figure 3



```
ubuntu@ubuntu:~$ ping www.ce.pdn.ac.lk
PING php.pdn.ac.lk (192.248.40.10) 56(84) bytes of data.
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=1 ttl=53 time=589 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=2 ttl=53 time=119 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=3 ttl=53 time=67.5 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=4 ttl=53 time=45.5 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=5 ttl=53 time=88.8 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=6 ttl=53 time=66.4 ms
64 bytes from php.pdn.ac.lk (192.248.40.10): icmp_seq=7 ttl=53 time=158 ms
^C
--- php.pdn.ac.lk ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 45.509/162.247/589.698/177.977 ms
ubuntu@ubuntu:~$
```

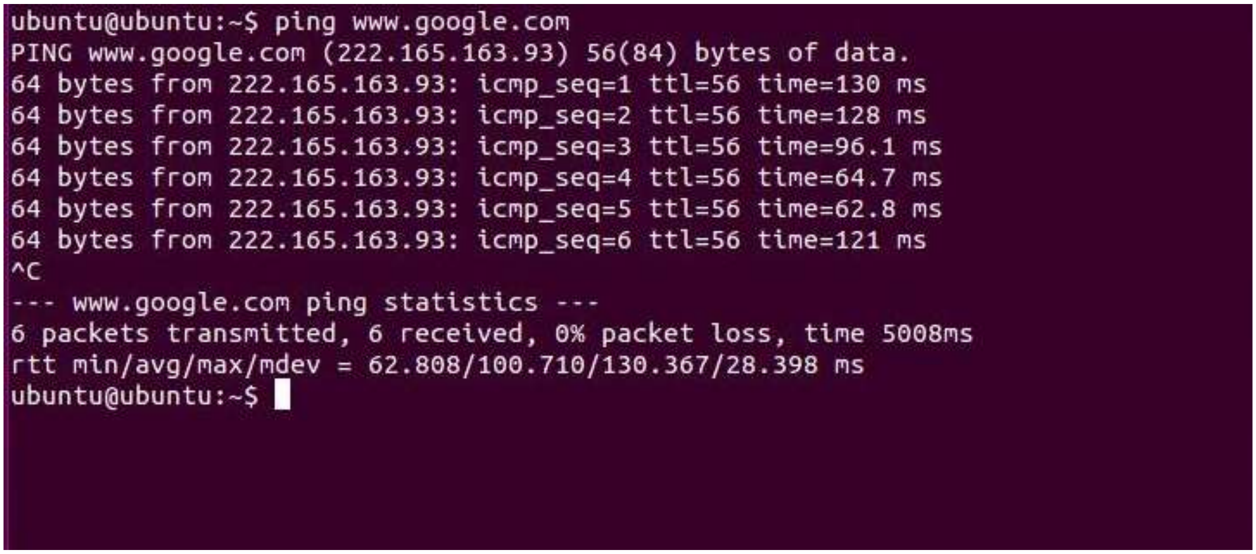
Figure 4

(2) ping test for www.google.com



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.google.com

Pinging www.google.com [222.165.163.88] with 32 bytes of data:
Reply from 222.165.163.88: bytes=32 time=64ms TTL=56
Reply from 222.165.163.88: bytes=32 time=58ms TTL=56
Reply from 222.165.163.88: bytes=32 time=54ms TTL=56
Reply from 222.165.163.88: bytes=32 time=60ms TTL=56

Ping statistics for 222.165.163.88:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 64ms, Average = 59ms

C:\WINDOWS\system32>_
```

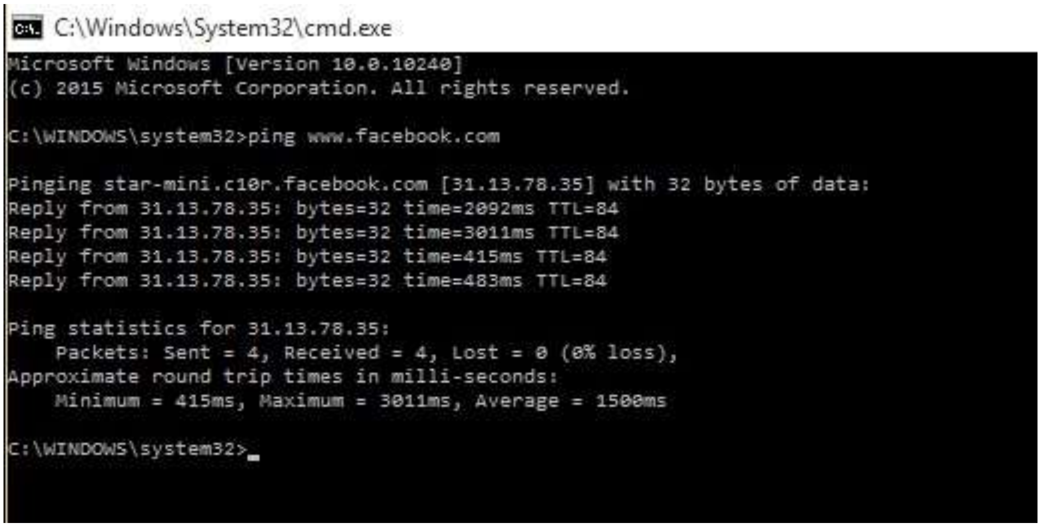
Figure 5



```
ubuntu@ubuntu:~$ ping www.google.com
PING www.google.com (222.165.163.93) 56(84) bytes of data.
64 bytes from 222.165.163.93: icmp_seq=1 ttl=56 time=130 ms
64 bytes from 222.165.163.93: icmp_seq=2 ttl=56 time=128 ms
64 bytes from 222.165.163.93: icmp_seq=3 ttl=56 time=96.1 ms
64 bytes from 222.165.163.93: icmp_seq=4 ttl=56 time=64.7 ms
64 bytes from 222.165.163.93: icmp_seq=5 ttl=56 time=62.8 ms
64 bytes from 222.165.163.93: icmp_seq=6 ttl=56 time=121 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 62.808/100.710/130.367/28.398 ms
ubuntu@ubuntu:~$
```

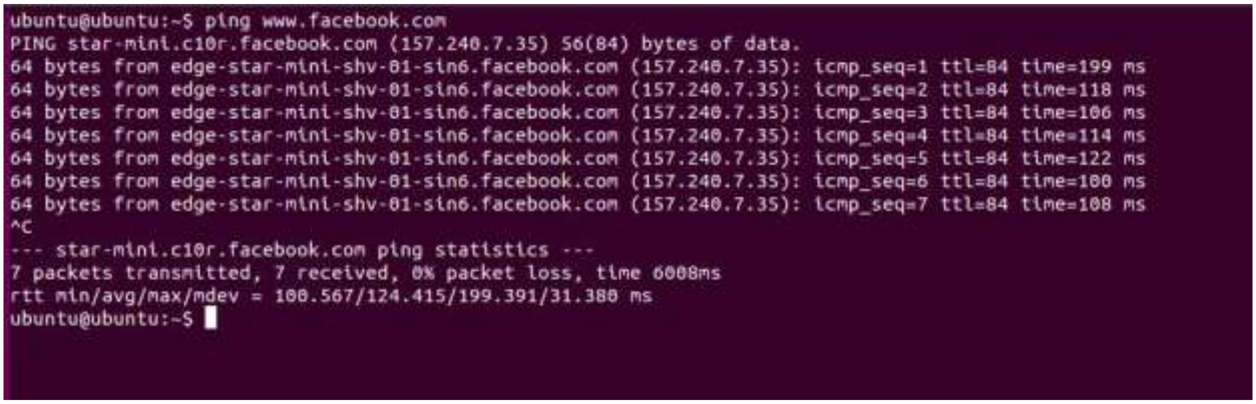
Figure 6

(3) ping test for www.facebook.com



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [31.13.78.35] with 32 bytes of data:
Reply from 31.13.78.35: bytes=32 time=2092ms TTL=84
Reply from 31.13.78.35: bytes=32 time=3011ms TTL=84
Reply from 31.13.78.35: bytes=32 time=415ms TTL=84
Reply from 31.13.78.35: bytes=32 time=483ms TTL=84

Ping statistics for 31.13.78.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 415ms, Maximum = 3011ms, Average = 1500ms

C:\WINDOWS\system32>_
```

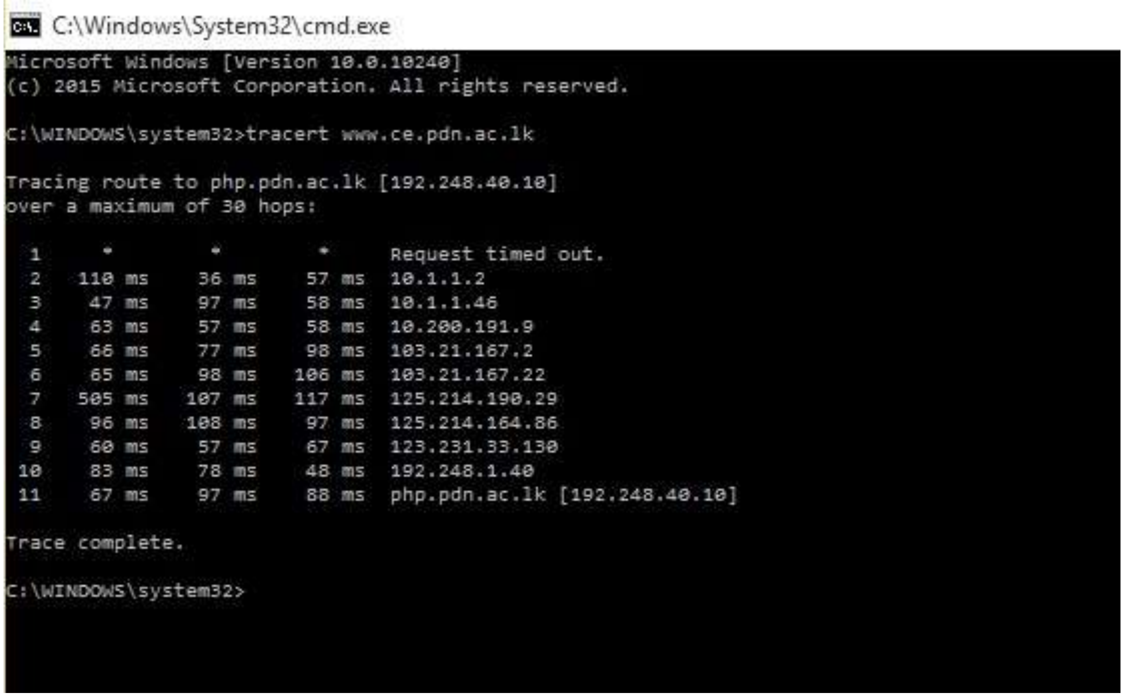
Figure 7



```
ubuntu@ubuntu:~$ ping www.facebook.com
PING star-mini.c10r.facebook.com (157.240.7.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35): icmp_seq=1 ttl=84 time=199 ms
64 bytes from edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35): icmp_seq=2 ttl=84 time=118 ms
64 bytes from edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35): icmp_seq=3 ttl=84 time=106 ms
64 bytes from edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35): icmp_seq=4 ttl=84 time=114 ms
64 bytes from edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35): icmp_seq=5 ttl=84 time=122 ms
64 bytes from edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35): icmp_seq=6 ttl=84 time=100 ms
64 bytes from edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35): icmp_seq=7 ttl=84 time=108 ms
^C
--- star-mini.c10r.facebook.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 100.567/124.415/199.391/31.380 ms
ubuntu@ubuntu:~$ 
```

Figure 8

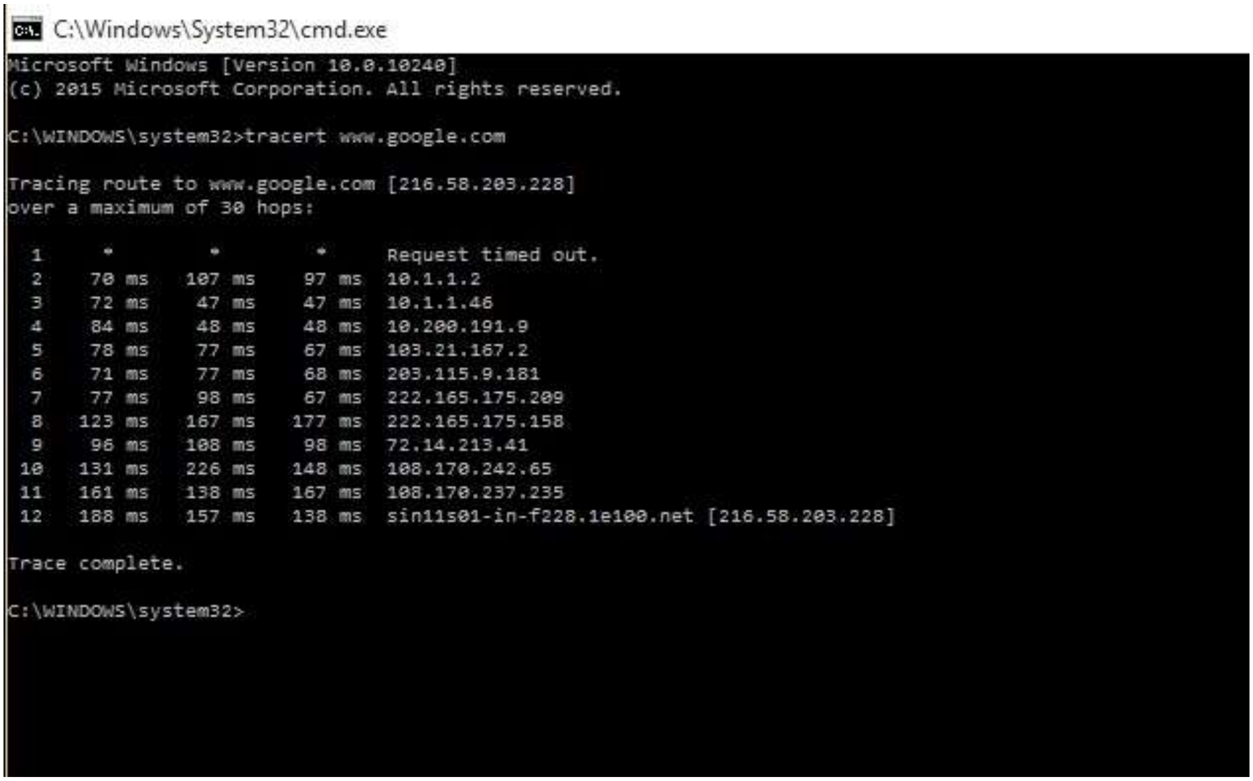
a) tracert test for www.ce.pdn.ac.lk



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert www.ce.pdn.ac.lk

Tracing route to php.pdn.ac.lk [192.248.40.10]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2   110 ms    36 ms    57 ms  10.1.1.2
  3    47 ms    97 ms    58 ms  10.1.1.46
  4    63 ms    57 ms    58 ms  10.200.191.9
  5    66 ms    77 ms    98 ms  103.21.167.2
  6    65 ms    98 ms   106 ms  103.21.167.22
  7   505 ms   107 ms   117 ms  125.214.190.29
  8    96 ms   108 ms    97 ms  125.214.164.86
  9    60 ms    57 ms    67 ms  123.231.33.130
 10    83 ms    78 ms    48 ms  192.248.1.40
 11    67 ms    97 ms    88 ms  php.pdn.ac.lk [192.248.40.10]

Trace complete.

C:\WINDOWS\system32>
```

Figure 9

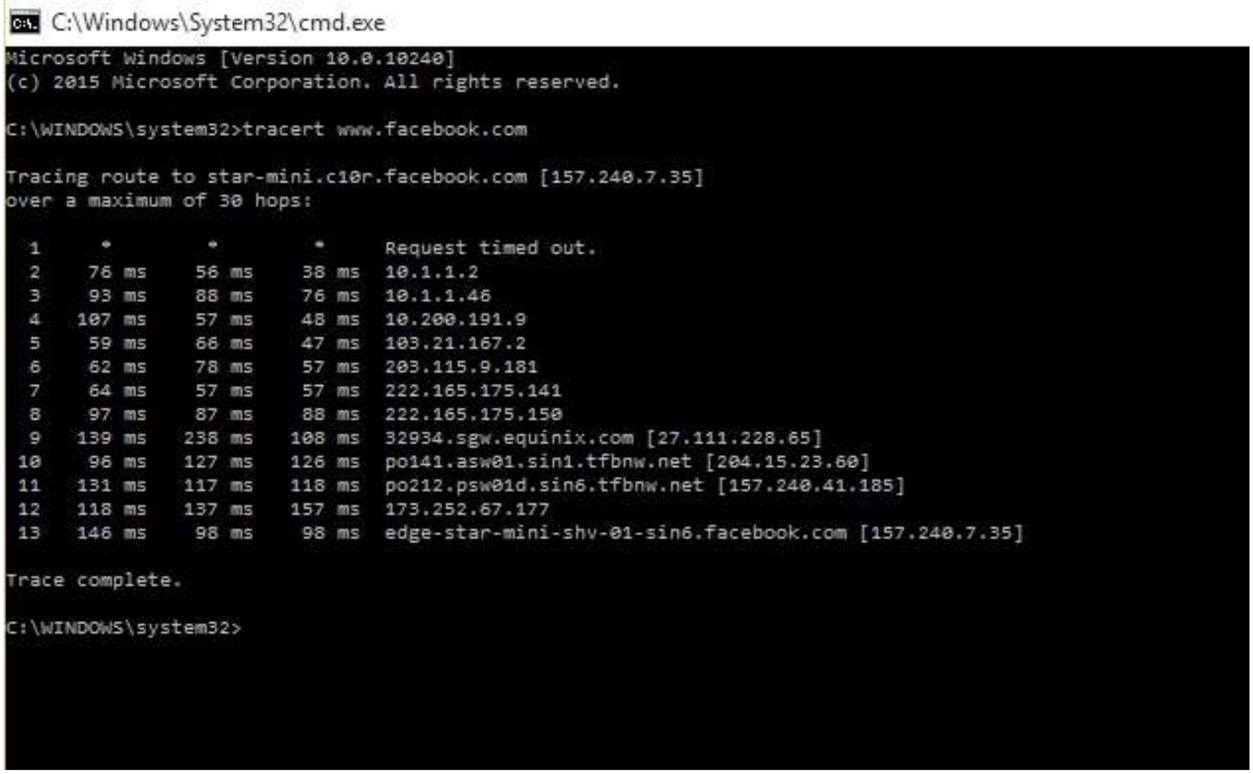
b) tracert test for www.google.com



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert www.google.com

Tracing route to www.google.com [216.58.203.228]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2    70 ms   107 ms    97 ms  10.1.1.2
  3    72 ms    47 ms    47 ms  10.1.1.46
  4    84 ms    48 ms    48 ms  10.200.191.9
  5    78 ms    77 ms    67 ms  103.21.167.2
  6    71 ms    77 ms    68 ms  203.115.9.181
  7    77 ms    98 ms    67 ms  222.165.175.209
  8   123 ms   167 ms   177 ms  222.165.175.158
  9    96 ms   108 ms    98 ms  72.14.213.41
 10   131 ms   226 ms   148 ms  108.170.242.65
 11   161 ms   138 ms   167 ms  108.170.237.235
 12   188 ms   157 ms   138 ms  sin11s01-in-f228.1e100.net [216.58.203.228]

Trace complete.

C:\WINDOWS\system32>
```

Figure 10

c) tracert test for www.facebook.com



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [157.240.7.35]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2    76 ms    56 ms    38 ms  10.1.1.2
  3    93 ms    88 ms    76 ms  10.1.1.46
  4   107 ms    57 ms    48 ms  10.200.191.9
  5    59 ms    66 ms    47 ms  103.21.167.2
  6    62 ms    78 ms    57 ms  203.115.9.181
  7    64 ms    57 ms    57 ms  222.165.175.141
  8    97 ms    87 ms    88 ms  222.165.175.150
  9   139 ms   238 ms   108 ms  32934.sgw.equinix.com [27.111.228.65]
 10    96 ms   127 ms   126 ms  po141.asw01.sin1.tfbnw.net [204.15.23.60]
 11   131 ms   117 ms   118 ms  po212.psw01d.sin6.tfbnw.net [157.240.41.185]
 12   118 ms   137 ms   157 ms  173.252.67.177
 13   146 ms    98 ms    98 ms  edge-star-mini-shv-01-sin6.facebook.com [157.240.7.35]

Trace complete.

C:\WINDOWS\system32>
```

Figure 11

- Calculations in the table below are considering figure 3, figure 5, figure 9 and figure 10

	Host	Delay measurement using ping tool / ms	Delay measurement using tracert tool / ms
(1)	www.ce.pdn.ac.lk	(348 ms)/2 = 174 ms	{(67+97+88)ms/3}/2 = 42 ms
(2)	www.google.com	(59 ms)/2 = 29.5 ms	{(188+157+138)ms/3}/2 = 80.5 ms
(3)	Part-1.a	5.484 ms	-
(4)	Part-1.b	-	14.628 ms

Table 1

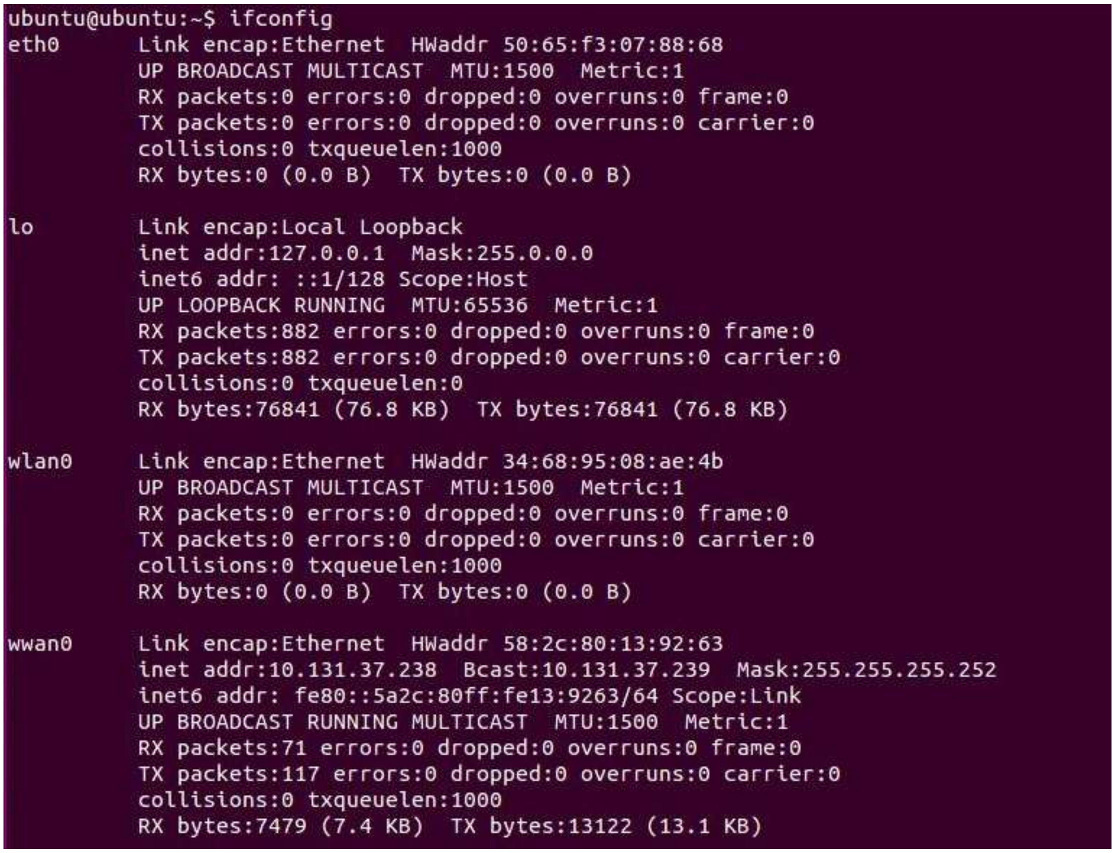
When consider the delay measurements taken by the ping tool in case (1), delay is greater than case (2). This is obvious that the delay is minimum as Google is a content provider network.

But the delay is greater in case (2) than case (1) when using tracert tool. This might be happened due to some network traffic occur in the network. For an example if many users access the host at the same time there might be delays like queuing delay and etc.

- According to the figure 10 delay shows an upper trend for each intermediate node towards the target host. But at some points there are some deviations too. For an example in figure 10, delays on 8th node have a considerable deviation. This might occur due to the data traffic (nodal processing, queuing, transmission and propagation delay) occur in particular host (In this case it’s 222.165.175.158) as many users are trying to use that network interface.

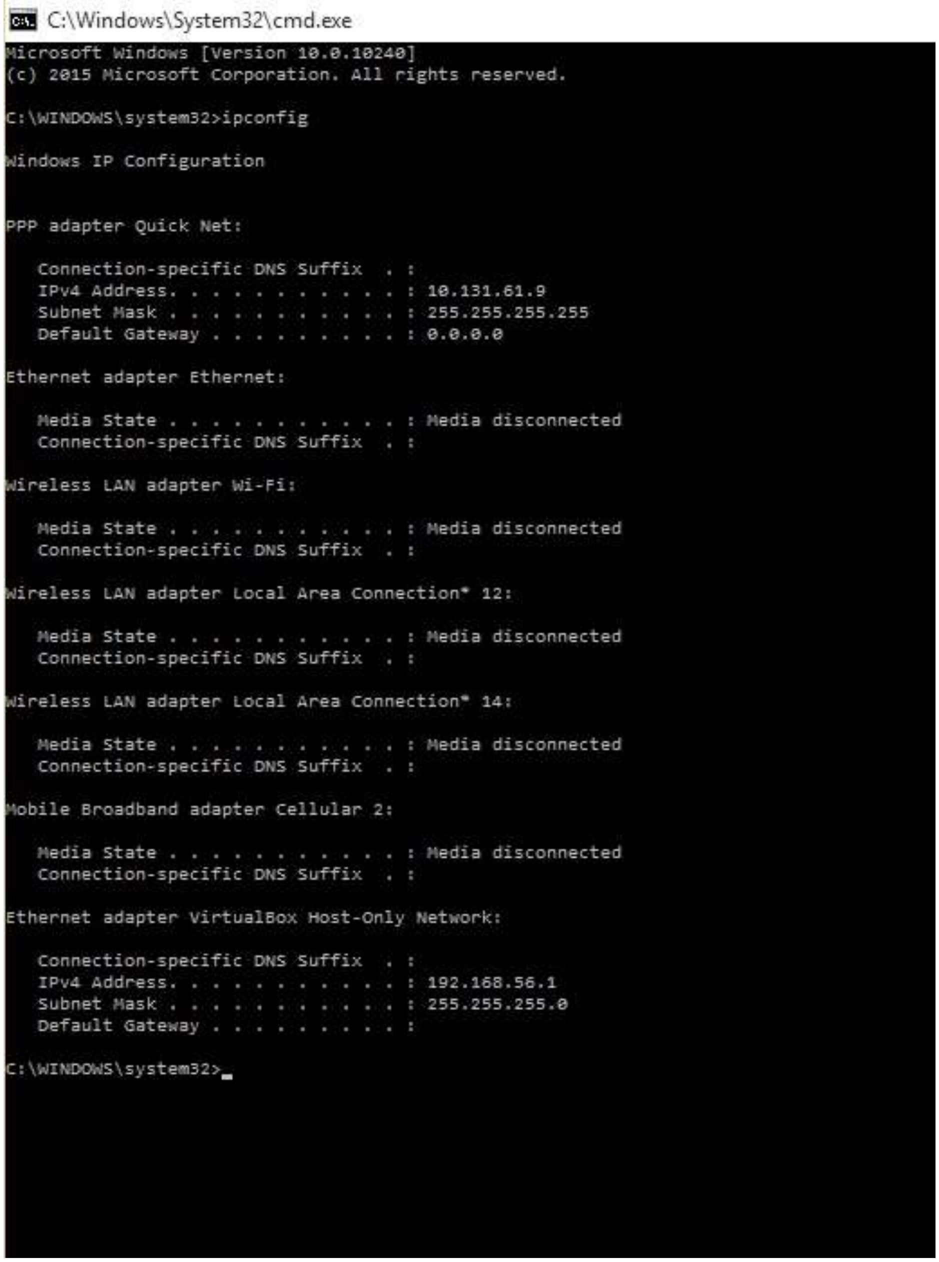
d)

- (1) ifconfig (or ipconfig in Windows)



```
ubuntu@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 50:65:f3:07:88:68
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:882 errors:0 dropped:0 overruns:0 frame:0
          TX packets:882 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:76841 (76.8 KB)  TX bytes:76841 (76.8 KB)

wlan0     Link encap:Ethernet  HWaddr 34:68:95:08:ae:4b
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wwan0     Link encap:Ethernet  HWaddr 58:2c:80:13:92:63
          inet addr:10.131.37.238  Bcast:10.131.37.239  Mask:255.255.255.252
          inet6 addr: fe80::5a2c:80ff:fe13:9263/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7479 (7.4 KB)  TX bytes:13122 (13.1 KB)
```

Figure 12



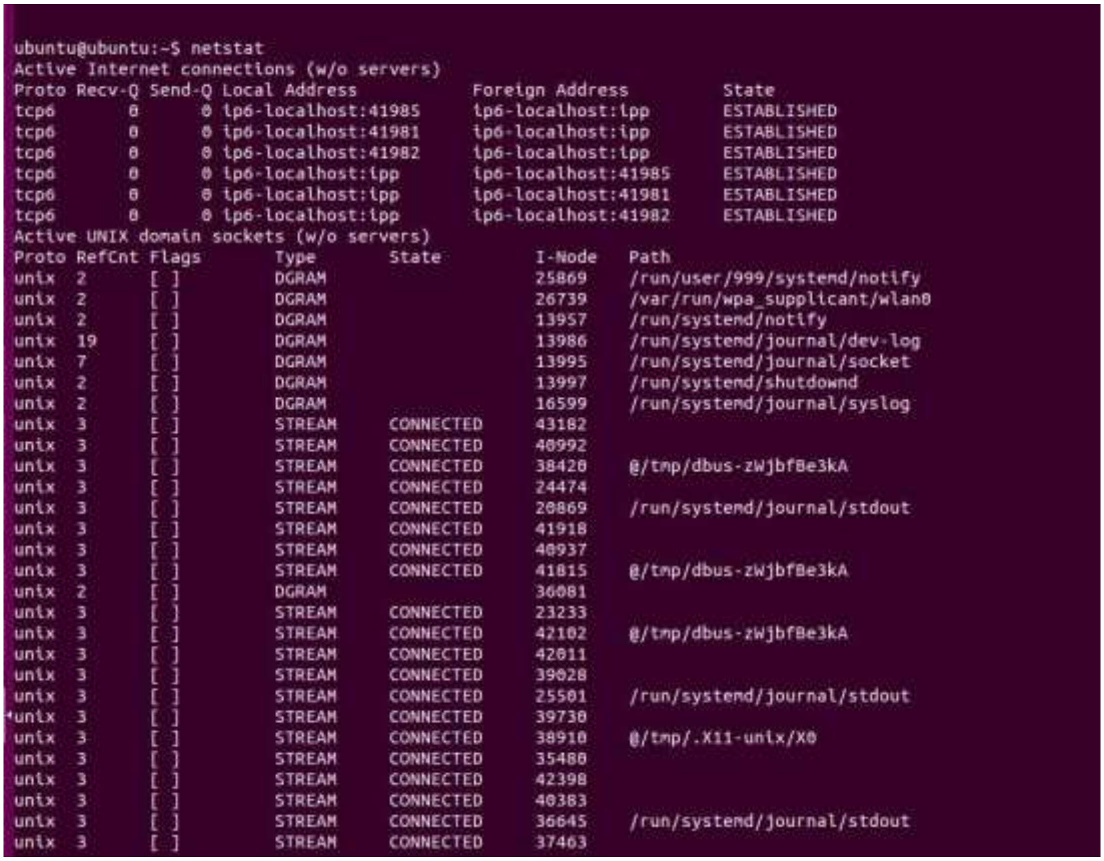
C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration


PPP adapter Quick Net:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.131.61.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 14:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Mobile Broadband adapter Cellular 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\WINDOWS\system32>_
```

Figure 13

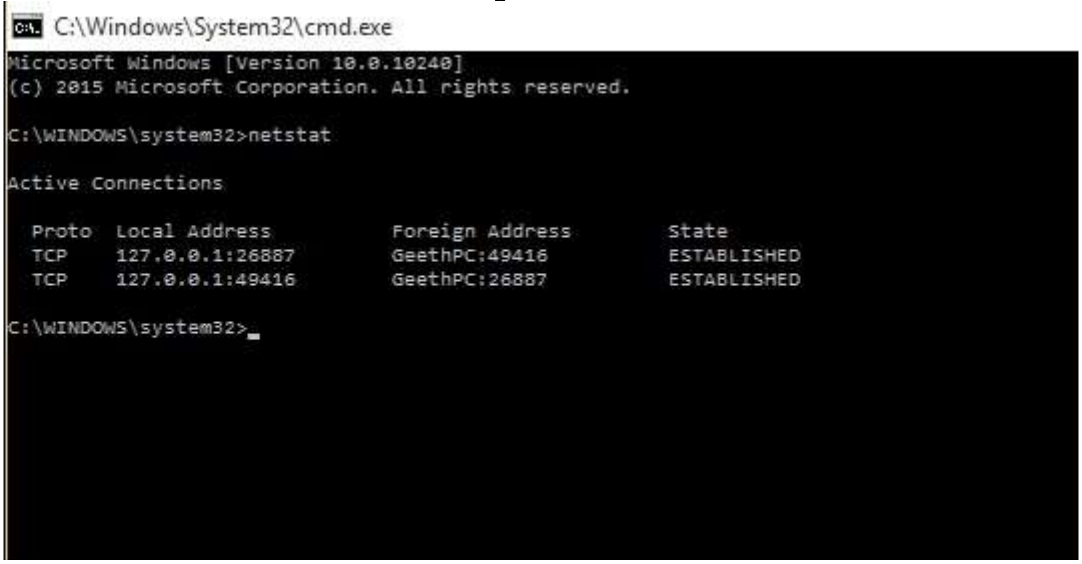
‘ifconfig’(interface configuration) or ‘ipconfig’(internet protocol configuration) is a tool/ command which is referred to display all the current TCP/IP network configuration values and network interface parameters. It shows the IPv4 and IPv6(if available) of particular interface and the host name(if available).

(2) netstat



```
ubuntu@ubuntu:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6       0      0 ip6-localhost:41985     ip6-localhost:ipp       ESTABLISHED
tcp6       0      0 ip6-localhost:41981     ip6-localhost:ipp       ESTABLISHED
tcp6       0      0 ip6-localhost:41982     ip6-localhost:ipp       ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       ip6-localhost:41985     ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       ip6-localhost:41981     ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       ip6-localhost:41982     ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    25869    /run/user/999/systemd/notify
unix  2      [ ]         DGRAM                    26739    /var/run/wpa_supplicant/wlan0
unix  2      [ ]         DGRAM                    13957    /run/systemd/notify
unix  19     [ ]         DGRAM                    13986    /run/systemd/journal/dev-log
unix  7      [ ]         DGRAM                    13995    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    13997    /run/systemd/shutdownd
unix  2      [ ]         DGRAM                    16599    /run/systemd/journal/syslog
unix  3      [ ]         STREAM     CONNECTED     43182    
unix  3      [ ]         STREAM     CONNECTED     40992    
unix  3      [ ]         STREAM     CONNECTED     38420    @/tmp/dbus-zWjbfBe3kA
unix  3      [ ]         STREAM     CONNECTED     24474    
unix  3      [ ]         STREAM     CONNECTED     20869    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     41918    
unix  3      [ ]         STREAM     CONNECTED     40937    
unix  3      [ ]         STREAM     CONNECTED     41815    @/tmp/dbus-zWjbfBe3kA
unix  2      [ ]         DGRAM                    36081    
unix  3      [ ]         STREAM     CONNECTED     23233    
unix  3      [ ]         STREAM     CONNECTED     42102    @/tmp/dbus-zWjbfBe3kA
unix  3      [ ]         STREAM     CONNECTED     42011    
unix  3      [ ]         STREAM     CONNECTED     39028    
unix  3      [ ]         STREAM     CONNECTED     25501    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     39730    
unix  3      [ ]         STREAM     CONNECTED     38910    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     35480    
unix  3      [ ]         STREAM     CONNECTED     42398    
unix  3      [ ]         STREAM     CONNECTED     40383    
unix  3      [ ]         STREAM     CONNECTED     36645    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     37463
```

Figure 14



C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:26887        GeethPC:49416          ESTABLISHED
  TCP    127.0.0.1:49416        GeethPC:26887          ESTABLISHED

C:\WINDOWS\system32>_
```

Figure 15

‘netstat’(network statistics) is a command/ tool that display network connections over TCP, routing tables and network protocol statistics. Type of data packets (ICMP,TCP,UDP) can be identified using this tool.

(3) tcpdump (or windump in Windows)

‘tcpdump’ is a command line packet sniffing (packet analyzing) tool which allow the user to view the packets(TCP/IP) received or transferred over a network interface which the computer is attached.

Part-2 Network Protocol Analyzer

a) Network Protocol Analyzer

- Network Protocol Analyzer is program that can intercept traffic data while transferring or receiving over a network interface. These programs are also known as packet sniffers as those programs are capable of capture each packet if needed, and analyze the content of that particular packet.

  This tool is very useful in detecting intrusions for a certain network, detecting misuses of users in a certain network, detecting bugs of networks and in many network regarding issues.

b) Using Wireshark

- In order to capture packets in a network using wireshark first the particular network interface should be introduced to the wireshark software by selecting capture → options in the menu bar.
- After selecting the certain network interface capturing can be start by selecting capture → start from the menu bar.
- Then the list of captured packets are displayed. By double clicking each one, details of each packet can be displayed.
- To save the list as a trace file select file → save in menu bar.

e) In quiet network mainly UDP(User Datagram Protocol), STP(Spanning Tree Protocol) and DHCP(Dynamic Host Configuration Protocol) packets can be identified.

But when considering the busy network when ping tool is used, ICMP(Internet Control Message Protocol) packets clusters can be identified easily which were transferring between the local and the host. Other than that there are few packets of DTP(Dynamic Trunk Protocol) too.

When the traceroute tool is used, it’s same as when the ping tool is used. The only difference that can be identified is the info about ICMP packet other than when the ping tool is used. And the number of UDP packets also greater than quiet network.