Subject: Computer Networks **Name of the Student:**	
Class:	**Roll no:**
PRN:	
Date of Performance:	**Date of Submission:**
Examined by:	

EXPERIMNT NO: B3

AIM.: To Observe and note the working of protocols using PING / TRACEROUTE / PATHPING and capture packets in LAN using packet capture and analysis tool.

THEORY

Traceroute, Ping, and PathPing are network tools or utilities that use the ICMP protocol to perform testing to diagnose issues on a network. Internet Control Message Protocol (ICMP) is an error reporting and diagnostic utility. ICMPs are used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts.

1Ping : The ping command sends an echo request to a host available on the network. Using this command, you can check if your remote host is responding well or not. Tracking and isolating hardware and software problems. Determining the status of the network and various foreign hosts. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device. The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response.

C:Users\Admin>ping mescoepune.org C: **C:**Users\Admin>ping www.facebook.com

2.Trace route:

Traceroute uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values. The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop. Traceroute is a network diagnostic tool used to track the pathway taken by a packet on an IP network from source to destination. Traceroute also records the time taken for each hop the packet makes during its route to the destination. Traceroute uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values.
The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop.

Traceroute sends packets with TTL values that gradually increase from packet to packet, starting with TTL value of one. Routers decrement TTL values of packets by one when routing and discard packets whose TTL value has reached zero, returning the ICMP error message ICMP Time Exceeded.

For the first set of packets, the first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of two, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

With the tracert command shown above, we're asking tracert to show us the path from the local computer all the way to the network device with the hostname.

3. **Pathping :** This network utility is a more advanced version of the Ping tool, which performs a ping to each hop along the route to the destination (unlike Ping, which just pings from the originating device to the destination device). It is extremely useful in diagnosing packet loss, and can help with diagnosing slow speed faults.

To PathPing a device, proceed as follows.

1. Open a Windows Command Prompt window.
2. At the command prompt, type, pathping <IP address/Website url>, as shown below.

   C:Users\Admin>pathping www.mescoepune.org

ICMP:

ICMP or Internet Control Message Protocol is **Internet** or **Network** layer protocol. In general it is used to check the reachability of a host or router in a network.

Uses of ICMP :

Ping or traceroute uses ICMP as inner protocol. Ping uses ICMP echo request and ICMP echo reply messages to check whether destination host is reachable or not.

Types of ICMP packet?

In general two types of ICMP packet

1.ICMP echo request messages.

2.ICMP echo reply messages.

How to get ICMP packet in Wireshark?

Step1: We can use ping tool to get ICMP request and reply.

Step2: Open command line or terminal in Windows or Linux respectively.

Step3: Run Wireshark.

Step4: Run below command

```
ping www.google.com
```

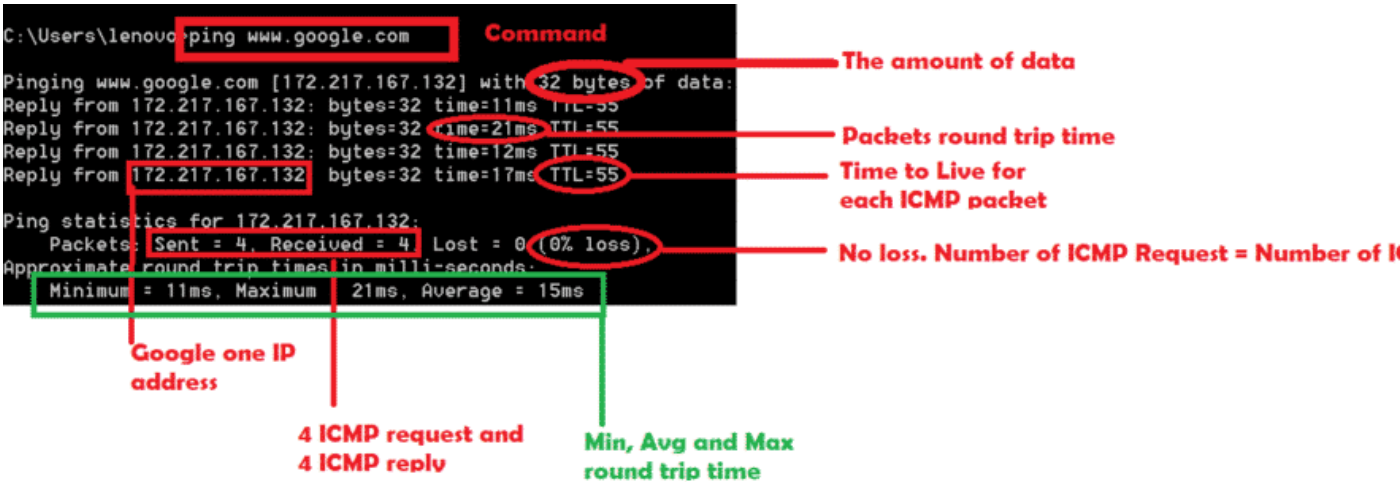
Make sure you have internet connection or ping will be failedJ. Here is the snapshot for successful ping to Google. We can see 0% loss. That means ICMP request packets = ICMP reply packets.

```
C:\Users\lenovo>ping www.google.com

Pinging www.google.com [172.217.167.132] with 32 bytes of data:
Reply from 172.217.167.132: bytes=32 time=11ms TTL=55
Reply from 172.217.167.132: bytes=32 time=21ms TTL=55
Reply from 172.217.167.132: bytes=32 time=12ms TTL=55
Reply from 172.217.167.132: bytes=32 time=17ms TTL=55

Ping statistics for 172.217.167.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 21ms, Average = 15ms
```

Here are the more details:



In this case we ping to Google web site. Instead we can do ping to ip address also.
OR
ping 192.168.1.1 [This is router IP address}

Step5: Stop Wireshark and put “ICMP” as filter in Wireshark.

Analysis on ICMP:

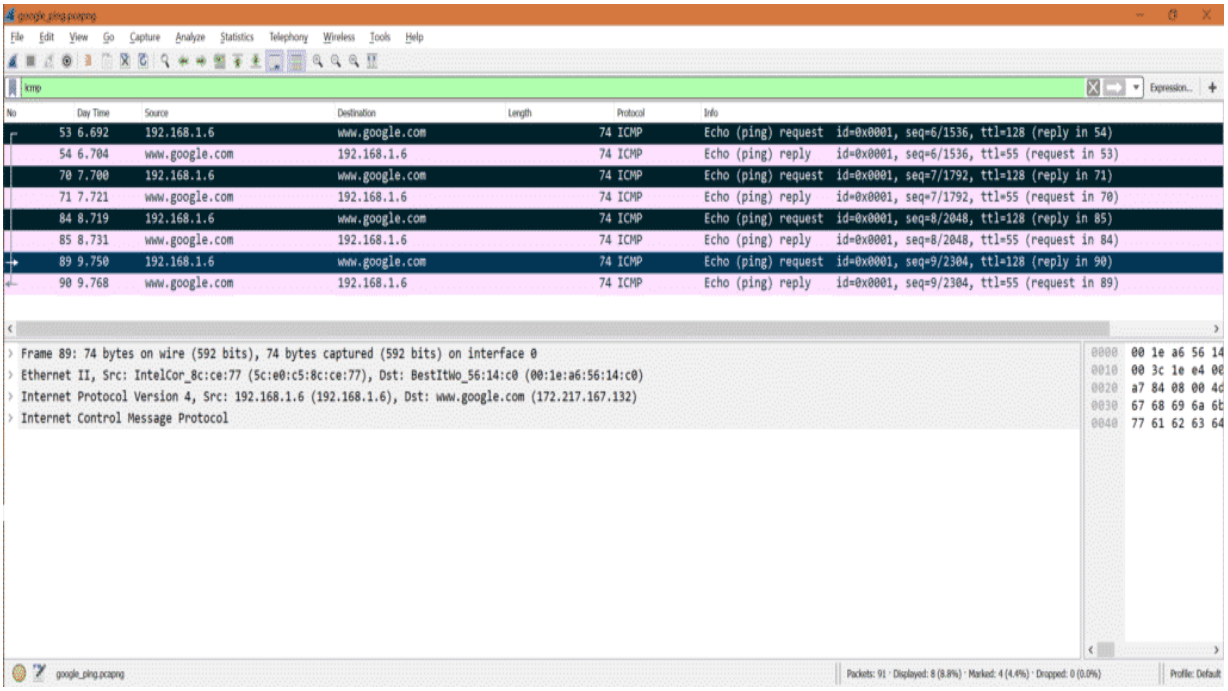
Let’s check what happens in Wireshark when we ping to Google or 192.168.1.1.

Here is the ICMP request and reply packets for Google ping.

Note: We have to put filter ‘icmp’ as we are interested only in ICMP packets.

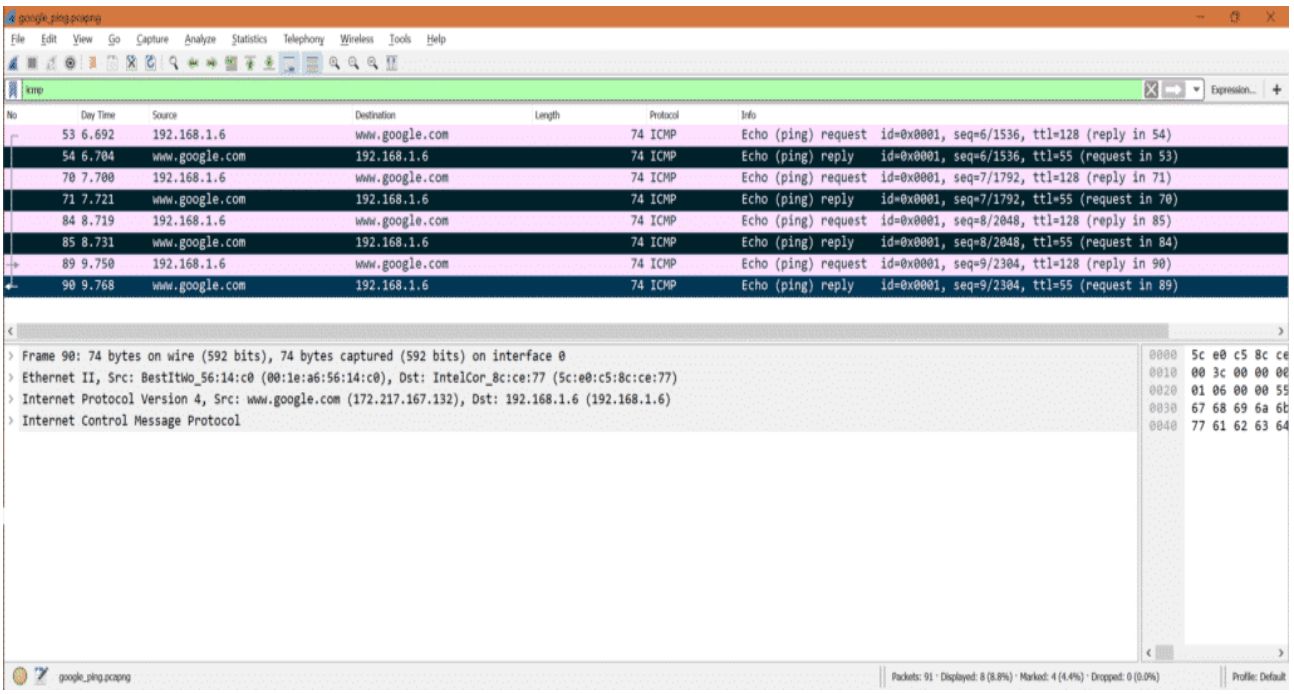
Number of ICMP request: From capture we can see there are 4 ICMP request packets.

Check the marked packets.



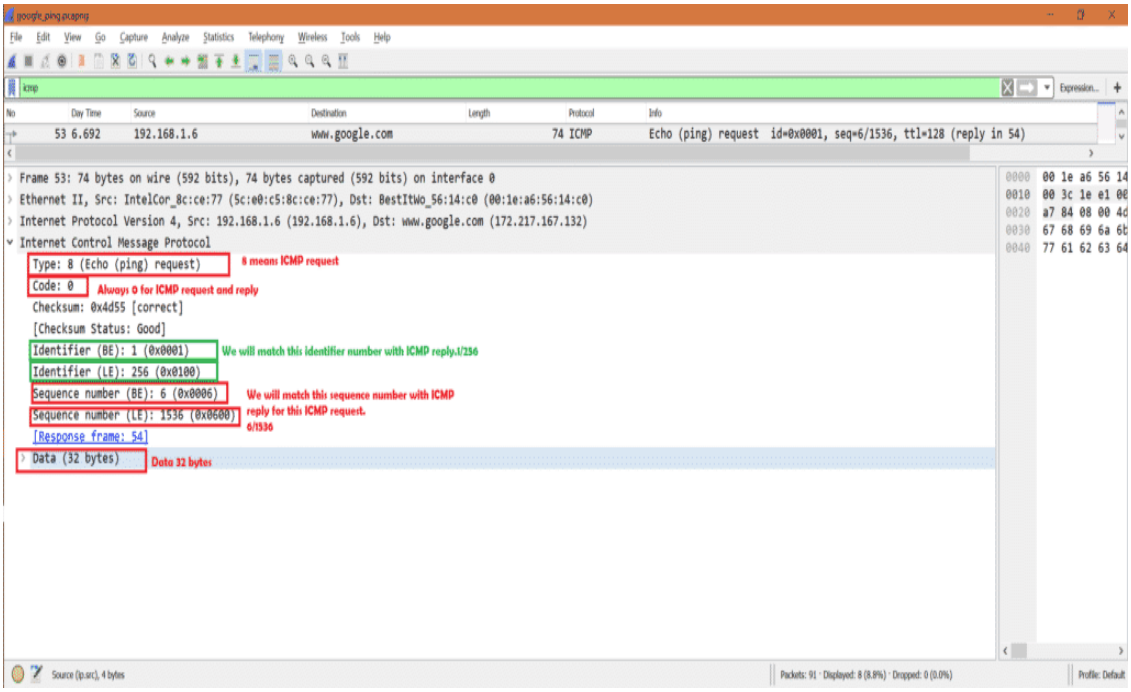
Number of ICMP reply: From capture we can see there are 4 ICMP reply packets.

Check the marked packets.



ICMP Request:

Now select ICMP request packet in Wireshark and look into IPv4 layer.
As this is ICMP request packet so we can see source IP as my system IP address and destination IP as Google's one IP address. Also IP layer mentioned the protocol as ICMP.
Here is the screenshot



Now for the same packet select ICMP part in Wireshark.

Information about important fields:

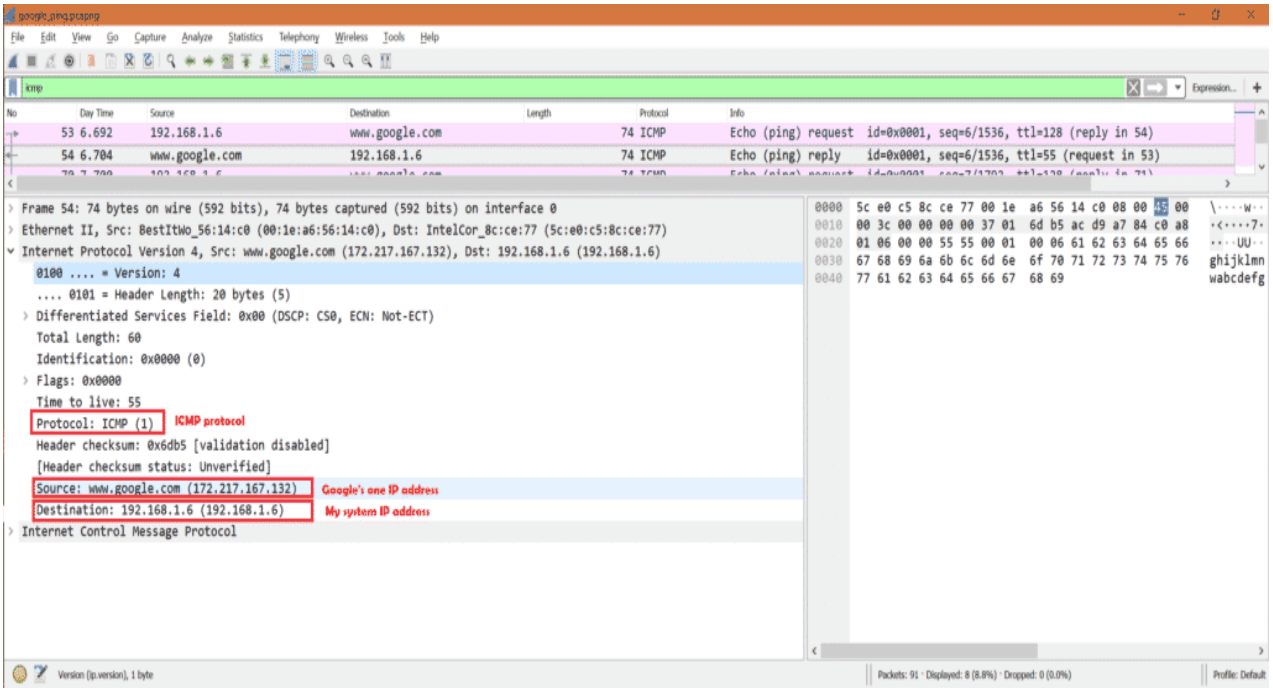
Type: 8 [Means its ICMP request]
Code: 0 [Always 0 for ICMP packets]
Identifier (BE): 1
Identifier (LE): 256
Sequence Number (BE): 6
Sequence Number (LE): 1536
*BE -> Big Endian
*LE -> Little Endian
Data -> Data present in ICMP packet.

Here is the screenshot

ICMP Reply:

Now select ICMP reply packet in Wireshark and look into IPv4 layer.

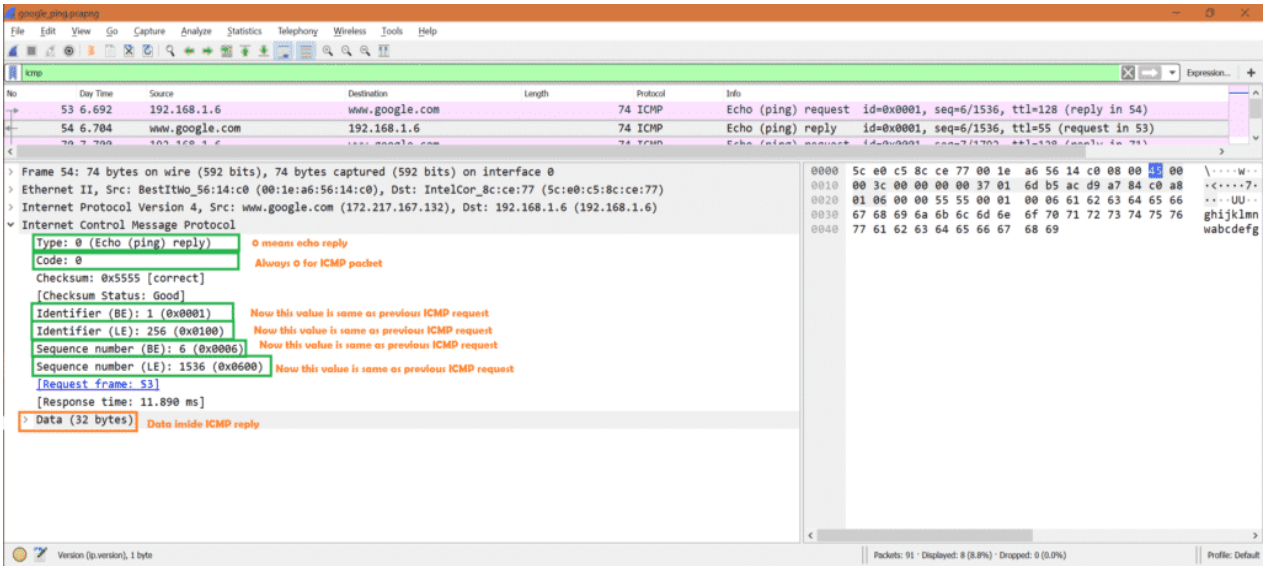
As this is ICMP reply packet so we can see destination IP as my system IP address and source IP as Google's one IP address. Also IP layer mentioned the protocol as ICMP.
Here is the screenshot



Now for the same packet select ICMP part in Wireshark.
Information about important fields:

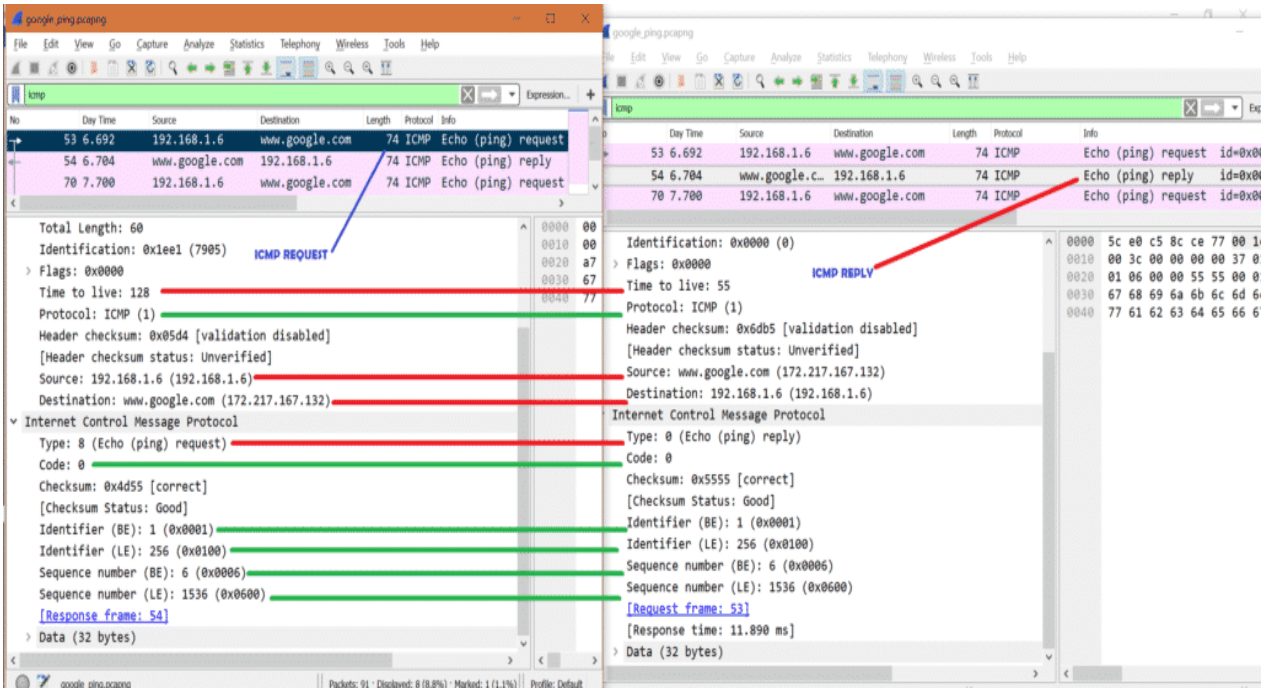
Type: 0 [Means its ICMP reply]
Code: 0 [Always 0 for ICMP packets]
Identifier (BE): 1
Identifier (LE): 256
Sequence Number (BE): 6
Sequence Number (LE): 1536
*BE -> Big Endian
*LE -> Little Endian
Data -> Data present in ICMP packet.

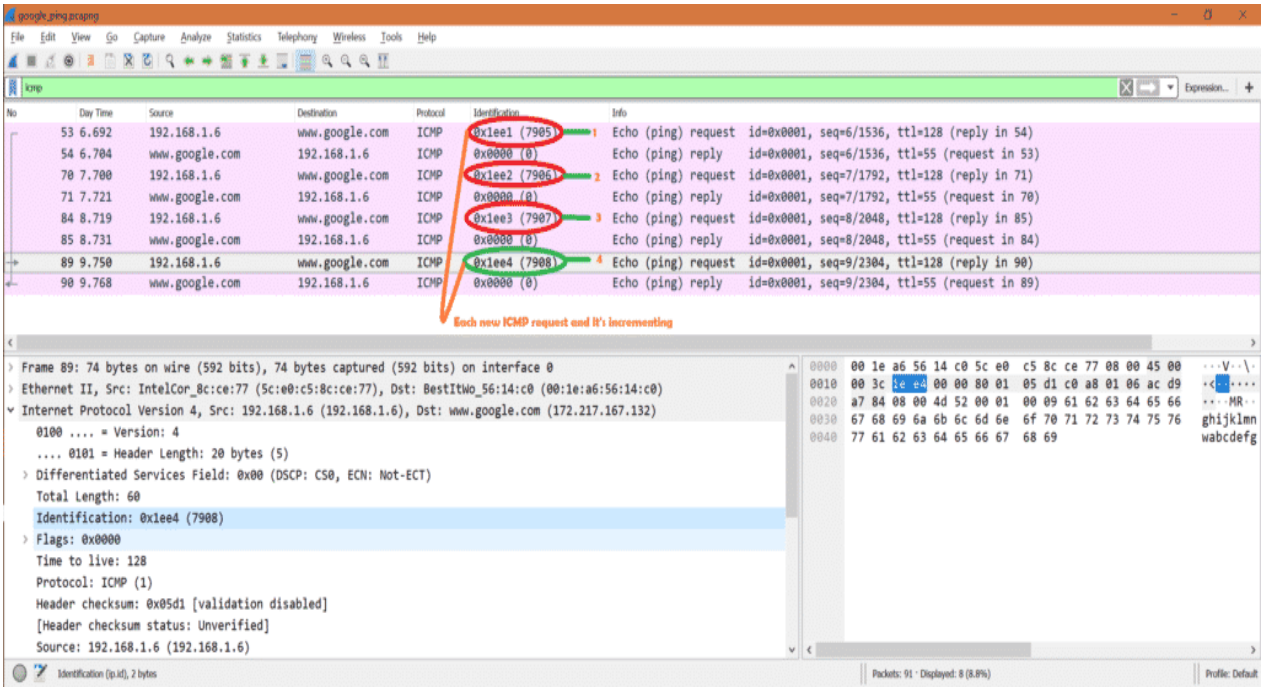
Here is the screenshot



Now let's see ICMP request and ICMP reply side by side in a picture.

*Red means it's different
*Green means it's same.





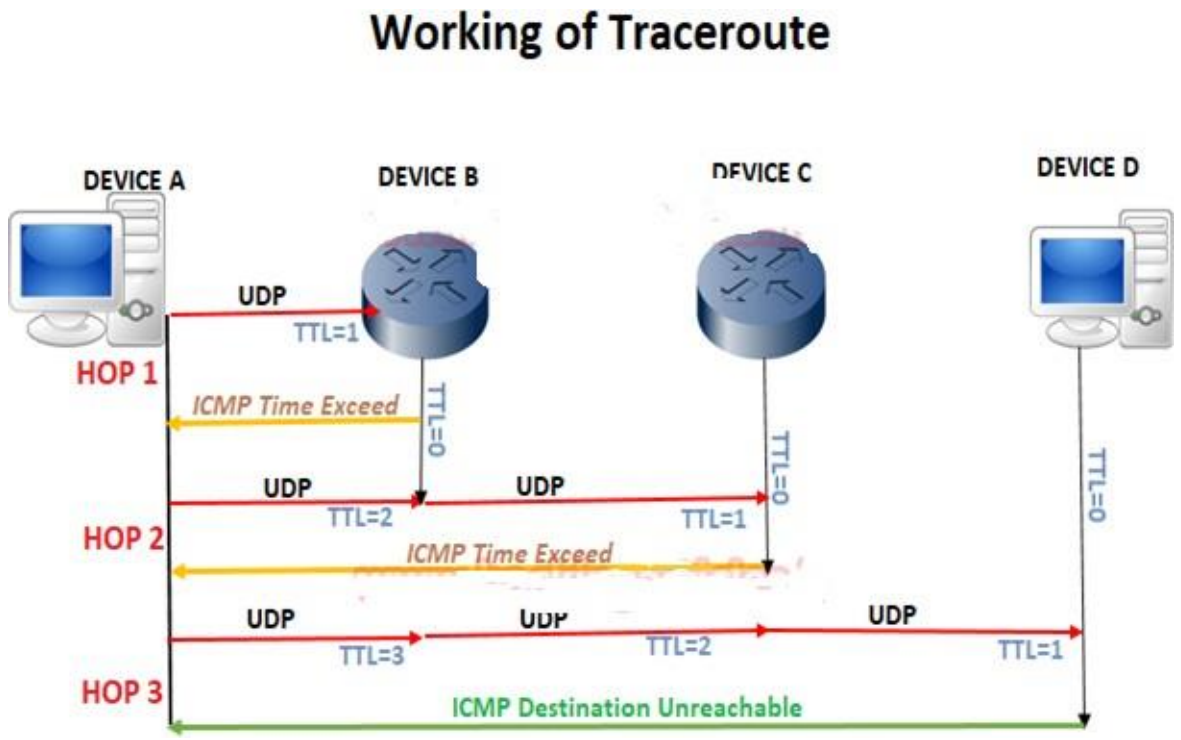
Traceroute or Tracert: It is a CUI based computer network diagnostic tools used in UNIX and Windows-like system respectively. It traces the path of a packet from the source machine to an Internet host such as Google.com by calculating the average time taken each hop. Traceroute sends a UDP packet to the destination by taking benefit of ICMP's messages. It uses the ICMP error-reporting messages –Destination Unreachable and Time exceeded.

TTL: The time-to-live value, also known as the hop limit, is a mechanism that limits the lifespan or lifetime of data in a computer or network.

Hop: A hop is one portion of the path between source and destination. Data packets pass through bridges, routers, and gateways as they travel between source and destination. On the internet, before the data reaches its final destination, it goes through several routers and a hop occurs when an incoming packet is forwarded to the next router.

The asterisk (*): Denotes probe timeout which means that the router at that hop doesn't respond to the packet received from the source used for the traceroute due to firewall filter.

Working of Traceroute



Read the below steps:

- Traceroute sends a UDP packet with a TTL = 1 from the source to destination.
- When the first router receives the UDP packet it reduces the TTL value by 1 (1-1=0) then drop the packet and sends an ICMP message "Time exceeded" to the source. Thus Traceroute makes a list of the router's address and the time taken for the round-trip.
  The TTL time exceeded ICMP message is sent after the TTL value of a UDP packet gets zero. In typical condition, a network doesn't have such a diameter that lead the TTL=0. This could be possible when there is a routing loop. In this case, as the packet is sent back and forth between the looping points, the TTL keeps getting decrement until it becomes zero. And at last, the source receives ICMP error message sent by the router.

- Again source device sends two more packets, in the same way, to get an average value of the round-trip time and again TTL gets zero when it reaches to the 2nd router and response through ICMP error message time exceeds.
- Traceroute keeps on doing this, and record the IP address and name of every router until the UDP packets reach to the destination address. Once it reaches at the destination address, Time exceeded ICMP message is NOT sent back to the source.
- Since Traceroute uses the random port for sending UDP packets as result destination machine will drop the packet and send a new ICMP error message-Destination Unreachable to the source which indicates the UDP packets has reached to the destination address.

Tracert with Wireshark

As discussed above tracert is CLI utility for windows system to trace the path of a packet from source to destination. So herewith help of the following command, we can observe the path of the packet which travels to reach Google DNS.

Syntax: tracert [options] Host IP

```
tracert 8.8.8.8
```

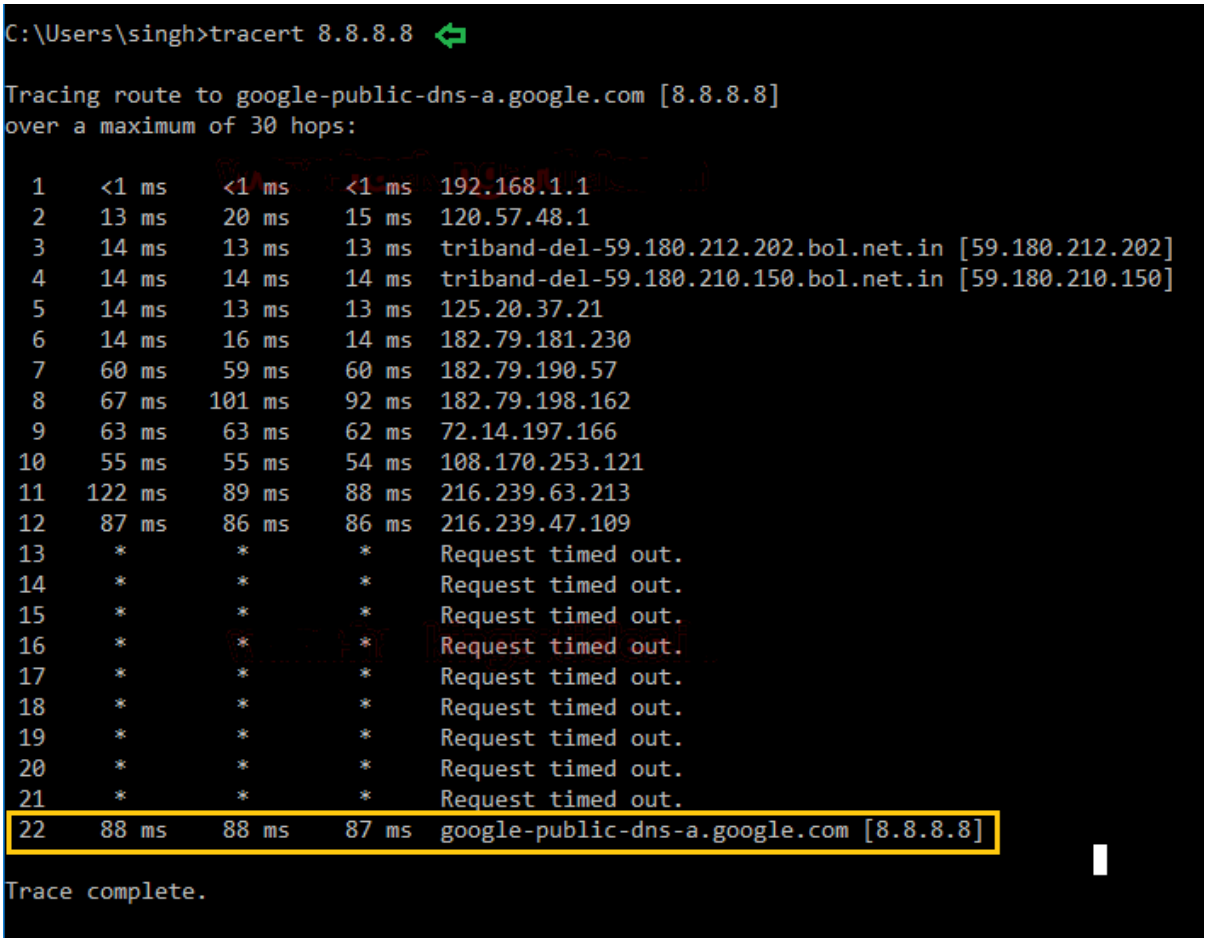
or

```
tracert -d 8.8.8.8
```

Traceroute generates a list of each hop by entering IP of routers that traversed between source and destination and average round-trip time. As a result **hop 22 denotes** entry of destination i.e. Google DNS.

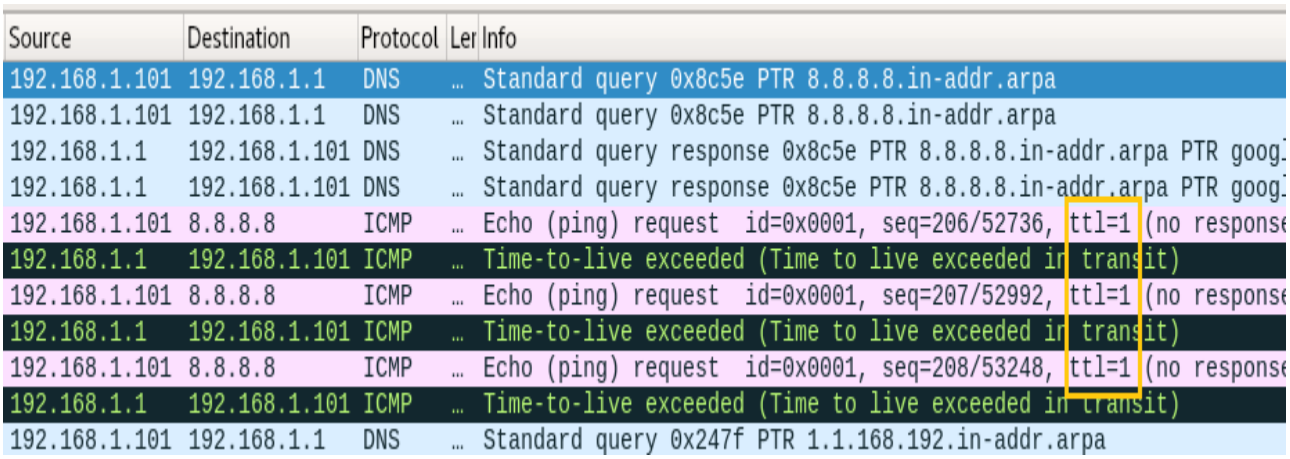
In order to notice the activity of traceroute, we have turned on Wireshark in the background.

Note: Result of tracert can vary each time for hop count but does not go beyond 30 hops because it is the maximum hop limit.



At Wireshark we notice the following points:

- ICMP echo request packet is used instead of UDP to send DNS query.
- The packet first goes from source 192.168.1.101 to first router 192.168.1.1 having ICMP echo request packet with TTL=1
- The router will drop that packet and send ICMP Time Exceeded error message to the source.
- All this happens 3 times before the source machine sends next packet by incrementing TTL value by 1 i.e. TTL=2.



Source	Destination	Protocol	Ler	Info
192.168.1.101	192.168.1.1	DNS	…	Standard query 0x8c5e PTR 8.8.8.8.in-addr.arpa
192.168.1.101	192.168.1.1	DNS	…	Standard query 0x8c5e PTR 8.8.8.8.in-addr.arpa
192.168.1.1	192.168.1.101	DNS	…	Standard query response 0x8c5e PTR 8.8.8.8.in-addr.arpa PTR goog
192.168.1.1	192.168.1.101	DNS	…	Standard query response 0x8c5e PTR 8.8.8.8.in-addr.arpa PTR goog
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request id=0x0001, seq=206/52736, ttl=1 (no response
192.168.1.1	192.168.1.101	ICMP	…	Time-to-live exceeded (Time to live exceeded in transit)
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request id=0x0001, seq=207/52992, ttl=1 (no response
192.168.1.1	192.168.1.101	ICMP	…	Time-to-live exceeded (Time to live exceeded in transit)
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request id=0x0001, seq=208/53248, ttl=1 (no response
192.168.1.1	192.168.1.101	ICMP	…	Time-to-live exceeded (Time to live exceeded in transit)
192.168.1.101	192.168.1.1	DNS	…	Standard query 0x247f PTR 1.1.168.192.in-addr.arpa

Form this image we can observe ICMP echo reply message is sent from 8.8.8.8 (destination) to 192.168.1.101 (source) for TTL 22.

192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request	id=0x0001, seq=268/3073,	ttl=21 (no respon
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request	id=0x0001, seq=269/3329,	ttl=22 (reply in
8.8.8.8	192.168.1.101	ICMP	…	Echo (ping) reply	id=0x0001, seq=269/3329,	ttl=46 (request i
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request	id=0x0001, seq=270/3585,	ttl=22 (reply in
8.8.8.8	192.168.1.101	ICMP	…	Echo (ping) reply	id=0x0001, seq=270/3585,	ttl=46 (request i
192.168.1.101	8.8.8.8	ICMP	…	Echo (ping) request	id=0x0001, seq=271/3841,	ttl=22 (reply in
8.8.8.8	192.168.1.101	ICMP	…	Echo (ping) reply	id=0x0001, seq=271/3841,	ttl=46 (request i

Conclusion: