Traceroute

What is Traceroute:

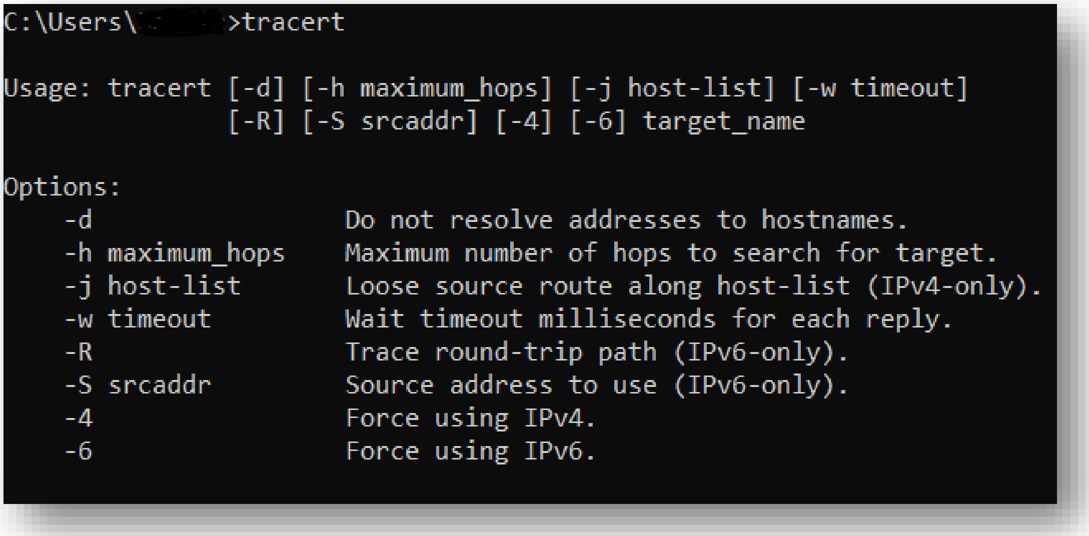
Traceroute is a network diagnostic tool by which we can get to know the route taken by a packet from source to destination. Traceroute uses Internet Control Message Protocol (ICMP) echo packets.

How it works:

Traceroute sends packets to the destination address with variable TTL (Time To Live) values and whenever a packet passes through a hop in the network the TTL value of the packet is decremented by 1. If the TTL value reaches zero the hop drops the packet and sends an echo message to the sender that the packet is dropped. This message will be recorded by the Traceroute. The first three packets are sent with TTL = 1, which implies that these packets will be dropped by the first hop in the path to the destination. Three packets are sent to get an accurate value of the RTT. Then it sends the next three with TTL = 2 and so on until the packets reach the destination.

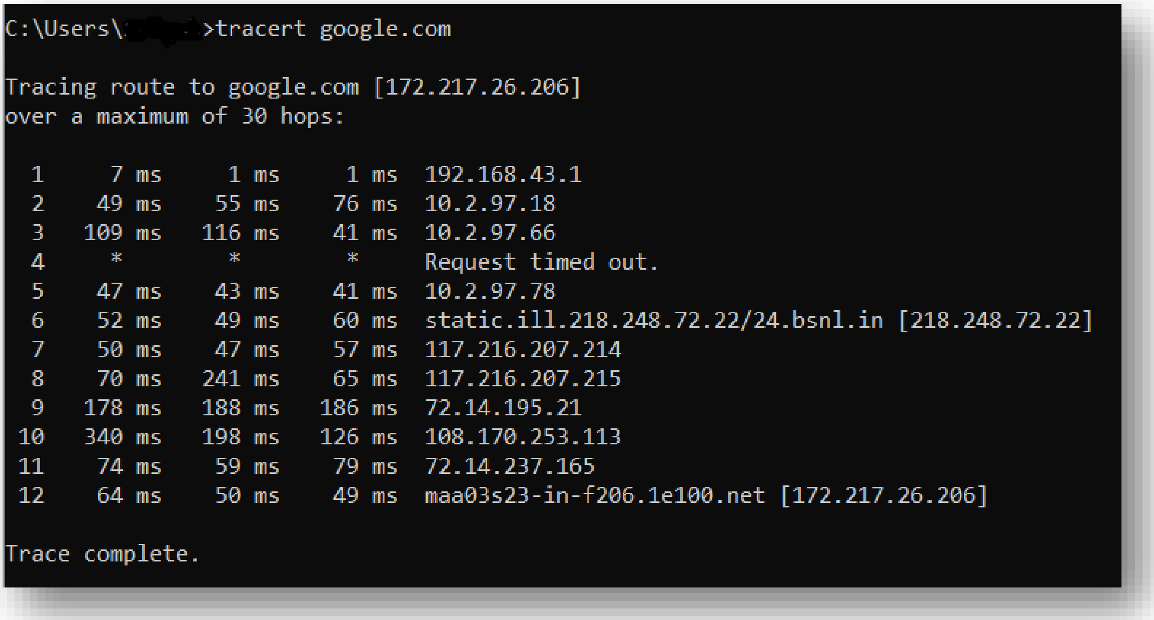
Working with Traceroute:

Traceroute program is available in almost all operating systems. In Windows, we can type “tracert” in the command prompt.



```
C:\Users\[redacted]>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

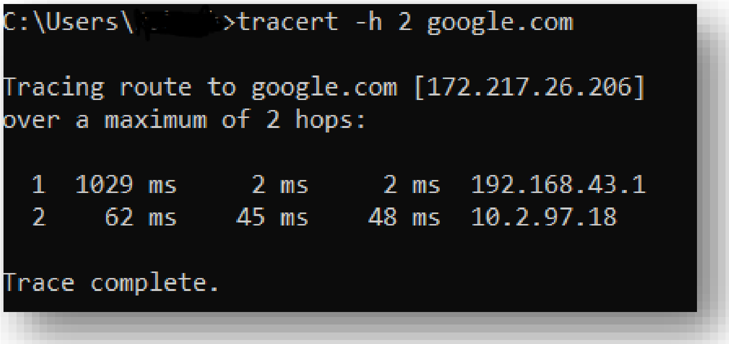
To know the path taken by a particular domain name we can type “tracert <Domain name>”



```
C:\Users\[redacted]>tracert google.com

Tracing route to google.com [172.217.26.206]
over a maximum of 30 hops:

  1     7 ms     1 ms     1 ms  192.168.43.1
  2    49 ms    55 ms    76 ms  10.2.97.18
  3   109 ms   116 ms    41 ms  10.2.97.66
  4     *        *        *     Request timed out.
  5    47 ms    43 ms    41 ms  10.2.97.78
  6    52 ms    49 ms    60 ms  static.ill.218.248.72.22/24.bsnl.in [218.248.72.22]
  7    50 ms    47 ms    57 ms  117.216.207.214
  8    70 ms   241 ms    65 ms  117.216.207.215
  9   178 ms   188 ms   186 ms  72.14.195.21
 10   340 ms   198 ms   126 ms  108.170.253.113
 11    74 ms    59 ms    79 ms  72.14.237.165
 12    64 ms    50 ms    49 ms  maa03s23-in-f206.1e100.net [172.217.26.206]

Trace complete.
```

Here we can see using the Traceroute program for domain name google.com.
The first column of the output represents the hop number. The next three values represent the RTT (Round Trip Time) to reach the hop and the last column represents the IP address of the particular hop in the path. It shows " * " if the hop is not responding. It will show up to 30 hops.
In this case, there are 11 hops to reach the google.com

There are a few options available in the traceroute program (we can see from the first image). With -h option we can limit our search to a particular number of hops. By typing "tracert -h 2 google.com", the program will display the first two hops in the path.



```
C:\Users\[redacted]>tracert -h 2 google.com

Tracing route to google.com [172.217.26.206]
over a maximum of 2 hops:

  1  1029 ms     2 ms     2 ms  192.168.43.1
  2    62 ms    45 ms    48 ms  10.2.97.18

Trace complete.
```