Assignment 4:

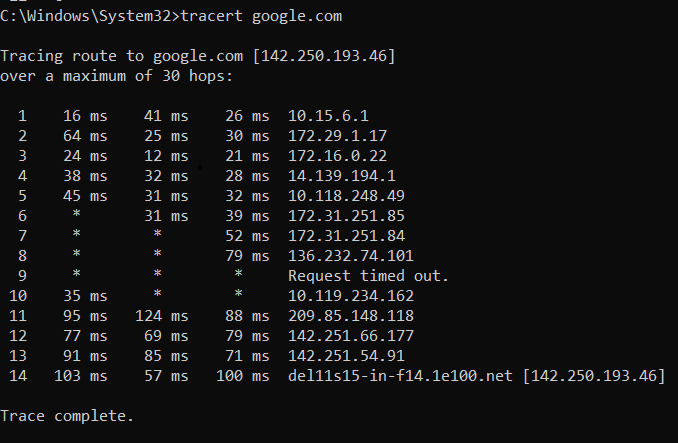
(Objective 1)

1)

The tracert (Trace Route) utility is a network diagnostic tool used to track the path that packets take from a source computer to a destination across an IP network. It helps identify the specific routers or hops where network issues might be occurring by displaying the route and measuring transit delays of packets.

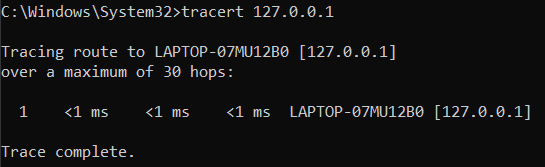
For example : tracert google.com

2)



The same type of output occurs in the case of localhost.

For example : tracert 127.0.0.1



**Hop Number:** The first number on each line (1, 2, 3, etc.) represents the sequence of hops the packet has taken.

**Round-Trip Time (RTT):** The three-time values (e.g., 10 ms) represent the time it took for the packet to travel to that hop and back to your machine. Multiple times are provided because tracert sends three packets to each hop by default.

**IP Address:** The next part of the line (e.g., 192.168.1.1) shows the IP address of the router at that hop.

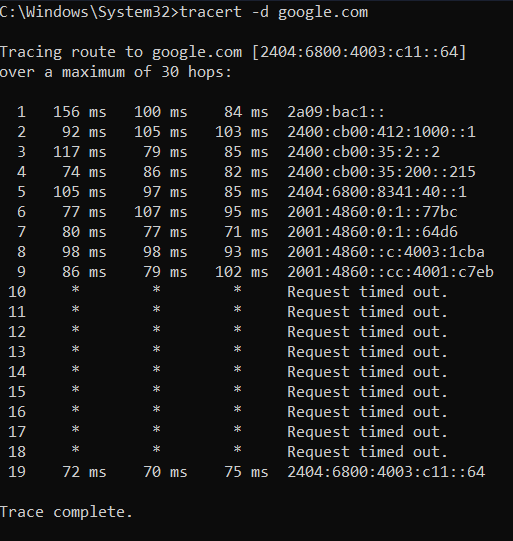
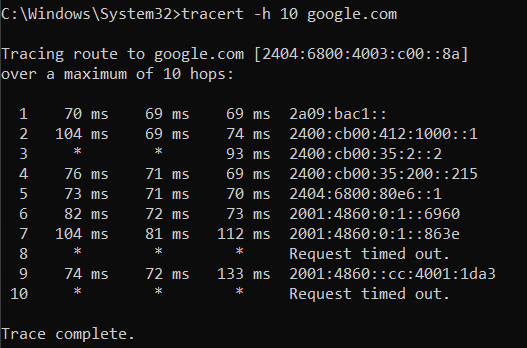
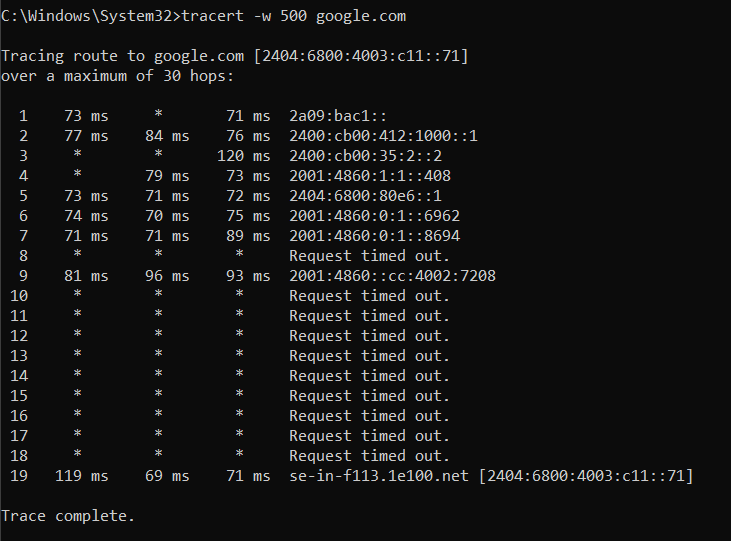
**Request Timed Out:** If a hop doesn't respond, you'll see "\* \* \* Request timed out," indicating a potential issue at that hop or that the router is configured to not respond to ICMP requests.

If the destination doesn’t exist, we get the following output :



3)

Tracert options:

1. -d (Do not resolve hostnames)  
   The -d option prevents tracert from resolving IP addresses to hostnames. This makes the trace process faster because it skips the DNS lookup, which would otherwise add time to resolve hostnames.  
   for example : tracert -d google.com  
   
2. -h (Maximum number of hops)  
   The -h option specifies the maximum number of hops (or routers) that tracert will trace through to reach the destination. If the destination is farther than the specified number of hops, tracert will stop after that limit.  
   for example : tracert -h 10 google.com  
   
3. -w (Timeout in millisecond)  
   The -w option sets the time (in milliseconds) to wait for each reply from a router or destination. If the router or destination does not respond within the specified time, the attempt is considered a timeout.  
   for example : tracert -w 500 google,com  
   

4)

Scenario:

Imagine you are unable to connect to a specific website (e.g., www.example.com), but other websites load without problems. You suspect there is an issue somewhere along the network path between your computer and the website’s server, and you want to use tracert to diagnose where the problem might be.

How to use tracert to diagnose this issue :

1. **Run tracert to Trace the Path**: First, run a basic tracert command to trace the path from your computer to the destination server. This command will show the IP addresses and hostnames of all routers (hops) between you and the destination.  
   for example : tracert example.com  
   **Analyze the Output**: The output will show a list of hops, with each hop indicating a router that the packet passes through. You will see the time (in milliseconds) it takes for packets to reach each hop and return.
2. If the trace takes too long because of DNS lookups, use the -d option to avoid resolving IP addresses into hostnames, speeding up the trace process.  
   for example : tracert -d example.com
3. If the trace takes too long because of DNS lookups, use the -d option to avoid resolving IP addresses into hostnames, speeding up the trace process.  
   for example : tracert -h 10 example.com
4. If some routers are slow to respond or if the network is congested, you can increase the wait time for each router using the -w option. This can prevent premature timeouts if the routers are just slow to reply.  
   for example : tracert -w 500 example.com
5. **Interpreting Timeouts and High Latency**:  
     
   **1) Timeouts**: If you see \* \* \* Request timed out repeatedly for several hops, it could indicate that a router is down or misconfigured. If timeouts start happening near the end of the trace, the issue may be with the destination server or its network.  
     
   **2) High Latency**: If response times (in milliseconds) are unusually high at one or more hops, this suggests network congestion or issues with the specific router. You can note which hop is causing the slowdown and contact the responsible network provider if necessary.

**5)**

The tracert utility (or traceroute in Linux) is an essential network diagnostic tool used to trace the path that data packets take from a source machine to a destination over an IP network. By mapping out the intermediate hops, tracert helps network administrators and users identify where potential issues or delays might occur during the journey of a packet. This tool provides valuable insights into the routing and latency of each hop, which can be used for network optimization and troubleshooting.  
  
Key Takeaways:

* **Path Discovery**: tracert identifies all intermediate routers that a packet passes through, giving an overview of the route from source to destination.
* **Latency Measurements**: It provides round-trip time (RTT) for each hop, allowing for the detection of bottlenecks, which can indicate network congestion or misconfigured devices.
* **Hop Count Limit**: By limiting the number of hops, tracert helps visualize whether a destination is too far or unreachable due to routing issues.

Limitations and Potential Issues:

While tracert is a valuable diagnostic tool, it does have limitations:

1. **Firewall Restrictions**: Some routers and firewalls may block ICMP packets or specific tracert queries, leading to incomplete results or timeouts.
2. **Asymmetric Routing**: If the path to a destination is different from the return path, the output may not reflect the true path packets take in both directions.
3. **Caching**: Routers may cache TTL-expired packets, causing subsequent tracert outputs to appear faster or less consistent than real-time conditions.
4. **Latency Variations**: Network conditions can fluctuate rapidly, meaning that running tracert at different times can produce inconsistent RTT measurements.

(Objective 2)

