# Department of Computer Science

**EE353: Computer Networks**

**Class: BESE-13AB**

**Lab 7: Tracing the path to a destination**

**CLO3,CLO4**

# Date: 25th October, 2023

**Instructor: Dr Huma Ghafoor**

**Lab Engineer: Syed Muhammad Ali Musa**

**Name:** Aimen Munawar

**Class:** BESE-13-A

**CMS ID:** 415867

**Lab 7: Tracing the path to a destination**

**Introduction and Objective:**

In this lab, we’ll explore several networking tools to trace the path followed by packets to a particular destination.

**Instructions:**

* Read carefully before starting the lab.
* These exercises are to be done individually.
* You are supposed to provide the answers to the questions listed at the end of this document, paste the screenshots of your working and upload the completed report to your course’s LMS site.
* Avoid plagiarism by copying from the Internet or from your peers. You may refer to source/ text but you must paraphrase the original work.

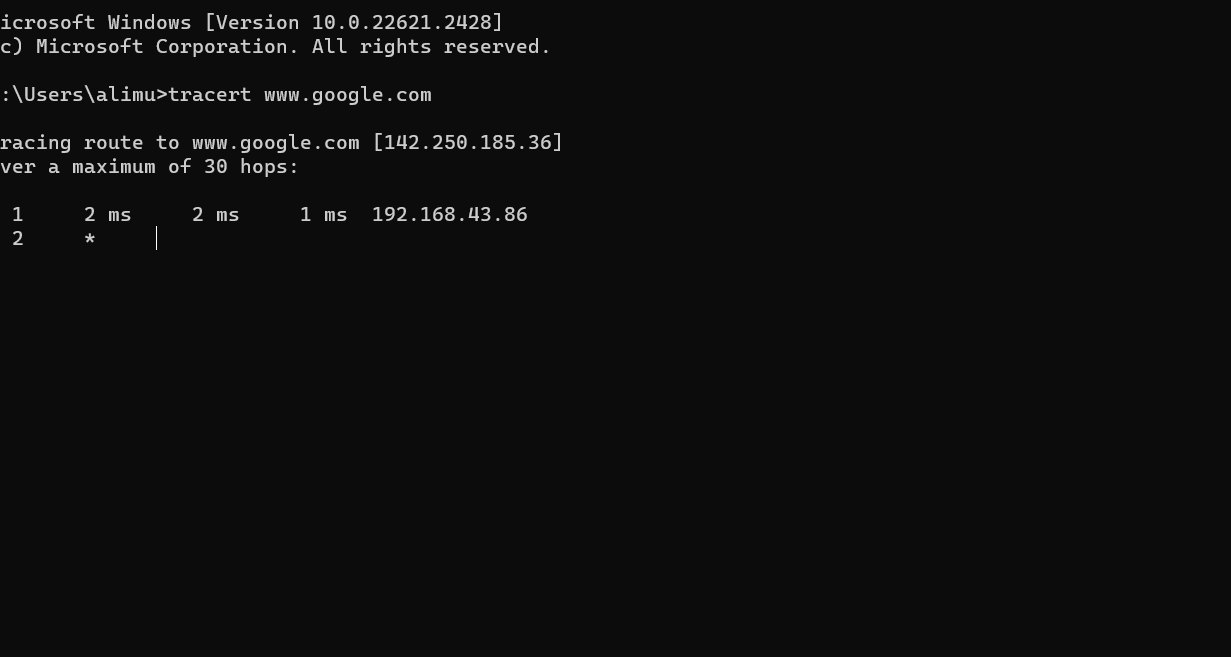
**Tools/Software Requirements:**

Tracert in Windows

**Traceroute**

***Background:***

Trace Route (called traceroute under UNIX and tracert under Windows) is a very useful tool for analyzing network behavior and isolating problems. It determines the path that your TCP/IP packets take to a given destination, entered as an IP address or domain name. The results are fairly straightforward.



Here is a completed trace from www.cs.cf.ac.uk to www.stairways.com:

Hop Min Avg Max Ip Name

1 0.001 0.002 0.004 131.251.1.42 mr1-e0.cf.ac.uk

2 0.010 0.034 0.076 194.83.178.17 c7000.cf.welshman.net.uk

3 0.006 0.008 0.010 146.97.252.93 welshnet.bristol-core.ja.net

4 0.015 0.017 0.019 146.97.252.190 ext-gw6.ja.net

5 0.012 0.017 0.023 193.63.94.95 us-gw3.ja.net

6 0.083 0.093 0.108 193.62.157.18 ny-pop.ja.net

7 0.088 0.090 0.094 207.45.196.141 if-8-2.core1.newyork.teleglobe.net

8 0.076 0.077 0.079 207.45.223.110 if-10-0.bb8.newyork.teleglobe.net

9 0.081 0.084 0.088 207.45.198.74 ix-8-0-1.bb8.newyork.teleglobe.net

10 0.083 0.087 0.092 152.63.22.218 518.at-6-0-0.xr1.nyc9.alter.net

11 0.083 0.087 0.090 152.63.20.66 181.at-2-0-0.tr1.nyc8.alter.net

12 0.192 0.200 0.206 152.63.5.214 124.at-6-0-0.tr1.por3.alter.net

13 0.189 0.192 0.198 152.63.104.253 297.atm6-0.xr1.sea1.alter.net

14 0.204 0.208 0.211 146.188.200.41 195.atm7-0.gw1.sea1.alter.net

15 0.163 0.164 0.166 137.39.136.6 ixa-gw.customer.alter.net

16 0.226 0.233 0.237 63.237.224.54

17 0.233 0.250 0.273 199.254.168.243

**Hop**

-- Gives the order in which the TCP/IP packets progress from machine to machine, called the 'distance' (in hops) from the originating machine.

**Result**

-- Received/Sent packets, or other information (see below). Assuming all is well, these numbers should match - if more packets are sent than received, there may be a problem.

**Min, Avg, & Max**

-- The Minimum, Average and Maximum round trip time in seconds that the packets took to go to and return from that machine.

**IP & Name**

-- The IP address and domain name of the remote machine which is conveying your TCP/IP packets. There are other possible values which can appear in the Result column, identifying network problems with the trace:

***How Trace Route Works: TTLs***

TTL (Time To Live): TTL is a value included in network packets, typically associated with the Internet Protocol (IP). It represents the maximum number of hops (routers) a packet can traverse before it is discarded. The TTL value is decremented at each hop.

Function of TTL: When a TCP packet is sent, its TTL is set. As it travels through routers, the TTL is reduced by one at each hop. When the TTL reaches zero, the packet is discarded, and an ICMP "time exceeded" message is generated by the router.

**Trace Route:** Trace Route is a network diagnostic tool that uses TTL to trace the route a packet takes to reach a destination host. It works by starting with a TTL of 1, sending a packet towards the destination, and listening for "time exceeded" responses.

**Identifying Intermediate Hops:** When the initiating machine receives a "time exceeded" response, it identifies the machine one hop away from the response packet. Then, it sends a new packet with a TTL of 2 and continues the process to identify the next hop, and so on.

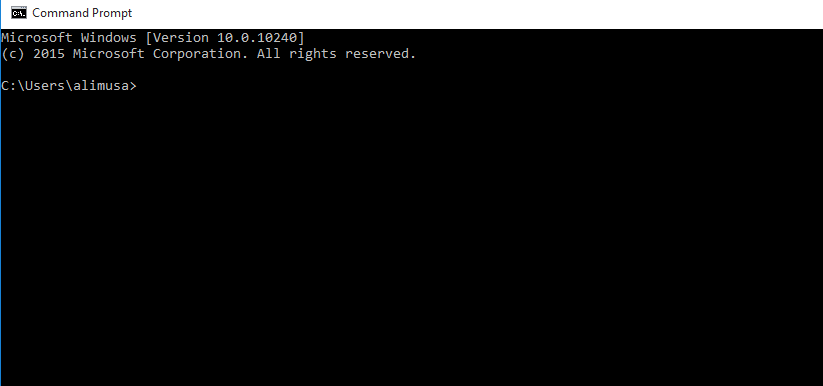
TCP Stack Variations: Not all TCP stacks behave the same way with respect to TTL. Some TCP stacks set the TTL for the ICMP "time exceeded" message to the value of the killed packet's TTL. This can result in two effects:

a**. Missing Information:** If an intermediate router has this behavior, it may not return "time exceeded" messages to the traceroute initiator, causing gaps in the trace.

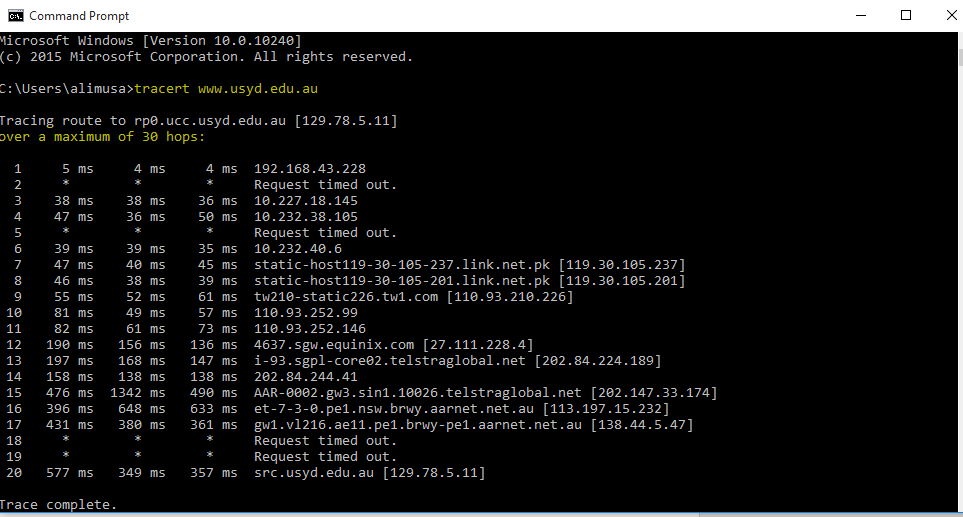
b. Missing Return Packets: If the destination host's TCP stack exhibits this behavior, return packets won't reach the originating machine unless the TTL is high enough to cover the round trip. This results in a number of failed connections in the trace, equal to the number of hops to the destination minus one.

**Steps for performing this lab:**

1. **Open the command prompt application**



1. Type “tracert www.sydney.edu.au”(or traceroute) in command prompt and press enter.

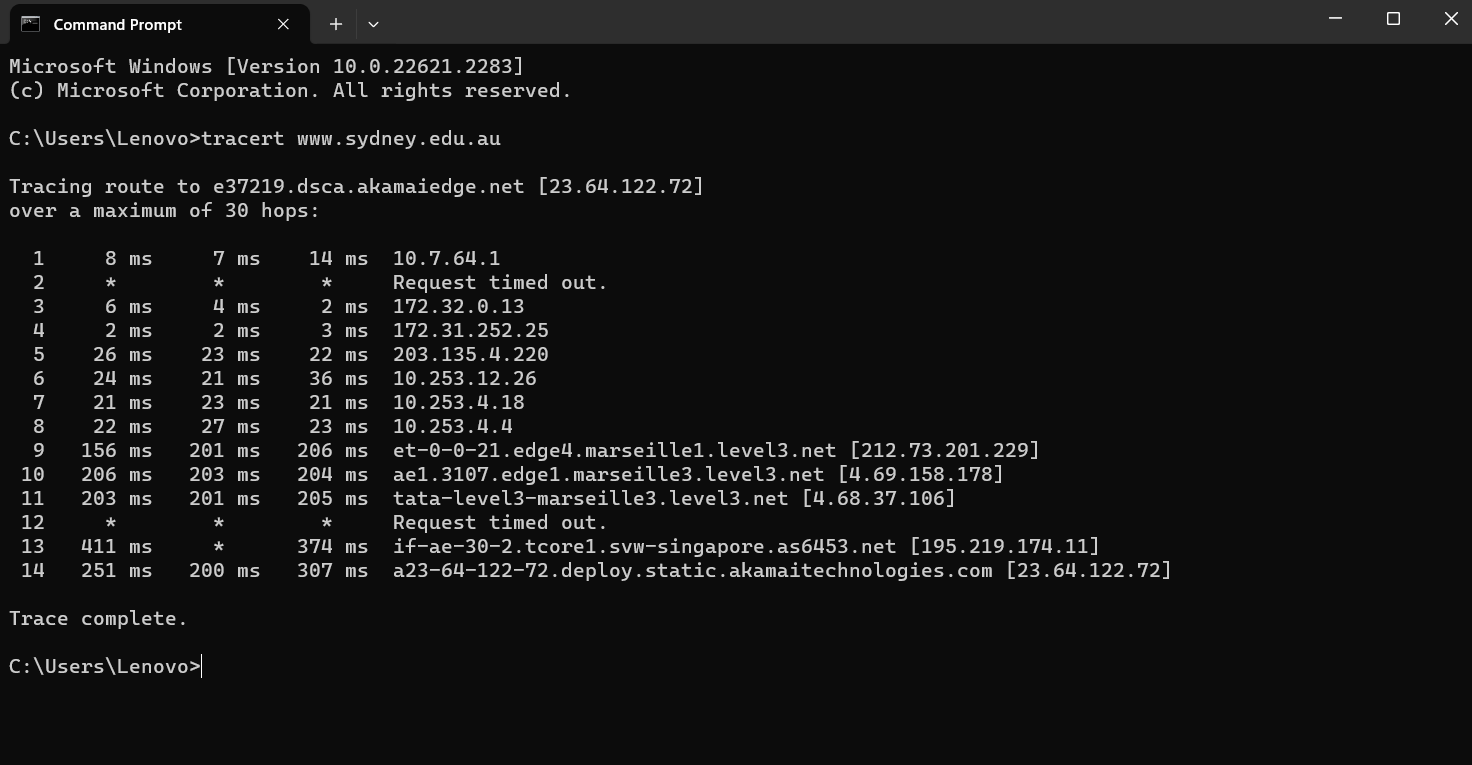


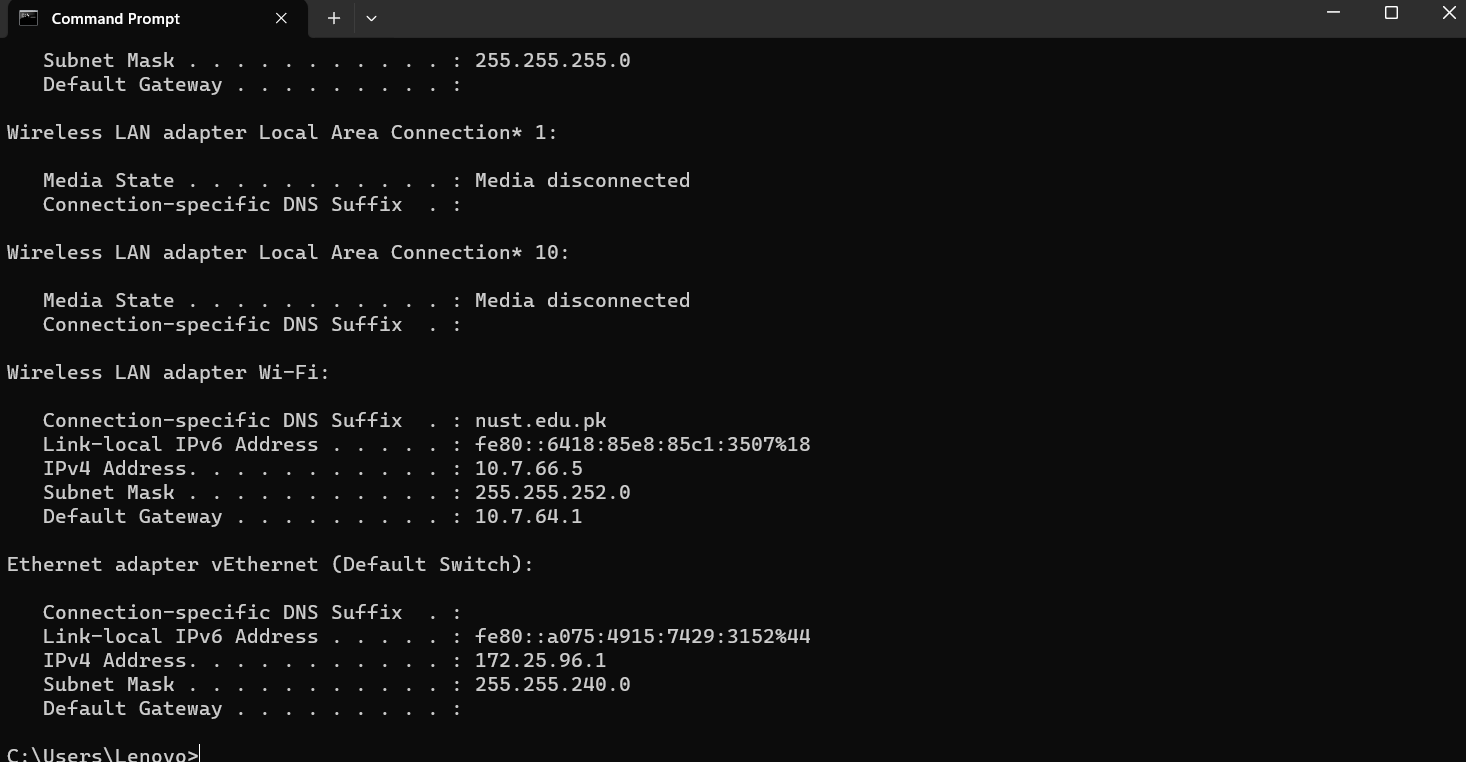
**Now answer the following questions:**

1. What are the IP address of the host www.sydney.edu.au and the IP of your machine?

**IP address of host** www.sydney.edu.au**:** 23.64.122.72

**IP address of my machine:** 10.7.66.5





1. How many hops is the destination host away from your machine?

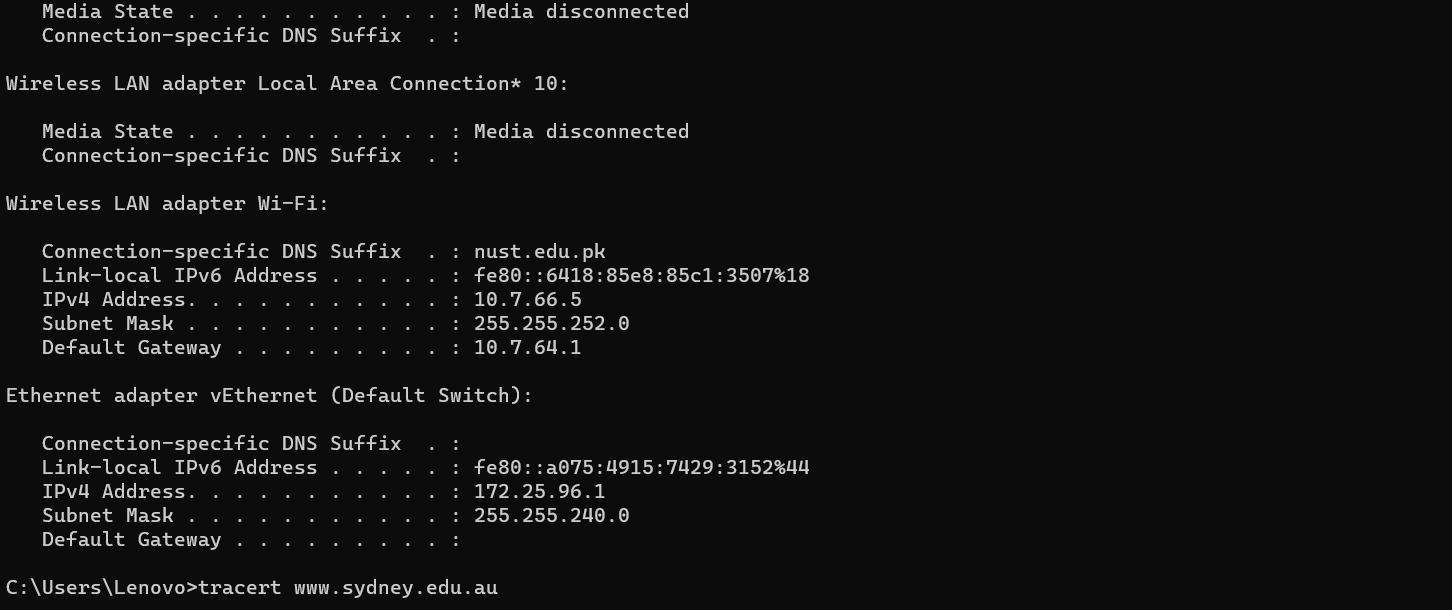
**The destination is 12 hops away from my machine.**

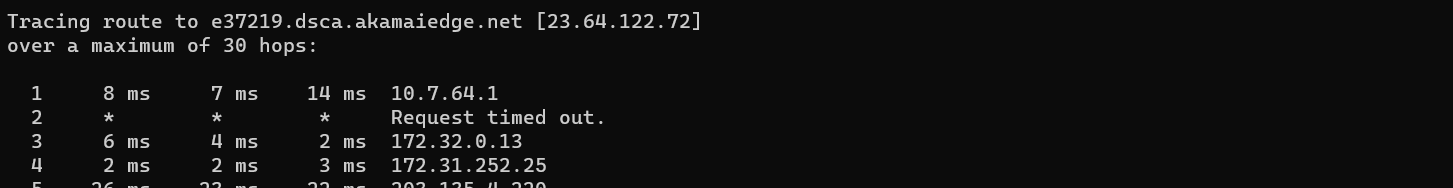
A screenshot of a computer

Description automatically generated

1. How many hops are between your machine and the NUST gateway router?

**My machine is one hops away from the NUST gateway router.**

****



1. How many routers does these packets visit in Pakistan?

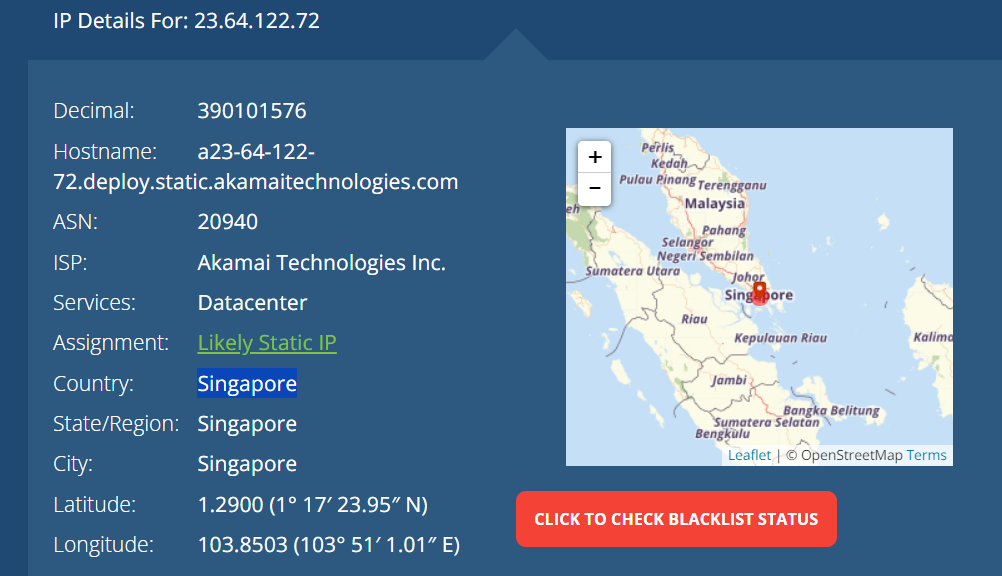
**The packet visits two routers with IP 10.7.64.1(NUST default gateway), IP 203.135.4.220 in Pakistan.**

**A computer screen with white text

Description automatically generated**

1. Where is the website www.sydney.edu.au hosted (city and country)?

This website is hosted in city of Singapore and country of Singapore.

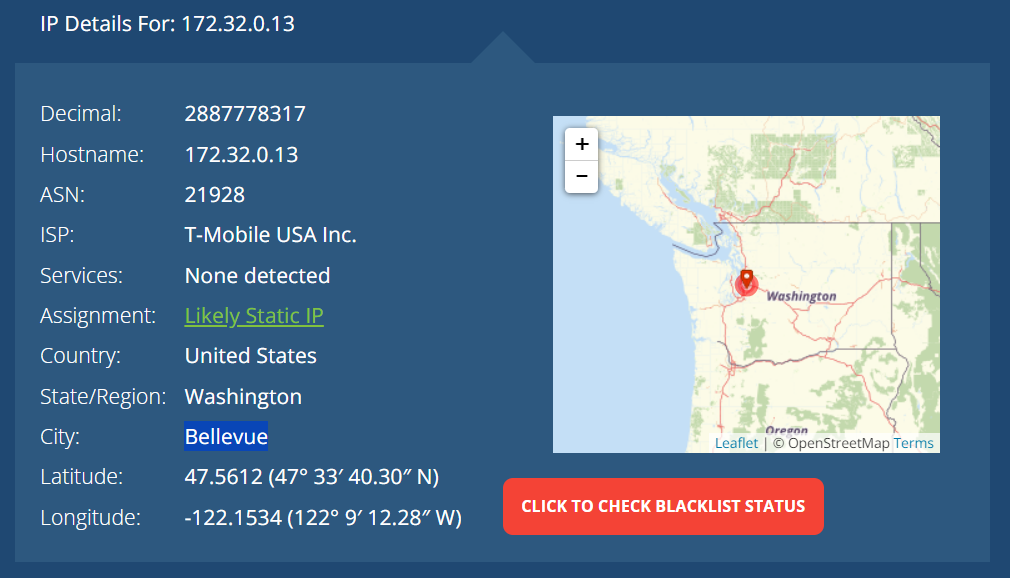


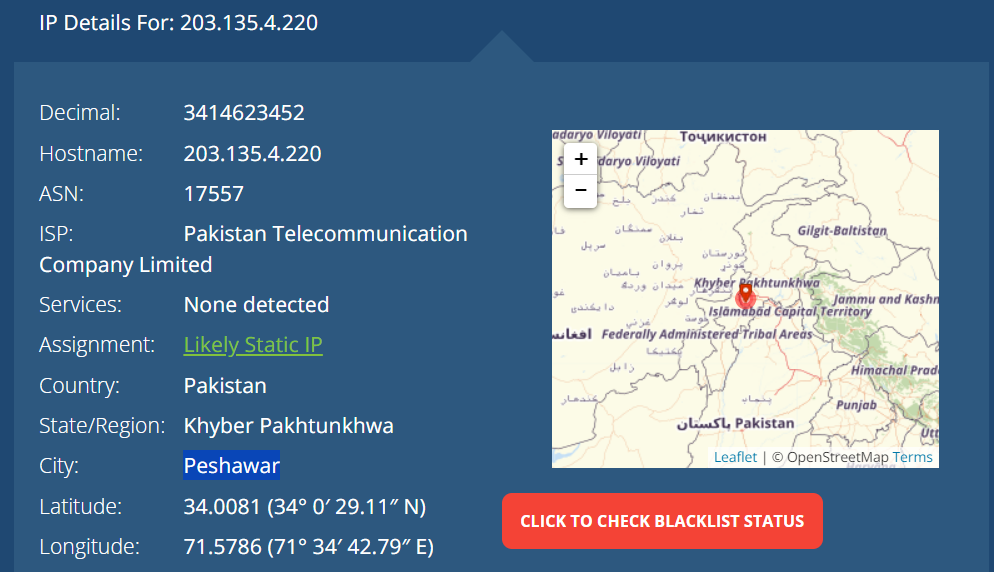
1. How many cities your packets have actually visited? List all these cities along with the name of country in the order these have been visited?

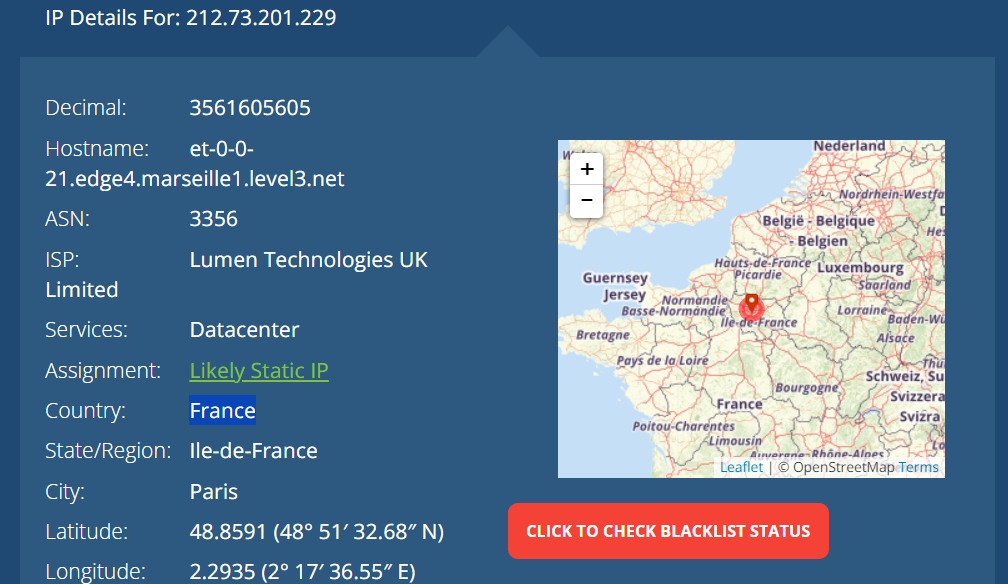
Hint> Check the result of tracert each and every IP indicate specific city country use ip location and ip finder apps

The packets have visited a total of 5 cities. i.e Bellevue, Peshawar, Paris, Marseille, Singapore.

|  |  |  |
| --- | --- | --- |
| **IP address** | **City** | **Country** |
| 10.7.64.1 | Private(unknown) | Private(unknown) |
| 172.32.0.13 | Bellevue | United States |
| 172.31.252.25 | Private(unknown) | Private(unknown) |
| 203.135.4.220 | Peshawar | Pakistan |
| 10.253.12.26 | Private(unknown) | Private(unknown) |
| 10.253.4.18 | Private(unknown) | Private(unknown) |
| 10.253.4.4 | Private(unknown) | Private(unknown) |
| 212.73.201.229 | Paris | France |
| 4.69.158.178 | Marseille | France |
| 4.68.37.106 | Marseille | France |
| 195.219.174.11 | Marseille | France |
| 23.64.122.72 | Singapore | Singapore |







A screenshot of a map

Description automatically generated

A screenshot of a map

Description automatically generated

A screenshot of a map

Description automatically generated

1. Comment if you observe any abnormal/wayward path followed by the traffic from your machine to the destination (It may be useful to roughly draw the path followed by the traffic on a map).

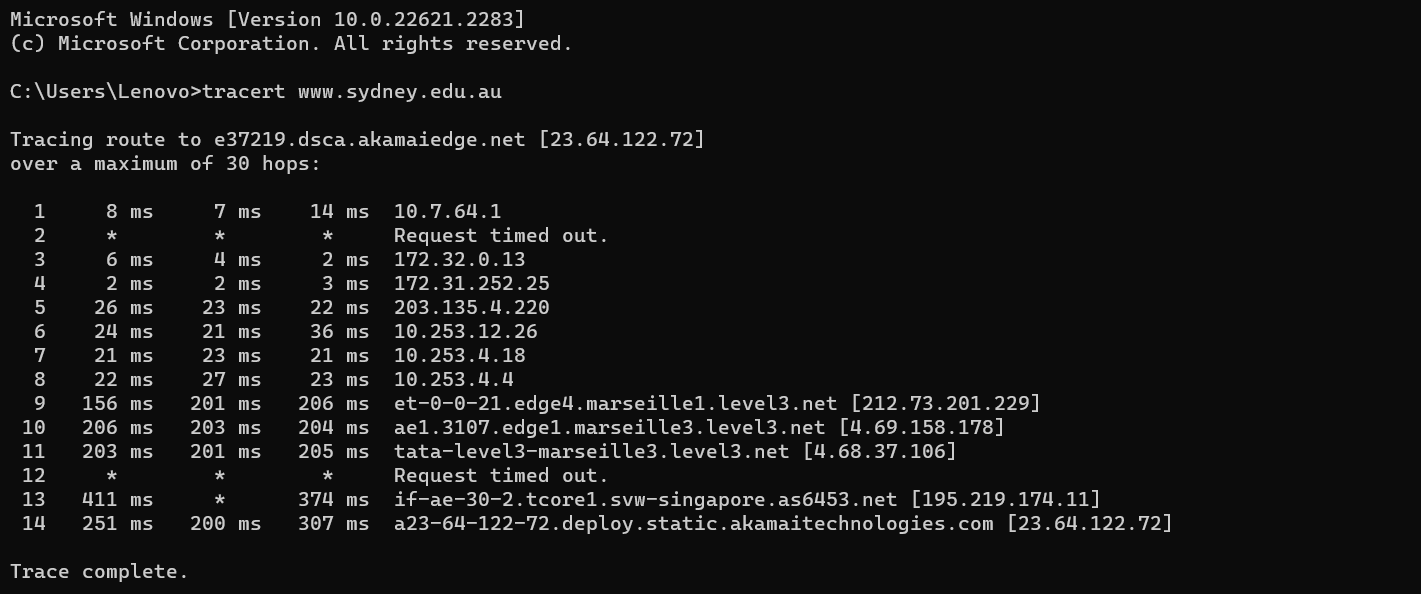
The path followed by the traffic from my machine to the destination is from Pakistan to United states then coming back to Pakistan then to France and then it reached the destination in Singapore. The abnormal path followed by my traffic is going from Pakistan to United States and then coming back to Pakistan.

1. Does the generated traffic always follow the same path to this destination?

Hint> Run tracert command and compare the results

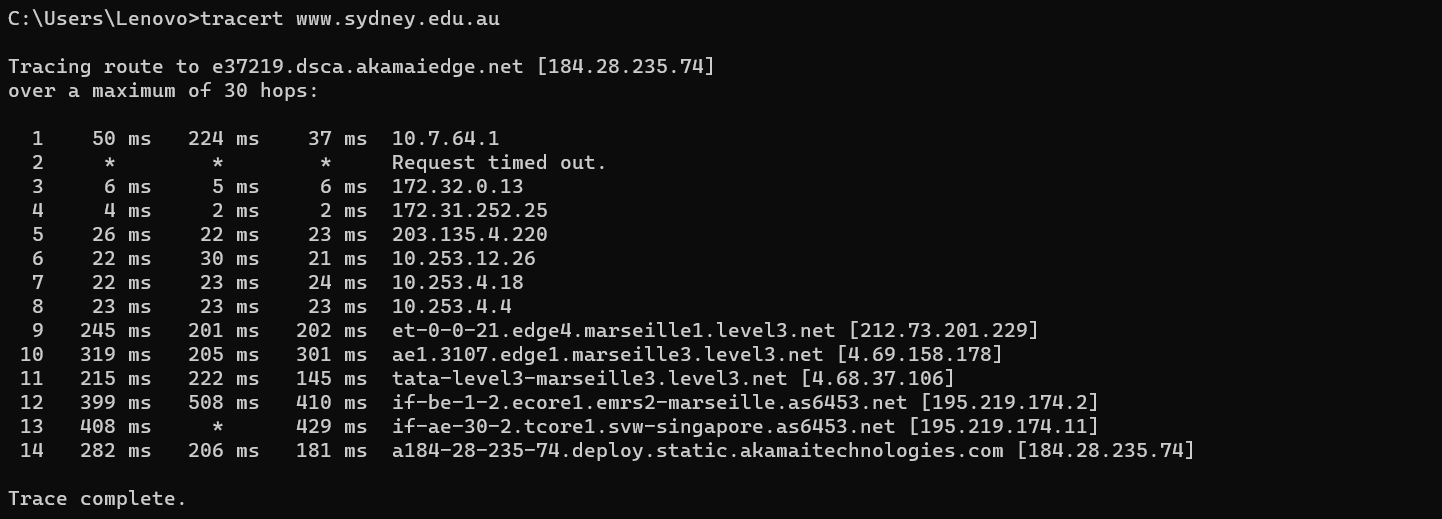
No, it does not always follow the same path to this destination.

**1st Trace Route:**



|  |  |  |
| --- | --- | --- |
| **IP address** | **City** | **Country** |
| 10.7.64.1 | Private(unknown) | Private(unknown) |
| 172.32.0.13 | Bellevue | United States |
| 172.31.252.25 | Private(unknown) | Private(unknown) |
| 203.135.4.220 | Peshawar | Pakistan |
| 10.253.12.26 | Private(unknown) | Private(unknown) |
| 10.253.4.18 | Private(unknown) | Private(unknown) |
| 10.253.4.4 | Private(unknown) | Private(unknown) |
| 212.73.201.229 | Paris | France |
| 4.69.158.178 | Marseille | France |
| 4.68.37.106 | Marseille | France |
| 195.219.174.11 | Marseille | France |
| 23.64.122.72 | Singapore | Singapore |

**2nd Trace Route:**

****

|  |  |  |
| --- | --- | --- |
| **IP Address** | **City** | **Country** |
| 10.7.64.1 | Private(unknown) | Private(unknown) |
| 172.32.0.13 | Washington | United States |
| 172.31.252.25 | Private(unknown) | Private(unknown) |
| 203.135.4.220 | Peshawar | Pakistan |
| 10.253.12.26 | Private(unknown) | Private(unknown) |
| 10.253.4.18 | Private(unknown) | Private(unknown) |
| 10.253.4.4 | Private(unknown) | Private(unknown) |
| 212.73.201.229 | Paris | France |
| 4.69.158.178 | Marseille | France |
| 4.68.37.106 | Marseille | France |
| 195.219.174.2 | Marseille | France |
| 195.219.174.11 | Marseille | France |
| 184.28.235.74 | Singapore | Singapore |

1. **How many routers in the path are working in “safe mode” (not replying to any query)?**

Two routers in the path are working in safe mode as their traceroute output is being shown by an asterisk (\*). This happens because some organizations block or discard the type of packets that traceroute rely on, instead of replying, using firewall or some configuration routers.

1. **Which hop is the longest in the path to the destination?**

The longest hop in the path is hop 10 with IP 4.69.158.178 and an average roundtrip time of 203ms.The shortest hop in the path is hop 3 with IP 172.31.252.25 and an average roundtrip time of 2ms.

