**ASSIGNMENT – 1**

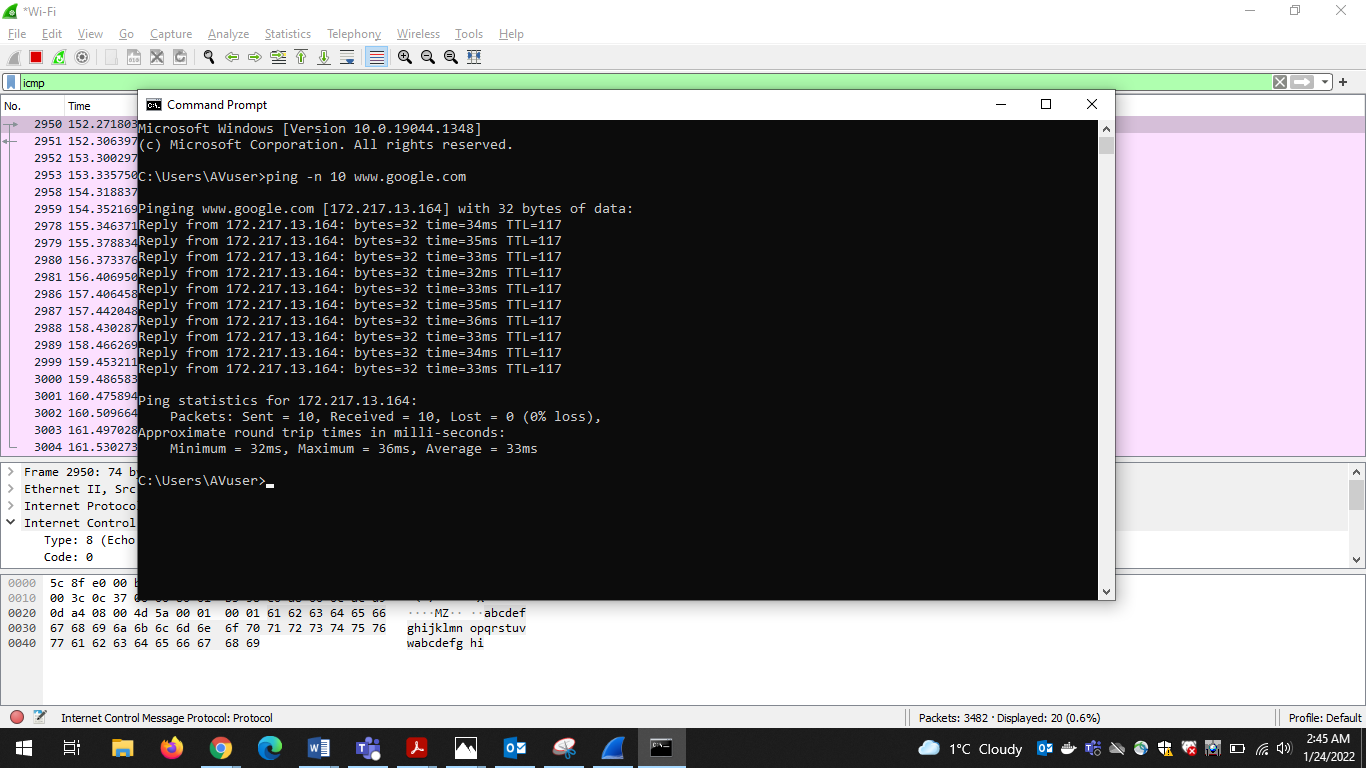
**CSCI-6708 Advanced Network Security**

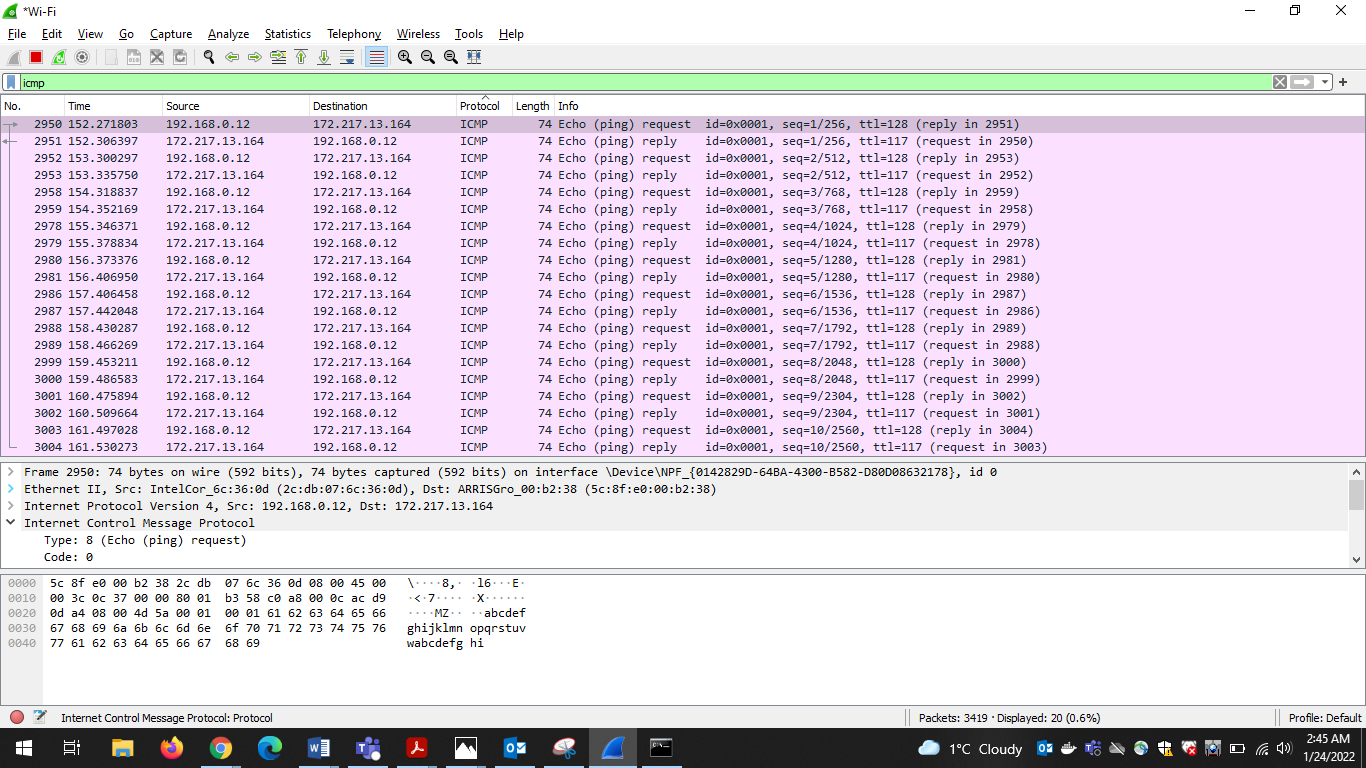
**Sumit Singh**

**B00882103**

[**Sm435410@dal.ca**](mailto:Sm435410@dal.ca)

**PART 1**





1. My IP address is :192.168.0.12

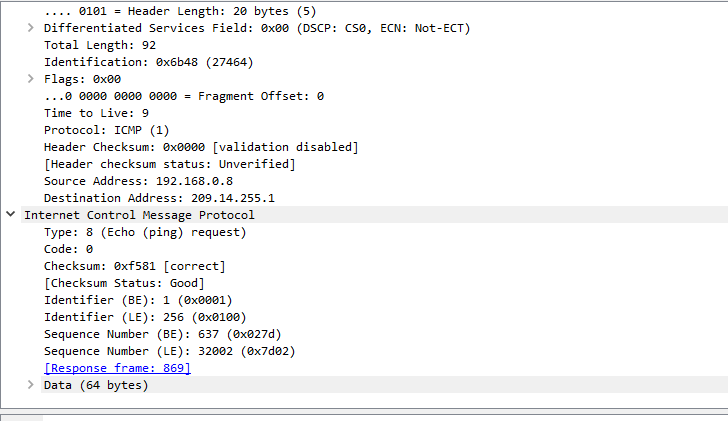
Destination IP Address is: 172.217.13.164

1. ICMP type: 8 (Echo (ping) request)

Code: 0

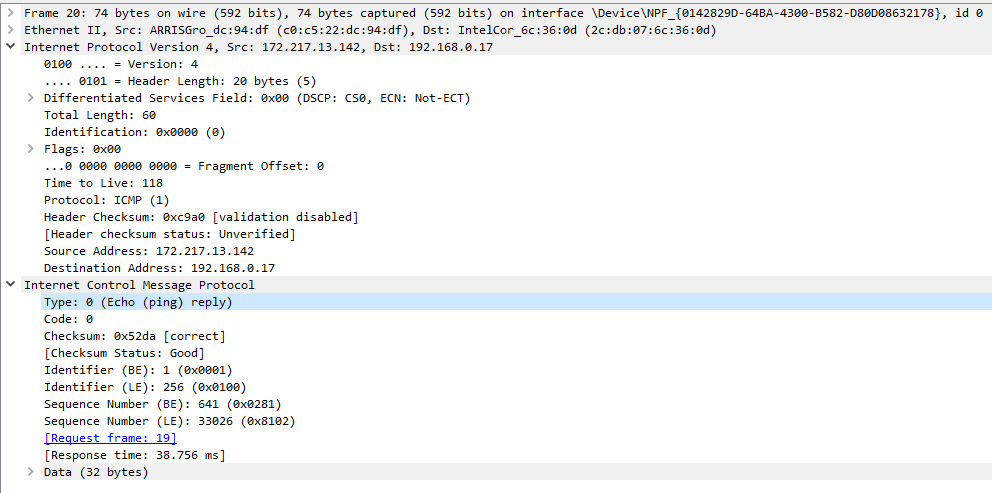
Type specifies the type of ICMP message, like type 8 means request message and type 0 is used for a reply also type 3 for destination unreachable message.

Code specifies what kind of ICMP message it is. Just for destination unreachable message we have 16 different codes. Code 0 means network was unreachable.

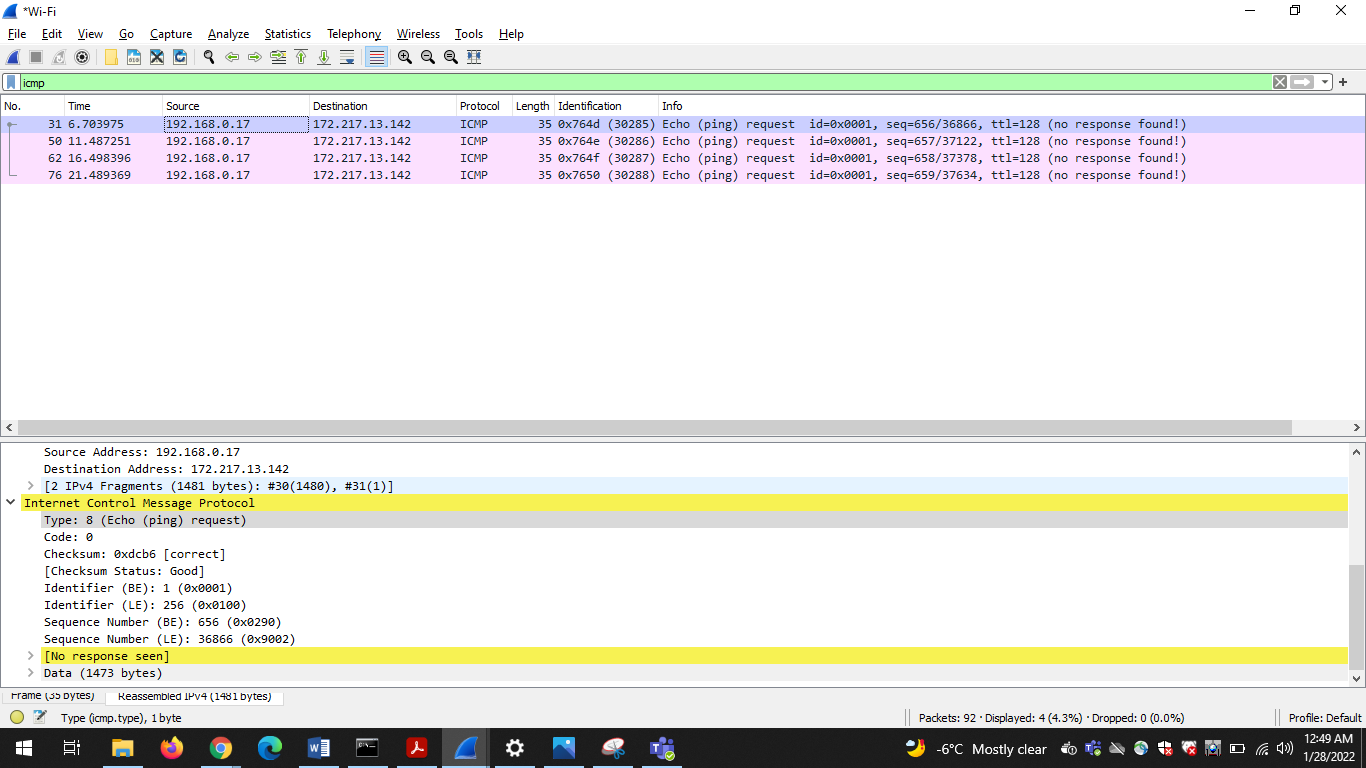
1. Port number are features of transport layer protocols such as TCP and UDP. ICMP packets do not have source and destination port number because it communicates network layer information between hosts and routers and not between application layer processes. Type and code combined is use to identify specific messages.
2. Following are the other fields in ICMP message and their values.
3. ICMP Type in reply packet is: 0 (Echo (ping) reply). ICMP message type 0 means Echo reply

Code for ICMP reply packet is: 0. Code 0 for net is unreachable.

1. Following are the other fields in ICMP reply message with their values.



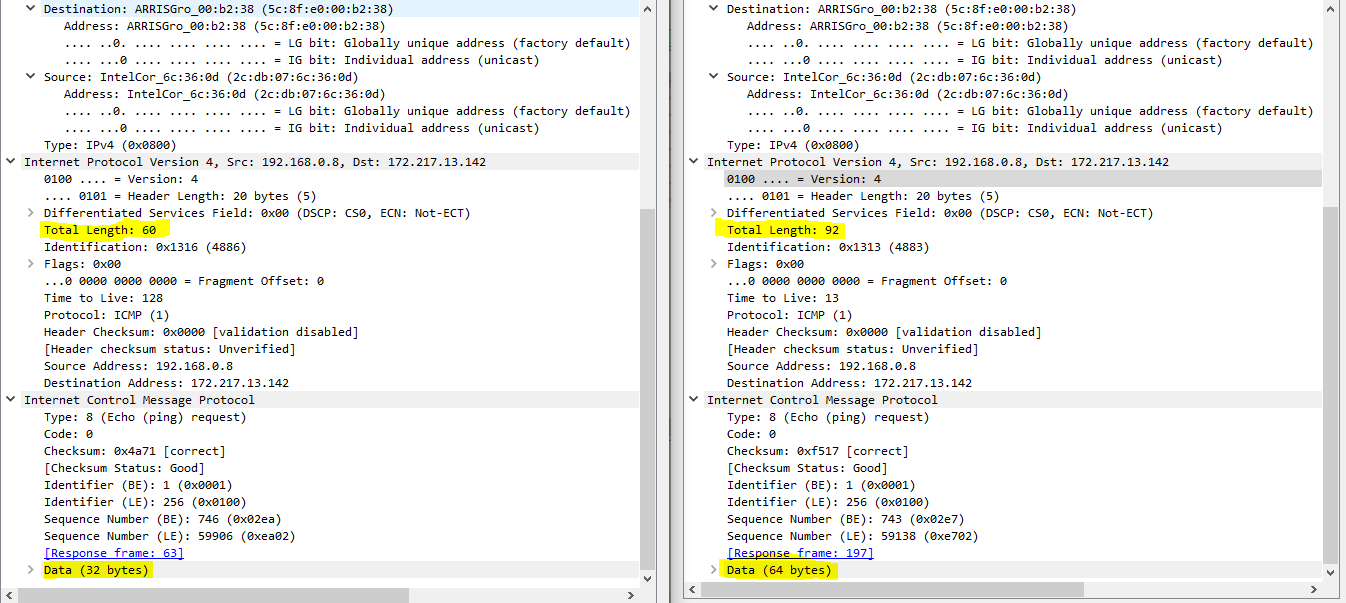
**Part 2:**



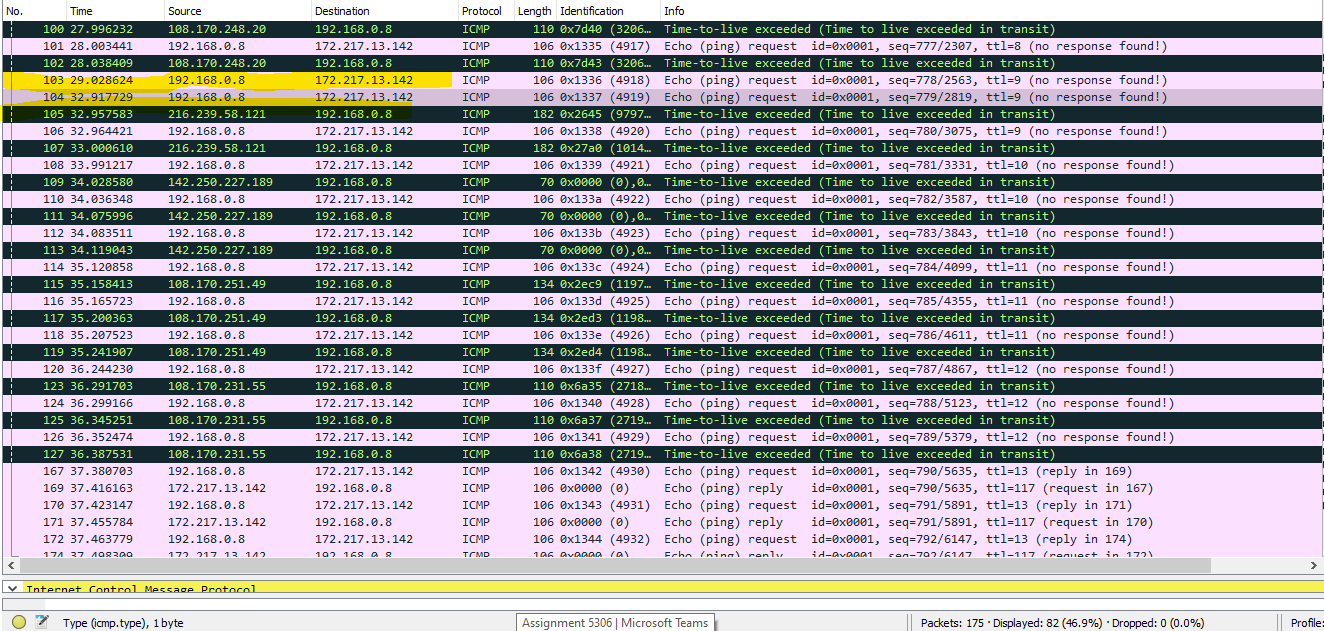
1. I was sending ping to google and its maximum packet size is 1472 bytes.
2. As we don’t have any reply packets it seems packet is being dropped at the very beginning.
3. Web servers prevent large pings to avoid issues like ping of death. It has to do with DoS attack where an attacker can deliberately send IP packet with larger then 65536. Other reason is to avoid PING FLOOD problem, it is a simple denial-of-service attack where attacker overwhelms the server with ICMP request ping packets which will consume large amount of CPU for this operation and leads to server slowdown.

**Part 3:**

1. The only difference I see in their request message is data size



Difference is same for reply packet too. Few other differences that can be observed in reply packet is response time for ping is greater and as tracert has multiple types of reply packet, few of them have ICMP reply time as 11.



There are few error responses in tracert command, the one highlighted yield to \* error in traceroute but has no error packer. And those in the black color are time-to-live exceeded error packets which has ICMP message type 11.

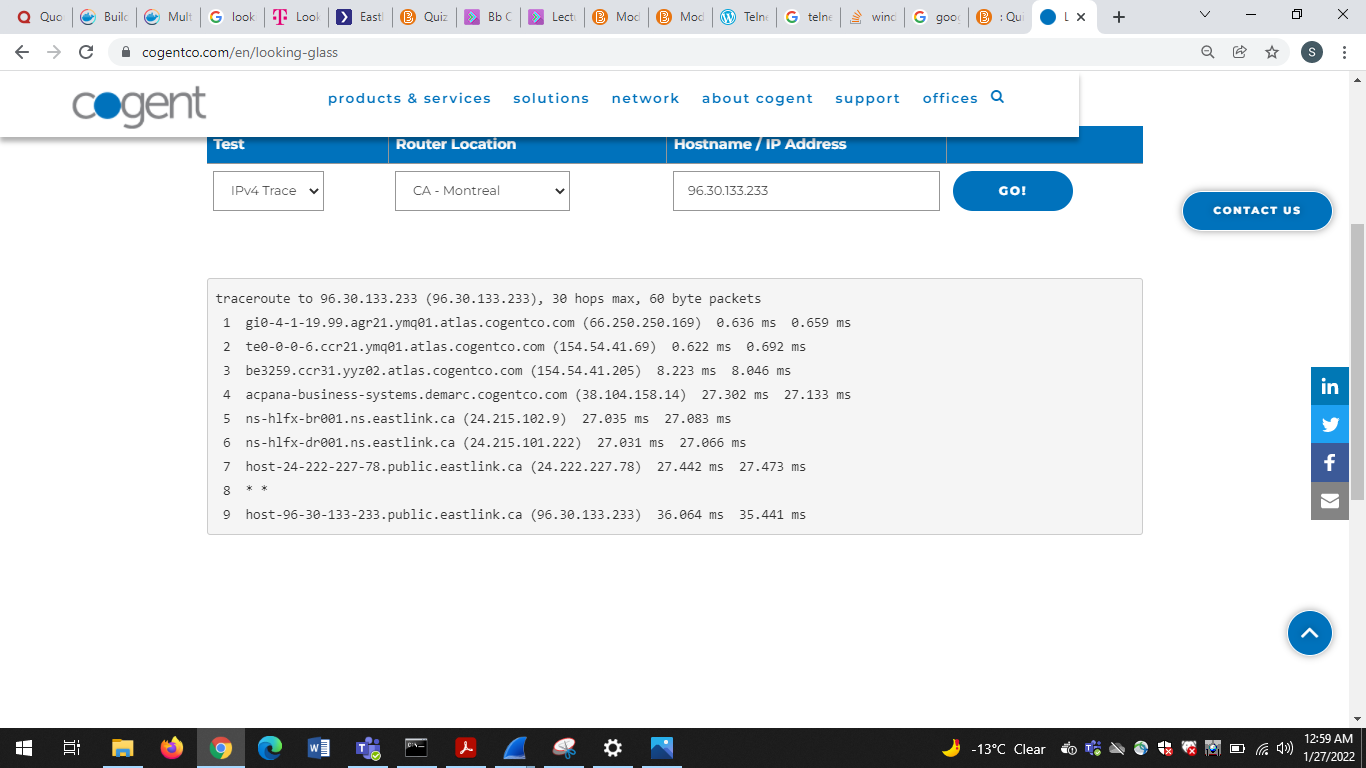
1. -T: option in linux is used for making use of TCP SYNC for the requests. I cannot find an alternative for this command in windows so I was unable to execute it.

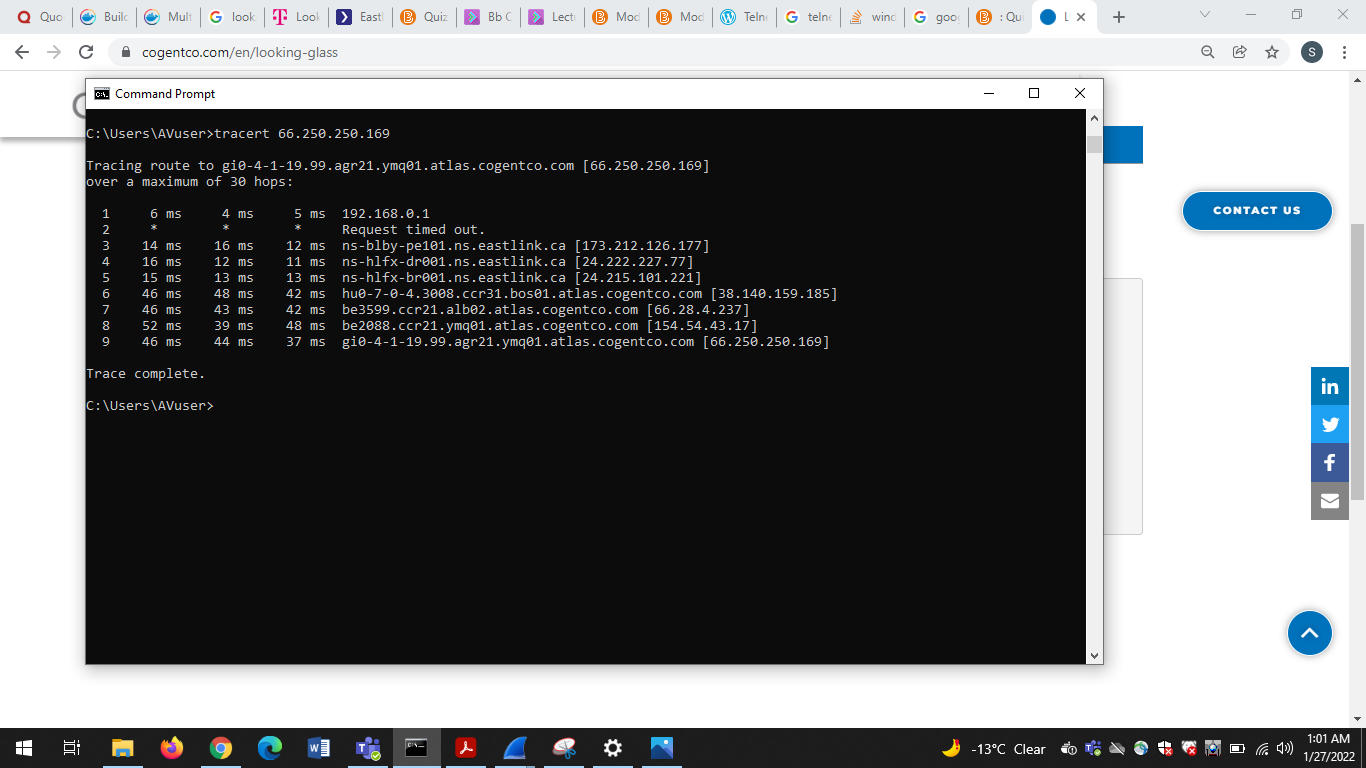
-d: option in unix version is used to enable debugging. But where as in windows it is used for not resolving address to hostname. There is no alternative in windows to -d, so I am unable to execute this command.

1. -S srcaddr option in linux enable use of IPv6 only source address, it makes use of ipv6 address given in command as source address. This option has few security issues as it results in address spoofing

**Part 4:**

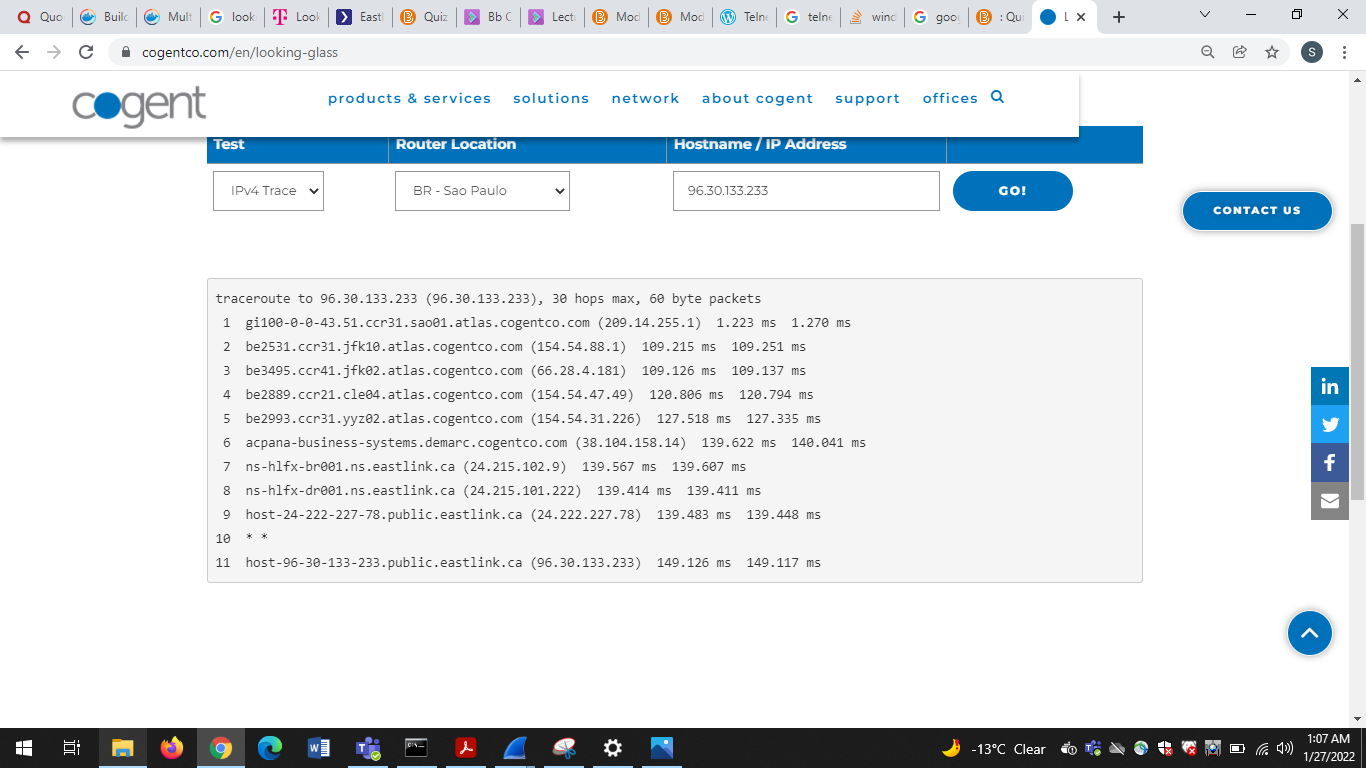
1. Cogentco server for north America.

Forward path:

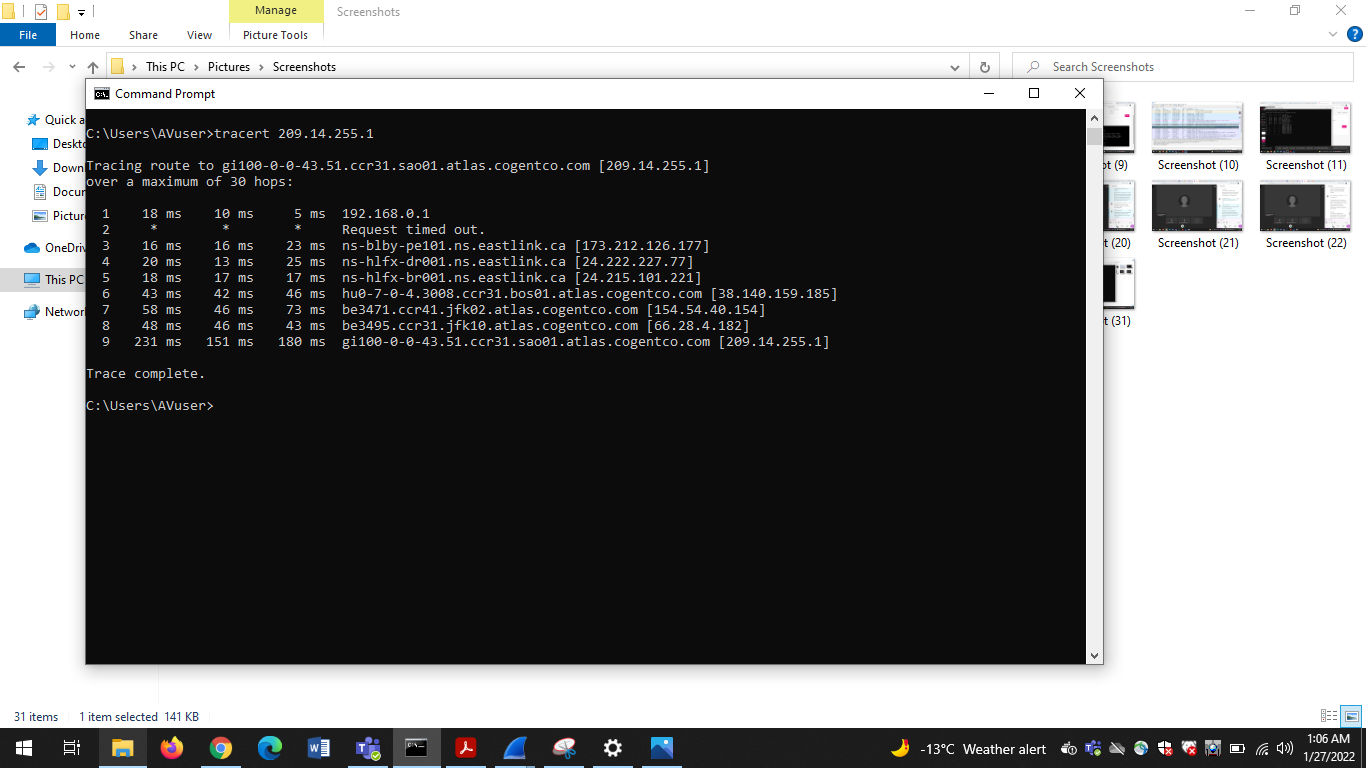
Reverse path: 

1. Cogentco server for South America

Forward path:

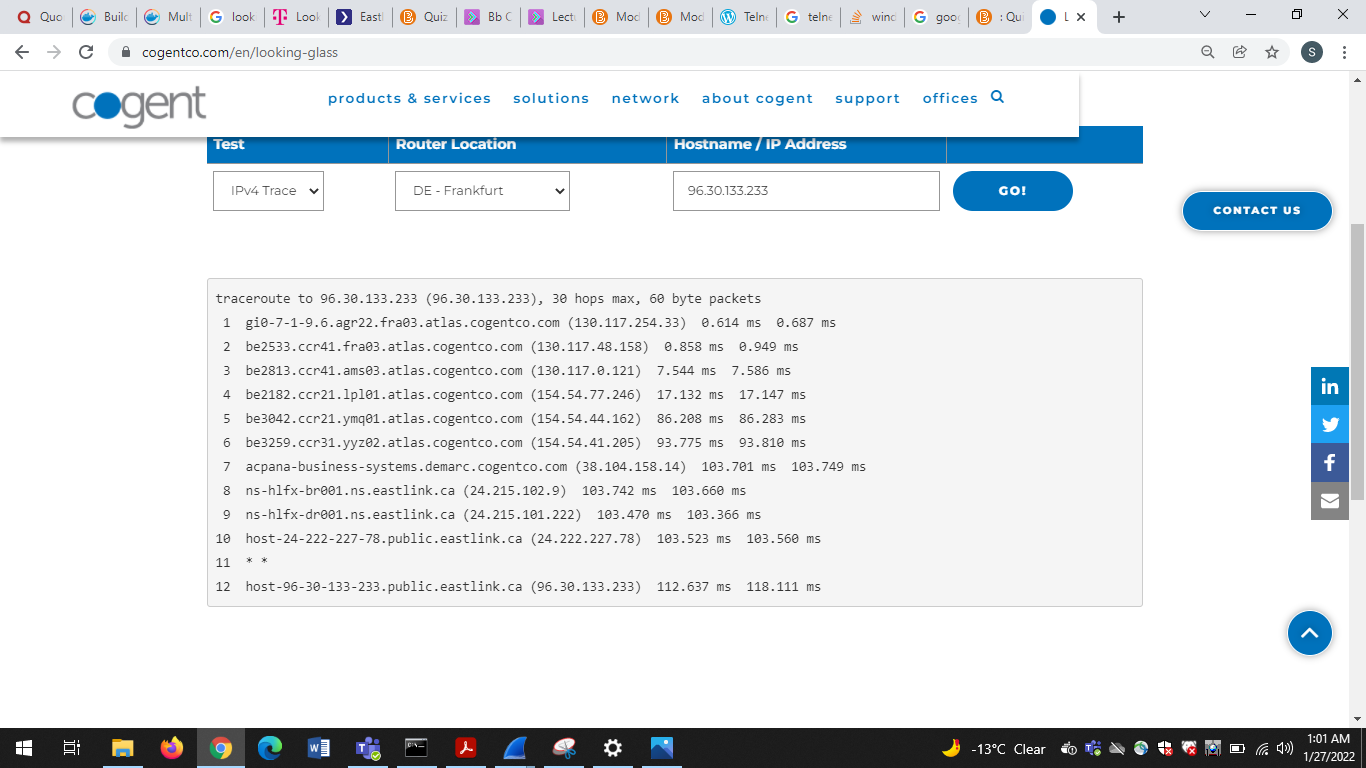


Reverse path:

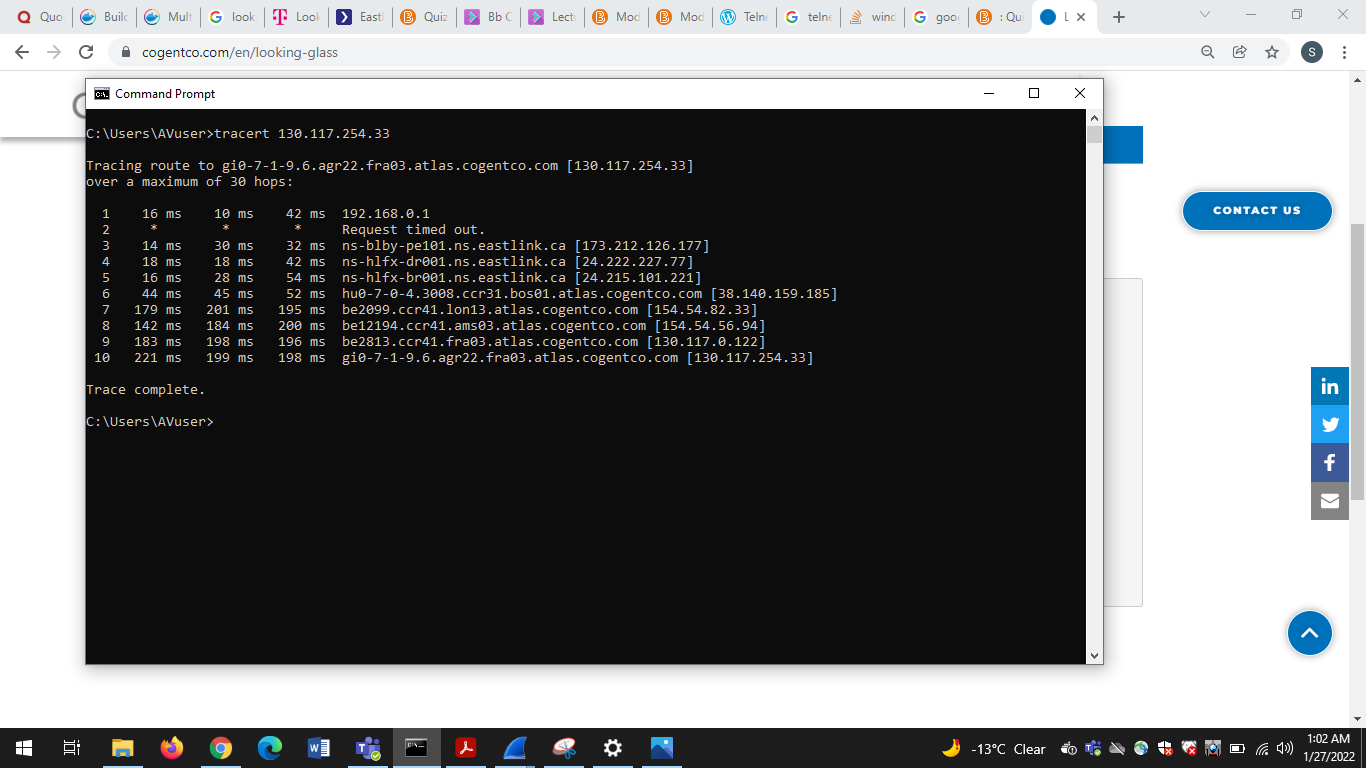


1. Cogentco server for Europe

Forward path:

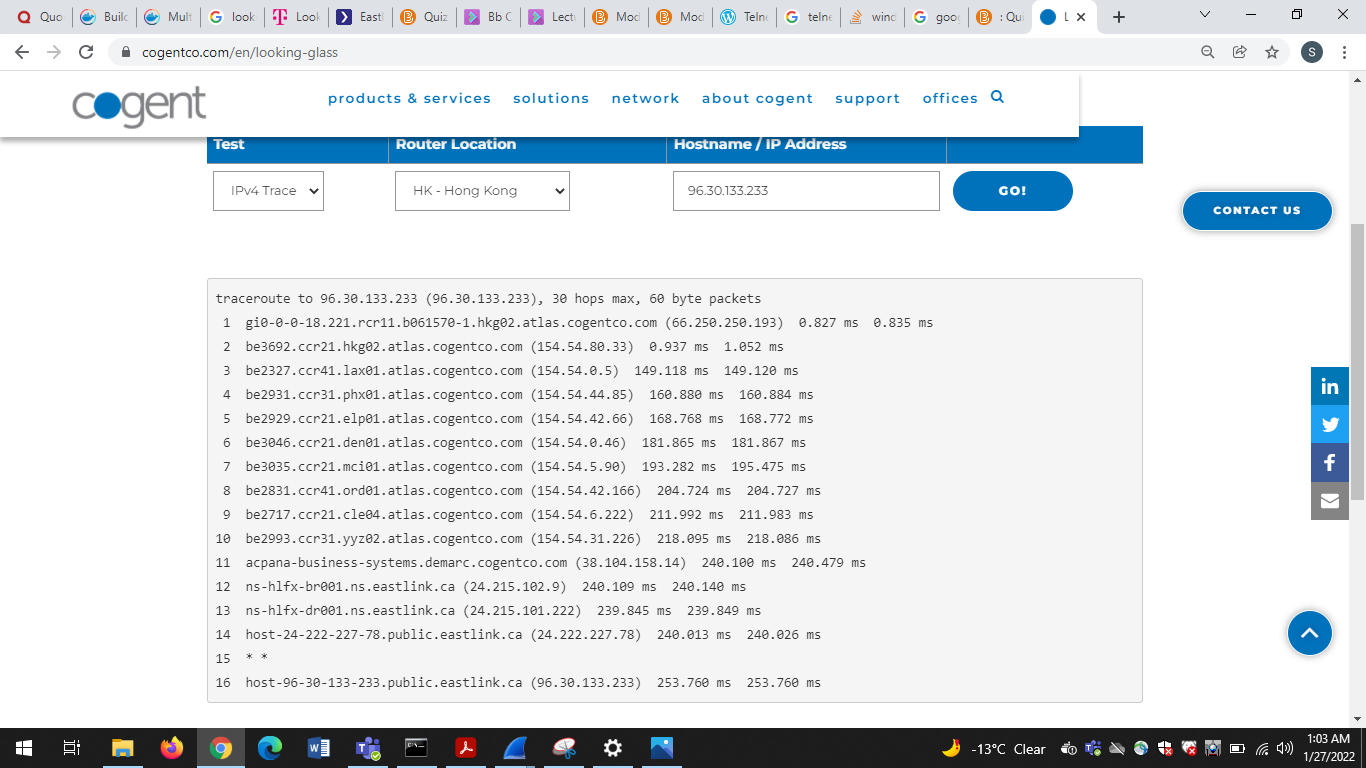


Reverse path:

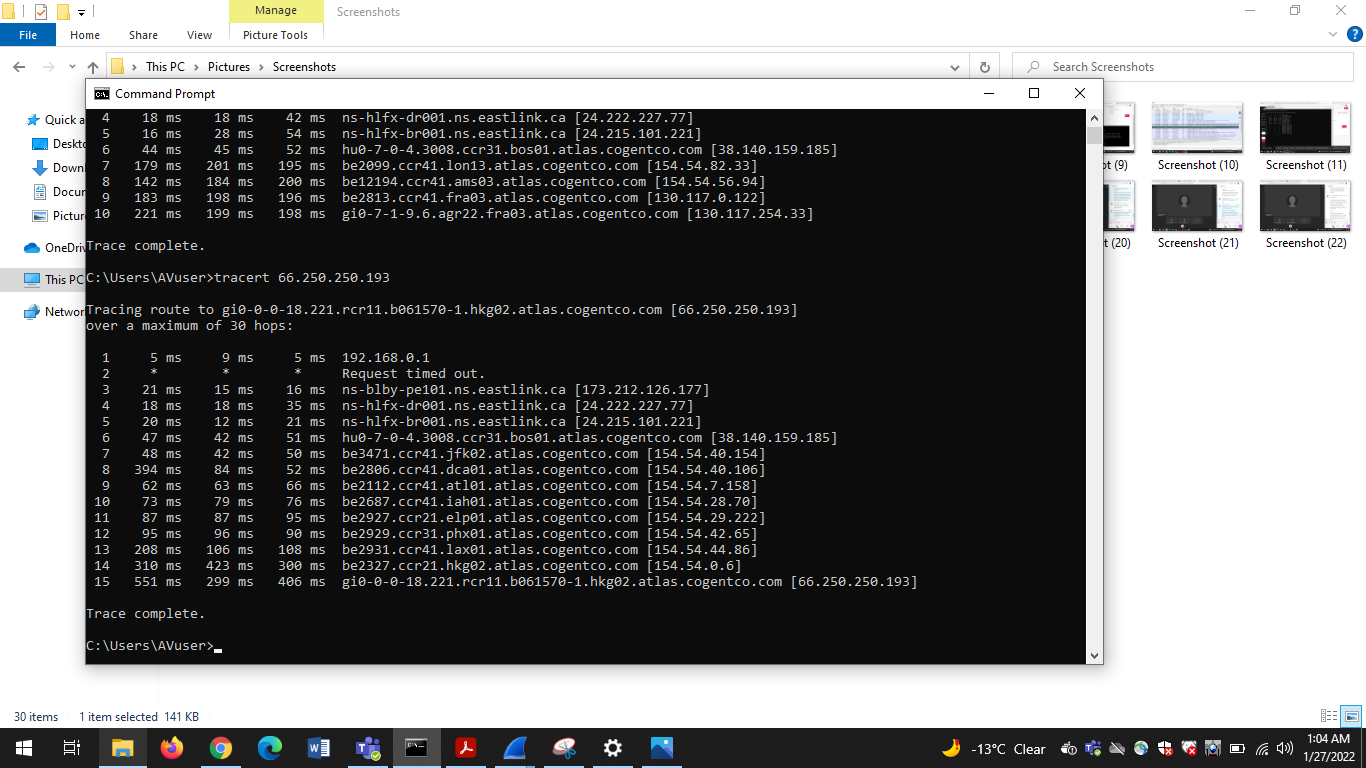


1. Cogentco server for Asia

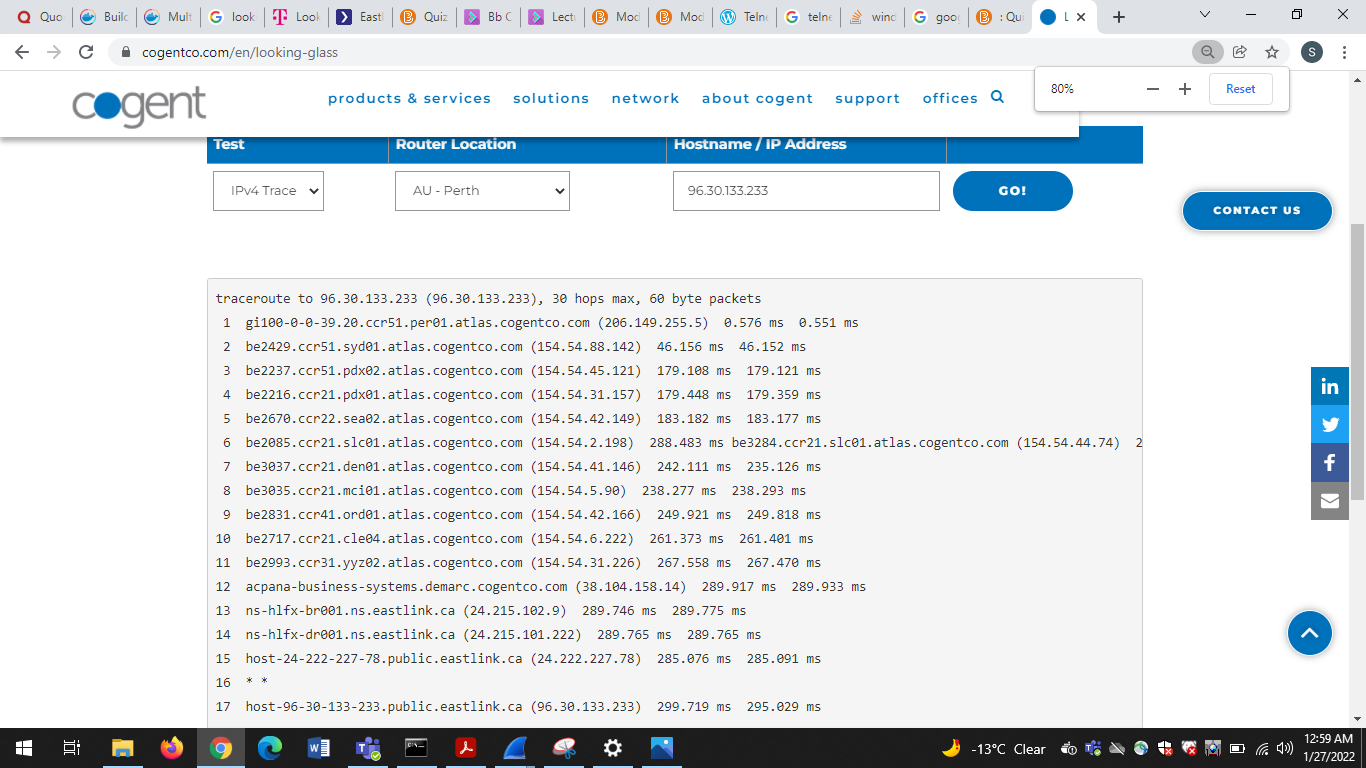
Forward path:



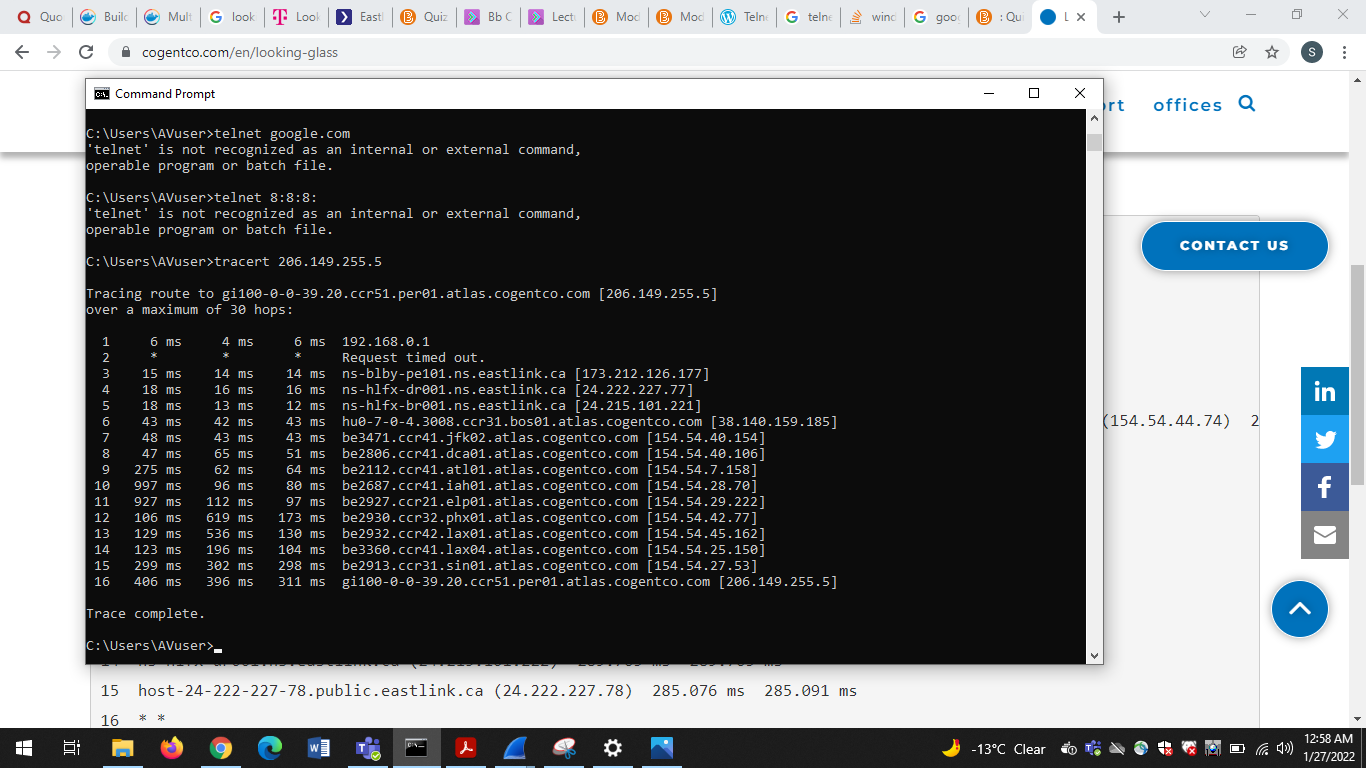
Reverse path:



1. Cogentco server for Australia

Forward path:

Reverse path:



The major difference that I can see between reverse and forward path is turnaround time. And number of hops are different from reverse to forward, forward path has more .no of hops. When looked at wired shark we see icmp messages for reverse but not for forward because it may be handled by other protocols at the server end.

**References:**

[1]M. Pramatarov, "Traceroute command and its options - ClouDNS Blog", *ClouDNS Blog*, 2022. [Online]. Available: https://www.cloudns.net/blog/traceroute-command-tracert/. [Accessed: 28- Jan- 2022]

[2]"ShieldSquare Captcha", *Networklessons.com*, 2022. [Online]. Available: https://networklessons.com/cisco/ccie-routing-switching-written/icmp-internet-control-message-protocol#:~:text=ICMP%20(Internet%20Control%20Message%20Protocol)%20is%20a%20network%20protocol%20used,for%20diagnostics%20and%20network%20management.&text=For%20example%2C%20type%208%20is,of%20ICMP%20message%20it%20is. [Accessed: 28- Jan- 2022]

[3]W. numbers?, B. Wankhede, R. Trunk, W. Tigger and R. Maupin, "Why doesn’t ICMP use port numbers?", *Network Engineering Stack Exchange*, 2022. [Online]. Available: https://networkengineering.stackexchange.com/questions/50955/why-doesn-t-icmp-use-port-numbers. [Accessed: 28- Jan- 2022]

[4]"Internet Control Message Protocol (ICMP) Parameters", *Iana.org*, 2022. [Online]. Available: https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-codes-0. [Accessed: 28- Jan- 2022]

[5]"ICMP (Internet Control Message Protocol)", *NetworkLessons.com*, 2022. [Online]. Available: https://networklessons.com/cisco/ccie-routing-switching-written/icmp-internet-control-message-protocol#:~:text=A%20good%20example%20is%20the,error%20message%20to%20the%20source.&text=When%20you%20see%20code%200,the%20destination%20host%20was%20unreachable. [Accessed: 28- Jan- 2022]

[6]W. &#39;ping&#39;?, V. M and A. Waters, "Why do companies block 'ping'?", *Super User*, 2022. [Online]. Available: https://superuser.com/questions/318870/why-do-companies-block-ping#:~:text=It%20has%20to%20do%20with,allowed%20by%20the%20IP%20protocol. [Accessed: 28- Jan- 2022]

[7]S. PING?, M. Jefferson and T. Pornin, "Security risk of PING?", *Information Security Stack Exchange*, 2022. [Online]. Available: https://security.stackexchange.com/questions/4440/security-risk-of-ping. [Accessed: 28- Jan- 2022]

[8]"Looking Glass", *Cogentco.com*, 2022. [Online]. Available: https://www.cogentco.com/en/looking-glass. [Accessed: 28- Jan- 2022]

[9]"What is a Denial-of-Service Attack?", *SearchSecurity*, 2022. [Online]. Available: https://searchsecurity.techtarget.com/definition/denial-of-service. [Accessed: 28- Jan- 2022]

[10]"What is a Traceroute and How Do Traceroutes Work? | Obkio", *Obkio*, 2022. [Online]. Available: https://obkio.com/blog/traceroutes-what-are-they-and-how-do-they-work/. [Accessed: 28- Jan- 2022]