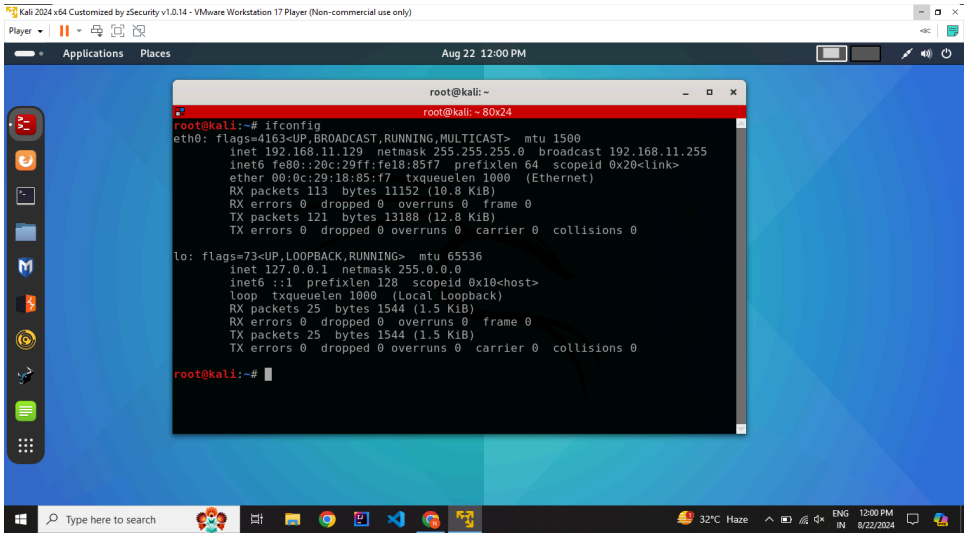
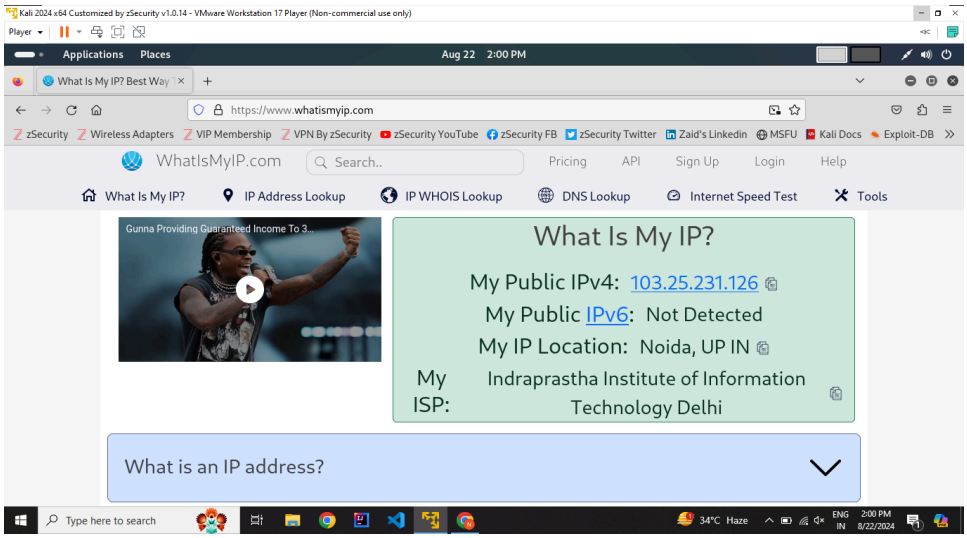
1) a) To figure out the IP address of our network interface we can use the ifconfig command which will display the Private IP address of the network interface.
Running ifconfig on the VM gave the following output with the Private IP address of the eth0 (wired ethernet) as below.
IPv4: 192.168.11.129
IPv6: fe80::20c:29ff:fe18:85f7

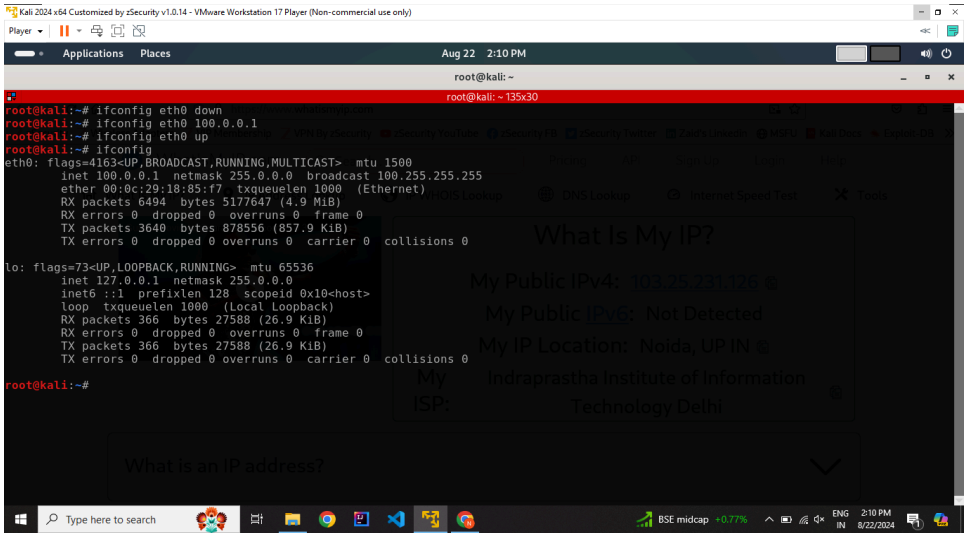



b) The IPv4 address shown on the website: https://www.whatismyip.com comes out to be: 103.25.231.126 as shown below:-

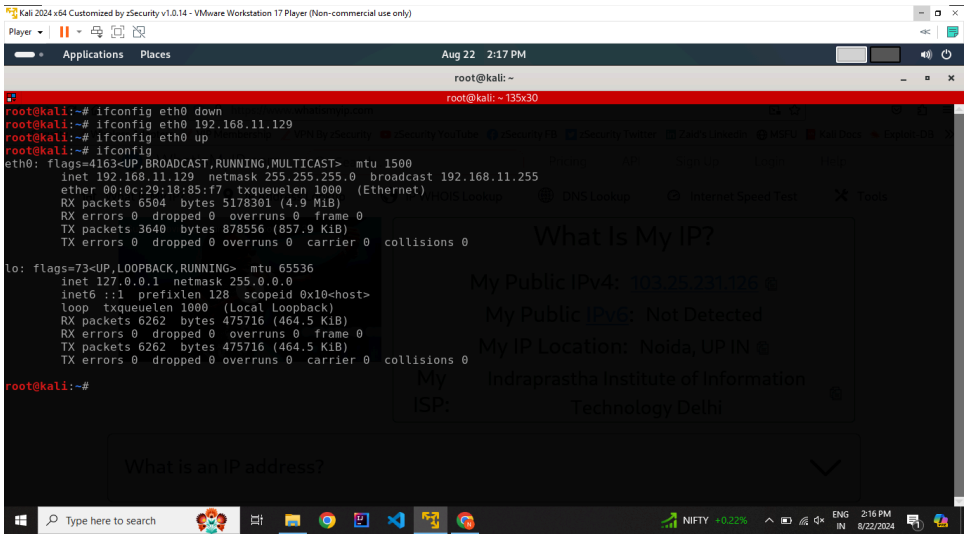



Both the addresses were different. Ths is because the command ifconfig shows the private IP address of the network interface which starts from 10.0. 0.0 to 10.255. 255.255, 172.16. 0.0 to 172.31. 255.255, 192.168. 0.0 to 192.168. 255.255. (mine was192.168.11.129) wheres the website gives us the public (global) IP address we used to connect to that website.

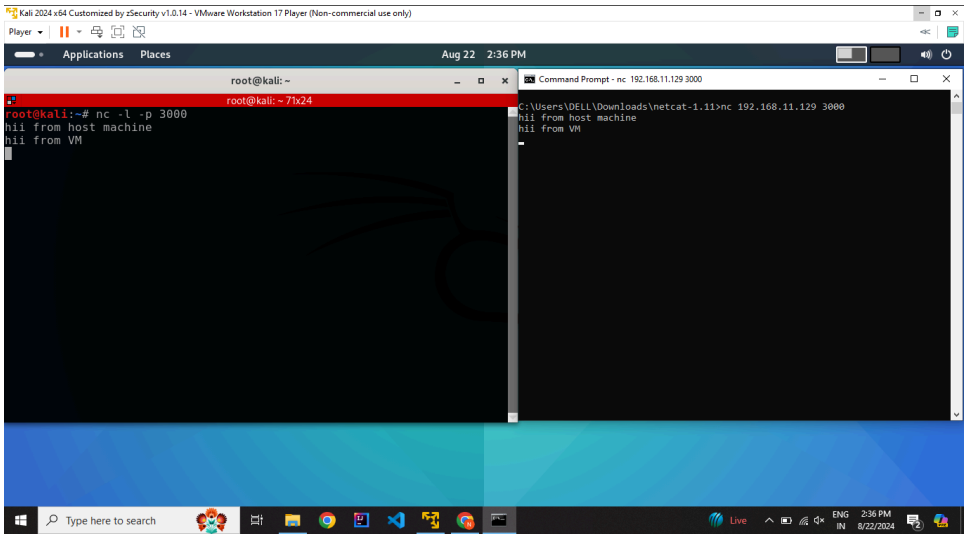
2) To change the IP address of the network interface (in my case eth0) we use the command ifconfig.
Fist we deactivate the interface using ifconfig eth0 down. Then we set a new IP address using the ifconfig command only while passing the network interface with it along with the IP we want to set and after that we activate our network interface using ifconfig eth0 up.
Below is the screenshot for the same.



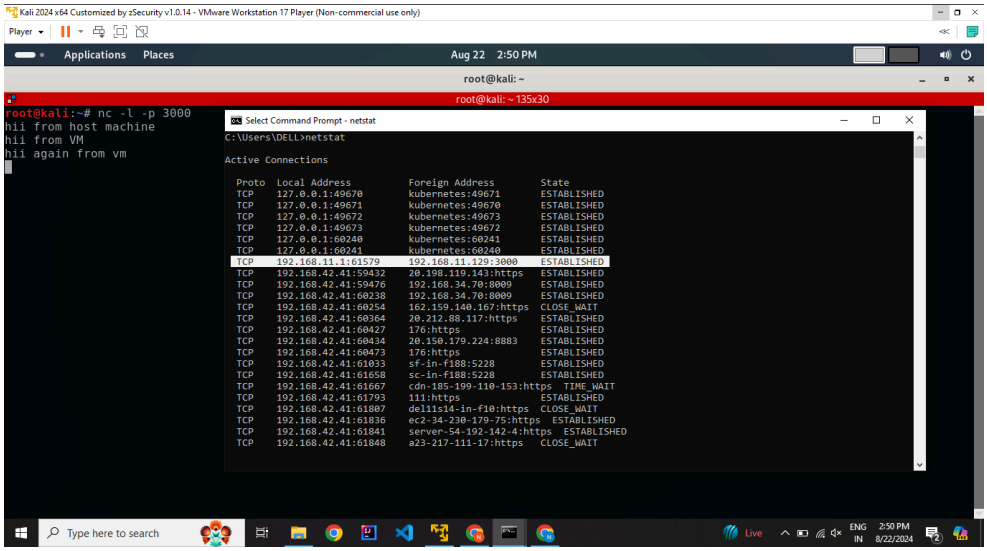

Now for going back to the original address we follow the same steps or we can also Just restart the machine, this will make the IP address resets to the original one.
Below is the screenshot for the same where i undo the steps done above.



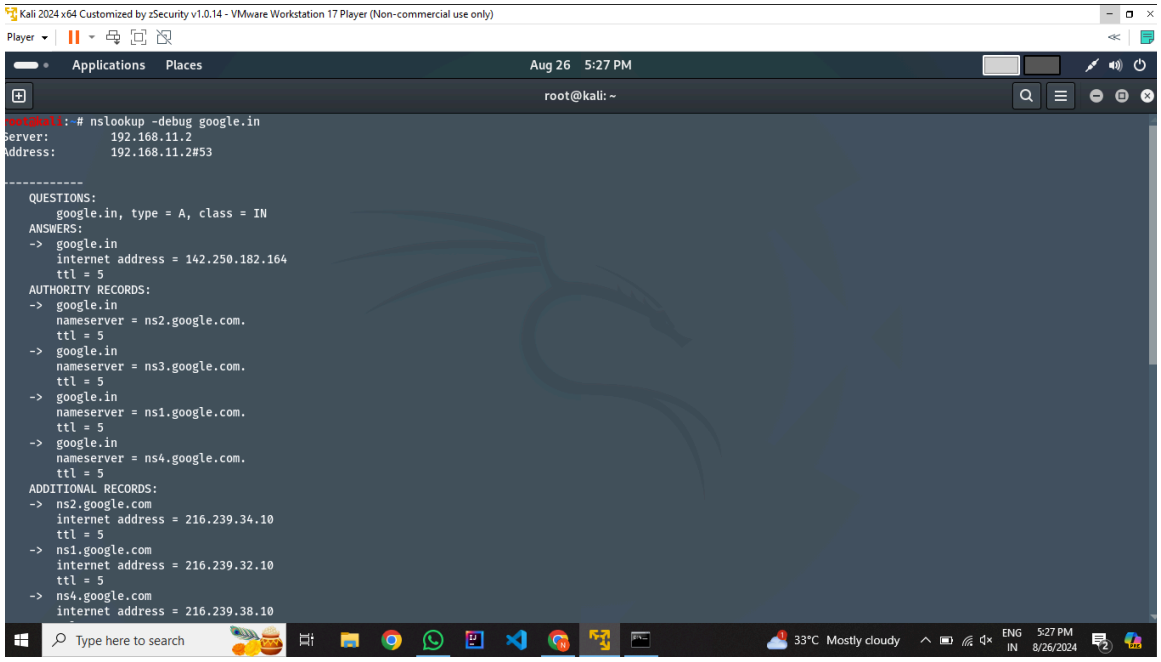
3) a) Using netcat we can set up a TCP client/server connection using the nc command with -l and -p flags for listen and for port number, this command will set up a server and now to connect to this server we can use nc in the windows with nc command with IP address of the host network with port number as well.
To use netcat on my Windows I downloaded it from the internet and used nc.exe.
I used port 3000 for setting up the server.
Server was my VM and client was host windows machine.
Below is the screenshot for the same where I sent some messages from the VM to my windows host machine.

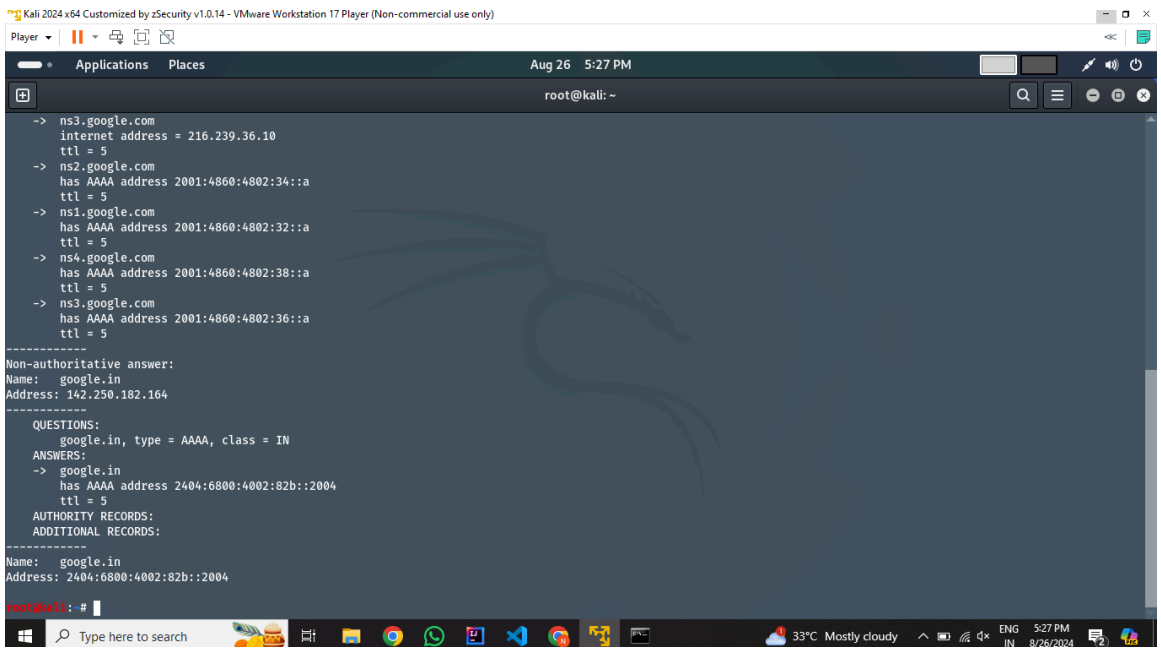



b) The state of this TCP connection was “ESTABLISHED” at the client side.
Below is the screenshot for the same where the highlighted one represents our TCP connection between VM and the host on port 3000.

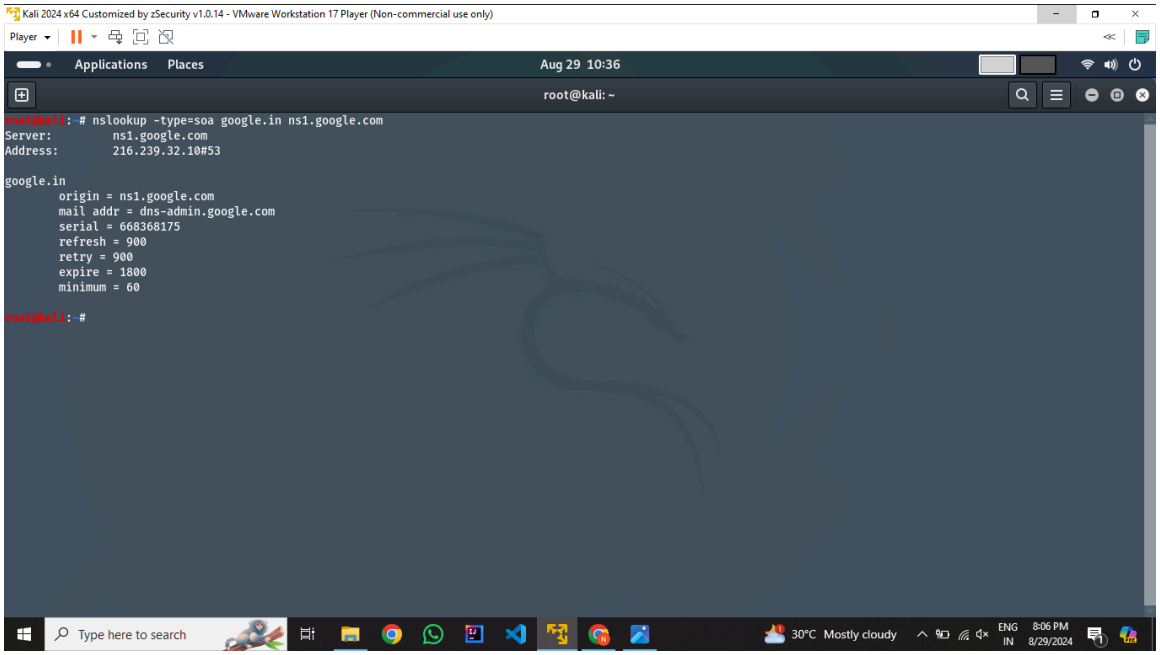


4) a) By running the command “nslookup google.in” in the terminal, we only get the non-authoritative answer. Now to get an authoritative report, we need to get the name of the named server for the same.
Hence first we have to get the name of the server which is the authoritative name server for the domain, and hence, we run the command “nslookup -debug google.in”.
Passing the flag -debug makes the output of the command more verbose and it gives more information including the name of the authoritative server. Below is the screenshot for the same:-

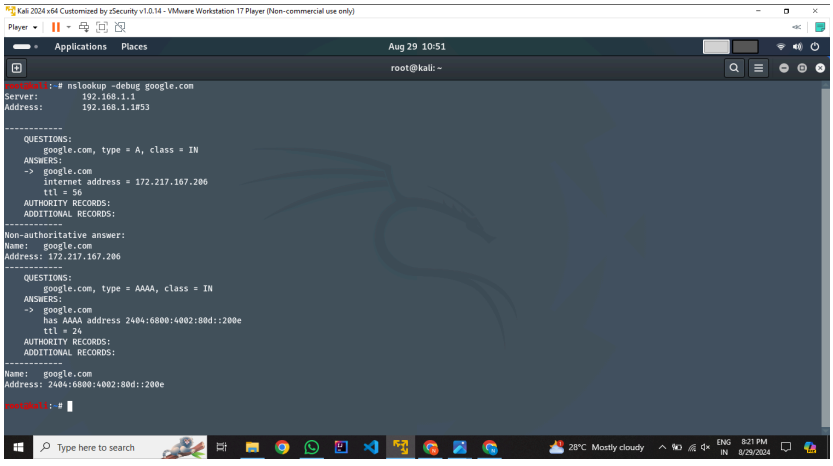


After getting the name of the authoritative answer, we can easily get the authoritative answer from the server using the nslookup command and by passing a flag “-type= soa” with the nslookup command. “soa” means the Start of Authority record of a domain. Below is the screenshot for the same.
The SOA record provides information about the authoritative DNS server for the domain and contains important details, including Primary nameserver, serial number, refresh rate, retry interval, expire limit, min ttl.

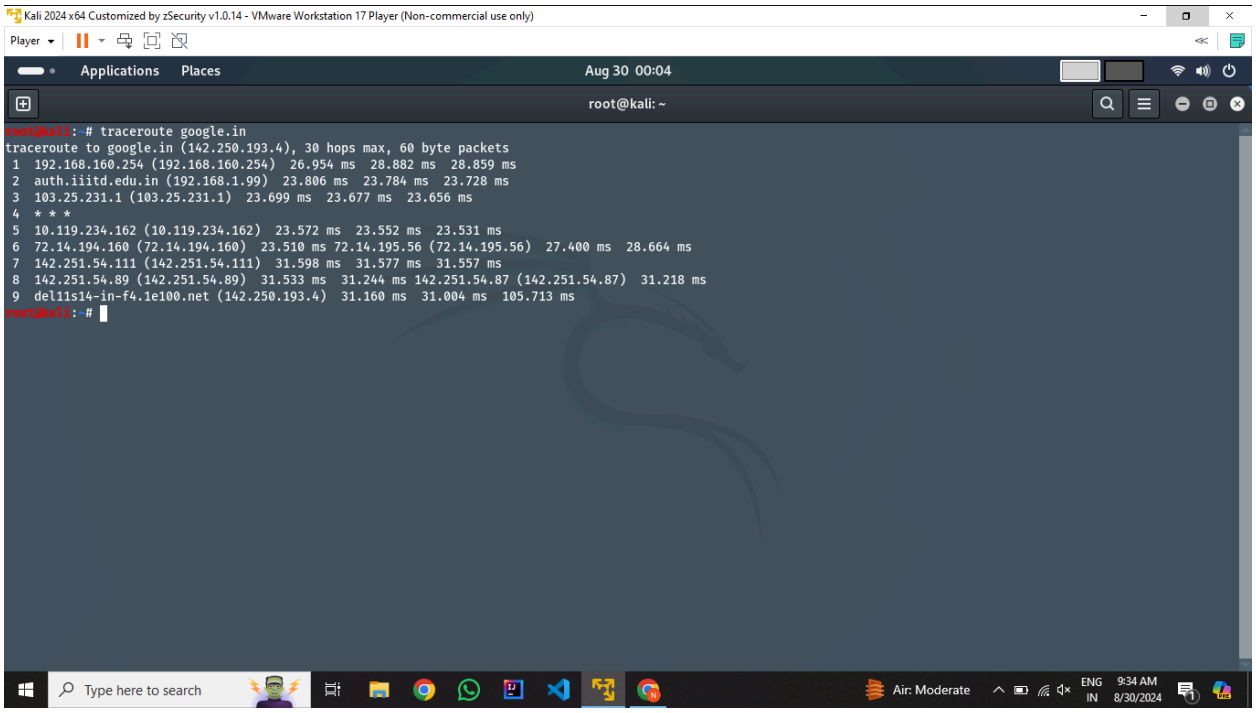



b) To find out the time to live for any website in the local DNS we can run the command: nslookup -debug <website_name>.
The flag “-debug” provides more verbose output and below is the screenshot for the same where I ran this command for google.com. The result had 2 sections one for the A record (Address record) and one for the AAAA (same as A, but for IPv6 address).
The time for the IPv4 address to live in the local DNS was: 56 seconds and for the IPv6 it was 24 seconds.

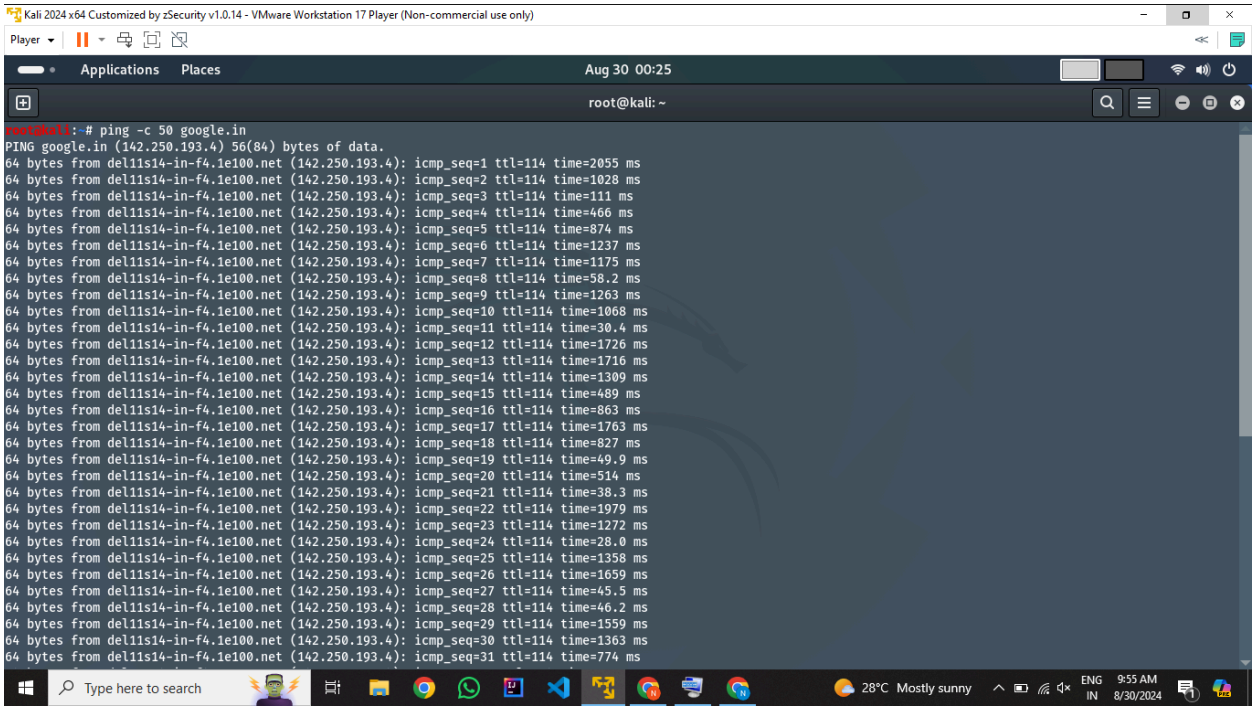


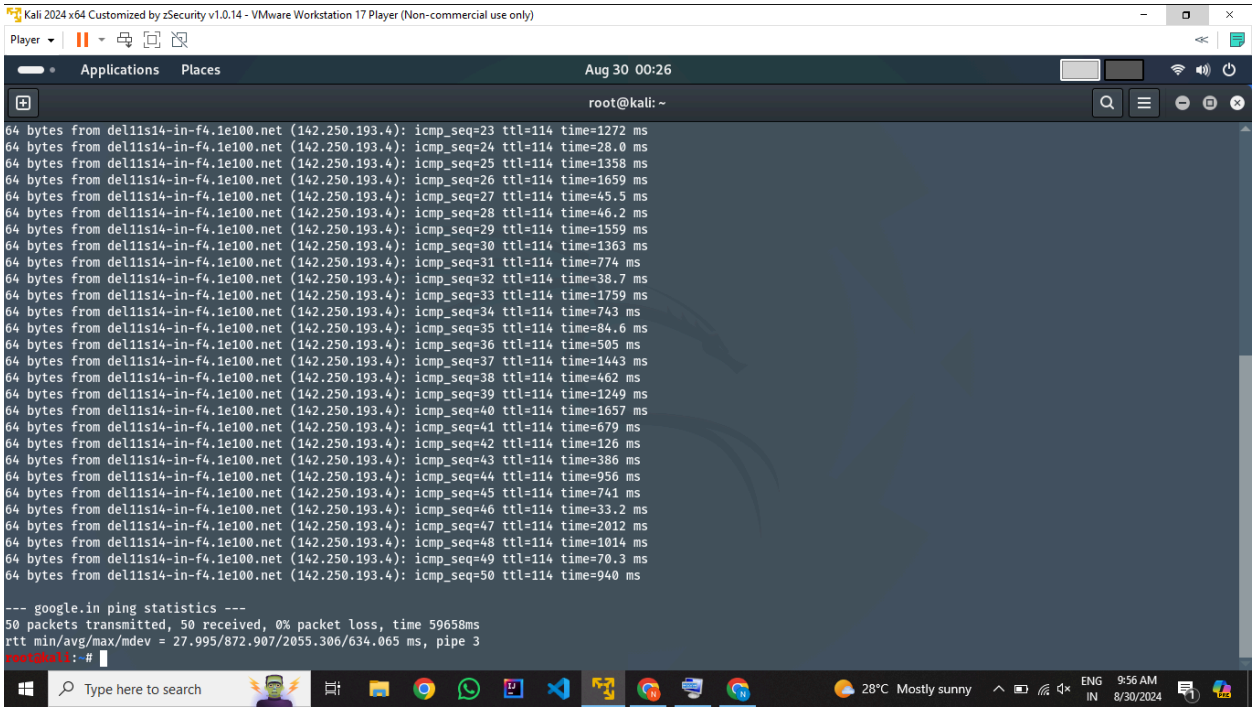
**For running the traceroute command I used an external wifi-adaptor, so there might be some differences in case of latency and the time taken.**

5) a) On running the command traceroute google.in there were in total 9 hosts, but one was marked as “*”, so excluding it makes 8 hosts in total. Following are their IP addresses and avg latency.
    1. 192.168.160.254  (26.954+28.882+28.859)/3 ms = 28.231667 ms
    2. 192.168.1.99 (23.806+23.784+23.728)/3 ms = 23.772667 ms
    3. 103.25.231.1 (23.669+23.677+23.656)/3 ms = 23.667333 ms
    4. 10.119.234.162 (23.572+23.552+23.531)/3 ms = 23.551667 ms
    5. 72.14.194.160 (23.510+27.400+28.664)/3 ms = 26.524667 ms (There were more than one IP for this router at this hop.)
    6. 142.251.54.111 (31.598+31.577+31.577)/3 ms = 31.577733 ms
    7. 142.251.54.89 (31.533+31.244+31.218)/3 ms = 31.331667 ms (There were more than one IP for this router at this hop.)
    8. 142.250.193.4 (31.160+31.004+105.713)/3 ms = 55.959 ms




b) Following is the avg latency for ping google.in with 50 packets
We use the command: ping -c 50 google.in
The avg latency was the sum of the time column (in output) of each ping/50 and it was 872.907 ms.


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications Places
Aug 30 00:25
root@kali: ~
root@kali:~# ping -c 50 google.in
PING google.in (142.250.193.4) 56(84) bytes of data.
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=1 ttl=114 time=2055 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=2 ttl=114 time=1028 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=3 ttl=114 time=111 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=4 ttl=114 time=466 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=5 ttl=114 time=874 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=6 ttl=114 time=1237 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=7 ttl=114 time=1175 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=8 ttl=114 time=58.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=9 ttl=114 time=1263 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=10 ttl=114 time=1068 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=11 ttl=114 time=30.4 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=12 ttl=114 time=1726 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=13 ttl=114 time=1716 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=14 ttl=114 time=1309 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=15 ttl=114 time=489 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=16 ttl=114 time=863 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=17 ttl=114 time=1763 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=18 ttl=114 time=827 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=19 ttl=114 time=49.9 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=20 ttl=114 time=514 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=21 ttl=114 time=38.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=22 ttl=114 time=1979 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=23 ttl=114 time=1272 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=24 ttl=114 time=28.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=25 ttl=114 time=1358 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=26 ttl=114 time=1659 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=27 ttl=114 time=45.5 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=28 ttl=114 time=46.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=29 ttl=114 time=1559 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=30 ttl=114 time=1363 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=31 ttl=114 time=774 ms
Type here to search
28°C Mostly sunny
ENG IN
9:55 AM 8/30/2024

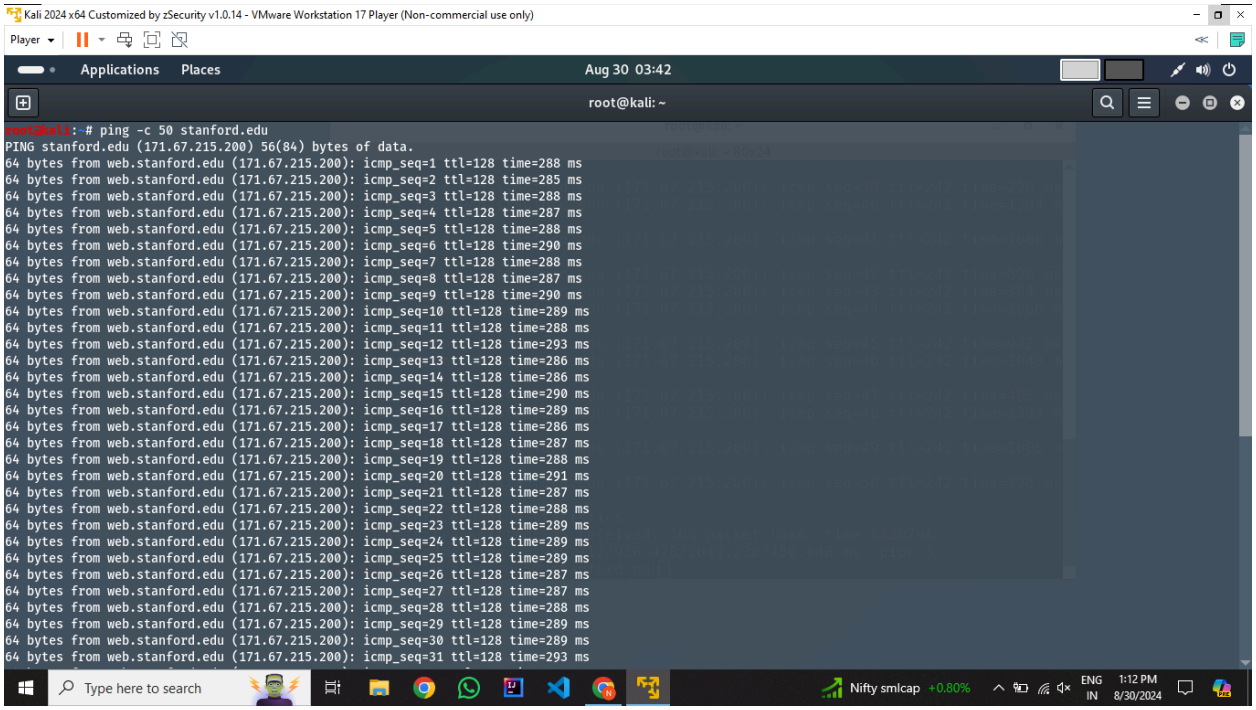

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications Places
Aug 30 00:26
root@kali: ~
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=23 ttl=114 time=1272 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=24 ttl=114 time=28.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=25 ttl=114 time=1358 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=26 ttl=114 time=1659 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=27 ttl=114 time=45.5 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=28 ttl=114 time=46.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=29 ttl=114 time=1559 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=30 ttl=114 time=1363 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=31 ttl=114 time=774 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=32 ttl=114 time=38.7 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=33 ttl=114 time=1759 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=34 ttl=114 time=743 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=35 ttl=114 time=84.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=36 ttl=114 time=505 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=37 ttl=114 time=1443 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=38 ttl=114 time=462 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=39 ttl=114 time=1249 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=40 ttl=114 time=1657 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=41 ttl=114 time=679 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=42 ttl=114 time=126 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=43 ttl=114 time=386 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=44 ttl=114 time=956 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=45 ttl=114 time=741 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=46 ttl=114 time=33.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=47 ttl=114 time=2012 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=48 ttl=114 time=1014 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=49 ttl=114 time=70.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=50 ttl=114 time=940 ms
--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 59658ms
rtt min/avg/max/mdev = 27.995/872.907/2055.306/634.065 ms, pipe 3
root@kali:~#
Type here to search
28°C Mostly sunny
ENG IN
9:56 AM 8/30/2024

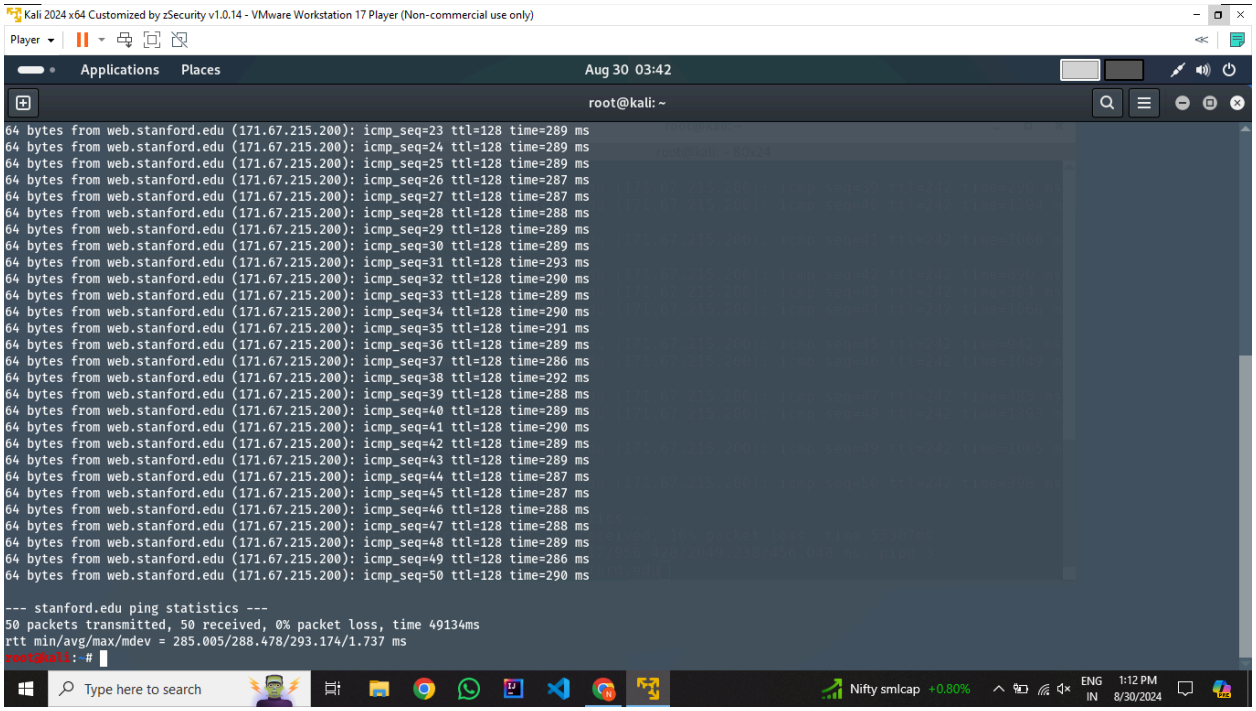
c)  Adding up the latency of the (a) gives us following (28.231667+23.772667+23.667333+23.551667+26.524667+31.577733+31.331667+55.959) = 244.616401 ms.
And the ping avg latency was: 872.907 ms
These values are not matching and the reason for this is that the latency shown for each hop in traceroute is only the time it takes for the packet to travel from our machine to that specific hop. The latency at each hop is not cumulative but it's the time for that segment of the journey, whereas for ping it is the total round trip time including the time taken to reach destination and reaching back to the client machine. The data packet travels across the network in one continuous flow, which takes round trip time and it is the time taken for the entire journey.
Other reasons could be network congestion, paths being different in case of traceroute and ping.

d) The maximum latency for an intermediate host in (a) is 105.713 ms and the maximum ping latency was 2055.306 ms. These values are very different and these are expected to be different as well, as also stated in (c) that the traceroute measures the the time taken to reach that intermediate host whereas ping measures the overall latency for a trip from source to destination and then back to source as well. Hence this clearly explains the reason for the same.

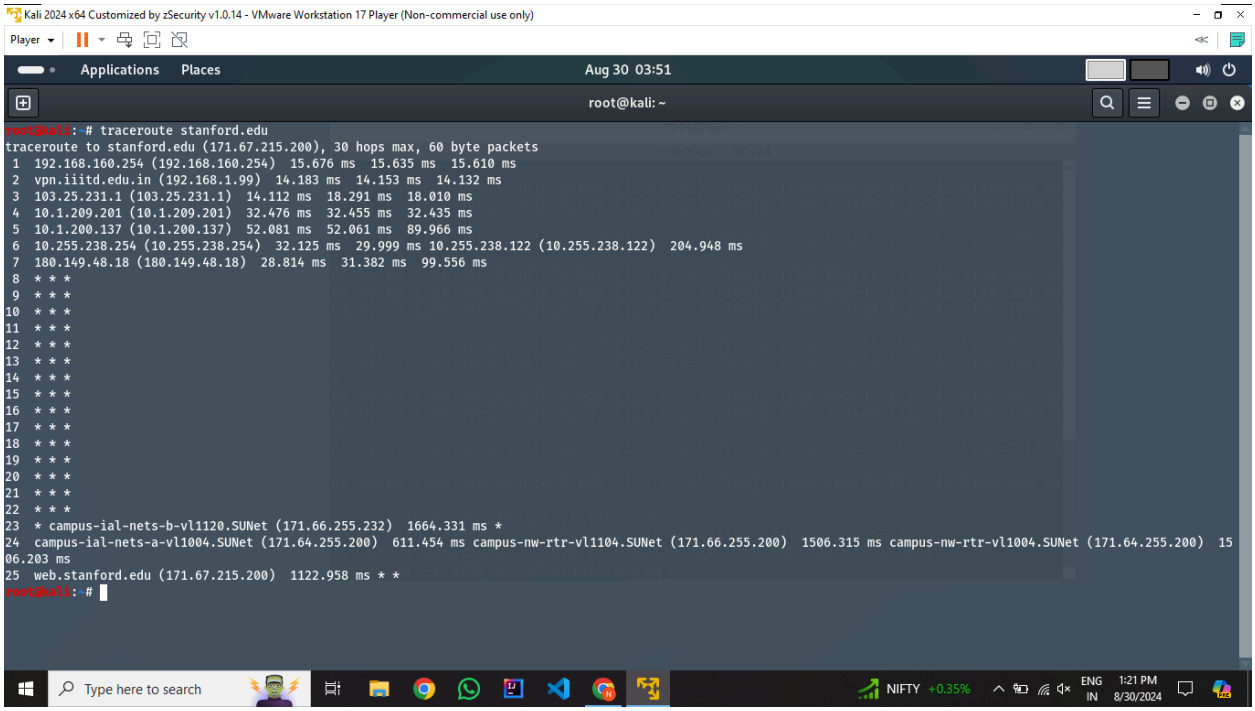
e) There can be many entries for a single hop while using traceroute, this is because there can be multiple paths or interfaces involved in forwarding the packet at that hop, this is usually done to balance the load of the network and routers may use different interfaces to respond to packets.

f) The avg latency was: 288.478 ms
Command used: ping -c 50 stanford.edu


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications Places
Aug 30 03:42
root@kali: ~
root@kali:~# ping -c 50 stanford.edu
PING stanford.edu (171.67.215.200) 56(84) bytes of data.
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=1 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=2 ttl=128 time=285 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=3 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=4 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=5 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=6 ttl=128 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=7 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=8 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=9 ttl=128 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=10 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=11 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=12 ttl=128 time=293 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=13 ttl=128 time=286 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=14 ttl=128 time=286 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=15 ttl=128 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=16 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=17 ttl=128 time=286 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=18 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=19 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=20 ttl=128 time=291 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=21 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=22 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=23 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=24 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=25 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=26 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=27 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=28 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=29 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=30 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=31 ttl=128 time=293 ms
Type here to search
Nifty smlcap +0.80%
ENG IN
1:12 PM 8/30/2024


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications Places
Aug 30 03:42
root@kali: ~
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=23 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=24 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=25 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=26 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=27 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=28 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=29 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=30 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=31 ttl=128 time=293 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=32 ttl=128 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=33 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=34 ttl=128 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=35 ttl=128 time=291 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=36 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=37 ttl=128 time=286 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=38 ttl=128 time=292 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=39 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=40 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=41 ttl=128 time=290 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=42 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=43 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=128 time=287 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=128 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=128 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=128 time=286 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=128 time=290 ms
--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49134ms
rtt min/avg/max/mdev = 285.005/288.478/293.174/1.737 ms
root@kali:~#
Type here to search
Nifty smlcap +0.80%
ENG IN
1:12 PM 8/30/2024

g) Following is the output for the traceroute stanford.edu




The number of hops in case of google.in was 8, excluding a hop marked as “*”.
The number of hops in case of stanford.edu was 10, excluding 15 hops marked as “*”.
So overall we can say that google.in had fewer hops as compared to stanford.edu.

h) There can mainly be 3 reasons for this. This includes following:-

1) Geographical location of google.in and stanford.edu servers. The server for google.in is likely to be hosted within India or nearby whereas stanford.edu is hosted in US, thus data has to travel farther in case of stanford.edu and hence takes more time.
2) Hops occurred: There are a lot of hops in case of stanford.edu as compared to google.in, hence the data has to travel over a complex route and hence has more latency.
3) Load balancing: Google has a very vast network of routers and servers with many data centres for optimizing the network path which can balance the load optimally and hence has lower latency as compared to stanford.edu.

6) To fail the ping command for the localhost which is: 127.0.0.1 we can simply make our lo (loopback interface) which is the local host, down by using ifconfig lo down. This will deactivate the localhost i.e- lo down and hence the ping command will fail with 100% packet loss and the reason for failing is that lo is deactivated hence it is not able to communicate with that which caused a failure of 100% packet loss.
Below is the screenshot for the same.
Commands used:-
ifconfig lo down
ping 127.0.0.1