Part 2

Working of Traceroute

Traceroute is a network diagnostic tool which helps us to visualize the path of the packets from source to destination.

-> I used the command ”tracert nasa.gov”. By this command tracerote is sending a series of special data packets to the destination(in this case it is nasa.gov).

-> These packets have a TTL(Time to Live) value. TTL tells each router/hop how long the packet should live. When TTL reaches to 0, the router discards the packet and sends back an acknowledgement to the source.

-> Traceroute records the time it takes to get acknowledgement back from each hop/router.

Using Wireshark to Observe Traceroute

-> Opened wireshark in windows by searching it in the search.

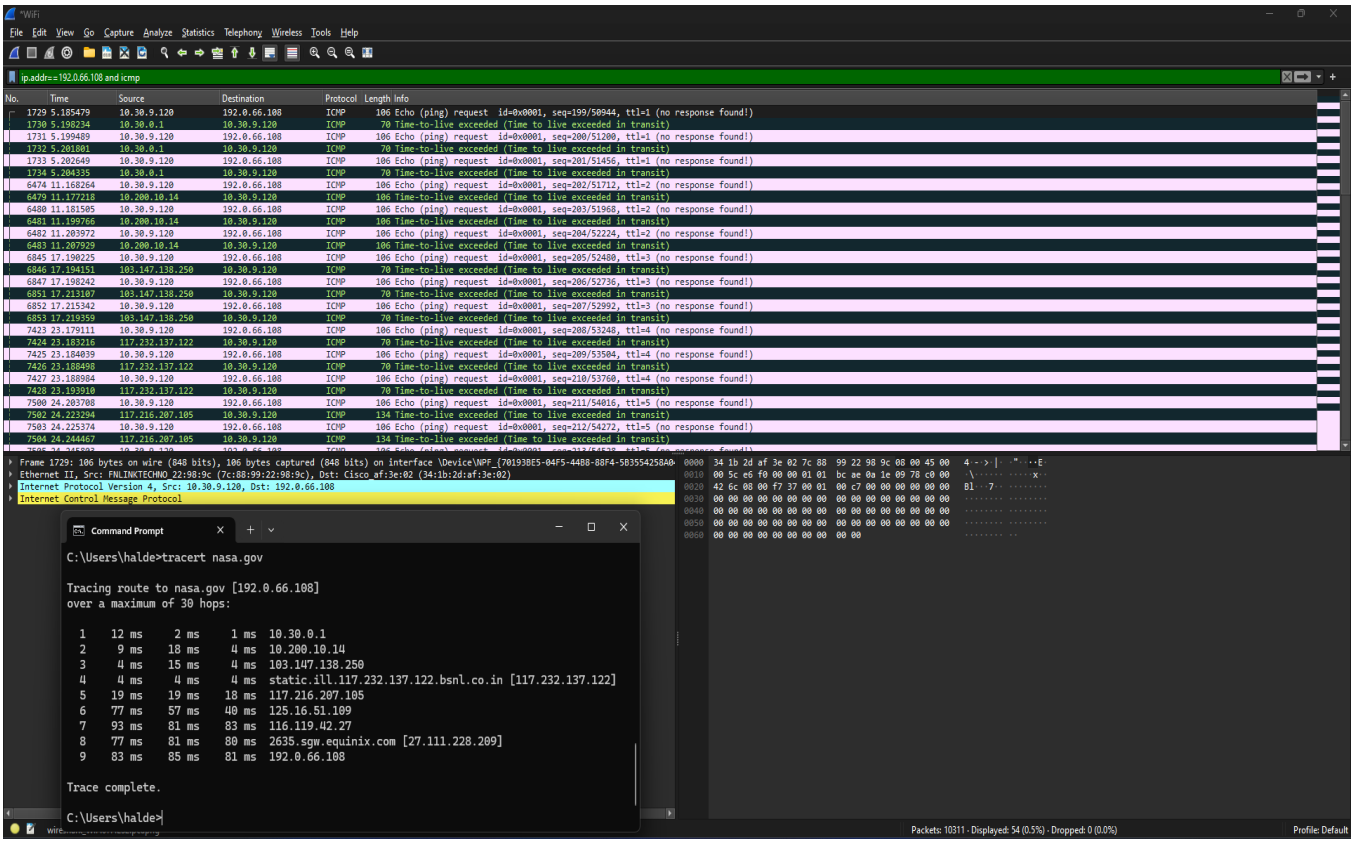
-> Selected wifi for interface.

-> Pressed “Start Capturing Packets” button.

-> In cmd run the command “tracert nasa.gov”

-> Now in the filter of Wireshark use this filter “ip.addr==192.0.66.108 and icmp” where 192.0.66.108 is the destination address(nasa.gov) and ICMP packets because these are the messages sent back by routers as traceroute progresses.

I also attached one screenshot in the next page which contains the output of traceroute and the Wireshark.


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==192.0.66.108 and icmp
No. Time Source Destination Protocol Length Info
1729 5.185479 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=199/50944, ttl=1 (no response found!)
1730 5.198234 10.30.0.1 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
1731 5.199489 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=200/51200, ttl=1 (no response found!)
1732 5.201801 10.30.0.1 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
1733 5.202649 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=201/51456, ttl=1 (no response found!)
1734 5.204335 10.30.0.1 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
6474 11.168264 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=202/51712, ttl=2 (no response found!)
6479 11.177218 10.200.10.14 10.30.9.120 ICMP 106 Time-to-live exceeded (Time to live exceeded in transit)
6480 11.181505 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=203/51968, ttl=2 (no response found!)
6481 11.199766 10.200.10.14 10.30.9.120 ICMP 106 Time-to-live exceeded (Time to live exceeded in transit)
6482 11.203972 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=204/52224, ttl=2 (no response found!)
6483 11.207929 10.200.10.14 10.30.9.120 ICMP 106 Time-to-live exceeded (Time to live exceeded in transit)
6845 17.190225 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=205/52480, ttl=3 (no response found!)
6846 17.194151 103.147.138.250 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
6847 17.198242 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=206/52736, ttl=3 (no response found!)
6851 17.213107 103.147.138.250 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
6852 17.215342 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=207/52992, ttl=3 (no response found!)
6853 17.219359 103.147.138.250 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
7423 23.179111 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=208/53248, ttl=4 (no response found!)
7424 23.183216 117.232.137.122 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
7425 23.184039 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=209/53504, ttl=4 (no response found!)
7426 23.188498 117.232.137.122 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
7427 23.188984 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=210/53760, ttl=4 (no response found!)
7428 23.193910 117.232.137.122 10.30.9.120 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
7500 24.203708 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=211/54016, ttl=5 (no response found!)
7502 24.223294 117.216.207.105 10.30.9.120 ICMP 134 Time-to-live exceeded (Time to live exceeded in transit)
7503 24.225374 10.30.9.120 192.0.66.108 ICMP 106 Echo (ping) request id=0x0001, seq=212/54272, ttl=5 (no response found!)
7504 24.244467 117.216.207.105 10.30.9.120 ICMP 134 Time-to-live exceeded (Time to live exceeded in transit)
Frame 1729: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{70193BE5-04F5-44B8-88F4-5B3554258A0
Ethernet II, Src: FNLINKTECHNO_22:98:9c (7c:88:99:22:98:9c), Dst: Cisco_af:3e:02 (34:1b:2d:af:3e:02)
Internet Protocol Version 4, Src: 10.30.9.120, Dst: 192.0.66.108
Internet Control Message Protocol
0000 34 1b 2d af 3e 02 7c 88 99 22 98 9c 08 00 45 00
0010 00 5c e6 f0 00 00 01 01 bc ae 0a 1e 09 78 c0 00
0020 42 6c 08 00 f7 37 00 01 00 c7 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00
Command Prompt
C:\Users\halde>tracert nasa.gov
Tracing route to nasa.gov [192.0.66.108]
over a maximum of 30 hops:
1 12 ms 2 ms 1 ms 10.30.0.1
2 9 ms 18 ms 4 ms 10.200.10.14
3 4 ms 15 ms 4 ms 103.147.138.250
4 4 ms 4 ms 4 ms static.ill.117.232.137.122.bsnl.co.in [117.232.137.122]
5 19 ms 19 ms 18 ms 117.216.207.105
6 77 ms 57 ms 40 ms 125.16.51.109
7 93 ms 81 ms 83 ms 116.119.42.27
8 77 ms 81 ms 80 ms 2635.sgw.equinix.com [27.111.228.209]
9 83 ms 85 ms 81 ms 192.0.66.108
Trace complete.
C:\Users\halde>
Packets: 10311 · Displayed: 54 (0.5%) · Dropped: 0 (0.0%)
Profile: Default