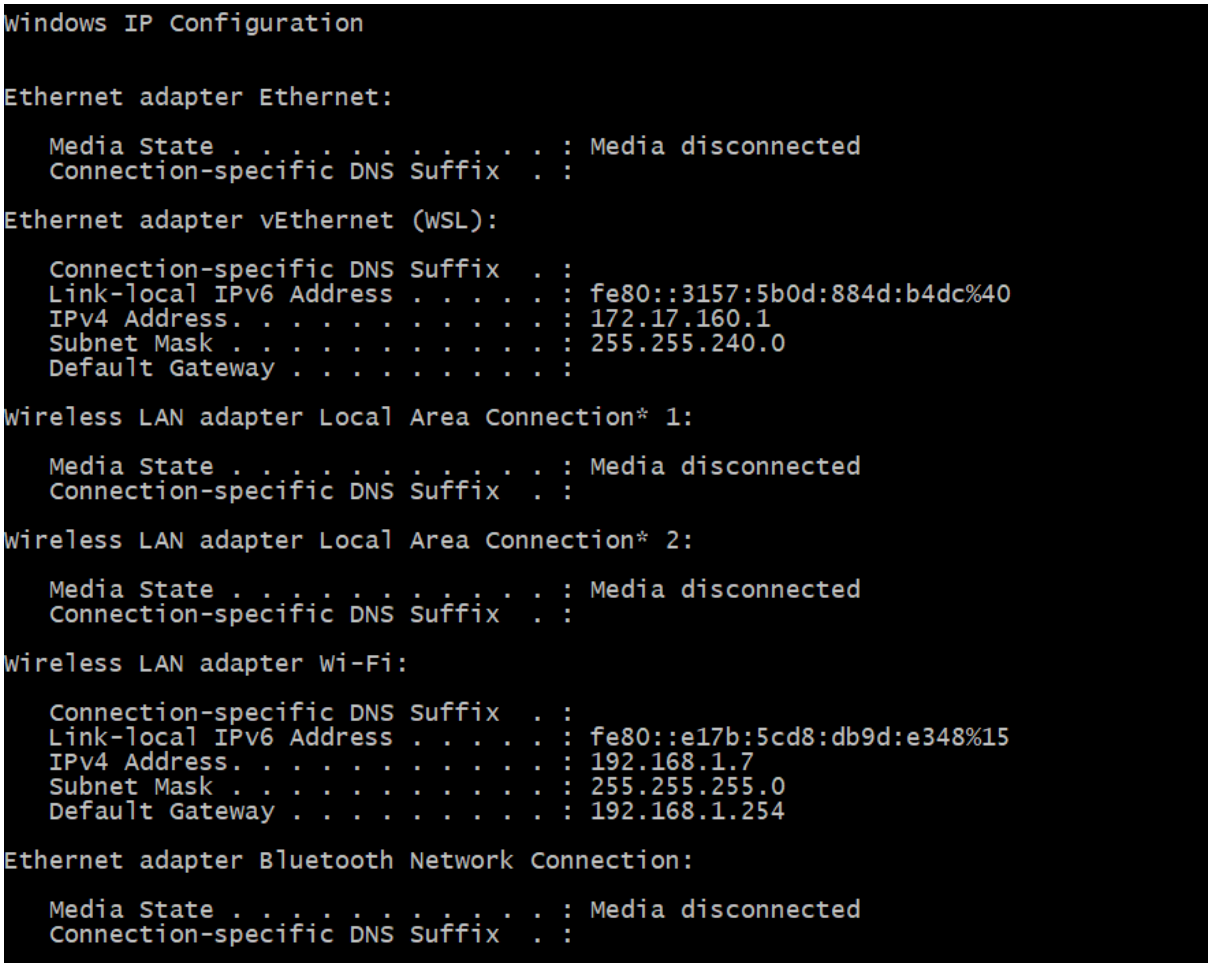
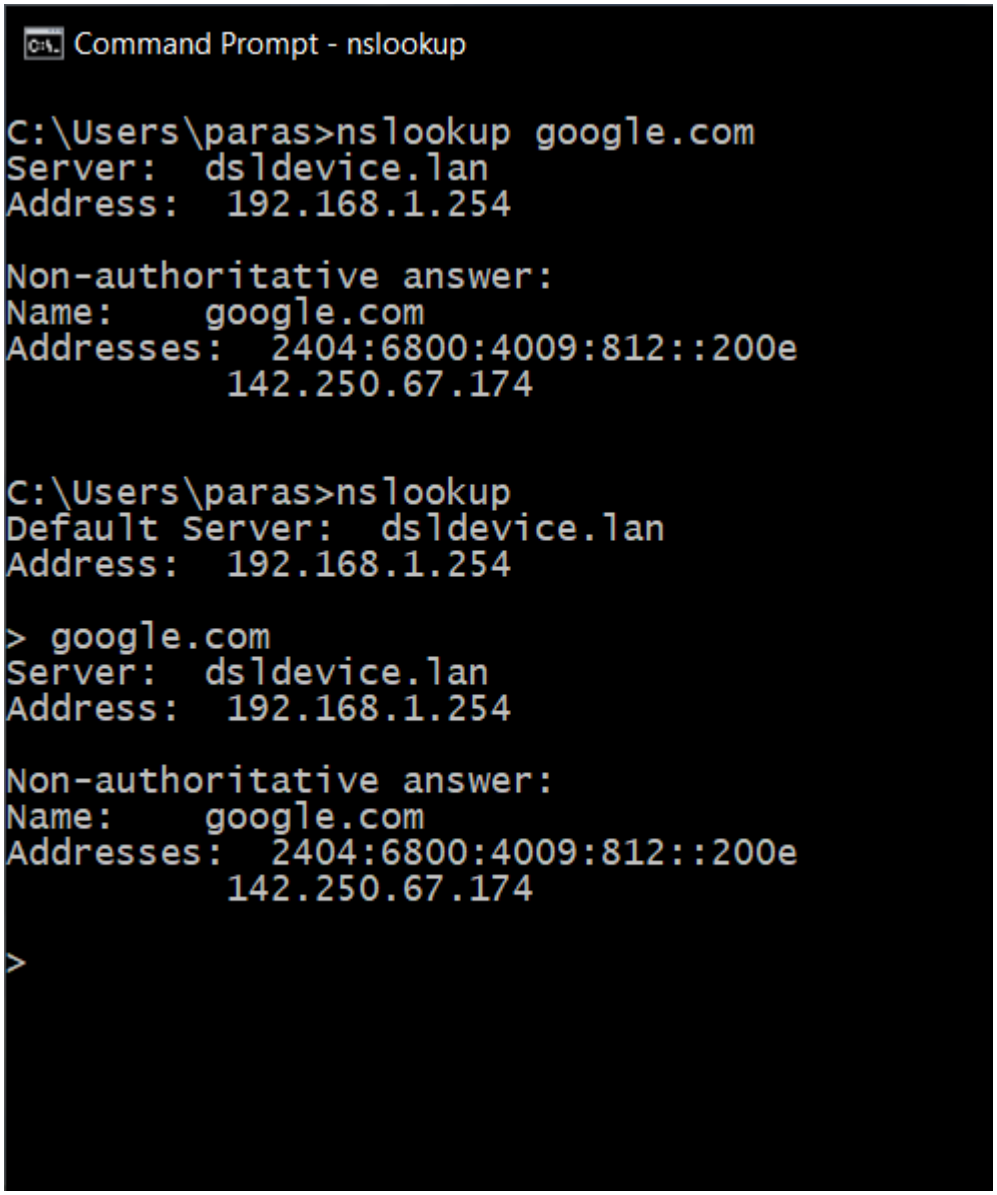
1) IPCONFIG: **IPCONFIG** stands for **Internet Protocol Configuration**. Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters. Default Gateway: ip address of nearest router or the router through which your pc is directly connected.

Subnet mask: It helps to identify either the node is at your local network or remote network.

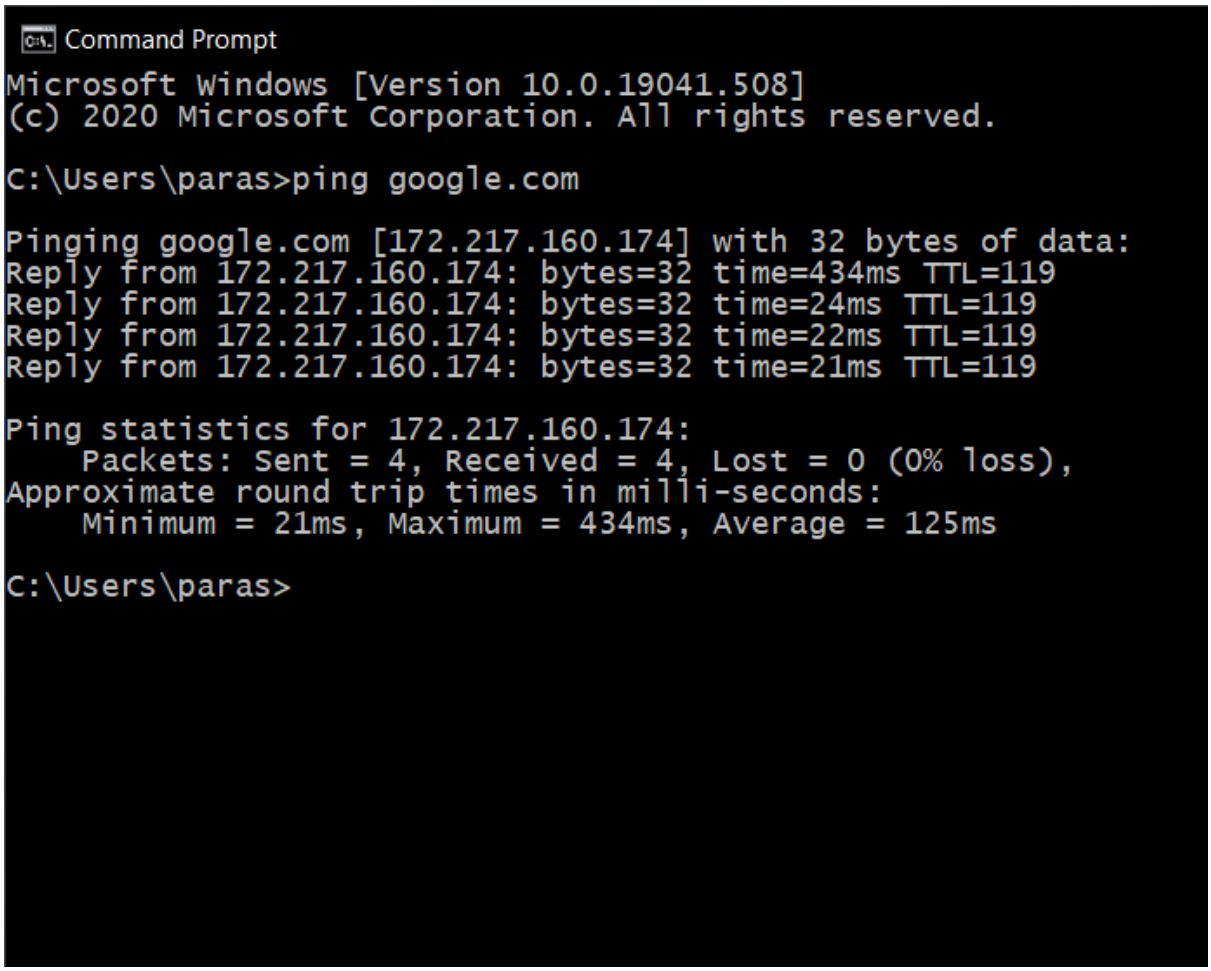


2) Nslookup (stands for “Name Server Lookup”) is used to get information from DNS(Domain Name Service) about any domain name or ip address from DNS records.



3) ping command is used to ensure that a computer can communicate to a specified device over the network. ping command sends Internet Control Message Protocol(ICMP) Echo Request messages in the form of packets to the destination computer and waits in order to get the response back. Once the packets are received by the destined computer, it starts sending the packets back.
ping command provides details such as

- number of packets transmitted
- number of packets received
- time taken by the packet to return



4) Tracert / traceroute:

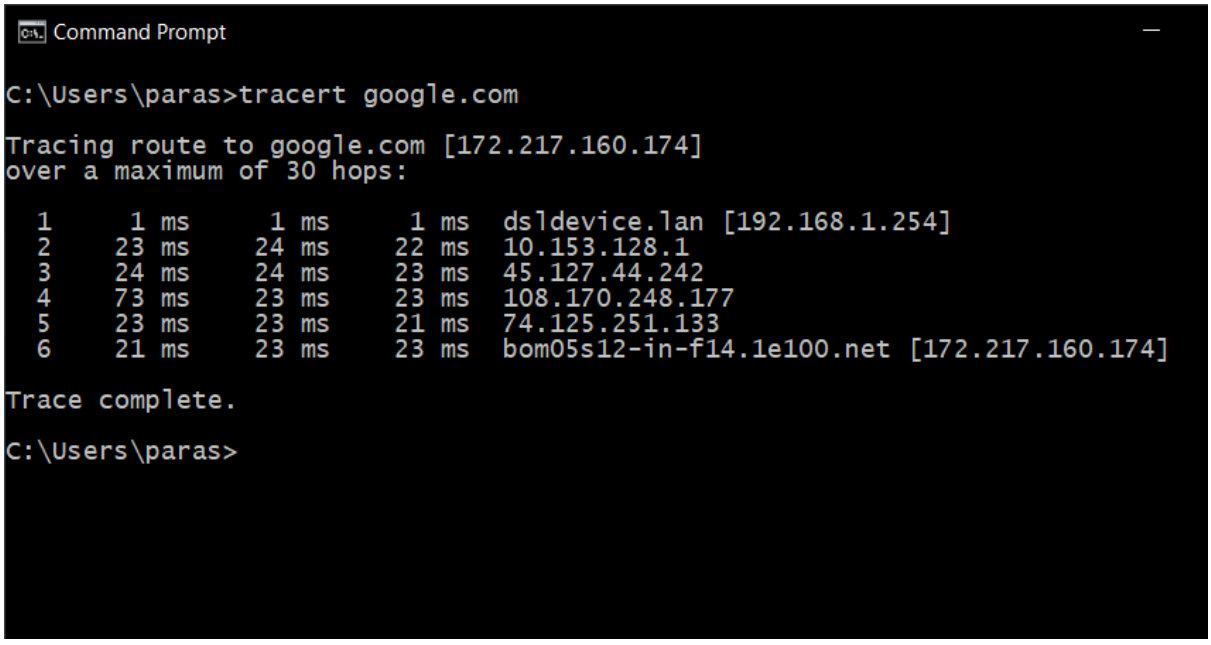
This command is used to get the route of a packet. In other words, traceroute command is used to determine the path along which a packet travels. It also returns the number of hops taken by the packet to reach the destination. This command prints to the console, a list of hosts through which the packet travels to the destination.

How to Use the TRACERT Utility

The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

TRACERT sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum TTL is reached. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. Note however that some routers silently drop packets that have expired TTLs, and these packets are invisible to TRACERT.

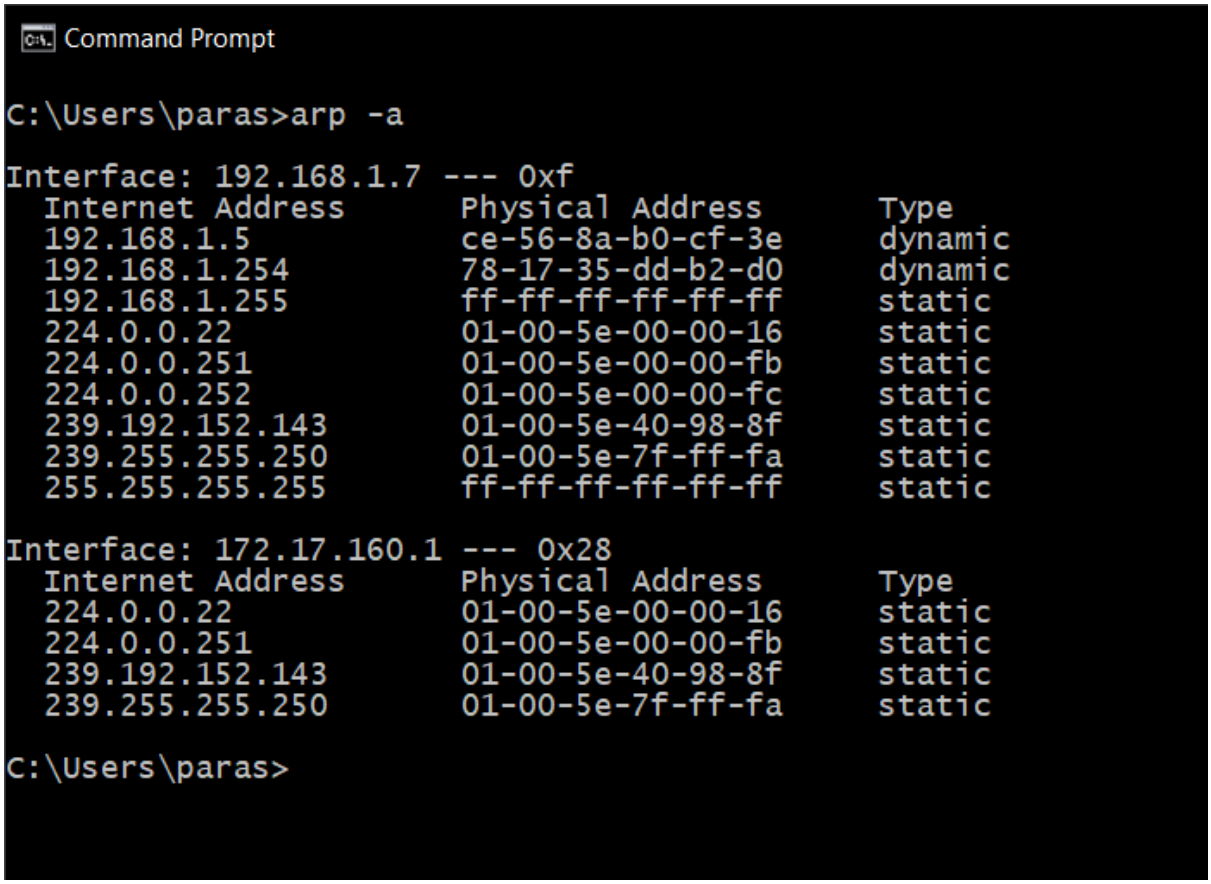
TRACERT prints out an ordered list of the intermediate routers that return ICMP "Time Exceeded" messages. Using the -d option with the tracert command instructs TRACERT not to perform a DNS lookup on each IP address, so that TRACERT reports the IP address of the near-side interface of the routers. 3 packets are sent.



5) ARP: Displays and modifies entries in the Address Resolution Protocol (ARP) cache. The ARP cache contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer. Used without parameters, **arp** displays help information.

ARP -a

Displays current arp cache tables for all interfaces.

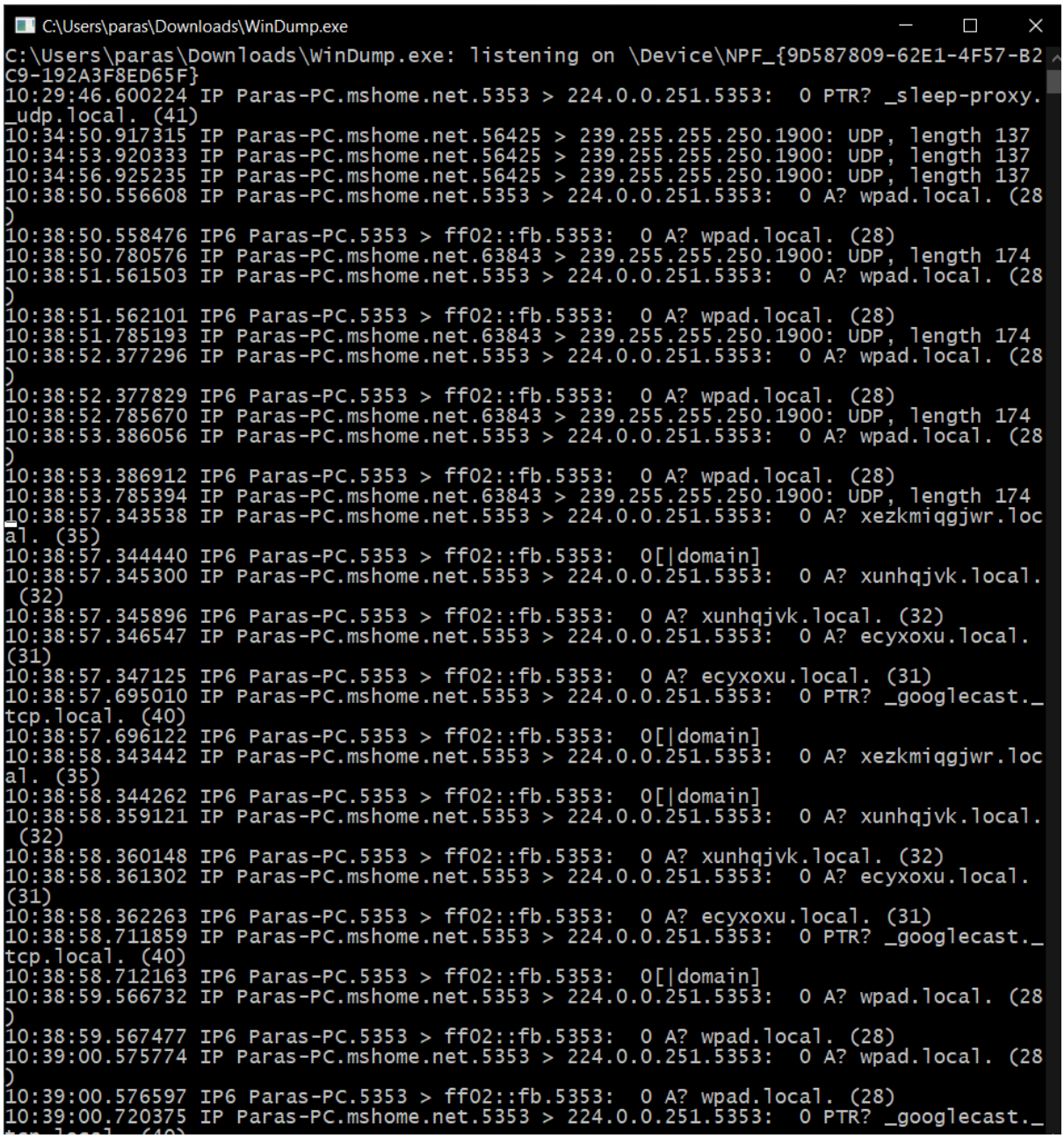


6)Rarp: Reverse Address Resolution Protocol. This is obsolete so it does not work on windows. Reverse mapping. Physical to ip address.

7) Hostname: Prints the name of current host. Basically your device name.

8) Whois: We needed to download whois.exe file to run this command. It is a query and response protocol that is used to find out details about any registered user or internet resource such as domain name, ip address and other info.

9) TCPdump/Windump: Windump is windows version of Tcpdump. We need to download winpcap and windump. Tcp dump is a packet analysing tool to troubleshoot connectivity issue in linux. It is used to capture, filter and analyse network traffic such as TCP/IP packets going through your system. It captures logs in the form of pcap file which can be opened through a tool called wireshark.



Netstat: Current listed connections. Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.