**Exp: no: 1**

**Aim:**

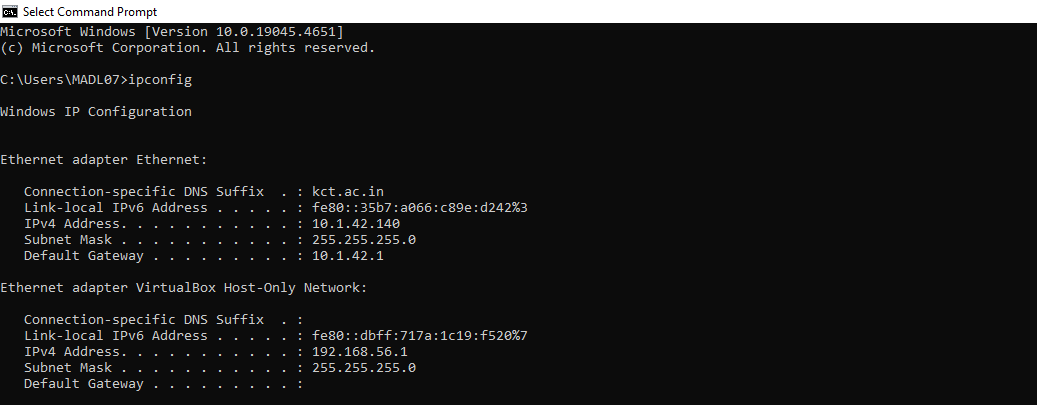
To demonstrate the working of network tools such as Ping, TCP Dump, Traceroute, Netstat and write the syntax, execute and place the screenshot for all the commands worked on.

1. Demonstrate the different *ipconfig* commands used to explore a system’s IP address.

*Sol:*

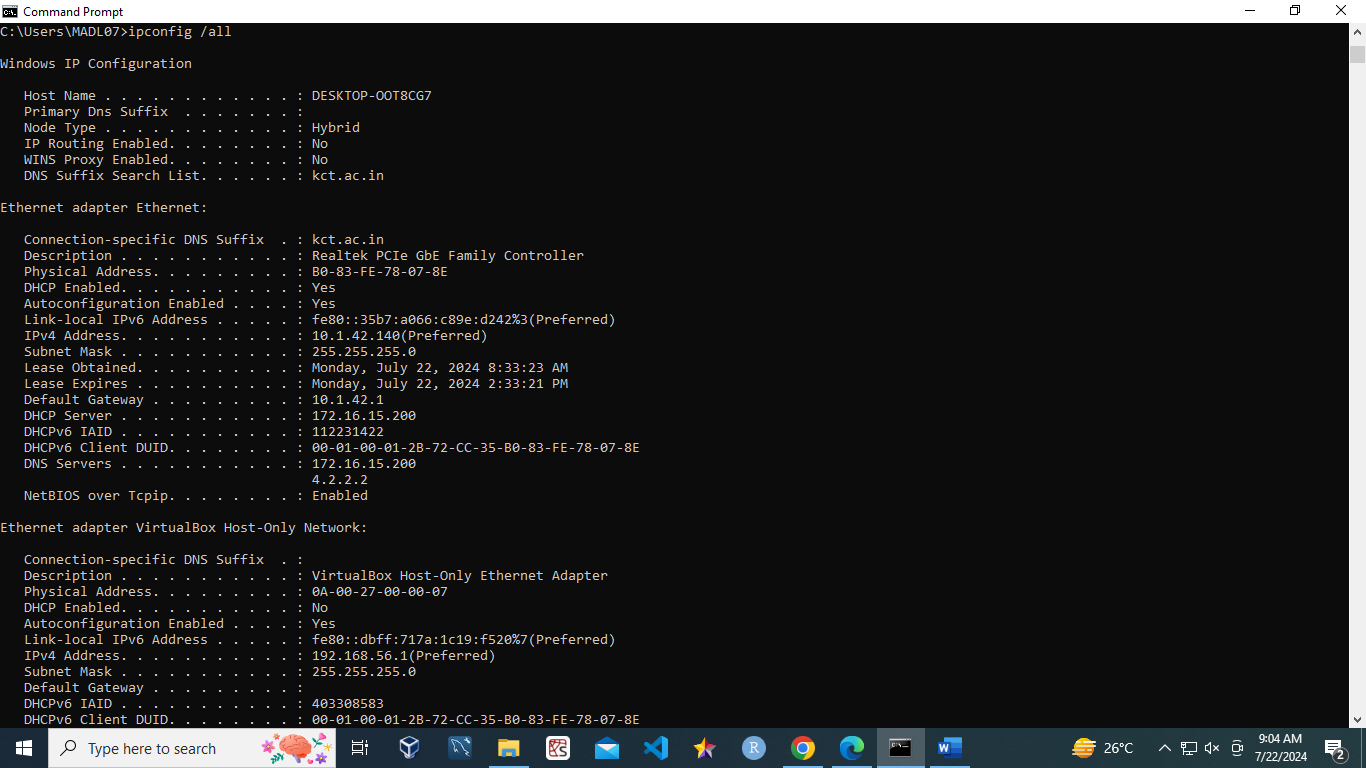
* **ipconfig**

ipconfig is a command-line utility in Windows that displays the current TCP/IP network configuration values for the computer. It is primarily used for troubleshooting network issues and managing network connections.



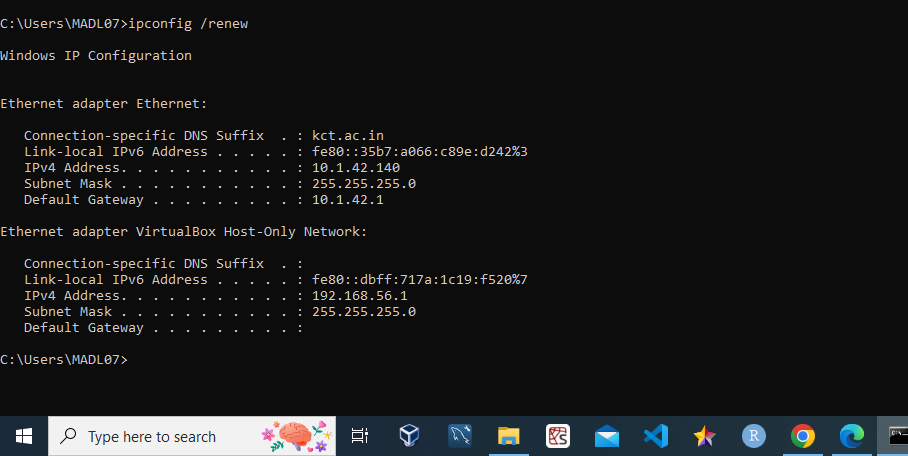
* **ipconfig /all**

**Description**: This command provides a detailed view of all network interfaces on the system, including physical (MAC) addresses, IP addresses, subnet masks, default gateways, DNS servers, and more.



* **ipconfig /renew**

The ipconfig /renew command requests a new IP address from a DHCP server for the specified network adapter in Windows.



1. To write the use of *ping* command and show the any 5 variants of the command.

**Ping Command**

The ping command is a fundamental network utility used to test connectivity between devices, measure round-trip time, diagnose network issues, perform name resolution testing, and monitor connection stability. The ping command is an essential tool for network diagnostics, providing valuable insights into the health and performance of network connections.

1. ping -t 10.1.42.140

* **Description**: Sends continuous ping requests to the specified host until interrupted (usually by pressing Ctrl + C).
* **Use Case**: Helpful for monitoring the stability of a connection over time or diagnosing intermittent connectivity issues.

A screenshot of a computer program

Description automatically generated

1. ping –a 10.1.42.140

* **Description**: Resolves the hostname of an IP address and displays it along with the ping results.
* **Use Case**: Useful for identifying the hostname of a given IP address, which can help in network diagnostics.

A computer screen with white text

Description automatically generated

1. ping -h

* **Description**: Displays help information for the ping command, including a list of available options and their descriptions.
* **Use Case**: Useful for quickly referencing the command syntax and available options.

A computer screen shot of a program

Description automatically generated

1. ping -l size 10.1.42.140

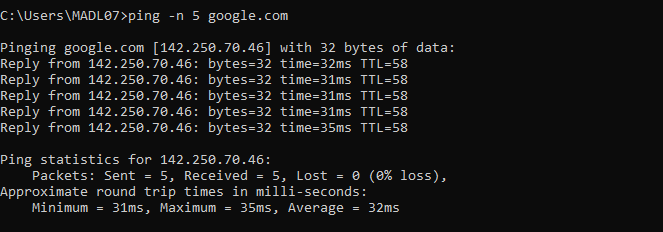
* **Description**: Specifies the size of the packet to be sent in bytes. The default size is typically 32 bytes.
* **Use Case**: Useful for testing how different packet sizes affect network performance and for diagnosing issues related to MTU (Maximum Transmission Unit) sizes.

A screen shot of a computer

Description automatically generated

1. ping -n 5 google.com

* **Description**: Sends a specified number of ping requests to the target host instead of the default continuous pings.
* **Use Case**: Useful for conducting a limited test to measure response times without overwhelming the network.



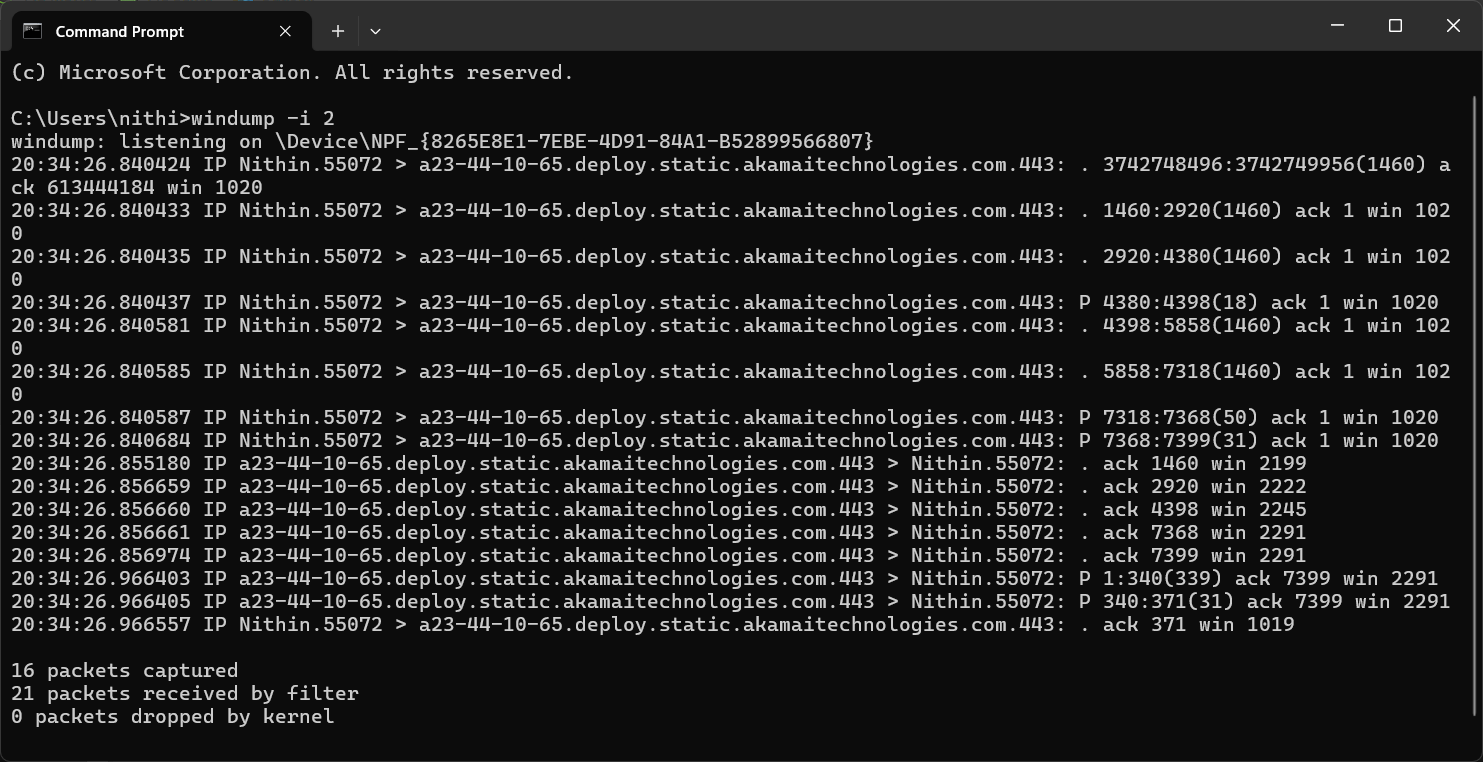
c. To write the use of *tcpdump(windump)* command execute the following commands.

**windump Command**

windump is the Windows port of the popular tcpdump tool used on Unix-like systems. It is a network packet analyzer that captures and displays the packet headers on a network interface. It can be used for network troubleshooting, monitoring, and analysis.

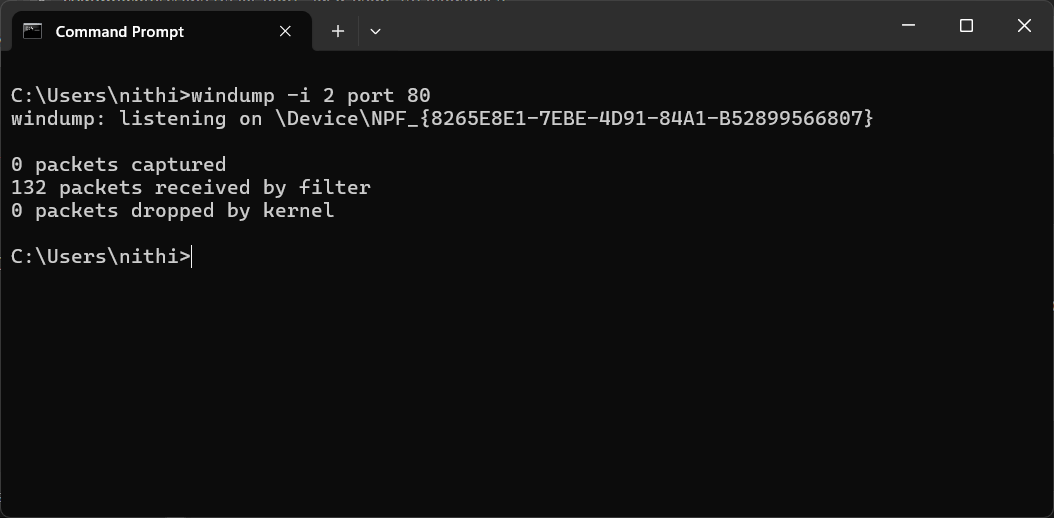
1. windump -i 1

* **Description:** Captures and displays all packets on the network interface with index 1 in real-time.
* **Use Case:** Useful for general network traffic monitoring and troubleshooting to understand the types and volume of traffic.



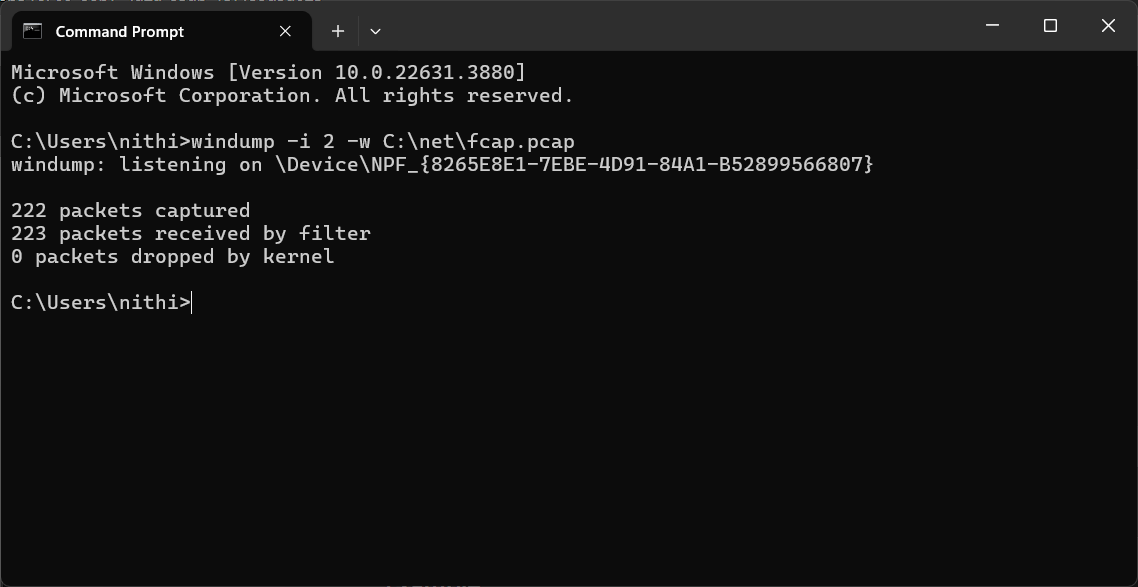
2. windump -i 1 port 80

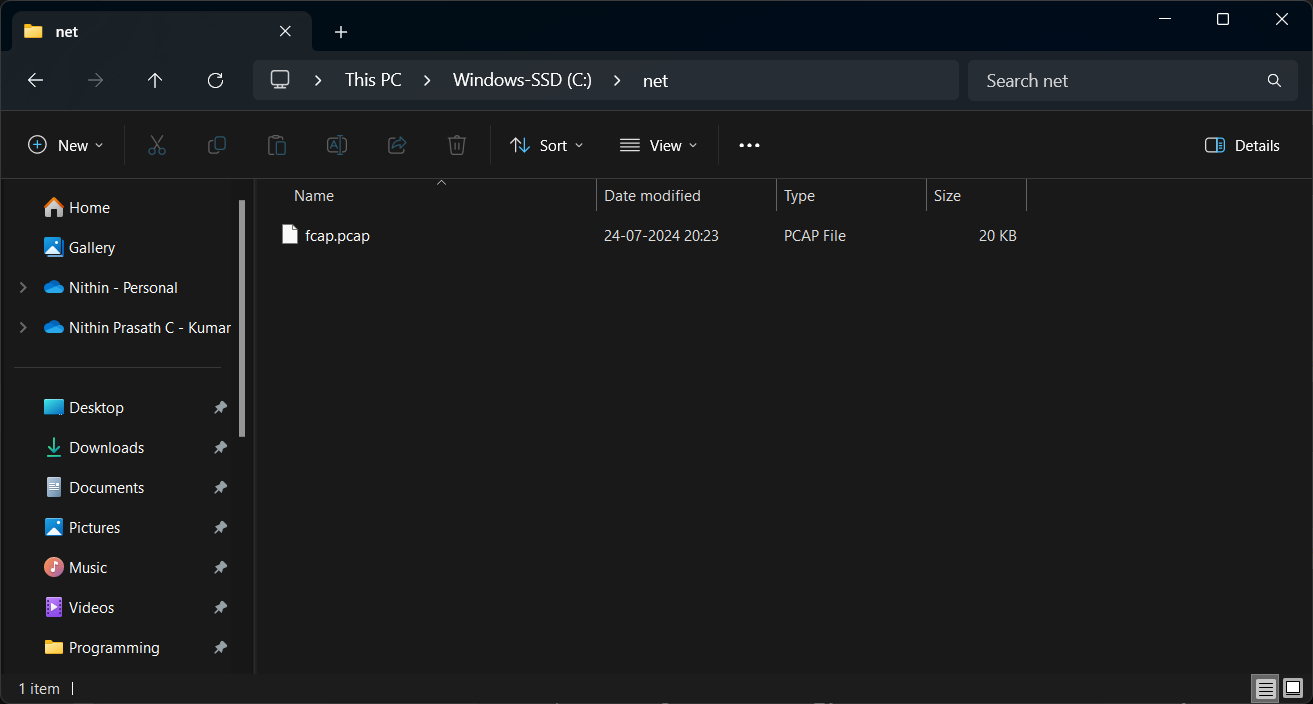
* **Description:** Captures packets on the network interface with index 1 that are destined for or originate from port 80 (HTTP traffic).
* **Use Case:** Ideal for monitoring and troubleshooting web traffic, allowing the analysis of HTTP communications between clients and servers.



3. windump -i 1 -w C:\net\fcap.pcap

* **Description:** Captures packets on the network interface with index 1 and writes them to a file named fcap.pcap in the C:\net directory.
* **Use Case:** Useful for saving network traffic data for later analysis with tools like Wireshark, aiding in detailed network forensic investigations.





d. To write the use of *traceroute* command and show the any 5 variants of the command.

Sol:

* 1. **Traceroute command**

The tracert command, known as traceroute in Unix-like systems, is a network diagnostic tool used to trace the path that packets take from a source to a destination over an IP network. It works by sending packets with incrementally increasing Time-To-Live (TTL) values, allowing it to identify each hop (router) along the route to the destination. This command helps network administrators troubleshoot connectivity issues by revealing where delays or packet losses occur, and it provides information about the round-trip time for each hop.

A screenshot of a computer program

Description automatically generated

* 1. tracert -j host-list 10.1.42.140
* **Description:** Specifies that the tracert command should use the "loose source routing" option to send packets to the destination. This allows you to specify a list of IP addresses that the packets should visit on the way to the destination.
* **Use Case:** Useful for testing connectivity through specific intermediate hosts or networks, or for bypassing certain network segments.

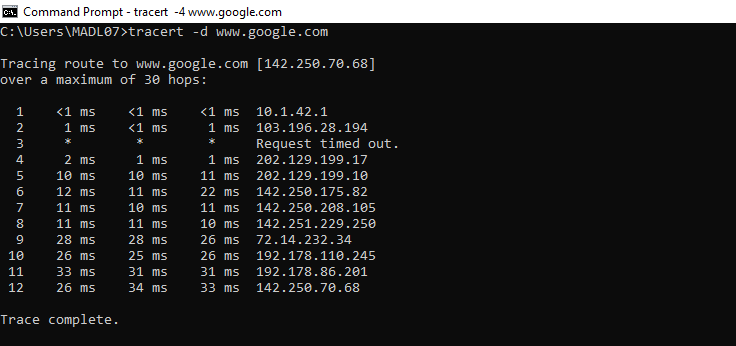
A screen shot of a computer

Description automatically generated

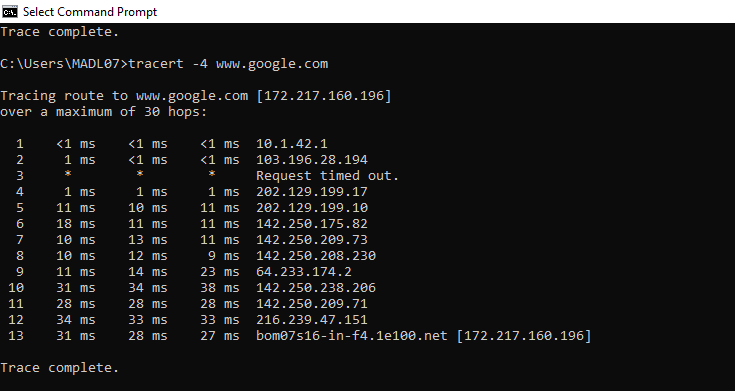
* 1. tracert -w 2000 www.google.com
* **Description**: Sets the maximum number of milliseconds to wait for a response to each probe. The default timeout is 4000 milliseconds (4 seconds).
* **Use Case**: Helpful for reducing the time spent waiting for unresponsive hops or for speeding up the overall traceroute process.



* 1. tracert -d www.google.com
* **Description**: Prevents tracert from attempting to resolve the IP addresses of intermediate hops to hostnames.
* **Use Case**: Speeds up the traceroute process by skipping the hostname resolution step, which can be slow or fail if DNS is not working properly.



* 1. tracert -4 www.google.com
* **Description**: Forces tracert to use IPv4 (-4) or IPv6 (-6) for the traceroute, even if the destination could be reached using the other protocol.
* **Use Case**: Useful for testing connectivity over a specific IP protocol version or for troubleshooting issues related to IPv4/IPv6 compatibility.



e. To write the use of *netstat* command and show the any 5 variants of the command.

*Sol:*

**netstat command**

The netstat command is a powerful networking tool used in Windows and other operating systems to display network connections, routing tables, interface statistics, and various network protocol statistics. It is essential for diagnosing network issues, monitoring network performance, and understanding the status of network connections.

1. netstat -a 10.1.42.140

* **Description**: Displays all active connections and listening ports, including both established connections and those that are waiting for incoming connections.
* **Use Case**: Useful for monitoring all network connections and identifying which ports are open and listening for connections.

A screen shot of a computer

Description automatically generated

1. netstat -h

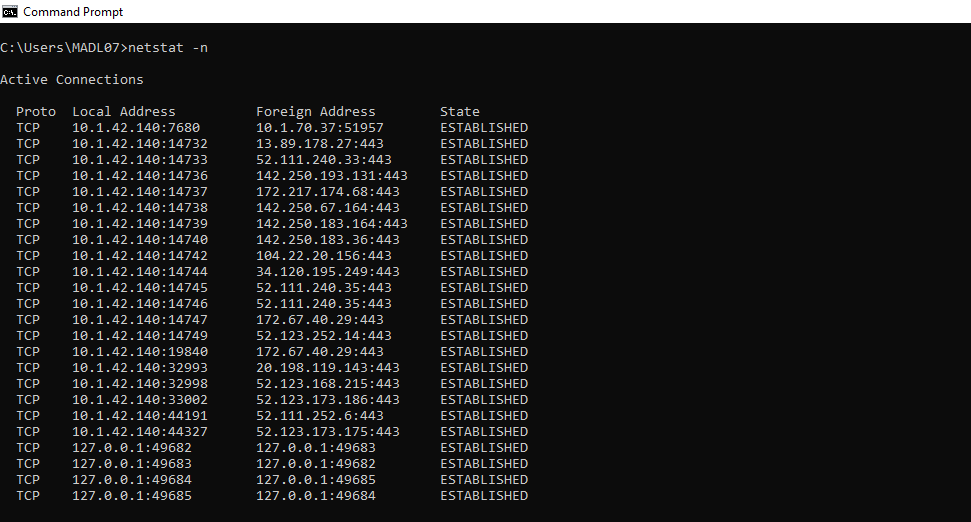
* **Description**: Displays help information about the netstat command, including available options and their descriptions.
* **Use Case**: Helpful for users who need guidance on how to use the command or want to explore its various options.

A screenshot of a computer screen

Description automatically generated

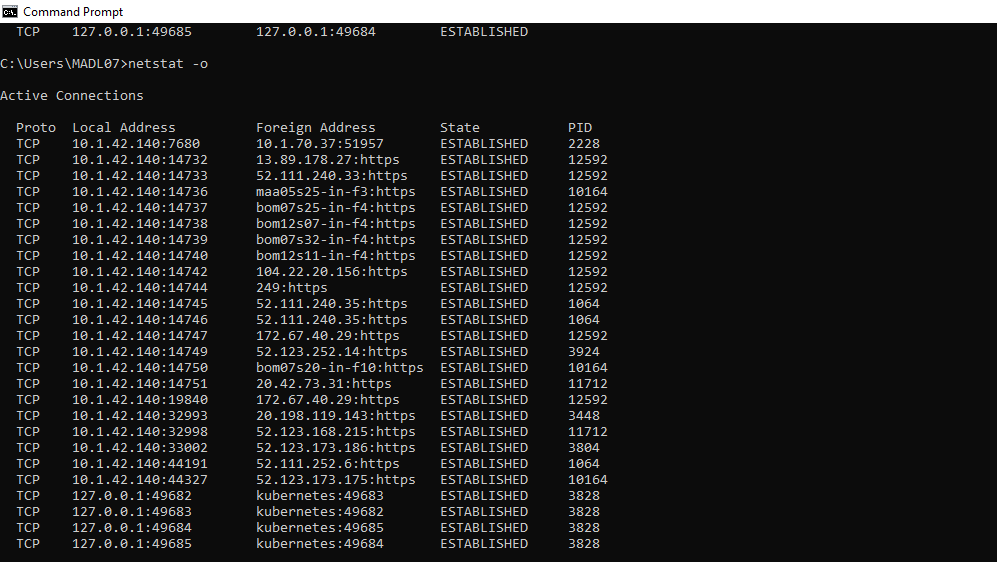
1. netstat -n

* **Description**: Displays addresses and port numbers in numerical format instead of resolving them to hostnames.
* **Use Case**: Useful for speeding up the output by avoiding DNS lookups, which can be slow or fail if there are DNS issues.



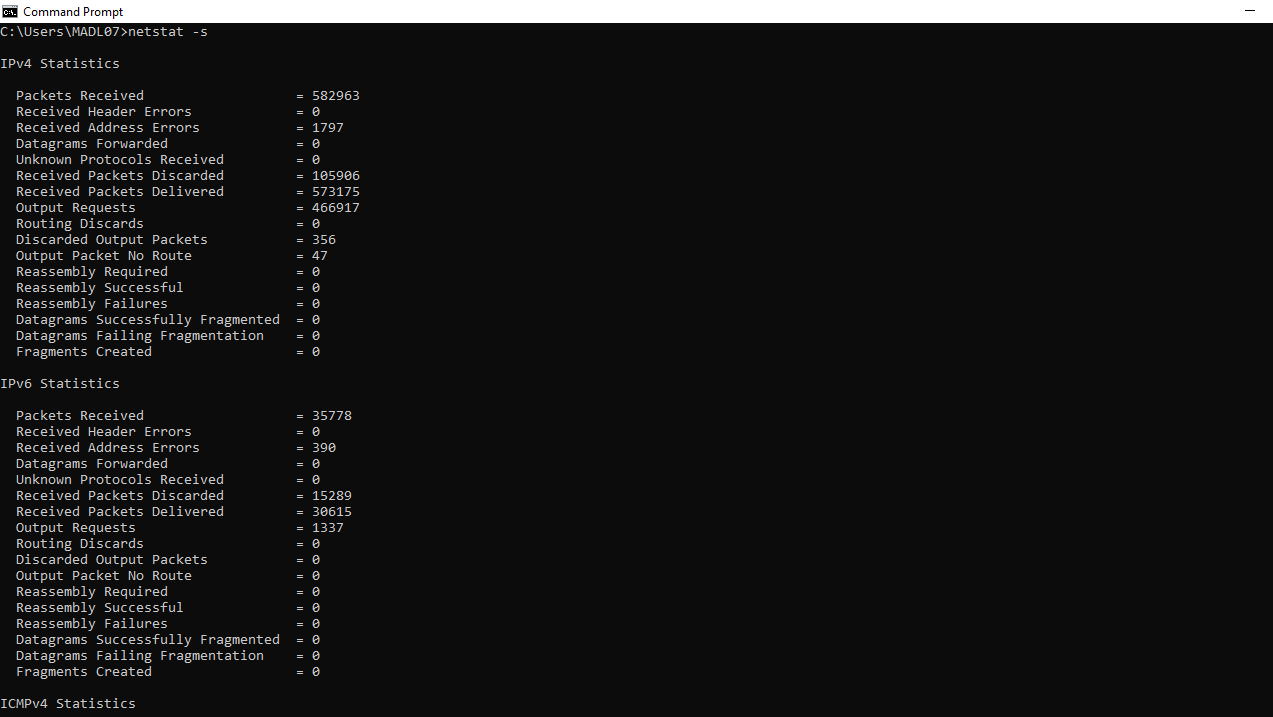
1. netstat -o

* **Description**: Displays active connections and includes the process ID (PID) associated with each connection.
* **Use Case**: Useful for identifying which applications are using specific network connections, aiding in troubleshooting and monitoring.



1. netstat -s

* **Description**: Displays statistics for each protocol (TCP, UDP, ICMP, etc.), providing detailed information about network activity and errors.
* **Use Case**: Helpful for diagnosing network issues by revealing statistics that indicate potential problems with specific protocols.



**Post Lab:**

**nslookup command:**

* **Description**: nslookup is a command-line tool used to query the Domain Name System (DNS) for information about domain names and IP addresses, enabling users to retrieve DNS records and perform reverse lookups.
* **Use Case:** It is commonly used for troubleshooting DNS issues by verifying domain name resolution, checking the IP address associated with a domain, and gathering DNS records to ensure proper configuration of web and email services.

A black screen with white text

Description automatically generated

**Result:**

All experiments have been successfully executed, with no errors or issues encountered. The expected results have been achieved, as demonstrated by the attached screenshots.