Networking commands:

* ipconfig / ifconfig  
   Purpose: Displays network configuration details for all network interfaces. Provides IP addresses, subnet masks, and default gateways. It’s useful for troubleshooting network settings.

Usage:

* 1. ipconfig (shows basic network configuration)
  2. ipconfig /all (shows detailed information including DNS servers and MAC addresses)
  3. ipconfig /release (releases the current IP address)
  4. ipconfig /renew (renews the IP address)
* ping (used for troubleshooting and how related to network)  
  Purpose: Tests network connectivity to a specific IP address or domain name. Sends ICMP Echo Requests and measures the round-trip time to check if a host is reachable.

Usage:

* 1. ping [hostname or IP] (e.g., ping google.com or ping 192.168.1.1)
  2. ping -t [hostname or IP] (continuously pings until stopped)
  3. ping -n [count] [hostname or IP] (sends a specified number of pings, e.g., ping -n 4 google.com)
* netstat  
  Purpose: Displays active network connections, listening ports, and network statistics. Useful for monitoring network activity and diagnosing issues.

Usage:

* 1. netstat (shows active connections and listening ports)
  2. netstat -an (shows all connections and listening ports with numerical addresses)
  3. netstat -r (shows the routing table)
  4. netstat -s (shows network statistics by protocol)
* tracert / traceroute (identify n use filters)  
  Purpose: Traces the route that packets take from your computer to a specified destination. Shows each hop along the way and helps diagnose routing issues and network delays.

Usage:

* 1. tracert [hostname or IP] (e.g., tracert google.com or tracert 8.8.8.8)
  2. tracert -d [hostname or IP] (disables hostname resolution to speed up the trace)
* ns lookup  
  Purpose: Queries DNS servers to obtain domain name or IP address mappings. Useful for diagnosing DNS issues and verifying DNS configurations.

Usage:

* 1. nslookup [hostname or IP] (e.g., nslookup google.com or nslookup 8.8.8.8)
  2. nslookup (starts interactive mode for further queries)
  3. nslookup [hostname] [DNS server] (queries a specific DNS server)
* dig   
  Purpose: Queries Domain Name System (DNS) servers to retrieve domain name or IP address information. Useful for diagnosing DNS issues and looking up DNS records.

Usage:

1. dig [domain]: Performs a DNS lookup for the specified domain (e.g., dig example.com). This will return the domain's A record by default.
2. dig [domain] [record type]: Queries for a specific type of DNS record (e.g., dig example.com MX for mail exchange records).
3. dig @server [domain]: Queries a specific DNS server (e.g., dig @8.8.8.8 example.com to query Google's DNS server).
4. dig -x [IP address]: Performs a reverse DNS lookup to find the domain associated with an IP address.

* hostname  
  Purpose: Displays the name of the computer as recognized on the network. Useful for identifying the system’s network name.

Usage:

* 1. hostname (shows the current hostname of the computer)
* systeminfo  
  Purpose: Provides detailed information about the computer’s configuration including OS version, build, hardware details, and system uptime.

Usage:

* 1. systeminfo (displays comprehensive system information)
* Ethtool  
  Purpose: Displays or modifies network interface parameters. Useful for managing and troubleshooting network interfaces on Linux systems.

Usage:

1. ethtool [interface]: Displays information about the specified network interface (e.g., eth0).
2. ethtool -s [interface] [options]: Sets specific parameters for the network interface. Options include settings like speed, duplex mode, and autonegotiation (e.g., ethtool -s eth0 speed 1000 duplex full).
3. ethtool -i [interface]: Displays driver information for the specified interface.
4. ethtool -p [interface]: Causes the LED on the network interface to blink, helping to physically locate the device.

* getmac (mac address of system)  
  Purpose: Displays the MAC addresses of network interfaces. Useful for identifying the hardware addresses of network adapters.

Usage:

* 1. getmac (lists MAC addresses of network interfaces)
  2. getmac /v (shows detailed information including the transport name)
* route   
  Purpose: Displays or modifies the IP routing table. Useful for managing routing entries and diagnosing routing issues.

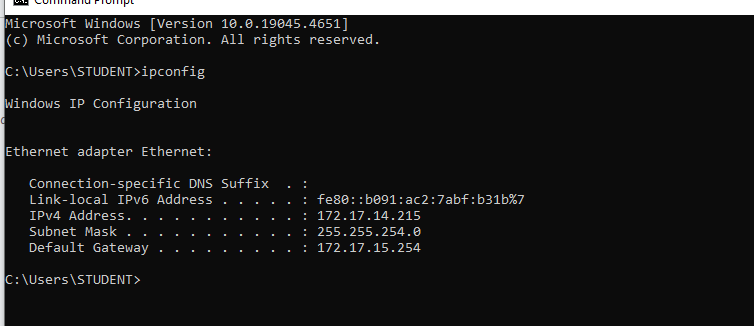
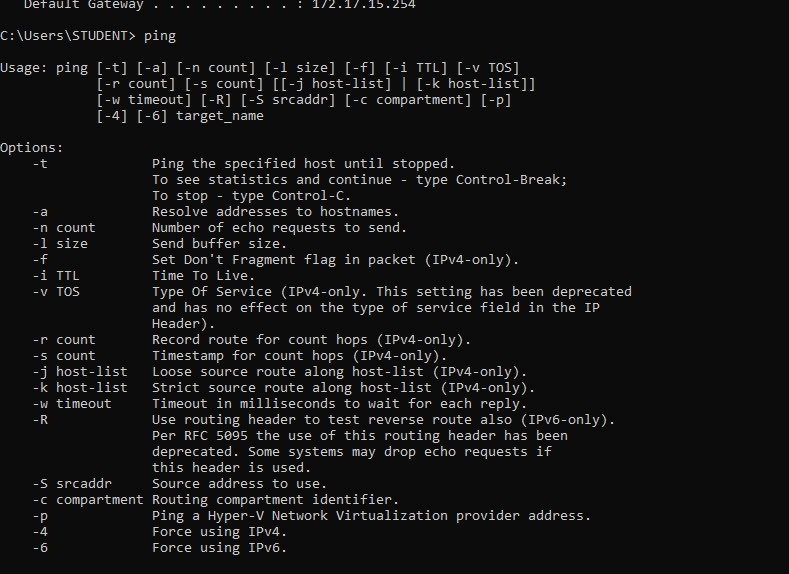
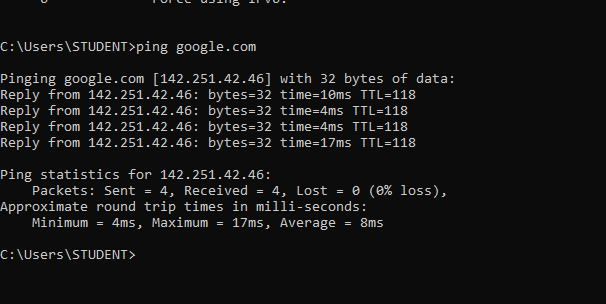
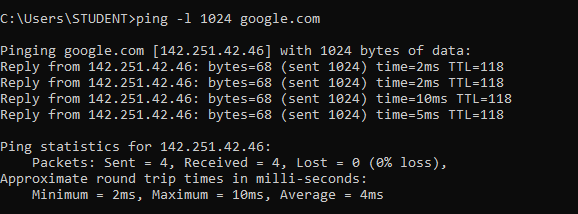
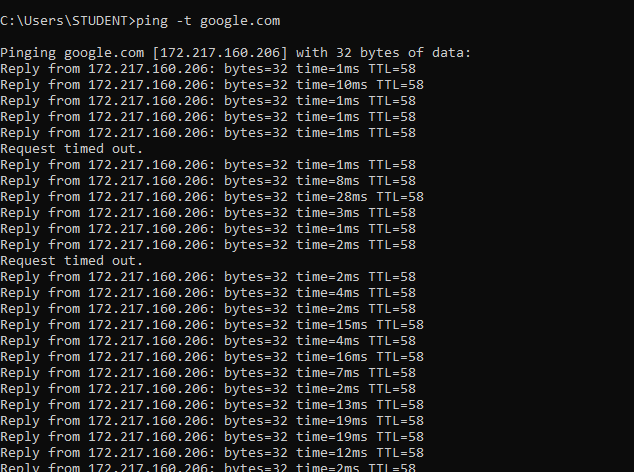
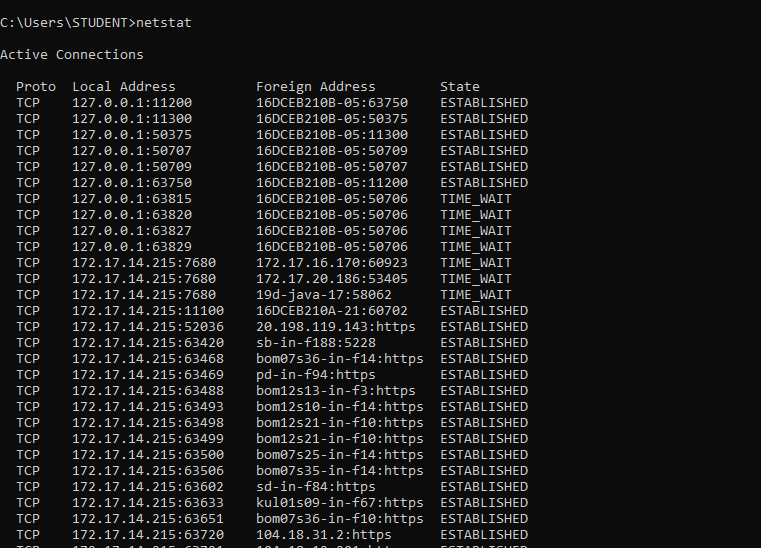
Usage:

* 1. route print (shows the routing table)
  2. route add [destination] mask [mask] [gateway] (adds a new route)
  3. route delete [destination] (removes a route)
* arp (address resolution protocol )  
  Purpose: Displays or modifies the ARP cache, which maps IP addresses to MAC addresses. Useful for managing address resolution and troubleshooting network issues.
* Usage:
  1. arp -a (shows the ARP table)
  2. arp -d [IP address] (deletes an ARP entry)
  3. arp -s [IP address] [MAC address] (adds a static ARP entry)

ping :

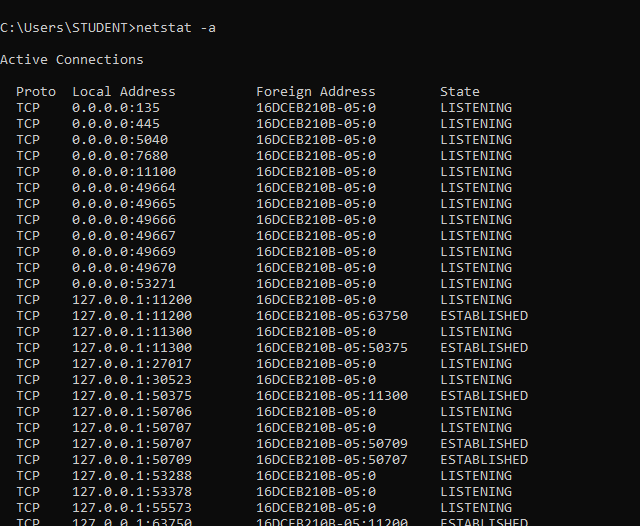
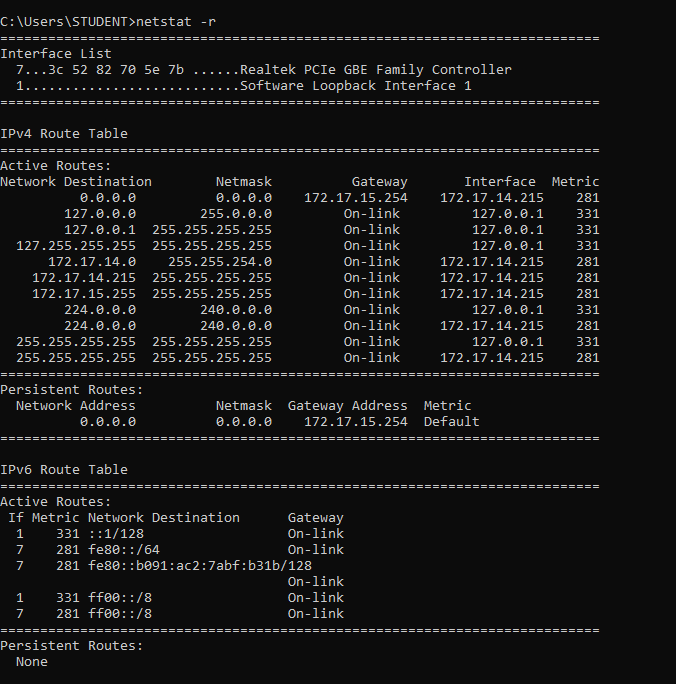
* The ping command is commonly used for troubleshooting network issues. The command sends ICMP packets to the host or the destination as ICMP echo requests. The host sends ICMP packets as a reply, and the system computes the time it took and displays the results.

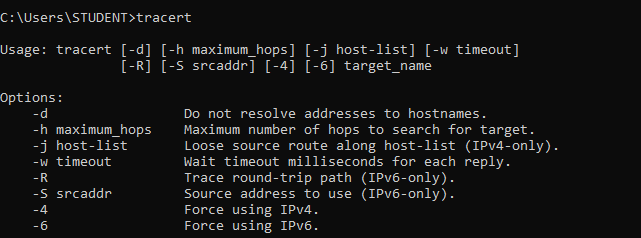
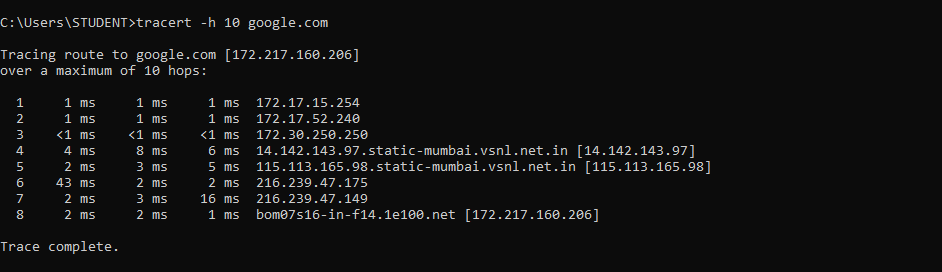
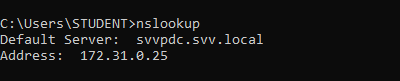
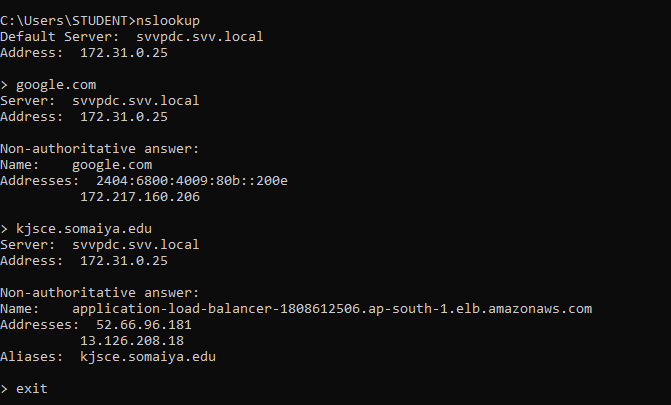
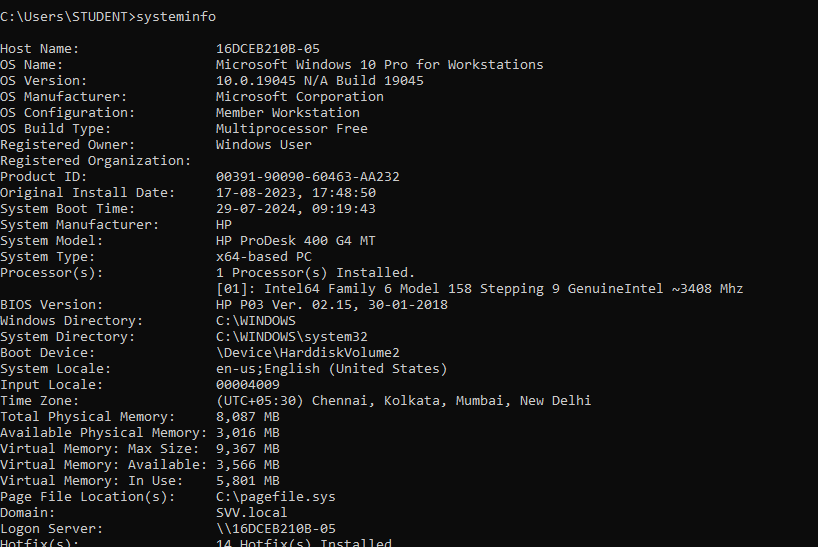
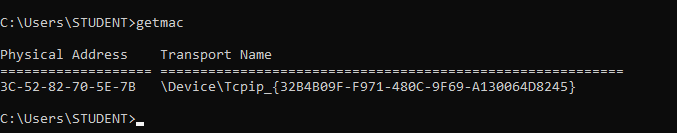
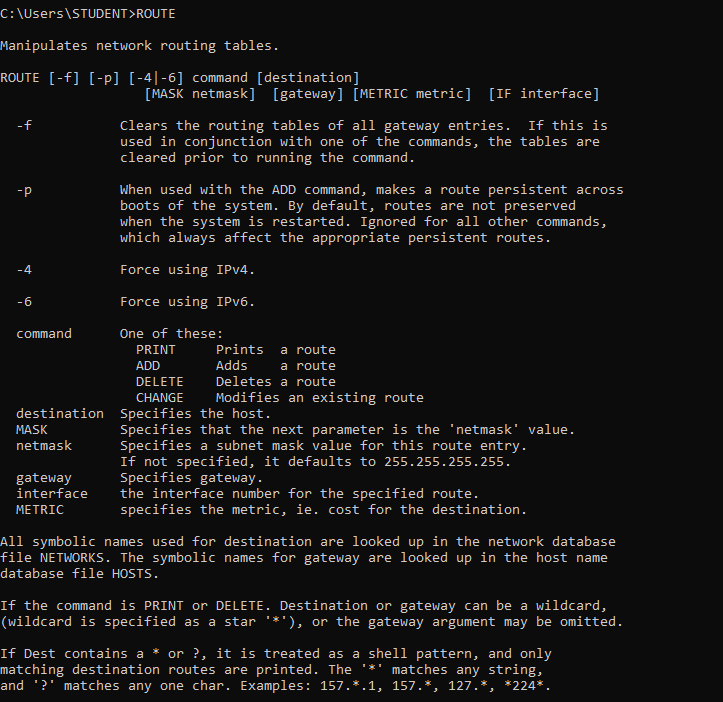
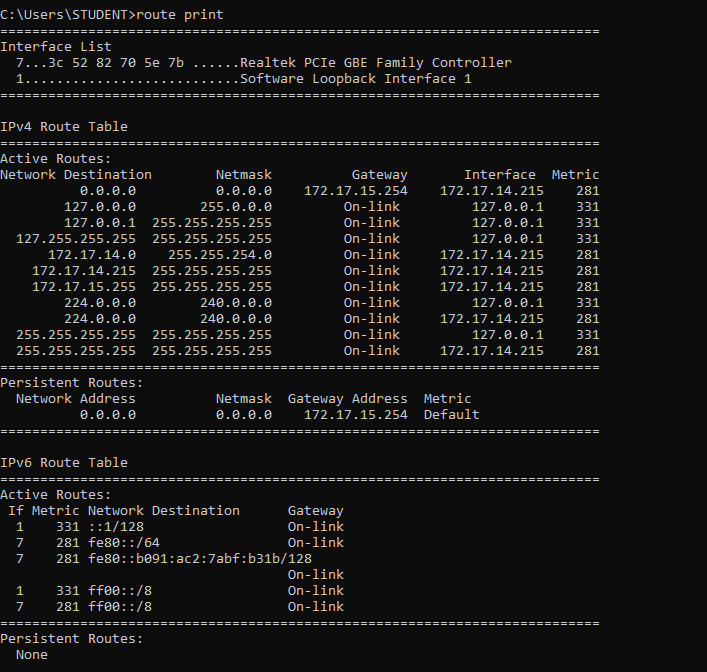
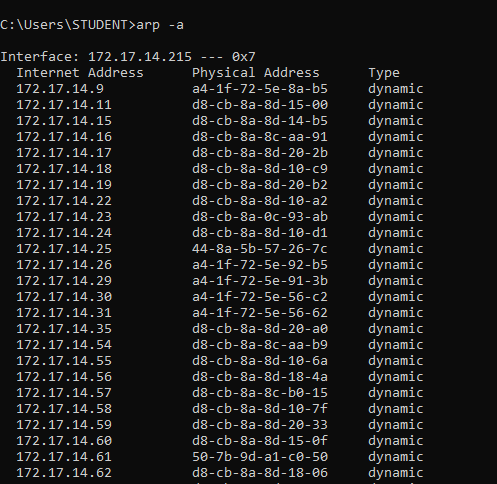
Windows:

* ipconfig / ifconfig  
  
* ping (used for troubleshooting and how related to network)  
    
    
  
* netstat  
    
  netstat -a (all connections and listening ports)

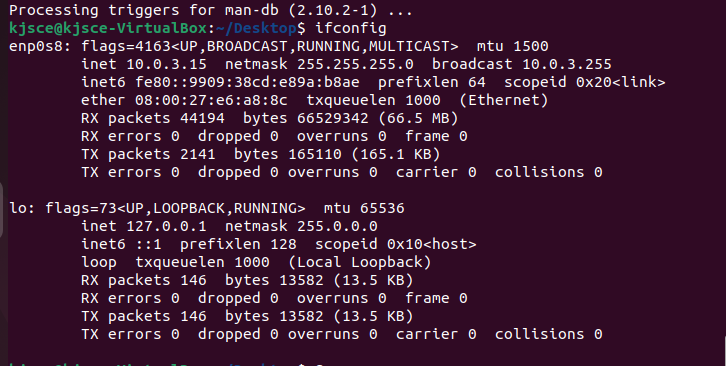
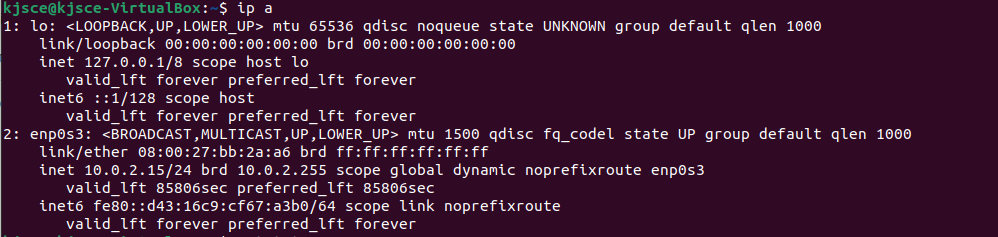
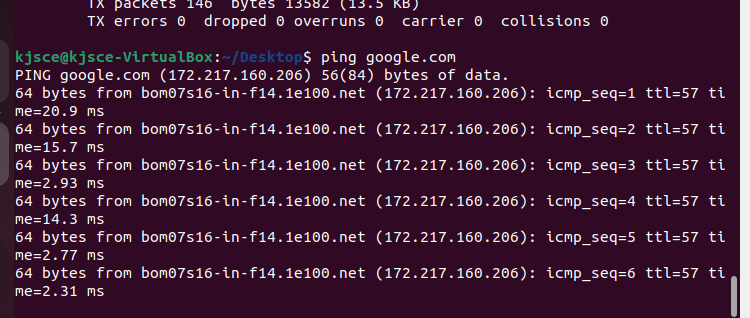
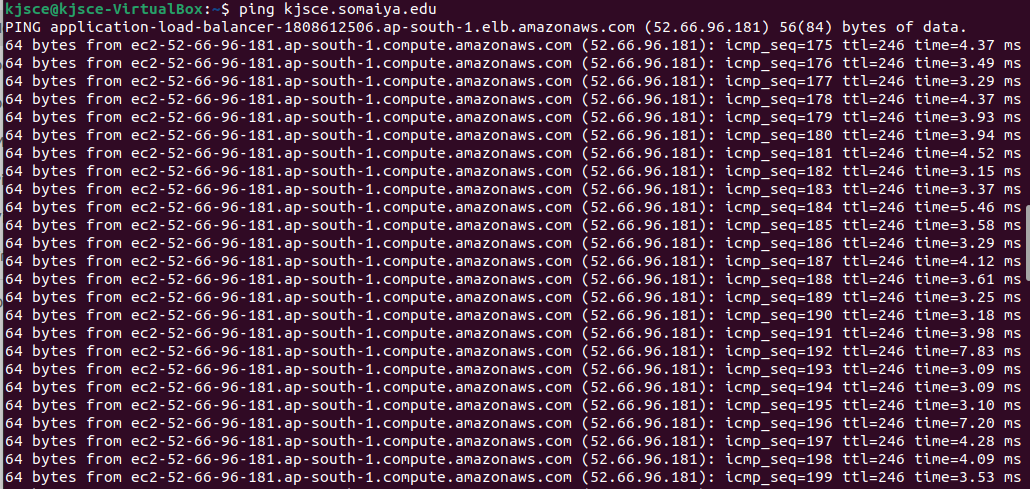
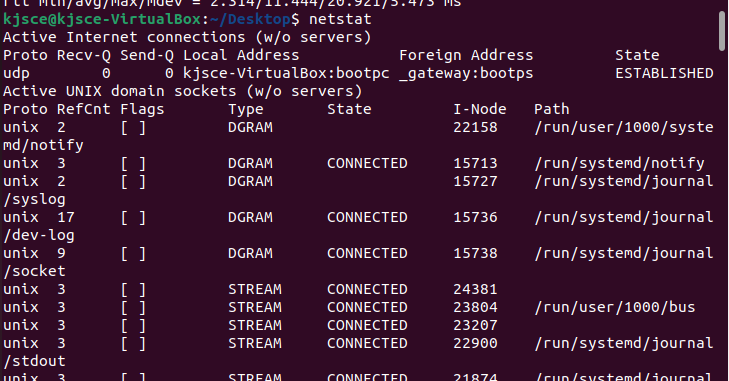
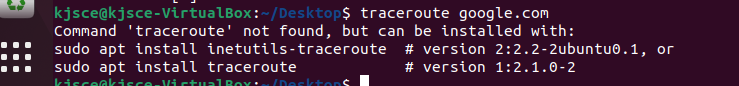
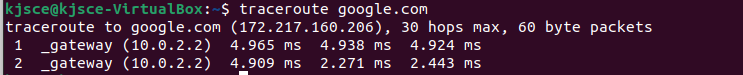
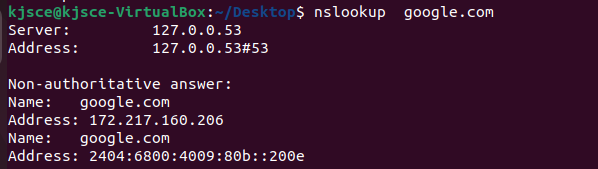
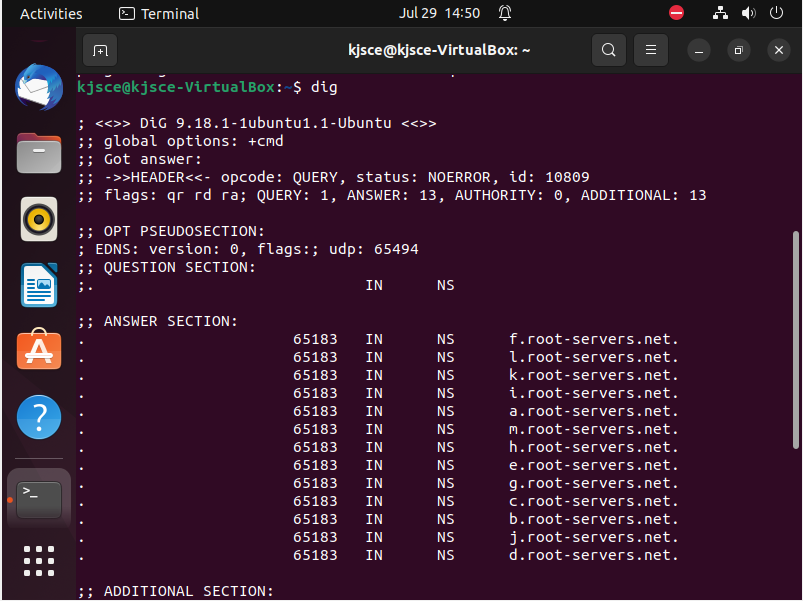
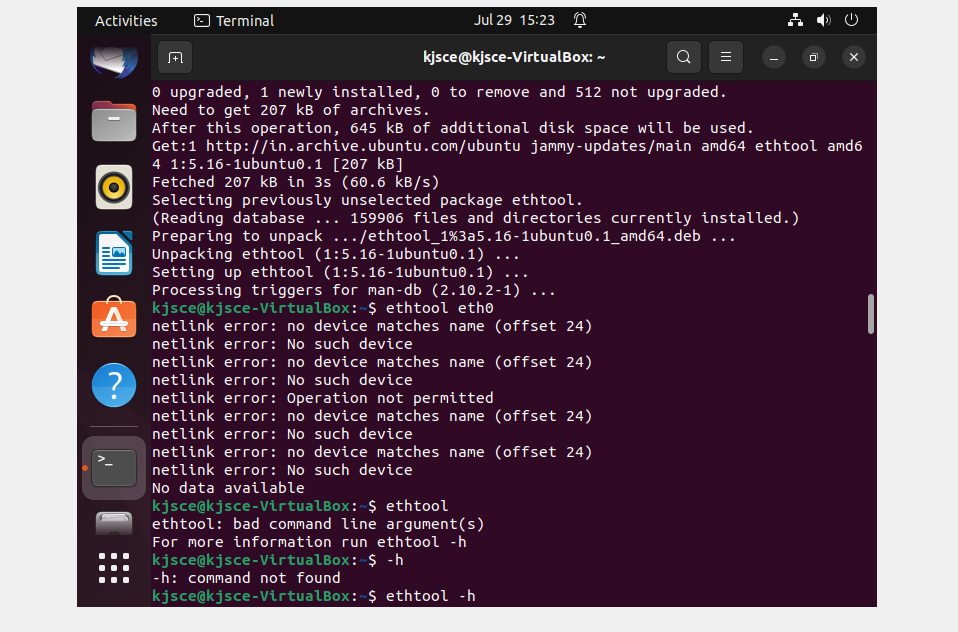
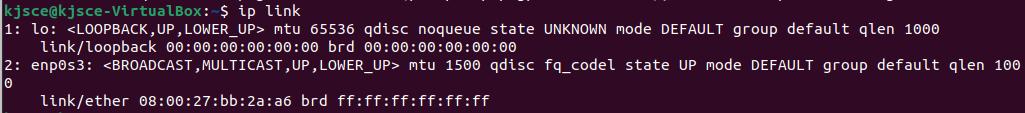
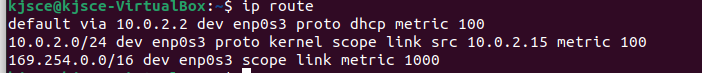
netstat -n (numerical addresses instead of resolving hostnames)

netstat -r (routing table)

* tracert / traceroute (identify n use filters)  
    
    
  
* ns lookup  
    
  
* Hostname  
  
* systeminfo   
  
* getmac (mac address of system)  
  
* route   
    
  
* arp (address resolution protocol )  
  

Linux:

* ipconfig / ifconfig   
    
  
* ping (used for troubleshooting and how related to network)  
    
  
* Netstat  
  
* tracert / traceroute (identify n use filters)  
    
  
* ns lookup  
  
* dig  
    
  
* hostname  
  
* ethtool  
  
* getmac (mac address of system) - ip link  
  
* route -iproute  
  
* arp (address resolution protocol )   
  