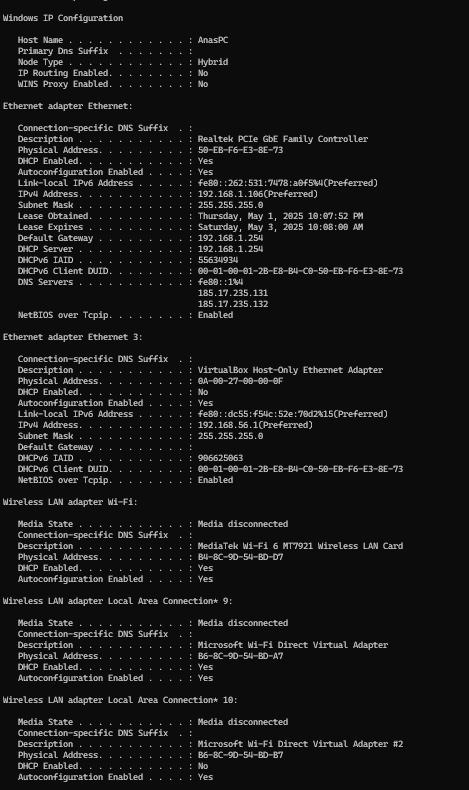
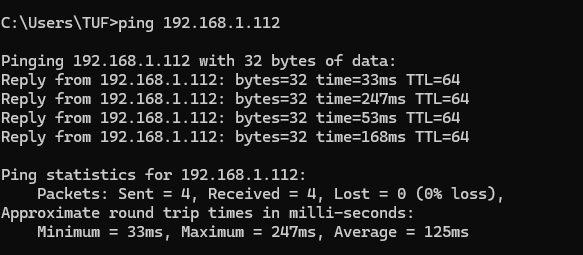
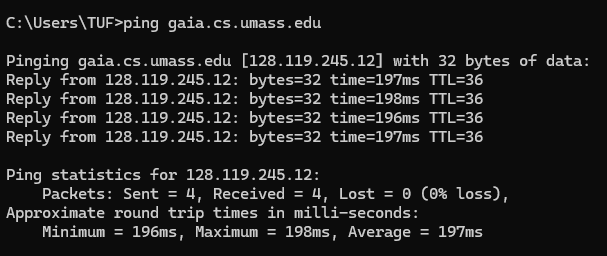
**Task 1:**

**(i) ipconfig**:  
 Displays the IP address, subnet mask, and default gateway for a computer’s network interfaces. It helps diagnose and manage network connections on Windows systems.



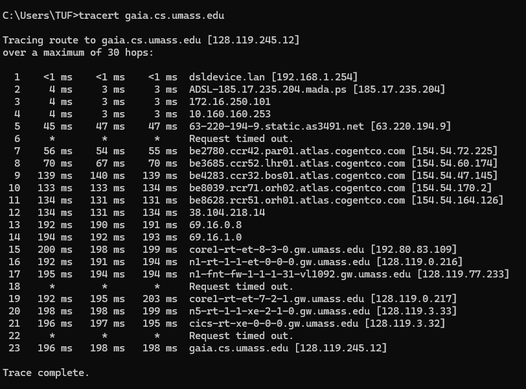
**(ii) ping**:  
 Sends test packets to a specified IP address or domain to check if it's reachable and measures response time. It's commonly used to troubleshoot network connectivity.



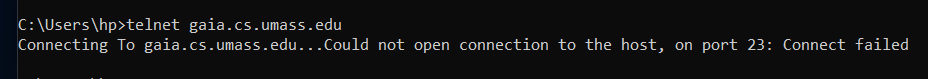


**(iii) tracert / traceroute**

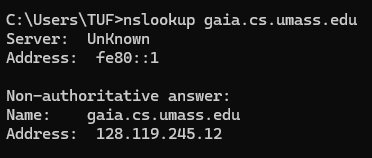
provides delay measurement from source to router along end-end Internet path towards destination



**(iv) telnet**:  
 Connects to remote devices over a network using the Telnet protocol, typically to test open ports or interact with services. It provides a text-based interface to communicate with the remote system.



**(v) nslookup**:  
 Queries DNS servers to obtain domain name or IP address mapping information. It's useful for troubleshooting DNS resolution issues.



Wireshark Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License version 2 or any later version.[3]

