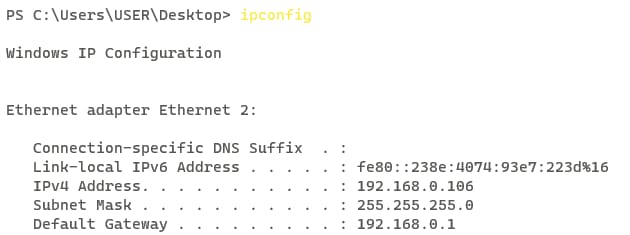
***Networking Lab Assignment***

**Part 1: Exploring Basic Networking Commands**

**Basic Networking Commands for Network Analysis**

**Identifying Network Configuration**

1. **Objective:** Understand the network configuration of your system.

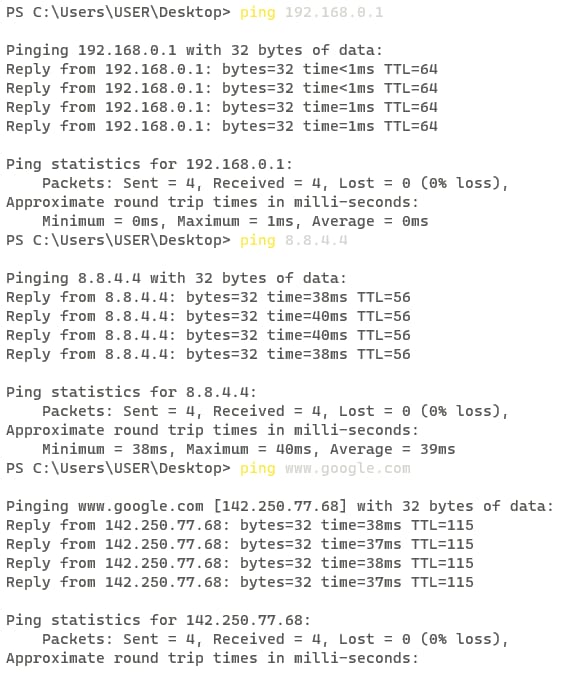


1. **Questions** 
   1. **What is your system's IP address?**

* System’s IP address is 192.168.0.106
  1. **What is the role of the default gateway in your network?**
  + **default gateway** serves as an intermediary device that routes traffic from your local network to external networks, often the internet.

**Testing Network Connectivity**

1. **Objective:** Use the **ping** command to test connectivity with other devices.



1. **Questions** 
   1. **Was the ping to each target successful?**
   * The success of each ping will depend on several factors such as the target's availability, network configuration, and any potential firewall restrictions.
   1. **If a ping failed, what might be the reason?**

* Network Congestion: Too much traffic on the network.
* Firewall Blocking: Firewall settings blocking ping requests.
* Host Unreachable: The target device is off or disconnected.
* Incorrect IP Address: The IP address is wrong or unassigned.
* Routing Issues: Problems with the routing configuration.
* ISP Issues: Connectivity problems with the Internet Service Provider.

**Tracing Routes**

1. **Objective:** Use the traceroute command to map the path to a destination.



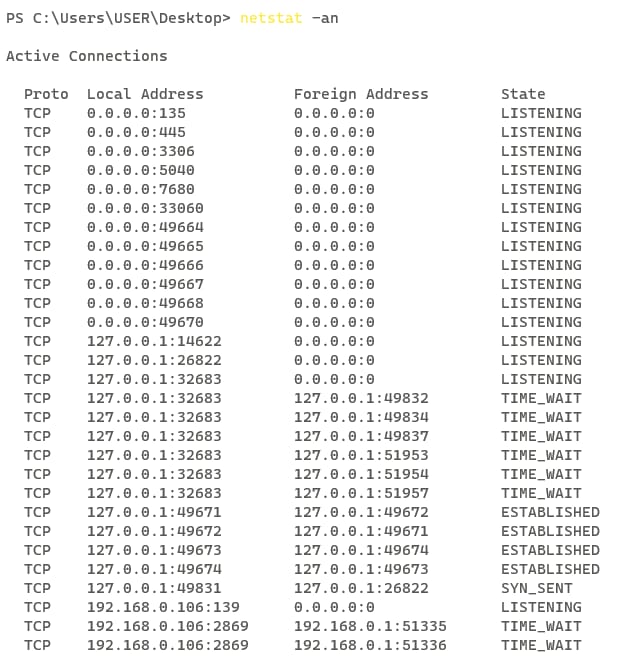
1. **Questions** 
   1. **How many hops did it take to reach** [**www.google.com**](http://www.google.com)**?**

* Maximum 30 hops it took to reach the [www.google.com](http://www.google.com)
  1. **Did any hops time out? If so, what could cause this?**
* possible causes:

1. **Network Congestion**: High traffic levels causing delays.
2. **Firewall Blocking**: Firewalls along the path blocking traceroute requests.
3. **Router Configuration**: Routers configured not to respond to traceroute requests.
4. **Down Device**: A router or device in the path might be offline or malfunctioning.
5. **IP Fragmentation**: Large packets being fragmented and some fragments getting lost.
6. **Routing Changes**: Dynamic changes in the routing path leading to temporary timeouts.

**Examining Active Connections**

1. **Objective:** Identify active network connections using netstat.



1. **Questions** 
   1. **What are the most common protocols (e.g., TCP, UDP) used in the active connections?**

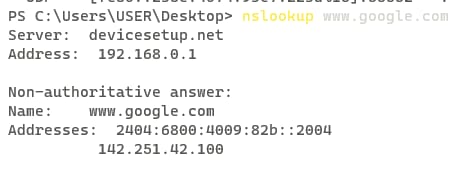
* In computer networks, some of the most commonly used protocols for active connections are:
  + TCP (Transmission Control Protocol)
  + UDP (User Datagram Protocol)
  + HTTP/HTTPS (Hypertext Transfer Protocol/Secure)
  + FTP (File Transfer Protocol)
  + SMTP (Simple Mail Transfer Protocol)
  + IMAP/POP3 (Internet Message Access Protocol/Post Office Protocol 3)
  + SSH (Secure Shell)
  1. **Why might some ports be in a listening state?**

Ports can be in a listening state for several reasons, primarily to allow applications and services to accept incoming connections. Here are some key reasons:

* Server Applications: Applications like web servers (HTTP/HTTPS), email servers (SMTP, IMAP), and file servers (FTP) keep their ports open to receive requests from clients.
* Remote Access Services: Services like SSH (Secure Shell) and RDP (Remote Desktop Protocol) keep ports open to allow remote management and access.
* Background Services: Various system services and background processes listen on specific ports to perform tasks like network management, authentication, and logging.

**DNS and Name Resolution**

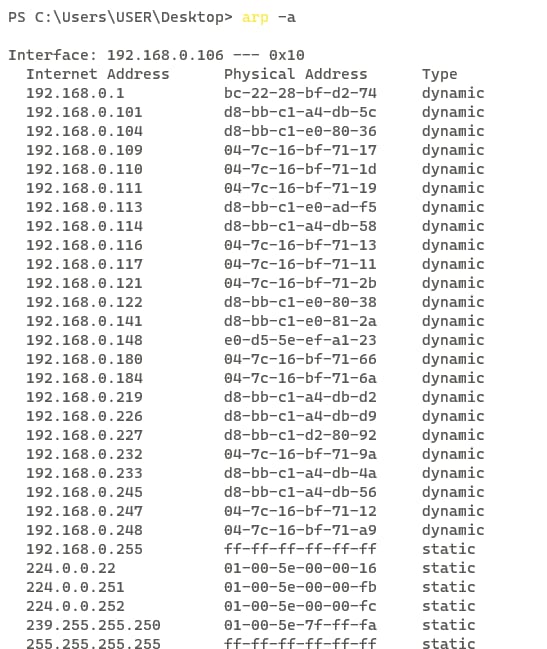
**Objective:** Understand how DNS resolves domain names to IP addresses.



* **Questions** 
  1. **What is the resolved IP address of** [**www.google.com**](http://www.google.com)**?**
* 2404:6800:4009:82b:2004
  1. **What happens if you try to resolve a non-existent domain (e.g.,** [**www.invalidexample.com**](http://www.invalidexample.com)**)?**
* DNS Error: Your DNS server will fail to find the corresponding IP address and return an error, typically a "NXDOMAIN" (Non-Existent Domain) response, indicating that the domain does not exist.

**Exploring ARP Cache**

1. **Objective:** View the ARP cache on your system.



1. **Questions**
   1. **What is the purpose of the ARP cache?**

* Its main purpose is to facilitate efficient and quick communication within a local network by avoiding repeated ARP requests
  1. **How can outdated ARP entries affect network communication?**
* Outdated ARP entries can cause several issues in network communication:
* Failed Communication: If the MAC address mapped to an IP address changes (e.g., a device is replaced), outdated entries can lead to failed data transmission.
* Network Congestion: Repeated failed attempts may lead to increased ARP traffic, congesting the network.

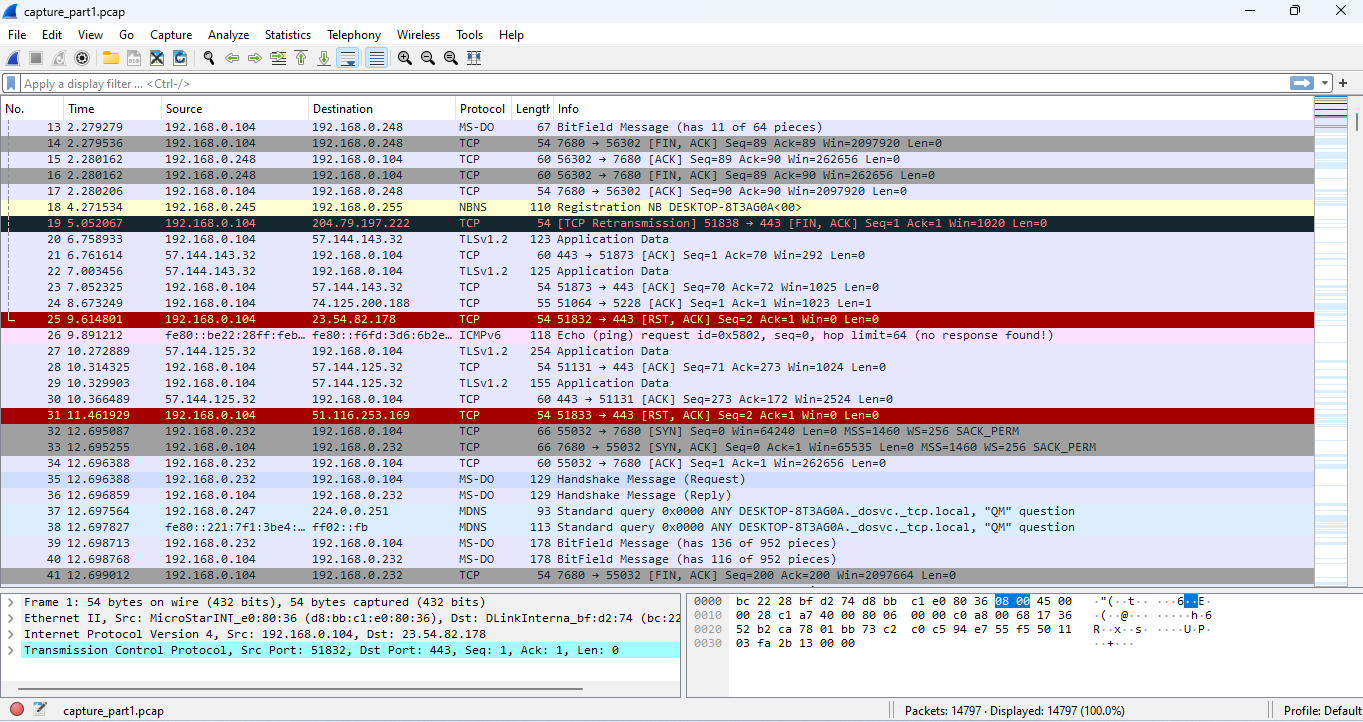
**Part 2: Packet Capture and Analysis Using Wireshark**

**Objective:**

This lab introduces students to network packet analysis using Wireshark. By completing the assignment, students will learn how to capture, filter, and analyze network traffic effectively.

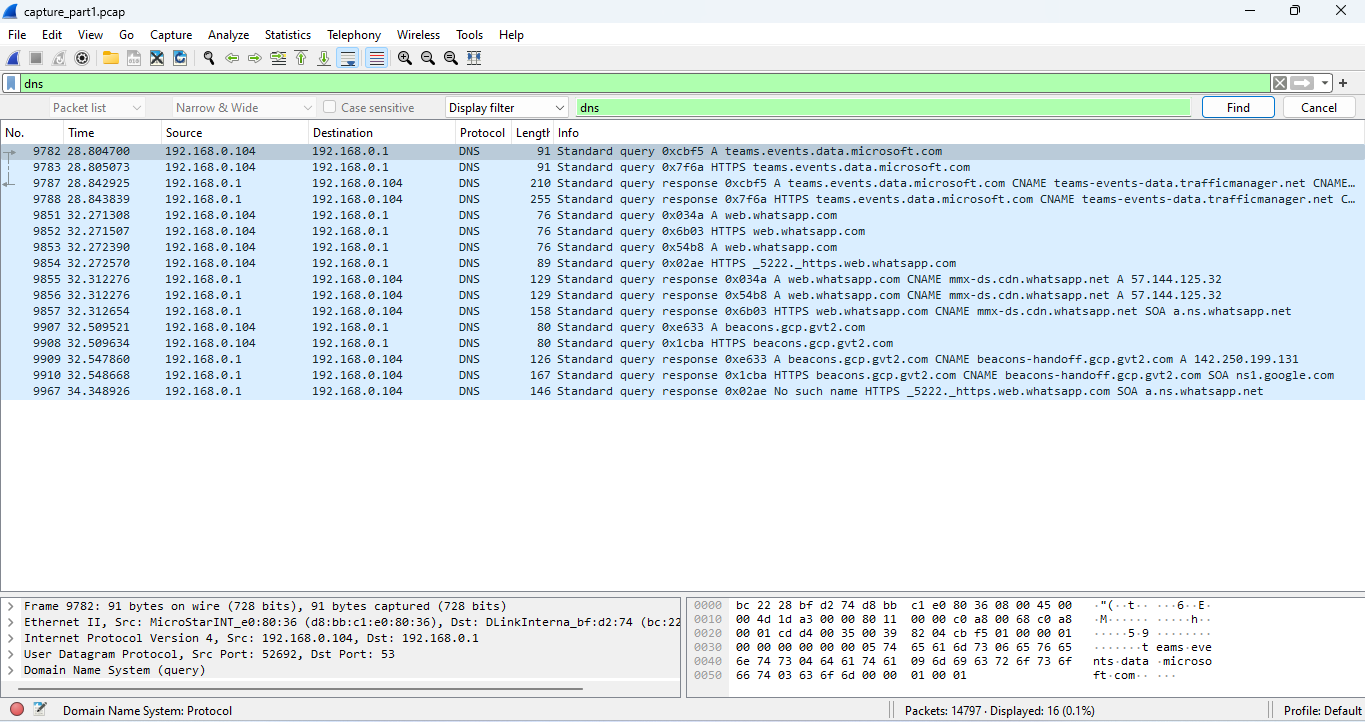
**Getting Started with Wireshark**

1. **Objective:** Familiarize students with the Wireshark interface and basic functionality.



**Applying Filters**

1. **Objective:** Learn to apply display filters to narrow down relevant packets.



**Analyzing Protocols**

1. **Objective:** Dive deeper into protocol details and packet structure.

