TASK 1 – INTRODUCTION TO NETWORK SECURITY BASICS

REPORT BY: UJJWAL AHUJA

INTRODUCTION

In today's digital age, network security is critical for protecting devices and data from unauthorized access and cyberattacks. This task introduced key security principles by simulating a small network environment and implementing basic protections such as firewall configuration and encrypted Wi-Fi. Through hands-on experience with tools like Windows Defender Firewall and Wireshark, I gained a practical understanding of how to identify threats and secure network communication.

TASK OBJECTIVE

This task focused on building a foundational understanding of network security by exploring various types of network threats and learning how to secure a basic home or test network. The objective was to simulate a small-scale secure network, configure firewalls, and monitor network traffic to detect suspicious activity.

NETWORK THREAT RESEARCH

Viruses and Worms

- Viruses are malicious programs that attach themselves to legitimate files or software. They require user action to spread — for example, opening an infected file or running a compromised program.
- Worms, on the other hand, are self-replicating and do not need any user interaction to propagate. They spread automatically through network connections, often exploiting software vulnerabilities.

  Real-World Impact:
  Worms like WannaCry and ILOVEYOU caused billions in damages by spreading across global networks within hours. These threats can consume bandwidth, overload systems, and disrupt services.

Trojans

- A Trojan horse (or simply “Trojan”) is malware that pretends to be legitimate software to trick users into installing it. Once activated, it may give hackers remote access to the system, log keystrokes, install additional malware, or steal sensitive data.

  Key Characteristics:

- Often hidden in email attachments or pirated software.
- Can open backdoors for further exploitation by attackers.

  Example:
  A common type of Trojan is a Remote Access Trojan (RAT) that allows the attacker to fully control the infected machine as if they were physically using it.

Phishing Attacks

- Phishing is a form of social engineering in which attackers impersonate trustworthy entities (like banks, email providers, or government services) to trick users into revealing personal information — such as usernames, passwords, or credit card details.

  How It Works:

- Victims receive an email or message with a fake link that leads to a copycat website.
- When users enter their credentials, the information is captured by the attacker.

  Real-World Relevance:
  Phishing is one of the most common attack methods today. It's often the first step in larger attacks like identity theft, business email compromise (BEC), and ransomware deployment.

Man-in-the-Middle (MitM) Attacks

- A Man-in-the-Middle attack occurs when an attacker secretly intercepts and potentially alters the communication between two parties (e.g., a user and a website) without either party knowing.

  Techniques Include:

- Intercepting public Wi-Fi traffic
- ARP spoofing (tricking devices into routing traffic through the attacker)

- HTTPS stripping (forcing unencrypted communication)

  Why It's Dangerous:
  MitM attacks allow hackers to eavesdrop on private conversations, steal login credentials, modify transactions, or inject malicious content into communications.

  Example Scenario:
  Imagine logging into your online bank from a coffee shop's unsecured Wi-Fi. An attacker running a MitM tool could intercept your session and steal your account information — even if you're on the correct website.

BASIC SECURITY MEASURES IMPLEMENTED

Step 1: Set Up a Small Network Environment

What I Did:

- Connected two devices (laptop and smartphone) to my Wi-Fi network.
- Used this setup to simulate a real-world home or office network.

Why:

- This small network allowed me to test security settings in a controlled environment.

Step 2: Enable and Configure Windows Defender Firewall

What I Did:

1. Opened the **Start Menu** and searched for "Windows Defender Firewall."
2. Clicked on **"Turn Windows Defender Firewall on or off."**
3. Made sure the firewall was **enabled for both private and public networks**.

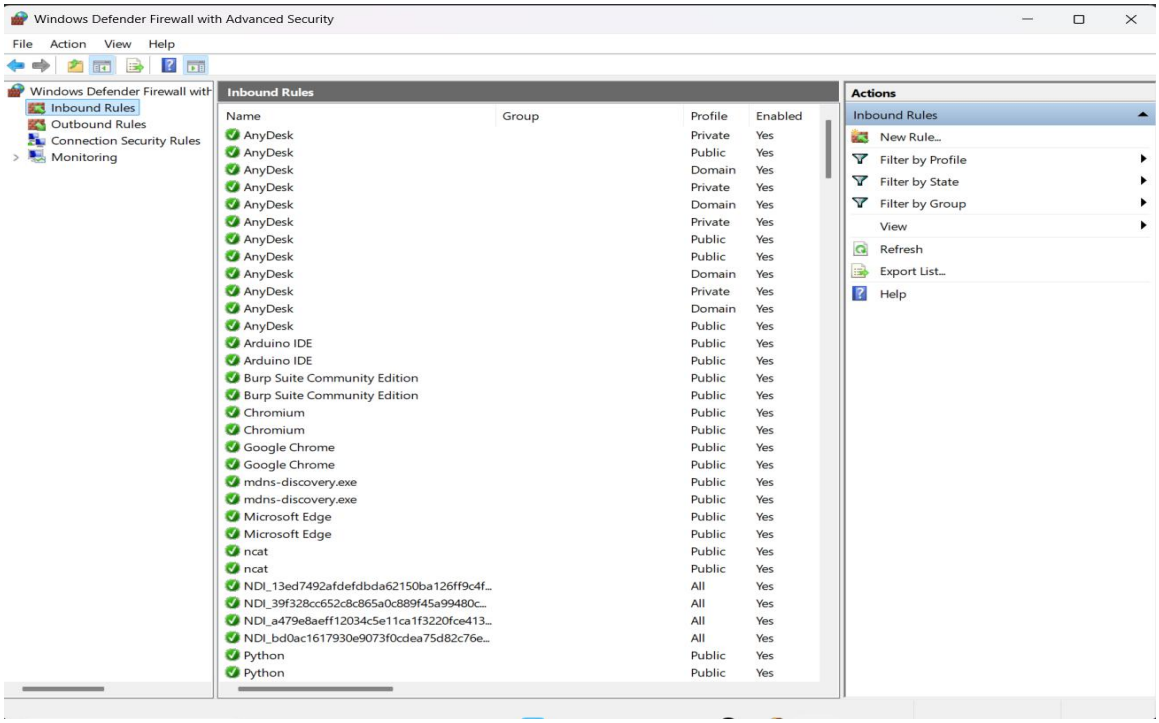
Advanced Configuration:
4. Clicked on **"Advanced Settings"** to open **Windows Firewall with Advanced Security**.
5. Created new rules to:

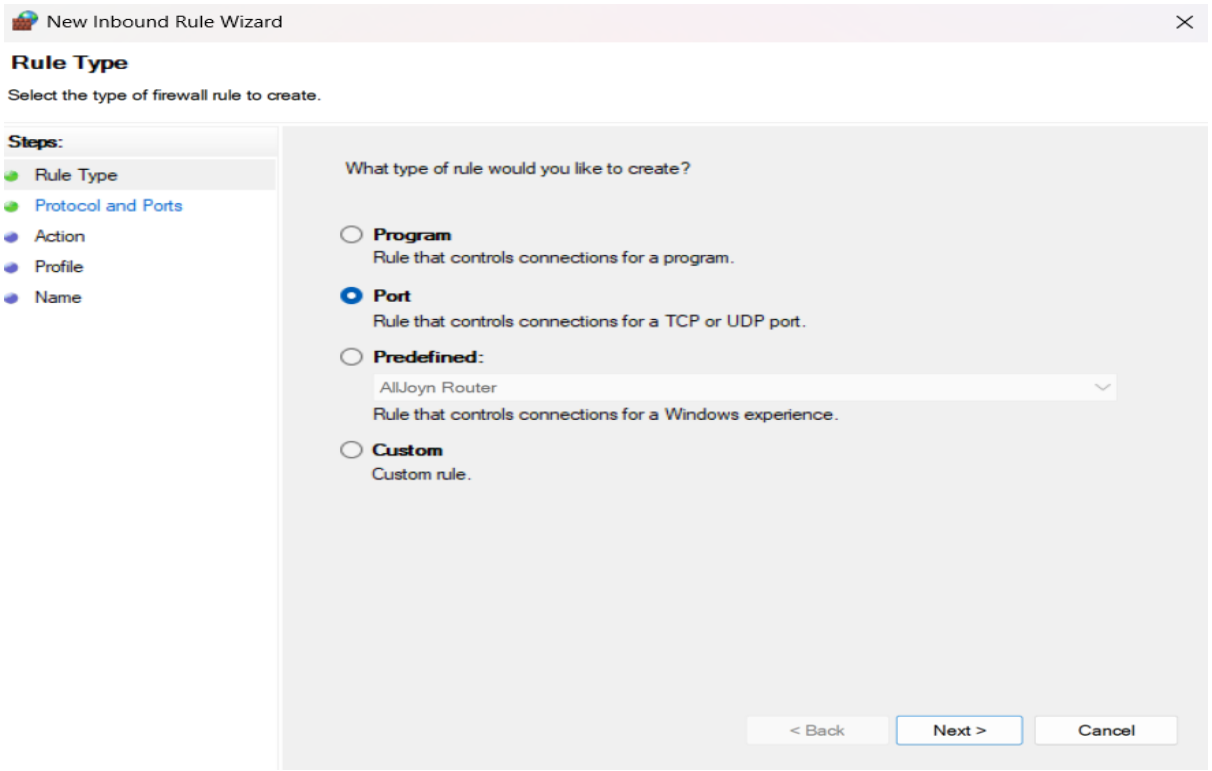
- Block all **inbound connections** (except those allowed).
- Allow specific apps like browsers and antivirus only.

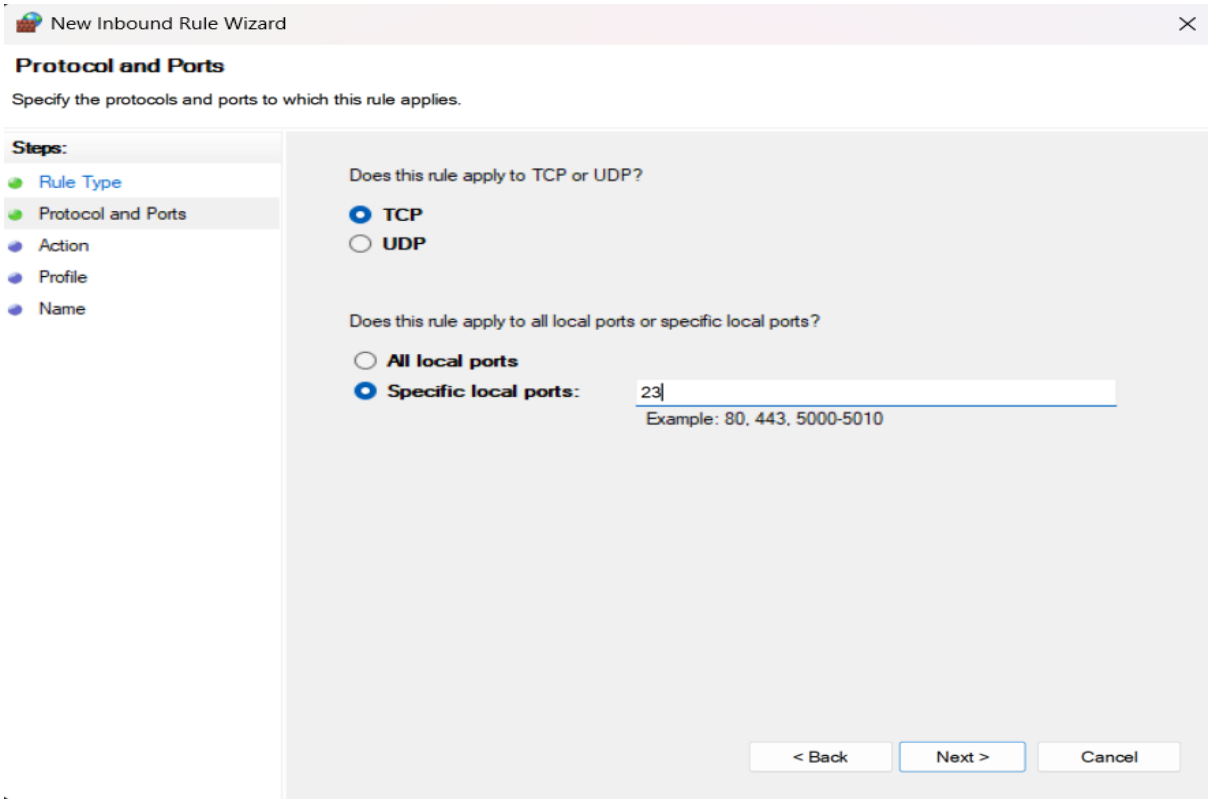
Why:

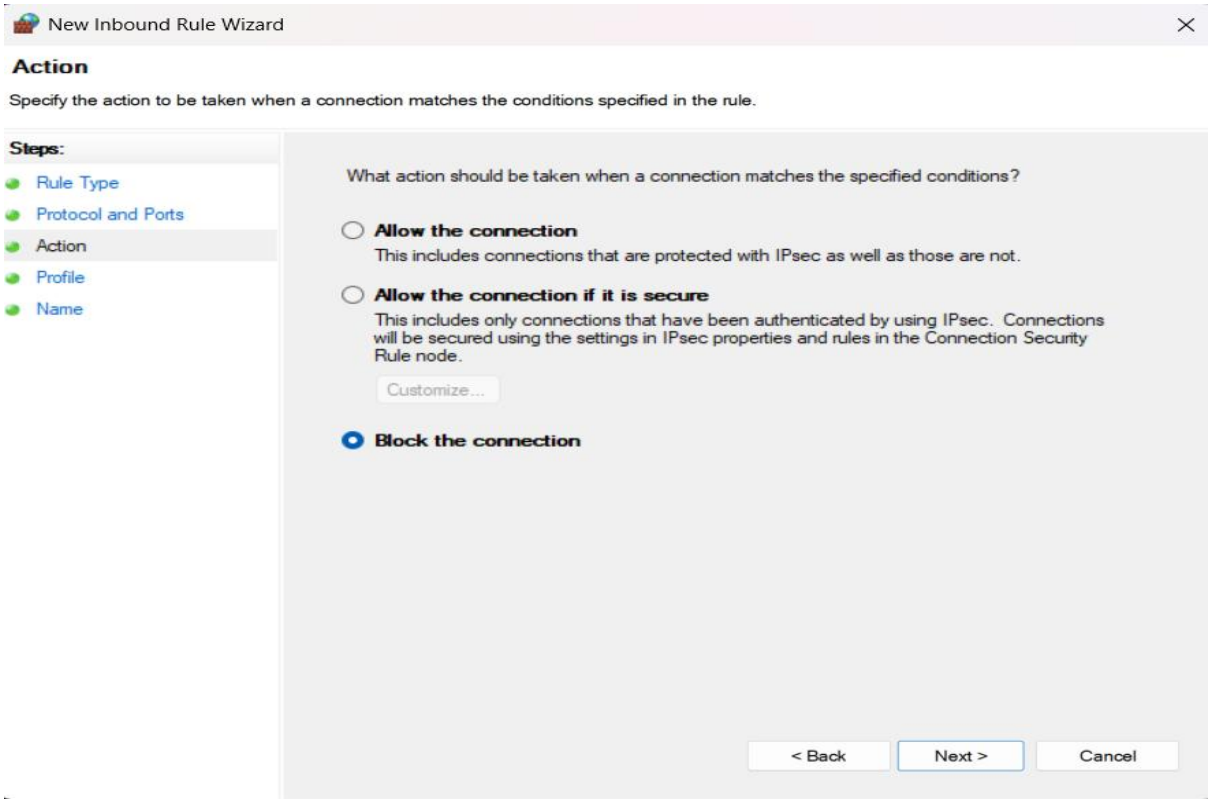
- Firewalls monitor and control incoming/outgoing network traffic.

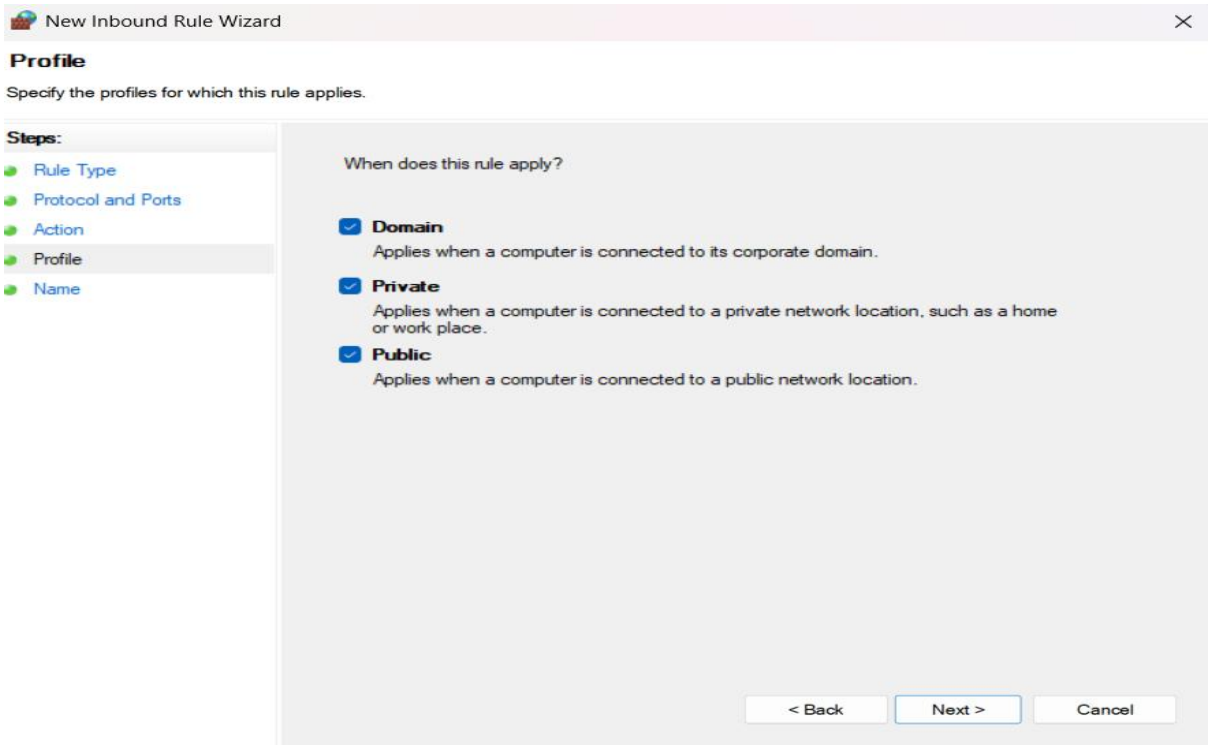
- Blocking unnecessary traffic reduces exposure to attacks.

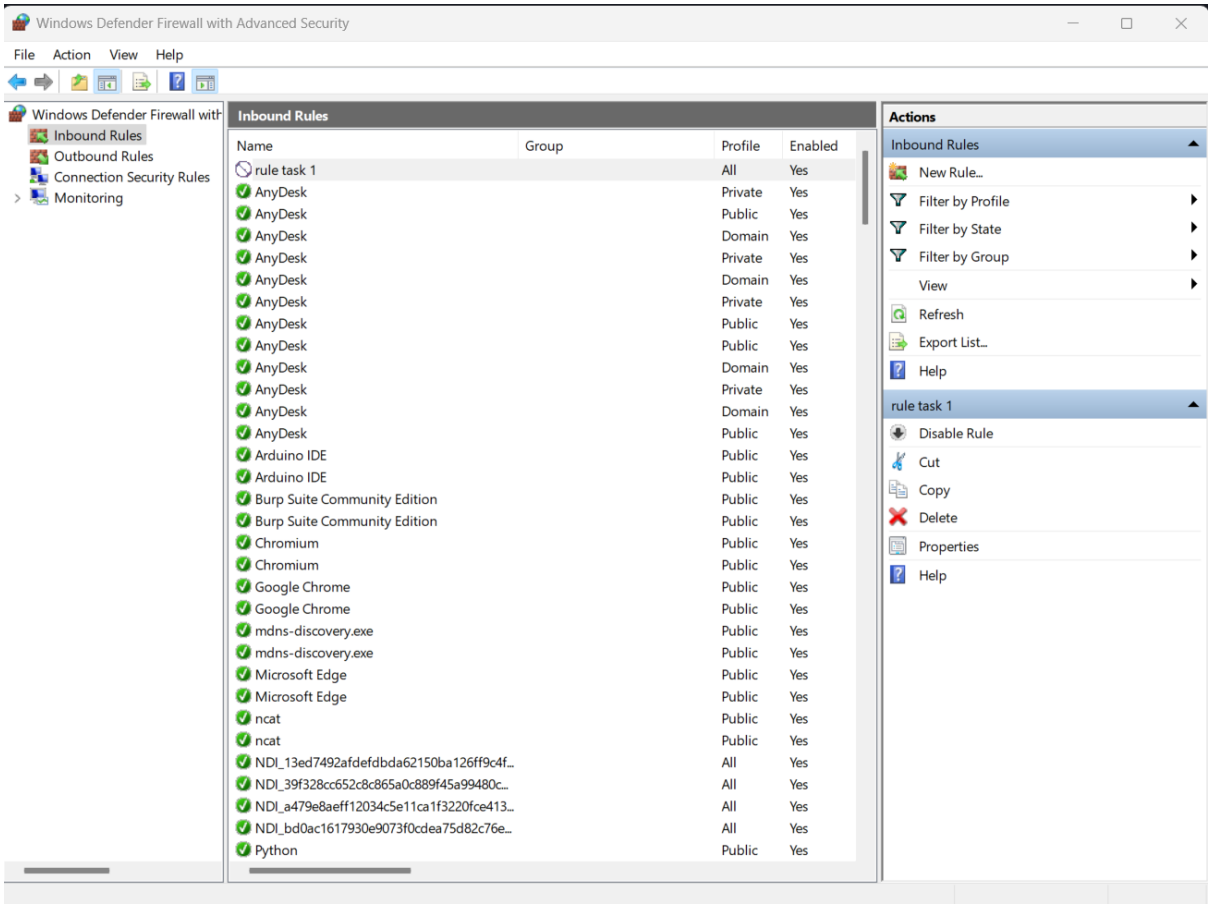


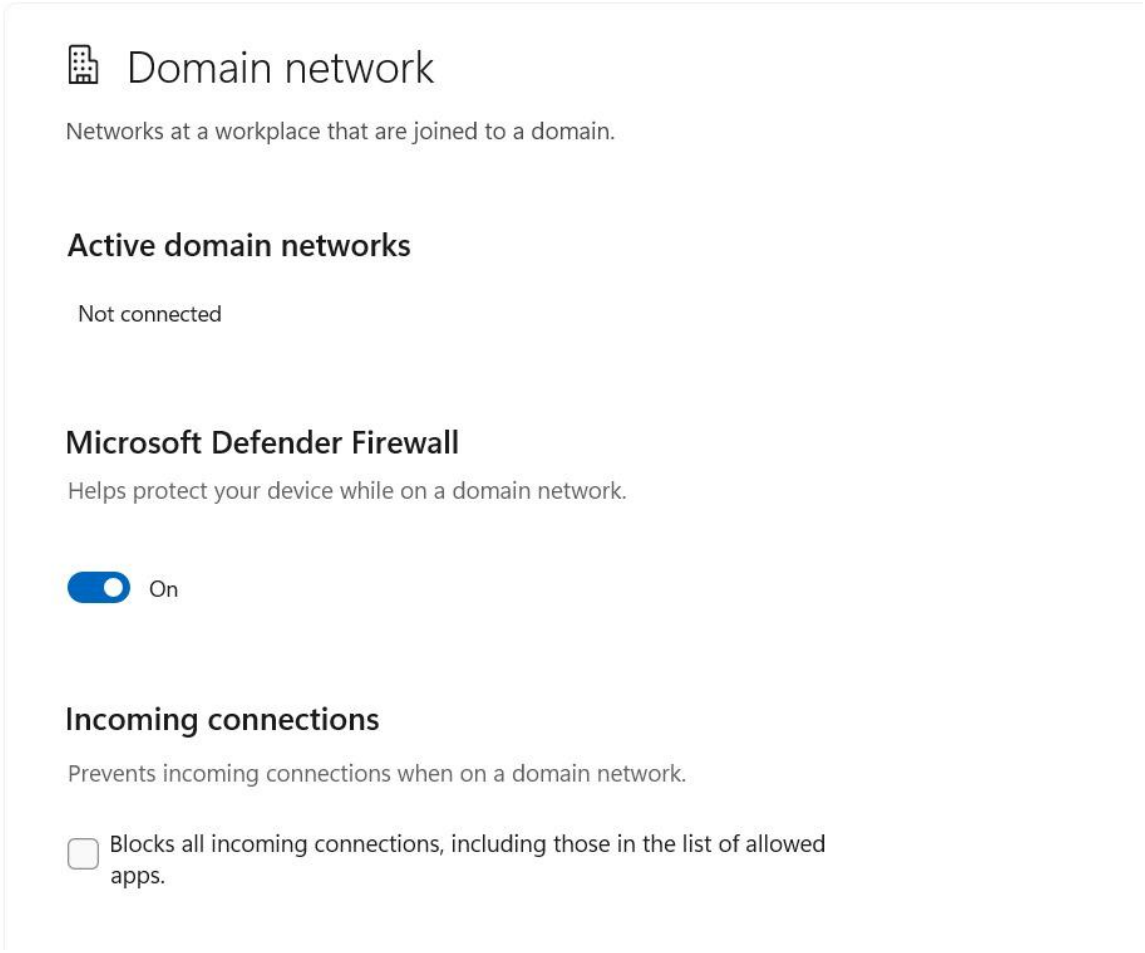



New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
23
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled
rule task 1 All Yes
AnyDesk Private Yes
AnyDesk Public Yes
AnyDesk Domain Yes
AnyDesk Private Yes
AnyDesk Domain Yes
AnyDesk Private Yes
AnyDesk Public Yes
AnyDesk Public Yes
AnyDesk Domain Yes
AnyDesk Private Yes
AnyDesk Domain Yes
AnyDesk Public Yes
Arduino IDE Public Yes
Arduino IDE Public Yes
Burp Suite Community Edition Public Yes
Burp Suite Community Edition Public Yes
Chromium Public Yes
Chromium Public Yes
Google Chrome Public Yes
Google Chrome Public Yes
mdns-discovery.exe Public Yes
mdns-discovery.exe Public Yes
Microsoft Edge Public Yes
Microsoft Edge Public Yes
ncat Public Yes
ncat Public Yes
NDI_13ed7492afdefdbda62150ba126ff9c4f... All Yes
NDI_39f328cc652c8c865a0c889f45a99480c... All Yes
NDI_a479e8aeff12034c5e11ca1f3220fce413... All Yes
NDI_bd0ac1617930e9073f0cdea75d82c76e... All Yes
Python Public Yes
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
rule task 1
Disable Rule
Cut
Copy
Delete
Properties
Help



Step 3: Change Default Router Username and Password

What I Did:

1. Logged into my router by typing its IP address (e.g., 192.168.1.1) into a browser.
2. Entered default credentials (usually admin / admin) to access settings.
3. Navigated to the **"Administration" or "System"** section.
4. Changed the **admin username and password** to something strong and unique.

Why:

- Routers often come with default login info, which attackers can easily guess.
- Changing it stops outsiders from accessing router settings remotely.

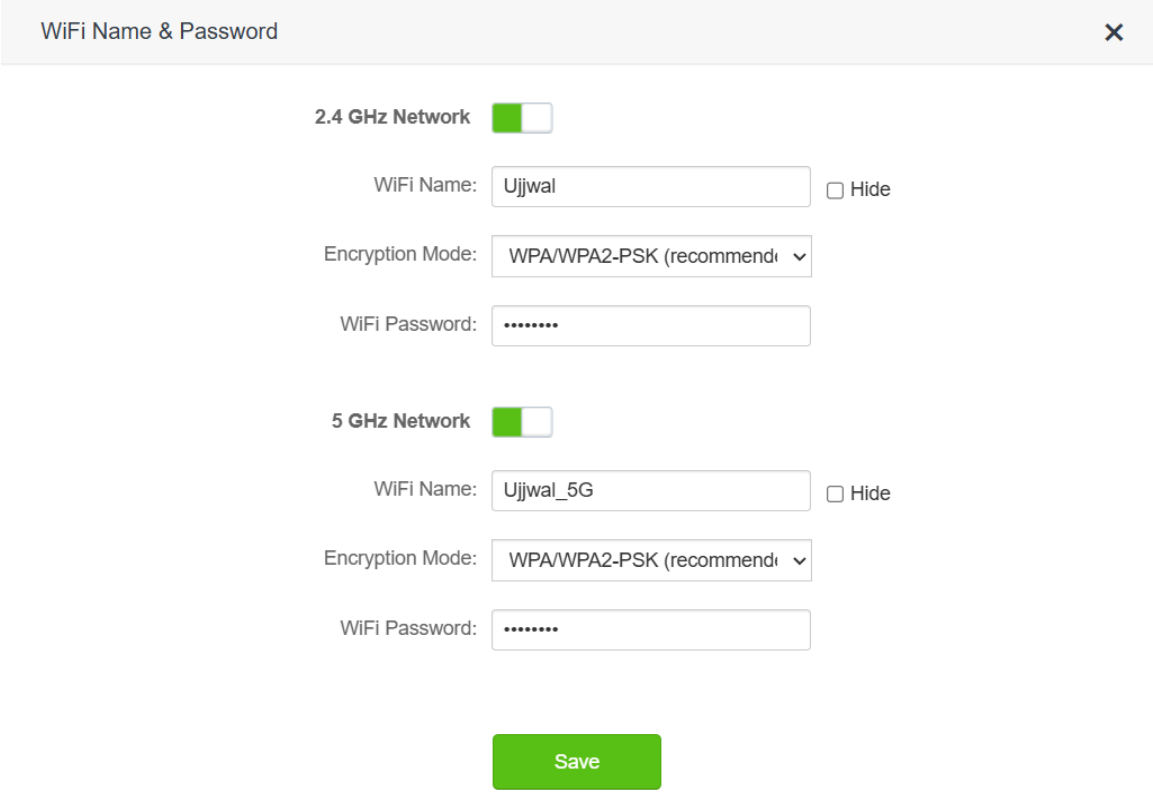
Step 4: Secure Wi-Fi with WPA3 or WPA2 Encryption

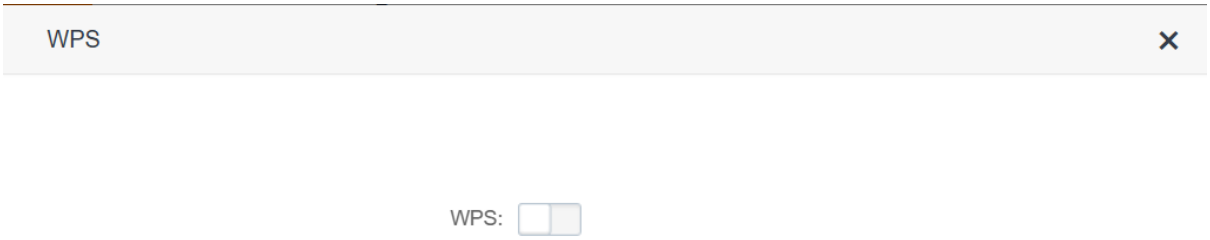
What I Did:

1. In the router settings, I went to the **Wireless Security** or **Wi-Fi Settings** tab.
2. Set the **Security Mode** to **WPA2-PSK** or **WPA3** (if available).
3. Created a **strong password** using a mix of uppercase, lowercase, numbers, and symbols.
4. Disabled **WPS (Wi-Fi Protected Setup)** if it was enabled.

Why:

- WPA2/WPA3 encrypts wireless traffic, preventing hackers from spying on data.
- Weak encryption (like WEP) can be easily cracked.





Step 5: Keep the System Updated

What I Did:

- Enabled **Windows Update** to install the latest security patches and features.
- Updated installed software and antivirus definitions.

Why:

- Many cyberattacks succeed by exploiting known vulnerabilities in outdated systems.

NETWORK TRAFFIC MONITORING USING WIRESHARK

Step 1: Installation and Setup of Wireshark

What I Did:

- Downloaded Wireshark from its official website: https://www.wireshark.org.
- Installed the software using the default settings.
- Launched Wireshark and saw a list of available **network interfaces** (e.g., Wi-Fi, Ethernet).
- Selected the **Wi-Fi interface**, since that was my active internet connection.

Why This Step Matters:

Wireshark only captures data from the network interface you select. Choosing the correct one is essential to see relevant traffic.

Step 2: Capturing Live Packet Data

What I Did:

- Clicked the **"Start Capture"** button (blue shark fin icon) on the Wi-Fi interface.
- Wireshark began listing all packets being sent or received.
- I triggered some activity by browsing websites, using ping commands, and allowing background apps to connect.

What I Saw:

Each row (packet) displayed:

- **Time**
- **Source and Destination IP addresses**
- **Protocol used (ICMP, TCP, TLS, DNS)**
- **Packet information summary**

Step 3: Analyzing Specific Protocol Traffic

Using the **"Filter"** bar, I applied filters to isolate and observe the four main protocols:

DNS (Domain Name System)

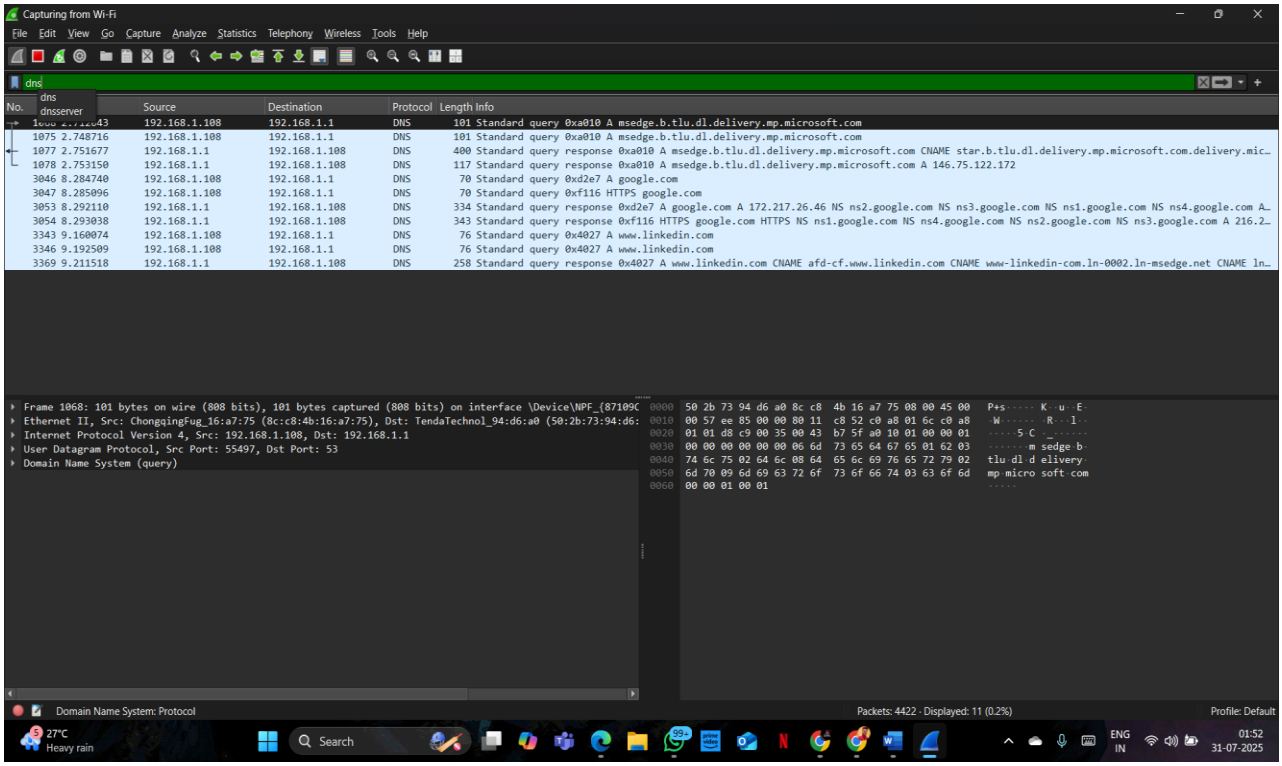
Filter used: dns

- DNS translates domain names (like example.com) into IP addresses.
- I observed that every time I opened a website, a DNS query was sent to resolve the domain name.

- The responses showed which IP addresses were returned by the DNS server.

Why It's Important:

- DNS traffic helps reveal where your system is trying to connect.
- It can also expose unusual domain lookups that may be linked to malware activity.



TCP (Transmission Control Protocol)

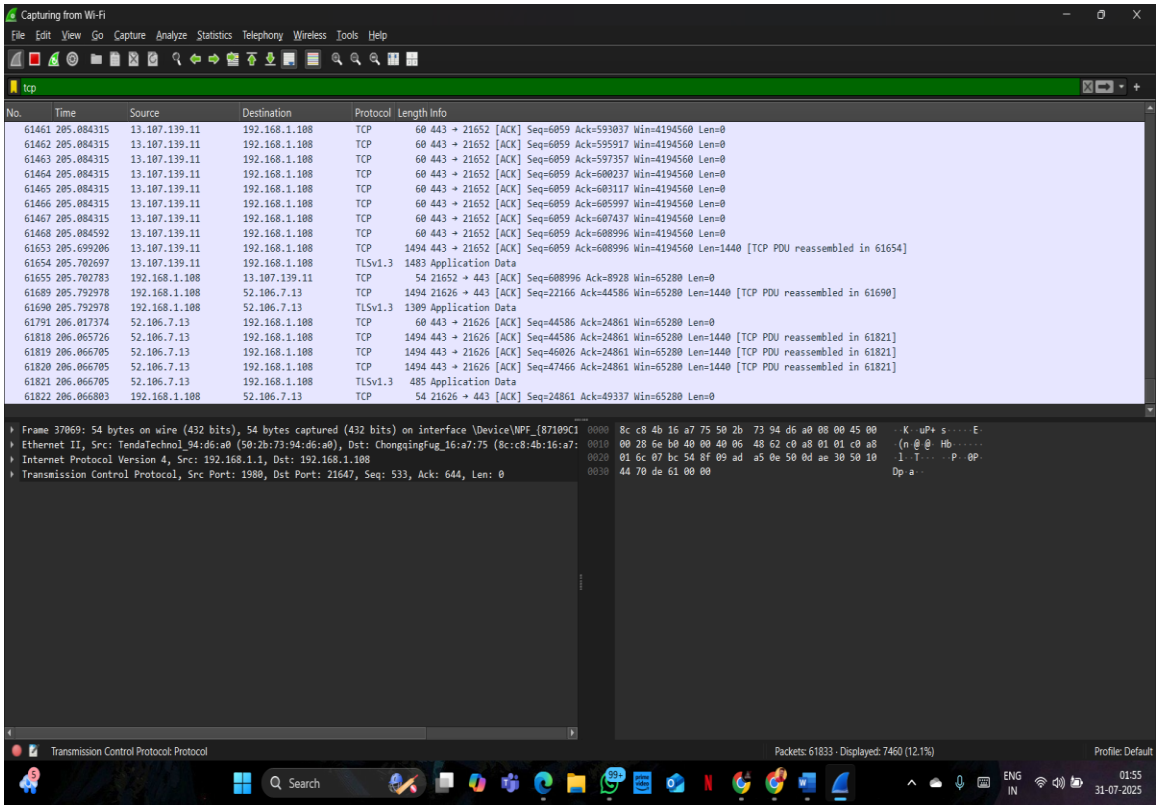
Filter used: tcp

- TCP is a connection-oriented protocol used for reliable data exchange.
- I saw the **3-way handshake** process:
    - SYN (synchronize)
    - SYN-ACK (synchronize-acknowledge)
    - ACK (acknowledge)
- This protocol was used in most communication with web servers and applications.

Why It's Important:

- TCP is the foundation of most internet communication.

- Unexpected or frequent connections to unknown IPs may indicate suspicious activity.



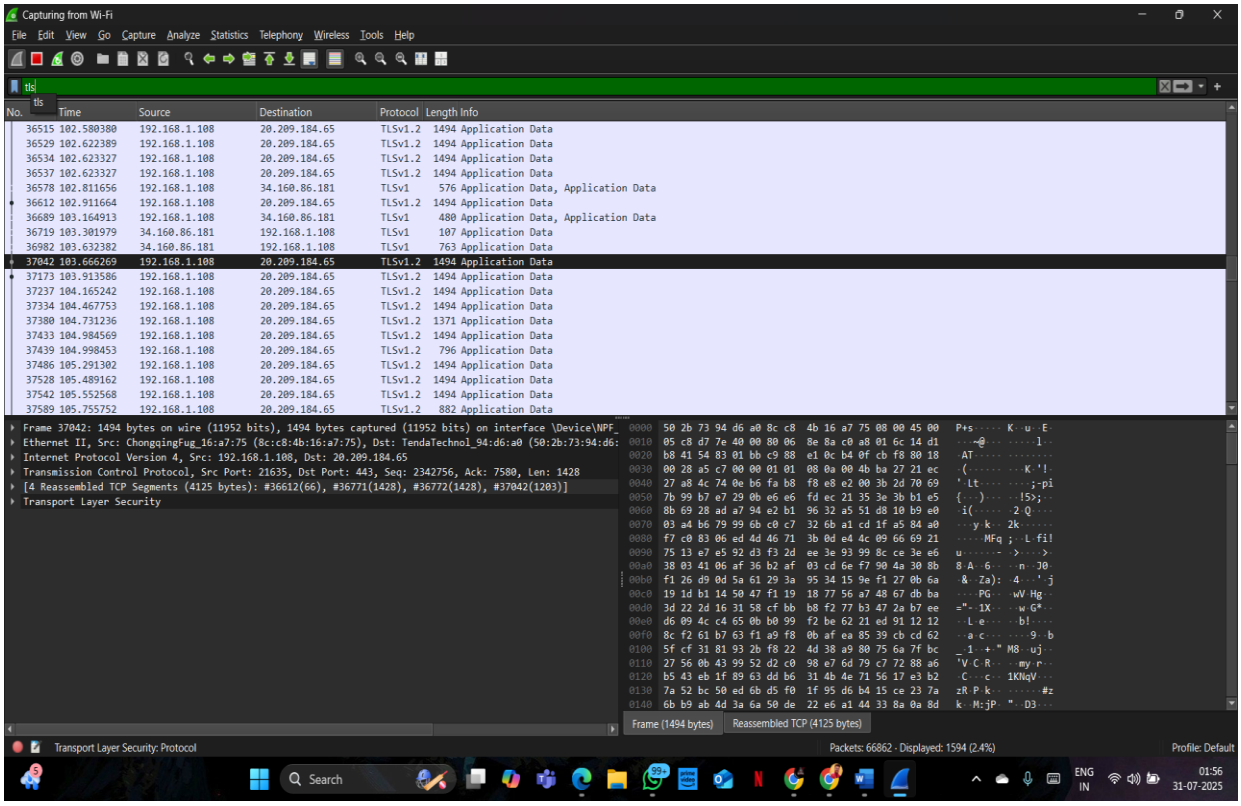
TLS (Transport Layer Security)

Filter used: tls (or ssl)

- TLS secures connections over the internet (like https:// websites).
- I was able to observe the **handshake process**, which includes:
    - Version negotiation
    - Certificate exchange
- However, the actual data is encrypted and not readable in Wireshark.

Why It's Important:

- TLS ensures that sensitive data (like passwords and personal info) is protected from interception.
- It also shows whether websites are using valid certificates.



ICMP (Internet Control Message Protocol)

Filter used: icmp

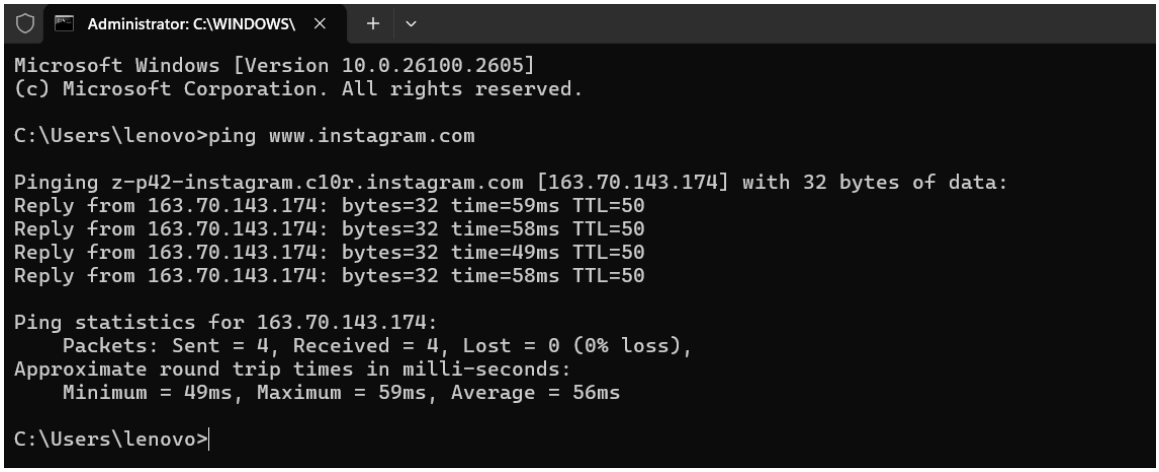
- ICMP is mainly used for diagnostic purposes, like with the ping command.
- I tested this by opening Command Prompt and typing:

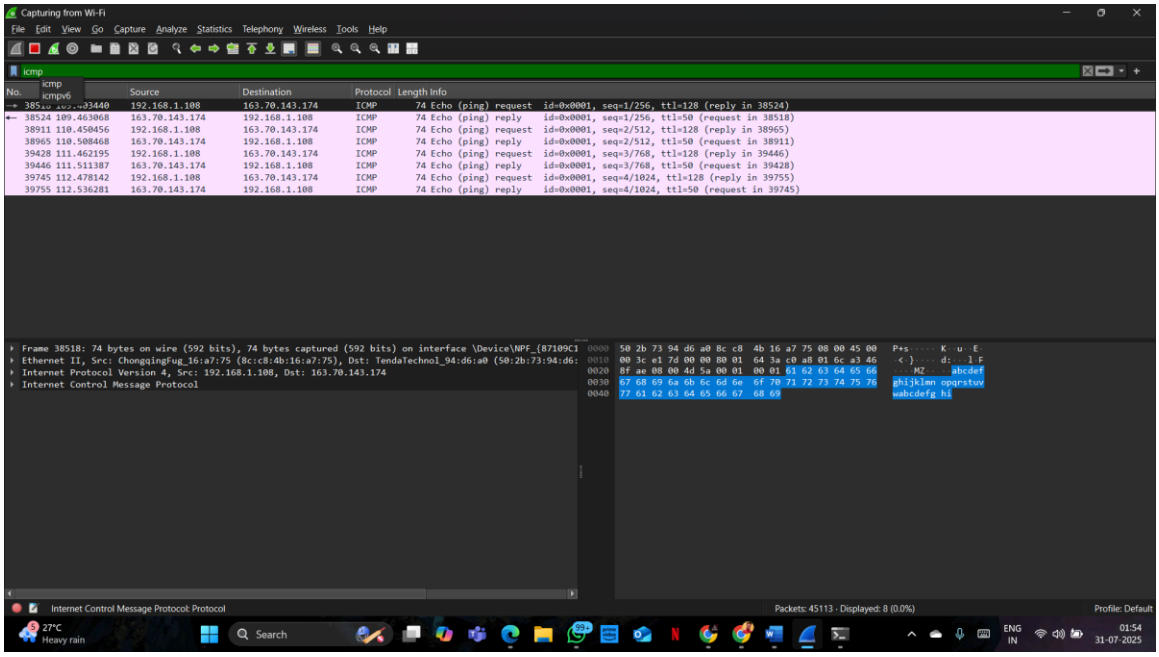
  ping www.google.com

- Wireshark displayed **Echo Request** and **Echo Reply** packets between my system and Google's server.

Why It's Important:

- ICMP can be used by administrators for troubleshooting, but attackers may also use it to map networks or perform Denial-of-Service (DoS) attacks.





Step 4: Observing Anomalies and Background Activity

To simulate basic threat detection, I observed:

- **Repeated or failed DNS queries** — which may indicate a misconfigured application or bot traffic.
- **Unusual TCP connections** to unknown or foreign IP addresses — possibly indicating tracking or hidden communication.
- **ICMP traffic without me initiating a ping** — could suggest external probing or scanning attempts.
- **TLS handshakes with unrecognized domains** — to check if any suspicious secure connections were being made.

I also noticed that **many apps generate traffic silently**, even when I'm not actively using them — highlighting how much background communication happens on modern systems.

REFLECTION AND AWARENESS

- Implement **Intrusion Detection and Prevention Systems (IDPS)** to monitor and block suspicious or malicious activities.
- Use **Network Access Control (NAC)** to ensure that only authorized devices can connect to the network.
- Set up **Virtual LANs (VLANs)** to segment traffic and isolate departments or sensitive systems.
- Deploy **internal firewalls** in addition to perimeter firewalls for layered protection.
- Enforce **Multi-Factor Authentication (MFA)** for accessing critical systems and admin panels.
- Perform **regular security audits and penetration testing** to proactively find and fix weaknesses.
- Use **automated tools** to apply security patches and updates across devices.
- Conduct **cybersecurity awareness training** for all staff to minimize human error and social engineering risks.

EDUCATING OTHERS ABOUT THE IMPORTANCE OF NETWORK SECURITY

- Use everyday examples (like locking doors) to explain the need for digital security.
- Emphasize that **cybersecurity is everyone's responsibility**, not just a technical team's job.
- Promote simple habits:
    - Creating **strong, unique passwords**
    - **Avoiding unknown links and downloads**
    - Keeping **software and antivirus up to date**
- Share real-world consequences of poor security, such as identity theft or data loss.

- Encourage awareness of **safe internet behaviour** both at home and in the workplace.

Report Submitted To: REDYNOX BY THE RED USER