# The Red Users Internship - TASK 1

By Himanshu Gandhi

Himanshukamboj135@gmail.com

- **Introduction to Network Security**

Network security encompasses practices, policies, and procedures to protect the integrity, confidentiality, and availability of network and data resources. As networks grow more complex and interconnected, the need for effective security measures becomes essential to defend against various cyber threats. This introductory report covers the basic principles, common network threats, and best practices for securing a small network.

- **Types of Network Threats**

To effectively secure a network, it's critical to understand the various types of threats that can compromise network resources. Common network threats include:

- **Malware:** Malicious software such as viruses, worms, ransomware, and spyware can infiltrate a network and compromise systems. Malware often spreads through infected files, links, or attachments, causing data loss, system corruption, and unauthorized data access.
- **Phishing Attacks:** In phishing, attackers trick users into providing sensitive information (such as passwords or credit card details) by impersonating trusted entities, often through deceptive emails or fake websites.
- **Denial-of-Service (DoS) Attacks:** DoS attacks overwhelm network resources with excessive traffic, rendering services inaccessible to legitimate users. Distributed Denial-of-Service (DDoS) attacks, a variation of DoS, utilize multiple compromised systems to amplify the attack's impact.
- **Man-in-the-Middle (MitM) Attacks:** In MitM attacks, attackers intercept and potentially alter communications between two parties without their knowledge, compromising the confidentiality and integrity of the information exchanged.

- **SQL Injection:** SQL injection attacks exploit vulnerabilities in web applications by inserting malicious SQL code into input fields. This can grant attackers unauthorized access to databases, allowing them to retrieve, alter, or delete data.
- **Password Attacks:** Brute-force and dictionary attacks attempt to guess or crack passwords to gain unauthorized access to network resources. Weak or reused passwords are particularly vulnerable to these types of attacks.

- **Basic Security Measures**

Implementing basic security measures is essential for protecting a small network from these threats. Here are some foundational security practices:

- **Firewalls:** Firewalls act as a barrier between a trusted network and external threats. Configuring firewall rules to block unauthorized access and filter incoming and outgoing traffic is crucial for preventing intrusion.
- **Antivirus Software:** Regularly updating antivirus software helps detect and remove malware before it can spread throughout the network. Antivirus programs scan files, emails, and other network resources for signs of infection.
- **Network Segmentation:** Segmenting a network into smaller sub-networks (or zones) can help contain threats and limit the potential damage in the event of a breach. Sensitive data can be isolated within secure zones accessible only to authorized users.
- **Strong Authentication Practices:** Implementing multi-factor authentication (MFA) requires users to provide two or more forms of verification before gaining access to network resources. This practice reduces the risk associated with compromised credentials.
- **Regular Updates and Patching:** Ensuring all devices and software within the network are regularly updated and patched reduces vulnerabilities that attackers could exploit.
- **Employee Training and Awareness:** Educating users about network security best practices (e.g., identifying phishing emails, choosing

strong passwords) is vital. Human error often plays a significant role in network breaches, and informed employees can help prevent attacks.

- **Understand about firewall**

A firewall is a critical component of network security, acting as a barrier that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls help to protect networks by blocking potentially harmful data while allowing legitimate traffic through, thus preventing unauthorized access to network resources.

**1. Purpose of Firewalls**

The primary purpose of a firewall is to create a protective boundary between a trusted internal network and untrusted external networks, such as the internet. By filtering traffic, a firewall helps prevent cyber threats, data breaches, and unauthorized access to private data.

**2. Types of Firewalls**

There are several types of firewalls, each serving specific security needs:

- Packet-Filtering Firewalls: The simplest form of firewall, packet-filtering firewalls examine packets (small data segments) that are sent over the network. They analyze packet headers (source and destination IPs, ports, and protocol types) and allow or deny them based on established rules. This type of firewall is fast but limited in scope since it doesn't inspect the packet content itself.
- Stateful Inspection Firewalls: These firewalls monitor the state of active connections and make filtering decisions based on the context of the traffic (e.g., whether a packet is part of an established session or a new request). Stateful firewalls are more secure than packet-filtering firewalls as they consider traffic flow and allow packets only if they are part of legitimate sessions.
- Proxy Firewalls (Application Gateways): Acting as intermediaries between users and internet resources, proxy firewalls filter traffic at the application level. They inspect packet contents, not just headers, which allows for more detailed filtering and threat detection, especially for web and email traffic.

- Next-Generation Firewalls (NGFWs): NGFWs combine traditional firewall capabilities with advanced features like intrusion prevention systems (IPS), deep packet inspection, and application awareness. These firewalls can identify specific applications (e.g., Facebook, Skype) rather than just protocols, making them highly effective against modern threats.
- Unified Threat Management (UTM) Firewalls: UTMs are all-in-one security solutions that integrate firewall, antivirus, content filtering, intrusion prevention, and more. They're commonly used in small to medium-sized businesses for simplicity and cost-efficiency.

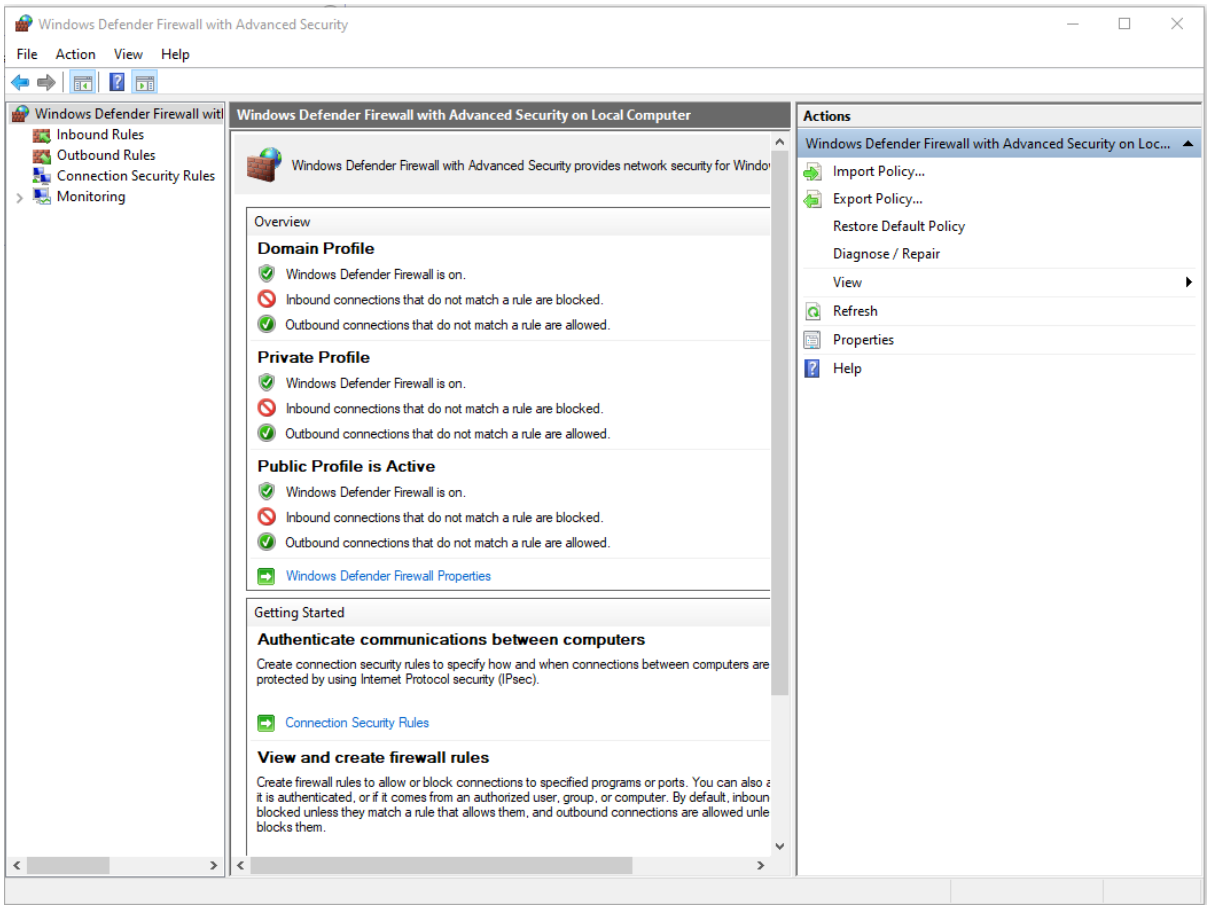
**3. How Firewalls Work**

Firewalls operate based on rules, filters, and policies that define which types of traffic are permitted or denied:

- Access Control Lists (ACLs): ACLs are sets of rules that specify whether to allow or deny traffic based on source/destination IP addresses, ports, and protocols. An organization's IT administrators typically set up these lists based on security requirements.
- Content Filtering: Firewalls can block or allow traffic based on its content, such as specific URLs or keywords. This capability is especially useful for filtering out harmful or inappropriate websites in business or educational environments.
- Traffic Logging and Alerts: Firewalls log traffic data for analysis and can be set to alert administrators about suspicious activities. Logs provide valuable insights into potential threats and are often essential in identifying attack patterns.
- **Firewall Configuration**

**1. Open Windows Firewall Settings**

1. **Access the Control Panel:**
    - Press Windows Key + S to open the search bar.
    - Type "Control Panel" and open it.
    - Select System and Security, then click Windows Defender Firewall.

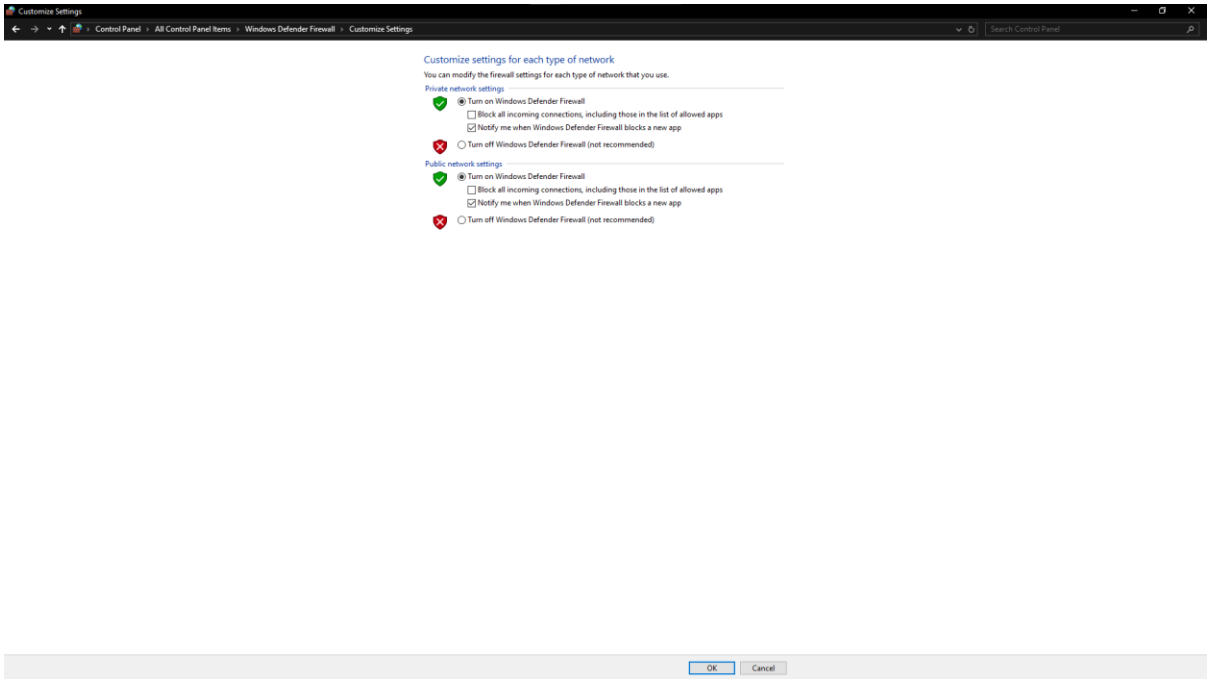



2. **Alternative Method via Settings (Windows 10/11):**
    - Go to Settings (Windows Key + I).
    - Choose Update & Security > Windows Security > Firewall & network protection.

---

## 2. Turn Windows Firewall On or Off

1. In the Windows Defender Firewall window, select Turn Windows Defender Firewall on or off from the left sidebar.




2. You'll see options for Private network settings and Public network settings:
    - Select Turn on Windows Defender Firewall under both network types for maximum protection.
    - Click OK to save changes.

---

### 3. Allow or Block Specific Apps

1. From the Windows Defender Firewall main screen, select Allow an app or feature through Windows Defender Firewall.
2. Click Change settings (admin privileges may be required).
3. Check the box next to the app you want to allow through the firewall for Private or Public network types as needed.
    - To block an app, uncheck the box beside it.
4. Click OK to apply changes.

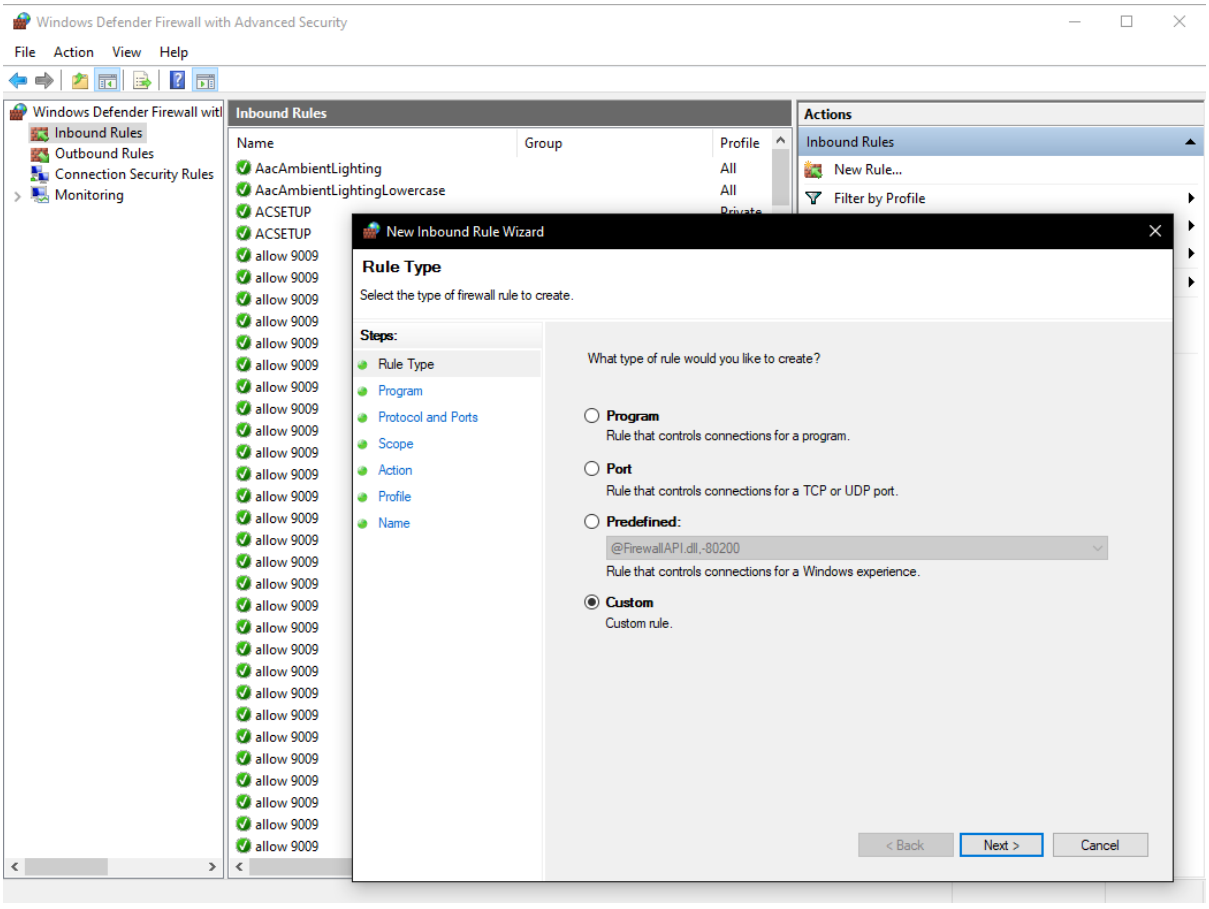
---

### 4. Configure Inbound and Outbound Rules

1. Open Advanced Settings:

- In the Windows Defender Firewall window, click Advanced settings in the left sidebar. This opens the Windows Firewall with Advanced Security console.

2. Create a New Inbound Rule:
    - In the console, right-click Inbound Rules on the left and select New Rule....
    - Choose the rule type (e.g., Port for port-based rules, Program for specific apps).




    - Define the rule specifics:
        - Program: Choose the path of the executable you want to allow or block.
        - Port: Specify the port number (e.g., 80 for HTTP, 443 for HTTPS) and protocol (TCP or UDP).

- Select Allow the connection or Block the connection based on your security needs.
- Apply the rule to Domain, Private, or Public profiles as required.
- Name the rule and click Finish.

3. **Create Outbound Rules (optional):**
   - Repeat the same steps under Outbound Rules to control outgoing traffic.

---

**5. Set Firewall Notifications**

1. Go to Advanced settings > Properties.
2. Under each profile (Domain, Private, Public), you can configure firewall notifications:
   - Under the Settings section, set Display a notification to "Yes" if you want to be alerted each time the firewall blocks a new app.
   - Click OK to save.

---

**6. Enable Logging for Troubleshooting**

1. In Advanced settings, right-click Windows Defender Firewall with Advanced Security on Local Computer and choose Properties.
2. Under the Logging tab:
   - Select Customize next to Logging settings.
   - Enable Log dropped packets and Log successful connections to monitor traffic for blocked and allowed connections.
3. Define a log file size and path if needed, then click OK.

- **Capturing Packet Using Wireshark**

**Wireshark** is a powerful, open-source network protocol analyzer used to capture and inspect network traffic in real time. It helps network

administrators, cybersecurity professionals, and developers troubleshoot network issues, analyze performance, and detect security vulnerabilities.

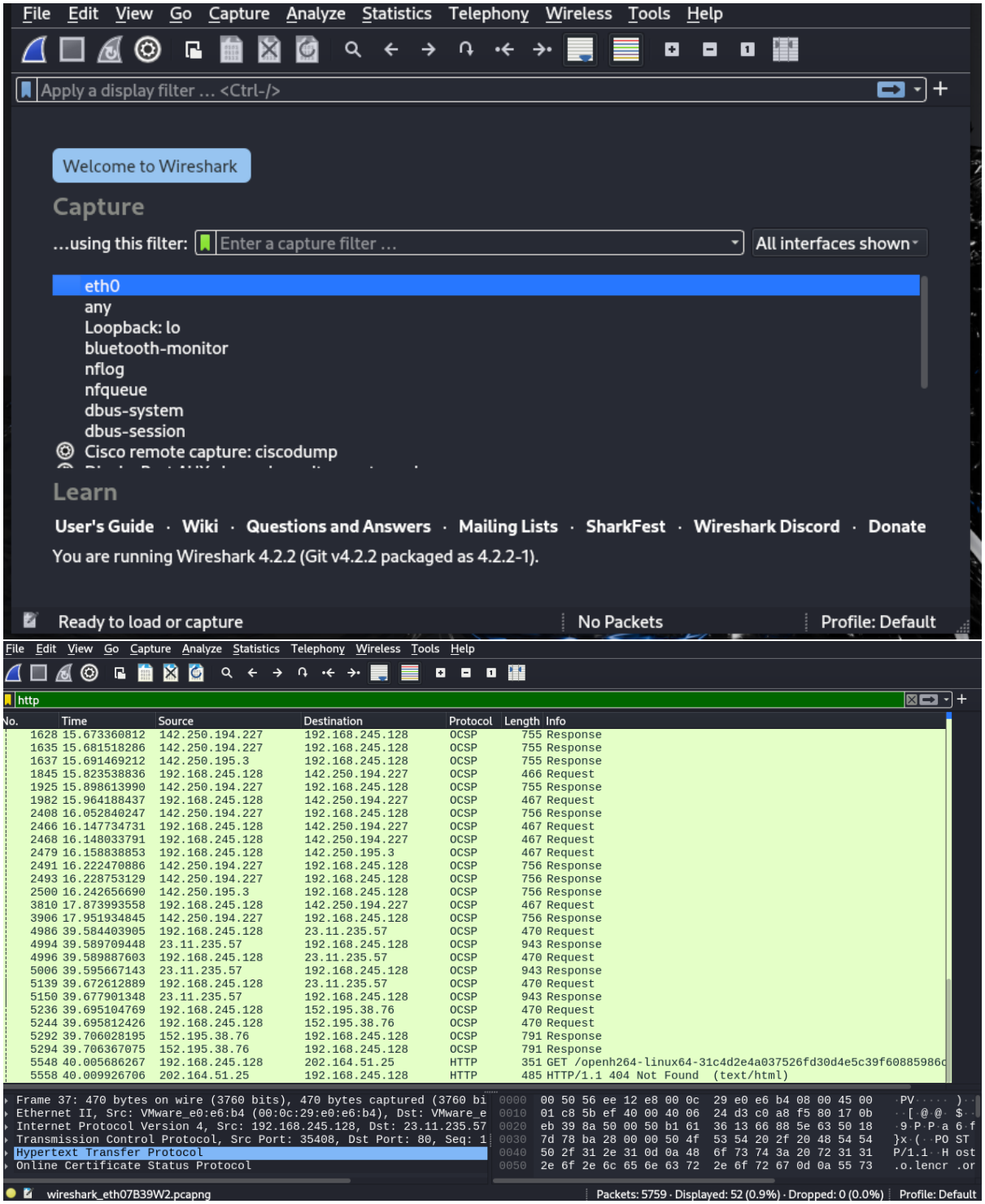
**Key Features of Wireshark**

1. **Packet Capture**: Wireshark captures packets (data units sent across a network) at a very detailed level, allowing users to examine individual packets and understand their contents, source, destination, and protocols used.
2. **Protocol Analysis**: Wireshark supports analysis of hundreds of protocols (e.g., HTTP, TCP, DNS, SSL/TLS) and can decode packets to show protocol details. This is useful for understanding how different services and applications communicate.
3. **Real-Time Network Monitoring**: Users can monitor live traffic on their network interface, providing a real-time view of network activity, which is helpful for troubleshooting and performance tuning.
4. **Filtering and Search Capabilities**: Wireshark has robust filtering options, allowing users to search for specific packet types, IP addresses, ports, or protocols, which simplifies the process of finding relevant data within large captures.
5. **Color-Coding and Visualization**: Different types of traffic and protocols can be color-coded to quickly identify key information. Wireshark also offers graphical tools for visualizing network data flow and performance.
6. **Packet Export and Analysis**: Captured data can be saved in various formats for later analysis. This feature is helpful for reviewing network events over time or sharing data with other analysts.

**Common Uses of Wireshark**

- **Network Troubleshooting**: Identifying issues such as connectivity problems, slow network performance, and dropped packets.
- **Security Analysis**: Detecting malicious activity or unauthorized access attempts, analyzing suspicious packets, and finding vulnerabilities.

- **Protocol Development**: Analyzing protocol performance and behavior, which is valuable for developers creating network applications.
- **Educational Tool**: Learning how data is transmitted across networks and how protocols interact, making it popular in IT and cybersecurity education.



**1. Install and Launch Wireshark**

- Download Wireshark from wireshark.org if you haven't already.
- Install the program, and open Wireshark.

---

**2. Select a Network Interface to Capture From**

1. Upon opening Wireshark, you'll see a list of available network interfaces on your computer (such as Ethernet, Wi-Fi, etc.).
2. Choose the interface you want to capture traffic from. For example, if you're on a Wi-Fi network, select the **Wi-Fi** interface.
3. (Optional) Double-check you've selected the correct interface by looking at the real-time graph showing network activity next to each interface.

---

**3. Start the Packet Capture**

1. After selecting the interface, click on the **Shark Fin (green button)** at the top left or press **Ctrl + E** to start capturing packets.
2. Wireshark will begin to capture packets in real time, and you'll see them displayed in the main window as they're captured.

---

**4. Apply Filters (Optional)**

1. To focus on specific traffic, you can apply **display filters**. Enter a filter in the "Filter" bar (e.g., http for HTTP traffic, tcp for TCP traffic, or an IP address to capture packets to or from a specific host).
2. Click **Apply** to activate the filter.

---

**5. Stop the Packet Capture**

1. When you have enough data, stop the capture by clicking the **Red Square (stop button)** at the top or pressing **Ctrl + E** again.

2. Wireshark will halt capturing, allowing you to review the packets in the capture window.

---

**6. Save the Captured Packets (Optional)**

1. To save the captured packets, go to **File > Save As**.
2. Choose a file location and format (typically .pcap or .pcapng), and click **Save**.