

NETWORK SECURITY ASSIGNMENT 4

Team Members:

1. Sneha Mazumder - 220905069
2. Venkatesh Durai - 220905253

GitHub Link:

<https://github.com/vxnkt/Wireshark-Implementation/tree/main>

Wireshark

Wireshark is a powerful and widely used open-source network protocol analyzer that enables users to capture and interactively browse the traffic running on a computer network.

Operating by capturing packets of data as they travel through a network interface, Wireshark provides a real-time or saved view of network activity, complete with filtering and deep packet analysis capabilities.

As an open-source tool, it is freely available and continuously improved by a global community of contributors. **Wireshark plays a crucial role in network security by helping identify suspicious traffic, diagnose network performance issues, detect intrusions, and analyze vulnerabilities.** Through its intuitive graphical interface and powerful features, it enables a deeper understanding of network behavior, thereby enhancing the overall security and reliability of networked systems.

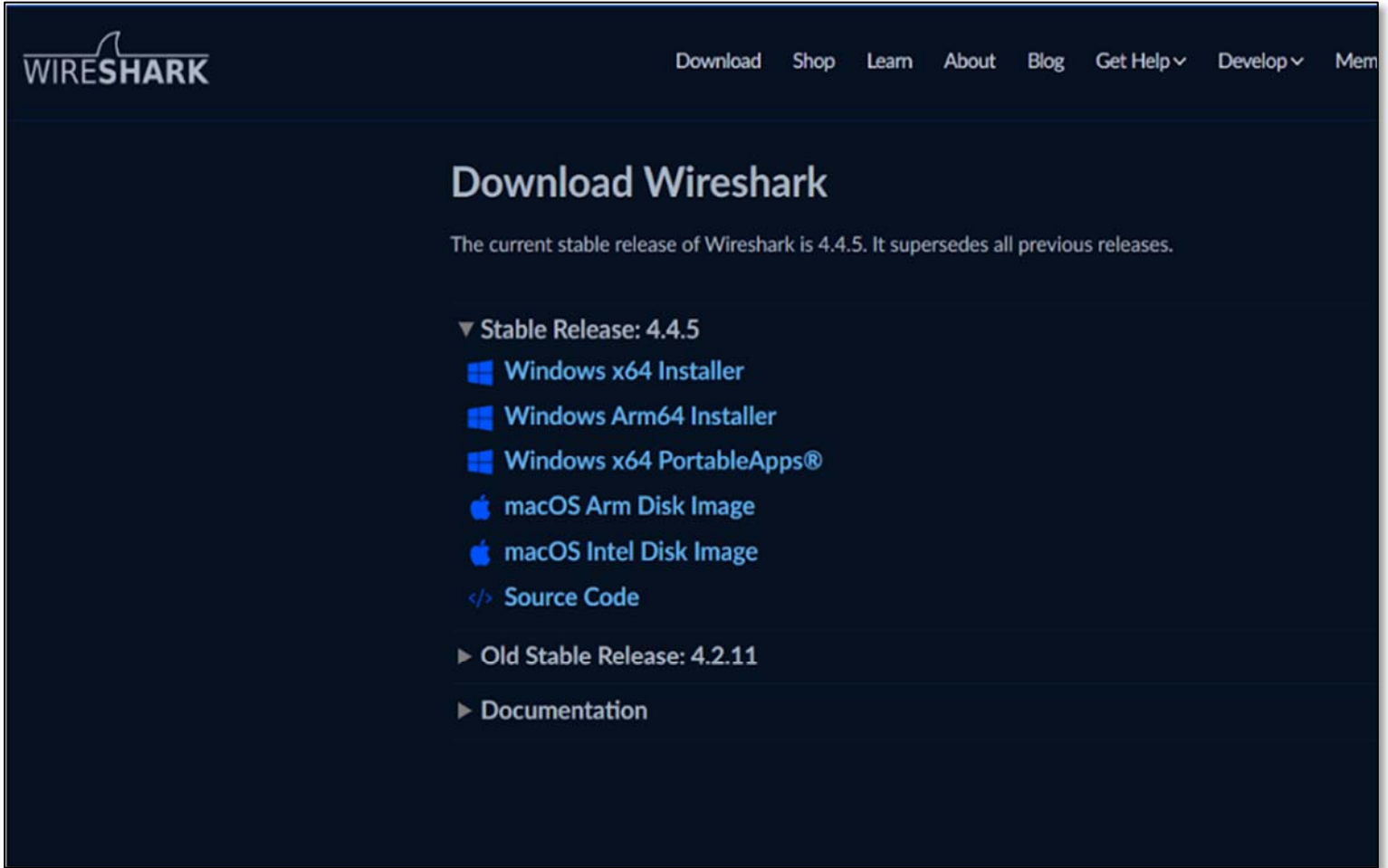
We chose to explore and report on Wireshark because it is one of the most widely used tools for network analysis and security. Its open-source nature, real-time packet capturing, and detailed protocol inspection make it an ideal tool for understanding how data flows through a network and identifying potential threats.

Key features such as deep packet inspection, customizable filters, and live traffic analysis allow users to detect suspicious behavior, diagnose issues, and strengthen overall network security. This directly relates to the knowledge gained in the Coursera course "*Connect and Protect: Networks and Network Security*," where we learned about how data travels across networks, common vulnerabilities, and the importance of monitoring tools.

Wireshark brought those concepts to life, offering hands-on experience with the principles covered in the course and helping bridge the gap between theory and practical application.

Download

Go to <https://www.wireshark.org/download.html> and on one of the stable releases according to your system OS. For this demo we installed the “Windows x64 Installer”



The screenshot shows the Wireshark website's download page. At the top, the Wireshark logo is on the left, and a navigation menu with links for Download, Shop, Learn, About, Blog, Get Help, Develop, and Mem is on the right. The main heading is "Download Wireshark". Below it, a message states: "The current stable release of Wireshark is 4.4.5. It supersedes all previous releases." A dropdown menu is open under "Stable Release: 4.4.5", showing options: "Windows x64 Installer" (with a Windows logo), "Windows Arm64 Installer" (with a Windows logo), "Windows x64 PortableApps®" (with a Windows logo), "macOS Arm Disk Image" (with an Apple logo), "macOS Intel Disk Image" (with an Apple logo), and "Source Code" (with a code icon). Below this, there are links for "Old Stable Release: 4.2.11" and "Documentation".

WIRESHARK

Download Shop Learn About Blog Get Help ▾ Develop ▾ Mem

Download Wireshark

The current stable release of Wireshark is 4.4.5. It supersedes all previous releases.

▼ Stable Release: 4.4.5

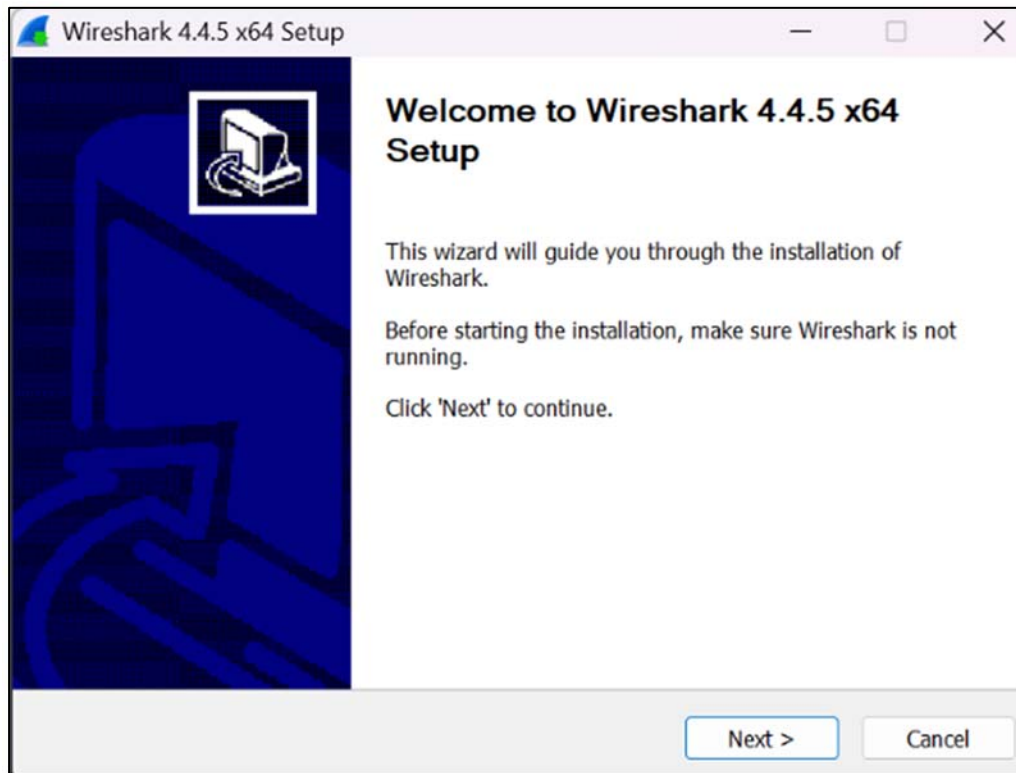
- Windows x64 Installer
- Windows Arm64 Installer
- Windows x64 PortableApps®
- macOS Arm Disk Image
- macOS Intel Disk Image
- Source Code

► Old Stable Release: 4.2.11

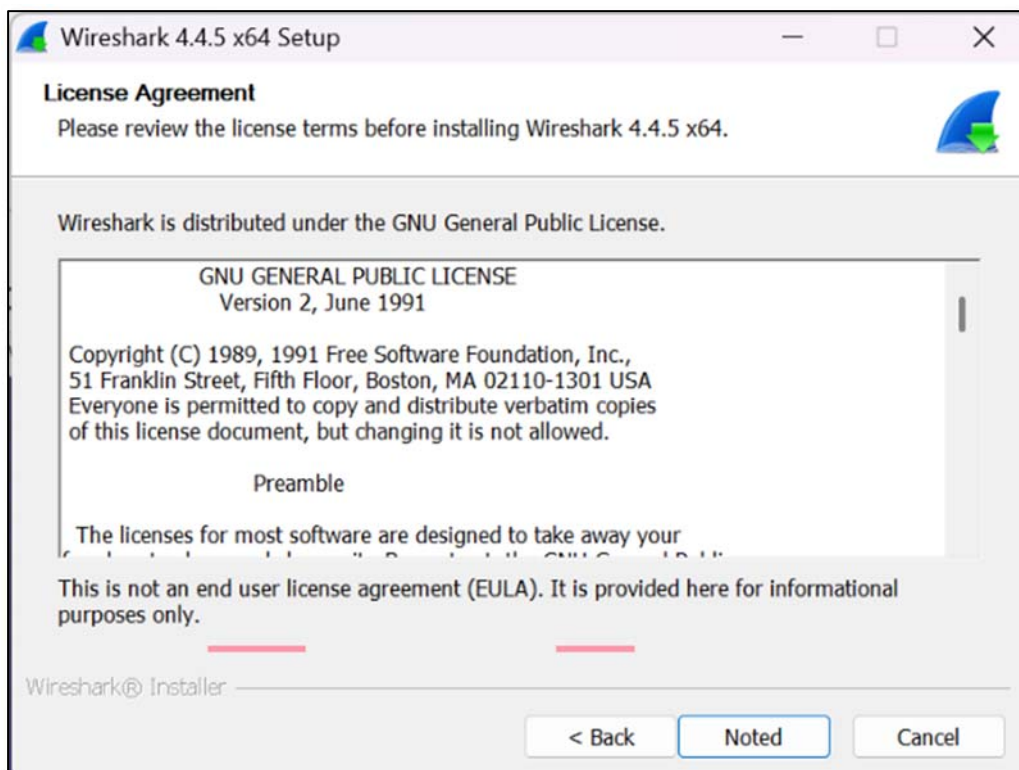
► Documentation

Setup

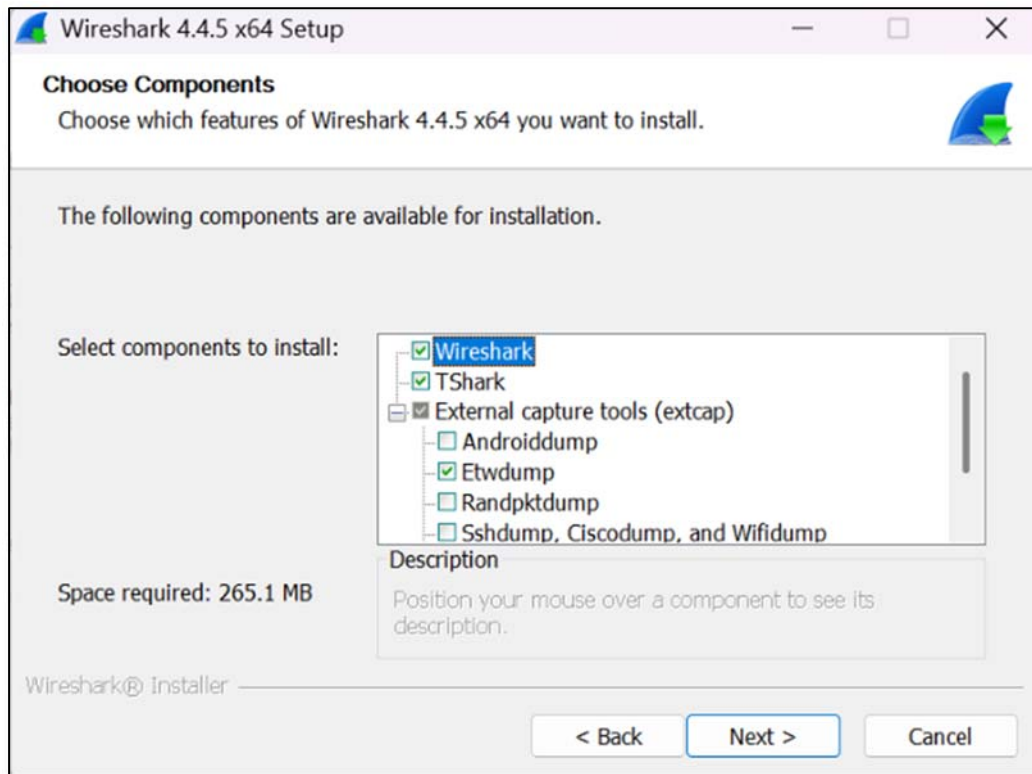
This is the first window that pops up during installation.



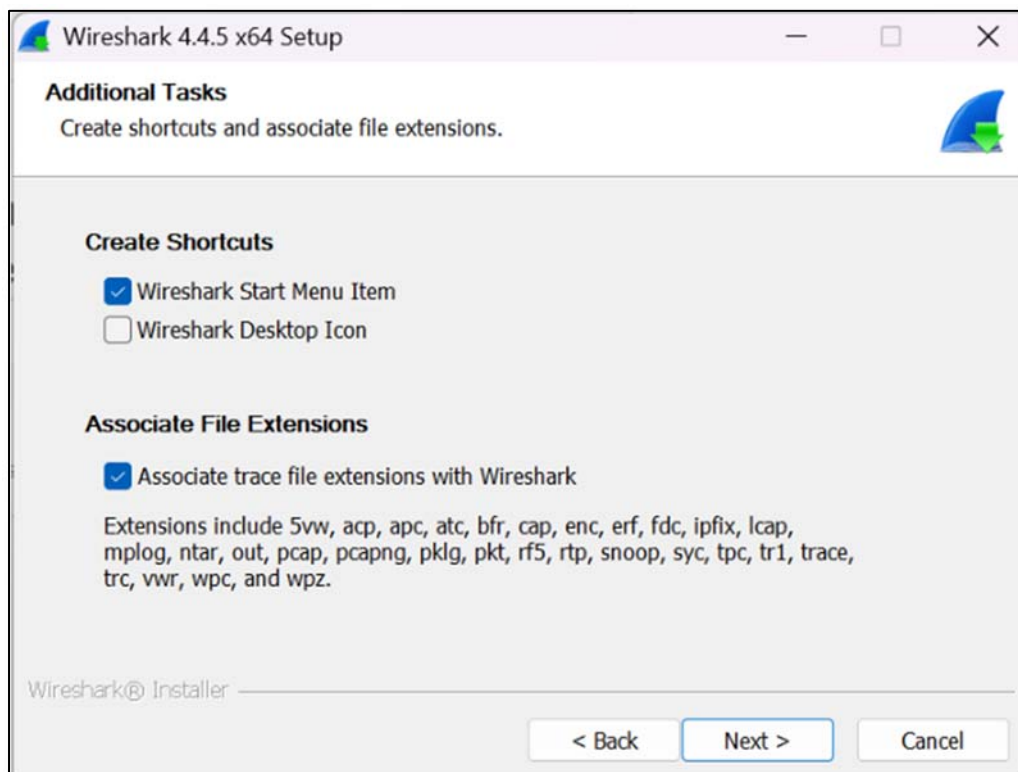
Click next.



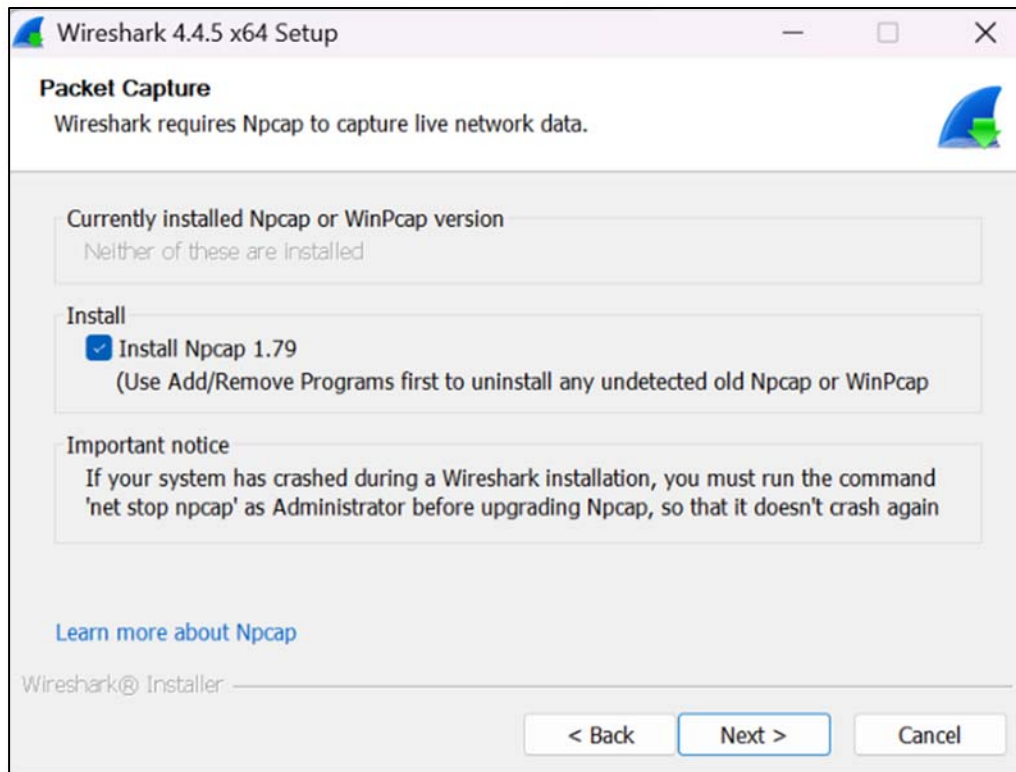
After reading license agreement, click noted.
Continue with the setup.



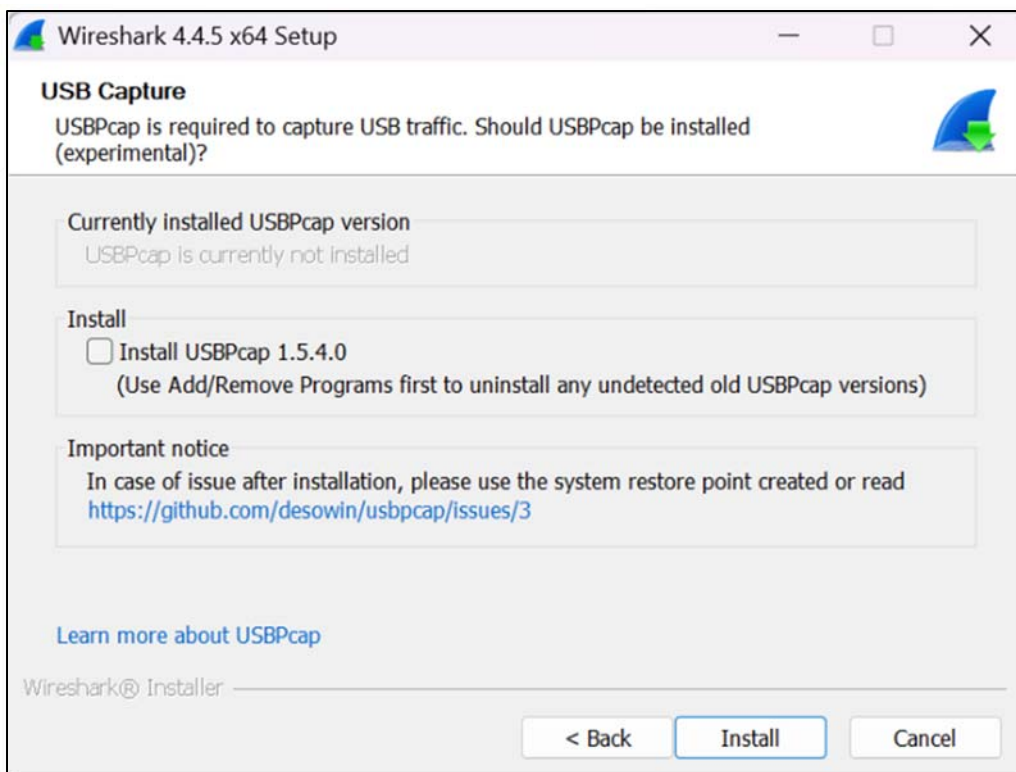
Leave it as it is and click next for default installation.



Continue with installation, choose an install location and click next.



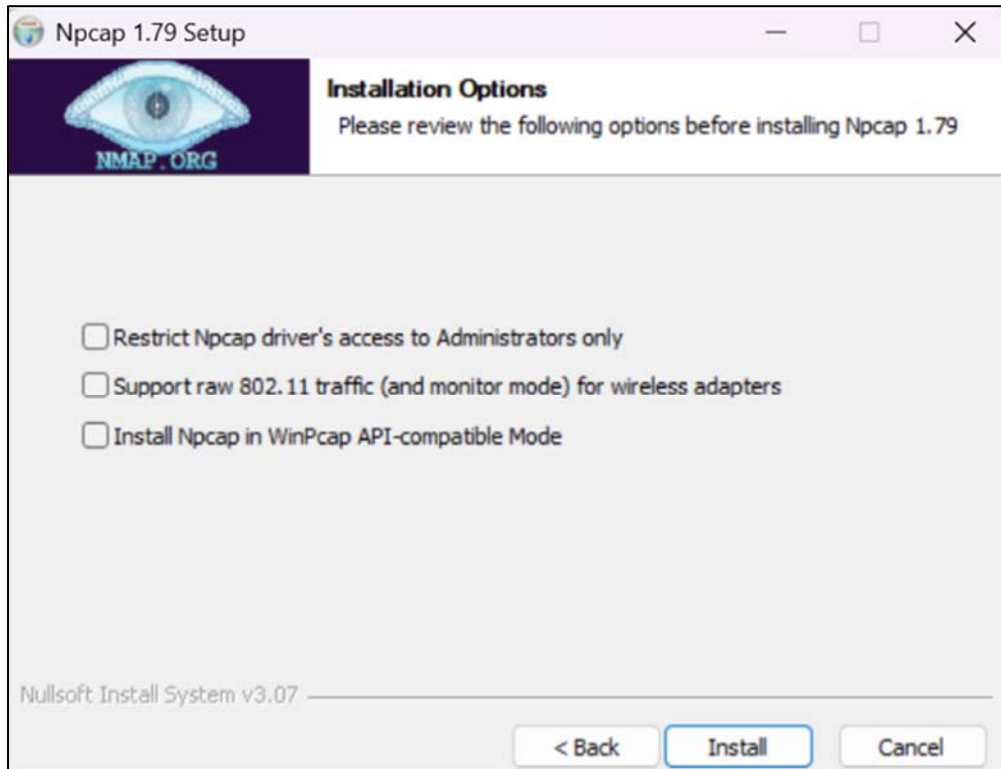
This is to capture packets, which is important so let it be and it will get installed automatically. Continue with the installation by clicking next.



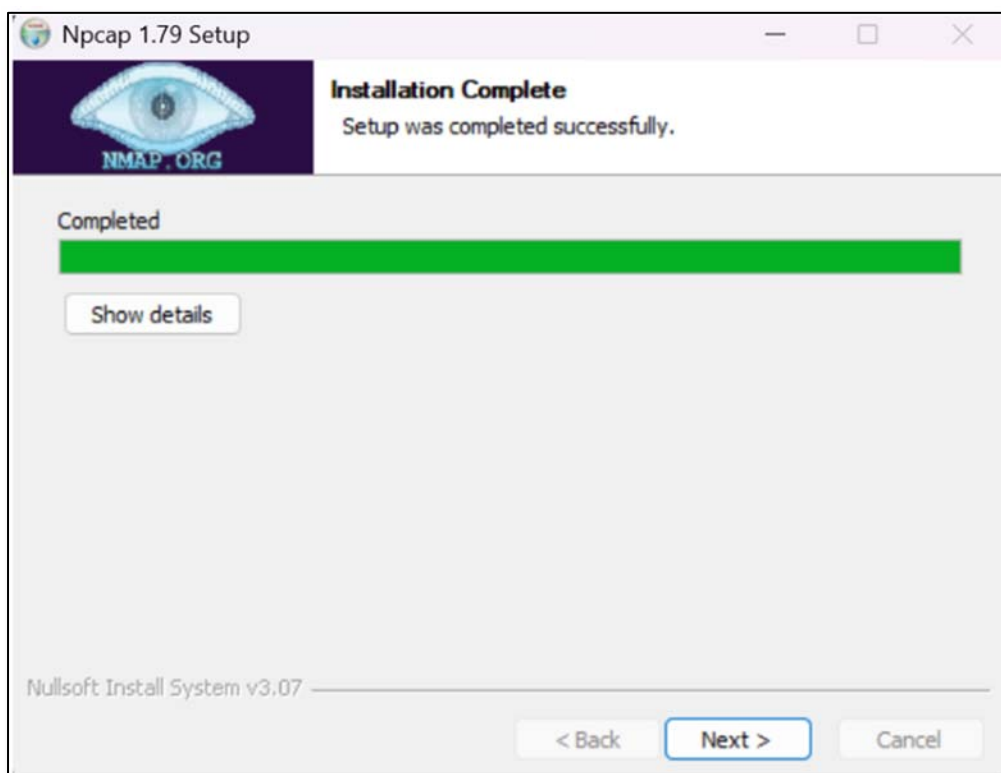
This is to capture USB traffic.

For this demonstration, we did not install USBcap and proceeded with the installation.

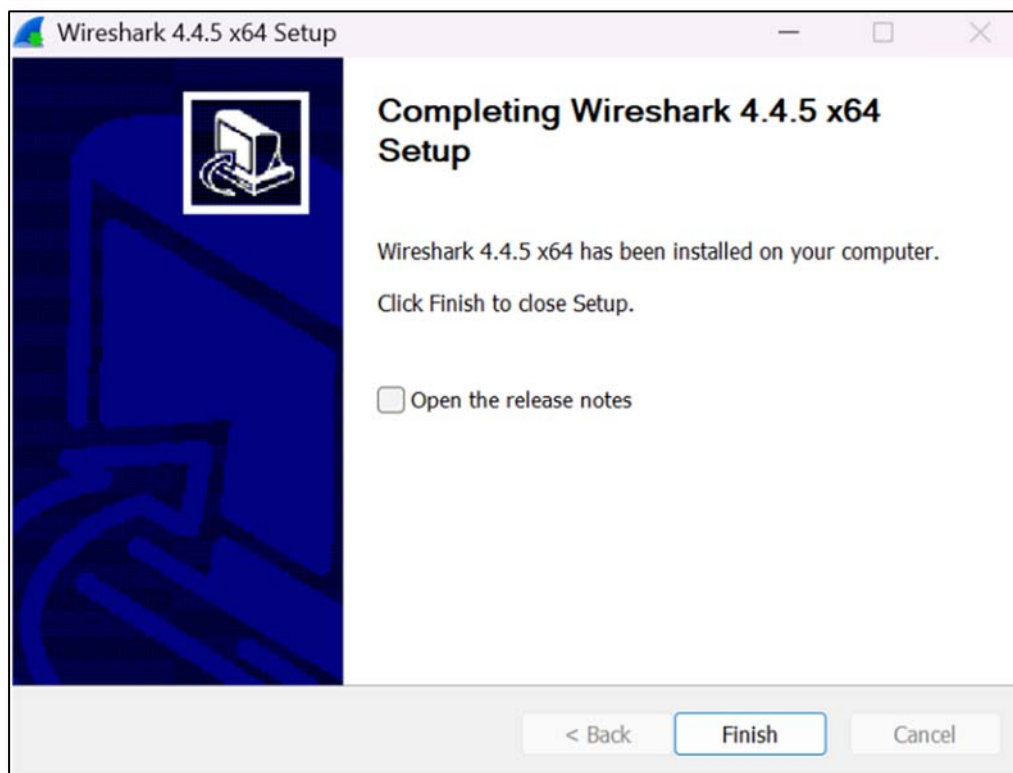
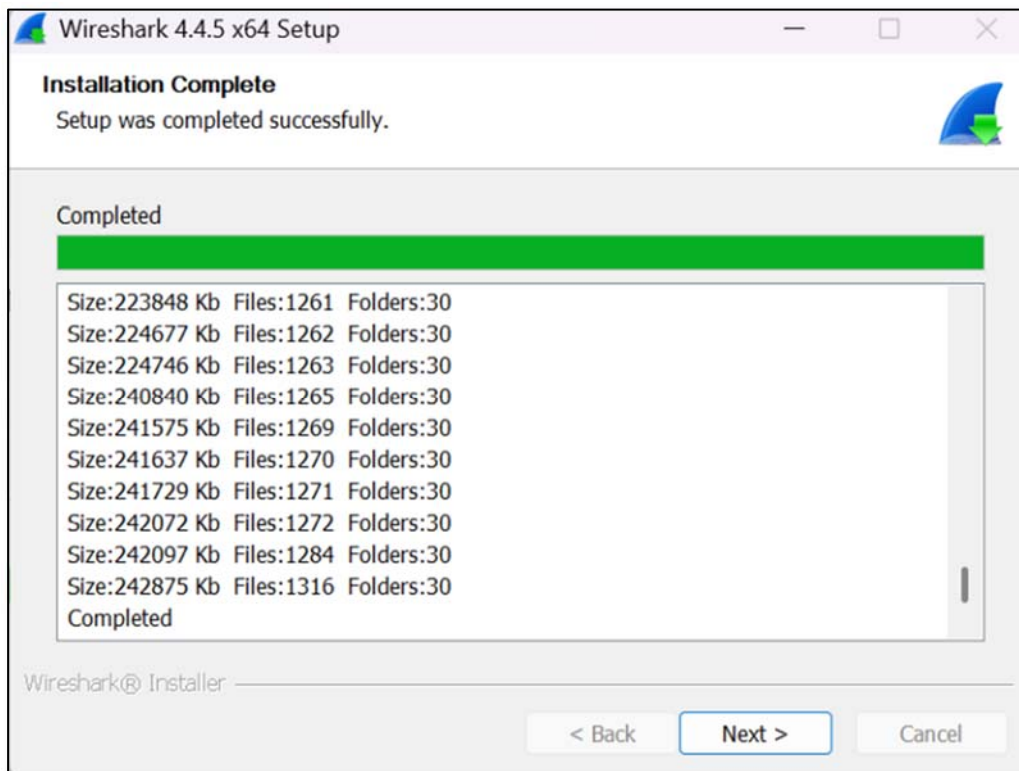
While installing, Npcap installation will also start.



Just proceed with default installation by clicking “Install”.



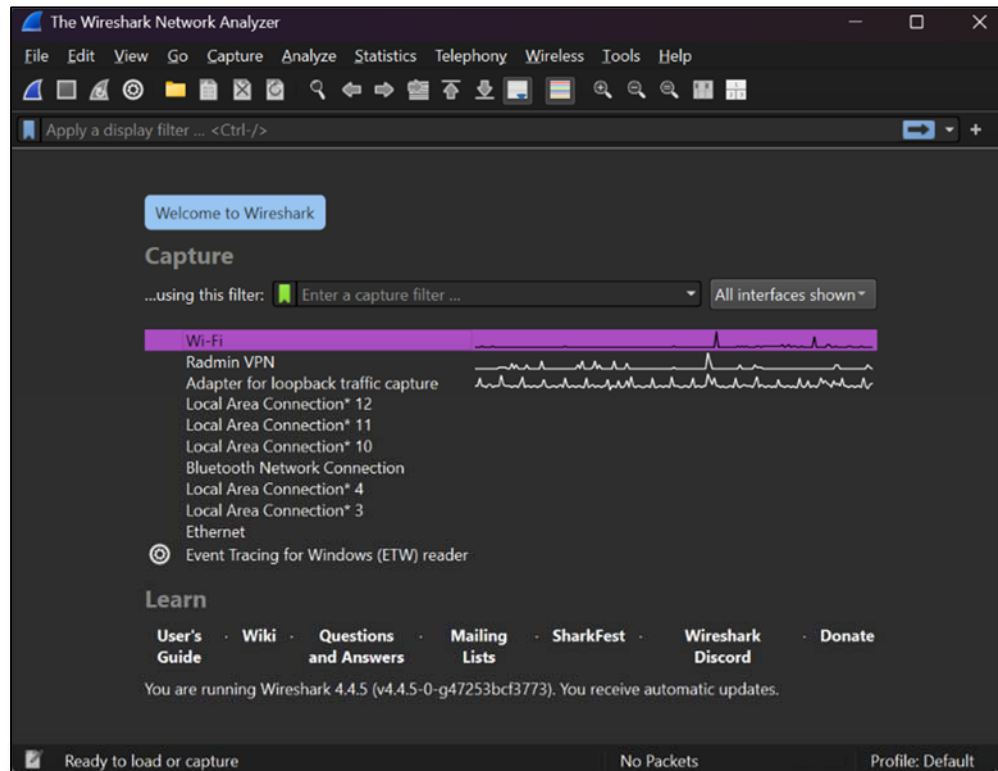
Once Npcap setup is finished, Wireshark installation will be complete.



Click “**Finish**” to complete setup.

Wireshark Application

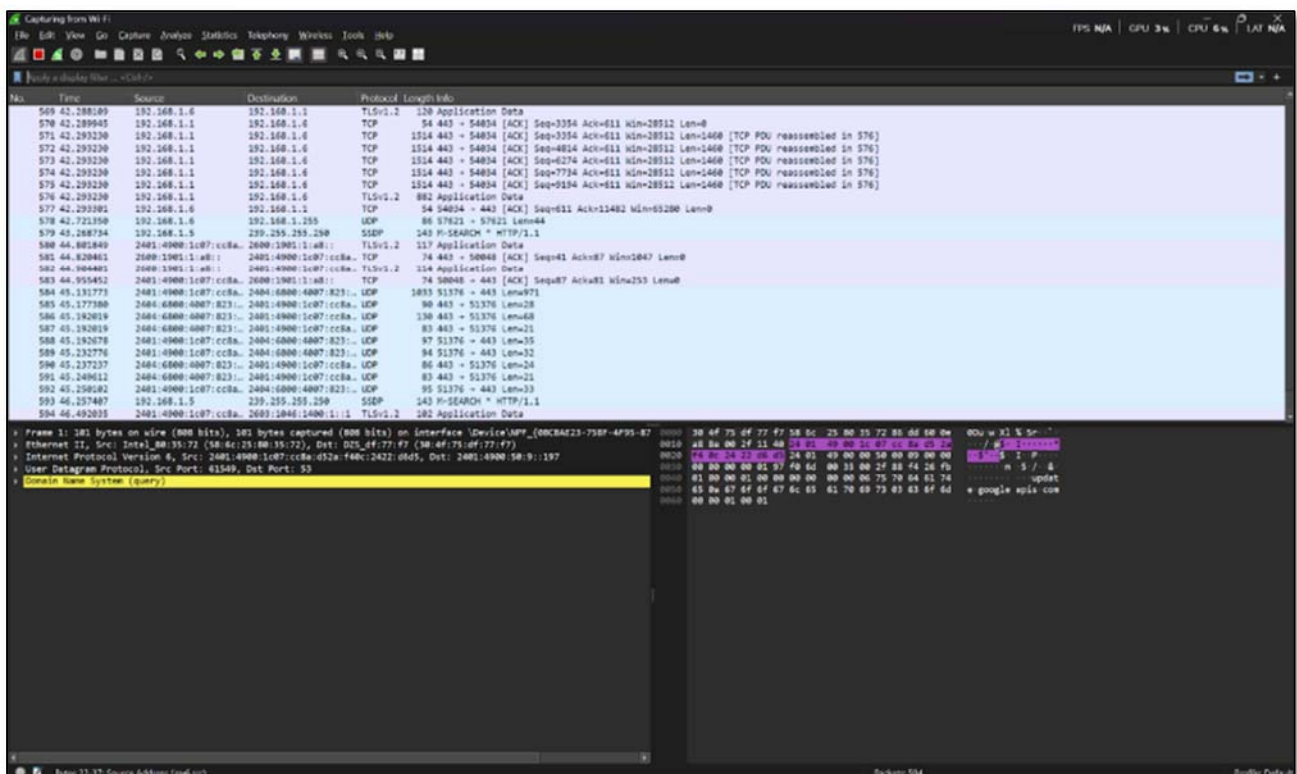
Run the Wireshark application.



This is the first screen where you can see all the connections you can capture packets from.

Double click on the connection you want to capture packets from.

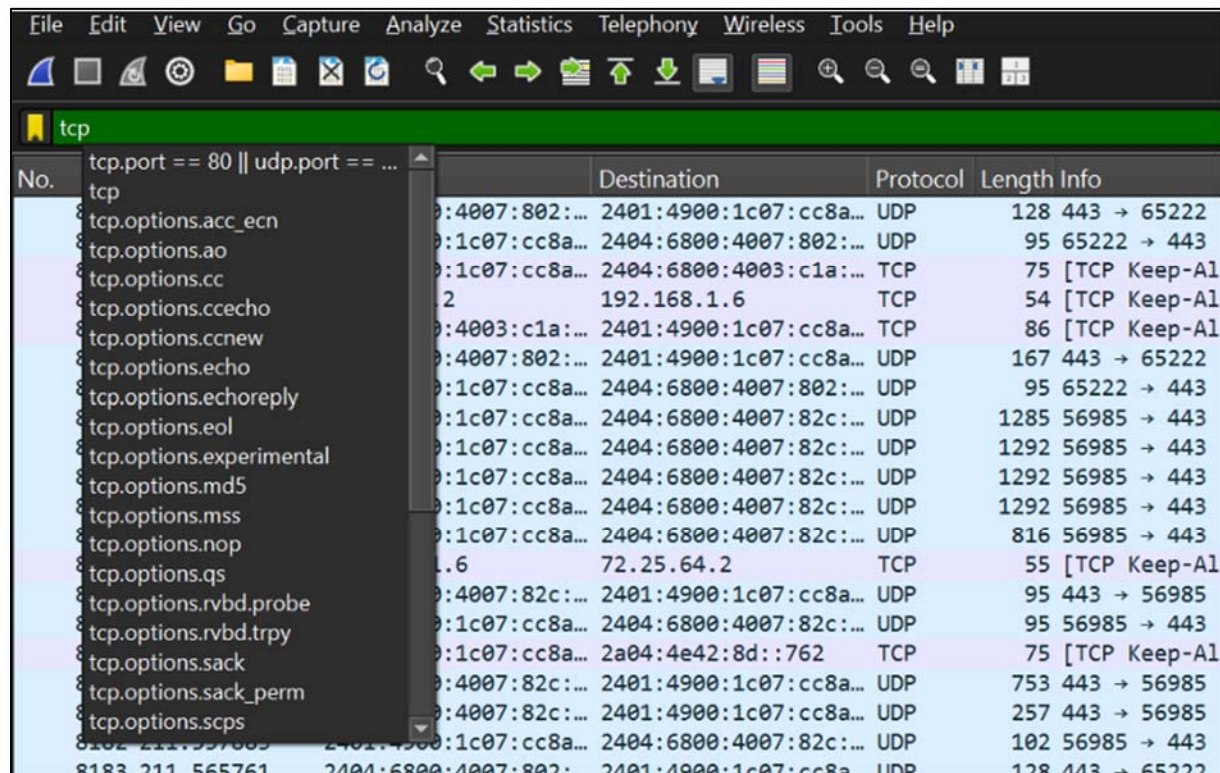
For this demonstration, we chose to track packets via Wi-Fi connection.



All the packets will be continuously traced via this network and the type of protocol used in the connection will also be visible. You can stop tracing the packets by clicking the **Red Square Icon** on the top left of the screen.

You can also filter the packets. For this example, we will filter web traffic packets. These packets use TCP and port 80.

Type “tcp” on the filter bar at the top of the screen.

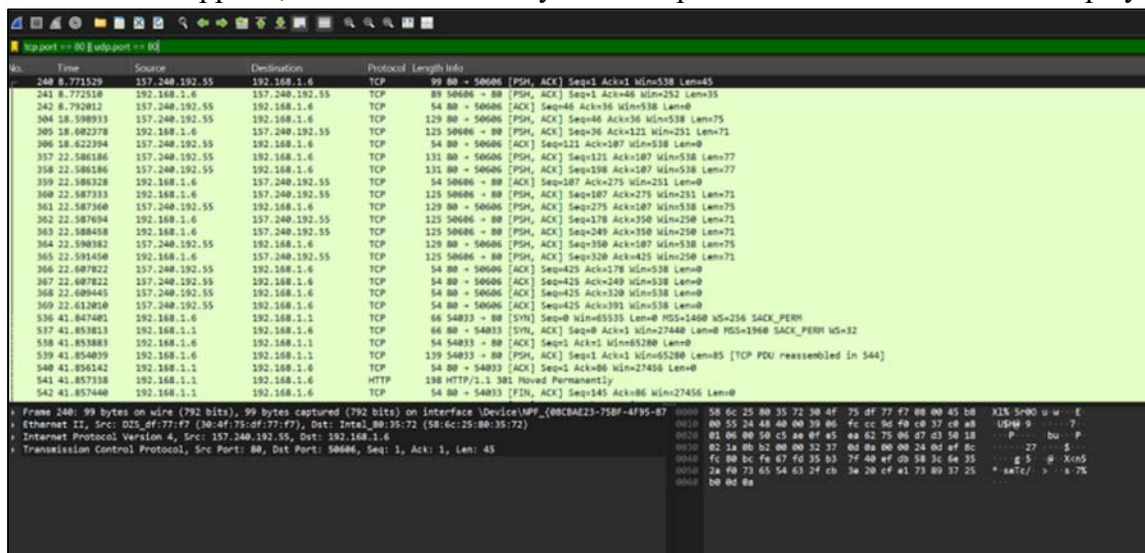


There will be many options for users to select. However, we will be selecting the first one, i.e. “tcp.port == 80 || udp.port == 80” to filter the packets to only show web traffic packets.

After selecting click the blue arrow on the right of the filter bar to apply filter:



After the filter is applied, we can see that only the TCP protocol connections will be displayed:



Use Cases of Wireshark in Network Security

- **Monitor Network Traffic:** Wireshark helps you see all the data being sent and received on a network, which is useful for spotting unusual or suspicious activity.
- **Detecting Attacks:** It can help identify signs of cyberattacks, like Denial of Service (DoS), unauthorized access, or malware trying to connect to the internet.
- **Analyze Individual Packets:** You can look at specific packets of data to check for errors, hidden threats, or sensitive information being leaked.
- **Support in Incident Response:** After a security issue, Wireshark helps trace what happened, how it happened, and what data was affected.
- **Find Network Weaknesses:** It can point out misconfigured settings or strange behavior in network protocols that might lead to security problems.
- **Detect Spoofing or Hacking:** Wireshark helps spot tricks like ARP spoofing or man-in-the-middle attacks, where hackers try to intercept or fake communication.

The setup and running were really simple, so we did not face any issues while downloading or running the program.

References:

[How to Install Wireshark and Trace Packets Easily on Windows 10/11 \(2024\)](#)