SSGMCE	SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGG.	LABORATORY MANUAL
	PRACTICAL EXPERIMENT INSTRUCTION SHEET	
	EXPERIMENT TITLE : Install Wireshark and analyses the data packet using Wireshark Packet Analyzer Tool.	
EXPERIMENT NO.: **SSGMCE/WI/IT/01/4IT06/05**	ISSUE NO. : 00	ISSUE DATE : 22.01.2024
REV. DATE :	REV. NO. :	DEPTT. : INFORMATION TECHNOLOGY
LABORATORY : Data Communication & Networking Lab (4IT06)	SEMESTER : IV	PAGE: 1 OF 8

01 AIM: Install Wireshark and analysis the data packet using Wireshark Packet Analyzer Tool.

02 SOCOPE:

- To provide hands-on experience with Wireshark, a leading network packet analyser tool.
- Install Wireshark on their respective operating systems, capture live network data, and analyse packets to understand the fundamentals of network protocols, traffic patterns, and potential security vulnerabilities within a network.

03 FACILITIES

SOFTWARE Wireshark

04 THEORY

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

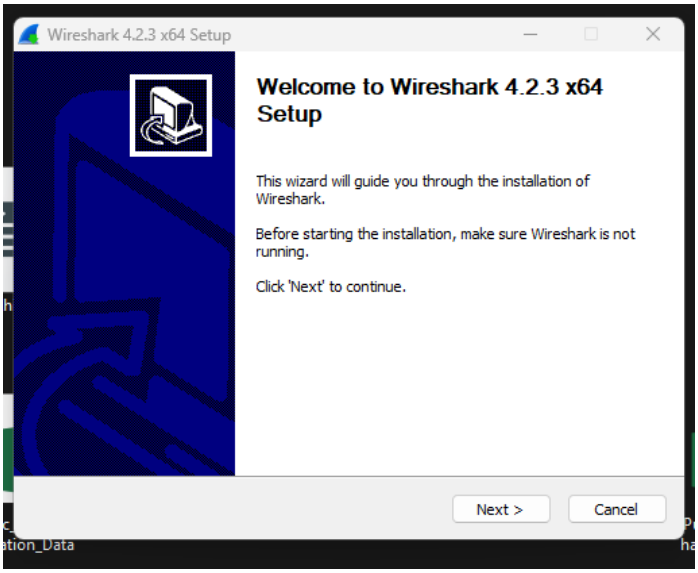
This practical provides a crucial skill set for those interested in network administration, security analysis, and troubleshooting network issues. By mastering Wireshark, you will be better equipped to maintain and secure networks in a real-world setting.

Download Wireshark (Windows)

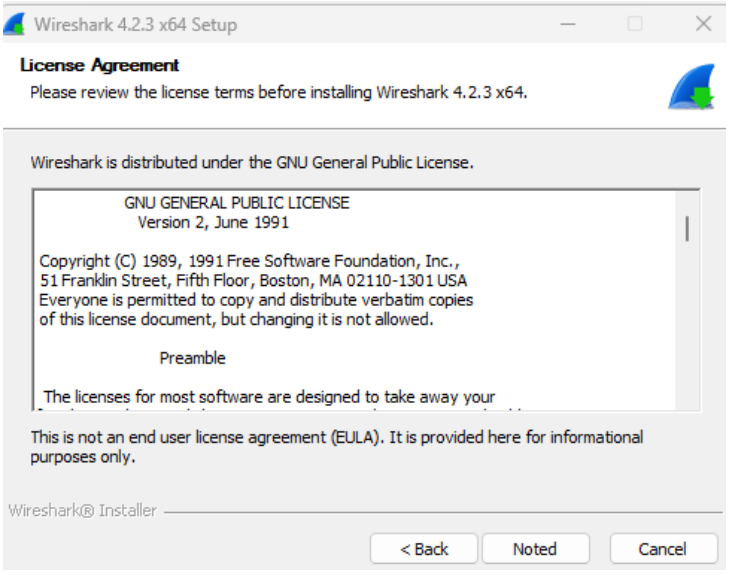
Download the Installer: Go to the Wireshark official website (https://www.wireshark.org/) and download the latest stable version of Wireshark for Windows.

You can keep the default selections or customize them based on your needs.

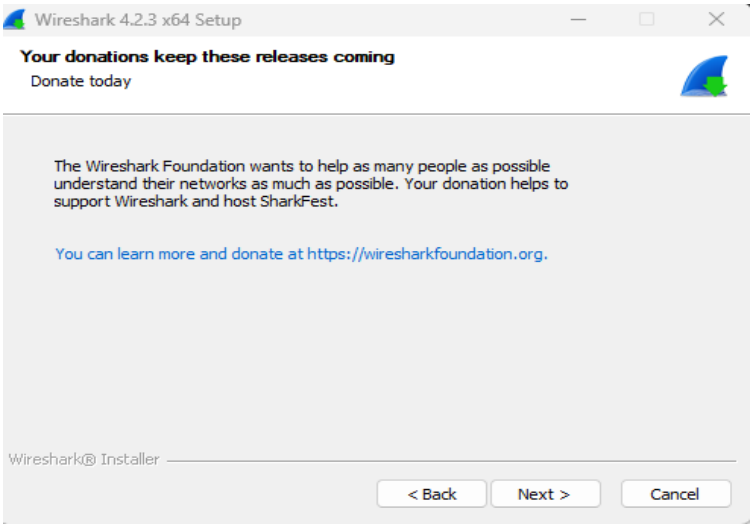
I. Run the Installer: Double-click the downloaded file to start the installation process



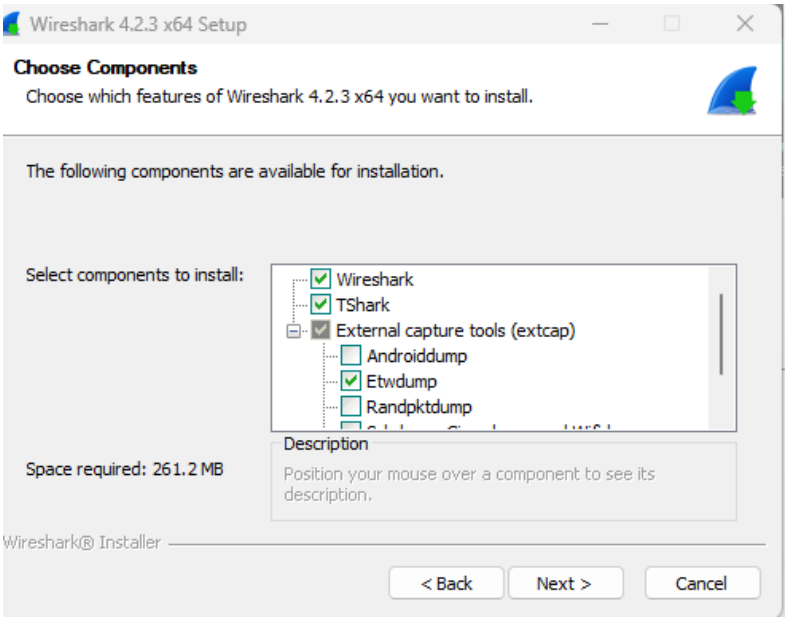
II. Review the license terms before installing Wireshark



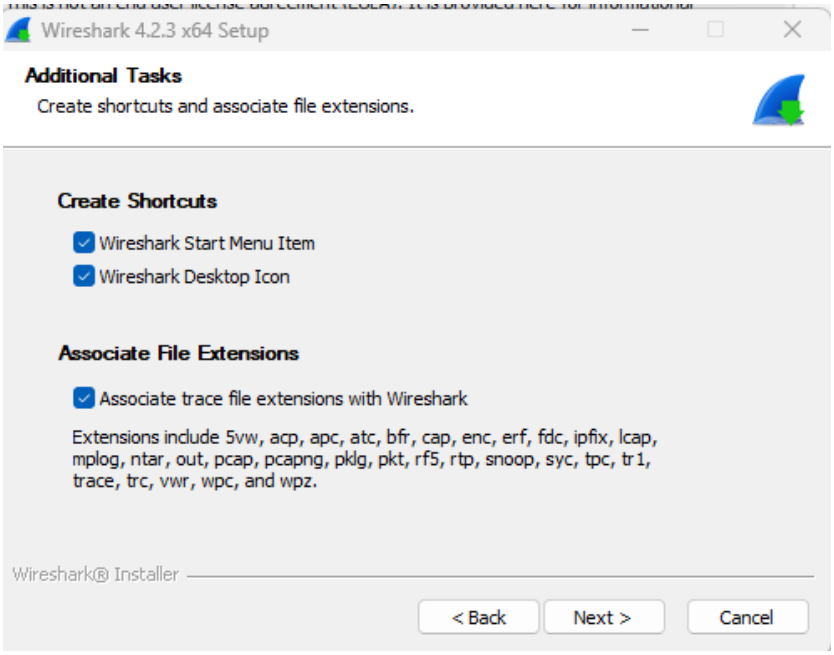
III. Check next to proceed further



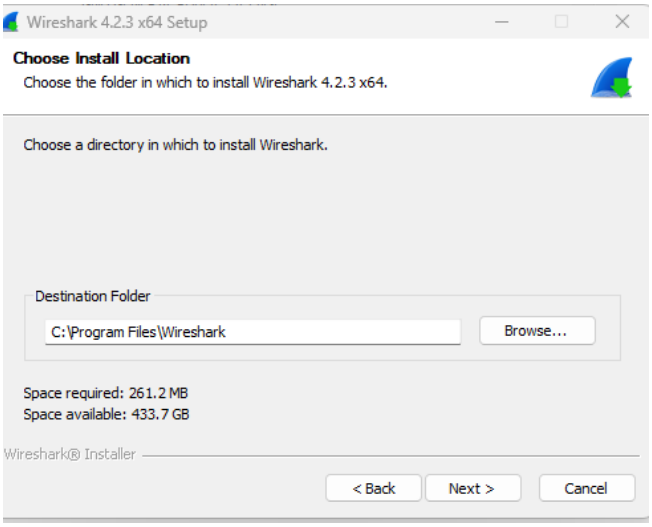
IV. Choose appropriate components features you want to install



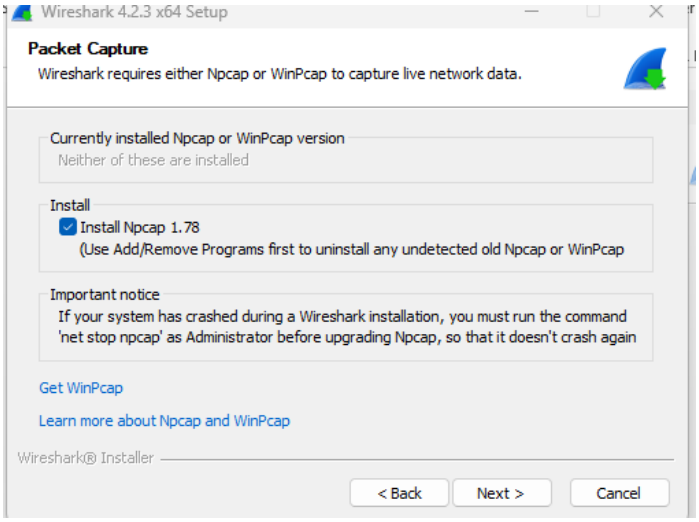
V. **Additional Task:** Crete shortcuts and associate file extension.



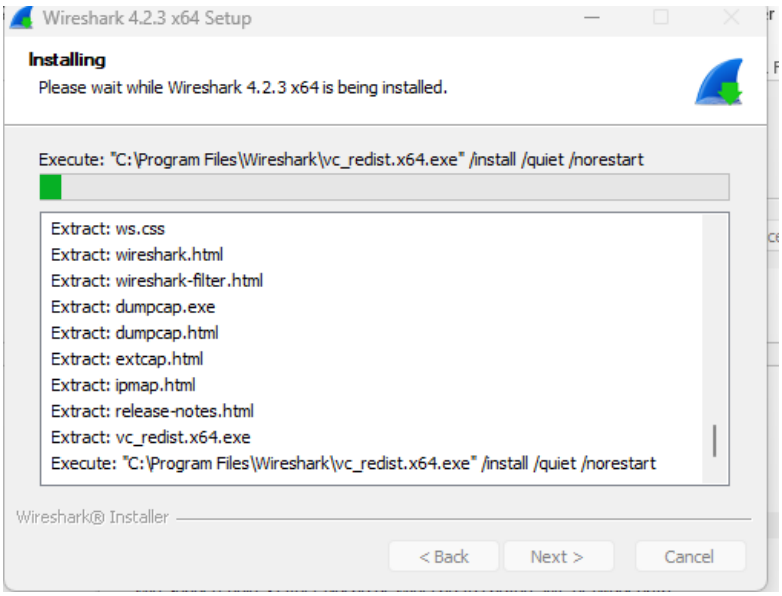
VI. **Directory:** Choose the location where you want to install Wireshark.



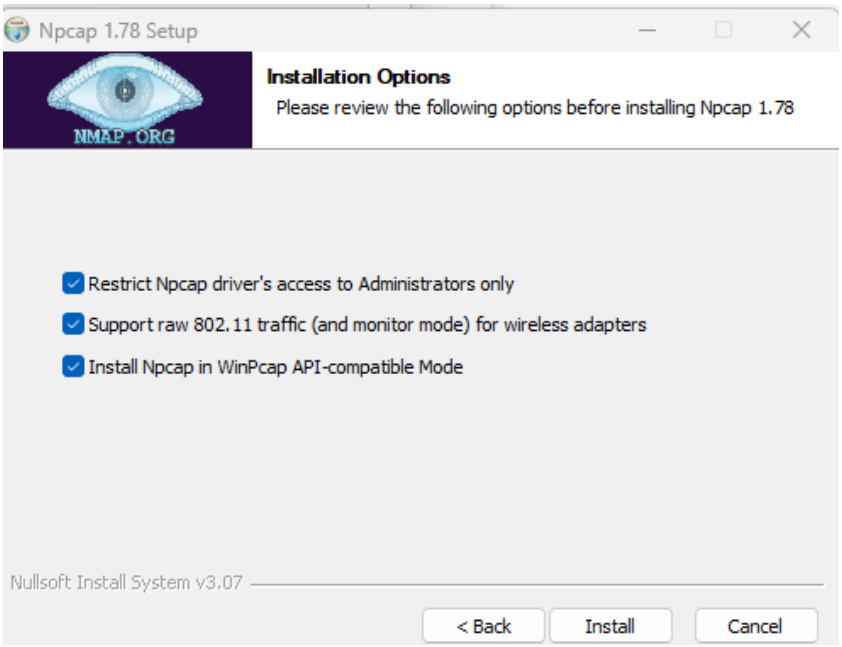
VII. Install WinPcap/Npcap: Wireshark requires a packet capture library. For modern versions, Npcap is recommended. The installer might prompt you to install Npcap if it's not already installed on your system.Installation



VIII. Complete the Installation: Follow the rest of the prompts to complete the installation. You might need to agree to license agreements or decide whether to create a desktop icon



IX. Select the Installation Option



X. Launch Wireshark: Once installed, you have to reboot your pc after that you can start Wireshark from the Start menu or the desktop icon, if you chose to create one.

Analyzing data packets using Wireshark, a network protocol analyzer tool, involves several steps. Here's a general overview of how to use Wireshark to analyze packets:

1. Install Wireshark: Download and install Wireshark from the official website.

2. Capture Packets:

- Open Wireshark.
- Select the network interface you want to capture packets from. This could be Ethernet for wired

connections or a Wi-Fi interface for wireless connections.

- Click on the shark fin icon to start capturing packets on that interface.

3. Capture Filters (Optional):

- If you are looking for specific traffic, you can use capture filters to only capture packets that match certain criteria, like IP addresses or protocols.

4. Stop Capture:

- After you have captured enough data for your analysis, stop the capture by clicking the red square on the toolbar.

5. Analyze Packets:

- Scroll through the captured packets in the top pane. Click on a packet to see more details in the middle pane and the raw data in the bottom pane.
- The middle pane breaks down the packet into its layers (Ethernet, IP, TCP/UDP, etc.), and you can expand these to see field-by-field details.

6. Use Display Filter:

- To narrow down the displayed packets, use the display filters. For example, `tcp.port == 80` will show only packets where the TCP port is 80 (typically HTTP traffic).
- Wireshark has a powerful filtering language, so you can get very specific about what you want to see.

7. Follow Streams:

- For TCP connections, you can right-click on a packet and select "Follow" > "TCP Stream" to see

the entire conversation between two endpoints.

8. Graphs and Statistics:

- Use the "Statistics" menu to see various graphs and summaries of the captured data. For example, "IO Graphs" can show data rates over time.

9. Inspect Individual Fields:

- In the packet details pane, you can click on individual fields to learn more about them. This can be useful for understanding protocol behavior and troubleshooting.

10. Export and Save Data:

- You can save your packet capture for later analysis or export specific packets or streams if needed.

Remember, the legality of capturing packets on a network depends on your jurisdiction and whether you have permission to monitor the network traffic. Always ensure you are authorized to capture packets to avoid legal issues.

05 CONCULSION

Upon completing this practical session, student will:

- Have Wireshark installed and configured on their systems.
- Understand how to capture and save network traffic data. Be able to identify common network protocols and analyse their behaviour in a network.
- Possess foundational skills to detect and investigate network anomalies or potential security threats in packet data.