WIRESHARK

Res. Asst. Melek ŞENTÜRK

WHAT IS WIRESHARK?

- It is a powerful open-source software used to analyze network traffic and inspect network packets.

- Network administrators, security experts, and developers use Wireshark to monitor data transmissions on the network, detect errors, and ensure network security.

KEY FEATURES

- **Packet Analysis:** Wireshark captures all data packets (HTTP, DNS, TCP, UDP, etc.) on the network and analyzes them in detail.

- **Protocol Support:** Wireshark can analyze a wide range of network protocols (TCP, IP, HTTP, FTP, DNS, ICMP, ARP, and more). These protocols are decoded and displayed in a readable format by Wireshark.

- **Filtering:** Wireshark allows users to quickly find the data they are interested in while analyzing large amounts of network traffic.

WHAT IS NPCAP?

- Npcap is a Windows-based packet capture library used for capturing and analyzing network traffic.

- Npcap, which is especially used in network analysis tools like Wireshark, provides the essential infrastructure needed for capturing network data and inspecting network packets.

NPCAP KEY FEATURES

- **Advanced Packet Capture:** Npcap provides features for capturing network traffic in more depth.

- **Encrypted Traffic Support:** Npcap provides the necessary decryption infrastructure for capturing network traffic that uses SSL/TLS encryption. This enables the analysis of traffic from applications with secure connections.

- **Loopback Support:** Npcap supports the loopback interface, allowing the monitoring of the computer's internal communication (e.g., data sent over localhost). This was a missing feature in WinPcap.

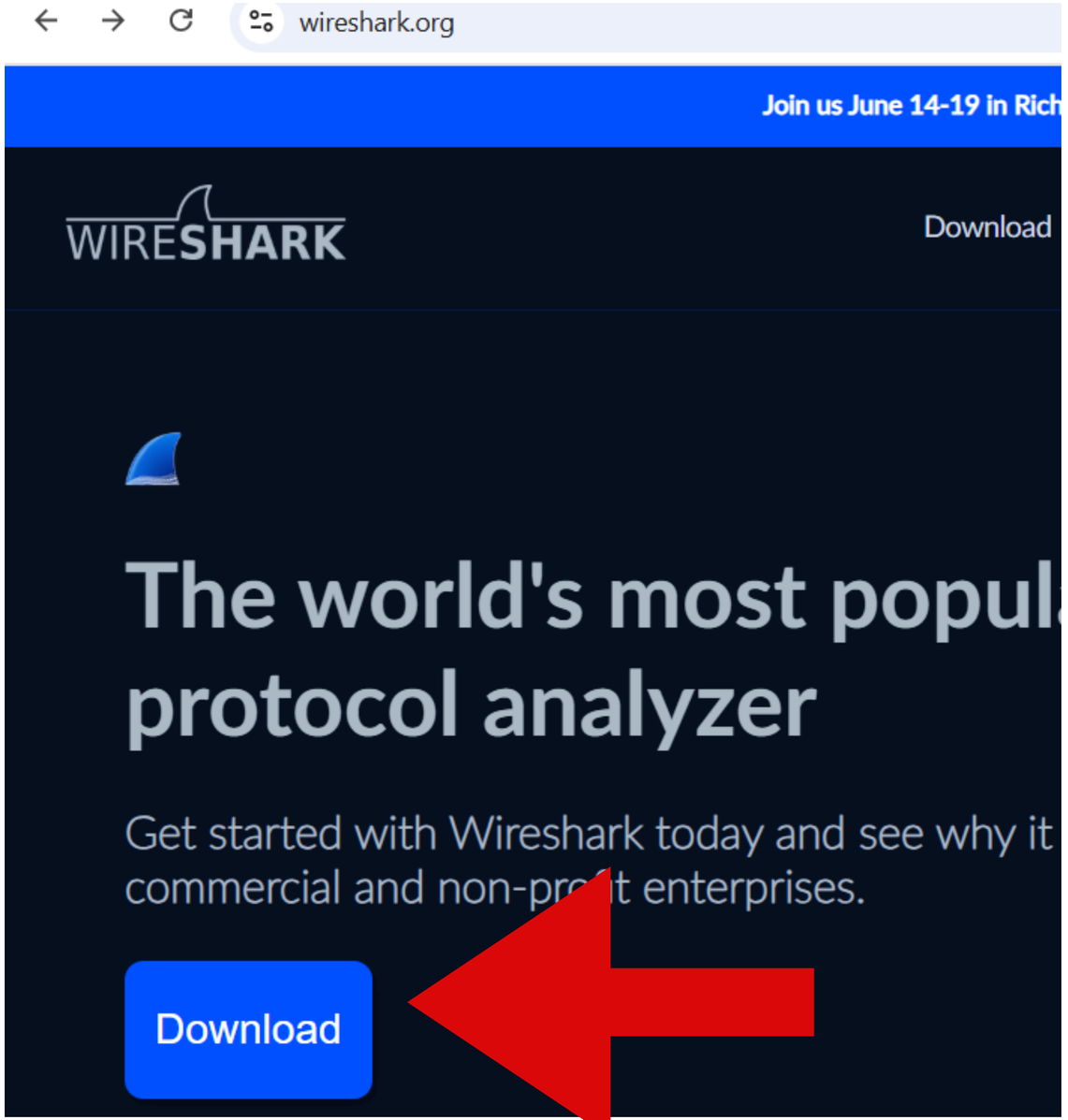
THE PACKET CAPTURE PROCESS OF NPCAP

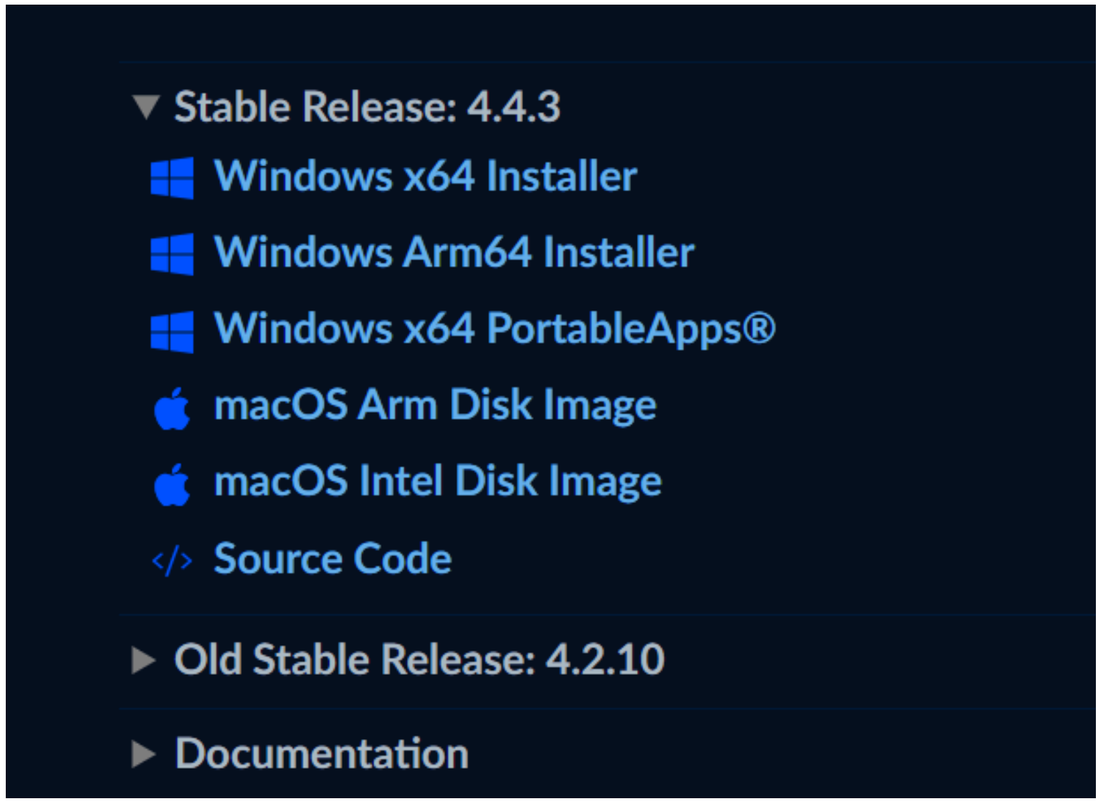
- Npcap first determines which network interface will be used to capture network traffic. These interfaces can include Ethernet, Wi-Fi, virtual network interfaces (VPN), and even local network interfaces like loopback.
- Once the selected network interface is chosen, Npcap starts listening to network traffic. During this process, all packets occurring on the network (data packets, control packets, error messages, etc.) are captured.
- Npcap decrypts the captured packets and analyzes them according to various network protocols (IP, TCP, UDP, DNS, HTTP, etc.). This analysis enables the data to be displayed in a meaningful format.
- Analysis tools like Wireshark use this decoded data to display protocol-based details to the user.

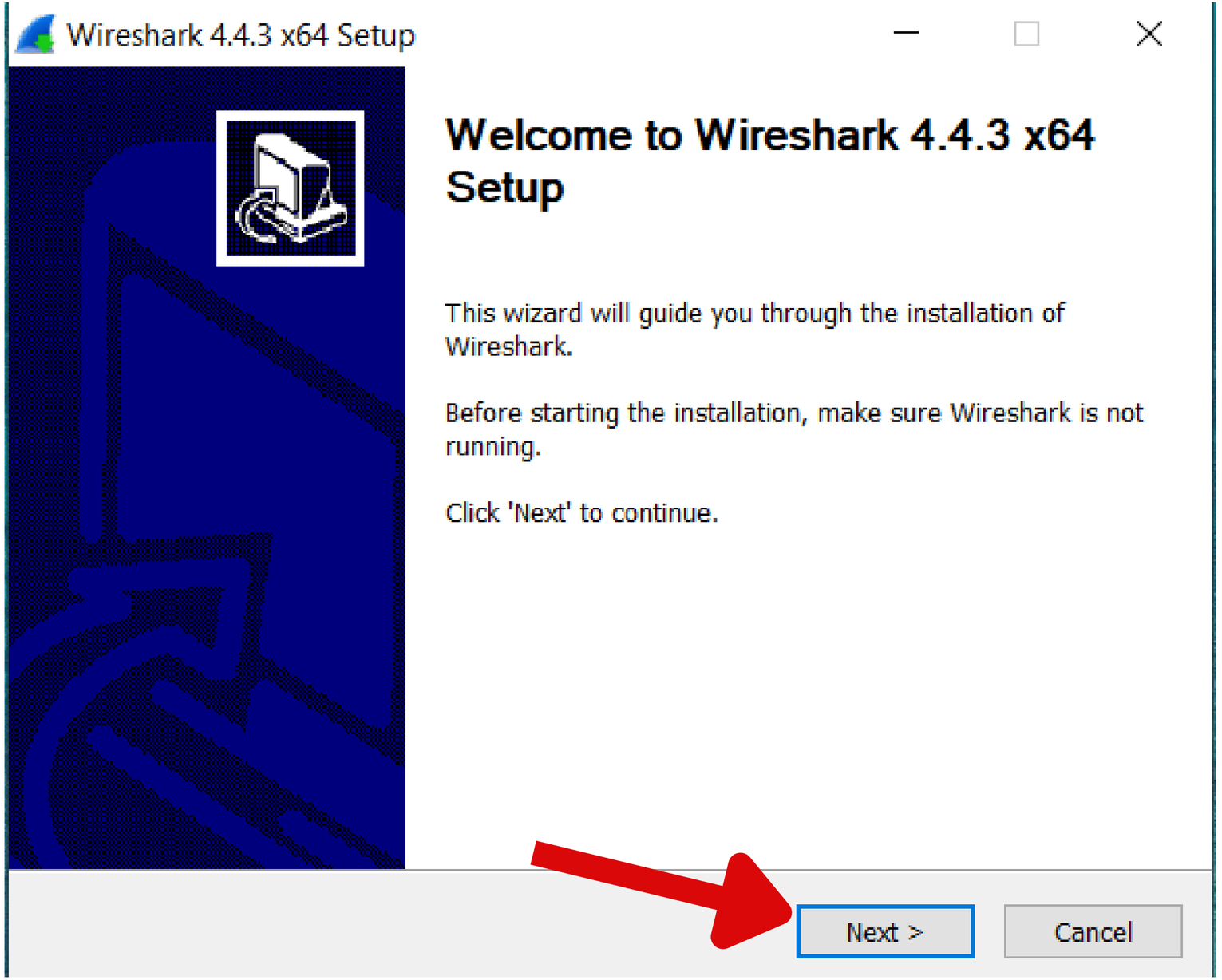
WIRESHARK USE CASES

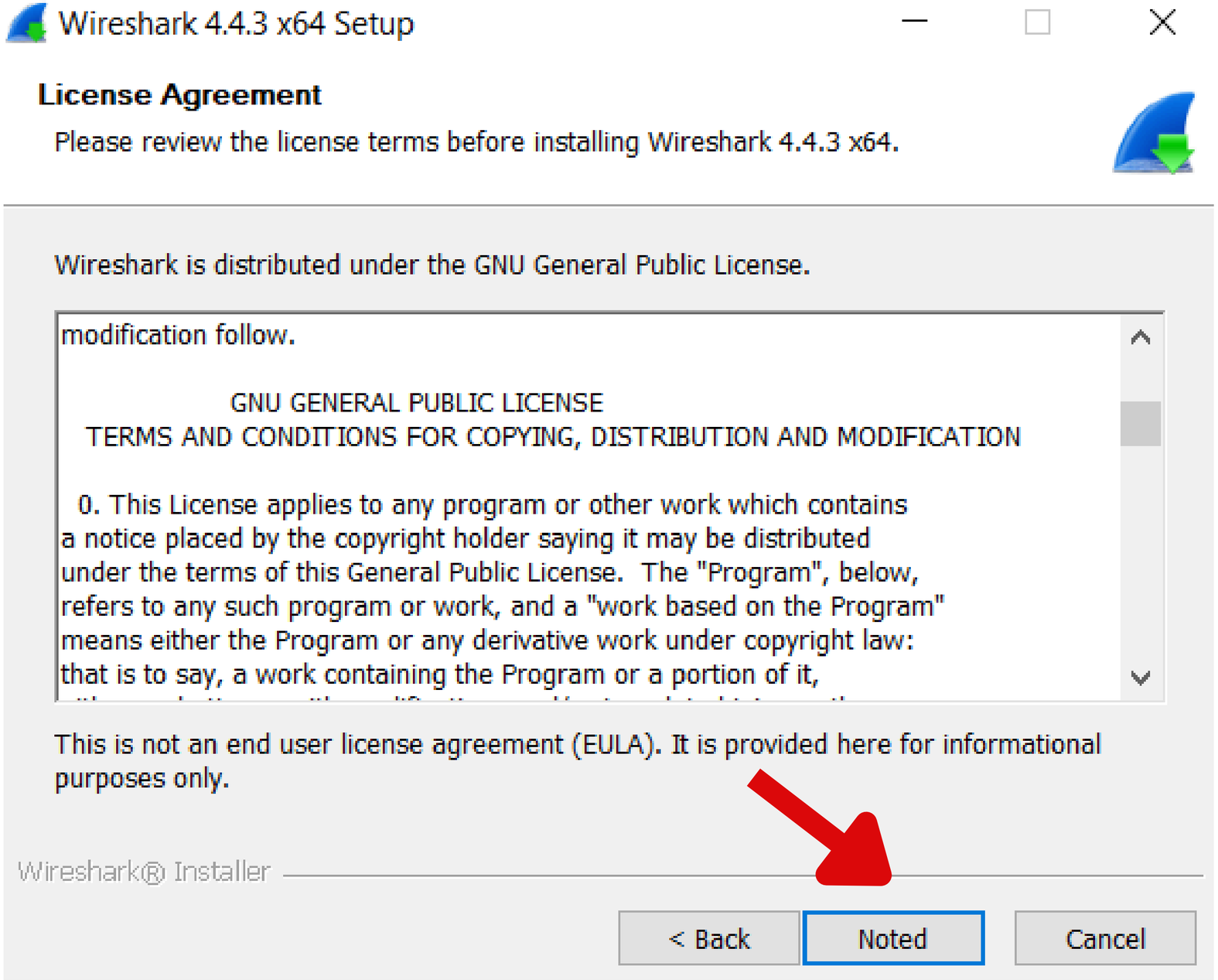
- **Cybersecurity –** Detecting suspicious traffic and attacks.
- **Network Management –** Optimizing network traffic and troubleshooting issues.
- **Ethical Hacking & Penetration Testing –** Analyzing security vulnerabilities.
- **Education & Research –** Learning and teaching network protocols.

WIRESHARK INSTALLATION






Wireshark 4.4.3 x64 Setup
Welcome to Wireshark 4.4.3 x64 Setup
This wizard will guide you through the installation of Wireshark.
Before starting the installation, make sure Wireshark is not running.
Click 'Next' to continue.
Next >
Cancel

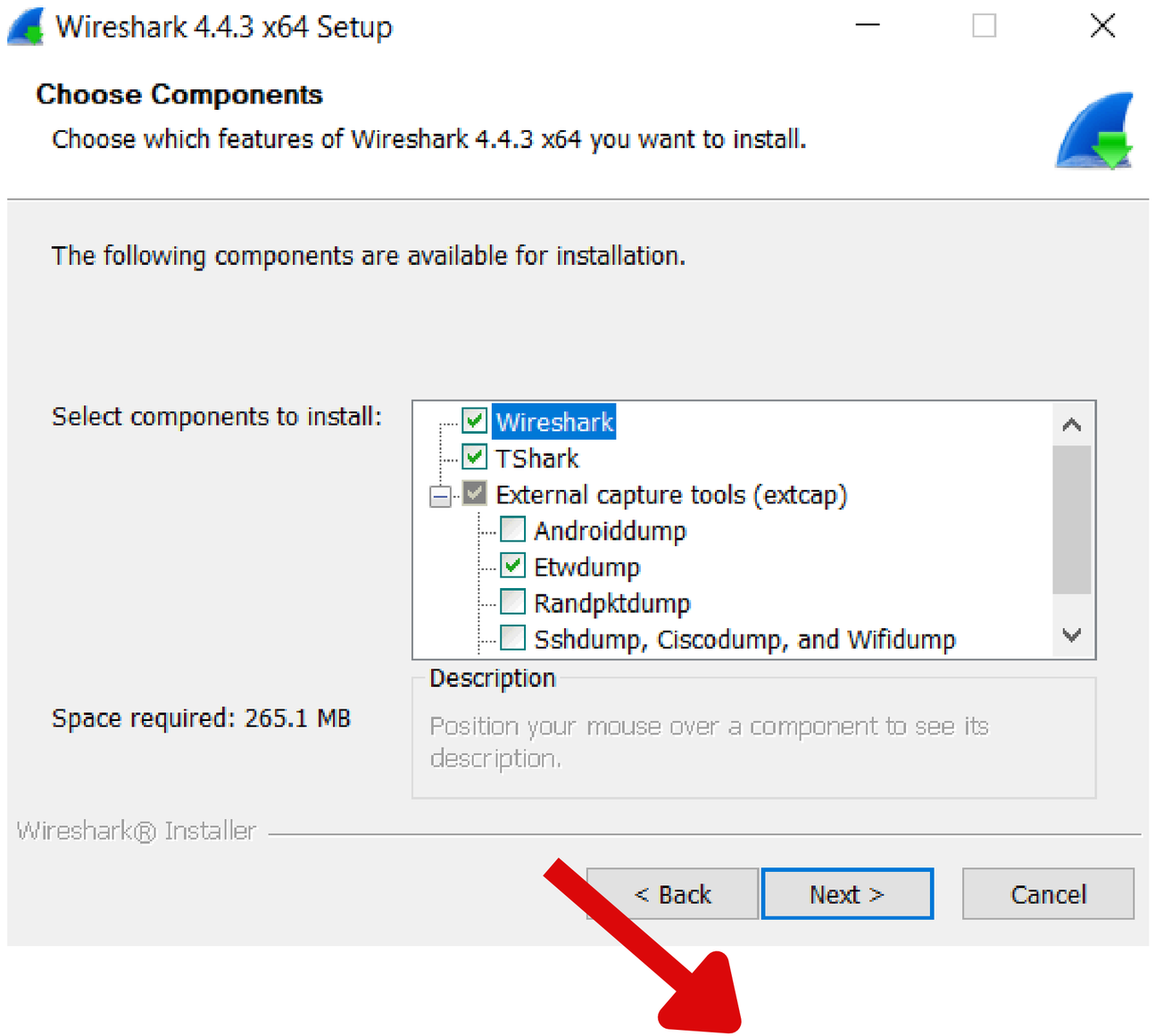

Wireshark 4.4.3 x64 Setup
License Agreement
Please review the license terms before installing Wireshark 4.4.3 x64.
Wireshark is distributed under the GNU General Public License.
modification follow.
GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION
0. This License applies to any program or other work which contains
a notice placed by the copyright holder saying it may be distributed
under the terms of this General Public License. The "Program", below,
refers to any such program or work, and a "work based on the Program"
means either the Program or any derivative work under copyright law:
that is to say, a work containing the Program or a portion of it,
This is not an end user license agreement (EULA). It is provided here for informational purposes only.
Wireshark® Installer
< Back
Noted
Cancel

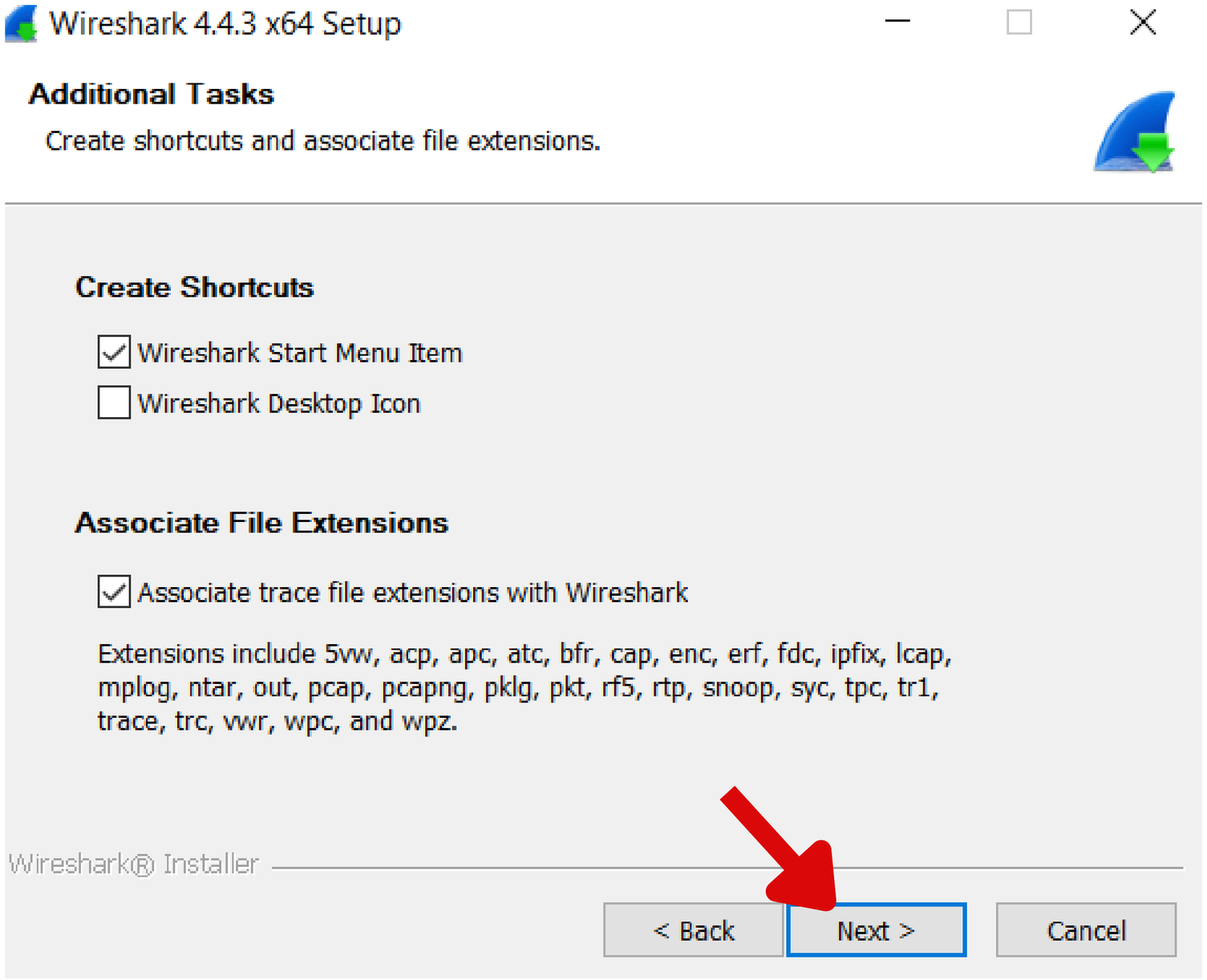
Tshark is the command-line version of Wireshark.

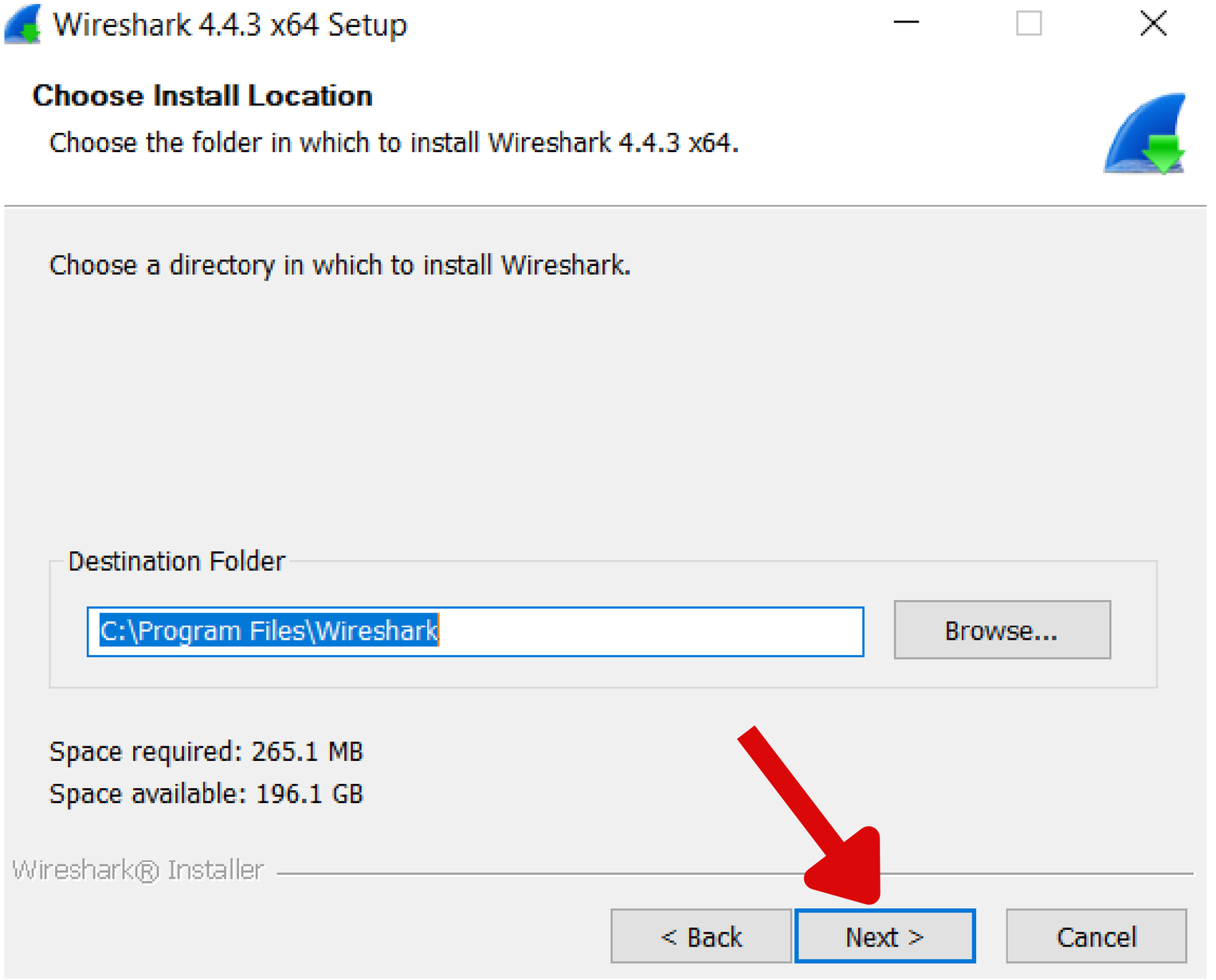
ETW (Event Tracing for Windows). ETW is a built-in tracing system in Windows operating systems.

Androiddump monitors network traffic on Android devices and captures a dump of it.

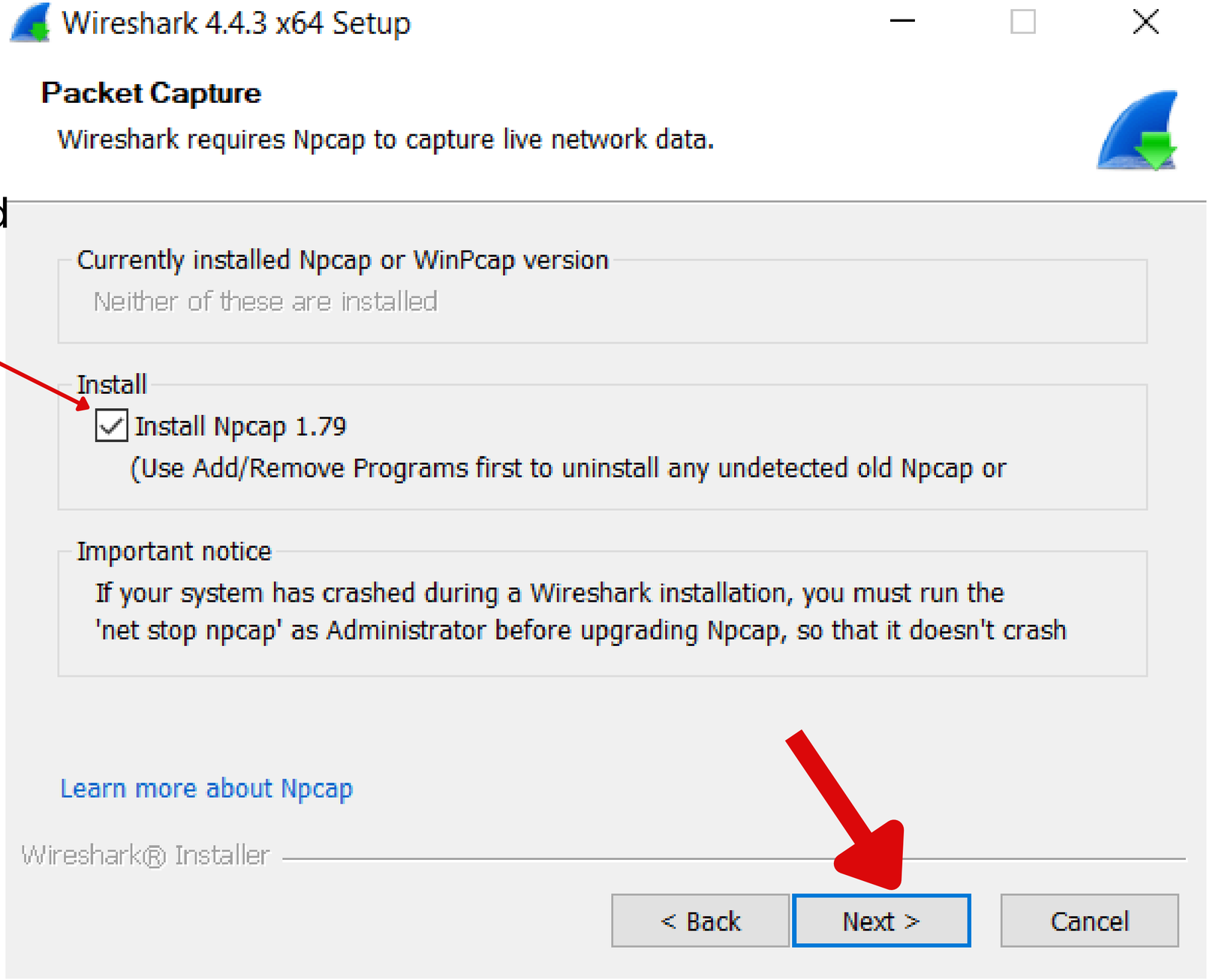
Randpkdump filters network packets and dumps a randomly selected sample of them.



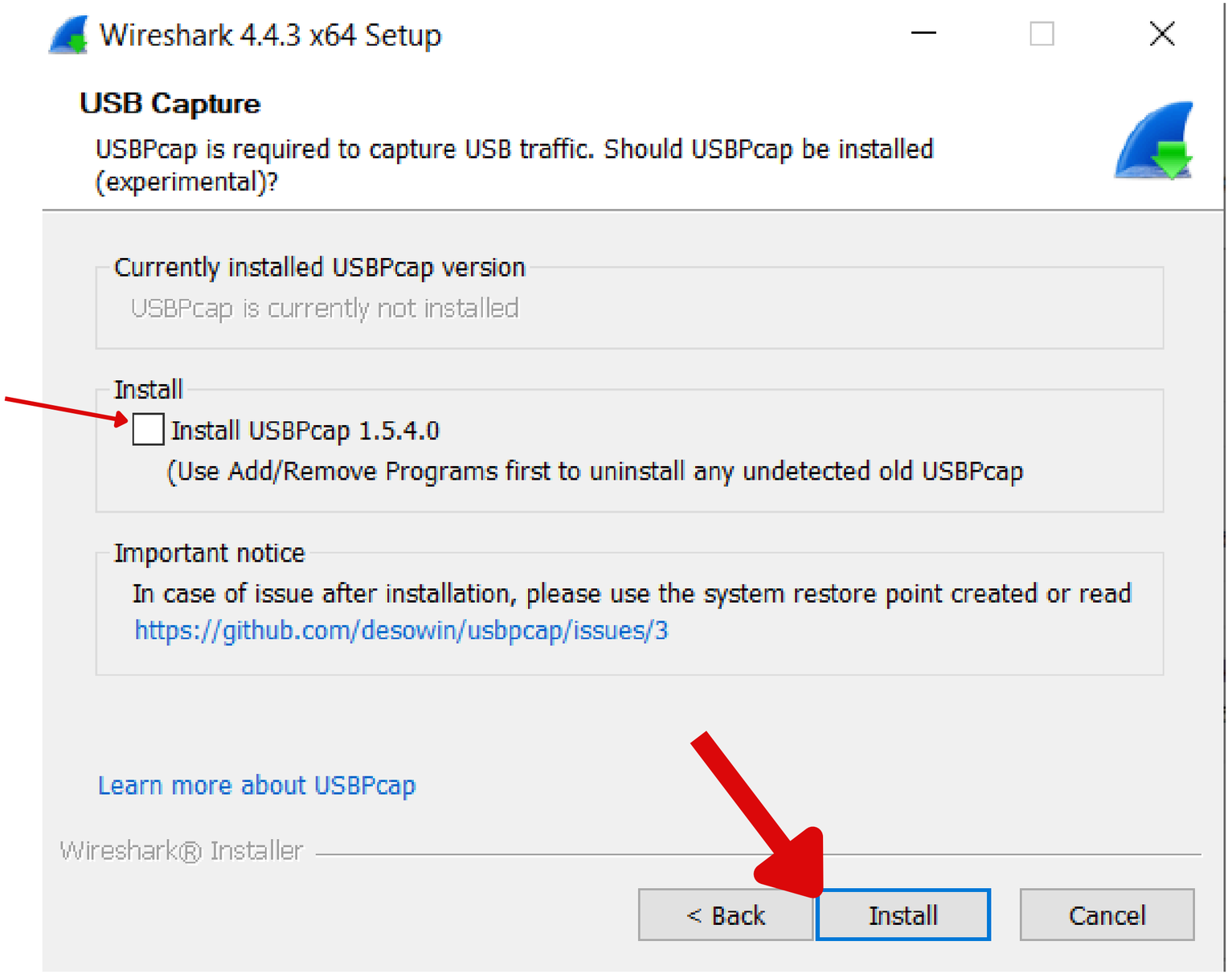

Wireshark 4.4.3 x64 Setup
Additional Tasks
Create shortcuts and associate file extensions.
Create Shortcuts
Wireshark Start Menu Item
Wireshark Desktop Icon
Associate File Extensions
Associate trace file extensions with Wireshark
Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, rtp, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.
Wireshark® Installer
< Back
Next >
Cancel

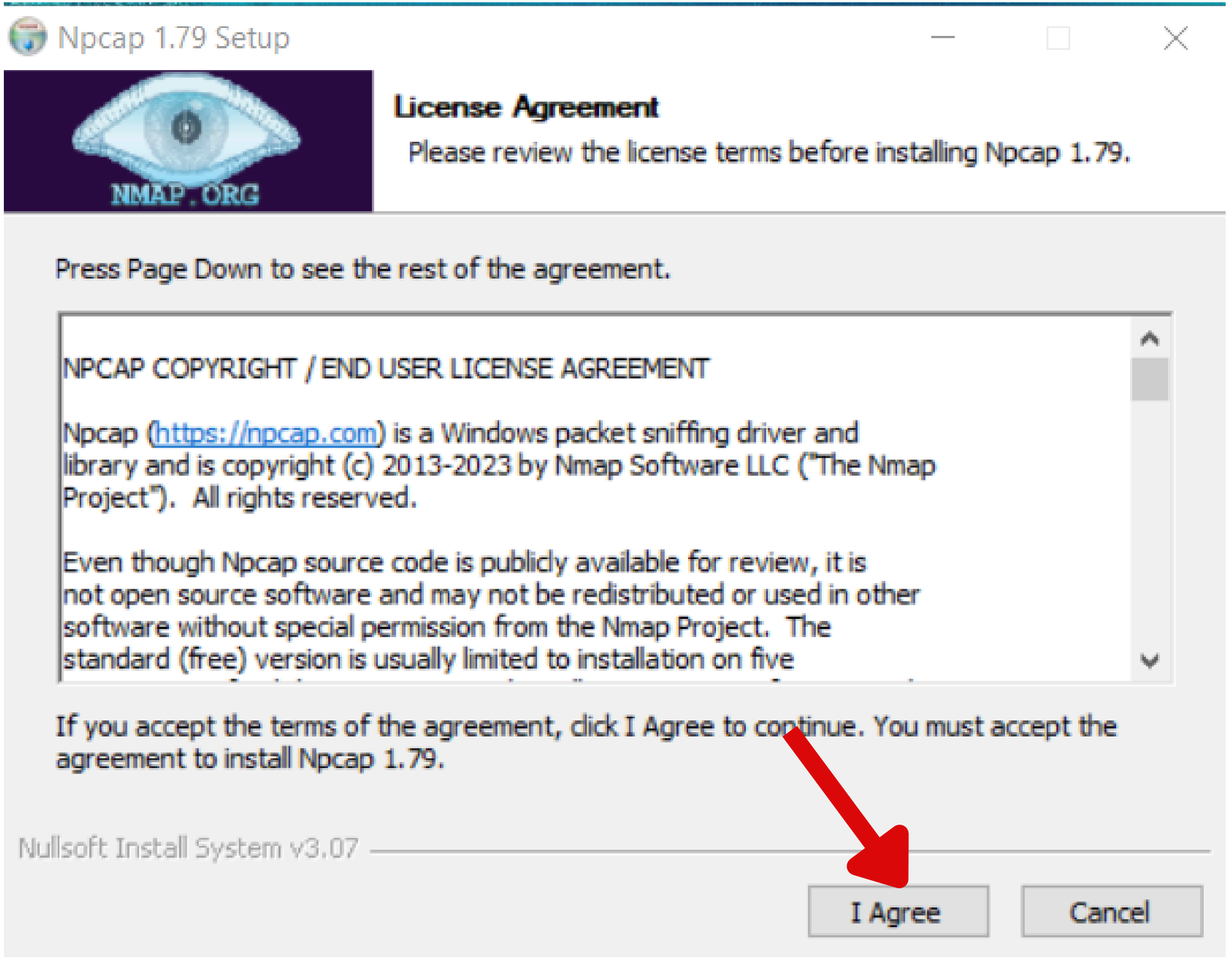

Wireshark 4.4.3 x64 Setup
Choose Install Location
Choose the folder in which to install Wireshark 4.4.3 x64.
Choose a directory in which to install Wireshark.
Destination Folder
C:\Program Files\Wireshark
Browse...
Space required: 265.1 MB
Space available: 196.1 GB
Wireshark® Installer
< Back
Next >
Cancel

Windows-based packet capture library



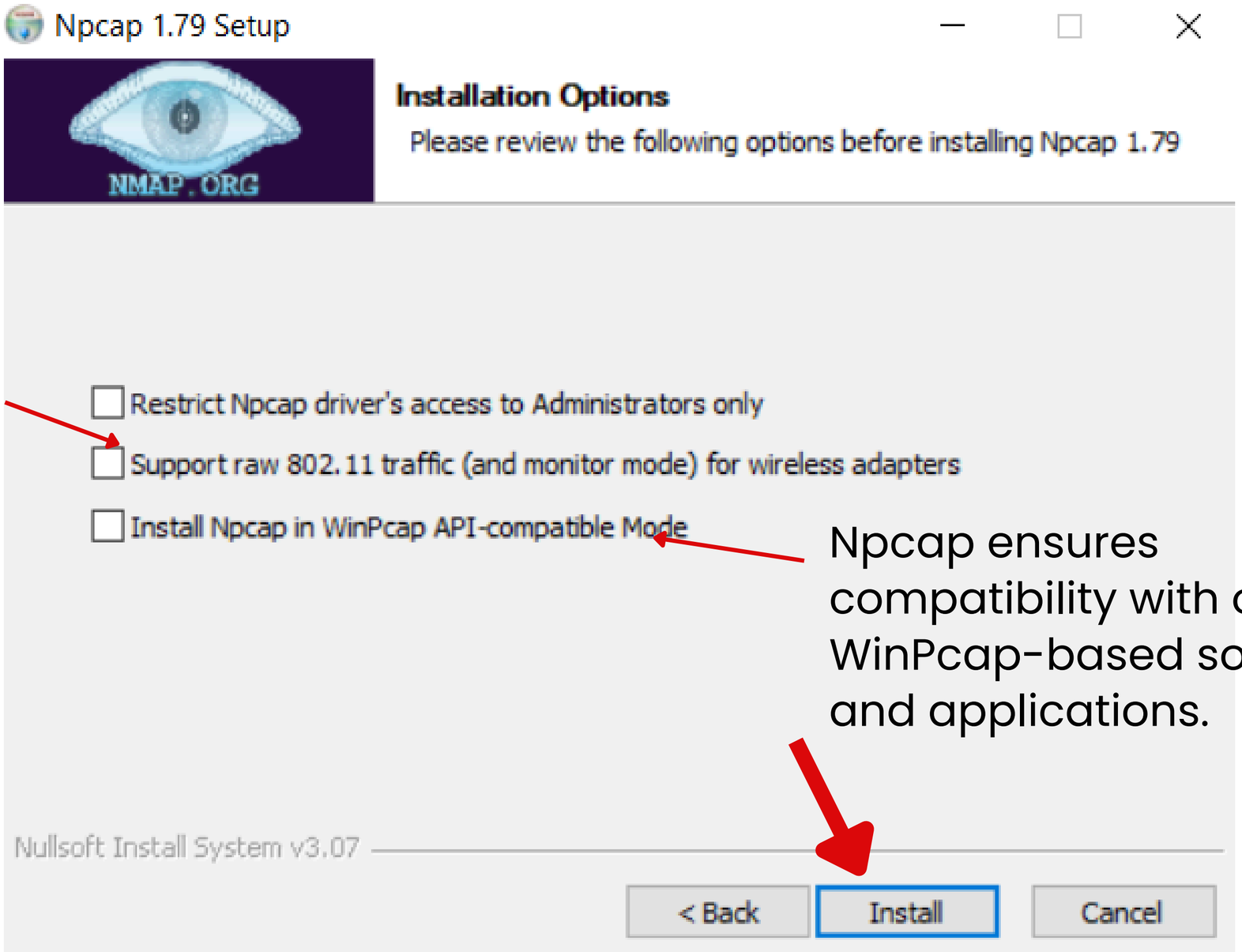
It is a tool used to capture and analyze network traffic of USB devices on the Windows operating system.




Npcap 1.79 Setup
NMAP.ORG
License Agreement
Please review the license terms before installing Npcap 1.79.
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap (https://npcap.com) is a Windows packet sniffing driver and
library and is copyright (c) 2013-2023 by Nmap Software LLC ("The Nmap
Project"). All rights reserved.
Even though Npcap source code is publicly available for review, it is
not open source software and may not be redistributed or used in other
software without special permission from the Nmap Project. The
standard (free) version is usually limited to installation on five
If you accept the terms of the agreement, click I Agree to continue. You must accept the
agreement to install Npcap 1.79.
Nullsoft Install System v3.07
I Agree
Cancel

It is a feature that indicates raw 802.11 traffic on wireless networks.

802.11 is a set of standards used for wireless network communication.



Npcap ensures compatibility with older WinPcap-based software and applications.