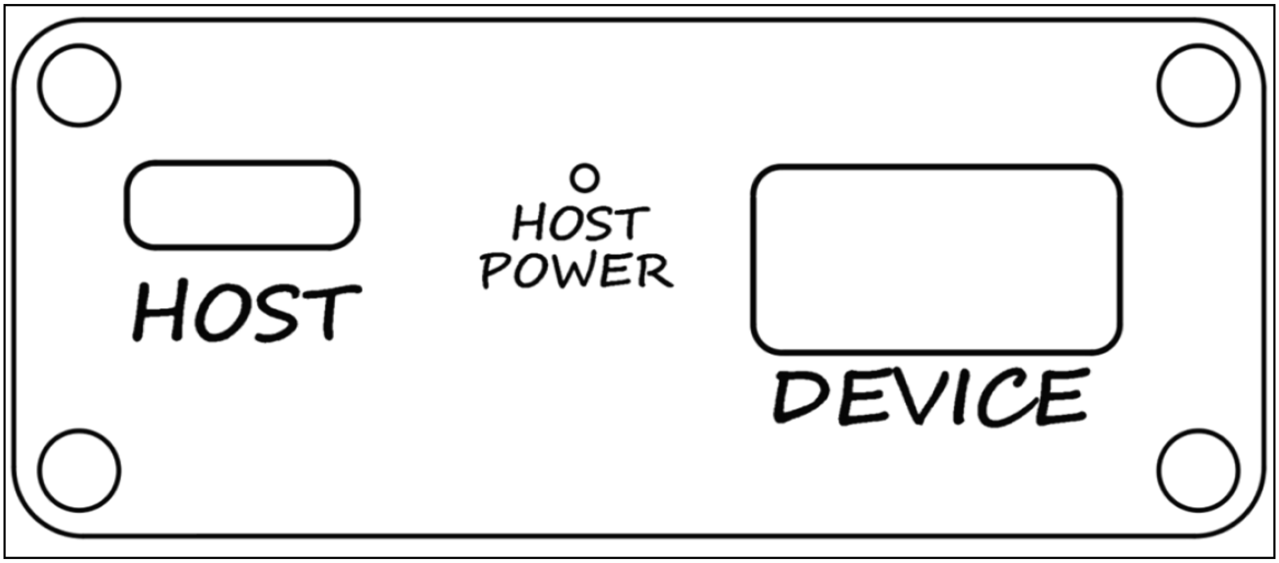
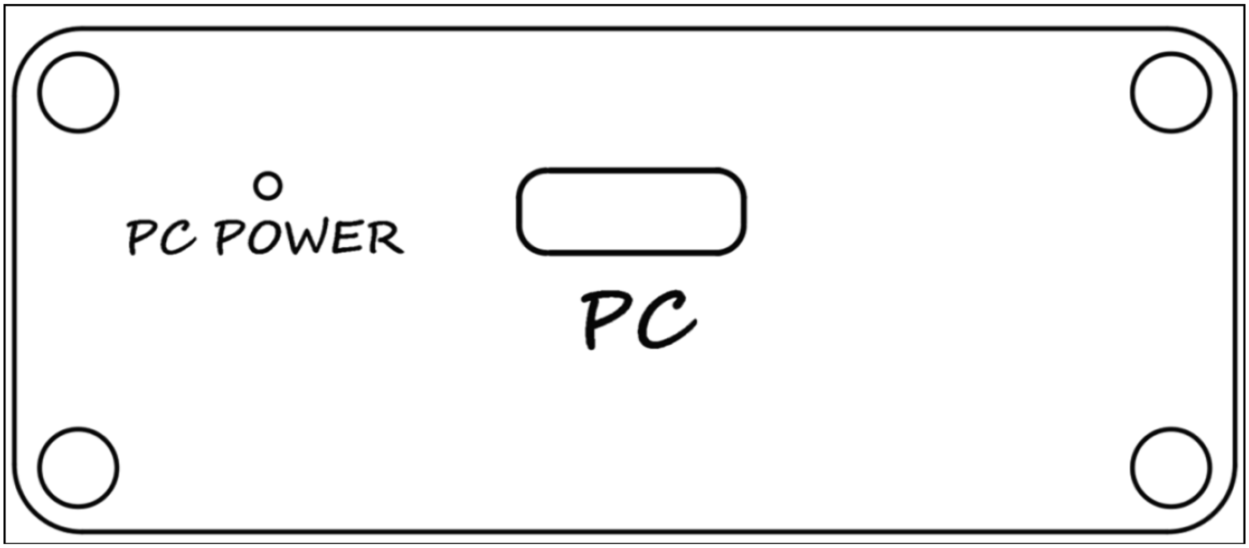
USB Sniffer

Download this manual and other resources for this USB sniffer from
https://roobjax.com/RJT835

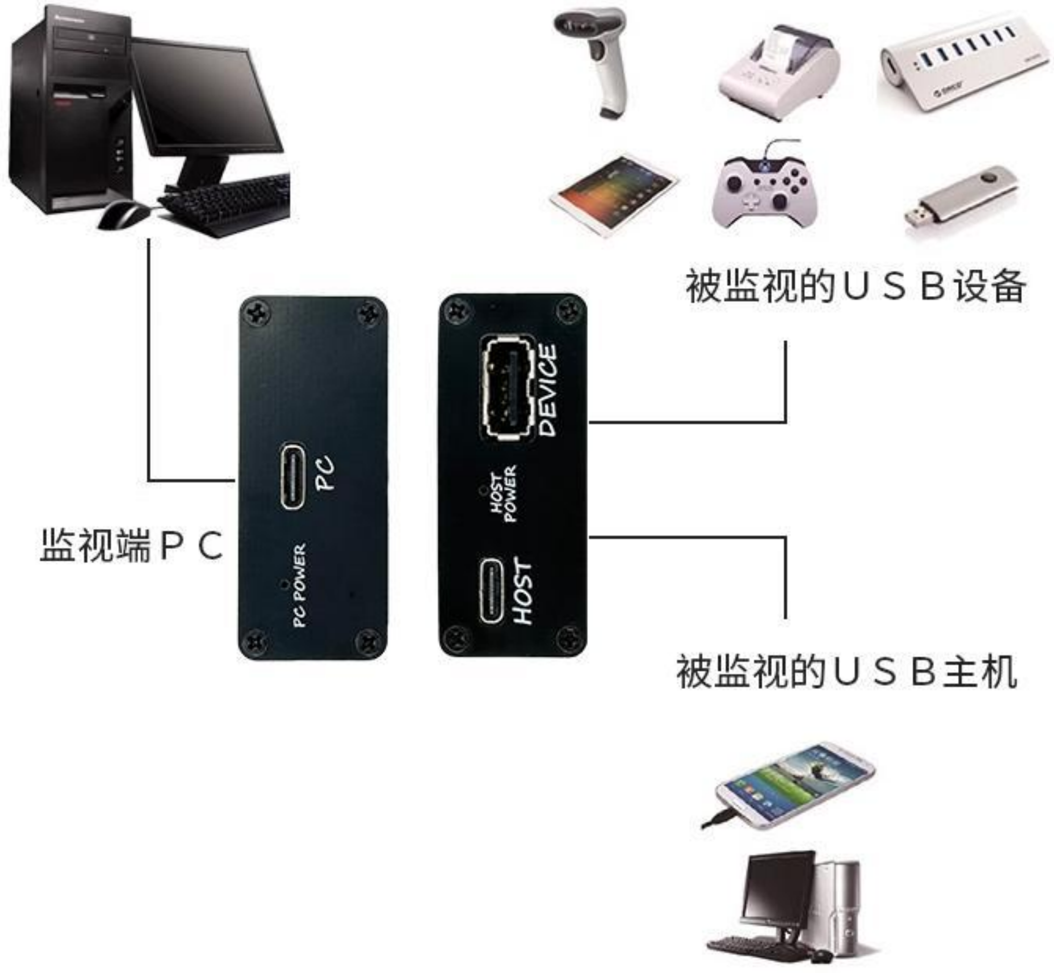
Device Overview

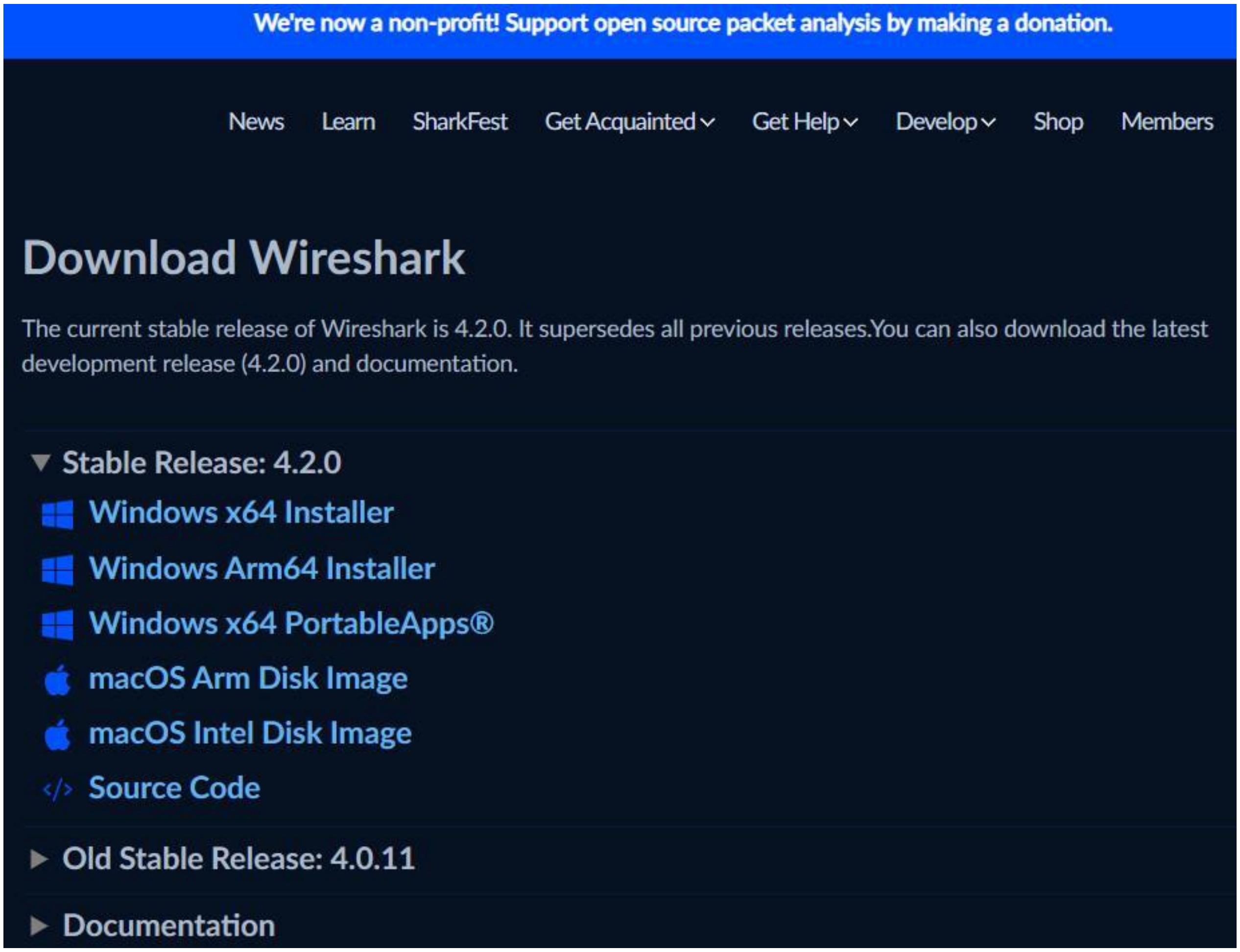
- **HOST**: The device (such as a computer or other equipment with a USB-A port) that connects to the device under test.
- **DEVICE**: The peripheral being tested, such as a USB flash drive, sound card, or camera.
- **HOST POWER**: Indicator light showing the power status of the HOST port.
- **PC**: A computer capable of running the latest version of Wireshark (version 4.0 or above).
- **PC POWER**: Indicator light showing the power status of the PC port.





1-Download wire sire
https://www.wireshark.org/download.html


被监视的ＵＳＢ设备
DEVICE
HOST POWER
PC
监视端ＰＣ
PC POWER
HOST
被监视的ＵＳＢ主机



We're now a non-profit! Support open source packet analysis by making a donation.

Download Wireshark

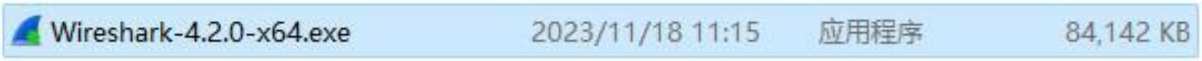
The current stable release of Wireshark is 4.2.0. It supersedes all previous releases.You can also download the latest development release (4.2.0) and documentation.

▼ Stable Release: 4.2.0

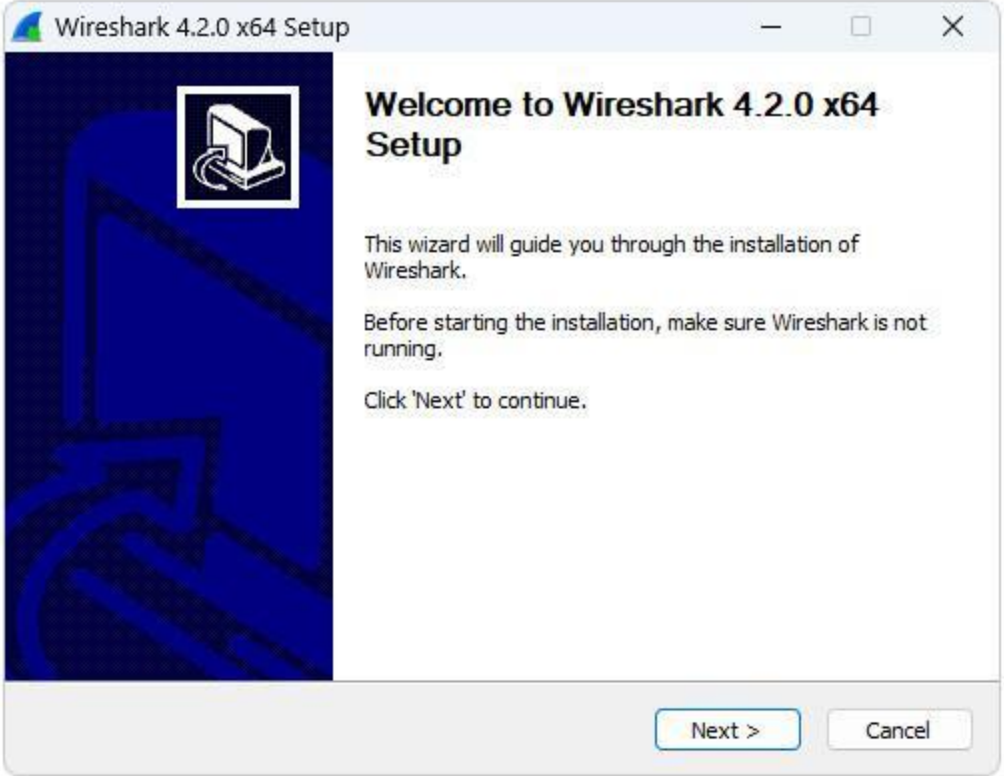
- Windows x64 Installer
- Windows Arm64 Installer
- Windows x64 PortableApps®
- macOS Arm Disk Image
- macOS Intel Disk Image
- </> Source Code

▶ Old Stable Release: 4.0.11

▶ Documentation



Wireshark-4.2.0-x64.exe 2023/11/18 11:15 应用程序 84,142 KB



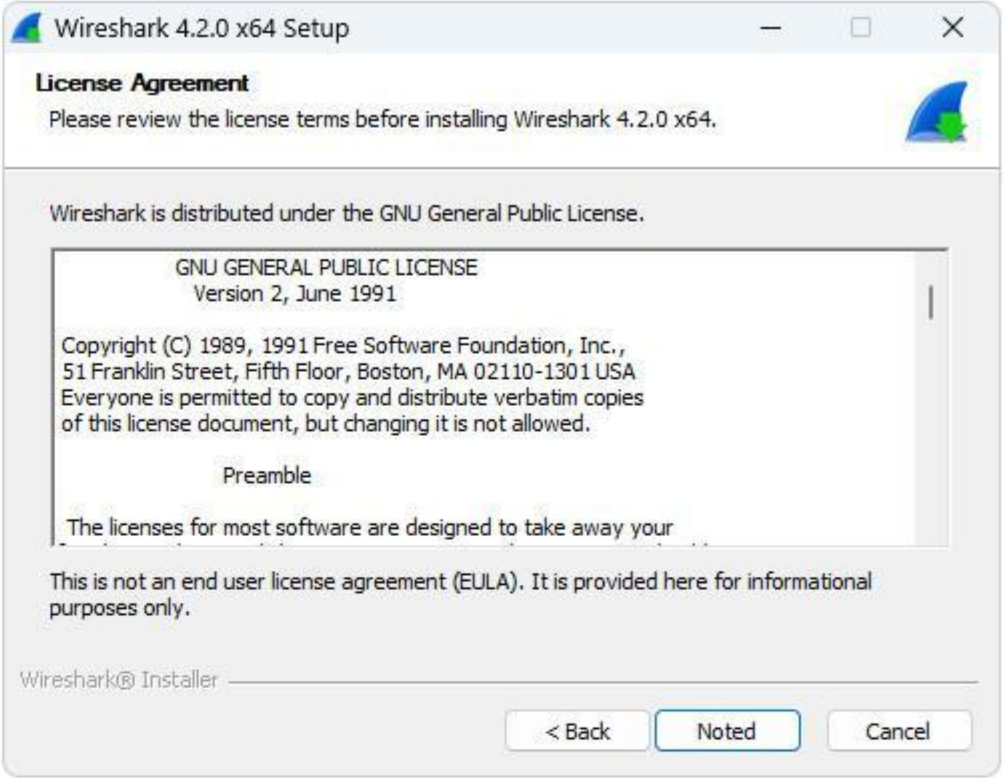
Wireshark 4.2.0 x64 Setup

Welcome to Wireshark 4.2.0 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.



Wireshark 4.2.0 x64 Setup

License Agreement

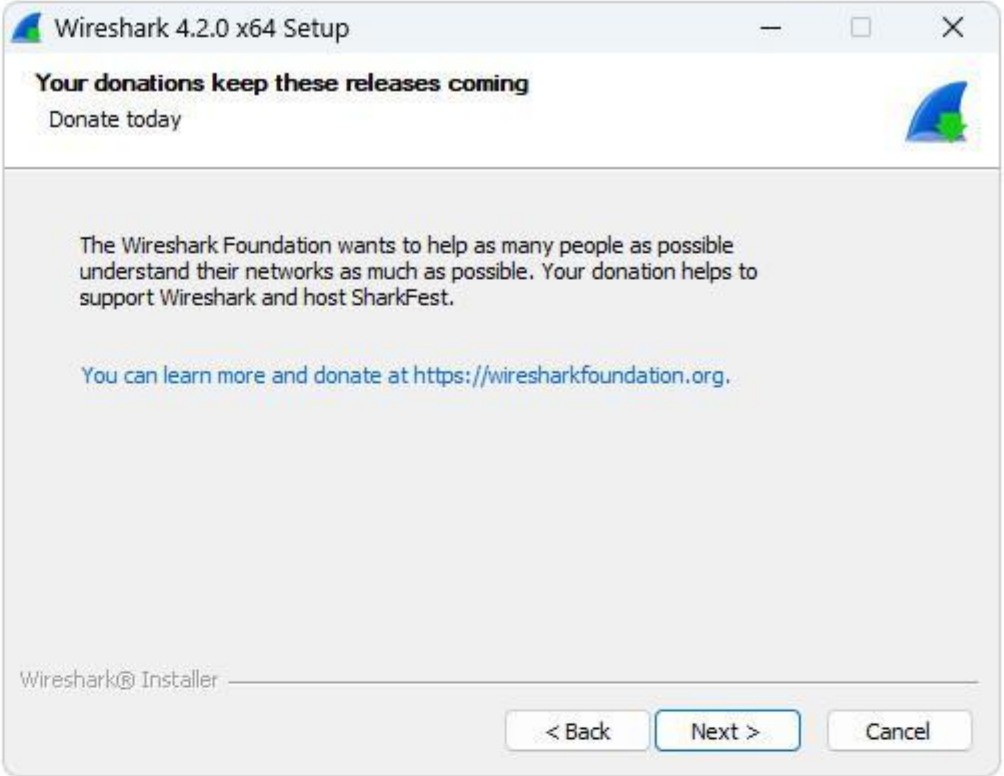
Please review the license terms before installing Wireshark 4.2.0 x64.

Wireshark is distributed under the GNU General Public License.

```
            GNU GENERAL PUBLIC LICENSE
              Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                    Preamble

 The licenses for most software are designed to take away your
```

This is not an end user license agreement (EULA). It is provided here for informational purposes only.

默认

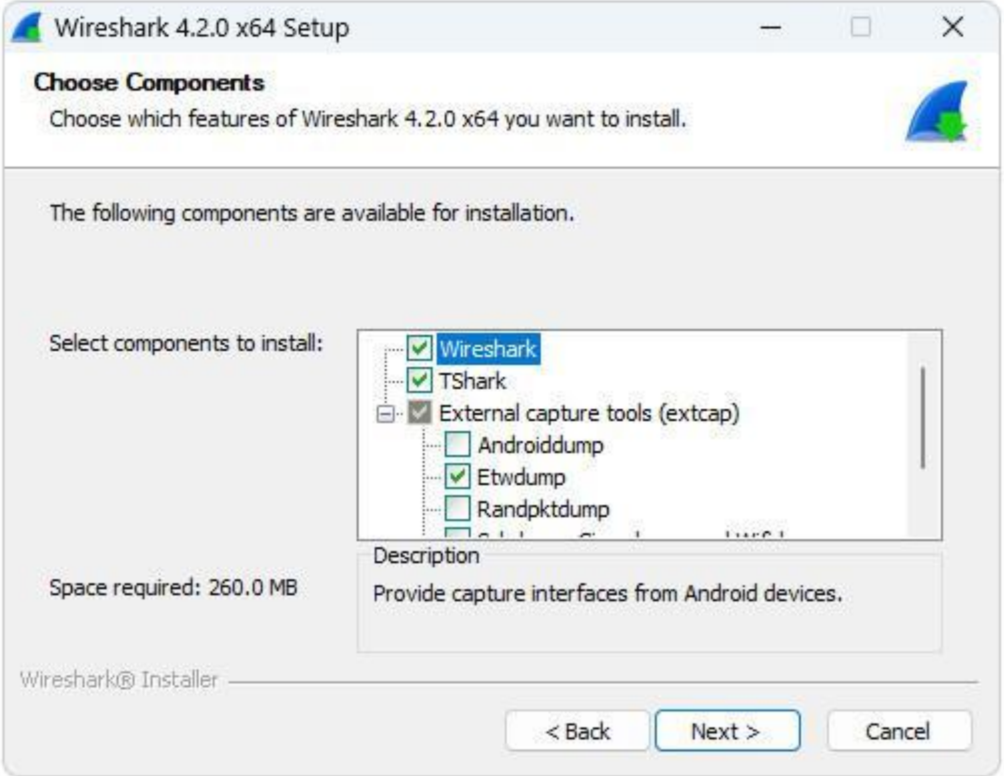


Your donations keep these releases coming

Donate today

The Wireshark Foundation wants to help as many people as possible understand their networks as much as possible. Your donation helps to support Wireshark and host SharkFest.

You can learn more and donate at https://wiresharkfoundation.org.



Choose Components

Choose which features of Wireshark 4.2.0 x64 you want to install.

The following components are available for installation.

Select components to install:

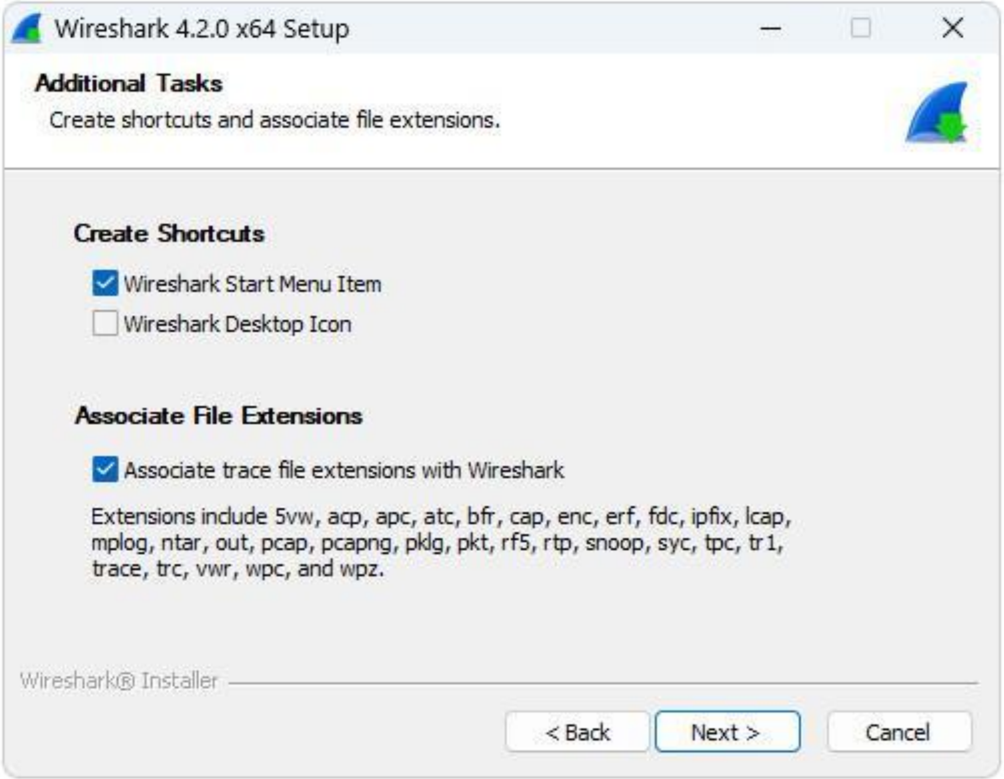
- ☑ Wireshark
- ☑ TShark
- ☑ External capture tools (extcap)
  - □ Androiddump
  - ☑ Etwdump
  - □ Randpktdump

Space required: 260.0 MB

Description

Provide capture interfaces from Android devices.

默认安装到 C 盘,少填坑



Additional Tasks

Create shortcuts and associate file extensions.

Create Shortcuts

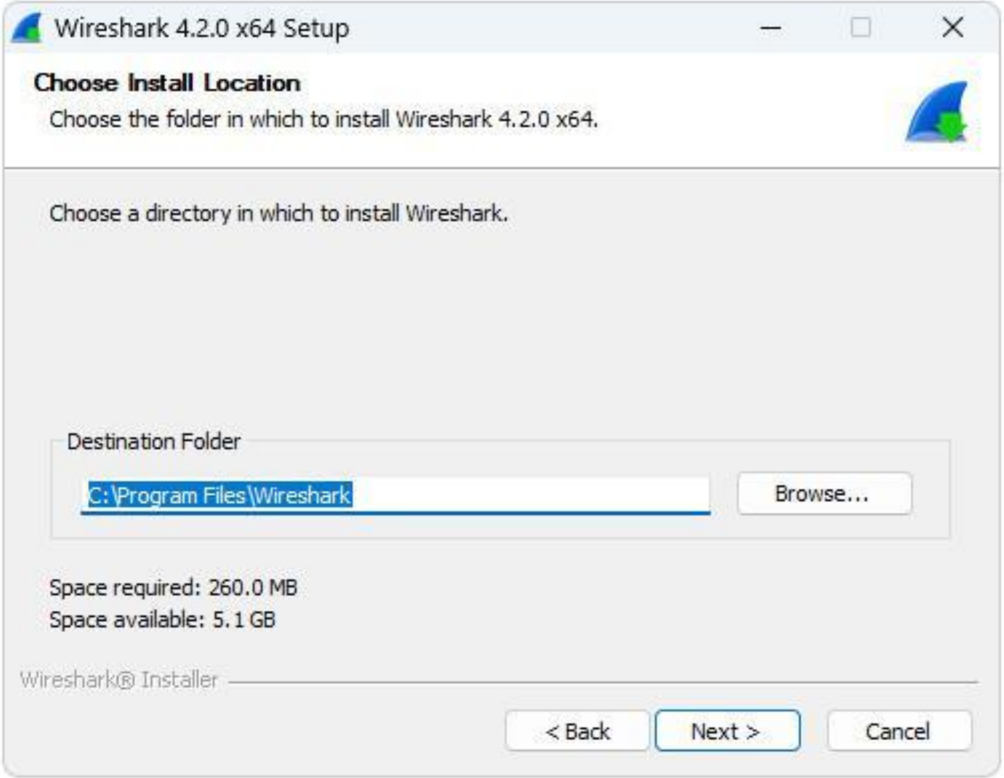
☑ Wireshark Start Menu Item

□ 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 4.2.0 x64 Setup

Choose Install Location

Choose the folder in which to install Wireshark 4.2.0 x64.

Choose a directory in which to install Wireshark.

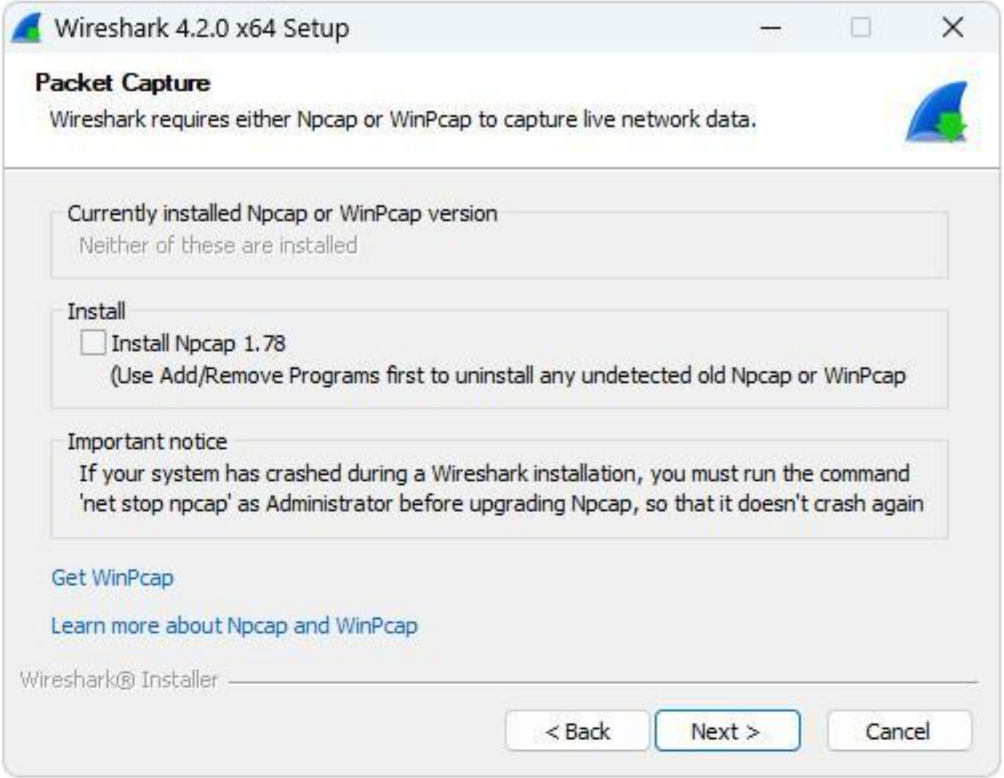
Destination Folder

C:\Program Files\Wireshark

Space required: 260.0 MB
Space available: 5.1 GB

不抓网络包的话可以不选 Npcap

我们不使用 usb 软抓包,因为我们已经有硬件抓包了.



Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap or WinPcap version

Neither of these are installed

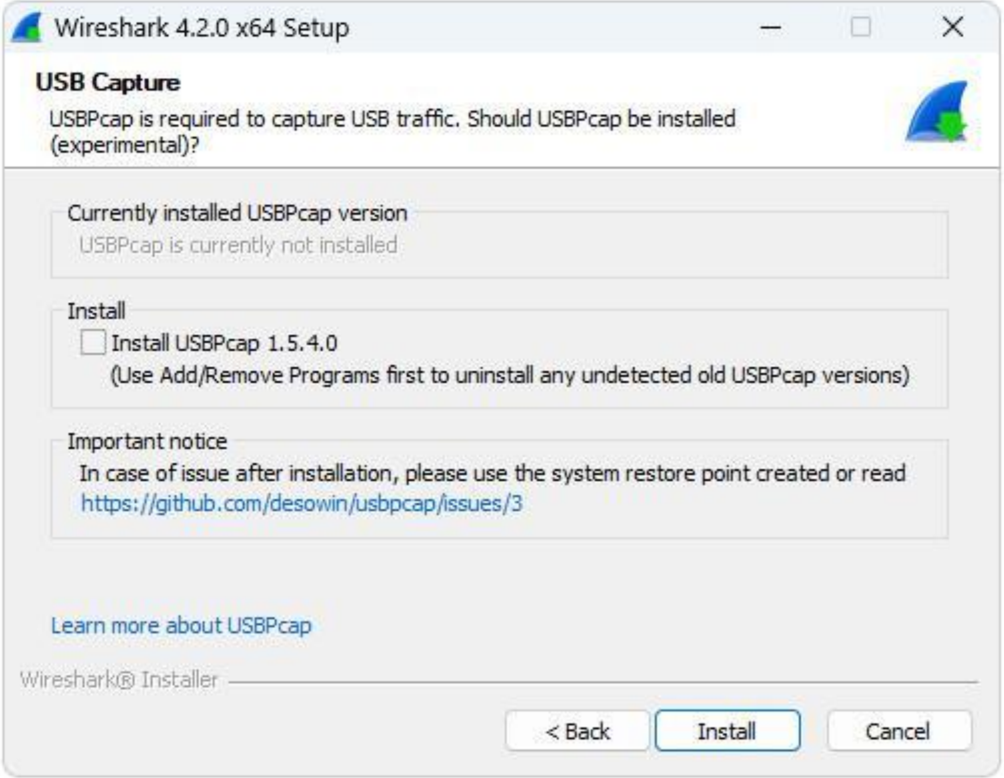
Install

□ Install Npcap 1.78

(Use Add/Remove Programs first to uninstall any undetected old Npcap or WinPcap

Important notice

If your system has crashed during a Wireshark installation, you must run the command 'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again



USB Capture

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?

Currently installed USBPcap version

USBPcap is currently not installed

Install

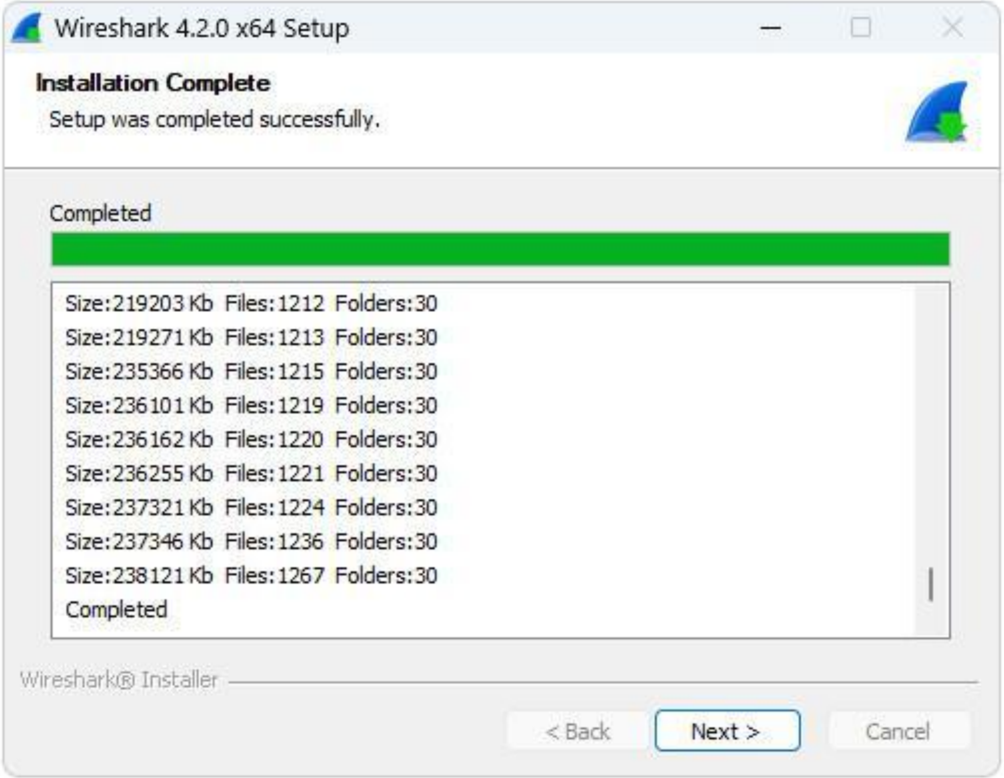
□ Install USBPcap 1.5.4.0

(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)

Important notice

In case of issue after installation, please use the system restore point created or read https://github.com/desowin/usbpcap/issues/3

2. Download usb_sniffer_win.exe from the provided Baidu Netdisk link:

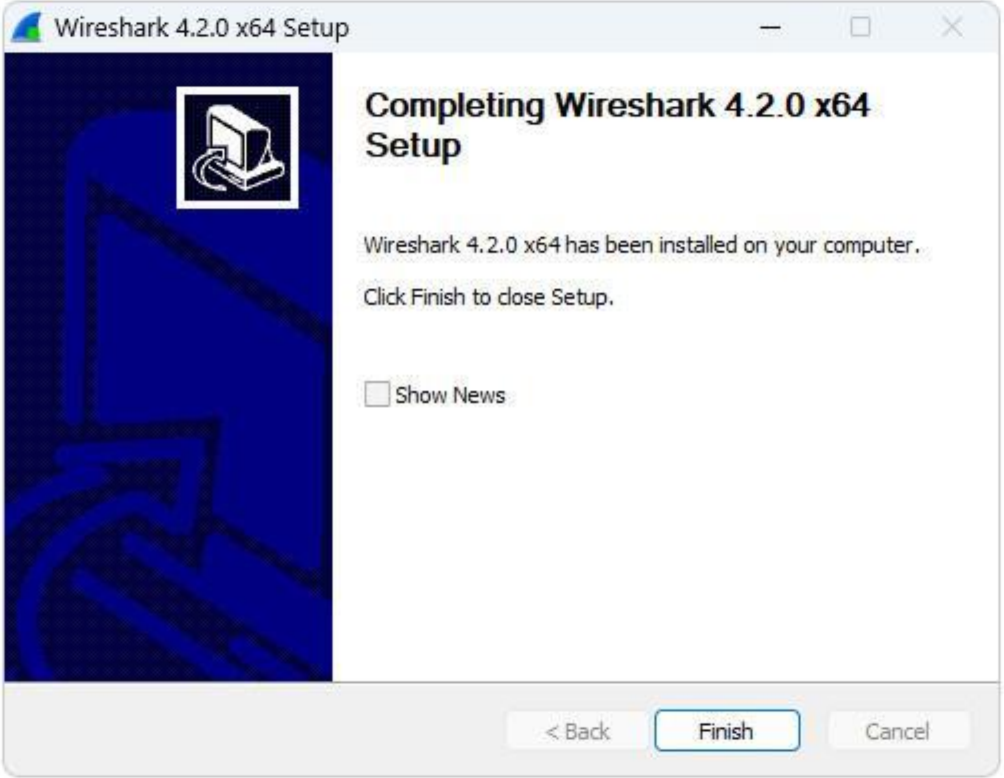


Installation Complete

Setup was completed successfully.

Completed

```
Size:219203 Kb  Files:1212  Folders:30
Size:219271 Kb  Files:1213  Folders:30
Size:235366 Kb  Files:1215  Folders:30
Size:236101 Kb  Files:1219  Folders:30
Size:236162 Kb  Files:1220  Folders:30
Size:236255 Kb  Files:1221  Folders:30
Size:237321 Kb  Files:1224  Folders:30
Size:237346 Kb  Files:1236  Folders:30
Size:238121 Kb  Files:1267  Folders:30
Completed
```



Completing Wireshark 4.2.0 x64 Setup

Wireshark 4.2.0 x64 has been installed on your computer.

Click Finish to close Setup.

□ Show News

https://pan.baidu.com/s/1_dmDVuAgBiMa6X3yIg_NlQ?pwd=usbs
Copy usb_sniffer_win.exe to the directory:

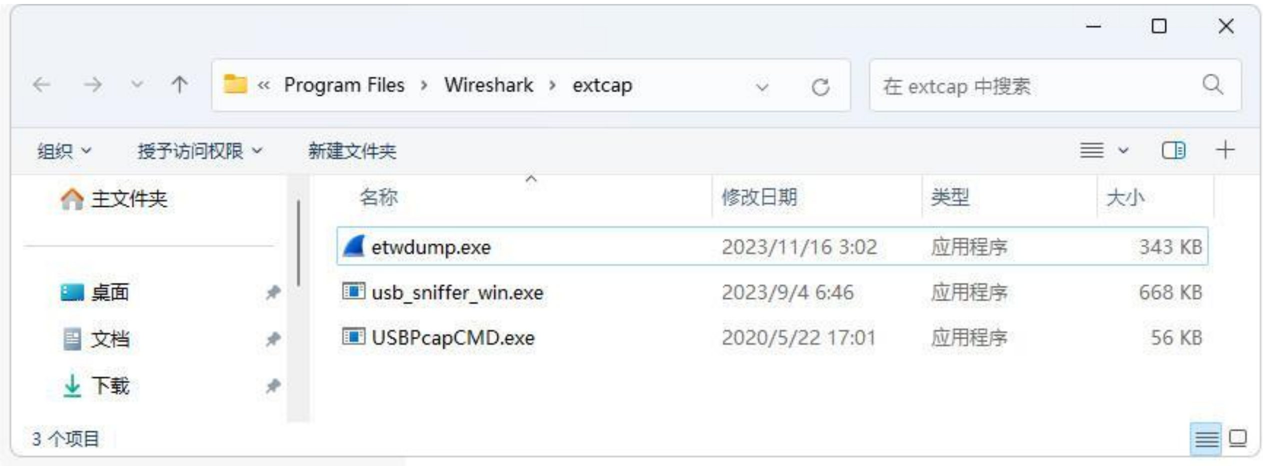
C:\Program Files\Wireshark\extcap\usb_sniffer_win.exe
If the directory does not exist, create it manually.

3. After copying, open Wireshark from the desktop icon.

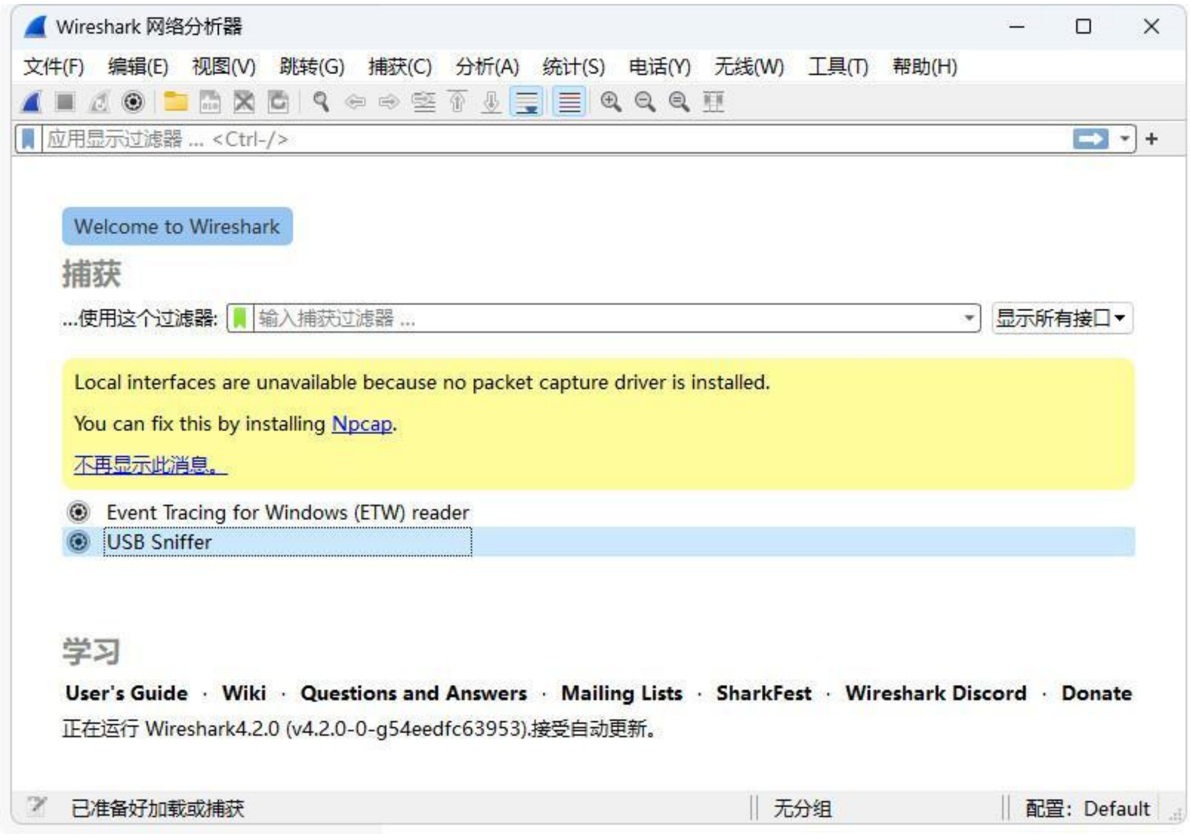
Select the "USB Sniffer" option in the capture interface. Click the gear icon to configure the sniffer.

If you do not see "USB Sniffer, usb_sniffer_win.exe " ensure the plugin was copied to the correct directory.

Configure Capture Settings



名称	修改日期	类型	大小
etwdump.exe	2023/11/16 3:02	应用程序	343 KB
usb_sniffer_win.exe	2023/9/4 6:46	应用程序	668 KB
USBPcapCMD.exe	2020/5/22 17:01	应用程序	56 KB


Wireshark 网络分析器
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
Welcome to Wireshark
显示所有接口▾
学习
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

捕获

...使用这个过滤器: 输入捕获过滤器 ...

Local interfaces are unavailable because no packet capture driver is installed.

You can fix this by installing Npcap.

不再显示此消息。

Event Tracing for Windows (ETW) reader

USB Sniffer

正在运行 Wireshark4.2.0 (v4.2.0-0-g54eedfc63953).接受自动更新。

已准备好加载或捕获 | 无分组 | 配置: Default

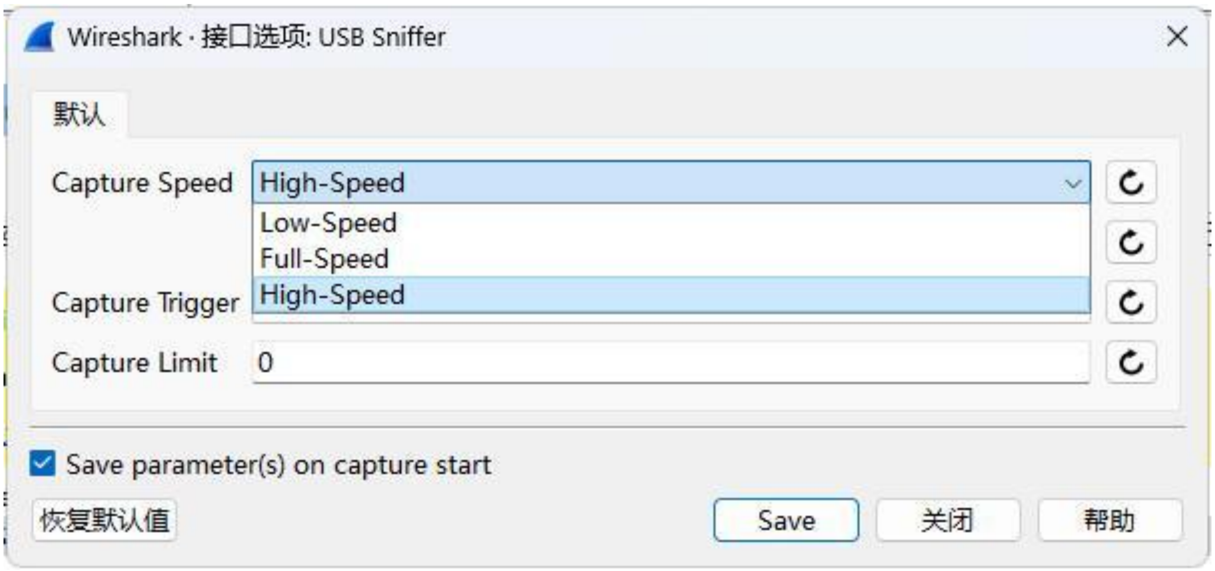
- Set the capture speed to "High-Speed" for most USB drives and cameras. For control devices like joysticks, keyboards, or USB serial devices, use "Full-Speed."

- Click "Save" to store your settings.

Connect Devices and Start Capture

- According to the first page's instructions, connect the PC and HOST interfaces. Do not connect the DEVICE interface yet—this is necessary to capture the enumeration process.

- Click the "Start" button to begin capturing. Then, insert the device (e.g., a USB flash drive) into the DEVICE port.



Wireshark · 接口选项: USB Sniffer

默认

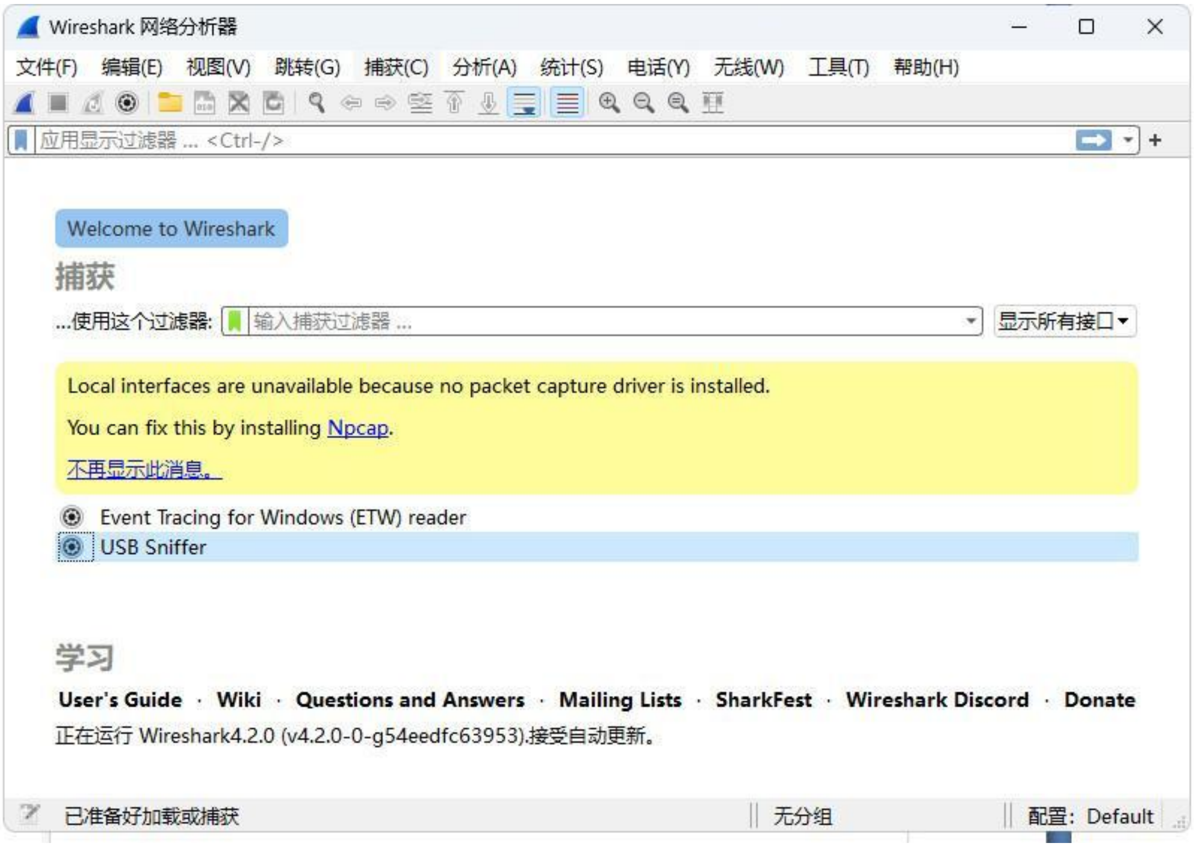
Capture Speed: High-Speed

Low-Speed
Full-Speed
High-Speed

Capture Trigger

Capture Limit: 0

☑ Save parameter(s) on capture start



Wireshark 网络分析器

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
Welcome to Wireshark

捕获

…使用这个过滤器: 输入捕获过滤器 … 显示所有接口▾

Local interfaces are unavailable because no packet capture driver is installed.

You can fix this by installing Npcap.

不再显示此消息。

Event Tracing for Windows (ETW) reader

USB Sniffer

学习

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

正在运行 Wireshark4.2.0 (v4.2.0-0-g54eedfc63953).接受自动更新。

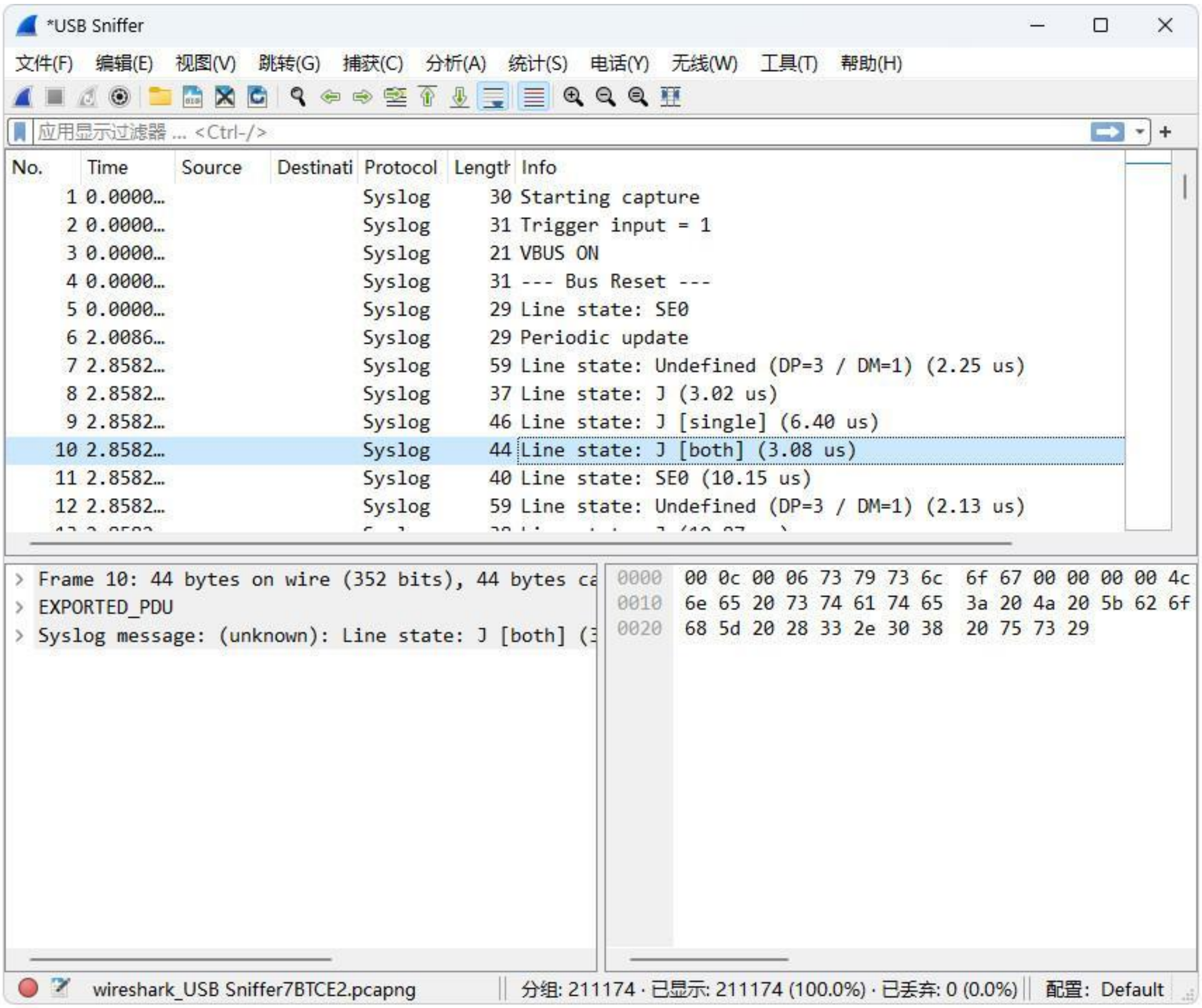
已准备好加载或捕获 | 无分组 | 配置: Default

Capture and Filter USB Traffic

- If everything is set up correctly, you should capture the complete enumeration process, including SE0, J, and K states.

- In the filter box, enter "USB" to filter out broadcast SOF, USBLL, and syslog messages, making the enumeration process clearer.

- For more advanced filtering, users can experiment with additional keywords. Typing "usb." in the filter box will provide detailed filter suggestions.

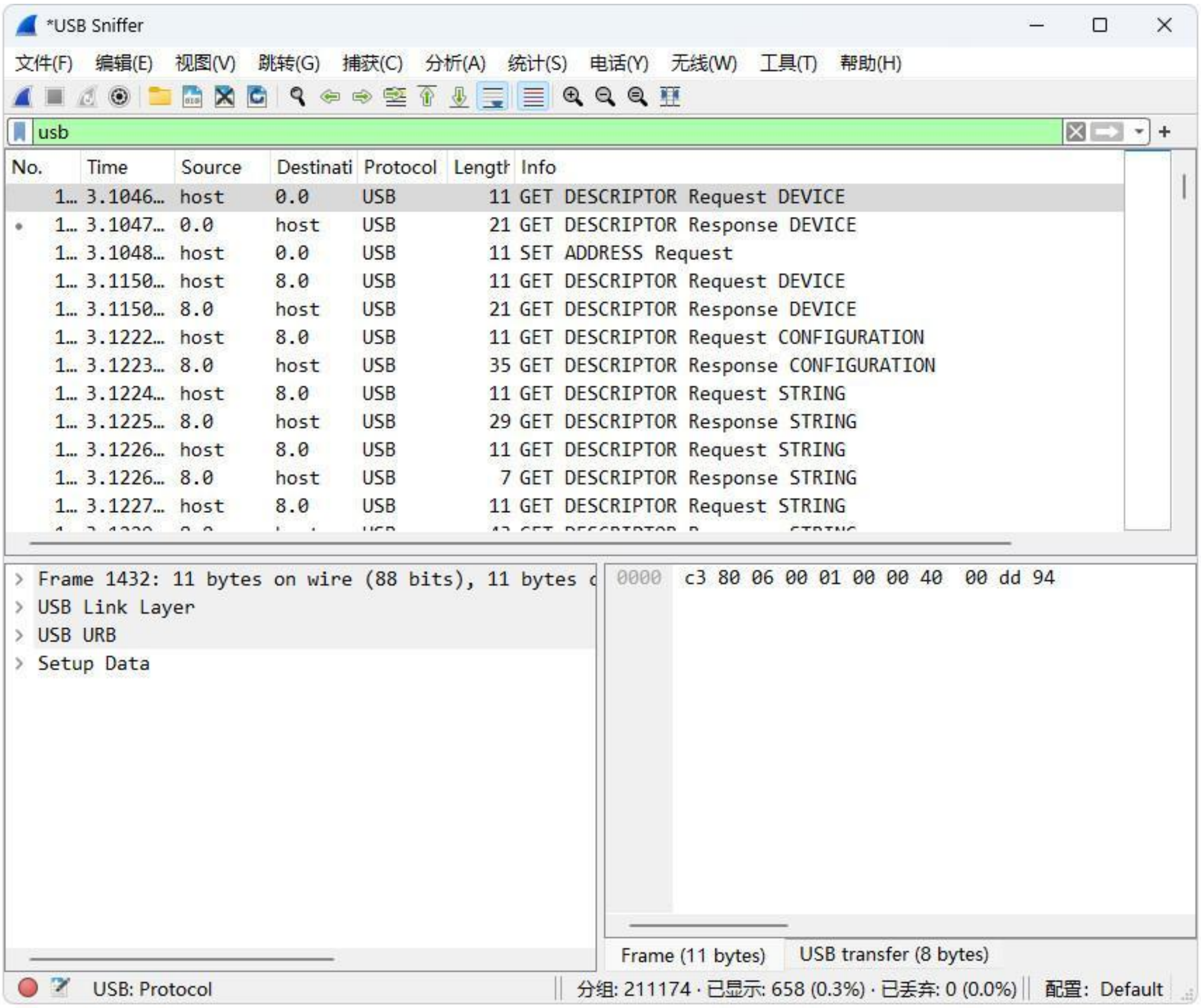


```
No.   Time       Source   Destinati Protocol  Lengtł Info
    1 0.0000...                     Syslog        30 Starting capture
    2 0.0000...                     Syslog        31 Trigger input = 1
    3 0.0000...                     Syslog        21 VBUS ON
    4 0.0000...                     Syslog        31 --- Bus Reset ---
    5 0.0000...                     Syslog        29 Line state: SE0
    6 2.0086...                     Syslog        29 Periodic update
    7 2.8582...                     Syslog        59 Line state: Undefined (DP=3 / DM=1) (2.25 us)
    8 2.8582...                     Syslog        37 Line state: J (3.02 us)
    9 2.8582...                     Syslog        46 Line state: J [single] (6.40 us)
   10 2.8582...                     Syslog        44 Line state: J [both] (3.08 us)
   11 2.8582...                     Syslog        40 Line state: SE0 (10.15 us)
   12 2.8582...                     Syslog        59 Line state: Undefined (DP=3 / DM=1) (2.13 us)
```

```
> Frame 10: 44 bytes on wire (352 bits), 44 bytes ca
> EXPORTED_PDU
> Syslog message: (unknown): Line state: J [both] (3
```

```
0000  00 0c 00 06 73 79 73 6c  6f 67 00 00 00 00 4c
0010  6e 65 20 73 74 61 74 65  3a 20 4a 20 5b 62 6f
0020  68 5d 20 28 33 2e 30 38  20 75 73 29
```

wireshark_USB Sniffer7BTCE2.pcapng | 分组: 211174 · 已显示: 211174 (100.0%) · 已丢弃: 0 (0.0%) | 配置: Default



usb

No.	Time	Source	Destinati	Protocol	Length	Info
1…	3.1046…	host	0.0	USB	11	GET DESCRIPTOR Request DEVICE
1…	3.1047…	0.0	host	USB	21	GET DESCRIPTOR Response DEVICE
1…	3.1048…	host	0.0	USB	11	SET ADDRESS Request
1…	3.1150…	host	8.0	USB	11	GET DESCRIPTOR Request DEVICE
1…	3.1150…	8.0	host	USB	21	GET DESCRIPTOR Response DEVICE
1…	3.1222…	host	8.0	USB	11	GET DESCRIPTOR Request CONFIGURATION
1…	3.1223…	8.0	host	USB	35	GET DESCRIPTOR Response CONFIGURATION
1…	3.1224…	host	8.0	USB	11	GET DESCRIPTOR Request STRING
1…	3.1225…	8.0	host	USB	29	GET DESCRIPTOR Response STRING
1…	3.1226…	host	8.0	USB	11	GET DESCRIPTOR Request STRING
1…	3.1226…	8.0	host	USB	7	GET DESCRIPTOR Response STRING
1…	3.1227…	host	8.0	USB	11	GET DESCRIPTOR Request STRING

```
> Frame 1432: 11 bytes on wire (88 bits), 11 bytes c
> USB Link Layer
> USB URB
> Setup Data
```

```
0000   c3 80 06 00 01 00 00 40  00 dd 94
```

USB: Protocol

分组: 211174 · 已显示: 658 (0.3%) · 已丢弃: 0 (0.0%)

配置: Default