Windows USB 网卡空口抓包说明（V1.5）

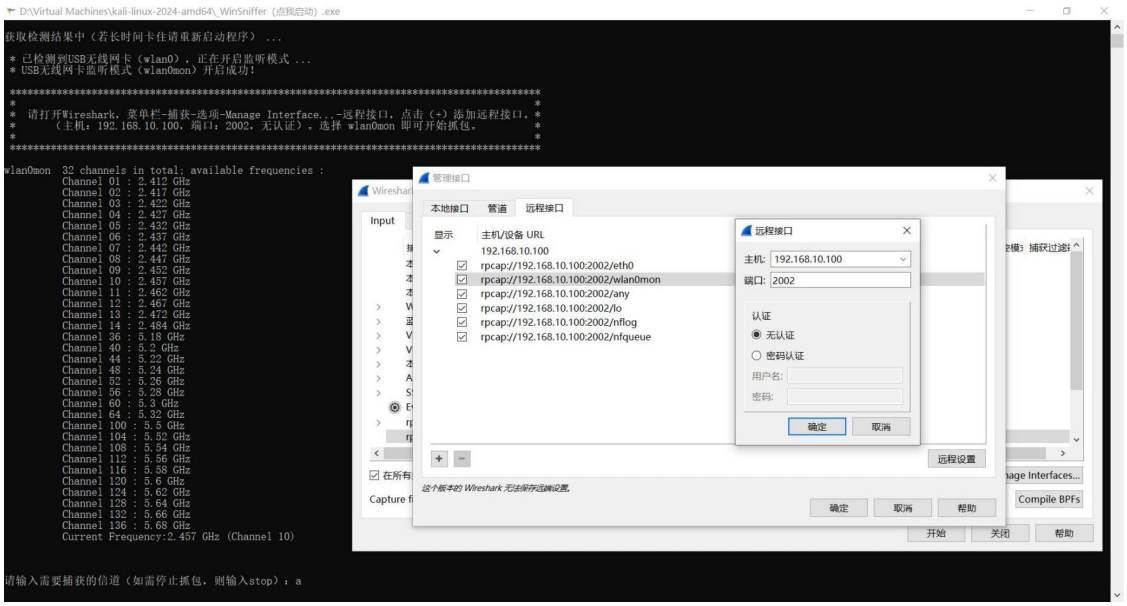
更新时间：2025.01.03　　作者：网洞（闲鱼名：网洞在线）

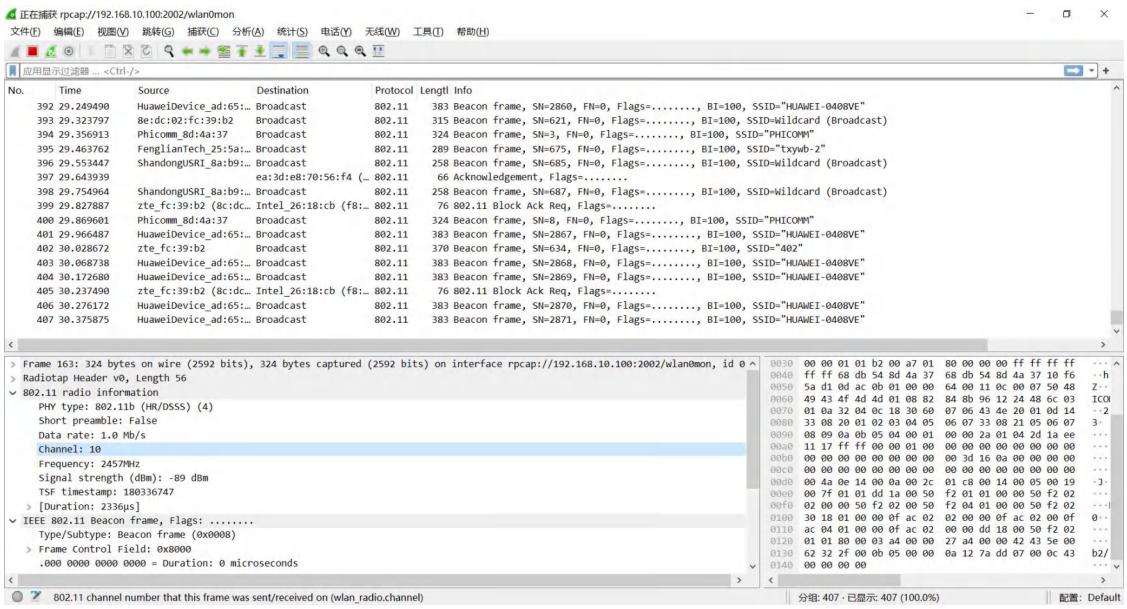
1 前言

~~PS：不想看废话可以直接跳到第三节看安装使用。~~

Windows 空口抓包的难点在于 Windows 下的网卡原生驱动都是不支持开启网卡监听模式的，而 Linux 下的原生驱动大多支持开启网卡监听模式，如果能将 Linux 中的驱动“移植”到 Windows 系统中，那就能很好解决这个问题。

根据此构想，笔者实现了一种简易、低成本、适用性广的 Windows 下空口抓包方案。通过 VMware 虚拟机启用一个 Kali 虚拟机，在 Kali 下开启无线网卡的监听模式，并使用 rpcapd 暴露虚拟机中的网卡接口，最后在 Windows 下使用 Wireshark 的远程抓包功能即可实现空口抓包。





这个方案相比 Omnipeek 抓包方案更为方便，不需要再去安装特殊的无线驱动，能做到即插即用，搭配使用免费的抓包软件 Wireshark 即可进行抓包。

同时笔者编写了一个 C#程序用于无 GUI 启动虚拟机和抓包参数设置，能做到傻瓜式操作，使用简单易上手。程序无需安装，开箱即用，只要电脑上安装了 VMware，笔者的程序就可以使用。由于是运行在虚拟机中，理论上支持 Win7/Win10/Win11 所有系统。

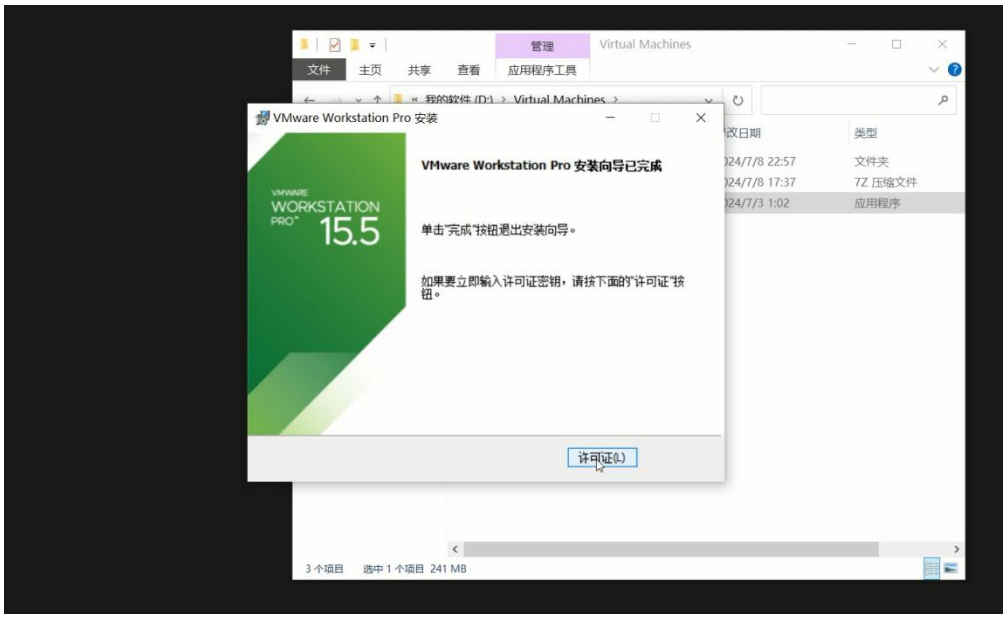
2 空口抓包操作

整体使用分三步：安装 VMware 虚拟机（如已安装直接跳过），启动 WinSniffer 程序并设置需要捕获的信道，使用 Wireshark 连接无线接口进行抓包。

- **视频教程：**https://www.bilibili.com/video/BV1s1ateZEWP/
- **程序链接 1（123 云盘）：**https://www.123pan.com/s/rzBKVv-CvUP3.html 提取码：wdzx
- **程序链接 2（百度云盘）：**https://pan.baidu.com/s/1jvwskVyWh0UOszbhwvqIOA?pwd=wdzx 提取码：wdzx
- 程序下载链接二选一即可。USB 无线抓包网卡和程序解压码到闲鱼搜“网洞在线”找到我可以提供：https://m.tb.cn/h.g7RIm0D?tk=TgSV3bWHWbA

2.1 安装 VMware 虚拟机

1. 安装 VMware 虚拟机,，这个没啥好说的，网上都资料很多，下载官方安装版，安装完找一个注册码激活即可。可以使用笔者提供的软件包，软件安装完可以自动激活，不需要手动填注册码。需要注意的是 **VMware 版本推荐使用高版本如 17.5（注意 Win7 系统最高只支持 15.5 版本）**，高版本 Bug 少。（之前有网友使用 16 版本有无法启动虚拟机/抓包漏包的情况）



2.2 启动 WinSniffer 程序

1. 把 WinSniffer 程序解压出来，找到 **WinSniffer.exe** 文件（如果启用了 Windows Defender 可能会把这个文件误杀删掉，需要信任下）。右键这个文件选择**属性**，点击**兼容性**选项卡，勾选**以管理员身份运行此程序**，确定保存。

2. 点击 **WinSniffer.exe** 程序启动即可，它会在无 GUI 模式下开启 Kali 虚拟机（注意文件路径不能含有中文，否则启动会报错）。

   PS：如果程序运行后显示**“虚拟机启动失败！”**，进入 kali-linux-2024-amd64 文件夹，双击.vmx 后缀的文件，使用 VMware 打开虚拟机，然后启动运行虚拟机查看有什么报错。

   （常见启动失败原因：路径有中文/BIOS 未启动虚拟化等）

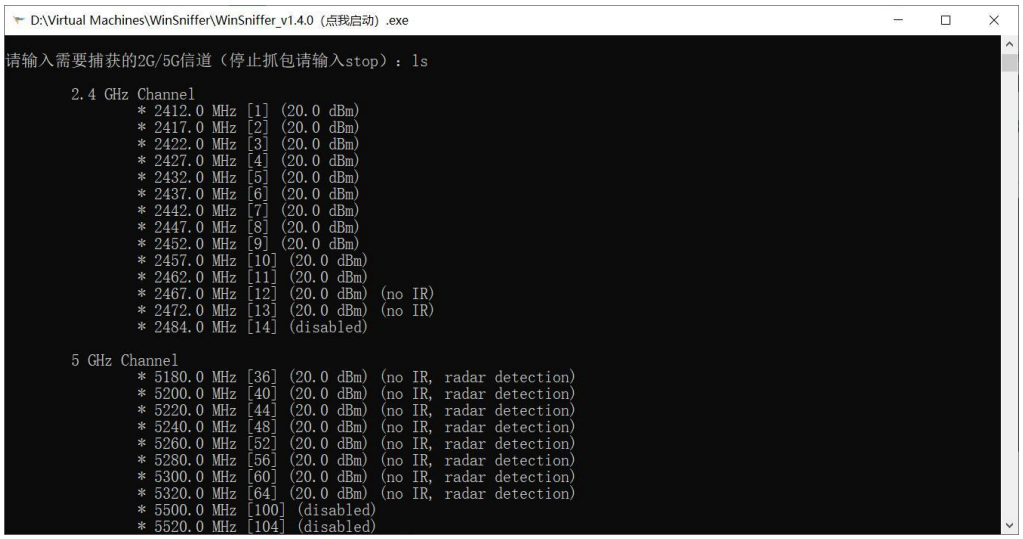
   如遇到报错“VMware Workstation 不可恢复错误: (vcpu-0) Exception 0xc0000005 (access violation) has occurred.”

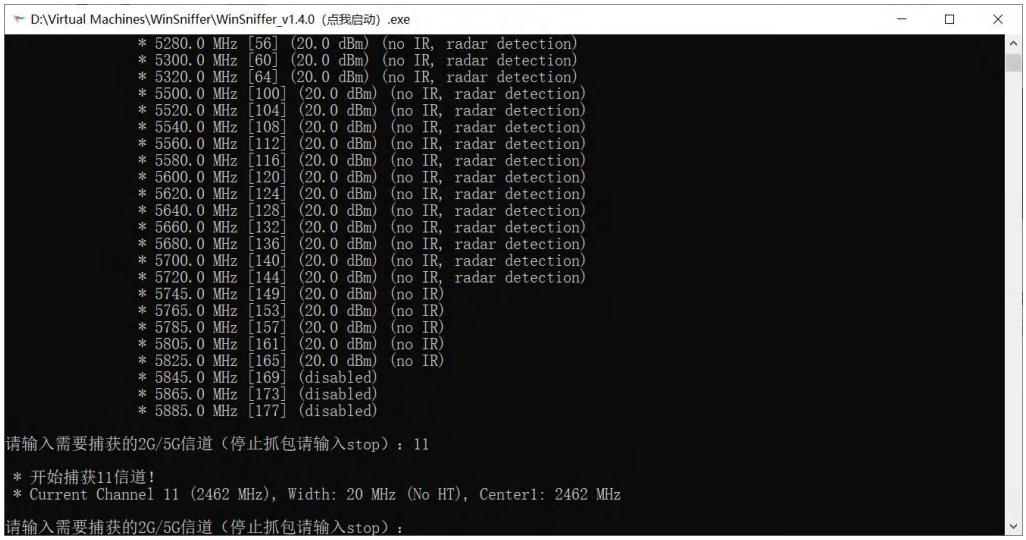
   参考解决方案：https://www.jb51.net/article/271136.htm

3. 虚拟机从启动到连接大概需要几十秒到一分钟不等（跟电脑性能等因素有关），虚拟机启动完会检测 USB 网卡有没有接入，如果接入了会开启网卡的监听模式。

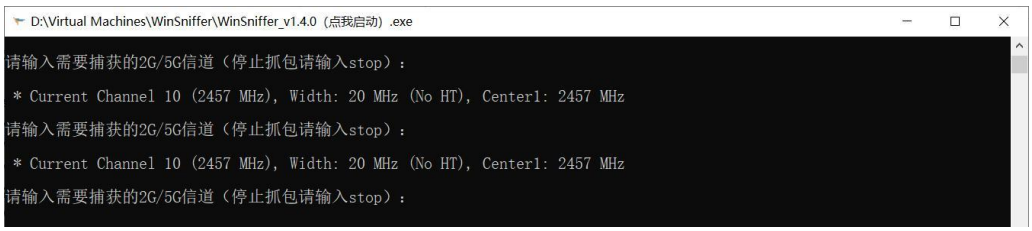
如果是程序启动前就接好了网卡，启动完就能识别到。如果程序启动后再接入网卡，有的网卡识别慢（如 MT7921）可能会需要再等待几十秒到一分多钟时间，期间可以通过一直按回车键获取网卡检测状态。

4. 根据自己需要设置想要捕获的信道即可，如输入 1 并回车则捕获 1 信道。可以输入 **listch（快捷命令 ls）**查看网卡的信道支持情况。



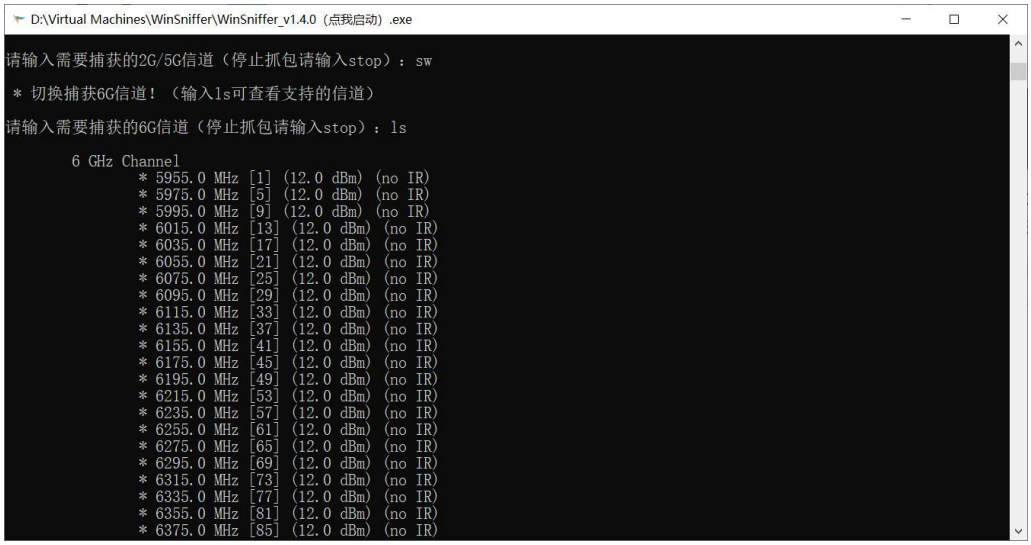


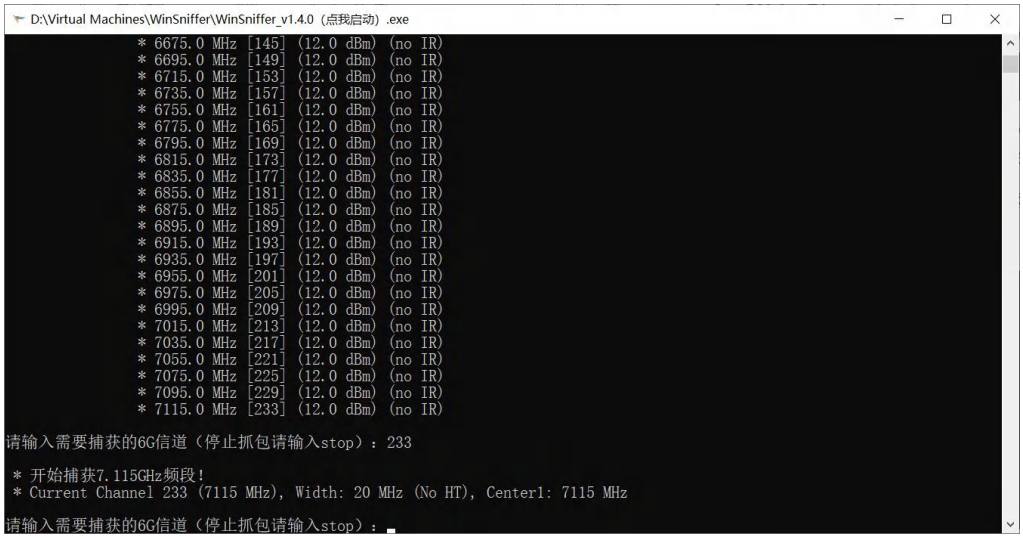
5. **补充说明 1**：目前内置了一些简单的命令，输入 **help（快捷命令 h）**可以查询到命令说明，如输入 **status（快捷命令直接敲回车）**是查看当前捕获的信道。



6. **补充说明 2**：如果需要**捕获 6G 报文**，先输入 **switch（快捷命令 sw）**切换捕获 6G 频段，再根据需要输入想要捕获的 6G 信道即可（可输入 **ls** 查看有哪些 6G 信道）。

   注意：抓 6G 报文需要网卡支持，要用到 **WiFi6E** 及以上的网卡，目前测试可用的网卡是 **MT7921** 芯片的网卡（后文有收录相关网卡）。

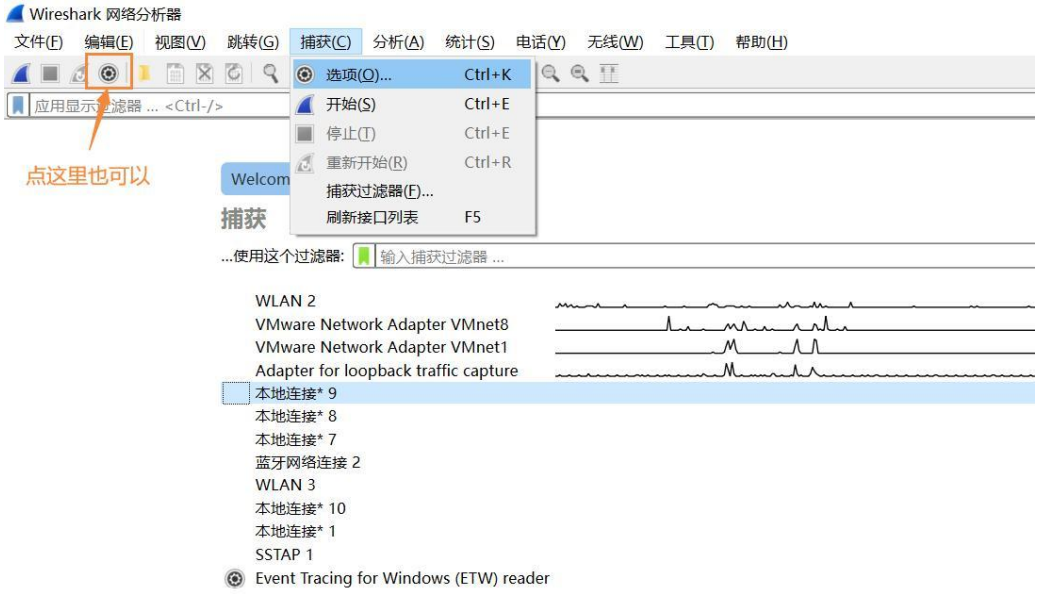


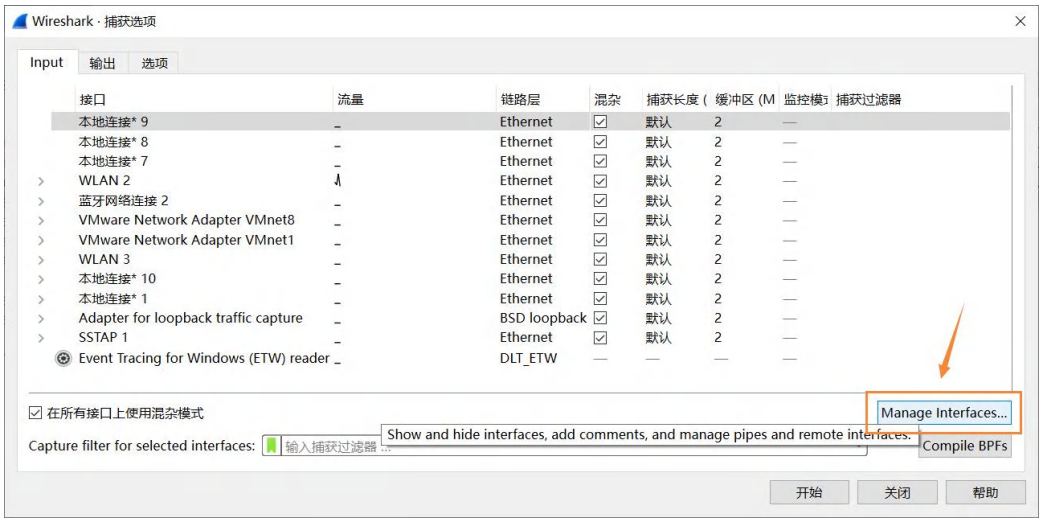


2.3 使用 Wireshark 抓包

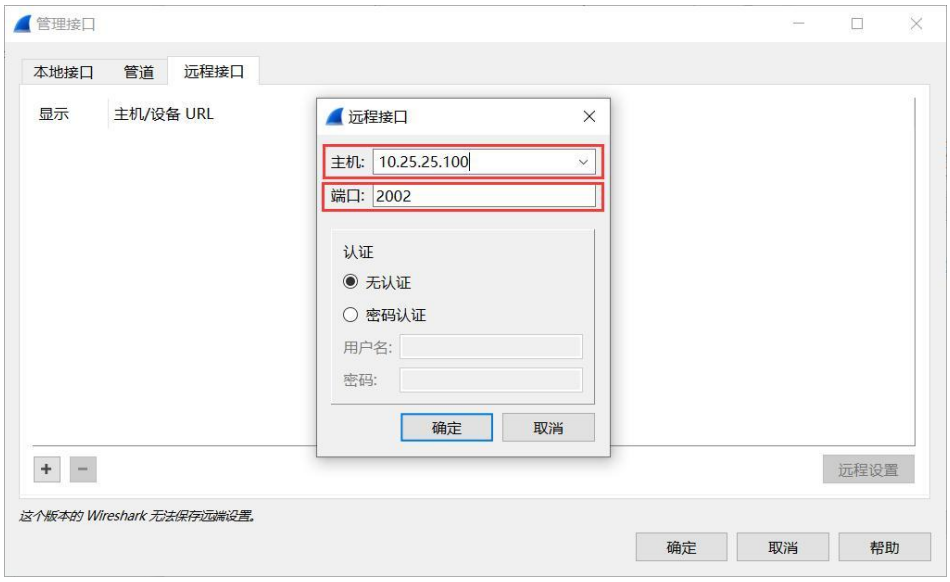
1. 打开 **Wireshark**（可以使用笔者提供的安装包，也可以到官网下载 https://www.wireshark.org/）

   点击**捕获-选项，管理接口（Manage Interface...）-远程接口。**

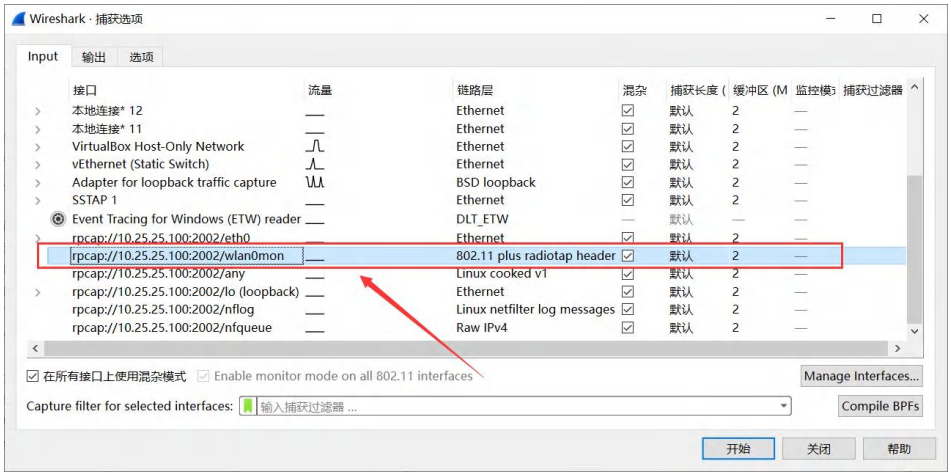


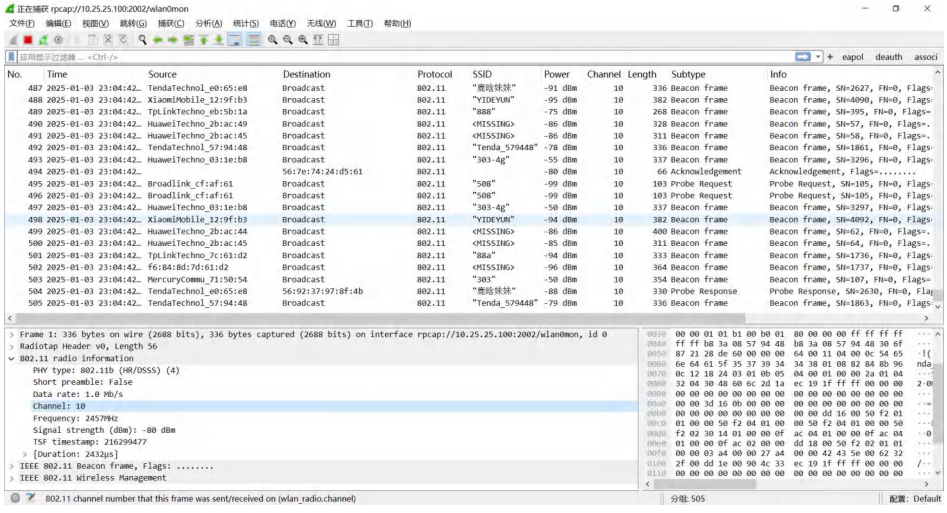


2. 点击加号（+）添加远程接口，**主机填 192.168.10.100，端口 2002**，无认证，确定即可（设置过一次后面就不用设置了）。

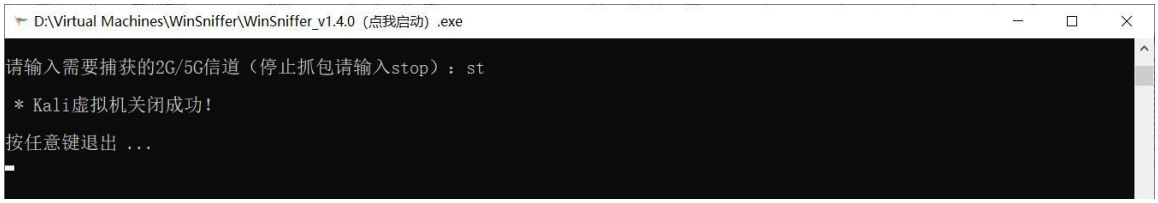


3. 点击选择 **wlan0mon（如没有则选 wlan0）**即可开始抓包。





补充说明：前面程序的命令行窗口是可以关闭的，关闭不影响抓包，重新打开再设置信道也可以。如果不需要抓包记得输入 **stop（快捷命令 st）**将虚拟机关闭。



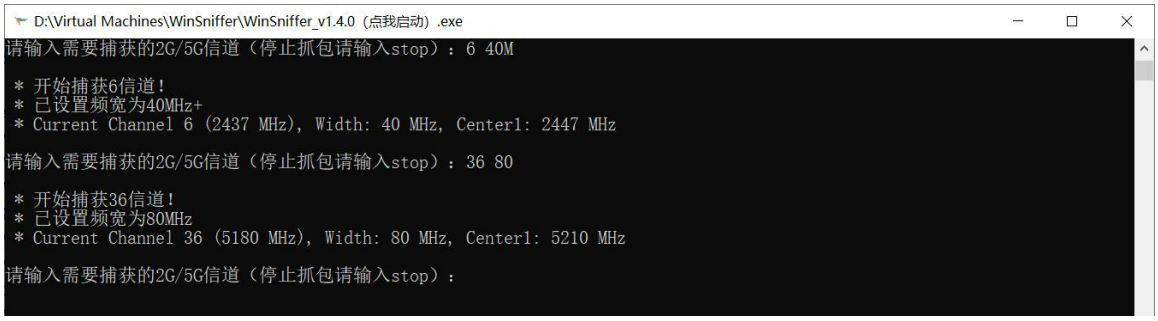
2.4 补充说明

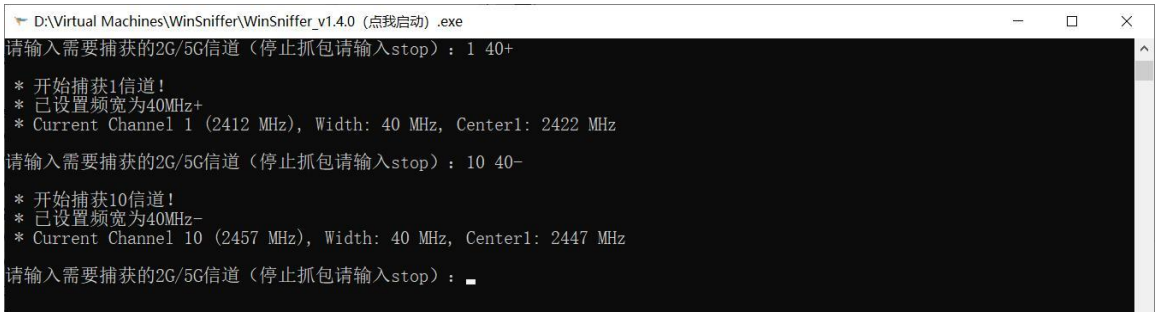
2.4.1 WinSniffer 内置命令说明

2.4.1.1 设置捕获频宽

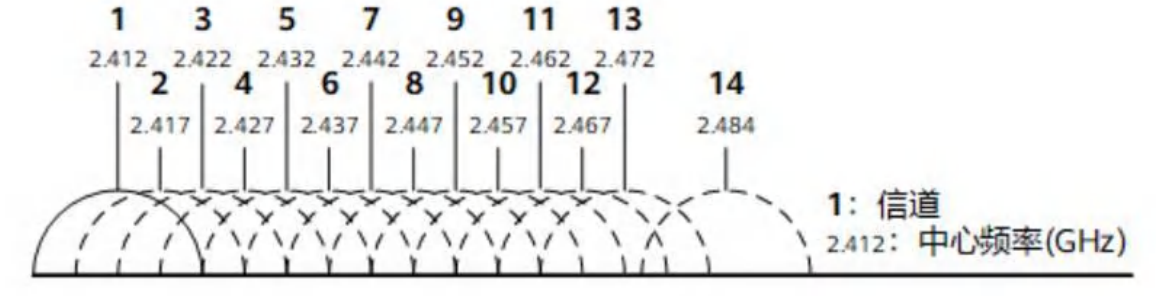
单信道模式下，在信道后加 20M/40M/80M/160M 后缀可设置捕获频宽（后面的 M 可以省略不写）

- **1 20M**：捕获 1 信道，捕获频宽为 20M。
- **6 40M+**：捕获 6 信道，捕获频宽为 40M（辅信道在上）。
- **10 40M-**：捕获 10 信道，捕获频宽 40M（辅信道在下）。
- **36 80M**：捕获 36 信道，捕获频宽 80M





注意频宽 40M 比较特殊，是由两个独立的 20M 信道绑定而成，根据绑定情况有两种情况，40M+和 40M-。40M+为辅信道在主信道上，40M-为辅信道在主信道下。（如：1 40M+为主信道 1 加辅信道 5；10 40-为主信道 10 加辅信道 6）



信道与频宽测试支持情况参考（示例为 mt7921u、rtl8811cu 和 rtl8812bu 三种芯片）：

00	mt7921				rtl8811cu				rtl8812bu			
2.4G	NOHT	20MHz	40MHz-	40MHz+	NOHT	20MHz	40MHz-	40MHz+	NOHT	20MHz	40MHz-	40MHz+
1	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK
2	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK
3	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK
4	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK
5	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
7	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
8	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
9	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
10	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*
11	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*
12	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*
13	OK	OK	OK	NOK*	OK	OK	OK	NOK*	OK	OK	OK	NOK*
14	OK	NOK	NOK*	NOK*	NOK***	NOK***	NOK***	NOK***	NOK***	NOK***	NOK***	NOK***

00	mt7921						rt18811cu						rt18812bu			
5G	NOHT	20MHz	40MHz-	40MHz+	80MHz	160MHz	NOHT	20MHz	40MHz-	40MHz+	80MHz	160MHz	NOHT	20MHz	40MHz-	40MHz+
36	OK	OK	NOK*	OK	OK		OK	OK	NOK*	OK	OK		OK	OK	NOK*	OK
40	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
44	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
48	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
52	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
56	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
60	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
64	OK	OK	OK	NOK*	OK		OK	OK	OK	NOK*	OK		OK	OK	OK	NOK*
100	OK	OK	NOK*	OK	OK		OK	OK	NOK*	OK	OK		OK	OK	NOK*	OK
104	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
108	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
112	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
116	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
120	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
124	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
128	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
132	OK	OK	OK	OK	OK		OK	OK	OK	OK	NOK*		OK	OK	OK	OK
136	OK	OK	OK	OK	OK		OK	OK	OK	OK	NOK*		OK	OK	OK	OK
140	OK	OK	OK	OK	OK		OK	OK	OK	NOK*	NOK*		OK	OK	OK	NOK*
144	OK	OK	OK	NOK*	OK		NOK***	NOK***	NOK***	NOK***	NOK***		NOK***	NOK***	NOK***	NOK***
149	OK	OK	NOK*	OK	OK		OK	OK	NOK*	OK	OK		OK	OK	NOK*	OK
153	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
157	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
161	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK		OK	OK	OK	OK
165	OK	OK	OK	NOK*	NOK		OK	OK	OK	NOK*	NOK		OK	OK	OK	NOK*
169	NOK***	NOK***	NOK***	NOK***	NOK***		NOK***	NOK***	NOK***	NOK***	NOK***		NOK***	NOK***	NOK***	NOK***
173	NOK***	NOK***	NOK***	NOK***	NOK***		NOK***	NOK***	NOK***	NOK***	NOK***		NOK***	NOK***	NOK***	NOK***
177	NOK***	NOK***	NOK***	NOK***	NOK***		NOK***	NOK***	NOK***	NOK***	NOK***		NOK***	NOK***	NOK***	NOK***

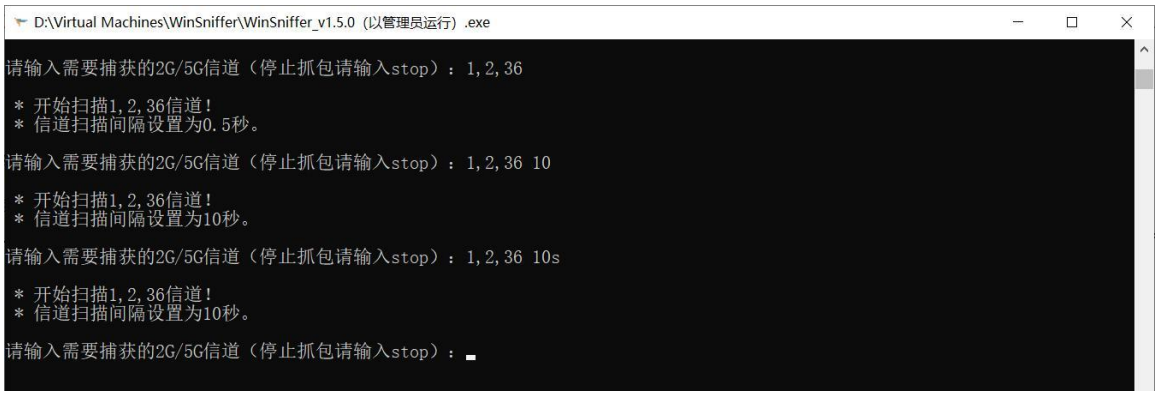
		US	mt7921						
		6G	NOHT	20MHz	40MHz-	40MHz+	80MHz	160MHz	320MHz
UNII-5	5955	1	OK	OK	NOK*	OK	OK		
	5975	5	OK	OK	OK	OK	OK		
	5995	9	OK	OK	OK	OK	OK		
	6015	13	OK	OK	OK	OK	OK		
	6035	17	OK	OK	OK	OK	OK		
	6055	21	OK	OK	OK	OK	OK		
	6075	25	OK	OK	OK	OK	OK		
	6095	29	OK	OK	OK	OK	OK		
	6115	33	OK	OK	OK	OK	OK		
	6135	37	OK	OK	OK	OK	OK		
	6155	41	OK	OK	OK	OK	OK		
	6175	45	OK	OK	OK	OK	OK		
	6195	49	OK	OK	OK	OK	OK		
	6215	53	OK	OK	OK	OK	OK		
	6235	57	OK	OK	OK	OK	OK		
	6255	61	OK	OK	OK	OK	OK		
	6275	65	OK	OK	OK	OK	OK		
	6295	69	OK	OK	OK	OK	OK		
	6315	73	OK	OK	OK	OK	OK		
	6335	77	OK	OK	OK	OK	OK		
	6355	81	OK	OK	OK	OK	OK		
	6375	85	OK	OK	OK	OK	OK		
	6395	89	OK	OK	OK	OK	OK		
	6415	93	OK	OK	OK	OK	OK		
UNII-6	6435	97	OK	OK	OK	OK	OK		
	6455	101	OK	OK	OK	OK	OK		
	6475	105	OK	OK	OK	OK	OK		
	6495	109	OK	OK	OK	OK	OK		
	6515	113	OK	OK	OK	OK	OK		
UNII-7	6535	117	OK	OK	OK	OK	OK		
	6555	121	OK	OK	OK	OK	OK		
	6575	125	OK	OK	OK	OK	OK		
	6595	129	OK	OK	OK	OK	OK		
	6615	133	OK	OK	OK	OK	OK		
	6635	137	OK	OK	OK	OK	OK		
	6655	141	OK	OK	OK	OK	OK		
	6675	145	OK	OK	OK	OK	OK		
	6695	149	OK	OK	OK	OK	OK		
	6715	153	OK	OK	OK	OK	OK		
	6735	157	OK	OK	OK	OK	OK		
	6755	161	OK	OK	OK	OK	OK		
	6775	165	OK	OK	OK	OK	OK		
	6795	169	OK	OK	OK	OK	OK		
	6815	173	OK	OK	OK	OK	OK		
	6835	177	OK	OK	OK	OK	OK		
	6855	181	OK	OK	OK	OK	OK		
	6875	185	OK	OK	OK	OK	OK		
UNII-8	6895	189	OK	OK	OK	OK	OK		
	6915	193	OK	OK	OK	OK	NOK		
	6935	197	OK	OK	OK	OK	NOK		
	6955	201	OK	OK	OK	OK	NOK		
	6975	205	OK	OK	OK	OK	NOK		
	6995	209	OK	OK	OK	OK	OK		
	7015	213	OK	OK	OK	OK	OK		
	7035	217	OK	OK	OK	OK	OK		
	7055	221	OK	OK	OK	OK	OK		
	7075	225	OK	OK	OK	OK	NOK		
	7095	229	OK	OK	OK	OK	NOK		
	7115	233	OK	OK	OK	NOK*	NOK		

2.4.1.2 捕获多个信道

输入多个信道，信道间用英文逗号隔开，可以捕获多个信道。（如：**1,2,36**，循环扫描 1、2、36 三个信道）

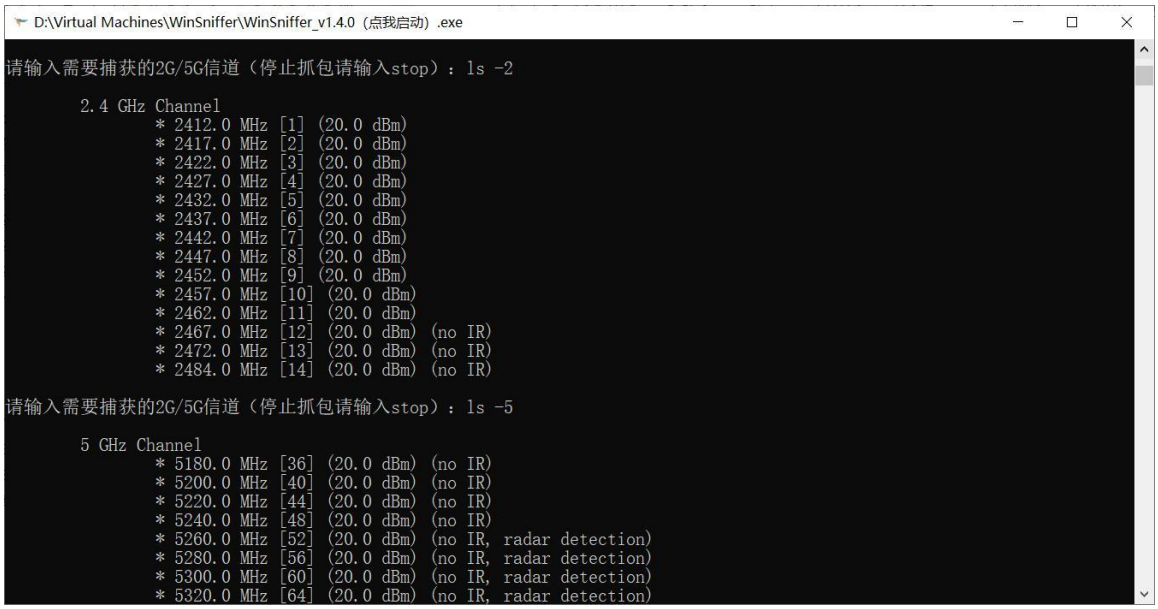
注意此捕获方式是通过循环切换网卡的监听信道实现，也称“扫描模式”，并不是同时捕获多个信道，因为网卡同一个时间内只能监听到一个信道/频段内的报文。

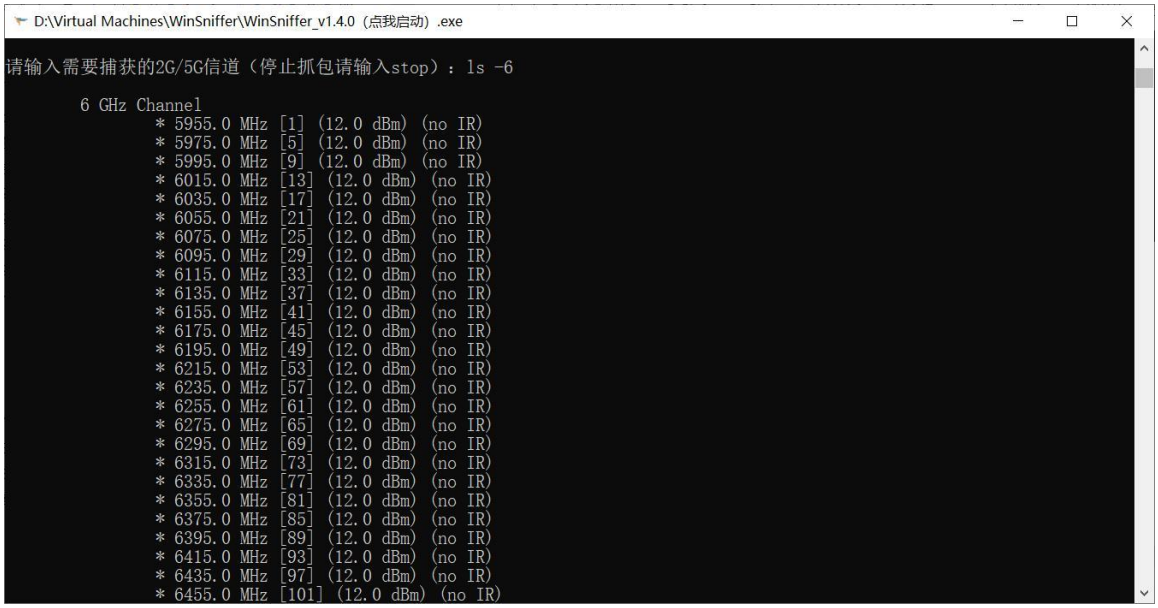
可设置扫描间隔，格式为：**1,2,36 10s** 或 **1,2,36 10**，循环扫描 1、2、36 三个信道，每个信道扫描 10 秒。不设置时默认扫描间隔为 0.5 秒。



2.4.1.2 查看支持信道

- **listch（快捷命令 ls）**：查看网卡信道支持情况。如信道后面带 **disable** 后缀，说明网卡不支持该信道，或由于政策原因不允许使用该信道（如雷达信道 169、173、177）。
- **ls -a**：查看 2.4G、5G、6G 所有信道。
- **ls -2**：查看 2.4G 信道。
- **ls -5**：查看 5G 信道。
- **ls -6**：查看 6G 信道。

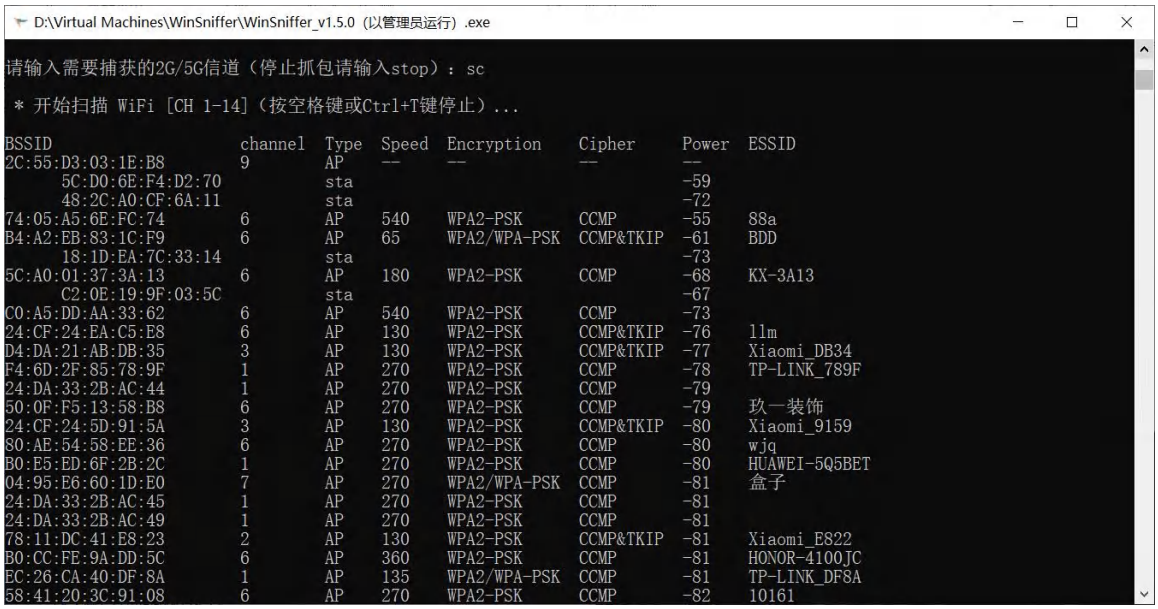




2.4.1.3 扫描 WiFi 信息

PS：扫描功能目前不支持 WiFi6（ax），但抓包支持抓 WiFi6（ax）报文。

- **scan（快捷命令 sc）：**扫描附近的 WiFi（按空格停止扫描），不输参数默认扫描 2.4G（1-14 信道）。



- **sc 144**：扫描信道为 144 的 WiFi。
- **sc 100-144**：扫描信道在 100 到 144 范围内的所有 WiFi。
- **sc -2**：扫描 2.4G WiFi（全频段，信道 1-14）。
- **sc -5**：扫描 5G WiFi（全频段，信道 36-177）。

  sc -5g1，扫描 5.2G WiFi（信道 36-64，5.18~5.32 GHz）

  sc -5g2，扫描 5.5G WiFi（信道 100-144，5.50~5.72 GHz）

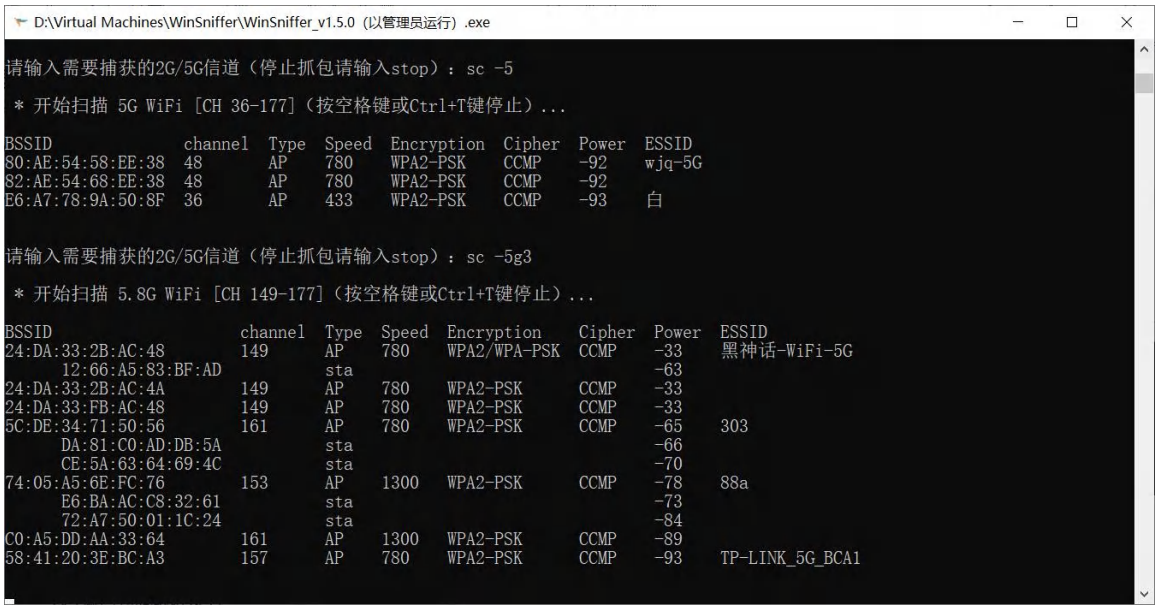
  sc -5g3，扫描 5.8G WiFi（信道 149-177，5.745~5.885 GHz）
- **sc -6**：扫描 6G WiFi（全频段，信道 1-233）。

  sc -6g1，扫描 6G UNII-5 频段（信道 1-93，5.955~6.415 GHz）

  sc -6g2，扫描 6G UNII-6 频段（信道 97-113，6.435~6.515 GHz）

  sc -6g3，扫描 6G UNII-7 频段（信道 117-185，6.535~6.875 GHz）

  sc -6g4 ，扫描 6G UNII-8 频段（信道 189-233，6.895~7.115 GHz）



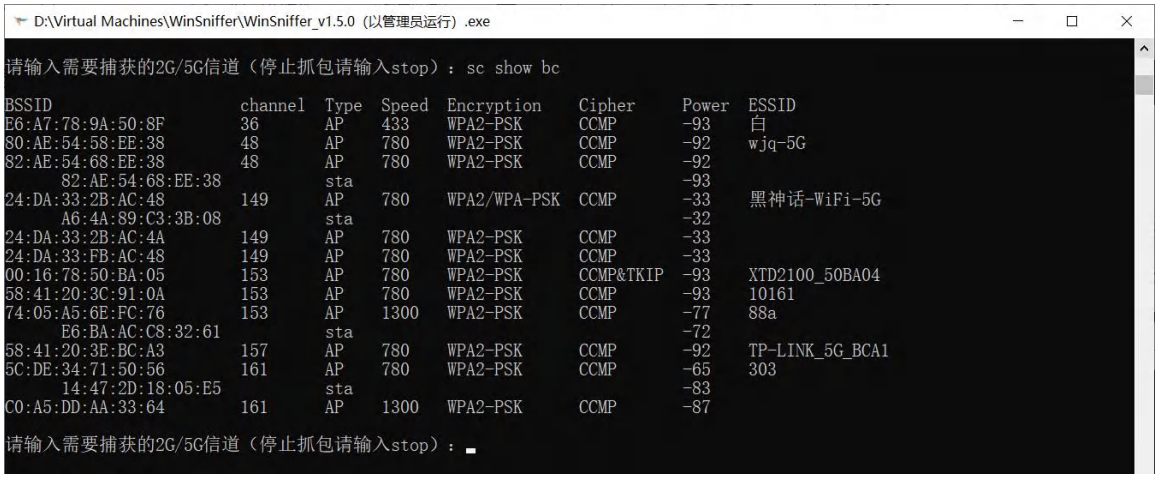
- **sc show**：显示上一次 WiFi 扫描结果。

  sc show bybssid（或 **sc show bb**），显示扫描结果，根据 BSSID 排序

  sc show bychannel（或 **sc show bc**），显示扫描结果，根据信道排序

  sc show byspeed（或 **sc show bs**），显示扫描结果，根据速率排序

  sc show bypower（或 **sc show bp**），根据强度排序（默认）



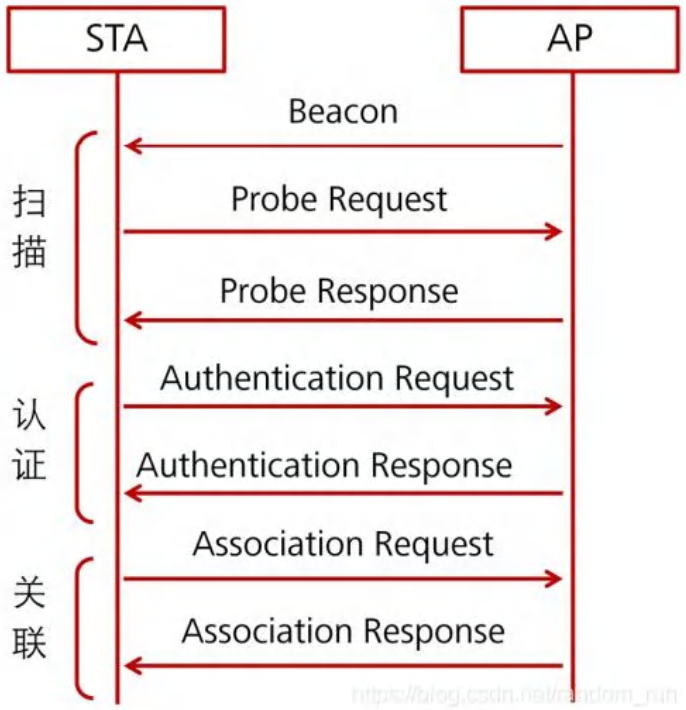
2.4.1.3 修改主机地址

- **set ip 192.168.20.100**：修改主机地址。如果默认虚拟机地址与其他设备存在冲突，可以使用 set ip 命令进行修改。修改成功后程序会重新连接虚拟机。

2.4.2 Wireshark 空口抓包技巧

2.4.2.1 无线报文过滤

提供一些常见 802.11 报文在 Wireshark 中过滤的关键字（显示过滤器），在报文上方的搜索框输入可快速找到一些我们需要的报文。



参考资料：
https://blog.csdn.net/maimang1001/article/details/128242641

- **Mac 地址过滤**

Wireshark 过滤关键字	说明
wlan.addr == mac address	specific client by mac address
wlan.ta == mac address	transmitter address
wlan.ra == mac address	receive address
wlan.sa == mac address	source address
wlan.da == mac address	destination address
wlan.bssid == ap mac address	radio mac address

- **13 个管理帧（management frames)**

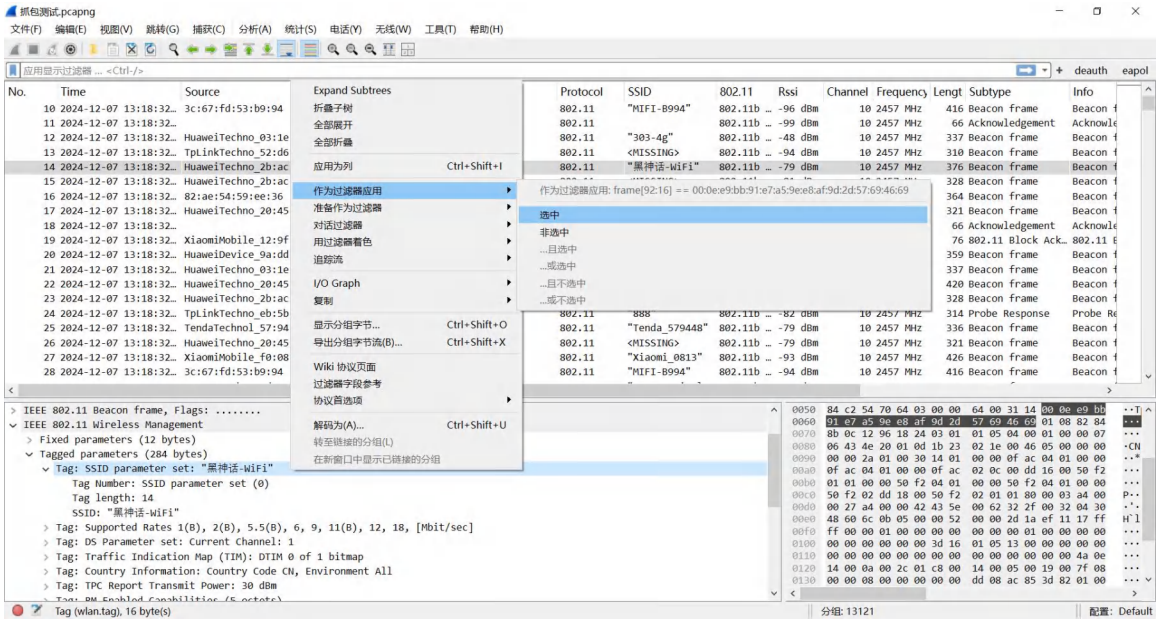
Wireshark 过滤关键字	说明
wlan.fc.type_subtype == 0	association requests
wlan.fc.type_subtype == 1	association response

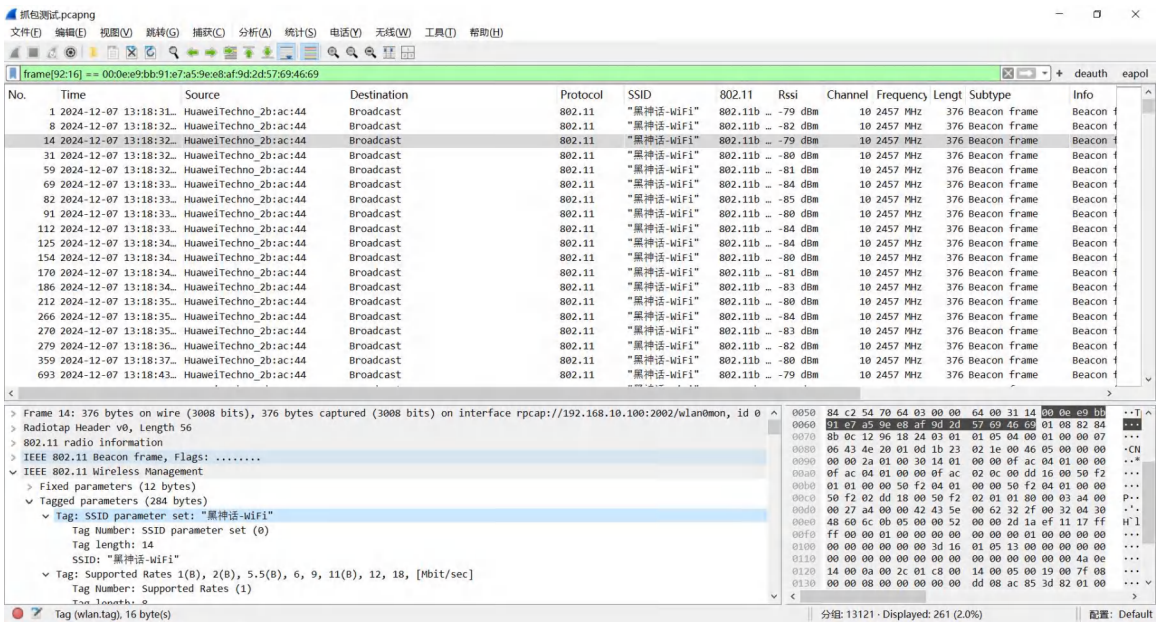
Wireshark 过滤关键字	说明
wlan.fc.type_subtype == 2	re-association request
wlan.fc.type_subtype == 3	re-association response
wlan.fc.type_subtype == 4	probe requests
wlan.fc.type_subtype == 5	probe responses
wlan.fc.type_subtype == 8	beacons
wlan.fc.type_subtype == 9	atims
wlan.fc.type_subtype == 10	disassosiations
wlan.fc.type_subtype == 11	authentications
wlan.fc.type_subtype == 12	deauthentications
wlan.fc.type_subtype == 13	actions

- **漫游三协议（802.11 k,v,r)**

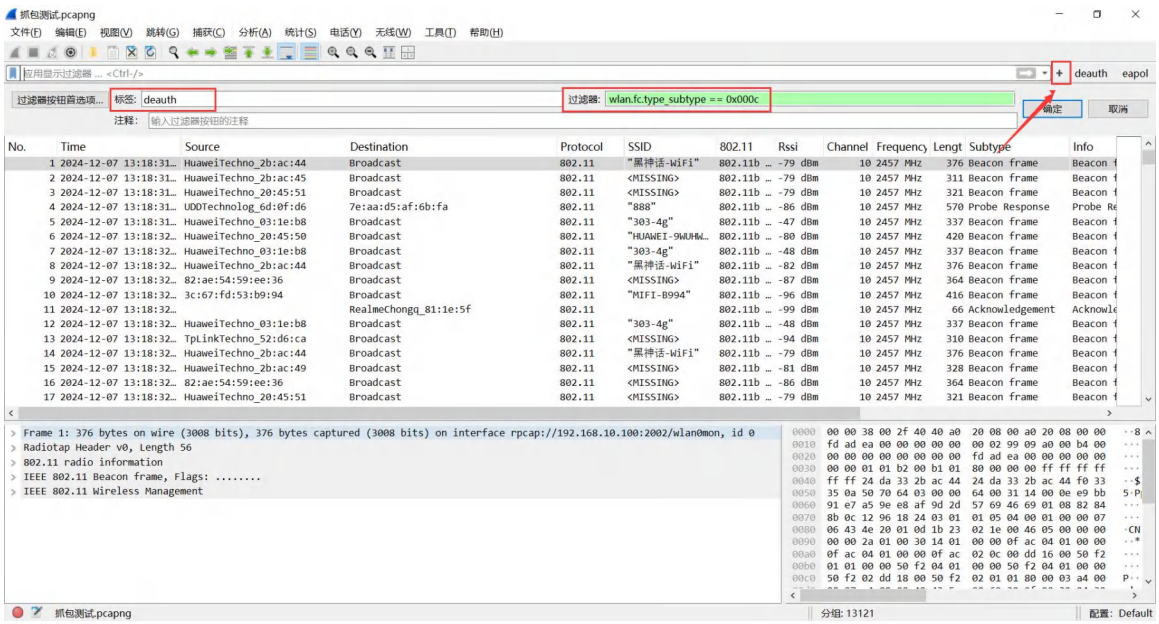
Wireshark 过滤关键字	说明
wlan.fixed.action_code ==23	802.11v dms request
wlan.fixed.action_code ==24	802.11v dms respose
wlan.rm.action_code ==4	802.11k neighbour request
wlan.rm.action_code ==5	802.11k neighbour response
(wlan.fc.type_subtype==0)&&(wlan.rsn.akms.type==3)	802.11r auth request
(wlan.fc.type_subtype==1)&&(wlan.tag.number==55)	802.11r auth response
(wlan.fc.type_subtype==2)&&(wlan.tag.number==55)	802.11r re-association request
(wlan.fc.type_subtype==3)&&(wlan.tag.number==55)	802.11r re-association response
wlan.fixed.action_code==7	BSS Transition (Steering)
wlan.fixed.action_code==8	BSS Transition (Steering)

还有一种方法不需要敲命令，就是选择某个报文后，展开报文的内容，找到需要过滤的信息，右键**作为过滤器应用 -> 选中。**





补充：若有一些报文经常需要过滤，可以点击搜索框右边的+号添加一些常用的过滤条件，然后点击生成的按钮就可以直接过滤。

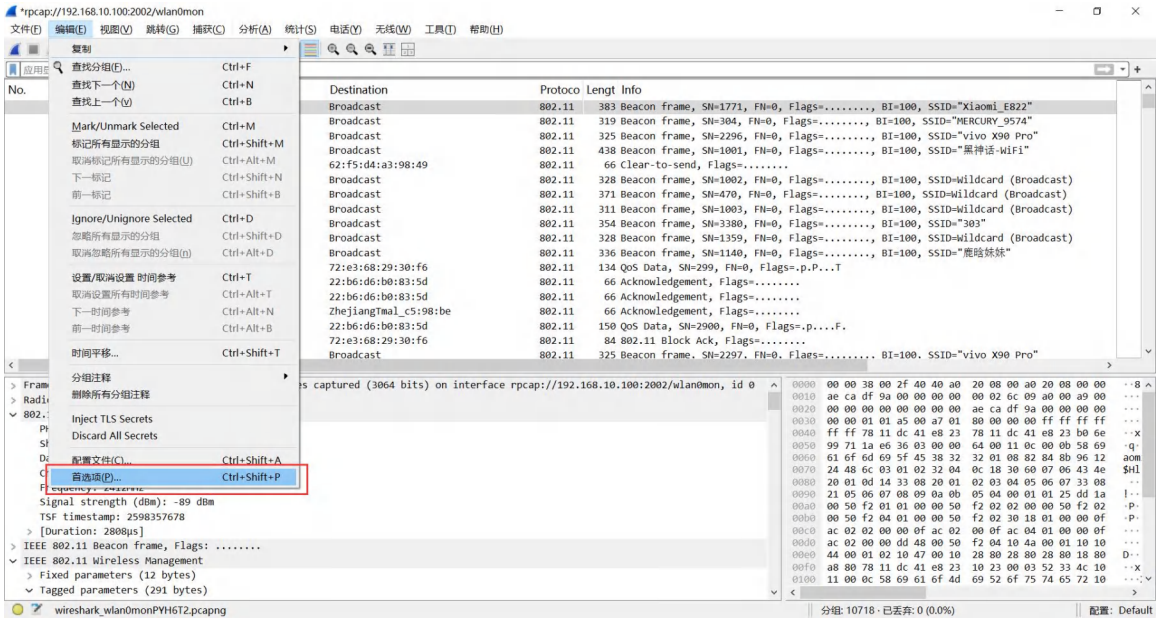


2.4.2.2 无线报文解密

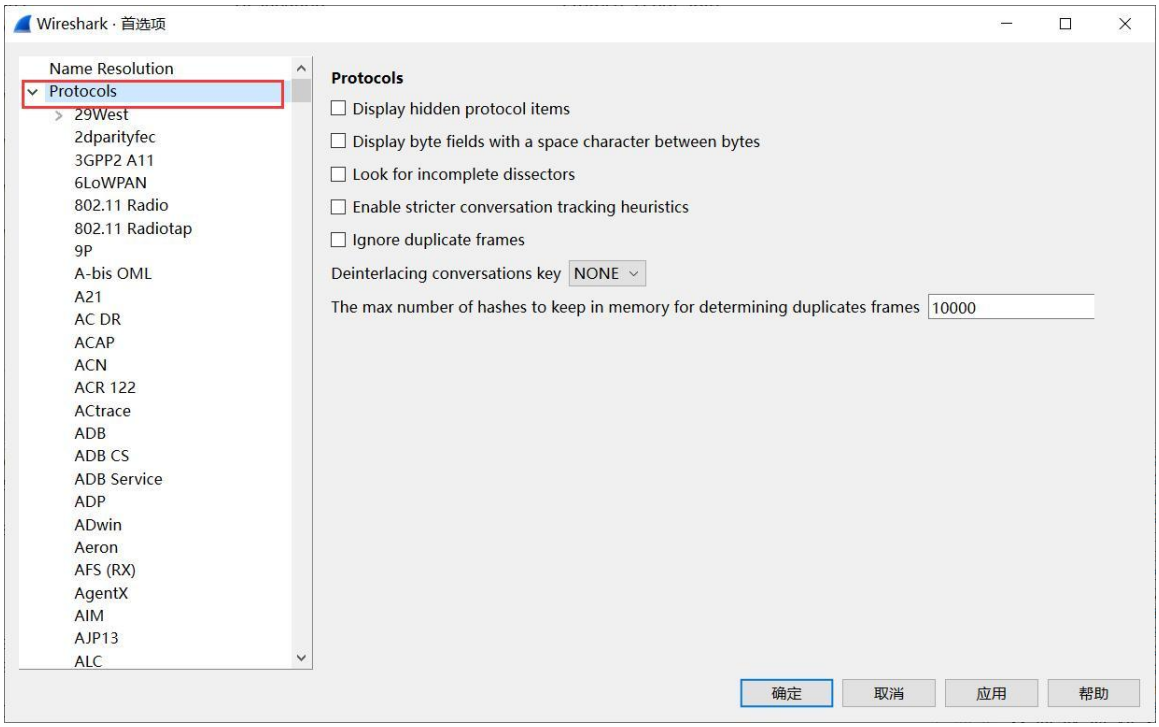
无线数据本身是加密的（open 模式除外），正常抓包只能看到管理帧和控制帧的内容。若要查看数据帧的内容（如无线终端的 Ping 包），则需要解密。需要在 Wireshark 中设置好秘钥，并在报文中抓取到终端连接过程中的握手包（EaPOL 报文）。

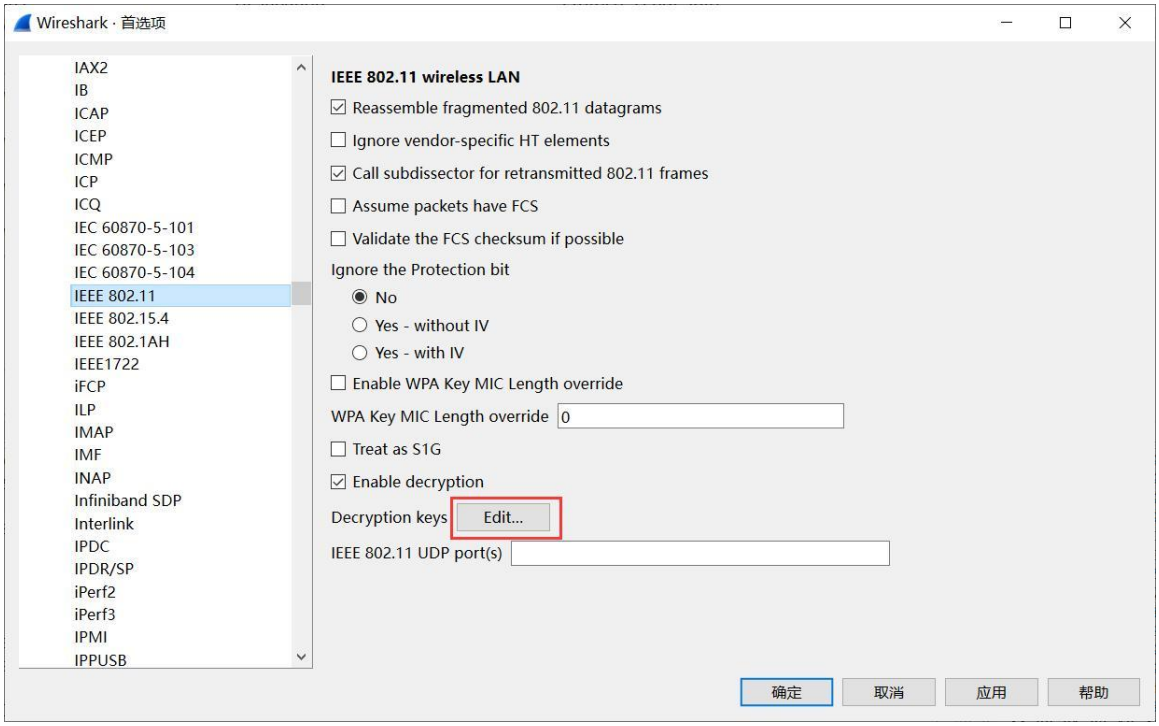
参考资料：
https://blog.csdn.net/2301_80361487/article/details/136028833

Wireshark 菜单栏点击**“编辑”**-**“首选项”**。



展开“**Protocol**”项，下拉找到“**IEEE 802.11**”，点击 Decryption keys 后的“**Edit**”。

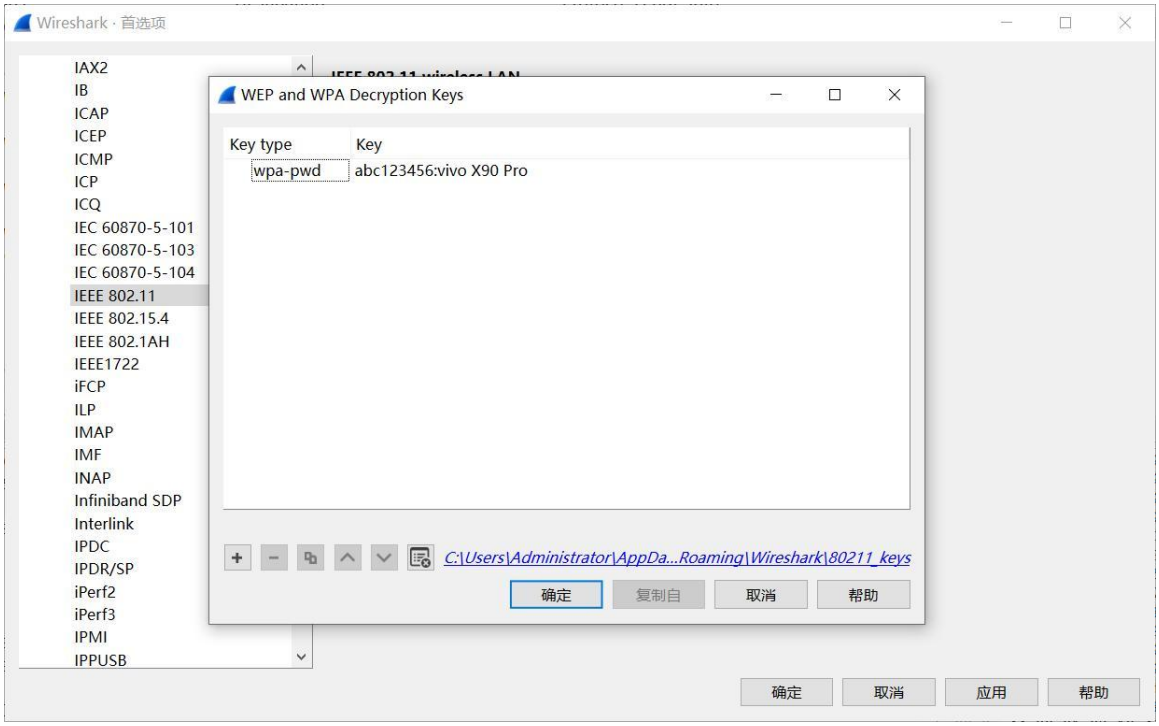




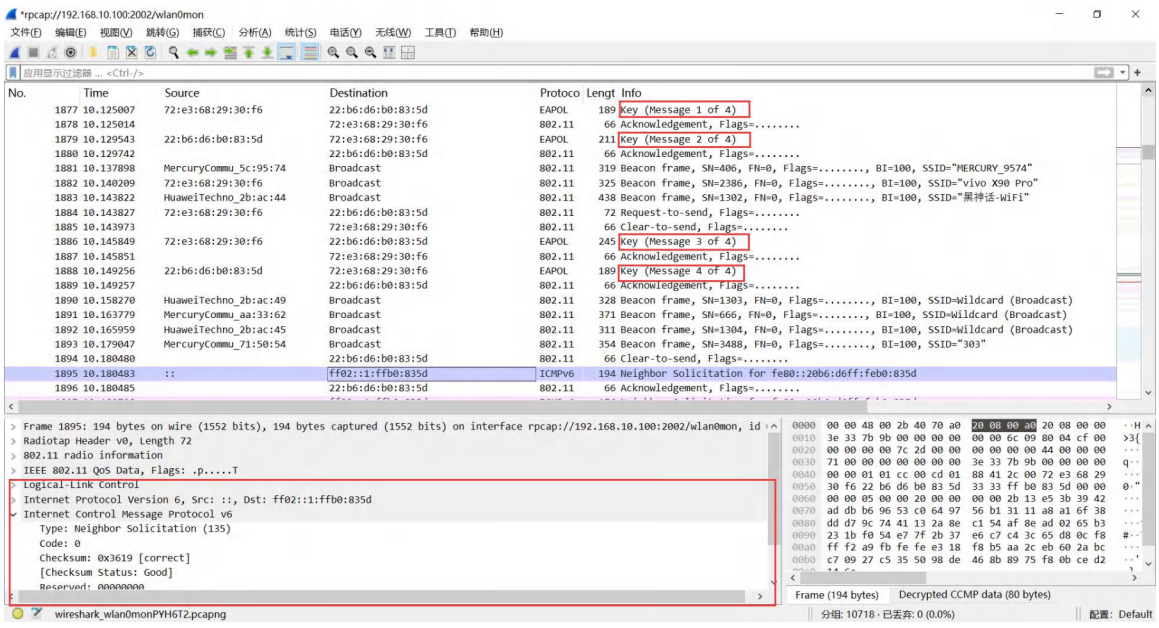
点击下发的“+”添加一个无线秘钥。Key type 选择 **wpa-pwd**，Key 中填写 SSID 密码跟 SSID 名称，格式为“**SSID 密码:SSID 名称**”，中间是英文冒号。

如我这里填写“abc123456:vivo X90 Pro”，其中前面 abc123456 是 WiFi 密码，后面 vivo X90 Pro 是 WiFi 名称，中间用英文的冒号“:”分隔开。

需要注意的是，Key 中如果输入特殊字符如中文会无法保存（软件 Bug），所以 **WiFi 的名称不能使用中文，如果有中文需要修改。**

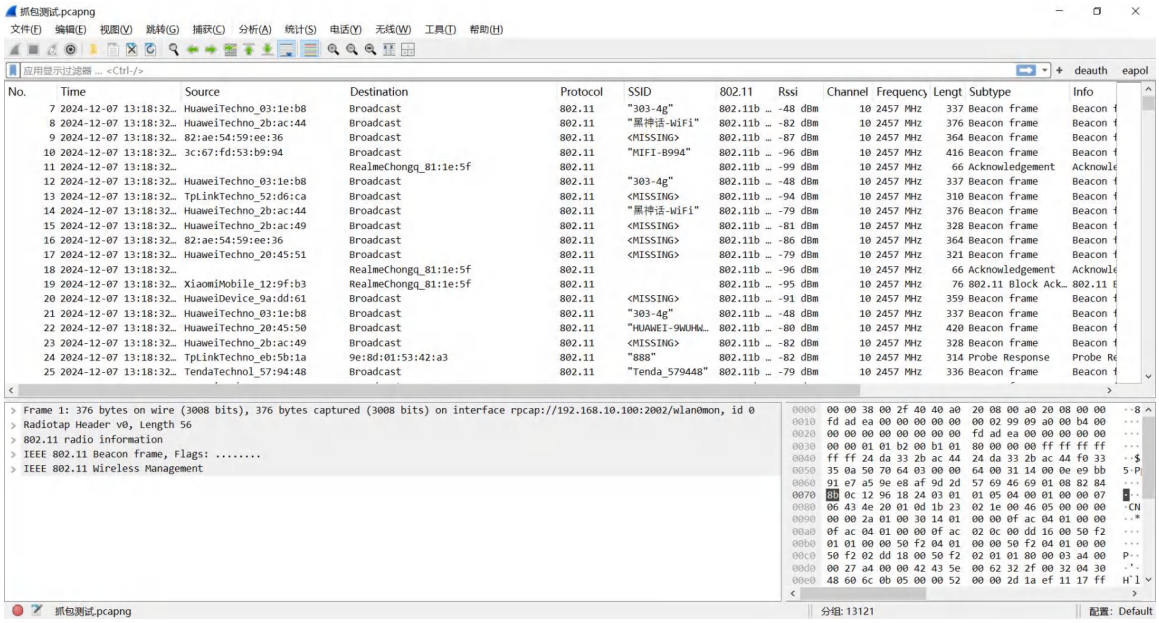


STA 先断开连接，然后开始抓包，STA 重新连接，抓取到 STA 连接的四次握手报文（eapol）后，Wireshark 就可以根据设置好的秘钥和握手包自动计算解密出后面捕获到的数据帧。

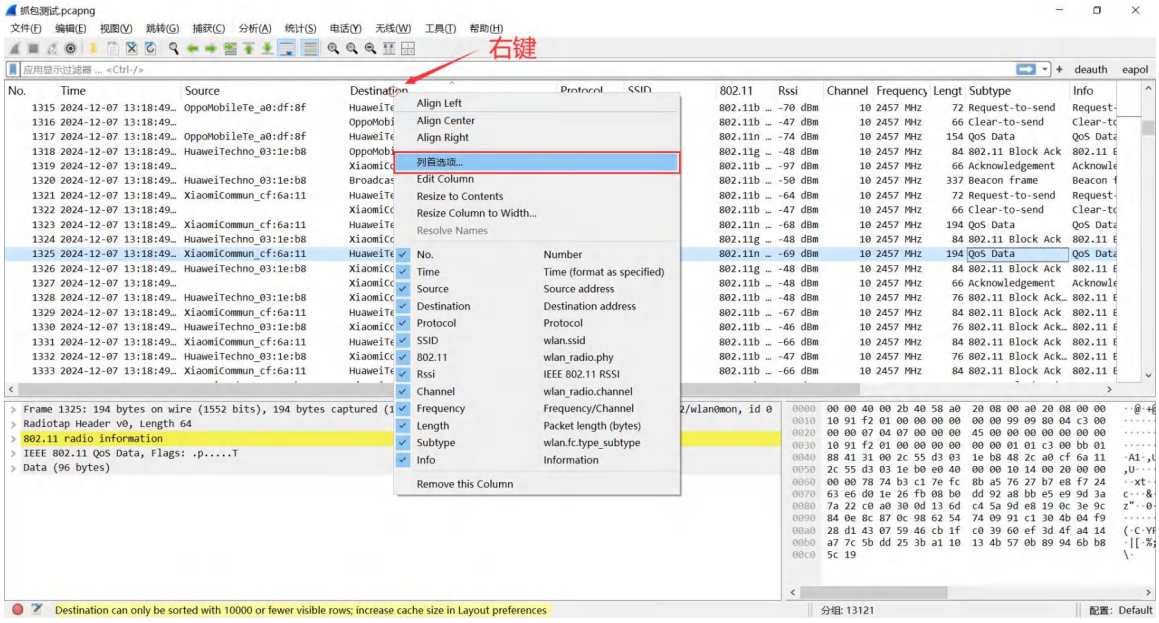


2.4.2.3 修改无线视图

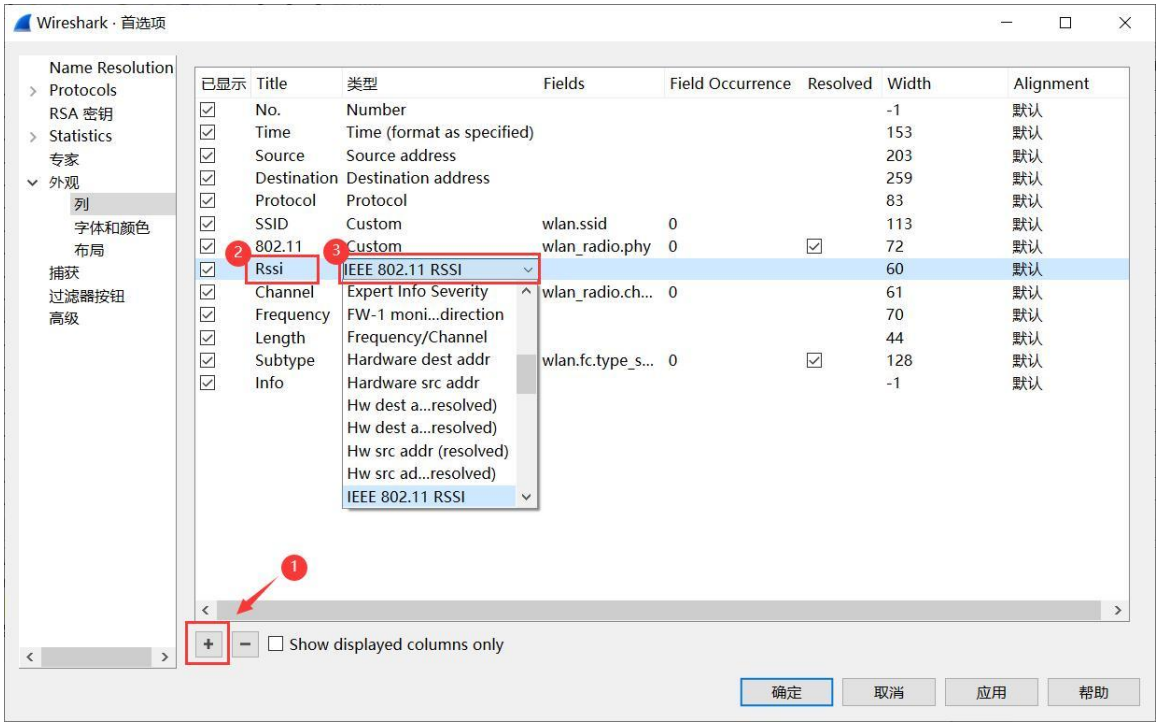
可以在抓包视图窗口添加一些无线信息（如信号强度、WiFi 名称、无线协议类型、信道、帧类型等）的列，以方便我们更直接看到报文有关 WiFi 的重要信息（如下图所示）。



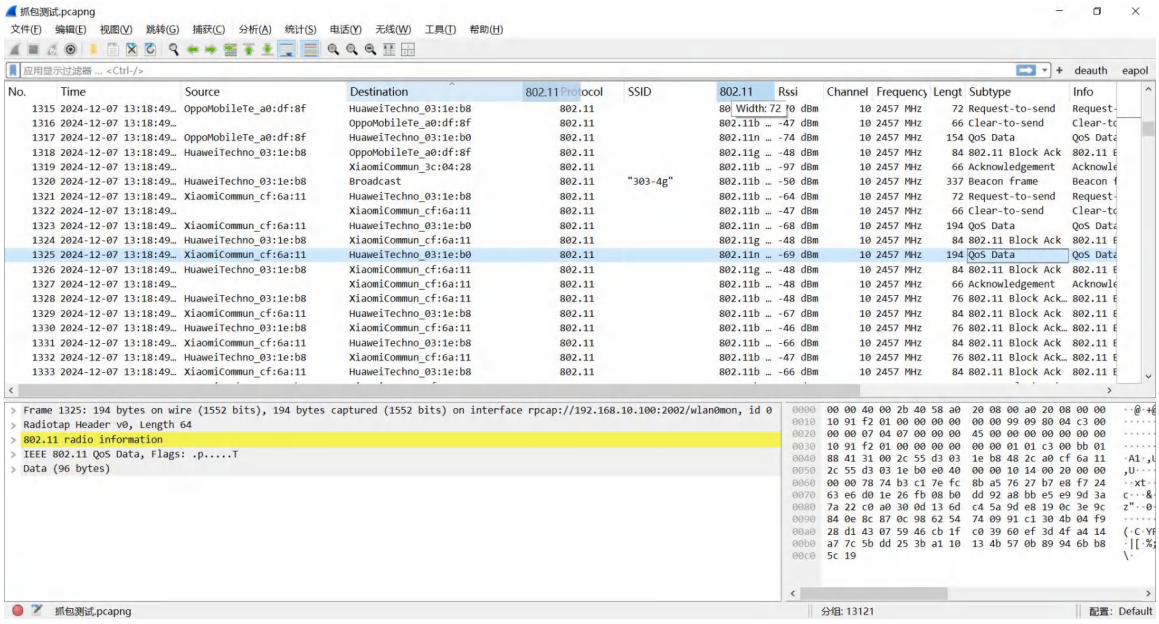
鼠标置于列的表头上，右键会出现小菜单，点击**列首选项**。



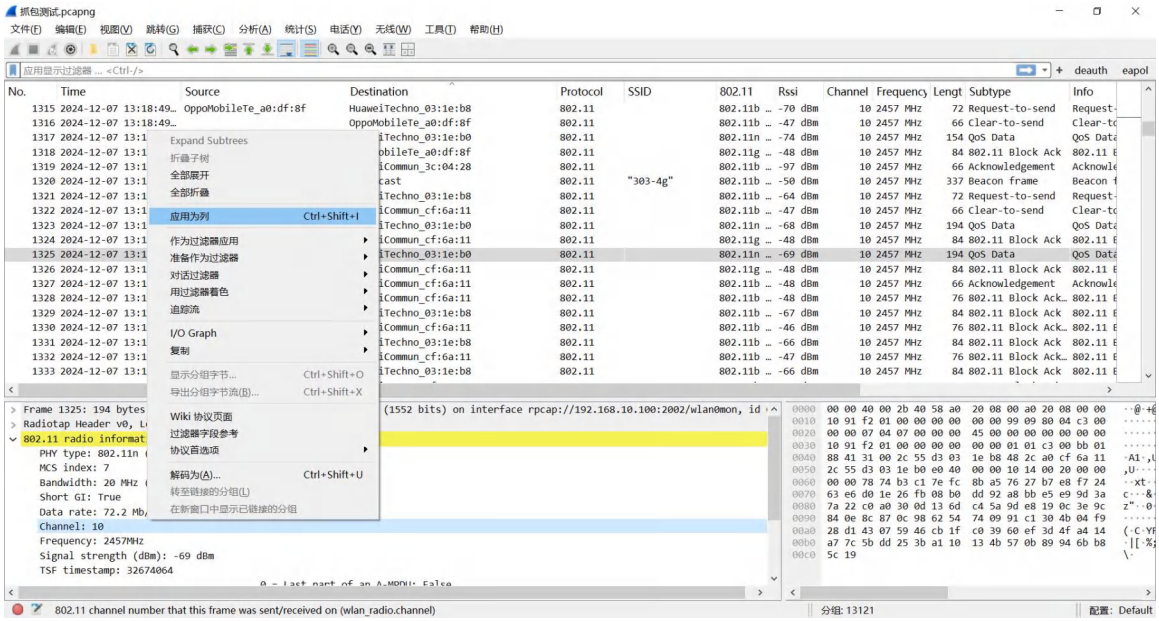
弹出的窗口中点击下方小加号（+），添加一列内容。然后在 **title** 栏填列名（可以自己随意设置），在**类型**栏选择这一列信息对应报文哪个部分的内容（可以双击在列表里找，若找不到想要的内容，不着急，往后看，后面还一种方法）。



新加的一列内容会显示在最末尾（需要拉到最右边才能看到），不方便观察。可以拖动到前面，根据需要进行排列，调整列宽。

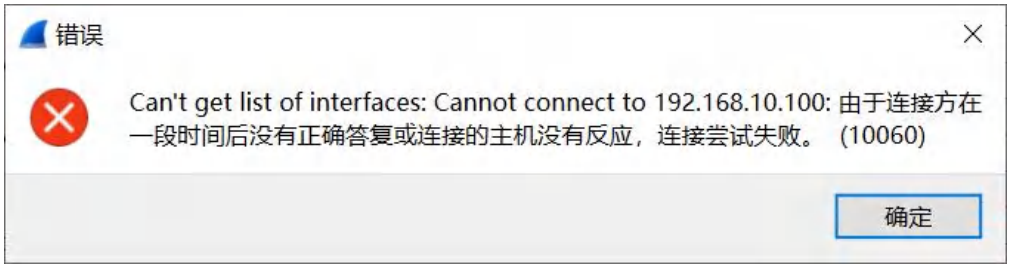


还有一种更方便的方法，就是展开某个报文，找到需要的内容，右键**应用为列**。

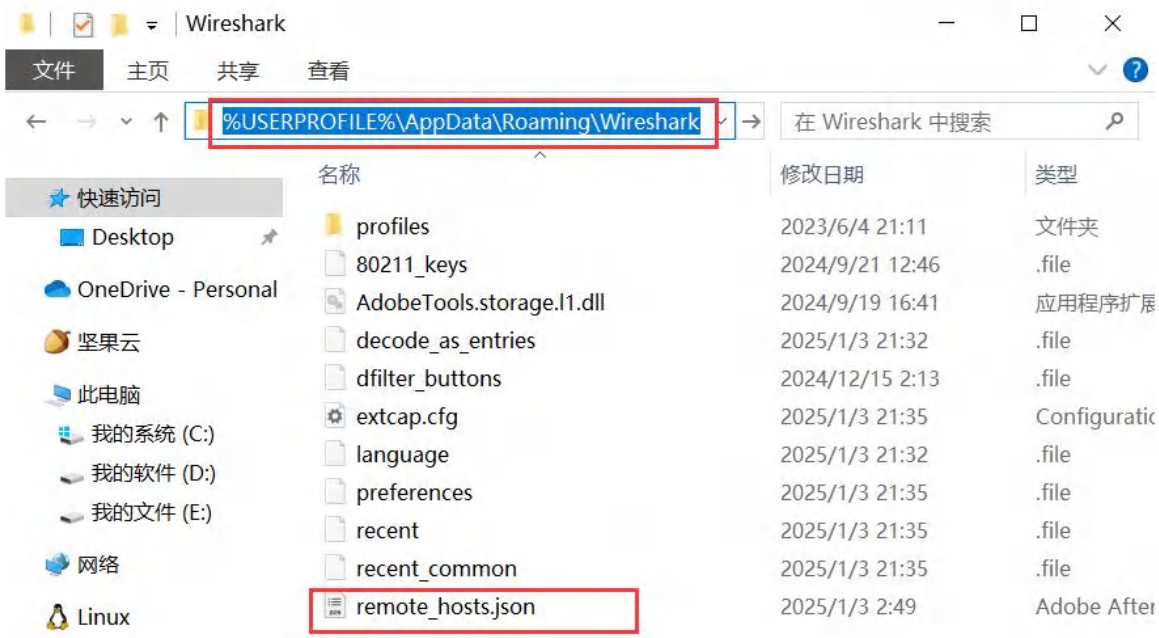


2.4.2.4 管理远程接口

Wireshark 中如果配置了多个远程连接的接口，每次启动时都会依次尝试连接，需要等待很久。



例如，配置了错误的远端接口或改变了抓包虚拟机的 ip 地址，那旧的接口就不需要用了，如何删掉之前保存的接口配置呢？我们可以在资源管理器上方的搜索框输入%USERPROFILE%\AppData\Roaming\Wireshark，进入 Wireshark 的个人配置文件夹，编辑 **remote_hosts.json** 这个文件可以管理已经保存的远程接口。如果需要清空之前的所有接口，也可以直接将这个文件删除。



2.4.2.5 长时间抓包配置

由于 Wireshark 默认会将正在捕获的报文临时存储在电脑内存中，如果我们进行长时间抓包，当数据量变得非常大时，电脑内存吃满便会卡死，丢失数据。

所以如果需要进行长时间抓包，建议配置自动将抓到的报文存储起来。Wireshake 菜单栏点击**捕获-选项-输出**，进行如下配置：

2.4.3 网友常见问题答疑汇总

Q1. 抓包漏包怎么办

无线资源是非常拥挤的，当同一信道中有多个 WiFi 时，由于干扰严重且报文量巨大，网卡性能吃不消所以抓包时可能产生漏包。

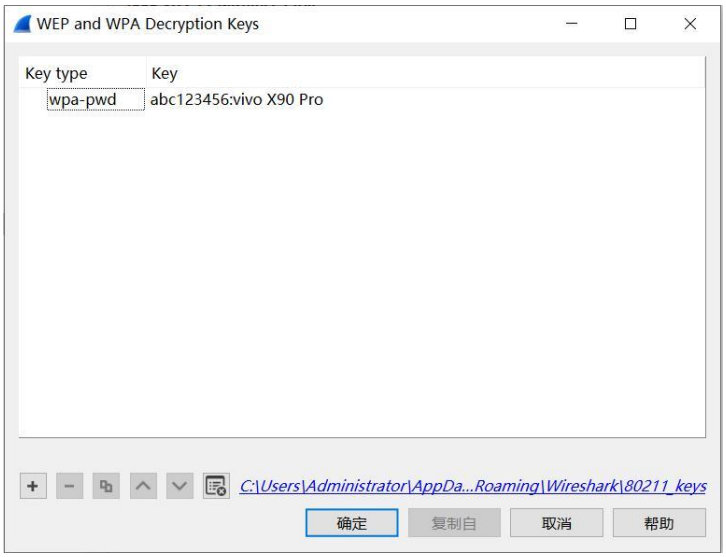
故一般排查无线问题时，一方面会使用 5G WiFi（5G 频段相对 2.4G 资源丰富，干扰小），一方面会将 WiFi 设置到不拥挤的信道（低信道如 36、40 信道使用较多，高信道 56、60 使用较少），以避免漏包的情况。

还有若要抓取 WiFi 数据帧，推荐将 WiFi 设为 5G、80MHz，同时在程序中也设置好抓包频宽为 80MHz。

Q2. 如何抓空口的 Ping 报文

如果要抓取 sta 跟 ap 之间的 ping 报文，涉及数据帧内容的捕获。

而由于数据帧在 WiFi 中是加密不可见的，一种方法是将 WiFi 设为 open 模式，即不设置密码；另一种方法则是抓取 sta 连接 WiFi 过程中的 eapol 报文后，在 Wireshark 中设置秘钥对报文进行解密（参考 2.4.2.2 章无线报文解密）。



Q3. 跟 Omnipeek 有什么区别

Omnipeek 抓包是通过 LiveAction 公司开发的一些特殊驱动，来在 Windows 下开启网卡的监听模式，以捕获空口报文。

作者的程序是通过将网卡接入虚拟机，使用 Linux 原生驱动来开启网卡的监听模式，以捕获空口报文。

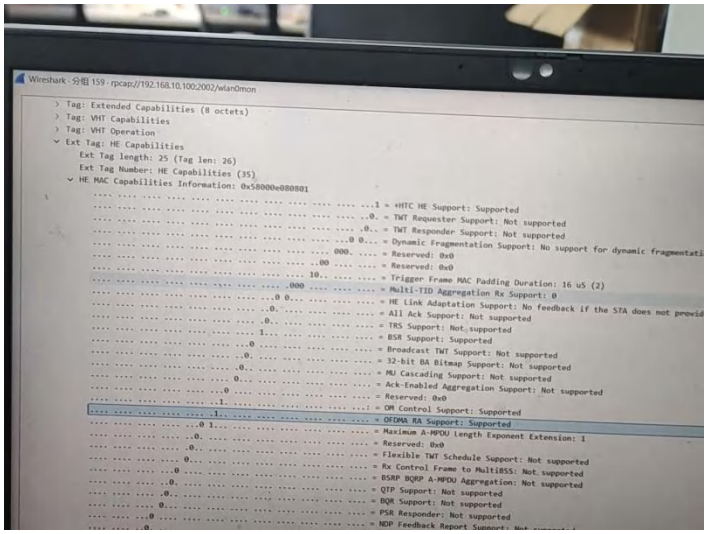
在抓包网卡的支持上，作者程序的支持性是比 Omnipeek 更广的，因为 Linux 原生驱动的生态是远大于 Omnipeek 驱动的生态的。一句话就是用 Omnipeek 能抓包的网卡用作者的程序也能抓，但用作者程序能抓包的网卡用 Omnipeek 就不一定能抓。

在程序使用便捷性上，作者程序也比 Omnipeek 易上手。因为 Omnipeek 需要安装特殊的网卡驱动（安装繁琐），且安装这个驱动后网卡就不能正常用来上网。而作者程序可以做到开箱即用，且关闭程序后网卡还可以正常使用。

在抓包软件的安装使用上，Omnipeek 安装需要破解，且界面相对复杂。作者的程序则结合使用免费开源的 Wireshark 抓包软件，界面清爽。

Q4. 能抓 WiFi6（ax）报文吗

目前使用 MT7921au 芯片（WiFi6e）的网卡测试可以抓取 WiFi6 报文，抓取到 beacon 帧中有 HE 信息（802.11ax(HE，HighEfficiency)）。



若使用 WiFi5 的网卡，理论上应该也能抓到 WiFi6 的报文，但可能识别不出其中的 WiFi6 的信息。目前作者没有测试条件，所以并不清楚，有测试条件的网友可以测试下跟作者反馈下结果。

Q5. 能抓 160MHz 频宽吗

截止目前（2025.01.03），市面上能稳定空口抓包的 USB 网卡频宽最多支持到 80MHz。CSDN 上有一篇使用 RTL8832cu（支持 160MHz）空口抓包的文章《WIFI6 802.11ax 无线抓包》，但笔者根据文章的方法打好驱动，网卡开启监听模式后系统会变得不稳定，偶尔能抓包，但切换信道时系统就会卡死。

可以等后续更新的 WiFi 芯片（如 MT7925）投入到 USB 网卡的使用。

3 抓包网卡收录

Github 上有一个叫 USB-WiFi 项目，里面统计了一些支持在 Linux 下开启监听模式的 USB 无线网卡。

参考资料：https://github.com/morrownr/USB-WiFi/blob/main/home/USB_WiFi_Chipsets.md

Chipset	Interface	Standard	Maximum Channel Width	Linux In-Kernel Driver	AP Mode	Monitor Mode	Recommended For Linux
Mediatek MT7922au	USB3	WiFi 6E	160	✓ 5.16+	✓	✓	[4]
Realtek RTL8852cu	USB?	WiFi 6E	160	✗ [6]			No
Realtek RTL8832cu	USB3	WiFi 6E	160	✗	?	?	No
Mediatek MT7921au	USB3	WiFi 6E	80	✓ 5.18+	✓	✓	Yes
Realtek RTL8852bu	USB?	WiFi 6	80	✗ [6]			No
Realtek RTL8832bu	USB3	WiFi 6	80	✗	✓	✓	No
Realtek RTL8852au	USB?	WiFi 6	80	✗ - avoid [2]	bad driver	bad driver	No
Realtek RTL8832au	USB3	WiFi 6	80	✗ - avoid	bad driver	bad driver	No
Realtek RTL8814au	USB3	WiFi 5	80	✗ - avoid	old driver	old driver	No
Mediatek MT7662u	USB2	WiFi 5	80	✓ 5.9+ [6]	✓	✓	No
Mediatek MT7612u	USB3	WiFi 5	80	✓ 4.19+	✓	✓	Yes
Realtek RTL8822bu	USB2 [5]	WiFi 5	80	✓ 6.2+ [3][6]	✓	✓	No
Realtek RTL8812bu	USB3	WiFi 5	80	✓ 6.2+ [3]	✓	✓	Yes
Realtek RTL8822cu	USB2 [5]	WiFi 5	80	✓ 6.2+ [3][6]	✓	✓	No
Realtek RTL8812cu	USB3	WiFi 5	80	✓ 6.2+ [3]	✓	✓	No
Realtek RTL8812au	USB3	WiFi 5	80	✗	✓	✓	No
Mediatek MT7610u	USB2	WiFi 5	80	✓ 4.19+	✓	✓	Yes
Realtek RTL8821cu	USB2	WiFi 5	80	✓ 6.2+ [3][6]	✓	✓	No
Realtek RTL8811cu	USB2	WiFi 5	80	✓ 6.2+ [3]	✓	✓	Yes
Realtek RTL8821au	USB2	WiFi 5	80	✗ [6]	✓	✓	No
Realtek RTL8811au	USB2	WiFi 5	80	✗	✓	✓	No
Ralink RT3573	USB2	WiFi 4	40	✓ 3.12+	✓	✓	Yes
Ralink RT5572	USB2	WiFi 4	40	✓ 3.10+	✓	✓	Yes
Ralink RT3572	USB2	WiFi 4	40	✓ 2.6.31+	✓	✓	Yes
Ralink RT5372	USB2	WiFi 4	40	✓ 3.0+	✓	✓	Yes
Realtek RTL8192cu	USB2	WiFi 4	40	✓ 2.6.33+	✓	✓	Yes
Mediatek MT7601u	USB2	WiFi 4	40	✓ 4.2+	✗	limited	Yes
Ralink RT5370	USB2	WiFi 4	40	✓ 3.0+	✓	✓	Yes
Atheros AR9271	USB2	WiFi 4	40	✓ 2.6.35+	✓	✓	Yes
Ralink RT3070	USB2	WiFi 4	40	✓ 2.6.31+	✓	✓	Yes

根据此表格，以及 USB-WiFi 项目中提供的一些网卡资料，对市面上符合要求的国内外网卡进行统计收录。只要网卡在 Linux 中免驱且支持监听模式，用笔者的程序就能实现 Windows 下空口抓包。

3.1 国内网卡（更新中）

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
1	Fenvi FU-AX1800（奋威）		65	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用
2	Fenvi FU-AX1801D（奋威）		99	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用
3	EDUP EP-AX1672（翼联）		98	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5G：1200Mbps，5.8G：1200Mbps	可用
4	双频 wifi6 无线 kali 网卡 1（无牌）		93	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
5	双频 wifi6 无线 kali 网卡 2（无牌）		93	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用
6	双频 wifi6 无线 kali 网卡 3（无牌）		93	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用
7	双频 wifi6 无线 kali 网卡 4（无牌）		93	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用
8	双频 wifi6 无线 kali 网卡 5（无牌）		96	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用
9	双频 wifi6 无线 kali 网卡 6（无牌）		-	mt7921au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用
*新增	-		147	rtl8832au	WiFi6（ax）	WPA2、WPA3	2.4G：574Mbps，5.8G：1201Mbps	可用

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
*新增	Fenvi FU-AX1800P（奋威）		99	rtl8832au	WiFi6（ax）	WPA2、WPA3	2.4G:574Mbps，5.8G:1201Mbps	可用
*新增	-		90	rtl8832au	WiFi6（ax）	WPA2、WPA3	2.4G:574Mbps，5.8G:1201Mbps	可用
*新增	-		129	rtl8832bu	WiFi6（ax）	WPA2、WPA3	2.4G:574Mbps，5.8G:1201Mbps	不可用
*新增	-		90	rtl8832bu	WiFi6（ax）	WPA2、WPA3	2.4G:574Mbps，5.8G:1201Mbps	不可用
*新增	-		70	rtl8832bu	WiFi6（ax）	WPA2、WPA3	2.4G:574Mbps，5.8G:1201Mbps	不可用
*新增	-		90	rtl8832cu	WiFi6（ax）	WPA2、WPA3	2.4G:574Mbps，5G:2402Mbps	不可用
*新增	-		129	rtl8832cu	WiFi6（ax）	-	2.4G:574Mbps，5G:2402Mbps	不可用

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
*新增	-		68	rtl8831bu	WiFi6（ax）	-	2.4G：286Mbps，5.8G：600Mbps	不可用
*新增	-		155	rtl8814au	WiFi5（ac）	-	2.4G：574Mbps，5.8G：1201Mbps	待测试
10	MT7162无线WIFI接收器双天线版（无牌）		132	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	可用
11	MT7162无线WIFI接收器双单线版（无牌）		103	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	可用
12	GRIS GE-LW09-4611AC（格瑞斯）		50	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	可用
*新增	-		85	rtl8812au	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	待测试

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
*新增	RTL8822BU 1300M 带蓝牙		50	rtl8822bu	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	可用
*新增	RTL8812BU 1200M 网卡		86	rtl8812bu	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	可用
*新增	-		40	rtl8812cu	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	可用
*新增	-		50	rtl8812cu	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	可用
13	GRIS GE-LW09-7610（格瑞斯)		40	mt7610u	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	待测试
*新增	-		37	rtl8811au	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	待测试
14	RTL8821CU 无线网卡（无牌)		78	rtl8821cu	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	可用

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
15	GRIS GE-LW09-4509（格瑞斯)		54	rtl8821cu	WiFi5（ac)	-	2.4G: 150Mbps, 5G: 443Mbps	可用
16	GRIS GE-LW09-W69L（格瑞斯)		54	rtl8821cu	WiFi5（ac)	-	2.4G: 150Mbps, 5G: 443Mbps	可用
17	GRIS GE-LW09-W69（格瑞斯)		53	rtl8821cu	WiFi5（ac)	-	2.4G: 150Mbps, 5G: 443Mbps	可用
18	GRIS GE-LW09-4508（格瑞斯)		53	rtl8821cu	WiFi5（ac)	-	2.4G: 150Mbps, 5G: 443Mbps	可用
19	GRIS GE-LW09-4512BT（格瑞斯)		50	rtl8821cu	WiFi5（ac)	-	2.4G: 150Mbps, 5G: 443Mbps	可用

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
20	RTL8811CU 双频无线网卡带天线（无牌）		31	rtl8811cu	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	可用
21	RTL8811CU 双频无线网卡无天线（无牌）		24	rtl8811cu	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	可用
22	EW-7733UND RT3573 芯片（无牌）		34	rt3573	WiFi4（an）	-	2.4G：450Mbps，5G：450Mbps	待测试
23	RT5572 N600（无牌）		37	rt5572	WiFi4（an）	-	2.4G：300Mbps，5G：300Mbps	可用
24	NW362 磊科 rtl8192cu（无牌）		33	rtl8192cu	WiFi4（b/n/g）	-	2.4G：300Mbps	待测试
25	RT5370 USB 无线网卡（无牌）		40	rt5370	WiFi4（b/n/g）	-	2.4G：150Mbps	待测试

序号	网卡名称	产品图	参考价(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
26	GRIS GE-LW06-9271（格瑞斯)		34	ar9271	WiFi4（b/n/g)	-	2.4G: 150Mbps	待测试
27	RT3070外置天线款（无牌)		50	rt3070	WiFi4（b/n/g)	-	2.4G: 150Mbps	待测试
28	RT3070L白色款		39	rt3070	WiFi4（b/n/g)	-	2.4G: 150Mbps	待测试
*新增	kali 单频无线网卡		37	mt7601	WiFi4（b/n/g)	-	2.4G: 150Mbps	可用

3.2 国外网卡

序号	网卡名称	产品图	参考价格(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
1	Netgear A8000（网件)		917	mt7921aun	WiFi6（ax)	WPA2、WPA3	-	未测试

序号	网卡名称	产品图	参考价格(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
2	ALFA AWUS036AXML（阿尔法）		704	mt7921aun	WiFi6（ax）	-	2.4G：600Mbps，5G：1200Mbps，6G：1200Mbps	未测试
3	ALFA AWUS036AXM（阿尔法）		637	mt7921aun	WiFi6（ax）	-	2.4G：600Mbps，5G：1200Mbps，6G：1200Mbps	未测试
4	ALFA AWUS036ACM（阿尔法）		758	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	未测试
5	Panda PAU0D		-	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	未测试
6	ALLNET ALL-WA1200AC		-	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	未测试
7	PIX-LINK LV-UAC04		-	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：	未测试

序号	网卡名称	产品图	参考价格(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
							867Mbps	
8	Netgear A6210（网件）		99	mt7612u	WiFi5（ac）	-	2.4G：300Mbps，5G：867Mbps	未测试
9	ALFA AWUS036ACHM（阿尔法）		618	mt7612u	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	未测试
10	PANDA - PAU0B		-	mt7612u	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	未测试
11	Asus USB-AC51		-	mt7612u	WiFi5（ac）	-	2.4G：150Mbps，5G：443Mbps	未测试
12	PANDA - PAU0A		-	mt7612u	WiFi5（ac）	WPA、WPA2	2.4G：150Mbps，5G：443Mbps	未测试
13	PANDA - PAU03		-	rt5370	WiFi4（b/n/g）	WEP、WPA、WPA2	2.4G：150Mbps	未测试

序号	网卡名称	产品图	参考价格(JD)	芯片	无线协议	支持加密标准	官标速率	测试结果
						、802.1x		
14	PANDA - PAU04		-	rt5370	WiFi4（b/n/g）	WEP、WPA、WPA2、802.1x	2.4G：150Mbps	未测试
15	ALFA AWUS036NHA（阿尔法）		592	ar9271	WiFi4（b/n/g）	-	2.4G：150Mbps	未测试

4 修订记录

序号	版本	作者	时间	备注
1	v1.0	网洞	2024.07.16	初稿。初代程序，支持 2.4G 和 5G 抓包和信道修改，支持 mt7921 网卡。
2	v1.2	网洞	2024.07.26	程序更新至 v1.2 版本。新增 6G 抓包支持与简单查询命令；新增 mt7612 网卡支持；优化部分逻辑等。
3	v1.3	网洞	2024.08.08	程序更新至 v1.3 版本。新增 WiFi 扫描功能；新增 rtl8811cu/rtl8821cu 网卡支持；优化部分逻辑等。
4	V1.4	网洞	2024.09.20	程序更新至 v1.4 版本。新增抓包频宽设置；新增地址和端口修改功能，无需再设置虚拟机的子网 ip 即可使用；新增 RT5572、mt7601 等网卡支持；优化部分逻辑等。
5	V1.5	网洞	2025.01.03	程序更新至 v1.5 版本。新增多信道捕获（扫描模式）；优化 WiFi 扫描功能，现在可以看到 AP 下的 sta；修改虚拟机初始 ip 为 10.25.25.100，降低冲突可能；新增 rtl8811au/rtl8832au/rtl8812bu/rtl8812cu 等网卡支持；优化部分逻辑，避免程序崩溃。

5 更多关于作者

闲鱼小铺（网洞在线）：抓包程序商品链接

CSDN 主页（网洞）：https://blog.csdn.net/DontDash

知乎主页（网洞）：https://www.zhihu.com/people/xiandaizhinan

BiliBili 主页（网洞）：https://space.bilibili.com/1961804712

抖音（网洞）：抖音空间主页

小红书（网洞）：小红书空间主页