Nexus Packet Sniffer 用户手册

Windows x64 数据包抓取、筛选与 PCAP 导出

项目	信息
产品版本	1.0
关于窗口版本	1.0 (2026.05.27)
手册版本	1.0

目录

1. 产品概述与适用范围

Nexus Packet Sniffer 是 Windows x64 桌面数据包抓取工具。它通过 WinDivert 在 NETWORK 层捕获符合条件的 IP 数据包，并写入 classic PCAP，供 Wireshark 或其他兼容工具分析。产品使用 WPF 图形界面管理筛选、抓取时间、文件大小和输出位置，不会将数据包重新注入网络。

适用场景

1. 针对特定源 / 目标 IP、端口或 TCP / UDP 通信进行短时间问题复现。
2. 生成可交付给网络、应用或安全团队的 PCAP 证据。
3. 在 Windows Server 上通过时间和大小限制控制抓取文件。
4. 排查本地服务、远程连接或指定应用协议的连通性问题。

项目	支持内容
数据包范围	IPv4 和 IPv6 的 IP 数据包；可选择全部、TCP+UDP、TCP 或 UDP
输出	classic PCAP，LINKTYPE_ETHERNET，扩展名 .pcap
操作系统	Windows Server 2012/2012 R2/2016/2019/2022/2025 x64；Windows 10/11 可用于开发和测试
权限	必须以管理员身份运行，才能加载和使用 WinDivert
不包括	ARP、RARP、STP 等非 IP / 链路层数据包；界面不显示 Payload

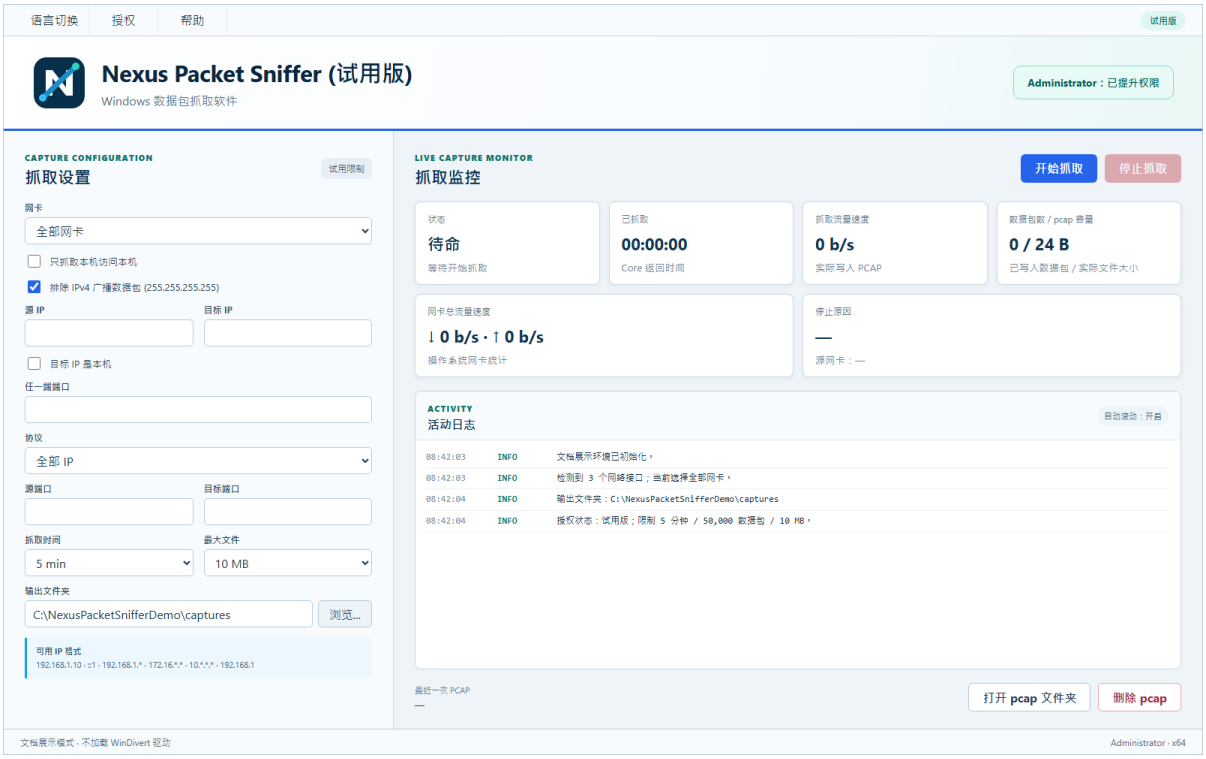
2. 系统要求、部署与启动

要求	说明
平台	64 位 Windows；不支持 32 位环境
运行权限	以管理员身份运行
驱动组件	WinDivert，需要与程序兼容的 x64 文件
磁盘空间	至少保留高于设置上限的可用空间，并考虑多次抓取和文件轮换

重要: 如果没有提升权限，程序可能无法加载 WinDivert、列出有效接口或开始抓取。

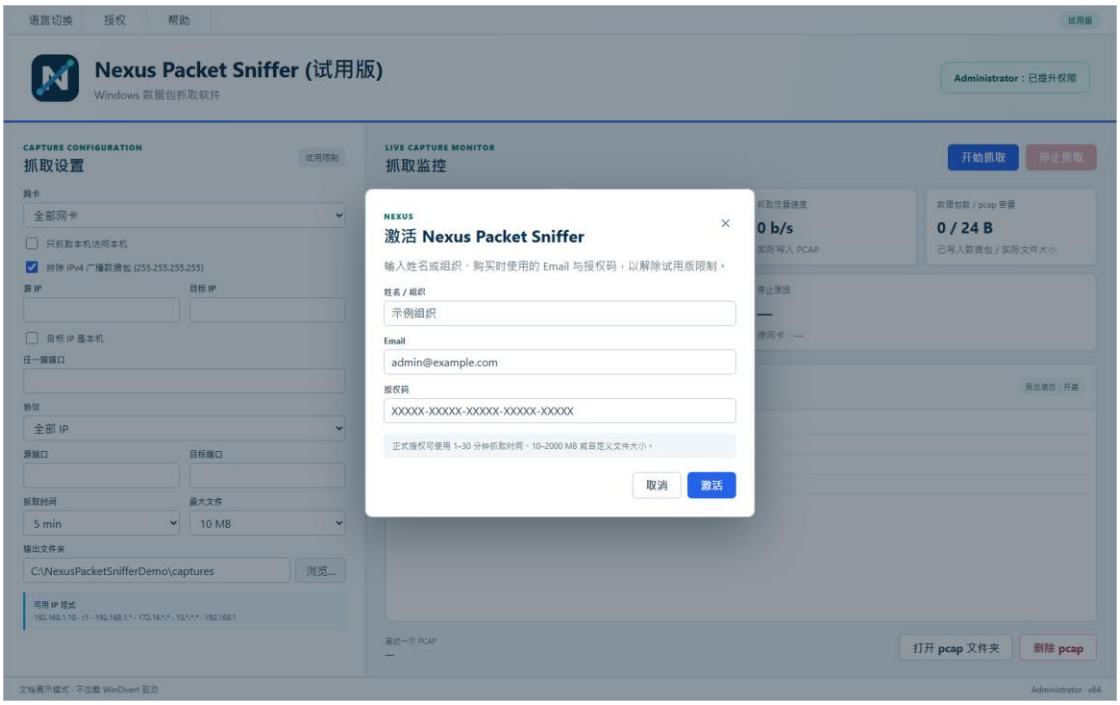
3. 试用版、授权与激活

未激活时产品以试用版运行。试用版可验证基本抓取流程，但时间、数据包数和文件大小均有限制；任何一项先达到都会停止。正式授权解除试用数据包数限制，并提供更长时间和更大文件选项。



1. 试用版主窗口和固定限制

功能	试用版	正式授权
最长时间	5 分钟	1、3、5、10、15、20、30 分钟
数据包数	50,000 个数据包	无试用数据包数上限
文件大小	10 MB	10、50、100、250、500、1000、2000 MB 或自定义
自定义大小	隐藏 / 不可用	可用



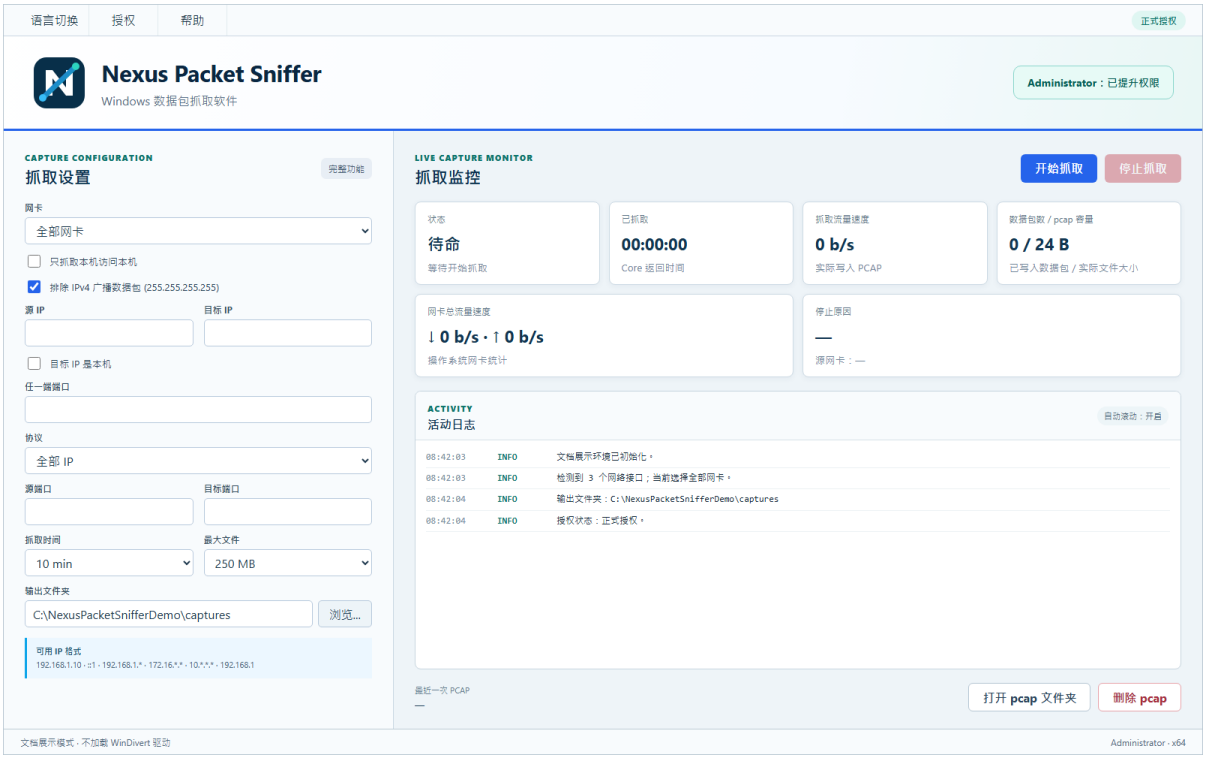
2. 授权激活窗口

激活

5. 打开“授权”菜单，选择输入授权密钥。
6. 输入姓名或组织、购买时使用的 Email 和正式授权码。
7. 单击“激活”，等待状态更新为正式授权。
8. 重新检查时间和文件大小列表是否显示完整选项。

4. 主窗口与菜单

主窗口左侧集中设置抓取条件，右侧显示实时监控和事件。顶部菜单提供语言、授权和帮助功能；状态徽章显示当前为试用版或正式授权。



3. 正式授权主窗口

区域	用途
顶部菜单	语言切换、授权、帮助和关于
抓取设置	接口、源 / 目标 IP、端口、协议和范围选项
限制与输出	抓取时间、文件大小、输出文件夹
控制	开始 / 停止抓取、打开 PCAP 文件夹、删除 PCAP
实时监控	状态、数据包数、字节数、经过时间、当前文件和停止原因
事件日志	启动、写入、停止和错误消息

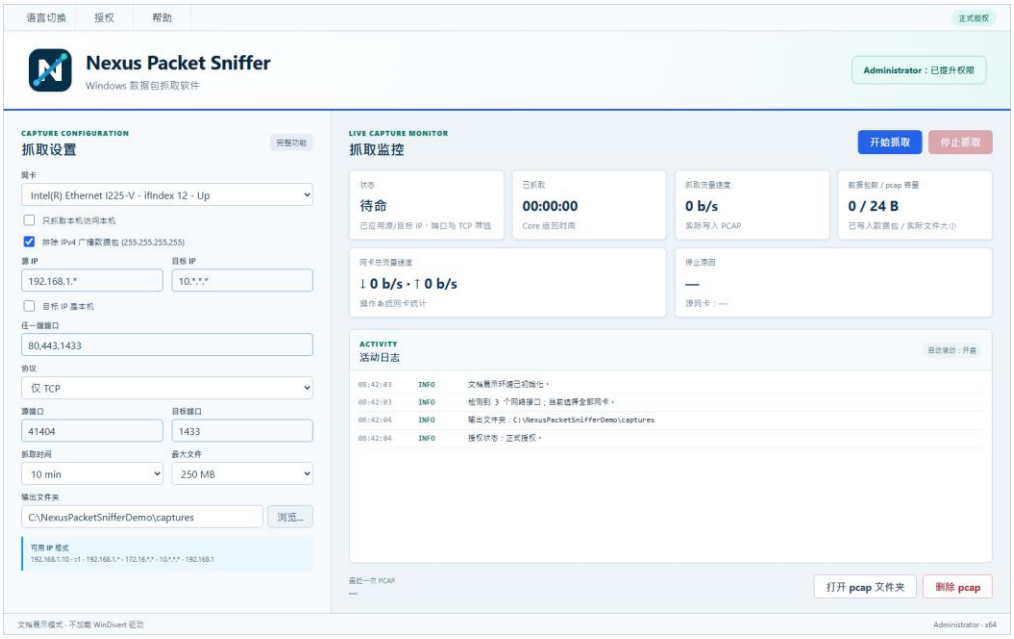
5. 快速开始：完成第一次抓取

9. 以管理员身份启动程序。
10. 选择要监控的网络接口；不确定时先选择当前承载流量的物理或虚拟接口。
11. 保持 IP、端口为空，协议选择全部 IP，先进行最小条件测试。
12. 试用版使用固定限制；正式版建议先选择 1 分钟、10 MB。
13. 选择输出文件夹，确认具有写入权限和足够空间。
14. 单击开始抓取，生成少量测试流量，观察数据包数和文件大小增加。
15. 单击停止，等待状态显示已停止，再打开文件夹和 PCAP。

重要: 第一次测试应生成非零大小的 .pcap，并可由 Wireshark 打开。如果数据包数保持 0，请先检查接口、方向和筛选。

6. 接口、IP、端口与协议筛选

源 IP、目标 IP、源端口、目标端口、协议和范围选项同时应用，彼此为 AND 关系。筛选越多，结果越精确，也越容易因条件不匹配而得到 0 个数据包。



4. 源 / 目标 IP、端口和 TCP 筛选示例

字段	格式与规则
IPv4 精确值	例如 192.168.1.25
IPv4 尾部通配符	例如 192.168.1.*、172.16.*.*、10.*.*.*；通配符只能连续出现在尾部
IPv4 前缀简写	例如 192.168.1，视为相同前缀范围
IPv6	支持完整或合法 IPv6 地址；不支持 IPv6 子网表示法和 zone ID
源 / 目标兼容性	同时指定时必须属于相同 IP 地址族
端口	1–65535，可用逗号分隔多个值，例如 80,443,1433
协议	全部 IP、TCP+UDP、TCP、UDP
仅本机	限制 loopback / 本机通信
目标为本机	限制目标端为本机的 inbound 数据包
排除广播	仅排除 IPv4 limited broadcast 255.255.255.255

7. 时间、文件大小与输出文件夹

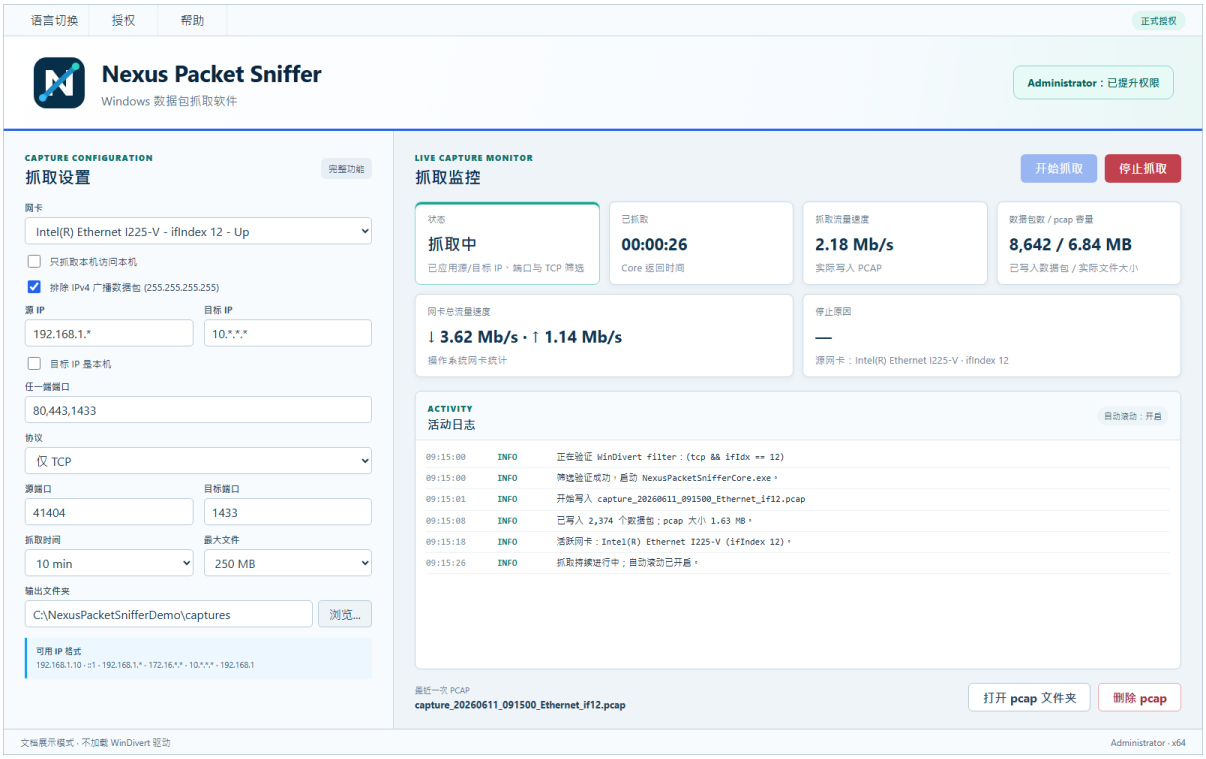
抓取时间和文件大小是保护磁盘与交付范围的主要控制。正式授权可选择预设值或自定义 MB；试用版固定为 5 分钟、50,000 个数据包、10 MB。

设置	建议
时间	问题复现通常先用 1–5 分钟；长时间抓取前先估算流量
文件大小	先以 10–100 MB 测试；高流量接口可能很快达到上限
自定义 MB	仅正式授权可用；输入正整数并预留磁盘空间
输出文件夹	使用本地固定磁盘；避免权限不稳定或可能中断的网络磁盘
文件名	包含开始时间和接口片段；同名时自动添加序号

重要: 停止判断以最先达到的限制为准。设置 30 分钟并不表示一定抓满 30 分钟，文件大小可能先达到上限。

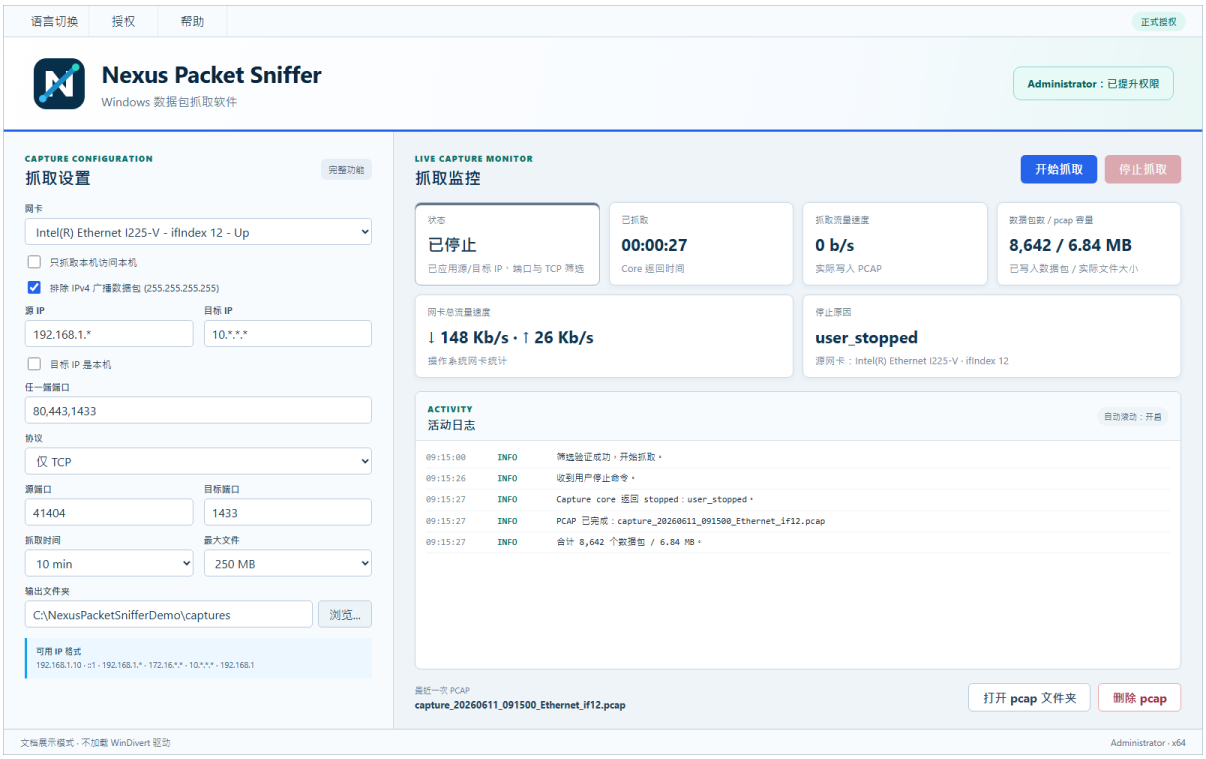
8. 抓取监控与停止条件

抓取开始后，设置字段会被锁定，避免运行中更改条件。监控区持续更新状态和计数；事件日志可用于判断是否成功启动、当前写入哪个文件以及停止原因。



5. 抓取中的实时监控

字段	说明
状态	starting、running、stopped 或 error
Packets	已写入 PCAP 的数据包数
Bytes	已处理 / 写入的数据量，实际显示按程序定义
Elapsed	本次抓取经过时间
File size	当前 PCAP 大小
Current file	本次抓取的完整输出文件名
Stop reason	用户停止、时间、数据包数、大小或错误



6. 停止后的结果与停止原因

停止原因	含义与后续操作
user_stopped	用户单击停止；等待文件关闭后再打开或移动
duration_limit	达到抓取时间上限；证据不足时可确认容量后重新抓取
packet_limit	试用版达到 50,000 个数据包
size_limit	达到文件大小上限；可缩小筛选或提高正式版上限
error	核心或文件写入错误；检查日志、权限、驱动和磁盘

重要: 单击停止后请等待状态变为已停止。强制结束程序可能导致 PCAP 未完整关闭。

9. PCAP 格式与 Wireshark 分析

输出采用 classic PCAP 和 LINKTYPE_ETHERNET。由于 WinDivert NETWORK 层提供 IP 数据包，程序会创建合成 Ethernet 头以提高分析工具兼容性；合成 MAC 不代表真实网卡地址。

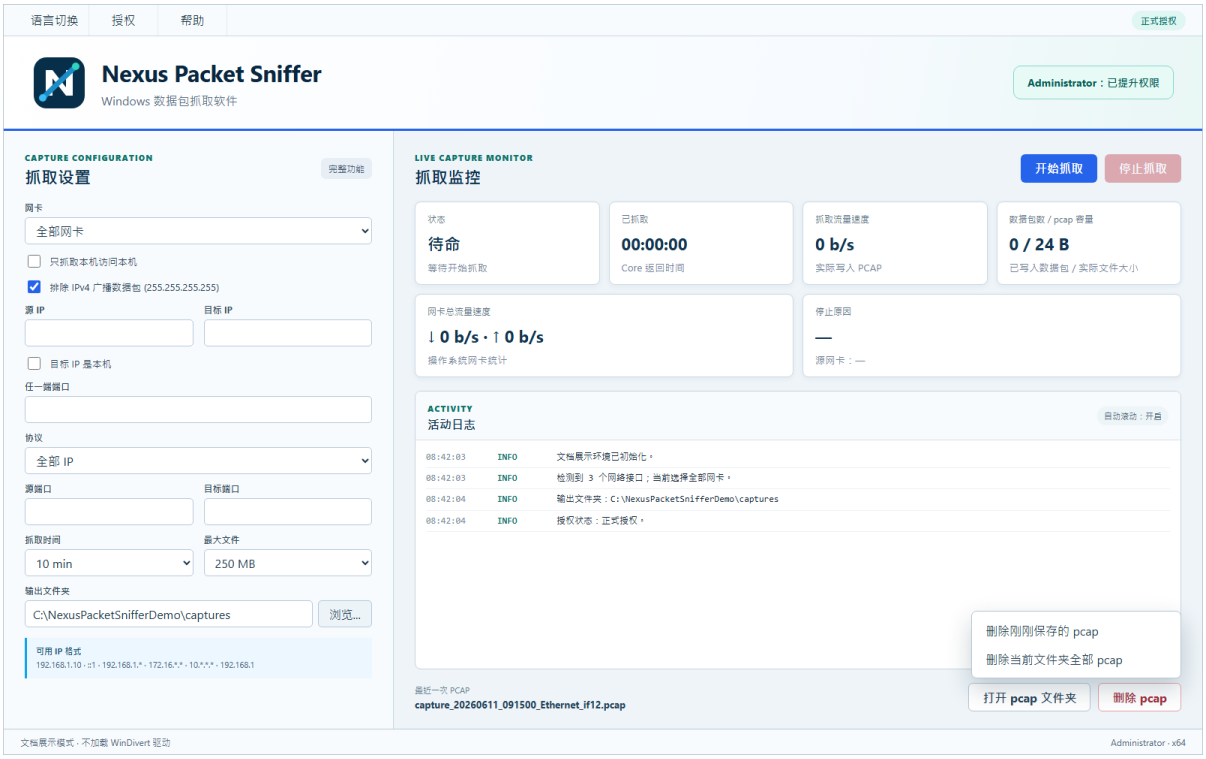
项目	值 / 说明
格式	classic PCAP (.pcap)
Link type	LINKTYPE_ETHERNET
合成源 MAC	02:00:00:00:00:01
合成目标 MAC	02:00:00:00:00:02
广播目标 MAC	ff:ff:ff:ff:ff:ff
Payload	界面不显示，但符合条件时保存在 PCAP 中

Wireshark 分析流程

16. 停止抓取并确认 PCAP 已关闭。
17. 在 Wireshark 选择 File > Open，打开输出的 .pcap。
18. 先使用 ip、ipv6、tcp、udp 或 tcp.port == 1433 等显示筛选器缩小范围。
19. 分析 IP、端口、标志、重传、延迟和 Payload 时，应以网络层内容为准。
20. 不要使用合成 MAC 推断物理设备、交换路径或真实二层拓扑。

10. PCAP 文件管理

主窗口可直接打开当前输出文件夹，或删除刚保存的 PCAP / 当前文件夹内全部 PCAP。抓取过程中删除功能不可用，以免移除正在写入的文件。

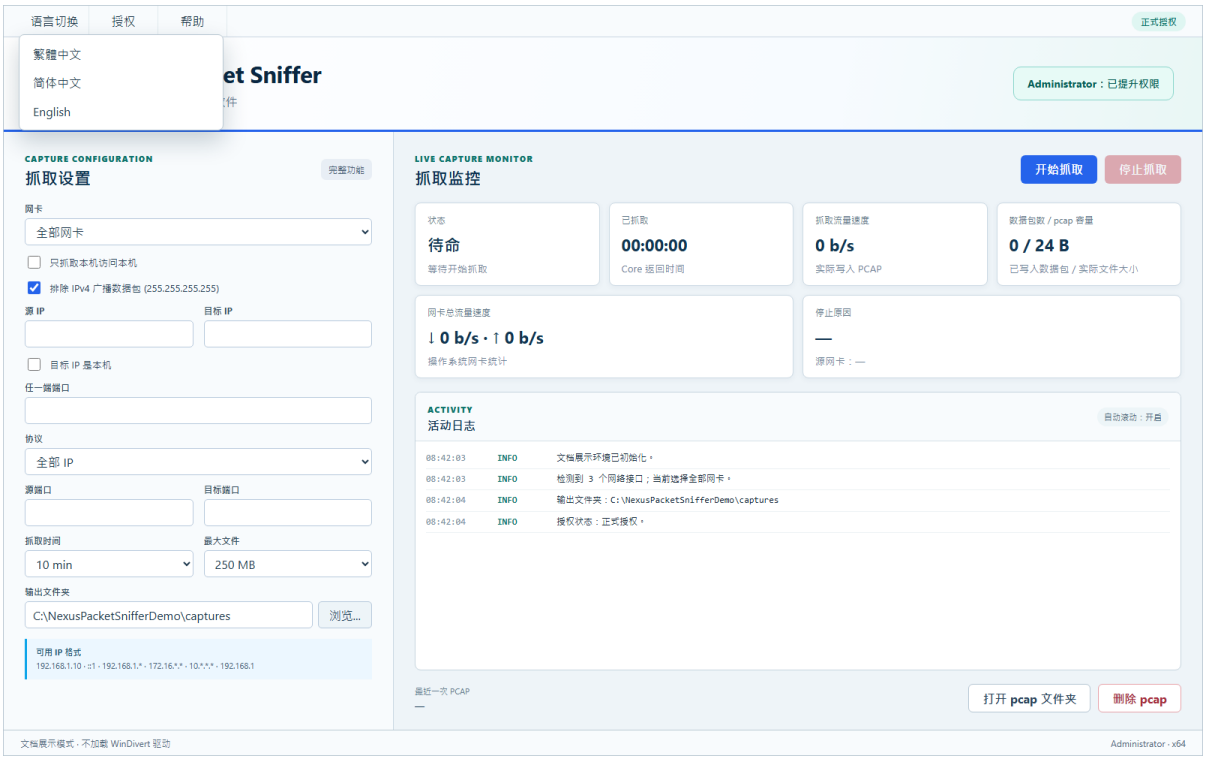


7. PCAP 删除菜单

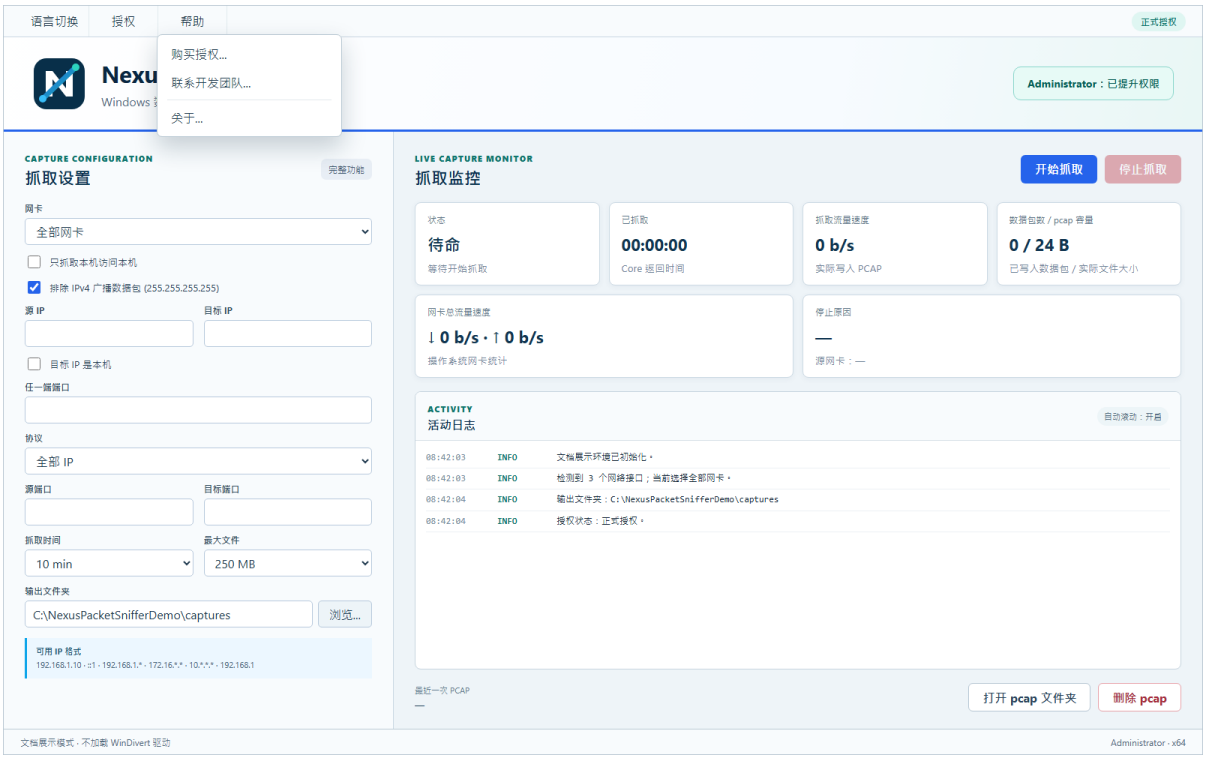
21. 先确认抓取状态为已停止。
22. 使用“打开 pcap 文件夹”核对目标文件夹和文件名。
23. 删除最新文件前，确认该文件不再需要分析或交付。
24. 删除全部 PCAP 前先备份需要保留的文件；操作范围是当前设置的输出文件夹。
25. 如果删除失败，关闭正在打开 PCAP 的分析工具并检查文件夹权限。

11. 语言、帮助与版本信息

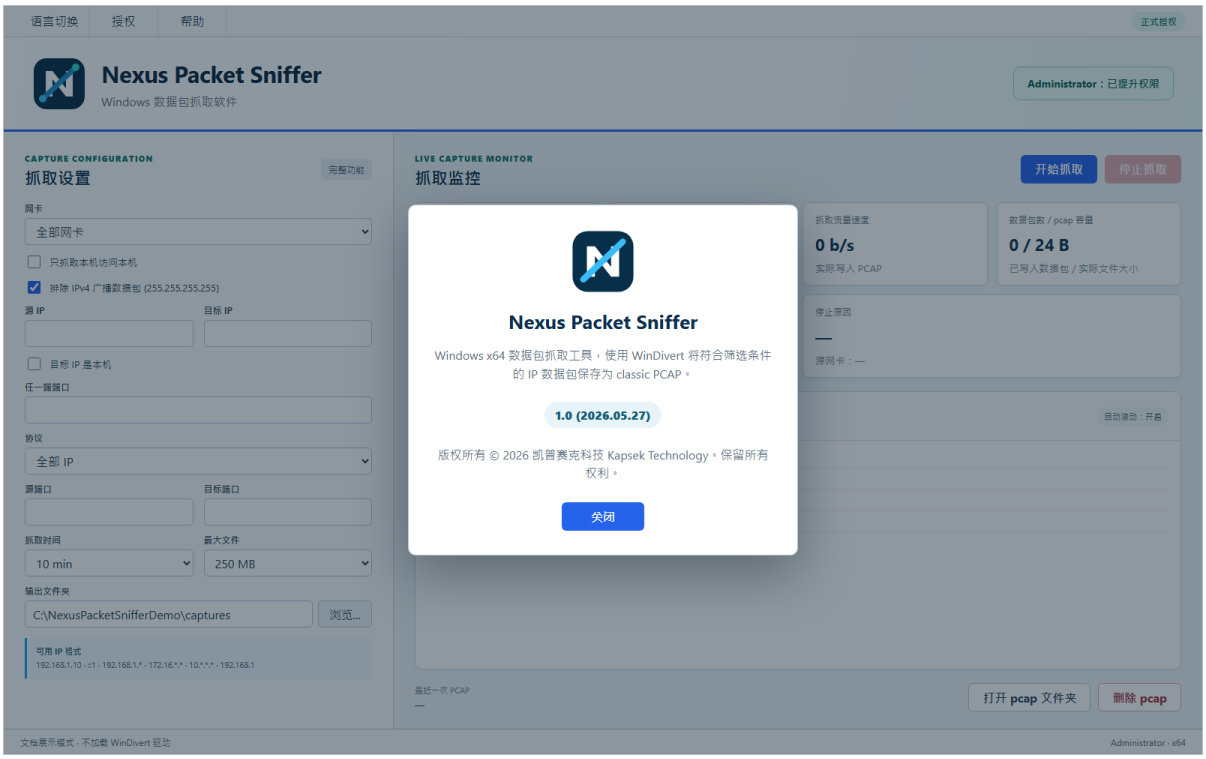
语言菜单可在繁体中文、简体中文和英文之间切换。切换后应检查当前字段和消息是否已更新。



8. 繁体中文、简体中文和英文菜单


语言切换
授权
帮助
正式授权
购买授权...
联系开发团队...
关于...
Nexu
Windows
Administrator：已提升权限
CAPTURE CONFIGURATION
抓取设置
完整功能
网卡
全部网卡
只抓取本机访问本机
排除 IPv4 广播数据包 (255.255.255.255)
源 IP
目标 IP
目标 IP 是本机
任一端口
协议
全部 IP
源端口
目标端口
抓取时间
10 min
最大文件
250 MB
输出文件夹
C:\NexusPacketSnifferDemo\captures
浏览...
可用 IP 格式
192.168.1.10 · ::1 · 192.168.1.* · 172.16.*.* · 10.*.*.* · 192.168.1
LIVE CAPTURE MONITOR
抓取监控
开始抓取
停止抓取
状态
待命
等待开始抓取
已抓取
00:00:00
Core 返回时间
抓取流量速度
0 b/s
实际写入 PCAP
数据包数 / pcap 容量
0 / 24 B
已写入数据包 / 实际文件大小
网卡总流量速度
↓ 0 b/s · ↑ 0 b/s
操作系统网卡统计
停止原因
—
源网卡：—
ACTIVITY
活动日志
自动滚动：开启
08:42:03 INFO 文档展示环境已初始化。
08:42:03 INFO 检测到 3 个网络接口；当前选择全部网卡。
08:42:04 INFO 输出文件夹：C:\NexusPacketSnifferDemo\captures
08:42:04 INFO 授权状态：正式授权。
最近一次 PCAP
—
打开 pcap 文件夹
删除 pcap
文档展示模式 · 不加载 WinDivert 驱动
Administrator · x64

9. 帮助与支持菜单



10. 关于窗口和版本信息

26. “购买授权”和“联系开发团队”应使用组织批准的正式渠道。

27. 提交支持信息时包括产品版本、Windows 版本、复现步骤、错误消息和脱敏后的事件日志。

28. 除非支持人员明确要求并已批准，不要直接附加未脱敏的 PCAP 或授权码。

29. 关于窗口显示版本 1.0 (2026.05.27)；报告问题时请一并提供。

12. 故障排除

现象	可能原因	处理方式
无法开始抓取	未以管理员运行、WinDivert 缺失 / 被阻止	提升权限；确认 x64 组件和企业终端防护策略
数据包数一直为 0	接口错误、筛选过严、方向不匹配	先清空 IP/端口、选择全部 IP，确认实际承载流量的接口
IP 格式错误	通配符位置不合法、IPv6 包含 zone ID	改用精确地址或合法的尾部 IPv4 通配符
端口格式错误	包含 0、超过 65535 或非数字	使用 1–65535 的逗号分隔整数
PCAP 很快停止	流量高，先达到大小 / 试用数据包上限	缩小筛选；正式版可提高大小或使用更短复现窗口
PCAP 无法删除	仍在抓取、Wireshark 正在使用、权限不足	停止抓取并关闭分析工具；检查文件夹权限
磁盘空间不足	输出文件夹容量不足	清理或更换本地文件夹；降低文件上限
Wireshark 显示陌生 MAC	产品使用合成 Ethernet 头	按 IP 和传输层字段分析，不按 MAC 判断物理来源

13. 已知限制与操作参考

已知限制

30. NETWORK 层不捕获 ARP、RARP、STP 等非 IP 数据包。
31. 排除广播仅针对 IPv4 limited broadcast 255.255.255.255，不表示排除全部 multicast 或 IPv6 multicast。
32. IPv4 通配符只能连续出现在尾部；不支持 192.*.1.*。
33. 不支持 IPv6 子网表示法和 zone ID。
34. 同时指定源和目标 IP 时必须使用相同 IP 地址族。
35. 主界面不显示 Payload；需在授权与安全条件下使用 Wireshark 检查 PCAP。
36. 合成 Ethernet MAC 不是物理 MAC，不能用于二层归属判断。

操作参考

类别	操作参考
试用停止条件	5 分钟、50,000 packets、10 MB，先达到者为准
正式时间	1 / 3 / 5 / 10 / 15 / 20 / 30 分钟
正式大小	10 / 50 / 100 / 250 / 500 / 1000 / 2000 MB 或自定义
端口	1–65535，逗号分隔
IP	精确 IPv4/IPv6；IPv4 尾部通配符 / 前缀简写
设置逻辑	字段之间为 AND；空白表示不限制
PCAP 命名	capture_{yyyyMMdd_HHmmss}_{adapterPart}.pcap，冲突时添加序号