Nexus Packet Sniffer 使用手冊

Windows x64 封包側錄、篩選與 PCAP 匯出

項目	資訊
產品版本	1.0
關於視窗版本	1.0 (2026.05.27)
手冊版本	1.0

目錄

1. 產品概觀與適用範圍

Nexus Packet Sniffer 是 Windows x64 桌面封包側錄工具。它透過 WinDivert 在 NETWORK 層擷取符合條件的 IP 封包，並寫入 classic PCAP，供 Wireshark 或其他相容工具分析。產品以 WPF 圖形介面管理篩選、錄製時間、檔案大小與輸出位置，不會將封包重新注入網路。

適合的工作情境

1. 針對特定來源 / 目的 IP、Port 或 TCP / UDP 通訊進行短時間問題重現。
2. 建立可交付給網路、應用程式或資安團隊的 PCAP 證據。
3. 在 Windows Server 上以有限時間與大小控制側錄檔案。
4. 排除本機服務、遠端連線或指定應用協定的連通性問題。

項目	支援內容
封包範圍	IPv4 與 IPv6 的 IP 封包；可選全部、TCP+UDP、TCP 或 UDP
輸出	classic PCAP，LINKTYPE_ETHERNET，副檔名 .pcap
作業系統	Windows Server 2012/2012 R2/2016/2019/2022/2025 x64；Windows 10/11 可用於開發與測試
權限	必須以系統管理員身分執行，才能載入與使用 WinDivert
不涵蓋	ARP、RARP、STP 等非 IP / 鏈路層封包；介面不顯示封包 Payload

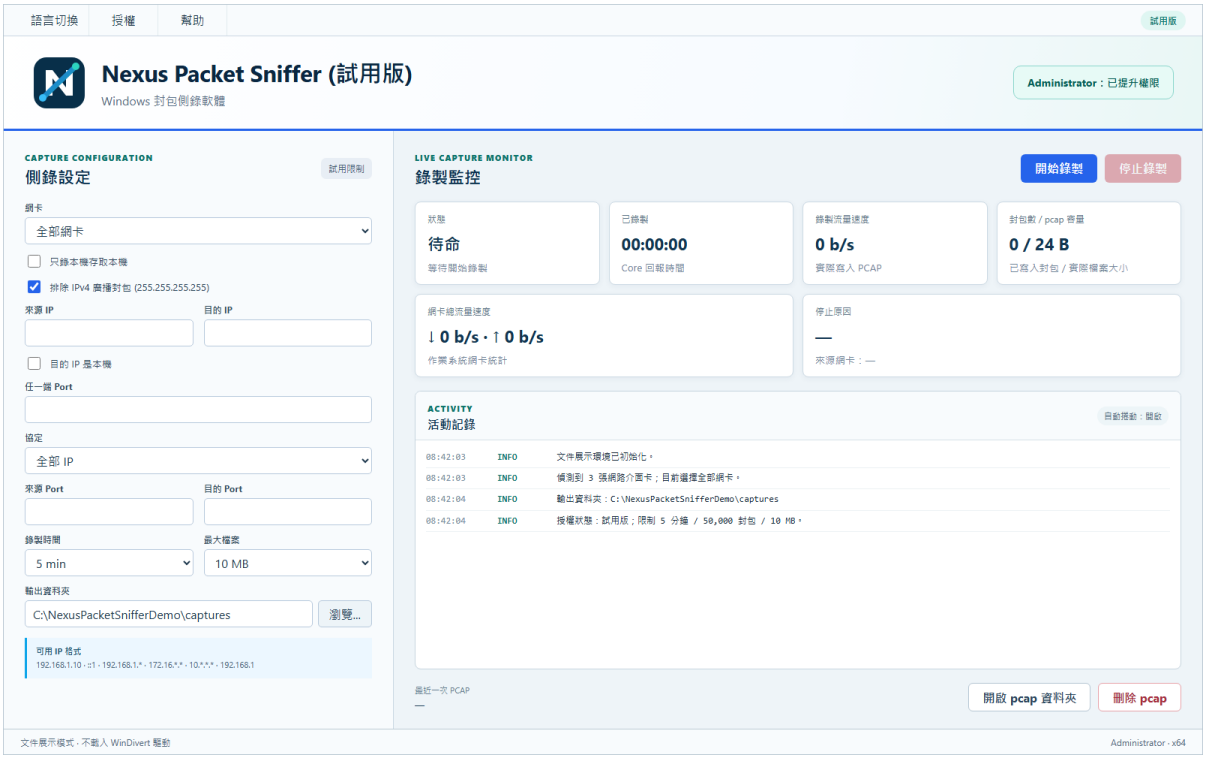
2. 系統需求、部署與啟動

需求	說明
平台	64 位元 Windows；產品不支援 32 位元環境
執行權限	以系統管理員身分執行
驅動元件	WinDivert ，需與程式使用相容的 x64 檔案
磁碟空間	至少保留高於設定上限的可用空間，並考量多次側錄與檔案輪替

重要: 若未提升權限，程式可能無法載入 WinDivert、列出有效介面或開始側錄。

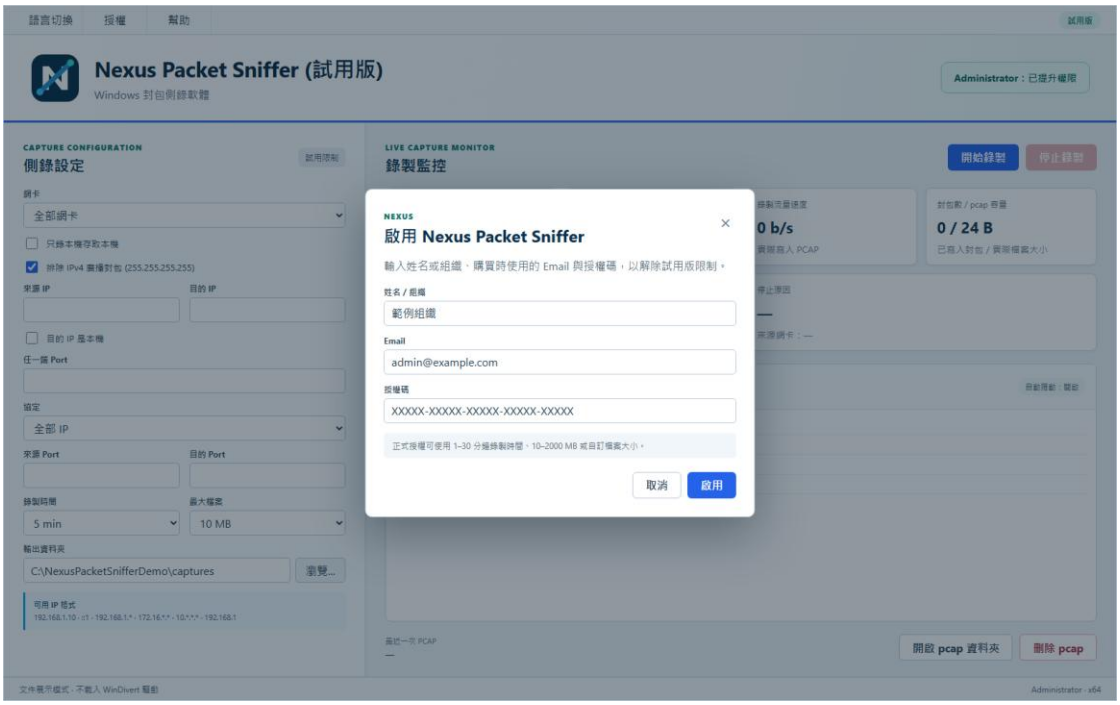
3. 試用版、授權與啟用

未啟用時產品以試用版執行。試用版可驗證基本側錄流程，但時間、封包數與檔案大小均有上限；任何一項先到達都會停止。正式授權會解除封包數限制，並提供較長時間與較大檔案選項。



1. 試用版主畫面與固定限制

功能	試用版	正式授權
最長時間	5 分鐘	1、3、5、10、15、20、30 分鐘
封包數	50,000 個封包	無試用封包數上限
檔案大小	10 MB	10、50、100、250、500、1000、2000 MB 或自訂
自訂大小	隱藏 / 不可用	可用



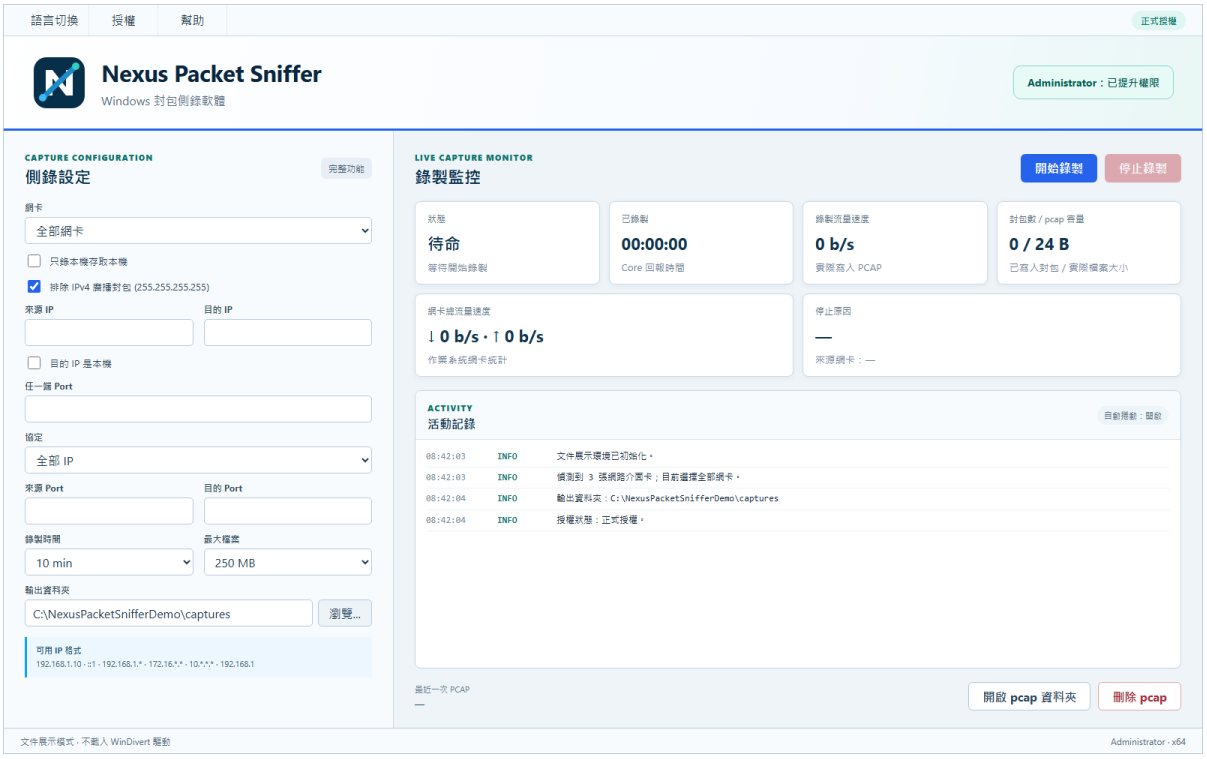
2. 授權啟用視窗

啟用

5. 開啟「授權」選單，選擇輸入授權金鑰。
6. 輸入姓名或組織、購買時使用的 Email 與正式授權碼。
7. 按下「啟用」，等待狀態更新為正式授權。
8. 重新檢查時間與檔案大小清單是否已顯示完整選項。

4. 主視窗與選單

主視窗左側集中設定側錄條件，右側顯示即時監控與事件。頂端選單提供語言、授權與說明功能；狀態徽章則顯示目前為試用版或正式授權。



3. 正式授權主視窗

區域	用途
頂端選單	語言切換、授權、說明與關於
側錄設定	介面、來源 / 目的 IP、Port、通訊協定與範圍選項
限制與輸出	錄製時間、檔案大小、輸出資料夾
控制	開始 / 停止側錄、開啟 PCAP 資料夾、刪除 PCAP
即時監控	狀態、封包數、位元組數、經過時間、目前檔案與停止原因
事件紀錄	啟動、寫入、停止與錯誤訊息

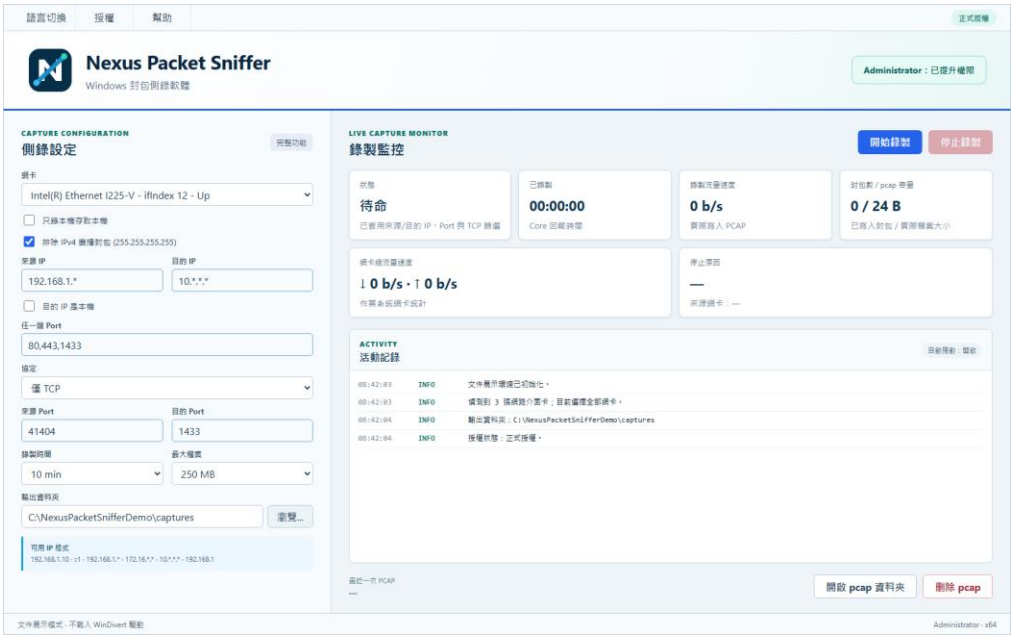
5. 快速開始：完成第一次側錄

9. 以系統管理員身分啟動程式。
10. 選擇要監控的網路介面；不確定時先選擇目前承載流量的實體或虛擬介面。
11. 保持 IP、Port 空白，通訊協定選擇全部 IP，先做最小條件測試。
12. 試用版使用固定限制；正式版建議先選 1 分鐘、10 MB。
13. 選擇輸出資料夾，確認有寫入權限與足夠空間。
14. 按下開始側錄，產生少量測試流量，觀察封包數與檔案大小增加。
15. 按下停止，等待狀態顯示已停止，再開啟資料夾與 PCAP。

重要: 第一次測試應產生非零大小的 .pcap，且可由 Wireshark 開啟。若封包數維持 0，先檢查介面、方向與篩選。

6. 介面、IP、Port 與通訊協定篩選

來源 IP、目的 IP、來源 Port、目的 Port、通訊協定與範圍選項同時套用，彼此為 AND 關係。篩選越多，結果越精確，也越容易因條件不符而得到 0 個封包。



4. 來源 / 目的 IP、Port 與 TCP 篩選範例

欄位	格式與規則
IPv4 精確值	例如 192.168.1.25
IPv4 尾端萬用字元	例如 192.168.1.*、172.16.*.*、10.*.*.*；萬用字元只能連續出現在尾端
IPv4 前綴簡寫	例如 192.168.1，視為相同前綴範圍
IPv6	支援完整或合法 IPv6 位址；不支援 IPv6 子網表示法與 zone ID
來源 / 目的相容性	同時指定時必須屬於相同 IP 家族
Port	1–65535，可用逗號分隔多個值，例如 80,443,1433
通訊協定	全部 IP、TCP+UDP、TCP、UDP
僅本機	限制 loopback / 本機通訊
目的為本機	限制目的端為本機的 inbound 封包
排除廣播	僅排除 IPv4 limited broadcast 255.255.255.255

7. 時間、檔案大小與輸出資料夾

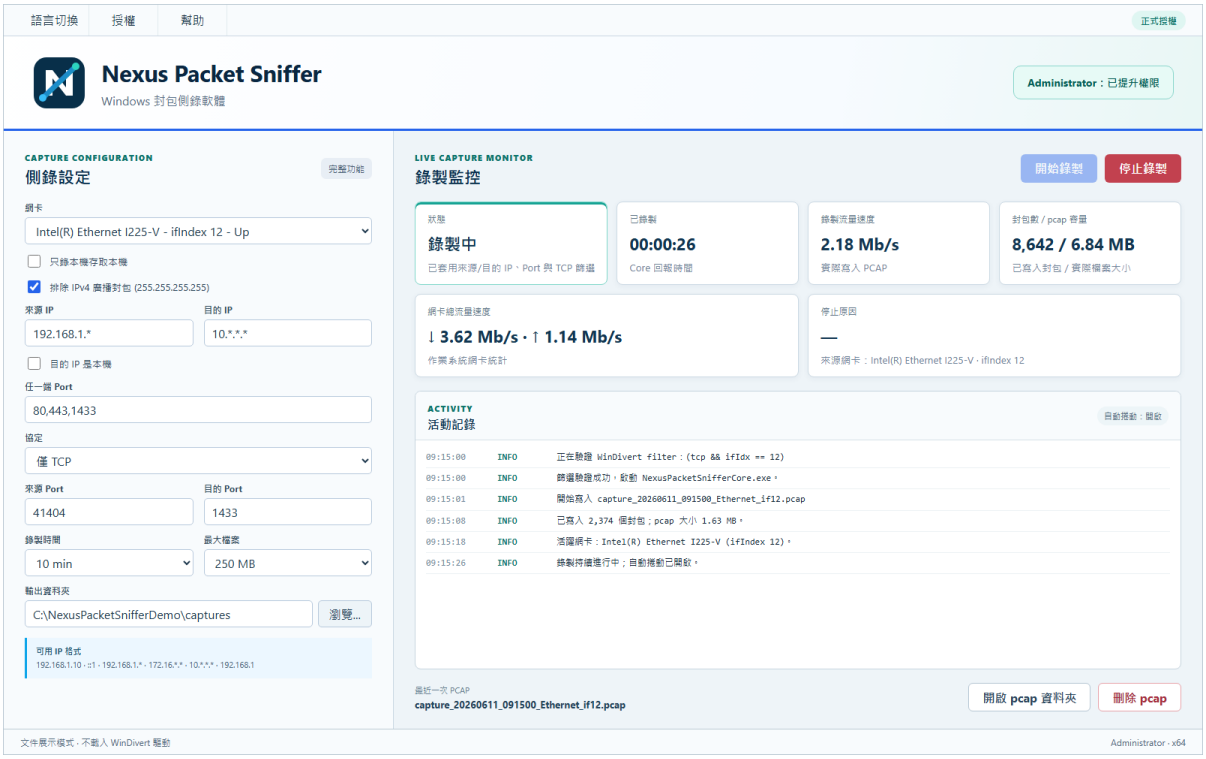
錄製時間與檔案大小是保護磁碟與交付範圍的主要控制。正式授權可選擇預設值或自訂 MB；試用版固定為 5 分鐘、50,000 個封包、10 MB。

設定	建議
時間	問題重現通常先用 1–5 分鐘；長時間側錄前先估算流量
檔案大小	先以 10–100 MB 測試；高流量介面可能很快到達上限
自訂 MB	僅正式授權可用；輸入正整數並預留磁碟空間
輸出資料夾	使用本機固定磁碟；避免權限不穩定或會中斷的網路磁碟
檔名	包含開始時間與介面片段；同名時自動加序號

重要: 停止判斷以先到達的限制為準。設定 30 分鐘不代表一定錄滿 30 分鐘，檔案大小可能先到上限。

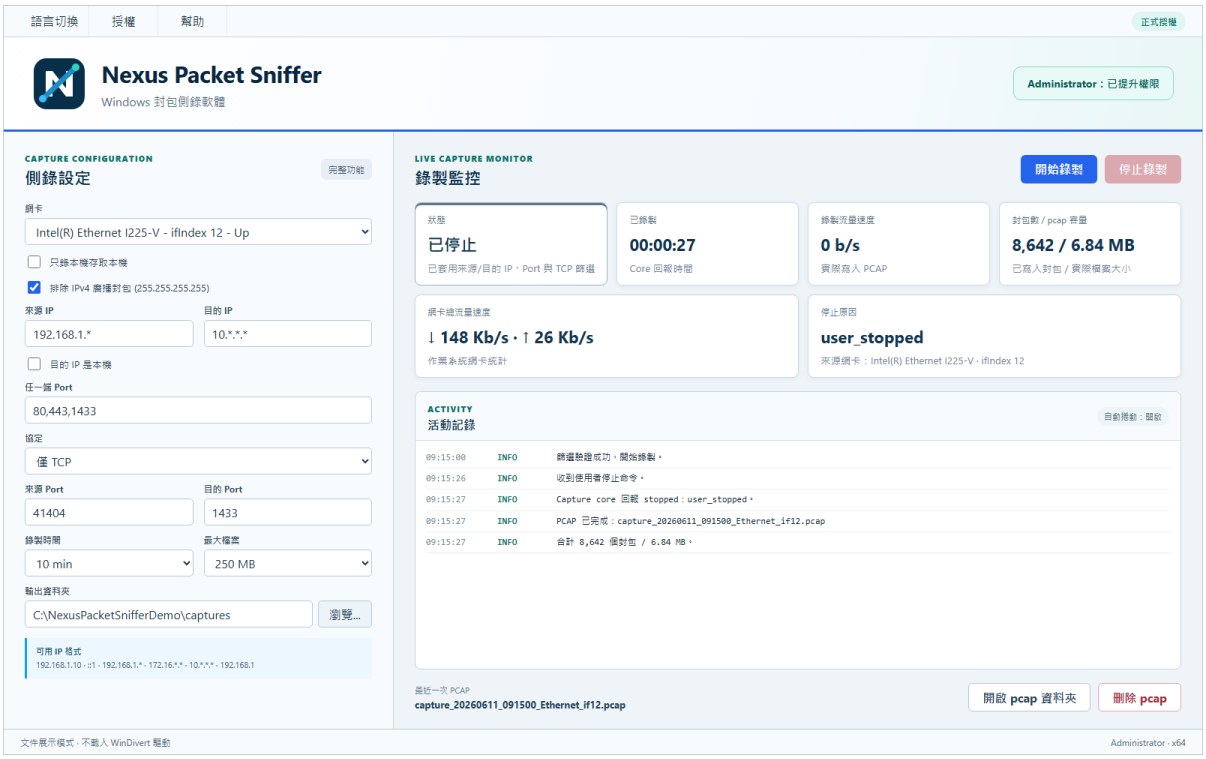
8. 側錄中監控與停止條件

側錄開始後，設定欄位會被鎖定，避免執行中變更條件。監控區持續更新狀態與計數；事件紀錄可用來判斷是否成功啟動、目前寫入哪個檔案，以及為何停止。



5. 側錄中即時監控

欄位	解讀方式
狀態	starting、running、stopped 或 error
Packets	已寫入 PCAP 的封包數
Bytes	已處理 / 寫入的資料量，實際顯示依程式定義
Elapsed	本次側錄經過時間
File size	目前 PCAP 的大小
Current file	本次側錄的完整輸出檔名
Stop reason	使用者停止、時間、封包數、大小或錯誤



6. 停止後的結果與停止原因

停止原因	意義與後續動作
user_stopped	使用者按下停止；等待檔案關閉後再開啟或移動
duration_limit	到達錄製時間上限；若證據不足，可在確認容量後重新錄製
packet_limit	試用版到達 50,000 個封包
size_limit	到達檔案大小上限；可縮小篩選或提高正式版上限
error	核心或檔案寫入錯誤；檢查紀錄、權限、驅動與磁碟

重要: 按下停止後請等候狀態變成已停止。強制結束程序可能造成 PCAP 未完整關閉。

9. PCAP 格式與 Wireshark 分析

輸出採 classic PCAP 與 LINKTYPE_ETHERNET。由於 WinDivert NETWORK 層提供的是 IP 封包，程式會建立合成 Ethernet 標頭，以提高分析工具相容性；合成 MAC 不代表真實網卡位址。

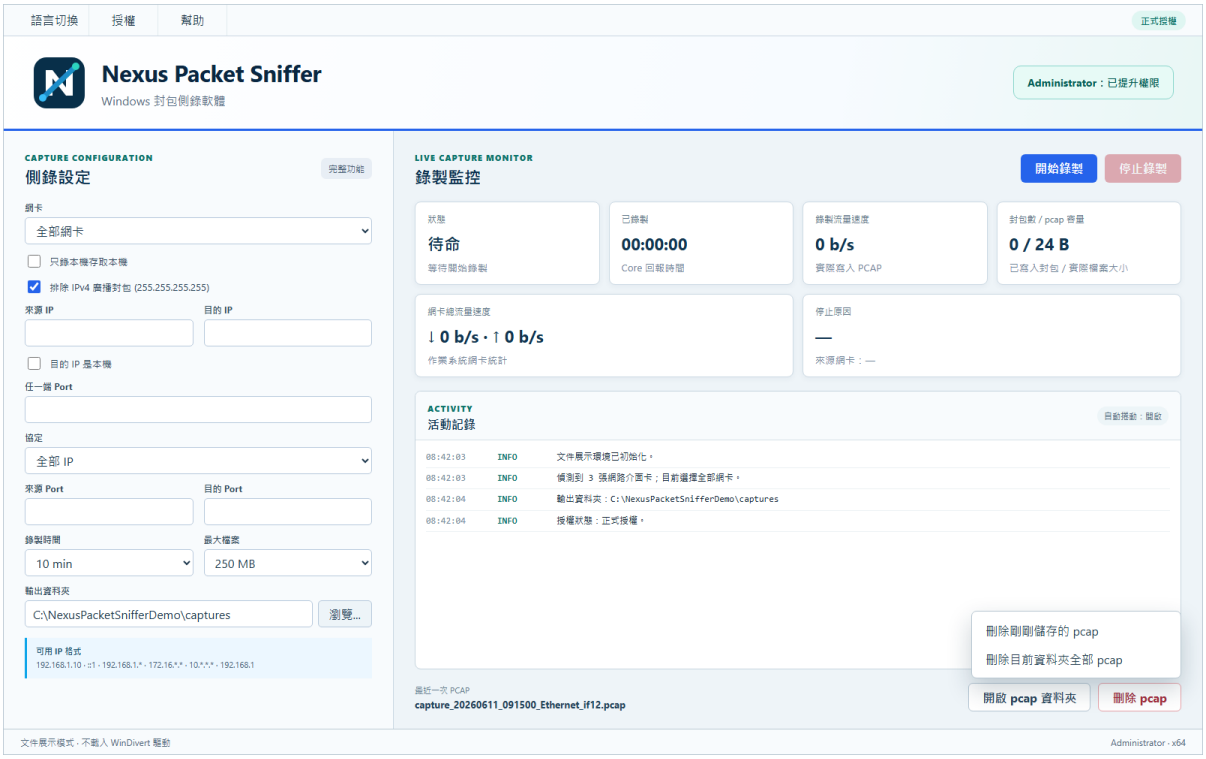
項目	值 / 說明
格式	classic PCAP (.pcap)
Link type	LINKTYPE_ETHERNET
合成來源 MAC	02:00:00:00:00:01
合成目的 MAC	02:00:00:00:00:02
廣播目的 MAC	ff:ff:ff:ff:ff:ff
Payload	介面不顯示，但符合條件時會保存在 PCAP

Wireshark 分析流程

16. 停止側錄並確認 PCAP 已關閉。
17. 在 Wireshark 選擇 File > Open，開啟輸出的 .pcap。
18. 先用 ip、ipv6、tcp、udp 或 tcp.port == 1433 等顯示篩選器縮小範圍。
19. 分析 IP、Port、旗標、重傳、延遲與 Payload 時，應以網路層內容為準。
20. 不要用合成 MAC 推斷實體設備、交換器路徑或真實二層拓樸。

10. PCAP 檔案管理

主視窗可直接開啟目前輸出資料夾，或刪除剛儲存的 PCAP / 目前資料夾內全部 PCAP。刪除功能在側錄中不可用，以避免移除正在寫入的檔案。

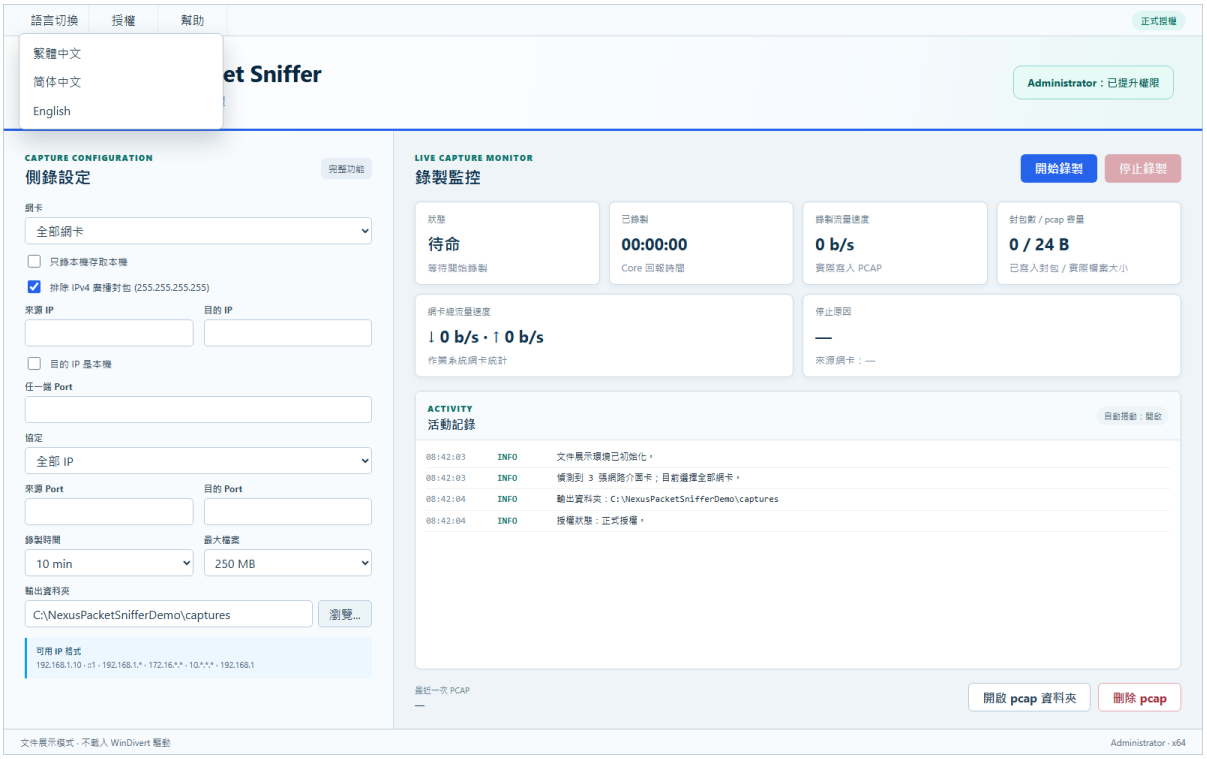


7. PCAP 刪除選單

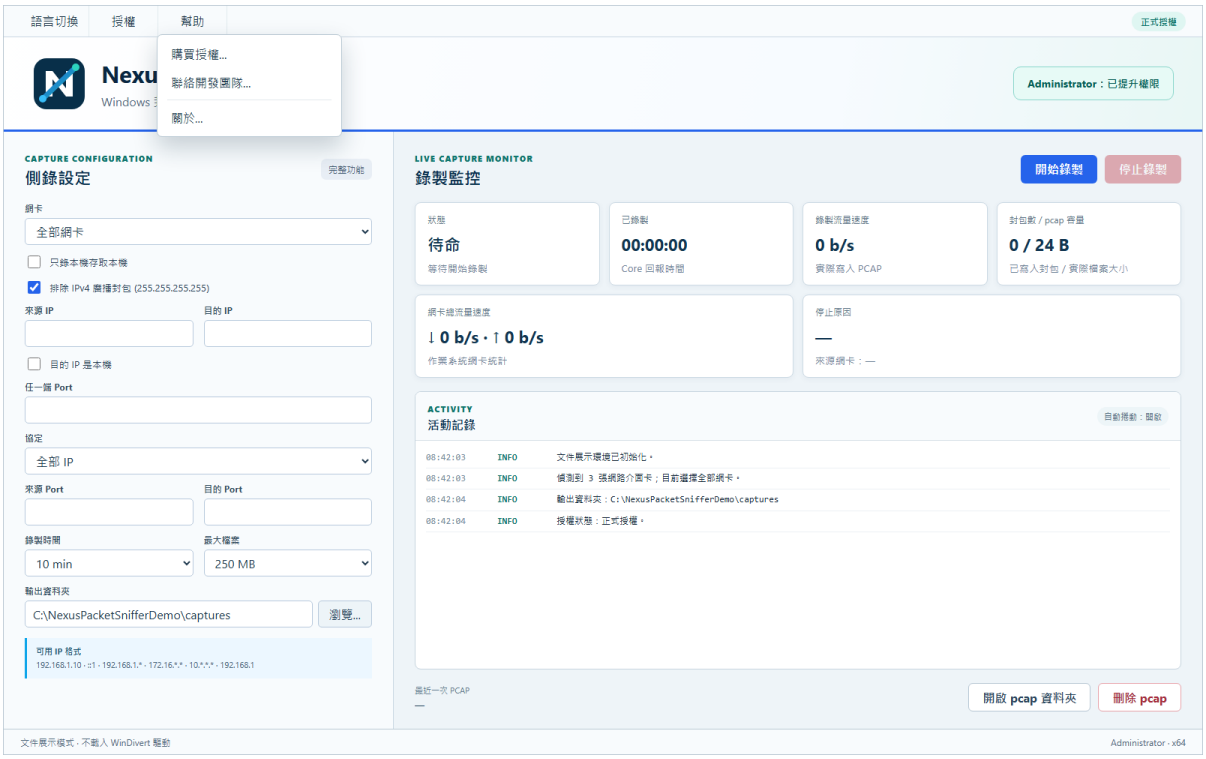
21. 先確認側錄狀態為已停止。
22. 使用「開啟 pcap 資料夾」核對目標資料夾與檔名。
23. 刪除最新檔案前，確認該檔案不再需要分析或交付。
24. 刪除全部 PCAP 前，先備份需要保留的檔案；操作範圍是目前設定的輸出資料夾。
25. 若刪除失敗，關閉正在開啟 PCAP 的分析工具並檢查資料夾權限。

11. 語言、說明與版本資訊

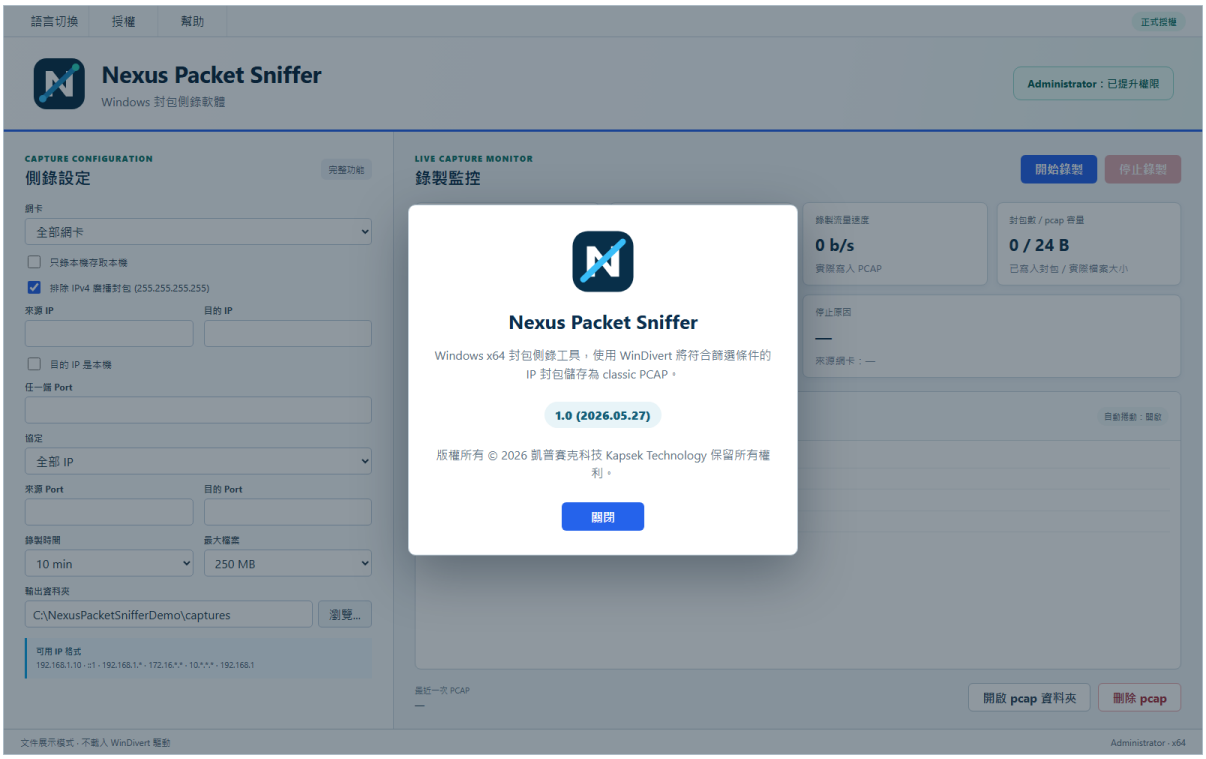
語言選單可在繁體中文、簡體中文與英文之間切換。切換後應檢查目前欄位與訊息是否已更新。



8. 繁體中文、簡體中文與英文選單


語言切換
授權
幫助
購買授權...
聯絡開發團隊...
關於...
正式授權
Nexu
Windows
Administrator：已提升權限
CAPTURE CONFIGURATION
側錄設定
完整功能
網卡
全部網卡
只錄本機存取本機
排除 IPv4 廣播封包 (255.255.255.255)
來源 IP
目的 IP
目的 IP 是本機
任一端 Port
協定
全部 IP
來源 Port
目的 Port
錄製時間
10 min
最大檔案
250 MB
輸出資料夾
C:\NexusPacketSnifferDemo\captures
瀏覽...
可用 IP 格式
192.168.1.10 · ::1 · 192.168.1.* · 172.16.*.* · 10.*.*.* · 192.168.1
LIVE CAPTURE MONITOR
錄製監控
開始錄製
停止錄製
狀態
待命
等待開始錄製
已錄製
00:00:00
Core 回報時間
錄製流量速度
0 b/s
實際寫入 PCAP
封包數 / pcap 容量
0 / 24 B
已寫入封包 / 實際檔案大小
網卡總流量速度
↓ 0 b/s · ↑ 0 b/s
作業系統網卡統計
停止原因
—
來源網卡：—
ACTIVITY
活動記錄
自動捲動：開啟
08:42:03 INFO 文件展示環境已初始化。
08:42:03 INFO 偵測到 3 張網路介面卡；目前選擇全部網卡。
08:42:04 INFO 輸出資料夾：C:\NexusPacketSnifferDemo\captures
08:42:04 INFO 授權狀態：正式授權。
最近一次 PCAP
—
開啟 pcap 資料夾
刪除 pcap
文件展示模式 · 不載入 WinDivert 驅動
Administrator · x64

9. 說明與支援選單



10. 關於視窗與版本資訊

26. 「購買授權」與「聯絡開發團隊」應使用組織核准的正式管道。

27. 送出支援資訊時包含產品版本、Windows 版本、重現步驟、錯誤訊息與去敏後的事件紀錄。

28. 除非支援人員明確要求且已核准，不要直接附上未去敏的 PCAP 或授權碼。

29. 關於視窗顯示版本 1.0 (2026.05.27)；回報問題時請一併提供。

12. 疑難排解

現象	可能原因	處理方式
無法開始側錄	未以管理員執行、WinDivert 缺失 / 被阻擋	提升權限；確認 x64 元件與企業端點防護政策
封包數一直是 0	介面選錯、篩選過嚴、方向不符	先清空 IP/Port、選全部 IP，確認實際承載流量的介面
IP 格式錯誤	萬用字元位置不合法、IPv6 含 zone ID	改用精確位址或合法尾端 IPv4 萬用字元
Port 格式錯誤	包含 0、超過 65535 或非數字	改用 1–65535 的逗號分隔整數
PCAP 很快停止	流量高，先到大小 / 試用封包上限	縮小篩選；正式版可提高大小或改用較短重現窗口
PCAP 無法刪除	仍在側錄、Wireshark 正在使用、權限不足	停止側錄並關閉分析工具；檢查資料夾權限
磁碟空間不足	輸出資料夾容量不足	清理或更換本機資料夾；降低檔案上限
Wireshark 顯示陌生 MAC	產品使用合成 Ethernet 標頭	以 IP 與傳輸層欄位分析，不以 MAC 判斷實體來源

13. 已知限制與操作參考

已知限制

30. NETWORK 層不擷取 ARP、RARP、STP 等非 IP 封包。
31. 排除廣播只針對 IPv4 limited broadcast 255.255.255.255，不代表排除所有 multicast 或 IPv6 multicast。
32. IPv4 萬用字元只能連續出現在尾端；不支援 192.*.1.*。
33. 不支援 IPv6 子網表示法與 zone ID。
34. 來源與目的 IP 同時指定時必須使用相同 IP 家族。
35. 主介面不顯示 Payload；需在授權與安全條件下使用 Wireshark 檢查 PCAP。
36. 合成 Ethernet MAC 不是實體 MAC，不能用於二層歸屬判斷。

操作參考

類別	操作參考
試用停止條件	5 分鐘、50,000 packets、10 MB，先到者為準
正式時間	1 / 3 / 5 / 10 / 15 / 20 / 30 分鐘
正式大小	10 / 50 / 100 / 250 / 500 / 1000 / 2000 MB 或自訂
Port	1–65535，逗號分隔
IP	精確 IPv4/IPv6；IPv4 尾端萬用字元 / 前綴簡寫
設定邏輯	欄位間為 AND；空白表示不限制
PCAP 命名	capture_{yyyyMMdd_HHmmss}_{adapterPart}.pcap，衝突時加序號