

Wireshark tutorial

Wireshark

- 開放原始碼，基於**GPL**授權
- 免費使用，而且功能十分強大
- 方便擷取網路上的封包，並檢視每一個封包的詳細資訊
- Wireshark支援
 - Windows
 - Linux
 - macOS
 - ...等多種作業系統
- 目前Wireshark的穩定版本為**3.4.9**

安裝Wireshark

- <https://www.wireshark.org/download.html>

Download Wireshark

The current stable release of Wireshark is 3.4.9. It supersedes all previous releases. You can also download the latest development release (3.6.0rc1) and documentation.

Stable Release (3.4.9)

↓ Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS Intel 64-bit .dmg
Source Code

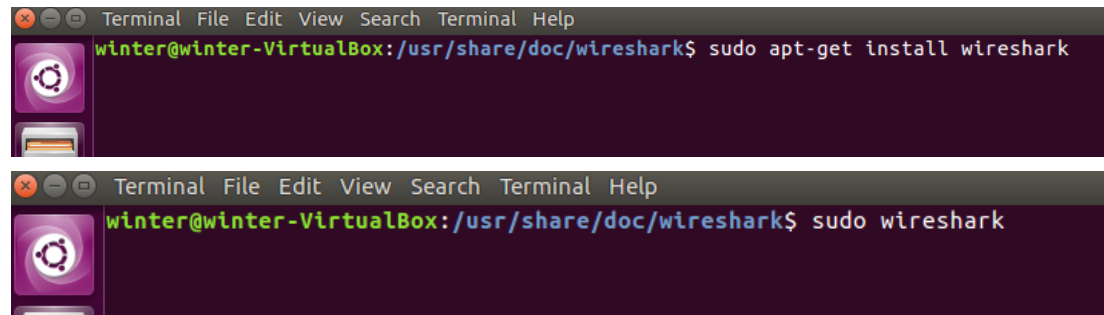
Old Stable Release (3.2.17)

Development Release (3.6.0rc1)

Documentation

安裝Wireshark

- Windows
 - 進入官網下載安裝檔
 - 執行安裝檔之後，一直按下一步即可
 - 中途會要求安裝WinPcap
 - WinPcap是Wireshark擷取封包會用到的Library
- Linux在Ubuntu的terminal輸入:"sudo apt-get install wireshark"
 - 輸入"sudo wireshark"執行Wireshark

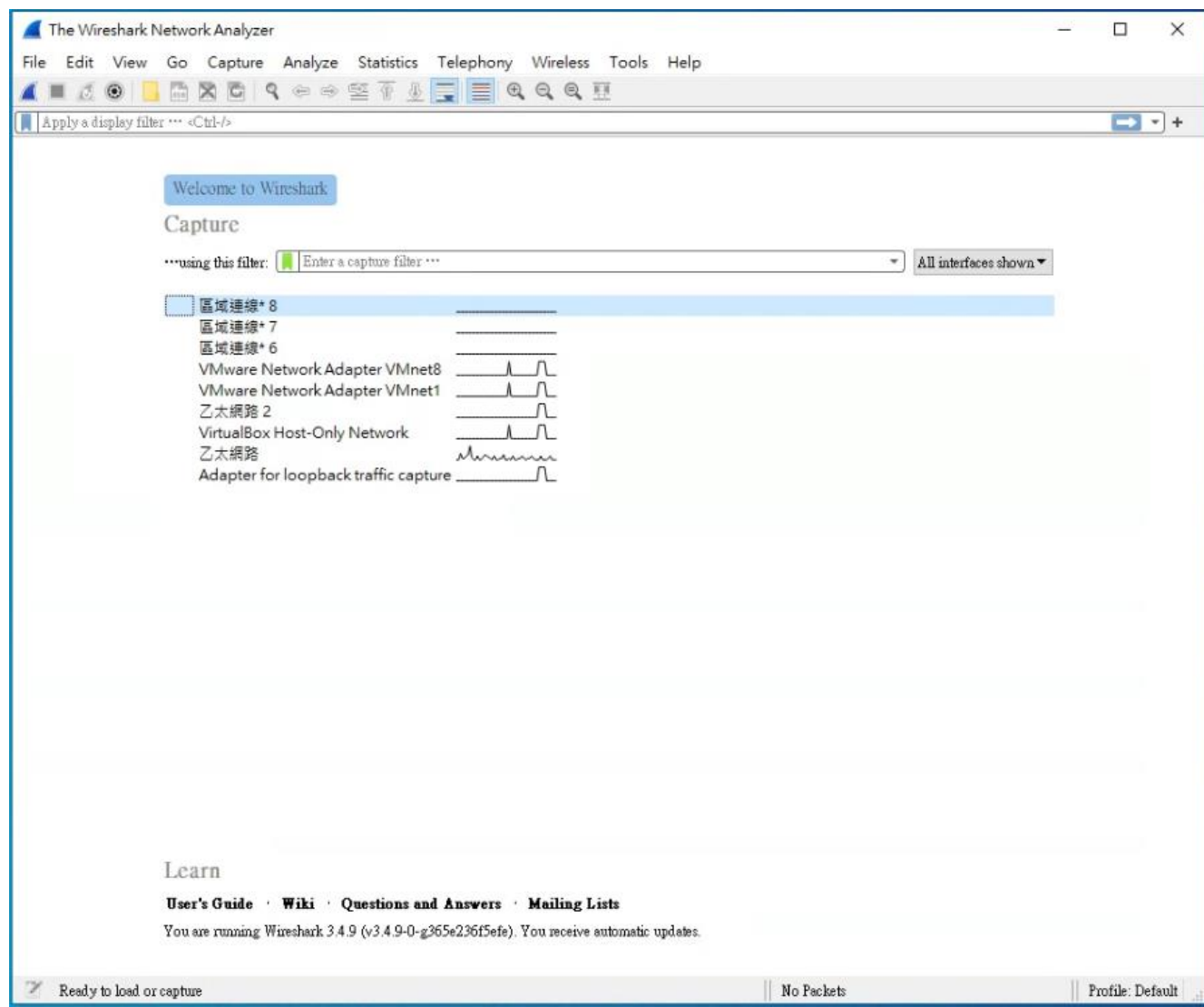


```
Terminal File Edit View Search Terminal Help
winter@winter-VirtualBox:/usr/share/doc/wireshark$ sudo apt-get install wireshark

Terminal File Edit View Search Terminal Help
winter@winter-VirtualBox:/usr/share/doc/wireshark$ sudo wireshark
```

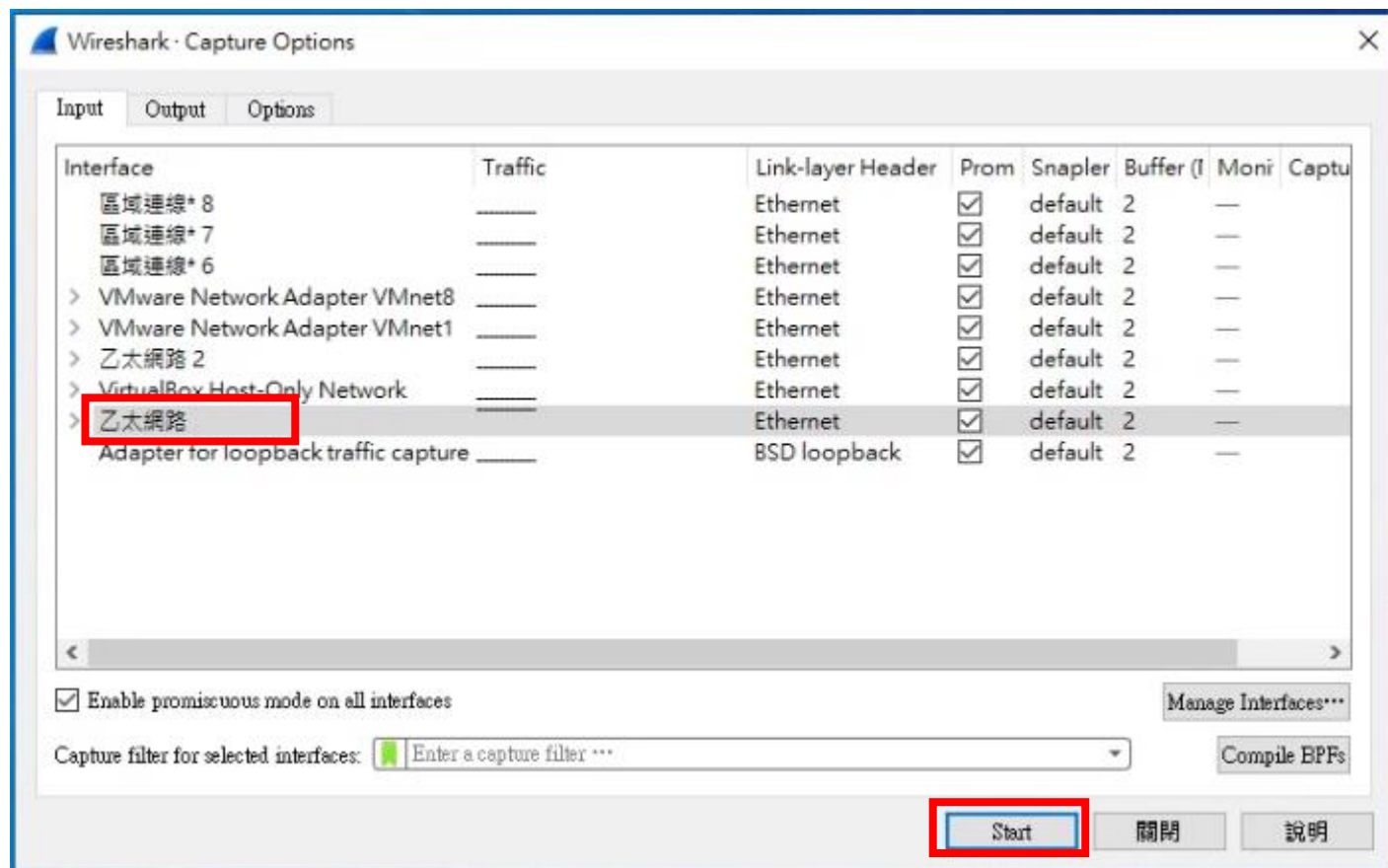
執行Wireshark

- 開啟Wireshark



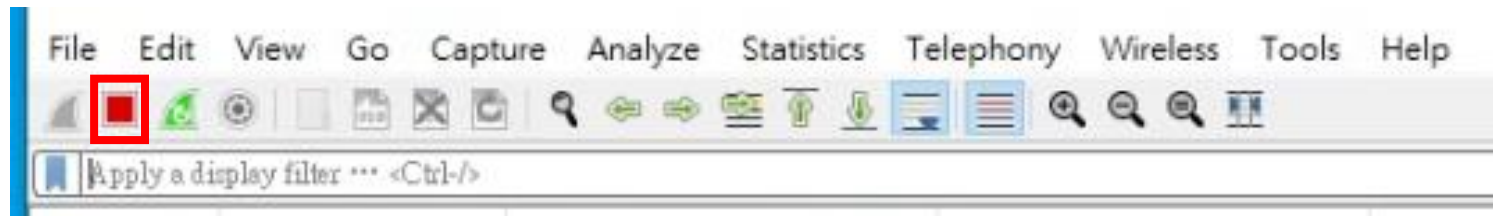
執行Wireshark

- 選擇監聽的interface
- 點選Capture options，會列出電腦中所有的Interface，選擇要進行封包擷取的網路卡，按下Start

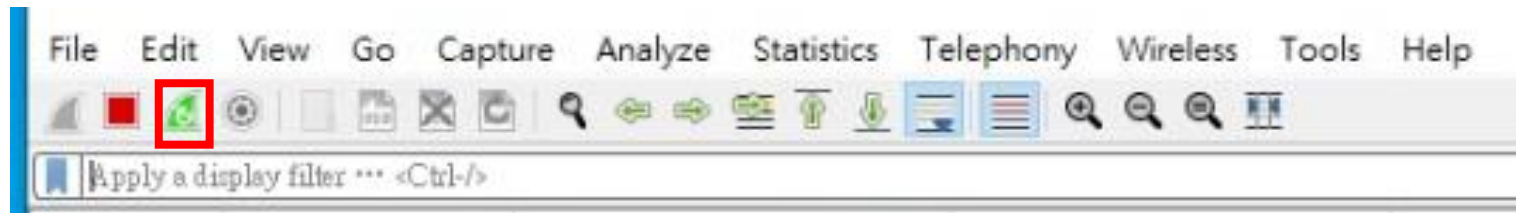


執行Wireshark

- 停止擷取封包
 - 按一下左上角的Stop the running capture

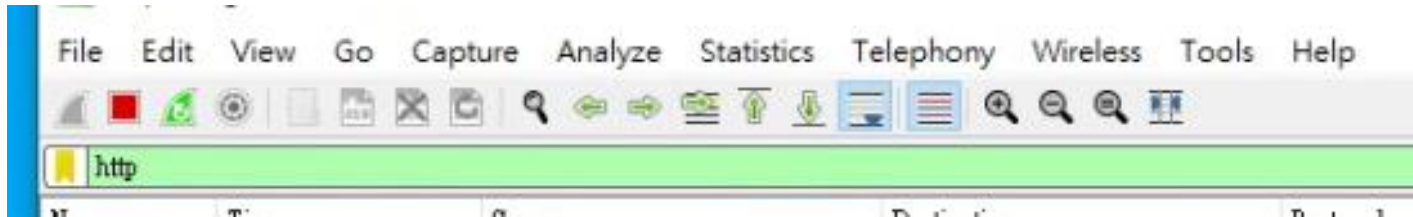


- 重新開始擷取封包
 - 按一下左上角的Restart the running capture

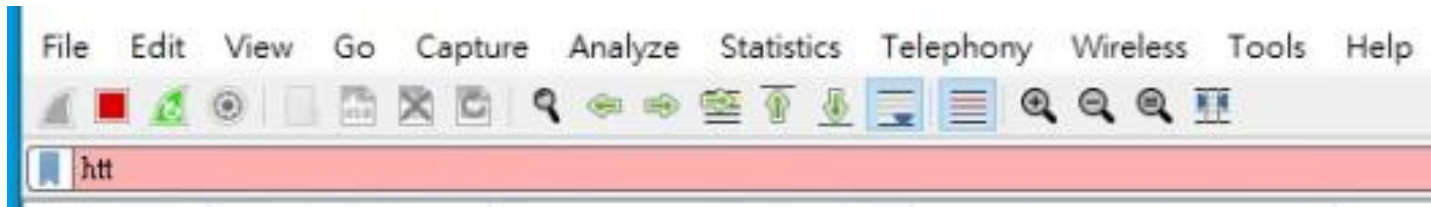


執行Wireshark

- 過濾封包(Filter)
- 在Filter欄位輸入條件後按Enter

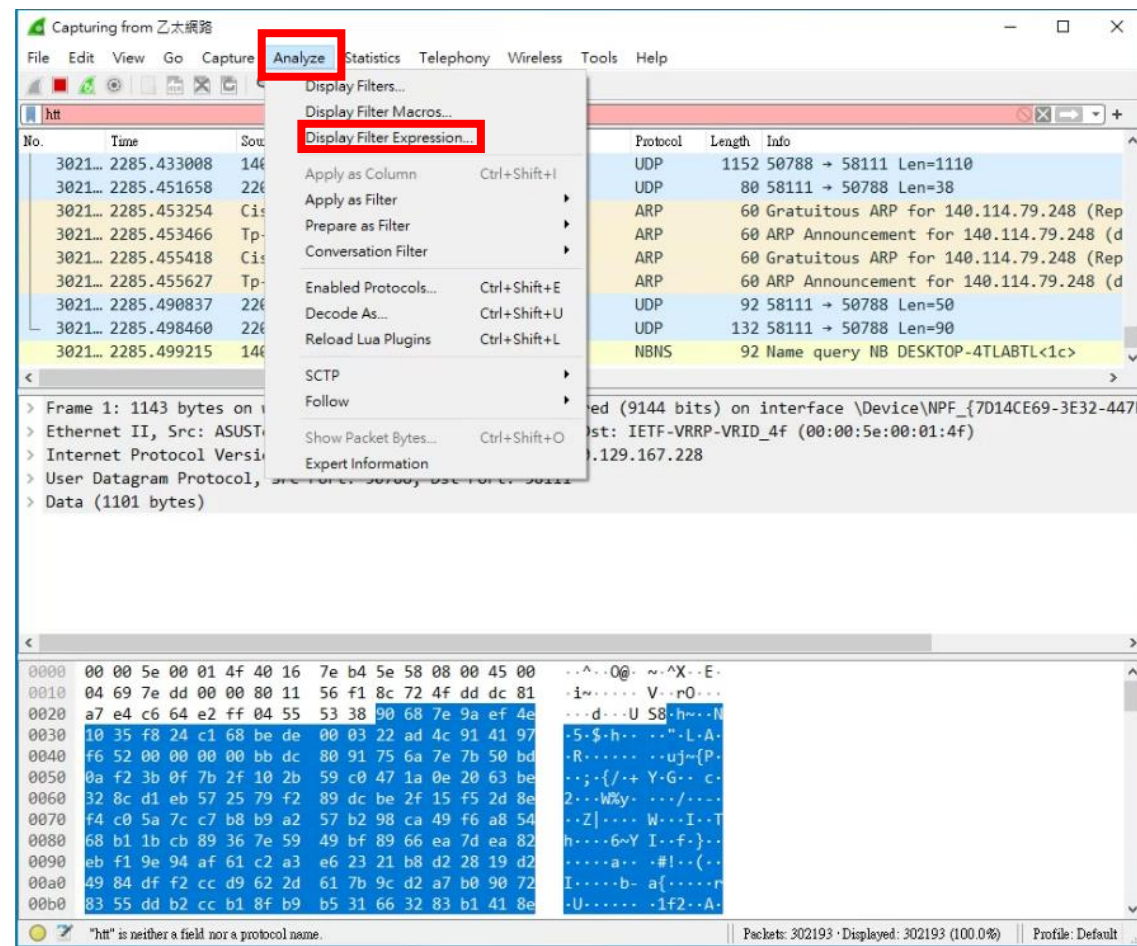


- 條件錯誤就會變成紅色



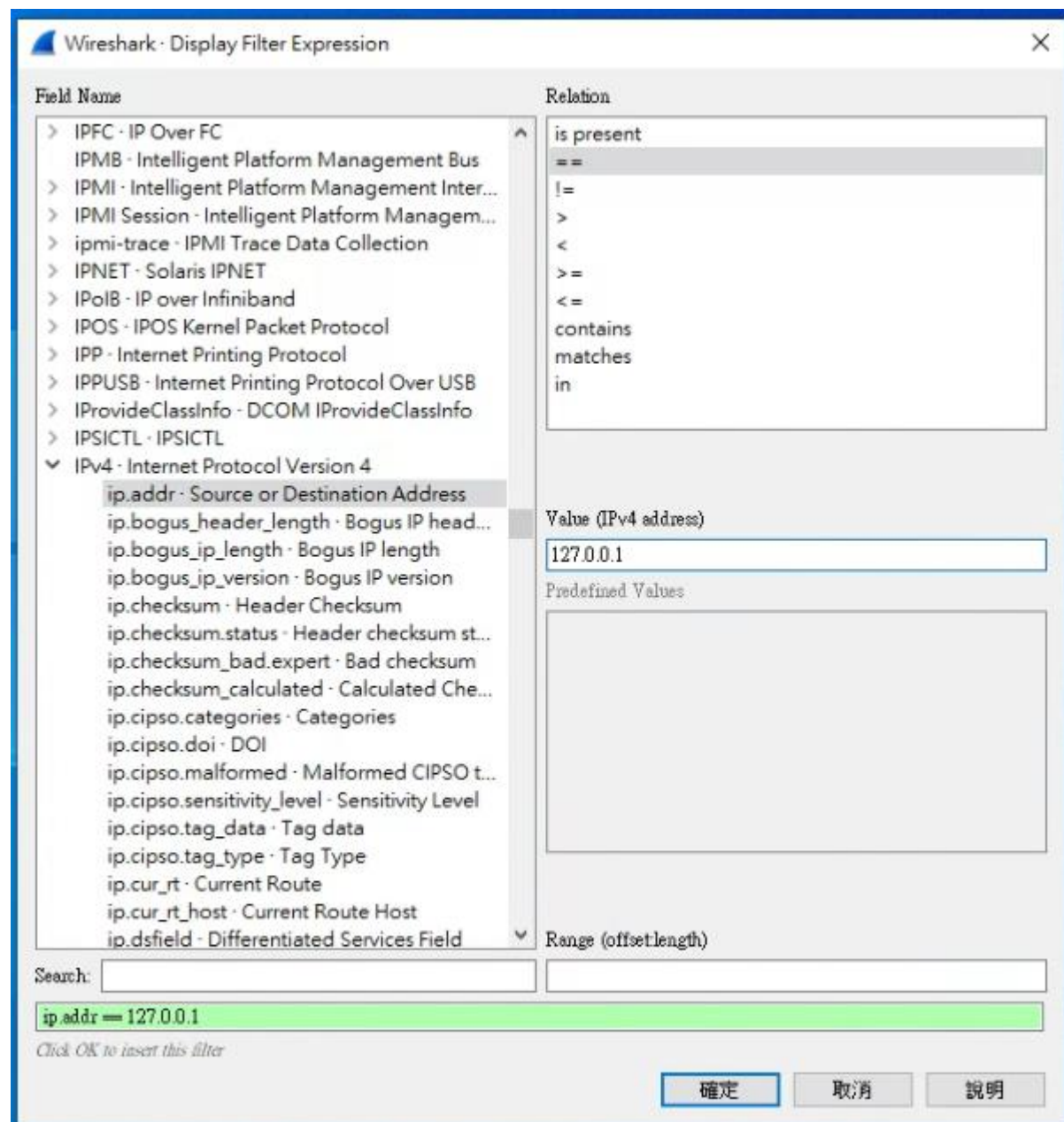
執行Wireshark

- Display Filter Expression
 - 可以看到Filter條件的選單
- Analyze -> Display Filter Expression



執行Wireshark

- Display Filter Expression

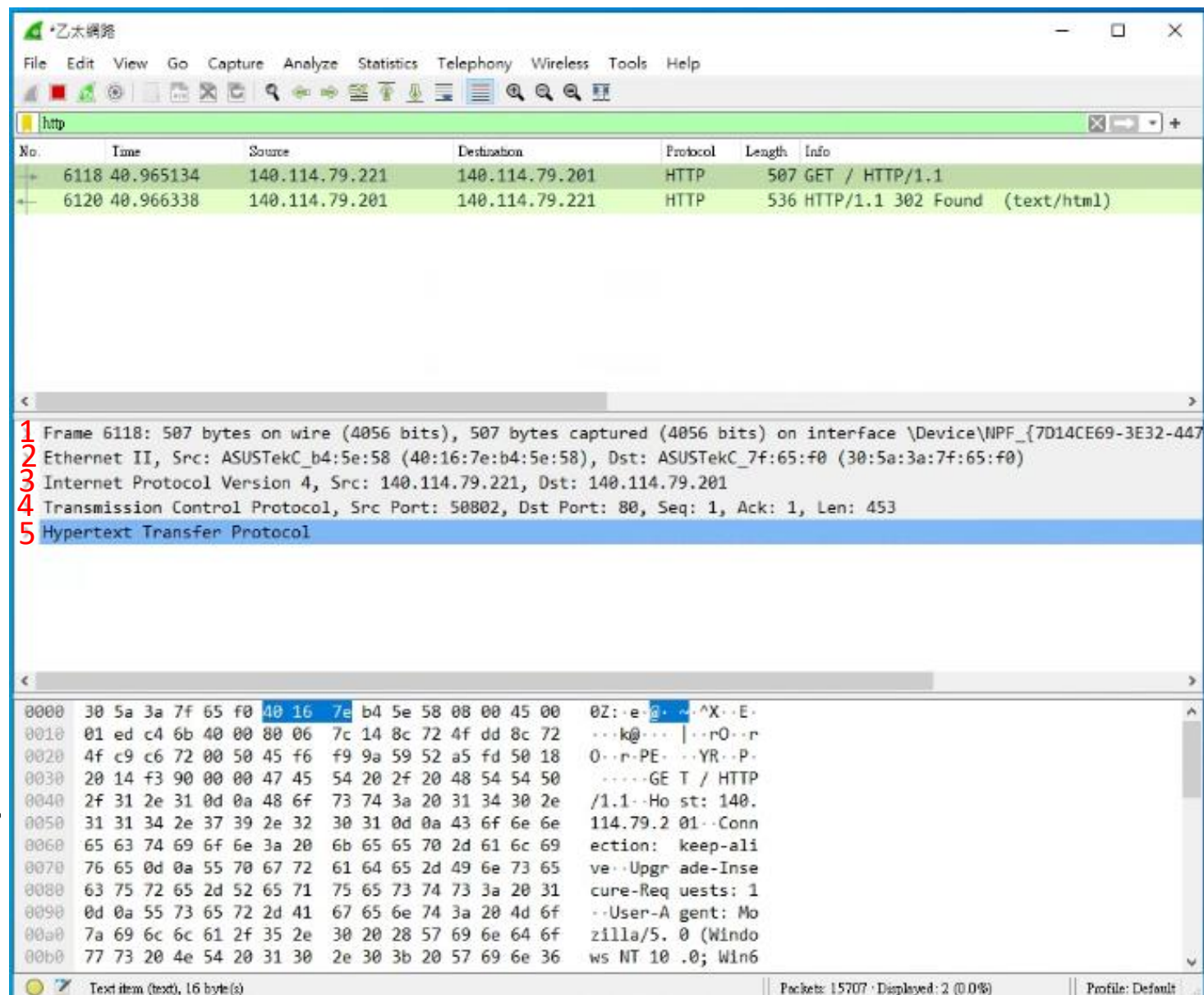


執行Wireshark

- 常用的Filter條件
- http
- ip.addr
 - IPv4 address
- tcp.port
 - TCP port
- 可用“&&”及“||”連接多個條件
 - Ex: tcp.port==80 && ip.addr==127.0.0.1
- 更多Filter條件可以自行嘗試Filter expression或上網查詢

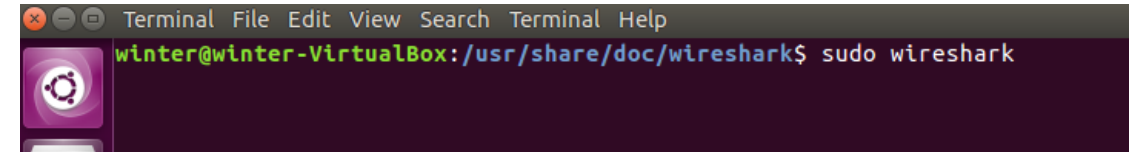
執行Wireshark

- 封包範例
- 1. Frame information
- 2. Data link layer header
 - EX: MAC address
- 3. Network layer header
 - EX: IP address
- 4. Transport layer header
 - EX: port number
- 5. Application layer header
 - EX: HTTP request

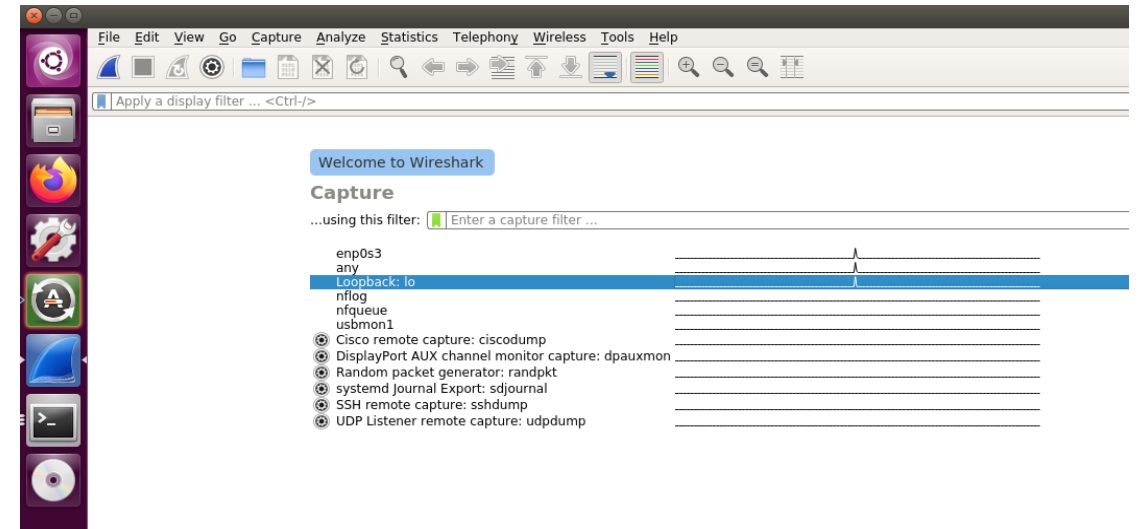


Loopback adaptor

- Localhost
 - 代表本機電腦，常用於內部測試
 - 127.0.0.1
- Linux環境
 - 輸入"sudo wireshark"執行Wireshark
 - 選擇“Loopback: lo”作為監聽的 interface 即可擷取localhost封包



```
Terminal File Edit View Search Terminal Help
winter@winter-VirtualBox: /usr/share/doc/wireshark$ sudo wireshark
```

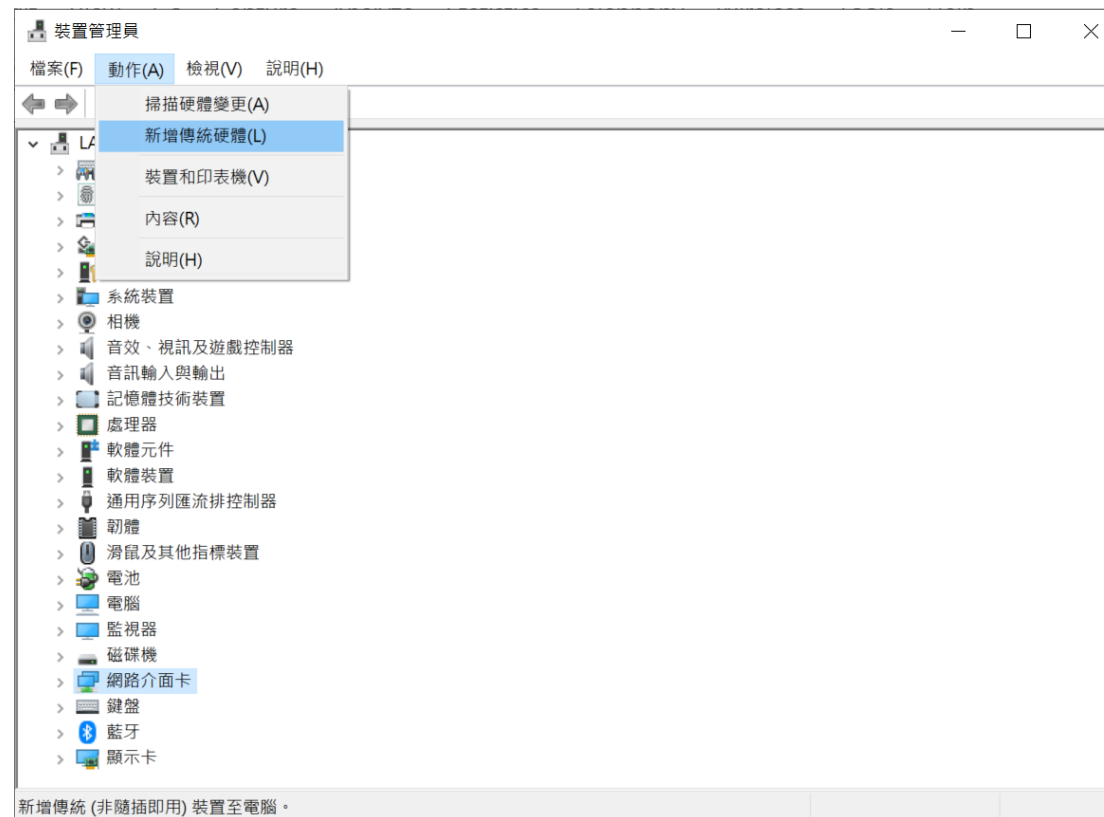


Loopback adaptor

- Localhost
 - 代表本機電腦，常用於內部測試
 - 127.0.0.1
- Windows環境下，Wireshark無法擷取localhost的封包
 - 在Windows環境下，需安裝“Microsoft Loopback Adapter”

安裝Loopback adaptor

- 開啟裝置管理員
- 點選「網路介面卡」
- 點選「動作」->「新增傳統硬體」



安裝Loopback adaptor

- 點選「下一步」



安裝Loopback adaptor

- 點選「安裝我從清單中手動選取的硬體(進階選項)」
- 點選「下一步」

新增硬體

這個精靈協助您安裝其他硬體

精靈可以搜尋其他硬體，並自動為您安裝它。如果您知道要安裝的硬體型號，您也可以從清單中選取。

您要精靈執行什麼工作？

- ☐ 搜尋並自動安裝硬體 (建議選項)(S)
- ☒ 安裝我從清單中手動選取的硬體(進階選項)(M)

< 上一步(B)

下一步(N) >

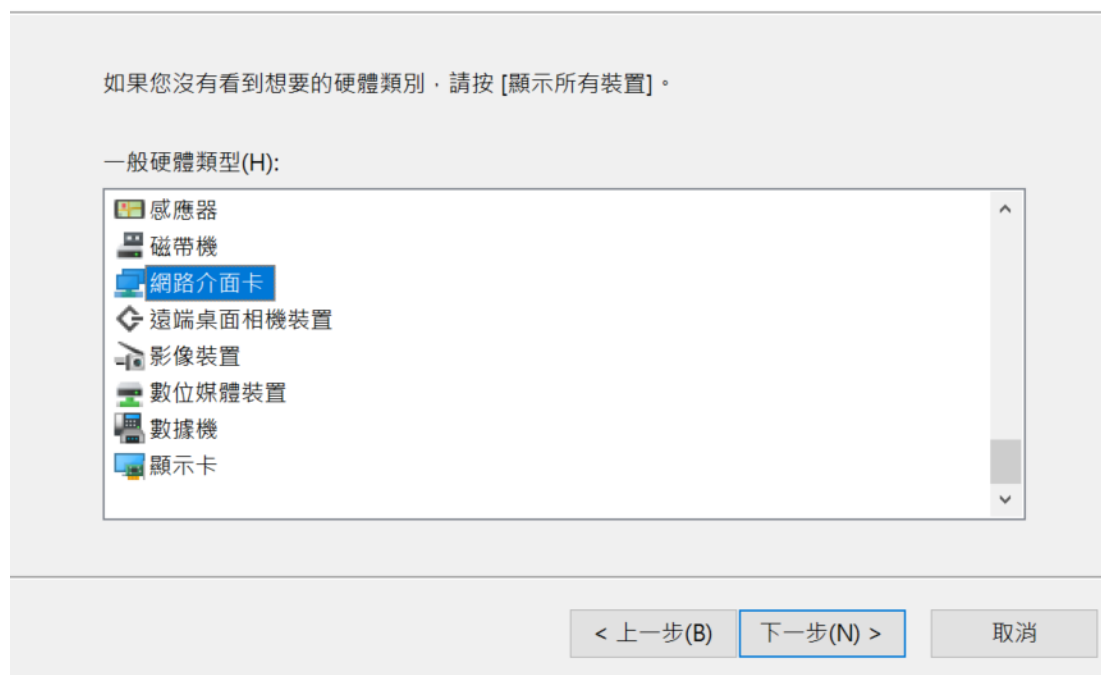
取消

安裝Loopback adaptor

- 點選「網路介面卡」
- 點選「下一步」

新增硬體

從以下清單選取您想要安裝的硬體類型

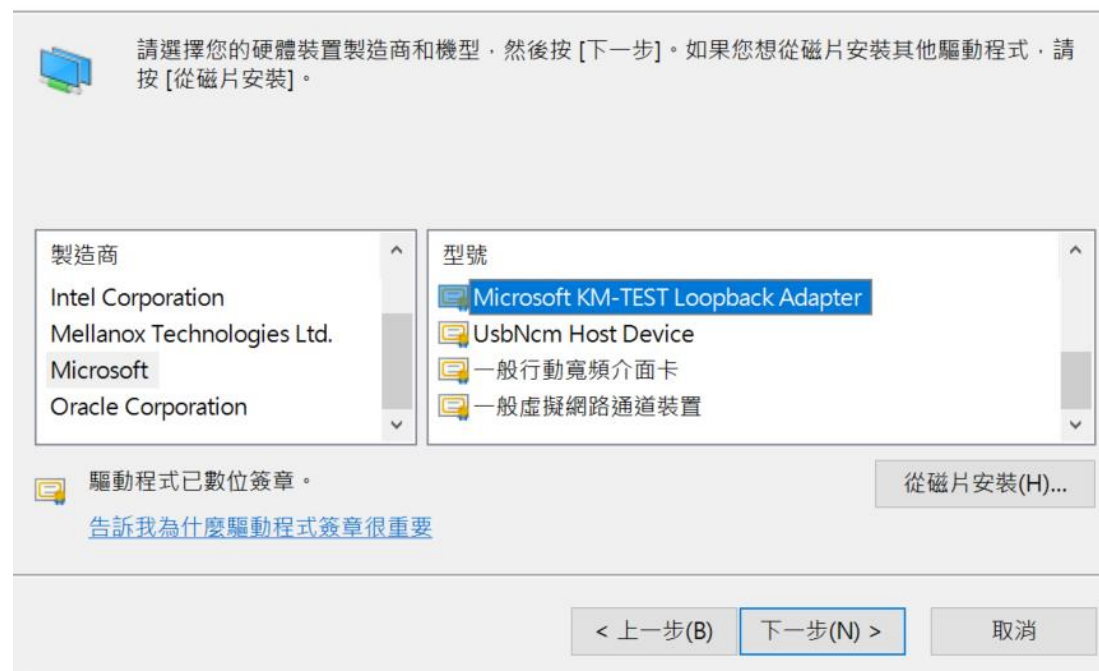


安裝Loopback adaptor

- 點選「Microsoft」
- 點選「Microsoft KM-TEST Loopback Adaptor」
- 點選「下一步」

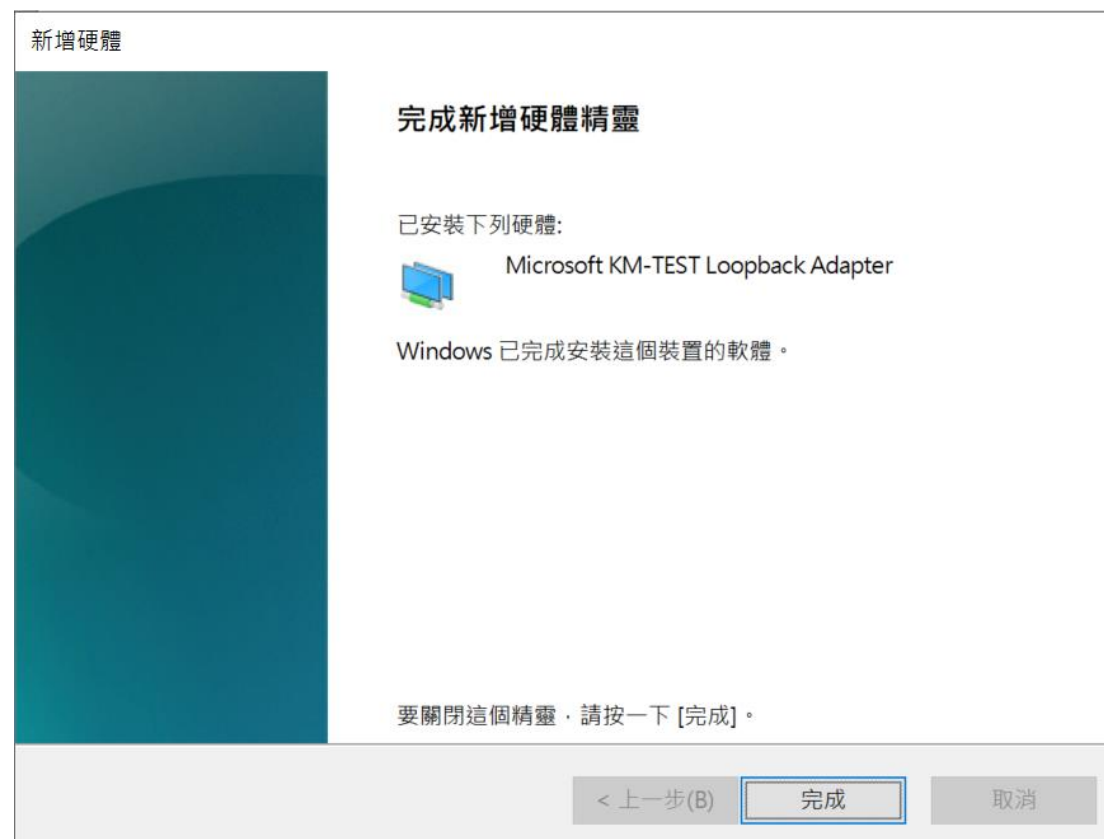
新增硬體

選取您要為這個硬體安裝的裝置驅動程式



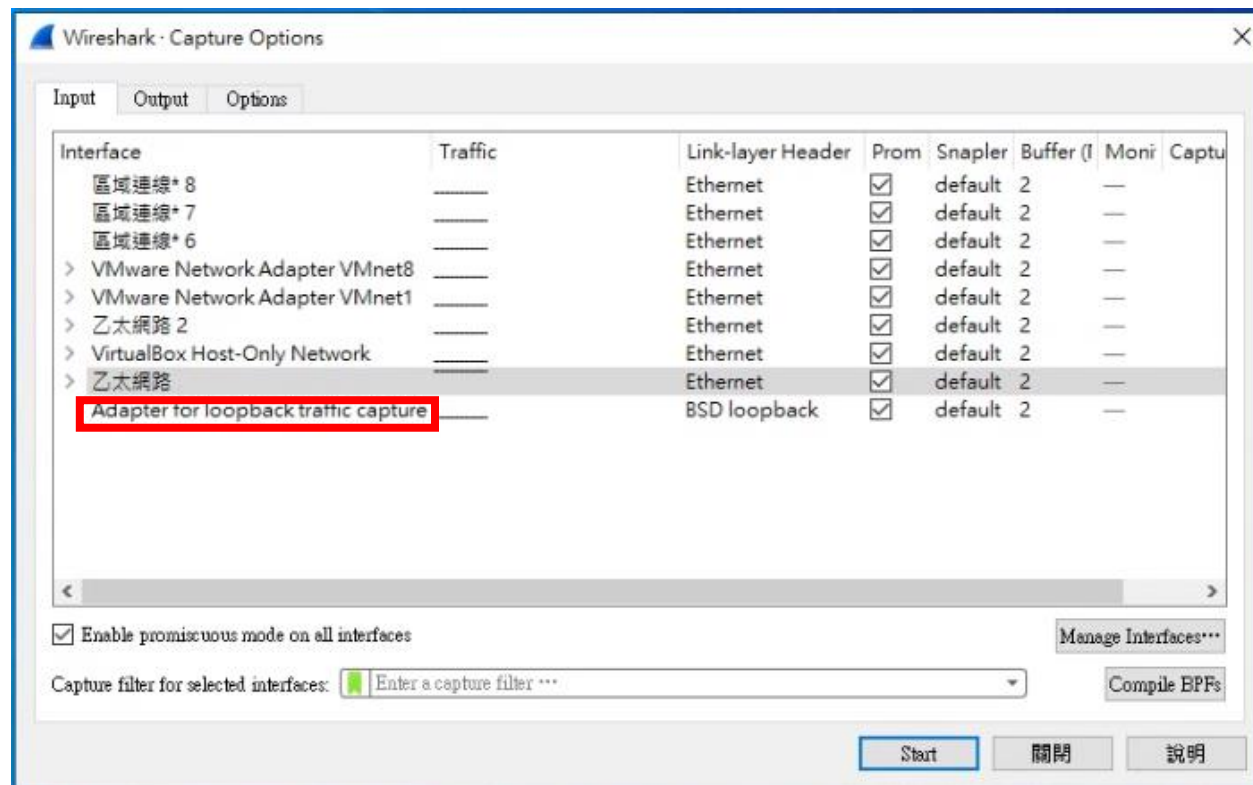
安裝Loopback adaptor

- 點選「完成」



Loopback adaptor

- interface選擇「Adapter for loopback traffic capture」即可擷取localhost的封包



Demo

- 利用Wireshark擷取final project中server及client間的封包

1. TCP handshaking是哪3個封包?
2. server, client的IP address?
3. 從server到client經過了幾個router?
4. server, client的port?
5. 封包data大小?