第一章 實習環境建立

本課程使用 Wireshark 與 Cisco Packet Tracer 等兩只軟套件，來建立實習環境，前者 Wireshark 是在實際環境下，擷取網路封包，並分析其運作程序；後者 Packet Trace 是一套網路模擬環境，它可模擬架設網路系統、模擬封包流動程序、與分析封包訊息。

為了讓讀者有較真實網路的接觸感，我們利用 Wireshark 套件擷取真實網路運作的封包，來分析它的運作程序。但網路系統非常龐大複雜，欲建構一套完整的網路環境以供實習，其費用非常昂貴，並非一般學校或訓練機構可承擔得起，因此，我們利用 Cisco Packet Tracer 來模擬建構網路環境，以供學習或學員實習使用。但讀者放心，Cisco 建立此模擬環境幾乎與實際環境相同，無論硬體更替、IOS 命令操作，幾乎與實際裝置沒有兩樣。

從另一方面而言，目前各家製造商的網路設備，其操作模式幾乎和 Cisco 公司產品相同，如果讀者利用 Packet Tracer 學會了網路架設與管理，在實際環境下遇到各家廠商的產品，幾乎可以應用自如，完成不會侷限於 Cisco 公司產品。

1-1 Cisco Packet Tracer 套件

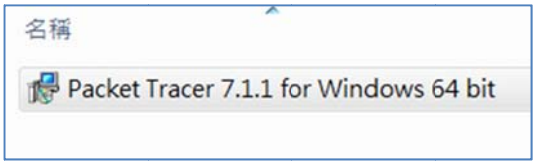
Packet Tracer 是 Cisco 公司發行的免費軟體，可執行於 Windows 或 Linux 系統上。它是供客戶模擬學習網路架設的技巧。在 Packet Tracer 上使用者可以圖形規劃網路架構，包含所有 Cisco 出產的所有網路產品，譬如 HUB、Switch、Router、Server、等等，還包含多種網路傳輸媒介，譬如光纖、Cat 5UTP、無線電波、藍芽、等等。將網路連線完成之後，還可利用 IOS 命令規劃其運作程序。當網路規劃完成之後，吾人還可選用 Simulation Mode 運作，以動畫方式觀察封包在網路流動的狀態，從中可以觀察所架構的網路有何缺陷，並尋找最佳規劃模式。

近幾年來，Packet Tracer 已成為學習網路規劃的最佳工具，又 Cisco 舉辦各種 CCNA 系列認證考試都使用此系統，無形之中，它也成為通過 CCNA 考試的必要工具。

1-1-1 Packet Tracer 下載與安裝

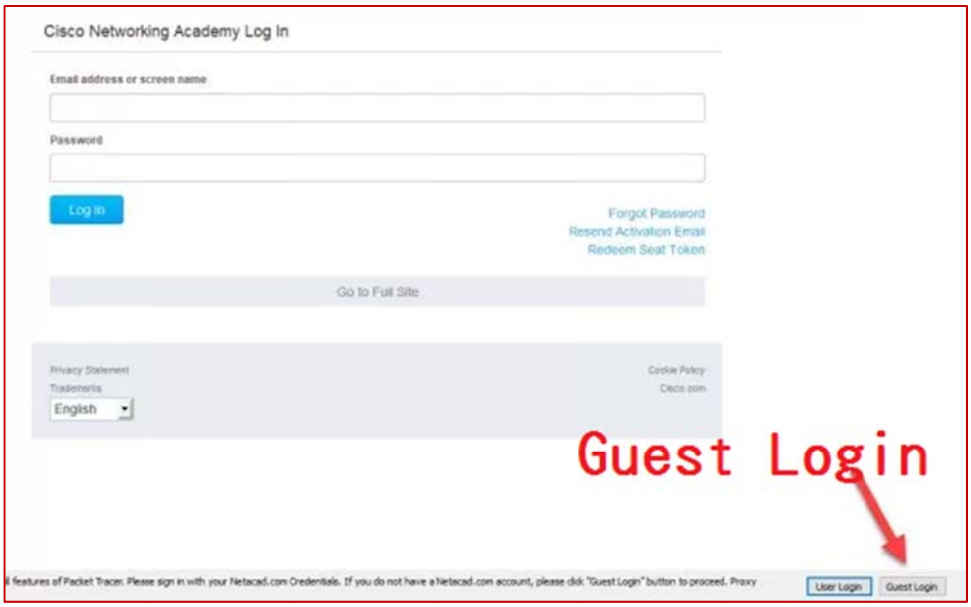
(A) Cisco 官方網站

下載後執行安裝。



(B) 登入帳號(Guest Login)

如願意建立帳號則輸入相關資料(沒有甚麼關係)，它會提供許多網路的學習管道，譬如，本人在 Cisco 網路大學上學到許多重要知識。如果不願意，則選擇『**Guest Login**』，也可以直接進入操作。

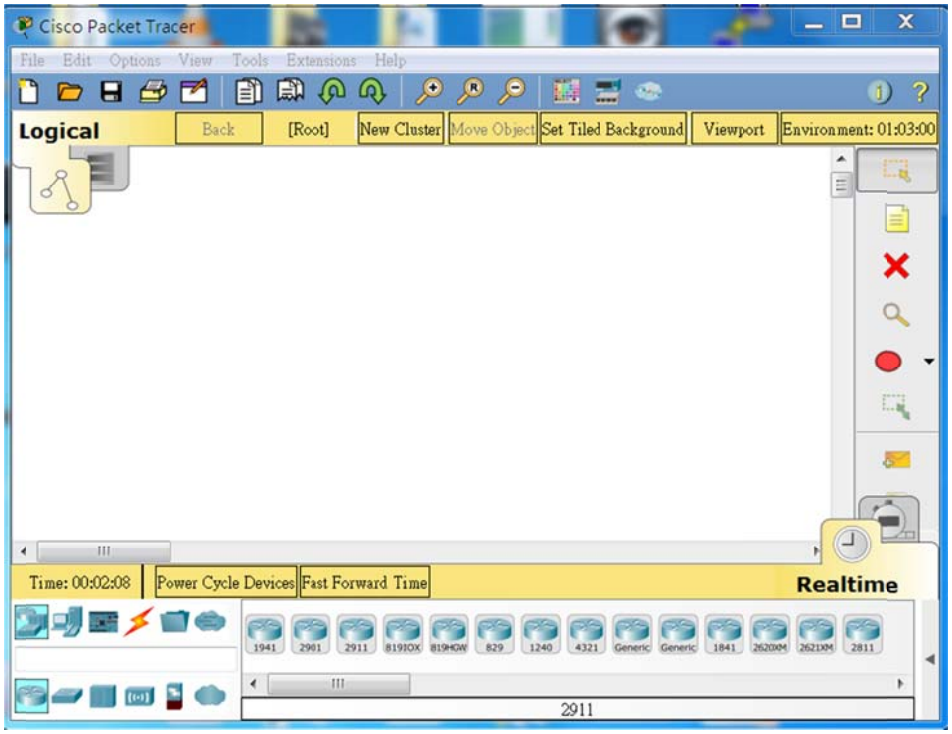


1-1-2 Packet tracer 操作說明

(A) 系統介面

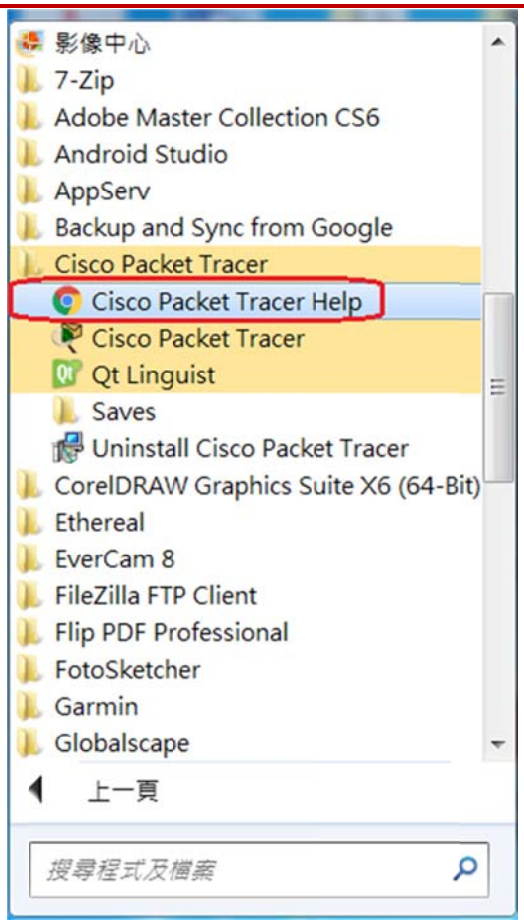
點選後，系統進入視窗如下：

進入後，立即產生 Packet Tracer 的工作平台。



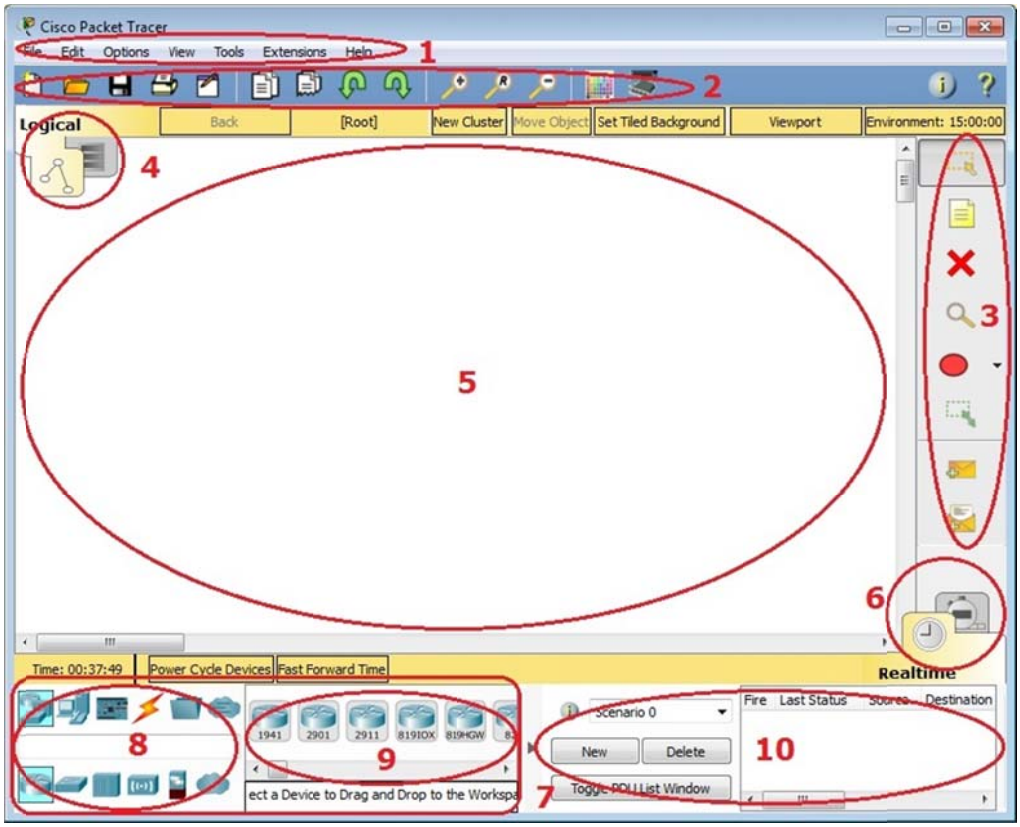
(B) 使用手冊

Cisco 內建有使用手冊，操作之前請先瀏覽一下，非常有幫助，由 Windows 7 開始按鈕進入，如下：



(C) 面板功能

下圖是 Cisco Packet Tracer 的操作視窗，共有 10 個功能區，說明如下：



(1) 功能表選單(Menu Bar)

(2) 主工具選單(Main Tool Bar)

(3) 命令工具選單(Command Tools Bar)：有刪除、註解、發送發包、、等功能。

(4) 邏輯/實體工具區與瀏覽選單(Logical/Physical Workspace and Navigation Bar)。

(5) 工作區(Workspace)：繪製網路架構圖。

(6) 即時/模擬選單(Realtime/Simulation Bar)：封包立即傳送或慢動作動畫傳送。

(7) 網路元件箱(Network Component Box)。

(8) 裝置型態選擇箱(Device-Type Selection)：有交換器、路由器、連線、、、等等。

(9) 裝置規格選擇箱(Device-Specific Selection Box)：選擇裝置(如交換器)後，立即顯示該裝置有哪些交換器可供選擇。

(10) 使用者產生封包：可供使用者自行設計封包。

1-1-3 預備事項

利用 Cisco Packet Tracer 練習規劃網路非常方便，尤其針對 CCNA 考試方面更能得心應手，但使用之前還須注意一下，下列事項：

(1) 僅 Cisco 產品可以加入規劃。

(2) 許多裝置允許 add-in 選擇插入多種網路模組，尤其是路由器，對於這些模組的功能需弄清楚。

(3) 需要熟練 IOS 的基本操作命令。

(4) 網路圖粗稿先畫出來，尤其是 IP 位址的配置。

1-2 Wireshark 網路封包分析器

Wireshark(以前稱 Ethereal) 是一個免費的網路封包分析軟體，他僅由網路上擷取封包，

並不會對網路發生任何影響。它不是入侵偵測軟體，網路發生異常現象，也不會發出警告訊息。我們僅能利用它擷取封包，再來分析網路狀況，能提供下列協助：

- 檢測網路問題、
- 檢查網路安全相關問題、
- 開發者對新的協定偵錯、
- 學習網路協定相關知識(此為我們主要目地)。

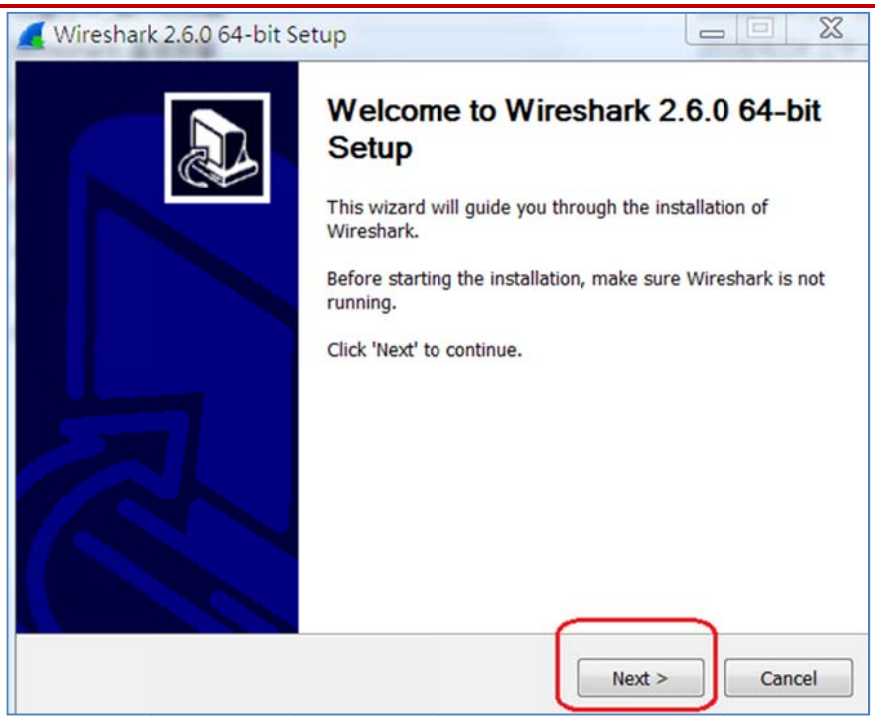
1-2-1 下載 Wireshark 套件

(A) 搜尋官方網站

在 Google 上搜尋 Wireshark 即可，如下：(選擇 Windows Installer(64bit)

(B) 安裝步驟

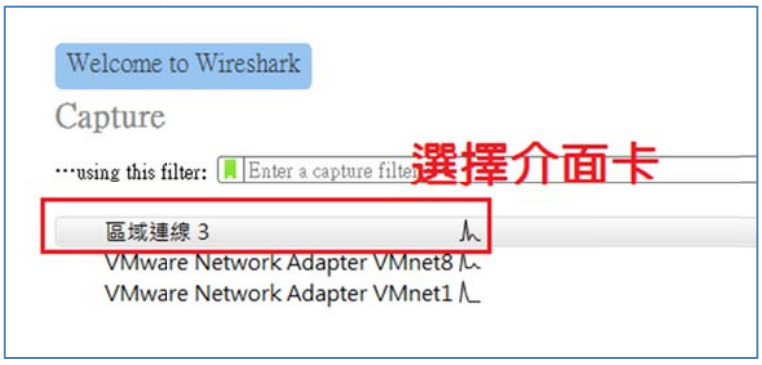
(只要繼續按下一步即可)



1-2-2 操作視窗說明

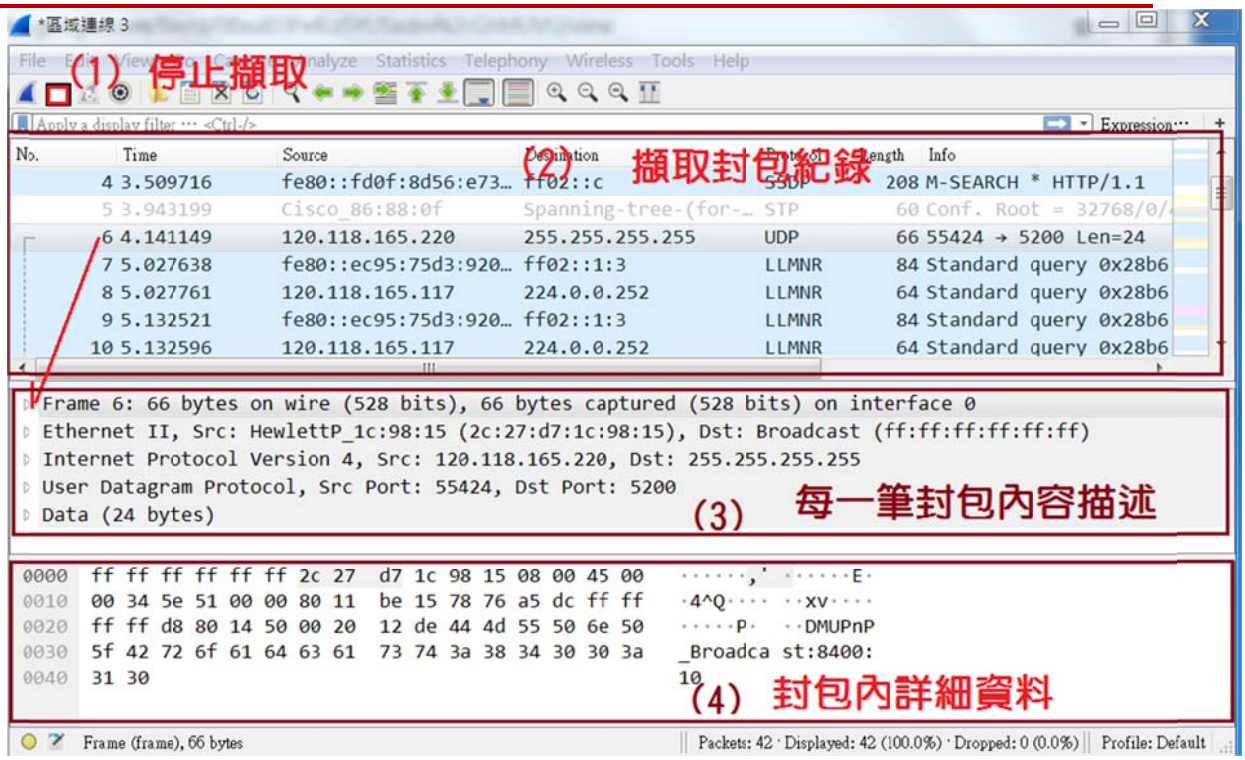
(A) 選擇介面卡：

進入後選擇由哪一個介面卡擷取封包。一般如安裝在 Windows 7/10 主機上，則只有主機上的網路架面卡。



(B) 擷取封包：

點選介面卡之後，立即開始擷取封包，須按“暫停”才會暫停擷取。於擷取視窗 (2) 是擷取到的每一個 IP 封包，可點選某一個封包，則在視窗 (3) 出現該封包的分析資料，而封包內的詳細資料如視窗 (4) 所示，畫面如下：



擷取封包紀錄視窗中有五個欄位，說明如下：

(1) No 欄位：擷取封包數。

(2) Time 欄位：封包擷取時間，預設值由 0 開始計時。

(3) Source 欄位：封包傳送的來源位址。

(4) Destination 欄位：封包傳送的目地位址。

(5) Length 欄位：封包的長度(Bytes)。

(6) Info 欄位：有關封包的訊息，譬如 TCP、UDP 封包標頭的訊息。

點選封包紀錄中某一筆資料，則在下一個視窗顯示該筆封包的展開內容。譬如點選一筆 UDP 紀錄，則依序由 Ethernet II、IPv4、UDP 顯示其標頭內容，最後再顯示 UDP 所承載的資料。

1-2-3 封包擷取操作

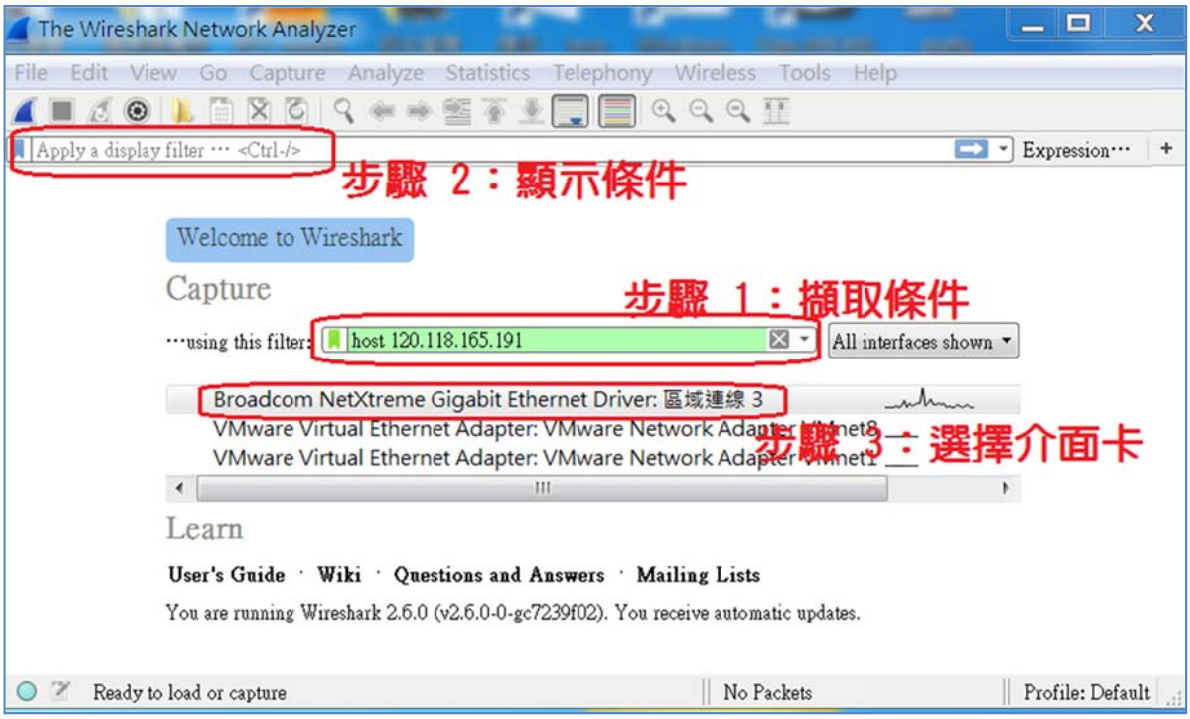
擷取封包必須注意事項如下：

- 選取介面卡：在操作電腦上也許會有多片實體網路卡，或經過虛擬機(如 VMware Player) 產生的介面卡，需選擇由哪一個介面卡擷取封包。

- 擷取篩選條件：如沒有設定擷取條件的話，封包數量將會非常多，很難找到所欲觀察的封包。即是，符合條件的封包材擷取，譬如僅擷取某一只 IP 位址發送或接收的封包。

- 顯示篩選條件：雖然經過擷取篩選後，所產生的封包也許還是很多，則可設定顯示篩選條件，譬如，僅顯示 TCP 封包。

擷取步驟如下圖所示，分別說明之：

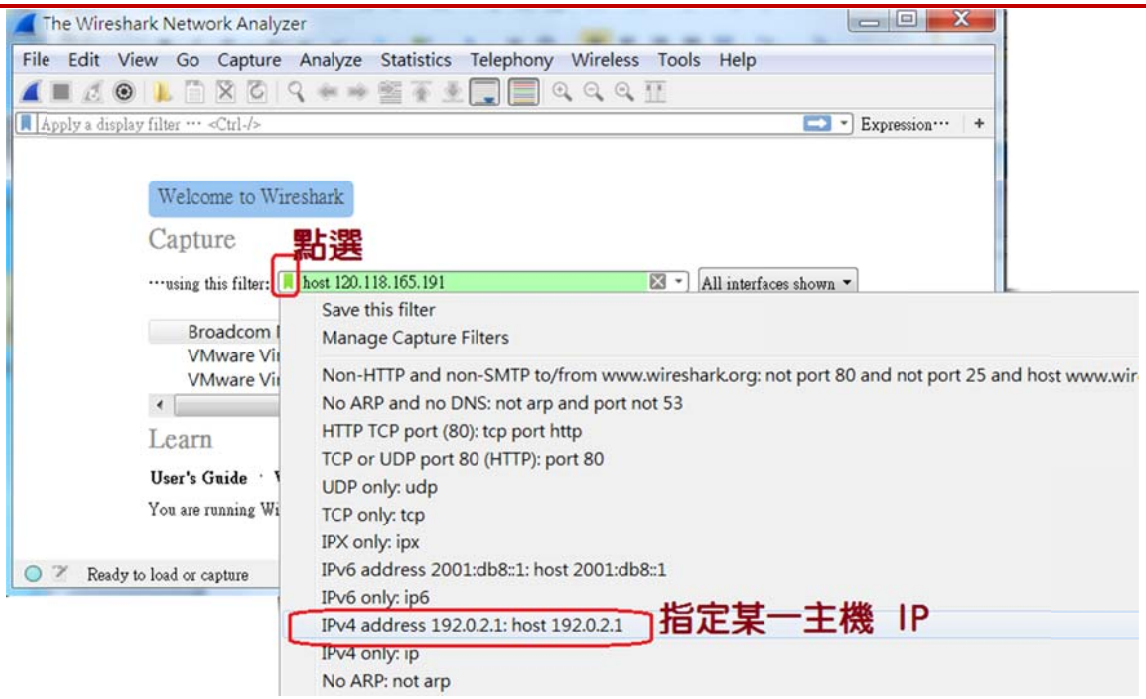


(1) 設定『擷取篩選條件』

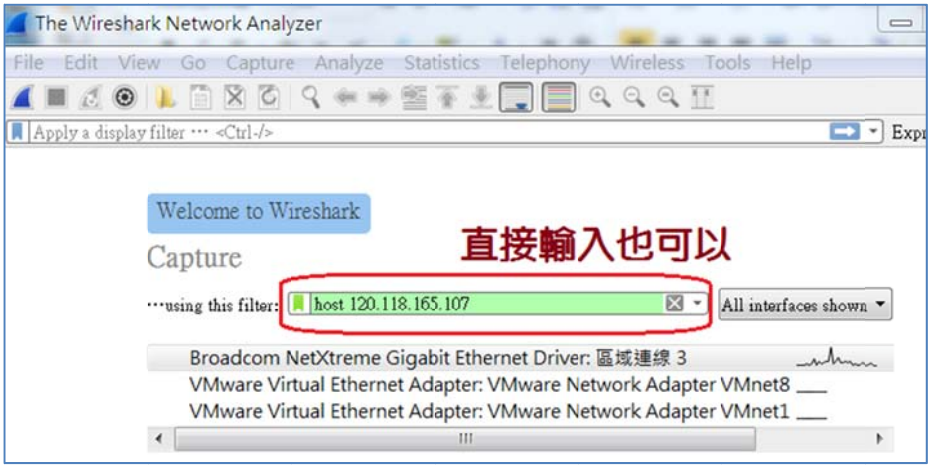
- 點選擷取條件鍵，則出現各種條件顯則、

- 選擇某一擷取條件，譬如 ip 位址、

- 再輸入相關資訊，譬如 120.118.165.107 之 ip 位址。

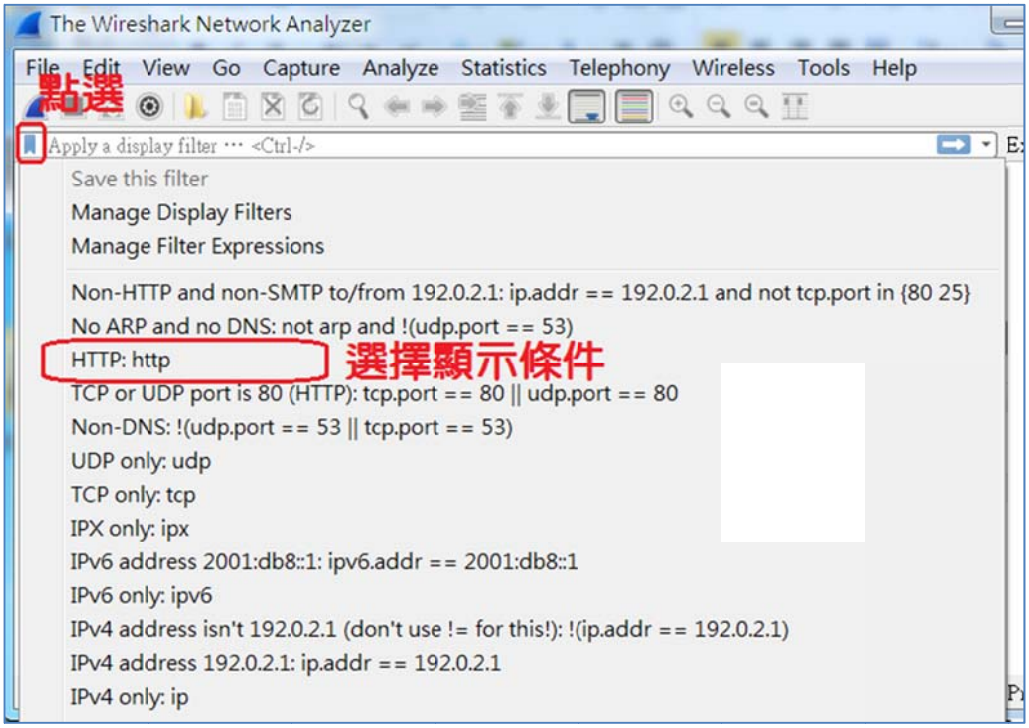


再輸入 IP 位址，如下：



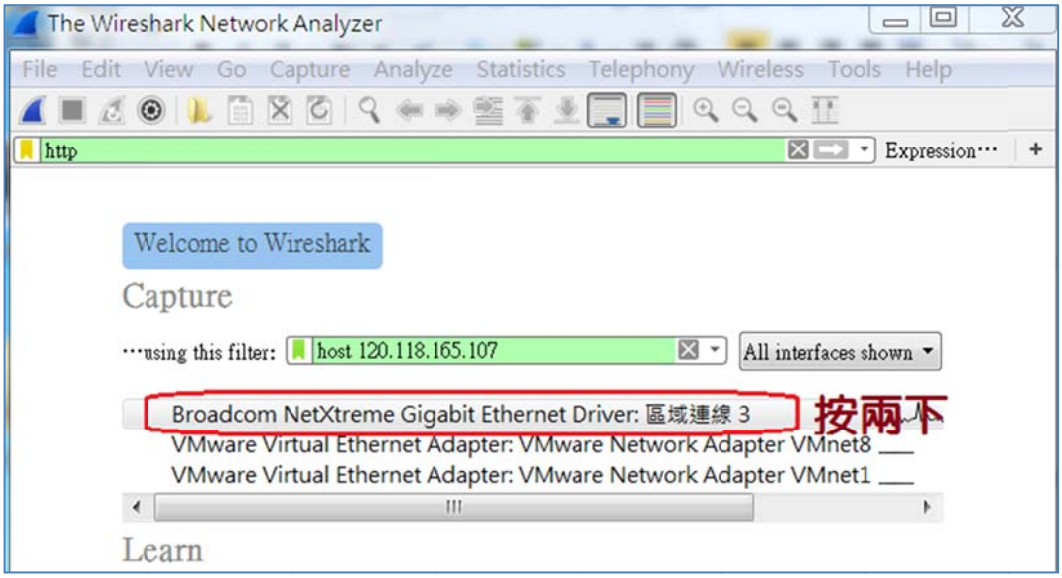
(2) 設定顯示篩選

由左上角點選『顯示篩選條件』按鈕，再選擇顯示條件，如下圖所示。

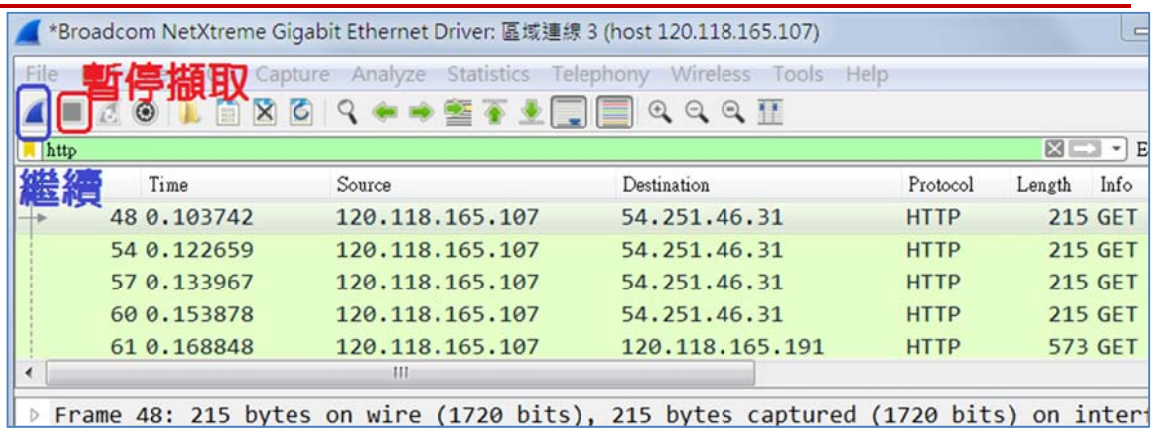


(3) 選擇介面卡

最後點選欲由哪一片網路卡擷取封包，如下：

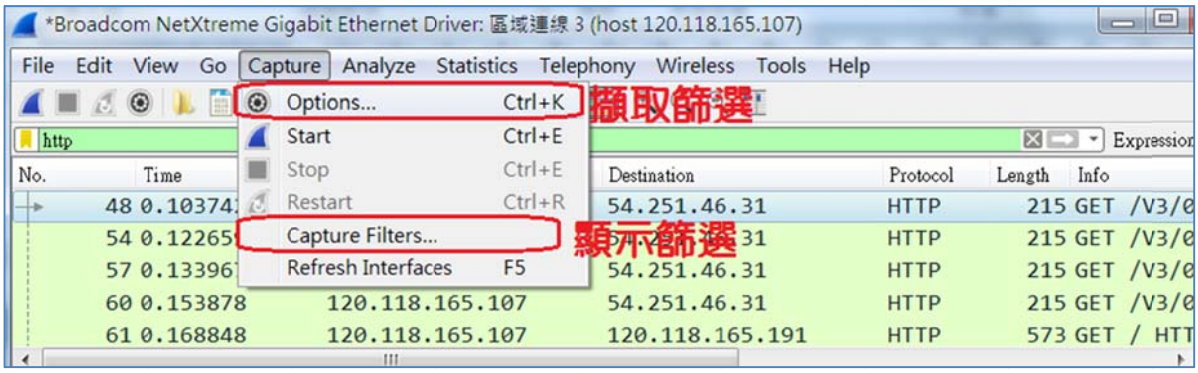


(4) 暫停/繼續擷取



(5) 下拉式選單操作

當然也可以由下拉式選單操作，如下：(請自行操作練習)



1-2-4 封包篩選條件組合

(1) 篩選條件運算子

篩選條件運算子如下：

關係	運算子	範例
等於	Eq、==	ip.proto == 1
不等於	Ne、!=	Ip.proto != 1
大於	Gt、>	Frame.pkt_len > 100
小於	Lt、<	Frame.pkt_len < 100

(2) 常用過濾範例

常用過濾範例如下：

類型		說明	範例
eth	dst	目的 MAC	Eth.dst == ff:ff:ff:ff:ff:ff
	src	來源 MAC	Eth.src == 01:34:45:56:a2:c2
	addr	MAC 位址	Eth.addr == 01:34:45:56:a2:c2
	type	下一層協定	Eth.type == 0x0800 (IP) Eth.type == 0x0806 (ARP)
ip	dst	目的 IP	Ip.dst == 192.168.10.3
	src	來源 IP	Ip.src == 192.168.10.4
	addr	IP 位址	Ip.addr == 192.168.10.5
	proto	下一層協定	Ip.proto == 0x06 (TCP) Ip.proto == 0x01 (ICMP) Ip.proto == 0x11 (UDP)
tcp	dstport	目的 Port	Tcp.dstport == 80 (HTTP)
	srcport	來源 Port	Tcp.srcport == 21 (FTP)
	port	埠口編號	Tcp.port == 23 (telnet)
udp	dstport	目的 Port	Udp.dstport == 53 (DNS)
	srcport	來源 Port	Udp.srcport == 53
	port	埠口編號	Udp.port == 53

(3) 篩選條件的邏輯運算子

篩選條件運算子如下：

邏輯	運算子	範例
AND	and	ip.proto == 1 and ip.dst == 192.168.10.2
	&&	ip.proto == 1 && ip.dst == 192.168.10.2
OR	or	ip.proto == 1 or ip.dst == 192.168.10.2
	||	ip.proto == 1 || ip.dst == 192.168.10.2
NOT	not	not(ip.proto == 1)
	!	!(ip.proto == 1)