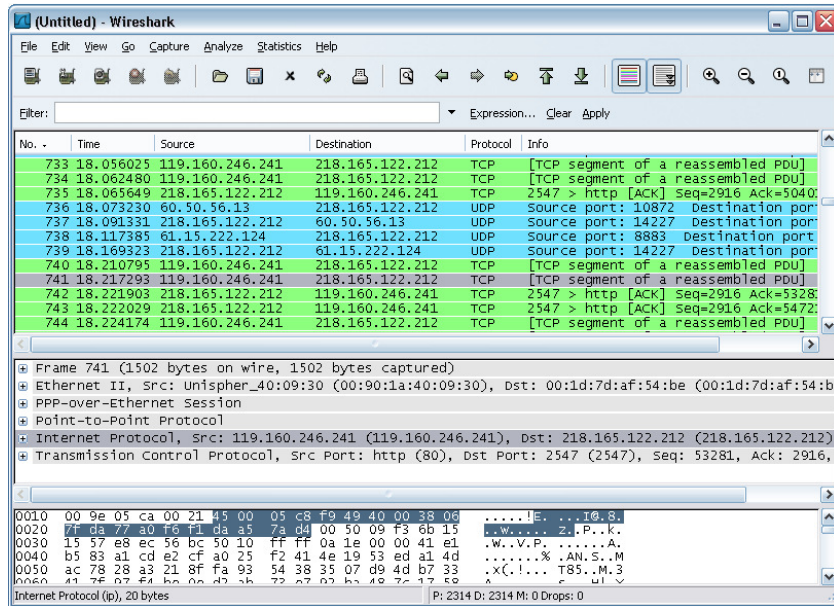


## 封包擷取與分析 - Wireshark



### 一、作業環境


(一) 安裝完成的執行作業視窗如左圖所示，在第一次執行時，由於沒有擷取的封包，畫面中間的內容是空白的

(二) 對於 Wireshark 宗握環境的說明，畫面除了上方下拉式功能表與下方的過濾器(Filter)之外，主要分為大致有「封包列表」、「協定說明」與「16 進位編碼說明」三個，在此分別說明如下：

#### 1. 「封包列表」欄位

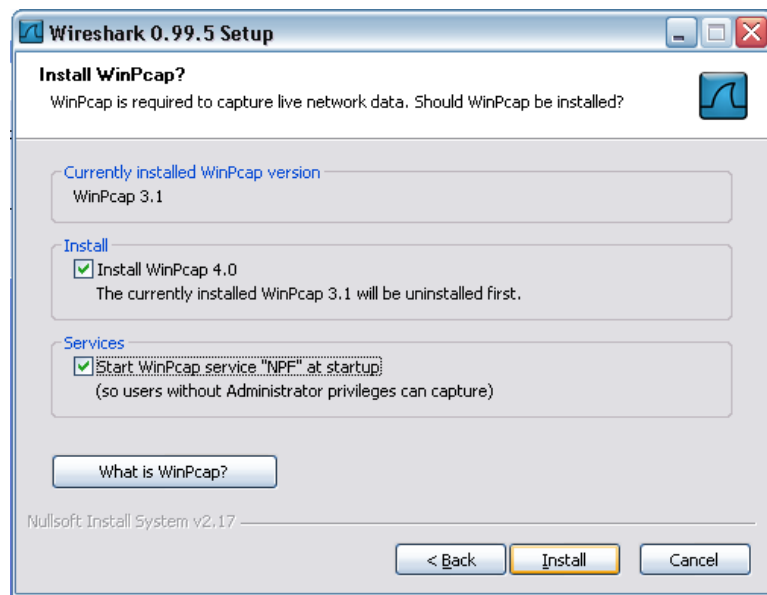
「封包列表」欄位在視窗上方的部分，列出目前所擷取到的封包，並對封包內容做簡要的說明。選取的封包項目會在下面「協定說明」與「16 進位編碼說明」部分進行顯示。

#### 2. 「協定說明」欄位

「協定說明」欄位在中間的部分，說明鎖店選方包嫌隙的協定內容，協定前若有  圖示，表示協定內容還可以再細分，以樹狀方式進一步對該協定內容進行顯示。

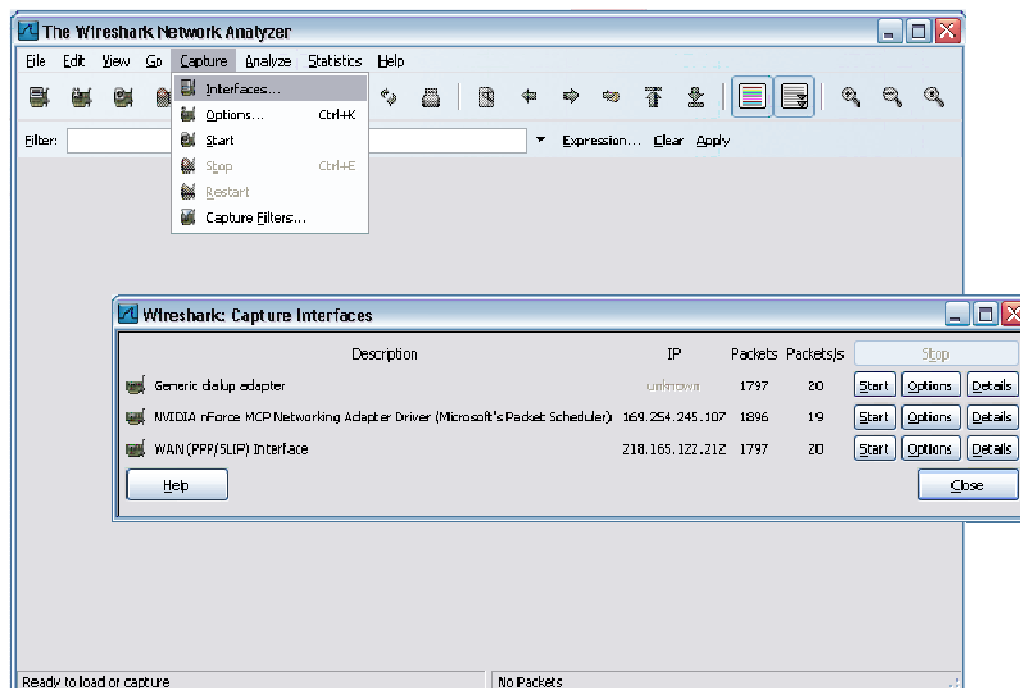
#### 3. 「16 進位編碼說明」欄位

「16 進位編碼說明」欄位在視窗下方的部分，將點選的封包內容以 16 進位方式呈現出來，右側則說明兩個 16 進位值(8 位元)的 ASCII 編碼結果。



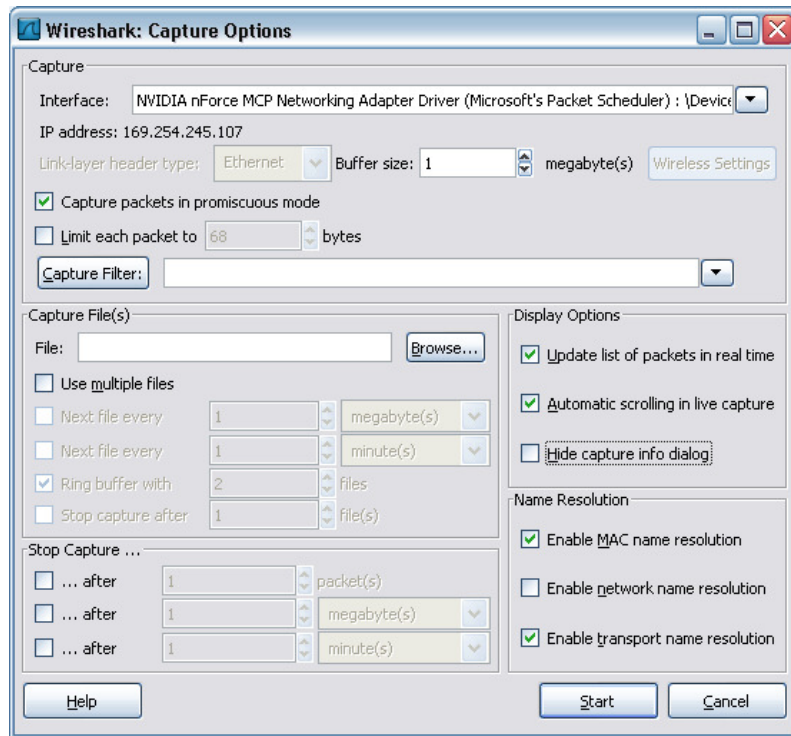
## 二、軟體安裝

執行 Wireshark 可以讀取既有以抓取的方包資料檔案，但如果要直接在網路上擷取封包，必須呼叫 WinPcap 再交由 Wireshark 進行分析；所以安裝 Wireshark 時，必須如左圖所示，選擇安裝 WinPcap 程式，並且勾選「Install」與「Start」選項，以便可以進行安裝與取得擷取封包的權限服務，否則進行封包擷取時會出現錯誤訊息



## 三、封包的擷取與分析

(一) 安裝完軟體，一開始中間的執行畫面會是空白的，要對網路上的封包進行截取分析必須如左圖所示，點選功能列表「Capture」按鈕，接著點選「Interfaces」選項，在另一視窗選擇「Start」項目或直接同時按 Ctrl 與 K 鍵進行方包的擷取工作。



(二)點選「Capture」按鈕，接著點選「Options」選項，會出現如左圖的視窗，有許多項目可以對封包的擷取情況進行選擇，選取的項目，在此針對其中幾個較常用的項目進行說明：

#### 1. 封包大小限定：

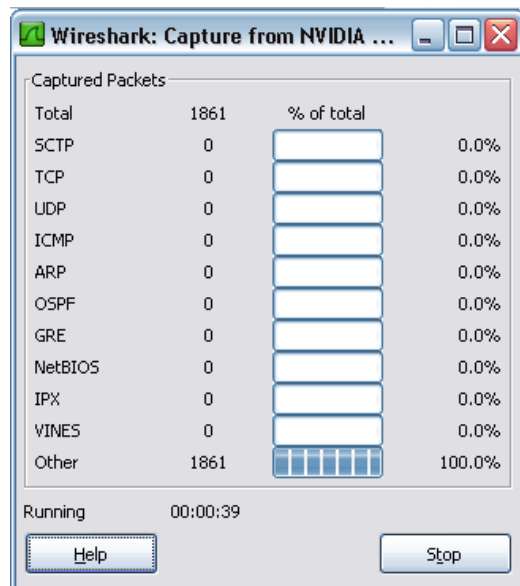
用來對最大封包位元組數進行限制，以乙太網路的封包而言，最大不會超過 1518 位元組，可對自己期望擷取的封包大小進行限定。若對方包大小情況為知，就不要進行設定。

#### 2. 過濾器：

與主畫面下方過濾器的部分相同，用以避免擷取到無用的封包，過濾出符合條件的封包進行截取。

#### 3. 檔案名稱：

用體將擷取的方包資料儲存在檔案中，對檔案名稱進行說明，以方便日後再進行分析。



#### 4. 即時顯示：

如果想馬上看到抓到哪些封包，點選「Update list of packets in real time」項目，封包內容在擷取的過程中就會及實地陸續出現在主畫面「封包列表」等欄位內；而「Hide capture info dialog」欄位則最好移除，才可以在抓封包的同時能出現如左圖的封包類別分析

Filter:

▼ Expression... Clear Apply

四、 過濾器條件的設定

封包擷取條件設定，可以在擷取選項中進行設定，也可以收取完封包後，在對封包進行過濾。Wireshark 過濾封包工具如左圖所示，在主畫面視窗下方的「過濾器(Filter)」進行，過濾器使用簡易的條件是幫助使用者過濾出想要分析的封包，以避免有過多無用封包項目的干擾，提升封包管理的效益。條件是輸入後，以「Apply」按鈕進行封包過濾，有回復原來所有封包則以「Reset」按鈕進行。

五、 以下列出運算子與常用封包過濾條件以及邏輯運算子

運算子

關係	運算子	範例
等於	eq	ip.proto eq 1
	==	ip.proto == 1
不等於	ne	ip.proto ne 1
	!=	ip.proto != 1
大於	gt	Frame.pkt_len gt 100
	>	Frame.pkt_len > 100
小於	lt	Frame.pkt_len lt 100
	<	Frame.pkt_len < 100

常用封包過濾條件

類型		作用說明	舉例
eth	dst	目的 MAC	eth.dst == ff:ff:ff:ff:ff
	src	來源 MAC	eth.src == 00:e0:18:64:ce:f2
	addr	MAC 位址	eth.addr == ff:ff:ff:ff:ff
	type	下一層協定	eth.type == 0x0800(IP) eth.type == 0x0806(ARP)

	ip	dst	目的 IP	ip.dst==140.134.4.1
		src	來源 IP	ip.src == 140.134.30.72
		addr	IP 位址	ip.addr ==140.134.30.72
		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)
		scrport	來源 Port	tcp.scrport ==21(FTP)
		port	Port 編號	tcp.port ==23(Telnet)
	udp	dstport	目的 Port	ucp.dstport == 53(DNS)
		scrport	來源 Port	ucp.scrport == 69(TFTP)
		port	Port 編號	ucp.port == 53

#### 邏輯運算子

邏輯	運算子	範例
AND	and	ip.proto == 1 and ip.dst == 140.134.30.72
	&&	ip.proto == 1 && ip.dst == 140.134.30.72
OR	or	ip.proto == 1 or ip.dst == 140.134.30.72
		ip.proto == 1    ip.dst == 140.134.30.72
NOT	Not	not(ip.proto == 1)
	!	!(ip.proto == 1)

請依據上述教學，回答並做出以下的要求

- 一、若只想抓取與自己 ip 相關的封包，該怎麼做？
- 二、若只想抓取與自己電腦的 mac address 相關的封包，該怎麼做？