PROTOCOL ANALYSIS

－ 網路通訊協定分析 －

WIRE**SHARK**

edit by 3.50

T A N e t 竹 苗 區 域 網 路 中 心

此份文件爲 Protocol Analysis 的教學講義，內容針對課程的內容做一個教學紀錄。

本課程於實做如有需要，可在課堂期間利用
ftp://　　.　　.　　.　　.
ftp://　　.　　.　　.　　.
ftp://　　.　　.　　.　　.
下載需要的檔案來協助您完成本課程。

如有不詳細或是錯誤之部分，歡迎來信討論 (350@ms12.url.com.tw)，或是到資策會 Life 網站尋找解答或是發問。

姓　名：張瑋麟 (350)
ＭＳＮ：taiwan_350@msn.com
E-Mail：350@ms12.url.com.tw
電　話：886-0921758350
　　852-68433705

書目

前言

各位好！首先歡迎各位參加此教育訓練，IT 的世界之大，無法獨身一人自修所有知識，所以希望藉由本課程來減少各位學習的時間，並期望各位能更了解網路架構與目前現況，更能推使各位學習未來新出現的知識與技術。

如果您在目前正在學習網路的基礎，應該是就是由最基礎的訊號存取方式、線材總類…等等，到網路的各項通訊協定，然後最終藉由這些知識開始學習如何在基礎的網路上架設許許多多的網路服務，並應用於自身工作上。

但是您一定會遇到網路或服務有問題的時候：「網路線有接啊！怎麼不能連？」、「設備錯誤燈也沒亮阿，怎麼不通？」、「網路卡也沒壞！未什麼一直說沒連接？」、「網路的設定值也都正確！上不了網？」、「爲什麼網路芳鄰裡面沒人？」怎麼辦？是什麼問題？

沒錯在網路的世界裡是一連串的電子訊號（0、1），網路不通絕對是網路時代裡最嚴重的問題，表面上相同的問題卻不是只有一個「正解」，因爲真正的問題可能「都不一樣」，至於可能的原因，現在的您應該可以列出 100 個可能出來！

所以即使您是個職場老手，在遇到一些問題時，常常一樣會摸不著頭緒，因爲人是無法直接視別那些電子訊號的，所以看不出真正問題是在哪裡！只能用猜測，實在是費功耗時。

而我們的課程內容就是要讓各位利用 WIRESHARK 來「分析」檢測網路狀態，甚至做到監視的作用，解決網路問題；而本課程採用互相交流與討論方式，也希望對於您目前工作有所啓發或更深一層的了解。

在這門課之後後，您應該會：

- 熟悉 WIRESHARK 的操作
- 了解不同服務應該會有哪些重要的通訊協定
- 由真實網路環境來印證 TCP/IP 的通訊協定
- 從封包中找出可能的錯誤
- 由封包看出使用者的問題

好好把握本課程的練習，希望可以帶給各位學習網路有幫助，祝福各位！

PROTOCOL ANALYSIS

Install WIRESHARK

WIRESHARK

Wireshark 是個分析網路封包的軟體， 是個完全自由以及免費的網路封包分析軟體，您可以藉由 Wireshark 分析您想了解的封包，並從中獲得資訊，甚至網路問題的解決方法。

Wireshark 自版本 1.2.0 起開始支援 64bit 作業系統安裝，並提供更友善的「開始畫面」，更支援分析更多的通訊協定，如果您時常得分析網路封包狀態，建議您時常的到 Wireshark 官方網站，檢查看看是否有沒有新的版本。

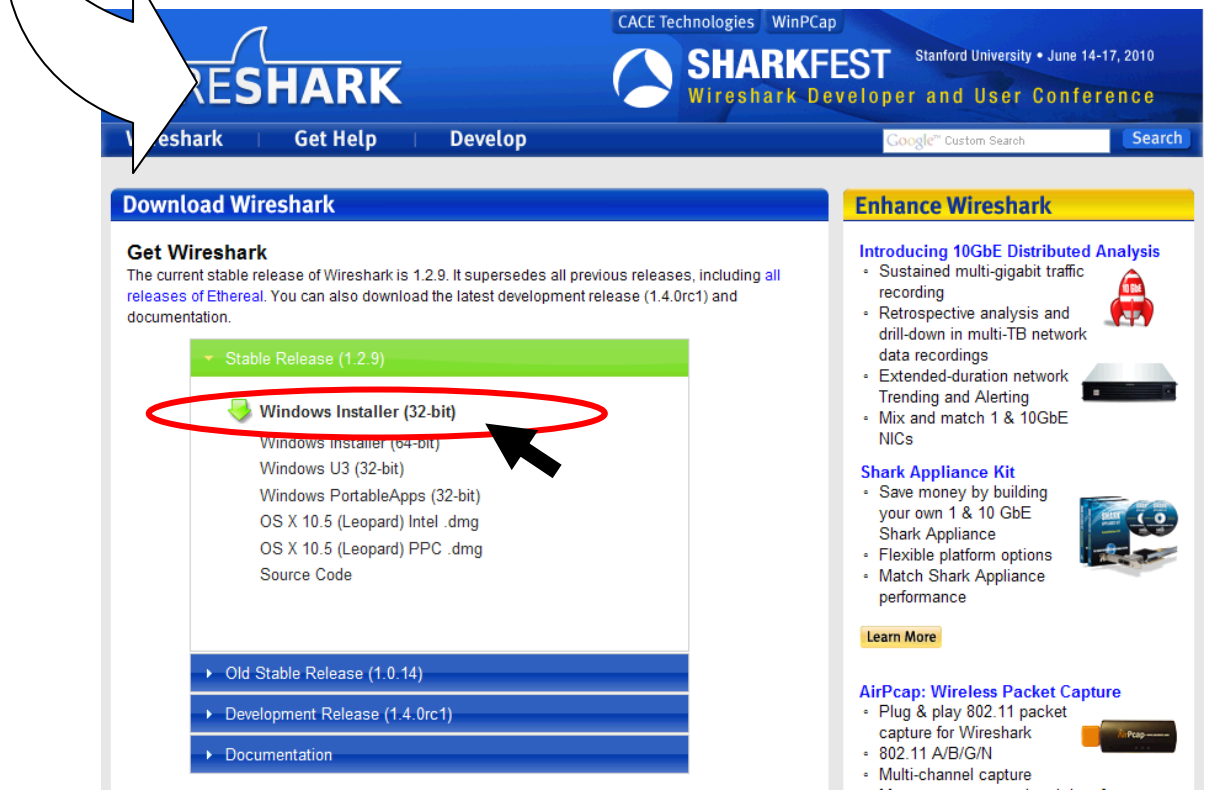
網址： http://www.wireshark.org/

附註：您應該知道，Wireshark 的前身叫做 Ethereal。

下載 WIRESHARK (1.2.9)

您可以在官方網站上直接點進「Download Wireshark」網頁取得最新版本，或是直接以瀏覽器開啓：http://www.wireshark.org/download.html

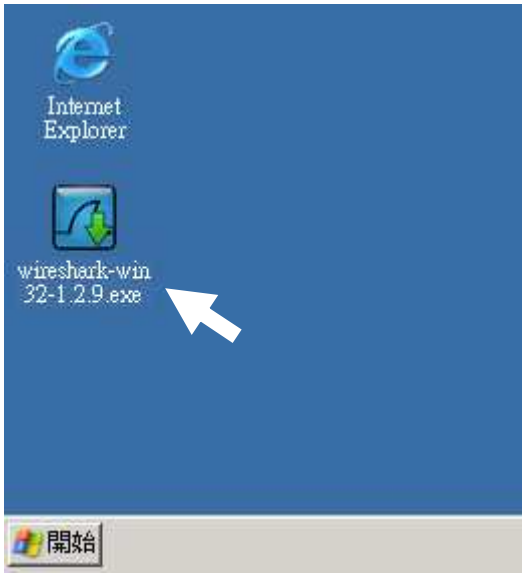
請選擇 「Download Wireshark」進入下載頁面



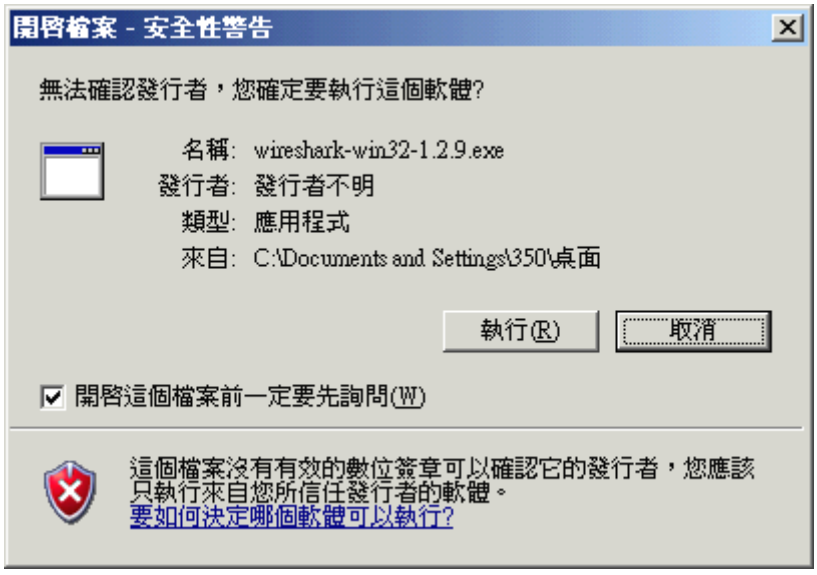
請下載您目前所用的作業系統的 Wireshark 版本，
本課程以 Windows XP 爲例，所以選取 Windows 32bit 版本

安裝 Wireshark (與 WinPcap)

本範例是將下載好的檔案「wireshark-win32-1.2.9.exe」存放在桌面上，請在您下載好的執行檔上點兩下開始安裝。

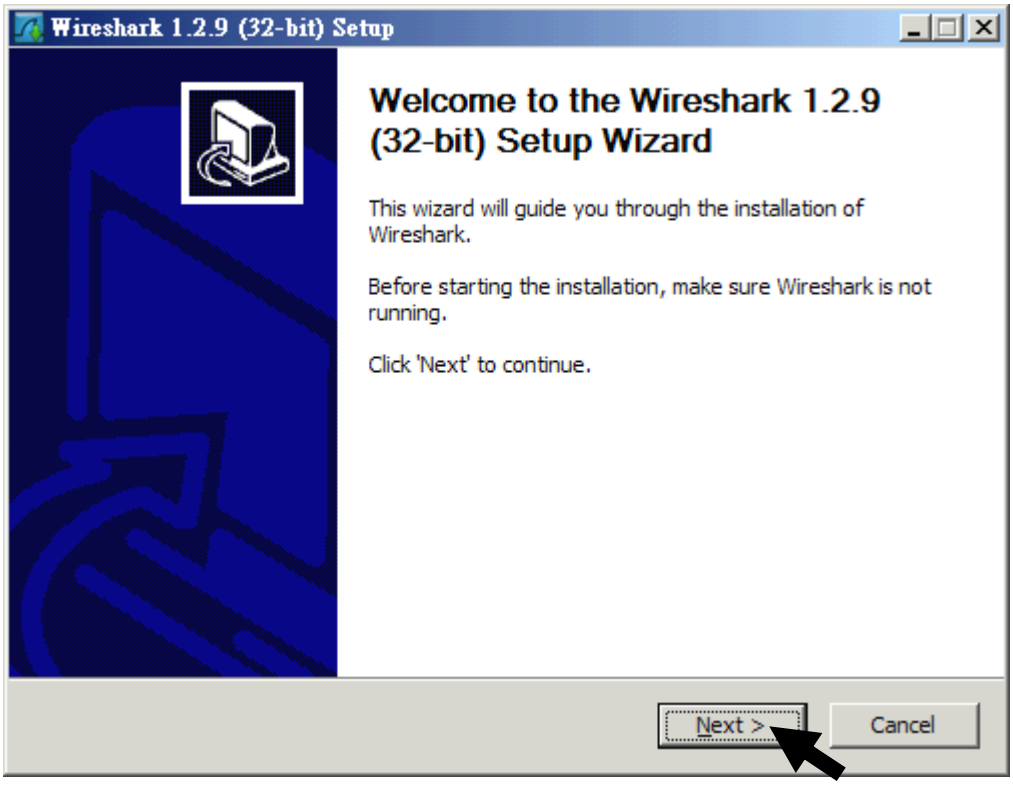


點兩下桌面的「wireshark-win32-1.2.9.exe」開始安裝

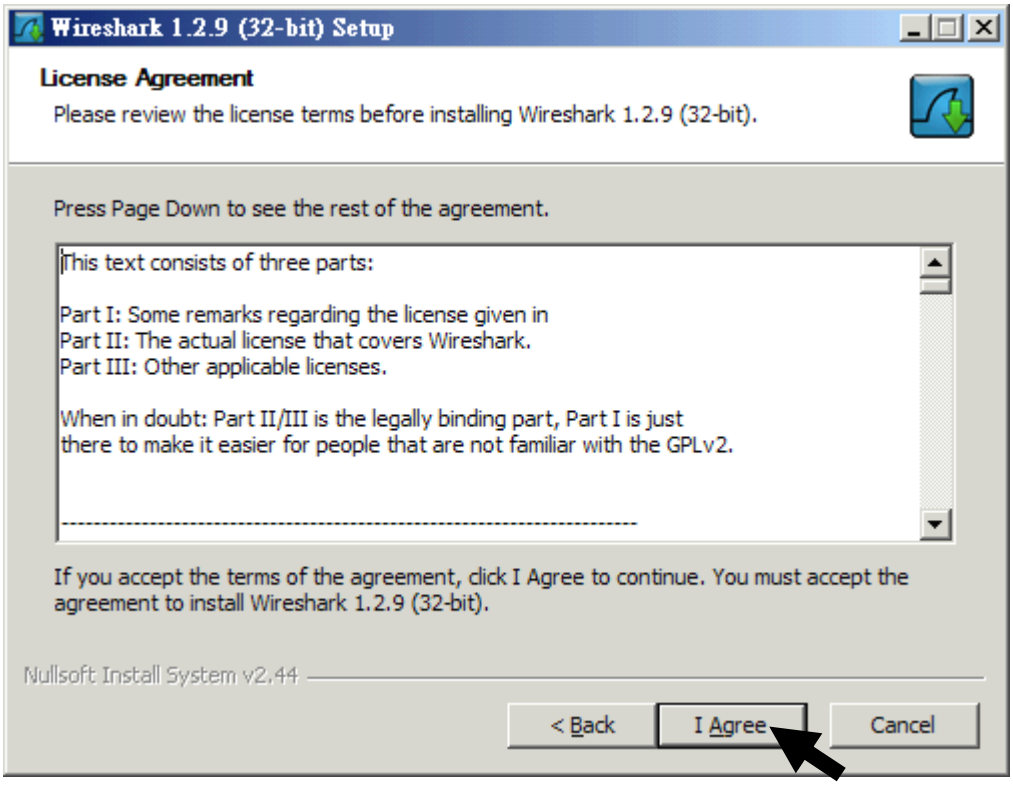


此爲 Windows XP 安全性警告，請暫時忽略並按「執行」繼續

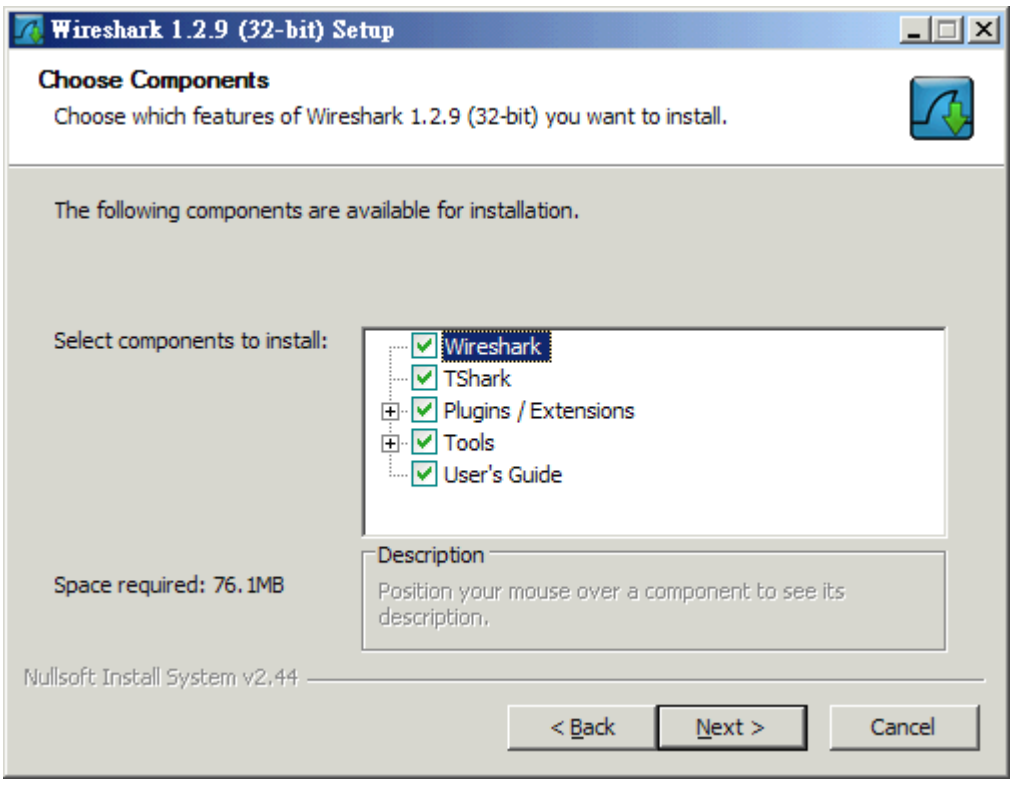
附註：如果您的作業系統爲 Windows Vista 或 Windows 7，請自行針對 UAC (User Account Control 使用者帳戶控制) 做設定。



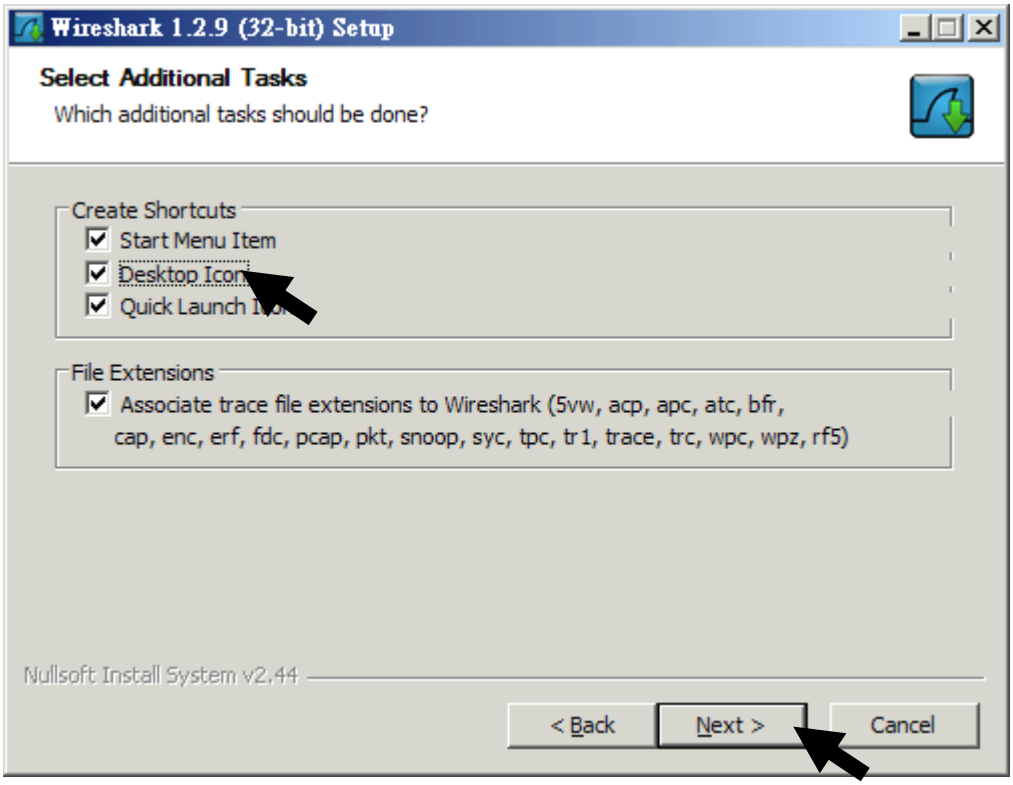
Wireshark 歡迎畫面，請按「Next」繼續



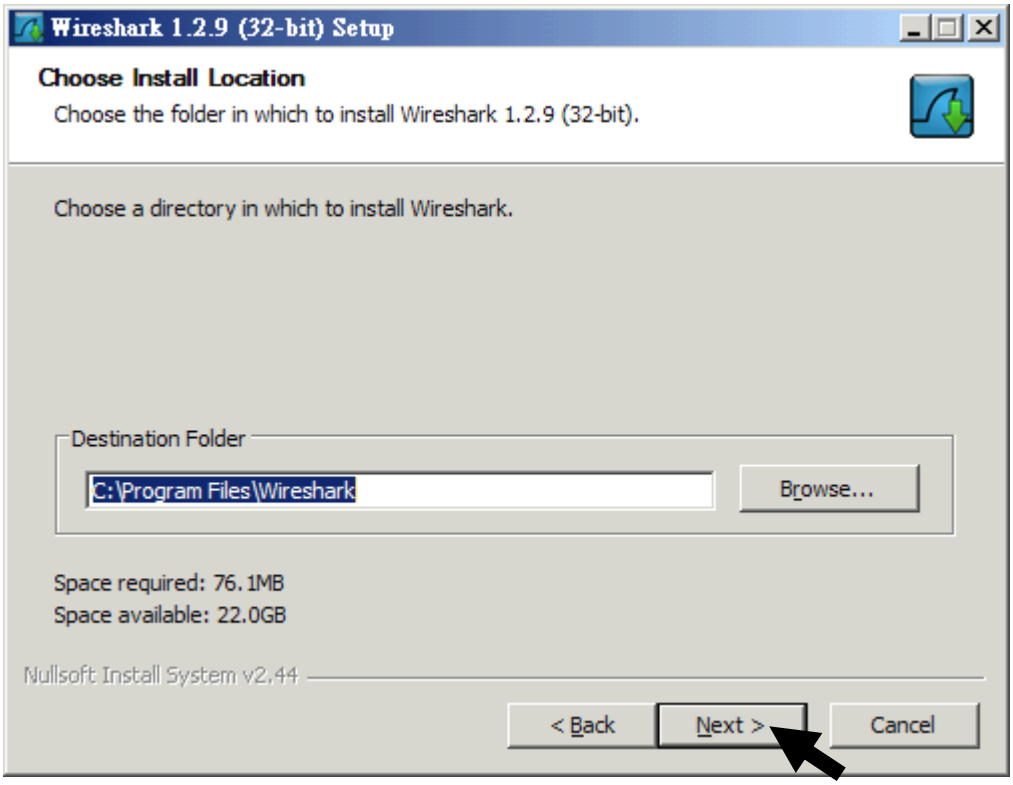
版權說明畫面，閱讀後如同意，請按「I Agree」繼續安裝



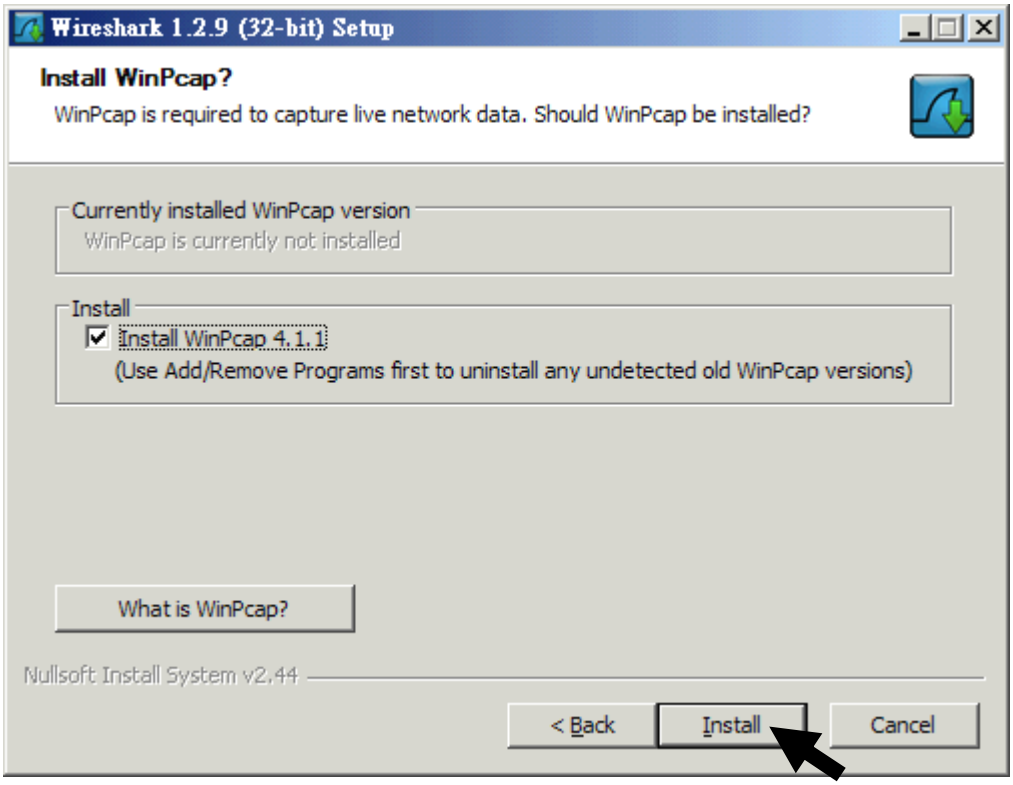
選擇安裝項目，這裡選擇預設安裝 (全選) 的方式，按下「Next」繼續



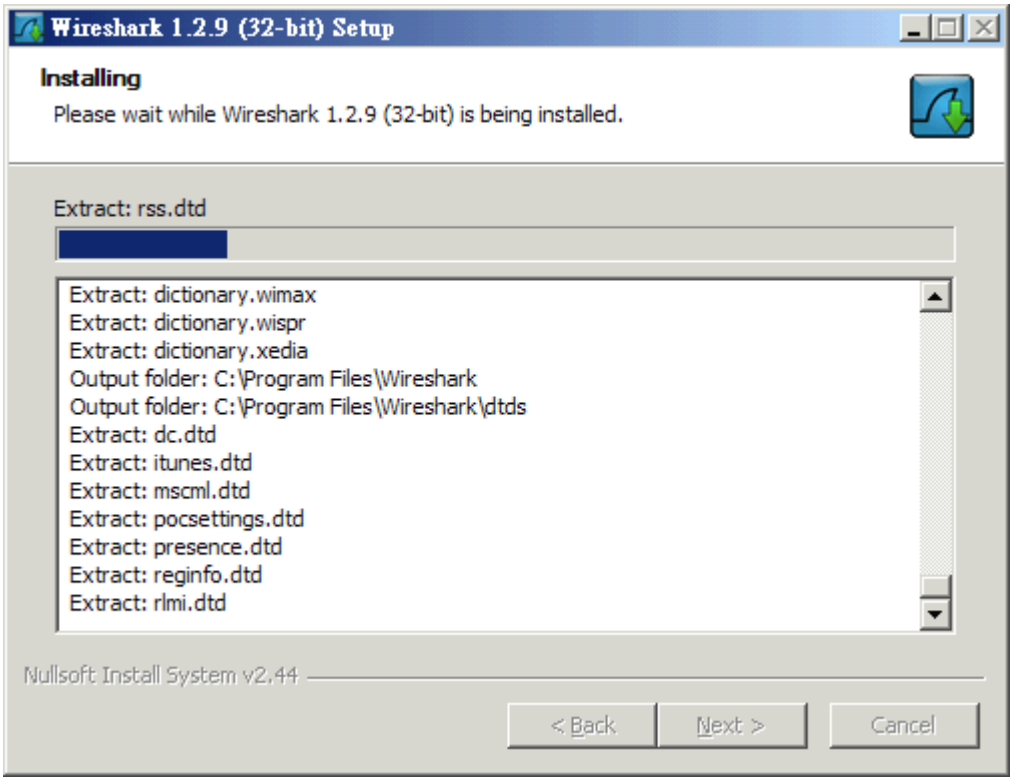
如果想在桌面有 Wireshark 捷徑，請選擇「Desktop Icon」，按下「Next」繼續



您可以指定安裝路徑，本範例使用預設路徑，按下「Next」繼續



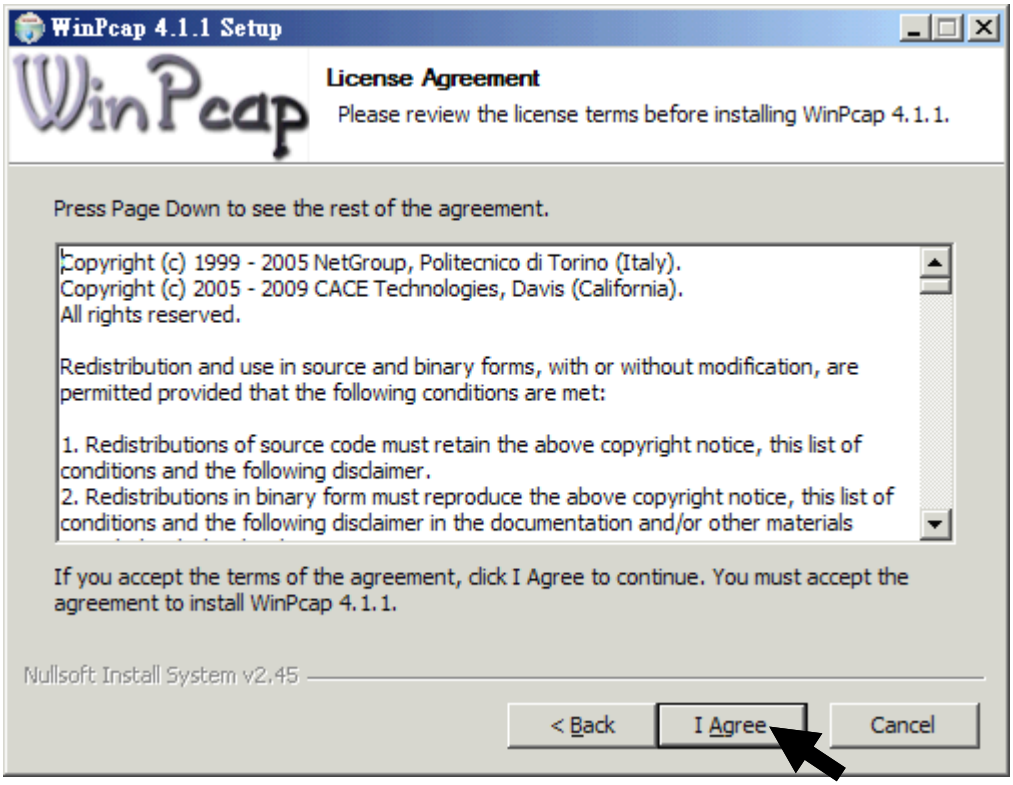
Wireshark 需 WinPcap（預設），按下「Next」繼續



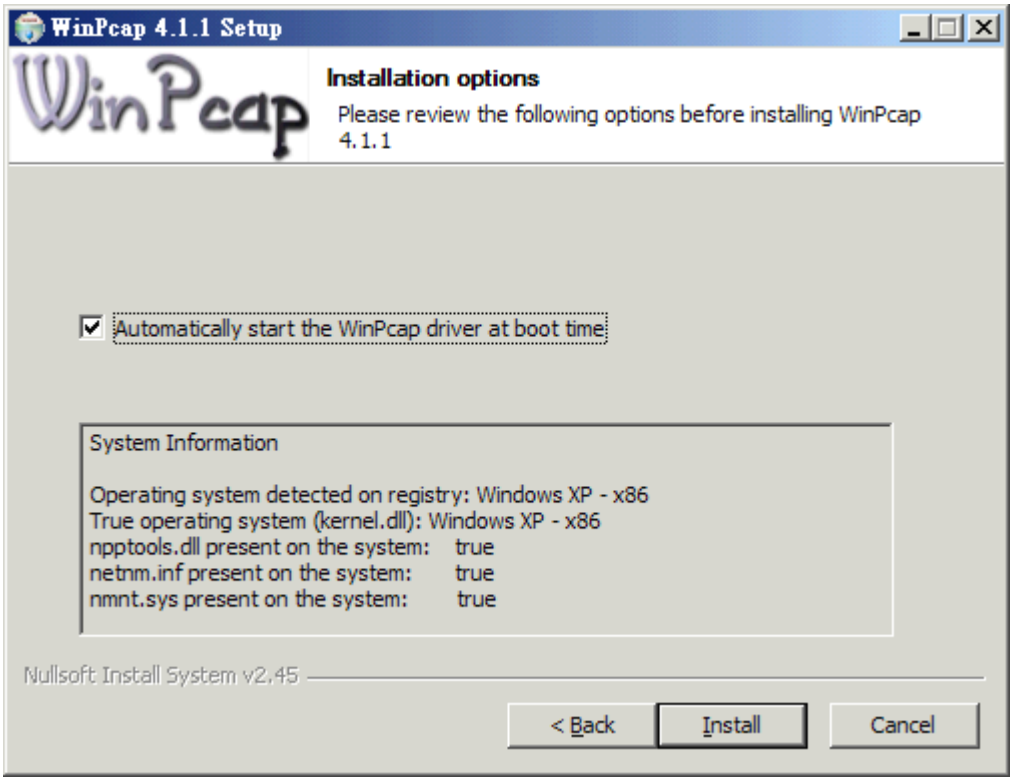
解壓縮 Wireshark，請稍待…

接下來安裝 WinPcap，按下「Next」繼續

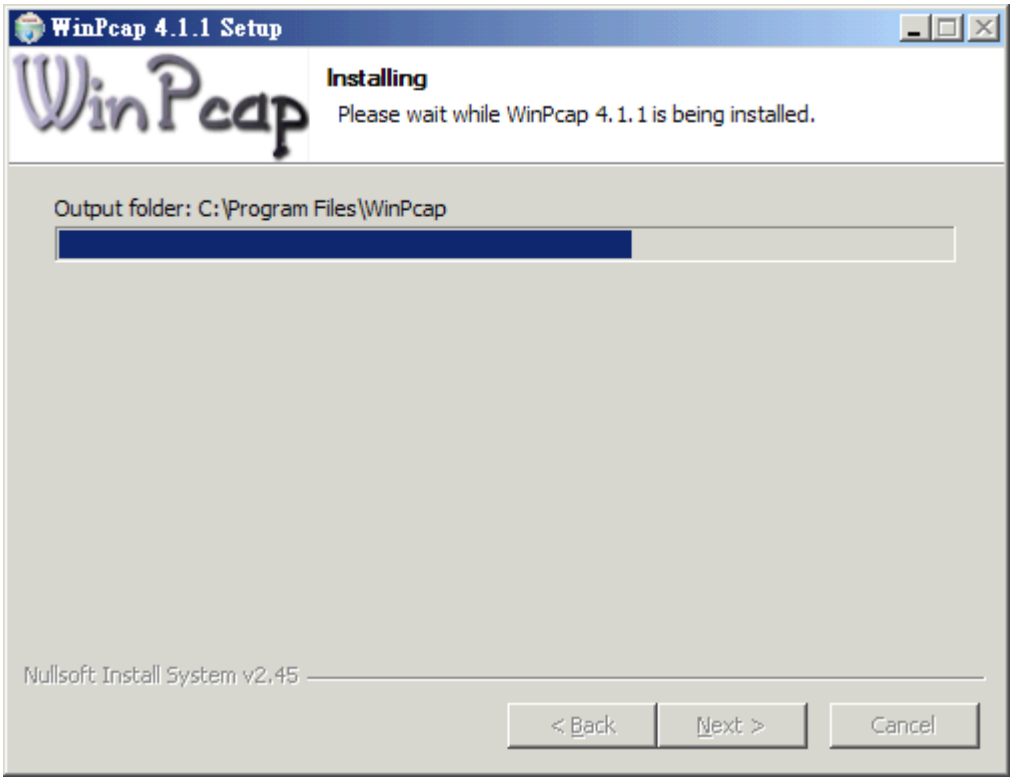
WinPcap 歡迎畫面，請按「Next」繼續



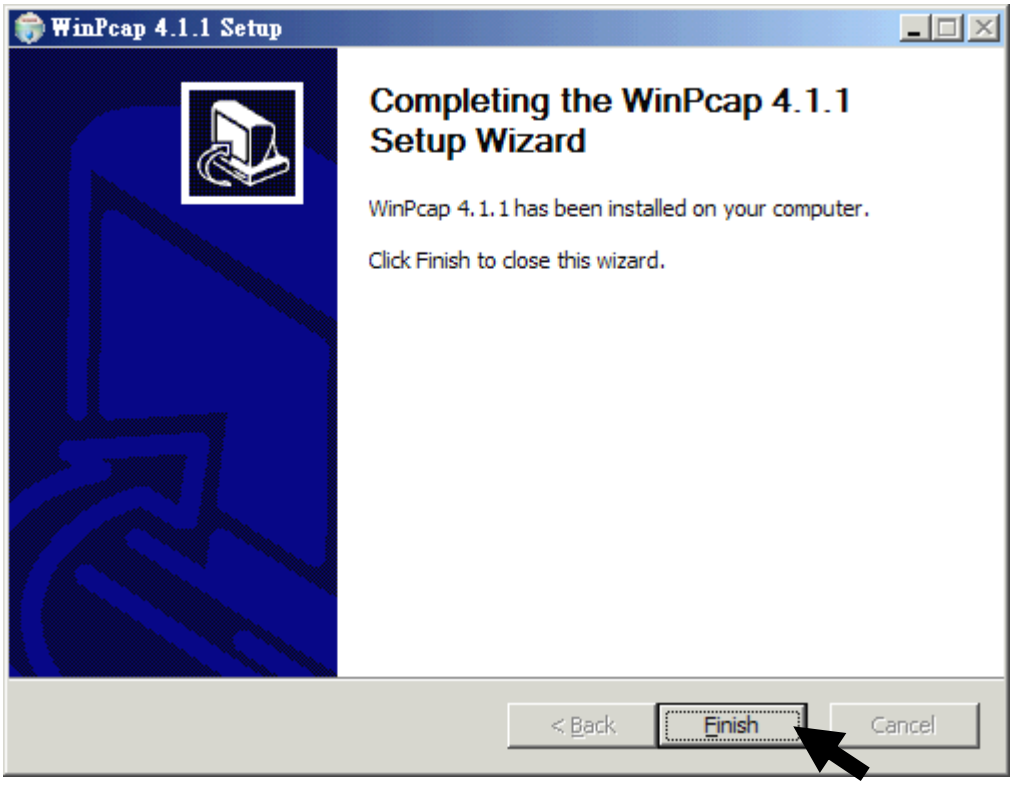
版權說明畫面，閱讀後如同意，請按「I Agree」繼續安裝



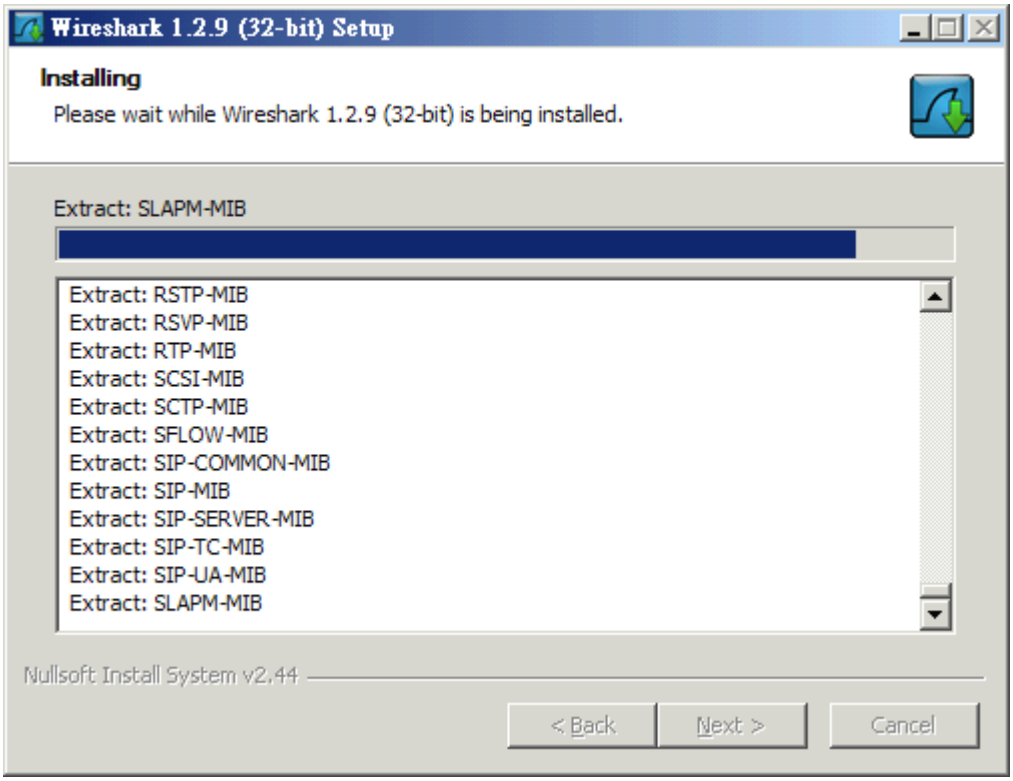
設定封包擷取程式 WinPcap 於開機時啓動 (預設爲啓動)，
按「Install」開始安裝



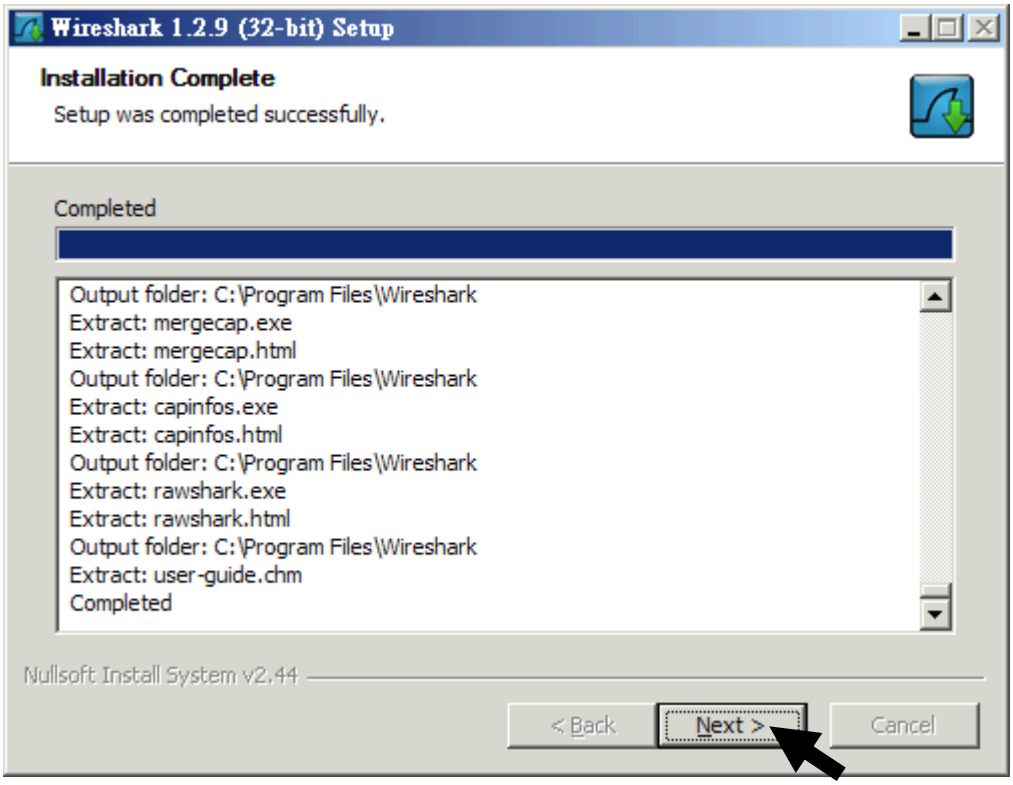
正在安裝 WinPcap，請稍待…



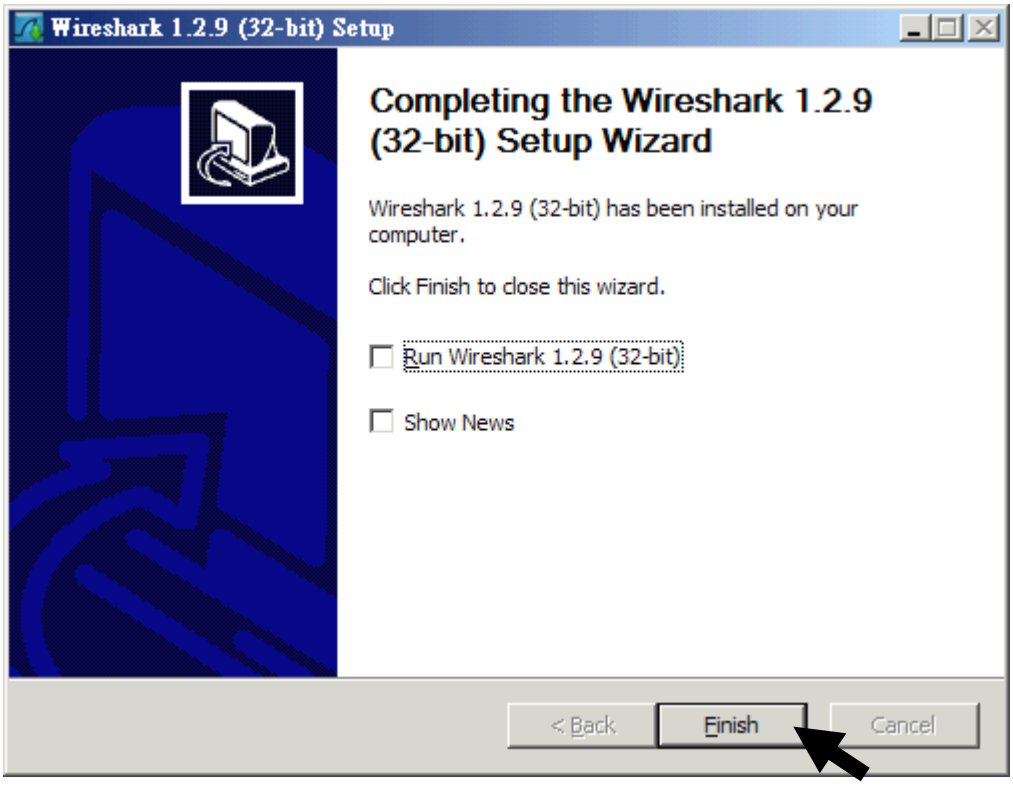
WinPcap 安裝完畢，請按「Finish」繼續



開始安裝 Wireshark，請稍待…



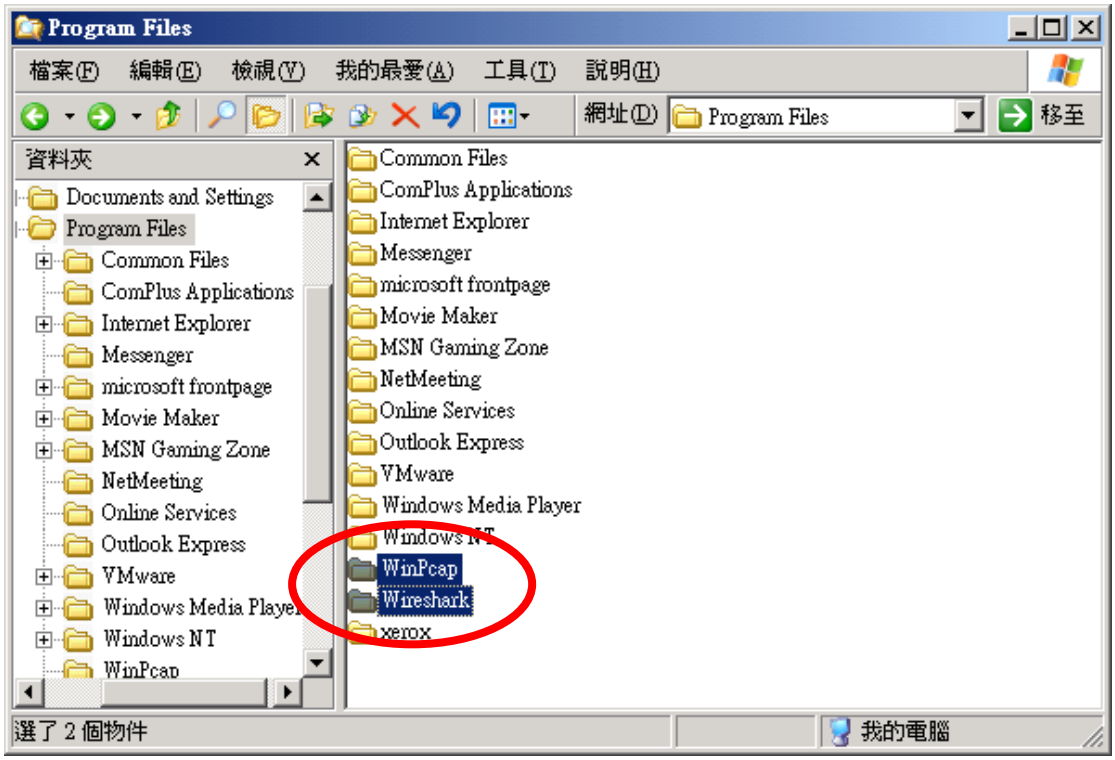
Wireshark 安裝完畢，請按「Next」繼續



Wireshark 安裝成功，請按「Finish」結束安裝程式

程式位置

如果您是與本範例一樣爲 Windows 系統，並採用預設安裝路徑，您將會在下方位置找到 Wireshark 與 WinPcap 兩個目錄。



Wireshark 與 WinPcap 安裝位置，

C:\Program Files\WinPcap

&

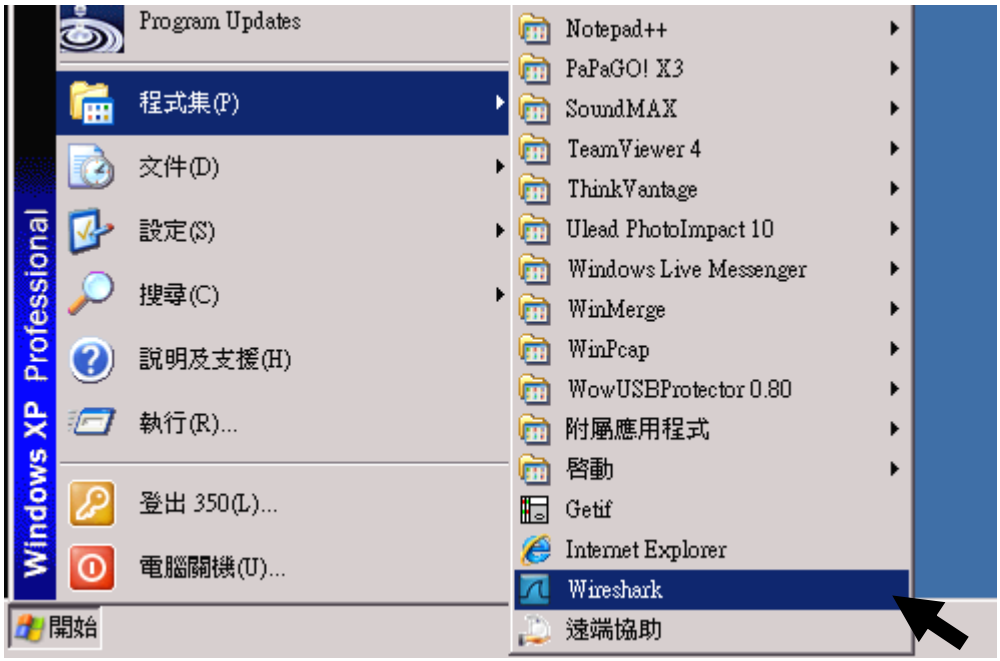
C:\Program Files\Wireshark

Wireshark 啓動方式 (一)

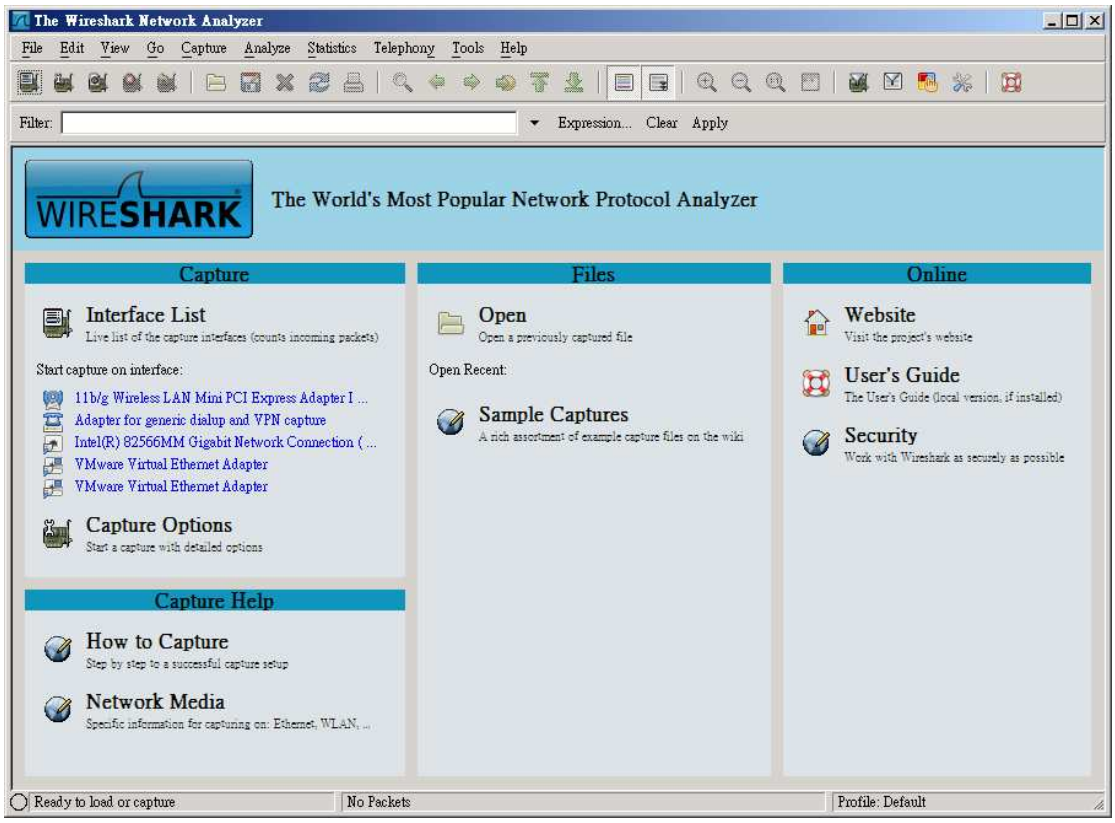
啓動 Wireshark 您可以選擇兩種方式，一種是於桌面捷徑的 Wireshark 圖示點兩下執行：

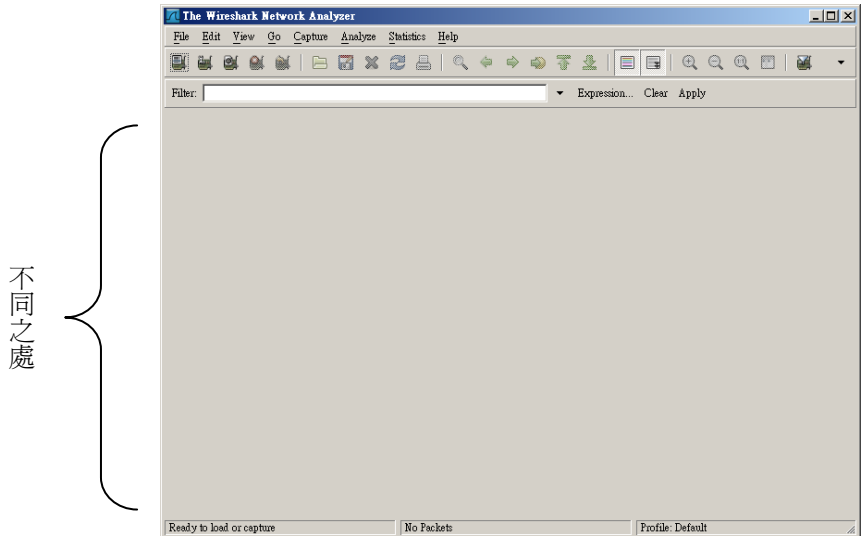
Wireshark 啓動方式 (二)

或是以「開始」→「程式集」→「Wireshark」來啓動。



下面爲 Wireshark 1.2.0 之後的版本，在歡迎畫面已經做了改變，直覺上更爲平易近人，但在與 Wireshark 1.2.0 之前的版本比較起來 (圖於最右下方)，除了開始頁面外，畫面幾乎完全相同。



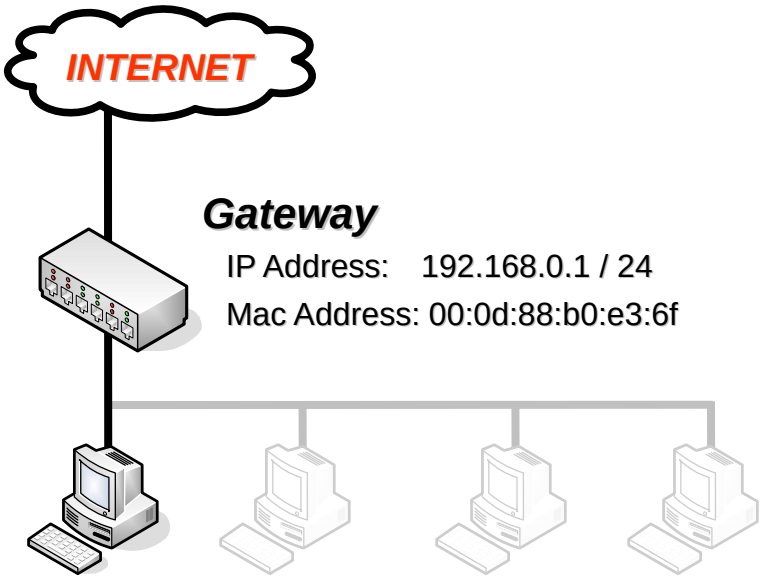


Wireshark 1.0.4 主畫面

PROTOCOL ANALYSIS

Quick Start With WIRESHARK

講義環境設定



Gateway

IP Address: 192.168.0.1 / 24

Mac Address: 00:0d:88:b0:e3:6f

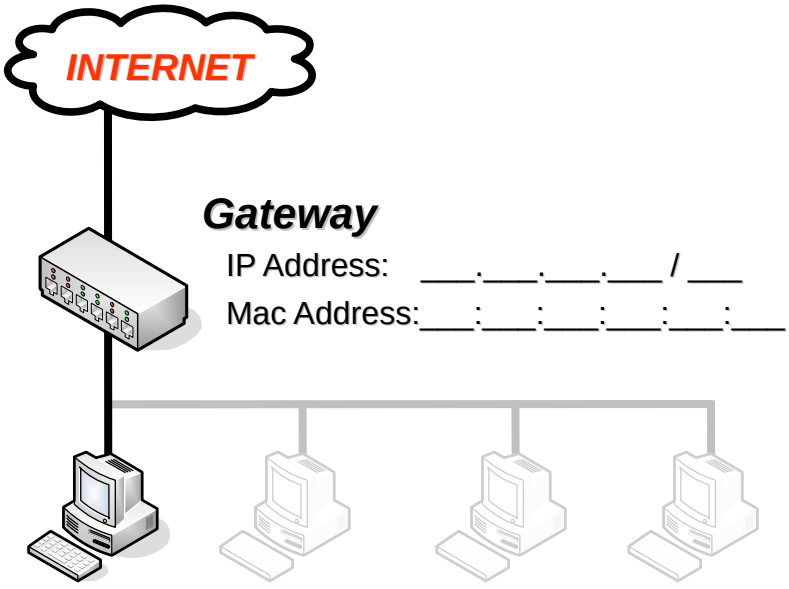
PC/Workstation

IP Address: 192.168.0.175 / 24

Mac Address: 00:1d:d9:60:19:c2

Gateway: 192.168.0.1

我的環境設定



Gateway

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

PC/Workstation

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

擷取封包的方式

請確認您的 Wireshark 以及 WinPcap 安裝正確，才可以順利啓動 Wireshark！

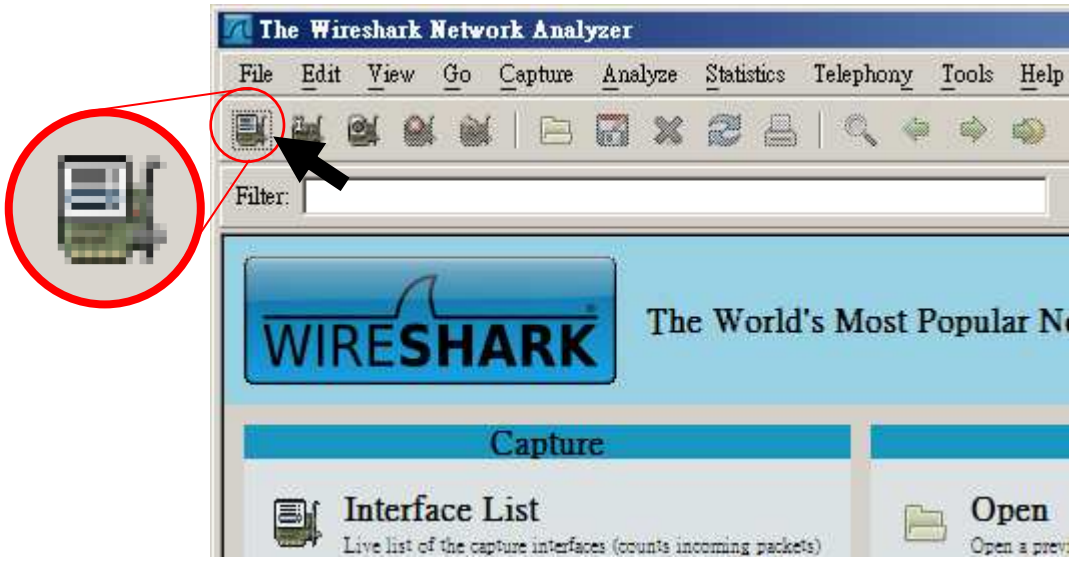
第一步，我們先快速的來擷取封包，在開始之前，您得先了解您目前的網路連線方式與環境，再來決定您擷取封包的方式， 350 將以兩的方向來作解釋，分別是「**有線網路**」以及「**無線網路**」:

Ａ：有線網路　擷取方式

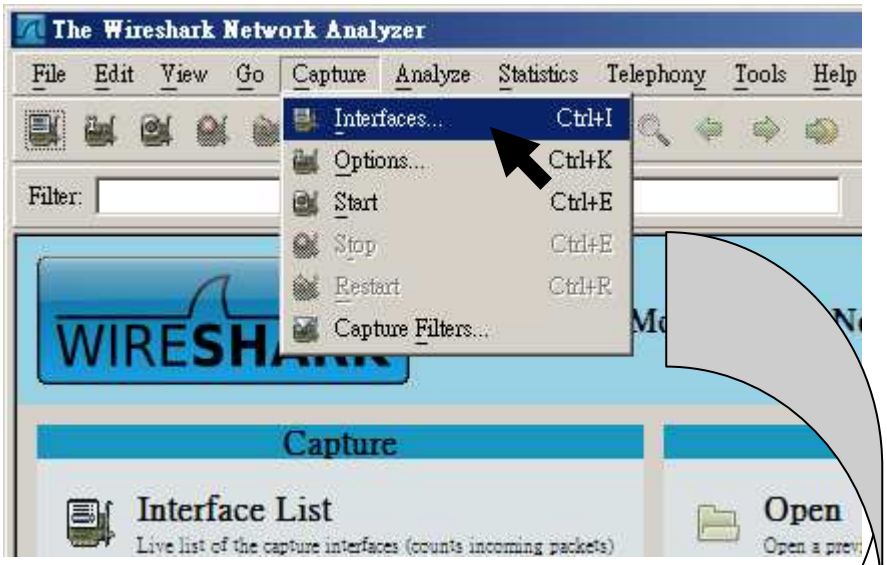
如果您是有線網路，我們這裡介紹兩種方式，讓您快速的啓動封包擷取：

啓動擷取介面選擇視窗：(請選下列Ａ1、A2 其一方式)

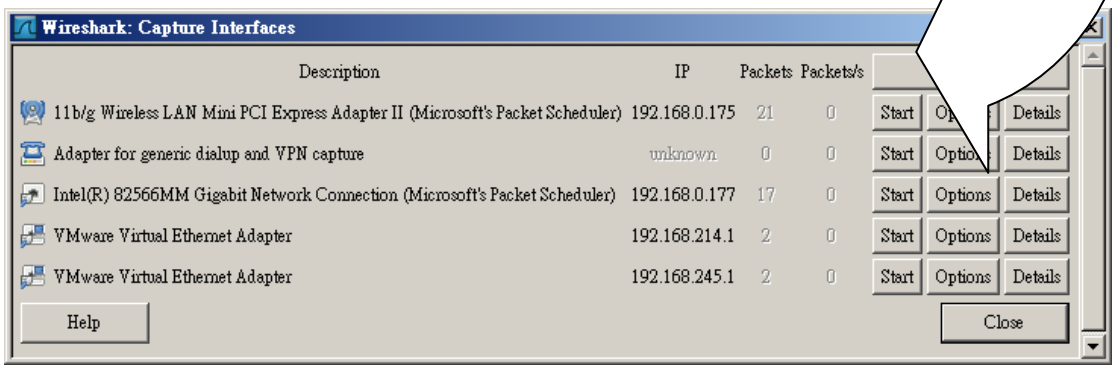
Ａ１：直接點選主畫面的圖示列「List the available capture interfaces...」



Ａ２：直接點選主畫面的功能列「Capture」→「interfaces…」

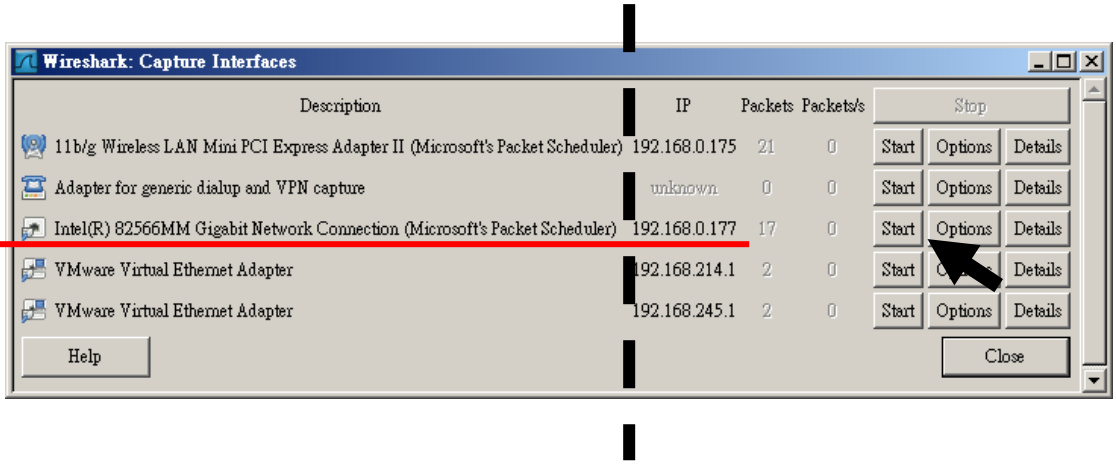


會出現您現在系統可以擷取的介面清單視窗：

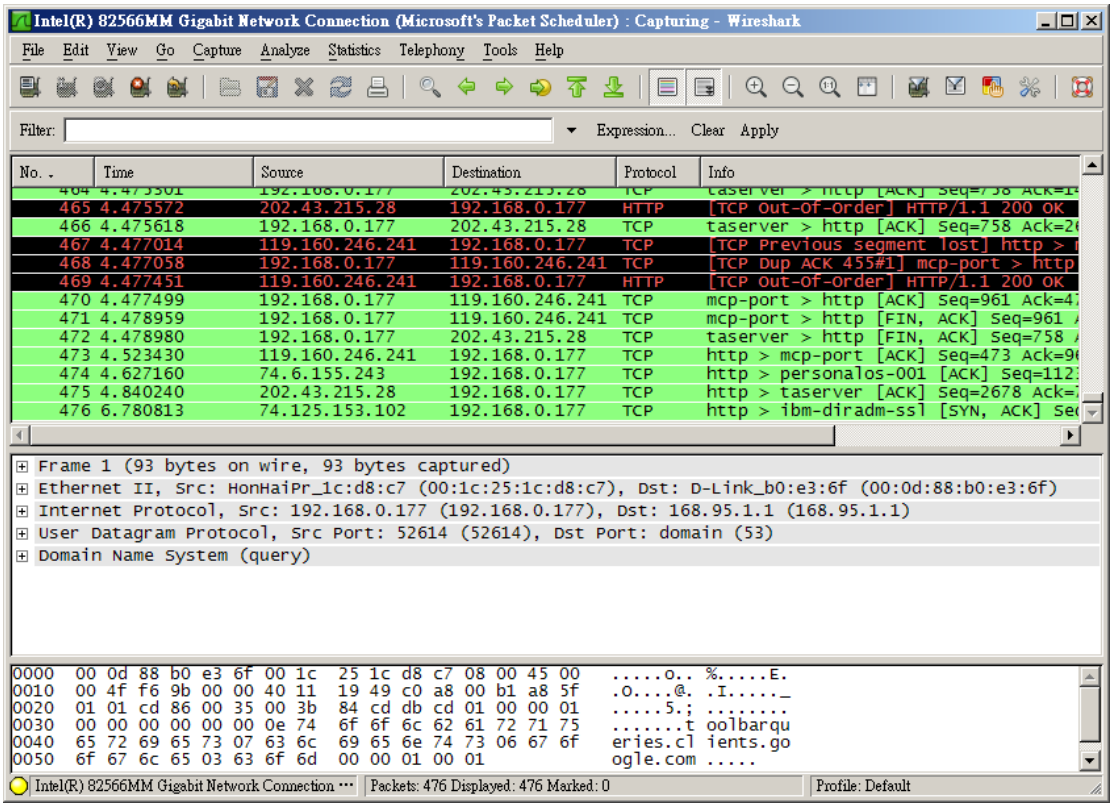


選擇擷取介面：（有線網路）

請直接按下您的有線網路（Intel(R) 82566MM Gigabit Network Connection 爲有線網路） 的「Start」

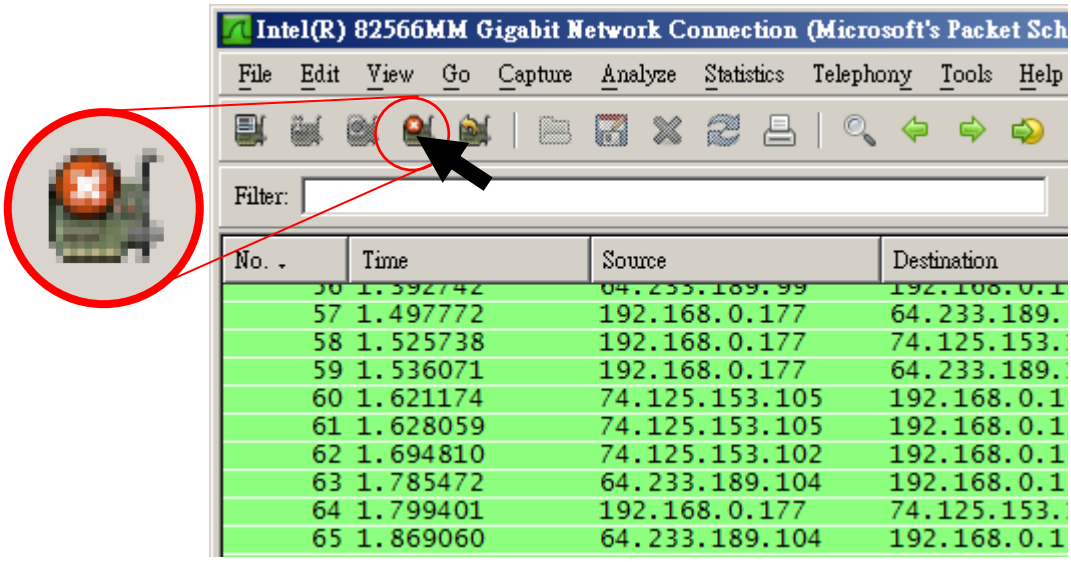


然後就開始擷取有線網路卡的封包了：

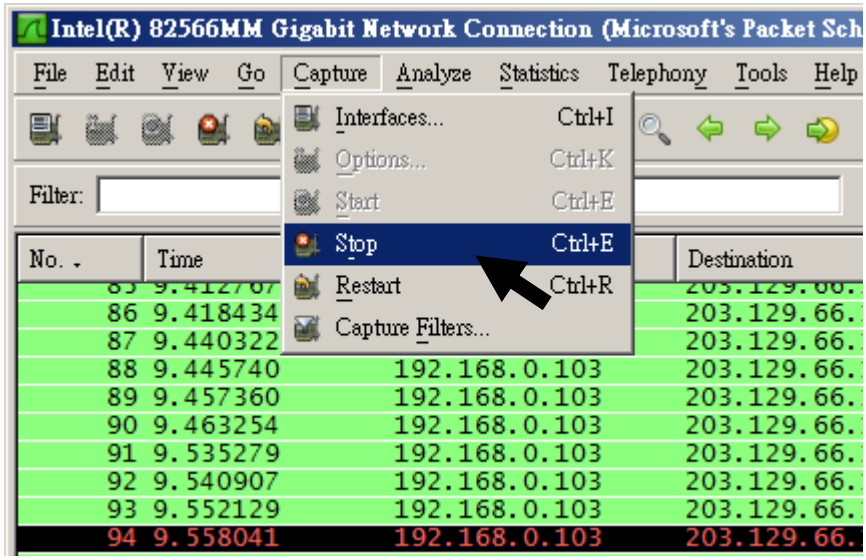


停止擷取：

Ａ１：直接點選主畫面的圖示列「Stop the running livie capture」



Ａ２：直接點選主畫面的功能列「Capture」→「Stop」



B：無線網路　擷取方式

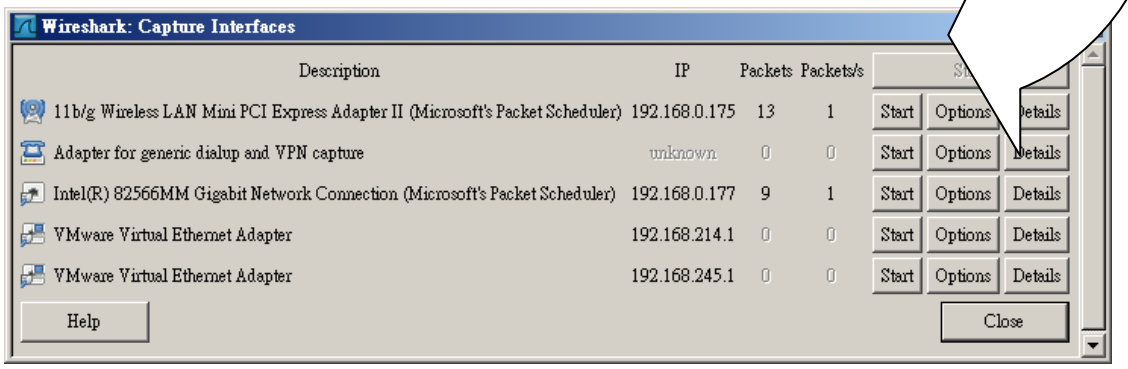
如果您是無線網路，我們這裡也介紹兩種方式，讓您快速的啓動封包擷取：

啓動擷取介面選擇視窗：（請選下列 B1、B2 其一方式）

Ｂ１：直接點選主畫面的圖示列「List the available capture interfaces...」

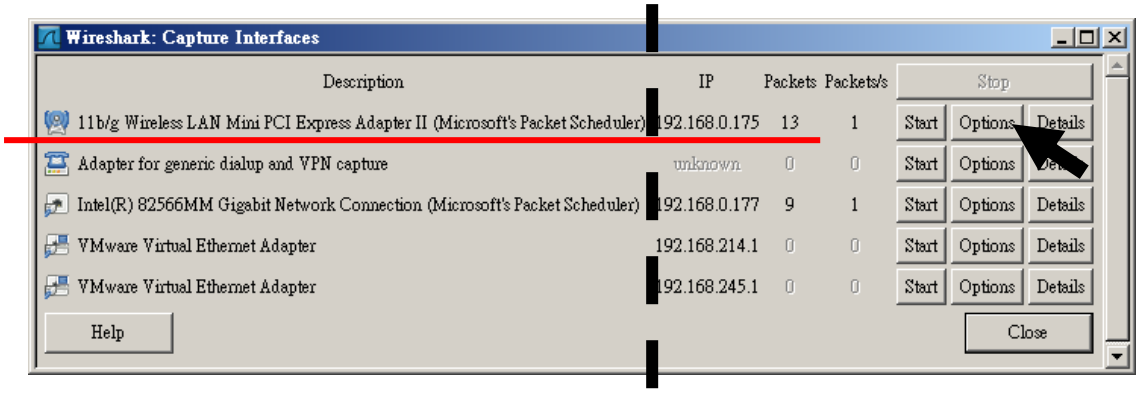
Ｂ２：直接點選主畫面的功能列「Capture」→「interfaces…」

會出現您現在系統可以擷取的介面清單視窗：

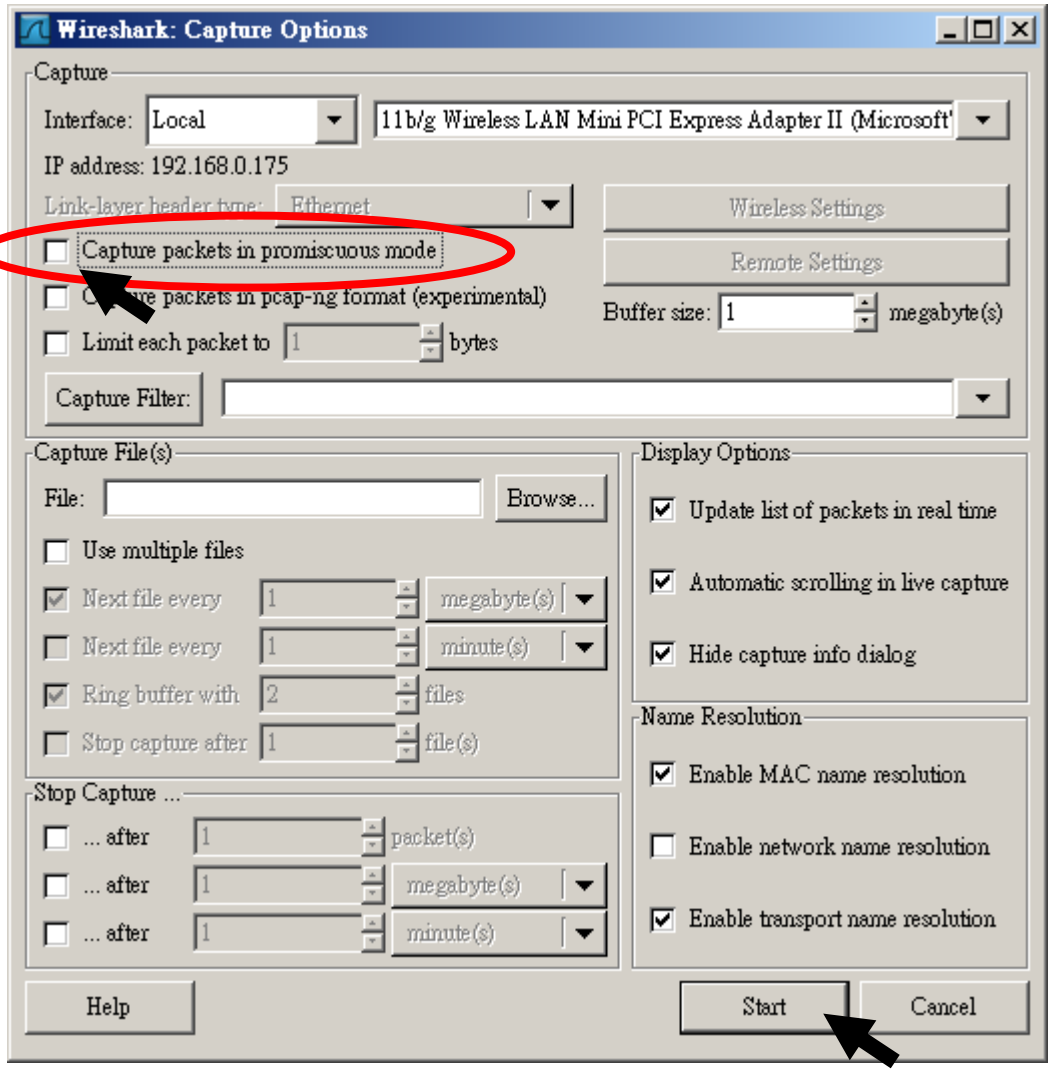


選擇擷取介面：（無線網路）

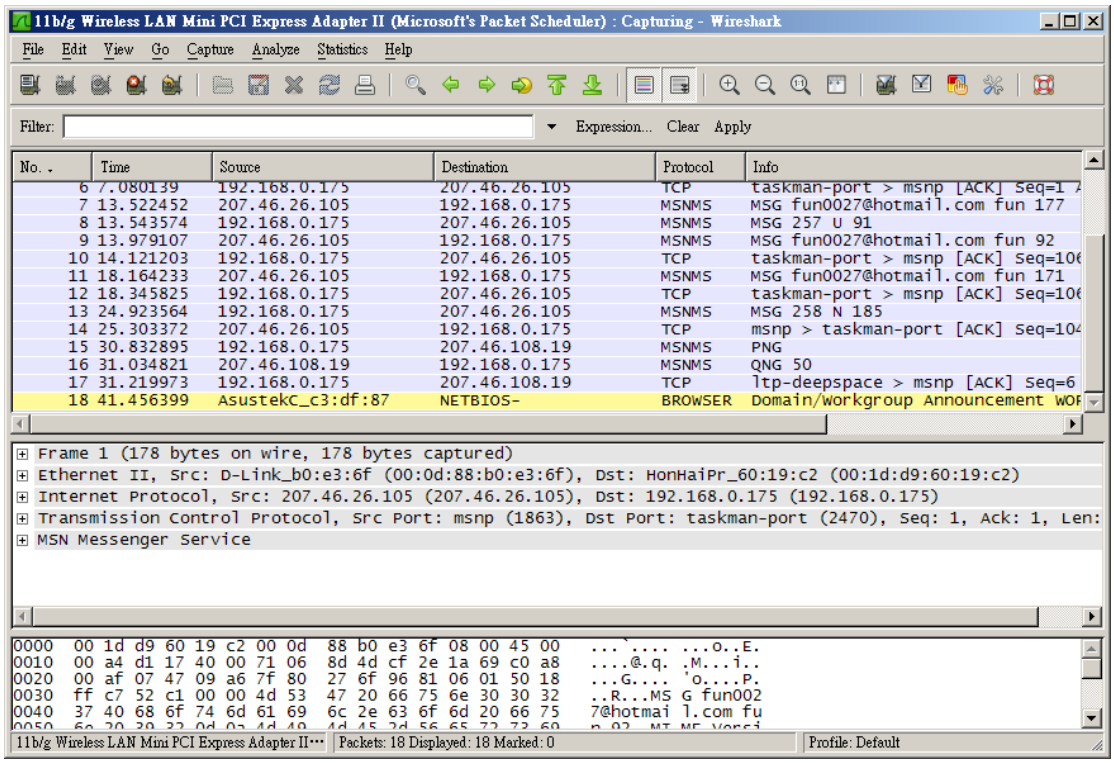
請直接按下您的有線網路 (11b/g Wireless LAN Mini PCI Express Adapter II 爲無線網路卡) 的「**Options**」



由於我們是用無線網路，所以我們無線網路卡不可以「Promiscuous Mode」啓動，不然會擷取不到封包！

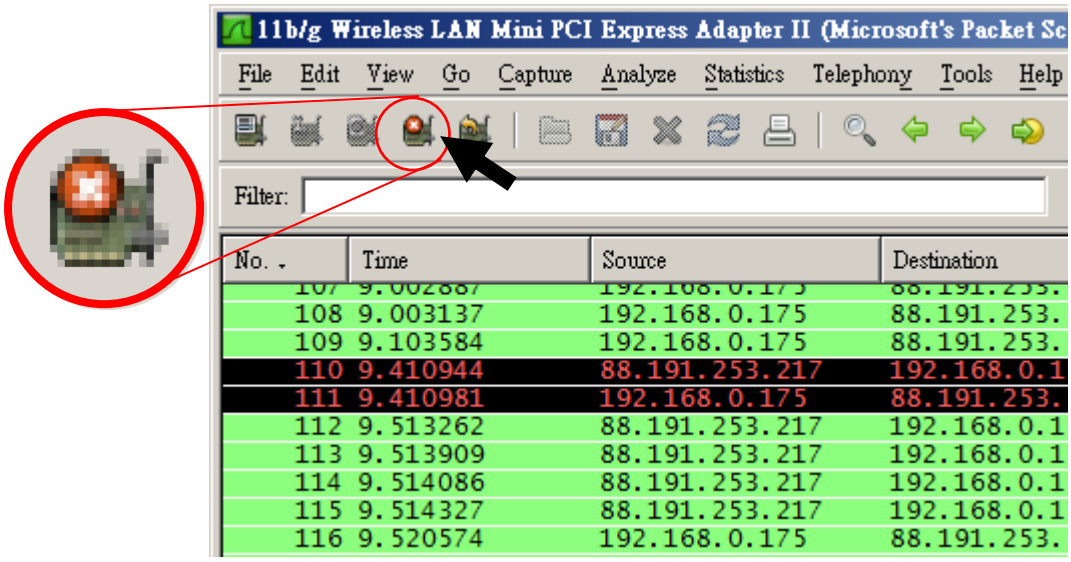


然後就會開始擷取無線網路卡的封包了：

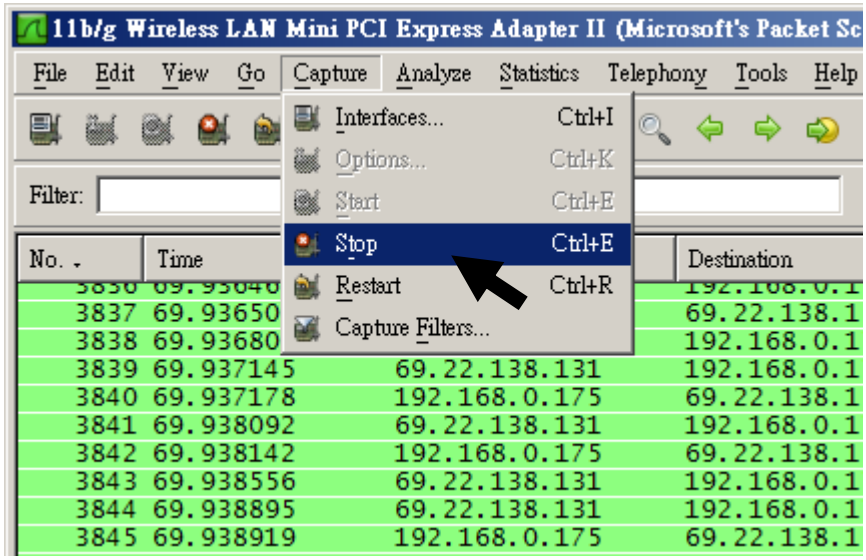


停止擷取：

Ｂ１：直接點選主畫面的圖示列「Stop the running live capture」

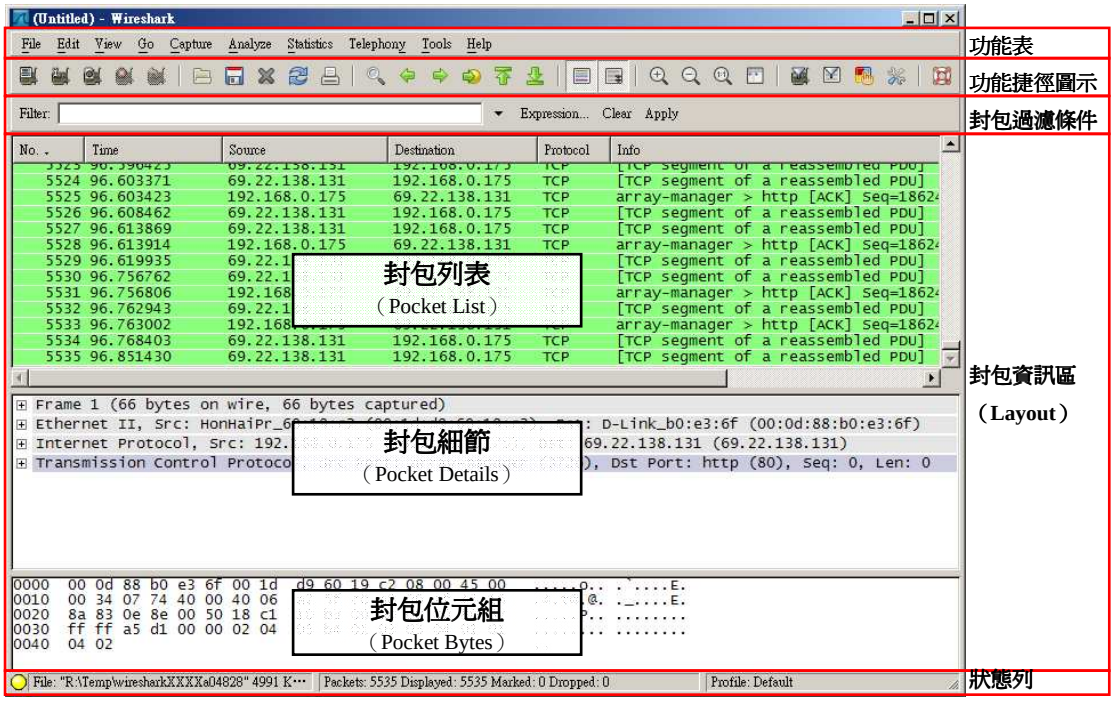


Ｂ２：直接點選主畫面的功能列「Capture」→「Stop」



主畫面介紹

下列是已經擷取到封包的畫面配置，在您的畫面中「封包資訊區（Layout）」區域應該有許多剛剛擷取的封包（有封包的狀態）。



功能表：所有的功能都可以在這些地方找到

功能捷徑圖示：常用的功能會放在此處

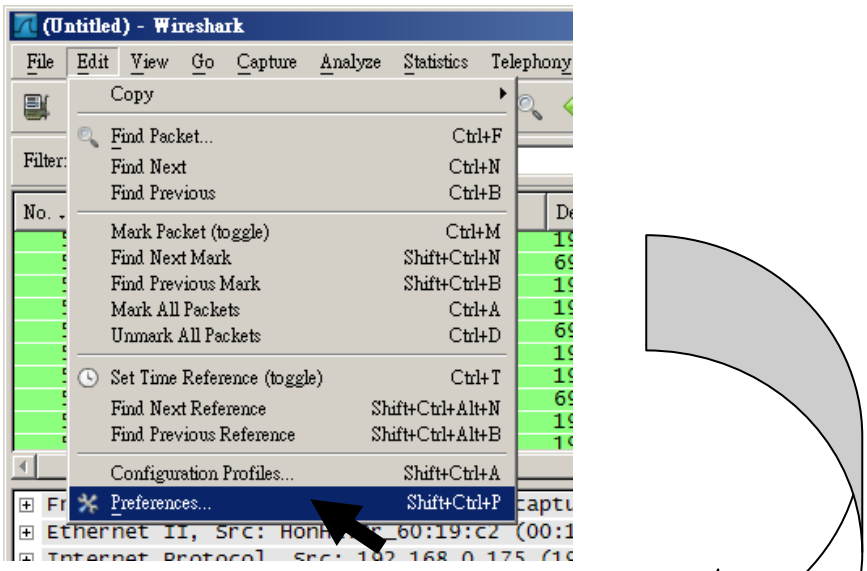
封包過濾條件：可以過濾出封包資訊區里特定的封包

封包資訊區：分成三塊，分別是封包列表、封包細節、封包位元組。

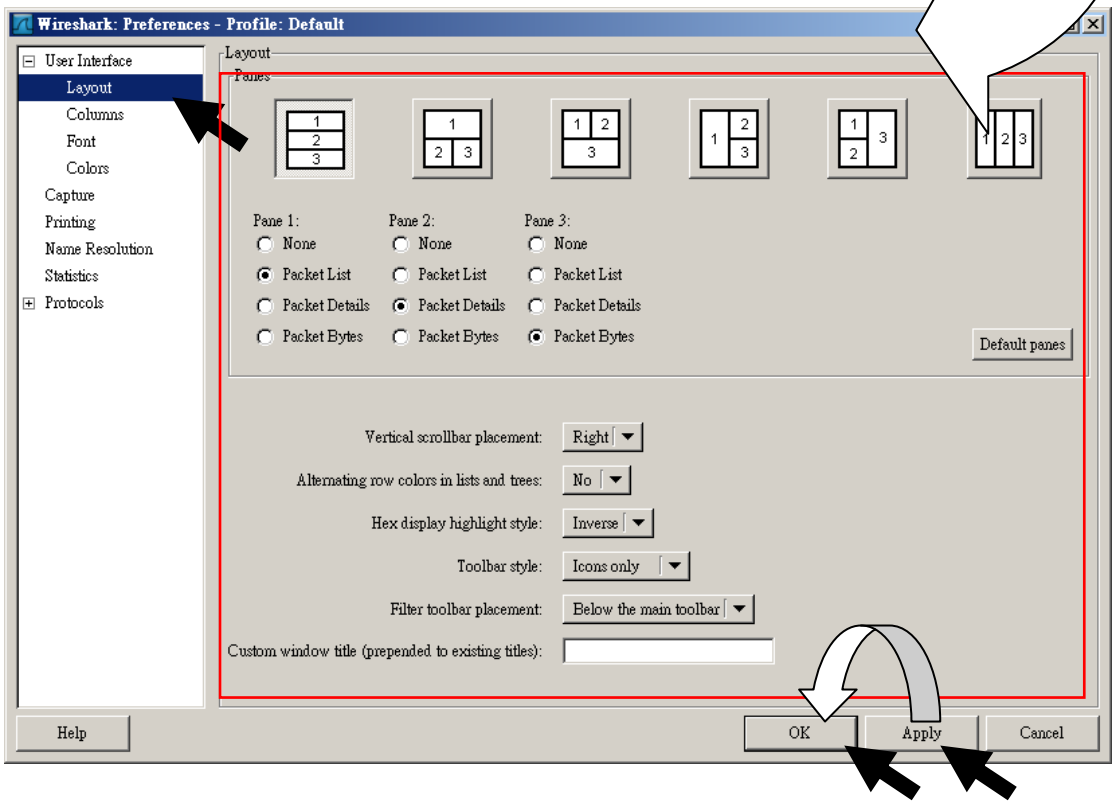
狀態列：這裡會顯示您的監視狀態，或是擷取重要提示資訊。

變更封包檢視方式 (Layout)

以上這是預設的基本畫面配置，當然您可以依照您的喜愛變更，如果您希望變更，請您可以跟著這樣做：



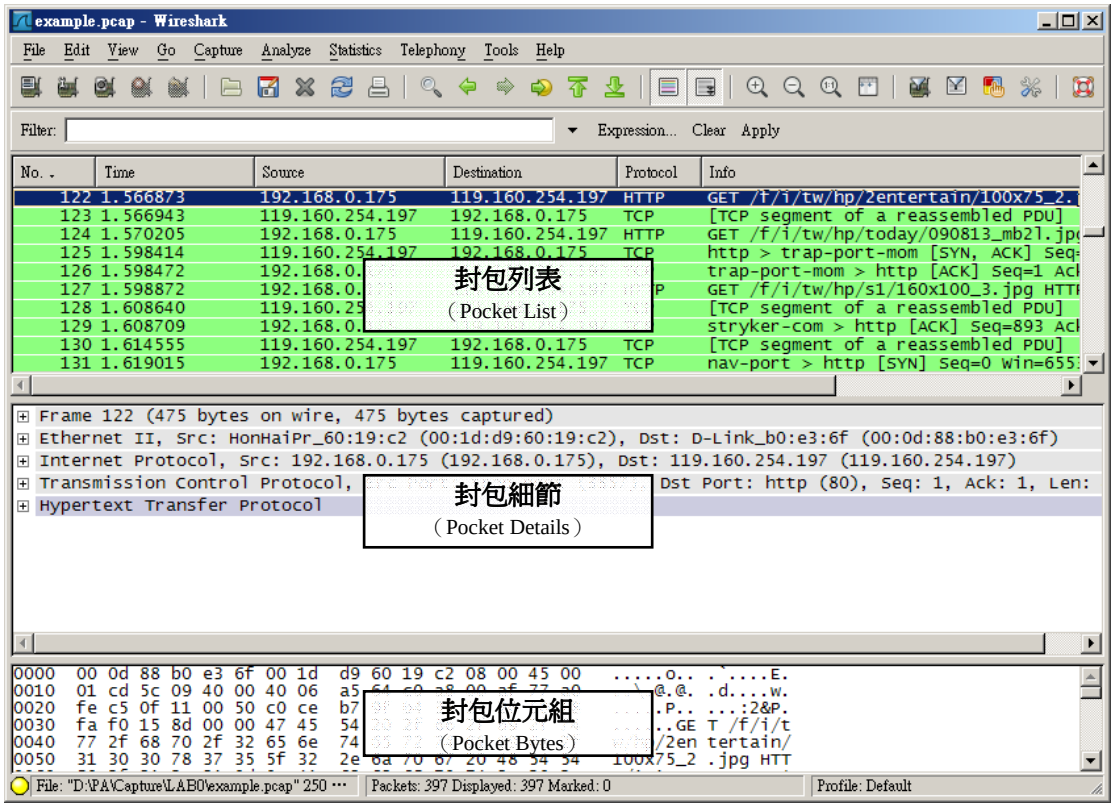
選擇「Edit」→「Preferences」



您可以在「User Interface」的「Layout」選擇您喜歡的封包檢視方式
然後按下「Apply」和「OK」來變更您的檢視方式

檢視封包資訊

如果您需要同步的與本講義做內容對照，您可以使用本章提供之範例（本範例可以在 \Capture\1-1_BASE\example.pcap 取得）。



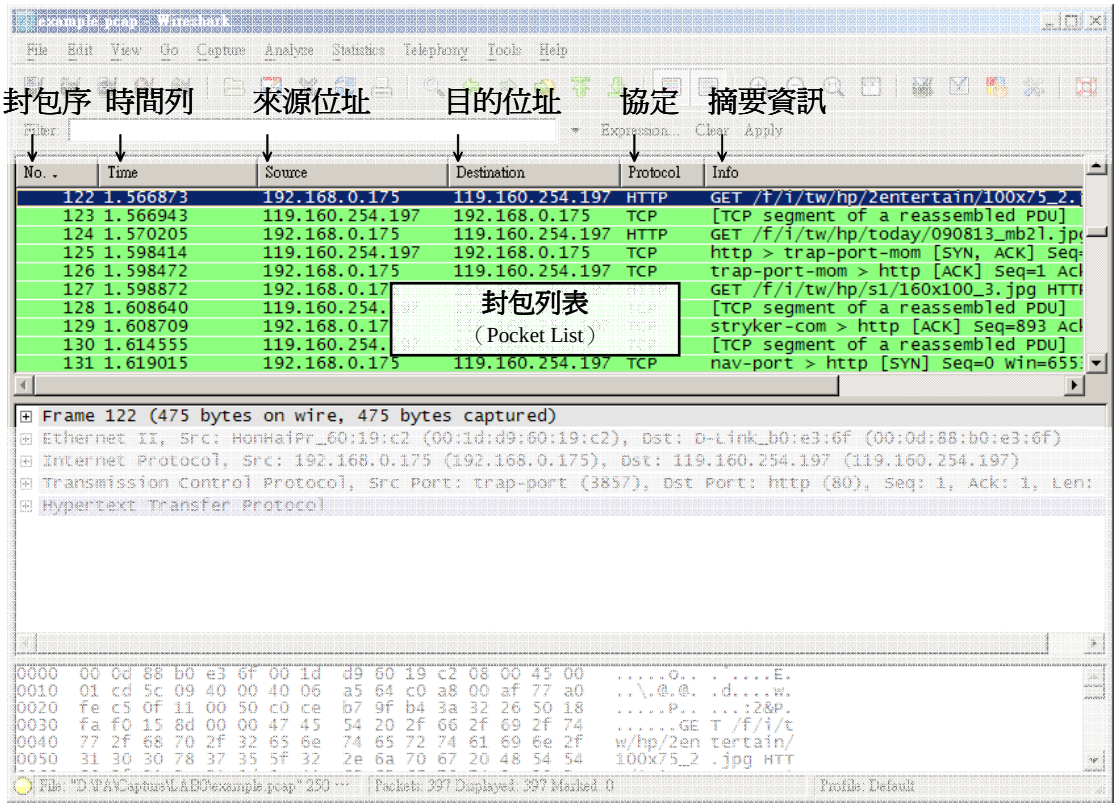
上圖是一個正常的 Wireshark 擷取封包畫面，通常我們就可以在此檢視到所有資訊了。

封包列表中，列出了所有您開始擷取封包到停止擷取中間的封包，一般我們只要點選封包列表（Pocket List）中的封包，封包細節（Pocket Details）與封包位元組（Pocket Bytes）就會跟著改變。

當然我們就可以針對擷取到的內容，來分析是否有狀況發生。

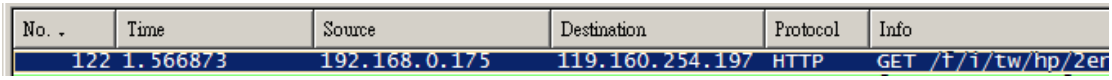
封包列表（**Pocket List**）

如果您已經正常擷取到封包，那您現在一定看見在封包列表（Pocket List）有許多封包，您可以立即觀察到封包的特性：



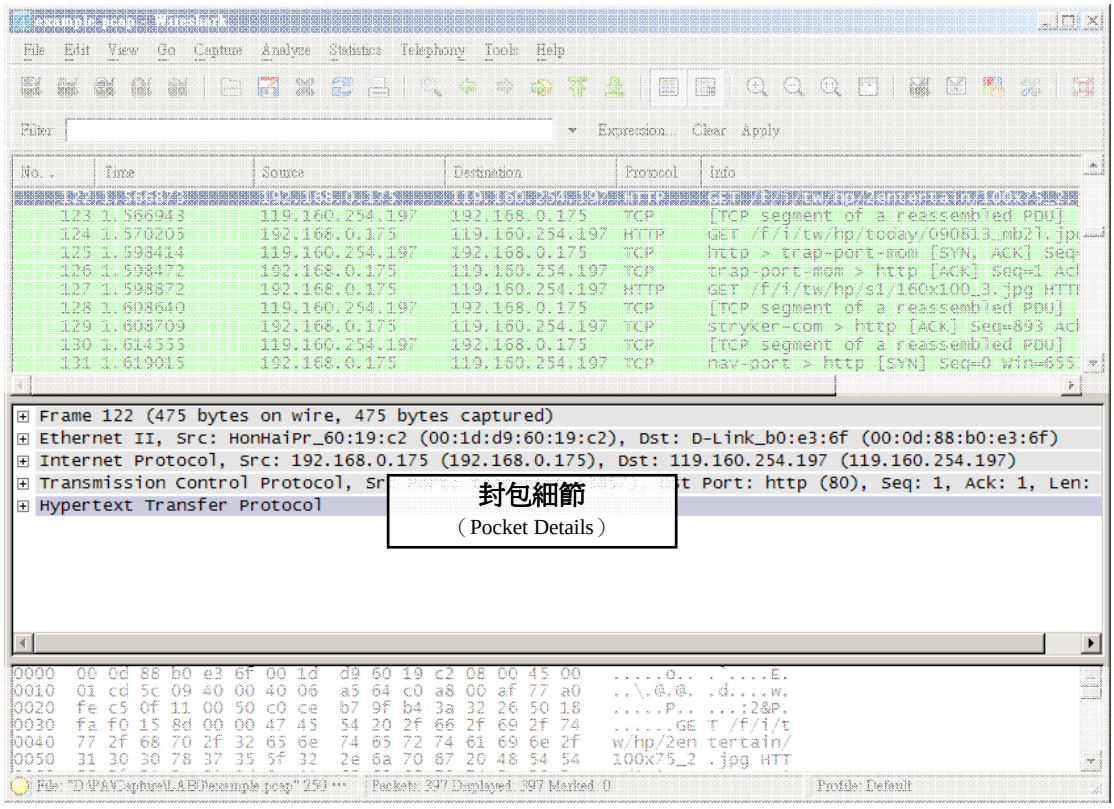
No. (封包序)：接受到封包的順序，通常爲流水號，每次從 1 開始。
Time (時間列)：指從開始擷取封包的時間到「這個」封包的時間。
Source (來源位址)：封包發送端（IP）
Destination (目的位址)：封包接收端（IP）
Protocol (協定)：指該封包用什麼通訊協定
Info (摘要資訊)：簡易的封包資訊摘要

範例：

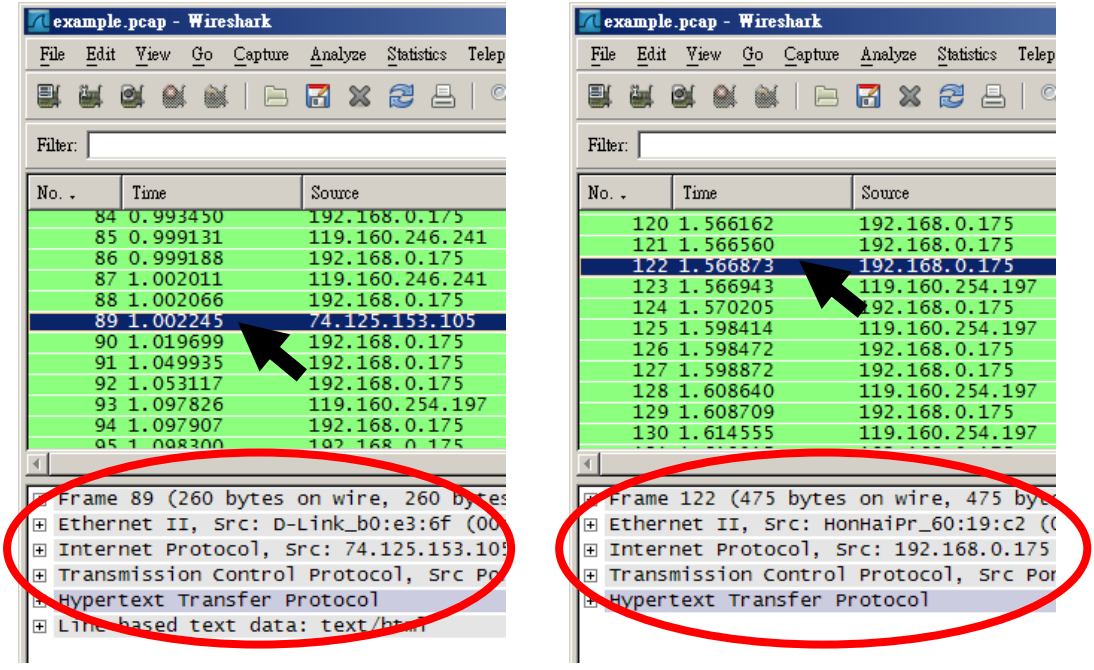


上面表示這個封包順序是第 122 個，是在第 1.566873 秒擷取到的，封包來源是 192.168.0.175 ，目的地是 119.160.245.197 ，使用 HTTP 通訊協定，欄位 info 告訴我們，是一個網頁的 GET 動作 (網頁瀏覽器)。

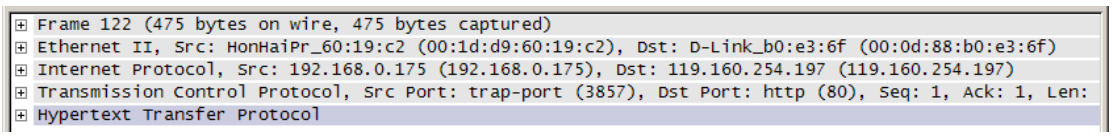
封包細節（Pocket Details）



封包細節裡面的內容會隨著您所選取的封包而改變，當您點選封包列表的任一個封包，封包細節內的資訊會立即更新爲該封包的細節。



接下來我們針對封包細節來簡單說明一下；請注意，不同協定或是擷取方式、媒介，顯示出來的內容會有所不同，下列爲**封包編號 122 的封包細節**：



[+] Frame 122 (475 bytes on wire, 475 bytes captured)

這裡相當於實體層（Physical Layer）的資訊，表示是第 122 個 Frame，大小是 475 bytes；您可以按 [+] 展開更詳細的內容。

[+] Ethernet II, Src: HonHaiPr_60:19:c2 (00:1d:d9:60:19:c2), Dst: D-Link_b0:e3:6f (00:0d:88:b0:e3:6f)

這裡相當於資料鏈結層（Data Link Layer），說明這是以乙太網路 Ethernet V2 爲協定，並說明來源端位置（ 廠牌_序號、Mac Address)以及目的端位置（ 廠牌_序號、Mac Address)；您可以按 [+] 展開更詳細的內容。

[+] Internet Protocol, Src: 192.168.0.175 (192.168.0.175), Dst: 119.160.254.197 (119.160.254.197)

這裡相當於網路層（Network Layer），目前顯示的是 IP (Internet Protocol) 協定的表頭（Header)，此列說明來源端以及目的端 IP，如想看更詳細的資訊內容，您可以按 [+] 展開更詳細的內容。

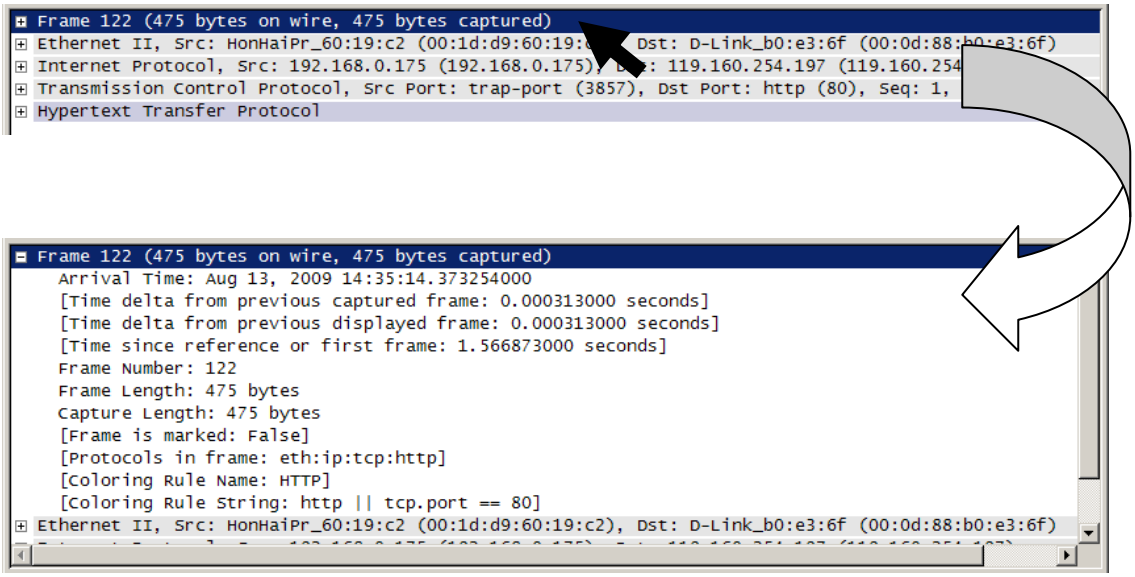
[+] Transmission Control Protocol, Src Port: trap-port (3857), Dst Port: http (80), Seq: 1, Ack: 1, Len: 421

這裡相當於傳輸層（Transport Layer)，目前顯示的是 TCP (Transmission Control Protocol) 協定的資訊，此列說明來源端以及目的端所使用的 Port、Ack 和長度…等等資訊；您可以按 [+] 展開更詳細的內容。

[+] Hypertext Transfer Protocol

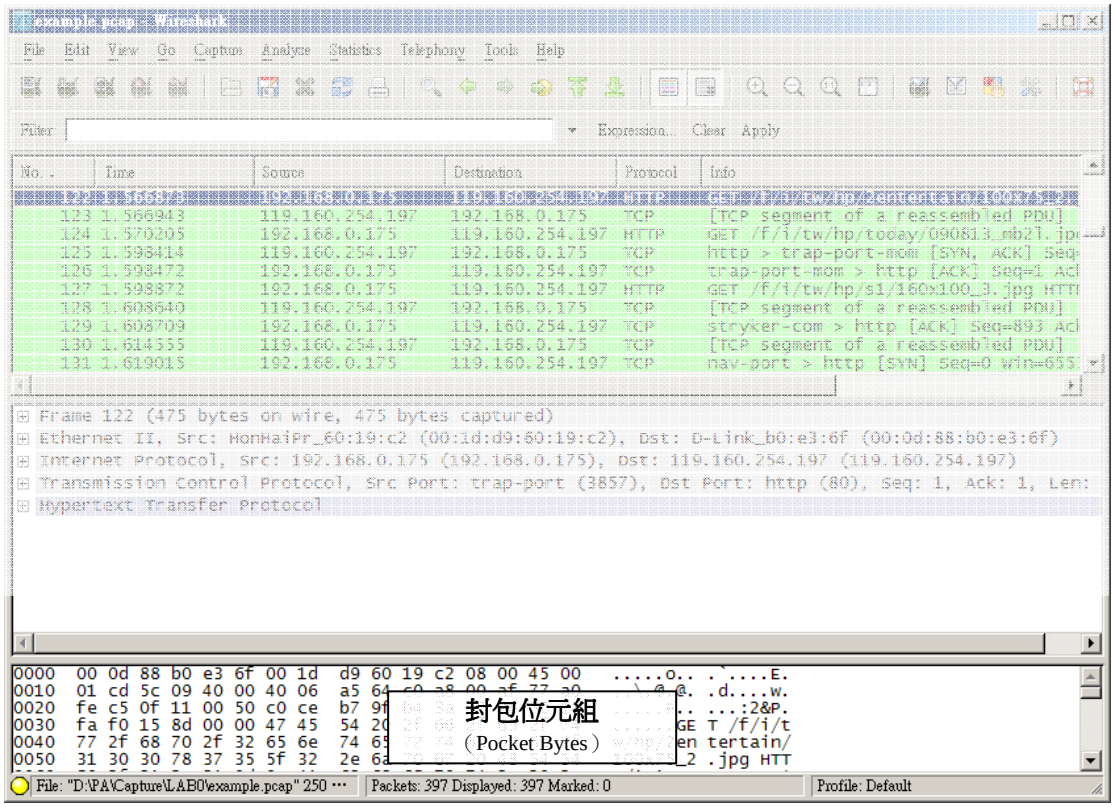
這裡相當於應用層（Application Layer)，目前顯示的是使用 HTTP (Hypertext Transfer Protocol) 協定的內容；您可以按 [+] 展開看到整個內容。

如果您覺得看的資訊不夠詳細，想更了解資訊更細部的資訊，可以選取封包細節，並對有興趣了解的內容部分按「＋」來展開更詳細的內容。

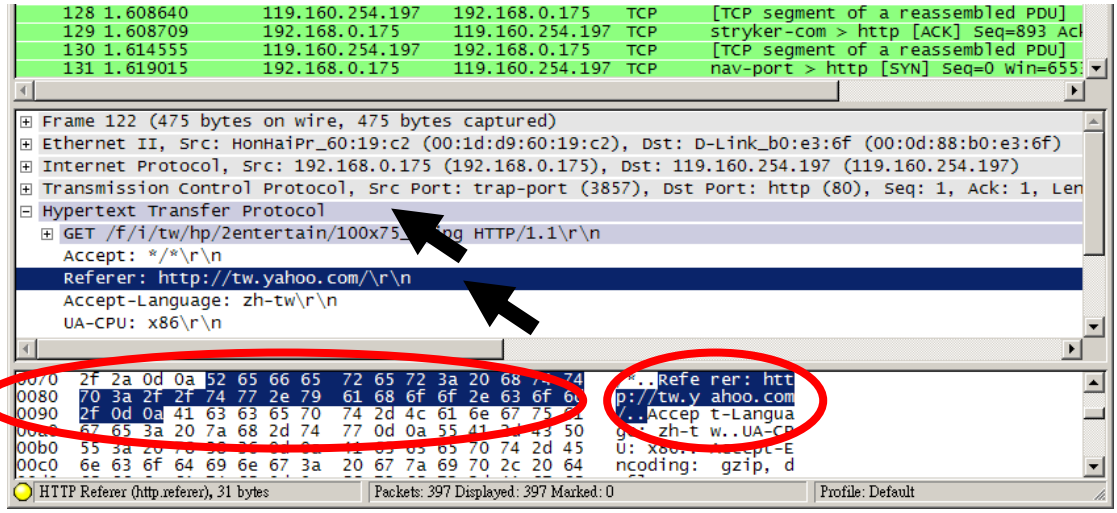


封包位元組（Pocket Bytes）

這是整個封包的 16bit 檢視與明碼檢視，您可以經由選擇封包細節的部份內容，自動幫您在這部份選出對應的內容。



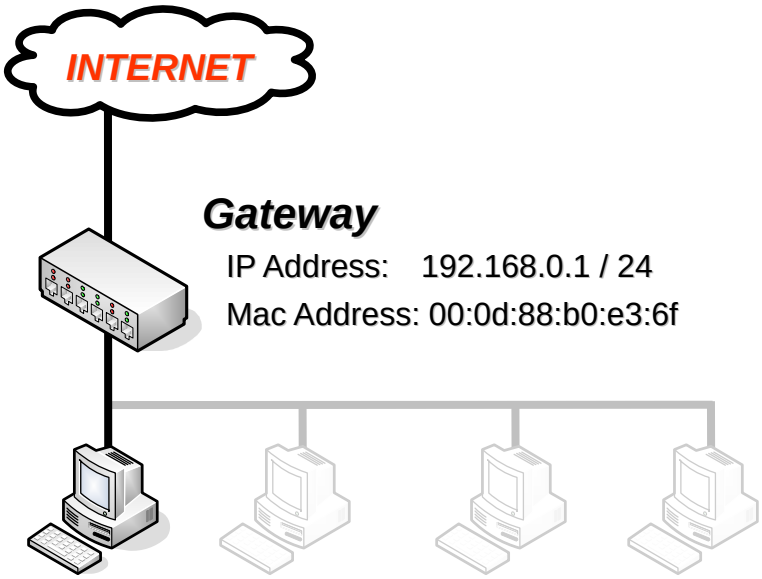
您也可以直接點選您有興趣的內容，Wireshark 會自動幫您對應出封包細節的內容：



PROTOCOL ANALYSIS

Filter With WIRESHARK

講義環境設定



Gateway

IP Address: 192.168.0.1 / 24

Mac Address: 00:0d:88:b0:e3:6f

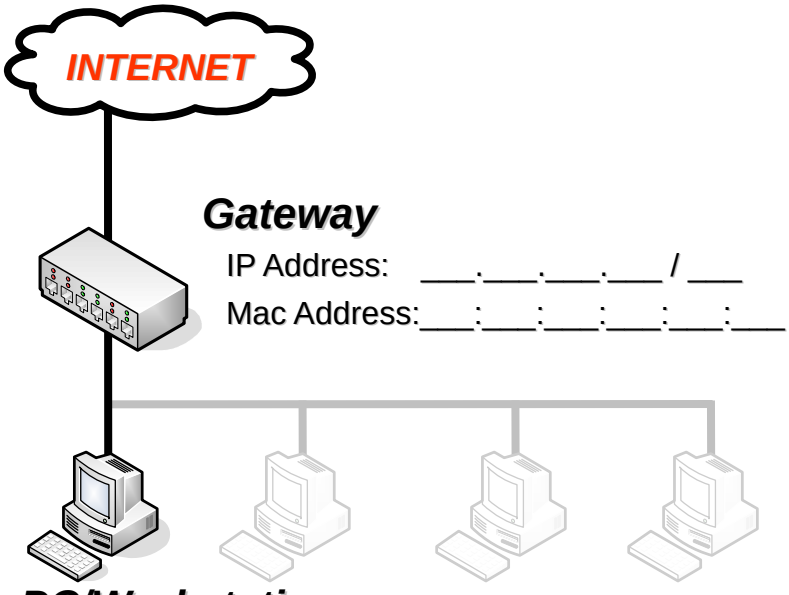
PC/Workstation

IP Address: 192.168.0.175 / 24

Mac Address: 00:1d:d9:60:19:c2

Gateway: 192.168.0.1

我的環境設定



Gateway

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

PC/Workstation

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

過濾封包 (Filter)

您現在已經會擷取網路封包了，且確實整個擷取的過程非常的簡單；但是如果您不是在實驗室的環境裡，在一般正常的網路環境中，並依照現在網路使用的頻率來看，在您擷取封包一段時間後，您將會發現擷取到的封包數量會超出您的想像，上千甚至上萬都是很正常的。

想想看五千個封包中，找出您想要的其中幾個封包該如何找？一個一個找？那絕對會很花您的時間和眼力的，聰明的您一定不會想這樣做吧！

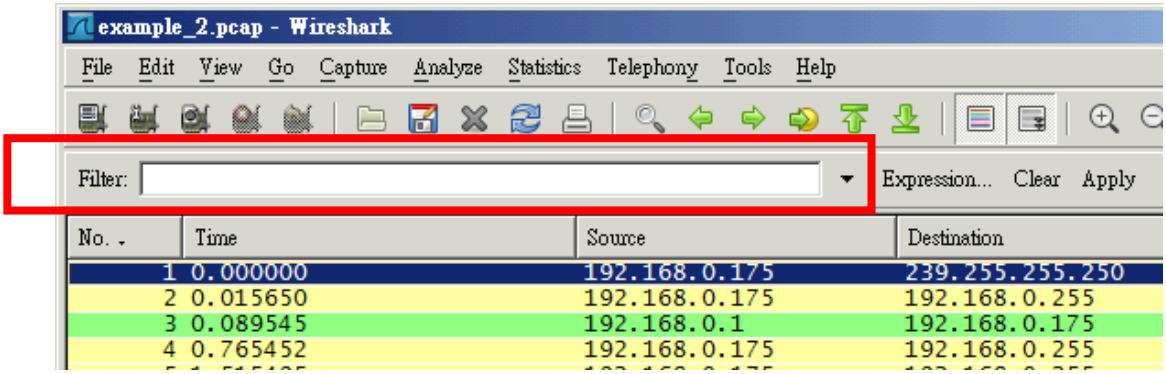
沒錯，我們要把專注力用在封包的分析上，而不是花時間在尋找我們要的封包；所以如何快速的找到我們要的封包，變成一個重要的課題！唯有快速找到我們要的封包，才能讓我們在分析網路狀況事半功倍！

當然，您一定想到「過濾」，用一些條件來過濾出我們所要的封包，排除我們不需要的封包，接下來我們就是要讓各位知道如何過濾想要的封包。

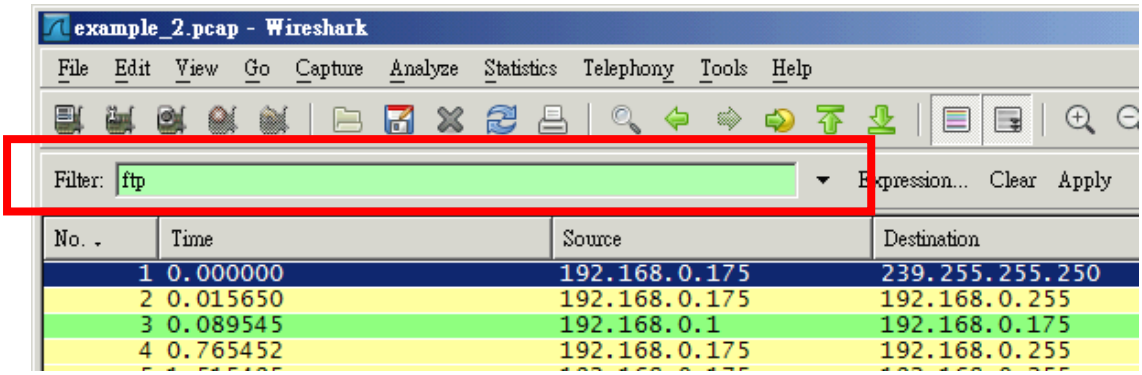
您可以擷取自己目前的網路環境並實際執行過濾條件（請最少擷取三分鐘到五分鐘），或是如果您需要同步的與本講義做內容對照，您可以開啓本章所提供之範例（本範例可以在 \Capture\1-1_BASE\example_2.pcap 取得）。

在何處過濾封包？

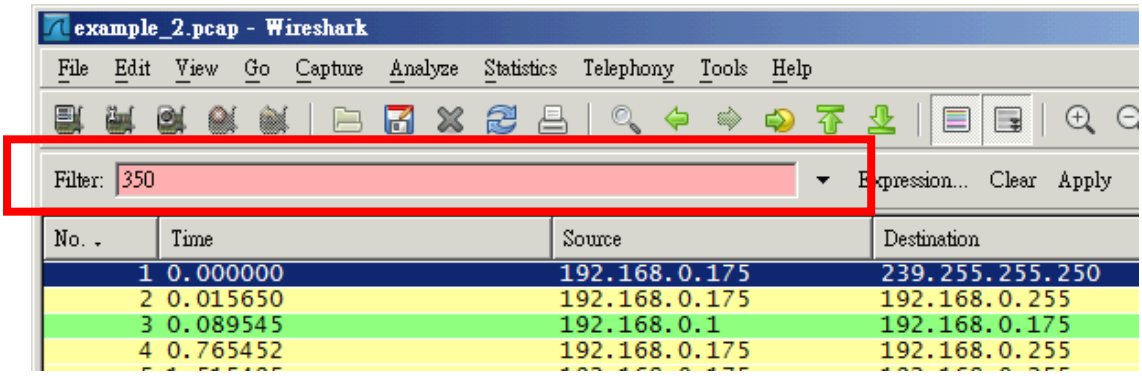
我們在前篇已經稍微提及到封包的過濾位置，如果您尚未下達過過濾條件，那麼在過濾欄位背景的顯示顏色將爲「**白色**」。



如果您下達過濾條件，且也爲正確條件，那麼在過濾欄位背景的顯示顏色將爲「**綠色**」。



如果您下達過濾條件，是錯誤或條件不完整時，那麼在過濾欄位背景的顯示顏色將爲「**紅色**」。

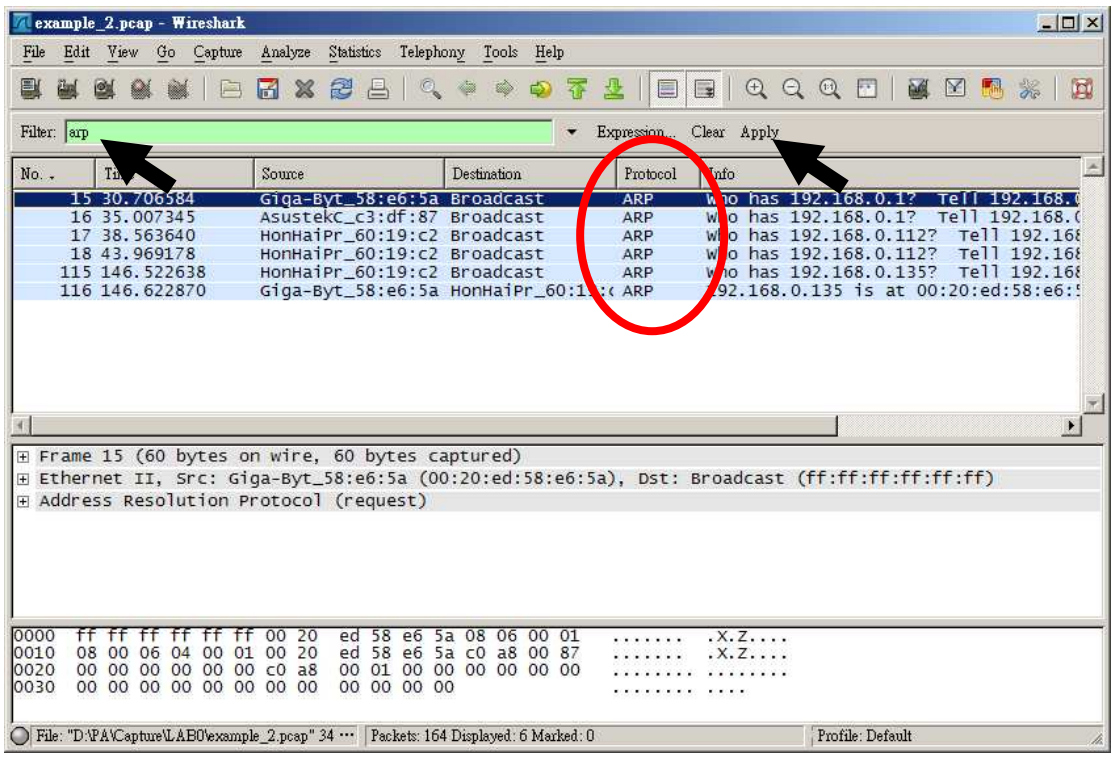


沒錯，過濾很簡單，只要在過濾欄位輸入您要的條件就可以了，但是要注意的是，當您在未輸入完整時過濾欄位背景的顏色都將會是紅色的，待您都輸入完畢後，如果 Wireshark 可以辨認出您所輸入的條件，過濾欄位背景的顏色就會變成綠色了。

別急，接下來就要教您如何過濾！

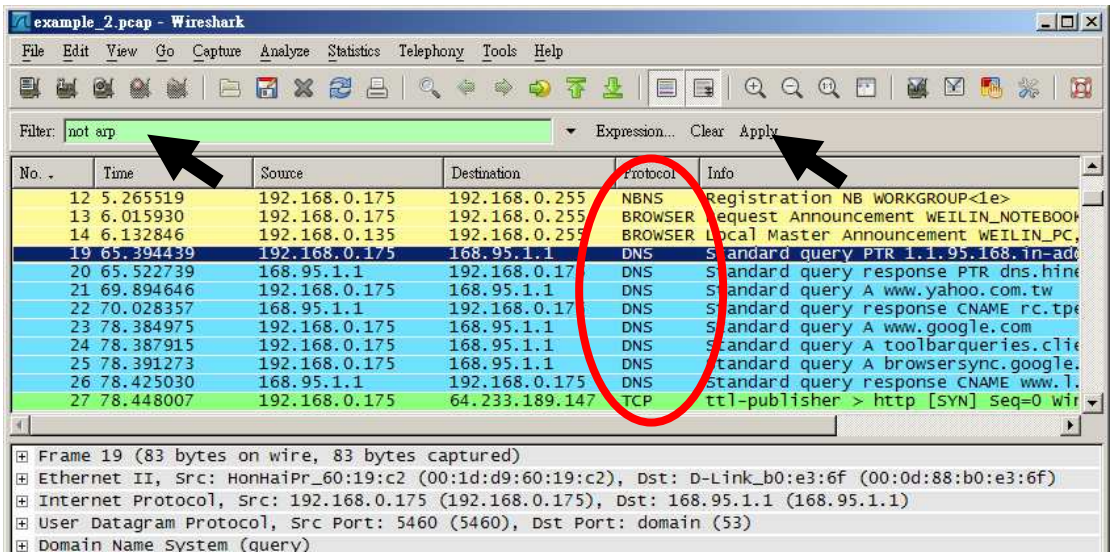
過濾出指定的協定 (ARP)

我們這裡示範來檢視 ARP 的協定封包，您可以在 Wireshark 的 Filter 裡輸入過濾條件「arp」後，按下「Apply」即可看見所有 ARP 協定封包。



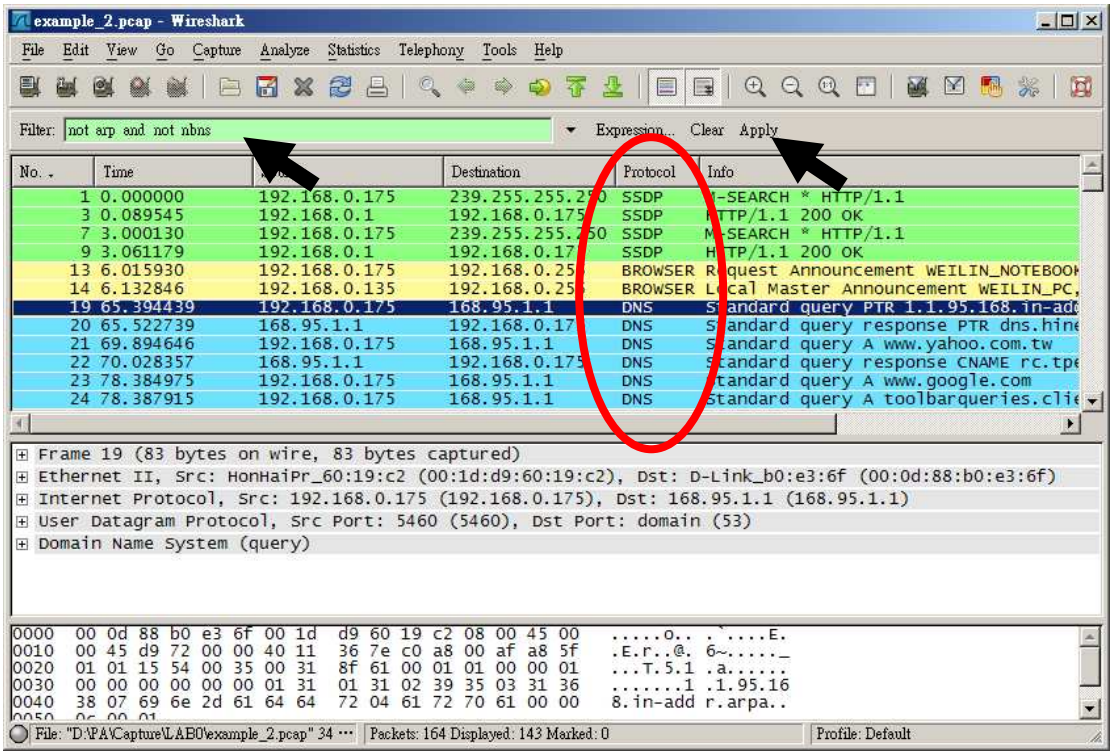
過濾掉指定的協定 (ARP)

如果您***不想看 ARP*** 的協定封包，可以在 Wireshark 的 Filter 裡輸入過濾條件「not　arp」後，按下「Apply」即可看見所有非 ARP 的協定封包。

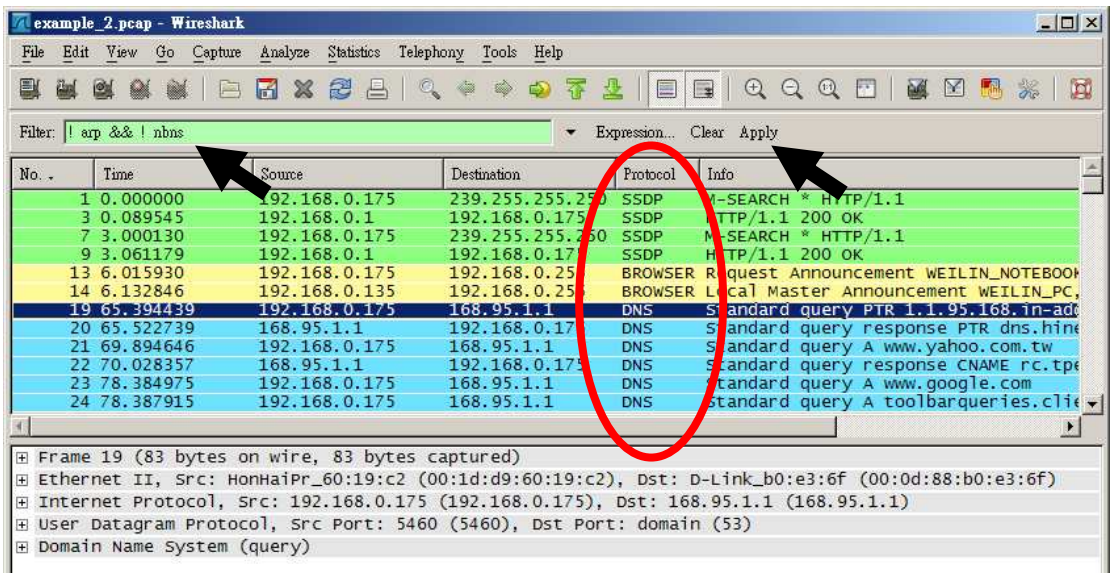


過濾掉多個指定協定 (ARP 與 nbns)

如果您*不想看* ***ARP*** *和* ***nbns*** 的協定封包，可以在 Wireshark 的 Filter 裡輸入過濾條件「not arp and not nbns」後，按下「Apply」即可看見所有非 ARP 和 NBNS 的協定封包。

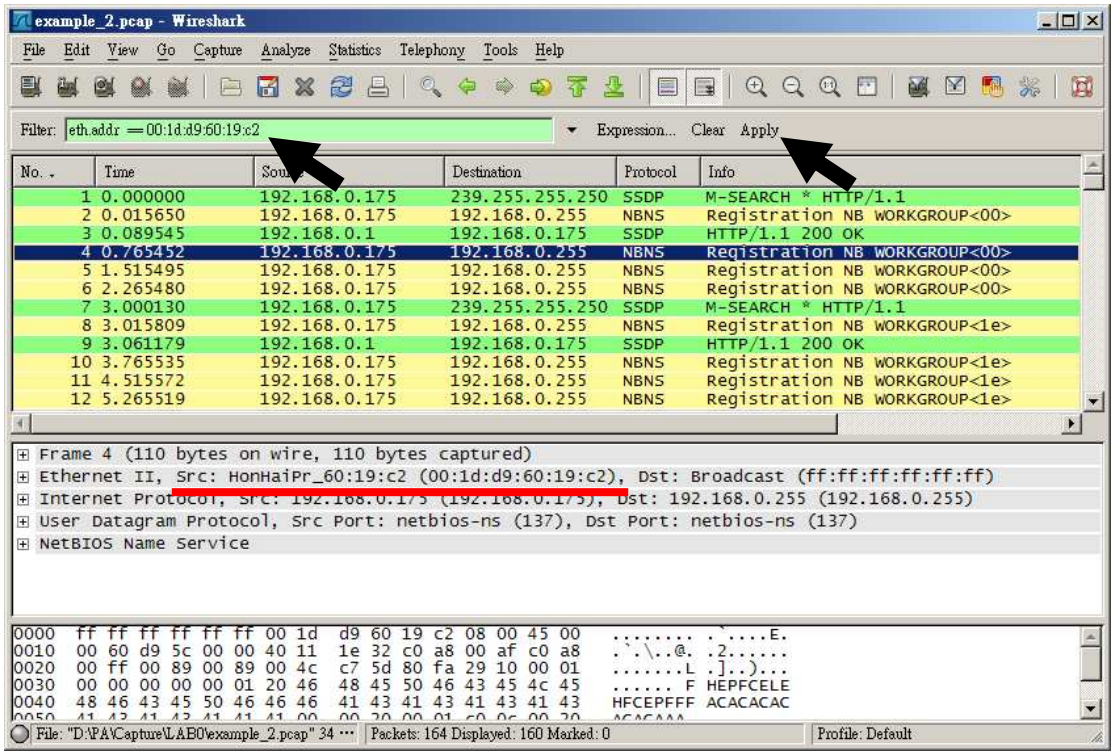


當然您如果用符號來輸入過濾條件「! arp && ! nbns」，過濾出來的封包會是一樣的！

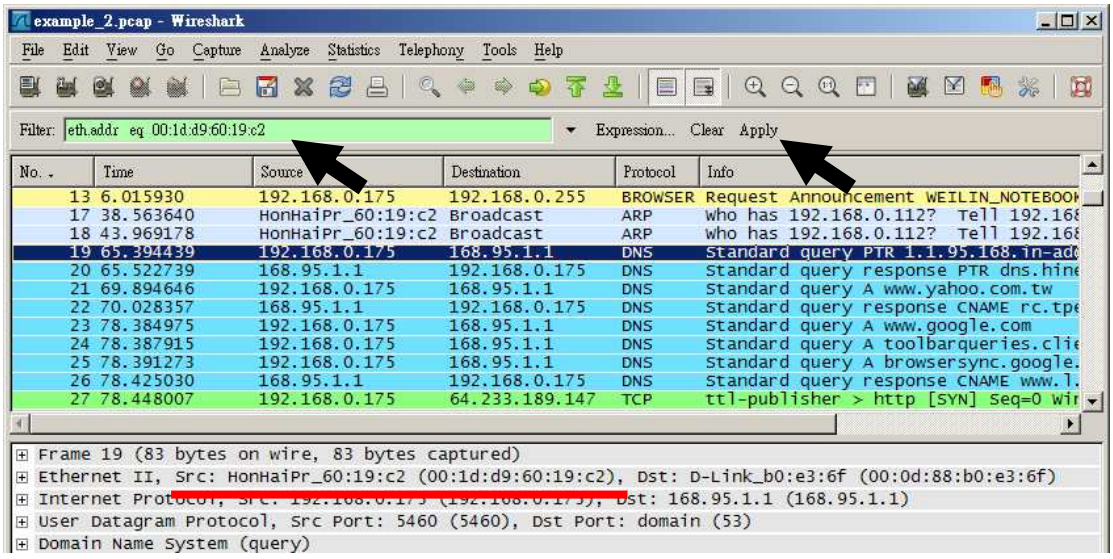


以 **Mac Address** 過封包

您可以用網路卡的 Mac Address 來過濾封包，我們找出屬於自己網卡（Mac Address）的封包，可以在 Wireshark 的 Filter 裡輸入過濾條件「eth.addr == 00:1d:d9:60:19:c2 」後，按下「Apply」即可看見所有屬於 00:1d:d9:60:19:c2 的封包。

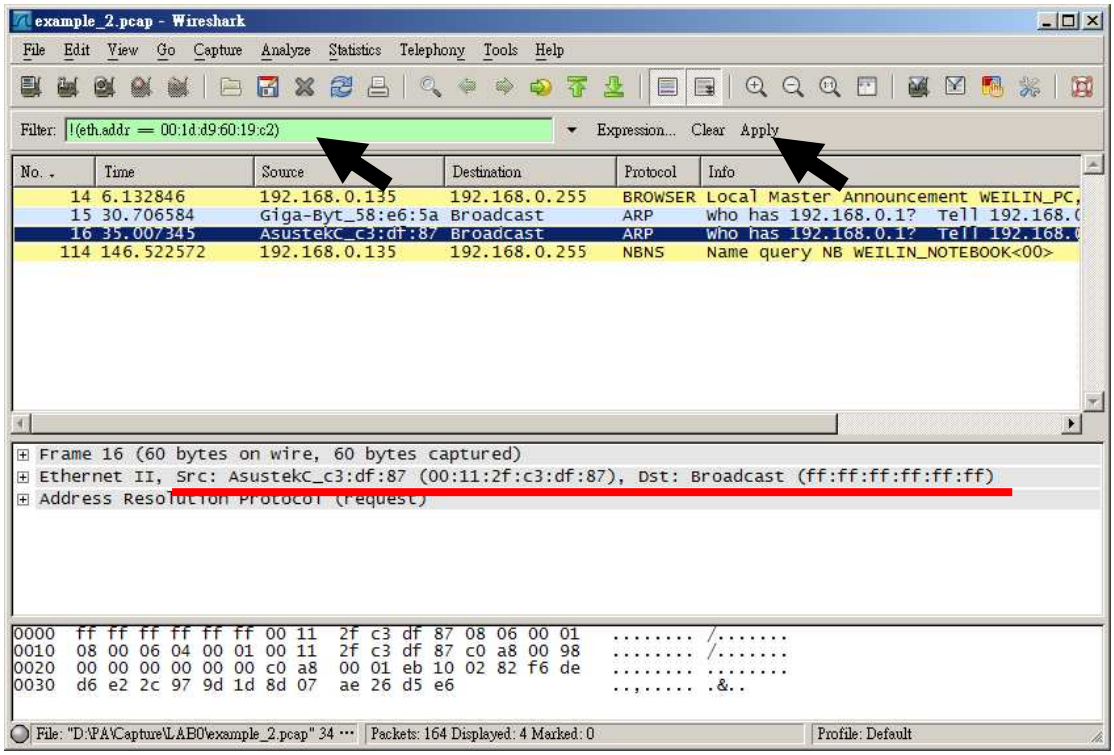


如果您不習慣用符號來下過濾條件，以「eth.addr eq 00:1d:d9:60:19:c2」過濾出來的封包會是一樣的！

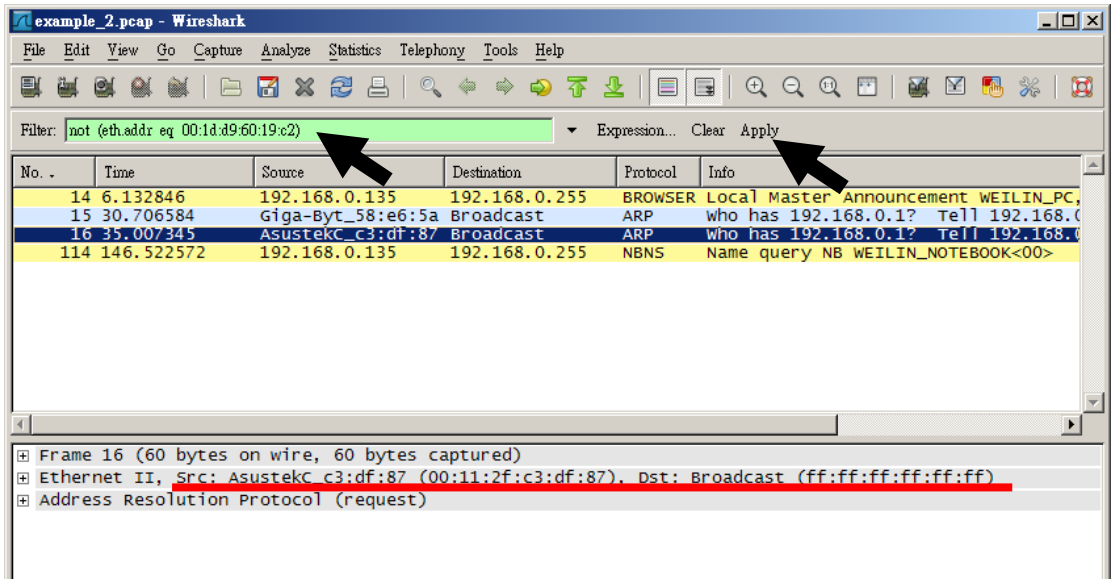


過濾掉自己 Mac Address 的封包

過濾掉非自己網卡的封包，可以在 Wireshark 的 Filter 裡輸入過濾條件「!(eth.addr == 00:1d:d9:60:19:c2) 」後，按下「Apply」即可看見所有非 00:1d:d9:60:19:c2 的封包。

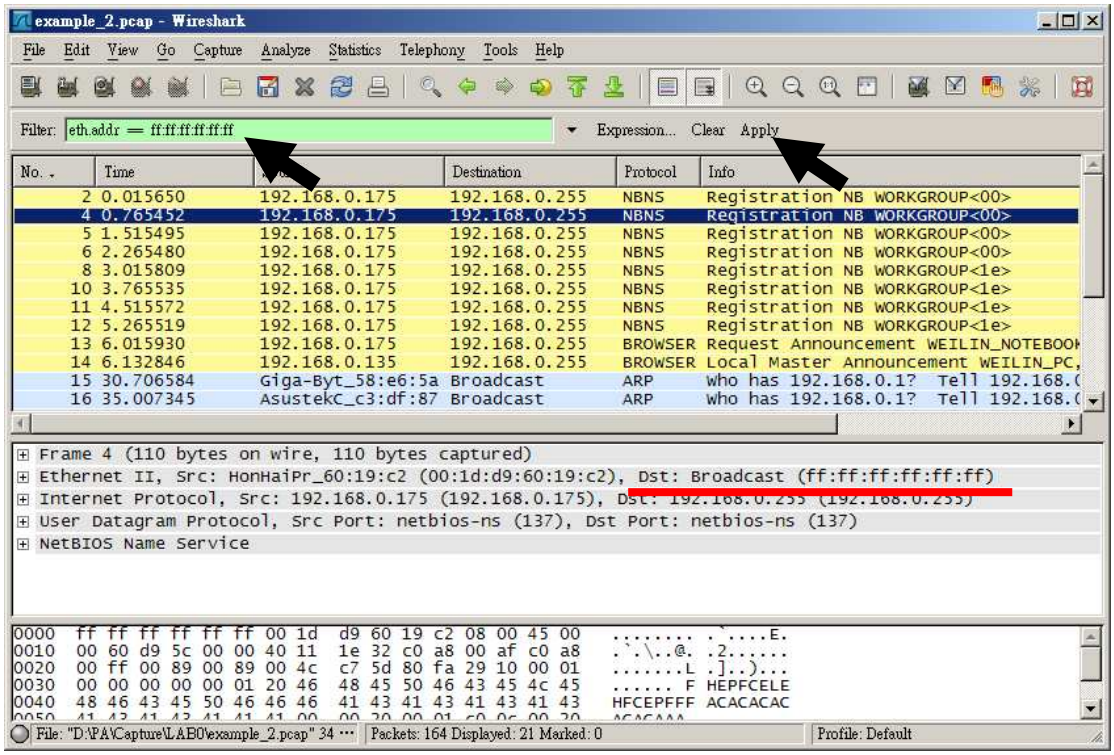


如果您不以符號來下過濾條件，用「not (eth.addr eq 00:1d:d9:60:19:c2)」過濾出來的封包會是一樣的！



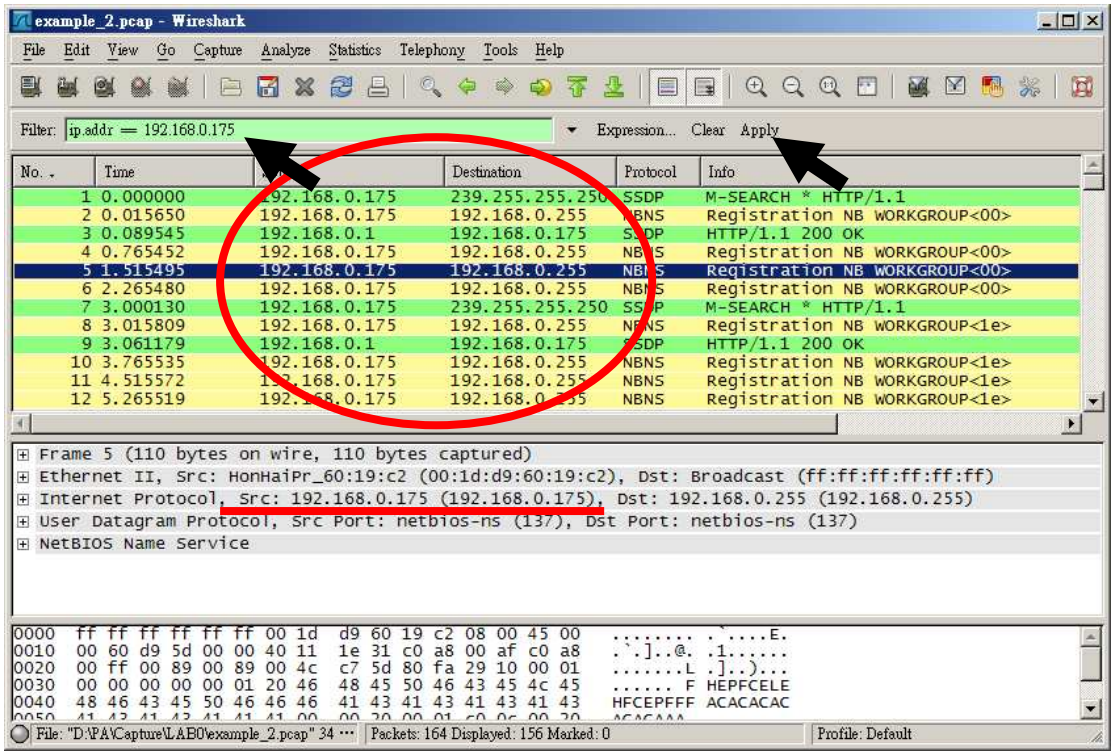
找出所有的廣播封包

廣播封包其實就是網卡位置爲 ff:ff:ff:ff:ff:ff，您可以在 Wireshark 的 Filter 裡輸入過濾條件「eth.addr == ff:ff:ff:ff:ff:ff」後，按下「Apply」即可看見所有的廣播封包。



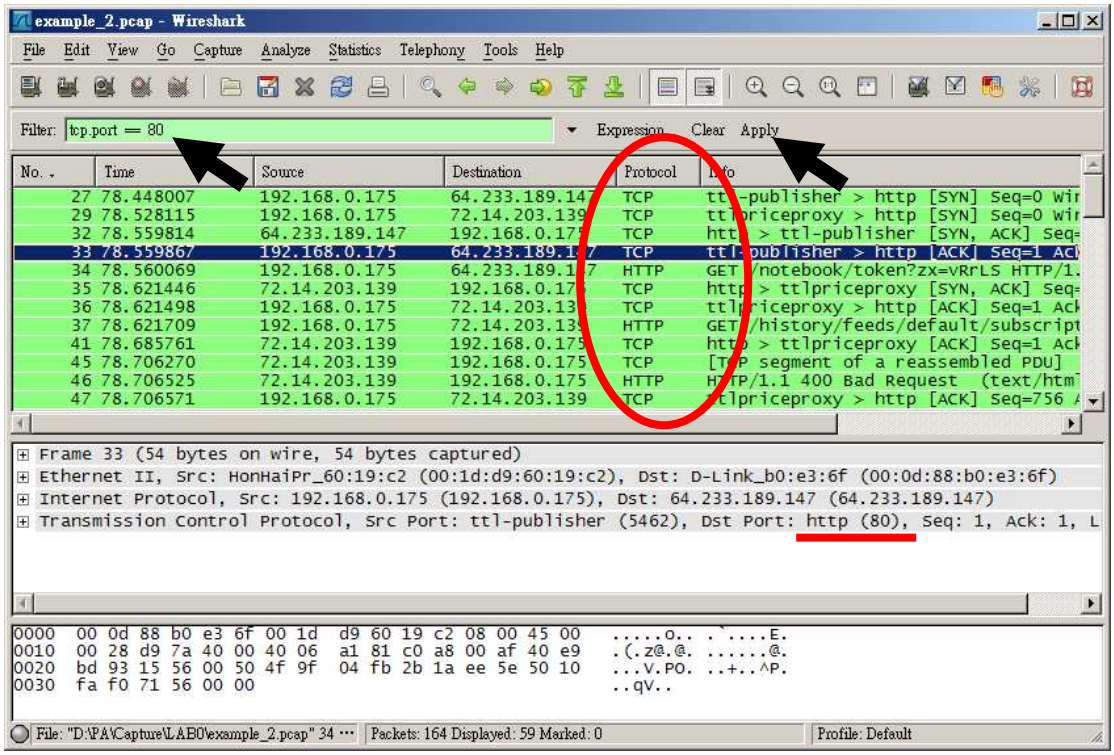
找出有關自己 IP 的封包

找出有關於自己 IP 發出的封包（ 發出或是接收 ），您可以在 Wireshark 的 Filter 裡輸入過濾條件「ip.addr == 192.168.0.175」後，按下「Apply」即可看見所有的自己 IP 有關的封包。



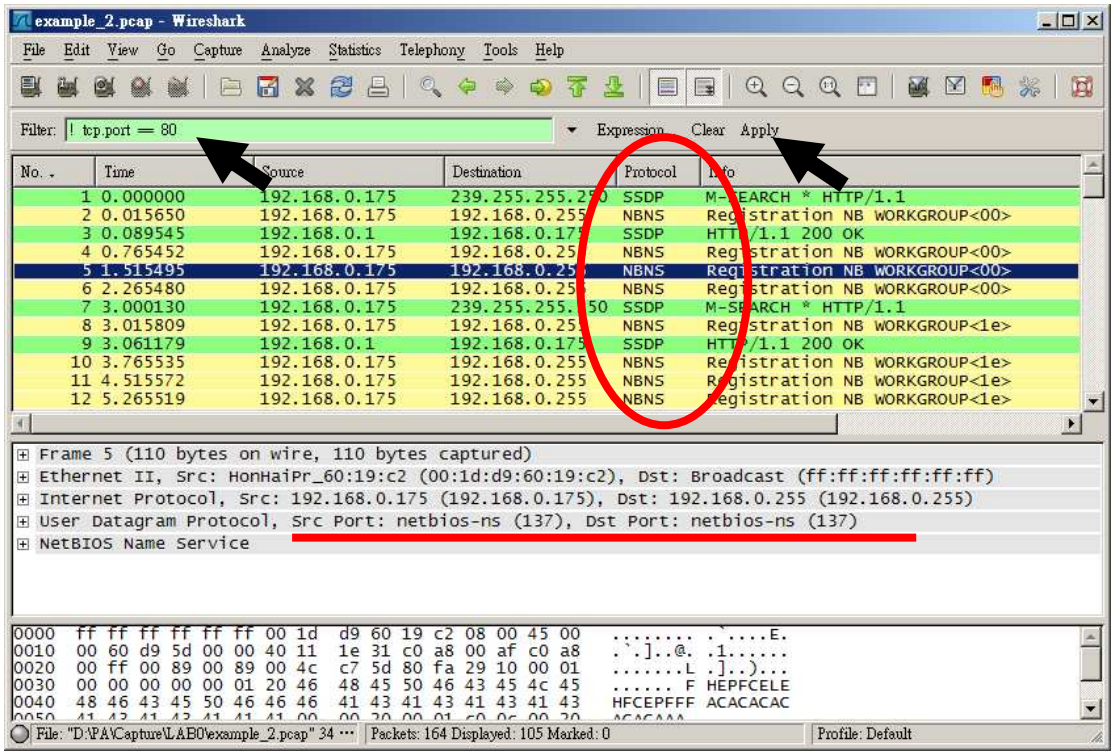
找出 Port 爲 80 的封包

要找出 Port 爲 80 的封包也很簡單，不過您要知道，您要找的是 tcp 還是 udp，我們範例是找出 tcp 的封包，所以可以在 Wireshark 的 Filter 裡輸入過濾條件「tcp.port == 80」後，按下「Apply」即可看見所有 Port 爲 80 的封包。



過濾掉非 Port 爲 80 的封包

現在要找出不是 Port 爲 80 的封包，所以可以在 Wireshark 的 Filter 裡輸入過濾條件「！ tcp.port == 80」後，按下「Apply」即可看見所有 Port 爲 80 的封包。



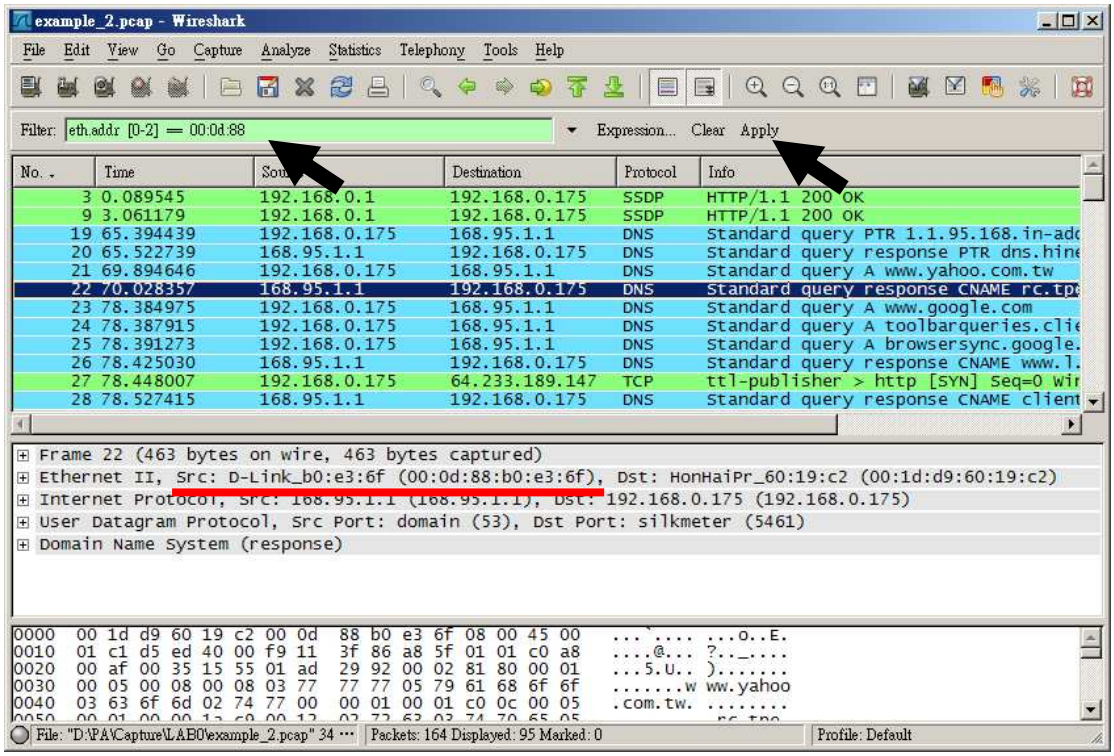
找出封包爲 D-Link 品牌網卡的封包

要找出爲 D-Link 品牌網卡的封包並不難，只是您要先知道網路卡 Mac Address 的編碼方式：

00 : 0D : 88 : B0 : E3 : 6F

廠商編號　　流水號

所以 D-Link 的廠商編號是 00:0D:88，我們只要找 Mac Address 的廠商編號爲 00:0D:88，只要是用同品牌的網路卡並正在使用中，就會被我們擷取到封包，您可以在 Wireshark 的 Filter 裡輸入過濾條件「eth.addr [0-2] == 00:0d:88」後，按下「Apply」即可看見。



課堂練習：

01.請找出所有 UDP 的封包

02.請找出所有有關 DNS 的封包

03.請找出所有有關 DNS 和 ICMP 的封包

04.請找出所有自己 IP 發出去的封包

05.請找出所有非自己 IP 的封包

06.請找出所有 UDP 80 Port 的封包

07.請找出所有 port 爲 21 和 20 的封包

08.請找出有關自己 IP 的 TCP Port 80 的封包

09.請找出由自己發出的廣播封包

10.請找出是 Gateway 的封包，但是不是廣播的封包

11.請找出是自己發出的封包，但是目的地不是給 168.95.1.1 的封包

12.請找出所有非自己發出，也非 Gateway 發出的封包

13.請找出所有來源 IP 的 80 Port 封包

14.請找出 TCP Port 大於 1000 的封包

15.請找出 沒有使用 IP 協定的封包

16.請找出 ARP 的查詢的封包，不要回覆的封包

17.請找出 ICMP 的回應封包

18.請找出所有發給自己的封包，且 IP 封包長度超過 1000 bytes 的封包

19.請找出本網段所有的封包

20.請找出有關 DNS 查詢 www.google.com 的查詢往來封包

21.請找出所有 D-Link 網卡接收到的封包

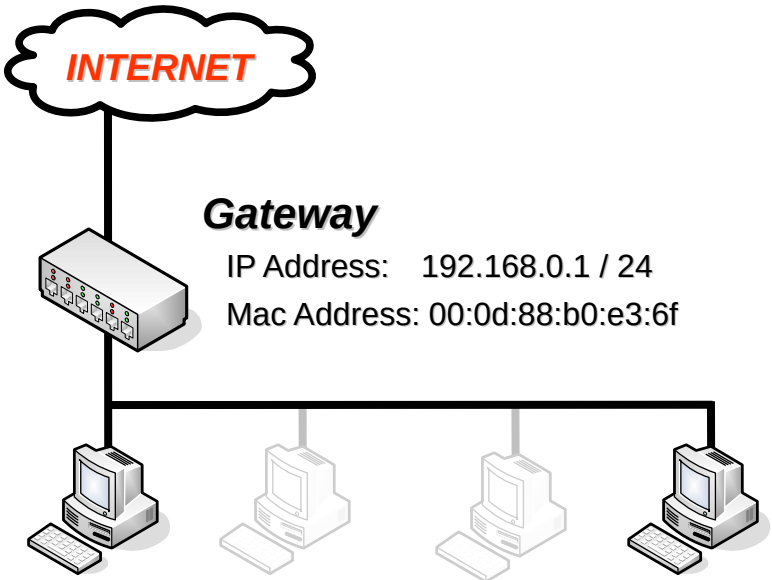
22.請找出非本網段的廣播封包

心得筆記：

PROTOCOL ANALYSIS

1-2-1 : PING

講義環境設定



Gateway

IP Address: 192.168.0.1 / 24

Mac Address: 00:0d:88:b0:e3:6f

PC/Workstation

IP Address: 192.168.0.175 / 24

Mac Address: 00:1d:d9:60:19:c2

Gateway: 192.168.0.1

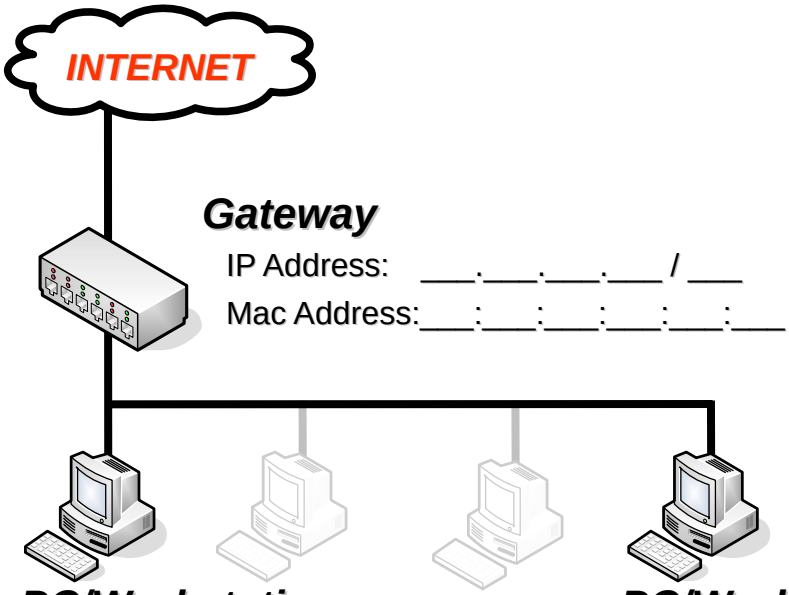
PC/Workstation(Other)

IP Address: 192.168.0.135 / 24

Mac Address: 00:20:ed:58:e6:5a

Gateway: 192.168.0.1

我的環境設定



Gateway

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

PC/Workstation

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

PC/Workstation(Other)

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

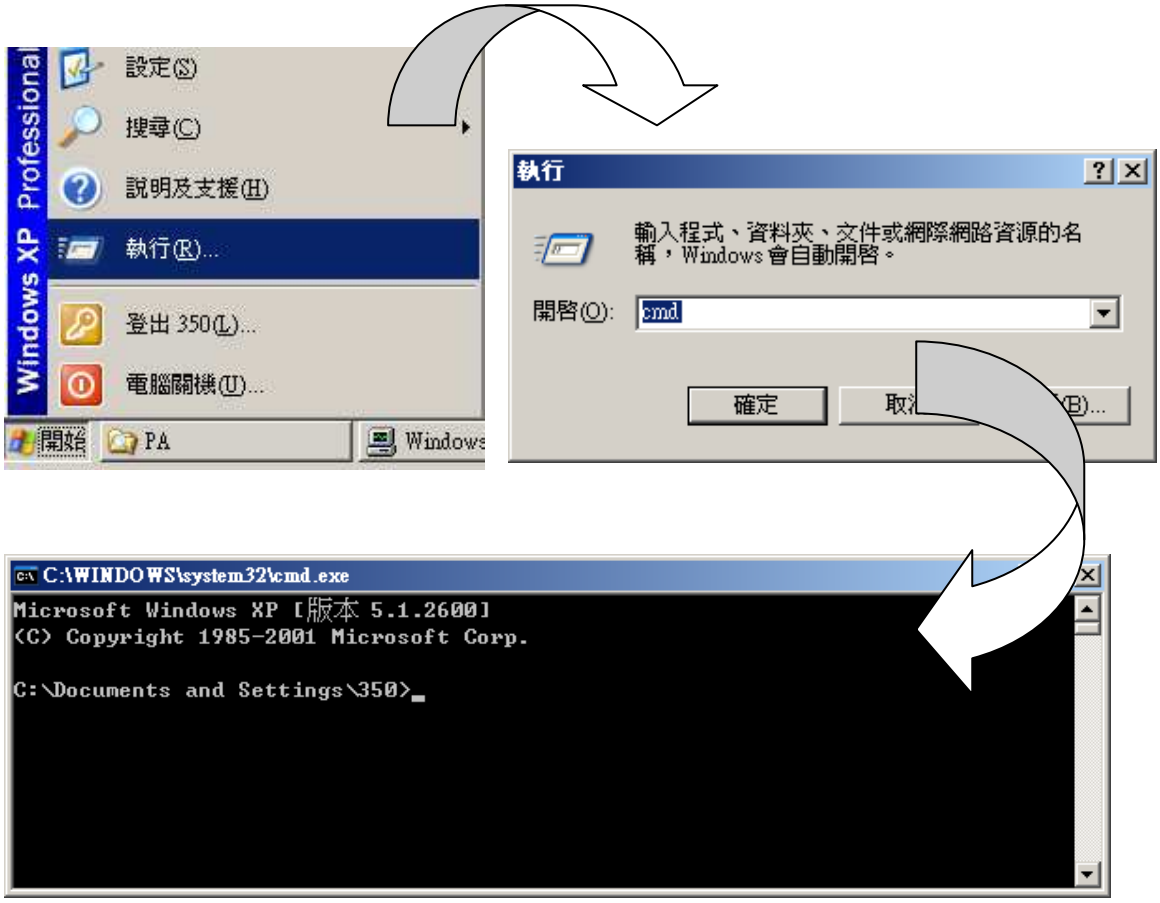
PING 到網路世界

剛進入網路世界探險的各位，除了從書本上獲得網路原理的理論和知識外，最重要的是如何印證書本上的種種；所以，我們從最簡單的 PING 來帶各位進入網路叢林中。

檢視封包的第一步，當然是開啓您的 Wireshark，並準備好您的網路擷取狀態；如果您還未了解如何啓動 Wireshark 擷取方式，請您回到前面回顧一下！

請現在啓動 Wireshark 並開始擷取封包

請開啓您的文字模式 (以 Windows 爲例)，所以請執行「開始」→「執行」，輸入「cmd」，按下確定。



PING to Gateway

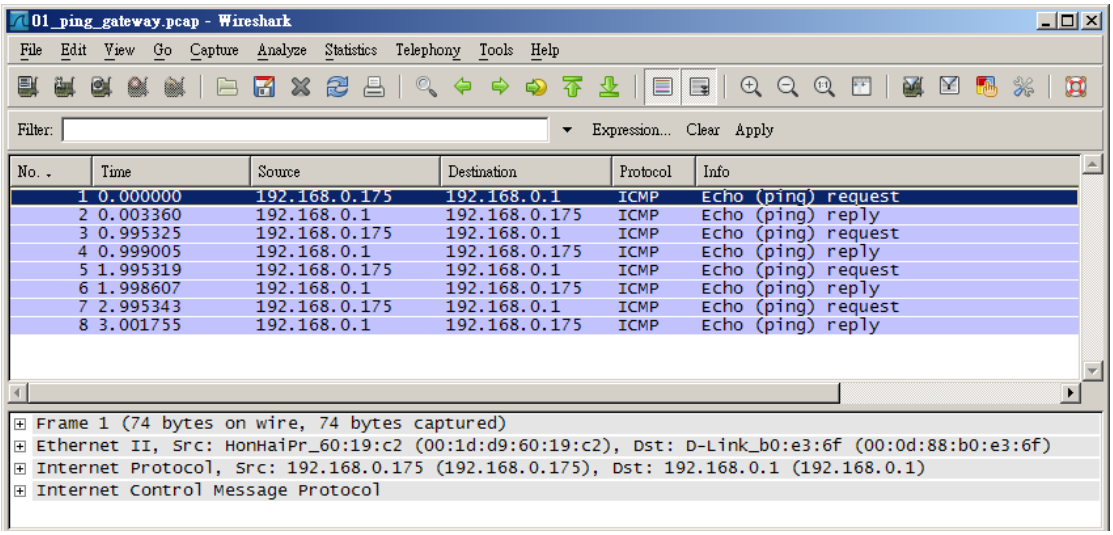
我們首先來 PING 我們的 Gateway，藉由 Gateway 給我們的回應封包，來檢查網路狀態以及回覆資訊。

請在文字模式中，按下指令「ping 192.168.0.1」，由於我們現在網路都是通的，所以您將會在文字模式看到下面這個訊息回應：

```
C:\Documents and Settings\350>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 3ms

C:\Documents and Settings\350>
```

請停止您 Wireshark 的擷取，開始觀察封包資訊

您已經可以在 Wireshark 裡看見許多關於 ICMP 的封包資訊（ 本範例可以在 \Capture\1-2-1_PING\01_ping_gateway.pcap 取得 ）：



我們現在有了 Windows 的 Ping 給我們帶來了 Gateway 的訊息，以及我們擷取到「真正」網路世界裡面的封包了，現在開始來一窺網路的真實世界囉！

不過開始之前，您應該先知道三個東西：

Frame header

802.3 (Ethernet II *)

PREAMBLE	SFD	DESTINATIONS MAC ADDRESS	SOURCE MAC ADDRESS	LENGTH (TYPE)	DATE	FCS

IP header

VERS	HLEN	SERVER TYPE	TOTAL LENGTH	
IDENTIFICATION			FLAGS	FRAGMENT OFFSET
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM	
SOURCE IP ADDRESS				
DESTINATION IP ADDRESS				
IP OPTIONS				PADDING
DATA				

ICMP header

TYPE	CODE	CHECKSUM
DATA		

PING to Gateway 筆記

PING to Other

我們剛剛 PING 了我們的 Gateway，藉由 Gateway 給我們的回應封包，來檢查網路狀態以及回覆資訊；現在我們來 PING 我們同網段電腦。

在開始之前，我們先檢視一個資訊，請在文字模式中輸入指令「arp -a」，您可以暫時不用了解這是什麼以及回應的內容是什麼：

```
C:\Documents and Settings\350>arp -a

Interface: 192.168.0.175 --- 0x4
  Internet Address      Physical Address      Type
  192.168.0.1           00-0d-88-b0-e3-6f     dynamic

C:\Documents and Settings\350>
```

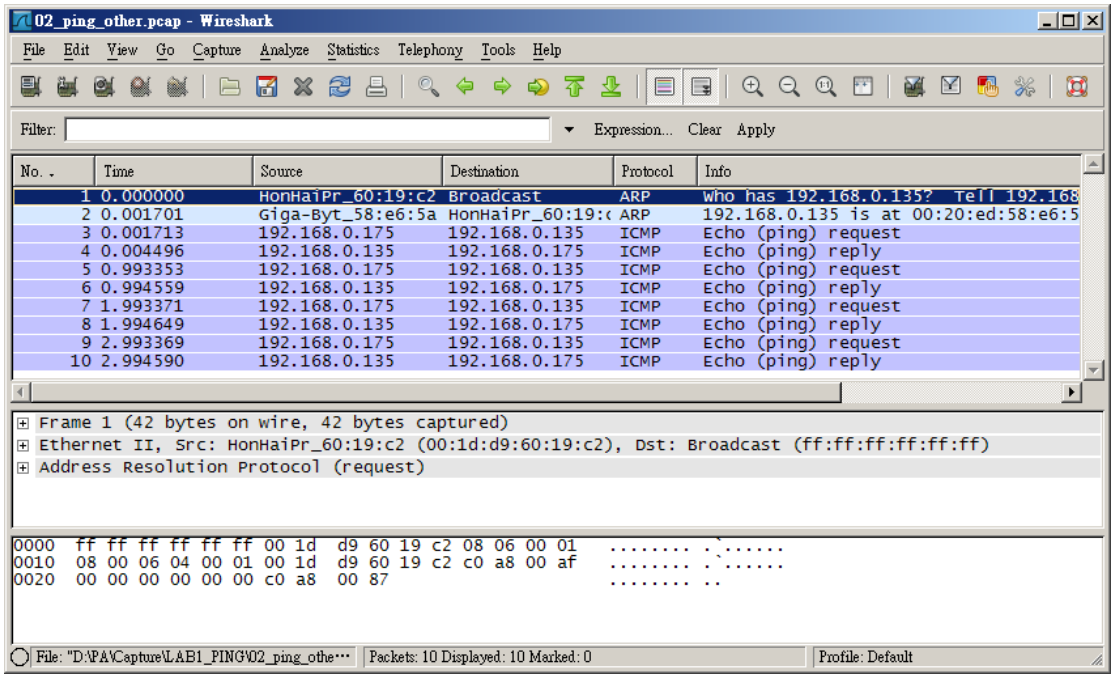
請現在啓動 Wireshark 並開始擷取封包

請在執行視窗中，按下指令「ping 192.168.0.135」，由於我們現在網路都是通的，所以您將會在文字模式看到下面這個訊息回應：

```
C:\Documents and Settings\350>ping 192.168.0.135

Pinging 192.168.0.135 with 32 bytes of data:

Reply from 192.168.0.135: bytes=32 time=4ms TTL=128
Reply from 192.168.0.135: bytes=32 time=1ms TTL=128
Reply from 192.168.0.135: bytes=32 time=1ms TTL=128
Reply from 192.168.0.135: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.135:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\Documents and Settings\350>
```

請停止您 Wireshark 的擷取，開始觀察封包資訊

以及在 Wireshark 所擷取到的訊息（本範例可以在 \Caputre\1-2-1_PING\02_ping_other.pcap 取得）：



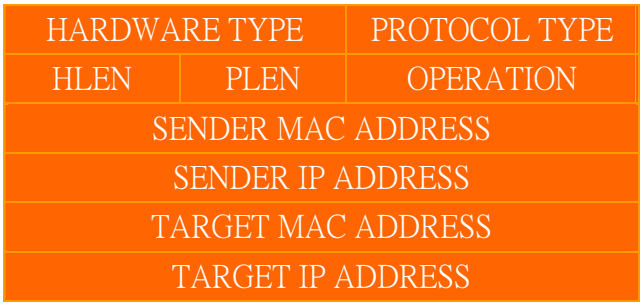
我們發現與剛剛 PING Gateway 所得到的回應以及擷取到得到的封包差不多，但是似乎又有點不一樣！是的，正常的話會多兩個 ARP 封包！

我們再來先重新檢視一個資訊，請到文字模式中輸入指令「arp -a」，您回去上一頁比照，會發現多了我們剛剛 PING 的那台腦：

```
C:\Documents and Settings\350>arp -a

Interface: 192.168.0.175 --- 0x4
  Internet Address      Physical Address      Type
  192.168.0.1           00-0d-88-b0-e3-6f     dynamic
  192.168.0.135         00-20-ed-58-e6-5a     dynamic

C:\Documents and Settings\350>
```

除了上一個章節的三個 Header 外，所以您應該再知道一個 Header，沒錯！就是 ARP header：

ARP Header



ARP 筆記

PING to Other 筆記

自由練習一：**PING to Nobody**

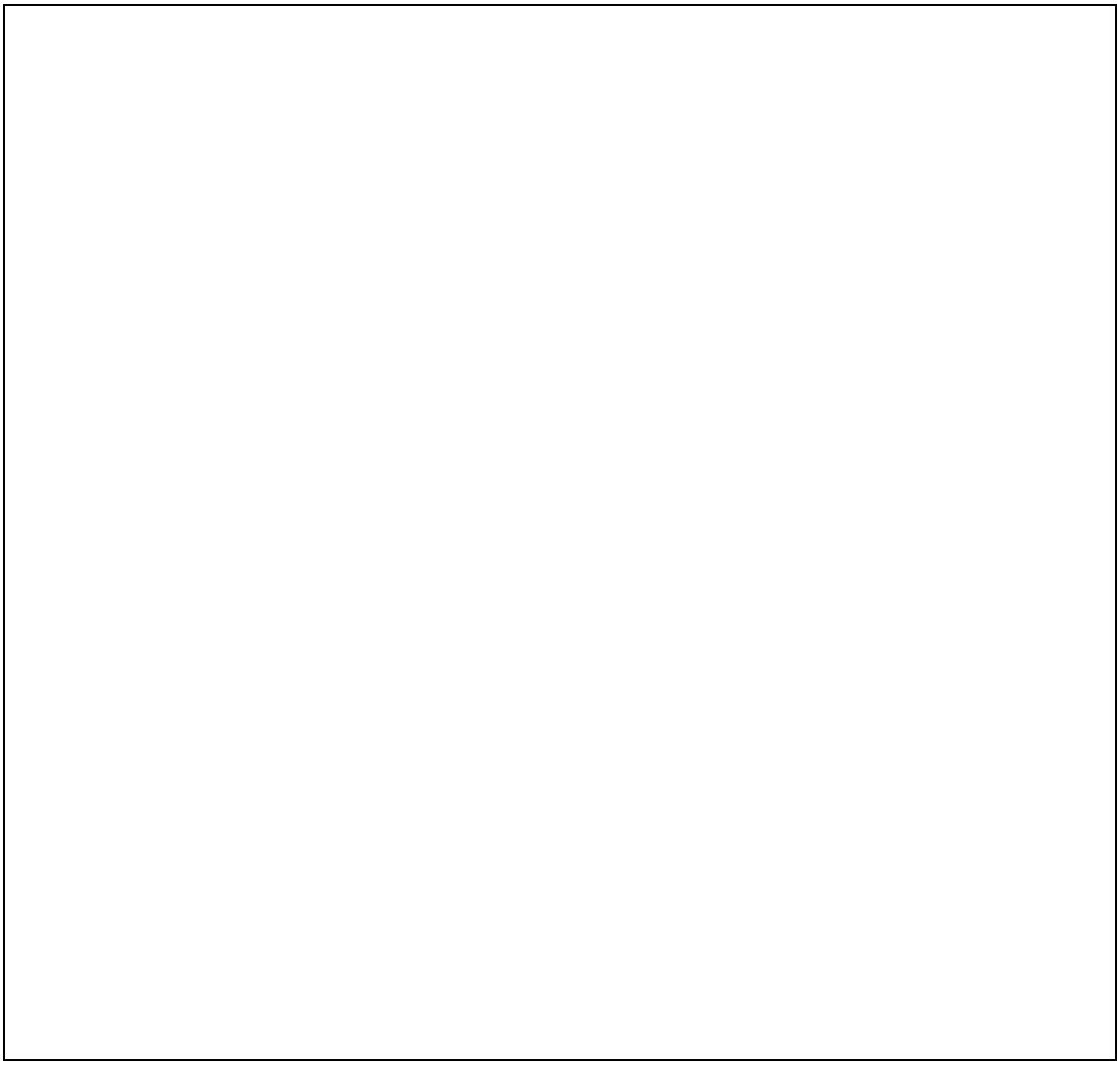
我們以 PING 一台同事實上不存在的 IP (網段及 IP 都正確) ，試想會發生什麼事情？再以實際封包分析來驗證！

```
C:\Documents and Settings\350>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
      Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\350>
```

自由練習二：**PING to Wrong**

我們以 PING 一台同事實上不存在的錯誤 IP (網段不正確)，試想會發生什麼事情？再以實際封包分析來驗證！

```
C:\Documents and Settings\350>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.100:
      Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\350>
```



自由練習三：**PING to ME**

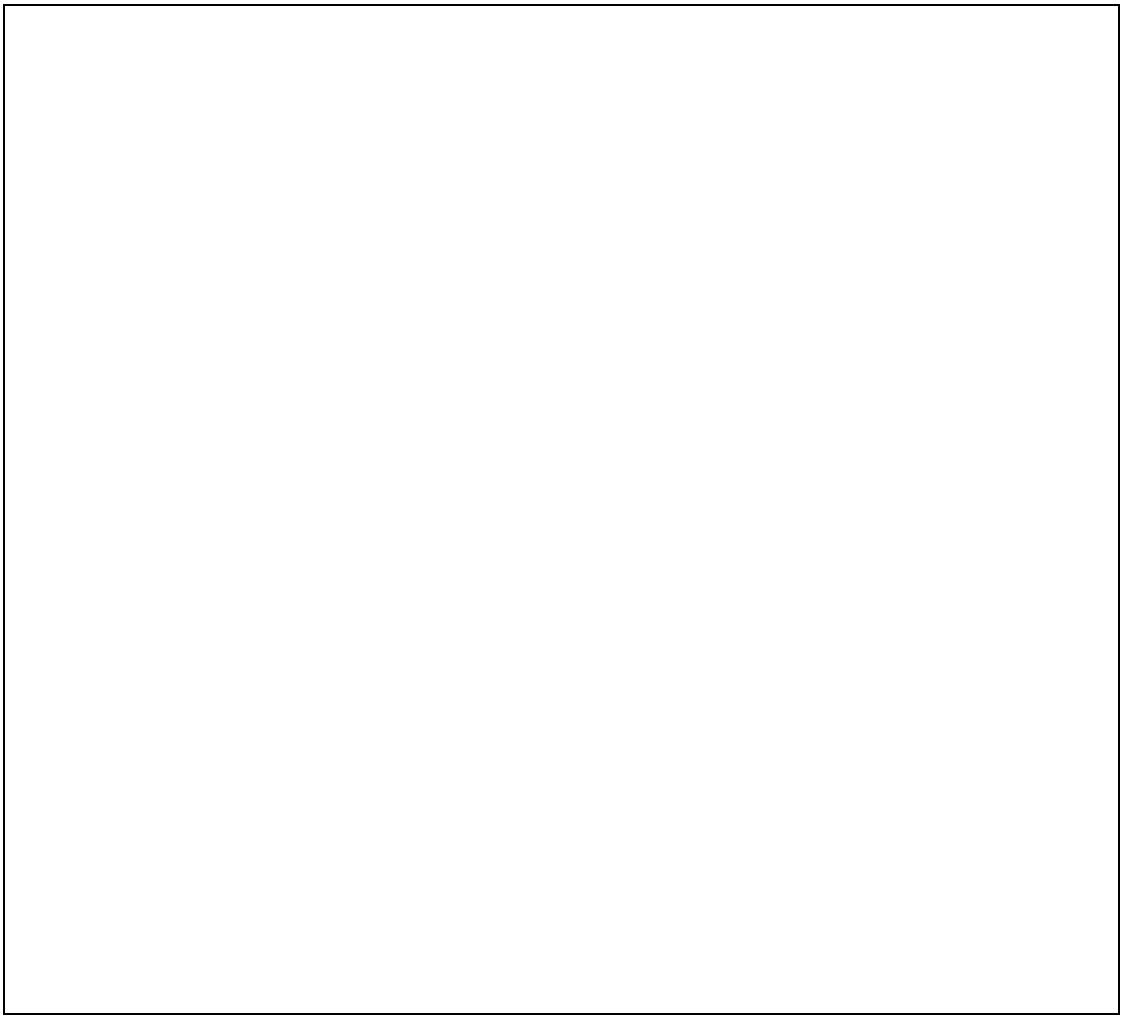
我們以 PING 自己本機的 IP (192.168.0.175)，試想會發生什麼事情？再以實際封包分析來驗證！

```
C:\Documents and Settings\350>ping 192.168.0.175

Pinging 192.168.0.175 with 32 bytes of data:

Reply from 192.168.0.175: bytes=32 time<1ms TTL=128
Reply from 192.168.0.175: bytes=32 time<1ms TTL=128
Reply from 192.168.0.175: bytes=32 time<1ms TTL=128
Reply from 192.168.0.175: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.175:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\350>
```

自由練習四：**PING to ME**

我們以 PING 自己本機的 Loopback Address (127.0.0.1)，試想會發生什麼事情？再以實際封包分析來驗證！

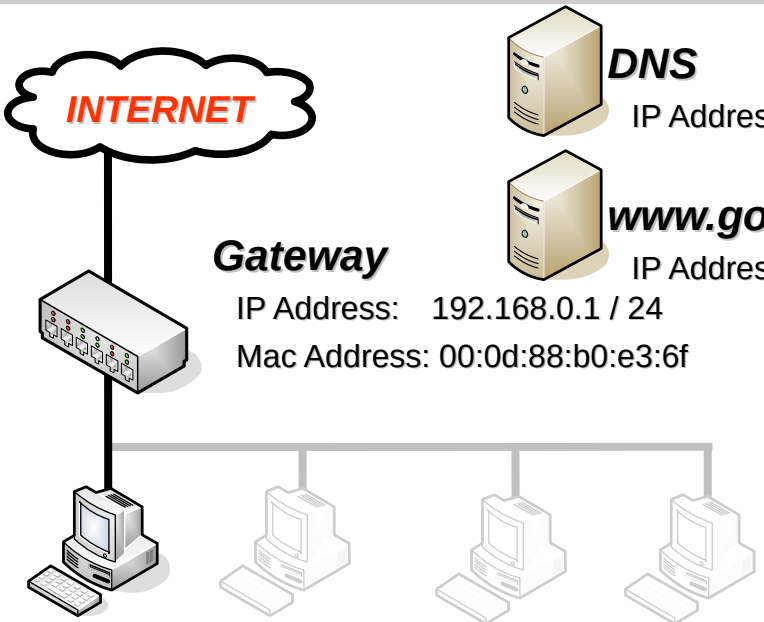
```
C:\Documents and Settings\350>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\350>
```



PROTOCOL ANALYSIS

1-2-2 : DNS

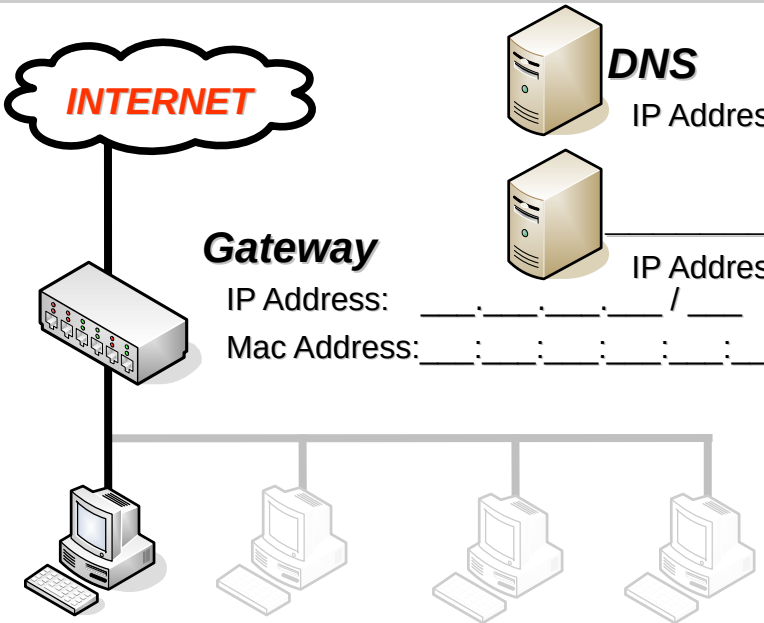
講義環境設定



PC/Workstation

IP Address: 192.168.0.175 / 24
Mac Address: 00:1d:d9:60:19:c2
Gateway: 192.168.0.1

我的環境設定



PC/Workstation

IP Address: ___.___.___.___ / ___
Mac Address:___:___:___:___:___:___
Gateway: ___.___.___.___

DNS 到網路世界

您知道中央氣象局的 IP 嗎？跟您說 IP 是「 210.65.0.71 」，如果想查氣象資訊請在瀏覽器上輸入 210.65.0.71，應該如下所示：

不過現在知道 IP，不代表您以後都記得，但是您要知道，在目前的網路世界中，是靠 IP 來辨別身分的，IP 是由四組數字組成，從 0.0.0.0 到 255.255.255.255，當然這不是您想要用就用，他是有一定的分配規則與管理單位的（ 詳細內容請翻閱 TCP/IP 相關書籍)；既然都是以 IP 作爲辨識，那可想而知一定很不好記住！

您一定會想，想到中央氣象局網站就直接輸入「 www.cwb.gov.tw 」就好了，何必記難記的四組數字？其實您只是在使用 DNS 服務而已，DNS 服務是什麼？DNS 最主要的就是將 www.cwb.gov.tw 轉成 210.65.0.71，所以您只要記住 www.cwb.gov.tw 這種有文字意義的網址就可以了，不必記住難記又無意義的數字。

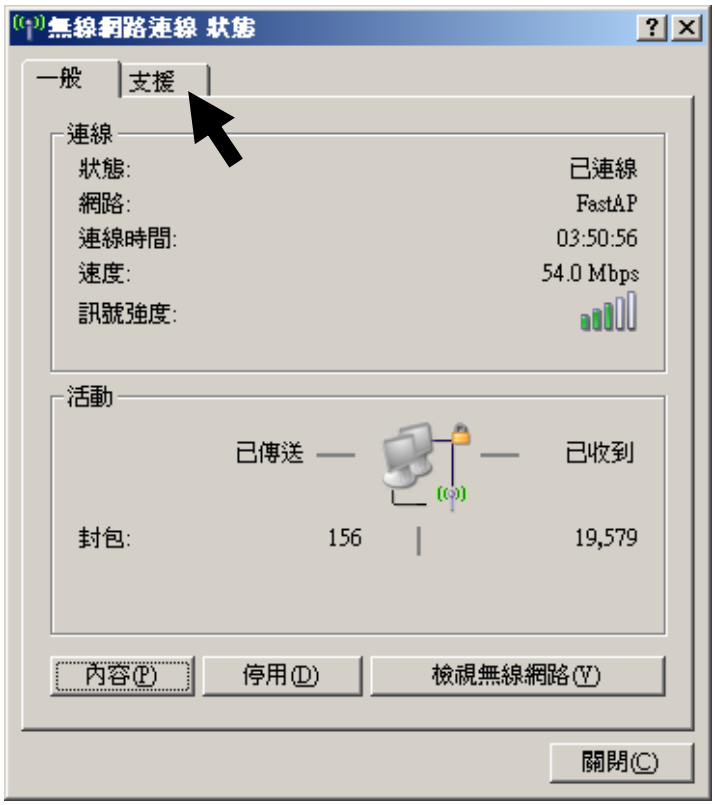
如果您以中央氣象局網站 www.cwb.gov.tw 進入網站，就算中央氣象局變更 IP 位址您也不會察覺，而您也不用在乎中央氣象局的 IP 是多少（ 排除駭客行爲)。

了解目前網路設定

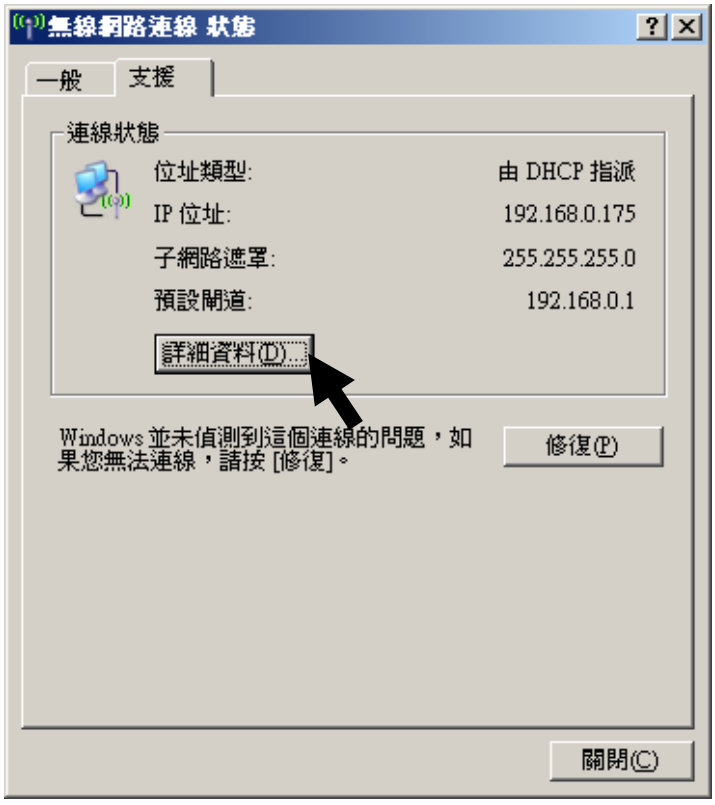
接下來，我們在開始了解 DNS 前，請先了解自己的網路設定資訊，並將相關資訊填入「我的環境資訊」裡：

桌面 → 網路上的芳鄰 → 滑鼠右鍵選「內容」

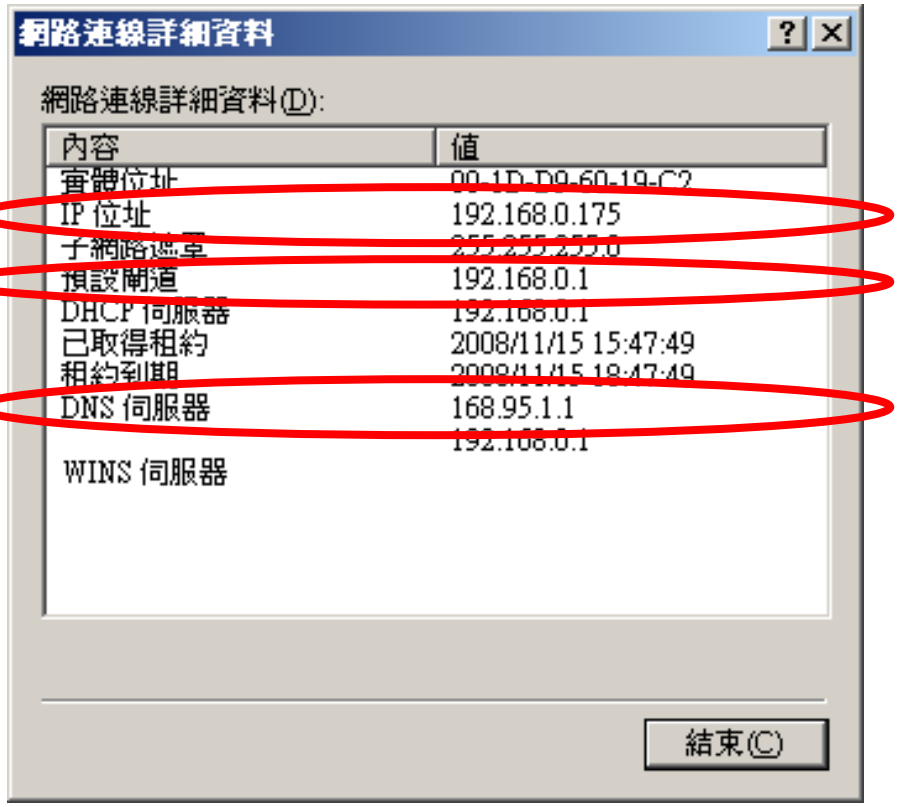
選擇您的網路介面（ 本範例爲無線網路 ）→ 滑鼠左鍵兩下



出現該介面卡的連線狀態，請選擇「支援」



再選擇「詳細資料」



裡面有我們想要的網路設定資訊！

清除 DNS 快取

我們待會會以台 **Wireshark** 網站爲例，如果您電腦曾經連線過，在 DNS 以及瀏覽器上，都會存留著快取資訊，這樣就會影響等會我們觀察 DNS 封包，而在本 LAB 中，我們只需要清除 DNS 快取即可。

請在文字模式中，按下指令「ipconfig /flushdns」，清除成功的話，您將會在文字模式看到下面這個訊息回應：

```
C:\Documents and Settings\350>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Documents and Settings\350>
```

開始擷取 DNS 封包

爲了不讓各位被其他封包混搖視線，我們還是以 ICMP (ping) 作爲前鋒，幫助我們觀察 DNS 封包，

請先別急著打開您網路瀏覽器，因爲於網頁封包部分 (HTTP) ，我們將會有另外章節來解釋。在這裡，我們只需要文字模式即可。

請開啓您的 Wireshark，準備好您的網路擷取狀態：

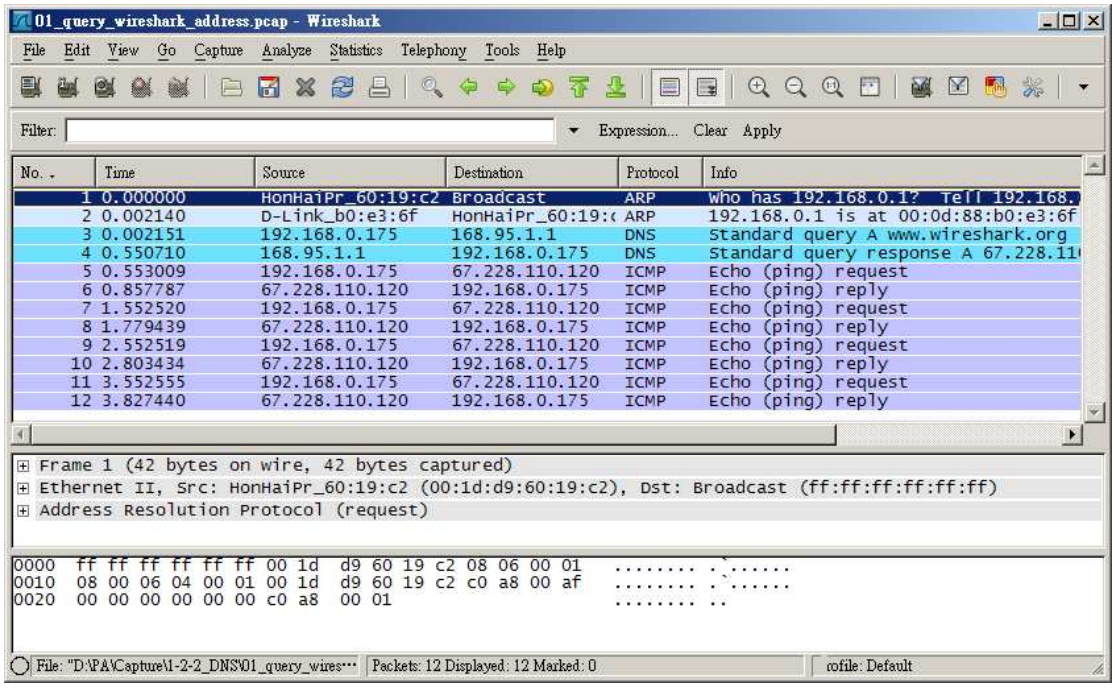
請現在啓動 Wireshark 並開始擷取封包

請在執行視窗中，按下指令「ping　tw.yahoo.com」，由於我們現在網路都是通的，所以您將會在文字模式看到下面這個訊息回應：

```
C:\Documents and Settings\350>ping    www.wireshark.org

Pinging www.wireshark.org [67.228.110.120] with 32 bytes of data:

Reply from 67.228.110.120: bytes=32 time=304ms TTL=45
Reply from 67.228.110.120: bytes=32 time=226ms TTL=45
Reply from 67.228.110.120: bytes=32 time=250ms TTL=45
Reply from 67.228.110.120: bytes=32 time=274ms TTL=45

Ping statistics for 67.228.110.120:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
      Minimum = 226ms, Maximum = 304ms, Average = 263ms

C:\Documents and Settings\350>
```

請停止您 Wireshark 的擷取，開始觀察封包資訊

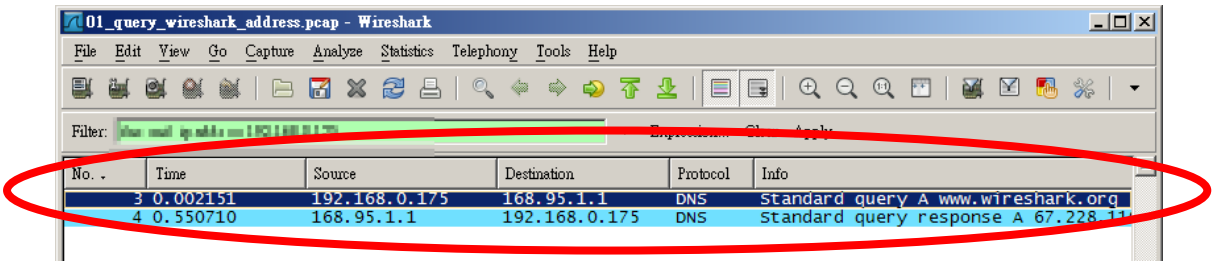
您已經可以在 Wireshark 裡看見許多關於這整個查詢以及的封包資訊（本範例可以在 \Caputre\1-2-2_DNS\01_query_wireshark_address.pcap 取得）：



過濾封包

沒錯，封包實在太多了，還有一堆網頁封包以及別人的封包，您應該知道怎麼過濾吧！試試看：

過濾出屬於自己的 DNS 封包



最主要爲「封包 1 」與 「封包 2」，***其他 DNS 封包是網頁內容去查詢的***。

開始觀察 **DNS** 封包

在開始觀察封包前，您應該知道 DNS 的封包格式：

IDENTIFICATION	QR	OPCODE	AA	TC	RD	RA	Z	AD	CD	RCODE
QUESTIONS			ANSWER RRS							
AUTHORITY RRS			ADDITIONAL RRS							

DNS 查詢流程筆記

自由練習一：請求錯誤的「Wireshark 台灣站」主機

我們試著查詢「www.wireshark.org.tw」，試想會發生什麼事情（事實上這個 Domain 沒有人使用）？再以實際封包分析來驗證！

自由練習二：請求不存在的 **Domain Name**

我們試著查詢「www.sharkshark.org」，試想會發生什麼事情（ 事實上這個 Domain 沒有人使用)？再以實際封包分析來驗證！

自由練習三：查詢不同 **DNS** 的回應

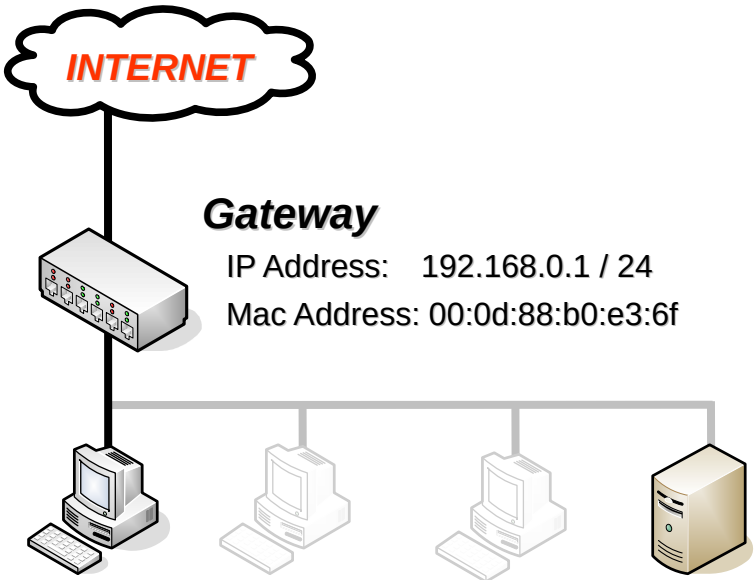
我們試著對不同 DNS 查詢「www.wireshark.org」，不同 DNS 的回應有何差別嗎？還是沒有差別？再以實際封包分析來驗證！(記得清除 DNS 快取)

Google Public DNS	8.8.8.8	GIGA DNS	203.133.1.6
HINET DNS	168.95.1.1	SO NET DNS	61.64.127.1
SEEDNET DSN (N)	139.175.55.244	Sparq DNS	61.56.211.185

PROTOCOL ANALYSIS

1-2-3 : FTP

講義環境設定



Gateway

IP Address: 192.168.0.1 / 24

Mac Address: 00:0d:88:b0:e3:6f

PC/Workstation

IP Address: 192.168.0.175 / 24

Mac Address: 00:1d:d9:60:19:c2

Gateway: 192.168.0.1

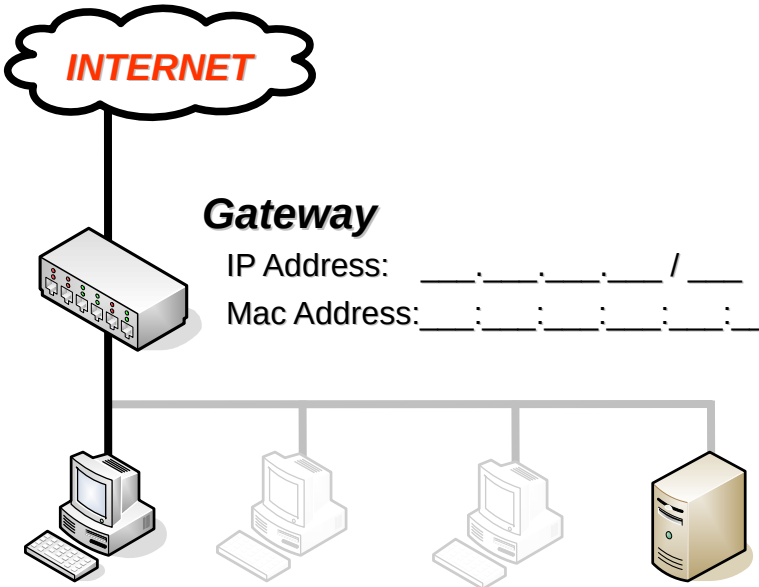
FTP Server (FileZilla)

IP Address: 192.168.0.135 / 24

Mac Address: 00:20:ed:58:e6:5a

Gateway: 192.168.0.1

我的環境設定



Gateway

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

PC/Workstation

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

FTP Server ( )

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

開始使用 **FTP**

本範例的 FTP Server 採用 Open Source 的 **FileZilla Server** ，在課程上都架設完畢了！您如果自行練習可以自行選用任何一個軟體或是套件。

首先開始前，請您啓動好 Wireshark 來擷取我們接下來的封包資訊喔！

請現在啓動 Wireshark 並開始擷取封包

首先，我們還是一樣啓動文字模式，並且登入 FTP ：「ftp 192.168.0.135」，連線成功將會出現 220 的歡迎訊息，並會要求您輸入 FTP 的使用者帳號，我們輸入「PA」。

```
C:\Documents and Settings\350>ftp 192.168.0.135
Connected to 192.168.0.135.
220-FileZilla Server version 0.9.34 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
User (192.168.0.135:(none)): PA
```

然後 FTP Sever 要求您輸入 pa 的密碼，密碼：「123456」。

```
331 Password required for pa
Password: 123456
```

出現登入成功後出現 230 Logged on，並出現提示 FTP 命令列，我們先查看整個 FTP 目錄，請輸入「dir」。

```
230 Logged on
ftp> dir
```

我們已經列出了目錄，請進入 Capture 下的 2-1-1_FTP 目錄並查一邊查看目錄列表，請跟著畫面指令操作。

```
200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:09 Capture
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:22 Doc
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:22 Software
226 Transfer OK
ftp: 171 bytes received in 0.00Seconds 171000.00Kbytes/sec.
ftp> cd  Capture

250 CWD successful. "/Capture" is current directory.
ftp> dir

200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 1-1_BASE
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 1-2-1_PING
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 1-2-2_DNS
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:07 1-2-3_FTP
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 1-2-SP1_DHCP
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 1-2-SP2_HTTP
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 1-2-SP3_MSN
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 Appendix_GeoIP
drwxr-xr-x 1 ftp ftp              0 Jul 23 15:06 Appendix_Statistics
226 Transfer OK
ftp: 563 bytes received in 0.00Seconds 563000.00Kbytes/sec.
ftp> cd  2-1-1_FTP

250 CWD successful. "Capture/1-2-3_FTP" is current directory.
ftp> dir
```

下載我們需要的檔案 test.txt，請輸入：「get　test.txt」

```
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              2217 Jul 23 15:07 01_command.txt
-r--r--r-- 1 ftp ftp              7966 Jul 23 15:07 01_FTP.pcap
-r--r--r-- 1 ftp ftp                26 Jul 23 13:11 test.txt
226 Transfer OK
ftp: 186 bytes received in 0.00Seconds 186000.00Kbytes/sec.
ftp> get  test.txt
```

下載完成後，我們離開 FTP！

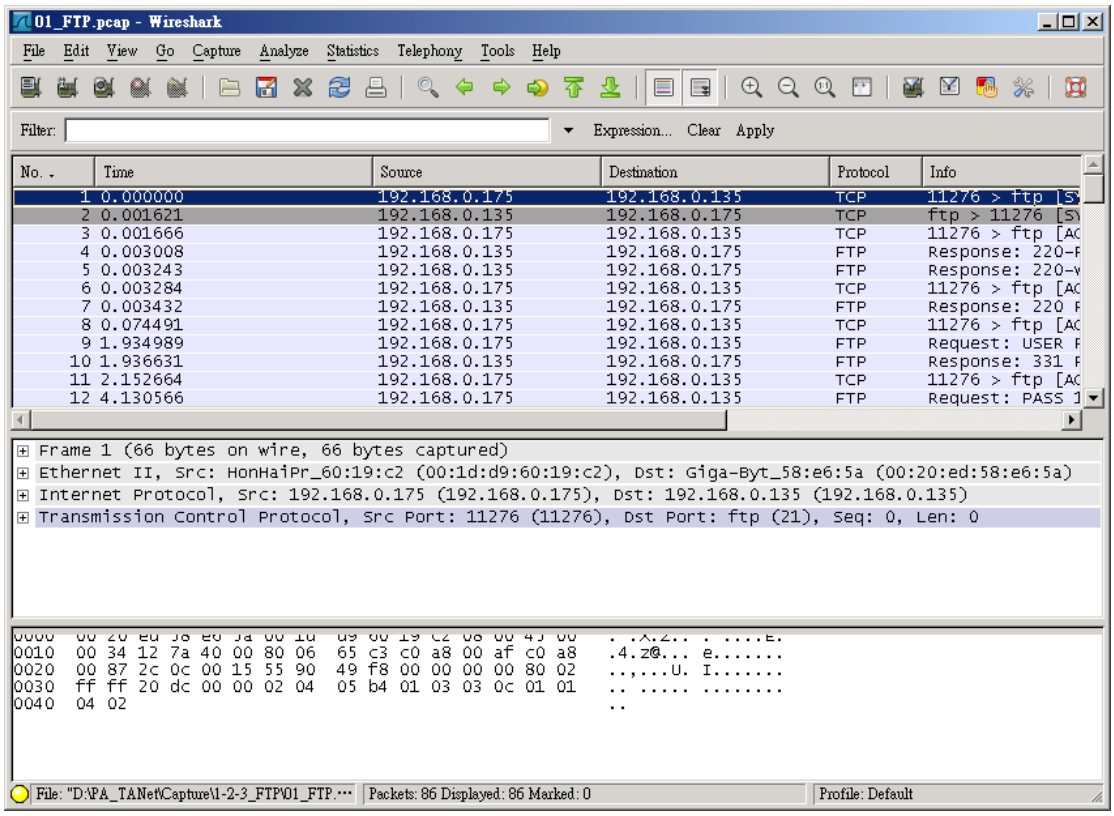
```
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 26 bytes received in 0.00Seconds 0.84Kbytes/sec.
ftp> bye

221 Goodbye

C:\Documents and Settings\350>
```

請停止您 **Wireshark** 的擷取，開始觀察封包資訊

解析封包內容資訊

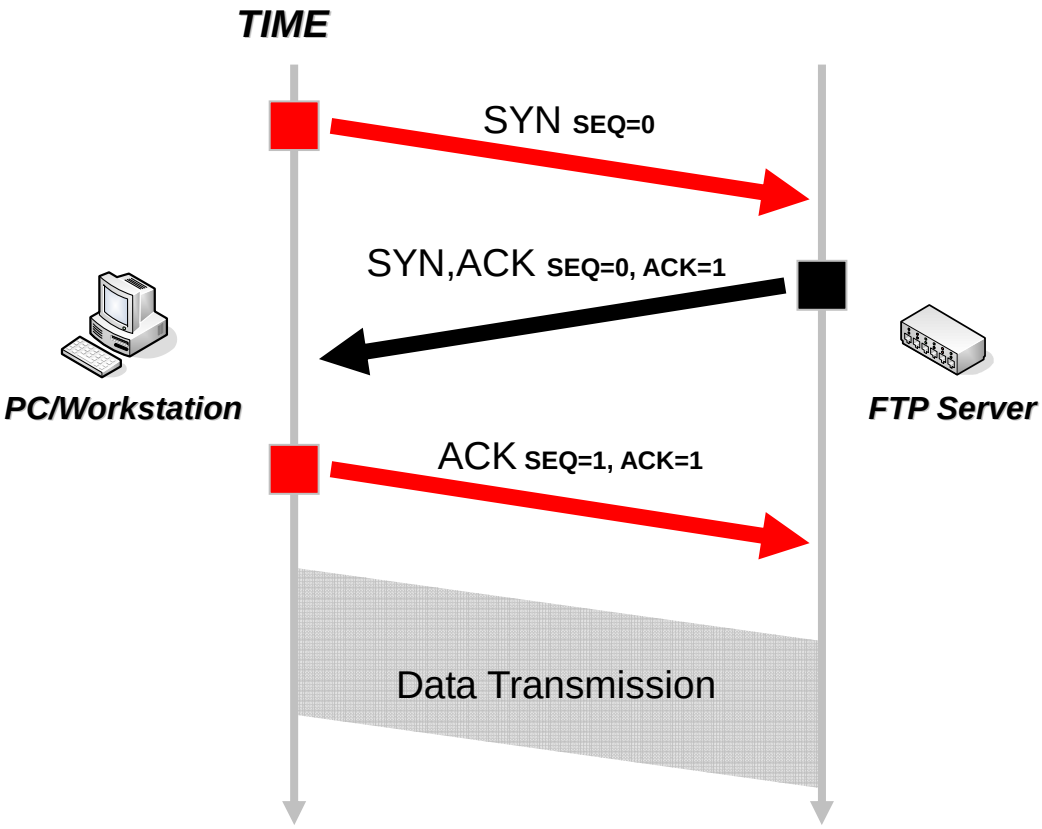
要開始 FTP 的封包分析時，當然您要先瞭解 **FTP 運作原理**，當然 350 會在上課時以投影片講解，所以如果還有不清楚的同學，麻煩再回去看一下投影片喔！

下列是剛剛整個過程所擷取的封包（本範例可以在 \Caputre\1-2-3_FTP\01_FTP.pcap 取得）：



三方交握

任何 TCP 在傳輸資料前都需要先建立一個虛擬線路(連線)，所以再建立時需以三方交握的方式來建立，下圖則爲兩方的交握過程，您可以搭配您的實際狀況來檢視是否現實連線確實如此：



三方交握筆記

連線模式

一般在 FTP 我們會因爲您的網路環境 (如：防火牆) 的原因，您需要採用不同的連線模式，一般來說分爲主動模式 (Active Mode)、被動模式 (Passive Mode)：

Mini Question：

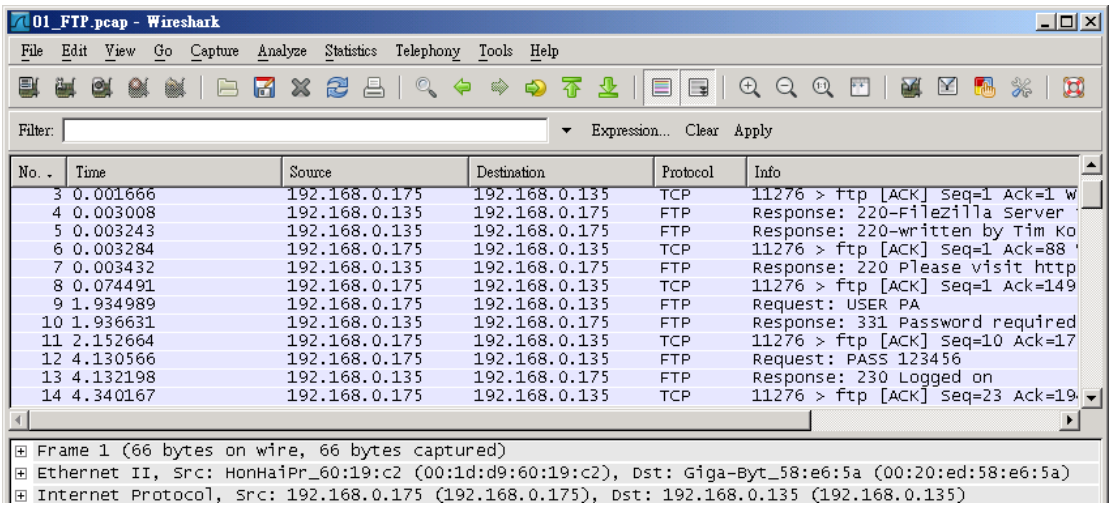
請問我們上課所採用的 FileZilla Server，當您連線該 Server 所產生的封包分析後，請問是什麼模式？

☐ 主動模式 (Active Mode)　　☐ 被動模式 (Passive Mode)

連線模式筆記

FTP 登入流程

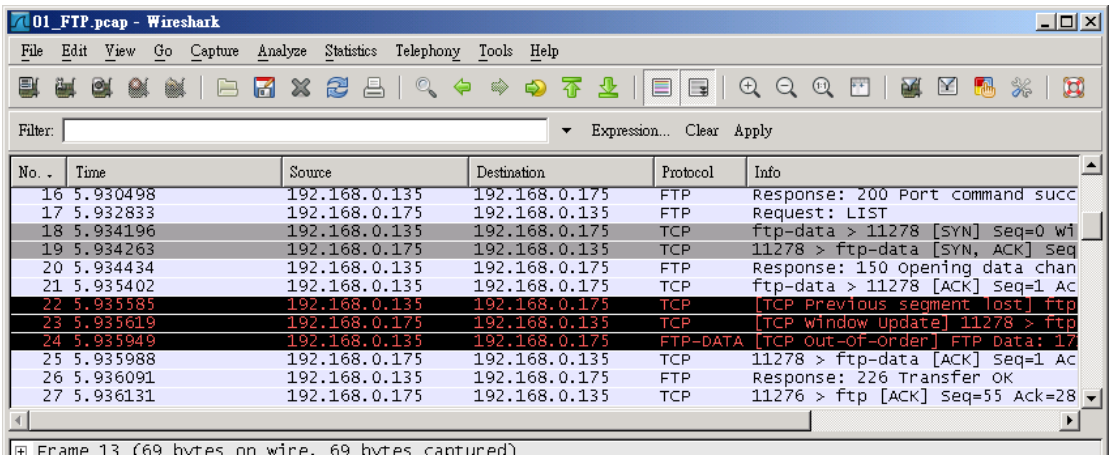
接下來我們要登入 FTP，從封包擷取的過程中，您應該了解這些過程，以及 FTP 帶來的隱憂：



FTP 登入流程筆記

資料傳輸與溝通

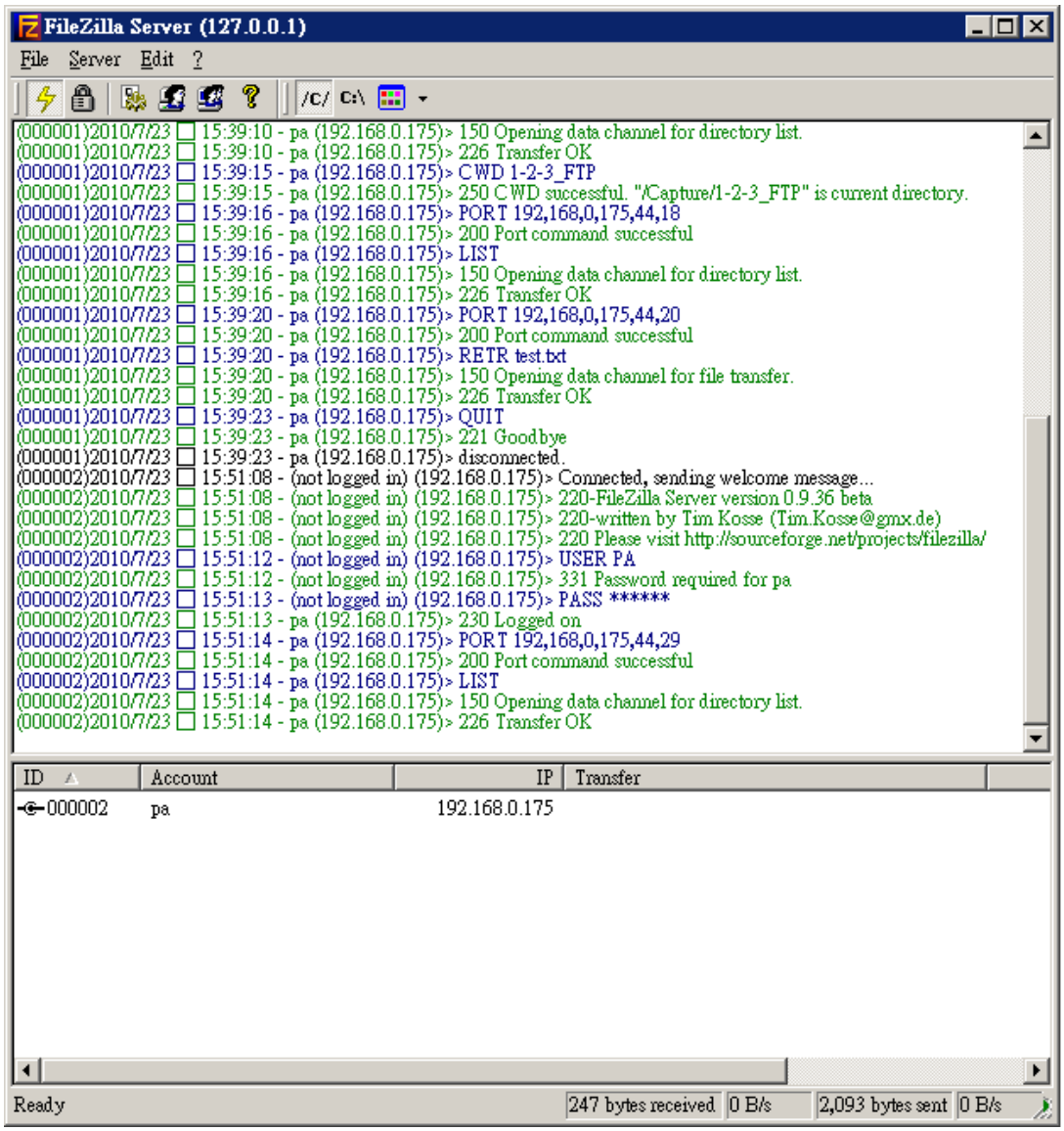
我們現在開始來分析登入後的指令溝通以及資料傳輸過程，如果您擷取了許多與自己無關的封包，請記得使用過濾功能：



資料傳輸與溝通筆記

Server 端訊息

在上課中，如果您是當 FTP Server 的同學，您可以打開檢視界面，我們可以由 FileZilla Server 上看到整個連線過程，不同的 FTP Server 套件的檢視方法不一定相同：



自由練習

您應該已經從這個 LAB 中發現傳統的 FTP 雖然方便，但是卻在本質上出現嚴重的問題(明碼帶來的隱憂)，請問您有什麼解決方案呢？

PROTOCOL ANALYSIS

附錄：協定資訊

Protocol Numbers List (updated 2009-06-18)

Registries included below:
- Assigned Internet Protocol Numbers

Registry Name: Assigned Internet Protocol Numbers
Reference: [RFC5237]
Registration Procedures: IESG Approval or Standards Action
Note: In the Internet Protocol version 4 (IPv4) [RFC791] there is a field called "Protocol" to identify the next level protocol. This is an 8 bit field. In Internet Protocol version 6 (IPv6) [RFC1883], this field is called the "Next Header" field.

Registry:

Decimal	Keyword	Protocol	References
0	HOPOPT	IPv6 Hop-by-Hop Option	[RFC1883]
1	ICMP	Internet Control Message	[RFC792]
2	IGMP	Internet Group Management	[RFC1112]
3	GGP	Gateway-to-Gateway	[RFC823]
4	IP	IP in IP (encapsulation)	[RFC2003]
5	ST	Stream	[RFC1190][RFC1819]
6	TCP	Transmission Control	[RFC793]
7	CBT	CBT	[Ballardie]
8	EGP	Exterior Gateway Protocol	[RFC888][DLM1]
9	IGP	any private interior gateway (used by Cisco for their IGRP)	[IANA]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]
11	NVP-II	Network Voice Protocol	[RFC741][SC3]
12	PUP	PUP	[PUP][XEROX]
13	ARGUS	ARGUS	[RWS4]
14	EMCON	EMCON	[BN7]
15	XNET	Cross Net Debugger	[IEN158][JFH2]
16	CHAOS	Chaos	[NC3]
17	UDP	User Datagram	[RFC768][JBP]
18	MUX	Multiplexing	[IEN90][JBP]
19	DCN-MEAS	DCN Measurement Subsystems	[DLM1]
20	HMP	Host Monitoring	[RFC869][RH6]
21	PRM	Packet Radio Measurement	[ZSU]
22	XNS-IDP	XEROX NS IDP	[ETHERNET][XEROX]
23	TRUNK-1	Trunk-1	[BWB6]
24	TRUNK-2	Trunk-2	[BWB6]
25	LEAF-1	Leaf-1	[BWB6]
26	LEAF-2	Leaf-2	[BWB6]
27	RDP	Reliable Data Protocol	[RFC908][RH6]
28	IRTP	Internet Reliable Transaction	[RFC938][TXM]
29	ISO-TP4	ISO Transport Protocol Class 4	[RFC905][RC77]
30	NETBLT	Bulk Data Transfer Protocol	[RFC969][DDC1]
31	MFE-NSP	MFE Network Services Protocol	[MFENET][BCH2]
32	MERIT-INP	MERIT Internodal Protocol	[HWB]
33	DCCP	Datagram Congestion Control Protocol	[RFC4340]
34	3PC	Third Party Connect Protocol	[SAF3]
35	IDPR	Inter-Domain Policy Routing Protocol	[MXS1]
36	XTP	XTP	[GXC]
37	DDP	Datagram Delivery Protocol	[WXC]
38	IDPR-CMTP	IDPR Control Message Transport Proto	[MXS1]

Decimal	Keyword	Protocol	References
39	TP++	TP++ Transport Protocol	[DXF]
40	IL	IL Transport Protocol	[Presotto]
41	IPv6	Ipv6	[Deering]
42	SDRP	Source Demand Routing Protocol	[DXE1]
43	IPv6-Route	Routing Header for IPv6	[Deering]
44	IPv6-Frag	Fragment Header for IPv6	[Deering]
45	IDRP	Inter-Domain Routing Protocol	[Hares]
46	RSVP	Reservation Protocol	[Braden]
47	GRE	General Routing Encapsulation	[Li]
48	DSR	Dynamic Source Routing Protocol	[RFC4728]
49	BNA	BNA	[Salamon]
50	ESP	Encap Security Payload	[RFC4303]
51	AH	Authentication Header	[RFC4302]
52	I-NLSP	Integrated Net Layer Security TUBA	[GLENN]
53	SWIPE	IP with Encryption	[JI6]
54	NARP	NBMA Address Resolution Protocol	[RFC1735]
55	MOBILE	IP Mobility	[Perkins]
56	TLSP	Transport Layer Security Protocol using Kryptonet key management	[Oberg]
57	SKIP	SKIP	[Markson]
58	IPv6-ICMP	ICMP for IPv6	[RFC1883]
59	IPv6-NoNxt	No Next Header for IPv6	[RFC1883]
60	IPv6-Opts	Destination Options for IPv6	[RFC1883]
61		any host internal protocol	[IANA]
62	CFTP	CFTP	[CFTP][HCF2]
63		any local network	[IANA]
64	SAT-EXPAK	SATNET and Backroom EXPAK	[SHB]
65	KRYPTOLAN	Kryptolan	[PXL1]
66	RVD	MIT Remote Virtual Disk Protocol	[MBG]
67	IPPC	Internet Pluribus Packet Core	[SHB]
68		any distributed file system	[IANA]
69	SAT-MON	SATNET Monitoring	[SHB]
70	VISA	VISA Protocol	[GXT1]
71	IPCV	Internet Packet Core Utility	[SHB]
72	CPNX	Computer Protocol Network Executive	[DXM2]
73	CPHB	Computer Protocol Heart Beat	[DXM2]
74	WSN	Wang Span Network	[VXD]
75	PVP	Packet Video Protocol	[SC3]
76	BR-SAT-MON	Backroom SATNET Monitoring	[SHB]
77	SUN-ND	SUN ND PROTOCOL-Temporary	[WM3]
78	WB-MON	WIDEBAND Monitoring	[SHB]
79	WB-EXPAK	WIDEBAND EXPAK	[SHB]
80	ISO-IP	ISO Internet Protocol	[MTR]
81	VMTP	VMTP	[DRC3]
82	SECURE-VMTP	SECURE-VMTP	[DRC3]
83	VINES	VINES	[BXH]
84	TTP	TTP	[JXS]
85	NSFNET-IGP	NSFNET-IGP	[HWB]
86	DGP	Dissimilar Gateway Protocol	[DGP][ML109]
87	TCF	TCF	[GAL5]
88	EIGRP	EIGRP	[CISCO][GXS]
89	OSPFIGP	OSPFIGP	[RFC1583][JTM4]
90	Sprite-RPC	Sprite RPC Protocol	[SPRITE][BXW]
91	LARP	Locus Address Resolution Protocol	[BXH]
92	MTP	Multicast Transport Protocol	[SXA]
93	AX.25	AX.25 Frames	[BK29]

Decimal	Keyword	Protocol	References
94	IPIP	IP-within-IP Encapsulation Protocol	[JI6]
95	MICP	Mobile Internetworking Control Pro.	[JI6]
96	SCC-SP	Semaphore Communications Sec. Pro.	[HXH]
97	ETHERIP	Ethernet-within-IP Encapsulation	[RFC3378]
98	ENCAP	Encapsulation Header	[RFC1241,RXB3]
99		any private encryption scheme	[IANA]
100	GMTP	GMTP	[RXB5]
101	IFMP	Ipsilon Flow Management Protocol	[Hinden]
102	PNNI	PNNI over IP	[Callon]
103	PIM	Protocol Independent Multicast	[Farinacci]
104	ARIS	ARIS	[Feldman]
105	SCPS	SCPS	[Durst]
106	QNX	QNX	[Hunter]
107	A/N	Active Networks	[Braden]
108	IPComp	IP Payload Compression Protocol	[RFC2393]
109	SNP	Sitara Networks Protocol	[Sridhar]
110	Compaq-Peer	Compaq Peer Protocol	[Volpe]
111	IPX-in-IP	IPX in IP	[Lee]
112	VRRP	Virtual Router Redundancy Protocol	[RFC3768]
113	PGM	PGM Reliable Transport Protocol	[Speakman]
114		any 0-hop protocol	[IANA]
115	L2TP	Layer Two Tunneling Protocol	[Aboba]
116	DDX	D-II Data Exchange (DDX)	[Worley]
117	IATP	Interactive Agent Transfer Protocol	[Murphy]
118	STP	Schedule Transfer Protocol	[JMP]
119	SRP	SpectraLink Radio Protocol	[Hamilton]
120	UTI	UTI	[Lothberg]
121	SMP	Simple Message Protocol	[Ekblad]
122	SM	SM	[Crowcroft]
123	PTP	Performance Transparency Protocol	[Welzl]
124	ISIS over IPv4		[Przygienda]
125	FIRE		[Partridge]
126	CRTP	Combat Radio Transport Protocol	[Sautter]
127	CRUDP	Combat Radio User Datagram	[Sautter]
128	SSCOPMCE		[Waber]
129	IPLT		[Hollbach]
130	SPS	Secure Packet Shield	[McIntosh]
131	PIPE	Private IP Encapsulation within IP	[Petri]
132	SCTP	Stream Control Transmission Protocol	[Stewart]
133	FC	Fibre Channel	[Rajagopal]
134	RSVP-E2E-IGNORE		[RFC3175]
135	Mobility Header		[RFC3775]
136	UDPLite		[RFC3828]
137	MPLS-in-IP		[RFC4023]
138	manet	MANET Protocols	[RFC5498]
139	HIP	Host Identity Protocol	[RFC5201]
140	Shim6	Shim6 Protocol	[RFC5533]
141-252		Unassigned	[IANA]
253		Use for experimentation and testing	[RFC3692]
254		Use for experimentation and testing	[RFC3692]
255	Reserved		[IANA]

Ethernet Type Codes

Ethernet		Exp. Ethernet		Description
decimal	Hex	decimal	octal	
000	0000-05DC	-	-	IEEE802.3 Length Field
257	0101-01FF	-	-	Experimental
512	0200	512	1000	XEROX PUP (see 0A00)
513	0201	-	-	PUP Addr Trans (see 0A01)
	0400			Nixdorf
1536	0600	1536	3000	XEROX NS IDP
	0660			DLOG
	0661			DLOG
2048	0800	513	1001	Internet IP (IPv4)
2049	0801	-	-	X.75 Internet
2050	0802	-	-	NBS Internet
2051	0803	-	-	ECMA Internet
2052	0804	-	-	Chaosnet
2053	0805	-	-	X.25 Level 3
2054	0806	-	-	ARP
2055	0807	-	-	XNS Compatability
2076	081C	-	-	Symbolics Private
2184	0888-088A	-	-	Xyplex
2304	0900	-	-	Ungermann-Bass net debugr
2560	0A00	-	-	Xerox IEEE802.3 PUP
2561	0A01	-	-	PUP Addr Trans
2989	0BAD	-	-	Banyan Systems
4096	1000	-	-	Berkeley Trailer nego
4097	1001-100F	-	-	Berkeley Trailer encap/IP
5632	1600	-	-	Valid Systems
16962	4242	-	-	PCS Basic Block Protocol
21000	5208	-	-	BBN Simnet
24576	6000	-	-	DEC Unassigned (Exp.)
24577	6001	-	-	DEC MOP Dump/Load
24578	6002	-	-	DEC MOP Remote Console
24579	6003	-	-	DEC DECNET Phase IV Route
24580	6004	-	-	DEC LAT
24581	6005	-	-	DEC Diagnostic Protocol
24582	6006	-	-	DEC Customer Protocol
24583	6007	-	-	DEC LAVC, SCA
24584	6008-6009	-	-	DEC Unassigned
24586	6010-6014	-	-	3Com Corporation
28672	7000	-	-	Ungermann-Bass download
28674	7002	-	-	Ungermann-Bass dia/loop
28704	7020-7029	-	-	LRT
28720	7030	-	-	Proteon
28724	7034	-	-	Cabletron
32771	8003	-	-	Cronus VLN
32772	8004	-	-	Cronus Direct
32773	8005	-	-	HP Probe
32774	8006	-	-	Nestar
32776	8008	-	-	AT&T
32784	8010	-	-	Excelan
32787	8013	-	-	SGI diagnostics
32788	8014	-	-	SGI network games
32789	8015	-	-	SGI reserved
32790	8016	-	-	SGI bounce server
32793	8019	-	-	Apollo Computers
32815	802E	-	-	Tymshare
32816	802F	-	-	Tigan, Inc.

Ethernet		Exp. Ethernet		Description
decimal	Hex	decimal	octal	
32821	8035	-	-	Reverse ARP
32822	8036	-	-	Aeonic Systems
32824	8038	-	-	DEC LANBridge
32825	8039-803C	-	-	DEC Unassigned
32829	803D	-	-	DEC Ethernet Encryption
32830	803E	-	-	DEC Unassigned
32831	803F	-	-	DEC LAN Traffic Monitor
32832	8040-8042	-	-	DEC Unassigned
32836	8044	-	-	Planning Research Corp.
32838	8046	-	-	AT&T
32839	8047	-	-	AT&T
32841	8049	-	-	ExperData
32859	805B	-	-	Stanford V Kernel exp.
32860	805C	-	-	Stanford V Kernel prod.
32861	805D	-	-	Evans & Sutherland
32864	8060	-	-	Little Machines
32866	8062	-	-	Counterpoint Computers
32869	8065	-	-	Univ. of Mass. @ Amherst
32870	8066	-	-	Univ. of Mass. @ Amherst
32871	8067	-	-	Veeco Integrated Auto.
32872	8068	-	-	General Dynamics
32873	8069	-	-	AT&T
32874	806A	-	-	Autophon
32876	806C	-	-	ComDesign
32877	806D	-	-	Computgraphic Corp.
32878	806E-8077	-	-	Landmark Graphics Corp.
32890	807A	-	-	Matra
32891	807B	-	-	Dansk Data Elektronik
32892	807C	-	-	Merit Internodal
32893	807D-807F	-	-	Vitalink Communications
32896	8080	-	-	Vitalink TransLAN III
32897	8081-8083	-	-	Counterpoint Computers
32923	809B	-	-	Appletalk
32924	809C-809E	-	-	Datability
32927	809F	-	-	Spider Systems Ltd.
32931	80A3	-	-	Nixdorf Computers
32932	80A4-80B3	-	-	Siemens Gammasonics Inc.
32960	80C0-80C3	-	-	DCA Data Exchange Cluster
	80C4			Banyan Systems
	80C5			Banyan Systems
32966	80C6	-	-	Pacer Software
32967	80C7	-	-	Applitek Corporation
32968	80C8-80CC	-	-	Intergraph Corporation
32973	80CD-80CE	-	-	Harris Corporation
32975	80CF-80D2	-	-	Taylor Instrument
32979	80D3-80D4	-	-	Rosemount Corporation
32981	80D5	-	-	IBM SNA Service on Ether
32989	80DD	-	-	Varian Associates
32990	80DE-80DF	-	-	Integrated Solutions TRFS
32992	80E0-80E3	-	-	Allen-Bradley
32996	80E4-80F0	-	-	Datability
33010	80F2	-	-	Retix
33011	80F3	-	-	AppleTalk AARP (Kinetics)
33012	80F4-80F5	-	-	Kinetics
33015	80F7	-	-	Apollo Computer
33023	80FF-8103	-	-	Wellfleet Communications
33031	8107-8109	-	-	Symbolics Private
33072	8130	-	-	Hayes Microcomputers
33073	8131	-	-	VG Laboratory Systems
	8132-8136			Bridge Communications

Ethernet		Exp. Ethernet		Description
decimal	Hex	decimal	octal	
33079	8137-8138	-	-	Novell, Inc.
33081	8139-813D	-	-	KTI
	8148			Logicraft
	8149			Network Computing Devices
	814A			Alpha Micro
33100	814C	-	-	SNMP
	814D			BIIN
	814E			BIIN
	814F			Technically Elite Concept
	8150			Rational Corp
	8151-8153			Qualcomm
	815C-815E			Computer Protocol Pty Ltd
	8164-8166			Charles River Data System
	817D-818C			Protocol Engines
	818D			Motorola Computer
	819A-81A3			Qualcomm
	81A4			ARAI Bunkichi
	81A5-81AE			RAD Network Devices
	81B7-81B9			Xyplex
	81CC-81D5			Apricot Computers
	81D6-81DD			Artisoft
	81E6-81EF			Polygon
	81F0-81F2			Comsat Labs
	81F3-81F5			SAIC
	81F6-81F8			VG Analytical
	8203-8205			Quantum Software
	8221-8222			Ascom Banking Systems
	823E-8240			Advanced Encryption Syste
	827F-8282			Athena Programming
	8263-826A			Charles River Data System
	829A-829B			Inst Ind Info Tech
	829C-82AB			Taurus Controls
	82AC-8693			Walker Richer & Quinn
	8694-869D			Idea Courier
	869E-86A1			Computer Network Tech
	86A3-86AC			Gateway Communications
	86DB			SECTRA
	86DE			Delta Controls
34543	86DF	-	-	ATOMIC
	86E0-86EF			Landis & Gyr Powers
	8700-8710			Motorola
	8A96-8A97			Invisible Software
36864	9000	-	-	Loopback
36865	9001	-	-	3Com(Bridge) XNS Sys Mgmt
36866	9002	-	-	3Com(Bridge) TCP-IP Sys
36867	9003	-	-	3Com(Bridge) loop detect
65280	FF00	-	-	BBN VITAL-LanBridge cache
	FF00-FF0F			ISC Bunker Ramo

Port Numbers List (updated 2009-09-25)

如果您對其他 Port Numbers 想知道的更多更詳細，可以到這裡瀏覽
http://www.iana.org/assignments/port-numbers

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
                  0/tcp    Reserved
                  0/udp    Reserved
#                          Jon Postel <postel&isi.edu>
spr-itunes        0/tcp    Shirt Pocket netTunes
spl-itunes        0/tcp    Shirt Pocket launchTunes
#                          David Nanian <dnanian&shirt-pocket.com> 28 September 2007
tcpmux            1/tcp    TCP Port Service Multiplexer
tcpmux            1/udp    TCP Port Service Multiplexer
#                          Mark Lottor <MKL&nisc.sri.com>
compressnet       2/tcp    Management Utility
compressnet       2/udp    Management Utility
compressnet       3/tcp    Compression Process
compressnet       3/udp    Compression Process
#                          Bernie Volz <volz&cisco.com>
#                 4/tcp    Unassigned
#                 4/udp    Unassigned
rje               5/tcp    Remote Job Entry
rje               5/udp    Remote Job Entry
#                          Jon Postel <postel&isi.edu>
#                 6/tcp    Unassigned
#                 6/udp    Unassigned
echo              7/tcp    Echo
echo              7/udp    Echo
#                          Jon Postel <postel&isi.edu>
#                 8/tcp    Unassigned
#                 8/udp    Unassigned
discard           9/tcp    Discard
discard           9/udp    Discard
#                          Jon Postel <postel&isi.edu>
discard           9/sctp   Discard
#                          IETF TSVWG
#                          Randall Stewart <rrs&cisco.com>
#                          [RFC4960]
discard           9/dccp   Discard SC:DISC
#                          IETF dccp WG, Eddie Kohler <kohler&cs.ucla.edu>, [RFC4340]
#                10/tcp    Unassigned
#                10/udp    Unassigned
systat           11/tcp    Active Users
systat           11/udp    Active Users
#                          Jon Postel <postel&isi.edu>
#                12/tcp    Unassigned
#                12/udp    Unassigned
daytime          13/tcp    Daytime (RFC 867)
daytime          13/udp    Daytime (RFC 867)
#                          Jon Postel <postel&isi.edu>
#                14/tcp    Unassigned
#                14/udp    Unassigned
#                15/tcp    Unassigned [was netstat]
#                15/udp    Unassigned
#                16/tcp    Unassigned
#                16/udp    Unassigned
qotd             17/tcp    Quote of the Day
qotd             17/udp    Quote of the Day
#                          Jon Postel <postel&isi.edu>
msp              18/tcp    Message Send Protocol
msp              18/udp    Message Send Protocol
#                          Rina Nethaniel <---none--->
chargen          19/tcp    Character Generator
chargen          19/udp    Character Generator
ftp-data         20/tcp    File Transfer [Default Data]
ftp-data         20/udp    File Transfer [Default Data]
#                          Jon Postel <postel&isi.edu>
ftp-data         20/sctp   FTP
#                          IETF TSVWG
#                          Randall Stewart <rrs&cisco.com>
#                          [RFC4960]
ftp              21/tcp    File Transfer [Control]
ftp              21/udp    File Transfer [Control]
#                          Jon Postel <postel&isi.edu>
ftp              21/sctp   FTP
#                          IETF TSVWG
#                          Randall Stewart <rrs&cisco.com>
#                          [RFC4960]
ssh              22/tcp    SSH Remote Login Protocol
ssh              22/udp    SSH Remote Login Protocol
#                          Tatu Ylonen <ylo&cs.hut.fi>
ssh              22/sctp   SSH
#                          IETF TSVWG
#                          Randall Stewart <rrs&cisco.com>
#                          [RFC4960]
```

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------

telnet           23/tcp    Telnet
telnet           23/udp    Telnet
#                          Jon Postel <postel&isi.edu>
                 24/tcp    any private mail system
                 24/udp    any private mail system
#                          Rick Adams <rick&UUNET.UU.NET>
smtp             25/tcp    Simple Mail Transfer
smtp             25/udp    Simple Mail Transfer
#                          Jon Postel <postel&isi.edu>
#                26/tcp    Unassigned
#                26/udp    Unassigned
nsw-fe           27/tcp    NSW User System FE
nsw-fe           27/udp    NSW User System FE
#                          Robert Thomas <BThomas&F.BBN.COM>
#                28/tcp    Unassigned
#                28/udp    Unassigned
msg-icp          29/tcp    MSG ICP
msg-icp          29/udp    MSG ICP
#                          Robert Thomas <BThomas&F.BBN.COM>
#                30/tcp    Unassigned
#                30/udp    Unassigned
msg-auth         31/tcp    MSG Authentication
msg-auth         31/udp    MSG Authentication
#                          Robert Thomas <BThomas&F.BBN.COM>
#                32/tcp    Unassigned
#                32/udp    Unassigned
dsp              33/tcp    Display Support Protocol
dsp              33/udp    Display Support Protocol
#                          Ed Cain <cain&edn-unix.dca.mil>
#                34/tcp    Unassigned
#                34/udp    Unassigned
                 35/tcp    any private printer server
                 35/udp    any private printer server
#                          Jon Postel <postel&isi.edu>
#                36/tcp    Unassigned
#                36/udp    Unassigned
time             37/tcp    Time
time             37/udp    Time
#                          Jon Postel <postel&isi.edu>
rap              38/tcp    Route Access Protocol
rap              38/udp    Route Access Protocol
#                          Robert Ullmann <ariel&world.std.com>
rlp              39/tcp    Resource Location Protocol
rlp              39/udp    Resource Location Protocol
#                          Mike Accetta <MIKE.ACCETTA&CMU-CS-A.EDU>
#                40/tcp    Unassigned
#                40/udp    Unassigned
graphics         41/tcp    Graphics
graphics         41/udp    Graphics
name             42/tcp    Host Name Server
name             42/udp    Host Name Server
nameserver       42/tcp    Host Name Server
nameserver       42/udp    Host Name Server
nicname          43/tcp    Who Is
nicname          43/udp    Who Is
mpm-flags        44/tcp    MPM FLAGS Protocol
mpm-flags        44/udp    MPM FLAGS Protocol
mpm              45/tcp    Message Processing Module [recv]
mpm              45/udp    Message Processing Module [recv]
mpm-snd          46/tcp    MPM [default send]
mpm-snd          46/udp    MPM [default send]
#                          Jon Postel <postel&isi.edu>
ni-ftp           47/tcp    NI FTP
ni-ftp           47/udp    NI FTP
#                          Steve Kille <S.Kille&isode.com>
auditd           48/tcp    Digital Audit Daemon
auditd           48/udp    Digital Audit Daemon
#                          Larry Scott <scott&zk3.dec.com>
tacacs           49/tcp    Login Host Protocol (TACACS)
tacacs           49/udp    Login Host Protocol (TACACS)
#                          Pieter Ditmars <pditmars&BBN.COM>
re-mail-ck       50/tcp    Remote Mail Checking Protocol
re-mail-ck       50/udp    Remote Mail Checking Protocol
#                          Steve Dorner <s-dorner&UIUC.EDU>
la-maint         51/tcp    IMP Logical Address Maintenance
la-maint         51/udp    IMP Logical Address Maintenance
#                          Andy Malis <malis_a&timeplex.com>
xns-time         52/tcp    XNS Time Protocol
xns-time         52/udp    XNS Time Protocol
#                          Susie Armstrong <Armstrong.wbst128@XEROX>
domain           53/tcp    Domain Name Server
domain           53/udp    Domain Name Server
#                          Paul Mockapetris <PVM&ISI.EDU>
xns-ch           54/tcp    XNS Clearinghouse
xns-ch           54/udp    XNS Clearinghouse
#                          Susie Armstrong <Armstrong.wbst128@XEROX>
isi-gl           55/tcp    ISI Graphics Language
isi-gl           55/udp    ISI Graphics Language
xns-auth         56/tcp    XNS Authentication
xns-auth         56/udp    XNS Authentication
#                          Susie Armstrong <Armstrong.wbst128@XEROX>
                 57/tcp    any private terminal access
                 57/udp    any private terminal access
#                          Jon Postel <postel&isi.edu>
```

Keyword	Decimal	Description	References
xns-mail	58/tcp	XNS Mail	
xns-mail	58/udp	XNS Mail	
#		Susie Armstrong <Armstrong.wbst128@XEROX>	
	59/tcp	any private file service	
	59/udp	any private file service	
#		Jon Postel <postel&isi.edu>	
	60/tcp	Unassigned	
	60/udp	Unassigned	
ni-mail	61/tcp	NI MAIL	
ni-mail	61/udp	NI MAIL	
#		Steve Kille <S.Kille&isode.com>	
acas	62/tcp	ACA Services	
acas	62/udp	ACA Services	
#		E. Wald <ewald&via.enet.dec.com>	
whois++	63/tcp	whois++	
whois++	63/udp	whois++	
#		Rickard Schoultz <schoultz&sunet.se>	
covia	64/tcp	Communications Integrator (CI)	
covia	64/udp	Communications Integrator (CI)	
#		Dan Smith <dan.smith&den.galileo.com>	
tacacs-ds	65/tcp	TACACS-Database Service	
tacacs-ds	65/udp	TACACS-Database Service	
#		Kathy Huber <khuber&bbn.com>	
sql*net	66/tcp	Oracle SQL*NET	
sql*net	66/udp	Oracle SQL*NET	
#		Jack Haverty <jhaverty&ORACLE.COM>	
bootps	67/tcp	Bootstrap Protocol Server	
bootps	67/udp	Bootstrap Protocol Server	
bootpc	68/tcp	Bootstrap Protocol Client	
bootpc	68/udp	Bootstrap Protocol Client	
#		Bill Croft <Croft&SUMEX-AIM.STANFORD.EDU>	
tftp	69/tcp	Trivial File Transfer	
tftp	69/udp	Trivial File Transfer	
#		David Clark <ddc&LCS.MIT.EDU>	
gopher	70/tcp	Gopher	
gopher	70/udp	Gopher	
#		Mark McCahill <mpm&boombox.micro.umn.edu>	
netrjs-1	71/tcp	Remote Job Service	
netrjs-1	71/udp	Remote Job Service	
netrjs-2	72/tcp	Remote Job Service	
netrjs-2	72/udp	Remote Job Service	
netrjs-3	73/tcp	Remote Job Service	
netrjs-3	73/udp	Remote Job Service	
netrjs-4	74/tcp	Remote Job Service	
netrjs-4	74/udp	Remote Job Service	
#		Bob Braden <Braden&ISI.EDU>	
	75/tcp	any private dial out service	
	75/udp	any private dial out service	
#		Jon Postel <postel&isi.edu>	
deos	76/tcp	Distributed External Object Store	
deos	76/udp	Distributed External Object Store	
#		Robert Ullmann <ariel&world.std.com>	
	77/tcp	any private RJE service	
	77/udp	any private RJE service	
#		Jon Postel <postel&isi.edu>	
vettcp	78/tcp	vettcp	
vettcp	78/udp	vettcp	
#		Christopher Leong <leong&kolmod.mlo.dec.com>	
finger	79/tcp	Finger	
finger	79/udp	Finger	
#		David Zimmerman <dpz&RUTGERS.EDU>	
http	80/tcp	World Wide Web HTTP	
http	80/udp	World Wide Web HTTP	
www	80/tcp	World Wide Web HTTP	
www	80/udp	World Wide Web HTTP	
www-http	80/tcp	World Wide Web HTTP	
www-http	80/udp	World Wide Web HTTP	
#		Tim Berners-Lee <timbl&W3.org>	
http	80/sctp	HTTP	
#		IETF TSVWG	
#		Randall Stewart <rrs&cisco.com>	
#		[RFC4960]	
#	81	Unassigned (Removed on 2007-09-06)	
xfer	82/tcp	XFER Utility	
xfer	82/udp	XFER Utility	
#		Thomas M. Smith <Thomas.M.Smith&lmco.com>	
mit-ml-dev	83/tcp	MIT ML Device	
mit-ml-dev	83/udp	MIT ML Device	
#		David Reed <--none--->	
ctf	84/tcp	Common Trace Facility	
ctf	84/udp	Common Trace Facility	
#		Hugh Thomas <thomas&oils.enet.dec.com>	
mit-ml-dev	85/tcp	MIT ML Device	
mit-ml-dev	85/udp	MIT ML Device	
#		David Reed <--none--->	
mfcobol	86/tcp	Micro Focus Cobol	
mfcobol	86/udp	Micro Focus Cobol	
#		Simon Edwards <--none--->	
	87/tcp	any private terminal link	
	87/udp	any private terminal link	
#		Jon Postel <postel&isi.edu>	
kerberos	88/tcp	Kerberos	
kerberos	88/udp	Kerberos	
#		B. Clifford Neuman <bcn&isi.edu>	

```
Keyword         Decimal    Description                     References
-------         -------    -----------                     ----------
su-mit-tg        89/tcp    SU/MIT Telnet Gateway
su-mit-tg        89/udp    SU/MIT Telnet Gateway
#                          Mark Crispin <MRC&PANDA.COM>
########## PORT 90 also being used unofficially by Pointcast #########
dnsix            90/tcp    DNSIX Securit Attribute Token Map
dnsix            90/udp    DNSIX Securit Attribute Token Map
#                          Charles Watt <watt&sware.com>
mit-dov          91/tcp    MIT Dover Spooler
mit-dov          91/udp    MIT Dover Spooler
#                          Eliot Moss <EBM&XX.LCS.MIT.EDU>
npp              92/tcp    Network Printing Protocol
npp              92/udp    Network Printing Protocol
#                          Louis Mamakos <louie&sayshell.umd.edu>
dcp              93/tcp    Device Control Protocol
dcp              93/udp    Device Control Protocol
#                          Daniel Tappan <Tappan&BBN.COM>
objcall          94/tcp    Tivoli Object Dispatcher
objcall          94/udp    Tivoli Object Dispatcher
#                          Tom Bereiter <--none--->
supdup           95/tcp    SUPDUP
supdup           95/udp    SUPDUP
#                          Mark Crispin <MRC&PANDA.COM>
dixie            96/tcp    DIXIE Protocol Specification
dixie            96/udp    DIXIE Protocol Specification
#                Tim Howes <Tim.Howes&terminator.cc.umich.edu>
swift-rvf        97/tcp    Swift Remote Virtural File Protocol
swift-rvf        97/udp    Swift Remote Virtural File Protocol
#                          Maurice R. Turcotte
#                          <mailrus!uflorida!rml!dnmrt%rmatl&uunet.UU.NET>
tacnews          98/tcp    TAC News
tacnews          98/udp    TAC News
#                          Jon Postel <postel&isi.edu>
metagram         99/tcp    Metagram Relay
metagram         99/udp    Metagram Relay
#                          Geoff Goodfellow <Geoff&FERNWOOD.MPK.CA.US>
newacct         100/tcp    [unauthorized use]
hostname        101/tcp    NIC Host Name Server
hostname        101/udp    NIC Host Name Server
#                          Jon Postel <postel&isi.edu>
iso-tsap        102/tcp    ISO-TSAP Class 0
iso-tsap        102/udp    ISO-TSAP Class 0
#                          Marshall Rose <mrose&dbc.mtview.ca.us>
gppitnp         103/tcp    Genesis Point-to-Point Trans Net
gppitnp         103/udp    Genesis Point-to-Point Trans Net
acr-nema        104/tcp    ACR-NEMA Digital Imag. & Comm. 300
acr-nema        104/udp    ACR-NEMA Digital Imag. & Comm. 300
#                          Patrick McNamee <--none--->
cso             105/tcp    CCSO name server protocol
cso             105/udp    CCSO name server protocol
#                          Martin Hamilton <martin&mrrl.lut.as.uk>
csnet-ns        105/tcp    Mailbox Name Nameserver
csnet-ns        105/udp    Mailbox Name Nameserver
#                          Marvin Solomon <solomon&CS.WISC.EDU>
3com-tsmux      106/tcp    3COM-TSMUX
3com-tsmux      106/udp    3COM-TSMUX
#                          Jeremy Siegel <jzs&NSD.3Com.COM>
##########      106        Unauthorized use by insecure poppassd protocol
rtelnet         107/tcp    Remote Telnet Service
rtelnet         107/udp    Remote Telnet Service
#                          Jon Postel <postel&isi.edu>
snagas          108/tcp    SNA Gateway Access Server
snagas          108/udp    SNA Gateway Access Server
#                          Kevin Murphy <murphy&sevens.lkg.dec.com>
pop2            109/tcp    Post Office Protocol - Version 2
pop2            109/udp    Post Office Protocol - Version 2
#                          Joyce K. Reynolds <jkrey&isi.edu>
pop3            110/tcp    Post Office Protocol - Version 3
pop3            110/udp    Post Office Protocol - Version 3
#                          Marshall Rose <mrose&dbc.mtview.ca.us>
sunrpc          111/tcp    SUN Remote Procedure Call
sunrpc          111/udp    SUN Remote Procedure Call
#                          Chuck McManis <cmcmanis&freegate.net>
mcidas          112/tcp    McIDAS Data Transmission Protocol
mcidas          112/udp    McIDAS Data Transmission Protocol
#                          Glenn Davis <support&unidata.ucar.edu>
ident           113/tcp
auth            113/tcp    Authentication Service
auth            113/udp    Authentication Service
#                          Mike St. Johns <stjohns&arpa.mil>
#               114        Deprecated June 2004
sftp            115/tcp    Simple File Transfer Protocol
sftp            115/udp    Simple File Transfer Protocol
#                          Mark Lottor <MKL&nisc.sri.com>
ansanotify      116/tcp    ANSA REX Notify
ansanotify      116/udp    ANSA REX Notify
#                          Nicola J. Howarth <njh&ansa.co.uk>
uucp-path       117/tcp    UUCP Path Service
uucp-path       117/udp    UUCP Path Service
sqlserv         118/tcp    SQL Services
sqlserv         118/udp    SQL Services
#                          Larry Barnes <barnes&broke.enet.dec.com>
nntp            119/tcp    Network News Transfer Protocol
nntp            119/udp    Network News Transfer Protocol
#                          Phil Lapsley <phil&UCBARPA.BERKELEY.EDU>
cfdptkt         120/tcp    CFDPTKT
cfdptkt         120/udp    CFDPTKT
```

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
#                          John Ioannidis <ji&close.cs.columbia.ed>
erpc            121/tcp    Encore Expedited Remote Pro.Call
erpc            121/udp    Encore Expedited Remote Pro.Call
#                          Jack O'Neil <---none--->
smakynet        122/tcp    SMAKYNET
smakynet        122/udp    SMAKYNET
#                          Pierre Arnaud <pierre.arnaud&iname.com>
ntp             123/tcp    Network Time Protocol
ntp             123/udp    Network Time Protocol
#                          Dave Mills <Mills&HUEY.UDEL.EDU>
ansatrader      124/tcp    ANSA REX Trader
ansatrader      124/udp    ANSA REX Trader
#                          Nicola J. Howarth <njh&ansa.co.uk>
locus-map       125/tcp    Locus PC-Interface Net Map Ser
locus-map       125/udp    Locus PC-Interface Net Map Ser
#                          Eric Peterson <lcc.eric&SEAS.UCLA.EDU>
nxedit          126/tcp    NXEdit
nxedit          126/udp    NXEdit
#                       Don Payette <Don.Payette&unisys.com>
##########Port 126 Previously assigned to application below#######
#unitary          126/tcp    Unisys Unitary Login
#unitary          126/udp    Unisys Unitary Login
#                          <feil&kronos.nisd.cam.unisys.com>
##########Port 126 Previously assigned to application above#######
locus-con       127/tcp    Locus PC-Interface Conn Server
locus-con       127/udp    Locus PC-Interface Conn Server
#                          Eric Peterson <lcc.eric&SEAS.UCLA.EDU>
gss-xlicen      128/tcp    GSS X License Verification
gss-xlicen      128/udp    GSS X License Verification
#                          John Light <johnl&gssc.gss.com>
pwdgen          129/tcp    Password Generator Protocol
pwdgen          129/udp    Password Generator Protocol
#                          Frank J. Wacho <WANCHO&WSMR-SIMTEL20.ARMY.MIL>
cisco-fna       130/tcp    cisco FNATIVE
cisco-fna       130/udp    cisco FNATIVE
cisco-tna       131/tcp    cisco TNATIVE
cisco-tna       131/udp    cisco TNATIVE
cisco-sys       132/tcp    cisco SYSMAINT
cisco-sys       132/udp    cisco SYSMAINT
statsrv         133/tcp    Statistics Service
statsrv         133/udp    Statistics Service
#                          Dave Mills <Mills&HUEY.UDEL.EDU>
ingres-net      134/tcp    INGRES-NET Service
ingres-net      134/udp    INGRES-NET Service
#                          Mike Berrow <---none--->
epmap           135/tcp    DCE endpoint resolution
epmap           135/udp    DCE endpoint resolution
#                          Joe Pato <pato&apollo.hp.com>
profile         136/tcp    PROFILE Naming System
profile         136/udp    PROFILE Naming System
#                          Larry Peterson <llp&ARIZONA.EDU>
netbios-ns      137/tcp    NETBIOS Name Service
netbios-ns      137/udp    NETBIOS Name Service
netbios-dgm     138/tcp    NETBIOS Datagram Service
netbios-dgm     138/udp    NETBIOS Datagram Service
netbios-ssn     139/tcp    NETBIOS Session Service
netbios-ssn     139/udp    NETBIOS Session Service
#                          Jon Postel <postel&isi.edu>
emfis-data      140/tcp    EMFIS Data Service
emfis-data      140/udp    EMFIS Data Service
emfis-cntl      141/tcp    EMFIS Control Service
emfis-cntl      141/udp    EMFIS Control Service
#                          Gerd Beling <GBELING&ISI.EDU>
bl-idm          142/tcp    Britton-Lee IDM
bl-idm          142/udp    Britton-Lee IDM
#                          Susie Snitzer <---none--->
imap            143/tcp    Internet Message Access Protocol
imap            143/udp    Internet Message Access Protocol
#                          Mark Crispin <MRC&CAC.Washington.EDU>
uma             144/tcp    Universal Management Architecture
uma             144/udp    Universal Management Architecture
#                          Jay Whitney <jw&powercenter.com>
uaac            145/tcp    UAAC Protocol
uaac            145/udp    UAAC Protocol
#                          David A. Gomberg <gomberg&GATEWAY.MITRE.ORG>
iso-tp0         146/tcp    ISO-IP0
iso-tp0         146/udp    ISO-IP0
iso-ip          147/tcp    ISO-IP
iso-ip          147/udp    ISO-IP
#                          Marshall Rose <mrose&dbc.mtview.ca.us>
jargon          148/tcp    Jargon
jargon          148/udp    Jargon
#                          Bill Weinman <wew&bearnet.com>
aed-512         149/tcp    AED 512 Emulation Service
aed-512         149/udp    AED 512 Emulation Service
#                          Albert G. Broscius <broscius&DSL.CIS.UPENN.EDU>
sql-net         150/tcp    SQL-NET
sql-net         150/udp    SQL-NET
#                          Martin Picard <<---none--->
hems            151/tcp    HEMS
hems            151/udp    HEMS
bftp            152/tcp    Background File Transfer Program
bftp            152/udp    Background File Transfer Program
#                          Annette DeSchon <DESCHON&ISI.EDU>
sgmp            153/tcp    SGMP
sgmp            153/udp    SGMP
```

Keyword	Decimal	Description	References
#		Marty Schoffstahl <schoff&NISC.NYSER.NET>	
netsc-prod	154/tcp	NETSC	
netsc-prod	154/udp	NETSC	
netsc-dev	155/tcp	NETSC	
netsc-dev	155/udp	NETSC	
#		Sergio Heker <heker&JVNCC.CSC.ORG>	
sqlsrv	156/tcp	SQL Service	
sqlsrv	156/udp	SQL Service	
#		Craig Rogers <Rogers&ISI.EDU>	
knet-cmp	157/tcp	KNET/VM Command/Message Protocol	
knet-cmp	157/udp	KNET/VM Command/Message Protocol	
#		Gary S. Malkin <GMALKIN&XYLOGICS.COM>	
pcmail-srv	158/tcp	PCMail Server	
pcmail-srv	158/udp	PCMail Server	
#		Mark L. Lambert <markl&PTT.LCS.MIT.EDU>	
nss-routing	159/tcp	NSS-Routing	
nss-routing	159/udp	NSS-Routing	
#		Yakov Rekhter <Yakov&IBM.COM>	
sgmp-traps	160/tcp	SGMP-TRAPS	
sgmp-traps	160/udp	SGMP-TRAPS	
#		Marty Schoffstahl <schoff&NISC.NYSER.NET>	
snmp	161/tcp	SNMP	
snmp	161/udp	SNMP	
snmptrap	162/tcp	SNMPTRAP	
snmptrap	162/udp	SNMPTRAP	
#		Marshall Rose <mrose&dbc.mtview.ca.us>	
cmip-man	163/tcp	CMIP/TCP Manager	
cmip-man	163/udp	CMIP/TCP Manager	
cmip-agent	164/tcp	CMIP/TCP Agent	
cmip-agent	164/udp	CMIP/TCP Agent	
#		Amatzia Ben-Artzi <---none--->	
xns-courier	165/tcp	Xerox	
xns-courier	165/udp	Xerox	
#		Susie Armstrong <Armstrong.wbst128&XEROX.COM>	
s-net	166/tcp	Sirius Systems	
s-net	166/udp	Sirius Systems	
#		Brian Lloyd <brian&lloyd.com>	
namp	167/tcp	NAMP	
namp	167/udp	NAMP	
#		Marty Schoffstahl <schoff&NISC.NYSER.NET>	
rsvd	168/tcp	RSVD	
rsvd	168/udp	RSVD	
#		Neil Todd <mcvax!ist.co.uk!neil&UUNET.UU.NET>	
send	169/tcp	SEND	
send	169/udp	SEND	
#		William D. Wisner <wisner&HAYES.FAI.ALASKA.EDU>	
print-srv	170/tcp	Network PostScript	
print-srv	170/udp	Network PostScript	
#		Brian Reid <reid&DECWRL.DEC.COM>	
multiplex	171/tcp	Network Innovations Multiplex	
multiplex	171/udp	Network Innovations Multiplex	
cl/1	172/tcp	Network Innovations CL/1	
cl/1	172/udp	Network Innovations CL/1	
#		Kevin DeVault <<---none--->	
xyplex-mux	173/tcp	Xyplex	
xyplex-mux	173/udp	Xyplex	
#		Bob Stewart <STEWART&XYPLEX.COM>	
mailq	174/tcp	MAILQ	
mailq	174/udp	MAILQ	
#		Rayan Zachariassen <rayan&AI.TORONTO.EDU>	
vmnet	175/tcp	VMNET	
vmnet	175/udp	VMNET	
#		Christopher Tengi <tengi&Princeton.EDU>	
genrad-mux	176/tcp	GENRAD-MUX	
genrad-mux	176/udp	GENRAD-MUX	
#		Ron Thornton <thornton&qm7501.genrad.com>	
xdmcp	177/tcp	X Display Manager Control Protocol	
xdmcp	177/udp	X Display Manager Control Protocol	
#		Robert W. Scheifler <RWS&XX.LCS.MIT.EDU>	
nextstep	178/tcp	NextStep Window Server	
nextstep	178/udp	NextStep Window Server	
#		Leo Hourvitz <leo&NEXT.COM>	
bgp	179/tcp	Border Gateway Protocol	
bgp	179/udp	Border Gateway Protocol	
#		Kirk Lougheed <LOUGHEED&MATHOM.CISCO.COM>	
bgp	179/sctp	BGP	
#		IETF TSVWG	
#		Randall Stewart <rrs&cisco.com>	
#		[RFC4960]	
ris	180/tcp	Intergraph	
ris	180/udp	Intergraph	
#		Dave Buehmann <ingr!daveb&UUNET.UU.NET>	
unify	181/tcp	Unify	
unify	181/udp	Unify	
#		Mark Ainsley <ianaportmaster&unify.com>	
audit	182/tcp	Unisys Audit SITP	
audit	182/udp	Unisys Audit SITP	
#		Gil Greenbaum <gcole&nisd.cam.unisys.com>	
ocbinder	183/tcp	OCBinder	
ocbinder	183/udp	OCBinder	
ocserver	184/tcp	OCServer	
ocserver	184/udp	OCServer	

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
#                          Jerrilynn Okamura <--none--->
remote-kis      185/tcp    Remote-KIS
remote-kis      185/udp    Remote-KIS
kis             186/tcp    KIS Protocol
kis             186/udp    KIS Protocol
#                          Ralph Droms <rdroms&NRI.RESTON.VA.US>
aci             187/tcp    Application Communication Interface
aci             187/udp    Application Communication Interface
#                          Rick Carlos <rick.ticipa.csc.ti.com>
mumps           188/tcp    Plus Five's MUMPS
mumps           188/udp    Plus Five's MUMPS
#                          Hokey Stenn <hokey&PLUS5.COM>
qft             189/tcp    Queued File Transport
qft             189/udp    Queued File Transport
#                          Wayne Schroeder <schroeder&SDS.SDSC.EDU>
gacp            190/tcp    Gateway Access Control Protocol
gacp            190/udp    Gateway Access Control Protocol
#                          C. Philip Wood <cpw&LANL.GOV>
prospero        191/tcp    Prospero Directory Service
prospero        191/udp    Prospero Directory Service
#                          B. Clifford Neuman <bcn&isi.edu>
osu-nms         192/tcp    OSU Network Monitoring System
osu-nms         192/udp    OSU Network Monitoring System
#                          Doug Karl <KARL-D&OSU-20.IRCC.OHIO-STATE.EDU>
srmp            193/tcp    Spider Remote Monitoring Protocol
srmp            193/udp    Spider Remote Monitoring Protocol
#                          Ted J. Socolofsky <Teds&SPIDER.CO.UK>
irc             194/tcp    Internet Relay Chat Protocol
irc             194/udp    Internet Relay Chat Protocol
#                          Jarkko Oikarinen <jto&TOLSUN.OULU.FI>
dn6-nlm-aud     195/tcp    DNSIX Network Level Module Audit
dn6-nlm-aud     195/udp    DNSIX Network Level Module Audit
dn6-smm-red     196/tcp    DNSIX Session Mgt Module Audit Redir
dn6-smm-red     196/udp    DNSIX Session Mgt Module Audit Redir
#                          Lawrence Lebahn <DIA3&PAXRV-NES.NAVY.MIL>
dls             197/tcp    Directory Location Service
dls             197/udp    Directory Location Service
dls-mon         198/tcp    Directory Location Service Monitor
dls-mon         198/udp    Directory Location Service Monitor
#                          Scott Bellew <smb&cs.purdue.edu>
smux            199/tcp    SMUX
smux            199/udp    SMUX
#                          Marshall Rose <mrose&dbc.mtview.ca.us>
src             200/tcp    IBM System Resource Controller
src             200/udp    IBM System Resource Controller
#                          Gerald McBrearty <---none--->
at-rtmp         201/tcp    AppleTalk Routing Maintenance
at-rtmp         201/udp    AppleTalk Routing Maintenance
at-nbp          202/tcp    AppleTalk Name Binding
at-nbp          202/udp    AppleTalk Name Binding
at-3            203/tcp    AppleTalk Unused
at-3            203/udp    AppleTalk Unused
at-echo         204/tcp    AppleTalk Echo
at-echo         204/udp    AppleTalk Echo
at-5            205/tcp    AppleTalk Unused
at-5            205/udp    AppleTalk Unused
at-zis          206/tcp    AppleTalk Zone Information
at-zis          206/udp    AppleTalk Zone Information
at-7            207/tcp    AppleTalk Unused
at-7            207/udp    AppleTalk Unused
at-8            208/tcp    AppleTalk Unused
at-8            208/udp    AppleTalk Unused
#                          Rob Chandhok <chandhok&gnome.cs.cmu.edu>
qmtp            209/tcp    The Quick Mail Transfer Protocol
qmtp            209/udp    The Quick Mail Transfer Protocol
#                          Dan Bernstein <djb&silverton.berkeley.edu>
z39.50          210/tcp    ANSI Z39.50
z39.50          210/udp    ANSI Z39.50
#                          Mark H. Needleman <markn&sirsi.com>
914c/g          211/tcp    Texas Instruments 914C/G Terminal
914c/g          211/udp    Texas Instruments 914C/G Terminal
#                          Bill Harrell <---none--->
anet            212/tcp    ATEXSSTR
anet            212/udp    ATEXSSTR
#                          Jim Taylor <taylor&heart.epps.kodak.com>
ipx             213/tcp    IPX
ipx             213/udp    IPX
#                          Don Provan <donp&xlnvax.novell.com>
vmpwscs         214/tcp    VM PWSCS
vmpwscs         214/udp    VM PWSCS
#                          Dan Shia <dset!shia&uunet.UU.NET>
softpc          215/tcp    Insignia Solutions
softpc          215/udp    Insignia Solutions
#                          Martyn Thomas <---none--->
CAIlic          216/tcp    Computer Associates Int'l License Server
CAIlic          216/udp    Computer Associates Int'l License Server
#                          Chuck Spitz <spich04&cai.com>
dbase           217/tcp    dBASE Unix
dbase           217/udp    dBASE Unix
#                          Don Gibson
#                          <sequent!aero!twinsun!ashtate.A-T.COM!dong&uunet.UU.NET>
mpp             218/tcp    Netix Message Posting Protocol
mpp             218/udp    Netix Message Posting Protocol
#                          Shannon Yeh <yeh&netix.com>
uarps           219/tcp    Unisys ARPs
uarps           219/udp    Unisys ARPs
```

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
#                          Ashok Marwaha <---none--->
imap3           220/tcp    Interactive Mail Access Protocol v3
imap3           220/udp    Interactive Mail Access Protocol v3
#                          James Rice <RICE&SUMEX-AIM.STANFORD.EDU>
fln-spx         221/tcp    Berkeley rlogind with SPX auth
fln-spx         221/udp    Berkeley rlogind with SPX auth
rsh-spx         222/tcp    Berkeley rshd with SPX auth
rsh-spx         222/udp    Berkeley rshd with SPX auth
cdc             223/tcp    Certificate Distribution Center
cdc             223/udp    Certificate Distribution Center
#                          Kannan Alagappan <kannan&sejour.enet.dec.com>
########### Possible Conflict of Port 222 with "Masqdialer"##############
### Contact for Masqdialer is Charles Wright <cpwright&villagenet.com>###
masqdialer      224/tcp    masqdialer
masqdialer      224/udp    masqdialer
#                          Charles Wright <cpwright&villagenet.com>
#               225-241    Reserved
#                          Jon Postel <postel&isi.edu>
direct          242/tcp    Direct
direct          242/udp    Direct
#                          Herb Sutter <HerbS&cntc.com>
sur-meas        243/tcp    Survey Measurement
sur-meas        243/udp    Survey Measurement
#                          Dave Clark <ddc&LCS.MIT.EDU>
inbusiness      244/tcp    inbusiness
inbusiness      244/udp    inbusiness
#                          Derrick Hisatake <derrick.i.hisatake&intel.com>
link            245/tcp    LINK
link            245/udp    LINK
dsp3270         246/tcp    Display Systems Protocol
dsp3270         246/udp    Display Systems Protocol
#                          Weldon J. Showalter <Gamma&MINTAKA.DCA.MIL>
subntbcst_tftp  247/tcp    SUBNTBCST_TFTP
subntbcst_tftp  247/udp    SUBNTBCST_TFTP
#                          John Fake <fake&us.ibm.com>
bhfhs           248/tcp    bhfhs
bhfhs           248/udp    bhfhs
#                          John Kelly <johnk&bellhow.com>
#               249-255    Reserved
#                          Jon Postel <postel&isi.edu>
rap             256/tcp    RAP
rap             256/udp    RAP
#                          J.S. Greenfield <greeny&raleigh.ibm.com>
set             257/tcp    Secure Electronic Transaction
set             257/udp    Secure Electronic Transaction
#                          Donald Eastlake <dee3&torque.pothole.com>
#               258        Unassigned (Removed 2006-09-13)
esro-gen        259/tcp    Efficient Short Remote Operations
esro-gen        259/udp    Efficient Short Remote Operations
#                          Mohsen Banan <mohsen&rostam.neda.com>
openport        260/tcp    Openport
openport        260/udp    Openport
#                          John Marland <jmarland&dean.openport.com>
nsiiops         261/tcp    IIOP Name Service over TLS/SSL
nsiiops         261/udp    IIOP Name Service over TLS/SSL
#                          Jeff Stewart <jstewart&netscape.com>
arcisdms        262/tcp    Arcisdms
arcisdms        262/udp    Arcisdms
#                          Russell Crook (rmc&sni.ca>
hdap            263/tcp    HDAP
hdap            263/udp    HDAP
#                          Troy Gau <troy&zyxel.com>
bgmp            264/tcp    BGMP
bgmp            264/udp    BGMP
#                          Dave Thaler <thalerd&eecs.umich.edu>
x-bone-ctl      265/tcp    X-Bone CTL
x-bone-ctl      265/udp    X-Bone CTL
#                          Joe Touch <touch&isi.edu>
sst             266/tcp    SCSI on ST
sst             266/udp    SCSI on ST
#                          Donald D. Woelz <don&genroco.com>
td-service      267/tcp    Tobit David Service Layer
td-service      267/udp    Tobit David Service Layer
td-replica      268/tcp    Tobit David Replica
td-replica      268/udp    Tobit David Replica
#                          Franz-Josef Leuders <development&tobit.com>
manet           269/tcp    MANET Protocols
manet           269/udp    MANET Protocols                [RFC-ietf-manet-iana-07.txt]
#               270-279    Unassigned
http-mgmt       280/tcp    http-mgmt
http-mgmt       280/udp    http-mgmt
#                          Adrian Pell
#                          <PELL_ADRIAN/HP-UnitedKingdom_om6&hplb.hpl.hp.com>
personal-link   281/tcp    Personal Link
personal-link   281/udp    Personal Link
#                          Dan Cummings <doc&cnr.com>
cableport-ax    282/tcp    Cable Port A/X
cableport-ax    282/udp    Cable Port A/X
#                          Craig Langfahl <Craig_J_Langfahl&ccm.ch.intel.com>
rescap          283/tcp    rescap
rescap          283/udp    rescap
#                          Paul Hoffman <phoffman&imc.org>
corerjd         284/tcp    corerjd
corerjd         284/udp    corerjd
```

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
#                          Chris Thornhill <port_contact&cjt.ca>
#               285        Unassigned
fxp             286/tcp    FXP Communication
fxp             286/udp    FXP Communication
#                          James Darnall <james_r_darnall&sbcglobal.net>
k-block         287/tcp    K-BLOCK
k-block         287/udp    K-BLOCK
#                          Simon P Jackson <jacko&kring.co.uk>
#               288-307    Unassigned
Novastorbakcup  308/tcp    Novastor Backup
Novastorbakcup  308/udp    Novastor Backup
#                          Brian Dickman <brian&novastor.com>
entrusttime     309/tcp    EntrustTime
entrusttime     309/udp    EntrustTime
#                          Peter Whittaker <pww&entrust.com>
bhmds           310/tcp    bhmds
bhmds           310/udp    bhmds
#                          John Kelly <johnk&bellhow.com>
asip-webadmin   311/tcp    AppleShare IP WebAdmin
asip-webadmin   311/udp    AppleShare IP WebAdmin
#                          Ann Huang <annhuang&apple.com>
vslmp           312/tcp    VSLMP
vslmp           312/udp    VSLMP
#                          Gerben Wierda <Gerben_Wierda&RnA.nl>
magenta-logic   313/tcp    Magenta Logic
magenta-logic   313/udp    Magenta Logic
#                          Karl Rousseau <kr&netfusion.co.uk>
opalis-robot    314/tcp    Opalis Robot
opalis-robot    314/udp    Opalis Robot
#                          Laurent Domenech, Opalis <ldomenech&opalis.com>
dpsi            315/tcp    DPSI
dpsi            315/udp    DPSI
#                          Tony Scamurra <Tony&DesktopPaging.com>
decauth         316/tcp    decAuth
decauth         316/udp    decAuth
#                          Michael Agishtein <misha&unx.dec.com>
zannet          317/tcp    Zannet
zannet          317/udp    Zannet
#                          Zan Oliphant <zan&accessone.com>
pkix-timestamp  318/tcp    PKIX TimeStamp
pkix-timestamp  318/udp    PKIX TimeStamp
#                          Robert Zuccherato <robert.zuccherato&entrust.com>
ptp-event       319/tcp    PTP Event
ptp-event       319/udp    PTP Event
ptp-general     320/tcp    PTP General
ptp-general     320/udp    PTP General
#                          John Eidson <eidson&hpl.hp.com>
pip             321/tcp    PIP
pip             321/udp    PIP
#                          Gordon Mohr <gojomo&usa.net>
rtsps           322/tcp    RTSPS
rtsps           322/udp    RTSPS
#                          Anders Klemets <anderskl&microsoft.com>
#               323-332    Unassigned
texar           333/tcp    Texar Security Port
texar           333/udp    Texar Security Port
#                          Eugen Bacic <ebacic&texar.com>
#               334-343    Unassigned
pdap            344/tcp    Prospero Data Access Protocol
pdap            344/udp    Prospero Data Access Protocol
#                          B. Clifford Neuman <bcn&isi.edu>
pawserv         345/tcp    Perf Analysis Workbench
pawserv         345/udp    Perf Analysis Workbench
zserv           346/tcp    Zebra server
zserv           346/udp    Zebra server
fatserv         347/tcp    Fatmen Server
fatserv         347/udp    Fatmen Server
csi-sgwp        348/tcp    Cabletron Management Protocol
csi-sgwp        348/udp    Cabletron Management Protocol
mftp            349/tcp    mftp
mftp            349/udp    mftp
#                          Dave Feinleib <davefe&microsoft.com>
matip-type-a    350/tcp    MATIP Type A
matip-type-a    350/udp    MATIP Type A
matip-type-b    351/tcp    MATIP Type B
matip-type-b    351/udp    MATIP Type B
#                          Alain Robert <arobert&par.sita.int>
# The following entry records an unassigned but widespread use
bhoetty         351/tcp    bhoetty (added 5/21/97)
bhoetty         351/udp    bhoetty
#                          John Kelly <johnk&bellhow.com>
dtag-ste-sb     352/tcp    DTAG (assigned long ago)
dtag-ste-sb     352/udp    DTAG
#                          Ruediger Wald <wald&ez-darmstadt.telekom.de>
# The following entry records an unassigned but widespread use
bhoedap4        352/tcp    bhoedap4 (added 5/21/97)
bhoedap4        352/udp    bhoedap4
#                          John Kelly <johnk&bellhow.com>
ndsauth         353/tcp    NDSAUTH
ndsauth         353/udp    NDSAUTH
#                          Jayakumar Ramalingam <jayakumar&novell.com>
bh611           354/tcp    bh611
bh611           354/udp    bh611
#                          John Kelly <johnk&bellhow.com>
datex-asn       355/tcp    DATEX-ASN
datex-asn       355/udp    DATEX-ASN
```

Keyword	Decimal	Description	References
#		Kenneth Vaughn <kvaughn&mail.viggen.com>	
cloanto-net-1	356/tcp	Cloanto Net 1	
cloanto-net-1	356/udp	Cloanto Net 1	
#		Michael Battilana <mcb-iana&cloanto.com>	
bhevent	357/tcp	bhevent	
bhevent	357/udp	bhevent	
#		John Kelly <johnk&bellhow.com>	
shrinkwrap	358/tcp	Shrinkwrap	
shrinkwrap	358/udp	Shrinkwrap	
#		Bill Simpson <wsimpson&greendragon.com>	
nsrmp	359/tcp	Network Security Risk Management Protocol	
nsrmp	359/udp	Network Security Risk Management Protocol	
#		Eric Jacksch <jacksch&tenebris.ca>	
scoi2odialog	360/tcp	scoi2odialog	
scoi2odialog	360/udp	scoi2odialog	
#		Keith Petley <keithp&sco.COM>	
semantix	361/tcp	Semantix	
semantix	361/udp	Semantix	
#		Semantix <xsSupport&semantix.com>	
srssend	362/tcp	SRS Send	
srssend	362/udp	SRS Send	
#		Curt Mayer <curt&emergent.com>	
rsvp_tunnel	363/tcp	RSVP Tunnel	
rsvp_tunnel	363/udp	RSVP Tunnel	
#		Andreas Terzis <terzis&cs.ucla.edu>	
aurora-cmgr	364/tcp	Aurora CMGR	
aurora-cmgr	364/udp	Aurora CMGR	
#		Philip Budne <budne&auroratech.com>	
dtk	365/tcp	DTK	
dtk	365/udp	DTK	
#		Fred Cohen <fc&all.net>	
odmr	366/tcp	ODMR	
odmr	366/udp	ODMR	
#		Randall Gellens <randy&qualcomm.com>	
Mortgageware	367/tcp	MortgageWare	
Mortgageware	367/udp	MortgageWare	
#		Ole Hellevik <oleh&interlinq.com>	
qbikgdp	368/tcp	QbikGDP	
qbikgdp	368/udp	QbikGDP	
#		Adrien de Croy <adrien&qbik.com>	
rpc2portmap	369/tcp	rpc2portmap	
rpc2portmap	369/udp	rpc2portmap	
codaauth2	370/tcp	codaauth2	
codaauth2	370/udp	codaauth2	
#		Robert Watson <robert&cyrus.watson.org>	
clearcase	371/tcp	Clearcase	
clearcase	371/udp	Clearcase	
#		Dave LeBlang <leglang&atria.com>	
ulistproc	372/tcp	ListProcessor	
ulistproc	372/udp	ListProcessor	
#		Anastasios Kotsikonas <tasos&cs.bu.edu>	
legent-1	373/tcp	Legent Corporation	
legent-1	373/udp	Legent Corporation	
legent-2	374/tcp	Legent Corporation	
legent-2	374/udp	Legent Corporation	
#		Keith Boyce <---none--->	
hassle	375/tcp	Hassle	
hassle	375/udp	Hassle	
#		Reinhard Doelz <doelz&comp.bioz.unibas.ch>	
nip	376/tcp	Amiga Envoy Network Inquiry Proto	
nip	376/udp	Amiga Envoy Network Inquiry Proto	
#		Heinz Wrobel <hwrobel&gmx.de>	
tnETOS	377/tcp	NEC Corporation	
tnETOS	377/udp	NEC Corporation	
dsETOS	378/tcp	NEC Corporation	
dsETOS	378/udp	NEC Corporation	
#		Tomoo Fujita <tf&arc.bs1.fc.nec.co.jp>	
is99c	379/tcp	TIA/EIA/IS-99 modem client	
is99c	379/udp	TIA/EIA/IS-99 modem client	
is99s	380/tcp	TIA/EIA/IS-99 modem server	
is99s	380/udp	TIA/EIA/IS-99 modem server	
#		Frank Quick <fquick&qualcomm.com>	
hp-collector	381/tcp	hp performance data collector	
hp-collector	381/udp	hp performance data collector	
hp-managed-node	382/tcp	hp performance data managed node	
hp-managed-node	382/udp	hp performance data managed node	
hp-alarm-mgr	383/tcp	hp performance data alarm manager	
hp-alarm-mgr	383/udp	hp performance data alarm manager	
#		Frank Blakely <frankb&hpptc16.rose.hp.com>	
arns	384/tcp	A Remote Network Server System	
arns	384/udp	A Remote Network Server System	
#		David Hornsby <djh&munnari.OZ.AU>	
ibm-app	385/tcp	IBM Application	
ibm-app	385/udp	IBM Application	
#		Lisa Tomita <---none--->	
asa	386/tcp	ASA Message Router Object Def.	
asa	386/udp	ASA Message Router Object Def.	
#		Steve Laitinen <laitinen&brutus.aa.ab.com>	
aurp	387/tcp	Appletalk Update-Based Routing Pro.	
aurp	387/udp	Appletalk Update-Based Routing Pro.	
#		Chris Ranch <cranch&novell.com>	
unidata-ldm	388/tcp	Unidata LDM	
unidata-ldm	388/udp	Unidata LDM	
#		Glenn Davis <support&unidata.ucar.edu>	
ldap	389/tcp	Lightweight Directory Access Protocol	
ldap	389/udp	Lightweight Directory Access Protocol	

Keyword	Decimal	Description	References
#		Tim Howes <Tim.Howes&terminator.cc.umich.edu>	
uis	390/tcp	UIS	
uis	390/udp	UIS	
#		Ed Barron <---none--->	
synotics-relay	391/tcp	SynOptics SNMP Relay Port	
synotics-relay	391/udp	SynOptics SNMP Relay Port	
synotics-broker	392/tcp	SynOptics Port Broker Port	
synotics-broker	392/udp	SynOptics Port Broker Port	
#		Illan Raab <iraab&synoptics.com>	
meta5	393/tcp	Meta5	
meta5	393/udp	Meta5	
#		Jim Kanzler <jim.kanzler&meta5.com>	
embl-ndt	394/tcp	EMBL Nucleic Data Transfer	
embl-ndt	394/udp	EMBL Nucleic Data Transfer	
#		Peter Gad <peter&bmc.uu.se>	
netcp	395/tcp	NETscout Control Protocol	
netcp	395/udp	NETscout Control Protocol	
#		Anil Singhal <---none--->	
netware-ip	396/tcp	Novell Netware over IP	
netware-ip	396/udp	Novell Netware over IP	
mptn	397/tcp	Multi Protocol Trans. Net.	
mptn	397/udp	Multi Protocol Trans. Net.	
#		Soumitra Sarkar <sarkar&vnet.ibm.com>	
kryptolan	398/tcp	Kryptolan	
kryptolan	398/udp	Kryptolan	
#		Peter de Laval <pdl&sectra.se>	
iso-tsap-c2	399/tcp	ISO Transport Class 2 Non-Control over TCP	
iso-tsap-c2	399/udp	ISO Transport Class 2 Non-Control over UDP	
#		Yanick Pouffary <pouffary&taec.enet.dec.com>	
work-sol	400/tcp	Workstation Solutions	
work-sol	400/udp	Workstation Solutions	
#		Jim Ward <jimw&worksta.com>	
ups	401/tcp	Uninterruptible Power Supply	
ups	401/udp	Uninterruptible Power Supply	
#		Charles Bennett <chuck&benatong.com>	
genie	402/tcp	Genie Protocol	
genie	402/udp	Genie Protocol	
#		Mark Hankin <---none--->	
decap	403/tcp	decap	
decap	403/udp	decap	
nced	404/tcp	nced	
nced	404/udp	nced	
ncld	405/tcp	ncld	
ncld	405/udp	ncld	
#		Richard Jones <---none--->	
imsp	406/tcp	Interactive Mail Support Protocol	
imsp	406/udp	Interactive Mail Support Protocol	
#		John Myers <jgm+&cmu.edu>	
timbuktu	407/tcp	Timbuktu	
timbuktu	407/udp	Timbuktu	
#		Marc Epard <marc&netopia.com>	
prm-sm	408/tcp	Prospero Resource Manager Sys. Man.	
prm-sm	408/udp	Prospero Resource Manager Sys. Man.	
prm-nm	409/tcp	Prospero Resource Manager Node Man.	
prm-nm	409/udp	Prospero Resource Manager Node Man.	
#		B. Clifford Neuman <bcn&isi.edu>	
decladebug	410/tcp	DECLadebug Remote Debug Protocol	
decladebug	410/udp	DECLadebug Remote Debug Protocol	
#		Anthony Berent <anthony.berent&reo.mts.dec.com>	
rmt	411/tcp	Remote MT Protocol	
rmt	411/udp	Remote MT Protocol	
#		Peter Eriksson <pen&lysator.liu.se>	
synoptics-trap	412/tcp	Trap Convention Port	
synoptics-trap	412/udp	Trap Convention Port	
#		Illan Raab <iraab&synoptics.com>	
smsp	413/tcp	Storage Management Services Protocol	
smsp	413/udp	Storage Management Services Protocol	
#		Murthy Srinivas <murthy&novell.com>	
infoseek	414/tcp	InfoSeek	
infoseek	414/udp	InfoSeek	
#		Steve Kirsch <stk&infoseek.com>	
bnet	415/tcp	BNet	
bnet	415/udp	BNet	
#		Jim Mertz <JMertz+RV09&rvdc.unisys.com>	
silverplatter	416/tcp	Silverplatter	
silverplatter	416/udp	Silverplatter	
#		Peter Ciuffetti <petec&silverplatter.com>	
onmux	417/tcp	Onmux	
onmux	417/udp	Onmux	
#		Stephen Hanna <hanna&world.std.com>	
hyper-g	418/tcp	Hyper-G	
hyper-g	418/udp	Hyper-G	
#		Frank Kappe <fkappe&iicm.tu-graz.ac.at>	
ariel1	419/tcp	Ariel 1	
ariel1	419/udp	Ariel 1	
#		Joel Karafin <jkarafin&infotrieve.com>	
smpte	420/tcp	SMPTE	
smpte	420/udp	SMPTE	
#		Si Becker <71362.22&CompuServe.COM>	
ariel2	421/tcp	Ariel 2	
ariel2	421/udp	Ariel 2	
ariel3	422/tcp	Ariel 3	
ariel3	422/udp	Ariel 3	

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
#                          Joel Karafin <jkarafin&infotrieve.com>
opc-job-start   423/tcp    IBM Operations Planning and Control Start
opc-job-start   423/udp    IBM Operations Planning and Control Start
opc-job-track   424/tcp    IBM Operations Planning and Control Track
opc-job-track   424/udp    IBM Operations Planning and Control Track
#                          Conny Larsson  <cocke&VNET.IBM.COM>
icad-el         425/tcp    ICAD
icad-el         425/udp    ICAD
#                          Larry Stone    <lcs&icad.com>
smartsdp        426/tcp    smartsdp
smartsdp        426/udp    smartsdp
#                          Marie-Pierre Belanger <belanger_marie&emc.com>
svrloc          427/tcp    Server Location
svrloc          427/udp    Server Location
#                          <veizades&ftp.com>
ocs_cmu         428/tcp    OCS_CMU
ocs_cmu         428/udp    OCS_CMU
ocs_amu         429/tcp    OCS_AMU
ocs_amu         429/udp    OCS_AMU
#                          Florence Wyman <wyman&peabody.plk.af.mil>
utmpsd          430/tcp    UTMPSD
utmpsd          430/udp    UTMPSD
utmpcd          431/tcp    UTMPCD
utmpcd          431/udp    UTMPCD
iasd            432/tcp    IASD
iasd            432/udp    IASD
#                          Nir Baroz <nbaroz&encore.com>
nnsp            433/tcp    NNSP
nnsp            433/udp    NNSP
#                          Rob Robertson <rob&gangrene.berkeley.edu>
mobileip-agent  434/tcp    MobileIP-Agent
mobileip-agent  434/udp    MobileIP-Agent
mobilip-mn      435/tcp    MobilIP-MN
mobilip-mn      435/udp    MobilIP-MN
#                          Kannan Alagappan <kannan&sejour.lkg.dec.com>
dna-cml         436/tcp    DNA-CML
dna-cml         436/udp    DNA-CML
#                          Dan Flowers <flowers&smaug.lkg.dec.com>
comscm          437/tcp    comscm
comscm          437/udp    comscm
#                          Jim Teague <teague&zso.dec.com>
dsfgw           438/tcp    dsfgw
dsfgw           438/udp    dsfgw
#                          Andy McKeen <mckeen&osf.org>
dasp            439/tcp    dasp      Thomas Obermair
dasp            439/udp    dasp      tommy&inlab.m.eunet.de
#                          Thomas Obermair <tommy&inlab.m.eunet.de>
sgcp            440/tcp    sgcp
sgcp            440/udp    sgcp
#                          Marshall Rose <mrose&dbc.mtview.ca.us>
decvms-sysmgt   441/tcp    decvms-sysmgt
decvms-sysmgt   441/udp    decvms-sysmgt
#                          Lee Barton <barton&star.enet.dec.com>
cvc_hostd       442/tcp    cvc_hostd
cvc_hostd       442/udp    cvc_hostd
#                          Bill Davidson <billd&equalizer.cray.com>
https           443/tcp    http protocol over TLS/SSL
https           443/udp    http protocol over TLS/SSL
#                          Kipp E.B. Hickman <kipp&mcom.com>
https           443/sctp   HTTPS
#                          IETF TSVWG
#                          Randall Stewart <rrs&cisco.com>
#                          [RFC4960]
snpp            444/tcp    Simple Network Paging Protocol
snpp            444/udp    Simple Network Paging Protocol
#                          [RFC1568]
microsoft-ds    445/tcp    Microsoft-DS
microsoft-ds    445/udp    Microsoft-DS
#                          Pradeep Bahl <pradeepb&microsoft.com>
ddm-rdb         446/tcp    DDM-Remote Relational Database Access
ddm-rdb         446/udp    DDM-Remote Relational Database Access
ddm-dfm         447/tcp    DDM-Distributed File Management
ddm-dfm         447/udp    DDM-Distributed File Management
#                          Steven Ritland <srr&us.ibm.com>
ddm-ssl         448/tcp    DDM-Remote DB Access Using Secure Sockets
ddm-ssl         448/udp    DDM-Remote DB Access Using Secure Sockets
#                               Steven Ritland <srr&us.ibm.com>
as-servermap    449/tcp    AS Server Mapper
as-servermap    449/udp    AS Server Mapper
#                          Barbara Foss <BGFOSS&rchvmv.vnet.ibm.com>
tserver         450/tcp    Computer Supported Telecomunication Applications
tserver         450/udp    Computer Supported Telecomunication Applications
#                          Harvey S. Schultz <harvey&acm.org>
sfs-smp-net     451/tcp    Cray Network Semaphore server
sfs-smp-net     451/udp    Cray Network Semaphore server
sfs-config      452/tcp    Cray SFS config server
sfs-config      452/udp    Cray SFS config server
#                          Walter Poxon <wdp&ironwood.cray.com>
creativeserver  453/tcp    CreativeServer
creativeserver  453/udp    CreativeServer
contentserver   454/tcp    ContentServer
contentserver   454/udp    ContentServer
creativepartnr  455/tcp    CreativePartnr
creativepartnr  455/udp    CreativePartnr
```

Keyword	Decimal	Description	References
#		Jesus Ortiz <jesus_ortiz&emotion.com>	
macon-tcp	456/tcp	macon-tcp	
macon-udp	456/udp	macon-udp	
#		Yoshinobu Inoue	
#		<shin&hodaka.mfd.cs.fujitsu.co.jp>	
scohelp	457/tcp	scohelp	
scohelp	457/udp	scohelp	
#		Faith Zack <faithz&sco.com>	
appleqtc	458/tcp	apple quick time	
appleqtc	458/udp	apple quick time	
#		Murali Ranganathan	
#		<murali_ranganathan&quickmail.apple.com>	
ampr-rcmd	459/tcp	ampr-rcmd	
ampr-rcmd	459/udp	ampr-rcmd	
#		Rob Janssen <rob&sys3.pelchl.ampr.org>	
skronk	460/tcp	skronk	
skronk	460/udp	skronk	
#		Henry Strickland <strick&yak.net>	
datasurfsrv	461/tcp	DataRampSrv	
datasurfsrv	461/udp	DataRampSrv	
datasurfsrvsec	462/tcp	DataRampSrvSec	
datasurfsrvsec	462/udp	DataRampSrvSec	
#		Diane Downie <downie&jibe.MV.COM>	
alpes	463/tcp	alpes	
alpes	463/udp	alpes	
#		Alain Durand <Alain.Durand&imag.fr>	
kpasswd	464/tcp	kpasswd	
kpasswd	464/udp	kpasswd	
#		Theodore Ts'o <tytso&MIT.EDU>	
urd	465/tcp	URL Rendesvous Directory for SSM	
igmpv3lite	465/udp	IGMP over UDP for SSM	
#		Toerless Eckert <eckert&cisco.com>	
digital-vrc	466/tcp	digital-vrc	
digital-vrc	466/udp	digital-vrc	
#		Peter Higginson <higginson&mail.dec.com>	
mylex-mapd	467/tcp	mylex-mapd	
mylex-mapd	467/udp	mylex-mapd	
#		Gary Lewis <GaryL&hq.mylex.com>	
photuris	468/tcp	proturis	
photuris	468/udp	proturis	
#		Bill Simpson <Bill.Simpson&um.cc.umich.edu>	
rcp	469/tcp	Radio Control Protocol	
rcp	469/udp	Radio Control Protocol	
#		Jim Jennings +1-708-538-7241	
scx-proxy	470/tcp	scx-proxy	
scx-proxy	470/udp	scx-proxy	
#		Scott Narveson <sjn&cray.com>	
mondex	471/tcp	Mondex	
mondex	471/udp	Mondex	
#		Bill Reding <redingb&nwdt.natwest.co.uk>	
ljk-login	472/tcp	ljk-login	
ljk-login	472/udp	ljk-login	
#		LJK Software, Cambridge, Massachusetts	
#		<support&ljk.com>	
hybrid-pop	473/tcp	hybrid-pop	
hybrid-pop	473/udp	hybrid-pop	
#		Rami Rubin <rami&hybrid.com>	
tn-tl-w1	474/tcp	tn-tl-w1	
tn-tl-w2	474/udp	tn-tl-w2	
#		Ed Kress <eskress&thinknet.com>	
tcpnethaspsrv	475/tcp	tcpnethaspsrv	
tcpnethaspsrv	475/udp	tcpnethaspsrv	
#		Charlie Hava <charlie&aladdin.co.il>	
tn-tl-fdl	476/tcp	tn-tl-fdl	
tn-tl-fdl	476/udp	tn-tl-fdl	
#		Ed Kress <eskress&thinknet.com>	
ss7ns	477/tcp	ss7ns	
ss7ns	477/udp	ss7ns	
#		Jean-Michel URSCH <ursch&taec.enet.dec.com>	
spsc	478/tcp	spsc	
spsc	478/udp	spsc	
#		Mike Rieker <mikea&sp32.com>	
iafserver	479/tcp	iafserver	
iafserver	479/udp	iafserver	
iafdbase	480/tcp	iafdbase	
iafdbase	480/udp	iafdbase	
#		ricky&solect.com <Rick Yazwinski>	
ph	481/tcp	Ph service	
ph	481/udp	Ph service	
#		Roland Hedberg <Roland.Hedberg&umdac.umu.se>	
bgs-nsi	482/tcp	bgs-nsi	
bgs-nsi	482/udp	bgs-nsi	
#		Jon Saperia <saperia&bgs.com>	
ulpnet	483/tcp	ulpnet	
ulpnet	483/udp	ulpnet	
#		Kevin Mooney <kevinm&bfs.unibol.com>	
integra-sme	484/tcp	Integra Software Management Environment	
integra-sme	484/udp	Integra Software Management Environment	
#		Randall Dow <rand&randix.m.isr.de>	
powerburst	485/tcp	Air Soft Power Burst	
powerburst	485/udp	Air Soft Power Burst	
#		<gary&airsoft.com>	
avian	486/tcp	avian	
avian	486/udp	avian	
#		Robert Ullmann	

```
Keyword         Decimal   Description                    References
-------         -------   -----------                    ----------
#                         <Robert_Ullmann/CAM/Lotus.LOTUS&crd.lotus.com>
saft            487/tcp   saft Simple Asynchronous File Transfer
saft            487/udp   saft Simple Asynchronous File Transfer
#                         Ulli Horlacher <framstag&rus.uni-stuttgart.de>
gss-http        488/tcp   gss-http
gss-http        488/udp   gss-http
#                         Doug Rosenthal <rosenthl&krypton.einet.net>
nest-protocol   489/tcp   nest-protocol
nest-protocol   489/udp   nest-protocol
#                         Gilles Gameiro <ggameiro&birdland.com>
micom-pfs       490/tcp   micom-pfs
micom-pfs       490/udp   micom-pfs
#                         David Misunas <DMisunas&micom.com>
go-login        491/tcp   go-login
go-login        491/udp   go-login
#                         Troy Morrison <troy&graphon.com>
ticf-1          492/tcp   Transport Independent Convergence for FNA
ticf-1          492/udp   Transport Independent Convergence for FNA
ticf-2          493/tcp   Transport Independent Convergence for FNA
ticf-2          493/udp   Transport Independent Convergence for FNA
#                         Mamoru Ito <Ito&pcnet.ks.pfu.co.jp>
pov-ray         494/tcp   POV-Ray
pov-ray         494/udp   POV-Ray
#                         POV-Team Co-ordinator
#                         <iana-port.remove-spamguard&povray.org>
intecourier     495/tcp   intecourier
intecourier     495/udp   intecourier
#                         Steve Favor <sfavor&tigger.intecom.com>
pim-rp-disc     496/tcp   PIM-RP-DISC
pim-rp-disc     496/udp   PIM-RP-DISC
#                         Dino Farinacci <dino&cisco.com>
dantz           497/tcp   dantz
dantz           497/udp   dantz
#                         Richard Zulch <richard_zulch&dantz.com>
siam            498/tcp   siam
siam            498/udp   siam
#                         Philippe Gilbert <pgilbert&cal.fr>
iso-ill         499/tcp   ISO ILL Protocol
iso-ill         499/udp   ISO ILL Protocol
#                         Mark H. Needleman <markn&sirsi.com>
isakmp          500/tcp   isakmp
isakmp          500/udp   isakmp
#                         Mark Schertler <mjs&tycho.ncsc.mil>
stmf            501/tcp   STMF
stmf            501/udp   STMF
#                         Alan Ungar <aungar&farradyne.com>
asa-appl-proto  502/tcp   asa-appl-proto
asa-appl-proto  502/udp   asa-appl-proto
#                         Dennis Dube <ddube&modicon.com>
intrinsa        503/tcp   Intrinsa
intrinsa        503/udp   Intrinsa
#                         Robert Ford <robert&intrinsa.com>
citadel         504/tcp   citadel
citadel         504/udp   citadel
#                         Art Cancro <ajc&uncensored.citadel.org>
mailbox-lm      505/tcp   mailbox-lm
mailbox-lm      505/udp   mailbox-lm
#                         Beverly Moody <Beverly_Moody&stercomm.com>
ohimsrv         506/tcp   ohimsrv
ohimsrv         506/udp   ohimsrv
#                         Scott Powell <spowell&openhorizon.com>
crs             507/tcp   crs
crs             507/udp   crs
#                         Brad Wright <bradwr&microsoft.com>
xvttp           508/tcp   xvttp
xvttp           508/udp   xvttp
#                         Keith J. Alphonso <alphonso&ncs-ssc.com>
snare           509/tcp   snare
snare           509/udp   snare
#                         Dennis Batchelder <dennis&capres.com>
fcp             510/tcp   FirstClass Protocol
fcp             510/udp   FirstClass Protocol
#                         Mike Marshburn <paul&softarc.com>
passgo          511/tcp   PassGo
passgo          511/udp   PassGo
#                         John Rainford <jrainford&passgo.com>
exec            512/tcp   remote process execution;
#                         authentication performed using
#                         passwords and UNIX login names
comsat          512/udp
biff            512/udp   used by mail system to notify users
#                         of new mail received; currently
#                         receives messages only from
#                         processes on the same machine
login           513/tcp   remote login a la telnet;
#                         automatic authentication performed
#                         based on priviledged port numbers
#                         and distributed data bases which
#                         identify "authentication domains"
who             513/udp   maintains data bases showing who's
#                         logged in to machines on a local
#                         net and the load average of the
#                         machine
shell           514/tcp   cmd
```

Keyword	Decimal	Description	References
#		like exec, but automatic authentication	
#		is performed as for login server	
syslog	514/udp		
printer	515/tcp	spooler	
printer	515/udp	spooler	
videotex	516/tcp	videotex	
videotex	516/udp	videotex	
#		Daniel Mavrakis <system&venus.mctel.fr>	
talk	517/tcp	like tenex link, but across	
#		machine - unfortunately, doesn't	
#		use link protocol (this is actually	
#		just a rendezvous port from which a	
#		tcp connection is established)	
talk	517/udp	like tenex link, but across	
#		machine - unfortunately, doesn't	
#		use link protocol (this is actually	
#		just a rendezvous port from which a	
#		tcp connection is established)	
ntalk	518/tcp		
ntalk	518/udp		
utime	519/tcp	unixtime	
utime	519/udp	unixtime	
efs	520/tcp	extended file name server	
router	520/udp	local routing process (on site);	
#		uses variant of Xerox NS routing	
#		information protocol - RIP	
ripng	521/tcp	ripng	
ripng	521/udp	ripng	
#		Robert E. Minnear <minnear&ipsilon.com>	
ulp	522/tcp	ULP	
ulp	522/udp	ULP	
#		Max Morris <maxm&MICROSOFT.com>	
ibm-db2	523/tcp	IBM-DB2	
ibm-db2	523/udp	IBM-DB2	
#		Juliana Hsu <jhsu&ca.ibm.com>	
ncp	524/tcp	NCP	
ncp	524/udp	NCP	
#		Don Provan <donp&sjf.novell.com>	
timed	525/tcp	timeserver	
timed	525/udp	timeserver	
tempo	526/tcp	newdate	
tempo	526/udp	newdate	
#		Unknown	
stx	527/tcp	Stock IXChange	
stx	527/udp	Stock IXChange	
custix	528/tcp	Customer IXChange	
custix	528/udp	Customer IXChange	
#		Ferdi Ladeira <ferdil&fraxion.biz>	
irc-serv	529/tcp	IRC-SERV	
irc-serv	529/udp	IRC-SERV	
#		Brian Tackett <cym&acrux.net>	
courier	530/tcp	rpc	
courier	530/udp	rpc	
conference	531/tcp	chat	
conference	531/udp	chat	
netnews	532/tcp	readnews	
netnews	532/udp	readnews	
netwall	533/tcp	for emergency broadcasts	
netwall	533/udp	for emergency broadcasts	
#		Andreas Heidemann <a.heidemann&ais-gmbh.de>	
windream	534/tcp	windream Admin	
windream	534/udp	windream Admin	
#		Uwe Honermann <u.honermann&windream.com>	
iiop	535/tcp	iiop	
iiop	535/udp	iiop	
#		Jeff M.Michaud <michaud&zk3.dec.com>	
opalis-rdv	536/tcp	opalis-rdv	
opalis-rdv	536/udp	opalis-rdv	
#		Laurent Domenech <ldomenech&opalis.com>	
nmsp	537/tcp	Networked Media Streaming Protocol	
nmsp	537/udp	Networked Media Streaming Protocol	
#		Paul Santinelli Jr. <psantinelli&narrative.com>	
gdomap	538/tcp	gdomap	
gdomap	538/udp	gdomap	
#		Richard Frith-Macdonald <richard&brainstorm.co.uk>	
apertus-ldp	539/tcp	Apertus Technologies Load Determination	
apertus-ldp	539/udp	Apertus Technologies Load Determination	
uucp	540/tcp	uucpd	
uucp	540/udp	uucpd	
uucp-rlogin	541/tcp	uucp-rlogin	
uucp-rlogin	541/udp	uucp-rlogin	
#		Stuart Lynne <sl&wimsey.com>	
commerce	542/tcp	commerce	
commerce	542/udp	commerce	
#		Randy Epstein <repstein&hostleasing.net>	
klogin	543/tcp		
klogin	543/udp		
kshell	544/tcp	krcmd	
kshell	544/udp	krcmd	
appleqtcsrvr	545/tcp	appleqtcsrvr	
appleqtcsrvr	545/udp	appleqtcsrvr	
#		Murali Ranganathan	
#		<Murali_Ranganathan&quickmail.apple.com>	
dhcpv6-client	546/tcp	DHCPv6 Client	
dhcpv6-client	546/udp	DHCPv6 Client	
dhcpv6-server	547/tcp	DHCPv6 Server	
dhcpv6-server	547/udp	DHCPv6 Server	

```
Keyword         Decimal    Description                     References
-------         -------    -----------                     ----------
#                          Jim Bound <bound&zk3.dec.com>
afpovertcp      548/tcp    AFP over TCP
afpovertcp      548/udp    AFP over TCP
#                          Leland Wallace <randall&apple.com>
idfp            549/tcp    IDFP
idfp            549/udp    IDFP
#                          Ramana Kovi <ramana&kovi.com>
new-rwho        550/tcp    new-who
new-rwho        550/udp    new-who
cybercash       551/tcp    cybercash
cybercash       551/udp    cybercash
#                          Donald E. Eastlake 3rd <dee&cybercash.com>
devshr-nts      552/tcp    DeviceShare
devshr-nts      552/udp    DeviceShare
#                          Benjamin Rosenberg <brosenberg&advsyscon.com>
pirp            553/tcp    pirp
pirp            553/udp    pirp
#                          D. J. Bernstein <djb&silverton.berkeley.edu>
rtsp            554/tcp    Real Time Streaming Protocol (RTSP)
rtsp            554/udp    Real Time Streaming Protocol (RTSP)
#                          Rob Lanphier <robla&prognet.com>
dsf             555/tcp
dsf             555/udp
remotefs        556/tcp    rfs server
remotefs        556/udp    rfs server
openvms-sysipc  557/tcp    openvms-sysipc
openvms-sysipc  557/udp    openvms-sysipc
#                          Alan Potter <potter&movies.enet.dec.com>
sdnskmp         558/tcp    SDNSKMP
sdnskmp         558/udp    SDNSKMP
teedtap         559/tcp    TEEDTAP
teedtap         559/udp    TEEDTAP
#                          Charlie Limoges <Charlie.Limoges&GDC4S.com>
rmonitor        560/tcp    rmonitord
rmonitor        560/udp    rmonitord
monitor         561/tcp
monitor         561/udp
chshell         562/tcp    chcmd
chshell         562/udp    chcmd
nntps           563/tcp    nntp protocol over TLS/SSL (was snntp)
nntps           563/udp    nntp protocol over TLS/SSL (was snntp)
#                          Kipp E.B. Hickman <kipp&netscape.com>
9pfs            564/tcp    plan 9 file service
9pfs            564/udp    plan 9 file service
whoami          565/tcp    whoami
whoami          565/udp    whoami
streettalk      566/tcp    streettalk
streettalk      566/udp    streettalk
banyan-rpc      567/tcp    banyan-rpc
banyan-rpc      567/udp    banyan-rpc
#                          Tom Lemaire <toml&banyan.com>
ms-shuttle      568/tcp    microsoft shuttle
ms-shuttle      568/udp    microsoft shuttle
#                          Rudolph Balaz <rudolphb&microsoft.com>
ms-rome         569/tcp    microsoft rome
ms-rome         569/udp    microsoft rome
#                          Rudolph Balaz <rudolphb&microsoft.com>
meter           570/tcp    demon
meter           570/udp    demon
meter         571/tcp    udemon
meter         571/udp    udemon
sonar           572/tcp    sonar
sonar           572/udp    sonar
#                          Keith Moore <moore&cs.utk.edu>
banyan-vip      573/tcp    banyan-vip
banyan-vip      573/udp    banyan-vip
#                          Denis Leclerc <DLeclerc&banyan.com>
ftp-agent       574/tcp    FTP Software Agent System
ftp-agent       574/udp    FTP Software Agent System
#                          Michael S. Greenberg <arnoff&ftp.com>
vemmi           575/tcp    VEMMI
vemmi           575/udp    VEMMI
#                          Daniel Mavrakis <mavrakis&mctel.fr>
ipcd            576/tcp    ipcd
ipcd            576/udp    ipcd
vnas            577/tcp    vnas
vnas            577/udp    vnas
ipdd            578/tcp    ipdd
ipdd            578/udp    ipdd
#                          Jay Farhat <jfarhat&ipass.com>
decbsrv         579/tcp    decbsrv
decbsrv         579/udp    decbsrv
#                          Rudi Martin <movies::martin"@movies.enet.dec.com>
sntp-heartbeat  580/tcp    SNTP HEARTBEAT
sntp-heartbeat  580/udp    SNTP HEARTBEAT
#                          Louis Mamakos <louie&uu.net>
bdp             581/tcp    Bundle Discovery Protocol
bdp             581/udp    Bundle Discovery Protocol
#                          Gary Malkin <gmalkin&xylogics.com>
scc-security    582/tcp    SCC Security
scc-security    582/udp    SCC Security
#                          Prashant Dholakia <prashant&semaphorecom.com>
philips-vc      583/tcp    Philips Video-Conferencing
philips-vc      583/udp    Philips Video-Conferencing
#                          Janna Chang <janna&pmc.philips.com>
keyserver       584/tcp    Key Server
keyserver       584/udp    Key Server
```

Keyword	Decimal	Description	References
#		Gary Howland <gary&systemics.com>	
#	585	De-registered (25 April 2006)	
#		Use of 585 is not recommended, use 993 instead	
password-chg	586/tcp	Password Change	
password-chg	586/udp	Password Change	
submission	587/tcp	Submission	
submission	587/udp	Submission	
#		[RFC4409]	
cal	588/tcp	CAL	
cal	588/udp	CAL	
#		Myron Hattig <Myron_Hattig&ccm.jf.intel.com>	
eyelink	589/tcp	EyeLink	
eyelink	589/udp	EyeLink	
#		Dave Stampe <dstampe&psych.toronto.edu>	
tns-cml	590/tcp	TNS CML	
tns-cml	590/udp	TNS CML	
#		Jerome Albin <albin&taec.enet.dec.com>	
http-alt	591/tcp	FileMaker, Inc. - HTTP Alternate (see Port 80)	
http-alt	591/udp	FileMaker, Inc. - HTTP Alternate (see Port 80)	
#		Clay Maeckel <clay_maeckel&filemaker.com>	
eudora-set	592/tcp	Eudora Set	
eudora-set	592/udp	Eudora Set	
#		Randall Gellens <randy&qualcomm.com>	
http-rpc-epmap	593/tcp	HTTP RPC Ep Map	
http-rpc-epmap	593/udp	HTTP RPC Ep Map	
#		Edward Reus <edwardr&microsoft.com>	
tpip	594/tcp	TPIP	
tpip	594/udp	TPIP	
#		Brad Spear <spear&platinum.com>	
cab-protocol	595/tcp	CAB Protocol	
cab-protocol	595/udp	CAB Protocol	
#		Winston Hetherington	
smsd	596/tcp	SMSD	
smsd	596/udp	SMSD	
#		Wayne Barlow <web&unx.dec.com>	
Ptcnameservice	597/tcp	PTC Name Service	
Ptcnameservice	597/udp	PTC Name Service	
#		Yuri Machkasov <yuri&ptc.com>	
sco-websrvrmg3	598/tcp	SCO Web Server Manager 3	
sco-websrvrmg3	598/udp	SCO Web Server Manager 3	
#		Simon Baldwin <simonb&sco.com>	
acp	599/tcp	Aeolon Core Protocol	
acp	599/udp	Aeolon Core Protocol	
#		Michael Alyn Miller <iana&aeolon.com>	
ipcserver	600/tcp	Sun IPC server	
ipcserver	600/udp	Sun IPC server	
#		Bill Schiefelbein <schief&aspen.cray.com>	
syslog-conn	601/tcp	Reliable Syslog Service	
syslog-conn	601/udp	Reliable Syslog Service	
#		RFC 3195	
xmlrpc-beep	602/tcp	XML-RPC over BEEP	
xmlrpc-beep	602/udp	XML-RPC over BEEP	
#		RFC3529 <ftp://ftp.isi.edu/in-notes/rfc3529.txt> March 2003	
idxp	603/tcp	IDXP	
idxp	603/udp	IDXP	
#		RFC4767	
tunnel	604/tcp	TUNNEL	
tunnel	604/udp	TUNNEL	
#		RFC3620	
soap-beep	605/tcp	SOAP over BEEP	
soap-beep	605/udp	SOAP over BEEP	
#		RFC3288 <ftp://ftp.isi.edu/in-notes/rfc3288.txt> April 2002	
urm	606/tcp	Cray Unified Resource Manager	
urm	606/udp	Cray Unified Resource Manager	
nqs	607/tcp	nqs	
nqs	607/udp	nqs	
#		Bill Schiefelbein <schief&aspen.cray.com>	
sift-uft	608/tcp	Sender-Initiated/Unsolicited File Transfer	
sift-uft	608/udp	Sender-Initiated/Unsolicited File Transfer	
#		Rick Troth <troth&rice.edu>	
npmp-trap	609/tcp	npmp-trap	
npmp-trap	609/udp	npmp-trap	
npmp-local	610/tcp	npmp-local	
npmp-local	610/udp	npmp-local	
npmp-gui	611/tcp	npmp-gui	
npmp-gui	611/udp	npmp-gui	
#		John Barnes <jbarnes&crl.com>	
hmmp-ind	612/tcp	HMMP Indication	
hmmp-ind	612/udp	HMMP Indication	
hmmp-op	613/tcp	HMMP Operation	
hmmp-op	613/udp	HMMP Operation	
#		Andrew Sinclair <andrsin&microsoft.com>	
sshell	614/tcp	SSLshell	
sshell	614/udp	SSLshell	
#		Simon J. Gerraty <sjg&quick.com.au>	
sco-inetmgr	615/tcp	Internet Configuration Manager	
sco-inetmgr	615/udp	Internet Configuration Manager	
sco-sysmgr	616/tcp	SCO System Administration Server	
sco-sysmgr	616/udp	SCO System Administration Server	
sco-dtmgr	617/tcp	SCO Desktop Administration Server	
sco-dtmgr	617/udp	SCO Desktop Administration Server	
#		Christopher Durham <chrisdu&sco.com>	
dei-icda	618/tcp	DEI-ICDA	
dei-icda	618/udp	DEI-ICDA	
#		David Turner <digital&Quetico.tbaytel.net>	
compaq-evm	619/tcp	Compaq EVM	
compaq-evm	619/udp	Compaq EVM	

Keyword	Decimal	Description	References
#		Jem Treadwell <Jem.Treadwell&compaq.com>	
sco-websrvrmgr	620/tcp	SCO WebServer Manager	
sco-websrvrmgr	620/udp	SCO WebServer Manager	
#		Christopher Durham <chrisdu&sco.com>	
escp-ip	621/tcp	ESCP	
escp-ip	621/udp	ESCP	
#		Lai Zit Seng <lzs&pobox.com>	
Collaborator	622/tcp	Collaborator	
Collaborator	622/udp	Collaborator	
#		Johnson Davis <johnsond&opteamasoft.com>	
oob-ws-http	623/tcp	DMTF out-of-band web services management protocol	
#		Jim Davis <jim.davis&wbemsolutions.com> June 2007	
asf-rmcp	623/udp	ASF Remote Management and Control Protocol	
#		Carl First <Carl.L.First&intel.com>	
cryptoadmin	624/tcp	Crypto Admin	
cryptoadmin	624/udp	Crypto Admin	
#		Tony Walker <tony&cryptocard.com>	
dec_dlm	625/tcp	DEC DLM	
dec_dlm	625/udp	DEC DLM	
#		Rudi Martin <Rudi.Martin&edo.mts.dec.com>	
asia	626/tcp	ASIA	
asia	626/udp	ASIA	
#		Michael Dasenbrock <dasenbro&apple.com>	
passgo-tivoli	627/tcp	PassGo Tivoli	
passgo-tivoli	627/udp	PassGo Tivoli	
#		John Rainford <john.rainford&passgo.com>	
qmqp	628/tcp	QMQP	
qmqp	628/udp	QMQP	
#		Dan Bernstein <djb&cr.yp.to>	
3com-amp3	629/tcp	3Com AMP3	
3com-amp3	629/udp	3Com AMP3	
#		Prakash Banthia <prakash_banthia&3com.com>	
rda	630/tcp	RDA	
rda	630/udp	RDA	
#		John Hadjioannou <john&minster.co.uk>	
ipp	631/tcp	IPP (Internet Printing Protocol)	
ipp	631/udp	IPP (Internet Printing Protocol)	
#		Carl-Uno Manros <manros&cp10.es.xerox.com>	
bmpp	632/tcp	bmpp	
bmpp	632/udp	bmpp	
#		Troy Rollo <troy&kroll.corvu.com.au>	
servstat	633/tcp	Service Status update (Sterling Software)	
servstat	633/udp	Service Status update (Sterling Software)	
#		Greg Rose <Greg_Rose&sydney.sterling.com>	
ginad	634/tcp	ginad	
ginad	634/udp	ginad	
#		Mark Crother <mark&eis.calstate.edu>	
rlzdbase	635/tcp	RLZ DBase	
rlzdbase	635/udp	RLZ DBase	
#		Michael Ginn <ginn&tyxar.com>	
ldaps	636/tcp	ldap protocol over TLS/SSL (was sldap)	
ldaps	636/udp	ldap protocol over TLS/SSL (was sldap)	
#		Pat Richard <patr&xcert.com>	
lanserver	637/tcp	lanserver	
lanserver	637/udp	lanserver	
#		Chris Larsson <clarsson&VNET.IBM.COM>	
mcns-sec	638/tcp	mcns-sec	
mcns-sec	638/udp	mcns-sec	
#		Kaz Ozawa <k.ozawa&cablelabs.com>	
msdp	639/tcp	MSDP	
msdp	639/udp	MSDP	
#		Dino Farinacci <dino&cisco.com>	
entrust-sps	640/tcp	entrust-sps	
entrust-sps	640/udp	entrust-sps	
#		Marek Buchler <Marek.Buchler&entrust.com>	
repcmd	641/tcp	repcmd	
repcmd	641/udp	repcmd	
#		Scott Dale <scott&Replicase.com>	
esro-emsdp	642/tcp	ESRO-EMSDP V1.3	
esro-emsdp	642/udp	ESRO-EMSDP V1.3	
#		Mohsen Banan <mohsen&neda.com>	
sanity	643/tcp	SANity	
sanity	643/udp	SANity	
#		Peter Viscarola <PeterGV&osr.com>	
dwr	644/tcp	dwr	
dwr	644/udp	dwr	
#		Bill Fenner <fenner&parc.xerox.com>	
pssc	645/tcp	PSSC	
pssc	645/udp	PSSC	
#		Egon Meier-Engelen <egon.meier-engelen&dlr.de>	
ldp	646/tcp	LDP	
ldp	646/udp	LDP	
#		Bob Thomas <rhthomas&cisco.com>	
dhcp-failover	647/tcp	DHCP Failover	
dhcp-failover	647/udp	DHCP Failover	
#		Bernard Volz <volz&cisco.com>	
rrp	648/tcp	Registry Registrar Protocol (RRP)	
rrp	648/udp	Registry Registrar Protocol (RRP)	
#		Scott Hollenbeck <shollenb&netsol.com>	
cadview-3d	649/tcp	Cadview-3d - streaming 3d models over the internet	
cadview-3d	649/udp	Cadview-3d - streaming 3d models over the internet	
#		David Cooper <david.cooper&oracle.com>	
obex	650/tcp	OBEX	
obex	650/udp	OBEX	
#		Jeff Garbers <FJG030&email.mot.com>	
ieee-mms	651/tcp	IEEE MMS	
ieee-mms	651/udp	IEEE MMS	

Keyword	Decimal	Description	References
#		Curtis Anderson <canderson&turbolinux.com>	
hello-port	652/tcp	HELLO_PORT	
hello-port	652/udp	HELLO_PORT	
#		Patrick Cipiere <Patrick.Cipiere&UDcast.com>	
repscmd	653/tcp	RepCmd	
repscmd	653/udp	RepCmd	
#		Scott Dale <scott&tioga.com>	
aodv	654/tcp	AODV	
aodv	654/udp	AODV	
#		Charles Perkins <cperkins&eng.sun.com>	
tinc	655/tcp	TINC	
tinc	655/udp	TINC	
#		Ivo Timmermans <itimmermans&bigfoot.com>	
spmp	656/tcp	SPMP	
spmp	656/udp	SPMP	
#		Jakob Kaivo <jkaivo&nodomainname.net>	
rmc	657/tcp	RMC	
rmc	657/udp	RMC	
#		Michael Schmidt <mmaass&us.ibm.com>	
tenfold	658/tcp	TenFold	
tenfold	658/udp	TenFold	
#		Louis Olszyk <lolszyk&10fold.com>	
#	659	Removed (2001-06-06)	
mac-srvr-admin	660/tcp	MacOS Server Admin	
mac-srvr-admin	660/udp	MacOS Server Admin	
#		Forest Hill <forest&apple.com>	
hap	661/tcp	HAP	
hap	661/udp	HAP	
#		Igor Plotnikov <igor&uroam.com>	
pftp	662/tcp	PFTP	
pftp	662/udp	PFTP	
#		Ben Schluricke <support&pftp.de>	
purenoise	663/tcp	PureNoise	
purenoise	663/udp	PureNoise	
#		Sam Osa <pristine&mailcity.com>	
oob-ws-https	664/tcp	DMTF out-of-band secure web services management protocol	
#		Jim Davis <jim.davis&wbemsolutions.com> June 2007	
asf-secure-rmcp	664/udp	ASF Secure Remote Management and Control Protocol	
#		Carl First <Carl.L.First&intel.com>	
sun-dr	665/tcp	Sun DR	
sun-dr	665/udp	Sun DR	
#		Harinder Bhasin <Harinder.Bhasin&Sun.COM>	
mdqs	666/tcp		
mdqs	666/udp		
doom	666/tcp	doom Id Software	
doom	666/udp	doom Id Software	
#		<ddt&idcube.idsoftware.com>	
disclose	667/tcp	campaign contribution disclosures - SDR Technologies	
disclose	667/udp	campaign contribution disclosures - SDR Technologies	
#		Jim Dixon <jim&lambda.com>	
mecomm	668/tcp	MeComm	
mecomm	668/udp	MeComm	
meregister	669/tcp	MeRegister	
meregister	669/udp	MeRegister	
#		Armin Sawusch <armin&esdl.esd.de>	
vacdsm-sws	670/tcp	VACDSM-SWS	
vacdsm-sws	670/udp	VACDSM-SWS	
vacdsm-app	671/tcp	VACDSM-APP	
vacdsm-app	671/udp	VACDSM-APP	
vpps-qua	672/tcp	VPPS-QUA	
vpps-qua	672/udp	VPPS-QUA	
cimplex	673/tcp	CIMPLEX	
cimplex	673/udp	CIMPLEX	
#		Ulysses G. Smith Jr. <ugsmith&cesi.com>	
acap	674/tcp	ACAP	
acap	674/udp	ACAP	
#		Chris Newman <chris.newman&sun.com>	
dctp	675/tcp	DCTP	
dctp	675/udp	DCTP	
#		Andre Kramer <Andre.Kramer&ansa.co.uk>	
vpps-via	676/tcp	VPPS Via	
vpps-via	676/udp	VPPS Via	
#		Ulysses G. Smith Jr. <ugsmith&cesi.com>	
vpp	677/tcp	Virtual Presence Protocol	
vpp	677/udp	Virtual Presence Protocol	
#		Klaus Wolf <wolf&cobrow.com>	
ggf-ncp	678/tcp	GNU Generation Foundation NCP	
ggf-ncp	678/udp	GNU Generation Foundation NCP	
#		Noah Paul <noahp&altavista.net>	
mrm	679/tcp	MRM	
mrm	679/udp	MRM	
#		Liming Wei <lwei&cisco.com>	
entrust-aaas	680/tcp	entrust-aaas	
entrust-aaas	680/udp	entrust-aaas	
entrust-aams	681/tcp	entrust-aams	
entrust-aams	681/udp	entrust-aams	
#		Adrian Mancini <adrian.mancini&entrust.com>	
xfr	682/tcp	XFR	
xfr	682/udp	XFR	
#		Noah Paul <noahp&ultranet.com>	
corba-iiop	683/tcp	CORBA IIOP	
corba-iiop	683/udp	CORBA IIOP	
corba-iiop-ssl	684/tcp	CORBA IIOP SSL	
corba-iiop-ssl	684/udp	CORBA IIOP SSL	
#		Andrew Watson <andrew&omg.org>	
mdc-portmapper	685/tcp	MDC Port Mapper	
mdc-portmapper	685/udp	MDC Port Mapper	

Keyword	Decimal	Description	References
#		Noah Paul <noahp&altavista.net>	
hcp-wismar	686/tcp	Hardware Control Protocol Wismar	
hcp-wismar	686/udp	Hardware Control Protocol Wismar	
#		David Merchant <d.f.merchant&livjm.ac.uk>	
Asipregistry	687/tcp	asipregistry	
Asipregistry	687/udp	asipregistry	
#		Erik Sea <sea&apple.com>	
realm-rusd	688/tcp	ApplianceWare managment protocol	
realm-rusd	688/udp	ApplianceWare managment protocol	
#		Stacy Kenworthy <skenworthy&applianceware.com>	
nmap	689/tcp	NMAP	
nmap	689/udp	NMAP	
#		Peter Dennis Bartok <peter&novonyx.com>	
vatp	690/tcp	Velazquez Application Transfer Protocol	
vatp	690/udp	Velazquez Application Transfer Protocol	
#		Velneo <velneo&velneo.com>	
msexch-routing	691/tcp	MS Exchange Routing	
msexch-routing	691/udp	MS Exchange Routing	
#		David Lemson <dlemson&microsoft.com>	
hyperwave-isp	692/tcp	Hyperwave-ISP	
hyperwave-isp	692/udp	Hyperwave-ISP	
#		Gerald Mesaric <gmesaric&hyperwave.com>	
connendp	693/tcp	almanid Connection Endpoint	
connendp	693/udp	almanid Connection Endpoint	
#		Ronny Bremer <rbremer&almanid.com>	
ha-cluster	694/tcp	ha-cluster	
ha-cluster	694/udp	ha-cluster	
#		Alan Robertson <alanr&unix.sh>	
ieee-mms-ssl	695/tcp	IEEE-MMS-SSL	
ieee-mms-ssl	695/udp	IEEE-MMS-SSL	
#		Curtis Anderson <ecanderson&turbolinux.com>	
rushd	696/tcp	RUSHD	
rushd	696/udp	RUSHD	
#		Greg Ercolano <erco&netcom.com>	
uuidgen	697/tcp	UUIDGEN	
uuidgen	697/udp	UUIDGEN	
#		James Falkner <james.falkner&sun.com>	
olsr	698/tcp	OLSR	
olsr	698/udp	OLSR	
#		Thomas Clausen <thomas.clausen&inria.fr>	
accessnetwork	699/tcp	Access Network	
accessnetwork	699/udp	Access Network	
#		Yingchun Xu <Yingchun_Xu&3com.com>	
epp	700/tcp	Extensible Provisioning Protocol	
epp	700/udp	Extensible Provisioning Protocol	
#		[RFC4934]	
lmp	701/tcp	Link Management Protocol (LMP)	
lmp	701/udp	Link Management Protocol (LMP)	
#		[RFC4204]	
iris-beep	702/tcp	IRIS over BEEP	
iris-beep	702/udp	IRIS over BEEP	
#		[RFC3983]	
#	703	Unassigned	
elcsd	704/tcp	errlog copy/server daemon	
elcsd	704/udp	errlog copy/server daemon	
agentx	705/tcp	AgentX	
agentx	705/udp	AgentX	
#		Bob Natale <bob.natale&appliedsnmp.com>	
silc	706/tcp	SILC	
silc	706/udp	SILC	
#		Pekka Riikonen <priikone&poseidon.pspt.fi>	
borland-dsj	707/tcp	Borland DSJ	
borland-dsj	707/udp	Borland DSJ	
#		Gerg Cole <gcole&corp.borland.com>	
#	708	Unassigned	
entrust-kmsh	709/tcp	Entrust Key Management Service Handler	
entrust-kmsh	709/udp	Entrust Key Management Service Handler	
entrust-ash	710/tcp	Entrust Administration Service Handler	
entrust-ash	710/udp	Entrust Administration Service Handler	
#		Peter Whittaker <pww&entrust.com>	
cisco-tdp	711/tcp	Cisco TDP	
cisco-tdp	711/udp	Cisco TDP	
#		Bruce Davie <bsd&cisco.com>	
tbrpf	712/tcp	TBRPF	
tbrpf	712/udp	TBRPF	
#		RFC3684	
iris-xpc	713/tcp	IRIS over XPC	
iris-xpc	713/udp	IRIS over XPC	
iris-xpcs	714/tcp	IRIS over XPCS	
iris-xpcs	714/udp	IRIS over XPCS	
#		[RFC4992]	
iris-lwz	715/tcp	IRIS-LWZ	
iris-lwz	715/udp	IRIS-LWZ	
#		[RFC4993]	
pana	716/udp	PANA Messages	
#		[RFC-ietf-pana-pana-18.txt]	
#	717-728	Unassigned	
netviewdm1	729/tcp	IBM NetView DM/6000 Server/Client	
netviewdm1	729/udp	IBM NetView DM/6000 Server/Client	
netviewdm2	730/tcp	IBM NetView DM/6000 send/tcp	
netviewdm2	730/udp	IBM NetView DM/6000 send/tcp	
netviewdm3	731/tcp	IBM NetView DM/6000 receive/tcp	
netviewdm3	731/udp	IBM NetView DM/6000 receive/tcp	
#		Philippe Binet (phbinet&vnet.IBM.COM)	
#	732-740	Unassigned	
netgw	741/tcp	netGW	
netgw	741/udp	netGW	

```
Keyword         Decimal   Description                    References
-------         -------   -----------                    ----------
#                         Oliver Korfmacher (okorf&netcs.com)
netrcs          742/tcp   Network based Rev. Cont. Sys.
netrcs          742/udp   Network based Rev. Cont. Sys.
#                         Gordon C. Galligher <gorpong&ping.chi.il.us>
#               743       Unassigned
flexlm          744/tcp   Flexible License Manager
flexlm          744/udp   Flexible License Manager
#                         Matt Christiano
#                         <globes@matt&oliveb.atc.olivetti.com>
#               745-746   Unassigned
fujitsu-dev     747/tcp   Fujitsu Device Control
fujitsu-dev     747/udp   Fujitsu Device Control
ris-cm          748/tcp   Russell Info Sci Calendar Manager
ris-cm          748/udp   Russell Info Sci Calendar Manager
kerberos-adm    749/tcp   kerberos administration
kerberos-adm    749/udp   kerberos administration
rfile           750/tcp
loadav          750/udp
kerberos-iv     750/udp   kerberos version iv
#                         Martin Hamilton <martin&mrrl.lut.as.uk>
pump            751/tcp
pump            751/udp
qrh             752/tcp
qrh             752/udp
rrh             753/tcp
rrh             753/udp
tell            754/tcp   send
tell            754/udp   send
#                         Josyula R. Rao <jrrao&watson.ibm.com>
#               755-756   Unassigned
nlogin          758/tcp
nlogin          758/udp
con             759/tcp
con             759/udp
ns              760/tcp
ns              760/udp
rxe             761/tcp
rxe             761/udp
quotad          762/tcp
quotad          762/udp
cycleserv       763/tcp
cycleserv       763/udp
omserv          764/tcp
omserv          764/udp
webster         765/tcp
webster         765/udp
#                         Josyula R. Rao <jrrao&watson.ibm.com>
#               766       Unassigned
phonebook       767/tcp   phone
phonebook       767/udp   phone
#                         Josyula R. Rao <jrrao&watson.ibm.com>
#               768       Unassigned
vid             769/tcp
vid             769/udp
cadlock         770/tcp
cadlock         770/udp
rtip            771/tcp
rtip            771/udp
cycleserv2      772/tcp
cycleserv2      772/udp
submit          773/tcp
notify          773/udp
rpasswd         774/tcp
acmaint_dbd     774/udp
entomb          775/tcp
acmaint_transd  775/udp
wpages          776/tcp
wpages          776/udp
#                         Josyula R. Rao <jrrao&watson.ibm.com>
multiling-http  777/tcp   Multiling HTTP
multiling-http  777/udp   Multiling HTTP
#                         Alejandro Bonet <babel&ctv.es>
#               778-779   Unassigned
wpgs            780/tcp
wpgs            780/udp
#                         Josyula R. Rao <jrrao&watson.ibm.com>
#               781-785   Unassigned
#               786       Unassigned (Removed 2002-05-08)
#               787       Unassigned (Removed 2002-10-08)
#               788-799   Unassigned
mdbs_daemon     800/tcp
mdbs_daemon     800/udp
device          801/tcp
device          801/udp
#               802-809   Unassigned
fcp-udp         810/tcp   FCP
fcp-udp         810/udp   FCP Datagram
#                         Paul Whittemore <paul&softarc.com>
#               811-827   Unassigned
itm-mcell-s     828/tcp   itm-mcell-s
itm-mcell-s     828/udp   itm-mcell-s
#                         Portnoy Boxman <portnoy_boxman&bmc.com>
pkix-3-ca-ra    829/tcp   PKIX-3 CA/RA
pkix-3-ca-ra    829/udp   PKIX-3 CA/RA
```

```
Keyword         Decimal    Description                    References
-------         -------    -----------                    ----------
#                          Carlisle Adams <Cadams&entrust.com>
netconf-ssh     830/tcp    NETCONF over SSH
netconf-ssh     830/udp    NETCONF over SSH
#                          [RFC4742]
netconf-beep    831/tcp    NETCONF over BEEP
netconf-beep    831/udp    NETCONF over BEEP
#                          [RFC4744]
netconfsoaphttp 832/tcp    NETCONF for SOAP over HTTPS
netconfsoaphttp 832/udp    NETCONF for SOAP over HTTPS
#                          [RFC4743]
netconfsoapbeep 833/tcp    NETCONF for SOAP over BEEP
netconfsoapbeep 833/udp    NETCONF for SOAP over BEEP
#                          [RFC4743]
#               834-846    Unassigned
dhcp-failover2  847/tcp    dhcp-failover 2
dhcp-failover2  847/udp    dhcp-failover 2
#                          Bernard Volz <volz&cisco.com>
gdoi            848/tcp    GDOI
gdoi            848/udp    GDOI
#                          [RFC3547]
#               849-859    Unassigned
iscsi           860/tcp    iSCSI
iscsi           860/udp    iSCSI
#                          RFC3720
owamp-control   861/tcp    OWAMP-Control
owamp-control   861/udp    OWAMP-Control
#                          [RFC4656]
#               862-872    Unassigned
rsync           873/tcp    rsync
rsync           873/udp    rsync
#                          Andrew Tridgell <tridge&samba.anu.edu.au>
#               874-885    Unassigned
iclcnet-locate  886/tcp    ICL coNETion locate server
iclcnet-locate  886/udp    ICL coNETion locate server
#                          Bob Lyon <bl&oasis.icl.co.uk>
iclcnet_svinfo  887/tcp    ICL coNETion server info
iclcnet_svinfo  887/udp    ICL coNETion server info
#                          Bob Lyon <bl&oasis.icl.co.uk>
accessbuilder   888/tcp    AccessBuilder
accessbuilder   888/udp    AccessBuilder
#                          Steve Sweeney <Steven_Sweeney&3mail.3com.com>
# The following entry records an unassigned but widespread use
cddbp           888/tcp    CD Database Protocol
#                          Steve Scherf <steve&moonsoft.com>
#
#               889-899    Unassigned
omginitialrefs  900/tcp    OMG Initial Refs
omginitialrefs  900/udp    OMG Initial Refs
#                          Christian Callsen <Christian.Callsen&eng.sun.com>
smpnameres      901/tcp    SMPNAMERES
smpnameres      901/udp    SMPNAMERES
#                          Leif Ekblad <leif&rdos.net>
ideafarm-door   902/tcp    self documenting Telnet Door
ideafarm-door   902/udp    self documenting Door: send 0x00 for info
ideafarm-panic  903/tcp    self documenting Telnet Panic Door
ideafarm-panic  903/udp    self documenting Panic Door: send 0x00 for info
#                          Wo'o Ideafarm <c74a39f7.9ad6f42c&ideafarm.com>
#               904-909    Unassigned
kink            910/tcp    Kerberized Internet Negotiation of Keys (KINK)
kink            910/udp    Kerberized Internet Negotiation of Keys (KINK)
#                          [RFC4430]
xact-backup     911/tcp    xact-backup
xact-backup     911/udp    xact-backup
#                          Bill Carroll <billc&xactlabs.com>
apex-mesh       912/tcp    APEX relay-relay service
apex-mesh       912/udp    APEX relay-relay service
apex-edge       913/tcp    APEX endpoint-relay service
apex-edge       913/udp    APEX endpoint-relay service
#                          [RFC3340]
#               914-988    Unassigned
ftps-data       989/tcp    ftp protocol, data, over TLS/SSL
ftps-data       989/udp    ftp protocol, data, over TLS/SSL
ftps            990/tcp    ftp protocol, control, over TLS/SSL
ftps            990/udp    ftp protocol, control, over TLS/SSL
#                          Christopher Allen <ChristopherA&consensus.com>
nas             991/tcp    Netnews Administration System
nas             991/udp    Netnews Administration System
#                          Vera Heinau <heinau&fu-berlin.de>
#                          Heiko Schlichting <heiko&fu-berlin.de>
telnets         992/tcp    telnet protocol over TLS/SSL
telnets         992/udp    telnet protocol over TLS/SSL
imaps           993/tcp    imap4 protocol over TLS/SSL
imaps           993/udp    imap4 protocol over TLS/SSL
ircs            994/tcp    irc protocol over TLS/SSL
ircs            994/udp    irc protocol over TLS/SSL
#                          Christopher Allen <ChristopherA&consensus.com>
pop3s           995/tcp    pop3 protocol over TLS/SSL (was spop3)
pop3s           995/udp    pop3 protocol over TLS/SSL (was spop3)
#                          Gordon Mangione <gordm&microsoft.com>
vsinet          996/tcp    vsinet
vsinet          996/udp    vsinet
```

Keyword	Decimal	Description	References
#		Rob Juergens <robj&vsi.com>	
maitrd	997/tcp		
maitrd	997/udp		
busboy	998/tcp		
puparp	998/udp		
garcon	999/tcp		
applix	999/udp	Applix ac	
puprouter	999/tcp		
puprouter	999/udp		
cadlock2	1000/tcp		
cadlock2	1000/udp		
#	1001-1009	Unassigned	
#	1008/udp	Possibly used by Sun Solaris????	
surf	1010/tcp	surf	
surf	1010/udp	surf	
#		Joseph Geer <jgeer&peapod.com>	
#	1011-1020	Reserved	
exp1	1021/tcp	RFC3692-style Experiment 1 (*)	[RFC4727]
exp1	1021/udp	RFC3692-style Experiment 1 (*)	[RFC4727]
exp2	1022/tcp	RFC3692-style Experiment 2 (*)	[RFC4727]
exp2	1022/udp	RFC3692-style Experiment 2 (*)	[RFC4727]
	1023/tcp	Reserved	
	1023/udp	Reserved	
#		IANA <iana&iana.org>	

Hardware type..

Value(16 bits)	Description
1	Ethernet.
2	Experimental Ethernet.
3	Amateur Radio AX.25.
4	Proteon ProNET Token Ring.
5	Chaos.
6	IEEE 802.
7	ARCNET.
8	Hyperchannel.
9	Lanstar.
10	Autonet Short Address.
11	LocalTalk.
12	LocalNet (IBM PCNet or SYTEK LocalNET).
13	Ultra link.
14	SMDS.
15	Frame Relay.
16	ATM, Asynchronous Transmission Mode.
17	HDLC.
18	Fibre Channel.
19	ATM, Asynchronous Transmission Mode.
20	Serial Line.
21	ATM, Asynchronous Transmission Mode.
22	MIL-STD-188-220.
23	Metricom.
24	IEEE 1394.1995.
25	MAPOS.
26	Twinaxial.
27	EUI-64.
28	HIPARP.
29	IP and ARP over ISO 7816-3.
30	ARPSec.
31	IPsec tunnel.
32	Infiniband.
33	CAI, TIA-102 Project 25 Common Air Interface.

ICMP – Type. 8 bits.

Type	Description	References
0	Echo reply.	RFC 792
1		
2		
3	Destination unreachable.	RFC 792
4	Source quench.	RFC 792
5	Redirect.	RFC 792
6	Alternate host address.	
7		
8	Echo request.	RFC 792
9	Router advertisement.	RFC 1256
10	Router solicitation.	RFC 1256
11	Time exceeded.	RFC 792
12	Parameter problem.	RFC 792
13	Timestamp request.	RFC 792
14	Timestamp reply.	RFC 792
15	Information request.Obsolete.	RFC 792
16	Information reply. Obsolete.	RFC 792
17	Address mask request.	RFC 950
18	Address mask reply.	RFC 950
19	reserved (for security).	
20		
-		
29	reserved (for robustness experiment).	
30	Traceroute.	RFC 1393
31	Conversion error.	RFC 1475
32	Mobile Host Redirect.	
33	IPv6 Where-Are-You.	
34	IPv6 I-Am-Here.	
35	Mobile Registration Request.	
36	Mobile Registration Reply.	
37	Domain Name request.	RFC 1788
38	Domain Name reply.	RFC 1788
39	SKIP Algorithm Discovery Protocol.	
40	Photuris, Security failures.	RFC 2521
41	Experimental mobility protocols.	RFC 4065
42		
-		
255	Reserved.	

ARP - Opcode. 16 bits.

Value	Description	References
1	Request.	RFC 826
2	Reply.	RFC 826, RFC 1868
3	Request Reverse.	RFC 903
4	Reply Reverse.	RFC 903
5	DRARP Request.	RFC 1931
6	DRARP Reply.	RFC 1931
7	DRARP Error.	RFC 1931
8	InARP Request.	RFC 1293
9	InARP Reply.	RFC 1293
10	ARP NAK.	RFC 1577
11	MARS Request.	
12	MARS Multi.	
13	MARS MServ.	
14	MARS Join.	
15	MARS Leave.	
16	MARS NAK.	
17	MARS Unserv.	
18	MARS SJoin.	
19	MARS SLeave.	
20	MARS Grouplist Request.	
21	MARS Grouplist Reply.	

DNS - QR, Query/Response. 1 bit.

Value	Description	References
0	QUERY, Standard query.	RFC 1035
1	IQUERY, Inverse query.	RFC 1035, RFC 3425
2	STATUS, Server status request.	RFC 1035
3	reserved.	
4	Notify.	RFC 1996
5	Update.	RFC 2136
6		
15	reserved.	

DNS - Opcode. 4 bits

Value	Description	References
0	QUERY, Standard query.	RFC 1035
1	IQUERY, Inverse query.	RFC 1035, RFC 3425
2	STATUS, Server status request.	RFC 1035
3	reserved.	
4	Notify.	RFC 1996
5	Update.	RFC 2136
6		
-		
15	reserved.	

DNS - AA, Authoritative Answer. 1 bit.

Value	Description
0	Not authoritative.
1	Is authoritative.

DNS - TC, Truncated. 1 bit

Value	Description
0	Recursion not desired.
1	Recursion desired.

DNS - RD, Recursion Desired. 1 bit

Value	Description
0	Recursion not desired.
1	Recursion desired.

DNS - RA, Recursion Available. 1 bit.

Value	Description
0	Recursive query support not available.
1	Recursive query support available.

DNS - Rcode, Return code. 4 bits.

Value	Description	References
0	No error. The request completed successfully.	RFC 1035
1	Format error. The name server was unable to interpret the query.	RFC 1035
2	Server failure. The name server was unable to process this query due to a problem with the name server.	RFC 1035
3	Name Error. Meaningful only for responses from an authoritative name server, this code signifies that the domain name referenced in the query does not exist.	RFC 1035
4	Not Implemented. The name server does not support the requested kind of query.	RFC 1035
5	Refused. The name server refuses to perform the specified operation for policy reasons. For example, a name server may not wish to provide the information to the particular requester, or a name server may not wish to perform a particular operation (e.g., zone transfer) for particular data.	RFC 1035
6	YXDomain. Name Exists when it should not.	RFC 2136
7	YXRRSet. RR Set Exists when it should not.	RFC 2136
8	NXRRSet. RR Set that should exist does not.	RFC 2136
9	NotAuth. Server Not Authoritative for zone.	RFC 2136
10	NotZone. Name not contained in zone.	RFC 2136
11 - 15	reserved.	
16	BADVERS.Bad OPT Version. BADSIG.TSIG Signature Failure.	RFC 2671 RFC 2845
17	BADKEY. Key not recognized.	RFC 2845
18	BADTIME. Signature out of time window.	RFC 2845
19	BADMODE. Bad TKEY Mode.	RFC 2930
20	BADNAME. Duplicate key name.	RFC 2930
21	BADALG. Algorithm not supported.	RFC 2930
22	BADTRUNC. Bad truncation.	RFC 4635
23 - 3840		
3841 - 4095	Private use.	

DNS - Type. 16 bits, unsigned.

Value	Description	References
0		
1	A, IPv4 address. RFC 1035	
2	NS, Authoritative name server.	RFC 1035
3	MD, Mail destination. Obsolete use MX instead.	RFC 1035
4	MF, Mail forwarder. Obsolete use MX instead.	RFC 1035
5	CNAME, Canonical name for an alias.	RFC 1035
6	SOA, Marks the start of a zone of authority.	RFC 1035
7	MB, Mailbox domain name.	RFC 1035
8	MG, Mail group member.	RFC 1035
9	MR, Mail rename domain name.	RFC 1035
10	NULL, Null resource record.	RFC 1035
11	WKS, Well known service description.	RFC 1035
12	PTR, Domain name pointer.	RFC 1035
13	HINFO, Host information.	RFC 1035
14	MINFO, Mailbox or mail list information.	RFC 1035
15	MX, Mail exchange.	RFC 1035
16	TXT, Text strings.	RFC 1035
17	RP, Responsible Person.	RFC 1183
18	AFSDB, AFS Data Base location.	RFC 1183
19	X25, X.25 PSDN address.	RFC 1183
20	ISDN, ISDN address.	RFC 1183
21	RT, Route Through.	RFC 1183
22	NSAP, NSAP address. NSAP style A record.	RFC 1706
23	NSAP-PTR.	RFC 1348
24	SIG, Security signature.	RFC 2931, RFC 4034
25	KEY, Security key.	RFC 3445, RFC 4034
26	PX, X.400 mail mapping information.	RFC 2163
27	GPOS, Geographical Position.	RFC 1712
28	AAAA, IPv6 Address.	RFC 3596
29	LOC, Location Information.	RFC 1876
30	NXT, Next Domain (obsolete).	RFC 2535
31	EID, Endpoint Identifier.	
32	NIMLOC, Nimrod Locator.	
	NB, NetBIOS general Name Service.	RFC 1002
33	SRV, Server Selection.	
	NBSTAT, NetBIOS NODE STATUS.	RFC 2052, RFC 2782 RFC 1002
34	ATMA, ATM Address.	
35	NAPTR, Naming Authority Pointer.	RFC 3403
36	KX, Key Exchanger.	RFC 2230
37	CERT. RFC 2538,	RFC 4398
38	A6. RFC 2874,	RFC 3226
39	DNAME.	RFC 2672
40	SINK.	
41	OPT.	RFC 2671
42	APL.	RFC 3123
43	DS, Delegation Signer.	RFC 3658
44	SSHFP, SSH Key Fingerprint.	RFC 4255
45	IPSECKEY.	RFC 4025
46	RRSIG.	RFC 3755
47	NSEC, NextSECure.	RFC 3755, RFC 3845
48	DNSKEY.	RFC 3755
49	DHCID, DHCP identifier.	RFC 4701
50	NSEC3.	RFC 5155

Value	Description	References
51	NSEC3PARAM.	RFC 5155
52		
53		
54		
55	HIP, Host Identity Protocol.	RFC 5205
56	NINFO.	
57	RKEY.	
58		
-		
98		
99	SPF, Sender Policy Framework.	RFC 4408
100	UINFO.	
101	UID.	
102	GID.	
103	UNSPEC.	
104		
-		
248		
249	TKEY. RFC 2930	
250	TSIG, Transaction Signature.	RFC 2845, RFC 3645
251	IXFR, Incremental transfer.	RFC 1995
252	AXFR, A request for a transfer of an entire zone.	RFC 1035
253	MAILB, A request for mailbox-related records (MB, MG or MR).	RFC 1035
254	MAILA, A request for mail agent RRs. Obsolete.	RFC 1035
255	*. A request for all records.	RFC 1035
256		
-		
32767		
32768	DNSSEC Trust Authorities.	
32769	DNSSEC Lookaside Validation. RFC 4431,	RFC 5074

FTP - FTP reply codes

Value	Description
110	Restart marker reply.
120	Service ready in nnn minutes.
125	Data connection already open; transfer starting.
150	File status okay; about to open data connection.
200	Command okay.
202	Command not implemented, superfluous at this site.
211	System status, or system help reply.
212	Directory status.
213	File status.
214	Help message.
215	NAME system type.
220	Service ready for new user.
221	Service closing control connection.
225	Data connection open; no transfer in progress.
226	Closing data connection.
227	Entering Passive Mode <h1,h2,h3,h4,p1,p2>.
228	Entering Long Passive Mode.
229	Extended Passive Mode Entered.
230	User logged in, proceed.
250	Requested file action okay, completed.
257	"PATHNAME" created.
331	User name okay, need password.
332	Need account for login.
350	Requested file action pending further information.
421	Service not available, closing control connection.
425	Can't open data connection.
426	Connection closed; transfer aborted.
450	Requested file action not taken.
451	Requested action aborted. Local error in processing.
452	Requested action not taken.
500	Syntax error, command unrecognized.
501	Syntax error in parameters or arguments.
502	Command not implemented.
503	Bad sequence of commands.
504	Command not implemented for that parameter.
521	Supported address families are <af1, .., afn>
522	Protocol not supported.
530	Not logged in.
532	Need account for storing files.
550	Requested action not taken.
551	Requested action aborted. Page type unknown.
552	Requested file action aborted.
553	Requested action not taken.
554	Requested action not taken: invalid REST parameter.
555	Requested action not taken: type or stru mismatch.

HTTP - Methods

Methods	Description
DELETE	RFC 1945
GET	RFC 1945
HEAD	RFC 1945
LINK	RFC 1945
OPTIONS	RFC 2068
PATCH	RFC 2068
POST	RFC 1945
PUT	RFC 1945
TRACE	RFC 2068
UNLINK	RFC 1945

HTTP - Header fields

Header field	References
A-IM	RFC 3229
Accept	RFC 2616
Accept-Additions	RFC 2324
Accept-Charset	RFC 2616
Accept-Encoding	RFC 2616
Accept-Features	RFC 2295
Accept-Language	RFC 2616
Accept-Ranges	RFC 2616
Age	RFC 2616
Allow	RFC 2616
Alternates	RFC 2295
Authentication-Info	RFC 2617
Authorization	RFC 2616
C-Ext	RFC 2774
C-Man	RFC 2774
C-Opt	RFC 2774
C-PEP deprecated.	
C-PEP-Info deprecated.	
Cache-Control	RFC 2616
Connection	RFC 2616
Content-Base	
Content-Disposition	RFC 2616
Content-Encoding	RFC 2616
Content-ID	
Content-Language	RFC 2616
Content-Length	RFC 2616
Content-Location	RFC 2616
Content-MD5	RFC 2616
Content-Range	RFC 2616
Content-Script-Type	
Content-Style-Type	
Content-Type	RFC 2616
Content-Version	
Cookie	RFC 2965
Cookie2	RFC 2965
DAV	RFC 2518
Date	RFC 2616
Default-Style	
Delta-Base	RFC 3229

Header field	References
Depth	RFC 2518
Derived-From	
Destination	RFC 2518
Differential-ID	
Digest	RFC 3230
ETag	RFC 2616
Expect	RFC 2616
Expires	RFC 2616
Ext	RFC 2774
From	RFC 2616
GetProfile	
Host	RFC 2616
IM	RFC 3229
If	RFC 2518
If-Match	RFC 2616
If-Modified-Since	RFC 2616
If-None-Match	RFC 2616
If-Range RFC 2616	
If-Unmodified-Since	RFC 2616
Keep-Alive	RFC 2068
Label	RFC 3253
Last-Modified	RFC 2616
Link	RFC 2068
Location	RFC 2616
Lock-Token	RFC 2518
MIME-Version	RFC 2616
Man	RFC 2774
Max-Forwards	RFC 2616
Meter	RFC 2227
Negotiate	RFC 2295
Opt	RFC 2774
Ordering-Type	RFC 3648
Overwrite	RFC 2518
P3P	
PEP	
Pep-Info	
PICS-Label	
Position	RFC 3648
Pragma	RFC 2616
ProfileObject	
Protocol	
Protocol-Info	
Protocol-Query	
Protocol-Request	
Proxy-Authenticate	RFC 2616
Proxy-Authentication-Info RFC 2617	
Proxy-Authorization	RFC 2616
Proxy-Features	
Proxy-Instruction	
Public	RFC 2068
Range	RFC 2616
Referer	RFC 2616
Retry-After	RFC 2616
Safe	RFC 2310
Security-Scheme	RFC 2660
Server	RFC 2616
Set-Cookie	RFC 2109
Set-Cookie2	RFC 2965
SetProfile	
SoapAction	
Status-URI	RFC 2518

Header field	References
Surrogate-Capability	
Surrogate-Control	
TCN	Transparent Content Negotiation. RFC 2295
TE	RFC 2616
Timeout	RFC 2518
Trailer	RFC 2616
Transfer-Encoding	RFC 2616
URI	RFC 2068
Upgrade	RFC 2616
User-Agent	RFC 2616
Variant-Vary	RFC 2295
Vary	RFC 2616
Via	RFC 2616
WWW-Authenticate	RFC 2616
Want-Digest	RFC 3230
Warning	RFC 2616

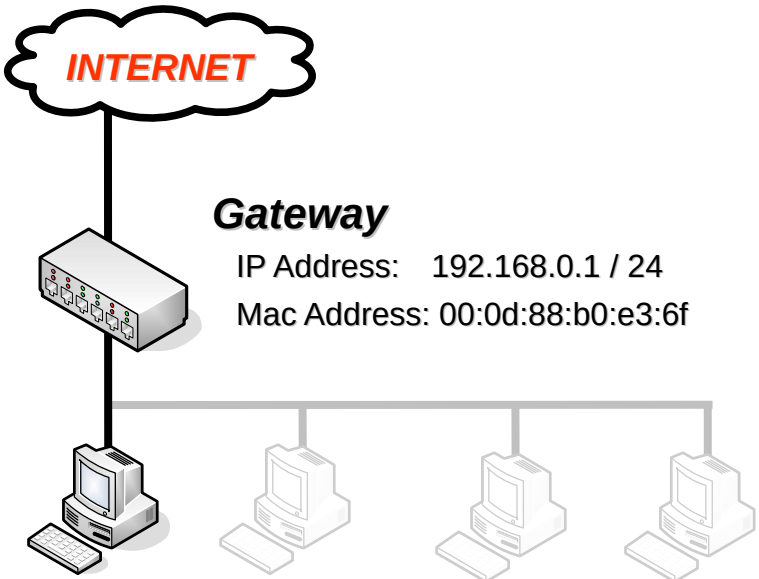
HTTP - HTTP status code

Code	Description	References
100	Continue.	
101	Switching protocols.	
200	Ok.	
201	Created.	
202	Accepted.	
203	Non-authoritive information.	
204	No content.	
205	Reset content.	
206	Partial content.	
226	IM used.	
300	Multiple choices.	
301	Moved permanently.	
302	Moved temporarily.	
303	See other.	
304	Not modified.	
305	Use proxy.	
400	Bad request.	
401	Unauthorized.	
402	Payment required.	
403	Forbidden.	
404	Not found.	
405	Method not allowed.	
406	Not acceptable.	
407	Proxy authentication required.	
408	Request timeout.	
409	Conflict.	
410	Gone.	
411	Length required.	
412	Precondition failed.	
413	Request entity too large.	
414	Request URI too large.	
415	Unsupported media type.	
426	Upgrade Required.	
500	Internal server error.	RFC 2616
501	Not implemented.	RFC 2616
502	Bad gateway.	RFC 2616
503	Service unavailable.	RFC 2616
504	Gateway timeout.	RFC 2616
505	HTTP version not supported.	RFC 2616
506	Variant Also Negotiates (Experimental).	RFC 2295
507	Insufficient Storage.	RFC 4918
508		
509		
510	Not Extended.	RFC 2774

PROTOCOL ANALYSIS

附錄 ：Statistics

講義環境設定



Gateway

IP Address: 192.168.0.1 / 24

Mac Address: 00:0d:88:b0:e3:6f

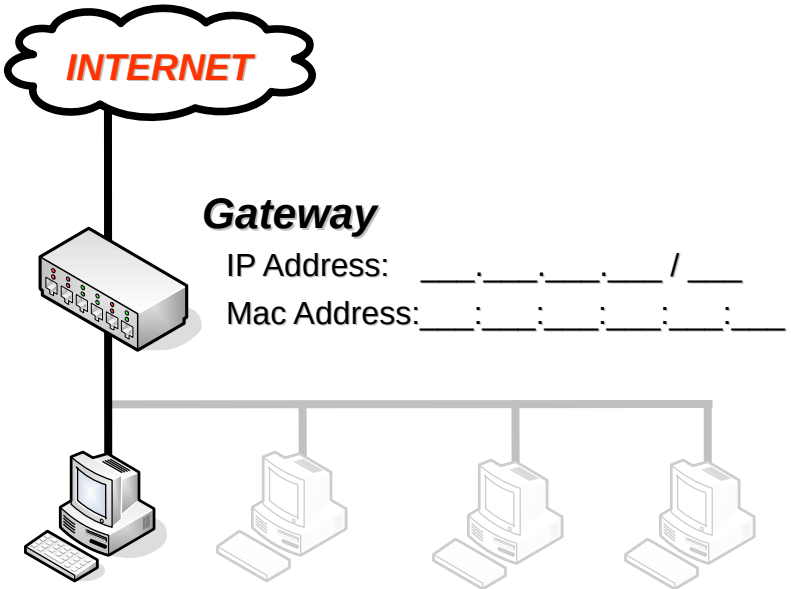
PC/Workstation

IP Address: 192.168.0.175 / 24

Mac Address: 00:1d:d9:60:19:c2

Gateway: 192.168.0.1

我的環境設定



Gateway

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

PC/Workstation

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

爲何需要統計封包？

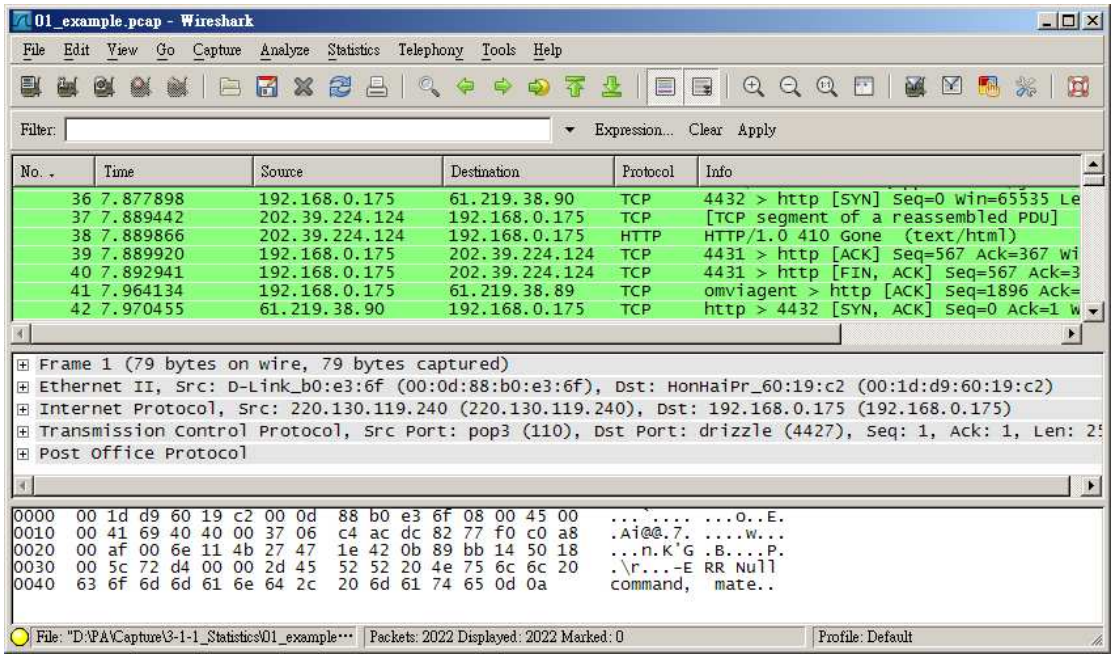
從本課程下來，現在您應該已經是個網路分析高手了，或許您可以開始從網路封包的分析，開始來改善網路效能；也或許有天您需要制定公司網路使用規範，讓有限的網路頻寬做更有效的應用，而所謂的制定不是憑空想像，您需要參考目前網路使用者的方式來制定。

您如果想禁止 P2P 的使用，卻發現全公司內的使用者對於 P2P 的使用幾乎沒興趣，那何必花時間去制定網路使用公約，或是購買可以禁止 P2P 的網路設備呢？如果發現公司內的使用者非常喜歡到某個網站去，那就有必要採取一些措施了；但是怎麼去了解這些狀況呢？沒錯，統計。

分析統計前的準備

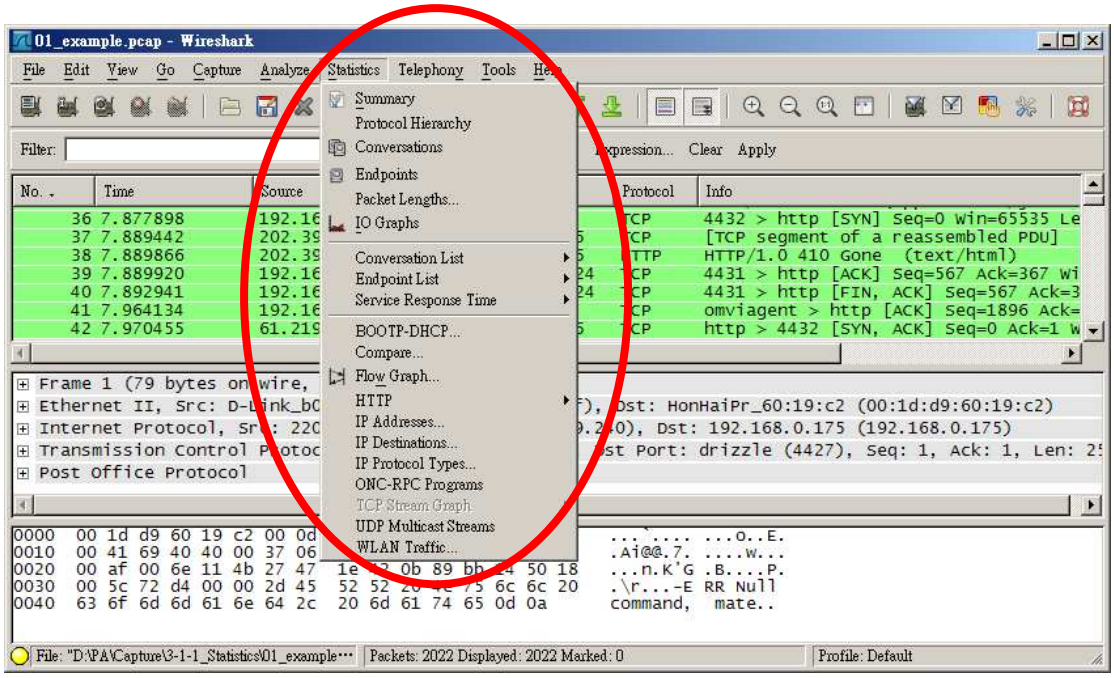
其實封包的統計在 Wireshark 裡是相當簡單與方便的，您只需要點點按按就可以輕鬆得到統計數據，當然，您還是得具備如同分析封包的知識。

爲了讓我們可以看出分析的效果，首先您需要擷取封包一段時間，讓 Wireshark 中有各式種類封包，***您應該知道要得到整個網路封包得在哪個節點切入***，而本範例並不是適當的節點（本範例可以在 \Capture\Appendix_Statistics\01_example.pcap 取得）。



可統計的方式

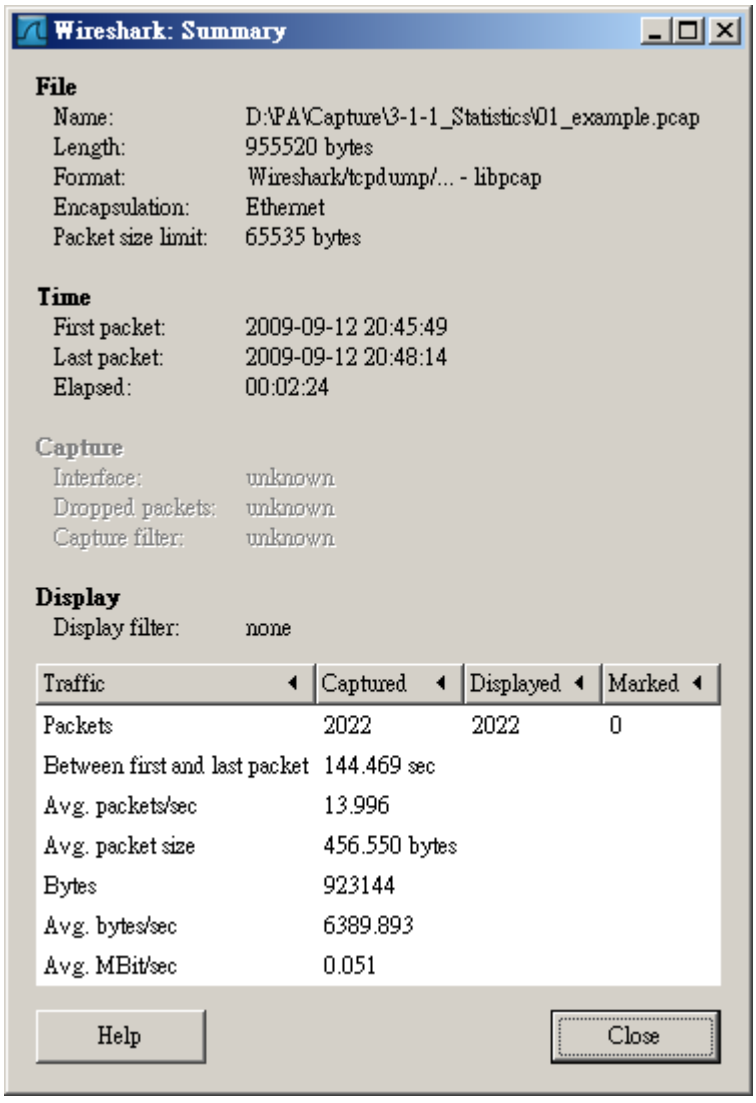
Wireshark 已經內建好不少統計方式，您可以直接在擷取好的狀態下，直接取得統計資料，Wireshark 所提供的統計方式都在功能表的「Statistics」裡：



接下來，我們以較爲常用的功能來解說：

摘要統計（Summary）

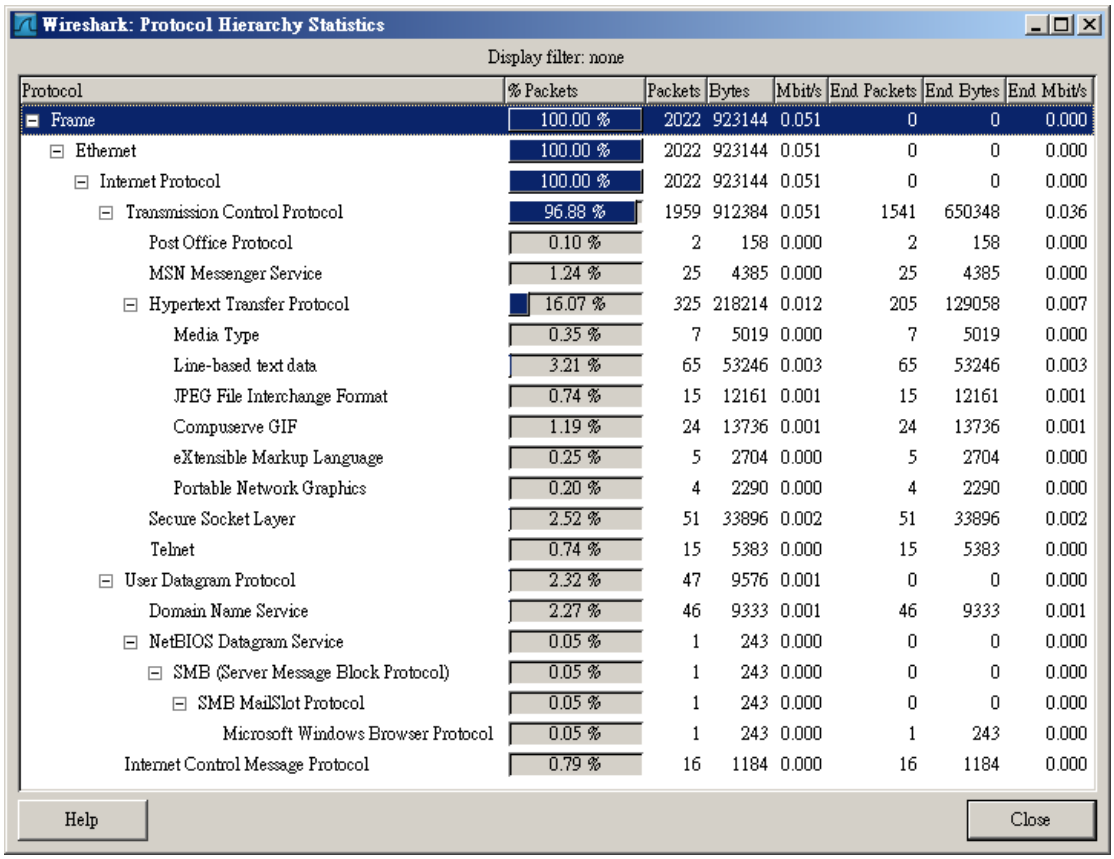
您可以在「Statistics」→「Summary」裡找到，這是簡易的封包摘要統計，只描述如檔案名稱 (檔案位置)、大小、擷取時間、擷取類型、封包數量、平均封包大小、流量…等等。



Summary 心得筆記

協定階層統計 (Protocol Hierarchy Statistics)

您可以在「Statistics」→「Protocol Hierarchy」裡找到，這是以協定做的階層式統計，只描述堆疊式的協定統計：

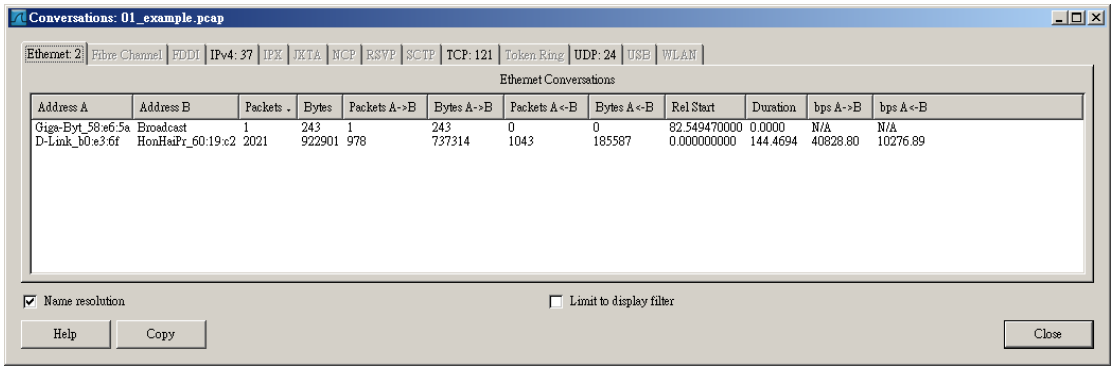


Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	2022	923144	0.051	0	0	0.000
Ethernet	100.00 %	2022	923144	0.051	0	0	0.000
Internet Protocol	100.00 %	2022	923144	0.051	0	0	0.000
Transmission Control Protocol	96.88 %	1959	912384	0.051	1541	650348	0.036
Post Office Protocol	0.10 %	2	158	0.000	2	158	0.000
MSN Messenger Service	1.24 %	25	4385	0.000	25	4385	0.000
Hypertext Transfer Protocol	16.07 %	325	218214	0.012	205	129058	0.007
Media Type	0.35 %	7	5019	0.000	7	5019	0.000
Line-based text data	3.21 %	65	53246	0.003	65	53246	0.003
JPEG File Interchange Format	0.74 %	15	12161	0.001	15	12161	0.001
Compuserve GIF	1.19 %	24	13736	0.001	24	13736	0.001
eXtensible Markup Language	0.25 %	5	2704	0.000	5	2704	0.000
Portable Network Graphics	0.20 %	4	2290	0.000	4	2290	0.000
Secure Socket Layer	2.52 %	51	33896	0.002	51	33896	0.002
Telnet	0.74 %	15	5383	0.000	15	5383	0.000
User Datagram Protocol	2.32 %	47	9576	0.001	0	0	0.000
Domain Name Service	2.27 %	46	9333	0.001	46	9333	0.001
NetBIOS Datagram Service	0.05 %	1	243	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.05 %	1	243	0.000	0	0	0.000
SMB MailSlot Protocol	0.05 %	1	243	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.05 %	1	243	0.000	1	243	0.000
Internet Control Message Protocol	0.79 %	16	1184	0.000	16	1184	0.000

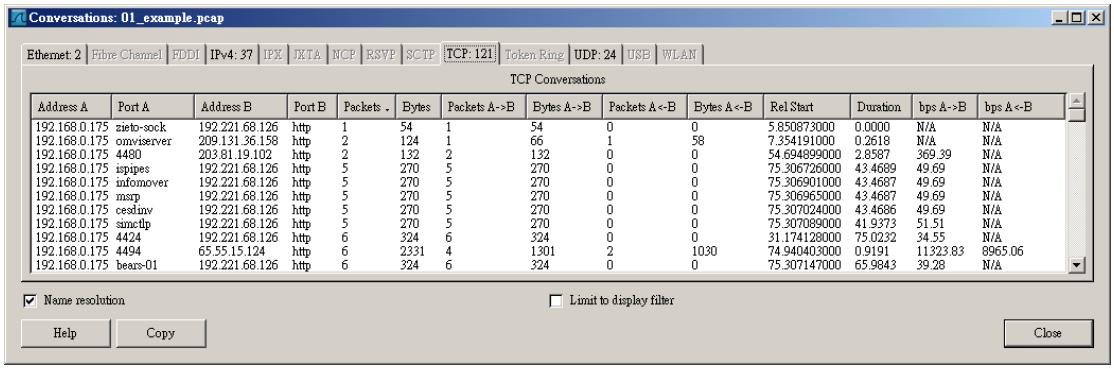
Protocol Hierarchy Statistics 心得筆記

溝通統計 (Conversations)

您可以在「Statistics」→「Conversations」裡找到，這是以兩個節點 (Address A and Address B) 的溝通爲基礎，再以不同協定分類統計：



這裡以 Ethernet 爲基礎，並找到 2 個端點

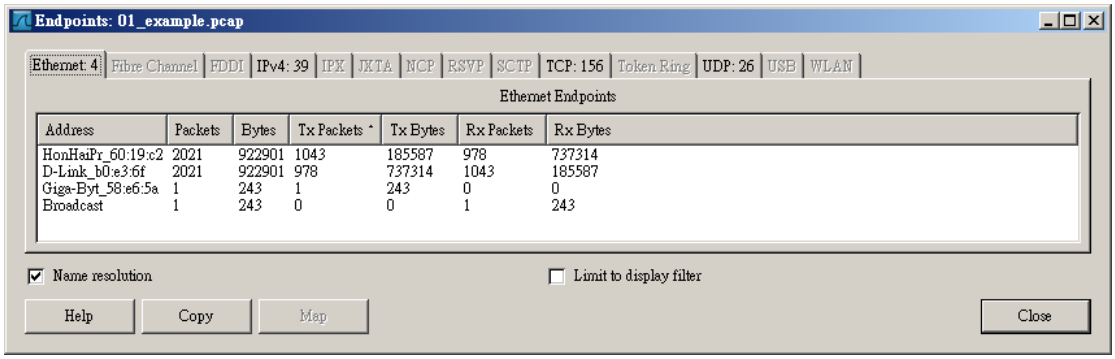


這裡以 TCP 爲基礎，並找到 121 個端點

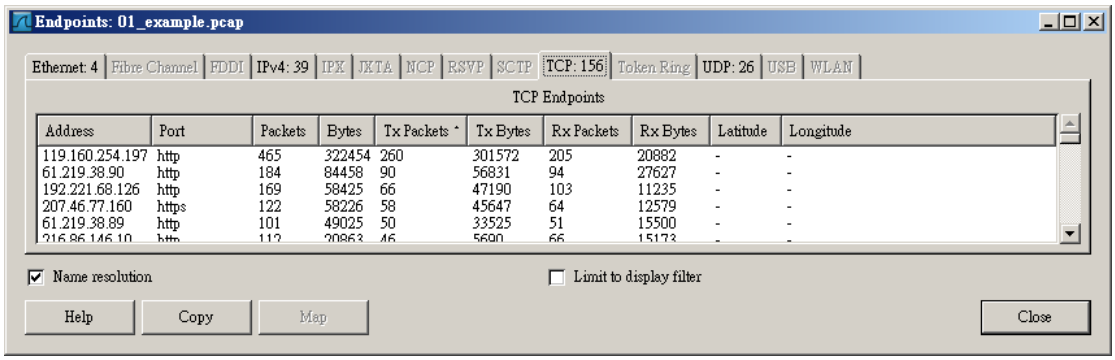
Conversations 心得筆記

節點統計 (Endpoints)

您可以在「Statistics」→「Endpoints」裡找到，與 Conversations 類似，不過這是以一個節點爲基礎，一樣以不同協定分類統計：



這裡以 Ethernet 爲基礎，並找到 4 個端點

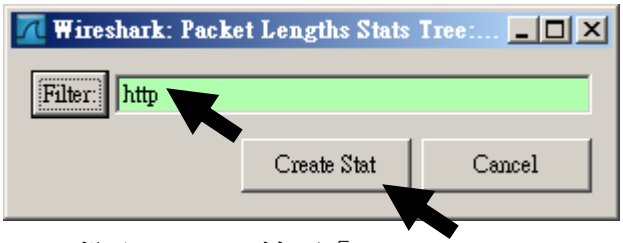


這裡以 TCP 爲基礎，並找到 156 個端點

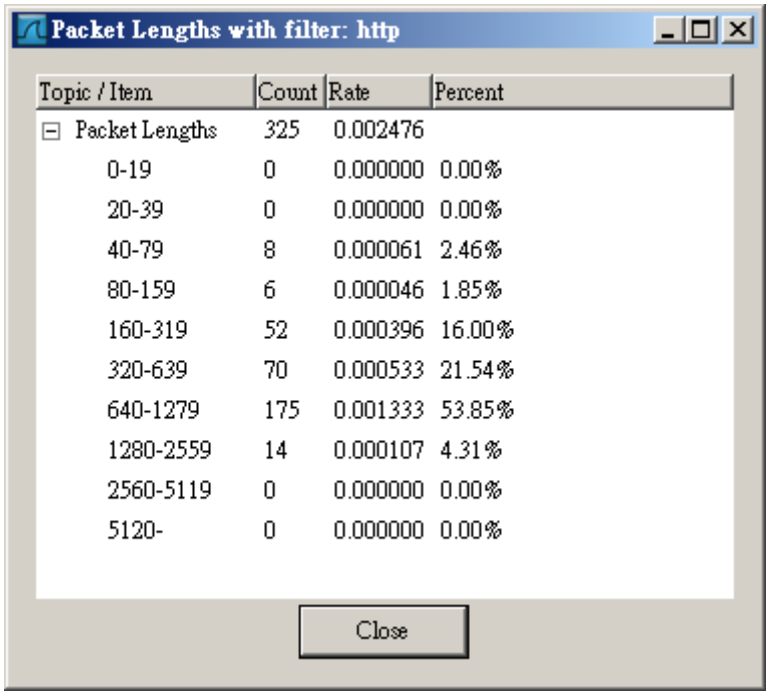
Endpoints 心得筆記

封包長度統計 (Pocket Lengths)*

您可以在「Statistics」→「Pocket Lengths」裡找到，這裡可以統計某種類的封包協定佔的長度分布，例如如果您想知道每個 http 協定的封包長度分佈，您可以參考下方範例：



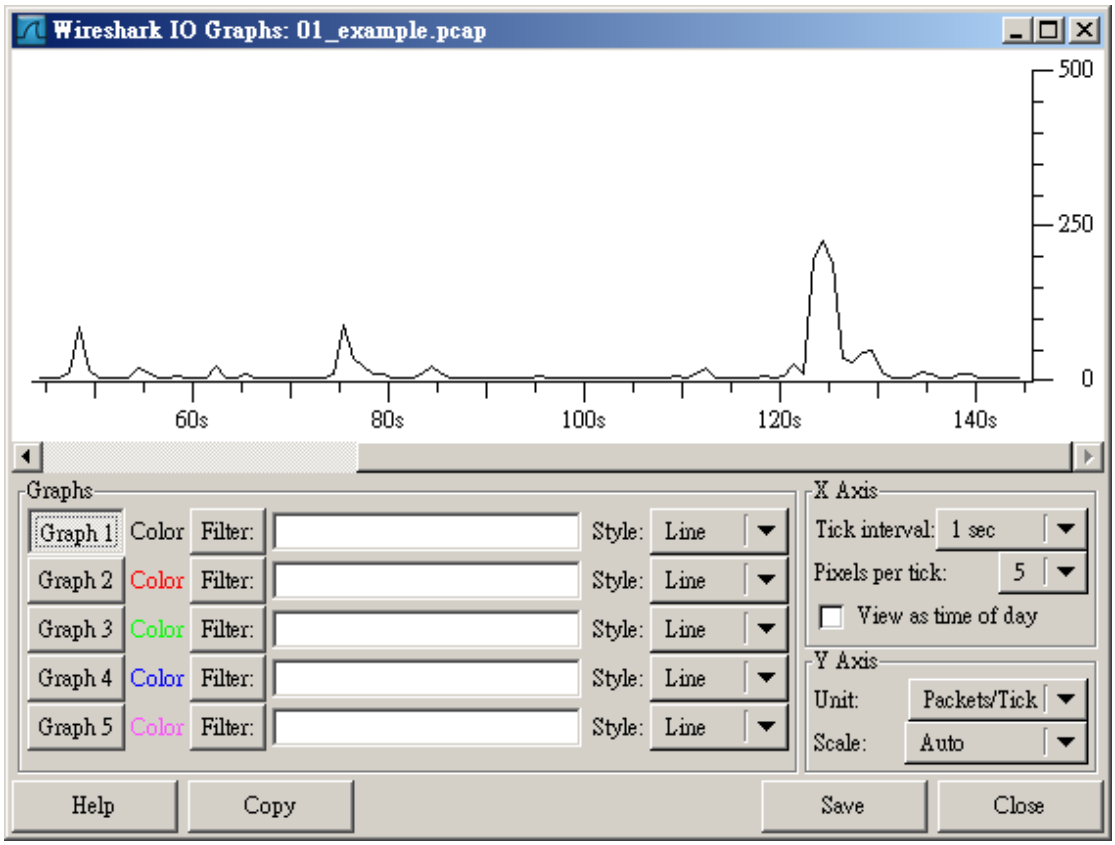
輸入 http ，按下「Create Stat」



Pocket Lengths 心得筆記

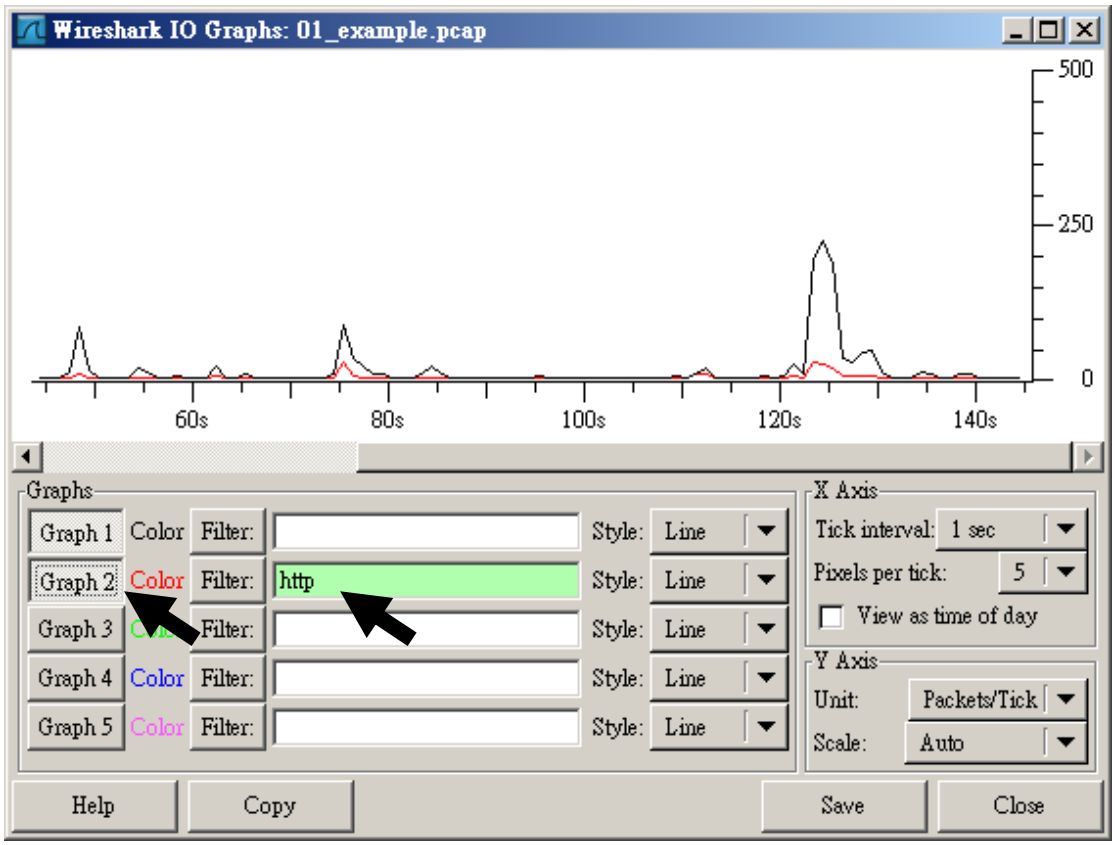
存取圖表（IO Graphs）

您可以在「Statistics」→「IO Graphs」裡找到，這裡可以繪出以時間、封包數的圖表，您可以知道某時間封包進出的數量，也可以繪出某特定封包的圖表：



這是預設圖表，以總封包量爲繪圖基礎

如果您想知道 HTTP 的封包進出圖表，您可以在 Graph 2 右邊的 Filter 填入 「http」，再按下「Graph 2」圖示，紅色的圖表立即顯現：

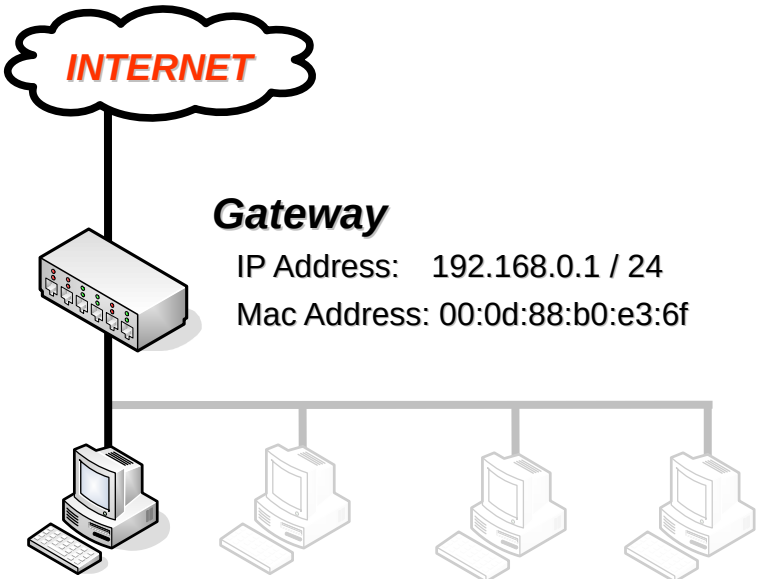


IO Graphs 心得筆記

PROTOCOL ANALYSIS

附錄 ：GeoIP

講義環境設定



Gateway

IP Address: 192.168.0.1 / 24

Mac Address: 00:0d:88:b0:e3:6f

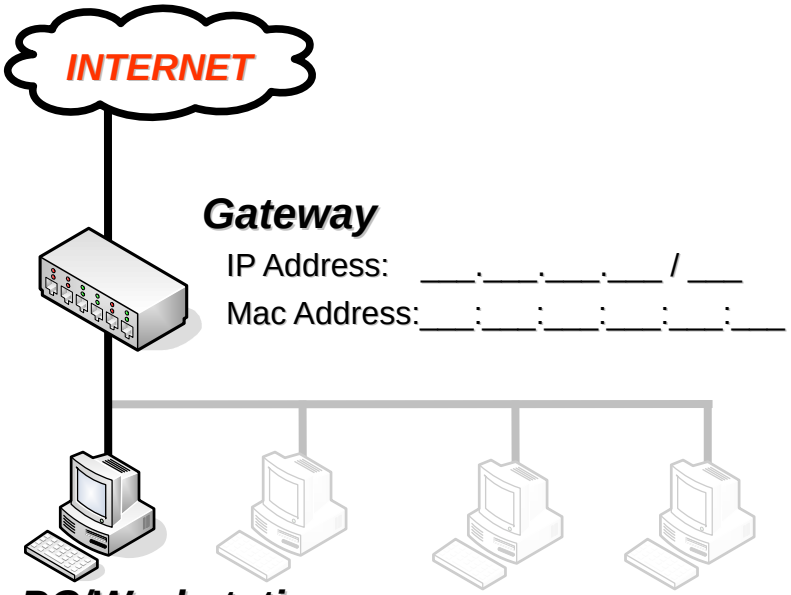
PC/Workstation

IP Address: 192.168.0.175 / 24

Mac Address: 00:1d:d9:60:19:c2

Gateway: 192.168.0.1

我的環境設定



Gateway

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

PC/Workstation

IP Address: ___.___.___.___ / ___

Mac Address:___:___:___:___:___:___

Gateway: ___.___.___.___

令 Wireshark 查詢分析更直覺

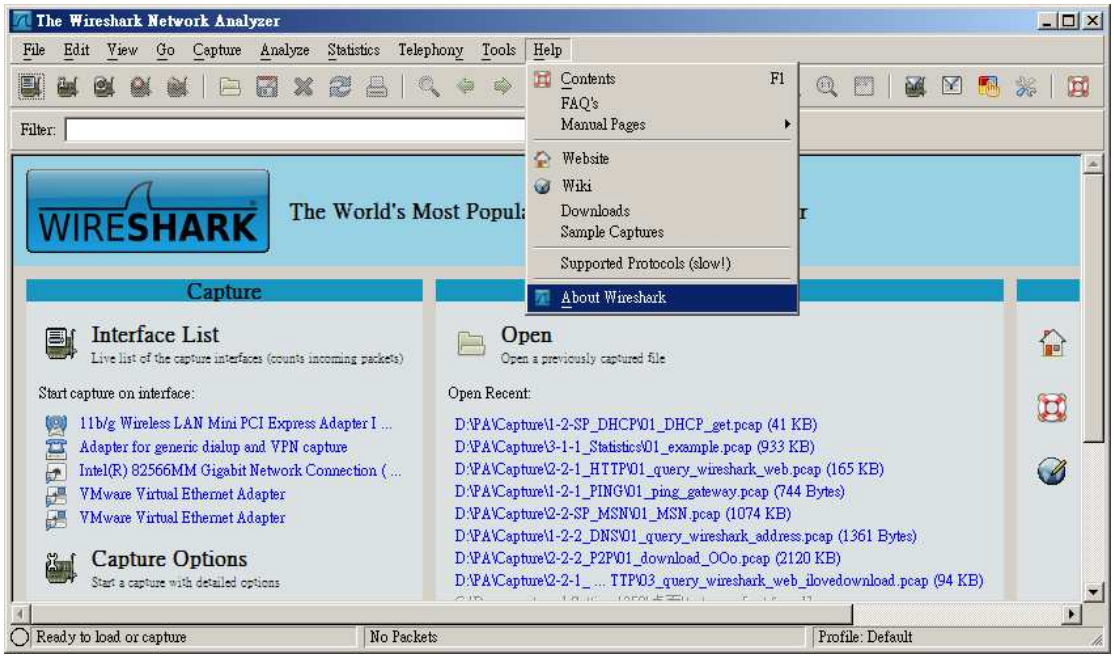
當您已經很熟悉如何分析封包時，您一定有個困擾，那就是面對一堆 IP 時的「無知」，沒錯，您沒有辦法立即辨別出這是哪裡的 IP，因爲它只是一組數字，即使您很容易分辨出 A ~ E Class，卻很難分辨出屬於哪個國家與城市。

雖然 IP 的資料並不是秘密 (也不得爲秘密)，許多網站都有提供 IP 查詢功能，但是在 Wireshark 有沒有什麼套件可以在擷取封包的同時就順便將 IP 所屬位置給查出來呢？

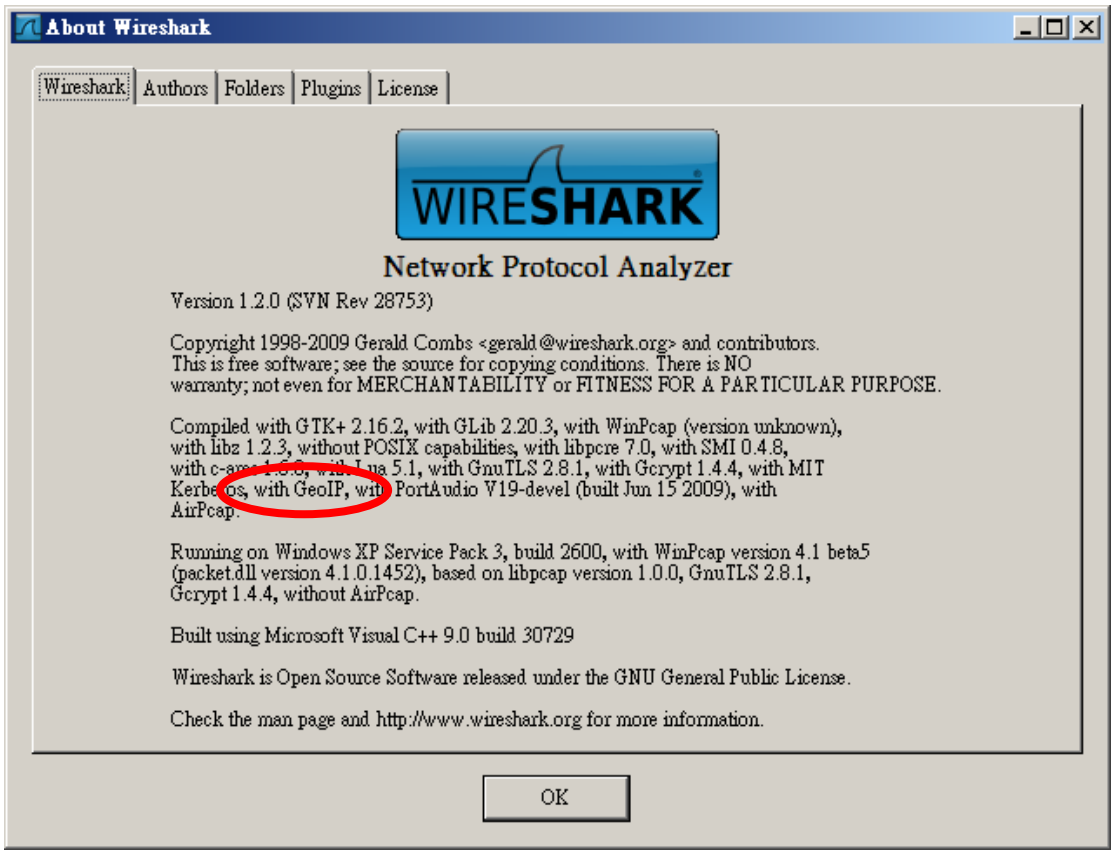
有的，MaxMind 的 GeoIP 辦的到，不過他並不是免費或是自由使用的，不過您可以下載 MaxMind 所提供的免費版本「GeoLite」。

檢查 Wireshark 是否支援

Wireshark 從 1.1.2 版本開始支援 MaxMind 的 GeoIP，如果您不確定您的 Wireshark 是否有支援，請檢查您的 Wireshark：



在功能表選擇「Help」→「About Wireshark」



有「with GeoIP」字樣，表示已有支援

如果您的 Wireshark 太舊，請到 Wireshark 下載更新您的 Wireshark 版本，才能繼續下面內容。

下載 GeoLite

由於 GeoLite 的資料庫有些份量，所以將資料庫依照不同屬性分成不同檔案，也就是說 GeoLite 包含了 City、Country 與 ASNum 三個部份：

GeoIP 網站：http://geolite.maxmind.com/download/geoip/database/

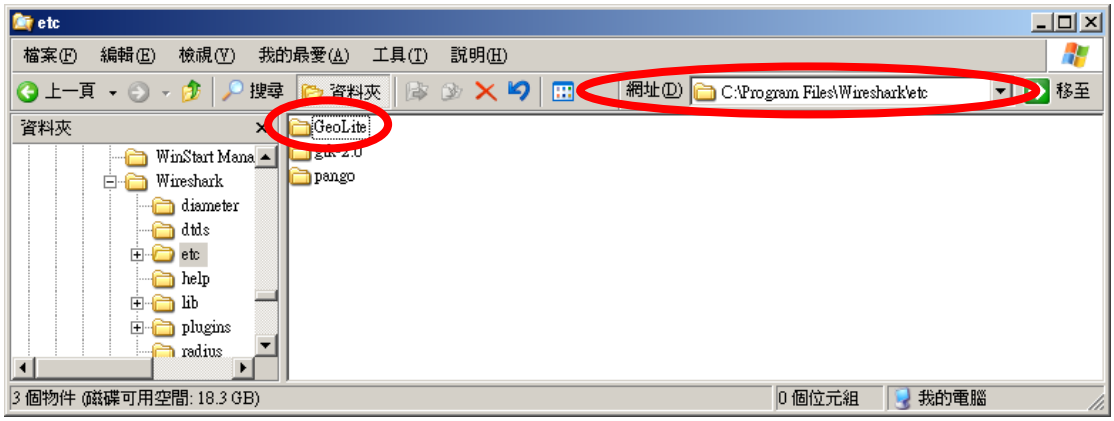
您也可以直接下載下方的連結，該連結都是最新的 GeoLite：

http://geolite.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz
http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
http://geolite.maxmind.com/download/geoip/database/asnum/GeoIPASNum.dat.gz

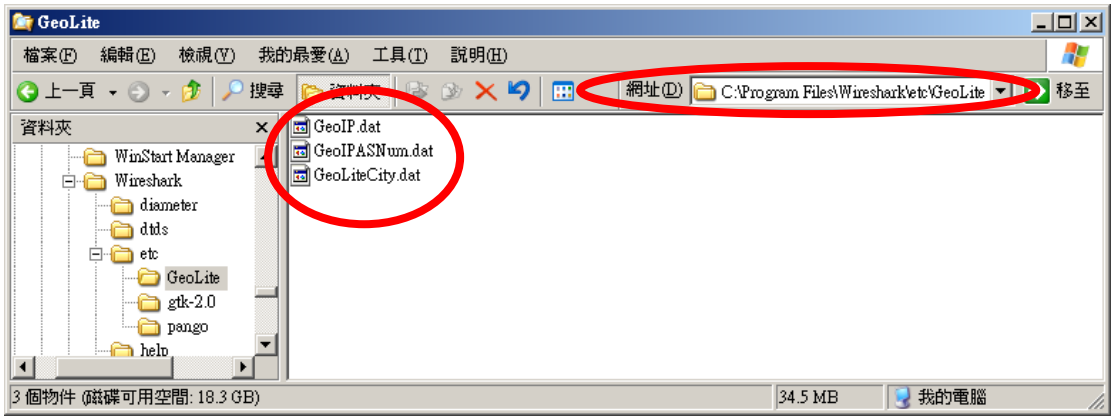
您也可以直接在課堂上的 FTP 上取得
(\Software\GeoLite\GeoIP.dat.gz、\Software\GeoLite\GeoLiteCity.dat.gz、\Software\GeoLite\GeoIPASNum.dat.gz)

安裝 GeoLite

下載好 GeoLite 的三個資料庫檔案後，請自行開啓檔案總管並於 C:\Porgram Files\Wireshark\etc\ 下建立 GeoLite 目錄。

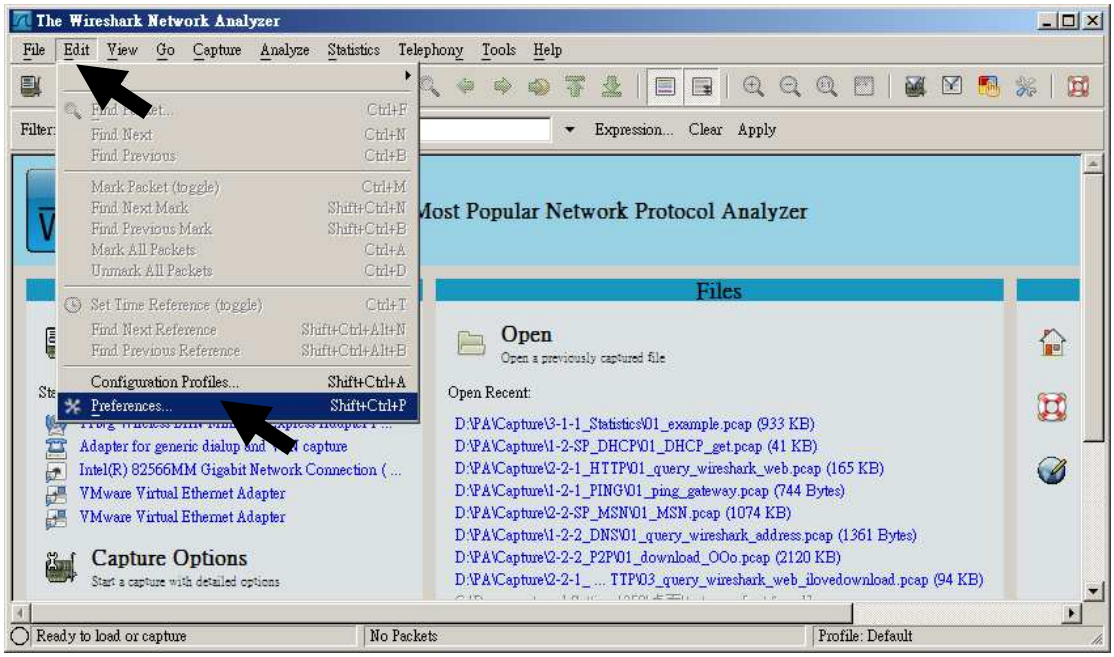


並將剛剛下載好的 GeoIP.dat.gz、GeoLiteCity.dat.gz、GeoIPASNum.dat.gz 解壓縮，並複製到 C:\Porgram Files\Wireshark\etc\GeoLite\ 目錄下

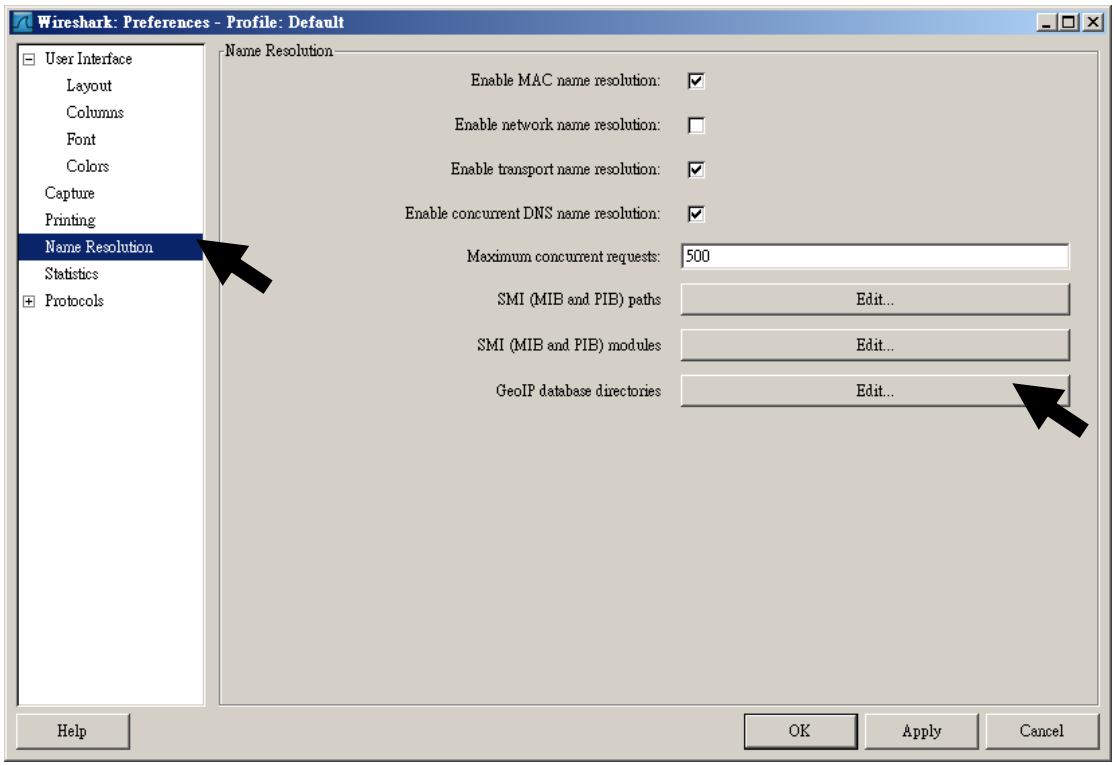


設定 GeoLite

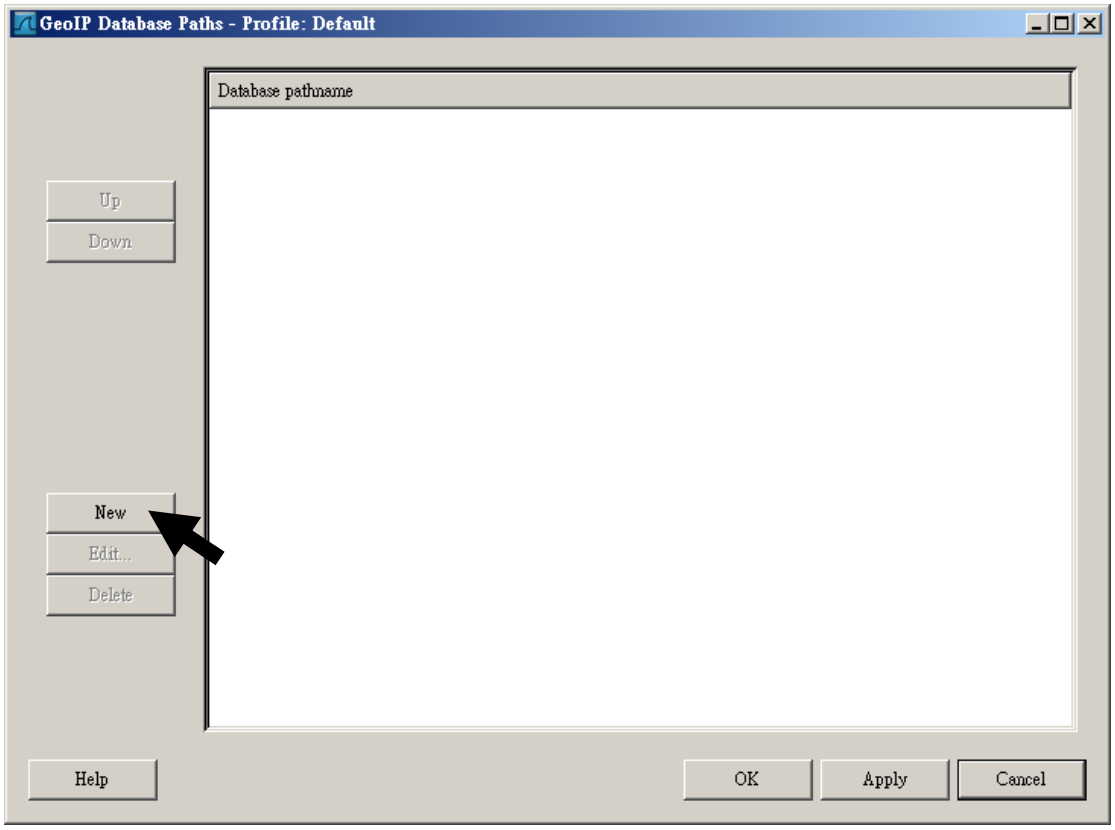
開啓您的 Wireshark，並開始設定，設定方式請參考下列步驟：



選擇「Edit」→「Preferences」

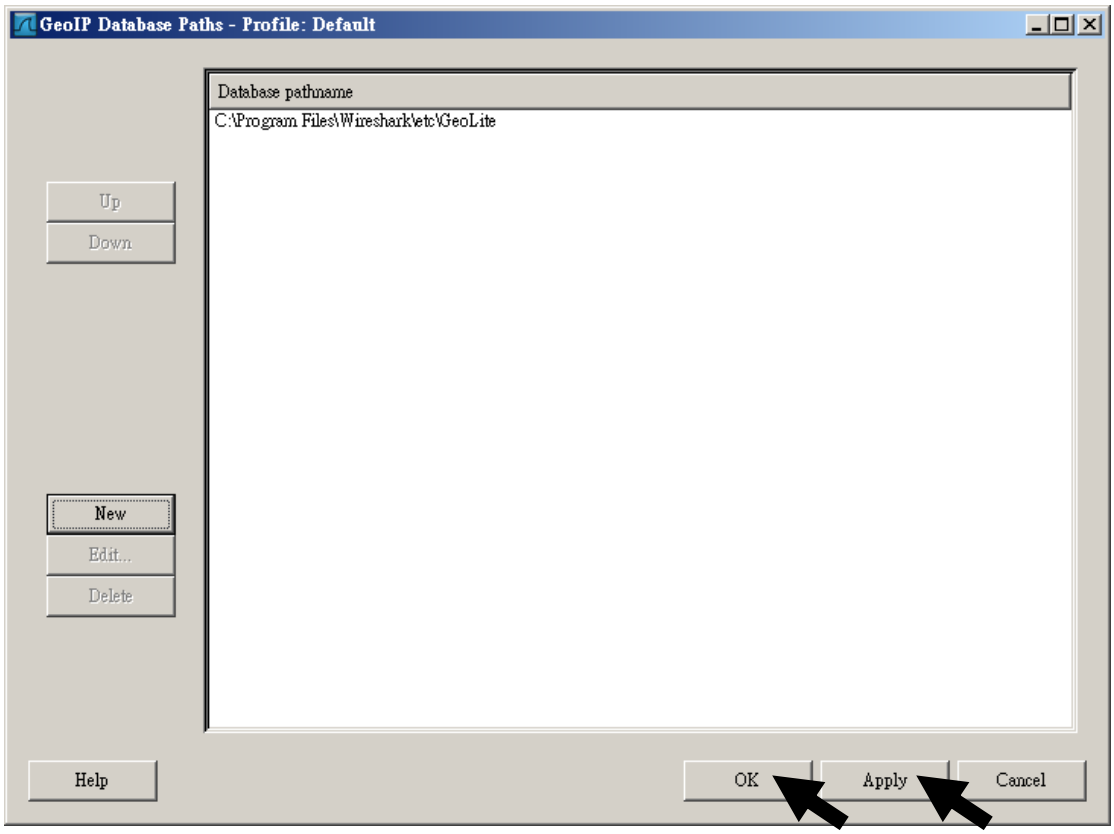


選擇「Name Resolution」，在選擇 GeoIP database directories 的「Edit」

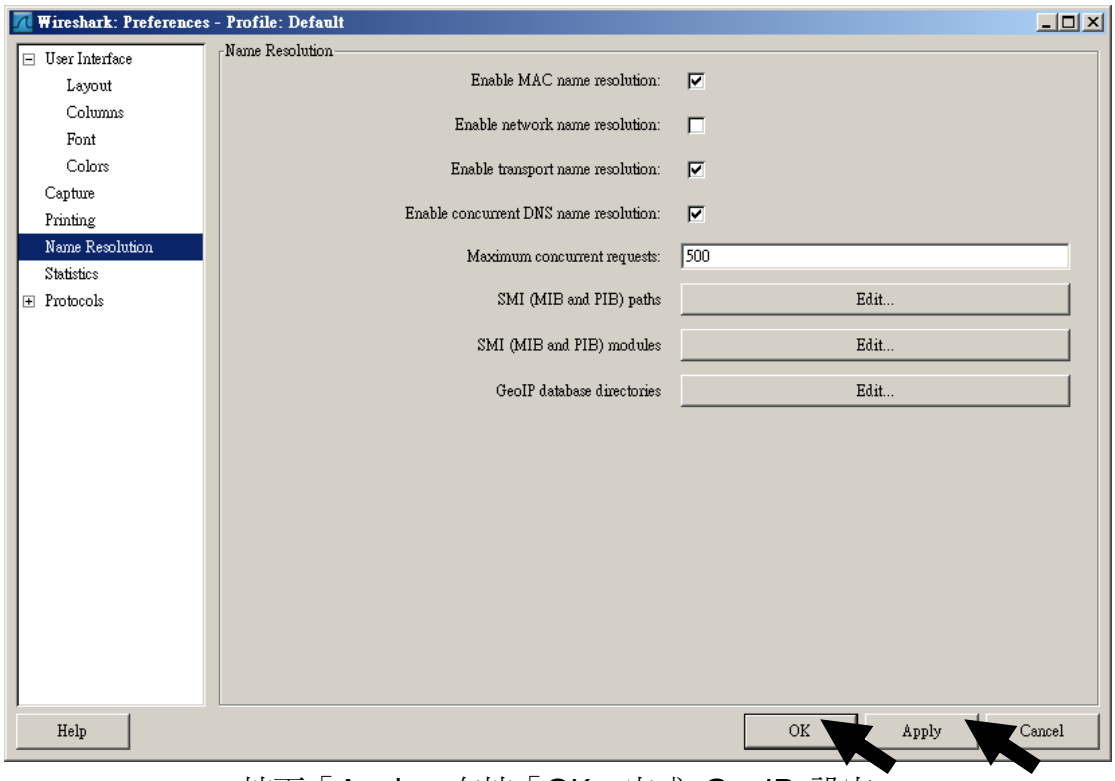


選擇「New」

輸入路徑「C:\Program Files\Wireshark\etc\GeoLite」，按下「OK」確定



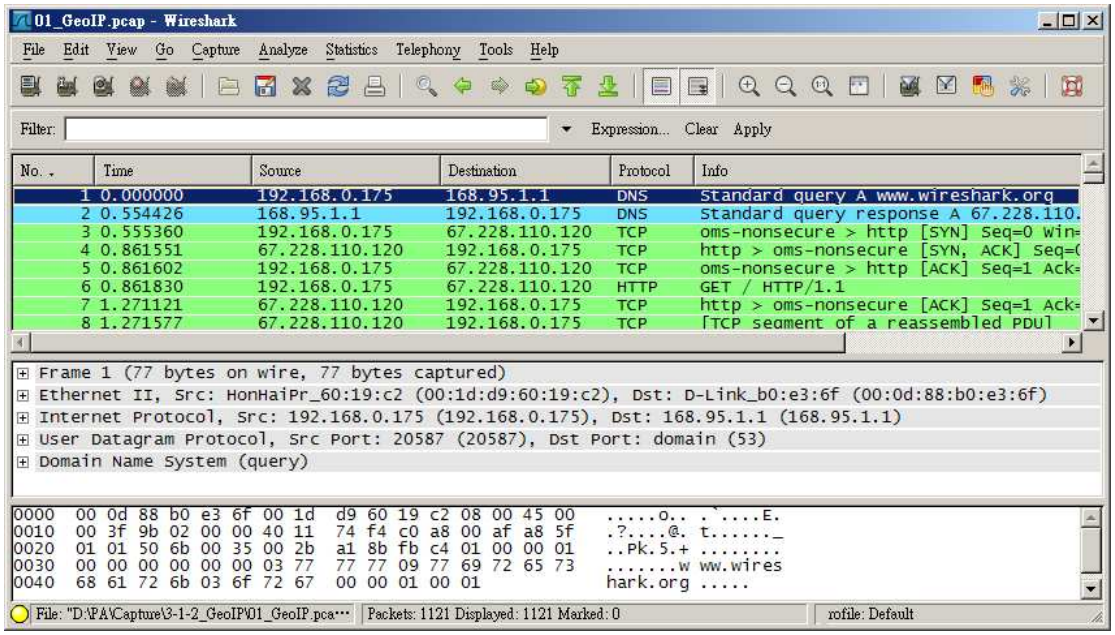
按下「Apply」在按「OK」完成路徑設定



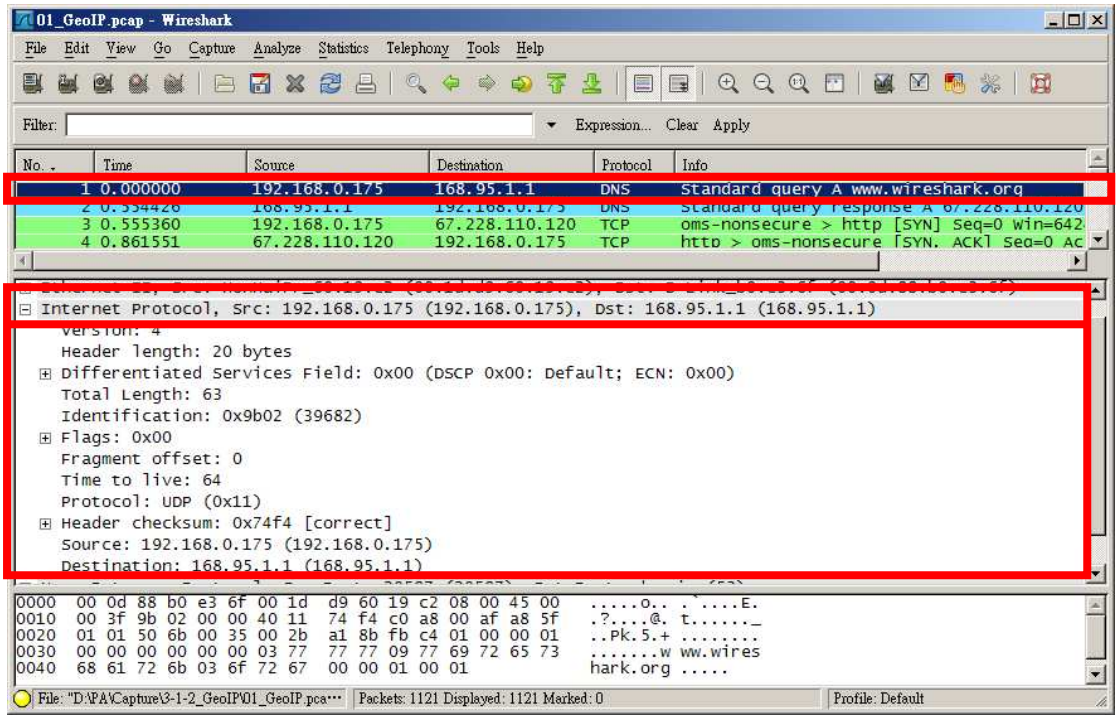
按下「Apply」在按「OK」完成 GeoIP 設定

開始使用 GeoLite

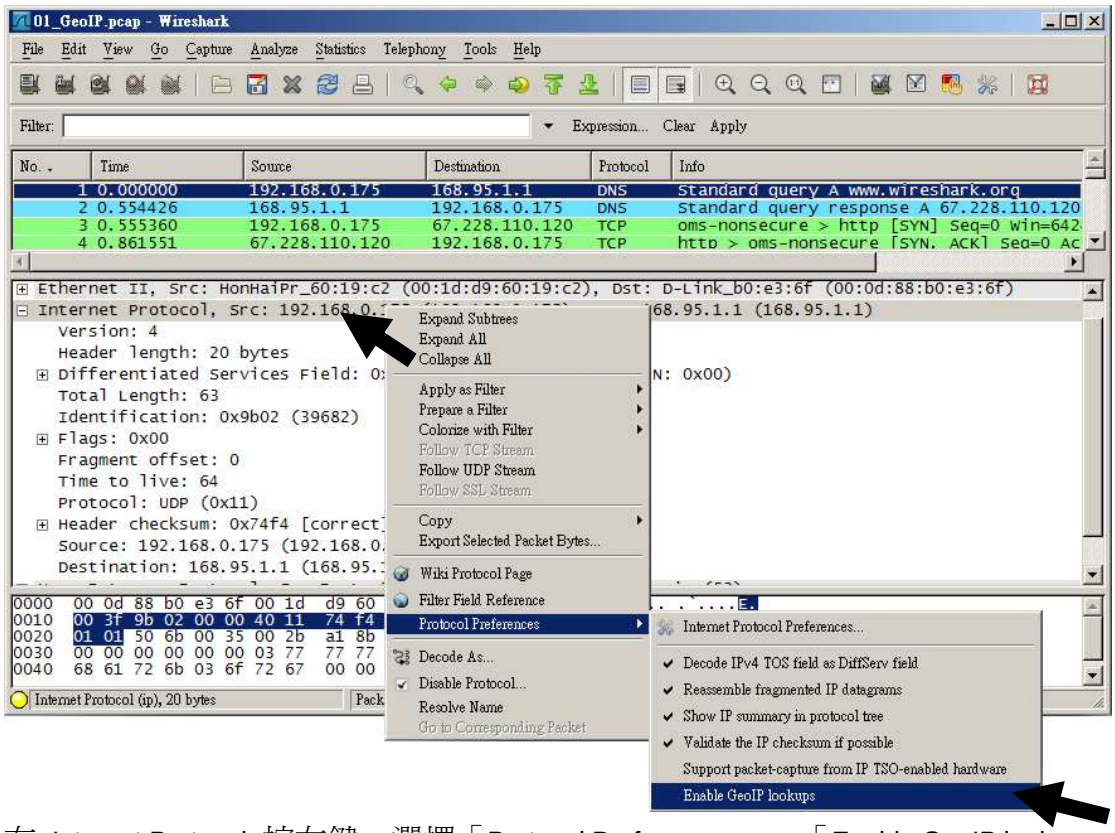
開始使用前，您需要擷取一些封包資料，您可以瀏覽幾個網站或是 Ping 幾個網址、IP，您也可以使用本章節所提供的範例 (本範例可以在 \Capture\Appendix_GeoIP\01_GeoIP.pcap 取得)：



雖然我們設定好 GeoIP (GeoLite)，但是 Wireshark 預設是關閉的，當然您要知道 GeoIP 是以 IP 做辨識，所以我們當然就針對 IP 協定：

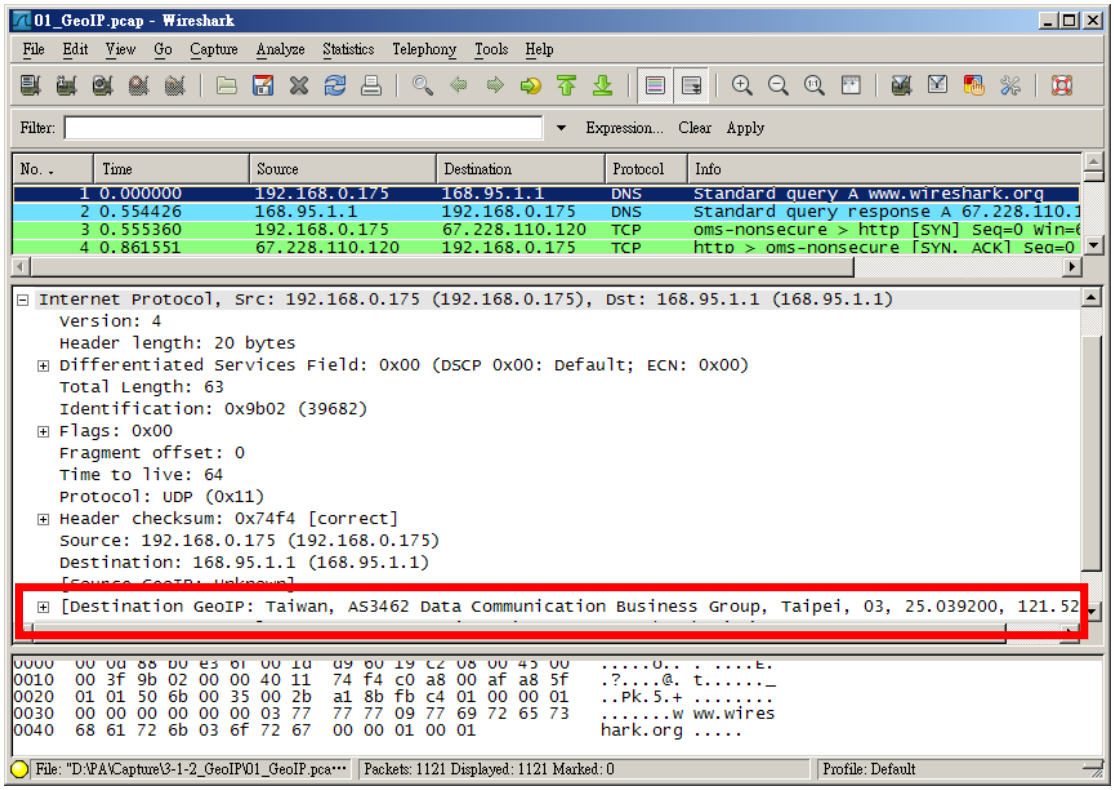


沒錯，似乎是正常的 Wireshark 的表示方法，不過如果開啓 GeoIP 就不一樣了，開啓方式如下：



在 Internet Protocol 按右鍵，選擇「Protocol Preferences」→「Enable GeoIP lookups」

現在已經出現 GeoIP 資料庫中的比對資料：



由於 GeoLite 所提供的內容沒有十分正確，所以如果您有準確度的需求，可以考慮購買 GeoIP 資料庫 (http://www.maxmind.com/app/products)，而安裝方式則都相同。

GeoIP 心得筆記