實驗 - 使用 Wireshark 來觀察 TCP 的三向交握

1. 拓樸

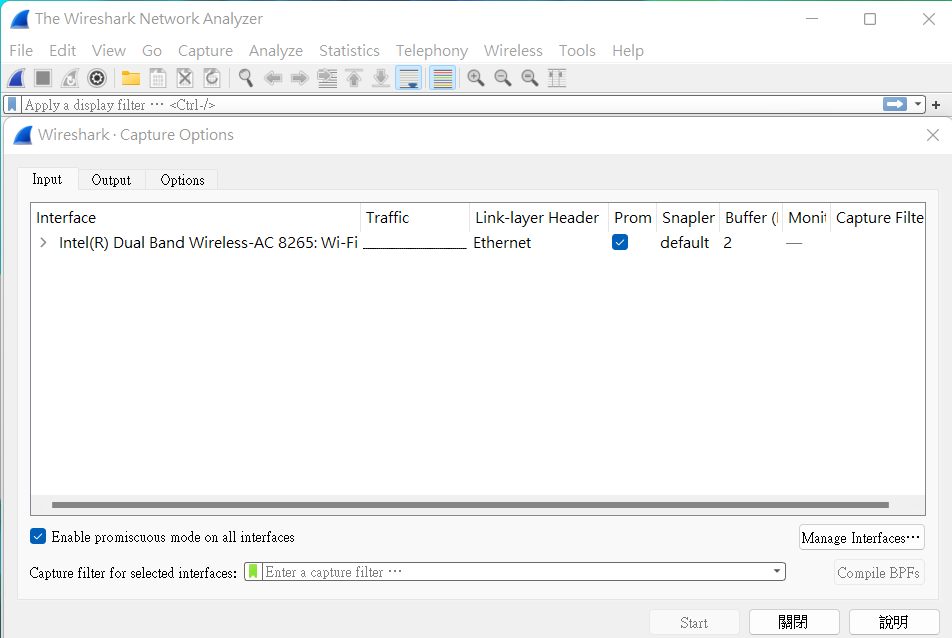


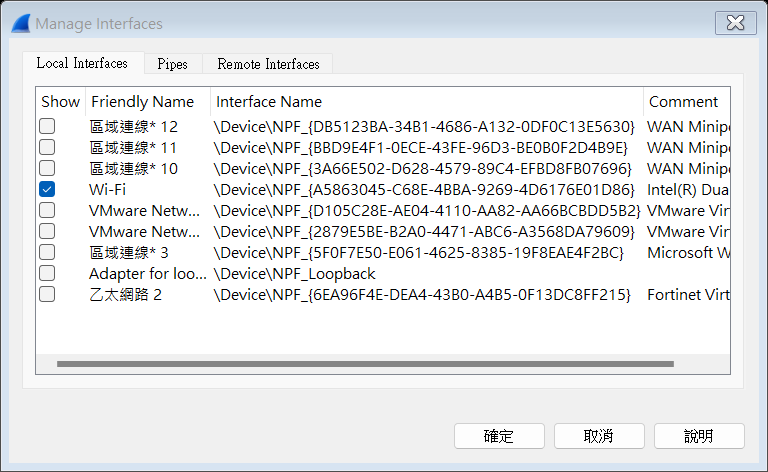
1. 下載：<https://www.wireshark.org/download.html>

安裝 Wireshark-win64-3.6.8.exe

1. 目標

第 1 部分：準備 Wireshark 以擷取封包

* 選擇適當的網卡介面以擷取封包。  
  

選擇適當的網卡介面以擷取封包。  
 

關閉

第 2 部分：擷取、找出和檢查封包

* ipconfig /flushdns
* 擷取到 www.google.com (示範是以www.ntub.edu.tw來做)的 Web 會談。  
  1. 開始 2. 進入瀏覽器開始瀏覽網頁 3. 停止
* 找出 Web 會談的相關封包。arp, dns, tcp, http...
* 檢查封包中的資訊，包括 IP 位址、TCP 連接埠號和 TCP 控制旗標。

1. 背景/場景

在本實驗中，你將使用 Wireshark 來擷取並檢查封包，封包是在使用超文字傳輸協定 (HTTP) 的 PC 瀏覽器和 Web 伺服器（例如 www.ntub.edu.tw or [www.google.com](http://www.google.com)）之間產生的。當一個應用程式，例如 HTTP 或檔案傳輸協定 (FTP)，在主機上首次啟動時，TCP 將使用三向交握來建立兩個主機之間的可靠 TCP 會談。例如，當 PC 使用 Web 瀏覽器瀏覽網際網路時，將會發起三向交握，而且 PC 主機和 Web 伺服器之間將建立會談。一個 PC 可以同時與多個網站進行多個活動的 TCP 會談。

**注意**：本實驗使用 Netlab 無法完成。本實驗假定你可以存取 Internet。

1. 所需資源

1 台 PC（採用 Windows 11 且可以存取命令提示字元和 Internet，並且已安裝 Wireshark）

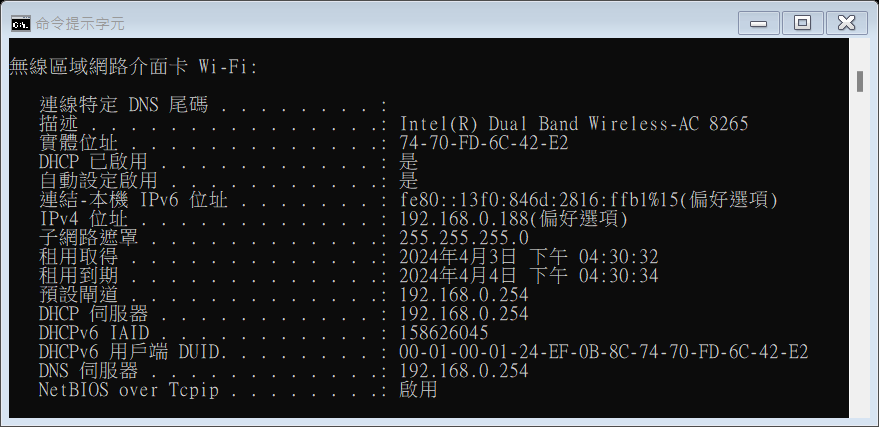
1. 準備 Wireshark 以擷取封包

在第 1 部分，你將啟動 Wireshark 程序並選擇適當的介面開始擷取封包。

1. 檢索 PC 的介面位址。

對於本實驗，你需要檢索 PC 的 IP 位址及其網路介面卡 (NIC) 實體位址（也稱為 MAC 位址）。

* + 1. 打開命令提示視窗，輸入 **ipconfig /all**，然後按下 Enter 鍵。



* + 1. 寫下與選中的乙太網路配接卡相關聯的 IP 位址和 MAC 位址，因為它是檢查擷取封包時所需的來源位址。

PC 的主機 IP 位址：\_\_\_\_\_\_\_\_\_\_\_\_192.168.0.188 \_\_\_\_\_\_\_\_\_\_\_[本次作業以此識別你的ID]

PC 的主機 MAC 位址：\_\_\_\_\_\_\_\_\_74-70-FD-6C-42-E2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 啟動 Wireshark 並選擇適當的介面。
   * 1. 按一下 Windows“**開始**”按鈕，並在彈出功能表中按兩下 **Wireshark**。
     2. 在 Wireshark 啟動之後，按一下 **Interface List**（介面清單）。

參考第 1 部分

* + 1. 在 **Wireshark: Capture Interfaces**（Wireshark：擷取介面）視窗，按一下與你的 LAN 連接的介面旁的核取方塊。

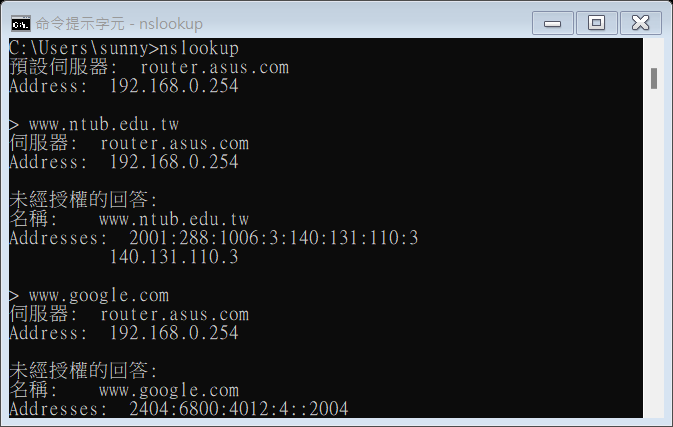
參考第 1 部分

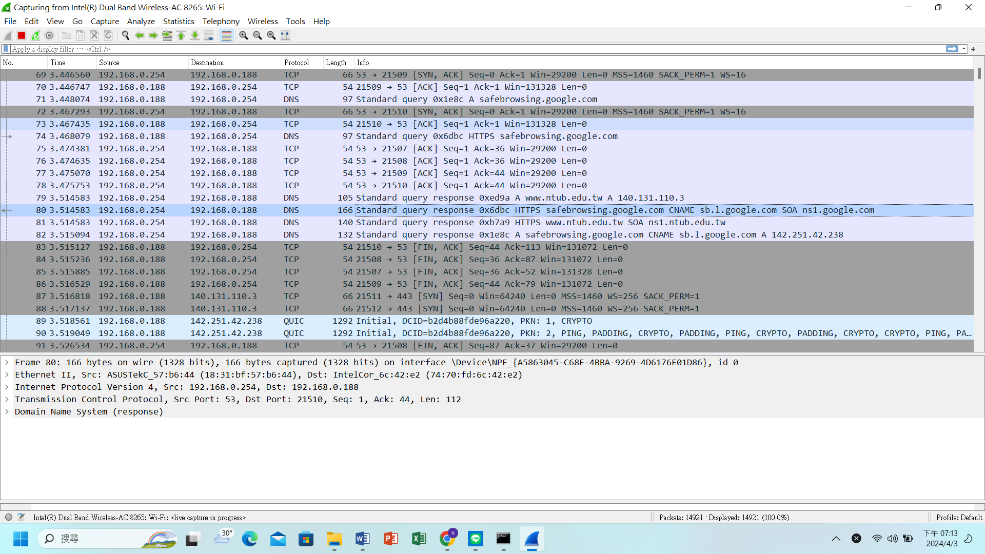
**注意**：如果列出了多個介面，而你不能確定要檢查那個介面，請按一下 **Details**（詳細資訊）。按一下**802.3 (Ethernet)** [802.3 (乙太網路)] 頁標籤，並驗證 MAC 位址是否與你在步驟 1b 中記錄的相匹配。驗證完成後關閉 Interface Details（介面詳細資訊）視窗。

1. 擷取、定位和檢查封包
2. (建議先清除DNS快取 ，命令ipconfig /flushdns)，按一下 Start（開始） 按鈕開始資料擷取。
   * 1. 存取以www.ntub.edu.tw來做。最小化 Google 視窗，然後返回 Wireshark。停止資料擷取 。你應該看到擷取的流量，和下面步驟 b 中顯示的類似。

**注意**：你的教師可能會提供其他網站。請在此寫下網站名稱或位址：

\_\_\_www.ntub.edu.tw:\_\_140.131.110.3[8c.83.6e.03]\_\_\_\_\_\_\_[www.google.com](http://www.google.com) :142.251.43.4,

   
\_\_\_tw.yahoo.com:\_\_180.222.102.201\_\_\_\_

* + 1. 現在擷取視窗處於活動狀態。找到 **Source**（來源）、**Destination**（目的地）和 **Protocol**（協定）欄。 

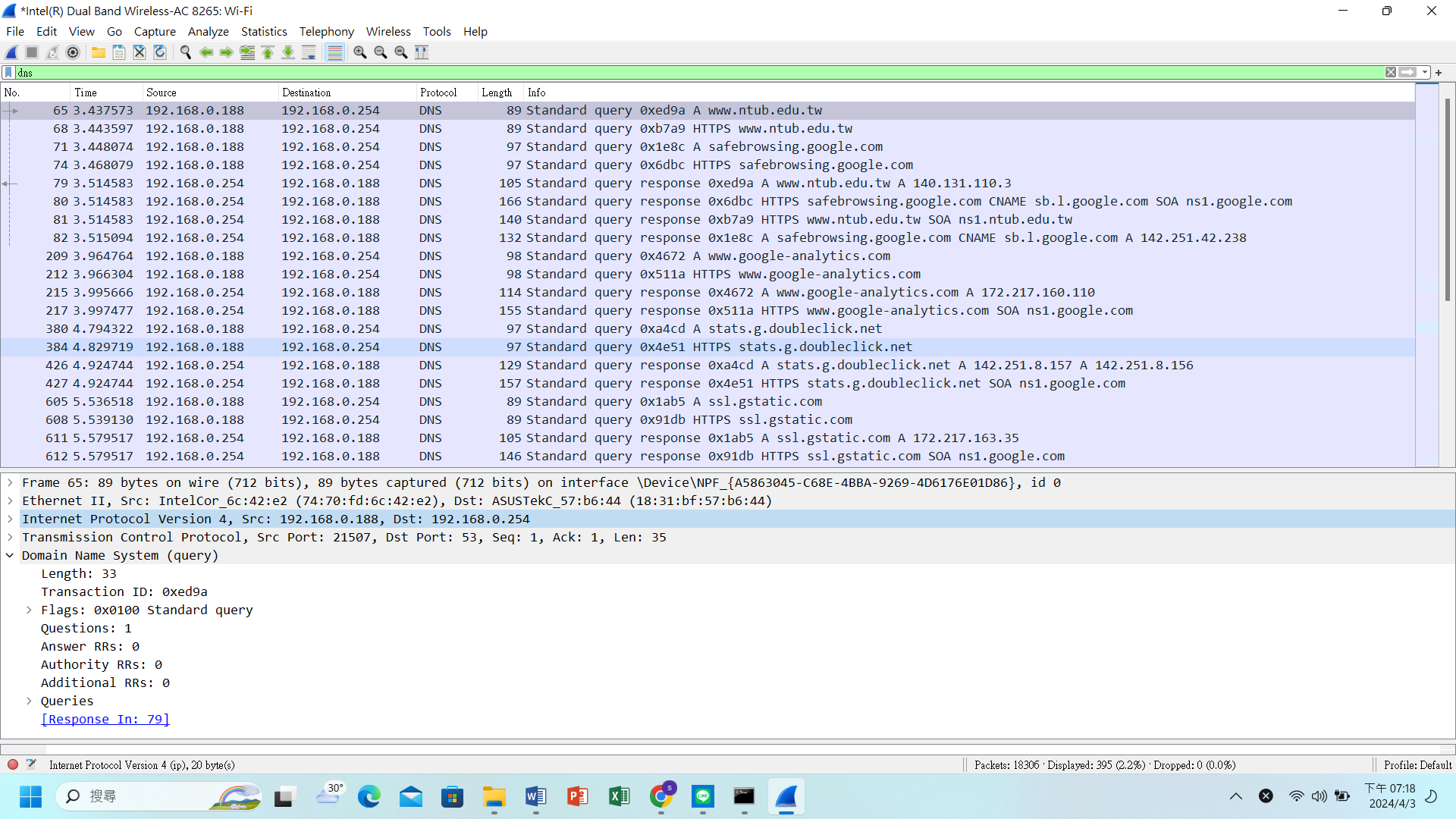
**抓到所有封包**

**封裝表頭資料**

[www.ntub.edu.tw:\_\_140.131.110.3[8c.83.6e.03]\_](http://www.ntub.edu.tw:__140.131.110.3[8c.83.6e.03]_)

建議你用分類的方式去找我們需要的封包

1. 過濾DNS封包，得到如下畫面，我家的DNS伺服器IP位址是192.168.0.254



**傳輸層資料：2024/4/2**5

**應用層資料**

frame 65：PC(192.168.0.188) -->查詢台北商業大學網域名稱的IP -->DNS伺服器IP 192.168.0.254

frame 79：DNS伺服器回應查到的IP是140.131.110.3

1. 查詢 Web 會談的相應封包。

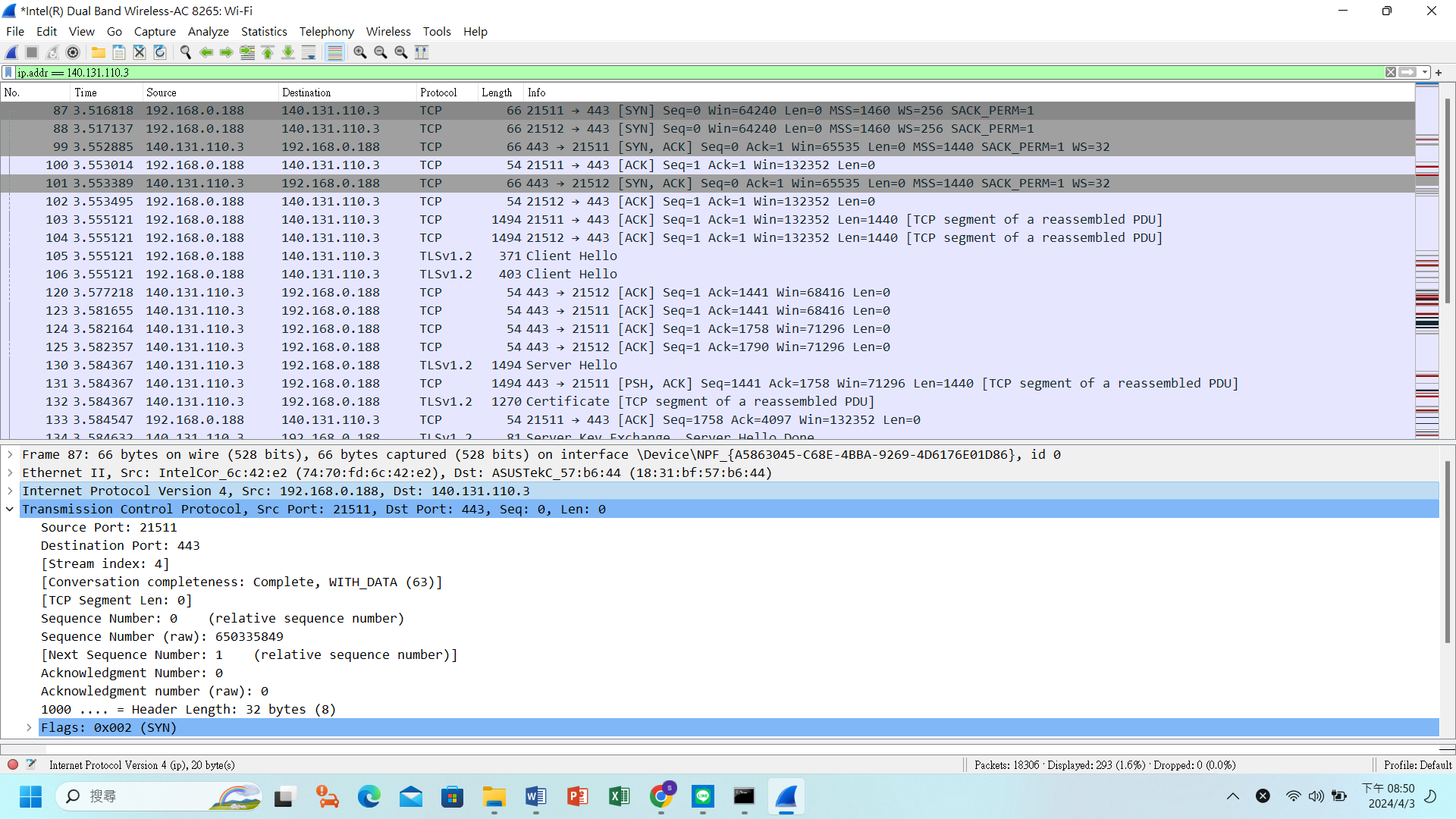
如果電腦是最近啟動的而且沒有存取網際網路，則你可以在擷取輸出中看到整個程序，包括位址解析通訊協定 (ARP)、網域名稱系統 (DNS) 和 TCP 三向交握。第 2 部分步驟 1 中的擷取頁面顯示電腦必須向www.ntub.edu.tw 傳送的所有封包。在本例中，PC 已經擁有預設閘道的 ARP 條目；因此它首先發出 DNS 查詢以解析 www.ntub.edu.tw。

* + 1. 訊框 65 顯示了從 PC 發送到 DNS 伺服器的 DNS 查詢，嘗試將網域名稱 (www.ntub.edu.tw) 解析為 Web 伺服器的 IP 位址。PC 必須獲取到該位址才能將第一個封包發送至 Web 伺服器。

電腦查詢的 DNS 伺服器的 IP 位址是多少？ \_\_192.168.0.254\_\_

* + 1. 訊框 79 是 DNS 伺服器作出的回應，其中含有 www.ntub.edu.tw 的 IP 位址？ \_\_\_\_\_140.131.110.3\_\_\_\_\_。
    2. 找到相應封包以開始三向交握。在本範例中，訊框 372 是 TCP 三向交握的開始。如果你有許多與 TCP 連接無關的封包，則可能需要使用 Wireshark 過濾器功能。在 Wireshark 的過濾器框中輸入**tcp**並按 Enter 鍵。[這步自行做]
* 先用 tcp 或 ip.addr==140.131.110.3 關鍵字去過濾封包
* 在找目的位址是140.131.110.3開始封包 ==> 訊框 372
* 訊框 372 是 TCP 三向交握的開始

以下是用IP的方法ip.addr == 140.131.110.3



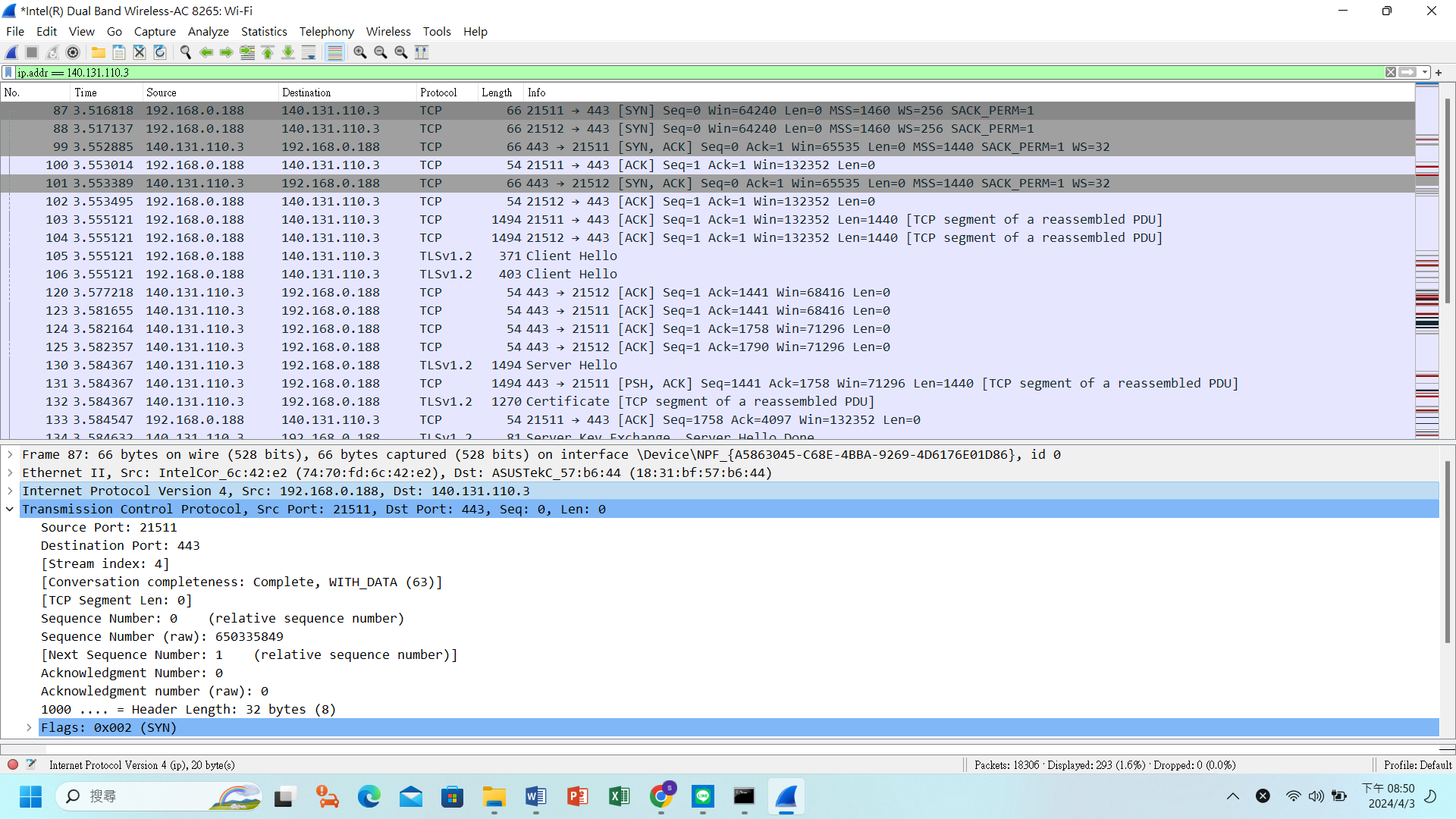
點開

傳輸層

1. 檢查封包中的資訊，包括 IP 位址、TCP 連接埠號和 TCP 控制旗標。

IP 位址

TCP 連接埠號

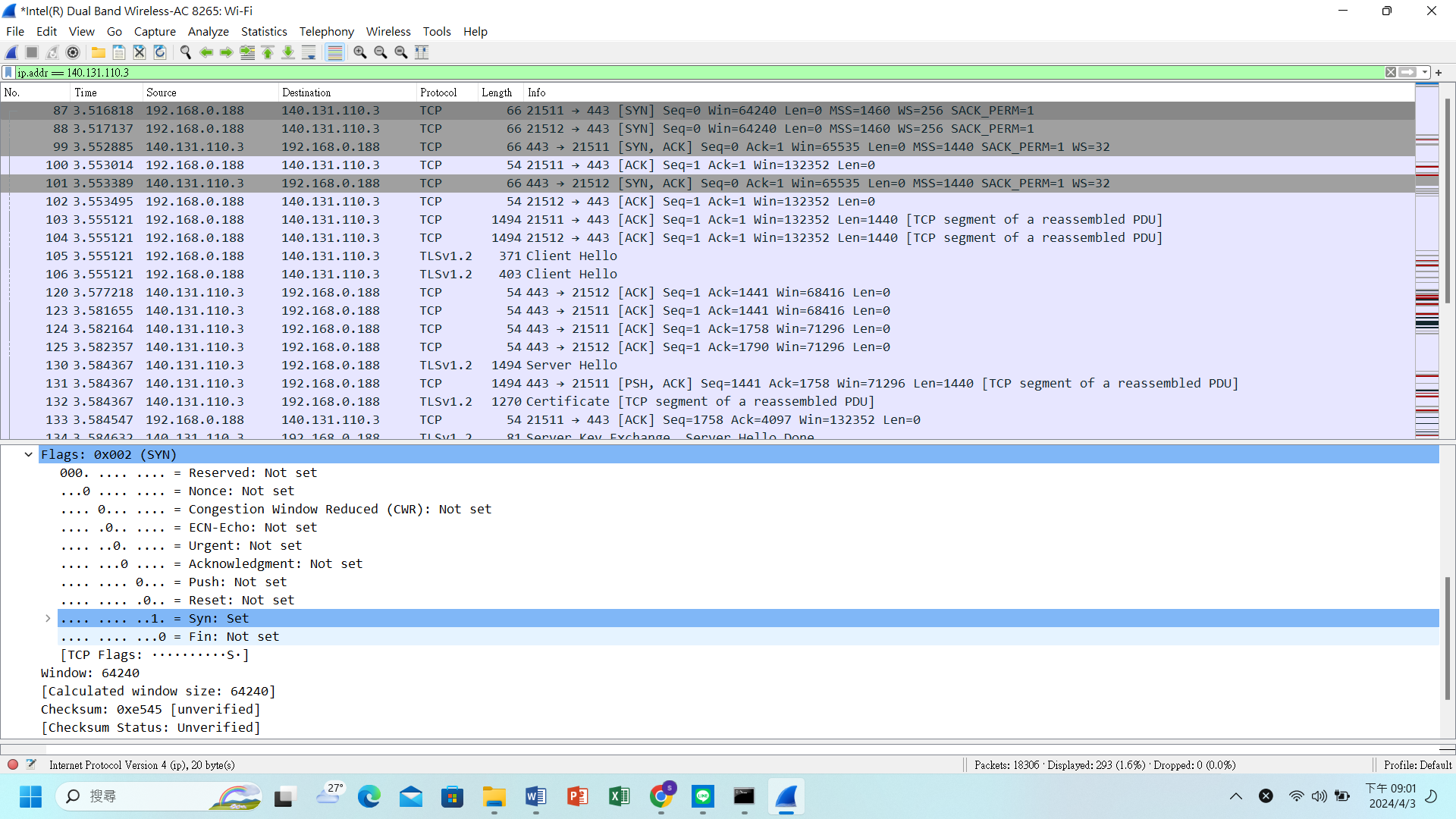


TCP控制旗標號

* + 1. 在我們的範例中，訊框 87 是 PC 和 NTUB Web 伺服器之間三向交握的開始。在封包清單窗格（主視窗的頂部）中選擇此訊框。這將使這一行反白顯示，並在下面兩個窗格中顯示該封包的解碼資訊。檢查封包詳細資訊窗格（主視窗的中間部分）中的 TCP 資訊。
    2. 按一下封包詳細資訊窗格中傳輸控制協定左側的**+**圖示展開 TCP 資訊顯示。

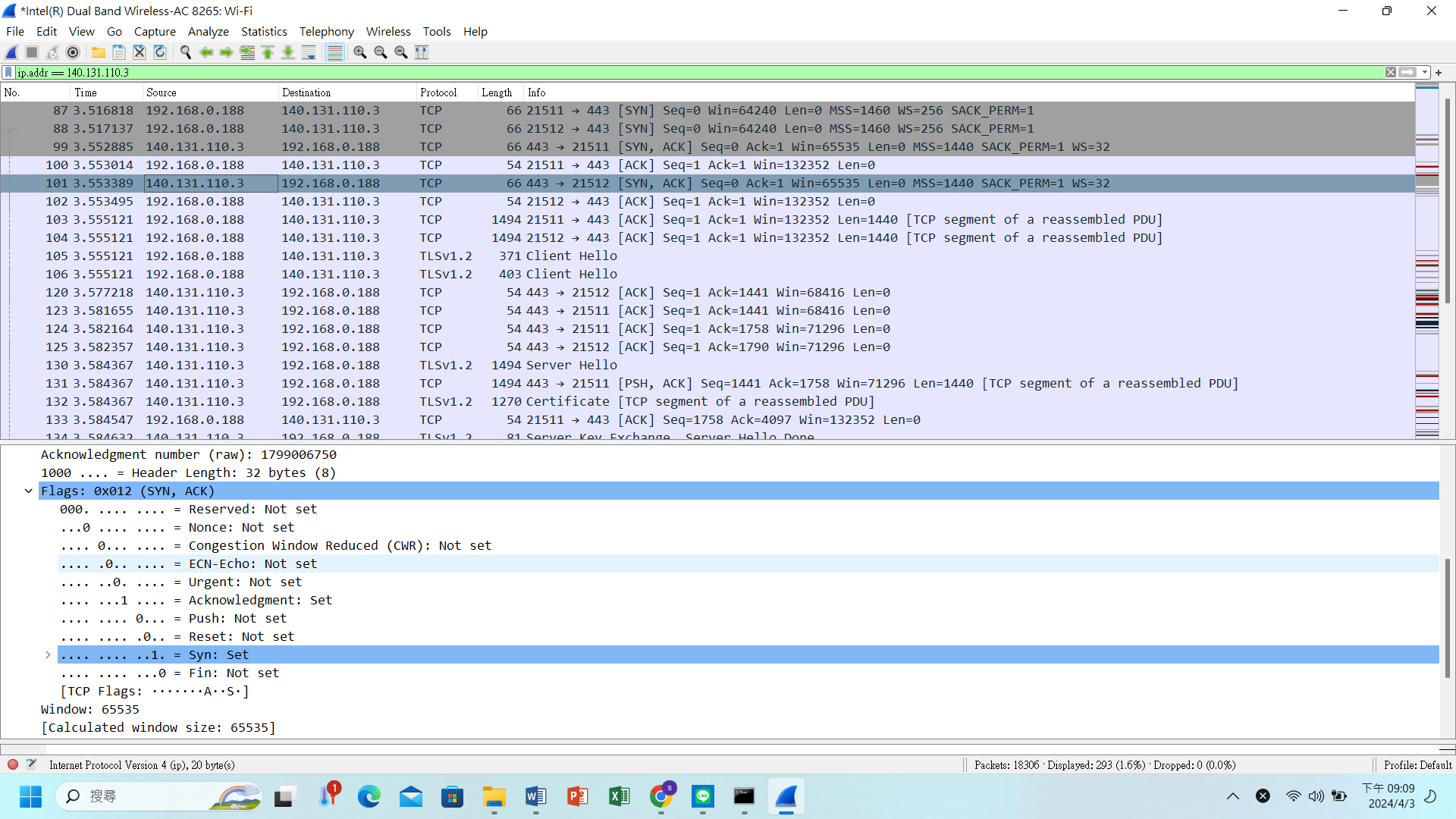
* + 1. 按一下 Flags（旗標）左側的**+**圖示。查看來源連接埠和目的連接埠以及所設定的旗標。

**注意**：你可能需要調整 Wireshark 中頂部和中間視窗的大小以顯示所需資訊。



TCP 的來源連接埠號是什麼？ \_\_\_\_21511\_\_\_\_\_\_\_\_\_\_\_\_\_   
你將對該來源連接埠如何歸類？ \_\_\_**私有**和/或**動態埠**\_\_\_\_\_\_   
TCP 的目的連接埠號是什麼？ \_\_\_\_\_\_443\_\_\_\_\_\_\_\_\_\_\_   
你將對該目的連接埠如何歸類？ \_\_\_**公認埠Well-known Ports** \_\_   
設定了什麼旗標？ \_\_\_\_SYN=1\_\_\_\_\_\_\_   
對應的序號設定為多少？ \_Sequence Number = 0\_\_\_\_

要選擇三向交握中的下一個訊框，請在 Wireshark 功能表中選擇 **Go**（轉至）並選擇 **Next Packet In Conversation**（對話中的下一封包）。在本範例中是訊框 373。

這是 NTUB Web 伺服器對啟動會談的初始請求作出的回應。 

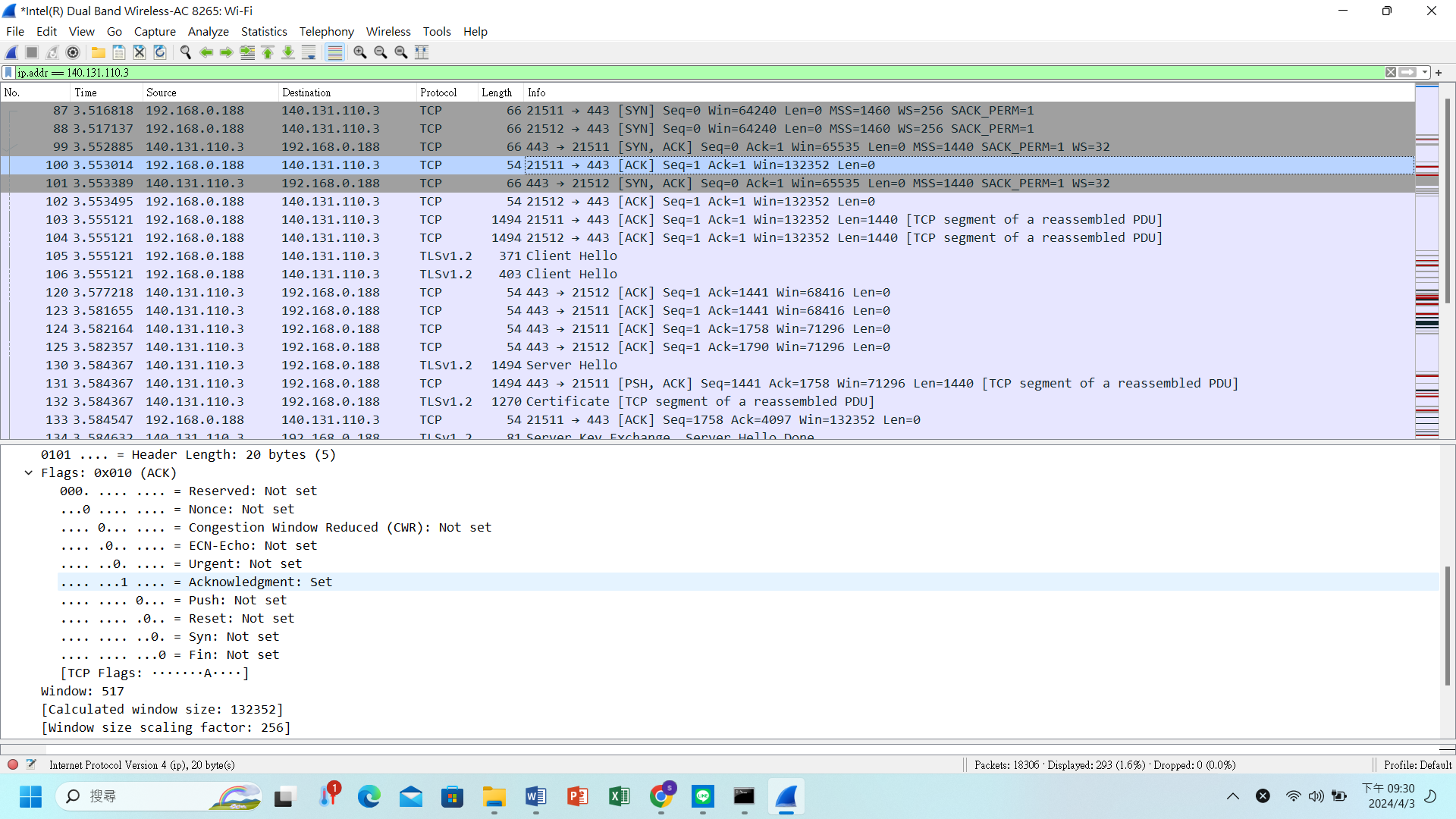
來源連接埠和目的連接埠的值是什麼？ \_\_來源連接埠=443, 目的連接埠=21511\_\_\_\_\_

設定了那些旗標？ \_\_Acknowledgment : set (=1), SYN=1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

對應的序號和確認號設定為什麼？

\_\_\_\_ Sequence Number : 0, Acknowledgment Number : 1\_\_\_\_\_\_\_\_\_

最後，檢查範例中三向交握的第三個封包。按一下視窗頂部的訊框 374 將顯示本範例中的以下資訊：



檢查交握的第三個和最後一個封包。

設定了什麼旗標？ \_\_\_ Acknowledgment : set (=1)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

將對應的序號和確認號設定為 1 作為起點。TCP 連接現已建立，來源電腦與 Web 伺服器之間可以開始通訊。

* + 1. 關閉 Wireshark 程序。

1. 思考
   1. 在 Wireshark 中有上百個過濾器可用。大型網路可以有多個過濾器和許多不同類型的流量。清單中的那三個過濾器可能對網路系統管理員最有用？

IP位置過濾器、協議過濾器、端口過濾器

* 1. Wireshark 在生產網路中的其他使用方式是什麼？

安全監控、威脅檢測、應用程序分析、故障排除