Wireshark Lab

組長:資管二甲 B0444132 張仁樵

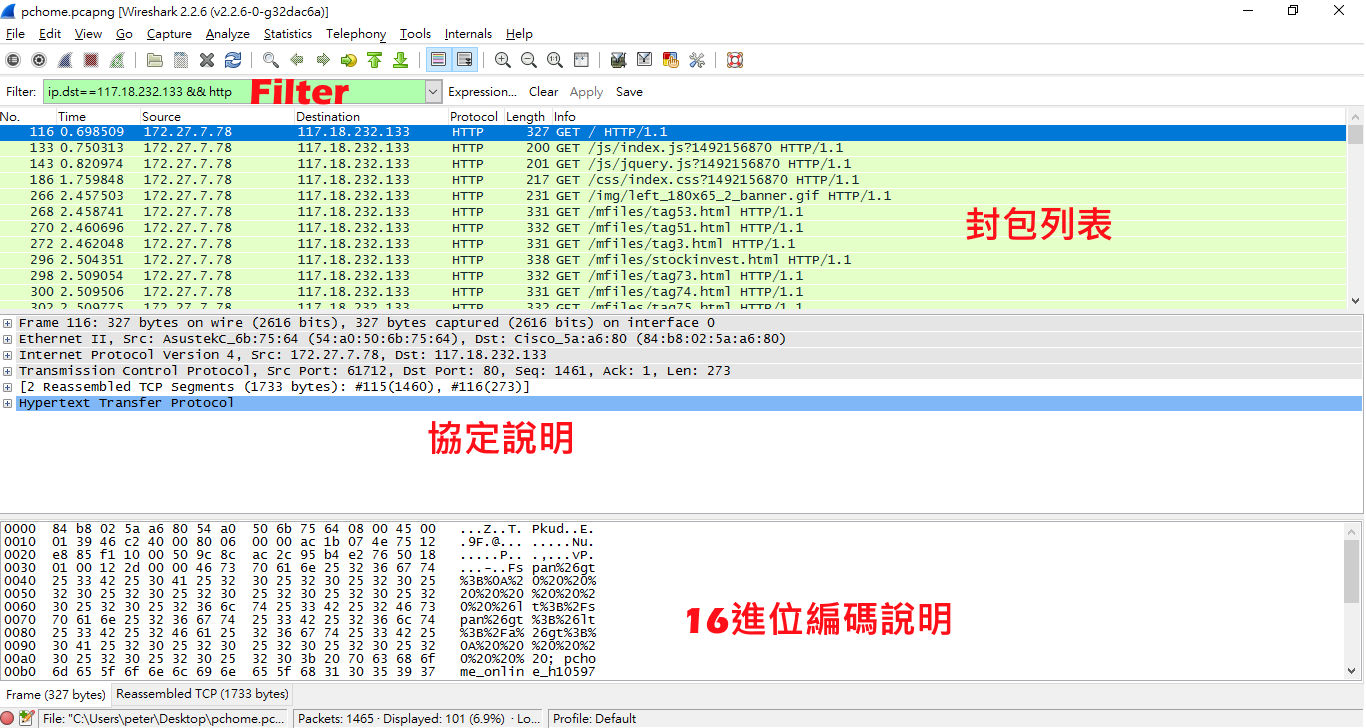
組員:資管二甲 B0444101 李積舜

組員:資管二甲 B0444138 潘楚華

組員:資管二甲 B0444146 林子由

壹、介面與功能

一、Wireshark的視窗介面



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

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

1.「封包列表」欄位(Packet List):

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

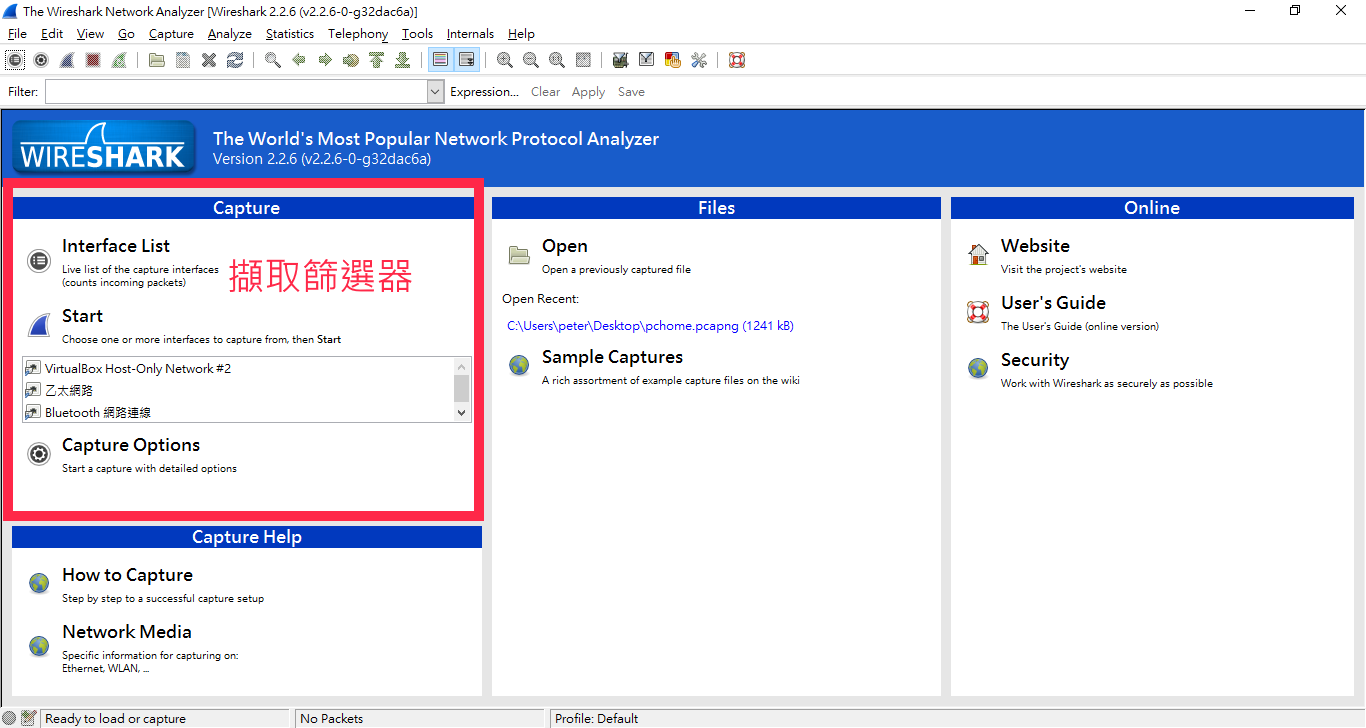
2.「協定說明」欄位(Packet Detail):

「協定說明」欄位在中間的部分，說明所點選封包詳細的協定內容，協定前若有+圖示，表示協定內容還可以再細分，以樹狀方式進一步對該協定內容進行顯示。

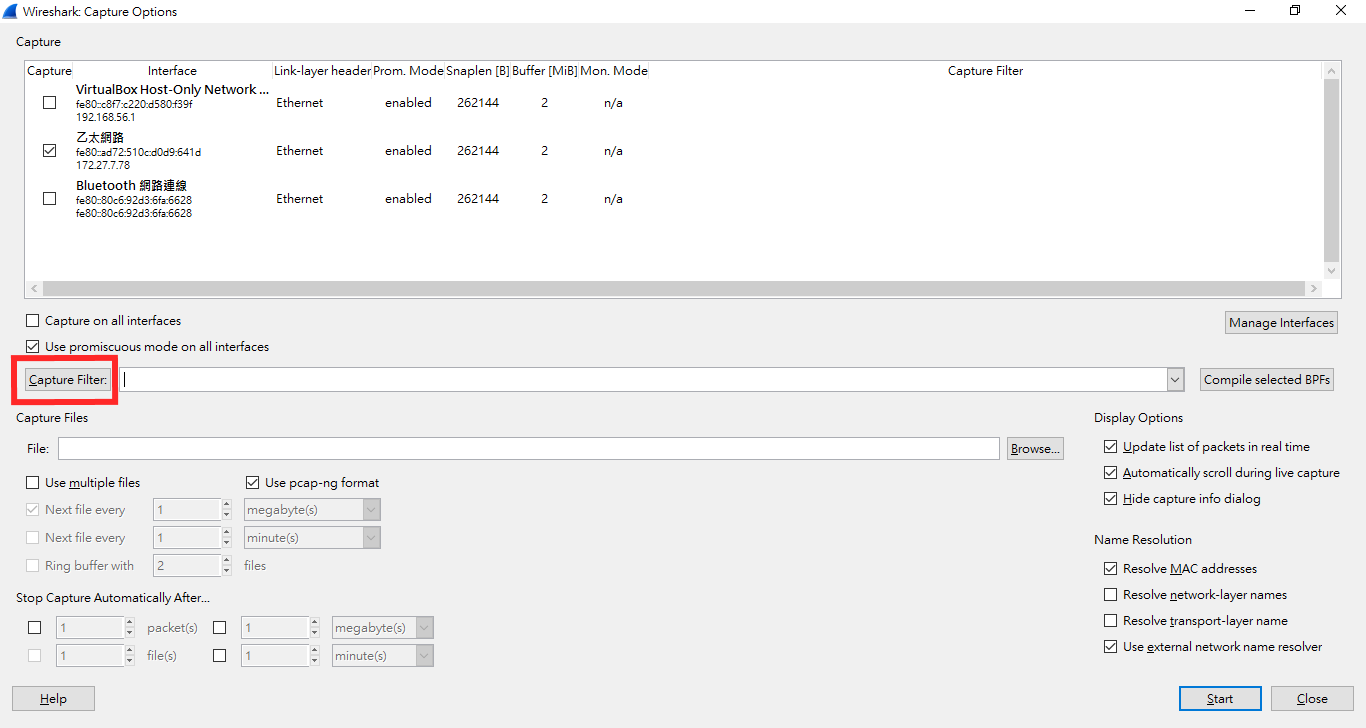
3.「16進位編碼說明」欄位(Packet Bytes):

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

二、擷取過濾器 (Capture Filter)



↑選擇完網路介面卡後(在此我們是使用乙太網路)，點選「Capture Options」後會進入下方的畫面。



↑如上圖所示，有許多項目可以對封包的擷取情況進行選擇，選取的項目，在此我們針對其中幾個常用的項目進行說明(在此我們使用過濾器的功能進行限制如下圖所示):

1.封包大小限定:

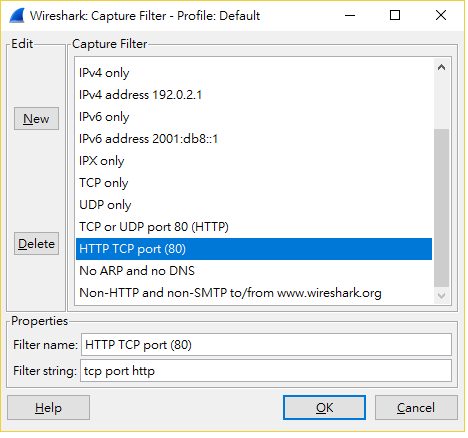
用來對最大封包位元組進行限制，以乙太網路的封包而言，最大不會超過1518位元組，可對自己期望擷取的封包大小進行限定。若對封包大小情況未知，就不要進行設定。

2.過濾器:

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

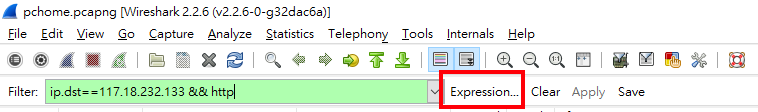
3.檔案名稱:

用於將擷取的封包資料儲存在檔案中，對檔案名稱進行說明，以方便日後再進行分析。

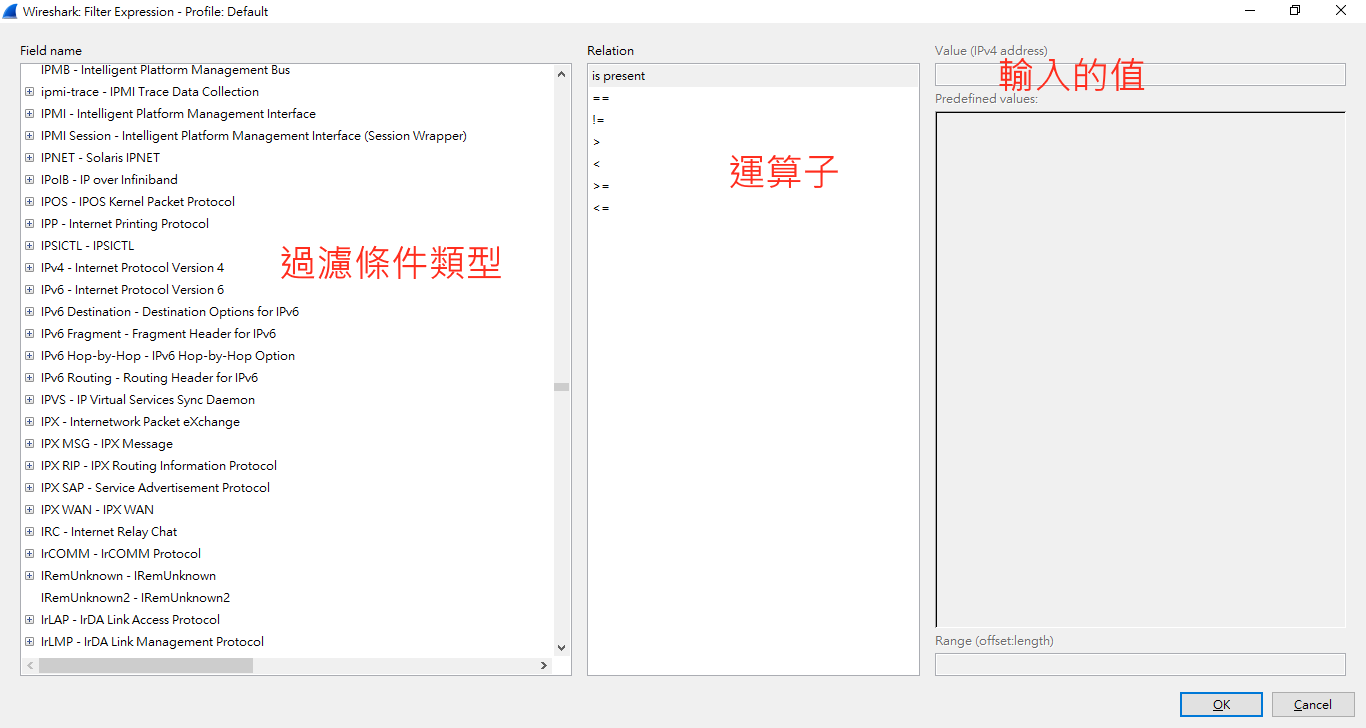


↑我們限制了TCP only以及HTTP TCP port(80)的條件

三、顯示過濾器 (Display Filter)



↑Wireshark過濾封包工具如上圖所示，在主畫面視窗下方的「過濾器(Filter)」進行，過濾器使用簡易的條件 是幫助使用者過濾出想要分析的封包，以避免有過多無用封包項目的干擾，提升封包管理的效益。條件是輸入後，以「Apply」按鈕進行封包過濾，或是按下「Expression」進入到下面的畫面進行過濾條件的過濾，而「Clear」則是清空所有的條件。



↑如果有+圖示，則可以點開有更詳細的內容可以進行選擇。

篩選語法:

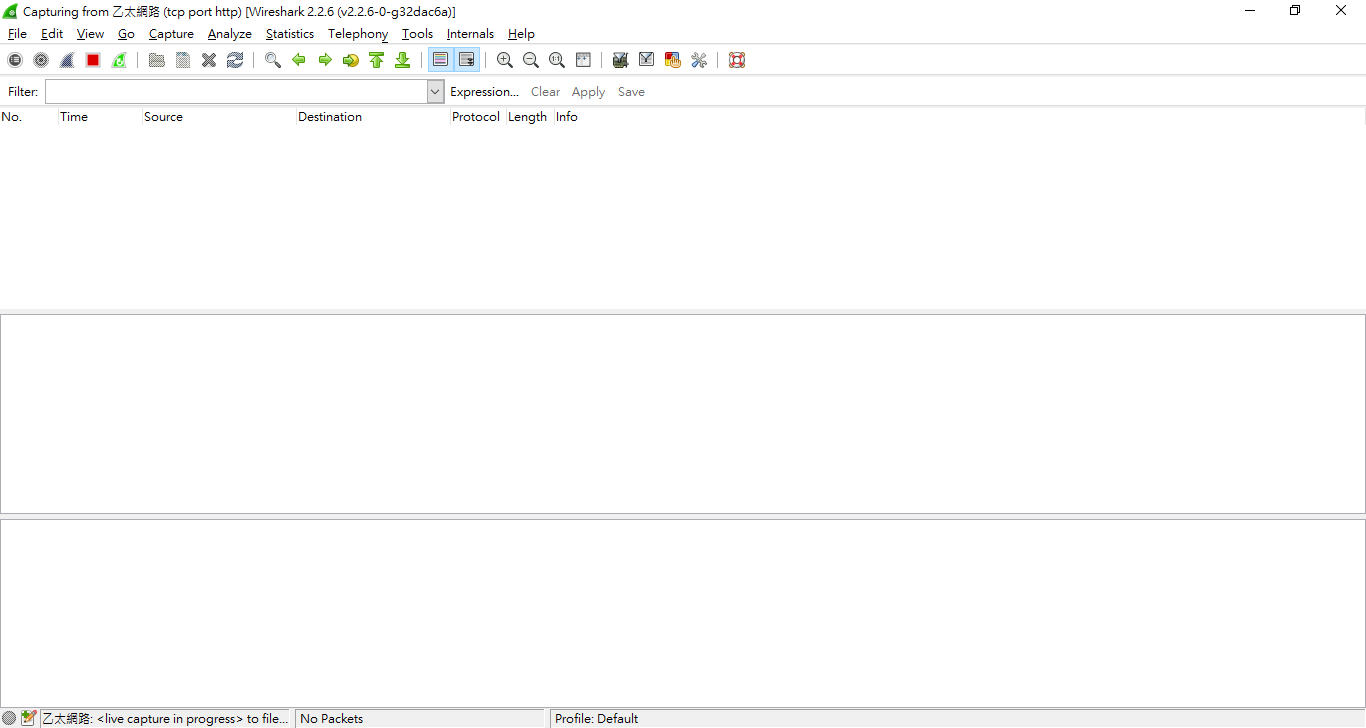
|  |  |  |
| --- | --- | --- |
| 關於 | 運算子 | 範例 |
| 等於 | eq | ip.proto eq 1 |
| == | ip.proto == 1 |
| 不等於 | ne | ip.proto ne 1 |
| != | ip.proto != 1 |
| 大於 | gt | Frame.pkt\_len gt 100 |
| > | Frame.pkt\_len > 100 |
| 小於 | lt | Frame.pkt\_len lt 100 |
| < | Frame.pkt\_len < 100 |

|  |  |  |  |
| --- | --- | --- | --- |
| 類型 | | 作用說明 | 舉例 |
| ip | dst | 目的IP | ip.dst==140.134.4.1 |
| src | 來源IP | ip.src == 140.134.30.72 |
| addr | IP位址 | ip.addr ==140.134.30.72 |
| proto | 下一層協定 | ip.proto == 0x06(TCP) ip.proto == 0x01(ICMP) ip.proto == 0x11(UDP) |

|  |  |  |
| --- | --- | --- |
| 邏輯 | 運算子 | 範例 |
| AND | and | ip.proto == 1 and ip.dst == 140.134.30.72 |
| && | ip.proto == 1 && ip.dst == 140.134.30.72 |
| OR | or | ip.proto == 1 or ip.dst == 140.134.30.7 |
| || | ip.proto == 1 || ip.dst == 140.134.30.72 |
| NOT | not | not(ip.proto == 1 |
| ! | !(ip.proto == 1) |

貳、應用一:PChome

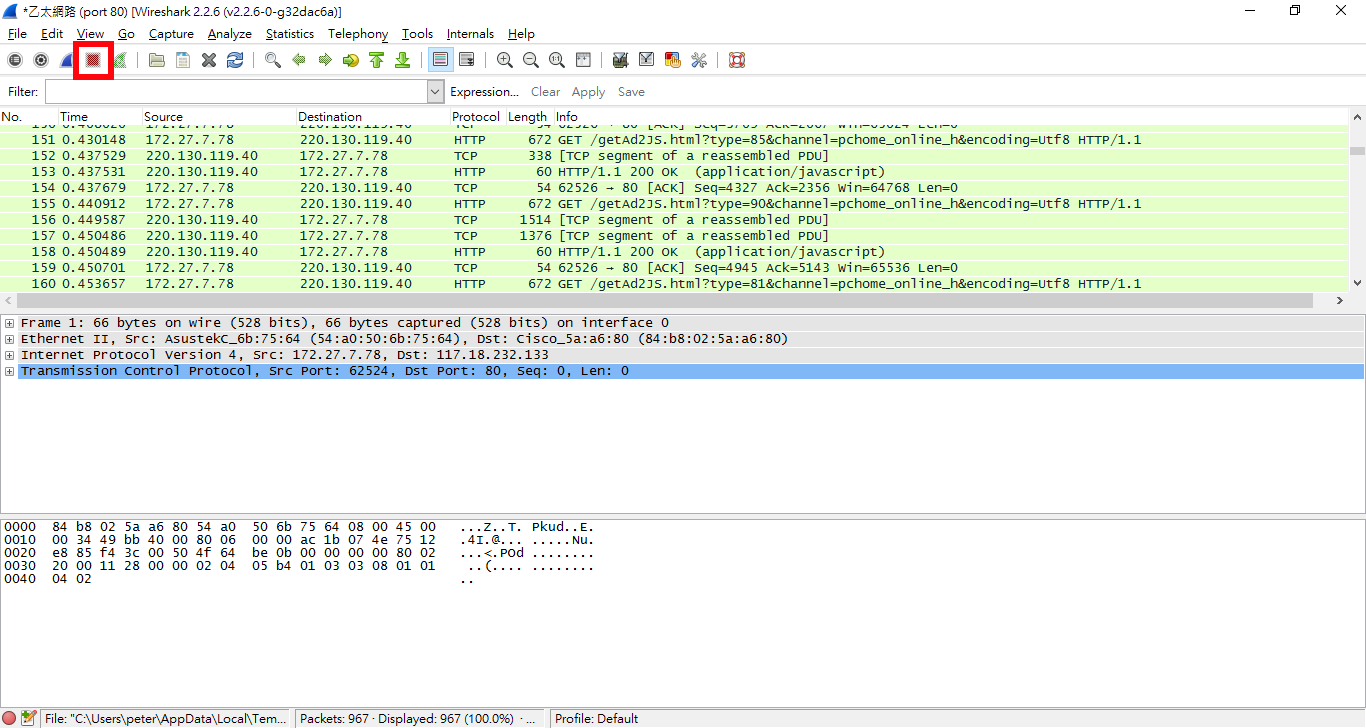
一、封包擷取



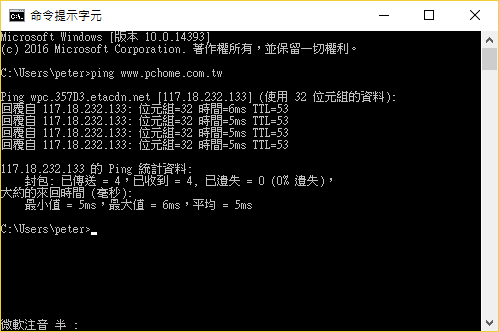
↑首先我們設定完擷取過濾器後。



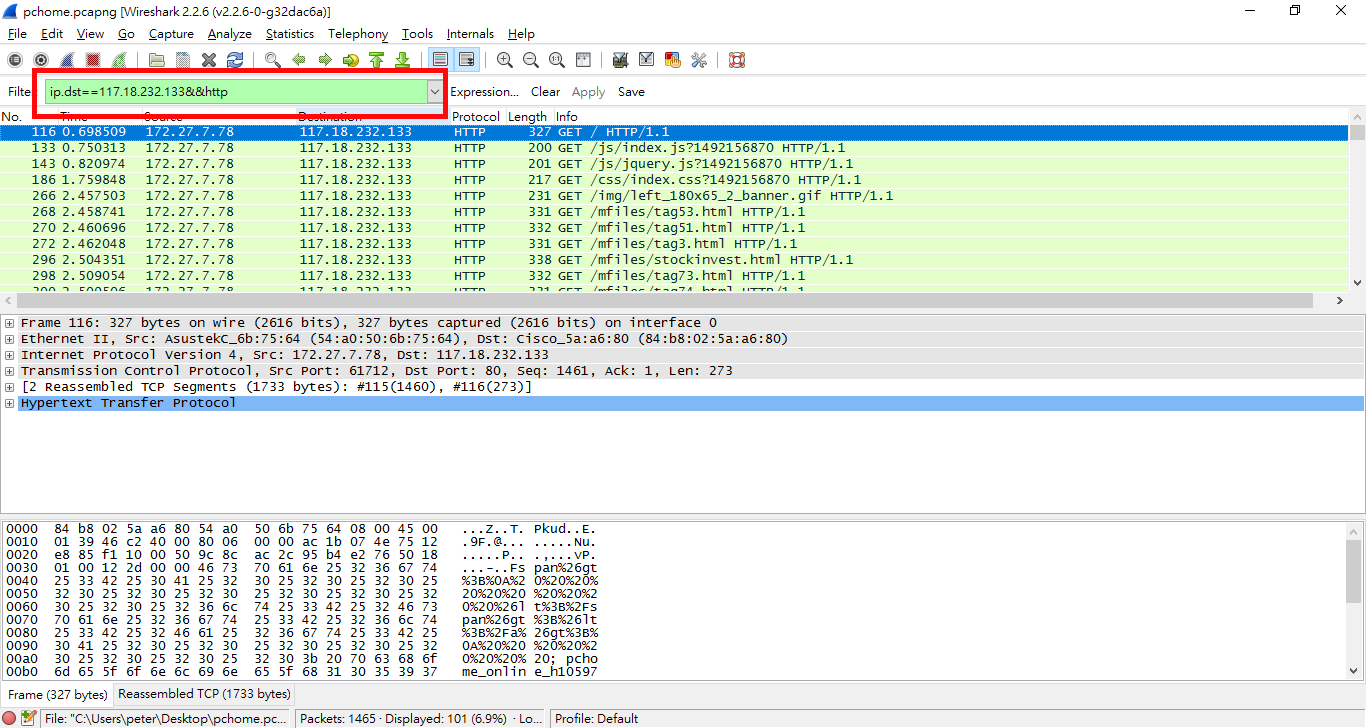
↑我們進入Google瀏覽器，進入PChome的首頁後。



↑接著我們回到Wireshark按下停止鈕。

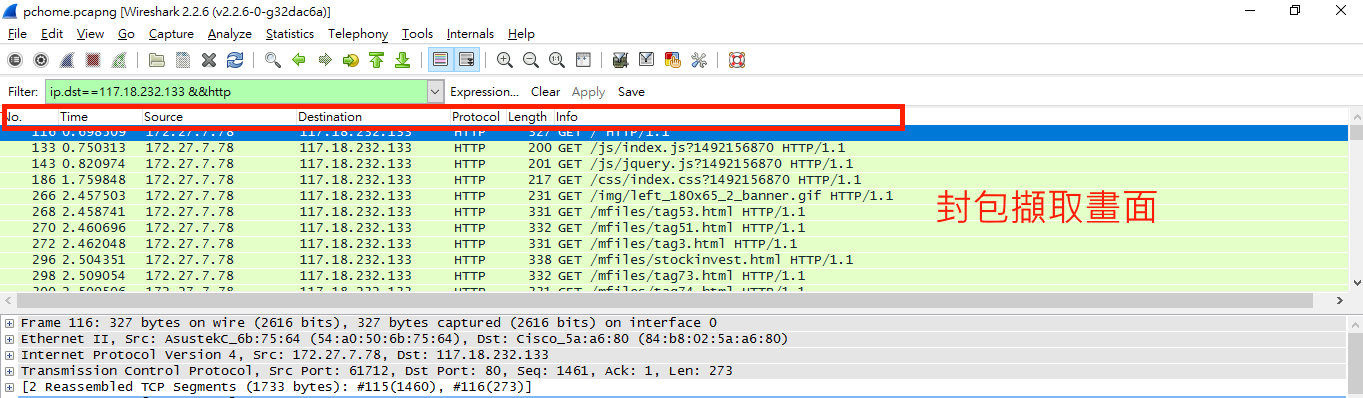


↑接著我們進入命令提示字元，輸入ping www.pchome.com.tw 的指令查PChome首頁的IP[117.18.232.133]。



↑接著我們利用顯示過濾器下ip.dst==117.18.232.133&&http的條件，ip.dst是確保我們抓到的是PChome的首頁，並且我們用http的條件來進行再次確認。

二、封包內容說明



1.No:封包的編號，PChome首頁的封包編號為116。

2.Time:封包的時間戳，可以通過View>>Time Display Format設定所要用的時間格式。

3.Source:封包的來源IP，通常為本機自己的IP，可以利用命令提示字元輸入ipconfig來進行查詢。

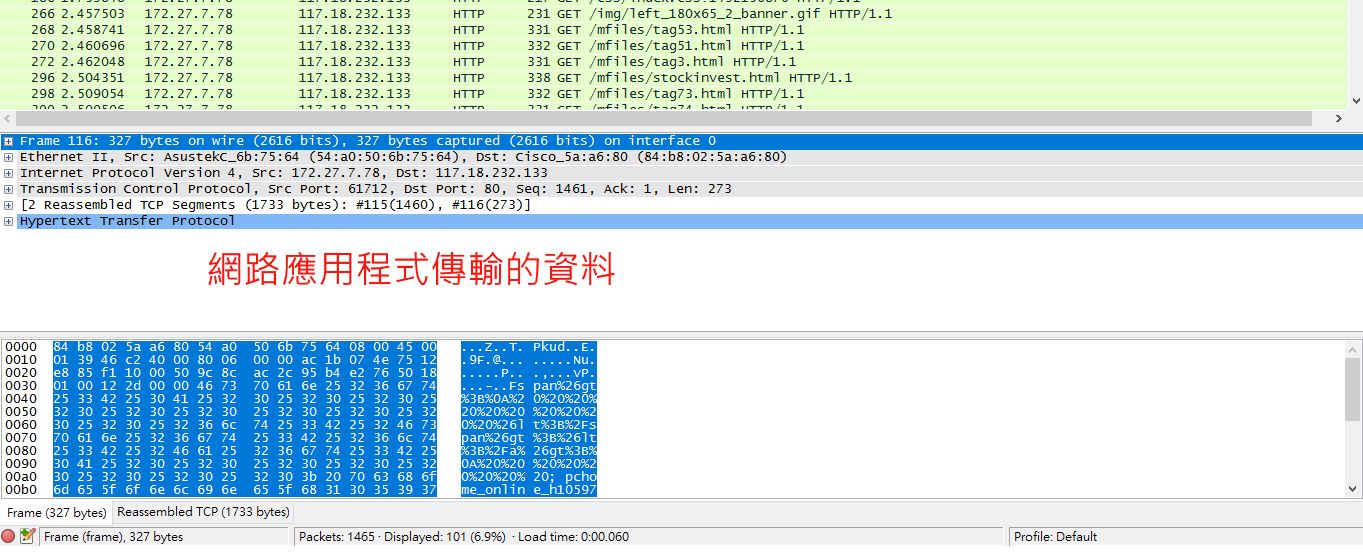
4.Destination:封包的目標IP，在此因為顯示過濾器的緣故，所以必為117.18.232.133，可以利用命令提示字元輸入ping 網址(不用https://)來進行查詢。

5.Protocol:封包的協定類型，針對不同協定類型，可以顯示不同的顏色，也可以關閉這一功能View>>Colorize Packet List，PChome走的是http。

6.Length:封包的長度(單位為bytes)。

7.Info:封包內容的附加信息，http前面通常為GET或POST，兩者即為傳遞資料方式的差別，嚴格來說一般的表單可以用 GET 直接傳遞，而需要保密的資料必須用 POST 來處理，像是會員登入的帳號密碼。

三、封包內容說明



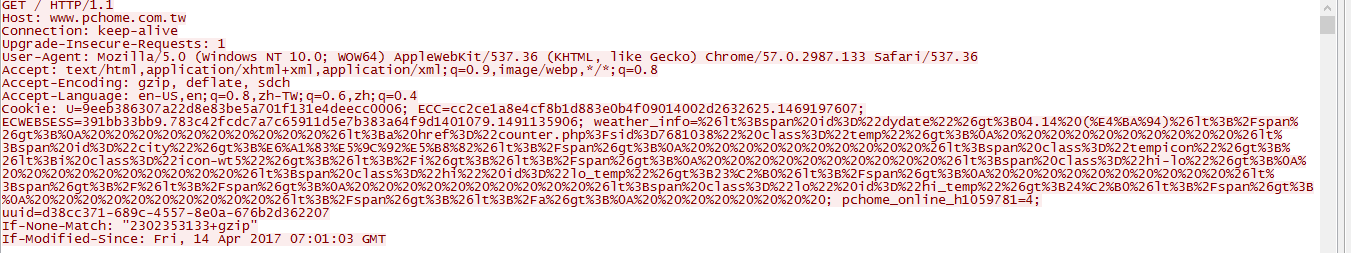
1.Frame116: 包括基本信息。

2. Ethernet II, Src:為連結層的資訊。

3. Internet Protocol Version 4, Src:為網路層的資訊，包括IP協定。

4.  Transmission Control Protocol, Src Port:為傳輸層的資訊，此封包使用了HTTP協定。

5. Hypertext Transfer Protocol:即封包中的數據內容。



↑Hypertext Transfer Protocol的內容為上圖所示

Host:表示端點主機(www.pchome.com.tw)

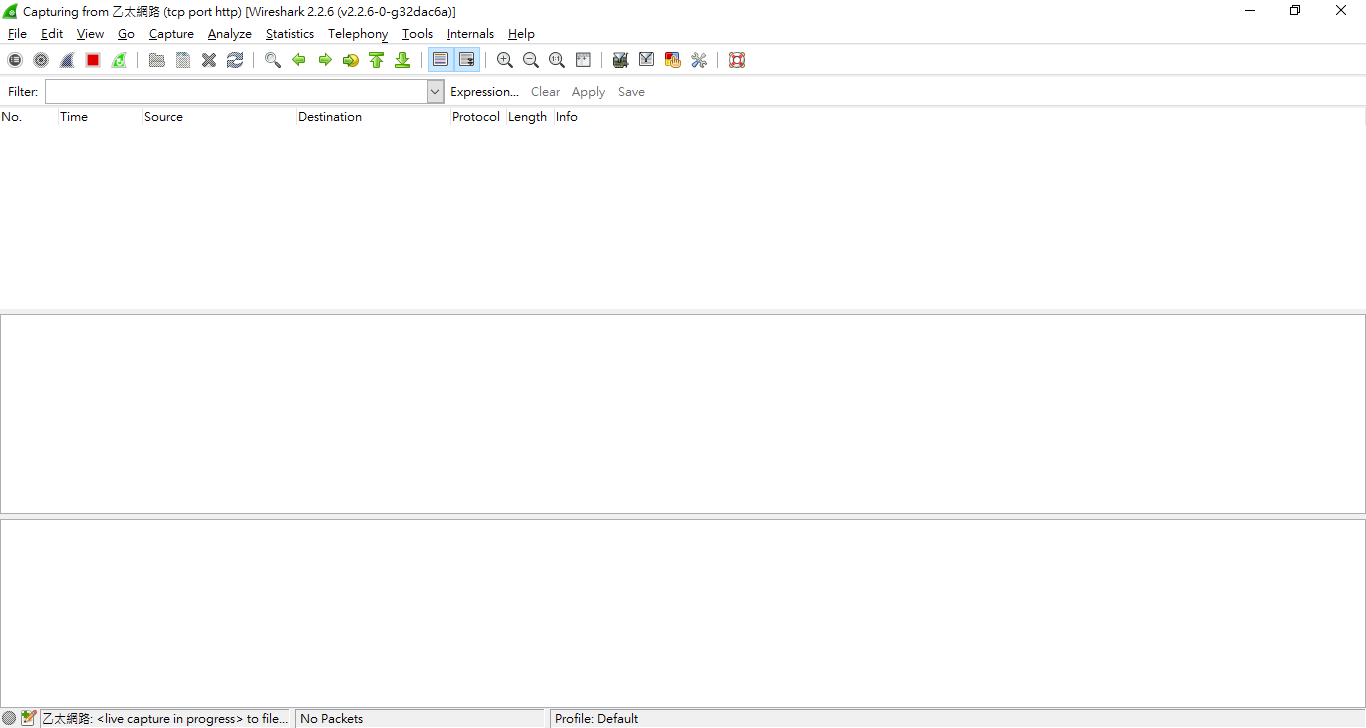
User-Agent:代表使用者使用的軟體

Accept-Encoding:可用的http解壓縮方案，像這裡可以接受gzip, deflate, sdch。

Accept-Language:可用的語言，像是這個網站就可以接受中文和英文。

參、應用二:長庚大學校務資訊系統

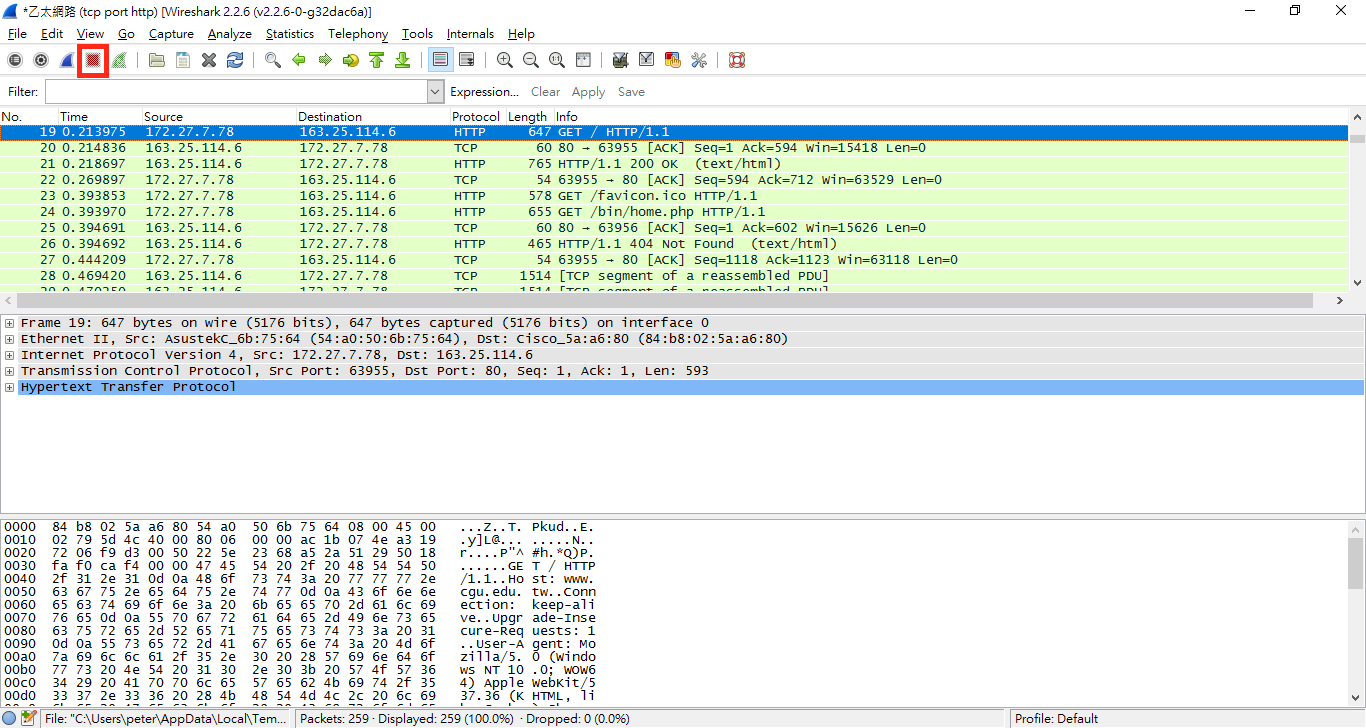
一、封包擷取



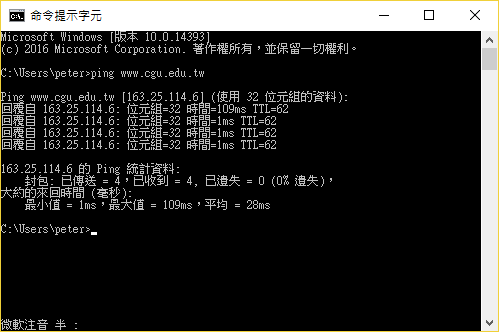
↑首先我們設定完擷取過濾器後。



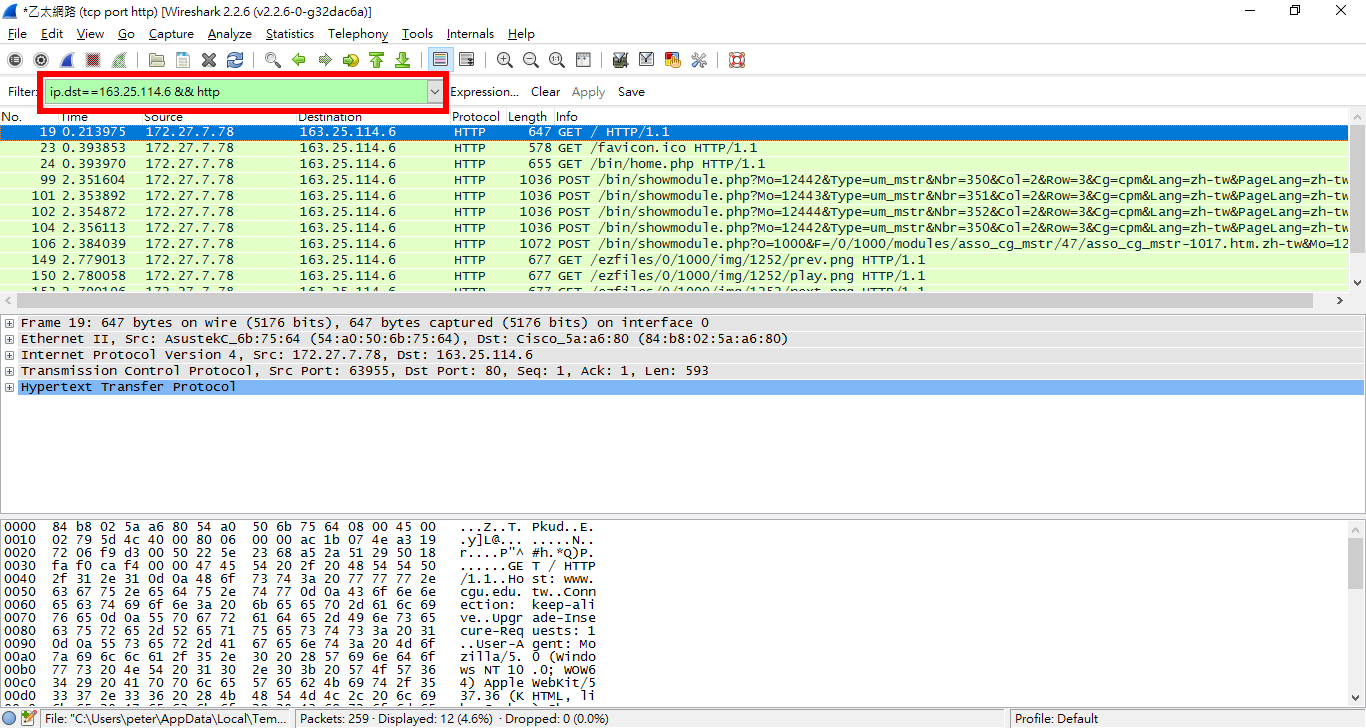
↑我們進入Google瀏覽器，進入長庚大學的首頁後。



↑接著我們回到Wireshark按下停止鈕。

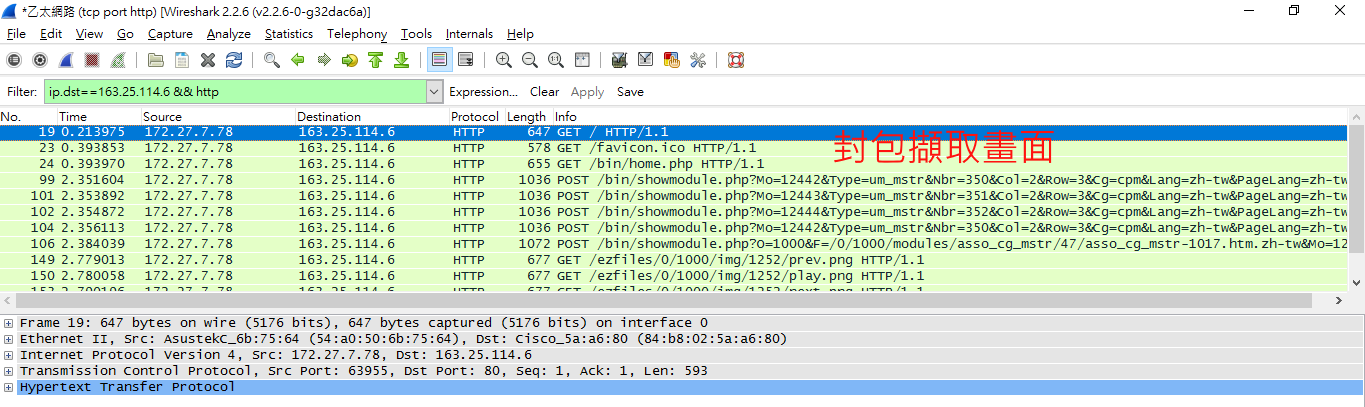


↑接著我們進入命令提示字元，輸入ping www.pchome.com.tw 的指令查長庚大學首頁的IP[163.25.114.6]。



↑接著我們利用顯示過濾器下ip.dst==163.25.114.6&&http的條件，ip.dst是確保我們抓到的是長庚大學的首頁，並且我們用http的條件來進行再次確認。

二、封包內容說明



1.No:封包的編號，長庚大學首頁編號為19，登入畫面為233。

2.Time:封包的時間戳，可以通過View>>Time Display Format設定所要用的時間格式。

3.Source:封包的來源IP，通常為本機自己的IP，可以利用命令提示字元輸入ipconfig來進行查詢。

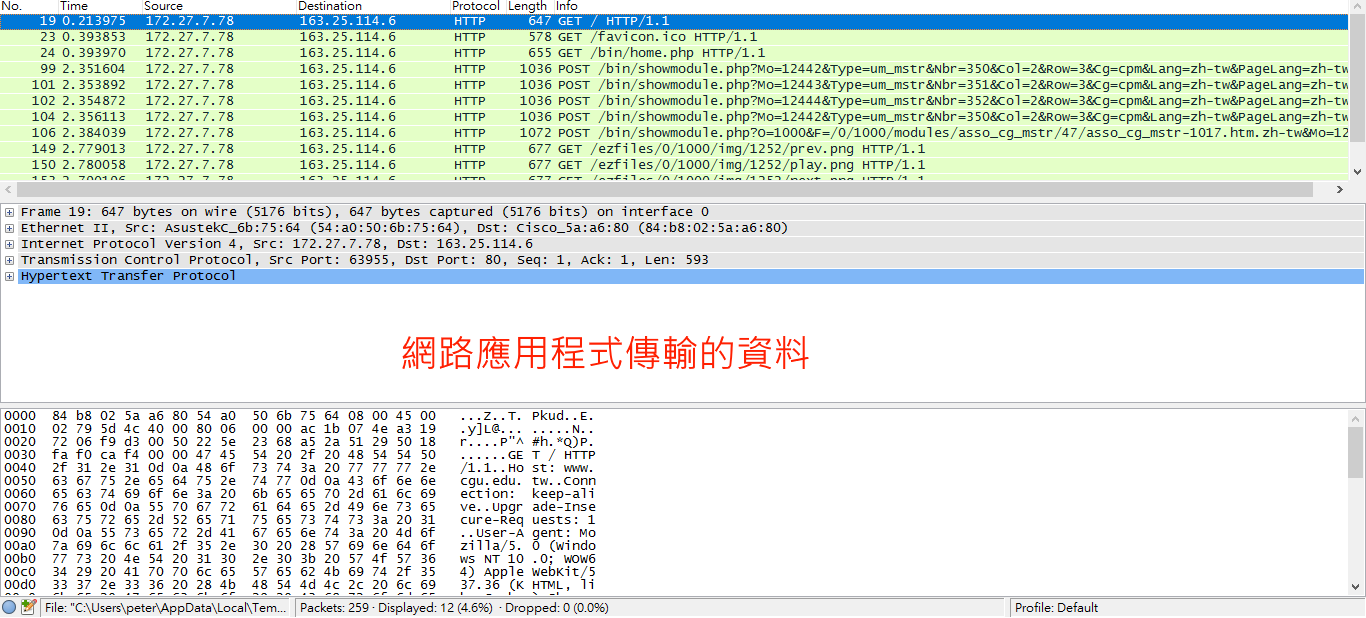
4.Destination:封包的目標IP，在此因為顯示過濾器的緣故，所以必為163.25.114.6，可以利用命令提示字元輸入ping 網址(不用https://)來進行查詢。

5.Protocol:封包的協定類型，針對不同協定類型，可以顯示不同的顏色，也可以關閉這一功能View>>Colorize Packet List，長庚大學走的是http。

6.Length:封包的長度(單位為bytes)。

7.Info:封包內容的附加信息，http前面通常為GET或POST，兩者即為傳遞資料方式的差別，嚴格來說一般的表單可以用 GET 直接傳遞，而需要保密的資料必須用 POST 來處理，像是會員登入的帳號密碼。

三、封包內容說明



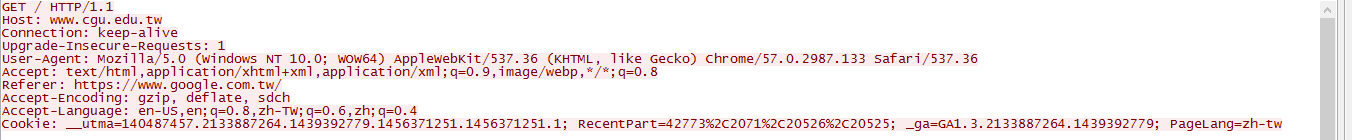
1.Frame19: 包括基本信息。

2. Ethernet II, Src:為連結層的資訊。

3. Internet Protocol Version 4, Src:為網路層的資訊，包括IP協定。

4.  Transmission Control Protocol, Src Port:為傳輸層的資訊，此封包使用了HTTP協定。

5. Hypertext Transfer Protocol:即封包中的數據內容。



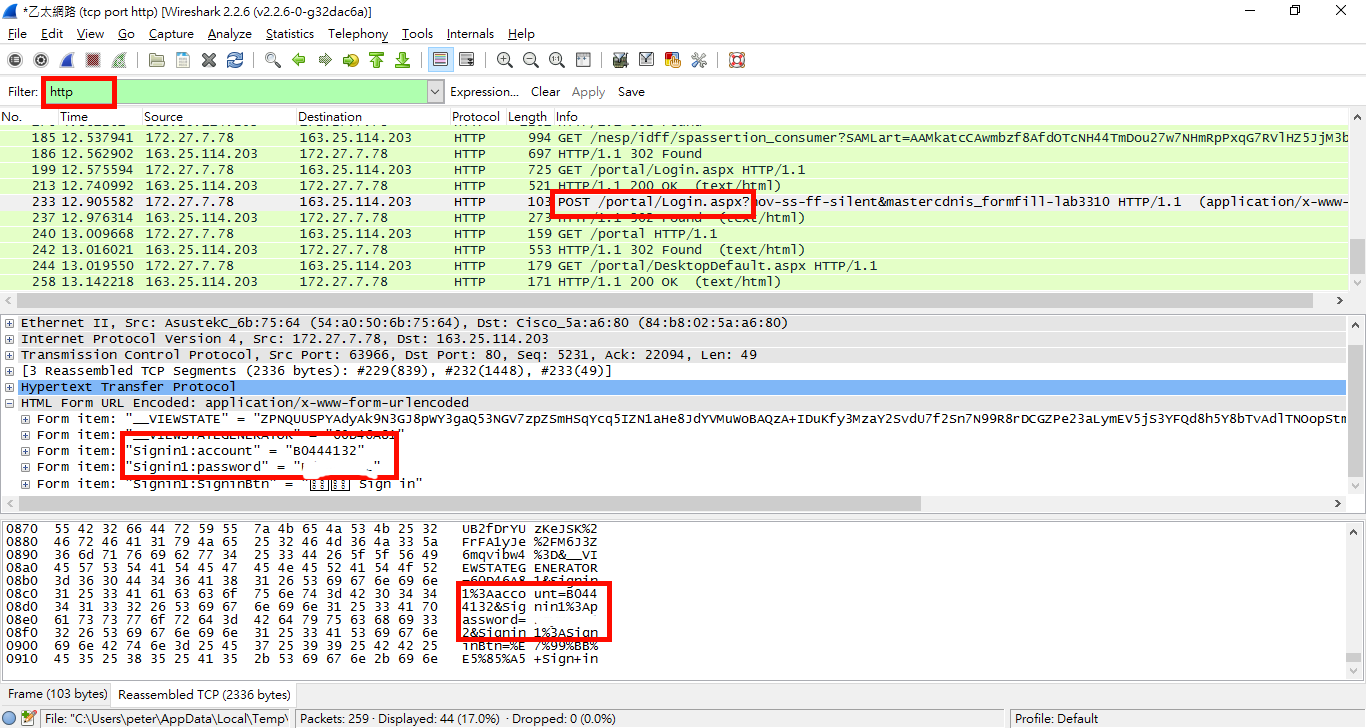
↑Hypertext Transfer Protocol的內容為上圖所示

Host:表示端點主機(www.cgu.edu.tw)

User-Agent:代表使用者使用的軟體

Accept-Encoding:可用的http解壓縮方案，像這裡可以接受gzip, deflate, sdch。

Accept-Language:可用的語言，像是這個網站就可以接受中文和英文。



↑接著我們為了找尋登入校務資訊系統後的封包，所以把顯示過濾器條件改為只有http，然後從封包擷取畫面中的Info中找Post開頭的(因為需要保密的資料通常都會用 POST 來處理)，然後找到後就會看能不僅只有看到IP位址，也能看到我們所登入的帳號密碼。

肆、心得

網際網路，已經與現我們的日常生活緊密結合，但真正了解其運作的人並不多。我們透過這次的作業實際操作，使得平日上課所學不再只是抽象的論述，而是直觀地去了解網路的運作、封包的傳遞和形式：透過sniffer軟體－－wireshark去抓取封包並分析。我們擷取了學校校務資訊系統的單一登入系統介面，在登入過程中擷取封包，並成功的取得我們登入時輸入的帳號以及密碼，這對第一次實際接觸封包內容的我們而言，是一種如拆開禮物的孩子ㄧ般的喜悅，在一堆英文數字中找到的那兩行字串(帳號密碼)，就像打開層層包裝，破解諸般謎題，最後獲取裡面的禮物，但這也證實了校務資訊系統使用的網路協定在傳送封包的同時，並未加密，具有一定的危險性。

現在我們透過封包能知曉的也大概只有明碼傳送的帳號密碼、網址、IP位址等等，希望以後能活用在更多層面。例如目前時下流行的網路遊戲，在維修快開機前，網路論壇上常有人把更新資料拆解出來，甚至包含一些官方系統設定，如果我們也能和他們一樣，將這門技巧應用到更高層次的地方上，想必能對整個網路環境有更進一步了解。