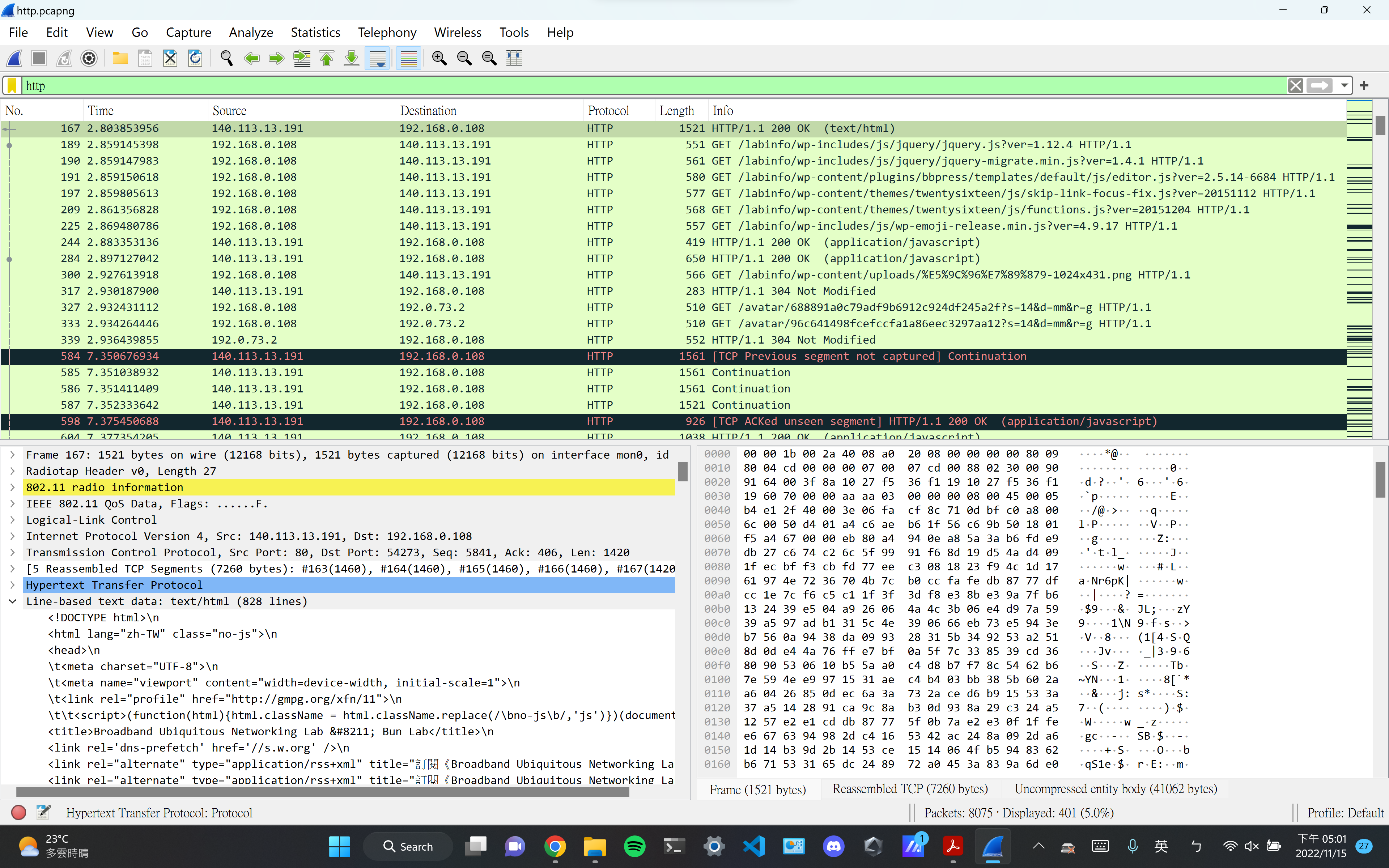
Lab1

311511034 黃聖偉

Q1 Open Access AP

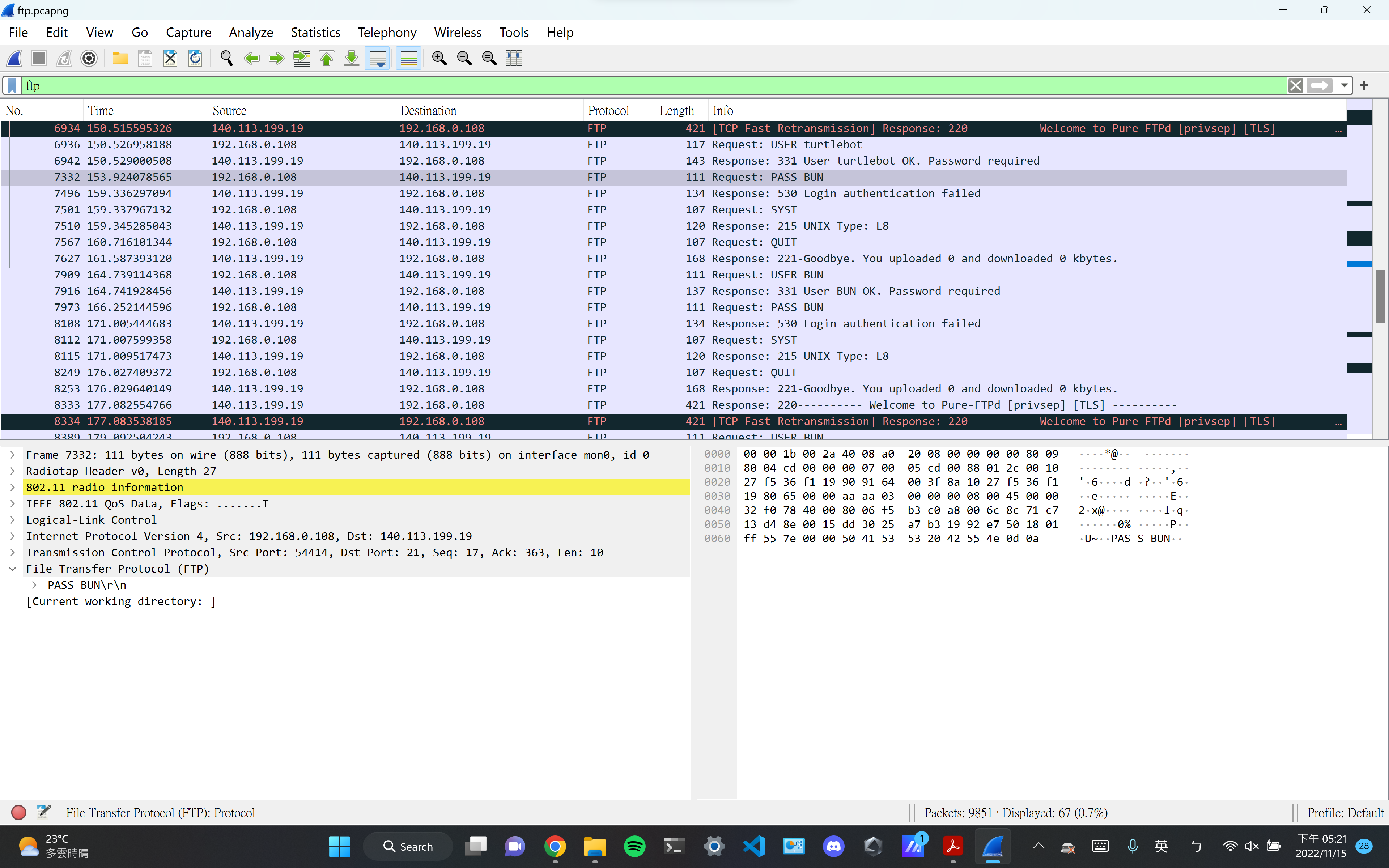
http



可以由http packet看到http是由TCP傳輸，而這個http session是與實驗室web server溝通，可以看到回傳200成功後所傳送的http payload是html檔案，也就是網頁的內容。而client傳往server的packet多是http get，也就是請求html檔案或是js檔案等資源的packet。

由於使用的協定是http而不是https，http payload沒有加密，而Open Access AP因此link layer也沒有加密，所以在收得到有效訊號空間中的所有裝置都能輕鬆地擷取並看到packet內容，資訊非常不安全。像是實驗室網站雖然有密碼保護，但是密碼是用http post傳送，再沒有https也沒有encrypted AP的情況下，如果有人輸入正確密碼，所有空間中的人都可以輕易獲取正確密碼。所以建議還是都使用https傳送資料比較安全。

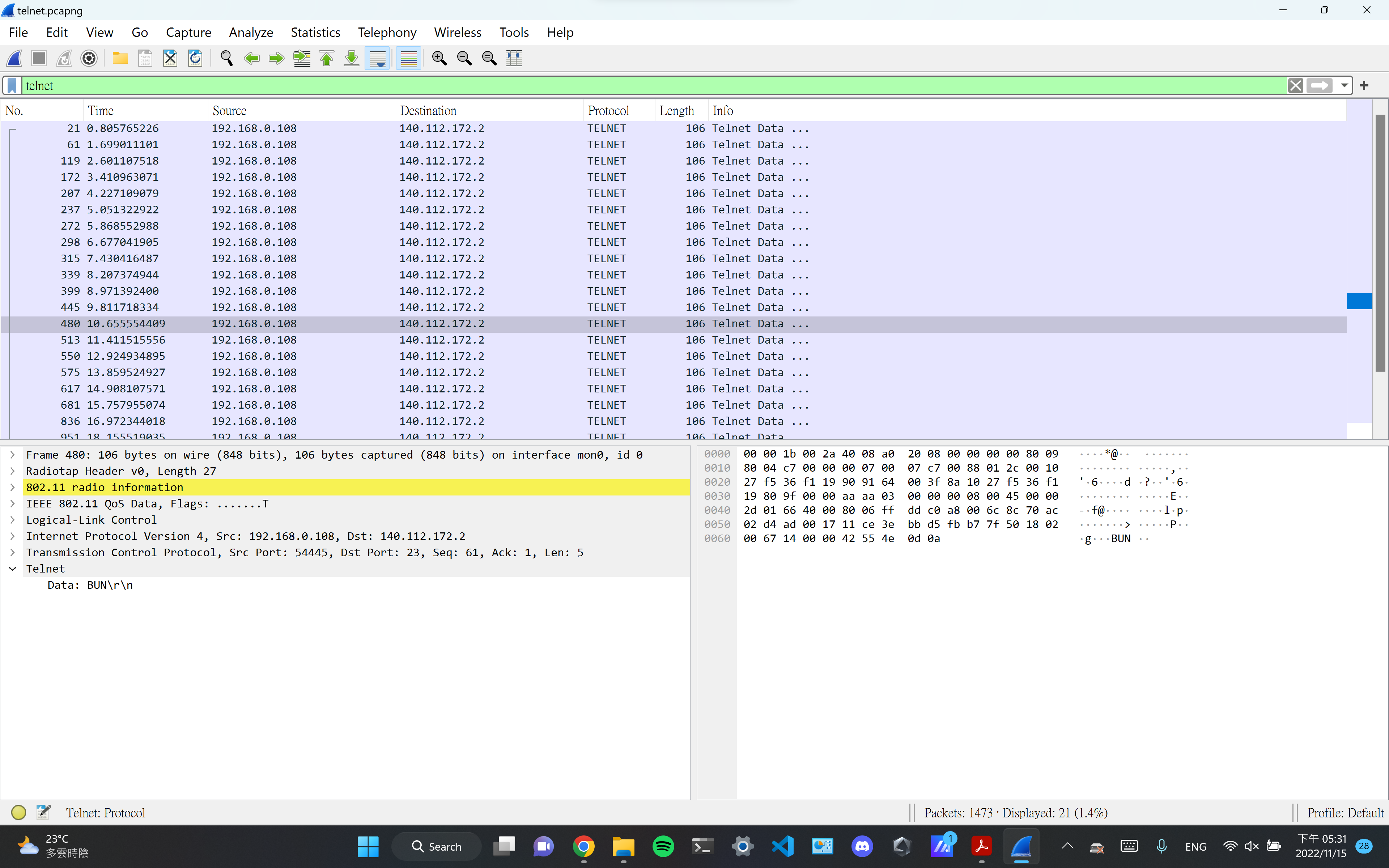
FTP



可以由擷取的封包看到ftp使用TCP傳輸，而這個ftp session主要在做使用者驗證相關的事，有USER來表明使用者身分、PASS來送出密碼做驗證、QUIT來關閉session。

由於ftp也是沒有加密的協定，在沒有encrypted AP的情況下，所有人都可以擷取並讀懂ftp packet，包含有密碼資訊的packet，像是我們就由收到的封包中可以得到模擬的帳號密碼資訊USER turtlebot, PASS BUN，雖然結果是authentication failed，但如果是真的帳號密碼，那所有空間中的人都可以輕易獲取，因此ftp也是非常不安全的協定。如果想安全傳輸檔案建議用ftps或sftp等有加密的協定。

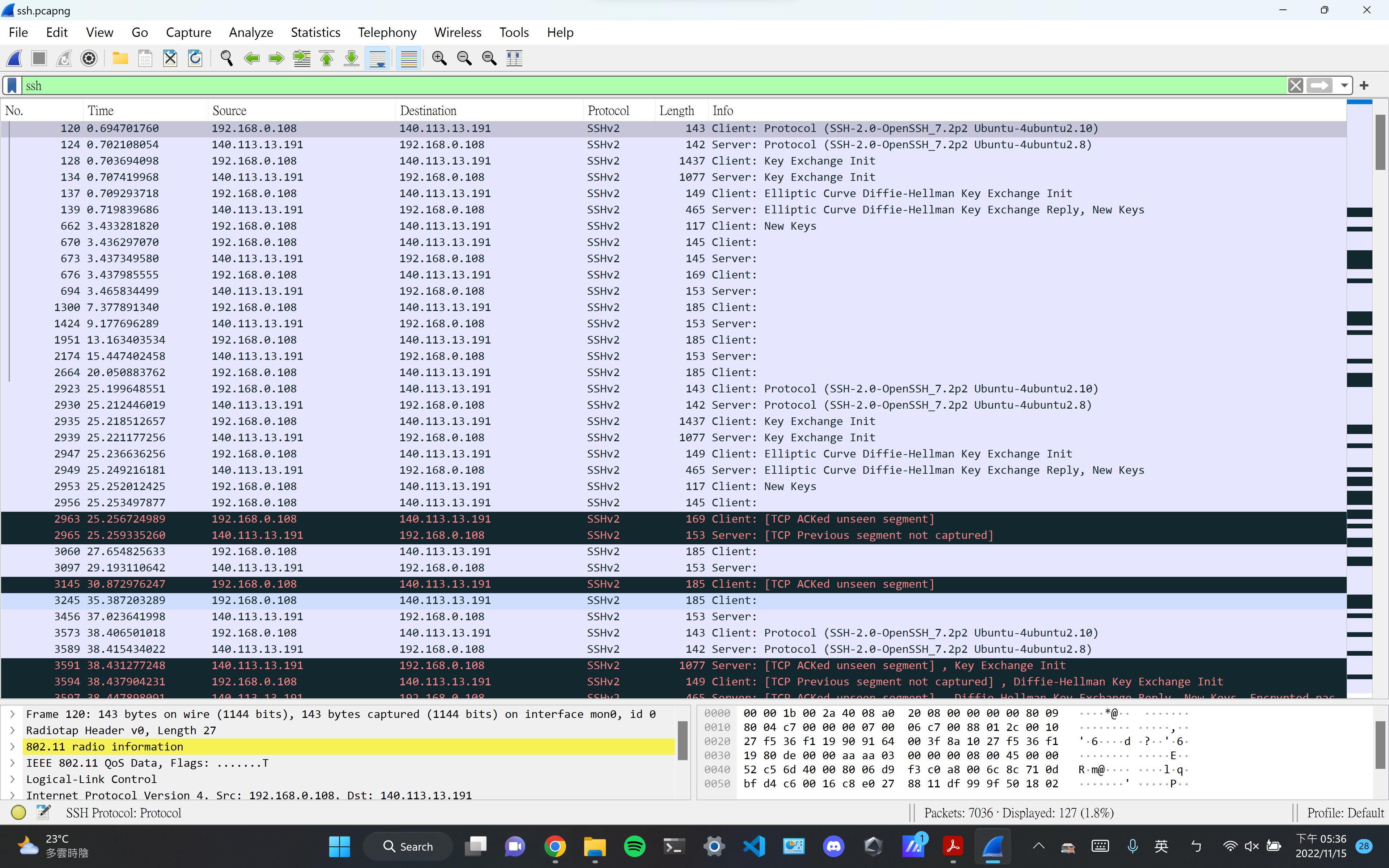
telnet



由擷取的telnet packet可以看到telnet使用tcp傳輸，而telnet做的事情基本上就是把client傳的訊息用tcp送給server與把server傳的訊息用tcp送給client，使用明文傳輸，因此在open access AP下每個人都可以看到與看懂訊息。

這個session中就是一直用telnet傳輸重複訊息BUN\r\n。

SSH



由擷取的SSH packet可以看到SSH使用tcp傳輸，SSH是這四個協定裡面最安全的，他的payload都有加密，我們基本上只看的到初始連線時做的key exchange與建立連線的步驟，其他中間內容都是加密的，因此就算使用open access AP傳送，收到的其他人也無法得知傳輸內容，只能看到加密後看不懂的payload。

Q2 Encrypt AP

一張含有 文字 的圖片

自動產生的描述 一張含有 文字 的圖片

自動產生的描述

一張含有 文字 的圖片

自動產生的描述 一張含有 文字 的圖片

自動產生的描述

可以看到當sender改成用encrypted AP發送訊號時，filter後的packet list都是空的。

一張含有 文字 的圖片

自動產生的描述

當我關掉filter後，我發現還是看得到SSID=bunexp傳出來的802.11 packet，但是由於更上層的協定(IP, TCP, HTTP, FTP…)都被當成802.11的payload加密了，沒有解密資訊的我們完全無法解析802.11 packet的payload，wireshark讀了以後只能把加密的上層協定當作data，沒辦法更進一步的解析，因此開啟filter時wireshark因為認不得加密後的http, FTP, telnet, SSH，因此filter後的packet list就會都是空的，因為wireshark從加密802.11 packet中無法找出我們filter的協定的packet。

從這次的實驗中，我得知了在wireless環境中link layer加密的重要性，因為在wireless環境不像在有線環境中，需要安裝複雜監聽裝置才能監聽一條線裡面的封包，在wireless環境只要有接收器，每個人都可以任意監聽空間中的packet，如果上層協定本身沒有加密，802.11也沒有加密的話，那所有收得到訊號的人都可以取得一密資訊。

另外，我也了解到了多層協定加密的重要性，像是在公開網路時，就算沒有802.11的加密，其他人要得到ssh或https等應用曾協定的被加密的payload還是很困難。有些重要機密資料甚至還會在https上再加密一層，像是在瀏覽器中傳送信用卡資料給銀行時，常常就將信用卡資訊再用RSA加密一次、然後https再加密一次、然後如果不在公開網路的話802.11再加密一次。就算一層加密被破解了，還有其他層保護。

高中時我曾經嘗試暴力破解我家wifi跟學校wifi的WPA2加密，方法跟這次實驗一樣先設定筆電wifi網卡為monitor模式，然後丟一些invalid的wifi packet使某個網路中的裝置斷線，去監聽斷線裝置重新連線時建立連線的packet，擷取到重新連線的加密packet後，就可以使用這些packet離線暴力破解。我家的密碼用常用字典10分鐘就被破解了，學校密碼用學校名稱、日期加上常用字典後也一個小時左右就破解出來。因此我認為只在802.11層加密有助於保護資料，但是是不夠的，在application layer也加密才能使資料傳輸足夠安全。