電腦網路實驗實驗報告 < Packet Analysis >

姓名：翁佳煌　　學號：409430030

1. 實驗名稱

網路封包擷取操作與分析

2. 實驗目的

這次實驗的三個 LAB 主要是透過使用 Wireshark 工具，學習如何在網路上進行封包擷取，並了解封包的基本格式、學習如何對擷取到的封包進行分析，包括協議、源地址、目的地址、端口號等相關資訊。透過本次實驗的操作，讓我更深入的了網路通訊的運作原理，並未來可自我學習如何用網路封包分析在網路安全、網路優化等方面的應用進行討論，以加深對網路封包分析的理解與應用。

3. 實驗設備

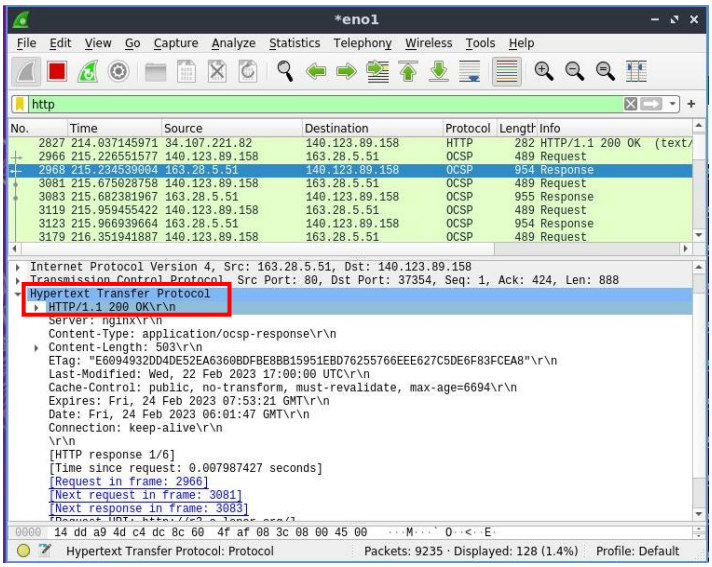
Linux 作業系統之電腦。
Wireshark。

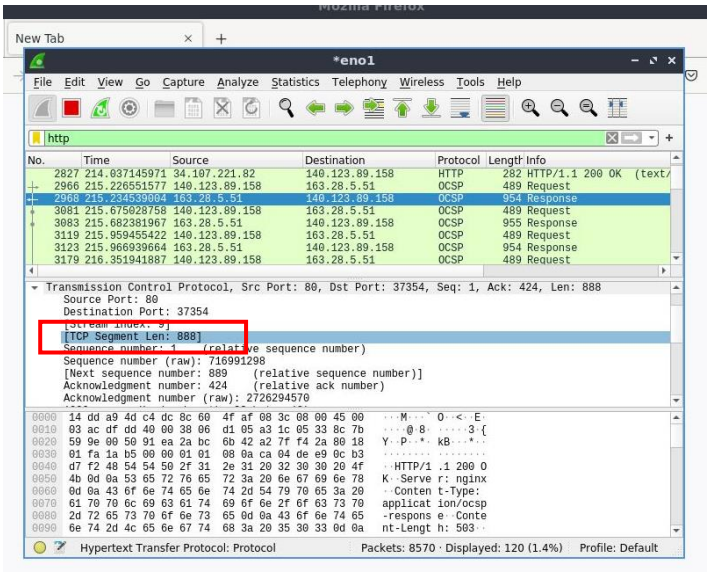
4. 實驗步驟

LAB1-使用 Wireshark 分析 packet 的內容:

1. 開啟 Wireshark。
2. 開啟國光客運的網站。

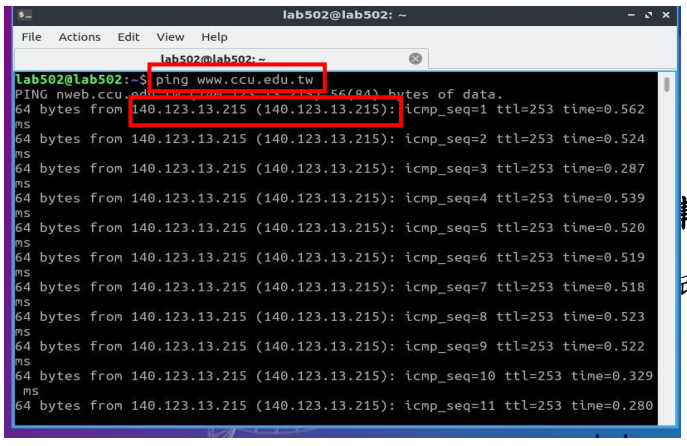
3. 擷取完畢後，經由 Filter 顯示 http 的封包，隱藏其他的封包。
4. 找出應用層和傳輸層的資訊。應用層為 HTTP， 傳輸層為 TCP，port number 為 80。我將會在問題與討論會探討這部分。

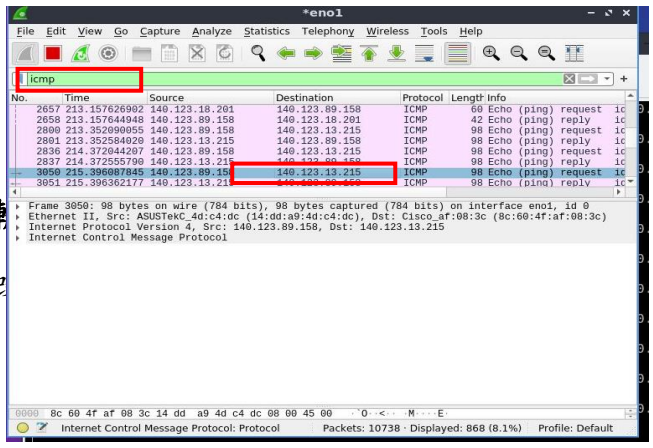




LAB2- 使用 Wireshark 觀察 ping 學校的首頁:

1. 開啟新的 terminal。
2. 在 terminal 中輸入 ping www.ccu.edu.tw，可發現學校的 ip 位址為 140.123.13.215。
3. 返回 Wireshark，在 filter 中過濾出 ICMP 的封包。我將會在問題與討論更深入解釋 ICMP 的功能。





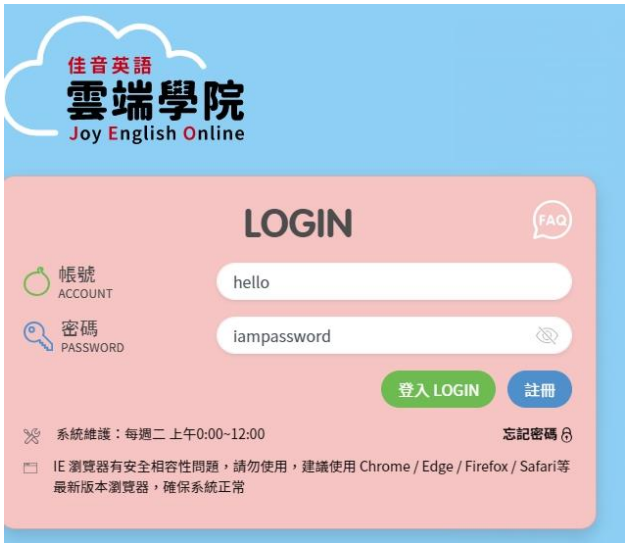
LAB3- 使用 Wireshark 取得佳音英語的內容

1. 開啟 terminal，使用 nslookup 找出佳音英語網站的 ip 地址。

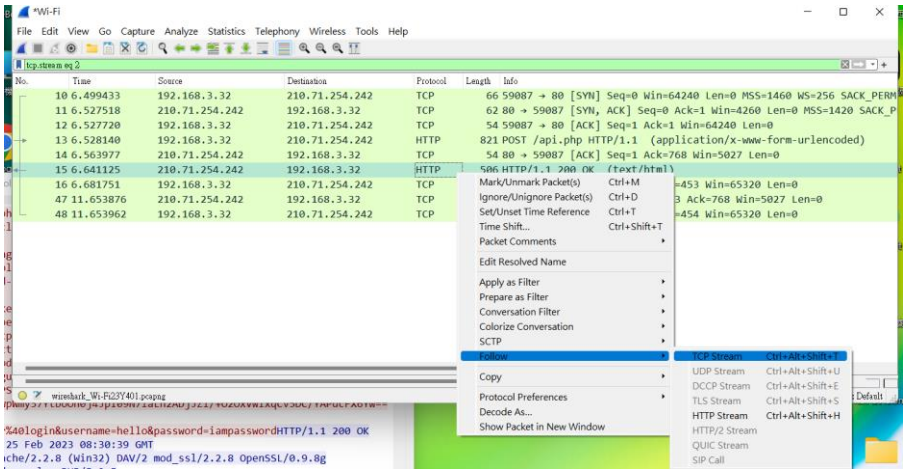
```
C:\WINDOWS\system32>nslookup testcloud.joy.com.tw
DNS request timed out.
    timeout was 2 seconds.
伺服器:  UnKnown
Address:  192.168.3.62

未經授權的回答:
名稱:    testcloud.joy.com.tw
Address:  210.71.254.242
```

2. 開啟 wireshark。

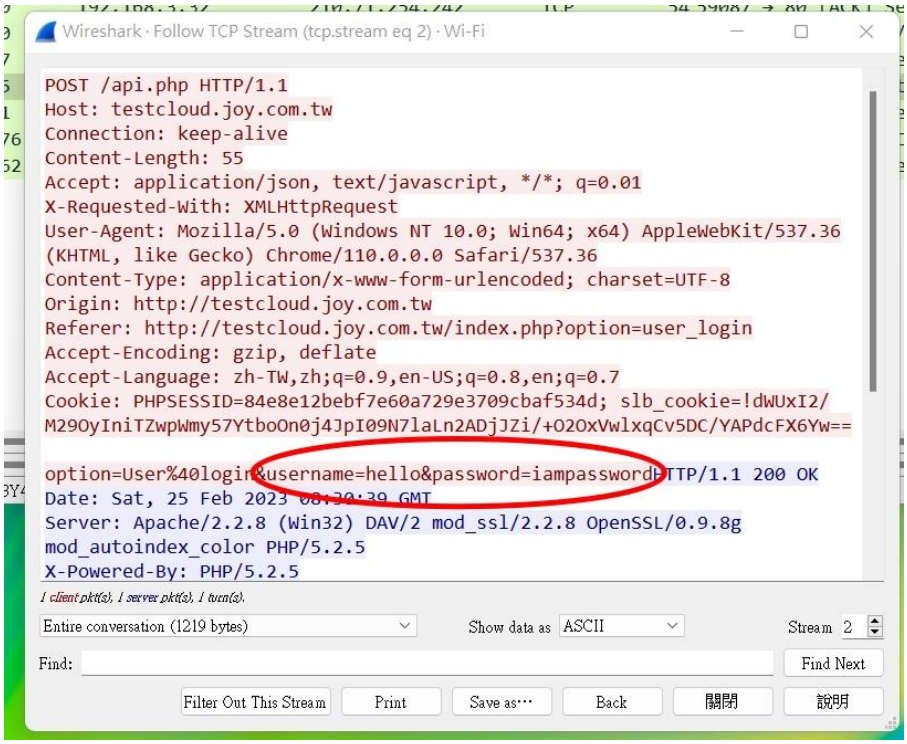
3. 到佳音英語網站輸入帳號以及密碼。



4. 對圖中的封包按右鍵點選 Follow->TCP Stream。



4. 觀察下圖，紅色的部分為我們送出的 DATA，紅色圈圈的部分就是步驟 3 輸入的帳號密碼，藍色的部分是我們收到的 DATA。另外，我將會在問題討論中補充防止帳密外洩的方法。



5. 問題與討論

1. HTTP 是一種用於網絡瀏覽器和網站服務器之間傳輸超文本的協定，而 Port 80 是 HTTP 數據傳輸的默認端口號。200 OK 是一種 HTTP 協議的狀態碼，表示伺服器已經成功處理了客戶端的請求並返回了所需的資源。

2. ICMP 是 Internet Control Message Protocol 的縮寫，是網際網路協定（IP）的一部分。它主要用於在 IP 網絡中進行錯誤報告、診斷和控制訊息的傳輸。ICMP 通常被用於協助網路診斷和故障排除，包括 Ping 和 Traceroute 等工具。Ping 工具使用 ICMP Echo 請求和 Echo 回應消息來檢查網路連通性。ICMP 訊息是在 IP 數據包的數據字段中傳輸的，並且通常不加密。因此，攻擊者可以通過修改或仿冒 ICMP 消息來攻擊網路，包括進行拒絕服務（DoS）攻擊和欺騙式攻擊等。為了維護網絡的安全性，需要使用適當的安全措施來防止 ICMP 攻擊。

3. 防止帳密外洩補充

   防止帳密外洩是一個重要的議題，以下是一些常見的方法：

   1. 使用強密碼：使用複雜且長度足夠的密碼，並且不要重複使用同一個密碼。

2. 使用雙重認證：使用雙重認證可以增加帳戶的安全性，例如使用簡訊驗證碼或者 Google Authenticator 等。

3. 盡量避免使用公共 Wi-Fi：公共 Wi-Fi 網路容易被監聽和攔截，因此盡量避免使用公共 Wi-Fi 連接。

4. 使用加密連接：使用 HTTPS 協定的網站可以加密資料傳輸，減少被攔截的風險。

5. 不要點擊未知來源的連結：避免點擊不明來源的連結，以防止惡意軟體或釣魚攻擊。

6. 定期更換密碼：定期更換密碼可以減少密碼泄漏的風險，如同學校的 ecourse2 作法。

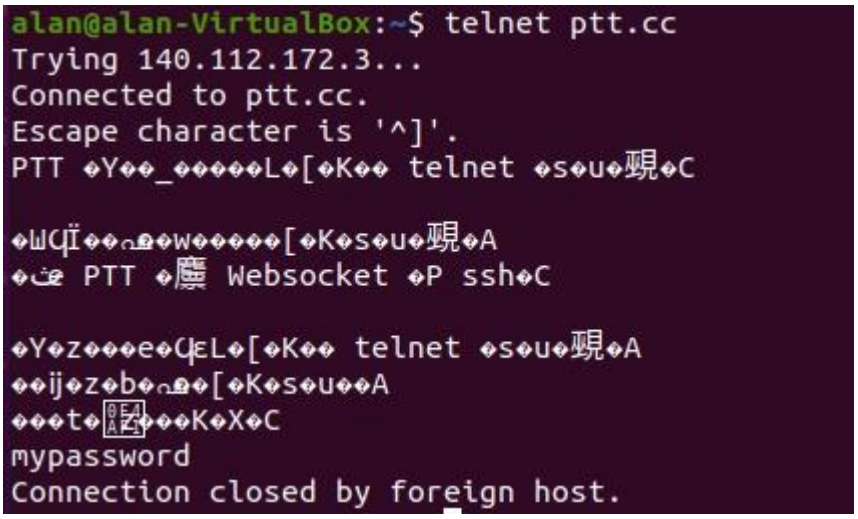
7. 使用安全的雲端儲存：如果使用雲端儲存服務，則應該選擇有良好安全紀錄的供應商。

8. 更新軟體和防毒軟體：定期更新電腦和手機的軟體和防毒軟體可以減少被惡意軟體入侵的風險。

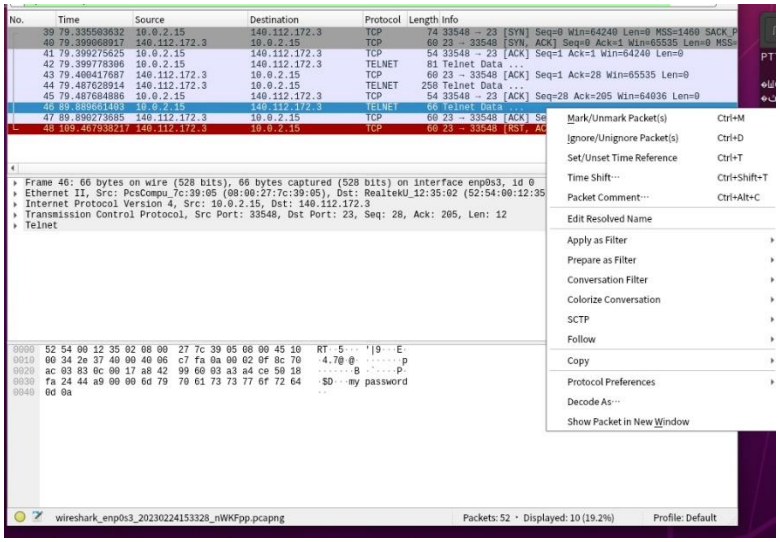
總之，要保持帳戶的安全，需要注意許多方面，包括密碼強度、連接方式、避免點擊不明來源的連結，以及定期更換密碼等。

4.雖然 ptt 關閉 telnet 連線了，但 LAB3 我依舊嘗試著輸入 telnet ptt.cc 去做觀察，發現以下:

1. 開啟新的 terminal。
2. 在 terminal 中輸入 telnet term.ptt.cc 會導致連線失敗，是因為 PTT 已經正式關閉了 TELNET 的連線功能。原因是因為 TELNET 是一種不安全的協定，資料傳輸時容易被竊聽和攔截，且無法進行加密保護，容易被駭客利用進行攻擊或竊取用戶的帳號和密碼等敏感資訊。**(參考文獻 3)**
3. 於是我改成輸入 telnet ptt.cc，雖然成功了，但會跑出我無法解釋的亂碼，但我依舊強硬輸入了”mypassword”去做觀察。



4.開啟 Wireshark，找到相對應的封包，案右鍵找到 Follow TCP Stream 並點選，可發現下方右圖所顯示，紅色的部分為我們送出的 DATA，也就是步驟 3 輸入的 mypassword，藍色的部分是我們收到的 DATA。



6. 心得與感想

這次 LAB 是整堂課的第一個實驗，在實作之前，助教很清楚明瞭地介紹了 Wireshark 的功能以及其用處，讓我們能夠很輕易的理解並且馬上動手操作去理解他，經由這 3 個 LAB，讓我對 Wireshark 這套工具有初步的認識以及理解，比較可惜的是，LAB3 由於 PTT 已經關閉 telnet 的連線功能，導致這個實驗必須更換成觀察其他使用 http 的網站，但這也同時讓我學到是因為 TELNET 是一種不安全的協定，資料傳輸時容易被竊聽和攔截，且無法進行加密保護，容易被駭客利用進行攻擊或竊取用戶的帳號和密碼等敏感資訊。也因此，PTT 為了加強資訊安全，決定停止 TELNET 的服務，改為僅提供加密保護的 SSH 協定來進行遠端連線。

整體來說，這次實驗受益匪淺，讓人期待下次 LAB 主題。

7. 參考文獻

1. LAB1:國光客運: http://www.kingbus.com.tw/
2. LAB2:學校網站: https://www.ccu.edu.tw/
3. LAB3 ： PTT 宣布關閉 Telnet 連線 ：
   https://term.ptt.cc/
   https://agirls.aotter.net/post/60636
   https://www.ptt.cc/bbs/Announce/M.1577824347.A.DEE.html?fbclid=IwAR1odeIJR42HzWKgRE9b_rPTWaxXqmFpI6XDCYVbtrxebfdwtvFxfQjsuxk
   http://testcloud.joy.com.tw/
4. https://zh.wikipedia.org/zh-tw/Telnet
5. https://zh.wikipedia.org/zh-tw/Wireshark
6. https://ithelp.ithome.com.tw/articles/10193287