

# Wireshark 基礎實驗(一)

姓名：陳美瑜

## 1. 實驗名稱

Wireshark 基礎實驗(一)

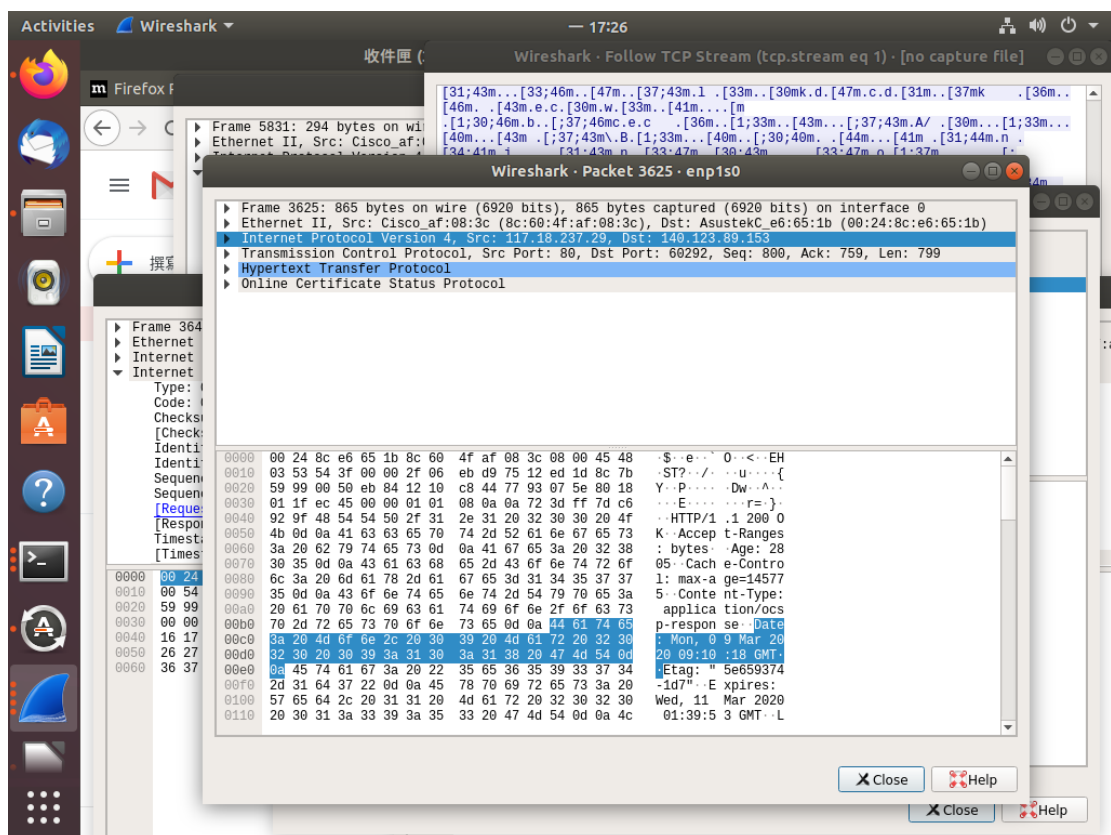
## 2. 實驗目的

這次的實驗，主要是要了解 Wireshark 的基本操作，以及如何使用 Wireshark 擷取封包，並查看封包裡面的內容，了解封包裏頭的資訊。

## 3. 實驗設備

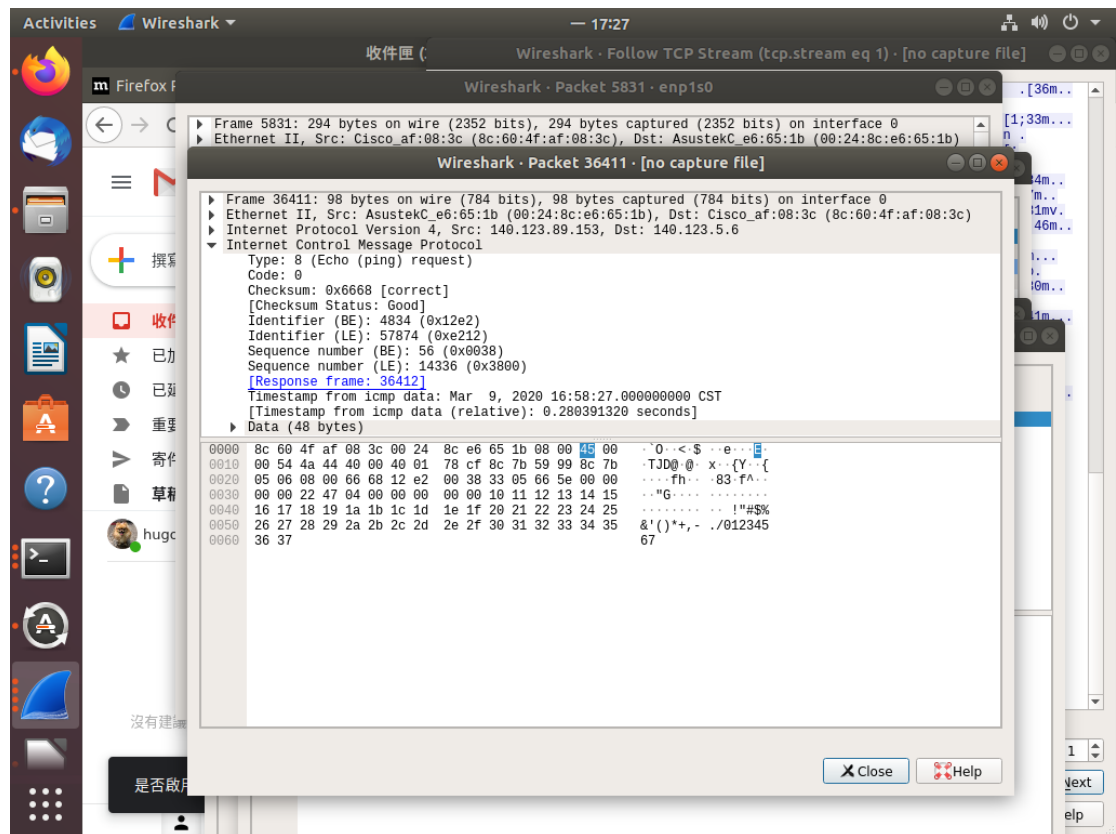
電腦、Wireshark。

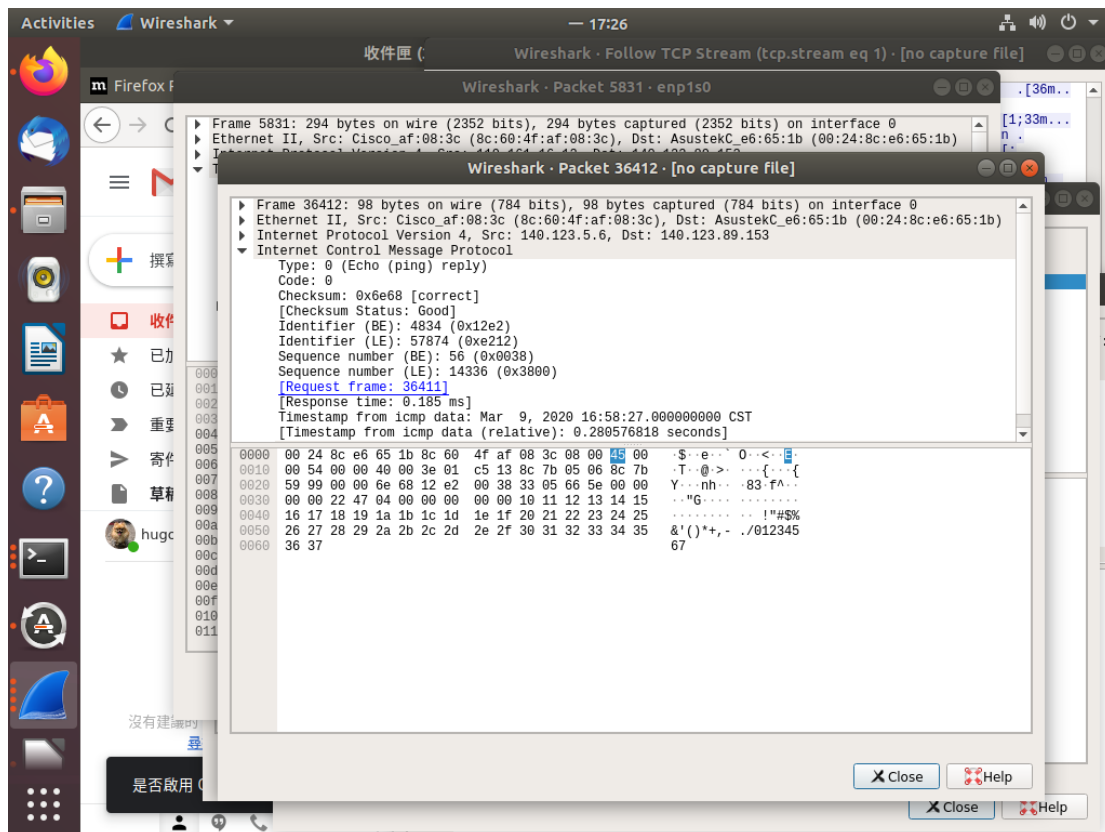
## 4. 實驗步驟



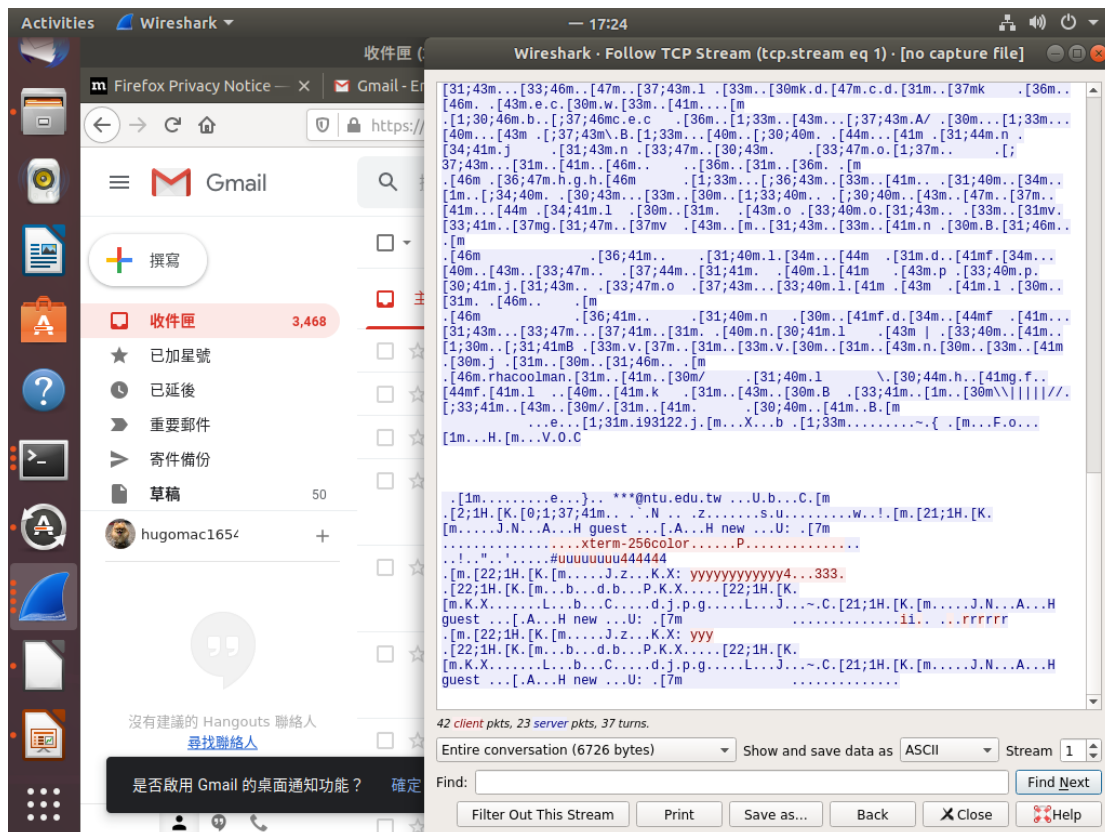
在 LAB1 當中，我們首先開啟 Wireshark 擷取封包，然後開啟 Yahoo 新聞的

由圖中的第二行可知第二層協定為 Ethernet，第三行可知第三層為 IPV4，第四行可知第四層為 TCP，第五行可知第五層為 HTTP。





在 LAB2 當中，我們首先開啟 Wireshark 擷取封包，然後開啟 Terminal ping [www.ccu.edu.tw](http://www.ccu.edu.tw)，回到 Wireshark 裡面過濾出 ICMP 的封包，可以看到如上面二圖，Request 的 Source 端為我們這台電腦，Destination 端為學校網站，Reply 的 Source 端為學校網站，Destination 端為我們的電腦。



在 LAB3 當中，我們首先開啟 Wireshark 擷取封包，然後開啟 Terminal 進入 PTT 網站並輸入帳號密碼，回到 Wireshark 裡面找到 Length 較大的封包，按下右鍵及 follow 後，可以得知上圖結果，紅色的 uuuuuuu444 為我們輸入的帳號，yyyyyyyyyyyy433 為我們輸入的密碼。