Wireshark 基礎實驗(二)

姓名：陳美瑜

1. 實驗名稱

Wireshark 基礎實驗(二)

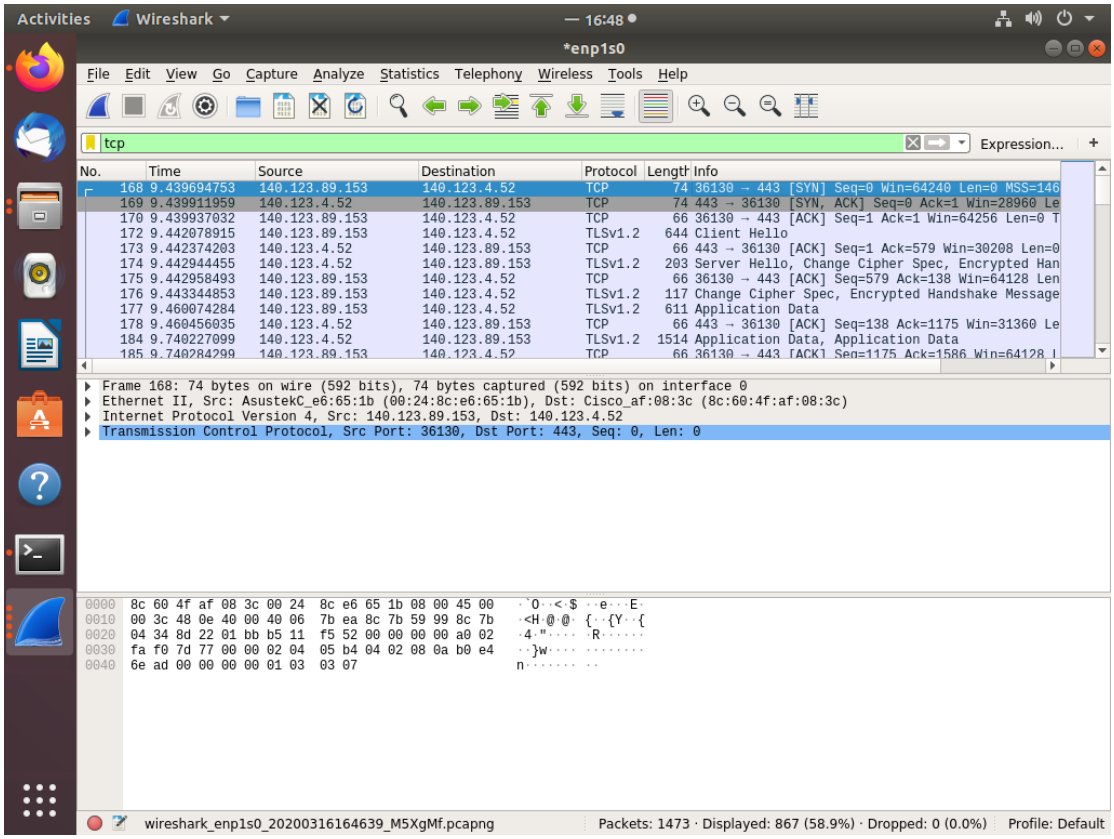
2. 實驗目的

這次的實驗，主要是要了解三向交握、HTTP 以及如何使用 nslookup。

3. 實驗設備

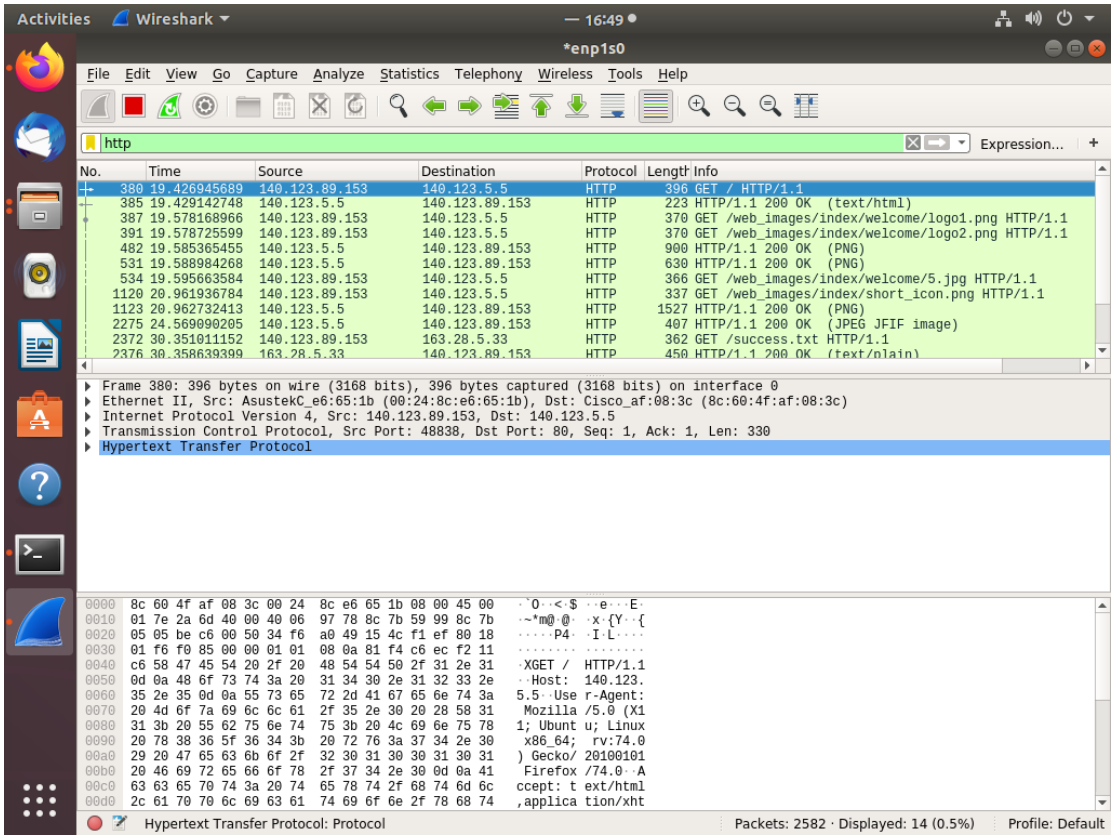
電腦、Wireshark。

4. 實驗步驟

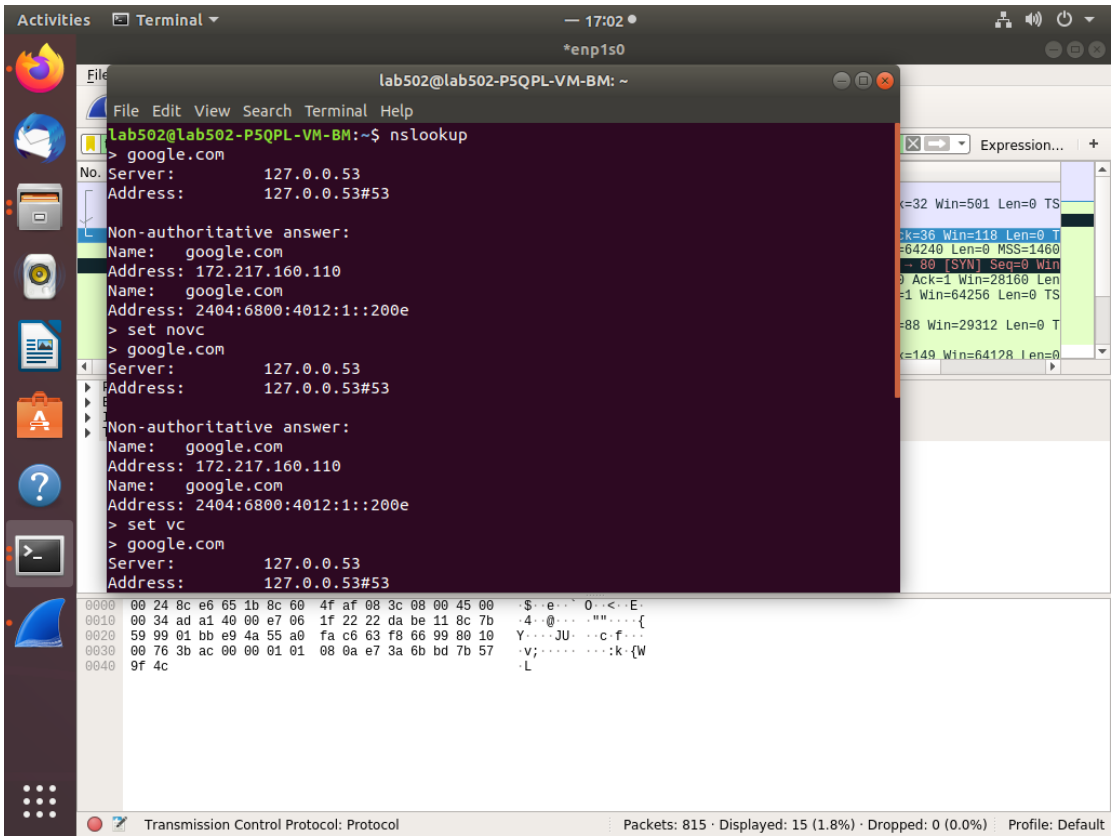


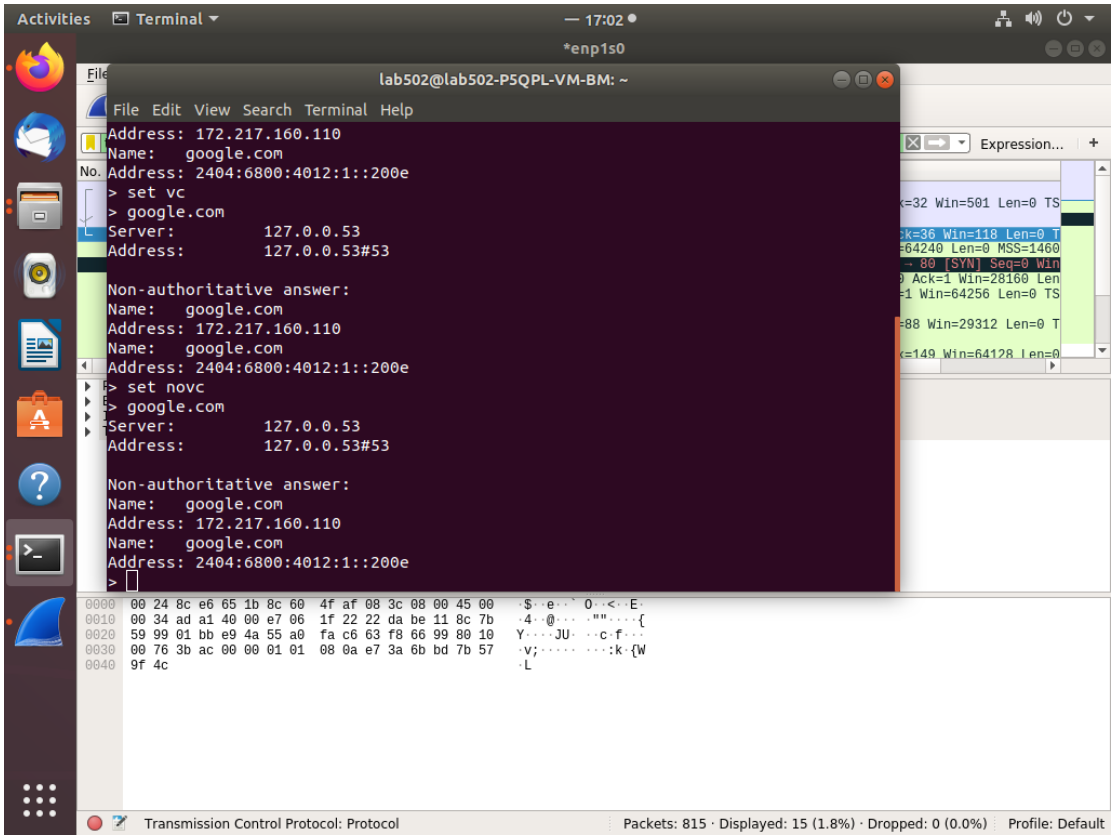
在 LAB1 當中，我們首先開啟 Wireshark 擷取封包，然後開啟學校網站，回到 Wireshark 後，過濾出 TCP，於是可以發現前三項有著 SYN 及 ACK 即是三

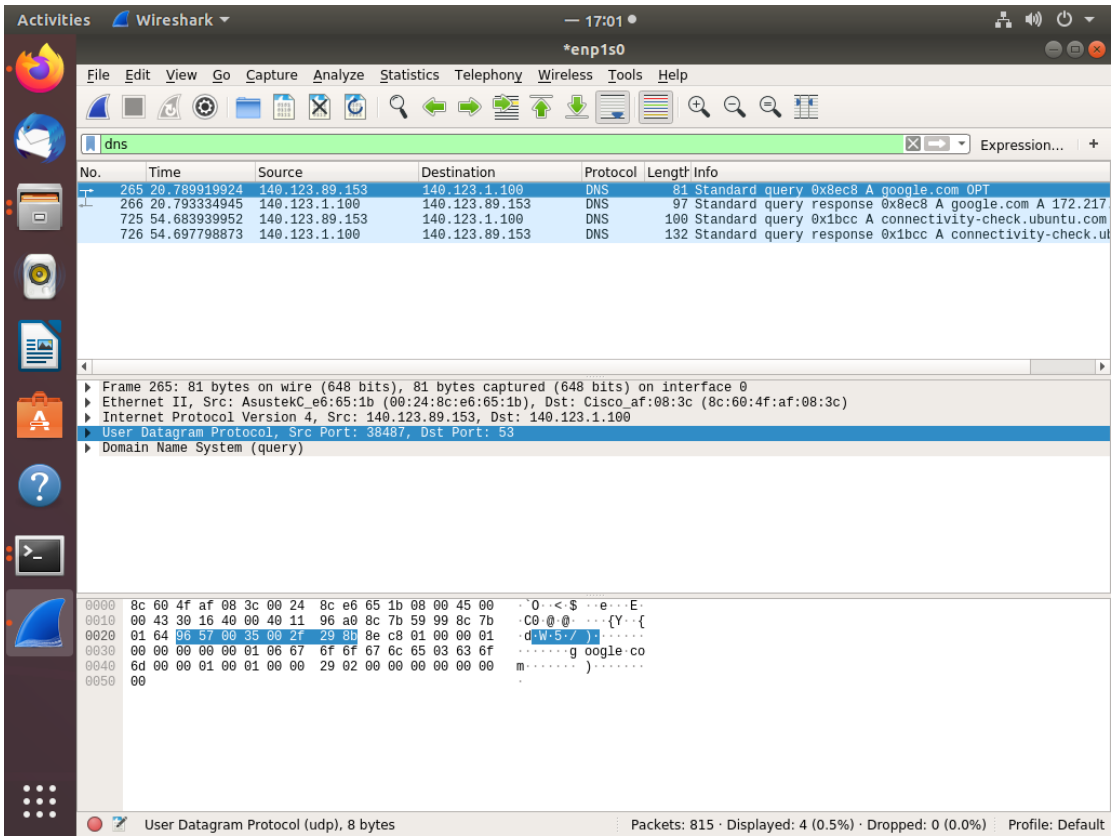
向交握的封包。



在 LAB2 當中，我們首先開啟 Wireshark 擷取封包，然後開啟學校網站，回到 Wireshark 後，過濾出 HTTP 封包，我們可以發現第一項 GET 開頭的封包為 Request，第二項有著 OK 的是 Response。


Activities
Terminal
17:02
*enp1s0
lab502@lab502-P5QPL-VM-BM: ~
File Edit View Search Terminal Help
lab502@lab502-P5QPL-VM-BM:~$ nslookup
> google.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
Name: google.com
Address: 172.217.160.110
Name: google.com
Address: 2404:6800:4012:1::200e
> set novc
> google.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
Name: google.com
Address: 172.217.160.110
Name: google.com
Address: 2404:6800:4012:1::200e
> set vc
> google.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Expression...
Transmission Control Protocol: Protocol
Packets: 815 · Displayed: 15 (1.8%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Terminal
17:02
*enp1s0
lab502@lab502-P5QPL-VM-BM: ~
File Edit View Search Terminal Help
Address: 172.217.160.110
Name: google.com
Address: 2404:6800:4012:1::200e
> set vc
> google.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
Name: google.com
Address: 172.217.160.110
Name: google.com
Address: 2404:6800:4012:1::200e
> set novc
> google.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
Name: google.com
Address: 172.217.160.110
Name: google.com
Address: 2404:6800:4012:1::200e
>
Expression...
Transmission Control Protocol: Protocol
Packets: 815 · Displayed: 15 (1.8%) · Dropped: 0 (0.0%)
Profile: Default



在 LAB3 當中，我們首先開啟 Wireshark 擷取封包，然後開啟 Terminal，輸入 nslookup，並輸入網址、set vc、set novc 等指令後，回到 Wireshark，過濾出 DNS 的封包，我們可以發現協定為 UDP 的封包，之所以沒有 TCP 是因為作業系統的關係。

5. 問題與討論

LAB1:

三向交握的第一個動作是封包發起，當用戶端想要對伺服器端連線時，就必須要送出一個要求連線的封包，此時用戶端必須隨機取用一個大於 1024 以上的埠口來做為程式溝通的介面。然後在 TCP 的表頭當中，必須要帶有 SYN 的主動連線，並且記下發送出連線封包給伺服器端的序號。

第二個動作是封包接收與確認封包傳送，當伺服器接到這個封包，並且確定要接收這個封包後，就會開始製作一個同時帶有 SYN=1, ACK=1 的封包，我們伺服器也必須要確認用戶端確實可以接收我們的封包才行，所以也會發送出一個 Sequence 給用戶端，並且開始等待用戶端給我們伺服器端的回應。

第三個動作是回送確認封包，當用戶端收到來自伺服器端的 ACK 數字後，就能夠確認之前那個要求封包被正確的收受了， 接下來如果用戶端也同意與伺服器端建立連線時，就會再次的發送一個確認封包（ACK=1）給伺

服器。
TCP 與 UDP 的差別在於 TCP 是雙向傳輸，UDP 是單向。TCP 傳送東西會有封包數據且可靠性高，UDP 可靠性低且傳送東西速度快。

LAB2:
Host 為伺服器的域名(用於虛擬主機)，以及伺服器所監聽的傳輸控制協定埠號。
Accept 為能夠接受的回應內容類型（Content-Types)。
Cookie 為由伺服器通過 Set- Cookie 傳送的一個超文字傳輸協定 Cookie。

LAB3:
因為 DNS 查詢的資料包較小、機制簡單，UDP 協定的額外開銷小、有著更好的性能表現。