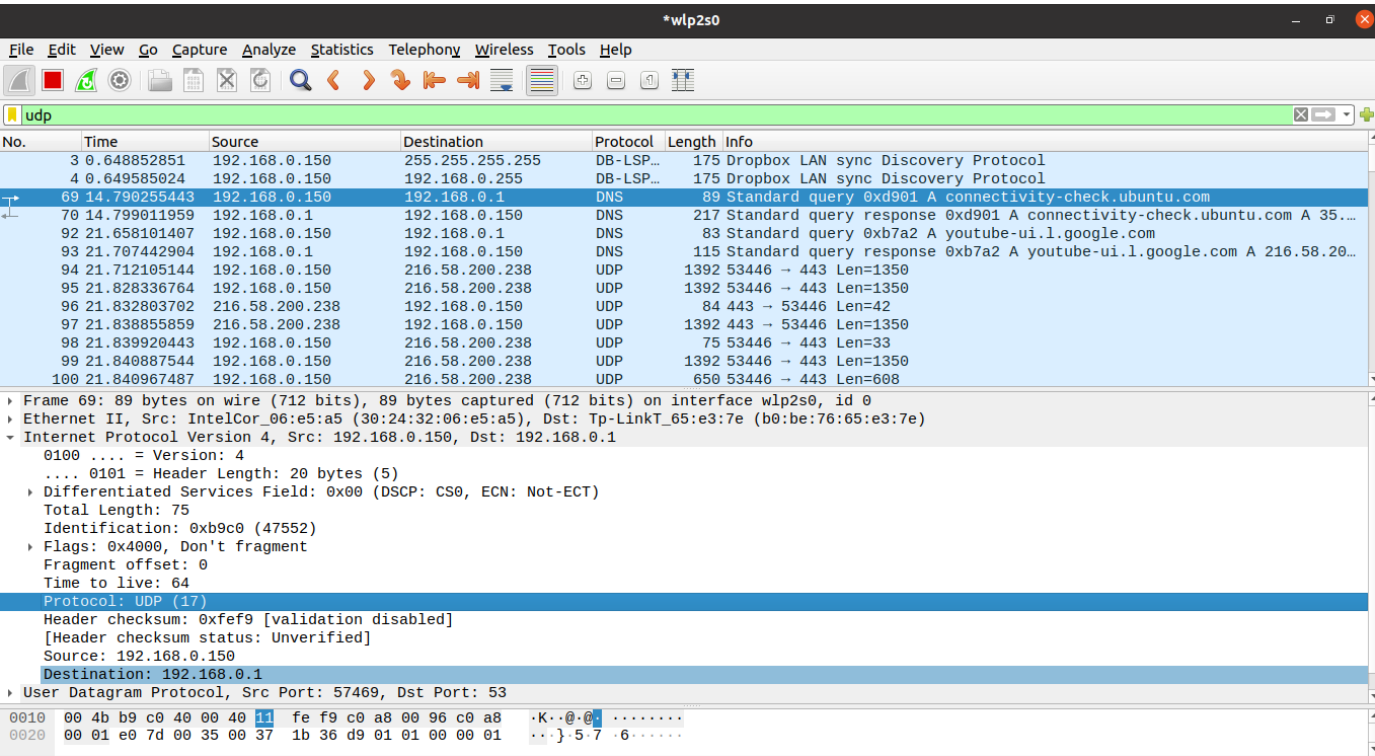


# Computer Networks HW1

b07902048 資工三 李宥靈

## 1



我找到使用UDP的service為本機發送DNS query時所使用的封包，發送的對象為外部的DNS server，但因為我的wireshark是在NAT下使用DHCP且沒有特別指定DNS，所以上面寫的destination為AP的IP，AP會幫我處理轉送。

## 2

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main window is divided into three panes:

- Packet list:** Displays a list of captured packets. The selected packet is No. 2210, Time 159.285216236, Source 140.112.28.111, Destination 192.168.62.129, Protocol TCP, Length 4398. The info column shows [PSH, ACK] Seq=1188718225 Ack=3 W....
- Packet details:** Shows the structure of the selected packet. It is a Transmission Control Protocol (TCP) packet, Src Port: 2769, Dst Port: 58770, Seq: 1188718225, Ack: 3, Len: 4344. The flags are 0x018 (PSH, ACK). The window size value is 64240. The checksum is 0xb91b [unverified].
- Packet bytes:** Shows the raw data of the packet in hexadecimal and ASCII.

At the bottom, a status bar indicates: Transmission Control Protocol (tcp), 20 bytes. Packets: 354280 · Displayed: 354224 (100.0%) · Dropped: 0 (0.0%) · Profile: Default.

server使用的port為2769

### 3

	TCP	UDP
連線特性	可靠(三向握手機制)	不可靠
速度	慢(有確認封包的機制)	快
掉包是否會重傳	是	否
適合用途	網頁資訊	影音串流

### 4

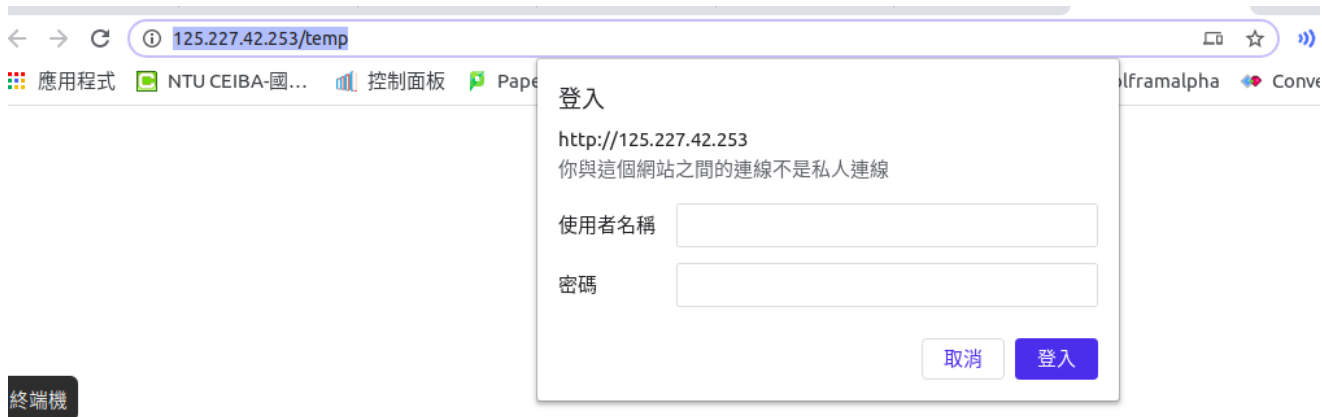
網頁名稱：台北市農會 員工專區的登入

網址：<http://125.227.42.253/temp> (<http://125.227.42.253/temp>)

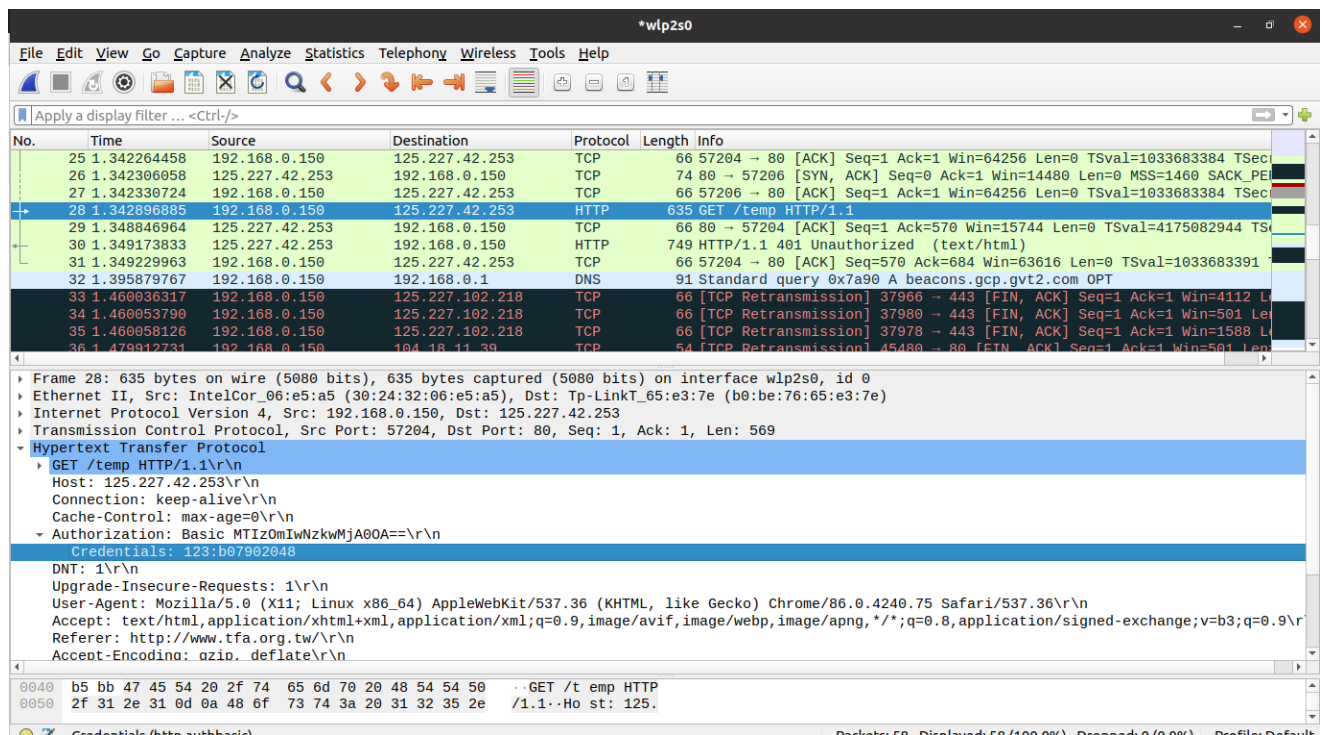
輸入資訊：

- 使用者名稱:123

- 密碼:b07902048



- 獲取封包結果：



- Why is it not safe to send passwords in plaintext ?  
使用明碼來傳輸資料，可能會使封包在網路中被攔截，進而被有心人士查看利用

## Additional

在查詢有關DNS封包的transmission protocol時，發現DNS伺服器其實兩種protocol都會使用，在recursive DNS與client端互傳域名解析的封包時使用的是UDP，而recursive DNS跟root DNS之間傳送request則是使用TCP。