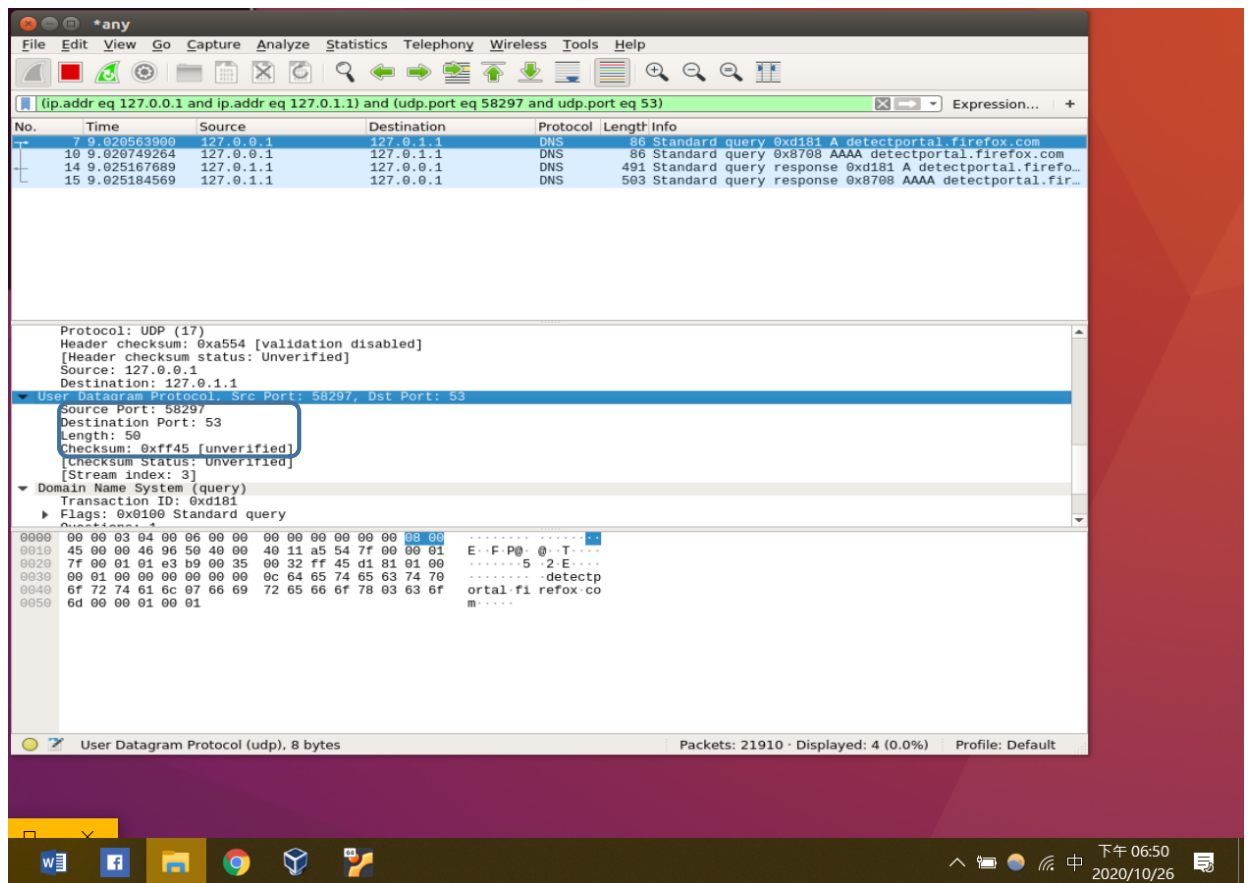


## 計算機網路作業

### Problem 1

#### analysis of UDP packets



我用 firefox 打開 youtube 播音樂，wireshark 抓到了這個 DNS，這個 DNS 功用是向 detectportal.firefox.com 提出要求

(detectportal.firefox.com is used to detect captive portals on public wifi networks to be able to redirect you to their logon screen  
節錄自 <https://support.mozilla.org/en-US/questions/1251590>)

為何 DNS 是 UDP package

1. DNS 在將網址轉成 ip 時使用的是 UDP 協議，因為 UDP 協議無須建立連結，能提供更快的書據訪問
2. 上面截圖看到的 protocol 是在 wireshark 下開 UDP filter 得到的結果，故此為 UDP package
3. 這個 package 包含 UDP header 下僅有的 4 個 field 分別為 source port , destination port , length , checksum  
=>總和以上 3 觀點此為一 UDP package

## Problem2

### Analysis of TCP packets

The image shows a Wireshark packet capture analysis of a TCP segment. The packet list on the left shows a packet of length 56 bytes, destination port 2769, and sequence number 81120637. The packet details pane on the right shows the following structure:

- Frame 22532: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 140.112.28.111
  - 0100 ... = Version: 4
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 48
  - Identification: 0x9753 (38739)
  - Flags: 0x0000, Don't fragment
  - Time to live: 64
  - Protocol: TCP (6)
  - Header checksum: 0xee8e [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 10.0.2.15
  - Destination: 140.112.28.111
- Transmission Control Protocol, Src Port: 57270, Dst Port: 2769, Seq: 3, Ack: 81120637, Len: 0
  - Source Port: 57270
  - Dst Port: 2769
  - [Stream index: 0]
  - [TCP Segment Len: 0]
  - Sequence number: 3 (relative sequence number)
  - [Next sequence number: 3 (relative sequence number)]
  - Acknowledgment number: 81120637 (relative ack number)
  - 0101 ... = Header Length: 20 bytes (5)
  - Flags: 0x010 (ACK)
  - Window size value: 65535
  - [Calculated window size: 65535]
  - [Window size scaling factor: -2 (no window scaling used)]
  - Checksum: 0xb508 [unverified]
  - [Checksum Status: Unverified]
  - Urgent pointer: 0
  - [SEQ/ACK analysis]
  - [Timestamps]

TCP server 使用的 port 為 2769 ，ip 為 140.112.28.111

## Problem3

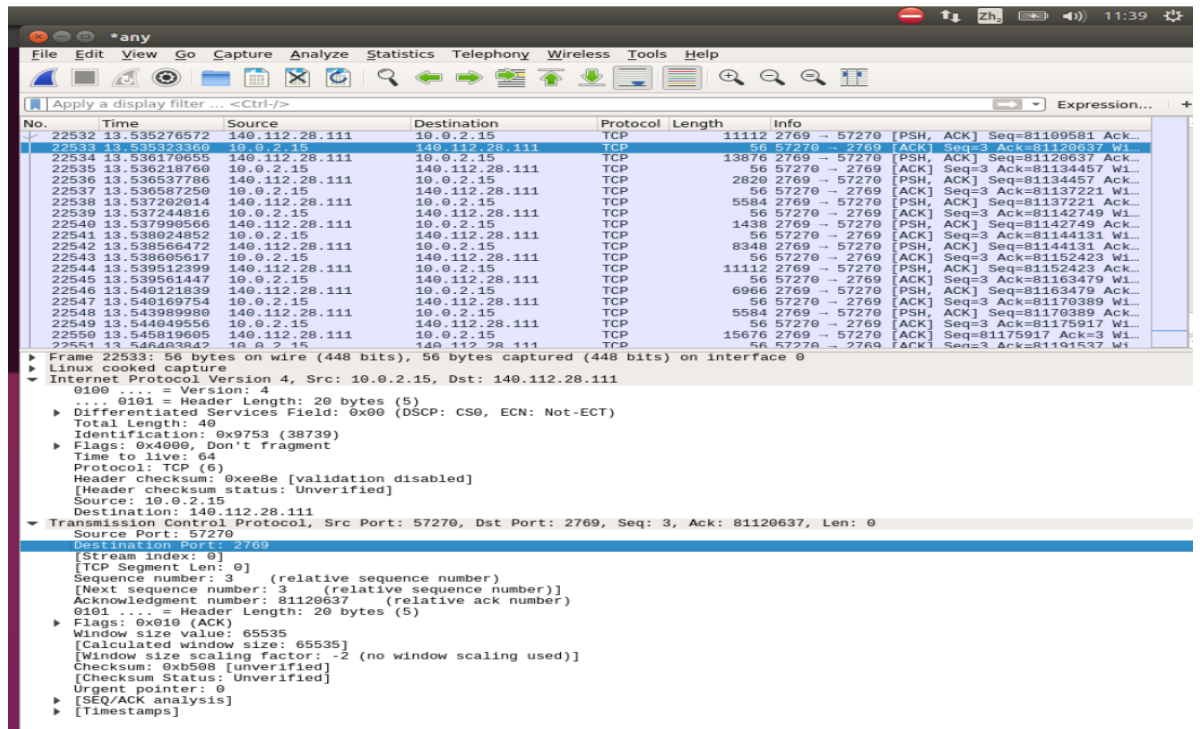
### Compare the headers of transport layer between TCP and UDP

<UDP>

The image shows a Wireshark packet capture analysis of a UDP segment. The packet list on the left shows a packet of length 86 bytes, destination port 53, and sequence number 16152. The packet details pane on the right shows the following structure:

- Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
- Linux cooked capture
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
  - 0100 ... = Version: 4
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 70
  - Identification: 0x3f18 (16152)
  - Flags: 0x4000, Don't fragment
  - Time to live: 64
  - Protocol: UDP (17)
  - Header checksum: 0xfc8c [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 127.0.0.1
  - Destination: 127.0.0.1
- User Datagram Protocol, Src Port: 56114, Dst Port: 53
  - Source Port: 56114
  - Destination Port: 53
  - Length: 56
  - Checksum: 0xff45 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 0]
  - Domain Name System (query)

<TCP>



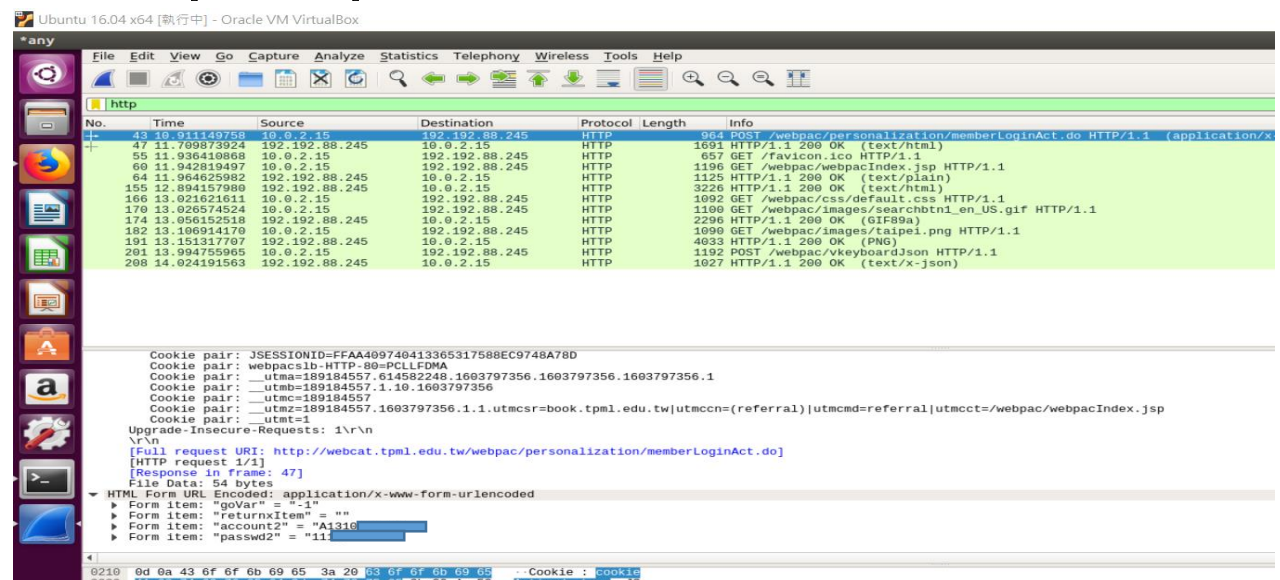
TCP UDP header 共同有 Source port 、Destination port 、Checksum

UDP 比 TCP 多了個 message length

TCP 比 UDP 多了 Sequence number 、acknowledge number 、Control flag 、  
Window size value 、Urgent pointer

## Problem 4

Find out a plaintext password



這是台北市立圖書館登入產生的 package

<https://book.tpml.edu.tw/webpac/webpacIndex.jsp>

Q: 為什麼以 plaintext 方式傳送密碼安全

A: 首先密碼不管是用 plaintext 或 hash 過，對有心人士來說都不算太難，其次我們能這麼簡單看到 plaintext 的密碼是因為 packet 是通過我們的 virtual machine 傳出去的，對其他人來說難度是存在的，故保護密碼最好的方式是透過 http 來保護，hash 過或 plaintext 不是這麼重要。