# Wireshark

NDHU ISC

https://www.wireshark.org/download.html

# Introduction

01

# Wireshark 用途

協助分析網路封包

藉此找出當中異常的行為、流量

呈現真實的網路情況

不會對任何封包做出警告、阻擋

# Wireshark 功能

觀察各個封包的詳細訊息

使用統計功能分析大量封包

紀錄網路數據資訊

# Practice

02

## 1.開啟 cmd 輸入 ipconfig 查詢自身 IP Address

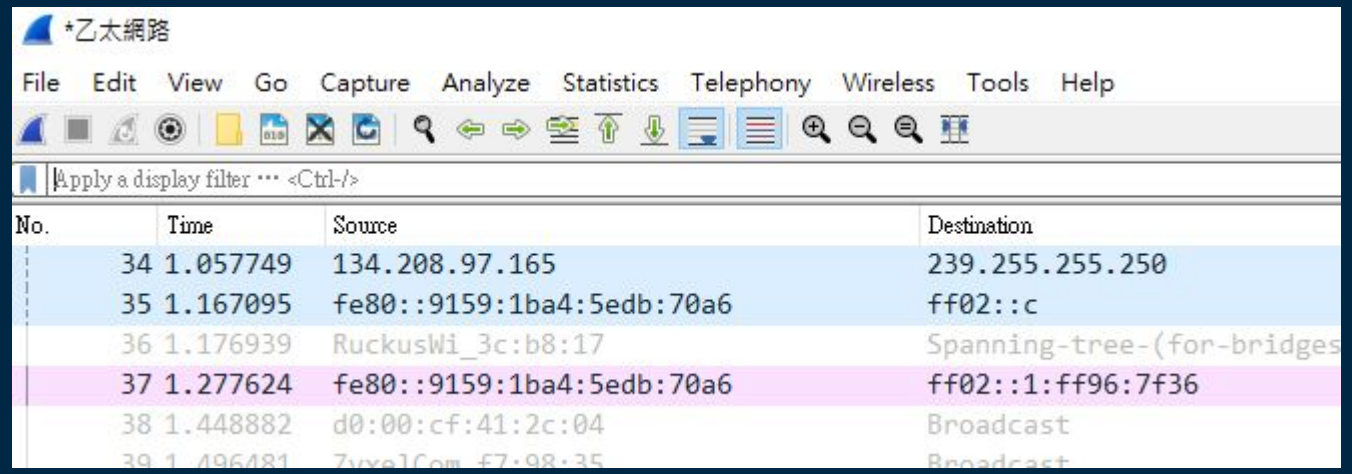
```
Windows IP 設定

乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . . :
   IPv6 位址. . . . . . . . . . . . . .: 2001:288:b001:28:48f0:2a5e:a567:f0dc
   臨時 IPv6 位址. . . . . . . . . . . : 2001:288:b001:28:9d18:86f8:3a93:7358
   連結-本機 IPv6 位址 . . . . . . . . : fe80::1c26:28b:33da:291b%16
   IPv4 位址 . . . . . . . . . . . . . : 134.208.97.146
   子網路遮罩 . . . . . . . . . . . . .: 255.255.255.0
   預設閘道 . . . . . . . . . . . . . .: fe80::[illegible]20ff:fe7e:29e6%16
                                         134.208.97.254
```

## 2. Ping 一個外部網域，取得其 IP

```
C:\Users>ping www.google.com

Ping www.google.com [142.251.43.4] (使用 32 位元組的資料):
回覆自 142.251.43.4: 位元組=32 時間=4ms TTL=115
回覆自 142.251.43.4: 位元組=32 時間=4ms TTL=115
回覆自 142.251.43.4: 位元組=32 時間=4ms TTL=115
回覆自 142.251.43.4: 位元組=32 時間=4ms TTL=115

142.251.43.4 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 4ms，最大值 = 4ms，平均 = 4ms
```

## 3. 開始追蹤封包，並在 cmd tracert 該IP

```
C:\Users>tracert 142.251.43.4

在上限 30 個躍點上
追蹤 tsa03s08-in-f4.1e100.net [142.251.43.4] 的路由:

  1    <1 ms    <1 ms    <1 ms  10.1.7.254
  2     1 ms    <1 ms    <1 ms  10.0.0.9
  3     1 ms     1 ms    <1 ms  10.0.0.1
  4     3 ms     3 ms     3 ms  192.192.61.162
  5     3 ms     4 ms     3 ms  192.192.61.184
  6     3 ms     3 ms     3 ms  192.192.61.203
  7     4 ms     4 ms     4 ms  72.14.202.60
  8     4 ms     4 ms     4 ms  172.253.50.121
  9     4 ms     4 ms     4 ms  142.251.77.87
 10     4 ms     4 ms     4 ms  tsa03s08-in-f4.1e100.net [142.251.43.4]

追蹤完成。
```




Filter → **ip.src == 134.208.xx.xx && ip.dst == xx.xx.xx.xx && ip.ttl == 1**

→ **ip.src == router ip && ip.dst == 134.208.xx.xx**

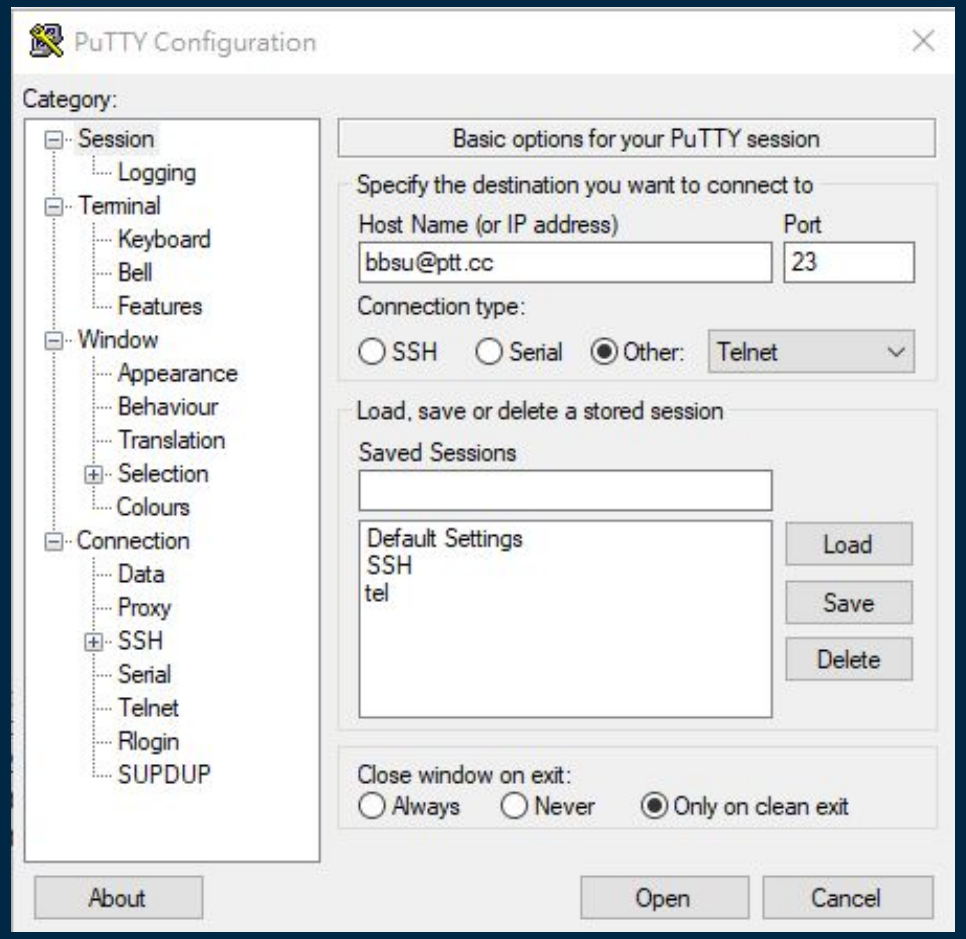
查看 tracert 路徑中的 router

# Telnet

***PUTTY*** https://reurl.cc/1e4WQ9

**Host Name 輸入 bbsu@ptt.cc**

**Connection type 選擇 telnet**

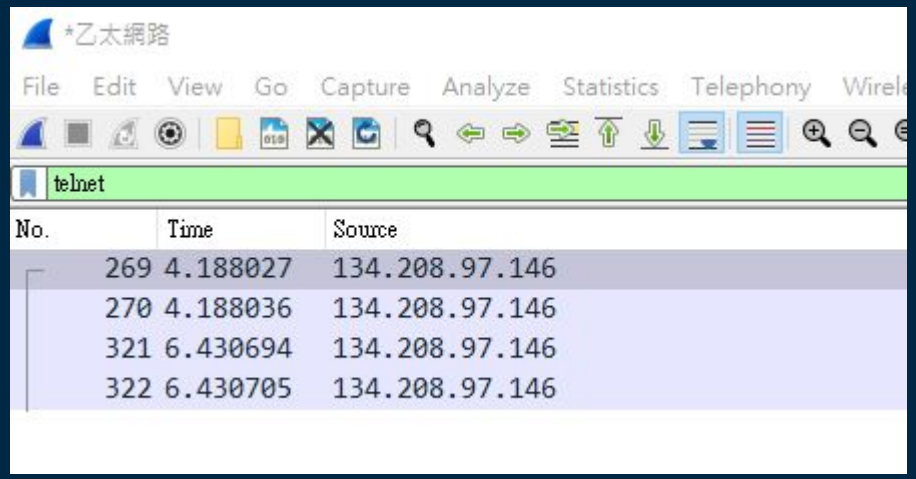


# Telnet

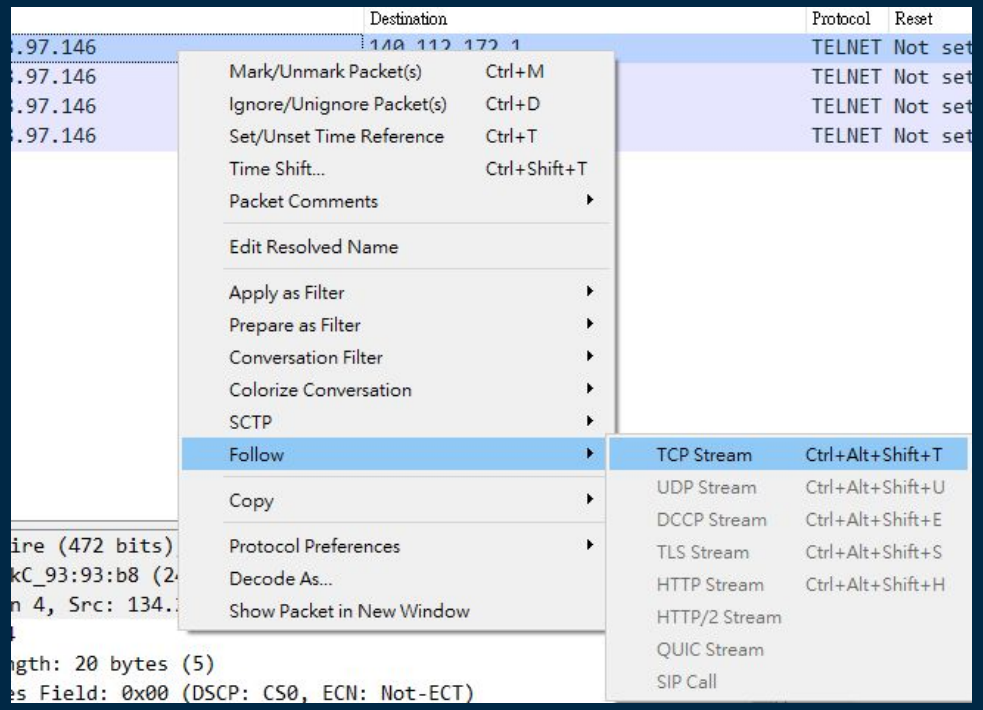
1. Wireshark 開始捕捉封包

2. 連上遠端主機後輸入文字訊息

3. Filter 過濾 telnet




4. 右鍵後 Follow => TCP Stream
即可觀察到訊息的明文

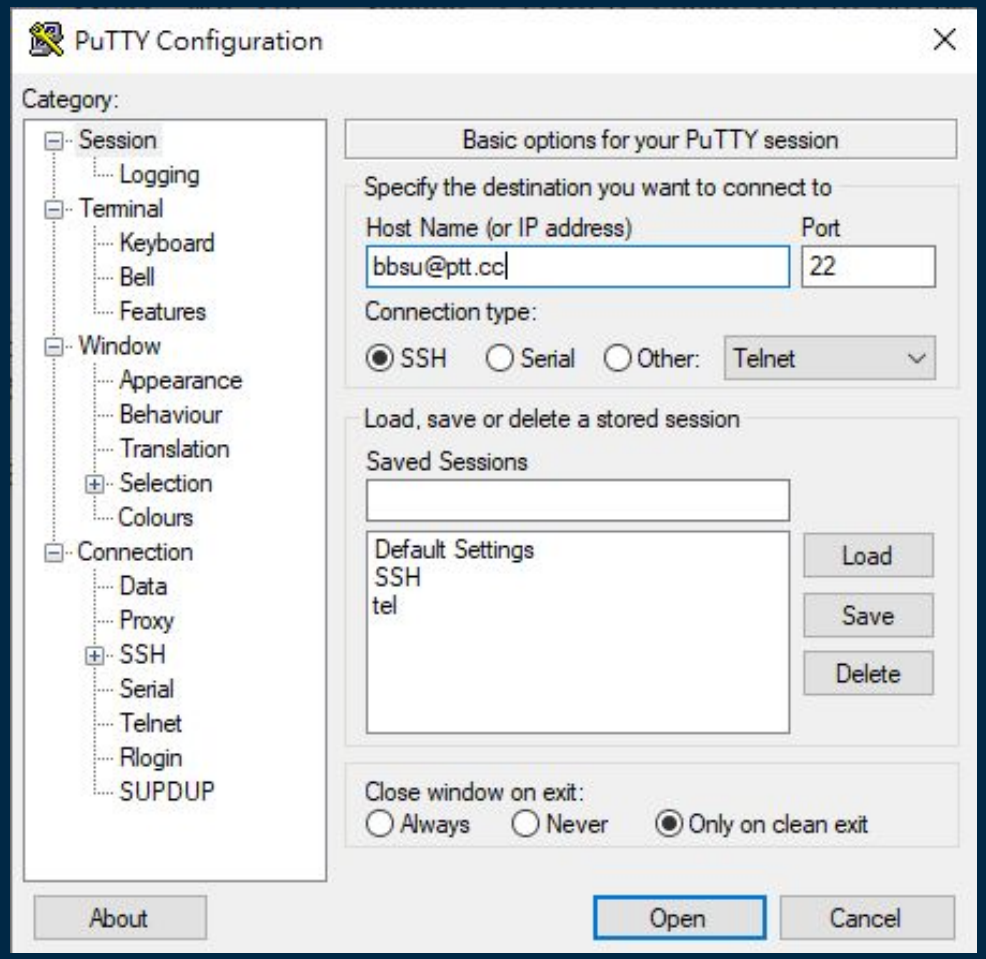


# SSH

***PUTTY*** https://reurl.cc/1e4WQ9

**Host Name 輸入 bbsu@ptt.cc**

**Connection type 選擇 SSH**

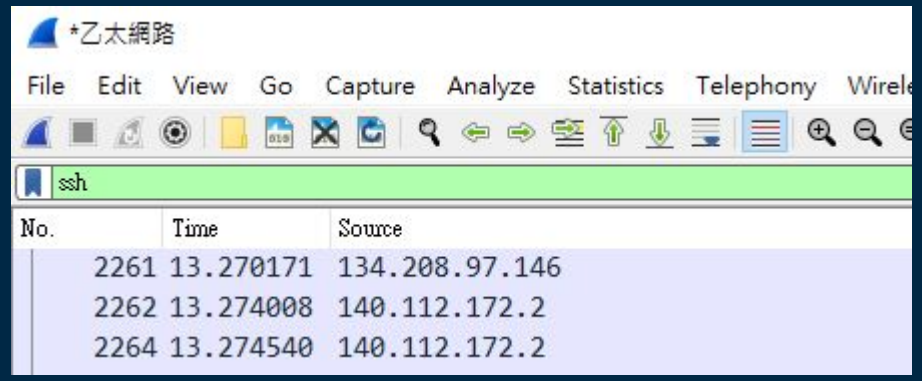


# SSH

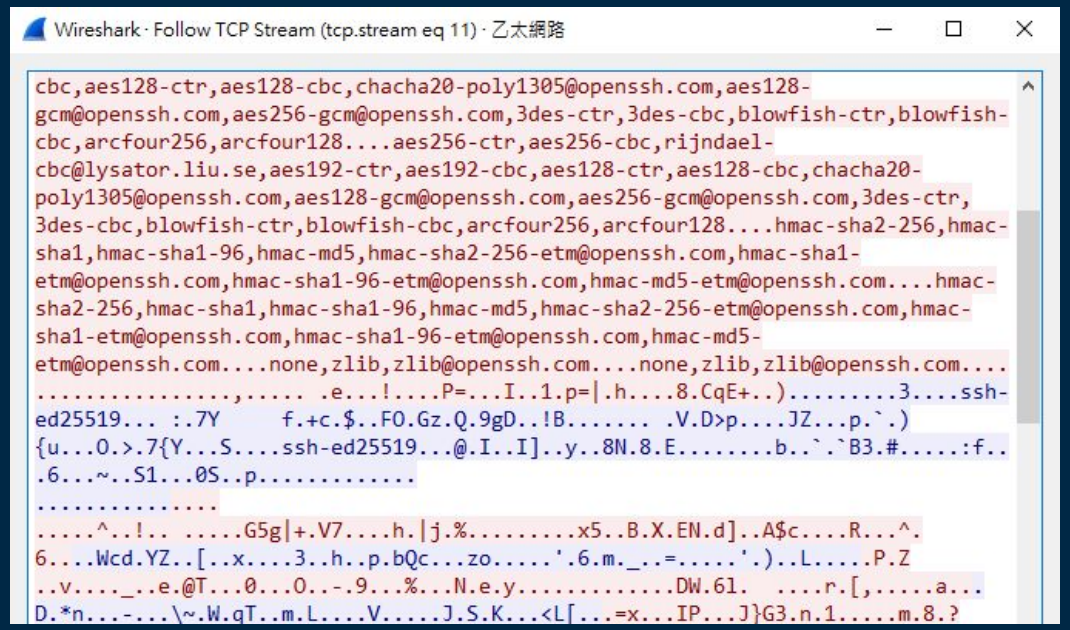
1. Wireshark 開始捕捉封包

2. 連上遠端主機後輸入文字訊息

3. Filter 過濾 ssh

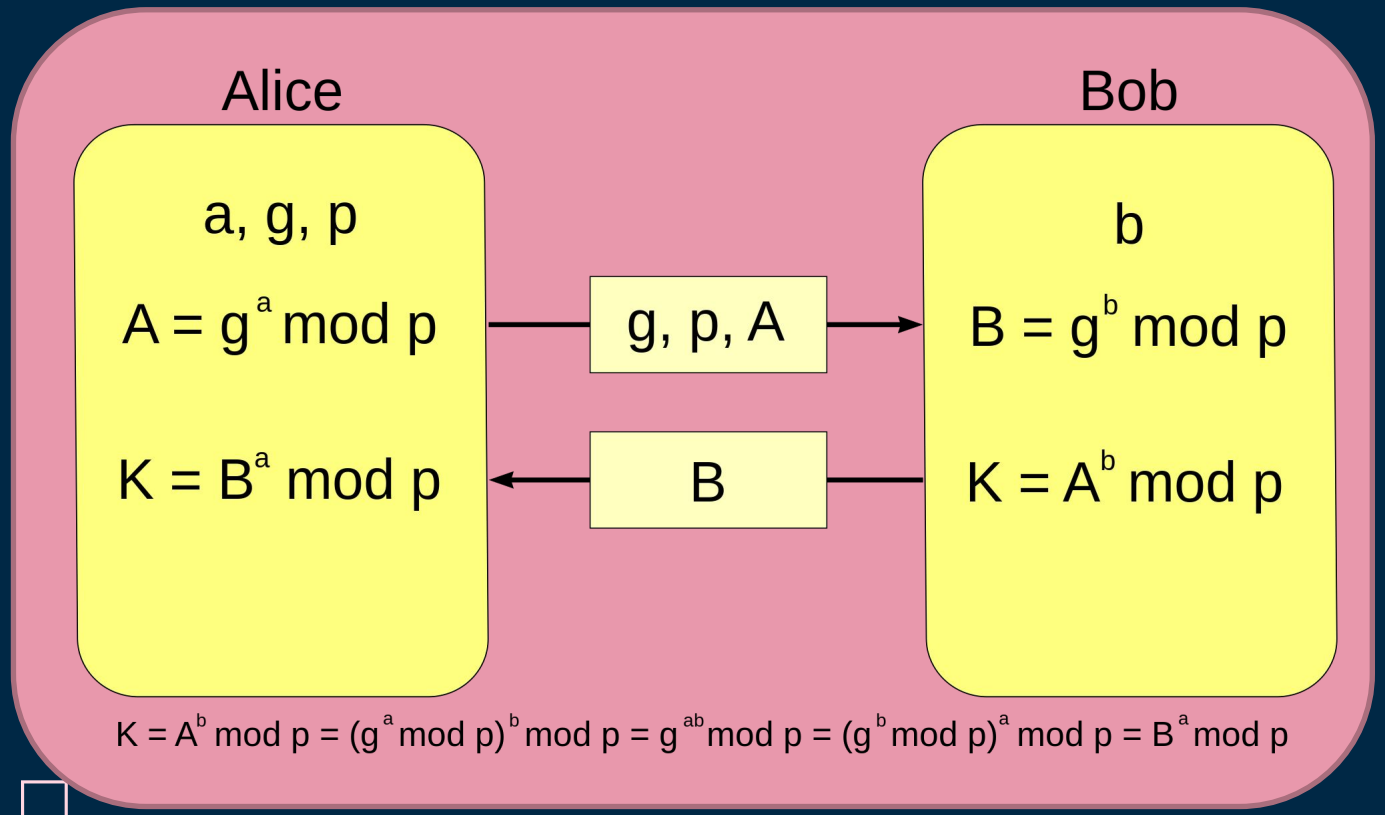


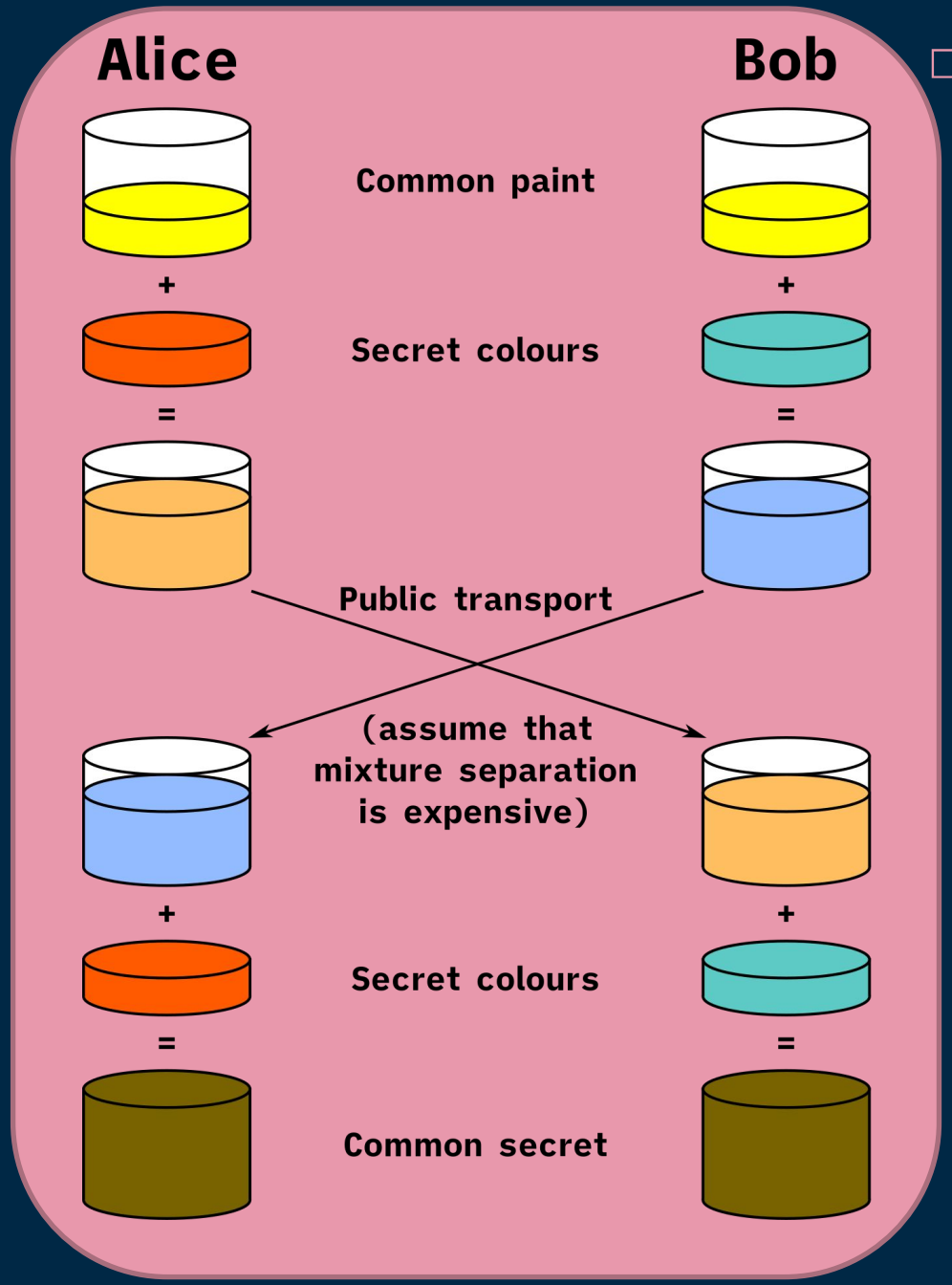

4. 右鍵後 Follow => TCP Stream
即可觀察到訊息為密文



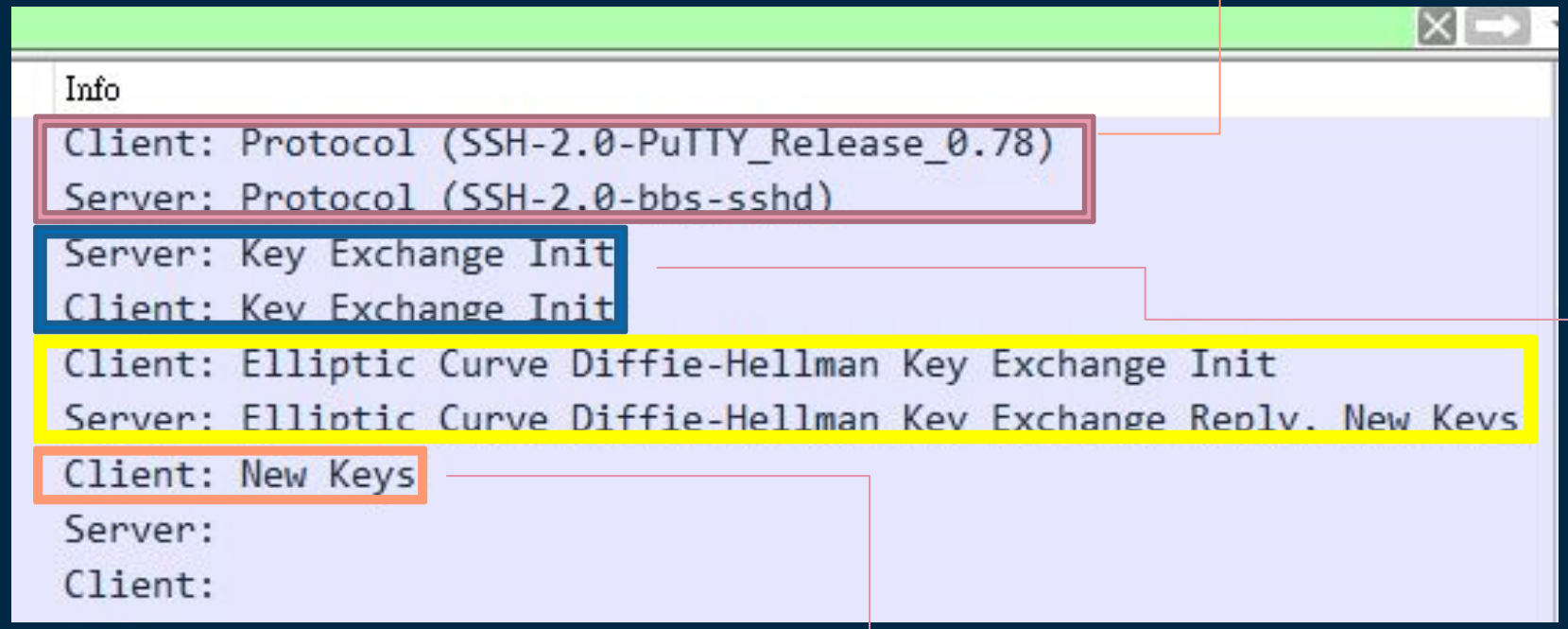
# Diffie-Hellman key exchange, D-H

**使雙方能夠在不安全的通道中建立起一個共享金鑰**



# SSH




雙方確認SSH協議版本

確認密鑰交換算法、
加密算法、MAC算法

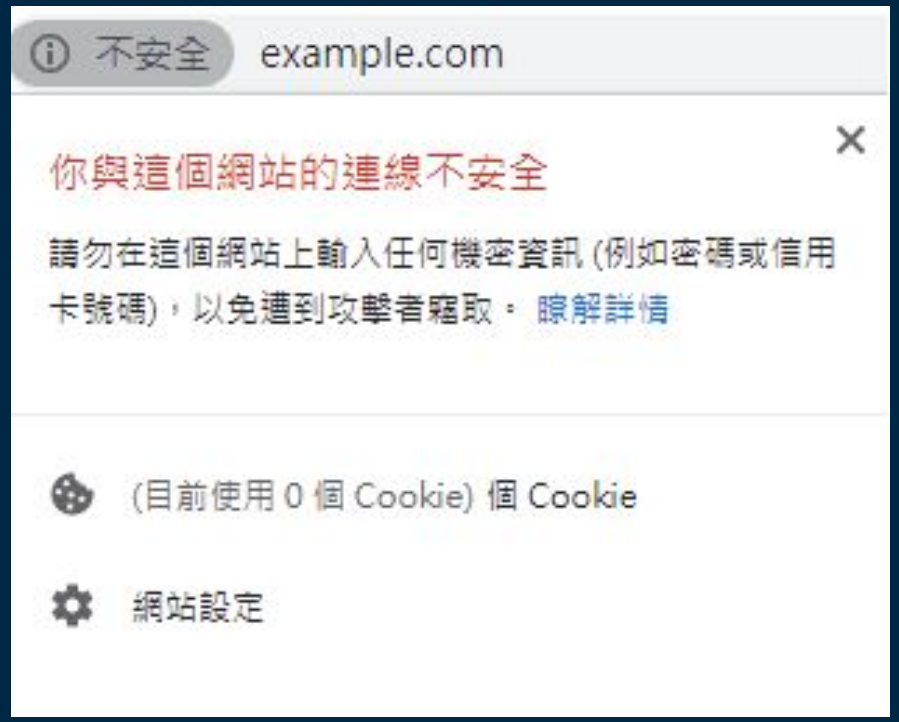
進行D-H密鑰交換

進行D-H密鑰交換

# HTTP

***HTTP*** *http://tutor.linker.tw/*

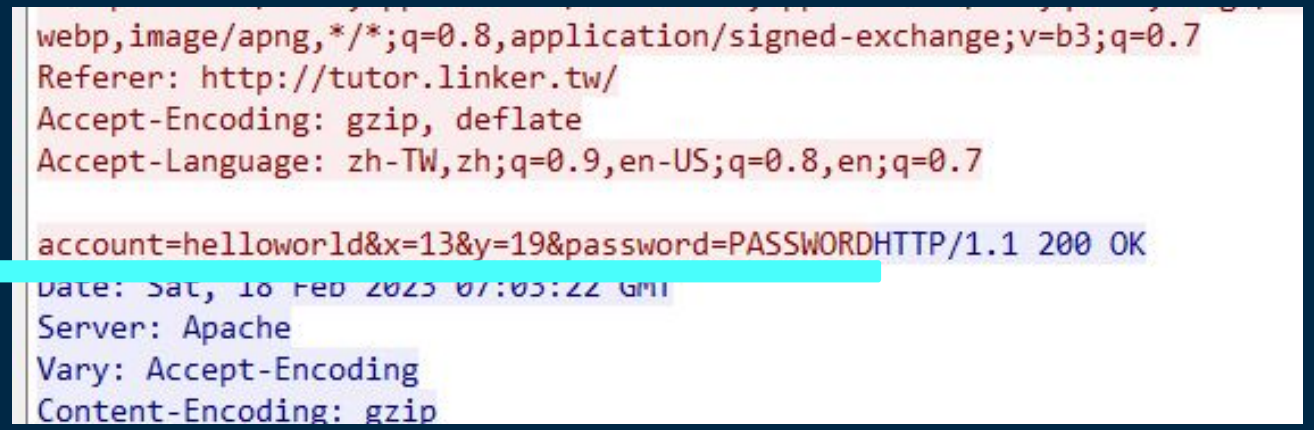
**在HTTP下，使用者和網頁是直接透過明文進行傳輸，並沒有任何保護，在網站中傳輸的資訊有外洩的風險。**



# HTTP

1. 開始擷取封包，並在網站上輸入帳號密碼


2. Filter 過濾 http
，並對封包 follow TCP Stream



# HTTP

***HTTP*** *http://www.transtaipei.idv.tw/*

1. 將wireshark 開啟後，瀏覽 http 網站

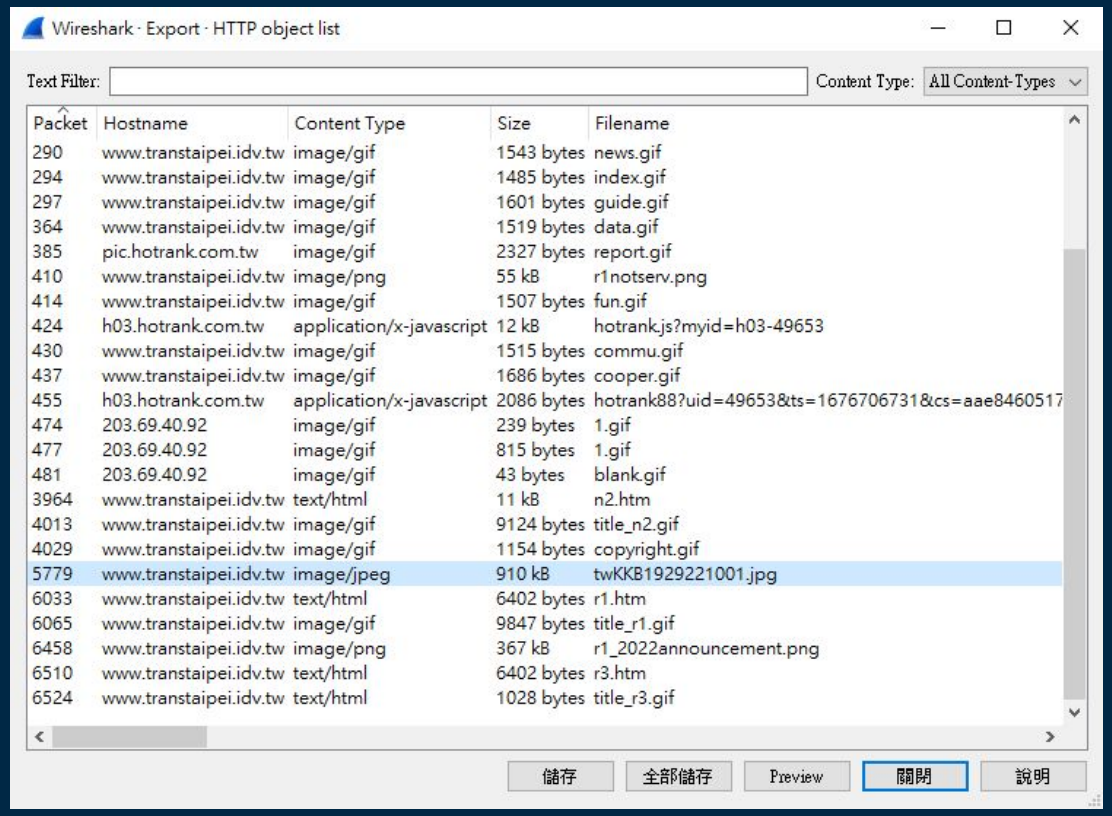
2. Filter http 並觀察封包

| Protocol | Reset | Info |
|---|---|---|
| HTTP | Not set | HTTP/1.1 200 OK (text/html) |
| HTTP | Not set | HTTP/1.1 200 OK (text/html) |
| HTTP | Not set | GET /title/title.gif HTTP/1.1 |
| HTTP | Not set | GET /r1notserv.png HTTP/1.1 |
| HTTP | Not set | GET /title/title_fblike.gif HTTP/1.1 |
| HTTP | Not set | HTTP/1.1 200 OK (GIF89a) |
| HTTP | Not set | GET /menu/index.gif HTTP/1.1 |
| HTTP | Not set | GET /menu/news.gif HTTP/1.1 |
| HTTP | Not set | GET /menu/guide.gif HTTP/1.1 |
| HTTP | Not set | HTTP/1.1 200 OK (GIF89a) |
| HTTP | Not set | GET /menu/data.gif HTTP/1.1 |

# HTTP 取出檔案

1. File → Export Objects → HTTP

2. 選取檔案後儲存



# HTTP 取出檔案

**HTTP** http://tgspp.org.tw/

**Hex editor** https://reurl.cc/WDLmLO

# HTTP 取出檔案

1. 開始擷取封包，並下載 .docx 檔案

2. Filter http，觀察封包資訊

| Protocol | Reset | Info |
|---|---|---|
| HTTP | Not set | HTTP/1.1 200 OK (text/html) |
| HTTP | Not set | GET /favicon.ico HTTP/1.1 |
| HTTP | Not set | HTTP/1.1 200 OK (image/vnd.microsoft.icon) |
| HTTP | Not set | GET /uploads/Download/Form/A01-%E5%85%A5%E5%AD%B8%E7%94%B3%E8%AB%8B%E6%9B%B8.docx HTTP/1.1 |
| HTTP | Not set | HTTP/1.1 200 OK (application/vnd.openxmlformats-officedocument.wordprocessingml.document) |

# HTTP 取出檔案

## 3. Follow TCP Stream

## 4. 觀察封包內容

*HTTP Request*

*HTTP Response*

*Docx 檔案*

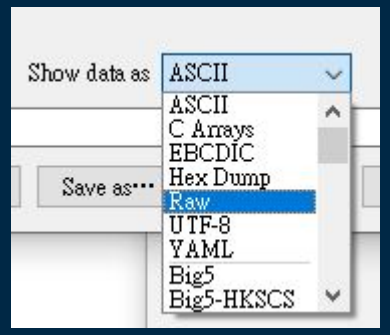
Wireshark · Follow TCP Stream (tcp.stream eq 7) · 乙太網路

```
GET /uploads/Download/Form/A01-
%E5%85%A5%E5%AD%B8%E7%94%B3%E8%AB%8B%E6%9B%B8.docx HTTP/1.1
Host: tgspp.org.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://tgspp.org.tw/
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: CMSSESSID168ef4a31272=2o2hmg8jldp4qmn2ds4ednoid6

HTTP/1.1 200 OK
Date: Sat, 18 Feb 2023 10:43:02 GMT
Server: Apache
Accept-Ranges: bytes
Content-Length: 25258
Cache-Control: public
Expires: Mon, 20 Mar 2023 10:43:02 GMT
X-Powered-By: PleskLin
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Type: application/vnd.openxmlformats-
officedocument.wordprocessingml.document

PK.........!....w....1.......[Content_Types].xml ...
(.......................................................................
.......................................................................
.......................................................................
.......................................................................
.......................................................................
.......................................................................
```

**List of file signatures**

# HTTP 取出檔案

5. Show data as Raw




6. Save as 儲存 data

7. 在 HxD 中打開 data

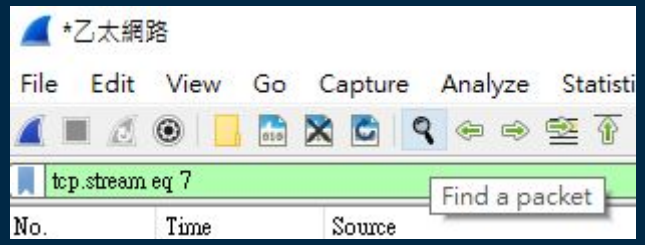
8. 在 HxD 中搜尋 “ 50 4B ”，並將前面的文字刪除

List of file signatures

9. 另存新檔，並將副檔名改成 .docx

# HTTP

1. 點擊 Find a packet




2. 搜尋 “ reassembled TCP Segment ”

3. 觀察 TCP 分段傳輸

```
  TCP payload (777 bytes)
  TCP segment data (777 bytes)
[18 Reassembled TCP Segments (25597 bytes): #322(1460), #323(1460), #325(1460), #326(1460), #328(1460), #329(1460), #331(1460), #332(1460), #334
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
```

# HTTPS

HTTPS 經由 HTTP 通訊，利用 SSL/TLS 加密封包

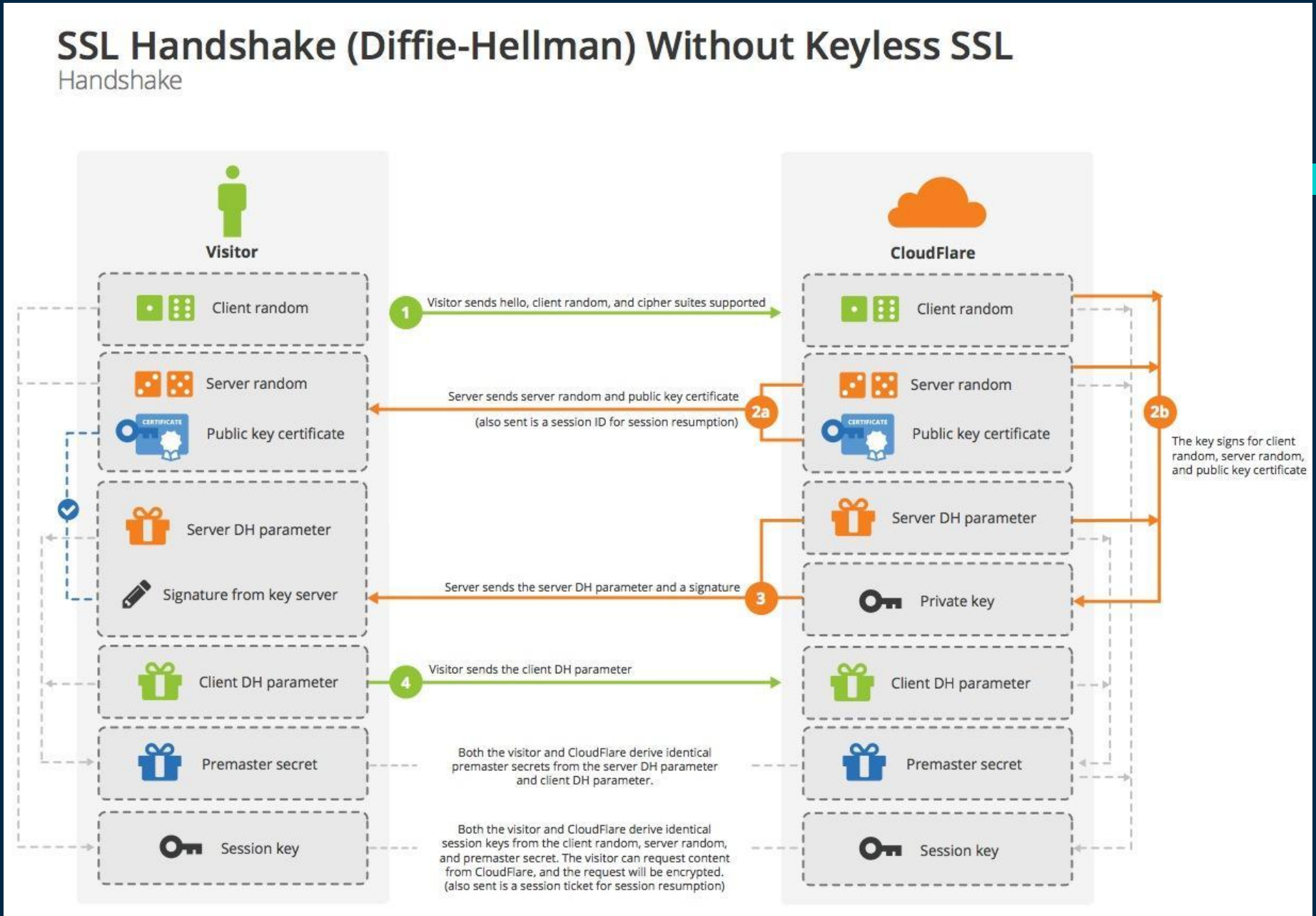
HTTP + SSL/TLS = HTTPS

# SSL / TLS

1. 加密傳輸
2. 身分驗證　　SSL/TLS 憑證
3. 確保數據完整性　Message Authentication Code, MAC

# HTTPS

## *SSL / TLS Handshake*



# HTTPS

1. 開啟 Wireshark 後進入一個 Https 網站

2. Wireshark filter “ tls ” ，對 Client Hello follow > TCP Stream

| Protocol | Reset | Info |
|---|---|---|
| TCP | Not set | 59650 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P |
| TCP | Not set | 443 → 59650 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SA |
| TCP | Not set | 59650 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0 |
| TLSv1.3 | Not set | Client Hello |
| TCP | Not set | 443 → 59650 [ACK] Seq=1 Ack=518 Win=66816 Len=0 |
| TLSv1.3 | Not set | Server Hello, Change Cipher Spec |
| TCP | Not set | 443 → 59650 [ACK] Seq=1413 Ack=518 Win=66816 Len=1412 [TCP seg |
| TCP | Not set | 443 → 59650 [ACK] Seq=2825 Ack=518 Win=66816 Len=1412 [TCP seg |
| TCP | Not set | 59650 → 443 [ACK] Seq=518 Ack=4237 Win=262400 Len=0 |
| TLSv1.3 | Not set | Application Data |
| TCP | Not set | 59650 → 443 [ACK] Seq=518 Ack=4496 Win=262144 Len=0 |
| TLSv1.3 | Not set | Change Cipher Spec, Application Data |
| TLSv1.3 | Not set | Application Data |

# HTTPS

SSL Version 、Supported ciphers 、Random number

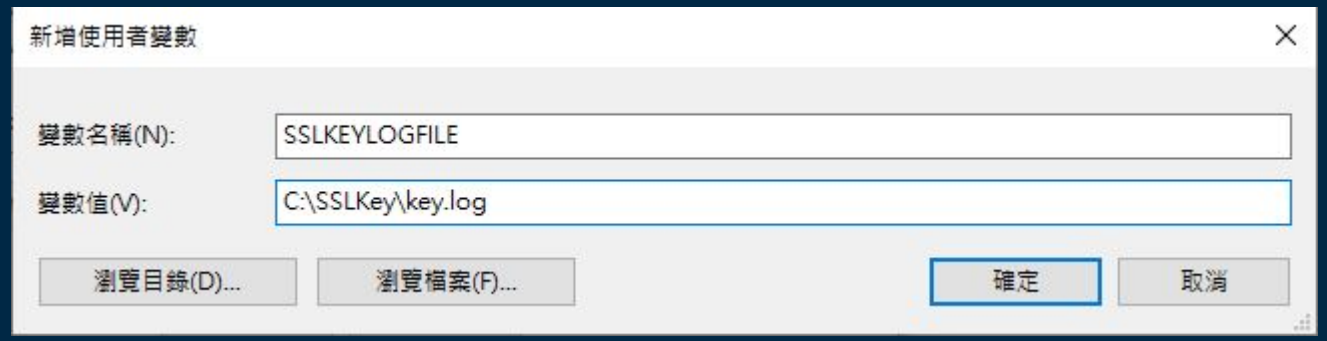
SSL Version 、
Selected ciphers 、
Random number 、
D-H Pubkey 、
SSL Certificate

| Protocol | Reset | Info |
|---|---|---|
| TCP | Not set | 59650 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P |
| TCP | Not set | 443 → 59650 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SA |
| TCP | Not set | 59650 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0 |
| TLSv1.3 | Not set | Client Hello |
| TCP | Not set | 443 → 59650 [ACK] Seq=1 Ack=518 Win=66816 Len=0 |
| TLSv1.3 | Not set | Server Hello, Change Cipher Spec |
| TCP | Not set | 443 → 59650 [ACK] Seq=1413 Ack=518 Win=66816 Len=1412 [TCP seg |
| TCP | Not set | 443 → 59650 [ACK] Seq=2825 Ack=518 Win=66816 Len=1412 [TCP seg |
| TCP | Not set | 59650 → 443 [ACK] Seq=518 Ack=4237 Win=262400 Len=0 |
| TLSv1.3 | Not set | Application Data |
| TCP | Not set | 59650 → 443 [ACK] Seq=518 Ack=4496 Win=262144 Len=0 |
| TLSv1.3 | Not set | Change Cipher Spec, Application Data |
| TLSv1.3 | Not set | Application Data |

D-H Pubkey

# HTTPS 流量解密

1. 系統 → 關於 → 進階系統設定 → 環境變數 → 新增使用者變數




2. 重新開啟 Wireshark 與 瀏覽器

# HTTPS 流量解密

3. 開始擷取封包，並開 啟 key.log 確認是否有成功紀錄 key.log

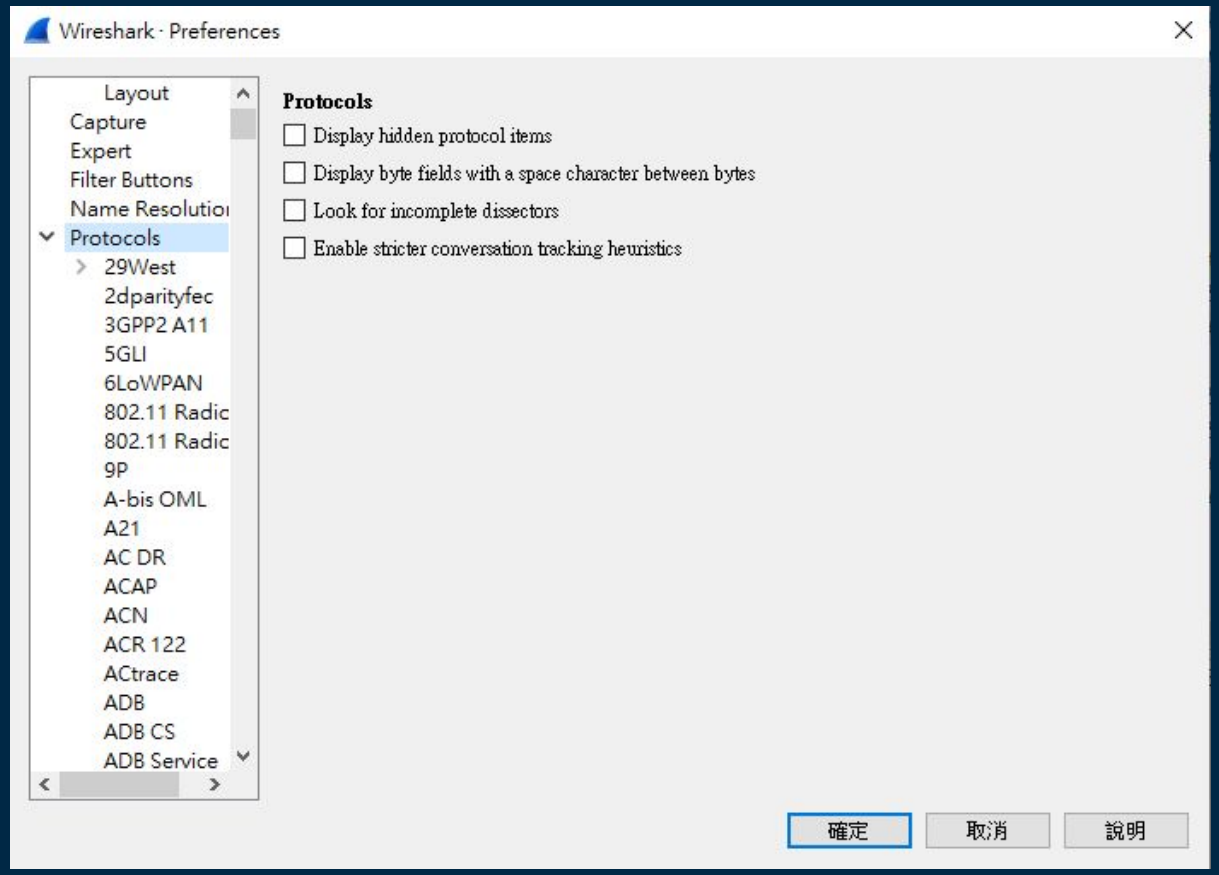
key.log - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

```
SERVER_TRAFFIC_SECRET_0 cdfefc2a76db2355c73d885e0ff52ccaff1d81ef5712ee0f0ee2427d214aca49 e6f5a37
EXPORTER_SECRET cdfefc2a76db2355c73d885e0ff52ccaff1d81ef5712ee0f0ee2427d214aca49 46e014008d97cb0
CLIENT_HANDSHAKE_TRAFFIC_SECRET 708e97e05a2613de6236d76f3e7cd7b0bc7392ccd9da861f0193333ffb16374a
SERVER_HANDSHAKE_TRAFFIC_SECRET 708e97e05a2613de6236d76f3e7cd7b0bc7392ccd9da861f0193333ffb16374a
CLIENT_TRAFFIC_SECRET_0 708e97e05a2613de6236d76f3e7cd7b0bc7392ccd9da861f0193333ffb16374a f39af5f
SERVER_TRAFFIC_SECRET_0 708e97e05a2613de6236d76f3e7cd7b0bc7392ccd9da861f0193333ffb16374a 6ca2ce5
```

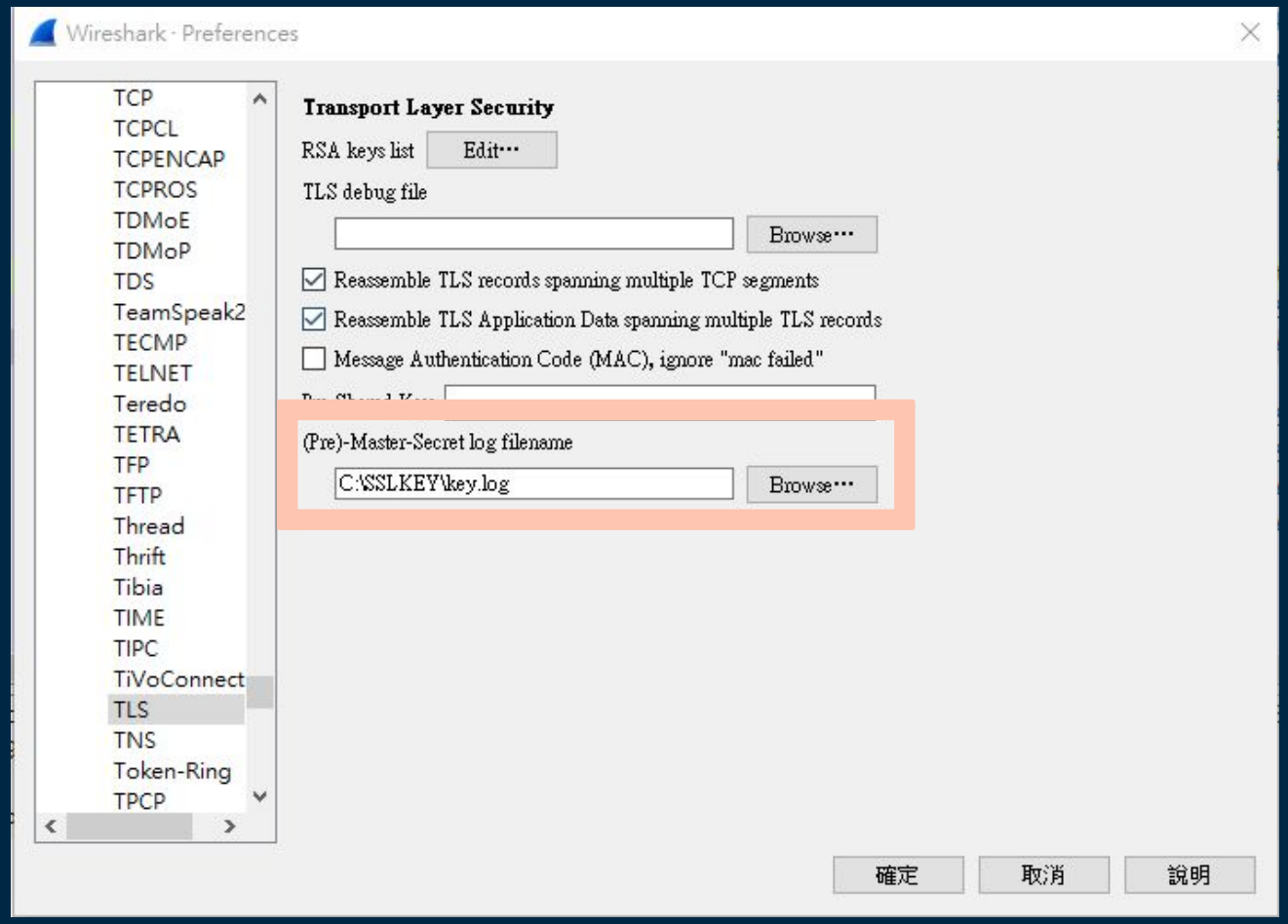
# HTTPS 流量解密

4. 於 Wireshark Edit → Preferences → Protocols



# HTTPS 流量解密

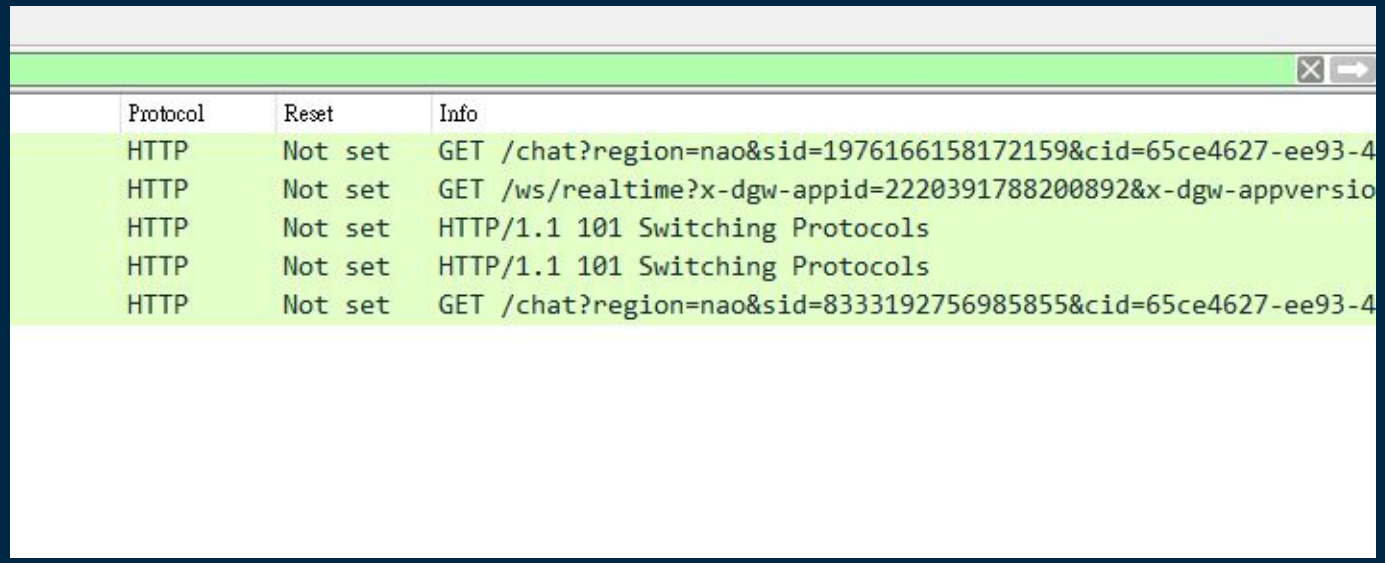
5. 找到 TLS，後在” Pre-Master-Secret log filename ” 中匯入 “ key.log “



# HTTPS 流量解密

6. 開啟 Wireshark ，即可觀察到底色為綠色的解密封包

7. Follow > HTTP ，即可觀察到明文

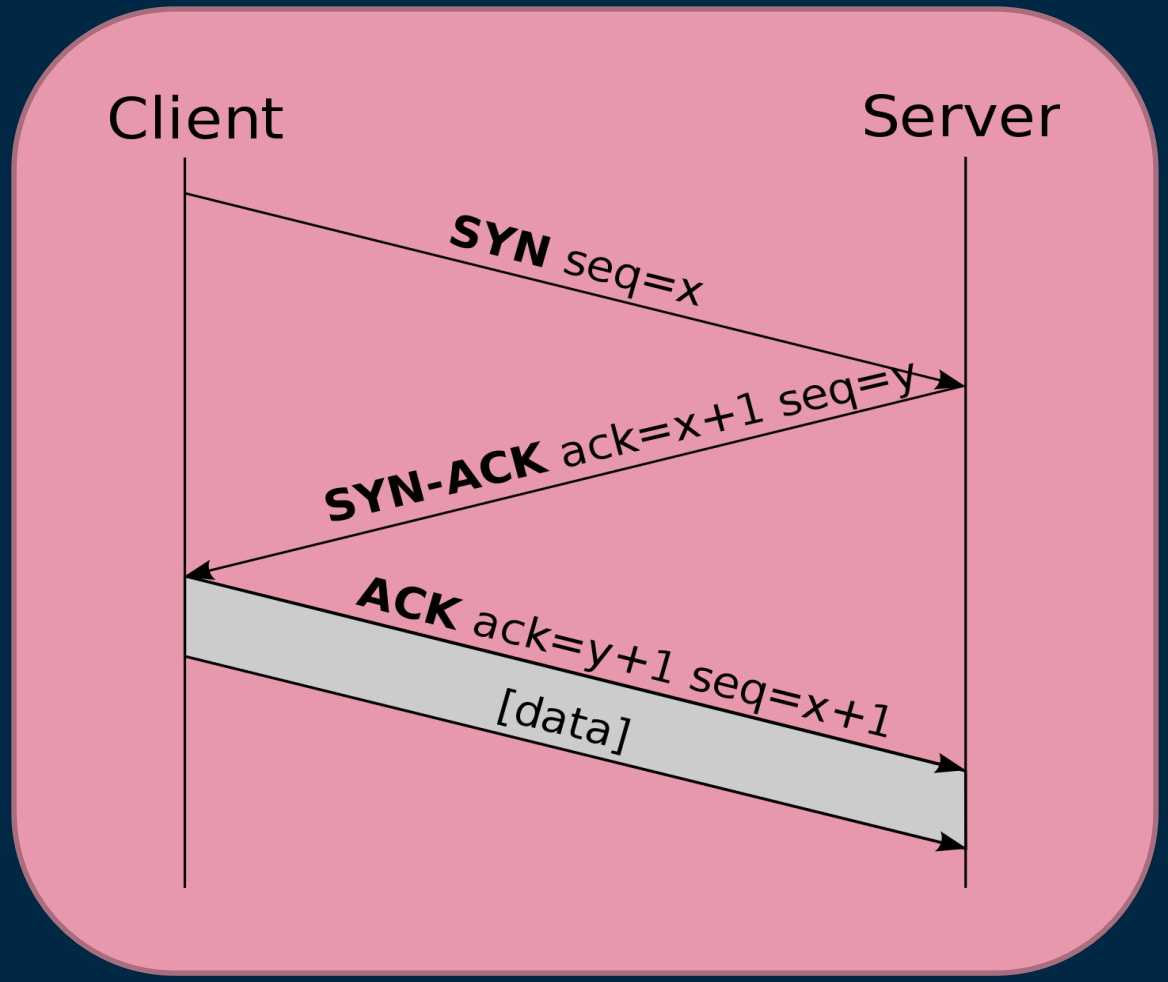


| Protocol | Reset | Info |
|---|---|---|
| HTTP | Not set | GET /chat?region=nao&sid=1976166158172159&cid=65ce4627-ee93-4 |
| HTTP | Not set | GET /ws/realtime?x-dgw-appid=2220391788200892&x-dgw-appversio |
| HTTP | Not set | HTTP/1.1 101 Switching Protocols |
| HTTP | Not set | HTTP/1.1 101 Switching Protocols |
| HTTP | Not set | GET /chat?region=nao&sid=8333192756985855&cid=65ce4627-ee93-4 |

# TCP Handshake

三向交握 (Three-way Handshake)

SYN + SYN/ACK + ACK = Established



# TCP Handshake

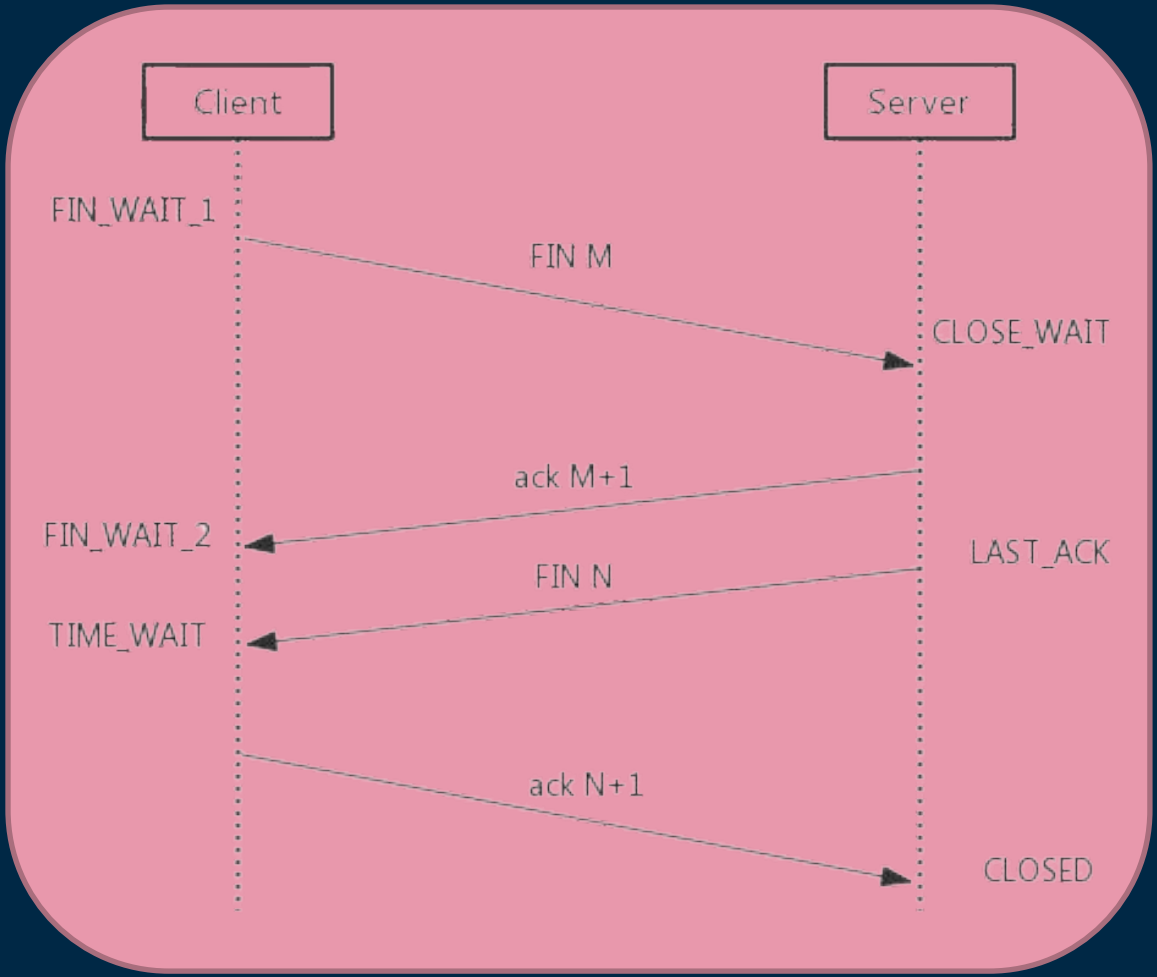
Filter “ tcp ”，對其中一個封包 Follow > TCP Stream

| Protocol | Reset | |
|---|---|---|
| TCP | Not set | 58385 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P |
| TCP | Not set | 443 → 58385 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SA |
| TCP | Not set | 58385 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0 |
| TLSv1.3 | Not set | |
| TCP | Not set | 443 → 58385 [ACK] Seq=1 Ack=518 Win=66816 Len=0 |
| TLSv1.3 | Not set | Server Hello, Change Cipher Spec, Encrypted Extensions, Finish |
| TLSv1.3 | Not set | Change Cipher Spec, Finished |
| HTTP | Not set | GET /ws/realtime?x-dgw-appid=2220391788200892&x-dgw-appversion |
| TCP | Not set | 443 → 58385 [ACK] Seq=219 Ack=1719 Win=69120 Len=0 |
| TLSv1.3 | Not set | New Session Ticket |
| TCP | Not set | 58385 → 443 [ACK] Seq=1719 Ack=396 Win=262656 Len=0 |
| HTTP | Not set | HTTP/1.1 101 Switching Protocols |
| WebSocket | Not set | WebSocket Binary [FIN] [MASKED] |
| WebSocket | Not set | WebSocket Binary [FIN] [MASKED] |
| WebSocket | Not set | WebSocket Binary [FIN] [MASKED] |
| WebSocket | Not set | WebSocket Binary [FIN] [MASKED] |
| WebSocket | Not set | WebSocket Binary [FIN] [MASKED] |
| WebSocket | Not set | WebSocket Binary [FIN] [MASKED] |

# TCP Handshake

## 四次揮手 (Four-Way Handshake)

**FIN + ACK + FIN + ACK = Terminated**



# TCP Handshake

Filter “ tcp ”，對其中一個封包 Follow > TCP Stream

| Protocol | Reset | Info |
|---|---|---|
| TLSv1.2 | Not set | Application Data |
| TCP | Not set | 443 → 58349 [ACK] Seq=1 Ack=30 Win=597 Len=0 |
| TLSv1.2 | Not set | Application Data |
| TCP | Not set | 58349 → 443 [ACK] Seq=30 Ack=26 Win=1022 Len=0 |
| TCP | Not set | 58349 → 443 [ACK] Seq=30 Ack=26 Win=1022 Len=1392 [TCP segment c |
| TLSv1.2 | Not set | Application Data |
| TCP | Not set | 443 → 58349 [ACK] Seq=26 Ack=1422 Win=608 Len=0 |
| TCP | Not set | 443 → 58349 [ACK] Seq=26 Ack=2726 Win=619 Len=0 |
| TLSv1.2 | Not set | Application Data |
| TLSv1.2 | Not set | Application Data |
| TCP | Not set | 58349 → 443 [ACK] Seq=2726 Ack=101 Win=1022 Len=0 |
| TLSv1.2 | Not set | Application Data |
| TCP | Not set | 443 → 58349 [ACK] Seq=101 Ack=2762 Win=619 Len=0 |
| TLSv1.2 | Not se | |
| TCP | Not se | 58349 → 443 [FIN, ACK] Seq=2792 Ack=101 Win=1022 Len=0 |
| TCP | Not se | 443 → 58349 [ACK] Seq=101 Ack=2792 Win=619 Len=0 |
| TCP | Not se | 443 → 58349 [FIN, ACK] Seq=101 Ack=2793 Win=619 Len=0 |
| TCP | Not se | 58349 → 443 [ACK] Seq=2793 Ack=102 Win=1022 Len=0 |