

03 我們示範用 Wireshark 判讀近期最熱門的網站 eTag 遠通電收

現況是我們根本不知道遠通電收的 IP
但是我們想知道
自己的電腦跟對方溝通了那些封包

首先

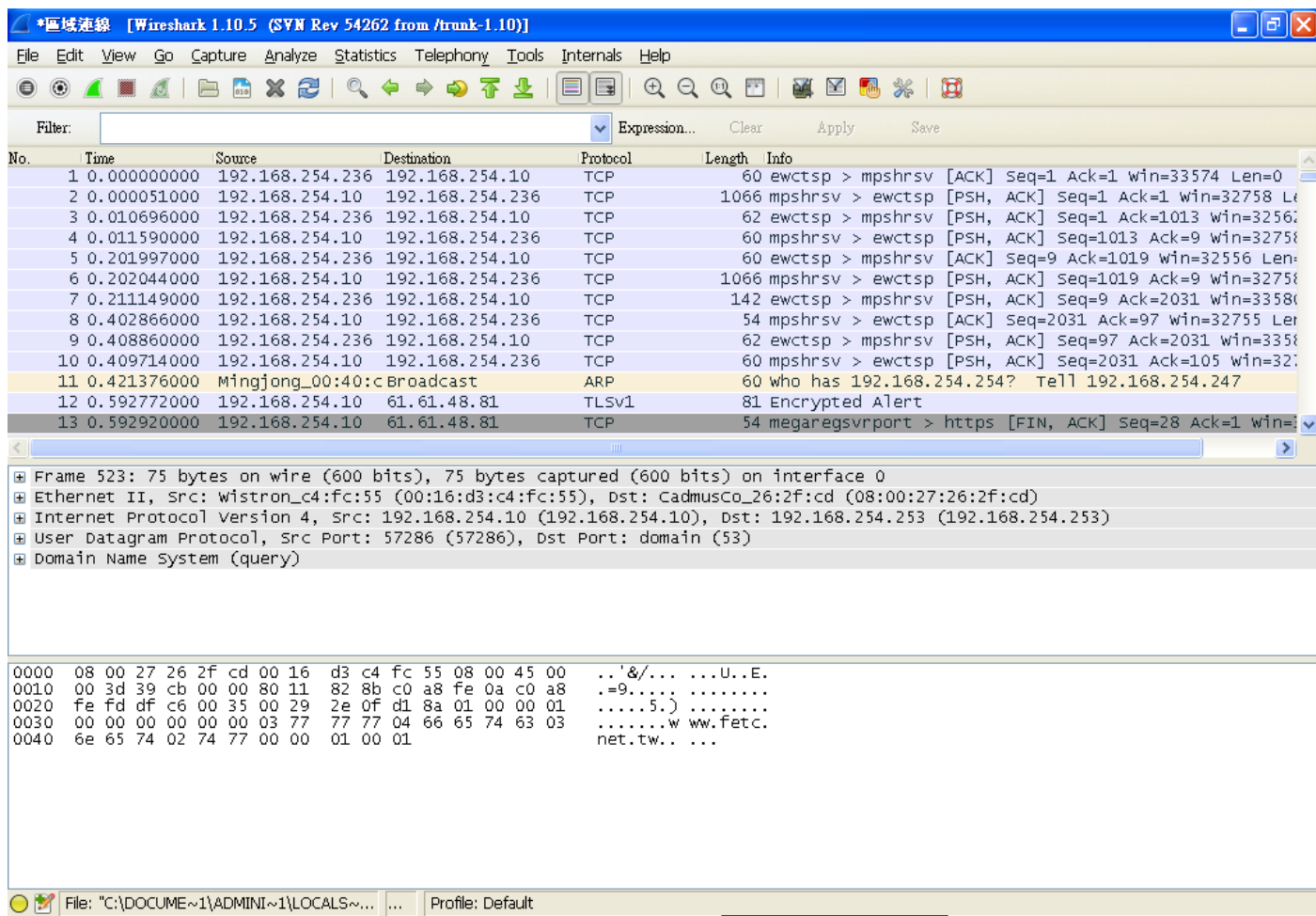
開啓 Wireshark 開始抓封包

然後開啓遠通電收的網頁

[http:// www.fetc.net.tw](http://www.fetc.net.tw)

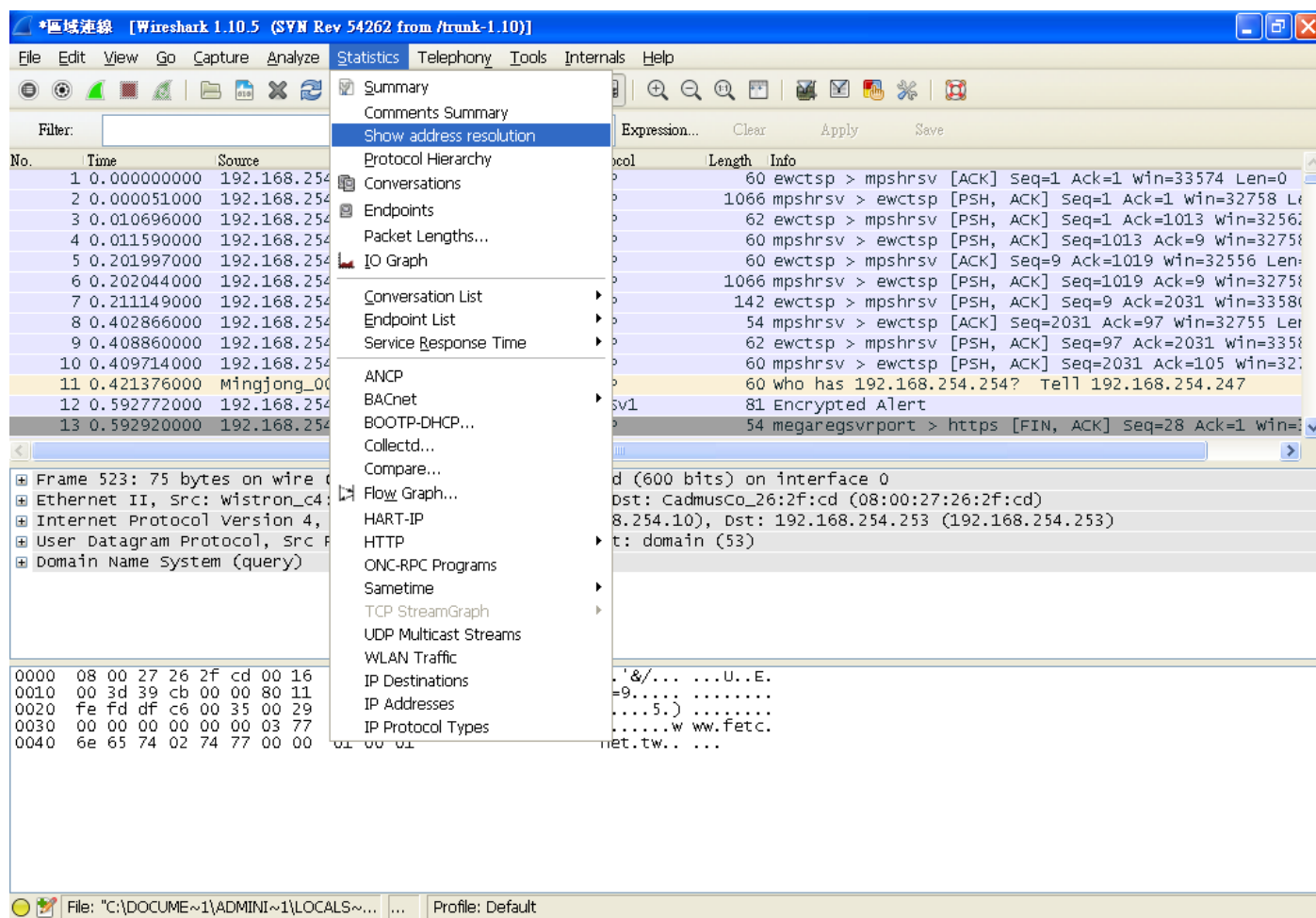


之後點停止



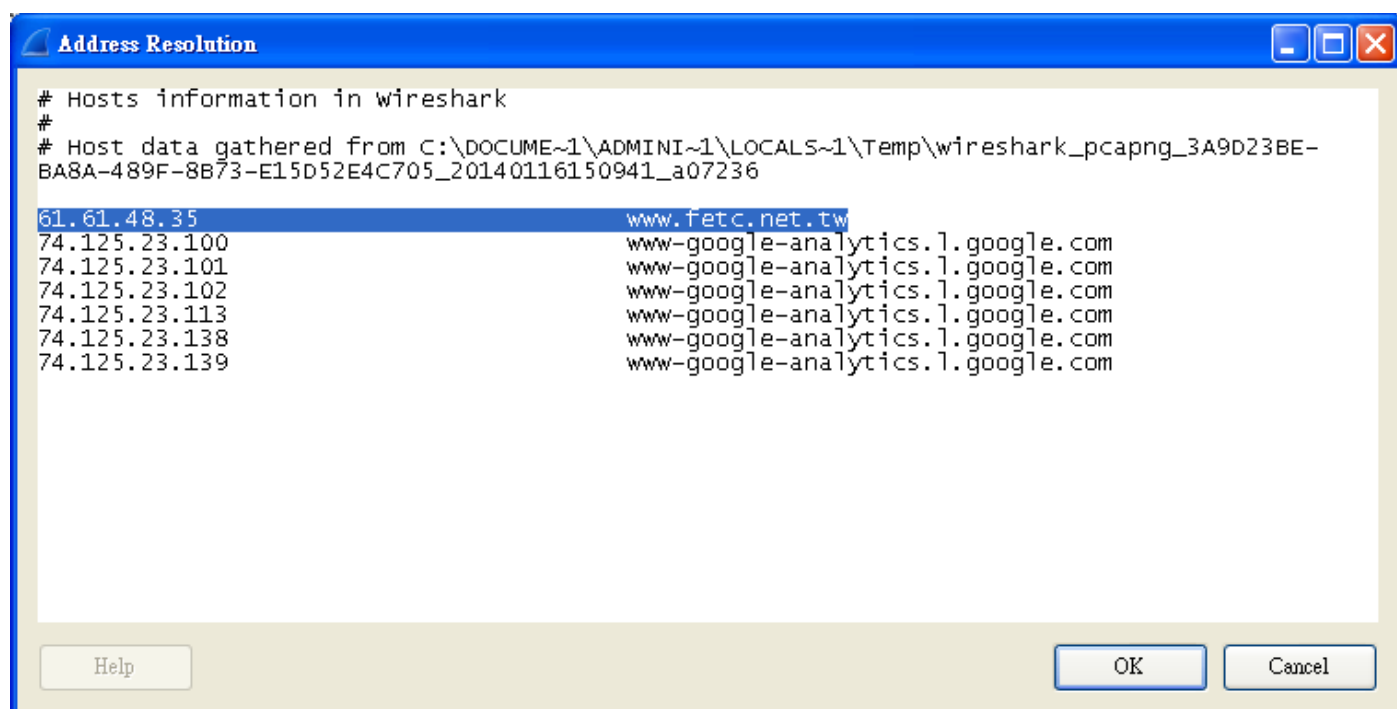
發現已經抓出一大堆的封包了

這個時候我們需要把遠通電收的 Domain 解出 IP



點 Statistics

Show address resolution

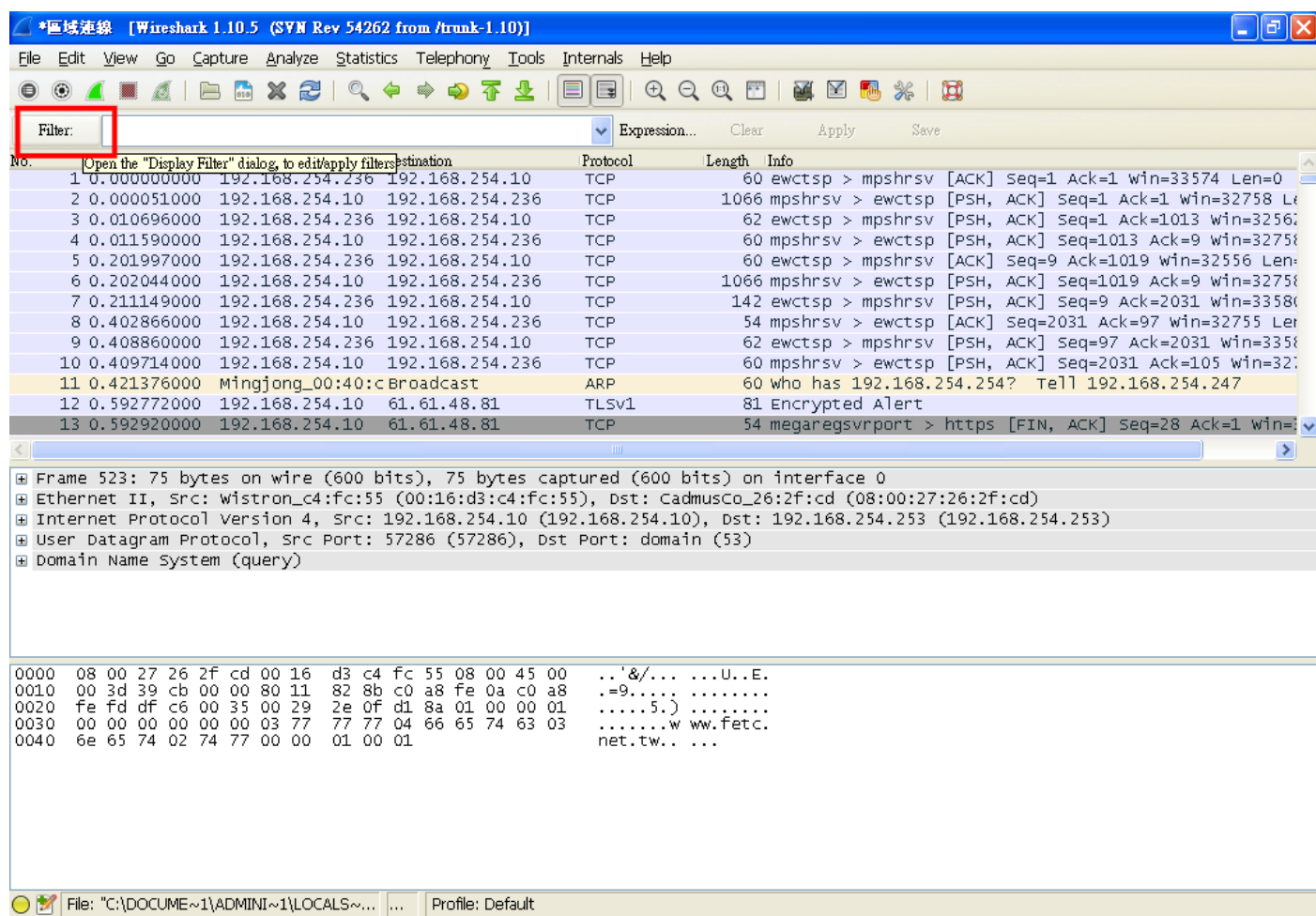


可以看見

我們連 www.fetc.net.tw 是連到 61.61.48.35

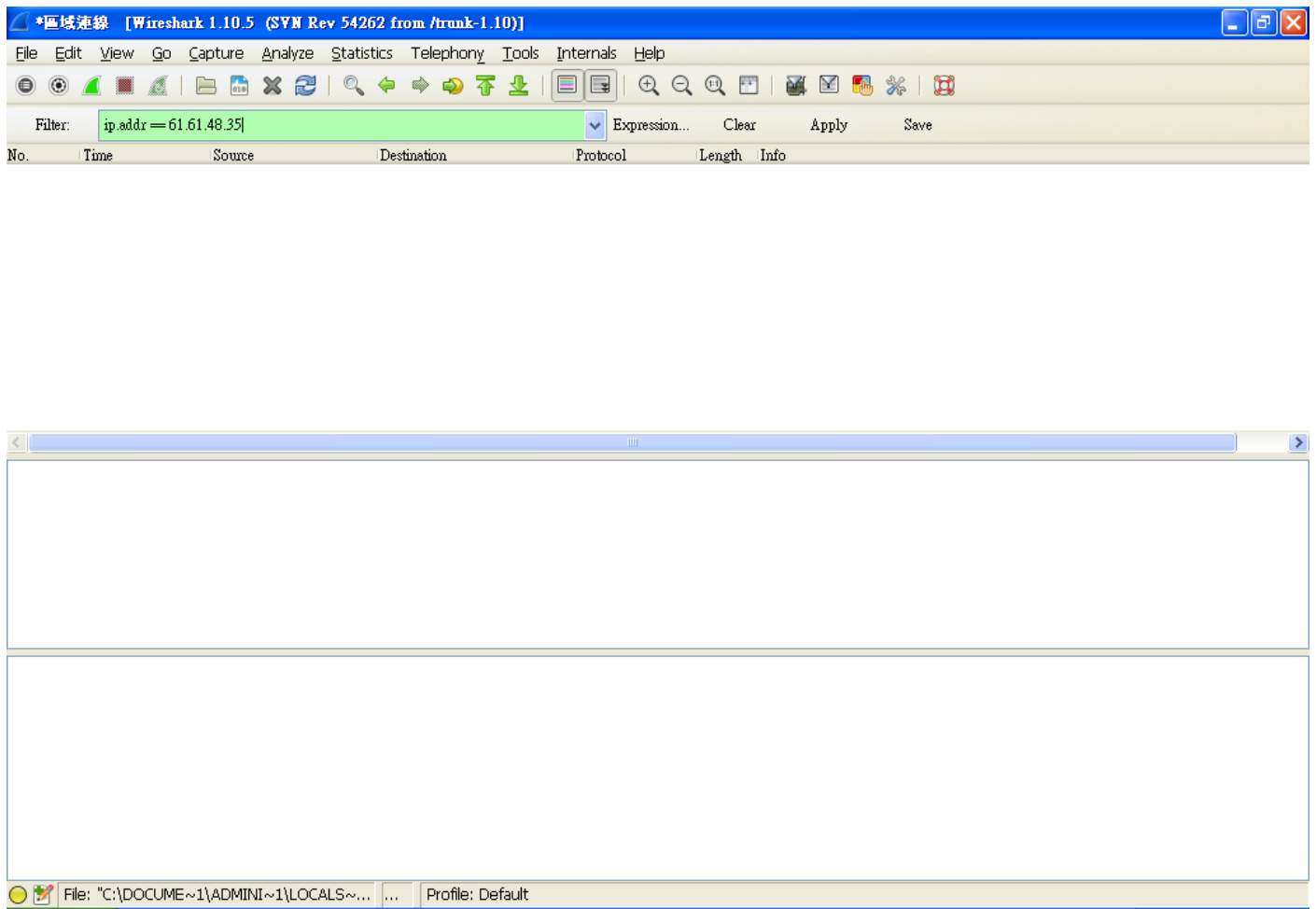
因為剛 Capture 封包我們是全抓

所以我們得下 Filter 過濾掉其他的 IP



所以在 Filetr 這邊先找 Sample

Ip address



改成我們要的

`ip.addr == 61.61.48.35`

再點 Apply 之後

The image shows a Wireshark 1.10.5 window with a filter set to 'ip.addr == 61.61.48.35'. The packet list shows several TCP and HTTP packets. The selected packet (No. 559) is a SYN packet from 192.168.254.10 to 61.61.48.35. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
559	11.897275000	192.168.254.10	61.61.48.35	TCP	66	emprise-11s > http [SYN] Seq=0 win=65535 Len=0 MSS=
560	11.908476000	61.61.48.35	192.168.254.10	TCP	66	http > emprise-11s [SYN, ACK] Seq=0 Ack=1 win=4356
561	11.908515000	192.168.254.10	61.61.48.35	TCP	54	emprise-11s > http [ACK] Seq=1 Ack=1 win=1048576
562	11.908688000	192.168.254.10	61.61.48.35	HTTP	819	GET / HTTP/1.1
563	11.922423000	61.61.48.35	192.168.254.10	TCP	60	http > emprise-11s [ACK] Seq=1 Ack=766 win=5121
564	11.924302000	61.61.48.35	192.168.254.10	HTTP	476	HTTP/1.1 301 Moved Permanently (text/html)
565	11.925251000	192.168.254.10	61.61.48.35	HTTP	893	GET /portal/ HTTP/1.1
566	11.938263000	61.61.48.35	192.168.254.10	TCP	60	http > emprise-11s [ACK] Seq=423 Ack=1605 win=5960
569	11.939955000	61.61.48.35	192.168.254.10	TCP	163	[TCP segment of a reassembled PDU]
570	11.942397000	61.61.48.35	192.168.254.10	TCP	1506	[TCP segment of a reassembled PDU]
571	11.942432000	192.168.254.10	61.61.48.35	TCP	54	emprise-11s > http [ACK] Seq=1605 Ack=1984 win=1048
572	11.942460000	61.61.48.35	192.168.254.10	TCP	522	[TCP segment of a reassembled PDU]
573	11.943092000	61.61.48.35	192.168.254.10	TCP	1506	[TCP segment of a reassembled PDU]

Frame 559: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

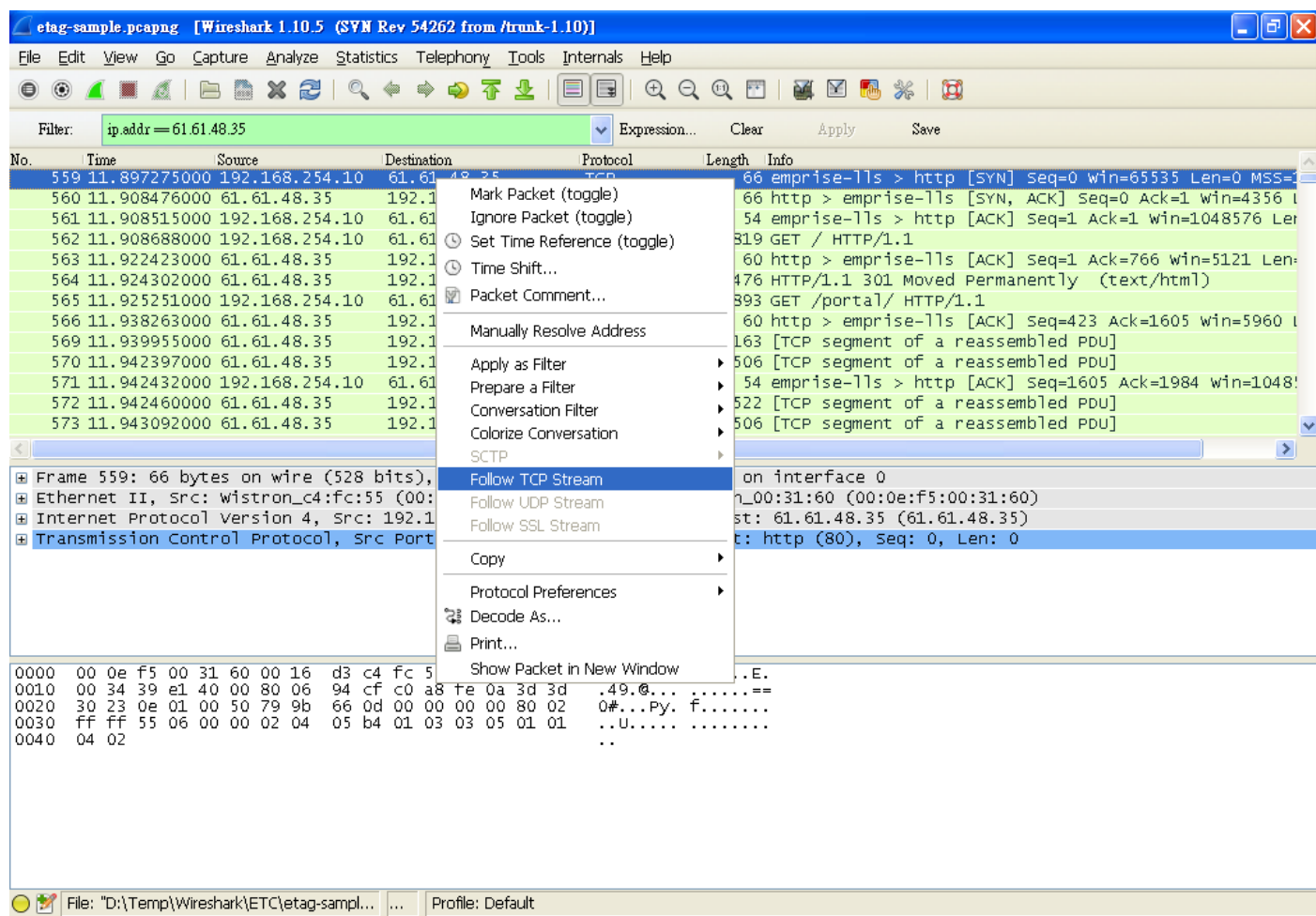
- Ethernet II, Src: wistron_c4:fc:55 (00:16:d3:c4:fc:55), Dst: IpacTech_00:31:60 (00:0e:f5:00:31:60)
- Internet Protocol Version 4, Src: 192.168.254.10 (192.168.254.10), Dst: 61.61.48.35 (61.61.48.35)
- Transmission Control Protocol, Src Port: emprise-11s (3585), Dst Port: http (80), Seq: 0, Len: 0

```

0000  00 0e f5 00 31 60 00 16 d3 c4 fc 55 08 00 45 00  ....1... ..U..E.
0010  00 34 39 e1 40 00 80 06 94 cf c0 a8 fe 0a 3d 3d  .49.@... ..==
0020  30 23 0e 01 00 50 79 9b 66 0d 00 00 00 80 02  0#...Py. f.....
0030  ff ff 55 06 00 00 02 04 05 b4 01 03 03 05 01 01  ..U.....
0040  04 02  ..

```

畫面中就只剩下我們需要的遠通電收網站連線的資料
但是這樣零散的資料看不懂對不對

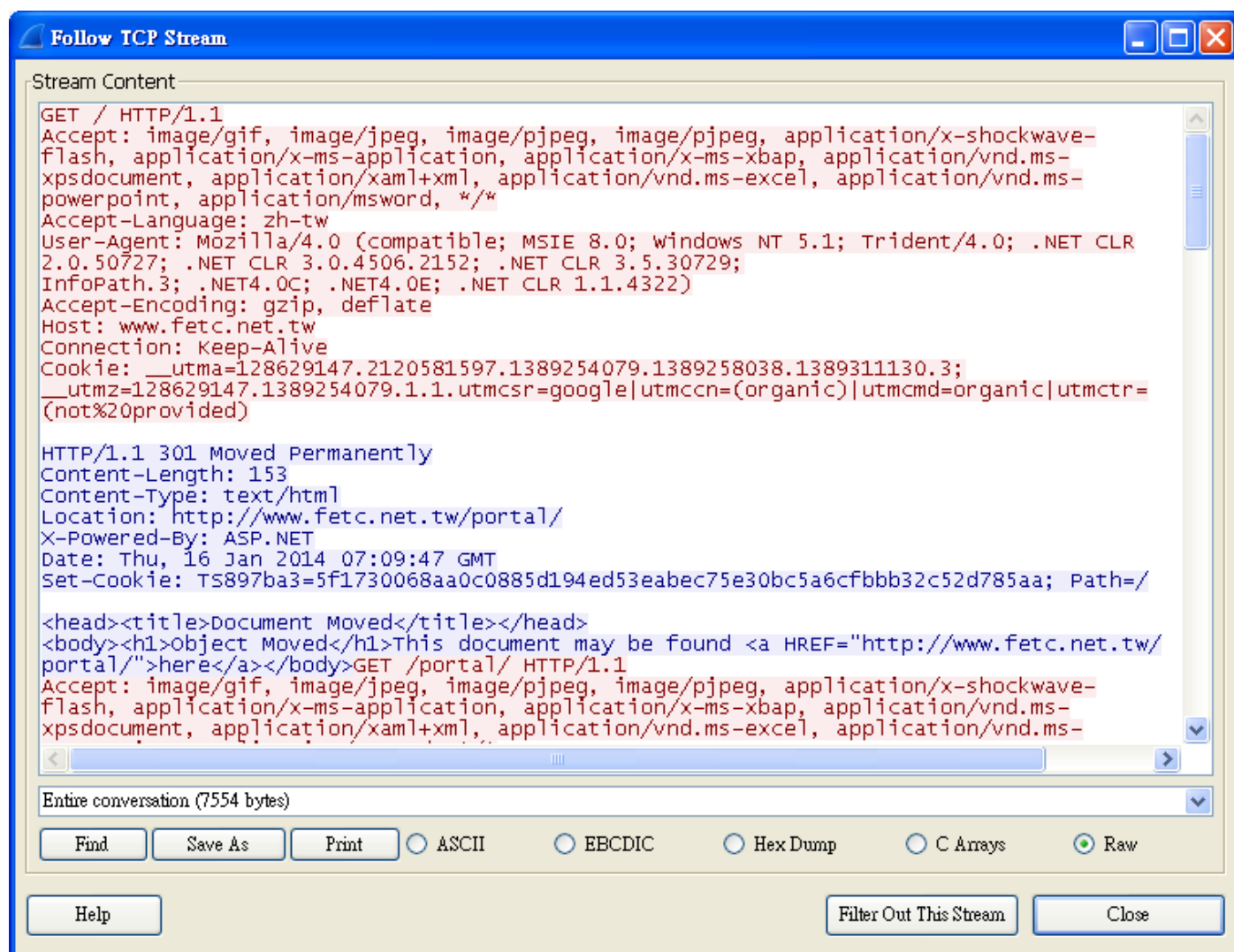


在第一個包按滑鼠右鍵

可以看見有一個選單

Follow TCP Stream

點一下



可以看見一些可以判讀的資料了
底下還有格式的控制