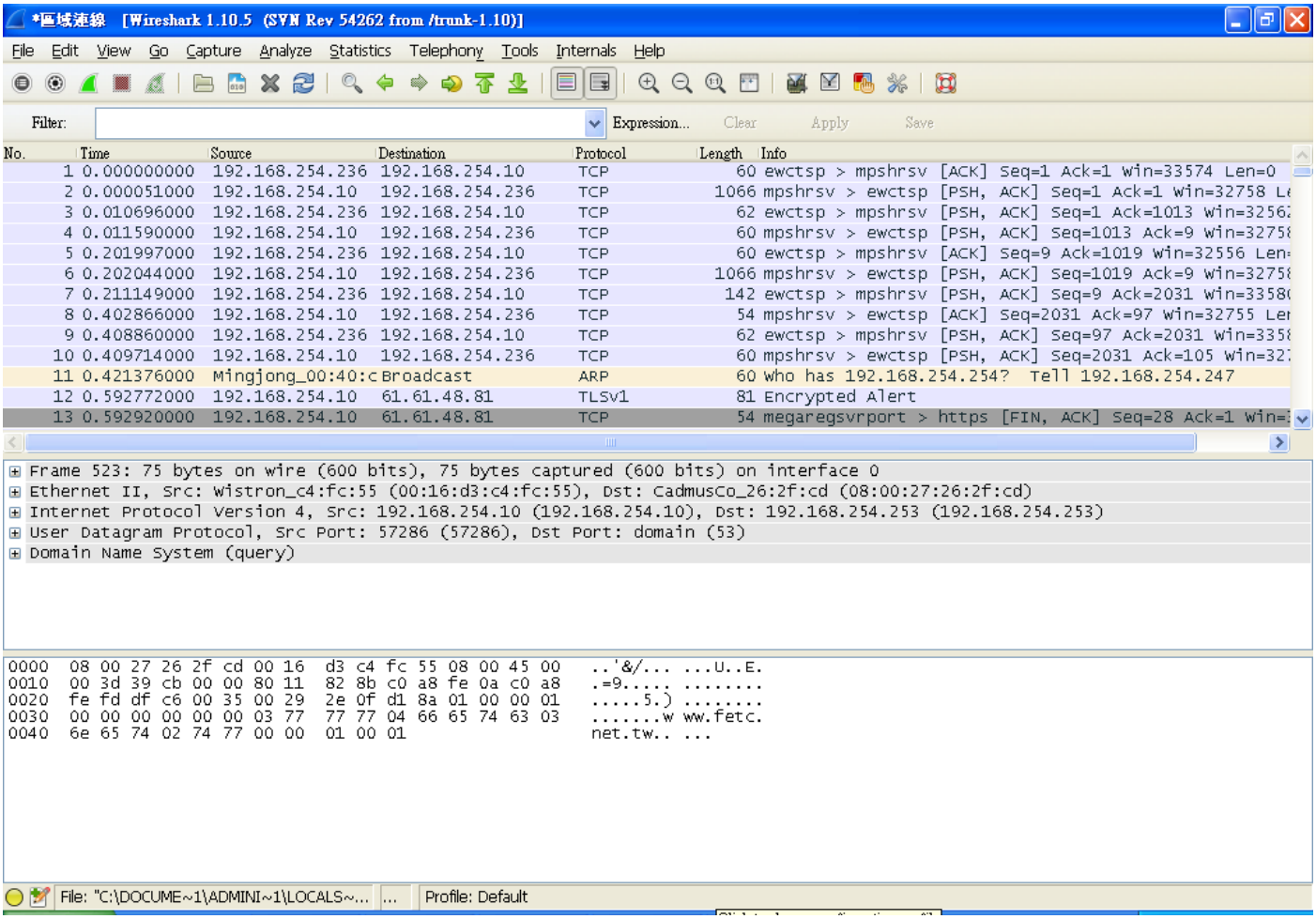
03 我們示範用 Wireshark 判讀近期最熱門的網站 eTag 遠通電收

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

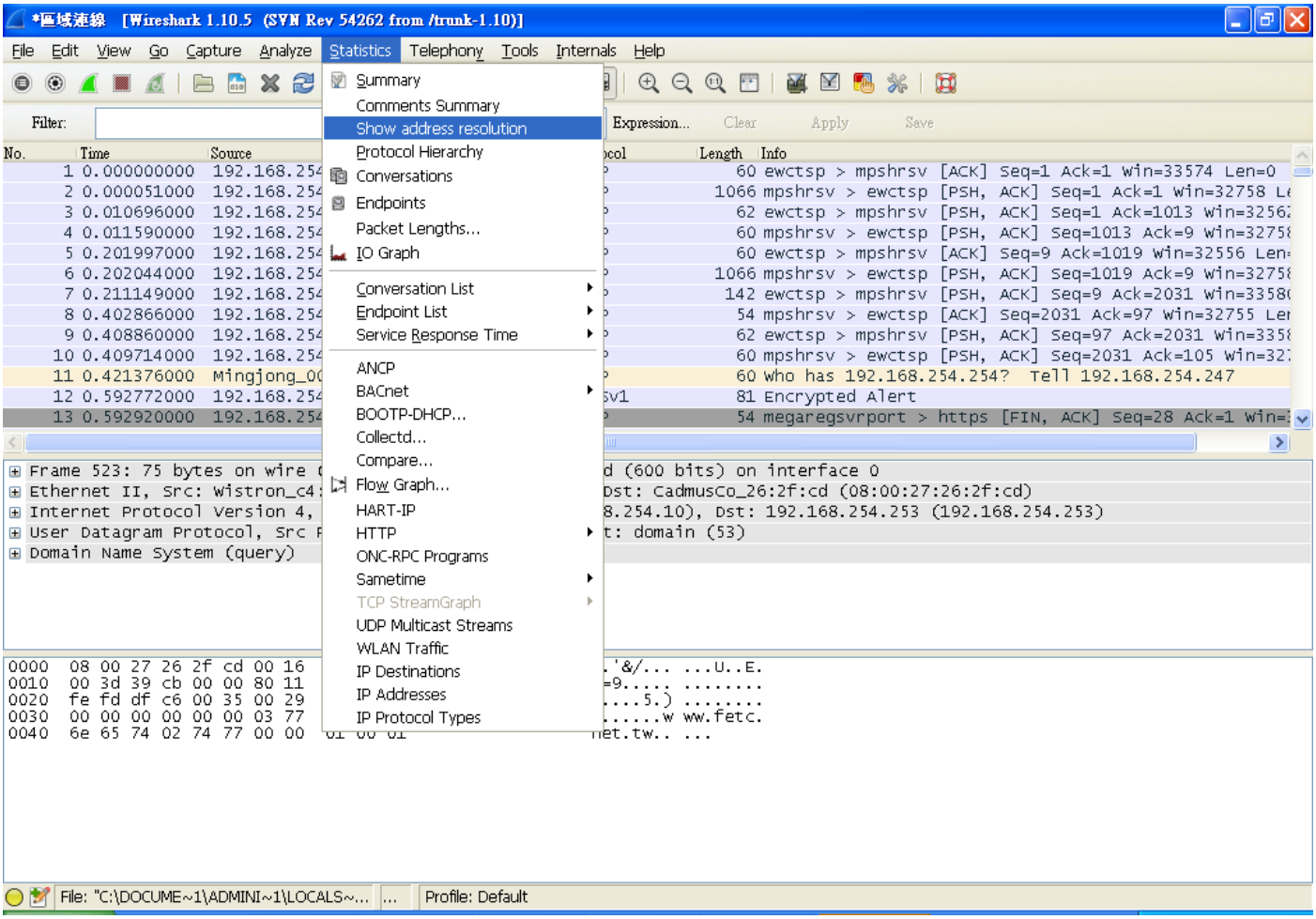
首先
開啓 Wireshark 開始抓封包
然後開啓遠通電收的網頁
http:// www.fetc.net.tw

之後點停止



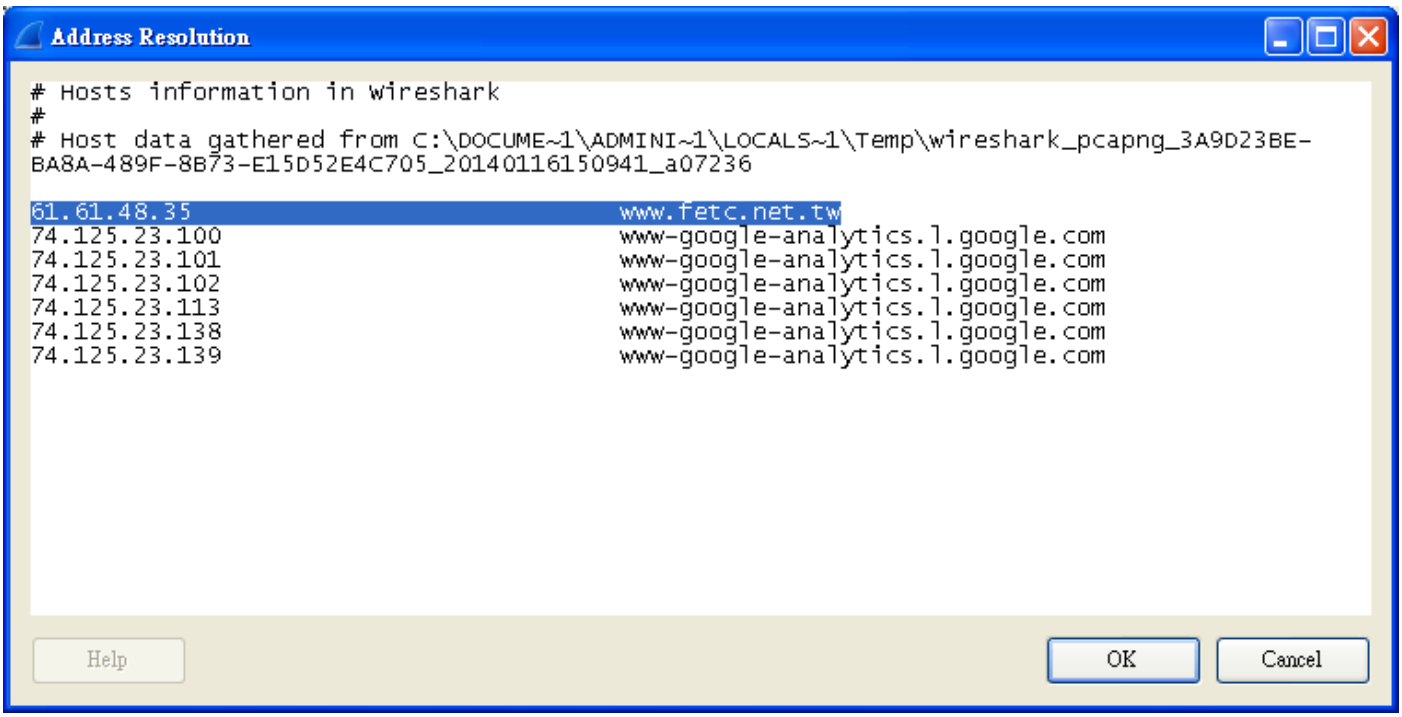
發現已經抓出一大堆的封包了

這個時候我們需要把遠通電收的 Domain 解出 IP



點 Statistics

Show address resolution

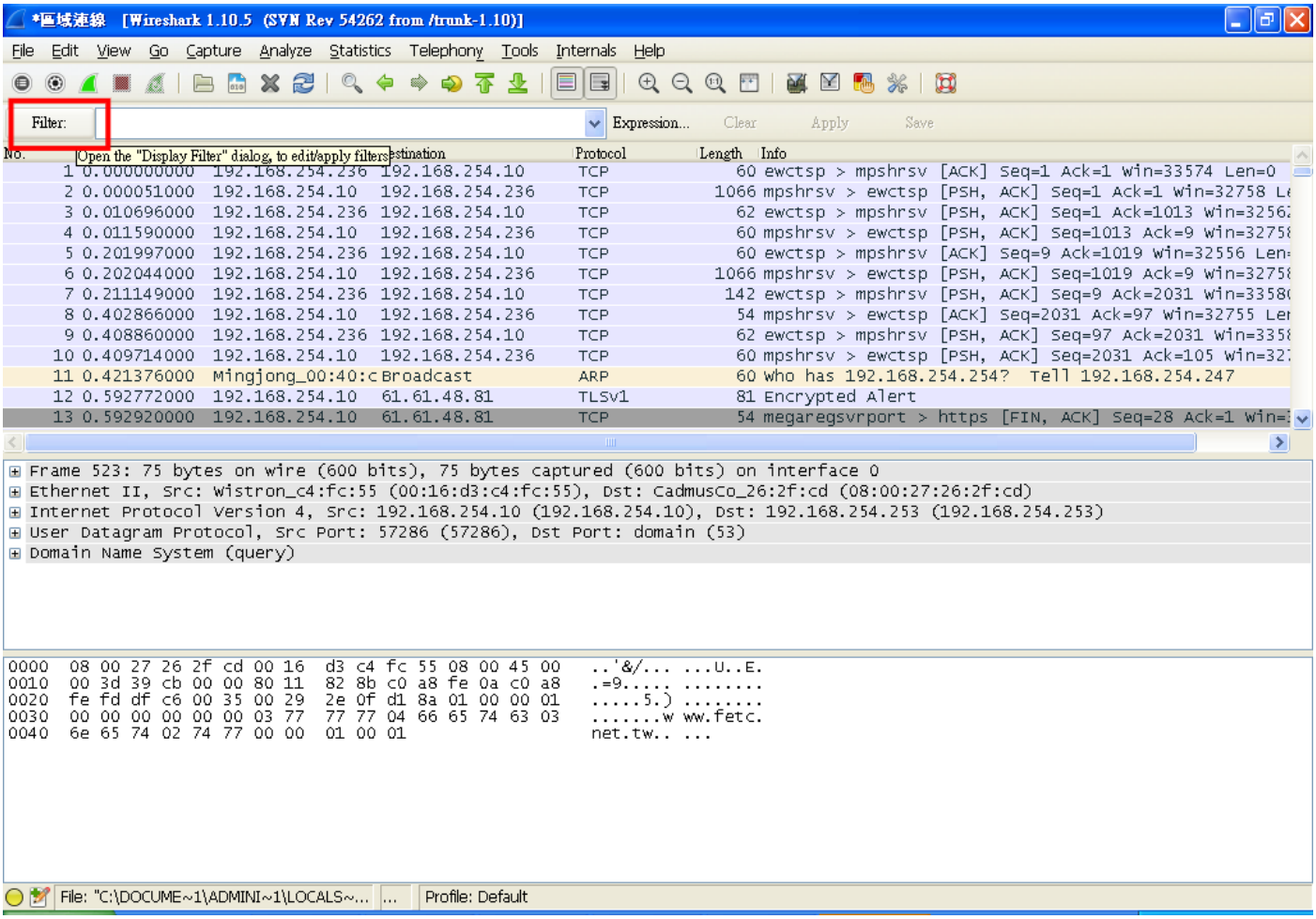


可以看見

我們連 www.fetc.net.tw 是連到 61.61.48.35

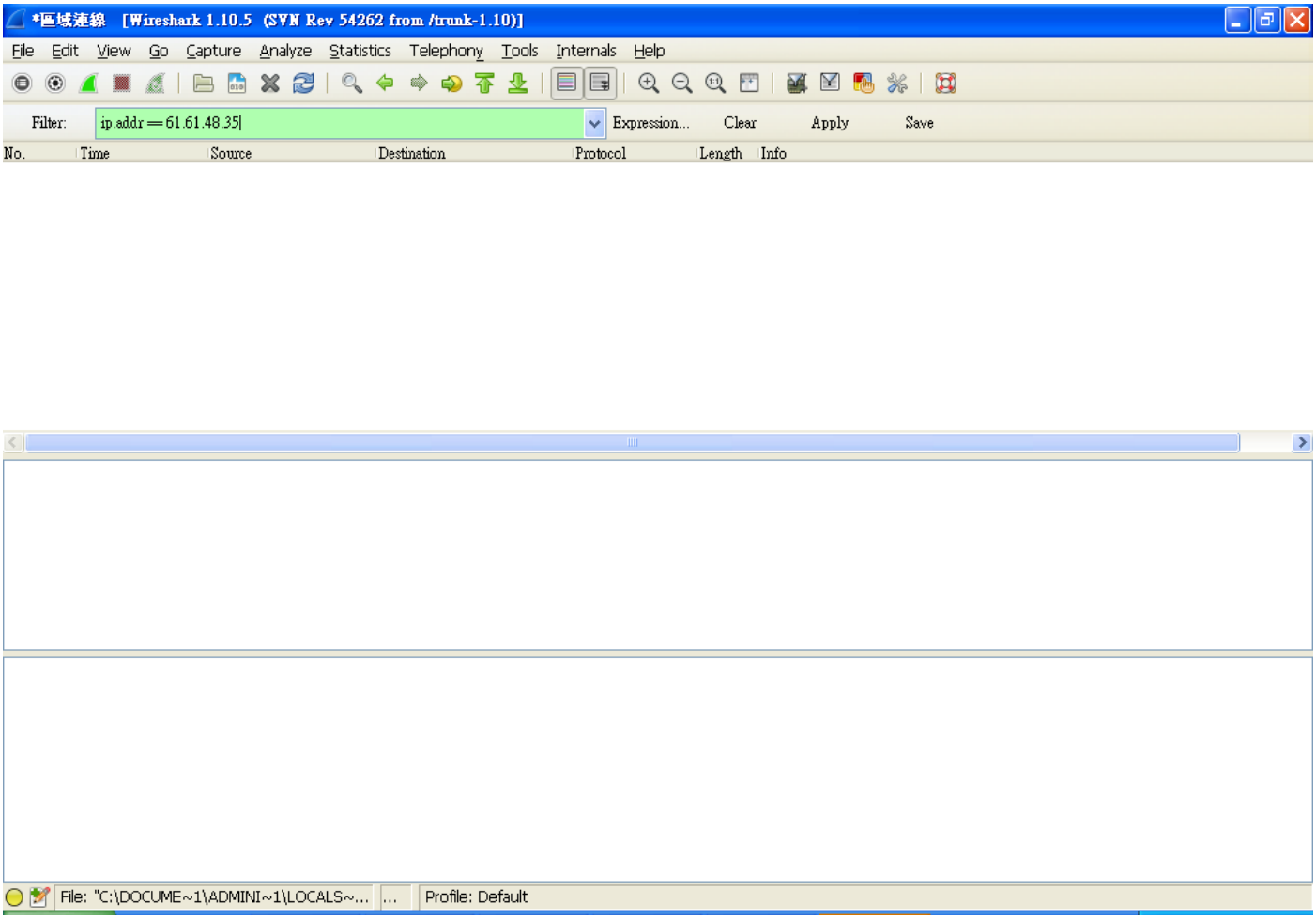
因爲剛 Capture 封包我們是全抓

所以我們得下 Filter 過濾掉其他的 IP



所以在 Filetr 這邊先找 Sample

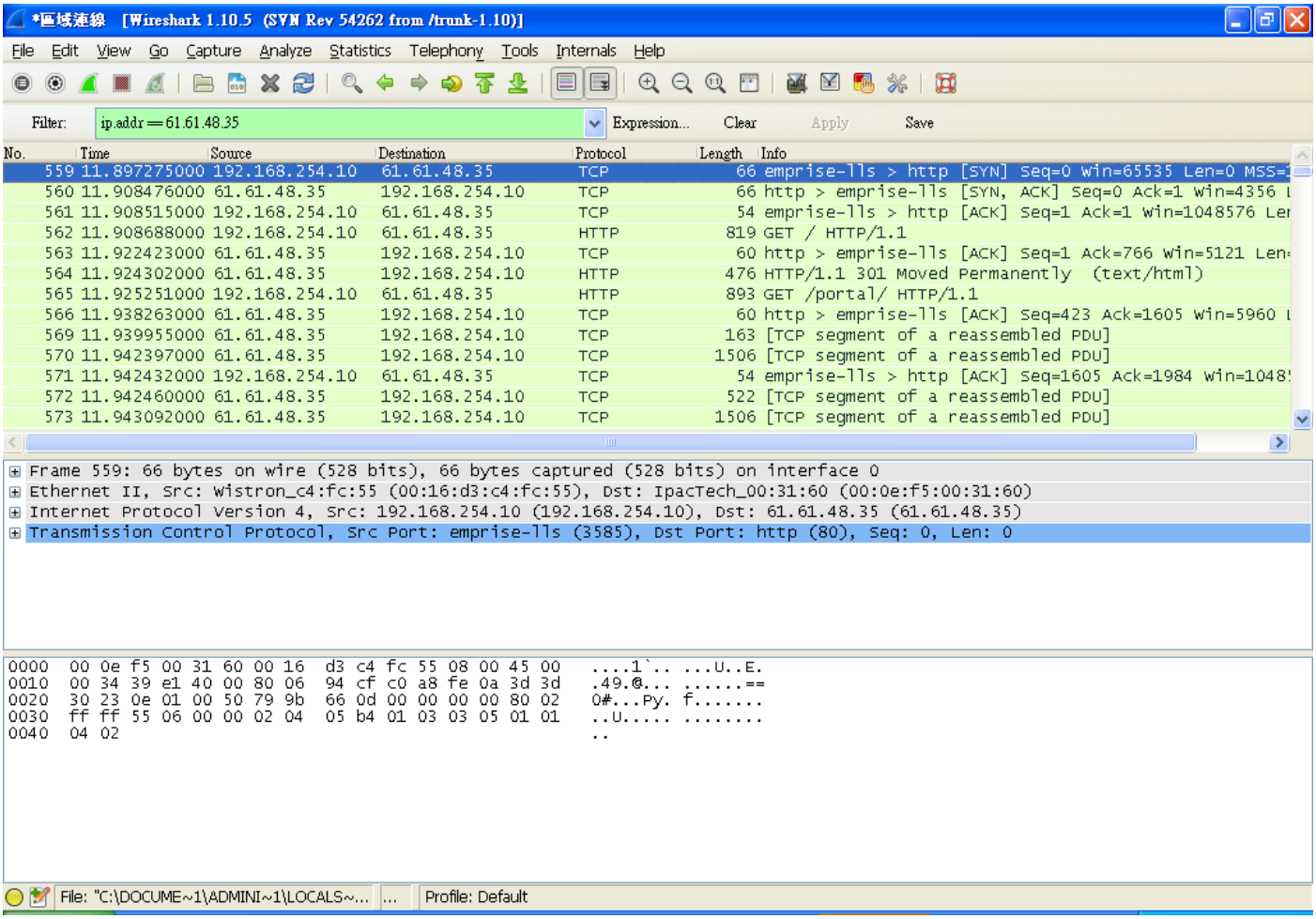
Ip address ….



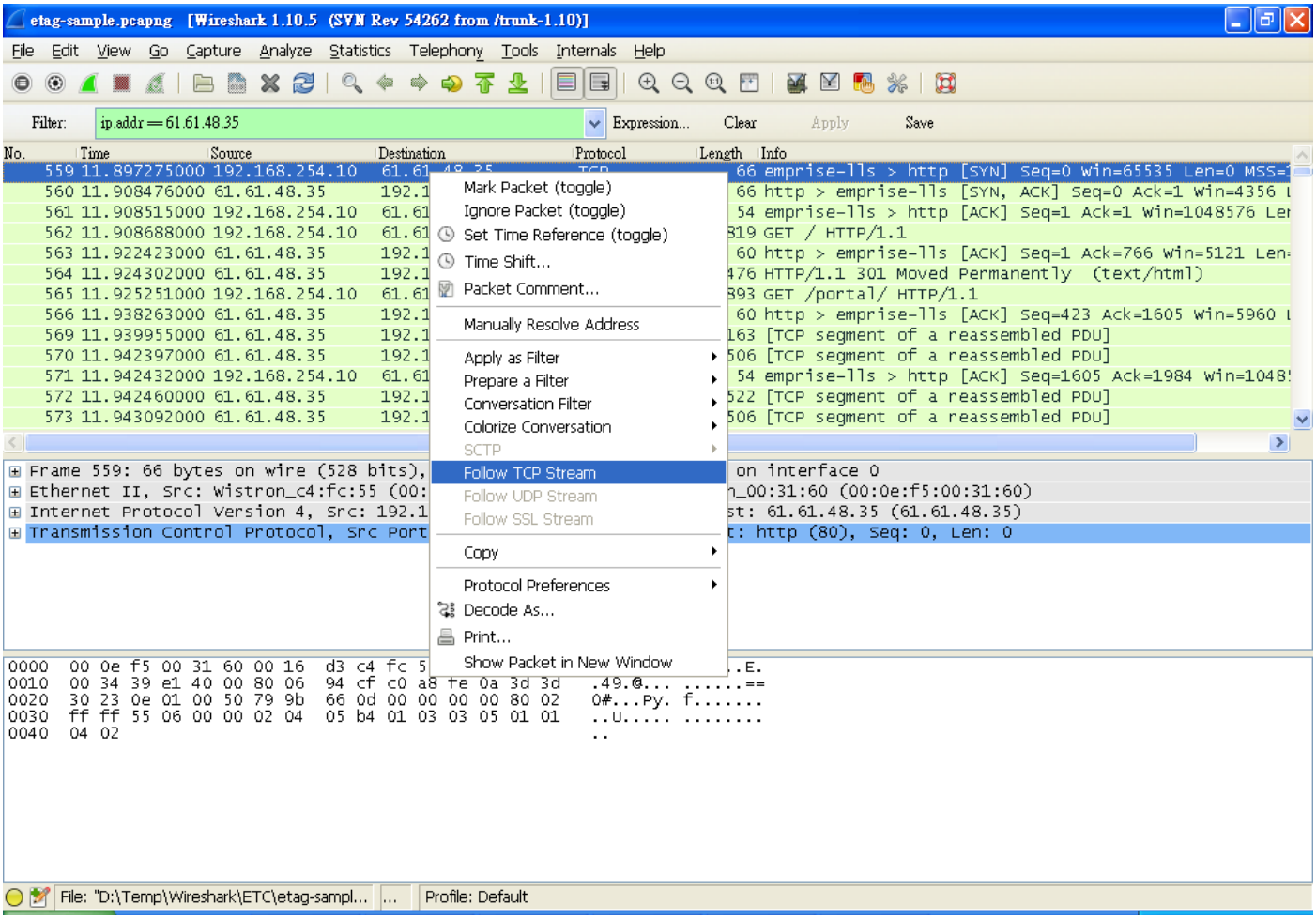
改成我們要的

ip.addr == 61.61.48.35

再點 Apply 之後



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

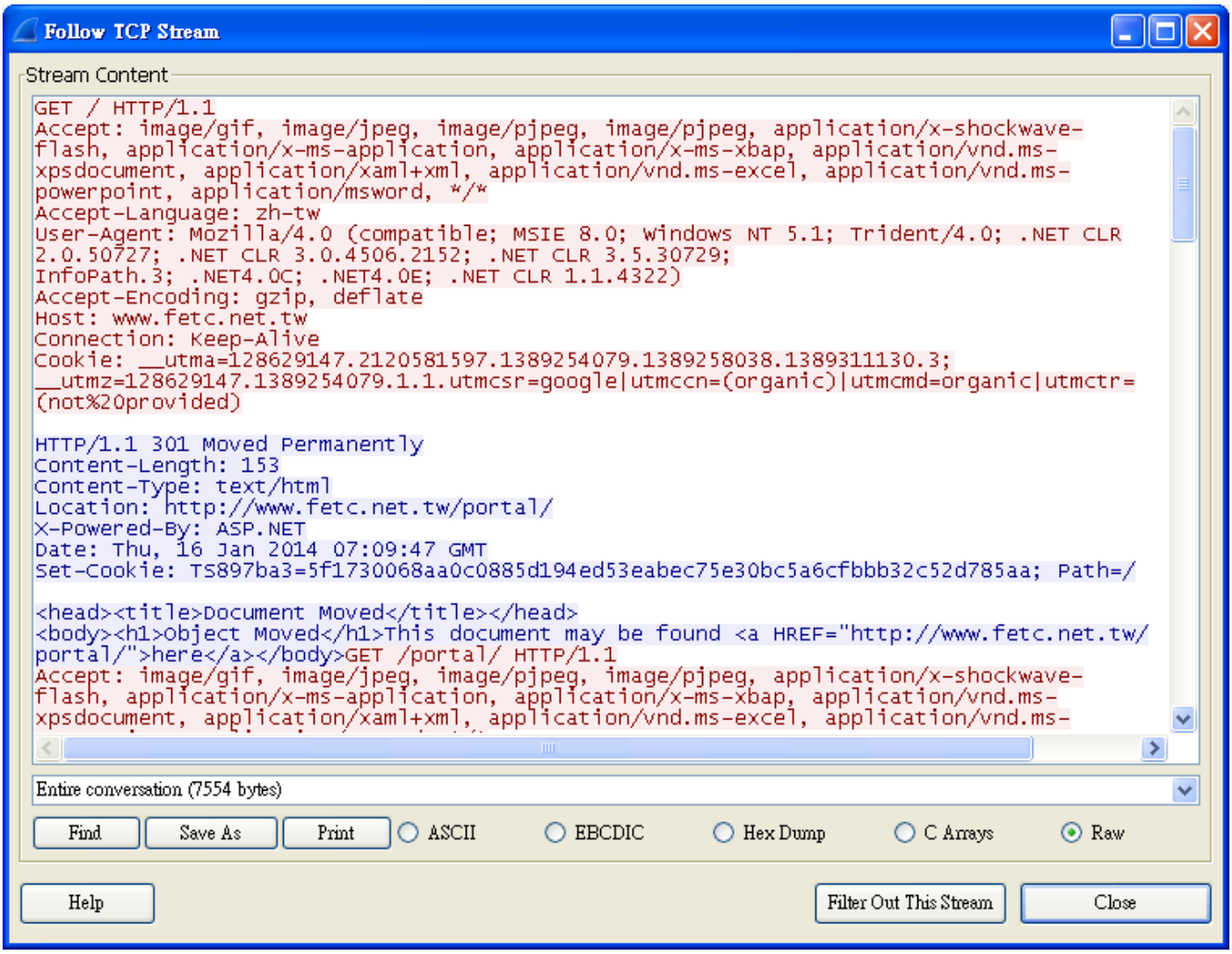


在第一個包按滑鼠右鍵

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