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

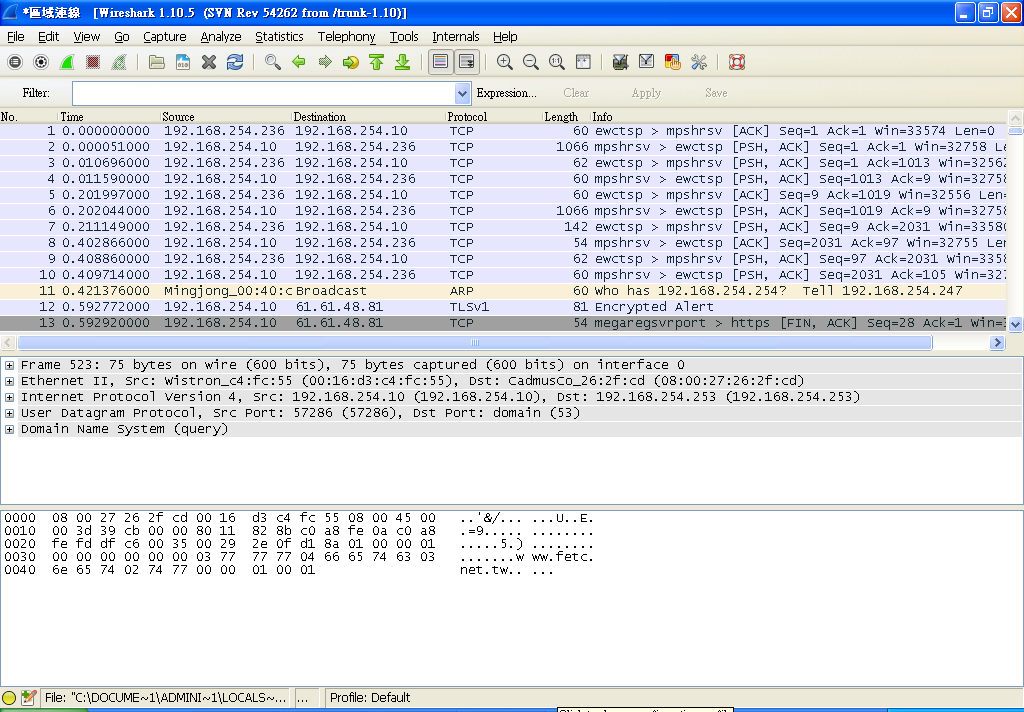
開啟Wireshark開始抓封包

然後開啟遠通電收的網頁

http:// www.fetc.net.tw

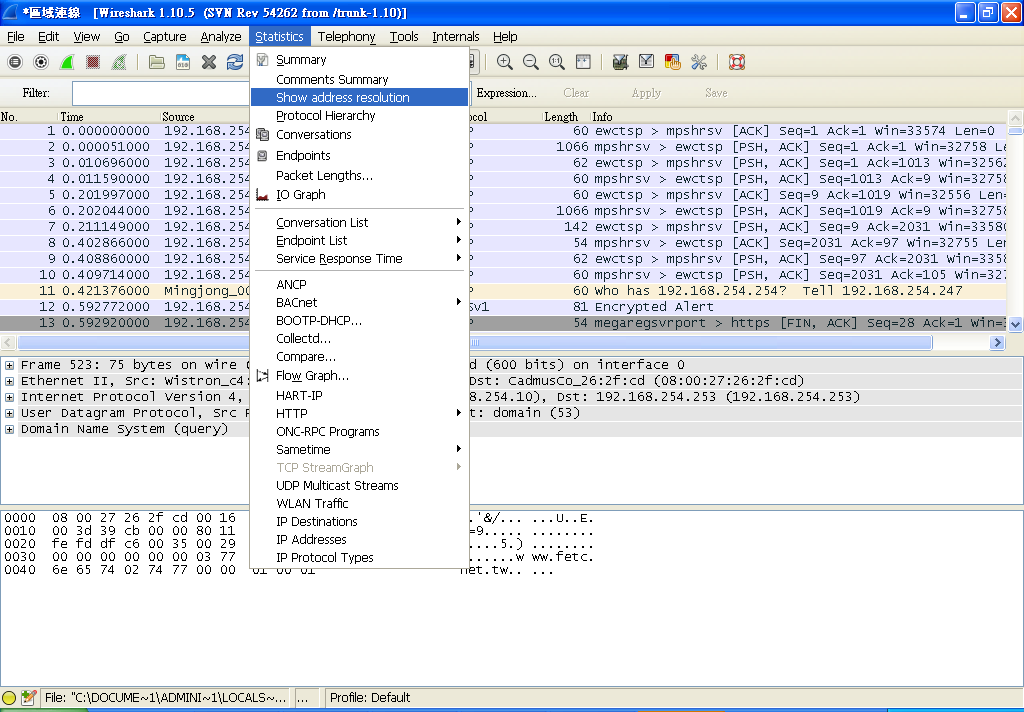


之後點停止



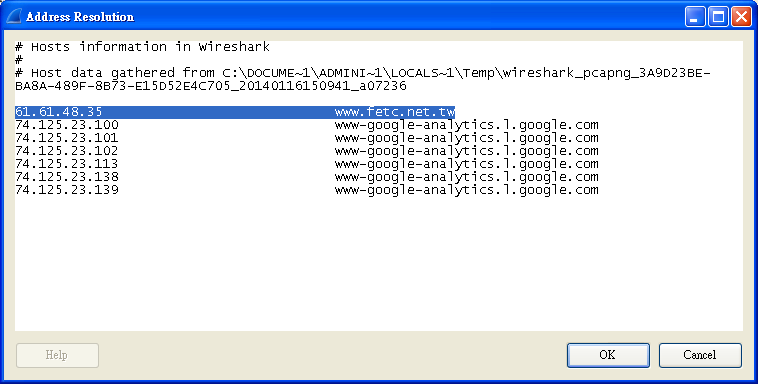
發現已經抓出一大堆的封包了

這個時候我們需要把遠通電收的Domain解出IP



點Statistics

Show address resolution

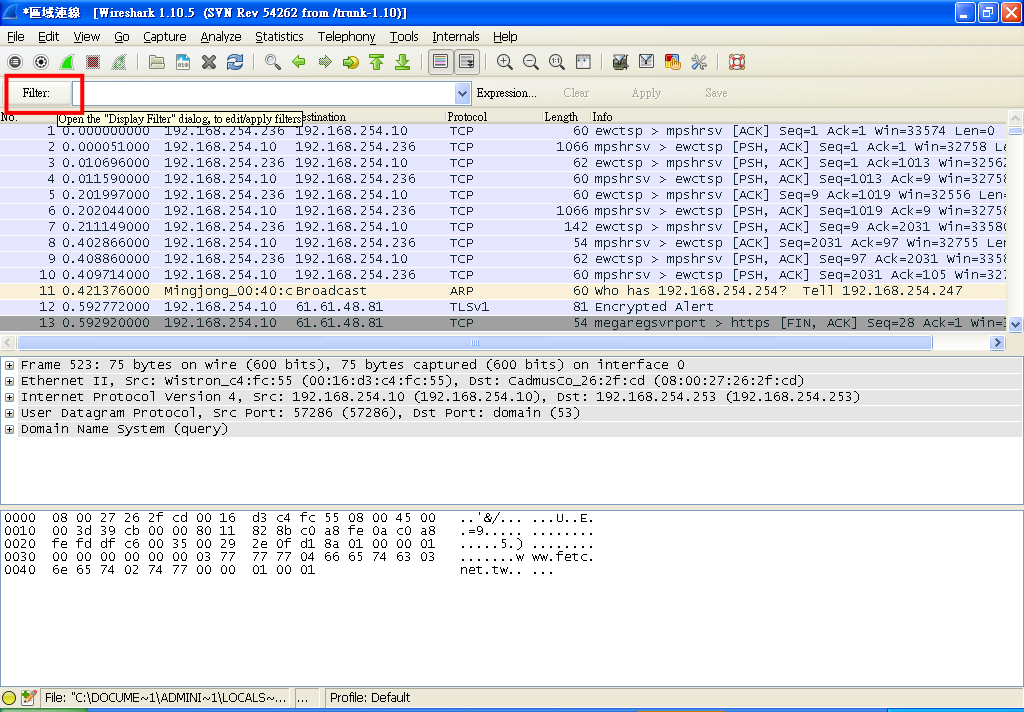


可以看見

我們連[www.fetc.net.tw是連到61.61.48.35](http://www.fetc.net.tw是連到61.61.48.35)

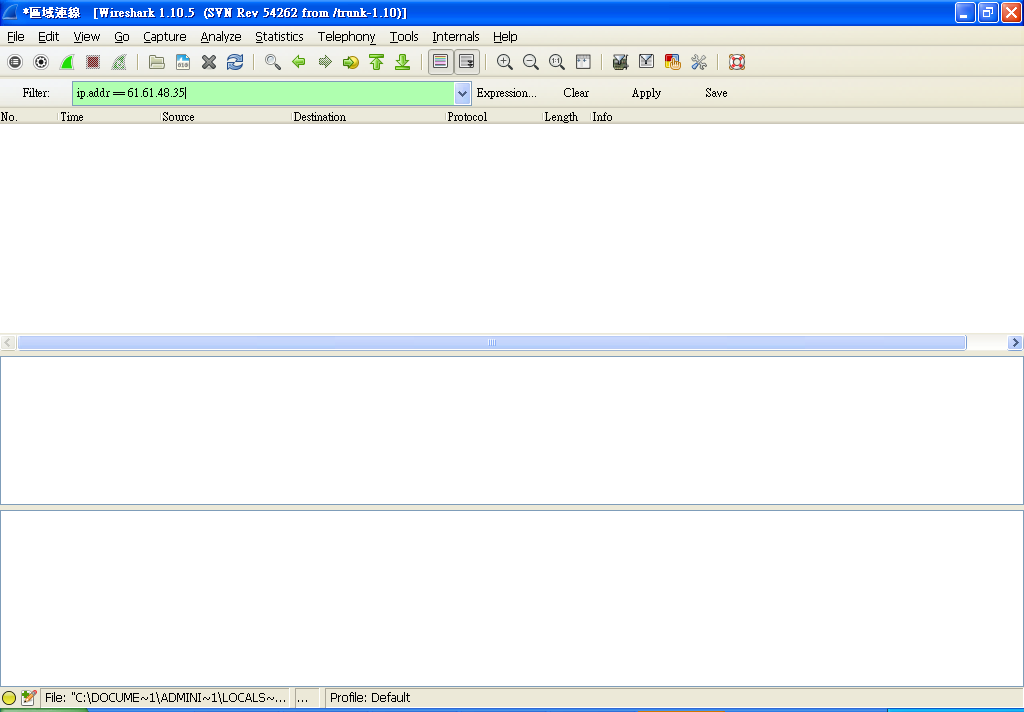
因為剛Capture封包我們是全抓

所以我們得下Filter過濾掉其他的IP



所以在Filetr這邊先找Sample

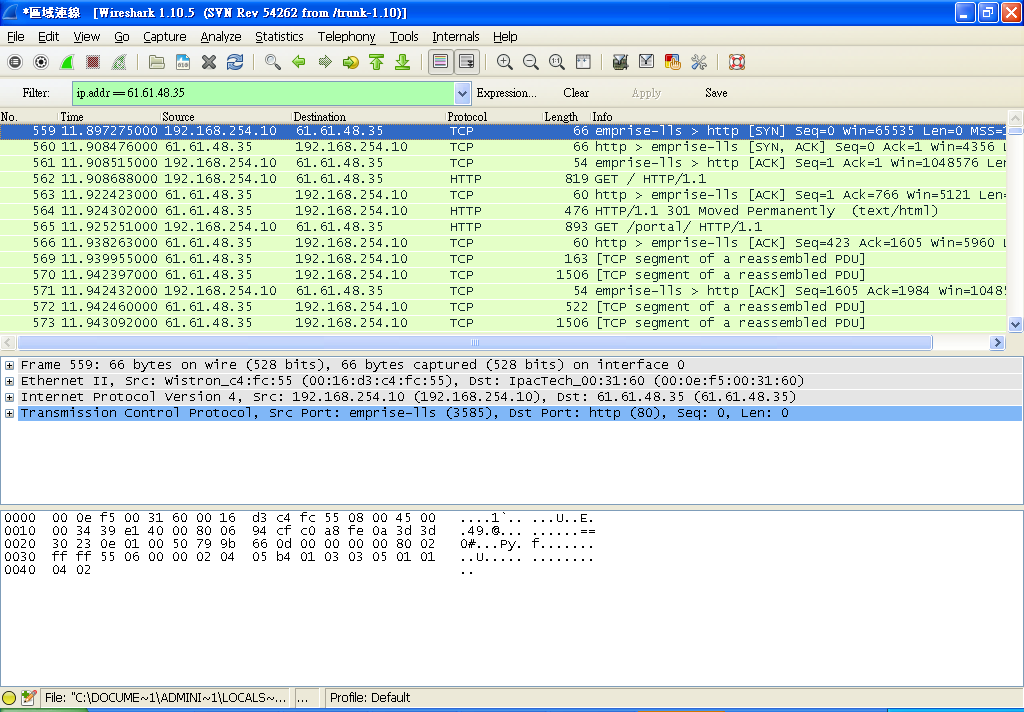
Ip address ….



改成我們要的

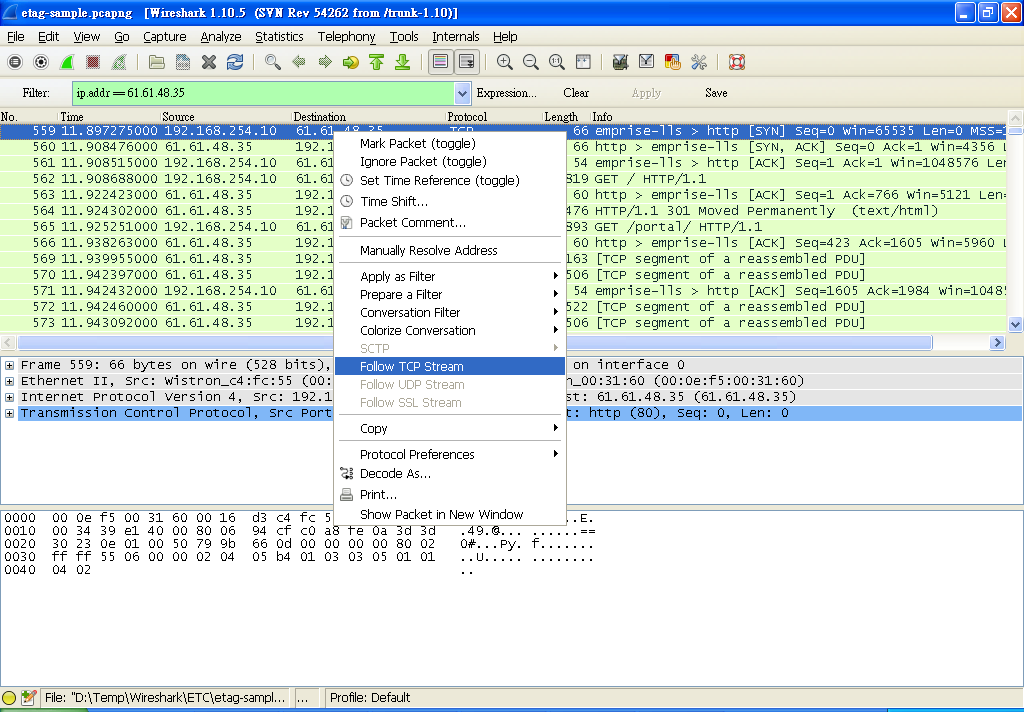
ip.addr == 61.61.48.35

再點Apply之後



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

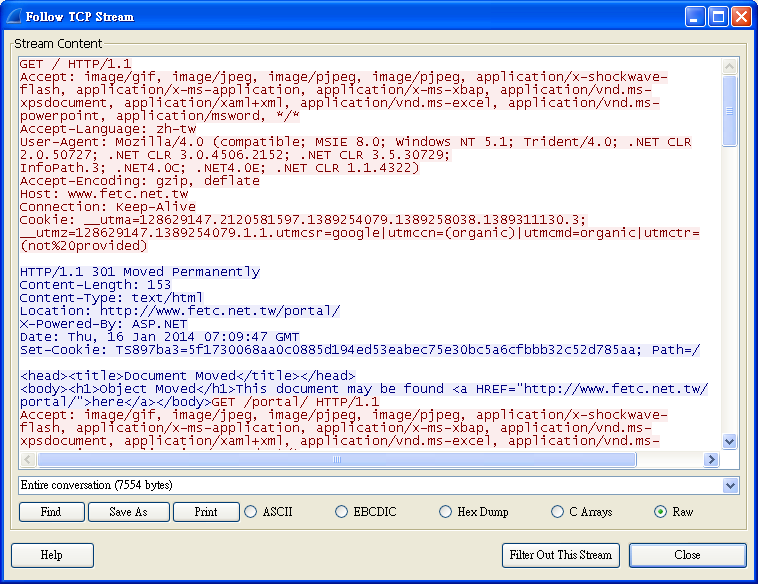


在第一個包按滑鼠右鍵

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