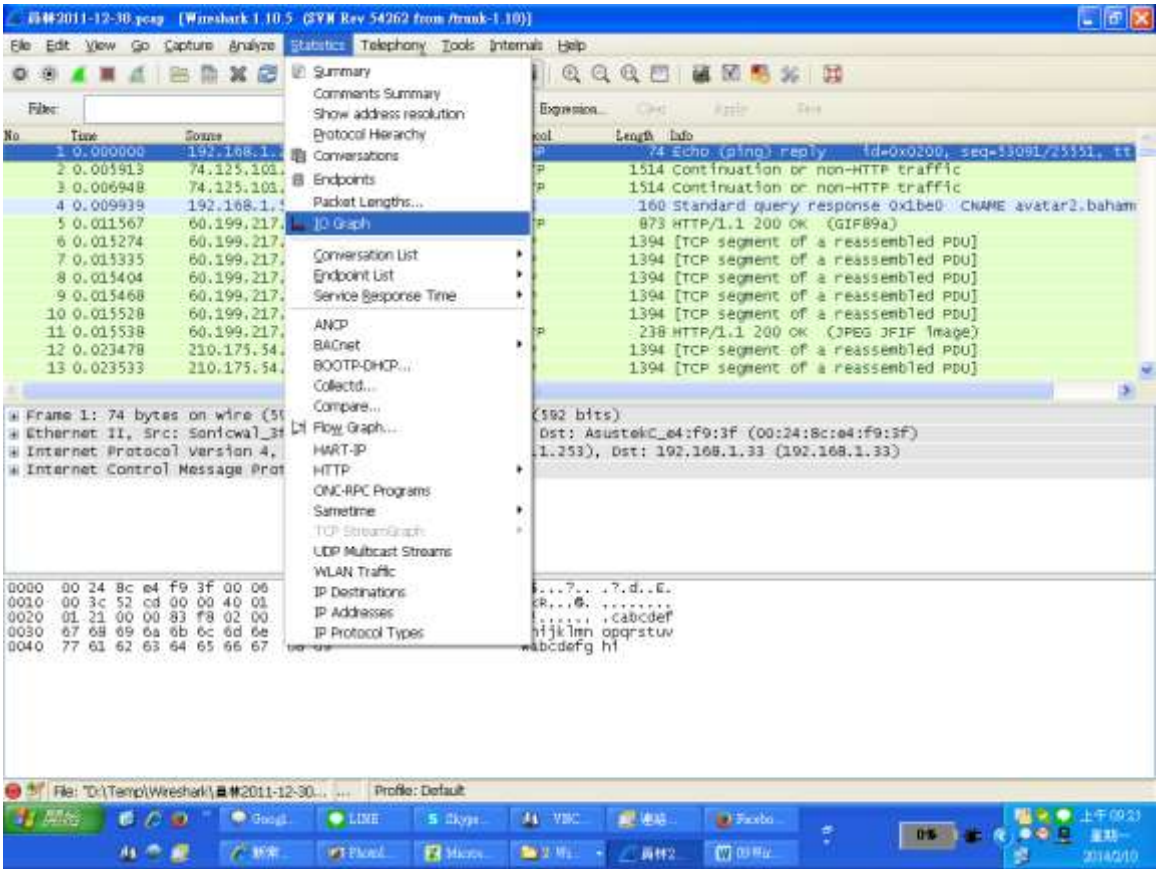
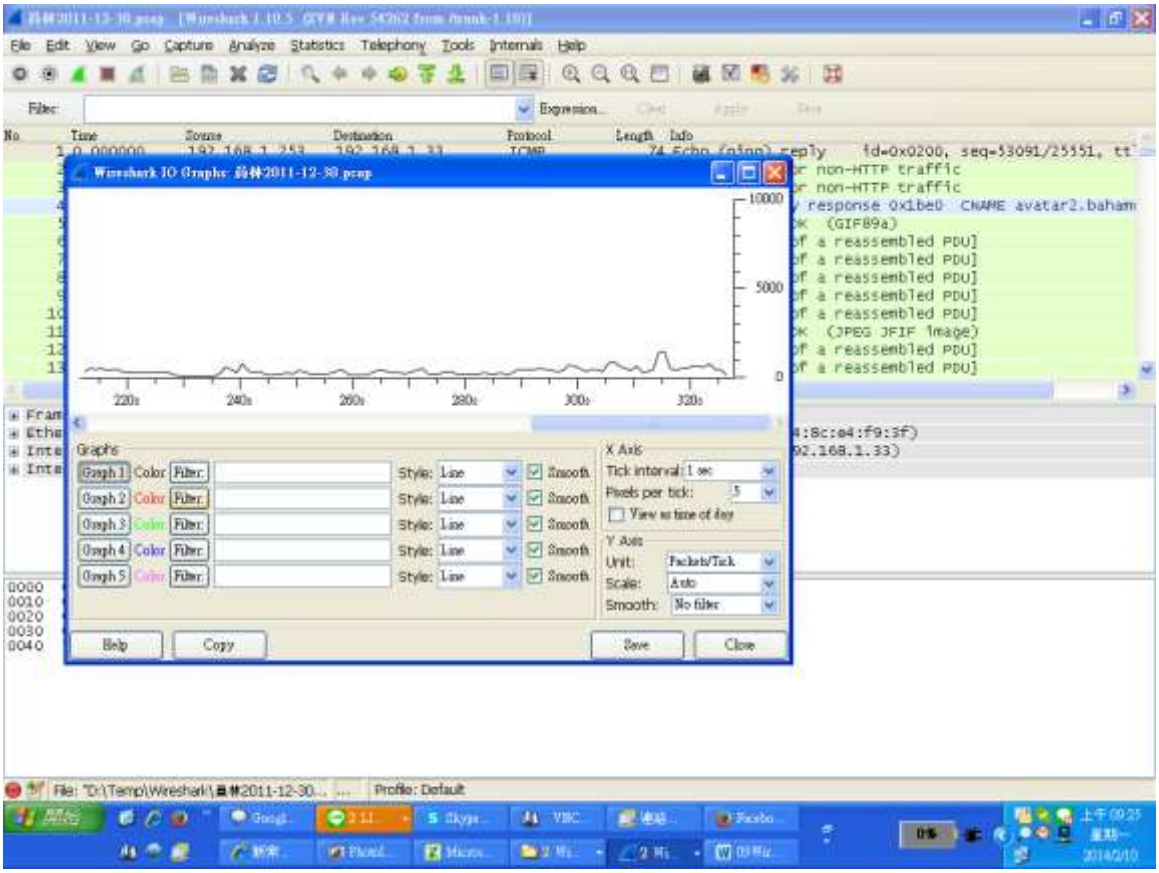
09 Wireshark 分析流量最高的那台電腦

有時候 MIS/IT 只是想找出佔流量最高的那台電腦
方法如下

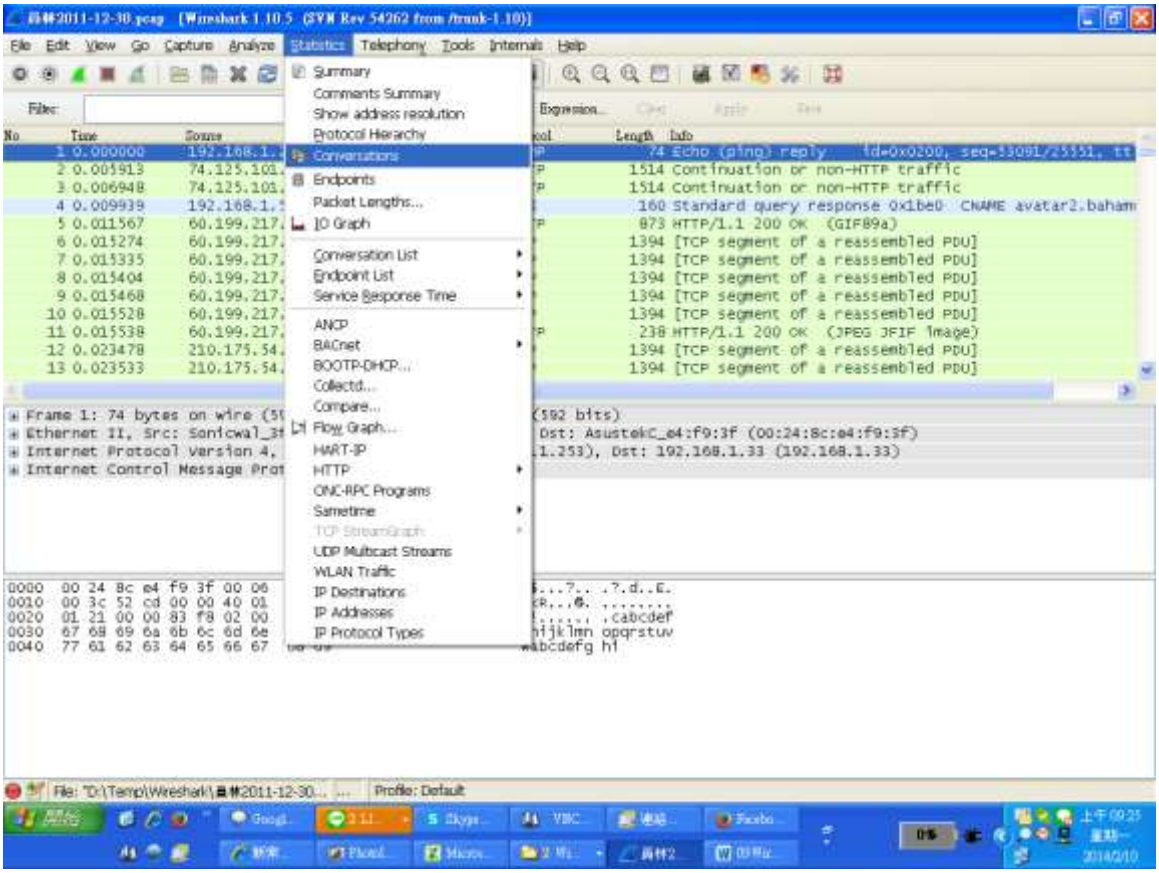
抓一段封包



先用 Statistics
IO Graph

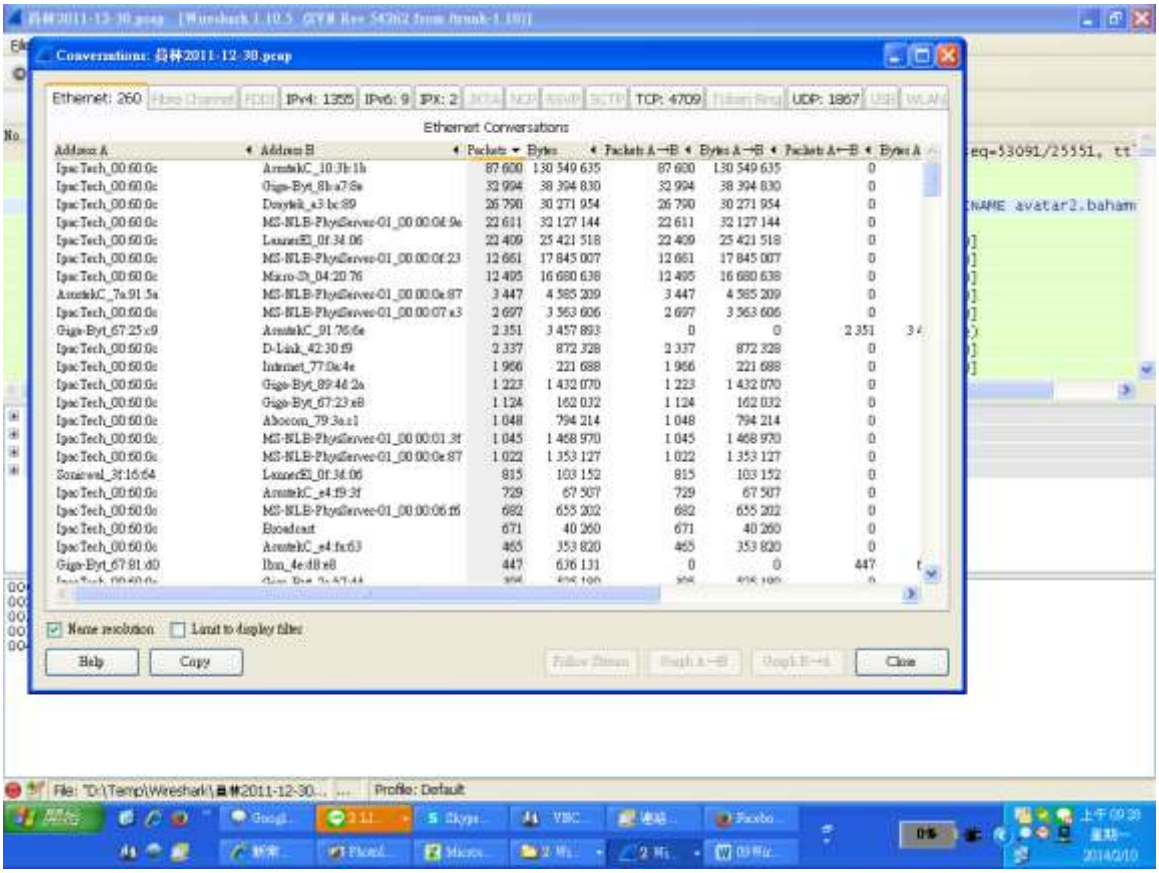


觀察流量最高的時間點



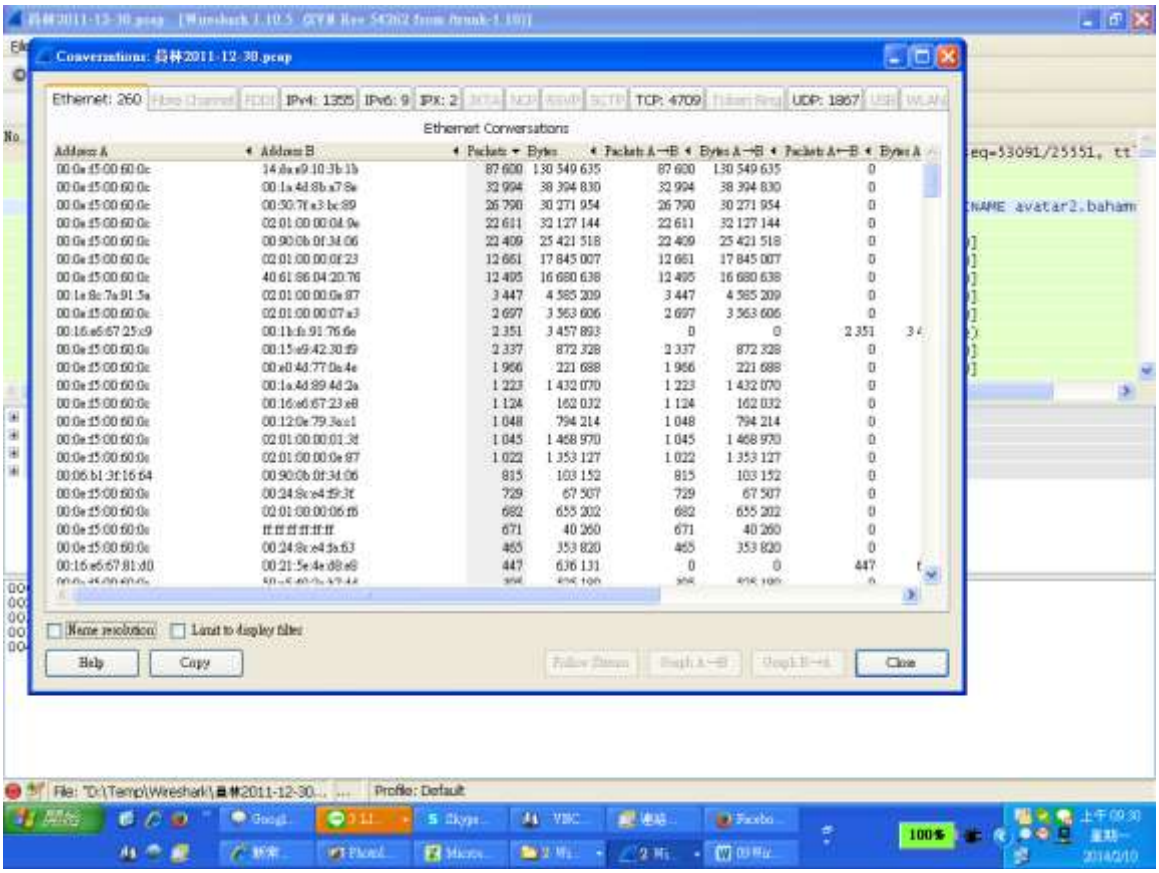
在 Statistics

Conversations



可以看出 Port 的統計

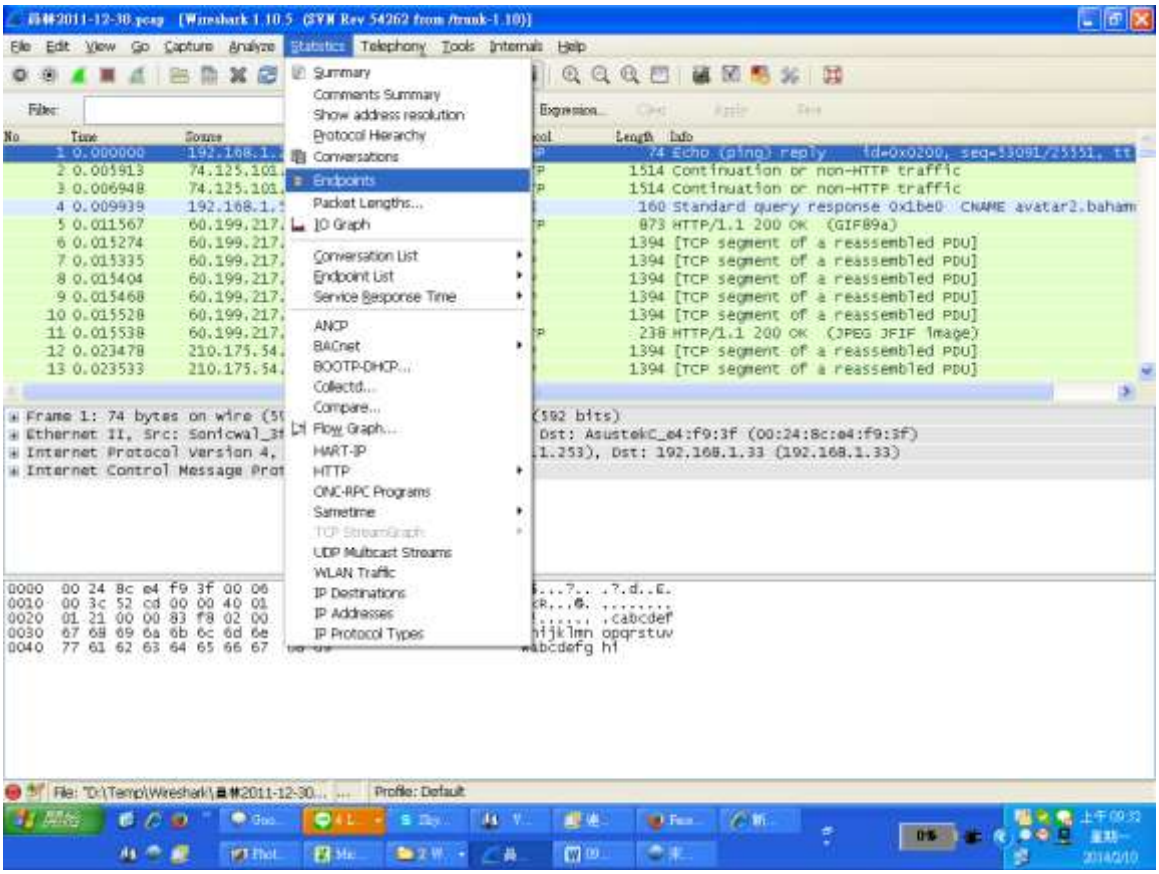
左下有一個 Name resolution 可以把製造公司名稱拿掉



變成純 MAC Address

這功能是分析 Port 的流量

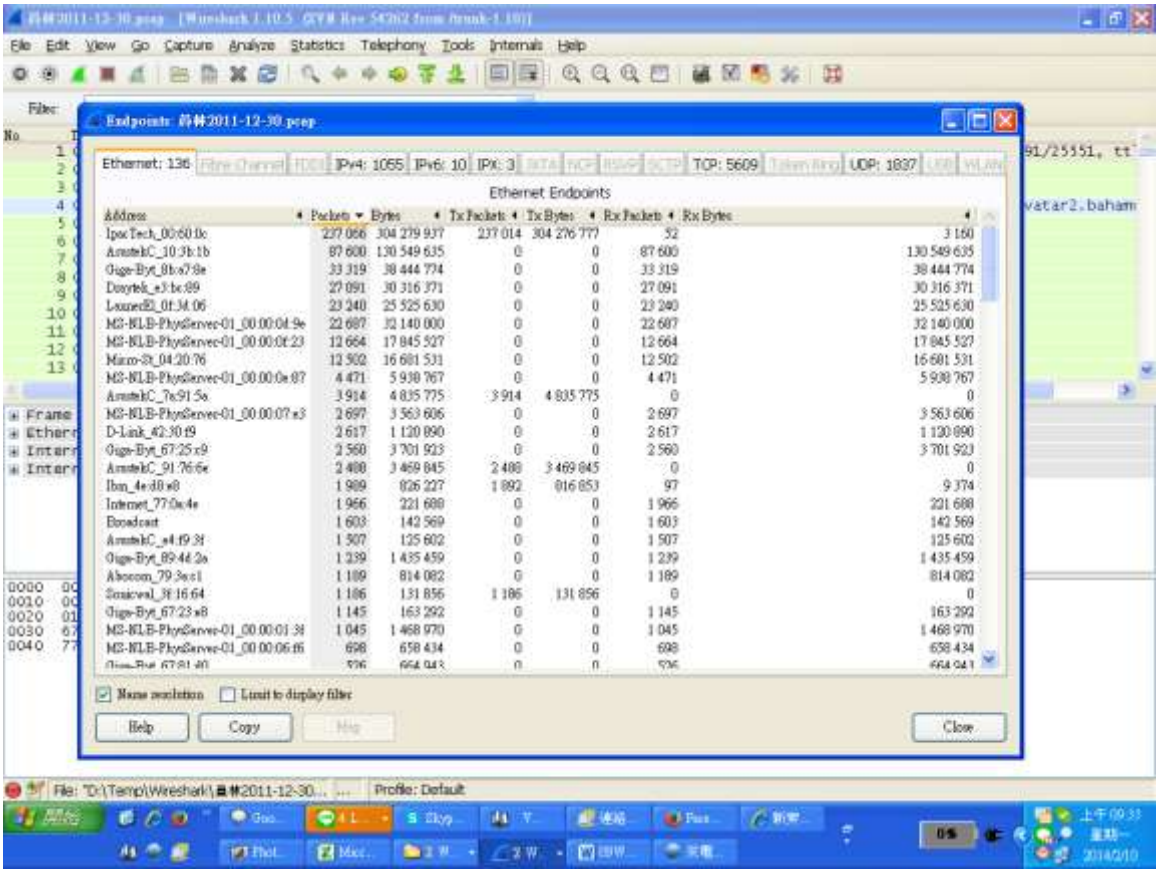
可以點排序



如果是要知道 IP 對 IP 的流量

要點 Statistics

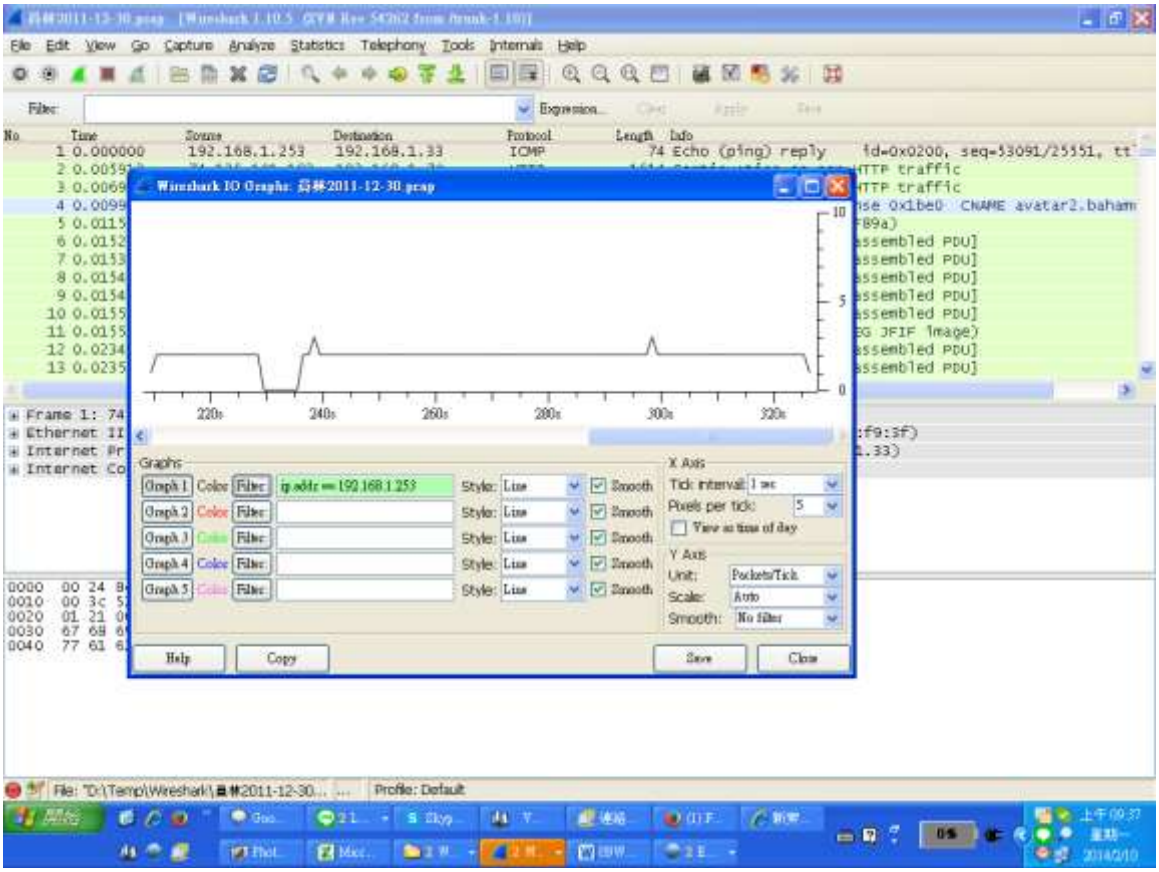
Endpoints



統計完之後再點

Packets 做排序

就可以回到剛剛的 IO Graph



做 Graph 1 的 Filter 的條件設定
就可以看出流量高的那台電腦的統計了