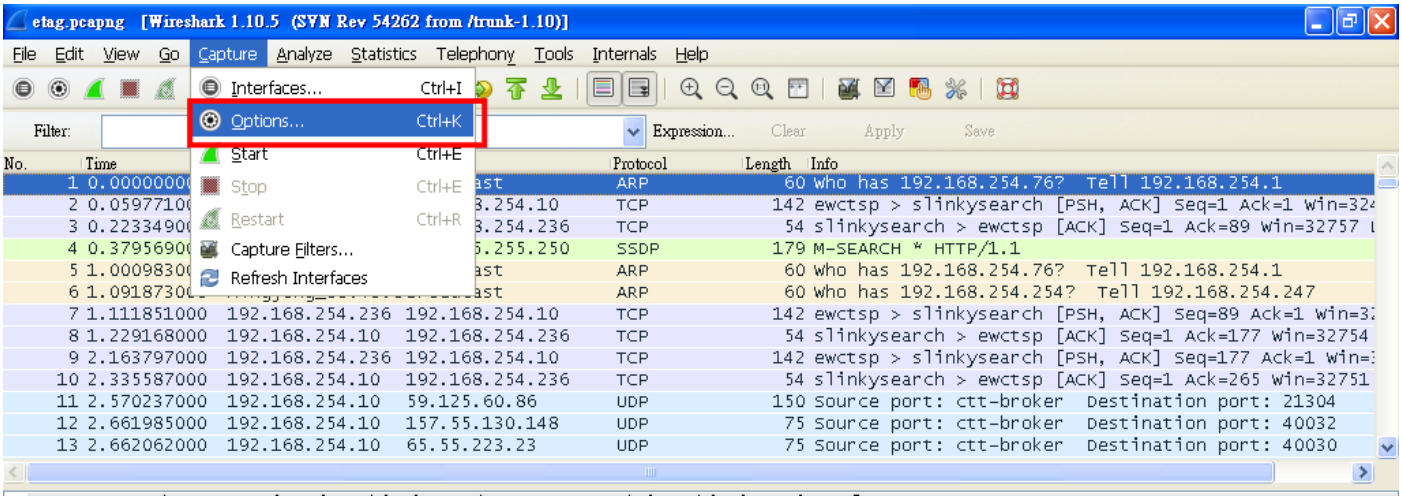
使用 Wireshark 抓特定 IP 或是 Port 的封包

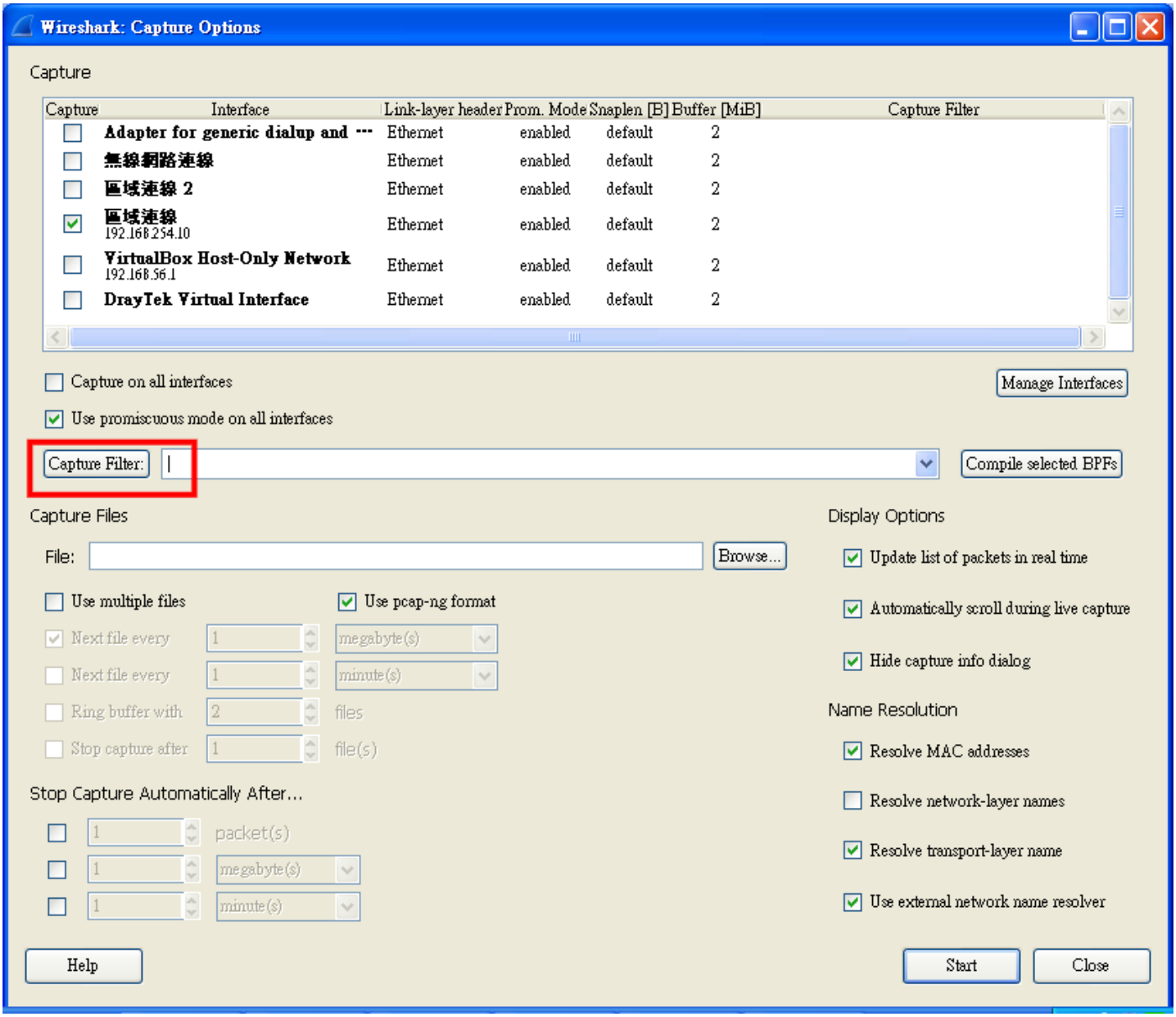
方法有兩種
一種是開始抓封包之前就先設定 Capture Filter

另外一種方式是全抓之後再做 Packet Filter

我們先講第一種

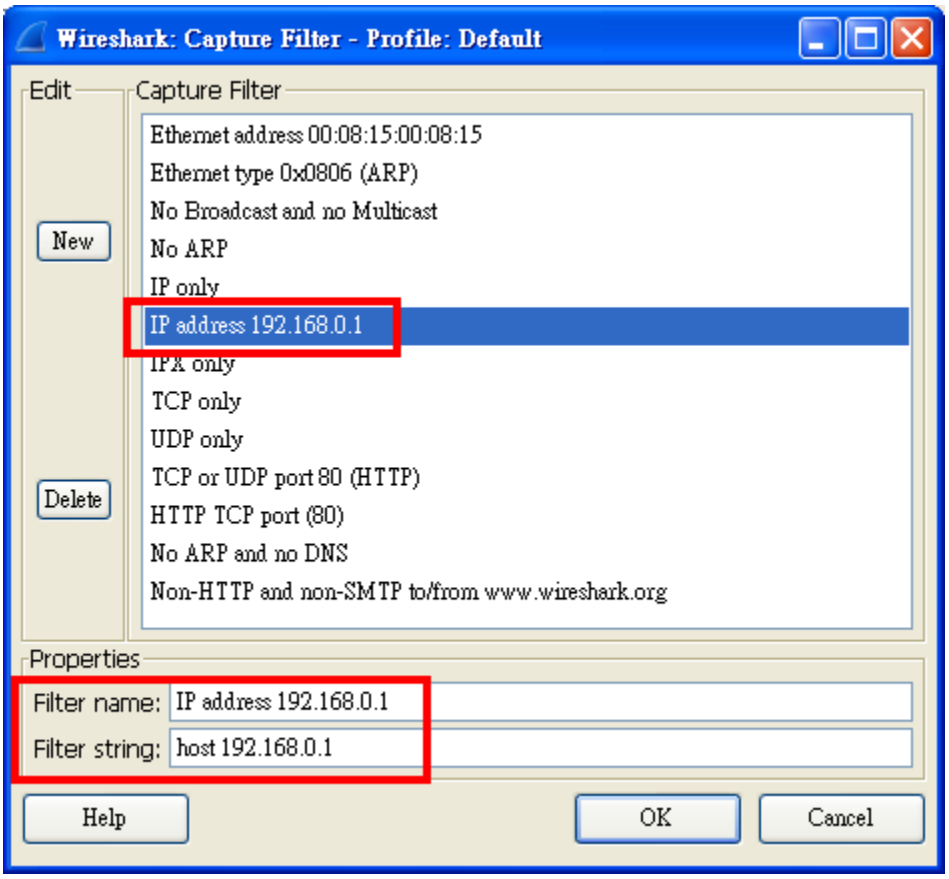


在 Capture
Option…點一下



跳出此視窗

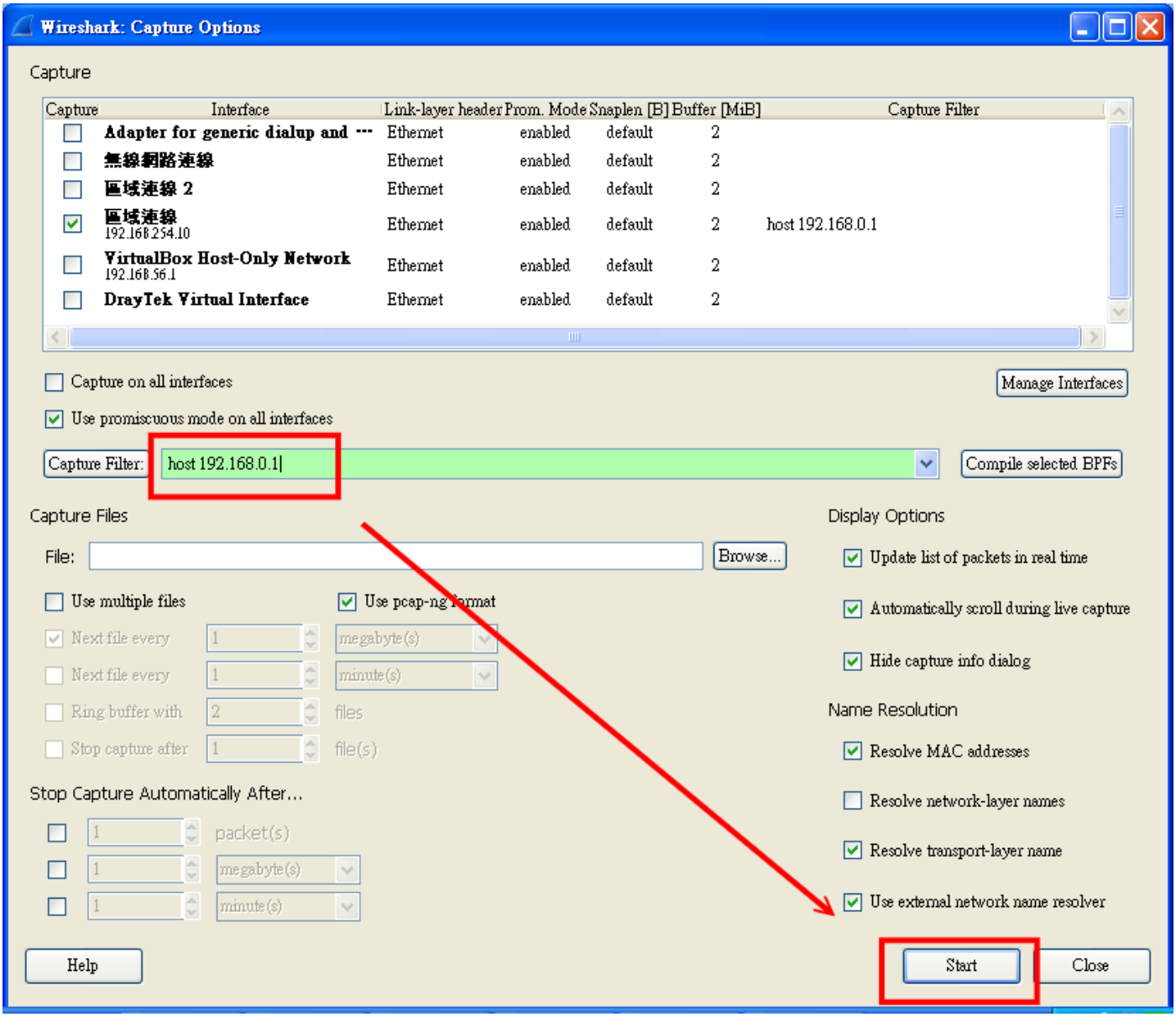
點一下 Capture Filter



出現範例

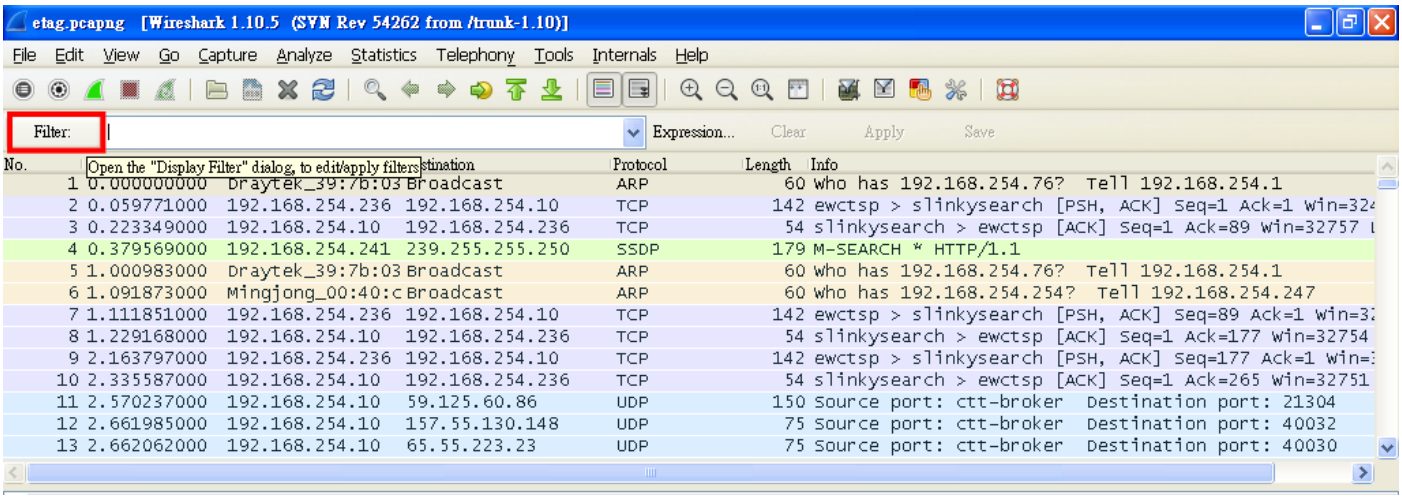
不管是 IP 或是特定的 Port 都可以指定

我們示範是 IP address 192.168.0.1



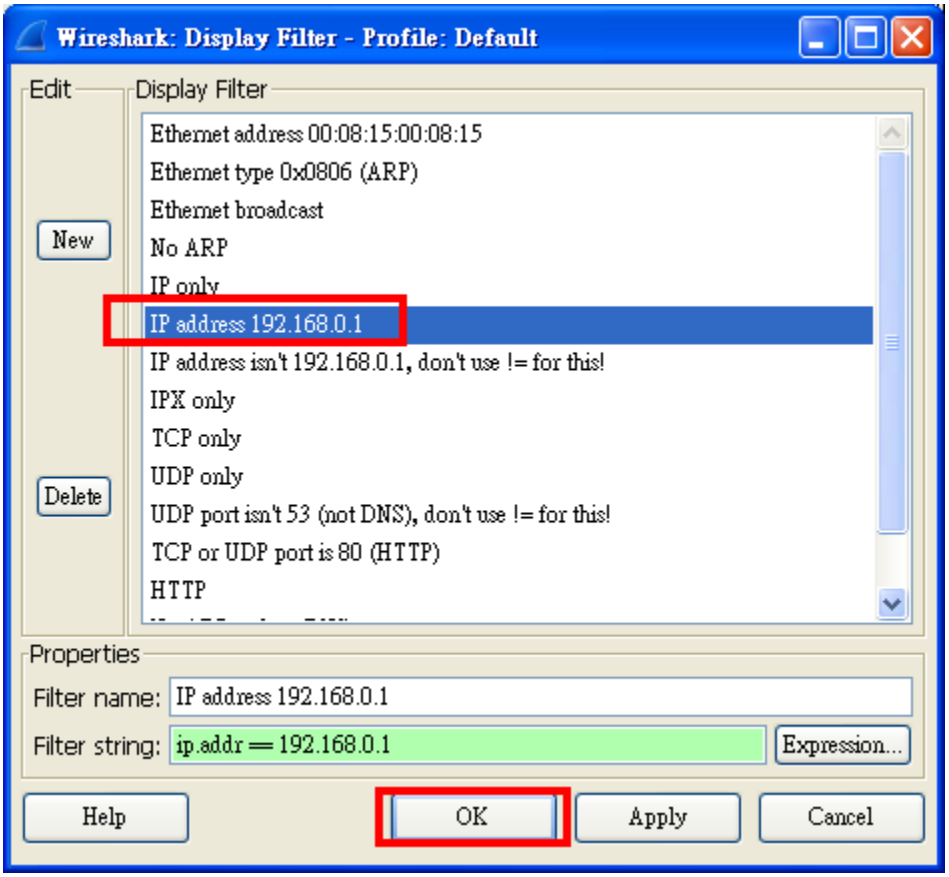
選進來之後
點 Start 就可以了

第二種方式是
已經抓好封包了
要過濾出特定的 IP 或是 Port



抓好之後

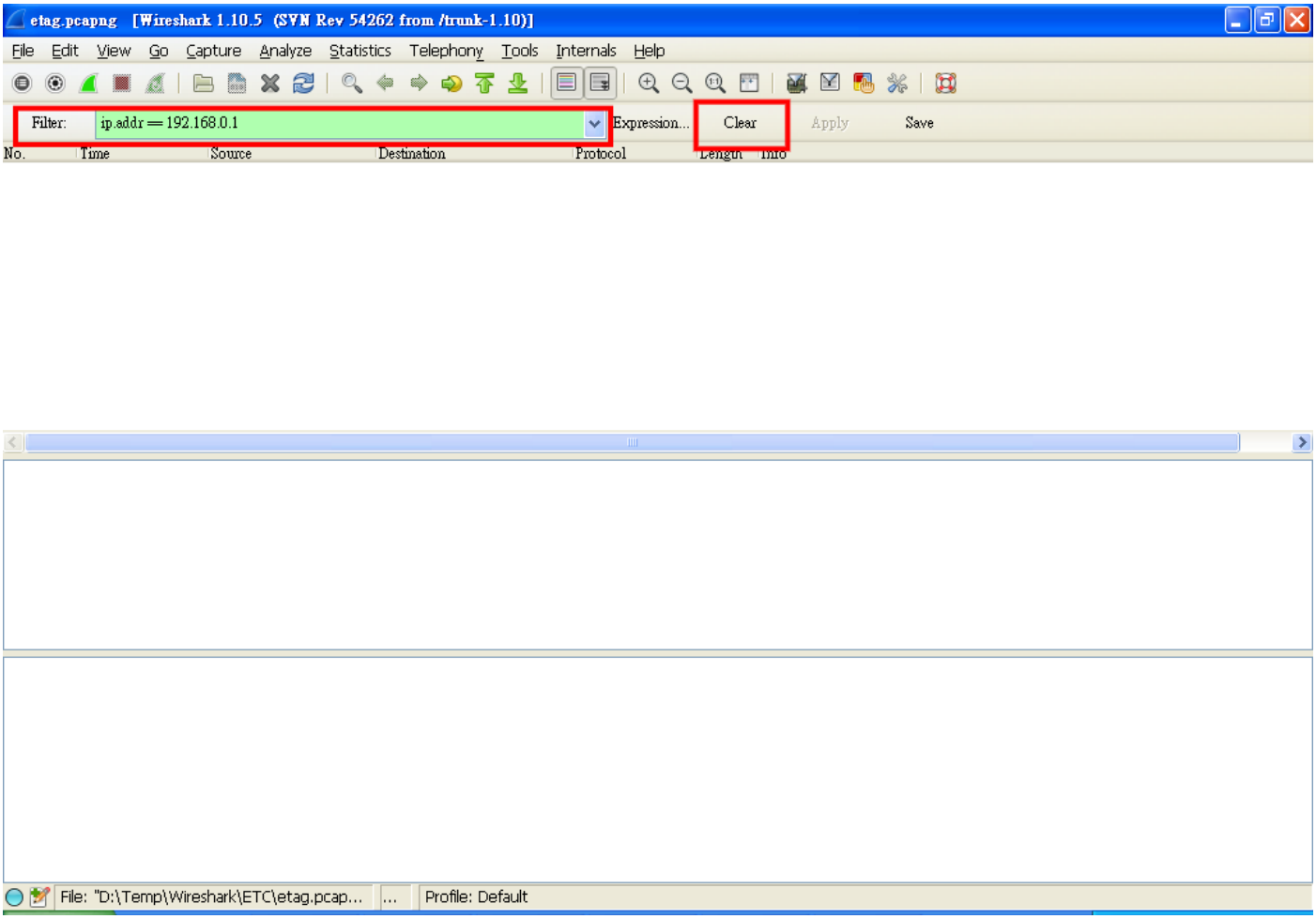
點 Filter



跳出 Sample

我們選 IP address 192.168.0.1

Ok 之後



他就會濾出我們要的封包

點 Clear 之後

他會還給我們全部的封包