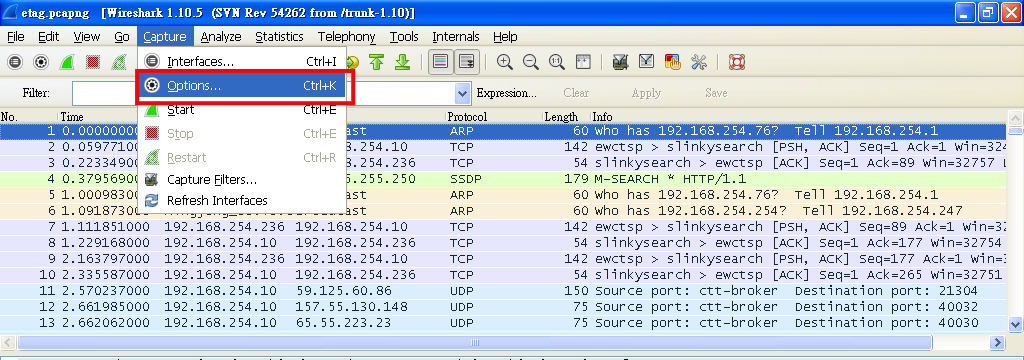
使用Wireshark抓特定IP或是Port的封包

方法有兩種

一種是開始抓封包之前就先設定Capture Filter

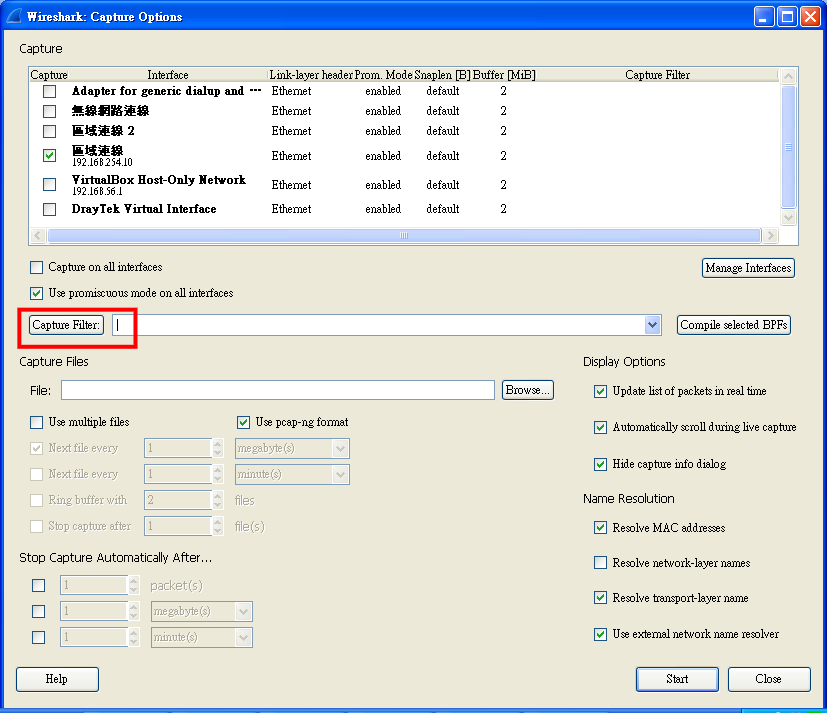
另外一種方式是全抓之後再做Packet Filter

我們先講第一種



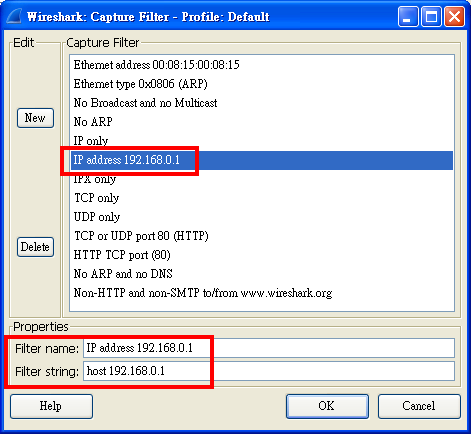
在Capture

Option…點一下



跳出此視窗

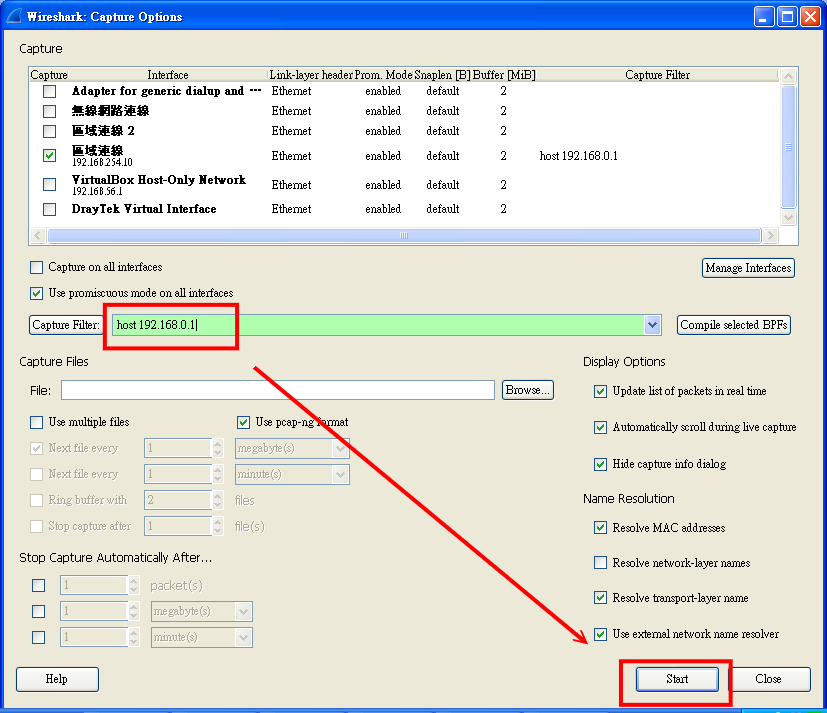
點一下Capture Filter



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



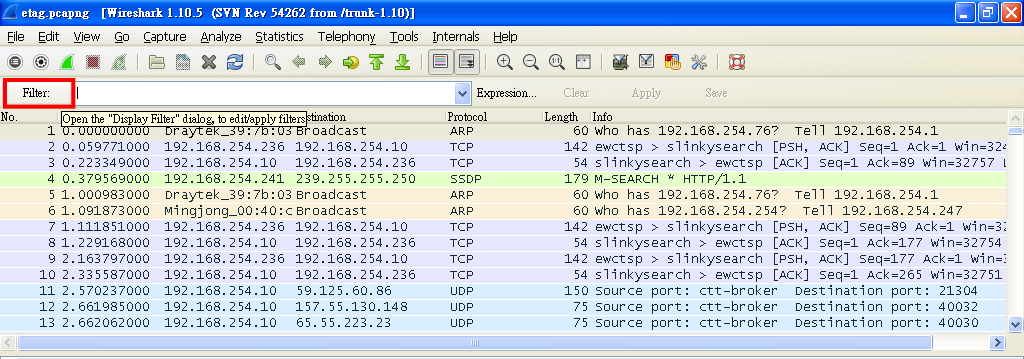
選進來之後

點Start就可以了

第二種方式是

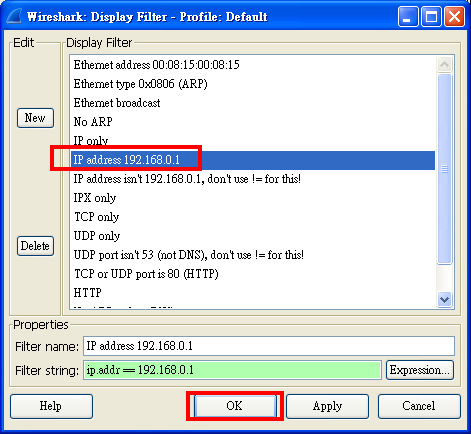
已經抓好封包了

要過濾出特定的IP或是Port



抓好之後

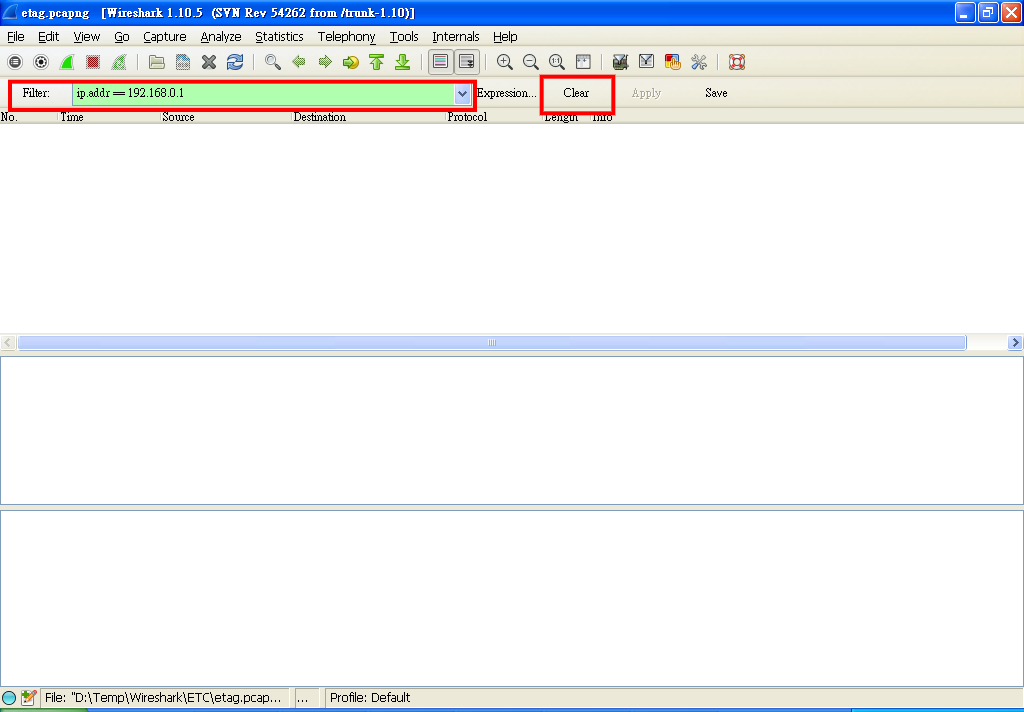
點Filter



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