摘要

隨著網路時代越來越發達，越來越多的人通過網路去瞭解世界。由網路產生的資訊也越來越多，這些資訊也就是我們所說的封包。一個封包不能做什麼，但是如果我們有幾萬甚至幾百萬的封包呢？網路時代的發達也預示著巨量資料的興起，我們不應單單只知道每個封包的內容，我們也應該從這些數量龐大的封包中，分析出對我們有用的資訊。Wireshark這個軟體就有對封包的內容進行展示以及部分的分析，但其分析的功能比較複雜，並不適合所有人使用。因此，我們想做出一個簡單的，方便操作的封包監測分析系統。這個系統可以分為抓取封包、展示封包和分析封包，也是我們這個系統最主要的功能。抓取封包我們借鑒wireshark的方式，建一個窗體程式，使用winpcap抓取封包程式，來抓取使用者電腦網卡的資訊；展示封包資訊，我們將抓到的封包以流來區分，最後展示到網頁上；圖形化一直是用來展示分析結果最好的方式，所以在我們的分析封包功能，我們將分析結果以柱狀圖和圓餅圖來呈現在網頁上。分析封包需要一定數量的封包，那抓到一定數量的封包是要時間的。為了讓使用者可以不用等候，我們有架設資料庫，使用者可以將抓到的封包資訊存到資料庫裏，之後有時間再來分析之前抓到的封包。我們不僅僅分析封包的內容，我們也對每個封包進行定位，在網頁上可以清楚地看到每個封包是從哪裏來的（僅限台灣地區）。