實驗日期:

2020/6/11

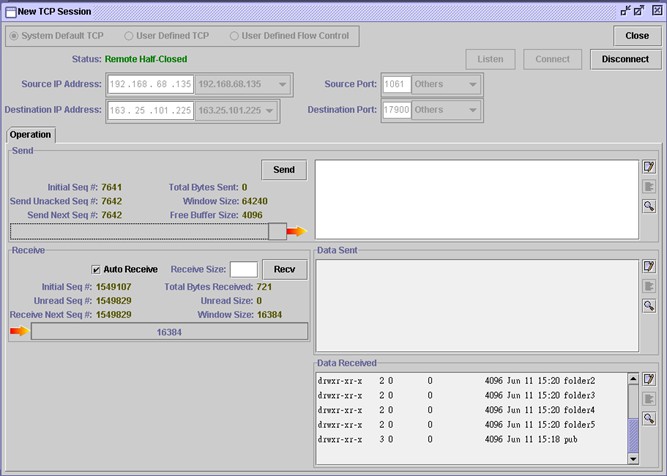
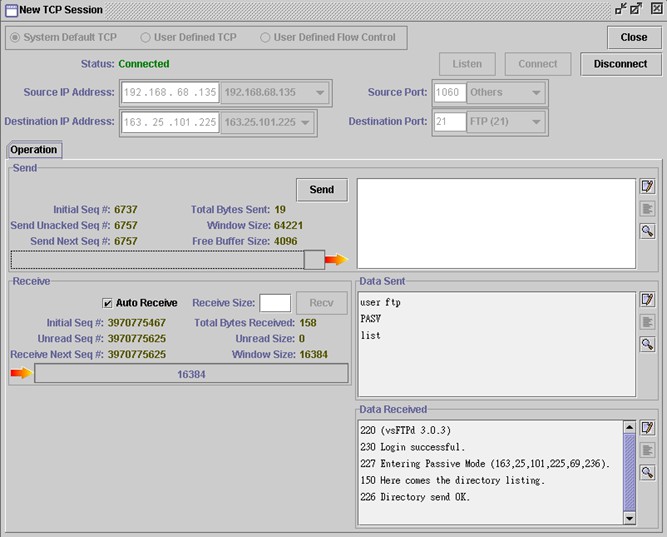
實驗名稱:

* ITS Exp. 21: FTP
* ITS Exp. 22: NAT
* ITS Exp. 23: Firewall

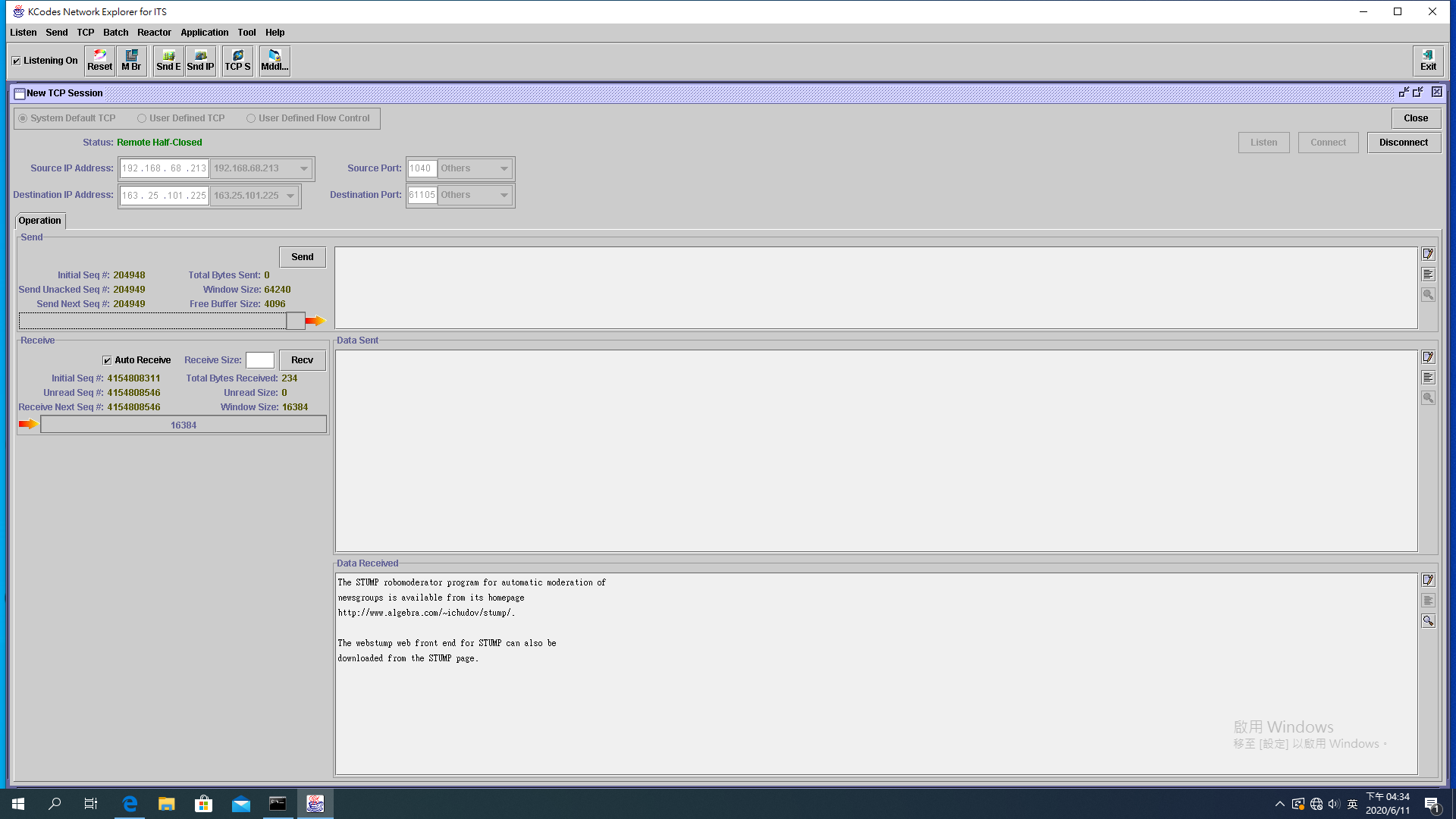
問題與答案:

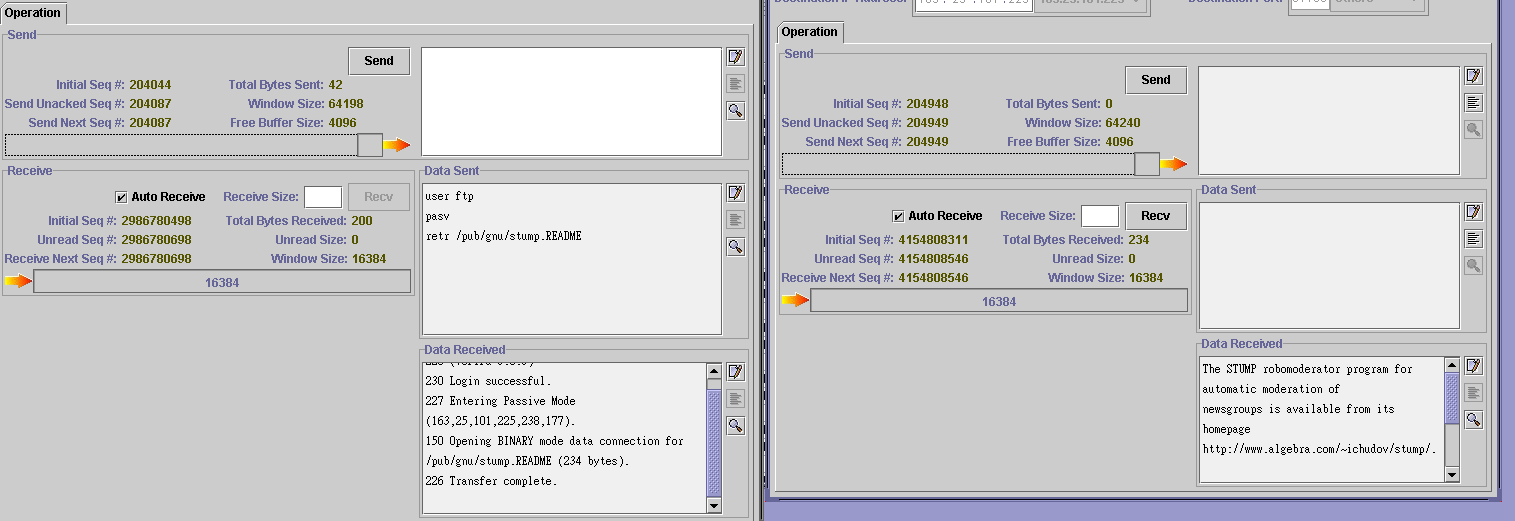
**Exp 21:**

驗收的圖



(因為進不去台大FTP，所以老師另設置了一個FTP:163.25.101.225，使能夠連入，並找到stump.README)





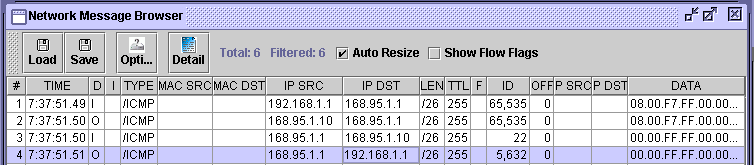
**Exp 22:**

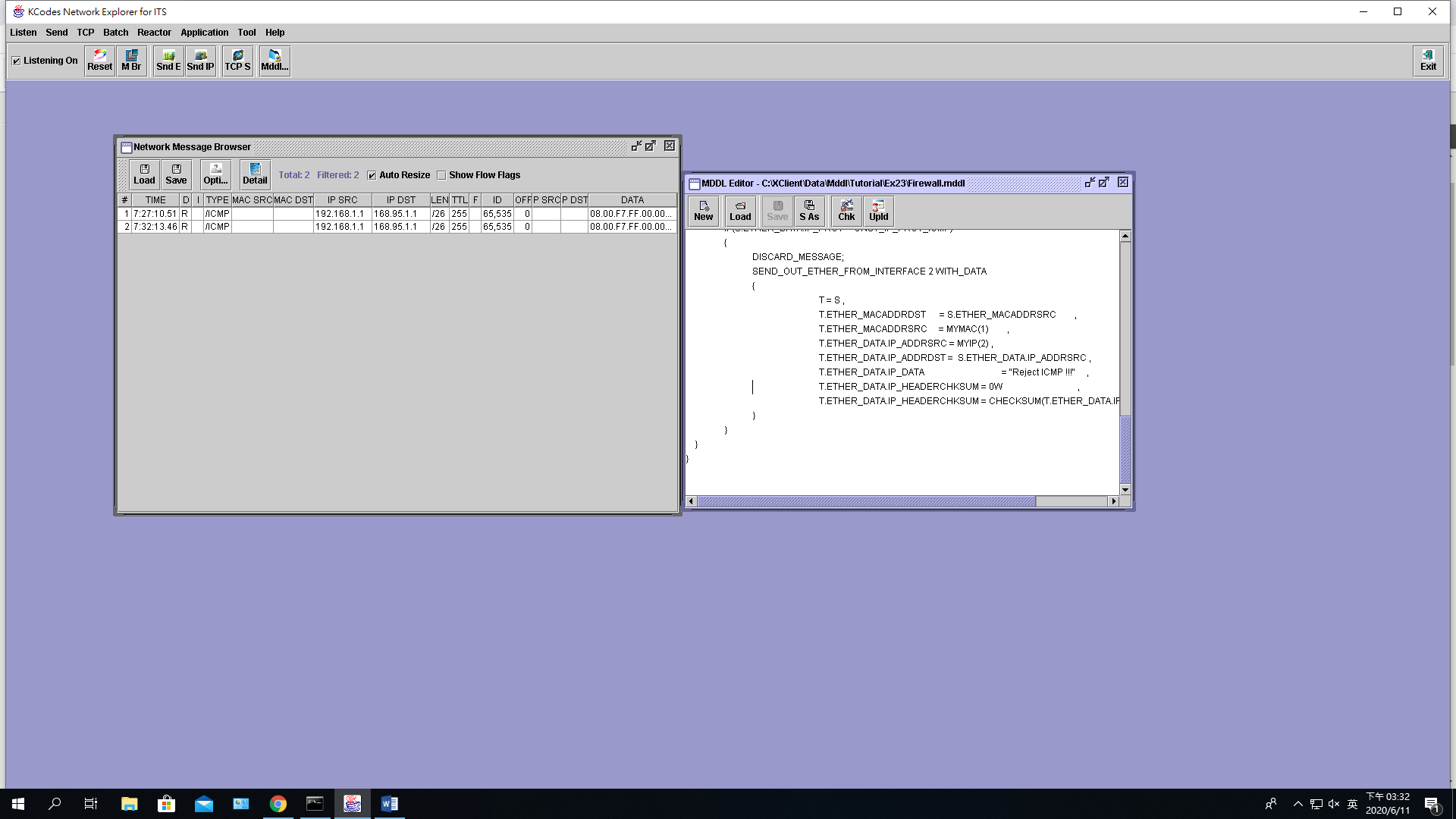
試著從任一ITS發送封包給其他ITS，觀察其現象並討論甚麼是「封裝偽裝(IP Masquerading)」?對網路來說有甚麼影響?

從ITS1傳送封包到ITS4時，ITS3的IP位置會被轉譯，這個就稱為封包偽裝，舉例當網路向外傳遞時，原本的位置會被轉成公用的位置。而當有ROUTER來回反覆走的時候。會用記憶判斷資料該轉發給哪個主機。

IP Masquerading 在電腦網路中是一種在IP封包通過路由器或防火牆時重寫來源IP地址或目的IP位址的技術，其允許在LAN上使用私有IP位址，並讓基於Linux的router執行IP位址和port的一些的轉換，將它從LAN上的機器接收到封包時，它記錄了封包的類型，如:TCP，UDP，ICMP等，並修改封包，使其看起來像生成的由路由器機器本身，當目的地主機接收到該封包時，它認為該封包來自路由主機，並將應答封包送回該位址。這種技術被普遍使用在有多台主機，但只通過一個公有IP位址存取網際網路的私有網路中，它是一個方便解得到廣泛應用的技術，當然NAT也讓主機之間的通訊變得複雜，導致了通訊效率的降低。

ITS1透過ITS3位置轉譯發送一個ICMP Echo Request給ITS4，ITS4回覆的ICMP Echo Request。





**Exp 23:**

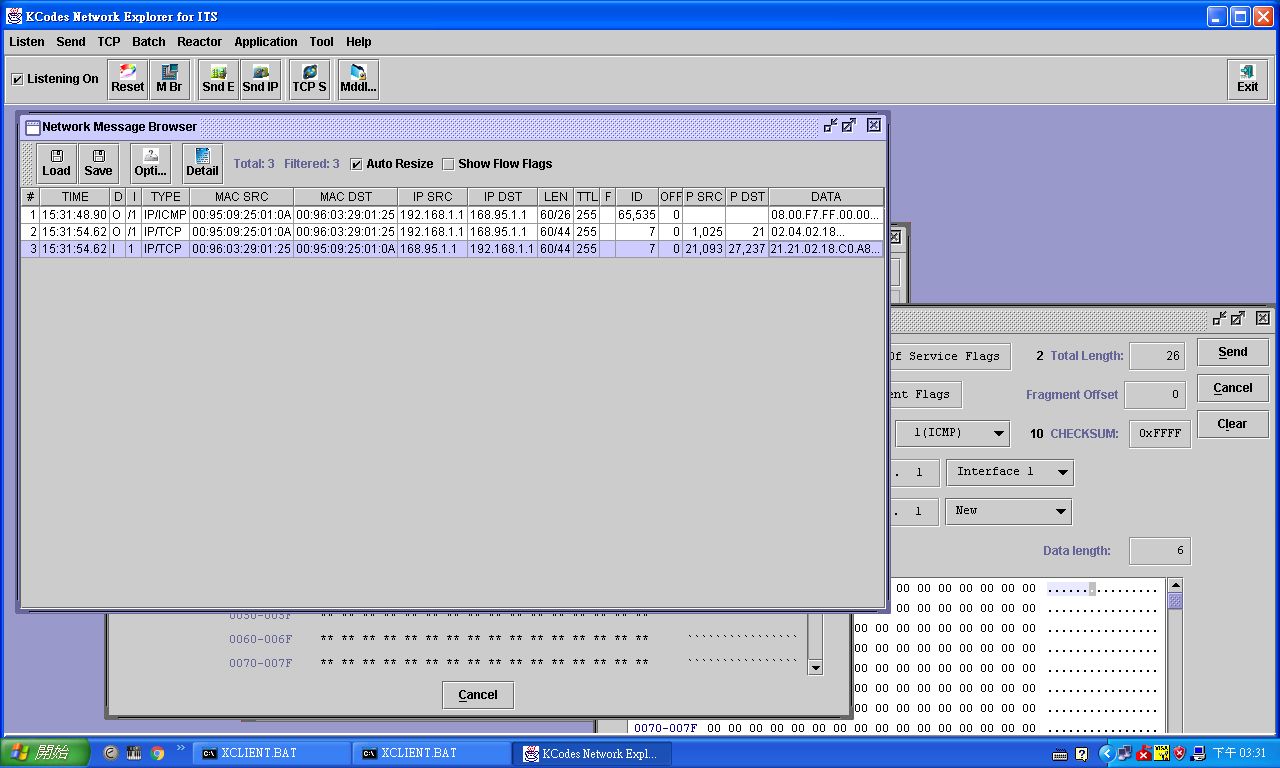
何謂「IP造假(IP spoofing)」?我們是不是可以用ITS設計一個防火牆解決這個問題?

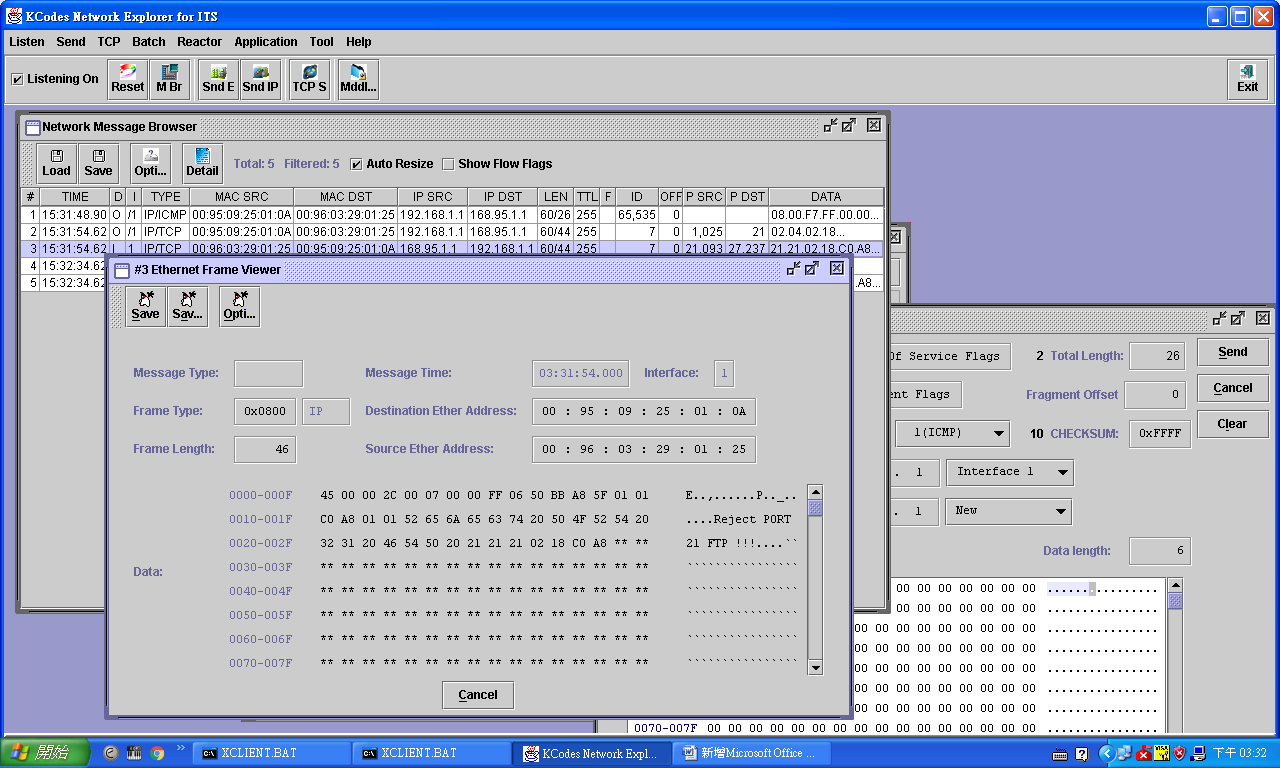
IP spoofing 是指帶有假的IP位址，目的是冒充另一個計算系統身分，使發送方可以保持匿名的一種技術是使用代理伺服器。其為一種攻擊方法，封包可能會採用受信任來源的IP位址來嘗試避開防火牆，這將使防火牆誤以為來自駭客的封包是來自受信任來源的；也可以僅用於隱藏攻擊的真實來源，入侵者使用其他電腦的IP位址來取得資訊或存取權限的程序，因此如果傳送回覆，該回覆將發往入侵者所偽造的位址，而非其入侵者的位址。

ITS1

(ITS1傳送封包給ITS4)

連線無法建立，ITS3阻擋了所有通訊port 為21的封包通過

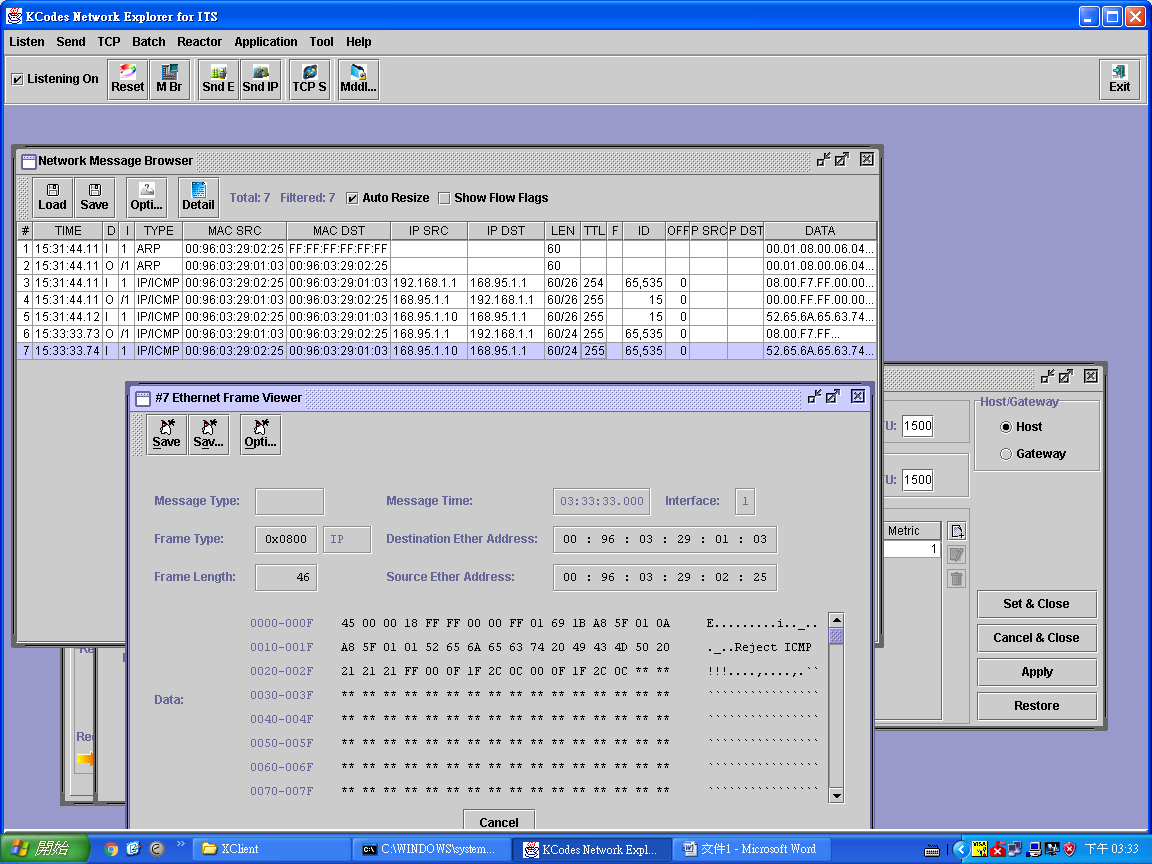




ITS4

(ITS4傳送封包給ITS1)

ITS4傳送ICMP Echo Request給ITS 1，ITS 3會攔截並回發ICMP Reply，顯示Reject ICMP



結果討論:

在做FTP實驗時，連了好久的台大FTP，就是連不到，試了很久像重開XClient等等都無法，之後老師架了一個FTP才完成實驗，花了很久的時間。