

- 全面監控：第二版(增加 Q&A)

科技帶來方便，但老闆們可不見得喜歡這些科技喔 !!

因為通常 MIS 或老闆們都想知道網路上發生了什麼事，為何有人老是報怨公司網路頻寬不夠，或者收到 ISP 發來的亂發廣告信的警告通知，甚至收到 IFPI 發函來說公司內部有人使用 P2P 的軟體在存放或共享非合法授權的軟體或音樂，哇 !! 光這些問題是不是就令人很頭大了！

就我們一般而言，我們都知道有一個軟體可以做到這個功能，組合國際的 eTrust Idtrusion Detection，組合國際的這套軟體非常強，可以記錄很多東西，但是可能價格高了一點，因此我們來介紹另外的一套軟體，可以做到 eTrust Idtrusion Detection 的大部份功能，Mail Log 和內容還有 Web 內容都一清二楚，以下我們就來好好介紹這一套軟體 Kerio Network Monitor

OK !!我們還是先下載他的 Network Monitor 軟體來用用，他的 Web 位址是

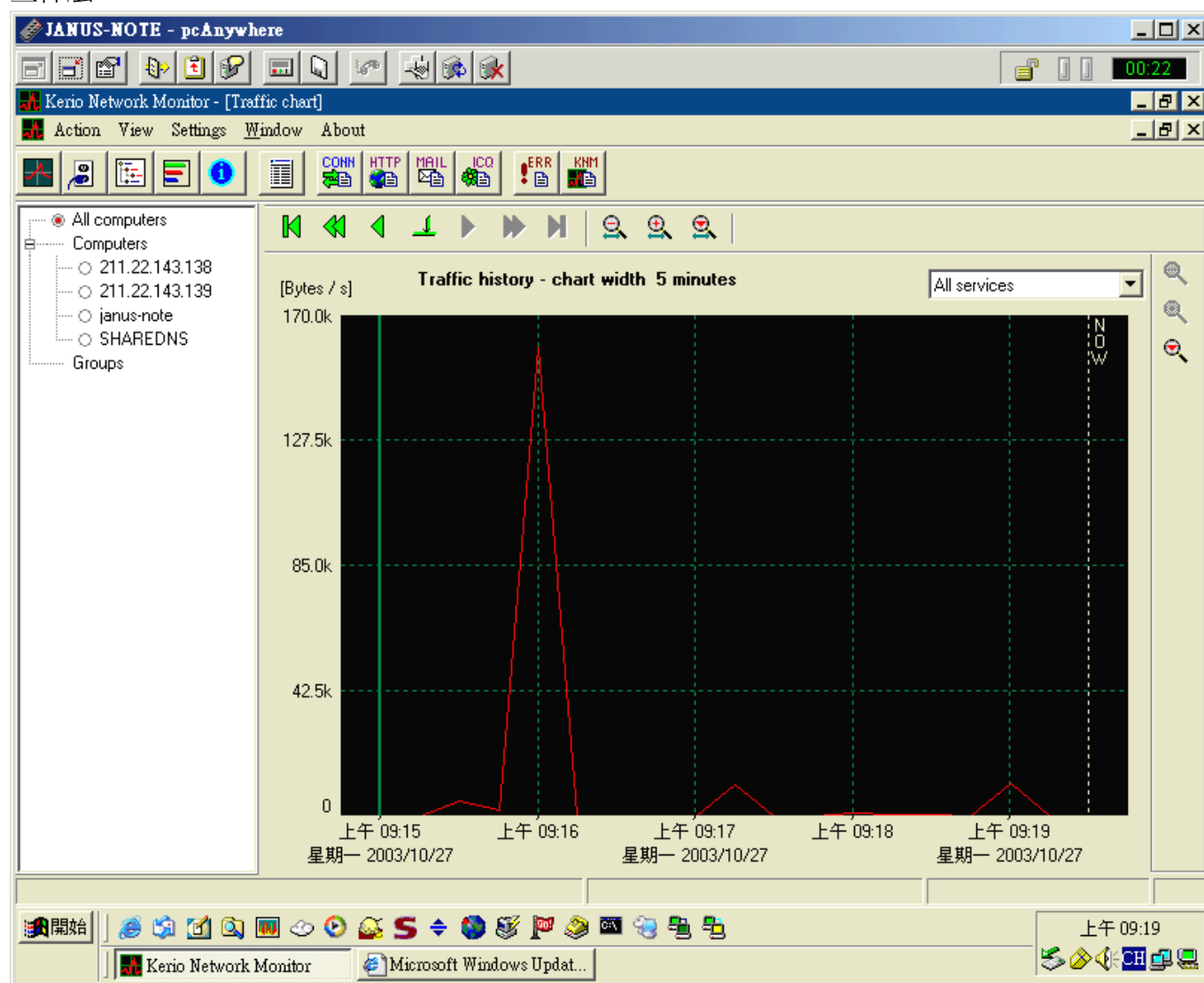
<http://www.kerio.com>

Products→Download→Kerio Network Monitor

Download 下來後請直接安裝，安裝過程我們將不介紹，安裝好之後，他會常駐一個

www.hatea.com.tw

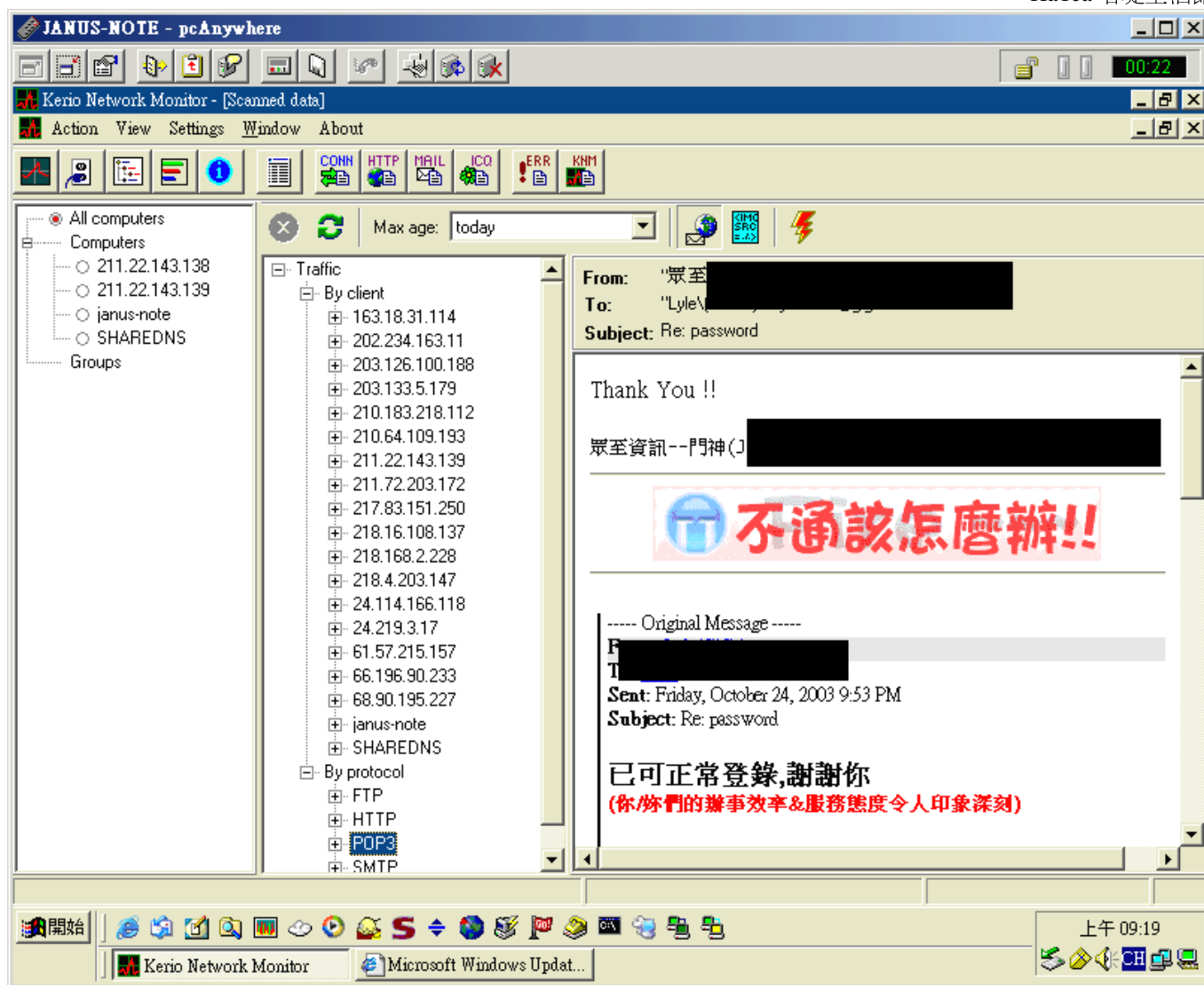
NetMon2.exe 的 Program，所以不用開主程式他就已經能開始記錄了，我們打開主程式看他記錄了些什麼 !!



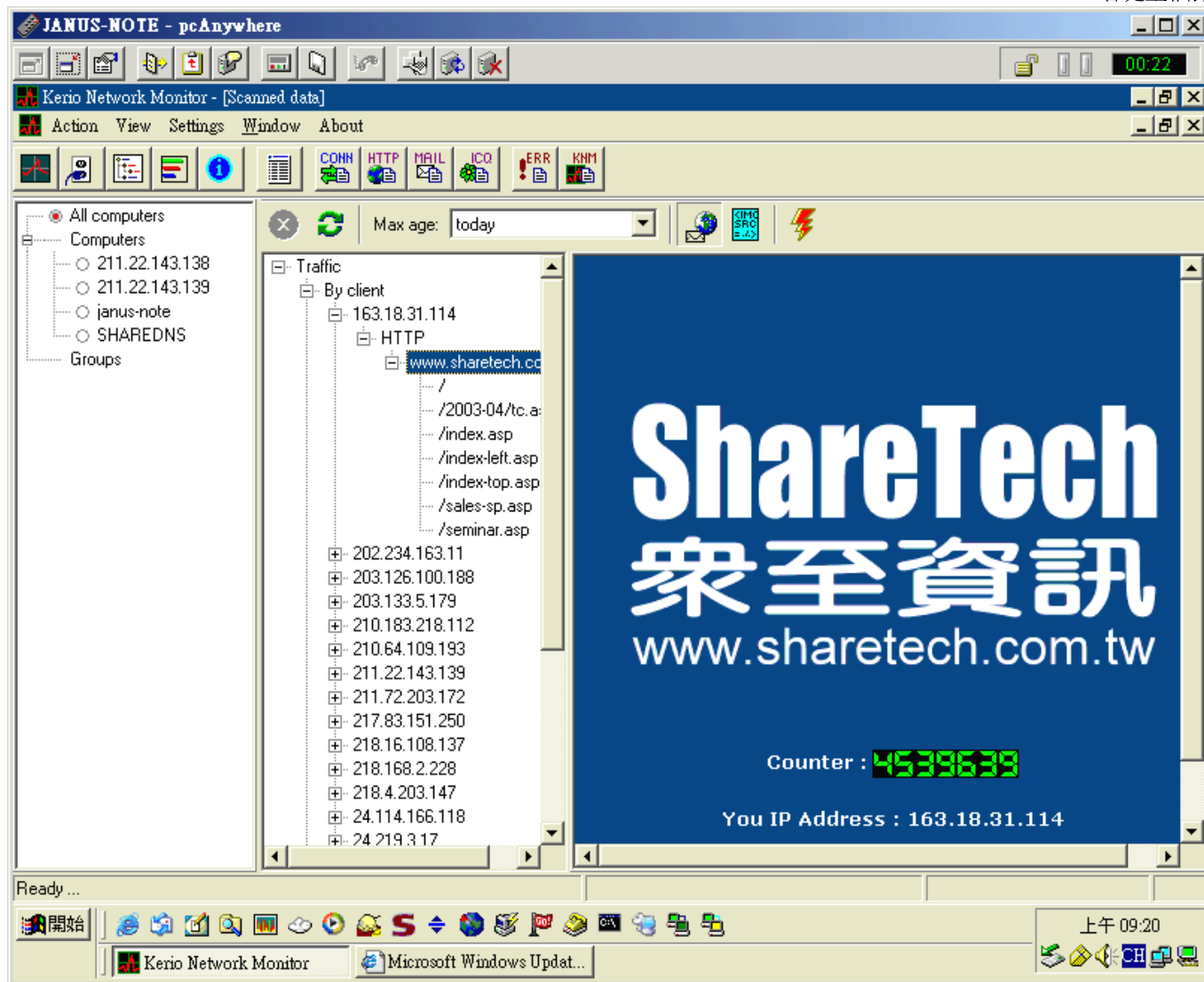
此程式會自動掃描，所以他會記錄下此 Network 有那些電腦在 Runing，但如果你的同一台電腦有安裝個人防火牆軟體，那麼則會擋下記錄，因此建議紀錄這台將個人防火牆軟體拿掉，還有他跟其他的 Traffic 軟體一樣，你想監看那邊，你就得放在那一層

我們第一個常看的就是流量表，這個軟體還幫我們區分了每一台的流量和服務 Port 的流量，所以我們可以知道是那一項 Service Port 佔的最多，或那一台佔的最多，紅色帶表整個全部的流量，而藍色部份是你點選的單台流量，我們還可以查歷史記錄喔 !!

光看到流量統計你有沒有覺得他實在是太強了，而如果你只爲了這樣的軟體功能就欣賞他，那底下要介紹給你的功能，你就會更大大的高興了 !!

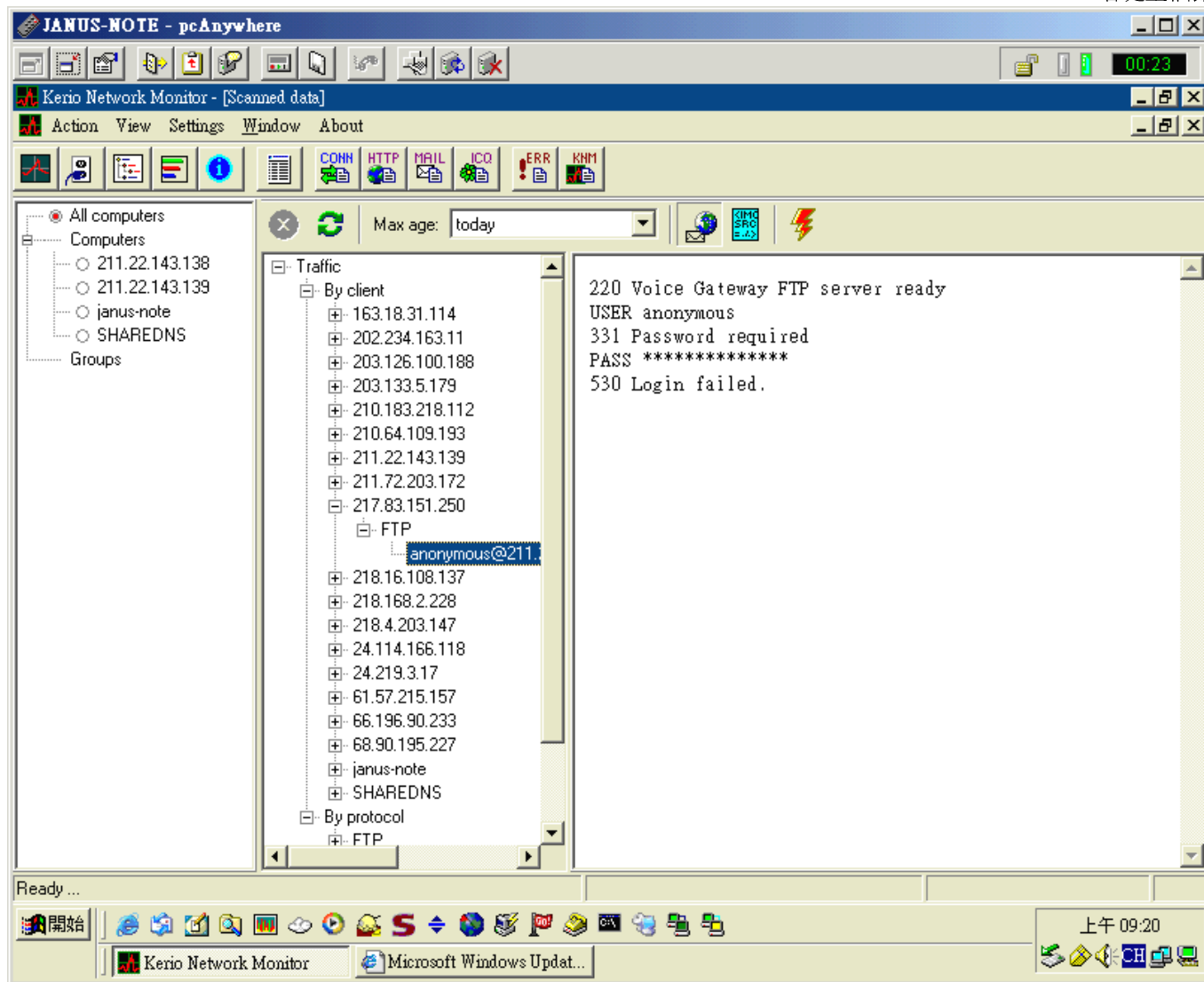


點選 Traffic , 啥米!!.....記錄了進出 Mail 的內容了 , 這...這...太神了 !!而且可以完整的顯示內容

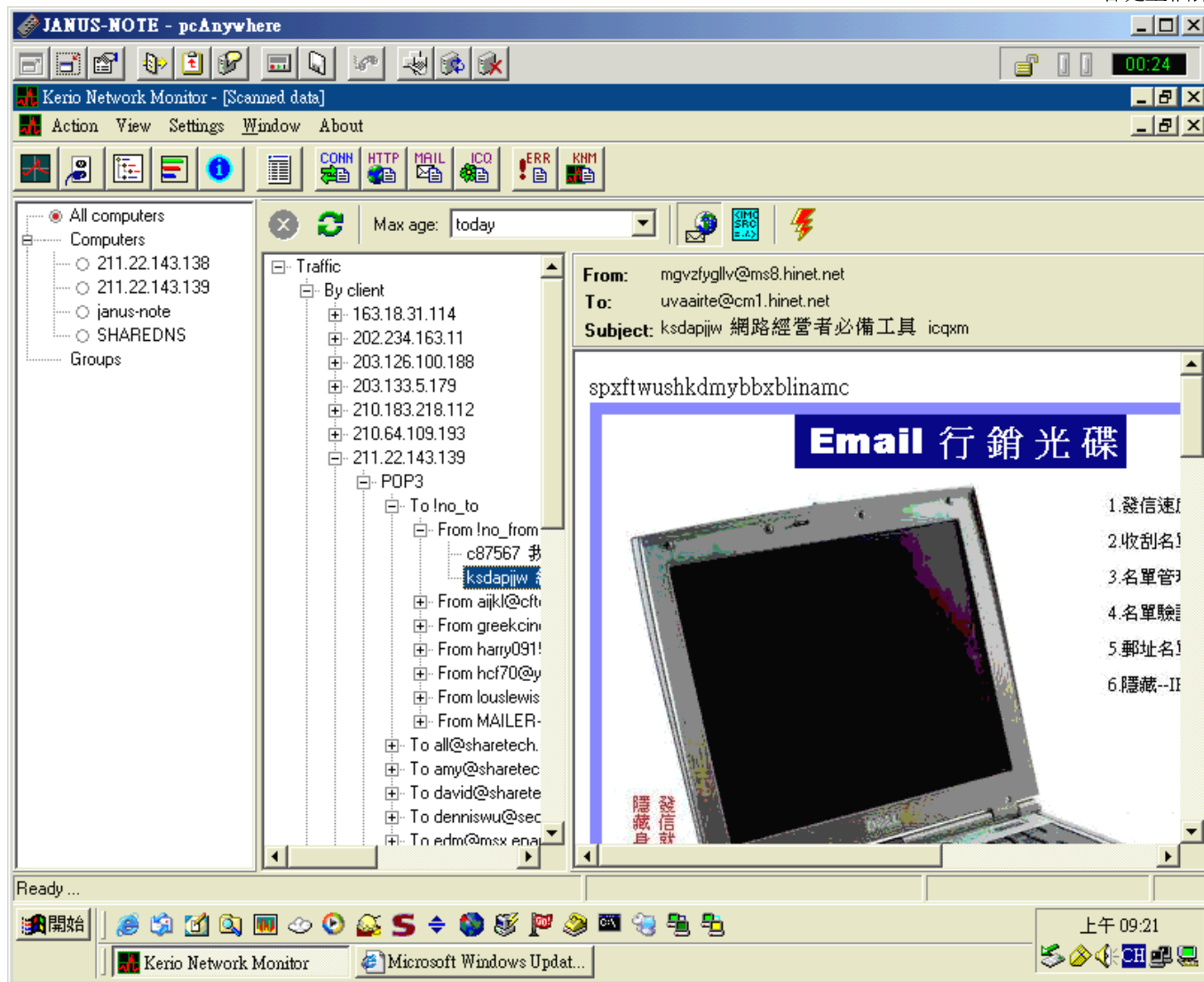


哇 !! 連其他人上網的封包都記錄下來了 , 真是網路無機密了啊 !!~~~~~

功能還很多喔 !!

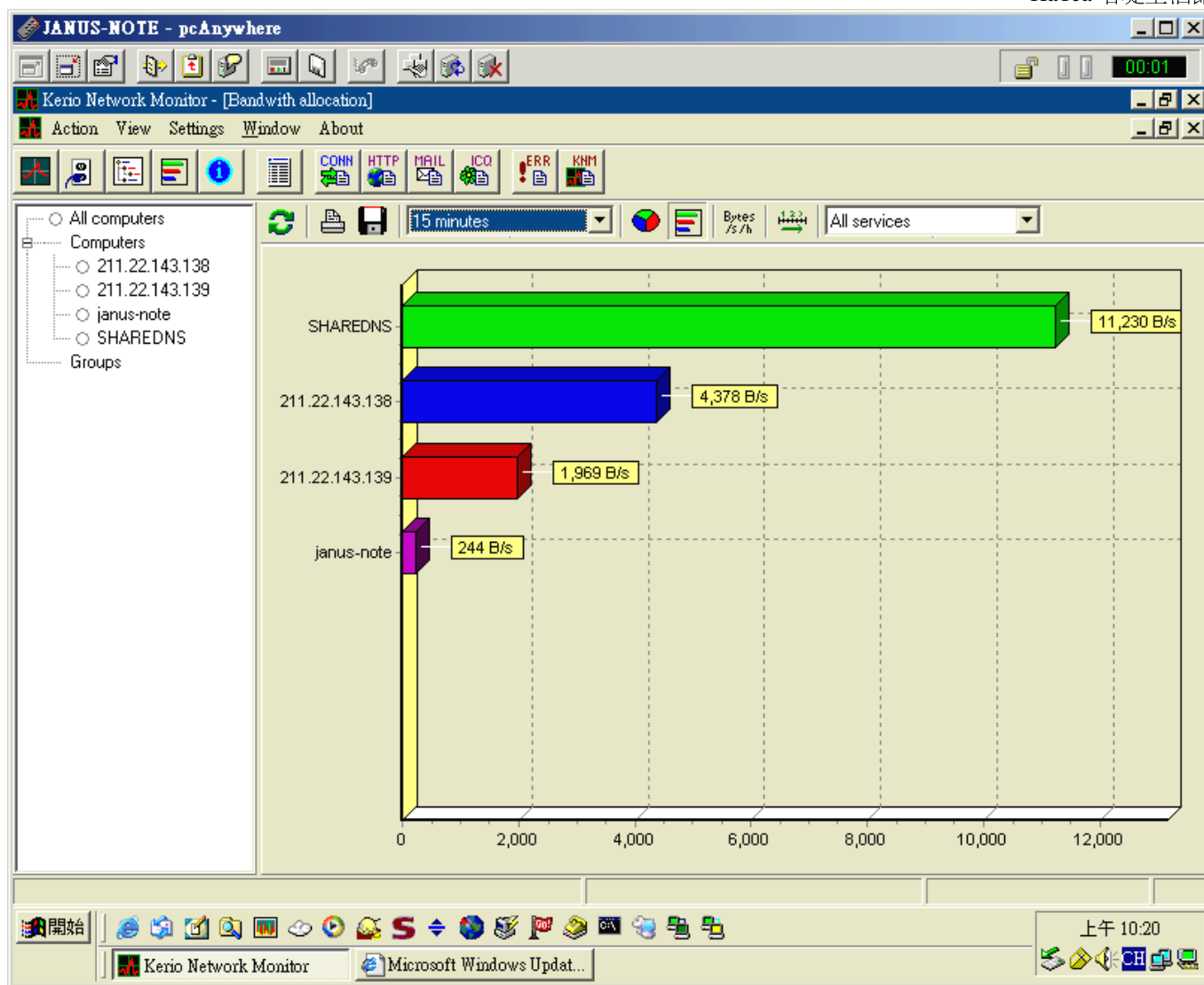


連 FTP 的動作都記錄下來了 !!



連誰在發廣告信都記錄下來了 !!

^^ 優卡答(日語)

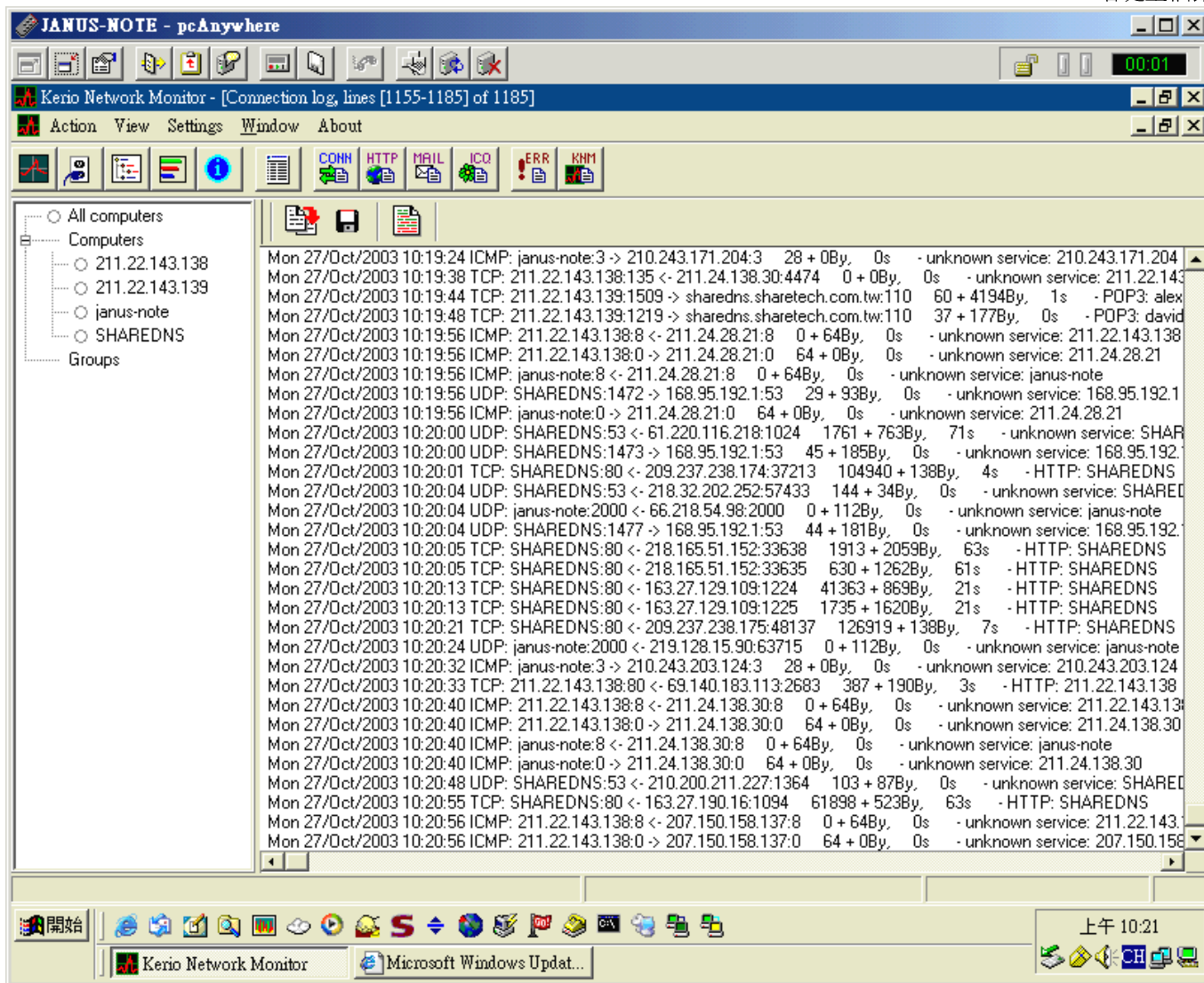


還有排名，連圓餅圖都有喔 !! 這樣就不難了解公司內部其他同仁為何老是在說頻寬不夠了 !!

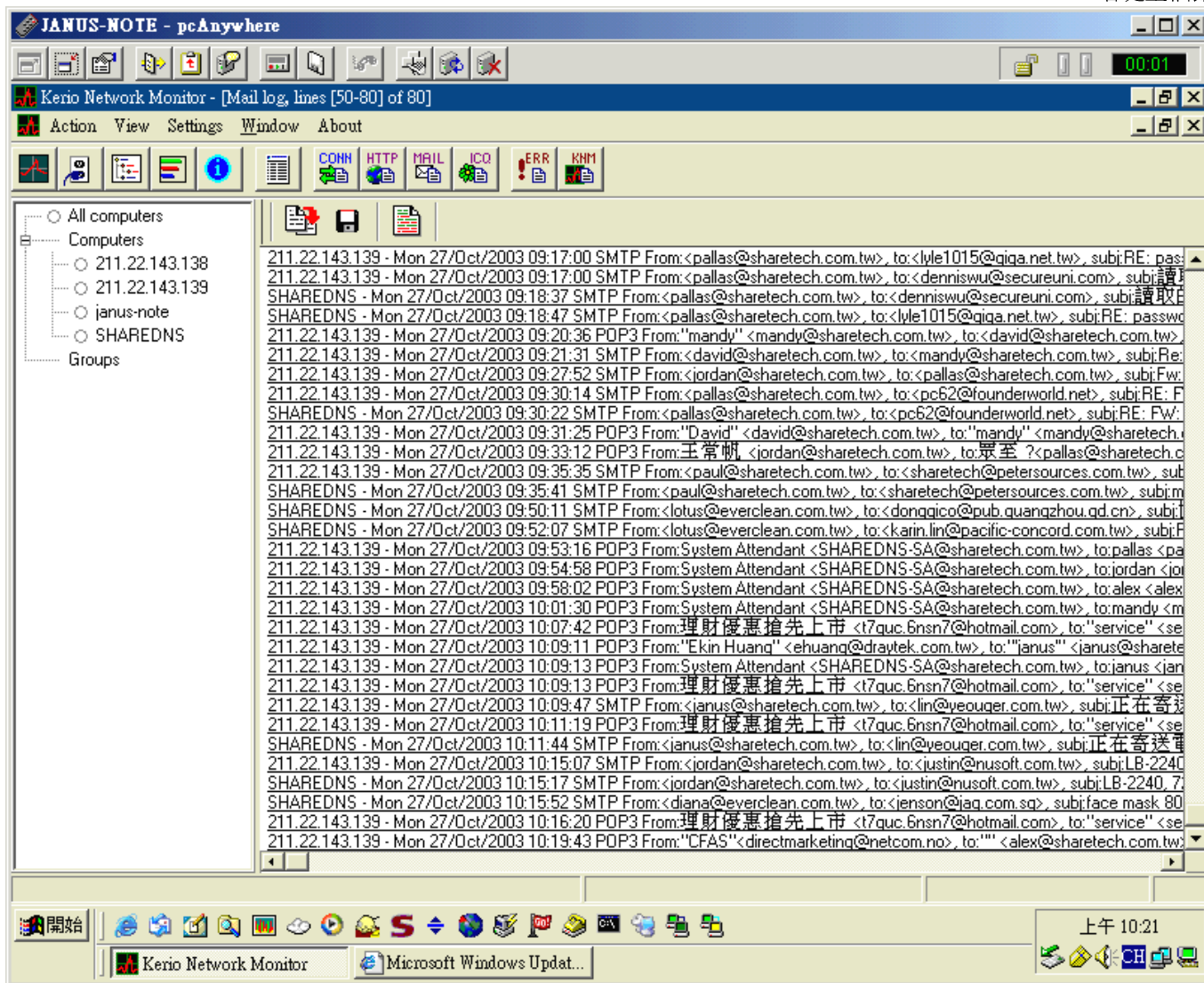
Kerio Network Monitor - [Accounting report for 2003/10/25 - 2003/10/27, All services]

	2003/10/25 星期六	2003/10/26 星期日	2003/10/27 星期一	2003/10/27 2003/10/27
All computers	0	0	47,819,504	47,819,504
211.22.143.138	0	0	3,656,637	3,656,637
211.22.143.139	0	0	8,581,318	8,581,318
janus-note	0	0	19,025,374	19,025,374
SHAREDNS	0	0	16,556,175	16,556,175

哇 !! 還有 Report , 有這些資料就可比讓公司的 MIS 或老闆評估我們是否真的需要加對外連線的線路了



哇 !! ~~~~~ 還有更細的 Log，有 CONN/HTTP/MAIL/ICQ/ERR/KNM 等等的 Log，如果我們要分析誰在攻擊我們的 Server，那麼這裏會留下更細的資料，我們可以將這些 Log 匯出成 TXT 檔，然後再用 Excel 或 Access 匯入做查詢以及統計分析動作，這樣我們也可知道我們為何受到入侵，然後知道了解駭客的手法是使用那一種方法，我們也可以即時的做好防護動作！



這是 Mail Log 的部份，可以看見進出信件的方向/標題/和寄件者和收件者等等的內容，這裏有一個大優點，如果公司內同仁不是使用貴公司的寄信伺服器，那麼這裏還是可以留下詳細的記錄的

如果你是一個 MIS 或老闆，我想這個軟體的功能對您想要達到監看的目地是夠的，但請小心使用，通常這類軟體的記錄檔會非常的大，小心硬碟空間不夠喔 !!

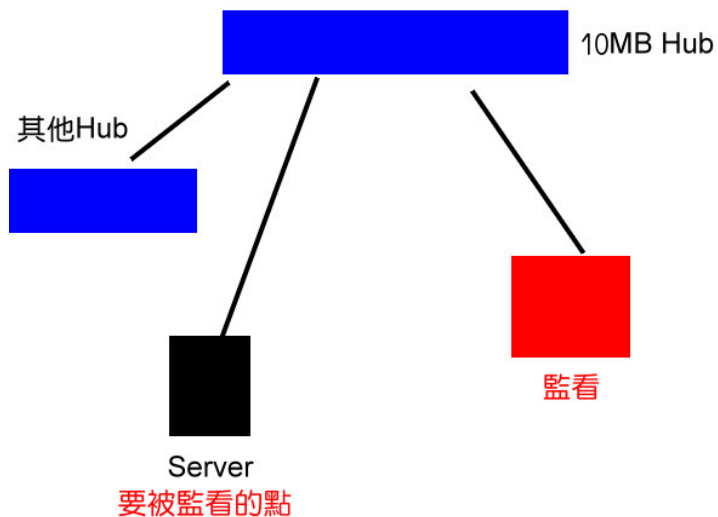
Q&A:

Q1:為何我抓不到你說的那麼多資料?

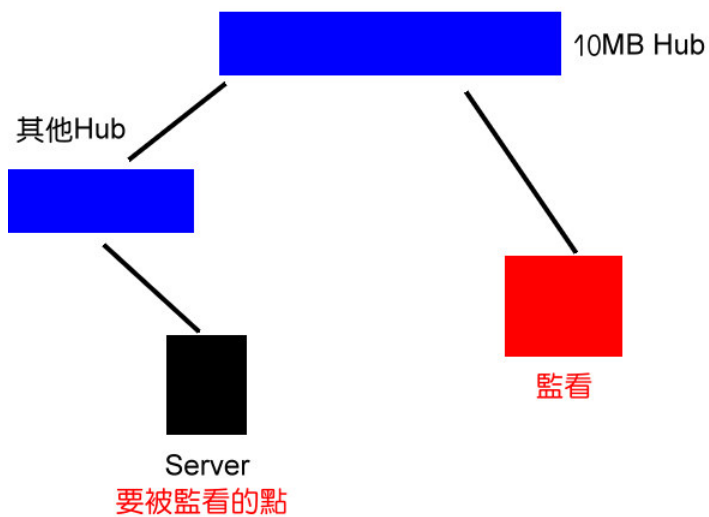
A1:這是因為你監控點和 Switch Hub 的因素所造成的，如果是 Sniffers/Traffic.....等等的軟體都一樣，如果不是裝在主偵測 Server 的話，那麼請備一個單速的 Hub，比如快把他丟了的 10MB Hub 或 100MB Hub 或 10/100 雙速 Hub，千萬不能用 Switch，這是因為 Hub 運作原理的關係所致

Q2:我已經用了 10MB 的 Hub，但為何還是抓不到封包?

A1:雖是一樣的 10MB Hub，有可能你手上的 Hub 是無法抓封包的，我就碰過好幾個型號(當中包含不少知名品牌)，不然就是你監控點接線方式錯了 !!請參考圖一和圖二，圖一是可以同步抓到 Server 封包，但圖二可不行



[圖一]



[圖二]

祝您用的開心 !!

門神 2003-10-27