Python SDN Lab

R03922133黃子軒

1. **流程** 因為本身電腦為windows8，先開啟VMWARE來執行Ubuntu 14.10上，並直接開啟Mininet及Wireshark。此實驗分兩步驟，一個是利用python來完成文件排版，另一個則是實作server端和client端，client端會先將文件input.txt讀入並存為字串，並將此字串發送給server端，server端收到後會回傳一個排版過的string，client端收到此string後，再將之輸出為學號.txt。
2. Python文件排版

原本的文件逗號後面都無空格，句號後面都無換行，且句號後面 沒有改為大寫，有些地方則是不該大寫。(figure1)

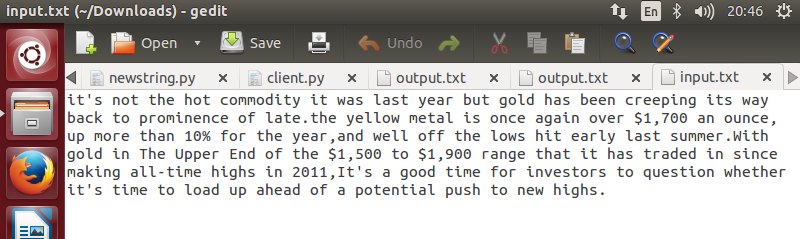
****

figure 1

經排版後，除了上述都有改正之外，每一行的character數也限制在60個字元內，且多了一行來計算總字數跟總character數。(figure2)

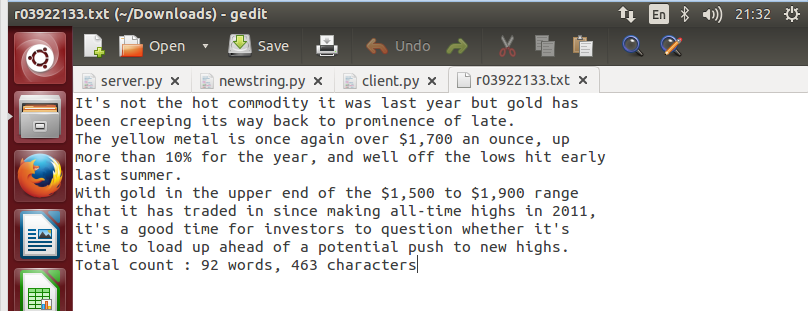
****

figure 2

1. Socket programming  
    實際將server架於學校的伺服器中(figure 3)，並將自己的電腦假設為client端並連線過去(figure 4)，client端會收到server端回傳的完整排版訊息。最後再透過wireshark去分析封包的行為。

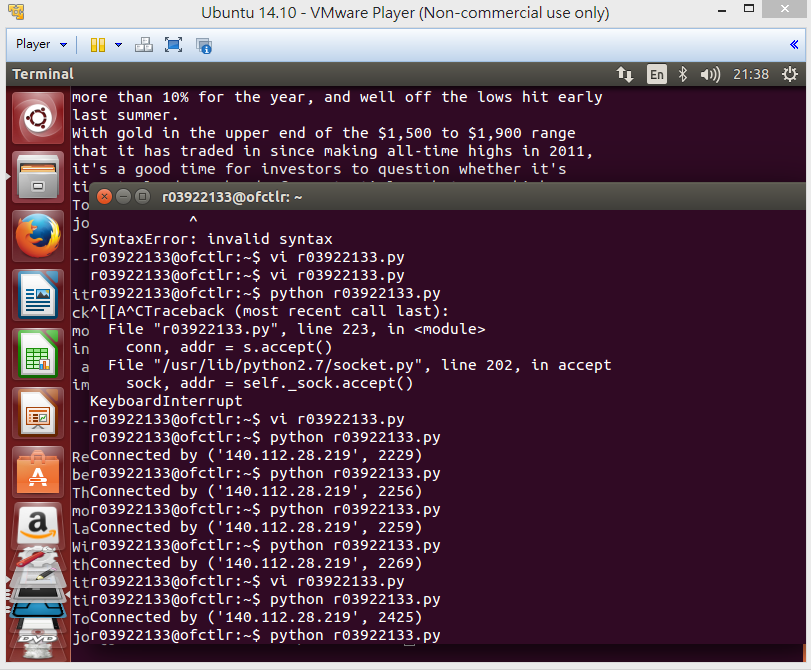
****

figure 3 (server IP: 140.112.149.69 , port: 30023)

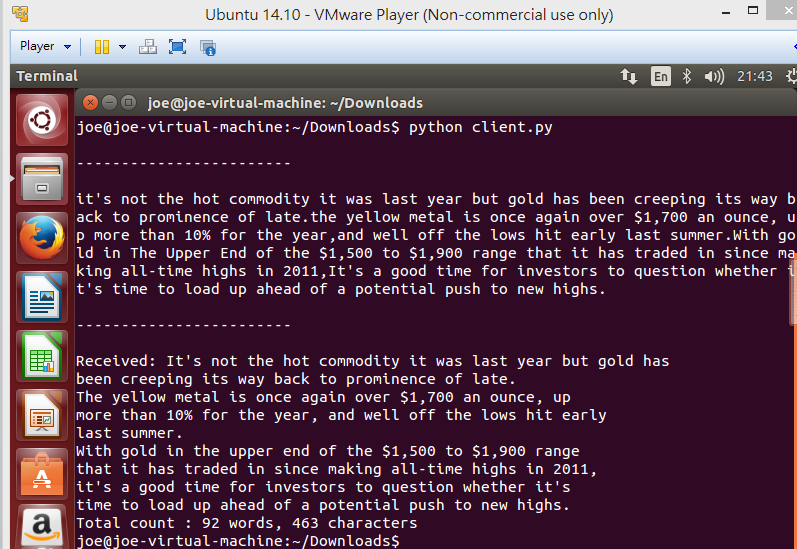
****

figure 4 (client receives message)

1. **分析**

在Wireshark中點選eth0並按開始，會發現只有走SSDP protocol的封包(figure 5)，但在啟動server.py和client.py之後可以發現開始有TCP封包交換的動作(figure6)。

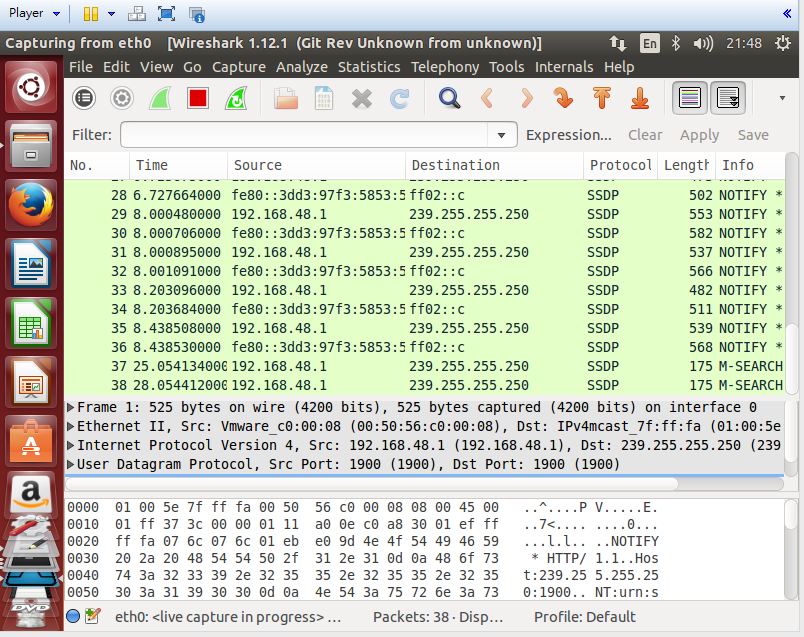
****

figure 5

SSDP: 簡單服務發現協定，是屬於應用層的協定，提供在局部網路裡發現裝置的機制。client端可以通過使用SSDP來根據自己的需求，查詢自己所在局部網路裡面提供特定服務的裝置。裝置也可以透過SSDP向自己所在的局部網路裏的控制點去宣告它的存在。因此當我們開啟wireshark去監控eth0時，只會看到SSDP的封包存在。

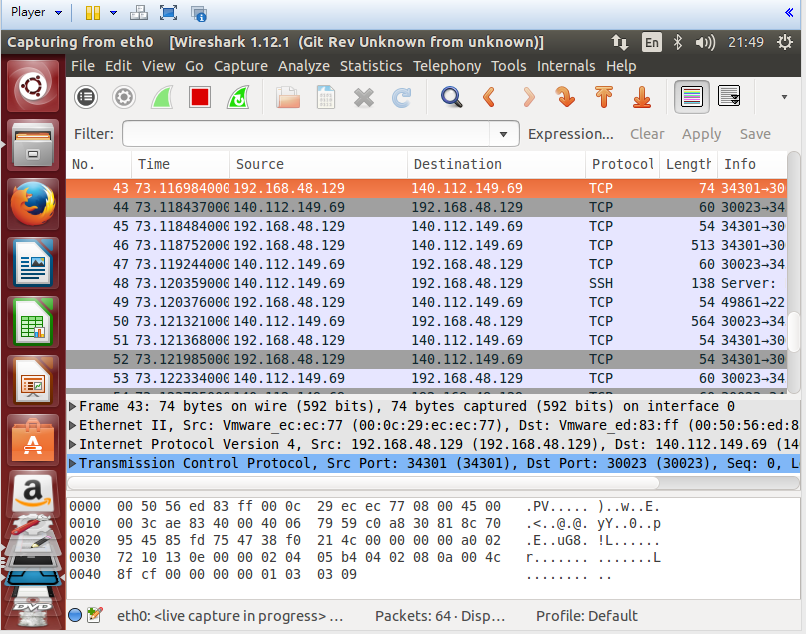


figure 6

當我們啟動server和client後可以發現，TCP的封包大量出現。原因是我們所寫的server和client是透過TCP的協定來溝通的。也可發現還有些許封包是透過SSH傳輸的，原因是我們會先透過SSH來連線的server。

TCP: 傳輸控制協定，為網路基礎通訊架構，提供點對點的連結機制，標準化了許多事項，包括:資料該如何封裝、定址、傳輸、路由以及如何在目的地接收。

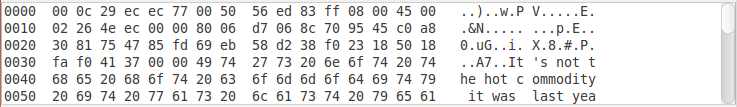
透過觀察封包長度，我們還可以發現有兩個封包的長度特別長，原因為那些封包就是我們傳送字串的封包，點開即可發現內容為我們先前所編輯過的字串以及一些經加密過後的內容，(figure7)  ****

figure 7

接著觀察封包傳送的起點和終點，我們可發現此兩封包的起點和終點正好是相反的，原因就是我們會先從client端發送此字串給server端，所以起點為192.168.48.129(ubuntu的IP)，終點為140.112.149.69(學校的IP) (figure8)

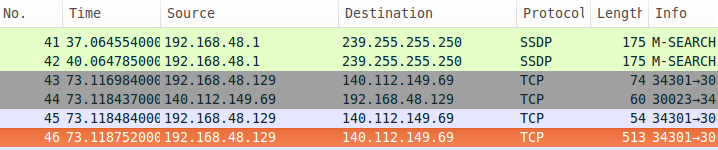


figure 8

另一個長封包就是從學校的server經過字串處理後，回傳給client端的封包，起點為140.112.149.69(學校的IP)，終點為192.168.48.129(ubuntu的IP)，因為有多了空行和顯示字數，長度會較剛剛那個封包長一點。(figure9)

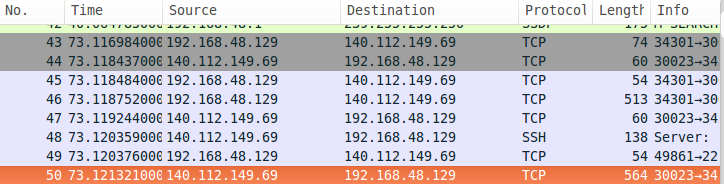
****

figure 9

經過一連串的封包交換後，client端會將收到的字串輸出成一個檔案，存在相同的目錄底下，所以回到資料夾，可發現多了一個檔案名為r03922133.txt (figure10)

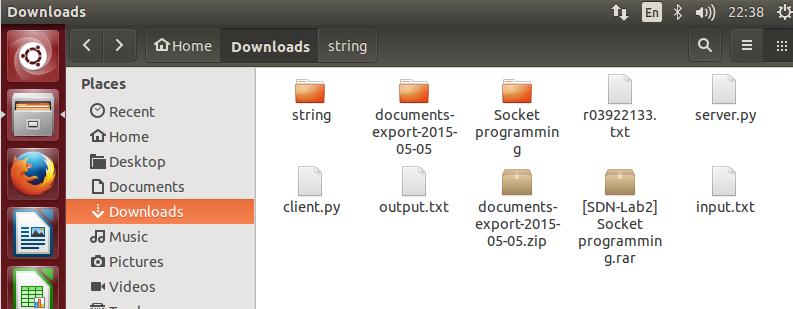
****

figure 10

**3. Reference  
 1.** <http://www.pcnet.idv.tw/pcnet/network/network_ip_tcp.htm>  **2.** <http://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol>