

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。

I. 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)

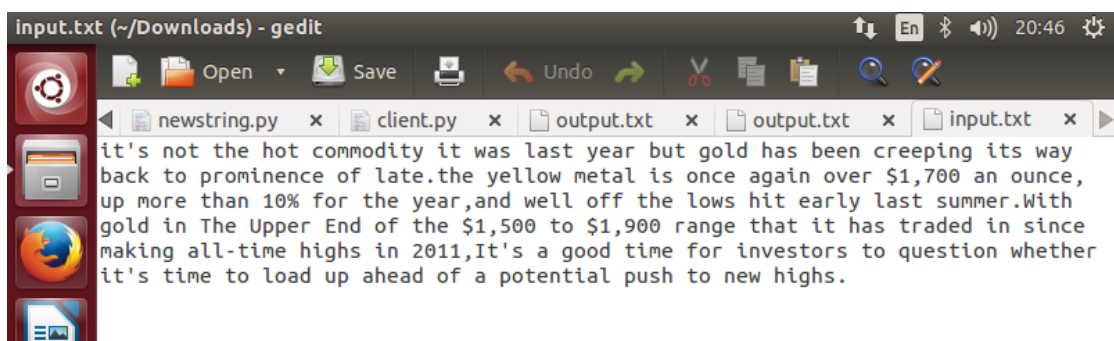


figure 1

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)

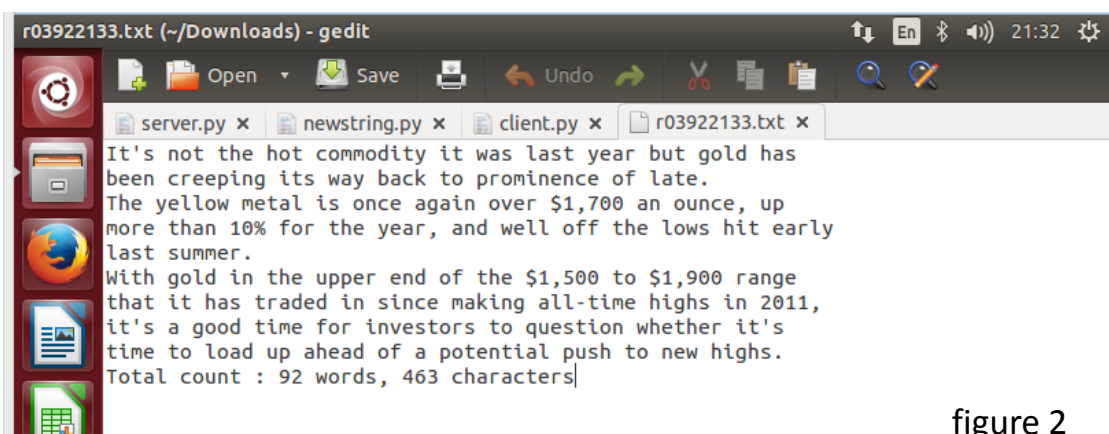
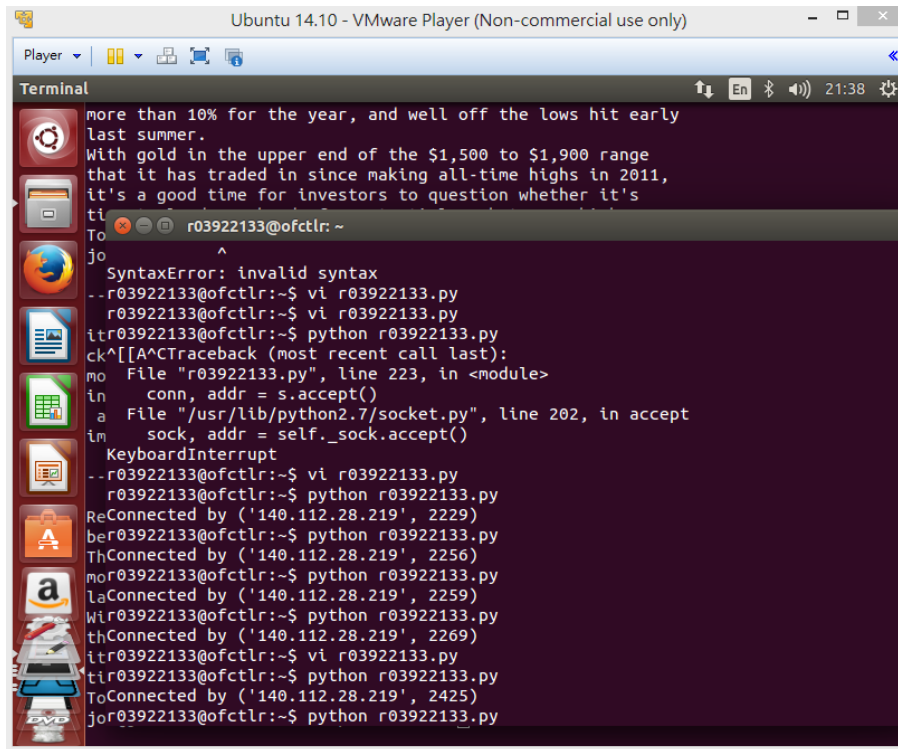


figure 2

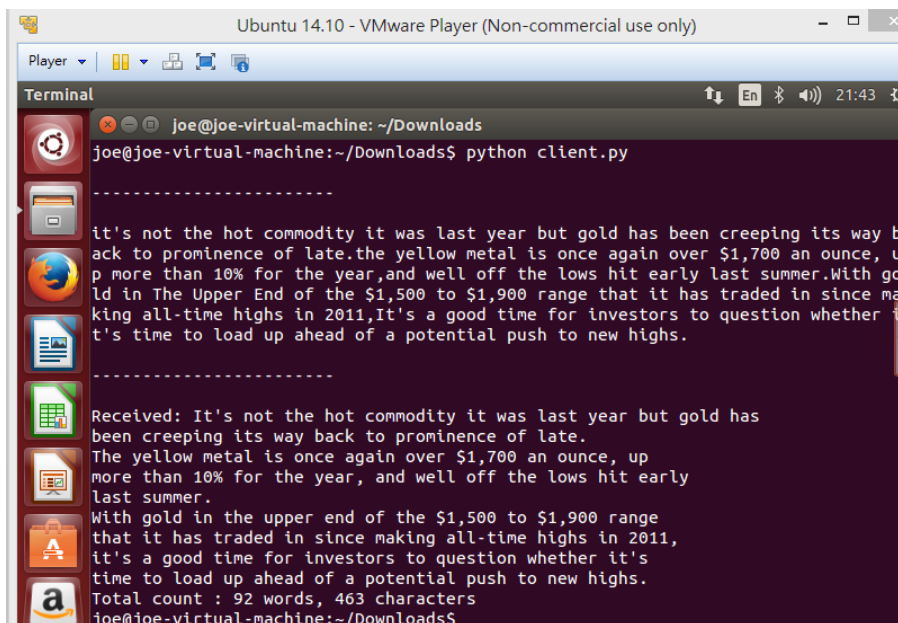
II. Socket programming

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。



```
more than 10% for the year, and well off the lows hit early
last summer.
With gold in the upper end of the $1,500 to $1,900 range
that it has traded in since making all-time highs in 2011,
it's a good time for investors to question whether it's
ti
To
To
jo
jo
SyntaxError: invalid syntax
--r03922133@ofctlr:~$ vi r03922133.py
r03922133@ofctlr:~$ vi r03922133.py
itr03922133@ofctlr:~$ python r03922133.py
ck^[[A^CTraceback (most recent call last):
  File "r03922133.py", line 223, in <module>
    conn, addr = s.accept()
  File "/usr/lib/python2.7/socket.py", line 202, in accept
    sock, addr = self._sock.accept()
KeyboardInterrupt
--r03922133@ofctlr:~$ vi r03922133.py
r03922133@ofctlr:~$ python r03922133.py
ReConnected by ('140.112.28.219', 2229)
ber03922133@ofctlr:~$ python r03922133.py
ThConnected by ('140.112.28.219', 2256)
mor03922133@ofctlr:~$ python r03922133.py
laConnected by ('140.112.28.219', 2259)
Wir03922133@ofctlr:~$ python r03922133.py
thConnected by ('140.112.28.219', 2269)
itr03922133@ofctlr:~$ vi r03922133.py
tir03922133@ofctlr:~$ python r03922133.py
ToConnected by ('140.112.28.219', 2425)
jor03922133@ofctlr:~$ python r03922133.py
```

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



```
joe@joe-virtual-machine: ~/Downloads
joe@joe-virtual-machine:~/Downloads$ python client.py

-----
it's not the hot commodity it was last year but gold has been creeping its way b
ack to prominence of late.the yellow metal is once again over $1,700 an ounce, u
p more than 10% for the year,and well off the lows hit early last summer.With go
ld in The Upper End of the $1,500 to $1,900 range that it has traded in since ma
king all-time highs in 2011,It's a good time for investors to question whether i
t's time to load up ahead of a potential push to new highs.

-----
Received: It's not the hot commodity it was last year but gold has
been creeping its way back to prominence of late.
The yellow metal is once again over $1,700 an ounce, up
more than 10% for the year, and well off the lows hit early
last summer.
With gold in the upper end of the $1,500 to $1,900 range
that it has traded in since making all-time highs in 2011,
it's a good time for investors to question whether it's
time to load up ahead of a potential push to new highs.
Total count : 92 words, 463 characters
joe@joe-virtual-machine:~/Downloads$
```

figure 4 (client receives message)

2. 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 (figure 6)。

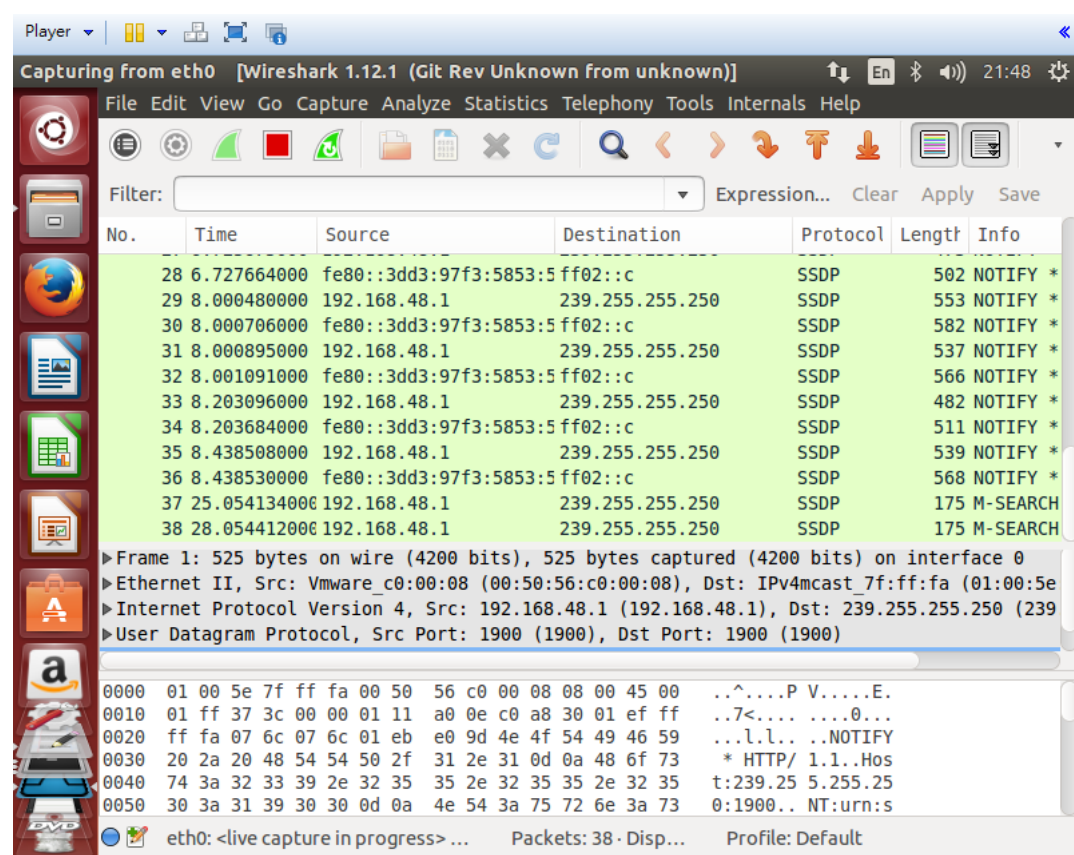


figure 5

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。

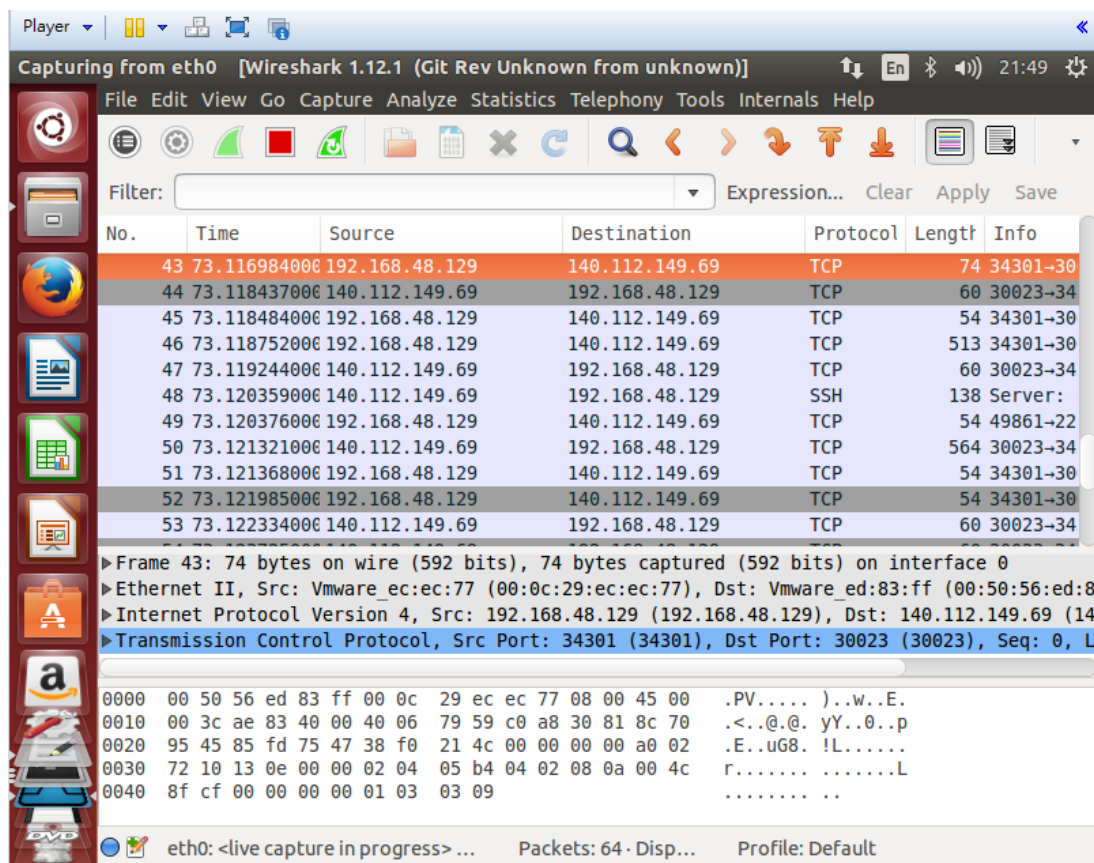


figure 6

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)

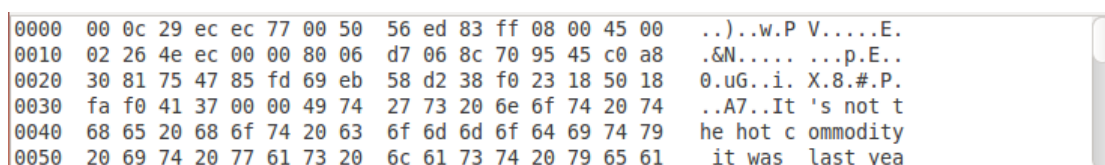


figure 7

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)

No.	Time	Source	Destination	Protocol	Length	Info
41	37.064554000	192.168.48.1	239.255.255.250	SSDP	175	M-SEARCH
42	40.064785000	192.168.48.1	239.255.255.250	SSDP	175	M-SEARCH
43	73.116984000	192.168.48.129	140.112.149.69	TCP	74	34301-30
44	73.118437000	140.112.149.69	192.168.48.129	TCP	60	30023-34
45	73.118484000	192.168.48.129	140.112.149.69	TCP	54	34301-30
46	73.118752000	192.168.48.129	140.112.149.69	TCP	513	34301-30

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)

No.	Time	Source	Destination	Protocol	Length	Info
43	73.116984000	192.168.48.129	140.112.149.69	TCP	74	34301-30
44	73.118437000	140.112.149.69	192.168.48.129	TCP	60	30023-34
45	73.118484000	192.168.48.129	140.112.149.69	TCP	54	34301-30
46	73.118752000	192.168.48.129	140.112.149.69	TCP	513	34301-30
47	73.119244000	140.112.149.69	192.168.48.129	TCP	60	30023-34
48	73.120359000	140.112.149.69	192.168.48.129	SSH	138	Server:
49	73.120376000	192.168.48.129	140.112.149.69	TCP	54	49861-22
50	73.121321000	140.112.149.69	192.168.48.129	TCP	564	30023-34

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)

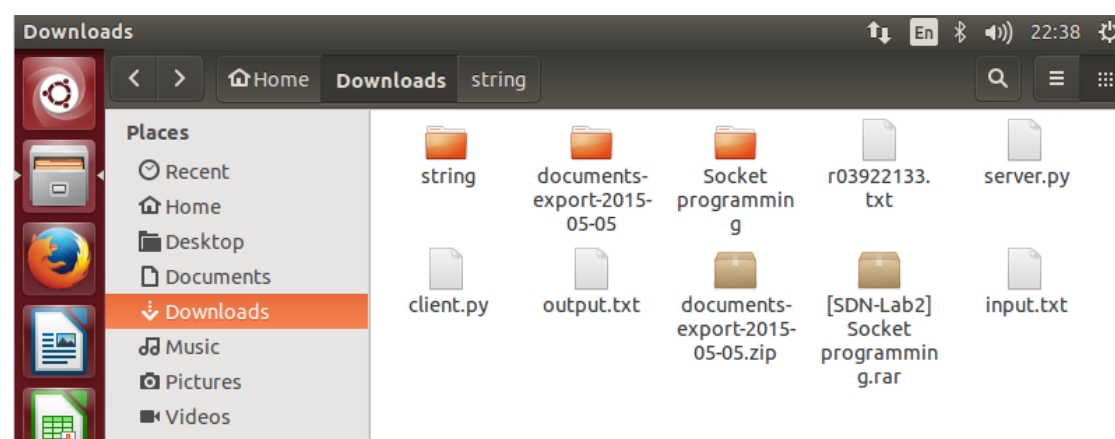


figure 10

3. Reference

1. http://www.pcnet.idv.tw/pcnet/network/network_ip_tcp.htm
2. http://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol