**NCTU CN2018 Lab.1-Packet Manipulation via Scapy**

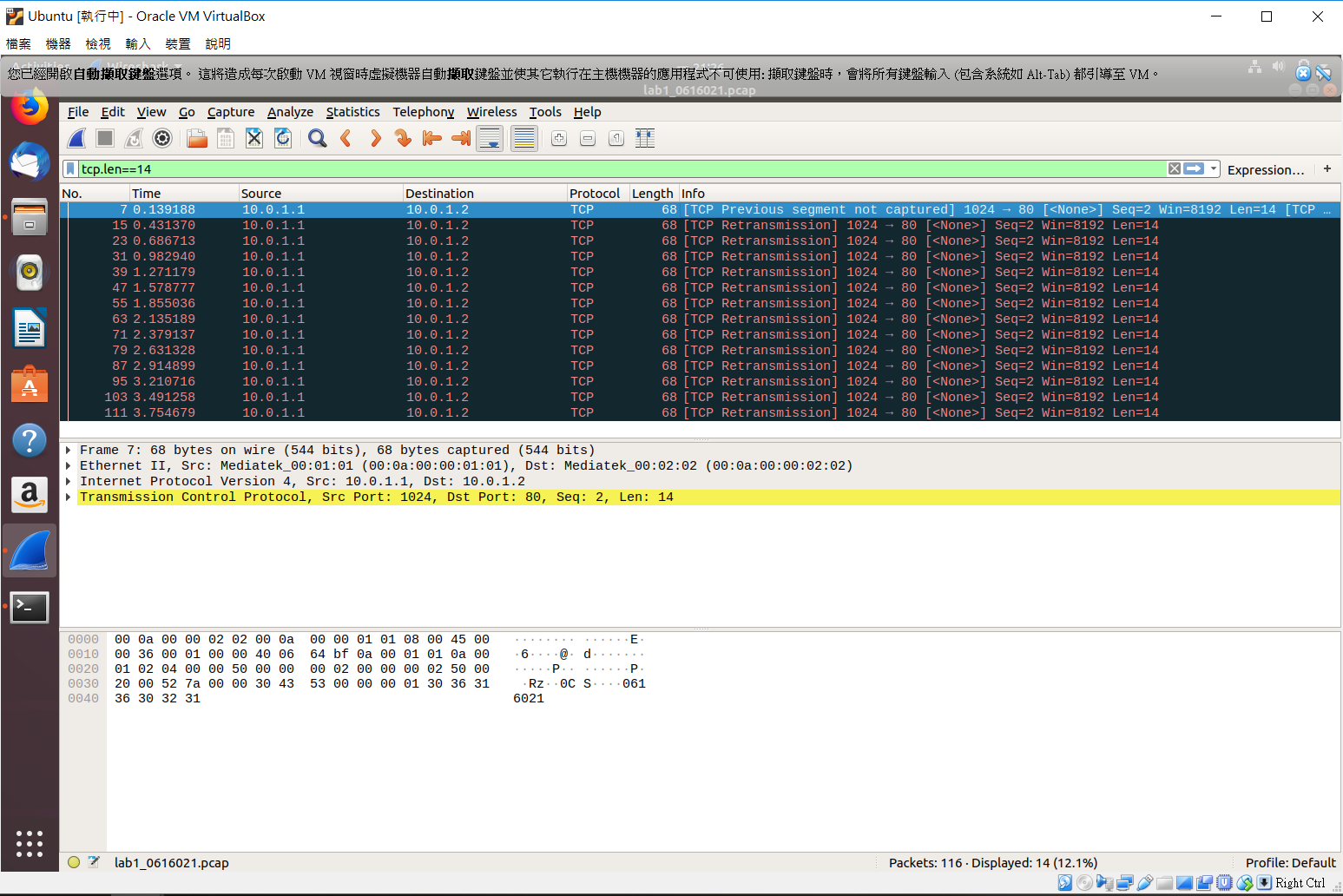
Student name : 陳巧錚 Student ID : 0616021 Department : CS

**Part A. Questions**

1. **What is your command to filter the packet with customized header on Wireshark?**

**Ans :** tcp.len==14

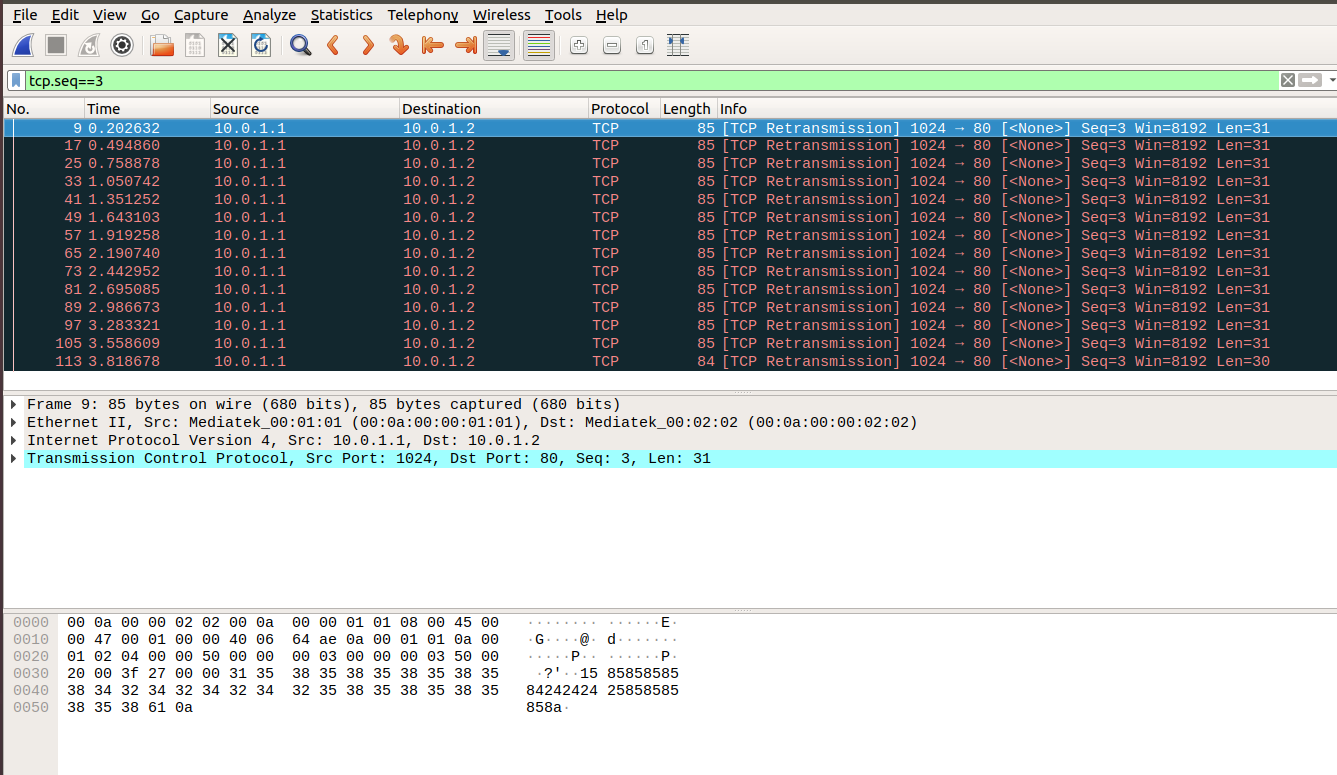
1. **Show the screenshot of filtering the packet with customized header.**



1. **What is your command to filter the packet with “secret” payload on Wireshark?**

**Ans :** tcp.seq==3

1. **Show the screenshot of filtering the packet with “secret” payload.**



**5. Show the result after decoding the “secret” payload.**

**Ans :** 12061601206160

**Part B. Description**

**Task 1 – Environment setup**

* Configure Dockerfile & Build the environment
  + 先將Dockerfile完成
  + 在 ./docker/路徑下建環境

**$ sudo chmod +x main.sh**

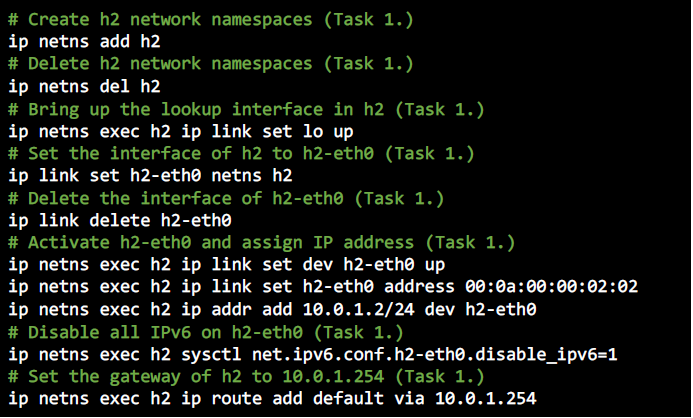
**$ ./main.sh build cn2018 9487**

* 用SSH登入Docker
* Ubuntu

**$ ssh root@0.0.0.0 –p 9487**

**Password: cn2018**

* Create the namespace in ./src/scripts/main.sh

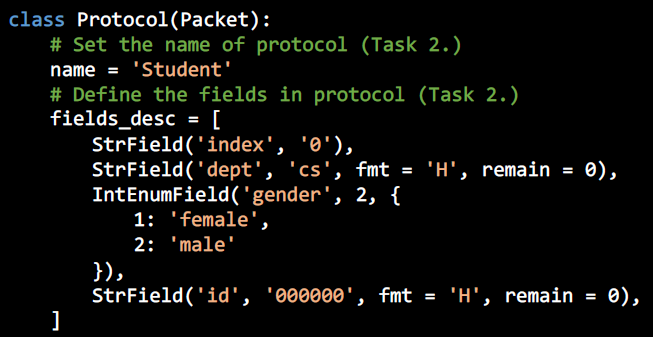


* 執行main.sh建namespace
* **$ chmod +x main.sh**

**$ ./main.sh net**

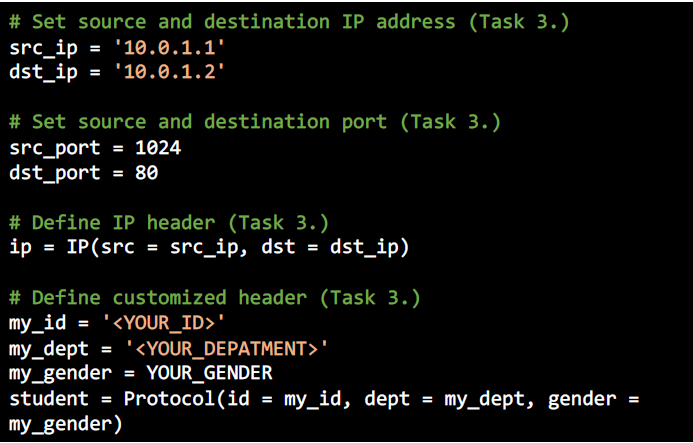
**Task 2 – Define protocol via Scapy**

* Define my protocol
* 把下列的code加入 ./src/Protocol.py，利用Scapy來建構新的協定

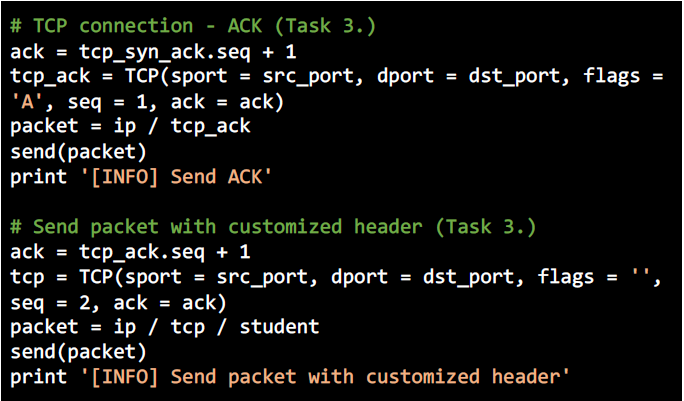


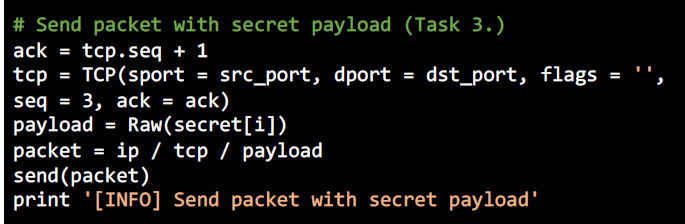
**Task 3 – Send packets**

* 修改./src/sender.py，用來設置來源、目的地的IP位置以及封包的標頭



* 建立封包的連線及設定





**Task 4 – Sniff packets**

* 完成 ./src/receiver.py檔案，用來監聽接收封包

**Task 5 – Run sender and receiver**

* Open tmux with horizontal two panes
* 在./src/路徑下輸入  **$ tmux**
* 按Ctrl-b Shift-% 分出兩個水平的pane
* 用Ctrl-b Arrow-left/right key 切換兩畫面
* 在左邊run namespace h1

**$ ./scripts/main.sh run h1**

* 在右邊run namespace h2

**$ ./scripts/main.sh run h2**

* 傳封包
* 先Run receiver.py(※不能先run sender.py)，用來接收

**h2> python receiver.py**

* 再Run sender.py，用來傳封包

**h1> python sender.py**

* 輸入以下指令show PCAP

**$ tcpdump -qns 0 -X -r <FILENAME>.pcap**

* 最後拿到lab1\_0616021.pcap、recv\_secret.txt兩個檔案，路徑在./src/out/

**Task 6 – Push your files to remote**

* Push image to Docker Hub
  + Create a new image form a container’s changes

**$ sudo docker commit cn2018\_c 0616021/cn2018\_lab1**

* + Login to my Docker registry

**$ sudo docker login**

* + Push an image to a registry

**$ docker push 0616021/cn2018\_lab1**

* Push files to GitHub
  + 設定識別資料

**$ git config --global user.name "chenchiaocheng"**

**$ git config --global user.email "h2252269690313@gmail.com"**

* + 將資料先暫存到staging area, add新增的資料

**$ git add .**

* + 將所有修改過的檔案都commit

**$ git commit –m "Commit lab1 in class”**

* + 更換Git遠端伺服器網址

**$ git remote set-url origin “https://github.com/nctucn/lab1-chenchiaocheng.git”**

* + 上傳master分支到origin伺服器

**$ git push origin master**

**Task 7 – Load PCAP via Wireshark**

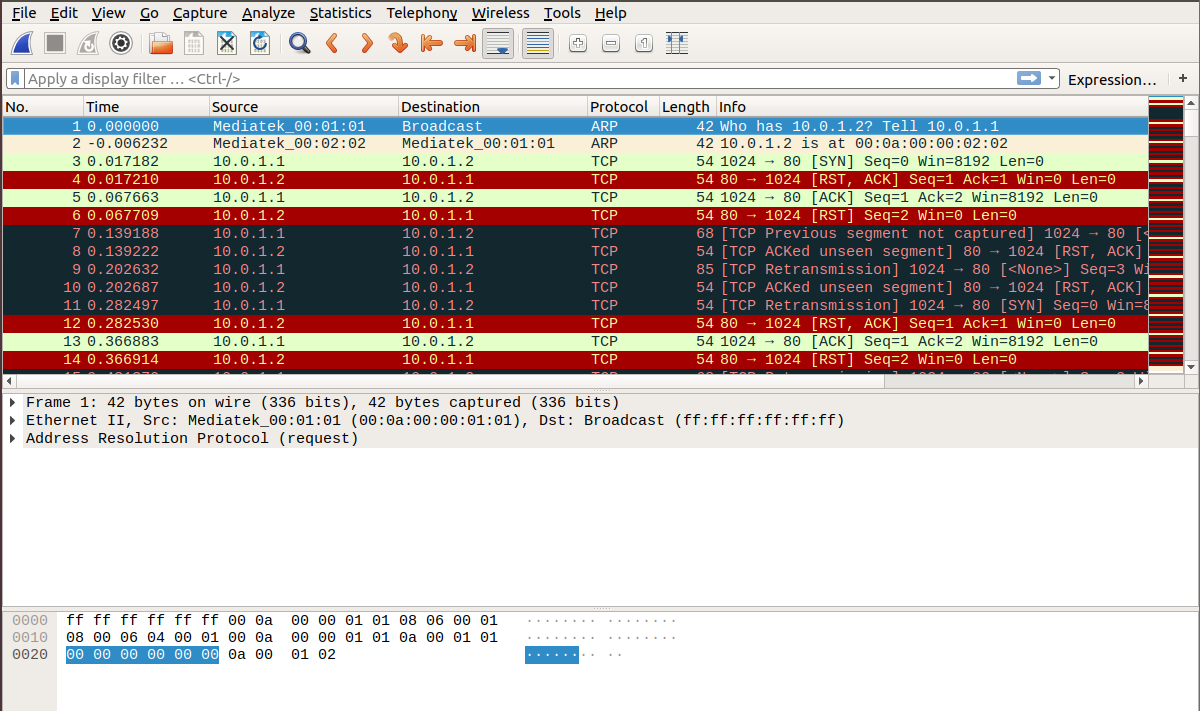
* Download the code from GitHub

**$ git clone “https://github.com/nctucn/lab1-chenchiaocheng.git”**

* Install Wireshark 2.6.3
  + Ubuntu

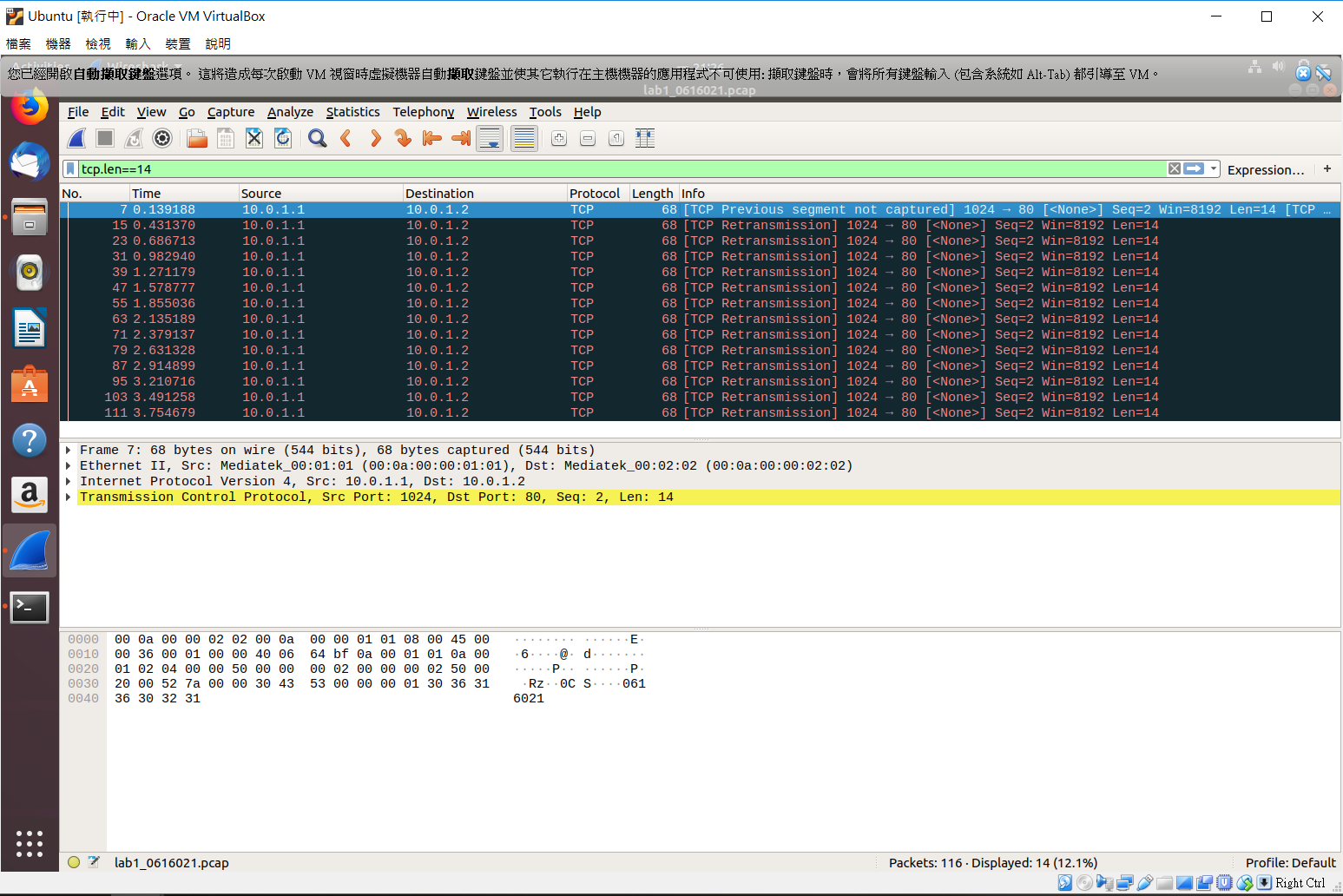
**$ sudo apt-get install wireshark**

* Open the PCAP file using Wireshark
  + Screenshot:

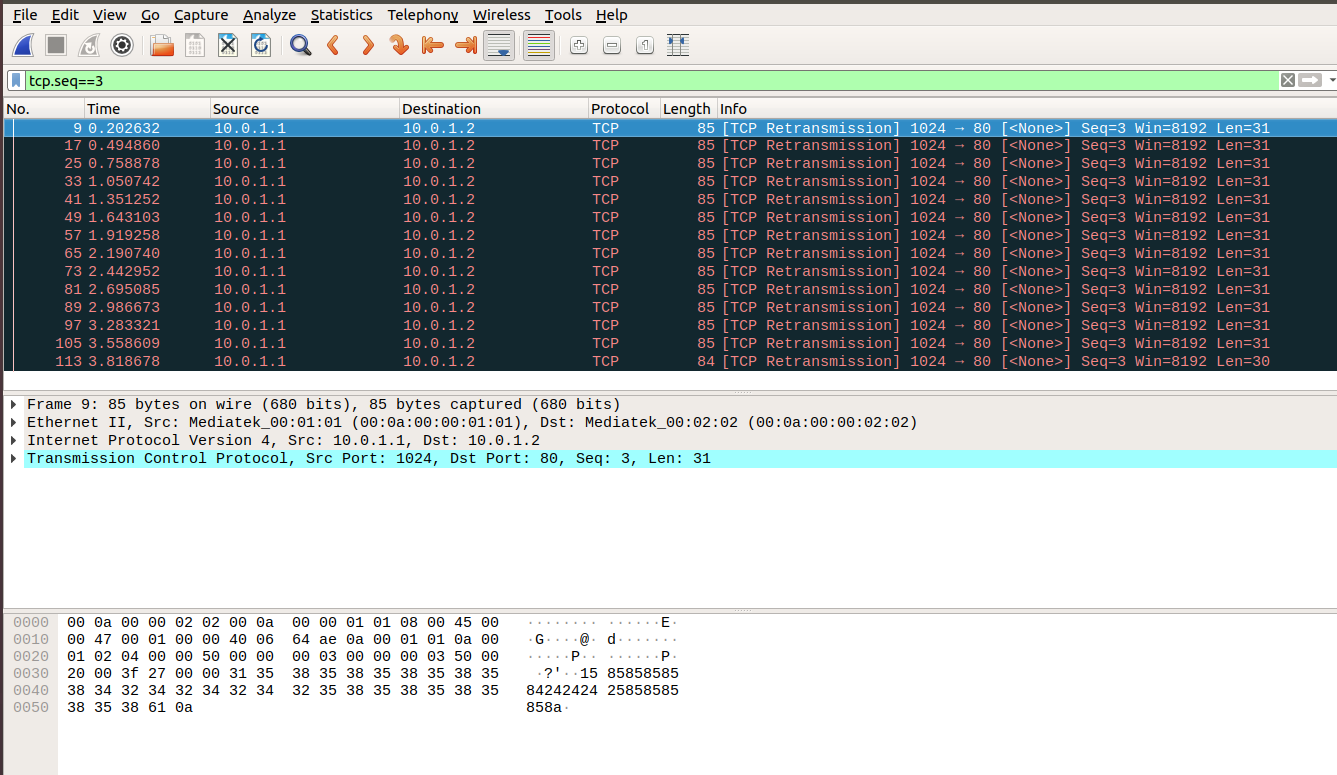


**Task 8 – Filter the target packet**

* Filter the packets of our defined protocol
  + Filter command : tcp.len==14
  + Screenshot:



* Filter the packets of our defined protocol
  + Filter command : tcp.seq==3
  + Screenshot:

****

* What is my secret key? How to find it?

Ans: a. 12061601206160;

b. 把14個secret payload的第一個數字都拉出來，就可以組合成我們要找的

secret key。

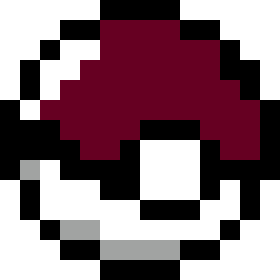
**Task 9 – Decode the secret key**

* Input the secret key into ./src/decoder.py on local machine
* Execute decoder.py

**$ python decoder.py 12061601206160**

* We will get an output file in ./src/out/ called lab1\_0616021.PNG

My result is :



**Part C. Bonus**

1. **What you have learned in this lab?**

學習到如何傳送及接收封包、使用wireshark過濾封包、使用Ubuntu、將檔案傳送到github上、cd ls之類的指令以及要如何在什麼都不懂的情況下，去尋求協助，努力搞懂一切等等，對於我來說這些大多是新的知識，每次操作完總會感到很驚嘆，有種發現新世界的感覺。

1. **What difficulty you have met in this lab?**

因為之前都沒有使用過github、虛擬器、CMD等等，所以花了很多時間在熟悉操作這些，在lab時對於很多指令也不太了解，一開始常常會不知道該將指令打在哪裡。Lab1時在課堂上把前面的部分做完了，但是最後只傳了src的資料夾，所以後來回去時，又重新做了一遍，還因為一個小地方打錯字，de了超久的bug。另外，不知道甚麼原因，我沒辦法將檔案傳到github上(目前還是沒辦法)，打開github一直出現404 Page not found，希望它等等會成功。在安裝Ubuntu時也花了很長的時間，還好有大神朋友在旁邊協助指點我，不然我應該會裝得更久。這個lab的過程就是一直上網搜尋神奇的指令，然後把它打下去看看發生什麼變化，還會經歷很多旁人沒有碰到的突發狀況，充滿了意外及收穫。