NCTU CN2018 Lab. 1 – Packet Manipulation via Scapy

Student name: 郭競友 Student ID: 0610025 Department: EECS

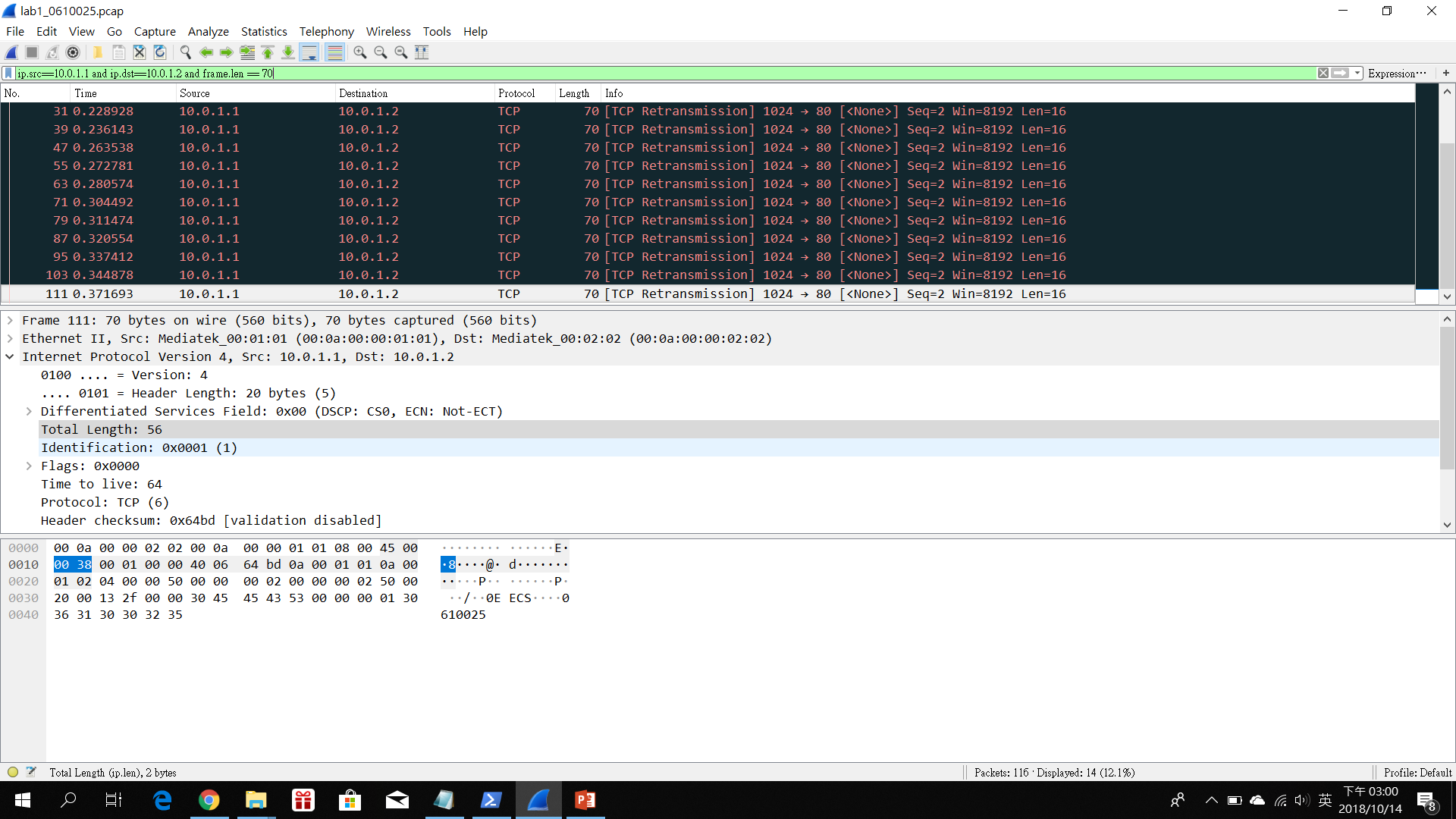
Part A. Question

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

ip.src==10.0.1.1 and ip.dst==10.0.1.2 and frame.len==70

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

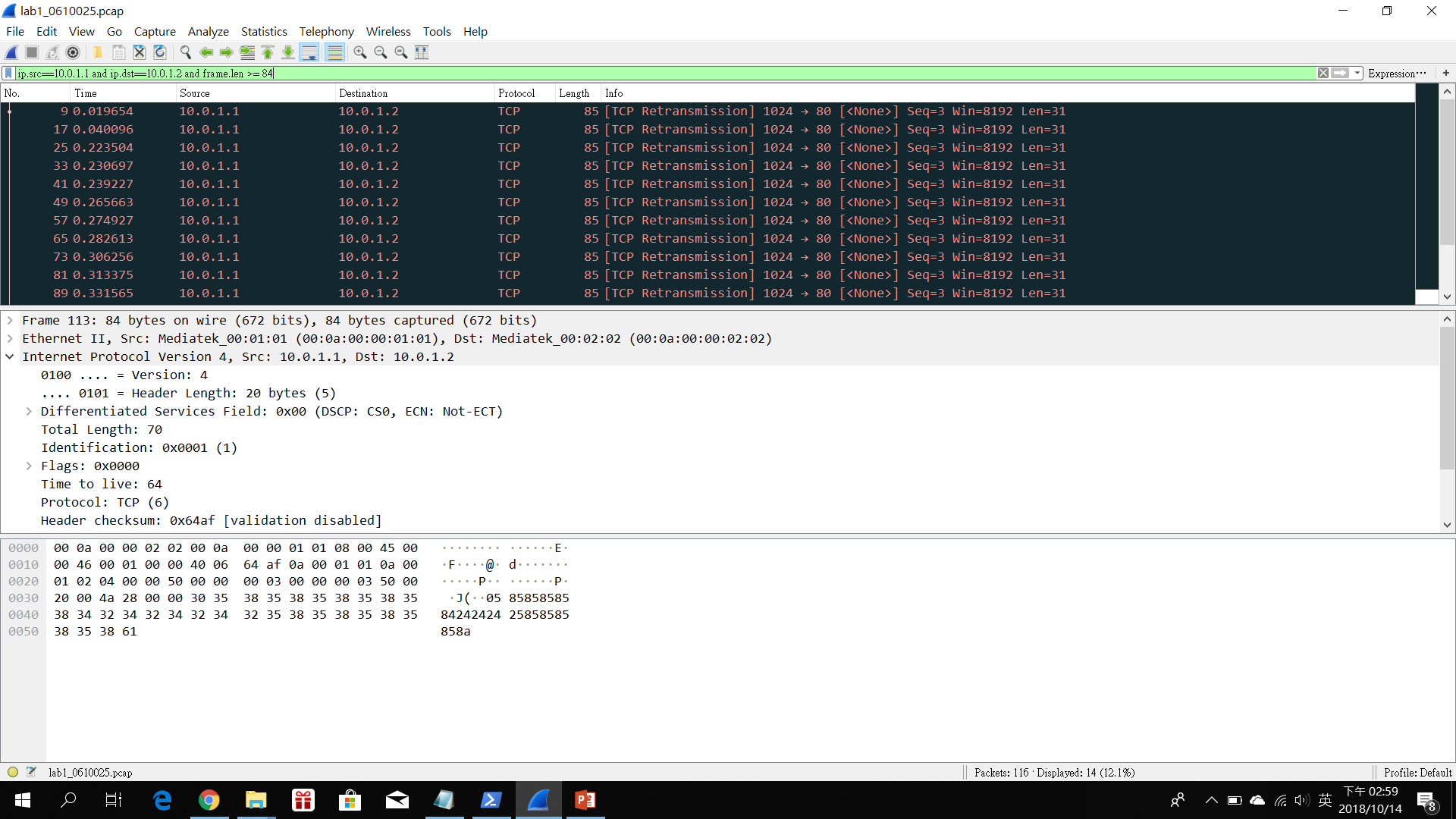
在我回家打開PCAP後發現，我的gender為0，有可能是因為在sender.py中我寫了my\_gender = female，不是設定的語法，導致這個結果。



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

ip.src==10.0.1.1 and ip.dst==10.0.1.2 and frame.len>=84

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



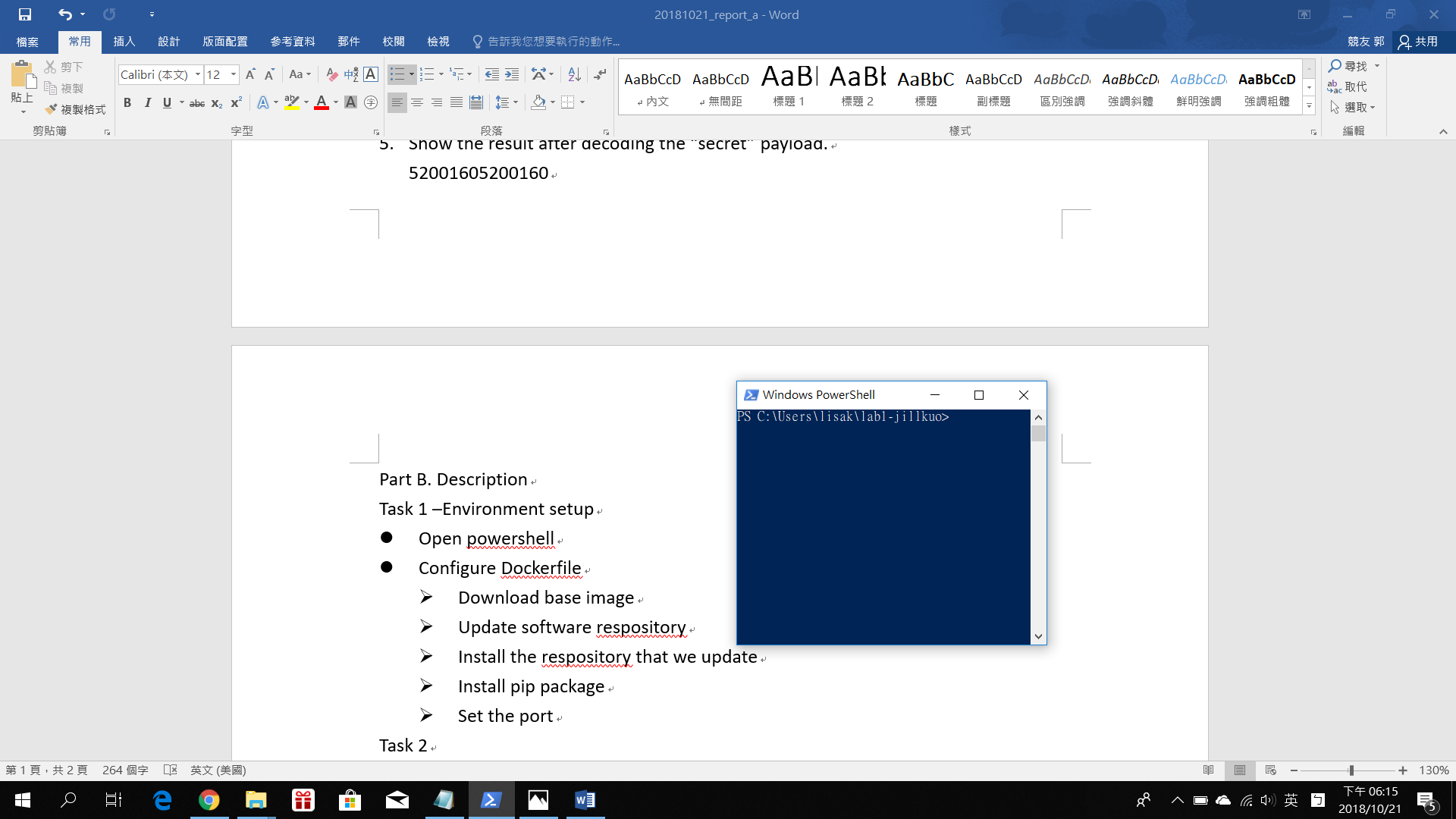
1. Show the result after decoding the “secret” payload.

52001605200160

Part B. Description

Task 1 –Environment setup

* Open powershell



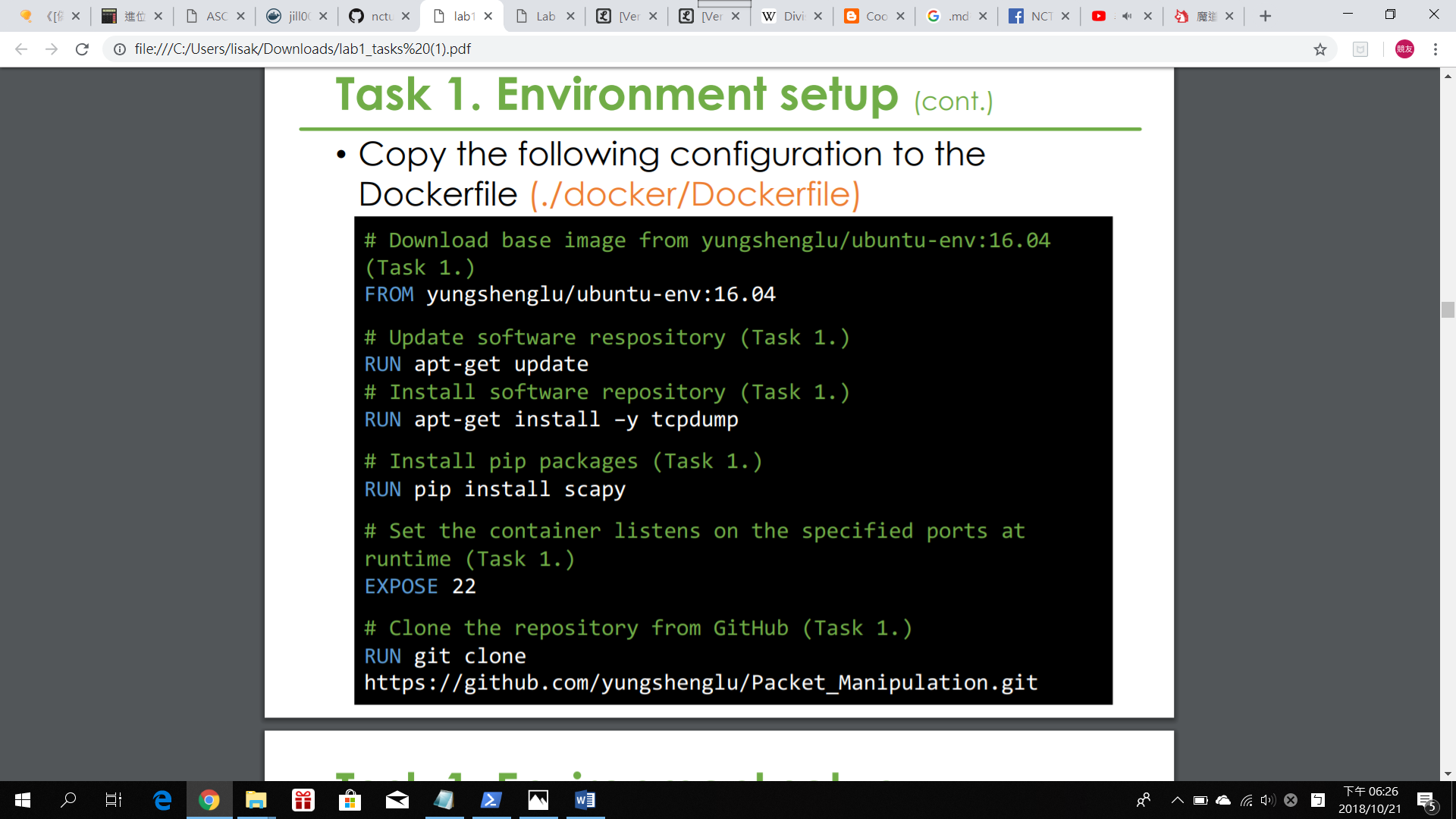
* Configure Dockerfile
* Download base image



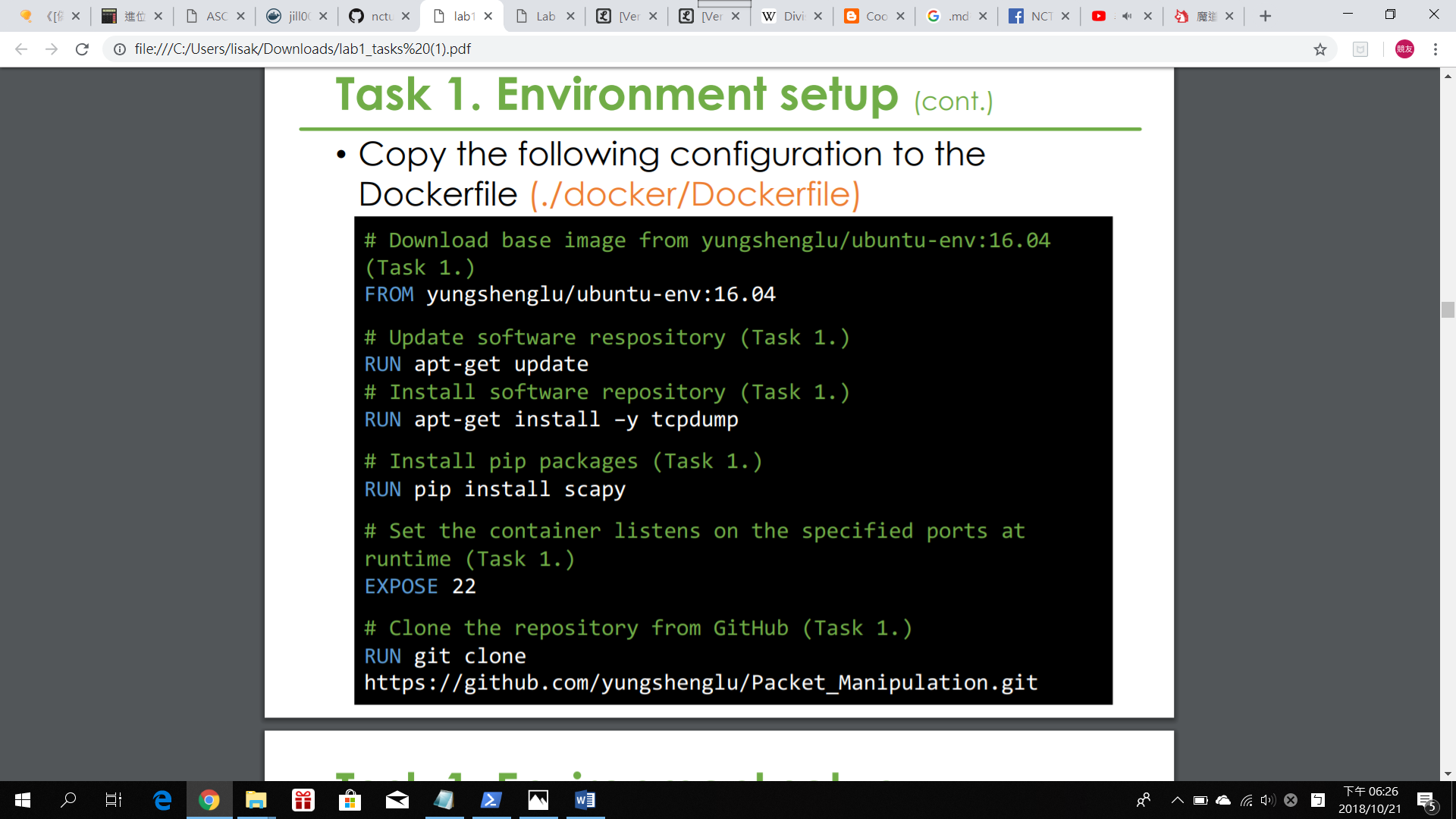
* Update software respository



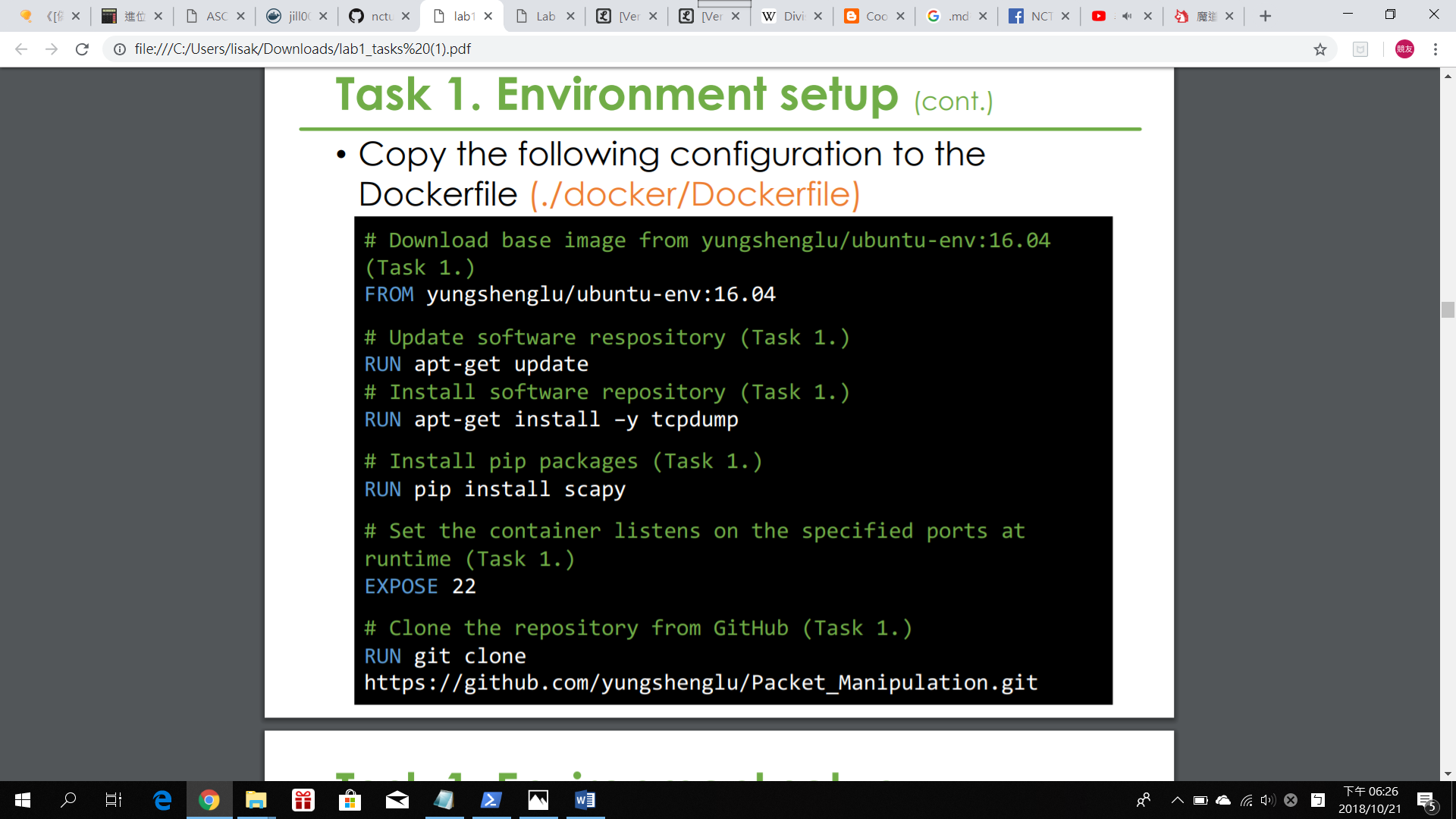
* Install the respository that we update



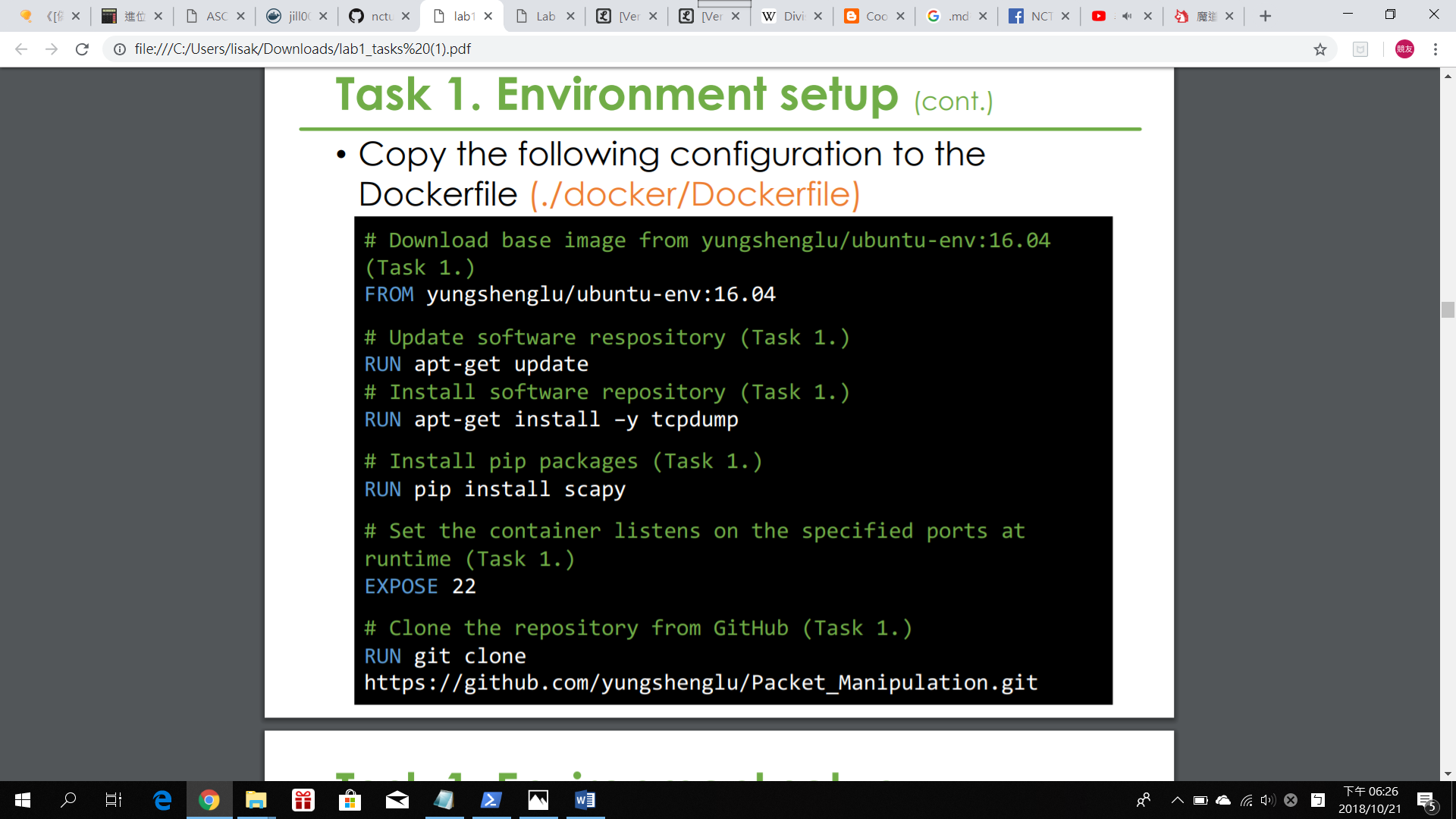
* Install pip package



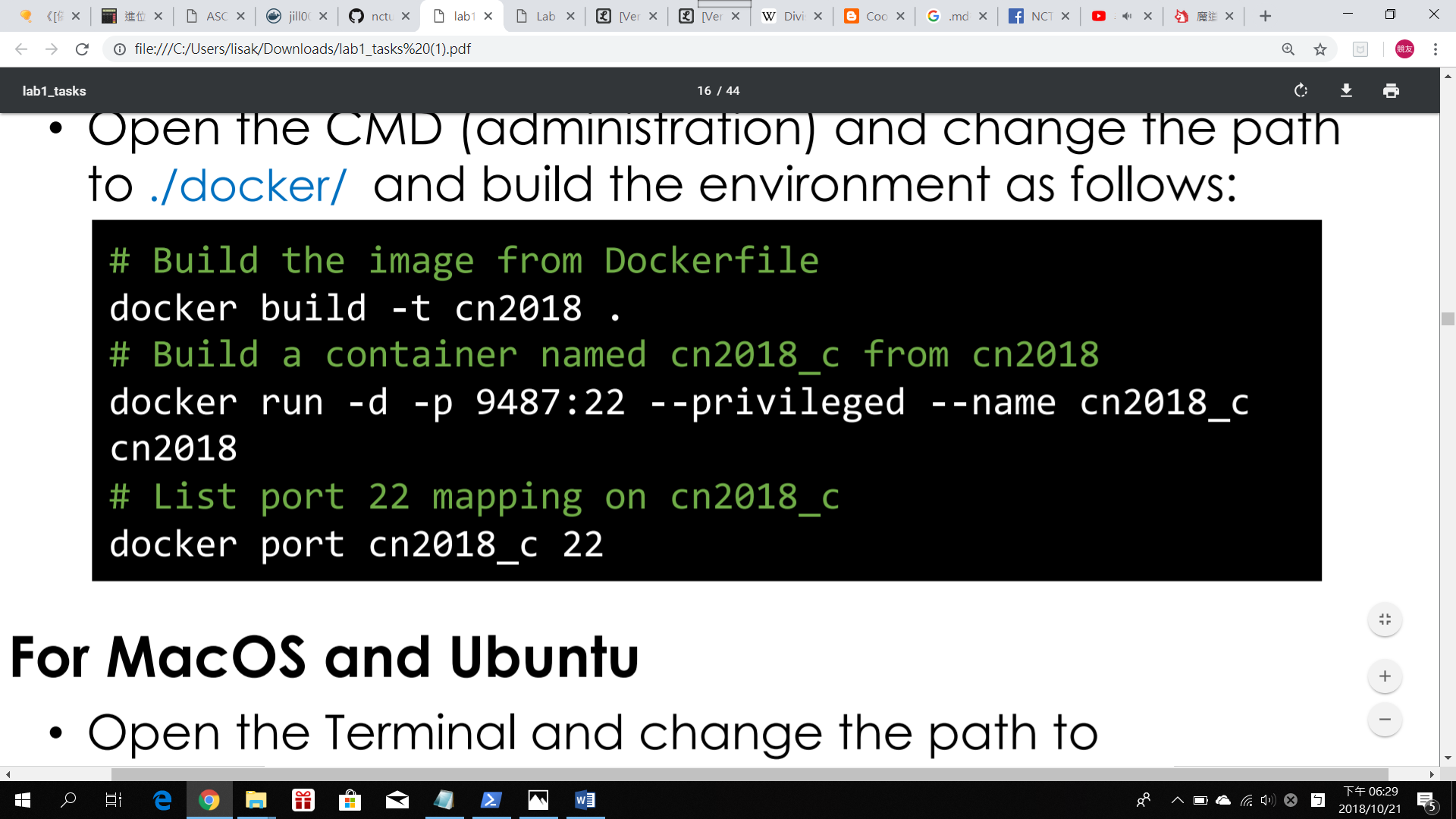
* Set the port



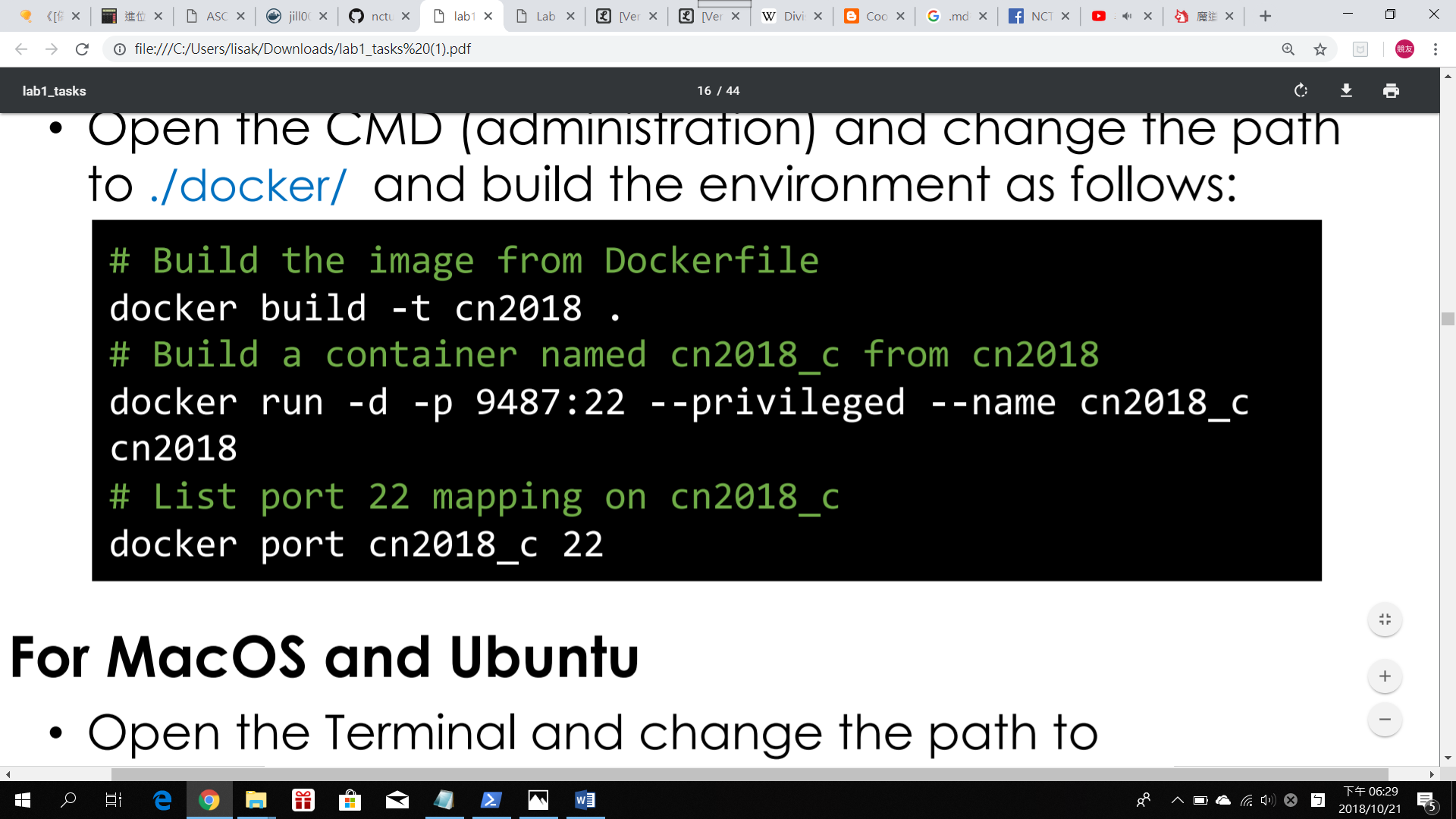
* Download the required files from TA’s GitHub



* Build the container with Dockerfile
* Open the CMD and change the path to ./docker/
* Build a container at cn2018, named cn2018\_c



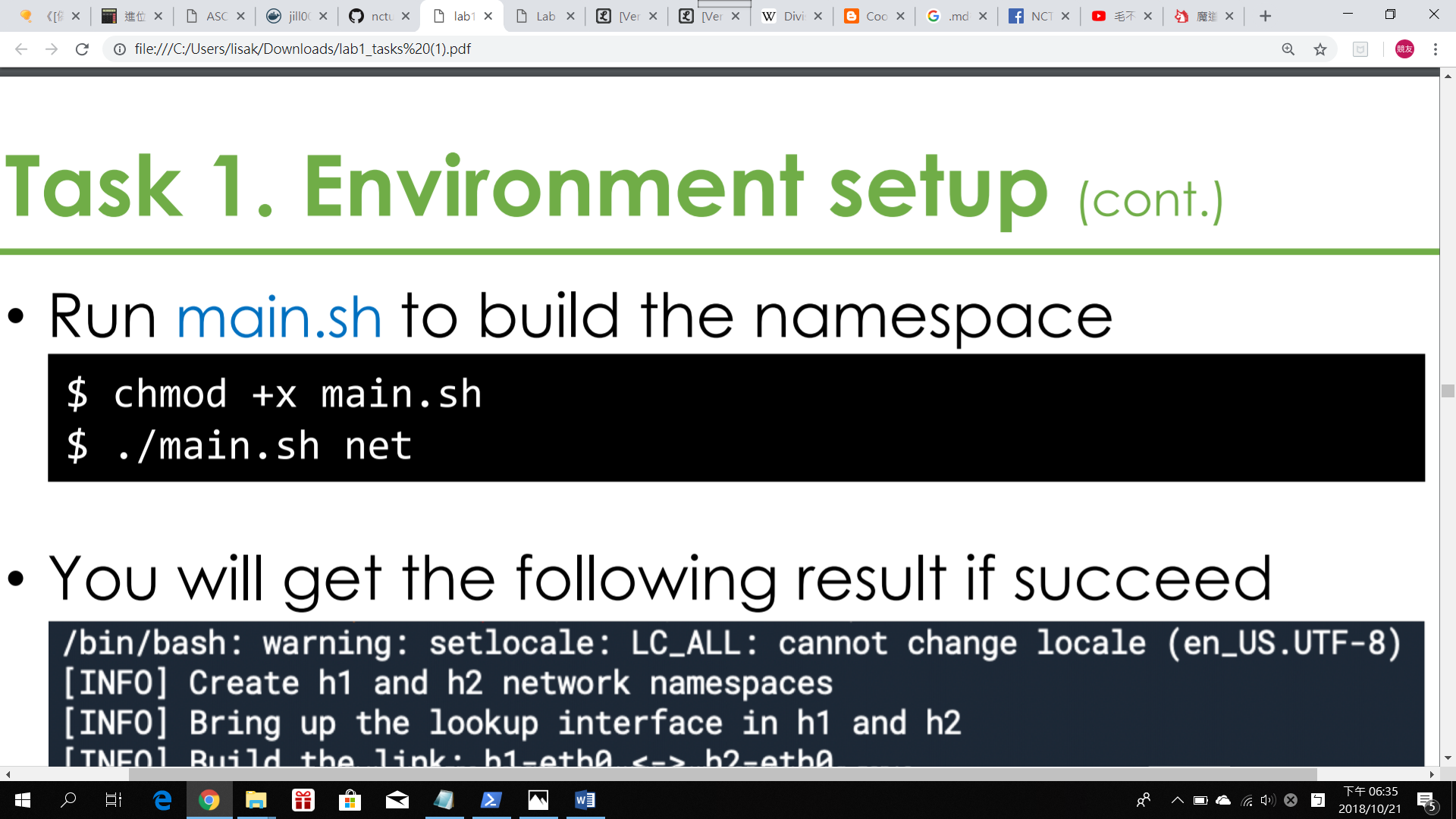
* Set the port 22 to map on cn2018\_c

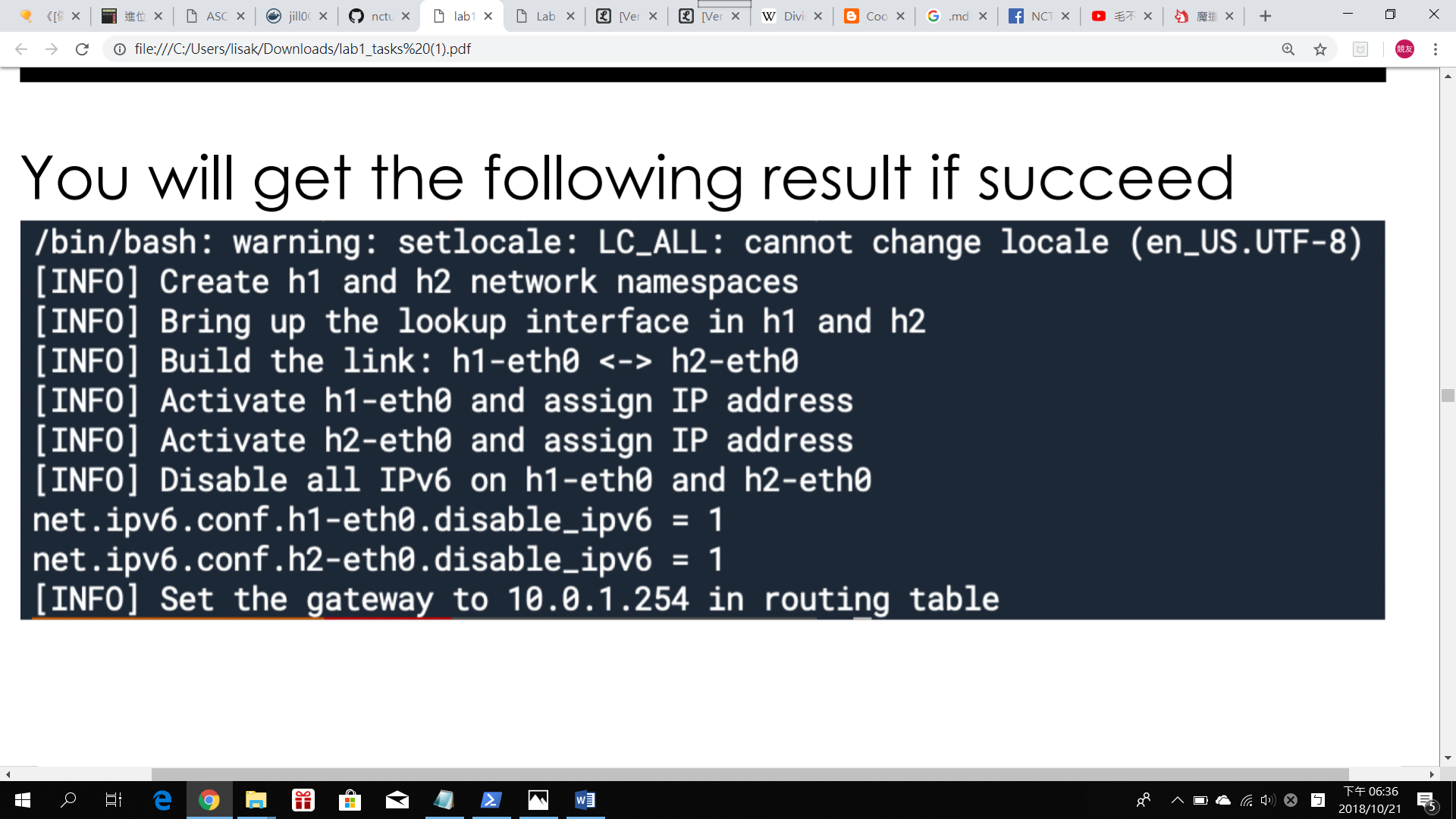


* Run PieTTY
* IP: given by TA on the lab
* Port: 9487
* Login: root, Password: cn2018
* Create namespace, h1(sender) and h2(receiver), in main.sh (finish main.sh)

將路徑設為./src/scripts並輸入vim main.sh來編輯檔案，按i開始編輯，將投影片中的code填入mash.sh正確的位置，再按ESC結束編輯，輸入:wq離開vim。

* Run main.sh



如果結果與下圖不同就是code錯了。

Task 2 –Define protocol via Scapy

* Define protocol

將路徑設為./src/並輸入vim Protocol.py來編輯檔案，按i開始編輯，將投影片中的code填入Protocol.py正確的位置，且要注意縮排(因為是用python)，再按ESC結束編輯，輸入:wq離開vim。

Task 3 –Send packets

* Set my own packet header

輸入vim sender.py來編輯檔案，按i開始編輯，將投影片中的code填入sender.py正確的位置，且要注意縮排(因為是用python)，再按ESC結束編輯，輸入:wq離開vim。

Task 4 –Sniff packets

* Sniff packets

輸入vim receiver.py來編輯檔案，按i開始編輯，將投影片中的code填入receiver.py正確的位置，且要注意縮排(因為是用python)，再按ESC結束編輯，輸入:wq離開vim。

Task 5 –Run sender and receiver

* Run tmux with 2 panes

輸入$ tmux

操作方法：

Ctrl-b + Shift-% 增加horizontal pane

Ctrl-b + Arrow-left/right key 切換pane

輸入exit離開

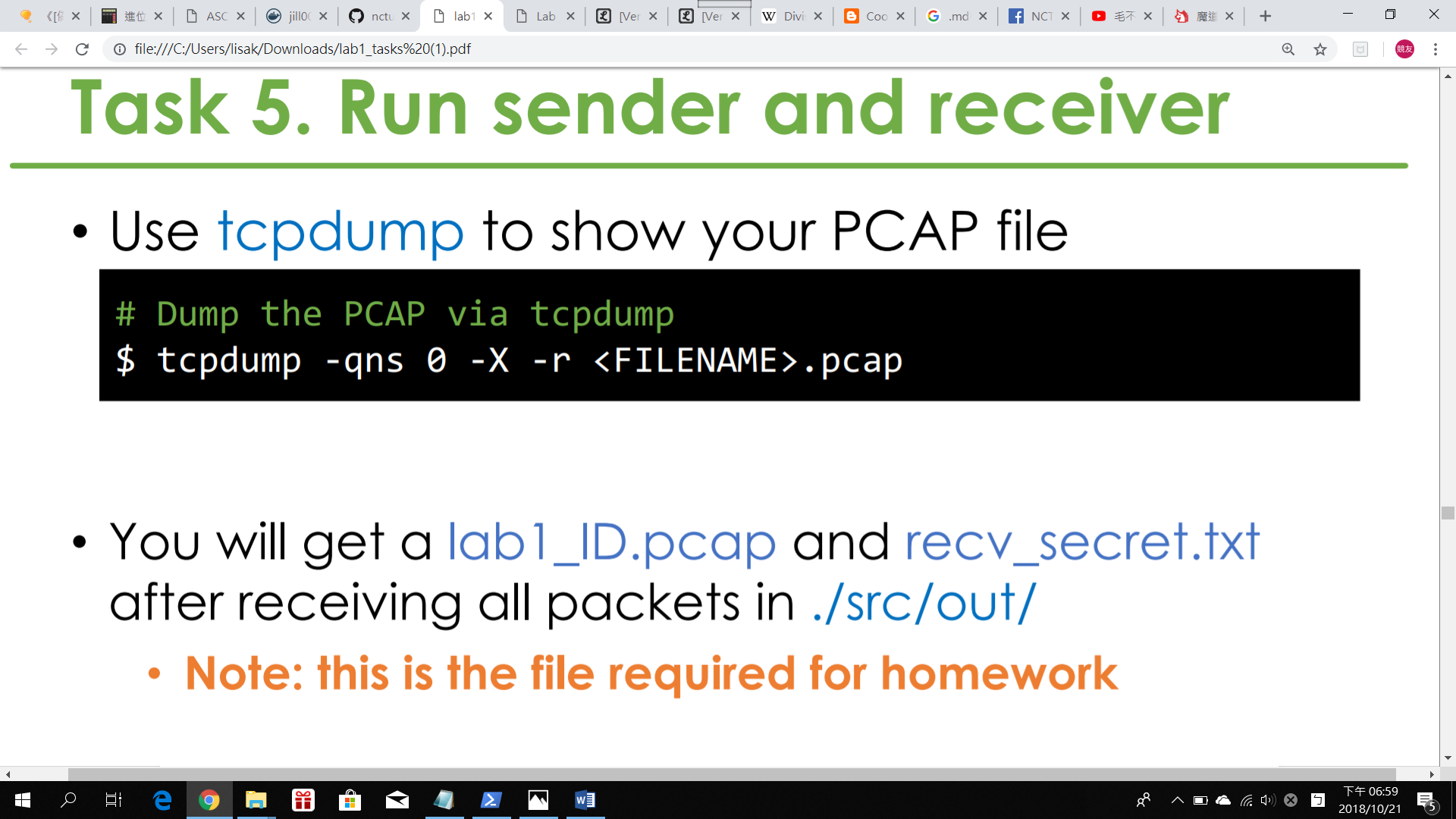
* Run receiver before sender

在left pane輸入$ ./scripts/main.sh run h1，在right pane輸入$ ./scripts/main.sh run h2

接下來**先後順序**很重要，在right pane輸入h2> python receiver.py，然後在left pane輸入h1> python sender.py

若按control\_c就會停止執行。

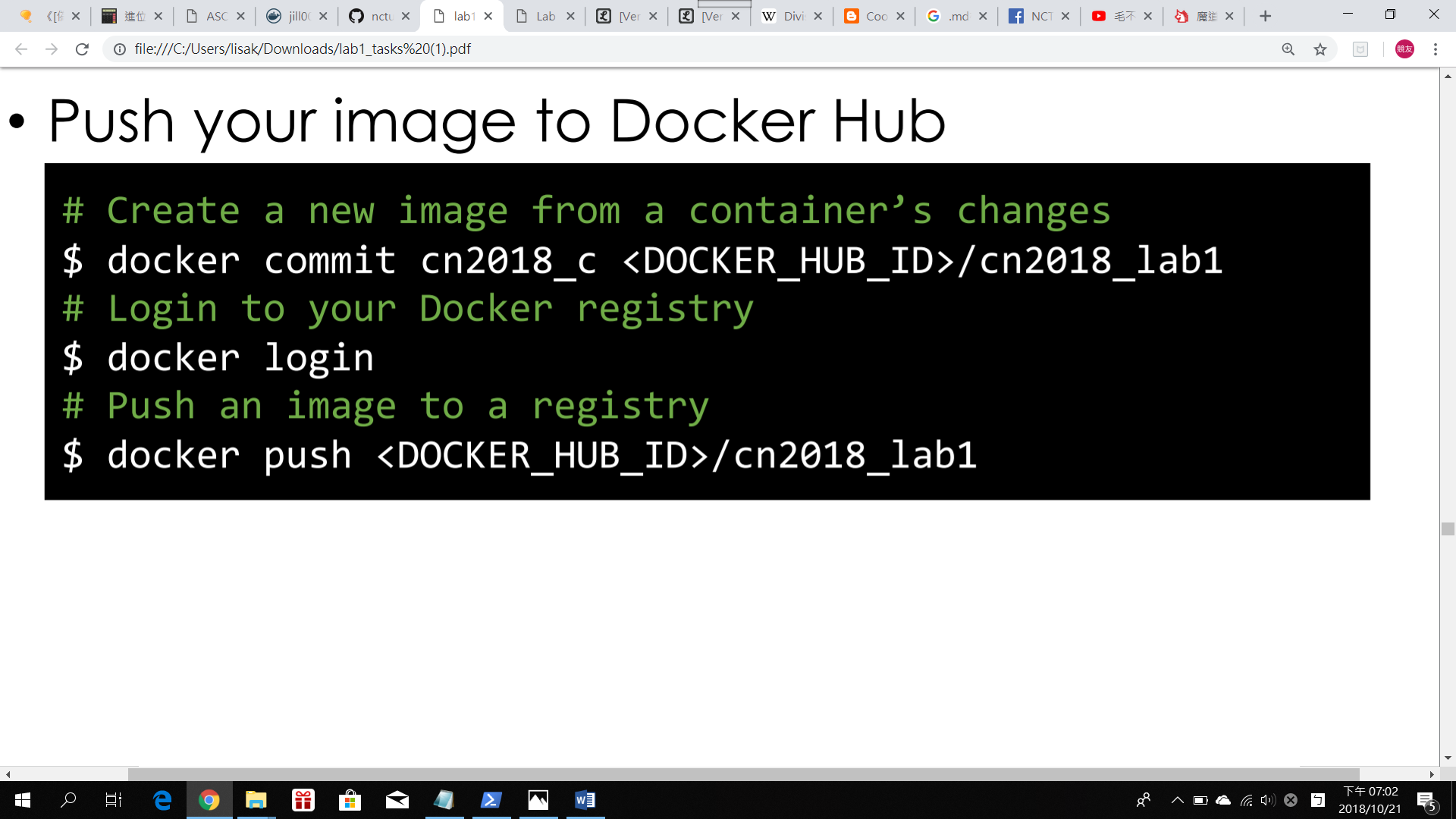
* Show my PCAP file



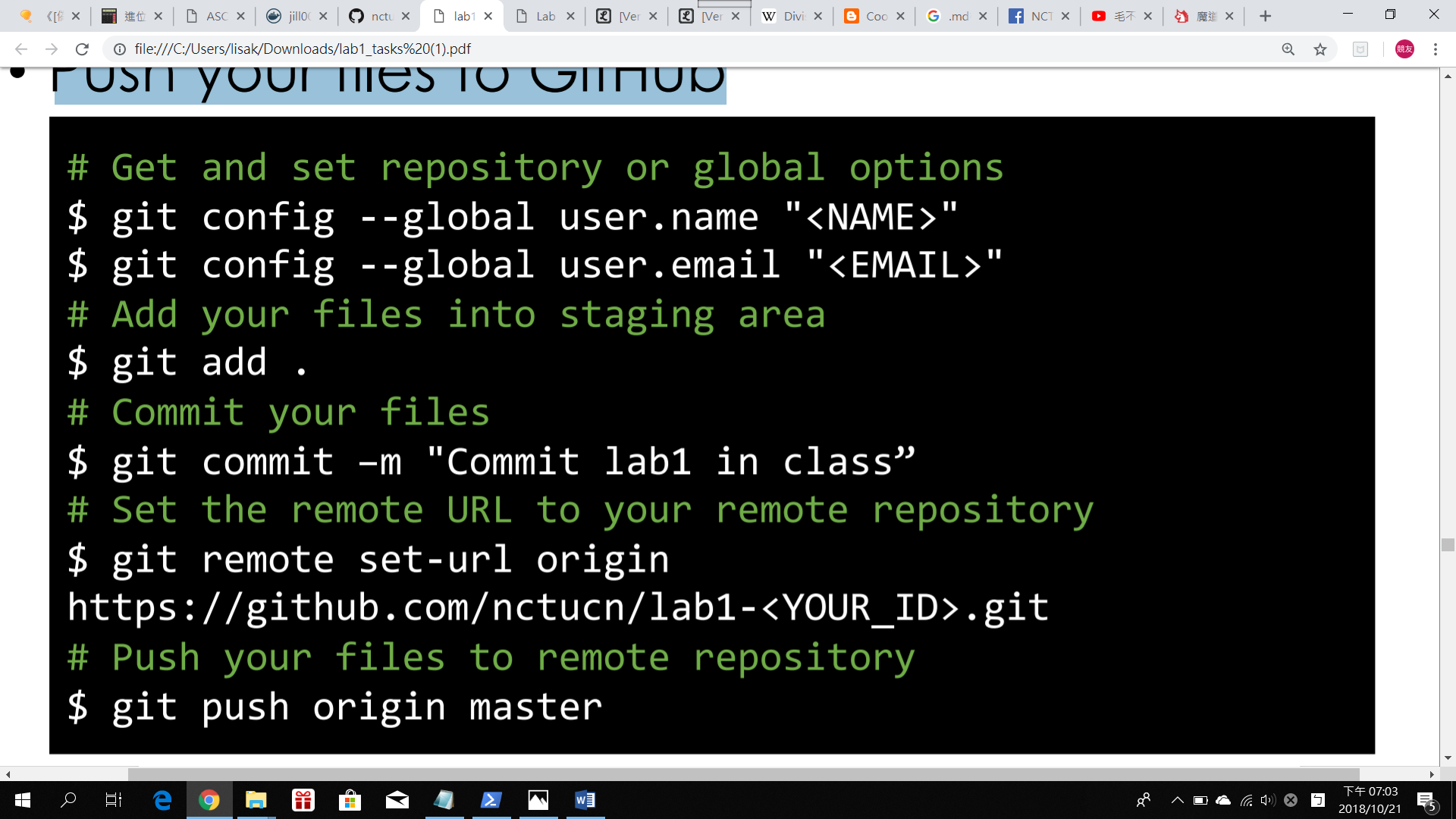
接下來就可以在./src/out/看到lab1\_ID.pcap和recv\_secret.txt

Task 6 –Push your files to remote

* Push the image to Docker Hub



* Push the files to GitHub

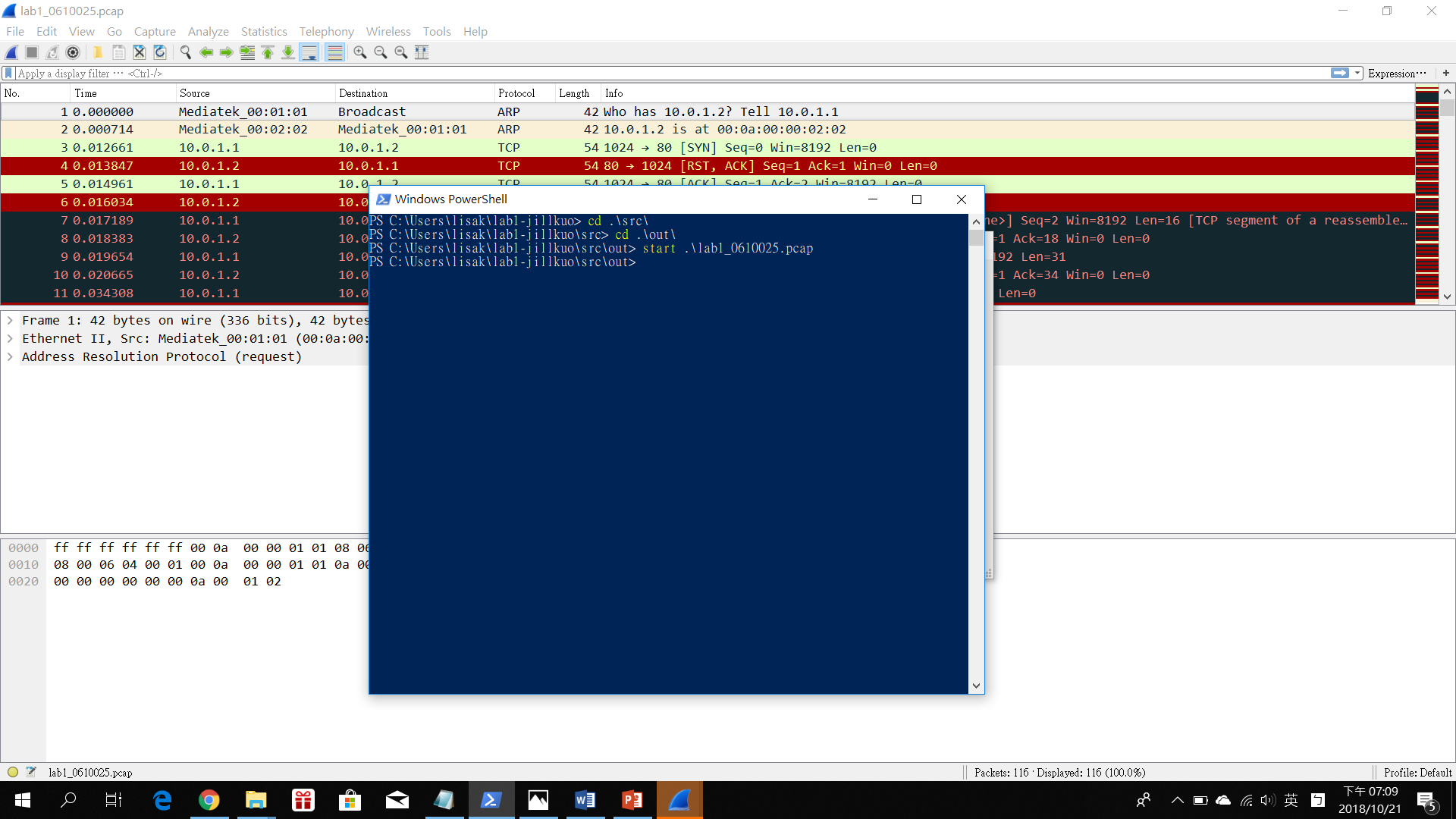


Task 7 –Load PCAP via Wireshark

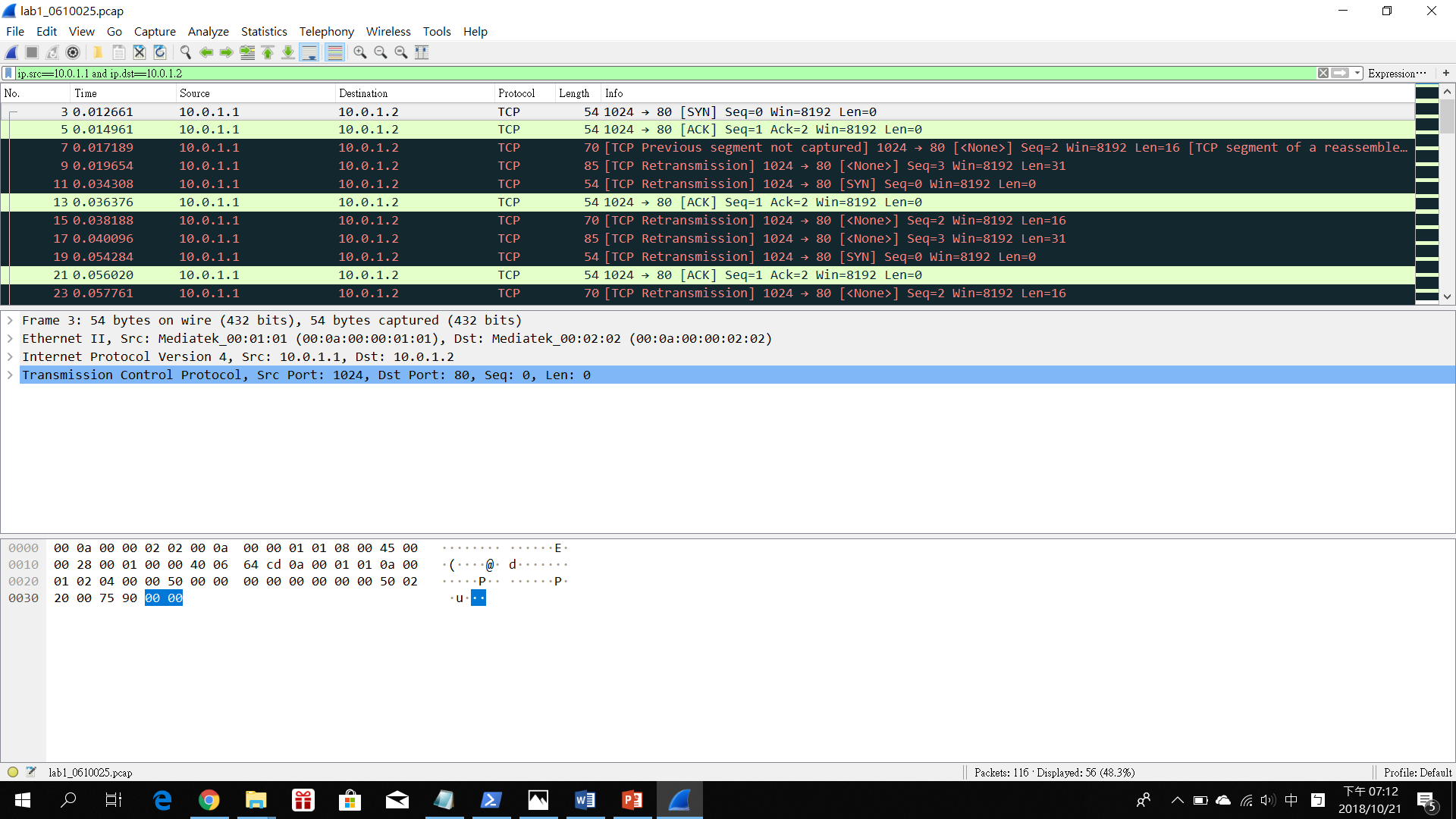
* Download the code from GitHub (use PC)

打開powershell輸入$ git clone https://github.com/nctucn/lab1- jillkuo.git

* Open the PCAP file using Wireshark



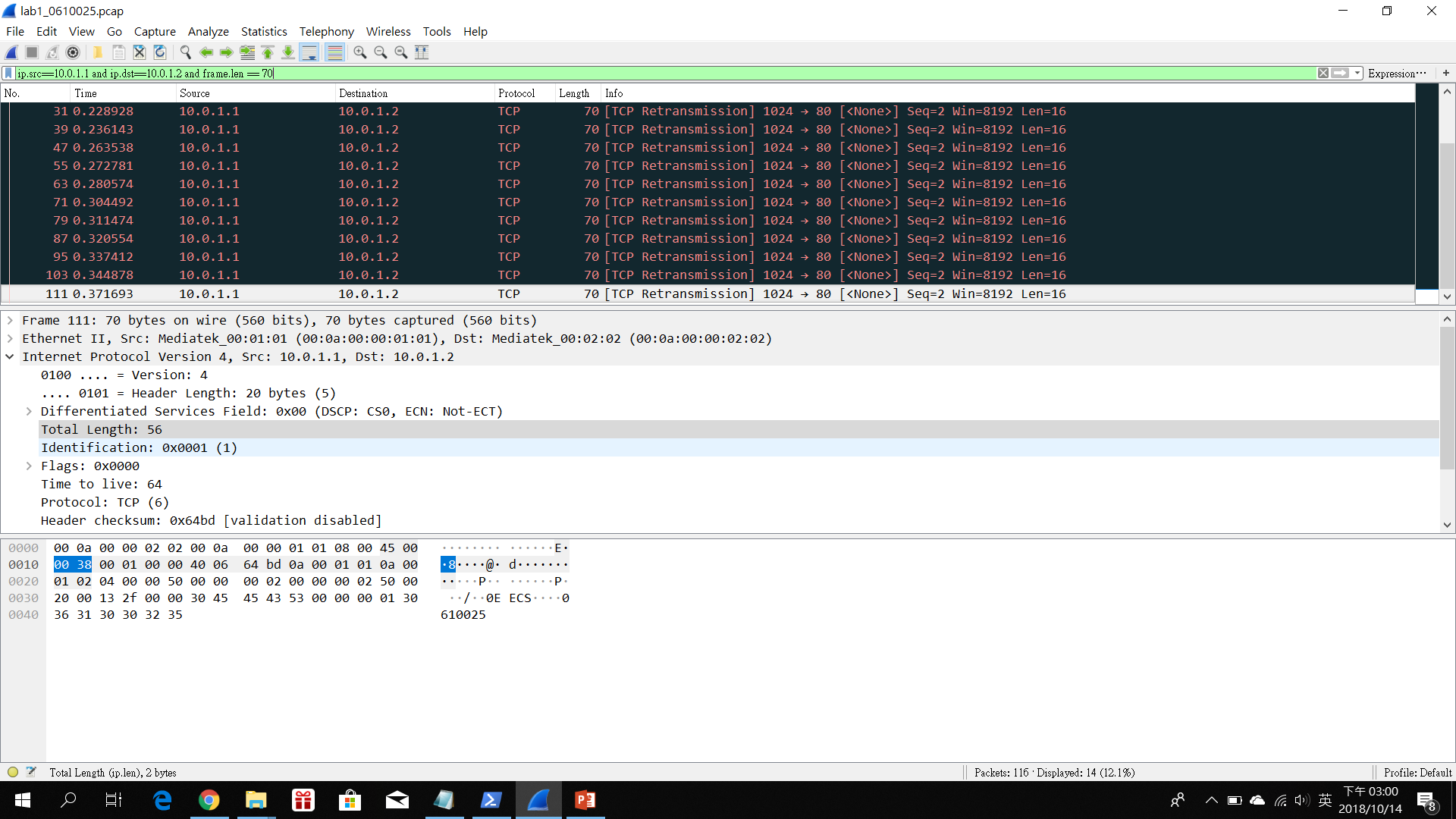
* 我發現當我篩選封包為ip.src==10.0.1.1 and ip.dst==10.0.1.2時，總共有4種封包



Task 8 –Filter the target packet

* Filter the packets of our defined protocol

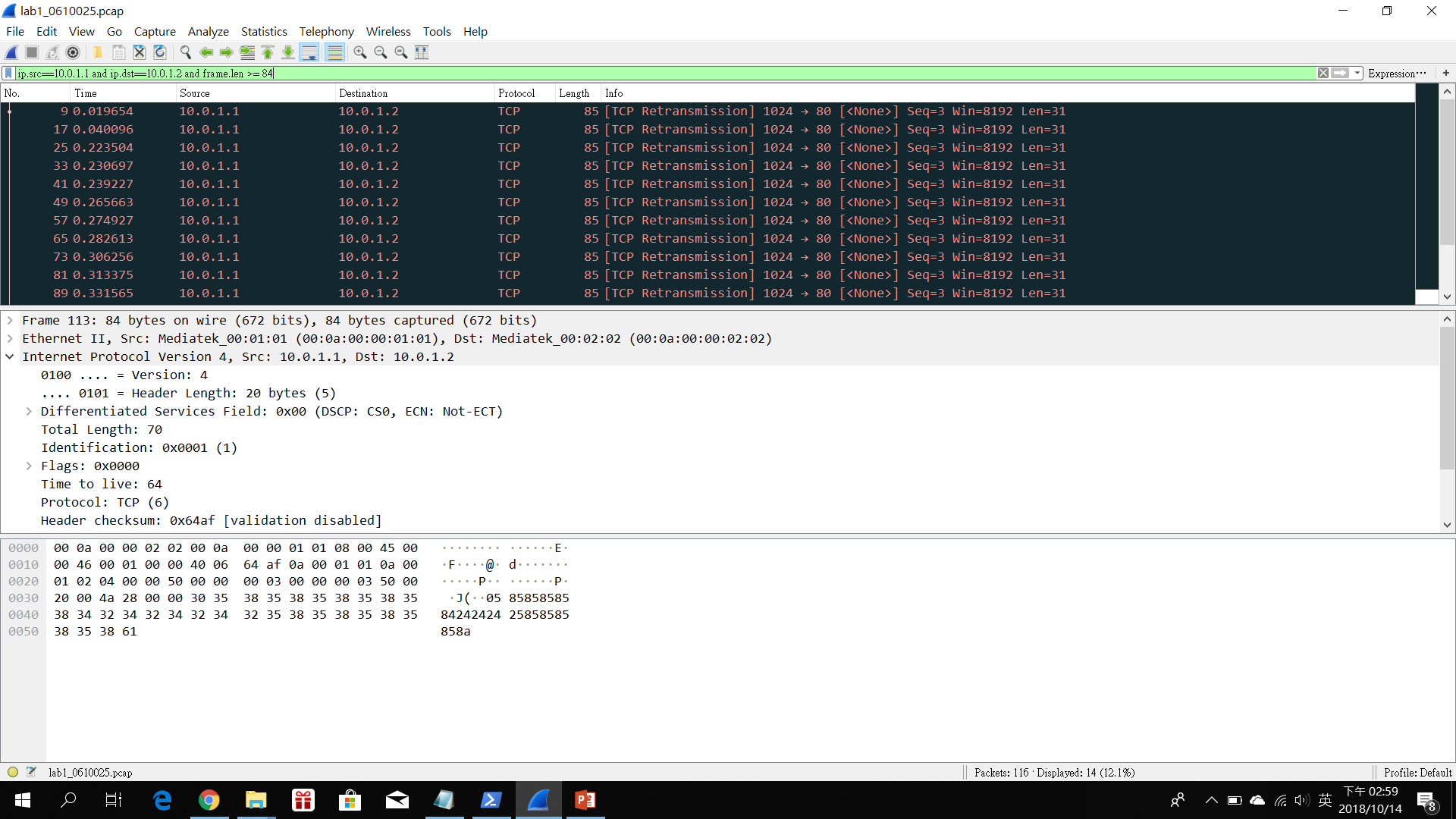
ip.src==10.0.1.1 and ip.dst==10.0.1.2 and frame.len==70



* Filter the packets with the “secret” bits

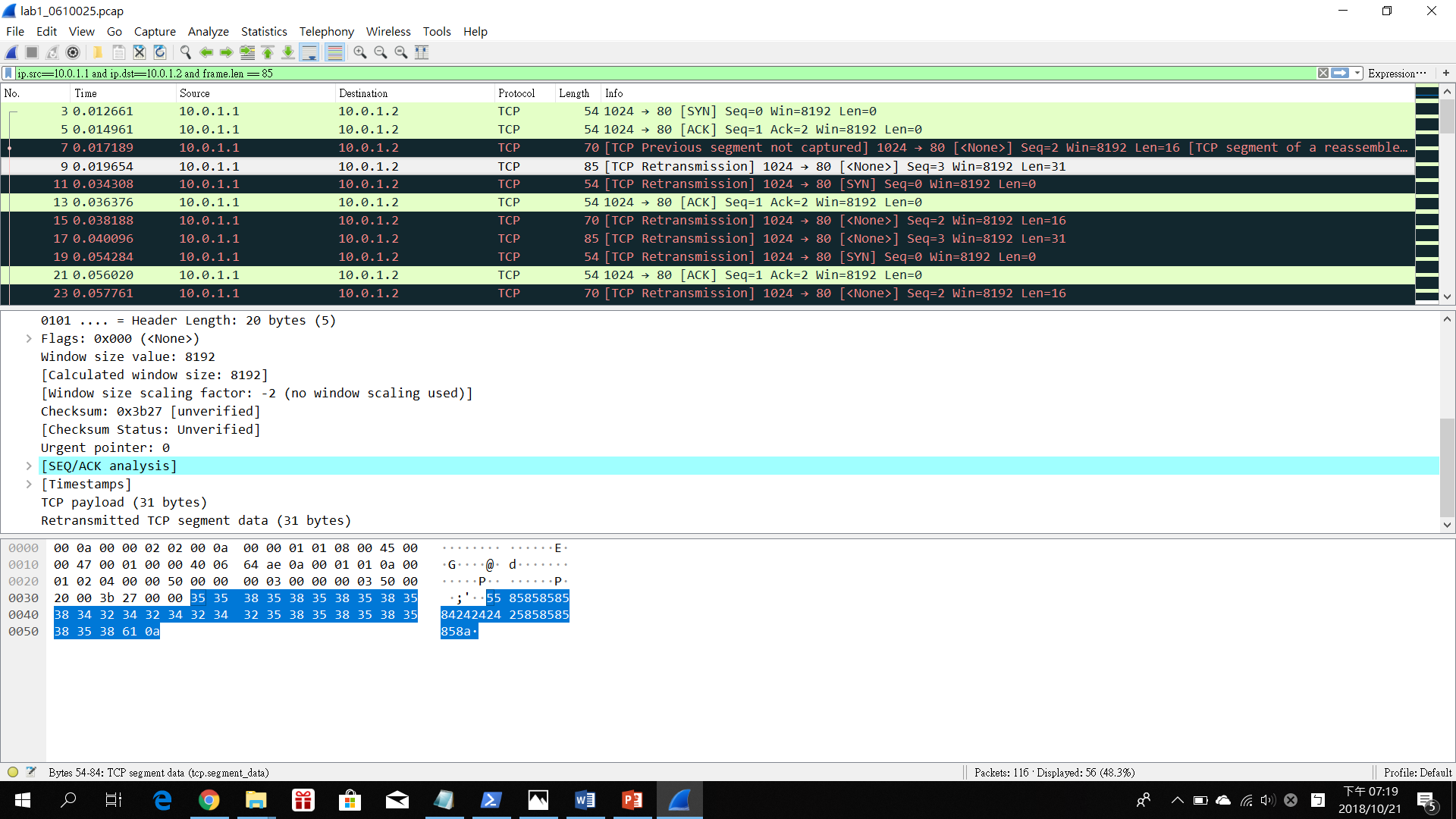
ip.src==10.0.1.1 and ip.dst==10.0.1.2 and frame.len>=84

我原本是設為frame.len==85，但是我發現最後一個secret封包的frame.len==84，因此將條件改為frame.len>=84



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

secret key藏在每一個secret封包中開頭第一個數字



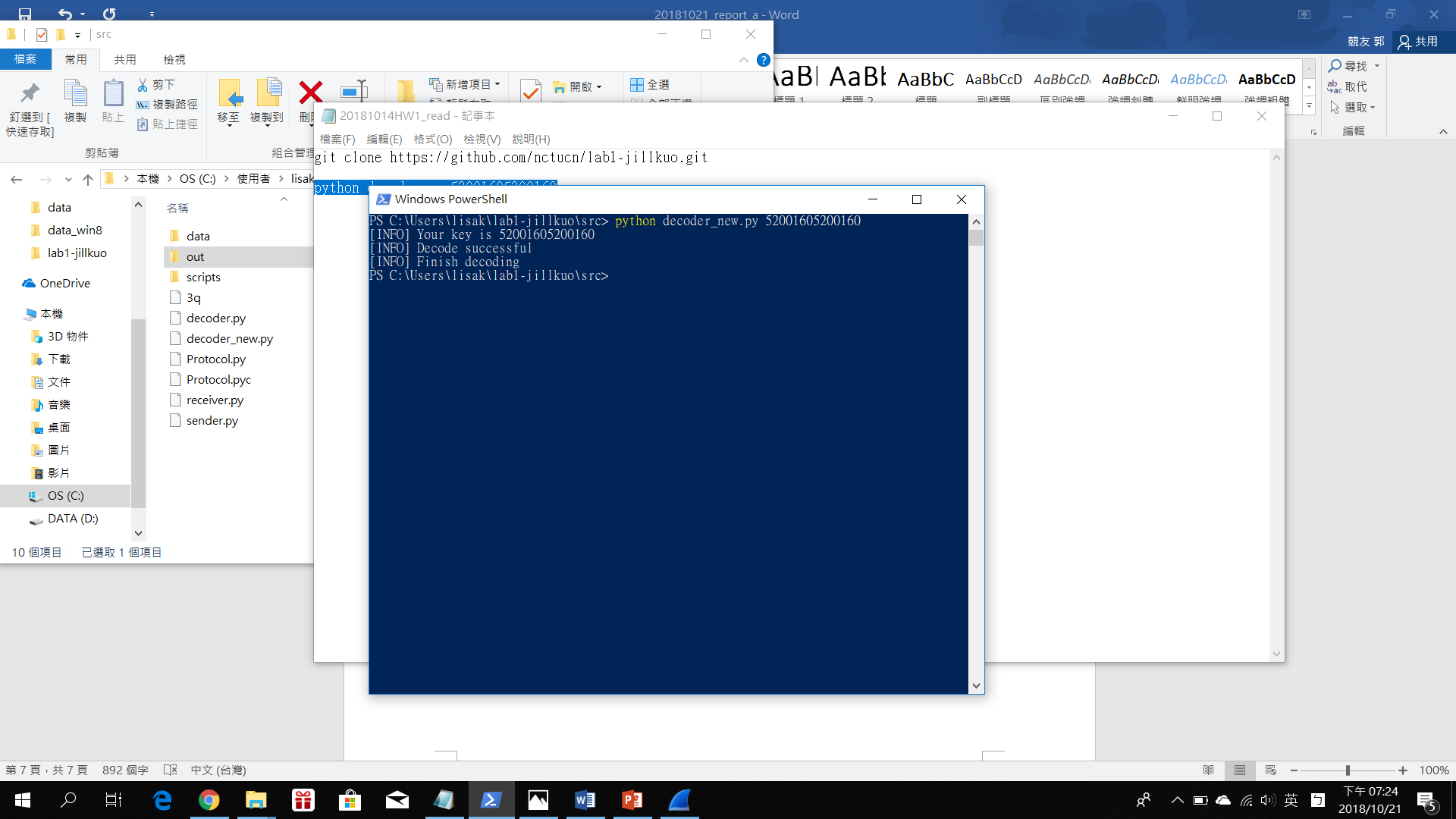
將14個封包按照順去將secret key找出來，最後得到52001605200160

Task 9 –Decode the secret key

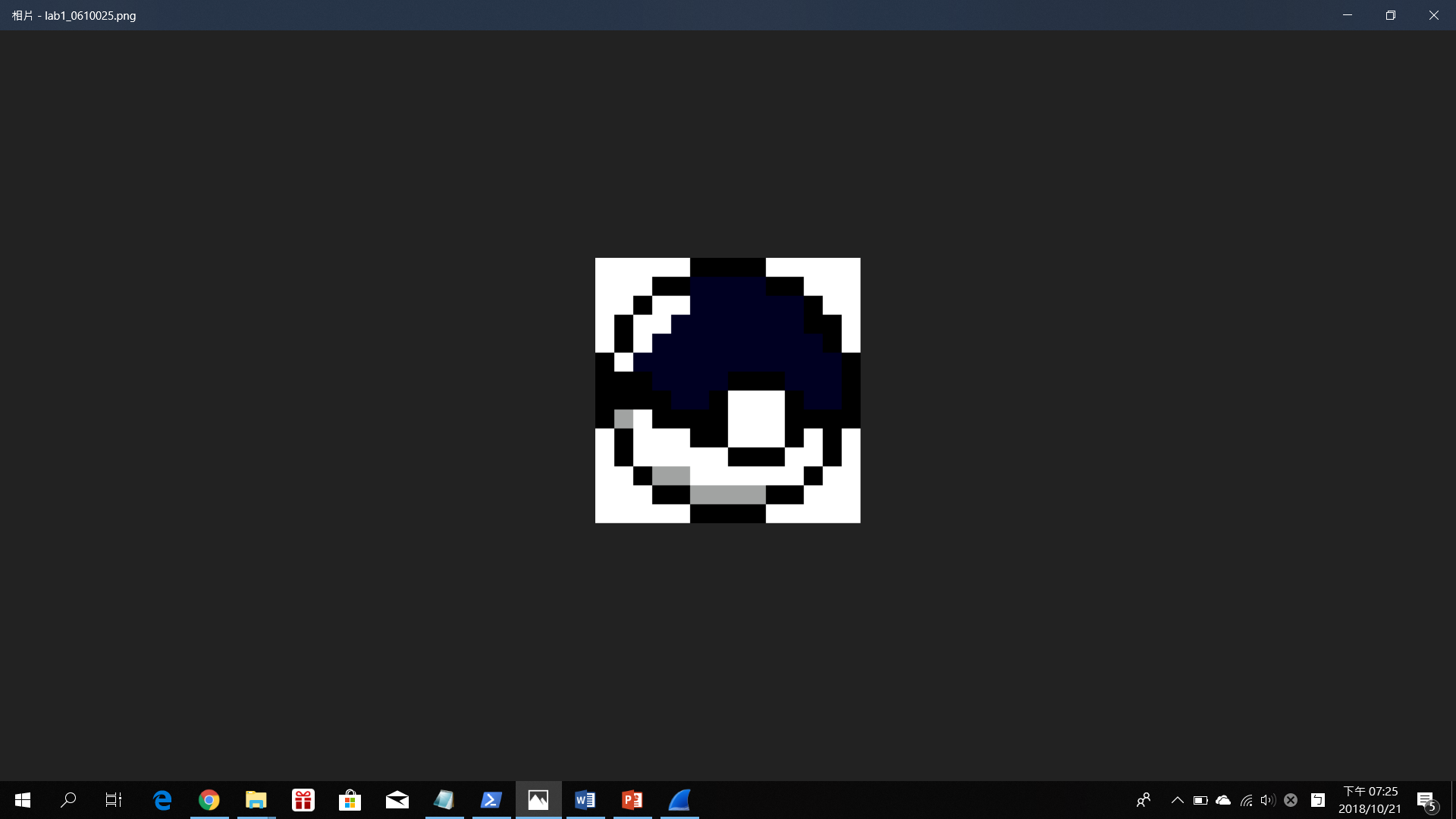
* Input the secret key into ./src/decoder.py on local machine

因為在後來有更新decoder.py，我為了不要覆蓋檔案，將新的檔案命名為decoder\_new.py

執行方式：



輸出圖案：



Bonus

* What you have learned in this lab?

1. 用powershell做一些操作
2. 在終端機改路徑的方法
3. vim的基本編輯方式
4. 在wireshark篩選封包
5. 上傳github時加入註解

* What difficulty you have met in this lab?

1. 一開始不會改路徑，一直在錯的資料夾
2. 一開始不是在vim做編輯，是在終端機外編輯.sh和.py，結果全部要從來
3. main.sh打錯後，執行出錯誤的結果，h1建立成功但是h2建立失敗，改好code後在執行一次時，出現錯誤訊息表示我已經建立一個h1了，最後花了一點時間才刪掉h1，再做一次