Assignment Link :
https://docs.google.com/presentation/d/1ivenFNAH88ZSngfLakE59cX7TDprD7_Z/edit?usp=share_link&ouid=101139848262573953517&rtpof=true&sd=true

---

Task 1: Use nslookup or dig to do a dns lookup on www.growthschool.io and see what is the response coming as.
>> Used 'ping growthschool.io' or 'nslookup growthschool.io' to get the IP address as 65.0.79.182.

Task 2: Figure out how can you use nslookup to find name and IP address of SMTP server of gmail.com.
>> Here are the steps:

Open a command prompt (CMD.exe)
Type nslookup and hit enter
Type set type=MX and hit enter
Type gmail.com and hit enter

Result :

```
gmail.com       MX preference = 10, mail exchanger =
alt1.gmail-smtp-in.l.google.com
gmail.com       MX preference = 20, mail exchanger =
alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger =
alt3.gmail-smtp-in.l.google.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 40, mail exchanger =
alt4.gmail-smtp-in.l.google.com
```

Task 3: Suppose you have a web server running on your network that is listening on

port 80. Write a TCPdump
command that captures all HTTP traffic coming to the server and saves it to a file called "http_traffic.pcap".
>> Step 1 : Since, I was using Windows system, did some research to do the equivalent task on a windows system. Got info about Winshark.
>> Step 2 : Installed Winshark and it also installed NPCAP along with Winshark installation.
>> Step 3 : Ran below command on cmd to get all the interface names

Input:
"C:\Program Files\Wireshark\dumpcap.exe" -D

Output:
1. \Device\NPF_{AFE046CC-65A2-46EE-97F6-7F1817BA1848} (Local Area Connection* 10)
2. \Device\NPF_{9CDC05C5-0992-433A-8D73-B4860C36F091} (Local Area Connection* 9)
3. \Device\NPF_{0DBB5B62-7DDE-4BAA-81DA-99675E25A117} (Local Area Connection* 8)
4. \Device\NPF_{418FCCA7-4735-418B-AAD8-318AB4A784CA} (Bluetooth Network Connection)
5. \Device\NPF_{FC91865F-21A0-4030-AA9A-8D47C50A1B4A} (Ethernet)
6. \Device\NPF_{C139163D-C934-44F6-9505-820D8BA48130} (Local Area Connection* 2)
7. \Device\NPF_{48520035-CC2C-4E9D-9A8E-F69E29A69CC7} (Local Area Connection* 1)
8. \Device\NPF_{9004BFFE-E90A-425D-9F2A-364FE6A010CE} (Wi-Fi)
9. \Device\NPF_Loopback (Adapter for loopback traffic capture)

>> Step 4 : Ran below command to capture the traffic and save it to desired file.

Input:
"C:\Program Files\Wireshark\dumpcap.exe" -i \Device\NPF_{FC91865F-21A0-4030-AA9A-8D47C50A1B4A} -w http_traffic.pcap -f "port 80"

Output:
Capturing on 'Ethernet'
File: http_traffic.pcap
Packets captured: 17
Packets received/dropped on interface 'Ethernet': 17/0 (pcap:0/dumpcap:0/flushed:0/ps_ifdrop:0) (100.0%)

The file named 'http_traffic' was created in my user in Disk C.
