https://github.com/Meruyert98/network

Network Parameters (15 points)
Using a terminal, check the network parameters cónfigured on the virtual machine:
* MAC address
ip link show

```
airflow@slamova98-GL62M-7REX:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN mode DEFAULT group default q
len 1000
    link/ether 30:9c:23:18:a6:3f brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DORMANT group default qlen
1000
    link/ether b4:d5:bd:a7:c3:76 brd ff:ff:ff:ff:ff:ff
4: br-96a8d281b912: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN mode DEFAULT g
roup default
    link/ether 02:42:8f:5c:f6:f9 brd ff:ff:ff:ff:ff:ff
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN mode DEFAULT group def
ault
    link/ether 02:42:93:f7:77:a3 brd ff:ff:ff:ff:ff:ff
```

Ethernet interface (wlp2s0)

MAC address: 30:9c:23:18:a6:3f

*** Local ARP table**
arp -n
ip neigh

```
airflow@slamova98-GL62M-7REX:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.1              ether   20:98:d8:09:d6:dd   C                     wlp2s0
airflow@slamova98-GL62M-7REX:~$ ip neigh
192.168.0.1 dev wlp2s0 lladdr 20:98:d8:09:d6:dd REACHABLE
```

*** Network interfaces and associated IP addresses**
ip addr show

```
airflow@slamova98-GL62M-7REX:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 30:9c:23:18:a6:3f brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether b4:d5:bd:a7:c3:76 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.20/24 brd 192.168.0.255 scope global dynamic noprefixroute wlp2s0
       valid_lft 28362sec preferred_lft 28362sec
    inet6 fe80::bb10:1ea:4711:3c11/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: br-96a8d281b912: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:8f:5c:f6:f9 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-96a8d281b912
       valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:93:f7:77:a3 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

*** Route table**

ip route show

```
airflow@slamova98-GL62M-7REX:~$ ip route show
default via 192.168.0.1 dev wlp2s0 proto dhcp metric 600
169.254.0.0/16 dev wlp2s0 scope link metric 1000
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.18.0.0/16 dev br-96a8d281b912 proto kernel scope link src 172.18.0.1 linkdown
192.168.0.0/24 dev wlp2s0 proto kernel scope link src 192.168.0.20 metric 600
```

*** List of open (listening) TCP ports**

sudo netstat -tuln

```
airflow@slamova98-GL62M-7REX:~$ sudo netstat -tulpn
[sudo] password for airflow:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:11369         0.0.0.0:*               LISTEN      8440/daxz
tcp        0      0 127.0.0.1:27017         0.0.0.0:*               LISTEN      1805/mongod
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      2024/mysqld
tcp        0      0 127.0.0.1:5939          0.0.0.0:*               LISTEN      3038/teamviewerd
tcp        0      0 127.0.0.1:55668         0.0.0.0:*               LISTEN      8440/daxz
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      968/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1824/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      7297/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      2059/postgres
tcp        0      0 0.0.0.0:5433            0.0.0.0:*               LISTEN      2064/postgres
tcp        0      0 127.0.0.1:5434          0.0.0.0:*               LISTEN      2065/postgres
tcp6       0      0 :::80                   :::*                    LISTEN      2012/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      1824/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      7297/cupsd
tcp6       0      0 :::5433                 :::*                    LISTEN      2064/postgres
udp        0      0 0.0.0.0:59679           0.0.0.0:*                           1440/avahi-daemon:
udp        0      0 224.0.0.251:5353        0.0.0.0:*                           5493/chrome --enabl
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           1440/avahi-daemon:
udp        0      0 127.0.0.53:53           0.0.0.0:*                           968/systemd-resolve
udp        0      0 0.0.0.0:68              0.0.0.0:*                           2773/dhclient
udp        0      0 0.0.0.0:631             0.0.0.0:*                           7298/cups-browsed
udp6       0      0 :::35495                :::*                                1440/avahi-daemon:
udp6       0      0 :::5353                 :::*                                1440/avahi-daemon:
```

ss -tuln

```
airflow@slamova98-GL62M-7REX:~$ ss -tulpn
Netid State  Recv-Q Send-Q   Local Address:Port    Peer Address:Port
udp   UNCONN 0      0            0.0.0.0:59679        0.0.0.0:*
udp   UNCONN 0      0          224.0.0.251:5353       0.0.0.0:*     users:(("chrome",pid=5493,fd=176))
udp   UNCONN 0      0            0.0.0.0:5353         0.0.0.0:*
udp   UNCONN 0      0        127.0.0.53%lo:53         0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:68           0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:631          0.0.0.0:*
udp   UNCONN 0      0               [::]:35495           [::]:*
udp   UNCONN 0      0               [::]:5353            [::]:*
tcp   LISTEN 0      10         127.0.0.1:11369        0.0.0.0:*
tcp   LISTEN 0      128        127.0.0.1:27017        0.0.0.0:*
tcp   LISTEN 0      80         127.0.0.1:3306         0.0.0.0:*
tcp   LISTEN 0      128        127.0.0.1:5939         0.0.0.0:*
tcp   LISTEN 0      5          127.0.0.1:55668        0.0.0.0:*
tcp   LISTEN 0      128      127.0.0.53%lo:53         0.0.0.0:*
tcp   LISTEN 0      128          0.0.0.0:22           0.0.0.0:*
tcp   LISTEN 0      5          127.0.0.1:631          0.0.0.0:*
tcp   LISTEN 0      128        127.0.0.1:5432         0.0.0.0:*
tcp   LISTEN 0      128          0.0.0.0:5433         0.0.0.0:*
tcp   LISTEN 0      128        127.0.0.1:5434         0.0.0.0:*
tcp   LISTEN 0      128                *:80                 *:*
tcp   LISTEN 0      128             [::]:22              [::]:*
tcp   LISTEN 0      5               [::1]:631            [::]:*
tcp   LISTEN 0      128             [::]:5433            [::]:*
```

Network Connectivity (15 points)

Using a terminal, check the network connectivity between the virtual machine and the internet (8.8.8.8 host):
1. Send 5 IMP packets and check the loss percentage and RTT.
ping -c 5 8.8.8.8

```
airflow@slamova98-GL62M-7REX:~$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=134 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=127 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=127 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=126 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=51 time=143 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 126.914/131.841/143.086/6.292 ms
```

2. Discover the path (route) that packets take to reach the destination host.

traceroute 8.8.8.8

```
airflow@slamova98-GL62M-7REX:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.991 ms  0.956 ms  1.503 ms
 2  JZK-C01-BR05.2day.kz (80.241.35.38)  2.714 ms  2.710 ms  2.699 ms
 3  172.16.242.33 (172.16.242.33)  5.355 ms  6.089 ms  6.405 ms
 4  * * *
 5  172.16.242.2 (172.16.242.2)  2.984 ms  2.978 ms  2.968 ms
 6  * * *
 7  172.16.242.81 (172.16.242.81)  4.430 ms  4.407 ms  4.417 ms
 8  LAG11.GRT01.SNBAV.ALM (80.241.35.190)  2.431 ms  2.433 ms  2.425 ms
 9  * * *
10  * * *
11  87-245-230-108.retn.net (87.245.230.108)  91.663 ms  90.917 ms  90.946 ms
12  ae10-9.rt.tnr.hki.fi.retn.net (87.245.233.140)  127.133 ms  128.555 ms  128.550 ms
13  87.245.208.1 (87.245.208.1)  128.928 ms  127.767 ms  128.713 ms
14  * * *
15  dns.google (8.8.8.8)  127.020 ms  126.696 ms  126.731 ms
```

IP Parameters (20 points)

* For the given CIDR-192.168.0.0/26-using bitwise arithmetic, calculate:

CIDR notation 192.168.0.0/26 means:

- **IP Address**: 192.168.0.0
- **Subnet Mask**: /26 (26 bits are used for the network portion)

192.168.0.0 to binary:

- 192 → 11000000
- 168 → 10101000
- 0 → 00000000
- 0 → 00000000

The binary representation of 192.168.0.0 is:
11000000.10101000.00000000.00000000

* Netmask

The subnet mask has 26 bits for the network part (as specified by /26), and the remaining bits (32-26 = 6 bits) are for the host part. The netmask is thus:

- Network bits (26): 1
- Host bits (6): 0

So the subnet mask in binary will look like this:
11111111.11111111.11111111.11000000

Now, convert it to decimal:

- 11111111 → 255
- 11111111 → 255
- 11111111 → 255
- 11000000 → 192

Thus, the **Netmask** in decimal is: **255.255.255.192**

*** Network address**

The Network Address is obtained by performing a bitwise AND operation between the IP address and the subnet mask.

11000000.10101000.00000000.00000000 (IP)
AND
11111111.11111111.11111111.11000000 (Netmask)

11000000.10101000.00000000.00000000 (Network Address)

This results in the Network Address: 192.168.0.0

*** Broadcast address**

The Broadcast Address is derived by performing a bitwise OR operation between the Network Address and the inverse of the subnet mask (inverted mask has 0 where the original mask had 1, and 1 where it had 0).

First, find the inverse of the subnet mask:

- Subnet Mask (binary): 11111111.11111111.11111111.11000000
- Inverted Mask (binary): 00000000.00000000.00000000.00111111

Now perform the bitwise OR between the Network Address and the Inverted Mask:
Network Address (binary): 11000000.10101000.00000000.00000000
Inverted Mask (binary): 00000000.00000000.00000000.00111111

Broadcast Address (binary): 11000000.10101000.00000000.00111111

Convert it back to decimal:

- 11000000 → 192
- 10101000 → 168

- 00000000 → 0
- 00111111 → 63

Thus, the Broadcast Address is: 192.168.0.63

*** Number of hosts in the subnet**

The number of hosts in the subnet is determined by the host bits. Since we have a /26 subnet (26 bits for the network), there are 6 bits left for the host portion.

The formula to calculate the number of hosts is: Number of Hosts = 2^n - 2

Number of Hosts = 2^6 - 2 = 64 - 2 = 62

Local Network Traffic (50 points)

Capture samples of local network traffic for different protocols (ARP, ICMP, TCP, and HTTP). Each subtask requires opening two terminal windows-one with a network sniffing tool launched with the required flags and another with the corresponding protocol tool.

*** ARP:**

1. Launch the network sniffing tool in ARP protocol filtering mode with DNS resolving disabled.

Show all interfaces: tcpdump -D

```
airflow@slamova98-GL62M-7REX:~$ tcpdump -D
1.wlp2s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.enp3s0 [Up]
5.docker0 [Up]
6.br-96a8d281b912 [Up]
7.bluetooth0 (Bluetooth adapter number 0)
8.nflog (Linux netfilter log (NFLOG) interface)
9.nfqueue (Linux netfilter queue (NFQUEUE) interface)
10.usbmon1 (USB bus number 1)
11.usbmon2 (USB bus number 2)
```

Open a terminal and launch Wireshark or tcpdump with an ARP filter and DNS resolution disabled:

sudo tcpdump -i wlp2s0 arp -n

```
airflow@slamova98-GL62M-7REX:~$ sudo tcpdump -i wlp2s0 arp -n
[sudo] password for airflow:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

2. Clear the local ARP cache.

sudo ip -s -s neigh flush all

```
airflow@slamova98-GL62M-7REX:~$ sudo ip -s -s neigh flush all
192.168.0.1 dev wlp2s0 lladdr 20:98:d8:09:d6:dd ref 1 used 4055/0/4055 probes 4
REACHABLE
192.168.0.11 dev wlp2s0 lladdr be:ae:c2:04:3c:0c used 3527/3587/3527 probes 0 ST
ALE

*** Round 1, deleting 2 entries ***
*** Flush is complete after 1 round ***
```

3. Send an ICMP request to the default gateway.

Ip route | grep default
ping -c 1 192.168.0.1

```
airflow@slamova98-GL62M-7REX:~$ ip route | grep default
default via 192.168.0.1 dev wlp2s0 proto dhcp metric 600
airflow@slamova98-GL62M-7REX:~$ ping -c 1 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=1.25 ms

--- 192.168.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.259/1.259/1.259/0.000 ms
```

4. Make a screenshot of the network sniffing tool showing the commands used with the flags and the ARP request/response in the output.

```
airflow@slamova98-GL62M-7REX:~$ sudo tcpdump -i wlp2s0 arp -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
00:05:22.930255 ARP, Request who-has 192.168.0.1 tell 192.168.0.20, length 28
00:05:22.931053 ARP, Reply 192.168.0.1 is-at 20:98:d8:09:d6:dd, length 28
00:05:38.280795 ARP, Request who-has 192.168.0.11 tell 192.168.0.1, length 28
```

ICMP:
1. Launch the network sniffing tool in ICMP protocol filtering mode.
sudo tcpdump -i wlp2s0 icmp -n

```
airflow@slamova98-GL62M-7REX:~$ sudo tcpdump -i wlp2s0 icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

2. Send 5 ICMP packets to 8.8.8.8.
ping -c 5 8.8.8.8

```
airflow@slamova98-GL62M-7REX:~$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=124 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=188 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=221 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=120 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=51 time=165 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 120.875/164.330/221.940/38.409 ms
```

3. Make a screenshot of the network sniffing tool showing the commands used with the flags and the echo request/reply messages in the output.

```
airflow@slamova98-GL62M-7REX:~$ sudo tcpdump -i wlp2s0 icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
00:11:06.826249 IP 192.168.0.20 > 8.8.8.8: ICMP echo request, id 28499, seq 1, length 64
00:11:06.951037 IP 8.8.8.8 > 192.168.0.20: ICMP echo reply, id 28499, seq 1, length 64
00:11:07.828284 IP 192.168.0.20 > 8.8.8.8: ICMP echo request, id 28499, seq 2, length 64
00:11:08.017175 IP 8.8.8.8 > 192.168.0.20: ICMP echo reply, id 28499, seq 2, length 64
00:11:08.828276 IP 192.168.0.20 > 8.8.8.8: ICMP echo request, id 28499, seq 3, length 64
00:11:09.050168 IP 8.8.8.8 > 192.168.0.20: ICMP echo reply, id 28499, seq 3, length 64
00:11:09.828198 IP 192.168.0.20 > 8.8.8.8: ICMP echo request, id 28499, seq 4, length 64
00:11:09.949039 IP 8.8.8.8 > 192.168.0.20: ICMP echo reply, id 28499, seq 4, length 64
00:11:10.830192 IP 192.168.0.20 > 8.8.8.8: ICMP echo request, id 28499, seq 5, length 64
00:11:10.995228 IP 8.8.8.8 > 192.168.0.20: ICMP echo reply, id 28499, seq 5, length 64
```

*** TCP, HTTP:**

1. Launch the network sniffing tool and set the filters to show only traffic for port 80 and the host "neverssl.com." Make sure you enable printing ASCHI representation for each packet.
sudo tcpdump -i wlp2s0 port 80 and host neverssl.com -A

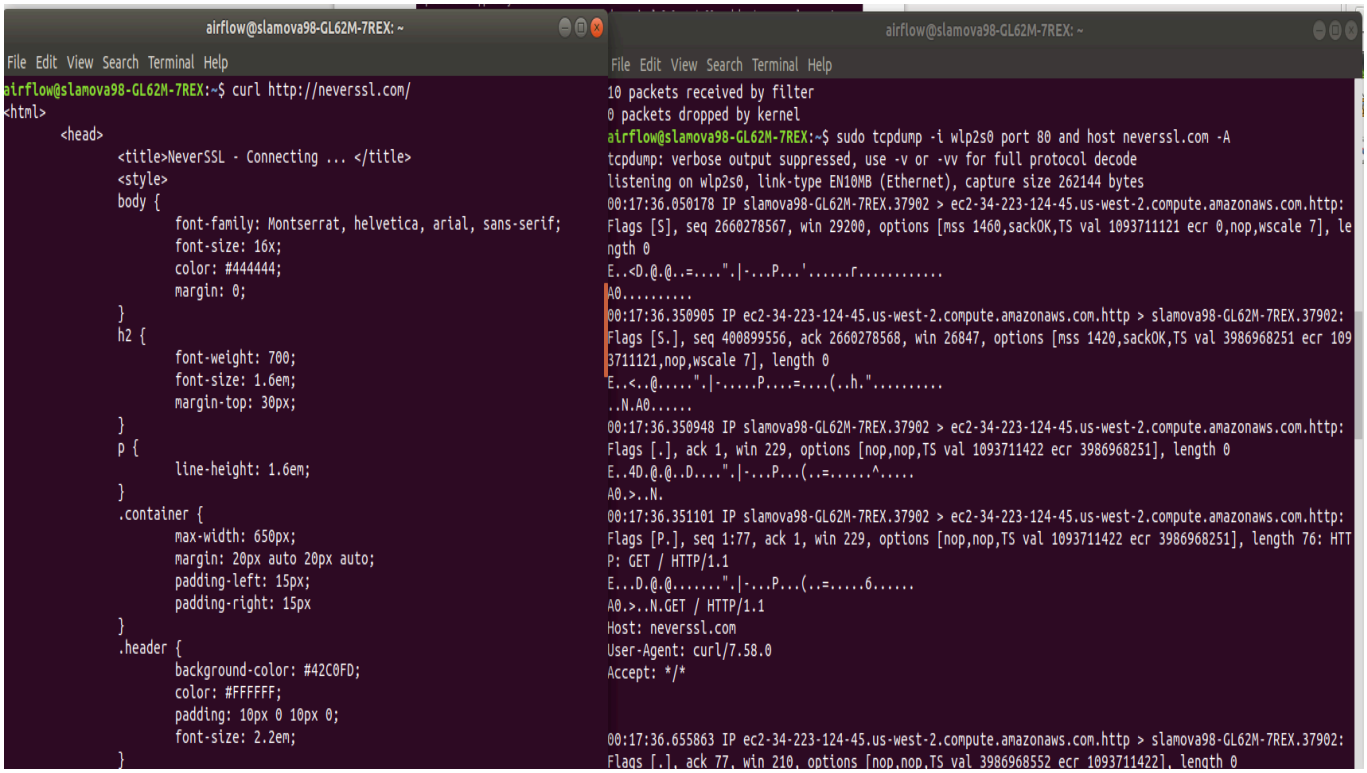
```
airflow@slamova98-GL62M-7REX:~$ sudo tcpdump -i wlp2s0 port 80 and host neverssl.com -A
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

2. Send an HTTP request to http://neverssl.com/.

curl http://neverssl.com/

```
airflow@slamova98-GL62M-7REX:~$ curl http://neverssl.com/
<html>
        <head>
                <title>NeverSSL - Connecting ... </title>
                <style>
                body {
                        font-family: Montserrat, helvetica, arial, sans-serif;
                        font-size: 16x;
                        color: #444444;
                        margin: 0;
                }
                h2 {
                        font-weight: 700;
                        font-size: 1.6em;
                        margin-top: 30px;
                }
                p {
```

3. Make a screenshot of the network sniffing tool showing the commands used with the flags and the output with a TCP three-way handshake and HTTP request headers.



```
airflow@slamova98-GL62M-7REX:~$ sudo tcpdump -i wlp2s0 port 80 and host neverssl.com -A
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
00:17:36.050178 IP slamova98-GL62M-7REX.37902 > ec2-34-223-124-45.us-west-2.compute.amazonaws.com.http: Fl
ags [S], seq 2660278567, win 29200, options [mss 1460,sackOK,TS val 1093711121 ecr 0,nop,wscale 7], length
 0
E..<D.@.@..=....".|-...P...'......r............
A0.........
00:17:36.350905 IP ec2-34-223-124-45.us-west-2.compute.amazonaws.com.http > slamova98-GL62M-7REX.37902: Fl
ags [S.], seq 400899556, ack 2660278568, win 26847, options [mss 1420,sackOK,TS val 3986968251 ecr 1093711
121,nop,wscale 7], length 0
E..<..@.....".|-.....P....=....(..h."..........
..N.A0......
00:17:36.350948 IP slamova98-GL62M-7REX.37902 > ec2-34-223-124-45.us-west-2.compute.amazonaws.com.http: Fl
ags [.], ack 1, win 229, options [nop,nop,TS val 1093711422 ecr 3986968251], length 0
E..4D.@.@..D....".|-...P...(..=......^.....
A0.>..N.
00:17:36.351101 IP slamova98-GL62M-7REX.37902 > ec2-34-223-124-45.us-west-2.compute.amazonaws.com.http: Fl
ags [P.], seq 1:77, ack 1, win 229, options [nop,nop,TS val 1093711422 ecr 3986968251], length 76: HTTP: G
ET / HTTP/1.1
E...D.@.@.......".|-...P...(..=.....6......
A0.>..N.GET / HTTP/1.1
Host: neverssl.com
User-Agent: curl/7.58.0
Accept: */*


00:17:36.655863 IP ec2-34-223-124-45.us-west-2.compute.amazonaws.com.http > slamova98-GL62M-7REX.37902: Fl
ags [.], ack 77, win 210, options [nop,nop,TS val 3986968552 ecr 1093711422], length 0
E..4gV@.....".|-.....P....=....t...........
..O.A0.>
00:17:36.655914 IP ec2-34-223-124-45.us-west-2.compute.amazonaws.com.http > slamova98-GL62M-7REX.37902: Fl
ags [.], seq 1:1409, ack 77, win 210, options [nop,nop,TS val 3986968552 ecr 1093711422], length 1408: HTT
P: HTTP/1.1 200 OK
E...gW@....#".|-.....P....=....t.....-.....
..O.A0.>HTTP/1.1 200 OK
```