Lab 1

Do not write your name or Net ID anywhere in this lab report. Also make sure that your name or Net ID should not appear anywhere in the screenshots.

Task 1. Capturing packets on your own

Overview: Run packet capture on your own and identify the activities on the network.

Steps:

1. Download and install Wireshark on your computer.
2. Come up with a random integer. Call it X.
3. Start capturing.
4. Open your browser and visit [X].neverssl.com. For example, my random number is 4567, then I would visit 4567.neverssl.com. Make sure that you have never visited [X].neverssl.com before.
5. Stop the packet capture.

Question 1.1:

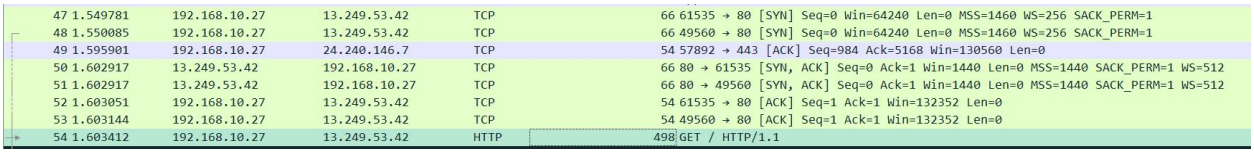
- What are the IP addresses (“A records”) associated with “[X].neverssl.com”?
- Explain how you arrive at this answer.
- Include a relevant Wireshark screenshot. In the screenshot, make sure to show the “Answers” section of the corresponding DNS request.

[Your response goes here.]
24.240.146.7
Through DNS response.

Question 1.2:

- Which IP address of [X].neverssl.com did your browser end up communicating with?
- Explain your response.
- Include a relevant Wireshark screenshot.

[Your response goes here.]
13.249.53.42
Through looking at the HTTP GET request destination.



47	1.549781	192.168.10.27	13.249.53.42	TCP	66	61535 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
48	1.550085	192.168.10.27	13.249.53.42	TCP	66	49560 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
49	1.595901	192.168.10.27	24.240.146.7	TCP	54	57892 → 443 [ACK] Seq=984 Ack=5168 Win=130560 Len=0
50	1.602917	13.249.53.42	192.168.10.27	TCP	66	80 → 61535 [SYN, ACK] Seq=0 Ack=1 Win=1440 Len=0 MSS=1440 SACK_PERM=1 WS=512
51	1.602917	13.249.53.42	192.168.10.27	TCP	66	80 → 49560 [SYN, ACK] Seq=0 Ack=1 Win=1440 Len=0 MSS=1440 SACK_PERM=1 WS=512
52	1.603051	192.168.10.27	13.249.53.42	TCP	54	61535 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
53	1.603144	192.168.10.27	13.249.53.42	TCP	54	49560 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
54	1.603412	192.168.10.27	13.249.53.42	HTTP	498	GET / HTTP/1.1

Question 1.3:

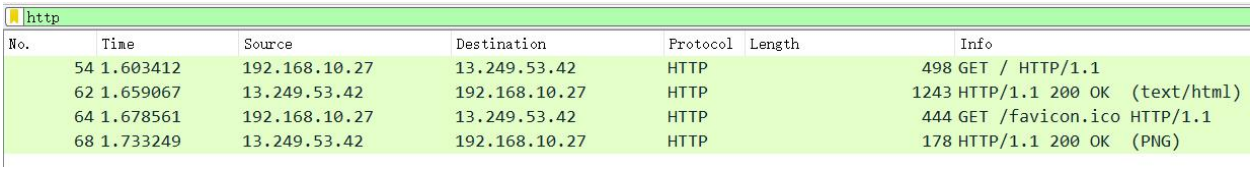
- How is the IP address in Question 1.2 related to the IP addresses in Question 1.1?
- Why?

[Your response goes here.]
Client host talks to the CDN server to find out the IP address where the content is stored. Because the dns lookup return an IP address of a CDN server, and the client setup connection with this address before talking to the IP address of x.neverssl.com.

Question 1.4:

- How many HTTP requests did your browser send in its communication with [X].neverssl.com?
- What are these requests?
- Include a relevant Wireshark screenshot.

[Your response goes here.]
2 requests
GET / HTTP/1.1 and GET /favicon.ico HTTP/1.1



http

No.	Time	Source	Destination	Protocol	Length	Info
54	1.603412	192.168.10.27	13.249.53.42	HTTP	498	GET / HTTP/1.1
62	1.659067	13.249.53.42	192.168.10.27	HTTP	1243	HTTP/1.1 200 OK (text/html)
64	1.678561	192.168.10.27	13.249.53.42	HTTP	444	GET /favicon.ico HTTP/1.1
68	1.733249	13.249.53.42	192.168.10.27	HTTP	178	HTTP/1.1 200 OK (PNG)

Question 1.5:

- Can your Internet service provider see these HTTP requests?
- Why or why not?

[Your response goes here.]
Yes it can.
Because those requests are using HTTP without TLS.

Task 2. Parsing existing pcap files

Overview: Given some existing pcap file, identify activities on the network.

Steps:

1. Download this pcap file on your computer.
2. Open the pcap file in Wireshark. If Wireshark reports an error, try this file instead. The two files are equivalent.
3. Examine all the packets in the file.

Question 2.0:

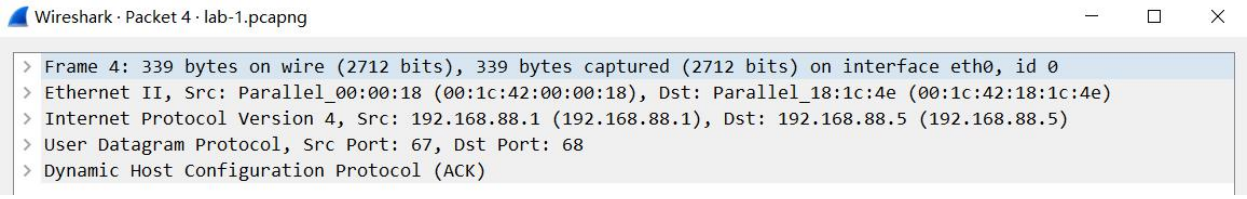
- How many packets are captured in the pcap file?

[Your response goes here.]
32

Question 2.1: As you can tell from the pcap, a host is trying to visit http://345678.neverssl.com. Let's call this host Alice.

- What is Alice's MAC address?
- What is Alice's IP address?
- How do you know?
- Include a relevant Wireshark screenshot.

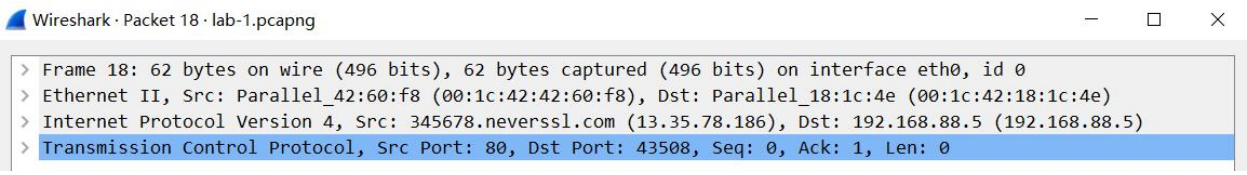
[Your response goes here.]
MAC: 00:1c:42:18:1c:4e
IP: 192.168.88.5
Through DHCP ACK.



Question 2.2: Let's now look at the server that hosts neverssl.com.

- What is its IP address?
- What is the MAC address of this server?
- How do you know?
- Include a relevant Wireshark screenshot.

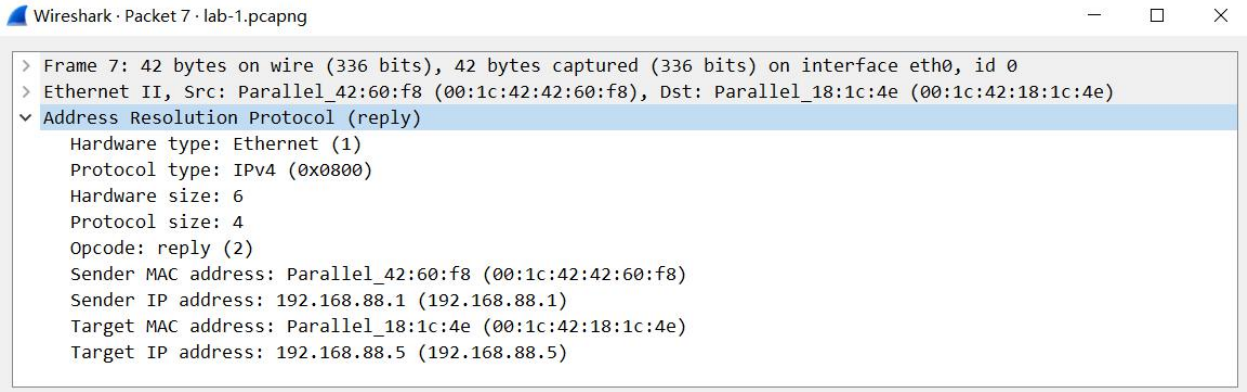
[Your response goes here.]
IP: 13.35.78.186
MAC address of the server is unknown, we only know the MAC of the last hop router.
Through looking at a TCP packet.



Question 2.3:

- What other hosts are on the same local network as Alice?
- What are their IP addresses and MAC addresses?
- How do you know?
- Include relevant Wireshark screenshots.

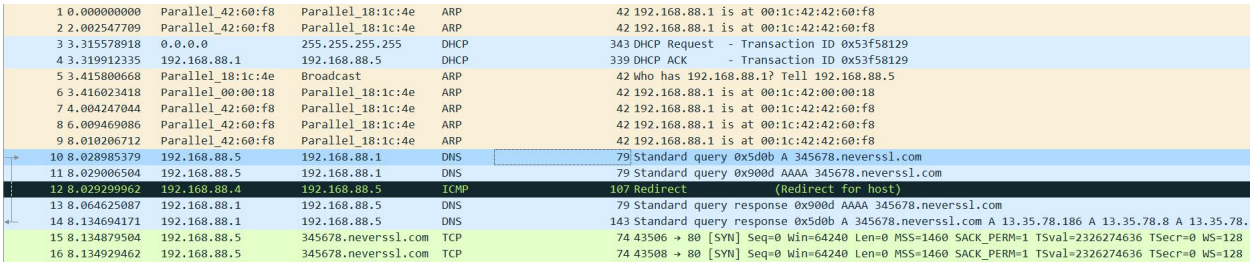
[Your response goes here.]
IP1: 192.168.88.1
MAC1: 00:1c:42:42:60:f8
Through packet statistics.



Question 2.4: The pcap shows that Alice is trying to visit http://345678.neverssl.com.

- What else is going on in this network?
- Include relevant Wireshark screenshots.

[Your response goes here.]
DHCP for Alice to obtain its ip address and other information about the LAN, ARP for Alice to obtain the MAC address of the gateway router, DNS for Alice to resolve the IP address of 345678.neverssl.com.



Task 3. Setting up SEED labs

Overview: Set up the SEED Lab environment in preparation for Lab 2. This task is optional, will not be graded, but is highly recommended.

Steps: Follow either Option A or Option B, but not both Options.

- Option A: Creating SEED labs on DigitalOcean.
    - Follow this guide. I strongly recommend using DigitalOcean as the cloud provider as the cost is predictable (i.e., $10/month). Follow Step 1, Step 2, and Step 3B of the guide; ignore Step 3A.
- Option B: Creating SEED labs on VirtualBox.
    - Follow this guide only if your personal computer runs Linux, Windows 10, or the Intel macOS. If you run the latest macOS on the M1 chip, you have to choose Option A.

My recommendation is to go for Option A. It is the easier way to set up the environment, and you'll be able to get more help from me or the Course Assistant as we are both familiar with Option A. The total cost will not exceed $30 in total for this semester if you use DigitalOcean. Although Option B is cheaper, you need to make sure that the host machine (which runs VirtualBox) should have good performance.

If you're a new GitHub user, you may be qualified for free $100 DigitalOcean credits. See this link.

Question 3.1:

- Which option did you choose, Option A or B?
- Why?

[Your response goes here.]
Option A, for it is recommended.

Question 3.2:

- Include a screenshot of your terminal when you run the following command:
  `sudo su seed`

[Your response goes here.]