Network assignment 2

Name: Xiankun Yan Student ID:1971068

# 1. Introduction

In this lab, we have to look at the network traffic and analysis some common protocols. There are four questions that we need to answer:

1. Could you see lots of traffic on the main interface and a small amount of traffic on the guest interface?
2. How does the guest virtual machine obtain an IP address?
3. Visit one simple web site then analysis what protocols are used and what traffic is exchanged between the web server and browser?
4. Visit <https://www.batten.eu.org>, then what do you see happening, and what do you think it means?

# 2.Tools and devices

I use one laptop of mac OS and install the virtual box (version:5.2.20) in my laptop. Then I set up the Ubuntu system (version:12.04 and OS type: 32-bit) in my virtual box. The version of the Firefox browser in Ubuntu is 26.0. Besides, I use the Wireshark (version:2.6.4) to monitor Internet and capture the packet.

# 3.Lab content

## 3.1: question 1

At the first step, I can see lots of traffic on the main interface though the Wireshark. However, no traffic exists on the guest interface (Fig. 3.1. and Fig. 3.2.). The host IP is 192.168.0.22 and the guest IP is 192.168.0.40

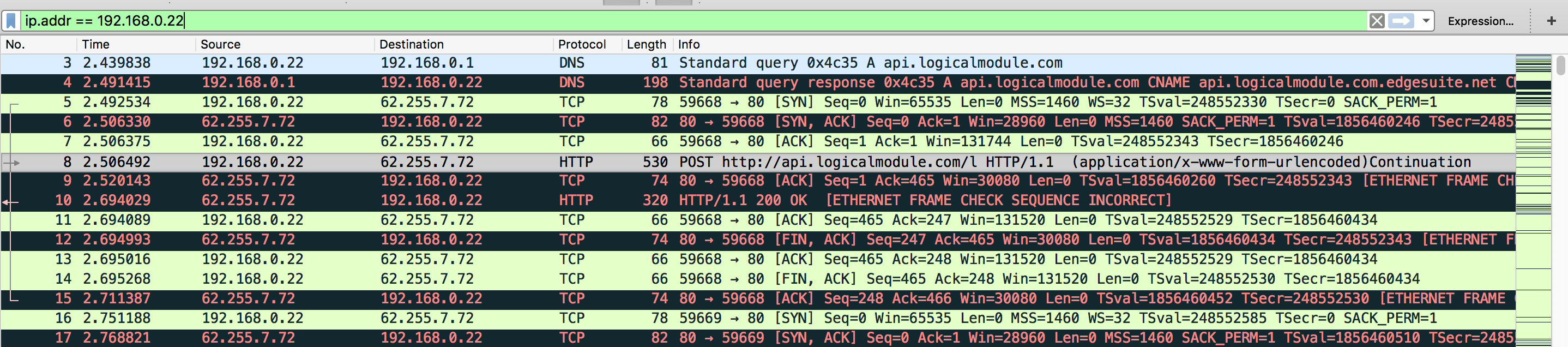


Fig. 3.1. The traffic on the main interface

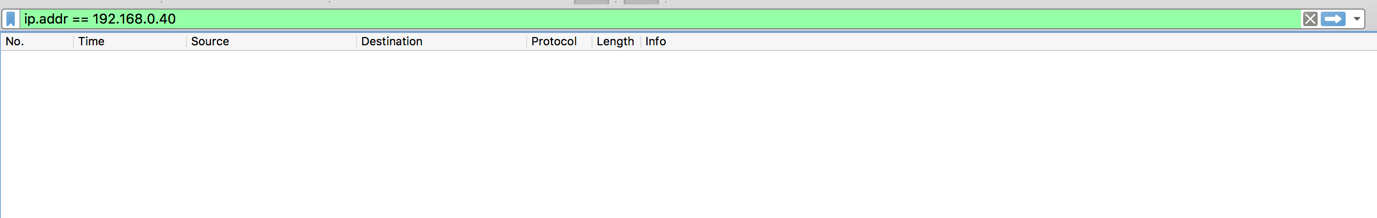


Fig. 3.2. The traffic on the guest interface

## 3.2: question 2

Then in order to find how the guest virtual machine obtain an IP address, I reboot the Ubuntu system after I set the filter to “bootp” that represents the DHCP protocol. I find there are four records about DHCP (Fig. 3.3.). It is vivid phenomenon in the port 67 and 68 that two interactions happen in the machine. At the first stage, the client broadcasts a DHCP DISCOVER message on the network subnet with the IP address 255.255.255.255. In the next step, when the server (IP address :192.168.0.1) receives the DHCP DISCOVER message, it allocates the client’s IP address and sends a DHCP OFFER message which includes the information about IP address (Fig. 3.4.) to client. On the third step, in response to the DHCP offer, the client broadcasts a DHCP REQUEST message to server, which requests the offered IP address. Finally, when the server gets the DHCP REQUEST message, it sends the DHCP ACK message that also contains the same information about IP address to client, which means the process of obtaining an IP address is successful.

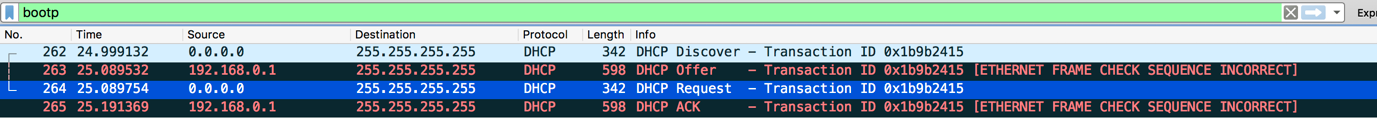


Fig. 3.3. The process of obtaining IP address

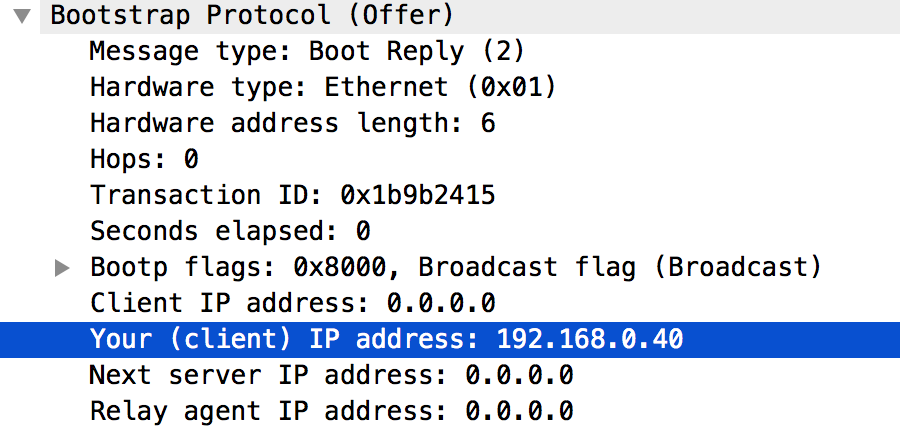


Fig. 3.4. The information about IP address in the DHCP OFFER message

## 3.3: question 3

In terms of the third question, I visit the web site <https://neverssl.com> in my virtual machine. I find some interesting things when I look at the Wireshark (Fig. 3.5.). During this process, it uses three protocols such as DNS, TCP and HTTP. At the beginning, the client (IP address:192.168.0.40) use the DNS protocol to send a query message about the web site to server (IP address:192.168.0.1). In response to the client, the server analyses the query message and then send another query message containing the IP address of this web server by DNS protocol. In the next three steps, it seems that there is a communication which is based on TCP protocol between the client and web server (IP address: 52.85.74.79). After this process, the client tells the web server to get the web site by HTTP protocol. Then, the web server continuously sends the message to the client four times. I notice that it uses the TCP protocol three times but in the fourth record, the HTTP protocol is used. The other interesting situation is that the client also responded to the web server three times by TCP protocol.

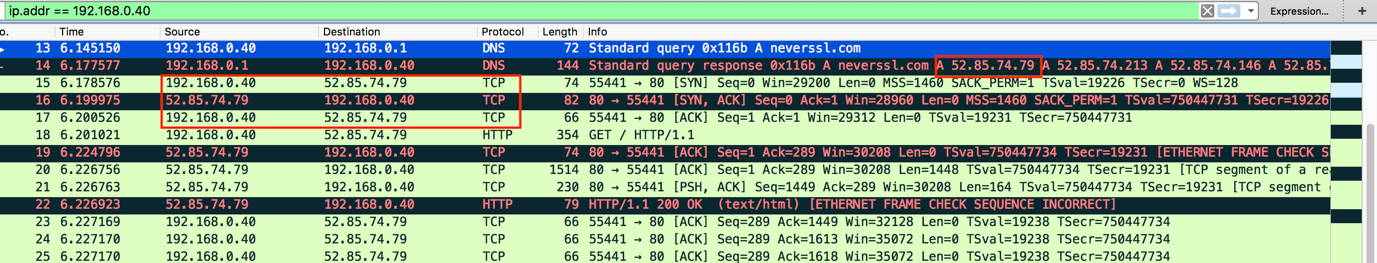


Fig. 3.5. The process of clicking the web site <https://neverssl.com>

## 3.4: Question 4

As for the fourth question, when I visit the web site <https://www.batten.eu.org> in the guest virtual machine, the Firefox browser shows an error (Fig.3.6.). Therefore, I look at my Wireshark and find some different things to compare to the process of visiting the web site <https://neverssl.com>(Fig. 3.7.). At the beginning, the client sends a query message to the server (IP address:192.168.0.1). After the IP address of this web site is obtained by the DNS protocols, the message including the IP information is given to the client from the server. The communication based on TCP protocol between the client and web server still happens in this time, but it still fails. In the Wireshark, I see one message that web server send to the client .it shows “Handshake Failure”. I guess this phenomenon means the client cannot connect to the web site <https://www.batten.eu.org>, so the browser shows an error. On the next four stages, there are four interactions between the client and web server, however the Flags are changed from “[SYN, ACK]” to “[FIN, ACK]”. I think in this time maybe the client request to cancel the connection with the web server.

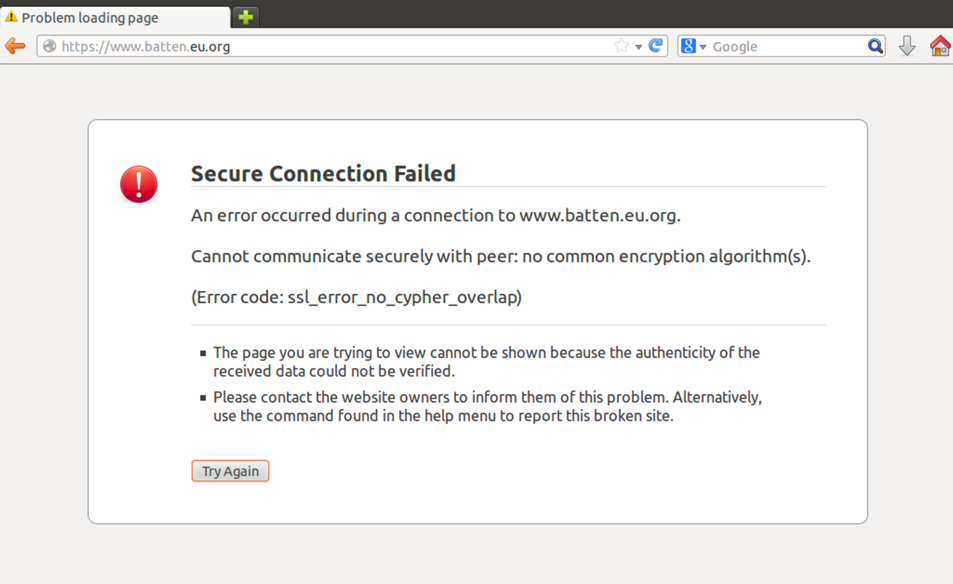


Fig. 3.6. The error of visiting the web site <https://www.batten.eu.org>

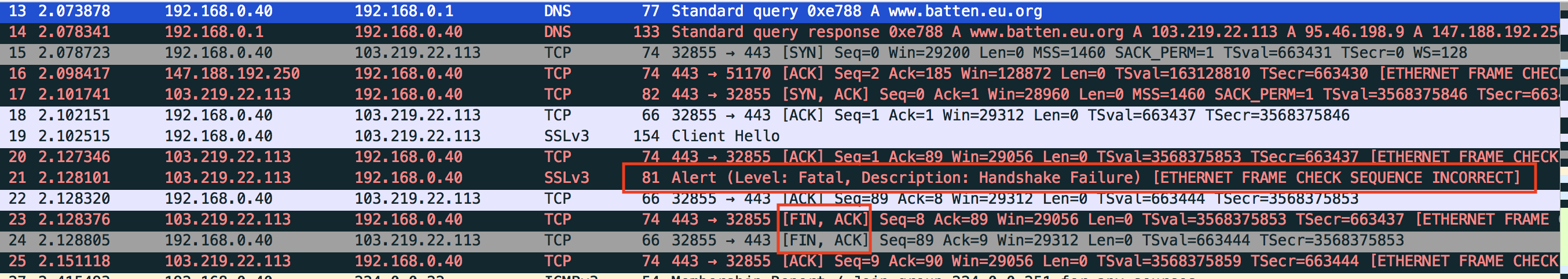


Fig. 3.7. The process of clicking the web site <https://www.batten.eu.org>

# 4.Summary

For this task, I complete all the questions. For first question, I can see lots of traffic in my host machine but no traffic machine in my virtual machine. In the second question, I notice the server offer the IP address to the virtual machine by DHCP protocol. And in the next question, there are some communication based on DNS and TCP protocol when I click a web link to visit a web site. Finally, in the last question, I see what happen on when I cannot visit the web site <https://www.batten.eu.org>.