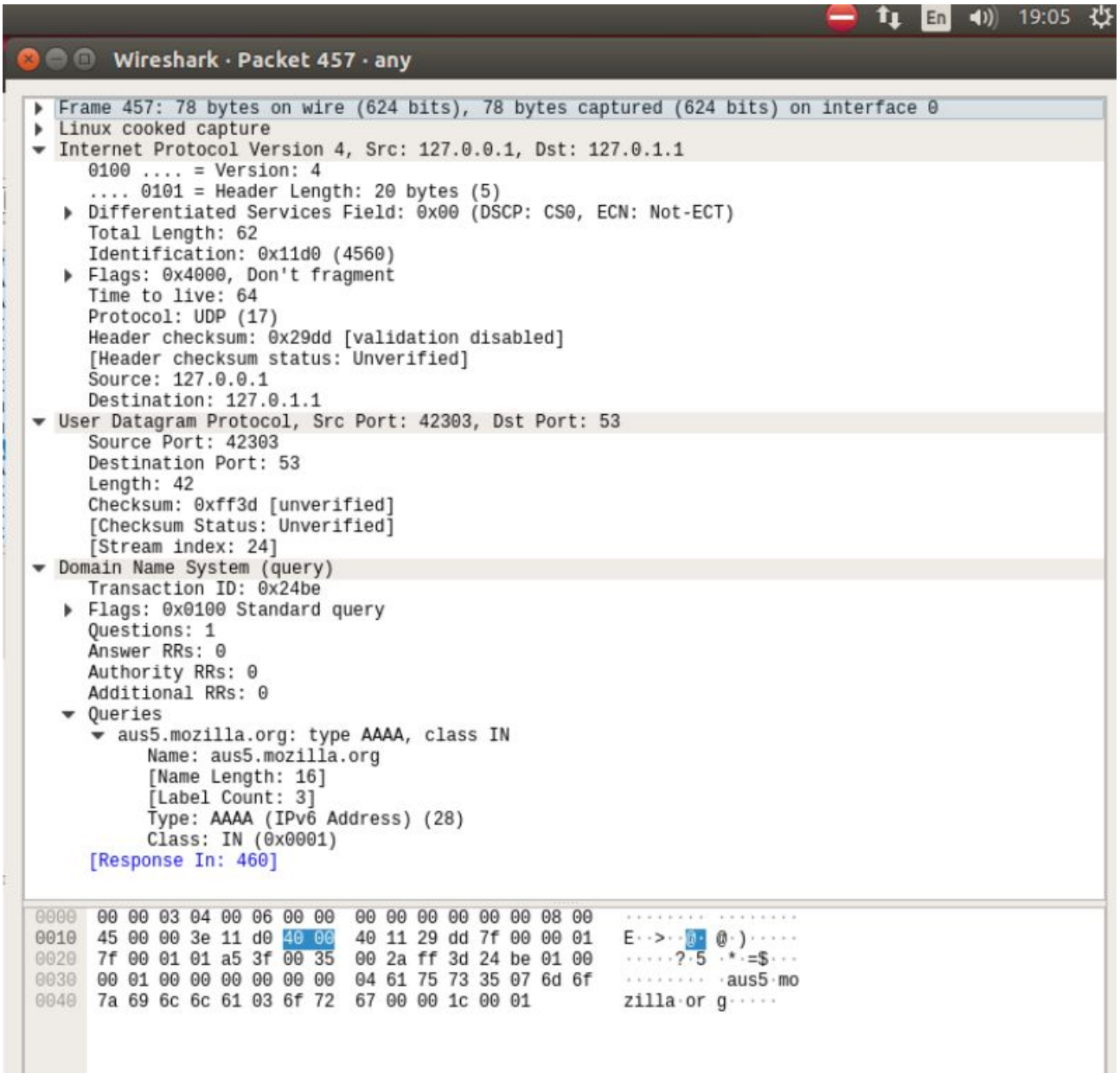
Computer Networks

B06902091 資工四 羅寶瑩

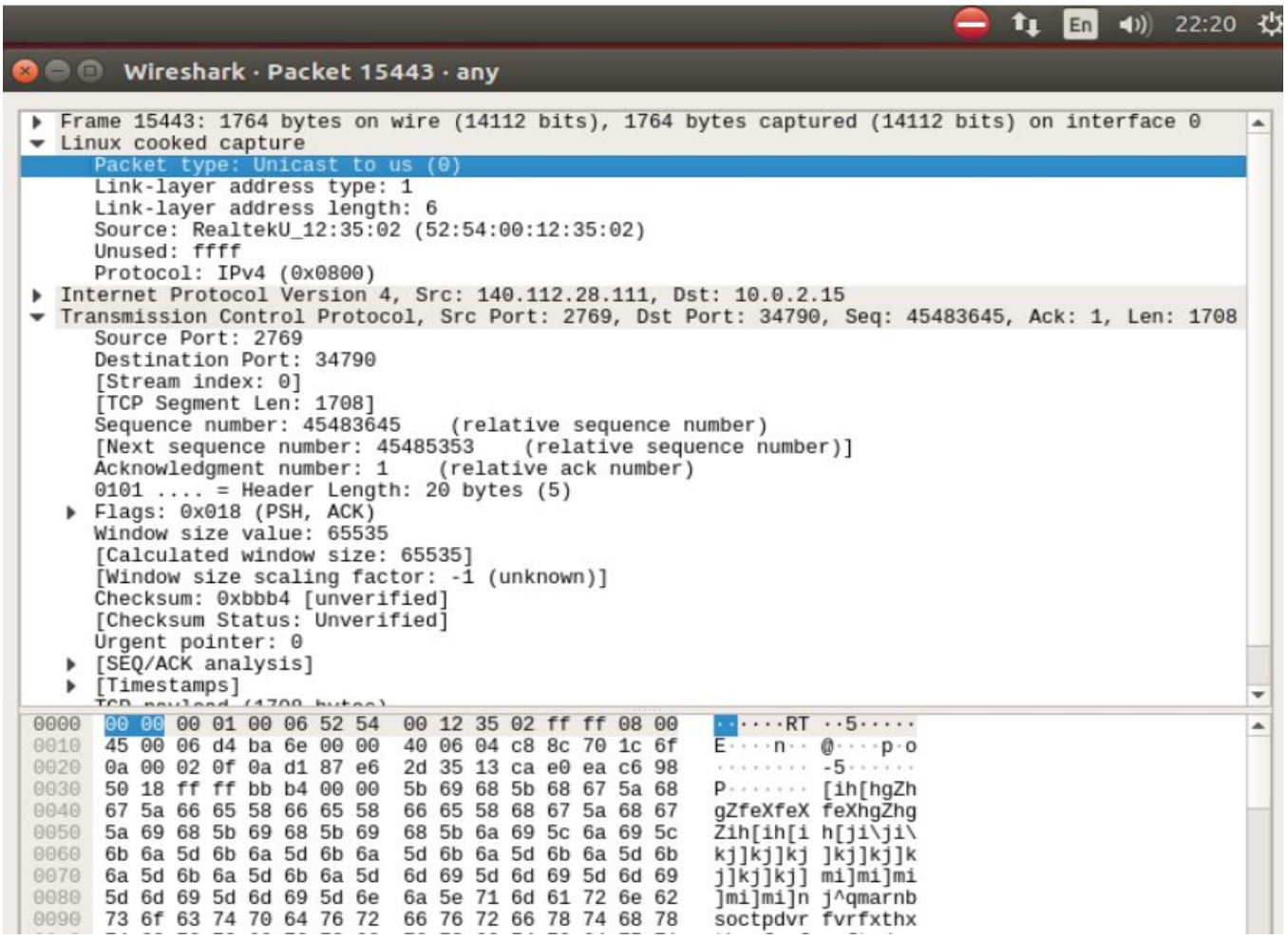
Assignment 1

01 Analysis of UDP packets



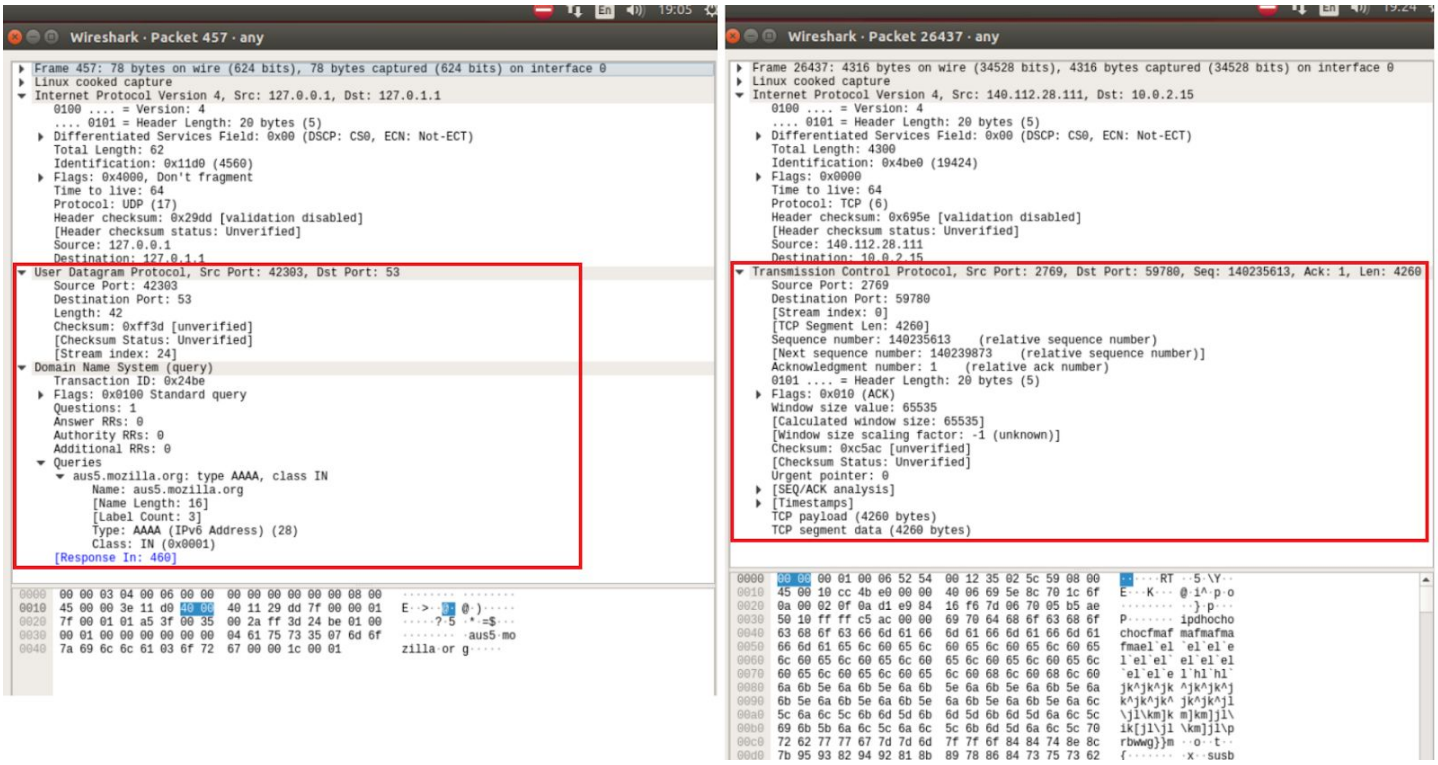
The webserver of the packet is aus5.mozilla.org. It is the current server that firefox would need to access for auto-update.

02 Analysis of TCP packets



The server uses port 2769 for this application.

03 Compare the headers of transport layer between TCP and UDP



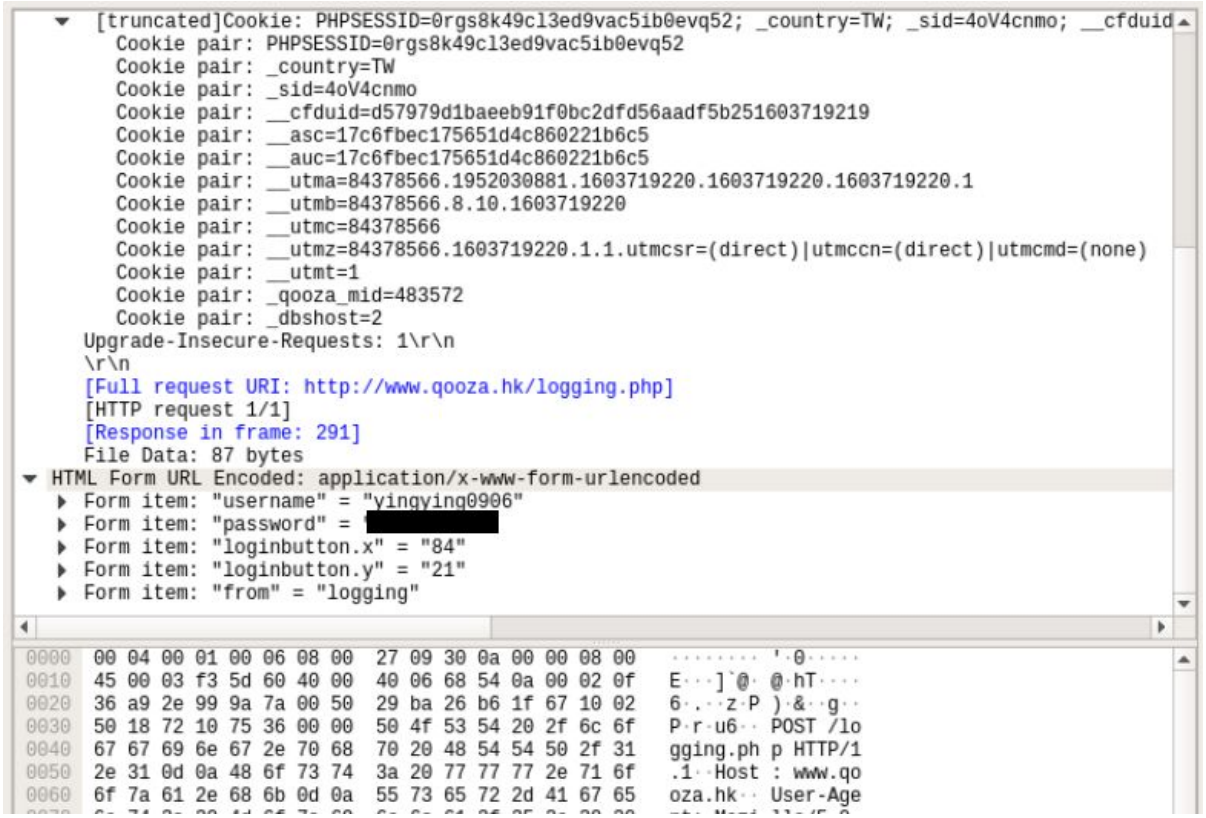
The headers of the TCP packet are similar to the headers of the UDP packet. They both have Frame, Linux cooked capture, and Internet protocol version 4. The difference between them is shown in the image above.

There are two headers called “user datagram protocol” and “domain name system” in the UDP packet. However, this kind of information in the TCP packets is combined in one header called “transmission control protocol”.

By comparing the fields in these headers, there are some fields in the TCP packet that the UDP packet doesn’t exist, such as acknowledgment number, next sequence number, sequence number, timestamp, SEQ/ACK analysis, etc.

Also, there are some fields in the UDP packet that TCP packet doesn’t exist, such as questions, answer RRs, authority RRs, additional RRs etc.

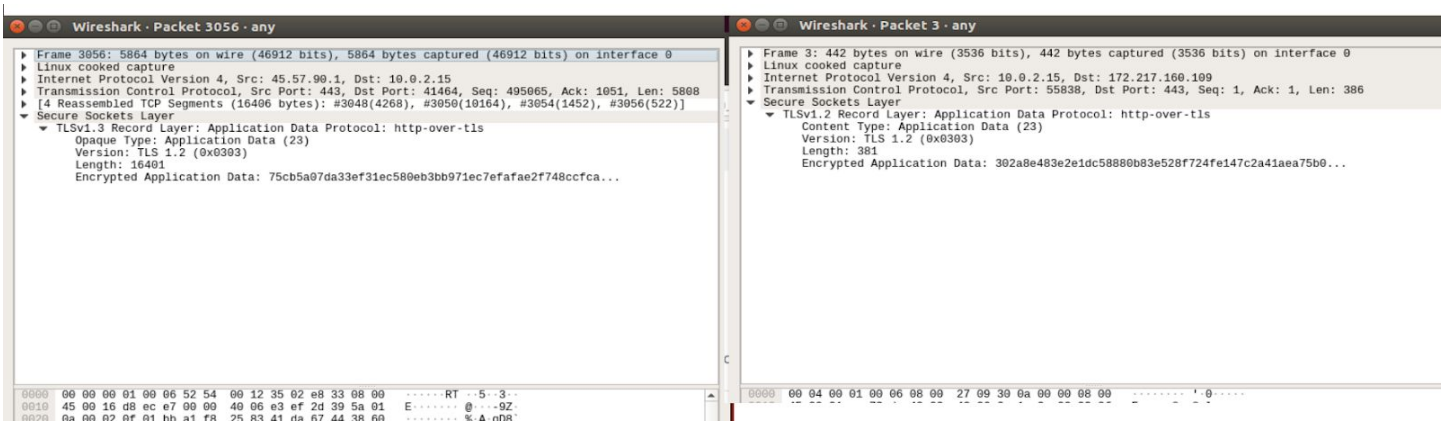
04 Find out a plaintext password



The website is called Qooza. It is a blog/weblog which was famous in Hong Kong since 2004 and it is still using HTTP. I typed my qooza account and found this packet in Wireshark.

It is not safe to send passwords in plaintext since the other people may get our password by capturing the packet that we send to the server. Once other people get our password, they can use our password to access the server to steal our personal information or carry out financial-related activities.

05 Other observations



I have tried to use the browser to browse two famous websites: Netflix and Gmail, and capture the packets of them. Both of them have a header called “secure sockets layer” and it shows that they are using http over tls.

Reference:

1. *https://support.mozilla.org/bm/questions/1224757 (question 1)*
2. *http://www.qooza.hk/*