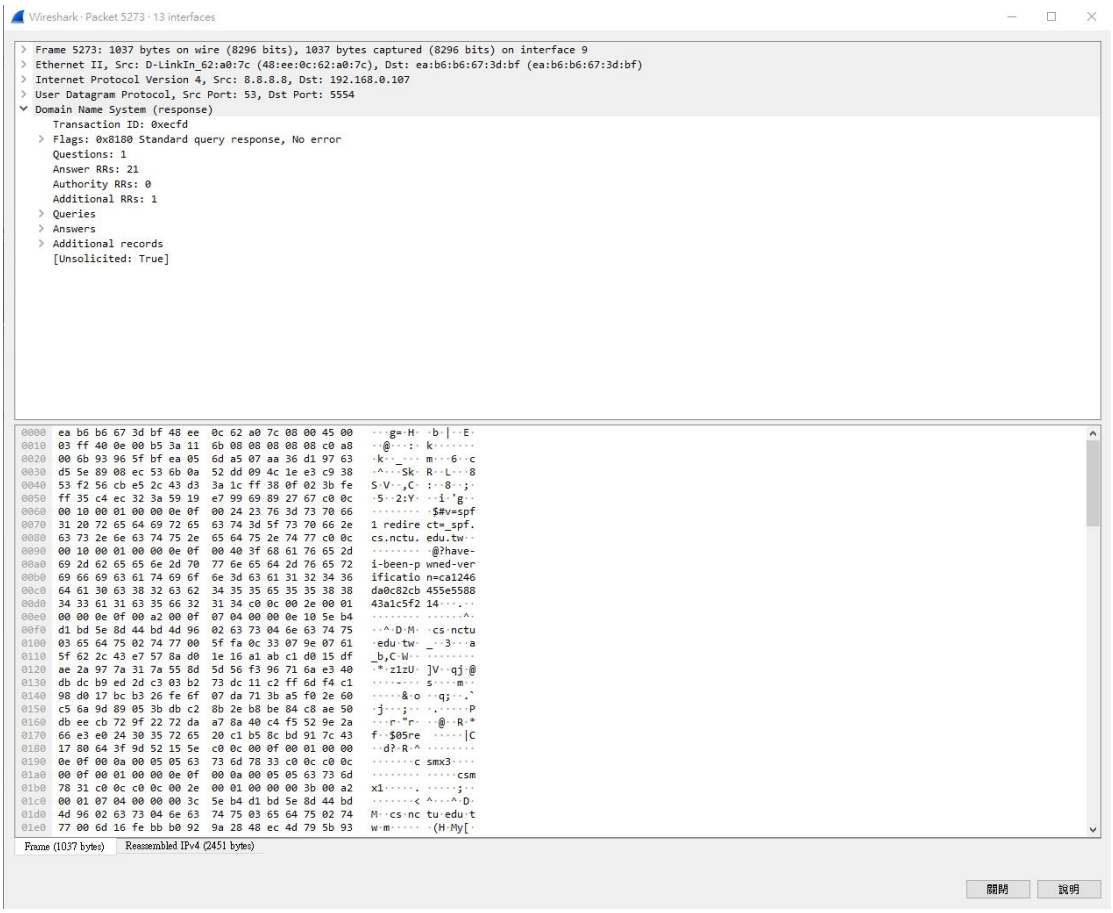
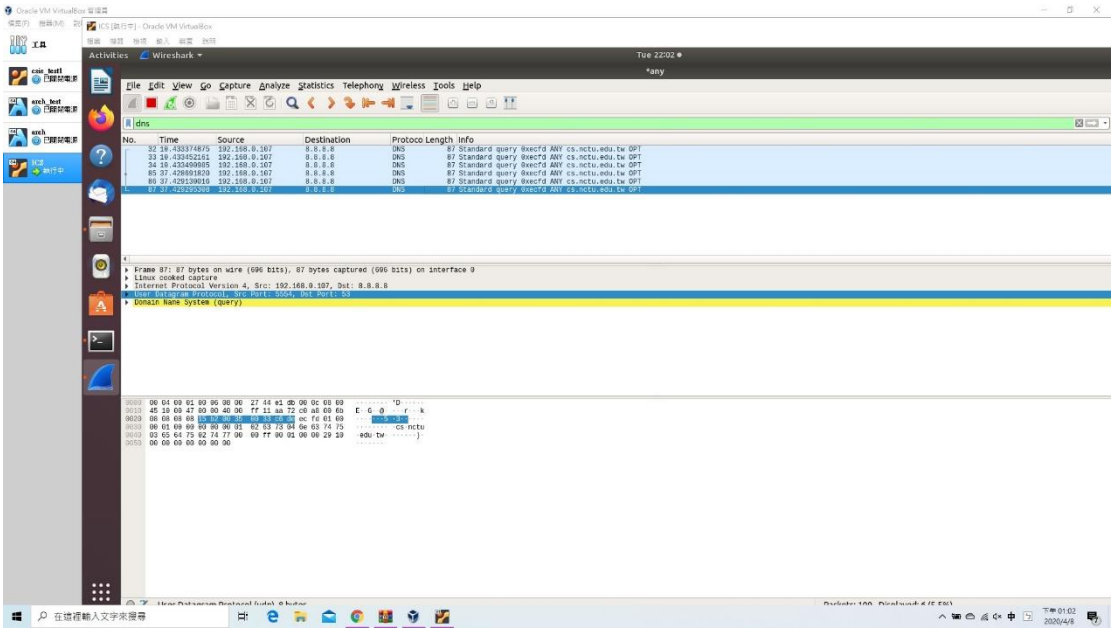
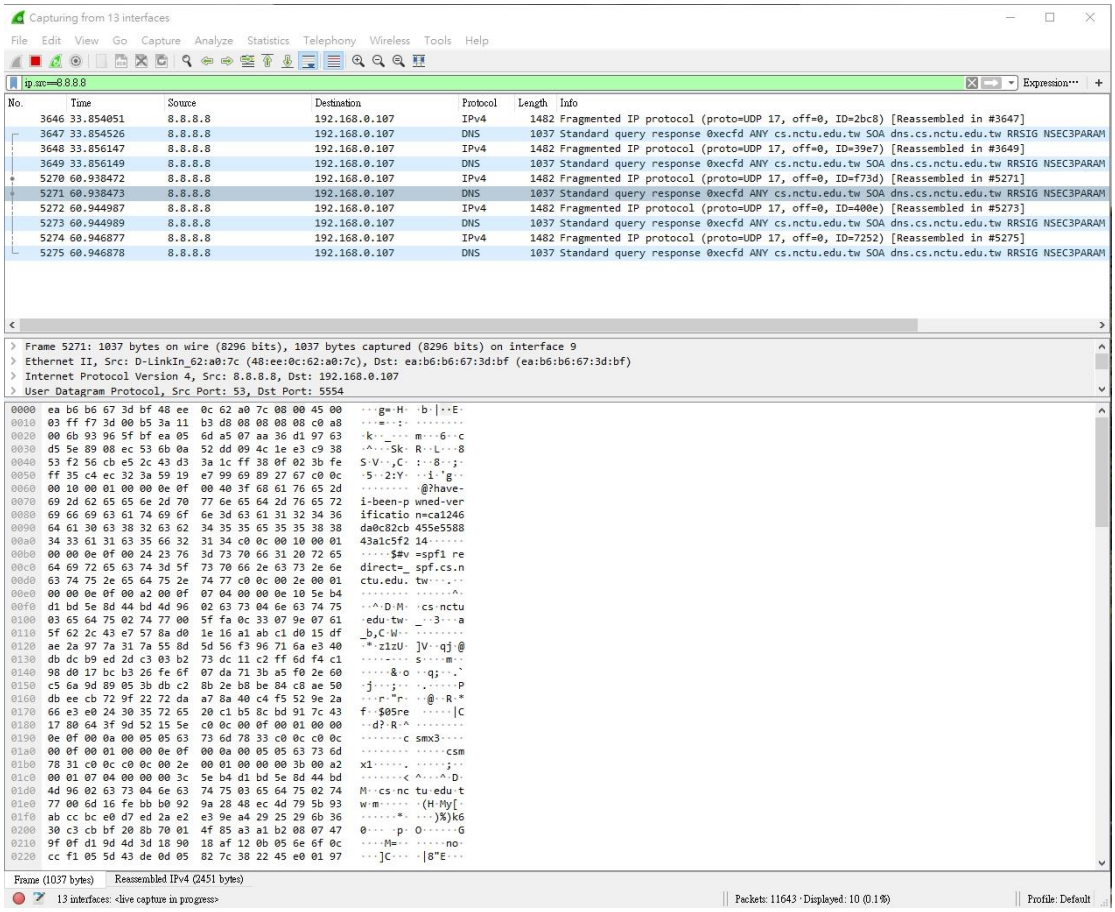
Computer Security Lab 1 Report

1. Please give evidence that you have finished Tasks I and II.







We got two response packets from the victim. One is the DNS packet, and the other is the IPv4 packet. These tow packets are nearly 29 times bigger than our request packet.

2. Please explain how you amplify the DNS response.

First, we open the Wireshark in our computer, and filter the packets using the keyword “DNS”. Then we check the packets with longer length, because we know that those destinations will respond us with a bigger packet than we sent, and we got the website “cs.nctu.edu.tw”. Besides of trying different destinations, we also change the query type into different resource records in order to try to get bigger response. Therefore, we chose 255, which means to send back all types of records which are known by the server. What’s more, we add an additional query after the normal DNS query to amplify the response. Finally, we send the packet using Virtual Box, and we get the response from the destination and using the question type we selected with a 29 times larger packet than we sent.

3. Please propose a solution that can defend against the DoS attack based on the DNS reflection.

We can use deep packet inspection (DPI) to check the packets we received are

malicious or not. DPI combines the functionality of an intrusion detection system (IDS) and an intrusion prevention system (IPS) with a traditional stateful firewall, while IPS compares the traffic signatures with the one it has within its database to detect the deviations, and IDS alerts the systems or takes actions to defense the attacks. So DPI, the combination of these two, can detect some attacks that can't be found by them. Using DPI can effective prevent attacks from viruses and worms. It can also be used at defense of DoS attacks.