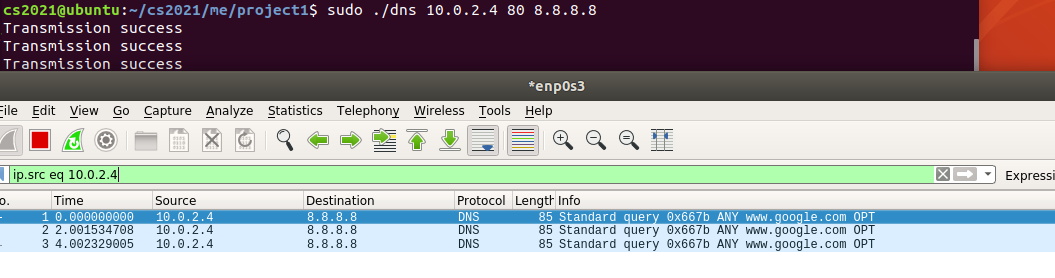
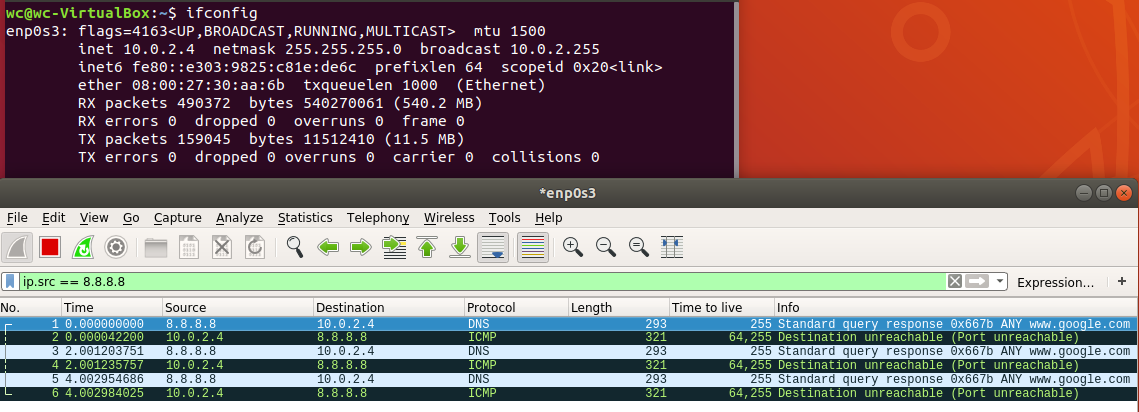
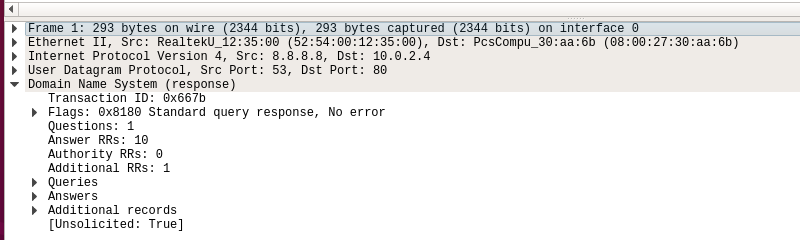
Item 1 (10%): please give evidence that you have finished Tasks I and II







The first picture is from the attacker, we run the code to spoof the victim ip 10.0.2.4 and pass DNS requests to 8.8.8.8.

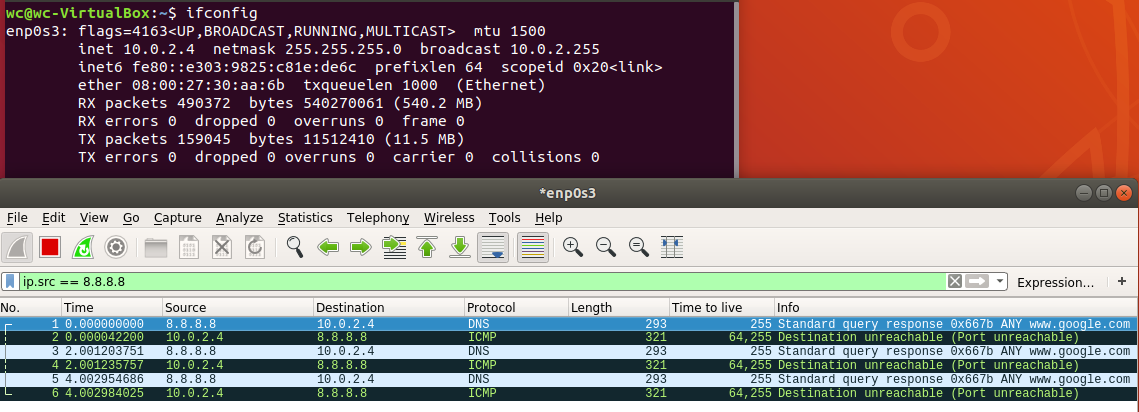
The second picture is from the victim, we can see the Uninvited DNS packet come from 8.8.8.8.

The third picture shows the transaction ID 0x667b which is my student id last 16 bits in hex.

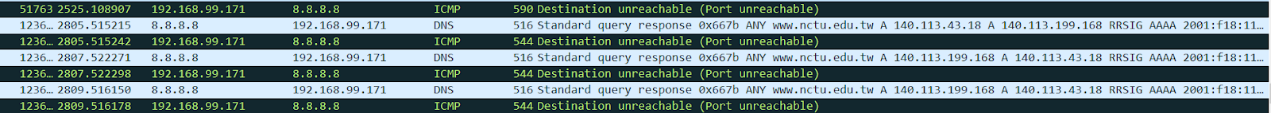
Item 2 (10%): please explain how you amplify the DNS response

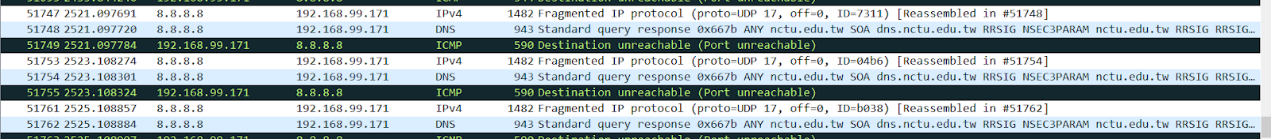
We found two ways to amplify dns response, first one is use EDNS extension to let response maximum size to 4096 bytes, so it can contain DNSSEC data, usually it can be ten times as large as before, but it is a little bit complicated.

Another way is to make the request ambiguous, which means it can contain not only a domain. We can see the response below.



This is a response from “[www.google.com](http://www.google.com)”, which size is 128.



This is a response from “[www.nctu.edu.tw](http://www.nctu.edu.tw)”, which size is 516.

This is the response from “nctu.edu.tw”, which size is 943.

Item 3 (10%): please propose a solution that can defend against the DoS attack based on the DNS reflection

I think using nat network which assign private IP dynamically is a good way to defend against the DoS attack based on DNS reflection, for users in nat network have no public IP, external attackers can’t target our computer easily.

In case there is a attacker who know our private IP and he/she is also in same nat network which mean he/she can spoof our IP address and DNS reply can pass nat and attack our computer, I think we can try to configure our gateway of nat to detect the unusual amount of DNS request from a specific IP address and actively request the host to change private IP address,  so attacker will loss the target ip address.

Last resort is to construct our own DNS server and block all DNS packets except the one we constructed, and observe the abnormal amount of requests in our server to find the attacker in our private network.