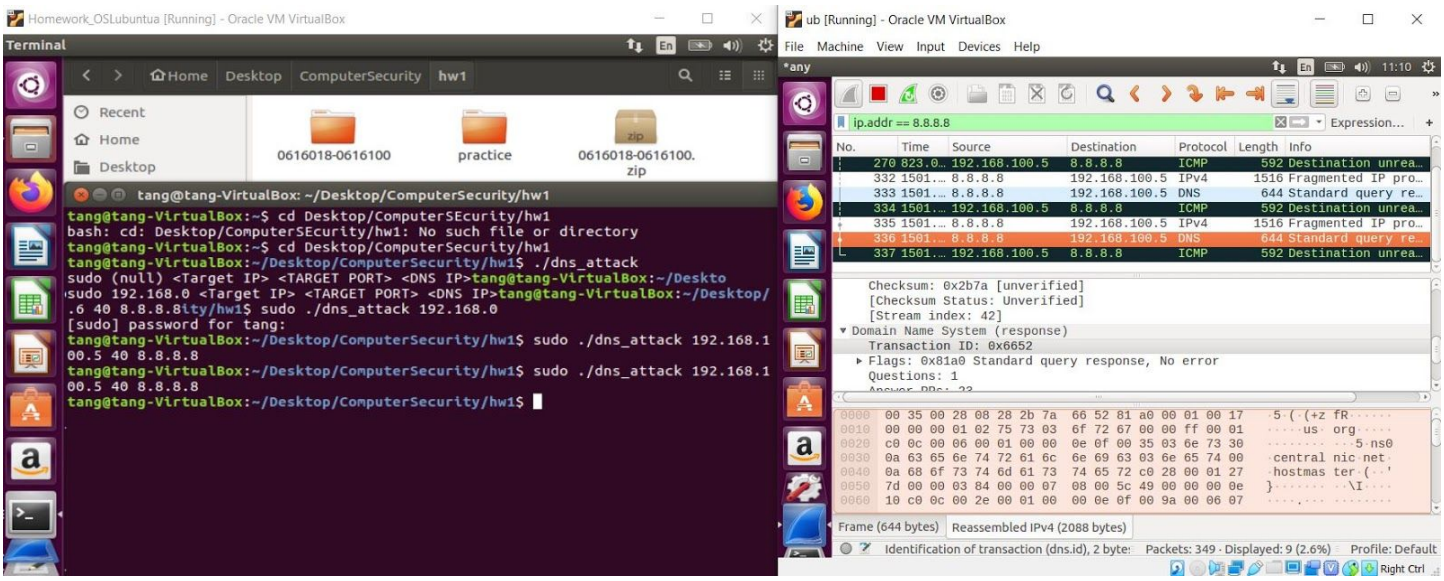
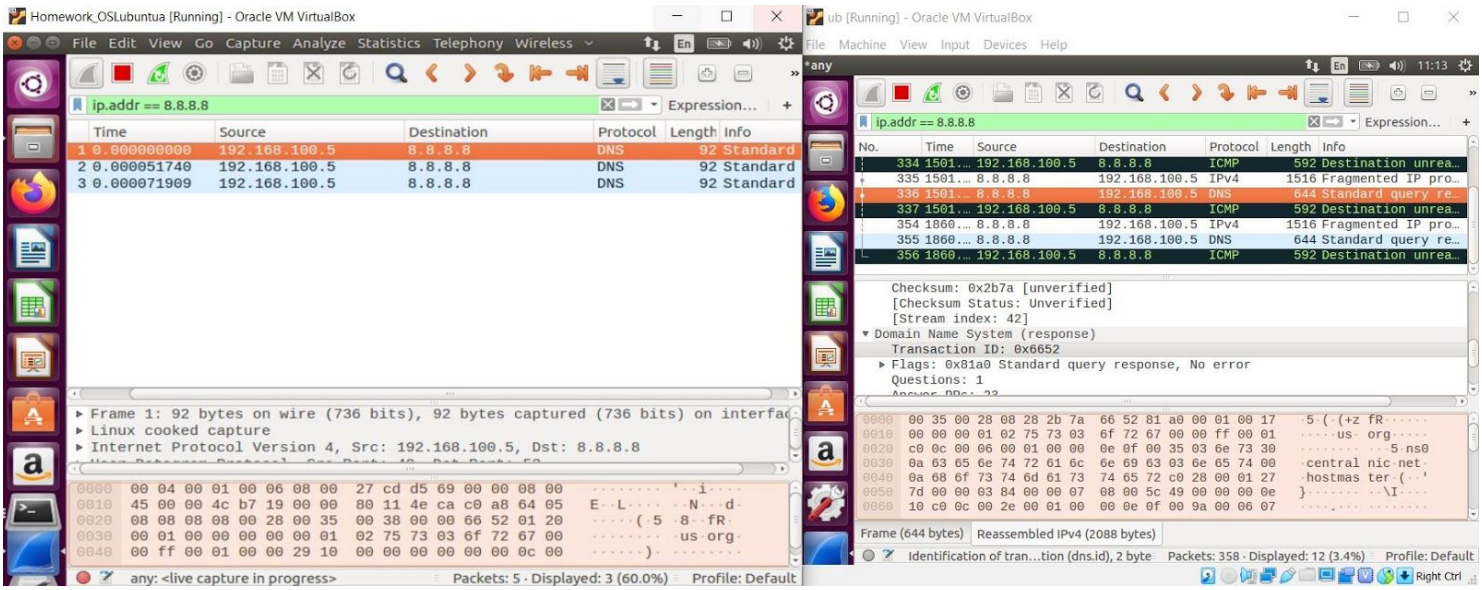
Report

Please give evidence that you have finished Tasks I and II



The screenshot above shows that we are able to reflect the DNS query from one to another.



This screenshot shows that the DNS Amplification is a success.

All files in the directory practice (./practice) are also evidences that we did the whole works. We search many references to get the work done.

please explain how you amplify the DNS response

1. We set the rd(recursive desired) to 1 to enable recursive functionality.
2. We try many query types and choose the one which has the largest response. The result is any which is 0xff .
3. We try many domain names and choose the one which has the best performance. The result is us.org .
4. We use extended dns to enlarge the dns response.

please propose a solution that can defend against the DoS attack based on the DNS reflection

1. Limit the packet from a specific source if it is too noisy.
2. Because of the identifiable structure of the DNS reflection, we can use regular expression filter to detect them.
3. Block some ports like UDP port 53.