**Cyber Network Security Project 2 | Undergraduate Group**

1. After DenisDNS gets a response from the recursive DNS server (i.e., the WSU DNS Server in this case), does it properly check the IP address of the recursive DNS server?

Answer Question 1:

After examining the project code, there does not seem to be at any point where the DenisDNS gets a response, there is no check at all to see if the received IP address is the IP address from the recursive server. All that happens is the address is simply sent into a buffer.

Image:

A screenshot of a social media post

Description automatically generated

1. Does DenisDNS properly check the transaction ID in responses from DNS server?

Answer Question 2:

No there is no check for the transaction ID, there should be a check for the transaction ID after a response is received but before the response is being displayed. Only after the transaction ID is checked should the response be discarded. See the image below to see where in the project that this is occurring.

Image:

A screenshot of a cell phone

Description automatically generated

1. After DenisDNS gets a reply from the recursive DNS server (i.e., the WSU DNS Server in this case), does it actually check whether the domain name in this response match the domain in the query?

Answer Question 3:

There is no check for the IP address of the recursive DNS server, it should do a check after the packet is received by the client. In the client() function, in the Denis.java it sets the address of a datagrampacket to send. It could get that address and store it to a variable before sending the datagrampacket.

The client receives a datagrampacket that is then used to construct a DnsResponse. Before the DnsResponse is made, the program could get the address of the packet and compare it to the variable it made before. If they are not the same, then the packet is discarded.

Image:

A screenshot of a cell phone

Description automatically generated

1. If DenisDNS gets a response, how long will it cache it for?

Answer Question 4:

From reviewing the code in the project, there seems to be no way to remove HostRecords from HostCashe. Meaning that the server is not able to remove Records from the cache while it is operational. This means that as long as the server exists, records in it’s cache will exist only ceasing to do so when the program execution ends and the memory is freed up by garbage collection.

Image:

A screenshot of a cell phone

Description automatically generated