Task 3.3

Important DNS Header fields:

ID : The identifier is necessary to math a reply to a specific request. Therefore this field is important to fake an answer for a specific request.

QR: This is a one bit field which makes a message a request (0) or a response(1). To spoof a response this field is important to be set at 1.

RCODE: This field needs to be set to 0 to communicate that there was no error at the name server while handling the request.

Important DNS Answer fields:

In my opinion, all fields of the DNS Answer are important to spoof a answer as this should be as realistic as possible and should be sure to be recognized as a real answer.

A special focus should be on the NAME field, which should be identically to the NAME of the query, and the RDATA which is the actual response.

The source code is located in the packetSniffer director.
The recorded output was piped to the snifferOutput.txt in the Task3_3 directory. Furthermore we recorded a pcap file to differ between Queries and Replies as well as see the actual Requests and Responses.