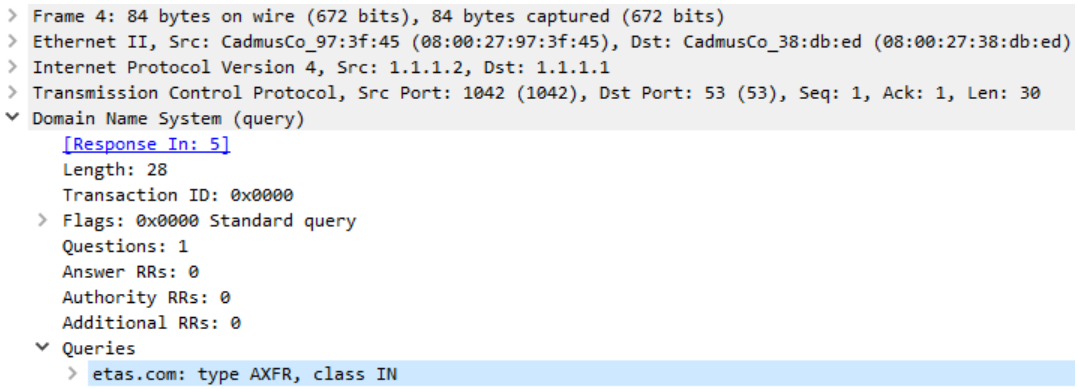
Network Traffic Analysis

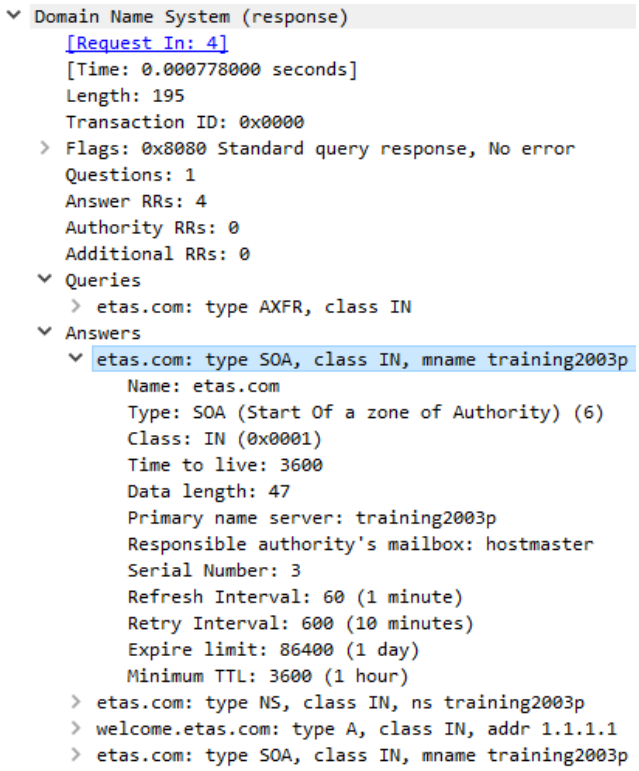
DNS (Easy)

This challenge evaluates the contestant's ability to understand a packet capture containing network traffic using the DNS protocol. Use Wireshark to solve the challenge.

Questions 1 and 2 can be solved by looking for a packet with "Standard query" in the info column (packet #4). Once found, the Wireshark dissector will yield the answers.



Questions 3 – 5 can be solved by looking for a packet with “Standard query response” in the info column (packet #5). Once found, the Wireshark dissector will yield the answers.



Question	Answer
What was the type of the DNS query requested?	AXFR
What domain was requested?	etas.com
How many items were in the response?	4
What is the TTL for all of the records?	3600
What is the IP address for the "welcome" subdomain?	1.1.1.1