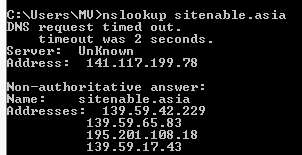
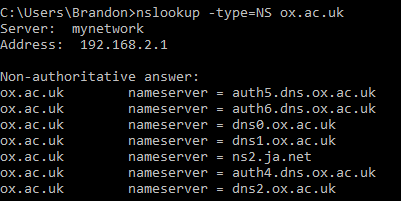
**Wireshark Lab: DNS**

**nslookup**

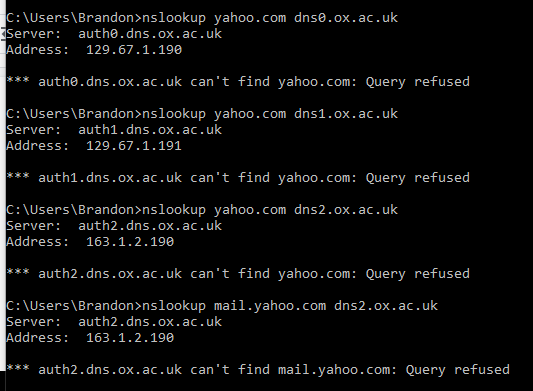
1. I conducted an nslookup on sitenable.asia



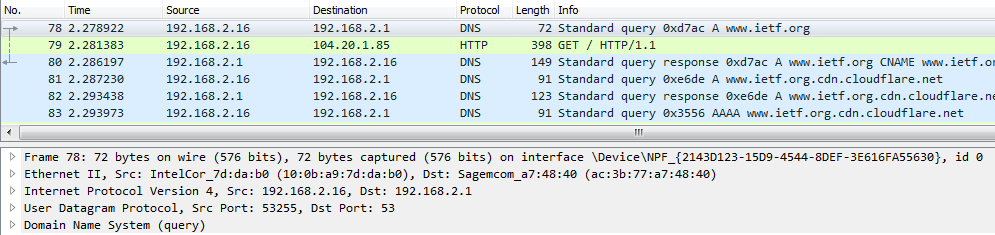
2.



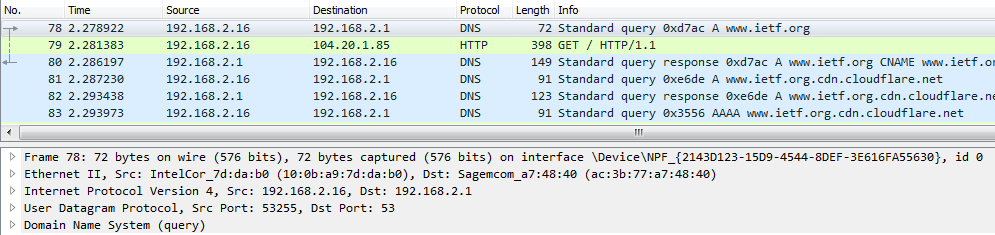
3.



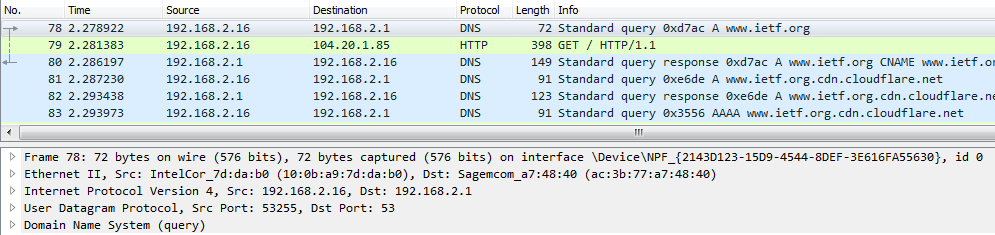
4. DNS query is sent over UDP

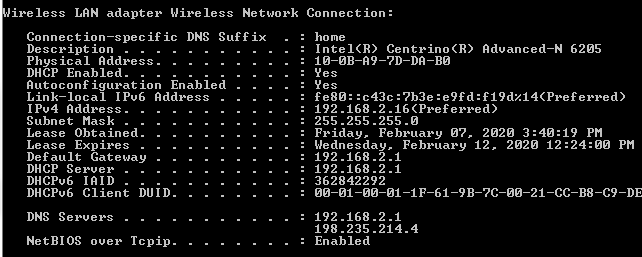


5. DST port is 53 and the SRC port is 53255

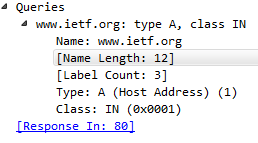


6. The Destination IP is 192.168.2.1 which is the IP of my local DNS server

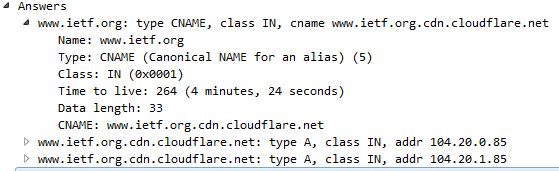




7. It is Type A, does not contain an answer

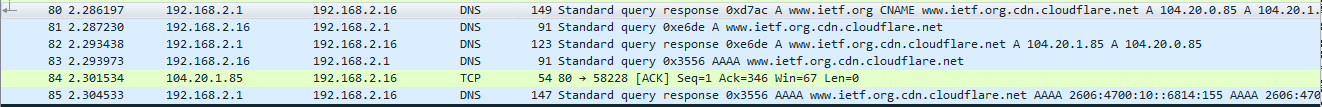


8. Contains 2 answers, one about the DNS server with Name, Type, Class, TTL, Data length and CNAME. Also contains CDN information.



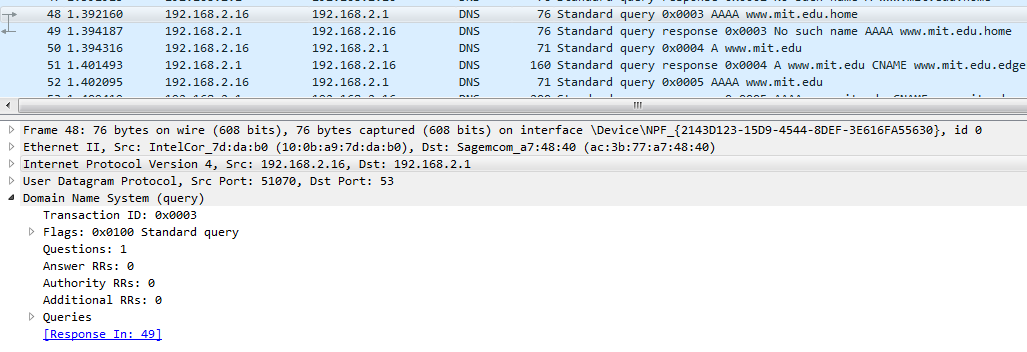
9. Yes, the destination address is the same as the address provided from the DNS server.

10. Yes, it issues more DNS queries to CDNs to load in more images for the website.

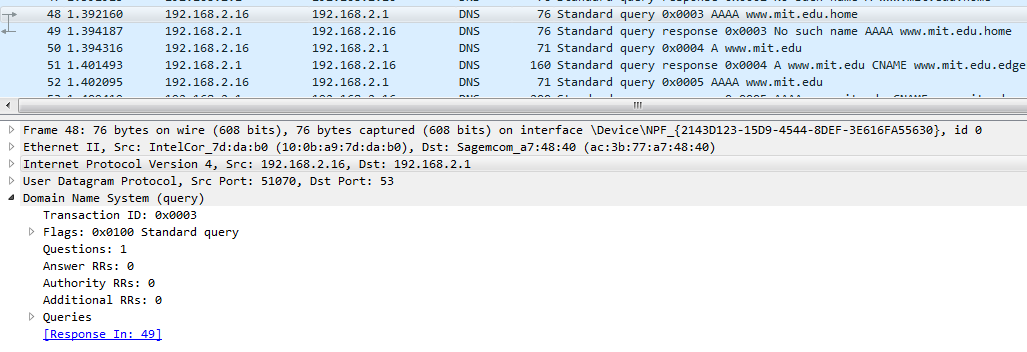


11. Destination Port for DNS Query Message: 53

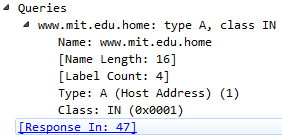
Source Port of Response DNS Response Message: 53



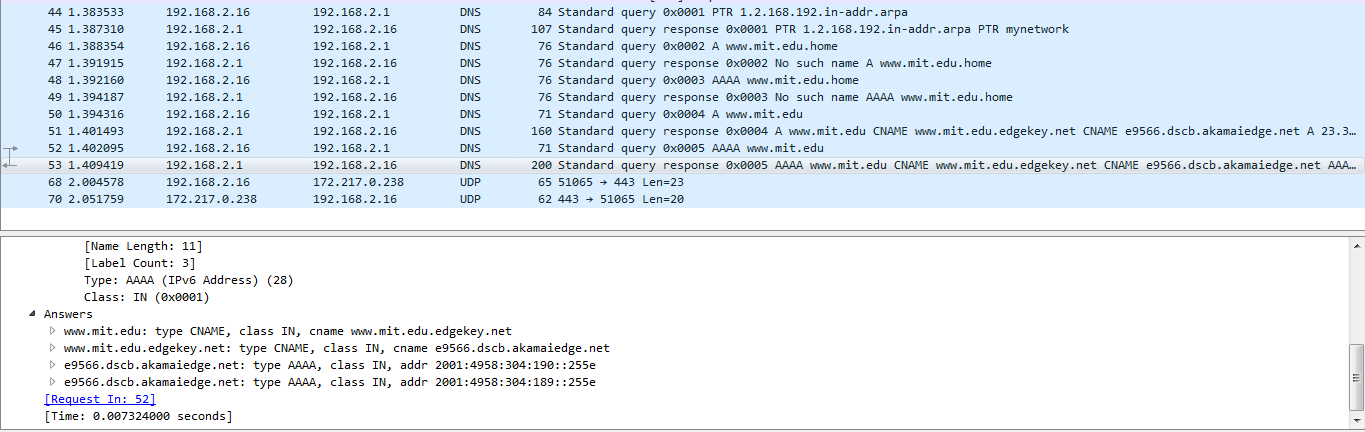
12. DNS query is sent to 192.168.2.1, that is my local DNS server



13. Type A, does not contain any answers



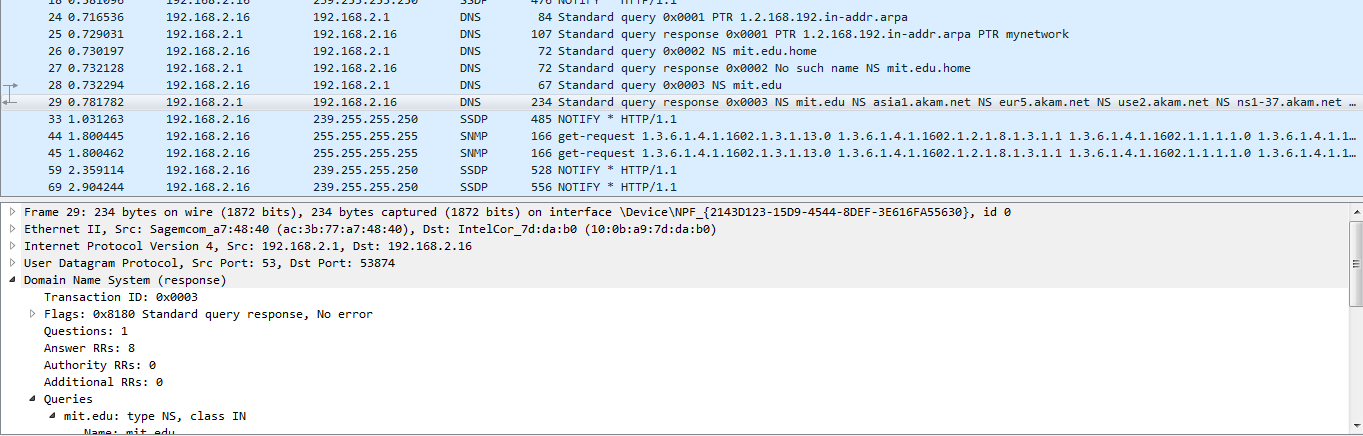
14. Answers are contained in the final response messages. This message is in response to a query of type AAAA. This final response message contains 4 answers. Each of these answers contain Name, Type, Class, TTL, Data length and CNAME. This can be seen in the screenshot below.

15. 

16. Yes, it is sent to 192.168.2.1, which is the default local DNS server.

17. Type is NS and does not contain any answers

18. Nameservers are Asia, Eur, USE, USW, and NS. Does not provide IP addresses of nameservers.

19. 

20. Query was sent to 18.0.72.3 which is the DNS server of bitsy.mit.edu. This is obviously not the address of the default local DNS server.

21. Type A, does not contain any answers.

22. No response messages were sent.

23. 