Thank you for your post, you provided some insightful information. Your hop count was 25 hops, which seems to be slightly longer than other results. Two of the hops had dropped due to exceeding the TTL of the packets (Parziale et al, 2006). As well the latency increased rather drastically from hop eight to nine. They consisted though and there were no drops towards the end, so it reached the destination with no problem. The name server and mail server results also were consistent with other user tests. Dig in particular is a powerful tool that provides a lot of built-in functionality. It can be a bit more complicated than nslookup in everyday use, however. As well, nslookup is technically deprecated, meaning it is good to learn other alternatives.

It is interesting to bring up how there are several name servers for redundancy. As you stated this would help against Denial of service(Dos) attacks, by providing redundancy. However, as shown in the work above, it is rather easy to find the IP addresses of these servers. A DDoS attack would be rather effective against this site (cisa, 2019). The scans show that other alternatives are needed to secure them such as the use of proxy or a NAT firewall.

References:

CISA.(2010) Understanding Denial-of-Service Attacks. Available from: <https://www.cisa.gov/uscert/ncas/tips/ST04-015> [Accessed 11 December 2021].

Parziale et al.(2006) *TCP/IP Tutorial and Technical Overview.* 8th ed. New York: IBM Redbooks. Available from: <https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf> [Accessed 11 December 2021].