Thank you, Zihaad, for the informative post. The dig command was utilised to identify the name servers, a valuable tool for finding the information quickly. The Domain Information Grouper (dig) allows you to specify all aspects of the query you wish to pursue.

Dig cleverly specifies arguments in any order and usually defines the type of record rather than the domain name you want to look up (O'Reilly & Associates, 2002). Therefore dig is helpful due to greater options and configuration changes for query information rather than the basic nslookup queries. Dig offers options to send queries to specified ports (-p port) instead of port 53, which is usually default and also send TCP based queries (+vc) (Parziale, 2006).

Limitations of this tool can stem from queries that do not hold information about the client who initiated the query. Therefore threat actors tend to prefer this as the server-side will only see the IP address where the query came from, and attackers could manipulate this.

Although the nslookup is a powerful tool, it supported the findings of the mail record in your investigation. It translated the domain names into IP addresses which is helpful for non-technical operators. In accompaniment to the dig command, they compliment network debugging.

O'Reilly & Associates. (2002). DNS and BIND. Available: [**https://docstore.mik.ua/orelly/networking\_2ndEd/dns/ch12\_09.htm**](https://docstore.mik.ua/orelly/networking_2ndEd/dns/ch12_09.htm)[Accessed 13 December 2021].

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006). *TCP/IP Tutorial And Technical Overview.*.8th ed. New York, IBM.