Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log

The traffic log indicates that a client (192.51.100.15) is trying to query the DNS server (203.0.113.2) for the IP address of the website "yummyrecipesforme.com". However, instead of receiving the expected IP address, the client is getting ICMP error messages from the DNS server, stating that the UDP port 53 (the standard port used for DNS queries) is unreachable.

Part 2: Explain your analysis of the data and provide one solution to implement

The log shows three attempts by the client to query the DNS server, each followed by an ICMP error message. The problem appears to be related to the DNS server being unable to respond to the queries on UDP port 53.
This could be caused by a network configuration, a failure of the DNS server, or the DNS server is under a DDoS or DoS attack.

One possible solution to try if you do not have access to the DNS server, is to temporarily switch to an alternative DNS server, for instance Google Public DNS or OpenDNS.