Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the client company website: yummyrecipesforme.com. Port 53 is normally utilized as a port for a DNS service. It is also substantiated by the query identification number 35084 which indicates flags with the UDP message and the “A?” symbol which indicates flags performing DNS protocol operations. This possibly indicates an issue with a firewall blocking access, an issue on the service provider’s behalf, or a malicious attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred just before 1:24 p.m. when several client customers reported they were not able to access the client company website. I am the initial responder on behalf of the security team and have begun running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS service(s), is unreachable. I and the rest of the security team will be investigating further on our end to resume access; including identifying if it is truly down or seeing if a firewall is blocking access to the specified port, but will also immediately contact the DNS service provider to determine whether it is a misconfiguration on their part or if a successful Denial of Service attack has been carried out.