# Cybersecurity Incident Report:
# Network Traffic Analysis

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

The UDP protocol reveals that port 53 is unreachable when attempting to reach yummyrecipesforme.com. Port 53 is usually used for DNS service, which indicates that the UDP requesting an IP address for the domain “yummyrecipesforme.com” did not go through the DNS server as no one was listening to the receiving DNS port. This is further explained by the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. This means the port is most likely not open or is blocked by a firewall or misconfiguration. It could also mean that the NDS service is not running or is routing to a non-existent DNS server. The service could also be facing downtime.

## Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The incident was confirmed to be existent at 1:24 pm. The incident was discovered as several customers of clients have reported they were not accessing the client company website www.yummyrecipesforme.com and saw the error “destination port unreachable” upon attempts to reach it. Investigations using a network analyzer tool (tcpdump) were attempted to analyze the network packets. The reports show that the UDP packets were not reaching port 53, which is used for DNS service. The unreachable indicates that the UDP message was not successfully sent due to no service listening on the receiving end of the port. The next steps include verifying the DNS server is running and actively listening on port 53, checking firewall rules that they are not blocking port 53 traffic, testing different DNS servers to see if the issue persists, checking the network routing as well as any other logs. The possible causes could include a Denial of Service attack or a misconfiguration.