Cybersecurity Incident Report:
Network Traffic Analysis

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

The DNS protocol reveals that the UDP protocol was used to contact the DSN server to retrieve the IP address for the domain name of yummyrecipesforme.com. The first 2 lines of the UDP message going from the client's browser to the DNS server are in the first two lines of the log. The third and fourth lines of the message contain the ICMP error response. The UDP protocol reveals that port 53 is unreachable when attempting to access the yummyrecipesforme.com website. This is based on the results of the network analysis, which show the query identification number of 35084 which indicates flags with the UDP message and the "A?" symbol indicating flags with performing DNS protocol operations.

The port noted in the error message (53) is used for: DNS services. The most likely issue is that the message did not go through to the DNS server because no service was listening or responding on the indicated port.

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

Time incident occurred this afternoon when several customers of yummyrecipesforme.com reported that they were unable to access the website and received an error stating "destination port unreachable" after waiting for the page to load. The IT department responded and began running tests with the network analyzer tool tcpdump and received first logs at 1:24pm. The resulting logs indicated that UDP port 53, used for DNS services, is unreachable or non-responsive. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server may be down due to a DoS attack or misconfiguration.