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 that was used to contact the DNS server to retrieve the IP address of a domain name reveals that port 53 is unreachable when attempting to connect to yummyrecipesforme website. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message udp port 53 unreachable on the third and fourth line. Port 53 is normally used for DNS traffic, therefore, we know this is an issue with the DNS server. Issues are further evident due to the flag of the message being "A?" which indicates DNS protocol operations. Due to the error message and the flag, it is highly likely that the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred earlier this afternoon at 13:24. Several customers reported that they were not able to access the client company website, and they were receiving the error "destination port unreachable". The IT department responded and began running tests with the network protocol analyser tool tcpdump. The resulting logs revealed that port 53, which is used for DNS traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. The message indicates that the request did not go through to the DNS server because no service was listening on the receiving DNS port. The possible root cause of this issue may be firewall configuration blocking port 53 or a possible malicious attack on the DNS server causing the server to be down.