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 the ICMP packet was undeliverable to port 53 of the DNS server. 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". The port noted in the error message is commonly used for DNS protocol traffic. 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 today at 1:23pm. We became aware of the incident through several customer reports stating they were not able to access the website and received the message "destination port unreachable". Security engineers are in the process of handling this incident so that users can visit the website again. In our investigation we conducted packet sniffing tests using tcpdump. The resulting logs revealed that port 53 is unreachable. This indicates that the message did not get through to the DNS server because no service was listening on the receiving DNS port. The next step is to determine if the DNS server is down or the traffic to port 53 is being blocked by the firewall. The likely cause of the incident is a Denial of Service attack or a misconfiguration.