Cybersecurity Incident Report:
Network Traffic Analysis

Summary of the problem found in the DNS and ICMP traffic log
Based on the network analysis results, it can be inferred that the DNS server is either down or unreachable. This conclusion is supported by the ICMP echo reply error message stating "udp port 53 unreachable." Port 53 is typically associated with DNS protocol traffic, indicating a high likelihood that the DNS server is not responding.

Analysis of the data and possible solution to implement.
at 1:23 p.m., the organization received reports from customers stating that they encountered the error message "destination port unreachable" when attempting to access the website. As a result, the organization's IT team was notified and has initiated an investigation to resolve the issue and restore website access for customers. During the investigation, network security professionals performed packet sniffing tests using tcpdump. Analysis of the resulting log file revealed that the DNS port 53 was unreachable. The next course of action is to determine whether the DNS server is offline or if traffic to port 53 is being blocked by the firewall. The unavailability of the DNS server could be attributed to a successful Denial of Service (DoS) attack or a misconfiguration.