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 DNS server is down or unreachable. As evident by the results of the network analysis, the ICMP echo reply returned the error message “udp port 53 unreachable”. Port 53 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 one solution to implement
This incident occurred around 1:24 pm when customers reported that they received the message “destination port unreachable” when they attempted to visit the website. The network security professionals within the organization are currently investigating the issue so customers can access the website again. In our investigation, we conducted packet sniffing tcpdump. In the resulting logs file, we found that port 53, which is used for DNS configuration, was unreachable. Our next steps include checking the firewall configuration to see if port 53 is blocked. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.