Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The network protocol analyzer log tells that the DNS server is not reachable. The ICMP reply was “udp port 53 unreachable” where port 53 is DNS protocol. So, most likely the DNS server is not responding to the request.

Part 2: Explain your analysis of the data and provide one solution to implement
This incident happened at 1:23 p.m. The customers informed the IT team that they received “destination port unreachable” message when they enter the website. The investigation regarding this issue was carried on where packet sniffing test using tcpdump was conducted. We found out that the DNS port 53 was unreachable. Next, we will identify if the DNS server is down or traffic to port 53 is blocked by the firewall. DNS server can be down due to a successful DoS attack or misconfiguration.