Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
DNS server is down as indicated by the UDP protocol. ICMP echo returned error message “upd port 53 unreachable”, port 53 is used for DNS protocol traffic. Likely that DNS server not responding.

Part 2: Explain your analysis of the data and provide one solution to implement
Clients called the company to let the IT team know that they were receiving messaging like “destination port unreachable” when visiting the website. Currently the issue is being investigated, current findings indicate that DNS port 53 is unreachable via UDP. Next step is to identify if the DNS server is down or if the traffic to port 53 is blocked by the firewall. DNS server might be down due to DOS attack.