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 port 53 is unreachable when attempting to access the webpage. The ICMP echo replies the error message “udp port 53 unreachable”. Normally the port 53 is used for DNS translating.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:23 p.m. Customers notified the company that they received the “destination port unreachable” message. The network security professionals within the organization are currently investigating the issue, we first conducted packet sniffing using tcpdump. Next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful DoS attack or a misconfiguration.