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 shows that the DNS server is unreachable. As for the result of the network analysis, the ICMP echo returned the error message “udp port 53 unreachable”, Port 53 is used for DNS protocol traffic. Most likely, the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred today at 1:23pm. Customers were reaching out to the organization to notify the IT team that a message of “destination port unreachable” was received when they attempted to visit the website. The security team within the organization is currently investigating the issue so the customers can proceed in accessing the website. Upon investigating, we conducted packet sniffing tests using tcpdump. As a result, we found that DNS port 53 was unreachable. The 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 Denial of Service (DoS) attack or misconfiguration.