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 DNS server is unreachable. This is based on the results of the network analysis, which shows the ICMP echo reply error message: udp port 53 unreachable. The port noted in the error message is used for domain name resolution. This most likely indicates an issue with the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred today at 1:23 pm. Customers contacted the company IT team to report their inability to access the company website. When trying to access the website, the error “destination port unreachable” appears. The organization's network security experts are actively examining the problem to restore customer access to the website. During our inquiry, we performed packet capture tests with tcpdump. In the log file, it is shown that DNS port 53 was inaccessible. Our subsequent task is to determine if the DNS server is offline or if traffic to port 53 is obstructed by the firewall. The DNS server's unavailability could also be a result from either a successful Denial of Service attack or a configuration issue.