Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The DNS server is offline or unreachable, according to the UDP protocol. The ICMP echo reply gave the error message "udp port 53 unreachable," which is consistent with the findings of the network investigation. Port 53 is frequently used for DNS protocol traffic. The likelihood that the DNS server is not responding is very high.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident took place around 1:23 p.m. Customers contacted the company to inform the IT department that when they tried to access the website, they were greeted with the notice "destination port unreachable". In order to restore customer access to the website, the organization's network security experts are now looking into the problem. Using tcpdump, we tested packet sniffing techniques as part of our examination of the problem. We discovered that DNS port 53 was unavailable in the resulting log file. The next step is to determine whether the DNS server is unavailable or the firewall is blocking communication to port 53. Due to a successful Denial of Service attack or a misconfiguration, the DNS server may be unavailable.