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 down or unreachable. The ICMP echo reply returned the error message “udp port 53 unreachable.” Port 53 is commonly used for DNS protocol traffic. It’s most plausible that 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 at 1:23 p.m. Customers contacted the organization to notify that they received the message “destination port unreachable” when they tried to visit the website. In the investigation of the issue, we used packet sniffing tests using tcpdump and 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 attack or a misconfiguration.