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. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “udp port 53 unreachable”. The port noted in the error message is used for DNS service. And the most likely issue is the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred in the afternoon, 1:23 p.m.. Several customers contacted the company to report that they received the message “destination port unreachable” when they attempted to visit the website. Then the team began running tests with the network protocol analyzer tool, tcpdump, and the resulting log file shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: “udp port 53 unreachable.” The DNS server might be down due to a successful DoS attack or a misconfiguration.