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. Shown in the ICMP echo reply as “udp port 53 unreachable”. This could mean that the DNS server is not responding as port 53 is commonly used for DNS servers.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident happened today at 1:24 pm. Network security was notified of an error message stating “destination port unreachable.” We conducted packet sniffing using tcpdump, and the resulting log file showed that port 53 was unreachable. The DNS server could be down due to successful DoS or not being set up properly. This could mean that the DNS server is down or traffic is being blocked by a firewall.