Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The network protocol analyzer logs indicate that port 53/UDP is unreachable when attempting to access the website. Port 53 UDP unreachable errors can occur when the DNS server is temporarily unavailable or offline. It is possible that this is an indication of a malicious attack on the DNS server.

Part 2: Explain your analysis of the data and provide one solution to implement
This incident occurred when several customers contacted the company to report that they could not access the company website and saw the error "destination port unreachable" after waiting for the page to load. I was tasked to analyze the situation. After visiting the website to ensure the error, I start running tests with the tcpdump tool. The resulting logs revealed that port 53/UDP, used for DNS traffic, is unreachable. I continue to investigate the root cause of the issue to determine how I can restore access to the website. My next steps include using an alternative DNS server to see if the issue persists and contacting the DNS server administrator. I suspect that the DNS server was intentionally flooded in order to bring down the website.