Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
To load the webpage, the browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the domain name of yummyrecipesforme.com. The network analyzer shows that when I send UDP packets to the DNS server, I receive ICMP packets containing the error message: “udp port 53 unreachable.” Since port 53 is associated with DNS protocol traffic, this issue is likely caused by the DNS server not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occured today at 13:24. Customers reported that they were not able to access the company website www.yummyrecipesforme.com, and received the error “destination port unreachable”. During our investigation into the issue, we conducted packet sniffing tests using tcpdump. We concluded that the issue is likely caused by the DNS server. The DNS server might be down due to a Denial of Service attack or a misconfiguration and the next step is to verify the integrity and configuration of the DNS server.