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 is unreachable when attempting to access ‘yummyrecipesforme.com’. Port 53 is aligned to the .domain extension in 203.0.113.2.domain, and is a well-known port for DNS service. The word “unreachable” in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.”

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24 when several customers contacted your company to report that they were not able to access the company website ‘yummyrecipesforme.com’. A cybersecurity analyst responded and began by first visiting the website and also received the error “destination port unreachable.” Next, the analyst loaded the network analyzer tool, tcpdump, and loaded the webpage again. The analyzer shows that when UDP packets are sent and an ICMP response is received, the results contain an error message: “udp port 53 unreachable.” This error suggests that the DNS server responsible for resolving the domain name 'yummyrecipesforme.com' was not available or was not responding on port 53, which is the standard DNS port. The issue that led to the inaccessibility of our company website appears to be the unavailability of the DNS service on the DNS server responsible for 'yummyrecipesforme.com.'