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 "www.yummyrecipesforme.com". Port 53 is normally used for DNS service. This most likely indicates that the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port. It is a possibility that this is an indication of a malicious attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred in the early afternoon at 1:24 pm. The IT department was notified of the incident after several reports came in from customers that they were not able to access the client company website "www.yummyrecipesforme.com" due to the error "destination port unreachable". I was tasked with analyzing the situation and started by attempting to visit the website myself and I also received the error "destination port unreachable". In order to troubleshoot this issue I used my network analyzer tool, tcpdump, and attempted to load up the webpage again. As a result of using the analyzer for sending UDP packets to the DNS server, I received ICMP packets containing the error message: "UDP port 53 unreachable". Likely cause of the incident is that no service was listening on the receiving end of the port therefore making the web page unreachable. In the meantime this incident is being handled by security engineers after the analysis team has reported the issue to the direct supervisor.