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 reveals that: Sending a DNS query to the web server www.yummyreciplesforme.com fails. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 unreachable length 254. The port noted in the error message is used for: DNS. The most likely issue is: No service was listening on the receiving DNS port.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: at 1:24 p.m. Explain how the IT team became aware of the incident: IT became aware of the incident because several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable”. Explain the actions taken by the IT department to investigate the incident: To investigate the incident, IT attempts to reach the client company website themselves and verifies that the issue persists. To troubleshoot the issue, IT uses the network analyzer tcpdump to track the requests sent to and from the web server. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): By doing so, IT discovers the error message “udp port 53 unreachable”. Note a likely cause of the incident: Taking the newfound error message into consideration, the likely cause of the incident was that no service was listening on the receiving DNS port.