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: the client's website is unreachable because when UDP packets are sent to the DNS server, an ICMP packet is received containing an error message. 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." Port 53 is utilized for DNS traffic and the log data indicates flags due to the plus sign and "A?" after the query ID number. The port noted in the error message is used for: port 53. The most likely issue is: the DNS service on port 53 is not responding due to possibly being overloaded with too much traffic.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: Earlier this afternoon at 13:24 when the client's customers attempted to access the client's website and received an error message stating, "destination port unreachable." Explain how the IT team became aware of the incident: The client notified as soon as they received multiple reports of the website being unreachable. Explain the actions taken by the IT department to investigate the incident: The IT department began by attempting to visit the website to recreate the error message. Then, the team utilized tcpdump, a network analyzer tool, to capture traffic. This log data showed that port 53, DNS server, was unresponsive. Next steps will be to check firewall configurations to make sure port 53 is not being blocked. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Possible rival companies or threat actors looking to inflict financial and reputational damage to the client. Note a likely cause of the incident: Some type of DoS attack flooding port 53 with packets or possible misconfiguration.