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: **It is currently down or has an error** 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"** The port noted in the error message is used for: **DNS protocol traffic** The most likely issue is: "**The DNS server has an issue or is down**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: **1:24 PM** Explain how the IT team became aware of the incident: **Multiple customers have contacted and said that they were not able to access the website. Upon further investigation, errors did pop up.** Explain the actions taken by the IT department to investigate the incident: **This includes loading up tools such as the analyzer tool and tcpdumping.** Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **The network analyzer received a lot of packets and when sending a UDP packs, the response given back the error: "udp port 53 unreachable"** Note a likely cause of the incident: **Because the DNS port 53 is unreachable this means that the DNS server might be down.**