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 ICMP packet was undeliverable to the port of the DNS server** 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: **A port for DNS service** The most likely issue is: **The message request is undeliverable to the DNS server. My browser is unable to obtain the IP address for the website.**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: **1:24PM, 32.192571 seconds** Explain how the IT team became aware of the incident: **Several customers contacted the company to report that they were unable to access the company website** Explain the actions taken by the IT department to investigate the incident: **First, I visited the website to be met with a "destination port unreachable" error. Next, I loaded the network analyzer tool, tcpdump, and loaded the website again. This time, I received a lot of packets in the network analyzer.** Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **The ICMP packets were sent twice more but received the same delivery error.** Note a likely cause of the incident: