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 UDP packet was not able to be delivered to port 53 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: ***DNS service*** The most likely issue is: ***DNS server is not responsive***

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: ***this afternoon at 1:24 pm*** Explain how the IT team became aware of the incident: ***Several customers of clients reported they weren't able to access the client company website.*** Explain the actions taken by the IT department to investigate the incident: ***We attempted to visit the website and received the same error "destination port unreachable". Then, we ran tests with the network protocol analyzer tcpdump.*** Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): ***We found that the error message from response to the UDP packet shows the UDP packet was undeliverable to port 53 of the DNS server. For the ICMP error response, the source address is the IP address for the DNS server and the destination is our computer's IP address. The UDP message requesting an IP address for the website's domain didn't go through to the DNS server because no service was listening on the receiving DNS port.*** Note a likely cause of the incident: ***DoS attack on the DNS server since DNS server is not able to respond to UDP requests signifying possible server crash***