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: Port 53 is unreachable when trying to access the website 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 Protocol traffic The most likely issue is: The DNS server is not responding

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 p.m. Explain how the IT team became aware of the incident: Customers notified the organization that they received the message “destination port unreachable”. Explain the actions taken by the IT department to investigate the incident: packet sniffing tests using tcpdump Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Next step is to identify whether the DNS server is down or traffic to port 53 is blocked by a firewall. Note a likely cause of the incident: Denial of Service attack or misconfiguration.