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 is sent to the DNS server, but the port in charge of managing the response (port 53) is unreachable. 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 53 The port noted in the error message is used for: DNS services The most likely issue is: no service was listening on the receiving DNS port.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: at midday, at exactly 13:24. Explain how the IT team became aware of the incident: many customers of clients reported that they were not able to access the client company website. Explain the actions taken by the IT department to investigate the incident: the team attempted to load the webpage again while using the network analyzer tool, tcpdump, to look into the packets. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The ICMP error message shows a change in the length reported. Note a likely cause of the incident: 1. The DNS service is not running in port 53, is misconfigured. 2. The request is being firewalled by the server.