# 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: No service was running on port 53, as such there was no domain name resolution.

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: Domain Name Resolution

The most likely issue is: No service was listening on the receiving DNS port as indicated by the ICMP error message.

## Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred: 1:24p.m

Explain how the IT team became aware of the incident: The website was inaccessible, and checking the logs with the network analyzer tool revealed that there was

Explain the actions taken by the IT department to investigate the incident: Checked the webpage using tcpdump which revealed that port 53 was unreachable.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

Note a likely cause of the incident: The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.