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 DNS server does note respond to service request properly.

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: the server is down or the port is improperly configured.

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

Time incident occurred: 1:24 PM

Explain how the IT team became aware of the incident: Climent report that they were not able to access the website.

Explain the actions taken by the IT department to investigate the incident:the IT department used network analyzer tool to troubleshoot and attempt sending a packegate to the website. Where they identify that port 53 for DNS services failed to respond. This is likely due to error in configuring the DNS server or changes to the domain name, or the DNS server is down.