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: there is an error with the communication with the designation 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: port 53 is used for both TCPand UDPcommunication.

The most likely issue is:we cannot perform an handshake to establish a connection with the requested website.

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

Time incident occurred:1:24 p.m., 32.192571 seconds

Explain how the IT team became aware of the incident:when the users contacted the service provider and told about the problem to open the requested website.

Explain the actions taken by the IT department to investigate the incident: they first tried to open the site and get an error message then they deployed a tool named tcpdump which is used to get information about the network traffic and the problems faced by which part in the communication.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): IT department found that the problems was with port 53 which is used for communication

Note a likely cause of the incident: