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: Destination port (53) is unreachable or inaccessible

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 commonly used for DNS queries and responses

The most likely issue is: There is possible flooding of DNS queries on Port 53

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

The IT team became aware of the incident when several customers of clients reported that they were not able to access the client company website.

The IT department confirmed the problem by attempting to access the website and encountered the same error. A network analyzer tool was then used to investigate the issue and resulted with an error message stating “udp port 53 unreachable”.

The ICMP error message "udp port 53 unreachable" suggests that the DNS server is not able to receive the UDP packets on port 53, indicating a DNS resolution issue.

Note a likely cause of the incident is due to a potential DOS attack from outsider threats.