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 issue with accessing the website www.yummyrecipesforme.com due to an error message “udp port 53 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” showed multiple times

The port noted in the error message is used for: DNS queries, specifically it’s UDP port 53 which is standard for domain name system (DNS) queries.

The most likely issue is: a network or configuration problem causing DNS queries to be blocked or unable to reach their destination.

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

Time incident occurred: The first recorded instance was at 13:24:32 as per tcpdump log.

Explain how the IT team became aware of the incident: Several customers reported they were not able to access www.yummyrecipesforme.com and received an error “destination port unreachable”.

Explain the actions taken by the IT department to investigate the incident:
Attempted to visit website and confirmed receiving same error
Loaded network analyzer tool, tcpdump, and attempted to load webpage again
Analyzed logs for any anomalies or errors

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
Each attempt to access website resulted in ICMP packets containing “udp port 53 unreachable”
Indicates issue with DNS server or network path leading to it

Note a likely cause of the incident: Possible causes could include misconfiguration on DNS server, firewall blocking UDP port 53, or issues with intermediary networking equipment.