Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The **DNS and ICMP traffic log** analysis revealed that there was a communication failure between the client's system and the DNS server. The **UDP protocol** was used to send a DNS query for resolving the domain name of `www.yummyrecipesforme.com` into an IP address, which is a normal process for loading a webpage.

However, the **ICMP echo reply** returned an error message: **"UDP port 53 unreachable"**. This message indicates that the DNS query sent to the DNS server on **UDP port 53** was not successfully delivered because the DNS service was not reachable.

- **Port 53** is specifically used for **DNS queries** (Domain Name System).
- The most likely issue is that the DNS server is either down, misconfigured, or blocked by a firewall, preventing the DNS query from resolving the requested domain.

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

Time incident occurred: The incident occurred today afternoon at **1:24:32.192571 p.m.**.

How the IT team became aware of the incident: Several customers reported that they could not access the client's website (`www.yummyrecipesforme.com`). Instead of the webpage loading, they received an error message: **"destination port unreachable"**, suggesting a DNS resolution failure.

Actions taken by the IT department: The network security team used the **tcpdump** network protocol analyzer to capture the network traffic. The logs showed that when a DNS query was sent to the DNS server, the client received an **ICMP error response** stating that **UDP port 53** was unreachable.

Key findings:

- The DNS queries from the client system to the DNS server (IP: 203.0.113.2) over **UDP port 53** failed.
- The ICMP error response came from the DNS server's IP (203.0.113.2), confirming that **port 53** was not available for DNS queries.

Likely cause of the incident: The most likely cause of this issue is that the DNS server at **203.0.113.2** is either **down**, **misconfigured**, or **not listening** on UDP port 53. Alternatively, a **firewall** or **security policy** on the network might be blocking access to UDP port 53