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 **affected network protocol** is **DNS (Domain Name System), which operates over UDP on port 53**. Because DNS is not resolving the website's IP address, users cannot access `www.yummyrecipesforme.com`.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:

The port noted in the error message is used for: UDP on port 53

The most likely issue is: **DNS server at 203.0.113.2 is down or misconfigured**, preventing it from responding to DNS queries.

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

Time incident occurred: 13:24 PM

Explain how the IT team became aware of the incident: The IT team became aware of the incident through **customer complaints**, then confirmed the issue using **network analysis tools**, which revealed that **DNS resolution was failing due to an unreachable DNS server on UDP port 53**.

Explain the actions taken by the IT department to investigate the incident: The IT department analyzed reports, tested access, used **tcpdump**, found ICMP errors on **UDP port 53**, and escalated the issue.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The IT department found that **UDP port 53 on DNS server 203.0.113.2 was unreachable**, causing DNS resolution failure.

Note a likely cause of the incident: DNS server failure or misconfiguration