Cybersecurity Incident Report

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The **DNS and ICMP traffic log** revealed that **UDP port 53 on the DNS server (203.0.113.2) was unreachable**, preventing DNS queries from resolving domain names. As a result, users were unable to access `www.yummyrecipesforme.com`. The **ICMP error message "udp port 53 unreachable"** confirmed that the DNS server was either down or misconfigured.

Part 2: Explain your analysis of the data and provide at least one cause of the incident
During the investigation, **tcpdump** was used to analyze network traffic. The logs showed that when a **DNS query** was sent via **UDP to port 53** on the DNS server (`203.0.113.2`), the request failed, and an **ICMP error message** was returned instead. The specific error, **"udp port 53 unreachable,"** indicates that the server was not accepting DNS queries. This suggests that the **DNS resolution process was disrupted**, preventing the browser from retrieving the IP address for `www.yummyrecipesforme.com`. Since DNS is essential for translating domain names into IP addresses, users were unable to access the website. A **likely cause** of this issue is that the **DNS server was down, misconfigured, or blocked by a firewall**. Possible reasons include: 1. **DNS Service Failure** – The DNS server may not have been running or crashed. 2. **Firewall or Network Policy Issues** – A firewall or security setting might have blocked **UDP traffic on port 53**, preventing queries from reaching the server. 3. **Server Overload or Network Connectivity Problems** – The DNS server may have been overwhelmed with requests or suffered from network issues, making it unreachable.