# Cybersecurity Incident Report: Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log. |
| --- |
| 1. As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address of the website " yummyrecipesforme.com". The ICMP(Internet Control Message Protocol) was used to respond with an error message indicating issue contacting the DNS server.<br><br>2. The first two lines of the log showing that my IP(192.51.100.15.52444) is sending request to DNS server(203.0.113.2.domain). The third and fourth lines showing that ICMP error message from the DNS server responding to my browser of every log event.<br><br>3. The error message(udp port 53 unreachable). Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the "A?" symbol indicates flags with performing DNS protocol operations.<br><br>4. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval. |

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

**Time incident occurred:** 13:24:32 (1:24 p.m.)

**Explain how the IT team became aware of the incident:** Customers notified the organization that they received the message "destination port unreachable" when they attempted to visit the website yummyrecipesforme.com.

**Explain the actions taken by the IT department to investigate the incident:** The cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again.

**Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):** In our investigation into the issue, we conducted packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable.

**Note a likely cause of the incident:** The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. DNS server might be down due to a successful Denial of Service attack or a misconfiguration.