# 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 DNS requests sent to the server at 203.0.113.2 resulted in ICMP error messages.

This is based on the results of the network analysis, which show that the ICMP error message "udp port 53 unreachable" was returned when attempting to query the DNS server.

The port noted in the error message, UDP port 53, is used for Domain Name System (DNS) services, which are responsible for resolving domain names into IP addresses.

The most likely issue is that the DNS server at 203.0.113.2 is either not operational, is misconfigured, or is blocked by a network device such as a firewall.

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

### Time incident occurred:

The initial DNS query was sent at 13:24:32. ICMP error messages were returned at 13:24:36, with additional attempts logged at 13:26:32 and 13:28:32.

### Explain how the IT team became aware of the incident:

Several customers reported being unable to access the client’s website, www.yummyrecipesforme.com. The IT team attempted to reproduce the issue and observed the same 'destination port unreachable' error.

### Explain the actions taken by the IT department to investigate the incident:

The IT team utilized tcpdump to capture network traffic and analyze the interaction between the client machine and the DNS server at 203.0.113.2. The analysis focused on UDP and ICMP traffic.

### Note key findings of the IT department's investigation:

1. DNS queries sent to 203.0.113.2 over UDP port 53 were undelivered.

2. The DNS server responded with ICMP error messages indicating that UDP port 53 was unreachable.

3. Multiple attempts to query the DNS server resulted in the same error, confirming a persistent issue.

### Note a likely cause of the incident:

The issue is likely caused by one of the following:

1. DNS service outage on the server at 203.0.113.2.

2. Firewall rules or network policies blocking UDP port 53 traffic.

3. Server misconfiguration or maintenance activities affecting the DNS service.