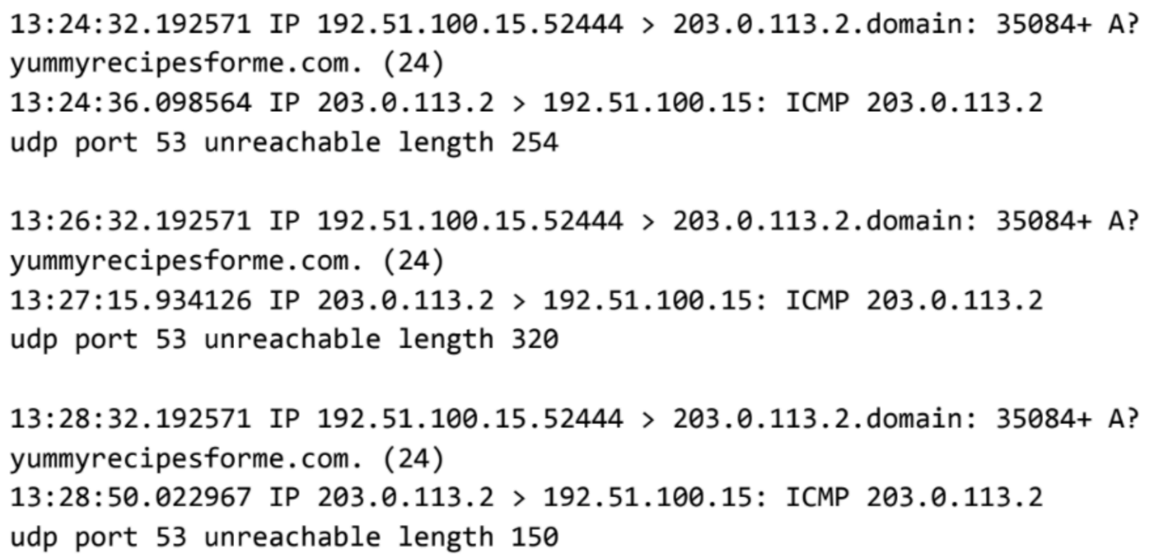

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Cybersecurity Incident Report

This report **example** is for a different security event than the scenario presented in the activity. This example should only be used to familiarize yourself with the expected report format.

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
● Several customers reported being unable to access the client’s website (**www.yummyrecipesforme.com**). ● Users encountered the error message: **“Destination port unreachable.”** ● A network analysis was conducted using **tcpdump**, which revealed ICMP error messages indicating **UDP port 53 unreachable** when attempting to resolve the domain name.

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

- To investigate, a network analysis was conducted using **tcpdump**, which revealed that when the browser attempted to query the DNS server via **UDP (port 53)** to resolve the domain name, the response was an **ICMP error message** indicating that UDP port 53 was unreachable. The repeated occurrence of this error suggests that the DNS service was unavailable at the time of testing.

- Based on the log analysis, the issue likely stems from a **misconfigured DNS server** or a **DNS service failure**, which could be due to the DNS server being down, firewall rules blocking UDP port 53, or an incorrect DNS configuration. The incident was first reported at **1:24 PM**, as indicated by the timestamp **13:24:32.192571** in the log. The sequence of events shows that multiple attempts to reach the DNS server resulted in the same ICMP error response, confirming a persistent issue with DNS resolution.

- The current status remains unresolved, and security engineers have been informed for further investigation. To mitigate the issue, we are trying to **verify the DNS server status**, **firewall configurations**, **restart the DNS service**, **monitor network traffic**, and **notify affected users**.