# 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:<br><br>**A request from my machine (192.51.100.15) was sent to the DNS server (203.0.113.2) on port 53 to access the site yummyrecipesforme.com.**<br><br>This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:<br><br>**“udp port 53 unreachable”**<br><br>The port noted in the error message is used for:<br><br>**This error message is used for reporting that a domain is not able to connect via the DNS.**<br><br>The most likely issue is:<br><br>**The DNS server, 203.0.113.2, is having a connection error and needs to be reestablished with the DNS service provider.**<br><br>**OR**<br><br>**The DNS service provider is having connection issues and needs to be reestablished in order to return service to the server, 203.0.113.2.** |

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred:<br><br>**An incident occurred at 1:24PM (32 sec.).**<br>**A second incident occurred at 1:26PM (32 sec.) and 1:27PM (15 sec.).**<br>**A third incident occurred at 1:28PM (32 sec.)/(50 sec.).** |

Explain how the IT team became aware of the incident:

**Some users tried to connect to yummyrecipesforme.com (203.0.11.2) and reported it to an analyst. I confirmed that error and began troubleshooting the issue.**

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

**A team member used tcpdump in order to begin investigating the route of a request to the domain, 203.0.11.2.**

**A team member observed the backend of the error in real-time, noting a connection issue on the DNS server's side.**

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

**DNS Server IP: 203.0.11.2**
**Port affected: UDP 53**
**Response from the server: ICMP timed out/unreachable**

```
o-taylor-bryant@taylor-terminal:~$ dig yummyrecipesforme.com
;; communications error to 203.0.113.2#53: timed out
;; communications error to 203.0.113.2#53: timed out
;; communications error to 203.0.113.2#53: timed out

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> yummyrecipesforme.com
;; global options: +cmd
;; no servers could be reached
```

Note a likely cause of the incident:

**The domain could be configured incorrectly and this would prevent the webpage from loading.**

**OR**

**The domain service is not running at all.**