# 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 server is unreachable through port 53. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message “udp port 53 unreachable length 254”. The port noted in the error message is used for DNS requests to get IP addresses. The most likely issue is: The DNS server is down. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred, Before 13:24 where several customers of our client who runs [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) , reported that they were not able to access the client company website. The IT department investigated the incident by visiting the website using tcpdump and encountered the same error “udp port 53 unreachable length 254”.  We are continuing to investigate the root cause of the issue to determine how we can restore access to the server.Our next step is to check if the server as any issues or the Firewall had a Improper security block to port 53 or if there was a DOS attack.Most likely cause of the incident should be, Improper security block to port 53 , DNS Service Down, DOS attack. |