# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| UDP protocol was used to contact the DNS server to retrieve the IP address of the domain name “[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)”. In response, the ICMP protocol was used with an error message: ICMP 203.0.113.2 udp port 53 unreachable, indicating issues contacting the DNS server  The result of the network analysis shows that the 3rd and 4th line of the the log event is the response of the DNS server which states an ICMP error with an error message “udp port 53 unreachable”  The most likely issue is that the DNS server is not responding. Which is further supported by a “A?” flag response | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 PM  Several customers reported that they cannot access the client website “[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)” and saw the error “destination port unreachable”  The response team’s first action was to access the website and found the same error message reported by the customers, then the response team then used a network analyzer tool, tcdump, and attempted to access the webpage again.  The result of the network analyzer tool is that udp port 53 is unreachable  The most likely issue is that the DNS server might be down due to Denial of Service attack(DoS) or misconfiguration. |