# 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 was used to contact the DNS server to retrieve the IP address of ‘yummyrecipesforme.com’. This is shown in the first two lines of the log file. The 3rd and 4th lines of the log file show that the ICMP protocol was used to respond with an error message that port 53 was unreachable. Port 53 is used for DNS protocol traffic, so this indicates that there was an issue with the DNS server. The ‘A?’ and ‘+’ symbols in the UDP message further indicate that there are flags associated with performing DNS protocols. Because of the message pertaining to port 53 and the flags, it is likely that the DNS server is down. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The problem was first reported at 1:24 pm. Customers informed the organization that they were receiving an error message when attempting to connect to the website ‘yummyrecipesforme.com’. This message was replicated with me connecting, and further replicated while connected with tcpdump. The cybersecurity team is currently investigating this issue. The message and the UDP messages indicate that there is a problem with the DNS server. Discovering whether the server is truly down or there are firewall problems preventing access to port 53 is the next step in correcting this problem. This could have been the result of a successful DOS attack or a misconfiguration from a firewall admin. |