# 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 for the given website. Here ICMP protocol was used to respond with an error message if there are any issues with connecting with a DNS server. A UDP message going from browser to server is shown in the first two lines of every log event. The error message that is ICMP message is shown in third and fourth line of every log event with error message “udp port 53 is unreachable ”but port 53 is associated with DNS protocol traffic, we can definitely say that it is issue from DNS server.the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The incident occurred today at 1:24 p.m. Customers notified the organization that they are receiving the message “destination port unreachable” when they attempt to visit the website yummyrecipesforme.com. The cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration. |