# 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: Requests to port 53 (DNS) of the URL “[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)” are failing and returning the error “destination port unreachable”.  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”  The port noted in the error message is used for: DNS  The most likely issue is: The DNS service of the web host is down or misconfigured | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 PM  Explain how the IT team became aware of the incident: Clients reported when attempting to access the client’s company URL “[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)” they were served the error “destination port unreachable”  Explain the actions taken by the IT department to investigate the incident: We first tried to access the website ourselves and received the same error reported by the clients. From there we reconnected using the network analyzer tool “tcpdump” to capture the traffic received back from the client’s web server for analysis.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): It seems the DNS service of the client website is unreachable.  Note a likely cause of the incident: The DNS service could be down or misconfigured |