# 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: **the initial ip address request to yummyrecipersforme.com was sent to the DNS server.**  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: **port 53 unreachable**  The port noted in the error message is used for: **DNS**  The most likely issue is: **the DNS server for yummyrecipersforme.com is not functioning properly.** | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1**:24 pm 32.192571 seconds**  Explain how the IT team became aware of the incident: **Several customers reported the error code to the Security Department**  Explain the actions taken by the IT department to investigate the incident: **The first course of action was to connect to the website via a web browser. After confirming the issue, a network analyzer tool was used to capture packets after trying to connect to the website again.**  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **According to the network analyzer tool, the request for the website’s ip address was never fulfilled.**  Note a likely cause of the incident: **The likely cause of this is the website’s DNS server not working properly. Perhaps it is being overloaded by packets from a DoS attack.** |