# 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: **port 53 is unreachable**  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  **port is unreachable**  The port noted in the error message is used for: **53**  The most likely issue is: **server or service is down** |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: **13:24:32 – 13:28:50 when investigation of issue occurred**  Explain how the IT team became aware of the incident: **Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com**  Explain the actions taken by the IT department to investigate the incident: **used the following tools**  **network analyzer tool, tcpdump, and attempted to load the webpage again.**  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **Unable to resolve company website www.yummyrecipesforme.com to IP address**  Note a likely cause of the incident: **service failure or server is offline.** |