# 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: DNS queries to port 53 were not deliverable because the server responded with ICMP ‘port unreachable’ messages.”  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 length 254  The port noted in the error message is used for: port 53  The most likely issue is: there is an issue with the dns server such as the server is currently down. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 p.m., 32.192571 seconds  Explain how the IT team became aware of the incident: We became aware of the incident when several clients of [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) reported they were unable to load the webpage and received the error message “destination port unreachable”  Explain the actions taken by the IT department to investigate the incident: We first visited the webpage to double check the error. We also received the same error “destination port unreachable”. We then loaded our network protocol analyzer and loaded the webpage again. We then received the information from the packet as per the logs. We kept trying be received the same errors.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Port 53 affected from the DNS server.  Note a likely cause of the incident: A likely cause is the server is DNS service for 203.0.113.2 is down therefore we are unable to connect. There could also be a firewall blocking port 53. |