# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log | |
| --- | --- |
| The network protocol analyzer was unable to access port 53 which is used for DNS interactions in the network. Being unable to establish a TCP connection. This could be because a firewall is blocking access to the port or the DNS server for the destination network is down. | |
|

| Part 2: Explain your analysis of the data and provide one solution to implement |
| --- |
| This incident occurred earlier in the afternoon when an employee was attempting to make a request to yummyrecipesforme.com. The network security team responded and began tests using the network protocol analyzer tool tcpdump. The logs show that the port 53, which is used for DNS, was unreachable. Possible causes for it are the DNS server being down or a firewall preventing access to the port. We are still investigating by changing firewall configuration and checking the servers for outages. |