# 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 down or unreachable when trying to access the website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “udp Port 53 is unreachable”  The port noted in the error message is used for: DNS protocol traffic.  The most likely issue is: that the DNS server was not responding. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: at 1:24pm  Explain how the IT team became aware of the incident: several customers called in the incident to the company when they were not able to reach the website.  Explain the actions taken by the IT department to investigate the incident: visited the website and was met with the error “destination port unreachable”. Used the Network analyzer tool, tcpdump and loaded it to the site.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): using the analyzer showed that when you send UDP packets and receive an ICMP response, the results contain an error message: “udp port 53 unreachable.”  Note a likely cause of the incident: the likely cause might have been a Denial of Service attack, or DOS attack, which caused the server to be down and unreachable. |