# 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 UDP protocol was utilized for sending queries from the browser to the DNS server to resolve the IP address of [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 unreachable”  The port noted in the error message is used for: port 53 is typically used for domain name system service (DNS service)  The most likely issue is: The DNS server was unreachable or not listening on port 53, leading to the failure to resolve the IP address for the domain name "[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/)." | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: The incident occurred at 13:24:32.192571 (1:24 p.m. and 32.192571 seconds).  Explain how the IT team became aware of the incident: The IT team became aware of the incident when several customers reported that they were unable to access the client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/) and received the error message "destination port unreachable." Subsequently, the cybersecurity analyst attempted to visit the website and encountered the same error.  Explain the actions taken by the IT department to investigate the incident: The IT department utilized a network protocol analyzer tool, tcpdump, to capture and analyze the traffic. They observed the communication between the browser and the DNS server, noting the UDP packets sent for DNS queries and the ICMP echo replies returning the error message "udp port 53 unreachable."  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * The ICMP echo replies returning the error message "udp port 53 unreachable." * The affected port being port 53, which is commonly associated with DNS service. * The DNS server's IP address being 203.0.113.2.   Note a likely cause of the incident:  A likely cause of the incident is that the DNS server was either down or misconfigured, leading to it being unreachable or not listening on port 53. This resulted in the failure to resolve the IP address for the domain name "[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/)." |