# Cybersecurity Incident Report: Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the tcpdump log |
| The 192.51.100.15.52444 > 203.0.113.2.domain indicates that the packet was sent from the local computer to the DNS server requesting IP address of yummyrecipesforme.com. The packet was sent using the UDP protocol.  The packet is sent at 1:24 p.m, and a response arrives soon as an ICMP packet. The error message udp port 53 unreachable indicates that the message was not received by the DNS server’s port 53. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred at 1:24 p.m. The problem is that the DNS server’s port 53 was unreachable. Thus any access to the website would not have been possible. This suggests that either the DNS server was not functional or traffic to port 53 was blocked. If the DNS server was not functional, it could have been due to a misconfiguration, or a DOS attack. |