# Cybersecurity Incident Report: Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the tcpdump log |
| The DNS request to resolve *yummyrecipesforme.com* used the UDP protocol, but the DNS server responded with an ICMP error: “**udp port 53 unreachable**.” Since port 53 handles DNS traffic, this indicates a DNS server issue. The outgoing UDP message includes multiple flags, further confirming a problem with DNS resolution. Based on the ICMP response and message flags, it's highly likely the DNS server is unresponsive. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred today at 1:24 p.m., when customers reported receiving a “destination port unreachable” error while trying to access *yummyrecipesforme.com*. The cybersecurity team is actively investigating to restore access. Packet sniffing using tcpdump revealed that DNS port 53 is unreachable. The next step is to determine whether the DNS server is down or if firewall rules are blocking traffic to port 53. Possible causes include a Denial of Service (DoS) attack or DNS server misconfiguration. |