# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The network traffic log revealed the use of **UDP** for DNS resolution and **ICMP** for error responses.  The system attempted to contact the DNS server on **port 53**, but received **ICMP “port unreachable”** messages.  This suggests the DNS server was either **down**, **misconfigured**, or **blocking port 53 traffic**, causing DNS resolution to fail and the website to become inaccessible. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| * The issue was first reported by users who saw a **“destination port unreachable”** error while visiting www.yummyrecipesforme.com. * On investigation, the browser first sent a DNS query (UDP on port 53), which failed. * tcpdump logs showed **ICMP “udp port 53 unreachable”**, meaning the DNS server was **not reachable** or **not responding**. * This prevented DNS name resolution, so the website could not load. * **Suspected root cause**: DNS server was down, misconfigured, or port 53 traffic was being blocked. * **Recommended solution**: Check the DNS server’s configuration and firewall rules. Ensure that it’s reachable on port 53 UDP. Use an alternative DNS resolver if needed. |