# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| According to the UDP protocol, the DNS server is unreachable. The ICMP error detailed the error “udp port 53 unreachable”, which could indicate that the DNS server is down since port 53 is a commonly used DND network trafficking port – but the DNS server not working is very unlikely. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| Using tcpdump, I conducted packet sniffing tests to verify that the UDP protocol was being used, and that traffic to the DNS server on port 53 was unreachable. A solution to this would be to determine if the issue is either the DNS server itself, or if traffic to port 53 is restricted by a firewall. Some further analysis to rule out DoS attacks would be essential as well. |