# 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 that the dns server can’t be reached.  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 53 noted in the error message is used for DNS service.The most likely issue is that the dns server is not responding | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred:The incident occured this afternoon at about 13:24 pm . The customers contacted the company to report that they were not able to access the website . The IT department immediately began to investigate the matter so as to restore business continuity . In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whetherthe DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack |