# 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 UDP protocol reveals the IP address for the domain name yummrecipesforme.com  **This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:**  The last two lines of each log event repeatedly showed the same error “udp port 53 unreachable.”  **The port noted in the error message is used for:**  The port is used for DNS traffic like query requests; therefore the issue resides in the DNS server.  **The most likely issue is:**  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:**  13:24.32.192571 or 1:24pm  **Explain how the IT team became aware of the incident:**  The IT team became aware due to many complaints from clients of not being able to reach the website yummyrecipesforme.com.  **Explain the actions taken by the IT department to investigate the incident:**  IT is following with UPD protocol by performing a tcpdump.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The tcpdump revealed that port 53 was unreachable.  Note a likely cause of the incident: Because port 53 is connected to the DNS server, that means the likely cause is either the DNS server is down or a possible DoS attack. |