Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The network protocol analyser logs indicate that UDP port 53 is unreachable when UDP packets are sent to the DNS server requesting the IP address of yummyrecipesforme.com. This may indicate that the DNS server has been compromised and is not functioning as expected.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident happened earlier this afternoon at 13:24 when it was reported by users that they could not access the website - “destination port unreachable”. The network security team investigated the issue and started running tests by analysing ICMP responses seen in tcpdump logs. It was discovered from the logs that port 53 was unreachable. By looking into firewall configurations it can be revealed whether port 53 has been blocked due to a misconfiguration or if a DoS attack is taking place.