Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

During the network analysis the UDP protocol has revealed that the indicated port 53 is unreachable when accessing the company website at www.yummyrecipesforme.com. DNS uses port 53 to transfer packets through UDP. This may indicate a problem with the DNS web server and an attack from a threat actor to overwhelm the company server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The incident first occurred at 1:24pm when several customers complained that our website cannot be reached. To be sure of the situation I tried to access the website myself and I got an error that the destination port is unreachable. The IT team has conducted packet sniffing to analyze the same website using the TCPdump network analysis tool to investigate the incident. In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whether the 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 or a misconfiguration.