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 connectivity to www.yummyrecipesforme.com is down. 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 noted in the error message is port 53, which is commonly used for DNS protocol traffic. The most likely issue is a misconfiguration. It is possible that this is a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The time the incident occurred was 1:24pm. Several customers contacted the company to report that they were not able to access the company’s website www.yummyrecipesforme.com. When they attempted to access the site, they received the error message “destination port unreachable”. The IT department attempted to access the site the same way as the customers and received the same error message. Then the IT department performed packet sniffing tests using tcpdump. The data packets collected from tcpdump showed that DNS port 53 was unreachable. Security engineers are working to resolve the issue. It is possible that a change to firewall settings caused a misconfiguration or that there was a DoS attack.