Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log
The tcpdump log file indicates an issue with Domain Name Service (DNS). The server hosting DNS is responding with an ICMP message indicating the destination is unreachable on port 53. As the DNS is being reported as unreachable, the website domain cannot be resolved to a destination IP address, and the website cannot be loaded in the browser.

Part 2: Explain your analysis of the data and provide one solution to implement
At approximately 1:25 PM several customers contacted us to report that they were not able to access the company website “www.yummyrecipesforme.com”, and saw the error “destination port unreachable” after waiting for the page to load. An analysis of the tcpdump log indicates that the Domain Name Service is not reachable. It was possible to reproduce the error by attempting to exercise the DNS directly. It is likely that the server hosting the DNS is down or otherwise unreachable because of a network issue. As a workaround the client could configure an alternate DNS, such as the Google Public DNS (8.8.8.8).