Cybersecurity Incident Report:
Network Traffic Analysis

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

The analysis of the UDP protocol indicates that the DNS server is likely not operational or cannot be accessed. This conclusion is supported by the outcome of the network analysis, where the ICMP echo reply produced an error statement indicating the unreachability of "udp port 53." Port 53 is the standard port for DNS protocol traffic, making it probable that the DNS server is failing to provide a response.

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

Today at 1:23 p.m., an incident unfolded. Customers reached out to the organization's IT team, reporting that they encountered a "destination port unreachable" message while attempting to access the website. To address this concern and reinstate customer access to the website, the organization's network security experts have initiated an investigation.

During our pursuit of the issue, we conducted packet sniffing tests through the utilization of tcpdump. Analysis of the resulting log file indicated that there was an inability to reach DNS port 53. Our next course of action involves discerning whether this inability stems from the DNS server being inoperative or if it results from the firewall blocking traffic to port 53.

The potential causes for the DNS server's unresponsiveness range from being compromised by a successful Denial of Service attack to encountering misconfiguration issues. Our ongoing investigation aims to pinpoint the root cause accurately.