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 analyzer logs indicate that port 53 is unreachable when attempting to access the website. Port 53 is normally used for DNS Server. This may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of 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 incident occurred in the afternoon around 1:20 pm when several customers reported to the company that they got error message destination port unreachable while waiting for the page to load. The security analyst began running test to analyze the traffic using network protocol analyzer tcpdump. The port 53 is used by DNS server is not reachable. Our next step will be to check the firewall configuration to check if port 53 is blocked and contacting the system administrator to check signs of system being attacked. The DNS server might be down because of Dos attack.