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 the DNS server is down and unreachable. 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 used for DNS protocol traffic. The most likely issue is the DNS Server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:23 PM. The customers called and notified the personnel with the expertise that they had received the message when they attempted to visit the site. The security professionals investigated the issue and conducted packet sniffing tests. In the resulting log file, it was found that DNS port 53 was unreachable. Next, identification as to whether the DNS Port is down or traffic to Port 53 was blocked by the firewall was conducted. The DNS server might be down due to a Denial-of-Service attack or a misconfiguration.