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 few customers were not able to access the client company website www.yummyrecipesforme.com This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message “udp port 53 is unreachable” Port 53 is the default port for DNS. It is the port most web applications expect to find DNS servers, which they use to translate domains into IP addresses. It is possible that this is an indication of a malicious attack on the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred 13:24:32 p.m. when several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. To start, we attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”