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 is used as part of the DNS protocol to retrieve the IP address for the domain name yummyrecipesforme.com. This is implied by the line "A? yummyrecipesforme.com", which represents a DNS A record lookup. The DNS query, sent over UDP, is visible in the first and second lines of the log. An ICMP error response appears in the third and fourth lines, containing the message "udp port 53 unreachable". This indicates that the DNS server could not be reached on port 53. The query includes 35084+, where the + signifies that the Recursion Desired flag was set. This means the client expected the DNS server to actively process the request and return a full response. However, no response was received from the DNS server. Instead, an ICMP error was returned, suggesting that the DNS server is likely not responding or unreachable.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
At approximately 1:24 p.m. today, customers reported receiving a “destination port unreachable” error when attempting to access the website yummyrecipesforme.com. The cybersecurity team supporting the client organization is currently investigating the issue to restore access. As part of the investigation, packet sniffing was conducted using tcpdump. The resulting logs revealed that DNS traffic over port 53 was unreachable. The next step is to determine whether the DNS server is offline or if traffic to port 53 is being blocked by a firewall. Possible causes include a successful Denial of Service (DoS) attack or a misconfiguration on the DNS server.