Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network analysis indicates that UDP port 53, which is typically used for DNS (Domain Name System) communication, is unavailable. This conclusion is based on an ICMP echo reply that returned the error message: "UDP port 53 unreachable, length 254." This message suggests that no service was actively listening on UDP port 53 at the destination. As a result, the DNS request for the domain www.yummyrecipesforme.com could not be processed, likely because it failed to reach a functioning DNS server. This implies that the DNS server at the receiving end may be down or misconfigured, preventing successful name resolution.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
In the afternoon, several customers reported that they were unable to access the client company's website, www.yummyrecipesforme.com. Upon attempting to load the page, they encountered the error message "destination port unreachable", indicating a connectivity issue. These user complaints alerted the IT team to a potential incident. The matter was escalated to the company's cybersecurity analyst, who promptly began an investigation. To analyze the issue, the analyst utilized tcpdump, a powerful packet capture tool, to monitor network traffic. The captured data revealed that UDP port 53, which is designated for DNS (Domain Name System) queries, was unreachable. This port is essential for domain name resolution, allowing users to access websites using human-readable URLs. The key finding of the investigation was that no service was listening on UDP port 53, resulting in the failure of DNS queries. Without DNS resolution, users were unable to translate the domain name into its corresponding IP address, effectively making the website inaccessible. The most likely cause of the incident was that the receiving DNS server was either down, misconfigured, or otherwise inaccessible, preventing DNS traffic from being processed and leading to service disruption for users attempting to visit the website.