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 client's browser attempted to request the IP address of the domain "http://www.yummyrecipesforme.com" by sending UDP packets to the DNS server. However, the ICMP error message "udp port 53 unreachable" was returned by the DNS server. This indicates that the UDP packet did not reach its destination because the DNS service on port 53 was unavailable. The error message specifically points to the DNS service port, which is commonly used for DNS queries. Consequently, the most likely issue is the unavailability or failure of the DNS service on port 53, leading to the UDP packet requesting the IP address being unreachable.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 13:24:32.192571 (1:24 p.m.). The IT team became aware of the issue when customers reported being unable to access the client company website, http://www.yummyrecipesforme.com, and received the error message "destination port unreachable." In response, the IT department investigated using a network protocol analyzer tool, tcpdump, to capture and analyze the network traffic between the client's browser and the DNS server. Analysis of the captured packets revealed that the DNS server returned ICMP error messages indicating that the UDP packets sent to port 53 were unreachable. This suggests that the DNS service on port 53 was either unavailable or not listening for incoming requests. The likely cause of the incident is a failure or misconfiguration of the DNS service on port 53, potentially due to network configuration issues, server misconfigurations, or service disruptions.