Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problems found in the DNS and ICMP traffic log.
The UDP protocol reveals that DNS queries for the domain "yummyrecipesforme.com" were unsuccessful. The ICMP error messages returned indicate that UDP port 53, which is used for DNS traffic, is unreachable. This suggests that there may be an issue with the DNS server or a network configuration problem blocking access to DNS services. The port noted in the error message is used for DNS queries (UDP port 53). The most likely issue is that UDP port 53 on the DNS server (203.0.113.2) is being blocked or is experiencing an issue, preventing successful DNS resolution.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred between 13:24:32 and 13:28:50, as observed in the tcpdump logs. The IT team became aware of the issue when users began reporting that they could not access the website "yummyrecipesforme.com." The inability to resolve the domain name indicated a possible DNS issue. The IT department responded by first verifying the Problem by trying to access the website and then analyzing the network traffic using tcpdump. The team reviewed the logs and observed multiple failed DNS queries for "yummyrecipesforme.com," all of which were met with ICMP "UDP port 53 unreachable" error messages from the DNS server (203.0.113.2). The DNS queries to 203.0.113.2 were repeatedly unsuccessful. ICMP messages showed that UDP port 53 on the DNS server was unreachable, indicating a potential firewall or network misconfiguration issue. No signs of a malicious attack were detected in the logs, but further investigation into the network configuration was recommended. The most likely cause of the incident is a misconfigured firewall or network device blocking UDP port 53. A DoS attack could also be a possibility, overwhelming the DNS server. Further investigation is needed to resolve the issue.