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 the UDP protocol shows an ICMP echo reply error message: "UDP port 53 unreachable." Port 53, as indicated in the error, is used for Domain Name System (DNS) services. The most probable cause of the issue is that the port is either closed or filtered, and DNS functionality is not enabled.

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 indicated by the timestamps. The IT team became aware of the issue when customers reported being unable to access the client company's website, www.yummyrecipesforme.com. In response, the IT department used TCPDump, a network analysis tool, to troubleshoot and attempt to replicate the incident. The investigation revealed that the IT team made three attempts to access the website at the IP address 203.0.113.2. However, each attempt resulted in an error message stating, "UDP port 53 unreachable." This suggested that DNS resolution was being blocked or interrupted. The most likely cause of the incident is that UDP port 53 is either closed or filtered, which would prevent proper DNS functionality. Several factors may have contributed to this issue, including a firewall blocking the port, the DNS server being down due to a Denial of Service (DoS) attack or misconfiguration, or the Internet Service Provider (ISP) intentionally blocking the port. The team will continue to investigate root cause.