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 server to which the request is being sent is not responding. - This is based on the network analysis results, which show that the ICMP echo reply returned the error message UDP port 53 unreachable. - The port noted in the error message is used for DNS servers. - The most likely issue is that the DNS server is unreachable.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
- Time incident occurred: 13:24-13:28 - The IT team became aware of the incident when several customers reported that they could not access the client company website, www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load. - The IT department's actions to investigate the incident were checking the logs and updating the team leader and the Engineering team. - Some Key findings of the IT department's investigation are that while the server was down from 13:24 to 28, three DNS requests were sent. - The incident is likely caused by the server being down or the specific port(53) being blocked. The server might be down due to a successful Dos attack.