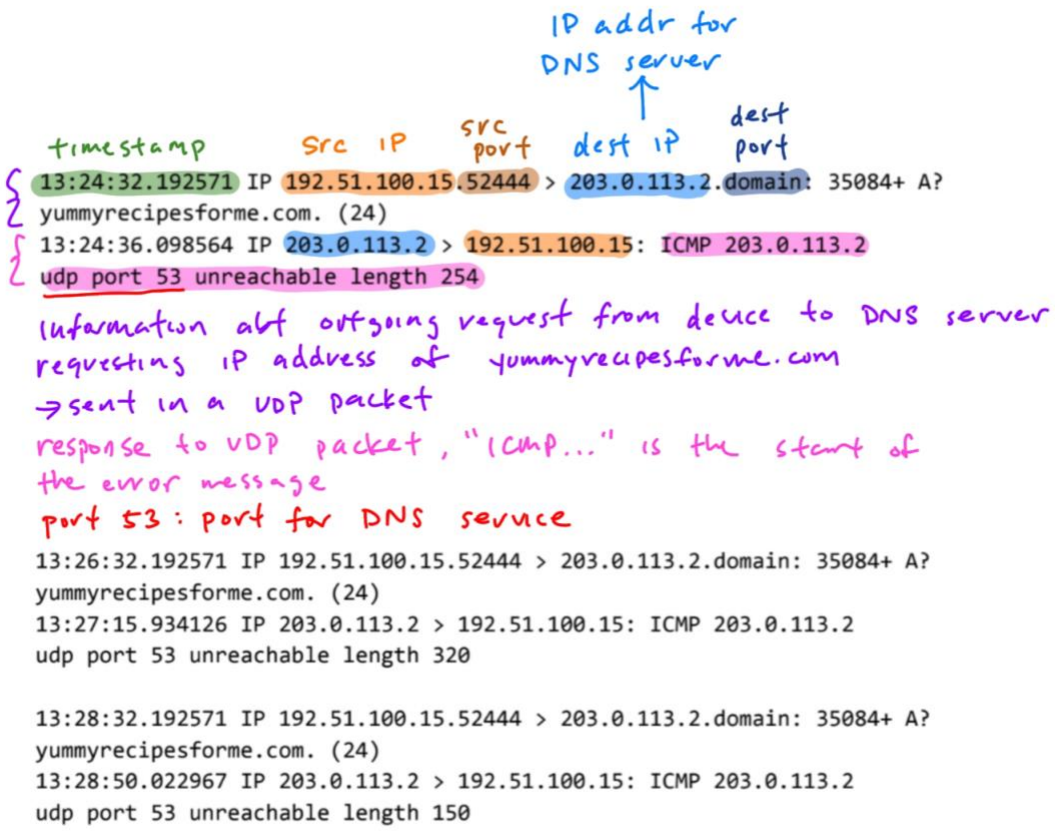
Cybersecurity Incident Report: Network Traffic Analysis



Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that the request for the IP address for "yummyrecipesforme.com" did not reach the DNS server because no service was listening on the receiving DNS port. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message "203.0.113.2 udp port 53 unreachable length 254" The port noted in the error message is used by the DNS protocol to retrieve the IP address of the target website (yummyrecipesforme.com) The most likely issue is an ICMP flood.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 13:24:32 (1:24:32 PM) The IT team became aware of the incident after customers of the client (yummyrecipesforme) reported that they were not able to access the client's website. Explain the actions taken by the IT department to investigate the incident: Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The logs show that port 53 of the DNS server is unreachable, blocking the customer's ability to access the client's website. This incident is likely caused by an outsider who instigated an ICMP flood against the server, overflowing the network traffic and causing the server to crash.