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: Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: Destination port 53 unreachable. The port noted in the error message is used for: The UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port. The most likely issue is: This may indicate a malicious attacker doing DDOS.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 p.m., 32.192571 seconds Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com

Explain the actions taken by the IT department to investigate the incident:
Attempted to visit the website and receive the error “destination port unreachable.”

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

Note a likely cause of the incident: